Attribute-Based Signatures for Range of Inner Product and Its Applications

Masahito Ishizaka and Kazuhide Fukushima

KDDI Research, Inc., Saitama, Japan.
{xma-ishizaka,ka-fukushima}@kddi.com

Abstract. In attribute-based signatures (ABS) for inner products, the digital signature analogue of attribute-based encryption for inner products (Katz et al., EuroCrypt'08), a signing-key (resp. signature) is labeled with an n-dimensional vector $\mathbf{x} \in \mathbb{Z}_p^n$ (resp. $\mathbf{y} \in \mathbb{Z}_p^n$) for a prime p, and the signing succeeds iff their inner product is zero, i.e., $\langle \mathbf{x}, \mathbf{y} \rangle = 0 \pmod p$. We generalize it to ABS for *range* of inner product (ARIP), requiring the inner product to be within an arbitrarily-chosen range $[L, R]$. As security notions, we define adaptive unforgeablity and perfect signer-privacy. The latter means that any signature reveals no more information about $\mathbf{x}$ than $\langle \mathbf{x}, \mathbf{y} \rangle \in [L, R]$. We propose two efficient schemes, secure under some Diffie-Hellman type assumptions in the standard model, based on non-interactive proof and linearly homomorphic signatures. The 2nd (resp. 1st) scheme is independent of the parameter n in secret-key size (resp. signature size and verification cost). We show that ARIP has many applications, e.g., ABS for range evaluation of polynomials/weighted averages, fuzzy identity-based signatures, time-specific signatures, ABS for range of Hamming/Euclidean distance and ABS for hyperellipsoid predicates.

Keywords: Attribute-based signatures for range of inner product, Adaptive unforgeablity, Signer-privacy, Symmetric bilinear groups of prime order.

1 Introduction

Attribute-Based Encryption (ABE) for Inner Products. In ABE for inner products [15], n-dimensional vector $\mathbf{x} \in \mathbb{Z}_p^n$ (resp. $\mathbf{y} \in \mathbb{Z}_p^n$) for a prime p is associated with secret-key (resp. ciphertext). The decryption succeeds iff $\langle \mathbf{x}, \mathbf{y} \rangle = 0 \pmod p$. It can be generically transformed into various ABE primitives, e.g., (anonymous) identity-based encryption (IBE), hidden-vector encryption (HVE) [10], the dual variant of HVE (= wildcarded IBE [1]), ABE for evaluation of polynomials/weighted averages, ABE for CNF and DNF formulas, and ABE for exact thresholds. Let us consider a generalized primitive, named ABE for arbitrarily-chosen inner product (ACIP), enabling a signer to choose a value of inner product $a \in \mathbb{Z}_p$. Obviously, ABE for ACIP with n dimensions can be transformed from the usual ABE for inner products with $n + 1$ dimensions[1].

[1] The $(n+1)$-th elements of $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^{n+1}$ are set to 1 and $-a \pmod p$, respectively.

Attribute-Based Signatures (ABS) for Inner Products (AIP). AIP is the signature analogue of the ABE for inner products. The signing succeeds iff $\langle \mathbf{x}, \mathbf{y} \rangle = 0 \pmod p$. A signer-privacy guarantees that any signature leaks no more information about $\mathbf{x}$ than $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. It has many applications, e.g., identity-based signatures (IBS), hidden-vector signatures (HVS) (= the signature analogue of HVE), the dual variant of HVS, ABS for evaluation of polynomials/weighted averages, ABS for CNF and DNF formulas, and ABS for exact thresholds.

ABS for Range of Inner Product (ARIP). We generalize a specific value of inner product to a *range* of values. A range $[L, R]$ with $L, R \in \mathbb{Z}_p$ is associated with a signature. If the inner product is within the range, the signing succeeds. The encryption analogue of ARIP, named ABE for range of inner product, can be transformed from ABE for ACIP in a simple manner, where for each integer $i \in [L, R]$, the encryptor generates a ciphertext C_i whose inner product is set to i[2]. The same transformation is not directly applicable to ARIP since the signer-privacy requires the real inner product $\langle \mathbf{x}, \mathbf{y} \rangle$ to be hidden. The ABS scheme by Sakai et al. [24] supporting any circuit as signer-predicate can be an ARIP scheme by properly configuring the circuit. A vector $\mathbf{x} \in \mathbb{Z}_p^n$ is transformed into a binary attribute $x \in \{0,1\}^{n\lambda}$. In their ABS scheme, at signature generation, a signer generates a commitment of the non-interactive witness indistinguishable proof (NIWI) system by Groth and Sahai (GS) [11] for each bit $x[i] \in \{0,1\}$ of x. Thus, at least, its signature length linearly increases with n.

Contribution of this work is threefold. First, we formally define the syntax and security of ARIP. Second, we propose two efficient ARIP schemes based on NIWI and linearly homomorphic signatures (LHS)[3] [9], one of which is independent of n in signature length. Third, we show that ARIP has various applications.

Formalization of ARIP. As the security requirements, we define adaptive existential unforgeability [18,24] and perfect signer-privacy [7]. The latter guarantees that any signature leaks no information about $\mathbf{x} \in \mathbb{Z}_p^n$ of the signer. Its definition is simulatability-based, which requires us to prove that any signature which should be generated using a specific revealed secret-key associated with a vector $\mathbf{x} \in \mathbb{Z}_p$ is simulatable even if without knowing the secret-key.

Our Efficient ARIP Schemes. We propose two efficient ARIP schemes, based on symmetric bilinear pairing groups of prime order, and secure under the computational Diffie-Hellman (CDH), flexible CDH (flexCDH) [6] and decisional linear (DLIN) assumptions. The 2nd (resp. 1st) scheme is independent of n in secret-key size (resp. signature size and verification cost). They are originally a generic

[2] A drawback of this simple approach is low efficiency. Ciphertext length and encryption cost linearly increase with the maximal cardinality of the range $[L, R]$, which is p if $L, R \in \mathbb{Z}_p$ or T if $L, R \in [0, T-1]$ for $T \in \mathbb{N}$.

[3] In LHS, any signature on a message of vector $\boldsymbol{v} \in \mathbb{Z}_p^n$ is labeled with a tag $\tau \in \{0,1\}^*$. Any entity collecting l signatures $\sigma_1, \cdots, \sigma_l$ with the same tag τ on $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_l \in \mathbb{Z}_p^n$ can derive a new $\overline{\sigma}$ on any linear combination $\overline{\boldsymbol{v}} = \sum_{i=1}^{l} \beta_i \cdot \boldsymbol{v}_i \in \mathbb{Z}_p^n$ with $\beta_i \in \mathbb{Z}_p$.

construction based on NIWI and LHS, which is instantiated from the GS NIWI system and a simplified variant of the LHS scheme by Attrapadung, Libert and Peters (ALP) [6].

The generic construction behind our 1st scheme is as follows. For a secret-key $sk_{\mathbf{x}}$ for $\mathbf{x} \in \mathbb{Z}_p^n$, we generate $n+4$ number of vectors $\{\boldsymbol{v}_i\}_{i=1}^{n+4}$. Each $\boldsymbol{v}_i \in \mathbb{Z}_p^{n+5}$ is set to $x_i | \boldsymbol{e}_i$ if $i \in [1, n]$, or $0 | \boldsymbol{e}_i$ otherwise, where $\boldsymbol{e}_i \in \mathbb{Z}_p^{n+4}$ is the i-th unit vector. Then, randomly choose a tag $\tau \in \{0,1\}^N$ and generate $n+4$ signatures $\sigma_1, \cdots, \sigma_{n+4}$ of the LHS on the vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_{n+4}$ under the tag τ. $sk_{\mathbf{x}}$ consists of all of the signatures. To sign a message $M \in \mathbb{Z}_p$ under a vector $\mathbf{y} \in \mathbb{Z}_p^n$ and a range $[L, R] \subseteq \mathbb{Z}_p$, we set $n+4$ number of weight coefficients $\beta_1, \cdots, \beta_{n+4}$ as $\beta_i := y_i$ for each $i \in [1, n]$, and $(\beta_{n+1}, \beta_{n+2}, \beta_{n+3}, \beta_{n+4}) := (L, R, M, 1)$. Then, derive a new signature $\overline{\sigma}$ on the linear combination $\overline{\boldsymbol{v}} := \sum_{i=1}^{n+4} \beta_i \boldsymbol{v}_i$. Note that $\overline{\boldsymbol{v}}$ is in the form of $(\langle \mathbf{x}, \mathbf{y} \rangle \pmod{p}, y_1, \cdots, y_n, L, R, M, 1)$. Finally, under the witness of $\langle \mathbf{x}, \mathbf{y} \rangle$, τ and $\overline{\sigma}$, generate an NIWI proof π that both of the following two conditions are satisfied, namely (1) $\overline{\sigma}$ *is a correct LHS signature on* $\overline{\boldsymbol{v}}$ *under* τ, and (2) $\langle \mathbf{x}, \mathbf{y} \rangle \in [L, R]$. In the GS NIWI system, the prover computes a commitment for each variable, then generates proofs that the variables satisfy a pairing-product equation in a form of $\prod_{i=1}^{m} e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^{m} \prod_{j=1}^{m} e(\mathcal{X}_i, \mathcal{X}_j)^{a_{ij}} = t_T$, where $\mathcal{X}_i \in \mathbb{G}$ are variables and $\mathcal{A}_i \in \mathbb{G}$, $a_{ij} \in \mathbb{Z}_p$ and $t_T \in \mathbb{G}_T$ are constants. Actually, the verification algorithm of the simplified ALP LHS scheme consists of only two such equations. Thus, proving for the 1st condition (1) is non-problematic. To prove for the 2nd condition (2), we adopt the tree-based range membership technique used for efficient time-specific encryption/signatures constructions [21,13].

In our 2nd scheme, each secret-key $sk_{\mathbf{x}}$ consists of only four LHS signatures $\sigma_1, \cdots, \sigma_4$ on vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_4$. Each $\boldsymbol{v}_i \in \mathbb{Z}_p^{n+4}$ is set to $(x_1, \cdots, x_n) | \boldsymbol{e}_i$ if $i = 1$, or $(0, \cdots, 0) | \boldsymbol{e}_i$ otherwise, where $\boldsymbol{e}_i \in \mathbb{Z}_p^4$ is the i-th unit vector. At signature generation, we derive a signature $\overline{\sigma}$ on $\overline{\boldsymbol{v}} := \sum_{i=1}^{4} \beta_i \boldsymbol{v}_i$, where $(\beta_1, \beta_2, \beta_3, \beta_4) := (1, L, R, M)$. Note that $\overline{\boldsymbol{v}} = (x_1, \cdots, x_n, 1, L, R, M) \in \mathbb{Z}_p^{n+4}$. Finally, under the witness of $\langle \mathbf{x}, \mathbf{y} \rangle$, τ, $\overline{\sigma}$ and $\mathbf{x}$, generate an NIWI proof that all of the following three conditions are satisfied, namely (1) $\overline{\sigma}$ *is a correct LHS signature on* $\overline{\boldsymbol{v}}$ *under* τ, (2) $\langle \mathbf{x}, \mathbf{y} \rangle \in [L, R]$ and (3) $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i \cdot y_i \pmod{p}$.

Applications of ARIP. Since ARIP is a generalization of AIP, any ABS primitive which can be transformed from AIP, can also be transformed from ARIP. And not only that, for some of such primitives, ARIP can transform into more generalized primitives. The first example is ABS for *range* evaluation of polynomials (AREP), which is a generalization of the ABS for evaluation of polynomial. In AREP, each signature is labeled with a polynomial $f : \mathbb{Z}_p \to \{0,1\}$ and a range $[L, R] \subseteq \mathbb{Z}_p$. A secret-key with $x \in \mathbb{Z}_p$ correctly signs iff $f(x) \in [L, R] \pmod{p}$. Another example is ABS for *range* evaluation of weighted average (resp. fuzzy identity-based signatures), which is a generalization of the ABS for evaluation of weighted averages (resp. the ABS for exact thresholds). Moreover, ARIP can be transformed into the following (original) ABS, namely time-specific signatures

[21,13], ABS for range of Hamming/Euclidean distance, and ABS for hypersphere/hyperellipsoid predicates. For the details, refer to Sect. 5.

Further Related Work. The idea of ABS was proposed by Maji et al. [17,18]. They proposed a generic construction, supporting monotone span programs as predicate, based on a non-interactive proof system and a digital signature scheme. Okamoto and Takashima [20] proposed an ABS scheme supporting non-monotone span programs as predicate based on the technique of dual pairing vector spaces. Sakai et al. [24] proposed an ABS scheme supporting arbitral circuits as predicate, built from the GS proof [11] and the structure-preserving signatures by Kiltz et al. [16]. Sakai et al. [25] proposed key-policy ABS for any deterministic Turing machines as predicate. Zhang et al. [27] proposed an ABS scheme for inner products, secure under a lattice assumption of Short Integer Solution problem in the random oracle model. In ABE for *non-zero* inner products [15], unlike ABE for inner products [15], the decryption succeeds iff the inner product is non-zero. A lot of secure schemes based on bilinear maps [3,4,19] or lattice assumptions [14] have been proposed. Phuong et al. [22] proposed a secure construction of edit distance based encryption (EdDBE). In EdDBE, each secret-key (resp. ciphertext) is associated with an alphabet string A (resp. an alphabet string A' and a threshold value t). The decryption succeeds iff the edit distance (aka. Levenshtein distance) between A and A' is smaller than t. Guo et al. [12] proposed the notion of Euclidean distance based encryption (EuDBE). In EuDBE, each secret-key (resp. ciphertext) is associated with a vector $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathbb{R}^n$ (resp. a vector $\boldsymbol{y} = (y_1, \cdots, y_n) \in \mathbb{R}^n$ and a threshold $t \in \mathbb{R}$) with a real number space $\mathbb{R}$. The decryption succeeds iff the Euclidean distance between $\boldsymbol{x}$ and $\boldsymbol{y}$ is smaller than t[4]. They proposed a generic EuDBE construction from any ABE for inner products [15].

Paper Organization. In Sect. 2, we explain some notations and define the CDH, FlexCDH and DLIN assumptions. In Sect. 3, we define the syntax and security of ABS for a general predicate f and ARIP. In Sect. 4, we propose two ARIP schemes and its optimized versions in terms of efficiency. In Sect. 5, we explain that ARIP has many applications. In Sect. 6, we summarize the paper, then discuss possible functional developments of ARIP.

2 Preliminaries

Notations. For $\lambda \in \mathbb{N}$, 1^λ denotes a security parameter. A function $f : \mathbb{N} \rightarrow \mathbb{R}$ is negligible if for every $c \in \mathbb{N}$, there exists $x_0 \in \mathbb{N}$ s.t. for every $x \geq x_0$, $f(x) \leq x^{-c}$. Given a binary string $x \in \{0,1\}^L$, for every $i \in [0, L-1]$, let $x[i] \in \{0,1\}$ denote its i-th bit. PPTA means probabilistic polynomial time algorithm. For a set A, $a \overset{\mathrm{U}}{\leftarrow} A$ means that an element a is chosen uniformly at random from A.

[4] The EuDBE is similar to the encryption analogue of our ABS for range of Euclidean distance, but more functionally-restricted than it, because in the latter, not only the upper bound R (of the Euclidean distance) but also the lower bound L can be chosen.

2.1 Symmetric Bilinear Pairing on Groups with Prime Order

$\mathcal{G}$ takes a security parameter 1^λ with $\lambda \in \mathbb{N}$ and outputs a group description $(p, \mathbb{G}, \mathbb{G}_T, e, g)$. p is a prime with length λ. $\mathbb{G}$ and $\mathbb{G}_T$ are multiplicative groups with order p. g is a generator of $\mathbb{G}$. $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is an efficiently-computable function which satisfies both of the following conditions.

Bilinearity. For any $a, b \in \mathbb{Z}_p$, $e(g^a, g^b) = e(g, g)^{ab}$
Non-degeneracy. $e(g, g) \neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ denotes the unit element of $\mathbb{G}_T$.

Assumptions. We define the three computational hardness assumptions.

Definition 1. *The computational Diffie-Hellman (CDH) assumption holds on the group $\mathbb{G}$ if for every PPT $\mathcal{A}$, $\texttt{Adv}^{\texttt{CDH}}_{\mathcal{A},\mathbb{G}}(\lambda) := \Pr[g^{ab} \leftarrow \mathcal{A}(g, g^a, g^b)]$ with $a, b \xleftarrow{\text{U}} \mathbb{Z}_p$, is negligible.*

Definition 2. *The flexible CDH (FlexCDH) assumption [6] holds on the group $\mathbb{G}$ if for every PPT $\mathcal{A}$, $\texttt{Adv}^{\texttt{FlexCDH}}_{\mathcal{A},\mathbb{G}}(\lambda) := \Pr[(g^\mu, g^{a\cdot\mu}, g^{ab\cdot\mu}) \leftarrow \mathcal{A}(g, g^a, g^b)]$ with $a, b \xleftarrow{\text{U}} \mathbb{Z}_p$ and $\mu \neq 0$, is negligible.*

Definition 3. *The decisional linear (DLIN) assumption holds on the group $\mathbb{G}$ if for every PPT $\mathcal{A}$, $\texttt{Adv}^{\texttt{DLIN}}_{\mathcal{A},\mathbb{G}}(\lambda) := |\Pr[1 \leftarrow \mathcal{A}(g^a, g^b, g^{ab}, g^{bd}, g^{c+d})]| - \Pr[1 \leftarrow \mathcal{A}(g^a, g^b, g^{ab}, g^{bd}, g^z)]$ with $a, b, c, d, z \xleftarrow{\text{U}} \mathbb{Z}_p$, is negligible.*

3 ABS for Range of Inner-Product (ARIP)

We define general ABS for predicate f in the first subsection, then show that ARIP is a concrete example of the general ABS in the second subsection.

