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

Markus Bläser[1], Zhili Chen[2], Dung Hoang Duong[3], Antoine Joux[4], Tuong Nguyen[3], Thomas Plantard[5], Youming Qiao[2], Willy Susilo[3], and Gang Tang[2]

[1] Department of Computer Science, Saarland University, Saarland Informatics Campus, Saarbrücken, Germany.
mblaeser@cs.uni-saarland.de

[2] 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

[3] 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

[4] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany.
joux@cispa.de

[5] Nokia Bell Labs, Murray Hill, New Jersey, United States.
thomas.plantard@nokia-bell-labs.com

Abstract. At Eurocrypt 2022, Tang et al. proposed a practical digital signature scheme in the context of post-quantum cryptography. Their construction is based on the assumed hardness of the alternating trilinear form equivalence problem (ATFE), the Goldreich-Micali-Widgerson (GMW) zero-knowledge protocol for graph isomorphisms, and the Fiat-Shamir (FS) transformation. We refer to that scheme as the ATFE-GMW-FS scheme. In this paper, we revisit and investigate several aspects of the ATFE-GMW-FS scheme. First, we provide an evidence that the ATFE-GMW-FS scheme is secure in the quantum random oracle model (QROM), which was left as an open problem, in two approaches based on the perfect unique response property and lossy identification schemes, respectively. Secondly, we further enable (linkable) ring signature constructions based on the ATFE-GMW-FS scheme, inspired by a recent result of Beullens, Katsumata and Pintore at Asiacrypt 2020 in the context of isogeny-based cryptography. Our results on QROM security and ring signatures apply more broadly to signature schemes based on isomorphism problems through the GMW-FS approach. Finally, we provide optimization and implementation approaches for our ring signature schemes. Preliminary experiments suggest that our scheme is competitive among existing post-quantum ring signatures.

1 Introduction

In [26], Goldreich, Micali and Wigderson described a zero-knowledge proof protocol for graph isomorphism (GI). The Fiat-Shamir transformation FS [25] 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 [39,40], not to mention Babai's quasipolynomial-time algorithm [3].

Fortunately, the Goldreich-Micali-Wigderson (GMW) 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 [42]. In isogeny-based cryptography, Couveignes proposed the use of class group actions on elliptic curves [18]. Both proposal have their own merits and issues; interested readers are referred to [47] for more details.

The recent advances in complexity theory [27,28] and algorithms [35,15,28] reveal a much clearer picture on the complexity of isomorphism problems of algebraic structures. Based on these advances, Tang et al. [47] 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 [47] as *the ATFE-GMW-FS scheme*.

The main message of [47] is that ATFE-GMW-FS scheme could serve as an alternative candidate for the NIST's post-quantum digital signatures. This is backed by 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 (QROM), and *ring signature* construction. For both aspects, we obtain positive results that support the ATFE-GMW-FS scheme.

1.1 Our Contributions

Security in the quantum random oracle model. The quantum random oracle model (QROM) was proposed by Boneh et al. [9] in 2011 and has received considerable attention since then. There are certain inherent difficulties to prove security in the QROM model, such as the adaptive programmability and rewinding [9]. Indeed, the QROM security of the Fiat-Shamir transformation was only recently shown after a series of works [51,34,37,21]. The QROM security of the ATFE-GMW-FS scheme was briefly discussed in [47] 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 [51,34,37,21]. 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 [47], 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 [31,2]. 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 [47], some arguments were provided to support that it is.

In particular, we do not need to modify the original ATFE-GMW-FS scheme in [47] to attain the security in QROM, i.e., as opposed to the context of isogeny-based cryptography, e.g., [22]. We will discuss more about this shortly.

Ring signature schemes. Ring signature, introduced by Rivest, Shamir and Tauman [44], 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 [36] 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 [46]) and e-voting [48].

Recently at Asiacrypt 2020, Beullens, Katsumata and Pintore [8] 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 [8], 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 further implement the ring signature protocol. Preliminary experiment results suggest that it's more balanced than Calamari and Falafl in terms of signature size and signing time; see Section 6.3 and Table 3 for the details.

Updated parameters, improved implementation, and ring signature protocol. Recently, Beullens [6] presented new algorithms for ATFE which broke some of the parameters proposed in [47] and reduced the security levels for other parameters. We carefully analyze Beullens' methods and propose new parameter sets based on this study. We then improve the implementations from [47], and implement the ring signature scheme described above.

Comparison with other ring signature schemes. Since we use the construction in [8], the signature size of our schemes also only depend on $\log R$, where R denotes the ring size. We see that our signature size can be estimated as $0.4 \log R +$ 8.5KB, while the signature sizes of Calamari and Falafl in [8] are estimated to be $\log R + 2.5$KB and $0.5 \log R + 28.5$KB respectively. For ring size $R = 8$, our signing time is 96ms which is very close to Falafl's 90ms and much smaller than Calamari's 79s. Meanwhile, our ring signature size is 9.7KB, while Falafl and Calamari have the signature size of 30KB and 5.4KB respectively. RAPTOR [38], and DualRing-LB [53] have shorter signature sizes than ours when the ring size is small. However, their sizes are linearly dependent on the number of ring users; therefore, the size significantly increases when the number of participants rises. We also provide another set of parameters that can reach NIST level 5 security in Table 1 for comparison. Note that the signing time is measured on 2.4 GHz Quad-Core Intel Core i5.

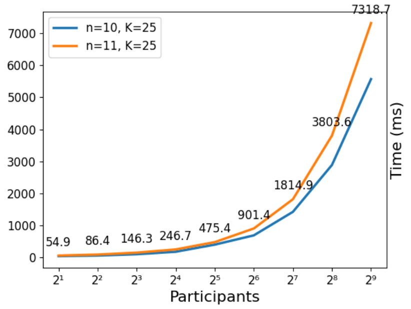

Fig. 1. Signature generation time

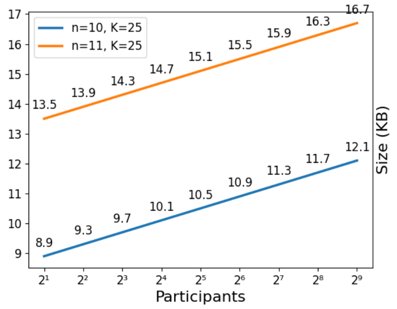

Fig. 2. Signature size

	R					Hardness	Secuirty
	2^1	2^3	2^6	2^{12}	2^{21}	assumption	level
KKW [32]	/	/	250	456	/	LowMC	NIST 5
MatRiCT [23]	/	18	19	59	/	MSIS, MLWE	NIST 1
RAPTOR [38]	2.5	10	81	5161	/	NTRU	100 bits
Calamari [8]	3.5	5.4	8.2	14	23	CSIDH-512	*
Falafl [8]	29	30	32	35	39	MSIS, MLWE	NIST 1
Falafl for 2 [8]	49	50	52	55	59	MSIS, MLWE	NIST 2
DualRing-LB [53]	/	4.6	6	106.6	/	MSIS, MLWE	NIST 1
Ours	8.9	9.7	10.9	13.2	16.9	ATFE	NIST 1
	18.7	21.9	26.7	36.3	50.7	ATFE	NIST 5

Table 1. Comparison of the signature size between our schemes and others

1.2 Discussions

Discussions on QROM security. Though tight QROM security proofs of Fiat-Shamir can be obtained by constructing lossy key generation [34], the lossy assumption seems very strong, so a natural question is to relax this assumption. In a pair of breakthrough papers [37] and [21], 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 [49], 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 offer experimental data to support it; see Section 3.4.

There is one further approach which could avoid analysing automorphism groups mathematically. In [37,21], a property called *quantum unique response* in [21] or collapsing sigma protocol in [37] is introduced, generalising the *collapsingness* which introduced by Unruh [50] 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 [22,8]. Still, there are substantial differences, so we compare our results with those in [22,8].

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 [22] is the diagonal action of the class group on two elliptic curves following [45]. One reason is that for the pseudorandom group action assumption [31] (cf. Definition 7) 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 signatures essentially follows the designs of their counterparts proposed by Beullens, Katsumata and Pintore [8]. 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 [47].

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 [14,18,31,2] 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 rephrase most of the results in this paper in the language of group actions. However, we choose to use the language of ATFE directly because it is more concrete and allows us to directly use the results and parameters from [47].

Concurrent Work. Very recently, D'Alconzo and Gangemi [19] obtained a ring signature from ATFE by also following the construction in [8]. The comparison is summarized as follows. First of all, D'Alconzo and Gangemi used the fixed weight challenges, specially, they encoded the challenge space. For the challenge space $C_{M,K}$, they enumerate the strings inside and encode them into integers to record the position in this order to send instead of sending a string. In this way the cost for challenge is $\log_2 \binom{M}{K}$. Our work considers the positions where the challenge is 0 for a string randomly sampled from the challenge space. Thus the cost is $K \log_2(M)$ for the challenge space $C_{M,K}$. However, we consider the different challenge space, that is, to divide M into K parts, and there exists one cha $= 0$ in each part. In this case, we have the cost $K \log_2(\frac{M}{K})$. Secondly, D'Alconzo and Gangemi defined tag associated to a group action $\tau \bullet A = \tau \circ A^{-1}$ while our associated group action is $\tau \bullet A = \tau \circ (A^t)^{-1}$. Last but not least, D'Alconzo and Gangemi do not provide implementations while in our work, we implemented the (linkable) ring signature and compared with other protocols.

2 Preliminaries

2.1 Notations

We collect some basic notation in this subsection. We use $\mathbb{F}_q$ to denote the finite field with q elements. 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 $\{1, \dots, k\}$.

2.2 Σ-protocol and digital signatures

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 $\mathcal{R}$ 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 anything 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 $a \leftarrow \mathcal{P}_1(x, w)$ 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 $r \leftarrow \mathcal{P}_2(x, w, a, c)$ 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.*

We assume the readers are familiar with the following properties of Σ-protocols: identification from Σ-protocol, completeness, post-quantum 2-soundness, honest verifier zero knowledge (HVZK), α-bit min-entropy, perfect and computational unique response, and commitment recoverable. For readers' convenience we collect them in Appendix A.1.

