Linear and Lossy Identification Schemes Derive Tightly Secure Multisignatures

Masayuki Fukumitsu[1], Shingo Hasegawa[2]

[1] Faculty of Information Media, Hokkaido Information University, Japan
[2] Graduate School of Information Sciences, Tohoku University, Japan
fukumitsu@do-johodai.ac.jp, shingo.hasegawa.b7@tohoku.ac.jp

Abstract

For the multisignature schemes, the tight security in the plain public key (PPK) model is considered as one of the desirable features. In this paper, we give a generic construction of multisignature schemes which is tightly secure in the PPK and random oracle model. Our construction can capture the known tightly secure multisignature schemes. The generic construction is derived from the identification (ID) scheme which has two properties called the linearity and the lossiness. Thus, we can obtain new tightly secure multisignature schemes by applying our construction to existing linear and lossy ID schemes. Moreover, we consider the relationship between these two properties to shrink the conditions required for our generic construction. We propose a new property of ID schemes, called the difference soundness, and show that the combination of the linearity and the difference soundness implies the lossiness.

Keywords: Linear identification scheme, Lossy identification scheme, Multisignature, Tight security, Plain public key model

1 Introduction

The multisignature scheme admits multiple signers in the signature generation. The signers compute a single signature on a single common message in an interactive manner. The resulting signature ensures that the signers having a corresponding public key used in the verification participated in the signature generation. This feature yields the advantage for the multisignature scheme in the case where each signer issues an ordinary signature individually because the size of a multisignature can be less than the total size of individual signatures by signers. Thus, the multisignature scheme is considered as an attractive building block to develop a resource-constrained technology such as the IoT and the blockchain.

The security in the plain public key (PPK) model [1] is considered as the standard security model of multisignature schemes. The PPK model requires no restriction on the public key generation rather than other security models [2-3] of multisignatures. Therefore, the forger can select public keys arbitrary in the security game of the PPK model, and then the security in PPK model is stronger than the one in other models.

The BN multisignature [1] is the first multisignature scheme whose security is proven in the PPK and random oracle (RO) model. This scheme is constructed based on the Schnorr signature [4] which is a Fiat-Shamir [5] type signature scheme. Thus, the security of the BN multisignature is carried from the Schnorr signature, namely it is proven under the discrete logarithm (DL) assumption in RO model [6].

There are some multisignature schemes secure in the PPK and RO model which are constructed by employing the strategy of the BN multisignature. Le, Bonnecaze, and Gaillon [7] proposed a DDH-based multisignature scheme. Their scheme is based on the Katz-Wang signature [8] and achieves the tight security in the RO model. Concerning another algebraic structure, El Bansarkhani and Sturm [9] proposed a lattice-based multisignature scheme, and its security is proven under the Ring-SIS assumption. Fukumitsu and Hasegawa [10] enhanced their multisignature scheme concerning the tightness. Namely, the scheme by [10] has a tight security reduction under the Ring-LWE assumption, whereas the original one of [9] is a loose reduction.

The tight security proof means that the probability that a probabilistic polynomial-time (PPT) algorithm breaks an underlying cryptographic assumption is almost the same as the probability that a PPT algorithm attacks the designated cryptographic scheme. If a cryptographic scheme is not tightly secure, we are required to set a large security parameter to maintain the security. On the other hand, a cryptographic scheme having the tight security allows a small parameter setting rather than the one having a loose security reduction only. Thus, achieving the tight security enables us to use cryptographic schemes efficiently.

*Corresponding Author: Masayuki Fukumitsu; E-mail: fukumitsu@do-johodai.ac.jp

DOI: 10.53106/160792642021092205018

There exist some multisignature schemes which have the tight security in the PPK and RO model. The representative schemes are the DDH-based scheme by [7] and the lattice-based scheme by [10]. Both schemes share some features. They are based on decisional assumptions, secure in the PPK and RO model, and employ the BN's construction. Therefore, it is a natural idea that we can obtain new tightly secure multisignature schemes by using these features.

1.1 Contribution

In this paper, we propose a generic construction of multisignature schemes with tight security in the PPK and RO model. We also give new instantiations of tightly secure multisignature schemes by using our generic construction. Our construction employs the linear identification (ID) scheme and the lossy ID scheme and, is obtained by incorporating these two ID schemes into the strategy of the BN's multisiganture construction.

The linear ID scheme [11] is defined by using the linear structure of modules. Many existing ID schemes are captured by the linear ID schemes. Moreover, the known multisignature schemes employing the BN's construction seem to use the linearity which originates in the underlying linear ID schemes.

The lossy ID scheme [12] is a specific variant of ID schemes which have another key generator, called a lossy key generator. It has two properties called the key indistinguishability and the lossiness. The key indistinguishability states that the distribution of lossy keys, public keys generated by the lossy key generator, is computationally indistinguishable from the one of regular public keys. The lossiness guarantees that an adversary cannot break the security of ID schemes when a lossy key is given, even if an adversary has unbounded computing power. The lossy ID scheme is employed to obtain tightly secure signature schemes via the Fiat-Shamir heuristic [8, 12-13]. Additionally, the tight security of the multisignature schemes by [7, 10] was proven by using the proof technique based on the lossy ID scheme.

The results and facts above suggest that we can obtain generic construction of multisignature schemes by abstracting the BN multisignature scheme with the linear ID scheme. Furthermore, we can add the tight security to the generic construction by incorporating the lossy ID scheme. The security is proven in the PPK and RO model.

In addition to the generic construction, we consider a more compact condition to give a tight security proof on the multisignature scheme. We consider the relationship between the lossiness and the linearity of ID schemes because we find that the known proofs of the lossy ID schemes are mostly based on the linearity. This means that lossy ID schemes can be constructed by using the linearity of ID schemes. However, the linearity seems not to imply the lossiness directly. Therefore, we introduce a new property, called the difference soundness on the ID scheme so that such an implication always holds. Then we prove that the linearity implies the lossiness with the help of the difference soundness. To the best of knowledge, this is the first sufficient condition to construct lossy ID schemes generally.

1.2 Applications

Our generic construction can be used to explain the existing tightly secure multisignature scheme. Moreover, we can obtain new multisiganture schemes by applying our generic construction to existing linear and lossy ID schemes. The DDH-based multisignature scheme by [7] is obtained from the DDH-based lossy ID scheme [8] via our generic construction. The lattice-based scheme [10] is also constructed from the lattice-based lossy ID scheme in [12]. In [12], other lossy ID schemes are proposed, the decisional short-discrete-logarithm (DSDL) based scheme and the subset-sum-based scheme. Applying our generic construction to these two lossy ID schemes, we can obtain the first tightly secure DSDL-based multisignature scheme and the first tightly secure subset-sum-based multisignature scheme, respectively.

We note the lossy ID schemes which are excluded from our construction such as [13-14]. The reason is that the key indistinguishability depends on groups of hidden order. In our generic construction, the signer's secret key and its public key are generated with respect to the predetermined public parameter which contains the representation of the underlying algebraic structure such as groups and rings. Since the order is necessary to generate the secret key for all signers in our setting, it is required to be contained in the public parameter. However, revealing the order breaks the security of the schemes above. Thus, we only consider the lossy ID schemes with the public order in this paper. It is an important question to construct a generic construction which is applicable to the hidden-order ID schemes.

1.3 Related Works

Multisignature schemes with tight security in the PPK model were proposed in [7, 10, 15-19]. The multisignature scheme proposed in [20] requires establishing a key authority. The construction of this paper does not require a key authority and thus the security can be proven in the PPK model. Most of the schemes above are pairing-based one [16-19], whereas the multisignature schemes [7, 10, 15] are paring-free. Since there are known pairing-free lossy ID schemes [12], we can add new instantiations of pairing-free multisignature schemes with tight security in the PPK model via our generic construction.

2 Preliminaries

In this section, we introduce notions and notations used in this paper. For a distribution D over a set X, we denote by $x \leftarrow_R D$ that $x \in X$ is chosen according to D. Let $U(X)$ be the uniform distribution over the finite set X. And $x \leftarrow_U X$ stands for $x \leftarrow_R U(X)$. For distributions D_1 and D_2 over a set X, the *statistical distance* is defined by $\frac{1}{2}\sum_{x \in X} |\Pr[x \leftarrow_R D_1] - \Pr[x \leftarrow_R D_2]|$. For an algorithm A, A($x$) means that A outputs y on input x. When A is probabilistic, A(x) is the random variable on input x, where the probability is taken over the internal coin flips of A. Let [D] denote the support of a distribution D, and let [A(x)] denote the set of all outputs which would be output by the probabilistic algorithm A on input x. We abbreviate "deterministic polynomial-time" and "probabilistic polynomial-time" to DPT and PPT, respectively.

2.1 Identification Scheme

An identification (ID) scheme [21] is an interactive protocol between a prover P and a verifier V by which P convinces V of the possession of a secret key *sk* which corresponds to a public key *pk*. We explain some specific types of ID schemes, linear or lossy ID schemes, below.

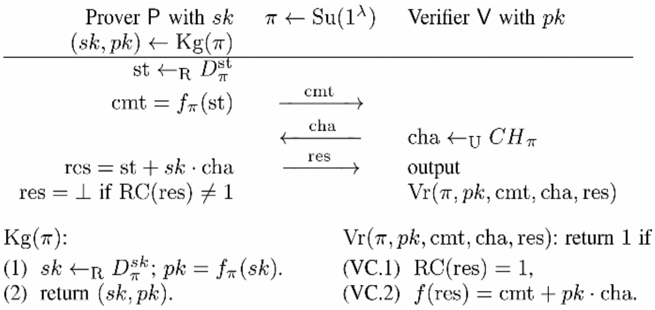
2.1.1 Linear ID Scheme

Linear ID (LID) schemes [11] are three-move ID schemes which are based on some specific algebraic structures. In this paper, we focus on some features of LID schemes only. Therefore, we hereafter define such a variant of LID schemes as succinct LID schemes. A *succinct LID scheme* consists of a tuple ($Su, \{D_\pi, R_\pi, S_\pi,\}_\pi,$ $\{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC$). Su is a PPT public parameter generator such that Su returns a public parameter π on a security parameter 1^λ. $\{D_\pi, R_\pi, S_\pi\}_\pi$ expresses a family of components to build *linear functions* $f_\pi : D_\pi \to R_\pi$ parameterized by a public parameter π. For any security parameter λ and public parameter $\pi \in [Su(1^\lambda)]$, f_π has the following properties:

- D_π and R_π are S_π-modules for the ring S_π.
- f_π can be evaluated in polynomial time in λ.
- f_π is linear, i.e., $f_\pi(x + y \cdot c) = f_\pi(x) + f(y) \cdot c$ for any $x, y \in D_\pi$ and any $c \in S_\pi$.

$\{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}$ is a family of samplable distributions D_π^{sk} and D_π^{st} over D_π, and a subset $CH_\pi \subseteq S_\pi$. The rejection checker RC is a DPT algorithm which returns either 0 or 1 on input string res.

