Adaptively Secure ABE for DFA from k-Lin and More

Junqing Gong[1,2,⋆] and Hoeteck Wee[2,⋆⋆]

[1] East China Normal University

[2] CNRS, ENS and PSL

{jgong,wee}@di.ens.fr

Abstract. In this work, we present:

– the first adaptively secure ABE for DFA from the k-Lin assumption in prime-order bilinear groups; this resolves one of open problems posed by Waters [CRYPTO'12];
– the first ABE for NFA from the k-Lin assumption, provided the number of accepting paths is smaller than the order of the underlying group; the scheme achieves selective security;
– the first compact adaptively secure ABE (supporting unbounded multi-use of attributes) for branching programs from the k-Lin assumption, which generalizes and simplifies the recent result of Kowalczyk and Wee for boolean formula (NC1) [EUROCRYPT'19].

Our adaptively secure ABE for DFA relies on a new combinatorial mechanism avoiding the exponential security loss in the number of states when naively combining two recent techniques from CRYPTO'19 and EUROCRYPT'19. This requires us to design a selectively secure ABE for NFA; we give a construction which is sufficient for our purpose and of independent interest. Our ABE for branching programs leverages insights from our ABE for DFA.

— Contents —

§1. Introduction, 1 §2. Preliminaries, 9 §3. DFA, NFA, and their Relationships, 10 §4. Semi-adaptively Secure ABE for NFA$^{\oplus p}$, 11 §5. Adaptively Secure ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ and DFA, 25 §6. Compact Adaptively Secure ABE for Branching Programs, 33 §A. An Example for Back-tracking Attack, 46 §B. Basic ABE for NFA$^{\oplus p}$ from ℓ-EBDHE assumption, 47 §C. An Example for Reversing DFA, 50 §D. Missing Material from Section 4, 51 §E. Missing Material from Section 5, 52 §F. Concrete ABE for DFA with Adaptive Security, 65 §G. Missing Material from Section 6, 66 §H. Concrete ABE for Branching Program with Adaptive Security, 71 §I. Adaptively Secure CP-ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ and DFA, 72 §J. Adaptively Secure CP-ABE for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$ and BP, 76

1 Introduction

Attribute-based encryption (ABE) [19,12] is an advanced form of public-key encryption that supports fine-grained access control for encrypted data. Here, ciphertexts are associated with an attribute x and keys with a policy Γ; decryption is possible only when $\Gamma(x) = 1$. One important class of policies we would like to support are those specified using deterministic finite automata (DFA). Such policies capture many real-world applications involving simple computation on data of unbounded size such as network logging application, tax returns and virus scanners.

Since the seminal work of Waters [21] introducing ABE for DFA and providing the first instantiation from pairings, substantial progress has been made in the design and analysis of ABE schemes for DFA [4,5,1,11,2,3], proving various trade-offs between security assumptions and security guarantees. However, two central problems posed by Waters [21] remain open. The first question pertains to security and assumptions:

> ***Q1**: Can we build an ABE for DFA with adaptive security from static assumptions in bilinear groups, notably the k-Lin assumption in prime-order bilinear groups?*

[⋆] Supported by NSFC-ISF Joint Scientific Research Program (61961146004) and ERC Project aSCEND (H2020 639554).
[⋆⋆] Supported by ERC Project aSCEND (H2020 639554).

From both a practical and theoretical stand-point, we would like to base cryptography on weaker and better understood assumptions, as is the case with the k-Lin assumption, while also capturing more realistic adversarial models, as is the case with adaptive security. Prior ABE schemes for DFA achieve either adaptive security from less desirable q-type assumptions [21,4,5,1], where the complexity of the assumption grows with the length of the string x, or very recently, selective security from the k-Lin assumption [2,11]. Indeed, this open problem was reiterated again in the latter work [11], emphasizing a security loss that is polynomial (and not exponential) in the size of the DFA.

The next question pertains to expressiveness:

> ***Q2****: Can we build an ABE for nondeterministic finite automata (NFA) with a polynomial dependency on the NFA size?*

The efficiency requirement rules out the naive approach of converting a NFA to a DFA, which incurs an exponential blow-up in size. Here, we do not know any construction even if we only require selective security under q-type assumptions. Partial progress was made very recently by Agrawal *et al.* [3] in the more limited secret-key setting, where encryption requires access to the master secret key. Throughout the rest of this work, we refer only to the standard public-key setting for ABE, and where the adversary can make an a-priori unbounded number of secret key queries.

1.1 Our Results

In this work, we address the afore-mentioned open problems:

- We present an adaptively secure ABE for DFA from the k-Lin assumption in prime-order bilinear groups, which affirmatively answers the first open problem. Our scheme achieves ciphertext and key sizes with linear complexity, as well as security loss that is polynomial in the size of the DFA and the number of key queries. Concretely, over the binary alphabet and under the SXDH (=1-Lin) assumption, our ABE for DFA achieves ciphertext and key sizes 2–3 times that of Waters' scheme (cf. Fig 4), while simultaneously improving on both the assumptions and security guarantees.
- We present a selectively secure ABE for NFA also from the k-Lin assumption, provided the number of accepting paths is smaller than p, where p is the order of the underlying group. We also present a simpler ABE for NFA with the same restriction from the same q-type assumption used in Waters' ABE for DFA. Both ABE schemes for NFA achieve ciphertext and key sizes with linear complexity.
- Finally, we present the first compact adaptively secure ABE for branching programs from the k-Lin assumption, which generalizes and simplifies the recent result of Kowalczyk and Wee [15] for boolean formula (NC1). Here, "compact" is also referred to as "unbounded multi-use of attributes" in [5]; each attribute/input bit can appear in the formula/program an unbounded number of times. Our construction leverages insights from our ABE for DFA, and works directly with any layered branching program and avoids both the pre-processing step in the latter work for transforming boolean formulas into balanced binary trees of logarithmic depth, as well as the delicate recursive pebbling strategy for binary trees.

We summarize the state of the art of ABE for DFA, NFA and branching programs in Fig 1, 2, 3, respectively.

In the rest of this section, we focus on our three ABE schemes that rely on the k-Lin assumption, all of which follow the high-level proof strategy in [11,15]. We design a series of hybrids that traces through the computation, and the analysis carefully combines (i) a "nested, two-slot" dual system argument [20,16,17,18,13,8], (ii) a new combinatorial mechanism for propagating entropy along the NFA computation path, and (iii) the piecewise guessing framework [14,15] for achieving adaptive security. We proceed to outline and motivate several of our key ideas. From now on, we use GWW to refer to the ABE for DFA by Gong *et al.* [11].

Adaptively secure ABE for DFA. Informally, the piecewise guessing framework [14,15] for ABE adaptive security says that if we have a selectively secure ABE scheme where proving indistinguishability of every pair of adjacent hybrids requires only knowing $\log L$ bits of information about the challenge attribute x, then the same scheme is adaptively secure with a security loss of L. Moreover, when combined with the dual system argument, it suffices to consider selective security when the adversary only gets a single key corresponding to a single DFA.

In the GWW security proof, proving indistinguishability of adjacent hybrids requires knowing the subset of DFA states that are reachable from the accept states by "back-tracking" the computation. This corresponds to $\log L = Q$ — we need Q bits to specify an arbitrary subset of $[Q]$— and a security loss of 2^Q. Our key insight for achieving adaptive security is that via a suitable transformation to the DFA, we can ensure that the subset of reachable states per input are always singleton sets, which correponds to $\log L = \log Q$ and a security loss of Q. The transformation is very simple: run the DFA "in reverse"! That is, start from the accept states, read the input bits in reverse order and the transitions also in reverse, and accept if we reach the start state. It is easy to see that this actually corresponds to an NFA computation, which means that we still need to design a selectively secure ABE for NFA. Also, back-tracking along this NFA corresponds to normal computation in the original DFA, and therefore always reaches singleton sets of states during any intermediate computation.

ABE for NFA. Next, we sketch our ABE for NFA, which uses an asymmetric bilinear group (G_1, G_2, G_T, e) of prime order p where $e : G_1 \times G_2 \to G_T$. As in Waters' ABE for DFA [21], an encryption of $x = (x_1, \ldots, x_\ell) \in \{0,1\}^\ell$ contains random scalars $s_0, \ldots, s_\ell \leftarrow \mathbb{Z}_p$ in the exponent in G_1. In the secret key, we pick a random scalar $d_u \leftarrow \mathbb{Z}_p$ for each state $u \in [Q]$. We can now describe the invariant used during decryption with g_1, g_2 being respective generators of G_1, G_2:

- In Waters' ABE for DFA, if the computation reaches a state $u_i \in [Q]$ upon reading $x_1, \ldots, x_i$, decryption computes $e(g_1, g_2)^{s_i d_{u_i}}$. In particular, the scheme allows the decryptor to compute the ratios

$$e(g_1, g_2)^{s_j d_v - s_{j-1} d_u}, \ \forall j \in [\ell], u \in [Q], v = \delta(u, x_j) \in [Q] \tag{1}$$

  where $\delta : [Q] \times \{0,1\} \to [Q]$ is the DFA transition function.
- The natural way to extend (1) to account for non-deterministic transitions in an NFA is to allow the decryptor to compute

$$e(g_1, g_2)^{s_j d_v - s_{j-1} d_u}, \ \forall j \in [\ell], u \in [Q], v \in \delta(u, x_j) \subseteq [Q] \tag{2}$$

  where $\delta : [Q] \times \{0,1\} \to 2^{[Q]}$ is the NFA transition function. As noted by Waters [21], such an ABE scheme for NFA is broken via a so-called "back-tracking attack", which we describe in Appendix A.
- In our ABE for NFA, we allow the decryptor to compute

$$e(g_1, g_2)^{s_j (\sum_{v \in \delta(u, x_j)} d_v) - s_{j-1} d_u}, \ \forall j \in [\ell], u \in [Q] \tag{3}$$

  A crucial distinction between (3) and (2) is that the decryptor can only compute *one* quantity for each j, u in the former (as is the case also in (1)), and up to Q quantities in the latter. The ability to compute multiple quantities in (2) is exactly what enables the back-tracking attack.

We clarify that our ABE for NFA imposes an extra restriction on the NFA, namely that the total number of accepting paths[3] be non-zero $\bmod\ p$ for accepting inputs; we use NFA$^{\oplus_p}$ to denote such NFAs. In particular, this is satisfied by standard NFA where the total number of accepting paths is less than p for all inputs. This is in general a non-trivial restriction since the number of accepting paths for an arbitrary NFA can be as large as Q^ℓ. Fortunately, for NFAs obtained by running a DFA "in reverse", the number of accepting paths is always either 0 or 1.

Indeed, the above idea, along with a suitable modification of Waters' proof strategy, already yields our selectively secure ABE for NFA$^{\oplus_p}$ under q-type assumptions in asymmetric bilinear groups of prime order p. We defer the details to Appendix B.

[3] An accepting path on input $x \in \{0,1\}^\ell$ is described by a sequence of states $u_0, \ldots, u_\ell \in [Q]$ where u_0 is the start state, u_ℓ is an accept state and $u_j \in \delta(u_{j-1}, x_j)$ for all $j \in [\ell]$.

reference	assumption	security	|sk|	|ct|
[21]	q-type	selective	$O(Q)$	$O(\ell)$
[5,4,1]	q-type + k-Lin	adaptive ✓	$O(Q)$	$O(\ell)$
[11]	k-Lin ✓	selective	$O(Q)$	$O(\ell)$
[3]	k-Lin ✓	selective*	$O(Q^2)$	$O(\ell^3)$
§ 5 (§ F)	k-Lin ✓	adaptive ✓	$O(Q)$	$O(\ell)$

Fig. 1. Summary of ABE schemes for DFA. In the table, Q is the number of states in the DFA associated with sk and ℓ is the length of x associated with ct, and where $|\Sigma| = O(1)$.

reference	|sk|	|ct|	type of NFA	public key?	assumption
[2]	poly(Q)	poly(ℓ)	standard ✓		LWE ✓
§ B	$O(Q)$	$O(\ell)$	$\mathrm{NFA}^{\oplus p}$	✓	q-type
§ 4	$O(Q)$	$O(\ell)$	$\mathrm{NFA}^{\oplus p}$	✓	k-Lin✓

Fig. 2. Summary of ABE schemes for NFA. In the table, Q is the number of states in the NFA associated with sk and ℓ is the length of x associated with ct.

reference	assumption	compact?
[7]	k-Lin ✓	
[5]	q-type + k-Lin	✓
	k-Lin ✓	
§ 6	k-Lin ✓	✓

Fig. 3. Summary of adaptively secure ABE schemes for branching programs (BP). Here "compact" is also referred to "unbounded multi-use" in [5].

- To obtain a selectively secure scheme based on k-Lin, we apply the same modifications as in GWW [11]. For the proof of security, entropy propagation is defined via back-tracking the NFA computation, in a way analogous to that for back-tracking the DFA computation.
- To obtain an adaptively secure scheme based on k-Lin, we adapt the selectively secure scheme to the piecewise guessing framework [15]. One naive approach is to introduce a new semi-functional space. In contrast, we introduce one extra components into master public key, secret key and ciphertext, respectively. With the extra components, we can avoid adding a new semi-functional subspace, by reusing an existing subspace as shown in previous unbounded ABE in [8]. Under k-Lin assumption, our technique roughly saves $k \cdot \ell$ elements in the ciphertext and $k \cdot (2|\Sigma| + 2)Q$ elements in the secret key over the general apporach. This way, we obtain ciphertext and key sizes that are almost the same as those in the GWW selectively secure scheme.

ABE for branching programs. We build our compact adaptively secure ABE for branching program (BP) in two steps analogous to our adaptively secure ABE for DFA. In particular, we first show how to transform branching programs to a subclass of nondeterministic branching programs (NBP) and construct adaptively secure ABE for such class of NBP. Note that the latter is sufficient to capture a special BP with permutation transition function (without transforming BP to NBP) and readily simplify the result of Kowalczyk and Wee [15] for boolean formula (NC1).

1.2 Technical Overview

We start by recalling the standard definitions of DFA and NFA using vector-matrix notation: that is, we describe the start and accept states using the character vectors, and specify the transition function via a transition matrix. The use of vector-matrix notation enables a more compact description of our ABE schemes, and also clarifies the connection to branching programs.

NFA, DFA, $\mathbf{NFA}^{\oplus p}$. An NFA Γ is specified using $(Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ where Σ is the alphabet and

$$Q \in \mathbb{N}; \quad \mathbf{M}_\sigma \in \{0,1\}^{Q\times Q}, \forall \sigma \in \Sigma; \quad \mathbf{u}, \mathbf{f} \in \{0,1\}^{1\times Q}.$$

reference	$\lvert\mathsf{ct}\rvert$	$\lvert\mathsf{sk}\rvert$	**assumption**	**security**
[21]	$(2\ell+3)\lvert G_1\rvert$	$(3\lvert\Sigma\rvert Q+4)\lvert G_2\rvert$	q-type	selective
[5]	$((2k+2)\ell+6k+6)\lvert G_1\rvert$	$((3k+3)\lvert\Sigma\rvert Q+5k+5)\lvert G_2\rvert$	q-type + k-Lin	adaptive ✓
	$(3\ell+12)\lvert G_1\rvert$	$(6\lvert\Sigma\rvert Q+10)\lvert G_2\rvert$	q-type + SXDH	adaptive ✓
[11]	$((3k+1)\ell+4k+1)\lvert G_1\rvert$	$((4k+2)\lvert\Sigma\rvert Q+(3k+1)Q+2k+1)\lvert G_2\rvert$	k-Lin ✓	selective
	$(4\ell+5)\lvert G_1\rvert$	$(6\lvert\Sigma\rvert Q+4Q+3)\lvert G_2\rvert$	SXDH✓	selective
§ 5 (§ F)	$((3k+1)\ell+6k+2)\lvert G_1\rvert$	$((4k+2)\lvert\Sigma\rvert Q+(5k+2)Q+2k+1)\lvert G_2\rvert$	k-Lin ✓	adaptive ✓
	$(4\ell+8)\lvert G_1\rvert$	$(6\lvert\Sigma\rvert Q+7Q+3)\lvert G_2\rvert$	SXDH ✓	adaptive ✓

Fig. 4. Concrete parameter sizes of pairing-based ABE schemes for DFA. Note that [21,11] are selectively secure whereas our scheme is adaptively secure; [3] is omitted from the table since the ciphertext and key sizes are asymptotically larger, see Fig 1. In the table, Q is the number of states in the DFA, Σ indicates the alphabet, ℓ is the length of input x. All the schemes work over bilinear groups (G_1, G_2, G_T, e) of prime order p where $e : G_1 \times G_2 \to G_T$. We note that all the schemes shown in the table have mpk of $O(|\Sigma|)$ group elements. In the $|\mathsf{ct}|$-column, we omit one G_T element. In the **assumption** column, SXDH means 1-Lin.

The NFA Γ accepts an input $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$, denoted by $\Gamma(x) = 1$, if

$$\mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_2}\mathbf{M}_{x_1}\mathbf{u}^\top > 0 \tag{4}$$

and rejects the input otherwise, denoted by $\Gamma(x) = 0$. We will also refer to the quantity $\mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_2}\mathbf{M}_{x_1}\mathbf{u}^\top$ as the number of accepting paths for x. The above relation (4) is equivalent to

$$\mathbf{u}\mathbf{M}_{x_1}^\top\mathbf{M}_{x_2}^\top \cdots \mathbf{M}_{x_\ell}^\top\mathbf{f}^\top > 0$$

The unusual choice of notation is to simplify the description of our ABE scheme. Let $\mathcal{E}_Q$ be the collection of Q elementary row vectors of dimension Q.

- A DFA Γ is a special case of NFA where $\mathbf{u} \in \mathcal{E}_Q$ and each column in every matrix $\mathbf{M}_\sigma$ is an elementary column vector (i.e., contains exactly one 1).
- An NFA$^{\oplus p}$, parameterized by a prime p, is the same as an NFA except we change the accept criterion in (4) to:

  $$\mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_2}\mathbf{M}_{x_1}\mathbf{u}^\top \neq 0 \bmod p$$

  Note that this coincides with the standard NFA definition whenever the total number of accepting paths for all inputs is less than p.

Throughout the rest of this work, when we refer to NFA, we mean NFA$^{\oplus p}$ unless stated otherwise.

ABE for NFA$^{\oplus p}$. Following our overview in Section 1.1, an encryption of $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$ contains random scalars $s_0, \ldots, s_\ell$ in the exponent, where the plaintext is masked by $e(g_1, g_2)^{s_\ell \alpha}$. To generate a secret key for an NFA$^{\oplus p}$ Γ, we first pick $\mathbf{d} = (d_1, \ldots, d_Q) \leftarrow \mathbb{Z}_p^Q$ as before. We allow the decryptor to compute the following quantities in the exponent over G_T:

$$\begin{aligned} &\text{(i)} && s_\ell(\alpha\mathbf{f} - \mathbf{d}) \\ &\text{(ii)} && s_j\mathbf{d}\mathbf{M}_{x_j} - s_{j-1}\mathbf{d},\ \forall j \in [\ell]\ \text{(corresponds to (3))} \\ &\text{(iii)} && s_0\mathbf{d}\mathbf{u}^\top \end{aligned} \tag{5}$$

If we write $\mathbf{u}_{j,x}^\top = \mathbf{M}_{x_j} \cdots \mathbf{M}_{x_1}\mathbf{u}^\top$ for all $j \in [\ell]$ and $\mathbf{u}_{0,x} = \mathbf{u}$, then we have

$$s_\ell\alpha \cdot \mathbf{f}\mathbf{u}_{\ell,x}^\top = \overbrace{s_\ell(\alpha\mathbf{f} - \mathbf{d})}^{\text{(i)}} \cdot \mathbf{u}_{\ell,x}^\top + \left(\sum_{j=1}^{\ell} \overbrace{(s_j\mathbf{d}\mathbf{M}_{x_j} - s_{j-1}\mathbf{d})}^{\text{(ii)}} \cdot \mathbf{u}_{j-1,x}^\top\right) + \overbrace{s_0\mathbf{d}\mathbf{u}_{0,x}^\top}^{\text{(iii)}}$$

This means that whenever $\mathbf{fu}_{\ell,x}^\top \neq 0 \bmod p$, as is the case when $\Gamma(x)=1$, the decryptor will be able to recover $e(g_1,g_2)^{s_\ell \alpha}$.

Indeed, it is straight-forward to verify that the following ABE scheme satisfies the above requirements, where $[\cdot]_1, [\cdot]_2, [\cdot]_T$ denote component-wise exponentiations in respective groups G_1, G_2, G_T [10].

$$\begin{aligned}
\mathsf{msk} &= \big(w_{\mathrm{start}}, w_{\mathrm{end}}, z, \{w_\sigma\}_{\sigma\in\Sigma}, \alpha\big) \qquad (6)\\
\mathsf{mpk} &= \big([w_{\mathrm{start}}]_1, [w_{\mathrm{end}}]_1, [z]_1, \{[w_\sigma]_1\}_{\sigma\in\Sigma}, [\alpha]_T\big)\\
\mathsf{ct}_x &= \begin{pmatrix} [s_0]_1,\ [s_0 w_{\mathrm{start}}]_1 \\ \big\{[s_j]_1,\ [s_{j-1}z + s_j w_{x_j}]_1\big\}_{j\in[\ell]} \\ [s_\ell]_1,\ [s_\ell w_{\mathrm{end}}]_1,\ [s_\ell \alpha]_T \cdot m \end{pmatrix}\\
\mathsf{sk}_\Gamma &= \begin{pmatrix} [\mathbf{du}^\top + w_{\mathrm{start}}\mathbf{ru}^\top]_2,\ [\mathbf{ru}^\top]_2 \\ \big\{[-\mathbf{d} + z\mathbf{r}]_2,\ [\mathbf{dM}_\sigma + w_\sigma \mathbf{r}]_2,\ [\mathbf{r}]_2\big\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + w_{\mathrm{end}}\mathbf{r}]_2,\ [\mathbf{r}]_2 \end{pmatrix}, \quad \mathbf{d},\mathbf{r} \leftarrow \mathbb{Z}_p^{1\times Q}
\end{aligned}$$

In Appendix B, we prove that this scheme is selectively secure under ℓ-EBDHE assumption; this is the assumption underlying Waters' selectively secure ABE for DFA [21].

Selective security from k-Lin. Following the GWW proof strategy which in turn builds on the dual system argument, we design a series of games $\mathsf{G}_0,\ldots,\mathsf{G}_\ell$ such that in G_i, the quantities s_i and $\mathbf{d}$ have some extra entropy in the so-called semi-functional space (which requires first modifying the above scheme). The entropy in $\mathbf{d}$ is propagated from G_0 to G_1, then G_2, and finally to G_ℓ via a combination of a computational and combinatorial arguments. In G_ℓ, we will have sufficient entropy to statistically mask α in the secret key, which allows us to argue that $e(g_1,g_2)^{s_\ell\alpha}$ statistically masks the plaintext. In this overview, we focus on the novel component, namely the combinatorial argument which exploits specific properties of our scheme for $\mathrm{NFA}^{\oplus p}$; the computational steps are completely analogous to those in GWW.

In more detail, we want to replace $\mathbf{d}$ with $\mathbf{d}+\mathbf{d}'_i$ in G_i, where $\mathbf{d}'_i \in \mathbb{Z}_p^Q$ corresponds to the extra entropy we introduce into the secret keys in the semi-functional space. Note that $\mathbf{d}'_i$ will depend on both the challenge attribute x^* as well as the underlying $\mathrm{NFA}^{\oplus p}$. We have the following constraints on $\mathbf{d}'_i$'s, arising from the fact that an adversarial distinguisher for $\mathsf{G}_0,\ldots,\mathsf{G}_\ell$ can always compute what a decryptor can compute in (5):

- to mask α in G_ℓ, we set $\mathbf{d}'_\ell = \Delta\mathbf{f}$ where $\Delta \leftarrow \mathbb{Z}_p$, so that

  $$\alpha\mathbf{f} - (\mathbf{d}+\mathbf{d}'_\ell) = (\alpha-\Delta)\mathbf{f} - \mathbf{d}$$

  perfectly hides α;
- (ii) implies that

  $$\begin{aligned}
  &\overbrace{s_i\mathbf{dM}_{x_i^*} - s_{i-1}(\mathbf{d}+\mathbf{d}'_{i-1})}^{\mathsf{G}_{i-1}} \approx_s \overbrace{s_i(\mathbf{d}+\mathbf{d}'_i)\mathbf{M}_{x_i^*} - s_{i-1}\mathbf{d}}^{\mathsf{G}_i}\\
  \Longrightarrow \qquad & \qquad\qquad -s_{i-1}\mathbf{d}'_{i-1} \approx_s s_i\mathbf{d}'_i\mathbf{M}_{x_i^*}
  \end{aligned}$$

  to prevent a distinguishing attack[4] between G_{i-1} and G_i by computing $s_i\mathbf{dM}_{x_i^*} - s_{i-1}\mathbf{d}$ in both games;
- (iii) implies that $s_0(\mathbf{d}+\mathbf{d}'_0)\mathbf{u}^\top = s_0\mathbf{du}^\top$, and therefore, $\mathbf{d}'_0\mathbf{u}^\top = 0 \bmod p$. This is to prevent a distinguishing attack[5] between the real keys and those in G_0.

In particular, we can satisfy the first two constraints by setting[6]

$$\mathbf{d}'_i = \Delta\cdot\mathbf{fM}_{x_\ell^*}\cdots\mathbf{M}_{x_{i+1}^*} \ \forall i \in [0,\ell]$$

[4] Looking ahead to the proof of security in Section 4, this "simplified" attack corresponds roughly to using $\mathsf{ct}_{x^*}^{i-1,i}$ to distinguish $\mathsf{sk}_\Gamma^{i-1,i}$ and sk_Γ^{i}; this comes up in the proof of $\mathsf{G}_{2.i.2} \approx_c \mathsf{G}_{2.i.3}$ in Lemma 17.

[5] In Section 4, this roughly corresponds to distinguish sk_Γ and sk_Γ^0 with $\mathsf{ct}_{x^*}^0$; this comes up in the proof of $\mathsf{G}_1 \approx_c \mathsf{G}_{2.1.0}$ in Lemma 6.

[6] We adopt the standard convention that the product of an empty sequence of matrices is the identity matrix. This means $\mathbf{d}'_\ell = \Delta\cdot\mathbf{f}$.

where $\approx_s$ holds over $\Delta \leftarrow \mathbb{Z}_p$, as long as $s_0, \ldots, s_\ell \neq 0$. Whenever $\Gamma(x^*) = 0$, we have

$$\mathbf{f}\mathbf{M}_{x^*_\ell} \cdots \mathbf{M}_{x^*_1} \mathbf{u}^\top = 0 \bmod p$$

and therefore the third constraint is also satisfied.

Two clarifying remarks. First, the quantity

$$\mathbf{f}\mathbf{M}_{x^*_\ell} \cdots \mathbf{M}_{x^*_{i+1}}$$

used in defining $\mathbf{d}'_i$ has a natural combinatorial interpretation: its u'th coordinate corresponds to the number of paths from the accept states to u, while back-tracking along $x^*_\ell, \ldots, x^*_{i+1}$. In the specific case of a DFA, this value is 1 if u is reachable from an accept state, and 0 otherwise. It is then easy to see that our proof strategy generalizes that of GWW for DFA: the latter adds Δ to d_u in G_i whenever u is reachable from accept state while back-tracking along the last $\ell - i$ bits of the challenge attribute (cf. [11, Sec. 3.2]). Second, the "naive" (and insecure) ABE for NFA that captures non-deterministic transitions as in (2) introduces more equations in (ii) in (5); this in turn yields more –and ultimately unsatisfiable– constraints on the $\mathbf{d}'_i$'s.

Finally, we remark that our ABE for NFA$^{\oplus p}$ (and ABE for DFA from GWW as well) can be proved in the semi-adaptive model [9], which is weaker than adaptive security but stronger than both selective and selective* model used in [3].

Adaptive security for restricted NFA$^{\oplus p}$ and DFA. Fix a set $\mathcal{F} \subseteq \mathbb{Z}^Q$. We say that an NFA or an NFA$^{\oplus p}$is $\mathcal{F}$-restricted if

$$\forall\, \ell \in \mathbb{N},\, x \in \Sigma^\ell,\, i \in [0,\ell] : \mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_{i+1}} \in \mathcal{F}$$

Note that $\mathbf{f}\mathbf{M}_{x^*_\ell} \cdots \mathbf{M}_{x^*_{i+1}}$ corresponding to the challenge attribute x^* is exactly what is used to define $\mathbf{d}'_i$ in the previous paragraph. Moreover, following GWW, knowing this quantity is sufficient to prove indistinguishability of G_{i-1} and G_i. This means that to prove selective security for $\mathcal{F}$-restricted NFAs, it suffices to know $\log|\mathcal{F}|$ bits about the challenge attribute, and via the piecewise guessing framework, this yields adaptive security with a security loss of $|\mathcal{F}|$. Unfortunately, $|\mathcal{F}|$ is in general exponentially large for general NFAs and DFAs. In particular, DFAs are $\{0,1\}^Q$-restricted, and naively applying this argument would yield adaptively secure DFAs with a 2^Q security loss.

Instead, we show how to transform DFAs into $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$, where $\mathcal{E}_Q \subset \{0,1\}^Q$ is the collection of Q elementary row vectors of dimension Q; this yields adaptively secure ABE for DFAs with a security loss of $|\mathcal{E}_Q| = Q$. Concretely, our adaptively secure ABE for DFA uses an adaptively secure ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$, and proceeds

- to encrypt $x = (x_1, \ldots, x_\ell)$, use the ABE for NFA to encrypt $x^\top = (x_\ell, \ldots, x_1)$;[7]
- to generate a secret key for a DFA $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}, \mathbf{u}, \mathbf{f})$, use the ABE for NFA to generate a key for $\Gamma^\top = (Q, \Sigma, \{\mathbf{M}_\sigma^\top\}, \mathbf{f}, \mathbf{u})$.

Note that we reversed x during encryption, and transposed $\mathbf{M}_\sigma$, and switched $\mathbf{u}, \mathbf{f}$ during key generation. Correctness essentially follows from the equality

$$\overbrace{\mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top}^{\Gamma(x)} = (\mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top)^\top = \overbrace{\mathbf{u}\mathbf{M}_{x_1}^\top \cdots \mathbf{M}_{x_\ell}^\top \mathbf{f}^\top}^{\Gamma^\top(x^\top)}.$$

Furthermore $\Gamma^\top = (Q, \Sigma, \{\mathbf{M}_\sigma^\top\}, \mathbf{f}, \mathbf{u})$ is indeed a $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$. This follows from the fact that for any DFA Γ:

$$\forall\, \ell \in \mathbb{N},\, x \in \Sigma^\ell,\, i \in [0,\ell] : (\mathbf{M}_{x_i} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top)^\top \in \mathcal{E}_Q$$

which is implied by the property of DFA: $\mathbf{u} \in \mathcal{E}_Q$ and each column in every matrix $\mathbf{M}_\sigma$ contains exactly one 1. We give an example of reversing DFA in Appendix C.

[7] We acknowledge that writing $x^\top$ constitutes an abuse of notation, but nonetheless convenient in analogy with $\mathbf{M}_\sigma^\top$.

	policy	security	decryption		proof	
			direction	information	direction	information
GWW [11]	DFA	selective	forward	reachability	backward	reachability
§ 5	DFA	adaptive	backward	reachability	forward	reachability
Naive,§ A	NFA	broken	forward	reachability	-	-
§ 4	NFA	selective	forward	# paths	backward	# paths

Fig. 5. Summary of tracing executions underlying GWW, our adaptively secure ABE for DFA, our selectively secure ABE for NFA$^{\oplus p}$ and naive extension of Waters' ABE for DFA.

1.3 Discussion

Tracing executions. Recall that a DFA is specified using a transition function $\delta : [Q] \times \Sigma \to [Q]$. A forward computation upon reading σ goes from a state u to $v = \delta(u, \sigma)$, whereas back-tracking upon reading σ goes from v to u if $v = \delta(u, \sigma)$.

- GWW selective ABE for DFA: Decryption follows normal "forward" computation keeping track of whether a state is reachable from the start state, whereas the security proof introduces entropy based on whether a state is reachable from the accept states via "back-tracking".
- Our adaptive ABE for DFA and branching programs: Decryption uses back-tracking and keeps track of whether a state is reachable from the accept states, whereas the security proof introduces entropy based on whether a state is reachable from the start state via forward computation. To achieve polynomial security loss, we crucially rely on the fact that when reading i input bits, exactly one state is reachable from the start state via forward computation.
- Naive and insecure ABE for NFA$^{\oplus p}$: Decryption follows normal forward computation keeping track of whether a state is reachable from the start state.
- Our selective ABE for NFA$^{\oplus p}$: Decryption follows normal forward computation keeping track of the number of paths from the start state, whereas the security proof introduces entropy scaled by the number of paths that are reachable from the accept states via back-tracking.

We summarize the discussion in Fig 5.

ABE for DFA vs branching programs. Our work clarifies that the same obstacle (having to guess a large subset of states that are reached upon back-tracking) arose in constructing adaptive ABE for DFA and compact adaptive ABE for branching programs from k-Lin, and presents a new technique that solves both problems simultaneously in the setting of KP-ABE. Furthermore, our results and techniques can carry over to the CP-ABE settings using more-or-less standard (but admittedly non-black-box) arguments, following e.g. [4, Sec.8] and [6, Sec.4]. See Appendix I and Appendix J for adaptively secure CP-ABE for DFA and branching programs, respectively.

Interestingly, the very recent work of Agarwal *et al.* [3,2] shows a related connection: namely that compact and unbounded adaptive KP and CP-ABE for branching programs[8] –for which they do not provide any instantiations– yields compact adaptive KP-ABE (as well as CP-ABE) for DFA. In particular, just getting to KP-ABE for DFA already requires both KP and CP-ABE for branching programs and also incurs a larger polynomial blow-up in the parameters compared to our constructions; furthermore, simply getting to compact, unbounded, adaptive KP-ABE for branching programs would also require most of the technical machinery used in this work, notably the "nested, two-slot" dual system argument and the piecewise guessing framework. Nonetheless, there is significant conceptual appeal to having a generic and modular transformation that also yields both KP-ABE and CP-ABE schemes. That said, at the core of our constructions and analysis is a very simple combinatorial object sketched in Section 1.2. We leave the question of properly formalizing this object and building a generic compiler to full-fledged KP-ABE and CP-ABE schemes to further work; in particular, such a compiler should (i) match or improve upon the concrete efficiency of our schemes,

[8] The statement in [3] refers to monotone span programs, which is a more powerful object, but we believe that branching program suffices.

as with prior compilers such as [7,5], and (ii) properly decouple the combinatorial arguments that are specific to DFA, NFA and branching programs from the computational arguments that are oblivious to the underlying computational model.

Organization. The next section gives some background knowledge. Section 3 shows the transformation from DFA to $\mathcal{E}$-restricted NFA$^{\oplus p}$. We show our selectively secure ABE for NFA$^{\oplus p}$ in Section 4 and upgrade to adaptive security for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in Section 5. The latter implies our adaptively secure ABE for DFA with concrete description appeared in Appendix F. Our basic selectively secure ABE for NFA$^{\oplus p}$ from q-type assumption can be found in Appendix B. Finally, in Section 6, we show how to get our compact adaptively secure ABE for branching programs. The concrete scheme can be found in Appendix H.

2 Preliminaries

Notation. We denote by $s \leftarrow S$ the fact that s is picked uniformly at random from a finite set S; by $U(S)$, we indicate uniform distribution over finite set S. We use $\approx_s$ to denote two distributions being statistically indistinguishable, and $\approx_c$ to denote two distributions being computationally indistinguishable. We use $\langle \mathcal{A}, \mathsf{G} \rangle = 1$ to denote that an adversary $\mathcal{A}$ wins in an interactive game G. We use lower case boldface to denote *row* vectors and upper case boldcase to denote matrices. We use $\mathbf{e}_i$ to denote the i'th elementary (row) vector (with 1 at the i'th position and 0 elsewhere) and let $\mathcal{E}_Q$ denote the set of all elementary vectors of dimension Q. For matrix $\mathbf{A}$, we use $\mathsf{span}(\mathbf{A})$ to denote the *row* span of $\mathbf{A}$ and use $\mathsf{basis}(\mathbf{A})$ to denote a basis of *column* span of $\mathbf{A}$. Throughout the paper, we use prime number p to denote the order of underlying groups.

2.1 Attribute-based encryption

Syntax. An attribute-based encryption (ABE) scheme for some class $\mathcal{C}$ consists of four algorithms:

$\mathsf{Setup}(1^\lambda, \mathcal{C}) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm gets as input the security parameter 1^λ and class description $\mathcal{C}$. It outputs the master public key mpk and the master secret key msk. We assume mpk defines the message space $\mathcal{M}$.

$\mathsf{Enc}(\mathsf{mpk}, x, m) \to \mathsf{ct}_x$. The encryption algorithm gets as input mpk, an input x and a message $m \in \mathcal{M}$. It outputs a ciphertext ct_x. Note that x is public given ct_x.

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma) \to \mathsf{sk}_\Gamma$. The key generation algorithm gets as input mpk, msk and $\Gamma \in \mathcal{C}$. It outputs a secret key sk_Γ. Note that Γ is public given sk_Γ.

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_x) \to m$. The decryption algorithm gets as input sk_Γ and ct_x such that $\Gamma(x) = 1$ along with mpk. It outputs a message m.

Correctness. For all input x and Γ with $\Gamma(x) = 1$ and all $m \in \mathcal{M}$, we require

$$\Pr\left[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_x) = m : \begin{array}{l} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{C}) \\ \mathsf{sk}_\Gamma \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma) \\ \mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, m) \end{array} \right] = 1.$$

Security definition. For a stateful adversary $\mathcal{A}$, we define the advantage function

$$\mathsf{Adv}^{\mathrm{ABE}}_{\mathcal{A}}(\lambda) := \Pr\left[\beta = \beta' : \begin{array}{l} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{C}) \\ (x^*, m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)}(\mathsf{mpk}) \\ \beta \leftarrow \{0,1\};\ \mathsf{ct}_{x^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*, m_\beta) \\ \beta' \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)}(\mathsf{ct}_{x^*}) \end{array} \right] - \frac{1}{2}$$

with the restriction that all queries Γ that $\mathcal{A}$ sent to $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)$ satisfy $\Gamma(x^*) = 0$. An ABE scheme is *adaptively secure* if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}^{\mathrm{ABE}}_{\mathcal{A}}(\lambda)$ is a negligible function in λ. The *selective* security is defined analogously except that the adversary $\mathcal{A}$ selects x^* before seeing mpk. A notion between selective and adaptive is so-called *semi-adaptive security* [9] where the adversary $\mathcal{A}$ is allowed to select x^* after seeing mpk but before making any queries.

2.2 Prime-order Groups

A generator $\mathcal{G}$ takes as input a security parameter 1^λ and outputs a description $\mathbb{G} := (p, G_1, G_2, G_T, e)$, where p is a prime of $\Theta(\lambda)$ bits, G_1, G_2 and G_T are cyclic groups of order p, and $e : G_1 \times G_2 \to G_T$ is a non-degenerate bilinear map. We require that the group operations in G_1, G_2, G_T and the bilinear map e are computable in deterministic polynomial time in λ. Let $g_1 \in G_1$, $g_2 \in G_2$ and $g_T = e(g_1, g_2) \in G_T$ be the respective generators. We employ the *implicit representation* of group elements: for a matrix $\mathbf{M}$ over $\mathbb{Z}_p$, we define $[\mathbf{M}]_1 := g_1^{\mathbf{M}}$, $[\mathbf{M}]_2 := g_2^{\mathbf{M}}$, $[\mathbf{M}]_T := g_T^{\mathbf{M}}$, where exponentiation is carried out component-wise. Also, given $[\mathbf{A}]_1, [\mathbf{B}]_2$, we let $e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{AB}]_T$. We recall the matrix Diffie-Hellman (MDDH) assumption on G_1 [10]:

Assumption 1 (MDDH$^d_{k,k'}$ Assumption) *Let $k' > k \geq 1$ and $d \geq 1$. We say that the MDDH$^d_{k,k'}$ assumption holds if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}^{\mathrm{MDDH}^d_{k,k'}}_{\mathcal{A}}(\lambda) := \left| \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_1, \boxed{[\mathbf{MS}]_1}) = 1] - \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{U}]_1) = 1] \right|$$

where $\mathbb{G} := (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$, $\mathbf{M} \leftarrow \mathbb{Z}_p^{k' \times k}$, $\mathbf{S} \leftarrow \mathbb{Z}_p^{k \times d}$ *and* $\mathbf{U} \leftarrow \mathbb{Z}_p^{k' \times d}$.

The MDDH assumption on G_2 can be defined in an analogous way. Escala *et al.* [10] showed that

$$k\text{-Lin} \Rightarrow \mathrm{MDDH}^1_{k,k+1} \Rightarrow \mathrm{MDDH}^d_{k,k'}\ \forall k' > k, d \geq 1$$

with a tight security reduction. We will use $\mathsf{Adv}^{k\text{-}\mathrm{LIN}}_{\mathcal{A}}(\lambda)$ to denote the advantage function w.r.t. k-Lin assumption.

3 DFA, NFA, and their Relationships

Let p be a global parameter and $\mathcal{E}_Q = \{\mathbf{e}_1, \ldots, \mathbf{e}_Q\}$ be the set of all elementary row vectors of dimension Q. This section describes various notions of DFA and NFA and studies their relationships.

Finite Automata. We use $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma \in \Sigma}, \mathbf{u}, \mathbf{f})$ to describe deterministic finite automata (DFA for short), nondeterministic finite automata (NFA for short), p-bounded NFA (NFA$^{<p}$ for short) and mod-p NFA (NFA$^{\oplus p}$ for short), where $Q \in \mathbb{N}$ is the number of states, vectors $\mathbf{u}, \mathbf{f} \in \{0,1\}^{1 \times Q}$ describe the start and accept states, a collection of matrices $\mathbf{M}_\sigma \in \{0,1\}^{Q \times Q}$ describe the transition function. Let $x = (x_1, \ldots, x_\ell)$ denote an input, then,

- for DFA Γ, we have $\mathbf{u} \in \mathcal{E}_Q$, each column in every matrix $\mathbf{M}_\sigma$ is an elementary column vector (i.e., contains exactly one 1) and $\Gamma(x) = 1 \iff \mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top = 1$;
- for NFA Γ, we have $\Gamma(x) = 1 \iff \mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top > 0$;
- for NFA$^{<p}$ Γ, we have $\mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top < p$ and $\Gamma(x) = 1 \iff \mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top > 0$;
- for NFA$^{\oplus p}$ Γ, we have $\Gamma(x) = 1 \iff \mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top \neq 0 \bmod p$.

We immediately have: DFA $\subset$ NFA$^{<p} \subset$ NFA $\cap$ NFA$^{\oplus p}$.

$\mathcal{E}_Q$-restricted NFA$^{\oplus p}$. We introduce the notion of $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ which is an NFA$^{\oplus p}$ $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma \in \Sigma}, \mathbf{u}, \mathbf{f})$ with an additional property: for all $\ell \in \mathbb{N}$ and all $x \in \Sigma^\ell$, it holds that

$$\mathbf{f}_{i,x} := \mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_{i+1}} \in \mathcal{E}_Q,\ \forall i \in [0, \ell]$$

Here $\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_{i+1}}$ for $i = \ell$ refers to $\mathbf{I}$ of size $Q \times Q$.

Transforming DFA to $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$. In general, a DFA is not necessarily a $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$. The next lemma says that we can nonetheless transform any DFA into a $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$:

Lemma 1 **(DFA to $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$).** *For each DFA $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$, we have NFA$^{\oplus p}$ $\Gamma^\top = (Q, \Sigma, \{\mathbf{M}_\sigma^\top\}_{\sigma\in\Sigma}, \mathbf{f}, \mathbf{u})$ such that*

1. *$\Gamma^\top$ is $\mathcal{E}_Q$-restricted;*
2. *for all $\ell \in \mathbb{N}$ and $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$, it holds that*

$$\Gamma(x) = 1 \iff \Gamma^\top(x^\top) = 1 \quad \textit{where } x^\top = (x_\ell, \ldots, x_1) \in \Sigma^\ell. \tag{7}$$

Proof. Recall that the definition of DFA implies two properties:

$$\mathbf{f} \in \{0,1\}^Q \tag{8}$$

$$\text{and} \quad (\mathbf{M}_{x_i} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top)^\top \in \mathcal{E}_Q, \quad \forall i \in [0, \ell]. \tag{9}$$

Property (9) comes from the facts that $\mathbf{u} \in \mathcal{E}_Q$ and each column in every matrix $\mathbf{M}_\sigma$ is an elementary column vector.

We parse $x^\top = (x_1^\top, \ldots, x_\ell^\top)$ and prove the two parts of the lemma as below.

1. $\Gamma^\top$ is $\mathcal{E}_Q$-restricted since we have

$$\mathbf{u}\mathbf{M}_{x_\ell^\top}^\top \cdots \mathbf{M}_{x_{i+1}^\top}^\top = (\mathbf{M}_{x_{\ell-i}} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top)^\top \in \mathcal{E}_Q, \quad \forall i \in [0, \ell]$$

   where the equality is implied by the structure of $\Gamma^\top, x^\top$ and we use property (9).

2. To prove (7), we rely on the fact

$$\begin{aligned}\Gamma(x) = 1 &\iff \mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top = 1 \\ &\iff \mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top \neq 0 \bmod p \\ &\iff \mathbf{u}\mathbf{M}_{x_\ell^\top}^\top \cdots \mathbf{M}_{x_1^\top}^\top \mathbf{f}^\top \neq 0 \bmod p \\ &\iff \Gamma^\top(x^\top) = 1.\end{aligned}$$

   The second $\iff$ follows from the fact that $\mathbf{f}\mathbf{M}_{x_\ell} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top \in \{0,1\}$ which is implied by property (8) and (9) while the third $\iff$ is implied by the structure of $\Gamma^\top, x^\top$. □

4 Semi-adaptively Secure ABE for NFA$^{\oplus p}$

In this section, we present our ABE for NFA$^{\oplus p}$ in prime-order groups. The scheme achieves semi-adaptive security under the k-Lin assumption. Our construction is based on GWW ABE for DFA [11] along with an extension of the key structure and decryption to NFA; the security proof follows that of GWW with our novel combinatorial arguments regarding our NFA extension. (See Section 1.2 for an overview.) We remark that our scheme and proof work well for a more general form of NFA$^{\oplus p}$ where $\mathbf{u}, \mathbf{f}, \mathbf{M}_\sigma$ are over $\mathbb{Z}_p$ instead of $\{0,1\}$.

4.1 Basis

We will use the same basis as GWW [11]:

$$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \quad \mathbf{a}_2 \leftarrow \mathbb{Z}_p^{1\times(2k+1)}, \quad \mathbf{A}_3 \leftarrow \mathbb{Z}_p^{k\times(2k+1)} \tag{10}$$

and use $(\mathbf{A}_1^\parallel \mid \mathbf{a}_2^\parallel \mid \mathbf{A}_3^\parallel)$ to denote the dual basis so that $\mathbf{A}_i\mathbf{A}_i^\parallel = \mathbf{I}$ (known as *non-degeneracy*) and $\mathbf{A}_i\mathbf{A}_j^\parallel = \mathbf{0}$ if $i \neq j$ (known as *orthogonality*). For notational convenience, we always consider $\mathbf{a}_2^\parallel$ as a column vector. We review $\mathrm{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{A}_3}$ and $\mathrm{DDH}^{G_2}_{d,Q}$ assumption from [8] which are parameterized for basis (10) and tightly implied by k-Lin assumption. By symmetry, we may permute the indices for $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_3$.

Lemma 2 **($\mathbf{MDDH}_{k,2k} \Rightarrow \mathbf{SD}^{G_1}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_3}$ [8]).** *Under the $\mathrm{MDDH}_{k,2k}$ assumption in G_1, there exists an efficient sampler outputting random* $([\mathbf{A}_1]_1, [\mathbf{a}_2]_1, [\mathbf{A}_3]_1)$ *along with base* $\mathsf{basis}(\mathbf{A}_1^{\parallel})$, $\mathsf{basis}(\mathbf{a}_2^{\parallel})$, $\mathsf{basis}(\mathbf{A}_1^{\parallel},\mathbf{A}_3^{\parallel})$ *(of arbitrary choice) such that the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{SD}^{G_1}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_3}}(\lambda) := \left|\Pr[\mathcal{A}(D,[\mathbf{t}_0]_1)=1] - \Pr[\mathcal{A}(D,[\mathbf{t}_1]_1)=1]\right|$$

where

$$D := (\,[\mathbf{A}_1]_1, [\mathbf{a}_2]_1, [\mathbf{A}_3]_1, \mathsf{basis}(\mathbf{A}_1^{\parallel}), \mathsf{basis}(\mathbf{a}_2^{\parallel}), \mathsf{basis}(\mathbf{A}_1^{\parallel},\mathbf{A}_3^{\parallel})\,),$$
$$\mathbf{t}_0 \leftarrow \boxed{\mathsf{span}(\mathbf{A}_1)},\ \mathbf{t}_1 \leftarrow \colorbox{lightgray}{$\mathsf{span}(\mathbf{A}_1,\mathbf{A}_3)$}.$$

More concretely, we have, for all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that* $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{SD}^{G_1}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_3}}(\lambda) \le \mathsf{Adv}_{\mathcal{A}}^{\mathrm{MDDH}_{k,2k}}(\lambda)$.

Lemma 3 **($\mathbf{MDDH}^{d}_{k,k+d} \Rightarrow \mathbf{DDH}^{G_2}_{d,Q}$ [8]).** *Let $d, Q \in \mathbb{N}$. Under the $\mathrm{MDDH}^{d}_{k,k+d}$ assumption in G_2, the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{DDH}^{G_2}_{d,Q}}(\lambda) := \left|\Pr[\mathcal{A}([\mathbf{WB}]_2,[\mathbf{B}]_2,\boxed{[\mathbf{WR}]_2},[\mathbf{R}]_2)=1] - \Pr[\mathcal{A}([\mathbf{WB}]_2,[\mathbf{B}]_2,\colorbox{lightgray}{$[\mathbf{WR}+\mathbf{U}]_2$},[\mathbf{R}]_2)=1]\right|$$

where $\mathbf{W} \leftarrow \mathbb{Z}_p^{d\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times Q}$ *and* $\mathbf{U} \leftarrow \mathbb{Z}_p^{d\times Q}$*. More concretely, we have, for all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that* $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{DDH}^{G_2}_{d,Q}}(\lambda) \le O(1)\cdot\mathsf{Adv}_{\mathcal{A}}^{\mathrm{MDDH}^{d}_{k,k+d}}(\lambda)$.

Lemma 4 **(statistical lemma [8]).** *With probability* $1-1/p$ *over* $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_3, \mathbf{A}_1^{\parallel}, \mathbf{a}_2^{\parallel}, \mathbf{A}_3^{\parallel}$*, the following two distributions are statistically identical.*

$$\left\{\mathbf{A}_1\mathbf{W}, \mathbf{A}_3\mathbf{W}, \boxed{\mathbf{a}_2\mathbf{W}}\right\} \quad \textit{and} \quad \left\{\mathbf{A}_1\mathbf{W}, \mathbf{A}_3\mathbf{W}, \colorbox{lightgray}{$\mathbf{w}$}\right\}$$

where $\mathbf{W} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ *and* $\mathbf{w} \leftarrow \mathbb{Z}_p^{1\times k}$.

4.2 Scheme

Our ABE for $\mathrm{NFA}^{\oplus p}$ in prime-order groups is described as follows:

- $\mathsf{Setup}(1^\lambda, \Sigma)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

  $$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k\times(2k+1)},\ \mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(2k+1)} \quad \text{and} \quad \mathbf{W}_{\mathsf{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{W}_{\mathsf{end}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k},\ \forall \sigma \in \Sigma.$$

  Output

  $$\mathsf{mpk} = \big(\,[\mathbf{A}_1, \mathbf{A}_1\mathbf{W}_{\mathsf{start}}, \mathbf{A}_1\mathbf{Z}_0, \mathbf{A}_1\mathbf{Z}_1, \{\mathbf{A}_1\mathbf{W}_{\sigma,0}, \mathbf{A}_1\mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma}, \mathbf{A}_1\mathbf{W}_{\mathsf{end}}\,]_1, [\mathbf{A}_1\mathbf{k}^{\top}]_T\big)$$
  $$\mathsf{msk} = \big(\mathbf{k}, \mathbf{W}_{\mathsf{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \{\mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma}, \mathbf{W}_{\mathsf{end}}\big).$$

- $\mathsf{Enc}(\mathsf{mpk}, x, m)$: Let $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$ and $m \in G_T$. Pick $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_\ell \leftarrow \mathbb{Z}_p^{1\times k}$ and output

  $$\mathsf{ct}_x = \left(\begin{array}{c} [\mathbf{s}_0\mathbf{A}_1]_1,\ [\mathbf{s}_0\mathbf{A}_1\mathbf{W}_{\mathsf{start}}]_1 \\ \left\{[\mathbf{s}_j\mathbf{A}_1]_1, [\mathbf{s}_{j-1}\mathbf{A}_1\mathbf{Z}_{j \bmod 2} + \mathbf{s}_j\mathbf{A}_1\mathbf{W}_{x_j, j \bmod 2}]_1\right\}_{j\in[\ell]} \\ [\mathbf{s}_\ell\mathbf{A}_1]_1,\ [\mathbf{s}_\ell\mathbf{A}_1\mathbf{W}_{\mathsf{end}}]_1,\ [\mathbf{s}_\ell\mathbf{A}_1\mathbf{k}^{\top}]_T\cdot m \end{array}\right).$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$: Let $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$. Pick $\mathbf{D} \leftarrow \mathbb{Z}_p^{(2k+1)\times Q}$, $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times Q}$ and output

  $$\mathsf{sk}_\Gamma = \left(\begin{array}{c} [\mathbf{D}\mathbf{u}^{\top} + \mathbf{W}_{\mathsf{start}}\mathbf{R}\mathbf{u}^{\top}]_2,\ [\mathbf{R}\mathbf{u}^{\top}]_2 \\ \left\{[-\mathbf{D} + \mathbf{Z}_b\mathbf{R}]_2, [\mathbf{D}\mathbf{M}_\sigma + \mathbf{W}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\right\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [\mathbf{k}^{\top}\mathbf{f} - \mathbf{D} + \mathbf{W}_{\mathsf{end}}\mathbf{R}]_2,\ [\mathbf{R}]_2 \end{array}\right).$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_x)$: Parse ciphertext for $x = (x_1, \ldots, x_\ell)$ and key for $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ as:

$$\mathsf{ct}_x = \begin{pmatrix} [\mathbf{c}_{0,1}]_1, [\mathbf{c}_{0,2}]_1 \\ \{[\mathbf{c}_{j,1}]_1, [\mathbf{c}_{j,2}]_1\}_j \\ [\mathbf{c}_{\ell,1}]_1, [\mathbf{c}_{\text{end}}]_1, C \end{pmatrix} \quad \text{and} \quad \mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{k}_0^\top]_2, [\mathbf{r}_0^\top]_2 \\ \{[\mathbf{K}_b]_2, [\mathbf{K}_{\sigma,b}]_2, [\mathbf{R}]_2\}_{\sigma,b} \\ [\mathbf{K}_{\text{end}}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

We define

$$\mathbf{u}_{j,x}^\top = \mathbf{M}_{x_j} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top \bmod p, \ \forall j \in [0, \ell] \tag{11}$$

and proceed as follows:

1. Compute
$$B_0 = e([\mathbf{c}_{0,1}]_1, [\mathbf{k}_0^\top]_2) \cdot e([\mathbf{c}_{0,2}]_1, [\mathbf{r}_0^\top]_2)^{-1};$$
2. For all $j \in [\ell]$, compute
$$[\mathbf{b}_j]_T = e([\mathbf{c}_{j-1,1}]_1, [\mathbf{K}_{j \bmod 2}]_2) \cdot e([\mathbf{c}_{j,1}]_1, [\mathbf{K}_{x_j, j \bmod 2}]_2) \cdot e([-\mathbf{c}_{j,2}]_1, [\mathbf{R}]_2) \quad \text{and} \quad B_j = [\mathbf{b}_j \mathbf{u}_{j-1,x}^\top]_T;$$
3. Compute
$$[\mathbf{b}_{\text{end}}]_T = e([\mathbf{c}_{\ell,1}]_1, [\mathbf{K}_{\text{end}}]_2) \cdot e([-\mathbf{c}_{\text{end}}]_1, [\mathbf{R}]_2) \quad \text{and} \quad B_{\text{end}} = [\mathbf{b}_{\text{end}} \mathbf{u}_{\ell,x}^\top]_T;$$
4. Compute
$$B_{\text{all}} = B_0 \cdot \textstyle\prod_{j=1}^{\ell} B_j \cdot B_{\text{end}} \quad \text{and} \quad B = B_{\text{all}}^{(\mathbf{f}\mathbf{u}_{\ell,x}^\top)^{-1}}$$
and output the message $m' \leftarrow C \cdot B^{-1}$.

Correctness. For $x = (x_1, \ldots, x_\ell)$ and $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ such that $\Gamma(x) = 1$, we have:

$$\begin{aligned}
B_0 &= [\mathbf{s}_0 \mathbf{A}_1 \mathbf{D} \mathbf{u}^\top]_T = [\mathbf{s}_0 \mathbf{A}_1 \mathbf{D} \mathbf{u}_{0,x}^\top]_T && (12)\\
\mathbf{b}_j &= \mathbf{s}_j \mathbf{A}_1 \mathbf{D} \mathbf{M}_{x_j} - \mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{D} && (13)\\
B_j &= [\mathbf{s}_j \mathbf{A}_1 \mathbf{D} \mathbf{u}_{j,x}^\top - \mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{D} \mathbf{u}_{j-1,x}^\top]_T && (14)\\
\mathbf{b}_{\text{end}} &= \mathbf{s}_\ell \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{D} && (15)\\
B_{\text{end}} &= [\mathbf{s}_\ell \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} \mathbf{u}_{\ell,x}^\top - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{D} \mathbf{u}_{\ell,x}^\top]_T && (16)\\
B_{\text{all}} &= [\mathbf{s}_\ell \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} \mathbf{u}_{\ell,x}^\top]_T && (17)\\
B &= [\mathbf{s}_\ell \mathbf{A}_1 \mathbf{k}^\top]_T && (18)
\end{aligned}$$

Here (16) is trivial; (14) and (18) follow from

$$\mathbf{u}_{j,x}^\top = \mathbf{M}_{x_j} \mathbf{u}_{j-1,x}^\top \bmod p, \ \forall j \in [\ell] \quad \text{and} \quad \Gamma(x) = 1 \Longleftrightarrow \mathbf{f}\mathbf{u}_{\ell,x}^\top \neq 0 \bmod p \tag{19}$$

by the definition in (11), the remaining equalities follow from:

$$\begin{aligned}
&(12) & \mathbf{s}_0 \mathbf{A}_1 \mathbf{D} \mathbf{u}^\top &= \mathbf{s}_0 \mathbf{A}_1 \cdot (\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\text{start}} \mathbf{R} \mathbf{u}^\top) - \mathbf{s}_0 \mathbf{A}_1 \mathbf{W}_{\text{start}} \cdot \mathbf{R}\mathbf{u}^\top\\
&(13) & \mathbf{s}_j \mathbf{A}_1 \mathbf{D} \mathbf{M}_{x_j} - \mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{D} &= \mathbf{s}_{j-1} \mathbf{A}_1 \cdot (-\mathbf{D} + \mathbf{Z}_{j \bmod 2} \mathbf{R}) + \mathbf{s}_j \mathbf{A}_1 \cdot (\mathbf{D}\mathbf{M}_{x_j} + \mathbf{W}_{x_j, j \bmod 2} \mathbf{R}) - (\mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{Z}_{j \bmod 2} + \mathbf{s}_j \mathbf{A}_1 \mathbf{W}_{x_j, j \bmod 2}) \cdot \mathbf{R}\\
&(15) & \mathbf{s}_\ell \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{D} &= \mathbf{s}_\ell \mathbf{A}_1 \cdot (\mathbf{k}^\top \mathbf{f} - \mathbf{D} + \mathbf{W}_{\text{end}} \mathbf{R}) - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{W}_{\text{end}} \cdot \mathbf{R}\\
&(17) & \mathbf{s}_\ell \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} \mathbf{u}_{\ell,x}^\top &= \mathbf{s}_0 \mathbf{A}_1 \mathbf{D} \mathbf{u}_{0,x}^\top + \textstyle\sum_{j=1}^{\ell} (\mathbf{s}_j \mathbf{A}_1 \mathbf{D} \mathbf{u}_{j,x}^\top - \mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{D} \mathbf{u}_{j-1,x}^\top) + (\mathbf{s}_\ell \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} \mathbf{u}_{\ell,x}^\top - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{D} \mathbf{u}_{\ell,x}^\top).
\end{aligned}$$

Security. We have the following theorem stating that our construction is selectively secure. We remark that our construction achieves semi-adaptive security as is and the proof is almost the same.

