On digital signatures based on isomorphism problems: QROM security and ring signatures

Zhili Chen[1], Dung Hoang Duong[2], Tuong Nguyen[2], Youming Qiao[1], Willy Susilo[2], and Gang Tang[1]

[1] Centre for Quantum Software and Information, School of Computer Science, Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW, Australia.
zhili.chen@student.uts.edu.au, Youming.Qiao@uts.edu.au, gang.tang-1@student.uts.edu.au

[2] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia.
hduong@uow.edu.au, ntn807@uowmail.edu.au, wsusilo@uow.edu.au

Abstract. At Eurocrypt 2022, Tang et al proposed a practical digital signature scheme in the context of post-quantum cryptography. The construction of that scheme is based on the assumed hardness of the alternating trilinear form equivalence problem (ATFE), the Goldreich-Micali-Widgerson (GMW) zero-knowledge protocol for graph isomorphism, and the Fiat-Shamir (FS) transformation. We refer to that scheme as the ATFE-GMW-FS scheme. The security of the ATFE-GMW-FS scheme was only proved in the random oracle model (ROM), and its security in the quantum random oracle model (QROM) was left as an open problem.
In this paper, we study the ATFE-GMW-FS scheme from two perspectives, namely the QROM security and (linkable) ring signature schemes. First, we provide two approaches of proving its QROM security, based on the perfect unique response property and lossy identification schemes, respectively. Second, we design (linkable) ring signatures based on the ATFE-GMW-FS scheme, inspired by a recent result of Beullens, Katsumata and Pintore (Asiacrypt 20) on isogeny-based cryptography.

1 Introduction

In [22], Goldreich, Micali and Wigderson described a zero-knowledge proof protocol for graph isomorphism (GI). The Fiat-Shamir transformation FS [21] can be applied to it to yield a digital signature scheme.This construction has been observed by several researchers since the 1990's. However, this scheme based on graph isomorphism is not secure, because GI can be solved effectively in practice [33,34], not to mention Babai's quasipolynomial-time algorithm [3].

Fortunately, the Goldreich-Micali-Wigderson zero-knowledge proof protocol applies to *any* isomorphism problem. This gives the hope that, by choosing an appropriate isomorphism problem, such a construction could be secure. This has been carried out to two areas in the context of post-quantum cryptography, namely multivariate cryptography and isogeny-based cryptography. In multivariate cryptography, Patarin proposed using polynomial isomorphism problems to replace graph isomorphism [36]. In isogeny-based cryptography, Couveignes proposed the use of class group actions on elliptic curves [16]. Both proposal have their own merits and issues; interested readers are referred to [40] for more details.

The recent advances in complexity theory [23,24] and algorithms [30,14,24] reveal a much clearer picture on the complexity of isomorphism problems of algebraic structures. Based on these advances, [40] proposed to use the isomorphism problem for alternating trilinear forms as the basis of this construction. For a detailed definition of the *alternating trilinear form equivalence* (ATFE) problem, see Section 2. For convenience, we shall refer to the digital signature scheme in [40] as *the ATFE-GMW-FS scheme*.

The main message of [40] is that ATFE-GMW-FS scheme could serve as an alternative candidate for the NIST's post-quantum digital signatures. This is backed by carefully-chosen concrete parameters based on both theoretical and practical attacks, and a prototype implementation which indicates fast running times in practice.

Therefore, it is desirable to study the ATFE-GMW-FS scheme further. In this paper, we investigate the ATFE-GMW-FS scheme from two important aspects: security in the *quantum random oracle* model, and *ring signature* schemes. For both aspects, we obtain good evidence that favors the ATFE-GMW-FS scheme.

Our Contributions

Security in the quantum random oracle model. The quantum random oracle model (QROM) was proposed in 2011 in [8] and has received considerable attention since then. There are certain inherent difficulties to prove security in the QROM model, such as the adaptive pragrammability and rewinding [8]. Indeed, the QROM security of the Fiat-Shamir transformation was only recently shown after a series of works [44,29,32,18]. The QROM security of the ATFE-GMW-FS scheme was briefly discussed in [40] but was left as an open problem.

In this paper we make progress on the QROM security of the ATFE-GMW-FS scheme based on the works [44,29,32,18]. Our results on this line can be informally summarised as follows.

1. The ATFE-GMW-FS scheme is secure in the QROM model, if the automorphism group of the initial alternating trilinear form is trivial. We then provide experimental results to support that, for certain parameters proposed in [40], a random alternating trilinear form has the trivial automorphism group.
2. The ATFE-GMW-FS scheme is secure in the QROM model, if the group action under ATFE satisfies the pseudorandom property as defined in [27,2]. In particular, in this setting the security proof is tight. Whether the group action under ATFE is pseudorandom or not is an open problem. In [40], some arguments were provided to support that it is.

In particular, we do not need to modify the original ATFE-GMW-FS scheme in [40] to attain the security in QROM, i.e., as opposed to the context of isogeny-based cryptography, e.g., [19]. We will discuss more about this shortly.

Ring signature schemes. Ring signature, introduced by Rivest, Shamir and Tauman, is a special type of digital signature, in which a signer can sign on behalf of a group chosen by himself while retaining anonymous within the group, and ring signatures are formed without a complex setup procedure or the requirement for a group manager. They simply require users to be part of an existing public key infrastructure. Linkable ring signatures [31] is a variant of ring signatures in which any signatures produced by the same signer can be publicly linked. Linkable ring signatures are suitable in many different practical applications, such as privacy-preserving digital currency (Monero [39]) and e-voting [41].

Recently at Asiacrypt 2020, Beullens, Katsumata and Pintore [7] proposed an elegant way to construct efficient ring and linkable ring signatures from commutative group actions, with instantiations in both isogeny and lattice settings. The advantage of their schemes are the scalability of signature sizes with the ring size, even compared to other logarithmic-size post-quantum ring signatures.

Inspired by Beullens, Katsumata and Pintore's construction [7], in this paper, we show that the ATFE-GMW-FS scheme can be adapted to allow for (linkable) ring signatures. The construction is described in Section 5. We are in the process of estimating the parameters and implementing the protocols, and the results will be reported in a future revision of this work in which we will provide a comparison with Calamari and Falafl, the counterparts in isogeny and lattice settings, proposed in [7].

Discussions

Discussions on QROM security. Though tight QROM security proofs of Fiat-Shamir can be obtained by constructing lossy key generation [29], the lossy assumption seems very strong, so a natural question is to relax this assumption. In a pair of breakthrough papers [32] and [18], security reductions from the Fiat-Shamir transform to the underlying Σ-protocol with mild losses were presented. Combining these results with the *perfect unique response* property introduced by Unruh [42], we can obtain the security of the ATFE-GMW-FS signature scheme based on the Fiat-Shamir transform under QROM assuming a certain property of automorphism groups of alternating trilinear forms. While we don't have a rigorous analysis of this automorphism group property, we have experimental data to support it; see 3.4.

There is one further approach which could avoid analysing automorphism groups mathematically. In [32,18], a property called *quantum unique response* in [18] or collapsing sigma protocol in [32] is introduced, generalising the *collapsingness* which introduced by Unruh [43] to the quantum setting. The definition of this property relies on a certain protocol and basically asks to distinguish between measuring or not measuring during the execution of the protocol. It is an interesting problem to study isomorphism problems from the point of this property, which would lead to another security proof under QROM.

Comparisons with results from isogeny based cryptography. Some of our results, such as the lossy identification scheme (cf. Section 4.3) and the ring signature schemes (cf. Section 5, are inspired by corresponding works in isogeny-based cryptography [19,7]. Still, there are substantial differences, so we compare our results with those in [19,7].

First, the group action underlying our lossy identification scheme is the same action as the original ATFE-GMW-FS scheme, while the group action underlying the lossy CSI-FiSh [19] is the diagonal action of the class group on two elliptic curves following [38]. One reason is that for the pseudorandom group action assumption [27] (cf. Definition 8) to be useful, it is necessary that the underlying group action is intransitive, but the class group action on the classes of elliptic curves is transitive, which is why two copies are needed there. This results in doubling of the public-key size in lossy CSI-FiSh compared to the original CSI-FiSh, as opposed to our case where the public key size remains the same.

Second, our (linkable) ring singatures essentially follows the designs of their counterparts proposed by Beullens, Katsumata and Pintore [7]. The main difference lies in the choice of group actions. The class group action leads to smaller signature sizes, but it suffers the problems of efficiently computing the group action and random sampling. The group action underlying ATFE allows for fast group action and random sampling computations, though the signature sizes are somewhat larger. For a more detailed comparison in these aspects we refer the reader to [40].

Discussions on generalising our results in group action based cryptography. Most of our results can be generalised to general group actions. We refer the reader to [13,16,27,2] for frameworks of cryptography based on group actions. Here we only briefly indicate the group action underying ATFE, using terminologies and notation introduced in Section 2. Let G be a group, S be a set, and $\alpha : G \times S \to S$ be a group action, i.e. a function satisfying certain axioms. In the case of ATFE, the group G is the general linear group $\mathrm{GL}(n, q)$, the set S is the set of all alternating trilinear forms as $\mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, and the group action is defined as in Section 2. Based on this example, it is not hard to rephrasemost of the results in this paper in the language of group actions. However, we adopt to use ATFE directly because it is more concrete and allows us to directly use the results and parameters from [40].

Organization. In Section 2, we will review notions and security of idenfitication protocol and the associated Fiat-Shamir signature. We also recall alternating trilinear forms, some hardness assumptions to be used throughout the paper, and the ATFE-GMW-FS signature scheme in [40]. Section 3 is devoted for the security proof in QROM of ATFE-GMW-FS under the assumption on the triviality of the automorphism group of associated alternating trilinear forms. We also present some experimental results supporting this assumption at the end of Section 3. In Section 4, we prove that the underlying sigma protocol of ATFE-GMW-FS is lossy and present the corresponding Fiat-Shamir signature scheme which is proved to be tightly secure in QROM. Section 5 is devoted for our construction of (linkable) ring signatures. We conclude in Section 6 with some discussions and open problems.

2 Preliminaries for the ATFE-GMW-FS scheme

2.1 Notations

We collect some basic notation in this subsection. We use $\mathbb{F}_q$ to denote the finite field of order q. The general linear group of degree n over $\mathbb{F}_q$ is denoted as $\mathrm{GL}(n, q)$. The base of logarithm is 2 unless otherwise specified. For a finite set S, we use $s \in_R S$ to denote that s is uniformly randomly sampled from S. Given a positive integer $k \geq 1$, we denote by $[k]$ the set $\{1, \cdots, k\}$.

2.2 Sigma Protocol

Let $\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$ be a binary relation, where $\mathcal{X}, \mathcal{W}, \mathcal{R}$ are recognizable finite sets. In other words, there is a polynomial time algorithm can decide whether $(x, w) \in \mathcal{R}$ for $x \in \mathcal{X}$ and $w \in \mathcal{W}$. Given an instance generator Gen of a relation $\mathcal{R}$, the relation $\mathcal{R}$ is *hard* if for any poly-time quantum algorithm $\mathcal{A}$, the probability $\Pr[(x, w') \in \mathcal{R} \mid (x, w) \leftarrow \mathsf{Gen}(1^\lambda), w' \leftarrow \mathcal{A}(x)]$ is negligible.

Given a hard relation $\mathcal{R}$, the Σ-protocol for $\mathcal{R}$ which is 3-move interactive protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$ in which the prover $\mathcal{P}$ who has the witness w for the statement x tries to convince the verifier $\mathcal{V}$ that he possesses a valid witness w without revealing any more than the fact that he knows w. Formally, Σ-protocol is defined as follows.

Definition 1. *Let $\mathcal{R}$ be a hard binary relation. Let* $\mathsf{ComSet}, \mathsf{ChSet}, \mathsf{ResSet}$ *be the commitment space, challenge space and response space respectively. The Σ-protocol Σ for a relation $\mathcal{R}$ consists of three PPT algorithms $(\mathcal{P} = (\mathcal{P}_1, \mathcal{P}_2), \mathcal{V})$, where V is deterministic and we assume that $\mathcal{P}_1$ and $\mathcal{P}_2$ share the same state, working as the following:*

- *The prover $\mathcal{P}$ first computes a commitment $a \leftarrow \mathcal{P}_1(w, x)$ and sends a to the verifier $\mathcal{V}$.*
- *On input a commitment a, the $\mathcal{V}$ samples a random challenge c from the challenge space* ChSet *and sends to $\mathcal{P}$.*
- *$\mathcal{P}$ computes a response $r \leftarrow \mathcal{P}_2(w, x, a, c)$ and sends to the $\mathcal{V}$ who will run $\mathcal{V}(x, a, c, r)$ and outputs 1 if the transcript (a, c, r) is valid and 0 otherwise.*

Identification from Σ-protocol. A Σ-protocol $(\mathcal{P}, \mathcal{V})$ with a key generation algorithm $\mathsf{ID.Gen}$ gives an identification scheme $(\mathsf{ID.Gen}, \mathcal{P}, \mathcal{V})$.

Completeness. The Σ-protocol is said to be complete if for all pair $(x, w) \in \mathcal{R}$, an honest prover $\mathcal{P}$ with $(\mathsf{pk}, \mathsf{sk})$, where $\mathsf{pk} := x$ and $\mathsf{sk} := w$, can always convince an honest verifier, i.e. $\Pr[\mathcal{V}(\mathsf{pk}, a, c, r) = 1 \mid a \leftarrow \mathcal{P}(\mathsf{sk}), c \in_R \mathsf{ChSet}, r \leftarrow \mathcal{P}_2(\mathsf{pk}, \mathsf{sk}, a, c)] = 1$.

Post-Quantum 2-Soundness. We say a Σ-protocol has post-quantum 2-soundness if for all pairs $(x, w) \in \mathcal{R}$, no poly-time quantum adversaries $\mathcal{A}$ with only the statement x, where $(x, w) \in \mathcal{R}$, can compute two valid transcripts (a, c, r) and (a, c', r') of different challenges $c \neq c'$ with non-negligible probability, i.e. $\Pr[\mathcal{V}(\mathsf{pk}, a, c, r) = 1 \wedge \mathcal{V}(\mathsf{pk}, a, c', r') = 1 \wedge c \neq c' \mid (a, c, r, c', r') \leftarrow \mathcal{A}(\mathsf{pk})] \leq \mathsf{negl}(\lambda)$.

