Improved (Almost) Tightly-Secure Simulation-Sound QA-NIZK with Applications

Masayuki Abe[1], Charanjit S. Jutla[2], Miyako Ohkubo[3], and Arnab Roy[4]

[1] NTT Corporation, Japan. `abe.masayuki.cp@hst.ntt.co.jp`
[2] IBM T. J. Watson Research Center, USA. `csjutla@us.ibm.com`
[3] Security Fundamentals Laboratories, CSR, NICT, Japan. `m.ohkubo@nict.go.jp`
[4] Fujitsu Laboratories of America, USA. `aroy@us.fujitsu.com`

Abstract. We construct the first (almost) tightly-secure unbounded-simulation-sound quasi-adaptive non-interactive zero- knowledge arguments (USS-QA-NIZK) for linear-subspace languages with compact (number of group elements independent of the security parameter) common reference string (CRS) and compact proofs under standard assumptions in bilinear-pairings groups. Specifically, our construction has $O(\log Q)$ reduction to the SXDH, DLIN and matrix-DDH assumptions, where Q is the number of simulated proofs given out. The USS-QA-NIZK primitive has many applications, including structure-preserving signatures (SPS), CCA2-secure publicly-verifiable public-key encryption (PKE), which in turn have applications to CCA-anonymous group signatures, blind signatures and unbounded simulation-sound Groth-Sahai NIZK proofs. We show that the almost tight security of our USS-QA-NIZK translates into constructions of all of the above applications with (almost) tight-security to standard assumptions such as SXDH and, more generally, $\mathcal{D}_k$-MDDH. Thus, we get the first publicly-verifiable (almost) tightly-secure multi-user/multi-challenge CCA2-secure PKE with practical efficiency under standard bilinear assumptions. Our (almost) tight SPS construction is also improved in the signature size over previously known constructions.

Keywords: QA-NIZK, simulation-soundness, tight security, public-key encryption, CCA, Structure-preserving signatures.

1 Introduction

Over the last decade, pairing-based cryptography has facilitated many new cryptographic protocols and applications that are provably-secure under static assumptions. Some of these static assumptions (SXDH, DLIN, MDDH) are now considered standard, as they generalize decisional-Diffie-Hellman (DDH) assumption to pairings-based groups. Some of the ground-breaking ideas include the Groth-Sahai (GS) non-interactive zero-knowledge (NIZK) proofs [GS12], fully-secure identity-based-encryption (IBE) [Wat09], structure-preserving signatures (SPS) [AFG$^+$10], quasi-adaptive NIZK arguments (QA-NIZK) [JR13], and tightly-secure IBE [CW13]. In particular, structure-preserving signatures use Groth-Sahai NIZK proof structure to enable a wide-range of privacy-preserving applications, such as, group signatures [AHO10], blind signatures [AO09a,AFG$^+$10], group encryption [CLY09], among others. Recent works [JR17,JOR18] have employed QA-NIZK to get more efficient SPS, and tightly-secure unbounded-simulation-sound QA-NIZK (USS-QA-NIZK [LPJY14,KW15]) to get tightly-secure CCA2-secure public-key encryption (PKE) in the multi-user and multi-challenge setting [LPJY15].

In this work we focus on the basic primitive of USS-QA-NIZK for linear-subspaces of vector spaces of bilinear groups, which has important implications as a structure-preserving version of it directly implies structure-preserving signatures. Further, it is already known to imply CCA2-secure PKE [LPJY15], which in turn leads to several new applications such as CCA-anonymous group signatures [AHO10], and UC-commitments [FLM11]. Further, an (almost) tightly-secure USS-QA-NIZK implies (almost) tightly-secure version of all the above applications. While an (almost) tightly-secure USS-QA-NIZK was given in [LPJY15] it required a large common reference string (CRS), which was of the order of the security parameter λ. In this work, we give the first (almost) tightly-secure USS-QA-NIZK for linear-subspaces with compact (number of group elements independent of λ) CRS and compact proofs. Moreover, the earlier construction only worked under the DLIN assumption in symmetric groups, and required non-standard assumptions in the asymmetric pairing-group setting, whereas we give a construction which is tightly-secure under the SXDH assumption in asymmetric groups. Asymmetric groups usually allow leaner constructions, which we validate below. At the same time, we make the CRS compact.

Related Techniques. In [KW15], Kiltz and Wee observed that QA-NIZK can be seen as a generalization of hash proof systems [CS98] to public-verifiability by publishing a "partial commitment" to the secret hash-key $\mathbf{k}$ in the second group $\mathbb{G}_2$ of a pairings-based groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. Simulation of proofs of statements then just requires hash computation using the secret hash-key $\mathbf{k}$. Computational-soundness is slightly more tricky to prove than in the hash-proof setting, but essentially an adversary cannot generate hash proofs of false statements given only the "partial commitment" to $\mathbf{k}$ and the projection-key (of the hash-proof system). In the simulation-soundness setting, the simulation of fake proofs would give additional information to the adversary about secret-hash key $\mathbf{k}$, and hence to obtain a USS-QA-NIZK, [KW15] encrypt the hash-proofs and employ a dual-system [Wat09] technique to achieve soundness. This methodology should be contrasted with the "OR" proof methodology of [LPJY15] (for USS-QA-NIZK) and [CCS09] (for unbounded simulation-sound GS-NIZK).

While the USS-QA-NIZK of [KW15] leads to compact proofs (of size only $(2k + 2)$ under the k-linear assumption), the security reduction to the underlying hardness assumption is not tight. The reason behind this being that the dual-system approach is itself not tight as at its heart it employs one-time simulation-soundness along with two-universal hash-proof systems [JR15], similar to Cramer-Shoup CCA2-encryption [CS98]. A nested-version of dual-system approach does lead to (almost) tight IBE [CW13], but then requires non-compact (master) public keys.

However, the concept of identity-space partitioning introduced in [CW13] is also applicable to signature schemes, and this technique repeatedly splits the message space into two based on the message or a tag. This idea was further enhanced in [Hof17] to adaptive partitioning in which the partitioning is decided dynamically based on an encrypted partitioning-bit. [AHN$^+$17] refined this technique by introducing new ideas using "OR" GS-NIZK systems and made the scheme structure-preserving. Since signature schemes, especially the ones considered in the above works, usually encrypt a secret and prove in zero-knowledge that such a secret is encrypted in the signature, the question arises if this refined adaptive-partitioning methodology can be employed to the USS-QA-NIZK of [KW15] discussed above that encrypted the hash-proofs. One main difference between NIZK proofs embedded in signature schemes is that they need only be "designated-prover" NIZK proofs. In other words, such NIZK proofs while still providing public verifiability, need only give the proving capability to a designated party, namely the CRS (or public-key) generator itself. Hence, such designated-prover NIZK proofs are much easier to devise and it is not immediately clear if such restricted NIZK proofs can be extended to usual NIZK proofs (especially in the tight USS-NIZK setting).

Finally, we argue that the recent constructions of tight CCA2-secure PKE [GHK17,Hof17] (along with [CCS09]) also do not easily imply tight USS-NIZK. [CCS09] requires proving an OR-statement where one of the disjuncts is that a CCA2-PKE ciphertext is well-formed. For [GHK17], this statement is not Groth-Sahai friendly as its own "qualified"-OR proof in the ciphertexts employs a mapping that maps group elements to $\mathbb{Z}_q$ elements. This should be contrasted with Cramer-Shoup CCA2-PKE, which also has such a tag, but that is publicly computable from other elements in the ciphertext. This is not the case for [GHK17] as the mapping is from private elements. As for [Hof17], it uses disjunctive hash-proofs from [ABP15] which require the hash proof to be in the target group; GS-proofs of such statements are only possible in the Witness-Indistinguishable setting.

Our Contributions. We show that a different "OR" system than considered in [AHN$^+$17] (or later works such as [JOR18]) does allow one to give (almost) tight (structure-preserving) USS-QA-NIZK for linear-subspaces with compact proof sizes and compact CRS-es. This "OR" system can be proved in the generic framework of [Ràf15], allowing us to obtain USS-QA-NIZKs under the SXDH assumption in asymmetric pairings groups, which was not previously known even for non-compact CRS. Our USS-QA-NIZK construction loses a factor of $O(\log Q)$ in the security reduction, where Q is the number of adversarial requests for simulated proofs. We also develop optimized "designated prover" and "designated verifier" versions with a tighter reduction as well, i.e., with only a $O(\log Q)$ factor loss.

As a first application, we show that the labeled version of our tight USS-QA-NIZK construction gives us a tight CCA2-secure *publicly-verifiable* labeled

PKE in the multi-user multi-challenge setting[5]. In Table 1, we compare our scheme with the state of the art schemes in [GHKW16,Hof17,GHK17] with the smallest possible assumption for each. While being practical by itself, our scheme is not the best one in terms of efficiency. What separates our scheme from other tightly secure schemes is the public verifiability, which allows anyone, without knowing the secret key, to check if a ciphertext decrypts to some plaintext. Feasibility results for publicly-verifiable tight CCA-PKE can be found in [HJ16] and [ADKNO13], but their ciphertext overhead is hundreds or even more than a thousand of group elements. Ours is the first practical publicly-verifiable scheme having only 19 elements of ciphertext overhead. Our scheme is also secure under the SXDH assumption with only a $O(\log Q)$ loss in security reduction, where Q is the total number of (multi-challenge, multi-user) encryption-oracle requests by the adversary. CCA2-secure PKE and its variants that encrypt long messages have further applications, such as UC commitments, and we refer the reader to [LPJY15] for a good introduction.

Table 1. Comparison of tightly-secure public-key encryption schemes when the underlying assumptions are set to minimum ones, SXDH or DDH. Sizes count the number of group elements and (n_1, n_2) denotes n_1 and n_2 elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Column 'Pairings?' shows necessity of pairing groups. SAE stands for symmetric authenticated encryption.

	$\lvert pk\rvert$	$\lvert ct\rvert - \lvert m\rvert$	Verifiabilty	Pairings?	Sec. Loss	Assumption
[GHKW16]	$O(\lambda)$	3	private	no	$O(\lambda)$	DDH
[Hof17]	28	6	private	yes	$O(\lambda)$	DLIN
[GHK17]	6	3	private	no	$O(\lambda)$	DDH+SAE
Ours §5.1	$(19, 4)$	$(16, 6)$	public	yes	$O(\log Q)$	SXDH

As a second application, we show that our designated-prover variant of structure-preserving USS-QA-NIZK from Section 5.2 yields an SPS scheme with the shortest signature size in the literature. Recall that unbounded simulation-soundness guarantees that it is hard to create a valid proof for any no-instances taken out of the legitimate subspace even after seeing simulated proofs for (also no-) instances of one's choice. If we look at the simulation trapdoor as a secret-key and the simulated proofs as signatures, the USS-QA-NIZK can be considered as a signature scheme for message space consisting of no-instances, and the notion of unbounded simulation-soundness is exactly the same as existential unforgeability against adaptive chosen-message attacks. As formally proven in [AAO18], for bringing this idea to reality, we need an efficient mapping from desired message space to these no-instances. Since our USS-QA-NIZK allows simulation of fake proofs and we present a simple and efficient construction of injective mapping from a sequence of group elements to no-instances, this construction suffers no overhead for unilateral messages. This, along with the more efficient

[5] This requires adapting our USS-QA-NIZK to the multi-language USS-QA-NIZK described in [LPJY15], but our scheme readily adapts to that.

(designated-prover) USS-QA-NIZK gives us the shortest SPS known under the SXDH assumption, and with only a $O(\log Q)$ factor loss in security-reduction (see Table 2).

Table 2. Comparison with existing SPS schemes for unilateral messages when assumptions are set to minimal ones. Columns labeled as $|M|$, $|\sigma|$, and $|pk|$ show number of group elements in a message, a signature and a public key. For [HJ12], the parameter d limits number of signing queries to 2^d.

	$\lvert M\rvert$	$\lvert\sigma\rvert$	$\lvert pk\rvert$	Sec. Loss	Assumption
[HJ12]	1	$10d+6$	13	8	DLIN
[ACD+12]	$(n_1, 0)$	$(7, 4)$	$(5, n_1+12)$	$O(Q)$	SXDH, XDLIN
[LPY15]	$(n_1, 0)$	$(10, 1)$	$(16, 2n_1+5)$	$O(Q)$	SXDH, XDLIN
[KPW15]	$(n_1, 0)$	$(6, 1)$	$(0, n_1+6)$	$O(Q^2)$	SXDH
[JR17]	$(n_1, 0)$	$(5, 1)$	$(0, n_1+6)$	$O(Q\log Q)$	SXDH
[AHN+17]	$(n_1, 0)$	$(13, 12)$	$(18, n_1+11)$	$O(\lambda)$	SXDH
[JOR18]	$(n_1, 0)$	$(11, 6)$	$(7, n_1+16)$	$O(\lambda)$	SXDH
[GHKP18]	$(n_1, 0)$	$(8, 6)$	$(2, n_1+9)$	$O(\log Q)$	SXDH
Ours (§5.2)	$(n_1, 0)$	$(6, 6)$	$(10, n_1+10)$	$O(\log Q)$	SXDH

Next, combining the above two applications, we give the first (almost) tightly-secure CCA-anonymous dynamic group signature scheme with compact signature sizes and compact public keys under standard assumptions. Our schemes can be given in both asymmetric pairings groups and symmetric pairing groups under the $\mathcal{D}_k$-MDDH assumption. We also instantiate a generic structure-preserving blind signature scheme of [Fis06] using our SPS to get an (almost) tight round-optimal scheme under $\mathcal{D}_k$-MDDH with compact signature size, whereas previous schemes in standard model were based on non-static assumptions [Fuc09,AO09b]. Finally, our (almost) tight CCA2-secure PKE scheme along with the generic construction of [CCS09], leads to a first (almost) tightly-secure unbounded simulation-sound Groth-Sahai NIZK proof system with compact CRS and proofs.

Acknowledgments and updates. We are indebted to Jiaxin Pan, who discovered an attack on an earlier version of this paper which appears in the proceedings of Asiacrypt 2018 [AJOR18]. This version fixes the protocol and the proof.

We thank the anonymous reviewers for detailed and insightful feedback on the paper. We especially thank Carla Ràfols for her significant effort in helping us revise the paper.

2 Preliminaries

We will consider cyclic groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ of prime order q, with an efficient bilinear map $\mathsf{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Group elements $\mathbf{g}_1$ and $\mathbf{g}_2$ will typically denote generators of the group $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. Following [EHK+13], we will use the notations $[a]_1, [a]_2$ and $[a]_T$ to denote $a\mathbf{g}_1, a\mathbf{g}_2$, and $a \cdot \mathsf{e}(\mathbf{g}_1, \mathbf{g}_2)$ respectively and use additive notations for group operations. When talking about a general group $\mathbb{G}$ with generator $\mathbf{g}$, we will just use the notation $[a]$ to denote $a\mathbf{g}$. The notation generalizes to vectors and matrices in a natural component-wise way.

For two vector or matrices A and B, we will denote the product $A^\top B$ as $A \cdot B$. The pairing product $\mathsf{e}([A]_1, [B]_2)$ evaluates to the matrix product $[AB]_T$ in the target group with pairing as multiplication and target group operation as addition.

2.1 Matrix-DDH Assumptions and Boosting

We recall the *Matrix Decisional Diffie-Hellman* or MDDH assumptions from [EHK+13]. A matrix distribution $\mathcal{D}_{l,k}$, where $l > k$, is defined to be an efficiently samplable distribution on $\mathbb{Z}_q^{l \times k}$ which is full-ranked with overwhelming probability. The *$\mathcal{D}_{l,k}$-MDDH assumption* in group $\mathbb{G}$ states that with samples $\mathbf{A} \leftarrow \mathcal{D}_{l,k}, \mathbf{s} \leftarrow \mathbb{Z}_q^k$ and $\mathbf{s}' \leftarrow \mathbb{Z}_q^l$, the tuple $([\mathbf{A}], [\mathbf{A}\mathbf{s}])$ is computationally indistinguishable from $([\mathbf{A}], [\mathbf{s}'])$. A matrix distribution $\mathcal{D}_{k+1,k}$ is simply denoted by $\mathcal{D}_k$.

It was shown in [JR16] that a $\mathcal{D}_k$-MDDH assumption can be *boosted* to generate additional (computationally) independently random elements.

For an $l \times k$ matrix $\mathbf{A}$, we denote $\bar{\mathbf{A}}$ to be the top $k \times k$ square sub-matrix of $\mathbf{A}$ and $\underline{\mathbf{A}}$ to be the bottom $(l-k) \times k$ sub-matrix of $\mathbf{A}$.

Theorem 1 (Boosting [JR16]). *Let $\mathcal{D}_k$ be a matrix distribution on $\mathbb{Z}_q^{(k+1)\times k}$. Define another matrix distribution $\mathcal{D}_{l,k}$ on $\mathbb{Z}_q^{l \times k}$ as follows: First sample matrices $\mathbf{A} \leftarrow \mathcal{D}_k$ and $\mathbf{R} \leftarrow \mathbb{Z}_q^{(l-k)\times k}$ and then output $\begin{pmatrix} \bar{\mathbf{A}} \\ \mathbf{R} \end{pmatrix}$. Then the $\mathcal{D}_k$-MDDH assumption implies the $\mathcal{D}_{l,k}$-MDDH assumption with an $(l-k)$ security reduction.*

They called *boosting* to be the process of stretching $\mathcal{D}_k$ to $\mathcal{D}_{l,k}$ as above. In our construction we will need to boost $\mathcal{D}_k$ to $\mathcal{D}_{2k,k}$.

2.2 Quasi-Adaptive NIZK Proofs

A witness relation is a binary relation on pairs of inputs, the first called a word and the second called a witness. Each witness relation R defines a corresponding language L which is the set of all words x for which there exists a witness w, such that $R(x, w)$ holds.

We will consider Quasi-Adaptive NIZK proofs [JR13] for a probability distribution $\mathcal{D}$ on a collection of (witness-) relations $\mathcal{R} = \{R_\rho\}$ (with corresponding languages L_ρ). Recall that in a quasi-adaptive NIZK, the CRS can be set after the language parameter has been chosen according to $\mathcal{D}$. Please refer to [JR13] for detailed definitions.

For our USS-QA-NIZK construction we will also need a property called true-simulation-soundness. We recall the definitions of these concepts below.

Definition 1 (QA-NIZK [JR13]). *We call a tuple of efficient algorithms* $(\mathsf{pargen}, \mathsf{crsgen}, \mathsf{prover}, \mathsf{ver})$ *a* quasi-adaptive non-interactive zero- knowledge *(QA-NIZK) proof system for witness-relations* $\mathcal{R}_\eta = \{R_\rho\}$ *with parameters sampled from a distribution* $\mathcal{D}$ *over associated parameter language* Lpar*, if there exist simulators* crssim *and* sim *such that for all non-uniform PPT adversaries* $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$*, we have (in all of the following probabilistic experiments, the experiment starts by setting* η *as* $\eta \leftarrow \mathsf{pargen}(1^\lambda)$*, and choosing* ρ *as* $\rho \leftarrow \mathcal{D}_\eta$*):*

Quasi-Adaptive Completeness:

$$\Pr\left[\begin{array}{l} \textsc{crs} \leftarrow \mathsf{crsgen}(\eta, \rho) \\ (x, w) \leftarrow \mathcal{A}_1(\textsc{crs}, \rho) \\ \pi \leftarrow \mathsf{prover}(\textsc{crs}, x, w) \end{array} : \begin{array}{c} \mathsf{ver}(\textsc{crs}, x, \pi) = 1 \textbf{ if} \\ R_\rho(x, w) \end{array}\right] = 1$$

Quasi-Adaptive Soundness:

$$\Pr\left[\begin{array}{l} \textsc{crs} \leftarrow \mathsf{crsgen}(\eta, \rho) \\ (x, \pi) \leftarrow \mathcal{A}_2(\textsc{crs}, \rho) \end{array} : \begin{array}{c} x \notin L_\rho \textbf{ and} \\ \mathsf{ver}(\textsc{crs}, x, \pi) = 1] \end{array}\right] \approx 0$$

Quasi-Adaptive Zero-Knowledge:

$$\Pr\left[\textsc{crs} \leftarrow \mathsf{crsgen}(\eta, \rho) \;:\; \mathcal{A}_3^{\mathsf{prover}(\textsc{crs}, \cdot, \cdot)}(\textsc{crs}, \rho) = 1\right]$$

$$\approx$$

$$\Pr\left[(\textsc{crs}, \mathsf{trap}) \leftarrow \mathsf{crssim}(\eta, \rho) \;:\; \mathcal{A}_3^{\mathsf{sim}^*(\textsc{crs}, \mathsf{trap}, \cdot, \cdot)}(\textsc{crs}, \rho) = 1\right],$$

where $\mathsf{sim}^*(\textsc{crs}, \mathsf{trap}, x, w) = \mathsf{sim}(\textsc{crs}, \mathsf{trap}, x)$ *for* $(x, w) \in R_\rho$ *and both oracles (i.e.* prover *and* sim^**) output failure if* $(x, w) \notin R_\rho$*.*

Definition 2 (True-Simulation-Sound [Har11]). *A QA-NIZK is called* **true -simulation-sound** *if soundness holds even when an adaptive adversary has access to simulated proofs on language members. More precisely, for all PPT* $\mathcal{A}$*,*

$$\Pr\left[\begin{array}{l} (\textsc{crs}, \mathsf{trap}) \leftarrow \mathsf{crssim}(\eta, \rho) \\ (x, \pi) \leftarrow \mathcal{A}^{\mathsf{sim}(\textsc{crs}, \mathsf{trap}, \cdot, \cdot)}(\textsc{crs}, \rho) \end{array} : \begin{array}{c} x \notin L_\rho \textbf{ and} \\ \mathsf{ver}(\textsc{crs}, x, \pi) = 1 \end{array}\right] \approx 0,$$

where the experiment aborts if the oracle is called with some $x \notin L_\rho$*.*

The construction of [JR14] yielded k element proofs of any linear subspace language membership and [KW15] generalized it to any $\mathcal{D}_k$-MDDH assumption. Both constructions are true-simulation-sound.

We now define the unbounded simulation-soundness (USS) property, which we seek to achieve in this paper. The prover and verifier can additionally accept a label which is bound to the proof.

Definition 3 (Unbounded Simulation-Soundness). *A QA-NIZK is called (labeled)* **unbounded simulation sound** *if soundness holds even when an adaptive adversary has access to simulated proofs on arbitrary words of its choice. More precisely, for all PPT* $\mathcal{A}$*,*

$$\Pr\left[\begin{array}{l} (\textsc{crs}, \mathsf{trap}) \leftarrow \mathsf{crssim}(\eta, \rho) \\ (x, \mathtt{lbl}, \pi) \leftarrow \mathcal{A}^{\mathsf{sim}(\textsc{crs}, \mathsf{trap}, \cdot, \cdot)}(\textsc{crs}, \rho) \end{array} : \begin{array}{c} x \notin L_\rho \;\wedge (x, \mathtt{lbl}) \notin \mathcal{Q} \\ \mathsf{ver}(\textsc{crs}, x, \pi, \mathtt{lbl}) = 1 \end{array}\right] \approx 0,$$

where the set $\mathcal{Q}$ records (word, label) tuples queried to the simulator.

A stronger notion called *Enhanced Unbounded Simulation-Soundness in the multi-CRS setting* was formalized by [LPJY15], where soundness holds even if the discrete logs of the language are given to the adversary and the adversary has access to multiple CRS-es and corresponding oracles. We note that our construction satisfies this property as well.

Our main construction is also *Structure-Preserving* as the CRS and proof elements are all in the base groups of the bilinear map and verification consists only of pairing product equations.