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.
- $\mathsf{Sign}(\mathsf{sk}, M)$*: 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 for all message M and $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, M)$, we always have that $\mathsf{Ver}(\mathsf{pk}, M, \sigma) = 1$.

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 choices, the probability that $\mathcal{A}$ can sign a message that he has not seen its signatures 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.

Fiat-Shamir transformation. The Fiat-Shamir transformation [25] 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 $\mathsf{pk} := \mathsf{ID.pk}$.
- $\mathsf{Sign}(\mathsf{sk}, M)$: 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 $H : \{0,1\}^* \to \mathsf{ChSet}$ 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 ([43]). *If an identification protocol is HVZK and satisfies special soundness, then $\mathsf{FS}[\mathsf{ID}]$ has $\mathsf{EUF\text{-}CMA}$ security in the ROM model.*

2.3 Ring signatures

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,*

- $\mathsf{RS.SetUp}(1^\lambda)$*: Given a security parameter λ, this algorithm outputs the corresponding public parameters* pp.
- $\mathsf{RS.KeyGen}(\mathsf{pp})$*: This algorithm generates, for a user i, a pair $(\mathsf{vk}_i, \mathsf{sk}_i)$ of the secret key sk_i and public key (verification key) vk_i.*
- $\mathsf{RS.Sign}(\mathsf{sk}_i, \mathsf{R}, \mathsf{M})$*: Given the secret key sk_i, a list of public keys $\mathsf{R} = \{\mathsf{vk}_1, \ldots, \mathsf{vk}_N\}$ 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 output 1 if this signature is valid or 0 otherwise.*

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

Correctness: A ring signature Π_{RS} is said to be correct if for any security parameter λ, polynomial $N = \mathsf{poly}(\lambda)$, any message M, $\mathsf{pp} \leftarrow \mathsf{RS.SetUp}(1^\lambda)$, $(\mathsf{vk}_1, \mathsf{sk}_1), \ldots, (\mathsf{vk}_N, \mathsf{sk}_N) \leftarrow \mathsf{RS.KeyGen}(\mathsf{pp})$, $\sigma \leftarrow \mathsf{RS.Sign}(\mathsf{sk}_i, \mathsf{R}, \mathsf{M})$ with $\mathsf{R} := \{\mathsf{vk}_1, \ldots, \mathsf{vk}_N\}$, it always holds that $\mathsf{RS.Verify}(\mathsf{R}, \mathsf{M}, \sigma) = 1$.
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 runs $\mathsf{pp} \leftarrow \mathsf{RS.SetUp}(1^\lambda)$ and generates key pairs $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{RS.KeyGen}(\mathsf{pp})$ for all $i \in [N]$ and samples $b \xleftarrow{\$} \{0,1\}$. Then it sends pp and the secret keys $\{\mathsf{sk}_i\}_{i\in[N]}$ to $\mathcal{A}$.

(2) $\mathcal{A}$ computes a challenge $(\mathsf{R}, \mathsf{M}, i_0, i_1)$, where R contains vk_{i_0} and vk_{i_1}, and sends it to the challenger.
(3) The challenger runs $\mathsf{RS.Sign}(\mathsf{sk}_{i_b}, \mathsf{R}, \mathsf{M}) \rightarrow \sigma$ and sends σ to $\mathcal{A}$.
(4) $\mathcal{A}$ outputs b'. If $b = b'$, then we say that $\mathcal{A}$ wins this game.

The advantage of $\mathcal{A}$ is

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

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 runs $\mathsf{pp} \leftarrow \mathsf{RS.SetUp}(1^\lambda)$ and generates key pairs $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{RS.KeyGen}(\mathsf{pp})$ for all $i \in [N]$. 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 $\mathsf{R}' \subseteq \mathsf{VK} \setminus \mathsf{CL}$, $(\cdot, \mathsf{R}', \mathsf{M}') \notin \mathsf{SL}$, and $\mathsf{RS.Verify}(\mathsf{R}', \mathsf{M}', \sigma') = 1$.

2.4 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 [47, Sec. 2.1 and 6.2].

Let $\mathbb{F}_q$ be the finite field of order q. A trilinear form $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ 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 $\phi, \psi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$, 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 [47].

Definition 5 **(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 $\phi_0, \phi_1, \dots, \phi_{K-1} : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, 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 $i, j \in \{0, 1, \dots, K-1\}$, $i \neq j$, such that $\phi_i = \phi_j \circ A$.*

In Section 3, we also need the following variation of Definition 5 by restricting to a particular orbit.

Definition 6 **(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 $\phi_0, \phi_1, \dots, \phi_{K-1} : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, such that for $i \in \{0, 1, \dots, K-1\}$, $\phi_i := \phi \circ A_i$, where $A_i \in_R \mathrm{GL}(n, q)$.*

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

The second algorithmic problem is obtained by applying the pseudorandom group action notion [31] to K-psATFE-RO.

Definition 7 **(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 $\phi_0, \phi_1, \dots, \phi_{K-1} : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, such that every $\phi_i \in_R \mathrm{ATF}(n, q)$.*

The pseudorandom distribution: *K alternating trilinear forms $\phi_0, \phi_1, \dots, \phi_{K-1} : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, 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.

2.5 The ATFE-GMW-FS scheme

As mentioned in Section 1, the ATFE-GMW-FS scheme in [47] 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 5.

For our purposes in this paper, the key is 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 [47, 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 $\phi_0, \phi_1, \ldots, \phi_{K-1}$ 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 3; here the Sign function is definied by $\mathsf{Sign}(c) = 0$ if $c = 0$ and $\mathsf{Sign}(c) = 1$ otherwise. The protocol needs to be repeated t times for appropriate t to attain the required security level.

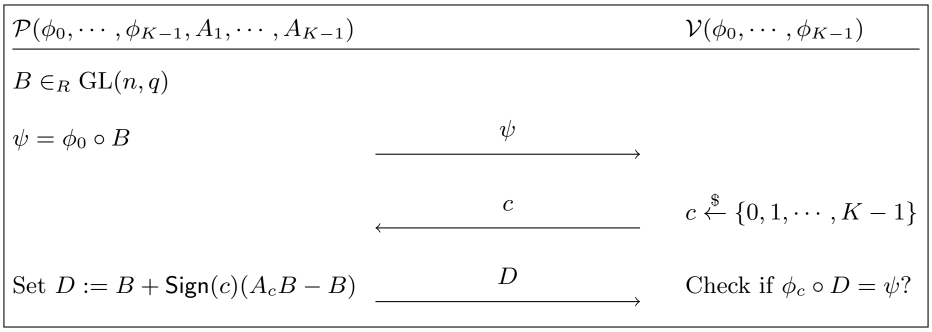
$\mathcal{P}(\phi_0, \cdots, \phi_{K-1}, A_1, \cdots, A_{K-1})$
$\mathcal{V}(\phi_0, \cdots, \phi_{K-1})$
$B \in_R \mathrm{GL}(n, q)$
$\psi = \phi_0 \circ B$
ψ
c
$c \overset{\$}{\leftarrow} \{0, 1, \cdots, K-1\}$
Set $D := B + \mathsf{Sign}(c)(A_c B - B)$
D
Check if $\phi_c \circ D = \psi$?

Fig. 3. The ATFE-GMW protocol.

It is known that ATFE-GMW protocol in Figure 3 has the following properties (see e.g. [47]): completeness, post-quantum 2-soundness, HVZK, min-entropy, and commitment recoverable. We provide some proof sketches for completeness in Appendix A.2.

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 same proof and Assumption 2, ATFE-GMW-$\mathcal{O}(\phi)$ protocol also has the above 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 [47].

3.1 Preliminaries on QROM

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 modeled as by a random oracle. However, ROM is insufficient when considering quantum adversaries, which leads to the proposal of the *quantum* ROM (QROM) [9]. One main reason comes from that quantum adversaries can make queries at 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 [9,52] .

Recently, thanks to a pair of breakthrough papers [21,37], 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 [49]. With this important property and some additional properties stated in Section 2.5, we can prove the security of the ATFE-GMW 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 2.5 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* $\text{Aut}(\phi)$ *is trivial.*

Proof. In the one direction, assume that $\text{Aut}(\phi)$ is trivial. If there are two valid transcripts (ψ, c, D) and (ψ, c, D') for the protocol in Figure 3. Then we have $\phi_c \circ D = \phi_c \circ D'$. It implies that $E \in \text{Aut}(\phi)$ 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 $\text{Aut}(\phi)$ 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 $\phi \in_R \text{ATF}(n, q)$ is trivial with a high probability.

Remark 2. Although perfect unique response for ATFE-GMW protocol can not be proved rigorously, statistical unique response[6] 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 8. *The alternating trilinear form automorphism problem is the following.*

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

Lemma 2 (Computationally Unique Response). *The ATFE-GMW protocol in Figure 3 supports computationally unique response iff no poly-time quantum algorithm can solve* ATF *automorphism problem in Definition 8 with a non-negligible probability.*

[6] 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 $x = \{\phi_0, \dots, \phi_{K-1}\} \subseteq \mathrm{ATF}(n,q)$, 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 $x = \{\phi_0, \dots, \phi_{K-1}\} \subseteq \mathrm{ATF}(n,q)$, 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 $\{\phi_0, \dots, \phi_{K-1}\} \subseteq \mathrm{ATF}(n,q)$, $\mathcal{A}$ can compute two transcripts (ψ, c, D) and (ψ, c, ED) with a non-negligible probability. □

Remark 3. 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

In this section, we provide a security proof in QROM for ATFE-GMW-FS-$\mathcal{O}(\phi)$ signature via results in [37]. There is another proof in Appendix E, which mainly uses the results from [21].