Honest Verifier Zero Knowledge. The Σ-protocol has honest verifier zero knowledge (HVZK) if for all pairs $(x, w) \in \mathcal{R}$, there is a simulator $\mathcal{S}$ with only the statement x, can always compute a valid transcript (a, c, r), i.e. $\Pr[\mathcal{V}(\mathsf{pk}, a, c, r) = 1 \mid (a, c, r) \leftarrow \mathcal{S}(\mathsf{pk})] = 1$. Moreover, the output distribution of $\mathcal{S}$ on input (x, c) is equal to the distribution of those outputs generated via an honest execution conditioned on the verifier using c as the challenge.

Min-entropy. The Σ-protocol has α-bit min-entropy, if

$$\Pr_{(x,w) \in_R \mathcal{R}}[\text{min-entropy}(a | a \leftarrow \mathcal{P}_1(x, w)) \geq \alpha] \geq 1 - 2^{-\alpha}.$$

Perfect Unique Response. The Σ-protocol has perfect unique response if for all pairs $(x, w) \in \mathcal{R}$, there is no two valid transcripts (a, c, r) and (a, c, r') of the same commitment a and challenge c but different responses $r \neq r'$, i.e. $\Pr[\mathcal{V}(x, a, c, r) = 1 \wedge \mathcal{V}(x, a, c, r') = 1 \wedge r \neq r'] = 0$.

Computationally Unique Response. The Σ-protocol has computationally unique response if for all pairs $(x, w) \in R$, no poly-time quantum adversaries $\mathcal{A}$ with a statement x can compute two valid transcripts (a, c, r) and (a, c, r') of different responses $r \neq r'$ with non-negligible probability, i.e.,

$$\Pr[\mathcal{V}(x, a, c, r) = 1 \wedge \mathcal{V}(x, a, c, r') = 1 \wedge r \neq r' \mid (a, c, r, r') \leftarrow \mathcal{A}(\mathsf{pk})] \leq \mathsf{negl}(\lambda).$$

Commitment Recoverability. The Σ-protocol is commitment recoverable if given c and r, there is a unique a such that (a, c, r) is a valid transcript. Therefore, the commitment can be computed with the input (c, r).

2.3 Digital signatures

Definition 2. *A digital signature consists of the following polynomial-time (possibly probabilistic) algorithms.*

- $\mathsf{Gen}(1^\lambda)$*: On input a security parameter* λ*, generates a pair* $(\mathsf{sk}, \mathsf{pk})$ *of secret key* sk *and verification key* pk.

– $\textsc{Sign}(\mathsf{sk}, M)$*: On input a message* M *and the secret key* sk*, it generates a signature* σ*.*
– $\mathsf{Ver}(\mathsf{pk}, M, \sigma)$*: On input the verification key* pk*, a message* M *and a signature* σ*, it returns* 1 *or* 0*.*

For correctness, it is required that

$$\Pr[\mathsf{Ver}(\mathsf{pk}, M, \textsc{Sign}(\mathsf{sk}, M)) = 1] = 1$$

where the probability is taken over the randomness of algorithms $\textsc{Sign}$ and Ver.

Definition 3 (Security of Signature Scheme). *The signature scheme is said to be unforgeable (i.e., EUF-CMA secure) if for any poly-time quantum adversaries* $\mathcal{A}$*, who has seen a number of signatures of messages of his choosing, the probability that* $\mathcal{A}$ *can sign a message that he has not seen its signature is negligible, i.e.,* $\Pr[\mathsf{Verify}(\mathsf{pk}, m, \sigma) = 1 \wedge (m, \sigma) \notin \Sigma | (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n),\ \sigma \leftarrow \mathcal{A}(\mathsf{pk}, m)] \leq \mathsf{negl}(\lambda)$*, where* Σ *is the list of all message-signature pairs that* $\mathcal{A}$ *has seen before.*

A stronger notion is *strongly unforgeablility* (sEUF-CMA) that allows an adversary $\mathcal{A}$ to output a different signature of a message whose signature he has already seen. The schemes presented in this paper satisfy this stronger notion of unforgeability.

The Fiat-Shamir transformation [21] FS turns an identification protocol $\mathsf{ID} = (\mathsf{ID.Gen}, \mathcal{P} = (\mathcal{P}_1, \mathcal{P}_2), \mathcal{V})$ into a signature scheme $\mathsf{FS}[\mathsf{ID}]$ as follows.

– $\mathsf{ID.Gen}(1^\lambda)$: On input a security parameter λ, run $(\mathsf{ID.sk}, \mathsf{ID.pk}) \leftarrow \mathsf{ID.Gen}(1^\lambda)$ and define the secret key $\mathsf{sk} := \mathsf{ID.sk}$ and verification key $\mathsf{pk} := \mathsf{ID.pk}$.
– $\textsc{Sign}(\mathsf{sk}, M)$: On input the secret key sk and a message M, do the following:
  - Run $a \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{pk})$.
  - Compute $c := H(M \| a)$ where $H : \{0, 1\}^* \rightarrow \mathsf{ChSet}$ is a secure hash function.
  - Run $r \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{pk}, a, c)$.
  - Return a signature $\sigma := (a, r)$.
– $\mathsf{Ver}(\mathsf{pk}, M, \sigma)$: On input a message M and a signature σ, do the following:
  - Compute $c := H(M \| a)$.
  - Return $\mathcal{V}(\mathsf{pk}, a, c, r)$.

Theorem 1 ([37]). *If an identification protocol is HVZK and satisfies special soundness, then* $\mathsf{FS}[\mathsf{ID}]$ *has* EUF-CMA *security in the QROM model.*

2.4 Ring signatures

In this section, we provide the definition of ring signature following Beullens, Katsumata and Pintore [7].

Definition 4 (Ring signature). *A ring signature scheme* Π_{RS} *consists of three PPT algorithms* $(\mathsf{RS.KeyGen}, \mathsf{RS.Sign}, \mathsf{RS.Verify})$ *where,*

– $\mathsf{RS.KeyGen}(1^\lambda)$*: This algorithm generates a list* $(\mathsf{R} = \{\mathsf{vk_1}, \ldots, \mathsf{vk_N}\}, \{\mathsf{sk_1}, \ldots, \mathsf{sk_N}\})$ *of the secret keys* vk_i *and public keys* sk_i*.*
– $\mathsf{RS.Sign}(\mathsf{sk}_i, \mathsf{R}, \mathsf{M})$*: Given the secret key* sk_i*, a list of public key* $\mathsf{R} = \{\mathsf{vk}_1, \ldots, \mathsf{vk}_N\}$ *and a message* M*, it outputs a signature* σ*.*
– $\mathsf{RS.Verify}(\mathsf{R}, \mathsf{M}, \sigma)$*: Given a list of public key* $\mathsf{R} = \{\mathsf{vk}_1, \ldots, \mathsf{vk}_N\}$*, a message* M *and a signature* σ*, this algorithm verifies if this signature is 1 (valid) or 0 (invalid).*

A ring signature needs to satisfy three properties: correctness, anonymity and unforgeability.

Correctness: A ring signature Π_{RS} is said to have correctness if for any security parameter λ, polynomial $N = \mathsf{poly}(\lambda)$ and message M, the following probability is 1:

$$\Pr\left[\mathsf{RS.Verify}(\mathsf{R}, \mathsf{M}, \sigma) = 1 \;\middle|\; \begin{array}{c} (\{\mathsf{vk_1}, \ldots, \mathsf{vk_N}\}, \{\mathsf{sk_1}, \ldots, \mathsf{sk_N}\}) \leftarrow \mathsf{RS.KeyGen}(1^\lambda) \\ \mathsf{R} := \{\mathsf{vk}_1, \ldots, \mathsf{vk}_N\} \\ \sigma \leftarrow \mathsf{RS.Sign}(\mathsf{sk}_i, \mathsf{R}, \mathsf{M}) \end{array}\right]$$

Anonymity: A ring signature Π_{RS} is said to be anonymous if for every security parameter λ and polynomial $N = \mathsf{poly}(\lambda)$, any PPT adversary $\mathcal{A}$ has at most negligible advantage in the following game:

(1) The challenger generates public keys and secret keys
$$(\{\mathsf{vk_1}, \ldots, \mathsf{vk_N}\}, \{\mathsf{sk_1}, \ldots, \mathsf{sk_N}\}) \leftarrow \mathsf{RS.KeyGen}(1^\lambda, \mathsf{r}),$$
where r is random bits, and samples $b \xleftarrow{\$} \{0, 1\}$. Then it sends random bits r to $\mathcal{A}$.
(2) $\mathcal{A}$ computes a challenge $(\mathsf{R}, \mathsf{M}, i_0, i_1)$, where R contains sk_{i_0} and sk_{i_1}, and sends it to challenger.
(3) Challenger runs $\mathsf{RS.Sign}(\mathsf{sk}_{i_b}, \mathsf{R}, \mathsf{M}) \to \sigma$ and sends σ to $\mathcal{A}$.
(4) $\mathcal{A}$ check if $\mathsf{RS.Verify}(\mathsf{R}, \mathsf{M}, \sigma) = 1$, and if so outputs b'. If $b = b'$, we say $\mathcal{A}$ wins this game.

The advantage of $\mathcal{A}$ is
$$\mathsf{Adv}_{\mathsf{RS}}^{\mathsf{Anon}}(\mathcal{A}) = |\Pr[\mathcal{A} \text{ wins}] - 1/2|\,.$$

Unforgeability: A ring signature Π_{RS} is said to be unforgeable if for every security parameter λ and polynomial $N = \mathsf{poly}(\lambda)$, any PPT adversary $\mathcal{A}$ has at most negligible probability to win the following game:

(1) The challenger generates public keys and secret keys
$$(\{\mathsf{vk_1}, \ldots, \mathsf{vk_N}\}, \{\mathsf{sk_1}, \ldots, \mathsf{sk_N}\}) \leftarrow \mathsf{RS.KeyGen}(1^\lambda, \mathsf{r} = \{\mathsf{r}_i\}_{i \in [N]}),$$
where random bits r_i is used to generate corresponding pair $\mathsf{vk}_i, \mathsf{sk}_i$. It sends the list of public keys $\mathsf{VK} = \{\mathsf{vk}_i\}_{i \in [N]}$ to $\mathcal{A}$ and prepares two empty list SL and CL.

(2) $\mathcal{A}$ can make polynomial times of signing queries and corrupting queries:
   - $(\mathsf{sign}, i, \mathsf{R}, \mathsf{M})$: The challenger outputs the signature $\sigma \leftarrow \mathsf{RS.Sign}(\mathsf{sk}_i, \mathsf{R}, \mathsf{M})$ to $\mathcal{A}$ and adds $(i, \mathsf{R}, \mathsf{M})$ to SL.
   - $(\mathsf{corrupt}, i)$ The challenger sends the random bits r_i to $\mathcal{A}$ and adds vk_i to CL.

(3) We say $\mathcal{A}$ wins this game if $\mathcal{A}$ outputs $(\mathsf{R}', \mathsf{M}', \sigma')$ such that $\mathsf{R}' \subseteq \mathsf{VK} \setminus \mathsf{CL}$, $(\cdot, \mathsf{M}', \mathsf{R}') \notin \mathsf{SL}$, and $\mathsf{RS.Verify}(\mathsf{R}', \mathsf{M}', \sigma') = 1$.

2.5 Linkable ring signatures

Linkable ring signature is a variant of ring signature in which the linkability can detect if a secret key is used more than once. The definition and properties of linkable ring signature, following [7], are provided as follows.

Definition 5 (Linkable ring signature). *A linkable ring signature scheme Π_{LRS} consists of three PPT algorithms in the ring signature in addition with a PPT algorithm such that:*

– $\mathsf{LRS.Link}(\sigma_0, \sigma_1)$*: It checks if two signatures σ_0, σ_1 are produced with a same secret key, and outputs 1 if it is the case and 0 otherwise.*

Correctness: A ring signature Π_{LRS} is said to have correctness if for any security parameter λ, polynomial $N = \mathsf{poly}(\lambda)$, messages $\mathsf{M}_0, \mathsf{M}_1$, and sets $D_0, D_1 \subseteq [N]$ that $j \in D_0 \cap D_1$, the following probability is 1:

$$\Pr\left[\begin{array}{c|c} \mathsf{LRS.Verify}(\mathsf{R}, \mathsf{M}, \sigma_b) = 1 & (\{\mathsf{vk}_1, \ldots, \mathsf{vk}_\mathsf{N}\}, \{\mathsf{sk}_1, \ldots, \mathsf{sk}_\mathsf{N}\}) \leftarrow \mathsf{LRS.KeyGen}(1^\lambda), \\ \forall b \in \{0,1\} \text{ and} & \mathsf{R}_b := \{\mathsf{vk}_i\}_{i \in D_b}, \\ \mathsf{LRS.Link}(\sigma_0, \sigma_1) = 1 & \sigma_b \leftarrow \mathsf{LRS.Sign}(\mathsf{sk}_j, \mathsf{R}_b, \mathsf{M}_b). \end{array}\right]$$

Linkability: A ring signature Π_{LRS} is said to be unforgeable if for every security parameter λ and polynomial $N = \mathsf{poly}(\lambda)$, any PPT adversary $\mathcal{A}$ has at most negligible probability to win the following game:

(1) The challenger sends λ to $\mathcal{A}$.

(2) $\mathcal{A}$ generates public keys and secret keys $(\{\mathsf{vk}_1, \ldots, \mathsf{vk}_\mathsf{N}\}, \{\mathsf{sk}_1, \ldots, \mathsf{sk}_\mathsf{N}\}) \leftarrow \mathsf{LRS.KeyGen}(1^\lambda)$, and then produces a set $(\sigma_i, \mathsf{M}_i, \mathsf{R}_i)_{i \in [N+1]}$.