2.3 Public-Key Encryption Schemes

Let GEN be an algortihm that, on input security parameter λ, outputs par that includes parameters of pairing groups.

Definition 4 (Public-key encryption). *A Public-Key Encryption (PKE) scheme consists of probabilistic polynomial-time algorithms* $\mathsf{PKE} := (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$*:*

- *Key generation algorithm* $\mathsf{KeyGen}(\mathsf{par})$ *takes* $\mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda)$ *as input and generates a pair of public and secret keys* $(\mathsf{pk}, \mathsf{sk})$*. Message space* $\mathcal{M}$ *is determined by* pk*.*
- *Encryption algorithm* $\mathsf{Enc}(\mathsf{pk}, \mathsf{M})$ *returns a ciphertext* ct*.*
- *Decryption algorithm* $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$ *is deterministic and returns a message* M*.*

For correctness, it must hold that, for all $\mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda)$*,* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{par})$*, messages* $\mathsf{M} \in \mathcal{M}$*, and* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{M})$*,* $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \mathsf{M}$*.*

Definition 5 ($\mathsf{IND\text{-}mCPA}$ Security [BBM00]). *A PKE scheme* PKE *is* indistinguishable against multi-instance chosen-plaintext attack ($\mathsf{IND\text{-}mCPA\text{-}secure}$) *if for any $q_e \geq 0$ and for all* PPT *adversaries $\mathcal{A}$ with access to oracle $\mathcal{O}_e$ at most q_e times the following advantage function* $\mathsf{Adv}^{\mathsf{mcpa}}_{\mathsf{PKE}}(\mathcal{A})$ *is negligible,*

$$\mathsf{Adv}^{\mathsf{mcpa}}_{\mathsf{PKE}}(\mathcal{A}) := \left| \Pr\left[b' = b \,\middle|\, \begin{array}{l} \mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda); (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{par}); \\ b \leftarrow \{0,1\}; b' \leftarrow \mathcal{A}^{\mathcal{O}_e(\cdot,\cdot)}(\mathsf{pk}) \end{array} \right] - \frac{1}{2} \right|,$$

where $\mathcal{O}_e(\mathsf{M}_0, \mathsf{M}_1)$ *runs* $\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{M}_b)$*, and returns* ct^* *to* $\mathcal{A}$*.*

There exist public-key encryption schemes that are structure-preserving, $\mathsf{IND\text{-}mCPA}$ secure, and have tight reductions based on compact assumptions. Examples are ElGamal encryption [ElG84] and Linear encryption [BBS04] based on the DDH assumption and the Decision Linear assumption, respectively. In particular, we will use the scheme of [EHK$^+$13], which is based on the $\mathcal{D}_k$-MDDH assumption. We will use the linear homomorphic property of this PKE in the construction - adding the ciphertexts implicitly adds the underlying plaintexts.

We now recall the definition of IND-CCA2 secure public key encryption scheme in the multi-challenge multi-user setting [BBM00], where the par are shared by multiple users while generating their own keys using KeyGen.

Definition 6 (Multi-CCA [BBM00] (or see [LPJY15])).

A public-key encryption scheme is (μ, q_e)-IND-CCA secure, for integers $\mu, q_e \in$ poly(λ), if no PPT adversary has non-negligible adavantage in the following game:

1. *The challenger first generates* $\mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda)$ *and runs* $(\mathsf{sk}^{(i)}, \mathsf{pk}^{(i)}) \leftarrow \mathsf{KeyGen}(\mathsf{par})$ *for $i = 1$ to μ. It gives $\{\mathsf{pk}^{(i)}\}_{i=1}^{\mu}$ to the adversary $\mathcal{A}$ and retains $\{\mathsf{sk}^{(i)}\}_{i=1}^{\mu}$. In addition, the challenger initializes a set $\mathcal{D} \leftarrow \phi$ and a counter $j_q \leftarrow 0$. Finally, it chooses a random bit $d \leftarrow \{0, 1\}$.*
2. *The adversary $\mathcal{A}$ adaptively makes queries to the following oracles on multiple occasions:*
   - *Encryption query: A chooses an index $i \in [1..\mu]$ and a pair (M_0, M_1) of equal length messages. If $j_q = q_e$, the oracle returns $\perp$. Otherwise, it computes $C \leftarrow \mathsf{Enc}(\mathsf{pk}^{(i)}, M_d)$ and returns C. In addition, it sets $\mathcal{D} := \mathcal{D} \cup \{(i, C)\}$ and $j_q := j_q + 1$.*
   - *Decryption query: A can also invoke the decryption oracle on arbitrary chiphertexts C and indices $i \in [1..\mu]$. If $(i, C) \in \mathcal{D}$, the oracle returns $\perp$. Otherwise, the oracle returns $M \leftarrow \mathsf{Dec}(\mathsf{sk}^{(i)}, C)$, which may be $\perp$ if C is an invalid ciphertext.*
3. *The adversary A outputs a bit d' and is deemed successful if $d' = d$. As usual, $\mathcal{A}$'s advantage is measured as the distance* $\mathsf{Adv}^{\mathsf{mcca}}(\mathcal{A}) = |2 \Pr[d' = d] - 1|$.

2.4 Structure-Preserving Signatures

Let GEN be a common parameter generation algorithm that outputs par for given security parameter λ.

Definition 7 (Structure-Preserving Signature). *A structure-preserving signature scheme SPS is a triple of probabilistic polynomial time (PPT) algorithms* $\mathsf{SPS} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$*:*

- *Key generation algorithm* $\mathsf{KeyGen}(\mathsf{par})$ *takes common parameter* par *and returns a public/secret key, (pk, sk), where $pk \in \mathbb{G}^{n_{pk}}$ for some $n_{pk} \in poly(\lambda)$. It is assumed that pk implicitly defines a message space $\mathcal{M} := \mathbb{G}^n$ for some $n \in poly(\lambda)$.*
- *Signing algorithm* $\mathsf{Sign}(sk, M)$ *takes secret key sk and a message $M \in \mathcal{M}$ as input and returns a signature $\sigma \in \mathbb{G}^{n_\sigma}$ for $n_\sigma \in poly(\lambda)$.*
- *Verification algorithm* $\mathsf{Verify}(pk, M, \sigma)$ *takes public key pk, message $M \in \mathcal{M}$, and signature σ and outputs 1 or 0. It only evaluates group membership operations and pairing product equations.*

Perfect correctness holds if for all $(pk, sk) \leftarrow$ $\mathsf{KeyGen}(\mathsf{par})$ *and all messages $M \in \mathcal{M}$ and all $\sigma \leftarrow$* $\mathsf{Sign}(sk, M)$ *we have* $\mathsf{Verify}(pk, M, \sigma) = 1$.

Definition 8 (Existential Unforgeability against Chosen Message Attack). *To an adversary A and scheme SPS we associate the advantage function:*

$$\mathsf{Adv}^{\mathsf{cma}}_{\mathsf{SPS}}(A) := \Pr\begin{bmatrix} \mathsf{par} \leftarrow \mathsf{GEN}(1^\lambda) & & \\ (pk, sk) \leftarrow \mathsf{KeyGen}(\mathsf{par}) & : & M^* \notin Q_{msg} \textbf{ and} \\ (M^*, \sigma^*) \leftarrow A^{SignO(\cdot)}(pk) & & \mathsf{Verify}(pk, M^*, \sigma^*) = 1 \end{bmatrix}$$

where SignO(M) runs $\sigma \leftarrow \mathsf{Sign}(sk, M)$, adds M to Q_{msg} (initialized with $\emptyset$) and returns σ to A. An SPS is said to be (unbounded) EUF-CMA-secure if for all PPT adversaries A, $\mathsf{Adv}^{\mathsf{cma}}_{\mathsf{SPS}}(A)$ is negligible.

3 The New (Almost) Tightly-Secure USS-QA-NIZK

The new USS-QA-NIZK scheme is formally described in Figure 1, with the CRS and proof simulators described in Figure 2. While a brief overview of the new scheme was given in the introduction, we now describe it in more detail.

We essentially combine techniques from the USS-QA-NIZK scheme of Kiltz and Wee [KW15] and the tightly secure SPS scheme of Jutla, Ohkubo and Roy [JOR18]. Following [KW15], we encrypt a basic QA-NIZK proof of the given word $\mathbf{y} = [\mathbf{M}\mathbf{x}]_1$ using an augmented ElGamal encryption scheme:

$$\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top,\ \gamma := \mathbf{x}^\top[\mathbf{p}_1]_1 + \mathbf{r}^\top[\mathbf{p}_2]_1$$

Notice that unlike [KW15], we did not use an integer tag in the encryption. This helps us keep the construction structure preserving. Now we extend this tuple with elements which enable adaptive partitioning as in [JOR18]. This includes a double ElGamal encryption of a bit z, along with a QA-NIZK proof of equality of plaintexts. In addition, there is an OR-NIZK proof Π_0 that proves either $(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}})$ is consistent, or that z is same as a bit x which is given encrypted in the public key. Intuitively, in several games in the proof, the OR proof enables us to randomize the ciphertexts in the partitions where the disjunct $z = x$ holds, while restricting the adversary to attempt a win only in the other partitions. In addition to the blueprint of [JOR18], we also need an encryption of a random element w in the CRS. The secret w will only be given to the simulator in some of the security games where it can provide an alternative (real) proof to another OR-NIZK Π_3 which proves that the given word is in the language, or that it can give another encryption ct_v of w. Intuitively, these extra elements are provided to introduce a seed randomness into γ in one of the hybrids. While in [JOR18], the seed randomness could be held private in the signing key, in a NIZK we need to hide it in the public CRS. Finally, we also include a QA-NIZK Π_2 certifying that $(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_v)$ is well-formed. Instantiations of OR-NIZKs are given in Section 4.

The (almost) tight security of this scheme is proved in the next section. We prove that this construction has an $O(\log Q)$ reduction to $\mathcal{D}_k$-MDDH, where Q is the number of simulated proofs given out. To prove $O(\log Q)$ reduction, we follow the partitioning strategy of [GHKP18], where the partition is done on the bits of the query index i, instead of a random function applied to the argument. In Section **??**, we provide another construction which builds upon this one and additionally takes a label as an input, which is useful for some applications like CCA-secure PKE. Finally, in Section 3.2, we describe some optimizations which reduce the size of the proofs even further.

```
crsgen $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n \times t})$ :
  Boost the given distribution $\mathcal{D}_{k+1,k}$ to $\mathcal{D}_{2k,k}$.
  Sample $\mathbf{B} \leftarrow \mathcal{D}_{2k,k}$-MDDH and $(\mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^k \times \mathbb{Z}_q^n$.
  Set $\mathbf{p}_1 := \mathbf{M}^\top \mathbf{k}_1, \mathbf{p}_2 := \bar{\mathbf{B}}^\top \mathbf{k}_2$ and $\mathbf{p}_3 = \mathbf{M}^\top \mathbf{k}_3$.
  Sample $(\text{CRS}_p^i, \text{CRS}_v^i) \leftarrow \mathit{\Pi}_i.\mathsf{crsgen}(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, \cdot)$ for $i \in [0\text{-}3]$, with
  parameters described below.

  Sample $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KeyGen}(\mathbb{G}_1)$ for $i \in [3]$.
  Sample $\mathbf{r}_x \leftarrow \mathbb{Z}_q^k$. Set $x := 0$ and $\mathsf{ct}_x := \mathsf{PKE.Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$.
  Sample $(k_0, \mathbf{r}_w) \leftarrow \mathbb{Z}_q \times \mathbb{Z}_q^k$. Set $w := k_0$ and $\mathsf{ct}_w := \mathsf{PKE.Enc}(\mathsf{pk}_3, w; \mathbf{r}_w)$.
  Let $\mathsf{crh}$ be a collision resistant hash from $\{0,1\}^*$ to $\mathbb{Z}_q$.

  Set $\text{CRS}_p := (\text{CRS}_p^{[0-3]}, [\mathbf{B}]_1, [\mathbf{p}_{[1..3]}]_1, \mathsf{pk}_{[1..3]}, \mathsf{ct}_x, \mathsf{ct}_w)$.
  Set $\text{CRS}_v := (\text{CRS}_v^{[0-3]}, [\mathbf{B}]_1, [\mathbf{p}_{[1..3]}]_1, \mathsf{pk}_{[1..3]}, \mathsf{ct}_x, \mathsf{ct}_w)$.

  Return $(\text{CRS}_p, \text{CRS}_v)$.

prover $(\text{CRS}_p,\ \mathbf{y} = [\mathbf{M}\mathbf{x}]_1,\ \mathbf{x},\ \mathtt{lbl})$:
  Sample $(\mathbf{r}, \mathbf{r}_z^1, \mathbf{r}_z^2, \mathbf{r}_v) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k \times \mathbb{Z}_q^k \times \mathbb{Z}_q^k$.
  Set $\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top$.

  Set $z := 0,\ \mathsf{ct}_z^1 := \mathsf{PKE.Enc}(\mathsf{pk}_1, z; \mathbf{r}_z^1)$ and $\mathsf{ct}_z^2 := \mathsf{PKE.Enc}(\mathsf{pk}_2, z; \mathbf{r}_z^2)$.
  Set $v := 0,\ \mathsf{ct}_v := \mathsf{PKE.Enc}(\mathsf{pk}_3, v; r_v)$.

  Set $\pi_0 := \mathit{\Pi}_0.\mathsf{prover}(\text{CRS}_p^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1, \mathsf{ct}_x),\ (\mathbf{r}, 0, 0, 0))$.
  Set $\pi_1 := \mathit{\Pi}_1.\mathsf{prover}(\text{CRS}_p^1,\ (\mathsf{ct}_z^1, \mathsf{ct}_z^2),\ (0, \mathbf{r}_z^1, \mathbf{r}_z^2))$.
  Set $\pi_3 := \mathit{\Pi}_3.\mathsf{prover}(\text{CRS}_p^3,\ (\mathbf{y}, \mathsf{ct}_w, \mathsf{ct}_v),\ (\mathbf{x}, 0, 0, 0))$.
  Set $\tau = \mathsf{crh}(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \mathsf{ct}_v, \pi_0, \pi_1, \pi_3, \mathtt{lbl})$.
  Set $\gamma := \mathbf{x}^\top [\mathbf{p}_1 + \tau \mathbf{p}_3]_1 + \mathbf{r}^\top [\mathbf{p}_2]_1$
  Set $\pi_2 := \mathit{\Pi}_2.\mathsf{prover}(\text{CRS}_p^2,\ (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_v, \text{tag} = \tau),\ (\mathbf{x}, \mathbf{r}, 0, \mathbf{r}_v))$.

  Return $\pi := (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \mathsf{ct}_v, \pi_0, \pi_1, \pi_2, \pi_3)$.

ver $(\text{CRS}_v,\ \mathbf{y},\ \pi,\ \mathtt{lbl})$ :
  Set $\tau = \mathsf{crh}(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \mathsf{ct}_v, \pi_0, \pi_1, \pi_3, \mathtt{lbl})$.
  Check all the NIZK proofs:
      $\mathit{\Pi}_0.\mathsf{ver}(\text{CRS}_v^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1, \mathsf{ct}_x),\ \pi_0)$ and $\mathit{\Pi}_1.\mathsf{ver}(\text{CRS}_v^1,\ (\mathsf{ct}_z^1, \mathsf{ct}_z^2),\ \pi_1)$
  and $\mathit{\Pi}_2.\mathsf{ver}(\text{CRS}_v^2,\ (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_v, \text{tag} = \tau),\ \pi_2)$ and $\mathit{\Pi}_3.\mathsf{ver}(\text{CRS}_v^3,\ (\mathbf{y}, \mathsf{ct}_w, \mathsf{ct}_v),\ \pi_3)$.
```

Languages:

$\mathit{\Pi}_0$ is an OR-NIZK for $L_0 \overset{\text{def}}{=} \{(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_1, \mathsf{ct}_2) \mid \exists(\mathbf{r}, m, \mathbf{r}_1, \mathbf{r}_2) :\ (\boldsymbol{\rho} = [\bar{\mathbf{B}}\mathbf{r}]_1^\top \textbf{ and } \hat{\boldsymbol{\rho}} = [\underline{\mathbf{B}}\mathbf{r}]_1^\top) \textbf{ or } (\mathsf{ct}_1 = \mathsf{PKE.Enc}(\mathsf{pk}_1, m; \mathbf{r}_1) \textbf{ and } \mathsf{ct}_2 = \mathsf{PKE.Enc}(\mathsf{pk}_1, m; \mathbf{r}_2))\}$. Instantiation is given in Fig. 4.

$\mathit{\Pi}_1$ is a QA-NIZK for $L_1 \overset{\text{def}}{=} \{(\mathsf{ct}_1, \mathsf{ct}_2) \mid \exists(m, \mathbf{r}_1, \mathbf{r}_2) : \mathsf{ct}_z^1 = \mathsf{PKE.Enc}(\mathsf{pk}_1, m; \mathbf{r}_1) \textbf{ and } \mathsf{ct}_2 = \mathsf{PKE.Enc}(\mathsf{pk}_2, m; \mathbf{r}_2)\}$, with parameters $(\mathsf{pk}_1, \mathsf{pk}_2)$. Instantiations as in [JR14,KW15].

$\mathit{\Pi}_2$ is a QA-NIZK for $L_2 \overset{\text{def}}{=} \{(\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}, \text{tag} = \tau) \mid \exists(\mathbf{x}, \mathbf{r}, v, \mathbf{r}_v) : \mathbf{y} = [\mathbf{M}\mathbf{x}]_1 \textbf{ and } \boldsymbol{\rho} = [\bar{\mathbf{B}}\mathbf{r}]_1^\top \textbf{ and } \hat{\boldsymbol{\rho}} = [\underline{\mathbf{B}}\mathbf{r}]_1^\top \textbf{ and } \gamma = \mathbf{x}^\top [\mathbf{p}_1 + \tau \mathbf{p}_3]_1 + \mathbf{r}^\top [\mathbf{p}_2]_1 + [v]_1 \textbf{ and } \mathsf{ct} = \mathsf{PKE.Enc}(\mathsf{pk}_3, v, \mathbf{r}_v)\}$, with parameters $([\mathbf{M}]_1, [\mathbf{B}]_1, [\mathbf{p}_{[1-3]}]_1, \mathsf{pk}_3)$. Instantiations as in [JR14,KW15].

$\mathit{\Pi}_3$ is an OR-NIZK for $L_3 \overset{\text{def}}{=} \{(\mathbf{y}, \mathsf{ct}_1, \mathsf{ct}_2) \mid \exists(\mathbf{x}, m, \mathbf{r}_1, \mathbf{r}_2) :\ \mathbf{y} = [\mathbf{M}\mathbf{x}]_1 \textbf{ or } (\mathsf{ct}_1 = \mathsf{PKE.Enc}(\mathsf{pk}_3, m; \mathbf{r}_1) \textbf{ and } \mathsf{ct}_2 = \mathsf{PKE.Enc}(\mathsf{pk}_3, m; \mathbf{r}_2))\}$. Instantiation is given in Fig. 4.

Fig. 1. Tightly-secure USS-QA-NIZK $\mathit{\Pi}$.

```
crssim $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n \times t})$ :
  Boost the given distribution $\mathcal{D}_{k+1,k}$ to $\mathcal{D}_{2k,k}$.
  Sample $\mathbf{B} \leftarrow \mathcal{D}_{2k,k}$-MDDH and $(\mathbf{k}_1, \mathbf{k}_2) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^k$.
  Set $\mathbf{p}_1 := \mathbf{M}^\top \mathbf{k}_1$ and $\mathbf{p}_2 := \bar{\mathbf{B}}^\top \mathbf{k}_2$.
  Sample $(\textsc{crs}_p^i, \textsc{crs}_v^i) \leftarrow \mathit{\Pi}_i.\mathsf{crsgen}(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, \cdot)$ for $i \in [0\text{-}1]$.
  Sample $(\textsc{crs}_p^i, \textsc{crs}_v^i, \mathsf{trap}^i) \leftarrow \mathit{\Pi}_i.\mathsf{crssim}(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, \cdot)$ for $i \in [2\text{-}3]$.

  Sample $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{PKE.KeyGen}(\mathbb{G}_1)$ for $i \in [3]$.
  Sample $\mathbf{r}_x \leftarrow \mathbb{Z}_q^k$. Set $x := 0$ and $\mathsf{ct}_x := \mathsf{PKE.Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$.
  Sample $(k_0, \mathbf{r}_w) \leftarrow \mathbb{Z}_q \times \mathbb{Z}_q^k$. Set $w := k_0$ and $\mathsf{ct}_w := \mathsf{PKE.Enc}(\mathsf{pk}_3, w; \mathbf{r}_w)$.

  Set $\textsc{crs}_p := (\textsc{crs}_p^{[0-3]}, [\mathbf{B}]_1, [\mathbf{p}_{[1-2]}]_1, \mathsf{pk}_{[1-3]}, \mathsf{ct}_x, \mathsf{ct}_w)$.
  Set $\textsc{crs}_v := (\textsc{crs}_v^{[0-3]}, [\mathbf{B}]_1, [\mathbf{p}_{[1-2]}]_1, \mathsf{pk}_{[1-3]}, \mathsf{ct}_x, \mathsf{ct}_w)$.
  Set $\mathsf{trap} := (\mathbf{k}_1, \mathsf{trap}^{[2-3]})$

  Return $(\textsc{crs}_p, \textsc{crs}_v, \mathsf{trap})$.

sim $(\textsc{crs}_p,\ \mathsf{trap},\ \mathbf{y})$:
  Sample $(\mathbf{r}, \mathbf{r}_z^1, \mathbf{r}_z^2, \mathbf{r}_v) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k \times \mathbb{Z}_q^k \times \mathbb{Z}_q^k$.
  Set $\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top,\ \gamma := \mathbf{y}^\top \mathbf{k}_1 + \mathbf{r}^\top [\mathbf{p}_2]_1$.

  Set $z := 0,\ \mathsf{ct}_z^1 := \mathsf{PKE.Enc}(\mathsf{pk}_1, z; \mathbf{r}_z^1)$ and $\mathsf{ct}_z^2 := \mathsf{PKE.Enc}(\mathsf{pk}_2, z; \mathbf{r}_z^2)$.
  Set $v := 0,\ \mathsf{ct}_v := \mathsf{PKE.Enc}(\mathsf{pk}_3, v; \mathbf{r}_v)$.

  Set $\pi_0 := \mathit{\Pi}_0.\mathsf{prover}(\textsc{crs}_p^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1, \mathsf{ct}_x),\ (\mathbf{r}, 0, 0, 0))$.
  Set $\pi_1 := \mathit{\Pi}_1.\mathsf{prover}(\textsc{crs}_p^1,\ (\mathsf{ct}_z^1, \mathsf{ct}_z^2),\ (0, \mathbf{r}_z^1, \mathbf{r}_z^2))$.
  Set $\pi_2 := \mathit{\Pi}_2.\mathsf{sim}(\textsc{crs}_p^2,\ \mathsf{trap}^2,\ (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_v))$.
  Set $\pi_3 := \mathit{\Pi}_3.\mathsf{sim}(\textsc{crs}_p^3,\ \mathsf{trap}^3, (\mathbf{y}, \mathsf{ct}_w, \mathsf{ct}_v))$.

  Return $\pi := (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \mathsf{ct}_v, \pi_0, \pi_1, \pi_2, \pi_3)$.
```

Fig. 2. CRS and Proof simulators for $\mathit{\Pi}$.

3.1 Security of the USS-QA-NIZK Scheme

In this section we state and prove the security of the USS-QA-NIZK scheme Π described in Figure 1, with simulators described in Figure 2.