3.1 General ABS for Predicate f

General ABS for predicate $f : \{0,1\}^* \to \{0,1\}$ in $\mathcal{F}$ consists of the following four polynomial-time algorithms. `Ver` is deterministic and the others are probabilistic.

Setup `Setup`: It takes a security parameter 1^λ for $\lambda \in \mathbb{N}$, then outputs a public parameter pp and master-key mk. Let $\mathcal{M}$ denote the message space. Note that the other algorithms implicitly take pp as input. $[(pp, mk) \leftarrow \texttt{Setup}(1^\lambda)]$
Key-Generation `KGen`: It takes mk and an attribute $x \in \{0,1\}^*$, then outputs a secret-key sk. $[sk \leftarrow \texttt{KGen}(mk, x)]$
Signing `Sig`: It takes a secret-key sk, a message $M \in \mathcal{M}$, a predicate $f \in \mathcal{F}$, then outputs a signature σ. $[\sigma \leftarrow \texttt{Sig}(sk, M, f)]$
Verification `Ver`: It takes a signature σ, a message $M \in \mathcal{M}$, a predicate $f \in \mathcal{F}$, then outputs 1 or 0. $[1/0 \leftarrow \texttt{Ver}(\sigma, M, f)]$

Every ABS scheme must be correct. Informally the property means that every correctly generated signature is accepted. Formally the property is defined as follows. An ABS scheme is correct if $\forall\lambda \in \mathbb{N}$, $\forall(pp, mk) \leftarrow \mathtt{Setup}(1^\lambda)$, $\forall x \in \{0,1\}^*$, $\forall sk \leftarrow \mathtt{KGen}(mk, x)$, $\forall M \in \mathcal{M}$, $\forall f \in \mathcal{F}$ s.t. $1 \leftarrow f(x)$, $\forall\sigma \leftarrow \mathtt{Sig}(sk, M, f)$, $1 \leftarrow \mathtt{Ver}(\sigma, M, f)$ holds.

As security for ABS, we require unforgeability and signer-privacy. As a notion of unforgeability, we define *(weak) existential unforgeability against adaptively-chosen messages and predicate attack* (EUF-CMA). For a PPT algorithm $\mathcal{A}$, we consider the following experiment.

```
$\boldsymbol{Expt}^{\texttt{EUF-CMA}}_{\Sigma_{\text{ABS}},\mathcal{A}}(1^\lambda)$:
  1. $(pp, mk) \leftarrow \mathtt{Setup}(1^\lambda)$. $(\sigma^*, M^* \in \mathcal{M}, f^* \in \mathcal{F}) \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(pp)$.
      - $\mathfrak{Reveal}(x \in \{0,1\}^*)$: $sk \leftarrow \mathtt{KGen}(mk, x)$. $Q := Q \cup \{x\}$. **Rtrn** $sk$.
      - $\mathfrak{Sign}(x \in \{0,1\}^*, M \in \mathcal{M}, f \in \mathcal{F})$: $sk \leftarrow \mathtt{KGen}(mk, x)$. $\sigma \leftarrow \mathtt{Sig}(sk, M, f)$.
          $Q' := Q' \cup \{(M, f, \sigma)\}$. **Rtrn** $\sigma$.
  2. **Rtrn** 1 if (1) $1 \leftarrow \mathtt{Ver}(\sigma^*, M^*, y^*)$, (2) $\forall x \in Q$, $0 \leftarrow f^*(x)$ and (3) $(M^*, f^*, \cdot) \notin Q'$. **Rtrn** 0.
```

Definition 4. *An ABS scheme Σ_{ABS} is EUF-CMA if for every $\lambda \in \mathbb{N}$ and every PPT $\mathcal{A}$, $\mathcal{A}$'s advantage $\boldsymbol{Adv}^{\textit{EUF-CMA}}_{\Sigma_{\text{ABS}},\mathcal{A}}(\lambda) := \Pr[1 \leftarrow \boldsymbol{Expt}^{\textit{EUF-CMA}}_{\Sigma_{\text{ABS}},\mathcal{A}}(1^\lambda)]$ is negligible.*

As a notion of signer-privacy, we define perfect signer-privacy (PRV). For a probabilistic algorithm $\mathcal{A}$, we consider the following two experiments.

```
$\boldsymbol{Expt}^{\texttt{PRV}}_{\Sigma_{\text{ABS}},\mathcal{A},0}(1^\lambda)$: // $\boldsymbol{Expt}^{\texttt{PRV}}_{\Sigma_{\text{ABS}},\mathcal{A},1}$
  $(pp, mk) \leftarrow \mathtt{Setup}(1^\lambda)$. $(pp, mk, \mu) \leftarrow \mathtt{SimSetup}(1^\lambda)$. **Rtrn** $b' \leftarrow \mathcal{A}^{\mathfrak{Reveal},\mathfrak{Sign}}(pp, mk)$.
      - $\mathfrak{Reveal}(x \in \{0,1\}^*)$: $sk \leftarrow \mathtt{KGen}(mk, x)$. $sk \leftarrow \mathtt{SimKGen}(mk, \mu, x)$. $Q := Q \cup \{(x, sk)\}$. **Rtrn** $sk$.
      - $\mathfrak{Sign}(x \in \{0,1\}^*, sk, M \in \mathcal{M}, f \in \mathcal{F})$:
          **Rtrn** $\perp$ if $(x, sk) \notin Q \vee 0 \leftarrow f(x)$. $\sigma \leftarrow \mathtt{Sig}(sk, M, f)$. $\sigma \leftarrow \mathtt{SimSig}(mk, \mu, M, f)$. **Rtrn** $\sigma$.
```

The latter is associated with 3 polynomial-time algorithms $\{$SimSetup, SimKGen, SimSig$\}$. The grey parts are considered in the latter, but ignored in the former.

Definition 5. *An ABS scheme Σ_{ABS} is perfectly signer-private (PRV) if for every $\lambda \in \mathbb{N}$ and every probabilistic algorithm $\mathcal{A}$, there exist polynomial-time algorithms $\{$SimSetup, SimKGen, SimSig$\}$ such that $\mathcal{A}$'s advantage $\boldsymbol{Adv}^{\textit{PRV}}_{\Sigma_{\text{ABS}},\mathcal{A}}(\lambda) := |\sum_{b=0}^{1}(-1)^b \Pr[1 \leftarrow \boldsymbol{Expt}^{\textit{PRV}}_{\Sigma_{\text{ABS}},\mathcal{A},b}(1^\lambda)]|$ is 0.*

3.2 ARIP

ARIP is a sub-class of the general ABS for predicate f. p denotes a prime number of bit length λ. $n \in \mathbf{poly}(\lambda)$ is an integer. An attribute $x \in \{0,1\}^*$ in the general ABS is changed into an n-dimensional vector $\mathbf{x} \in \mathbb{Z}_p^n$ in ARIP. A predicate $f \in \mathcal{F}$ is associated with an n-dimensional vector $\mathbf{y} \in \mathbb{Z}_p^n$ and a range $[L, R]$ with $L, R \in \mathbb{Z}_p$. We parse $\mathbf{x}$ (resp. $\mathbf{y}$) as $(x_1, \cdots, x_n)$ (resp. $(y_1, \cdots, y_n)$). The predicate outputs 1 if (and only if) $\langle\mathbf{x}, \mathbf{y}\rangle(:= \sum_{i=1}^{n} x_i \cdot y_i) \in [L, R] \pmod{p}$.

4 Our ARIP Schemes

Non-Interactive Witness-Indistinguishable Proof (NIWI). An NIWI system by Groth and Sahai (GS) [11], based on a group $\mathbb{G}$ whose order is a prime p, is secure under the DLIN assumption. The CRS consists of 3 vectors $\vec{f}_1, \vec{f}_2, \vec{f}_3 \in \mathbb{G}^3$, where $\vec{f}_1 = (f_1, 1, g)$, $\vec{f}_2 = (1, f_2, g)$ and $f_1, f_2 \in \mathbb{G}$. A commitment $\vec{C}$ to a group element $X \in \mathbb{G}$ is given as $\vec{C} := (1, 1, X) \cdot \vec{f}_1^{\,r} \cdot \vec{f}_2^{\,s} \cdot \vec{f}_3^{\,t}$, where $r, s, t \xleftarrow{\mathrm{U}} \mathbb{Z}_p$. The CRS is in one of the following two settings, (1) perfect soundness setting and (2) perfect witness-indistinguishability (WI) setting. The CRS in the former setting satisfies $\vec{f}_3 = \vec{f}_1^{\,\xi_1} \cdot \vec{f}_2^{\,\xi_2}$ with $\xi_1, \xi_2 \in \mathbb{Z}_p$. From any commitment $\vec{C} = (f_1^{r+\xi_1 t}, f_2^{s+\xi_2 t}, X \cdot g^{r+s+t(\xi_1+\xi_2)})$ distributing as a Boneh-Boyen-Shacham (BBS) ciphertext [8], the committed variable X is extracted by using $\beta_1 = \log_g(f_1)$ and $\beta_2 = \log_g(f_2)$. In the latter setting, where the element $\vec{f}_3$ is chosen outside the span of $\vec{f}_1$ and $\vec{f}_2$, any commitment is perfectly hiding. In the GS NIWI system, the prover can efficiently prove that committed variables satisfy a paring-product equation in the form of $\prod_{i=1}^{m} e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^{m} \prod_{j=1}^{m} e(\mathcal{X}_i, \mathcal{X}_j)^{a_{ij}} = t_T$ for variables $\mathcal{X}_i \in \mathbb{G}$ and constants $\mathcal{A}_i \in \mathbb{G}$, $a_{ij} \in \mathbb{Z}_p$ and $t_T \in \mathbb{G}_T$. Definitions of the syntax and security notions for NIWI, namely perfect witness-indistinguishability and perfect (witness-)extractability, are given in Subsect. A.1.

Linearly Homomorphic Signatures (LHS) [9]. In LHS, each signature on a message of vector $\boldsymbol{v} \in \mathbb{Z}_p^n$ is labeled with a tag $\tau \in \{0,1\}^N$. Any entity collecting l number of signatures $\sigma_1, \cdots, \sigma_l$ labeled with the same tag τ on messages $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_l \in \mathbb{Z}_p^n$ can derive a new signature $\overline{\sigma}$ on any linear combination $\overline{\boldsymbol{v}} = \sum_{i=1}^{l} \beta_i \cdot \boldsymbol{v}_i \in \mathbb{Z}_p^n$ with $\beta_i \in \mathbb{Z}_p$. The unforgeability security informally means that no PPT adversary, given q number of signatures $\{\sigma_i\}_{i=1}^{q}$ with $q \in \mathbf{poly}(\lambda)$ on arbitrarily and adaptively chosen vectors $\{\boldsymbol{v}_i\}_{i=1}^{q}$ with tags $\{\tau_i\}_{i=1}^{q}$, can find a correct signature on a vector $\boldsymbol{v}^* \notin V_{\tau^*}$ on a tag τ^* with a non-negligible probability, where V_{τ^*} denotes the subspace spanned by all of the vectors $\boldsymbol{v}_i$ s.t. $\tau_i = \tau^*$. Attrapadung, Libert and Peters (ALP) [6] proposed unforgeable and complete context-hiding (CCH) secure scheme, based on the CDH and FlexCDH assumptions. The CCH notion [5] and a weaker notion called strong context-hiding (SCH) [2] are unlinkability-related notions, which guarantee that any derived signature (from some of the other signatures) distributes identically to a fresh signature directly generated by the signing-key. Our ARIP schemes do not need these unlinkablity notions. We consider the following simplified variant of the ALP LHS scheme lacking CCH security. The verification-key includes group elements $g, v, \{g_i\}_{i=1}^{n}, u'$ and $\{u_i\}_{i=0}^{N-1}$. The signing-key is $\alpha \in \mathbb{Z}_p$. A signature on $\boldsymbol{v} \in \mathbb{Z}_p^n$ under a tag $\tau \in \{0,1\}^N$ distributes as $((\prod_{i=1}^{n} g_i^{v_i} v^s)^{\alpha} H_{\mathbb{G}}(\tau)^r, g^r, g^s, g^{s \cdot \alpha})$ with randomnesses $r, s \xleftarrow{\mathrm{U}} \mathbb{Z}_p$, where $H_{\mathbb{G}}(\tau) = u' \prod_{i=0}^{N-1} u_i^{\tau[i]}$. The definitions of unforgeability, CCH and SCH are given in Subsect. A.2, and the simplified variant of the ALP LHS scheme is described in Sect. B.

4.1 Our First ARIP Scheme

Generic Construction Based on NIWI and LHS. A secret-key $sk_{\mathbf{x}}$ for $\mathbf{x} \in \mathbb{Z}_p^n$ consists of a tag $\tau \in \{0,1\}^N$ for $N \in \mathbb{N}$ and $n+4$ signatures $\{\sigma_i\}_{i=1}^{n+4}$ of LHS. The tag is uniform-randomly chosen for each secret-key. The LHS signature σ_i is on a vector $\boldsymbol{v}_i \in \mathbb{Z}_p^{n+5}$. Each vector $\boldsymbol{v}_i$ is set to $x_i|\boldsymbol{e}_i$ if $i \in [1,n]$, or $0|\boldsymbol{e}_i$ otherwise, where $\boldsymbol{e}_i \in \mathbb{Z}_p^{n+4}$ is the i-th unit vector. The signer with $sk_{\mathbf{x}}$ signs a message $M \in \mathbb{Z}_p$ under a vector $\mathbf{y} \in \mathbb{Z}_p^n$ and a range $[L,R]$ with $L,R \in \mathbb{Z}_p$ as follows. Compute the weights $\beta_1,\cdots,\beta_{n+4} \in \mathbb{Z}_p$ as follows. β_i for $i \in [1,n]$ is set to y_i. β_i for $i \in [n+1,n+4]$ is set to L, R, M, and 1, respectively. Derive an LHS signature $\overline{\sigma}$ on the weighted vector $\overline{\boldsymbol{v}} := \sum_{i=1}^{n+4} \beta_i \cdot \boldsymbol{v}_i = (\langle \mathbf{x},\mathbf{y}\rangle \pmod p, y_1,\cdots, y_n, L, R, M, 1) \in \mathbb{Z}_p^{n+5}$. Finally, using $\langle \mathbf{x},\mathbf{y}\rangle$, τ and $\overline{\sigma}$ as witness, generate NIWI proofs that both of the following two conditions are satisfied, namely (a) *$\overline{\sigma}$ is a correct signature on the vector $\overline{\boldsymbol{v}}$ under the tag τ* and (b) $\langle \mathbf{x},\mathbf{y}\rangle \in [L,R]$. Since the verification algorithm of the simplified variant of the ALP LHS scheme consists of only two pairing-product equations, generating GS proofs for the first condition (a) is non-problematic. For the second condition (b), we adopt the tree-based range membership technique used for the efficient constructions of time-specific encryption/signatures [21,13].

Formal Description. For any $X \in \mathbb{G}$, $\iota(X)$ denotes $(1,1,X) \in \mathbb{G}^3$. For any $X \in \mathbb{G}_T$, $\iota_{\mathbb{G}_T}(X)$ denotes the 3×3 matrix which has X as the $(3,3)$-th element and $1_{\mathbb{G}_T}$ as any of the other elements. For any $h, g_1, g_2, g_3 \in \mathbb{G}$, $E(h,(g_1,g_2,g_3))$ denotes $(e(h,g_1), e(h,g_2), e(h,g_3)) \in \mathbb{G}_T^3$. For any $\overrightarrow{X} = (X_1,X_2,X_3) \in \mathbb{G}^3$ and $\overrightarrow{Y} = (Y_1,Y_2,Y_3) \in \mathbb{G}^3$, $F(\overrightarrow{X},\overrightarrow{Y}) := \tilde{F}(\overrightarrow{X},\overrightarrow{Y})^{1/2} \cdot \tilde{F}(\overrightarrow{Y},\overrightarrow{X})^{1/2} \in \mathbb{G}_T^{3\times 3}$, where $\tilde{F}(\overrightarrow{X},\overrightarrow{Y}) \in \mathbb{G}_T^{3\times 3}$ contains $e(X_i,Y_j)$ as the (i,j)-th element for all $i,j \in \{1,2,3\}$.

`Setup`$(1^\lambda, n)$**:** Choose bilinear groups $(\mathbb{G},\mathbb{G}_T)$ whose order is a prime p of bit length λ. Conduct the following steps.

1. Choose $\alpha \xleftarrow{\text{U}} \mathbb{Z}_p$. Choose $g, v, g_1, \cdots, g_{n+5} \xleftarrow{\text{U}} \mathbb{G}$.
2. Choose $u', u_0, \cdots, u_{N-1} \xleftarrow{\text{U}} \mathbb{G}$ for $N \in \mathbb{N}$. We define $H_{\mathbb{G}} : \{0,1\}^N \to \mathbb{Z}_p$ as a function which takes $\tau \in \{0,1\}^N$ and outputs $u' \prod_{i=0}^{N-1} u_i^{\tau[i]} \in \mathbb{G}$.
3. Generate a GS CRS $\boldsymbol{f} = (\overrightarrow{f}_1, \overrightarrow{f}_2, \overrightarrow{f}_3)$ for the perfect WI setting as $\overrightarrow{f}_1 := (f_1,1,g)$, $\overrightarrow{f}_2 := (1,f_2,g)$ and $\overrightarrow{f}_3 := \overrightarrow{f}_1^{\xi_1} \cdot \overrightarrow{f}_2^{\xi_2} \cdot (1,1,g)^{-1}$, where $f_1, f_2 \xleftarrow{\text{U}} \mathbb{G}, \xi_1, \xi_2 \xleftarrow{\text{U}} \mathbb{Z}_p$.

Output (pp, mk), where $pp := (\mathbb{G}, \mathbb{G}_T, g, g^\alpha, v, \{g_i\}_{i=1}^{n+5}, u', \{u_i\}_{i=0}^{N-1}, \boldsymbol{f})$ and $mk := \alpha$.

