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

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. An isomorphism problem asks whether two combinatorial or algebraic structures are essentially the same. Based on the assumed hardness of an isomorphism problem, there is a well-known digital signature design based on the Goldreich–Micali–Widgerson (GMW) zero-knowledge protocol for graph isomorphism and the Fiat–Shamir (FS) transformation. Recently, there is a revival of activities on this design, as witnessed by the schemes SeaSign (Eurocrypt 2019), CSI-FiSh (Asiacrypt 2019), LESS (Africacrypt 2020), ATFE (Eurocrypt 2022), and MEDS (Africacrypt 2023).

The contributions of this paper are two-folds: the first is about the GMW-FS design in general, and the second is on the ATFE-GMW-FS scheme.

First, we study the QROM security and ring signatures of the GMW-FS design in the group action framework. We distil properties of the underlying isomorphism problem for the GMW-FS design to be secure in the quantum random oracle model (QROM). We also show that this design supports a linkable ring signature construction following the work of Beullens, Katsumata and Pintore (Asiacrypt 2020).

Second, we apply the above results to prove the security of the ATFE-GMW-FS scheme in the QROM model. We then describe a linkable ring signature scheme based on it, and provide an implementation of the ring signature scheme. Preliminary experiments suggest that our scheme is competitive among existing post-quantum ring signatures. We also discuss the parameter choices of the ATFE-GMW-FS scheme based on the recent attack by Beullens (Cryptology ePrint Archive, Paper 2022/1528), and the MPC-in-the-head construction for general group actions by Joux (Cryptology ePrint Archive, Paper 2023/664).

1 Introduction

1.1 Background: group actions in cryptography and the GMW-FS digital signature design

Group actions in (post-quantum) cryptography. The use of group actions in cryptography has a long tradition. Indeed, the discrete logarithm problem can be interpreted as a problem about cyclic group actions [29]. As far as we know, the first treatment of *abstract* group actions in cryptography goes back to Brassard and Yung [22], who proposed the notion of *one-way* group actions. When the groups are abelian (commutative), this was further developed by Couveignes [29]. Recently, two independent works [49] and [2] enriched this framework further by introducing the notion of (weakly) pseudorandom group actions, which generalises the celebrated Decisional Diffie–Hellman assumptions [15].

Besides setting up frameworks, many cryptographic primitives can be realised, such as claw-free one-way functions and bit commitment [22], quantum-secure pseudorandom functions [49], and zero-knowledge identification protocols [29,49]. When the groups are abelian (commutative), more functions are possible, such as key exchange [29], smooth projective hasing, and dual-mode public-key encryption [2].

Since discrete logarithm can be solved efficiently on quantum computers [67], it is desirable to explore group actions suitable for post-quantum cryptography. As in the lattice case [64], the research into hidden subgroup problems is of particular relevance here, especially the hidden shift problems [26] and symmetric or general linear groups [45]. We will discuss this further below.

The GMW-FS digital signature design. A major cryptographic application of group actions is the following design of digital signature. In [41], Goldreich, Micali and Wigderson described a zero-knowledge proof protocol for graph isomorphism (GI). The Fiat-Shamir transformation FS [40] 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 [57,58], 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 was already carried out to two areas in the context of post-quantum cryptography, that is multivariate cryptography and isogeny-based cryptography. In multivariate cryptography, Patarin proposed using polynomial isomorphism problems to replace graph isomorphism [60]. In isogeny-based cryptography, Stolbunov applied this construction to the class group actions on elliptic curves [29,68]. However, these efforts met some issues. For example, the parameters proposed by Patarin were too optimistic [21], and computational costs and uniform sampling for class group actions are tricky issues [25].

The recent revival of the GMW-FS design. Recently, there is a revival of the study of the GMW-FS design, which is attributed to two research directions.

The first direction is the study of elliptic curve isogeny, following Couveignes and Stolbunov. As mentioned above, the issues here are mostly due to the computational aspects of group actions. To remedy this, the commutative group action CSIDH based on supersingular curves over prime fields was introduced in [25]. This led to the schemes SeaSign [39] and CSI-FiSh [13], which greatly improve the situation by introducing either computational or protocol optimisations; see also the recent nice survey on this and more [11].

The second direction may be viewed as a continuation of the polynomial isomorphism direction by Patarin. Three schemes are proposed and implemented, including LESS [14] based on linear code monomial equivalence, ATFE [70] based on alternating trilinear form equivalence, and MEDS [27] based on matrix code equivalence[6]. Recent progress in complexity theory [43] shows that (1) linear code monomial equivalence reduces to matrix code equivalence in polynomial time [42,30], and (2) alternating trilinear form equivalence, isomorphism of quadratic polynomials with two secrets, cubic form equivalence, and matrix code equivalence are polynomial-time equivalent [43,44] (see also [65] for some of these equivalences).

The studies above are of particular interest in post-quantum cryptography. For the class group actions in the isogeny setting, even though the group action underlying CSIDH is commutative, the best quantum algorithms are still subexponential [61,17]. For the group actions underlying LESS, ATFE and MEDS, the groups are symmetric or general linear groups, so the previous negative evidence for standard techniques (such as coset sampling) in hidden subgroup problem for graph isomorphism [45] applies.

1.2 Our Contributions

Our contributions in this paper can be classified into two sets.

The first set of results is for the GMW-FS design based on abstract group actions. Briefly speaking, we first distil properties for group actions to be secure in the quantum random oracle model (QROM) based on the works [52,55,33]. We then present the linkable ring signature construction of Beullens, Katsumata and Pintore [12] with abstract group actions.

The second set of results is for the ATFE-GMW-FS scheme in [70]. We first discuss the parameter choices of this scheme in light of the recent beautiful attacks by Beullens [9], and demonstrate an improvement to the implementation from [70]. We also show that the MPC-in-the-head paradigm for group actions [50] help to reduce the signature sizes for the ATFE-GMW-FS scheme. We then

[6] Matrix code equivalence is also known as 3-tensor isomorphism in [43].

apply the results from the first set to the ATFE-GMW-FS scheme to demonstrate its QROM security. We then implement the ring signature scheme above for ATFE-GMW-FS, and our preliminary experiments suggest that this scheme is competitive among existing post-quantum ring signatures.

We now explain these in more detail.

Results for the GMW-FS design. In the following, we always let G denote a group, S a set, and $\alpha : G \times S \to S$ a group action.

Security in the quantum random oracle model. The quantum random oracle model (QROM) was proposed by Boneh et al. [16] 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 [16]. Indeed, the QROM security of the Fiat-Shamir transformation was only recently shown after a series of works [74,52,55,33].

In this paper we make progress on the QROM security of the GMW-FS design based on the works [74,52,55,33]. Our results on this line can be informally summarised as follows.

Recall that $\alpha : G \times S \to S$ is a group action. In the GMW-FS design, the protocol starts with some (chosen or randomly sampled) set element $s \in S$. For $s \in S$, the stabilizer group $\mathrm{Stab}(s) := \{g \in G \mid \alpha(g, s) = s\}$.

1. The GMW-FS scheme is secure in the QROM model, if $\mathrm{Stab}(s)$ is trivial, i.e. $|\mathrm{Stab}(s)| = 1$.
2. The GMW-FS scheme is secure in the QROM model, if the group action under ATFE satisfies the pseudorandom property as defined in [49,2] (see Definition 6), and the non-trivial automorphism hardness property (see Definition 8). In particular, in this setting the security proof is tight.

The GMW-FS-BKP ring signature design. Ring signature, introduced by Rivest, Shamir and Tauman [66], is a special type of digital signature, in which a signer can sign on behalf of a group chosen by him-or-herself, while retaining anonymous within the group. In particular, 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.

A linkable ring signature [54] 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 [69] and e-voting [71].

Beullens, Katsumata and Pintore [12] proposed an elegant way to construct efficient linkable ring signatures from group actions. Their focus was on 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.

While [12] focussed on commutative group actions, their ring signature construction is readily applicable to general group actions. In fact, for our group action framework, the scheme becomes a bit simpler because [12] needs to work with rejection sampling. We call this ring signature design the GMW-FS-BKP design, and describe its construction in Section 5. The linkability property deserves some more discussions there as it calls for some interesting property of pairs of group actions.

Comparisons with some previous works. QROM securities and ring signature schemes have been shown for concrete schemes based on group actions. For example, the QROM security of CSI-FiSh based on the perfect unique response was observed in [13], and the tight QROM security based on a lossy version of CSI-FiSh was shown in [35]. The ring signature scheme in [12] has been shown for the group actions underlying CSI-FiSh [12], LESS [5], and MEDS [27].

Therefore, we view our results above as mostly conceptual, and we aim to make these results convenient for future uses. That is, we distil properties of group actions (pairs) that are key to the QROM security (Definition 8) or for linkable ring signatures (Definition 10). We hope that these will not only help with existing schemes, but also facilitate future schemes based on the GMW-FS design. Furthermore, to the best of our knowledge, the connection of the lossy approach for QROM security [52] with the pseudorandom group action assumption [49,2] and the non-trivial automorphism hardness assumption (Definition 8) was not stated explicitly before. Such results should benefit the LESS and MEDS schemes, which either only briefly touched the QROM security issue [14], or did not address it [27].

Results for the ATFE-GMW-FS scheme. After working with the general GMW-FS design, we focus on the ATFE-GMW-FS scheme from [70].

Updated parameters, improved implementation, and the MPC-in-the-head paradigm. Recently, Beullens [9] presented new algorithms for ATFE which broke some of the parameters proposed in [70] and reduced the security levels for other parameters. We carefully analyse Beullens' methods and propose new parameter sets based on this study.

We then improve the implementation from [70] by incorporating the standard unbalanced challenge technique, together with speeding the group action computation by a factor of 1.75. As a result, our implementation can even achieve smaller public key + signature size for some case than [70], while maintaining the signing and verification quite fast (see Table 2).

Another recent contribution to the GMW-FS design is by Joux [50], who showed that the multiparty-computation (MPC) in the head paradigm can be applied to a generic group action. This paradigm allows for shorter signature sizes at the cost of longer computation time, and the ATFE-GMW-FS scheme is a nice example to which such a tradeoff can bring benefits. Our calculation suggests that this has the effect of reducing the signature size by about one third (comparing Table 2 and Table 3).

The QROM security of the ATFE-GMW-FS scheme. The QROM security of the ATFE-GMW-FS scheme was briefly discussed in [70] but was left as an open problem. Based on the results from the first part, there are two approaches to show its QROM security: the first is based on the automorphism group order statistics, and the second is based on the pseudorandom group action assumption. The sEUF-CMA security in QROM of ATFE-GMW-FS scheme can be achieved by both two approaches.

For the first approach, we provide experimental results to support that, for certain parameters proposed in [70], a random alternating trilinear form has the trivial automorphism group. This requires us to implement an algorithm for the automorphism group order computation.

For the second approach, the group action under ATFE is pseudorandom or not is an open problem. In [70], some arguments were provided to support that it is. In particular, we do not need to modify the original ATFE-GMW-FS scheme in [70] to attain the security in QROM, i.e., as opposed to the lossy CSI-FiSh scheme [35]. We will discuss more about this in Section 1.3.

An implementation of the ATFE-GMW-FS-BKP ring signature scheme. We implement the ring signature protocol from [12] for ATFE-GMW-FS. Preliminary experiment results suggest that it's more balanced than Calamari and Falafl in terms of signature size and signing time. We refer the reader to Section 6.5 and Table 1 for the details. Here we give a brief summary and comparison with some previous ring signature schemes.

Since we use the construction in [12], the signature size of our schemes only depends on $\log R$, where R denotes the ring size. We see that our signature size can be estimated as $0.8 \log R + 8$KB, while the signature sizes of Calamari and Falafl in [12] 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 10.5KB, while Falafl and Calamari have the signature size of 30KB and 5.4KB respectively. RAPTOR [56], and DualRing-LB [76] 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. Regarding MRr-DSS [8], while it performs well for low to medium users ($<= 2^7$), our protocol can outperform it in this range. Recently, Barenghi et al. [6] adapted the same idea but instantiated the group action via the code equivalence problem. Our protocol still outperform it in the regime of Table 1. Finally, Fig 1 reports the signing time of our protocol. Note that the signing time is measured on 2.4 GHz Quad-Core Intel Core i5.

1.3 Discussions

Discussions on QROM security. The QROM security for the GMW-FS design was shown based on perfect unique responses and lossy schemes. There is one further approach which could avoid analysing automorphism groups mathematically. In [55,33], a property called *quantum unique response* in [33] or collapsing

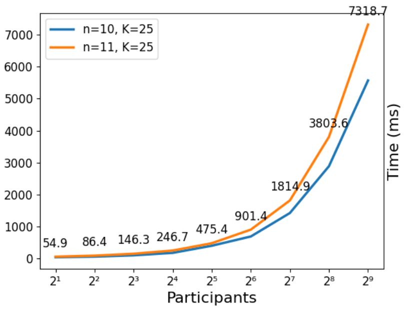

Fig. 1. Signature generation time

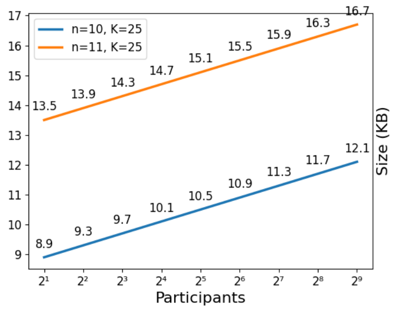

Fig. 2. Signature size

	R					Hardness	Secuirty
	2^1	2^3	2^6	2^{12}	2^{21}	assumption	level
MatRiCT [36]	/	18	19	59	/	MSIS, MLWE	NIST 1
RAPTOR [56]	2.5	10	81	5161	/	NTRU	100 bits
Calamari [12]	3.5	5.4	8.2	14	23	CSIDH-512	*
Falafl [12]	29	30	32	35	39	MSIS, MLWE	NIST 1
Falafl for 2 [12]	49	50	52	55	59	MSIS, MLWE	NIST 2
DualRing-LB [76]	/	4.6	6	106.6	/	MSIS, MLWE	NIST 1
MRr-DSS [8]	/	27	36	422	/	MinRank	NIST 1
LESS [6]	/	10.8	13.7	19.7	28.6	Code Equiv.	NIST 1
Ours	8.9	10.5	12.9	17.7	24.9	ATFE	NIST 1

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

sigma protocol in [55] is introduced, generalising the *collapsingness* which introduced by Unruh [73] 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. 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 [35] is the diagonal action of the class group on two elliptic curves following [68]. One reason is that for the pseudorandom group action assumption [49] (cf. Section 2.4) 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, we compare the GMW-FS-BKP design applied to ATFE here with that of the class group action [12]. 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, though the signature sizes are larger.