Theorem 2. *For any efficient adversary $\mathcal{A}$, which makes at most Q simulator queries before attempting a forged proof, its probability of success ($\text{ADV}^{\mathsf{uss}}_{\Pi}(Q)$) in the USS game against the scheme Π is at most*

$$\text{ADV}^{\mathsf{tss}}_{\Pi_2} + 2 \cdot \text{ADV}^{\mathsf{zk}}_{\Pi_3} + 12L \cdot \text{ADV}^{\mathsf{tss}}_{\Pi_1} + (12L+1)\text{ADV}^{\mathsf{zk}}_{\Pi_0}$$

$$+(4L+2) \cdot \text{ADV}^{\mathsf{mcpa}}_{\mathsf{PKE}} + 8L \cdot \text{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}} + \frac{6L+Q}{q}$$

Here L is the least integer greater than the bit size of Q and hence is $O(\log Q)$.

Remark 1. $\text{ADV}^{\mathsf{tss}}_{\Pi_i}$ of a QA-NIZK Π_i reduces to $\mathcal{D}_k$-MDDH by a factor of $(n-t)$ where the (affine) linear subspace language is of dimension t within a full space of dimension n. Also, $\text{ADV}^{\mathsf{zk}}_{\Pi_i}$ of an OR-NIZK Π_i reduces to $\mathcal{D}_k$-MDDH by a factor of 1. Finally, $\mathcal{D}_{2k,k}$-MDDH reduces to $\mathcal{D}_k$-MDDH by a factor of k by boosting (See Section 2.1). Thus the overall reduction in Theorem 2 to $\mathcal{D}_k$-MDDH is $O(\log Q)$.

Proof Intuition. At the highest level, we go through a sequence of games (0-4), starting from Game 0 which is the NIZK simulator of Figure 2 playing against a USS adversary and ending with Game 4, where the adversary has information theoretically negligible chance of winning. We start off with introducing a random mask k_0 into the γ components of the simulated proofs in Game 1. Then in going from Game 2 to Game 3, the γ component is masked with an independently random element which depends on the query number. Then finally in Game 4, the quantity $\mathbf{k}_1$ is shifted by a random vector in the kernel of the language matrix $\mathbf{M}$. This still keeps the CRS unchanged and since the simulated proofs have been masked by independently random elements, they are also independent of this random kernel vector. However, the random kernel vector shows up in the winning condition of Game 4 and makes it statistically hard for the adversary to satisfy verification with a non-member word.

Going from Game 2 to 3 requires another set of hybrid games in which we independently randomize the mask elements going into the γ's, starting from the same mask k_0 for all the simulated proofs. The games proceed based on the bits of the query number i. In every hybrid j, which runs from 0 to $L(=\log Q)$, the mask depends on the first j bits of the bit-string representation of i. The mask function is inductively defined as follows:

$$\text{RF}_j(i|_j) \overset{\text{def}}{=} \begin{Bmatrix} \text{RF}_{j-1}(i|_{j-1}), \text{ if } (i_j = \beta) \\ \text{RF}'_{j-1}(i|_{j-1}), \text{ if } (i_j \neq \beta) \end{Bmatrix},$$

where RF_j is a random function from $\{0,1\}^j$ to $\mathbb{Z}_q$, and β is a bit which is freshly sampled in each hybrid. RF'_{j-1} is another independently random function from $\{0,1\}^{j-1}$ to $\mathbb{Z}_q$. The 0-th hybrids start as Game 2 with the k_0 mask, which is the value of $\textsc{rf}_0(\epsilon)$. The L-th hybrids end in Game 3 with the mask depending on all the bits of i, hence independently random for each query.

The adaptive partitioning technique of [Hof17,GHKP18] helps us switching from $\textsc{rf}_{j-1}$ to $\textsc{rf}_j$ with a constant number of MDDH reductions. Essentially, in the j-th hybrid, the j-th bit of i induces two partitions of the message space: (1) where the bit is β, soundness is enforced to hold in the winning condition and (2) where the bit is $1-\beta$, all such simulated proofs can be switched in one go with a constant number of MDDH transitions. Formal details follow.

Proof. We go through a sequence of Games $\mathbf{G}_0$ to $\mathbf{G}_3$ which are described below and summarized in Figure 3. In the following, $\Pr_i[X]$ will denote probability of predicate X holding in probability space defined in game $\mathbf{G}_i$ and WIN_i will denote the winning condition for the adversary in game $\mathbf{G}_i$.

Game $\mathbf{G}_0$: This game exactly replicates the simulator construction to the adversary. So the adversary's advantage in $\mathbf{G}_0$ (defined as WIN_0 below) is the USS advantage we seek to bound.

$$\mathsf{WIN}_0 \overset{\triangle}{=} \ (\mathbf{y}^* \not\in \{\mathbf{y}^i\}_i \cup \mathrm{span}([\mathbf{M}]_1)) \textbf{ and } \mathsf{ver}(\textsc{crs}_v,\ \mathbf{y}^*,\ \pi^*)$$

Game $\mathbf{G}_{0.2}$: In this game, the challenger first moves to simulation mode for Π_0, so that $\mathbf{r}$ is not explicitly required for computing π_0. Next it uses IND-CPA security to change v in each of the simulated-proof-queries from 0 to k_0. Note, there is no decryption going on at this point, i.e., $\mathbf{p}_2$ and sk_3 are not being used, and hence CPA-security suffices.

Game $\mathbf{G}_{0.3}$: In this game, the challenger moves to binding mode for Π_3 and uses witness $(\mathbf{r}_w, \mathbf{r}_v)$ for the second disjunct in each simulated-proof-query.

Game $\mathbf{G}_1$: The challenge-response in this game is the same as $\mathbf{G}_0$. The winning condition is now defined as:

$$\begin{aligned} \mathsf{WIN}_1 \overset{\triangle}{=} \mathsf{WIN}_0 \textbf{ and } & \pi^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \cdots) : \\ & \exists\theta : \left\{ \begin{array}{l} \gamma^* = \mathbf{y}^{*\top}(\mathbf{k}_1{+}\tau\mathbf{k}_3) + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 \\ \textbf{and } (\theta \in \mathcal{Z} \textbf{ or } \mathbf{y}^* \in \mathrm{span}([\mathbf{M}]_1)) \end{array} \right\} \\ & \textbf{and } (\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1), \end{aligned}$$

where $\mathcal{Z}$ is the singleton set $\{k_0\}$. Hence, the difference in advantages of the adversary is upper bounded by the unbounded true-simulation-soundness of Π_2 (and the soundness of Π_3). Here, we use the crucial fact, that if a QA-NIZK is defined for a language $\mathcal{L}$, i.e. is sound for a language $\mathcal{L}$, then it is true-simulation sound for any language $\mathcal{L}'$ which is a superset of $\mathcal{L}$, as long as all simulated proofs are for elements from $\mathcal{L}'$. Thus, consider the language $\mathcal{L}'$ defined as follows:

$$\mathcal{L}' \overset{\text{def}}{=} \left\{ \begin{array}{c} (\mathbf{y}, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}) \mid \exists(\mathbf{m}, \mathbf{r}, \mathbf{r}_v, v) : \\ \mathbf{y} = [\mathbf{M}\mathbf{m}]_1 \textbf{ and } \boldsymbol{\rho}^\top = [\bar{\mathbf{B}}\mathbf{r}]_1 \textbf{ and } \hat{\boldsymbol{\rho}}^\top = [\underline{\mathbf{B}}\mathbf{r}]_1 \\ \textbf{and } \gamma = [(\mathbf{M}\mathbf{m})^\top(\mathbf{k}_1 + \tau\mathbf{k}_3) + v + \mathbf{r}^\top\mathbf{k}_2]_1 \\ \textbf{and } \mathsf{ct} = \mathsf{PKE.enc}(\mathsf{pk}, v; \mathbf{r}_v) \end{array} \right\},$$

```
                   $\mathsf{crssim}()$ : $\cdots$
Games 0, 0.3-1.1   $\textsc{crs}^0 \leftarrow \mathit{\Pi}_0.\mathsf{crsgen}()$
Games 0.2, 2-4     $(\textsc{crs}^0, \mathsf{trap}^0) \leftarrow \mathit{\Pi}_0.\mathsf{crssim}()$
Game 0-0.3         $\textsc{crs}^1 \leftarrow \mathit{\Pi}_1.\mathsf{crsgen}()$
Games 1-4          $(\textsc{crs}^1, \mathsf{trap}^1) \leftarrow \mathit{\Pi}_1.\mathsf{crssim}()$
Game 0.3-1         $\textsc{crs}^3 \leftarrow \mathit{\Pi}_3.\mathsf{crsgen}()$
Games 0-0.2, 1.1-4 $(\textsc{crs}^3, \mathsf{trap}^3) \leftarrow \mathit{\Pi}_3.\mathsf{crssim}()$

                   Sample $(\mathbf{k}_1',\ \mathbf{u}) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^{n-t}$
Games 0-3          Set $\mathbf{k}_1 := \mathbf{k}_1'$
Game 4             Set $\mathbf{k}_1 := \mathbf{k}_1' + \mathbf{M}^\perp \mathbf{u}$

Games 0-1          Set $w := k_0$
Game 1.1-4         Set $w := 0$
                   $\cdots$
```

```
                   $\mathsf{sim}(\mathbf{y}^i \in \mathbb{G}_1^n)$ : $\cdots$
                   Set $(v, \boldsymbol{\rho}^i, \hat{\boldsymbol{\rho}}^i, \gamma^i) :=$
Game 0                 $(0, [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top,\ [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top,\ \mathbf{y}^{i\top}\mathbf{k}_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$
Games 0.2-2            $(k_0, [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top,\ [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [k_0]_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$
Game 3                 $(k_0, [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top,\ [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [\textsc{rf}_L(i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$
Game 4                 $(k_0, [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top,\ [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top,\ \mathbf{y}^{i\top}\mathbf{k}_1' + \mathbf{y}^{i\top}\mathbf{M}^\perp\mathbf{u} + [\textsc{rf}_L(i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$
                   $\cdots$
```

```
                   $\mathsf{WIN} \overset{\text{def}}{=}$ $\pi^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \mathsf{ct}_z^{1*}, \mathsf{ct}_z^{2*}, \mathsf{ct}_v^*, \pi_0^*, \pi_1^*, \pi_2^*, \pi_3^*)$ :
                       $(\mathbf{y}^* \notin \{\mathbf{y}^i\}_i \cup \mathrm{span}([\mathbf{M}]_1))$ and $\mathsf{ver}(\textsc{crs}_v,\ \mathbf{y}^*,\ \pi^*)$
Games 1-3               and $\exists\theta \in \mathcal{Z} : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$
Game 4                  and $\exists\theta \in \mathcal{Z} : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1' + \mathbf{y}^{*\top}\mathbf{M}^\perp\mathbf{u} + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$
Games 1-4               and $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$
```

Fig. 3. Top level games and winning conditions

with parameters $([\mathbf{B}]_1, [\mathbf{k}_1]_1, [\mathbf{k}_2]_1, \mathsf{pk})$. We therefore have:

$$|\Pr_1[\mathsf{WIN}_1] - \Pr_0[\mathsf{WIN}_0]| \le \textsc{adv}^{\mathsf{tss}}_{\Pi_2} \tag{1}$$

Since the condition WIN_0 has a conjunct that $\mathbf{y}^*$ is not in span of $[\mathbf{M}]_1$, we can equivalently state the winning condition as:

$$\begin{aligned}\mathsf{WIN}_1 \overset{\triangle}{=} \mathsf{WIN}_0 \ \textbf{and}\ \pi^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \cdots) :& \\ \exists \theta \in \mathcal{Z} : \gamma^* = \mathbf{y}^{*\top}(\mathbf{k}_1 + \tau\mathbf{k}_3) + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2& \\ \textbf{and}\ (\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1).&\end{aligned}$$

Game $\mathbf{G}_{1.1}$: In this game the Challenger moves to hiding CRS for Π_3. The proofs for Π_3 in each of the simulated-proof queries are generated without witness now. Next, using IND-CPA security of $\mathsf{PKE.enc}$ it sets $w = 0$ in c_w. Note, v in each of the simulated proofs still remains k_0.

The indistinguishablity of the games follows by IND-CPA of PKE and ZK of Π_3.

Game $\mathbf{G}_2$: In this game, Π_0 is switched from real mode to simulation mode.

The winning condition WIN_2 remains the same as WIN_1. Indistinguishability follows by the ZK property of Π_0:

$$|\Pr_2[\mathsf{WIN}_2] - \Pr_1[\mathsf{WIN}_1]| \le \textsc{adv}^{\mathsf{zk}}_{\Pi_0} \tag{2}$$

Game $\mathbf{G}_3$: In this game, the challenger also lazily maintains a function $\textsc{rf}_L$ mapping $(L = \log Q)$-bit strings to $\mathbb{Z}_q$. The function $\textsc{rf}_L$ has the property that it is a random and independent function from L-bit strings to $\mathbb{Z}_q$. In $\mathbf{G}_3$, each signature component γ^i is generated as $\mathbf{y}^{i\top}\mathbf{k}_1 + [\textsc{rf}_L(i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$, instead of $\mathbf{y}^{i\top}\mathbf{k}_1 + [k_0]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$ The winning condition WIN_3 remains the same as WIN_2. The set $\mathcal{Z}$ is now defined as

$$\mathcal{Z} = \{\textsc{rf}_L(i)\}_{i\in[Q]}.$$

To be precise, the WIN condition is now

$$\begin{aligned}\mathsf{WIN}_1 \overset{\triangle}{=} \mathsf{WIN}_0 \ \textbf{and}\ \pi^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \cdots) :& \\ \exists \theta \in \mathcal{Z} : \gamma^* = \mathbf{y}^{*\top}(\mathbf{k}_1 + \tau\mathbf{k}_3) + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2& \\ \textbf{and}\ (\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1),&\end{aligned}$$

where $\mathcal{Z}$ is $\{\textsc{rf}_L(i)\}_{i\in[Q]}$.

Lemma 1. $\Pr_2[\mathsf{WIN}_2] \le \Pr_3[\mathsf{WIN}_3] +$

$$12L \cdot \textsc{adv}^{\mathsf{tss}}_{\Pi_1} + 8L \cdot \textsc{adv}_{\mathcal{D}_{2k,k}}\text{-MDDH}$$

$$+12L \cdot \textsc{adv}^{\mathsf{zk}}_{\Pi_0} + 4L \cdot \textsc{adv}^{\mathsf{mcpa}}_{\mathsf{PKE}} + \frac{6L}{q}$$

We will prove this lemma in Appendix A.

Game $\mathbf{G}_4$: In this game, the challenger samples $(\mathbf{k}_1', \mathbf{u}) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^{n-t}$,$(\mathbf{k}_3', \mathbf{v}) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^{n-t}$ and generates $\mathbf{k}_1$ (and $\mathbf{k}_3$) differently as $\mathbf{k}_1' + \mathbf{M}^{\perp}\mathbf{u}$ ($\mathbf{k}_3' + \mathbf{M}^{\perp}\mathbf{v}$ resp., where $\mathbf{M}^{\perp}$ is a $\mathbb{Z}_q^{t\times(n-t)}$ matrix such that $\mathbf{M}^{\top}\mathbf{M}^{\perp} = \mathbf{0}^{t\times(n-t)}$. Observe that the public key component $[\mathbf{p}]_1$ becomes $[\mathbf{M}^{\top}\mathbf{k}_1]_1 = [\mathbf{M}^{\top}\mathbf{k}_1']_1$. So $\mathbf{u}$ does not show up in the public key. Similarly, $\mathbf{v}$ does not show up in the public key.

Consequently, the computations of γ^i's are changed to $\mathbf{y}^{i\top}(\mathbf{k}_1'+\tau\mathbf{k}_3')+ \mathbf{y}^{i\top}\mathbf{M}^{\perp}(\mathbf{u}+\tau\mathbf{v}) + [\mathrm{RF}_L(i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$. Also, the winning condition check on γ^* is modified accordingly to

$$\exists\theta \in \mathcal{Z} : \ \gamma^* = \mathbf{y}^{*\top}(\mathbf{k}_1' + \tau^*\mathbf{k}_3') + \mathbf{y}^{*\top}\mathbf{M}^{\perp}(\mathbf{u} + \tau^*\mathbf{v}) + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2.$$

We now claim that $\Pr_3[\mathsf{WIN}_3] \le Q/q$. We prove this claim by employing the union bound, and prove that for each simulated-proof-query j, the probability of WIN_3 holding with $\theta = \mathrm{RF}_L(j)$ is at most $1/q$. Now, observe that each entry in $\mathcal{Z}$ is absent from the public key as well as from all the simulated proofs, except at most one response by the property of RF_L. For all queries $i \ne j$, we observe that $\mathrm{RF}_L(i)$ is uniformly random and independent of both k_0 and $\mathrm{RF}_L(j)$. So all the γ^i-s, for $i \ne j$, might as well be sampled independently and randomly.

Coming back to the j-th query, let $k^* = \mathrm{RF}_L(j)$. Now either $\mathbf{y}^* - \mathbf{y}^j \notin \mathrm{span}([\mathbf{M}]_1)$, in which case $[k^*]_1 + \mathbf{y}^{*\top}\mathbf{M}^{\perp}\mathbf{u}$ is uniformly random and independent of $[k^*]_1\mathbf{y}^{j\top}\mathbf{M}^{\perp}\mathbf{u}$, or else $\mathbf{y}^* - \mathbf{y}^j \in \mathrm{span}([\mathbf{M}]_1)$. In the latter case, because of the collision-resistance property of crh, we can assume that $\tau^* \ne \tau^j$. Then, given that $\mathbf{y}^* \notin \mathrm{span}([\mathbf{M}]_1)$, the quantity $(\tau^* - \tau^j)\mathbf{y}^{*\top}\mathbf{M}^{\perp}\mathbf{v}$ is random and independent of all other quantities. Thus, In either caee, the probability of the adversary producing $\gamma^* - \boldsymbol{\rho}^*\mathbf{k}_2 = \mathbf{y}^{*\top}(\mathbf{k}_1' + \tau^*\mathbf{k}_3')+ \mathbf{y}^{*\top}\mathbf{M}^{\perp}(\mathbf{u} + \tau^*\mathbf{v}) + [k^*]_1$ is bounded in probability by $1/q$:

$$\Pr_3[\mathsf{WIN}_3] \le Q/q.$$

3.2 Optimizations

In this section, we describe two optimizations which reduce the size of the proofs further by $2k$ elements under the $\mathcal{D}_k$-MDDH assumption.

ElGamal Encryption with Common Randomness. As described in [AHN+17], the randomnesses $\mathbf{r}_z^1$ and $\mathbf{r}_z^2$ of ciphertexts ct_z^1 and ct_z^2 can be shared and merged into a single k-element $\mathbf{r}_z$. In more details, let's say $\mathsf{ct}_z^1 = ([\bar{\mathbf{A}}_1\mathbf{r}_z^1]_1, [z + \underline{\mathbf{A}}_1\mathbf{r}_z^1]_1)$ and $\mathsf{ct}_z^2 = ([\bar{\mathbf{A}}_2\mathbf{r}_z^2]_1, [z + \underline{\mathbf{A}}_2\mathbf{r}_z^2]_1)$, which are encryptions of z under public keys $[\mathbf{A}_1]_1$ and $[\mathbf{A}_2]_1$. Then instead of computing the ciphertexts independently, we can merge them into $([\bar{\mathbf{A}}_1\mathbf{r}_z]_1, [z+\underline{\mathbf{A}}_1\mathbf{r}_z]_1), [z+\underline{\mathbf{A}}_2\mathbf{r}_z]_1)$. This saves us k elements. Importantly, we can still enable transitions where we can expose the decryption key of one system, while switching the plaintext of the other.

Merge QA-NIZKs in the Same Group. The reason we did not combine Π_1 and Π_2 is that we needed to use the true-simulation-soundness of one system, while producing proofs over fake instances with the other. However, we show in Appendix C, that we can still merge the proofs into one proof over the combined linear system, and still be independently able to use the true-simulation-soundness of its parts. This saves us k elements from Π.

In more details, let the combined language be defined by the matrix $\mathbf{M} = \begin{pmatrix} \mathbf{M}_1^{n_1 \times t} \\ \mathbf{M}_2^{n_2 \times t} \end{pmatrix}$, where both n_1 and n_2 are greater than t. What we show is, provided the words corresponding to $[\mathbf{M}_1]_1$ are not faked then even if the words corresponding to $[\mathbf{M}_2]_1$ are faked, true-simulation-soundness holds for the $[\mathbf{M}_1]_1$ components.

4 NIZK for Disjunction of Linear Subspaces

We have critically used an "OR"-NIZK in our USS-QA-NIZK construction. In this section we describe three flavors of OR-NIZKs. The first one is a standard NIZK where both the prover and verifier are public algorithms. The second one is a designated prover system where only the verifier is public - this flavor is useful for signature schemes where the signing key is held private. The final one is a designated verifier system where the prover is public, but the verifier is private - this is useful in public-key encryption schemes where the public encryption algorithm is required to prove consistency, but only the private decryption algorithm needs to check a proof.

4.1 Public CRS Setting

In this section we describe a NIZK proof system for languages of the following type:

$$L^{\vee} \stackrel{\text{def}}{=} \left\{ \begin{matrix} ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1) \in \mathbb{G}_1^{n_0} \times \mathbb{G}_1^{n_1} \mid \\ \exists \mathbf{r}_0 \in \mathbb{Z}_q^{t_0} : [\mathbf{x}_0]_1 = [\mathbf{A}_0]_1 \mathbf{r}_0 \ \textbf{or} \ \exists \mathbf{r}_1 \in \mathbb{Z}_q^{t_1} : [\mathbf{x}_1]_1 = [\mathbf{A}_1]_1 \mathbf{r}_1 \end{matrix} \right\}$$

The system is described in Figure 4 and is based on [Ràf15] with syntax based on [GHKP18]. The proofs of completeness, zero-knowledge and soundness are similar to these papers. We only give a sketch below.

The completeness of the system is straightforward. Zero-knowledge is proved by transitioning to a different way of generating the CRS along with a trapdoor. The transition is enabled by the $\mathcal{D}_k$-MDDH assumption on $([\mathbf{D}]_1, [\mathbf{z}]_1)$ and the resulting CRS and proof simulators are also given in the same figure.