`KGen`$(mk, \mathbf{x})$**:** Choose a tag $\tau \xleftarrow{\text{U}} \{0,1\}^N$. Conduct the following steps.

1. Generate $n+4$ vectors $\boldsymbol{v}_i \in \mathbb{Z}_p^{n+5}$ as follows. For each $i \in [1,n]$,

$$\boldsymbol{v}_i := (x_i, \underbrace{\underbrace{0,\cdots,0}_{i-1},1,\underbrace{0,\cdots,0}_{n-i}}_{n},\underbrace{0,0,0,0}_{4}).$$

The others are

$$\begin{aligned}\boldsymbol{v}_{n+1} &:= (0,0,\cdots,0,1,0,0,0),\\ \boldsymbol{v}_{n+2} &:= (0,0,\cdots,0,0,1,0,0),\\ \boldsymbol{v}_{n+3} &:= (0,0,\cdots,0,0,0,1,0),\end{aligned}$$

$$\boldsymbol{v}_{n+4} := (0, \underbrace{0, \cdots, 0}_{n}, \underbrace{0, 0, 0, 1}_{4}).$$

Each vector is parsed as $(v_{i,1}, \cdots, v_{i,n+5})$ with $v_{i,j} \in \mathbb{Z}_p$ for all $j \in [1, n+5]$.

2. Compute an ALP signature $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4})$ on $\boldsymbol{v}_i$ as follows.

$$(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4}) := \left(\prod_{j=1}^{n+5} g_i^{v_{i,j}} v^{s_i})^{\alpha} H_{\mathbb{G}}(\tau)^{r_i}, g^{r_i}, g^{s_i}, g^{\alpha \cdot s_i} \right),$$

where $r_i, s_i \overset{\mathrm{U}}{\longleftarrow} \mathbb{Z}_p$.

Output the secret-key $sk := (\mathbf{x}, \tau, \{\{\sigma_{i,j}\}_{j=1}^{4}\}_{i=1}^{n+4})$.

`Sig`$(sk, M, \mathbf{y}, L, R)$**:** Conduct the following five steps first.

1. Calculate the inner product $d := \langle \mathbf{x}, \mathbf{y} \rangle \pmod p$. Assume that $d \in [L, R]$.
2. Choose $\overline{r} \overset{\mathrm{U}}{\longleftarrow} \mathbb{Z}_p$. For each $i \in [1, n]$, $\beta_i := y_i$. Set $(\beta_{n+1}, \beta_{n+2}, \beta_{n+3}, \beta_{n+4}) := (L, R, M, 1)$. Derive a new ALP signature $(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4)$ as

$$\left(\prod_{i=1}^{n+4} \sigma_{i,1}^{\beta_i} \cdot H_{\mathbb{G}}(\tau)^{\overline{r}}, \prod_{i=1}^{n+4} \sigma_{i,2}^{\beta_i} \cdot g^{\overline{r}}, \prod_{i=1}^{n+4} \sigma_{i,3}^{\beta_i}, \prod_{i=1}^{n+4} \sigma_{i,4}^{\beta_i} \right).$$

Note that if sk is a correct secret-key with inner-randomness $\{r_j, s_j\}_{j=1}^{n+4}$, the computed ALP signature distributes as

$$\left(\left\{ g_1^{\langle \mathbf{x}, \mathbf{y} \rangle} \cdot \prod_{i=1}^{n} g_{i+1}^{y_i} \cdot g_{n+2}^{L} \cdot g_{n+3}^{R} \cdot g_{n+4}^{M} \cdot g_{n+5} \cdot v^{\sum_{j=1}^{n+4} y_j s_j} \right\}^{\alpha} H_{\mathbb{G}}(\tau)^{\sum_{j=1}^{n+4} y_j r_j + \overline{r}}, \right.$$
$$\left. g^{\sum_{j=1}^{n+4} y_j r_j + \overline{r}}, g^{\sum_{j=1}^{n+4} y_j s_j}, g^{\alpha \sum_{j=1}^{n+4} y_j s_j} \right). \qquad (1)$$

3. Compute the GS commitments for all of the following variables in $\mathbb{G}$.
   (a) $g^{\tau[i]}$ and $g^{1-\tau[i]}$
   (for all $i \in [0, N-1]$)
   (b) $H_{\mathbb{G}}(\tau)$
   (c) $g_1^{d[i]}$ and $g_1^{1-d[i]}$
   (for all $i \in [0, \lambda-1]$)
   (d) g_1^{d}
   (e) $\overline{\sigma}_1, \overline{\sigma}_3$ and $\overline{\sigma}_4$

   Let the commitments be denoted by $\vec{C}_{\tau[i]}$, $\vec{C}_{1-\tau[i]}$, $\vec{C}_{H_{\mathbb{G}}(\tau)}$, $\vec{C}_{d[i]}$, $\vec{C}_{1-d[i]}$, $\vec{C}_{d}$, $\vec{C}_{\overline{\sigma}_1}$, $\vec{C}_{\overline{\sigma}_3}$, $\vec{C}_{\overline{\sigma}_4} \in \mathbb{G}^3$ respectively. The GS commitment $\vec{C}_X$ for a variable $X \in \mathbb{G}$ is computed as $\iota(X) \cdot \vec{f}_1^{\,r} \cdot \vec{f}_2^{\,s} \cdot \vec{f}_3^{\,t}$, where $r, s, t \overset{\mathrm{U}}{\longleftarrow} \mathbb{Z}_p$.
4. Compute the GS proofs that the variables satisfy the following relations.
   [a] $e(g^{\tau[i]}, g^{1-\tau[i]}) = 1_{\mathbb{G}_T}$ and $e(g^{\tau[i]}, g) \cdot e(g^{1-\tau[i]}, g) = e(g, g)$
   (for all $i \in [0, N-1]$)
   [b] $e(H_{\mathbb{G}}(\tau), g) = e(u', g) \prod_{i=0}^{N-1} e(u_i, g^{\tau[i]})$

[c] $e(g_1^{d[i]}, g_1^{1-d[i]}) = 1_{\mathbb{G}_T}$ and $e(g_1^{d[i]}, g_1) \cdot e(g_1^{1-d[i]}, g_1) = e(g_1, g_1)$
(for all $i \in [0, \lambda - 1]$)

[d] $e(g_1^{d}, g) = \prod_{i=0}^{\lambda-1} e(g_1^{d[i]}, g^{2^i})$

[e] $e(\overline{\sigma}_1, g) = e(g_1^{d}, g^{\alpha}) \cdot e(\prod_{i=1}^{n+4} g_{i+1}^{y_i}, g^{\alpha}) \cdot e(v, \overline{\sigma}_4) \cdot e(H_{\mathbb{G}}(\tau), \overline{\sigma}_2)$

[f] $e(\overline{\sigma}_3, g^{\alpha}) = e(g, \overline{\sigma}_4)$

The relations [a] guarantee that the variable $\tau[i]$ used in the committed variables $g^{\tau[i]}$ and $g^{1-\tau[i]}$ is one bit value. Likewise, the ones [c] guarantee that the variable $d[i]$ is one bit value. The above GS proofs are categorized into two groups, namely type-1 (resp. type-2) proofs consisting of 3 (resp. 9) elements in $\mathbb{G}$. Specifically, the proofs for the relations with the grey background ▨ are type-2, and the others are type-1. Let the proofs be denoted by $\vec{\pi}_{\tau[i]} \in \mathbb{G}^9$, $\vec{\pi}'_{\tau[i]} \in \mathbb{G}^3$, $\vec{\pi}_{H_{\mathbb{G}}(\tau)} \in \mathbb{G}^3$, $\vec{\pi}_{d[i]} \in \mathbb{G}^9$, $\vec{\pi}'_{d[i]} \in \mathbb{G}^3$, $\vec{\pi}_{d} \in \mathbb{G}^3$, $\vec{\pi}_{\overline{\sigma}_1} \in \mathbb{G}^3$, $\vec{\pi}_{\overline{\sigma}_3} \in \mathbb{G}^3$, respectively.

What remains is proving that $d \in [L, R]$.

Consider a complete binary tree with p leaf nodes. The root node is associated with the null value. Any non-leaf node associated with a binary value $a \in \{0,1\}^{\leq \lambda}$ has two subordinates associated with $a||0$ and $a||1$ respectively. The p leaf nodes are associated with $0, 1, \cdots, p-1$ from left to right.

We derive a set of intermediate nodes Θ which *covers* two leaf nodes L and R. For an intermediate node with $\theta \in \{0,1\}^{\leq \lambda}$, $\mathbf{LEAVES}_{\theta}$ denotes a set of leaf nodes, each of which is descendant of the node with θ. The covering set Θ consists of nodes with $\theta \in \{0,1\}^{\leq \lambda}$ such that (1) *the union set of* $\mathbf{LEAVES}_{\theta}$ *for all* $\theta \in \Theta$ *is identical to the set of leaf nodes for* $[L, R]$, and (2) *the cardinality of* Θ*, i.e.,* $|\Theta|$*, is the minimum*[5]. Parse Θ as $\{\theta \in \{0,1\}^{\leq \lambda}\}$.

For each θ, we define a Boolean variable $A_{\theta} \in \{0,1\}$ as follows.

[A_{θ} :] *Be* 1 *if the leaf node with* $d \in \{0,1\}^{\lambda}$ *is descendant of the leaf node with* $\theta \in \{0,1\}^{\leq \lambda}$. *Be* 0 *otherwise.*

Note that if $d \in [L, R]$, there must exist (at most) one node $\theta^* \in \Theta$ which has the leaf node d as descendant. The highest $|\theta^*|$ bits of d are identical to θ^*. For each $\theta \in \Theta$ and $j \in [1, |\theta|]$, we define two Boolean variables $A_{\theta,j}, A'_{\theta,j} \in \{0,1\}$ as follows.

[$A_{\theta,j}$:] *Be* 1 *if the* j*-th highest bit of* $d \in \{0,1\}^{\lambda}$ *is identical to the one of* $\theta \in \{0,1\}^{\leq \lambda}$*, i.e.,* $d[\lambda - j] = \theta[|\theta| - j]$. *Be* 0 *otherwise.*

[$A'_{\theta,j}$:] *Be* 1 *if all of the* j *highest bits of* $d \in \{0,1\}^{\lambda}$ *are identical to the ones of* $\theta \in \{0,1\}^{\leq \lambda}$*, i.e.,* $d[\lambda - k] = \theta[|\theta| - k]$ *for all* $k \in [1, j]$. *Be* 0 *otherwise. Obviously,* $A'_{\theta,|\theta|} = A_{\theta}$.

Finally, conduct the following two steps.

1. Compute the GS commitments for all of the following variables in $\mathbb{G}$.

   (f) $g_1^{A_{\theta}}$
   (for all $\theta \in \Theta$)

   (g) $g_1^{A_{\theta,j}}$ and $g_1^{A'_{\theta,j}}$
   (for all $\theta \in \Theta$ and $j \in [1, |\theta|]$)

   Let the commitments be denoted by $\vec{C}_{A_{\theta}}, \vec{C}_{A_{\theta,j}}, \vec{C}'_{A_{\theta,j}} \in \mathbb{G}^3$.

[5] Note that $|\Theta|$ is maximized when $[L, R] = [1, p-2]$ and becomes $2\lambda - 2$.

2. Compute the GS proofs that the above variables satisfy the followings.

   [g] $e(g_1^{A_{\theta,j}}, g) = \begin{cases} e(g_1^{d[\lambda-j]}, g) & (\text{if } \theta[|\theta|-j]=1) \\ e(g_1^{1-d[\lambda-j]}, g) & (\text{otherwise}) \end{cases}$

   (for all $\theta \in \Theta$ and $j \in [1, |\theta|]$)

   [h] $e(g_1^{A'_{\theta,1}}, g_1) = e(g_1^{A_{\theta,1}}, g_1)$

   (for all $\theta \in \Theta$)

   [i] $e(g_1^{A'_{\theta,j}}, g_1) = e(g_1^{A'_{\theta,j-1}}, g_1^{A_{\theta,j}})$

   (for all $\theta \in \Theta$ and $j \in [2, |\theta|]$)

   [j] $\prod_{\theta\in\Theta} e(g_1^{A'_{\theta,|\theta|}}, g) = e(g_1, g)$

   Let the computed GS proofs be denoted by $\pi_{A_{\theta,j}} \in \mathbb{G}^3$, $\vec{\pi}'_{A_{\theta,1}} \in \mathbb{G}^3$, $\vec{\pi}'_{A_{\theta,j}} \in \mathbb{G}^9$ and $\pi_A \in \mathbb{G}^3$ respectively.

The signature σ consists of all of the GS commitments and proofs, and the second ALP signature element $\overline{\sigma}_2 \in \mathbb{G}$.

`Ver`$(\sigma, M, \mathbf{y}, L, R)$**:** Each GS proof $\pi \in \mathbb{G}^3$ (resp. $\vec{\pi} \in \mathbb{G}^9$), composed of 3 (resp. 9) elements in $\mathbb{G}$, is parsed as (π_1, π_2, π_3) (resp. $(\vec{\pi}_1, \vec{\pi}_2, \vec{\pi}_3)$ with $\vec{\pi}_i \in \mathbb{G}^3$). Output 1 if all of the following equations are satisfied.

1. $F(\vec{C}_{\tau[i]}, \vec{C}_{1-\tau[i]}) = \iota_{\mathbb{G}_T}(1_{\mathbb{G}_T}) \cdot \prod_{k=1}^{3} F(\vec{\pi}_{\tau[i],k}, \vec{f}_k)$

   (for all $i \in [0, N-1]$)
2. $E(g, \vec{C}_{\tau[i]}) \cdot E(g, \vec{C}_{1-\tau[i]}) = E(g, \iota(g)) \cdot \prod_{k=1}^{3} E(\pi'_{\tau[i],k}, \vec{f}_k)$

   (for all $i \in [0, N-1]$)
3. $E(g, \vec{C}_{H_{\mathbb{G}}(\tau)}) = E(u', \iota(g)) \cdot \prod_{i=0}^{N-1} E(u_i, \vec{C}_{\tau[i]}) \cdot \prod_{k=1}^{3} E(\pi_{H_{\mathbb{G}}(\tau),k}, \vec{f}_k)$
4. $F(\vec{C}_{d[i]}, \vec{C}_{1-d[i]}) = \iota_{\mathbb{G}_T}(1_{\mathbb{G}_T}) \cdot \prod_{k=1}^{3} F(\vec{\pi}_{d[i],k}, \vec{f}_k)$

   (for all $i \in [0, \lambda-1]$)
5. $E(g, \vec{C}_{d[i]}) = E(g, \iota(g)) \cdot E(g, \vec{C}_{1-d[i]}) \cdot \prod_{k=1}^{3} E(\pi'_{d[i],k}, \vec{f}_k)$

   (for all $i \in [0, \lambda-1]$)
6. $E(g, \vec{C}_d) = \prod_{i=0}^{\lambda-1} E(g^{2^i}, \vec{C}_{d[i]}) \cdot \prod_{k=1}^{3} E(\pi_{d,k}, \vec{f}_k)$
7. $E(g, \vec{C}_{\overline{\sigma}_1}) = E(g^\alpha, \vec{C}_d) \cdot E(\prod_{i=1}^{n+4} g_{i+1}^{y_i}, \iota(g^\alpha)) \cdot E(v, \vec{C}_{\overline{\sigma}_4}) \cdot E(\overline{\sigma}_2, \vec{C}_{H_{\mathbb{G}}(\tau)}) \cdot \prod_{k=1}^{3} E(\pi_{\overline{\sigma}_1,k}, \vec{f}_k)$
8. $E(g^\alpha, \vec{C}_{\overline{\sigma}_3}) = E(g, \vec{C}_{\overline{\sigma}_4}) \cdot \prod_{k=1}^{3} E(\pi_{\overline{\sigma}_3,k}, \vec{f}_k)$
9. $E(g, \vec{C}_{A_{\theta,j}}) = \begin{cases} E(g, \vec{C}_{d[\lambda-j]}) \cdot \prod_{k=1}^{3} E(\pi_{A_{\theta,j},k}, \vec{f}_k) & (\text{if } \theta[|\theta|-j]=1) \\ E(g, \vec{C}_{1-d[\lambda-j]}) \cdot \prod_{k=1}^{3} E(\pi_{A_{\theta,j},k}, \vec{f}_k) & (\text{otherwise}) \end{cases}$

   (for all $\theta \in \Theta$ and $j \in [1, |\theta|]$)
10. $E(g_1, \vec{C}'_{A_{\theta,1}}) = E(g_1, \vec{C}_{A_{\theta,1}}) \cdot \prod_{k=1}^{3} E(\pi'_{A_{\theta,1},k}, \vec{f}_k)$

    (for all $\theta \in \Theta$)
11. $F(\iota(g_1), \vec{C}'_{A_{\theta,j}}) = F(\vec{C}'_{A_{\theta,j-1}}, \vec{C}_{A_{\theta,j}}) \cdot \prod_{k=1}^{3} F(\vec{\pi}'_{A_{\theta,j},k}, \vec{f}_k)$

    (for all $\theta \in \Theta$ and $j \in [2, |\theta|]$)
12. $\prod_{\theta\in\Theta} E(g, \vec{C}'_{A_{\theta,|\theta|}}) = E(g_1, \iota(g)) \cdot \prod_{k=1}^{3} E(\pi_{A,k}, \vec{f}_k)$

Output 0 otherwise.

Unforgeability. We present the following theorem.

Theorem 1. *Our 1st ARIP scheme is* `EUF-CMA` *if the DLIN, CDH and FlexCDH assumptions hold in the group* $\mathbb{G}$.

Proof. To prove the theorem, we define the following 5 experiments.