The protocol between P and V constructed by $(Su, \{D_\pi, R_\pi, S_\pi,\}_\pi, \{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC)$ is depicted in Figure 1. Intuitively, a public key *pk* and a first message cmt, called *commitment*, are made by $f_\pi(sk)$ for a secret key $sk \leftarrow_R D_\pi^{sk}$ and f_π(st) for a state string $st \leftarrow_R D_\pi^{st}$, respectively. A second message cha, called *challenge*, is chosen uniformly at random from CH_π. Then, a third message res, called *response*, is set to $st + sk \cdot cha \in D_\pi$. The verification is done by checking whether or not res passes the check of RC and $f_\pi(res) = cmt + pk \cdot cha$ holds over R_π by the linearity of f_π.



Prover P with sk
$(sk, pk) \leftarrow \mathrm{Kg}(\pi)$
$\pi \leftarrow \mathrm{Su}(1^\lambda)$
Verifier V with pk
$\mathrm{st} \leftarrow_{\mathrm{R}} D_\pi^{\mathrm{st}}$
$\mathrm{cmt} = f_\pi(\mathrm{st})$
$\xrightarrow{\mathrm{cmt}}$
$\xleftarrow{\mathrm{cha}}$
$\mathrm{cha} \leftarrow_{\mathrm{U}} CH_\pi$
$\mathrm{res} = \mathrm{st} + sk \cdot \mathrm{cha}$
$\xrightarrow{\mathrm{res}}$
$\mathrm{res} = \perp$ if $\mathrm{RC}(\mathrm{res}) \neq 1$
output
$\mathrm{Vr}(\pi, pk, \mathrm{cmt}, \mathrm{cha}, \mathrm{res})$
$\mathrm{Kg}(\pi)$:
(1) $sk \leftarrow_{\mathrm{R}} D_\pi^{sk}$; $pk = f_\pi(sk)$.
(2) return (sk, pk).
$\mathrm{Vr}(\pi, pk, \mathrm{cmt}, \mathrm{cha}, \mathrm{res})$: return 1 if
(VC.1) $\mathrm{RC}(\mathrm{res}) = 1$,
(VC.2) $f(\mathrm{res}) = \mathrm{cmt} + pk \cdot \mathrm{cha}$.

Figure 1. Description of succinct LID scheme

We note that the succinct ID scheme can capture ID schemes using rejection sampling [12] by setting RC appropriately.

The representative properties of ID schemes [12, 21] are listed as follows: Consider any λ, any $\pi \in [Su(1^\lambda)]$, any $(sk, pk) \in [Kg(\pi)]$, and any (cmt, cha, res) generates as in Figure 1,

- ϵ-completeness: It holds that $res \neq \perp$ with at least probability ϵ (λ). And Vr(π, *pk*, cmt, cha, res) = 1 always holds if $res \neq \perp$.
- ϵ_s-simulatability: There exists an PPT algorithm Sim which returns $(\overline{\mathrm{cmt}}, \overline{\mathrm{cha}}, \overline{\mathrm{res}})$ on (π, pk) satisfying the followings:
  (A) the statistical distance between the distribution of $(\overline{\mathrm{cmt}}, \overline{\mathrm{cha}}, \overline{\mathrm{res}})$ and that of (cmt,cha,res) under the condition that RC(res) = 1 is at most ϵ_s (λ); and
  (B) $Vr(\pi, pk, \overline{\mathrm{cmt}}, \overline{\mathrm{cha}}, \overline{\mathrm{res}}) = 1$.
- η-commitment-min-entropy: The minimum value of $\log_2 1/\alpha(\pi, sk)$ is η, where $\alpha(\pi, sk)$ means the maximum probability that cmt = f_π(st) with $sk \leftarrow_R D_\pi^{st}$ for any fixed cmt $\in R_\pi$.

2.1.2 Lossy Identification Scheme

A lossy ID scheme [12, 22] is another variant of an ID scheme which has a PPT algorithm Kg$_L$. Since we now focus on succinct LID schemes rather than ordinary ID schemes, we directly add the lossy property to succinct LID schemes $(Su, \{D_\pi, R_\pi, S_\pi,\}_\pi,$ $\{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC)$. Kg$_L$ returns a *lossy public key*

$\overline{pk}$ on $\pi \in [Su(1^\lambda)]$, and it has the following properties: Let $\pi \in [Su(1^\lambda)]$ for any λ.

- (T_K, ϵ_K)-indistinguishability: For any probabilistic algorithm A of running time at most T_K, A can determine that a given public key pk is generated by either $\mathrm{Kg}_L(\pi)$ or $\mathrm{Kg}(\pi)$ with the probability at most $\epsilon_K(\lambda)$.
- ϵ_L -lossiness: The expected value of the maximum probability that res which induces that $Vr(\pi, \overline{pk}, cmt, cha, res) = 1$ exists is at most $\epsilon_L(\lambda)$, where $\overline{pk} \to Kg_L(\pi)$, $cha \leftarrow_U CH_\pi$ and the maximum is considered among $cmt \in D_\pi$.

2.2 Multisignature Schemes

A multisignature scheme [1] with S signers $\{S_i\}_{i=1}^S$ consists of the four algorithms (Setup, KGen, Sign, Ver). Given a security parameter 1^λ, Setup returns a public parameter pp. For each $1 \le i \le S$, S_i issues a pair (sk_i, pk_i) of a secret key sk_i and its public key pk_i by using KGen on pp. Each S_i executes Sign on a tuple (pp, sk_i, L, M) of a public parameter pp, S_i's secret key sk_i, a set $L = \{pk_j\}_{j=1}^S$ of all signers' public keys and a message M to issue a multisignature σ on the pair (L, M) with the interaction among all signers. Ver returns 1 on a tuple (pp, L, M, σ) of a public parameter pp, a set L of public keys, a message M and a multisignature σ if σ is valid.

- Correctness: For any λ, any $pp \in [Setup(1^\lambda)]$ and any message M, for each $1 \le i \le S$, S_i issues a pair $(sk_i, pk_i) \leftarrow KGen(pp)$ and then for $L = \{pk_j\}_{j=1}^S$, executes $Sign(pp, sk_i, L, M)$ to issue a multisignature σ on (L, M). Then, Ver(pp, L, M, σ) = 1 holds.
- Security: We introduce the security in the plain public key model [1]. This is defined by the security game as in Figure 2. Then, a multisignature scheme is (S, T, q_s, ϵ)-*secure in the plain public key model* if any PPT forger F of running time at most T and making at most q_s queries in Signing phase can win the game with S signers with the probability ϵ. In the case of the random oracle model, the (S, T, q_0, q_1, ..., q_s, ϵ)-*security in the plain public key model* means the (S, T, q_s, ϵ)-security in the plain public key model in which F can make at most q_k queries to the random oracle H_k.

3 Relationship between Linearity and Lossiness

We discuss the relationship between the linearity and the lossiness of ID schemes. We first show that a succinct LID scheme $(Su, \{D_\pi, R_\pi, S_\pi, \}_\pi,$ $\{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC)$ as in Figure 1 with a lossy key generator Kg_L has the lossiness.

- Init: C generates $pp \leftarrow$ Setup(1^λ) and (sk^*, pk^*) $\leftarrow$ KGen(pp), then sends (pp, pk^*) to F.
- Signing: When F queries a pair ($L^{(t)}$, $M^{(t)}$), then C and F run the signing protocol to issue a multisignature $\sigma^{(t)}$. Here, C plays the role of the signer owning sk^*, whereas F does that of the other co-signers.
- Challenge: When F finally returns (L^*, M^*, σ^*), F wins if the followings hold:
  (1) $pk^* \in L^*$.
  (2) (L^*, M^*) is not queried in Signing phase.
  (3) Ver(pp, L^*, M^*, σ^*) = 1.

Figure 2. Plain public key game

We first introduce a new property called *the difference soundness*. Intuitively, the difference soundness states that there are no distinct pairs (cha, res) which satisfy the specific formula concerning f_π and pk except the small probability. The formal definition of the difference soundness is given as follows.

Definition 1. For any λ and any $\pi \in [Su(1^\lambda)]$, let X be a family of sets $X_\pi \subseteq D_\pi$ parameterized by π. Then the (X, ϵ_{dif})-difference soundness states that the probability that there exist $cha \ne cha' \in CH_\pi$ and $res, res' \in X_\pi$ such that $f_\pi(res - res') = pk \cdot (cha - cha')$ is at most $\epsilon_{\mathrm{dif}}(\lambda)$, where the probability is taken over $\pi \leftarrow Su(1^\lambda)$ and $pk \leftarrow Kg_L(\pi)$.

We show that the difference soundness implies the lossiness in succinct LID schemes.

Lemma 1. *Let* $(Su, \{D_\pi, R_\pi, S_\pi, \}_\pi, \{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC)$ *be a succinct LID with a lossy key generator Kg_L. And, let RS = $\{RS_\pi\}_\pi$ be a family of sets* $RS_\pi = \{res \in D_\pi \mid RC(res) = 1\}$. *Assume that the succinct LID has the* (RS, ϵ_{dif}) *-difference soundness. Then, it is* ($1/|CH_\pi|$ $+ \epsilon_{\mathrm{dif}}$) *-lossy.*

Proof. Let $\pi \leftarrow Su(1^\lambda)$ and $pk \leftarrow Kg_L(\pi)$. We first show that for any $cmt \in R_\pi$, the probability that there exist two pairs $(cha, res), (cha', res') \in CH_\pi \times RS_\pi$ such that $cha \ne cha'$ and Vr(π, pk, cmt, cha, res) = Vr(π, pk, cmt, cha', res') = 1 is at most ϵ_{dif}. Assume that there are two such pairs. This implies that $f_\pi(res) = cmt + pk \cdot cha$ and $f_\pi(res') = cmt + pk \cdot cha'$. Hence, we have $f_\pi(res - res') = f_\pi(res) - f(res') = pk \cdot (cha - cha')$. It follows from the ($RS$, ϵ_{dif})-difference soundness that such a probability is at most ϵ_{dif}.

Assume that for any $cmt \in R_\pi$, there are only one $(cha, res) \in CH_\pi \times RS_\pi$ such that Vr(π, pk, cmt, cha, res) = 1. Due to $cha \leftarrow_U CH_\pi$, the probability that such a challenge cha appears is $1/|CH_\pi|$. Totally, we can ensure the $(1/|CH_\pi| + \epsilon_{\mathrm{dif}})$-lossiness.

To propose a generic construction of multisignature schemes in the next section, we introduce new notions, *batch rejection checker*, and *summing lossiness*.