We now prove perfect soundness. Since $\mathbf{z}_0 + \mathbf{z}_1 = \mathbf{z} \notin \text{span}(\mathbf{D})$, at least one of $\mathbf{z}_0$ and $\mathbf{z}_1$ should be outside the span of $\mathbf{D}$. WLOG, let this be $\mathbf{z}_0$. Therefore, there should be a vector $\mathbf{d}^{\perp} \in \mathbb{Z}_q^{k+1}$, such that $\mathbf{D}^{\top}\mathbf{d}^{\perp} = \mathbf{0}$ and $\mathbf{z}_0^{\top}\mathbf{d}^{\perp} = 1$. Right multiplying this vector to the verification equation $\mathbf{A}_0\mathbf{C}_0 = \mathbf{P}_0\mathbf{D}^{\top} + \mathbf{x}_0\mathbf{z}_0^{\top}$ gives us $\mathbf{A}_0\mathbf{C}_0\mathbf{d}^{\perp} = \mathbf{x}_0$. This means $\mathbf{r}_0 \stackrel{\text{def}}{=} \mathbf{C}_0\mathbf{d}^{\perp}$ satisfies the disjunct $\mathbf{x}_0 = \mathbf{A}_0\mathbf{r}_0$.

```
OR Languages :
  Let $L^\vee \overset{\text{def}}{=} \left\{ \begin{matrix} ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1) \in \mathbb{G}_1^{n_0} \times \mathbb{G}_1^{n_1} \mid \\ \exists \mathbf{r}_0 \in \mathbb{Z}_q^{t_0} : \mathbf{x}_0 = [\mathbf{A}_0 \mathbf{r}_0]_1 \textbf{ or } \exists \mathbf{r}_1 \in \mathbb{Z}_q^{t_1} : [\mathbf{x}_1]_1 = [\mathbf{A}_1 \mathbf{r}_1]_1 \end{matrix} \right\}$.

crsgen $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$ :
  Sample $\mathbf{D} \leftarrow \mathcal{D}_k\text{-MDDH}$ and $\mathbf{z} \leftarrow \mathbb{Z}_q^{k+1} \setminus \mathrm{span}(\mathbf{D})$.
  Return $\textsc{crs} := ([\mathbf{D}]_2, [\mathbf{z}]_2)$.

prover $(\textsc{crs},\ ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1),\ (j, \mathbf{r}_j))$:
  Sample $(\mathbf{v},\ \mathbf{S}_0, \mathbf{S}_1) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^{t_0 \times k} \times \mathbb{Z}_q^{t_1 \times k}$.
  Set $[\mathbf{z}_{1-j}]_2 := [\mathbf{D}]_2 \mathbf{v}$ and $[\mathbf{z}_j]_2 := [\mathbf{z}]_2 - [\mathbf{z}_{1-j}]_2$.
  Set $[\mathbf{C}_j]_2 := \mathbf{S}_j [\mathbf{D}]_2^\top + \mathbf{r}_j [\mathbf{z}_j]_2^\top$ and $[\mathbf{P}_j]_1 := [\mathbf{A}_j]_1 \mathbf{S}_j$.
  Set $[\mathbf{C}_{1-j}]_2 := \mathbf{S}_{1-j} [\mathbf{D}]_2^\top$ and $[\mathbf{P}_{1-j}]_1 := [\mathbf{A}_{1-j}]_1 \mathbf{S}_{1-j} - [\mathbf{x}_{1-j}]_1 \mathbf{v}^\top$.
  Return $\pi := ([\mathbf{z}_0]_2, [\mathbf{C}_0]_2, [\mathbf{P}_0]_1, [\mathbf{C}_1]_2, [\mathbf{P}_1]_1) \in \mathbb{G}_1^{(n_0+n_1)k} \times \mathbb{G}_2^{(t_0+t_1+1)(k+1)}$.

ver $(\textsc{crs},\ ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1),\ \pi)$ :
  Set $[\mathbf{z}_1]_2 := [\mathbf{z}]_2 - [\mathbf{z}_0]_2$.
  Check the following equations for all $j \in \{0, 1\}$:
      $\mathsf{e}([\mathbf{A}_j]_1, [\mathbf{C}_j]_2) = \mathsf{e}([\mathbf{P}_j]_1, [\mathbf{D}]_2^\top) \cdot \mathsf{e}([\mathbf{x}_j]_1, [\mathbf{z}_j]_2^\top)$.

crssim $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$ :
  Sample $\mathbf{D} \leftarrow \mathcal{D}_k\text{-MDDH}$ and $\mathbf{u} \leftarrow \mathbb{Z}_q^k$.
  Set $\mathbf{z} := \mathbf{D}\mathbf{u}$
  Return $\textsc{crs} := ([\mathbf{D}]_2, [\mathbf{z}]_2)$ and $\mathsf{trap} := \mathbf{u}$.

sim $(\textsc{crs},\ \mathsf{trap},\ ([\mathbf{x}_0]_1, [\mathbf{x}_1]_1))$:
  Sample $(\mathbf{v},\ \mathbf{S}_0, \mathbf{S}_1) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^{t_0 \times k} \times \mathbb{Z}_q^{t_1 \times k}$.
  Set $[\mathbf{z}_0]_2 := [\mathbf{D}]_2 \mathbf{v}$ and $[\mathbf{z}_1]_2 := [\mathbf{z}]_2 - [\mathbf{z}_0]_2$.
  Set $[\mathbf{C}_0]_2 := \mathbf{S}_0 [\mathbf{D}]_2^\top$ and $[\mathbf{P}_0]_1 := [\mathbf{A}_0]_1 \mathbf{S}_0 - [\mathbf{x}_0]_1 \mathbf{v}^\top$.
  Set $[\mathbf{C}_1]_2 := \mathbf{S}_1 [\mathbf{D}]_2^\top$ and $[\mathbf{P}_1]_1 := [\mathbf{A}_1]_1 \mathbf{S}_1 - [\mathbf{x}_1]_1 (\mathbf{u} - \mathbf{v})^\top$.
  Return $\pi := ([\mathbf{z}_0]_2, [\mathbf{C}_0]_2, [\mathbf{P}_0]_1, [\mathbf{C}_1]_2, [\mathbf{P}_1]_1)$.
```

Fig. 4. NIZK for OR languages based on [Ràf15].

4.2 Designated Prover Setting

In Figure 4 we saw an efficient NIZK proof for the "OR" languages of Figure 1, where one of the disjuncts was a predicate on group elements in the CRS of the USS-QA-NIZK, namely that ct_x (and ct_w) was a binding commitment to x using randomness r_x (resp. w using randomess r_w). The quantity r_x cannot be made public in this general setting as proving simulation-soundness requires us to hide

x from the public. However, in the application of USS-QA-NIZK to build SPS, the quantity r_x can indeed be given to a "designated" prover, i.e. the signer, and the quantity still remains private. In particular, in a forgery attempt, the adversary does not have access to r_x, as the signer is an honest party. In such a situation, i.e. where r_x in the commitment to x is available to the designated prover, we can give an even more efficient NIZK. For ease of exposition, we will restrict ourselves to the SXDH asymmetric pairings-group setting in this section. The results can easily be generalized to $\mathcal{D}_k$-MDDH setting.

There is another optimization that can be achieved in the designated prover setting, namely that the OR-NIZK $\mathit{\Pi}_3$ is not required at all. The main purpose of this OR-NIZK in the general setting was to introduce a random affine element $v = k_0$ in the expression for γ. However in the designated prover setting, the designated prover can be given w_0 in the clear and hence it can generate γ in the real world with v set to k_0 (as opposed to $v = 0$ in the general setting). So, we are left with only one OR-NIZK, i.e. $\mathit{\Pi}_0$, which we next show can be further optimized in the designated prover setting. These optimizations and the resulting SPS scheme is described in detail in Figure 7.

Consider the "OR" language,

$$\mathcal{L} = \left\{ \begin{array}{c} \boldsymbol{\alpha}, \hat{\boldsymbol{\alpha}}, \boldsymbol{x} \mid \exists r, r_x \in \mathbb{Z}_q : \\ (\boldsymbol{\alpha} = r[1]_1 \textbf{ and } \hat{\boldsymbol{\alpha}} = r[b]_1) \textbf{ or } \boldsymbol{x} = \mathrm{com}(0; r_x) \end{array} \right\}$$

where $\mathrm{com}(x; r_x)$ is a binding commitment to x using randomness r_x (e.g. a GS-commitment or ElGamal encryption), and $[b]_1$ is public.

It is not difficult to see that the above is implied by the following (i.e. $\mathcal{L}_1 \subseteq \mathcal{L}$)

$$\mathcal{L}_1 = \left\{ \begin{array}{c} \boldsymbol{\alpha}, \hat{\boldsymbol{\alpha}}, \boldsymbol{x} \mid \exists x, r_x, \hat{x} \in \mathbb{Z}_q : \\ \hat{\boldsymbol{\alpha}} \cdot x - [b]_1 \cdot \hat{x} = 0 \textbf{ and } [1]_1 \cdot \hat{x} - \boldsymbol{\alpha} \cdot x = 0 \textbf{ and } \boldsymbol{x} = \mathrm{com}(x; r_x) \end{array} \right\}$$

since if $x \neq 0$ in $\mathcal{L}_1$, one can take $r = \hat{x}/x$, and otherwise $\boldsymbol{x}$ is commitment to zero with r_x. Thus soundness of NIZK proof of $\mathcal{L}_1$ implies the tuple is in $\mathcal{L}$.

Now, consider another language $\mathcal{L}_2$,

$$\mathcal{L}_2 = \left\{ \begin{array}{c} \boldsymbol{\alpha}, \hat{\boldsymbol{\alpha}}, \boldsymbol{x} \mid \exists r, x, r_x \in \mathbb{Z}_q : \\ ((\boldsymbol{\alpha} = r[1]_1 \textbf{ and } \hat{\boldsymbol{\alpha}} = r[b]_1) \textbf{ or } (x = 0)) \textbf{ and } \boldsymbol{x} = \mathrm{com}(x; r_x) \end{array} \right\}$$

Thus, in the language the value $\boldsymbol{x}$ is always a commitment to x under r_x. First note that $\mathcal{L}_2$ implies $\mathcal{L}_1$, i.e. $\mathcal{L}_2 \subseteq \mathcal{L}_1$. This is so because if $x = 0$ in $\mathcal{L}_2$, then we just set $\hat{x} = 0$ as well, and if there is a good r, then we set $\hat{x} = r \cdot x$.

Since the "designated" prover always knows x and r_x in the commitment $\boldsymbol{x}$, then if it has an (r, x) which satisfies the "or" part of $\mathcal{L}_2$, it can generate the witnesses required to satisfy membership in $\mathcal{L}_1$ and hence give a valid NIZK proof.

Under the SXDH assumption, $\mathcal{L}_1$ can be proved by using two group elements and in addition two elements for commitment to $\hat{x}$ (and not counting the two for $\boldsymbol{x}$ which is commitment to x) using the technique by Escala and Groth in [EG14]. Namely, the size of π_0 is $(2, 2)$. For this to work, we also need to sample public keys pk_1 of ElGamal encryption (i.e. com) from $\mathbb{G}_2$. Furthermore, pk_1 is taken from $\textsc{crs}^1$ (see Figure 1). We note that this dependency of pk_1 to $\textsc{crs}^1$ does not affect the security proof since we can use ciphertext with respect to pk_2 when $\textsc{crs}^1$ is set to the simulation mode. We further optimize ct_z^1 and ct_z^2 by applying the common randomness technique from Section 3.2. With these modifications, ct_z^1 and ct_z^2 together consist of $(0, 3)$ elements, and proof π_1 is a single element in $\mathbb{G}_2$ (rather than in $\mathbb{G}_1$ in the original construction). Other components, $\boldsymbol{\rho}$, $\hat{\boldsymbol{\rho}}$, γ, and π_2 are unchanged; each of them is represented by a single element in $\mathbb{G}_1$. In total, the proof size will be $(6, 6)$. Under general $\mathcal{D}_k$-MDDH assumption [EHK+13], the optimized proof will consist of $(5k + 1, 4k + 2)$ elements.

4.3 Designated Verifier Setting

As the most expensive part (from the size of USS-QA-NIZK perspective and applications) is the size of the "OR"-proof considered in our general construction, we now consider the designated-verifier setting [ES02]. In the designated-verifier setting of a NIZK, the CRS is split into two parts, $\textsc{crs}_p$ and $\textsc{crs}_v$, and only a designated-verifier gets access to $\textsc{crs}_v$ and the public information is only $\textsc{crs}_p$ (required by the prover). Alternatively, one can think of designated-verifier NIZKs as hash-proof systems, as the $\textsc{crs}_v$ is just the secret hash-key, and $\textsc{crs}_p$ is the projection hash-key – by the fact that hash-proofs can be generated without the witness (but using the secret hash-key), zero-knowledge is automatic; further, soundness is information-theoretic. Since hash-proofs for linear subspace languages are well known [CS98], and we even have hash-proofs for "OR"-languages [ABP15], so we have designated-verifier NIZK proofs for our "OR"-language used in the USS-QA-NIZK construction. Consequently, we have smaller sized (almost) tightly-secure designated-verifier USS-QA-NIZKs.

For this idea to work, we instantiate PKE in $\mathbb{G}_2$ in our construction so that the OR-language consists of relations from both $\mathbb{G}_1$ and $\mathbb{G}_2$. This allows us to use the hash proof system of [ABP15]. The downside of such a construction is that we have more $\mathbb{G}_2$ elements in the proof and the USS-QA-NIZK is itself in the target group $\mathbb{G}_T$, as the construction of [ABP15] generates hashes in the target group. Since these elements require much longer representation we give a more precise estimation. In the original construction of our USS-QA-NIZK with optimizations in Section 3.2, a proof consists of $(11, 6)$ elements in the SXDH setting, of which $(3, 6)$ are for proof π_0. In remaining $(8, 0)$ elements, $(4, 0)$ are the ciphertext of PKE and proof π_1. Moving the $(4, 0)$ elements to $\mathbb{G}_2$ and replacing $(3, 6)$ of π_0 with a target group element, the proof size of our designated-verifier USS-QA-NIZK will be $(4, 4)$ source group elements and 1 target group element. Thus it saves $(7, 2)$ elements in exchange of having an extra target group element. Since the target group element is computed from a product of four pairings, it can also be represented by randomized $(4, 4)$ group elements by using the PPE randomization technique of [AFG+16]. However, either representation requires larger space than original $(7, 2)$ elements. Thus, the known approach with [ABP15] does not seem to yield shorter proofs than our original construction in the designated verifier setting.

5 Applications

In this section, we demonstrate that our tightly secure USS-QA-NIZK can be used to develop CCA2-secure public key encryption and structure-preserving signatures (SPS). Besides being (almost) tightly secure under standard matrix assumptions in bilinear groups, these applications have particular advantage over previous constructions. Our CCA2-secure public-key encryption is *publicly verifiable* and our SPS scheme yields the *shortest signatures.* By plugging our CCA2-secure public key encryption and SPS into the generic frameworks of blind signatures [Fis06], group signatures [Gro07], and simulation-sound NIZKs [CCS09] we have blind SPS, group SPS, and simulation-sound Groth-Sahai proofs, all of which have (almost) tight reduction to standard matrix assumptions in bilinear groups and efficiency improvements over known schemes.

5.1 (Almost) Tight CCA2-Secure PKE Scheme

In this section we show that the labeled (enhanced) USS-QANIZK for linear-subspaces can be used to build a publicly verifiable labeled CCA-secure public-key encryption (PKE) scheme (described in Fig. 5) which is (almost) tightly-secure in the multi-user, multi-challenge setting. The security reduction to USS-QA-NIZK is tight and is independent of the number of decryption-oracle requests of the CCA2 adversary.

Theorem 3. *Under the $\mathcal{D}_k$-MDDH assumption, and using the labeled USS-QA-NIZK Π' of Fig. 1, the public-key encryption scheme described in Fig 5 is (μ, q_e) IND-CCA secure with Adversary's advantage $\mathcal{A}$ upper-bounded by*

$$2 \cdot \text{ADV}^{\mathsf{tss}}_{\Pi'} + 6k \cdot \text{ADV}_{\mathcal{D}_k\text{-MDDH}} + 2 \cdot \text{ADV}^{\mathsf{uss}}_{\Pi'}(q_e) + O(1/q).$$

The proof of this theorem can be found in Appendix D.

Remark. The public-key encryption construction in Fig. 5, during encryption, uses randomness $\mathbf{r}$ to construct $\boldsymbol{\rho}$. Then, it calls USS-QA-NIZK prover in a black-box manner to obtain π. The USS-QA-NIZK construction itself picks another $\mathbf{s}$ and constructs its own $\boldsymbol{\rho}$. We remark that in a non-black box construction of tight CCA2-secure public key encryption scheme, i.e., by utilizing the USS-QA-NIZK construction in a non-black fashion, one can use the same $\bar{\mathbf{B}}$ matrix in the PKE construction above and the USS-QA-NIZK construction, while keeping $\underline{\mathbf{B}}$ matrices sampled ranomly and independently. This leads to a savings of k group elements. The proof of the (almost) tight security of this scheme combines the proof given in Appendix D with the labeled USS-QA-NIZK tight-security (Theorem 2).

5.2 Direct Construction of Tight SPS from Tight USS-QA-NIZK

Recall that unbounded simulation-soundness assures that, after having simulated proofs for chosen instances, it is hard for the adversary to find a valid proof for

```
$\mathsf{KeyGen}\ (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$ :
  [Boost distribution $\mathcal{D}_{k+1,k}$ to $\mathcal{D}_{2k,k}$.]
  Sample $\mathbf{B} \leftarrow \mathcal{D}_{2k,k}$-MDDH and $\mathbf{k} \leftarrow \mathbb{Z}_q^k$,
  Sample $(\textsc{crs}_p, \textsc{crs}_v) \leftarrow \mathit{\Pi}'.\mathsf{crsgen}(\langle q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2 \rangle, [\mathbf{B}]_1)$,
  Set $\mathbf{p} := \bar{\mathbf{B}}^\top \mathbf{k}$, $\mathsf{pk} := (\textsc{crs}_p, [\mathbf{B}]_1, [\mathbf{p}]_1)$, $\mathsf{sk} := (\textsc{crs}_v, \mathbf{k})$.

  Return $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{Enc}\ (\mathsf{pk} = (\textsc{crs}_p, [\mathbf{B}], [\mathbf{p}]_1),\ M \in \mathbb{G}_1,\ \mathtt{lbl})$:
  Sample $\mathbf{r} \leftarrow \mathbb{Z}_q^k$, and set $\boldsymbol{\rho} := [\bar{\mathbf{B}}\mathbf{r}]_1^\top,\ \hat{\boldsymbol{\rho}} := [\underline{\mathbf{B}}\mathbf{r}]_1^\top,\ \gamma := M + \mathbf{r}^\top [\mathbf{p}]_1$,
  $\pi := \mathit{\Pi}'.\mathsf{prover}(\textsc{crs}_p, \langle \boldsymbol{\rho}, \hat{\boldsymbol{\rho}} \rangle, \mathbf{r}, \langle \gamma, \mathtt{lbl} \rangle)$.

  Return $\mathtt{ctxt} := (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \pi)$.

$\mathsf{Dec}\ (\mathsf{sk} = (\textsc{crs}_v, \mathbf{k}),\ \mathtt{ctxt} = (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \pi),\ \mathtt{lbl})$ :
  If the NIZK proof verification
        $\mathit{\Pi}'.\mathsf{ver}(\textsc{crs}_v,\ \langle \boldsymbol{\rho}, \hat{\boldsymbol{\rho}} \rangle,\ \langle \gamma, \mathtt{lbl} \rangle,\ \pi)$
  returns true then return $\gamma - \boldsymbol{\rho}\mathbf{k}$ else return $\perp$.

Language for $\mathit{\Pi}'$:
  $L \overset{\mathrm{def}}{=} \{(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}) \mid \exists \mathbf{r} :\ \boldsymbol{\rho} = [\bar{\mathbf{B}}\mathbf{r}]_1^\top$ and $\hat{\boldsymbol{\rho}} = [\underline{\mathbf{B}}\mathbf{r}]_1^\top\}$ with parameters $([\mathbf{B}]_1)$.
```

Fig. 5. CCA2 Public-Key Encryption using labeled (strong) USS-QA-NIZK.

any fresh no-instances. In [AAO18], it is pointed out that simulation-soundness of a NIZK system corresponds to unforgeability against adaptive chosen message attacks of a signature scheme where no adversary can find a valid signature for any fresh messages after seeing signatures for any chosen messages. Syntactically, an unbounded simulation-sound NIZK system can be seen as a signature scheme whose key generation, signature generation, and signature verification functions correspond to CRS simulation, proof simulation, and proof verification functions of the NIZK system, respectively. This observation is proven formally in a more general setting (allowing errors in correctness, etc) in [AAO18], but we use the simplest form of their result with adjustment to the syntax of USS-QA-NIZK. Concretely, our construction relies on a property of our USS-QA-NIZK that its simulation algorithm works for any no-instance in a certain set. What remains to do is to construct a collision resistant mapping from the desired message space for the signature scheme to the set of no-instances of our USS-QA-NIZK.

Let $\mathit{\Pi} := (\mathsf{pargen}, \mathsf{crsgen}, \mathsf{prover}, \mathsf{ver}, \mathsf{crssim}, \mathsf{sim})$ be a designated prover USS-QA-NIZK system for $\mathcal{L} := \mathrm{span}([\mathbf{M}]_1) \subset \mathbb{G}_1^n$ with soundness advantage $\mathsf{Adv}_{\mathit{\Pi}}^{\mathsf{uss}}(A)$. We assume that $\mathit{\Pi}$ is *perfectly no-instance simulation correct* with respect to $\mathcal{C} := \mathbb{G}_1^n \setminus \mathrm{span}([\mathbf{M}]_1)$ which means that, for any $\textsc{crs}_v$ and trap generated by $\mathit{\Pi}.\mathsf{crssim}$, $y \in \mathcal{C}$, $\pi \leftarrow \mathit{\Pi}.\mathsf{sim}(\mathsf{trap}, y)$, $1 \leftarrow \mathit{\Pi}.\mathsf{ver}(\textsc{crs}_v, y, \pi)$ holds with probability 1.

Let $[\mathbf{M}]_1 \leftarrow \mathbb{G}_1^{n \times t}$ denote a sampling where matrix $\mathbf{M}$ is chosen uniformly with constraint that its upper square sub-matrix is full rank. For message space $\mathcal{M} := \mathbb{G}_1^t$ and $n \geq 2t+1$, we construct a function $H : \mathcal{M} \rightarrow \mathcal{C}$ as follows. Choose $\mathbf{c}$ uniformly from $\mathbb{G}_1^{n-t}$. Then define $H(M)$ for $M \in \mathbb{G}_1^t$ as $M||\mathbf{c}$. For any $\mathbf{M}$ and $M \in \mathbb{G}_1^t$, with probability at least $1 - 1/q$ over the choice of $\mathbf{c}$, there exists no $\mathbf{x}$ that satisfies $(M||\mathbf{c})^\top = [\mathbf{Mx}]_1$. Thus H is an efficiently computable injection from $\mathcal{M}$ to $\mathcal{C}$. Following this idea, we construct a signature scheme as shown in Figure 6.

Theorem 4. *With the above USS-QA-NIZK system Π,* SIG *in Figure 6 is a signature scheme for message space $\mathcal{M} := \mathbb{G}_1^t$. It is tightly unforgeable against adaptive chosen message attacks, i.e., for every* PPT *adversary $\mathcal{A}$ breaking the unforgeability of* SIG *with a chosen message attack with advantage* $\mathsf{Adv}_{\mathsf{SIG}}^{\mathsf{cma}}(\mathcal{A})$*, there exists a* PPT *algorithm $\mathcal{B}$ that breaks unbounded simulation soundness of Π with advantage* $\mathsf{Adv}_{\Pi}^{\mathsf{uss}}(\mathcal{B}) \geq \mathsf{Adv}_{\mathsf{SIG}}^{\mathsf{cma}}(\mathcal{A}) - 1/q$ *and almost the same running time as $\mathcal{A}$. Furthermore, if Π is structure preserving, so is* SIG.

Proof. To show unforgeability, we construct $\mathcal{B}$ using $\mathcal{A}$ as black-box as follows. Given CRS, $[\mathbf{M}]_1$, $\mathcal{B}$ picks $\mathbf{c} \leftarrow \mathbb{G}_1^{n-t}$ and sends $\mathsf{pk} := (\text{CRS}, \mathbf{c})$ to $\mathcal{A}$. For message M queried from $\mathcal{A}$, $\mathcal{B}$ sends $\mathbf{y} := M||\mathbf{c}$ to its oracle, receives a simulated proof π, and returns $\sigma := \pi$ to $\mathcal{A}$. Given a forgery (M^*, σ^*) from $\mathcal{A}$, $\mathcal{B}$ outputs $\mathbf{y}^* := M^*||\mathbf{c}$ and $\pi^* := \sigma^*$. Since $H(M) := M||\mathbf{c}$ is an injection to $\mathbb{G}_1^n \backslash \text{span}([\mathbf{M}]_1)$ with probability at least $1 - 1/q$, $\mathbf{y}^*$ is a fresh instance not in $\text{span}([\mathbf{M}]_1)$, and $(\mathbf{y}^*, \pi^*)$ passes the verification whenever $\mathcal{A}$ succeeds. Hence we have $\mathsf{Adv}_{\Pi}^{\mathsf{uss}}(\mathcal{B}) \geq \mathsf{Adv}_{\mathsf{SIG}}^{\mathsf{cma}}(\mathcal{A}) - 1/q$. Running time of $\mathcal{B}$ is the same as $\mathcal{A}$ except for performing concatenation and parsing. Structure-preserving property is obvious from the construction.