Theorem 1 (Selectively secure ABE for NFA$^{\oplus p}$). *The ABE scheme for NFA$^{\oplus p}$ in prime-order bilinear groups described above is selectively secure (cf. Section 2.1) under the k-Lin assumption with security loss $O(\ell \cdot |\Sigma|)$. Here ℓ is the length of the challenge input x^*.*

4.3 Game Sequence

The proof is analogous to GWW's proof. We show the proof in the one-key setting where the adversary asks for at most one secret key; this is sufficient to motivate the proof in the next section. As in [11], it is straightforward to handle many keys, see Appendix D.2 for more details. Let $x^* \in \Sigma^\ell$ denote the selective challenge and let $\bar{\ell} = \ell \bmod 2$. Without loss of generality, we assume $\ell > 1$. We begin with some auxiliary distributions.

Auxiliary distributions. We describe the auxiliary ciphertext and key distributions that we use in the proof. Throughout, the distributions are the same as the original distributions except for the so-called $\mathbf{a}_2$-components which is defined as below.

$\mathbf{a}_2$*-components.* For a ciphertext in the following form, capturing real and all auxiliary ciphertexts (defined below):

$$\mathsf{ct}_x = \begin{pmatrix} [\mathbf{c}_0]_1,\, [\mathbf{c}_0\mathbf{W}_{\text{start}}]_1 \\ \{[\mathbf{c}_j\mathbf{A}_1]_1, [\mathbf{c}_{j-1}\mathbf{Z}_{j \bmod 2} + \mathbf{c}_j\mathbf{W}_{x_j, j \bmod 2}]_1\}_j \\ [\mathbf{c}_\ell]_1, [\mathbf{c}_\ell\mathbf{W}_{\text{end}}]_1,\, [\mathbf{c}_\ell\mathbf{k}^\top]_T \cdot m \end{pmatrix} \text{ with } \mathbf{c}_j = \mathbf{s}_j\mathbf{A}_1 + s_j\mathbf{a}_2 + \tilde{\mathbf{s}}_j\mathbf{A}_3, \forall j \tag{20}$$

where $\mathbf{s}_j, \tilde{\mathbf{s}}_j \in \mathbb{Z}_p^k$ and $s_j \in \mathbb{Z}_p$, we define its $\mathbf{a}_2$-components, denoted by $\mathsf{ct}_x[2]$, as follows:

$$\mathsf{ct}_x[2] = \begin{pmatrix} [s_0]_1,\, [s_0\mathbf{a}_2\mathbf{W}_{\text{start}}]_1 \\ \{[s_j]_1, [s_{j-1}\mathbf{a}_2\mathbf{Z}_{j \bmod 2} + s_j\mathbf{a}_2\mathbf{W}_{x_j, j \bmod 2}]_1\}_j \\ [s_\ell]_1, [s_\ell\mathbf{a}_2\mathbf{W}_{\text{end}}]_1,\, [s_\ell\mathbf{a}_2\mathbf{k}^\top]_T \cdot m \end{pmatrix}.$$

For a key in the following form, capturing real and all auxiliary keys (defined below):

$$\mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{k}_0^\top]_2, [\mathbf{r}_0^\top]_2 \\ \{[\mathbf{K}_b]_2, [\mathbf{K}_{\sigma,b}]_2, [\mathbf{R}]_2\}_{\sigma,b} \\ [\mathbf{K}_{\text{end}}]_2, [\mathbf{R}]_2 \end{pmatrix} \tag{21}$$

where $\mathbf{k}_0 \in \mathbb{Z}_p^{1\times(2k+1)}$, $\mathbf{K}_b, \mathbf{K}_{\sigma,b}, \mathbf{K}_{\text{end}} \in \mathbb{Z}_p^{(2k+1)\times Q}$ and $\mathbf{r}_0 \in \mathbb{Z}_p^{1\times k}, \mathbf{R} \in \mathbb{Z}_p^{k\times Q}$, we define its $\mathbf{a}_2$-components, denoted by $\mathsf{sk}_\Gamma[2]$, as follows:

$$\mathsf{sk}_\Gamma[2] = \begin{pmatrix} [\mathbf{a}_2\mathbf{k}_0^\top]_2, [\mathbf{r}_0^\top]_2 \\ \{[\mathbf{a}_2\mathbf{K}_b]_2, [\mathbf{a}_2\mathbf{K}_{\sigma,b}]_2, [\mathbf{R}]_2\}_{\sigma,b} \\ [\mathbf{a}_2\mathbf{K}_{\text{end}}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

For notation simplicity of $\mathsf{ct}_x[2]$ and $\mathsf{sk}_\Gamma[2]$ with $\mathbf{k}, \mathbf{D}, \mathbf{W}_{\text{start}}, \mathbf{W}_{\text{end}}, \mathbf{Z}_b, \mathbf{W}_{\sigma,b}$, we write

$$\alpha = \mathbf{a}_2\mathbf{k}^\top,\ \mathbf{d} = \mathbf{a}_2\mathbf{D},\ \mathbf{w}_{\text{start}} = \mathbf{a}_2\mathbf{W}_{\text{start}},\ \mathbf{w}_{\text{end}} = \mathbf{a}_2\mathbf{W}_{\text{end}},\ \mathbf{z}_b = \mathbf{a}_2\mathbf{Z}_b,\ \mathbf{w}_{\sigma,b} = \mathbf{a}_2\mathbf{W}_{\sigma,b},\ \forall \sigma, b$$

and call them the $\mathbf{a}_2$-components of $\mathbf{k}^\top, \mathbf{D}, \mathbf{W}_{\text{start}}, \mathbf{W}_{\text{end}}, \mathbf{Z}_b, \mathbf{W}_{\sigma,b}$, respectively. We also omit zeroes and adjust the order of terms in $\mathsf{ct}_x[2]$. Furthermore, for all $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_3$, mpk and various forms of $\mathsf{ct}_x, \mathsf{sk}_\Gamma$ we will use in the proof, we have

$$\begin{gathered} \mathsf{ct}_x[2],\, \mathsf{sk}_\Gamma[2],\, \{\mathbf{A}_i\mathbf{k}^\top, \mathbf{A}_i\mathbf{D}, \mathbf{A}_i\mathbf{W}_{\text{start}}, \mathbf{A}_i\mathbf{W}_{\text{end}}, \mathbf{A}_i\mathbf{Z}_b, \mathbf{A}_i\mathbf{W}_{\sigma,b}\}_{i\in\{1,3\},\sigma\in\Sigma,b\in\{0,1\}} \\ \approx_s \mathsf{ct}_x[2],\, \mathsf{sk}_\Gamma[2],\, \{\mathbf{A}_i\widetilde{\mathbf{k}}^\top, \mathbf{A}_i\widetilde{\mathbf{D}}, \mathbf{A}_i\widetilde{\mathbf{W}}_{\text{start}}, \mathbf{A}_i\widetilde{\mathbf{W}}_{\text{end}}, \mathbf{A}_i\widetilde{\mathbf{Z}}_b, \mathbf{A}_i\widetilde{\mathbf{W}}_{\sigma,b}\}_{i\in\{1,3\},\sigma\in\Sigma,b\in\{0,1\}} \end{gathered}$$

where $\widetilde{\mathbf{k}} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}, \widetilde{\mathbf{D}} \leftarrow \mathbb{Z}_p^{(2k+1)\times Q}, \widetilde{\mathbf{W}}_{\text{start}}, \widetilde{\mathbf{W}}_{\text{end}}, \widetilde{\mathbf{Z}}_b, \widetilde{\mathbf{W}}_{\sigma,b} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ are fresh. This follows from Lemma 4 and the fact that all matrices $\mathbf{W} \in \mathbb{Z}_p^{(2k+1)\times k'}$ with $k' \in \mathbb{N}$ can be decomposed as

$$\mathbf{W} = \mathbf{A}_1^\parallel \cdot \mathbf{A}_1\mathbf{W} + \mathbf{a}_2^\parallel \cdot \mathbf{a}_2\mathbf{W} + \mathbf{A}_3^\parallel \cdot \mathbf{A}_3\mathbf{W}.$$

The property allows us to simulate $\mathsf{mpk}, \mathsf{ct}_x, \mathsf{sk}_\Gamma$ from $\mathsf{ct}_x[2], \mathsf{sk}_\Gamma[2]$ and $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_3$ so that we can focus on the crucial argument over $\mathbf{a}_2$-components in the proofs, e.g., those in Section 4.4, 4.5, 4.7 and 4.8.

Ciphertext distributions. We sample $s_0, s_1, \ldots, s_\ell \leftarrow \mathbb{Z}_p$ and define:

- for $i \in [0,\ell]$: $\mathsf{ct}^i_{x^*}$ is the same as ct_{x^*} except we replace $\mathbf{s}_i\mathbf{A}_1$ with $\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$;
- for $i \in [\ell]$: $\mathsf{ct}^{i-1,i}_{x^*}$ is the same as ct_{x^*} except we replace $\mathbf{s}_{i-1}\mathbf{A}_1, \mathbf{s}_i\mathbf{A}_1$ with $\mathbf{s}_{i-1}\mathbf{A}_1 + s_{i-1}\mathbf{a}_2, \mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$.

That is, we have: writing $\tau = i \bmod 2$,

$$\mathsf{ct}^i_{x^*}[2] = \begin{cases} [s_0\mathbf{w}_{\mathrm{start}}]_1,\ [s_0]_1,\ [s_0\mathbf{z}_1]_1 & \text{if } i = 0 \\ [s_i\mathbf{w}_{x^*_i,\tau}]_1,\ [s_i]_1,\ [s_i\mathbf{z}_{1-\tau}]_1 & \text{if } i \in [\ell-1] \\ [s_\ell\mathbf{w}_{x^*_\ell,\bar{\ell}}]_1,\ [s_\ell]_1,\ [s_\ell\mathbf{w}_{\mathrm{end}}]_1,\ [s_\ell\alpha]_T\cdot m_\beta & \text{if } i = \ell \end{cases}$$

$$\mathsf{ct}^{i-1,i}_{x^*}[2] = \begin{cases} [s_0\mathbf{w}_{\mathrm{start}}]_1,\ [s_0]_1,\ [s_0\mathbf{z}_1 + s_1\mathbf{w}_{x^*_1,1}]_1,\ [s_1]_1,\ [s_1\mathbf{z}_0]_1 & \text{if } i = 1 \\ [s_{i-1}\mathbf{w}_{x^*_{i-1},1-\tau}]_1,\ [s_{i-1}]_1,\ [s_{i-1}\mathbf{z}_\tau + s_i\mathbf{w}_{x^*_i,\tau}]_1,\ [s_i]_1,\ [s_i\mathbf{z}_{1-\tau}]_1 & \text{if } i \in [2,\ell-1] \\ [s_{\ell-1}\mathbf{w}_{x^*_{\ell-1},1-\bar{\ell}}]_1,\ [s_{\ell-1}]_1,\ [s_{\ell-1}\mathbf{z}_{\bar{\ell}} + s_\ell\mathbf{w}_{x^*_\ell,\bar{\ell}}]_1,\ [s_\ell]_1,\ [s_\ell\mathbf{w}_{\mathrm{end}}]_1,\ [s_\ell\alpha]_T\cdot m_\beta & \text{if } i = \ell \end{cases}$$

They are exactly the same as those used in GWW's proof [11].

Secret key distributions. Given $x^* \in \Sigma^\ell$ and $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$, we define

$$\mathbf{f}_{i,x^*} = \mathbf{f}\mathbf{M}_{x^*_\ell}\cdots\mathbf{M}_{x^*_{i+1}} \bmod p,\ \forall i \in [0,\ell]. \tag{22}$$

For all $i \in [\ell]$, we sample $\Delta \leftarrow \mathbb{Z}_p$ and define:

- sk^0_Γ is the same as sk_Γ except we replace $\mathbf{D}$ with $\mathbf{D} + \mathbf{a}^\parallel_2 \cdot s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*}$ in the term $[\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2$;
- sk^i_Γ is the same as sk_Γ except we replace $\mathbf{D}$ with $\mathbf{D} + \mathbf{a}^\parallel_2 \cdot s_i^{-1}\Delta\cdot\mathbf{f}_{i,x^*}$ in the term $[\mathbf{D}\mathbf{M}_{x^*_i} + \mathbf{W}_{x^*_i, i \bmod 2}\mathbf{R}]_2$;
- $\mathsf{sk}^{i-1,i}_\Gamma$ is the same as sk_Γ except we replace $-\mathbf{D}$ with $-\mathbf{D} + \mathbf{a}^\parallel_2 \cdot s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*}$ in the term $[-\mathbf{D} + \mathbf{Z}_{i \bmod 2}\mathbf{R}]_2$;
- $\mathsf{sk}^{\ell,*}_\Gamma$ is the same as sk_Γ except we replace $-\mathbf{D}$ with $-\mathbf{D} + \mathbf{a}^\parallel_2 \cdot s_\ell^{-1}\Delta\cdot\mathbf{f}_{\ell,x^*}$ in the term $[\mathbf{k}^\top\mathbf{f} - \mathbf{D} + \mathbf{W}_{\mathrm{end}}\mathbf{R}]_2$.

That is, we have: writing $\tau = i \bmod 2$,

$$\mathsf{sk}^0_\Gamma[2] = \begin{pmatrix} [(\mathbf{d} + \boxed{s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*}})\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\mathsf{sk}^i_\Gamma[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_\tau\mathbf{R}]_2, [(\mathbf{d} + \boxed{s_i^{-1}\Delta\cdot\mathbf{f}_{i,x^*}})\mathbf{M}_{x^*_i} + \mathbf{w}_{x^*_i,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\} \\ \{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\}_{\sigma\neq x^*_i} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\mathsf{sk}^{i-1,i}_\Gamma[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \boxed{s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*}} + \mathbf{z}_\tau\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\mathsf{sk}^{\ell,*}_\Gamma[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [\alpha\mathbf{f} - \mathbf{d} + \boxed{s_\ell^{-1}\Delta\cdot\mathbf{f}_{\ell,x^*}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

They are analogous to those used in GWW's proof [11] with a novel way to change $\mathbf{a}_2$-components[9]. Following the notations in Section 1.2, we use $\mathbf{d}'_i = s_i^{-1}\Delta\cdot\mathbf{f}_{i,x^*}$ rather than $\mathbf{d}'_i = \Delta\cdot\mathbf{f}_{i,x^*}$. We remark that they are essentially the same but the former helps to simplify the exposition of the proof. Also, we note that s_i is independent of the challenge input x^* which will be crucial for the adaptive security in the next section.

[9] We also change the definition of sk^i_Γ, $i \in [0,\ell]$, with the goal of improving the exposition.

Game sequence. As in GWW's proof, we prove Theorem 1 via a series of games summarized in Fig 6:

- G_0: Identical to the real game.
- G_1: Identical to G_0 except that the challenge ciphertext is $\mathsf{ct}^0_{x^*}$.
- $\mathsf{G}_{2.i.0}$, $i \in [\ell]$: In this game, the challenge ciphertext is $\mathsf{ct}^{i-1}_{x^*}$ and the secret key is sk^{i-1}_Γ.
- $\mathsf{G}_{2.i.1}$, $i \in [\ell]$: Identical to $\mathsf{G}_{2.i.0}$ except that the secret key is $\mathsf{sk}^{i-1,i}_\Gamma$.
- $\mathsf{G}_{2.i.2}$, $i \in [\ell]$: Identical to $\mathsf{G}_{2.i.1}$ except that the challenge ciphertext is $\mathsf{ct}^{i-1,i}_{x^*}$.
- $\mathsf{G}_{2.i.3}$, $i \in [\ell]$: Identical to $\mathsf{G}_{2.i.2}$ except that the secret key is sk^{i}_Γ.
- $\mathsf{G}_{2.i.4}$, $i \in [\ell]$: Identical to $\mathsf{G}_{2.i.3}$ except that the challenge ciphertext is $\mathsf{ct}^{i}_{x^*}$.
- G_3: Identical to $\mathsf{G}_{2.\ell.4}$ except that secret key is $\mathsf{sk}^{\ell,*}_\Gamma$.

Note that $\mathsf{G}_{2.1.0}$ is identical to G_1 except that the secret key is sk^0_Γ and we have $\mathsf{G}_{2.i.0} = \mathsf{G}_{2.i-1.4}$ for all $i \in [2,\ell]$. The remaining of this section will be devoted to proving the indistinguishability of each pair of adjacent games described above. The proofs will be analogous to those for GWW, however, crucially use the property of $\mathbf{f}_{0,x^*},\ldots,\mathbf{f}_{\ell,x^*}$.

Useful lemmas. Before proceed to the proof, we show the next lemma describing the property of $\mathbf{f}_{0,x^*},\ldots,\mathbf{f}_{\ell,x^*}$.

Lemma 5 (Property of $\{\mathbf{f}_{i,x^*}\}_{i\in[0,\ell]}$). *For any NFA$^{\oplus p}$ $\Gamma = (Q,\Sigma,\{\mathbf{M}_\sigma\},\mathbf{u},\mathbf{f})$ and input $x^* \in \Sigma^\ell$, we have:*

1. $\Gamma(x^*) = 0 \iff \mathbf{f}_{0,x^*}\mathbf{u}^\top = 0 \bmod p$;
2. $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{x^*_i} \bmod p$ *for all* $i \in [\ell]$;
3. $\mathbf{f}_{\ell,x^*} = \mathbf{f}$.

Proof. The lemma directly follows from the definitions of NFA$^{\oplus p}$ in Section 3 and $\mathbf{f}_{0,x^*},\ldots,\mathbf{f}_{\ell,x^*}$ in (22). □

4.4 Initializing

It is standard to prove $\mathsf{G}_0 \approx_c \mathsf{G}_1$, see Appendix D.1. We only show the proof sketch for $\mathsf{G}_1 \approx_c \mathsf{G}_{2.1.0}$.

Lemma 6 ($\mathsf{G}_1 = \mathsf{G}_{2.1.0}$)**.** *For all $\mathcal{A}$, we have*

$$\Pr[\langle\mathcal{A},\mathsf{G}_1\rangle = 1] = \Pr[\langle\mathcal{A},\mathsf{G}_{2.1.0}\rangle = 1].$$

Proof. Roughly, we will prove that

$$\big(\mathsf{mpk}, \mathsf{ct}^0_{x^*}, \boxed{\mathsf{sk}_\Gamma}\big) = \big(\mathsf{mpk}, \mathsf{ct}^0_{x^*}, \mathsf{sk}^0_\Gamma\big)$$

where we have

$$\mathsf{sk}_\Gamma[2] \;=\; \begin{pmatrix} [\boxed{\mathbf{du}^\top} + \mathbf{w}_{\mathrm{start}}\mathbf{Ru}^\top]_2, [\mathbf{Ru}^\top]_2 \\ \big\{[-\mathbf{d}+\mathbf{z}_b\mathbf{R}]_2, [\mathbf{dM}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix},$$

$$\mathsf{sk}^0_\Gamma[2] \;=\; \begin{pmatrix} [(\mathbf{d} + s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*})\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{Ru}^\top]_2, [\mathbf{Ru}^\top]_2 \\ \big\{[-\mathbf{d}+\mathbf{z}_b\mathbf{R}]_2, [\mathbf{dM}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix},$$

and

$$\mathsf{ct}^0_{x^*}[2] = \big([s_0\mathbf{w}_{\mathrm{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1]_1\big).$$

This follows from the statement:

$$\overbrace{\big\{\boxed{\mathbf{du}^\top} + \mathbf{w}_{\mathrm{start}}\mathbf{Ru}^\top, \mathbf{Ru}^\top\big\}}^{\mathsf{sk}_\Gamma[2]} = \overbrace{\big\{(\mathbf{d} + s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*})\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{Ru}^\top, \mathbf{Ru}^\top\big\}}^{\mathsf{sk}^0_\Gamma[2]} \text{ given } \mathbf{d}, \overbrace{\mathbf{w}_{\mathrm{start}}}^{\mathsf{ct}^0_{x^*}[2]}$$

which is implied by the fact $\Gamma(x^*) = 0 \iff \mathbf{f}_{0,x^*}\mathbf{u}^\top = 0 \bmod p$ (see Lemma 5). This is sufficient for the proof. □

Game	ct_{x^*}	$\mathsf{sk}_\Gamma[2]$						Remark
			$? \cdot \mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top$	$? \cdot \mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}$	$? + \mathbf{z}_\tau \mathbf{R}$	$? \cdot \mathbf{M}_{x^*_i} + \mathbf{w}_{x^*_i,\tau}\mathbf{R}$	$\alpha\mathbf{f} + ? + \mathbf{z}_{\text{end}}\mathbf{R}$	
0	ct_{x^*}	sk_Γ	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	real game
1	$\boxed{\mathsf{ct}^0_{x^*}}$	sk_Γ	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	SD
2.1.0	$\mathsf{ct}^0_{x^*}$	$\boxed{\mathsf{sk}^0_\Gamma}$	$\mathbf{d} + \boxed{s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{f}_{0,x^*}\mathbf{u}^\top = 0 \bmod p$ (Lemma 5)
2.i.0	$\mathsf{ct}^{i-1}_{x^*}$	sk^{i-1}_Γ	$\mathbf{d}$	$\mathbf{d} + s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$i \in [2,\ell]$
2.i.1	$\mathsf{ct}^{i-1}_{x^*}$	$\boxed{\mathsf{sk}^{i-1,i}_\Gamma}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d} + \boxed{s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*}}$	$\mathbf{d}$	$-\mathbf{d}$	change of variables + DDH
2.i.2	$\boxed{\mathsf{ct}^{i-1,i}_{x^*}}$	$\mathsf{sk}^{i-1,i}_\Gamma$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d} + s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*}$	$\mathbf{d}$	$-\mathbf{d}$	switching lemma
2.i.3	$\mathsf{ct}^{i-1,i}_{x^*}$	$\boxed{\mathsf{sk}^i_\Gamma}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d} + \boxed{s_i^{-1}\Delta \cdot \mathbf{f}_{i,x^*}}$	$-\mathbf{d}$	transition lemma, $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{x^*_i} \bmod p$ (Lemma 5)
2.i.4	$\boxed{\mathsf{ct}^i_{x^*}}$	sk^i_Γ	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d} + s_i^{-1}\Delta \cdot \mathbf{f}_{i,x^*}$	$-\mathbf{d}$	switching lemma
3	$\mathsf{ct}^\ell_{x^*}$	$\boxed{\mathsf{sk}^{\ell,*}_\Gamma}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d} + \boxed{s_\ell^{-1}\Delta \cdot \mathbf{f}_{\ell,x^*}}$	change of variables + DDH

Fig. 6. Game sequence for our selectively secure ABE for $\text{NFA}^{\oplus p}$ where $i \in [\ell]$. In the table, we only show the $\mathbf{a}_2$-components of secret key. In the **Remark** column, "SD" and "DDH" indicate $\text{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1,\mathbf{a}_2}$ and $\text{DDH}^{G_2}_{1,Q}$ assumption, respectively; switching lemma and transition lemma were given in GWW, cf. Lemma 16 and Lemma 13.

4.5 Switching secret keys I

In this section, we will show that $\mathsf{G}_{2.i.0} \approx_c \mathsf{G}_{2.i.1}$ for all $i \in [\ell]$ and $\mathsf{G}_{2.\ell.4} \approx_c \mathsf{G}_3$. The proofs for them are similar. We begin with the following lemma stating that $\mathsf{G}_{2.1.0} \approx_c \mathsf{G}_{2.1.1}$ and sketch the proofs for the remaining statements.

Lemma 7 **($\mathsf{G}_{2.1.0} \approx_c \mathsf{G}_{2.1.1}$).** *For all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.0}\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.1}\rangle = 1] \le O(|\Sigma|) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DDH}_{1,Q}^{G_2}}(\lambda).$$

Overview. Roughly, we will prove that

$$\big(\mathsf{mpk}, \mathsf{ct}^0_{x^*}, \boxed{\mathsf{sk}^0_\Gamma}\big) = \big(\mathsf{mpk}, \mathsf{ct}^0_{x^*}, \colorbox{lightgray}{$\mathsf{sk}^{0,1}_\Gamma$}\big)$$

By Lemma 4, we focus on $\mathbf{a}_2$-components and prove:

$$\mathsf{sk}^0_\Gamma[2] = \begin{pmatrix} [(\boxed{\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}})\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[\boxed{-\mathbf{d}} + \mathbf{z}_1\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[-\mathbf{d} + \mathbf{z}_0\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} \approx_c \begin{pmatrix} [\colorbox{lightgray}{$\mathbf{d}$}\,\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[\colorbox{lightgray}{$-\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$} + \mathbf{z}_1\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[-\mathbf{d} + \mathbf{z}_0\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} = \mathsf{sk}^{0,1}_\Gamma[2]$$

given

$$\mathsf{ct}^0_{x^*}[2] = \big([s_0\mathbf{w}_{\text{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1]_1\big).$$

Clearly, change of variables $\mathbf{d} \mapsto \mathbf{d} - s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$ is at the core of the above statement, which ensures that: for all s_0 and Δ, we have

$$\overbrace{\{(\boxed{\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}})\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top, \boxed{-\mathbf{d}} + \mathbf{z}_1\mathbf{R}, \mathbf{R}\}}^{\mathsf{sk}^0_\Gamma[2]} \approx_s \overbrace{\{\colorbox{lightgray}{$\mathbf{d}$}\,\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top, \colorbox{lightgray}{$-\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$} + \mathbf{z}_1\mathbf{R}, \mathbf{R}\}}^{\mathsf{sk}^{0,1}_\Gamma[2]} \quad \text{given } \overbrace{\mathbf{w}_{\text{start}}, \mathbf{z}_1}^{\mathsf{ct}^0_{x^*}[2]} \tag{23}$$

However this does not hold if $\mathbf{d}$ is also given out on the both sides which corresponds to $\mathbf{d}$'s appeared at other positions, as is our case. We address this issue by hiding other occurrences of $\mathbf{d}$'s via $\mathrm{DDH}_{1,Q}^{G_2}$ assumption before the change of variable and getting them back via $\mathrm{DDH}_{1,Q}^{G_2}$ assumption again after that.

Auxiliary hybrids. Formally, we need two more auxiliary hybrids:

- $\mathsf{G}_{2.1.0.a}$ is the same as $\mathsf{G}_{2.1.0}$ except that, for key query Γ, we return

$$\begin{pmatrix} [(\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*})\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_1\mathbf{R}]_2, [\boxed{\mathbf{0}} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[\boxed{\mathbf{0}} + \mathbf{z}_0\mathbf{R}]_2, [\boxed{\mathbf{0}} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \boxed{\mathbf{0}} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}.$$

- $\mathsf{G}_{2.1.1.a}$ is the same as $\mathsf{G}_{2.1.1}$ except that, for key query Γ, we return

$$\begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*} + \mathbf{z}_1\mathbf{R}]_2, [\boxed{\mathbf{0}} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[\boxed{\mathbf{0}} + \mathbf{z}_0\mathbf{R}]_2, [\boxed{\mathbf{0}} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \boxed{\mathbf{0}} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}.$$

Then we prove that:

$$\mathsf{G}_{2.1.0} \overset{\mathrm{DDH}}{\approx_c} \mathsf{G}_{2.1.0.a} \overset{(23)}{\approx_s} \mathsf{G}_{2.1.1.a} \overset{\mathrm{DDH}}{\approx_c} \mathsf{G}_{2.1.1} \tag{24}$$

which is summarized in Fig 7.

Game	$? \cdot \mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top$	$? + \mathbf{z}_1\mathbf{R}$	$? \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}$	$? + \mathbf{z}_0\mathbf{R}$	$? \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}$	$\alpha\mathbf{f} - ? + \mathbf{w}_{\mathrm{end}}\mathbf{R}$	Remark
2.1.0	$\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$\mathbf{d}$	$\mathsf{sk}_\Gamma^0[2]$
2.1.0.a	$\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$	$-\mathbf{d}$	$\boxed{\mathbf{0}}$	$\boxed{\mathbf{0}}$	$\boxed{\mathbf{0}}$	$\boxed{\mathbf{0}}$	DDH
2.1.1.a	$\mathbf{d}$	$-\mathbf{d} + \boxed{s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{d} \mapsto \mathbf{d} - s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$
2.1.1	$\mathbf{d}$	$-\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$	$\boxed{\mathbf{d}}$	$\boxed{-\mathbf{d}}$	$\boxed{\mathbf{d}}$	$\boxed{\mathbf{d}}$	DDH, $\mathsf{sk}_\Gamma^{0,1}[2]$

Fig. 7. Game sequence for $\mathsf{G}_{2.1.0} \approx_c \mathsf{G}_{2.1.1}$. In the table, we only show changes of secret key and focus on its $\mathbf{a}_2$-components; all secret key elements in the fourth and sixth column are quantified over $\sigma \in \Sigma$. In the **Remark** column, "DDH" indicates $\mathrm{DDH}_{1,Q}^{G_2}$ assumption.

Lemmas. We describe and prove the following lemmas which imply Lemma 7 by (24).

Lemma 8 ($\mathsf{G}_{2.1.0} \approx_c \mathsf{G}_{2.1.0.a}$)**.** *For all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.0}\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.0.a}\rangle = 1] \le O(|\Sigma|) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DDH}_{1,Q}^{G_2}}(\lambda).$$

Proof. By Lemma 4, it suffices to prove the lemma over $\mathbf{a}_2$-components which roughly means:

$$\mathsf{sk}_\Gamma^0[2] = \begin{pmatrix} [(\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*})\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_1\mathbf{R}]_2, [\boxed{\mathbf{d}} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[-\boxed{\mathbf{d}} + \mathbf{z}_0\mathbf{R}]_2, [\boxed{\mathbf{d}} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \boxed{\mathbf{d}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} \approx_c \begin{pmatrix} [(\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*})\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_1\mathbf{R}]_2, [\mathbf{0} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[\mathbf{0} + \mathbf{z}_0\mathbf{R}]_2, [\mathbf{0} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{0} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

in the presence of

$$\mathsf{ct}_{x^*}^0[2] = \big([s_0\mathbf{w}_{\mathrm{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1]_1\big).$$

One can sample basis $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_3, \mathbf{A}_1^\|, \mathbf{a}_2^\|, \mathbf{A}_3^\|$ and trivially simulate mpk, $\mathsf{ct}_{x^*}^0$ and secret key using terms given out above. Furthermore, this follows from $\mathrm{DDH}_{1,Q}^{G_2}$ assumption w.r.t $\mathbf{z}_0, \mathbf{w}_{\sigma,0}, \mathbf{w}_{\sigma,1}, \mathbf{w}_{\mathrm{end}}$ with $\sigma \in \Sigma$ which implies:

$$\big([\mathbf{z}_0\mathbf{R}]_2, \{[\mathbf{w}_{\sigma,0}\mathbf{R}]_2\}_{\sigma\in\Sigma}, \{[\mathbf{w}_{\sigma,1}\mathbf{R}]_2\}_{\sigma\in\Sigma}, [\mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2\big) \approx_c U\big((G_2^{1\times Q})^{2|\Sigma|+2} \times G_2^{k\times Q}\big)$$

where $\mathbf{z}_0, \mathbf{w}_{\sigma,0}, \mathbf{w}_{\sigma,1}, \mathbf{w}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1\times k}$ for all $\sigma \in \Sigma$ and $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times Q}$. Here we use the fact that $\mathsf{ct}_{x^*}^0[2]$ does not leak $\mathbf{z}_0$, $\mathbf{w}_{\sigma,1}$, $\mathbf{w}_{\sigma,0}$, $\mathbf{w}_{\mathrm{end}}$ with $\sigma \in \Sigma$. This completes the proof. □

Lemma 9. *For all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.0.a}\rangle = 1] = \Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.1.a}\rangle = 1].$$

Proof. This immediately follows from (23) implied by the change of variables: $\mathbf{d} \mapsto \mathbf{d} - s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$. □

Lemma 10. *For all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.1.a}\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.1}\rangle = 1] \le O(|\Sigma|) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DDH}_{1,Q}^{G_2}}(\lambda).$$

Proof. The proof is analogous to that for Lemma 8. □

Via the same proof idea, we can prove the following two lemmas stating that $\mathsf{G}_{2.i.0} \approx_c \mathsf{G}_{2.i.1}$ for all $i \in [2, \ell]$ and $\mathsf{G}_{2.\ell.4} \approx_c \mathsf{G}_3$, respectively. We only sketch the proof for each lemma.

Lemma 11 ($\mathsf{G}_{2.i.0} \approx_c \mathsf{G}_{2.i.1}$)**.** *For all $i \in [2, \ell]$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.i.0}\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.i.1}\rangle = 1] \le O(|\Sigma|) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DDH}_{1,Q}^{G_2}}(\lambda).$$

Proof (sketch). We will prove that

$$\big(\mathsf{mpk}, \mathsf{ct}^{i-1}_{x^*}, \boxed{\mathsf{sk}^{i-1}_{\Gamma}}\big) = \big(\mathsf{mpk}, \mathsf{ct}^{i-1}_{x^*}, \mathsf{sk}^{i-1,i}_{\Gamma}\big)$$

Recall that $\tau = i \bmod 2$, the proof is analogous to that for Lemma 7: roughly, we want to prove the following statement over $\mathbf{a}_2$-components:

$$\mathsf{sk}^{i-1}_{\Gamma}[2] \;=\; \begin{pmatrix} [\mathbf{d}\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^{\top}]_2, [\mathbf{R}\mathbf{u}^{\top}]_2 \\ \big\{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [(\boxed{\mathbf{d} + s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*}})\mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\} \\ \big\{[\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2\big\}_{\sigma\neq x^*_{i-1}} \\ \big\{[\boxed{-\mathbf{d}} + \mathbf{z}_{\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\approx_c \begin{pmatrix} [\mathbf{d}\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^{\top}]_2, [\mathbf{R}\mathbf{u}^{\top}]_2 \\ \big\{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\} \\ \big\{[\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2\big\}_{\sigma\neq x^*_{i-1}} \\ \big\{[-\mathbf{d} + s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*} + \mathbf{z}_{\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} = \mathsf{sk}^{i-1,i}_{\Gamma}[2]$$

given

$$\mathsf{ct}^{i-1}_{x^*}[2] = \big([s_{i-1}\mathbf{w}_{x^*_{i-1},1-\tau}]_1, [s_{i-1}]_1, [s_{i-1}\mathbf{z}_{\tau}]_1\big).$$

This relies on:

- change of variables $\mathbf{d} \mapsto \mathbf{d} - s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*}$; this ensures that, for all s_{i-1} and Δ, we have

  $$\overbrace{\big\{(\boxed{\mathbf{d} + s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*}})\mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}, \boxed{-\mathbf{d}} + \mathbf{z}_{\tau}\mathbf{R}, \mathbf{R}\big\}}^{\mathsf{sk}^{i-1}_{\Gamma}[2]} \approx_s \overbrace{\big\{\mathbf{d}\mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}, -\mathbf{d} + s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*} + \mathbf{z}_{\tau}\mathbf{R}, \mathbf{R}\big\}}^{\mathsf{sk}^{i-1,i}_{\Gamma}[2]}$$

  in the presence of $\mathbf{w}_{x^*_{i-1},1-\tau}, \mathbf{z}_{\tau}$ leaked via $\mathsf{ct}^{i-1}_{x^*}[2]$.
- $\mathrm{DDH}^{G_2}_{1,Q}$ assumption w.r.t $\mathbf{w}_{\mathrm{start}}, \mathbf{z}_{1-\tau}, \{\mathbf{w}_{\sigma,1-\tau}\}_{\sigma\neq x^*_{i-1}}, \{\mathbf{w}_{\sigma,\tau}\}_{\sigma\in\Sigma}, \mathbf{w}_{\mathrm{end}}$; this implies that

  $$\big([\mathbf{w}_{\mathrm{start}}\mathbf{R}]_2, [\mathbf{z}_{1-\tau}\mathbf{R}]_2, \big\{[\mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2\big\}_{\sigma\neq x^*_{i-1}}, \big\{[\mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\big\}_{\sigma\in\Sigma}, [\mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2\big) \approx_c U\big((G_2^{1\times Q})^{2|\Sigma|+2} \times G_2^{k\times Q}\big)$$

  and will be used to hide all $\mathbf{d}$'s irrelevant with the change of variables. □

Lemma 12 ($\mathsf{G}_{2.\ell.4} \approx_c \mathsf{G}_3$)**.** *For all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle\mathcal{A}, \mathsf{G}_{2.\ell.4}\rangle = 1] - \Pr[\langle\mathcal{A}, \mathsf{G}_3\rangle = 1] \leq O(|\Sigma|)\cdot\mathsf{Adv}^{\mathrm{DDH}^{G_2}_{1,Q}}_{\mathcal{B}}(\lambda).$$

Proof (sketch). We will prove that

$$\big(\mathsf{mpk}, \mathsf{ct}^{\ell}_{x^*}, \boxed{\mathsf{sk}^{\ell}_{\Gamma}}\big) = \big(\mathsf{mpk}, \mathsf{ct}^{\ell}_{x^*}, \mathsf{sk}^{\ell,*}_{\Gamma}\big)$$

Recall that $\bar{\ell} = \ell \bmod 2$, the proof is analogous to that for Lemma 7: roughly, we want to prove the following statement over $\mathbf{a}_2$-components:

$$\mathsf{sk}^{\ell}_{\Gamma}[2] \;=\; \begin{pmatrix} [\mathbf{d}\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^{\top}]_2, [\mathbf{R}\mathbf{u}^{\top}]_2 \\ \big\{[-\mathbf{d} + \mathbf{z}_{\bar{\ell}}\mathbf{R}]_2, [(\boxed{\mathbf{d} + s_{\ell}^{-1}\Delta\cdot\mathbf{f}_{\ell,x^*}})\mathbf{M}_{x^*_{\ell}} + \mathbf{w}_{x^*_{\ell},\bar{\ell}}\mathbf{R}]_2, [\mathbf{R}]_2\big\} \\ \big\{[\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,\bar{\ell}}\mathbf{R}]_2\big\}_{\sigma\neq x^*_{\ell}} \\ \big\{[-\mathbf{d} + \mathbf{z}_{1-\bar{\ell}}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,1-\bar{\ell}}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f}\,\boxed{-\mathbf{d}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\approx_c \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \big\{[-\mathbf{d}+\mathbf{z}_{\bar\ell}\mathbf{R}]_2, [\colorbox{lightgray}{$\mathbf{d}$}\mathbf{M}_{x^*_\ell} + \mathbf{w}_{x^*_\ell,\bar\ell}\mathbf{R}]_2, [\mathbf{R}]_2\big\} \\ \big\{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\bar\ell}\mathbf{R}]_2\big\}_{\sigma\neq x^*_\ell} \\ \big\{[-\mathbf{d}+\mathbf{z}_{1-\bar\ell}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\bar\ell}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f}\ \colorbox{lightgray}{$-\mathbf{d}+s_\ell^{-1}\Delta\cdot\mathbf{f}_{\ell,x^*}$} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} = \mathsf{sk}_\Gamma^{\ell,*}[2]$$

given

$$\mathsf{ct}_{x^*}^\ell[2] = \big([s_\ell\mathbf{w}_{x^*_\ell,\bar\ell}]_1, [s_\ell]_1, [s_\ell\mathbf{w}_{\text{end}}]_1, [s_\ell\alpha]_T\cdot m_\beta\big).$$

This relies on:

- change of variables $\mathbf{d}\mapsto\mathbf{d}-s_\ell^{-1}\Delta\cdot\mathbf{f}_{\ell,x^*}$; this ensures that, for all s_ℓ and Δ, we have

$$\overbrace{\big\{(\boxed{\mathbf{d}+s_\ell^{-1}\Delta\cdot\mathbf{f}_{\ell,x^*}})\mathbf{M}_{x^*_\ell} + \mathbf{w}_{x^*_\ell,\bar\ell}\mathbf{R}, \boxed{-\mathbf{d}} + \mathbf{w}_{\text{end}}\mathbf{R}, \mathbf{R}\big\}}^{\mathsf{sk}_\Gamma^\ell[2]} \approx_s \overbrace{\big\{\colorbox{lightgray}{$\mathbf{d}$}\mathbf{M}_{x^*_\ell} + \mathbf{w}_{x^*_\ell,\bar\ell}\mathbf{R}, \colorbox{lightgray}{$-\mathbf{d}+s_\ell^{-1}\Delta\cdot\mathbf{f}_{\ell,x^*}$} + \mathbf{w}_{\text{end}}\mathbf{R}, \mathbf{R}\big\}}^{\mathsf{sk}_\Gamma^{\ell,*}[2]}$$

  in the presence of $\mathbf{w}_{x^*_\ell,\bar\ell}, \mathbf{w}_{\text{end}}$ leaked via $\mathsf{ct}_{x^*}^\ell[2]$.
- $\mathrm{DDH}_{1,Q}^{G_2}$ assumption w.r.t $\mathbf{w}_{\text{start}}, \mathbf{z}_0, \mathbf{z}_1, \{\mathbf{w}_{\sigma,\bar\ell}\}_{\sigma\neq x^*_\ell}, \{\mathbf{w}_{\sigma,1-\bar\ell}\}_{\sigma\in\Sigma}$; this implies that

$$\big([\mathbf{w}_{\text{start}}\mathbf{R}]_2, [\mathbf{z}_0\mathbf{R}]_2, [\mathbf{z}_1\mathbf{R}]_2, \big\{[\mathbf{w}_{\sigma,\bar\ell}\mathbf{R}]_2\big\}_{\sigma\neq x^*_\ell}, \big\{[\mathbf{w}_{\sigma,1-\bar\ell}\mathbf{R}]_2\big\}_{\sigma\in\Sigma}, [\mathbf{R}]_2\big) \approx_c U\big((G_2^{1\times Q})^{2|\Sigma|+2}\times G_2^{k\times Q}\big)$$

  and will be used to hide all $\mathbf{d}$'s irrelevant with the change of variables. □

4.6 Switching ciphertexts

In this section, we show that $\mathsf{G}_{2.i.1}\approx_c\mathsf{G}_{2.i.2}$ and $\mathsf{G}_{2.i.3}\approx_c\mathsf{G}_{2.i.4}$ for all $i\in[\ell]$ using the switching lemma from GWW [11].

Lemma 13 **($(\mathbf{s},\mathbf{W})$-switching lemma [11]).** *We have*

$$\begin{aligned} &\mathsf{aux},\ [\mathbf{s}\mathbf{A}_1]_1, \qquad\qquad [\mathbf{a}_2^\parallel\cdot\bar\Delta + \mathbf{W}\mathbf{r}^\top]_2,\ [\mathbf{r}^\top]_2 \\ \approx_c\ &\mathsf{aux},\ [\mathbf{s}\mathbf{A}_1 + \boxed{s\mathbf{a}_2}]_1,\ [\mathbf{a}_2^\parallel\cdot\bar\Delta + \mathbf{W}\mathbf{r}^\top]_2,\ [\mathbf{r}^\top]_2 \end{aligned}$$

where $\mathsf{aux} = ([\mathbf{A}_1,\mathbf{a}_2,\mathbf{A}_1\mathbf{W},\mathbf{a}_2\mathbf{W}]_1, [\mathbf{W}\mathbf{B},\mathbf{B}]_2)$ *and* $\mathbf{W}\leftarrow\mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B}\leftarrow\mathbb{Z}_p^{k\times k}$, $\mathbf{s},\mathbf{r}\leftarrow\mathbb{Z}_p^{1\times k}$, $\bar\Delta, s\leftarrow\mathbb{Z}_p$. *Concretely, the advantage function* $\mathsf{Adv}_{\mathcal{B}}^{\text{SWITCH}}(\lambda)$ *is bounded by* $O(1)\cdot\mathsf{Adv}_{\mathcal{B}_0}^{k\text{-LIN}}(\lambda)$ *with* $\mathsf{Time}(\mathcal{B}_0)\approx\mathsf{Time}(\mathcal{B})$.

We begin with the following lemma stating that $\mathsf{G}_{2.i.1}\approx_c\mathsf{G}_{2.i.2}$ for all $i\in[\ell]$ and sketch the proof of $\mathsf{G}_{2.i.3}\approx_c\mathsf{G}_{2.i.4}$ for all $i\in[\ell]$, which is analogous.

Lemma 14 **($\mathsf{G}_{2.i.1}\approx_c\mathsf{G}_{2.i.2}$).** *For all* $i\in[\ell]$ *and all* $\mathcal{A}$, *there exists* $\mathcal{B}$ *with* $\mathsf{Time}(\mathcal{B})\approx\mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle\mathcal{A},\mathsf{G}_{2.i.1}\rangle = 1] - \Pr[\langle\mathcal{A},\mathsf{G}_{2.i.2}\rangle = 1] \leq \mathsf{Adv}_{\mathcal{B}}^{\text{SWITCH}}(\lambda).$$

Overview. We will prove that

$$\big(\mathsf{mpk}, \boxed{\mathsf{ct}_{x^*}^{i-1}}, \mathsf{sk}_\Gamma^{i-1,i}\big) \approx_c \big(\mathsf{mpk}, \colorbox{lightgray}{$\mathsf{ct}_{x^*}^{i-1,i}$}, \mathsf{sk}_\Gamma^{i-1,i}\big).$$

This roughly means that we will show that

$$\overbrace{[\mathbf{s}_i\mathbf{A}_1]_1}^{\mathsf{ct}_{x^*}^{i-1}} \approx_c \overbrace{[\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2]_1}^{\mathsf{ct}_{x^*}^{i-1,i}} \quad \text{given} \quad \overbrace{[-\mathbf{D}+\mathbf{a}_2^\parallel\cdot s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*} + \mathbf{Z}_\tau\mathbf{R}]_2, [\mathbf{R}]_2}^{\mathsf{sk}_\Gamma^{i-1,i}}.$$

The occurrence of $\mathbf{a}_2^\parallel$ hinders a direct application of $\mathrm{SD}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{a}_2}^{G_1}$ assumption. We will use $(\mathbf{s}_i,\mathbf{Z}_\tau)$-switching lemma in the proof, which roughly states that $[\mathbf{s}_i\mathbf{A}_1]_1\approx_c[\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2]_1$ given $[\mathbf{a}_2^\parallel\cdot\bar\Delta + \mathbf{Z}_\tau\mathbf{r}^\top]_2$ and $[\mathbf{r}^\top]_2$; the auxiliary terms given out in the lemma will be used to simulate the terms involving $\mathbf{a}_2^\parallel$.

Proof. Recall that $\tau = i \bmod 2$. We prove the lemma using $(\mathbf{s}_i, \mathbf{Z}_\tau)$-switching lemma. On input

$$\mathsf{aux},\ [\mathbf{c}_i]_1,\ [\mathbf{a}_2^{\parallel} \cdot \bar{\Delta} + \mathbf{Z}_\tau \mathbf{r}^\top]_2,\ [\mathbf{r}^\top]_2$$

where $\mathsf{aux} = ([\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_1\mathbf{Z}_\tau, \mathbf{a}_2\mathbf{Z}_\tau]_1, [\mathbf{Z}_\tau\mathbf{B}, \mathbf{B}]_2)$ and $\mathbf{Z}_\tau \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{r} \leftarrow \mathbb{Z}_p^{1\times k}$, $\bar{\Delta} \leftarrow \mathbb{Z}_p$ and

$$\mathbf{c}_i = \boxed{\mathbf{s}_i\mathbf{A}_1} \text{ or } \mathbf{c}_i = \colorbox{lightgray}{$\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$}, \quad \mathbf{s}_i \leftarrow \mathbb{Z}_p^{1\times k}, s_i \leftarrow \mathbb{Z}_p$$

the reduction works as follows:

(Simulating mpk**)** We sample $\mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}, \mathbf{W}_{\text{start}}, \mathbf{Z}_{1-\tau}, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{W}_{\text{end}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ for all $\sigma \in \Sigma$, and then we can trivially simulate mpk from $[\mathbf{A}_1, \mathbf{A}_1\mathbf{Z}_\tau]_1$.

(Simulating challenge ciphertext) On input (m_0, m_1), we want to create a challenge ciphertext in the following form, which is either $\mathsf{ct}_{x^*}^{i-1}$ or $\mathsf{ct}_{x^*}^{i-1,i}$ depending on $\mathbf{c}_i$:

$$\begin{pmatrix} [\mathbf{c}_0]_1,\ [\mathbf{c}_0\mathbf{W}_{\text{start}}]_1 \\ \left\{[\mathbf{c}_j]_1, \boxed{[\mathbf{c}_{j-1}\mathbf{Z}_\tau]_1} \cdot [\mathbf{c}_j\mathbf{W}_{x_j^*,\tau}]_1\right\}_{j=i \bmod 2} \\ \left\{[\mathbf{c}_j]_1, [\mathbf{c}_{j-1}\mathbf{Z}_{1-\tau}]_1 \cdot [\mathbf{c}_j\mathbf{W}_{x_j^*,1-\tau}]_1\right\}_{j\neq i \bmod 2} \\ [\mathbf{c}_\ell]_1, [\mathbf{c}_\ell\mathbf{W}_{\text{end}}]_1,\ [\mathbf{c}_\ell\mathbf{k}^\top]_T \cdot m_\beta \end{pmatrix} \text{ where } \begin{cases} \mathbf{c}_i \in \{\boxed{\mathbf{s}_i\mathbf{A}_1}, \colorbox{lightgray}{$\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$}\} \\ \mathbf{c}_{i-1} = \mathbf{s}_{i-1}\mathbf{A}_1 + s_{i-1}\mathbf{a}_2 \\ \mathbf{c}_j = \mathbf{s}_j\mathbf{A}_1 \quad \forall j \notin \{i-1, i\} \end{cases}$$

Observe that,

- when $\mathbf{c}_i = \boxed{\mathbf{s}_i\mathbf{A}_1}$, the distribution is identical to $\boxed{\mathsf{ct}_{x^*}^{i-1}}$;
- when $\mathbf{c}_i = \colorbox{lightgray}{$\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$}$, the distribution is identical to $\colorbox{lightgray}{$\mathsf{ct}_{x^*}^{i-1,i}$}$.

We proceed to create the challenge ciphertext as follows:

- We sample $s_{i-1} \leftarrow \mathbb{Z}_p$, $\mathbf{s}_j \leftarrow \mathbb{Z}_p^{1\times k}$ for all $j \neq i$ and simulate $\{[\mathbf{c}_j]_1\}_{j\neq i}$ using $[\mathbf{A}_1, \mathbf{a}_2]_1$; note that $[\mathbf{c}_i]_1$ is given out in the lemma as the challenge term.
- We rewrite terms in the dashed box as:

$$[\mathbf{c}_j\mathbf{Z}_\tau]_1 = \begin{cases} [\mathbf{s}_j\mathbf{A}_1\mathbf{Z}_\tau]_1 & \text{if } j \neq i-1 \text{ and } j \neq i \bmod 2 \\ [\mathbf{s}_{i-1}\mathbf{A}_1\mathbf{Z}_\tau]_1 \cdot [s_{i-1}\mathbf{a}_2\mathbf{Z}_\tau]_1 & \text{if } j = i-1 \text{ (and } j \neq i \bmod 2) \end{cases}$$

  which can be simulated using $\{\mathbf{s}_j\}_{j\neq i \bmod 2}$, s_{i-1} and $[\mathbf{A}_1\mathbf{Z}_\tau, \mathbf{a}_2\mathbf{Z}_\tau]_1$; here we use the fact that we do not have any terms involving $[\mathbf{c}_i\mathbf{Z}_\tau]_1$ in the challenge ciphertext.
- We simulate all remaining terms using $\{[\mathbf{c}_j]_1\}_{j\in[0,\ell]}$ and $\mathbf{k}, \mathbf{W}_{\text{start}}, \mathbf{Z}_{1-\tau}, \{\mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma}, \mathbf{W}_{\text{end}}$.

(Simulating secret key) On input Γ, we want to return a secret key for Γ in the form

$$\mathsf{sk}_\Gamma^{i-1,i} = \begin{pmatrix} [\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \left\{\boxed{[-\mathbf{D} + \mathbf{a}_2^{\parallel} \cdot s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*} + \mathbf{Z}_\tau\mathbf{R}]_2}, [\mathbf{D}\mathbf{M}_\sigma + \mathbf{W}_{\sigma,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\right\}_{\sigma\in\Sigma} \\ \left\{[-\mathbf{D} + \mathbf{Z}_{1-\tau}\mathbf{R}]_2, [\mathbf{D}\mathbf{M}_\sigma + \mathbf{W}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\right\}_{\sigma\in\Sigma} \\ [\mathbf{k}^\top\mathbf{f} - \mathbf{D} + \mathbf{W}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}.$$

We sample $\mathbf{D} \leftarrow \mathbb{Z}_p^{(2k+1)\times Q}$ and $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{k\times Q}$ and implicitly set

$$\Delta = s_{i-1}\bar{\Delta} \quad \text{and} \quad \mathbf{R} = \mathbf{r}^\top \cdot \mathbf{f}_{i-1,x^*} + \mathbf{B} \cdot \widetilde{\mathbf{R}}.$$

We proceed to simulate $\mathsf{sk}_\Gamma^{i-1,i}$ as follows:

- We simulate $[\mathbf{R}]_2$ from $[\mathbf{r}^\top]_2, [\mathbf{B}]_2$ and $\mathbf{f}_{i-1,x^*}, \widetilde{\mathbf{R}}$.

- We can rewrite the term in the dashed box as:

$$[-\mathbf{D} + (\mathbf{a}_2^{\parallel} \cdot \bar{\Delta} + \mathbf{Z}_\tau \mathbf{r}^\top) \cdot \mathbf{f}_{i-1,x^*} + \mathbf{Z}_\tau \mathbf{B} \cdot \widetilde{\mathbf{R}}]_2$$

  which can be simulated using $[\mathbf{a}_2^{\parallel} \cdot \bar{\Delta} + \mathbf{Z}_\tau \mathbf{r}^\top]_2$, $[\mathbf{Z}_\tau \mathbf{B}]_2$ and $\mathbf{D}, \mathbf{f}_{i-1,x^*}, \widetilde{\mathbf{R}}$.
- We simulate all remaining terms using $[\mathbf{R}]_2$ and $\mathbf{k}, \mathbf{D}, \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_{1-\tau}, \mathbf{W}_{\sigma,\tau}, \mathbf{W}_{\sigma,1-\tau}, \mathbf{W}_{\mathrm{end}}$.

Observe that, when $\mathbf{c}_i = \boxed{\mathbf{s}_i \mathbf{A}_1}$, the challenge ciphertext is $\boxed{\mathsf{ct}_{x^*}^{i-1}}$ and the simulation is identical to $\mathsf{G}_{2.i.1}$; when $\mathbf{c}_i = \colorbox{lightgray}{$\mathbf{s}_i \mathbf{A}_1 + s_i \mathbf{a}_2$}$, the challenge ciphertext is $\colorbox{lightgray}{$\mathsf{ct}_{x^*}^{i-1,i}$}$ and the simulation is identical to $\mathsf{G}_{2.i.2}$. This completes the proof. □

Via the same idea, we can prove the following lemmas stating that $\mathsf{G}_{2.i.3} \approx_c \mathsf{G}_{2.i.4}$ for all $i \in [\ell]$. We only sketch the proof by highlighting the difference.

Lemma 15 ($\mathsf{G}_{2.i.3} \approx_c \mathsf{G}_{2.i.4}$)**.** *For all $i \in [\ell]$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.i.3} \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.i.4} \rangle = 1] \leq \mathsf{Adv}_{\mathcal{B}}^{\mathrm{SWITCH}}(\lambda).$$

Proof (sketch). We will prove that

$$\big(\mathsf{mpk}, \boxed{\mathsf{ct}_{x^*}^{i-1,i}}, \mathsf{sk}_\Gamma^i\big) \approx_c \big(\mathsf{mpk}, \colorbox{lightgray}{$\mathsf{ct}_{x^*}^{i}$}, \mathsf{sk}_\Gamma^i\big)$$

which roughly means that we need to prove that

$$\overbrace{[\mathbf{s}_{i-1}\mathbf{A}_1 + s_{i-1}\mathbf{a}_2]_1}^{\mathsf{ct}_{x^*}^{i-1,i}} \approx_c \overbrace{[\mathbf{s}_{i-1}\mathbf{A}_1]_1}^{\mathsf{ct}_{x^*}^{i}} \quad \text{given} \quad \overbrace{[\mathbf{D}\mathbf{M}_{x_i^*} + \mathbf{a}_2^{\parallel} \cdot s_i^{-1} \Delta \cdot \mathbf{f}_{i,x^*} + \mathbf{W}_{x_i^*,\tau}\mathbf{R}]_2, [\mathbf{R}]_2}^{\mathsf{sk}_\Gamma^i}.$$

The proof is analogous to that of Lemma 14 except that we use $(\mathbf{s}_{i-1}, \mathbf{W}_{x_i^*,\tau})$-switching lemma instead of $(\mathbf{s}_i, \mathbf{Z}_\tau)$-switching lemma so that we can simulate the challenge ciphertext from the challenge term in the lemma and simulate secret key using the auxiliary terms given out in the lemma. □

4.7 Switching secret keys II

This section proves $\mathsf{G}_{2.i.2} \approx_c \mathsf{G}_{2.i.3}$ for all $i \in [\ell]$ using the the transition lemma from GWW [11].

Lemma 16 (**($\mathbf{z}, \mathbf{w}$)-transition lemma [11]**)**.** *For all $s_{i-1}, s_i \neq 0$ and $\bar{\Delta} \in \mathbb{Z}_p$, we have*

$$\begin{aligned} &\mathsf{aux},\ s_{i-1}\mathbf{z} + s_i\mathbf{w},\ [\boxed{s_{i-1}^{-1}\bar{\Delta}} + \mathbf{z}\mathbf{r}^\top]_2, && [\mathbf{w}\mathbf{r}^\top]_2,\ [\mathbf{r}^\top]_2 \\ \approx_c\ &\mathsf{aux},\ s_{i-1}\mathbf{z} + s_i\mathbf{w}, \qquad [\mathbf{z}\mathbf{r}^\top]_2, && [\boxed{s_i^{-1}\bar{\Delta}} + \mathbf{w}\mathbf{r}^\top]_2,\ [\mathbf{r}^\top]_2 \end{aligned}$$

where $\mathsf{aux} = ([\mathbf{z}\mathbf{B}, \mathbf{w}\mathbf{B}, \mathbf{B}]_2)$ *and* $\mathbf{z}, \mathbf{w} \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{r} \leftarrow \mathbb{Z}_p^{1\times k}$. *Concretely, the advantage function* $\mathsf{Adv}_{\mathcal{B}}^{\mathrm{TRANS}}(\lambda)$ *is bounded by* $O(1) \cdot \mathsf{Adv}_{\mathcal{B}_0}^{k\text{-}\mathrm{LIN}}(\lambda)$ *with* $\mathsf{Time}(\mathcal{B}_0) \approx \mathsf{Time}(\mathcal{B})$.

Lemma 17 ($\mathsf{G}_{2.i.2} \approx_c \mathsf{G}_{2.i.3}$)**.** *For all $i \in [\ell]$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.i.2} \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.i.3} \rangle = 1] \leq \mathsf{Adv}_{\mathcal{B}}^{\mathrm{TRANS}}(\lambda).$$

Overview. This roughly means

$$\big(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \boxed{\mathsf{sk}_\Gamma^{i-1,i}}\big) \approx_c \big(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \colorbox{lightgray}{sk_Γ^{i}}\big);$$

more concretely, we want to prove the following statement over $\mathbf{a}_2$-components:

$$\begin{aligned} &[-\mathbf{d} + \boxed{s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*} + \mathbf{z}_\tau \mathbf{R}}]_2, && [\mathbf{d}\mathbf{M}_{x_i^*} + \boxed{\mathbf{w}_{x_i^*,\tau}\mathbf{R}}]_2,\ [\mathbf{R}]_2 && //\mathsf{sk}_\Gamma^{i-1,i}[2] \\ \approx_c\ &[-\mathbf{d} + \colorbox{lightgray}{$\mathbf{z}_\tau \mathbf{R}$}]_2,\ [\mathbf{d}\mathbf{M}_{x_i^*} + && \colorbox{lightgray}{$s_i^{-1}\Delta \cdot \mathbf{f}_{i,x^*}\mathbf{M}_{x_i^*} + \mathbf{w}_{x_i^*,\tau}\mathbf{R}$}]_2,\ [\mathbf{R}]_2 && //\mathsf{sk}_\Gamma^{i}[2] \end{aligned}$$

given $\mathbf{d}, \Delta, s_{i-1}, s_i, s_{i-1}\mathbf{z}_\tau + s_i \mathbf{w}_{x_i^*,\tau}$ revealed by $\mathsf{ct}_{x^*}^{i-1,i}$. This can be handled by the $(\mathbf{z}_\tau, \mathbf{w}_{x_i^*,\tau})$-transition lemma and the fact that $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{x_i^*} \bmod p$ (see Lemma 5).