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 repetitions 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 K-psATFE-$\mathcal{O}(\phi)$ problem such that,*

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

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-$\mathcal{O}(\phi)$ 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 9. *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.*

$$\Pr\left[\mathcal{V}.\mathsf{Ver}(\mathsf{pk}, a, c, r) = 1 \mid a \leftarrow \mathcal{A}_0^{\mathcal{O}_{\mathcal{P},\mathcal{V}}}(\mathsf{pk}) \wedge c \xleftarrow{\$} \{0,1\}^\lambda \wedge r \leftarrow \mathcal{A}_1^{\mathcal{O}_{\mathcal{P},\mathcal{V}}}(\mathsf{pk}, a, c)\right] \leq \mathsf{negl}(\lambda).$$

Liu and Zhandry show that post-quantum identification soundness can be satisfied if sigma protocol has weakly collapsing property and extra properties [37, Theorem 1]. Since the perfect unique response is a stronger property than weakly collapsing property, we can state the result in [37] as follows.

Theorem 3 ([37]). *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,*

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

Theorem 4. *The t repetitions of ATFE-GMW-$\mathcal{O}(\phi)$ Σ-protocol in Figure 3 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-psATFE-$\mathcal{O}(\phi)$ problem such that,*

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

Proof. By the Assumption 3 and the Lemma 1, the Σ-protocol in Figure 3 has perfect unique response. We also proved that it has completeness, 2-soundness, and HVZK in the Section 2.5. Since the The t repetitions of Σ-protocol in Figure 3 has an exponentially large challenge space, we complete the proof using the result of Theorem 3. □

Security of ATFE-GMW-FS-$\mathcal{O}(\phi)$ signature. Liu and Zhandry [37, 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 [54]. 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 ([37], Theorem 1). *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,*

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

Theorem 6. *If the t repetitions of $\mathsf{ATFE\text{-}GMW\text{-}}\mathcal{O}(\phi)$ protocol showed in Figure 3 has post-quantum ID soundness, then the corresponding Fiat-Shamir signature has $\mathsf{EUF\text{-}CMA}$ security that for any polynomial-time quantum adversary $\mathcal{A}$ querying the quantum random oracle Q_H times against $\mathsf{EUF\text{-}CMA}$ security of $\mathsf{ATFE\text{-}GMW\text{-}FS\text{-}}\mathcal{O}(\phi)$ signature, there are quantum adversary $\mathcal{B}$ against ID-soundness of $\mathsf{ATFE\text{-}GMW\text{-}}\mathcal{O}(\phi)$ 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 repetitions of Σ-protocol showed in Figure 3 has post-quantum ID soundness. We proved that it has $\log_2(|\mathcal{O}|)$ bits min-entropy in Section 2.5, and $|\mathcal{O}| = 2^{\Omega(\lambda)}$. Now we complete the proof utilizing the result of Theorem 5. □

3.4 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 [47], (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. For example, our experiments gave that, for $q = 2$ and $n = 10, 11$, all 100 sampled random alternating trilinear forms return trivial automorphism groups, and for $q = 3$ and $n = 10, 11$, all 10 samples return trivial automorphism groups. Due to the lack of space, we put more detailed discussions in Appendix D.

4 Tightly Secure Signature from ATFE in QROM

4.1 Definition

In this section, we recall the definition of lossy identification protocol [1,22] and a security result of its associated Fiat-Shamir signature in QROM from [34].

Definition 10. *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 [34,37,21]. The following is from [22, Theorem 2.5] which is derived from [34, 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 3. Here, we consider a relation $\mathcal{R}$ consisting of statement-witness pairs (x, w) with $x = \{\phi_0, \phi_1, \dots, \phi_{K-1}\} \subseteq \mathrm{ATF}(n, q)$ and $w = \{A_1, \dots, A_{K-1}\} \subseteq \mathrm{GL}(n, q)$, where $\phi_0 \circ A_i^{-1} = \phi_i$ for each $i \in [K - 1]$.

The lossy identification scheme for the relation $\mathcal{R}$ defined as above with challenge space $\{0, 1, \cdots, K-1\}$ consists of five algorithms $(\mathsf{IGen}, \mathsf{LossyGen}, \mathcal{P}_1, \mathcal{P}_2, \mathcal{V})$ 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 $D = B + \mathsf{Sign}(c)(A_c B - B)$.
- 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 3, 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 solve the K-PR-psATFE-RO problem defined in Definition 7 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 [22, 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 3, 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 4. 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 [25] 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 [47]) 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 [47] with the use of a secure PRF to derandomize the signature generation, as similar in [22].

```
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 $\phi_i$'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 $\phi_0 : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$.
  Randomly sample invertible matrices $A_1, \cdots, A_{K-1} \in \mathrm{GL}(n, q)$.
  Compute $\phi_i = \phi_0 \circ A_i^{-1}$ for $i = 1, \cdots, K-1$.
  $E \leftarrow \mathcal{K}$                                   #Sample a key for PRF
  return Public key: $\phi_0, \phi_1, \cdots, \phi_{K-1}$. Private Key: $A_1, \cdots, A_{K-1}, E$
```

```
Algorithm 2: Signature generation.
  Input: Public key pk, secret key sk and a message $M$.
  Output: A signature $\sigma$.
  for $k \in \{1, \cdots, t\}$ do
      $B_k \in_R \mathrm{GL}(n, q)$      #Derive randomness using PRF$(E, M\|k)$
      $\psi_k := \phi_0 \circ B_k$
  end
  $(c_1, \cdots, c_t) = H(\psi_1\| \cdots \|\psi_t\|M)$
  for $k \in \{1, \cdots, t\}$ do
      $D_k := B + \mathsf{Sign}(c_k)(A_{c_k}B - B)$
  end
  $\sigma := (c_1, \cdots, c_t, D_1, \cdots, D_t)$
  return $\sigma$
```

```
Algorithm 3: Verification.
  Input: Public key pk, a message $M$ and a signature $\sigma$.
  Output: 0 or 1.
  Parse $\sigma$ as $(c_1, \cdots, c_t, D_1, \cdots, D_t)$
  for $k \in \{1, \cdots, t\}$ do
      Compute $\psi_k = \phi_0 \circ D_k$
  end
  $(c'_1, \cdots, c'_t) = H(\psi_1\| \cdots \|\psi_t\|M)$
  if $(c'_1, \cdots, c'_t) == (c_1, \cdots, c_t)$ then
      return 1
  else
      return 0
  end
```

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

against the PRF *such that*

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

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 [21, 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 5. 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 [8] 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 4. We will first describe the base OR-Sigma protocol from ATFE in Section 5.1 and its optimization in Section 5.2. The security proof is deferred to the Appendix A.3.

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 4, 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[7] 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.

[7] Note that the Merkle tree used here is slightly modified. It is index-hiding Merkle tree, please see [8, Section 2.6]

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 $\widetilde{\mathsf{root}}$ by path and $\tilde{\mathsf{C}}$. Finally the verifier checks whether $\widetilde{\mathsf{root}} = \mathsf{root}$.
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.

```
$\mathcal{P}_1(\phi_1, \ldots, \phi_N)$
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
  $\psi_i \leftarrow \phi_i \circ B$
  $\mathsf{C}_i \leftarrow \mathsf{Com}(\psi_i, \mathsf{bits}_i)$
$(\mathsf{root}, \mathsf{tree}) \leftarrow \mathsf{MerkleTree}(\mathsf{C}_1, \ldots, \mathsf{C}_N)$
$\mathsf{com} \leftarrow \mathsf{root}$
$\mathcal{P}$ sends com to $\mathcal{V}$
```

```
$\mathcal{V}_1(\mathsf{com})$
$c \xleftarrow{\$} \{0,1\}$
$\mathsf{cha} \leftarrow c$
$\mathcal{V}$ sends cha to $\mathcal{P}$
```

```
$\mathcal{P}_2(A_I, I, \mathsf{cha})$
$c \leftarrow \mathsf{cha}$
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
  $\mathsf{rsp} \leftarrow \mathsf{seed}$
$\mathcal{P}$ sends rsp to $\mathcal{V}$
```

```
$\mathcal{V}_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, \phi_0, \phi_1, \ldots, \phi_N)$
$(\mathsf{root}, c) \leftarrow (\mathsf{com}, \mathsf{cha})$
if $c = 0$ then
  $(D, \mathsf{path}, \mathsf{bits}) \leftarrow \mathsf{rsp}$
  $\tilde{\psi} \leftarrow \phi_0 \circ D$
  $\tilde{\mathsf{C}} \leftarrow \mathsf{Com}(\tilde{\psi}, \mathsf{bits})$
  $\widetilde{\mathsf{root}} \leftarrow \mathsf{ReconstructRoot}(\tilde{\mathsf{C}}, \mathsf{path})$
  if $\widetilde{\mathsf{root}} = \mathsf{root}$ then
    $\mathcal{V}$ outputs accept
  else
    $\mathcal{V}$ outputs reject
else
  $\mathsf{seed} \leftarrow \mathsf{rsp}$
  $\widetilde{\mathsf{root}} \leftarrow \mathcal{P}_1((\phi_1, \ldots, \phi_N), \mathsf{seed})$
  if $\widetilde{\mathsf{root}} = \mathsf{root}$ then
    $\mathcal{V}$ outputs accept
  else
    $\mathcal{V}$ outputs reject
```

Fig. 4. OR-Sigma protocol.

5.2 Optimization

Following some optimization techniques used in [8], we can have a more efficient OR-Sigma protocol. We just briefly describe the following three techniques, for more details please see [8, 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. Note that here we divide M leaves into K parts, and put a leaf corresponding to $c_{i,i\in[M]} = 0$ in each part, which leads to a smaller upper bound $K \cdot \log_2(\frac{M}{K})$ for the internal 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 [20], without affecting too much efficiency.

After applying the above methods, we obtain the optimized base OR sigma protocol shown in Figure 5 where we simplify internal seeds $\mathsf{seeds}_{\mathsf{internal}}$ as $\mathsf{seeds}_{\mathsf{int}}$, the $\mathsf{SeedTree}$ function as Sd, the $\mathsf{ReleaseSeeds}$ function as Rls, the $\mathsf{RecoverLeaves}$ function as Rcv, the seed expander and the commitment scheme $\mathcal{O}(\mathsf{salt}||\cdot)$ with salt as $\mathcal{O}_\mathsf{s}$ and the seed expander and the commitment scheme $\mathcal{O}(\mathsf{salt}|||i||\cdot)$ with salt and the ith instance as $\mathcal{O}_{\mathsf{s}i}$.