- batch rejection checker[1]: For each $1 \le i \le S$, let $res_i \in RS_\pi$. The batch rejection checker BRC is a DPT algorithm which returns 1 on res if $res = \sum_{i=1}^{S} res_i$ and $\mathrm{RC}(\mathrm{res}_i) = 1$ for all $1 \le i \le S$.
- ϵ_L-summing lossiness: The expected value of the maximum probability that res satisfies the condition $f_\pi(res) = cmt + pk^* \cdot cha + \sum_{i=2}^{S} pk_i \cdot ch_i$ is at most ϵ_L, where $\pi \leftarrow \mathrm{Su}(1^\lambda)$, $pk^* \leftarrow \mathrm{Kg}_L(\pi)$ and $cha \leftarrow_U CH_\pi$, the maximum is considered among the choice of cmt, $(pk_2, ..., pk_S)$ and $(\mathrm{cha}_2, ..., \mathrm{cha}_S)$.

In a similar manner to Lemma 1, we can show the following lemma on the summing lossiness.

Lemma 2. *Let* $(Su, \{D_\pi, R_\pi, S_\pi,\}_\pi, \{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC)$ *be a succinct LID with a lossy key generator* Kg_L. *And, let* $RS^{sres} = \{RS_\pi^{sres}\}_\pi$ *be a family of sets* $RS_\pi^{sres} = \{res = \sum_{i=1}^{S} res_i \mid \forall 1 \le i \le S, res_i \in RS_\pi\}$. *Assume that the succinct LID has the* $(RS^{sres}, \epsilon_{\mathrm{dif}})$*-difference soundness. Then, it is* $(1/|CH_\pi| + \epsilon_{\mathrm{dif}})$*-summing lossy.*

Proof. Assume that $\pi \leftarrow \mathrm{Su}(1^\lambda)$ and $pk^* \leftarrow \mathrm{Kg}_L(\pi)$. We consider the tuple $(pk_2, ..., pk_S)$ of public keys and the tuple $(\mathrm{cha}_2, ..., \mathrm{cha}_S)$ of elements in CH_π. We first show that for any cmt, there is only one $(cha, res) \in CH_\pi \times RS_\pi^{sres}$ such that the verification formula $f_\pi(res) = cmt + pk^* \cdot cha + \sum_{i=1}^{S} pk_i \cdot cha_i$ is satisfied except the probability ϵ_{dif}. Assume that there are two such pairs $(cha, res), (cha', res') \in CH_\pi \times RS_\pi^{sres}$ such that cha', cha'. Then, we have

$$f_\pi(res) = cmt + pk^* \cdot cha + \sum_{i=1}^{S} pk_i \cdot cha_i,$$

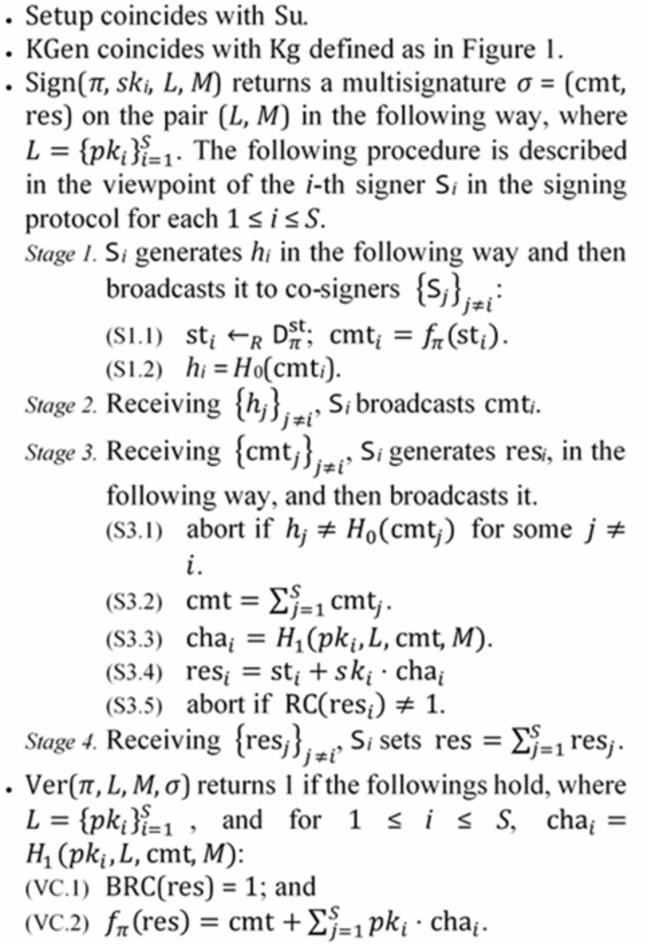
$$f_\pi(res') = cmt + pk^* \cdot cha' + \sum_{i=1}^{S} pk_i \cdot cha_i,$$

This implies that $f_\pi(\mathrm{res} - \mathrm{res}') = f_\pi(\mathrm{res}) - f_\pi(\mathrm{res}') = pk^* \cdot (\mathrm{cha} - \mathrm{cha}')$. By the $(RS^{\mathrm{sres}}, \epsilon_{\mathrm{dif}})$-difference soundness, the probability that such equation holds is at most ϵ_{dif}.

Due to $cha \leftarrow_U CH_\pi$, we can ensure the $(1/|CH_\pi| + \epsilon_{\mathrm{dif}})$-summing lossy.

4 Proposed Multisignature

In this section, we propose a generic construction of multisignature schemes from succinct LID schemes. Let $LID = (Su, \{D_\pi, R_\pi, S_\pi,\}_\pi, \{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC)$ be a succinct LID which has the batch rejection checker. For a polynomial δ, let H_0: $R_\pi \rightarrow \{0,1\}^\delta$ and H_1 : $\{0,1\}^* \rightarrow CH_\pi$ be hash functions. The hash functions H_0 and H_1 are treated as the random oracle, respectively. Then, our proposed construction MS[*LID*] is given in Figure 3.



- Setup coincides with Su.
- KGen coincides with Kg defined as in Figure 1.
- Sign(π, sk_i, L, M) returns a multisignature σ = (cmt, res) on the pair (L, M) in the following way, where $L = \{pk_i\}_{i=1}^S$. The following procedure is described in the viewpoint of the *i*-th signer S_i in the signing protocol for each $1 \le i \le S$.

Stage 1. S_i generates h_i in the following way and then broadcasts it to co-signers $\{\mathsf{S}_j\}_{j \ne i}$:

(S1.1) $\mathrm{st}_i \leftarrow_R \mathrm{D}_\pi^{\mathrm{st}}$; $\mathrm{cmt}_i = f_\pi(\mathrm{st}_i)$.

(S1.2) $h_i = H_0(\mathrm{cmt}_i)$.

Stage 2. Receiving $\{h_j\}_{j \ne i}$, S_i broadcasts cmt_i.

Stage 3. Receiving $\{\mathrm{cmt}_j\}_{j \ne i}$, S_i generates res_i, in the following way, and then broadcasts it.

(S3.1) abort if $h_j \ne H_0(\mathrm{cmt}_j)$ for some $j \ne i$.

(S3.2) $\mathrm{cmt} = \sum_{j=1}^S \mathrm{cmt}_j$.

(S3.3) $\mathrm{cha}_i = H_1(pk_i, L, \mathrm{cmt}, M)$.

(S3.4) $\mathrm{res}_i = \mathrm{st}_i + sk_i \cdot \mathrm{cha}_i$

(S3.5) abort if $\mathrm{RC}(\mathrm{res}_i) \ne 1$.

Stage 4. Receiving $\{\mathrm{res}_j\}_{j \ne i}$, S_i sets $\mathrm{res} = \sum_{j=1}^S \mathrm{res}_j$.

- Ver(π, L, M, σ) returns 1 if the followings hold, where $L = \{pk_i\}_{i=1}^S$, and for $1 \le i \le S$, $\mathrm{cha}_i = H_1(pk_i, L, \mathrm{cmt}, M)$:

(VC.1) BRC(res) = 1; and

(VC.2) $f_\pi(\mathrm{res}) = \mathrm{cmt} + \sum_{j=1}^S pk_i \cdot \mathrm{cha}_i$.

Figure 3. Proposed Multisignature Scheme MS [*LID*]

4.1 Correctness

The correctness of MS[*LID*] can be proven in the following way. For any security parameter λ, let us consider the situation that for any $\pi \in [\mathrm{Setup}(1^\lambda)]$, any message *M* and for each $1 \le i \le S$, S_i issues a pair $(sk_i, pk_i) \in [\mathrm{KGen}(\pi)]$ and executes Sign(π, sk_i, L, M) to issue a multisignature σ = (cmt, res) of *M* with respect

[1] This condition was called the "product verifying condition" in the proceeding version. We rename it so that the new name represents the requirement of this condition intuitively, since BRC considers only the results of RC for all res_i, not all conditions required in the verification.

to $L = \{pk_i\}_{i=1}^{S}$. Assume that for each 1 ≤ i ≤ S, S_i passes (S3.5) in Sign. Namely, for each 1 ≤ i ≤ S, we have RC(res$_i$) = 1. It follows from the definition of the batch rejection checker and $res = \sum_{i=1}^{S} res_i$ that BRC(res) = 1. Therefore, the condition (VC.1) is satisfied.

The procedures (S1.1), (S3.3) and (S3.4), the definitions of Kg in Figure 1 and the linearity of f_π implies that

$$\begin{aligned} f_\pi(res) &= f_\pi\left(\sum_{i=1}^{S} res_i\right) \\ &= \sum_{i=1}^{S} f_\pi(res_i) \\ &= \sum_{i=1}^{S} f_\pi(st_i + sk_i \cdot cha_i) \\ &= \sum_{i=1}^{S} (f_\pi(st_i) + f_\pi(sk_i) \cdot cha_i) \qquad \textbf{(1)} \\ &= \sum_{i=1}^{S} (cmt_i + pk_i \cdot cha_i) \\ &= \sum_{i=1}^{S} cmt_i + \sum_{i=1}^{S} pk_i \cdot cha_i \\ &= cmt + \sum_{i=1}^{S} pk_i \cdot cha_i \end{aligned}$$

Therefore, the condition (VC.2) is satisfied.

We next evaluate the abort probability in (S3.5). We fix an index 1 ≤ i ≤ S. Since the random oracle H_1 chooses cha$_i$, cha$_i$ distributes uniformly over CH_π. This is the same as in Figure 1. On the other hand, cmt$_i$ and res$_i$ are computed as in Figure 1 in (S1.1) and (S3.4), respectively. The ϵ -completeness implies that S$_i$ does not abort with the probability over ϵ. In this signing protocol, all signers are required to pass this check simultaneously. Thus, the abort probability during the protocol is $1-\epsilon^{S}$.

4.2 Security Proof

In this section, we show the tight security of our proposed multisignature scheme.