We remark that we can remove $1/q$ term in the above bound in an enhanced model [LPJY15,JR13] where $\mathbf{M}$ is given to the adversary playing the simulation soundness game.

In Figure 7 we present an instantiation of SIG in Figure 6 using our optimized designated prover USS-QA-NIZK from Section 4.2 under the SXDH assumption. Designated prover is sufficient in this application as the signing key is private. The signature size is exactly the same as the proof size of the underlying USS-QA-NIZK and it retains structure preserving property. Hence the signature scheme in Figure 7 is an SPS scheme having signatures consisting of $(6, 6)$ elements for unilateral messages. (Under $\mathcal{D}_k$-MDDH assumption, the signature size will be $(5k + 1, 4k + 2)$). For bilateral messages $(M_1, M_2) \in \mathbb{G}_1^{t_1} \times \mathbb{G}_2^{t_2}$ where $t_1 = t - 1$ and t_2 is arbitrary, we follow a generic construction in [ACD$^+$16, Sec. 6.3] that combines partially one-time signature for a part of messages in $\mathbb{G}_2$. It requires extra $(0, t_2)$ public-key elements, and the signature size increases by $(1, 2)$ elements sacrificing one group element in the message space $\mathbb{G}_1^{t_1}$. A signature thus consists of $(7, 8)$ elements for a bilateral message.

```
Common parameters: $\mathsf{par} := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})$.

$\mathsf{KeyGen}(1^m)$ :
  $\lambda := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2) \leftarrow \Pi.\mathsf{pargen}(1^m)$
  $[\mathbf{M}]_1 \leftarrow \mathbb{G}_1^{n\times t}$
  $\mathbf{c} \leftarrow \mathbb{G}_1^{n-t}$
  $(\textsc{crs}, \mathsf{trap}) \leftarrow \Pi.\mathsf{crssim}(\lambda, [\mathbf{M}]_1)$
  $\mathsf{pk} := (\textsc{crs}, \mathbf{c})$,  $\mathsf{sk} := (\mathsf{trap}, \mathbf{c})$
  $\mathsf{return}(\mathsf{pk}, \mathsf{sk})$

$\mathsf{Sign}(\mathsf{sk}, M)$ :
  $(\mathsf{trap}, \mathbf{c}) \leftarrow \mathsf{sk}$
  $\mathbf{y} := M||\mathbf{c}$
  $\sigma \leftarrow \Pi.\mathsf{sim}(\mathsf{trap}, y)$
  $\mathsf{return}(\sigma)$

$\mathsf{Verify}(\mathsf{pk}, M, \sigma)$ :
  $(\textsc{crs}, \mathbf{c}) \leftarrow \mathsf{pk}$
  $\mathbf{y} := M||\mathbf{c}$
  $b \leftarrow \Pi.\mathsf{ver}(\textsc{crs}, y, \sigma)$
  $\mathsf{return}(b)$
```

Fig. 6. Signature scheme SIG for unilateral messages in $\mathbb{G}_1^t$ based on USS-QA-NIZK Π for a linear subspace language.

5.3 Tightly-secure Blind Structure-Preserving Signature Scheme Based on the Tight-SPS

A generic construction of blind signature scheme is presented in [Fis06]. It is a simple commit-sign-nizk style construction summarized as follows. A user commits to a message m by c and the signer signs c. Given a signature σ, the user computes a NIZK proof π of a correct signature σ with respect to message c and correctness of m as an opening of commitment c without revealing c and σ. Given m and π, a verifier accepts if all proofs are verified. This yields a round-optimal structure-preserving blind signature scheme with tight security in the common reference string model provided that every component is structure-preserving and tightly secure with respect to its underlying assumptions.

We instantiate the generic construction using ElGamal encryption scheme as a commitment scheme $\mathsf{COM} := \{\mathsf{Key}, \mathsf{Com}\}$, the signature scheme $\mathsf{SIG} := \{\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify}\}$ from Section 5.2, and the Groth-Sahai proof system $\mathsf{GS} := \{\mathsf{pargen}, \mathsf{crsgen}, \mathsf{prover}, \mathsf{ver}\}$ from [GS12] where $\mathsf{GS.pargen}$ outputs common parameter λ in the SXDH setting that is compatible with other building blocks.

- In the setup, given common parameters λ, $\mathsf{COM.Key}$ generates a commitment key $f \in \mathbb{G}_1$ and $\mathsf{GS.crsgen}$ generates common reference string $\mathsf{crs}_{\mathsf{gs}}$ for the GS proof system. Then $\mathsf{crs} := (\lambda, f, \mathsf{crs}_{\mathsf{gs}})$ is published as the common reference string for the blind signature scheme.
- The signer generates a key pair by $(vk, sk) \leftarrow \mathsf{SIG.Gen}(\lambda)$.
- In the signature issuing protocol, a user commits to message $m \in \mathbb{G}_1$ by computing $(c, d, z) \leftarrow \mathsf{COM.Com}(f, m; y)$ where $(c, d, z) := (mf^y, g^y, \tilde{g}^y) \in$

```
Common parameters: $\mathsf{par} := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2, [\mathbf{M}]_1 \in \mathbb{G}_1^{n \times t})$.

$\mathsf{KeyGen}(\mathsf{par})$:
  Sample $\textsc{crs}^0 \leftarrow \mathit{\Pi}_0.\mathsf{crsgen}(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{e}, [1]_1, [1]_2)$,
$(\textsc{crs}_p^1, \textsc{crs}_v^1) \leftarrow \mathit{\Pi}_1.\mathsf{crsgen}(\mathsf{par})$, and $(\textsc{crs}_p^2, \textsc{crs}_v^2, \mathsf{trap}^2) \leftarrow \mathit{\Pi}_2.\mathsf{crssim}(\mathsf{par})$.
  Let $([u_1]_2, [u_2]_2, [u_3]_2)$ denote elements of $\mathbb{G}_2$ in $\textsc{crs}^0$.
  Set $\mathsf{pk}_1 := [u_3]_2$ and $\mathsf{sk}_1 := u_3$.
  Sample $\mathsf{sk}_2 \leftarrow \mathbb{Z}_q$ and set $\mathsf{pk}_2 := [\mathsf{sk}_2]_2$.
  Sample $\mathbf{B} \leftarrow \mathcal{D}_{2,1}$-MDDH and $(k_0, \mathbf{k}_1, \mathsf{k}_2) \leftarrow \mathbb{Z}_q \times \mathbb{Z}_q^n \times \mathbb{Z}_q$.
  Set $\mathbf{p}_1 := \mathbf{M}^\top \mathbf{k}_1$ and $\mathbf{p}_2 := \bar{\mathbf{B}}^\top \mathsf{k}_2$

  Sample $\mathsf{r}_x \leftarrow \mathbb{Z}_q$. Set $x := 0$, $R_x := [\mathsf{r}_x]_2$, and $E_x := [x]_2 + \mathsf{r}_x\, \mathsf{pk}_1$.

  Set $\textsc{crs}_p := (\textsc{crs}^0, \textsc{crs}_p^1, \textsc{crs}_p^2, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1, \mathsf{pk}_1, \mathsf{pk}_2, E_x, R_x)$.
  Set $\textsc{crs}_v := (\textsc{crs}^0, \textsc{crs}_v^1, \textsc{crs}_v^2, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathbf{p}_2]_1, \mathsf{pk}_1, \mathsf{pk}_2, E_x, R_x)$.
  Set $\mathsf{trap} := (\mathbf{k}_1, \mathsf{trap}^2)$.
  Set $\mathbf{c} \leftarrow \mathbb{G}_1^{n-t}$.
  Set $\mathsf{pk} := (\textsc{crs}_v, \mathbf{c})$,  $\mathsf{sk} := (\textsc{crs}_p, \mathsf{trap}, \mathbf{c}, [k_0]_1)$.
  Return $(\mathsf{pk}, \mathsf{sk})$.


$\mathsf{Sign}(\mathsf{sk}, M \in \mathbb{G}_1^t)$:
  Parse $(\textsc{crs}_p, \mathsf{trap}, \mathbf{c}) \leftarrow \mathsf{sk}$, and set $\mathbf{y} := M || \mathbf{c}$.

  Sample $(\mathsf{r}, \mathsf{r}_z) \leftarrow \mathbb{Z}_q \times \mathbb{Z}_q$.
  Set $\rho := [\bar{\mathbf{B}}\mathsf{r}]_1^\top$, $\hat{\rho} := [\underline{\mathbf{B}}\mathsf{r}]_1^\top$, $\gamma := [k_0]_1 + \mathbf{y}^\top \mathbf{k}_1 + \mathsf{r}^\top [\mathsf{p}_2]_1$.

  Set $z := 0$. Compute $R_z := [\mathsf{r}_z]_2$.
  Compute $E_z^i := [z]_2 + \mathsf{r}_z\, \mathsf{pk}_i$ for $i = 1, 2$.
  Set $E_\delta := E_z^1 - E_x$, $R_\delta := R_z - R_x$,  $\mathsf{r}_\delta := \mathsf{r}_x - \mathsf{r}_z$.

  Set $\pi_0 := \mathit{\Pi}_0.\mathsf{prover}(\textsc{crs}^0,\ (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, E_\delta, R_\delta),\ (x, \mathsf{r}_\delta, \hat{x}))$.
  Set $\pi_1 := \mathit{\Pi}_1.\mathsf{prover}(\textsc{crs}_p^1,\ (E_z^1, E_z^2, R_z),\ (0, \mathsf{r}_z))$.
  Set $\pi_2 := \mathit{\Pi}_2.\mathsf{sim}(\textsc{crs}_p^2,\ \mathsf{trap}^2,\ (\mathbf{y}, \rho, \hat{\rho}, \gamma))$.

  Return $\sigma := (\rho, \hat{\rho}, \gamma, E_z^1, E_z^2, R_z, \pi_0, \pi_1, \pi_2)$.


$\mathsf{Verify}(\mathsf{pk}, M, \sigma)$:
  Parse $(\textsc{crs}_v, \mathbf{c}) \leftarrow \mathsf{pk}$, and set $\mathbf{y} := M || \mathbf{c}$.
  Parse $(\rho, \hat{\rho}, \gamma, E_z^1, E_z^2, R_z, \pi_0, \pi_1, \pi_2) \leftarrow \sigma$.

  Check all the NIZK proofs:
    $\mathit{\Pi}_0.\mathsf{ver}(\textsc{crs}^0,\ (\rho, \hat{\rho}, E_\delta, R_\delta),\ \pi_0)$
     and $\mathit{\Pi}_1.\mathsf{ver}(\textsc{crs}_v^1,\ (E_z^1, E_z^2, R_z),\ \pi_1)$
     and $\mathit{\Pi}_2.\mathsf{ver}(\textsc{crs}_v^2,\ (\mathbf{y}, \rho, \hat{\rho}, \gamma),\ \pi_2)$.
```

Languages:

$\mathit{\Pi}_0$ is a NIZK proof for OR-language $L_0 \overset{\text{def}}{=} \{(\rho, \hat{\rho}, E_\delta, R_\delta) \mid \exists x, \mathsf{r}_\delta, \hat{x} \in \mathbb{Z}_q : x\,\hat{\rho} - \hat{x}\,[\underline{\mathbf{B}}]_1 = [0]_1 \textbf{ and } \hat{x}\,[1]_1 - x\,\rho = [0]_1 \textbf{ and } (E_\delta, R_\delta) = \mathrm{com}_2(x; \mathsf{r}_\delta)\}$ by Escala-Groth proof system for multi scalar multiplication equations.

$\mathit{\Pi}_1$ is a QA-NIZK for linear language $L_1 \overset{\text{def}}{=} \{(E_z^1, E_z^2, R_z) \mid \exists (z, \mathsf{r}_z) : E_z^1 := [z]_2 + \mathsf{r}_z\,\mathsf{pk}_1 \textbf{ and } E_z^2 := [z]_2 + \mathsf{r}_z\,\mathsf{pk}_2\}$ with parameters $(\mathsf{pk}_1, \mathsf{pk}_2)$.

$\mathit{\Pi}_2$ is a split-CRS QA-NIZK for affine language $L_2 \overset{\text{def}}{=} \{(\mathbf{y}, \rho, \hat{\rho}, \gamma) \mid \exists (\mathbf{x}, \mathsf{r}) : \mathbf{y} = [\mathbf{M}\mathbf{x}]_1 \textbf{ and } \rho = [\bar{\mathbf{B}}\mathsf{r}]_1^\top \textbf{ and } \hat{\rho} = [\underline{\mathbf{B}}\mathsf{r}]_1^\top \textbf{ and } \gamma = [k_0]_1 + \mathbf{x}^\top [\mathbf{p}_1]_1 + \mathsf{r}^\top [\mathsf{p}_2]_1\}$ with parameters $([\mathbf{M}]_1, [\mathbf{B}]_1, [\mathbf{p}_1]_1, [\mathsf{p}_2]_1, [k_0]_1)$.

Fig. 7. An SPS constructed directly by using the customized USS-QA-NIZK with designated prover (in Section 4.2) with optimizations from Section 3.2.

$\mathbb{G}_1^2 \times \mathbb{G}_2$. The signer signs to (c, d) by $\sigma \leftarrow \mathsf{SIG.Sign}(sk, (c, d))$ where $\sigma := (\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, \mathsf{ct}_z^1, \mathsf{ct}_z^2, \pi_0, \pi_1, \pi_2) \in \mathbb{G}_1^6 \times \mathbb{G}_2^6$.

– Given σ, the user computes GS-proofs as follows:
  - For correctness of commitment, prove pairing product equations

$$e(c/m, \tilde{g}) = e(f, z), \quad \text{and} \quad e(d, \tilde{g}) = e(g, z)$$

    where (c, d, z) is a witness. It yields GS-commitments and proofs consisting of $(4, 2)$ and $(8, 8)$ elements, respectively.
  - For correctness of σ, prove the equation for verifying π_0 with $(\pi_0, \boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \mathsf{ct}_z^1 - \mathsf{ct}_x)$ as a witness. Since it consists of four non-linear equations that verify the first two relations in $\mathcal{L}_1$ of Section 4.2, the proof consists of $4 \times (4, 4)$ elements. Also prove a linear equation for verifying π_1 with $(\pi_1, \mathsf{ct}_z^1, \mathsf{ct}_z^2)$ as a witness. (The equation is obtained by applying the optimization on the ElGamal encryption in L_1 in Figure **??**.) This part yields a GS-proof consisting of $(2, 0)$ elements. Further prove equations for verifying π_2 with $(\boldsymbol{\rho}, \hat{\boldsymbol{\rho}}, \gamma, c, d)$ as a witness. This part yields a GS-proof consisting of $(0, 2)$ elements. The GS-commitments of the witnesses for these proofs require $(12, 12)$ elements. (Note that c and d are already counted in the previous step.)

  Summing up, the resulting blind signature σ_{bs} consists of $|\sigma_{bs}| = (4, 2) + (8, 8) + 4 \times (4, 4) + (2, 0) + (0, 2) + (12, 12) = (42, 40)$ elements.

– Given (σ_{bs}, m), a verifier verifies all proofs in σ_{bs}.

In the literature, there are round optimal blind signature schemes in the common reference string model without random oracles or generic groups [FHS15] or complexity leveraging [GRS$^+$11,GG14] whose signatures consist of about 30 elements [Fuc09,AO09b]. However, they rely on so-called q-type assumptions.

5.4 Tightly-secure Group Signature Scheme with Concurrent Join

In [KY05], a generic construction of CPA-anonymous group signature scheme using a signature scheme and a NIZK proof is shown. CCA-anonymity is achieved in [Gro07] by additionally using selective-tag CCA-secure encryption and a strongly unforgeable one-time signature scheme. In [AFG$^+$16], a scheme that allows concurrent joining of members is constructed by using structure-preserving signatures. The latest work in [LPY15] enjoys compact signature size using QA-NIZK and structure-preserving signatures but the security reduction is not tight.

We instantiate a generic construction of CCA-anonymous group signature scheme in [Gro07,AFG$^+$16] using tightly secure structure-preserving signature scheme SIG from Section 5.2, tagged CCA-secure public-key encrypiton scheme TBE from Section 5.1, the Groth-Sahai proof system GS from [GS12], and a one-time signature scheme OTS from [ACIK10] all in the SXDH setting. This results in the first tightly CCA-secure group signature scheme. Note that our goal is not structure-preserving one. Indeed, the tag-based encryption allows binary strings as a tag (yet it is compatible with the Groth-Sahai proof system for correctness proof), and we use OTS in combination with a collision resistant hash function to deal with long messages. Let us briefly review OTS. One-time secret key consists of k_1, k_2, s_1, s_2 in $\mathbb{Z}_q$ and one-time verification key is $([s_1]_1, [s_2]_1, [s_1 k_1 + s_2 k_2]_1)$. For a (hashed) message $m \in \mathbb{Z}_q$, a one-time signature is $(z_1, z_2) \in \mathbb{Z}_q$ that satisfies $s_1 k_1 + s_2 k_2 = m + s_1 z_1 + s_2 z_2$. The signature is valid if $m[1]_1 + z_1[s_1]_1 + z_2[s_2]_1 = [s_1 k_1 + s_2 k_2]_1$. In [ACIK10], it is shown that the scheme is one-time chosen message unforgeable under the discrete logarithm assumption in $\mathbb{G}_1$ and the security reduction is tight (by factor of 2). Due to the random self-reducibility of the discrete logarithm problem in $\mathbb{G}_1$, the tightness of the reduction retains in multi-challenge setting where multiple one-time keys are challenged.

We sketch the construction as follows.

- The group manager generates a key pair (v_c, s_c) of SIG and $\textsc{crs}$ of GS. The parameter is set so that it can sign bilateral messages consisting of $(9, 12)$ elements.
- The opening manager generates a key pair (e, d) of TBE.
- To join the group, a member generates a key pair (v_u, s_u) of SIG so that it can sign messages consisting of two elements in $\mathbb{G}_1$. This results in v_u consisting of $(9, 12)$ elements. He then asks the group manager to certify v_u. The group manager rejects if v_u is not unique among all keys registered so far. Otherwise, the manager signs to v_u with v_c and return the certificate σ_c to the user. The certificate consists of $(7, 8)$ elements.
- To sign message m, the member first generates a one-time key pair (v_o, s_o) of OTS and signs on one-timekey v_o. The resulting signature σ_u consists of two elements in $\mathbb{G}_1$ by using SIG with s_u. Next he encrypts σ_u and v_u by using TBE with encryption key e and v_o as a tag obtaining a ciphertext ψ. He then creates a proof π for his possession of correct certificate σ_c and signature σ_u, and correctness of the encryption without revealing σ_c, v_u, and σ_u. Finally, he uses OTS with s_o to obtain one-time signature σ_m on message (m, v_o, π, ψ) and outputs $\sigma_g := (v_o, \pi, \psi)$ as a group signature.
- A verifier receiving m and σ_g accepts if π is verified.
- To open a signature, the opening manager decrypts ψ with d and verifies obtained σ_u and v_u with respect to message m.

The opening manager may also convince a verifier, known as a judge, by using standard means such as issuing a Groth-Sahai NIZK proof of correct decryption using other independent crs.

For formal security notions, we refer to [Gro07]. Tightness of CCA-anonymity holds directly from tightness of CCA-security of TBE under the multi-user and multi-challenge setting. Tightness in terms of traceability is due to multi-challenge tight security of OTS and SIG.

With the above mentioned building blocks, a group signature will consist of more than seven hundreds of group elements. A large part of the signature elements comes from encryption of public-key v_u and signature σ_u to the one-time key and related proofs. They can be reduced by encrypting an element in v_u instead of encrypting whole v_u and consider the element as a fingerprint of v_u by letting the group manager verify its uniqueness at the time of registration. This will save several hundreds of elements in a group signature. Yet the signature size will be far larger than non-tight schemes and we have to look this result as a feasibility proof.

5.5 (Almost) Tight Simulation-Sound Groth-Sahai NIZK

Camenisch, Chandran and Shoup [CCS09] gave a generic scheme for unbounded simulation-sound Gorth-Sahai NIZK proofs based on a strong one-time signature scheme and a labeled CCA2-secure public-key encryption scheme. The construction also needs a NIZK system for algebraic "OR" statements, which can itself be proved using (standard) Groth-Sahai NIZK proofs. Finally, the security proof is also based on the CDH assumption in one of the groups of the bilinear pairing group (which is implied tightly by $\mathcal{D}_k$-MDDH). The security reduction to the hardness of CDH, the one-time signature scheme, and the multi-challenge CCA2-security of the public key encryption scheme are tight. Thus, using the (almost) tightly-secure multi-challenge CCA2-secure public-key encryption scheme of Section 5.1, and the tightly-secure one-time signature scheme of [ACD$^+$16], we get an (almost) tightly-secure USS-NIZK for algebraic languages considered in [GS12].

References

[AAO18] Masayuki Abe, Miguel Ambrona, and Miyako Ohkubo. Simulation-sound NIZK and (almost) signature schemes, 2018. Unpublished manuscript.

[ABP15] Michel Abdalla, Fabrice Benhamouda, and David Pointcheval. Disjunctions for hash proof systems: New constructions and applications. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 69–100, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

[ACD$^+$12] Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 4–24, Beijing, China, December 2–6, 2012. Springer, Heidelberg, Germany.

[ACD$^+$16] Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. *Journal of Cryptology*, 29(4):833–878, October 2016.

[ACIK10] Masayuki Abe, Yang Cui, Hideki Imai, and Eike Kiltz. Efficient hybrid encryption from id-based encryption. *Des. Codes Cryptography*, 54(3):205–240, 2010.

[AFG$^+$10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *Advances in Cryptology –*

CRYPTO 2010, volume 6223 of *Lecture Notes in Computer Science*, pages 209–236, Santa Barbara, CA, USA, August 15–19, 2010. Springer, Heidelberg, Germany.

[AFG+16] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. *Journal of Cryptology*, 29(2):363–421, April 2016.

[AHN+17] Masayuki Abe, Dennis Hofheinz, Ryo Nishimaki, Miyako Ohkubo, and Jiaxin Pan. Compact structure-preserving signatures with almost tight security. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 548–580, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany.

[AHO10] Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010. http://eprint.iacr.org/2010/133.

[AJOR18] Masayuki Abe, Charanjit S. Jutla, Miyako Ohkubo, and Arnab Roy. Improved (almost) tightly-secure simulation-sound QA-NIZK with applications. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 627–656, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Heidelberg, Germany.

[AO09a] Masayuki Abe and Miyako Ohkubo. A framework for universally composable non-committing blind signatures. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 435–450, Tokyo, Japan, December 6–10, 2009. Springer, Heidelberg, Germany.

[AO09b] Masayuki Abe and Miyako Ohkubo. A framework for universally composable non-committing blind signatures. Cryptology ePrint Archive, Report 2009/494, 2009. http://eprint.iacr.org/2009/494.

[BBM00] Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 259–274, Bruges, Belgium, May 14–18, 2000. Springer, Heidelberg, Germany.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

[CCS09] Jan Camenisch, Nishanth Chandran, and Victor Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In Antoine Joux, editor, *Advances in Cryptology – EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 351–368, Cologne, Germany, April 26–30, 2009. Springer, Heidelberg, Germany.

