On digital signatures based on group actions: QROM security and ring signatures

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. Group action based cryptography was formally proposed in the seminal paper of Brassard and Yung (Crypto 1990). Based on one-way group action, there is a well-known digital signature design based on the Goldreich–Micali–Widgerson (GMW) zero-knowledge protocol for the graph isomorphism problem and the Fiat–Shamir (FS) transformation. Recently, there is a revival of activities on group action based cryptography and the GMW-FS 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-fold: 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. We distil properties of the underlying group action 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 support 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.

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 [30]. As far as we know, the first treatment of *abstract* group actions in cryptography goes back to Brassard and Yung [23], who proposed the notion of *one-way* group actions. When the groups are abelian (commutative), this was further developed by Couveignes [30]. Recently, two independent works [52] and [2] enriched this framework further by introducing the notion of (weakly) pseudorandom group actions, which generalises the celebrated Decisional Diffie–Hellman assumption [33,16].

Besides setting up frameworks, many cryptographic primitives can be realised, such as claw-free one-way functions and bit commitment [23], quantum-secure pseudorandom functions [52], and zero-knowledge identification protocols [30,52]. When the groups are abelian (commutative), more functions are possible, such as key exchange [30], smooth projective hashing, and dual-mode public-key encryption [2].

The GMW-FS digital signature design. A major cryptographic application of group actions is the following digital signature design. In [44], Goldreich, Micali and Wigderson described a zero-knowledge proof protocol for the graph isomorphism (GI) problem. The Fiat–Shamir transformation FS [43] 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 efficiently in practice [61,62], not to mention Babai's quasipolynomial-time algorithm [3].

Fortunately, the Goldreich–Micali–Wigderson (GMW) zero-knowledge proof protocol applies to *any* isomorphism problem. In fact, one way to formulate isomorphism problems is through group actions, and the hardness of an isomorphism problem naturally translates to the one-way assumption of the group action. This gives hope that, by choosing an appropriate group action (or isomorphism problem), such a construction could be secure. This was already carried out in 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 [64]. In isogeny-based cryptography, Stolbunov applied this construction to the class group actions on elliptic curves [30,73]. However, these efforts met with some issues. For example, the parameters proposed by Patarin were too optimistic [22], and computational costs and uniform sampling for class group actions are tricky issues [26].

The recent revival of the GMW-FS design. Recently, there has been 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 isogenies, 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 [26]. This led to the schemes SeaSign [42] and CSI-FiSh [13], which greatly improve the situation by introducing both computational and protocol optimizations; see also the recent nice survey on this and more in [11].

The second direction may be viewed as a continuation of the polynomial isomorphism direction by Patarin [64]. Three schemes submitted to the most recent NIST call for post-quantum digital signatures [72] fall into this category, namely LESS [14] based on linear code monomial equivalence, ATFE [75] based on alternating trilinear form equivalence, and MEDS [28] based on matrix code equivalence[6]. Recent progress in complexity theory [46] shows that (1) linear code monomial equivalence reduces to matrix code equivalence in polynomial time [45,31], and (2) alternating trilinear form equivalence, isomorphism of quadratic polynomials with two secrets, cubic form equivalence, and matrix code equivalence are polynomial-time equivalent [46,47] (see also [69] for some of these equivalences).

The studies above are of particular interest in post-quantum cryptography. Since discrete logarithms can be solved efficiently on quantum computers [71], it is desirable to explore group actions suitable for post-quantum cryptography. As in the lattice case [68], the research into hidden subgroup problems is of particular relevance here, especially the hidden shift problems [27] and symmetric or general linear groups [48]. 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 [65,18]. 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 the hidden subgroup problem for graph isomorphisms [48] 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 [55,58,35]. We then present the linkable ring signature construction of Beullens, Katsumata and Pintore [12] with abstract group actions.

We then apply the results to a concrete setting, namely the digital signature scheme introduced in [75], which we refer to as the ATFE-GMW-FS scheme[7]. More

[6] Matrix code equivalence is also known as 3-tensor isomorphism in [46].

[7] Since the appearance of ATFE-GMW-FS, some nice cryptanalysis works were done, such as by Beullens [9], and by Ran, Samardjiska and Trimoska [67]. A submission to NIST's call for additional post-quantum digital signatures [72] is based on this scheme, and we refer the interested readers to [15] for its specifications.

specifically we demonstrate its QROM security, and implement the ring signature scheme above for ATFE-GMW-FS. Our preliminary experiments suggest that this scheme is competitive among existing post-quantum ring signatures. Finally, we show that the MPC-in-the-head paradigm for group actions [53] helps to reduce the signature sizes for the ATFE-GMW-FS scheme.

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. [17] 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 [17]. Indeed, the QROM security of the Fiat–Shamir transformation was only recently shown after a series of works [79,55,58,35].

In this paper we make progress on the QROM security of the GMW-FS design based on the works [79,55,58,35]. 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. $|\mathrm{Stab}(s)| = 1$ and α satisfies the C-one-way-$\mathcal{O}(s)$ assumption (see Definition 6 and Remark 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 [52,2] (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 [70], 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 anonymity 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 [57] 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 [74] and e-voting [76].

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 is 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 due to certain stronger assumptions on the group actions. We call this ring signature design the GMW-FS-BKP design, and describe its construction in Section 5. The linkability property requires extra discussions as it calls for an 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 (resp. MEDS, LESS) based on the perfect unique response was observed in [13] (resp. [28], [14]), and the tight QROM security based on a lossy version of CSI-FiSh was shown in [37]. The ring signature scheme in [12] has been shown for the group actions underlying CSI-FiSh [12], LESS [4], and MEDS [28].

Indeed, we view our results for the GMW-FS design as mostly conceptual. Our aim is 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 [55] with the pseudorandom group action assumption [52,2] and the non-trivial automorphism hardness assumption (Definition 8) was not stated explicitly before. Such results should benefit the LESS and MEDS schemes, which only discussed their QROM securities based on perfect unique response (but not the lossy scheme).