Proof. Recall that $\tau = i \bmod 2$. By Lemma 4, it suffices to prove the lemma over $\mathbf{a}_2$-components which roughly means:

$$\mathsf{sk}_{\Gamma}^{i-1,i}[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^{\top}]_2, [\mathbf{R}\mathbf{u}^{\top}]_2 \\ [-\mathbf{d} + \boxed{s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*} + \mathbf{z}_{\tau}\mathbf{R}}]_2, [\mathbf{d}\mathbf{M}_{x_i^*} + \boxed{\mathbf{w}_{x_i^*,\tau}\mathbf{R}}]_2, [\mathbf{R}]_2 \\ \{[\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\}_{\sigma \neq x_i^*} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma \in \Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\approx_c \begin{pmatrix} [\mathbf{d}\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^{\top}]_2, [\mathbf{R}\mathbf{u}^{\top}]_2 \\ [-\mathbf{d} + \colorbox{lightgray}{$\mathbf{z}_{\tau}\mathbf{R}$}]_2, [\mathbf{d}\mathbf{M}_{x_i^*} + \colorbox{lightgray}{$s_i^{-1}\Delta \cdot \mathbf{f}_{i,x^*}\mathbf{M}_{x_i^*} + \mathbf{w}_{x_i^*,\tau}\mathbf{R}$}]_2, [\mathbf{R}]_2 \\ \{[\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\}_{\sigma \neq x_i^*} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma \in \Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} = \mathsf{sk}_{\Gamma}^{i}[2]$$

in the presence of

$$\mathsf{ct}_{x^*}^{i-1,i}[2] = \begin{cases} [s_0\mathbf{w}_{\mathrm{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1 + s_1\mathbf{w}_{x_1^*,1}]_1, [s_1]_1, [s_1\mathbf{z}_0]_1 & \text{if } i = 1 \\ [s_{i-1}\mathbf{w}_{x_{i-1}^*,1-\tau}]_1, [s_{i-1}]_1, [s_{i-1}\mathbf{z}_{\tau} + s_i\mathbf{w}_{x_i^*,\tau}]_1, [s_i]_1, [s_i\mathbf{z}_{1-\tau}]_1 & \text{if } i \in [2, \ell - 1] \\ [s_{\ell-1}\mathbf{w}_{x_{\ell-1}^*,1-\bar{\ell}}]_1, [s_{\ell-1}]_1, [s_{\ell-1}\mathbf{z}_{\bar{\ell}} + s_{\ell}\mathbf{w}_{x_{\ell}^*,\bar{\ell}}]_1, [s_{\ell}]_1, [s_{\ell}\mathbf{w}_{\mathrm{end}}]_1, [s_{\ell}\alpha]_T \cdot m_{\beta} & \text{if } i = \ell \end{cases}$$

One can sample basis $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_3, \mathbf{A}_1^{\parallel}, \mathbf{a}_2^{\parallel}, \mathbf{A}_3^{\parallel}$ and trivially simulate mpk, $\mathsf{ct}_{x^*}^{i-1,i}$ and secret key using terms given out above. Furthermore, we prove this using $(\mathbf{z}_{\tau}, \mathbf{w}_{x_i^*,\tau})$-transition lemma. On input

$$\mathsf{aux}, [\bar{\Delta}_0 + \mathbf{z}_{\tau}\mathbf{r}^{\top}]_2, [\bar{\Delta}_1 + \mathbf{w}_{x_i^*,\tau}\mathbf{r}^{\top}]_2, [\mathbf{r}^{\top}]_2$$

where $(\bar{\Delta}_0, \bar{\Delta}_1) \in \{\boxed{(s_{i-1}^{-1}\bar{\Delta}, 0)}, \colorbox{lightgray}{$(0, s_i^{-1}\bar{\Delta})$}\}$ and

$$\mathsf{aux} = (\bar{\Delta}, s_{i-1}, s_i, s_{i-1}\mathbf{z}_{\tau} + s_i\mathbf{w}_{x_i^*,\tau}, [\mathbf{z}_{\tau}\mathbf{B}, \mathbf{w}_{x_i^*,\tau}\mathbf{B}, \mathbf{B}]_2)$$

with $\mathbf{z}_{\tau}, \mathbf{w}_{x_i^*,\tau} \leftarrow \mathbb{Z}_p^{1 \times k}, \mathbf{B} \leftarrow \mathbb{Z}_p^{k \times k}, \mathbf{r} \leftarrow \mathbb{Z}_p^{1 \times k}$ and $\bar{\Delta} \leftarrow \mathbb{Z}_p$, we sample $\alpha \leftarrow \mathbb{Z}_p, \mathbf{w}_{\mathrm{start}}, \mathbf{z}_{1-\tau}, \mathbf{w}_{\sigma,1-\tau}, \mathbf{w}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1 \times k}$ for all $\sigma \in \Sigma$ and $\mathbf{w}_{\sigma,\tau} \leftarrow \mathbb{Z}_p^{1 \times k}$ for all $\sigma \neq x_i^*$ and proceed as follows:

(Simulating challenge ciphertext) On input (m_0, m_1), we trivially simulate $\mathsf{ct}_{x^*}^{i-1,i}[2]$ using $s_{i-1}, s_i, s_{i-1}\mathbf{z}_{\tau} + s_i\mathbf{w}_{x_i^*,\tau}$ in aux and α, $\mathbf{w}_{\mathrm{start}}$, $\mathbf{w}_{\sigma,1-\tau}$, $\mathbf{z}_{1-\tau}$, $\mathbf{w}_{\mathrm{end}}$ as well.

(Simulating secret key) On input Γ, we want to return a secret key for Γ in the form:

$$\begin{pmatrix} [\mathbf{d}\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^{\top}]_2, [\mathbf{R}\mathbf{u}^{\top}]_2 \\ \boxed{[-\mathbf{d} + \Delta_0 \cdot \mathbf{f}_{i-1,x^*} + \mathbf{z}_{\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{x_i^*} + \Delta_1 \cdot \mathbf{f}_{i-1,x^*} + \mathbf{w}_{x_i^*,\tau}\mathbf{R}]_2}, [\mathbf{R}]_2 \\ \{[\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\}_{\sigma \neq x_i^*} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{\sigma} + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma \in \Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} \text{ where } (\Delta_0, \Delta_1) \in \{\boxed{(s_{i-1}^{-1}\Delta, 0)}, \colorbox{lightgray}{$(0, s_i^{-1}\Delta)$}\}.$$

Observe that

- when $(\Delta_0, \Delta_1) = \boxed{(s_{i-1}^{-1}\Delta, 0)}$, the distribution is identical to $\boxed{\mathsf{sk}_{\Gamma}^{i-1,i}[2]}$;
- when $(\Delta_0, \Delta_1) = \colorbox{lightgray}{$(0, s_i^{-1}\Delta)$}$, the distribution is identical to $\colorbox{lightgray}{$\mathsf{sk}_{\Gamma}^{i}[2]$}$ since $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{x_i^*} \bmod p$ (see Lemma 5).

We sample $\mathbf{d} \leftarrow \mathbb{Z}_p^{1 \times Q}$ and $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{k \times Q}$ and implicitly set

$$\Delta = \bar{\Delta}, \quad (\Delta_0, \Delta_1) = (\bar{\Delta}_0, \bar{\Delta}_1) \quad \text{and} \quad \mathbf{R} = \mathbf{r}^{\top} \cdot \mathbf{f}_{i-1,x^*} + \mathbf{B} \cdot \widetilde{\mathbf{R}}.$$

We then generate the key for Γ as follows:

- We simulate $[\mathbf{R}]_2$ from $[\mathbf{r}^\top]_2, [\mathbf{B}]_2$ and $\mathbf{f}_{i-1,x^*}, \widetilde{\mathbf{R}}$.
- We rewrite the terms in the dashed box as follows:

$$[-\mathbf{d} + (\bar{\Delta}_0 + \mathbf{z}_\tau \mathbf{r}^\top) \cdot \mathbf{f}_{i-1,x^*} + \mathbf{z}_\tau \mathbf{B} \cdot \widetilde{\mathbf{R}}]_2,\ [\mathbf{d}\mathbf{M}_{x_i^*} + (\bar{\Delta}_1 + \mathbf{w}_{x_i^*,\tau}\mathbf{r}^\top) \cdot \mathbf{f}_{i-1,x^*} + \mathbf{w}_{x_i^*,\tau}\mathbf{B} \cdot \widetilde{\mathbf{R}}]_2$$

  and simulate them using $[\bar{\Delta}_0 + \mathbf{z}_\tau \mathbf{r}^\top]_2, [\bar{\Delta}_1 + \mathbf{w}_{x_i^*,\tau}\mathbf{r}^\top]_2, [\mathbf{z}_\tau \mathbf{B}]_2, [\mathbf{w}_{x_i^*,\tau}\mathbf{B}]_2$ and $\mathbf{d}, \mathbf{f}_{i-1,x^*}, \widetilde{\mathbf{R}}$.
- We simulate all remaining terms using $[\mathbf{R}]_2$ and α, $\mathbf{d}$, $\mathbf{w}_{\text{start}}$, $\mathbf{z}_{1-\tau}$, $\{\mathbf{w}_{\sigma,\tau}\}_{\sigma \neq x_i^*}$, $\{\mathbf{w}_{\sigma,1-\tau}\}_{\sigma\in\Sigma}$, $\mathbf{w}_{\text{end}}$.

Observe that, when $(\bar{\Delta}_0, \bar{\Delta}_1) = \boxed{(s_{i-1}^{-1}\bar{\Delta}, 0)}$, we have $(\Delta_0, \Delta_1) = \boxed{(s_{i-1}^{-1}\Delta, 0)}$, then the secret key is $\boxed{\mathsf{sk}_\Gamma^{i-1,i}[2]}$ and the simulation is identical to $\mathsf{G}_{2.i.2}$; when $(\bar{\Delta}_0, \bar{\Delta}_1) = (0, s_i^{-1}\bar{\Delta})$, we have $(\Delta_0, \Delta_1) = (0, s_i^{-1}\Delta)$, then the secret key is $\mathsf{sk}_\Gamma^{i}[2]$ and the simulation is identical to $\mathsf{G}_{2.i.3}$. This completes the proof. □

4.8 Finalize

We finally prove that the adversary wins G_3 with probability $1/2$.

Lemma 18. $\Pr[\langle \mathcal{A}, \mathsf{G}_3 \rangle = 1] \approx 1/2$.

Proof. First, we argue that the secret key $\mathsf{sk}_\Gamma^{\ell,*}$ in this game perfectly hides the $\mathbf{a}_2$-component of $\mathbf{k}^\top$, i.e., $\alpha = \mathbf{a}_2\mathbf{k}^\top$. Recall the $\mathbf{a}_2$-components of the secret key:

$$\mathsf{sk}_\Gamma^{\ell,*}[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [\alpha\mathbf{f} - \mathbf{d} + \boxed{s_\ell^{-1}\Delta \cdot \mathbf{f}_{\ell,x^*}} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}.$$

By the property $\mathbf{f}_{\ell,x^*} = \mathbf{f}$ (see Lemma 5), we can see that $\mathsf{sk}_\Gamma^{\ell,*}[2]$ can be simulated using $\alpha + s_\ell^{-1}\Delta$, which means the secret key perfectly hides $\alpha = \mathbf{a}_2\mathbf{k}^\top$. Therefore, the unique term involving $\mathbf{k}$ in $\mathsf{ct}_{x^*}^{\ell}$, i.e., $[\mathbf{s}_\ell\mathbf{A}_1\mathbf{k}^\top + s_\ell\mathbf{a}_2\mathbf{k}^\top]_T$, is independently and uniformly distributed and thus statistically hides message m_β. □

5 Adaptively Secure ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ and DFA

In this section, we present our adaptively secure ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$. By our transformation from DFA to $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ (cf. Lemma 1), this readily gives us an adaptively secure ABE for DFA. We defer the concrete construction to Appendix F.

Overview. Our starting point is the selectively secure ABE scheme in Section 4. To achieve adaptive security, we handle key queries one by one following standard dual system method [20]; for each key, we carry out the one-key selective proof in Section 4 with piecewise guessing framework [15].[10] However this does not work immediately, we will make some changes to the scheme and proof in Section 4.

Recall that, in the one-key setting, the (selective) proof in Section 4 roughly tells us

$$(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_{x^*}) \approx_c (\mathsf{mpk}, \boxed{\mathsf{sk}_\Gamma^{\ell,*}}, \boxed{\mathsf{ct}_{x^*}^{\ell}}). \tag{25}$$

The two-key setting, for example, is expected to be handled by hybrid arguments:

$$(\mathsf{mpk}, \mathsf{sk}_{\Gamma_1}, \mathsf{sk}_{\Gamma_2}, \mathsf{ct}_{x^*}) \approx_c (\mathsf{mpk}, \boxed{\mathsf{sk}_{\Gamma_1}^{\ell,*}}, \mathsf{sk}_{\Gamma_2}, \boxed{\mathsf{ct}_{x^*}^{\ell}}) \approx_c (\mathsf{mpk}, \mathsf{sk}_{\Gamma_1}^{\ell,*}, \boxed{\mathsf{sk}_{\Gamma_2}^{\ell,*}}, \mathsf{ct}_{x^*}^{\ell})$$

[10] Handling all key queries simultaneously as in the selective model will cause a security loss exponential in the number of queries.

The first step seems to be feasible with some natural extension but the second one is problematic. Since we can not switch the challenge ciphertext back to ct_{x^*} due to the presence of $\mathsf{sk}_{\Gamma_1}^{\ell,*}$, the argument (25) can not be applied to the second key sk_{Γ_2} literally. In more detail, recall that

$$\mathsf{ct}_{x^*}^{\ell}[2] = \big([s_\ell \mathbf{w}_{x^*_\ell,\bar{\ell}}]_1, [s_\ell]_1, [s_\ell \mathbf{w}_{\mathrm{end}}]_1 \big) \tag{26}$$

leaks information of $\mathbf{w}_{x^*_\ell,\bar{\ell}}$ and $\mathbf{w}_{\mathrm{end}}$ while we need them to be hidden in some steps of the one-key proof; for example, Lemma 4.7 for $\mathsf{G}_{2.i.2} \approx_c \mathsf{G}_{2.i.3}$. We quickly argue that the natural solution of adding an extra subspace for fresh copies of $\mathbf{w}_{x^*_\ell,\bar{\ell}}$ and $\mathbf{w}_{\mathrm{end}}$ blows up the ciphertext and key sizes (see Section 1.1 for discussion).

Our approach reuses the existing $\mathbf{a}_2$-components as in [8]. Recall that, our one-key proof (25) uses a series of hybrids with random coins $s_0, s_1, \ldots$ and finally stops at a hybrid with s_ℓ (cf. (25) and (26)). Roughly, we change the scheme by adding an extra random coin s into the ciphertext and move one more step in the proof so that we finally stop at a new hybrid with the new s only. This allows us to release s_ℓ and reuse $\mathbf{w}_{x^*_\ell,\bar{\ell}}, \mathbf{w}_{\mathrm{end}}$ for the next key. More concretely, starting with the scheme in Section 4.2, we introduce a new component $[\mathbf{W}]_1 \in G_1^{(2k+1)\times k}$ into mpk:

- during encryption, we pick one more random coin $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ and replace the last three components in ct_x with

  $$[\mathbf{s}\mathbf{A}_1]_1, [\mathbf{s}_\ell \mathbf{A}_1 \mathbf{W}_{\mathrm{end}} + \mathbf{s}\mathbf{A}_1\mathbf{W}]_1, [\mathbf{s}\mathbf{A}_1\mathbf{k}^\top]_T \cdot m;$$

  this connects the last random coin $\mathbf{s}_\ell$ with the newly introduced $\mathbf{s}$; and $\mathbf{s}$ corresponds to s in the proof;
- during key generation, we replace the last two components in sk_Γ with

  $$[-\mathbf{D} + \mathbf{W}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{k}^\top \mathbf{f} + \mathbf{W}\mathbf{R}]_2, [\mathbf{R}]_2;$$

  the decryption will recover $[\mathbf{s}\mathbf{A}_1\mathbf{k}^\top\mathbf{f} - \mathbf{s}_\ell\mathbf{A}_1\mathbf{D}]_T$ instead of $[\mathbf{s}_\ell\mathbf{A}_1\mathbf{k}^\top\mathbf{f} - \mathbf{s}_\ell\mathbf{A}_1\mathbf{D}]_T$;
- during the proof, we extend the proof in Section 4.3 by one more step (see the dashed box):

  $$(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_{x^*}) \overset{\S 4.3}{\approx_c} (\mathsf{mpk}, \boxed{\mathsf{sk}_\Gamma^{\ell,*}}, \boxed{\mathsf{ct}_{x^*}^{\ell}}) \boxed{\approx_c (\mathsf{mpk}, \boxed{\mathsf{sk}_\Gamma^{*}}, \boxed{\mathsf{ct}_{x^*}^{*}})}$$

  so that $\mathsf{ct}_{x^*}^*[2]$ is in the following form:

  $$\mathsf{ct}_{x^*}^*[2] = \big([s\mathbf{w}]_1, [s]_1, [s\alpha]_1 \cdot m_\beta \big)$$

  which leaks $\mathbf{w} = \mathbf{a}_2\mathbf{W}$ instead of $\mathbf{w}_{x^*_\ell,\bar{\ell}}, \mathbf{w}_{\mathrm{end}}$; by this, we can carry out the one-key proof (25) for the next key (with some natural extensions).

Conceptually, we can interpret this as letting the NFA move to a specific dummy state whenever it accepts the input. Such a modification has been mentioned in [4] for simplifying the description rather than improving security and efficiency. In our formal description below, we will rename $\mathbf{W}_{\mathrm{end}}, \mathbf{W}, \mathbf{s}, s$ as $\mathbf{Z}_{\mathrm{end}}, \mathbf{W}_{\mathrm{end}}, \mathbf{s}_{\mathrm{end}}, s_{\mathrm{end}}$, respectively.

5.1 Scheme

Our adaptively secure ABE for $\mathcal{E}_Q$-restricted $\mathrm{NFA}^{\oplus p}$ in prime-order groups use the same basis as described in Section 4.1 and is described as follows:

- $\mathsf{Setup}(1^\lambda, \Sigma)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

  $$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(2k+1)} \quad \text{and} \quad \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{Z}_{\mathrm{end}}, \mathbf{W}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}, \ \forall \sigma \in \Sigma.$$

  Output

  $$\begin{aligned} \mathsf{mpk} &= \big([\mathbf{A}_1, \mathbf{A}_1\mathbf{W}_{\mathrm{start}}, \mathbf{A}_1\mathbf{Z}_0, \mathbf{A}_1\mathbf{Z}_1, \{\mathbf{A}_1\mathbf{W}_{\sigma,0}, \mathbf{A}_1\mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma}, \mathbf{A}_1\mathbf{Z}_{\mathrm{end}}, \mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1, [\mathbf{A}_1\mathbf{k}^\top]_T \big) \\ \mathsf{msk} &= \big(\mathbf{k}, \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \{\mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma}, \mathbf{Z}_{\mathrm{end}}, \mathbf{W}_{\mathrm{end}} \big). \end{aligned}$$

- $\mathsf{Enc}(\mathsf{mpk}, x, m)$: Let $x = (x_1, \dots, x_\ell) \in \Sigma^\ell$ and $m \in G_T$. Pick $\mathbf{s}_0, \mathbf{s}_1, \dots, \mathbf{s}_\ell, \mathbf{s}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1\times k}$ and output

$$\mathsf{ct}_x = \begin{pmatrix} [\mathbf{s}_0\mathbf{A}_1]_1,\ [\mathbf{s}_0\mathbf{A}_1\mathbf{W}_{\mathrm{start}}]_1 \\ \big\{[\mathbf{s}_j\mathbf{A}_1]_1, [\mathbf{s}_{j-1}\mathbf{A}_1\mathbf{Z}_{j \bmod 2} + \mathbf{s}_j\mathbf{A}_1\mathbf{W}_{x_j, j \bmod 2}]_1\big\}_{j\in[\ell]} \\ [\mathbf{s}_{\mathrm{end}}\mathbf{A}_1]_1, [\mathbf{s}_\ell\mathbf{A}_1\mathbf{Z}_{\mathrm{end}} + \mathbf{s}_{\mathrm{end}}\mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1,\ [\mathbf{s}_{\mathrm{end}}\mathbf{A}_1\mathbf{k}^\top]_T \cdot m \end{pmatrix}.$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$: Let $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$. Pick $\mathbf{D} \leftarrow \mathbb{Z}_p^{(2k+1)\times Q}$, $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times Q}$ and output

$$\mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \big\{[-\mathbf{D} + \mathbf{Z}_b\mathbf{R}]_2, [\mathbf{D}\mathbf{M}_\sigma + \mathbf{W}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{D} + \mathbf{Z}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{k}^\top\mathbf{f} + \mathbf{W}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}.$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_x)$: Parse ciphertext for $x = (x_1, \dots, x_\ell)$ and key for $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ as

$$\mathsf{ct}_x = \begin{pmatrix} [\mathbf{c}_{0,1}]_1, [\mathbf{c}_{0,2}]_1 \\ \big\{[\mathbf{c}_{j,1}]_1, [\mathbf{c}_{j,2}]_1\big\}_j \\ [\mathbf{c}_{\mathrm{end},1}]_1, [\mathbf{c}_{\mathrm{end},2}]_1, C \end{pmatrix} \quad \text{and} \quad \mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{k}_0^\top]_2, [\mathbf{r}_0^\top]_2 \\ \big\{[\mathbf{K}_b]_2, [\mathbf{K}_{\sigma,b}]_2, [\mathbf{R}]_2\big\}_{\sigma,b} \\ [\mathbf{K}_{\mathrm{end},1}]_2, [\mathbf{K}_{\mathrm{end},2}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

  We define $\mathbf{u}_{j,x}^\top$ for all $j \in [0,\ell]$ as (11) in Section 4.2 and proceed as follows:

  1. Compute
  $$B_0 = e([\mathbf{c}_{0,1}]_1, [\mathbf{k}_0^\top]_2) \cdot e([\mathbf{c}_{0,2}]_1, [\mathbf{r}_0^\top]_2)^{-1};$$
  2. For all $j \in [\ell]$, compute
  $$[\mathbf{b}_j]_T = e([\mathbf{c}_{j-1,1}]_1, [\mathbf{K}_{j \bmod 2}]_2) \cdot e([\mathbf{c}_{j,1}]_1, [\mathbf{K}_{x_j, j \bmod 2}]_2) \cdot e([-\mathbf{c}_{j,2}]_1, [\mathbf{R}]_2) \quad \text{and} \quad B_j = [\mathbf{b}_j\mathbf{u}_{j-1,x}^\top]_T;$$
  3. Compute
  $$[\mathbf{b}_{\mathrm{end}}]_T = e([\mathbf{c}_{\ell,1}]_1, [\mathbf{K}_{\mathrm{end},1}]_2) \cdot e([\mathbf{c}_{\mathrm{end},1}]_1, [\mathbf{K}_{\mathrm{end},2}]_2) \cdot e([-\mathbf{c}_{\mathrm{end},2}]_1, [\mathbf{R}]_2) \quad \text{and} \quad B_{\mathrm{end}} = [\mathbf{b}_{\mathrm{end}}\mathbf{u}_{\ell,x}^\top]_T;$$
  4. Compute
  $$B_{\mathrm{all}} = B_0 \cdot \textstyle\prod_{j=1}^{\ell} B_j \cdot B_{\mathrm{end}} \quad \text{and} \quad B = B_{\mathrm{all}}^{(\mathbf{f}\mathbf{u}_{\ell,x}^\top)^{-1}}$$
  and output the message $m' \leftarrow C \cdot B^{-1}$.

It is direct to verify the correctness as in Section 4.2. See Appendix E.1 for more details.

Security. We prove the following theorem stating the adaptive security of the above ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$. This readily implies our adaptively secure ABE for DFA thanks to Lemma 1.

Theorem 2 (Adaptively seucre ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$). *The ABE scheme for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in prime-order bilinear groups described above is adaptively secure (cf. Section 2.1) under the k-Lin assumption with security loss $O(q \cdot \ell \cdot |\Sigma|^3 \cdot Q^2)$. Here ℓ is the length of the challenge input x^* and q is the number of key queries.*

5.2 Proof of Main Theorem

From a high level, we employ the standard dual system proof switching the challenge ciphertext and keys into semi-functional forms in a one-by-one manner. To switch a secret key, we employ the proof technique for one-key selective setting in Section 4 in the piecewise guessing framework [15,14]. We will capture this by a core lemma. Let $x^* \in \Sigma^\ell$ denote the adaptive challenge. We begin with auxiliary distributions and use the notation for $\mathbf{a}_2$-components in Section 4.3.

Auxiliary distributions. We sample $s_{\mathrm{end}} \leftarrow \mathbb{Z}_p$, $\Delta \leftarrow \mathbb{Z}_p$ and define semi-functional ciphertext and key:

- $\mathsf{ct}^*_{x^*}$ is the same as ct_{x^*} except we replace $\mathbf{s}_{\mathrm{end}}\mathbf{A}_1$ with $\mathbf{s}_{\mathrm{end}}\mathbf{A}_1 + s_{\mathrm{end}}\mathbf{a}_2$;
- sk^*_Γ is the same as sk_Γ except we replace $\mathbf{k}^\top$ with $\mathbf{k}^\top + \mathbf{a}_2^\parallel \cdot s_{\mathrm{end}}^{-1}\Delta$ in the term $[\mathbf{k}^\top\mathbf{f} + \mathbf{W}_{\mathrm{end}}\mathbf{R}]_2$.

That is, we have:

$$\begin{aligned}
\mathsf{ct}^*_{x^*}[2] &= \big([s_{\mathrm{end}}\mathbf{w}_{\mathrm{end}}]_1, [s_{\mathrm{end}}]_1, [s_{\mathrm{end}}\alpha]_T \cdot m_\beta\big)\\
\mathsf{sk}^*_\Gamma[2] &= \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{d} + \mathbf{z}_{\mathrm{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \boxed{s_{\mathrm{end}}^{-1}\Delta\cdot\mathbf{f}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}
\end{aligned}$$

Game sequence and core lemma. We prove Theorem 2 via a series of games following standard dual system method [20]:

- G_0: Identical to the real game.
- G_1: Identical to G_0 except that the challenge ciphertext is semi-functional, i.e., $\mathsf{ct}^*_{x^*}$.
- $\mathsf{G}_{2.\kappa}$ for $\kappa \in [0, q]$: Identical to G_1 except that the first κ secret keys are semi-functional, i.e., sk^*_Γ.
- G_3: Identical to $\mathsf{G}_{2.q}$ except that the challenge ciphertext is an encryption of a random message.

Here we have $\mathsf{G}_{2.0} = \mathsf{G}_1$. It is standard to prove $\mathsf{G}_0 \approx_c \mathsf{G}_1$, $\mathsf{G}_{2.q} \approx_s \mathsf{G}_3$ and show that adversary in G_3 has no advantage. We sketch the proofs in Appendix E.2. To prove $\mathsf{G}_{2.\kappa-1} \approx_c \mathsf{G}_{2.\kappa}$ for all $\kappa \in [q]$, we use core lemma:

Lemma 19 (Core lemma). *For all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ and*

$$\mathsf{Adv}^{\mathrm{CORE}}_{\mathcal{A}}(\lambda) = \Pr[\langle\mathcal{A}, \mathsf{H}_0\rangle = 1] - \Pr[\langle\mathcal{A}, \mathsf{H}_1\rangle = 1] \le O(\ell\cdot|\Sigma|^3\cdot Q^2)\cdot\mathsf{Adv}^{k\text{-}\mathrm{LIN}}_{\mathcal{B}}(\lambda)$$

where, for all $b \in \{0,1\}$, we define:

$$\langle\mathcal{A}, \mathsf{H}_b\rangle := \big\{b' \leftarrow \mathcal{A}^{\mathsf{OEnc}(\cdot),\mathsf{OKey}(\cdot)}(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2)\big\}$$

where

$$\begin{aligned}
\mathsf{mpk} &= \big([\mathbf{A}_1, \mathbf{A}_1\mathbf{W}_{start}, \mathbf{A}_1\mathbf{Z}_0, \mathbf{A}_1\mathbf{Z}_1, \{\mathbf{A}_1\mathbf{W}_{\sigma,0}, \mathbf{A}_1\mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma}, \mathbf{A}_1\mathbf{Z}_{end}, \mathbf{A}_1\mathbf{W}_{end}]_1, [\mathbf{A}_1\mathbf{k}^\top]_T\big)\\
\mathsf{aux}_1 &= \big([\mathbf{k}, \mathbf{B}, \mathbf{W}_{start}\mathbf{B}, \mathbf{Z}_0\mathbf{B}, \mathbf{Z}_1\mathbf{B}, \{\mathbf{W}_{\sigma,0}\mathbf{B}, \mathbf{W}_{\sigma,1}\mathbf{B}\}_{\sigma\in\Sigma}, \mathbf{Z}_{end}\mathbf{B}, \mathbf{W}_{end}\mathbf{B}]_2\big)\\
\mathsf{aux}_2 &= \big([\mathbf{r}^\top, \mathbf{W}_{start}\mathbf{r}^\top, \mathbf{Z}_0\mathbf{r}^\top, \mathbf{Z}_1\mathbf{r}^\top, \{\mathbf{W}_{\sigma,0}\mathbf{r}^\top, \mathbf{W}_{\sigma,1}\mathbf{r}^\top\}_{\sigma\in\Sigma}, \mathbf{Z}_{end}\mathbf{r}^\top, \mathbf{a}_2^\parallel\cdot s_{end}^{-1}\Delta + \mathbf{W}_{end}\mathbf{r}^\top]_2\big)
\end{aligned}$$

with $\mathbf{W}_{start}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{Z}_{end}, \mathbf{W}_{end} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{r} \leftarrow \mathbb{Z}_p^{1\times k}$, $s_{end}, \Delta \leftarrow \mathbb{Z}_p$ and the two oracles work as follows:

- $\mathsf{OEnc}(x^*, m)$*: output* $\mathsf{ct}^*_{x^*}$ *using* s_{end} *in* aux_2*;*
- $\mathsf{OKey}(\Gamma)$*: output* $\boxed{\mathsf{sk}_\Gamma}$ *if $b = 0$; output* $\colorbox{lightgray}{$\mathsf{sk}^*_\Gamma$}$ *using Δ and s_{end} in* aux_2 *if $b = 1$;*

with the restrictions that (1) $\mathcal{A}$ makes only one query to each oracle; (2) queries Γ and x^* satisfy $\Gamma(x^*) = 0$.

It is direct to see that the core lemma implies $\mathsf{G}_{2.\kappa-1} \approx_c \mathsf{G}_{2.\kappa}$; here aux_1 and aux_2 are sufficient to simulate other $q-1$ keys which are either sk_Γ or sk^*_Γ, see Appendix E.2 for more details. The remaining of this section will be devoted to the proof of the core lemma, which completes the proof of Theorem 2.

5.3 Piecewise guessing framework

We briefly review the piecewise guessing framework [15] we will use in the proof of core lemma. Suppose we have two adaptive games H_0 and H_1 which we would like to show to be indistinguishable. In both games, an adversary $\mathcal{A}$ makes some adaptive choice $z^* \in \{0,1\}^R$. Informally, the piecewise guessing framework tells us that if we can show that $\mathsf{H}_0, \mathsf{H}_1$ are ϵ-indistinguishable in the selective setting where (1) all choices z^* are committed to in advance via a series of $L+1$ hybrids and (2) each hybrid depends only on at most $R' \ll R$ bits of information about z^*, then $\mathsf{H}_0, \mathsf{H}_1$ are $2^{2R'} \cdot L \cdot \epsilon$-indistinguishable in the adaptive setting. More formally, we define

- a family of games $\{\mathsf{H}^u\}_{u\in\{0,1\}^{R'}}$ where the messages sent to the adversary depend on u;
- a family of h-functions $h_0, \ldots, h_L : \{0,1\}^R \mapsto \{0,1\}^{R'}$ which describes the hybrids;

the piecewise guessing framework ensures that $\mathsf{H}_0 \approx_c \mathsf{H}_1$ if $\{\mathsf{H}^u\}_{u\in\{0,1\}^{R'}}$ and $h_0, \ldots, h_L$ satisfy

- end-point equivalence, which means:

$$\mathsf{H}_0 = \mathsf{H}^{h_0(z^*)},\ \mathsf{H}_1 = \mathsf{H}^{h_L(z^*)} \quad \forall z^* \in \{0,1\}^R;$$

- neighbor indistinguishability, which means:

$$\widehat{\mathsf{H}}_{i,0}(u_0, u_1) \approx_c \widehat{\mathsf{H}}_{i,1}(u_0, u_1) \quad \forall i \in [L], u_0, u_1 \in \{0,1\}^{R'}$$

  where $\widehat{\mathsf{H}}_{i,b}(u_0, u_1)$ is the same as H^{u_b} except we output 0 whenever $(h_{i-1}(z^*), h_i(z^*)) \neq (u_0, u_1)$.

This is captured by the *adaptive security lemma* in [15]:

Lemma 20 (adaptive security lemma [15]). *Fix* $\mathsf{H}_0, \mathsf{H}_1$ *along with* $h_0, h_1, \ldots, h_L : \{0,1\}^R \to \{0,1\}^{R'}$ *and* $\{\mathsf{H}^u\}_{u\in\{0,1\}^{R'}}$ *such that*

$$\forall\ z^* \in \{0,1\}^R : \mathsf{H}^{h_0(z^*)} = \mathsf{H}_0,\ \mathsf{H}^{h_L(z^*)} = \mathsf{H}_1$$

Suppose there exists an adversary $\mathcal{A}$ *such that*

$$\Pr[\langle \mathcal{A}, \mathsf{H}_0 \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{H}_1 \rangle = 1] \geq \epsilon$$

then there exists $i \in [L]$ *and* $u_0, u_1 \in \{0,1\}^{R'}$ *such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{i,0}(u_0, u_1) \rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{i,1}(u_0, u_1) \rangle = 1] \geq \frac{\epsilon}{2^{2R'} L}.$$

5.4 Proof of Core Lemma

Observe that the core lemma roughly captures the one-key adaptive setting with mpk, key and ciphertext similar to our selectively secure ABE in 4.2. We prove the core lemma, Lemma 19, by combining the proof for one-key selective security in Section 4.3 with the piecewise guessing framework reviewed above. In particular, we will use a family of hybrids, defined by H^u and h-functions, analogous to those in Section 4.3. Let $\bar{\ell} = \ell \bmod 2$ and assume $\ell > 1$, we begin with more auxiliary distributions.

More auxiliary distributions. The auxiliary distributions we use here are motivated by those in Section 4.3.

Ciphertext distributions. We sample $s_0, s_1, \dots, s_\ell \leftarrow \mathbb{Z}_p$ and define:

- for $i \in [0,\ell]$: $\mathsf{ct}^i_{x^*}$ is the same as $\boxed{\mathsf{ct}^*_{x^*}}$ except we replace $\mathbf{s}_i\mathbf{A}_1$ with $\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$;
- for $i \in [\ell]$: $\mathsf{ct}^{i-1,i}_{x^*}$ is the same as $\boxed{\mathsf{ct}^*_{x^*}}$ except we replace $\mathbf{s}_{i-1}\mathbf{A}_1, \mathbf{s}_i\mathbf{A}_1$ with $\mathbf{s}_{i-1}\mathbf{A}_1 + s_{i-1}\mathbf{a}_2, \mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$.

That is, we have: writing $\tau = i \bmod 2$,

$$\mathsf{ct}^i_{x^*}[2] = \begin{cases} [s_0\mathbf{w}_{\mathsf{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1]_1, \boxed{[s_{\mathsf{end}}\mathbf{w}_{\mathsf{end}}]_1, [s_{\mathsf{end}}]_1, [s_{\mathsf{end}}\alpha]_T \cdot m} & \text{if } i = 0 \\ [s_i\mathbf{w}_{x_i^*,\tau}]_1, [s_i]_1, [s_i\mathbf{z}_{1-\tau}]_1, \boxed{[s_{\mathsf{end}}\mathbf{w}_{\mathsf{end}}]_1, [s_{\mathsf{end}}]_1, [s_{\mathsf{end}}\alpha]_T \cdot m} & \text{if } i \in [\ell-1] \\ [s_\ell\mathbf{w}_{x_\ell^*,\bar{\ell}}]_1, [s_\ell]_1, [s_\ell\mathbf{z}_{\mathsf{end}} + \boxed{s_{\mathsf{end}}\mathbf{w}_{\mathsf{end}}}]_1, \boxed{[s_{\mathsf{end}}]_1, [s_{\mathsf{end}}\alpha]_T \cdot m} & \text{if } i = \ell \end{cases}$$

$$\mathsf{ct}^{i-1,i}_{x^*}[2] = \begin{cases} [s_0\mathbf{w}_{\mathsf{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1 + s_1\mathbf{w}_{x_1^*,1}]_1, [s_1]_1, [s_1\mathbf{z}_0]_1, \boxed{[s_{\mathsf{end}}\mathbf{w}_{\mathsf{end}}]_1, [s_{\mathsf{end}}]_1, [s_{\mathsf{end}}\alpha]_T \cdot m} & \text{if } i = 1 \\ [s_{i-1}\mathbf{w}_{x_{i-1}^*,1-\tau}]_1, [s_{i-1}]_1, [s_{i-1}\mathbf{z}_\tau + s_i\mathbf{w}_{x_i^*,\tau}]_1, [s_i]_1, [s_i\mathbf{z}_{1-\tau}]_1, \boxed{[s_{\mathsf{end}}\mathbf{w}_{\mathsf{end}}]_1, [s_{\mathsf{end}}]_1, [s_{\mathsf{end}}\alpha]_T \cdot m} & \text{if } i \in [2,\ell-1] \\ [s_{\ell-1}\mathbf{w}_{x_{\ell-1}^*,1-\bar{\ell}}]_1, [s_{\ell-1}]_1, [s_{\ell-1}\mathbf{z}_{\bar{\ell}} + s_\ell\mathbf{w}_{x_\ell^*,\bar{\ell}}]_1, [s_\ell]_1, [s_\ell\mathbf{z}_{\mathsf{end}} + \boxed{s_{\mathsf{end}}\mathbf{w}_{\mathsf{end}}}]_1, \boxed{[s_{\mathsf{end}}]_1, [s_{\mathsf{end}}\alpha]_T \cdot m} & \text{if } i = \ell \end{cases}$$

The auxiliary ciphertext distributions here are analogous to those in Section 4.3 except that they have extra terms $[s_{\mathsf{end}}\mathbf{w}_{\mathsf{end}}]_1, [s_{\mathsf{end}}]_1, [s_{\mathsf{end}}\alpha]_T \cdot m$ inherited from $\mathsf{ct}^*_{x^*}$. We highlighted the differences by dashed boxes.

Secret key distributions. Recall that a query to OKey is $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$. For all $i \in [\ell]$, $\chi \in \Sigma$ and $\mathbf{p} \in \mathcal{E}_Q$, we define:

- $\mathsf{sk}^0_{\Gamma,\mathbf{p}}$ is the same as sk_Γ except we replace $\mathbf{D}$ with $\mathbf{D} + \mathbf{a}_2^{\parallel} \cdot s_0^{-1}\Delta \cdot \mathbf{p}$ in the term $[\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\mathsf{start}}\mathbf{R}\mathbf{u}^\top]_2$;
- $\mathsf{sk}^i_{\Gamma,\chi,\mathbf{p}}$ is the same as sk_Γ except we replace $\mathbf{D}$ with $\mathbf{D} + \mathbf{a}_2^{\parallel} \cdot s_i^{-1}\Delta \cdot \mathbf{p}$ in the term $[\mathbf{D}\mathbf{M}_\chi + \mathbf{W}_{\chi,i \bmod 2}\mathbf{R}]_2$;
- $\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{p}}$ is the same as sk_Γ except we replace $-\mathbf{D}$ with $-\mathbf{D} + \mathbf{a}_2^{\parallel} \cdot s_{i-1}^{-1}\Delta \cdot \mathbf{p}$ in the term $[-\mathbf{D} + \mathbf{Z}_{i \bmod 2}\mathbf{R}]_2$;
- $\mathsf{sk}^{\ell,*}_\Gamma$ is the same as sk_Γ except we replace $-\mathbf{D}$ with $-\mathbf{D} + \mathbf{a}_2^{\parallel} \cdot s_\ell^{-1}\Delta \cdot \mathbf{f}$ in the term $[-\mathbf{D} + \mathbf{Z}_{\mathsf{end}}\mathbf{R}]_2$.

That is, we have: writing $\tau = i \bmod 2$,

$$\mathsf{sk}^0_{\Gamma,\mathbf{p}}[2] = \begin{pmatrix} [(\mathbf{d} + \boxed{s_0^{-1}\Delta \cdot \mathbf{p}})\mathbf{u}^\top + \mathbf{w}_{\mathsf{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{d} + \mathbf{z}_{\mathsf{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\mathsf{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\mathsf{sk}^i_{\Gamma,\chi,\mathbf{p}}[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\mathsf{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_\tau\mathbf{R}]_2, [(\mathbf{d} + \boxed{s_i^{-1}\Delta \cdot \mathbf{p}})\mathbf{M}_\chi + \mathbf{w}_{\chi,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\} \\ \{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\}_{\sigma\neq\chi} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [-\mathbf{d} + \mathbf{z}_{\mathsf{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\mathsf{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{p}}[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\mathsf{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \boxed{s_{i-1}^{-1}\Delta \cdot \mathbf{p}} + \mathbf{z}_\tau\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [-\mathbf{d} + \mathbf{z}_{\mathsf{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\mathsf{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\mathsf{sk}^{\ell,*}_\Gamma[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\mathsf{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{d} + \boxed{s_\ell^{-1}\Delta \cdot \mathbf{f}} + \mathbf{z}_{\mathsf{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\mathsf{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

The auxiliary secret key distributions here are analogous to those in Section 4.3 except that we use general χ and $\mathbf{p}$ in the place of x_i^* and $\mathbf{f}_{i,x^*}$. Note that these correspond to the piecewise information we need to guess in the proof.

Hybrids $\{\mathsf{H}^u\}_u$ and h-functions. We are ready to define $\{\mathsf{H}^u\}_u$ and h-functions in the adaptive security lemma (Lemma 20).

Defining u and H^u. For our setting, we require u to determine the forms of ciphertext (output by OEnc) and key (output by OKey) in a hybrid, this includes the superscripts of key and ciphertext and piecewise information χ and $\mathbf{p}$. For this purpose, we define

$$u \in I \times I \times \Sigma \times \mathcal{E}_Q$$

where

$$I = \{0, 1, \ldots, \ell, *\} \cup \{(0,1), (1,2) \ldots, (\ell-1, \ell), (\ell, *)\}$$

is the set of superscripts of auxiliary keys and ciphertexts, Σ and $\mathcal{E}_Q$ includes all possibilities of χ and $\mathbf{p}$, respectively. We allow a special symbol "$\perp$" at any positions indicating an empty output. Then, for all $u = (\mathrm{C}, \mathrm{S}, \chi, \mathbf{p}) \in I \times I \times \Sigma \times \mathcal{E}_Q$, we define hybrid $\mathsf{H}^{\mathrm{C},\mathrm{S},\chi,\mathbf{p}}$ to be identical to H_0 (or H_1) except that

- oracle $\mathsf{OEnc}(x^*, m)$ returns $\mathsf{ct}^{\mathrm{C}}_{x^*}$;
- oracle $\mathsf{OKey}(\Gamma)$ returns $\mathsf{sk}^{\mathrm{S}}_{\Gamma,\mathsf{yyy}}$ with yyy depending on S or sk_Γ when $\mathrm{S} = \perp$.

Here we always assume that C and S indicate well-defined auxiliary ciphertext and key distributions and yyy is always provided in u (i.e., not "$\perp$").

Defining h-functions. In both H_0 and H_1, the adversary $\mathcal{A}$ adaptively chooses Γ and x^*, therefore we employ a family of functions

$$h_{\mathsf{xxx}} : \mathrm{NFA}^{\oplus p} \times \Sigma^* \to I \times I \times \Sigma \times \mathcal{E}_Q$$

with the first input being $\mathcal{E}_Q$-restricted. Recall that, for an input x^* of length ℓ and a $\mathcal{E}_Q$-restricted $\mathrm{NFA}^{\oplus p}$ Γ, we can define $\mathbf{f}_{0,x^*}, \ldots, \mathbf{f}_{\ell,x^*} \in \mathcal{E}_Q$ as (22) in Section 4.3. We define h-functions as below which describes a series of hybrids analogous to those for selective security in Section 4.3. We show the corresponding selective game for each function as a remark.

$$\begin{array}{lllllll}
h_0 & : (\Gamma, x^*) \longmapsto (\{*\}, & \perp, & \perp, & \perp &); & /\!/\ \mathsf{G}_0 \\
h_1 & : (\Gamma, x^*) \longmapsto (\{0\}, & \perp, & \perp, & \perp &); & /\!/\ \mathsf{G}_1 \\
h_{2.1.0} & : (\Gamma, x^*) \longmapsto (\{0\}, & \{0\}, & \perp, & \mathbf{f}_{0,x^*} &); & /\!/\ \mathsf{G}_{2.1.0} \\
h_{2.i.0} & : (\Gamma, x^*) \longmapsto (\{i-1\}, & \{i-1\}, & x^*_{i-1}, & \mathbf{f}_{i-1,x^*} &); \forall\, i \in [2, \ell]; & /\!/\ \mathsf{G}_{2.i.0} \\
h_{2.i.1} & : (\Gamma, x^*) \longmapsto (\{i-1\}, & \{i-1, i\}, & \perp, & \mathbf{f}_{i-1,x^*} &); \forall\, i \in [\ell]; & /\!/\ \mathsf{G}_{2.i.1} \\
h_{2.i.2} & : (\Gamma, x^*) \longmapsto (\{i-1, i\}, & \{i-1, i\}, & \perp, & \mathbf{f}_{i-1,x^*} &); \forall\, i \in [\ell]; & /\!/\ \mathsf{G}_{2.i.2} \\
h_{2.i.3} & : (\Gamma, x^*) \longmapsto (\{i-1, i\}, & \{i\}, & x^*_i, & \mathbf{f}_{i,x^*} &); \forall\, i \in [\ell]; & /\!/\ \mathsf{G}_{2.i.3} \\
h_{2.i.4} & : (\Gamma, x^*) \longmapsto (\{i\}, & \{i\}, & x^*_i, & \mathbf{f}_{i,x^*} &); \forall\, i \in [\ell]; & /\!/\ \mathsf{G}_{2.i.4} \\
h_3 & : (\Gamma, x^*) \longmapsto (\{\ell\}, & \{\ell, *\}, & \perp, & \perp &); & /\!/\ \mathsf{G}_3 \\
h_4 & : (\Gamma, x^*) \longmapsto (\{\ell\}, & \{*\}, & \perp, & \perp &); & \\
h_5 & : (\Gamma, x^*) \longmapsto (\{*\}, & \{*\}, & \perp, & \perp &); &
\end{array}$$

Note that we have $h_{2.i.0} = h_{2.i-1.4}$ for all $i \in [2, \ell]$ and $\mathsf{ct}^*_{x^*}, \mathsf{sk}^*_\Gamma$ are shown in Section 5.2. Fix Γ and x^*, we summarize all h-functions by showing hybrids $\mathsf{H}^{h_{\mathsf{xxx}}(\Gamma,x^*)}$ in Fig 8 (which is analogous to Fig 6 in Section 4.3).

Outline of the proof. Roughly, the adaptive security lemma [15] (see Lemma 20) says that we only need to check (1) end-point equivalence and (2) neighbor indistinguishability.

End-point equivalence. It is clear that our hybrids $\{\mathsf{H}^u\}_u$ and h-functions satisfy the end-point equivalence. This follows from the fact that h_0 and h_5 are constant functions which indicate the same types of ciphertext and key as in H_0 and H_1, respectively. Formally, we give the following lemma.

Lemma 21 (End-point equivalence). *For all $(\Gamma, x^*) \in \{0,1\}^R$, we have*

$$\mathsf{H}^{h_0(\Gamma,x^*)} = \mathsf{H}_0 \quad \text{and} \quad \mathsf{H}^{h_5(\Gamma,x^*)} = \mathsf{H}_1.$$

h_{xxx}	$\mathsf{ct}^{\mathrm{C}}_{x^*}$	$\mathsf{sk}^{\mathrm{S}}_{\Gamma,\chi,\mathbf{p}}[2]$							Remark
			$? \cdot \mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top$	$? \cdot \mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}$	$? + \mathbf{z}_\tau \mathbf{R}$	$? \cdot \mathbf{M}_{x^*_i} + \mathbf{w}_{x^*_i,\tau}\mathbf{R}$	$? + \mathbf{z}_{\mathrm{end}}\mathbf{R}$	$? \cdot \mathbf{f} + \mathbf{w}_{\mathrm{end}}\mathbf{R}$	
0	$\mathsf{ct}^*_{x^*}$	sk_Γ	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	α	real game
1	$\boxed{\mathsf{ct}^0_{x^*}}$	sk_Γ	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	α	switching lemma
2.1.0	$\mathsf{ct}^0_{x^*}$	$\boxed{\mathsf{sk}^0_{\Gamma,\mathbf{f}_{0,x^*}}}$	$\mathbf{d} + \boxed{s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	α	$\mathbf{f}_{0,x^*}\mathbf{u}^\top = 0 \bmod p$ (Lemma 5)
2.i.0	$\mathsf{ct}^{i-1}_{x^*}$	$\mathsf{sk}^{i-1}_{\Gamma,x^*_{i-1},\mathbf{f}_{i-1,x^*}}$	$\mathbf{d}$	$\mathbf{d} + s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	α	$i \in [2,\ell]$
2.i.1	$\mathsf{ct}^{i-1}_{x^*}$	$\boxed{\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{f}_{i-1,x^*}}}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d} + \boxed{s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*}}$	$\mathbf{d}$	$-\mathbf{d}$	α	change of variables, DDH
2.i.2	$\boxed{\mathsf{ct}^{i-1,i}_{x^*}}$	$\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{f}_{i-1,x^*}}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d} + s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*}$	$\mathbf{d}$	$-\mathbf{d}$	α	switching lemma
2.i.3	$\mathsf{ct}^{i-1,i}_{x^*}$	$\boxed{\mathsf{sk}^{i}_{\Gamma,x^*_i,\mathbf{f}_{i,x^*}}}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d} + \boxed{s_i^{-1}\Delta \cdot \mathbf{f}_{i,x^*}}$	$-\mathbf{d}$	α	transition lemma, $\mathbf{f}_{i-1,x^*} = \mathbf{M}_{x^*_i}\mathbf{f}_{i,x^*} \bmod p$ (Lemma 5)
2.i.4	$\boxed{\mathsf{ct}^{i}_{x^*}}$	$\mathsf{sk}^{i}_{\Gamma,x^*_i,\mathbf{f}_{i,x^*}}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d} + s_i^{-1}\Delta \cdot \mathbf{f}_{i,x^*}$	$-\mathbf{d}$	α	switching lemma
3	$\mathsf{ct}^{\ell}_{x^*}$	$\boxed{\mathsf{sk}^{\ell,*}_{\Gamma}}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d} + \boxed{s_\ell^{-1}\Delta \cdot \mathbf{f}}$	α	change of variables, DDH, $\mathbf{f}_{\ell,x^*} = \mathbf{f}$ (Lemma 5)
4	$\mathsf{ct}^{\ell}_{x^*}$	$\boxed{\mathsf{sk}^{*}_{\Gamma}}$	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\alpha + \boxed{s_{\mathrm{end}}^{-1}\Delta}$	transition lemma
5	$\boxed{\mathsf{ct}^{*}_{x^*}}$	sk^{*}_{Γ}	$\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\alpha + s_{\mathrm{end}}^{-1}\Delta$	switching lemma

Fig. 8. Definition of h-functions with $i \in [\ell]$. In the table, we show both ciphertext and key in $\mathsf{H}^{h_{\mathsf{xxx}}(\Gamma,x^*)}$; as in Fig 6, we only describe the $\mathbf{a}_2$-components of the key. In the **Remark** column, "DDH" indicates $\mathrm{DDH}^{G_2}_{1,Q}$ assumption.

Neighbor indistinguishability. We first define several pairs of hybrids with $b \in \{0,1\}$:

- $\widehat{\mathsf{H}}_0^b(u_0,u_1)$ is the same as H^{u_b} except that we output 0 whenever
$$(h_0(\Gamma,x^*),h_1(\Gamma,x^*)) \neq (u_0,u_1).$$
- $\widehat{\mathsf{H}}_1^b(u_0,u_1)$ is the same as H^{u_b} except that we output 0 whenever
$$(h_1(\Gamma,x^*),h_{2.1.0}(\Gamma,x^*)) \neq (u_0,u_1).$$
- $\widehat{\mathsf{H}}_{2.i.i'}^b(u_0,u_1)$, for $i \in [\ell]$ and $i' \in [4]$, is the same as H^{u_b} except that we output 0 whenever
$$(h_{2.i.i'-1}(\Gamma,x^*),h_{2.i,i'}(\Gamma,x^*)) \neq (u_0,u_1).$$
- $\widehat{\mathsf{H}}_3^b(u_0,u_1)$ is the same as H^{u_b} except that we output 0 whenever
$$(h_{2.\ell.4}(\Gamma,x^*),h_3(\Gamma,x^*)) \neq (u_0,u_1).$$
- $\widehat{\mathsf{H}}_4^b(u_0,u_1)$ is the same as H^{u_b} except that we output 0 whenever
$$(h_3(\Gamma,x^*),h_4(\Gamma,x^*)) \neq (u_0,u_1).$$
- $\widehat{\mathsf{H}}_5^b(u_0,u_1)$ is the same as H^{u_b} except that we output 0 whenever
$$(h_4(\Gamma,x^*),h_5(\Gamma,x^*)) \neq (u_0,u_1).$$

We will prove that each pair of hybrids are indistinguishable for all $u_0,u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$. Straightforward extensions of the proofs in Section 4 are sufficient for the proof, we formally describe the lemma and defer all details to Appendix E.3.

Lemma 22 (Neighbor indistinguishability). *For all* $\mathsf{xxx} \in \{0,1,3,4,5\} \cup \{2.i.i' : i \in [\ell], i' \in [4]\}$, $u_0,u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ *and all* $\mathcal{A}$*, there exists* $\mathcal{B}$ *with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*
$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{\mathsf{xxx}}^0(u_0,u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{\mathsf{xxx}}^1(u_0,u_1)\rangle = 1] \leq O(|\Sigma|) \cdot \mathsf{Adv}_{\mathcal{B}}^{k\text{-LIN}}(\lambda).$$

Summary. By the adaptive security lemma (Lemma 20), Lemma 21 and Lemma 22 imply the core lemma, Lemma 19, with the following two facts:

- all our h-functions have range of size at most $O(|\Sigma|Q)$ since the first two outputs are constant and $|\mathcal{E}_Q| = Q$; that is, we have $R' = O(\log|\Sigma|) + O(\log Q)$;
- our proof employs $O(\ell)$ h-functions; that is we have $L = O(\ell)$.

6 Compact Adaptively Secure ABE for Branching Programs

In this section, we present our compact adaptively secure ABE for branching programs. We follow the same technical line as that for our adaptively secure ABE for DFA from Section 3 to Section 5. In particular, we construct a semi-adaptively secure ABE for $\mathrm{NBP}^{\oplus_p}$, which is an analogue of $\mathrm{NFA}^{\oplus_p}$; then prove that the same scheme is adaptively secure for a subclass of $\mathrm{NBP}^{\oplus_p}$ in the piecewise guessing framework. This is sufficient to derive our scheme for branching program. Before that, we begin with various notions of branching programs and their relationship.

6.1 (Layered) Branching Programs: Notions and Relationship

Recall that p is a global parameter and $\mathcal{E}_Q = \{\mathbf{e}_1,\ldots,\mathbf{e}_Q\}$ is the set of all elementary row vectors of dimension Q. In this section, we focus on *layered* branching programs.

Branching Programs. As in Section 3, we use vector-matrix notation $\Gamma = (Q, \ell_{\mathrm{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$ to describe branching program (BP for short), nondeterministic branching program (NBP for short), p-bounded NBP (NBP$^{<p}$ for short) and mod-p NBP (NBP$^{\oplus p}$ for short) where width $Q \in \mathbb{N}$ corresponds to the number states in NFA, $\ell_{\mathrm{BP}}, \ell \in \mathbb{N}$ describe program and input length, Σ is the alphabet, $\mathbf{u}, \mathbf{f} \in \{0,1\}^Q$ correspond to the start and accept states in NFA; $\mathbf{M}_{j,\sigma} \in \{0,1\}^{Q\times Q}$ and $\rho : [\ell_{\mathrm{BP}}] \to [\ell]$ describe the transition function and index-to-input map. Let $x = (x_1, \ldots, x_\ell)$ denote an input, then,

- for BP Γ, we have $\mathbf{u} \in \mathcal{E}_Q$, each column in every matrix $\mathbf{M}_{j,\sigma}$ is an elementary column vector (i.e., contains exactly one 1) and $\Gamma(x) = 1 \iff \mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top = 1$;
- for NBP Γ, we have $\Gamma(x) = 1 \iff \mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top \geq 1$;
- for NBP$^{<p}$ Γ, we have $\mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top < p$ and $\Gamma(x) = 1 \iff \mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top \geq 1$;
- for NBP$^{\oplus p}$ Γ, we have $\Gamma(x) = 1 \iff \mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top \neq 0 \bmod p$.

As various notions of DFA and NFA, we have: BP $\subset$ NBP$^{<p}$$\subset$ NBP $\cap$ NBP$^{\oplus p}$.

$\mathcal{E}_Q$-restricted NBP$^{\oplus p}$. We introduce the notion of $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$ which is analogous to that of $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in Section 3. An NBP$^{\oplus p}$ $\Gamma = (Q, \ell_{\mathrm{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$ is $\mathcal{E}_Q$-restricted if for all $x \in \Sigma^\ell$, it holds that

$$\mathbf{f}_{i,x} := \mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{i+1,x_{\rho(i+1)}} \in \mathcal{E}_Q, \ \forall i \in [0, \ell].$$

Here $\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{i+1,x_{\rho(i+1)}}$ for $i = \ell_{\mathrm{BP}}$ refers to $\mathbf{I}$ of size $Q \times Q$.

Transforming BP to $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$. In general, a BP is not necessarily a $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$. The next lemma says that we can nonetheless transform any BP into a $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$:

Lemma 23 (BP to $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$). *For each branching program $\Gamma = (Q, \ell_{BP}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{BP}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$, we have NBP$^{\oplus p}$ $\Gamma^\top = (Q, \ell_{BP}, \ell, \Sigma, \{\mathbf{M}^\top_{\tau(j),\sigma}\}_{j\in[\ell_{BP}],\sigma\in\Sigma}, \rho\circ\tau, \mathbf{f}, \mathbf{u})$ with $\tau(j) = \ell_{BP} + 1 - j$ for all $j \in [\ell_{BP}]$ such that*

1. *$\Gamma^\top$ is $\mathcal{E}_Q$-restricted;*
2. *for all $x \in \Sigma^\ell$, it holds that*
$$\Gamma(x) = \Gamma^\top(x). \tag{27}$$

Proof. Recall that the definition of BP implies two properties:

$$\mathbf{f} \in \{0,1\}^Q \tag{28}$$
$$\text{and} \quad (\mathbf{M}_{i,x_{\rho(i)}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top)^\top \in \mathcal{E}_Q, \quad \forall i \in [0, \ell_{\mathrm{BP}}]. \tag{29}$$

Property (29) comes from the facts that $\mathbf{u} \in \mathcal{E}_Q$ and each column in every matrix $\mathbf{M}_{j,\sigma}$ is an elementary column vector.

We prove the two parts of the lemma as below.

- $\Gamma^\top$ is $\mathcal{E}_Q$-restricted since we have
$$\mathbf{u}\mathbf{M}^\top_{\tau(\ell_{\mathrm{BP}}),x_{\rho\circ\tau(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}^\top_{\tau(i+1),x_{\rho\circ\tau(i+1)}} = (\mathbf{M}_{\ell_{\mathrm{BP}}-i,x_{\rho(\ell_{\mathrm{BP}}-i)}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top)^\top \in \mathcal{E}_Q, \quad \forall i \in [0, \ell_{\mathrm{BP}}]$$
where the equality is implied by the structure of $\Gamma^\top$ and we use property (29).
- To prove (27), we rely on the fact
$$\begin{aligned}\Gamma(x) = 1 &\iff \mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top = 1\\ &\iff \mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top \neq 0 \bmod p\\ &\iff \mathbf{u}\mathbf{M}^\top_{\tau(\ell_{\mathrm{BP}}),x_{\rho\circ\tau(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}^\top_{\tau(1),x_{\rho\circ\tau(1)}}\mathbf{f}^\top \neq 0 \bmod p\\ &\iff \Gamma^\top(x) = 1.\end{aligned}$$
The second $\iff$ follows from the fact that $\mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top \in \{0,1\}$ which is implied by property (28) and (29) while the third $\iff$ is implied by the structure of $\Gamma^\top$. □

6.2 Our ABE scheme for $\mathsf{NBP}^{\oplus_p}$

In this section, we describe our ABE scheme for $\mathsf{NBP}^{\oplus_p}$ in the prime-order group which is motivated by our ABE scheme for $\mathsf{NFA}^{\oplus_p}$ in Section 4. We will prove that this scheme is semi-adaptively secure under k-Lin assumption (see Section 6.3) and adaptively secure if the policy is $\mathcal{E}_Q$-restricted under the same assumption (see Section 6.4). We remark that our scheme and proofs work for a more general form of $\mathsf{NBP}^{\oplus_p}$ where $\mathbf{u}, \mathbf{f}, \mathbf{M}_{j,\sigma}$ are over $\mathbb{Z}_p$ instead of $\{0,1\}$.