Expt$_0$**:** The standard $\texttt{EUF-CMA}$ experiment for the ARIP scheme.
Expt$_1$**:** The same as ***Expt***$_0$ except that it aborts when we choose a tag on the key-revelation or signing oracle, the tag matches a tag previously chosen.
Expt$_2$**:** The same as ***Expt***$_1$ except that the ALP signature $(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4)$ used on the signing oracle $\mathfrak{Sign}$ is directly generated by the master-key $mk (= \alpha)$ as follows.

$$\left(\left\{ g_1^{\langle \mathbf{x},\mathbf{y}\rangle} \prod_{i=1}^{n} g_{i+1}^{y_i} \cdot g_{n+2}^{L} \cdot g_{n+3}^{R} \cdot g_{n+4}^{M} \cdot g_{n+5} \cdot v^{s} \right\}^{\alpha} \cdot H_{\mathbb{G}}(\tau)^{r}, g^{r}, g^{s}, g^{\alpha s}\right),$$

where $r, s \xleftarrow{\text{U}} \mathbb{Z}_p$ and $\tau \xleftarrow{\text{U}} \{0,1\}^N$.
Expt$_3$**:** The same as ***Expt***$_2$ except that the GS CRS $\boldsymbol{f} = (\vec{f}_1, \vec{f}_2, \vec{f}_3)$ is generated as a perfectly sound one. Specifically, $\vec{f}_1 := (f_1, 1, g)$, $\vec{f}_2 := (1, f_2, g)$ and $\vec{f}_3 := \vec{f}_1^{\xi_1} \cdot \vec{f}_2^{\xi_2}$, where $f_1 := g^{\phi_1}$, $f_2 := g^{\phi_2}$ and $\phi_1, \phi_2, \xi_1, \xi_2 \xleftarrow{\text{U}} \mathbb{Z}_p$. Note that in this experiment and the next experiment ***Expt***$_4$, all GS commitments are perfectly binding ones. We use the BBS decryption keys (ϕ_1, ϕ_2) to extract all of the hidden variables from the GS commitments in the forged signature σ^*. Since the GS proofs in σ^* are perfectly sound, the extracted variables satisfy all of the relations [a], [b], $\cdots$, [j]. Hereafter, some of the extracted variables are denoted by $\tau^* \in \{0,1\}^N$, $d^* \in \mathbb{Z}_p$, $\overline{\sigma}_1^*, \overline{\sigma}_3^*, \overline{\sigma}_4^* \in \mathbb{G}$. Let $\overline{\sigma}_2^* \in \mathbb{G}$ denote the 2nd ALP signature element included in σ^*.
Expt$_4$**:** The same as ***Expt***$_3$ except that it aborts if the tag τ^* matches none of the tags chosen on the key-revelation or signing oracle.

W_i denotes the event where ***Expt***$_i$ outputs 1. We obtain

$$\texttt{Adv}^{\texttt{EUF-CMA}}_{\Sigma_{\text{ARIP}},\mathcal{A},n}(\lambda) = \Pr[W_0] \leq \sum_{i=1}^{4} |\Pr[W_{i-1}] - \Pr[W_i]| + \Pr[W_4]$$

$$\leq q(q-1)/2^{N+1} + \texttt{Adv}^{\texttt{DLIN}}_{\mathcal{B}_1,\mathbb{G}}(\lambda) + 4q(N+1)(\texttt{Adv}^{\texttt{CDH}}_{\mathcal{B}_2,\mathbb{G}}(\lambda) + \texttt{Adv}^{\texttt{FlexCDH}}_{\mathcal{B}_3,\mathbb{G}}(\lambda) + 2/p),$$

where $q \in \mathbb{N}$ is number that $\mathcal{A}$ uses the key-revelation and signing oracles. The last inequality is because of the following lemmas. We omit the proof of Lemma 3 which is obviously true. □

Lemma 1. *$|\Pr[W_0] - \Pr[W_1]| \leq q(q-1)/2^{N+1}$.*

Proof. For $i \in [1, q]$, τ_i denotes the tag chosen on the i-th key-revelation or signing oracle. E_i denotes the event where τ_i is the first tag which matches one of the tags previously chosen. ***Expt***$_0$ and ***Expt***$_1$ are identical except for the case where an event from $E_2, \cdots, E_q$ occurs. Thus, we obtain $|\Pr[W_0] - \Pr[W_1]| \leq \Pr[\bigvee_{i=2}^{q} E_i] \leq \sum_{i=2}^{q} \Pr[E_i]$. We derive an upper bound for $\Pr[E_i]$. A denotes the event where no one from $\tau_1, \cdots, \tau_{i-1}$ matches another. B denotes the event where τ_i matches one of $\tau_1, \cdots, \tau_{i-1}$. Obviously, $\Pr[E_i] = \Pr[A] \cdot \Pr[B \mid A] \leq \Pr[B \mid A] = \frac{i-1}{2^N}$. Hence, $|\Pr[W_0] - \Pr[W_1]| \leq \frac{1}{2^N} + \cdots + \frac{q-1}{2^N} = \frac{1}{2^N} \cdot \frac{q(q-1)}{2} = \frac{q(q-1)}{2^{N+1}}$. □

Lemma 2. *$|\Pr[W_1] - \Pr[W_2]| = 0$.*

Proof. In $\boldsymbol{Expt}_1$, on the signing oracle, a secret-key $sk_{\mathbf{x}}$ for $\mathbf{x} \in \mathbb{Z}_p^n$ is generated. Parse $sk_{\mathbf{x}}$ as $(\mathbf{x}, \tau, \{\{\sigma_{ij}\}_{j=1}^4\}_{i=1}^{n+4})$. For each $i \in [1, n+4]$, $r_i, s_i \in \mathbb{Z}_p$ denote the randomness used for the ALP signature $\{\sigma_{ij}\}_{j=1}^4$. Using $sk_{\mathbf{x}}$, we generate a signature σ on M associated with $\mathbf{y} \in \mathbb{Z}_p^n$ and $L, R \in \mathbb{Z}_p$. Let $\overline{\sigma} = (\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4)$ denote the ALP signature generated during the generation of σ. $\overline{\sigma}$ is expressed as follows, where $\overline{r} \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p$.

$$\Bigg(\left\{ g_1^{\langle \mathbf{x}, \mathbf{y} \rangle} \cdot \prod_{i=1}^{n} g_{i+1}^{y_i} \cdot g_{n+2}^{L} \cdot g_{n+3}^{R} \cdot g_{n+4}^{M} \cdot g_{n+5} \cdot v^{\sum_{i=1}^{n+4} y_i s_i} \right\}^{\alpha} \cdot H_{\mathbb{G}}(\tau)^{\sum_{i=1}^{n+4} y_i r_i + \overline{r}},$$
$$g^{\sum_{i=1}^{n+4} y_i r_i + \overline{r}}, g^{\sum_{i=1}^{n+4} y_i s_i}, g^{(\sum_{i=1}^{n+4} y_i s_i)\alpha} \Bigg)$$

Since any information about $\{r_i, s_i\}_{i=1}^{n+4}$ is not revealed to $\mathcal{A}$, both $\sum_{i=1}^{n+4} y_i r_i$ and $\sum_{i=1}^{n+4} y_i s_i$ distribute uniformly at random in $\mathbb{Z}_p$. Hence, $\overline{\sigma}$ in $\boldsymbol{Expt}_1$ distributes identically to the one in $\boldsymbol{Expt}_2$. □

Lemma 3. *There is a PPTA $\mathcal{B}_1$ s.t. $|\Pr[W_2] - \Pr[W_3]| \le \boldsymbol{Adv}_{\mathcal{B}_1, \mathbb{G}}^{\mathtt{DLIN}}(\lambda)$.*

Lemma 4. *There is a PPTA $\mathcal{B}_2$ s.t. $|\Pr[W_3] - \Pr[W_4]| \le 4q(N+1)(\boldsymbol{Adv}_{\mathcal{B}_2, \mathbb{G}}^{\mathtt{CDH}}(\lambda) + 1/p)$.*

Proof. E denotes the event where $\mathcal{A}$ makes $\boldsymbol{Expt}_3$ output 1. F denotes the event where $\mathcal{A}$ makes $\boldsymbol{Expt}_4$ abort. By a basic theorem, $\Pr[E] - \Pr[E \wedge \neg F] = \Pr[E \wedge F]$. Since $\Pr[E] = \Pr[W_3]$ and $\Pr[E \wedge \neg F] = \Pr[W_4]$, we obtain $\Pr[W_3] - \Pr[W_4] = \Pr[E \wedge F]$. Assume that $\mathcal{A}$ is a PPTA which makes the event $E \wedge F$ occur with a non-negligible probability. Let $\mathcal{B}_2$ be a PPTA who attempts to solve the CDH problem by using $\mathcal{A}$. $\mathcal{B}_2$ behaves as follows.

Receive (g, g^a, g^b) as an instance of the CDH problem. Conduct the following four steps.

1. Set $l := 2q$. Choose uniformly at random an integer k satisfying $0 \le k \le N$. Assume that $l(N+1) \le p$.
2. Set $g^{\alpha} := g^a$. Choose $\kappa_v, \kappa_1, \delta_1, \cdots, \kappa_{n+5}, \delta_{n+5} \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p$. Set $v := g^{\kappa_v}$ and $g_i := (g^b)^{\kappa_i} g^{\delta_i}$ for $i \in [1, n+5]$.
3. Choose $x', x_0, \cdots, x_{N-1} \overset{\text{U}}{\longleftarrow} \mathbb{Z}_l$ and $y', y_0, \cdots, y_{N-1} \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p$. For a tag $\tau \in \{0,1\}^N$, define two functions $F, J : \{0,1\}^N \to \mathbb{Z}_p$ as $F(\tau) := x' + \sum_{i=0}^{N-1} x_i \cdot \tau[i] - lk$ and $J(\tau) := y' + \sum_{i=0}^{N-1} y_i \cdot \tau[i]$. Set $u' := (g^b)^{-lk+x'} \cdot g^{y'}$ and $u_i := (g^b)^{x_i} \cdot g^{y_i}$ for $i \in [0, N-1]$. It holds that $u' \prod_{i=0}^{N-1} u_i^{\tau[i]} = (g^b)^{-lk+x'+\sum_{i=0}^{N-1} x_i \cdot \tau[i]} \cdot g^{y'+\sum_{i=0}^{N-1} y_i \cdot \tau[i]} = (g^b)^{F(\tau)} \cdot g^{J(\tau)}$.
4. Generate the GS CRS $\boldsymbol{f} = (\vec{f}_1, \vec{f}_2, \vec{f}_3)$ as perfectly sound one.

Set $pp := (\mathbb{G}, \mathbb{G}_T, g, g^{\alpha}, v, \{g_i\}_{i=1}^{n+5}, u', \{u_i\}_{i=0}^{N-1}, \boldsymbol{f})$ and send it to $\mathcal{A}$. When $\mathcal{A}$ issues a query to the key-revelation or signing oracle, $\mathcal{B}_2$ behaves as follows.

Key-Revelation $\mathfrak{Reveal}(\mathbf{x})$: Let $\tau \overset{\text{U}}{\longleftarrow} \{0,1\}^N$. Consider the following two cases, (1) $F(\tau) \neq 0 \pmod{l}$ and (2) $F(\tau) = 0 \pmod{l}$. If the case (2) occurs, abort the simulation. If the case (1) occurs, continue as follows. Since we have assumed that $l(N+1) < p$ and $0 \leq k \leq N$, it holds that $F(\tau) = 0 \pmod{p} \implies F(\tau) = 0 \pmod{l}$ for any τ. Its contraposition is that $F(\tau) \neq 0 \pmod{l} \implies F(\tau) \neq 0 \pmod{p}$ for any τ.
Choose $r \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p$. Compute $(d_1, d_2) := ((g^\alpha)^{-\frac{J(\tau)}{F(\tau)}}(u' \prod_{i=0}^{N-1} u_i^{\tau[i]})^r, (g^\alpha)^{-\frac{1}{F(\tau)}} g^r)$. Let $\tilde{r} := r - \alpha/F(\tau)$. Obviously, $d_2 = g^{\tilde{r}}$. It holds that $d_1 = (g^b)^\alpha H_{\mathbb{G}}(\tau)^{\tilde{r}}$ since $d_1 = (g^b)^\alpha \{(g^b)^{F(\tau)} g^{J(\tau)}\}^{-\frac{\alpha}{F(\tau)}} \{(g^b)^{F(\tau)} g^{J(\tau)}\}^r = (g^b)^\alpha H_{\mathbb{G}}(\tau)^{r - \frac{\alpha}{F(\tau)}}$.
Generate $n+4$ vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_{n+4} \in \mathbb{Z}_p^{n+5}$ in the normal manner. For each $i \in [1, n+4]$, generate an ALP signature $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4})$ as

$$\left(d_1^{\sum_{j=1}^{n+5} \kappa_j v_{ij}} (g^\alpha)^{s_i \kappa_v + \sum_{j=1}^{n+5} \delta_j v_{ij}} H_{\mathbb{G}}(\tau)^{r_i}, d_2^{\sum_{j=1}^{n+5} \kappa_j v_{ij}} g^{r_i}, g^{s_i}, (g^\alpha)^{s_i} \right),$$

where $r_i, s_i \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p$. Let $\hat{r}_i := \tilde{r} \sum_{j=1}^{n+5} \kappa_j v_{ij} + r_i$. Obviously, $\sigma_{i,2} = g^{\hat{r}_i}$. It holds that $\sigma_{i,1} = (\prod_{j=1}^{n+5} g_j^{v_{ij}} v^{s_i})^\alpha H_{\mathbb{G}}(\tau)^{\hat{r}_i}$ since

$$\begin{aligned} \sigma_{i,1} &= (g^{b\alpha})^{\sum_{j=1}^{n+5} \kappa_j v_{ij}} \cdot H_{\mathbb{G}}(\tau)^{\tilde{r} \sum_{j=1}^{n+5} \kappa_j v_{ij} + r_i} \cdot (g^\alpha)^{s_i \kappa_v + \sum_{j=1}^{n+5} \delta_j v_{ij}} \\ &= \{(g^b)^{\sum_{j=1}^{n+5} \kappa_j v_{ij}} g^{s_i \kappa_v + \sum_{j=1}^{n+5} \delta_j v_{ij}}\}^\alpha H_{\mathbb{G}}(\tau)^{\hat{r}_i} = \left[\prod_{j=1}^{n+5} \{(g^b)^{\kappa_j} g^{\delta_j}\}^{v_{ij}} g^{s_i \kappa_v} \right]^\alpha H_{\mathbb{G}}(\tau)^{\hat{r}_i}. \end{aligned}$$

Finally, return $sk_{\mathbf{x}} := (\mathbf{x}, \tau, \{\{\sigma_{ij}\}_{j=1}^4\}_{i=1}^{n+4})$ to $\mathcal{A}$.

Signing $\mathfrak{Sign}(\mathbf{x}, M, \mathbf{y}, L, R)$: Compute $d := \langle \mathbf{x}, \mathbf{y} \rangle \pmod{p}$. Choose $\tau \overset{\text{U}}{\longleftarrow} \{0,1\}^L$. If $F(\tau) = 0 \pmod{l}$, abort the simulation. Else if $F(\tau) \neq 0 \pmod{l}$, as the key-revelation oracle, $\mathcal{B}_2$ derives the variables (d_1, d_2), then an ALP signature $(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4)$ on the vector $\overline{\boldsymbol{v}} = (d, y_1, \cdots, y_n, L, R, M, 1)$. In the normal manner, compute all of the GS commitments and proofs. Return a signature σ, composed of all of the GS commitments/proofs and $\overline{\sigma}_2$, to $\mathcal{A}$.

$\mathcal{B}_2$ receives a forged signature σ^* from $\mathcal{A}$. Set $\boldsymbol{v}^* := (d^*, y_1^*, \cdots, y_n^*, L^*, R^*, M^*, 1) \in \mathbb{Z}_p^{n+5}$. Parse it as $(v_1^*, \cdots, v_{n+5}^*)$. The ALP signature $(\overline{\sigma}_1^*, \overline{\sigma}_2^*, \overline{\sigma}_3^*, \overline{\sigma}_4^*)$ extracted from the forged signature σ^* satisfies that $\overline{\sigma}_1^* = (\prod_{i=1}^{n+5} g_i^{v_i^*} v^{s^*})^\alpha H_{\mathbb{G}}(\tau^*)^{r^*}$, $\overline{\sigma}_2^* = g^{r^*}$, $\overline{\sigma}_3^* = g^{s^*}$ and $\overline{\sigma}_4^* = g^{s^* \cdot \alpha}$ for some $r^*, s^* \in \mathbb{Z}_p$.

We assume that it holds $\kappa_{n+5} \neq -\sum_{i=1}^{n+4} \kappa_i v_i^* \pmod{p}$, which implies $\sum_{i=1}^{n+5} \kappa_i v_i^* \neq 0 \pmod{p}$. Since κ_{n+5} has not been used yet from $\mathcal{A}$'s viewpoint and κ_{n+5} has been chosen uniformly at random from $\mathbb{Z}_p$, the probability that $\kappa_{n+5} = -\sum_{i=1}^{n+4} \kappa_i v_i^* \pmod{p}$ is at most $1/p$. Hence, this assumption is reasonable.