Results for the ATFE-GMW-FS scheme. After working with the general GMW-FS design, we focus on the ATFE-GMW-FS scheme from [75,15], which demonstrates concrete uses of the results we obtained for abstract group actions.

The QROM security of the ATFE-GMW-FS scheme. The QROM security of the ATFE-GMW-FS scheme was briefly discussed in [75] 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 those parameters proposed in [75], 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 question of whether the group action under ATFE is pseudorandom or not is an open problem. In [75], some arguments were provided to support that it is. In particular, we do not need to modify the original

ATFE-GMW-FS scheme in [75] to attain the security in QROM, i.e., as opposed to the lossy CSI-FiSh scheme [37]. 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 experimental 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 6.2 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 $0.8 \log R + 19.7$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 205ms which is twice Falafl's 90ms and much smaller than Calamari's 79s. Meanwhile, our ring signature size is 22.1KB, while Falafl and Calamari have the signature size of 30KB and 5.4KB respectively. RAPTOR [59], and DualRing-LB [81] 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. For more comparisons with other ring signatures, please see Table 1. Finally, Fig 1 reports the signing time of our protocol; there, n, M and K are the parameters in the ATFE-GMW-FS-BKP scheme as defined in Section 6.2. Note that the signing time is measured on a 2.4 GHz Quad-Core Intel Core i5.

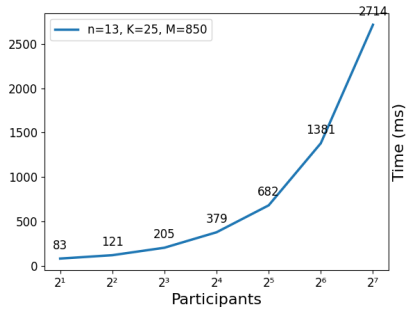

Fig. 1. Signature generation time

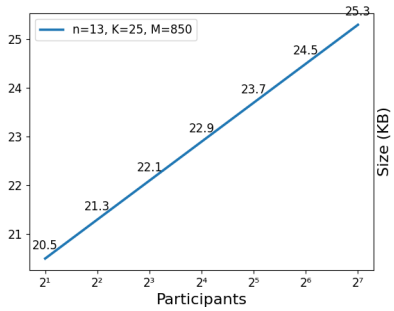

Fig. 2. Signature size

MPC-in-the-head paradigm. Another recent contribution to the GMW-FS design is by Joux [53], who showed that the multiparty-computation (MPC) in the head paradigm can be applied to a generic group action. This paradigm allows

	R								Hardness assumption	Secuirty level
	2^1	2^3	2^5	2^6	2^{10}	2^{12}	2^{15}	2^{21}		
MatRiCT [39]	18	19	/	31	/	59	/	148	MSIS, MLWE	128 bits
SMILE [60]	/	/	16	/	18	/	19	/	MSIS, MLWE	128 bits
MatRiCT$^+$ [38]	5.4	8.2	11	12.4	18	20.8	25	33.4	MSIS, MLWE	128 bits
RAPTOR [59]	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	128 bits
DualRing-LB [81]	/	4.6	/	6	/	106.6	/	/	MSIS, MLWE	128 bits
MRr-DSS [8]	/	27	/	36	/	422	/	/	MinRank	128 bits
LESS [4]	/	10.8	/	13.7	/	19.7	/	28.6	Code Equiv.	128 bits
Ours	20.5	22.1	23.7	24.5	27.7	29.3	31.7	36.5	ATFE	128 bits

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

for shorter signature sizes at the cost of longer computation time, and the ATFE-GMW-FS scheme is a nice example of 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 4 and Table 5).

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 that could avoid analysing automorphism groups mathematically. In [58,35], a property called *quantum unique response* in [35] or collapsing sigma protocol in [58] is introduced, generalising the *collapsingness* which is introduced by Unruh [78] 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 [37] is the diagonal action of the class group on two elliptic curves following [73]. One reason is that for the pseudorandom group action assumption [52] (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 a 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 [32] 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. More specifically, they encode the challenge space as follows. 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 the 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 a tag associated with a group action $\beta(g, s) = \alpha(g^{-1}, s)$ while our associated group action is $\beta(g, s) = \alpha(g^{-t}, s)$, see more details in Section 5. Last but not least, D'Alconzo and Gangemi do not provide implementations while in our work, we implemented the ring signature and compared it 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 the logarithm is 2 unless otherwise specified. For a finite set S, we use $s \xleftarrow{\$} S$ to denote that s is uniformly randomly sampled from S. Given a positive integer k, 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 that 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. As most of them are classical, we collect them in Appendix A.1 for the readers' convenience, and only explain perfect and computational unique responses as they are key to the QROM security later.

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 $(x, w) \leftarrow \mathsf{Gen}(1^\lambda)$:

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

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 Schemes). *The signature scheme is said to be existentially unforgeable (i.e., EUF-CMA secure) if for any poly-time quantum adversaries $\mathcal{A}$, who can query some signatures of messages of his choices,*

the probability that $\mathcal{A}$ can sign a message whose signature hasn't been produced is negligible, i.e., $\Pr[\mathsf{Verify}(\mathsf{pk}, m, \sigma) = 1 \wedge m \notin \Sigma | (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n),\ (\sigma, m) \leftarrow \mathcal{A}(\mathsf{pk})] \leq \mathsf{negl}(\lambda)$*, 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 that has been queried before. The schemes presented in this paper satisfy this stronger notion of existential unforgeability.