[CLY09] Julien Cathalo, Benoît Libert, and Moti Yung. Group encryption: Non-interactive realization in the standard model. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 179–196, Tokyo, Japan, December 6–10, 2009. Springer, Heidelberg, Germany.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO'98*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25, Santa Barbara, CA, USA, August 23–27, 1998. Springer, Heidelberg, Germany.

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64, Amsterdam, The Netherlands, April 28 – May 2, 2002. Springer, Heidelberg, Germany.

[CW13] Jie Chen and Hoeteck Wee. Fully, (almost) tightly secure IBE and dual system groups. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 435–460, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[EG14] Alex Escala and Jens Groth. Fine-tuning Groth-Sahai proofs. In Hugo Krawczyk, editor, *PKC 2014: 17th International Conference on Theory and Practice of Public Key Cryptography*, volume 8383 of *Lecture Notes in Computer Science*, pages 630–649, Buenos Aires, Argentina, March 26–28, 2014. Springer, Heidelberg, Germany.

[EHK$^+$13] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 129–147, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[ElG84] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18, Santa Barbara, CA, USA, August 19–23, 1984. Springer, Heidelberg, Germany.

[ES02] Edith Elkind and Amit Sahai. A unified methodology for constructing public-key encryption schemes secure against adaptive chosen-ciphertext attack. Cryptology ePrint Archive, Report 2002/042, 2002. http://eprint.iacr.org/2002/042.

[FHS15] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 233–253, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[Fis06] Marc Fischlin. Round-optimal composable blind signatures in the common reference string model. In Cynthia Dwork, editor, *Advances in Cryptology – CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 60–77, Santa Barbara, CA, USA, August 20–24, 2006. Springer, Heidelberg, Germany.

[FLM11] Marc Fischlin, Benoît Libert, and Mark Manulis. Non-interactive and reusable universally composable string commitments with adaptive security. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 468–485, Seoul, South Korea, December 4–8, 2011. Springer, Heidelberg, Germany.

[Fuc09] Georg Fuchsbauer. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. Cryptology ePrint Archive, Report 2009/320, 2009. http://eprint.iacr.org/2009/320.

[GG14] Sanjam Garg and Divya Gupta. Efficient round optimal blind signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 477–495, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany.

[GHK17] Romain Gay, Dennis Hofheinz, and Lisa Kohl. Kurosawa-desmedt meets tight security. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 133–160, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany.

[GHKP18] Romain Gay, Dennis Hofheinz, Lisa Kohl, and Jiaxin Pan. More efficient (almost) tightly secure structure-preserving signatures. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 230–258, Tel Aviv, Israel, April 29 – May 3, 2018. Springer, Heidelberg, Germany.

[GHKW16] Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. Tightly CCA-secure encryption without pairings. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 1–27, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany.

[Gro07] Jens Groth. Fully anonymous group signatures without random oracles. In Kaoru Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 164–180, Kuching, Malaysia, December 2–6, 2007. Springer, Heidelberg, Germany.

[GRS$^+$11] Sanjam Garg, Vanishree Rao, Amit Sahai, Dominique Schröder, and Dominique Unruh. Round optimal blind signatures. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 630–648, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany.

[GS12] Jens Groth and Amit Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM J. Comput.*, 41(5):1193–1232, 2012.

[Har11] Kristiyan Haralambiev. *Efficient cryptographic primitives for non-interactive zero-knowledge proofs and applications*. PhD thesis, New York University, 2011.

[HJ12] Dennis Hofheinz and Tibor Jager. Tightly secure signatures and public-key encryption. In *Crypto*, volume 7417, pages 590–607. Springer, 2012.

[Hof17] Dennis Hofheinz. Adaptive partitioning. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 489–518, Paris, France, April 30 – May 4, 2017. Springer, Heidelberg, Germany.

[JOR18] Charanjit S. Jutla, Miyako Ohkubo, and Arnab Roy. Improved (almost) tightly-secure structure-preserving signatures. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018: 21st International Conference on Theory* *and Practice of Public Key Cryptography, Part II*, volume 10770 of *Lecture Notes in Computer Science*, pages 123–152, Rio de Janeiro, Brazil, March 25–29, 2018. Springer, Heidelberg, Germany.

[JR13] Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology – ASIACRYPT 2013, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 1–20, Bengalore, India, December 1–5, 2013. Springer, Heidelberg, Germany.

[JR14] Charanjit S. Jutla and Arnab Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014, Part II*, volume 8617 of *Lecture Notes in Computer Science*, pages 295–312, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Heidelberg, Germany.

[JR15] Charanjit S. Jutla and Arnab Roy. Dual-system simulation-soundness with applications to UC-PAKE and more. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 630–655, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

[JR16] Charanjit Jutla and Arnab Roy. Smooth NIZK arguments with applications to asymmetric UC-PAKE. Cryptology ePrint Archive, Report 2016/233, 2016. http://eprint.iacr.org/2016/233.

[JR17] Charanjit S. Jutla and Arnab Roy. Improved structure preserving signatures under standard bilinear assumptions. In Serge Fehr, editor, *PKC 2017: 20th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 10175 of *Lecture Notes in Computer Science*, pages 183–209, Amsterdam, The Netherlands, March 28–31, 2017. Springer, Heidelberg, Germany.

[KPW15] Eike Kiltz, Jiaxin Pan, and Hoeteck Wee. Structure-preserving signatures from standard assumptions, revisited. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 275–295, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[KW15] Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 101–128, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

[KY05] Aggelos Kiayias and Moti Yung. Group signatures with efficient concurrent join. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 198–214, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.

[LPJY14] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 514–532, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany.

[LPJY15] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Compactly hiding linear spans - tightly secure constant-size simulation-sound QA-NIZK proofs and applications. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 681–707, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

[LPY15] Benoît Libert, Thomas Peters, and Moti Yung. Short group signatures via structure-preserving signatures: Standard model security from simple assumptions. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 296–316, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[Ràf15] Carla Ràfols. Stretching groth-sahai: NIZK proofs of partial satisfiability. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015: 12th Theory of Cryptography Conference, Part II*, volume 9015 of *Lecture Notes in Computer Science*, pages 247–276, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany.

[Wat09] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636, Santa Barbara, CA, USA, August 16–20, 2009. Springer, Heidelberg, Germany.

A Proof of Lemma 1

To prove Lemma 1, we go through a series of L games, each of which has several sub-games. Without loss of generality, we will assume that the total number of queries is a power of two ($\leq 2^L$). We will identify $\mathbf{G}_2$ with $\mathbf{G}_{2,1,0}$ and $\mathbf{G}_3$ with $\mathbf{G}_{2,L,10}$. These games are summarized in Figure 8 with a table of transitions given in Figure 10.

In the following games, we will consider a sequence of functions $\textsc{rf}_j$, for $j \in [0, L]$, where $\textsc{rf}_j$ maps $\{0,1\}^j$ to $\mathbb{Z}_q$. Define $\textsc{rf}_0(\epsilon) = k_0$, where ϵ denotes the empty string.

Game $\mathbf{G}_{2,j,0}$: The challenger also lazily defines a function $\textsc{rf}_{j-1}$ which is random everywhere and independent for each input. For all simulator responses i, let $i|_{j-1}$ be the $(j-1)$-length prefix of i. We generate γ^i as $\mathbf{y}^{i\top}\mathbf{k}_1$ + $[\textsc{rf}_{j-1}(i|_{j-1})]_1$ + $\boldsymbol{\rho}^i\mathbf{k}_2$. Further, the set $\mathcal{Z}$ is defined to be $\bigcup_i\{\textsc{rf}_{j-1}(i|_{j-1})\}$, where i ranges over the query indices.

In the base case, i.e., when $j = 1$, $\mathbf{G}_{2,j,0}$ is indeed the same as $\mathbf{G}_2$ by definition of $\textsc{rf}_0(\epsilon)$ and definition of $\mathcal{Z}$ in $\mathbf{G}_2$. For the inductive case, we defer the proof of equivalence of $\mathbf{G}_{2,j,0}$ and $\mathbf{G}_{2,j-1,10}$ till the description of the latter game.

We will maintain the induction hypothesis (over $j \in [1, L]$) that the function $\textsc{rf}_{j-1}$ is a random function from $\{0,1\}^{j-1}$ to $\mathbb{Z}_q$. Clearly, the induction hypothesis holds for the base case.

Game $\mathbf{G}_{2,j,1}$: We also sample $(\mathbf{k}_2, \mathbf{k}'_2) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k$ and substitute $\mathbf{p}_2 = \bar{\mathbf{B}}^\top\mathbf{k}_2$ with $\bar{\mathbf{B}}^\top\mathbf{k}_2 + \underline{\mathbf{B}}^\top\mathbf{k}'_2$, which has the same distribution $\mathcal{U}(\mathbb{Z}_q^k)$. Consequently, we

```
                  $\mathsf{crssim}()$ : $\cdots$
       Games (2,j,3-7)   $\text{CRS}^0 \leftarrow \mathit{\Pi}_0.\mathsf{crsgen}()$
  Games (2,j,0-2,8-10)   $(\text{CRS}^0, \mathsf{trap}^0) \leftarrow \mathit{\Pi}_0.\mathsf{crssim}()$

                         Sample $\beta \leftarrow \{0,1\}$ and $\mathbf{r}_x \leftarrow \mathbb{Z}_q^k$
    Games (2,j,0-2,10)   Set $x := 0$
       Games (2,j,3-9)   Set $x := 1 - \beta$
       Games (2,j,3-7)   $\mathsf{ct}_x = \mathsf{PKE.Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$
  Games (2,j,0-2,8-10)   $\mathsf{ct}_x = \mathsf{PKE.Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)$

    Games (2,j,0,7-10)   Sample $\mathbf{k}_2 \leftarrow \mathbb{Z}_q^k$
       Games (2,j,1-6)   Sample $(\mathbf{k}_2,\ \mathbf{k}_2') \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k$
                         $\cdots$
```

```
        $\mathsf{sim}(\mathbf{y}^i \in \mathbb{G}_1^n)$ : $\cdots$
        Game (2,j,0,10)  Set $z^i := 0$
        Games (2,j,1-9)  Set $z^i := i_j$
        Games (2,j,3-7)  Set $\mathsf{ct}_z^{1i} := \mathsf{PKE.Enc}(\mathsf{pk}_1, z^i; \mathbf{r}_z^i)$
   Games (2,j,0-2,8-10)  Set $\mathsf{ct}_z^{1i} := \mathsf{PKE.Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^i)$

                         Set $(\hat{\boldsymbol{\rho}}^{i\top}, \gamma^i) :=$
          Games (2,j,0)      $([\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [\text{RF}_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$
        Games (2,j,1-4)      $\left([\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [\text{RF}_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'\right)$
        Games (2,j,5-6)      $\left([\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + \begin{bmatrix}\text{RF}_{j-1}(i|_{j-1}),\ \text{if } (i_j = \beta) \\ \text{RF}'_{j-1}(i|_{j-1}),\ \text{if } (i_j \neq \beta)\end{bmatrix}_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'\right)$
       Games (2,j,7-10)      $([\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [\text{RF}_j(i|_j)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$
                         $\cdots$
```

```
                $\mathsf{WIN} \overset{\text{def}}{=}$
        Games (2,j,2-8)     if ($\mathsf{ChkAbort}$) return false; else
                            $\pi^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \mathsf{ct}_z^{1*}, \mathsf{ct}_z^{2*}, \mathsf{ct}_v^*, \pi_0^*, \pi_1^*, \pi_2^*, \pi_3^*)$ :
                              $(\mathbf{y}^* \notin \{\mathbf{y}^i\}_i \cup \text{span}([\mathbf{M}]_1))$ and $\mathsf{ver}(\text{CRS}_v,\ \mathbf{y}^*,\ \pi^*)$
     Games (2,j,0,7-10)       and $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$
        Games (2,j,1-6)       and $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$
   Games (2,j,0-3,6-10)       and $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \text{span}([\mathbf{B}]_1)$
```

Fig. 8. Going from Game 2 to 3

change the winning condition's γ^*-test conjunct to $\gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$, which is same as the earlier winning condition as that condition also has the conjunct $(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$. Also set z^i equal to i_j.

The difference in advantage is the $\mathsf{IND\text{-}mCPA}$ security of the PKE scheme, in switching all the z^i plaintexts. Rest of the changes are information theoretic as x is committed with a simulated CRS and $\mathbf{p}_2$ has the same distribution.

Game $\mathbf{G}_{2,j,2}$: In this game, the challenger samples $\beta \leftarrow \{0,1\}$. In the winning condition we introduce a predicate called $\mathsf{ChkAbort}$ which behaves as follows: it returns true and forces the adversary to lose outright if the decryption of ct_z^{2*} is zero or one and equals β. In the case that decryption of ct_z^{2*} is not zero or one, then it still forces the adversary to lose at random with probability half. If the $\mathsf{ChkAbort}$ predicate does not force a loss for the adversary, then the rest of the winning condition remains the same as the previous game.

Since β is information theoretically hidden from the adversary, the adversary's advantage goes down by exactly a factor of 2.

Game $\mathbf{G}_{2,j,3}$: The challenger sets $x = 1 - \beta$. It goes back to the binding-CRS for Π_0. Thus, z^i as set above is used in the encryption ct_z^{1i} to z^i. Since $(\boldsymbol{\rho}^i\|\hat{\boldsymbol{\rho}}^i)^\top \in \mathrm{span}([\mathbf{B}]_1)$ for all i, a correct proof can be generated by Π_0.

The difference in the adversary's advantage is at most $\mathrm{ADV}^{\mathsf{zk}}_{\Pi_0}$.

Game $\mathbf{G}_{2,j,4}$: The challenger removes the conjunct $(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ from the winning condition.

We first check that QA-NIZK Π_1 is in true-simulation mode, i.e., the simulator for this QA-NIZK is only issuing simulated proofs on true statements. This is true since both the ciphertexts ct_z^{1i} and ct_z^{2i} encrypt the same z^i. Now, since $\mathsf{dec}(\mathsf{ct}_z^{2*}) \neq x$ is in the scope of this removed conjunct, by true-simulation soundness of Π_2, $z^* \neq x$ is also in the scope of the removed conjunct. This implies by the soundness of the NIZK that $(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$. Thus this conjunct is indeed redundant and can be removed. The difference in advantage is at most $\mathrm{ADV}^{\mathsf{tss}}_{\Pi_1}$.

Game $\mathbf{G}_{2,j,5}$: We change the computation of γ^i from

$$\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$$

to

$$\mathbf{y}^{i\top}\mathbf{k}_1 + \begin{bmatrix}\mathrm{RF}_{j-1}(i|_{j-1}), \text{ if } (i_j = \beta)\\ \mathrm{RF}'_{j-1}(i|_{j-1}), \text{ if } (i_j \neq \beta)\end{bmatrix}_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2.$$

Here RF'_{j-1} is another independent random function from $(j-1)$-bit strings to $\mathbb{Z}_q$.

Lemma 2. $|\Pr_{2,j,4}[\mathsf{WIN}_{2,j,4}] - \Pr_{2,j,5}[\mathsf{WIN}_{2,j,5}]| \leq$

$$4 \cdot \mathrm{ADV}^{\mathsf{tss}}_{\Pi_1} + 4 \cdot \mathrm{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}} + 4 \cdot \mathrm{ADV}^{\mathsf{zk}}_{\Pi_0} + \frac{3}{q}$$

We prove this lemma in Appendix B using another sequence of hybrid games.

Game $\mathbf{G}_{2,j,6}$: We now start rolling the games back. In this game we add back the condition $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ into the winning condition.

Since $z^* \neq x$ in the scope of this clause, the difference in advantage is $\textsc{adv}^{\mathsf{tss}}_{\Pi_1}$ due to the true-simulation soundness of the QA-NIZK and the perfect soundness of OR-NIZK Π_0.

Game $\mathbf{G}_{2,j,7}$: The challenger (lazily) defines $\textsc{rf}_j$ as follows:

$$\textsc{rf}_j(i|_j) \overset{\text{def}}{=} \left\{ \begin{matrix} \textsc{rf}_{j-1}(i|_{j-1}), \text{ if } (i_j = \beta) \\ \textsc{rf}'_{j-1}(i|_{j-1}), \text{ if } (i_j \neq \beta) \end{matrix} \right\}$$

Since $\textsc{rf}'$ is random and independent of $\textsc{rf}$, the induction hypothesis related to $\textsc{rf}$ continues to hold.

The challenger also goes back to sampling $\mathbf{p}_2$ as $\bar{\mathbf{B}}^\top \mathbf{k}_2$, instead of as $\bar{\mathbf{B}}^\top \mathbf{k}_2 + \underline{\mathbf{B}}\mathbf{k}'_2$. γ^i is now computed as $(\mathbf{y}^{i\top}\mathbf{k}_1 + [\textsc{rf}_j(i|_j)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2)$. It also changes the winning condition γ^*-conjunct to $\gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + \boldsymbol{\rho}^*\mathbf{k}_1$, which holds as $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$. Further, instead of defining $\mathcal{Z}$ as union of $\textsc{rf}_{j-1}(i|_{j-1})$, the set $\mathcal{Z}$ is now defined as $\bigcup_i \{\textsc{rf}_j(i|_j)\}$.

Changes in this game are statistically indistinguishable from the previous, except for the change in the definition of $\mathcal{Z}$. Since we assumed w.l.o.g. that the number of queries is a power of two, the set $\bigcup_i \{i|_{j-1}\}$ is same as the set $\bigcup_i \{i|_{j-1} \mid i_j = \beta\}$. Thus, by definition of $\textsc{rf}_j$ above, the new set $\mathcal{Z}$ is a superset of the previous set $\mathcal{Z}$. Hence, the adversary's advantage in this game can only be higher than its advantage in the previous game.

Game $\mathbf{G}_{2,j,8}$: The challenger goes back to generating the simulated CRS for the OR-NIZK Π_0 and the proofs are now generated using $(\mathbf{r}^i, 0, 0, 0)$. Further, ct_x and ct_z^{1i}'s are all set to encryptions of 0.

The difference in adversary's advantage is at most $\textsc{adv}^{\mathsf{zk}}_{\Pi_0} + \textsc{adv}^{\mathsf{mcpa}}_{\mathsf{PKE}}$.

Game $\mathbf{G}_{2,j,9}$: In the winning condition, we remove the $\mathsf{ChkAbort}$ disjunct where the adversary lost outright in the previous games, i.e., if the decryption of ct_z^{2*} was 0/1 and equaled β, or with probability half if the decryption was non-0/1.

Since β is information theoretically hidden from the adversary, the adversary's advantage goes up by exactly a factor of 2.

Game $\mathbf{G}_{2,j,10}$: The challenger sets $z^i = 0$, and sets the two encryption of z^i correctly. It also sets x back to 1.

The difference in adversary's advantage is the $\mathsf{IND\text{-}mCPA}$ security of the two PKE's, in switching all the z^i plaintexts and x.

We now observe that game $\mathbf{G}_{2,j,10}$ is same as $\mathbf{G}_{2,j+1,0}$ for $j < L$ and same as $\mathbf{G}_3$ for $j = L$. This concludes our proof.

B Proof of Lemma 2

The various hybrid games to prove this lemma are depicted in Figure 9 with a table of transitions given in Figure 11.

Game $\mathbf{H}_0$: Game $\mathbf{H}_0$ is same as the game $\mathbf{G}_{2,j,4}$.

Game $\mathbf{H}_1$: In this game, the challenger generates the OR-NIZK Π_0 CRS as a simulated CRS. Further, for each query i, if i_j is not equal to β, then instead of just picking $\mathbf{r}^i$, the challenger picks $\mathbf{r}_1^i$ and $\mathbf{r}_2^i$ at random, and sets $\mathbf{r}^i = \mathbf{r}_1^i + \mathbf{r}_2^i$. Further, it sets $\boldsymbol{\rho}^i = [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$, $\hat{\boldsymbol{\rho}}^i = [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top$, and a similar change in the generation of γ^i.

By the zero-knowledge property of OR-NIZK Π_0, and since rest of the game is statistically the same as the previous game, the adversary's advantage of winning is at most $\text{ADV}_{\Pi_0}^{\mathsf{zk}}$.

Game $\mathbf{H}_2$: In this game, the adversary also samples $\underline{\mathbf{B}}' \leftarrow \mathbb{Z}_q^{1\times k}$. Next, for each query i, if i_j is not equal to β, then the challenger picks $\mathbf{r}_1^i$ and $\mathbf{r}_2^i$ at random, and sets $\mathbf{r}^i = \mathbf{r}_1^i + \mathbf{r}_2^i$. Then it sets $\boldsymbol{\rho}^i = [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$, $\hat{\boldsymbol{\rho}}^i = [\underline{\mathbf{B}}\mathbf{r}_1^i + \underline{\mathbf{B}}'\mathbf{r}_2^i]_1^\top$ and a similar change in generation of γ^i (see Figure 9).

We now prove that the absolute value of the difference of the advantage in adversary's winning probability in $\mathbf{H}_2$ and $\mathbf{H}_1$ is at most the maximum advantage of winning in a $\mathcal{D}_{2k,k}$-MDDH game. In other words,

$$|\Pr_{\mathbf{H}_2}(\mathsf{WIN}_{\mathbf{H}_2}) - \Pr_{\mathbf{H}_1}(\mathsf{WIN}_{\mathbf{H}_1})| \le \text{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}}.$$

To this end, for each Adversary $\mathcal{A}$ playing against the challenger in games $\mathbf{H}_1$ and $\mathbf{H}_2$, we will build another adversary $\mathcal{B}$ that plays against the $\mathcal{D}_{2k,k}$-MDDH challenge. Say, the adversary $\mathcal{B}$ receives an $\mathcal{D}_{2k,k}$-MDDH challenge $([\mathbf{B}]_1, [\bar{\mathbf{B}}\mathbf{w}]_1, [\mathbf{v}]_1)$, all elements in $\mathbb{G}_1$, where either $\mathbf{v}$ is a real $\mathcal{D}_{2k,k}$-MDDH vector, i.e., $\mathbf{v} = \underline{\mathbf{B}}\mathbf{w}$ or $\mathbf{v}$ is a fake $\mathcal{D}_{2k,k}$-MDDH vector, i.e., is random and independent of the other components. First we extend this to k independent $\mathcal{D}_{2k,k}$-MDDH challenges by random self-reducibility [EHK$^+$13]: Sample $(\mathbf{e}, \mathbf{F}) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^{k\times k}$ and set $\mathbf{W} := \mathbf{w}\mathbf{e}^\top + \mathbf{F}$ and $\mathbf{V} := \mathbf{v}\mathbf{e}^\top + \underline{\mathbf{B}}\mathbf{F}$. Observe that $\mathbf{W}$ is uniformly distributed and that $([\mathbf{B}]_1, [\bar{\mathbf{B}}\mathbf{W}]_1, [\mathbf{V}]_1)$ provides k independent $\mathcal{D}_{2k,k}$-MDDH challenges.

Adversary $\mathcal{B}$ next emulates the challenger $\mathcal{C}$ against $\mathcal{A}$ as follows. It starts emulating $\mathcal{C}$ by letting the first element of the challenge being the group generator for $\mathbb{G}_1$. Next, it emulates rest of $\mathcal{C}$ perfectly, except for queries i where i_j is not equal to β. In this case, it picks $(\mathbf{r}_1^i, \mathbf{r}_2^i) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k$, and sets $\boldsymbol{\rho}^i = [\bar{\mathbf{B}}\mathbf{r}_1^i + \bar{\mathbf{B}}\mathbf{W}\mathbf{r}_2^i]_1^\top$ and $\hat{\boldsymbol{\rho}}^i = [\underline{\mathbf{B}}\mathbf{r}_1^i + \mathbf{V}\mathbf{r}_2^i]_1^\top$. It does not need to set $\mathbf{r}^i$'s, as these quantities are only needed in the OR-NIZK Π_0 proof, but in game $\mathbf{H}_1$ we switched to the simulation setting. The quantity γ^i is also generated using the just defined $\boldsymbol{\rho}^i$ and $\hat{\boldsymbol{\rho}}^i$ (as well as $\mathbf{k}_2$ and $\mathbf{k}_2'$). Also, the public key includes $\mathbf{B}$, which is just replicated from the $\mathcal{D}_{2k,k}$-MDDH challenge.