Overview. Thanks to the similarity between $\mathsf{NFA}^{\oplus_p}$ and $\mathsf{NBP}^{\oplus_p}$ (cf. Section 3 and Section 6.1), we build our ABE for $\mathsf{NBP}^{\oplus_p}$ following the same paradigm as the ABE for $\mathsf{NFA}^{\oplus_p}$ in Section 4. In particular, we pick $\mathbf{W}_{\eta,\sigma}$ for each $\eta \in \ell$ and $\sigma \in \Sigma$ and pick $\mathbf{D}_j$ for each $j \in [0, \ell_{\mathrm{BP}}]$.

- During the key generation, we encode each $\mathbf{M}_{j,\sigma}$ as follows, which follows the spirit of our ABE for $\mathsf{NFA}^{\oplus_p}$:

$$[\mathbf{D}_j\mathbf{M}_{j,\sigma} - \mathbf{D}_{j-1} + \mathbf{W}_{\rho(j),\sigma}\mathbf{R}_j]_2,\ [\mathbf{R}_j]_2;$$

- During the encryption of $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$, we have the following terms in the ciphertext as common ABEs:

$$[\mathbf{s}\mathbf{A}_1]_1,\ \big\{[\mathbf{s}\mathbf{A}_1\mathbf{W}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]},\ [\mathbf{s}\mathbf{A}_1\mathbf{k}^\top]_T \cdot m.$$

In contrast to ABE for $\mathsf{NFA}^{\oplus_p}$, we use fresh random coin $\mathbf{R}_j$ for each j in secret keys. This is crucial to handle non-injective ρ, see Appendix G.1 for an attack in the case of sharing random coins.

Basis. We will use the following basis used in [7,15] (which is distinct from that in Section 4 and 5):

$$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k\times(k+1)}, \quad \mathbf{a}_2 \leftarrow \mathbb{Z}_p^{1\times(k+1)}$$

and use $(\mathbf{A}_1^{\parallel} \mid \mathbf{a}_2^{\parallel})^\top$ to denote its dual basis. The assumption $\mathrm{SD}^{G_1}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{a}_2}$ and $\mathrm{DDH}^{G_2}_{d,Q}$ can be defined as in Section 4.1.

Scheme. Our ABE for $\mathsf{NBP}^{\oplus_p}$ in prime-order groups is described as follows:

- $\mathsf{Setup}(1^\lambda, \ell, \Sigma)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

$$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k\times(k+1)}, \mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(k+1)} \quad \text{and} \quad \mathbf{W}_{\mathrm{start}}, \mathbf{W}_{\eta,\sigma}, \mathbf{W}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{(k+1)\times k} \ \text{ for all } \eta \in [\ell], \sigma \in \Sigma.$$

  Output

$$\begin{aligned} \mathsf{mpk} &= \big([\mathbf{A}_1, \mathbf{A}_1\mathbf{W}_{\mathrm{start}}, \{\mathbf{A}_1\mathbf{W}_{\eta,\sigma}\}_{\eta\in[\ell],\sigma\in\Sigma}, \mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1, [\mathbf{A}_1\mathbf{k}^\top]_T\big) \\ \mathsf{msk} &= \big(\mathbf{k}, \mathbf{W}_{\mathrm{start}}, \{\mathbf{W}_{\eta,\sigma}\}_{\eta\in[\ell],\sigma\in\Sigma}, \mathbf{W}_{\mathrm{end}}\big). \end{aligned}$$

- $\mathsf{Enc}(\mathsf{mpk}, x, m)$: Let $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$ and $m \in G_T$. Pick $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ and output

$$\mathsf{ct}_x = \Big([\mathbf{s}\mathbf{A}_1]_1, [\mathbf{s}\mathbf{A}_1\mathbf{W}_{\mathrm{start}}]_1, \big\{[\mathbf{s}\mathbf{A}_1\mathbf{W}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]}, [\mathbf{s}\mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1, [\mathbf{s}\mathbf{A}_1\mathbf{k}^\top]_T \cdot m\Big).$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$: Let $\Gamma = (Q, \ell_{\mathrm{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$. Pick

$$\mathbf{D}_0, \mathbf{D}_1, \ldots, \mathbf{D}_{\ell_{\mathrm{BP}}} \leftarrow \mathbb{Z}_p^{(k+1)\times Q},\ \mathbf{R}_1, \ldots, \mathbf{R}_{\ell_{\mathrm{BP}}}, \mathbf{R}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{k\times Q},\ \mathbf{r} \leftarrow \mathbb{Z}_p^{1\times k}$$

  and output

$$\mathsf{sk}_\Gamma = \left(\begin{array}{c} [\mathbf{D}_0\mathbf{u}^\top + \mathbf{W}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{D}_j\mathbf{M}_{j,\sigma} - \mathbf{D}_{j-1} + \mathbf{W}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [\mathbf{k}^\top\mathbf{f} - \mathbf{D}_{\ell_{\mathrm{BP}}} + \mathbf{W}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{array}\right).$$

- $\mathsf{Dec}(\mathsf{mpk},\mathsf{sk}_\Gamma,\mathsf{ct}_x)$: Parse ciphertext for $x=(x_1,\ldots,x_\ell)$ and key for $\Gamma=(Q,\ell_{\mathrm{BP}},\ell,\Sigma,\{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma},\rho,\mathbf{u},\mathbf{f})$ as:

  $$\mathsf{ct}_x=\big([\mathbf{c}]_1,[\mathbf{c}_{\mathrm{start}}]_1,\big\{[\mathbf{c}_\eta]_1\big\}_\eta,[\mathbf{c}_{\mathrm{end}}]_1,C\big)\quad\text{and}\quad \mathsf{sk}_\Gamma=\begin{pmatrix}[\mathbf{k}_{\mathrm{start}}^\top]_2,[\mathbf{r}^\top]_2\\ \big\{[\mathbf{K}_{j,\sigma}]_2,[\mathbf{R}_j]_2\big\}_{j,\sigma}\\ [\mathbf{K}_{\mathrm{end}}]_2,[\mathbf{R}_{\mathrm{end}}]_2\end{pmatrix}$$

  We define

  $$\mathbf{u}_{j,x}^\top=\mathbf{M}_{j,x_{\rho(j)}}\cdots\mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top \bmod p,\ \forall\, j\in[0,\ell_{\mathrm{BP}}] \tag{30}$$

  which are analogous to (11) for $\mathrm{NFA}^{\oplus p}$ in Section 4.2 and proceed as follows:

  1. Compute
  $$B_{\mathrm{start}}=e([\mathbf{c}]_1,[\mathbf{k}_{\mathrm{start}}^\top]_2)\cdot e([\mathbf{c}_{\mathrm{start}}]_1,[\mathbf{r}^\top]_2)^{-1};$$
  2. For all $j=1,\ldots,\ell_{\mathrm{BP}}$, compute
  $$[\mathbf{b}_j]_T=e([\mathbf{c}]_1,[\mathbf{K}_{j,x_{\rho(j)}}]_2)\cdot e([-\mathbf{c}_{\rho(j)}]_1,[\mathbf{R}_j]_2)\quad\text{and}\quad B_j=[\mathbf{b}_j\mathbf{u}_{j-1,x}^\top]_T;$$
  3. Compute
  $$[\mathbf{b}_{\mathrm{end}}]_T=e([\mathbf{c}]_1,[\mathbf{K}_{\mathrm{end}}]_2)\cdot e([-\mathbf{c}_{\mathrm{end}}]_1,[\mathbf{R}_{\mathrm{end}}]_2)\quad\text{and}\quad B_{\mathrm{end}}=[\mathbf{b}_{\mathrm{end}}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top]_T;$$
  4. Compute
  $$B_{\mathrm{all}}=B_{\mathrm{start}}\cdot\textstyle\prod_{j=1}^{\ell_{\mathrm{BP}}}B_j\cdot B_{\mathrm{end}}\quad\text{and}\quad B=B_{\mathrm{all}}^{(\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top)^{-1}}$$
  and output the message $m'\leftarrow C\cdot B^{-1}$.

Correctness. For $x=(x_1,\ldots,x_\ell)$ and $\Gamma=(Q,\ell_{\mathrm{BP}},\ell,\Sigma,\{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma},\rho,\mathbf{u},\mathbf{f})$ such that $\Gamma(x)=1$, we have:

$$\begin{aligned}
B_{\mathrm{start}} &= [\mathbf{s}\mathbf{A}_1\mathbf{D}_0\mathbf{u}^\top]_T=[\mathbf{s}\mathbf{A}_1\mathbf{D}_0\mathbf{u}_{0,x}^\top]_T && (31)\\
\mathbf{b}_j &= \mathbf{s}\mathbf{A}_1\mathbf{D}_j\mathbf{M}_{j,x_{\rho(j)}}-\mathbf{s}\mathbf{A}_1\mathbf{D}_{j-1} && (32)\\
B_j &= [\mathbf{s}\mathbf{A}_1\mathbf{D}_j\mathbf{u}_{j,x}^\top-\mathbf{s}\mathbf{A}_1\mathbf{D}_{j-1}\mathbf{u}_{j-1,x}^\top]_T && (33)\\
\mathbf{b}_{\mathrm{end}} &= \mathbf{s}\mathbf{A}_1\mathbf{k}^\top\mathbf{f}-\mathbf{s}\mathbf{A}_1\mathbf{D}_{\ell_{\mathrm{BP}}} && (34)\\
B_{\mathrm{end}} &= [\mathbf{s}\mathbf{A}_1\mathbf{k}^\top\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top-\mathbf{s}\mathbf{A}_1\mathbf{D}_{\ell_{\mathrm{BP}}}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top]_T && (35)\\
B_{\mathrm{all}} &= [\mathbf{s}\mathbf{A}_1\mathbf{k}^\top\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top]_T && (36)\\
B &= [\mathbf{s}\mathbf{A}_1\mathbf{k}^\top]_T && (37)
\end{aligned}$$

Here (35) is trivial; (33) and (37) follow from facts

$$\mathbf{u}_{j,x}^\top=\mathbf{M}_{j,x_{\rho(j)}}\mathbf{u}_{j-1,x}^\top \bmod p,\ \forall\, j\in[\ell_{\mathrm{BP}}]\quad\text{and}\quad \Gamma(x)=1\Longleftrightarrow \mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top\neq 0 \bmod p \tag{38}$$

by the definition in (30), the remaining equalities follow from:

$$\begin{aligned}
&\text{(31)} & \mathbf{s}\mathbf{A}_1\mathbf{D}_0\mathbf{u}^\top &= \mathbf{s}\mathbf{A}_1\cdot(\mathbf{D}_0\mathbf{u}^\top+\mathbf{W}_{\mathrm{start}}\mathbf{r}^\top)-\mathbf{s}\mathbf{A}_1\mathbf{W}_{\mathrm{start}}\cdot\mathbf{r}^\top\\
&\text{(32)} & \mathbf{s}\mathbf{A}_1\mathbf{D}_j\mathbf{M}_{j,x_{\rho(j)}}-\mathbf{s}\mathbf{A}_1\mathbf{D}_{j-1} &= \mathbf{s}\mathbf{A}_1\cdot(\mathbf{D}_j\mathbf{M}_{j,x_{\rho(j)}}-\mathbf{D}_{j-1}+\mathbf{W}_{\rho(j),x_{\rho(j)}}\mathbf{R}_j)-\mathbf{s}\mathbf{A}_1\mathbf{W}_{\rho(j),x_{\rho(j)}}\cdot\mathbf{R}_j\\
&\text{(34)} & \mathbf{s}\mathbf{A}_1\mathbf{k}^\top\mathbf{f}-\mathbf{s}\mathbf{A}_1\mathbf{D}_{\ell_{\mathrm{BP}}} &= \mathbf{s}\mathbf{A}_1\cdot(\mathbf{k}^\top\mathbf{f}-\mathbf{D}_{\ell_{\mathrm{BP}}}+\mathbf{W}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}})-\mathbf{s}\mathbf{A}_1\mathbf{W}_{\mathrm{end}}\cdot\mathbf{R}_{\mathrm{end}}\\
&\text{(36)} & \mathbf{s}\mathbf{A}_1\mathbf{k}^\top\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top &= \mathbf{s}\mathbf{A}_1\mathbf{D}_0\mathbf{u}_{0,x}^\top+\textstyle\sum_{j=1}^{\ell_{\mathrm{BP}}}(\mathbf{s}\mathbf{A}_1\mathbf{D}_j\mathbf{u}_{j,x}^\top-\mathbf{s}\mathbf{A}_1\mathbf{D}_{j-1}\mathbf{u}_{j-1,x}^\top)+(\mathbf{s}\mathbf{A}_1\mathbf{k}^\top\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top-\mathbf{s}\mathbf{A}_1\mathbf{D}_{\ell_{\mathrm{BP}}}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top).
\end{aligned}$$

Correctness follows readily.

6.3 Semi-adaptive Security Security

We have the following theorem stating that the scheme in Section 6.2 is selectively secure. We remark that the proof described in this subsection can be naturally extended to prove semi-adaptive security.

Theorem 3 (Selectively secure ABE for NBP$^{\oplus p}$). *The ABE scheme for NBP$^{\oplus p}$ in prime-order bilinear groups described above is selectively secure (cf. Section 2.1) under the k-Lin assumption with security loss $O(q \cdot \ell_{BP} \cdot |\Sigma|)$. Here ℓ_{BP} are maximal length of all NBPs in adversary's key queries and q is the number of key queries.*

We will give the proof in the one-key setting which is sufficient to motivate adaptive proof in Section 6.4 where we will handle multiple key queries. Due to the similarity between NBP$^{\oplus p}$ and NFA$^{\oplus p}$, our proof technique for NBP$^{\oplus p}$ in this section is borrowed from that for NFA$^{\oplus p}$ in Section 4. We begin with auxiliary distributions.

Auxiliary distributions. Let $x^* \in \Sigma^\ell$ denote the selective challenge and assume $\ell_{\mathrm{BP}} > 1$. We describe the auxiliary ciphertext and key distributions that we use in the proof of security. Throughout, the distributions are the same as the original distributions except for the $\mathbf{a}_2$-components which are defined analogous to Section 4.3; we will use the same notation for them.

Ciphertext distribution. We sample $s \leftarrow \mathbb{Z}_p$ and define:

- $\mathsf{ct}^*_{x^*}$ is the same as ct_{x^*} except we replace $\mathbf{s}\mathbf{A}_1$ with $\mathbf{s}\mathbf{A}_1 + s\mathbf{a}_2$.

That is, we have:

$$\mathsf{ct}^*_{x^*}[2] = \big([s]_1, [s\mathbf{w}_{\mathrm{start}}]_1, \big\{[s\mathbf{w}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]}, [s\mathbf{w}_{\mathrm{end}}]_1, [s\alpha]_T \cdot m_\beta\big).$$

Secret key distributions. For any $\Gamma = (Q, \ell_{\mathrm{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$, we define

$$\mathbf{f}_{i,x^*} = \mathbf{f}\mathbf{M}_{\ell_{\mathrm{BP}},x^*_{\rho(\ell_{\mathrm{BP}})}} \cdots \mathbf{M}_{i+1,x^*_{\rho(i+1)}} \bmod p,\ \forall i \in [0,\ell_{\mathrm{BP}}] \tag{39}$$

analogous to (22) for NFA$^{\oplus p}$ in Section 4.3. For all $i \in [\ell_{\mathrm{BP}}]$, we sample $\Delta \leftarrow \mathbb{Z}_p$ and define:

- sk^0_Γ is the same as sk_Γ except we replace $\mathbf{D}_0$ with $\mathbf{D}_0 + \mathbf{a}_2^\parallel \cdot \Delta \cdot \mathbf{f}_{0,x^*}$ in the term $[\mathbf{D}_0\mathbf{u}^\top + \mathbf{W}_{\mathrm{start}}\mathbf{r}^\top]_2$;
- sk^i_Γ is the same as sk_Γ except we replace $\mathbf{D}_i$ with $\mathbf{D}_i + \mathbf{a}_2^\parallel \cdot \Delta \cdot \mathbf{f}_{i,x^*}$ in the term $[\mathbf{D}_i\mathbf{M}_{i,\sigma} - \mathbf{D}_{i-1} + \mathbf{W}_{\rho(i),\sigma}\mathbf{R}_i]_2$ for all $\sigma \in \Sigma$;
- $\mathsf{sk}^{i-1,i}_\Gamma$ is the same as sk_Γ except we replace $-\mathbf{D}_{i-1}$ with $-\mathbf{D}_{i-1} + \mathbf{a}_2^\parallel \cdot \Delta \cdot \mathbf{f}_{i-1,x^*}$ in the term $[\mathbf{D}_i\mathbf{M}_{i,\sigma} - \mathbf{D}_{i-1} + \mathbf{W}_{\rho(i),\sigma}\mathbf{R}_i]_2$ for all $\sigma \in \Sigma$;
- sk^*_Γ is the same as sk_Γ except we replace $-\mathbf{D}_{\ell_{\mathrm{BP}}}$ with $-\mathbf{D}_{\ell_{\mathrm{BP}}} + \mathbf{a}_2^\parallel \cdot \Delta \cdot \mathbf{f}$ to the term $[\mathbf{k}^\top\mathbf{f} - \mathbf{D}_{\ell_{\mathrm{BP}}} + \mathbf{W}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2$.

That is, we have:

$$\mathsf{sk}^0_\Gamma[2] = \begin{pmatrix} [(\mathbf{d}_0 + \boxed{\Delta\cdot\mathbf{f}_{0,x^*}})\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2,\ [\mathbf{R}_j]_2\big\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}$$

$$\mathsf{sk}^i_\Gamma[2] = \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[(\mathbf{d}_i + \boxed{\Delta\cdot\mathbf{f}_{i,x^*}})\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\big\}_{\sigma\in\Sigma} \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}$$

$$\mathsf{sk}^{i-1,i}_\Gamma[2] = \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \boxed{\Delta\cdot\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\big\}_{\sigma\in\Sigma} \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}$$

$$\mathsf{sk}^*_\Gamma[2] \;=\; \left(\begin{array}{c} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2,\, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2,\, [\mathbf{R}_j]_2\big\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [\alpha\mathbf{f} + \boxed{\Delta\cdot\mathbf{f}} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2,\, [\mathbf{R}_{\mathrm{end}}]_2 \end{array}\right).$$

The definition for keys for NBP$^{\oplus p}$ follows the spirit of those for NFA$^{\oplus p}$ in Section 4.3.

Game sequence. We prove Theorem 3 via a series of games summarized in Fig 9:

- G_0: Identical to the real game.
- G_1: Identical to G_0 except that the challenge ciphertext is $\mathsf{ct}^*_{x^*}$.
- $\mathsf{G}_{2.i.0}$, $i \in [\ell_{\mathrm{BP}}]$: In this game, the challenge ciphertext is $\mathsf{ct}^*_{x^*}$ and the secret key is sk^{i-1}_Γ.
- $\mathsf{G}_{2.i.1}$, $i \in [\ell_{\mathrm{BP}}]$: Identical to $\mathsf{G}_{2.i.0}$ except that the secret key is $\mathsf{sk}^{i-1,i}_\Gamma$.
- $\mathsf{G}_{2.i.2}$, $i \in [\ell_{\mathrm{BP}}]$: Identical to $\mathsf{G}_{2.i.1}$ except that the secret key is sk^{i}_Γ.
- G_3: Identical to $\mathsf{G}_{2.\ell_{\mathrm{BP}}.2}$ except that the secret key is sk^*_Γ.

Here we have $\mathsf{G}_{2.1.0} = \mathsf{G}_1$ and $\mathsf{G}_{2.i.0} = \mathsf{G}_{2.i-1.2}$ for $i \in [2, \ell_{\mathrm{BP}}]$. We note that the game sequence is quite similar to that in Section 4.3: the games listed above roughly correspond to G_0, G_1, $\mathsf{G}_{2.i.0}$, $\mathsf{G}_{2.i.1}$, $\mathsf{G}_{2.i.3}$ and G_3 there, respectively, and we only change the ciphertext distribution once for all. Furthermore, we will borrow the proof technique from Section 4 to show the indistinguishability of each pair of adjacent games. The distinction is that we crucially use the property of $\mathbf{f}_{0,x^*}, \ldots, \mathbf{f}_{\ell_{\mathrm{BP}},x^*}$ defined in (39), which will be captured by the following lemma.

Useful Lemma. We describe the lemma which is analogous to Lemma 5.

Lemma 24 (Property of $\{\mathbf{f}_{i,x^*}\}_{i\in[0,\ell_{\mathrm{BP}}]}$). *For any $\Gamma = (Q, \ell_{BP}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{BP}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$ and $x^* \in \Sigma^\ell$, we have:*

1. $\Gamma(x^*) = 0 \iff \mathbf{f}_{0,x^*}\mathbf{u}^\top = 0 \bmod p$;
2. $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{i,x^*_{\rho(i)}} \bmod p$ *for all* $i \in [\ell_{BP}]$;
3. $\mathbf{f}_{\ell_{BP},x^*} = \mathbf{f}$.

Proof. The lemma directly follows from the definitions of NBP$^{\oplus p}$ in Section 6.1 and $\mathbf{f}_{0,x^*}, \ldots, \mathbf{f}_{\ell_{\mathrm{BP}},x^*}$ in (39). □

Initializing & Finalizing. It is standard to prove that $\mathsf{G}_0 \approx_c \mathsf{G}_1$ and $\Pr[\langle \mathcal{A}, \mathsf{G}_3\rangle = 1] = 1/2$. (See Appendix G.2 for details.) We prove the following lemma stating that $\mathsf{G}_1 \approx_c \mathsf{G}_{2.1.0}$, which is analogous to Lemma 6.

Lemma 25. *For all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_1\rangle = 1] = \Pr[\langle \mathcal{A}, \mathsf{G}_{2.1.0}\rangle = 1]$$

Proof. Roughly, we will prove that

$$\big(\mathsf{mpk}, \mathsf{ct}^*_{x^*}, \boxed{\mathsf{sk}_\Gamma}\big) = \big(\mathsf{mpk}, \mathsf{ct}^*_{x^*}, \colorbox{lightgray}{sk^0_Γ}\big)$$

where we have

$$\mathsf{sk}_\Gamma[2] \;=\; \left(\begin{array}{c} [\boxed{\mathbf{d}_0\mathbf{u}^\top} + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2,\, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2,\, [\mathbf{R}_j]_2\big\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2,\, [\mathbf{R}_{\mathrm{end}}]_2 \end{array}\right),$$

$$\mathsf{sk}^0_\Gamma[2] \;=\; \left(\begin{array}{c} [\colorbox{lightgray}{$(\mathbf{d}_0 + \Delta\cdot\mathbf{f}_{0,x^*})\mathbf{u}^\top$} + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2,\, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2,\, [\mathbf{R}_j]_2\big\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2,\, [\mathbf{R}_{\mathrm{end}}]_2 \end{array}\right)$$

and

$$\mathsf{ct}^*_{x^*}[2] = \Big([s]_1,\, [s\mathbf{w}_{\mathrm{start}}]_1,\, \big\{[s\mathbf{w}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]},\, [s\mathbf{w}_{\mathrm{end}}]_1,\, [s\alpha]_T\cdot m_\beta\Big).$$

Game	ct_{x^*}		$\mathsf{sk}_\Gamma[2]$				Remark
			$? \cdot \mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top$	$? \cdot \mathbf{M}_{i-1,\sigma} + ? + \mathbf{w}_{\rho(i-1),\sigma}\mathbf{R}_{i-1}$	$? \cdot \mathbf{M}_{i,\sigma} + ? + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$	$\alpha\mathbf{f} + ? + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}$	
0	ct_{x^*}	sk_Γ	$\mathbf{d}_0$	$\mathbf{d}_{i-1}, -\mathbf{d}_{i-2}$	$\mathbf{d}_i, -\mathbf{d}_{i-1}$	$-\mathbf{d}_{\ell_{\mathrm{BP}}}$	Real game
1	$\boxed{\mathsf{ct}^*_{x^*}}$	sk_Γ	$\mathbf{d}_0$	$\mathbf{d}_{i-1}, -\mathbf{d}_{i-2}$	$\mathbf{d}_i, -\mathbf{d}_{i-1}$	$-\mathbf{d}_{\ell_{\mathrm{BP}}}$	SD
2.1.0	$\mathsf{ct}^*_{x^*}$	$\boxed{\mathsf{sk}^0_\Gamma}$	$\boxed{\mathbf{d}_0 + \Delta \cdot \mathbf{f}_{0,x^*}}$	$\mathbf{d}_{i-1}, -\mathbf{d}_{i-2}$	$\mathbf{d}_i, -\mathbf{d}_{i-1}$	$-\mathbf{d}_{\ell_{\mathrm{BP}}}$	$\mathbf{f}_{0,x^*}\mathbf{u}^\top = 0 \bmod p$ (Lemma 24)
2.i.0	$\mathsf{ct}^*_{x^*}$	$\boxed{\mathsf{sk}^{i-1}_\Gamma}$	$\mathbf{d}_0$	$\boxed{\mathbf{d}_{i-1} + \Delta \cdot \mathbf{f}_{i-1,x^*}}, -\mathbf{d}_{i-2}$	$\mathbf{d}_i, -\mathbf{d}_{i-1}$	$-\mathbf{d}_{\ell_{\mathrm{BP}}}$	$i \in [2, \ell_{\mathrm{BP}}]$
2.i.1	$\mathsf{ct}^*_{x^*}$	$\boxed{\mathsf{sk}^{i-1,i}_\Gamma}$	$\mathbf{d}_0$	$\mathbf{d}_{i-1}, -\mathbf{d}_{i-2}$	$\mathbf{d}_i, \boxed{-\mathbf{d}_{i-1} + \Delta \cdot \mathbf{f}_{i-1,x^*}}$	$-\mathbf{d}_{\ell_{\mathrm{BP}}}$	change of variables
2.i.2	$\mathsf{ct}^*_{x^*}$	$\boxed{\mathsf{sk}^i_\Gamma}$	$\mathbf{d}_0$	$\mathbf{d}_{i-1}, -\mathbf{d}_{i-2}$	$\boxed{\mathbf{d}_i + \Delta \cdot \mathbf{f}_{i,x^*}}, \boxed{-\mathbf{d}_{i-1}}$	$-\mathbf{d}_{\ell_{\mathrm{BP}}}$	DDH, $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{i,x_{\rho(i)}} \bmod p$ (Lemma 24)
3	$\mathsf{ct}^*_{x^*}$	$\boxed{\mathsf{sk}^*_\Gamma}$	$\mathbf{d}_0$	$\mathbf{d}_{i-1}, -\mathbf{d}_{i-2}$	$\mathbf{d}_i, -\mathbf{d}_{i-1}$	$\boxed{-\mathbf{d}_{\ell_{\mathrm{BP}}} + \Delta \cdot \mathbf{f}}$	change of variables, $\mathbf{f}_{\ell_{\mathrm{BP}},x^*} = \mathbf{f}$ (Lemma 24)

Fig. 9. Game sequence for selectively secure ABE for $\mathrm{NBP}^{\oplus p}$ with $i \in [\ell_{\mathrm{BP}}]$. We focus on the $\mathbf{a}_2$-components of sk_Γ and all terms in the fifth and sixth columns are quantified over $\sigma \in \Sigma$. In the **Remark** column, "SD" and "DDH" indicate $\mathrm{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{a}_2}$ and $\mathrm{DDH}^{G_2}_{1,Q}$ assumption, respectively.

This follows from the statement:

$$\overbrace{\{\boxed{\mathbf{d}_0\mathbf{u}^\top}+\mathbf{w}_{\mathrm{start}}\mathbf{r}^\top,\mathbf{r}^\top\}}^{\mathsf{sk}_\Gamma[2]}=\overbrace{\{\colorbox{lightgray}{$(\mathbf{d}_0+\Delta\cdot\mathbf{f}_{0,x^*})\mathbf{u}^\top$}+\mathbf{w}_{\mathrm{start}}\mathbf{r}^\top,\mathbf{r}^\top\}}^{\mathsf{sk}^0_\Gamma[2]}\quad\text{given}\quad\mathbf{d}_0,\overbrace{\mathbf{w}_{\mathrm{start}}}^{\mathsf{ct}^*_{x^*}[2]}$$

which is implied by the fact $\Gamma(x^*)=0\iff\mathbf{f}_{0,x^*}\mathbf{u}^\top=0 \bmod p$, see Lemma 24. □

Key switching I. We will prove that $\mathsf{G}_{2.i.0}\approx_s\mathsf{G}_{2.i.1}$ for all $i\in[\ell_{\mathrm{BP}}]$ and $\mathsf{G}_{2.\ell_{\mathrm{BP}}.2}\approx_s\mathsf{G}_3$.The proofs of them are similar. We begin with the following lemma stating that $\mathsf{G}_{2.1.0}\approx_s\mathsf{G}_{2.1.1}$, which is analogous to Lemma 7, and sketch the proofs for remaining statements.

Lemma 26. *For all $\mathcal{A}$, we have*

$$\Pr[\langle\mathcal{A},\mathsf{G}_{2.1.0}\rangle=1]\approx\Pr[\langle\mathcal{A},\mathsf{G}_{2.1.1}\rangle=1].$$

Proof. Roughly, we will prove that

$$\big(\mathsf{mpk},\mathsf{ct}^*_{x^*},\boxed{\mathsf{sk}^0_\Gamma}\big)\approx_s\big(\mathsf{mpk},\mathsf{ct}^*_{x^*},\colorbox{lightgray}{$\mathsf{sk}^{0,1}_\Gamma$}\big)$$

By Lemma 4, this means that

$$\mathsf{sk}^0_\Gamma[2]=\begin{pmatrix}[\boxed{(\mathbf{d}_0+\Delta\cdot\mathbf{f}_{0,x^*})}\mathbf{u}^\top+\mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2,[\mathbf{r}^\top]_2\\ \{[\mathbf{d}_1\mathbf{M}_{1,\sigma}\boxed{-\mathbf{d}_0}+\mathbf{w}_{\rho(1),\sigma}\mathbf{R}_1]_2,\ [\mathbf{R}_1]_2\}_{\sigma\in\Sigma}\\ \{[\mathbf{d}_j\mathbf{M}_{j,\sigma}-\mathbf{d}_{j-1}+\mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2,[\mathbf{R}_j]_2\}_{j\neq1,\sigma\in\Sigma}\\ [\alpha\mathbf{f}-\mathbf{d}_{\ell_{\mathrm{BP}}}+\mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2,[\mathbf{R}_{\mathrm{end}}]_2\end{pmatrix}\approx_s\begin{pmatrix}[\colorbox{lightgray}{$\mathbf{d}_0$}\mathbf{u}^\top+\mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2,[\mathbf{r}^\top]_2\\ \{[\mathbf{d}_1\mathbf{M}_{1,\sigma}\colorbox{lightgray}{$-\mathbf{d}_0+\Delta\cdot\mathbf{f}_{0,x^*}$}+\mathbf{w}_{\rho(1),\sigma}\mathbf{R}_1]_2,\ [\mathbf{R}_1]_2\}_{\sigma\in\Sigma}\\ \{[\mathbf{d}_j\mathbf{M}_{j,\sigma}-\mathbf{d}_{j-1}+\mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2,\ [\mathbf{R}_j]_2\}_{j\neq1,\sigma\in\Sigma}\\ [\alpha\mathbf{f}-\mathbf{d}_{\ell_{\mathrm{BP}}}+\mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2,[\mathbf{R}_{\mathrm{end}}]_2\end{pmatrix}=\mathsf{sk}^{0,1}_\Gamma[2]$$

given

$$\mathsf{ct}^*_{x^*}[2]=\big([s]_1,\ [s\mathbf{w}_{\mathrm{start}}]_1,\ \{[s\mathbf{w}_{\eta,x_\eta}]_1\}_{\eta\in[\ell]},\ [s\mathbf{w}_{\mathrm{end}}]_1,\ [s\alpha]_T\cdot m_\beta\big).$$

This immediately follows from change of variables $\mathbf{d}_0\mapsto\mathbf{d}_0-\Delta\cdot\mathbf{f}_{0,x^*}$. Here we use the fact that $\mathbf{d}_0$ does not appear elsewhere. □

Via the same proof idea, we can prove the following two lemmas stating that $\mathsf{G}_{2.i.0}\approx_c\mathsf{G}_{2.i.1}$ for all $i\in[2,\ell_{\mathrm{BP}}]$ and $\mathsf{G}_{2.\ell_{\mathrm{BP}}.2}\approx_c\mathsf{G}_3$, respectively. The first lemma relies on change of variable $\mathbf{d}_{i-1}\mapsto\mathbf{d}_{i-1}-\Delta\cdot\mathbf{f}_{i-1,x^*}$; while the second lemma relies on change of variable $\mathbf{d}_{\ell_{\mathrm{BP}}}\mapsto\mathbf{d}_{\ell_{\mathrm{BP}}}-\Delta\cdot\mathbf{f}_{\ell_{\mathrm{BP}},x^*}$ and the fact that $\mathbf{f}_{\ell_{\mathrm{BP}},x^*}=\mathbf{f}$, see Lemma 24. We give the lemmas and omit the proofs.

Lemma 27. *For all $i\in[2,\ell_{BP}]$ and all $\mathcal{A}$, we have*

$$\Pr[\langle\mathcal{A},\mathsf{G}_{2.i.0}\rangle=1]\approx\Pr[\langle\mathcal{A},\mathsf{G}_{2.i.1}\rangle=1].$$

Lemma 28. *For all $\mathcal{A}$, we have*

$$\Pr[\langle\mathcal{A},\mathsf{G}_{2.\ell_{BP}.2}\rangle=1]\approx\Pr[\langle\mathcal{A},\mathsf{G}_3\rangle=1].$$

Key switching II. We prove the following lemma stating that $\mathsf{G}_{2.i.1}\approx_c\mathsf{G}_{2.i.2}$ for all $i\in[\ell_{\mathrm{BP}}]$, which is analogous to Lemma 17 and relies on the property of $\mathbf{f}_{0,x^*},\dots,\mathbf{f}_{\ell_{\mathrm{BP}},x^*}$, see Lemma 24.

Lemma 29. *For all $i\in[\ell_{BP}]$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B})\approx\mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle\mathcal{A},\mathsf{G}_{2.i.1}\rangle=1]-\Pr[\langle\mathcal{A},\mathsf{G}_{2.i.2}\rangle=1]\le O(|\Sigma|)\cdot\mathsf{Adv}^{\mathrm{DDH}^{G_2}_{1,Q}}_{\mathcal{B}}(\lambda).$$

Overview. Roughly, we are proving

$$\left(\mathsf{mpk}, \mathsf{ct}^*_{x^*}, \boxed{\mathsf{sk}_\Gamma^{i-1,i}}\right) \approx_c \left(\mathsf{mpk}, \mathsf{ct}^*_{x^*}, \mathsf{sk}_\Gamma^{i}\right)$$

More concretely, we want to prove the following statement over $\mathbf{a}_2$-components:

$$\overbrace{\left\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \Delta\cdot\boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\right\}_{\sigma\in\Sigma}}^{\mathsf{sk}_\Gamma^{i-1,i}[2]} \approx_c \overbrace{\left\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \Delta\cdot\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\right\}_{\sigma\in\Sigma}}^{\mathsf{sk}_\Gamma^{i}[2]}$$

given $\mathbf{w}_{\rho(i),x^*_{\rho(i)}}$ leaked by $\mathsf{ct}^*_{x^*}[2]$ and $\mathbf{d}_i, \mathbf{d}_{i-1}$ appeared in other subkeys. Then,

- we handle terms with $\sigma \neq x^*_{\rho(i)}$ using $\mathrm{DDH}^{G_2}_{1,Q}$ assumption w.r.t. $\mathbf{w}_{\rho(i),\sigma}$; this relies on the fact that $\mathbf{w}_{\rho(i),\sigma}$ with $\sigma \neq x^*_{\rho(i)}$ are not leaked;
- we handle the remaining term, i.e., one with $\sigma = x^*_{\rho(i)}$, by the fact that $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{i,x^*_{\rho(i)}} \bmod p$, see Lemma 24; note that we cannot use $\mathrm{DDH}^{G_2}_{1,Q}$ assumption for this case since $\mathbf{w}_{\rho(i),x^*_{\rho(i)}}$ is leaked via $\mathsf{ct}^*_{x^*}[2]$.

Proof. By Lemma 4, it suffices to prove the lemma over $\mathbf{a}_2$-components which roughly means:

$$\mathsf{sk}_\Gamma^{i-1,i}[2] = \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \left\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \boxed{\Delta\cdot\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\right\}_{\sigma\in\Sigma} \\ \left\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\right\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}$$

$$\approx_c \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \left\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \Delta\cdot\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\right\}_{\sigma\in\Sigma} \\ \left\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\right\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix} = \mathsf{sk}_\Gamma^{i}[2]$$

in the presence of

$$\mathsf{ct}^*_{x^*}[2] = \left([s]_1,\ [s\mathbf{w}_{\mathrm{start}}]_1,\ \{[s\mathbf{w}_{\eta,x_\eta}]_1\}_{\eta\in[\ell]},\ [s\mathbf{w}_{\mathrm{end}}]_1,\ [s\alpha]_T\cdot m_\beta\right).$$

One can sample basis $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_1^\parallel, \mathbf{a}_2^\parallel$ and trivially simulate mpk, $\mathsf{ct}^*_{x^*}$ and secret key using terms given out above. Furthermore, we prove this using the following statement implied by $\mathrm{DDH}^{G_2}_{1,Q}$ assumption: for all $\Delta\in\mathbb{Z}_p$, we have

$$\left\{[\mathbf{w}_{\rho(i),\sigma}\mathbf{B}]_2, [\mathbf{B}]_2, [\Delta\cdot\boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2, [\mathbf{R}_i]_2\right\}_{\sigma\neq x^*_{\rho(i)}} \approx_c \left\{[\mathbf{w}_{\rho(i),\sigma}\mathbf{B}]_2, [\mathbf{B}]_2, [\Delta\cdot\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2, [\mathbf{R}_i]_2\right\}_{\sigma\neq x^*_{\rho(i)}}$$

where $\mathbf{w}_{\rho(i),\sigma} \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$ and $\mathbf{R}_i \leftarrow \mathbb{Z}_p^{k\times Q}$. On input $\left\{[\mathbf{w}_{\rho(i),\sigma}\mathbf{B}]_2, [\mathbf{B}]_2, [\mathbf{t}_\sigma]_2, [\mathbf{R}_i]_2\right\}_{\sigma\neq x^*_{\rho(i)}}$ where

$$\mathbf{t}_\sigma = \Delta\cdot\boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i \quad\text{or}\quad \mathbf{t}_\sigma = \Delta\cdot\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i,$$

we sample $\alpha \leftarrow \mathbb{Z}_p, \mathbf{w}_{\mathrm{start}}, \mathbf{w}_{\rho(i),x^*_{\rho(i)}}, \mathbf{w}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1\times k}$ and $\mathbf{w}_{\eta,\sigma} \leftarrow \mathbb{Z}_p^{1\times k}$ for all $\eta\neq\rho(i), \sigma\in\Sigma$ and proceed as follows:

(Simulating the ciphertext) On input (m_0, m_1), we sample $s \leftarrow \mathbb{Z}_p$ and simulate $\mathsf{ct}^*_{x^*}[2]$ using the knowledge of $\mathbf{w}_{\rho(i),x^*_{\rho(i)}}$ and $\{\mathbf{w}_{\eta,x^*_\eta}\}_{\eta\neq\rho(i)}$. Here we use the fact that the ciphertext does not involve $\{\mathbf{w}_{\rho(i),\sigma}\}_{\sigma\neq x^*_{\rho(i)}}$.

(Simulating the secret key) On input Γ, we want to simulate secret key for Γ in the following form:

$$\begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \left\{[\mathbf{d}_i\mathbf{M}_{i,x^*_{\rho(i)}} - \mathbf{d}_{i-1} + \Delta\cdot\mathbf{f}_{i-1,x^*} + \mathbf{w}_{\rho(i),x^*_{\rho(i)}}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\right\} \\ \left\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \mathbf{t}_\sigma]_2,\ [\mathbf{R}_i]_2\right\}_{\sigma\neq x^*_{\rho(i)}} \\ \left\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\right\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}$$

Observe that,

- when $\mathbf{t}_\sigma = \Delta \cdot \boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$, the distribution is identical to $\boxed{\mathsf{sk}_\Gamma^{i-1,i}[2]}$;
- when $\mathbf{t}_\sigma = \Delta \cdot \colorbox{lightgray}{$\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma}$} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$, the distribution is identical to $\colorbox{lightgray}{$\mathsf{sk}_\Gamma^{i}[2]$}$ since $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{i,x^*_{\rho(i)}} \bmod p$, see Lemma 24.

We sample $\mathbf{d}_0, \ldots, \mathbf{d}_{\ell_{\mathrm{BP}}} \leftarrow \mathbb{Z}_p^{1\times Q}$ and simulate the key as follows:

- We simulate the terms in the second row using $[\mathbf{R}_i]_2$ and $\mathbf{w}_{\rho(i),x^*_{\rho(i)}}$;
- We simulate the terms in the third row using $[\mathbf{t}_\sigma]_2$ and $[\mathbf{R}_i]_2$;
- All remaining terms can be simulated using $\{\mathbf{w}_{\eta,\sigma}\}_{\eta\neq\rho(i),\sigma\in\Sigma}$, $\{[\mathbf{w}_{\rho(i),\sigma}\mathbf{B}]_2\}_{\sigma\neq x^*_{\rho(i)}}$, $\mathbf{w}_{\rho(i),x^*_{\rho(i)}}$, $\mathbf{w}_{\mathrm{start}}$, $\mathbf{w}_{\mathrm{end}}$ and $[\mathbf{B}]_2$.

Observe that, when $\mathbf{t}_\sigma = \Delta \cdot \boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$, the secret key is $\boxed{\mathsf{sk}_\Gamma^{i-1,i}[2]}$ and the simulation is identical to $\mathsf{G}_{2.i.1}$; when $\mathbf{t}_\sigma = \Delta \cdot \colorbox{lightgray}{$\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma}$} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$, the secret key is $\colorbox{lightgray}{$\mathsf{sk}_\Gamma^{i}[2]$}$ and the simulation is identical to $\mathsf{G}_{2.i.2}$. This completes the proof. □

6.4 Adaptive Security for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$

In this subsection, we prove that the scheme in Section 6.2 is adaptively secure for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$. By Lemma 23, this immediately gives us our compact adaptively secure ABE for branching program. We prove the following theorem for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$ and defer the resultant concrete construction of ABE for branching programs to Appendix H.

Theorem 4 (Adaptively secure ABE for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$). *The ABE scheme for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$ in prime-order bilinear groups described in Section 6.2 is adaptively secure (cf. Section 2.1) under the k-Lin assumption with security loss $O(q\cdot\ell_{BP}\cdot|\Sigma|^2\cdot Q^2)$. Here ℓ_{BP} are maximal length of all NBPs in adversary's key queries and q is the number of key queries.*

We will prove the theorem using the proof technique for the one-key selective security in Section 6.3 and the piecewise guessing framework [15]. This is analogous to the proof in Section 5. Let $x^* \in \Sigma^\ell$ denote the adaptive challenge. Without loss of generality, we assume $\ell_{\mathrm{BP}} > 1$.

Game sequence. We prove Theorem 4 via a series of games following the standard dual system method [20]:

- G_0: Identical to the real game.
- G_1: Identical to G_0 except that the challenge ciphertext is $\mathsf{ct}^*_{x^*}$.
- $\mathsf{G}_{2.\kappa}$ for $\kappa \in [0,q]$: Identical to G_1 except that the first κ secret keys are sk^*_Γ.
- G_3: Identical to $\mathsf{G}_{2.q}$ except that the challenge ciphertext is an encryption of a random message.

Here we have $\mathsf{G}_{2.0} = \mathsf{G}_1$. It is standard to prove $\mathsf{G}_0 \approx_c \mathsf{G}_1$, $\mathsf{G}_{2.q} \approx_c \mathsf{G}_3$ and show that adversary in G_3 has no advantage. To prove $\mathsf{G}_{2.\kappa-1} \approx_c \mathsf{G}_{2.\kappa}$ for all $\kappa \in [q]$, we use the following core lemma.

Lemma 30 (Core lemma). *For all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ and*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{CORE}}(\lambda) = \Pr[\langle \mathcal{A}, \mathsf{H}_0\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{H}_1\rangle = 1] \le O(\ell\cdot|\Sigma|^2\cdot Q^2)\cdot \mathsf{Adv}_{\mathcal{B}}^{k\text{-}\mathrm{LIN}}(\lambda)$$

where, for all $b \in \{0,1\}$, we define:

$$\langle \mathcal{A}, \mathsf{H}_b\rangle := \{b' \leftarrow \mathcal{A}^{\mathsf{OEnc}(\cdot),\mathsf{OKey}(\cdot)}(\mathsf{aux})\}$$

where

$$\mathsf{aux} = \left([\mathbf{B}, \{\mathbf{w}_{j,\sigma}\mathbf{B}\}_{j\in[\ell],\sigma\in\Sigma}]_2, \alpha, \Delta, \mathbf{w}_{start}, \mathbf{w}_{end}\right)$$

with $\mathbf{w}_{start}, \mathbf{w}_{end}, \mathbf{w}_{j,\sigma} \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\Delta \leftarrow \mathbb{Z}_p$ and the two oracles work as follows:

- $\mathsf{OEnc}(x^*)$*: output* $\{\mathbf{w}_{\eta,x^*_\eta}\}_{\eta\in[\ell]}$*;*

- $\mathsf{OKey}(\Gamma)$*: output* $\boxed{\mathsf{sk}_\Gamma[2]}$ *if* $b=0$*; output* $\mathsf{sk}^*_\Gamma[2]$ *using* Δ *in* aux *if* $b=1$*;*

with the restrictions that (1) $\mathcal{A}$ *makes only one query to each oracle; (2) queries* Γ *and* x^* *satisfy* $\Gamma(x^*)=0$.

It is direct to see that the core lemma implies $\mathsf{G}_{2.\kappa-1} \approx_c \mathsf{G}_{2.\kappa}$; here aux are used to simulate other $q-1$ keys. (See Appendix G.3 for details.) In the remaining of this section, we will focus on proving the core lemma, which completes the proof of Theorem 4. For this purpose, we employ the piecewise guessing framework along with a series of hybrids, defined by H^u and h-functions, analogous to Section 6.3. We begin with more auxiliary distributions.

More auxiliary distributions. Recall that the query to OKey is $\mathcal{E}_Q$-restricted. For all $i \in [\ell_{\mathrm{BP}}]$ and $\mathbf{p} \in \mathcal{E}_Q$, we define:

- $\mathsf{sk}^0_{\Gamma,\mathbf{p}}[2]$ is the same as $\mathsf{sk}_\Gamma[2]$ except we replace $\mathbf{d}_0$ with $\mathbf{d}_0 + \Delta\cdot\mathbf{p}$ in the term $[\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2$;
- $\mathsf{sk}^i_{\Gamma,\mathbf{p}}[2]$ is the same as $\mathsf{sk}_\Gamma[2]$ except we replace $\mathbf{d}_i$ with $\mathbf{d}_i + \Delta\cdot\mathbf{p}$ in the term $[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2$ for all $\sigma\in\Sigma$;
- $\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{p}}[2]$ is the same as $\mathsf{sk}_\Gamma[2]$ except we replace $-\mathbf{d}_{i-1}$ with $-\mathbf{d}_{i-1}+\Delta\cdot\mathbf{p}$ in the term $[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2$ for all $\sigma\in\Sigma$;

That is, we have:

$$\mathsf{sk}^0_{\Gamma,\mathbf{p}}[2] = \begin{pmatrix} [(\mathbf{d}_0 + \boxed{\Delta\cdot\mathbf{p}})\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2,\ [\mathbf{R}_j]_2\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}$$

$$\mathsf{sk}^i_{\Gamma,\mathbf{p}}[2] = \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \{[(\mathbf{d}_i + \boxed{\Delta\cdot\mathbf{p}})\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\}_{\sigma\in\Sigma} \\ \{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}$$

$$\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{p}}[2] = \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \boxed{\Delta\cdot\mathbf{p}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2,\ [\mathbf{R}_i]_2\}_{\sigma\in\Sigma} \\ \{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}.$$

The auxiliary distributions here are analogous to those in Section 6.3 except that we use general $\mathbf{p}$ in the place of $\mathbf{f}_{i,x^*}$. Note that this corresponds to the piecewise information we need to guess in the proof.

Hybrids $\{\mathsf{H}^u\}_u$ and h-functions. We are ready to define $\{\mathsf{H}^u\}_u$ and h-functions in the adaptive security lemma (Lemma 20).

Defining u and H^u. For our setting, we require u to determine the forms of key (output by OKey) in a hybrid, this includes the superscript of key and piecewise information $\mathbf{p}$. For this purpose, we define

$$u \in I \times \mathcal{E}_Q$$

where

$$I = \{0,1,\ldots,\ell_{\mathrm{BP}},*\} \cup \{(0,1),(1,2)\ldots,(\ell_{\mathrm{BP}}-1,\ell_{\mathrm{BP}})\}$$

is the set of superscripts of auxiliary keys and $\mathcal{E}_Q$ includes all possibilities of $\mathbf{p}$. Again, we allow a special symbol "$\perp$" at any positions indicating an empty output. Then, for all $u = (\mathsf{s},\mathbf{p}) \in I\times\mathcal{E}_Q$, we define hybrid $\mathsf{H}^{\mathsf{s},\mathbf{p}}$ to be identical to H_0 (or H_1) except that

- oracle $\mathsf{OKey}(\Gamma)$ returns $\mathsf{sk}^{\mathsf{s}}_{\Gamma,\mathsf{yyy}}[2]$ with yyy depending on s or $\mathsf{sk}_\Gamma[2]$ when $\mathsf{s}=\perp$.

Defining h-functions. In both H_0 and H_1, the adversary $\mathcal{A}$ adaptively chooses Γ and x^*, therefore we employ a family of functions

$$h_{\mathsf{xxx}} : \mathrm{NBP}^{\oplus p} \times \Sigma^* \to I \times \mathcal{E}_Q$$

with the first input being $\mathcal{E}_Q$-restricted. Recall that, for x^* and a $\mathcal{E}_Q$-restricted $\mathrm{NBP}^{\oplus p}$ Γ of length ℓ_{BP}, we can define $\mathbf{f}_{0,x^*}, \ldots, \mathbf{f}_{\ell_{\mathrm{BP}},x^*} \in \mathcal{E}_Q$ as (39) as in Section 6.3. We define h-functions as below which describes a series of hybrids analogous to that for selective security. We show the corresponding selective game for each function as a remark.

$$\begin{array}{llllll} h_0 & : (\Gamma, x^*) \longmapsto (\bot, & \bot &); & & // \ \mathsf{G}_1 \\ h_{1.i.0} & : (\Gamma, x^*) \longmapsto (\{i-1\}, & \mathbf{f}_{i-1,x^*} &); & \forall\, i \in [\ell_{\mathrm{BP}}]; & // \ \mathsf{G}_{2.i.0} \\ h_{1.i.1} & : (\Gamma, x^*) \longmapsto (\{i-1, i\}, & \mathbf{f}_{i-1,x^*} &); & \forall\, i \in [\ell_{\mathrm{BP}}]; & // \ \mathsf{G}_{2.i.1} \\ h_{1.i.2} & : (\Gamma, x^*) \longmapsto (\{i\}, & \mathbf{f}_{i,x^*} &); & \forall\, i \in [\ell_{\mathrm{BP}}]; & // \ \mathsf{G}_{2.i.2} \\ h_2 & : (\Gamma, x^*) \longmapsto (\{*\}, & \bot &); & & // \ \mathsf{G}_3 \end{array}$$

Note that we have $h_{1.i.0} = h_{1.i-1.2}$ for all $i \in [2, \ell_{\mathrm{BP}}]$ and sk^*_Γ is shown in Section 6.3.

Proving the core lemma. As in Section 5.4, we check (1) end-point equivalence and (2) neighbor indistinguishability.

End-point equivalence. It is clear that our hybrids $\{\mathsf{H}^u\}_u$ and h-functions satisfy the end-point equivalence. This follows from the fact that h_0 and h_2 are constant functions which indicate the same types of keys as in H^0 and H^1, respectively. Formally, we give the following lemma.

Lemma 31 (End-point equivalence). *For all $(\Gamma, x^*) \in I \times \mathcal{E}_Q$, we have*

$$\mathsf{H}^{h_0(\Gamma,x^*)} = \mathsf{H}_0 \quad \textit{and} \quad \mathsf{H}^{h_2(\Gamma,x^*)} = \mathsf{H}_1.$$

Neighbor indistinguishability. We first define several pairs of hybrids with $b \in \{0,1\}$:

- $\widehat{\mathsf{H}}^b_0(u_0, u_1)$ is the same as H^{u_b} except that we output 0 whenever

$$(h_0(\Gamma, x^*), h_{1.1.0}(\Gamma, x^*)) \neq (u_0, u_1).$$

- $\widehat{\mathsf{H}}^b_{1.i.i'}(u_0, u_1)$, for $i \in [\ell_{\mathrm{BP}}]$ and $i' \in [2]$, is the same as H^{u_b} except that we output 0 whenever

$$(h_{1.i.i'-1}(\Gamma, x^*), h_{1.i,i'}(\Gamma, x^*)) \neq (u_0, u_1).$$

- $\widehat{\mathsf{H}}^b_2(u_0, u_1)$ is the same as H^{u_b} except that we output 0 whenever

$$(h_{1.\ell_{\mathrm{BP}}.2}(\Gamma, x^*), h_2(\Gamma, x^*)) \neq (u_0, u_1).$$

and claim that each pair of hybrids are indistinguishable for all $u_0, u_1 \in I \times \mathcal{E}_Q$. Formally, we have the following lemma. The proof essentially follows those in Section 6.3. (See Appendix G.4 for more details.)

Lemma 32 (Neighbor indistinguishability). *For all* $\mathsf{xxx} \in \{0,2\} \cup \{1.i.i' : i \in [\ell_{BP}], i' \in [2]\}$*,* $u_0, u_1 \in I \times \mathcal{E}_Q$ *and all* $\mathcal{A}$*, there exists* $\mathcal{B}$ *with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_{\mathsf{xxx}}(u_0, u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{\mathsf{xxx}}(u_0, u_1)\rangle = 1] \le O(|\Sigma|^2) \cdot \mathsf{Adv}^{k\text{-}\mathrm{LIN}}_{\mathcal{B}}(\lambda).$$

Summary. By the adaptive security lemma (Lemma 20), we have that Lemma 31 and Lemma 32 imply the core lemma, Lemma 30, with the following two facts:

- all our h-functions have range of size at most $O(Q)$ since the first output is constant and $|\mathcal{E}_Q| = Q$; that is, we have $R' = O(\log Q)$;
- our proof employs $O(\ell_{\mathrm{BP}})$ h-functions; that is we have $L = O(\ell_{\mathrm{BP}})$.

Acknowledgments. We thank Brent Waters for insightful discussions on adaptive security, as well as the anonymous reviewers for constructive feedback on our write-up.

References

1. S. Agrawal and M. Chase. Simplifying design and analysis of complex predicate encryption schemes. In J. Coron and J. B. Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 627–656. Springer, Heidelberg, Apr. / May 2017.
2. S. Agrawal, M. Maitra, and S. Yamada. Attribute based encryption (and more) for nondeterministic finite automata from LWE. In A. Boldyreva and D. Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 765–797. Springer, Heidelberg, Aug. 2019.
3. S. Agrawal, M. Maitra, and S. Yamada. Attribute based encryption for deterministic finite automata from DLIN. In *TCC*, 2019.
4. N. Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 557–577. Springer, Heidelberg, May 2014.
5. N. Attrapadung. Dual system encryption framework in prime-order groups via computational pair encodings. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 591–623. Springer, Heidelberg, Dec. 2016.
6. N. Attrapadung and S. Yamada. Duality in ABE: Converting attribute based encryption for dual predicate and dual policy via computational encodings. In K. Nyberg, editor, *CT-RSA 2015*, volume 9048 of *LNCS*, pages 87–105. Springer, Heidelberg, Apr. 2015.
7. J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Heidelberg, Apr. 2015.
8. J. Chen, J. Gong, L. Kowalczyk, and H. Wee. Unbounded ABE via bilinear entropy expansion, revisited. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 503–534. Springer, Heidelberg, Apr. / May 2018.
9. J. Chen and H. Wee. Semi-adaptive attribute-based encryption and improved delegation for Boolean formula. In M. Abdalla and R. D. Prisco, editors, *SCN 14*, volume 8642 of *LNCS*, pages 277–297. Springer, Heidelberg, Sept. 2014.
10. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, Aug. 2013.
11. J. Gong, B. Waters, and H. Wee. ABE for DFA from k-lin. In A. Boldyreva and D. Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 732–764. Springer, Heidelberg, Aug. 2019.
12. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. Vimercati, editors, *ACM CCS 06*, pages 89–98. ACM Press, Oct. / Nov. 2006. Available as Cryptology ePrint Archive Report 2006/309.
13. D. Hofheinz, J. Koch, and C. Striecks. Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 799–822. Springer, Heidelberg, Mar. / Apr. 2015.
14. Z. Jafargholi, C. Kamath, K. Klein, I. Komargodski, K. Pietrzak, and D. Wichs. Be adaptive, avoid overcommitting. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 133–163. Springer, Heidelberg, Aug. 2017.
15. L. Kowalczyk and H. Wee. Compact adaptively secure ABE for $\mathsf{NC}s^1$ from k-lin. In V. Rijmen and Y. Ishai, editors, *EUROCRYPT 2019, Part I*, LNCS, pages 3–33. Springer, Heidelberg, May 2019.
16. A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In D. Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 455–479. Springer, Heidelberg, Feb. 2010.
17. A. B. Lewko and B. Waters. Unbounded HIBE and attribute-based encryption. In K. G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 547–567. Springer, Heidelberg, May 2011.
18. T. Okamoto and K. Takashima. Fully secure unbounded inner-product and attribute-based encryption. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 349–366. Springer, Heidelberg, Dec. 2012.
19. A. Sahai and B. R. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Heidelberg, May 2005.
20. B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, Heidelberg, Aug. 2009.
21. B. Waters. Functional encryption for regular languages. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 218–235. Springer, Heidelberg, Aug. 2012.
22. H. Wee. Dual system encryption via predicate encodings. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer, Heidelberg, Feb. 2014.