Concurrent Work. Recently, D'Alconzo and Gangemi [31] obtained a ring signature from ATFE by also following the construction in [12]. 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 $\beta(g,s) = \alpha(g^{-1},s)$ while our associated group action is $\beta(g,s) = \alpha(g^{-t},s)$. 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 $\{1,\ldots,k\}$.

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 queried 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.,* $\Pr[\mathsf{Verify}(\mathsf{pk}, m, \sigma) = 1 \wedge m \notin \Sigma | (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n),\ \sigma \leftarrow \mathcal{A}(\mathsf{pk}, m)] \leq \mathsf{negl}(\lambda)$*, where Σ is the list of all messages that $\mathcal{A}$ has queried before.*

A stronger notion is *strongly unforgeable* (sEUF-CMA) that allows an adversary $\mathcal{A}$ to output a different signature of a message which has been queried before. The schemes presented in this paper satisfy this stronger notion of unforgeability.

Definition 4 (Stronger Security). *The signature scheme is said to be strongly unforgeable (i.e., sEUF-CMA secure) if for any poly-time quantum adversaries $\mathcal{A}$, who has queried a number of signatures of messages of his choices, the probability that $\mathcal{A}$ can sign a message that the corresponding message-signature pair hasn't been seen 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 queried before.*

Fiat-Shamir transformation. The Fiat-Shamir transformation [40] 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 $H : \{0,1\}^* \rightarrow \mathsf{ChSet}$ is a secure hash function.
  - Run $r \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{pk}, a, c)$.
  - Return a signature $\sigma := (a, r)$.
- $\mathsf{Ver}(\mathsf{pk}, M, \sigma)$: On input a message M and a signature σ, do the following:
  - Compute $c := H(M\|a)$.
  - Return $\mathcal{V}(\mathsf{pk}, a, c, r)$.

Theorem 1 ([62]). *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 5 (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 $b \leftarrow_R \{0,1\}$. 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 $\mathsf{RS.Sign}(\mathsf{sk}_{i_b}, \mathsf{R}, \mathsf{M}) \to \sigma$ 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 Abstract group actions in cryptography

Let G be a group and S be a set. A group action is a function $\alpha : G \times S \to S$ satisfying certain natural axioms. There are several frameworks of group actions in cryptography [22,29,49,2], which are mostly the same but can be different in some details. In this paper, we use the following model.

Some notation. Let $\alpha : G \times S \to S$ be a group action. For $s \in S$, its *orbit* under α is $\mathcal{O}(s) := \{t \in S \mid \exists g \in G, \alpha(g, s) = t\}$, and its *stabilizer group* under α is $\mathrm{Stab}(s) = \{g \in G \mid \alpha(g, s) = s\}$. An element in $\mathrm{Stab}(s)$ is called an *automorphism* of s. By the orbit-stabilizer theorem, $|\mathcal{O}(s)| \cdot |\mathrm{Stab}(s)| = |G|$.

Computational assumptions. We first make the following computational assumptions for using a group action in algorithms.

1. We work with group families $G = \{G_k\}_{k\in\mathbb{N}}$ and set families $S = \{S_k\}_{k\in\mathbb{N}}$.
2. For a fixed k, G_k and S_k are finite, where $|G_k| = N_k$ and $|S_k| = M_k$, and $\log N_k$ and $\log M_k$ are upper bounded by some polynomial in k.
3. The following tasks can be done in time polynomial in k: computing group product and inverse, deciding the equivalence of group elements, computing the group action function, and uniformly sampling group and set elements.

In the following, when k is clear from the context, we may just write G and S, and set $|G| = N$ and $|S| = M$.

We note that it is not necessary for a group action to satisfy all the above to be useful in cryptography. For example, the group action underlying CSIDH [25] cannot be efficiently computed for all group elements, though it can be modelled as a "restricted effective group action" as in [2].

Cryptographic assumptions. We now list the following assumptions for a group action to be useful in cryptography. Let $\alpha : G \times S \to S$ be a group action. Given $s \in S$, we shall often use the fact that we can sample from $\mathcal{O}(s)$ uniformly. This is because we can uniformly sample $g \in G$ and return $\alpha(g, s)$.

1. One-way assumption: for $s \leftarrow_R S$ and $t \leftarrow \mathcal{O}(s)$, there is no probabilistic or quantum polynomial-time algorithm that returns g' such that $\alpha(g', s) = t$.
2. Pseudorandom assumption: there is no probabilistic or quantum polynomial-time algorithm that can distinguish the following two distributions with non-negligible probability:
   (a) The random distribution: $(s, t) \in S \times S$ where $s, t \leftarrow_R S$.
   (b) The pseudorandom distribution: $(s, t) \in S \times S$ where $s \leftarrow_R S, t \leftarrow_R \mathcal{O}(s)$.

The above assumptions can be generalised to the following K-instance version.

Definition 6. *Let $\alpha : G \times S \to S$ be a group action.*

1. *We say that α satisfies the C-*one-way assumption*, if for $s_0 \leftarrow_R S$, given s_0 and $s_1, \ldots, s_{C-1} \leftarrow_R \mathcal{O}(s_0)$, there is no probabilistic or quantum polynomial-time algorithm that returns g', $i, j \in \{0, 1, \ldots, C-1\}$, $i \neq j$, such that $\alpha(g', s_i) = s_j$, with non-negligible probability.*
2. *We say that α satisfies the C-*pseudorandom assumption*, if there is no probabilistic or quantum polynomial-time algorithm that can distinguish the following two distributions with non-negligible probability:*
   (a) The random distribution: $(s_0, \ldots, s_{C-1}) \in S^C$ where $s_i \leftarrow_R S$.
   (b) The pseudorandom distribution: $(s_0, \ldots, s_{C-1}) \in S^C$ where $s_0 \leftarrow_R S$, and $s_1, \ldots, s_{C-1} \leftarrow_R \mathcal{O}(s_0)$.

Remark 1. These assumptions can also be restricted to the versions that work with a fixed s_0 rather than a random one. That is, in the above, replace $s_0 \leftarrow_R S$ with a fixed choice $s_0 \in S$. We shall call these C-one-way-$\mathcal{O}(s_0)$ and C-pseudorandom-$\mathcal{O}(s_0)$ assumptions, respectively.

The GMW-FS digital signature design. Let $\alpha : G \times S \to S$ be a group action. As mentioned in Section 1, we can obtain a digital signature by applying the Fiat-Shamir (FS) transformation to the Goldreich-Micali-Wigderson (GMW) zero-knowledge protocol instantiated with the group action α, assuming that the group action satisfies the C-one-way assumption. We call this digital signature the $\alpha(\mathsf{G}, \mathsf{S})$-GMW-FS scheme.

For our purposes in this paper, the key is the GMW protocol instantiated with α with the C-one-way assumption. This protocol is easily interpreted as an identification protocol, and we shall refer it as the $\alpha(\mathsf{G},\mathsf{S})$-GMW protocol. Therefore, we describe the $\alpha(\mathsf{G},\mathsf{S})$-GMW protocol in detail.

In the $\alpha(\mathsf{G},\mathsf{S})$-GMW protocol, the public key consists of set elements $s_0, \ldots, s_{C-1}$ such that $s_0 \leftarrow_R S$, and $s_1, \ldots, s_{C-1} \leftarrow_R \mathcal{O}(s_0)$. The private keys consists of $g_0 = \text{id}, g_1, \ldots, g_{C-1}$ such that $\alpha(g_i, s_0) = s_i$. In this protocol, the goal of the prover is to convince the verifier that, for every $i \neq j$, the prover knows some h such that $\alpha(h, s_i) = s_j$.

Define the relation $R := \{x = \{s_0, \ldots, s_{C-1}\}, w = \{g_1, \ldots, g_{C-1}\} \mid x \subseteq S, w \subseteq G, \alpha(g_i, s_1) = s_i, \forall i \in \{1, \ldots, C-1\}\}$. The protocol is described in Figure 3; it needs to be repeated several times to attain the required security level.

$\mathcal{P}(s_0, \ldots, s_{C-1}, g_0 = \text{id}, g_1, \ldots, g_{C-1})$		$\mathcal{V}(s_0, \ldots, s_{C-1})$
$h \in_R G$		
$t = \alpha(h, s_0)$	$\xrightarrow{t}$	
	$\xleftarrow{c}$	$c \leftarrow_R \{0, \ldots, C-1\}$
Set $f := h * g_c^{-1}$	$\xrightarrow{f}$	Check if $\alpha(f, s_c) = t$?

Fig. 3. The $\alpha(\mathsf{G},\mathsf{S})$-GMW protocol.

It is known that $\alpha(\mathsf{G},\mathsf{S})$-GMW protocol in Figure 3 has the following properties (see e.g. [70]): completeness, post-quantum 2-soundness, HVZK, min-entropy, and commitment recoverable. We provide some proof sketches for completeness in Appendix A.2.

The $\alpha(\mathsf{G},\mathsf{S})$-*GMW-FS-*$\mathcal{O}(s)$ *scheme.* In Section 3, we will need a variant of the $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s)$ scheme, following Remark 1. Briefly speaking, this variant restricts to an orbit of some specific $s \in S$ instead of working in the orbit of a random $s \leftarrow_R S$. We call such a scheme the $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s)$ scheme.

2.5 Some candidates of group actions for the GMW-FS design

The group action in [70]. Let $\mathbb{F}_q$ be the finite field of order q. A trilinear form $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is *alternating*, if ϕ evaluates to 0 whenever two arguments are the same. We use $\text{ATF}(n, q)$ 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 $(\phi \circ A)(u, v, w) := \phi(A^t(u), A^t(v), A^t(w))$. This yields a group action of $\mathrm{GL}(n, q)$ on $\mathrm{ATF}(n, q)$ used in [70].

The group action underlying LESS. For $1 \leq d \leq n$, let $\mathrm{M}(d \times n, \mathbb{F}_q)$ be the linear space of $d \times n$ matrices over $\mathbb{F}_q$. Let $\mathrm{Mon}(n, q)$ be the group of $n \times n$ monomial matrices over $\mathbb{F}_q$. The group $G = \mathrm{GL}(n, q) \times \mathrm{Mon}(n, q)$, the set $S = \mathrm{M}(d \times n, \mathbb{F}_q)$, and the action is defined as $(A, C) \in \mathrm{GL}(n, q) \times \mathrm{Mon}(n, q)$ sending $B \in \mathrm{M}(d \times n, q)$ to ABC^t.

The group action underlying MEDS. Let $n_1, n_2, n_3 \in \mathbb{N}$. The set S is $\mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2} \otimes \mathbb{F}_q^{n_3}$. The group $G = \mathrm{GL}(n_1, q) \times \mathrm{GL}(n_2, q) \times \mathrm{GL}(n_3, q)$. The action is defined as $(A_1, A_2, A_3) \in G$ sending $u_1 \otimes u_2 \otimes u_3$ to $A_1(u_1) \otimes A_2(u_2) \otimes A_3(u_3)$, and then linearly extending this to the whole $\mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2} \otimes \mathbb{F}_q^{n_3}$.

The class group action such as CSIDH (for SeaSign and CSI-FiSh). Let E be an elliptic curve over $\mathbb{F}_p$, and let $O := \mathrm{End}_{\mathbb{F}_p}(E)$. The ideal class group $\mathrm{Cl}(O)$ acts on the set of $\mathbb{F}_p$-isomorphism classes of elliptic curves with $\mathbb{F}_p$-rational endomorphism ring O via a natural action. For details we refer the reader to [39,13,11]. Note that this action does not satisfy all the properties in Section 2.4; see [2].

Further group actions in cryptography. We note that more isomorphism problems and group actions have been proposed for cryptographic uses, such as lattice isomorphism [34] and knot equivalence [37]. While these are interesting, we did not discuss these here, because they have not been used with the GMW-FS design which is the focus on this paper.

3 QROM security via perfect unique responses

In this section, we show that the $\alpha(\mathsf{G}, \mathsf{S})$-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 $\alpha(\mathsf{G}, \mathsf{S})$-GMW protocol to certain properties about stabilizer groups. In Section 3.3, we formally state Theorem 2 QROM security of the $\alpha(\mathsf{G}, \mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ scheme, with proof sketches in Appendices C and D.

3.1 Preliminaries on QROM

The random oracle model (ROM) was first proposed in 1993 by Bellare and Rogaway in [7] 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) [16]. 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 [16,75] .

Recently, thanks to a pair of breakthrough papers [33,55], the QROM security of the Fiat-Shamir transform is now much better understood. Based on these papers, we study the relation between the $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW}$ scheme and the *perfect unique response* property introduced by Unruh [72]. With this important property and some additional properties stated in Appendix A.2, we can prove the security of the $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW}$ protocol under quantum ROM.

3.2 Perfect and computationally unique responses of the $\alpha(\mathsf{G},\mathsf{S})$-GMW protocol

We require some extra properties such that the $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW}$ or $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW}$-$\mathcal{O}(s_0)$ protocols in Appendix A.2 meet the *perfect unique response* and *computationally unique response* properties.

Lemma 1 (Perfect Unique Response). *The $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ protocol supports perfect unique response iff* $\mathrm{Stab}(s_0)$ *is trivial.*

Proof. To prove the completeness, assume that $\mathrm{Stab}(s_0)$ is trivial. If there are two valid transcripts (t, c, g_1) and (t, c, g_2) for the protocol in Figure 3. Then we have $\alpha(g_1, t) = \alpha(g_2, t)$. It implies that $g_2 * g_1^{-1} \in \mathrm{Stab}(s_0)$ and thus $g_1 = g_2$.