Theorem 1. For a succinct LID scheme $LID = (Su, \{D_\pi, R_\pi, S_\pi, \}_\pi, \{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC)$ having the batch rejection checker BRC and the lossy key generator Kg$_L$, assume that LID is ϵ -complete, ϵ_s -simulatable, η-commitment-min-entropy, (T_K, ϵ_K) -indistinguishable and ϵ_L -summing lossy. Then, MS [LID] is (S, T, q_0, q_1, q_s, ϵ)-secure in the plain public key model and the random oracle model, where

$$\begin{aligned} &T = T_K - poly, \\ &\epsilon \le \epsilon_K + q_s\epsilon_S + \epsilon_L \\ &\quad + \frac{(q_0 + q_s S - 1)(q_0 + q_s S)}{2^{\delta}} \\ &\quad + \frac{1}{|R_\pi|} + \frac{(q_0 + q_s - 1)(q_1 + q_s)}{2^{\eta}}. \end{aligned}$$

Proof. We show the statement by the hybrid argument. Assume that F is a forger which wins the ppk game with probability ϵ. For any $0 \le k \le 5$, let **Game**$_k$ be the security game defined below and W_k be the event that F wins **Game**$_k$, respectively.

The idea of the proof is based on [12]. Namely, Signing phase is replaced with a simulator which does not use the secret key by utilizing the simulatability of the underlying linear ID scheme and the programming technique which is allowed in the random oracle model. It is mainly done in **Game**$_4$, while the preparation for the simulation is done in **Game**$_1$ to **Game**$_3$. In **Game**$_5$, the challenge public key pk^* given to C is replaced with the lossy one. Note that the key indistinguishability guarantees this replacement. We evaluate the difference of the winning probabilities of F between the games. Finally, the winning probability by any unbounded forger F in **Game**$_5$ is shown to be negligible.

Game$_0$: This game is the ppk game of the proposed multisignature scheme as in Figure 4. Therefore, we have

$$\Pr[W_0] = \epsilon. \qquad \textbf{(2)}$$

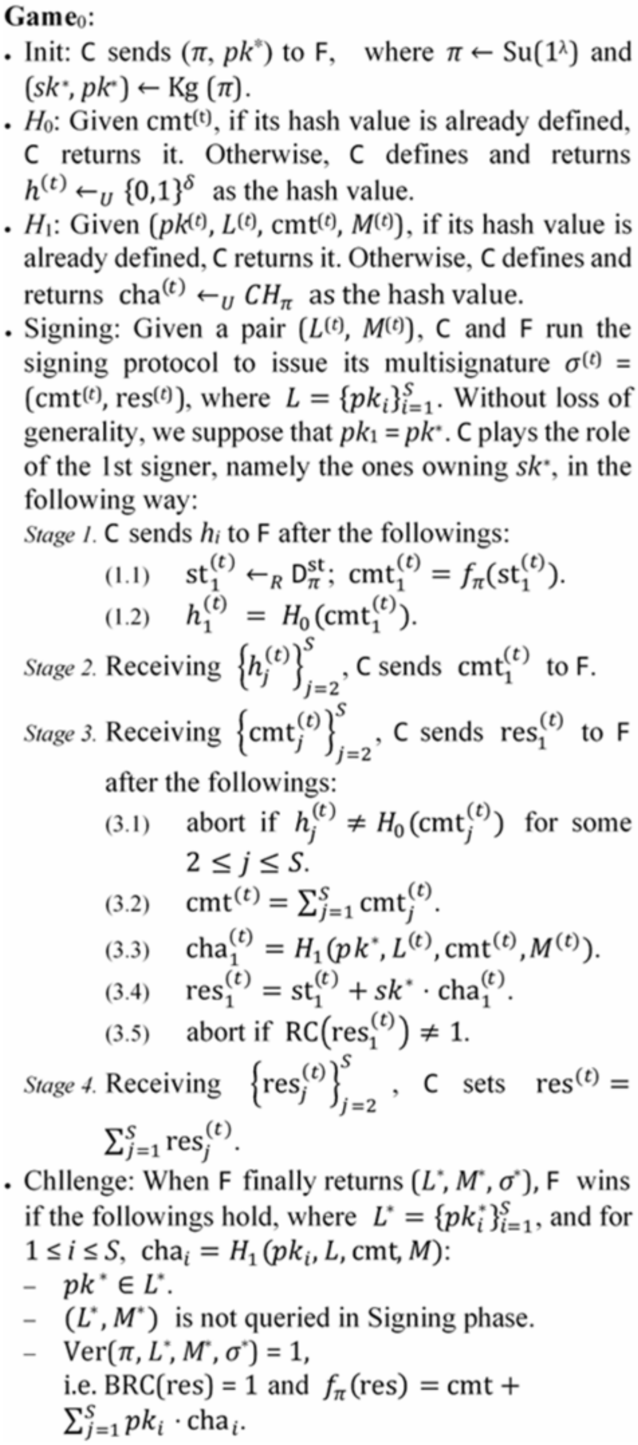
Game$_1$: In H_0 phase, C aborts this game if the value $h^{(t)}$ is already set as the hash value of some previous query as described in Figure 5.

To evaluate the difference between W$_1$ and W$_0$, we now estimate the abort probability. Before proceeding to H_0 phase on a t'-th query, at most t' − 1 distinct hash values on H_0 are already defined. Since H_0 phase is totally queried at most q_0 times by F and at most q_sS times by C in Signing phase, the abort probability is evaluated as follows:

$$\begin{aligned} &\Pr_{h_t \leftarrow_U \{0,1\}^{\delta}}[h_t \in \{h_{t'}\}_{t'=1}^{t-1}] \\ &= \sum_{t=1}^{q_0+q_sS} \frac{t-1}{2^{\delta}} \\ &\le \frac{(q_0 + q_s S - 1)(q_0 + q_s S)}{2^{\delta}} \end{aligned}$$

Thus, we have

$$\begin{aligned} &|\Pr[W_1] - \Pr[W_0]| \le \\ &\frac{(q_0 + q_s S - 1)(q_0 + q_s S)}{2^{\delta}}. \qquad \textbf{(3)} \end{aligned}$$



Game$_0$:

- Init: C sends (π, pk^*) to F, where $\pi \leftarrow \mathsf{Su}(1^\lambda)$ and $(sk^*, pk^*) \leftarrow \mathsf{Kg}(\pi)$.
- H_0: Given $\mathrm{cmt}^{(t)}$, if its hash value is already defined, C returns it. Otherwise, C defines and returns $h^{(t)} \leftarrow_U \{0,1\}^\delta$ as the hash value.
- H_1: Given $(pk^{(t)}, L^{(t)}, \mathrm{cmt}^{(t)}, M^{(t)})$, if its hash value is already defined, C returns it. Otherwise, C defines and returns $\mathrm{cha}^{(t)} \leftarrow_U CH_\pi$ as the hash value.
- Signing: Given a pair $(L^{(t)}, M^{(t)})$, C and F run the signing protocol to issue its multisignature $\sigma^{(t)} = (\mathrm{cmt}^{(t)}, \mathrm{res}^{(t)})$, where $L = \{pk_i\}_{i=1}^S$. Without loss of generality, we suppose that $pk_1 = pk^*$. C plays the role of the 1st signer, namely the ones owning sk^*, in the following way:

  Stage 1. C sends h_i to F after the followings:

  (1.1) $\mathrm{st}_1^{(t)} \leftarrow_R \mathrm{D}_\pi^{\mathrm{st}}$; $\mathrm{cmt}_1^{(t)} = f_\pi(\mathrm{st}_1^{(t)})$.

  (1.2) $h_1^{(t)} = H_0(\mathrm{cmt}_1^{(t)})$.

  Stage 2. Receiving $\left\{h_j^{(t)}\right\}_{j=2}^S$, C sends $\mathrm{cmt}_1^{(t)}$ to F.

  Stage 3. Receiving $\left\{\mathrm{cmt}_j^{(t)}\right\}_{j=2}^S$, C sends $\mathrm{res}_1^{(t)}$ to F after the followings:

  (3.1) abort if $h_j^{(t)} \neq H_0(\mathrm{cmt}_j^{(t)})$ for some $2 \le j \le S$.

  (3.2) $\mathrm{cmt}^{(t)} = \sum_{j=1}^S \mathrm{cmt}_j^{(t)}$.

  (3.3) $\mathrm{cha}_1^{(t)} = H_1(pk^*, L^{(t)}, \mathrm{cmt}^{(t)}, M^{(t)})$.

  (3.4) $\mathrm{res}_1^{(t)} = \mathrm{st}_1^{(t)} + sk^* \cdot \mathrm{cha}_1^{(t)}$.

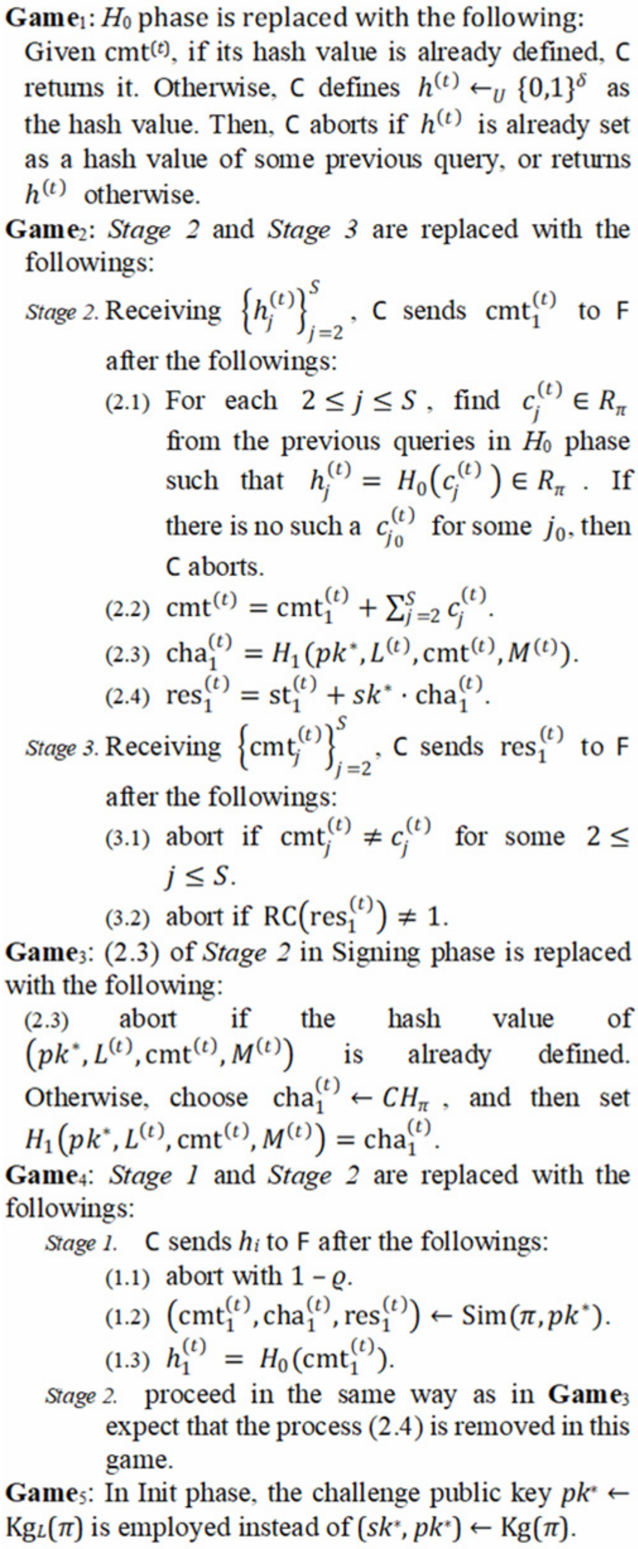
  (3.5) abort if $\mathrm{RC}(\mathrm{res}_1^{(t)}) \neq 1$.