Compute (ω_1^*, ω_2^*) as

$$\left(\left\{ \frac{\overline{\sigma}_1^*}{(\overline{\sigma}_4^*)^{\kappa_v} (g^\alpha)^{\sum_{i=1}^{n+5} \delta_i v_i^*}} \right\}^{1/\sum_{i=1}^{n+5} \kappa_i v_i^*}, \{\overline{\sigma}_2^*\}^{1/\sum_{i=1}^{n+5} \kappa_i v_i^*} \right).$$

Let $\tilde{r}^* := r^*/\sum_{i=1}^{n+5}\kappa_i v_i^*$. Obviously, $\omega_2^* = g^{\tilde{r}^*}$. It holds $\omega_1^* = g^{ab}H_{\mathbb{G}}(\tau^*)^{\tilde{r}^*}$ since

$$\omega_1^* = \left\{\frac{(\prod_{i=1}^{n+5} g_i^{v_i^*} v^{s^*})^{\alpha} H_{\mathbb{G}}(\tau^*)^{r^*}}{(g^{\alpha})^{s^*\kappa_v + \sum_{i=1}^{n+5}\delta_i v_i^*}}\right\}^{1/\sum_{i=1}^{n+5}\kappa_i v_i^*} = \left[\frac{\{\prod_{i=1}^{n+5}(g^{b\kappa_i}g^{\delta_i})^{v_i^*} g^{s^*\kappa_v}\}^{\alpha} H_{\mathbb{G}}(\tau^*)^{r^*}}{(g^{\alpha})^{s^*\kappa_v + \sum_{i=1}^{n+5}\delta_i v_i^*}}\right]^{1/\sum_{i=1}^{n+5}\kappa_i v_i^*}$$

$$= \left\{(g^{b\alpha})^{\sum_{i=1}^{n+5}\kappa_i v_i^*} H_{\mathbb{G}}(\tau^*)^{r^*}\right\}^{1/\sum_{i=1}^{n+5}\kappa_i v_i^*} = g^{ab}H_{\mathbb{G}}(\tau^*)^{r^*/\sum_{i=1}^{n+5}\kappa_i v_i^*}.$$

Consider the following two cases, (1) $F(\tau^*) = 0 \pmod p$ and (2) $F(\tau^*) \neq 0 \pmod p$. If the second case occurs, abort the simulation. If the first occurs, $\mathcal{B}_2$ outputs $\frac{\omega_1^*}{(\omega_2^*)^{J(\tau^*)}}$, which is equivalent to $\frac{g^{ab}H_{\mathbb{G}}(\tau^*)^{\tilde{r}^*}}{(g^{\tilde{r}^*})^{J(\tau^*)}} = g^{ab}$ because $H_{\mathbb{G}}(\tau^*) = (g^b)^{F(\tau^*)}g^{J(\tau^*)} = g^{J(\tau^*)}$, as the correct answer to the CDH problem.

Consider a situation where $\mathcal{B}_2$ has not aborted and $\mathcal{A}$ has made $E \wedge F$ occur. Except for the case where $\kappa_{n+5} = \sum_{i=1}^{n+4}\kappa_i v_i^* \pmod p$ which occurs with the probability $1/p$ at most, $\mathcal{B}_2$ outputs the correct answer for the CDH problem. Thus, it holds $\Pr[E \wedge F \wedge \neg\mathsf{abort}] - \mathtt{Adv}^{\mathtt{CDH}}_{\mathcal{B}_2,\mathbb{G}}(\lambda) \leq 1/p$, where abort is the event where $\mathcal{B}_2$ aborts the simulation. The first term is equivalent to $\Pr[\neg\mathsf{abort}]\cdot\Pr[E \wedge F \mid \neg\mathsf{abort}] = \Pr[\neg\mathsf{abort}]\cdot\Pr[E\wedge F]$. We obtain $\Pr[E\wedge F] \leq \frac{1}{\Pr[\neg\mathsf{abort}]}(\mathtt{Adv}^{\mathtt{CDH}}_{\mathcal{B}_2,\mathbb{G}}(\lambda) + \frac{1}{p})$. In the same manner as [26], the lower bound of $\Pr[\neg\mathsf{abort}]$ is derived, i.e., $\frac{1}{4q(N+1)}$. Details of the derivation are described in Subsect. C. □

Lemma 5. *There is a PPTA $\mathcal{B}_3$ s.t.* $\Pr[W_4] \leq 4q(N+1)(\mathit{Adv}^{\mathit{FlexCDH}}_{\mathcal{B}_3,\mathbb{G}}(\lambda) + 1/p)$.

Proof. Assume that $\mathcal{A}$ is a PPT algorithm which makes $\boldsymbol{Expt}_4$ outputs 1 with a non-negligible probability. Let $\mathcal{B}_3$ be a PPT simulator who attempts to solve the FlexCDH problem by using $\mathcal{A}$.

Receive (g, g^a, g^b) as an instance of the FlexCDH problem. As the proof of Lemma 4, compute the variables $l, k, \kappa_1, \delta_1, \cdots, \kappa_{n+5}, \delta_{n+5}, x', x_0, y_0, \cdots, x_{N-1}, y_{N-1}$ and $\boldsymbol{f}$, and define the functions F and J.

Set $g^{\alpha} := g^a$, $v := g^b$, $g_i := (g^b)^{\kappa_i}g^{\delta_i}$, $u' := (g^a)^{-lk+x'} \cdot g^{y'}$ and $u_i := (g^a)^{x_i} \cdot g^{y_i}$ for $i \in [0, N-1]$. It holds that $u'\prod_{i=0}^{N-1} u_i^{\tau[i]} = (g^a)^{F(\tau)} \cdot g^{J(\tau)}$. Set $pp := (\mathbb{G}, \mathbb{G}_T, g, g^{\alpha}, v, \{g_i\}_{i=1}^{n+5}, u', \{u_i\}_{i=0}^{N-1}, \boldsymbol{f})$ and send it to $\mathcal{A}$. When $\mathcal{A}$ issues a query to the key-revelation or signing oracle, $\mathcal{B}_3$ behaves as follows.

Key-Revelation $\mathfrak{Reveal}(\mathbf{x})$: Choose $\tau \in \{0,1\}^N$. Generate the $n+4$ vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_{n+4} \in \mathbb{Z}_p^{n+5}$ in the normal way. As the proof of the previous lemma, consider the following two cases.

(1) $F(\tau) \neq 0 \pmod l$**:** For each $i \in [1, n+4]$, generate an ALP signature $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4})$ as $((g^a)^{\sum_{j=1}^{n+5}\delta_j v_{ij}}(g^b)^{-\frac{J(\tau)}{F(\tau)}(\sum_{j=1}^{n+5}\kappa_j v_{ij}+s_i)}H_{\mathbb{G}}(\tau)^{r_i}, (g^b)^{-\frac{\sum_{j=1}^{n+5}\kappa_j v_{ij}+s_i}{F(\tau)}}g^{r_i}, g^{s_i}, (g^{\alpha})^{s_i})$, where $r_i, s_i \xleftarrow{\mathrm{U}} \mathbb{Z}_p$. Let $\tilde{r}_i := r_i - b\frac{\sum_{j=1}^{n}\kappa_j v_{ij}+s_i}{F(\tau)}$. Obviously, $\sigma_{i,2} = g^{\tilde{r}_i}$. The ALP signature correctly distributes since $(\prod_{j=1}^{n+5} g_j^{v_{ij}} \cdot v^{s_i})^{\alpha} \cdot H_{\mathbb{G}}(\tau)^{\tilde{r}_i} = [\prod_{j=1}^{n+5}\{(g^b)^{\kappa_j}g^{\delta_j}\}^{v_{ij}} \cdot (g^b)^{s_i}]^{\alpha} \cdot H_{\mathbb{G}}(\tau)^{r_i - b\frac{\sum_{j=1}^{n}\kappa_j v_{ij}+s_i}{F(\tau)}} = \cancel{\{(g^b)^{\sum_{j=1}^{n+5}\kappa_j v_{ij}+s_i}}\}^{\alpha}\cdot(g^{\sum_{j=1}^{n+5}\delta_j v_{ij}})^{\alpha}\cdot H_{\mathbb{G}}(\tau)^{r_i}\cdot\cancel{(g^{\alpha})^{-b(\sum_{j=1}^{n+5}\kappa_j v_{ij}+s_i)}}\cdot g^{-b\frac{J(\tau)}{F(\tau)}(\sum_{j=1}^{n+5}\kappa_j v_{ij}+s_i)}$ is equivalent to the above $\sigma_{i,1}$.

(2) $F(\tau) = 0 \pmod{l}$**:** Immediately abort the simulation if this condition has already been satisfied by a tag previously chosen on the key-revelation or signing oracle. For each $i \in [1, n+4]$, choose $r_i \xleftarrow{\text{U}} \mathbb{Z}_p$, set $s_i := -\sum_{j=1}^{n+5} \kappa_j v_{ij}$, then generate an ALP signature $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4})$ as $((g^a)^{\sum_{j=1}^{n+5} \delta_j v_{ij}} H_{\mathbb{G}}(\tau)^{r_i}, g^{r_i}, g^{s_i}, (g^\alpha)^{s_i})$. Since the vectors $\{\boldsymbol{v}_i\}_{i=1}^{n+4}$ are linearly independent and any of $\{\kappa_i\}_{i=1}^{n+5}$ has been chosen randomly from $\mathbb{Z}_p$, any of $\{s_i\}_{i=1}^{n+4}$ distributes randomly in $\mathbb{Z}_p$. The ALP signature correctly distributes since $(\prod_{j=1}^{n+5} g_j^{v_{ij}} \cdot v^{s_i})^\alpha \cdot H_{\mathbb{G}}(\tau)^{r_i} = [\prod_{j=1}^{n+5} \{(g^b)^{\kappa_i} g^{\delta_i}\}^{v_{ij}} \cdot (g^b)^{-\sum_{j=1}^{n+5} \kappa_j v_{ij}}]^\alpha \cdot H_{\mathbb{G}}(\tau)^{r_i}$ is equivalent to the above $\sigma_{i,1}$.

Finally, return $sk_{\mathbf{x}} := (\mathbf{x}, \tau, \{\{\sigma_{ij}\}_{j=1}^4\}_{i=1}^{n+4})$ to $\mathcal{A}$.

Signing $\mathfrak{Sign}(\mathbf{x}, M, \mathbf{y}, L, R)$**:** Compute $d := \langle \mathbf{x}, \mathbf{y} \rangle \pmod{p}$. Choose $\tau \xleftarrow{\text{U}} \{0,1\}^N$. As the key-revelation oracle, consider the mutually exclusive two cases w.r.t. $F(\tau) \in \mathbb{Z}_p$, and in each case compute an ALP signature $(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4)$ on the message $\overline{\boldsymbol{v}} = (d, y_1, \cdots, y_n, L, R, M, 1)$. In the normal manner, compute all of the GS commitments and proofs. Return a signature σ, composed of all of the GS commitments/proofs and $\overline{\sigma}_2$, to $\mathcal{A}$.

$\mathcal{B}_3$ receives a forged signature σ^* from $\mathcal{A}$. Consider the following two cases, namely (1) $F(\tau^*) = 0 \pmod{p}$ and (2) $F(\tau^*) \neq 0 \pmod{p}$. If the case (2) occurs, abort the simulation. If the case (1) occurs, compute the three variables ξ_1, ξ_2, ξ_3 as follows.

$$\begin{aligned}
\xi_1 &:= \overline{\sigma}_3^* \cdot g^{\sum_{j=1}^{n+5} \kappa_j v_j^*} \\
\xi_2 &:= \overline{\sigma}_4^* \cdot (g^\alpha)^{\sum_{j=1}^{n+5} \kappa_j v_j^*} \\
\xi_3 &:= \overline{\sigma}_1^* \cdot (\overline{\sigma}_2^*)^{-J(\tau^*)} \cdot (g^\alpha)^{-\sum_{j=1}^{n+5} \delta_j v_j^*}
\end{aligned}$$

Let $\hat{s}^* := s^* + \sum_{j=1}^{n+5} \kappa_j v_j^*$. Obviously, $\xi_1 := g^{\hat{s}^*}$ and $\xi_2 := g^{a\hat{s}^*}$. It holds that $\xi_3 = [\prod_{i=1}^{n+5} \{(g^b)^{\kappa_i} \cancel{g^{\delta_i}}\}^{v_i^*} \cdot (g^b)^{s^*}]^\alpha \cdot \cancel{H_{\mathbb{G}}(\tau^*)^{r^*}} \cancel{(g^{r^*})^{-J(\tau^*)}} \cdot \cancel{(g^\alpha)^{-\sum_{j=1}^{n+5} \delta_j v_i^*}} = (g^{ab})^{s^* + \sum_{j=1}^{n+5} \kappa_j v_j^*} = g^{ab\hat{s}^*}$.

Thus, (ξ_1, ξ_2, ξ_3) is the correct answer to the FlexCDH problem under an assumption that it holds $\hat{s}^* \neq 0 \pmod{p} \Leftrightarrow s^* \neq -\sum_{j=1}^{n+5} \kappa_j v_j^* \pmod{p}$. This assumption is reasonable since the probability $\Pr[s^* = -\sum_{j=1}^{n+5} \kappa_j v_j^* \pmod{p}]$ is at most $1/p$. As the proof of the previous lemma, we obtain $\Pr[1 \leftarrow \boldsymbol{Expt}_4(1^\lambda, n)] \leq 4q(N+1)(\mathtt{Adv}_{\mathcal{B}_3,\mathbb{G}}^{\mathtt{FlexCDH}}(\lambda) + \frac{1}{p})$. □

Signer-Privacy. We present the following theorem.

Theorem 2. *Our 1st ARIP scheme is perfectly signer-private.*

Proof. $\boldsymbol{Expt}_1$ is associated with the three simulation algorithms `SimSetup`, `SimKGen` and `SimSig`. The first two are the same as the original ones of our scheme[6]. `SimSig` is defined as follows.

[6] The auxiliary variable μ has no information, i.e., $\mu = \text{␣}$

$\texttt{SimSig}(mk, M, \mathbf{y}, L, R)$**:** Arbitrarily choose an attribute $\mathbf{x}^* \in \mathbb{Z}_p^n$ s.t. $\langle \mathbf{x}^*, \mathbf{y} \rangle \pmod{p} \in [L, R]$. Arbitrarily choose $\tau^* \in \{0,1\}^N$. Generate an ALP signature $(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4)$ as $(\{g_1^{\langle \mathbf{x}^*, \mathbf{y} \rangle} \cdot \prod_{i=1}^n g_{i+1}^{y_i} \cdot g_{n+2}^L \cdot g_{n+3}^R \cdot g_{n+4}^M \cdot g_{n+5} \cdot v^s\}^\alpha \cdot H_{\mathbb{G}}(\tau^*)^r, g^r, g^s, g^{\alpha s})$, where $r, s \overset{\mathrm{U}}{\longleftarrow} \mathbb{Z}_p$. As the original signing algorithm, generate all of the GS commitments and proofs. Return a signature, composed of all of the GS commitments/proofs and $\overline{\sigma}_2$.

In $\boldsymbol{Expt}_0$, an ALP signature used to generate a signature on the signing oracle distributes as (1). Its second element $\overline{\sigma}_2$ distributes identically to the one in $\boldsymbol{Expt}_1$ because of $\overline{r} \overset{\mathrm{U}}{\longleftarrow} \mathbb{Z}_p$. Even though the adversary $\mathcal{A}$ directly knows of $\mathbf{x}, \tau$ and indirectly knows of $\{s_i\}_{i=1}^n$, because of the perfect WI of the GS NIWI system, all of the GS commitments (incl. the ones related to $\langle \mathbf{x}, \mathbf{y} \rangle, \tau, \overline{\sigma}_1, \overline{\sigma}_3, \overline{\sigma}_4$) and proofs distribute identically to the ones in $\boldsymbol{Expt}_1$. □

4.2 Efficiency Analysis

We analyze efficiency of our 1st ARIP scheme. Precisely, we calculate (1) bit length of a secret-key, (2) bit length of a signature, and (3) computational cost of signature verification.

(1) Size of Secret-Key. Let $|g|$ denote bit length of an element in $\mathbb{G}$. A secret-key consists of a tag with bit length L and $4(n+4)$ elements in $\mathbb{G}$. Its length is expressed as $|sk| = L + 4(n+4)|g|$[7].

(2) Size of Signature. Each signature consists of 3 types of element, namely the ALP signature element $\overline{\sigma}_2$, GS commitments, and GS proofs. If we denote the bit length of the 3 types of element by s_1, s_2, s_3 respectively, bit length of a signature is $|\sigma| = s_1 + s_2 + s_3$. Obviously, $s_1 = |g|$. Total number of the GS commitments is $\underset{(b),(d),(e)}{\underline{5}} + \underset{(a)}{\underline{2N}} + \underset{(c)}{\underline{2\lambda}} + \underset{(f)}{\underline{|\Theta|}} + \underset{(g)}{\underline{2\sum_{\theta \in \Theta} |\theta|}}$. Note that the blue alphabet below each number indicates the alphabet assigned to each committed variable in the signing algorithm of our ARIP scheme. Both of the two terms $|\Theta|$ and $\sum_{\theta \in \Theta} |\theta|$ are maximized when $[L, R] = [1, p-2]$ and become $2\lambda - 2$ and $(2+3+\cdots+\lambda) \times 2 = \lambda^2 + \lambda - 2$ respectively. As a result, total number of the GS commitments is upper bounded by $2N + 6\lambda + 2\lambda^2 - 1$, which is asymptotically $\mathcal{O}(N + \lambda^2)$. Since each GS commitment consists of 3 group elements, $s_2 = \mathcal{O}(N + \lambda^2)|g|$. Total number of the type-1 (resp. type-2) GS proofs is $4 + N + \lambda + \sum_{\theta \in \Theta} |\theta| + 2$ (resp. $N + \lambda + \sum_{\theta \in \Theta}(|\theta| - 1)$), either of which is asymptotically $\mathcal{O}(N + \lambda^2)$. Since a type-1 (resp. type-2) GS proof consists of 3 (resp. 9) group elements, $s_1 = \mathcal{O}(N + \lambda^2)|g|$. Hence, $|\sigma| = \mathcal{O}(N + \lambda^2)|g|$.

(3) Cost of Verification. We derive total number of multiplication and exponentiation on the group $\mathbb{G}_T$ and calculation of the paring function e. In verification,

[7] Note that bit length of $\mathbf{x} \in \mathbb{Z}_p^n$ is ignored here.

Table 1. Efficiency of Our ARIP Schemes.