For the soundness, assume that the $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW}$-$\mathcal{O}(s_0)$ protocol satisfies the perfect unique response property. If $\mathrm{Stab}(s_0)$ is non-trivial, i.e., there exists a group element $h \neq \mathrm{id}$ such that $\alpha(h, s_0) = s_0$. Therefore, all the elements in $\{s_0, \ldots, s_{C-1}\}$ satisfy $\alpha(h, s_i) = s_i$. It follows that for the statement $\{s_0, \ldots, s_{C-1}\}$, any commitments $t \in S$, and any challenge $c \in \{0, 1, \ldots, C-1\}$, there are two different responses $g \in G$ and $h * g \in G$ such that (t, c, g) and $(t, c, h * g)$ are valid transcripts, which is a contradiction. □

Remark 2. For the $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW}$, since s_0 is not fixed, in general we can only say that the stabilizer group of a random $s_0 \leftarrow_R S$ is trivial with high probability. This is called the statistical unique response property. 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 group actions, we define the following algorithm problem.

Definition 7. *The $\alpha(\mathsf{G},\mathsf{S})$-stabilizer problem is the following.*

Input: *An element $s \in_R S$.*

Output: *Some $g \in G, g \neq \mathrm{id}$ such that $s = \alpha(g, s)$.*

The $\alpha(\mathsf{G}, \mathsf{S})$-stabilizer problem is also known as the automorphism group problem in the literature (see e.g. the graph automorphism problem [53]).

Lemma 2 (Computationally Unique Response). *The $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$ protocol in Figure 3 supports computationally unique response iff no poly-time quantum algorithm can solve the $\alpha(\mathsf{G}, \mathsf{S})$-stabilizer problem in Definition 7 with a non-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 $x = \{s_0, \ldots, s_{C-1}\} \subseteq S$, it can compute two valid transcripts (t, c, g_1) and (t, c, g_2), where $g_1 \neq g_2$, with a non-negligible probability. Then there is an algorithm $\mathcal{A}_1$ using $\mathcal{A}$ as subroutine such that for any $c \in \{0, 1, \ldots, C-1\}$, it can produce an $h = g_2 * g_1^{-1}$ such that $\alpha(h, s_c) = s_c$ with a non-negligible probability.

Assume that no poly-time quantum algorithm can solve the $\alpha(\mathsf{G}, \mathsf{S})$-stabilizer problem with a non-negligible probability. If there is a poly-time quantum algorithm $\mathcal{A}_1$ such that, for any $s \in S$, it produces a stabilizer element h such that $\alpha(h, s_c) = s_c$ with a non-negligible probability. By the HVZK property, there exists a simulator $\mathcal{S}$ such that, for any $x = \{s_0, \ldots, s_{C-1}\} \subseteq S$, it produces a valid transcript (s, c, g). Then there is an adversary $\mathcal{A}$ using $\mathcal{A}_1$ and $\mathcal{S}$ as subroutines such that it firstly computes a valid transcript (s, c, g) by $\mathcal{S}$, and then computes h such that $\alpha(h, s_c) = s_c$ by $\mathcal{A}_1$. Thus, for any statement $\{s_0, \ldots, s_{C-1}\}$, $\mathcal{A}$ computes two transcripts (s, c, g) and $(s, c, h * g)$ with a non-negligible probability. □

Remark 3. For a fixed $s_0 \in S$, we can define the $\alpha(\mathsf{G}, \mathsf{S})$-stabilizer-$\mathcal{O}(s_0)$ problem by restricting the input to $s \in_R \mathcal{O}(s_0)$. Then the above proof can be applied to show the same result for $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$-$\mathcal{O}(s_0)$.

Based on the above, we define the following properties of group actions.

Definition 8. *Let $\alpha : G \times S \to S$ be a group action.*

1. *We say that α satisfies the (statistical) trivial stabiliser assumption, if for a random $s \in S$, $\mathrm{Stab}(s)$ is trivial.*
2. *We say that α satisfies the non-trivial automorphism hardness assumption, if no probabilistic or quantum polynomial-time algorithm can solve the $\alpha(\mathsf{G}, \mathsf{S})$-stabilizer problem with non-negligible probability.*

3.3 QROM security via perfect unique response

Lemma 1 interprets the perfect unique response property as a property of group actions. Based on this, it is easy to adapt the results in [55] to give a security proof in QROM for $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$-$\mathsf{FS}$-$\mathcal{O}(s_0)$ signature scheme assuming the stabilizer group being trivial.

Theorem 2. *Suppose $s_0 \in S$ satisfies that $\mathrm{Stab}(s_0)$ is trivial. The $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ signature based on the t repetitions of $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ protocol has 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 $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ signature, there is a quantum adversary $\mathcal{B}$ for C-one-way-$\mathcal{O}(s_0)$ problem such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\alpha(\mathsf{G},\mathsf{S})-\mathit{EUF\text{-}CMA}} \leq O\left({Q_H}^9 \cdot \left(\mathsf{Adv}_{\mathcal{B}}^{C-one-way-\mathcal{O}(s_0)}\right)^{\frac{1}{3}}\right).$$

For readers' convenience, we present a proof of Theorem 2 in Appendix C. Another proof with different parameters based on [33] is in Appendix D.

Remark 4. The EUF-CMA security in QROM here can be strengthened to the sEUF-CMA security by assuming the computationally unique response property[52, Theorem 3.2]. Since we assume that the stabilizer group is trivial (perfect unique response) which implies the computationally unique response, $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ signature here is sEUF-CMA secure.

4 QROM security via lossy schemes

4.1 Definitions and previous results

In this section, we recall the definition of lossy identification protocol [1,35] and a security result of its associated Fiat-Shamir signature in QROM from [52].

Definition 9. *An identification protocol ID is called lossy, denoted by $\mathsf{ID}_{\mathsf{ls}}$, if it has one additional PPT algorithm* LossyGen*, called lossy key generation 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

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

is negligible.

Statistical lossy soundness. Consider following experiment $\mathsf{Exp}_{\mathsf{ID},\mathcal{A}}^{\mathsf{ls}}(\lambda)$ 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 [52,55,33].

Theorem 3 ([52, Theorem 3.1]). *Assume that the identification protocol ID is lossy, perfect HVZK, has α bits of min-entropy, and it is ϵ_{ls}-lossily 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 a quantum adversaries $\mathcal{B}$ against the lossiness and $\mathcal{C}$ against the computation unique response such that*

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

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

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

4.2 Lossy identification protocol from abstract group actions

In this section, we define a lossy identification protocol based on the K-pseudorandom assumption in Definition 6. The underlying sigma protocol is the $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$ protocol in Figure 3. Here, we consider a relation $\mathcal{R}$ consisting of statement-witness pairs (x, w) with $x = \{s_0, s_1, \ldots, s_{C-1}\} \subseteq S$ and $w = \{g_1, \ldots, g_{C-1}\} \subseteq G$, where $\alpha(g_i^{-1}, s_0) = s_i$ for each $i \in [C-1]$.

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

- Algorithm IGen randomly samples an element $s_0 \in S$ and group elements $g_1, \cdots, g_{C-1} \in_R G$. It outputs a statement $x = (s_0, s_1, \cdots, s_{C-1})$ with $s_i = \alpha(g_i^{-1}, s_0)$ for $i = 1, \cdots, C-1$, and a witness $w = (g_1, \cdots, g_{C-1})$.
- Algorithm $\mathsf{LossyGen}$ randomly samples set elements $s_0, s_1, \cdots, s_{K-1} \in S$ and outputs a lossy statement $x_{\mathsf{ls}} = (s_0, s_1, \cdots, s_{C-1})$.
- On input a statement-witness pair (x, w), $\mathcal{P}_1$ samples a random group element $h \in_R G$ and outputs the commitment $t = \alpha(h, s_0)$.
- On input (x, w, t, c) where $c \in \{0, 1, \cdots, C-1\}$ is a challenge, $\mathcal{P}_2$ outputs a response $f = h * g_c$.
- On input (x, t, c, f), the verification algorithm $\mathcal{V}$ check whether $t = \alpha(f, s_c)$.

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.

Lemma 3. *Suppose $\alpha : G \times S \to S$ satisfies the C-pseudorandom assumption as in Definition 6. Then the lossy identification protocol satisfies lossy statement indistinguishability.*

Proof. The lossy generator of our protocol just random samples C elements $s_0, s_1, \cdots, s_{C-1} \in_R S$. By the hardness assumption of the C-pseudorandom problem, lossy statements and real statements are indistinguishable. □

Lemma 4. *The lossy identification protocol satisfies statistical ϵ_{ls}-lossy soundness for $\epsilon_{\mathsf{ls}} = \frac{1}{C} \prod_{i=1}^{C-1} \frac{A-iB}{A} + \left(1 - \prod_{i=1}^{C-1} \frac{A-iB}{A}\right)$, where $B = |G|$, $A = |S|$.*

Proof. This proof is similar to the proof of [35, Lemma 3.3]. Let $\mathcal{X}$ be the set of the statements such that given a commitment $t \in_R S$, there is only one challenge c resulting in a valid transcript. Consider other commitment t with two valid transcripts (t, c_0, g_0) and (t, c_1, g_1) where these two transcripts satisfy following equations:

$$\alpha(g_0, s_{c_0}) = t$$
$$\alpha(g_1, s_{c_1}) = t$$

It implies that $\alpha(g_0 * g_1^{-1}, s_{c_0}) = s_{c_1}$, i.e., s_{c_0} and s_{c_1} 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 $A \prod_{i=1}^{C-1} (A - i|\mathcal{O}_i|) \geq A \prod_{i=1}^{C-1} (A - iB)$, where $|\mathcal{O}_i|$ is the size of $\mathcal{O}_i$ and $|\mathcal{O}_i| \leq B$. The number of all statements is A^C. Then we can have the probability that a statement is in $\mathcal{X}$: $\Pr[x \in \mathcal{X} \mid x \leftarrow \mathsf{LossyGen}] \geq \prod_{i=1}^{C-1} \frac{A-iB}{A}$. We can obtain the probability that an adversary wins as follows:

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

This completes the proof. □

Lemma 4 implies the following for a t parallel repetition of the lossy identification protocol.

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 $\epsilon_{\mathsf{ls}} = \frac{1}{C^t} \prod_{i=1}^{C-1} \frac{A-iB}{A} + \left(1 - \prod_{i=1}^{C-1} \frac{A-iB}{A}\right)$, where $B = |G|$, $A = |S|$.*

4.3 Tightly secure signature scheme in QROM from abstract group actions

A digital signature scheme can be obtained by applying the Fiat-Shamir transformation to the lossy identification protocol in Section 4.2. We call this the $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW\text{-}FS\text{-}lossy}$ scheme. Note that this result is essentially the same scheme as the $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW\text{-}FS}$ scheme, as the additional $\mathsf{LossyGen}$ algorithm used for lossy key generation is only used for security analysis.

We now prove the QROM security of $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW\text{-}FS\text{-}lossy}$ based on the C-pseudorandom assumption and the computational unique response assumption as in Lemma 2.

Theorem 4. *For any quantum adversary $\mathcal{A}$ against the $\mathsf{sEUF\text{-}CMA}$ security of $\alpha(\mathsf{G},\mathsf{S})$-$\mathsf{GMW\text{-}FS\text{-}lossy}$ that issues at most Q_H queries to the quantum random oracle, there exists a quantum adversary $\mathcal{B}$ against the C-pseudorandomness (Definition 6), a quantum adversary $\mathcal{C}$ against the $\alpha(\mathsf{G},\mathsf{S})$-stabilizer problem (Definition 7) such that*

$$\begin{aligned}
&\mathsf{Adv}_{\mathcal{A}}^{\alpha(\mathsf{G},\mathsf{S})\text{-}\mathsf{GMW\text{-}FS\text{-}lossy}-\mathsf{sEUF\text{-}CMA}(\lambda)}\\
\leq\ &\mathsf{Adv}_{\mathcal{B}}^{C-pseudorandom}(\lambda)+\frac{2}{|\mathcal{O}|}\\
&+8(Q_H+1)^2\cdot\left(\frac{1}{C^t}\prod_{i=1}^{C-1}\frac{A-iB}{A}+\left(1-\prod_{i=1}^{C-1}\frac{A-iB}{A}\right)\right)\\
&+\mathsf{Adv}_{\mathcal{C}}^{\alpha(\mathsf{G},\mathsf{S})\text{-}\mathsf{Stab}}(\lambda)
\end{aligned}$$

and $\mathsf{Time}(\mathcal{B})=\mathsf{Time}(\mathcal{A})+Q_H\cong\mathsf{Time}(\mathcal{A})$. *Here $|\mathcal{O}|$ is the size of the orbit where elements of the statement $x=(s_0,s_1,\cdots,s_{K-1})$ are in.*

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

Proof. The proof initializes with Lemma 2 and Section 4.2 that the underlying sigma protocol has computational unique response, lossiness, lossy-soundness, perfect HVZK and at least λ bits of min-entropy. The result now follows from Theorem 3. □

5 Linkable ring signatures from abstract group actions

In this section, we describe the construction of linkable ring signatures from abstract group actions. It follows the framework of Beullens, Katsumata and Pintore [12], so we call it the $\mathsf{GMW\text{-}FS\text{-}BKP}$ design. While [12] focussed on commutative group actions, their ring signature construction is readily applicable to general group actions. In fact, for our group action framework, the scheme becomes a bit simpler because [12] needs to work with rejection sampling. This has been observed and applied to LESS [6] and MEDS [27]. Therefore, here we will only briefly describe the main ideas, with a focus on presenting another assumption on group actions to achieve linkability.

The Beullens-Katsumata-Pintore design. Briefly speaking, the $\mathsf{GMW\text{-}FS\text{-}BKP}$ ring signature is obtained by applying the Fiat-Shamir transformation to an OR-Sigma protocol. Here, we describe the base OR-Sigma protocol for an abstract group action. Some optimisation and the security proof are reproduced in Appendix E for the readers' convenience.