  Stage 4. Receiving $\left\{\mathrm{res}_j^{(t)}\right\}_{j=2}^S$, C sets $\mathrm{res}^{(t)} = \sum_{j=1}^S \mathrm{res}_j^{(t)}$.
- Chllenge: When F finally returns (L^*, M^*, σ^*), F wins if the followings hold, where $L^* = \{pk_i^*\}_{i=1}^S$, and for $1 \le i \le S$, $\mathrm{cha}_i = H_1(pk_i, L, \mathrm{cmt}, M)$:
  - $pk^* \in L^*$.
  - (L^*, M^*) is not queried in Signing phase.
  - $\mathrm{Ver}(\pi, L^*, M^*, \sigma^*) = 1$, i.e. $\mathrm{BRC}(\mathrm{res}) = 1$ and $f_\pi(\mathrm{res}) = \mathrm{cmt} + \sum_{j=1}^S pk_i \cdot \mathrm{cha}_i$.

Figure 4. Game$_0$

Game$_2$: For each query to Signing phase, a hash value $cha_1^{(t)}$ of H_1 is computed in *Stage 2* instead of *Stage 3* as in Figure 5.

We fix a t-th query to Signing phase. Assume that C does not abort in (2.1) during **Game**$_2$. Namely, for all $2 \le j \le S$, there exists $c_j^{(t)} \in R_\pi$ such that the hash value of $c_j^{(t)}$ on H_0 is already defined as h_j which is given by F. Then, we show that the replaced condition $cmt_j^{(t)} \neq c_j^{(t)}$ at (3.1) in **Game**$_2$ is equivalent to the one $h_j^{(t)} \neq H_0(cmt_j^{(t)})$ which is the original condition. We fix an index $2 \le j \le S$. If $cmt_j^{(t)} = c_j^{(t)}$, then the assumption implies that $h_j^{(t)} = H_0(c_j^{(t)}) = H_0(cmt_j^{(t)})$. On the other hand, if $h_j^{(t)} = H_0(cmt_j^{(t)})$, then we have $cmt_j^{(t)} = c_j^{(t)}$. This is because $h_j^{(t)} = H_0(c_j^{(t)})$ is assumed and there is only one $c \in R_\pi$ such that $h_j^{(t)} = H_0(c)$ by the setting at **Game**$_1$.



Game$_1$: H_0 phase is replaced with the following: Given $\mathrm{cmt}^{(t)}$, if its hash value is already defined, C returns it. Otherwise, C defines $h^{(t)} \leftarrow_U \{0,1\}^\delta$ as the hash value. Then, C aborts if $h^{(t)}$ is already set as a hash value of some previous query, or returns $h^{(t)}$ otherwise.

Game$_2$: *Stage 2* and *Stage 3* are replaced with the followings:

Stage 2. Receiving $\left\{h_j^{(t)}\right\}_{j=2}^S$, C sends $\mathrm{cmt}_1^{(t)}$ to F after the followings:

(2.1) For each $2 \le j \le S$, find $c_j^{(t)} \in R_\pi$ from the previous queries in H_0 phase such that $h_j^{(t)} = H_0\left(c_j^{(t)}\right) \in R_\pi$. If there is no such a $c_{j_0}^{(t)}$ for some j_0, then C aborts.

(2.2) $\mathrm{cmt}^{(t)} = \mathrm{cmt}_1^{(t)} + \sum_{j=2}^S c_j^{(t)}$.

(2.3) $\mathrm{cha}_1^{(t)} = H_1(pk^*, L^{(t)}, \mathrm{cmt}^{(t)}, M^{(t)})$.

(2.4) $\mathrm{res}_1^{(t)} = \mathrm{st}_1^{(t)} + sk^* \cdot \mathrm{cha}_1^{(t)}$.

Stage 3. Receiving $\left\{\mathrm{cmt}_j^{(t)}\right\}_{j=2}^S$, C sends $\mathrm{res}_1^{(t)}$ to F after the followings:

(3.1) abort if $\mathrm{cmt}_j^{(t)} \neq c_j^{(t)}$ for some $2 \le j \le S$.

(3.2) abort if $\mathrm{RC}(\mathrm{res}_1^{(t)}) \neq 1$.

Game$_3$: (2.3) of *Stage 2* in Signing phase is replaced with the following:

(2.3) abort if the hash value of $\left(pk^*, L^{(t)}, \mathrm{cmt}^{(t)}, M^{(t)}\right)$ is already defined. Otherwise, choose $\mathrm{cha}_1^{(t)} \leftarrow CH_\pi$, and then set $H_1\left(pk^*, L^{(t)}, \mathrm{cmt}^{(t)}, M^{(t)}\right) = \mathrm{cha}_1^{(t)}$.

Game$_4$: *Stage 1* and *Stage 2* are replaced with the followings:

Stage 1. C sends h_i to F after the followings:

(1.1) abort with $1 - \varrho$.

(1.2) $\left(\mathrm{cmt}_1^{(t)}, \mathrm{cha}_1^{(t)}, \mathrm{res}_1^{(t)}\right) \leftarrow \mathrm{Sim}(\pi, pk^*)$.

(1.3) $h_1^{(t)} = H_0(\mathrm{cmt}_1^{(t)})$.

Stage 2. proceed in the same way as in **Game**$_3$ expect that the process (2.4) is removed in this game.

Game$_5$: In Init phase, the challenge public key $pk^* \leftarrow \mathsf{Kg}_L(\pi)$ is employed instead of $(sk^*, pk^*) \leftarrow \mathsf{Kg}(\pi)$.

Figure 5. Game$_1$–Game$_5$

We next evaluate the abort probability at (2.1). The abortion at this point means that F sends $h_j^{(t)}$ which is not obtained from H_0 phase for some $2 \le j \le S$. On the other hand, F is required to find c such that $h_j^{(t)} = H_0(c)$. However, the hash value of c on H_0 is distributed uniformly at random over R_π as in H_0 phase. It follows that the abort probability is evaluated by at most $1/|R_\pi|$. Thus, we have

$$|\Pr[W_2] - \Pr[W_1]| \le \frac{1}{|R_\pi|}. \qquad \textbf{(4)}$$

Game$_3$: For each t-th execution of (2.3), C aborts if the hash value of (pk^*, $L^{(t)}$, cmt$^{(t)}$, $M^{(t)}$) on H_1 is already defined. Otherwise, the hash value is programmed to $cha_1^{(t)} \leftarrow_U CH_\pi$.

For each t-th execution of (2.3), such a programming is succeeded if the hash value of (pk^*, $L^{(t)}$, cmt$^{(t)}$, $M^{(t)}$) on H_1 is not defined yet before the execution. This can be evaluated by the probability that cmt$^{(t)}$ already appears as part of some previous query at H_1 phase. Recall that cmt$^{(t)}$ is set as in $cmt_1^{(t)} + \sum_{j=2}^{S} c_j^{(t)}$ in (2.1). η-commitment-min-entropy implies that for any $\{c_j^{(t)}\}_{j=2}^{S}$, such a probability is evaluated as $1/2^\eta$.

On the other hand, (2.3) is executed at most $q_1 + q_s$ times. In a similar manner to the evaluation of the abort probability in **Game**$_1$, the abort probability is therefore at most $\sum_{t=1}^{q_1+q_S} \frac{(t-1)}{2^\eta} \le \frac{(q_1+q_S-1)(q_1+q_S)}{2^\eta}$.

Thus, we

$$|\Pr[W_3] - \Pr[W_2]| \le \frac{(q_1+q_S-1)(q_1+q_S)}{2^\eta}. \qquad \textbf{(5)}$$

Game$_4$: A tuple $(cmt_1^{(t)}, cha_1^{(t)}, res_1^{(t)})$ is computed by using Sim in (1.2). More precisely, *Stage 1*, and *Stage 2* in this game are depicted in Figure 5.

Observe that $(cmt_1^{(t)}, cha_1^{(t)}, res_1^{(t)})$ in **Game**$_3$ is generated as in Figure 1 by $cha_1^{(t)} \leftarrow_U CH_\pi$. ϵ-completeness implies that $RC(res_1^{(t)}) \ne 1$ with the probability $1 - \epsilon$. In other words, **Game**$_3$ aborts with the probability $1 - \epsilon$ due to ϵ-completeness. To capture this situation in **Game**$_4$, C aborts **Game**$_4$ with the same probability in (1.1) because $(cmt_1^{(t)}, cha_1^{(t)}, res_1^{(t)})$ by Sim always passes the verification.

We consider the situation where C does not abort. In this situation, $(cmt_1^{(t)}, cha_1^{(t)}, res_1^{(t)})$ in **Game**$_3$ is generated as in Figure 1 so that $RC(res_1^{(t)}) = 1$, whereas it in **Game**$_4$ is generated by the simulator Sim. The ϵ_s-simulatability implies that the statistical distance of the distributions of $(cmt_1^{(t)}, cha_1^{(t)}, res_1^{(t)})$ in both games is at most ϵ_s. Since Signing phase is executed as most q_s times, we have

$$|\Pr[W_4] - \Pr[W_3]| \le q_S\epsilon_s. \qquad \textbf{(6)}$$

Game$_5$: A challenge public key pk^* is generated by using Kg$_L$ instead of KGen = Kg as in Figure 5.

Since this change is directly implied by the (T_K, ϵ_K)-indistinguishability of *LID*, we have

$$|\Pr[W_5] - \Pr[W_4]| \le \epsilon_K. \qquad \textbf{(7)}$$

The upper bound that W_5 occurs: For $L^* = \{pk_i^*\}_{i=1}^{S}$ such that $pk_i^* = pk^*$ and $\sigma^* = (cmt^*, res^*)$, let ($L^*$, M^*, σ^*) be the final output of F at **Game**$_5$. The probability of W_5 is evaluated by the chance to set a "good" challenge cha_1^*, which induces the acceptance, as the hash value of (pk^*, L^*, cmt^*, M^*) on H_1. This is naturally evaluated by the ϵ_L-summing lossiness. Thus, we have

$$\Pr[W_5] \le \epsilon_L. \qquad \textbf{(8)}$$

Putting together with Eqs. (2)-(8), it holds that

$$\epsilon \le \epsilon_K + q_s\epsilon_S + \epsilon_L + \frac{(q_0+q_sS-1)(q_0+q_sS)}{2^\delta} + \frac{1}{|R_\pi|} + \frac{(q_0+q_s-1)(q_0+q_s)}{2^\delta}.$$

By combining Theorem 1 and Lemma 2, the following holds.