Definition 4 (Strong Security of Signature Schemes). *The signature scheme is said to be strongly existentially unforgeable (i.e., sEUF-CMA secure) if for any poly-time quantum adversaries $\mathcal{A}$, who can query signatures of messages of his choices, the probability that $\mathcal{A}$ can sign a message that the corresponding message-signature pair hasn't been produced is negligible, i.e.,* $\Pr[\mathsf{Verify}(\mathsf{pk}, m, \sigma) = 1 \wedge (m, \sigma) \notin \Sigma | (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n),\ (\sigma, m) \leftarrow \mathcal{A}(\mathsf{pk})] \leq \mathsf{negl}(\lambda)$*, where Σ is the list of all message-signature pairs that $\mathcal{A}$ has obtained before.*

Fiat-Shamir transformation. The Fiat-Shamir (FS) transformation [43] 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 ([66]). *If an identification protocol is HVZK and satisfies special soundness, then FS[ID] has EUF-CMA security in the ROM model.*

2.3 Ring signatures

In this section, we provide the definition of the ring signature. The definition and properties of linkable ring signatures are provided in Appendix D.1.

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 $b \xleftarrow{\$} \{0, 1\}$. Then it sends pp and the secret keys $\{\mathsf{sk}_i\}_{i\in[N]}$ to $\mathcal{A}$.
(2) $\mathcal{A}$ computes a challenge $(\mathsf{R}, \mathsf{M}, i_0, i_1)$, where R contains vk_{i_0} and vk_{i_1}, and sends it to the challenger.
(3) The challenger runs $\mathsf{RS.Sign}(\mathsf{sk}_{i_b}, \mathsf{R}, \mathsf{M}) \to \sigma$ 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 sk_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. We use $*$ to denote the group multiplication. 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 [23,30,52,2], 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 $|S_k| = A_k$ and $|G_k| = B_k$, and $\log A_k$ and $\log B_k$ 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 $|S| = A$ and $|G| = B$.

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 [26] 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 $s \xleftarrow{\$} S$ and $t \xleftarrow{\$} \mathcal{O}(s)$, 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 $s, t \xleftarrow{\$} S$.
   (b) The pseudorandom distribution: $(s, t) \in S \times S$ where $s \xleftarrow{\$} S$, $t \xleftarrow{\$} \mathcal{O}(s)$.

Those assumptions can be generalised to the following C-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 $s_0 \xleftarrow{\$} S$, given s_0 and $s_1, \ldots, s_{C-1} \xleftarrow{\$} \mathcal{O}(s_0)$, 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 $s_i \xleftarrow{\$} S$.*
   (b) *The pseudorandom distribution: $(s_0, \ldots, s_{C-1}) \in S^C$ where $s_0 \xleftarrow{\$} S$, and $s_1, \ldots, s_{C-1} \xleftarrow{\$} \mathcal{O}(s_0)$.*

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 $s_0 \xleftarrow{\$} S$ 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 $s_0 \xleftarrow{\$} S$, and $s_1, \ldots, s_{C-1} \xleftarrow{\$} \mathcal{O}(s_0)$. The private keys consists of $g_0 = \mathrm{id}, g_1, \ldots, g_{C-1}$ 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, which will be repeated several times to attain the required security level.

It is known that $\alpha(\mathsf{G}, \mathsf{S})$-GMW protocol in Figure 3 has the following properties (see e.g. [75]): 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 also discuss a variant of the $\alpha(\mathsf{G}, \mathsf{S})$-GMW-FS 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 $s \xleftarrow{\$} S$. We call such a scheme the $\alpha(\mathsf{G}, \mathsf{S})$-GMW-FS-$\mathcal{O}(s)$ scheme.

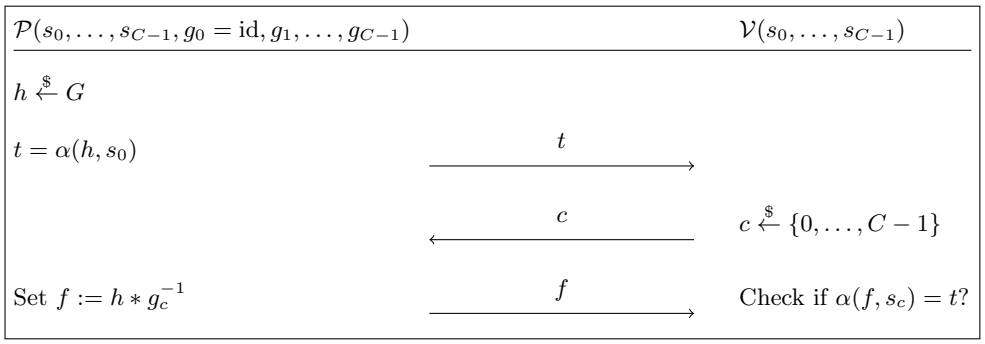

Fig. 3. The $\alpha(\mathsf{G}, \mathsf{S})$-GMW protocol.

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

The group action underlying ALTEQ [75] Let $\mathbb{F}_q$ be the finite field of order q. A trilinear form $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is *alternating*, if ϕ evaluates to 0 whenever two arguments are the same. We use $\mathrm{ATF}(n, q)$ to denote the set of all alternating trilinear forms defined over $\mathbb{F}_q^n$. Let A be an invertible matrix of size $n \times n$ over $\mathbb{F}_q$. Then A sends ϕ to another alternating trilinear form $\phi \circ A$, defined as $(\phi \circ A)(u, v, w) := \phi(A^{\mathrm{t}}(u), A^{\mathrm{t}}(v), A^{\mathrm{t}}(w))$.

The group action underlying LESS [14]. 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 [28]. 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 underlying CSIDH [26] (such as for SeaSign [42] and CSI-FiSh [13]). 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 [42,13,11]. 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 [36] and knot equivalence [40]. While these are interesting, we did not discuss these here due to space limitations.

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 QROM security of the $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ scheme in Theorem 2, with proof sketches in Appendix B.

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) [17]. 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 cause collapse, etc. Indeed, there exist protocols that are secure in ROM but not in QROM [17,80].