Appendix

A An Example for Back-tracking Attack

We assume an (asymmetric) bilinear group $\mathbb{G} = (p, G_1, G_2, G_T, e)$ of prime order p and use $[\cdot]_1, [\cdot]_2, [\cdot]_T$ to denote component-wise exponentiations in respective groups G_1, G_2, G_T [10]. The natural NFA extension of Waters' ABE for DFA [21] mentioned in Section 1.1 can be formally described as follows:

$$\begin{aligned}
\mathsf{msk} &= \big(w_{\mathrm{start}}, w_{\mathrm{end}}, z, \{w_\sigma\}_{\sigma\in\Sigma}, \alpha\big) \\
\mathsf{mpk} &= \big([w_{\mathrm{start}}]_1, [w_{\mathrm{end}}]_1, [z]_1, \big\{[w_\sigma]_1\big\}_{\sigma\in\Sigma}, [\alpha]_T\big) \\
\mathsf{ct}_x &= \begin{pmatrix} [s_0]_1,\ [s_0 w_{\mathrm{start}}]_1 \\ \big\{[s_j]_1,\ [s_{j-1}z + s_j w_{x_j}]_1\big\}_{j\in[\ell]} \\ [s_\ell]_1,\ [s_\ell w_{\mathrm{end}}]_1,\ [s_\ell \alpha]_T \cdot m \end{pmatrix} \\
\mathsf{sk}_\Gamma &= \begin{pmatrix} \big\{[d_u + w_{\mathrm{start}} r_{\mathrm{start},u}]_2,\ [r_{\mathrm{start},u}]_2\big\}_{u\in S} \\ \big\{[-d_u + z r_{u,\sigma,v}]_2,\ [d_v + w_\sigma r_{u,\sigma,v}]_2,\ [r_{u,\sigma,v}]_2\big\}_{u\in[Q],\sigma\in\Sigma,v\in\delta(u,\sigma)} \\ \big\{[\alpha - d_u + w_{\mathrm{end}} r_{\mathrm{end},u}]_2,\ [r_{\mathrm{end},u}]_2\big\}_{u\in F} \end{pmatrix}
\end{aligned} \tag{40}$$

where Σ is the alphabet, $S, F \subseteq [Q]$ are the sets of start states and accept states, respectively, and $\delta : [Q] \times \Sigma \to 2^{[Q]}$ is the NFA transition function. Clearly, as (2) in Section 1.1, ct_x and sk_Γ allow us to compute quantities:

$$[s_j d_v - s_{j-1} d_u]_T,\ \forall\, j \in [\ell], u \in [Q], v \in \delta(u, x_j) \subseteq [Q]. \tag{41}$$

We illustrate the back-tracking attack against (40) by an example. Consider a concrete NFA Γ defined by $Q = 4, \Sigma = \{0\}, S = \{1\}, F = \{4\}$ and δ describing two nondeterministic transitions: $1 \xmapsto{0} \{1,2\}$ and $3 \xmapsto{0} \{2,4\}$, whose key will be

$$\mathsf{sk}_\Gamma = \begin{pmatrix} [d_1 + w_{\mathrm{start}} r_0]_2,\ [r_0]_2 \\ [-d_1 + z r_1]_2,\ [d_1 + w r_1]_2,\ [r_1]_2 \\ [-d_1 + z r_2]_2,\ [d_2 + w r_2]_2,\ [r_2]_2 \\ [-d_3 + z r_3]_2,\ [d_2 + w r_3]_2,\ [r_3]_2 \\ [-d_3 + z r_4]_2,\ [d_4 + w r_4]_2,\ [r_4]_2 \\ [\alpha - d_4 + w_{\mathrm{end}} r]_2,\ [r]_2 \end{pmatrix}$$

and input x being a single 0, whose ciphertext will be

$$\mathsf{ct}_x = \begin{pmatrix} [s_0]_1,\ [s_0 w_{\mathrm{start}}]_1 \\ [s_1]_1,\ [s_0 z + s_1 w]_1 \\ [s_1]_1,\ [s_1 w_{\mathrm{end}}]_1,\ [s_1 \alpha]_T \cdot m \end{pmatrix}$$

Clearly, since the NFA Γ does not accept $x = 0$, the key sk_Γ is not supposed to decrypt the ciphertext ct_x. However this is not the case for (40). Following (41), we can recover the following quantities:

$$D_0 = [s_0 d_1]_T,\ D_1 = [s_1 d_2 - s_0 d_1]_T,\ D_2 = [s_1 d_2 - s_0 d_3]_T,\ D_3 = [s_1 d_4 - s_0 d_3]_T,\ D_4 = [s_1 \alpha - s_1 d_4]_T$$

and compute the masking value:

$$[s_1 \alpha]_T = D_0 \cdot D_1 \cdot D_2^{-1} \cdot D_3 \cdot D_4.$$

Intuitively, this corresponds to running the NFA normally with transition $1 \xmapsto{0} 2$, and back-tracking along the transition $3 \xmapsto{0} 2$, which allows us to restart from state 3 and finally reaching the accept state 4 by transition $3 \xmapsto{0} 4$.

B Basic ABE for NFA$^{\oplus p}$ from ℓ-EBDHE assumption

In this section, we describe our basic ABE scheme for NFA$^{\oplus p}$ from (asymmetric) bilinear group $\mathbb{G} = (p, G_1, G_2, G_T, e)$ of prime order p. We assume that respective generators for every groups are described in $\mathbb{G}$ and use $[\cdot]_1, [\cdot]_2, [\cdot]_T$ to denote component-wise exponentiations in the prime-order groups G_1, G_2, G_T [10]. The scheme is selectively secure under ℓ-EBDHE assumption (in the asymmetric prime-order bilinear groups). The proof is an extension of Waters' proof for the ABE for DFA in [21] based on the same assumption. We review the ℓ-EBDHE assumption [21] in the asymmetric bilinear group of prime order.

Assumption 2 (ℓ-EBDHE assumption) *We say that the ℓ-EBDHE assumption holds if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\ell\text{-EBDHE}}(\lambda) := \big|\Pr[\mathcal{A}(\mathbb{G},[D]_1,[D]_2,[t_0]_T)=1] - \Pr[\mathcal{A}(\mathbb{G},[D]_1,[D]_2,[t_1]_T)=1]\big|$$

where $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$ *and*

$$D = \begin{pmatrix} a,\, b,\, ab/d,\, b/d & \\ a^i s,\, a^i bs/c_j & \forall i \in [0, 2\ell+1] \setminus \{\ell+1\}, j \in [0, \ell+1] \\ a^i b/c_i,\, c_i,\, a^i d,\, abc_i/d,\, bc_i/d & \forall i \in [0, \ell+1] \\ a^i bd/c_j & \forall i \in [0, 2\ell+1], j \in [0, \ell+1] \\ a^i bc_j/c_i & \forall i, j \in [0, \ell+1], i \neq j \end{pmatrix} \quad \text{and} \quad t_0 = a^{\ell+1} bs,\ t_1 \leftarrow \mathbb{Z}_p$$

with $a, b, c_0, \ldots, c_\ell, d, s \leftarrow \mathbb{Z}_p$.

Scheme. Our basic ABE for NFA$^{\oplus p}$ in the asymmetric bilinear groups is as follows:

- $\mathsf{Setup}(1^\lambda, \Sigma)$: Run $\mathbb{G} = (p, G_1, G_2,, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

$$\alpha, w_{\text{start}}, w_{\text{end}}, z, w_\sigma \leftarrow \mathbb{Z}_p,\ \forall \sigma \in \Sigma.$$

  Output

$$\begin{aligned} \mathsf{mpk} &= \big([w_{\text{start}}]_1, [w_{\text{end}}]_1, [z]_1, \{[w_\sigma]_1\}_{\sigma\in\Sigma}, [\alpha]_T\big) \\ \mathsf{msk} &= \big(w_{\text{start}}, w_{\text{end}}, z, \{w_\sigma\}_{\sigma\in\Sigma}, \alpha\big). \end{aligned}$$

- $\mathsf{Enc}(\mathsf{mpk}, x, m)$: Let $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$ and $m \in G_T$. Pick $s_0, s_1, \ldots, s_\ell \leftarrow \mathbb{Z}_p$ and output

$$\mathsf{ct}_x = \begin{pmatrix} [s_0]_1,\, [s_0 w_{\text{start}}]_1 \\ \big\{[s_j]_1,\, [s_{j-1}z + s_j w_{x_j}]_1\big\}_{j\in[\ell]} \\ [s_\ell]_1,\, [s_\ell w_{\text{end}}]_1,\, [s_\ell \alpha]_T \cdot m \end{pmatrix}.$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$: Let $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$. Pick $\mathbf{d} \leftarrow \mathbb{Z}_p^{1\times Q}$, $r_{\text{start}} \leftarrow \mathbb{Z}_p$, $\mathbf{r}_\sigma, \mathbf{r}_{\text{end}} \leftarrow \mathbb{Z}_p^{1\times Q}$ for all $\sigma \in \Sigma$ and output

$$\mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + w_{\text{start}} r_{\text{start}}]_2,\, [r_{\text{start}}]_2 \\ \big\{[-\mathbf{d} + z\mathbf{r}_\sigma]_2,\, [\mathbf{d}\mathbf{M}_\sigma + w_\sigma \mathbf{r}_\sigma]_2,\, [\mathbf{r}_\sigma]_2\big\}_{\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d} + w_{\text{end}}\mathbf{r}_{\text{end}}]_2,\, [\mathbf{r}_{\text{end}}]_2 \end{pmatrix}.$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_x)$: Parse ciphertext for $x = (x_1, \ldots, x_\ell)$ and key for $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ as

$$\mathsf{ct}_x = \begin{pmatrix} [s_0]_1, [c_0]_1 \\ \big\{[s_j]_1, [c_j]_1\big\}_j \\ [s_\ell]_1, [c_{\text{end}}]_1, C \end{pmatrix} \quad \text{and} \quad \mathsf{sk}_\Gamma = \begin{pmatrix} [k_{\text{start}}]_2, [r_{\text{start}}]_2 \\ \big\{[\mathbf{k}_{\sigma,1}]_2, [\mathbf{k}_{\sigma,2}]_2, [\mathbf{r}_\sigma]_2\big\}_\sigma \\ [\mathbf{k}_{\text{end}}]_2, [\mathbf{r}_{\text{end}}]_2 \end{pmatrix}$$

  We define

$$\mathbf{u}_{j,x}^\top = \mathbf{M}_{x_j} \cdots \mathbf{M}_{x_1} \mathbf{u}^\top \bmod p,\ \forall j \in [\ell]$$

  as (11) and proceed as follows:

1. Compute
$$B_0 = e([s_0]_1, [k_{\mathsf{start}}]_2) \cdot e([c_0]_1, [r_{\mathsf{start}}]_2)^{-1};$$
2. For all $j \in [\ell]$, compute
$$[\mathbf{b}_j]_T = e([s_{j-1}]_1, [\mathbf{k}_{x_j,1}]_2) \cdot e([s_j]_1, [\mathbf{k}_{x_j,2}]_2) \cdot e([-c_j]_1, [\mathbf{r}_{x_j}]_2) \quad \text{and} \quad B_j = [\mathbf{b}_j \mathbf{u}_{j-1,x}^{\top}]_T$$
3. Compute
$$[\mathbf{b}_{\mathsf{end}}]_T = e([s_\ell]_1, [\mathbf{k}_{\mathsf{end}}]_2) \cdot e([-c_{\mathsf{end}}]_1, [\mathbf{r}_{\mathsf{end}}]_2) \quad \text{and} \quad B_{\mathsf{end}} = [\mathbf{b}_{\mathsf{end}} \mathbf{u}_{\ell,x}^{\top}]_T$$
4. Compute
$$B_{\mathsf{all}} = B_0 \cdot \textstyle\prod_{j=1}^{\ell} B_j \cdot B_{\mathsf{end}} \quad \text{and} \quad B = B_{\mathsf{all}}^{(\mathbf{f}\mathbf{u}_{\ell,x}^{\top})^{-1}}$$
and output the message $m' \leftarrow C \cdot B^{-1}$.

The correctness is direct.

Selective security. We prove the following theorem.

Theorem 5. *The above ABE scheme for NFA$^{\oplus p}$ in the asymmetric bilinear groups of prime order p is selectively secure under the ℓ-EBDHE assumption (cf. Assumption 2). Here ℓ is the length of the challenge input x^*.*

Proof. Let x^* be the selective challenge input of length ℓ, we use ℓ-EBDHE assumption. For convenience, we artificially set $x_0^* = x_{\ell+1}^* = \perp \notin \Sigma$. On input $(\mathbb{G}, [D]_1, [D]_2, [t]_T)$ where either $t = a^{\ell+1}bs$ or $t \leftarrow \mathbb{Z}_p$, the reduction works as follows:

(Simulating mpk) We sample $\tilde{w}_{\mathsf{start}}, \tilde{w}_{\mathsf{end}}, \tilde{z}, \tilde{w}_\sigma \leftarrow \mathbb{Z}_p$ for all $\sigma \in \Sigma$ and implicitly set
$$\alpha = ab, \quad w_{\mathsf{start}} = \tilde{w}_{\mathsf{start}} - \sum_{i \in [\ell]} a^{\ell+1-i} b / c_{\ell+1-i}, \quad w_{\mathsf{end}} = \tilde{w}_{\mathsf{end}} - \sum_{i \in [0,\ell-1]} a^{\ell+1-i} b / c_{\ell+1-i}$$
$$z = \tilde{z} + ab/d, \quad w_\sigma = \tilde{w}_\sigma - b/d - \sum_{i \in [0,\ell+1], \sigma \neq x_i^*} a^{\ell+1-i} b / c_{\ell+1-i}, \; \forall \sigma \in \Sigma$$
Then terms in mpk can be simulated using $[a, b, ab/d, b/d, \{a^i b / c_i\}_{i \in [0,\ell+1]}]_1$ provided in $[D]_1$.

(Simulating challenge ciphertext) On input (m_0, m_1), we sample $\tilde{s}_0, \ldots, \tilde{s}_\ell \leftarrow \mathbb{Z}_p$, $\beta \leftarrow \{0,1\}$ and implicitly set
$$s_i = \tilde{s}_\ell + a^i s, \; \forall i \in [0,\ell]$$
and want to simulate a challenge ciphertext in the following form:
$$\begin{pmatrix} [s_0]_1, \; [s_0 w_{\mathsf{start}}]_1 \\ \big\{ [s_i]_1, \; [s_{i-1} z + s_i w_{x_i}]_1 \big\}_{i \in [\ell]} \\ [s_\ell]_1, \; [s_\ell w_{\mathsf{end}}]_1, \; [t]_T \cdot e([a]_1, [b]_2)^{\tilde{s}_\ell} \cdot m_\beta \end{pmatrix}$$
Observe that, when $t = a^{\ell+1} bs$, the ciphertext is identical to the real one; when $t \leftarrow \mathbb{Z}_p$, the ciphertext perfectly hides β. We proceed to simulate each term in the challenge ciphertext as below:

- We can simulate $[s_i]_1 = [\tilde{s}_i]_1 \cdot [a^i s]_1$ for all $i \in [0,\ell]$ using $\{[a^i s]_1\}_{i \in [0,\ell]}$ from $[D]_1$.
- We can simulate $[s_0 w_{\mathsf{start}}]_1$ where
$$s_0 w_{\mathsf{start}} = (\tilde{s}_0 + s) \cdot \Big(\tilde{w}_{\mathsf{start}} - \sum_{i \in [\ell]} a^{\ell+1-i} b / c_{\ell+1-i} \Big),$$
using $[s, \{a^i b / c_i, a^i bs / c_i\}_{i \in [\ell]}]_1$ in $[D]_1$.

- We can simulate $[s_\ell w_{\mathrm{end}}]_1$ where

$$s_\ell w_{\mathrm{end}} = (\tilde{s} + a^\ell s) \cdot \Big(\tilde{w}_{\mathrm{end}} - \sum_{i \in [0,\ell-1]} a^{\ell+1-i} b / c_{\ell+1-i}\Big)$$

  using $[a^\ell s, \{a^i b/c_i, a^{\ell+i} bs/c_i\}_{i \in [2,\ell+1]}]_1$ in $[D]_1$.
- For all $j \in [\ell]$, we can simulate $[s_{j-1} z + s_j w_{x_j^*}]_1$ where

$$s_{j-1} z + s_j w_{x_j^*} = (\tilde{s}_{j-1} + a^{j-1} s) \cdot (\tilde{z} + ab/d) + (\tilde{s}_j + a^j s) \cdot \Big(\tilde{w}_\sigma - b/d - \sum_{i \in [0,\ell+1], x_j^* \neq x_i^*} a^{\ell+1-i} b / c_{\ell+1-i}\Big)$$

  using $[a^{j-1} s, a^j s, b/d, \{a^i b/c_i, a^{i+j} bs/c_i\}_{i \in [0,\ell+1], i+j \neq \ell+1}]_1$ from $[D]_1$. This follows from $a^{j-1} s \cdot ab/d - a^j s \cdot b/d = 0$.

(Simulating secret key) On input Γ, we compute $\{\mathbf{f}_{i,x^*}\}_{i \in [0,\ell]}$ as in Section 1.2 (also see (22) in Section 4.3) and artificially set $\mathbf{f}_{-1,x^*} = \mathbf{f}_{\ell+1,x^*} = \mathbf{0}$. We sample $\tilde{\mathbf{d}}, \tilde{\mathbf{r}}_\sigma, \tilde{\mathbf{r}}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1 \times Q}$, $\tilde{r}_{\mathrm{start}} \leftarrow \mathbb{Z}_p$ for all $\sigma \in \Sigma$ and implicitly set

$$\begin{aligned}
\mathbf{d} &= \tilde{\mathbf{d}} + \sum_{i \in [0,\ell]} a^{\ell+1-i} b \cdot \mathbf{f}_{i,x^*} \\
r_{\mathrm{start}} &= \tilde{r}_{\mathrm{start}} + \sum_{i \in [\ell]} c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*} \mathbf{u}^\top \\
\mathbf{r}_\sigma &= \tilde{\mathbf{r}}_\sigma + \sum_{i \in [0,\ell]} a^{\ell-i} d \cdot \mathbf{f}_{i,x^*} + \sum_{i \in [0,\ell+1]} c_{\ell+1-i} \cdot (\mathbf{f}_{i,x^*} \mathbf{M}_\sigma - \mathbf{f}_{i-1,x^*}),\ \forall \sigma \in \Sigma \\
\mathbf{r}_{\mathrm{end}} &= \tilde{\mathbf{r}}_{\mathrm{end}} + \sum_{i \in [0,\ell-1]} c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*}
\end{aligned}$$

We proceed to simulate each term in the secret key as below:

- We can simulate $[r_{\mathrm{start}}]_2$, $[\mathbf{r}_\sigma]_2$, $[\mathbf{r}_{\mathrm{end}}]_2$ from $[\{c_i\}_{i \in [0,\ell+1]}, \{a^i d\}_{i \in [0,\ell]}]_2$ provided in $[D]_2$.
- We can simulate $[\mathbf{d}\mathbf{u}^\top + w_{\mathrm{start}} r_{\mathrm{start}}]_2$ where

$$\mathbf{d}\mathbf{u}^\top + w_{\mathrm{start}} r_{\mathrm{start}} = \Big(\tilde{\mathbf{d}} + \sum_{i \in [0,\ell]} a^{\ell+1-i} b \cdot \mathbf{f}_{i,x^*} \mathbf{u}^\top\Big) + \Big(\tilde{w}_{\mathrm{start}} - \sum_{i \in [\ell]} a^{\ell+1-i} b / c_{\ell+1-i}\Big) \cdot \Big(\tilde{r}_{\mathrm{start}} + \sum_{i \in [\ell]} c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*} \mathbf{u}^\top\Big)$$

  using $[\{c_i\}_{i \in [\ell]}, \{a^i b/c_i\}_{i \in [\ell]}, \{a^i b c_j / c_i\}_{i,j \in [\ell], i \neq j}]_2$ from $[D]_2$. This follows from

$$\begin{aligned}
&\sum_{i \in [0,\ell]} a^{\ell+1-i} b \cdot \mathbf{f}_{i,x^*} \mathbf{u}^\top - \sum_{i \in [\ell]} a^{\ell+1-i} b / c_{\ell+1-i} \cdot \sum_{i \in [\ell]} c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*} \mathbf{u}^\top \\
= &\sum_{i \in [\ell]} a^{\ell+1-i} b \cdot \mathbf{f}_{i,x^*} \mathbf{u}^\top - \sum_{i \in [\ell]} a^{\ell+1-i} b / c_{\ell+1-i} \cdot \sum_{i \in [\ell]} c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*} \mathbf{u}^\top \\
= -&\sum_{i,j \in [\ell], i \neq j} a^{\ell+1-i} b c_{\ell+1-j} / c_{\ell+1-i} \mathbf{f}_{j,x^*} \mathbf{u}^\top
\end{aligned}$$

  in which all terms of the form $a^i b$ are canceled out. Here the first equality uses the fact that $\mathbf{f}_{0,x^*} \mathbf{u}^\top = 0 \bmod p$.
- We can simulate $[\alpha \mathbf{f} - \mathbf{d} + w_{\mathrm{end}} \mathbf{r}_{\mathrm{end}}]_2$ where

$$\alpha \mathbf{f} - \mathbf{d} + w_{\mathrm{end}} \mathbf{r}_{\mathrm{end}} = ab \cdot \mathbf{f} - \Big(\tilde{\mathbf{d}} + \sum_{i \in [0,\ell]} a^{\ell+1-i} b \cdot \mathbf{f}_{i,x^*}\Big) + \Big(\tilde{w}_{\mathrm{end}} - \sum_{i \in [0,\ell-1]} a^{\ell+1-i} b / c_{\ell+1-i}\Big) \cdot \Big(\tilde{\mathbf{r}}_{\mathrm{end}} + \sum_{i \in [0,\ell-1]} c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*}\Big)$$

  using $[\{c_i\}_{i \in [2,\ell+1]}, \{a^i b / c_i\}_{i \in [2,\ell+1]}, \{a^i b c_j / c_i\}_{i,j \in [2,\ell+1], i \neq j}]_2$ from $[D]_2$. This follows form

$$\begin{aligned}
&ab \cdot \mathbf{f} - \sum_{i \in [0,\ell]} a^{\ell+1-i} b \cdot \mathbf{f}_{i,x^*} - \sum_{i \in [0,\ell-1]} a^{\ell+1-i} b / c_{\ell+1-i} \cdot \sum_{i \in [0,\ell-1]} c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*} \\
= -&\sum_{i \in [0,\ell-1]} a^{\ell+1-i} b \cdot \mathbf{f}_{i,x^*} - \sum_{i \in [0,\ell-1]} a^{\ell+1-i} b / c_{\ell+1-i} \cdot \sum_{i \in [0,\ell-1]} c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*} \\
= -&\sum_{i,j \in [0,\ell-1], i \neq j} a^{\ell+1-i} b c_{\ell+1-j} / c_{\ell+1-i} \cdot \mathbf{f}_{i,x^*}
\end{aligned}$$

  in which all terms of the form $a^i b$ are canceled out. Here the first equality utilizes the definition $\mathbf{f}_{\ell,x^*} = \mathbf{f}$.

- For all σ, we can simulate $[-\mathbf{d}+z\mathbf{r}_\sigma]_2$ where

$$-\mathbf{d}+z\mathbf{r}_\sigma = -\Big(\tilde{\mathbf{d}} + \sum_{i\in[0,\ell]} a^{\ell+1-i} b\cdot \mathbf{f}_{i,x^*}\Big) + (\tilde{z}+ab/d)\cdot\Big(\tilde{\mathbf{r}}_\sigma + \sum_{i\in[0,\ell]} a^{\ell-i} d\cdot\mathbf{f}_{i,x^*} + \sum_{i\in[0,\ell+1]} c_{\ell+1-i}\cdot(\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - \mathbf{f}_{i-1,x^*})\Big)$$

  using $[ab/d, \{a^i d\}_{i\in[0,\ell]}, \{c_i\}_{i\in[0,\ell+1]}, \{abc_i/d\}_{i\in[0,\ell+1]}]_2$ from $[D_2]$. This follows from

$$-\sum_{i\in[0,\ell]} a^{\ell+1-i} b\cdot\mathbf{f}_{i,x^*} + ab/d\cdot\sum_{i\in[0,\ell]} a^{\ell-i} d\cdot\mathbf{f}_{i,x^*} = -\sum_{i\in[0,\ell]} a^{\ell+1-i} b\cdot\mathbf{f}_{i,x^*} + \sum_{i\in[0,\ell]} a^{\ell+1-i} b\cdot\mathbf{f}_{i,x^*} = \mathbf{0}.$$

- For all σ, we can simulate $[\mathbf{d}\mathbf{M}_\sigma + w_\sigma\mathbf{r}_\sigma]_2$ where

$$\begin{aligned}
&\mathbf{d}\mathbf{M}_\sigma + w_\sigma\mathbf{r}_\sigma\\
=&\Big(\tilde{\mathbf{d}} + \sum_{i\in[0,\ell]} a^{\ell+1-i} b\cdot\mathbf{f}_{i,x^*}\mathbf{M}_\sigma\Big)\\
&+\Big(\tilde{w}_\sigma - b/d - \sum_{i\in[0,\ell+1],\sigma\neq x_i^*} a^{\ell+1-i} b/c_{\ell+1-i}\Big)\cdot\Big(\tilde{\mathbf{r}}_\sigma + \sum_{i\in[0,\ell]} a^{\ell-i} d\cdot\mathbf{f}_{i,x^*} + \sum_{i\in[0,\ell+1]} c_{\ell+1-i}\cdot(\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - \mathbf{f}_{i-1,x^*})\Big)
\end{aligned}$$

  using $[b/d, \{a^i d\}_{i\in[0,\ell]}, \{c_i\}_{i\in[0,\ell+1]}, \{bc_i/d\}_{i\in[0,\ell+1]}, \{a^{i+j-1} bd/c_i\}_{i,j\in[\ell+1]}]_2$ and $\{a^i bc_j/c_i\}_{i,j\in[0,\ell+1],i\neq j}]_2$ from $[D]_2$. This follows from

$$\begin{aligned}
&\sum_{i\in[0,\ell]} a^{\ell+1-i} b\cdot\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - b/d\cdot\sum_{i\in[0,\ell]} a^{\ell-i} d\cdot\mathbf{f}_{i,x^*} - \sum_{i\in[0,\ell+1],\sigma\neq x_i^*} a^{\ell+1-i} b/c_{\ell+1-i}\cdot\sum_{i\in[0,\ell+1]} c_{\ell+1-i}\cdot(\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - \mathbf{f}_{i-1,x^*})\\
=&\sum_{i\in[0,\ell]} a^{\ell+1-i} b\cdot\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - \sum_{i\in[1,\ell+1]} a^{\ell+1-i} b\cdot\mathbf{f}_{i-1,x^*} - \sum_{i\in[0,\ell+1],\sigma\neq x_i^*} a^{\ell+1-i} b/c_{\ell+1-i}\cdot\sum_{i\in[0,\ell+1]} c_{\ell+1-i}\cdot(\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - \mathbf{f}_{i-1,x^*})\\
=&\sum_{i\in[0,\ell+1],\sigma\neq x_i^*} a^{\ell+1-i} b\cdot(\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - \mathbf{f}_{i-1,x^*}) - \sum_{i\in[0,\ell+1],\sigma\neq x_i^*} a^{\ell+1-i} b/c_{\ell+1-i}\cdot\sum_{i\in[0,\ell+1]} c_{\ell+1-i}\cdot(\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - \mathbf{f}_{i-1,x^*})\\
=&-\sum_{i,j\in[0,\ell+1],i\neq j,\sigma\neq x_i^*} a^{\ell+1-i} bc_{\ell+1-j}/c_{\ell+1-i}\cdot(\mathbf{f}_{i,x^*}\mathbf{M}_\sigma - \mathbf{f}_{i-1,x^*})
\end{aligned}$$

  in which all terms of the form $a^i b$ are canceled out. Here the second equality utilizes the fact that $\mathbf{f}_{i,x^*}\mathbf{M}_{x_i^*} = \mathbf{f}_{i-1,x^*} \bmod p$, see Lemma 5.

Observe that, when $t = a^{\ell+1} bs$, the simulation is identical to the real game; when $t \leftarrow \mathbb{Z}_p$, the simulation hides β perfectly and adversary's advantage is 0. This readily proves the lemma. □

C An Example for Reversing DFA

In this section, we give an example showing the idea of reversing DFA. Consider the regular language $01\{0,1\}^*$ recognized by DFA Γ with $Q = 3, \Sigma = \{0,1\}, F = \{3\}$ and δ describing transitions:

$$1 \overset{0}{\mapsto} 2, \quad 2 \overset{1}{\mapsto} 3, \quad 3 \overset{0/1}{\mapsto} 3.$$

On input $x = 0100$, the sets U_i of states reachable from start state after reading the first i bits and the sets F_i of states reachable by back-tracking from accept states after reading the last i bits are as follows:

$$U_0 = \{1\}, U_1 = \{2\}, U_2 = \{3\}, U_3 = \{3\}, U_4 = \{3\}$$

$$F_0 = \{3\}, F_1 = \{3\}, F_2 = \{3\}, F_3 = \{2,3\}, F_4 = \{1,3\}$$

Clearly, Γ is *not* $\mathcal{E}_3$-restricted; since $|F_3| > 1$ and $|F_4| > 1$, we cannot use elementary row vectors in $\mathcal{E}_3$ to express them.

The reversed DFA $\Gamma^\top$ is defined by the same Q and Σ but with set of start states $U = \{3\}$, set of accept states $F = \{1\}$ and δ describing transitions:

$$3 \overset{0}{\mapsto} \{3\}, \quad 3 \overset{1}{\mapsto} \{2,3\}, \quad 2 \overset{0}{\mapsto} \{1\}.$$

Here we have a transition $u \overset{\sigma}{\mapsto} v$ whenever there is a transition $v \overset{\sigma}{\mapsto} u$ in the original DFA. For correctness, we also reverse the input as $x^\top = 0010$; note that the original $x = 0100$ will be rejected by $\Gamma^\top$. Then we have

$$U_0 = \{3\}, U_1 = \{3\}, U_2 = \{3\}, U_3 = \{2,3\}, U_4 = \{1,3\}$$

$$F_0 = \{1\}, F_1 = \{2\}, F_2 = \{3\}, F_3 = \{3\}, F_4 = \{3\}$$

One can see that $\Gamma^\top$ is an NFA due to the nondeterministic transition on input bit 1, but now we indeed have $|F_i| = 1$ for all $i = 0,1,2,3,4$ that is desirable for the proof. In fact this holds for all inputs and $\Gamma^\top$ is $\mathcal{E}_3$-restricted (see Section 3 for formal proof). Roughly, by reversing DFA, we exchange the role of U_i and F_i and the $\mathcal{E}_3$-restriction of the reversed DFA immediately comes from the determinism of the original DFA which ensures that $|U_i| = 1$ (for DFA).

D Missing Material from Section 4

D.1 Initializing

In this section, we sketch the proof of $\mathsf{G}_0 \approx_c \mathsf{G}_1$.

Lemma 33 ($\mathsf{G}_0 \approx_c \mathsf{G}_1$)**.** *For all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_0 \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_1 \rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\mathrm{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{a}_2}}(\lambda).$$

Proof (sketch). Roughly, we will prove that

$$\big(\mathsf{mpk}, \boxed{\mathsf{ct}_{x^*}}, \mathsf{sk}_\Gamma\big) \approx_c \big(\mathsf{mpk}, \mathsf{ct}^0_{x^*}, \mathsf{sk}_\Gamma\big).$$

Recall that, we have $\boxed{[\mathbf{s}_0 \mathbf{A}_1]_1}$ in ct_{x^*} while $[\mathbf{s}_0 \mathbf{A}_1 + s_0 \mathbf{a}_2]_1$ in $\mathsf{ct}^0_{x^*}$. This relies on $\mathrm{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{a}_2}$ assumption which implies

$$\big([\mathbf{A}_1]_1, \boxed{[\mathbf{s}_0 \mathbf{A}_1]_1}\big) \approx_c \big([\mathbf{A}_1]_1, [\mathbf{s}_0 \mathbf{A}_1 + s_0 \mathbf{a}_2]_1\big)$$

where $\mathbf{s}_0 \leftarrow \mathbb{Z}_p^{1 \times k}$ and $s_0 \leftarrow \mathbb{Z}_p$. Let x^* be the selective challenge, the reduction algorithm is sketched as follows:

- we sample $\mathbf{k}, \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{W}_{\mathrm{end}}$ for all $\sigma \in \Sigma$ and create $(\mathsf{mpk}, \mathsf{msk})$ honestly using $[\mathbf{A}_1]_1$.
- on input key query Γ, we honestly run $\mathsf{sk}_\Gamma \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$ using mpk and msk;
- on input challenge query (m_0, m_1), we sample $\beta, \mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_\ell$ and create the challenge ciphertext for x^* using the term given out in the statement above. □

D.2 Selective Security in Many-key Setting

Our proof for selective security in Section 4 can be extended to the many-key setting in a straight-forward way as in [11]. Without loss of generality, we assume that all key queries $\Gamma_1, \ldots, \Gamma_q$ share the same state space $[Q]$ and alphabet Σ, and extend notations $\mathbf{d}, \mathbf{R}, \mathbf{f}_{i,x^*}$ for Γ_κ with an additional subscript κ. Then we sketch the changes that are needed to handle the many-key setting:

Game sequence. We employ the game sequence described in Section 4.3 except that

- secret keys in $\mathsf{G}_{2.i.0}$, $\mathsf{G}_{2.i.1}$, $\mathsf{G}_{2.i.3}$ and G_3 are $\mathsf{sk}^{i-1}_{\Gamma_\kappa}$, $\mathsf{sk}^{i-1,i}_{\Gamma_\kappa}$, $\mathsf{sk}^{i}_{\Gamma_\kappa}$ and $\mathsf{sk}^{\ell,*}_{\Gamma_\kappa}$, respectively, for *all* $\kappa \in [q]$;
- in each game, *all* q secret keys share the same $\Delta \leftarrow \mathbb{Z}_p$.

Lemmas and Proofs. Lemma 33,6,7,11,12,14,15,17,18 hold in the many-key setting:

- The proof for Lemma 33,6 can be trivially extended to the many-key setting.
- The proofs for Lemma 7,11,12 can work in the many-key setting due to the fact that
  - $\mathbf{d}_\kappa$ are fresh for each $\kappa \in [q]$; this ensures that all changes of variables still hold with multiple keys;
  - $\mathbf{R}_\kappa$ are fresh for each $\kappa \in [q]$; this ensures that all DDH-based arguments still hold with multiple keys.
- The proofs for Lemma 14,15 and Lemma 17 can be extended to the many-key setting using $(\mathbf{s}, \mathbf{W})$-switching lemma and $(\mathbf{z}, \mathbf{w})$-transition lemma, respectively.
- To prove Lemma 18 with many keys, we argue that *all* q secret keys $\mathsf{sk}^{\ell,*}_{\Gamma_1}, \ldots, \mathsf{sk}^{\ell,*}_{\Gamma_q}$ only leak $\alpha + s_\ell^{-1}\Delta$; here we use the fact that $\mathbf{f}_\kappa = \mathbf{f}_{\ell,x^*,\kappa}$ for all $\kappa \in [q]$.

E Missing Material from Section 5

E.1 Correctness of Adaptively Secure ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in Section 5.1

For $x = (x_1, \ldots, x_\ell)$ and $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma \in \Sigma}, \mathbf{u}, \mathbf{f})$ such that $\Gamma(x) = 1$, we have:

$$\begin{aligned}
B_0 &= [\mathbf{s}_0 \mathbf{A}_1 \mathbf{D} \mathbf{u}^\top]_T = [\mathbf{s}_0 \mathbf{A}_1 \mathbf{D} \mathbf{u}_{0,x}^\top]_T && (42)\\
\mathbf{b}_j &= \mathbf{s}_j \mathbf{A}_1 \mathbf{D} \mathbf{M}_{x_j} - \mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{D} && (43)\\
B_j &= [\mathbf{s}_j \mathbf{A}_1 \mathbf{D} \mathbf{u}_{j,x}^\top - \mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{D} \mathbf{u}_{j-1,x}^\top]_T && (44)\\
\mathbf{b}_{\mathrm{end}} &= \mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{D} && (45)\\
B_{\mathrm{end}} &= [\mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} \mathbf{u}_{\ell,x}^\top - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{D} \mathbf{u}_{\ell,x}^\top]_T && (46)\\
B_{\mathrm{all}} &= [\mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} \mathbf{u}_{\ell,x}^\top]_T && (47)\\
B &= [\mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \mathbf{k}^\top]_T && (48)
\end{aligned}$$

Here (46) is trivial; (44) and (48) follow from facts (19); the remaining equalities follow from:

$$\begin{aligned}
&(42) & \mathbf{s}_0 \mathbf{A}_1 \mathbf{D} \mathbf{u}^\top &= \mathbf{s}_0 \mathbf{A}_1 \cdot (\mathbf{D} \mathbf{u}^\top + \mathbf{W}_{\mathrm{start}} \mathbf{R} \mathbf{u}^\top) - \mathbf{s}_0 \mathbf{A}_1 \mathbf{W}_{\mathrm{start}} \cdot \mathbf{R} \mathbf{u}^\top\\
&(43) & \mathbf{s}_j \mathbf{A}_1 \mathbf{D} \mathbf{M}_{x_j} - \mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{D} &= \mathbf{s}_{j-1} \mathbf{A}_1 \cdot (-\mathbf{D} + \mathbf{Z}_{j \bmod 2} \mathbf{R}) + \mathbf{s}_j \mathbf{A}_1 \cdot (\mathbf{D} \mathbf{M}_{x_j} + \mathbf{W}_{x_j, j \bmod 2} \mathbf{R}) - (\mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{Z}_{j \bmod 2} + \mathbf{s}_j \mathbf{A}_1 \mathbf{W}_{x_j, j \bmod 2}) \cdot \mathbf{R}\\
&(45) & \mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{D} &= \mathbf{s}_\ell \mathbf{A}_1 \cdot (-\mathbf{D} + \mathbf{Z}_{\mathrm{end}} \mathbf{R}) + \mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \cdot (\mathbf{k}^\top \mathbf{f} + \mathbf{W}_{\mathrm{end}} \mathbf{R}) - (\mathbf{s}_\ell \mathbf{A}_1 \mathbf{Z}_{\mathrm{end}} + \mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \mathbf{W}_{\mathrm{end}}) \cdot \mathbf{R}\\
&(47) & \mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} \mathbf{u}_{\ell,x}^\top &= \mathbf{s}_0 \mathbf{A}_1 \mathbf{D} \mathbf{u}_{0,x}^\top + \textstyle\sum_{j=1}^{\ell} (\mathbf{s}_j \mathbf{A}_1 \mathbf{D} \mathbf{u}_{j,x}^\top - \mathbf{s}_{j-1} \mathbf{A}_1 \mathbf{D} \mathbf{u}_{j-1,x}^\top) + (\mathbf{s}_{\mathrm{end}} \mathbf{A}_1 \mathbf{k}^\top \mathbf{f} \mathbf{u}_{\ell,x}^\top - \mathbf{s}_\ell \mathbf{A}_1 \mathbf{D} \mathbf{u}_{\ell,x}^\top).
\end{aligned}$$

Correctness follows readily.

E.2 Missing Proofs in Section 5.2

In this section, we prove $\mathsf{G}_0 \approx_c \mathsf{G}_1$, $\mathsf{G}_{2.\kappa-1} \approx_c \mathsf{G}_{2.\kappa}$ (from the core lemma, Lemma 19), $\mathsf{G}_{2.q} \approx_s \mathsf{G}_3$ and show that adversary in G_3 has no advantage. All games are defined in Section 5.2.

Lemma 34 **($\mathsf{G}_0 \approx_c \mathsf{G}_1$).** *For all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_0 \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_1 \rangle = 1] \leq \mathsf{Adv}_{\mathcal{B}}^{\mathrm{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{a}_2}}(\lambda).$$

Proof (sketch). This relies on $\mathrm{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{a}_2}$ assumption which implies

$$\big([\mathbf{A}_1]_1, \boxed{[\mathbf{s}_{\mathrm{end}} \mathbf{A}_1]_1}\big) \approx_c \big([\mathbf{A}_1]_1, [\mathbf{s}_{\mathrm{end}} \mathbf{A}_1 + s_{\mathrm{end}} \mathbf{a}_2]_1\big)$$

where $\mathbf{s}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1 \times k}$ and $s_{\mathrm{end}} \leftarrow \mathbb{Z}_p$. The reduction algorithm is sketched as follows:

- we sample $\mathbf{k}, \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{Z}_{\mathrm{end}}, \mathbf{W}_{\mathrm{end}}$ for all $\sigma \in \Sigma$ and create $(\mathsf{mpk}, \mathsf{msk})$ honestly using $[\mathbf{A}_1]_1$.
- on key query Γ, we honestly run $\mathsf{sk}_\Gamma \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$ using mpk and msk;

- on input challenge query (x^*, m_0, m_1), we sample $\beta, \mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_\ell$ and create the challenge ciphertext using the term given out in the statement above. □

Lemma 35 **(Lemma 19 $\Rightarrow \mathsf{G}_{2.\kappa-1} \approx_c \mathsf{G}_{2.\kappa}$).** *For all $\kappa \in [q]$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ and*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa-1} \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa} \rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\text{CORE}}(\lambda)$$

where $\mathsf{Adv}_{\mathcal{B}}^{\text{CORE}}(\lambda)$ is defined in Lemma 19.

Proof (sketch). On input $(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2)$, we sketch the reduction $\mathcal{B}$ as follows:

- Forward mpk to $\mathcal{A}$.
- On input Γ, proceed as follows:
  - for the first $\kappa - 1$ queries Γ, output sk_Γ^* which can be created from aux_1 and aux_2;
  - for the κ'th query Γ, forward the result of $\mathsf{OKey}(\Gamma)$ to $\mathcal{A}$;
  - for the remaining query Γ, output sk_Γ which can be created from aux_1;
- On input (x^*, m_0, m_1), pick $\beta \leftarrow \{0,1\}$ and forward the result of $\mathsf{OEnc}(x^*, m_\beta)$ to $\mathcal{A}$.

Observe that, if $\mathsf{OKey}(\Gamma)$ outputs sk_Γ, the simulation is identical to $\mathsf{G}_{2.\kappa-1}$; if $\mathsf{OKey}(\Gamma)$ outputs sk_Γ^*, the simulation is identical to $\mathsf{G}_{2.\kappa}$. This completes the proof. □

Lemma 36 $(\mathsf{G}_{2.q} \approx_s \mathsf{G}_3)$**.** *For all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.q} \rangle = 1] \approx \Pr[\langle \mathcal{A}, \mathsf{G}_3 \rangle = 1].$$

Proof. First, we argue that all q secret keys perfectly hide the $\mathbf{a}_2$-component of $\mathbf{k}^\top$, i.e., $\alpha = \mathbf{a}_2\mathbf{k}^\top$. Recall that $\mathbf{a}_2$-components of all q secret keys are in the following form:

$$\mathsf{sk}_\Gamma^*[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{d} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \boxed{s_{\text{end}}^{-1}\Delta \cdot \mathbf{f}} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

we can simulate all of them using $\alpha + s_{\text{end}}^{-1}\Delta$ which means all secret keys perfectly hides $\alpha = \mathbf{a}_2\mathbf{k}^\top$. Therefore, the unique term involving $\mathbf{k}$ in $\mathsf{ct}_{x^*}^*$, i.e., $[\mathbf{s}_{\text{end}}\mathbf{A}_1\mathbf{k}^\top + s_{\text{end}}\mathbf{a}_2\mathbf{k}^\top]_T$, is independently and uniformly distributed and thus statistically hides message m_β. □

Lemma 37 **(Advantage in G_3).** *For all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_3 \rangle = 1] = 1/2.$$

Proof (sketch). This follows from the fact that the challenge ciphertext is independent of β in G_3. □

E.3 Detailed Proofs of Neighbor Indistinguishability in Section 5.4

This section provides the detailed for proving Lemma 22 (in Section 5.4) restated below.

Lemma 38 **(Neighbor indistinguishability).** *For all $\mathsf{xxx} \in \{0,1,3,4,5\} \cup \{2.i.i' : i \in [\ell], i' \in [4]\}$, $u_0, u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{\mathsf{xxx}}^0(u_0, u_1) \rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{\mathsf{xxx}}^1(u_0, u_1) \rangle = 1] \le O(|\Sigma|) \cdot \mathsf{Adv}_{\mathcal{B}}^{k\text{-Lin}}(\lambda).$$

All proofs essentially follows those for the selective security of our ABE for $\mathsf{NFA}^{\oplus p}$ in Section 4. We will also employ the notation of $\mathbf{a}_2$-components described in Section 4.3; in particular, the $\mathbf{a}_2$-components of aux_1 and aux_2 are defined analogously to sk_Γ and denoted by $\mathsf{aux}_1[2]$ and $\mathsf{aux}_2[2]$, respectively.

Initializing & Finalizing. We show that $\widehat{\mathsf{H}}_0^0(u_0,u_1) \approx_c \widehat{\mathsf{H}}_0^1(u_0,u_1)$, $\widehat{\mathsf{H}}_5^0(u_0,u_1) \approx_c \widehat{\mathsf{H}}_5^1(u_0,u_1)$ and $\widehat{\mathsf{H}}_1^0(u_0,u_1) \approx_s \widehat{\mathsf{H}}_1^1(u_0,u_1)$ for all u_0,u_1. The proofs for the former two are similar. We begin with the following lemma stating that $\widehat{\mathsf{H}}_0^0(u_0,u_1) \approx_c \widehat{\mathsf{H}}_0^1(u_0,u_1)$ for all u_0,u_1 and sketch the proof for the other one.

Lemma 39. *For all $u_0,u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_0^0(u_0,u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_0^1(u_0,u_1)\rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\mathrm{SWITCH}}(\lambda).$$

Overview. Fix Γ and x^*, we will prove that

$$\big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \boxed{\mathsf{ct}_{x^*}^*}, \mathsf{sk}_\Gamma\big) \approx_c \big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}_{x^*}^0, \mathsf{sk}_\Gamma\big)$$

which roughly means that

$$\overbrace{[\mathbf{s}_0\mathbf{A}_1]_1}^{\mathsf{ct}_{x^*}^*} \approx_c \overbrace{[\mathbf{s}_0\mathbf{A}_1 + s_0\mathbf{a}_2]_1}^{\mathsf{ct}_{x^*}^0} \quad \text{given} \quad \overbrace{[\mathbf{a}_2^{\parallel} \cdot s_{\mathrm{end}}^{-1}\Delta + \mathbf{W}_{\mathrm{end}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2}^{\mathsf{aux}_2}.$$

This is similar to Lemma 14 stating that $\mathsf{G}_{2.i.1} \approx_c \mathsf{G}_{2.i.2}$; therefore we prove the lemma analogously but using $(\mathbf{s}_0, \mathbf{W}_{\mathrm{end}})$-switching lemma instead of $(\mathbf{s}_i, \mathbf{Z}_\tau)$-switching lemma so that we can simulate the challenge ciphertext from the challenge term in the lemma and simulate aux_2 using the auxiliary terms given out in the lemma.

Proof. We prove the lemma for the case

$$u_0 = (\boxed{\{*\}}, \perp, \perp, \perp), \quad u_1 = (\{0\}, \perp, \perp, \perp)$$

with all Γ and x^* adaptively chosen by $\mathcal{A}$; the lemma trivially holds in all other cases. Recall that the difference between the two games lies in $\mathsf{OEnc}(x^*, m)$: the former returns $\mathsf{ct}_{x^*}^*$ and the latter returns $\mathsf{ct}_{x^*}^0$; oracle $\mathsf{OKey}(\Gamma)$ always returns sk_Γ. We prove the lemma using $(\mathbf{s}_0, \mathbf{W}_{\mathrm{end}})$-switching lemma (see Lemma 13). On input

$$\mathsf{aux},\ [\mathbf{c}_0]_1, [\mathbf{a}_2^{\parallel} \cdot \bar{\Delta} + \mathbf{W}_{\mathrm{end}}\mathbf{r}^\top]_2,\ [\mathbf{r}^\top]_2$$

where $\mathsf{aux} = ([\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_1\mathbf{W}_{\mathrm{end}}, \mathbf{a}_2\mathbf{W}_{\mathrm{end}}]_1, [\mathbf{W}_{\mathrm{end}}\mathbf{B}, \mathbf{B}]_2)$ and $\mathbf{W}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{r} \leftarrow \mathbb{Z}_p^{1\times k}$, $\bar{\Delta} \leftarrow \mathbb{Z}_p$ and

$$\mathbf{c}_0 = \boxed{\mathbf{s}_0\mathbf{A}_1} \text{ or } \mathbf{c}_0 = \mathbf{s}_0\mathbf{A}_1 + s_0\mathbf{a}_2, \quad \mathbf{s}_0 \leftarrow \mathbb{Z}_p^k, s_0 \leftarrow \mathbb{Z}_p$$

the reduction works as follows:

(Simulating mpk **and** aux_1**)** We sample $\mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}, \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{Z}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ for all $\sigma \in \Sigma$. Then we can trivially simulate mpk with $[\mathbf{A}_1, \mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1$ and simulate aux_1 with $[\mathbf{B}, \mathbf{W}_{\mathrm{end}}\mathbf{B}]_2$.

(Simulating aux_2**)** We sample $s_{\mathrm{end}} \leftarrow \mathbb{Z}_p$ and implicitly set

$$\Delta = s_{\mathrm{end}}\bar{\Delta}.$$

Then we can rewrite aux_2 as

$$[\mathbf{r}^\top]_2,\ [\mathbf{W}_{\mathrm{start}}\mathbf{r}^\top]_2,\ [\mathbf{Z}_0\mathbf{r}^\top]_2,\ [\mathbf{Z}_1\mathbf{r}^\top]_2,\ \big\{[\mathbf{W}_{\sigma,0}\mathbf{r}^\top]_2, [\mathbf{W}_{\sigma,1}\mathbf{r}^\top]_2\big\}_{\sigma\in\Sigma},\ [\mathbf{Z}_{\mathrm{end}}\mathbf{r}^\top]_2,\ [\mathbf{a}_2^{\parallel} \cdot \bar{\Delta} + \mathbf{W}_{\mathrm{end}}\mathbf{r}^\top]_2$$

which can be trivially simulated with $[\mathbf{a}_2^{\parallel} \cdot \bar{\Delta} + \mathbf{W}_{\mathrm{end}}\mathbf{r}^\top]_2$, $[\mathbf{r}^\top]_2$ given out in the lemma and $\mathbf{W}_{\mathrm{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{Z}_{\mathrm{end}}$.

(Answering OKey**)** On input Γ, we return sk_Γ which can be generated using aux_1.

(Answering OEnc) On input (x^*, m), we want to create a ciphertext in the following form, which is either $\mathsf{ct}^*_{x^*}$ or $\mathsf{ct}^0_{x^*}$ depending on $\mathbf{c}_0$:

$$\begin{pmatrix} [\mathbf{c}_0]_1,\ [\mathbf{c}_0\mathbf{W}_{\mathrm{start}}]_1 \\ \big\{[\mathbf{c}_j]_1, [\mathbf{c}_{j-1}\mathbf{Z}_{j \bmod 2}]_1 \cdot [\mathbf{c}_j\mathbf{W}_{x^*_j, j \bmod 2}]_1\big\}_{j\in[\ell]} \\ [\mathbf{c}_{\mathrm{end}}]_1, [\mathbf{c}_\ell\mathbf{Z}_{\mathrm{end}}]_1 \cdot \boxed{[\mathbf{c}_{\mathrm{end}}\mathbf{W}_{\mathrm{end}}]_1}, [\mathbf{c}_{\mathrm{end}}\mathbf{k}^\top]_T \cdot m \end{pmatrix} \text{ where } \begin{cases} \mathbf{c}_0 \in \{\boxed{\mathbf{s}_0\mathbf{A}_1}, \colorbox{lightgray}{$\mathbf{s}_0\mathbf{A}_1 + s_0\mathbf{a}_2$}\} \\ \mathbf{c}_j = \mathbf{s}_j\mathbf{A}_1 \text{ for all } j \in [\ell] \\ \mathbf{c}_{\mathrm{end}} = \mathbf{s}_{\mathrm{end}}\mathbf{A}_1 + s_{\mathrm{end}}\mathbf{a}_2 \end{cases}$$

Observe that,

- when $\mathbf{c}_0 = \boxed{\mathbf{s}_0\mathbf{A}_1}$, the distribution is identical to $\boxed{\mathsf{ct}^*_{x^*}}$;
- when $\mathbf{c}_0 = \colorbox{lightgray}{$\mathbf{s}_0\mathbf{A}_1 + s_0\mathbf{a}_2$}$, the distribution is identical to $\colorbox{lightgray}{$\mathsf{ct}^0_{x^*}$}$.

We proceed to create the ciphertext as follows:

- We sample $\mathbf{s}_1, \ldots, \mathbf{s}_\ell, \mathbf{s}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1\times k}$, $s_{\mathrm{end}} \leftarrow \mathbb{Z}_p$ and simulate $\{[\mathbf{c}_j]_1\}_{j\in[\ell]}$ and $[\mathbf{c}_{\mathrm{end}}]_1$ using $[\mathbf{A}_1, \mathbf{a}_2]_1$; note that $[\mathbf{c}_0]_1$ is given out in the lemma as the challenge term.
- We rewrite the term in the dashed box as:

$$[\mathbf{c}_{\mathrm{end}}\mathbf{W}_{\mathrm{end}}]_1 = [\mathbf{s}_{\mathrm{end}}\mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1 \cdot [s_{\mathrm{end}}\mathbf{a}_2\mathbf{W}_{\mathrm{end}}]_1$$

  which can be simulated using $\mathbf{s}_{\mathrm{end}}, s_{\mathrm{end}}$ and $[\mathbf{A}_1\mathbf{W}_{\mathrm{end}}, \mathbf{a}_2\mathbf{W}_{\mathrm{end}}]_1$; here we use the fact that we do not have any terms involving $[\mathbf{s}_0\mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1$ in the ciphertext.
- We simulate all remaining terms using $\{[\mathbf{c}_j]_1\}_{j\in[0,\ell]}$, $[\mathbf{c}_{\mathrm{end}}]_1$ and $\mathbf{k}, \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{Z}_{\mathrm{end}}$.

Observe that, when $\mathbf{c}_0 = \boxed{\mathbf{s}_0\mathbf{A}_1}$, oracle $\mathsf{OEnc}(x^*, m)$ returns $\boxed{\mathsf{ct}^*_{x^*}}$ and the simulation is identical to $\widehat{\mathsf{H}}^0_0(u_0, u_1)$; when $\mathbf{c}_0 = \colorbox{lightgray}{$\mathbf{s}_0\mathbf{A}_1 + s_0\mathbf{a}_2$}$, oracle $\mathsf{OEnc}(x^*, m)$ returns $\colorbox{lightgray}{$\mathsf{ct}^0_{x^*}$}$ and the simulation is identical to $\widehat{\mathsf{H}}^1_0(u_0, u_1)$. This completes the proof. □

Via the same proof idea, we can prove the following lemma stating that $\widehat{\mathsf{H}}^0_5(u_0, u_1) \approx_c \widehat{\mathsf{H}}^1_5(u_0, u_1)$ for all u_0, u_1. We only sketch the proof.

Lemma 40. *For all $u_0, u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_5(u_0, u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_5(u_0, u_1)\rangle = 1] \leq \mathsf{Adv}^{\mathrm{SWITCH}}_{\mathcal{B}}(\lambda).$$

Proof (sketch). We prove the lemma for the case

$$u_0 = (\boxed{\{\ell\}}, \{*\}, \perp, \perp), \quad u_1 = (\colorbox{lightgray}{$\{*\}$}, \{*\}, \perp, \perp)$$

with all Γ and x^* adaptively chosen by $\mathcal{A}$; the lemma trivially holds in all other cases. Namely, we will prove that

$$\big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \boxed{\mathsf{ct}^\ell_{x^*}}, \mathsf{sk}^*_\Gamma\big) \approx_c \big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \colorbox{lightgray}{$\mathsf{ct}^*_{x^*}$}, \mathsf{sk}^*_\Gamma\big)$$

which roughly means that

$$\overbrace{[\mathbf{s}_\ell\mathbf{A}_1 + s_\ell\mathbf{a}_2]_1}^{\mathsf{ct}^\ell_{x^*}} \approx_c \overbrace{[\mathbf{s}_\ell\mathbf{A}_1]_1}^{\mathsf{ct}^*_{x^*}} \quad \text{given} \quad \overbrace{[\mathbf{a}_2^\parallel \cdot s_{\mathrm{end}}^{-1}\Delta + \mathbf{W}_{\mathrm{end}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2}^{\mathsf{aux}_2, \mathsf{sk}^*_\Gamma}.$$

Then the proof is analogous to that for Lemma 39 except that we use $(\mathbf{s}_\ell, \mathbf{W}_{\mathrm{end}})$- instead of $(\mathbf{s}_0, \mathbf{W}_{\mathrm{end}})$-switching lemma and we need aux_2 to answer OKey query; in particular,

- we simulate $\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2$ as in the proof of Lemma 39;
- we answer $\mathsf{OKey}(\Gamma)$ by generating sk^*_Γ using both aux_1 and aux_2.

– we answer $\mathsf{OEnc}(x^*, m)$ using the challenge term in the lemma analogously; but we rely on the fact that there is no term with $[\mathbf{s}_\ell\mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1$. □

We finally prove the lemma stating that $\widehat{\mathsf{H}}_1^0(u_0,u_1) \approx_c \widehat{\mathsf{H}}_1^1(u_0,u_1)$ for all u_0,u_1, which is analogous to Lemma 6.

Lemma 41. *For all $u_0,u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_1^0(u_0,u_1)\rangle = 1] = \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_1^1(u_0,u_1)\rangle = 1]$$

Proof (sketch). We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\{0\}, \boxed{\bot,\bot,\bot}),\ u_1 = (\{0\}, \colorbox{lightgray}{$\{0\},\bot,\mathbf{f}_{0,x^*}$});$$

the lemma trivially holds in all other cases. This roughly means that

$$\left(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}_{x^*}^0, \boxed{\mathsf{sk}_\Gamma}\right) \approx_c \left(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}_{x^*}^0, \colorbox{lightgray}{$\mathsf{sk}_{\Gamma,\mathbf{f}_{0,x^*}}^0$}\right)$$

where

$$\mathsf{sk}_\Gamma[2] \ = \begin{pmatrix} [\boxed{\mathbf{d}\mathbf{u}^\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d}+\mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{d}+\mathbf{z}_{\mathrm{end}}\mathbf{R}]_2, [\alpha\mathbf{f}+\mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix},$$

$$\mathsf{sk}_{\Gamma,\mathbf{f}_{0,x^*}}^0[2] \ = \begin{pmatrix} [\colorbox{lightgray}{$(\mathbf{d}+s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*})\mathbf{u}^\top$} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d}+\mathbf{z}_b\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{d}+\mathbf{z}_{\mathrm{end}}\mathbf{R}]_2, [\alpha\mathbf{f}+\mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

with

$$\mathsf{ct}_{x^*}^0[2] = \left([s_0\mathbf{w}_{\mathrm{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1]_1, [s_{\mathrm{end}}\mathbf{w}_{\mathrm{end}}]_1, [s_{\mathrm{end}}]_1, [s_{\mathrm{end}}\alpha]_T\cdot m\right)$$

and

$$\begin{aligned} \mathsf{aux}_1[2] \ &= \ \left([\alpha, \mathbf{B}, \mathbf{w}_{\mathrm{start}}\mathbf{B}, \mathbf{z}_0\mathbf{B}, \mathbf{z}_1\mathbf{B}, \{\mathbf{w}_{\sigma,0}\mathbf{B}, \mathbf{w}_{\sigma,1}\mathbf{B}\}_{\sigma\in\Sigma}, \mathbf{z}_{\mathrm{end}}\mathbf{B}, \mathbf{w}_{\mathrm{end}}\mathbf{B}]_2\right) \\ \mathsf{aux}_2[2] \ &= \ \left([\mathbf{r}^\top, \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top, \mathbf{z}_0\mathbf{r}^\top, \mathbf{z}_1\mathbf{r}^\top, \{\mathbf{w}_{\sigma,0}\mathbf{r}^\top, \mathbf{w}_{\sigma,1}\mathbf{r}^\top\}_{\sigma\in\Sigma}, \mathbf{z}_{\mathrm{end}}\mathbf{r}^\top, s_{\mathrm{end}}^{-1}\Delta + \mathbf{w}_{\mathrm{end}}\mathbf{r}^\top]_2\right). \end{aligned}$$

This immediately follows from the fact $\Gamma(x^*) = 0 \iff \mathbf{f}_{0,x^*}\mathbf{u}^\top = 0 \bmod p$ (see Lemma 5). □

Switching secret keys I. We show that $\widehat{\mathsf{H}}_{2.i.1}^0(u_0,u_1) \approx_c \widehat{\mathsf{H}}_{2.i.1}^1(u_0,u_1)$, $\widehat{\mathsf{H}}_3^0(u_0,u_1) \approx_c \widehat{\mathsf{H}}_3^1(u_0,u_1)$ for all $i \in [\ell]$ and all u_0,u_1. The proofs for them are similar. We begin with the following lemma stating that $\widehat{\mathsf{H}}_{2.1.1}^0(u_0,u_1) \approx_c \widehat{\mathsf{H}}_{2.1.1}^1(u_0,u_1)$ for all u_0,u_1, which is analogous to Lemma 7, and sketch the proofs for remaining statements.