Let $g_1, g_2, \ldots, g_N \leftarrow_R G$ be the secret keys, and $s_1 = \alpha(g_1, s_0), \ldots, s_N = \alpha(g_N, s_0)$ be the public keys, Com be a commitment scheme. The base OR-Sigma protocol with *statement* $\{s_0, \ldots, s_N \in S\}$ and *witness* $\{g_I \in G, I \in [N]$ such that $\alpha(g_I, s_0) = s_I\}$, works as follows.

1. First, the prover random sample a group element $h \in G$, and apply it to $s_1, \ldots, s_N$ respectively. Specifically, $t_1 = \alpha(h, s_1), \ldots, t_N = \alpha(h, s_N)$. Then the prover samples $\mathsf{bits}_i \leftarrow_R \{0,1\}^\lambda$ and commits to t_i with $\mathsf{C}_i = \mathsf{Com}(t_i, \mathsf{bits}_i)$. 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.
2. When the verifier receives the commitment, it will randomly sample a challenge $c \leftarrow_R \{0,1\}$ and response it to the prover.
3. If $c = 0$, then the prover computes $f = h * g_I$ and the authenticated path for C_I. The prover sends back a response $\mathsf{rsp} = (f, \mathsf{path}, \mathsf{bits}_I)$. The verifier applies f to s_0 to get $\tilde{t}$ and computes $\tilde{\mathsf{C}} = \mathsf{Com}(\tilde{t}, \mathsf{bits}_I)$. 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 $(h, \mathsf{bits}_1, \ldots, \mathsf{bits}_N)$ to the verifier. This information allows verifier to rebuild a Merkle tree as in step 1, and then check that the roots are consistent.

A more formal description can be found as Figure 4 in Section E.

The linkable property. Linkable ring signatures were first introduced by Liu and Wong [54] 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. The approach in [12] is to first construct a linkable OR sigma protocol and then apply Fiat-Shamir transformation to obtain a linkable ring signature. We describe this construction for general group actions in Appendix F.

Here we only briefly indicate how to construct a linkable OR sigma protocol. For this, we add a tag $r_0 \in S$ associated with a group action $\beta : G \times S \to S$ into the relation. The group action β is defined as $\beta(g, s) = \alpha(g^{-t}, s)$ where t is an involution of G. This tag r_0 is used to track if some secret key is signed more than once. In addition, we restrict the initial public key s_0 is sampled from an orbit $\mathcal{O}(s_0)$ with a trivial automorphism group. By the discussions in Section 6.4, a randomly sampled form s_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,

[7] Note that the Merkle tree used here is slightly modified. It is index-hiding Merkle tree, please see [12, Section 2.6]

we can get a linkable OR sigma protocol shown in the Figure 6. Then we apply the same optimization methods in Section E.1 to this protocol.

A linkable digital signature needs to satisfy linkability, linkable anonymity, and non-frameability (see Appendix F.1). These properties can be translated to properties about group actions as done in [12, Definition 4.2] and also [6,27] (see Definition 14). For example, the linkable anonymity is captured by the following property about group action pairs.

Definition 10. *Let $\alpha, \beta : G \times S \to S$ be two group actions. We say that the (α, β) pair satisfies the* pseudorandom *assumption at $(s_0, r_0) \in S \times S$, if no probabilistic or quantum polynomial-time algorithms can distinguish the following two distributions with non-negligible probability:*

1. *The random distribution: $(s_1, r_1) \in S \times S$, where $s_1, r_1 \leftarrow_R S$.*
2. *The pseudorandom distribution: $(s_1, r_1) \in S \times S$, where $g \leftarrow_R G$, and $s_1 = \alpha(g, s_0)$ and $r_1 = \beta(g, r_0)$.*

Furthermore, if the group actions α and β also satisfy the trivial stabiliser assumption (Definition 8), then the linkability and non-frameability also follow. These together suffice to prove the security of the linkable GMW-FS-BKP design based on the action pair (α, β), as proved in Theorem 13. We note that the above strategy was already used in MEDS [27] for the action underlying the matrix code equivalence problem.

Instantiations of pseudorandom group action pairs. Let $\alpha : G \times S \to S$ be a group action. There are some generic recipes in the literature about finding another action $\beta : G \times S \to S$ so that (α, β) is pseudorandom. In [12], β is constructed as $\beta(g, s) = \alpha(g^2, s)$. In [14,27], β is constructed as $\beta(g, s) = \alpha(g^{-1}, s)$. Note that here β is actually a right action (if α is a left action). It follows that the responses need to involve both gh and hg where h is a random group element and g is the secret.

We note that it is possible to do slightly better than the above, if we have an involution t of G, i.e. an anti-automorphism of order 2. This means that t is an automorphism, $g^t = g$, and $(g * h)^t = h^t * g^t$. We can then define $\beta(g, s) = \alpha(g^{-t}, s)$. In the case of $G = \mathrm{GL}(n, q)$ as of interest in ATFE (and MEDS), this t can be simply taken as the transpose of matrices. This gives a concrete linkable ring signature scheme based on ATFE-GMW-FS-BKP. Of course, further research is required to verify whether this instantiation does give a pseudorandom group action pair.

6 Results for the ATFE-GMW-FS scheme

6.1 New criteria of n and q in light of Beullens' algorithms

In [9], Beullens presented several algorithms for ATFE. We briefly outline some of them here, because they are both crucial and beautiful.

Suppose we want to test equivalence of alternating trilinear forms $\phi, \psi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$. Beullens' results are based on rank statistics of alternating trilinear forms and guided by the some graphs associated with alternating trilinear forms.

Rank statistics. Let $\mathbb{P}(\mathbb{F}_q^n)$ be 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 $\hat{v} := \{u \in \mathbb{F}_q^n \mid u = \alpha \cdot v, \alpha \in \mathbb{F}_q\}$. For $\hat{v} \in \mathbb{P}(\mathbb{F}_q^n)$, let $\mathrm{rk}_\phi(\hat{v})$ be the rank of the bilinear form $\phi_{\hat{v}} := \phi(v, \cdot, \cdot)$. When it is clear from the context, we may just write as $\mathrm{rk}(\hat{v})$.

Let $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be a random alternating trilinear form. That is, each of the $\binom{n}{3}$ coefficients is uniformly randomly sampled from $\mathbb{F}_q$. For given n, q, and $r \in \mathbb{N}$, we are interested in the average number of $\hat{v}$ such that $\phi_{\hat{v}}$ is of rank r. Experimental data of such distributions for small n and q were shown in [70], and [9, Theorem 1] gave formulas for such distributions.

Theorem 5 ([9, Theorem 1]). *Let $\phi \in \mathrm{ATF}(n, q)$ be an alternating trilinear form. Let $d, d_1, d_2 \in [n]$ such that $n - d$, $n - d_1$, $n - d_2$ are even numbers. Let $G(\phi, d) := \{\hat{v} \in \mathbb{P}(\mathbb{F}_q^n) \mid \mathrm{rk}_\phi(\hat{v}) = n - d\}$, and $G(\phi, d_1, d_2) := \{(\hat{v_1}, \hat{v_2}) \mid v_2 \in \ker(\phi_{\hat{v}}), \mathrm{rk}_\phi(\hat{v_1}) = n - d_1, \mathrm{rk}_\phi(\hat{v}) = n - d_2\}$.*

As $q \to \infty$, the average size of $|G(\phi, d)|$ over a uniformly randomly sampled alternating trilinear form ϕ tends to $q^{n-2+(-d^2+3d)/2}$, and the average size of $|G(\phi, d_1, d_2)|$ over a uniformly randomly sampled alternating trilinear form ϕ tends to $q^{n-6+(-d_1^2-d_2^2+5(d_1+d_2))/2}$.

We discovered a part of this theorem independently, so we include a proof in Appendix B.

The low-rank collision approach. Beullens' main algorithm approach may be called the low-rank collision approach. Let $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$. Suppose by Theorem 5, it is expected that there are roughly q^k many $\hat{v} \in \mathbb{P}(\mathbb{F}_q^n)$, such that $\mathrm{rk}_\phi(\hat{v}) = r$.

To test isomorphism from ϕ to ψ, we can first sample $q^{k/2}$ rank-r (projective) points each from ϕ and ψ, and then find a collision, i.e. $(\hat{u}, \hat{v})$ such that the isomorphism $A(\hat{u}) = \hat{v}$, via the Gröbner basis with partial information method[8].

the cost of the low-rank collision attack is of the following form:

$$O(q^{k/2} \cdot \mathsf{samp\text{-}cost} + q^k \cdot \mathsf{col\text{-}cost}).$$

The collision cost $\mathsf{col\text{-}cost}$ can be estimated as $O(n^6)$ by [20]. The sampling cost $\mathsf{samp\text{-}cost}$ refers to the cost of sampling a rank-r (projective) point.

[8] As in [9], the Gröbner basis with partial information method needs to be strengthened as follows. Suppose $v \in \mathbb{F}_q^n$ satisfies that the rank of the bilinear form $\phi_{\hat{v}} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is $r < n$. Then it is sufficient to guess the image of v under the matrix X *up to a scalar*, as the kernel of $\phi_{\hat{v}}$ can be incorporated to provide further information.

The straightforward way to sample a rank-r point is to formulate it as a min-rank problem, but this involves matrices with structures so it is not straightforward to estimate the costs based on current literature of min-rank such as [4]. Beullens' main novel contribution lies in the sampling step, which he called the graph walking method. We note that such graph-theoretic algorithms have been proposed for other similar problems [21].

The graph associated with an alternating trilinear form. 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 $x \in \mathbb{F}_q^n$. 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 [21].

We can then assign labels to the vertices of $G(\phi)$ as follows. 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.

Sampling based on graph walking. To sample a rank-r point $\hat{v}$, Beullens uses the graph walk method. That is, 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 with only $n - r$ matrices. Beullens uses the estimate of min-rank by Bardet et al [4]. 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.

The final algorithm running times. Based on the graph walking method, the sampling cost $\mathsf{samp\text{-}cost}$ for odd n and $r = n-5$ can be estimated as $O(q^2 \cdot n^{11})$, and for even n and $r = n - 4$ can be estimated as $O(n^3)$. Combining with the $O(n^6)$-time algorithm for the Gröbner basis with partial information method [20,70], this leads to an algorithm in time $O(q^{(n-3)/2} \cdot n^{11} + q^{n-7} \cdot n^6)$ for odd n and $r = n - 5$, and $O(q^{(n-4)/2} \cdot n^3 + q^{n-4} \cdot n^6)$ even n and $r = n - 4$. These will be used as our criteria for choosing n and q.

Other algorithms by Beullens. For $n = 9$, Beullens discovered a beautiful structure of the graph $G(\phi)$ restricted to rank-4 points, and devised an algorithm that works in time $O(q)$. This attack completely destroys the choice of $n = 9$.

Based on Theorem 5, Beullens noted that for some n, there are weak keys [9]. Take $n = 10$ as an example. The highest rank in this setting is 8. By Theorem 5, with probability $\sim 1/q$, there is a unique $\hat{v}$ of rank 4. This can then be combined with the Gröbner basis with partial information method, to give a fast algorithm, as the problem completely boils down to find this unique $\hat{v}$.

A new direct Göbner basis attack. Recently, a new formulation of polynomial systems for solving ATFE was proposed in [63], leading to another direct Gröbner basis attack. While this is interesting and timely, it can be verified that all rank-1 matrices and some rank-2 matrices are in the solution space of this system. Furthermore, the semi-regularity assumption seems not hold due to the existence of some syzygies. It is an interesting problem to understand the aftermaths of this nice method better.

6.2 Improvements to the previous implementation

The unbalanced challenge technique. The unbalanced challenge technique is a classical technique which can be traced back to Fiat and Shamir's original paper [40]. The idea is to observe that, in the case of challenge 0, the response would be a random group element which can be expanded from a short seed, so sending the seed reduces the communication. As a result, the number of rounds needs to be increased.

Corollary 2. *The lossy identification protocol based on* ATFE *with the unbalanced challenge, satisfies statistical ϵ_{ls}-lossy soundness for*

$$\epsilon_{\mathsf{ls}} = \frac{1}{(\binom{M}{K}(C-1)^K)} \prod_{i=1}^{C-1} \frac{A-iB}{A} + \left(1 - \prod_{i=1}^{C-1} \frac{A-iB}{A}\right),$$

where $A = |\mathrm{ATF}(n,q)|$, $B = |\,\mathrm{GL}(n,q)|$.

Proof. Since the size of unbalanced challenge space is $\binom{M}{K}(C-1)^K)$, we have that $\Pr[\mathcal{A} \text{ wins} \mid x \in \mathcal{X}] \leq \frac{1}{(\binom{M}{K}(C-1)^K)}$. The result follows the proof for Lemma 4. □

Let M be the round number and K be the number of non-zero challenges. To achieve λ-bit security, we should choose the proper M and K such that $\binom{M}{K} \cdot (C-1)^K \geq 2^\lambda$. Our new public key, private key and signature size in terms of bits are as follows.

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

Speeding up the group action computation. We improve the implementation of group actions in [70]. The new idea is as follows: 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. While not all invertible matrices can be decomposed in such product (without the use of a permutation matrix), the number of matrices not decomposable directly in such product of column matrices is negligible.

An equivalent trick was already used in [70] to generate invertible matrices without having to compute a costly determinant. In [70] 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.

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 reduce the number of field multiplications from $7/4 \cdot n^4$ to $1/2 \cdot n^4$ of 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 the 128-bit security level and present the data in Table 2.