(3) We say $\mathcal{A}$ wins this game if all the following conditions are satisfied:
   - $\forall i \in [N+1]$, have $\mathsf{R}_i \subseteq \mathsf{VK}$;
   - $\forall i \in [N+1]$, have $\mathsf{LRS.Verify}(\mathsf{R}_i, \mathsf{M}_i, \sigma_i) = 1$;
   - $\forall i, j \in [N+1]$, where $i \neq j$, have $\mathsf{LRS.Link}(\sigma_i, \sigma_j) = 0$.

Linkable Anonymity: A ring signature Π_{LRS} is said to be linkable anonymous if for every security parameter λ and polynomial $N = \mathsf{poly}(\lambda)$, any PPT adversary $\mathcal{A}$ has at most negligible advantage in the following game:

(1) The challenger generates public keys and secret keys

$$(\{\mathsf{vk_0}, \ldots, \mathsf{vk_N}\}, \{\mathsf{sk_1}, \ldots, \mathsf{sk_N}\}) \leftarrow \mathsf{RS.KeyGen}(1^\lambda, \mathsf{r} = \{\mathsf{r}_i\}_{i\in[N]}),$$

where random bits r_i is used to generate corresponding pair $\mathsf{vk}_i, \mathsf{sk}_i$ and it also samples a ramdom bit $b \in \{0,1\}$. Then it sends the public keys $\mathsf{VK} = \{\mathsf{vk}_0, \ldots, \mathsf{vk}_N\}$ to $\mathcal{A}$.
(2) $\mathcal{A}$ sends two public keys $\mathsf{vk}'_0, \mathsf{vk}'_1$ to the challenger, and we let $\mathsf{sk}'_0, \mathsf{sk}'_1$ be the corresponding secret keys.
(3) The challenger outputs r_i of the corresponding $\mathsf{vk}_i \subseteq \mathsf{VK} \setminus \{\mathsf{vk}'_0, \mathsf{vk}'_1\}$.
(4) $\mathcal{A}$ chooses a public key $\mathsf{vk} \in \{\mathsf{vk}'_0, \mathsf{vk}'_1\}$ and provides a massage M and a ring R that $\{\mathsf{vk}'_0, \mathsf{vk}'_1\} \subseteq \mathsf{R}$ to query the challenger:
   - If $\mathsf{vk} = \mathsf{vk}'_0$, the challenger outputs the signature $\mathsf{LRS.Sign}(sk_b, \mathsf{R}, \mathsf{M}) \rightarrow \sigma$.
   - If $\mathsf{vk} = \mathsf{vk}'_1$, the challenger outputs the signature $\mathsf{LRS.Sign}(sk_{1-b}, \mathsf{R}, \mathsf{M}) \rightarrow \sigma$.
(5) $\mathcal{A}$ check if $\mathsf{LRS.Verify}(\mathsf{R}, \mathsf{M}, \sigma) = 1$, and if so outputs b'. If $b = b'$, we say $\mathcal{A}$ wins this game.

The advantage of $\mathcal{A}$ is $\mathsf{Adv}^{\mathsf{Anon}}_{\mathsf{LRS}}(\mathcal{A}) = |\Pr[\mathcal{A} \text{ wins}] - 1/2|$.

Non-frameability: A ring signature Π_{LRS} is said to be non-frameable if for every security parameter λ and polynomial $N = \mathsf{poly}(\lambda)$, any PPT adversary $\mathcal{A}$ has at most negligible probability to win the following game:

(1) The challenger generates public keys and secret keys $\mathsf{LRS.KeyGen}(1^\lambda, \mathsf{r} = \{\mathsf{r}_i\}_{i\in[N]}) \rightarrow (\{\mathsf{vk_0}, \ldots, \mathsf{vk_N}\}, \{\mathsf{sk_1}, \ldots, \mathsf{sk_N}\})$, where random bits r_i is used to generate corresponding pair $\mathsf{vk}_i, \mathsf{sk}_i$. It sends the list of public keys $\mathsf{VK} = \{\mathsf{vk}_i\}_{i\in[N]}$ to $\mathcal{A}$ and prepares two empty list SL and CL.
(2) $\mathcal{A}$ can make polynomial times of signing queries and corrupting queries:
   - $(\mathsf{sign}, i, \mathsf{R}, \mathsf{M})$: The challenger outputs the signature $\mathsf{LRS.Sign}(\mathsf{sk}_i, \mathsf{R}, \mathsf{M}) \rightarrow \sigma$ to $\mathcal{A}$ and adds $(i, \mathsf{R}, \mathsf{M})$ to SL.
   - $(\mathsf{corrupt}, i)$: The challenger sends the random bits r_i to $\mathcal{A}$ and adds vk_i to CL.
(3) We say $\mathcal{A}$ wins this game if $\mathcal{A}$ outputs $(\mathsf{R}', \mathsf{M}', \sigma')$ such that $(\cdot, \mathsf{M}', \mathsf{R}') \notin \mathsf{SL}$, $\mathsf{LRS.Verify}(\mathsf{R}', \mathsf{M}', \sigma') = 1$, and for some query $(i, \mathsf{R}, \mathsf{M}) \in \mathsf{SL}$ where the identity i satisfies $\mathsf{vk}_i \in \mathsf{VK} \setminus \mathsf{CL}$, the challenger outputs a signature σ that $\mathsf{LRS.Link}(\sigma', \sigma) = 1$ holds.

Unforgeability: The definition of unforgeability remains the same as that of the normal ring signature. The unforgeability can be easily derived from the linkable anonymity and the non-frameability.

2.6 Alternating trilinear forms and their isomorphisms

In this section, we briefly review the notions of alternating trilinear forms, their isomorphisms, how to represent these in algorithms, and the algorithmic problems relevant to us. For details the reader is referred to [40, Sec. 2.1 and 6.2].

Let $\mathbb{F}_q$ be the finite field of order q. A trilinear form $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is *alternating*, if ϕ evaluates to 0 whenever two arguments are the same. We use $\mathrm{ATF}(n, q)$ to denote the set of all alternating trilinear forms defined over $\mathbb{F}_q^n$.

Let A be an invertible matrix of size $n \times n$ over $\mathbb{F}_q$. Then A sends ϕ to another alternating trilinear form $\phi \circ A$, defined as $(\phi \circ A)(u, v, w) := \phi(A^{\mathrm{t}}(u), A^{\mathrm{t}}(v), A^{\mathrm{t}}(w))$. This yields a group action of $\mathrm{GL}(n, q)$ on $\mathrm{ATF}(n, q)$. Given an alternating trilinear form $\phi \in \mathrm{ATF}(n, q)$, the orbit of ϕ, denoted by $\mathcal{O}(\phi)$, is the set of all $\phi \circ A$ for $A \in \mathrm{GL}(n, q)$. The automorphism group of ϕ (also known as the stabilizer group of ϕ), denoted by $\mathrm{Aut}(\phi)$, is the subgroup of $\mathrm{GL}(n, q)$ fixing ϕ, i.e., $\mathrm{Aut}(\phi) := \{A \in \mathrm{GL}(n, q) \mid \phi \circ A = \phi\}$. By the orbit-stabilizer theorem, we have that $|\mathcal{O}(\phi)| \cdot |\mathrm{Aut}(\phi)| = |\,\mathrm{GL}(n, q)|$.

The *alternating trilinear form equivalence* (ATFE) problem asks to decide, given two alternating trilinear forms $\phi, \psi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, whether there exists an invertible matrix A such that $\phi = \psi \circ A$.

In algorithms, an alternating trilinear form is represented by $\binom{n}{3}$ field elements in $\mathbb{F}_q$. The group action of $\mathrm{GL}(n, q)$ on $\mathrm{ATF}(n, q)$ can be computed in time $O(n^4 \cdot \log q)$. Uniformly sampling an element in $\mathrm{ATF}(n, q)$ or an element in $\mathrm{GL}(n, q)$ can be done in time $\mathsf{poly}(n, \log q)$.

The following two algorithmic problems are of key relevance to the use in cryptography. The first algorithmic problem is a slight modification of the m-psATFE problem in [40].

Definition 6 (K-psATFE-RO). *The promised search version of the alternating trilinear form equivalence problem with K random instances from a random orbit (K-psATFE-RO) is the following.*

Input: *K alternating trilinear forms $\phi_0, \phi_1, \ldots, \phi_{K-1} : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, such that: (1) $\phi_0 \in_R \mathrm{ATF}(n, q)$, and (2) for $i \in [K-1]$, $\phi_i := \phi_0 \circ A_i$, where $A_i \in_R \mathrm{GL}(n, q)$.*

Output: *Some $A \in \mathrm{GL}(n, q)$ and $i, j \in \{0, 1, \ldots, K-1\}$, $i \neq j$, such that $\phi_i = \phi_j \circ A$.*

In Section 3, we also need the following variation of Definition 6 by restricting to a particular orbit.

Definition 7 (K-psATFE-$\mathcal{O}(\phi)$). *Let $\phi \in \mathrm{ATF}(n, q)$. The promised search version of the alternating trilinear form equivalence problem with K random instances in the orbit of ϕ (K-psATFE-$\mathcal{O}(\phi)$) is the following.*

Input: *K alternating trilinear forms $\phi_0, \phi_1, \ldots, \phi_{K-1} : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, such that for $i \in \{0, 1, \ldots, K-1\}$, $\phi_i := \phi \circ A_i$, where $A_i \in_R \mathrm{GL}(n, q)$.*

Output: *Some $A \in \mathrm{GL}(n, q)$ and $i, j \in \{0, 1, \ldots, K-1\}$, $i \neq j$, such that $\phi_i = \phi_j \circ A$.*

The second algorithmic problem is obtained by applying the pseudorandom group action notion [27] to K-psATFE-RO.

Definition 8 (*K*-**PR-psATFE-RO**). *The pseudorandom version of the alternating trilinear form equivalence problem with K random instances from a random orbit (K-PR-psATFE-RO) asks to distinguish the following two distributions.*

The random distribution: *K alternating trilinear forms $\phi_0, \phi_1, \ldots, \phi_{K-1}$: $\mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, such that every $\phi_i \in_R \mathrm{ATF}(n, q)$.*

The pseudorandom distribution: *K alternating trilinear forms $\phi_0, \phi_1, \ldots, \phi_{K-1} : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, such that: (1) $\phi_0 \in_R \mathrm{ATF}(n, q)$, and (2) for $i \in [K-1]$, $\phi_i := \phi_0 \circ A_i$, where $A_i \in_R \mathrm{GL}(n, q)$.*

Remark 1. Since two random alternating trilinear forms are unlikely to be in the same orbit for reasonably large n, an algorithm that solves K-psATFE-RO can be used to distinguish the two distributions in K-PR-psATFE-RO with high probability.

Assumption 1. No quantum polynomial-time algorithm can solve K-psATFE-RO problem with a non-negligible probability.

Assumption 2. No quantum polynomial-time algorithm can solve K-psATFE-$\mathcal{O}(\phi)$ problem with a non-negligible probability.

2.7 The ATFE-GMW-FS scheme

As mentioned in Section 1, the ATFE-GMW-FS scheme in [40] is obtained by applying the Fiat-Shamir (FS) transformation to the Goldreich-Micali-Wigderson (GMW) zero-knowledge protocol instantiated with the ATFE problem, or more precisely, the K-psATFE-RO problem as in Definition 6.

For our purposes in this paper, the key is that the GMW protocol instantiated with the K-psATFE-RO problem. This protocol is easily interpreted as an identification protocol, and we shall refer it as the ATFE-GMW protocol. Therefore, we describe the ATFE-GMW protocol in detail, and refer the reader to [40, Section 3.1] for a detailed description of the ATFE-GMW-FS signature scheme.

In the ATFE-GMW protocol, the public key consists of alternating trilinear forms $\phi_0, \phi_1, \cdots, \phi_{K-1}$ such that $\phi_0 \in_R \mathrm{ATF}(n, q)$, $\phi_i \circ A_i^{-1} = \phi_0$ for $i = 1, \cdots, K-1$, and $A_i \in_R \mathrm{GL}(n, q)$. The private key consists of $A_i \in \mathrm{GL}(n, q)$, $i \in [k]$. In this protocol, the goal of the prover is to convince the verifier that, for every $i \neq j$, the prover knows some $A \in \mathrm{GL}(n, q)$ such that $\phi_i = \phi_j \circ A$.

Define the relation $R := \{x = \{\phi_0, \phi_1, \ldots, \phi_{K-1}\}, w = \{A_1, \ldots, A_{K-1}\} \mid x \subseteq \mathrm{ATF}(n, q), w \subseteq \mathrm{GL}(n, q), \phi_0 \circ A_i^{-1} = \phi_i, \forall i \in [K-1]\}$. The protocol is described in Figure 1. The protocol needs to be repeated t times for appropriate t to attain the required security level.

It is known that ATFE-GMW protocol in Figure 1 has the following properties; see e.g. [40]. Here we provide some proof sketches for completeness.

Completeness. It is clear that the honest provers with statement and witness (x, w) following the Σ-protocol can always convince the honest verifiers.

$\mathcal{P}(\phi_0, \cdots, \phi_{K-1}, A_1, \cdots, A_{K-1})$		$\mathcal{V}(\phi_0, \cdots, \phi_{K-1})$
$B \in_R \mathrm{GL}(n, q)$		
$\psi = \phi_0 \circ B$		
	$\xrightarrow{\psi}$	
		$c \xleftarrow{\$} \{0, 1, \cdots, K-1\}$
	$\xleftarrow{c}$	
Set $D := B + \textsc{Sign}(c)(A_c B - B)$		
	$\xrightarrow{D}$	
		Check if $\phi_c \circ D = \psi$?

Fig. 1. The ATFE-GMW protocol.

Post-Quantum 2-Soundness. If there is a poly-time quantum adversary $\mathcal{A}$ with statement $x = \{\phi_0, \ldots, \phi_{K-1}\}$ who can compute two valid transcripts (ψ, c, D) and (ψ, c', D') where $c \neq c'$. Since $\phi_c \circ D = \psi$ and $\phi'_c \circ D' = \psi$, the $\mathcal{A}$ can get $E = D'D^{-1}$ such that $\phi_c = \phi'_c \circ E$, which is contradicted to the Assumption 1.