Lemma 42. *For all $u_0,u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{2.1.1}^0(u_0,u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{2.1.1}^1(u_0,u_1)\rangle = 1] \le O(|\Sigma|)\cdot \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DDH}_{1,Q}^{G_2}}(\lambda).$$

Overview. Fix Γ and x^*, we will prove that

$$\left(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}_{x^*}^0, \boxed{\mathsf{sk}_{\Gamma,\mathbf{f}_{0,x^*}}^0}\right) \approx_c \left(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}_{x^*}^0, \colorbox{lightgray}{$\mathsf{sk}_{\Gamma,\mathbf{f}_{0,x^*}}^{0,1}$}\right).$$

By Lemma 4, we focus on the $\mathbf{a}_2$-components and prove:

$$\mathsf{sk}_{\Gamma,\mathbf{f}_{0,x^*}}^0[2] = \begin{pmatrix} [(\boxed{\mathbf{d}+s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*}})\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[\boxed{-\mathbf{d}} + \mathbf{z}_1\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[-\mathbf{d}+\mathbf{z}_0\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [-\mathbf{d}+\mathbf{z}_{\mathrm{end}}\mathbf{R}]_2, [\alpha\mathbf{f}+\mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} \approx_c \begin{pmatrix} [\colorbox{lightgray}{$\mathbf{d}$}\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[\colorbox{lightgray}{$-\mathbf{d}+s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*}$} + \mathbf{z}_1\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[-\mathbf{d}+\mathbf{z}_0\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [-\mathbf{d}+\mathbf{z}_{\mathrm{end}}\mathbf{R}]_2, [\alpha\mathbf{f}+\mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} = \mathsf{sk}_{\Gamma,\mathbf{f}_{0,x^*}}^{0,1}[2]$$

given

$$\mathsf{ct}^0_{x^*}[2] = \big([s_0\mathbf{w}_{\text{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1]_1, [s_{\text{end}}\mathbf{w}_{\text{end}}]_1, [s_{\text{end}}]_1, [s_{\text{end}}\alpha]_T \cdot m\big)$$

and

$$\begin{aligned}\mathsf{aux}_1[2] &= \big([\alpha, \mathbf{B}, \mathbf{w}_{\text{start}}\mathbf{B}, \mathbf{z}_0\mathbf{B}, \mathbf{z}_1\mathbf{B}, \{\mathbf{w}_{\sigma,0}\mathbf{B}, \mathbf{w}_{\sigma,1}\mathbf{B}\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{B}, \mathbf{w}_{\text{end}}\mathbf{B}]_2\big)\\ \mathsf{aux}_2[2] &= \big([\mathbf{r}^\top, \mathbf{w}_{\text{start}}\mathbf{r}^\top, \mathbf{z}_0\mathbf{r}^\top, \mathbf{z}_1\mathbf{r}^\top, \{\mathbf{w}_{\sigma,0}\mathbf{r}^\top, \mathbf{w}_{\sigma,1}\mathbf{r}^\top\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{r}^\top, s_{\text{end}}^{-1}\Delta + \mathbf{w}_{\text{end}}\mathbf{r}^\top]_2\big).\end{aligned}$$

Clearly, change of variables $\mathbf{d} \mapsto \mathbf{d} - s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*}$ is at the core of the above statement, which ensures that, for all s_0 and Δ, we have

$$\overbrace{\{(\boxed{\mathbf{d} + s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*}})\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top, \boxed{-\mathbf{d}} + \mathbf{z}_1\mathbf{R}, \mathbf{R}\}}^{\mathsf{sk}^0_{\Gamma,\mathbf{f}_{0,x^*}}[2]} \approx_s \overbrace{\{\mathbf{d}\,\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top, -\mathbf{d} + s_0^{-1}\Delta\cdot\mathbf{f}_{0,x^*} + \mathbf{z}_1\mathbf{R}, \mathbf{R}\}}^{\mathsf{sk}^{0,1}_{\Gamma,\mathbf{f}_{0,x^*}}[2]} \quad \text{given } \overbrace{\mathbf{w}_{\text{start}}, \mathbf{z}_1}^{\mathsf{ct}^0_{x^*}[2]}$$

As in the proof of Lemma 7, we need to hide all irrelevant $\mathbf{d}$'s via $\mathrm{DDH}^{G_2}_{1,Q}$ assumption before and after the change of variable via $\mathrm{DDH}^{G_2}_{1,Q}$ assumption. Note that, besides $\mathbf{w}_{\text{start}}$ and $\mathbf{z}_1$, $\mathsf{ct}^0_{x^*}[2]$ also leaks $\mathbf{w}_{\text{end}}$, which means we cannot apply $\mathrm{DDH}^{G_2}_{1,Q}$ assumption w.r.t. $\mathbf{w}_{\text{end}}$; however the term $[\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2$ does not contain $\mathbf{d}$ either and will not interfere in the change of variable with respect to $\mathbf{d}$.

Auxiliary hybrids. Formally, fix $u_0 = (\{0\}, \{0\}, \perp, \mathbf{p})$ and $u_1 = (\{0\}, \{0,1\}, \perp, \mathbf{p})$, we define two more auxiliary hybrids:

- $\widehat{\mathsf{H}}^0_{2.1.1.a}(u_0, u_1)$ is the same as $\widehat{\mathsf{H}}^0_{2.1.1}(u_0, u_1)$ except that $\mathsf{OKey}(\Gamma)$ outputs

$$\left(\begin{array}{c}[(\mathbf{d} + s_0^{-1}\Delta\cdot\mathbf{p})\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2\\ \{[-\mathbf{d} + \mathbf{z}_1\mathbf{R}]_2, [\boxed{\mathbf{0}}\cdot\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma}\\ \{[\boxed{\mathbf{0}} + \mathbf{z}_0\mathbf{R}]_2, [\boxed{\mathbf{0}}\cdot\mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma}\\ [\boxed{\mathbf{0}} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2\end{array}\right)$$

- $\widehat{\mathsf{H}}^1_{2.1.1.a}(u_0, u_1)$ is the same as $\widehat{\mathsf{H}}^1_{2.1.1}(u_0, u_1)$ except that $\mathsf{OKey}(\Gamma)$ outputs

$$\left(\begin{array}{c}[\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2\\ \{[-\mathbf{d} + s_0^{-1}\Delta\cdot\mathbf{p} + \mathbf{z}_1\mathbf{R}]_2, [\boxed{\mathbf{0}}\cdot\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma}\\ \{[\boxed{\mathbf{0}} + \mathbf{z}_0\mathbf{R}]_2, [\boxed{\mathbf{0}}\cdot\mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma}\\ [\boxed{\mathbf{0}} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2\end{array}\right)$$

Then we prove that:

$$\widehat{\mathsf{H}}^0_{2.1.1}(u_0, u_1) \approx_c \widehat{\mathsf{H}}^0_{2.1.1.a}(u_0, u_1) \approx_s \widehat{\mathsf{H}}^1_{2.1.1.a}(u_0, u_1) \approx_c \widehat{\mathsf{H}}^1_{2.1.1}(u_0, u_1). \tag{49}$$

which is summarized in Fig 10 with fixed Γ and x^*.

Lemmas. We describe and prove the following lemmas which imply Lemma 42 by (49).

Lemma 43. *For all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle\mathcal{A}, \widehat{\mathsf{H}}^0_{2.1.1}(u_0, u_1)\rangle = 1] - \Pr[\langle\mathcal{A}, \widehat{\mathsf{H}}^0_{2.1.1.a}(u_0, u_1)\rangle = 1] \leq O(|\Sigma|)\cdot\mathsf{Adv}^{\mathrm{DDH}^{G_2}_{1,Q}}_{\mathcal{B}}(\lambda).$$

Proof. We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\{0\}, \{0\}, \perp, \mathbf{f}_{0,x^*}),\ u_1 = (\{0\}, \{0,1\}, \perp, \mathbf{f}_{0,x^*});$$

Game	$? \cdot \mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top$	$? + \mathbf{z}_1\mathbf{R}$	$? \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}$	$? + \mathbf{z}_0\mathbf{R}$	$? \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}$	$? + \mathbf{z}_{\text{end}}\mathbf{R}$	Remark
$\widehat{\mathsf{H}}^0_{2.1.1}$	$\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{p}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathbf{d}$	$-\mathbf{d}$	$\mathsf{sk}^0_{\Gamma,\mathbf{p}}[2]$
$\widehat{\mathsf{H}}^0_{2.1.1.a}$	$\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{p}$	$-\mathbf{d}$	$\boxed{\mathbf{0}}$	$\boxed{\mathbf{0}}$	$\boxed{\mathbf{0}}$	$\boxed{\mathbf{0}}$	DDH
$\widehat{\mathsf{H}}^1_{2.1.1.a}$	$\mathbf{d}$	$-\mathbf{d} + \boxed{s_0^{-1}\Delta \cdot \mathbf{p}}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{d} \mapsto \mathbf{d} - s_0^{-1}\Delta \cdot \mathbf{p}$
$\widehat{\mathsf{H}}^1_{2.1.1}$	$\mathbf{d}$	$-\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{p}$	$\boxed{\mathbf{d}}$	$\boxed{-\mathbf{d}}$	$\boxed{\mathbf{d}}$	$\boxed{-\mathbf{d}}$	DDH, $\mathsf{sk}^{0,1}_{\Gamma,\mathbf{p}}[2]$

Fig. 10. Game sequence for $\widehat{\mathsf{H}}^0_{2.1.1}(u_0, u_1) \approx_c \widehat{\mathsf{H}}^1_{2.1.1}(u_0, u_1)$. In the table, we only show changes of secret key and focus on its $\mathbf{a}_2$-components; all secret key elements in the fourth and sixth column are quantified over $\sigma \in \Sigma$. In the **Remark** column, "DDH" indicates $\text{DDH}^{G_2}_{1,Q}$ assumption.

the lemma trivially holds in all other cases. By Lemma 4, it suffices to prove the lemma over $\mathbf{a}_2$-components which roughly means:

$$\mathsf{sk}^0_{\Gamma,\mathbf{f}_{0,x^*}}[2] = \begin{pmatrix} [(\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*})\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_1\mathbf{R}]_2, [\boxed{\mathbf{d}} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[-\boxed{\mathbf{d}} + \mathbf{z}_0\mathbf{R}]_2, [\boxed{\mathbf{d}} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [-\boxed{\mathbf{d}} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} \approx_c \begin{pmatrix} [(\mathbf{d} + s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*})\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \{[-\mathbf{d} + \mathbf{z}_1\mathbf{R}]_2, [\colorbox{lightgray}{$\mathbf{0}$} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,1}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ \{[\colorbox{lightgray}{$\mathbf{0}$} + \mathbf{z}_0\mathbf{R}]_2, [\colorbox{lightgray}{$\mathbf{0}$} \cdot \mathbf{M}_\sigma + \mathbf{w}_{\sigma,0}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma} \\ [\colorbox{lightgray}{$\mathbf{0}$} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

in the presence of

$$\mathsf{ct}^0_{x^*}[2] = \big([s_0\mathbf{w}_{\text{start}}]_1, [s_0]_1, [s_0\mathbf{z}_1]_1, [s_{\text{end}}\mathbf{w}_{\text{end}}]_1, [s_{\text{end}}]_1, [s_{\text{end}}\alpha]_T \cdot m\big)$$

and

$$\begin{aligned} \mathsf{aux}_1[2] &= \big([\alpha, \mathbf{B}, \mathbf{w}_{\text{start}}\mathbf{B}, \mathbf{z}_0\mathbf{B}, \mathbf{z}_1\mathbf{B}, \{\mathbf{w}_{\sigma,0}\mathbf{B}, \mathbf{w}_{\sigma,1}\mathbf{B}\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{B}, \mathbf{w}_{\text{end}}\mathbf{B}]_2\big) \\ \mathsf{aux}_2[2] &= \big([\mathbf{r}^\top, \mathbf{w}_{\text{start}}\mathbf{r}^\top, \mathbf{z}_0\mathbf{r}^\top, \mathbf{z}_1\mathbf{r}^\top, \{\mathbf{w}_{\sigma,0}\mathbf{r}^\top, \mathbf{w}_{\sigma,1}\mathbf{r}^\top\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{r}^\top, s_{\text{end}}^{-1}\Delta + \mathbf{w}_{\text{end}}\mathbf{r}^\top]_2\big) \end{aligned}$$

One can sample basis $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_3, \mathbf{A}_1^\parallel, \mathbf{a}_2^\parallel, \mathbf{A}_3^\parallel$ and trivially simulate mpk, $\mathsf{aux}_1, \mathsf{aux}_2$, $\mathsf{ct}^0_{x^*}$ and secret key using terms given out above. Furthermore, this follows from $\text{DDH}^{G_2}_{1,Q}$ assumption w.r.t $\mathbf{z}_0, \mathbf{w}_{\sigma,0}, \mathbf{w}_{\sigma,1}, \mathbf{z}_{\text{end}}$ with $\sigma \in \Sigma$ which implies:

$$\big([\mathbf{z}_0\mathbf{R}]_2, \{[\mathbf{w}_{\sigma,0}\mathbf{R}]_2\}_{\sigma\in\Sigma}, \{[\mathbf{w}_{\sigma,1}\mathbf{R}]_2\}_{\sigma\in\Sigma}, [\mathbf{z}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2\big) \approx_c U\big((G_2^{1\times Q})^{2|\Sigma|+2} \times G_2^{k\times Q}\big)$$

given $\mathsf{aux} = [\mathbf{B}, \mathbf{z}_0\mathbf{B}, \{\mathbf{w}_{\sigma,0}\mathbf{B}, \mathbf{w}_{\sigma,1}\mathbf{B}\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{B}]_2$ where $\mathbf{z}_0, \mathbf{w}_{\sigma,0}, \mathbf{w}_{\sigma,1}, \mathbf{z}_{\text{end}} \leftarrow \mathbb{Z}_p^{1\times k}$ for all $\sigma \in \Sigma$ and $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times Q}$. Here we use the fact that $\mathsf{ct}^0_{x^*}[2]$ does not leak $\mathbf{z}_0$, $\mathbf{w}_{\sigma,1}$, $\mathbf{w}_{\sigma,0}$, $\mathbf{z}_{\text{end}}$ with $\sigma \in \Sigma$. This completes the proof. □

Lemma 44. *For all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_{2.1.1.a}(u_0, u_1)\rangle = 1] = \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{2.1.1.a}(u_0, u_1)\rangle = 1]$$

Proof. This immediately follows from the change of variables: $\mathbf{d} \mapsto \mathbf{d} - s_0^{-1}\Delta \cdot \mathbf{f}_{0,x^*}$. □

Lemma 45. *For all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{2.1.1.a}(u_0, u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{2.1.1}(u_0, u_1)\rangle = 1] \le O(|\Sigma|) \cdot \mathsf{Adv}_{\mathcal{B}}^{\text{DDH}^{G_2}_{1,Q}}(\lambda).$$

Proof. The proof is analogous to that for Lemma 43. □

Via the same proof idea, we can prove the following lemmas stating that $\widehat{\mathsf{H}}^0_{2.i.1}(u_0, u_1) \approx_c \widehat{\mathsf{H}}^1_{2.i.1}(u_0, u_1)$ for all $i \in [2, \ell]$ and $\widehat{\mathsf{H}}^0_3(u_0, u_1) \approx_c \widehat{\mathsf{H}}^1_3(u_0, u_1)$, respectively. We only sketch the proof for each lemma.

Lemma 46. *For all $i \in [2, \ell]$, $u_0, u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_{2.i.1}(u_0, u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{2.i.1}(u_0, u_1)\rangle = 1] \le O(|\Sigma|) \cdot \mathsf{Adv}_{\mathcal{B}}^{\text{DDH}^{G_2}_{1,Q}}(\lambda).$$

Proof (sketch). We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\{i-1\}, \boxed{\{i-1\}, x^*_{i-1}}, \mathbf{f}_{i-1,x^*}),\ \ u_1 = (\{i-1\}, \colorbox{lightgray}{$\{i-1,i\}, \bot$}, \mathbf{f}_{i-1,x^*});$$

the lemma trivially holds in other cases. Namely, we need to prove that

$$\big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}^{i-1}_{x^*}, \boxed{\mathsf{sk}^{i-1}_{\Gamma, x^*_{i-1}, \mathbf{f}_{i-1,x^*}}}\big) \approx_c \big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}^{i-1}_{x^*}, \colorbox{lightgray}{$\mathsf{sk}^{i-1,i}_{\Gamma, \mathbf{f}_{i-1,x^*}}$}\big).$$

Recall that $\tau = i \bmod 2$, this roughly means that

$$\mathsf{sk}^{i-1}_{\Gamma, x^*_{i-1}, \mathbf{f}_{i-1,x^*}}[2] \ = \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \big\{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [(\boxed{\mathbf{d} + s^{-1}_{i-1}\Delta \cdot \mathbf{f}_{i-1,x^*}})\mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\} \\ \big\{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2\big\}_{\sigma \neq x^*_{i-1}} \\ \big\{[\boxed{-\mathbf{d}} + \mathbf{z}_\tau\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [-\mathbf{d} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\approx_c \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \big\{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\colorbox{lightgray}{$\mathbf{d}$}\mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\} \\ \big\{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2\big\}_{\sigma \neq x^*_{i-1}} \\ \big\{[\colorbox{lightgray}{$-\mathbf{d} + s^{-1}_{i-1}\Delta \cdot \mathbf{f}_{i-1,x^*}$} + \mathbf{z}_\tau\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [-\mathbf{d} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} = \mathsf{sk}^{i-1,i}_{\Gamma, \mathbf{f}_{i-1,x^*}}[2]$$

given

$$\mathsf{ct}^{i-1}_{x^*}[2] = \big([s_{i-1}\mathbf{w}_{x^*_{i-1},1-\tau}]_1, [s_{i-1}]_1, [s_{i-1}\mathbf{z}_\tau]_1, [s_{\text{end}}\mathbf{w}_{\text{end}}]_1, [s_{\text{end}}]_1, [s_{\text{end}}\alpha]_T \cdot m\big)$$

and

$$\begin{aligned} \mathsf{aux}_1[2] \ &= \big([\alpha, \mathbf{B}, \mathbf{w}_{\text{start}}\mathbf{B}, \mathbf{z}_0\mathbf{B}, \mathbf{z}_1\mathbf{B}, \{\mathbf{w}_{\sigma,0}\mathbf{B}, \mathbf{w}_{\sigma,1}\mathbf{B}\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{B}, \mathbf{w}_{\text{end}}\mathbf{B}]_2\big) \\ \mathsf{aux}_2[2] \ &= \big([\mathbf{r}^\top, \mathbf{w}_{\text{start}}\mathbf{r}^\top, \mathbf{z}_0\mathbf{r}^\top, \mathbf{z}_1\mathbf{r}^\top, \{\mathbf{w}_{\sigma,0}\mathbf{r}^\top, \mathbf{w}_{\sigma,1}\mathbf{r}^\top\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{r}^\top, s^{-1}_{\text{end}}\Delta + \mathbf{w}_{\text{end}}\mathbf{r}^\top]_2\big) \end{aligned}$$

This relies on:

- change of variables $\mathbf{d} \mapsto \mathbf{d} - s^{-1}_{i-1}\Delta \cdot \mathbf{f}_{i-1,x^*}$; this ensures that, for all s_{i-1} and Δ, we have

  $$\overbrace{\big\{(\boxed{\mathbf{d} + s^{-1}_{i-1}\Delta \cdot \mathbf{f}_{i-1,x^*}})\mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}, \boxed{-\mathbf{d}} + \mathbf{z}_\tau\mathbf{R}, \mathbf{R}\big\}}^{\mathsf{sk}^{i-1}_{\Gamma, x^*_{i-1}, \mathbf{f}_{i-1,x^*}}[2]} \approx_s \overbrace{\big\{\colorbox{lightgray}{$\mathbf{d}$}\mathbf{M}_{x^*_{i-1}} + \mathbf{w}_{x^*_{i-1},1-\tau}\mathbf{R}, \colorbox{lightgray}{$-\mathbf{d} + s^{-1}_{i-1}\Delta \cdot \mathbf{f}_{i-1,x^*}$} + \mathbf{z}_\tau\mathbf{R}, \mathbf{R}\big\}}^{\mathsf{sk}^{i-1,i}_{\Gamma, \mathbf{f}_{i-1,x^*}}[2]}$$

  in the presence of $\mathbf{w}_{x^*_{i-1},1-\tau}, \mathbf{z}_\tau$ leaked via $\mathsf{ct}^{i-1}_{x^*}[2]$.
- $\mathrm{DDH}^{G_2}_{1,Q}$ assumption w.r.t $\mathbf{w}_{\text{start}}, \mathbf{z}_{1-\tau}, \{\mathbf{w}_{\sigma,1-\tau}\}_{\sigma \neq x^*_{i-1}}, \{\mathbf{w}_{\sigma,\tau}\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}$; this implies that

  $$\big([\mathbf{w}_{\text{start}}\mathbf{R}]_2, [\mathbf{z}_{1-\tau}\mathbf{R}]_2, \big\{[\mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2\big\}_{\sigma \neq x^*_{i-1}}, \big\{[\mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\big\}_{\sigma\in\Sigma}, [\mathbf{z}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2\big) \approx_c U\big((G_2^{1\times Q})^{2|\Sigma|+2} \times G_2^{k\times Q}\big)$$

  and will be used to hide all **d**'s irrelevant with the change of variables. □

Lemma 47. *For all $u_0, u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_3(u_0, u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_3(u_0, u_1)\rangle = 1] \le O(|\Sigma|) \cdot \mathsf{Adv}^{\mathrm{DDH}^{G_2}_{1,Q}}_{\mathcal{B}}(\lambda).$$

Proof (sketch). We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\{\ell\}, \boxed{\{\ell\}, x^*_\ell, \mathbf{f}_{\ell,x^*}}),\ u_1 = (\{\ell\}, \colorbox{lightgray}{$\{\ell, *\}, \bot, \mathbf{f}$});$$

the lemma trivially holds in other cases. By the fact that $\mathbf{f}_{\ell,x^*} = \mathbf{f}$ (see Lemma 5), we need to prove that

$$\big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}^{\ell}_{x^*}, \boxed{\mathsf{sk}^{\ell}_{\Gamma,x^*_\ell,\mathbf{f}}}\big) \approx_c \big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \mathsf{ct}^{\ell}_{x^*}, \colorbox{lightgray}{$\mathsf{sk}^{\ell,*}_{\Gamma,\mathbf{f}}$}\big);$$

this roughly means:

$$\mathsf{sk}^{\ell}_{\Gamma,x^*_\ell,\mathbf{f}}[2] \;=\; \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \big\{[-\mathbf{d} + \mathbf{z}_{\bar\ell}\mathbf{R}]_2, [(\boxed{\mathbf{d} + s_\ell^{-1}\Delta\cdot\mathbf{f}})\mathbf{M}_{x^*_\ell} + \mathbf{w}_{x^*_\ell,\bar\ell}\mathbf{R}]_2, [\mathbf{R}]_2\big\} \\ \big\{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\bar\ell}\mathbf{R}]_2\big\}_{\sigma\neq x^*_\ell} \\ \big\{[-\mathbf{d} + \mathbf{z}_{1-\bar\ell}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\bar\ell}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [\boxed{-\mathbf{d}} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\approx_c \begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\text{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \big\{[-\mathbf{d} + \mathbf{z}_{\bar\ell}\mathbf{R}]_2, [\colorbox{lightgray}{$\mathbf{d}$}\mathbf{M}_{x^*_\ell} + \mathbf{w}_{x^*_\ell,\bar\ell}\mathbf{R}]_2, [\mathbf{R}]_2\big\} \\ \big\{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\bar\ell}\mathbf{R}]_2\big\}_{\sigma\neq x^*_\ell} \\ \big\{[-\mathbf{d} + \mathbf{z}_{1-\bar\ell}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\bar\ell}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [\colorbox{lightgray}{$-\mathbf{d} + s_\ell^{-1}\Delta\cdot\mathbf{f}$} + \mathbf{z}_{\text{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} = \mathsf{sk}^{\ell,*}_{\Gamma}[2]$$

given

$$\mathsf{ct}^{\ell}_{x^*}[2] = \big([s_\ell\mathbf{w}_{x^*_\ell,\bar\ell}]_1, [s_\ell]_1, [s_\ell\mathbf{z}_{\text{end}} + s_{\text{end}}\mathbf{w}_{\text{end}}]_1, [s_{\text{end}}]_1, [s_{\text{end}}\alpha]_T\cdot m\big)$$

and

$$\begin{aligned} \mathsf{aux}_1[2] &= \big([\alpha, \mathbf{B}, \mathbf{w}_{\text{start}}\mathbf{B}, \mathbf{z}_0\mathbf{B}, \mathbf{z}_1\mathbf{B}, \{\mathbf{w}_{\sigma,0}\mathbf{B}, \mathbf{w}_{\sigma,1}\mathbf{B}\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{B}, \mathbf{w}_{\text{end}}\mathbf{B}]_2\big) \\ \mathsf{aux}_2[2] &= \big([\mathbf{r}^\top, \mathbf{w}_{\text{start}}\mathbf{r}^\top, \mathbf{z}_0\mathbf{r}^\top, \mathbf{z}_1\mathbf{r}^\top, \{\mathbf{w}_{\sigma,0}\mathbf{r}^\top, \mathbf{w}_{\sigma,1}\mathbf{r}^\top\}_{\sigma\in\Sigma}, \mathbf{z}_{\text{end}}\mathbf{r}^\top, s_{\text{end}}^{-1}\Delta + \mathbf{w}_{\text{end}}\mathbf{r}^\top]_2\big) \end{aligned}$$

This relies on:

- change of variables $\mathbf{d} \mapsto \mathbf{d} - s_\ell^{-1}\Delta\cdot\mathbf{f}$; this ensures that, for all s_ℓ and Δ, we have

  $$\overbrace{\{(\boxed{\mathbf{d} + s_\ell^{-1}\Delta\cdot\mathbf{f}})\mathbf{M}_{x^*_\ell} + \mathbf{w}_{x^*_\ell,\bar\ell}\mathbf{R}, \boxed{-\mathbf{d}} + \mathbf{z}_{\text{end}}\mathbf{R}, \mathbf{R}\}}^{\mathsf{sk}^{\ell}_{\Gamma,x^*_\ell,\mathbf{f}}[2]} \approx_s \overbrace{\{\colorbox{lightgray}{$\mathbf{d}$}\mathbf{M}_{x^*_\ell} + \mathbf{w}_{x^*_\ell,\bar\ell}\mathbf{R}, \colorbox{lightgray}{$-\mathbf{d} + s_\ell^{-1}\Delta\cdot\mathbf{f}$} + \mathbf{z}_{\text{end}}\mathbf{R}, \mathbf{R}\}}^{\mathsf{sk}^{\ell,*}_{\Gamma}[2]}$$

  in the presence of $\mathbf{w}_{x^*_\ell,\bar\ell}, \mathbf{z}_{\text{end}}$ leaked via $\mathsf{ct}^{\ell}_{x^*}[2]$.
- $\mathrm{DDH}^{G_2}_{1,Q}$ assumption w.r.t $\mathbf{w}_{\text{start}}, \mathbf{z}_0, \mathbf{z}_1, \{\mathbf{w}_{\sigma,\bar\ell}\}_{\sigma\neq x^*_\ell}, \{\mathbf{w}_{\sigma,1-\bar\ell}\}_{\sigma\in\Sigma}$; this implies that

  $$\big([\mathbf{w}_{\text{start}}\mathbf{R}]_2, [\mathbf{z}_0\mathbf{R}]_2, [\mathbf{z}_1\mathbf{R}]_2, \big\{[\mathbf{w}_{\sigma,\bar\ell}\mathbf{R}]_2\big\}_{\sigma\neq x^*_\ell}, \big\{[\mathbf{w}_{\sigma,1-\bar\ell}\mathbf{R}]_2\big\}_{\sigma\in\Sigma}, [\mathbf{R}]_2\big) \approx_c U\big((G_2^{1\times Q})^{2|\Sigma|+2} \times G_2^{k\times Q}\big)$$

  and will be used to hide all $\mathbf{d}$'s irrelevant with the change of variables. □

Switching ciphertexts. We show that $\widehat{\mathsf{H}}^0_{2.i.2}(u_0,u_1) \approx_c \widehat{\mathsf{H}}^1_{2.i.2}(u_0,u_1)$ and $\widehat{\mathsf{H}}^0_{2.i.4}(u_0,u_1) \approx_c \widehat{\mathsf{H}}^1_{2.i.4}(u_0,u_1)$ for all $i \in [\ell]$ and all u_0, u_1. The proofs for them are similar. We begin with the following lemma for the former one and sketch the proof for the latter.

Lemma 48. *For all $i = 1,\ldots,\ell$, $u_0, u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle\mathcal{A}, \widehat{\mathsf{H}}^0_{2.i.2}(u_0,u_1)\rangle = 1] - \Pr[\langle\mathcal{A}, \widehat{\mathsf{H}}^1_{2.i.2}(u_0,u_1)\rangle = 1] \le \mathsf{Adv}^{\text{EXT-SWITCH}}_{\mathcal{B}}(\lambda).$$

Overview. Fix Γ and x^*. We will prove that

$$\big(\mathsf{mpk},\ \mathsf{aux}_1, \boxed{\mathsf{aux}_2}, \boxed{\mathsf{ct}_{x^*}^{i-1}}, \mathsf{sk}_{\Gamma,\mathbf{f}_{i-1,x^*}}^{i-1,i}\big) \approx_c \big(\mathsf{mpk},\ \mathsf{aux}_1, \boxed{\mathsf{aux}_2}, \colorbox{lightgray}{$\mathsf{ct}_{x^*}^{i-1,i}$}, \mathsf{sk}_{\Gamma,\mathbf{f}_{i-1,x^*}}^{i-1,i}\big)$$

which roughly means that

$$\overbrace{[\mathbf{s}_i\mathbf{A}_1]_1}^{\mathsf{ct}_{x^*}^{i-1}} \approx_c \overbrace{[\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2]}^{\mathsf{ct}_{x^*}^{i-1,i}} \quad \text{given} \quad \boxed{\overbrace{[\mathbf{a}_2^{\parallel}\cdot s_{\mathrm{end}}^{-1}\Delta + \mathbf{W}_{\mathrm{end}}\mathbf{r}^{\top}]_2}^{\mathsf{aux}_2}}, \overbrace{[-\mathbf{D} + \mathbf{a}_2^{\parallel}\cdot s_{i-1}^{-1}\Delta\cdot\mathbf{f}_{i-1,x^*} + \mathbf{Z}_\tau\mathbf{R}]_2}^{\mathsf{sk}_{\Gamma,\mathbf{f}_{i-1,x^*}}^{i-1,i}}.$$

This is similar to Lemma 14 stating that $\mathsf{G}_{2.i.1} \approx_c \mathsf{G}_{2.i.2}$ except that we need to simulate an extra term involving $\mathbf{a}_2^{\parallel}$ from aux_2 (highlighted by dashed box). Therefore, we use an extension of $(\mathbf{s}_i, \mathbf{Z}_\tau)$-switching lemma (Lemma 49) so that we can simulate the challenge ciphertext and secret key as in the proof of Lemma 14 and also handle aux_2.

Lemma 49 **($(\mathbf{s},\mathbf{Z},\mathbf{W})$-switching lemma).** *We have*

$$\begin{aligned}
&\mathsf{aux},\ [\mathbf{s}\mathbf{A}_1]_1, && [\mathbf{a}_2^{\parallel}\cdot\bar{\Delta} + \mathbf{Z}\mathbf{t}^{\top}]_2, && [\mathbf{W}\mathbf{t}^{\top}]_2,\ [\mathbf{t}^{\top}]_2\\
& && [\mathbf{Z}\mathbf{r}^{\top}]_2,\ [\mathbf{a}_2^{\parallel}\cdot\bar{\Delta} + \mathbf{W}\mathbf{r}^{\top}]_2, && [\mathbf{r}^{\top}]_2\\
\approx_c\ &\mathsf{aux},\ [\mathbf{s}\mathbf{A}_1 + \boxed{s\mathbf{a}_2}]_1, && [\mathbf{a}_2^{\parallel}\cdot\bar{\Delta} + \mathbf{Z}\mathbf{t}^{\top}]_2, && [\mathbf{W}\mathbf{t}^{\top}]_2,\ [\mathbf{t}^{\top}]_2\\
& && [\mathbf{Z}\mathbf{r}^{\top}]_2,\ [\mathbf{a}_2^{\parallel}\cdot\bar{\Delta} + \mathbf{W}\mathbf{r}^{\top}]_2, && [\mathbf{r}^{\top}]_2
\end{aligned}$$

where $\mathsf{aux} = ([\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_1\mathbf{Z}, \mathbf{a}_2\mathbf{Z}, \mathbf{A}_1\mathbf{W}, \mathbf{a}_2\mathbf{W}]_1, [\mathbf{Z}\mathbf{B}, \mathbf{W}\mathbf{B}, \mathbf{B}]_2)$ *and* $\mathbf{Z}, \mathbf{W} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{s}, \mathbf{r}, \mathbf{t} \leftarrow \mathbb{Z}_p^{1\times k}$, $s, \bar{\Delta} \leftarrow \mathbb{Z}_p$. *Concretely, the advantage function* $\mathsf{Adv}_{\mathcal{B}}^{\text{EXT-SWITCH}}(\lambda)$ *is bounded by* $O(1)\cdot\mathsf{Adv}_{\mathcal{B}_0}^{k\text{-LIN}}(\lambda)$ *with* $\mathsf{Time}(\mathcal{B}_0) \approx \mathsf{Time}(\mathcal{B})$.

The proof for Lemma 49 is similar to that for the original $(\mathbf{s},\mathbf{W})$-switching lemma, cf. [11]. We omit the proof here.

Proof (of Lemma 48). We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\boxed{\{i-1\}}, \{i-1, i\}, \perp, \mathbf{f}_{i-1,x^*}),\ \ u_1 = (\colorbox{lightgray}{$\{i-1, i\}$}, \{i-1, i\}, \perp, \mathbf{f}_{i-1,x^*});$$

the lemma trivially holds in other cases. Recall that $\tau = i \bmod 2$. We prove the lemma using $(\mathbf{s}_i, \mathbf{Z}_\tau, \mathbf{W}_{\mathrm{end}})$-switching lemma. On input

$$\begin{aligned}
&\mathsf{aux},\ [\mathbf{c}_i]_1,\ [\mathbf{a}_2^{\parallel}\cdot\bar{\Delta} + \mathbf{Z}_\tau\mathbf{t}^{\top}]_2, && [\mathbf{W}_{\mathrm{end}}\mathbf{t}^{\top}]_2,\ [\mathbf{t}^{\top}]_2\\
& [\mathbf{Z}_\tau\mathbf{r}^{\top}]_2,\ [\mathbf{a}_2^{\parallel}\cdot\bar{\Delta} + \mathbf{W}_{\mathrm{end}}\mathbf{r}^{\top}]_2, && [\mathbf{r}^{\top}]_2
\end{aligned}$$

where $\mathsf{aux} = ([\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_1\mathbf{Z}_\tau, \mathbf{a}_2\mathbf{Z}_\tau, \mathbf{A}_1\mathbf{W}_{\mathrm{end}}, \mathbf{a}_2\mathbf{W}_{\mathrm{end}}]_1, [\mathbf{Z}_\tau\mathbf{B}, \mathbf{W}_{\mathrm{end}}\mathbf{B}, \mathbf{B}]_2)$ and $\mathbf{Z}_\tau$, $\mathbf{W}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{r}, \mathbf{t} \leftarrow \mathbb{Z}_p^{1\times k}$, $\bar{\Delta} \leftarrow \mathbb{Z}_p$ and

$$\mathbf{c}_i = \boxed{\mathbf{s}_i\mathbf{A}_1} \text{ or } \mathbf{c}_i = \colorbox{lightgray}{$\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$},\quad \mathbf{s}_i \leftarrow \mathbb{Z}_p^{1\times k}, s_i \leftarrow \mathbb{Z}_p$$

the reduction works as follows:

(Simulating mpk and aux_1) We sample $\mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$, $\mathbf{W}_{\mathrm{start}}, \mathbf{Z}_{1-\tau}, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{Z}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ for all $\sigma \in \Sigma$, and then we can trivially simulate mpk from $[\mathbf{A}_1, \mathbf{A}_1\mathbf{Z}_\tau, \mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1$ and simulate aux_1 from $[\mathbf{Z}_\tau\mathbf{B}, \mathbf{W}_{\mathrm{end}}\mathbf{B}, \mathbf{B}]_2$.

(Simulating aux_2) We sample $s_{\mathrm{end}} \leftarrow \mathbb{Z}_p$ and implicitly set $\Delta = s_{\mathrm{end}}\bar{\Delta}$; then we can rewrite aux_2 as

$$\boxed{[\mathbf{r}^{\top}]_2}, [\mathbf{W}_{\mathrm{start}}\mathbf{r}^{\top}]_2, \boxed{[\mathbf{Z}_\tau\mathbf{r}^{\top}]_2}, [\mathbf{Z}_{1-\tau}\mathbf{r}^{\top}]_2, \{[\mathbf{W}_{\sigma,0}\mathbf{r}^{\top}]_2, [\mathbf{W}_{\sigma,1}\mathbf{r}^{\top}]_2\}_{\sigma\in\Sigma}, [\mathbf{Z}_{\mathrm{end}}\mathbf{r}^{\top}]_2, \boxed{[\mathbf{a}_2^{\parallel}\cdot\bar{\Delta} + \mathbf{W}_{\mathrm{end}}\mathbf{r}^{\top}]_2}.$$

All terms in the dashed boxes are provided in the lemma; all remaining terms can be simulated using $[\mathbf{r}^{\top}]_2$ and $\mathbf{W}_{\mathrm{start}}$, $\mathbf{Z}_{1-\tau}$, $\mathbf{W}_{\sigma,0}$, $\mathbf{W}_{\sigma,1}$, $\mathbf{Z}_{\mathrm{end}}$.

(Answering OEnc**)** On input (x^*, m), we want to create a ciphertext in the following form, which is either $\mathsf{ct}_{x^*}^{i-1}$ or $\mathsf{ct}_{x^*}^{i-1,i}$ depending on $\mathbf{c}_i$:

$$\begin{pmatrix} [\mathbf{c}_0]_1,\ [\mathbf{c}_0\mathbf{W}_{\mathrm{start}}]_1 \\ \big\{[\mathbf{c}_j]_1, \boxed{[\mathbf{c}_{j-1}\mathbf{Z}_\tau]_1} \cdot [\mathbf{c}_j\mathbf{W}_{x_j,\tau}]_1\big\}_{j=i \bmod 2} \\ \big\{[\mathbf{c}_j]_1, [\mathbf{c}_{j-1}\mathbf{Z}_{1-\tau}]_1 \cdot [\mathbf{c}_j\mathbf{W}_{x_j,1-\tau}]_1\big\}_{j\neq i \bmod 2} \\ [\mathbf{c}_{\mathrm{end}}]_1, [\mathbf{c}_\ell\mathbf{Z}_{\mathrm{end}}]_1 \cdot \boxed{[\mathbf{c}_{\mathrm{end}}\mathbf{W}_{\mathrm{end}}]_1}, [\mathbf{c}_{\mathrm{end}}\mathbf{k}^\top]_T \cdot m \end{pmatrix} \quad \text{where} \quad \begin{cases} \mathbf{c}_i \in \{\boxed{\mathbf{s}_i\mathbf{A}_1}, \mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2\} \\ \mathbf{c}_{i-1} = \mathbf{s}_{i-1}\mathbf{A}_1 + s_{i-1}\mathbf{a}_2 \\ \mathbf{c}_{\mathrm{end}} = \mathbf{s}_{\mathrm{end}}\mathbf{A}_1 + s_{\mathrm{end}}\mathbf{a}_2 \\ \mathbf{c}_j = \mathbf{s}_j\mathbf{A}_1 \quad \text{if } j \notin \{i-1, i\} \end{cases}$$

Observe that,

- when $\mathbf{c}_i = \boxed{\mathbf{s}_i\mathbf{A}_1}$, the distribution is identical to $\boxed{\mathsf{ct}_{x^*}^{i-1}}$;
- when $\mathbf{c}_i = \mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$, the distribution is identical to $\mathsf{ct}_{x^*}^{i-1,i}$.

We proceed as follows:

- We sample $\mathbf{s}_j \leftarrow \mathbb{Z}_p^{1\times k}$ for all $j \neq i$, $s_{i-1} \leftarrow \mathbb{Z}_p$ and simulate $\{[\mathbf{c}_j]_1\}_{j\neq i}$ and $[\mathbf{c}_{\mathrm{end}}]_1$ using $[\mathbf{A}_1, \mathbf{a}_2]_1$; note that $[\mathbf{c}_i]_1$ is given out in the lemma as the challenge term.
- We rewrite terms in the first dashed box as:

$$[\mathbf{c}_j\mathbf{Z}_\tau]_1 = \begin{cases} [\mathbf{s}_j\mathbf{A}_1\mathbf{Z}_\tau]_1 & \text{if } j \neq i-1 \text{ and } j \neq i \bmod 2 \\ [\mathbf{s}_{i-1}\mathbf{A}_1\mathbf{Z}_\tau]_1 \cdot [s_{i-1}\mathbf{a}_2\mathbf{Z}_\tau]_1 & \text{if } j = i-1\,(\text{and } j \neq i \bmod 2) \end{cases}$$

  which can be simulated using $\{\mathbf{s}_j\}_{j\neq i \bmod 2}$, s_{i-1} and $[\mathbf{A}_1\mathbf{Z}_\tau, \mathbf{a}_2\mathbf{Z}_\tau]_1$; here we use the fact that we do not have any terms involving $[\mathbf{c}_i\mathbf{Z}_\tau]_1$ in the ciphertext.
- We write term in the second dashed box as:

$$[\mathbf{c}_{\mathrm{end}}\mathbf{W}_{\mathrm{end}}]_1 = [\mathbf{s}_{\mathrm{end}}\mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1 \cdot [s_{\mathrm{end}}\mathbf{a}_2\mathbf{W}_{\mathrm{end}}]_1$$

  which can be simulated using $\mathbf{s}_{\mathrm{end}}, s_{\mathrm{end}}$ and $[\mathbf{A}_1\mathbf{W}_{\mathrm{end}}, \mathbf{a}_2\mathbf{W}_{\mathrm{end}}]_1$; here we use the fact that we do not have any terms involving $[\mathbf{s}_i\mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1$ in the ciphertext.
- We simulate all remaining terms using $\{[\mathbf{c}_j]_1\}_{j\in[0,\ell]}, [\mathbf{c}_{\mathrm{end}}]_1$ and $\mathbf{k}, \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_{1-\tau}, \{\mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma}, \mathbf{Z}_{\mathrm{end}}$.

(Answering OKey**)** On input Γ, we want to return a secret key for Γ in the form

$$\mathsf{sk}_{\Gamma,\mathbf{f}_{i-1,x^*}}^{i-1,i} = \begin{pmatrix} [\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \big\{\boxed{[-\mathbf{D} + \mathbf{a}_2^{\parallel} \cdot s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*} + \mathbf{Z}_\tau\mathbf{R}]_2}, [\mathbf{D}\mathbf{M}_\sigma + \mathbf{W}_{\sigma,\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ \big\{[-\mathbf{D} + \mathbf{Z}_{1-\tau}\mathbf{R}]_2, [\mathbf{D}\mathbf{M}_\sigma + \mathbf{W}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [-\mathbf{D} + \mathbf{Z}_{\mathrm{end}}\mathbf{R}]_2, \boxed{[\mathbf{k}^\top\mathbf{f} + \mathbf{W}_{\mathrm{end}}\mathbf{R}]_2}, [\mathbf{R}]_2 \end{pmatrix}.$$

We sample $\mathbf{D} \leftarrow \mathbb{Z}_p^{(2k+1)\times Q}$ and $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{k\times Q}$ and implicitly set

$$\mathbf{R} = \mathbf{t}^\top \cdot s_{i-1}^{-1} s_{\mathrm{end}} \cdot \mathbf{f}_{i-1,x^*} + \mathbf{B} \cdot \widetilde{\mathbf{R}}.$$

We proceed to simulate $\mathsf{sk}_{\Gamma,\mathbf{f}_{i-1,x^*}}^{i-1,i}$ as follows:

- We simulate $[\mathbf{R}]_2$ from $[\mathbf{t}^\top]_2$, $[\mathbf{B}]_2$ and $\mathbf{f}_{i-1,x^*}, \widetilde{\mathbf{R}}, s_{i-1}, s_{\mathrm{end}}$.
- Recall that we set $\Delta = s_{\mathrm{end}}\bar{\Delta}$, we can rewrite terms in the dashed boxes as:

$$[-\mathbf{D} + (\mathbf{a}_2^{\parallel} \cdot \bar{\Delta} + \mathbf{Z}_\tau\mathbf{t}^\top) \cdot s_{i-1}^{-1} s_{\mathrm{end}} \cdot \mathbf{f}_{i-1,x^*} + \mathbf{Z}_\tau\mathbf{B} \cdot \widetilde{\mathbf{R}}]_2 \quad \text{and} \quad [\mathbf{k}^\top\mathbf{f} + \mathbf{W}_{\mathrm{end}}\mathbf{t}^\top \cdot s_{i-1}^{-1} s_{\mathrm{end}} \cdot \mathbf{f}_{i-1,x^*} + \mathbf{W}_{\mathrm{end}}\mathbf{B} \cdot \widetilde{\mathbf{R}}]_2$$

  which can be simulated using $[\mathbf{a}_2^{\parallel} \cdot \bar{\Delta} + \mathbf{Z}_\tau\mathbf{t}^\top]_2, [\mathbf{W}_{\mathrm{end}}\mathbf{t}^\top]_2, [\mathbf{Z}_\tau\mathbf{B}]_2, [\mathbf{W}_{\mathrm{end}}\mathbf{B}]_2$ and $\mathbf{D}, \mathbf{k}, \mathbf{f}_{i-1,x^*}, \widetilde{\mathbf{R}}, s_{i-1}, s_{\mathrm{end}}$.
- We simulate all remaining terms using $[\mathbf{R}]_2$ and $\mathbf{D}, \mathbf{W}_{\mathrm{start}}, \mathbf{Z}_{1-\tau}, \mathbf{W}_{\sigma,\tau}, \mathbf{W}_{\sigma,1-\tau}, \mathbf{Z}_{\mathrm{end}}$.

Observe that, when $\mathbf{c}_i = \boxed{\mathbf{s}_i\mathbf{A}_1}$, oracle $\mathsf{OEnc}(x^*, m)$ returns $\boxed{\mathsf{ct}_{x^*}^{i-1}}$ and the simulation is identical to $\widehat{\mathsf{H}}_{2.i.2}^0(u_0, u_1)$; when $\mathbf{c}_i = \colorbox{lightgray}{$\mathbf{s}_i\mathbf{A}_1 + s_i\mathbf{a}_2$}$, oracle $\mathsf{OEnc}(x^*, m)$ returns $\colorbox{lightgray}{$\mathsf{ct}_{x^*}^{i-1,i}$}$ and the simulation is identical to $\widehat{\mathsf{H}}_{2.i.2}^1(u_0, u_1)$. This completes the proof. □

Via the same proof idea, we can prove the following lemmas stating that $\widehat{\mathsf{H}}_{2.i.4}^0(u_0, u_1) \approx_c \mathsf{H}_{2.i.4}^1(u_0, u_1)$ for all $i \in [\ell]$ and all u_0, u_2. We only sketch the proof.

Lemma 50. *For all $i \in [\ell]$, $u_0, u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{2.i.4}^0(u_0, u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{2.i.4}^1(u_0, u_1)\rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\text{EXT-SWITCH}}(\lambda).$$

Proof (sketch). We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\boxed{\{i-1, i\}}, \{i\}, x_i^*, \mathbf{f}_{i,x^*}),\ \ u_1 = (\colorbox{lightgray}{$\{i\}$}, \{i\}, x_i^*, \mathbf{f}_{i,x^*});$$

the lemma trivially holds in other cases. Namely, we will prove that

$$\big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \boxed{\mathsf{ct}_{x^*}^{i-1,i}}, \mathsf{sk}_{\Gamma, x_i^*, \mathbf{f}_{i,x^*}}^i\big) \approx_c \big(\mathsf{mpk}, \mathsf{aux}_1, \mathsf{aux}_2, \colorbox{lightgray}{$\mathsf{ct}_{x^*}^i$}, \mathsf{sk}_{\Gamma, x_i^*, \mathbf{f}_{i,x^*}}^i\big)$$

which roughly means that

$$\overbrace{[\mathbf{s}_{i-1}\mathbf{A}_1 + s_{i-1}\mathbf{a}_2]_1}^{\mathsf{ct}_{x^*}^{i-1,i}} \approx_c \overbrace{[\mathbf{s}_{i-1}\mathbf{A}_1]_1}^{\mathsf{ct}_{x^*}^i} \quad \text{given} \quad \overbrace{[\mathbf{a}_2^{\parallel} \cdot s_{\mathrm{end}}^{-1}\Delta + \mathbf{W}_{\mathrm{end}}\mathbf{r}^{\top}]_2}^{\mathsf{aux}_2}, \overbrace{[\mathbf{D}\mathbf{M}_{x_i^*} + \mathbf{a}_2^{\parallel} \cdot s_i^{-1}\Delta \cdot \mathbf{f}_{i,x^*} + \mathbf{W}_{x_i^*,\tau}\mathbf{R}]_2}^{\mathsf{sk}_{\Gamma, x_i^*, \mathbf{f}_{i,x^*}}^i}.$$

The proof is analogous to that of Lemma 48 except that we use $(\mathbf{s}_{i-1}, \mathbf{W}_{x_i^*,\tau}, \mathbf{W}_{\mathrm{end}})$- instead of $(\mathbf{s}_i, \mathbf{Z}_\tau, \mathbf{W}_{\mathrm{end}})$-switching lemma so that we can simulate the challenge ciphertext from the challenge term in the lemma and simulate both secret key and aux_2 using the auxiliary terms given out in the lemma. □

Switching secret keys II. We show that $\widehat{\mathsf{H}}_{2.i.3}^0(u_0, u_1) \approx_c \widehat{\mathsf{H}}_{2.i.3}^1(u_0, u_1)$ and $\widehat{\mathsf{H}}_4^0(u_0, u_1) \approx_c \widehat{\mathsf{H}}_4^1(u_0, u_1)$ for all $i \in [\ell]$ and u_0, u_1. The proofs for them are similar. We begin with the following lemma stating that $\widehat{\mathsf{H}}_{2.i.3}^0(u_0, u_1) \approx_c \widehat{\mathsf{H}}_{2.i.3}^1(u_0, u_1)$, which is analogous to Lemma 17, and sketch the proof for the latter one.

Lemma 51. *For all $i \in [\ell]$, $u_0, u_1 \in I \times I \times \Sigma \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{2.i.3}^0(u_0, u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}_{2.i.3}^1(u_0, u_1)\rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\text{TRANS}}(\lambda).$$

Proof. We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\{i-1, i\}, \boxed{\{i-1, i\}, \perp, \mathbf{f}_{i-1,x^*}}),\ \ u_1 = (\{i-1, i\}, \colorbox{lightgray}{$\{i\}, x_i^*, \mathbf{f}_{i,x^*}$});$$

the lemma trivially holds in other cases. Recall that $\tau = i \bmod 2$. By Lemma 4, it suffices to prove the lemma over $\mathbf{a}_2$-components which roughly means:

$$\mathsf{sk}_{\Gamma, \mathbf{f}_{i-1,x^*}}^{i-1,i}[2] = \begin{pmatrix} [\mathbf{d}\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^{\top}]_2, [\mathbf{R}\mathbf{u}^{\top}]_2 \\ [-\mathbf{d} + \boxed{s_{i-1}^{-1}\Delta \cdot \mathbf{f}_{i-1,x^*} + \mathbf{z}_\tau\mathbf{R}}]_2, [\mathbf{d}\mathbf{M}_{x_i^*} + \boxed{\mathbf{w}_{x_i^*,\tau}\mathbf{R}}]_2, [\mathbf{R}]_2 \\ \{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\}_{\sigma \ne x_i^*} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma \in \Sigma} \\ [-\mathbf{d} + \mathbf{z}_{\mathrm{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}$$

$$\approx_c \begin{pmatrix} [\mathbf{d}\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^{\top}]_2, [\mathbf{R}\mathbf{u}^{\top}]_2 \\ [-\mathbf{d} + \colorbox{lightgray}{$\mathbf{z}_\tau\mathbf{R}$}]_2, [\mathbf{d}\mathbf{M}_{x_i^*} + \colorbox{lightgray}{$s_i^{-1}\Delta \cdot \mathbf{f}_{i,x^*}\mathbf{M}_{x_i^*} + \mathbf{w}_{x_i^*,\tau}\mathbf{R}$}]_2, [\mathbf{R}]_2 \\ \{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\}_{\sigma \ne x_i^*} \\ \{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma \in \Sigma} \\ [-\mathbf{d} + \mathbf{z}_{\mathrm{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} = \mathsf{sk}_{\Gamma, x_i^*, \mathbf{f}_{i,x^*}}^i[2]$$

in the presence of

$$\mathsf{ct}_{x^*}^{i-1,i}[2] = \begin{cases} [s_0\mathbf{w}_{\mathrm{start}}]_1,\, [s_0]_1,\, [s_0\mathbf{z}_1 + s_1\mathbf{w}_{x_1^*,1}]_1,\, [s_1]_1,\, [s_1\mathbf{z}_0]_1,\, [s_{\mathrm{end}}\mathbf{w}_{\mathrm{end}}]_1,\, [s_{\mathrm{end}}]_1,\, [s_{\mathrm{end}}\alpha]_T\cdot m & \text{if } i=1 \\ [s_{i-1}\mathbf{w}_{x_{i-1}^*,1-\tau}]_1,\, [s_{i-1}]_1,\, [s_{i-1}\mathbf{z}_\tau + s_i\mathbf{w}_{x_i^*,\tau}]_1,\, [s_i]_1,\, [s_i\mathbf{z}_{1-\tau}]_1,\, [s_{\mathrm{end}}\mathbf{w}_{\mathrm{end}}]_1,\, [s_{\mathrm{end}}]_1,\, [s_{\mathrm{end}}\alpha]_T\cdot m & \text{if } i\in[2,\ell-1] \\ [s_{\ell-1}\mathbf{w}_{x_{\ell-1}^*,1-\bar{\ell}}]_1,\, [s_{\ell-1}]_1,\, [s_{\ell-1}\mathbf{z}_{\bar{\ell}} + s_\ell\mathbf{w}_{x_\ell^*,\bar{\ell}}]_1,\, [s_\ell]_1,\, [s_\ell\mathbf{z}_{\mathrm{end}} + s_{\mathrm{end}}\mathbf{w}_{\mathrm{end}}]_1,\, [s_{\mathrm{end}}]_1,\, [s_{\mathrm{end}}\alpha]_T\cdot m & \text{if } i=\ell \end{cases}$$

and

$$\begin{aligned} \mathsf{aux}_1[2] &= \big([\alpha, \mathbf{B}, \mathbf{w}_{\mathrm{start}}\mathbf{B}, \mathbf{z}_0\mathbf{B}, \mathbf{z}_1\mathbf{B}, \{\mathbf{w}_{\sigma,0}\mathbf{B}, \mathbf{w}_{\sigma,1}\mathbf{B}\}_{\sigma\in\Sigma}, \mathbf{z}_{\mathrm{end}}\mathbf{B}, \mathbf{w}_{\mathrm{end}}\mathbf{B}]_2\big) \\ \mathsf{aux}_2[2] &= \big([\mathbf{r}^\top, \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top, \mathbf{z}_0\mathbf{r}^\top, \mathbf{z}_1\mathbf{r}^\top, \{\mathbf{w}_{\sigma,0}\mathbf{r}^\top, \mathbf{w}_{\sigma,1}\mathbf{r}^\top\}_{\sigma\in\Sigma}, \mathbf{z}_{\mathrm{end}}\mathbf{r}^\top, s_{\mathrm{end}}^{-1}\Delta + \mathbf{w}_{\mathrm{end}}\mathbf{r}^\top]_2\big) \end{aligned}$$

One can sample basis $\mathbf{A}_1, \mathbf{a}_2, \mathbf{A}_3, \mathbf{A}_1^{\parallel}, \mathbf{a}_2^{\parallel}, \mathbf{A}_3^{\parallel}$ and trivially simulate mpk, $\mathsf{ct}_{x^*}^{i-1,i}$ and secret key using terms given out above. Furthermore, we prove this using $(\mathbf{z}_\tau, \mathbf{w}_{x_i^*,\tau})$-transition lemma. On input

$$\mathsf{aux}, [\bar{\Delta}_0 + \mathbf{z}_\tau\mathbf{r}^\top]_2, [\bar{\Delta}_1 + \mathbf{w}_{x_i^*,\tau}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2$$

where $(\bar{\Delta}_0, \bar{\Delta}_1) \in \big\{\boxed{(s_{i-1}^{-1}\bar{\Delta}, 0)}, \colorbox{lightgray}{$(0, s_i^{-1}\bar{\Delta})$}\big\}$ and $\mathsf{aux} = (\bar{\Delta}, s_{i-1}, s_i, s_{i-1}\mathbf{z}_\tau + s_i\mathbf{w}_{x_i^*,\tau},\, [\mathbf{z}_\tau\mathbf{B}, \mathbf{w}_{x_i^*,\tau}\mathbf{B}, \mathbf{B}]_2)$ with $\mathbf{z}_\tau, \mathbf{w}_{x_i^*,\tau} \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$, $\mathbf{r} \leftarrow \mathbb{Z}_p^{1\times k}$ and $\Delta \leftarrow \mathbb{Z}_p$, we sample $\alpha \leftarrow \mathbb{Z}_p, \mathbf{w}_{\mathrm{start}}, \mathbf{z}_{1-\tau}, \mathbf{w}_{\sigma,1-\tau}, \mathbf{z}_{\mathrm{end}}, \mathbf{w}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1\times k}$ for all $\sigma \in \Sigma$ and $\mathbf{w}_{\sigma,\tau} \leftarrow \mathbb{Z}_p^{1\times k}$ for all $\sigma \neq x_i^*$ and proceed as follows:

(Simulating aux_1 **and** aux_2**)** We sample $s_{\mathrm{end}} \leftarrow \mathbb{Z}_p$ and implicitly set $\Delta = \bar{\Delta}$. Then we can simulate $\mathsf{aux}_1[2], \mathsf{aux}_2[2]$ from $[\mathbf{z}_\tau\mathbf{B}, \mathbf{w}_{x_i^*,\tau}\mathbf{B}, \mathbf{B}]_2$ and $\bar{\Delta}$ given out in aux along with s_{end}, α, $\mathbf{w}_{\mathrm{start}}$, $\mathbf{z}_{1-\tau}$, $\{\mathbf{w}_{\sigma,1-\tau}\}_{\sigma\in\Sigma}$, $\{\mathbf{w}_{\sigma,\tau}\}_{\sigma\neq x_i^*}$, $\mathbf{z}_{\mathrm{end}}$, $\mathbf{w}_{\mathrm{end}}$.

(Answering OEnc**)** On input (x^*, m), we trivially simulate $\mathsf{ct}_{x^*}^{i-1,i}[2]$ using s_{i-1}, s_i, $s_{i-1}\mathbf{z}_\tau + s_i\mathbf{w}_{x_i^*,\tau}$ in aux and s_{end}, α, $\mathbf{w}_{\mathrm{start}}$, $\mathbf{w}_{\sigma,1-\tau}$, $\mathbf{z}_{1-\tau}$, $\mathbf{z}_{\mathrm{end}}$, $\mathbf{w}_{\mathrm{end}}$.

(Answering OKey**)** On input Γ, we want to return a key for Γ in the form:

$$\begin{pmatrix} [\mathbf{d}\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{R}\mathbf{u}^\top]_2, [\mathbf{R}\mathbf{u}^\top]_2 \\ \boxed{[-\mathbf{d} + \Delta_0\cdot\mathbf{f}_{i-1,x^*} + \mathbf{z}_\tau\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_{x_i^*} + \Delta_1\cdot\mathbf{f}_{i-1,x^*} + \mathbf{w}_{x_i^*,\tau}\mathbf{R}]_2}, [\mathbf{R}]_2 \\ \big\{[\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,\tau}\mathbf{R}]_2\big\}_{\sigma\neq x_i^*} \\ \big\{[-\mathbf{d} + \mathbf{z}_{1-\tau}\mathbf{R}]_2, [\mathbf{d}\mathbf{M}_\sigma + \mathbf{w}_{\sigma,1-\tau}\mathbf{R}]_2, [\mathbf{R}]_2\big\}_{\sigma\in\Sigma} \\ [-\mathbf{d} + \mathbf{z}_{\mathrm{end}}\mathbf{R}]_2, [\alpha\mathbf{f} + \mathbf{w}_{\mathrm{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix} \text{ where } (\Delta_0, \Delta_1) \in \big\{\boxed{(s_{i-1}^{-1}\Delta, 0)}, \colorbox{lightgray}{$(0, s_i^{-1}\Delta)$}\big\}.$$

Observe that

- when $(\Delta_0, \Delta_1) = \boxed{(s_{i-1}^{-1}\Delta, 0)}$, the distribution is identical to $\boxed{\mathsf{sk}_{\Gamma,\mathbf{f}_{i-1,x^*}}^{i-1,i}[2]}$;
- when $(\Delta_0, \Delta_1) = \colorbox{lightgray}{$(0, s_i^{-1}\Delta)$}$, the distribution is identical to $\colorbox{lightgray}{$\mathsf{sk}_{\Gamma,x_i^*,\mathbf{f}_{i,x^*}}^{i}[2]$}$ since $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{x_i^*} \bmod p$, see Lemma 5.