5.3 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, and 7 respectively.

```
$\mathcal{P}_1'(\phi_1, \ldots, \phi_N)$
$\mathsf{seed}_{\mathsf{root}} \xleftarrow{\$} \{0,1\}^{\lambda}$
$\mathsf{salt} \xleftarrow{\$} \{0,1\}^{2\lambda}$
$(\mathsf{seed}_1, \ldots, \mathsf{seed}_M) \leftarrow \mathsf{Sd}^{\mathcal{O}_\mathsf{s}}(\mathsf{seed}_{\mathsf{root}}, M)$
for $i$ from 1 to $M$ do
    $\mathsf{com_i} \leftarrow \mathcal{P}_1^{\mathcal{O}_{si}}((\phi_1, \ldots, \phi_N), \mathsf{seed}_i)$
$\mathsf{com} \leftarrow (\mathsf{salt}, \mathsf{com}_1, \ldots, \mathsf{com}_M)$
$\mathcal{P}$ sends $\mathsf{com}$ to $\mathcal{V}$
```

```
$\mathcal{V}_1'(\mathsf{com})$
$\mathbf{c} \xleftarrow{\$} C_{M,K}$
$\mathsf{cha} \leftarrow \mathbf{c}$
$\mathcal{V}$ sends $\mathsf{cha}$ $\mathcal{P}$
```

```
$\mathcal{P}_2'(A_I, I, \mathsf{cha})$
$\mathbf{c} = (c_1, \ldots, c_M) \leftarrow \mathsf{cha}$
for $i$ s.t. $c_i = 0$ do
    $\mathsf{rsp}_i \leftarrow \mathcal{P}_2(A_I, I, c_i, \mathsf{seed}_i)$
$\mathsf{seeds}_{\mathsf{int}} \leftarrow \mathsf{Rls}^{\mathcal{O}_\mathsf{s}}(\mathsf{seed}_{\mathsf{root}}, \mathsf{salt}, \mathbf{c})$
$\mathsf{rsp} \leftarrow (\mathsf{seeds}_{\mathsf{int}}, \{\mathsf{rsp}_i\}_{i \text{ s.t. } c_i=0})$
$\mathcal{P}$ sends $\mathsf{rsp}$ to $\mathcal{V}$
```

```
$\mathcal{V}_2'(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, \phi_0, \phi_1, \ldots, \phi_N)$
$(\mathsf{salt}, \mathsf{com}_1, \ldots, \mathsf{com}_M) \leftarrow \mathsf{com}$
$\mathbf{c} = (c_1, \ldots, c_M) \leftarrow \mathsf{cha}$
$(\mathsf{seeds}_{\mathsf{int}}, \{\mathsf{rsp}_i\}_{i \text{ s.t. } c_i=0}) \leftarrow \mathsf{rsp}$
$\{\mathsf{rsp}_i\}_{i \text{ s.t. } c_i=1} \leftarrow \mathsf{Rcv}^{\mathcal{O}_\mathsf{s}}(\mathsf{seeds}_{\mathsf{int}}, \mathbf{c})$
for $i$ from 1 to $M$ do
    if $\mathcal{V}_2^{\mathcal{O}_{si}}(\mathsf{com}_i, c_i, \mathsf{rsp}_i) = \mathsf{reject}$ then
        $\mathcal{V}$ outputs $\mathsf{reject}$
$\mathcal{V}$ outputs $\mathsf{accept}$
```

Fig. 5. Optimized OR sigma protocol.

```
Algorithm 4: Set Up
Input: The security parameter $\lambda$.
Output: Public paramater: variable number $n \in \mathbb{N}$, a prime power $q$ and an alternating trilinear form $\phi_0 \in \mathrm{ATF}(n, q)$.
Choose $n \in \mathbb{N}$ and a prime power $q$ corresponding to the security parameter $\lambda$.
Randomly sample an alternating trilinear form $\phi_0$ from $\mathrm{ATF}(n, q)$.
return Public parameter: $n, q, \phi_0$.
```

```
Algorithm 5: Key generation
Input: public parameter $n, q, \phi_0$, the user $i$.
Output: Public key for the user $i$: an alternating trilinear forms $\phi_i \in \mathrm{ATF}(n, q)$.
Private key for the user $i$: An invertible matrix $A_i$ such that $\phi_i = \phi_0 \circ A_i$.
Randomly sample a matrix $A_i$ from $\mathrm{GL}(n, q)$.
Compute $\phi_i \leftarrow \phi_0 \circ A_i$.
return Public key: $\phi_i$. Private key: $A_i$.
```

Algorithm 6: Signing procedure

```
Input: The public key: $\phi_0, \ldots, \phi_N$, he private key $A_I$ of a user $I \in [N]$, a message $\mathsf{msg}$, a commitment scheme $\mathsf{Com} : \{0,1\}^* \to \{0,1\}^\lambda$, a hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.
Output: A signature $\mathsf{Sig}$ on $\mathsf{msg}$.
$\mathsf{com} = (\mathsf{salt}, (\mathsf{com}_i)_{i \in [M]}) \leftarrow \mathcal{P}'_1(\phi_1, \ldots, \phi_N)$
$\mathsf{cha} \leftarrow \mathcal{H}(\mathsf{msg}||\phi_1|| \cdots ||\phi_N||\mathsf{com})$
$\mathsf{rsp} \leftarrow \mathcal{P}'_2(A_I, I, \mathsf{cha})$
return $\mathsf{Sig} = (\mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$
```

Algorithm 7: 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 $\mathsf{msg}$. A hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.
Output: "Yes" if $\mathsf{Sig}$ is a valid signature for $\mathsf{msg}$. "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 Parameters and implementation

6.1 New parameters in light of Beullens' algorithms

Beullens' algorithms. Beullens' algorithms for ATFE [6] are based on walking on a graph associated an alternating trilinear form. Such graph-theoretic algorithm has been proposed for other similar problems [13], while Beullens' novel technique is to incorporate min-rank algorithms in the exploration of such graphs. We review his algorithms in Appendix D.

Selection criteria of n and q. We then recall the following estimates of Beullens' algorithm. For odd n, Beullens' algorithm runs in time $O(q^{(n-5)/2} \cdot n^{11} + q^{n-7} \cdot n^6)$. For even n, Beullens' algorithm runs in time $O(q^{(n-4)/2} \cdot n^3 + q^{n-4} \cdot n^6)$. These will be used as our criteria for choosing n and q. Note that we will need to avoid weak keys.

6.2 Improvements to the previous implementation

The unbalanced challenge technique. In section 5.2, we introduce the unbalanced challenge technique for the ring signature. We can also apply this idea to the basic signatue which proposed by Tang et al [47]. This new tradeoff will lead to multiple parameter sets. To achieve the λ bits security, we should choose the proper M and K such that $(\frac{M}{K})^K \cdot (C-1)^K \geq 2^\lambda$. Our new public key, private key and signature size in terms of bits are as follows.

$$\begin{aligned}
\text{Public Key Size} &= C \cdot \binom{n}{3} \cdot \lceil \log_2 q \rceil + \lambda, \\
\text{Private Key Size} &= C \cdot n^2 \cdot \lceil \log_2 q \rceil, \\
\text{Signature Size} &= K(\lceil \log_2 \binom{M}{K} \rceil + \log_2(C)) + K \cdot \lceil \log_2 \binom{M}{K} \rceil \cdot \lambda + K \cdot n^2 \cdot \lceil \log_2 q \rceil.
\end{aligned}$$

More technical improvements. Furthermore, we improve the implementation of [47]. When generating a random invertible matrix, we represent it as the product of n invertible column matrices. A column matrix is equal to the identity matrix for each coefficient but one column. All invertible matrices cannot be decomposed in such product (without the use of a permutation matrix), however, the number of matrices not decomposable directly in such product of column matrices is negligible. An equivalent trick was already used in [47] to generate invertible matrices without having to compute a costly determinant. In [47] the authors were generating two invertible LU matrices (a lower triangular and an upper one) before multiplying the two matrices to obtain the invertible matrix A. However, once in the form of the product of n columns matrices, a matrix can be applied to an alternating trilinear form in simpler and faster way: each column matrix, one after the other, can be applied directly to the alternating trilinear without passing by a costly tensor form. Consequently, we obtain a reduction from $7/4 \cdot n^4$ to $1/2 \cdot n^4$ of the number of field multiplications required. This gain applies only to the matrices generated from a random seed, however in the case of unbalanced techniques it represents the vast majority.

New parameters. We consider two different security levels, namely 128-bit and 256-bit, as presented in Table 2 and Table 3, respectively.

Parameters					Size in Bytes		Time in μs		
n	q	$C = 2^c$	M	K	Public key	Signature	Set-Up	Sign	Verify
10	$262139(\sim 2^{18})$	46	770	11	12436	3725	975.1	20637.8	20146.4
		17	1200	12	4606	4062	374.1	31649.8	31117
11	$131217689(\sim 2^{27})$	72	1000	10	40111	5221	2434.6	40416.7	39688.5
		17	1200	12	9483	6263	603.6	47672.4	46917.6

Table 2. Parameters of 128-bit security

Comparison with the previous implementation Our implementation is more balanced in terms of efficiency and signature size than previous implementations proposed by Tang et al [47]. Due to recent attacks from Beullens [6], the parameter q has increased relatively. For example, when $n = 10$, we need to take

Parameters					Size in Bytes	
n	q	$C = 2^c$	M	K	pubkey size	sig size
10	549755813881 ($\sim 2^{39}$)	46	770	11	26942	7845
		17	1200	12	9977	8558
11	288230376151711717 ($\sim 2^{58}$)	72	1000	10	86162	11030
		17	1200	12	20368	13233

Table 3. Parameters of 256-bit security

$q = 262139$ instead of $q = 131071$. Since the unbalanced challenge technology will increase the number of rounds, we can analyze the signature and verification time of each round. The result is that our implementation still maintains the same signature time as before under the new attack, of course there will be some increase in the public and signature size. Since the signing time of the protocol is very fast, we can properly sacrifice the speed to ensure a smaller signature length as we showed in Table 2.