HVZK. Given a statement $x = \{\phi_0, \ldots, \phi_{K-1}\}$, there is a simulator $\mathcal{S}$ first sampling $c \in_R \{0, \ldots, K-1\}$ and $D \in_R \mathrm{GL}(n, q)$ and then computing $\psi = \phi_c \circ D$. (ψ, c, D) is a valid transcript. Then the distributions of D and c are uniform, and $\psi = \phi_c \circ D$ is uniformly from the orbit where statement x is in. The distribution of $(a, c, r) \leftarrow \mathcal{S}(x)$ is equal to the distribution of real transcripts since the both are uniform distribution on commitments, challenges, and responses.

Min-Entropy. Since commitment ψ is uniformly taken from the orbit $\mathcal{O}$ where elements of the statement $x = \{\phi_0, \ldots, \phi_{K-1}\}$ are in, the ATFE-GMW protocol has α-bit min-entropy with $\alpha = \log_2(|\mathcal{O}|)$ and $|\mathcal{O}|$ is the size of orbit $\mathcal{O}$.

Remark 2. By the orbit-stabiliser theorem, for an alternating trilinear form ϕ over $\mathbb{F}_q^n$, we have $|\mathcal{O}(\phi)| = |\mathrm{GL}(n, q)|/|\mathrm{Aut}(\phi)|$. In Section 3.4, some results on the automorphism group orders, and therefore orbit sizes, of random alternating trilinear forms will be presented.

Commitment Recoverable. The ATFE-GMW protocol is commitment recoverable. In fact, given a challenge c and a response D, there is only one commitment ψ computed by $\psi = \phi_c \circ D$.

The ATFE-GMW-FS-$\mathcal{O}(\phi)$ *scheme.* In Section 3, we will need a variant of the ATFE-GMW-FS scheme as follows. Briefly speaking, this variant restricts to an orbit of some specific $\phi \in \mathrm{ATF}(n,q)$ instead of working in the orbit of a random $\phi \in \mathrm{ATF}(n,q)$. That is, we fix a specific $\phi \in \mathrm{ATF}(n,q)$, and in the key generation step, we randomly sample $A_i \in_R \mathrm{GL}(n,q)$ for $i \in \{0,1,\dots,K-1\}$ to compute $\phi_i = \phi \circ A_i$ for $i \in \{0,1,\dots,K-1\}$. The rest is the same as the ATFE-GMW-FS scheme. We shall call such a scheme the ATFE-GMW-FS-$\mathcal{O}(\phi)$ scheme, and its underlying Sigma-protocol the ATFE-GMW-$\mathcal{O}(\phi)$ protocol. Follow the above proof and Assumption 2, ATFE-GMW-$\mathcal{O}(\phi)$ protocol also has these properties.

3 QROM security via perfect unique responses

In this section, we show that the ATFE-GMW-FS scheme is secure in the quantum random oracle model (QROM) subject to a certain condition on the automorphism group of the alternating trilinear form in use.

This section is organised as follows. In Section 3.1, we review some basics of the quantum random oracle model. In Section 3.2, we translate perfect and computational unique response properties of the ATFE-GMW protocol to certain properties about automorphism groups of alternating trilinear forms. In Section 3.3, we formally state the theorem on QROM security of the ATFE-GMW-FS scheme. Finally in Section 3.4, we provide theoretical and experiment results on the automorphism group orders of random alternating trilinear forms for the parameters proposed in [40].

3.1 Preliminaries on the quantum random oracle model

The random oracle model (ROM) was first proposed in 1993 by Bellare and Rogaway in [5] as a heuristic to provide security proofs in cryptography. Briefly speaking, in the ROM model, the hash function is replaced by a random oracle. However, ROM is insufficient when considering quantum adversaries, which leads to the proposal of the *quantum* ROM (QROM) [8]. One main reason comes from that quantum adversaries can make queries as a superposition. For example, let $H : \mathcal{X} \to \mathcal{Y}$ be a hash function, a quantum adversary will make superposition queries to evaluate this function, that is, for input $\sum_x \beta_x |x\rangle$ return $\sum_x \beta_x |x\rangle |H(x)\rangle$. Security proof migration from ROM to QROM is not an easy task, due to several obstacles from some properties in the quantum setting, such as whether the query is a superposition, quantum no cloning, and quantum measurement causes collapse, etc. Indeed, there exist that protocols that are secure in ROM but not in QROM [8,45] .

Recently, thanks to a pair of breakthrough papers [18,32], the QROM security of the Fiat-Shamir transform is now much better understood. Based on these papers, we study the relation between the ATFE-GMW scheme and the *perfect unique response* property introduced by Unruh [42]. With this important property and some additional properties we state in Section 2.7, we can prove the security of the ATFE-GWM protocol under quantum ROM.

3.2 Perfect and computationally unique responses of the ATFE-GMW protocol

We require some extra properties such that the ATFE-GMW or ATFE-GMW-$\mathcal{O}(\phi)$ protocols in Section 2.7 meet the *perfect unique response* and *computationally unique response* properties.

Lemma 1 (Perfect Unique Response). *The ATFE-GMW-$\mathcal{O}(\phi)$ protocol supports perfect unique response iff* $\mathrm{Aut}(\phi)$ *is trivial.*

Proof. In the one direction, assume that $\mathrm{Aut}(\phi)$ is trivial. If there are two valid transcripts (ψ, c, D) and (ψ, c, D') for the protocol in 1. Then we have $\phi_c \circ D = \phi_c \circ D'$. It implies that $E \in \mathrm{Aut}(\phi)$ where $E = D'D^{-1}$ and thus $D = D'$.

Now assume that the ATFE-GMW-$\mathcal{O}(\phi)$ protocol satisfies the perfect unique response property. If $\mathrm{Aut}(\phi)$ is non-trivial, i.e., there exists an invertible matrix $E \neq I_n$ such that $\phi \circ E = \phi$. Therefore, all elements in $\{\phi_0, \ldots, \phi_{K-1}\}$ have non-trivial automorphism groups. Due to the completeness, there is a valid transcript (ψ, c, D) for any ψ and any $c \in \{0,1\}^{K-1}$. Hence, for the statement $\{\phi_0, \ldots, \phi_{K-1}\}$, every commitment ψ, and every challenge c, there are two different responses D and ED such that (ψ, c, D) and (ψ, c, ED) are valid transcripts, which is a contradiction. This completes the proof. □

We have the following triviality assumption on the autormophism group of alternating trilinear forms. We present some experimental support for this Assumption in Section 3.4.

Assumption 3. The automorphism group of an alternating trilinear form $\phi \in_R \mathrm{ATF}(n, q)$ is trivial with a high probability.

Remark 3. Although perfect unique response for ATFE-GMW protocol can not be proved rigorously, statistical unique response[3] can be proved based on Assumption 3. However, it is not known if statistical unique response is enough to prove the quantum proof of knowledge.

To illustrate the relation between the computationally unique response and alternating trilinear form, we claim a new algorithm problem.

Definition 9. *The alternating trilinear form automorphism problem is the following.*

Input: *An alternating trilinear forms* $\phi \in_R \mathrm{ATF}(n, q) : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$.
Output: *Some* $A \in \mathrm{GL}(n, q), A \neq I_n$ *such that* $\phi = \phi \circ A$.

Lemma 2 (Computationally Unique Response). *The ATFE-GMW protocol in 1 supports computationally unique response iff no poly-time quantum algorithm can solve* ATF *automorphism problem in Definition 9 with a non-negligible probability.*

[3] Given commitment and challenge, there are more than one possible valid response with a negligible probability.

Proof. Assume that the Σ-protocol supports computationally unique response. If there is a poly-time quantum adversary $\mathcal{A}$ such that for any statement $x = \{\phi_0, \ldots, \phi_{K-1}\} \subseteq \mathrm{ATF}(n, q)$, it can compute two valid transcripts (ψ, c, D) and (ψ, c, D'), where $D \neq D'$, with a non-negligible probability. Then there is an algorithm $\mathcal{A}_1$ using $\mathcal{A}$ as subroutine such that for any $\phi_c \in \mathrm{ATF}(n, q)$, it can produce an $E = D'D^{-1}$ such that $\phi_c \circ E = \phi_c$ with a non-negligible probability.

Assume that no poly-time quantum algorithm can solve ATF automorphism problem with a non-negligible probability.If there is a poly-time quantum algorithm $\mathcal{A}_1$ such that, for any $\phi \in \mathrm{ATF}(n, q)$, it can get an automorphism E such that $\phi_c \circ E = \phi_c$ with a non-negligible probability. By the HVZK property, there exists a simulator $\mathcal{S}$ such that, for any $x = \{\phi_0, \ldots, \phi_{K-1}\} \subseteq \mathrm{ATF}(n, q)$, it can produce a valid transcript (ψ, c, D). Then there is an adversary $\mathcal{A}$ using $\mathcal{A}_1$ and $\mathcal{S}$ as subroutines such that it firstly computes a valid transcript (ψ, c, D) by $\mathcal{S}$, and then computes E such that $\phi_c \circ E = \phi_c$ by $\mathcal{A}_1$. Thus, for any statement $\{\phi_0, \ldots, \phi_{K-1}\} \subseteq \mathrm{ATF}(n, q)$, $\mathcal{A}$ can compute two transcripts (ψ, c, D) and (ψ, c, ED) with a non-negligible probability. □

Remark 4. The above proof can be applied to show the same result for ATFE-GMW-$\mathcal{O}(\phi)$.

3.3 QROM security via perfect unique responses

Theorem 2. *Suppose $\phi \in \mathrm{ATF}(n, q)$ satisfies that $\mathrm{Aut}(\phi)$ is trivial. The ATFE-GMW-FS-$\mathcal{O}(\phi)$ signature based on the t repeatitions of ATFE-GMW-$\mathcal{O}(\phi)$ protocol has strong existential unforgeability under chosen-message attack (EUF-CMA) security. More specifically, for any polynomial-time quantum adversary $\mathcal{A}$ querying the quantum random oracle Q_H times against EUF-CMA security of ATFE-GMW-FS-$\mathcal{O}(\phi)$ signature, there is a quantum adversary $\mathcal{B}$ for m-psATFE-$\mathcal{O}(\phi)$ problem such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ATFE-EUF-CMA}} \leq O\left({Q_H}^9 \cdot \left(\mathsf{Adv}_{\mathcal{B}}^{m-\mathsf{psATFE}} \right)^{\frac{1}{3}} \right).$$

Proof. By Theorem 4, we have a Σ-protocol with post-quantum ID soundness. Then the EUF-CMA security can be achieved by Theorem 6. □

Post-Quantum ID soundness of ATFE-GMW Σ-protocol When a Σ-protocol is for identification, we need a definition of ID soundness to protect against the adversaries with eavesdropping attack.

Definition 10. *A Σ-protocol has* post-quantum ID soundness *if for any $(x, w) \in R$, every adversary $\mathcal{A}^{\mathcal{O}_{\mathcal{P},\mathcal{V}}} = \left(\mathcal{A}_0^{\mathcal{O}_{\mathcal{P},\mathcal{V}}}, \mathcal{A}_1^{\mathcal{O}_{\mathcal{P},\mathcal{V}}} \right)$ with only the* pk *and polynomial times of queries to the valid transcripts generated with an honest prover $\mathcal{P}$ with* pk *and* sk *and an honest verifier $\mathcal{V}$ with* pk *can convince an honest verifier $\mathcal{V}$ with a negligible probability, i.e.*

$$\Pr\left[\mathcal{V}.\mathsf{Ver}(\mathsf{pk}, a, c, r) = 1 \mid a \leftarrow \mathcal{A}_0^{\mathcal{O}_{\mathcal{P},\mathcal{V}}}(\mathsf{pk}) \wedge c \xleftarrow{\$} C_n \wedge r \leftarrow \mathcal{A}_1^{\mathcal{O}_{\mathcal{P},\mathcal{V}}}(\mathsf{pk}, a, c) \right] \leq \mathsf{negl}(\lambda).$$

Liu and Zhandry show that post-quantum identification soundness can be satisfied if sigma protocol has weakly collapsing property and extra properties [32, Theorem 1]. Since the perfect unique response is a stronger property than weakly collapsing property, we can state the result in [32] as follows.

Theorem 3 ([32]). *If a Σ-protocol with an exponentially large challenge space has completeness, post-quantum 2-soundness, HVZK, and perfect unique response, it is a Σ-protocol with post-quantum ID soundness that for any polynomial-time quantum adversary $\mathcal{A}$ against post-quantum ID soundness, there is a quantum adversary $\mathcal{B}$ for 2-soundness such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\textsf{\textit{ID-sound}}} \leq O\left(\left(\mathsf{Adv}_{\mathcal{B}}^{\textsf{\textit{2-sound}}}\right)^{\frac{1}{3}}\right).$$

Theorem 4. *The t repeatitions of $\textsf{\textit{ATFE-GMW-}}\mathcal{O}(\phi)$ Σ-protocol in Figure 1 is a Σ-protocol with post-quantum ID soundness that for any polynomial-time quantum adversary $\mathcal{A}$ against post-quantum ID soundness, there is a quantum adversary $\mathcal{B}$ for K-$\textsf{\textit{psATFE}}$ problem such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\textsf{\textit{ATFE}}-\textsf{\textit{ID}}} \leq O\left(\left(\mathsf{Adv}_{\mathcal{B}}^{K-\textsf{\textit{psATFE}}}\right)^{\frac{1}{3}}\right).$$

Proof. By the Assumption 3 and the Lemma 1, the Σ-protocol in Figure 1 has perfect unique response. We also proved that it has completeness, 2-soundness, and HVZK in the Section 2.7. Since the The t repeatitions of Σ-protocol in Figure 1 has an exponentially large challenge space, we complete the proof using the result of Theorem 3. □

Security of ATFE-GMW-FS signature Liu and Zhandry [32, Theorem 11] showed that the signature security can be reduced to the underlying Σ-protocol with post-quantum ID soundness through a variant of Zhandry's compressed oracle model [46]. Since min-entropy $\alpha = \Omega(\lambda)$ implies that the Σ-protocol has unpredictable commitment, we can substitute unpredictable commitment with $\Omega(n)$ bits min-entropy to have the following theorem.