Corollary 1. For a succinct LID scheme $LID = (Su, \{D_\pi, R_\pi, S_\pi,\}_\pi, \{D_\pi^{sk}, D_\pi^{st}, CH_\pi\}, RC)$ having the batch rejection checker BRC and the lossy key generator Kg$_{\rm L}$, and the family $RS^{sres} = \{RS_\pi^{sres}\}_\pi$ defined in Lemma 2, assume that *LID* is ϵ-complete, ϵ_s-simulatable, η-commitment-min-entropy, (T_K, ϵ_K)-indistinguishable and (RS^{sres}, $\epsilon_{\rm dif}$)-difference sound. Then, MS[LID] is (S, T, q_0, q_1, q_s, ϵ)-secure in the plain public key model and the random oracle model, where

$$T = T_K - poly(\lambda),$$

$$\epsilon \le \epsilon_K + q_s\epsilon_S + \epsilon_L + \frac{1}{|CH_\pi|} + \epsilon_{\rm dif} + \frac{(q_0+q_sS-1)(q_0+q_sS)}{2^\delta} + + \frac{1}{|R_\pi|} + \frac{(q_0+q_s-1)(q_0+q_s)}{2^\eta}.$$

5 Application of Proposed Generic Construction

In this section, we show that our generic construction can be used to explain the existing tightly secure multisignature scheme and to obtain new multisiganture schemes by applying our generic construction to existing linear and lossy ID schemes. We consider the existing lossy ID schemes proposed in [8, 12], and observe that they satisfy linearity.

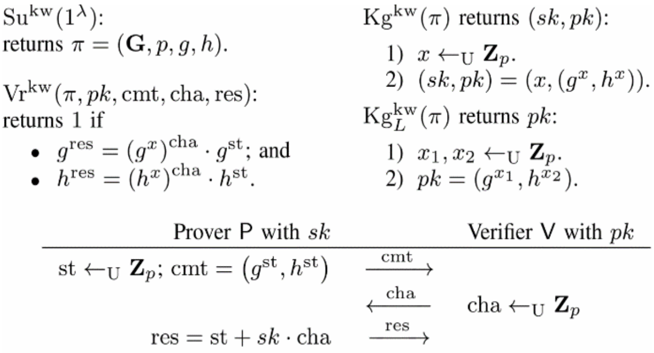
5.1 Mathematical Notations

Let **G** be a group of prime order p with generators g and h. For any natural number n, let $\boldsymbol{Z}_n$ and $\boldsymbol{Z}_n^*$ be the residue ring modulo n and its multiplicative group. $[a, b]$ denotes the set of all integers x satisfying $a \le x \le b$ for any integers $a \le b$. For any natural number n, $\boldsymbol{Z}_{|n|} = [-n, n]$. For natural numbers q and n, R represents $\boldsymbol{Z}_q[X]/(X^n + 1)$. And $R^\times$ is the set of all invertible elements in R. By letting $\boldsymbol{w} = \sum_{i=0}^{n-1} w_i X^i \in R$, the absolute value $|w_i|$ is considered to be less than $(q - 1)/2$, and $|w|$ means $\max_{0 \le i \le n-1} |w_i|$. For any number $\beta \le q$, $R^{\le\beta}$ is the set of all elements $w \in R$ such that $|w| \le \beta$. D_β stands for the distribution that assigns the probability proportional to $\exp(-\pi|y|^2/\beta^2)$ for any $y \in R$, where β is a number, and y is now represented as the n-dimensional coefficient vectors, or 0 otherwise.

We represent any vector as a column vector in this paper. For a vector $\boldsymbol{a}$, $\boldsymbol{a}^{\mathrm{T}}$ denotes the transpose of $\boldsymbol{a}$. For any vectors $\boldsymbol{a}$ and $\boldsymbol{x}$, $\langle \boldsymbol{a}, \boldsymbol{x} \rangle$ is defined by $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}$. A function ϵ is said to be *negligible in* λ, if for any polynomial v, there exists a natural number λ_0 such that for any $\lambda > \lambda_0$, $\epsilon(\lambda) < 1/v(\lambda)$. We write negl to denote some negligible function in λ.

5.2 KW ID Scheme

Figure 6 and Table 1 illustrate KW ID scheme [8], and the setting which is suitable to the succinct linearity of KW ID scheme, respectively. By applying our generic construction to KW ID scheme with the setting in Table 1, we can obtain the multisiganture scheme which is almost the same as the multisiganture scheme by [7]. The completeness, the simulatability, and the indistinguishability of KW ID scheme are discussed in [8]. The summing lossiness of KW ID was proven in [7]. Since BRC defined in Table 1 always returns 1, it is the batch rejection checker of KW ID. Therefore, the security of the resulting multisiganture can be interpreted by Theorem 1.



$\mathrm{Su}^{\mathrm{kw}}(1^\lambda)$:
returns $\pi = (\mathbf{G}, p, g, h)$.

$\mathrm{Vr}^{\mathrm{kw}}(\pi, pk, \mathrm{cmt}, \mathrm{cha}, \mathrm{res})$:
returns 1 if

- $g^{\mathrm{res}} = (g^x)^{\mathrm{cha}} \cdot g^{\mathrm{st}}$; and
- $h^{\mathrm{res}} = (h^x)^{\mathrm{cha}} \cdot h^{\mathrm{st}}$.

$\mathrm{Kg}^{\mathrm{kw}}(\pi)$ returns (sk, pk):
1) $x \leftarrow_{\mathrm{U}} \mathbf{Z}_p$.
2) $(sk, pk) = (x, (g^x, h^x))$.

$\mathrm{Kg}_L^{\mathrm{kw}}(\pi)$ returns pk:
1) $x_1, x_2 \leftarrow_{\mathrm{U}} \mathbf{Z}_p$.
2) $pk = (g^{x_1}, h^{x_2})$.

Prover P with sk | Verifier V with pk

$\mathrm{st} \leftarrow_{\mathrm{U}} \mathbf{Z}_p$; $\mathrm{cmt} = (g^{\mathrm{st}}, h^{\mathrm{st}})$ $\xrightarrow{\mathrm{cmt}}$

$\xleftarrow{\mathrm{cha}}$ $\mathrm{cha} \leftarrow_{\mathrm{U}} \mathbf{Z}_p$

$\mathrm{res} = \mathrm{st} + sk \cdot \mathrm{cha}$ $\xrightarrow{\mathrm{res}}$

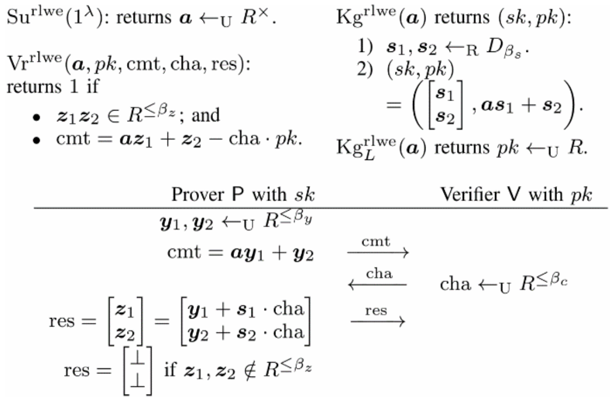
Figure 6. KW ID scheme [8]

Table 1. Setting of succinct LID based on KW ID scheme

π	(**G**, p, g, h)
D_π	$\mathbf{Z}_{\mathrm{p}}$
R_π	$\mathbf{G} \times \mathbf{G}$
S_π	$\mathbf{Z}_{\mathrm{p}}$
f_π	$x \mapsto (g^x, h^x)$
D_π^{sk}	$U(\mathbf{Z}_{\mathrm{p}})$
D_π^{st}	$U(\mathbf{Z}_{\mathrm{p}})$
CH_π	$\mathbf{Z}_{\mathrm{p}}$
RC (res)	always return 1
BRC (res)	always return 1

5.3 AFLT Lattice ID Scheme

In a similar manner to KW ID scheme, the succinct linearity of AFLT lattice ID scheme (Figure 7) can be discussed as in Table 2. The multisignature scheme given by applying our generic construction to the setting in Table 2 is almost the same as Fukumitsu-Hasegawa multisignature scheme [10], in which they showed the summing lossiness. The following lemma shows that AFLT lattice ID scheme has a batch rejection checker. Thus, the security of this multisignature is guaranteed by Theorem 1.



$\mathrm{Su}^{\mathrm{rlwe}}(1^\lambda)$: returns $\boldsymbol{a} \leftarrow_{\mathrm{U}} R^\times$.

$\mathrm{Vr}^{\mathrm{rlwe}}(\boldsymbol{a}, pk, \mathrm{cmt}, \mathrm{cha}, \mathrm{res})$:
returns 1 if

- $\boldsymbol{z}_1 \boldsymbol{z}_2 \in R^{\le\beta_z}$; and
- $\mathrm{cmt} = \boldsymbol{a}\boldsymbol{z}_1 + \boldsymbol{z}_2 - \mathrm{cha} \cdot pk$.

$\mathrm{Kg}^{\mathrm{rlwe}}(\boldsymbol{a})$ returns (sk, pk):
1) $\boldsymbol{s}_1, \boldsymbol{s}_2 \leftarrow_{\mathrm{R}} D_{\beta_s}$.
2) $(sk, pk) = \left(\begin{bmatrix}\boldsymbol{s}_1\\ \boldsymbol{s}_2\end{bmatrix}, \boldsymbol{a}\boldsymbol{s}_1 + \boldsymbol{s}_2\right)$.

$\mathrm{Kg}_L^{\mathrm{rlwe}}(\boldsymbol{a})$ returns $pk \leftarrow_{\mathrm{U}} R$.