Recall that we set $\Delta = \bar{\Delta}$ which means we also implicitly set

$$(\Delta_0, \Delta_1) = (\bar{\Delta}_0, \bar{\Delta}_1).$$

We sample $\mathbf{d} \leftarrow \mathbb{Z}_p^{1\times Q}$ and $\widetilde{\mathbf{R}} \leftarrow \mathbb{Z}_p^{k\times Q}$ and implicitly set

$$\mathbf{R} = \mathbf{r}^\top\cdot\mathbf{f}_{i-1,x^*} + \mathbf{B}\cdot\widetilde{\mathbf{R}}.$$

We then generate the key for Γ as follows:

- We simulate $[\mathbf{R}]_2$ from $[\mathbf{r}^\top]_2, [\mathbf{B}]_2$ and $\mathbf{f}_{i-1,x^*}, \widetilde{\mathbf{R}}$.

- We rewrite the terms in the dashed box as follows:

$$[-\mathbf{d}+(\bar{\Delta}_0+\mathbf{z}_\tau\mathbf{r}^\top)\cdot\mathbf{f}_{i-1,x^*}+\mathbf{z}_\tau\mathbf{B}\cdot\widetilde{\mathbf{R}}]_2,\ [\mathbf{d}\mathbf{M}_{x_i^*}+(\bar{\Delta}_1+\mathbf{w}_{x_i^*,\tau}\mathbf{r}^\top)\cdot\mathbf{f}_{i-1,x^*}+\mathbf{w}_{x_i^*,\tau}\mathbf{B}\cdot\widetilde{\mathbf{R}}]_2$$

  and simulate them using $[\bar{\Delta}_0+\mathbf{z}_\tau\mathbf{r}^\top]_2, [\bar{\Delta}_1+\mathbf{w}_{x_i^*,\tau}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2, [\mathbf{z}_\tau\mathbf{B}]_2, [\mathbf{w}_{x_i^*,\tau}\mathbf{B}]_2$ and $\mathbf{d}, \mathbf{f}_{i-1,x^*}, \widetilde{\mathbf{R}}$.
- We simulate all remaining terms using $[\mathbf{R}]_2$ and $\mathbf{d}$, $\mathbf{w}_{\text{start}}$, $\mathbf{z}_{1-\tau}$, $\{\mathbf{w}_{\sigma,\tau}\}_{\sigma\neq x_i^*}$, $\{\mathbf{w}_{\sigma,1-\tau}\}_{\sigma\in\Sigma}$, $\mathbf{z}_{\text{end}}$, $\mathbf{w}_{\text{end}}$.

Observe that, when $(\bar{\Delta}_0,\bar{\Delta}_1)=\boxed{(s_{i-1}^{-1}\bar{\Delta},0)}$, we have $(\Delta_0,\Delta_1)=\boxed{(s_{i-1}^{-1}\Delta,0)}$, then oracle $\mathsf{OKey}(\Gamma)$ returns $\boxed{\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{f}_{i-1,x^*}}\ [2]}$ and the simulation is identical to $\widehat{\mathsf{H}}^0_{2.i.3}(u_0,u_1)$; when $(\bar{\Delta}_0,\bar{\Delta}_1)=\colorbox{lightgray}{$(0,s_i^{-1}\bar{\Delta})$}$, we have $(\Delta_0,\Delta_1)=\colorbox{lightgray}{$(0,s_i^{-1}\Delta)$}$, then oracle $\mathsf{OKey}(\Gamma)$ returns $\colorbox{lightgray}{$\mathsf{sk}^{i}_{\Gamma,x_i^*,\mathbf{f}_{i,x^*}}\ [2]$}$ and the simulation is identical to $\widehat{\mathsf{H}}^1_{2.i.3}(u_0,u_1)$. This completes the proof. □

Via the same proof idea, we can prove the following lemmas stating that $\widehat{\mathsf{H}}^0_4(u_0,u_1)\approx_c\widehat{\mathsf{H}}^1_4(u_0,u_1)$ for all u_0,u_2. We only sketch the proof.

Lemma 52. *For all $u_0,u_1\in I\times I\times\Sigma\times\mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B})\approx\mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle\mathcal{A},\widehat{\mathsf{H}}^0_4(u_0,u_1)\rangle=1]-\Pr[\langle\mathcal{A},\widehat{\mathsf{H}}^1_4(u_0,u_1)\rangle=1]\leq\mathsf{Adv}^{\text{TRANS}}_{\mathcal{B}}(\lambda).$$

Proof (sketch). We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0=(\{\ell\},\boxed{\{\ell,*\}},\perp,\perp),\ u_1=(\{\ell\},\colorbox{lightgray}{$\{*\}$},\perp,\perp);$$

the lemma trivially holds in other cases. Namely, we will prove that

$$\big(\mathsf{mpk},\mathsf{aux}_1,\mathsf{aux}_2,\mathsf{ct}^{\ell}_{x^*},\boxed{\mathsf{sk}^{\ell,*}_{\Gamma}}\big)\approx_c\big(\mathsf{mpk},\mathsf{aux}_1,\mathsf{aux}_2,\mathsf{ct}^{\ell}_{x^*},\colorbox{lightgray}{sk^{*}_{Γ}}\big);$$

which roughly means that we need to show:

$$\begin{array}{rrll} & [-\mathbf{d}+\boxed{s_\ell^{-1}\Delta\cdot\mathbf{f}+\mathbf{z}_{\text{end}}\mathbf{R}}]_2, & [\alpha\mathbf{f}+\boxed{\mathbf{w}_{\text{end}}\mathbf{R}}]_2,\ [\mathbf{R}]_2 & //\mathsf{sk}^{\ell,*}_{\Gamma} \\ \approx_c & [-\mathbf{d}+\colorbox{lightgray}{$\mathbf{z}_{\text{end}}\mathbf{R}$}]_2, & [\alpha\mathbf{f}+\colorbox{lightgray}{$s_{\text{end}}^{-1}\Delta\cdot\mathbf{f}+\mathbf{w}_{\text{end}}\mathbf{R}$}]_2,\ [\mathbf{R}]_2 & //\mathsf{sk}^{*}_{\Gamma} \end{array}$$

given $\mathbf{d},\alpha,\Delta,s_\ell,s_{\text{end}},s_\ell\mathbf{z}_{\text{end}}+s_{\text{end}}\mathbf{w}_{\text{end}}$. This can be handled using $(\mathbf{z}_{\text{end}},\mathbf{w}_{\text{end}})$-transition lemma. □

F Concrete ABE for DFA with Adaptive Security

In this section, we show our concrete ABE for DFA with adaptive security. This is derived from our adaptively secure ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in Section 5.1 and the transformation from DFA to $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in Section 3, see Lemma 1.

- $\mathsf{Setup}(1^\lambda,\Sigma)$: Run $\mathbb{G}=(p,G_1,G_2,G_T,e)\leftarrow\mathcal{G}(1^\lambda)$. Sample

$$\mathbf{A}_1\leftarrow\mathbb{Z}_p^{k\times(2k+1)},\mathbf{k}\leftarrow\mathbb{Z}_p^{1\times(2k+1)}\quad\text{and}\quad\mathbf{W}_{\text{start}},\mathbf{Z}_0,\mathbf{Z}_1,\mathbf{W}_{\sigma,0},\mathbf{W}_{\sigma,1},\mathbf{Z}_{\text{end}},\mathbf{W}_{\text{end}}\leftarrow\mathbb{Z}_p^{(2k+1)\times k},\forall\sigma\in\Sigma.$$

  Output

$$\begin{aligned}\mathsf{mpk}&=\big([\mathbf{A}_1,\mathbf{A}_1\mathbf{W}_{\text{start}},\mathbf{A}_1\mathbf{Z}_0,\mathbf{A}_1\mathbf{Z}_1,\{\mathbf{A}_1\mathbf{W}_{\sigma,0},\mathbf{A}_1\mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma},\mathbf{A}_1\mathbf{Z}_{\text{end}},\mathbf{A}_1\mathbf{W}_{\text{end}}]_1,[\mathbf{A}_1\mathbf{k}^\top]_T\big)\\ \mathsf{msk}&=\big(\mathbf{k},\mathbf{W}_{\text{start}},\mathbf{Z}_0,\mathbf{Z}_1,\{\mathbf{W}_{\sigma,0},\mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma},\mathbf{Z}_{\text{end}},\mathbf{W}_{\text{end}}\big).\end{aligned}$$

- $\mathsf{Enc}(\mathsf{mpk},x,m)$: Let $x=(x_1,\ldots,x_\ell)\in\Sigma^\ell$. Pick $\mathbf{s}_0,\mathbf{s}_1,\ldots,\mathbf{s}_\ell,\mathbf{s}_{\text{end}}\leftarrow\mathbb{Z}_p^{1\times k}$ and output

$$\mathsf{ct}_x=\begin{pmatrix}[\mathbf{s}_0\mathbf{A}_1]_1,[\mathbf{s}_0\mathbf{A}_1\mathbf{W}_{\text{start}}]_1\\ \big\{[\mathbf{s}_j\mathbf{A}_1]_1,[\mathbf{s}_{j-1}\mathbf{A}_1\mathbf{Z}_{j\bmod 2}+\mathbf{s}_j\mathbf{A}_1\mathbf{W}_{x_{\ell+1-j},j\bmod 2}]_1\big\}_{j\in[\ell]}\\ [\mathbf{s}_{\text{end}}\mathbf{A}_1]_1,[\mathbf{s}_\ell\mathbf{A}_1\mathbf{Z}_{\text{end}}+\mathbf{s}_{\text{end}}\mathbf{A}_1\mathbf{W}_{\text{end}}]_1,[\mathbf{s}_{\text{end}}\mathbf{A}_1\mathbf{k}^\top]_T\cdot m.\end{pmatrix}.$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$: Pick $\mathbf{D} \leftarrow \mathbb{Z}_p^{(2k+1)\times Q}$, $\mathbf{R} \leftarrow \mathbb{Z}_p^{k\times Q}$ and output

$$\mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{D}\mathbf{f}^\top + \mathbf{W}_{\text{start}}\mathbf{R}\mathbf{f}^\top]_2, [\mathbf{R}\mathbf{f}^\top]_2 \\ \{[-\mathbf{D} + \mathbf{Z}_b\mathbf{R}]_2, [\mathbf{D}\mathbf{M}_\sigma^\top + \mathbf{W}_{\sigma,b}\mathbf{R}]_2, [\mathbf{R}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{D} + \mathbf{Z}_{\text{end}}\mathbf{R}]_2, [\mathbf{k}^\top\mathbf{u} + \mathbf{W}_{\text{end}}\mathbf{R}]_2, [\mathbf{R}]_2 \end{pmatrix}.$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_x)$: Parse ciphertext for string $x = (x_1, \ldots, x_\ell)$ andkey for $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ as

$$\mathsf{ct}_x = \begin{pmatrix} [\mathbf{c}_{0,1}]_1, [\mathbf{c}_{0,2}]_1 \\ \{[\mathbf{c}_{j,1}]_1, [\mathbf{c}_{j,2}]_1\}_j \\ [\mathbf{c}_{\text{end},1}]_1, [\mathbf{c}_{\text{end},2}]_1, C \end{pmatrix} \quad \text{and} \quad \mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{k}_0^\top]_2, [\mathbf{r}_0^\top]_2 \\ \{[\mathbf{K}_b]_2, [\mathbf{K}_{\sigma,b}]_2, [\mathbf{R}]_2\}_{\sigma,b} \\ [\mathbf{K}_{\text{end},1}]_2, [\mathbf{K}_{\text{end},2}]_2, [\mathbf{R}]_2 \end{pmatrix}.$$

  We define $\mathbf{f}_{j,x}$ for all $j \in [0, \ell]$ as (22) and proceed as follows:

  1. Compute
  $$B_0 = e([\mathbf{c}_{0,1}]_1, [\mathbf{k}_0^\top]_2) \cdot e([\mathbf{c}_{0,2}]_1, [\mathbf{r}_0^\top]_2)^{-1};$$
  2. For all $j = 1, \ldots, \ell$, compute
  $$[\mathbf{b}_j]_T = e([\mathbf{c}_{j-1,1}]_1, [\mathbf{K}_{j \bmod 2}]_2) \cdot e([\mathbf{c}_{j,1}]_1, [\mathbf{K}_{x_{\ell+1-j}, j \bmod 2}]_2) \cdot e([-\mathbf{c}_{j,2}]_1, [\mathbf{R}]_2) \quad \text{and} \quad B_j = [\mathbf{b}_j\mathbf{f}_{\ell+1-j,x}^\top]_T;$$
  3. Compute
  $$[\mathbf{b}_{\text{end}}]_T = e([\mathbf{c}_{\ell,1}]_1, [\mathbf{K}_{\text{end},1}]_2) \cdot e([\mathbf{c}_{\text{end},1}]_1, [\mathbf{K}_{\text{end},2}]_2) \cdot e([-\mathbf{c}_{\text{end},2}]_1, [\mathbf{R}]_2) \quad \text{and} \quad B_{\text{end}} = [\mathbf{b}_{\text{end}}\mathbf{f}_{0,x}^\top]_T;$$
  4. Compute
  $$B_{\text{all}} = B_0 \cdot \textstyle\prod_{j=1}^{\ell} B_j \cdot B_{\text{end}} \quad \text{and} \quad B = B_{\text{all}}^{(\mathbf{u}\mathbf{f}_{0,x}^\top)^{-1}}$$
  and output the message $m' \leftarrow C \cdot B^{-1}$.

G Missing Material from Section 6

G.1 An Attack for Non-injective ρ with Shared Random Coins

We consider the following ABE scheme, which is the ABE scheme for $\mathsf{NBP}^{\oplus_p}$ in Section 6.2 but with $\mathbf{R}_j = \mathbf{R} \leftarrow \mathbb{Z}_p^{k\times Q}$ for all $j \in \ell_{\text{BP}}$, as is the case mentioned in the **Overview** paragraph at the beginning of Section 6.2.

$$\mathsf{mpk} = \big([\mathbf{A}_1, \mathbf{A}_1\mathbf{W}_{\text{start}}, \{\mathbf{A}_1\mathbf{W}_{\eta,\sigma}\}_{\eta\in[\ell],\sigma\in\Sigma}, \mathbf{A}_1\mathbf{W}_{\text{end}}]_1, [\mathbf{A}_1\mathbf{k}^\top]_T\big);$$
$$\mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{D}_0\mathbf{u}^\top + \mathbf{W}_{\text{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \{[\mathbf{D}_j\mathbf{M}_{j,\sigma} - \mathbf{D}_{j-1} + \mathbf{W}_{\rho(j),\sigma}\mathbf{R}]_2, [\mathbf{R}]_2\}_{j\in[\ell_{\text{BP}}],\sigma\in\Sigma} \\ [\mathbf{k}^\top\mathbf{f} - \mathbf{D}_{\ell_{\text{BP}}} + \mathbf{W}_{\text{end}}\mathbf{R}_{\text{end}}]_2, [\mathbf{R}_{\text{end}}]_2 \end{pmatrix};$$
$$\mathsf{ct}_x = \Big([\mathbf{s}\mathbf{A}_1]_1, [\mathbf{s}\mathbf{A}_1\mathbf{W}_{\text{start}}]_1, \big\{[\mathbf{s}\mathbf{A}_1\mathbf{W}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]}, [\mathbf{s}\mathbf{A}_1\mathbf{W}_{\text{end}}]_1, [\mathbf{s}\mathbf{A}_1\mathbf{k}^\top]_T \cdot m\Big).$$

We will show a concrete attack when ρ is non-injective.

Let us consider an $\mathsf{NBP}^{\oplus_p}$ $\Gamma = (Q, \ell_{\text{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\text{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$ where $Q = 2$, $\ell_{\text{BP}} = 2$, $\ell = 1$, $\Sigma = \{a, b\}$,

$$\mathbf{M}_{1,a} = \mathbf{M}_{1,b} = \mathbf{M}_{2,b} = \mathbf{I}, \quad \mathbf{M}_{2,a} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathbf{P}, \quad \mathbf{u} = \mathbf{f} = \mathbf{e}_1, \quad \rho(1) = \rho(2) = 1$$

and an input $x = a$. Then we have mpk, key for Γ and ciphertext for x as follows:

$$\mathsf{mpk} = \big([\mathbf{A}_1, \mathbf{A}_1\mathbf{W}_{\text{start}}, \mathbf{A}_1\mathbf{W}_a, \mathbf{A}_1\mathbf{W}_b, \mathbf{A}_1\mathbf{W}_{\text{end}}]_1, [\mathbf{A}_1\mathbf{k}^\top]_T\big);$$

$$\mathsf{sk}_\Gamma = \left(\begin{array}{c} [\mathbf{D}_0\mathbf{e}_1^\top + \mathbf{W}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ [\mathbf{K}_{1,a}]_2 = [\mathbf{D}_1 - \mathbf{D}_0 + \mathbf{W}_a\mathbf{R}]_2, [\mathbf{R}]_2 \\ [\mathbf{K}_{1,b}]_2 = [\mathbf{D}_1 - \mathbf{D}_0 + \mathbf{W}_b\mathbf{R}]_2, [\mathbf{R}]_2 \\ [\mathbf{K}_{2,a}]_2 = [\mathbf{D}_2\mathbf{P} - \mathbf{D}_1 + \mathbf{W}_a\mathbf{R}]_2, [\mathbf{R}]_2 \\ [\mathbf{K}_{2,b}]_2 = [\mathbf{D}_2 - \mathbf{D}_1 + \mathbf{W}_b\mathbf{R}]_2, [\mathbf{R}]_2 \\ [\mathbf{k}^\top\mathbf{e}_1 - \mathbf{D}_2 + \mathbf{W}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{array}\right);$$

$$\mathsf{ct}_x = \Big([\mathbf{sA}_1]_1, [\mathbf{sA}_1\mathbf{W}_{\mathrm{start}}]_1, [\mathbf{sA}_1\mathbf{W}_a]_1, [\mathbf{sA}_1\mathbf{W}_{\mathrm{end}}]_1, [\mathbf{sA}_1\mathbf{k}^\top]_T \cdot m\Big).$$

One can check that $\Gamma(x) = 0$ since $\mathbf{fM}_{2,a}\mathbf{M}_{1,a}\mathbf{u} = \mathbf{e}_1 \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \mathbf{Ie}_1^\top = 0 \bmod p$, which means the secret key sk_Γ is not supposed to recover message m from ct_x. However we show that this is not the case. Normal decryption computes

$$D_0 = [\mathbf{sA}_1\mathbf{D}_0\mathbf{e}_1^\top]_T,\ D_1 = [\mathbf{sA}_1(\mathbf{D}_1 - \mathbf{D}_0)]_T,\ D_2 = [\mathbf{sA}_1(\mathbf{D}_2\mathbf{P} - \mathbf{D}_1)]_T,\ D_3 = [\mathbf{sA}_1(\mathbf{k}^\top\mathbf{e}_1 - \mathbf{D}_2)]_T.$$

Besides that the shared $\mathbf{R}$ allows us to compute more; in particular, we compute:

$$[\mathbf{K}]_2 = [(\mathbf{K}_{2,b} - \mathbf{K}_{1,b}) - (\mathbf{K}_{2,a} - \mathbf{K}_{1,a})]_2 = [\mathbf{D}_2 - \mathbf{D}_2\mathbf{P}]_2 \quad \text{and} \quad K = e([\mathbf{sA}_1]_1, [\mathbf{K}]_2) = [\mathbf{sA}_1(\mathbf{D}_2 - \mathbf{D}_2\mathbf{P})]_T$$

This allows us to compute

$$D_2' = [\overbrace{\mathbf{sA}_1(\mathbf{D}_2 - \mathbf{D}_2\mathbf{P})}^{K} + \overbrace{\mathbf{sA}_1(\mathbf{D}_2\mathbf{P} - \mathbf{D}_1)}^{D_2}]_T = [\mathbf{sA}_1(\mathbf{D}_2 - \mathbf{D}_1)]_T$$

and recover $[\mathbf{sA}_1\mathbf{k}^\top]_T$ from D_0, D_1, D_2', D_3:

$$[\mathbf{sA}_1\mathbf{k}^\top]_T = [\overbrace{\mathbf{sA}_1\mathbf{D}_0\mathbf{e}_1^\top}^{D_0} + \overbrace{\mathbf{sA}_1(\mathbf{D}_1 - \mathbf{D}_0)}^{D_1}\mathbf{e}_1^\top + \overbrace{\mathbf{sA}_1(\mathbf{D}_2 - \mathbf{D}_1)}^{D_2'}\mathbf{e}_1^\top + \overbrace{\mathbf{sA}_1(\mathbf{k}^\top\mathbf{e}_1 - \mathbf{D}_2)}^{D_3}\mathbf{e}_1^\top]_T.$$

G.2 Missing Proof in Section 6.3

In this section, we prove that $\mathsf{G}_0 \approx_c \mathsf{G}_1$ and the advantage of adversary in G_3 is 0. All games are defined in Section 6.3.

Lemma 53 **($\mathsf{G}_0 \approx_c \mathsf{G}_1$).** *For all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle\mathcal{A}, \mathsf{G}_0\rangle = 1] - \Pr[\langle\mathcal{A}, \mathsf{G}_1\rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\mathrm{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{a}_2}}(\lambda).$$

Proof (sketch). This relies on $\mathrm{SD}^{G_1}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{a}_2}$ assumption which implies

$$\big([\mathbf{A}_1]_1, \boxed{[\mathbf{sA}_1]_1}\big) \approx_c \big([\mathbf{A}_1]_1, \colorbox{lightgray}{$[\mathbf{sA}_1 + s\mathbf{a}_2]_1$}\big)$$

where $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ and $s \leftarrow \mathbb{Z}_p$. Let x^* be the selective challenge, the reduction algorithm is sketched as follows:

- we sample $\mathbf{k}, \mathbf{W}_{\mathrm{start}}, \mathbf{W}_{\eta,\sigma}, \mathbf{W}_{\mathrm{end}}$ for all $\eta \in [\ell], \sigma \in \Sigma$ and create $(\mathsf{mpk}, \mathsf{msk})$ honestly using $[\mathbf{A}_1]_1$.
- on key query Γ, we honestly run $\mathsf{sk}_\Gamma \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$ using mpk and msk;
- on input challenge query (m_0, m_1), we sample β and create the challenge ciphertext using the term given out in the statement above. □

Lemma 54 **(Advantage in G_3).** *For all $\mathcal{A}$, we have*

$$\Pr[\langle\mathcal{A}, \mathsf{G}_3\rangle = 1] = 1/2.$$

Proof (sketch). First, we argue that the secret key sk_Γ^* perfectly hides the $\mathbf{a}_2$-component of $\mathbf{k}^\top$, i.e., $\alpha = \mathbf{a}_2\mathbf{k}^\top$. Recall the $\mathbf{a}_2$-components of the key

$$\mathsf{sk}_\Gamma^*[2] = \left(\begin{array}{c} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [\alpha\mathbf{f} + \boxed{\Delta\cdot\mathbf{f}} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{array}\right)$$

We observe that it only leaks $\alpha + \Delta$ which means that the key perfectly hides α. Therefore, the unique term involving $\mathbf{k}$ in $\mathsf{ct}_{x^*}^*$, i.e., $[\mathbf{sA}_1\mathbf{k}^\top + s\mathbf{a}_2\mathbf{k}^\top]_T$, is independently and uniformly distributed and thus statistically hides message m_β. □

G.3 Missing Proof in Section 6.4

We show that the core lemma, Lemma 30, implies $\mathsf{G}_{2.\kappa-1} \approx_c \mathsf{G}_{2.\kappa}$ for all $\kappa \in [q]$.

Lemma 55 (Lemma 30 ⇒ $\mathsf{G}_{2.\kappa-1} \approx_c \mathsf{G}_{2.\kappa}$). *For all $\kappa \in [q]$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ and*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa-1} \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa} \rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\mathrm{CORE}}(\lambda)$$

where $\mathsf{Adv}_{\mathcal{B}}^{\mathrm{CORE}}(\lambda)$ is defined in Lemma 30.

Proof (sketch). By Lemma 4, we only focus on $\mathbf{a}_2$-components. On input aux, reduction $\mathcal{B}$ works as follows:

- On input Γ, it proceeds as follows:
  - for the κ'th query, return the result of oracle query $\mathsf{OKey}(\Gamma)$;
  - for the remaining queries, output $\mathsf{sk}_\Gamma[2]$ or $\mathsf{sk}_\Gamma^*[2]$ which can be created from aux;
- On input (x^*, m_0, m_1), make an oracle query $\mathsf{OEnc}(x^*)$ and create the challenge ciphertext with the help of aux.

Observe that, if $\mathsf{OKey}(\Gamma)$ outputs $\mathsf{sk}_\Gamma[2]$, the simulation is identical to $\mathsf{G}_{2.\kappa-1}$; if $\mathsf{OKey}(\Gamma)$ outputs $\mathsf{sk}_\Gamma^*[2]$, the simulation is identical to $\mathsf{G}_{2.\kappa}$. This completes the proof. □

G.4 Detailed Proofs of Neighbor Indistinguishability

This section provides the detailed for proving Lemma 32 restated below. The proofs are similar to those for selective security in Section 6.3.

Lemma 56 (Neighbor indistinguishability). *For all $\mathsf{xxx} \in \{0,2\} \cup \{1.i.i' : i \in [\ell_{BP}], i' \in [2]\}$, $u_0, u_1 \in I \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_{\mathsf{xxx}}(u_0, u_1) \rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{\mathsf{xxx}}(u_0, u_1) \rangle = 1] \le O(|\Sigma|^2) \cdot \mathsf{Adv}_{\mathcal{B}}^{k\text{-LIN}}(\lambda).$$

Initializing. We prove the following lemma stating that $\widehat{\mathsf{H}}^0_0(u_0, u_1) \approx_c \widehat{\mathsf{H}}^1_0(u_0, u_1)$ for all u_0, u_1. This is analogous to Lemma 25.

Lemma 57. *For all $u_0, u_1 \in I \times \mathcal{E}_Q$ and all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_0(u_0, u_1) \rangle = 1] = \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_0(u_0, u_1) \rangle = 1]$$

Proof (sketch). We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\boxed{\perp, \perp}),\ u_1 = (\ \{0\}, \mathbf{f}_{0,x^*}\ );$$

the lemma trivially holds in all other cases. Roughly, in this case, we prove

$$\big(\mathsf{aux}, \mathsf{OEnc}(x^*), \boxed{\mathsf{sk}_\Gamma[2]}\big) = \big(\mathsf{aux}, \mathsf{OEnc}(x^*),\ \mathsf{sk}^0_{\Gamma, \mathbf{f}_{0,x^*}}[2]\ \big)$$

where we have

$$\mathsf{sk}_\Gamma[2] = \begin{pmatrix} [\boxed{\mathbf{d}_0 \mathbf{u}^\top} + \mathbf{w}_{\mathrm{start}} \mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{ [\mathbf{d}_j \mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma} \mathbf{R}_j]_2, [\mathbf{R}_j]_2 \big\}_{j \in [\ell_{\mathrm{BP}}], \sigma \in \Sigma} \\ [\alpha \mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}} \mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix},$$

$$\mathsf{sk}^0_{\Gamma, \mathbf{f}_{0,x^*}}[2] = \begin{pmatrix} [\ (\mathbf{d}_0 + \Delta \cdot \mathbf{f}_{0,x^*}) \mathbf{u}^\top\ + \mathbf{w}_{\mathrm{start}} \mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{ [\mathbf{d}_j \mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma} \mathbf{R}_j]_2, [\mathbf{R}_j]_2 \big\}_{j \in [\ell_{\mathrm{BP}}], \sigma \in \Sigma} \\ [\alpha \mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}} \mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}$$

and

$$\overbrace{[\mathbf{B}, \{\mathbf{w}_{\eta,\sigma} \mathbf{B}\}_{\eta \in [\ell], \sigma \in \Sigma}]_2, \alpha, \Delta, \mathbf{w}_{\mathrm{start}}, \mathbf{w}_{\mathrm{end}}}^{\mathsf{aux}} \quad \text{and} \quad \overbrace{\{\mathbf{w}_{\eta, x^*_\eta}\}_{\eta \in [\ell]}}^{\mathsf{OEnc}(x^*)}.$$

The lemma immediately follows from the fact $\Gamma(x^*) = 0 \iff \mathbf{f}_{0,x^*} \mathbf{u}^\top = 0 \bmod p$, see Lemma 24. □

Key switching I. We will prove that $\widehat{\mathsf{H}}^0_{1.i.1}(u_0,u_1) \approx_s \widehat{\mathsf{H}}^1_{1.i.1}(u_0,u_1)$ and $\widehat{\mathsf{H}}^0_2(u_0,u_1) \approx_s \widehat{\mathsf{H}}^1_2(u_0,u_1)$ for all $i \in [\ell_{\mathrm{BP}}]$ and all u_0,u_1. The proofs for them are similar. We begin with the following lemma stating that $\widehat{\mathsf{H}}^0_{1.1.1}(u_0,u_1) \approx_s \widehat{\mathsf{H}}^1_{1.1.1}(u_0,u_1)$ for all u_0,u_1, which is analogous to Lemma 26, and sketch the proof for remaining statements.

Lemma 58. *For all $u_0,u_1 \in I \times \mathcal{E}_Q$ and all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_{1.1.1}(u_0,u_1)\rangle = 1] \approx \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{1.1.1}(u_0,u_1)\rangle = 1].$$

Proof. We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\boxed{\{0\}}, \mathbf{f}_{0,x^*}),\ u_1 = (\{0,1\} , \mathbf{f}_{0,x^*});$$

the lemma trivially holds in all other cases. Roughly, in this case, we prove that

$$\big(\mathsf{aux}, \mathsf{OEnc}(x^*), \boxed{\mathsf{sk}^0_{\Gamma,\mathbf{f}_{0,x^*}}[2]}\big) = \big(\mathsf{aux}, \mathsf{OEnc}(x^*), \mathsf{sk}^{0,1}_{\Gamma,\mathbf{f}_{0,x^*}}[2]\big).$$

More concretely, this means that

$$\mathsf{sk}^0_{\Gamma,\mathbf{f}_{0,x^*}}[2] = \begin{pmatrix} [\boxed{(\mathbf{d}_0 + \Delta\cdot\mathbf{f}_{0,x^*})}\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_1\mathbf{M}_{1,\sigma}\boxed{-\mathbf{d}_0} + \mathbf{w}_{\rho(1),\sigma}\mathbf{R}_1]_2, [\mathbf{R}_1]_2\big\}_{\sigma\in\Sigma} \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\neq 1,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix} \approx_s \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_1\mathbf{M}_{1,\sigma} -\mathbf{d}_0 + \Delta\cdot\mathbf{f}_{0,x^*} + \mathbf{w}_{\rho(1),\sigma}\mathbf{R}_1]_2, [\mathbf{R}_1]_2\big\}_{\sigma\in\Sigma} \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\neq 1,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix} = \mathsf{sk}^{0,1}_{\Gamma,\mathbf{f}_{0,x^*}}[2]$$

given

$$\overbrace{[\mathbf{B}, \{\mathbf{w}_{\eta,\sigma}\mathbf{B}\}_{\eta\in[\ell],\sigma\in\Sigma}]_2, \alpha, \Delta, \mathbf{w}_{\mathrm{start}}, \mathbf{w}_{\mathrm{end}}}^{\mathsf{aux}} \quad \text{and} \quad \overbrace{\{\mathbf{w}_{\eta,x^*_\eta}\}_{\eta\in[\ell]}}^{\mathsf{OEnc}(x^*)}.$$

This immediately follows from change of variables $\mathbf{d}_0 \mapsto \mathbf{d}_0 - \Delta\cdot\mathbf{f}_{0,x^*}$. □

Via the same proof idea, we can prove the following two lemmas stating that $\widehat{\mathsf{H}}^0_{1.i.1}(u_0,u_1) \approx_c \widehat{\mathsf{H}}^1_{1.i.1}(u_0,u_1)$ for all $i \in [2,\ell_{\mathrm{BP}}]$ and $\widehat{\mathsf{H}}^0_2(u_0,u_1) \approx_c \widehat{\mathsf{H}}^1_2(u_0,u_1)$, respectively. The first lemma relies on change of variable $\mathbf{d}_{i-1} \mapsto \mathbf{d}_{i-1} - \Delta\cdot\mathbf{f}_{i-1,x^*}$; while the second lemma relies on change of variable $\mathbf{d}_{\ell_{\mathrm{BP}}} \mapsto \mathbf{d}_{\ell_{\mathrm{BP}}} - \Delta\cdot\mathbf{f}_{\ell_{\mathrm{BP}},x^*}$. We give the lemmas but omit the proofs.

Lemma 59. *For all $i \in [2,\ell_{BP}]$, $u_0,u_1 \in I \times \mathcal{E}_Q$ and all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_{1.i.1}(u_0,u_1)\rangle = 1] \approx \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{1.i.1}(u_0,u_1)\rangle = 1].$$

Lemma 60. *For all $u_0,u_1 \in I \times \mathcal{E}_Q$ and all $\mathcal{A}$, we have*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_2(u_0,u_1)\rangle = 1] \approx \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_2(u_0,u_1)\rangle = 1].$$

Key switching II. We prove the following lemma stating that $\widehat{\mathsf{H}}^0_{1.i.2}(u_0,u_1) \approx_c \widehat{\mathsf{H}}^1_{1.i.2}(u_0,u_1)$ for all $i \in [\ell_{\mathrm{BP}}]$ and all u_0,u_1. This is analogous to Lemma 29.

Lemma 61. *For all $i \in [\ell_{BP}]$, $u_0,u_1 \in I \times \mathcal{E}_Q$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$\Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^0_{1.i.2}(u_0,u_1)\rangle = 1] - \Pr[\langle \mathcal{A}, \widehat{\mathsf{H}}^1_{1.i.2}(u_0,u_1)\rangle = 1] \leq O(|\Sigma|^2)\cdot \mathsf{Adv}^{\mathrm{DDH}^{G_2}_{1,Q}}_{\mathcal{B}}(\lambda).$$

Proof. We consider the case that the adversary adaptively chooses Γ and x^* in the hybrids parameterized by

$$u_0 = (\boxed{\{i-1,i\},\mathbf{f}_{i-1,x^*}}),\ u_1 = (\{i\},\mathbf{f}_{i,x^*});$$

the lemma trivially holds in other cases. Roughly, we prove that

$$\big(\mathsf{aux}, \mathsf{OEnc}(x^*), \boxed{\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{f}_{i-1,x^*}}[2]}\big) \approx_c \big(\mathsf{aux}, \mathsf{OEnc}(x^*), \mathsf{sk}^{i}_{\Gamma,\mathbf{f}_{i,x^*}}[2]\big)$$

which means:

$$
\begin{aligned}
\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{f}_{i-1,x^*}}[2] \;&=\; \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \boxed{\Delta\cdot\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2, [\mathbf{R}_i]_2\big\}_{\sigma\in\Sigma} \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix} \\
&\approx_c \begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \colorbox{lightgray}{$\Delta\cdot\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma}$} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2, [\mathbf{R}_i]_2\big\}_{\sigma\in\Sigma} \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix} = \mathsf{sk}^{i}_{\Gamma,\mathbf{f}_{i,x^*}}[2];
\end{aligned}
$$

in the presence of

$$
\overbrace{[\mathbf{B}, \{\mathbf{w}_{\eta,\sigma}\mathbf{B}\}_{\eta\in[\ell],\sigma\in\Sigma}]_2, \alpha, \Delta, \mathbf{w}_{\mathrm{start}}, \mathbf{w}_{\mathrm{end}}}^{\mathsf{aux}} \quad \text{and} \quad \overbrace{\{\mathbf{w}_{\eta,x^*_\eta}\}_{\eta\in[\ell]}}^{\mathsf{OEnc}(x^*)}.
$$

We randomly guess $x^*_{\rho(i)} \leftarrow \Sigma$, which causes a multiplicative security loss of $|\Sigma|$, and prove this using the following statement implied by $\mathrm{DDH}^{G_2}_{1,Q}$ assumption: for all $\Delta \in \mathbb{Z}_p$, we have

$$
\big\{[\mathbf{w}_{\rho(i),\sigma}\mathbf{B}]_2, [\mathbf{B}]_2, [\Delta\cdot\boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2, [\mathbf{R}_i]_2\big\}_{\sigma\neq x^*_{\rho(i)}} \approx_c \big\{[\mathbf{w}_{\rho(i),\sigma}\mathbf{B}]_2, [\mathbf{B}]_2, [\Delta\cdot\colorbox{lightgray}{$\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma}$} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i]_2, [\mathbf{R}_i]_2\big\}_{\sigma\neq x^*_{\rho(i)}}
$$

where $\mathbf{w}_{\rho(i),\sigma} \leftarrow \mathbb{Z}_p^{1\times k}$, $\mathbf{B} \leftarrow \mathbb{Z}_p^{k\times k}$ and $\mathbf{R}_i \leftarrow \mathbb{Z}_p^{k\times Q}$. On input $\big\{[\mathbf{w}_{\rho(i),\sigma}\mathbf{B}]_2, [\mathbf{B}]_2, [\mathbf{t}_\sigma]_2, [\mathbf{R}_i]_2\big\}_{\sigma\neq x^*_{\rho(i)}}$ where

$$
\mathbf{t}_\sigma = \Delta\cdot\boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i \;\text{ or }\; \mathbf{t}_\sigma = \Delta\cdot\colorbox{lightgray}{$\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma}$} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i
$$

we sample $\alpha \leftarrow \mathbb{Z}_p, \mathbf{w}_{\mathrm{start}}, \mathbf{w}_{\rho(i),x^*_{\rho(i)}}, \mathbf{w}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1\times k}$ and $\mathbf{w}_{\eta,\sigma} \leftarrow \mathbb{Z}_p^{1\times k}$ for all $\eta \neq \rho(i), \sigma \in \Sigma$ and proceed as follows:

(Simulating aux**)** We can trivially simulate aux using Δ, $\big\{[\mathbf{w}_{\rho(i),\sigma}\mathbf{B}]_2, [\mathbf{B}]_2\big\}_{\sigma\neq x^*_{\rho(i)}}$ given in the lemma and $\alpha, \mathbf{w}_{\mathrm{start}}, \mathbf{w}_{\mathrm{end}}, \mathbf{w}_{\rho(i),x^*_{\rho(i)}}, \{\mathbf{w}_{\eta,\sigma}\}_{\eta\neq\rho(i),\sigma\in\Sigma}$ sampled by ourselves.

(Answering OEnc**)** On input x^*, we can answer $\mathsf{OEnc}(x^*)$ using the knowledge of $\mathbf{w}_{\rho(i),x^*_{\rho(i)}}$ and $\{\mathbf{w}_{\eta,x^*_\eta}\}_{\eta\neq\rho(i)}$. Here we use the fact that the oracle does not involve $\{\mathbf{w}_{\rho(i),\sigma}\}_{\sigma\neq x^*_{\rho(i)}}$.

(Answering OKey**)** On input Γ, we want to simulate secret key in the form:

$$
\begin{pmatrix} [\mathbf{d}_0\mathbf{u}^\top + \mathbf{w}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{d}_i\mathbf{M}_{i,x^*_{\rho(i)}} - \mathbf{d}_{i-1} + \Delta\cdot\mathbf{f}_{i-1,x^*} + \mathbf{w}_{\rho(i),x^*_{\rho(i)}}\mathbf{R}_i]_2, [\mathbf{R}_i]_2\big\} \\ \big\{[\mathbf{d}_i\mathbf{M}_{i,\sigma} - \mathbf{d}_{i-1} + \mathbf{t}_\sigma]_2, [\mathbf{R}_i]_2\big\}_{\sigma\neq x^*_{\rho(i)}} \\ \big\{[\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\mathbf{R}_j]_2, [\mathbf{R}_j]_2\big\}_{j\neq i,\sigma\in\Sigma} \\ [\alpha\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}
$$

Observe that,

- when $\mathbf{t}_\sigma = \Delta\cdot\boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$, the distribution is identical to $\boxed{\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{f}_{i-1,x^*}}[2]}$;
- when $\mathbf{t}_\sigma = \Delta\cdot\colorbox{lightgray}{$\mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma}$} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$, the distribution is identical to $\colorbox{lightgray}{$\mathsf{sk}^{i}_{\Gamma,\mathbf{f}_{i,x^*}}[2]$}$ since $\mathbf{f}_{i-1,x^*} = \mathbf{f}_{i,x^*}\mathbf{M}_{i,x^*_{\rho(i)}} \bmod p$, see Lemma 24.

We sample $\mathbf{d}_0, \ldots, \mathbf{d}_{\ell_{\mathrm{BP}}} \leftarrow \mathbb{Z}_p^{1\times Q}$ and simulate the key as follows:

- We simulate the terms in the second row using $[\mathbf{R}_i]_2$ and $\mathbf{w}_{\rho(i),x^*_{\rho(i)}}$;
- We simulate the terms in the third row using $[\mathbf{t}_\sigma]_2$ and $[\mathbf{R}_i]_2$;

- All remaining terms can be simulated using aux.

Observe that, when $\mathbf{t}_\sigma = \Delta \cdot \boxed{\mathbf{f}_{i-1,x^*}} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$, oracle $\mathsf{OKey}(\Gamma)$ returns $\boxed{\mathsf{sk}^{i-1,i}_{\Gamma,\mathbf{f}_{i-1,x^*}}[2]}$ and the simulation is identical to $\widehat{\mathsf{H}}^0_{1.i.2}(u_0,u_1)$; when $\mathbf{t}_\sigma = \Delta \cdot \mathbf{f}_{i,x^*}\mathbf{M}_{i,\sigma} + \mathbf{w}_{\rho(i),\sigma}\mathbf{R}_i$, oracle $\mathsf{OKey}(\Gamma)$ returns $\mathsf{sk}^{i}_{\Gamma,\mathbf{f}_{i,x^*}}[2]$ and the simulation is identical to $\widehat{\mathsf{H}}^1_{1.i.2}(u_0,u_1)$. This completes the proof. □

H Concrete ABE for Branching Program with Adaptive Security

In this section, we show our compact adaptively secure ABE for branching program (BP). This is derived from our adaptively secure ABE for $\mathcal{E}_Q$-restricted $\mathrm{NBP}^{\oplus p}$ in Section 6.2 and the transformation from BP to $\mathcal{E}_Q$-restricted $\mathrm{NBP}^{\oplus p}$ in Section 6.1, see Lemma 23.

- $\mathsf{Setup}(1^\lambda, \ell, \Sigma)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

$$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{k\times(k+1)}, \mathbf{k} \leftarrow \mathbb{Z}_p^{1\times(k+1)} \quad \text{and} \quad \mathbf{W}_{\mathrm{start}}, \mathbf{W}_{\eta,\sigma}, \mathbf{W}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{(k+1)\times k}, \forall \eta \in [\ell], \sigma \in \Sigma.$$

  Output

$$\begin{aligned} \mathsf{mpk} &= \big([\mathbf{A}_1, \mathbf{A}_1\mathbf{W}_{\mathrm{start}}, \{\mathbf{A}_1\mathbf{W}_{\eta,\sigma}\}_{\eta\in[\ell],\sigma\in\Sigma}, \mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1, [\mathbf{A}_1\mathbf{k}^\top]_T\big) \\ \mathsf{msk} &= \big(\mathbf{k}, \mathbf{W}_{\mathrm{start}}, \{\mathbf{W}_{\eta,\sigma}\}_{\eta\in[\ell],\sigma\in\Sigma}, \mathbf{W}_{\mathrm{end}}\big). \end{aligned}$$

- $\mathsf{Enc}(\mathsf{mpk}, x, m)$: Let $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$ and $m \in G_T$. Pick $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ and output

$$\mathsf{ct}_x = \Big([\mathbf{s}\mathbf{A}_1]_1, [\mathbf{s}\mathbf{A}_1\mathbf{W}_{\mathrm{start}}]_1, \big\{[\mathbf{s}\mathbf{A}_1\mathbf{W}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]}, [\mathbf{s}\mathbf{A}_1\mathbf{W}_{\mathrm{end}}]_1, [\mathbf{s}\mathbf{A}_1\mathbf{k}^\top]_T \cdot m\Big).$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \Gamma)$: Let $\Gamma = (Q, \ell_{\mathrm{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$. Pick

$$\mathbf{D}_0, \mathbf{D}_1, \ldots, \mathbf{D}_{\ell_{\mathrm{BP}}} \leftarrow \mathbb{Z}_p^{(k+1)\times Q},\ \mathbf{R}_1, \ldots, \mathbf{R}_{\ell_{\mathrm{BP}}}, \mathbf{R}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{k\times Q},\ \mathbf{r} \leftarrow \mathbb{Z}_p^{1\times k}$$

  output

$$\mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{D}_0\mathbf{f}^\top + \mathbf{W}_{\mathrm{start}}\mathbf{r}^\top]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{D}_j\mathbf{M}^\top_{\ell_{\mathrm{BP}}+1-j,\sigma} - \mathbf{D}_{j-1} + \mathbf{W}_{\rho(\ell_{\mathrm{BP}}+1-j),\sigma}\mathbf{R}_j]_2,\ [\mathbf{R}_j]_2\big\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [\mathbf{k}^\top\mathbf{u} - \mathbf{D}_{\ell_{\mathrm{BP}}} + \mathbf{W}_{\mathrm{end}}\mathbf{R}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}.$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_\Gamma, \mathsf{ct}_x)$: Parse ciphertext for $x = (x_1, \ldots, x_\ell)$ and key for $\Gamma = (Q, \ell_{\mathrm{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$ as

$$\mathsf{ct}_x = \big([\mathbf{c}]_1, [\mathbf{c}_{\mathrm{start}}]_1, \big\{[\mathbf{c}_\eta]_1\big\}_{\eta\in[\ell]}, [\mathbf{c}_{\mathrm{end}}]_1, C\big) \quad \text{and} \quad \mathsf{sk}_\Gamma = \begin{pmatrix} [\mathbf{k}^\top_{\mathrm{start}}]_2, [\mathbf{r}^\top]_2 \\ \big\{[\mathbf{K}_{j,\sigma}]_2, [\mathbf{R}_j]_2\big\}_{j,\sigma} \\ [\mathbf{K}_{\mathrm{end}}]_2, [\mathbf{R}_{\mathrm{end}}]_2 \end{pmatrix}.$$

  We define $\mathbf{f}_{j,x}$ for all $j \in [0, \ell_{\mathrm{BP}}]$ as (39) and proceed as follows:

  1. Compute

$$B_{\mathrm{start}} = e([\mathbf{c}]_1, [\mathbf{k}^\top_{\mathrm{start}}]_2) \cdot e([\mathbf{c}_{\mathrm{start}}]_1, [\mathbf{r}^\top]_2)^{-1};$$

  2. For all $j \in [\ell_{\mathrm{BP}}]$, compute

$$[\mathbf{b}_j]_T = e([\mathbf{c}]_1, [\mathbf{K}_{j,x_{\rho(\ell_{\mathrm{BP}}+1-j)}}]_2) \cdot e([-\mathbf{c}_{\rho(\ell_{\mathrm{BP}}+1-j)}]_1, [\mathbf{R}_j]_2) \quad \text{and} \quad B_j = [\mathbf{b}_j\mathbf{f}^\top_{\ell_{\mathrm{BP}}+1-j,x}]_T;$$

  3. Compute

$$[\mathbf{b}_{\mathrm{end}}]_T = e([\mathbf{c}]_1, [\mathbf{K}_{\mathrm{end}}]_2) \cdot e([-\mathbf{c}_{\mathrm{end}}]_1, [\mathbf{R}]_2) \quad \text{and} \quad B_{\mathrm{end}} = [\mathbf{b}_{\mathrm{end}}\mathbf{f}^\top_{0,x}]_T;$$

  4. Compute

$$B_{\mathrm{all}} = B_{\mathrm{start}} \cdot \textstyle\prod_{i=j}^{\ell_{\mathrm{BP}}} B_j \cdot B_{\mathrm{end}} \quad \text{and} \quad B = B_{\mathrm{all}}^{(\mathbf{u}\mathbf{f}^\top_{0,x})^{-1}}$$

  and output the message $m' \leftarrow C \cdot B^{-1}$.

I Adaptively Secure CP-ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ and DFA

In this section, we construct adaptively secure CP-ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ from k-Lin assumption. The scheme is based on our adaptively secure KP-ABE for the same class in Section 5 and dual conversion in [4,6]. This readily gives us an adaptively secure CP-ABE for DFA by Lemma 1.

I.1 Basis

We will use the following two sets of bases for ciphertexts and keys, respectively:

$$\mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{2k\times k} \quad \text{and} \quad (\mathbf{B}_1, \mathbf{B}_2) \leftarrow \mathbb{Z}_p^{k\times(3k+1)} \times \mathbb{Z}_p^{(2k+1)\times(3k+1)}.$$

We use $\mathbf{A}_1^{\perp}, \mathbf{A}_2^{\perp} \in \mathbb{Z}_p^{k\times 2k}$ to denote the dual basis of $(\mathbf{A}_1, \mathbf{A}_2)$ such that $\mathbf{A}_i^{\perp}\mathbf{A}_i = \mathbf{I}$ for $i \in \{1,2\}$ and $\mathbf{A}_i^{\perp}\mathbf{A}_j = \mathbf{0}$ for $i \neq j$. Analogously, we use $(\mathbf{B}_1^{\perp}, \mathbf{B}_2^{\perp}) \in \mathbb{Z}_p^{(3k+1)\times k} \times \mathbb{Z}_p^{(3k+1)\times(2k+1)}$ to denote the dual basis of $(\mathbf{B}_1, \mathbf{B}_2)$. In the proof, we will use $\mathsf{SD}^{G_2}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{A}_2}$ and $\mathsf{SD}^{G_1}_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_2}$ assumption, cf. Section 4.1.

I.2 Scheme

For notational convenience, especially reusing NFA notations in Section 5, we will generate ciphertexts over G_2 and keys over G_1. Our CP-ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in prime-order groups is described as follows:

- $\mathsf{Setup}(1^\lambda, \Sigma)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$. Sample

  $$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{2k\times k}, \mathbf{B}_1 \leftarrow \mathbb{Z}_p^{k\times(3k+1)}, \mathbf{k} \leftarrow \mathbb{Z}_p^{1\times 2k} \quad \text{and} \quad \mathbf{W}_{\mathsf{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_0, \mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}, \mathbf{Z}_{\mathsf{end}}, \mathbf{W}_{\mathsf{end}} \leftarrow \mathbb{Z}_p^{(3k+1)\times 2k}, \ \forall \sigma \in \Sigma.$$

  Output

  $$\begin{aligned} \mathsf{mpk} &= \big([\mathbf{A}_1, \mathbf{W}_{\mathsf{start}}\mathbf{A}_1, \mathbf{Z}_0\mathbf{A}_1, \mathbf{Z}_1\mathbf{A}_1, \mathbf{W}_0\mathbf{A}_1, \{\mathbf{W}_{\sigma,0}\mathbf{A}_1, \mathbf{W}_{\sigma,1}\mathbf{A}_1\}_{\sigma\in\Sigma}, \mathbf{Z}_{\mathsf{end}}\mathbf{A}_1, \mathbf{W}_{\mathsf{end}}\mathbf{A}_1]_2, [\mathbf{k}\mathbf{A}_1]_T \big) \\ \mathsf{msk} &= \big(\mathbf{k}, \mathbf{B}_1, \mathbf{W}_{\mathsf{start}}, \mathbf{Z}_0, \mathbf{Z}_1, \mathbf{W}_0, \{\mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}\}_{\sigma\in\Sigma}, \mathbf{Z}_{\mathsf{end}}, \mathbf{W}_{\mathsf{end}} \big). \end{aligned}$$

- $\mathsf{Enc}(\mathsf{mpk}, \Gamma, m)$: Let $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ and $m \in G_T$. Pick $\mathbf{D} \leftarrow \mathbb{Z}_p^{(3k+1)\times Q}$, $\mathbf{S} \leftarrow \mathbb{Z}_p^{k\times Q}$, $\mathbf{s} \leftarrow \mathbb{Z}_p^{1\times k}$ and output

  $$\mathsf{ct}_\Gamma = \begin{pmatrix} [\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\mathsf{start}}\mathbf{A}_1\mathbf{S}\mathbf{u}^\top]_2, [\mathbf{A}_1\mathbf{S}\mathbf{u}^\top]_2 \\ \big\{[-\mathbf{D} + \mathbf{Z}_b\mathbf{A}_1\mathbf{S}]_2, [\mathbf{D}\mathbf{M}_\sigma + \mathbf{W}_{\sigma,b}\mathbf{A}_1\mathbf{S}]_2, [\mathbf{A}_1\mathbf{S}]_2\big\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{D} + \mathbf{Z}_{\mathsf{end}}\mathbf{A}_1\mathbf{S}]_2, [(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f} + \mathbf{W}_{\mathsf{end}}\mathbf{A}_1\mathbf{S}]_2, [\mathbf{A}_1\mathbf{S}]_2 \\ [\mathbf{A}_1\mathbf{s}^\top]_2, [\mathbf{k}\mathbf{A}_1\mathbf{s}^\top]_T \cdot m \end{pmatrix}.$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, x)$: Let $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$. Pick $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_\ell, \mathbf{r}_{\mathsf{end}} \leftarrow \mathbb{Z}_p^{1\times k}$ and output

  $$\mathsf{sk}_x = \begin{pmatrix} [\mathbf{r}_0\mathbf{B}_1]_1, [\mathbf{r}_0\mathbf{B}_1\mathbf{W}_{\mathsf{start}}]_1 \\ \big\{[\mathbf{r}_j\mathbf{B}_1]_1, [\mathbf{r}_{j-1}\mathbf{B}_1\mathbf{Z}_{j \bmod 2} + \mathbf{r}_j\mathbf{B}_1\mathbf{W}_{x_j, j \bmod 2}]_1\big\}_{j\in[\ell]} \\ [\mathbf{r}_{\mathsf{end}}\mathbf{B}_1]_1, [\mathbf{r}_\ell\mathbf{B}_1\mathbf{Z}_{\mathsf{end}} + \mathbf{r}_{\mathsf{end}}\mathbf{B}_1\mathbf{W}_{\mathsf{end}}]_1 \\ [\mathbf{r}_{\mathsf{end}}\mathbf{B}_1\mathbf{W}_0 + \mathbf{k}]_1 \end{pmatrix}.$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_x, \mathsf{ct}_\Gamma)$: Parse key for $x = (x_1, \ldots, x_\ell)$ and ciphertext for $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ as

  $$\mathsf{sk}_x = \begin{pmatrix} [\mathbf{k}_{0,1}]_1, [\mathbf{k}_{0,2}]_1 \\ \big\{[\mathbf{k}_{j,1}]_1, [\mathbf{k}_{j,2}]_1\big\}_j \\ [\mathbf{k}_{\mathsf{end},1}]_1, [\mathbf{k}_{\mathsf{end},2}]_1 \\ [\mathbf{k}_{\mathsf{end}}]_1 \end{pmatrix} \quad \text{and} \quad \mathsf{ct}_\Gamma = \begin{pmatrix} [\mathbf{c}_{0,1}^\top]_2, [\mathbf{c}_{0,2}^\top]_2 \\ \big\{[\mathbf{C}_b]_2, [\mathbf{C}_{\sigma,b}]_2, [\mathbf{C}]_2\big\}_{\sigma,b} \\ [\mathbf{C}_{\mathsf{end},1}]_2, [\mathbf{C}_{\mathsf{end},2}]_2, [\mathbf{C}]_2 \\ [\mathbf{c}^\top]_2, C \end{pmatrix}.$$

  We define

  $$\mathbf{u}_{j,x}^\top = \mathbf{M}_{x_j} \cdots \mathbf{M}_{x_1}\mathbf{u}^\top \bmod p, \ \forall j \in [0, \ell]$$

  as (11) in Section 4.2 and proceed as follows:

1. Compute
$$B_0 = e([\mathbf{k}_{0,1}]_1, [\mathbf{c}_{0,1}^\top]_2) \cdot e([\mathbf{k}_{0,2}]_1, [\mathbf{c}_{0,2}^\top]_2)^{-1};$$
2. For all $j \in [\ell]$, compute
$$[\mathbf{b}_j]_T = e([\mathbf{k}_{j-1,1}]_1, [\mathbf{C}_{j \bmod 2}]_2) \cdot e([\mathbf{k}_{j,1}]_1, [\mathbf{C}_{x_j, j \bmod 2}]_2) \cdot e([-\mathbf{k}_{j,2}]_1, [\mathbf{C}]_2) \quad \text{and} \quad B_j = [\mathbf{b}_j \mathbf{u}_{j-1,x}^\top]_T;$$
3. Compute
$$[\mathbf{b}_{\text{end}}]_T = e([\mathbf{k}_{\ell,1}]_1, [\mathbf{C}_{\text{end},1}]_2) \cdot e([\mathbf{k}_{\text{end},1}]_1, [\mathbf{C}_{\text{end},2}]_2) \cdot e([-\mathbf{k}_{\text{end},2}]_1, [\mathbf{C}]_2) \quad \text{and} \quad B_{\text{end}} = [\mathbf{b}_{\text{end}} \mathbf{u}_{\ell,x}^\top]_T;$$
4. Compute
$$B_{\text{all}} = B_0 \cdot \textstyle\prod_{j=1}^{\ell} B_j \cdot B_{\text{end}} \quad \text{and} \quad B = B_{\text{all}}^{(\mathbf{f}\mathbf{u}_{\ell,x}^\top)^{-1}}$$
5. Compute
$$D = e([\mathbf{k}_{\text{end}}]_1, [\mathbf{c}^\top]_2) \cdot B^{-1}$$
and output the message $m' \leftarrow C \cdot D^{-1}$.

Correctness. For $x = (x_1, \ldots, x_\ell)$ and $\Gamma = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ such that $\Gamma(x) = 1$, we have:

$$\begin{aligned}
B_0 &= [\mathbf{r}_0\mathbf{B}_1\mathbf{D}\mathbf{u}^\top]_T = [\mathbf{r}_0\mathbf{B}_1\mathbf{D}\mathbf{u}_{0,x}^\top]_T && (50)\\
\mathbf{b}_j &= \mathbf{r}_j\mathbf{B}_1\mathbf{D}\mathbf{M}_{x_j} - \mathbf{r}_{j-1}\mathbf{B}_1\mathbf{D} && (51)\\
B_j &= [\mathbf{r}_j\mathbf{B}_1\mathbf{D}\mathbf{u}_{j,x}^\top - \mathbf{r}_{j-1}\mathbf{B}_1\mathbf{D}\mathbf{u}_{j-1,x}^\top]_T && (52)\\
\mathbf{b}_{\text{end}} &= \mathbf{r}_{\text{end}}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f} - \mathbf{r}_\ell\mathbf{B}_1\mathbf{D} && (53)\\
B_{\text{end}} &= [\mathbf{r}_{\text{end}}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}\mathbf{u}_{\ell,x}^\top - \mathbf{r}_\ell\mathbf{B}_1\mathbf{D}\mathbf{u}_{\ell,x}^\top]_T && (54)\\
B_{\text{all}} &= [\mathbf{r}_{\text{end}}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}\mathbf{u}_{\ell,x}^\top]_T && (55)\\
B &= [\mathbf{r}_{\text{end}}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)]_T && (56)\\
D &= [\mathbf{k}\mathbf{A}_1\mathbf{s}^\top]_T && (57)
\end{aligned}$$

Here (54) is trivial; (52) and (56) follow from facts (19); the remaining equalities follow from:

$$\begin{aligned}
&(50) & \mathbf{r}_0\mathbf{B}_1\mathbf{D}\mathbf{u}^\top &= \mathbf{r}_0\mathbf{B}_1 \cdot (\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\text{start}}\mathbf{A}_1\mathbf{S}\mathbf{u}^\top) - \mathbf{r}_0\mathbf{B}_1\mathbf{W}_{\text{start}} \cdot \mathbf{A}_1\mathbf{S}\mathbf{u}^\top\\
&(51) & \mathbf{r}_j\mathbf{B}_1\mathbf{D}\mathbf{M}_{x_j} - \mathbf{r}_{j-1}\mathbf{B}_1\mathbf{D} &= \mathbf{r}_{j-1}\mathbf{B}_1 \cdot (-\mathbf{D} + \mathbf{Z}_{j \bmod 2}\mathbf{A}_1\mathbf{S}) + \mathbf{r}_j\mathbf{B}_1 \cdot (\mathbf{D}\mathbf{M}_{x_j} + \mathbf{W}_{x_j, j \bmod 2}\mathbf{A}_1\mathbf{S})\\
&&&\qquad - (\mathbf{r}_{j-1}\mathbf{B}_1\mathbf{Z}_{j \bmod 2} + \mathbf{r}_j\mathbf{B}_1\mathbf{W}_{x_j, j \bmod 2}) \cdot \mathbf{A}_1\mathbf{S}\\
&(53) & \mathbf{r}_{\text{end}}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f} - \mathbf{r}_\ell\mathbf{B}_1\mathbf{D} &= \mathbf{r}_\ell\mathbf{B}_1 \cdot (-\mathbf{D} + \mathbf{Z}_{\text{end}}\mathbf{A}_1\mathbf{S}) + \mathbf{r}_{\text{end}}\mathbf{B}_1 \cdot (\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top\mathbf{f} + \mathbf{W}_{\text{end}}\mathbf{A}_1\mathbf{S}) - (\mathbf{r}_\ell\mathbf{B}_1\mathbf{Z}_{\text{end}} + \mathbf{r}_{\text{end}}\mathbf{B}_1\mathbf{W}_{\text{end}}) \cdot \mathbf{A}_1\mathbf{S}\\
&(55) & \mathbf{r}_{\text{end}}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}\mathbf{u}_{\ell,x}^\top &= \mathbf{r}_0\mathbf{B}_1\mathbf{D}\mathbf{u}_{0,x}^\top + \textstyle\sum_{j=1}^{\ell}(\mathbf{r}_j\mathbf{B}_1\mathbf{D}\mathbf{u}_{j,x}^\top - \mathbf{r}_{j-1}\mathbf{B}_1\mathbf{D}\mathbf{u}_{j-1,x}^\top) + (\mathbf{r}_{\text{end}}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}\mathbf{u}_{\ell,x}^\top - \mathbf{r}_\ell\mathbf{B}_1\mathbf{D}\mathbf{u}_{\ell,x}^\top)\\
&(57) & \mathbf{k}\mathbf{A}_1\mathbf{s}^\top &= (\mathbf{r}_{\text{end}}\mathbf{B}_1\mathbf{W}_0 + \mathbf{k}) \cdot \mathbf{A}_1\mathbf{s}^\top - \mathbf{r}_{\text{end}}\mathbf{B}_1\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top
\end{aligned}$$

Correctness follows readily.