Theorem 5 ([32]). *If a Σ-protocol has post-quantum ID soundness and $\Omega(n)$ bits min-entropy, the Fiat-Shamir transformation can produce a signature scheme with EUF-CMA security that for any polynomial-time quantum adversary $\mathcal{A}$ querying the quantum random oracle Q_H times against EUF-CMA security, there is a quantum adversary $\mathcal{B}$ against ID-soundness of the underlying protocol such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\textsf{\textit{EUF-CMA}}} \leq O\left(Q_H^9 \cdot \mathsf{Adv}_{\mathcal{B}}^{\textsf{\textit{ID-sound}}}\right).$$

Theorem 6. *If the t repeatitions of $\textsf{\textit{ATFE-GMW-}}\mathcal{O}(\phi)$ protocol showed in Figure 1 has post-quantum ID soundness, then the corresponding Fiat-Shamir signature has EUF-CMA security that for any polynomial-time quantum adversary*

$\mathcal{A}$ *querying the quantum random oracle* Q_H *times against EUF-CMA security of* ATFE-GMW-FS *signature, there are quantum adversary* $\mathcal{B}$ *against ID-soundness of* ATFE-GMW-$\mathcal{O}(\phi)$ *protocol such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ATFE-EUF\text{-}CMA}} \leq O\left(Q_H^9 \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathsf{ATFE-ID}}\right).$$

Proof. Assume the t repeatitions of Σ-protocol showed in Figure 1 has post-quantum ID soundness. We proved that it has $\log_2(|\mathcal{O}|)$ bits min-entropy in Section 2.7, and $|\mathcal{O}| = 2^{\Omega(\lambda)}$. Now we complete the proof utilizing the result of Theorem 5 □

3.4 On the automorphism group orders of alternating trilinear forms

The above results indicate the key role played by the automorphism groups of the alternating trilinear forms in use. In this section we present some theoretical and experiment results on this topic. The main messages are, for certain (n, q) of interest in cryptography proposed in [40], (1) there exist many alternating trilinear forms with trivial automorphism groups, and (2) a random alternating trilinear form is expected to have a trivial automorphism group, but to our best knowledge, to estimate this probability is open.

Let $\phi \in \mathrm{ATF}(n, q)$, and let $\mathrm{Aut}(\phi) := \{A \in \mathrm{GL}(n, q) \mid \phi = \phi \circ A\}$. Some basic facts about $\mathrm{Aut}(\phi)$ are as follows. First, note that if $3|q-1$, then $\mathrm{Aut}(\phi)$ cannot be trivial. This is because $3|q-1$ implies the existence of $\lambda \in \mathbb{F}_q$, $\lambda \neq 1$, and $\lambda^3 = 1$. Therefore $\lambda I_n \in \mathrm{Aut}(\phi)$. Second, for (a) $n = 7$ and (b) $n = 8$ and $\mathrm{char}(\mathbb{F}_q) \neq 3$, there exist no alternating trilinear forms with trivial automorphism groups, by classifications of alternating trilinear forms in these cases [15,35,25]. Third, for $n = 9$ and $q = 2$, by the classification of alternating trilinear forms [26], there exists a unique orbit of alternating trilinear forms with trivial automorphism groups.

In general, because of the difference between the dimension of $\mathrm{GL}(n, q)$ (which is n^2) and the difference between the dimension of $\mathrm{ATF}(n, q)$ (which is $\binom{n}{3}$), it is expected that for $n \geq 10$ and $3 \nmid q-1$, most alternating trilinear forms would have the trivial automorphism group. To verify this, we wrote a program in Magma [9] for computing automorphism group orders of alternating trilinear forms. Built on the Magma program in [40], our program implements the following procedure. Let $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an alternating trilinear form.

1. Enumerate every $v \in \mathbb{F}_q^n$ and compute the rank of $\phi(v, \cdot, \cdot)$ as an alternating bilinear form. Let $S \subseteq \mathbb{F}_q^n$ be the set of non-zero vectors such that $\phi(v, \cdot, \cdot)$ is of lowest rank.
2. Fix $u \in S$. Let X and Y be two $n \times n$ variable matrices. For every $v \in S$, set up a system of polynomial equations expressing the following:
   (a) $\phi \circ X = \phi$, and $\phi = \phi \circ Y$.
   (b) For any $a, b, c \in \mathbb{F}^n$, $\phi(X(a), X(b), c) = \phi(a, b, Y(c))$, and $\phi(X(a), b, c) = \phi(a, Y(b), Y(c))$.

(c) $XY = I_n$, and $YX = I_n$.
(d) $X(u) = v$, and $Y(v) = u$.
The use the Gröbner basis algorithm implemented in Magma to compute the number of solutions to this system of polynomial equations. Let it be s_v.
3. Sum over s_v over $v \in S$ as the order of $\mathrm{Aut}(\phi)$.

This algorithm runs in time $q^n \cdot \mathsf{poly}(n, \log q)$. The use of Gröbner computations follows the practices of works in multivariate cryptography for solving polynomial isomorphism [20,10,11,12]. The reason for Step 1 is to limit the number of Gröbner basis computations, which are more costly compared to computing the ranks. This idea could be found, for example, in [14]. The way we set up the equations is from [40].

Our experiment results are as follows.

- For $q = 2$ and $n = 9$, out of 100 samples there are three ones with trivial automorphism groups. This is consistent with the fact that in this setting, there exists exactly one orbit of alternating trilinear forms, which implies that the probability of sampling one from this orbit is $|\mathrm{GL}(2, 9)|/2^{84} \approx 3.6169\%$.
- For $q = 2$ and $n = 10, 11$, all 100 samples return trivial automorphism groups.
- For $q = 3$ and $n = 10, 11$, all 10 samples return trivial automorphism groups.
- For $q = 3$ and $n = 9$, all 100 samples return *non-trivial* automorphism groups.
- For $q = 5$ and $n = 9$, all 3 samples return *non-trivial* automorphism groups.

These suggest that for $n = 10$ and q satisfying $3 \nmid q - 1$, a random alternating trilinear form has the trivial automorphism group with good probability. To the best of our knowledge, to give an estimation of this probability (depending on q and n) is open.

4 Tightly Secure Signature from ATFE in QROM

4.1 Definition

In this section, we recall the definition of lossy identification protocol [1,19] and a security result of its associated Fiat-Shamir signature in QROM from [29].

Definition 11. *An identification protocol ID is called lossy, denoted by $\mathsf{ID}_{\mathsf{ls}}$, if it has one additional PPT algorithm* $\mathsf{LossyGen}$*, called lossy key generatation that on input the security parameter outputs a lossy verification key* pk*. To be more precise,* $\mathsf{LossyGen}(1^\lambda)$ *generates* $x_{\mathsf{ls}} \leftarrow \mathsf{LossyGen}(1^\lambda)$ *such that there are no* $w \in \mathcal{W}$ *satisfying* $(x_{\mathsf{ls}}, w) \in \mathcal{R}$.

A lossy identification protocol is required to satisfy the following additional properties.

Indistinguishability of lossy statements. It is requires that the lossy statements generated by $\mathsf{LossyGen}(1^\lambda)$ is indistinguishable with ones generated by $\mathsf{Gen}(1^\lambda)$, i.e., . for any PPT (or quantum PT) adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ against the indistinguishability of lossy statements

$$\begin{aligned}\mathsf{Adv}^{\mathsf{ls}}_{\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(x_{\mathsf{ls}} = 1) | x_{\mathsf{ls}} \leftarrow \mathsf{LossyGen}(1^\lambda)]\\ - \Pr[\mathcal{A}(x) = 1 | (x, w) \leftarrow \mathsf{Gen}(1^\lambda)]\end{aligned}$$

is negligible.

Statistical lossy soundness. Consider following experiment $\mathsf{Exp}^{\mathsf{ls}}_{\mathsf{ID},\mathcal{A}}(\lambda)$ between an adversary $\mathcal{A}$ and a challenger.

- The challenger runs $x_{\mathsf{ls}} \leftarrow \mathsf{LossyGen}(1^\lambda)$ and provides x_{ls} to the adversary $\mathcal{A}$.
- On input x_{ls}, the adversary $\mathcal{A}$ selects a commitment a and sends it to the challenger who responds with a random challenge c.
- On input (a, c), the adversary $\mathcal{A}$ outputs a response r.
- Return 1 if (a, c, r) is a valid transcript for x_{ls}, and 0 otherwise.

We say that the lossy identification protocol $\mathsf{ID}_{\mathsf{ls}}$ is ϵ_{ls}-lossy sound if for any unbounded (possibly quantum) adversary $\mathcal{A}$, the probability of winning the experiment $\mathsf{Exp}^{\mathsf{ls}}_{\mathsf{ID},\mathcal{A}}(\lambda)$ is less than ϵ_{ls}, i.e.,

$$\Pr[\mathsf{Exp}^{\mathsf{ls}}_{\mathsf{ID},\mathcal{A}}(\lambda) = 1] \leq \epsilon_{\mathsf{ls}}.$$

Fiat-Shamir transformation applied to a lossy identification protocol yields a tightly secure signature in QROM [29,32,18]. The following is from [19, Theorem 2.5] which is derived from [29, Theorem 3.1] with the derandomization by a pseudorandom function PRF.

Theorem 7. *Assume that the identification protocol ID is lossy, perfect HVZK, has α bits of min-entropy, has perfect unique response, and is ϵ_{ls}-lossy sound. Then the signature scheme $\mathsf{FS}[\mathsf{ID}]$ obtained from applying the Fiat-Shamir transformation to ID is such that for any quantum adversary $\mathcal{A}$ against the $\mathsf{sEUF\text{-}CMA}$ security that issues at most Q_H queries to the quantum random oracle, there exist quantum adversaries $\mathcal{B}, \mathcal{D}$ such that*

$$\mathsf{Adv}^{\mathsf{sEUF\text{-}CMA}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{ls}}_{\mathcal{B}}(\lambda) + 8(Q_h + 1)^2 \cdot \epsilon_{\mathsf{ls}} + 2^{-\alpha+1} + \mathsf{Adv}^{\mathsf{PRF}}_{\mathcal{D}}(\lambda),$$

and $\mathsf{Time}(\mathcal{B}) = \mathsf{Time}(\mathcal{D}) = \mathsf{Time}(\mathcal{A}) + Q_H \cong \mathsf{Time}(\mathcal{A})$.

In the classical setting, we can replace $8(Q_h + 1)^2$ by $(Q_h + 1)$.

4.2 Lossy identification protocol from ATFE

In this section, we construct a lossy identification protocol based on the psATFE problem. The underlying sigma protocol is the $\mathsf{ATFE\text{-}GMW}$ protocol in Figure 1. Here, we consider a relation $\mathcal{R}$ consisting of statement-witness pairs (x, w) with

$x = \{\phi_0, \phi_1, \ldots, \phi_{K-1}\} \subseteq \mathrm{ATF}(n,q)$and $w = \{A_1, \ldots, A_{K-1}\} :\subseteq \mathrm{GL}(n,q)$, where $\phi_0 \circ A_i^{-1} = \phi_i$ for each $i = 1, \cdots, K-1$.

The lossy identification scheme for the relation $\mathcal{R}$ defined as above with challenge space $\{0, 1, \cdots, K-1\}$ consists of five algorithms (IGen, $\mathsf{LossyGen}$, $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{V}$) as follows.

- Algorithm IGen randomly samples an alternating trilinear form $\phi_0 : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ and invertible matrices $A_1, \cdots, A_{k-1} \in_R \mathrm{GL}(n,q)$. It outpus a statement $x = (\phi_0, \phi_1, \cdots, \phi_{K-1})$ with $\phi_i = \phi_0 \circ A_i^{-1}$ for $i = 1, \cdots, K-1$, and a witness $w = (A_1, \cdots, A_{K-1})$.
- Algorithm $\mathsf{LossyGen}$ randomly samples alternating trilinear forms $\phi_0, \phi_1, \cdots, \phi_{K-1} \in \mathrm{ATF}(n,q)$ and outputs a lossy statement $x_{\mathsf{ls}} = (\phi_0, \phi_1, \cdots, \phi_{K-1})$.
- On input a statement-witness pair (x, w), $\mathcal{P}_1$ samples a random invertible matrix $B \in_R \mathrm{GL}(n,q)$ and outputs the commitment $\psi = \phi_0 \circ B$.
- On input (x, w, ψ, c) where $c \in \{0, 1, \cdots, K-1\}$ is a challenge, $\mathcal{P}_2$ outputs a response $D = B + \textsc{Sign}(c)(A_c B - B)$.
- On input (x, ψ, c, D), the verification algorithm $\mathcal{V}$ check whether $\psi = \phi_c \circ D$.

Security analysis Since the underlying protocol is the same as in Figure 1, it is clear that our lossy identification protocol is complete, has α-bit min-entropy with $\alpha \approx \log_2 |\mathcal{O}|$, satisfies HVZK property and commitment recoverability. It remains to show that our protocol has indistinguishablity of lossy statements and statistical lossy soundness.

Assumption 4. No quantum polynomial-time algorithm can distinguish the K-PR-psATFE-RO problem defined in Definition 8 with a non-negligible probability.

Lemma 3. *Assume the hardness of the K-PR-psATFE-RO problem, our lossy indenfication protocol satisfies lossy statement indistinguishability.*

Proof. The lossy generator of our protocol just random samples K elements $\phi_0, \phi_1, \cdots, \phi_{K-1} \in_R \mathrm{ATF}(n,q)$. By the hardness assumption of the K-PR-psATFE-RO problem, lossy statements and real statements are indistinguishable. □

Lemma 4. *The lossy identification protocol satisfies statistical ϵ_{ls}-lossy soundness for $\epsilon_{\mathsf{ls}} = \frac{1}{K}\prod_{i=1}^{K-1}\frac{N-iM}{N} + \left(1 - \prod_{i=1}^{K-1}\frac{N-iM}{N}\right)$, where $M = |\,\mathrm{GL}(n,q)|$, $N = |\mathrm{ATF}(n,q)|$.*

Proof. This proof is similar to the proof of [19, Lemma 3.3]. Let $\mathcal{X}$ be the set of the statements such that given a commitment ψ, there is only one challenge c resulting in a valid transcript. Assume that for a given commitment ψ, there are two valid transcripts (ψ, c, D) and (ψ, c', D') then these two transcripts satisfies following equations:

$$\phi_c \circ D = \psi$$
$$\phi_{c'} \circ D' = \psi$$

It implies that $\phi_c \circ (DD'^{-1}) = \phi_{c'}$, i.e., ϕ_c and $\phi_{c'}$ are in the same orbit. Therefore, if any two elements in the statement are not in the same orbit, the statement can't have two valid transcripts with different challenges.