Now, it is easy to check that if the $\mathcal{D}_{2k,k}$-MDDH challenge was real, then $\mathcal{B}$ emulated game $\mathbf{H}_1$ to $\mathcal{A}$, and if the $\mathcal{D}_{2k,k}$-MDDH challenge was fake, then $\mathcal{B}$

emulated $\mathbf{H}_2$ to $\mathcal{A}$. Essentially, $\mathbf{r}_2^i$ is simulated by $\mathbf{W}\mathbf{r}_2^i$ and $\underline{\mathbf{B}}'$ is simulated by $\mathbf{V}^\top\mathbf{W}^{-1}$ in Game $\mathbf{H}_2$. This proves the claim above.

Game $\mathbf{H}_3$: In this game, the Challenger goes back to generating the OR-NIZK Π_0 CRS using the binding CRS generator. It also generates all the proofs using real witnesses, i.e., $(\mathbf{r}^i, 0, 0, 0)$ or $(0, 1-\beta, \mathbf{r}_z^{1i}, \mathbf{r}_x)$. it also re-introduces the conjunct $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ in the winning condition.

We now show that the adversary's advantage in winning in $\mathbf{H}_3$ is different from its advantage in winning in game $\mathbf{H}_2$ by

$$\textsc{adv}_{\Pi_1}^{\mathsf{tss}} + \textsc{adv}_{\Pi_0}^{\mathsf{zk}}.$$

We first prove that the real witnesses satisfy the language L_0. Indeed, if $z_j^i = i_j$ is equal to $\beta = 1 - x$, i.e., $z_j^i \neq x$, then the challenger generated $(\boldsymbol{\rho}^i \| \hat{\boldsymbol{\rho}}^i)^\top \in \mathrm{span}([\mathbf{B}]_1)$, thus the disjunction holds. On the other hand, if $z_j^i = x$ then the disjunction also holds. Thus, by zero-knowledge, the adversary's advantage in distinguishing between the two games is at most $\textsc{adv}_{\Pi_0}^{\mathsf{zk}}$.

Next, we prove that the other conjuncts in the winning condition already imply $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$. To ascertain this, we must first check that the QA-NIZK Π_1 is in true-simulation mode, which is true as the challenger does encrypt z^i in ct_z^{2i}. Then, by the true-simulation soundness of Π_1, and the perfect soundness of the OR-NIZK Π_0 it follows that $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ is implied by the other conjuncts in the winning condition – the argument is same as given in proof of Lemma 1 in the indistinguishability of Game $\mathbf{G}_{2,j,4}$ and Game $\mathbf{G}_{2,j,3}$.

Game $\mathbf{H}_4$: In this game, instead of picking $\mathbf{k}_2$ and $\mathbf{k}_2'$ at random, the challenger picks $(\mathbf{k}_2, \mathbf{l}_2) \leftarrow \mathbb{Z}_q^k \times \mathbb{Z}_q^k$. Note $\mathbf{k}_2$ and $\mathbf{k}_2'$ are independent of $\underline{\mathbf{B}}$ and $\underline{\mathbf{B}}'$. The challenger changes the γ^*-test conjunct in the winning condition by replacing $\boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$ by $\boldsymbol{\rho}^*\mathbf{k}_2$. Further, in each signature query output it modifies the computation of γ^i as follows: if $i_j = \beta$ then $\boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'$ is replaced by $\boldsymbol{\rho}^i\mathbf{k}_2$. Otherwise, it replaces $(\boldsymbol{\rho}_1^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}_1^i\mathbf{k}_2') + (\boldsymbol{\rho}_2^i\mathbf{k}_2 + [\underline{\mathbf{B}}'\mathbf{r}_2^i]_1\mathbf{k}_2')$ by $\boldsymbol{\rho}_1^i\mathbf{k}_2 + \boldsymbol{\rho}_2^i\mathbf{l}_2$, where $\boldsymbol{\rho}_1^i = [\bar{\mathbf{B}}\mathbf{r}_1^i]_1^\top$, $\hat{\boldsymbol{\rho}}_1^i = [\underline{\mathbf{B}}\mathbf{r}_1^i]_1^\top$, $\boldsymbol{\rho}_2^i = [\bar{\mathbf{B}}\mathbf{r}_2^i]_1^\top$ and $\mathbf{l}_2 = \mathbf{k}_2 + \bar{\mathbf{B}}^{-\top}\underline{\mathbf{B}}'\mathbf{k}_2'$.

First note that since $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ is a conjunct in the winning condition, replacing $\mathbf{k}_2\boldsymbol{\rho}^* + \mathbf{k}_2'\hat{\boldsymbol{\rho}}^*$ by $\mathbf{k}_2\rho^*$ is equivalent if $\bar{\mathbf{B}}^\top\mathbf{k}_2 + \underline{\mathbf{B}}^\top\mathbf{k}_2'$ is replaced by $\bar{\mathbf{B}}^\top\mathbf{k}_2$. It is easy to see (by pairwise independence) that the adversary's view in the two games $\mathbf{H}_3$ and $\mathbf{H}_4$ is statistically indistinguishable, except if $\underline{\mathbf{B}}' = \underline{\mathbf{B}}$ which happens with probability at most $1/q$.

Game $\mathbf{H}_5$: In this game the challenger again removes the conjunct $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ from the winning condition.

We again, first check that the QA-NIZK Π_1 is in true-simulation mode. Then by the same argument as given in $\mathbf{H}_3$ indistinguishability from $\mathbf{H}_2$, the adversary's advantage is different from advantage in game $\mathbf{H}_4$ by at most $\textsc{adv}_{\Pi_1}^{\mathsf{tss}}$.

Game $\mathbf{H}_6$: In this game the challenger again generates the OR-NIZK Π_0 CRS using the hiding CRS generator and the OR proofs are simulated.

The adversary's advantage in game $\mathbf{H}_6$ is different from its advantage in $\mathbf{H}_5$ by at most $\textsc{adv}^{\mathsf{zk}}_{\Pi_0}$.

Game $\mathbf{H}_7$: In this game, the adversary need not pick $\underline{\mathbf{B}}'$. Next, for each query i, if i_j is not equal to β, then the challenger picks $\mathbf{r}_1^i$ and $\mathbf{r}_2^i$ at random, and sets $\mathbf{r}^i = \mathbf{r}_1^i + \mathbf{r}_2^i$. It also sets $\boldsymbol{\rho}^i = [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$ and $\hat{\boldsymbol{\rho}}^i = [\underline{\mathbf{B}}\mathbf{r}^i]_1$. Note that $\mathbf{r}^i$'s are not used in the OR proofs. There is no change in the generation of γ^i as it uses $\mathbf{k}_2$ and $\mathbf{k}_2'$.

By a reduction argument similar to that given for games $\mathbf{H}_1$ and $\mathbf{H}_2$, the adversary's advantage in distinguishing between $\mathbf{H}_6$ and $\mathbf{H}_7$ is at most $\textsc{adv}_{\mathcal{D}_{2k,k}\text{-MDDH}}$.

Game $\mathbf{H}_8$: In this game the Challenger lazily defines another random and independent function $\textsc{rf}'_{j-1}$ from $\{0,1\}^{j-1}$ to $\mathbb{Z}_q$. Then, for all i such that i_j is not equal to β, it replaces in the computation of γ^i, the function $\textsc{rf}_{j-1}$ by $\textsc{rf}'_{j-1}$.

Since in each query i, $\mathbf{r}_1^i$ and $\mathbf{r}_2^i$ are chosen afresh randomly and independently, and since all other terms (i.e., other that γ^i) use one linear combination of $\mathbf{r}_1^i$ and $\mathbf{r}_2^i$, namely $\mathbf{r}_1^i + \mathbf{r}_2^i$, and γ^i uses a different linear combination, namely $\mathbf{k}_2\mathbf{r}_1^i + \mathbf{l}_2\mathbf{r}_2^i$, then conditioned on $\mathbf{k}_2 \neq \mathbf{l}_2$, the transcripts in games $\mathbf{H}_7$ and $\mathbf{H}_8$ are statistically identical. The probability of $\mathbf{k}_2 = \mathbf{l}_2$ is at most $1/q$, and hence that is the statistical distance between the distributions of the transcripts in $\mathbf{H}_7$ and $\mathbf{H}_8$. Thus, this is also an upper bound on the difference in adversary's advantage in the two games.

Game $\mathbf{H}_9$: In this game, the adversary also picks $\underline{\mathbf{B}}' \leftarrow \mathbb{Z}_q^{1\times k}$. Next, for each query i, if i_j is not equal to β, then the challenger picks $\mathbf{r}_1^i$ and $\mathbf{r}_2^i$ at random, and sets $\mathbf{r}^i = (\mathbf{r}_1^i + \mathbf{r}_2^i)$. It also sets $\boldsymbol{\rho}^i = [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$ and $\hat{\boldsymbol{\rho}}^i = [\underline{\mathbf{B}}\mathbf{r}_1^i + \underline{\mathbf{B}}'\mathbf{r}_2^i]_1$. Note that $\mathbf{r}^i$'s are not used in the OR proofs. There is no change in generation of γ^i (see Figure 9).

Again, by a similar reduction argument to $\mathcal{D}_{2k,k}$-MDDH assumption, the difference in adversary's advantage in games $\mathbf{H}_9$ and $\mathbf{H}_8$ is at most $\textsc{adv}_{\mathcal{D}_{2k,k}\text{-MDDH}}$.

Game $\mathbf{H}_{10}$: In this game, the challenger generates the OR-NIZK Π_0 CRS using the binding CRS generator. It also uses the real witnesses, i.e. $(\mathbf{r}^i, 0, 0, 0)$ or $(0, 1-\beta, \mathbf{r}_z^i, \mathbf{r}_x)$ in generating the OR proofs. In this game, the challenger also re-introduces the conjunct $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \text{span}([\mathbf{B}]_1)$.

First note that the witnesses do satisfy the language L_0 for all queries i, by an argument similar to that given for games $\mathbf{H}_3$ and $\mathbf{H}_2$. Then by repeating the argument there, we also conclude that $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \text{span}([\mathbf{B}]_1)$ is implied by other conjuncts. Thus, the difference in adversary's advantage is at most

$$\textsc{adv}^{\mathsf{tss}}_{\Pi_1} + \textsc{adv}^{\mathsf{zk}}_{\Pi_0}.$$

Game $\mathbf{H}_{11}$: In this game, the challenger picks $\mathbf{k}_2, \mathbf{k}_2'$ randomly and independently (instead of picking $\mathbf{k}_2$ and $\mathbf{l}_2$) and reverts back to the setting of Game

$\mathbf{H}_3$. The challenger also changes the γ^*-test in the winning condition by replacing $\boldsymbol{\rho}^*\mathbf{k}_2$ by $\boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$. Further, similar changes are made in the computation of γ^i (see Figure 9).

With the conjunct $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ in place in the winning condition, the new winning condition is equivalent to the previous winning condition. Moreover, conditioned on $\underline{\mathbf{B}}' \neq \underline{\mathbf{B}}$, the distribution of $\mathbf{k}_2$ and $\mathbf{k}_2'$ remains same as in game $\mathbf{H}_{10}$. Thus, the difference in adversary's advantage is at most $1/q$.

Game $\mathbf{H}_{12}$: In this game, the challenger drops the conjunct $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ from the winning condition.

Again, by arguments similar to that given for games $\mathbf{H}_2$ and $\mathbf{H}_3$ the difference in adversary's advantage is at most $\textsc{adv}^{\mathsf{tss}}_{\Pi_1}$.

Game $\mathbf{H}_{13}$: In this game, the adversary need not pick $\underline{\mathbf{B}}'$. Next, for each query i, if i_j is not equal to β, then the challenger picks $\mathbf{r}_1^i$ and $\mathbf{r}_2^i$ at random, and sets $\mathbf{r}^i = \mathbf{r}_1^i + \mathbf{r}_2^i$. It also sets $\boldsymbol{\rho}^i = [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$, $\hat{\boldsymbol{\rho}}^i = [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top$ and a similar change in the generation of γ^i (see Figure 9).

This is essentially the rewind of going from game $\mathbf{H}_1$ to $\mathbf{H}_2$. Hence, by a similar argument, the difference in adversary's advantage in games $\mathbf{H}_{13}$ and $\mathbf{H}_{12}$ is at most $\textsc{adv}_{\mathcal{D}_{2k,k}\text{-MDDH}}$.

Game $\mathbf{H}_{14}$: In this game, even for i such that i_j is not equal to β, the challenger just picks $\mathbf{r}^i$, and defines $\boldsymbol{\rho}^i = [\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$ and $\hat{\boldsymbol{\rho}}^i = [\underline{\mathbf{B}}\mathbf{r}^i]_1^\top$.

There is no statistical difference in the two games $\mathbf{H}_{14}$ and $\mathbf{H}_{13}$. Now, note that game $\mathbf{H}_{14}$ is identical to game $\mathbf{G}_{2,j,5}$. This completes the proof.

$\mathsf{crssim}() : \cdots$

Games $H_{0,3-5,10-14}$ $\quad \textsc{crs}^0 \leftarrow \Pi_0.\mathsf{crsgen}()$

Games $H_{1-2,6-9}$ $\quad (\textsc{crs}^0, \mathsf{trap}^0) \leftarrow \Pi_0.\mathsf{crssim}()$

$\mathsf{sim}(\mathbf{y}^i \in \mathbb{G}_1^n) : \quad \cdots$

Let $(\hat{\boldsymbol{\rho}}^{i\top}, \gamma^i) :=$

Games (2,j,4)
$$\left([\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'\right)$$

Game H_0
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2', & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2', & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_1
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2', & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}(\mathbf{r}_1^i + \mathbf{r}_2^i)]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + (\boldsymbol{\rho}_1^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}_1^i\mathbf{k}_2') + (\boldsymbol{\rho}_2^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}_2^i\mathbf{k}_2'), & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_2, H_3
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2', & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}\mathbf{r}_1^i + \underline{\mathbf{B}}'\mathbf{r}_2^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + (\boldsymbol{\rho}_1^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}_1^i\mathbf{k}_2') + (\boldsymbol{\rho}_2^i\mathbf{k}_2 + [\underline{\mathbf{B}}'\mathbf{r}_2^i]_1^\top\mathbf{k}_2'), & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_4, H_5, H_6
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2, & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}\mathbf{r}_1^i + \underline{\mathbf{B}}'\mathbf{r}_2^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}_1^i\mathbf{k}_2 + \boldsymbol{\rho}_2^i\mathbf{l}_2, & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_7
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2, & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}(\mathbf{r}_1^i + \mathbf{r}_2^i)]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}_1^i\mathbf{k}_2 + \boldsymbol{\rho}_2^i\mathbf{l}_2, & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_8
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2, & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}(\mathbf{r}_1^i + \mathbf{r}_2^i)]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}_1^i\mathbf{k}_2 + \boldsymbol{\rho}_2^i\mathbf{l}_2, & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_9, H_{10}
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2, & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}\mathbf{r}_1^i + \underline{\mathbf{B}}'\mathbf{r}_2^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}_1^i\mathbf{k}_2 + \boldsymbol{\rho}_2^i\mathbf{l}_2, & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_{11}, H_{12}
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2', & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}\mathbf{r}_1^i + \underline{\mathbf{B}}'\mathbf{r}_2^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i|_{j-1})]_1 + (\boldsymbol{\rho}_1^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}_1^i\mathbf{k}_2') + (\boldsymbol{\rho}_2^i\mathbf{k}_2 + [\underline{\mathbf{B}}'\mathbf{r}_2^i]_1^\top\mathbf{k}_2'), & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_{13}
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2', & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}(\mathbf{r}_1^i + \mathbf{r}_2^i)]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i|_{j-1})]_1 + (\boldsymbol{\rho}_1^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}_1^i\mathbf{k}_2') + (\boldsymbol{\rho}_2^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}_2^i\mathbf{k}_2'), & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Game H_{14}
$$\begin{pmatrix} [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2', & \text{if } (i_j = \beta) \\ [\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2', & \text{if } (i_j \neq \beta) \end{pmatrix}$$

Games (2,j,5)
$$\left([\underline{\mathbf{B}}\mathbf{r}^i]_1,\ \mathbf{y}^{i\top}\mathbf{k}_1 + \begin{bmatrix} RF_{j-1}(i|_{j-1}), & \text{if } (i_j = \beta) \\ RF'_{j-1}(i|_{j-1}), & \text{if } (i_j \neq \beta) \end{bmatrix}_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'\right)$$

$\cdots$

$\mathsf{WIN} \overset{\triangle}{=}$ **if** $(\mathsf{ChkAbort})$ **return false; else**

$\pi^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \mathsf{ct}_z^{1*}, \mathsf{ct}_z^{2*}, \mathsf{ct}_v^*, \pi_0^*, \pi_1^*, \pi_2^*, \pi_3^*) :$

$(\mathbf{y}^* \notin \{\mathbf{y}^i\}_i \cup \mathrm{span}([\mathbf{M}]_1))$ **and** $\mathsf{ver}(\textsc{crs}_v,\ \mathbf{y}^*,\ \pi^*)$

Games H_0-H_3, H_{11}-H_{14} $\quad$ **and** $\exists\theta \in \mathcal{Z} : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$

Games H_4-H_{10} $\quad$ **and** $\exists\theta \in \mathcal{Z} : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$

Games H_3-H_4, H_{10}-H_{11} $\quad$ **and** $(\boldsymbol{\rho}^* \| \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$

Fig. 9. Going from Game (2,j,4) to (2,j,5).

#	CRS^0	CRS^1	x	ct_x	$\mathbf{k}_1$	z^i	ct_z^{1i}	$\boldsymbol{\rho}^i$	$\hat{\boldsymbol{\rho}}^{i\top}$	γ^i	CRS^3	w	v	for π_3	win. cond
0	BG	BS	0	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$\mathbf{k}_1 := \mathbf{k}_1'$	0	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	HG	k_0	0	$\mathbf{y} = [\mathbf{Mx}]_1$	WIN_0
0.2	$\boxed{\text{HG}}$	BS	0	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$\mathbf{k}_1 := \mathbf{k}_1'$	0	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [k_0]_1 + \boldsymbol{\rho}^i\mathbf{k}_2}$	HG	k_0	$\boxed{k_0}$	$\mathbf{y} = [\mathbf{Mx}]_1$	WIN_0
0.3	$\boxed{\text{BG}}$	BS	0	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$\mathbf{k}_1 := \mathbf{k}_1'$	0	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [k_0]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$\boxed{\text{BG}}$	k_0	k_0	$\boxed{(\mathbf{r}_w, \mathbf{r}_v)}$	WIN_0
1	BG	$\boxed{\text{HG}}$	0	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$\mathbf{k}_1 := \mathbf{k}_1'$	0	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [k_0]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	BG	k_0	k_0	$(\mathbf{r}_w, \mathbf{r}_v)$	WIN_0 $\boxed{(\boldsymbol{\rho}^* \Vert \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)}$ $\boxed{\exists \theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2}$
1.1	BG	HG	0	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$\mathbf{k}_1 := \mathbf{k}_1'$	0	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [k_0]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$\boxed{\text{HG}}$	$\boxed{0}$	k_0	$(\mathbf{r}_w, \mathbf{r}_v)$	WIN_0 $(\boldsymbol{\rho}^* \Vert \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists \theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$
2	$\boxed{\text{HG}}$	HG	0	$\boxed{\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)}$	$\mathbf{k}_1 := \mathbf{k}_1'$	0	$\boxed{\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})}$	$[\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [k_0]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	HG	0	k_0	$(\mathbf{r}_w, \mathbf{r}_v)$	WIN_0 $(\boldsymbol{\rho}^* \Vert \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists \theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$
3	HG	HG	0	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)$	$\mathbf{k}_1 := \mathbf{k}_1'$	0	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})$	$[\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_L(i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2}$	HG	0	k_0	$(\mathbf{r}_w, \mathbf{r}_v)$	WIN_0 $(\boldsymbol{\rho}^* \Vert \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists \theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$
4	HG	HG	0	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)$	$\boxed{\mathbf{k}_1 := \mathbf{k}_1' + \mathbf{M}^\perp\mathbf{u}}$	0	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})$	$[\bar{\mathbf{B}}\mathbf{r}^i]_1^\top$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1' + \mathbf{y}^\top\mathbf{M}^\perp\mathbf{u} + [\mathrm{RF}_L(i)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2}$	HG	0	k_0	$(\mathbf{r}_w, \mathbf{r}_v)$	WIN_0 $(\boldsymbol{\rho}^* \Vert \hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\boxed{\exists \theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1' + \mathbf{y}^{*\top}\mathbf{M}^\perp\mathbf{u} + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2}$

Fig. 10. Summary of the top level games and winning conditions.

#	CRS^0	x	ct_x	$\mathbf{k}_2$	z^i	ct_z^{1i}	$\hat{\boldsymbol{\rho}}^{i\top}$	γ^i	additional-win. cond	abort.
$2.j.0$	HG	0	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)$	$\mathbf{k}_2$	0	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	
$2.j.1$	HG	0	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)$	$\boxed{(\mathbf{k}_2,\ \mathbf{k}_2')}$	$\boxed{i_j}$	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'}$	$(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\boxed{\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'}$	
$2.j.2$	HG	0	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)$	$(\mathbf{k}_2,\ \mathbf{k}_2')$	i_j	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'$	$(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$	$\boxed{\text{check}}$
$2.j.3$	$\boxed{\text{BG}}$	$\boxed{1-\beta}$	$\boxed{\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)}$	$(\mathbf{k}_2,\ \mathbf{k}_2')$	i_j	$\boxed{\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)}$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'$	$(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$	check
$2.j.4$	BG	$1-\beta$	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$(\mathbf{k}_2,\ \mathbf{k}_2')$	i_j	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'$	$\boxed{\phantom{(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top}}$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$	check
$2.j.5$	BG	$1-\beta$	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$(\mathbf{k}_2,\ \mathbf{k}_2')$	i_j	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + \begin{bmatrix}\mathrm{RF}_{j-1}(i\|_{j-1}),\ \text{if } (i_j = \beta) \\ \mathrm{RF}'_{j-1}(i\|_{j-1}),\ \text{if } (i_j \neq \beta)\end{bmatrix}_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'}$		check
$2.j.6$	BG	$1-\beta$	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$(\mathbf{k}_2,\ \mathbf{k}_2')$	i_j	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + \begin{bmatrix}\mathrm{RF}_{j-1}(i\|_{j-1}),\ \text{if } (i_j = \beta) \\ \mathrm{RF}'_{j-1}(i\|_{j-1}),\ \text{if } (i_j \neq \beta)\end{bmatrix}_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}_2'$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$ $\boxed{(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)}$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}_2'$	check
$2.j.7$	BG	$1-\beta$	$\mathsf{Enc}(\mathsf{pk}_1, x; \mathbf{r}_x)$	$\boxed{\mathbf{k}_2}$	i_j	$\mathsf{Enc}(\mathsf{pk}_1, z^i; r_z^i)$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_j(i\|_j)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2}$	$(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\boxed{\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2}$	check
$2.j.8$	$\boxed{\text{HG}}$	$1-\beta$	$\boxed{\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)}$	$\mathbf{k}_2$	i_j	$\boxed{\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})}$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_j(i\|_j)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	check
$2.j.9$	HG	$1-\beta$	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)$	$\mathbf{k}_2$	i_j	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_j(i\|_j)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	$\boxed{\phantom{\text{check}}}$
$2.j.10$	HG	$\boxed{0}$	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_x)$	$\mathbf{k}_2$	$\boxed{0}$	$\mathsf{Enc}(\mathsf{pk}_1, 0; \mathbf{r}_z^{1i})$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [\mathrm{RF}_j(i\|_j)]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$(\boldsymbol{\rho}^*\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	

Fig. 11. Game transition from Game 2 to 3.