Recently, thanks to a pair of breakthrough papers [35,58], the QROM security of the Fiat-Shamir transform is now much better understood. Based on these papers, we study the relation between the $\alpha(\mathsf{G},\mathsf{S})$-GMW scheme and the *perfect unique response* property introduced by Unruh [77], so we can prove the security of the $\alpha(\mathsf{G},\mathsf{S})$-GMW protocol in 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 $\alpha(\mathsf{G},\mathsf{S})$-GMW or $\alpha(\mathsf{G},\mathsf{S})$-GMW-$\mathcal{O}(s_0)$ protocols meet the *perfect unique response* and *computationally unique response* properties, as recalled in Section 2.2.

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

Proof. 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 $g_1 = g_2$.

Now assume that the $\alpha(\mathsf{G},\mathsf{S})$-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 $\alpha(\mathsf{G},\mathsf{S})$-GMW, since s_0 is not fixed, in some cases, we can only say that the stabilizer group of a random $s_0 \leftarrow_R S$ is trivial with high probability. Such a property is known as 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 [56]).

Lemma 2 (Computationally Unique Response). *The $\alpha(\mathsf{G},\mathsf{S})$-GMW protocol in Figure 3 supports computationally unique response if and only if 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 polynomial-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 there is a polynomial-time quantum algorithm $\mathcal{A}_1$ such that, for any $s \in S$, it produces a stabilizer element h such that $\alpha(h, s) = s$ 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 (t, 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 (t, 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 (t, c, g) and $(t, c, h * g)$ 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 $\alpha(\mathsf{G},\mathsf{S})$-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 straightforward to adapt the results in [58] to give a security proof in QROM for $\alpha(\mathsf{G},\mathsf{S})$-GMW-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, and assume the C-one-way-$\mathcal{O}(s_0)$ is hard. 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,*

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

For readers' convenience, we present the proof of Theorem 2 based on [58] in Appendix B.

Remark 4. The EUF-CMA security in QROM here can be strengthened to the sEUF-CMA security by assuming the computationally unique response property [55, 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.

Remark 5. The ATFE instantiation in Section 6 provides meaningful realization of Theorem 2 in a concrete group action setting. In fact, in Section 6.1, we experimentally verify that for a random alternating trilinear form, its stabilizer group is trivial, hence supporting the security of ATFE-GMW-FS signature in the QROM model; see Section 6.1 for more detail.

4 QROM security via lossy schemes

4.1 Definitions and previous results

In this section, we recall the definition of lossy identification protocol [1,37] and a security result of its associated Fiat-Shamir signature in QROM from [55].

Definition 9. *An identification protocol ID is called lossy, denoted by $\mathsf{ID}_{\mathsf{ls}}$, if it has one additional PPT algorithm* $\mathsf{LossyGen}$*, called the lossy key generation that on inputs 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 required that the lossy statements generated by $\mathsf{LossyGen}(1^\lambda)$ is indistinguishable with ones generated by $\mathsf{Gen}(1^\lambda)$, i.e., . for any PPT (or quantum PT) adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ against the indistinguishability of lossy statements

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

is negligible.

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

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

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

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

Fiat-Shamir transformation applied to a lossy identification protocol yields a tightly secure signature in QROM [55,58,35].

Theorem 3 ([55, 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 adversary $\mathcal{B}$ against the lossiness and $\mathcal{C}$ against the computation unique response such that*

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

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 $\alpha(\mathsf{G},\mathsf{S})$-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 $\alpha(g_i, s_0) = s_i$ 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 $s_i = \alpha(g_i, s_0)$ 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 indistinguishability of lossy statements, and to calculate the 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 the 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. □

The following lemma calculates the lossy soundness parameter ϵ_{ls}.

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

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

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 $\mathcal{X}$ is $\Pr[x \in \mathcal{X} \mid x \leftarrow \mathsf{LossyGen}] \geq \prod_{i=1}^{C-1} \frac{A-iB}{A}$. We can obtain the probability that an adversary wins as follows:

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

Note that the second inquality is due to $\Pr[\mathcal{A} \text{ wins } \mid x \in \mathcal{X}] - 1 \leq 0$. 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 $A = |S|$, $B = |G|$, and $|C|$ is the size of the challenge space.*

Remark 6. For our ATFE instantiation in Section 6, B is the order of the general linear group $\mathrm{GL}(n, q)$ and A is the size of $\mathrm{ATF}(n, q)$ which is far greater than B as the parameter n is large enough. Therefore, the error ϵ_{ls} is estimated to be $2^{-\lambda}$ where λ is the security level; see Section 6.1 for the detail.

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 t-fold parallel repetition of the lossy identification protocol in Section 4.2. We call this the $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$-$\mathsf{FS}$-$\mathsf{lossy}$ scheme. Note that this result is essentially the same scheme as the $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$-$\mathsf{FS}$ 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 $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-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 sEUF-CMA security of $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-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*

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

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

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

Proof. The proof initialises with Lemma 2 and Section 4.2 that the underlying sigma protocol has computational unique response, lossiness, lossy-soundness, perfect HVZK and at least $\log(|\mathcal{O}|)$ 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 GMW-FS-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 [4] and MEDS [28]. 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 GMW-FS-BKP ring signature is obtained by applying the Fiat-Shamir transformation to an OR-Sigma protocol, which is an interactive protocol in which a prover convinces a verifier that she knows the witness of one of given several inputs without revealing which one. Here, we describe the base OR-Sigma protocol for an abstract group

action. Some optimization and the security proof are reproduced in Appendix C for the readers' convenience.

Let $g_1, g_2, \ldots, g_N \xleftarrow{\$} G$ 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, assumed to be the I-th user in the ring, 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 $\mathsf{bits}_i \xleftarrow{\$} \{0,1\}^\lambda$ and commits to t_i with $\mathsf{C}_i = \mathsf{Com}(t_i, \mathsf{bits}_i)$. The prover further builds a Merkle tree[8] 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 $c \xleftarrow{\$} \{0,1\}$ and respond 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 the 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 in Appendix C.