The number of different statements in $\mathcal{X}$ is $N \prod_{i=1}^{K-1}(N - i|\mathcal{O}_i|) \geq N \prod_{i=1}^{K-1}(N - iM)$, where $|\mathcal{O}_i|$ is the size of $\mathcal{O}_i$ and $|\mathcal{O}_i| \leq M$. The number of all statements is N^K. Then we can have the probability that a statement is in $\mathcal{X}$: $\Pr[x \in \mathcal{X} \mid x \leftarrow \mathsf{LossyGen}] \geq \prod_{i=1}^{K-1} \frac{N-iM}{N}$. We can obtain the probability that an adversary wins as follows:

$$\begin{aligned}
\Pr[\mathcal{A} \text{ wins}] &= \Pr[\mathcal{A} \text{ wins} \mid x \in \mathcal{X}] \Pr[x \in \mathcal{X}] + \Pr[\mathcal{A} \text{ wins} \mid x \notin \mathcal{X}] \Pr[x \notin \mathcal{X}] \\
&\leq \Pr[\mathcal{A} \text{ wins} \mid x \in \mathcal{X}] \prod_{i=1}^{K-1} \frac{N-iM}{N} + \left(1 - \prod_{i=1}^{K-1} \frac{N-iM}{N}\right) \\
&= \frac{1}{K} \prod_{i=1}^{K-1} \frac{N-iM}{N} + \left(1 - \prod_{i=1}^{K-1} \frac{N-iM}{N}\right).
\end{aligned}$$

This completes the proof. □

Corollary 1. *The lossy identification protocol in Figure 1, that is run t parallel rounds with the same statement-witness pair, satisfies statistical ϵ_{ls}-lossy soundness for $\epsilon_{\mathsf{ls}} = \frac{1}{K^t} \prod_{i=1}^{K-1} \frac{N-iM}{N} + \left(1 - \prod_{i=1}^{K-1} \frac{N-iM}{N}\right)$, where $M = |\operatorname{GL}(n, q)|$, $N = |\operatorname{ATF}(n, q)|$.*

Proof. The proof is straight-forward from that of Lemma 4. Note that for a statement $x \in \mathcal{X}$, the adversary has at most $\frac{1}{K^t}$ probability in winning the lossy impersonation game. The result follows. □

Remark 5. Since $M = q^{n^2}$ and $N = q^{\binom{n}{3}}$, $N \gg M$ as the security parameter λ is large enough. Therefore, the lossy soundness $\epsilon_{ls} \approx \frac{1}{K^t} \approx \frac{1}{2^\lambda}$.

4.3 Tightly secure signature scheme in QROM from ATFE

Construction In this section, we instatiate our signature scheme from applying the Fiat-Shamir transformation [21] to the lossy identification protocol in Section 4.2. The signature scheme depicted in Algorithms 1, 2, 3. The parameter K and t are chosen such that $t \cdot \log_2(K) \cong \lambda$ in the classical setting (as in [40]) and such that $t \cdot \log_2(K) \cong \lambda + \log_2(Q_H)$, where Q_H is the number of queries to the quantum random oracle, in the quantum setting. We call our signature ATFE-Sig. Here $H : \{0,1\}^* \to \{0, 1, \cdots, K-1\}^t$ is a secure hash function. In fact, it is the ATFE-GMW-FS scheme in [40] with the use of a secure PRF to derandomize the signature generation, as similar in [19].

Theorem 8. *Let ATFE-Sig be the signature defined as in Algorithms 1, 2, 3 and assume that the hash functions are modeled as quantum random oracle models. Then for any quantum adversary $\mathcal{A}$ against sEUF-CMA security of ATFE-Sig that issues at most Q_H queies to the quantum random oracle, there exists a quantum*

Algorithm 1: Key generation.

Input: The variable number $n \in \mathbb{N}$, a prime power q, a parameter $K \in \mathbb{N}$.
Output: Public key: K alternating trilinear forms
$\phi_0, \phi_1, \cdots, \phi_{K-1} \in \mathrm{ATF}(n, q)$ such that the ϕ_i's are isomorphic.
Private key: Invertible matrices $A_1, \cdots, A_{K-1} \in \mathrm{GL}(n, q)$ such that
$\phi_0 \circ A_i^{-1} = \phi_i$ for $i = 1, \cdots, K-1$.

```
Randomly sample an alternating trilinear form φ_0 : F_q^n × F_q^n × F_q^n → F_q.
Randomly sample invertible matrices A_1, ⋯ , A_{K−1} ∈ GL(n, q).
Compute φ_i = φ_0 ∘ A_i^{−1} for i = 1, ⋯ , K.
E ← 𝒦                                              #Sample a key for PRF
return Public key: φ_0, φ_1, ⋯ , φ_{K−1}. Private Key: A_1, ⋯ , A_{K−1}, E
```

Algorithm 2: Signature generation.

Input: Public key pk, secret key sk and a message M.
Output: A signature σ.

```
for k ∈ {1, ⋯ , t} do
    B_k ∈_R GL(n, q)                    #Derive randomness using PRF(E, M‖k)
    ψ_k := φ_0 ∘ B_k
end
(c_1, ⋯ , c_t) = H(ψ_1‖ ⋯ ‖ψ_t‖M)
for k ∈ {1, ⋯ , t} do
    D_k := B + SIGN(c_k)(A_{c_k} B − B)
end
σ := (c_1, ⋯ , c_t, D_1, ⋯ , D_t)
return σ
```

Algorithm 3: Verification.

Input: Public key pk, a message M and a signature σ.
Output: 0 or 1.

```
Parse σ as (c_1, ⋯ , c_t, D_1, ⋯ , D_t)
for k ∈ {1, ⋯ , t} do
    Compute ψ_k = φ_0 ∘ D_k
end
(c'_1, ⋯ , c'_t) = H(ψ_1‖ ⋯ ‖ψ_t‖M)
if (c'_1, ⋯ , c'_t) == (c_1, ⋯ , c_t) then
    return 1
else
    return 0
end
```

adversary $\mathcal{B}$ against the K-PR-psATFE problem and a quantum adversary $\mathcal{D}$ against the PRF *such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\textsf{sEUF-CMA}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}}^{K-PR-\textsf{psATFE}}(\lambda) + \mathsf{Adv}_{\mathcal{D}}^{\mathsf{PRF}}(\lambda) + \frac{2}{|\mathcal{O}|}$$
$$+ 8(Q_H+1)^2 \cdot \left(\frac{1}{K^t} \prod_{i=1}^{K-1} \frac{N-iM}{N} + \left(1 - \prod_{i=1}^{K-1} \frac{N-iM}{N}\right)\right)$$

and $\mathsf{Time}(\mathcal{B}) = \mathsf{Time}(\mathcal{D}) = \mathsf{Time}(\mathcal{A}) + Q_H \cong \mathsf{Time}(\mathcal{A})$. *Here* $|\mathcal{O}|$ *is the size of the orbit where elements of the statement* $x = (\phi_0, \phi_1, \cdots, \phi_{K-1})$ *are in.*

In the classical setting, we can replace $8(Q_H+1)^2$ *with* $Q_H + 1$.

Proof. The proof is similar to that of [18, Theorem 5.1]. It follows from Section 3.4, Lemma 1 and Section 4.2 that the underlying sigma protocol has perfect unique response, perfect HVZK and at least λ bits of min-entropy. The result now follows from Theorem 7. □

Remark 6. Since our results about min entropy and lossy soundness, Assumption 4, and further assume the hardness of pseudorandom function, all items in Theorem 8 are negligible. Therefore, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sEUF\text{-}CMA}}(\lambda)$ is negligible.

5 Ring Singatures from ATFE

In this section, we describe the construction of ring signatures from ATFE. The design follows the framework of Beullens, Katsumata and Pintore [7] in the context of commutative group actions. The ring signature is obtained by applying the Fiat-Shamir transformation to an OR-Sigma protocol, which is described in Figure 2.

5.1 Base OR-Sigma protocol from ATFE

In particular, let $A_1, A_2, \ldots, A_N \xleftarrow{\$} G$ be the secret keys, and $\phi_1 = \phi_0 \circ A_1, \ldots, \phi_N = \phi_0 \circ A_N$ be the public keys, Com be a commitment scheme. The base OR-Sigma protocol in Figure 2, with **statement** $\{\phi_0, \ldots, \phi_N \in \mathrm{ATF}(n,q)\}$ and **witness** $\{A_I \in \mathrm{GL}(n,q), I \in [N]$ such that $\phi_0 \circ A_I = \phi_I\}$, works as follows:

1. First, the prover random sample an invertible matrix $B \in GL(n,q)$, and apply it to $\phi_1, \ldots, \phi_N$ respectively. Specifically, $\psi_1 = \phi_1 \circ B, \ldots, \psi_N = \phi_N \circ B$. Then the prover samples $\mathsf{bits}_i \xleftarrow{\$} \{0,1\}^\lambda$ and commits to ψ_i with $\mathsf{C}_i = \mathsf{Com}(\psi_i, \mathsf{bits}_i)$. The prover further builds a Merkle tree[4] with the $(\mathsf{C}_1, \ldots, \mathsf{C}_N)$ as its leaves. The prover computes the root root of the Merkle tree and sends it to the verifier as the commitment.

[4] Note that the Merkle tree used here is slightly modified. It is index-hiding Merkle tree, please see [7, Section 2.6]

$\mathcal{P}_1(\phi_1, \ldots, \phi_N)$

$\mathsf{seed} \xleftarrow{\$} \{0,1\}^\lambda$
$(B, \mathsf{bits}_1, \ldots, \mathsf{bits}_N) \leftarrow \mathsf{PRG}(\mathsf{seed})$
for i from 1 to N **do**
    $\psi_i \leftarrow \phi_i \circ B$
    $\mathsf{C}_i \leftarrow \mathsf{Com}(\psi_i, \mathsf{bits}_i)$
$(\mathsf{root}, \mathsf{tree}) \leftarrow \mathsf{MerkleTree}(\mathsf{C}_1, \ldots, \mathsf{C}_N)$
$\mathsf{com} \leftarrow \mathsf{root}$
The prover $\mathcal{P}$ sends the commitment com to the verifier $\mathcal{V}$

$\mathcal{V}_1(\mathsf{com})$

$c \xleftarrow{\$} \{0,1\}$
$\mathsf{cha} \leftarrow c$
The verifier $\mathcal{V}$ sends the challenge cha to the prover $\mathcal{P}$

$\mathcal{P}_2(A_I, I, \mathsf{cha})$

$c \leftarrow \mathsf{cha}$
if $c = 0$ **then**
    $D \leftarrow BA_I$
    $\mathsf{path} \leftarrow \mathsf{getMerklePath}(\mathsf{tree}, I)$
    $\mathsf{rsp} \leftarrow (D, \mathsf{path}, \mathsf{bits}_I)$
else
    $\mathsf{rsp} \leftarrow \mathsf{seed}$
The prover $\mathcal{P}$ sends the response rsp to the verifier $\mathcal{V}$

$\mathcal{V}_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, \phi_0, \phi_1, \ldots, \phi_N)$

$(\mathsf{root}, c) \leftarrow (\mathsf{com}, \mathsf{cha})$
if $c = 0$ **then**
    $(D, \mathsf{path}, \mathsf{bits}) \leftarrow \mathsf{rsp}$
    $\tilde{\psi} \leftarrow \phi_0 \circ D$
    $\tilde{\mathsf{C}} \leftarrow \mathsf{Com}(\tilde{\psi}, \mathsf{bits})$
    $\widetilde{\mathsf{root}} \leftarrow \mathsf{ReconstructRoot}(\tilde{\mathsf{C}}, \mathsf{path})$
    The verifier $\mathcal{V}$ outputs accept if $\widetilde{\mathsf{root}} = \mathsf{root}$, else outputs reject
else
    $\mathsf{seed} \leftarrow \mathsf{rsp}$
    $\widetilde{\mathsf{root}} \leftarrow \mathcal{P}_1((\phi_1, \ldots, \phi_N), \mathsf{seed})$
    The verifier $\mathcal{V}$ outputs accept if $\widetilde{\mathsf{root}} = \mathsf{root}$, else outputs reject

Fig. 2. OR-Sigma protocol.

2. When the verifier receives the commitment, it will randomly sample a challenge $c \xleftarrow{\$} \{0, 1\}$ and response it to the prover.
3. If $c = 0$, then the prover computes $D = BA_I$ and the authenticated path for C_I. The prover sends back a response $\mathsf{rsp} = (D, \mathsf{path}, \mathsf{bits}_I)$. The verifier applies D to ϕ_0 to get $\tilde{\psi}$ and computes $\tilde{\mathsf{C}} = \mathsf{Com}(\tilde{\psi}, \mathsf{bits}_I)$. The verifier then get a root $\tilde{\mathsf{root}}$ by path and $\tilde{\mathsf{C}}$. Finally the verifier checks whether $\tilde{\mathsf{root}} = \mathsf{root}$.
4. If $c = 1$, then the prover sends $(B, \mathsf{bits}_1, \ldots, \mathsf{bits}_N)$ to the verifier. This information allows verifier to rebuild a Merkle tree as in step 1, and then check that the roots are consistent.

5.2 Optimization

Following some optimization techniques used in [7], we can have a more efficient OR-Sigma protocol. We just briefly describe the following three techniques, for more details please see [7, Section 3.4].