Our Schemes	Size of Secret-Key $\lvert sk\rvert$	Size of Signature $\lvert\sigma\rvert$	Cost of Verification		
			# of Mul.	# of Exp.	# of Pair.
The 1st Scheme (Subsect. 4.1)	$N+(4n+16)\lvert g\rvert$	$\mathcal{O}(N+\lambda^2)\lvert g\rvert$	$\mathcal{O}(N+\lambda^2)$		
→ Its Optimization (Subsect. 4.3)	$N+(4n+16)\lvert g\rvert$	$\mathcal{O}(N+\log^2 T)\lvert g\rvert$	$\mathcal{O}(N+\log^2 T)$		
The 2nd Scheme (Subsect. 4.4)	$N+16\lvert g\rvert$	$\mathcal{O}(N+\lambda^2+n)\lvert g\rvert$	$\mathcal{O}(N+\lambda^2+n)$		
→ Its Optimization	$N+16\lvert g\rvert$	$\mathcal{O}(N+\log^2 T+n)\lvert g\rvert$	$\mathcal{O}(N+\log^2 T+n)$		

a verifier checks whether all of the 12 equations hold or not. The verifier conducts following 4 types of calculation, namely (a) *calculation of the function* E, (b) *calculation of* F, (c) *multiplication of two vectors in* $\mathbb{G}_T^3$ *outputted by* E, and (d) *multiplication of two matrices in* $\mathbb{G}_T^{3\times 3}$ *outputted by* F. They require the following number of multiplication, exponentiation and pairing, respectively, (a) $(0,0,3)$, (b) $(9,9,9)$, (c) $(3,0,0)$, and (d) $(9,0,0)$. Total number of the 4 types of calculation executed in one verification is derived as follows.

- $N_a := \underbrace{5N}_{2} + \underbrace{5+N}_{3} + \underbrace{5\lambda}_{5} + \underbrace{4+\lambda}_{6} + \underbrace{8}_{7} + \underbrace{5}_{8} + \underbrace{\sum_{\theta\in\Theta}\sum_{j=1}^{|\theta|} 5}_{9} + \underbrace{5|\Theta|}_{10} + \underbrace{|\Theta|+4}_{12}$
  $= L + 6\lambda + 26 + 6|\Theta| + \sum_{\theta\in\Theta}\sum_{j=1}^{|\theta|} 5$
- $N_b := \underbrace{4N}_{1} + \underbrace{4\lambda}_{4} + \underbrace{\sum_{\theta\in\Theta}\sum_{j=2}^{|\theta|} 5}_{11}$
- $N_c := \underbrace{4N}_{2} + \underbrace{N+3}_{3} + \underbrace{4\lambda}_{5} + \underbrace{\lambda+2}_{6} + \underbrace{6}_{7} + \underbrace{3}_{8} + \underbrace{\sum_{\theta\in\Theta}\sum_{j=1}^{|\theta|} 3}_{9} + \underbrace{3|\Theta|}_{10} + \underbrace{|\Theta|-1+3}_{12}$
  $= 5N + 5\lambda + 16 + 4|\Theta| + \sum_{\theta\in\Theta}\sum_{j=1}^{|\theta|} 3$
- $N_d := \underbrace{3N}_{1} + \underbrace{3\lambda}_{4} + \underbrace{\sum_{\theta\in\Theta}\sum_{j\in[2,|\theta|]} 3}_{11}$

Note that the blue number below each number indicates the identification number assigned to each equation verified in the verification algorithm of our ARIP scheme. Each of them is asymptotically $\mathcal{O}(N+\lambda^2)$. Each of number of multiplication, number of exponentiation and number of pairing per one verification is the linear summation of N_a, N_b, N_c and N_d with coefficients of integers from 0 to 9. Thus, $\mathcal{O}(N+\lambda^2)$.

As a result we obtain the 1st entry in Table 1. The 2nd, 3rd and 4th entries are for the other our schemes explained in later subsections.

4.3 Efficiency Optimization

The prime p is exponentially large in λ. In some applications of ARIP, it is possible that for every vectors $\mathbf{x},\mathbf{y}\in\mathbb{Z}_p$, their inner product $\langle\mathbf{x},\mathbf{y}\rangle$ is upper-bounded by $T-1$ for an integer $T\in\mathbf{poly}(\lambda)$ s.t. $T\ll p$. In this case, our 1st scheme (in Subsect. 4.1) can be optimized in terms of efficiency.

The inner product $d:=\langle\mathbf{x},\mathbf{y}\rangle\in[0,T-1]$ is $\log T\in\mathbb{N}$ bit. Since for every $i\in[\log T,\lambda{-}1]$, $d[i]$ ($=$ the i-th bit of d) must be 0, we do not need to generate the GS commitments $\vec{C}_{d[i]},\vec{C}_{1-d[i]}\in\mathbb{G}^3$ and the related GS proofs $\vec{\pi}_{d[i]},\vec{\pi}'_{d[i]}\in\mathbb{G}^3$. The complete binary tree used to prove that $d\in[L,R]$ has only T leaf nodes associated with 0 to $T-1$ from left to right. Both cardinality of the set Θ (consisting of nodes covering all of the leaf nodes from L to R) and $\sum_{\theta \in \Theta} |\theta|$ are maximized when $[L, R] = [1, \log T - 2]$ and become $2\log T - 2$ and $\log T^2 + \log T - 2$. As a result we obtain the 2nd entry in Table. 1.

4.4 Our 2nd ARIP Scheme with Constant-Size Secret-Keys

We propose another scheme that a trade-off relationship in terms of efficiency holds with our 1st scheme. Its secret-key length is independent of n. In return, any of its signature length and verification cost linearly increases with n.

A secret-key $sk_{\mathbf{x}}$ consists of only four ALP signatures $\sigma_1, \cdots, \sigma_4$ on the following four vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_4 \in \mathbb{Z}_p^{n+4}$.

$$\boldsymbol{v}_1 := (\underbrace{x_1, \cdots, x_n}_{n}, \underbrace{1, 0, 0, 0}_{4}) \tag{2}$$

$$\boldsymbol{v}_2 := (\underbrace{0, \cdots, 0}_{n}, 0, 1, 0, 0) \tag{3}$$

$$\boldsymbol{v}_3 := (\underbrace{0, \cdots, 0}_{n}, 0, 0, 1, 0) \tag{4}$$

$$\boldsymbol{v}_4 := (\underbrace{0, \cdots, 0}_{n}, 0, 0, 0, 1) \tag{5}$$

At signature generation, the signer derives an ALP LHS signature $\overline{\sigma}$ on $\overline{\boldsymbol{v}} := \sum_{i=1}^{4} \beta_i \cdot \boldsymbol{v}_i$, where $(\beta_1, \beta_2, \beta_3, \beta_4) := (1, L, R, M)$. It holds that

$$\overline{\boldsymbol{v}} = (x_1, \cdots, x_n, 1, L, R, M) \in \mathbb{Z}_p^{n+4}.$$

The signer has to compute GS commitments for $x_1, \cdots, x_n \in \mathbb{Z}_p$ and $d (:= \langle \mathbf{x}, \mathbf{y} \rangle) \in \mathbb{Z}_p$ then prove that d is genuinely the inner product of $\mathbf{x}$ and $\mathbf{y}$. Actually, the signer computes GS commitments for g^{x_i} and $g_i^{x_i}$ for all $i \in [1, n]$. Then, the signer computes GS proofs for the following two relations,

– $e(g^{x_i}, g_i) = e(g, g_i^{x_i})$ for all $i \in [1, n]$, and
– $e(g_1^d, g) = \prod_{i=1}^{n} e(g^{x_i}, g_1^{y_i})$.

Moreover, the relation [e] (in our 1st scheme) is modified into $e(\overline{\sigma}_1, g) = e(\prod_{i=1}^{n} g_i^{x_i}, g^{\alpha}) \cdot e(\prod_{i=1}^{4} g_{i+n}^{\beta_i}, g^{\alpha}) \cdot e(v, \overline{\sigma}_4) \cdot e(H_{\mathbb{G}}(\tau), \overline{\sigma}_2)$. The formal description of our 2nd scheme is given in Subsect. D.

Theorem 3. *Our 2nd ARIP scheme is* **EUF-CMA** *if the DLIN, CDH and Flex-CDH assumptions hold in the group* $\mathbb{G}$ *and perfectly signer-private.*

5 Applications of ARIP

Katz et al. [15] showed that attribute-based encryption (ABE) for inner products[8] can be transformed into various ABE primitives, namely (anonymous)

[8] Like ARIP, vectors $\mathbf{x}, \mathbf{y}$ are associated with secret-key and ciphertext respectively. The decryption succeeds if the inner product is 0.

identity-based encryption (IBE), hidden-vector encryption (HVE), the dual version of HVE (= wildcarded IBE [1]), ABE for evaluation of polynomials/weighted averages/CNF and DNF formulas, and ABE for exact thresholds. Based on the same techniques, its digital signature analogue named ABS for inner products can be transformed into identity-based signatures (IBS), hidden-vector signatures (HVS), the dual of HVS (= wildcarded IBS), ABS for evaluation of polynomials/weighted averages/CNF and DNF formulas, and ABS for exact thresholds. Since ARIP is a generalization of the ABS for inner products, it can be transformed into more generalized (or powerful) ABS primitives as follows.

(1) ABS for Range Evaluation of Polynomials (AREP): Assume that the polynomial is univariate. AREP is a sub-class of the general ABS in Subsect. 3.1. The attribute $x \in \{0,1\}^*$ in the general ABS is changed into a single variable $x \in \mathbb{Z}_p$ in AREP. The predicate f_{AREP}, associated with a d-dimensional polynomial ϕ with coefficients $a_d, \cdots, a_0 \in \mathbb{Z}_p$ and a range $[L, R]$ with $L, R \in \mathbb{Z}_p$, is defined as

$$f_{\mathrm{AREP}}(x) := \begin{cases} 1 & (\text{If } \phi(x) := \sum_{i=0}^{d} a_i \cdot x^i \in [L, R] \pmod{p}) \\ 0 & (\text{Otherwise}). \end{cases}$$

An AREP scheme is transformed from any ARIP scheme of $d+1$ dimensions. The vector $\mathbf{x} \in \mathbb{Z}_p^{d+1}$ in ARIP is changed into $(x^d, x^{d-1}, \cdots, x, 1)$. The vector $\mathbf{y} \in \mathbb{Z}_p^{d+1}$ in ARIP is $(a_d, a_{d-1}, \cdots, a_1, a_0)$. The AREP scheme is correct because if $\phi(x) = \sum_{i=0}^{d} a_i \cdot x^i \in [L, R]$ implies $\langle \mathbf{x}, \mathbf{y} \rangle \in [L, R]$. Even if the polynomial is multivariate with t variables, the transformation still works. In this case, we need an ARIP scheme of $(d^t + 1)$ dimensions.

(2) ABS for Range Evaluation of Weighted Average (AREWA): The attribute x consists of t variables $x_1, \cdots, x_t \in \mathbb{Z}_p$. The predicate f_{AREWA}, associated with t coefficients $a_1, \cdots, a_t \in \mathbb{Z}_p$ and a range $[L, R]$ for $L, R \in \mathbb{Z}_p$, is defined as

$$f_{\mathrm{AREWA}}(x_1, \cdots, x_t) := \begin{cases} 1 & (\text{If } \sum_{i=1}^{t} a_i \cdot x_i \in [L, R] \pmod{p}) \\ 0 & (\text{Otherwise}). \end{cases}$$

An AREWA scheme is transformed from an ARIP scheme of $n = t$ dimensions. The vector $\mathbf{x} \in \mathbb{Z}_p^t$ (resp. $\mathbf{y} \in \mathbb{Z}_p^t$) in ARIP is $(x_1, \cdots, x_t)$ (resp. $(a_1, \cdots, a_t)$). The AREWA scheme obviously satisfies the correctness.

(3) Fuzzy IBS (FIBS): This is a generalization of the ABS for exact thresholds. Let A be $\{1, \cdots, l\}$ for $l \in \mathbb{N}$. The attribute x is a set of attributes $S \subseteq A$. The predicate f_{FIBS}, associated with a set of attributes $S' \subseteq A$ and a range $[L, R]$ for $0 \leq L \leq R \leq l$, is defined as

$$f_{\mathrm{FIBS}}(S) := \begin{cases} 1 & (\text{If } |S \cap S'| \in [L, R]) \\ 0 & (\text{Otherwise}). \end{cases}$$

This FIBS is a further generalization of the signature analogue of FIBE [23] since the upper bound R of the overlapped attributes can be set.

Table 2. Efficiency of Existing and Our TSS Schemes.

TSS Schemes	$\lvert pp\rvert$	$\lvert mk\rvert$	$\lvert sk\rvert$	$\lvert\sigma\rvert$	**Assumptions**
FSS-Based [13]	$(2\log T + m + 3)$ $\cdot(\lvert g\rvert + \lvert\tilde{g}\rvert)$	$\lvert g\rvert$	$\mathcal{O}(\log T)\lvert g\rvert$	$(2\log T + 2)\lvert g\rvert$	co-CDH
WIBRS-Based [13]	$\mathcal{O}(\log T)\lvert\tilde{g}\rvert$	$\mathcal{O}(\log T)\lvert g\rvert$	$\mathcal{O}(1)(\lvert g\rvert + \lvert\tilde{g}\rvert)$	$\mathcal{O}(\log^2 T)(\lvert g\rvert + \lvert\tilde{g}\rvert)$	SXDH
Ours 1	$(N+9)\lvert g\rvert$	λ	$(N+20)\lvert g\rvert$	$\mathcal{O}(N + \log^2 T)\lvert g\rvert$	CDH,FlexCDH,DLIN
Ours 2	$(N+8)\lvert g\rvert$	λ	$(N+16)\lvert g\rvert$	$\mathcal{O}(N + \log^2 T)\lvert g\rvert$	CDH,FlexCDH,DLIN

Note: Both of the FSS-based and WIBRS-based schemes [13] use an asymmetric bilinear map $e : \mathbb{G} \times \tilde{\mathbb{G}} \to \mathbb{G}_T$. $|g|$ (resp. $|\tilde{g}|$) denotes bit length of an element in $\mathbb{G}$ (resp. $\tilde{\mathbb{G}}$). For the FSS-based scheme, $m \in \mathbb{N}$ denotes bit length of a message. SXDH means Symmetric External Diffie-Hellman.

An FIBS scheme is transformed from an ARIP scheme with $n = l$ dimensions. For the vector $\mathbf{x} \in \mathbb{Z}_p^l$, its i-th element x_i is set to 1 if $i \in S$ or 0 otherwise. For the vector $\mathbf{y} \in \mathbb{Z}_p^l$, y_i is 1 if $i \in S'$ or 0 otherwise. The FIBS scheme is correct since $\langle \mathbf{x}, \mathbf{y} \rangle = |S \cap S'|$.

Additionally, we present the following 4 applications.

(4) **Time-Specific Signatures (TSS) [21,13]:** TSS is a sub-class of the ABS. The attribute $x \in \{0,1\}^*$ is a time-period $t \in [0, T-1]$ for an integer $T \in \mathbb{N}$. The predicate f_{TSS}, associated with a range $[L, R]$ with $L, R \in [0, T-1]$, is defined as

$$f_{\mathrm{TSS}}(t) := \begin{cases} 1 & (\text{If } t \in [L, R] \\ 0 & (\text{Otherwise}). \end{cases}$$

We use an ARIP scheme of 1 dimension. The scalar $x_1 \in \mathbb{Z}_p$ in ARIP is t. The scalar $y_1 \in \mathbb{Z}_p$ in ARIP is always 1. The TSS scheme is correct because $t \in [L, R]$ implies $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 \cdot y_1 = t \in [L, R]$.

In [21], TSS was firstly mentioned and its secure construction was presented as a open problem. In [13], the authors formally defined TSS and proposed two secure schemes based on forward-secure signatures (FSS) and wildcarded identity-based ring signatures (WIBRS), respectively. In Table 5, their TSS schemes [13] and ours are compared in terms of efficiency and security assumptions. Ours 1 (resp. Ours 2) is the TSS scheme obtained by instantiating the optimized variant of our 1st (resp. 2nd) ARIP scheme. Ours are the first ones whose $|pp|$, $|mk|$ and $|sk|$ are independent of the parameter T.

(5) **ABS for Range of Hamming Distance (ARHD):** A signer with a (binary) string $x \in \{0,1\}^l$ can sign a message under a string $y \in \{0,1\}^l$ iff the Hamming distance between x and y is within a range $[L, R]$. The attribute x in the ABS is a string $x \in \{0,1\}^l$. The predicate f_{ARHD} is defined as

$$f_{\mathrm{ARHD}}(x) := \begin{cases} 1 & (\text{If } \mathbf{HD}(x, y) \in [L, R]) \\ 0 & (\text{Otherwise}), \end{cases}$$

where the function $\mathbf{HD}(x, y)$ returns $\sum_{i=0}^{l-1} |x[i] - y[i]|$ which is the Hamming distance between x and y.

We use an ARIP scheme of $2l$ dimensions. The strings $x, y \in \{0,1\}^l$ are changed into $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^{2l}$ as follows. For each $i \in [0, l-1]$, (x_{2i+1}, x_{2i+2}) (resp. (y_{2i+1}, y_{2i+2})) is set to $(0,1)$ (resp. $(1,0)$) if $x[i] = 0$, or $(1,0)$ (resp. $(0,1)$) otherwise. Obviously, $x_{2i+1} \cdot y_{2i+1} + x_{2i+2} \cdot y_{2i+2}$ is 1 if $x[i] \neq y[i]$, or 0 otherwise. The ARHD scheme is correct because $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{HD}(x, y)$.