The linkable property. Linkable ring signatures were first introduced by Liu and Wong [57] 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.

Here we only briefly indicate how to construct a linkable OR sigma protocol. More details can be found in Appendix D.

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 6.1, 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, we can get a linkable OR sigma protocol and apply certain optimisation methods to it for more efficiency.

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

A linkable digital signature needs to satisfy linkability, linkable anonymity, and non-frameability, which can be translated to properties about group actions as done in [12, Definition 4.2] and also [4,28].We refer the interested readers to Appendix D for formal definitions of these notions. 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 $s_1, r_1 \xleftarrow{\$} S$.*
2. *The pseudorandom distribution: $(s_1, r_1) \in S \times S$, where $g \xleftarrow{\$} G$, 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). We note that the above strategy was already used in MEDS [28] 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 [14,28], 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.

Remark 7. Note that our ring signature obtained from OR-Sigma protocol is proven securely only in ROM. As far as we are aware, whether it is secure in QROM is still an open problem.

6 Results for the ATFE-GMW-FS scheme

We now apply the results obtained in Sections 3, 4, and 5 to a concrete setting, namely the digital signature scheme introduced in [75], which we refer to as the ATFE-GMW-FS scheme.

For the QROM security, this requires us to examine the group action underlying the ATFE problem, to show that it satisfies the properties required for the QROM security. For the ring signature scheme, we provide an implementation of the ring signature scheme based on ATFE-GMW-FS. These provide evidence for the usefulness of the results obtained in the abstract group action framework.

Finally, we demonstrate that the MPC-in-the-head paradigm provided by Joux [53] can be applied to ATFE-GMW-FS to further reduce the signature size (at the cost of increasing the signing time).

6.1 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 and assume the C-one-way-$\mathcal{O}(\phi)$, where ϕ is instantiated as an alternating trilinear form. To decide whether $\mathrm{Stab}(\phi)$ is trivial or not is a difficult algorithmic problem; see [75, 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 [29,63,49]. Third, for $n = 9$ and $q = 2$, by the classification of alternating trilinear forms [50], 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 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 [19] 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 [41,20,21,22]. 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 [24]. The way we set up the equations is from [75].

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 [50], 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. This also implies that for larger n and q such that $3 \nmid q - 1$, a random alternating trilinear form has the trivial automorphism group with high probability, as the gap between the space dimension and the group dimension becomes larger as n increases. To the best of our knowledge, to give an estimation of this probability (depending on q and n) is an open problem.

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 [75, Conjecture 1], the authors conjectured that this is indeed the case, and provided some supporting evidences, some of which traced back to [52]. Here we briefly explain that, a key argument in [75] is that there seem no easy-to-compute isomorphism invariants for ATFE, as such isomorphism invariants could be used to distinguish non-equivalent alternating trilinear forms.

If the above holds, then $B = |\mathrm{GL}(n, q)| \approx q^{n^2}$ and $A = |\mathrm{ATF}(n, q)| = q^{\binom{n}{3}}$, $A \gg B$ as the security parameter λ is large enough. Therefore, the lossy soundness $\epsilon_{ls} \approx \frac{1}{C^t} \approx \frac{1}{2^\lambda}$.

Lossy schemes with unbalanced challenges. The unbalanced challenge technique is a classical technique that can be traced back to Fiat and Shamir's original paper [43]. The idea is to observe that, in the case of challenge 0, the response would be a random group element that 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. This is a standard technique that turns out to be useful in practice as witnessed in [6,28,15].

The parameters involved in the ATFE-GMW-FS scheme with unbalanced challenges are as follows. Let M be the round number, K be the number of non-zero challenges, and C the number of alternating trilinear forms in each round. To achieve λ-bit security, we should choose the proper M and K such that $\binom{M}{K} \cdot (C-1)^K \geq 2^\lambda$. Some care is then needed to demonstrate the lossy soundness in this setting.

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 the 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. □

6.2 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. Recall that M is the round number, K is the number of non-zero challenges, R is the ring size, and C is the number of alternating trilinear forms in each round. To achieve the λ-bits security, we should choose the proper M and K such that $(\frac{M}{K})^K \geq 2^\lambda$. Here we use a trick that evenly divides 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 are 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.

$$\text{Public Key Size} = (R+1) \cdot \binom{n}{3} \lceil \log_2 q \rceil,$$

$$\text{Private Key Size} = \binom{n}{3} \lceil \log_2 q \rceil + R \cdot n^2 \lceil \log_2 q \rceil,$$

$$\text{Signature Size} = K(\lambda \cdot \lceil \log_2 \left(\frac{M}{K} \right) \rceil + n^2 \lceil \log_2 q \rceil + 2\lambda \cdot \lceil \log_2 R \rceil + \lambda) + 3\lambda.$$

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

$$\text{Public Key Size} = (R+1) \cdot \binom{n}{3} \lceil \log_2 q \rceil,$$

$$\text{Private Key Size} = \binom{n}{3} \lceil \log_2 q \rceil + R \cdot n^2 \lceil \log_2 q \rceil,$$

$$\text{Signature Size} = K(\lambda \cdot \lceil \log_2 \left(\frac{M}{K} \right) \rceil + n^2 \lceil \log_2 q \rceil + 2\lambda \cdot \lceil \log_2 R \rceil + \lambda) + 3\lambda + \binom{n}{3} \lceil \log_2 q \rceil.$$

Concrete parameters and reports on the performance. We provide the performance evaluation of our schemes in terms of signature size, as shown in Tables 2. Furthermore, Table 3 illustrates the signature generation time for our schemes. Our constructions are implemented and measured on a 2.4 GHz Quad-Core Intel Core i5.