1. The challenge space of original challenge space is binary. One can observe that the response with challenge $\mathsf{cha} = 0$ is more costly than that challenge $\mathsf{cha} = 1$. Instead of choosing the challenge bit uniformly in each round, we execute OR sigma protocol $M > \lambda$ rounds and fix exactly K rounds with challenge $\mathsf{cha} = 0$. To satisfy the λ bits of security, we can choose proper parameters M, K such that $\binom{M}{K} \geq 2^\lambda$. Denote $C_{M,K}$ as the set of strings in $\{0, 1\}^M$ with K-bits of 0.
2. With the unbalanced challenge space technique, we do M executions of OR sigma protocol and $M - K$ executions respond with random seeds. Instead of randomly sample M independent seeds, we can utilize seed tree to generate these seeds. Then prover can responsd with $\mathsf{seeds}_{\mathsf{internal}} \leftarrow \mathsf{ReleaseSeeds}(\mathsf{seed}_{\mathsf{root}}, \mathbf{c})$ instead of $M - K$ seeds, where $\mathbf{c}$ is randomly sampled from $C_{M,K}$. The verifier can use $\mathsf{seeds}_{\mathsf{internal}}$ and $\mathbf{c}$ to recover $M - K$ seeds.
3. Adding salt is a well-known technique that allows us to have tighter security proofs for zero-knowledge. Also it avoids multi-target attacks, as in [17], without affecting too much efficiency.

After applying the above methods, we obtain the optimized base OR sigma protocol shown in Figure 3.

5.3 Security proof for the optimized base OR-Sigma protocol

Theorem 9. *Define the following relation*

$$R = \left\{ ((\phi_0, \phi_1, \ldots, \phi_N), (A, I)) \middle| \begin{array}{c} A \in \mathrm{GL}(n, q), \phi_i \in \mathrm{ATF}(n, q) \\ I \in [N], \phi_I = \phi_0 \circ A \end{array} \right\},$$

$\mathcal{P}_1'(\phi_1, \ldots, \phi_N)$

$\mathsf{seed}_{\mathsf{root}} \xleftarrow{\$} \{0,1\}^{\lambda}$
$\mathsf{salt} \xleftarrow{\$} \{0,1\}^{2\lambda}$
$(\mathsf{seed}_1, \ldots, \mathsf{seed}_M) \leftarrow \mathsf{SeedTree}^{\mathcal{O}(\mathsf{salt}||\cdot)}(\mathsf{seed}_{\mathsf{root}}, M)$
for i from 1 to M **do**
  $\mathsf{com}_{\mathsf{i}} \leftarrow \mathcal{P}_1^{\mathcal{O}(\mathsf{salt}||i||\cdot)}((\phi_1, \ldots, \phi_N), \mathsf{seed}_i)$
$\mathsf{com} \leftarrow (\mathsf{salt}, \mathsf{com}_1, \ldots, \mathsf{com}_M)$
The prover $\mathcal{P}$ sends the commitment com to the verifier $\mathcal{V}$

$\mathcal{V}_1'(\mathsf{com})$

$\mathbf{c} \xleftarrow{\$} C_{M,K}$
$\mathsf{cha} \leftarrow \mathbf{c}$
The verifier $\mathcal{V}$ sends the challenge cha to the prover $\mathcal{P}$

$\mathcal{P}_2'(A_I, I, \mathsf{cha})$

$\mathbf{c} = (c_1, \ldots, c_M) \leftarrow \mathsf{cha}$
for i s.t. $c_i = 0$ **do**
  $\mathsf{rsp}_i \leftarrow \mathcal{P}_2(A_I, I, c_i, \mathsf{seed}_i)$
$\mathsf{seeds}_{\mathsf{internal}} \leftarrow \mathsf{ReleaseSeeds}^{\mathcal{O}(\mathsf{salt}||\cdot)}(\mathsf{seed}_{\mathsf{root}}, \mathsf{salt}, \mathbf{c})$
$\mathsf{rsp} \leftarrow (\mathsf{seeds}_{\mathsf{internal}}, \{\mathsf{rsp}_i\}_{i \text{ s.t. } c_i=0})$
The prover $\mathcal{P}$ sends the response rsp to the verifier $\mathcal{V}$

$\mathcal{V}_2'(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, \phi_0, \phi_1, \ldots, \phi_N)$

$((\mathsf{salt}, \mathsf{com}_1, \ldots, \mathsf{com}_M)) \leftarrow \mathsf{com}$
$\mathbf{c} = (c_1, \ldots, c_M) \leftarrow \mathsf{cha}$
$(\mathsf{seeds}_{\mathsf{internal}}, \{\mathsf{rsp}_i\}_{i \text{ s.t. } c_i=0}) \leftarrow \mathsf{rsp}$
$\{\mathsf{rsp}_i\}_{i \text{ s.t. } c_i=1} \leftarrow \mathsf{RecoverLeaves}^{\mathcal{O}(\mathsf{salt}||\cdot)}(\mathsf{seeds}_{\mathsf{internal}}, \mathbf{c})$
for i from 1 to M **do**
  if $\mathcal{V}_2^{\mathcal{O}(\mathsf{salt}||i||\cdot)}(\mathsf{com}_i, c_i, \mathsf{rsp}_i)$ outputs reject **then**
    The verifier $\mathcal{V}$ outputs reject
The verifier $\mathcal{V}$ outputs accept

Fig. 3. Optimized OR sigma protocol.

and the relaxed relation

$$R = \left\{ ((\phi_0, \phi_1, \ldots, \phi_N), w) \middle| \begin{array}{rr} & A \in \mathrm{GL}(n,q), \phi_i \in \mathrm{ATF}(n,q) \\ w = (A, I): & I \in [N], \phi_I = \phi_0 \circ A \\ w = (x, x'): & \mathit{or}\ x \neq x', \mathcal{H}_{\mathsf{Coll}}(x) = \mathcal{H}_{\mathsf{Coll}}(x') \\ & \mathit{or}\ \mathsf{Com}(x) = \mathsf{Com}(x') \end{array} \right\},$$

Then the optimized base OR sigma protocol shown in Figure 3 has correctness, relaxed special soundness and honest-verifier zero-knowledge for the relation R.

Proof. Let $G, S_1, S_2 \coloneqq \mathrm{GL}(n,q)$, $\mathcal{X} \coloneqq \mathrm{ATF}(n,q)$, $D_{\mathcal{X}} = \{\circ\}$ and $\delta = 1$. Then assume the ATFE problem is hard, $(G, \mathcal{X}, S_1, S_2, D_{\mathcal{X}})$ is a 1-admissible group action satisfied the properties (1), (2), (3) in the [7, Definition 3.1]. By the Theorem 3.5 and Theorem 3.6 in [7], our OR sigma protocol is proved to have correctness, relaxed special soundness and honest-verifier zero-knowledge. $\square$

5.4 From OR-Sigma protocol to ring signatures

In this section, we obtain a ring signature by applying the Fiat-Shamir's transformation to the OR-Sigma protocol. The Key generation, signature generation and verification of the ring signature scheme are described in Algorithms 4 5 6 respectively.

Algorithm 4: Key generation

Input: The variable number $n \in \mathbb{N}$, a prime power q, the ring size N.
Output: Public key: N alternating trilinear forms $\phi_0, \ldots, \phi_N \in \mathrm{ATF}(n,q)$.
Private key: N matrices $A_1, \ldots, A_N$ such that $\phi_i = \phi_0 \circ A_i$ for $i \in [N]$.

1 Randomly sample an alternating trilinear form ϕ_0 from $\mathrm{ATF}(n,q)$.
2 Randomly sample N matrices $A_1, \ldots, A_N$ from $\mathrm{GL}(n,q)$.
3 For every $i \in [N]$, $\phi_i \leftarrow \phi_0 \circ A_i$.
4 **return** *Public key:* $\phi_0, \phi_1, \ldots, \phi_N$. *Private key:* $A_1, \ldots, A_N$.

Algorithm 5: Signing procedure

Input: The public key: $\phi_0, \ldots, \phi_N$. The private key: $A_1, \ldots, A_N$. The security parameter λ. The message msg. The commitment scheme $\mathsf{Com} : \{0,1\}^* \to \{0,1\}^\lambda$. A hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.
Output: The signature Sig on msg.

1 $\mathsf{com} = (\mathsf{salt}, (\mathsf{com}_i)_{i \in [M]}) \leftarrow \mathcal{P}_1'(\phi_1, \ldots, \phi_N)$
2 $\mathsf{cha} \leftarrow \mathcal{H}(\mathsf{msg} || \phi_1 || \cdots || \phi_N || \mathsf{com})$
3 $\mathsf{rsp} \leftarrow \mathcal{P}_2'(A_I, I, \mathsf{cha})$
4 **return** $\mathsf{Sig} = (\mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$

Algorithm 6: Verification procedure

Input: The public key $\phi_0, \ldots, \phi_N \in \mathrm{ATF}(n, q)$. The signature $\mathsf{Sig} = (\mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$. The message msg. A hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.

Output: "Yes" if Sig is a valid signature for msg. "No" otherwise.

$\mathsf{com} \leftarrow \mathsf{RecoverCom}(\phi_0, \ldots, \phi_N, \mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$

if $\mathsf{accept} = \mathcal{V}_2'(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}) \wedge \mathsf{cha} = \mathcal{H}(\mathsf{msg}||\phi|| \cdots ||\phi_N||\mathsf{com})$ **then**

  return *Yes*

else

  return *No*

6 Linkable ring signature from ATFE

6.1 Tag

To construct a linkable OR sigma protocol, we add a tag $\tau_0 \in \mathrm{ATF}(n, q)$ associated with a group action $\bullet$ into the relation. The group action $\bullet$ on $\mathrm{ATF}(n, q)$ is defined as $\tau \bullet A := \tau \circ (A^t)^{-1}$. This tag τ_0 is used to track if some secret key is signed more than once. In addition, we restrict the initial public key ϕ_0 is sampled from an orbit $\mathcal{O}(\phi)$ with a trivial automorphism group. By the discussions in Section 3.4, a randomly sampled form ϕ_0 has a high probability to be in an orbit with the trivial automorphism group if we choose a proper parameter n and q, adding this restriction is reasonable. After adding the tag into the base OR sigma protocol, we can get a linkable OR sigma protocol shown in the Figure 4. Then we apply the same optimization methods in Section 5.2 to this protocol.

6.2 Security proof for linkable OR sigma protocol

To derive the security proof for linkable OR sigma protocol, we introduce an algorithm problem here and assume this problem is hard.

Definition 12 (PR-itATFE). *The pseudorandom inverse-transpose alternating trilinear form equivalence problem with* 2 *pair of forms asks to distinguish the following two distributions.*

The random distribution: 2 *pair of alternating trilinear forms* $(\phi_0, \phi_1), (\tau_0, \tau_1) : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$*, such that* $\phi_0, \phi_1, \tau_0, \tau_1 \in_R \mathrm{ATF}(n, q)$.

The pseudorandom distribution: K *alternating trilinear forms* $(\phi_0, \phi_1), (\tau_0, \tau_1) : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$*, such that: (1)* $\phi_0, \tau_0 \in_R \mathrm{ATF}(n, q)$*, and (2)* $\phi_1 := \phi_0 \circ A$ *and* $\tau_1 := \tau_0 \bullet A$*, where* $A \in_R \mathrm{GL}(n, q)$.

Note that a similar proposal in the context of code equivalence was proposed in [4].

$\mathcal{P}_1(\phi_1, \ldots, \phi_N, \tau)$

- $\mathsf{seed} \xleftarrow{\$} \{0,1\}^\lambda$
- $(B, \mathsf{bits}_1, \ldots, \mathsf{bits}_N) \leftarrow \mathsf{PRG}(\mathsf{seed})$
- $\tau' \leftarrow \tau \bullet B$
- **for** i from 1 to N **do**
  - $\psi_i \leftarrow \phi_i \circ B$
  - $\mathsf{C}_i \leftarrow \mathsf{Com}(\psi_i, \mathsf{bits}_i)$
- $(\mathsf{root}, \mathsf{tree}) \leftarrow \mathsf{MerkleTree}(\mathsf{C}_1, \ldots, \mathsf{C}_N)$
- $h \leftarrow \mathcal{H}_{\mathsf{Coll}}(\tau', \mathsf{root})$
- The prover $\mathcal{P}$ sends the commitment $\mathsf{com} \leftarrow h$ to the verifier $\mathcal{V}$

$\mathcal{V}_1(\mathsf{com})$

- $c \xleftarrow{\$} \{0,1\}$
- The verifier $\mathcal{V}$ sends the challenge $\mathsf{cha} \leftarrow c$ to the prover $\mathcal{P}$

$\mathcal{P}_2(A_I, I, \mathsf{cha})$

- $c \leftarrow \mathsf{cha}$
- **if** $c = 0$ **then**
  - $D \leftarrow BA_I$
  - $\mathsf{path} \leftarrow \mathsf{getMerklePath}(\mathsf{tree}, I)$
  - $\mathsf{rsp} \leftarrow (D, \mathsf{path}, \mathsf{bits}_I)$
- **else**
  - $\mathsf{rsp} \leftarrow \mathsf{seed}$
- The prover $\mathcal{P}$ sends the response rsp to the verifier $\mathcal{V}$

$\mathcal{V}_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, \phi_0, \phi_1, \ldots, \phi_N, \tau_0, \tau)$

- $(h, c) \leftarrow (\mathsf{com}, \mathsf{cha})$
- **if** $c = 0$ **then**
  - $(D, \mathsf{path}, \mathsf{bits}) \leftarrow \mathsf{rsp}$
  - $\tilde{\psi} \leftarrow \phi_0 \circ D$
  - $\tilde{\mathsf{C}} \leftarrow \mathsf{Com}(\tilde{\psi}, \mathsf{bits})$
- $\tilde{\tau}' \leftarrow \tau_0 \bullet D$
  - $\tilde{\mathsf{root}} \leftarrow \mathsf{ReconstructRoot}(\tilde{\mathsf{C}}, \mathsf{path})$
  - The verifier $\mathcal{V}$ outputs accept if $h = \mathcal{H}_{\mathsf{Coll}}(\tilde{\tau}', \tilde{\mathsf{root}})$, else outputs reject
- **else**
  - $\mathsf{seed} \leftarrow \mathsf{rsp}$
  - $\tilde{\mathsf{root}} \leftarrow \mathcal{P}_1((\phi_1, \ldots, \phi_N), \mathsf{seed})$
  - The verifier $\mathcal{V}$ outputs accept if $\tilde{\mathsf{root}} = \mathsf{root}$, else outputs reject

Fig. 4. Linkable OR sigma protocol.