(6) ABS for Range of Euclidean Distance (ARED): A signer with a vector $\overrightarrow{X} \in \mathbb{Z}_p^n$ declares another vector $\overrightarrow{Y} \in \mathbb{Z}_p^n$ and a range $[L, R]$. If the Euclidean distance between the two vectors is within the range, the signing succeeds. The predicate f_{ARED} is defined as

$$f_{\mathrm{ARED}}(\overrightarrow{X}) := \begin{cases} 1 & (\text{If } \mathbf{ED}(\overrightarrow{X}, \overrightarrow{Y}) \in [L, R]) \\ 0 & (\text{Otherwise}), \end{cases}$$

where the function $\mathbf{ED}(\overrightarrow{X}, \overrightarrow{Y})$ returns $\sqrt{\sum_{i=1}^n (X_i - Y_i)^2} \in [L, R]$ which is the Euclidean distance between $\overrightarrow{X}$ and $\overrightarrow{Y}$.

An ARIP scheme with $2n+1$ dimensions is available. The vectors $\overrightarrow{X}, \overrightarrow{Y} \in \mathbb{Z}_p^n$ for ARED are transformed into $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^{2n+1}$ as follows.

– $(x_{2i-1}, x_{2i}) := (X_i^2, X_i)$ for all $i \in [1, n]$ and $x_{2n+1} := 1$.

– $(y_{2i-1}, y_{2i}) := (1, -2Y_i)$ for all $i \in [1, n]$ and $y_{2n+1} := \sum_{i=1}^n Y_i^2$.

The range $[L, R]$ for ARED is extended into $[L^2 \pmod{p}, R^2 \pmod{p}]$ for ARIP. The ARED scheme is correct since it holds $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{2n+1} x_i \cdot y_i = \sum_{i=1}^n X_i^2 - 2X_iY_i + Y_i^2 = \sum_{i=1}^n (X_i - Y_i)^2 = \mathbf{ED}(\overrightarrow{X}, \overrightarrow{Y})^2$, which implies $\mathbf{ED}(\overrightarrow{X}, \overrightarrow{Y}) \in [L, R] \Leftrightarrow \langle \mathbf{x}, \mathbf{y} \rangle (= \mathbf{ED}(\overrightarrow{X}, \overrightarrow{Y})^2) \in [L^2, R^2]$.

(7) ABS for Hyperellipsoid Predicates (AHEP): An n-dimensional hypersphere is a set of points (or vectors) whose Euclidean distance to the central point is constant. Let us consider a special type of ABS, where a secret-key is associated with a vector $\overrightarrow{X} \in \mathbb{Z}_p^n$, a signature is associated with a hypersphere with center $\overrightarrow{Y} \in \mathbb{Z}_p^n$ and radius $a \in \mathbb{Z}_p$ and the signing succeeds iff the vector $\overrightarrow{X}$ is inside of the hypersphere, named ABS for hypersphere predicates (AHSP). Obviously, AHSP is transformed from ARED defined above.

AHEP is a generalization of AHSP. Each hypersphere is generalized to a hyperellipsoid. The predicate f_{AHEP} is defined as

$$f_{\mathrm{AHEP}}(\overrightarrow{X}) := \begin{cases} 1 & (\text{If } \sum_{i=1}^n (X_i - Y_i)^2 / a_i^2 \leq 1), \\ 0 & (\text{Otherwise}), \end{cases}$$

where $\overrightarrow{Y} \in \mathbb{Z}_p^n$ is the center and $a_i \in \mathbb{Z}_p$ is the radius in the i-th axis.

An AHEP scheme is transformed from an ARIP scheme with $2n+1$ dimensions. For $i \in [1, n]$, let $\delta_i := (\prod_{j=1}^n a_j^2)/a_i^2$. The vectors $\overrightarrow{X}, \overrightarrow{Y} \in \mathbb{Z}_p^n$ for AHEP are transformed into $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^{2n+1}$ as follows.

– $(x_{2i-1}, x_{2i}) := (X_i^2, X_i)$ for all $i \in [1, n]$ and $x_{2n+1} := 1$.

– $(y_{2i-1}, y_{2i}) := (\delta_i, -2\delta_i Y_i)$ for all $i \in [1, n]$ and $y_{2n+1} := \sum_{i=1}^n \delta_i Y_i^2$.

The range $[L, R]$ for ARIP is set to $[1, \prod_{i=1}^n a_i^2 \pmod{p}]$. The AHEP scheme is correct since $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{2n+1} x_i \cdot y_i = \sum_{i=1}^n \delta_i (X_i - Y_i)^2 = \sum_{i=1}^n \frac{\prod_{j=1}^n a_j^2}{a_i^2} (X_i - Y_i)^2 \in [0, \sum_{j=1}^n a_j^2] \Leftrightarrow \sum_{i=1}^n (X_i - Y_i)^2 / a_i^2 \in [0, 1]$.

6 Conclusion

We formally defined ARIP and proposed two efficient schemes secure under standard assumptions, i.e., the CDH, FlexCDH and DLIN assumptions, in the standard model, based on the GS NIWI system [11] and a simplified variant of the ALP LHS scheme [6]. The 2nd (resp. 1st) scheme is independent of the number of dimensions $n \in \mathbf{poly}(\lambda)$ in secret-key length (resp. signature length and verification cost). We also optimized their efficiency for the case where each possible variable for $x_i, y_i, L, R, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}_p$ is upper-bounded by $T-1$ with $T \ll p$. We showed that ARIP can be generically transformed into various ABS. Since this work is the first research on ARIP, ARIP can develop in many directions. Some of the examples are given below.

***Key-Policy* ARIP (KPARIP):** A range $[L, R]$ is associated with each secret-key (but not signature). The transformations from ARIP to various ABS (in Sect. 5) work for KPARIP. Specifically, KPARIP can be transformed into the key-policy analogues of AREP, AREWA, TSS, ARHD, ARED and AHEP.

***Multi-Dimensional* ARIP:** Each secret-key has l number of n-dimensional vectors $\mathbf{x}_1, \cdots, \mathbf{x}_l \in \mathbb{Z}_p^n$. Each signature has l number of n-dimensional vectors $\mathbf{y}_1, \cdots, \mathbf{y}_l \in \mathbb{Z}_p^n$ and ranges $[L_1, R_1], \cdots, [L_l, R_l] \subseteq \mathbb{Z}_p$, and a Boolean formula $f : \underbrace{\{0,1\} \times \cdots \times \{0,1\}}_{l} \to \{0,1\}$. For each $i \in [1, l]$, a Boolean variable z_i is set to 1 if $\langle \mathbf{x}_i, \mathbf{y}_i \rangle \in [L_i, R_i]$, or 0 otherwise. If $f(z_1, \cdots, z_l) = 1$, the signing succeeds. For the form of f, we have various options, e.g., AND, OR or Threshold function, CNF or DNF formula, and a general circuit.

Attribute-Based *Encryption* for Range of Inner-Product: The transformations from ARIP to various ABS (in Sect. 5) also work for the encryption analogue of ARIP. Specifically, it can be transformed into the encryption analogues of AREP, AREWA, TSS, ARHD, ARED and AHEP.

References

1. M. Abdalla, J. Birkett, D. Catalano, A.W Dent, J. Malone-Lee, G. Neven, J.C.N. Schuldt, and N.P. Smart. Wildcarded identity-based encryption. *Journal of Cryptology*, 24(1):42–82, 2011.
2. J.H. Ahn, D. Boneh, J. Camenisch, S. Hohenberger, A. Shelat, and B. Waters. Computing on authenticated data. In *TCC 2012*, pp. 1–20. Springer, 2012.
3. N. Attrapadung and B. Libert. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In *PKC 2010*, pp. 384–402. Springer, 2010.
4. N. Attrapadung, B. Libert, and E. D. Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *PKC 2011*, pp. 90–108. Springer, 2011.
5. N. Attrapadung, B. Libert, and T. Peters. Computing on authenticated data: New privacy definitions and constructions. In *ASIACRYPT 2012*, pp. 367–385. Springer, 2012.

6. N. Attrapadung, B. Libert, and T. Peters. Efficient completely context-hiding quotable and linearly homomorphic signatures. In *PKC 2013*, pp. 386–404. Springer, 2013.
7. J. Blömer, F. Eidens, and J. Juhnke. Enhanced security of attribute-based signatures. In *CANS 2018*, pp. 235–255. Springer, 2018.
8. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *CRYPTO 2004*, pp. 41–55. Springer, 2004.
9. D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In *PKC 2009*, pp. 68–87. Springer, 2009.
10. D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC 2007*, pp. 535–554. Springer, 2007.
11. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT 2008*, pp. 415–432. Springer, 2008.
12. F. Guo, W. Susilo, and Y. Mu. Distance-based encryption: How to embed fuzziness in biometric-based encryption. *IEEE Transactions on Information Forensics and Security*, 11(2):247–257, 2015.
13. M. Ishizaka and S. Kiyomoto. Time-specific signatures. In *ISC 2020*, pp. 20–38. Springer, 2020.
14. S. Katsumata and S. Yamada. Non-zero inner product encryption schemes from various assumptions: Lwe, ddh and dcr. In *PKC 2019*, pp. 158–188. Springer, 2019.
15. J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT 2008*, pp. 146–162. Springer, 2008.
16. E. Kiltz, J. Pan, and H. Wee. Structure-preserving signatures from standard assumptions, revisited. In *CRYPTO 2015*, pp. 275–295. Springer, 2015.
17. H.K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. Cryptology ePrint Archive: Report 2008/394, 2008.
18. H.K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures. In *CT-RSA 2011*, pp. 376–392. Springer, 2011.
19. T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *CRYPTO 2010*, pp. 191–208. Springer, 2010.
20. T. Okamoto and K. Takashima. Efficient attribute-based signatures for non-monotone predicates in the standard model. In *PKC 2011*, pp. 207–222. Springer, 2011.
21. K. G. Paterson and E. A. Quaglia. Time-specific encryption. In *SCN 2010*, pp. 1–16. Springer, 2010.
22. T.V.X. Phuong, G. Yang, W. Susilo, and K. Liang. Edit distance based encryption and its application. In *ACISP 2016*, pp. 103–119. Springer, 2016.
23. A. Sahai and B. Waters. Fuzzy identity-based encryption. In *EUROCRYPT 2005*, pp. 457–473. Springer, 2005.
24. Y. Sakai, N. Attrapadung, and G. Hanaoka. Attribute-based signatures for circuits from bilinear map. In *PKC 2016*, pp. 283–300. Springer, 2016.
25. Y. Sakai, S. Katsumata, N. Attrapadung, and G. Hanaoka. Attribute-based signatures for unbounded languages from standard assumptions. In *ASIACRYPT 2018*, pp. 493–522. Springer, 2018.
26. B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT 2005*, pp. 114–127. Springer, 2005.
27. Y. Zhang, X. Liu, Y. Hu, Q. Zhang, and H. Jia. Attribute-based signatures for inner-product predicate from lattices. In *CSS 2019*, pp. 173–185. Springer, 2019.

A Omitted Definitions

A.1 Non-Interactive Witness-Indistinguishable Proof (NIWI)

Syntax. An NIWI system for the NP relation $R : \{0,1\}^* \times \{0,1\}^* \to 1/0$ consists of the following 3 polynomial-time algorithms. Note that $\texttt{Ver}$ is deterministic and the others are probabilistic.

Setup $\texttt{Setup}$: It takes a security parameter 1^λ for $\lambda \in \mathbb{N}$, then outputs a common reference string (CRS) crs.
$[crs \leftarrow \texttt{Setup}(1^\lambda)]$

Proving $\texttt{Pro}$: It takes the CRS crs, a statement $x \in \{0,1\}^*$ and a witness $w \in \{0,1\}^*$, then outputs a proof π.
$[\pi \leftarrow \texttt{Pro}(crs, x, w)]$

Verification $\texttt{Ver}$: It takes the CRS crs, a statement $x \in \{0,1\}^*$ and a proof π, then outputs a verification result, which is 1 (accept) or 0 (reject).
$[1/0 \leftarrow \texttt{Ver}(crs, x, \pi)]$

We require every NIWI system to be correct. An NIWI system is correct if for every $\lambda \in \mathbb{N}$, every $crs \leftarrow \texttt{Setup}(1^\lambda)$, every $x \in \{0,1\}^*$, every $w \in \{0,1\}^*$ s.t. $1 \leftarrow R(x, w)$, and every $\pi \leftarrow \texttt{Pro}(crs, x, w)$, it holds that $1 \leftarrow \texttt{Ver}(crs, x, \pi)$.

Security. We define two security requirements, namely

1. perfect witness-indistinguishability ($\texttt{WI}$), and
2. perfect witness-extractability ($\texttt{WE}$).

Definition 6. *An NIWI system is perfectly witness-indistinguishable ($\texttt{WI}$), if for every $\lambda \in \mathbb{N}$, every $crs \leftarrow \texttt{Setup}(1^\lambda)$, every $x \in \{0,1\}^*$, and every $w_0, w_1 \in \{0,1\}^*$ s.t. $1 \leftarrow R(x, w_b)$ for each $b \in \{0,1\}$, $\texttt{Pro}(crs, x, w_0)$ distributes identically to $\texttt{Pro}(crs, x, w_1)$.*

Definition 7. *An NIWI system is perfectly witness-extractable ($\texttt{WE}$), if for every $\lambda \in \mathbb{N}$, there exist two algorithms $\texttt{SimSetup}$ and $\texttt{Extract}$ that satisfy both of the following two conditions.*

1. *For every PPT $\mathcal{A}$,*

$$\left|\Pr\left[1 \leftarrow \mathcal{A}(crs) \mid crs \leftarrow \texttt{Setup}(1^\lambda)\right] - \Pr\left[1 \leftarrow \mathcal{A}(crs) \mid (crs, ek) \leftarrow \texttt{SimSetup}(1^\lambda)\right]\right|$$

   is negligible.

2. *For every PPT $\mathcal{A}$,*

$$\Pr\left[\begin{array}{c} (crs, ek) \leftarrow \texttt{SimSetup}(1^\lambda); (x, \pi) \leftarrow \mathcal{A}(crs); \\ w \leftarrow \texttt{Extract}(crs, ek, x, \pi) : 1 \leftarrow \texttt{Ver}(crs, x, \pi) \wedge 0 \leftarrow R(x, w) \end{array}\right] = 0.$$

A.2 Linearly Homomorphic Signatures (LHS)

Syntax. An LHS scheme consists of the following 4 polynomial-time algorithms. Note that `Setup` and `Sig` are probabilistic, `Ver` is deterministic and `Derive` is (possibly) probabilistic.

Key-Generation `KGen`: It takes a security parameter 1^λ for $\lambda \in \mathbb{N}$ and an integer $n \in \mathbb{N}$, being polynomial in λ, that indicates the dimension of a vector to be signed, then outputs a key-pair (pk, sk).
$[(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, n)]$

Signing `Sig`: It takes the secret-key sk, a tag (called a file identifier in [5]) $\tau \in \{0,1\}^*$ and a vector $\boldsymbol{v} \in \mathbb{Z}_p^n$ to be signed, then outputs a signature σ.
$[\sigma \leftarrow \texttt{Sig}(sk, \tau, \boldsymbol{v})]$

Derivation `Derive`: It takes the public-key pk, a tag $\tau \in \{0,1\}^*$ and l triples $\{\boldsymbol{v}_i, \sigma_i, \beta_i\}_{i=1}^l$, consisting of a vector $\boldsymbol{v}_i \in \mathbb{Z}_p^n$, a signature σ_i and a weight β_i, then outputs a signature $\overline{\sigma}$ on the weighted vector $\overline{\boldsymbol{v}} := \sum_{i=1}^l \beta_i \cdot \boldsymbol{v}_i \in \mathbb{Z}_p^n$.
$[\overline{\sigma} \leftarrow \texttt{Derive}(pk, \tau, \{\boldsymbol{v}_i, \sigma_i, \beta_i\}_{i=1}^l)]$

Verification `Ver`: It takes the public-key pk, a tag $\tau \in \{0,1\}^*$, a vector $\boldsymbol{v} \in \mathbb{Z}_p^n$ and a signature σ, then outputs a verification result 1 or 0.
$[1/0 \leftarrow \texttt{Ver}(pk, \tau, \boldsymbol{v}, \sigma)]$

We require every LHS scheme to be correct. An LHS scheme is correct if for every $\lambda \in \mathbb{N}$, every $n \in \mathbf{poly}(\lambda)$ and every $(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, n)$, both of the following conditions hold.

1. For every tag $\tau \in \{0,1\}^*$ and every vector $\boldsymbol{v} \in \mathbb{Z}_p^n$, it holds that $1 \leftarrow \texttt{Ver}(pk, \tau, \boldsymbol{v}, \texttt{Sig}(sk, \tau, \boldsymbol{v}))$.
2. For every tag $\tau \in \{0,1\}^*$, every integer $l \in \mathbb{N}$ and every l triples $\{\boldsymbol{v}_i \in \mathbb{Z}_p^n, \sigma_i, \beta_i \in \mathbb{Z}_p\}_{i=1}^l$ such that $1 \leftarrow \texttt{Ver}(pk, \tau, \boldsymbol{v}_i, \sigma_i)$ for all i, it holds that $1 \leftarrow \texttt{Ver}(pk, \tau, \sum_{i=1}^l \beta_i \boldsymbol{v}_i, \texttt{Derive}(pk, \tau, \{\boldsymbol{v}_i, \sigma_i, \beta_i\}_{i=1}^l))$.

Security. As security properties for LHS, we define

1. unforgeability,
2. strong context-hiding (SCH) [2], and
3. complete context-hiding (CCH) [5].