Parameters				Size in Bytes				
				R				
n	q	M	K	2^1	2^3	2^6	2^{12}	2^{21}
13	4294967291($\sim 2^{32}$)	850	25	20.5	22.1	24.5	29.3	36.5

Table 2. The signature size (KB) of the ring signature. The security meets the NIST level 1.

6.3 Signature size reduction by the MPC in the head paradigm

The multiparty computation (MPC) in the head paradigm was initially introduced in [51] as a means to enhance the theoretical and asymptotic constructions of zero-knowledge (ZK) protocols. Recently, Joux [53] 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.

Parameters				Time in ms						
				R						
n	q	M	K	2^1	2^2	2^3	2^4	2^5	2^6	2^7
13	4294967291($\sim 2^{32}$)	850	25	83	121	205	379	682	1381	2714

Table 3. The signing time (ms) of the ring signature. The security meets the NIST level 1.

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 satisfies 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.

Remark 8. The puncturable PRFs can be practically realized, and an elegant approach to achieve this is through the GGM tree construction. This method requires a length-doubling PRF, which, in practice, proves to be efficient and viable; see [25, page 14] for reference. Furthermore, it is feasible under the group action model [53].

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 has 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 the round number of offset maps along with the challenge. The size (in terms of bit) of the signature is evaluated 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 revealing the unpuncturable key without revealing the offset 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 is evaluated as follows:

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

New parameter set based on MPC-in-the-head. For the optimisation by MPC-in-the-head, we consider the security level 128-bit as shown in Table 5. Here we set the N to be 10. Compared with the data in Table 4 as used in the current ALTEQ specification [15], we can see that the signature sizes in Table 5 are between 64% to 72% of the sizes in Table 4.

Parameters					Size in Bytes	
n	q	C	M	K	Public key	Signature
13	$2^{32}-5$	7	84	22	8024	15896
		458	16	14	523968	9528

Table 4. Parameters of 128-bit security from [15].

Parameters					Size in Bytes	
n	q	C	M	K	pubkey size	sig size
13	$2^{32}-5$	7	94	13	8024	10132
		458	13	10	523968	6856

Table 5. Parameters of 128-bit security using the MPC-in-the-head paradigm with $N = 10$.

References

1. Abdalla, M., Fouque, P., Lyubashevsky, V., Tibouchi, M.: Tightly-secure signatures from lossy identification schemes. In: Pointcheval, D., Johansson, T. (eds.)

Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7237, pp. 572–590. Springer (2012)
2. Alamati, N., Feo, L.D., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. In: Moriai, S., Wang, H. (eds.) 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. Lecture Notes in Computer Science, vol. 12492, pp. 411–439. Springer (2020)
3. Babai, L.: 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. pp. 684–697 (2016)
4. Barenghi, A., Biasse, J.F., Ngo, T., Persichetti, E., Santini, P.: Advanced signature functionalities from the code equivalence problem. International Journal of Computer Mathematics: Computer Systems Theory **7**(2), 112–128 (2022)
5. Barenghi, A., Biasse, J.F., Ngo, T., Persichetti, E., Santini, P.: Advanced signature functionalities from the code equivalence problem. International Journal of Computer Mathematics: Computer Systems Theory **7**(2), 112–128 (2022)
6. Barenghi, A., Biasse, J.F., Persichetti, E., Santini, P.: Less-fm: fine-tuning signatures from the code equivalence problem. In: Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12. pp. 23–43. Springer (2021)
7. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. pp. 62–73 (1993)
8. Bellini, E., Esser, A., Sanna, C., Verbel, J.: Mr-dss–smaller minrank-based (ring-) signatures. In: Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings. pp. 144–169. Springer (2022)
9. Beullens, W.: Graph-theoretic algorithms for the alternating trilinear form equivalence problem. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III. Lecture Notes in Computer Science, vol. 14083, pp. 101–126. Springer (2023). https://doi.org/10.1007/978-3-031-38548-3_4, https://doi.org/10.1007/978-3-031-38548-3_4
10. Beullens, W., Dobson, S., Katsumata, S., Lai, Y.F., Pintore, F.: Group signatures and more from isogenies and lattices: Generic, simple, and efficient. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022. pp. 95–126. Springer International Publishing, Cham (2022)
11. Beullens, W., Feo, L.D., Galbraith, S.D., Petit, C.: Proving knowledge of isogenies – a survey. Cryptology ePrint Archive, Paper 2023/671 (2023), https://eprint.iacr.org/2023/671, https://eprint.iacr.org/2023/671
12. Beullens, W., Katsumata, S., Pintore, F.: Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In: Moriai, S., Wang, H. (eds.) 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. Lecture Notes in Computer Science, vol. 12492, pp. 464–492. Springer (2020). https://doi.org/10.1007/978-3-030-64834-3_16, https://doi.org/10.1007/978-3-030-64834-3_16

13. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient isogeny based signatures through class group computations. In: Advances in Cryptology - ASIACRYPT 2019. Lecture Notes in Computer Science, vol. 11921, pp. 227–247. Springer (2019)
14. Biasse, J., Micheli, G., Persichetti, E., Santini, P.: LESS is more: Code-based signatures without syndromes. In: Nitaj, A., Youssef, A.M. (eds.) Progress in Cryptology - AFRICACRYPT 2020 - 12th International Conference on Cryptology in Africa, Cairo, Egypt, July 20-22, 2020, Proceedings. Lecture Notes in Computer Science, vol. 12174, pp. 45–65. Springer (2020). https://doi.org/10.1007/978-3-030-51938-4_3, https://doi.org/10.1007/978-3-030-51938-4_3
15. Bläser, M., Duong, D.H., Narayanan, A.K., Plantard, T., Qiao, Y., Sipasseuth, A., Tang, G.: The alteq signature scheme: Algorithm specifications and supporting documentation (2023), https://pqcalteq.github.io/ALTEQ_spec_2023.09.18.pdf
16. Boneh, D.: The decision Diffie-Hellman problem. In: Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings. pp. 48–63 (1998). https://doi.org/10.1007/BFb0054851
17. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) 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. Lecture Notes in Computer Science, vol. 7073, pp. 41–69. Springer (2011). https://doi.org/10.1007/978-3-642-25385-0_3, https://doi.org/10.1007/978-3-642-25385-0_3
18. Bonnetain, X., Schrottenloher, A.: Quantum security analysis of CSIDH. In: Canteaut, A., Ishai, Y. (eds.) 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. Lecture Notes in Computer Science, vol. 12106, pp. 493–522. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_17, https://doi.org/10.1007/978-3-030-45724-2_17
19. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**(3-4), 235–265 (1997). https://doi.org/10.1006/jsco.1996.0125, http://dx.doi.org/10.1006/jsco.1996.0125, computational algebra and number theory (London, 1993)
20. Bouillaguet, C.: Etudes d'hypotheses algorithmiques et attaques de primitives cryptographiques. Ph.D. thesis, PhD thesis, Université Paris-Diderot–École Normale Supérieure (2011)
21. Bouillaguet, C., Faugère, J.C., Fouque, P.A., Perret, L.: Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In: International Workshop on Public Key Cryptography. pp. 473–493. Springer (2011)
22. Bouillaguet, C., Fouque, P., Véber, A.: Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In: Advances in Cryptology - EUROCRYPT 2013. pp. 211–227 (2013)
23. Brassard, G., Yung, M.: One-way group actions. In: Advances in Cryptology - CRYPTO 1990. pp. 94–107 (1990)
24. Brooksbank, P.A., Li, Y., Qiao, Y., Wilson, J.B.: Improved algorithms for alternating matrix space isometry: From theory to practice. In: Grandoni, F., Herman, G., Sanders, P. (eds.) 28th Annual European Symposium on Algorithms, ESA 2020, September 7-9, 2020, Pisa, Italy (Virtual Conference). LIPIcs,

vol. 173, pp. 26:1–26:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2020). https://doi.org/10.4230/LIPICS.ESA.2020.26, https://doi.org/10.4230/LIPIcs.ESA.2020.26
25. Carozza, E., Couteau, G., Joux, A.: Short signatures from regular syndrome decoding in the head. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 532–563. Springer (2023)
26. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). pp. 395–427. Springer (2018)
27. Childs, A., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology **8**(1), 1–29 (2014)
28. Chou, T., Niederhagen, R., Persichetti, E., Randrianarisoa, T.H., Reijnders, K., Samardjiska, S., Trimoska, M.: Take your meds: Digital signatures from matrix code equivalence. In: Progress in Cryptology - AFRICACRYPT 2023 (2023), to appear
29. Cohen, A.M., Helminck, A.G.: Trilinear alternating forms on a vector space of dimension 7. Communications in algebra **16**(1), 1–25 (1988)
30. Couveignes, J.M.: Hard homogeneous spaces. IACR Cryptology ePrint Archive (2006), http://eprint.iacr.org/2006/291
31. Couvreur, A., Debris-Alazard, T., Gaborit, P.: On the hardness of code equivalence problems in rank metric. arXiv preprint arXiv:2011.04611 (2020)
32. D'Alconzo, G., Gangemi, A.: Trifors: Linkable trilinear forms ring signature. Cryptology ePrint Archive (2022)
33. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory **22**(6), 644–654 (1976)
34. Dinur, I., Nadler, N.: Multi-target attacks on the picnic signature scheme and related protocols. In: Ishai, Y., Rijmen, V. (eds.) 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. Lecture Notes in Computer Science, vol. 11478, pp. 699–727. Springer (2019). https://doi.org/10.1007/978-3-030-17659-4_24, https://doi.org/10.1007/978-3-030-17659-4_24
35. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Security of the fiat-shamir transformation in the quantum random-oracle model. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 356–383. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_13, https://doi.org/10.1007/978-3-030-26951-7_13
36. Ducas, L., van Woerden, W.: 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. pp. 643–673. Springer (2022)
37. El Kaafarani, A., Katsumata, S., Pintore, F.: Lossy CSI-FiSh: Efficient Signature Scheme with Tight Reduction to Decisional CSIDH-512. In: Public-Key Cryptog-

raphy - PKC 2020. Lecture Notes in Computer Science, vol. 12111, pp. 157–186. Springer (2020)
38. Esgin, M.F., Steinfeld, R., Zhao, R.K.: Matrict+: More efficient post-quantum private blockchain payments. In: 2022 IEEE Symposium on Security and Privacy (SP). pp. 1281–1298. IEEE (2022)
39. Esgin, M.F., Zhao, R.K., Steinfeld, R., Liu, J.K., Liu, D.: Matrict: efficient, scalable and post-quantum blockchain confidential transactions protocol. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. pp. 567–584 (2019)
40. Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., Shor, P.: Quantum money from knots. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. pp. 276–289 (2012)
41. Faugère, J., Perret, L.: Polynomial equivalence problems: Algorithmic and theoretical aspects. In: Advances in Cryptology - EUROCRYPT 2006. pp. 30–47 (2006)
42. Feo, L.D., Galbraith, S.D.: Seasign: Compact isogeny signatures from class group actions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science, vol. 11478, pp. 759–789. Springer (2019). https://doi.org/10.1007/978-3-030-17659-4_26
43. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Advances in Cryptology – CRYPTO 1986. pp. 186–194 (1986)
44. Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. J. ACM **38**(3), 691–729 (1991). https://doi.org/10.1145/116825.116852
45. Grochow, J.A., Qiao, Y.: On p-group isomorphism: search-to-decision, counting-to-decision, and nilpotency class reductions via tensors. In: 36th Computational Complexity Conference, LIPIcs. Leibniz Int. Proc. Inform., vol. 200, pp. Art. No. 16, 38. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern (2021). https://doi.org/10.4230/LIPIcs.CCC.2021.16
46. Grochow, J.A., Qiao, Y.: On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness. In: Lee, J.R. (ed.) 12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference. LIPIcs, vol. 185, pp. 31:1–31:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2021). https://doi.org/10.4230/LIPIcs.ITCS.2021.31, https://doi.org/10.4230/LIPIcs.ITCS.2021.31
47. Grochow, J.A., Qiao, Y., Tang, G.: Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. In: Bläser, M., Monmege, B. (eds.) 38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021, March 16-19, 2021, Saarbrücken, Germany (Virtual Conference). LIPIcs, vol. 187, pp. 38:1–38:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2021)
48. Hallgren, S., Moore, C., Rötteler, M., Russell, A., Sen, P.: Limitations of quantum coset states for graph isomorphism. J. ACM **57**(6), 34:1–34:33 (Nov 2010). https://doi.org/10.1145/1857914.1857918
49. Hora, J., Pudlák, P.: Classification of 8-dimensional trilinear alternating forms over gf (2). Communications in Algebra **43**(8), 3459–3471 (2015)
50. Hora, J., Pudlák, P.: Classification of 9-dimensional trilinear alternating forms over gf (2). Finite Fields and Their Applications **70**, 101788 (2021)
51. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Zero-knowledge from secure multiparty computation. In: STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing. pp. 21–30. ACM, New