Prover P with sk | Verifier V with pk

$\boldsymbol{y}_1, \boldsymbol{y}_2 \leftarrow_{\mathrm{U}} R^{\le\beta_y}$

$\mathrm{cmt} = \boldsymbol{a}\boldsymbol{y}_1 + \boldsymbol{y}_2$ $\xrightarrow{\mathrm{cmt}}$

$\xleftarrow{\mathrm{cha}}$ $\mathrm{cha} \leftarrow_{\mathrm{U}} R^{\le\beta_c}$

$\mathrm{res} = \begin{bmatrix}\boldsymbol{z}_1\\ \boldsymbol{z}_2\end{bmatrix} = \begin{bmatrix}\boldsymbol{y}_1 + \boldsymbol{s}_1 \cdot \mathrm{cha}\\ \boldsymbol{y}_2 + \boldsymbol{s}_2 \cdot \mathrm{cha}\end{bmatrix}$ $\xrightarrow{\mathrm{res}}$

$\mathrm{res} = \begin{bmatrix}\perp\\ \perp\end{bmatrix}$ if $\boldsymbol{z}_1, \boldsymbol{z}_2 \notin R^{\le\beta_z}$

Figure 7. AFLT lattice ID scheme [12], where $\boldsymbol{q}, \boldsymbol{n}, \boldsymbol{\beta}_s, \boldsymbol{\beta}_y, \boldsymbol{\beta}_c$, and $\boldsymbol{\beta}_z$ are some designated parameters [10, 12]

Table 2. Setting of succinct LID based on AFLT lattice ID scheme

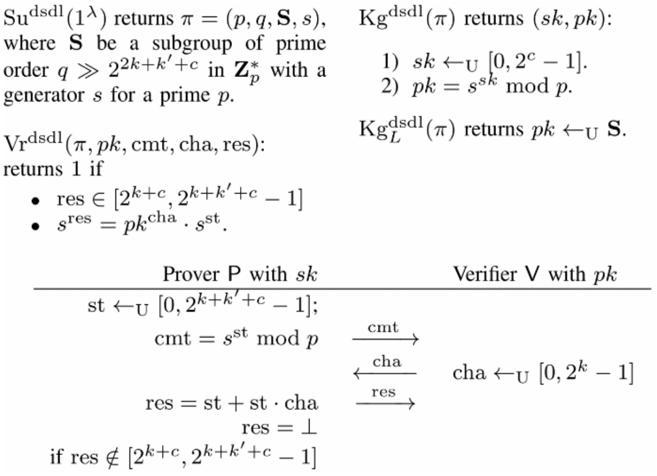
π	$\boldsymbol{a} \times R^{\times}$
Dπ	$R \times R$
Rπ	R
Sπ	R
fπ	$(x_1, x_2) \mapsto \boldsymbol{a}x_1 + x_2$
D_{π}^{sk}	$D\beta_s \times D\beta_s$
D_{π}^{st}	$U(R\leq^{\beta y}) \times U(R\leq^{\beta y})$
CH_{π}	$R^{\leq\beta c}$
RC (res)	return 1 if $\mathbf{z}_1, \mathbf{z}_2 \in R\leq^{\beta z}$ for res = $(\mathbf{z}_1, \mathbf{z}_2)$
BRC (res)	return 1 if $\mathbf{z}_1, \mathbf{z}_2 \in R\leq^{S\beta z}$ for res = $(\mathbf{z}_1, \mathbf{z}_2)$

Lemma 3. *BRC defined in Table 2 is a batch rejection checker of AFLT lattice ID scheme.*

Proof. Assume that RC(res_i) = 1 for each $1 \leq i \leq S$. This implies that $z_{i,1}, z_{i,2} \in R^{\leq\beta}$ for each $1 \leq i \leq S$, where $\text{res}_i = (z_{i,1}, z_{i,2})$. It follows from $res = (z_1, z_2) = \sum_{i=1}^{S} res_i$ that $z_1, z_2 \in R^{\leq S\beta_z}$. Thus, BRC returns 1 on input res = (z_1, z_2).

5.4 AFLT Decisional Short-discrete-logarithm ID Scheme

The description AFLT decisional short-discrete-logarithm (DSDL) ID scheme [12] is illustrated in Figure 8. And the setting for the succinct linearity is given in Table 3. We show that AFLT DSDL ID scheme has the batch rejection checker and the difference soundness by the following lemmas, respectively. Hence, we can obtain the multisignature scheme based on the DSDL assumption by the setting in Table 3 and Corollary 1.



$\text{Su}^{\text{dsdl}}(1^{\lambda})$ returns $\pi = (p, q, \mathbf{S}, s)$, where $\mathbf{S}$ be a subgroup of prime order $q \gg 2^{2k+k'+c}$ in $\mathbf{Z}_p^*$ with a generator s for a prime p.

$\text{Kg}^{\text{dsdl}}(\pi)$ returns (sk, pk):

1) $sk \leftarrow_{\text{U}} [0, 2^c - 1]$.
2) $pk = s^{sk} \bmod p$.

$\text{Kg}_L^{\text{dsdl}}(\pi)$ returns $pk \leftarrow_{\text{U}} \mathbf{S}$.

$\text{Vr}^{\text{dsdl}}(\pi, pk, \text{cmt}, \text{cha}, \text{res})$: returns 1 if

- $\text{res} \in [2^{k+c}, 2^{k+k'+c} - 1]$
- $s^{\text{res}} = pk^{\text{cha}} \cdot s^{\text{st}}$.

Prover P with sk		Verifier V with pk
$\text{st} \leftarrow_{\text{U}} [0, 2^{k+k'+c} - 1]$;		
$\text{cmt} = s^{\text{st}} \bmod p$	$\xrightarrow{\text{cmt}}$	
	$\xleftarrow{\text{cha}}$	$\text{cha} \leftarrow_{\text{U}} [0, 2^k - 1]$
$\text{res} = \text{st} + \text{st} \cdot \text{cha}$	$\xrightarrow{\text{res}}$	
$\text{res} = \perp$		
if $\text{res} \notin [2^{k+c}, 2^{k+k'+c} - 1]$		

Figure 8. AFLT DSDL ID scheme, where *k*, *k'* and *c* are some designated natural numbers [12]

Lemma 4. *BRC defined in Table 3 is a batch rejection checker of AFLT DSDL ID scheme.*

Proof. Assume that RC(res_i) = 1 for each $1 \leq i \leq S$. This implies that $\text{res}_i \in [2^{k+c}, 2^{k+k'+c} - 1]$ for each $1 \leq i \leq S$. It follows from $res = \sum_{i=1}^{S} res_i$ that res $\in [S2^{k+c}, S(2^{k+k'+c} - 1)]$. Therefore, BRC returns 1 on input res.

Table 3. Setting of succinct LID based on AFLT DSDL ID scheme

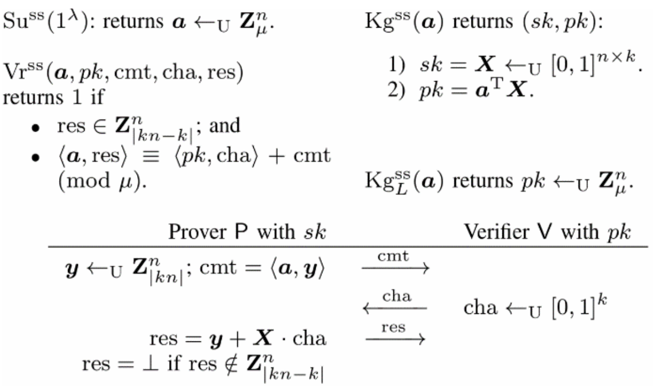
π	(p, q, **S**, s)
Dπ	**Z**p
Rπ	**S**
Sπ	**Z**p
fπ	$\boldsymbol{x} \mapsto \boldsymbol{s}^{\boldsymbol{x}}$
D_{π}^{sk}	$U([\mathbf{0}, \mathbf{2}^{c} - \mathbf{1}])$
D_{π}^{st}	$U([\mathbf{0}, \mathbf{2}^{k+k'+c} - \mathbf{1}])$
CH_{π}	$[\mathbf{0}, \mathbf{2}^{k} - \mathbf{1}]$
RC (res)	return 1 if res $\in [2^{k+c}, 2^{k+k'+c} - 1]$
BRC (res)	return 1 if res $\in [S2^{k+c}, S(2^{k+k'+c}–)]$

Lemma 5. *Let (p, q,* ***S****, s)* $\leftarrow Su^{dsdl}(1^{\lambda})$*, and let* $pk \leftarrow Kg_L^{dsdl}(p, q, \boldsymbol{S}, s)$. *For any* $S \geq 1$ $S \geq 1$*, AFLT DSDL ID scheme is* ($[S2^{k+c}, S(2^{k+k'+c} - 1)]$, $S2^{k+k'+c+2}/q$) *- difference sound.*

Proof. Let $pk \leftarrow Kg_L^{dsdl}(p, q, \boldsymbol{S}, s)$. This implies that there exists $x \in \boldsymbol{Z}_q$ such that $pk = s^x$, and x is uniformly distributed over $\boldsymbol{Z}_q$. Assume that there exist cha, cha' $\in [0, 2^k - 1]$ and res, res' $\in [S2^{k+c}, S(2^{k+k'+c} - 1)]$ such that $cha \neq cha'$ and $f_{\pi}(res - res') = pk(cha - cha')$. . The linearity and $cha - cha' \in \boldsymbol{Z}_q^*$ imply that $pk = f_{\pi}\left(\frac{(res - res')}{(cha - cha')}\right)$. Since $cha - cha' \in [-(2^k - 1), 2^k - 1]$ and $res - res' \in [-S(2^{k+k'+c} - 1), S(2^{k+k'+c} - 1)]$, there are at most $(2(2^k - 1) + 1)(2S(2^{k+k'+c} - 1) + 1) \leq S2^{2k+k'+c+2}$ possibilities of the value (res – res')/(cha – cha'). Therefore, such cha, cha', res and res' exist with probability at most $S2^{k+k'+c+2}/q$.

5.5 AFLT Subset-sum ID Scheme

To consider the linearity of AFLT subset-sum ID scheme [12] (Figure 9), we should note the definition of a linear function. As in Table 4, we bypass defining the set S_{π} in the definition. Instead, we slightly modify the construction of ID scheme from Figure 1 in the following way, to represent their ID scheme by the linear function. The key generation algorithm Kg^{ss} generates a pair (*sk*, *pk*) by choosing $sk = (x_1, ..., x_k)$ for each $x_i \leftarrow_R D_{\pi}^{sk}$, and then setting $pk = (f_{\pi}(x_1), ..., f_{\pi}(x_k))$. Then, the batch rejection checker and the difference soundness of AFLT subset-sum ID scheme are verified by the sequential lemmas below. This implies that we can obtain the multisignature scheme based on the subset-sum problem and its security is proven by Corollary 1.



$\mathrm{Su}^{\mathrm{ss}}(1^\lambda)$: returns $\boldsymbol{a} \leftarrow_{\mathrm{U}} \mathbf{Z}^n_\mu$.

$\mathrm{Vr}^{\mathrm{ss}}(\boldsymbol{a}, pk, \mathrm{cmt}, \mathrm{cha}, \mathrm{res})$
returns 1 if

- $\mathrm{res} \in \mathbf{Z}^n_{|kn-k|}$; and
- $\langle \boldsymbol{a}, \mathrm{res}\rangle \equiv \langle pk, \mathrm{cha}\rangle + \mathrm{cmt} \pmod{\mu}$.

$\mathrm{Kg}^{\mathrm{ss}}(\boldsymbol{a})$ returns (sk, pk):

1) $sk = \boldsymbol{X} \leftarrow_{\mathrm{U}} [0,1]^{n\times k}$.
2) $pk = \boldsymbol{a}^{\mathrm{T}}\boldsymbol{X}$.