6.3 Implementing the ring signature scheme

Some formulas for parameters. To achieve the λ-bits security, we should choose the proper M and K such that $(\frac{M}{K})^K \geq 2^\lambda$. We use R denotes the size of ring. Here we use a trick that evenly dividing M rounds into K sections with length of $\lceil \frac{M}{K} \rceil$. For each section, we can construct a seed tree of which the internal seeds is of the size at most $\lambda \cdot \lceil \log_2(\frac{M}{K}) \rceil$.

1. The public key, private key and signature size of (non-linkable) ring signature in terms of bits are as follows.

$$\begin{aligned}\text{Public Key Size} &= (R+1) \cdot \binom{n}{3} \lceil \log_2 q \rceil, \\ \text{Private Key Size} &= \binom{n}{3} \lceil \log_2 q \rceil + R \cdot n^2 \lceil \log_2 q \rceil, \\ \text{Signature Size} &= K(\lambda \cdot \lceil \log_2 \left(\frac{M}{K}\right) \rceil + n^2 \lceil \log_2 q \rceil + 2\lambda \cdot \lceil \log_2 R \rceil + \lambda) + 3\lambda.\end{aligned}$$

2. The public key, private key and signature size of linkable ring signature in terms of bits are as follows.

$$\begin{aligned}\text{Public Key Size} &= (R+1) \cdot \binom{n}{3} \lceil \log_2 q \rceil, \\ \text{Private Key Size} &= \binom{n}{3} \lceil \log_2 q \rceil + R \cdot n^2 \lceil \log_2 q \rceil, \\ \text{Signature Size} &= K(\lambda \cdot \lceil \log_2 \left(\frac{M}{K}\right) \rceil + n^2 \lceil \log_2 q \rceil + 2\lambda \cdot \lceil \log_2 R \rceil + \lambda) + 3\lambda + \binom{n}{3} \lceil \log_2 q \rceil.\end{aligned}$$

Concrete parameters and reports on the performance. We provide the performance evaluation of our schemes in terms of signature size, as shown in Tables 4 and 5. Furthermore, Table 6 illustrates the signature generation time for our schemes. Our constructions are implemented and measured on a 2.4 GHz Quad-Core Intel Core i5.

Parameters				Size in Bytes				
n	q	M	K			R		
				2^1	2^3	2^6	2^{12}	2^{21}
10	262139($\sim 2^{18}$)	850	25	8873	9673	10873	13273	16873
11	131217689($\sim 2^{27}$)	850	25	13473	14273	15473	17873	21473

Table 4. The signature size (Bytes) of the ring signature. The security meets the NIST level 1.

Parameters				Size in Bytes				
n	q	M	K			R		
				2^1	2^3	2^6	2^{12}	2^{21}
10	549755813881 ($\sim 2^{39}$)	850	25	18683	21883	26683	36283	50683
11	288230376151711717 ($\sim 2^{58}$)	850	25	28427	31627	36427	46027	60427

Table 5. The signature size (Bytes) of the ring signature. The security meets the NIST level 5.

Parameters				Time in μs						
n	q	M	K				R			
				2^1	2^2	2^3	2^4	2^5	2^6	2^7
10	262139($\sim 2^{18}$)	850	25	35526.9	55714.4	96379.3	174050.1	369691.1	686969	1421279
11	131217689($\sim 2^{27}$)	850	25	54949.1	86427.9	146263.1	246734.5	475435.7	901354.7	1814951

Table 6. The signing time (μs) of the ring signature. The security meets the NIST level 1.

References

1. M. Abdalla, P. Fouque, V. Lyubashevsky, and M. Tibouchi. Tightly-secure signatures from lossy identification schemes. In *EUROCRYPT 2012*, 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 *ASIACRYPT 2020*, volume 12492 of *Lecture Notes in Computer Science*, pages 411–439. Springer, 2020.

3. L. Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *STOC 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 *ACM 1993*, pages 62–73, 1993.
6. W. Beullens. Graph-theoretic algorithms for the alternating trilinear form equivalence problem. *IACR Cryptol. ePrint Arch.*, page 1528, 2022.
7. 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 *EUROCRYPT 2022*, pages 95–126, 2022. Springer International Publishing.
8. W. Beullens, S. Katsumata, and F. Pintore. Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In *ASIACRYPT 2020*, volume 12492 of *Lecture Notes in Computer Science*, pages 464–492. Springer, 2020.
9. D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.
10. 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).
11. C. Bouillaguet. *Etudes d'hypotheses algorithmiques et attaques de primitives cryptographiques*. PhD thesis, PhD thesis, Université Paris-Diderot–École Normale Supérieure, 2011.
12. 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 *PKC 2011*, pages 473–493. Springer, 2011.
13. C. Bouillaguet, P. Fouque, and A. Véber. Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In *EUROCRYPT 2013*, pages 211–227, 2013.
14. G. Brassard and M. Yung. One-way group actions. In *CRYPTO 1990*, pages 94–107, 1990.
15. P. A. Brooksbank, Y. Li, Y. Qiao, and J. B. Wilson. Improved algorithms for alternating matrix space isometry: from theory to practice. In *ESA 2020*, 2020.
16. L. Carlitz. Representations by skew forms in a finite field. *Archiv der Mathematik*, 5:19–31, 1954.
17. 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.
18. J. M. Couveignes. Hard homogeneous spaces. *IACR Cryptology ePrint Archive*, 2006.
19. G. D'Alconzo and A. Gangemi. Trifors: Linkable trilinear forms ring signature. *Cryptology ePrint Archive*, 2022.
20. I. Dinur and N. Nadler. Multi-target attacks on the picnic signature scheme and related protocols. In *Advances in Cryptology - EUROCRYPT 2019*, volume 11478 of *Lecture Notes in Computer Science*, pages 699–727. Springer, 2019.
21. J. Don, S. Fehr, C. Majenz, and C. Schaffner. Security of the fiat-shamir transformation in the quantum random-oracle model. In *CRYPTO 2019* , volume 11693 of *Lecture Notes in Computer Science*, pages 356–383. Springer, 2019.
22. A. El Kaafarani, S. Katsumata, and F. Pintore. Lossy CSI-FiSh: Efficient Signature Scheme with Tight Reduction to Decisional CSIDH-512. In *PKC 2020*, volume 12111 of *Lecture Notes in Computer Science*, pages 157–186. Springer, 2020.

23. M. F. Esgin, R. K. Zhao, R. Steinfeld, J. K. Liu, and D. Liu. Matrict: efficient, scalable and post-quantum blockchain confidential transactions protocol. In *ACM SIGSAC 2019*, pages 567–584, 2019.
24. J. Faugère and L. Perret. Polynomial equivalence problems: Algorithmic and theoretical aspects. In *EUROCRYPT 2006*, pages 30–47, 2006.
25. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *CRYPTO 1986*, pages 186–194, 1986.
26. 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.
27. J. A. Grochow and Y. Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness. In ITCS 2021, volume 185 of *LIPIcs*, pages 31:1–31:19
28. J. A. Grochow, Y. Qiao, and G. Tang. Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. In *STACS 2021*, pages 38:1-38:17, 2021. arXiv:2012.01085.
29. J. Hora and P. Pudlák. Classification of 8-dimensional trilinear alternating forms over gf (2). *Communications in Algebra*, 43(8):3459–3471, 2015.
30. J. Hora and P. Pudlák. Classification of 9-dimensional trilinear alternating forms over gf (2). *Finite Fields and Their Applications*, 70:101788, 2021.
31. Z. Ji, Y. Qiao, F. Song, and A. Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In *TCC 2019*, volume 11891, pages 251–281. Springer, 2019.
32. J. Katz, V. Kolesnikov, and X. Wang. Improved non-interactive zero knowledge with applications to post-quantum signatures. In *ACM CCS 2018*, pages 525–537, 2018.
33. J. Katz and N. Wang. Efficiency improvements for signature schemes with tight security reductions. In *ACM CCS 2003*, pages 155–164, 2003.
34. E. Kiltz, V. Lyubashevsky, and C. Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In *EUROCRYPT 2018*, pages 552–586. Springer, 2018.
35. Y. Li and Y. Qiao. Linear algebraic analogues of the graph isomorphism problem and the Erdős–Rényi model. In *FOCS 2017*, pages 463–474. IEEE Computer Society, 2017.
36. J. K. Liu and D. S. Wong. Linkable ring signatures: Security models and new schemes. In *ICCSA 2005*, volume 3481 of *Lecture Notes in Computer Science*, pages 614–623. Springer, 2005.
37. Q. Liu and M. Zhandry. Revisiting post-quantum fiat-shamir. In *CRYPTO 2019*, volume 11693 of *Lecture Notes in Computer Science*, pages 326–355. Springer, 2019.
38. X. Lu, M. H. Au, and Z. Zhang. Raptor: A practical lattice-based (linkable) ring signature. In R. H. Deng, V. Gauthier-Umaña, M. Ochoa, and M. Yung, editors, *Applied Cryptography and Network Security*, pages 110–130, Cham, 2019. Springer International Publishing.
39. B. D. McKay. Practical graph isomorphism. *Congr. Numer.*, pages 45–87, 1980.
40. B. D. McKay and A. Piperno. Practical graph isomorphism, II. *J. Symb. Comput.*, 60:94–112, 2014.
41. 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.

42. J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In *EUROCRYPT 1996*, pages 33–48, 1996.
43. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of cryptology*, 13(3):361–396, 2000.
44. R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.
45. A. Stolbunov. *Cryptographic schemes based on isogenies.* PhD thesis, Norwegian University of Science and Technology, 2012.
46. 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 *ESORICS 2017*, volume 10493 of *Lecture Notes in Computer Science*, pages 456–474. Springer, 2017.
47. 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 *EUROCRYPT 2022*, volume 13277 of *Lecture Notes in Computer Science*, pages 582–612. Springer, 2022.
48. P. P. Tsang and V. K. Wei. Short linkable ring signatures for e-voting, e-cash and attestation. In *ISPEC 2005*, volume 3439 of *Lecture Notes in Computer Science*, pages 48–60. Springer, 2005.
49. D. Unruh. Quantum proofs of knowledge. In *Advances in Cryptology – Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, April 2012.
50. D. Unruh. Computationally binding quantum commitments. In *Advances in Cryptology – Eurocrypt 2016*, pages 497–527. Springer, 2016.
51. 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.
52. 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.
53. T. H. Yuen, M. F. Esgin, J. K. Liu, M. H. Au, and Z. Ding. Dualring: Generic construction of ring signatures with efficient instantiations. In T. Malkin and C. Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 251–281, Cham, 2021. Springer International Publishing.
54. M. Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Advances in Cryptology – CRYPTO 2019*, pages 239–268, Cham, 2019. Springer International Publishing.