Parameters					Size in Bytes		Time in μs		
n	q	C	M	K	Public key	Signature	Set-Up	Sign	Verify
10	262139($\sim 2^{18}$)	43	50	16	11626	4176	953.0	1436.2	967.4
		19	50	20	5146	5012	451.2	1499.9	948.2
11	131217689($\sim 2^{27}$)	43	50	16	23961	7110	1460.3	2245.4	1483.2
		19	50	20	10596	8679	1631.2	2520.0	1631.2

Table 2. Parameters of 128-bit security

Comparison with the previous implementation. Our improved implementation is more balanced in terms of efficiency and signature size than previous implementations proposed by Tang et al [70]. Due to Beullens' algorithms for ATFE [9], the parameter q needs to be increased. For example, when $n = 10$, we need to take $q = 262139$ instead of $q = 131071$. While the unbalanced challenge technique increases the number of rounds, we reduce the time of group actions in each round. The result is that our implementation can even achieve smaller public key + signature size for $n = 10$ compared to [70, Table 5], while maintaining the signing and verification quite fast. 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 Signature size reduction by the MPC in the head paradigm

The multiparty computation (MPC) in the head paradigm was initially introduced in [48] as a means to enhance the theoretical and asymptotic constructions of zero-knowledge (ZK) protocols. More recently, Joux [50] proposed the application of MPC-in-the-head for creating signatures from isomorphism problems and group actions. By applying MPC-in-the-head, the identification scheme based on group action and additional primitive named *puncturable pseudo-random functions* (puncturable PRFs) are as follows.

Puncturable pseudo-random functions A puncturable PRF family F defined on $[N]$ refers to a PRF family that is indexed by a key K and has a domain of $[N]$. This family satifies the following properties:

- For any given key K and index i, there exists a punctured key K_i^* along with an efficient algorithm $\mathcal{A}$ such that:
$$\forall j \in [N] \backslash \{i\} : \mathcal{A}(K_i^*, j) = F_K(j).$$
- Given the puncturable key K_i^*, the value of F_K at i should be computationally indistinguishable from a randomly chosen value.

Group action based identification scheme using MPC-in-the-head Given an expander Expand and a puncturable PRF family F, where Expand sends the output of F into a group element. Note here we consider there are two set elements $s_0, s_1 \in S$ such that $\alpha(g, s_0) = s_1$ as the public keys. We have the identification scheme as follows.

- The prover randomly chooses a puncturable key K and lets $g^{(i)} = \mathsf{Expand}(F_K(i))$ such that $s^{(i)} = \alpha(g^{(i)}, s^{(i-1)})$ for $i \in [N]$. Note there $s^{(0)} = s_0$. Then the prover sends the hash value $h = H(s^{(1)}||s^{(2)}|| \cdots ||s^{(N)})$ as the commitment.
- The verifier randomly chooses an index $i^* \in [N]$ and sends back to the prover.
- The prover responses the puncturable key K_i^* and the offset map g^{Δ} such that $g^{\Delta} * g^{(N)} * g^{(N-1)} * \cdots * g^{(1)} = g$.
- The verifier can efficiently generate $g^{(j)}$ for $j \in [N] \backslash i^*$. Then the verifier computes all $s^{(i)}$ by forward computation from $s^{(0)}$ up to $s^{(i^*-1)}$ and by a backward computation from $s^{(N)}$ down to $s^{(i^*)}$. Finally he checks the commitment h.

This protocol has a soundness of $\frac{1}{2N}$. If we enlarge the public key size to C set elements then we have a soundness of $\frac{1}{N(C-1)}$.

Reducing the signature size As mentioned above, the new identification scheme have a soundness of $\frac{1}{N(C-1)}$ if the public key consists of C set elements. Thus we need $\lambda = M \cdot \log_2(N(C-1))$ instead of $\lambda = M \cdot \log_2 C$ to achieve λ bit security. The new signature consists of a puncturable key and round number of offset map along with the challenge. The size (in terms of bit) of the signature evaluate as follows:

$$3\lambda + M \cdot \lambda \cdot \log_2 N + M \cdot [\text{the bitsize of group elements}].$$

Of course it's possible to extend the $N(C-1)$ to $N(C-1)+1$ options. The extra option is actually of revealing the unpuncturable key without revealing the offse map. Thus in this case, unbalanced challenge space is applied. We need $\lambda = \log_2(\binom{M}{K}(N(C-1))^K)$ to achieve λ bit security. By applying the unbalanced challenge, the size (in terms of bit) of the signature evaluate as follows:

$$3\lambda + \lambda \cdot (M - K) + K \cdot [\text{the bitsize of group elements}].$$

Parameters					Size in Bytes	
n	q	C	M	K	pubkey size	sig size
10	$262139(\sim 2^{18})$	43	50	19	11626	3019
		19	54	12	5146	3404
11	$131217689(\sim 2^{27})$	43	50	19	23961	5036
		19	54	12	10596	5604

Table 3. Parameters of 128-bit security with the MPC-in-the-head paradigm for $N = 10$.

New parameter set based on MPC-in-the-head For the optimization by MPC-in-the-head, we consider the security level 128-bit as shown in Table 3. Here we set the N to be 10. Compared with the data in Table 2, we can see that the signature sizes in Table 3 are between 64% to 72% of the sizes in Table 2.

6.4 The QROM security of the ATFE-GMW-FS scheme

Based on the results in Sections 3, there are two approaches to show the QROM security of the ATFE-GMW-FS scheme.

QROM security via perfect unique response. 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. Recall that $\mathrm{Stab}(\phi) := \{A \in \mathrm{GL}(n, q) \mid \phi \circ A = \phi\}$.

By Lemma 1, the ATFE-GMW-FS-$\mathcal{O}(\phi)$ is secure in the quantum model, if $\mathrm{Stab}(\phi)$ is trivial. To decide whether $\mathrm{Stab}(\phi)$ is trivial or not is a difficult algorithmic problem; see [70, Section 3.2] for a discussion. Still, we make progress by running experiments for those n of interest in our context.

Basic facts about $\mathrm{Stab}(\phi)$. First, note that if $3|q-1$, then $\mathrm{Stab}(\phi)$ 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 [28,59,46]. Third, for $n = 9$ and $q = 2$, by the classification of alternating trilinear forms [47], 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.

A Magma program to compute the stabilizer group order. We implemented a program in Magma [18] for computing automorphism group orders of alternating trilinear forms as follows.

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 $\mathrm{Stab}(\phi)$.

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 [38,19,20,21]. 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 [23]. The way we set up the equations is from [70].

Report on the results. Our experiment results are as follows.

- For $q = 2$ and $n = 9$, out of 100 samples there are three ones with trivial stabilizer groups. This is consistent with the fact that there exists exactly one orbit of alternating trilinear forms [47], so 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 stabilizer groups.
- For $q = 3$ and $n = 10, 11$, all 10 samples return trivial stabilizer 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.

QROM security via lossy schemes. In the above, we presented evidence for the ATFE-GMW-FS scheme to satisfy the perfect unique response property for $n \geq 10$, supporting its QROM security by the results in Section 3. However, the reduction in this approach is not tight. Instead, the QROM security via the lossy scheme approach gives a tight reduction.

To apply the results in Section 4 to the ATFE-GMW-FS scheme, we need to examine whether the group action underlying ATFE is pseudorandom. In [70, Conjecture 1], the authors conjectured that this is indeed the case, and provided some supporting evidences, some of which traced back to [49]. Here we briefly explain that, a key argument in [70] is that there seem no easy-to-compute isomorphism invariants for ATFE, as such isomorphism invariants can be used to distinguish non-equivalent alternating trilinear forms.

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

6.5 An implementation of the ATFE-GMW-FS-BKP ring signature scheme

We implement the GMW-FS-BKP ring signature design based on ATFE. Here, we report the formulas for calculating the parameters, and preliminary experiment results. Some comparisons with known ring signature schemes were presented in Section 1.2.

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.

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

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. Furthermore, Table 5 illustrates the signature generation time for our schemes. Our constructions are implemented and measured on a 2.4 GHz Quad-Core Intel Core i5.

Acknowledgement. We would like to thank Ward Beullens, Monika Trimoska, and Lars Ran for their help with understanding their algorithms for ATFE.

Parameters				Size in Bytes				
				R				
n	q	M	K	2^1	2^3	2^6	2^{12}	2^{21}
10	262139($\sim 2^{18}$)	850	25	8873	10473	12873	17673	24873
11	131217689($\sim 2^{27}$)	850	25	13457	15057	17457	22257	29457

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

Parameters				Time in μs						
				R						
n	q	M	K	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 5. 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 D. Pointcheval and T. Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 572–590. Springer, 2012.
2. N. Alamati, L. D. Feo, H. Montgomery, and S. Patranabis. Cryptographic group actions and applications. In S. Moriai and H. Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 411–439. Springer, 2020.
3. L. Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 684–697, 2016.
4. M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. A. Perlner, D. Smith-Tone, J. Tillich, and J. A. Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In S. Moriai and H. Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 507–536. Springer, 2020.
5. 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.
6. 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.

7. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
8. E. Bellini, A. Esser, C. Sanna, and J. Verbel. Mr-dss–smaller minrank-based (ring-) signatures. In *Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings*, pages 144–169. Springer, 2022.
9. W. Beullens. Graph-theoretic algorithms for the alternating trilinear form equivalence problem. *IACR Cryptol. ePrint Arch.*, page 1528, 2022.
10. W. Beullens, S. Dobson, S. Katsumata, Y.-F. Lai, and F. Pintore. Group signatures and more from isogenies and lattices: Generic, simple, and efficient. In O. Dunkelman and S. Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 95–126, Cham, 2022. Springer International Publishing.
11. W. Beullens, L. D. Feo, S. D. Galbraith, and C. Petit. Proving knowledge of isogenies – a survey. Cryptology ePrint Archive, Paper 2023/671, 2023. `https://eprint.iacr.org/2023/671`.
12. W. Beullens, S. Katsumata, and F. Pintore. Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In S. Moriai and H. Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 464–492. Springer, 2020.
13. W. Beullens, T. Kleinjung, and F. Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In *Advances in Cryptology - ASIACRYPT 2019*, volume 11921 of *Lecture Notes in Computer Science*, pages 227–247. Springer, 2019.
14. J. Biasse, G. Micheli, E. Persichetti, and P. Santini. LESS is more: Code-based signatures without syndromes. In A. Nitaj and A. M. Youssef, editors, *Progress in Cryptology - AFRICACRYPT 2020 - 12th International Conference on Cryptology in Africa, Cairo, Egypt, July 20-22, 2020, Proceedings*, volume 12174 of *Lecture Notes in Computer Science*, pages 45–65. Springer, 2020.
15. D. Boneh. The decision Diffie-Hellman problem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, pages 48–63, 1998.
16. D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.
17. X. Bonnetain and A. Schrottenloher. Quantum security analysis of CSIDH. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 493–522. Springer, 2020.
18. 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).
19. C. Bouillaguet. *Etudes d'hypotheses algorithmiques et attaques de primitives cryptographiques.* PhD thesis, PhD thesis, Université Paris-Diderot–École Normale Supérieure, 2011.

20. C. Bouillaguet, J.-C. Faugère, P.-A. Fouque, and L. Perret. Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In *International Workshop on Public Key Cryptography*, pages 473–493. Springer, 2011.
21. C. Bouillaguet, P. Fouque, and A. Véber. Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In *Advances in Cryptology - EUROCRYPT 2013*, pages 211–227, 2013.
22. G. Brassard and M. Yung. One-way group actions. In *Advances in Cryptology - CRYPTO 1990*, pages 94–107, 1990.
23. P. A. Brooksbank, Y. Li, Y. Qiao, and J. B. Wilson. Improved algorithms for alternating matrix space isometry: from theory to practice. In *28th Annual European Symposium on Algorithms, ESA 2020*, page to appear, 2020.
24. L. Carlitz. Representations by skew forms in a finite field. *Archiv der Mathematik*, 5:19–31, 1954.
25. W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, pages 395–427. Springer, 2018.
26. A. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014.
27. T. Chou, R. Niederhagen, E. Persichetti, T. H. Randrianarisoa, K. Reijnders, S. Samardjiska, and M. Trimoska. Take your meds: Digital signatures from matrix code equivalence. In *Progress in Cryptology - AFRICACRYPT 2023*, 2023. to appear.
28. 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.
29. J. M. Couveignes. Hard homogeneous spaces. *IACR Cryptology ePrint Archive*, 2006.
30. A. Couvreur, T. Debris-Alazard, and P. Gaborit. On the hardness of code equivalence problems in rank metric. arXiv preprint arXiv:2011.04611, 2020.
31. G. D'Alconzo and A. Gangemi. Trifors: Linkable trilinear forms ring signature. *Cryptology ePrint Archive*, 2022.
32. I. Dinur and N. Nadler. Multi-target attacks on the picnic signature scheme and related protocols. In Y. Ishai and V. Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 699–727. Springer, 2019.
33. J. Don, S. Fehr, C. Majenz, and C. Schaffner. Security of the fiat-shamir transformation in the quantum random-oracle model. In A. Boldyreva and D. Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 356–383. Springer, 2019.
34. L. Ducas and W. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In *Advances in Cryptology–EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30–June 3, 2022, Proceedings, Part III*, pages 643–673. Springer, 2022.