I.3 Adaptive Security

We prove the following theorem.

Theorem 6 (Adaptively Secure CP-ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$). *The ABE scheme for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in prime-order bilinear groups described in Section I.2 is adaptively secure (cf. Section 2.1) under the k-Lin assumption with security loss $O(q \cdot \ell \cdot |\Sigma|^3 \cdot Q^2)$. Here ℓ is the maximum length of the q key queries.*

The proof employs standard dual system argument where we handle key queries one by one; for each key, we rely on the core lemma, Lemma 19, for our adaptively secure KP-ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ (in Section 5). We only show the game sequence and sketch the proof.

Auxiliary distributions. We use $\Gamma^* = (Q, \Sigma, \{\mathbf{M}_\sigma\}_{\sigma\in\Sigma}, \mathbf{u}, \mathbf{f})$ to denote the adaptive challenge NFA and $x = (x_1, \ldots, x_\ell)$ a key query. We describe the auxiliary ciphertext and key distributions that we use in the proof.

Ciphertext distributions. We sample $\hat{\mathbf{S}} \leftarrow \mathbb{Z}_p^{k\times Q}$, $\hat{\mathbf{s}} \leftarrow \mathbb{Z}_p^{1\times k}$ and define:

- N: the real ciphertext in the scheme;
- SF: identical to an N ciphertext except that we replace $\mathbf{A}_1\mathbf{S}$ and $\mathbf{A}_1\mathbf{s}^\top$ with $\mathbf{A}_1\mathbf{S}+\mathbf{A}_2\hat{\mathbf{S}}$ and $\mathbf{A}_1\mathbf{s}^\top+\mathbf{A}_2\hat{\mathbf{s}}^\top$, respectively.

That is, we write

$$\mathsf{ct}_{\Gamma^*}^{\mathsf{SF}} = \begin{pmatrix} [\mathbf{D}\mathbf{u}^\top + \mathbf{W}_{\mathrm{start}}(\mathbf{A}_1\mathbf{S}+\boxed{\mathbf{A}_2\hat{\mathbf{S}}})\mathbf{u}^\top]_2, [(\mathbf{A}_1\mathbf{S}+\boxed{\mathbf{A}_2\hat{\mathbf{S}}})\mathbf{u}^\top]_2 \\ \{[-\mathbf{D}+\mathbf{Z}_b(\mathbf{A}_1\mathbf{S}+\boxed{\mathbf{A}_2\hat{\mathbf{S}}})]_2, [\mathbf{D}\mathbf{M}_\sigma + \mathbf{W}_{\sigma,b}(\mathbf{A}_1\mathbf{S}+\boxed{\mathbf{A}_2\hat{\mathbf{S}}})]_2, [\mathbf{A}_1\mathbf{S}+\boxed{\mathbf{A}_2\hat{\mathbf{S}}}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{D}+\mathbf{Z}_{\mathrm{end}}(\mathbf{A}_1\mathbf{S}+\boxed{\mathbf{A}_2\hat{\mathbf{S}}})]_2, [(\mathbf{W}_0(\mathbf{A}_1\mathbf{s}^\top+\boxed{\mathbf{A}_2\hat{\mathbf{s}}^\top}))\mathbf{f}+\mathbf{W}_{\mathrm{end}}(\mathbf{A}_1\mathbf{S}+\boxed{\mathbf{A}_2\hat{\mathbf{S}}})]_2, [\mathbf{A}_1\mathbf{S}+\boxed{\mathbf{A}_2\hat{\mathbf{S}}}]_2 \\ [\mathbf{A}_1\mathbf{s}^\top+\boxed{\mathbf{A}_2\hat{\mathbf{s}}^\top}]_2, [\mathbf{k}(\mathbf{A}_1\mathbf{s}^\top+\boxed{\mathbf{A}_2\hat{\mathbf{s}}^\top})]_T \cdot m_\beta \end{pmatrix}.$$

Secret key distributions. We sample $\mathbf{\Delta} \leftarrow \mathbb{Z}_p^{1\times k}$, $\hat{\mathbf{r}}_j, \hat{\mathbf{r}}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$ for all $j \in [0,\ell]$ and define

- N: the real key in the scheme;
- SF: identical to an N key except that we replace $\mathbf{k}$ with $\mathbf{\Delta}\mathbf{A}_2^\perp + \mathbf{k}$;
- $\mathsf{P\text{-}N}$: identical to an N key except that we replace $\mathbf{r}_j\mathbf{B}_1$, $\mathbf{r}_{\mathrm{end}}\mathbf{B}_1$ with $\mathbf{r}_j\mathbf{B}_1+\hat{\mathbf{r}}_j\mathbf{B}_2$, $\mathbf{r}_{\mathrm{end}}\mathbf{B}_1+\hat{\mathbf{r}}_{\mathrm{end}}\mathbf{B}_2$;
- $\mathsf{P\text{-}SF}$: identical to an SF key except that we replace $\mathbf{r}_j\mathbf{B}_1$, $\mathbf{r}_{\mathrm{end}}\mathbf{B}_1$ with $\mathbf{r}_j\mathbf{B}_1+\hat{\mathbf{r}}_j\mathbf{B}_2$, $\mathbf{r}_{\mathrm{end}}\mathbf{B}_1+\hat{\mathbf{r}}_{\mathrm{end}}\mathbf{B}_2$.

That is, we write

$$\mathsf{sk}_x^{\mathsf{SF}} = \begin{pmatrix} [\mathbf{r}_0\mathbf{B}_1]_1,\ [\mathbf{r}_0\mathbf{B}_1\mathbf{W}_{\mathrm{start}}]_1 \\ \{[\mathbf{r}_j\mathbf{B}_1]_1, [\mathbf{r}_{j-1}\mathbf{B}_1\mathbf{Z}_{j \bmod 2} + \mathbf{r}_j\mathbf{B}_1\mathbf{W}_{x_j, j \bmod 2}]_1\}_{j\in[\ell]} \\ [\mathbf{r}_{\mathrm{end}}\mathbf{B}_1]_1, [\mathbf{r}_\ell\mathbf{B}_1\mathbf{Z}_{\mathrm{end}} + \mathbf{r}_{\mathrm{end}}\mathbf{B}_1\mathbf{W}_{\mathrm{end}}]_1, \\ [\mathbf{r}_{\mathrm{end}}\mathbf{B}_1\mathbf{W}_0 + \boxed{\mathbf{\Delta}\mathbf{A}_2^\perp} + \mathbf{k}]_1 \end{pmatrix};$$

$$\mathsf{sk}_x^{\mathsf{P\text{-}N}} = \begin{pmatrix} [\mathbf{r}_0\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_0\mathbf{B}_2}]_1,\ [(\mathbf{r}_0\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_0\mathbf{B}_2})\mathbf{W}_{\mathrm{start}}]_1 \\ \{[\mathbf{r}_j\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_j\mathbf{B}_2}]_1, [(\mathbf{r}_{j-1}\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_{j-1}\mathbf{B}_2})\mathbf{Z}_{j \bmod 2} + (\mathbf{r}_j\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_j\mathbf{B}_2})\mathbf{W}_{x_j, j \bmod 2}]_1\}_{j\in[\ell]} \\ [\mathbf{r}_{\mathrm{end}}\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_{\mathrm{end}}\mathbf{B}_2}]_1, [(\mathbf{r}_\ell\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_\ell\mathbf{B}_2})\mathbf{Z}_{\mathrm{end}} + (\mathbf{r}_{\mathrm{end}}\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_{\mathrm{end}}\mathbf{B}_2})\mathbf{W}_{\mathrm{end}}]_1, \\ [(\mathbf{r}_{\mathrm{end}}\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_{\mathrm{end}}\mathbf{B}_2})\mathbf{W}_0 + \mathbf{k}]_1 \end{pmatrix};$$

$$\mathsf{sk}_x^{\mathsf{P\text{-}SF}} = \begin{pmatrix} [\mathbf{r}_0\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_0\mathbf{B}_2}]_1,\ [(\mathbf{r}_0\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_0\mathbf{B}_2})\mathbf{W}_{\mathrm{start}}]_1 \\ \{[\mathbf{r}_j\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_j\mathbf{B}_2}]_1, [(\mathbf{r}_{j-1}\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_{j-1}\mathbf{B}_2})\mathbf{Z}_{j \bmod 2} + (\mathbf{r}_j\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_j\mathbf{B}_2})\mathbf{W}_{x_j, j \bmod 2}]_1\}_{j\in[\ell]} \\ [\mathbf{r}_{\mathrm{end}}\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_{\mathrm{end}}\mathbf{B}_2}]_1, [(\mathbf{r}_\ell\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_\ell\mathbf{B}_2})\mathbf{Z}_{\mathrm{end}} + (\mathbf{r}_{\mathrm{end}}\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_{\mathrm{end}}\mathbf{B}_2})\mathbf{W}_{\mathrm{end}}]_1, \\ [(\mathbf{r}_{\mathrm{end}}\mathbf{B}_1+\boxed{\hat{\mathbf{r}}_{\mathrm{end}}\mathbf{B}_2})\mathbf{W}_0 + \mathbf{\Delta}\mathbf{A}_2^\perp + \mathbf{k}]_1 \end{pmatrix}.$$

Game sequences. We prove Theorem 6 via a series of games following the standard dual system method [20,22,4]:

- G_0: Identical to the real game where all keys and challenge ciphertext are $\mathsf{sk}_x^{\mathsf{N}}$ and $\mathsf{ct}_{\Gamma^*}^{\mathsf{N}}$, respectively.
- G_1: Identical to G_0 except that the challenge ciphertext is $\mathsf{ct}_{\Gamma^*}^{\mathsf{SF}}$.
- $\mathsf{G}_{2.\kappa.0}$ for $\kappa \in [q]$: Identical to G_1 except that the first $\kappa - 1$ secret keys are $\mathsf{sk}_x^{\mathsf{SF}}$.
- $\mathsf{G}_{2.\kappa.1}$ for $\kappa \in [q]$: Identical to $\mathsf{G}_{2.\kappa.0}$ except that the κ-th secret key is $\mathsf{sk}_x^{\mathsf{P\text{-}N}}$.
- $\mathsf{G}_{2.\kappa.2}$ for $\kappa \in [q]$: Identical to $\mathsf{G}_{2.\kappa.1}$ except that the κ-th secret key is $\mathsf{sk}_x^{\mathsf{P\text{-}SF}}$.
- $\mathsf{G}_{2.\kappa.3}$ for $\kappa \in [q]$: Identical to $\mathsf{G}_{2.\kappa.2}$ except that the κ-th secret key $\mathsf{sk}_x^{\mathsf{SF}}$.
- G_3: Identical to $\mathsf{G}_{2.q.3}$ except that the challenge ciphertext is an encryption of a random message.

Note that we have $\mathsf{G}_{2.1.0} = \mathsf{G}_1$ and $\mathsf{G}_{2.\kappa.0} = \mathsf{G}_{2.\kappa-1.3}$ for $q \in [2, q]$.

Proof sketch. Most proofs are standard: $\mathsf{G}_0 \approx_c \mathsf{G}_1$ follows from $\mathrm{SD}^{G_2}_{\mathbf{A}_1 \mapsto \mathbf{A}_1, \mathbf{A}_2}$ assumption; both $\mathsf{G}_{2.\kappa.0} \approx_c \mathsf{G}_{2.\kappa.1}$ and $\mathsf{G}_{2.\kappa.2} \approx_c \mathsf{G}_{2.\kappa.3}$ with $\kappa \in [q]$ follow from $\mathrm{SD}^{G_1}_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_2}$ assumption and $\mathsf{G}_{2.q.3} \approx_s \mathsf{G}_3$ is straightforward by a standard statistical argument involving $\mathbf{k}$ and $\mathbf{\Delta}$. We focus on $\mathsf{G}_{2.\kappa.1} \approx_c \mathsf{G}_{2.\kappa.2}$ for all $\kappa \in [q]$.

Lemma 62 ($\mathsf{G}_{2.\kappa.1} \approx_c \mathsf{G}_{2.\kappa.2}$)**.** *For all $\kappa \in [q]$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ and*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.1} \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.2} \rangle = 1] \le O(\ell \cdot |\Sigma|^3 \cdot Q^2) \cdot \mathsf{Adv}^{k\text{-}\textsc{Lin}}_{\mathcal{B}}(\lambda)$$

Proof (sketch). We use the core lemma, Lemma 19, to prove the lemma. By the core lemma, it is sufficient to prove that for all κ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.1} \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.2} \rangle = 1] \le \mathsf{Adv}^{\textsc{core}}_{\mathcal{B}}(\lambda).$$

For this, we define two auxiliary games $\hat{\mathsf{G}}_{2.\kappa.1}$ and $\hat{\mathsf{G}}_{2.\kappa.2}$ by the following change of variables in both $\mathsf{G}_{2.\kappa,1}$ and $\mathsf{G}_{2.\kappa.2}$:

$$\begin{aligned}
\mathbf{W}_{\mathrm{start}} &\mapsto \mathbf{W}_{\mathrm{start}} + \mathbf{B}_2^{\perp} \hat{\mathbf{W}}_{\mathrm{start}} \mathbf{A}_2^{\perp}, \\
\mathbf{Z}_b &\mapsto \mathbf{Z}_b + \mathbf{B}_2^{\perp} \hat{\mathbf{Z}}_b \mathbf{A}_2^{\perp}, \quad \forall b \in \{0,1\}, \\
\mathbf{W}_{\sigma,b} &\mapsto \mathbf{W}_{\sigma,b} + \mathbf{B}_2^{\perp} \hat{\mathbf{W}}_{\sigma,b} \mathbf{A}_2^{\perp}, \quad \forall \sigma \in \Sigma, b \in \{0,1\} \\
\mathbf{Z}_{\mathrm{end}} &\mapsto \mathbf{Z}_{\mathrm{end}} + \mathbf{B}_2^{\perp} \hat{\mathbf{Z}}_{\mathrm{end}} \mathbf{A}_2^{\perp}, \\
\mathbf{W}_{\mathrm{end}} &\mapsto \mathbf{W}_{\mathrm{end}} + \mathbf{B}_2^{\perp} \hat{\mathbf{W}}_{\mathrm{end}} \mathbf{A}_2^{\perp}, \\
\mathbf{D} &\mapsto \mathbf{D} + \mathbf{B}_2^{\perp} \hat{\mathbf{D}}
\end{aligned}$$

and

$$\mathbf{W}_0 \mapsto \mathbf{W}_0 - \mathbf{B}_2^{\perp} \big(\beta (\hat{\mathbf{r}}_{\mathrm{end}} \hat{\mathbf{b}}_2^{\perp})^{-1} \cdot \hat{\mathbf{b}}_2^{\perp} \mathbf{\Delta} \big) \mathbf{A}_2^{\perp}, \quad \text{where} \quad \beta = \begin{cases} 0 & \text{in } \mathsf{G}_{2.\kappa.1} \\ 1 & \text{in } \mathsf{G}_{2.\kappa.2} \end{cases}$$

where $\hat{\mathbf{W}}_{\mathrm{start}}, \hat{\mathbf{Z}}_b, \hat{\mathbf{W}}_{\sigma,b}, \hat{\mathbf{Z}}_{\mathrm{end}}, \hat{\mathbf{W}}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ for all $\sigma \in \Sigma, b \in \{0,1\}$, $\hat{\mathbf{D}} \leftarrow \mathbb{Z}_p^{(2k+1)\times Q}$ and $\hat{\mathbf{b}}_2^{\perp} \leftarrow \mathbb{Z}_p^{2k+1}$. Looking ahead, $\hat{\mathbf{b}}_2^{\perp}$ is a part of dual basis of (59) defined later. It is clear that we have

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.1} \rangle = 1] = \Pr[\langle \mathcal{A}, \hat{\mathsf{G}}_{2.\kappa.1} \rangle = 1] \quad \text{and} \quad \Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.2} \rangle = 1] = \Pr[\langle \mathcal{A}, \hat{\mathsf{G}}_{2.\kappa.2} \rangle = 1]$$

since the change of variables does not change the two games. Now it is sufficient to prove that

$$\Pr[\langle \mathcal{A}, \hat{\mathsf{G}}_{2.\kappa.1} \rangle = 1] - \Pr[\langle \mathcal{A}, \hat{\mathsf{G}}_{2.\kappa.2} \rangle = 1] \le \mathsf{Adv}^{\textsc{core}}_{\mathcal{B}}(\lambda). \tag{58}$$

Observe that, in the new games, we have mpk, $\mathsf{sk}_x^{\mathsf{N}}$ and $\mathsf{sk}_x^{\mathsf{SF}}$ unchanged due to the fact that $\mathbf{A}_2^{\perp}\mathbf{A}_1 = \mathbf{0}$ and $\mathbf{B}_1\mathbf{B}_2^{\perp} = \mathbf{0}$; the challenge ciphertext is in the form of

$$\mathsf{ct}^{\mathsf{SF}}_{\Gamma^*} \cdot \boxed{\begin{pmatrix} [\mathbf{B}_2^{\perp}\hat{\mathbf{D}}\mathbf{u}^{\top} + \mathbf{B}_2^{\perp}\hat{\mathbf{W}}_{\mathrm{start}}\hat{\mathbf{S}}\mathbf{u}^{\top}]_2, [\mathbf{0}]_2 \\ \{[-\mathbf{B}_2^{\perp}\hat{\mathbf{D}} + \mathbf{B}_2^{\perp}\hat{\mathbf{Z}}_b\hat{\mathbf{S}}]_2, [\mathbf{B}_2^{\perp}\hat{\mathbf{D}}\mathbf{M}_{\sigma} + \mathbf{B}_2^{\perp}\hat{\mathbf{W}}_{\sigma,b}\hat{\mathbf{S}}]_2, [\mathbf{0}]_2\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\mathbf{B}_2^{\perp}\hat{\mathbf{D}} + \mathbf{B}_2^{\perp}\hat{\mathbf{Z}}_{\mathrm{end}}\hat{\mathbf{S}}]_2, [-\mathbf{B}_2^{\perp} \cdot \beta(\hat{\mathbf{r}}_{\mathrm{end}}\hat{\mathbf{b}}_2^{\perp})^{-1} \cdot \hat{\mathbf{b}}_2^{\perp}\mathbf{\Delta}\hat{\mathbf{s}}^{\top} \cdot \mathbf{f} + \mathbf{B}_2^{\perp}\hat{\mathbf{W}}_{\mathrm{end}}\hat{\mathbf{S}}]_2, [\mathbf{0}]_2 \\ [\mathbf{0}]_2, [\mathbf{0}]_T \end{pmatrix}} \quad \text{where} \quad \beta = \begin{cases} 0 & \text{in } \hat{\mathsf{G}}_{2.\kappa.1} \\ 1 & \text{in } \hat{\mathsf{G}}_{2.\kappa.2} \end{cases}$$

while the κ-th key in the two games are in the form of

$$\mathsf{sk}_x^{\mathsf{P\text{-}N}} \cdot \boxed{\begin{pmatrix} [\mathbf{0}]_1,\ [\hat{\mathbf{r}}_0\hat{\mathbf{W}}_{\mathrm{start}}\mathbf{A}_2^{\perp}]_1 \\ \{[\mathbf{0}]_1, [\hat{\mathbf{r}}_{j-1}\hat{\mathbf{Z}}_{j \bmod 2}\mathbf{A}_2^{\perp} + \hat{\mathbf{r}}_j\hat{\mathbf{W}}_{x_j, j \bmod 2}\mathbf{A}_2^{\perp}]_1\}_{j\in[\ell]} \\ [\mathbf{0}]_1, [\hat{\mathbf{r}}_{\ell}\hat{\mathbf{Z}}_{\mathrm{end}}\mathbf{A}_2^{\perp} + \hat{\mathbf{r}}_{\mathrm{end}}\hat{\mathbf{W}}_{\mathrm{end}}\mathbf{A}_2^{\perp}]_1 \\ [\mathbf{0}]_1 \end{pmatrix}}.$$

It is clear that the two games are identical except that boxed parts, so it is sufficient to prove the indistinguishability between the boxed parts in games. Formally, we capture this by the following claim. Note that we neglect $\mathbf{B}_2^{\perp}$ and $\mathbf{A}_2^{\perp}$ which are unrelated to the argument and give out $\hat{\mathbf{S}}$ and $\hat{\mathbf{r}}_j, \hat{\mathbf{r}}_{\mathrm{end}}$ in order to simulate $\mathsf{ct}^{\mathsf{SF}}_{\Gamma^*}$-part of the challenge ciphertext and $\mathsf{sk}_x^{\mathsf{P\text{-}N}}$-part of the κ-th key.

Claim. For all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ and

$$\Pr[\langle \mathcal{A}, \mathsf{H}_0 \rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{H}_1 \rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\mathrm{CORE}}(\lambda)$$

where we define:

$$\langle \mathcal{A}, \mathsf{H}_\beta \rangle := \left\{ \beta' \leftarrow \mathcal{A}^{\mathsf{OEnc}(\cdot),\mathsf{OKey}(\cdot)} \right\}$$

and the two oracles work as follows:

- $\mathsf{OEnc}(\Gamma)$: output

$$\begin{pmatrix} [\hat{\mathbf{D}}\mathbf{u}^\top + \hat{\mathbf{W}}_{\mathrm{start}}\hat{\mathbf{S}}\mathbf{u}^\top]_2, [\hat{\mathbf{S}}\mathbf{u}^\top]_2 \\ \left\{ [-\hat{\mathbf{D}} + \hat{\mathbf{Z}}_b\hat{\mathbf{S}}]_2, [\hat{\mathbf{D}}\mathbf{M}_\sigma + \hat{\mathbf{W}}_{\sigma,b}\hat{\mathbf{S}}]_2, [\hat{\mathbf{S}}]_2 \right\}_{\sigma\in\Sigma, b\in\{0,1\}} \\ [-\hat{\mathbf{D}} + \hat{\mathbf{Z}}_{\mathrm{end}}\hat{\mathbf{S}}]_2, [\beta(\hat{\mathbf{r}}_{\mathrm{end}}\hat{\mathbf{b}}_2^\perp)^{-1} \cdot \hat{\mathbf{b}}_2^\perp \mathbf{\Delta}\hat{\mathbf{s}}^\top \cdot \mathbf{f} + \hat{\mathbf{W}}_{\mathrm{end}}\hat{\mathbf{S}}]_2, [\hat{\mathbf{S}}]_2 \end{pmatrix}$$

- $\mathsf{OKey}(x)$: output

$$\begin{pmatrix} [\hat{\mathbf{r}}_0]_1,\ [\hat{\mathbf{r}}_0\hat{\mathbf{W}}_{\mathrm{start}}]_1 \\ \left\{ [\hat{\mathbf{r}}_j]_1, [\hat{\mathbf{r}}_{j-1}\hat{\mathbf{Z}}_{j \bmod 2} + \hat{\mathbf{r}}_j\hat{\mathbf{W}}_{x_j, j \bmod 2}]_1 \right\}_{j\in[\ell]} \\ [\hat{\mathbf{r}}_{\mathrm{end}}]_1, [\hat{\mathbf{r}}_\ell\hat{\mathbf{Z}}_{\mathrm{end}} + \hat{\mathbf{r}}_{\mathrm{end}}\hat{\mathbf{W}}_{\mathrm{end}}]_1 \end{pmatrix}$$

with the restrictions that (1) $\mathcal{A}$ makes only one query to each oracle; (2) queries Γ and x satisfy $\Gamma(x) = 0$.

It is direct to verify that the terms given out in the claim are sufficient to simulate both games and readily implies (58). This leaves us with the proof for the claim which is sketched as follows.

Proof of Claim (sketch). The claim relies on the core lemma, Lemma 19, for adaptively secure KP-ABE for $\mathcal{E}_Q$-restricted NFA$^{\oplus p}$ in Section 5. Consider another set of basis which is motivated by that used for our KP-ABE for $\mathcal{E}_Q$-NFA$^{\oplus p}$, i.e.,

$$\hat{\mathbf{B}}_1 \leftarrow \mathbb{Z}_p^{k\times(2k+1)}, \quad \hat{\mathbf{b}}_2 \leftarrow \mathbb{Z}_p^{1\times(2k+1)}, \quad \hat{\mathbf{B}}_3 \leftarrow \mathbb{Z}_p^{k\times(2k+1)} \tag{59}$$

and use $(\hat{\mathbf{B}}_1^\perp, \hat{\mathbf{b}}_2^\perp, \hat{\mathbf{B}}_2^\perp) \in \mathbb{Z}_p^{(2k+1)\times k} \times \mathbb{Z}_p^{2k+1} \times \mathbb{Z}_p^{(2k+1)\times k}$ to denote this dual as in Section 4.1. Note that $\hat{\mathbf{b}}_2$ has appeared in the reply of $\mathsf{OEnc}(\Gamma)$. Then we define two auxiliary games as follows:

- H'_β is identical to H_β except that we sample $\hat{\mathbf{r}}_j \leftarrow \mathsf{span}(\hat{\mathbf{B}}_1)$ for all $j \in [0,\ell]$ and $\hat{\mathbf{r}}_{\mathrm{end}} \leftarrow \mathsf{span}(\hat{\mathbf{B}}_1, \hat{\mathbf{b}}_2)$.

It is direct to prove that

- $\mathsf{H}_0 \approx_c \mathsf{H}'_0$ by $\mathrm{SD}^{G_1}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_3}$ assumption (for $\hat{\mathbf{r}}_{\mathrm{end}}$) and $\mathrm{SD}^{G_1}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{b}_2,\mathbf{B}_3}$ assumption (for $\hat{\mathbf{r}}_j$);
- $\mathsf{H}_1 \approx_c \mathsf{H}'_1$ by $\mathrm{SD}^{G_1}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{B}_3}$ assumption and $(\cdot, \hat{\mathbf{W}}_{\mathrm{end}})$-switching lemma (for $\hat{\mathbf{r}}_j$) due to the presence of $\hat{\mathbf{b}}_2^\perp$;
- $\mathsf{H}'_0 \approx_c \mathsf{H}'_1$ by the core lemma, Lemma 19.

This readily proves the claim and the lemma. □

J Adaptively Secure CP-ABE for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$ and BP

In this section, we construct a compact adaptively secure CP-ABE for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$. The scheme is based on our KP-ABE for the same class in Section 6 and dual conversion in [4,6]. This readily gives us a compact adaptively secure CP-ABE for BP by Lemma 23 where the key size grows linearly with the length of input and independent of the program size.

J.1 Basis

We will use the following two sets of bases for ciphertexts and keys, respectively:

$$\mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{2k\times k} \quad \text{and} \quad (\mathbf{B}_1, \mathbf{b}_2) \leftarrow \mathbb{Z}_p^{k\times(k+1)} \times \mathbb{Z}_p^{1\times(k+1)}.$$

We use $\mathbf{A}_1^\perp, \mathbf{A}_2^\perp \in \mathbb{Z}_p^{k\times 2k}$ to denote the dual basis of $(\mathbf{A}_1, \mathbf{A}_2)$ such that $\mathbf{A}_i^\perp\mathbf{A}_i = \mathbf{I}$ for $i \in \{1,2\}$ and $\mathbf{A}_i^\perp\mathbf{A}_j = \mathbf{0}$ for $i \ne j$. Analogously, we use $(\mathbf{B}_1^\perp, \mathbf{b}_2^\perp) \in \mathbb{Z}_p^{(k+1)\times k} \times \mathbb{Z}_p^{(k+1)\times 1}$ to denote the dual basis of $(\mathbf{B}_1, \mathbf{b}_2)$. In the proof, we will use $\mathrm{SD}^{G_2}_{\mathbf{A}_1 \mapsto \mathbf{A}_1,\mathbf{A}_2}$ and $\mathrm{SD}^{G_1}_{\mathbf{B}_1 \mapsto \mathbf{B}_1,\mathbf{b}_2}$ assumption, cf. Section 4.1.

J.2 Scheme

For notational convenience, especially reusing the branching program notations in Section 6, we will generate ciphertexts over G_2 and keys over G_1. Our CP-ABE for $\mathcal{E}_Q$-restricted $\mathsf{NBP}^{\oplus p}$ in prime-order groups is described as follows:

- $\mathsf{Setup}(1^\lambda,\ell,\Sigma)$: Run $\mathbb{G}=(p,G_1,G_2,G_T,e)\leftarrow\mathcal{G}(1^\lambda)$. Sample

$$\mathbf{A}_1\leftarrow\mathbb{Z}_p^{2k\times k},\ \mathbf{B}_1\leftarrow\mathbb{Z}_p^{k\times(k+1)},\ \mathbf{k}\leftarrow\mathbb{Z}_p^{1\times 2k}\quad\text{and}\quad \mathbf{W}_{\mathsf{start}},\mathbf{W}_{\eta,\sigma},\mathbf{W}_{\mathsf{end}},\mathbf{W}_0\leftarrow\mathbb{Z}_p^{(k+1)\times 2k},\ \forall\,\eta\in[\ell],\sigma\in\Sigma.$$

  Output

$$\begin{aligned}\mathsf{mpk}&=\big([\mathbf{A}_1,\mathbf{W}_{\mathsf{start}}\mathbf{A}_1,\{\mathbf{W}_{\eta,\sigma}\mathbf{A}_1\}_{\eta\in[\ell],\sigma\in\Sigma},\mathbf{W}_{\mathsf{end}}\mathbf{A}_1,\mathbf{W}_0\mathbf{A}_1]_2,\ [\mathbf{k}\mathbf{A}_1]_T\big)\\ \mathsf{msk}&=\big(\mathbf{k},\mathbf{B}_1,\mathbf{W}_{\mathsf{start}},\{\mathbf{W}_{\eta,\sigma}\}_{\eta\in[\ell],\sigma\in\Sigma},\mathbf{W}_{\mathsf{end}},\mathbf{W}_0\big).\end{aligned}$$

- $\mathsf{Enc}(\mathsf{mpk},\Gamma,m)$: Let $\Gamma=(Q,\ell_{\mathrm{BP}},\ell,\Sigma,\{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma},\rho,\mathbf{u},\mathbf{f})$ and $m\in G_T$. Pick

$$\mathbf{D}_0,\mathbf{D}_1,\ldots,\mathbf{D}_{\ell_{\mathrm{BP}}}\leftarrow\mathbb{Z}_p^{(k+1)\times Q},\ \mathbf{S}_1,\ldots,\mathbf{S}_{\ell_{\mathrm{BP}}},\mathbf{S}_{\mathsf{end}}\leftarrow\mathbb{Z}_p^{k\times Q},\ \mathbf{s}_{\mathsf{start}},\mathbf{s}\leftarrow\mathbb{Z}_p^{1\times k}$$

  and output

$$\mathsf{ct}_\Gamma=\left(\begin{array}{c}[\mathbf{D}_0\mathbf{u}^\top+\mathbf{W}_{\mathsf{start}}\mathbf{A}_1\mathbf{s}_{\mathsf{start}}^\top]_2,\ [\mathbf{A}_1\mathbf{s}_{\mathsf{start}}^\top]_2\\ \big\{[\mathbf{D}_j\mathbf{M}_{j,\sigma}-\mathbf{D}_{j-1}+\mathbf{W}_{\rho(j),\sigma}\mathbf{A}_1\mathbf{S}_j]_2,\ [\mathbf{A}_1\mathbf{S}_j]_2\big\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}\\ [(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}-\mathbf{D}_{\ell_{\mathrm{BP}}}+\mathbf{W}_{\mathsf{end}}\mathbf{A}_1\mathbf{S}_{\mathsf{end}}]_2,\ [\mathbf{A}_1\mathbf{S}_{\mathsf{end}}]_2\\ [\mathbf{A}_1\mathbf{s}^\top]_2,\ [\mathbf{k}\mathbf{A}_1\mathbf{s}^\top]_T\cdot m\end{array}\right).$$

- $\mathsf{KeyGen}(\mathsf{mpk},\mathsf{msk},x)$: Let $x=(x_1,\ldots,x_\ell)\in\Sigma^\ell$. Pick $\mathbf{r}\leftarrow\mathbb{Z}_p^{1\times k}$ and output

$$\mathsf{sk}_x=\Big([\mathbf{r}\mathbf{B}_1]_1,\ [\mathbf{r}\mathbf{B}_1\mathbf{W}_0+\mathbf{k}]_1,\ [\mathbf{r}\mathbf{B}_1\mathbf{W}_{\mathsf{start}}]_1,\ \{[\mathbf{r}\mathbf{B}_1\mathbf{W}_{\eta,x_\eta}]_1\}_{\eta\in[\ell]},\ [\mathbf{r}\mathbf{B}_1\mathbf{W}_{\mathsf{end}}]_1\Big).$$

- $\mathsf{Dec}(\mathsf{mpk},\mathsf{sk}_x,\mathsf{ct}_\Gamma)$: Parse key for $x=(x_1,\ldots,x_\ell)$ and ciphertext for $\Gamma=(Q,\ell_{\mathrm{BP}},\ell,\Sigma,\{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma},\rho,\mathbf{u},\mathbf{f})$ as

$$\mathsf{sk}_x=\big([\mathbf{r}_0]_1,[\mathbf{k}_0]_1,[\mathbf{k}_{\mathsf{start}}]_1,\{[\mathbf{k}_\eta]_1\}_\eta,[\mathbf{k}_{\mathsf{end}}]_1\big)\quad\text{and}\quad\mathsf{ct}_\Gamma=\left(\begin{array}{c}[\mathbf{c}_{\mathsf{start},1}^\top]_2,[\mathbf{c}_{\mathsf{start},2}^\top]_2\\ \big\{[\mathbf{C}_{j,\sigma}]_2,[\mathbf{C}_j]_2\big\}_{j,\sigma}\\ [\mathbf{C}_{\mathsf{end},1}]_2,[\mathbf{C}_{\mathsf{end},2}]_2\\ [\mathbf{c}^\top]_2,C\end{array}\right).$$

  We define

$$\mathbf{u}_{j,x}^\top=\mathbf{M}_{j,x_{\rho(j)}}\cdots\mathbf{M}_{1,x_{\rho(1)}}\mathbf{u}^\top \bmod p,\ \forall\,j\in[0,\ell_{\mathrm{BP}}]$$

  as (30) in Section 6.2 and proceed as follows:

  1. Compute

$$B_{\mathsf{start}}=e([\mathbf{r}_0]_1,[\mathbf{c}_{\mathsf{start},1}^\top]_2)\cdot e([\mathbf{k}_{\mathsf{start}}]_1,[\mathbf{c}_{\mathsf{start},2}^\top]_2)^{-1};$$

  2. For all $j\in[\ell_{\mathrm{BP}}]$, compute

$$[\mathbf{b}_j]_T=e([\mathbf{r}_0]_1,[\mathbf{C}_{j,x_{\rho(j)}}]_2)\cdot e([-\mathbf{k}_{\rho(j)}]_1,[\mathbf{C}_j]_2)\quad\text{and}\quad B_j=[\mathbf{b}_j\mathbf{u}_{j-1,x}^\top]_T;$$

  3. Compute

$$[\mathbf{b}_{\mathsf{end}}]_T=e([\mathbf{r}_0]_1,[\mathbf{C}_{\mathsf{end},1}]_2)\cdot e([-\mathbf{k}_{\mathsf{end}}]_1,[\mathbf{C}_{\mathsf{end},2}]_2)\quad\text{and}\quad B_{\mathsf{end}}=[\mathbf{b}_{\mathsf{end}}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top]_T;$$

  4. Compute

$$B_{\mathsf{all}}=B_{\mathsf{start}}\cdot\textstyle\prod_{j=1}^{\ell_{\mathrm{BP}}}B_j\cdot B_{\mathsf{end}}\quad\text{and}\quad B=B_{\mathsf{all}}^{(\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top)^{-1}}$$

  5. Compute

$$D=e([\mathbf{k}_0]_1,[\mathbf{c}^\top]_2)\cdot B^{-1}$$

  and output the message $m'\leftarrow C\cdot D^{-1}$.

Correctness. For $x = (x_1, \ldots, x_\ell)$ and $\Gamma = (Q, \ell_{\mathrm{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$ such that $\Gamma(x) = 1$, we have:

$$\begin{aligned}
B_{\mathrm{start}} &= [\mathbf{r}\mathbf{B}_1\mathbf{D}_0\mathbf{u}^\top]_T = [\mathbf{r}\mathbf{B}_1\mathbf{D}_0\mathbf{u}_{0,x}^\top]_T && (60)\\
\mathbf{b}_j &= \mathbf{r}\mathbf{B}_1\mathbf{D}_j\mathbf{M}_{j,x_{\rho(j)}} - \mathbf{r}\mathbf{B}_1\mathbf{D}_{j-1} && (61)\\
B_j &= [\mathbf{r}\mathbf{B}_1\mathbf{D}_j\mathbf{u}_{j,x}^\top - \mathbf{r}\mathbf{B}_1\mathbf{D}_{j-1}\mathbf{u}_{j-1,x}^\top]_T && (62)\\
\mathbf{b}_{\mathrm{end}} &= \mathbf{r}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f} - \mathbf{r}\mathbf{B}_1\mathbf{D}_{\ell_{\mathrm{BP}}} && (63)\\
B_{\mathrm{end}} &= [\mathbf{r}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top - \mathbf{r}\mathbf{B}_1\mathbf{D}_{\ell_{\mathrm{BP}}}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top]_T && (64)\\
B_{\mathrm{all}} &= [\mathbf{r}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top]_T && (65)\\
B &= [\mathbf{r}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)]_T && (66)\\
D &= [\mathbf{k}\mathbf{A}_1\mathbf{s}^\top]_T. && (67)
\end{aligned}$$

Here (64) is trivial; (62) and (66) follow from facts (38), the remaining equalities follow from:

$$\begin{aligned}
&(60) & \mathbf{r}\mathbf{B}_1\mathbf{D}_0\mathbf{u}^\top &= \mathbf{r}\mathbf{B}_1\cdot(\mathbf{D}_0\mathbf{u}^\top + \mathbf{W}_{\mathrm{start}}\mathbf{A}_1\mathbf{s}_{\mathrm{start}}^\top) - \mathbf{r}\mathbf{B}_1\mathbf{W}_{\mathrm{start}}\cdot\mathbf{A}_1\mathbf{s}_{\mathrm{start}}^\top\\
&(61) & \mathbf{r}\mathbf{B}_1\mathbf{D}_j\mathbf{M}_{j,x_{\rho(j)}} - \mathbf{r}\mathbf{B}_1\mathbf{D}_{j-1} &= \mathbf{r}\mathbf{B}_1\cdot(\mathbf{D}_j\mathbf{M}_{j,x_{\rho(j)}} - \mathbf{D}_{j-1} + \mathbf{W}_{\rho(j),x_{\rho(j)}}\mathbf{A}_1\mathbf{S}_j) - \mathbf{r}\mathbf{B}_1\mathbf{W}_{\rho(j),x_{\rho(j)}}\cdot\mathbf{A}_1\mathbf{S}_j\\
&(63) & \mathbf{r}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f} - \mathbf{r}\mathbf{B}_1\mathbf{D}_{\ell_{\mathrm{BP}}} &= \mathbf{r}\mathbf{B}_1\cdot((\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f} - \mathbf{D}_{\ell_{\mathrm{BP}}} + \mathbf{W}_{\mathrm{end}}\mathbf{A}_1\mathbf{S}_{\mathrm{end}}) - \mathbf{r}\mathbf{B}_1\mathbf{W}_{\mathrm{end}}\cdot\mathbf{A}_1\mathbf{S}_{\mathrm{end}}\\
&(65) & \mathbf{r}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top &= \mathbf{r}\mathbf{B}_1\mathbf{D}_0\mathbf{u}_{0,x}^\top + \textstyle\sum_{j=1}^{\ell_{\mathrm{BP}}}(\mathbf{r}\mathbf{B}_1\mathbf{D}_j\mathbf{u}_{j,x}^\top - \mathbf{r}\mathbf{B}_1\mathbf{D}_{j-1}\mathbf{u}_{j-1,x}^\top) + (\mathbf{r}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top)\mathbf{f}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top - \mathbf{r}\mathbf{B}_1\mathbf{D}_{\ell_{\mathrm{BP}}}\mathbf{u}_{\ell_{\mathrm{BP}},x}^\top).\\
&(67) & \mathbf{k}\mathbf{A}_1\mathbf{s}^\top &= (\mathbf{r}\mathbf{B}_1\mathbf{W}_0 + \mathbf{k})\cdot\mathbf{A}_1\mathbf{s}^\top - \mathbf{r}\mathbf{B}_1(\mathbf{W}_0\mathbf{A}_1\mathbf{s}^\top).
\end{aligned}$$

Correctness follows readily.

J.3 Adaptive Security

We prove the following theorem.

Theorem 7 (Adaptively Secure CP-ABE for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$). *The ABE scheme for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$ in prime-order bilinear groups described in Section J.2 is adaptively secure (cf. Section 2.1) under the k-Lin assumption with security loss $O(q\cdot\ell_{BP}\cdot|\Sigma|^2\cdot Q^2)$. Here ℓ_{BP} are program length in adversary's challenge query and q is the number of key queries.*

The proof employs standard dual system argument where we handle key queries one by one; for each key, we rely on the core lemma, Lemma 30, for our adaptively secure KP-ABE for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$ (in Section 6). We only show the game sequence and sketch the proof.

Auxiliary distributions. We use $\Gamma^* = (Q, \ell_{\mathrm{BP}}, \ell, \Sigma, \{\mathbf{M}_{j,\sigma}\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma}, \rho, \mathbf{u}, \mathbf{f})$ to denote the adaptive challenge NBP and $x = (x_1, \ldots, x_\ell)$ a key query. We describe the auxiliary ciphertext and key distributions that we use in the proof.

Ciphertext distributions. We sample $\hat{\mathbf{S}}_1, \ldots, \hat{\mathbf{S}}_{\ell_{\mathrm{BP}}}, \hat{\mathbf{S}}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{k\times Q}$, $\hat{\mathbf{s}}_{\mathrm{start}}, \hat{\mathbf{s}} \leftarrow \mathbb{Z}_p^{1\times k}$ and define:

- N: the real ciphertext in the scheme;
- SF: identical to an N ciphertext except that we replace $\mathbf{A}_1\mathbf{s}_{\mathrm{start}}^\top, \mathbf{A}_1\mathbf{S}_j, \mathbf{A}_1\mathbf{S}_{\mathrm{end}}, \mathbf{A}_1\mathbf{s}^\top$ with $\mathbf{A}_1\mathbf{s}_{\mathrm{start}}^\top + \mathbf{A}_2\hat{\mathbf{s}}_{\mathrm{start}}^\top, \mathbf{A}_1\mathbf{S}_j + \mathbf{A}_2\hat{\mathbf{S}}_j, \mathbf{A}_1\mathbf{S}_{\mathrm{end}} + \mathbf{A}_2\hat{\mathbf{S}}_{\mathrm{end}}, \mathbf{A}_1\mathbf{s}^\top + \mathbf{A}_2\hat{\mathbf{s}}^\top$, respectively.

That is, we write

$$\mathsf{ct}_\Gamma^{\mathsf{SF}} = \begin{pmatrix} [\mathbf{D}_0\mathbf{u}^\top + \mathbf{W}_{\mathrm{start}}(\mathbf{A}_1\mathbf{s}_{\mathrm{start}}^\top + \boxed{\mathbf{A}_2\hat{\mathbf{s}}_{\mathrm{start}}^\top})]_2, [\mathbf{A}_1\mathbf{s}_{\mathrm{start}}^\top + \boxed{\mathbf{A}_2\hat{\mathbf{s}}_{\mathrm{start}}^\top}]_2 \\ \{[\mathbf{D}_j\mathbf{M}_{j,\sigma} - \mathbf{D}_{j-1} + \mathbf{W}_{\rho(j),\sigma}(\mathbf{A}_1\mathbf{S}_j + \boxed{\mathbf{A}_2\hat{\mathbf{S}}_j})]_2,\ [\mathbf{A}_1\mathbf{S}_j + \boxed{\mathbf{A}_2\hat{\mathbf{S}}_j}]_2\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [(\mathbf{W}_0(\mathbf{A}_1\mathbf{s}^\top + \boxed{\mathbf{A}_2\hat{\mathbf{s}}^\top}))\mathbf{f} - \mathbf{D}_{\ell_{\mathrm{BP}}} + \mathbf{W}_{\mathrm{end}}(\mathbf{A}_1\mathbf{S}_{\mathrm{end}} + \boxed{\mathbf{A}_2\hat{\mathbf{S}}_{\mathrm{end}}})]_2, [\mathbf{A}_1\mathbf{S}_{\mathrm{end}} + \boxed{\mathbf{A}_2\hat{\mathbf{S}}_{\mathrm{end}}}]_2 \\ [\mathbf{A}_1\mathbf{s}^\top + \boxed{\mathbf{A}_2\hat{\mathbf{s}}^\top}]_2,\ [\mathbf{k}(\mathbf{A}_1\mathbf{s}^\top + \boxed{\mathbf{A}_2\hat{\mathbf{s}}^\top})]_T\cdot m_\beta \end{pmatrix}.$$

Secret key distributions. We sample $\mathbf{\Delta} \leftarrow \mathbb{Z}_p^{1\times k}$, $\hat{r} \leftarrow \mathbb{Z}_p$ and define:

- N: the real key in the scheme;
- SF: identical to an N key except that we replace $\mathbf{k}$ with $\mathbf{\Delta}\mathbf{A}_2^{\perp} + \mathbf{k}$;
- P-N: identical to an N key except that we replace $\mathbf{r}\mathbf{B}_1$ with $\mathbf{r}\mathbf{B}_1 + \hat{r}\mathbf{b}_2$;
- P-SF: identical to an SF key except that we replace $\mathbf{r}\mathbf{B}_1$ with $\mathbf{r}\mathbf{B}_1 + \hat{r}\mathbf{b}_2$.

That is, we write

$$\begin{aligned}
\mathsf{sk}_x^{\mathsf{SF}} &= \Big([\mathbf{r}\mathbf{B}_1]_1,\, [\mathbf{r}\mathbf{B}_1\mathbf{W}_0 + \boxed{\mathbf{\Delta}\mathbf{A}_2^{\perp}} + \mathbf{k}]_1,\, [\mathbf{r}\mathbf{B}_1\mathbf{W}_{\mathrm{start}}]_1,\, \big\{[\mathbf{r}\mathbf{B}_1\mathbf{W}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]},\, [\mathbf{r}\mathbf{B}_1\mathbf{W}_{\mathrm{end}}]_1\Big);\\
\mathsf{sk}_x^{\mathsf{P\text{-}N}} &= \Big([\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2}]_1,\, [(\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2})\mathbf{W}_0 + \mathbf{k}]_1,\, [(\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2})\mathbf{W}_{\mathrm{start}}]_1,\, \big\{[(\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2})\mathbf{W}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]},\, [(\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2})\mathbf{W}_{\mathrm{end}}]_1\Big);\\
\mathsf{sk}_x^{\mathsf{P\text{-}SF}} &= \Big([\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2}]_1,\, [(\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2})\mathbf{W}_0 + \mathbf{\Delta}\mathbf{A}_2^{\perp} + \mathbf{k}]_1,\, [(\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2})\mathbf{W}_{\mathrm{start}}]_1,\, \big\{[(\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2})\mathbf{W}_{\eta,x_\eta}]_1\big\}_{\eta\in[\ell]},\, [(\mathbf{r}\mathbf{B}_1 + \boxed{\hat{r}\mathbf{b}_2})\mathbf{W}_{\mathrm{end}}]_1\Big).
\end{aligned}$$

Game sequences. We prove Theorem 7 via a series of games following the standard dual system method [20,22,4]:

- G_0: Identical to the real game where all keys and challenge ciphertext are $\mathsf{sk}_x^{\mathsf{N}}$ and $\mathsf{ct}_{\Gamma^*}^{\mathsf{N}}$, respectively.
- G_1: Identical to G_0 except that the challenge ciphertext is $\mathsf{ct}_{\Gamma^*}^{\mathsf{SF}}$.
- $\mathsf{G}_{2.\kappa.0}$ for $\kappa \in [q]$: Identical to G_1 except that the first $\kappa - 1$ secret keys are $\mathsf{sk}_x^{\mathsf{SF}}$.
- $\mathsf{G}_{2.\kappa.1}$ for $\kappa \in [q]$: Identical to $\mathsf{G}_{2.\kappa.0}$ except that the κ-th secret key is $\mathsf{sk}_x^{\mathsf{P\text{-}N}}$.
- $\mathsf{G}_{2.\kappa.2}$ for $\kappa \in [q]$: Identical to $\mathsf{G}_{2.\kappa.1}$ except that the κ-th secret key is $\mathsf{sk}_x^{\mathsf{P\text{-}SF}}$.
- $\mathsf{G}_{2.\kappa.3}$ for $\kappa \in [q]$: Identical to $\mathsf{G}_{2.\kappa.2}$ except that the κ-th secret key $\mathsf{sk}_x^{\mathsf{SF}}$.
- G_3: Identical to $\mathsf{G}_{2.q.3}$ except that the challenge ciphertext is an encryption of a random message.

Note that we have $\mathsf{G}_{2.1.0} = \mathsf{G}_1$ and $\mathsf{G}_{2.\kappa.0} = \mathsf{G}_{2.\kappa-1.3}$ for $q \in [2, q]$.

Proof sketch. Most proofs are standard: $\mathsf{G}_0 \approx_c \mathsf{G}_1$ follows from $\mathrm{SD}^{G_2}_{\mathbf{A}_1\mapsto\mathbf{A}_1,\mathbf{A}_2}$ assumption; both $\mathsf{G}_{2.\kappa.0} \approx_c \mathsf{G}_{2.\kappa.1}$ and $\mathsf{G}_{2.\kappa.2} \approx_c \mathsf{G}_{2.\kappa.3}$ with $\kappa \in [q]$ follow from $\mathrm{SD}^{G_1}_{\mathbf{B}_1\mapsto\mathbf{B}_1,\mathbf{b}_2}$ assumption and $\mathsf{G}_{2.q.3} \approx_s \mathsf{G}_3$ is straightforward by a standard statistical argument involving $\mathbf{k}$ and $\mathbf{\Delta}$. We focus on $\mathsf{G}_{2.\kappa.1} \approx_c \mathsf{G}_{2.\kappa.2}$ for all $\kappa \in [q]$.

Lemma 63 ($\mathsf{G}_{2.\kappa.1} \approx_c \mathsf{G}_{2.\kappa.2}$)**.** *For all $\kappa \in [q]$ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ and*

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.1}\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.2}\rangle = 1] \le O(\ell_{BP} \cdot |\Sigma|^2 \cdot Q^2) \cdot \mathsf{Adv}_{\mathcal{B}}^{k\text{-LIN}}(\lambda)$$

Proof (sketch). We use the core lemma, Lemma 30, to prove the lemma. By the lemma, it is sufficient to prove that for all κ and all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.1}\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.2}\rangle = 1] \le \mathsf{Adv}_{\mathcal{B}}^{\mathrm{CORE}}(\lambda).$$

For this, we define two auxiliary games $\hat{\mathsf{G}}_{2.\kappa.1}$ and $\hat{\mathsf{G}}_{2.\kappa.2}$ by the following change of variables in both $\mathsf{G}_{2.\kappa,1}$ and $\mathsf{G}_{2.\kappa.2}$:

$$\begin{aligned}
\mathbf{W}_{\mathrm{start}} &\mapsto \mathbf{W}_{\mathrm{start}} + \mathbf{b}_2^{\perp}\mathbf{w}_{\mathrm{start}}\mathbf{A}_2^{\perp},\\
\mathbf{W}_{\eta,\sigma} &\mapsto \mathbf{W}_{\eta,\sigma} + \mathbf{b}_2^{\perp}\mathbf{w}_{\eta,\sigma}\mathbf{A}_2^{\perp}, \quad \forall \eta \in [\ell], \sigma \in \Sigma\\
\mathbf{W}_{\mathrm{end}} &\mapsto \mathbf{W}_{\mathrm{end}} + \mathbf{b}_2^{\perp}\mathbf{w}_{\mathrm{end}}\mathbf{A}_2^{\perp},\\
\mathbf{D}_j &\mapsto \mathbf{D}_j + \mathbf{b}_2^{\perp}\mathbf{d}_j, \quad \forall j \in [\ell_{\mathrm{BP}}]
\end{aligned}$$

and

$$\mathbf{W}_0 \mapsto \mathbf{W}_0 - \mathbf{b}_2^{\perp}(\beta\hat{r}^{-1}\mathbf{\Delta})\mathbf{A}_2^{\perp}, \quad \text{where} \quad \beta = \begin{cases} 0 & \text{in } \mathsf{G}_{2.\kappa.1} \\ 1 & \text{in } \mathsf{G}_{2.\kappa.2} \end{cases}$$

where $\mathbf{w}_{\mathrm{start}}, \mathbf{w}_{\eta,\sigma}, \mathbf{w}_{\mathrm{end}} \leftarrow \mathbb{Z}_p^{1\times k}$ for all $\eta \in [\ell], \sigma \in \Sigma$ and $\mathbf{d}_0, \ldots, \mathbf{d}_{\ell_{\mathrm{BP}}} \leftarrow \mathbb{Z}_p^{1\times Q}$. It is clear that we have

$$\Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.1}\rangle = 1] = \Pr[\langle \mathcal{A}, \hat{\mathsf{G}}_{2.\kappa.1}\rangle = 1] \quad \text{and} \quad \Pr[\langle \mathcal{A}, \mathsf{G}_{2.\kappa.2}\rangle = 1] = \Pr[\langle \mathcal{A}, \hat{\mathsf{G}}_{2.\kappa.2}\rangle = 1]$$

since the change of variables do not change the two games. Now it is sufficient to prove that

$$\Pr[\langle \mathcal{A}, \hat{\mathsf{G}}_{2.\kappa.1}\rangle = 1] - \Pr[\langle \mathcal{A}, \hat{\mathsf{G}}_{2.\kappa.2}\rangle = 1] \le \mathsf{Adv}^{\mathrm{CORE}}_{\mathcal{B}}(\lambda). \tag{68}$$

Observe that, in the new games, we have mpk, $\mathsf{sk}_x^{\mathsf{N}}$ and $\mathsf{sk}_x^{\mathsf{SF}}$ unchanged due to the fact that $\mathbf{A}_2^{\perp}\mathbf{A}_1 = \mathbf{0}$ and $\mathbf{B}_1\mathbf{b}_2^{\perp} = \mathbf{0}$; the challenge ciphertext is in the form of

$$\mathsf{ct}^{\mathsf{SF}}_{\Gamma^*} \cdot \boxed{\begin{pmatrix} [\mathbf{b}_2^{\perp}\mathbf{d}_0\mathbf{u}^{\top} + \mathbf{b}_2^{\perp}\mathbf{w}_{\mathrm{start}}\hat{\mathbf{s}}_{\mathrm{start}}^{\top}]_2,\, [\mathbf{0}]_2 \\ \{\, [\mathbf{b}_2^{\perp}\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{b}_2^{\perp}\mathbf{d}_{j-1} + \mathbf{b}_2^{\perp}\mathbf{w}_{\rho(j),\sigma}\hat{\mathbf{S}}_j]_2,\, [\mathbf{0}]_2 \,\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [-\mathbf{b}_2^{\perp}\cdot\beta\hat{r}^{-1}\boldsymbol{\Delta}\hat{\mathbf{s}}^{\top}\mathbf{f} - \mathbf{b}_2^{\perp}\mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{b}_2^{\perp}\mathbf{w}_{\mathrm{end}}\hat{\mathbf{S}}_{\mathrm{end}}]_2,\, [\mathbf{0}]_2 \\ [\mathbf{0}]_2,\, [\mathbf{0}]_T \end{pmatrix}} \quad \text{where} \quad \beta = \begin{cases} 0 & \text{in } \hat{\mathsf{G}}_{2.\kappa.1} \\ 1 & \text{in } \hat{\mathsf{G}}_{2.\kappa.2} \end{cases}$$

while the κ-th key in the two games are in the form of

$$\mathsf{sk}_x^{\mathsf{P\text{-}N}} \cdot \boxed{\left([\mathbf{0}]_1,\, [\mathbf{0}]_1,\, [\hat{r}\mathbf{w}_{\mathrm{start}}\mathbf{A}_2^{\perp}]_1,\, \left\{[\hat{r}\mathbf{w}_{\eta,x_\eta}\mathbf{A}_2^{\perp}]_1\right\}_{\eta\in[\ell]},\, [\hat{r}\mathbf{w}_{\mathrm{end}}\mathbf{A}_2^{\perp}]_1\right)}.$$

It is clear that the two games are identical except that boxed part, so it is sufficient to prove the indistinguishability between the boxed parts in games. Formally, we capture this by the following claim. Note that we neglect $\mathbf{b}_2^{\perp}$ and $\mathbf{A}_2^{\perp}$ which are unrelated to the argument and give out $\hat{\mathbf{s}}_{\mathrm{start}}, \hat{\mathbf{S}}_j, \hat{\mathbf{S}}_{\mathrm{end}}$ for the simulation of $\mathsf{sk}^{\mathsf{SF}}_{\Gamma^*}$-part of the challenge ciphertext.

Claim. For all $\mathcal{A}$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ and

$$\Pr[\langle \mathcal{A}, \mathsf{H}_0\rangle = 1] - \Pr[\langle \mathcal{A}, \mathsf{H}_1\rangle = 1] \le \mathsf{Adv}^{\mathrm{CORE}}_{\mathcal{B}}(\lambda)$$

where we define:

$$\langle \mathcal{A}, \mathsf{H}_\beta\rangle := \{\beta' \leftarrow \mathcal{A}^{\mathsf{OEnc}(\cdot),\mathsf{OKey}(\cdot)}\}$$

and the two oracles work as follows:

- $\mathsf{OEnc}(\Gamma)$: output

$$\begin{pmatrix} [\mathbf{d}_0\mathbf{u}^{\top} + \mathbf{w}_{\mathrm{start}}\hat{\mathbf{s}}_{\mathrm{start}}^{\top}]_2, [\hat{\mathbf{s}}_{\mathrm{start}}^{\top}]_2 \\ \{\, [\mathbf{d}_j\mathbf{M}_{j,\sigma} - \mathbf{d}_{j-1} + \mathbf{w}_{\rho(j),\sigma}\hat{\mathbf{S}}_j]_2,\, [\hat{\mathbf{S}}_j]_2 \,\}_{j\in[\ell_{\mathrm{BP}}],\sigma\in\Sigma} \\ [-\beta\hat{r}^{-1}\boldsymbol{\Delta}\hat{\mathbf{s}}^{\top}\mathbf{f} - \mathbf{d}_{\ell_{\mathrm{BP}}} + \mathbf{w}_{\mathrm{end}}\hat{\mathbf{S}}_{\mathrm{end}}]_2, [\hat{\mathbf{S}}_{\mathrm{end}}]_2 \end{pmatrix}$$

- $\mathsf{OKey}(x)$: output

$$\left(\mathbf{w}_{\mathrm{start}},\, \left\{\mathbf{w}_{\eta,x_\eta}\right\}_{\eta\in[\ell]},\, \mathbf{w}_{\mathrm{end}}\right).$$

with the restrictions that (1) $\mathcal{A}$ makes only one query to each oracle; (2) queries Γ and x satisfy $\Gamma(x) = 0$.

It is direct to verify that the terms given out in the claim are sufficient to simulate both games and readily implies (68). Furthermore, the claim itself is straightforward by the core lemma, Lemma 30, for adaptively secure KP-ABE for $\mathcal{E}_Q$-restricted NBP$^{\oplus p}$ in Section 6. This proves the lemma. □