A Σ-protocols based on ATFE

A.1 Properties of Σ-protocols

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. A 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 any λ and any poly-time quantum adversary $\mathcal{A}$, the following probability is negligible, taken over the randomness of $(x, w) \leftarrow \mathsf{Gen}(1^\lambda)$: $\Pr[\mathcal{V}(\mathsf{pk}, a, c, r) = 1 \wedge \mathcal{V}(\mathsf{pk}, a, c', r') = 1 \wedge c \neq c' \mid (a, c, r, c', r') \leftarrow \mathcal{A}(\mathsf{pk})] \leq \mathsf{negl}(\lambda)$.

Honest Verifier Zero Knowledge. A 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. A 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. A 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. A Σ-protocol has computationally unique response, if for any λ and any poly-time quantum adversary $\mathcal{A}$, the following probability is negligible, taken over the randomness of $(x, w) \leftarrow \mathsf{Gen}(1^\lambda)$:

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

Commitment Recoverability. A Σ-protocol is commitment recoverable if given c and r, there is a unique a such that (a, c, r) is a valid transcript. Such a commitment may be publicly computed with the input (x, c, r). In particular, our identification scheme support this property.

A.2 Properties of the Σ-protocol based on ATFE

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

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 adversary $\mathcal{A}$ 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 $\psi = \phi_c \circ D$. It follows that (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 $x = \{\phi_0, \ldots, \phi_{K-1}\}$ belong to, the $\mathsf{ATFE\text{-}GMW}$ protocol has α-bit min-entropy with $\alpha = \log_2(|\mathcal{O}|)$ and $|\mathcal{O}|$ is the size of orbit $\mathcal{O}$.

Remark 6. By the orbit-stabiliser theorem, for an alternating trilinear form ϕ over $\mathbb{F}_q^n$, we have $|\mathcal{O}(\phi)| = |\operatorname{GL}(n, q)|/|\operatorname{Aut}(\phi)|$. 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 $\mathsf{ATFE\text{-}GMW}$ protocol is commitment recoverable. In fact, given a challenge c and a response D, there is only one commitment ψ computed by $\psi = \phi_c \circ D$.

A.3 Security proof for the optimized base OR-Sigma protocol

Theorem 9. *Define the following relation*

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

and the relaxed relation

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

Then the optimized base OR sigma protocol shown in Figure 5 has correctness, relaxed special soundness and honest-verifier zero-knowledge for the relation R.

Proof. Let $G, S_1, S_2 := \operatorname{GL}(n, q)$, $\mathcal{X} := \operatorname{ATF}(n, q)$, $D_{\mathcal{X}} = \{\circ\}$ 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 [8, Definition 3.1]. By the Theorem 3.5 and Theorem 3.6 in [8], our OR sigma protocol is proved to have correctness, relaxed special soundness and honest-verifier zero-knowledge. □

B An outline of Beullens' algorithm for ATFE

We briefly outline some of the main ideas behind Beullens' algorithms for ATFE [6].

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. The graph associated with ϕ is $G(\phi) = (V, E)$ where $V = \mathbb{P}(\mathbb{F}_q^n)$, and for $u, v \in \mathbb{P}(\mathbb{F}_q^n)$, $\{u, v\} \in E$ if and only if $\phi(u, v, x) = 0$ for all $x \in \mathbb{F}_q^n$. Here $\mathbb{P}(\mathbb{F}_q^n)$ is the projective space associated with $\mathbb{F}_q^n$, consisting of lines in $\mathbb{F}_q^n$. That is, for $v \in \mathbb{F}_q^n$, $v \neq 0$, we let $\hat{v} := \{u \in \mathbb{F}_q^n \mid u = \alpha \cdot v, \alpha \in \mathbb{F}_q\}$. Note that $\{u, v\} \in E$ if and only if the linear form obtained by instantiating the first two arguments of ϕ to u and v is the zero linear form. Such graphs have been used in algorithms for other related isomorphism problems [13].

We can then assign labels to the vertices of $G(\phi)$ as follows. For $\hat{v} \in \mathbb{P}(\mathbb{F}_q^n)$, let $\mathrm{rk}_\phi(\hat{v})$ be the rank of the bilinear form $\phi(v, \cdot, \cdot)$. When it is clear from the context, we may just write as $\mathrm{rk}(\hat{v})$. It is clear that $\mathrm{rk}(\hat{v})$ is an isomorphism invariant, that is, if ϕ and ψ are equivalent, then any isomorphism sends $\hat{v}$ of $\mathrm{rk}(\hat{v}) = r$ to some $\hat{u}$ of the same label.

Now suppose $\phi, \psi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ are equivalent via $A \in \mathrm{GL}(n, q)$. One heuristic method in [47] (as also from [13]) is that, once the image of A at some non-zero vector u is recovered, then the whole A can be computed in polynomial time via Gröbner basis. This observation was strengthened in [6], where it was observed that one only needs to know the image of $\hat{u}$ for the Gröbner basis method to be efficient.

Based on the above, the basic strategy in [6] is to sample those vertices of $G(\phi)$ of "small" ranks based on walking on $G(\phi)$. This requires the following two ingredients.

First, this requires an estimation of distributions of ranks of vertices in $G(\phi)$. Experimental data of such distributions for small n and q were shown in [47], and [6, Theorem 1] gave closed-form formulas for such distributions. We independently discovered such formulas, and the proofs are put in Appendix C.

Second, to sample vertices of small ranks, the key idea of Beullens is to make use of min-rank solvers. For example, suppose we start with $\hat{v}$ of a large rank (i.e. $\mathrm{rk}(\hat{v}) = n-1$ if n is odd, and $\mathrm{rk}(\hat{v}) = n-2$ if n is even). It is easy to compute the neighbours of $\hat{v}$ on $G(\phi)$ by computing the kernel of the matrix $\phi(v, \cdot, \cdot)$. Then the question of whether the kernel contains a low-rank vector $\hat{u}$ can be modelled as a min-rank problem, which asks to compute a matrix of small rank in a linear space of matrices. The min-rank problem for the parameters of interest in [47] can be solved effectively in practice. Combining with the rank distributions, the probability of the neighbours in $\hat{v}$ having a small-rank one can be computed. This leads to a sampling procedure of low-rank vectors.

Besides the basic strategy, another key observation is to exploit some weak keys. Take $n = 10$ as an example. The highest rank in this setting is 8. It can be shown that with probability $\sim 1/q$, there is a unique $\hat{v}$ of rank 4. This can then be exploited to give a fast algorithm, as the problem completely boils down to find this unique $\hat{v}$.

Of course there are more ideas and techniques, especially for $n = 10$ in Beullens' beautiful paper, but the above are the main ideas for $n = 10$ and 11.

What is the prospect of further improving over Beullens' algorithms? The current bottleneck is on the number of low-rank vectors, which can still be a large number. To go beyond that, we would need more distinguishing isomorphism invariants (such as the rank statistics of the neighbours), which in turn would take more costs to compute. Such a trade-off between distinguishing power of new isomorphism invariants and their computational costs will be an interesting topic for future study, but so far it seems difficult, if possible at all, to exploit new isomorphism invariants.

C On the rank statistics of random alternating trilinear forms

Contractions of alternating trilinear forms. Let V be a vector space of dimension n. Let $b_1, \ldots, b_n$ be a basis of V^* An alternating trilinear form $t : V^3 \to V$ can be represented as

$$\sum_{1 \leq i < j < k \leq n} t_{i,j,k} b_i \wedge b_j \wedge b_k.$$

Assume that the underlying field F is finite and that the $t_{i,j,k}$ are drawn uniformly at random. Let $v \in V$ be nonzero. Assume that $b_1(v) \neq 0$. Let $\hat{b}_1 = 1/b_1(v) \cdot b_1$. By setting $\hat{b}_i := b_i - \alpha_i b_1$ for some suitable $\alpha_i \in F$, we can assume that $\hat{b}_i(v) = 0$. The new coefficients $\hat{t}_{i,j,k}$ in the basis $\hat{b}_1, \hat{b}_2, \ldots, \hat{b}_n$ are again uniformly random. Now

$$\begin{aligned} \hat{t}(v, ., .) &= \sum_{1 \leq i < j < k \leq n} \hat{t}_{i,j,k} \hat{b}_i(v) \wedge \hat{b}_j \wedge \hat{b}_k \\ &= \sum_{2 \leq j < k \leq n} \hat{t}_{1,j,k} \hat{b}_j \wedge \hat{b}_k \end{aligned}$$

Thus $\hat{t}(v, ., .)$ is a random alternating bilinear form, or equivalently, a random alternating matrix.

Proposition 1. *The probability that $t(v, ., .)$ has rank $2r$ equals the probability that a random alternating $(n-1) \times (n-1)$-matrix has rank $2r$.*

The number of alternating matrices of given rank. Let $S(m, 2r)$ be the number of alternating $m \times m$-matrices of rank $2r$.

Theorem 10 (Carlitz [16]).

$$S(m, 2r) = q^{r(r-1)} \frac{\prod_{i=0}^{2r-1} (q^{m-i} - 1)}{\prod_{i=1}^{r} (q^{2i} - 1)}$$

Putting it together. For an alternating trilinear form $t : V^3 \to V$ and $v \in V$, let $t_v : V^2 \to V$ be the alternating bilinear form $t(v, ., .)$. Let $R_{t,\rho} = \{u \in V \mid \mathrm{rk}(t_u) = \rho\}$.

The total number of alternating $m \times m$-matrices is $q^{\binom{m}{2}}$. The total number of alternating trilinear forms on V is $q^{\binom{n}{3}}$.