35. A. El Kaafarani, S. Katsumata, and F. Pintore. Lossy CSI-FiSh: Efficient Signature Scheme with Tight Reduction to Decisional CSIDH-512. In *Public-Key Cryptography - PKC 2020*, volume 12111 of *Lecture Notes in Computer Science*, pages 157–186. Springer, 2020.
36. 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 *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 567–584, 2019.
37. E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor. Quantum money from knots. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 276–289, 2012.
38. J. Faugère and L. Perret. Polynomial equivalence problems: Algorithmic and theoretical aspects. In *Advances in Cryptology - EUROCRYPT 2006*, pages 30–47, 2006.
39. L. D. Feo and S. D. Galbraith. Seasign: Compact isogeny signatures from class group actions. In Y. Ishai and V. Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, volume 11478 of *Lecture Notes in Computer Science*, pages 759–789. Springer, 2019.
40. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology – CRYPTO 1986*, pages 186–194, 1986.
41. 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.
42. J. A. Grochow and Y. Qiao. On p-group isomorphism: search-to-decision, counting-to-decision, and nilpotency class reductions via tensors. In *36th Computational Complexity Conference*, volume 200 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 16, 38. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2021.
43. J. A. Grochow and Y. Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness. In J. R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*, volume 185 of *LIPIcs*, pages 31:1–31:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.
44. J. A. Grochow, Y. Qiao, and G. Tang. Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. In *The 38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021*, page to appear, 2021. arXiv:2012.01085.
45. S. Hallgren, C. Moore, M. Rötteler, A. Russell, and P. Sen. Limitations of quantum coset states for graph isomorphism. *J. ACM*, 57(6):34:1–34:33, Nov. 2010.
46. J. Hora and P. Pudlák. Classification of 8-dimensional trilinear alternating forms over gf (2). *Communications in Algebra*, 43(8):3459–3471, 2015.
47. J. Hora and P. Pudlák. Classification of 9-dimensional trilinear alternating forms over gf (2). *Finite Fields and Their Applications*, 70:101788, 2021.
48. Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. Zero-knowledge from secure multiparty computation. In *STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 21–30. ACM, New York, 2007.
49. Z. Ji, Y. Qiao, F. Song, and A. Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In D. Hofheinz and A. Rosen, editors, *Theory of Cryptography - 17th International Conference, TCC 2019*, volume 11891, pages 251–281. Springer, 2019.

50. A. Joux. Mpc in the head for isomorphisms and group actions. Cryptology ePrint Archive, Paper 2023/664, 2023. `https://eprint.iacr.org/2023/664`.
51. J. Katz and N. Wang. Efficiency improvements for signature schemes with tight security reductions. In *Proceedings of the 10th ACM conference on Computer and communications security*, pages 155–164, 2003.
52. E. Kiltz, V. Lyubashevsky, and C. Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In *Advances in Cryptology – EUROCRYPT 2018*, pages 552–586. Springer, 2018.
53. J. Köbler, U. Schöning, and J. Torán. *The Graph Isomorphism Problem.* Basel Birkhüser, 1993.
54. J. K. Liu and D. S. Wong. Linkable ring signatures: Security models and new schemes. In O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan, editors, *Computational Science and Its Applications - ICCSA 2005, International Conference, Singapore, May 9-12, 2005, Proceedings, Part II*, volume 3481 of *Lecture Notes in Computer Science*, pages 614–623. Springer, 2005.
55. Q. Liu and M. Zhandry. Revisiting post-quantum fiat-shamir. In A. Boldyreva and D. Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 326–355. Springer, 2019.
56. 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.
57. B. D. McKay. Practical graph isomorphism. *Congr. Numer.*, pages 45–87, 1980.
58. B. D. McKay and A. Piperno. Practical graph isomorphism, II. *J. Symb. Comput.*, 60:94–112, 2014.
59. 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.
60. J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology – EUROCRYPT 1996*, pages 33–48, 1996.
61. C. Peikert. He gives c-sieves on the CSIDH. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 463–492. Springer, 2020.
62. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of cryptology*, 13(3):361–396, 2000.
63. L. Ran, K. Reijnders, S. Samardjiska, and M. Trimoska. Algebraic attack on the alternating trilinear form equivalence problem, 2023. presented at CBCrypto'23.
64. O. Regev. Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760, 2004.
65. K. Reijnders, S. Samardjiska, and M. Trimoska. Hardness estimates of the code equivalence problem in the rank metric. Cryptology ePrint Archive, Paper 2022/276, 2022. `https://eprint.iacr.org/2022/276`.
66. R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold*

Coast, Australia, December 9-13, 2001, Proceedings, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.

67. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
68. A. Stolbunov. *Cryptographic schemes based on isogenies.* PhD thesis, Norwegian University of Science and Technology, 2012.
69. S. Sun, M. H. Au, J. K. Liu, and T. H. Yuen. Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In S. N. Foley, D. Gollmann, and E. Snekkenes, editors, *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*, volume 10493 of *Lecture Notes in Computer Science*, pages 456–474. Springer, 2017.
70. G. Tang, D. H. Duong, A. Joux, T. Plantard, Y. Qiao, and W. Susilo. Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In O. Dunkelman and S. Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 582–612. Springer, 2022.
71. P. P. Tsang and V. K. Wei. Short linkable ring signatures for e-voting, e-cash and attestation. In R. H. Deng, F. Bao, H. Pang, and J. Zhou, editors, *Information Security Practice and Experience, First International Conference, ISPEC 2005, Singapore, April 11-14, 2005, Proceedings*, volume 3439 of *Lecture Notes in Computer Science*, pages 48–60. Springer, 2005.
72. D. Unruh. Quantum proofs of knowledge. In *Advances in Cryptology – Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, April 2012.
73. D. Unruh. Computationally binding quantum commitments. In *Advances in Cryptology – Eurocrypt 2016*, pages 497–527. Springer, 2016.
74. 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.
75. 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.
76. 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.
77. M. Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In A. Boldyreva and D. Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 239–268, Cham, 2019. Springer International Publishing.

A Σ-protocols based on abstract group actions

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 abstract group actions

Completeness. It is clear that the honest prover with statement and witness (x, w) following the $\alpha(\mathsf{G}, \mathsf{S})$-GMW protocol showed in Figure 3 can always convince the honest verifiers.

Post-Quantum 2-Soundness. If there is a poly-time quantum adversary $\mathcal{A}$ with statement $x = \{s_0, \ldots, s_{C-1}\}$ who can compute two valid transcripts (t, c, h) and (t, c', h') where $c \neq c'$. Since $\alpha(h, s_c) = t$ and $\alpha(h', s_{c'}) = t$, the adversary $\mathcal{A}$ can get $f = h^{-1} * h'$ such that $s_c = \alpha(f, s_{c'})$, which is contradicted to the group action one-way assumption.

HVZK. Given a statement $x = \{s_0, \ldots, s_{C-1}\}$, there is a simulator $\mathcal{S}$ first sampling $c \in_R \{0, \ldots, C-1\}$ and $h \in_R G$ and then computing $t = \alpha(h, s_c)$. It follows that (t, c, h) is a valid transcript. Then the distributions of h and c are uniform, and $t = \alpha(h, s_c)$ is uniformly from the orbit where statement x is in. The distribution of $(t, c, h) \leftarrow \mathcal{S}(x)$ is equal to the distribution of real transcripts since the both are uniform distribution on commitments, challenges, and responses.

Min-Entropy. Since commitment t is uniformly taken from the orbit $\mathcal{O}$ which elements of the statement $x = \{s_0, \ldots, s_{C-1}\}$ belong to, the $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$ protocol has α-bit min-entropy with $\alpha = \log_2(|\mathcal{O}|)$ and $|\mathcal{O}|$ is the size of orbit $\mathcal{O}$.

Remark 5. 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 6.4, some results on the automorphism group orders, and therefore orbit sizes, of random alternating trilinear forms will be presented.

Commitment Recoverable. The $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$ protocol is commitment recoverable. In fact, given a challenge c and a response h, there is only one commitment t computed by $t = \alpha(h, s_c)$.

B 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 6 (Carlitz [24]).

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

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 [70, Table 3], only the cases when 100 simulations were done and the characteristic was odd.

The following data in Table 6 are from [70, Table 3].

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 6.

Our formula yields (rounded) the following data in Table 7, which match the data in Table 6 closely.

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 7.

C Proof of Theorem 2

To prove Theorem 2 we first need some preparations.

Post-Quantum ID soundness of $\alpha(\mathsf{G},\mathsf{S})$-$\mathit{GMW}$-$\mathcal{O}(s_0)$ 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 11. *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., the probability*

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

is negligible.

Liu and Zhandry show that post-quantum identification soundness can be satisfied if a Σ-protocol has the weakly collapsing property and some extra properties [55, Theorem 1]. Since the perfect unique response is a stronger property than weakly collapsing property, we can state the result in [55] as follows.

Theorem 7 ([55]). *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,*

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

Corollary 3. *Let $\alpha : G \times S \to S$ be a group action. Suppose we have some $s_0 \in S$ such that $\mathrm{Stab}(s_0)$ is trivial. The t repetitions of $\alpha(\mathsf{G},\mathsf{S})$-$\mathit{GMW}$-$\mathcal{O}(s_0)$ 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 C-one-way-$\mathcal{O}(s_0)$ problem such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\alpha(\mathsf{G},\mathsf{S})-\mathit{ID}} \leq O\left(\left(\mathsf{Adv}_{\mathcal{B}}^{C-one-way-\mathcal{O}(s_0)}\right)^{\frac{1}{3}}\right).$$

Proof. As $\mathrm{Stab}(s_0)$ is trivial, by Lemma 1, the Σ-protocol in Figure 3 has perfect unique response. It also satisfies completeness, 2-soundness, and HVZK in the Appendix A.2. Since the t repetitions of Σ-protocol in Figure 3 has an exponentially large challenge space, we can conclude the proof by Theorem 7. □

Security of $\alpha(\mathsf{G},\mathsf{S})$-*GMW-FS*-$\mathcal{O}(s_0)$ *signature.* Liu and Zhandry [55, 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 [77]. 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 8 ([55], 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,*

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

Corollary 4. *If the t repetitions of $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ protocol showed in Figure 3 has post-quantum ID soundness, then the corresponding Fiat-Shamir signature has* EUF-CMA *security that for any polynomial-time quantum adversary $\mathcal{A}$ querying the quantum random oracle Q_H times against* EUF-CMA *security of $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ signature, there are quantum adversary $\mathcal{B}$ against ID-soundness of $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ protocol such that,*

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

Proof. Assume the t repetitions of Σ-protocol showed in Figure 3 has post-quantum ID soundness. We proved that it has $\log_2(|\mathcal{O}(s_0)|)$ bits min-entropy in Appendix A.2, and $|\mathcal{O}(s_0)| = 2^{\Omega(\lambda)}$. Now we complete the proof utilizing the result of Theorem 8. □

We are now ready to prove Theorem 2.

Proof of Theorem 2. By Corollary 3, we have a Σ-protocol with post-quantum ID soundness. Then the EUF-CMA security can be achieved by Corollary 4. □

D An alternative QROM security proof based on perfect unique response

Theorem 9. *Suppose $s_0 \in S$ satisfies that* $\mathrm{Stab}(s_0)$ *is trivial. The $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ signature based on the t repetitions of $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ protocol in Figure 3 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 $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ signature, there is a quantum adversary $\mathcal{B}$ for C-one-way-$\mathcal{O}(s_0)$ problem such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\alpha(\mathsf{G},\mathsf{S})-\textit{sEUF-CMA}} \leq O\left({Q_H}^2 \cdot \left(\mathsf{Adv}_{\mathcal{B}}^{C-one-way-\mathcal{O}(s_0)}\right)^{\frac{1}{3}}\right).$$

Proof. By Corollary 5, we have a Σ-protocol with post-quantum weakly ID soundness. Then the sEUF-CMA security can be achieved by Corollary 6. □

Post-Quantum weak ID soundness of $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ 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 12. *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.*

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

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

Liu and Zhandry show that post-quantum identification soundness can be satisfied if sigma protocol has weakly collapsing property and extra properties [55, 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 [55].

Theorem 10 ([55], 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,*

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

Corollary 5. *Suppose the stabilizer $\mathrm{Stab}s_0$ is trivial. The t repetitions of $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ 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 $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ Σ-protocol, there is a quantum adversary $\mathcal{B}$ for C-one-way-$\mathcal{O}(s_0)$ problem such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\alpha(\mathsf{G},\mathsf{S})-\textit{wID}} \leq O\left(\left(\mathsf{Adv}_{\mathcal{B}}^{C-one-way-\mathcal{O}(s_0)}\right)^{\frac{1}{3}}\right).$$

Proof. By 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 Appendix A.2. Since t repetitions of Σ-protocol in Figure 3 has an exponentially large challenge space, we complete the proof using the result of Theorem 10. □

Security of $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ 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 [33]. We use their main technology [33, Theorem 8] to preserve the weak ID soundness from underlying protocol to Fiat-Shamir signature.

Theorem 11. *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 EUF-NMA security, there is a static quantum adversary $\mathcal{B}$ against post-quantum weakly ID-soundness of the underlying protocol such that,*

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

proof (sketch). The idea is similar to the proof of the Lemma 12, Corollary 13 and Theorem 21 in [33]. 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 EUF-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 [33] 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. [52] 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 [52].

Theorem 12. *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*

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

Corollary 6. *Suppose* $\mathrm{Stab}(s_0)$ *is trivial. If the t repetitions of* $\alpha(\mathsf{G}, \mathsf{S})$*-GMW-*$\mathcal{O}(s_0)$ *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* $\alpha(\mathsf{G}, \mathsf{S})$*-GMW-FS-*$\mathcal{O}(s_0)$ *signature, there are quantum adversary $\mathcal{B}$ against post-quantum weak ID-soundness of* $\alpha(\mathsf{G}, \mathsf{S})$*-GMW-*$\mathcal{O}(s_0)$ *protocol such that,*

$$\mathsf{Adv}_{\mathcal{A}}^{\alpha(\mathsf{G},\mathsf{S})-\textsf{sEUF-CMA}} \leq O\left({Q_H}^2\right) \cdot \mathsf{Adv}_{\mathcal{B}}^{\alpha(\mathsf{G},\mathsf{S})-\textsf{wID}}.$$

Proof. Assume the t repetitions of Σ-protocol showed in Figure 3 has post-quantum weak ID soundness. The $\alpha(\mathsf{G}, \mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ signature based on it has EUF-NMA security using Theorem 11.