$\mathrm{Kg}^{\mathrm{ss}}_L(\boldsymbol{a})$ returns $pk \leftarrow_{\mathrm{U}} \mathbf{Z}^n_\mu$.

$$\begin{array}{rcl}
\text{Prover P with } sk & & \text{Verifier V with } pk \\
\hline
\boldsymbol{y} \leftarrow_{\mathrm{U}} \mathbf{Z}^n_{|kn|};\ \mathrm{cmt} = \langle \boldsymbol{a}, \boldsymbol{y}\rangle & \xrightarrow{\mathrm{cmt}} & \\
 & \xleftarrow{\mathrm{cha}} & \mathrm{cha} \leftarrow_{\mathrm{U}} [0,1]^k \\
\mathrm{res} = \boldsymbol{y} + \boldsymbol{X}\cdot \mathrm{cha} & \xrightarrow{\mathrm{res}} & \\
\mathrm{res} = \perp \text{ if } \mathrm{res} \notin \mathbf{Z}^n_{|kn-k|} & &
\end{array}$$

Figure 9. AFLT subset-sum ID scheme, μ is a prime greater than $(2kn+1)^n 3^{2k}$ [12]

Table 4. Setting of succinct LID based on AFLT subset-sum ID scheme

π	$\boldsymbol{a} \in \boldsymbol{Z}^n_\mu$
Dπ	$\mathbf{Z}^{\mathrm{n}}$
Rπ	$\mathbf{Z}\mu$
fπ	$\boldsymbol{x} \mapsto \langle \boldsymbol{a}, \boldsymbol{x}\rangle \bmod \mu = \boldsymbol{a}^T\boldsymbol{x} \bmod \mu$
D^{sk}_π	$U([0,1]^n)$
D^{st}_π	$U(\boldsymbol{Z}^n_{\lvert kn\rvert})$
CHπ	$[0,1]^n$
RC(res)	return 1 if $res \in \boldsymbol{Z}^n_{\lvert kn-k\rvert}$
BRC(res)	return 1 if $res \in \boldsymbol{Z}^n_{\lvert S(kn-k)\rvert}$

Lemma 6. *BRC defined in Table 4 is a batch rejection checker of AFLT subset-sum ID scheme.*

Proof. Asume that RC(res$_i$) = 1 for each $1 \le i \le S$. This implies that $res \in \boldsymbol{Z}^n_{|kn-k|}$ for each $1 \le i \le S$. It follows from $res \in \sum_{i=1}^{S} res_i$ that $res \in \boldsymbol{Z}^n_{|S(kn-k)|}$. Therefore, BRC returns 1 on input res.

Lemma 7. *Let* $\boldsymbol{a} \leftarrow Su^{ss}(1^\lambda)$, *and let* $pk \leftarrow Kg^{ss}_L(\boldsymbol{a})$. *For any* $S \ge 1$, *AFLT subset-sum ID scheme is* $\left(\boldsymbol{Z}^n_{|S(kn-k)|}, \dfrac{(3^k(2S(kn+k)-1)^n}{\mu}\right)$*-difference sound.*

Proof. $pk \leftarrow Kg^{ss}_L(\boldsymbol{a})$. This implies that pk is uniformly distributed over $\boldsymbol{Z}^n_\mu$. Assume that there exist $cha, cha' \in [0,1]^k$ and $res, res' \in \boldsymbol{Z}^n_{|S(kn-k)|}$ such that $cha \ne cha'$ and $f_\pi(res - res') = pk \cdot (cha - cha')$. It follows from $f_\pi(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x}\rangle$ mod μ that $\langle \boldsymbol{a}, (res - res')\rangle - \langle pk, (cha - cha')\rangle \equiv 0(\bmod\ \mu)$. In a similar manner to the proof of Lemma 5, there are at most $3^k(2S(kn+k)-1)^n$ pairs $(cha - cha', res - res')$. Since $\boldsymbol{a}$ and pk are uniformly chosen from $\boldsymbol{Z}^n_\mu$ and μ is prime, the probability that $\langle \boldsymbol{a}, (res - res')\rangle - \langle pk, (cha - cha')\rangle \equiv 0(\bmod\ \mu)$ holds is at most $\dfrac{3^k(2S(kn+k)-1)^n}{\mu}$ as in the discussion in Section 6 on [12].

6 Concluding Remarks

In this paper, we have proposed a generic construction of multisignature schemes with the tight security proof in the plain public key and random oracle model. Our construction employs the linear ID scheme and the lossy ID scheme and is obtained by incorporating these two ID schemes into the strategy of the multisignature scheme by [1]. Our generic construction can be used not only to explain the existing tightly secure multisignature scheme but also to obtain new multisiganture schemes by applying it to existing linear and lossy ID schemes. We have also proposed a more compact condition to give a tightly secure multisignature scheme. We have introduced the difference soundness on the ID scheme and have shown that the combination of the linearity and the difference soundness implies the lossiness. To the best of knowledge, this is the first sufficient condition to construct lossy ID schemes generally.

We finally note the signing protocol of our generic construction. The signing protocol aborts when the rejection checker rejects the response, whereas some multisignature schemes [9-10, 23] restarts the signing protocol in such a case. We remain an open question to consider a generic construction which supports the restart in the signing protocol.

Acknowledgments

We would like to thank anonymous reviewers for their valuable comments and suggestions. This work was supported in part by JSPS KAKENHI Grant Numbers JP18K11288 and JP19K20272.

References

[1] M. Bellare, G. Neven, Multi-signatures in the Plain Public-key Model and a General Forking Lemma, *the 13th ACM Conference on Computer and Communications Security*, Alexandria, VA, 2006, pp. 390-399.

[2] S. Micali, K. Ohta, L. Reyzin, Accountable-subgroup Multisignatures: Extended abstract, *the 8th ACM Conference on Computer and Communications Security*, Philadelphia, PA, 2001, pp. 245-254.

[3] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, B. Waters, Sequential Aggregate Signatures and Multisignatures without Random Oracles, *EUROCRYPT 2006*, Saint Petersburg, Russia, 2006, pp. 465-485.

[4] C. P. Schnorr, Efficient Identification and Signatures for

Smart Cards, *CRYPTO'89*, Santa Barbara, CA, 1989, pp. 239-252.

[5] A. Fiat, A. Shamir, How to Prove Yourself: Practical Solutions to Identification and Signature Problems, *CRYPTO' 86*, Santa Barbara, CA, 1986, pp. 186-194.

[6] M. Bellare, P. Rogaway, Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols, *the 1st ACM Conference on Computer and Communications Security*, Fairfax, VA, 1993, pp. 62-73.

[7] D.-P. Le, A. Bonnecaze, A. Gabillon, Multisignatures as Secure as the Diffie-Hellman Problem in the Plain Public-key Model, *Pairing-Based Cryptography 2009*, Palo Alto, CA, pp. 35-51.

[8] J. Katz, N. Wang, Efficiency Improvements for Signature Schemes with Tight Security Reductions, *the 10th ACM Conference on Computer and Communications Security*, Washington, DC, 2003, pp. 155-164.

[9] R. El Bansarkhani, J. Sturm, An Efficient Lattice-based Multisignature Scheme with Applications to Bitcoins, *15th International Conference on Cryptology and Network Security*, Milan, Italy, 2016, pp. 140-155.

[10] M. Fukumitsu, S. Hasegawa, A Tightly-secure Lattice-based Multisignature, *the 6th on ASIA Public-Key Cryptography Workshop*, Auckland, New Zealand, 2019, pp. 3-11.

[11] M. Backendal, M. Bellare, J. Sorrell, J. Sun, The Fiat-Shamir Zoo: Relating the Security of Different Signature Variants, *The 23rd Nordic Conference on Secure IT Systems*, Oslo, Norway, 2018, pp. 154-170.

[12] M. Abdalla, P.-A. Fouque, V. Lyubashevsky, M. Tibouchi, Tightly Secure Signatures from Lossy Identification Schemes, *Journal of Cryptology*, Vol. 29, No. 3, pp. 597-631, July, 2016.

[13] S. Hasegawa, S. Isobe, A Lossy Identification Scheme Using the Subgroup Decision Assumption, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E97.A, No. 6, pp. 1296-1306, June, 2014.

[14] M. Abdalla, F. B. Hamouda, D. Pointcheval, Tighter Reductions for Forward-secure Signature Schemes, *Public-Key Cryptography 2013*, Nara, Japan, 2013, pp. 292-311.

[15] D.-P. Le, G. Yang, A. Ghorbani, DDH-based Multisignatures with Public Key Aggregation, *Cryptology ePrint Archive*, Report 2019/771, July, 2019.

[16] H. Qian, X. Li, X. Huang, Tightly Secure Non-interactive Multisignatures in the Plain Public Key Model, *Informatica*, Vol. 23, No. 3, p. 443-460, 2012.

[17] L. Wei, J. Ai, S. Liu, A Tightly Secure Multi-party-signature Protocol in the Plain Model, *2015 8th International Conference on Biomedical Engineering and Informatics*, Shenyang, China, 2015, pp. 672-677.

[18] N. Yanai, T. Iwasaki, M. Inamura, K. Iwamura, Provably Secure Structured Signature Schemes with Tighter Reductions, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E100.A, No. 9, pp. 1870-1881, September, 2017.

[19] N. Yanai, Meeting Tight Security for Multisignatures in the Plain Public Key Model, *IEICE Transactions on Fundamentals of Electronics*, *Communications and Computer Sciences*, Vol. E101.A, No. 9, pp. 1484-1493, September, 2018.

[20] Z. Wang, T. Si, H. Qian, Z. Li, A CDH-based Multi-signature Scheme with Tight Security Reduction, *2008 The 9th International Conference for Young Computer Scientists*, Hunan, China, 2008, pp. 2096-2101.

[21] M. Abdalla, J. H. An, M. Bellare, C. Namprempre, From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-security, *EUROCRYPT 2002*, Amsterdam, The Netherlands, 2002, pp. 418-433.

[22] E. Kiltz, V. Lyubashevsky, C. Schaffner, A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-oracle Model, *EUROCRYPT 2018*, Tel Aviv, Israel, 2018, pp. 552-586.

[23] I. Damgård, C. Orlandi, A. Takahashi, M. Tibouchi, Two-round n-out-of-n and Multi-signatures and Trapdoor Commitment from Lattices, *PKC 2021*, 2021, pp. 99-130.

Biographies

Masayuki Fukumitsu received his B.S. degree in software and information science from Iwate Prefectural University, Japan, in 2009, and M.S. and Ph.D degrees in information sciences, Tohoku University, Japan, in 2011 and 2014, respectively. He is an Associate Professor in Hokkaido Information University. His research interests include cryptography and security.

Shingo Hasegawa received his B.Eng. degree from Tohoku University, Japan, in 2003, and M.S. and Ph.D degrees in information sciences, Tohoku University, Japan, in 2005 and 2009, respectively. He is an Assistant Professor in Tohoku University. His research interests include information security theory, computational complexity, and discrete mathematics.