The number of pairs (u, t) with $u \in V \setminus \{0\}$ and t being an alternating trilinear form such that $u \in R_{t,2r}$ is

$$\underbrace{(q^n - 1)}_{\text{number of } u} \cdot \underbrace{q^{\binom{n}{3}}}_{\text{number of } t} \cdot \underbrace{\frac{S(n-1, 2r)}{q^{\binom{n-1}{2}}}}_{\text{prob for rank } 2r}.$$

Thus the expected size is

$$E_t(|R_{t,2r}|) = (q^n - 1)\frac{S(n-1, 2r)}{q^{\binom{n-1}{2}}}.$$

In particular, if r is small compared to n and both values are fixed, then the quantity goes to zero when q grows. For $\rho = 2r = 4$, it is about $q^{6.5n-15-0.5n^2}$.

Comparison. We compare with [47, Table 3], only the cases when 100 simulations were done and the characteristic was odd.

n	q	2	4	6	8
7	5	5.76	16218.24	61900	—
9	3	0	30	7064.24	12587.76
10	3	0	0.96	2451.74	56595.3

Table 7.

Our formula yields (rounded)

n	q	2	4	6	8
7	5	5.21	16139.4	61979.4	—
9	3	0.0015	30.56	7073.83	12577.6
10	3	0.000006	1.13	2448.59	56598.3

Table 8.

D Automorphism group orders of random alternating trilinear forms

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 [17,41,29]. Third, for $n = 9$ and $q = 2$, by the classification of alternating trilinear forms [30], 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 [10] for computing automorphism group orders of alternating trilinear forms. Built on the Magma program in [47], 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 [24,11,12,13]. 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 [15]. The way we set up the equations is from [47].

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.

E Alternative QROM security proof

Theorem 11. *The $\mathsf{ATFE\text{-}GMW\text{-}FS\text{-}}\mathcal{O}(\phi)$ signature based on the t repetitions of $\mathsf{ATFE\text{-}GMW\text{-}}\mathcal{O}(\phi)$ Σ-protocol in Figure 3 has $\mathsf{sEUF\text{-}CMA}$ security that for any polynomial-time quantum adversary $\mathcal{A}$ querying the quantum random oracle Q_H times against $\mathsf{sEUF\text{-}CMA}$ security of $\mathsf{ATFE\text{-}GMW\text{-}FS\text{-}}\mathcal{O}(\phi)$ signature, there is a quantum adversary $\mathcal{B}$ for K-psATFE-$\mathcal{O}(\phi)$ problem such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ATFE-sEUF-CMA}} \leq O\left({Q_H}^2 \cdot \left(\mathsf{Adv}_{\mathcal{B}}^{K-\mathsf{psATFE}-\mathcal{O}(\phi)}\right)^{\frac{1}{3}}\right).$$

Proof. By Theorem 13, we have a Σ-protocol with post-quantum weakly ID soundness. Then the $\mathsf{sEUF\text{-}CMA}$ security can be achieved by Theorem 16. □

Post-Quantum weak ID soundness of $\mathsf{ATFE\text{-}GMW\text{-}}\mathcal{O}(\phi)$ Σ-protocol When a Σ-protocol is for identification, we need a definition of ID soundness to protect against the adversaries. Here we consider the weak ID soundness property only against adversaries without eavesdropping attack. The definition of this property is as follows:

Definition 11. *A Σ-protocol has post-quantum weak ID soundness if for any $(x, w) \in R$, every adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ with only the x can convince an honest verifier $\mathcal{V}$ with a negligible probability, i.e.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{wID}}(\lambda) = \Pr\left[\mathcal{V}(x, a, c, r) = 1 \mid a \leftarrow \mathcal{A}_0(x) \wedge c \overset{\$}{\leftarrow} \mathsf{ChSet} \wedge r \leftarrow \mathcal{A}_1(x, a, c)\right] \leq \mathsf{negl}(\lambda).$$

For convenience, we write the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{wID}}(\lambda)$ as $\Pr[v = 1 \mid v \leftarrow \langle \mathcal{A}(x), \mathcal{V}(x) \rangle]$.

Liu and Zhandry show that post-quantum identification soundness can be satisfied if sigma protocol has weakly collapsing property and extra properties [37, Theorem 1]. We relax the ID soundness to the weak ID soundness, so the HVZK property isn't required here. Moreover, since the perfect unique response is a stronger property than weakly collapsing property, we can modify the result in [37].

Theorem 12 ([37], Theorem 1). *If a Σ-protocol with an exponentially large challenge space has completeness, post-quantum 2-soundness 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 weak ID soundness, there is a quantum adversary $\mathcal{B}$ for 2-soundness such that,*

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

Theorem 13. *The t repetitions of $\mathsf{ATFE\text{-}GMW\text{-}}\mathcal{O}(\phi)$ Σ-protocol in Figure 3 is a Σ-protocol with post-quantum weak ID soundness that for any polynomial-time quantum adversary $\mathcal{A}$ against post-quantum ID soundness of $\mathsf{ATFE\text{-}GMW\text{-}}\mathcal{O}(\phi)$ Σ-protocol, there is a quantum adversary $\mathcal{B}$ for K-$\mathsf{psATFE\text{-}}\mathcal{O}(\phi)$ problem such that,*

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

Proof. By the Assumption 3 and the Lemma 1, the Σ-protocol in Figure 3 has perfect unique response. We also proved that it has completeness and post-quantum 2-soundness in 2.5. Since t repetitions of Σ-protocol in Figure 3 has an exponentially large challenge space, we complete the proof using the result of Theorem 12. □

Security of ATFE-GMW-FS-$\mathcal{O}(\phi)$ signature Don et al. showed that the security of signature can be reduced to the security of underlying protocol through their measure-and-reprogram strategy [21]. We use their main technology [21, Theorem 8] to preserve the weak ID soundness from underlying protocol to Fiat-Shamir signature.

Theorem 14. *If a Σ-protocol with a superpolynomially challenge space has weakly post-quantum ID soundness, the Fiat-Shamir transformation can produce a secure signature that for any polynomial-time quantum adversary $\mathcal{A}$ querying the quantum random oracle Q_H times against $\mathsf{EUF\text{-}NMA}$ security, there is a static quantum adversary $\mathcal{B}$ against post-quantum weakly ID-soundness of the underlying protocol such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{EUF\text{-}NMA} \leq O\left({Q_H}^2\right) \cdot \mathsf{Adv}_{\mathcal{B}}^{wID}.$$

proof (sketch). The idea is similar to the proof of the Lemma 12, Corollary 13 and Theorem 21 in [21]. Assume for any static adversary $\mathcal{B}$ such that,

$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{wID}}(\lambda) = \Pr\left[v = 1 \mid v \leftarrow \langle \mathcal{B}(x), \mathcal{V}(x)\rangle\right],$$

for any $x \in \mathcal{X}$. Then there is a polynomial-time quantum adversary $\mathcal{A}$ querying the quantum random oracle H Q_H times against $\mathsf{EUF\text{-}NMA}$ security such that,

$$\begin{aligned}\mathsf{Adv}_{\mathcal{A}}^{\mathsf{EUF\text{-}NMA}}(\lambda) &= \Pr[\mathsf{Ver}(\mathsf{pk}, m, \sigma) = 1 \mid (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \wedge (m, \sigma) \leftarrow \mathcal{A}^H(\mathsf{pk})] \\ &= \sum_{(x', w') \leftarrow \mathsf{Gen}} \Pr[\mathsf{Ver}(x, m, \sigma) = 1 \mid (m, \sigma) \leftarrow \mathcal{A}^H(x)] \Pr[x = x'] \\ &\leq \sum_{(x', w') \leftarrow \mathsf{Gen}} O({Q_H}^2) \Pr\left[v = 1 \mid v \leftarrow \left\langle \mathcal{S}^{\mathcal{A}}(x), \mathcal{V}(x)\right\rangle\right] \Pr[x = x'] \\ &+ \mathsf{negl}(\lambda).\end{aligned}$$

At this inequality, we use the Theorem 8 in [21] to reduce the adversary against the weak ID soundness to the adversary against Fiat-Shamir signature. Thus, we can obtain that,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{EUF\text{-}NMA}}(\lambda) \leq O\left({Q_H}^2\right) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathsf{wID}}.$$

The proof completes. □

This security is not enough if we consider the chosen-message attack. [34] contains the proof of reduction from chosen-message attack to no-message attack. Although their final result are based on lossy property, this reduction is for general case. We can still use the Theorem 3.3 in [34].

Theorem 15. *Assume that the scheme is HVZK, has α bits of min-entropy, and has computationally unique response. Then for any quantum adversary $\mathcal{A}$ against the sEUF-CMA security that issues at most q queries to the classical signing oracle, there exist quantum adversaries $\mathcal{B}, \mathcal{D}$ such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sEUF\text{-}CMA}} \leq \mathsf{Adv}_{\mathcal{B}}^{\mathsf{EUF\text{-}NMA}} + q \cdot 2^{-\alpha+1} + \mathsf{Adv}_{\mathcal{D}}^{\mathsf{CUR}}.$$

Assumption 5. No poly-time quantum algorithm can solve ATF automorphism problem in Definition 8 with a non-negligible probability.

Theorem 16. *If the t repetitions of ATFE-GMW-$\mathcal{O}(\phi)$ Σ-protocol showed in Figure 3 has post-quantum weakly ID soundness, then the corresponding Fiat-Shamir signature has sEUF-CMA security that for any polynomial-time quantum adversary $\mathcal{A}$ querying the quantum random oracle Q_H times against sEUF-CMA security of ATFE-GMW-FS-$\mathcal{O}(\phi)$ signature, there are quantum adversary $\mathcal{B}$ against post-quantum weak ID-soundness of ATFE-GMW-$\mathcal{O}(\phi)$ protocol such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ATFE-sEUF\text{-}CMA}} \leq O\left({Q_H}^2\right) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathsf{ATFE-wID}}.$$

Proof. Assume the t repetitions of Σ-protocol showed in Figure 3 has post-quantum weak ID soundness. The ATFE-GMW-FS-$\mathcal{O}(\phi)$ signature based on it has EUF-NMA security using Theorem 14.