We proved that it has $\alpha = \log_2(|\mathcal{O}(s_0)|)$ bits min-entropy in Appendix A.2, and $|\mathcal{O}(s_0)| = 2^{\Omega(\lambda)}$, and thereby $2^{-\alpha+1}$ is negligible. Since the $\alpha(\mathsf{G}, \mathsf{S})$-GMW-$\mathcal{O}(s_0)$ protocol has perfect unique response, the advantage of adversaries against computationally unique response is 0. Now we complete the proof utilizing the result of Theorem 12 □

E More on the GMW-FS-BKP ring signature design

E.1 Optimization

Following some optimization techniques used in [12], we can have a more efficient OR-Sigma protocol. We just briefly describe the following three techniques, for more details please see [12, 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

```
$\mathcal{P}_1(s_1, \ldots, s_N)$
seed $\leftarrow_R \{0,1\}^\lambda$
$(h, \mathsf{bits}_1, \ldots, \mathsf{bits}_N) \leftarrow \mathsf{PRG}(\mathsf{seed})$
for $i$ from 1 to $N$ do
    $t_i \leftarrow \alpha(h, s_i)$
    $\mathsf{C}_i \leftarrow \mathsf{Com}(t_i, \mathsf{bits}_i)$
$(\mathsf{root}, \mathsf{tree}) \leftarrow \mathsf{MerkleTree}(\mathsf{C}_1, \ldots, \mathsf{C}_N)$
$\mathsf{com} \leftarrow \mathsf{root}$
The prover $\mathcal{P}$ sends the commitment com to the verifier $\mathcal{V}$

$\mathcal{V}_1(\mathsf{com})$
$c \leftarrow_R \{0,1\}$
$\mathsf{cha} \leftarrow c$
The verifier $\mathcal{V}$ sends the challenge cha to the prover $\mathcal{P}$

$\mathcal{P}_2(g_I, I, \mathsf{cha})$
$c \leftarrow \mathsf{cha}$
if $c = 0$ then
    $f \leftarrow h * g_I$
    $\mathsf{path} \leftarrow \mathsf{getMerklePath}(\mathsf{tree}, I)$
    $\mathsf{rsp} \leftarrow (f, \mathsf{path}, \mathsf{bits}_I)$
else
    $\mathsf{rsp} \leftarrow \mathsf{seed}$
The prover $\mathcal{P}$ sends the response rsp to the verifier $\mathcal{V}$

$\mathcal{V}_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, s_0, s_1, \ldots, s_N)$
$(\mathsf{root}, c) \leftarrow (\mathsf{com}, \mathsf{cha})$
if $c = 0$ then
    $(f, \mathsf{path}, \mathsf{bits}) \leftarrow \mathsf{rsp}$
    $\tilde{t} \leftarrow \alpha(f, s_0)$
    $\tilde{\mathsf{C}} \leftarrow \mathsf{Com}(\tilde{t}, \mathsf{bits})$
    $\widetilde{\mathsf{root}} \leftarrow \mathsf{ReconstructRoot}(\tilde{\mathsf{C}}, \mathsf{path})$
    The verifier $\mathcal{V}$ outputs accept if $\widetilde{\mathsf{root}} = \mathsf{root}$, else outputs reject
else
    $\mathsf{seed} \leftarrow \mathsf{rsp}$
    $\widetilde{\mathsf{root}} \leftarrow \mathcal{P}_1((s_1, \ldots, s_N), \mathsf{seed})$
    The verifier $\mathcal{V}$ outputs accept if $\widetilde{\mathsf{root}} = \mathsf{root}$, else outputs reject
```

Fig. 4. OR-Sigma protocol.

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 [32], 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 SeedTree function as Sd, the ReleaseSeeds function as Rls, the 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 $\mathcal{O}_{\mathsf{s}i}$.

```
$\mathcal{P}'_1(s_1, \dots, s_N)$
$\mathsf{seed}_{\mathsf{root}} \leftarrow_R \{0,1\}^{\lambda}$
$\mathsf{salt} \leftarrow_R \{0,1\}^{2\lambda}$
$(\mathsf{seed}_1, \dots, \mathsf{seed}_M) \leftarrow \mathsf{Sd}^{\mathcal{O}_{\mathsf{s}}}(\mathsf{seed}_{\mathsf{root}}, M)$
for $i$ from 1 to $M$ do
    $\mathsf{com_i} \leftarrow \mathcal{P}_1^{\mathcal{O}_{\mathsf{s}i}}((s_1, \dots, s_N), \mathsf{seed}_i)$
$\mathsf{com} \leftarrow (\mathsf{salt}, \mathsf{com}_1, \dots, \mathsf{com}_M)$
$\mathcal{P}$ sends com to $\mathcal{V}$
```

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

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

```
$\mathcal{V}'_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, s_0, s_1, \dots, s_N)$
$(\mathsf{salt}, \mathsf{com}_1, \dots, \mathsf{com}_M) \leftarrow \mathsf{com}$
$\mathbf{c} = (c_1, \dots, c_M) \leftarrow \mathsf{cha}$
$(\mathsf{seeds}_{\mathsf{int}}, \{\mathsf{rsp}_i\}_{i \text{ s.t. } c_i=0}) \leftarrow \mathsf{rsp}$
$\{\mathsf{rsp}_i\}_{i \text{ s.t. } c_i=1} \leftarrow \mathsf{Rcv}^{\mathcal{O}_{\mathsf{s}}}(\mathsf{seeds}_{\mathsf{int}}, \mathbf{c})$
for $i$ from 1 to $M$ do
    if $\mathcal{V}_2^{\mathcal{O}_{\mathsf{s}i}}(\mathsf{com}_i, c_i, \mathsf{rsp}_i) = \mathsf{reject}$ then
        $\mathcal{V}$ outputs reject
$\mathcal{V}$ outputs accept
```

Fig. 5. Optimized OR sigma protocol.

Note that the group action α with one-way assumption satisfies the definition of *admissible group action* in [12]. Then we prove the security of the optimized base OR-Sigma protocol showed in Figure 5 as follows.

Corollary 7. *Define the following relation*

$$R = \left\{ ((s_0, s_1, \ldots, s_N), (g, I)) \middle| \begin{array}{c} g \in G, s_i \in S \\ I \in [N], s_I = \alpha(g, s_0) \end{array} \right\},$$

and the relaxed relation

$$R = \left\{ ((s_0, s_1, \ldots, s_N), w) \middle| \begin{array}{rc} & g \in G, s_i \in S \\ w = (g, I): & I \in [N], s_I = \alpha(g, s_0) \\ w = (x, x'): & or\ x \neq x', \mathcal{H}_{\mathsf{Coll}}(x) = \mathcal{H}_{\mathsf{Coll}}(x') \\ & or\ \mathsf{Com}(x) = \mathsf{Com}(x') \end{array} \right\},$$

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. Based on the group action one-way assumption, it's straightforward to see that our optimized base OR sigma protocol satisfies the properties in [12, Definition 3.1]. By the Theorem 3.5 and Theorem 3.6 in [12], the optimized base OR sigma protocol satisfies correctness, relaxed special soundness and honest-verifier zero-knowledge. □

E.2 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 1, 2, 3, and 4 respectively.

Algorithm 1: Set Up

```
Input: The security parameter $\lambda$.
Output: Public paramater: variable number $n \in \mathbb{N}$, a prime power $q$ and an element $s_0 \in S$.
Choose $n \in \mathbb{N}$ and a prime power $q$ corresponding to the security parameter $\lambda$.
Randomly sample an element $s_0$ from $S$.
return Public parameter: $n, q, s_0$.
```

Algorithm 2: Key generation

```
Input: public parameter $n, q, s_0$, the user $i$.
Output: Public key for the user $i$: an element $s_i \in S$.
Private key for the user $i$: A group element $g_i$ such that $s_i = \alpha(g_i, s_0)$.
Randomly sample a group element $g_i$ from $G$.
Compute $s_i \leftarrow \alpha(g_i, s_0)$.
return Public key: $s_i$. Private key: $g_i$.
```

Algorithm 3: Signing procedure

```
Input: The public key $s_0, \ldots, s_N$, the private key $g_I$ of a user $I \in [N]$,
       a message 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 Sig on msg.
$\mathsf{com} = (\mathsf{salt}, (\mathsf{com}_i)_{i \in [M]}) \leftarrow \mathcal{P}'_1(s_1, \ldots, s_N)$
$\mathsf{cha} \leftarrow \mathcal{H}(\mathsf{msg}||s_1|| \cdots ||s_N||\mathsf{com})$
$\mathsf{rsp} \leftarrow \mathcal{P}'_2(g_I, I, \mathsf{cha})$
return $\mathsf{Sig} = (\mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$
```

Algorithm 4: Verification procedure

```
Input: The public key $s_0, \ldots, s_N \in S$. The signature $\mathsf{Sig} = (\mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$.
       The message msg. A hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.
Output: "Yes" if Sig is a valid signature for msg. "No" otherwise.
$\mathsf{com} \leftarrow \mathsf{RecoverCom}(s_0, \ldots, s_N, \mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$
if $\mathsf{accept} = \mathcal{V}'_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}) \wedge \mathsf{cha} = \mathcal{H}(\mathsf{msg}||s|| \cdots ||s_N||\mathsf{com})$ then
    return Yes
else
    return No
```

Remark 6. Since the optimized base OR sigma protocol is proved to satisfy all properties in Corollary 7, and by Appendix A.1 in [12], the ring signature in Algorithm 1, 2, 3 and 4 has correctness, anonymity and unforgeability.

F Linkable ring signature from abstract group actions

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 [12], are provided as follows.

Definition 13 (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, the following properties of the pair of group actions are needed; see [12, Definition 4.2], and also [6,27].

Definition 14. *Given two group actions $\alpha : G \times S \to S$ and $\beta : G \times S \to S$. We define the following properties:*

1. *Efficiency: One can efficiently compute $\alpha(g, s)$ and $\beta(g, s)$ for any $g \in G$ and $s \in S$, uniformly sample from G and S, and represent elements in G and S uniquely.*
2. *Linkability: Given $(s_0, r_0) \in S \times S$, it's hard to produce $g, g' \in G$ such that $\alpha(g, s_0) = \alpha(g', s_0)$ and $\beta(g, r_0) \neq \beta(g', r_0)$*
3. *Linkable Anonymity: Given $(s_0, r_0) \in S \times S$, the pair $(s_1, r_1) = (\alpha(g, s_0), \beta(g, r_0))$ is computationally indistinguishable from (s_2, r_2) where $g \in_R G$ and $s_2, r_2 \in_R S$.*
4. *Non-Frameability: Given $(s_0, r_0) \in S \times S$, $s_1 = \alpha(g, s_0)$ and $r_1 = \alpha(g, r_0)$, it's hard to find a group element g' such that $r_1 = \alpha(g', r_0)$*

We introduce an algorithm problem here and assume this problem is hard to demonstrate the linkable anonymity.

Definition 15 (Pair-pseudorandom). *The pseudorandom pairs equivalence under group action problem with 2 pairs of elements asks to distinguish the following two distributions given $(s_0, r_0) \in S \times S$:*

The random distribution: *A pair of element (s_1, r_1) where $(s_1, r_1) \in_R S \times S$.*
The pseudorandom distribution: *A pair of elements (s_1, r_1) where $s_1 := \alpha(g, s_0)$ and $r_1 := \beta(g, r_0)$ for $g \in_R G$.*

Note that a similar proposal in the context of code equivalence was proposed in [5].

Then we define the following relation

$$R = \left\{ ((s_0, s_1, \ldots, s_N, r_0, r), (g, I)) \;\middle|\; \begin{array}{c} g \in G, s_i \in S \\ I \in [N], s_I = \alpha(g, s_0) \\ r \in S, r = \beta(g_I, r_0) \end{array} \right\},$$

and the relaxed relation

$$\tilde{R} = \left\{ ((s_0, s_1, \dots, s_N, r_0, r), w) \;\middle|\; \begin{array}{rr} & g \in G, s_i \in S \\ & I \in [N], s_I = \alpha(g, s_0) \\ w = (g, I): & r \in S, r = \beta(g_I, r_0) \\ w = (x, x'): & \text{or } x \neq x', \\ & \mathcal{H}_{\mathsf{Coll}}(x) = \mathcal{H}_{\mathsf{Coll}}(x') \\ & \text{or } \mathsf{Com}(x) = \mathsf{Com}(x') \end{array} \right\}$$

for the relaxed special soundness.

```
$\mathcal{P}_1(s_1, \dots, s_N, r)$
seed $\leftarrow_R \{0,1\}^\lambda$
$(h, \mathsf{bits}_1, \dots, \mathsf{bits}_N) \leftarrow \mathsf{PRG}(\mathsf{seed})$
$r' \leftarrow \beta(h, r)$
for $i$ from 1 to $N$ do
  $t_i \leftarrow \alpha(h, s_i)$
  $\mathsf{C}_i \leftarrow \mathsf{Com}(t_i, \mathsf{bits}_i)$
$(\mathsf{root}, \mathsf{tree}) \leftarrow \mathsf{MerkleTree}(\mathsf{C}_1, \dots, \mathsf{C}_N)$
$h \leftarrow \mathcal{H}_{\mathsf{Coll}}(r', \mathsf{root})$
$\mathsf{com} \leftarrow h$
$\mathcal{P}$ sends com to $\mathcal{V}$
```

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

```
$\mathcal{P}_2(A_I, I, \mathsf{cha})$
$c \leftarrow \mathsf{cha}$
if $c = 0$ then
  $f \leftarrow h * g_I$
  $\mathsf{path} \leftarrow \mathsf{getMerklePath}(\mathsf{tree}, I)$
  $\mathsf{rsp} \leftarrow (f, \mathsf{path}, \mathsf{bits}_I)$
else
  $\mathsf{rsp} \leftarrow \mathsf{seed}$
$\mathcal{P}$ sends rsp to $\mathcal{V}$
```

```
$\mathcal{V}_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, s_0, s_1, \dots, s_N, r_0, r)$
$(h, c) \leftarrow (\mathsf{com}, \mathsf{cha})$
if $c = 0$ then
  $(f, \mathsf{path}, \mathsf{bits}) \leftarrow \mathsf{rsp}$
  $\tilde{t} \leftarrow \alpha(f, s_0)$
  $\tilde{\mathsf{C}} \leftarrow \mathsf{Com}(\tilde{t}, \mathsf{bits})$
$\tilde{r'} \leftarrow \beta(f, r_0)$
  $\widetilde{\mathsf{root}} \leftarrow \mathsf{ReconstructRoot}(\tilde{\mathsf{C}}, \mathsf{path})$
  if $h = \mathcal{H}_{\mathsf{Coll}}(\tilde{r'}, \widetilde{\mathsf{root}})$ then
    $\mathcal{V}$ outputs accept
  else
    $\mathcal{V}$ outputs reject
else
  $\mathsf{seed} \leftarrow \mathsf{rsp}$
  $\widetilde{\mathsf{root}} \leftarrow \mathcal{P}_1((s_1, \dots, s_N), \mathsf{seed})$
  if $h = \mathcal{H}_{\mathsf{Coll}}(\tilde{r'}, \widetilde{\mathsf{root}})$ then
    $\mathcal{V}$ outputs accept
  else
    $\mathcal{V}$ outputs reject
```

Fig. 6. Linkable OR sigma protocol.