		If $i_j = \beta$		If $i_j \neq \beta$			
#	CRS^0	$\hat{\boldsymbol{\rho}}^{i\top}$	γ^i	$\hat{\boldsymbol{\rho}}^{i\top}$	γ^i	additional-win. cond	abort.
$2.j.4$	BG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$	check
H_0	BG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$	check
H_1	$\boxed{\text{HG}}$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$\boxed{[\underline{\mathbf{B}}(\mathbf{r}^i_1 + \mathbf{r}^i_2)]_1}$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + (\boldsymbol{\rho}^i_1\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i_1\mathbf{k}'_2) + (\boldsymbol{\rho}^i_2\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i_2\mathbf{k}'_2)}$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$	check
H_2	HG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$\boxed{[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1}$	$\boxed{[\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + (\boldsymbol{\rho}^i_1\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i_1\mathbf{k}'_2) + (\boldsymbol{\rho}^i_2\mathbf{k}_2 + [\underline{\mathbf{B}}'\mathbf{r}^i_2]_1^\top\mathbf{k}'_2}$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$	check
H_3	$\boxed{\text{BG}}$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + (\boldsymbol{\rho}^i_1\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i_1\mathbf{k}'_2) + (\boldsymbol{\rho}^i_2\mathbf{k}_2 + [w^i]_1\mathbf{k}'_2)$	$\boxed{(\boldsymbol{\rho}^*\\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)}$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$	check
H_4	BG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2}$	$[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i_1\mathbf{k}_2 + \boldsymbol{\rho}^i_2\mathbf{l}_2}$	$(\boldsymbol{\rho}^*\\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\boxed{\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2}$	check
H_5	BG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i_1\mathbf{k}_2 + \boldsymbol{\rho}^i_2\mathbf{l}_2$	$\boxed{\qquad\qquad}$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	check
H_6	$\boxed{\text{HG}}$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i_1\mathbf{k}_2 + \boldsymbol{\rho}^i_2\mathbf{l}_2$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	check
H_7	HG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$\boxed{[\underline{\mathbf{B}}(\mathbf{r}^i_1 + \mathbf{r}^i_2)]_1}$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i_1\mathbf{k}_2 + \boldsymbol{\rho}^i_2\mathbf{l}_2$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	check
H_8	HG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$[\underline{\mathbf{B}}(\mathbf{r}^i_1 + \mathbf{r}^i_2)]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i_1\mathbf{k}_2 + \boldsymbol{\rho}^i_2\mathbf{l}_2}$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	check
H_9	HG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$\boxed{[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1}$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i_1\mathbf{k}_2 + \boldsymbol{\rho}^i_2\mathbf{l}_2$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	check
H_{10}	$\boxed{\text{BG}}$	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2$	$[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i_1\mathbf{k}_2 + \boldsymbol{\rho}^i_2\mathbf{l}_2$	$\boxed{(\boldsymbol{\rho}^*\\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)}$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2$	check
H_{11}	BG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2}$	$[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i\|_{j-1})]_1 + (\boldsymbol{\rho}^i_1\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i_1\mathbf{k}'_2) + (\boldsymbol{\rho}^i_2\mathbf{k}_2 + [\underline{\mathbf{B}}'\mathbf{r}^i_2]_1^\top\mathbf{k}'_2)}$	$(\boldsymbol{\rho}^*\\|\hat{\boldsymbol{\rho}}^*)^\top \in \mathrm{span}([\mathbf{B}]_1)$ $\boxed{\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2}$	check
H_{12}	BG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$[\underline{\mathbf{B}}\mathbf{r}^i_1 + \underline{\mathbf{B}}'\mathbf{r}^i_2]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i\|_{j-1})]_1 + (\boldsymbol{\rho}^i_1\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i_1\mathbf{k}'_2) + (\boldsymbol{\rho}^i_2\mathbf{k}_2 + [\underline{\mathbf{B}}'\mathbf{r}^i_2]_1^\top\mathbf{k}'_2)$	$\boxed{\qquad\qquad}$ $\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$	check
H_{13}	BG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$\boxed{[\underline{\mathbf{B}}(\mathbf{r}^i_1 + \mathbf{r}^i_2)]_1}$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i\|_{j-1})]_1 + (\boldsymbol{\rho}^i_1\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i_1\mathbf{k}'_2) + (\boldsymbol{\rho}^i_2\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i_2\mathbf{k}'_2)}$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$	check
H_{14}	BG	$[\underline{\mathbf{B}}\mathbf{r}^i]_1$	$\mathbf{y}^{i\top}\mathbf{k}_1 + [RF_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2$	$\boxed{[\underline{\mathbf{B}}\mathbf{r}^i]_1}$	$\boxed{\mathbf{y}^{i\top}\mathbf{k}_1 + [RF'_{j-1}(i\|_{j-1})]_1 + \boldsymbol{\rho}^i\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^i\mathbf{k}'_2}$	$\exists\theta \in Z : \gamma^* = \mathbf{y}^{*\top}\mathbf{k}_1 + [\theta]_1 + \boldsymbol{\rho}^*\mathbf{k}_2 + \hat{\boldsymbol{\rho}}^*\mathbf{k}'_2$	check

Fig. 12. Game transition from Game (2.j.4) to (2.j.5).

C Independently-TSS QA-NIZK

The construction is same as [KW15], which we reproduce below to explain the proof.

crsgen: Let $[\mathbf{M}^{(n_1+n_2)\times t}]_1$ be the parameter supplied to crsgen. Let $n = n_1 + n_2$. Sample a matrix $\mathbf{K} \leftarrow \mathbb{Z}_q^{n\times k}$ and a matrix $\mathbf{A} \leftarrow \mathcal{D}_k$. Let $\bar{\mathbf{A}}$ be the top $k \times k$ square matrix of $\mathbf{A}$.

The common reference string (CRS) has two parts $\textsc{crs}_p$ and $\textsc{crs}_v$ which are to be used by the prover and the verifier respectively.

$$\textsc{crs}_p^{t\times k} := ([\mathbf{P}]_1 = [\mathbf{M}^\top \mathbf{K}]_1) \qquad\qquad \textsc{crs}_v := ([\mathbf{C}]_2^{n\times k} = [\mathbf{K}\bar{\mathbf{A}}]_2, \quad [\bar{\mathbf{A}}]_2^{k\times k})$$

prover: Given candidate $\mathbf{y} = [\mathbf{M}]_1\mathbf{x}$ with witness vector $\mathbf{x}^{t\times 1}$, the prover generates the following proof consisting of k elements in $\mathbb{G}_1$:

$$\pi := \mathbf{x}^\top \textsc{crs}_p$$

ver: Given $\textsc{crs}_v$ as above, candidate $\mathbf{y} \in \mathbb{G}_1^n$, and proof π, check:

$$e(\mathbf{y}^\top, [\mathbf{K}\bar{\mathbf{A}}]_2) = e(\pi, [\bar{\mathbf{A}}]_2).$$

crssim: This is exactly the algorithm crsgen, except additionally the following trapdoor is given: $\mathsf{trap} := \mathbf{K}$

sim: Given candidate $\mathbf{y}$, the proof simulator generates the following proof consisting of k elements in $\mathbb{G}_1$:

$$\pi := \mathbf{y}^\top \mathbf{K}$$

Proof of Independent TSS. We prove Independent True-Simulation-Soundness by transforming the system over a sequence of games. Game $\mathbf{G}_0$ just replicates the construction, but samples $\mathbf{A}$ from a distribution $\mathcal{D}_{k+n-t,k}$ obtained by boosting the given distribution $\mathcal{D}_k$ by boosting lemma. The construction only uses the top $k \times k$ sub-matrix $\bar{\mathbf{A}}$ of the sample which is distributed identically for both $\mathcal{D}_k$ and $\mathcal{D}_{k+n-t,k}$. Let $\underline{\mathbf{A}}$ be the bottom $(n-t) \times k$ sub-matrix of $\mathbf{A}$.

In Game $\mathbf{G}_1$, the challenger efficiently samples $[\mathbf{M}]_1$ according to distribution $\mathcal{D}$, along with witness $\mathbf{M}$ (since $\mathcal{D}$ is an efficiently witness samplable distribution).

Let $\mathbf{M} = \begin{pmatrix} \mathbf{M}_1^{n_1\times t} \\ \mathbf{M}_2^{n_2\times t} \end{pmatrix}$. Since $\mathbf{M}_1$ is an $n_1 \times t$ dimensional rank t matrix, there is a rank $n_1 - t$ matrix $\mathbf{M}_1^\perp$ of dimension $n_1 \times (n_1 - t)$ whose columns form a complete basis for the kernel of $\mathbf{M}_1^\top$, which means $\mathbf{M}_1^\top \mathbf{M}_1^\perp = 0^{t\times(n_1-t)}$. In this game, the NIZK CRS is computed as follows: Generate matrix $\mathbf{K}_1'^{n\times k} \overset{\text{def}}{=} \begin{pmatrix} \mathbf{K}_1'^{n_1\times k} \\ \mathbf{K}_2'^{n_2\times k} \end{pmatrix}$ and let matrix $\mathbf{T}^{(n_1-t)\times k} = \underline{\mathbf{A}}\bar{\mathbf{A}}^{-1}$. Implicitly set: $\mathbf{K} = \mathbf{K}' + \begin{pmatrix} \mathbf{M}_1^{\perp}\mathbf{T} \\ 0 \end{pmatrix}$. Therefore we have,

$$\text{CRS}_p^{t\times k} = [\mathbf{M}^{\top}\mathbf{K}]_1 = \left[\mathbf{M}_1^{\top}(\mathbf{K}_1' + \mathbf{M}_1^{\perp}\mathbf{T}) + \mathbf{M}_2^{\top}\mathbf{K}_2'\right]_1 = [\mathbf{M}^{\top}\mathbf{K}']_1$$

$$[\mathbf{C}]_2^{n\times k} = \begin{bmatrix} (\mathbf{K}_1' + \mathbf{M}_1^{\perp}\mathbf{T})\bar{\mathbf{A}} \\ \mathbf{K}_2'\bar{\mathbf{A}} \end{bmatrix}_2 = \begin{pmatrix} \mathbf{K}_1'[\bar{\mathbf{A}}]_2 + \mathbf{M}_1^{\perp}[\underline{\mathbf{A}}]_2 \\ \mathbf{K}_2'[\bar{\mathbf{A}}]_2 \end{pmatrix}$$

Now let's say we are given a $\mathcal{D}_{k+n_1-t,k}$ challenge which is either "real": $([\mathbf{A}]_2, [\bar{\mathbf{A}}\mathbf{s}]_2, [\underline{\mathbf{A}}\mathbf{s}]_2)$ or "fake": $([\mathbf{A}]_2, [\mathbf{s}']_2, [\mathbf{s}'']_2)$.

For an adversary supplied $(\mathbf{y}_1^*\|\ \mathbf{y}_2^*) \in \mathbb{G}_1^{n_1} \times \mathbb{G}_1^{n_2}$ and proof π, such that $\mathbf{y}_1^* \notin \text{span}([\mathbf{M}_1]_1)$, we have $\mathbf{y}_1^{*\top}\mathbf{M}_1^{\perp} \neq 0^{1\times(n_1-t)}$. If the proof verifies, that means:

$$\mathbf{y}_1^{*\top}(\mathbf{K}_1'\bar{\mathbf{A}} + \mathbf{M}_1^{\perp}\underline{\mathbf{A}}) + \mathbf{y}_2^{*\top}\mathbf{K}_2'\bar{\mathbf{A}} = \pi\bar{\mathbf{A}} \implies (\mathbf{y}_1^{*\top}\mathbf{M}_1^{\perp})\underline{\mathbf{A}} = (\pi - \mathbf{y}_1^{*\top}\mathbf{K}_1' - \mathbf{y}_2^{*\top}\mathbf{K}_2')\bar{\mathbf{A}}$$

Since the LHS is nonzero, $\mathbf{y}_1^{*\top}\mathbf{M}_1^{\perp}$ and $\pi - \mathbf{y}_1^{*\top}\mathbf{K}_1' - \mathbf{y}_2^{*\top}\mathbf{K}_2'$ can be employed to detect the real $\mathcal{D}_{k+n_1-t,k}$ challenge by pairing.

D Proof of Tight Security of Multi-Challenge CCA2-PKE

Theorem 3. (re-stated) Under the $\mathcal{D}_k$-MDDH assumption, and using the labeled USS-QA-NIZK Π' of Fig. **??**, the public-key encryption scheme described in Fig 5 is (μ, q_e) IND-CCA secure with Adversary's advantage $\mathcal{A}$ upper-bounded by

$$2 \cdot \text{ADV}_{\Pi'}^{\mathsf{tss}} + 6k \cdot \text{ADV}_{\mathcal{D}_k\text{-MDDH}} + 2 \cdot \text{ADV}_{\Pi'}^{\mathsf{uss}}(q_e) + O(1/q).$$

For ease of reading, we will consider only the the case $\mu = 1$, i.e., a single user and multi-challenges. The proof easily generalizes to multi-user setting by considering the USS-QA-NIZK generalized to simultaneous multiple CRS-es (and languages) as done in [LPJY15]. Alternatively, one may consider the same CRS for all users by letting $\mathbf{B}$ being the same and generated as part of group parameters par.

Proof. In the following we consider several games between a challenger $\mathcal{C}$ and the adversary $\mathcal{A}$, and $\Pr_i[X]$ will denote the probability of predicate X holding in probability space defined in game $\mathbf{G}_i$. We will first bound the advantage of the adversary in terms of $\mathcal{D}_{2k,k}$-MDDH. Then, using the boosting lemma (see section 2.1, we can bound the advantage in terms of $\mathcal{D}_k$-MDDH.

Game $\mathbf{G}_0$: This is same as the game between the challenger and the adversary in the definition 6. Recall, it boosts the distribution $\mathcal{D}_{k+1,k}$ to $\mathcal{D}_{2k,k}$ by using boosting (see Section 2.1). Also recall, the challenger picks a bit d at random.

Game $\mathbf{G}_1$: In this game, the challenger picks $\mathbf{k}$ differently: it picks two vectors $\mathbf{k}_1, \mathbf{k}_2$, and sets $\mathbf{k} = \mathbf{k}_1 + \bar{\mathbf{B}}^{-\top}\underline{\mathbf{B}}\mathbf{k}_2$. Moreover, it decrypts as follows: instead of computing $(\gamma - \boldsymbol{\rho}\mathbf{k})$, it now computes $(\gamma - (\boldsymbol{\rho}\mathbf{k}_1 + \hat{\boldsymbol{\rho}}\mathbf{k}_2))$.

Since, $\bar{\mathbf{B}}$ is invertible with high probability under the $\mathcal{D}_{2k,k}$-MDDH assumption, and by soundness of the USS-QA-NIZK it follows the the difference in the adversary's view between the games $\mathbf{G}_0$ and $\mathbf{G}_1$ is bounded by $O(1/q) + \textsc{adv}^{\mathsf{tss}}_{\Pi'}$.

Game $\mathbf{G}_2$: In this game, the challenger generates the $(\textsc{crs}_p, \textsc{crs}_v, \mathsf{trap})$ using the CRS simulator of Π'. Moreover, it computes all proofs using the proof simulator of Π' (using trap, and not requiring $\mathbf{r}$).

By perfect zero-knowledge simulation of the USS-QA-NIZK, the Adversary's view is unchanged in going from game $\mathbf{G}_1$ to $\mathbf{G}_2$.

Game $\mathbf{G}_3$: In this game the simulator picks another $\underline{\mathbf{B}}'$ at random from $\mathbb{Z}_q^{k \times k}$, and serves Encryption queries (slightly differently) as follows: $\hat{\boldsymbol{\rho}}$ is now computed as $[\underline{\mathbf{B}}'^{\top}\mathbf{r}]_1$ and γ is now computed as $M_d + \mathbf{r}^\top \bar{\mathbf{B}}^\top\ (\mathbf{k}_1 + \bar{\mathbf{B}}^{-\top}(\underline{\mathbf{B}}')^\top \mathbf{k}_2)$.

It is not difficult to show that the probability that $\mathcal{A}$ can distinguish its views in the games $\mathbf{G}_2$ and $\mathbf{G}_3$ is at most $\textsc{adv}_{\mathcal{D}_{2k,k}\text{-MDDH}}$. Note, the challenger can simulate the games completely with only one instance of $\mathcal{D}_{2k,k}$-MDDH.

Game $\mathbf{G}_4$: In this game, the challenger serves decryption queries by computing $(\gamma - (\boldsymbol{\rho}(\mathbf{k}_1 + \bar{\mathbf{B}}^{-\top}\underline{\mathbf{B}}^\top \mathbf{k}_2))$.

We now show that the probability of the adversary $\mathcal{A}$ distinguishing its views in the games $\mathbf{G}_3$ and $\mathbf{G}_4$ is at most $\textsc{adv}^{\mathsf{uss}}_{\Pi'}(q_e) + O(1/q)$. We prove this by showing that if the Adversary $\mathcal{A}$ can distinguish between the two games with probability p, then we can build an adversary $\mathcal{B}$ that can forge a false proof in the unbounded simulation-soundness game of USS-QA-NIZK of Π' with probability $p - O(1/q)$.

First note that the view of the Adversary in the games $\mathbf{G}_3$ and $\mathbf{G}_4$ is identical unless for some (at least one) of its decryption requests $\mathtt{ctxt}^* = (\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*, \gamma^*, \pi^*)$ it is the case that $\hat{\boldsymbol{\rho}}^* \neq \boldsymbol{\rho}^* \bar{\mathbf{B}}^{-\top}\underline{\mathbf{B}}$, or in other words $(\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*)$ is not in language L of Π' (unless $\bar{\mathbf{B}}$ is singular, which happens with negligible probability). Moreover, since the challenger generated $\mathbf{B}$ (see Fig 5 and definition of game $\mathbf{G}_0$), it can efficiently test if some $\mathtt{ctxt}^*$ has its $(\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*)$ not in L. It can then use that pair (and the label γ^*, and proof π^*) to claim a false proof that verifies (since the challenger already checked that $\Pi'.\mathsf{ver}$ holds as a first step in the decryption process). We also need to check that the tuple $(\boldsymbol{\rho}^*, \hat{\boldsymbol{\rho}}^*)$, and label γ^*, and proof π^* is not the same as in some simulated-proof oracle request. But, that would imply that the decryption request $\mathtt{ctxt}^*$ is same as one in the set $\mathcal{D}$ that the challenger is maintaining, and hence the challenger never actually decrypted that request. Finally, recall the (enhanced) USS-QA-NIZK simulation-soundness game allows the (USS-QA-NIZK-) Adversary to be given the discrete logarithms of the language defining parameters, which in this case is $[\mathbf{B}]_1$. Thus the challenger, serving as adversary in the USS-QA-NIZK game, can forge with probability at least $p - O(1/q)$.

Game $\mathbf{G}_5$: In this game, instead of setting $\mathbf{k} = \mathbf{k}_1 + \bar{\mathbf{B}}^{-\top}\underline{\mathbf{B}}^\top \mathbf{k}_2$, it picks $\mathbf{k}$ directly at random from $\mathbb{Z}_q^k$. It also picks a random and independent $\mathbf{l}_2$ from $\mathbb{Z}_q^k$. It continues by picking $\underline{\mathbf{B}}'$ at random from $\mathbb{Z}_q^{k \times k}$. Hence, it serves decryption queries by computing $(\gamma - \boldsymbol{\rho}\mathbf{k})$. However, for encryption queries, it now computes $\hat{\boldsymbol{\rho}}$ as $[\underline{\mathbf{B}}'\mathbf{r}]_1$ and γ as $M_d + \mathbf{r}^\top \mathbf{l}_2$.

We now claim that the view of the adversary in games $\mathbf{G}_4$ and $\mathbf{G}_5$ is identical with high probability. this follows easily be noting that for any non-zero $\underline{\mathbf{B}}', \underline{\mathbf{B}}, \mathbf{k}_2$ and $(\underline{\mathbf{B}}' - \underline{\mathbf{B}})$ non-singular, the k-vectors $\mathbf{k}_1 + \bar{\mathbf{B}}^{-\top}\underline{\mathbf{B}}^\top \mathbf{k}_2$ and $\mathbf{k}_1 + \bar{\mathbf{B}}^{-\top}(\underline{\mathbf{B}}')^\top \mathbf{k}_2$ are random and independent (and independent of $\underline{\mathbf{B}}'$, $\underline{\mathbf{B}}$). The statistical difference between the views of the adversary is at most $O(1/q)$.

Game $\mathbf{G}_6$: In this game, in the encryption queries, $\hat{\boldsymbol{\rho}}$ is computed as $[\underline{\mathbf{B}}\mathbf{r}]_1$.

The probability that adversary can distinguish between the two games is at most $\text{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}}$.

Game $\mathbf{G}_7$: In this game, in the encryption queries, γ is set to $M_d + \mathbf{r}^\top(\underline{\mathbf{B}}')^\top \mathbf{l}_2$, where $\underline{\mathbf{B}}'$ is a random matrix from $\mathbb{Z}_q^{k\times k}$.

The view of the Adversary is statistically identical (with statistical difference $O(1/q)$) in games $\mathbf{G}_6$ and $\mathbf{G}_7$, since $\mathbf{l}_2$ is random, and with high probability $\underline{\mathbf{B}}'$ is full-ranked.

Game $\mathbf{G}_8$: In this game, in all the encryption queries, γ_i is computed as $M_d^{(i)} + \mathbf{r'}_i^\top(\underline{\mathbf{B}}')^\top \mathbf{l}_2$, where for each i, $\mathbf{r'}_i$ is a random and independent vector from $\mathbb{Z}_q^k$.

The probability that the Adversary can distinguish between games $\mathbf{G}_7$ and $\mathbf{G}_8$ is at most $\text{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}}$, by the random self-reducibility of $\mathcal{D}_{2k,k}$-MDDH [EHK$^+$13].

Game $\mathbf{G}_9$: In this game, in all the encryption queries, γ_i is computed as $M_0^{(i)} + \mathbf{r'}_i^\top(\underline{\mathbf{B}}')^\top \mathbf{l}_2$, i.e. independent of the bit d.

The view of the adversary is identical in the games $\mathbf{G}_8$ and $\mathbf{G}_9$ with high probability.

We now unwind the above games, going backwards to a game $\mathbf{G}_{10}$ which is identical to game $\mathbf{G}_0$, except that $M_0^{(i)}$ is used instead of $M_d^{(i)}$ in all encryption oracle requests.

Now, note that since the view of the Adversary in game $\mathbf{G}_{10}$ is independent of d, the probability that an adversary can guess d in game $\mathbf{G}_{10}$ (i.e. be deemed successful) is at most $1/2$. Thus, the probability that an adversary can guess d in game $\mathbf{G}_0$ is at most

$$1/2 + O(1/q) + 2\cdot \text{ADV}_{\Pi'}^{\mathsf{tss}} + 6\cdot \text{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}} + 2\cdot \text{ADV}_{\Pi'}^{\mathsf{uss}}.$$

The lemma follows, since $\text{ADV}_{\mathcal{D}_{2k,k}\text{-MDDH}} \le k\cdot \text{ADV}_{\mathcal{D}_k\text{-MDDH}}$ by boosting lemma.