We proved that it has $\alpha = \log_2(|\mathcal{O}|)$ bits min-entropy in Section 2.5, and $|\mathcal{O}| = 2^{\Omega(\lambda)}$, and thereby $2^{-\alpha+1}$ is negligible. By Assumption 5 and Lemma 2, the advantage of adversaries against computationally unique response is negligible. Now we complete the proof utilizing the result of Theorem 15 □

F Linkable ring signature from ATFE

Linkable ring signatures were first introduced by Liu and Wong [36] that allow public checking whether two ring signatures are 'linked', i.e., generated by one user. A typical approach to construct a linkable ring signature is to add a tag, which uniquely define the real signer, to a signature. We first construct a linkable OR sigma protocol and then apply Fiat-Shamir transformation to obtain a linkable ring signature, as similar to the work of Beullens et al. [8] in the context of isogeny-based cryptography

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 6. Then we apply the same optimization methods in Section 5.2 to this protocol.

F.1 Linkable ring signatures

We first review some basic notions related to 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 [8], are provided as follows.

Definition 12 (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 linkable ring signature Π_{LRS} is said to have correctness if for any security parameter λ, polynomial $N = \mathsf{poly}(\lambda)$, two messages $\mathsf{M}_0, \mathsf{M}_1$, two sets $D_0, D_1 \subseteq [N]$ such that $j \in D_0 \cap D_1$, $\mathsf{pp} \leftarrow \mathsf{LRS.SetUp}(1^\lambda)$, $\{(\mathsf{vk}_1, \mathsf{sk}_1), \ldots, (\mathsf{vk}_N, \mathsf{sk}_N)\} \leftarrow \mathsf{RS.KeyGen}(\mathsf{pp})$, a random bit $b \leftarrow \{0,1\}$, $\sigma_b \leftarrow \mathsf{LRS.Sign}(\mathsf{sk}_j, \mathsf{R}_b, \mathsf{M}_b)$ with $\mathsf{R}_b := \{\mathsf{vk}_i\}_{i \in D_b}$, it always holds that $\mathsf{LRS.Verify}(\mathsf{R}, \mathsf{M}, \sigma_b) = 1$ and $\mathsf{LRS.Link}(\sigma_0, \sigma_1) = 1$.

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 runs $\mathsf{pp} \leftarrow \mathsf{LRS.SetUp}(1^\lambda)$ and send pp to $\mathcal{A}$.
(2) $\mathcal{A}$ generates public keys and secret keys $(\{\mathsf{vk}_i, \mathsf{sk}_i\}) \leftarrow \mathsf{LRS.KeyGen}(\mathsf{pp}))$ for $i \in [N]$, 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 runs $\mathsf{pp} \leftarrow \mathsf{LRS.SetUp}(1^\lambda)$ generates public keys and secret keys $(\{\mathsf{vk}_i, \mathsf{sk}_i\}) \leftarrow \mathsf{RS.KeyGen}(\mathsf{pp})$ for $i \in [N]$ 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 message 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 $\mathsf{LRS.Sign}(sk_b, \mathsf{R}, \mathsf{M}) \to \sigma$.
   - If $\mathsf{vk} = \mathsf{vk}'_1$, the challenger outputs the signature $\mathsf{LRS.Sign}(sk_{1-b}, \mathsf{R}, \mathsf{M}) \to \sigma$.

(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 runs $\mathsf{pp} \leftarrow \mathsf{LRS.SetUp}(1^\lambda)$ generates public keys and secret keys $(\{\mathsf{vk}_i, \mathsf{sk}_i\}) \leftarrow \mathsf{RS.KeyGen}(\mathsf{pp})$ for $i \in [N]$. 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 $\mathsf{LRS.Sign}(\mathsf{sk}_i, \mathsf{R}, \mathsf{M}) \to \sigma$ 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.

F.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 13 (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].

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 17. *The linkable OR sigma protocol shown in the Figure 6 after the optimization has correctness, high min-entropy, special zero-knowledge and relaxed special soundness.*

Proof. Let $G, S_1, S_2 := \mathrm{GL}(n, q)$, $\mathcal{X}, \mathcal{T} := \mathrm{ATF}(n, q)$, $D_{\mathcal{X}} := \{\circ\}$, $D_{\mathcal{T}} := \{\bullet\}$ and $\mathsf{Link}_{\mathsf{GA}}$ be the equivalent relation. Then assume the K-psATFE problem and PR-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 [8]. For the property (5), we can derive this property by restricting the orbit of ϕ_0 has trivial automorphism. Finally, by the PR-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 [8], our OR sigma protocol is proved to have correctness, relaxed special soundness and honest-verifier zero-knowledge. □

```
$\mathcal{P}_1(\phi_1, \ldots, \phi_N, \tau)$
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
    $\psi_i \leftarrow \phi_i \circ B$
    $\mathsf{C}_i \leftarrow \mathsf{Com}(\psi_i, \mathsf{bits}_i)$
$(\mathsf{root}, \mathsf{tree}) \leftarrow \mathsf{MerkleTree}(\mathsf{C}_1, \ldots, \mathsf{C}_N)$
$h \leftarrow \mathcal{H}_{\mathsf{Coll}}(\tau', \mathsf{root})$
$\mathsf{com} \leftarrow h$
$\mathcal{P}$ sends com to $\mathcal{V}$
```

```
$\mathcal{V}_1(\mathsf{com})$
$c \xleftarrow{\$} \{0,1\}$
$\mathsf{cha} \leftarrow c$
$\mathcal{V}$ sends cha to $\mathcal{P}$
```

```
$\mathcal{P}_2(A_I, I, \mathsf{cha})$
$c \leftarrow \mathsf{cha}$
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
    $\mathsf{rsp} \leftarrow \mathsf{seed}$
$\mathcal{P}$ sends rsp to $\mathcal{V}$
```

```
$\mathcal{V}_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, \phi_0, \phi_1, \ldots, \phi_N, \tau_0, \tau)$
$(h, c) \leftarrow (\mathsf{com}, \mathsf{cha})$
if $c = 0$ then
    $(D, \mathsf{path}, \mathsf{bits}) \leftarrow \mathsf{rsp}$
    $\tilde{\psi} \leftarrow \phi_0 \circ D$
    $\tilde{\mathsf{C}} \leftarrow \mathsf{Com}(\tilde{\psi}, \mathsf{bits})$
    $\tilde{\tau}' \leftarrow \tau_0 \bullet D$
    $\widetilde{\mathsf{root}} \leftarrow \mathsf{ReconstructRoot}(\tilde{\mathsf{C}}, \mathsf{path})$
    if $h = \mathcal{H}_{\mathsf{Coll}}(\tilde{\tau}', \widetilde{\mathsf{root}})$ then
        $\mathcal{V}$ outputs accept
    else
        $\mathcal{V}$ outputs reject
else
    $\mathsf{seed} \leftarrow \mathsf{rsp}$
    $\widetilde{\mathsf{root}} \leftarrow \mathcal{P}_1((\phi_1, \ldots, \phi_N), \mathsf{seed})$
    if $h = \mathcal{H}_{\mathsf{Coll}}(\tilde{\tau}', \widetilde{\mathsf{root}})$ then
        $\mathcal{V}$ outputs accept
    else
        $\mathcal{V}$ outputs reject
```

Fig. 6. Linkable OR sigma protocol.

F.3 Linkable ring signature

After applying the Fiat-Shamir transformation to the linkable OR sigma protocol, we obtain a linkable ring signature shown in Algorithms 8, 9, 10, 11 and 12. The linkable ring signature is similar to the normal ring signature in addition with a link algorithm.

```
Algorithm 8: Set Up
Input: The security parameter $\lambda$.
Output: Public paramater: variable number $n \in \mathbb{N}$, a prime power $q$ and alternating trilinear forms $\phi_0, \tau_0 \in \mathrm{ATF}(n, q)$.
Choose $n \in \mathbb{N}$ and a prime power $q$ corresponding to the security parameter $\lambda$.
Randomly sample an alternating trilinear form $\phi_0, \tau_0$ from $\mathrm{ATF}(n, q)$.
return Public parameter: $n, q, \phi_0, \tau_0$.
```

```
Algorithm 9: Linkable key generation
Input: Public parameter $n, q, \phi_0, \tau_0$ and the user $i$.
Output: Public key for the user $i$: alternating trilinear forms $\phi_i \in \mathrm{ATF}(n, q)$.
        Private key for the user $i$: A matrix $A_i$ such that $\phi_i = \phi_0 \circ A_i$.
Randomly sample a matrix $A_i$ from $\mathrm{GL}(n, q)$.
Compute $\phi_i \leftarrow \phi_0 \circ A_i$.
return Public key: $\phi_i$. Private key: $A_i$.
```

Algorithm 10: 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 11: Linkable signing procedure

```
Input: The public key: $\phi_0, \ldots, \phi_N$. The private key: $A_I$. The security parameter $\lambda$. The message $\mathsf{msg}$. 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 $\mathsf{Sig}$ on $\mathsf{msg}$.
$\tau \leftarrow \tau_0 \bullet A_I$
$\mathsf{com} = (\mathsf{salt}, (\mathsf{com}_i)_{i\in[M]}) \leftarrow \mathcal{P}_1'(\phi_0, \phi_1, \ldots, \phi_N, \tau)$
$\mathsf{cha} \leftarrow \mathcal{H}(\mathsf{msg}||\phi_1|| \cdots ||\phi_N||\tau||\mathsf{com})$
$\mathsf{rsp} \leftarrow \mathcal{P}_2'(A_I, I, \mathsf{cha})$
return $\mathsf{Sig} = (\mathsf{salt}, \tau, \mathsf{cha}, \mathsf{rsp})$
```

Algorithm 12: 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 $\mathsf{msg}$. A hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.
Output: "Yes" if $\mathsf{Sig}$ is a valid signature for $\mathsf{msg}$. "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
```

Remark 7. Since the linkable OR sigma protocol is proved to satisfy all conditions in Theorem 17, and by the Theorem 4.7 in [8], the linkable ring signature in Algorithm 9, 10, 11 and 12 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*[25]. Beullens et.al. proposed a new property called online extractability [7], which is used to obtain a almost tight security reduction of ring signature.Further they use some techniques including the Katz-Wang technique [33] 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.