Theorem 13. *Assume the stabilizers* $\mathrm{Stab}(s_0)$ *and* $\mathrm{Stab}(r_0)$ *are trivial and the pair-pseudorandom problem defined in Definition 15 is hard. The linkable OR sigma protocol shown in the Figure 6 after the optimization satisfies the properties defined in Definition 14.*

Proof. For the linkability, we derive this property by restricting the orbit $\mathcal{O}(s_0)$ has a trivial stabilizer. Then by the pair-pseudorandom assumption, it's straightforward to see that our protocol has the linkable anonymity. For the non-frameability, we restrict the stabilizer $\mathrm{Stab}(r_0)$ to be trivial as well, and then the group element g satisfying $s_1 = \alpha(g, s_0)$ and $r_1 = \alpha(g, r_0)$ is unique. It follows that if one can break non-frameability, the pair-pseudorandom assumption can be broken as well. □

Corollary 8. *The linkable OR sigma protocol shown in the Figure 6 after the optimization satisfies correctness, high min-entropy, special zero-knowledge and relaxed special soundness.*

Proof. By Theorem 13 and [12, Theorem 4.5,Theorem 4.6], our OR sigma protocol satisfies correctness, relaxed special soundness and honest-verifier zero-knowledge. □

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 5, 6, 7, 8 and 9. The linkable ring signature is similar to the normal ring signature in addition with a link algorithm.

```
Algorithm 5: Set Up
  Input: The security parameter $\lambda$.
  Output: Public paramater: variable number $n \in \mathbb{N}$, a prime power $q$ and elements $s_0, r_0 \in S$.
Choose $n \in \mathbb{N}$ and a prime power $q$ corresponding to the security parameter $\lambda$.
Randomly sample elements $s_0, r_0$ from $S$.
return Public parameter: $n, q, s_0, r_0$.
```

```
Algorithm 6: Linkable key generation
  Input: Public parameter $n, q, s_0, r_0$ and the user $i$.
  Output: Public key for the user $i$: an element $s_i \in S$.
  Private key for the user $i$: A group element $g_i$ such that $s_i = \alpha(g_i, s_0)$.
Randomly sample a group element $g_i$ from $G$.
Compute $s_i \leftarrow \alpha(g_i, s_0)$.
return Public key: $s_i$. Private key: $g_i$.
```

Algorithm 7: Link procedure

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

Algorithm 8: Linkable signing procedure

```
Input: The public key: $s_0, \dots, s_N$. The private key: $g_I$. 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 $\mathsf{msg}$.
$r \leftarrow \beta(g_I, r_0)$
$\mathsf{com} = (\mathsf{salt}, (\mathsf{com}_i)_{i \in [M]}) \leftarrow \mathcal{P}_1'(s_0, s_1, \dots, s_N, r)$
$\mathsf{cha} \leftarrow \mathcal{H}(\mathsf{msg}||s_1|| \cdots ||s_N||r||\mathsf{com})$
$\mathsf{rsp} \leftarrow \mathcal{P}_2'(g_I, I, \mathsf{cha})$
return $\mathsf{Sig} = (\mathsf{salt}, r, \mathsf{cha}, \mathsf{rsp})$
```

Algorithm 9: Linkable verification procedure

```
Input: The public key $s_0, \dots, s_N \in S$. The signature $\mathsf{Sig} = (\mathsf{salt}, r, \mathsf{cha}, \mathsf{rsp})$. 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.
$\mathsf{com} \leftarrow \mathsf{RecoverCom}(s_0, \dots, s_N, r, \mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$
if $\mathsf{accept} = \mathcal{V}_2'(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}) \wedge \mathsf{cha} = \mathcal{H}(\mathsf{msg}||s|| \cdots ||s_N||r||\mathsf{com})$ then
    return Yes
else
    return No
```

Remark 7. Since the linkable OR sigma protocol is proved to satisfy all conditions in Corollary 8, and by the Theorem 4.7 in [12], the linkable ring signature in Algorithm 6, 7, 8 and 9 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*[40]. Beullens et.al. proposed a new property called online extractability [10], which is used to obtain a almost tight security reduction of ring signature.Further they use some techniques including the Katz-Wang technique [51] 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.

G Column matrix decomposition and action on trilinear forms

G.1 LUP-decomposition

Fact 1 (LUP decomposition)**.** For every invertible matrix $A \in F^{n\times n}$, there is a lower triangular matrix L with ones on the main diagonal, an upper triangular matrix U, and a permutation matrix P such that

$$A = LUP.$$

An easy proof goes like this: Write $A = LU$ and think of each of the matrices as a block matrix with a 1×1-block in the upper left corner and an $(n-1)\times(n-1)$-block in the lower right corner, that is,

$$\begin{pmatrix} a_{1,1} & b \\ c & A' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \ell & L' \end{pmatrix} \begin{pmatrix} u_{1,1} & v \\ 0 & U' \end{pmatrix} = \begin{pmatrix} u_{1,1} & v \\ \ell u_{1,1} & \ell v + L'U' \end{pmatrix}$$

If $a_{1,1} \neq 0$, then $u_{1,1} = a_{1,1}$, $v = b$, and $\ell = c/u_{1,1}$. We then can recurse on $L'U' = A - \ell v$. If $a_{1,1} = 0$, then we there is a permutation matrix Q such the $(1,1)$-entry of AQ equals one and we work with this matrix. At the end, we can bring the final permutations matrix to the righthand side and obtain the LUP decomposition.

We can also use Gaussian elimination (with pivoting) to bring A into upper triangular form, this gives a decomposition $LAP = U$. Since L^{-1} is again lower diagonal with ones on the main diagonal, we get the desired decomposition.

We can write L as a product $L = L_1 \cdots L_{n-1}$ with

$$L_i = \begin{pmatrix} 1 \dots 0 & 0 & 0 \dots 0 \\ \vdots \ddots \vdots & \vdots & \vdots \quad \vdots \\ 0 \dots 1 & 0 & 0 \dots 0 \\ 0 \dots 0 & 1 & 0 \dots 0 \\ 0 \dots 0 & \ell_{i+1,i} & 1 \dots 0 \\ \vdots \quad \vdots & \vdots & \vdots \ddots \vdots \\ 0 \dots 0 & \ell_{n,i} & 0 \dots 1 \end{pmatrix}.$$

Each L_i can be further decomposes as $L_i = L_{i,i+1,} \cdots L_{i,n}$ with

$$L_{i,j} = \begin{pmatrix} 1 \dots 0 & 0 & 0 \dots 0 \\ \vdots \ddots \vdots & \vdots & \vdots \quad \vdots \\ 0 \dots 1 & 0 & 0 \dots 0 \\ 0 \dots 0 & 1 & 0 \dots 0 \\ 0 \dots 0 & \text{⋰} & 1 \dots 0 \\ \vdots \quad \vdots & \ell_{i,j} & \vdots \ddots \vdots \\ 0 \dots 0 & \dots & 0 \dots 1 \end{pmatrix}.$$

Each $L_{i,j}$ is an elementary matrix with at most one nonzero entry $\ell_{i,j}$ except the ones on the main diagonal. For each i, $L_{i,i+1}, \dots, L_{i,n}$ mutually commute.

The matrix $\hat{U} := U \cdot \operatorname{diag}(u_{1,1}, \dots, u_{n,n})$, where $u_{i,i}$ are the diagonal entries of U, is upper triangular and has ones on the main diagonal. Like L, is can be written as the product of $n-1$ matrices, but with nonzero entries above the main diagonal.

Definition 16. *A matrix $C \in F^{n \times n}$ is a column matrix, if it is of the form*

$$C = \begin{pmatrix} 1 \dots 0 & c_1 & 0 \dots 0 \\ \vdots \ddots \vdots & \vdots & \vdots \quad \vdots \\ 0 \dots 1 & c_{i-1} & 0 \dots 0 \\ 0 \dots 0 & c_i & 0 \dots 0 \\ 0 \dots 0 & c_{i+1} & 1 \dots 0 \\ \vdots \quad \vdots & \vdots & \vdots \ddots \vdots \\ 0 \dots 0 & c_n & 0 \dots 1 \end{pmatrix}$$

for some i.

Corollary 9. *For every invertible matrix A, there is a permutation matrix P such that such that AP is the product of $2(n-1)$ column matrices.*

Note that the diagonal matrix in the definition of $\hat{U}$ can be merged with the matrices of the factoriztion of $\hat{U}$ into column matrices.

G.2 Multiplication of alternating trilinear forms with column matrices

Let C be a column matrix with entries $c_1, \dots, c_n$ in column i. The matrix C maps an unit vector e_h to

$$Ce_h = \begin{cases} e_h & \text{if } h \neq i, \\ \sum_{j=1}^{n} c_j e_j & \text{otherwise.} \end{cases}$$

Let T be an alternating trilinear form, that is,

$$T = \sum_{1 \le r < s < t \le n} t_{r,s,t} \cdot e_r \wedge e_s \wedge e_t.$$

We have

$$C^{\wedge 3} T = \sum_{1 \le r < s < t \le n} t_{r,s,t} \cdot C(e_r) \wedge C(e_s) \wedge C(e_t).$$

C only changes e_i. e_i appears in $\binom{n-1}{2}$ of the summands. Consider each summand separately. Assume w.l.o.g. that e_i appears in the first position,

$$t_{i,r,s} \cdot e_i \wedge e_r \wedge e_s.$$

$C^{\wedge 3}$ maps this summand to

$$t_{i,r,s} \cdot \left(\sum_{i=1}^{n} c_j e_j \right) \wedge e_r \wedge e_s = \sum_{j=1}^{n} \underbrace{c_j \cdot t_{i,r,s}}_{\text{1 mult.}} \cdot e_j \wedge e_r \wedge e_s.$$

Thus, we have to compute n multiplications and $n-1$ additions (updates of the entries $e_j \wedge e_r \wedge e_s$ with $j \neq i$). Therefore, the total costs are $\binom{n-1}{2} \cdot n \le n^3/2$ multiplications and $\binom{n-1}{2} \cdot (n-1) \le n^3/2$ additions.

If the matrix C has only k nonzero entries in column i, then the bounds reduce to $\binom{n-1}{2} \cdot j \le n^2 \cdot j/2$ multiplications and $\binom{n-1}{2} \cdot (j-1) \le n^2 \cdot j/2$ additions. The LUP decomposition yields a decomposition of any invertible matrix A into $2(n-1)$ column matrix with a total of $\approx n^2$ nonzero entries. Therefore, we can implement the action of $A^{\wedge 3}$ with $n^4/2$ multiplications and $n^4/2$ additions.

In the actual implementation, we have to do a modular reduction after each application of a column matrix. Therefore, we try to minimize the number of column matrices in a decomposition of A. (Obviously, it cannot be lower than n.)

G.3 Optimal decomposition into column matrices

Let

$$A = \begin{pmatrix} 1 \dots 0 & a_1 & * \dots * \\ \vdots \ddots \vdots & \vdots & \vdots \quad \vdots \\ 0 \dots 1 & a_{i-1} & * \dots * \\ 0 \dots 0 & a_i & * \dots * \\ 0 \dots 0 & a_{i+1} & * \dots * \\ \vdots \quad \vdots & \vdots & \vdots \ddots \vdots \\ 0 \dots 0 & a_n & * \dots * \end{pmatrix}.$$

If $a_i \neq 0$, then let B be the column matrix

$$B = \begin{pmatrix} 1 \dots 0 & -a_1/a_i & 0 \dots 0 \\ \vdots \ddots \vdots & \vdots & \vdots \quad \vdots \\ 0 \dots 1 & -a_{i-1}/a_i & 0 \dots 0 \\ 0 \dots 0 & 1/a_i & 0 \dots 0 \\ 0 \dots 0 & -a_{i+1}/a_i & 1 \dots 0 \\ \vdots \quad \vdots & \vdots & \vdots \ddots \vdots \\ 0 \dots 0 & -a_n/a_i & 0 \dots 1 \end{pmatrix}.$$

Then

$$BA = \begin{pmatrix} 1 \dots 0 \; 0 \; * \dots * \\ \vdots \ddots \vdots \; \vdots \; \vdots \quad \vdots \\ 0 \dots 1 \; 0 \; * \dots * \\ 0 \dots 0 \; 1 \; * \dots * \\ 0 \dots 0 \; 0 \; * \dots * \\ \vdots \quad \vdots \; \vdots \; \vdots \ddots \vdots \\ 0 \dots 0 \; 0 \; * \dots * \end{pmatrix}.$$

By using induction, we can find column matrices $B_1, \dots, B_n$ with B_i having column i such that

$$B_n B_{n-1} \cdots B_1 A = I.$$

The inverse of B is

$$B^{-1} = \begin{pmatrix} 1 \dots 0 & a_1 & 0 \dots 0 \\ \vdots \ddots \vdots & \vdots & \vdots \quad \vdots \\ 0 \dots 1 & a_{i-1} & 0 \dots 0 \\ 0 \dots 0 & a_i & 0 \dots 0 \\ 0 \dots 0 & a_{i+1} & 1 \dots 0 \\ \vdots \quad \vdots & \vdots & \vdots \ddots \vdots \\ 0 \dots 0 & a_n & 0 \dots 1 \end{pmatrix}.$$

We can write

$$A = B_1^{-1} B_2^{-1} \cdots B_n^{-1}.$$

By counting dimension, it is obvious that there cannot be a shorter decomposition of A into column matrices.