For the definition of unforgeability, we have referred to [5]. We define the following experiment that a PPT adversary $\mathcal{A}$ participates. $\mathcal{H}$ denotes the space of handles for the queue Q.

```
$\boldsymbol{Expt}^{\texttt{UNF}}_{\Sigma_{\mathrm{LHS}},\mathcal{A}}(1^\lambda, n)$:
  1. $(pk, sk) \leftarrow \texttt{Setup}(1^\lambda, n)$. $(\tau^* \in \{0,1\}^*, \boldsymbol{v}^* \in \mathbb{Z}_p^n, \sigma^*) \leftarrow \mathcal{A}^{\mathfrak{Sign}, \mathfrak{Derive}, \mathfrak{Reveal}}(pk)$.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    - $\mathfrak{Sign}(\tau \in \{0,1\}^*, \boldsymbol{v} \in \mathbb{Z}_p^n)$:
      Choose a handle $h \xleftarrow{\mathrm{U}} \mathcal{H}$. $\sigma \leftarrow \texttt{Sig}(sk, \tau, \boldsymbol{v})$. $Q := Q \cup \{(h, \tau, \boldsymbol{v}, \sigma)\}$. **Rtrn** $h$.
    - $\mathfrak{Derive}(\tau \in \{0,1\}^*, \{h_i \in \mathcal{H}, \sigma_i, \beta_i \in \mathbb{Z}_p\}_{i=1}^l)$:
      **Rtrn** $\perp$ if $\exists i \in [1, l]$ s.t. $[\nexists \boldsymbol{v}_i$ s.t. $(h_i, \tau, \boldsymbol{v}_i, \sigma_i) \notin Q]$.
      Choose a handle $h \xleftarrow{\mathrm{U}} \mathcal{H}$. $\overline{\sigma} \leftarrow \texttt{Derive}(pk, \tau, \{\boldsymbol{v}_i, \sigma_i, \beta_i\}_{i=1}^l)$.
      $Q := Q \cup \{(h, \tau, \sum_{i=1}^l \beta_i \boldsymbol{v}_i, \overline{\sigma})\}$. **Rtrn** $h$.
    - $\mathfrak{Reveal}(h \in \mathcal{H}, \tau \in \{0,1\}^*, \boldsymbol{v} \in \mathbb{Z}_p^n)$:
```

Rtrn $\perp$ if $\nexists\sigma$ s.t. $(h, \tau, \boldsymbol{v}, \sigma) \in Q$. $Q' := Q' \cup \{(\tau, \boldsymbol{v})\}$. **Rtrn** σ.

- -

2. **Rtrn** 1 if (1) $1 \leftarrow \texttt{Ver}(pk, \tau^*, \boldsymbol{v}^*, \sigma^*)$ and (2) one of the following conditions is satisfied.
   (a) $\tau^* \neq \tau_i$ for any entry $(\tau_i, \cdot) \in Q'$ and $\boldsymbol{v}^* \neq \mathbf{0}$.
   (b) $\tau^* = \tau_i$ for $k > 0$ entries $(\tau_i, \boldsymbol{v}_i)$ in Q' and $\boldsymbol{v}^* \notin \mathbf{span}\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_k\}$.

Definition 8. *An LHS scheme Σ_{LHS} is unforgeable if for every $\lambda \in \mathbb{N}$, every $n \in \mathbf{poly}(\lambda)$ and every PPT $\mathcal{A}$, $\mathcal{A}$'s advantage defined as $\boldsymbol{Adv}^{\textit{UNF}}_{\Sigma_{\text{LHS}},\mathcal{A}}(\lambda) := \Pr[1 \leftarrow \boldsymbol{Expt}^{\textit{UNF}}_{\Sigma_{\text{LHS}},\mathcal{A}}(1^\lambda, n)]$ is negligible.*

Both SCH and CCH are security notions guaranteeing that no signature generated by the deriving algorithm `Derive` based on some original signatures can be linked to the original ones. In the former, the original signatures have been honestly generated by the signing algorithm `Sig`. In the latter, the condition that the original signatures must satisfy is that they are correct ones, which means that they might have been dishonestly generated. Obviously, the latter notion is truly stronger than the former.

Definition 9 ([2]). *An LHS scheme is strongly context-hiding (SCH) if for every $\lambda \in \mathbb{N}$, every $n \in \mathbf{poly}(\lambda)$, every $(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, n)$, every tag $\tau \in \{0,1\}^*$, every integer $l \in [1, n]$, all l linearly-independent vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_l \in \mathbb{Z}_p^n$ and all l weights $\beta_1, \cdots, \beta_l \in \mathbb{Z}_p$, the following two distributions are statistically close, namely*

- $\{sk, \{\sigma_i\}_{i=1}^l, \texttt{Derive}(pk, \tau, \{\boldsymbol{v}_i, \sigma_i, \beta_i\}_{i=1}^l)\}$ *and*
- $\{sk, \{\sigma_i\}_{i=1}^l, \texttt{Sig}(sk, \tau, \sum_{i=1}^l \beta_i \boldsymbol{v}_i)\}$,

where $\sigma_i \leftarrow \texttt{Sig}(sk, \tau, \boldsymbol{v}_i)$ for each $i \in [1, l]$.

Definition 10 ([5]). *An LHS scheme is completely context-hiding (CCH) if for every $\lambda \in \mathbb{N}$, every $n \in \mathbf{poly}(\lambda)$, every $(pk, sk) \leftarrow \texttt{KGen}(1^\lambda, n)$, every tag $\tau \in \{0,1\}^*$, every integer $l \in [1, n]$, all l linearly-independent vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_l \in \mathbb{Z}_p^n$, all l correct signatures $\sigma_1, \cdots, \sigma_l$ s.t. $1 \leftarrow \texttt{Ver}(pk, \tau, \boldsymbol{v}_i)$, and all l weights $\beta_1, \cdots, \beta_l \in \mathbb{Z}_p$, the following two distributions are statistically close, namely*

- $\{sk, \{\sigma_i\}_{i=1}^l, \texttt{Derive}(pk, \tau, \{\boldsymbol{v}_i, \sigma_i, \beta_i\}_{i=1}^l)\}$ *and*
- $\{sk, \{\sigma_i\}_{i=1}^l, \texttt{Sig}(sk, \tau, \sum_{i=1}^l \beta_i \boldsymbol{v}_i)\}$.

B The Simplified Variant of the ALP LHS Scheme [6]

$\texttt{KGen}(1^\lambda, n)$**:** Choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ whose order is a prime p of bit lengh λ. Choose $\alpha \xleftarrow{\text{U}} \mathbb{Z}_p$. Let $g, v, g_1, \cdots, g_n \xleftarrow{\text{U}} \mathbb{G}$. Let $u', u_0, \cdots, u_{N-1} \xleftarrow{\text{U}} \mathbb{G}$ for an integer $N \in \mathbb{N}$. Let $H_{\mathbb{G}}$ be a function which takes $\tau \in \{0,1\}^N$ as input, then outputs $u' \prod_{i=0}^{N-1} u_i^{\tau[i]} \in \mathbb{G}$. Output (pk, sk), where $pk := (\mathbb{G}, \mathbb{G}_T, g, g^\alpha, v, \{g_i\}_{i=1}^n, u', \{u_i\}_{i=0}^{N-1})$ and $sk := \alpha$.

$\texttt{Sig}(sk, \tau \in \{0,1\}^N, \boldsymbol{v} \in \mathbb{Z}_p^n)$**:** Parse $\boldsymbol{v}$ as $(v_1, \cdots, v_n)$. Choose $r, s \overset{\mathrm{U}}{\longleftarrow} \mathbb{Z}_p$. Compute

$$(\sigma_1, \sigma_2, \sigma_3, \sigma_4) := \left((\prod_{j=1}^{n} g_i^{v_i} v^s)^\alpha H_{\mathbb{G}}(\tau)^r, g^r, g^s, g^{\alpha \cdot s} \right).$$

Output $\sigma := (\boldsymbol{v}, \tau, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$.

$\texttt{Derive}(pk, \tau \in \{0,1\}^N, \{\boldsymbol{v}_i \in \mathbb{Z}_p^n, \sigma_i, \beta_i \in \mathbb{Z}_p\})$**:** Parse σ_i as $(\boldsymbol{v}, \tau, \sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4})$. Choose $\overline{r} \overset{\mathrm{U}}{\longleftarrow} \mathbb{Z}_p$. Compute

$$(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4) := \left(\prod_{i=1}^{l} \sigma_{i,1}^{\beta_i} \cdot H_{\mathbb{G}}(\tau)^{\overline{r}}, \prod_{i=1}^{l} \sigma_{i,2}^{\beta_i} \cdot g^{\overline{r}}, \prod_{i=1}^{l} \sigma_{i,3}^{\beta_i}, \prod_{i=1}^{l} \sigma_{i,4}^{\beta_i} \right).$$

Output $\overline{\sigma} := (\sum_{i=1}^{l} \beta_i \cdot \boldsymbol{v}_i, \tau, \overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4)$.

$\texttt{Ver}(pk, \tau \in \{0,1\}^N, \boldsymbol{v} \in \mathbb{Z}_p^n, \sigma)$**:** Parse $\boldsymbol{v} \in \mathbb{Z}_p^n$ as $(v_1, \cdots, v_n)$. Parse σ as $(\boldsymbol{v}, \tau, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$. Output 1 if both of the following two conditions hold.

$$\begin{aligned} e(g, \sigma_1) &= e(\prod_{i=1}^{n} g_i^{v_i}, g^\alpha) \cdot e(v, \sigma_4) \cdot e(H_{\mathbb{G}}(\tau), \sigma_2) \\ e(g^\alpha, \sigma_2) &= (g, \sigma_4) \end{aligned}$$

Output 0 otherwise.

We have not rigorously proven, but it is expected that the following theorem holds.

Theorem 4. *The simplified variant of the ALP LHS scheme is unforgeable (under Definition 8) if the CDH and FlexCDH assumptions hold in the group* $\mathbb{G}$.

C Analysis of the Probability $\Pr[\neg\mathsf{abort}]$ in the Proof of Lemma 4

Let $\tau_i \in \{0,1\}^N$ for $i \in [1, q]$ denote the tag chosen at the i-th key-revelation or signing oracle. We obtain

$$\begin{aligned} \Pr[\neg\mathsf{abort}] &= \Pr\left[F(\tau^*) = 0 \pmod{p} \bigwedge_{i=1}^{q} F(\tau_i) \neq 0 \pmod{l} \right] \\ &= \Pr\left[F(\tau^*) = 0 \pmod{p} \right] \\ &\quad \cdot \Pr\left[\bigwedge_{i=1}^{q} F(\tau_i) \neq 0 \pmod{l} \mid F(\tau^*) = 0 \pmod{p} \right]. \end{aligned} \tag{6}$$

We analyze each of the two terms in (6) one by one. The first term is analyzed as follows.

$$\Pr\left[F(\tau^*) = 0 \pmod{p} \right]$$

$$
\begin{aligned}
&= \Pr\left[F(\tau^*) = 0 \pmod{p} \wedge F(\tau^*) = 0 \pmod{l}\right] \\
&= \Pr\left[F(\tau^*) = 0 \pmod{l}\right] \Pr\left[F(\tau^*) = 0 \pmod{p} \mid F(\tau^*) = 0 \pmod{l}\right] \\
&= \frac{1}{l}\frac{1}{N+1}. \qquad (7)
\end{aligned}
$$

The second term is analyzed as follows.

$$
\begin{aligned}
&\Pr\left[\bigwedge_{i=1}^{q} F(\tau_i) \neq 0 \pmod{l} \mid F(\tau^*) = 0 \pmod{p}\right] \\
&= 1 - \Pr\left[\bigvee_{i=1}^{q} F(\tau_i) = 0 \pmod{l} \mid F(\tau^*) = 0 \pmod{p}\right] \\
&\geq 1 - \sum_{i=1}^{q} \Pr\left[F(\tau_i) = 0 \pmod{l} \mid F(\tau^*) = 0 \pmod{p}\right] \\
&= 1 - \frac{q}{l}. \qquad (8)
\end{aligned}
$$

By (6), (7), (8), we obtain

$$
\Pr[\neg\mathsf{abort}] \geq \frac{1}{l}\frac{1}{N+1}(1 - \frac{q}{l}) = \frac{1}{4q(N+1)},
$$

because $l = 2q$.

D Our 2nd ARIP Scheme

$\mathtt{Setup}(1^\lambda, n)$: The same as the one of our 1st ARIP scheme except that number of the variables $\{g_i\}_{i=1}^{n+5}$ is reduced to $n+4$.

$\mathtt{KGen}(mk, \mathbf{x})$: Parse $\mathbf{x}$ as $(x_1, \cdots, x_n)$. Choose a tag $\tau \overset{\mathrm{U}}{\leftarrow} \{0,1\}^N$. Generate 4 vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_4 \in \mathbb{Z}_p^{n+4}$ in the manner explained in Subsect 4.4, i.e., (2)-(5). For each $i \in [1,4]$, parse $\boldsymbol{v}_i$ as $(v_{i,1}, v_{i,2}, \cdots, v_{i,n+4})$, and compute an ALP signature $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4})$ as

$$
\sigma_{i,1} := \left(\prod_{j=1}^{n+4} g_i^{v_{i,j}} v^{s_i}\right)^{\alpha} H_{\mathbb{G}}(\tau)^{r_i},\ \ \sigma_{i,2} := g^{r_i},\ \ \sigma_{i,3} := g^{s_i},\ \ \sigma_{i,4} := g^{\alpha \cdot s_i},
$$

where $r_i, s_i \overset{\mathrm{U}}{\leftarrow} \mathbb{Z}_p$. Finally, output the secret-key $sk := (\mathbf{x}, \tau, \{\{\sigma_{i,j}\}_{j=1}^4\}_{i=1}^4)$.

$\mathtt{Sig}(sk, M, \mathbf{y}, L, R)$: Parse sk as $(\mathbf{x}, \tau, \{\{\sigma_{i,j}\}_{j=1}^4\}_{i=1}^4)$. Parse $\mathbf{y}$ as $(y_1, \cdots, y_n)$. To generate a signature σ, conduct the following five steps first.

1. Set $d := \langle \mathbf{x}, \mathbf{y} \rangle \pmod{p}$. Assume that $d \in [L, R]$.
2. Choose $\overline{r} \overset{\mathrm{U}}{\leftarrow} \mathbb{Z}_p$. Set $(\beta_1, \beta_2, \beta_3, \beta_4) := (1, L, R, M)$.
3. Compute

$$
(\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4) := \left(\prod_{i=1}^{4} \sigma_{i,1}^{y_i} \cdot H_{\mathbb{G}}(\tau)^{\overline{r}}, \prod_{i=1}^{4} \sigma_{i,2}^{y_i} \cdot g^{\overline{r}}, \prod_{i=1}^{4} \sigma_{i,3}^{y_i}, \prod_{i=1}^{4} \sigma_{i,4}^{y_i}\right).
$$

Note that if sk is a correct secret-key with inner-randomness $\{r_j, s_j\}_{j=1}^4$, the computed ALP signature distributes as

$$\left(\left\{ \prod_{i=1}^{n} g_i^{x_i} \cdot g_{n+1} \cdot g_{n+2}^{L} \cdot g_{n+3}^{R} \cdot g_{n+4}^{M} \cdot v^{\sum_{j=1}^4 \beta_j s_j} \right\}^{\alpha} H_{\mathbb{G}}(\tau)^{\sum_j \beta_j r_j + \overline{r}}, \right.$$
$$\left. g^{\sum_j \beta_j r_j + \overline{r}}, g^{\sum_j \beta_j s_j}, g^{\alpha \sum_j \beta_j s_j} \right).$$

4. As our 1st ARIP scheme, compute the GS commitments for all of the variables (a), $\cdots$, (e). Additionally, compute the commitments for all of the following variables.
   - g^{x_i} and $g_i^{x_i}$

     (for all $i \in [1, n]$)

   Let the commitments be denoted by $\vec{C}_{x_i}, \vec{C'}_{x_i} \in \mathbb{G}^3$, respectively.
5. As our 1st ARIP scheme, compute the GS proofs for all of the relations [a], $\cdots$, [f] except for the relation [e] which is modified as follows.

   [e'] $e(\overline{\sigma}_1, g) = \prod_{i=1}^n (g_i^{x_i}, g^{\alpha}) \cdot e(\prod_{i=1}^4 g_{i+n}^{y_i}, g^{\alpha}) \cdot e(v, \overline{\sigma}_4) \cdot e(H_{\mathbb{G}}(\tau), \overline{\sigma}_2)$

   Additionally, compute the GS proofs for all of the following relations.
   - $e(g^{x_i}, g_i) = e(g, g_i^{x_i})$

     (for all $i \in [1, n]$)
   - $e(g_1^d, g) = \prod_{i=1}^n e(g^{x_i}, g_1^{y_i})$

Let the proofs be denoted by $\vec{\pi}_{x_i}, \vec{\pi}_{\mathtt{ip}} \in \mathbb{G}^3$, respectively.

As our 1st ARIP scheme, generate the GS commitments/proofs for the fact that $d \in [L, R]$.

The signature σ consists of all of the GS commitments and proofs generated so far, and the second ALP signature element $\overline{\sigma}_2 \in \mathbb{G}$.

$\mathtt{Ver}(\sigma, M, \mathbf{y}, L, R)$**:** As our 1st ARIP scheme, verify the 12 equations except for the 7th equation which is modified as follows.

7'. $E(g, \vec{C}_{\overline{\sigma}_1}) = \prod_{i=1}^n E(g^{\alpha}, \vec{C'}_{x_i}) \cdot E(\prod_{i=1}^4 g_{i+n}^{y_i}, \iota(g^{\alpha})) E(v, \vec{C}_{\overline{\sigma}_4}) \cdot E(\overline{\sigma}_2, \vec{C}_{H_{\mathbb{G}}(\tau)}) \cdot \prod_{k=1}^3 E(\pi_{\overline{\sigma}_1,k}, \vec{f}_k)$

Additionally, verify the following 13rd and 14th equations.

13. $E(g_i, \vec{C}_{x_i}) = E(g, \vec{C'}_{x_i}) \cdot \prod_{k=1}^3 E(\pi_{x_i,k}, \vec{f}_k)$

    (for all $i \in [1, n]$)
14. $E(g, \vec{C}_d) = \prod_{i=1}^n E(g_1^{y_i}, \vec{C}_{x_i}) \cdot \prod_{k=1}^3 E(\pi_{\mathtt{ip},k}, \vec{f}_k)$