Then we define the following relation

$$R = \left\{ ((\phi_0, \phi_1, \ldots, \phi_N, \tau_0, \tau), (A, I)) \;\middle|\; \begin{array}{c} A \in \mathrm{GL}(n,q), \phi_i \in \mathrm{ATF}(n,q) \\ I \in [N], \phi_I = \phi_0 \circ A \\ \tau \in \mathrm{ATF}(n,q), \tau = \tau_0 \bullet A_I \end{array} \right\},$$

and the relaxed relation

$$\tilde{R} = \left\{ ((\phi_0, \phi_1, \ldots, \phi_N, \tau_0, \tau), w) \;\middle|\; \begin{array}{rc} & A \in \mathrm{GL}(n,q), \phi_i \in \mathrm{ATF}(n,q) \\ & I \in [N], \phi_I = \phi_0 \circ A \\ w = (A, I) : & \tau \in \mathrm{ATF}(n,q), \tau = \tau_0 \bullet A_I \\ w = (x, x') : & \text{or } x \neq x', \\ & \mathcal{H}_{\mathsf{Coll}}(x) = \mathcal{H}_{\mathsf{Coll}}(x') \\ & \text{or } \mathsf{Com}(x) = \mathsf{Com}(x') \end{array} \right\}$$

for the relaxed special soundness.

Theorem 10. *The linkable OR sigma protocol shown in the Figure 4 after the optimization has correctness, high min-entropy, special zero-knowledge and relaxed special soundness.*

Proof. Let $G, S_1, S_2 \coloneqq \mathrm{GL}(n,q)$, $\mathcal{X}, \mathcal{T} \coloneqq \mathrm{ATF}(n,q)$, $D_{\mathcal{X}} \coloneqq \{\circ\}$, $D_{\mathcal{T}} \coloneqq \{\bullet\}$ and $\mathsf{Link}_{\mathsf{GA}}$ be the equivalent relation. Then assume the K-psATFE problem and $\mathsf{PR\text{-}itATFE}$ problem are hard, it's easy to see that $(G, \mathcal{X}, \mathcal{T}, S_1, S_2, D_{\mathcal{X}}, D_{\mathcal{X}}, \mathsf{Link}_{\mathsf{GA}})$ satisfise the properties (1), (2), (3) in the Definition 3.1 and (1), (2), (3) in the Definition 4.2 of [7]. For the property (5), we can derive this property by restricting the orbit of ϕ_0 has trivial automorphism. Finally, by the $\mathsf{PR\text{-}iATFE}$ assumption, we can have property (4) and (6). Therefore, we obtain an 1-admissible group action. By the Theorem 4.5 and Theorem 4.6 in [7], our OR sigma protocol is proved to have correctness, relaxed special soundness and honest-verifier zero-knowledge. □

6.3 Linkable ring signature

After applying the Fiat-Shamir transformation to the linkable OR sigma protocol, we obtain a linkable ring signature shown in Algorithm 7, 8, 9 and 10. The linkable ring signature is similar to the normal ring signature in addition with a link algorithm.

Remark 7. Since the linkable OR sigma protocol is proved to satisfy all conditions in Theorem 10, and by the Theorem 4.7 in [7], the linkable ring signature in Algorithm 7, 8, 9 and 10 has correctness, linkability, linkable anonymity and non-frameability.

Remark 8. The above security proof is derived from the rewinding technique, but its security reduction is non-tight due to the loss of *forking lemma*[21]. Beullens

Algorithm 7: Linkable key generation

Input: The variable number $n \in \mathbb{N}$, a prime power q, the ring size N.
Output: Public key: N alternating trilinear forms $\phi_0, \ldots, \phi_N \in \mathrm{ATF}(n, q)$.
Private key: N matrices $A_1, \ldots, A_N$ such that $\phi_i = \phi_0 \circ A_i$ for $i \in [N]$.

Randomly sample an alternating trilinear form ϕ_0, τ_0 from $\mathrm{ATF}(n, q)$.
Randomly sample N matrices $A_1, \ldots, A_N$ from $\mathrm{GL}(n, q)$.
For every $i \in [N]$, $\phi_i \leftarrow \phi_0 \circ A_i$.
return *Public key:* $\phi_0, \phi_1, \ldots, \phi_N$. *Private key:* $A_1, \ldots, A_N$.

Algorithm 8: Link procedure

Input: Two signature $\mathsf{Sig} = (\mathsf{salt}, \tau, \mathsf{cha}, \mathsf{rsp})$ and $\mathsf{Sig}' = (\mathsf{salt}', \tau', \mathsf{cha}', \mathsf{rsp}')$.
Output: "Yes" if two signatures are produced by a same secret key. "No" otherwise.

if $\tau = \tau'$ **then**
  return *Yes*
else
  return *No*

Algorithm 9: Linkable signing procedure

Input: The public key: $\phi_0, \ldots, \phi_N$. The private key: A_I. The security parameter λ. The message msg. The commitment scheme $\mathsf{Com} : \{0,1\}^* \to \{0,1\}^\lambda$. A hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.
Output: The signature Sig on msg.

$\tau \leftarrow \tau_0 \bullet A_I$
$\mathsf{com} = (\mathsf{salt}, (\mathsf{com}_i)_{i \in [M]}) \leftarrow \mathcal{P}_1'(\phi_0, \phi_1, \ldots, \phi_N, \tau)$
$\mathsf{cha} \leftarrow \mathcal{H}(\mathsf{msg} || \phi_1 || \cdots || \phi_N || \tau || \mathsf{com})$
$\mathsf{rsp} \leftarrow \mathcal{P}_2'(A_I, I, \mathsf{cha})$
return $\mathsf{Sig} = (\mathsf{salt}, \tau, \mathsf{cha}, \mathsf{rsp})$

Algorithm 10: Linkable verification procedure

Input: The public key $\phi_0, \ldots, \phi_N \in \mathrm{ATF}(n, q)$. The signature $\mathsf{Sig} = (\mathsf{salt}, \tau, \mathsf{cha}, \mathsf{rsp})$. The message msg. A hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.
Output: "Yes" if Sig is a valid signature for msg. "No" otherwise.

$\mathsf{com} \leftarrow \mathsf{RecoverCom}(\phi_0, \ldots, \phi_N, \tau, \mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$
if $\mathsf{accept} = \mathcal{V}_2'(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}) \wedge \mathsf{cha} = \mathcal{H}(\mathsf{msg} || \phi || \cdots || \phi_N || \tau || \mathsf{com})$ **then**
  return *Yes*
else
  return *No*

et.al. proposed a new property called online extractability [6], which is used to obtain a almost tight security reduction of ring signature.Further they use some techniques including the Katz-Wang technique [28] to obtain the tight security. Since our ring signature is following their construction, if append above property and techniques to our ring signature, we can get a tight security reduction as well.

References

1. M. Abdalla, P. Fouque, V. Lyubashevsky, and M. Tibouchi. Tightly-secure signatures from lossy identification schemes. In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 572–590. Springer, 2012.
2. N. Alamati, L. D. Feo, H. Montgomery, and S. Patranabis. Cryptographic group actions and applications. In S. Moriai and H. Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 411–439. Springer, 2020.
3. L. Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 684–697, 2016.
4. A. Barenghi, J.-F. Biasse, T. Ngo, E. Persichetti, and P. Santini. Advanced signature functionalities from the code equivalence problem. *International Journal of Computer Mathematics: Computer Systems Theory*, 7(2):112–128, 2022.
5. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
6. W. Beullens, S. Dobson, S. Katsumata, Y.-F. Lai, and F. Pintore. Group signatures and more from isogenies and lattices: Generic, simple, and efficient. In O. Dunkelman and S. Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 95–126, Cham, 2022. Springer International Publishing.
7. W. Beullens, S. Katsumata, and F. Pintore. Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In S. Moriai and H. Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 464–492. Springer, 2020.
8. D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.
9. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

10. C. Bouillaguet. *Etudes d'hypotheses algorithmiques et attaques de primitives cryptographiques*. PhD thesis, PhD thesis, Université Paris-Diderot–École Normale Supérieure, 2011.
11. C. Bouillaguet, J.-C. Faugère, P.-A. Fouque, and L. Perret. Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In *International Workshop on Public Key Cryptography*, pages 473–493. Springer, 2011.
12. C. Bouillaguet, P. Fouque, and A. Véber. Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In *Advances in Cryptology - EUROCRYPT 2013*, pages 211–227, 2013.
13. G. Brassard and M. Yung. One-way group actions. In *Advances in Cryptology - CRYPTO 1990*, pages 94–107, 1990.
14. P. A. Brooksbank, Y. Li, Y. Qiao, and J. B. Wilson. Improved algorithms for alternating matrix space isometry: from theory to practice. In *28th Annual European Symposium on Algorithms, ESA 2020*, page to appear, 2020.
15. A. M. Cohen and A. G. Helminck. Trilinear alternating forms on a vector space of dimension 7. *Communications in algebra*, 16(1):1–25, 1988.
16. J. M. Couveignes. Hard homogeneous spaces. *IACR Cryptology ePrint Archive*, 2006.
17. I. Dinur and N. Nadler. Multi-target attacks on the picnic signature scheme and related protocols. In Y. Ishai and V. Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 699–727. Springer, 2019.
18. J. Don, S. Fehr, C. Majenz, and C. Schaffner. Security of the fiat-shamir transformation in the quantum random-oracle model. In A. Boldyreva and D. Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 356–383. Springer, 2019.
19. A. El Kaafarani, S. Katsumata, and F. Pintore. Lossy CSI-FiSh: Efficient Signature Scheme with Tight Reduction to Decisional CSIDH-512. In *Public-Key Cryptography - PKC 2020*, volume 12111 of *Lecture Notes in Computer Science*, pages 157–186. Springer, 2020.
20. J. Faugère and L. Perret. Polynomial equivalence problems: Algorithmic and theoretical aspects. In *Advances in Cryptology - EUROCRYPT 2006*, pages 30–47, 2006.
21. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology – CRYPTO 1986*, pages 186–194, 1986.
22. O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991.
23. J. A. Grochow and Y. Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness. In J. R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*, volume 185 of *LIPIcs*, pages 31:1–31:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

24. J. A. Grochow, Y. Qiao, and G. Tang. Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. In *The 38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021*, page to appear, 2021. arXiv:2012.01085.
25. J. Hora and P. Pudlák. Classification of 8-dimensional trilinear alternating forms over gf (2). *Communications in Algebra*, 43(8):3459–3471, 2015.
26. J. Hora and P. Pudlák. Classification of 9-dimensional trilinear alternating forms over gf (2). *Finite Fields and Their Applications*, 70:101788, 2021.
27. Z. Ji, Y. Qiao, F. Song, and A. Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In D. Hofheinz and A. Rosen, editors, *Theory of Cryptography - 17th International Conference, TCC 2019*, volume 11891, pages 251–281. Springer, 2019.
28. J. Katz and N. Wang. Efficiency improvements for signature schemes with tight security reductions. In *Proceedings of the 10th ACM conference on Computer and communications security*, pages 155–164, 2003.
29. E. Kiltz, V. Lyubashevsky, and C. Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In *Advances in Cryptology – EUROCRYPT 2018*, pages 552–586. Springer, 2018.
30. Y. Li and Y. Qiao. Linear algebraic analogues of the graph isomorphism problem and the Erdős–Rényi model. In C. Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 463–474. IEEE Computer Society, 2017.
31. J. K. Liu and D. S. Wong. Linkable ring signatures: Security models and new schemes. In O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan, editors, *Computational Science and Its Applications - ICCSA 2005, International Conference, Singapore, May 9-12, 2005, Proceedings, Part II*, volume 3481 of *Lecture Notes in Computer Science*, pages 614–623. Springer, 2005.
32. Q. Liu and M. Zhandry. Revisiting post-quantum fiat-shamir. In A. Boldyreva and D. Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 326–355. Springer, 2019.
33. B. D. McKay. Practical graph isomorphism. *Congr. Numer.*, pages 45–87, 1980.
34. B. D. McKay and A. Piperno. Practical graph isomorphism, II. *J. Symb. Comput.*, 60:94–112, 2014.
35. N. Midoune and L. Noui. Trilinear alternating forms on a vector space of dimension 8 over a finite field. *Linear and Multilinear Algebra*, 61(1):15–21, 2013.
36. J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology – EUROCRYPT 1996*, pages 33–48, 1996.
37. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of cryptology*, 13(3):361–396, 2000.
38. A. Stolbunov. *Cryptographic schemes based on isogenies.* PhD thesis, Norwegian University of Science and Technology, 2012.
39. S. Sun, M. H. Au, J. K. Liu, and T. H. Yuen. Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In S. N. Foley, D. Gollmann, and E. Snekkenes, editors, *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*, volume 10493 of *Lecture Notes in Computer Science*, pages 456–474. Springer, 2017.

40. G. Tang, D. H. Duong, A. Joux, T. Plantard, Y. Qiao, and W. Susilo. Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In O. Dunkelman and S. Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 582–612. Springer, 2022.
41. P. P. Tsang and V. K. Wei. Short linkable ring signatures for e-voting, e-cash and attestation. In R. H. Deng, F. Bao, H. Pang, and J. Zhou, editors, *Information Security Practice and Experience, First International Conference, ISPEC 2005, Singapore, April 11-14, 2005, Proceedings*, volume 3439 of *Lecture Notes in Computer Science*, pages 48–60. Springer, 2005.
42. D. Unruh. Quantum proofs of knowledge. In *Advances in Cryptology – Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, April 2012.
43. D. Unruh. Computationally binding quantum commitments. In *Advances in Cryptology – Eurocrypt 2016*, pages 497–527. Springer, 2016.
44. D. Unruh. Post-quantum security of fiat-shamir. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 65–95. Springer, 2017.
45. T. Yamakawa and M. Zhandry. Classical vs quantum random oracles. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 568–597. Springer, 2021.
46. M. Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In A. Boldyreva and D. Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 239–268, Cham, 2019. Springer International Publishing.