York (2007). https://doi.org/10.1145/1250790.1250794, https://doi.org/10.1145/1250790.1250794
52. Ji, Z., Qiao, Y., Song, F., Yun, A.: General linear group action on tensors: A candidate for post-quantum cryptography. In: Hofheinz, D., Rosen, A. (eds.) Theory of Cryptography - 17th International Conference, TCC 2019. vol. 11891, pp. 251–281. Springer (2019)
53. Joux, A.: Mpc in the head for isomorphisms and group actions. Cryptology ePrint Archive, Paper 2023/664 (2023), https://eprint.iacr.org/2023/664, https://eprint.iacr.org/2023/664
54. Katz, J., Wang, N.: Efficiency improvements for signature schemes with tight security reductions. In: Proceedings of the 10th ACM conference on Computer and communications security. pp. 155–164 (2003)
55. Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In: Advances in Cryptology – EUROCRYPT 2018. pp. 552–586. Springer (2018)
56. Köbler, J., Schöning, U., Torán, J.: The Graph Isomorphism Problem. Basel Birkhüser (1993)
57. Liu, J.K., Wong, D.S.: Linkable ring signatures: Security models and new schemes. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganà, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) Computational Science and Its Applications - ICCSA 2005, International Conference, Singapore, May 9-12, 2005, Proceedings, Part II. Lecture Notes in Computer Science, vol. 3481, pp. 614–623. Springer (2005). https://doi.org/10.1007/11424826_65, https://doi.org/10.1007/11424826_65
58. Liu, Q., Zhandry, M.: Revisiting post-quantum fiat-shamir. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 326–355. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_12, https://doi.org/10.1007/978-3-030-26951-7_12
59. Lu, X., Au, M.H., Zhang, Z.: Raptor: A practical lattice-based (linkable) ring signature. In: Deng, R.H., Gauthier-Umaña, V., Ochoa, M., Yung, M. (eds.) Applied Cryptography and Network Security. pp. 110–130. Springer International Publishing, Cham (2019)
60. Lyubashevsky, V., Nguyen, N.K., Seiler, G.: Smile: set membership from ideal lattices with applications to ring signatures and confidential transactions. In: Annual International Cryptology Conference. pp. 611–640. Springer (2021)
61. McKay, B.D.: Practical graph isomorphism. Congr. Numer. pp. 45–87 (1980)
62. McKay, B.D., Piperno, A.: Practical graph isomorphism, II. J. Symb. Comput. **60**, 94–112 (2014)
63. Midoune, N., Noui, L.: Trilinear alternating forms on a vector space of dimension 8 over a finite field. Linear and Multilinear Algebra **61**(1), 15–21 (2013)
64. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Advances in Cryptology – EUROCRYPT 1996. pp. 33–48 (1996)
65. Peikert, C.: He gives c-sieves on the CSIDH. In: Canteaut, A., Ishai, Y. (eds.) 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. Lecture Notes in Computer Science, vol. 12106, pp. 463–492. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_16, https://doi.org/10.1007/978-3-030-45724-2_16

66. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. Journal of cryptology **13**(3), 361–396 (2000)
67. Ran, L., Samardjiska, S., Trimoska, M.: Algebraic attack on the alternating trilinear form equivalence problem (2023), presented at CBCrypto'23
68. Regev, O.: Quantum computation and lattice problems. SIAM J. Comput. **33**(3), 738–760 (2004). https://doi.org/10.1137/S0097539703440678
69. Reijnders, K., Samardjiska, S., Trimoska, M.: Hardness estimates of the code equivalence problem in the rank metric. Designs, Codes and Cryptography pp. 1–30 (2024)
70. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) 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. Lecture Notes in Computer Science, vol. 2248, pp. 552–565. Springer (2001). https://doi.org/10.1007/3-540-45682-1_32, https://doi.org/10.1007/3-540-45682-1_32
71. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997). https://doi.org/10.1137/S0097539795293172, https://doi.org/10.1137/S0097539795293172
72. of Standards, N.I., Technology: Call for additional digital signature schemes for the post-quantum cryptography standardization process (October 2022), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf
73. Stolbunov, A.: Cryptographic schemes based on isogenies. Ph.D. thesis, Norwegian University of Science and Technology (2012)
74. Sun, S., Au, M.H., Liu, J.K., Yuen, T.H.: Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In: Foley, S.N., Gollmann, D., Snekkenes, E. (eds.) Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II. Lecture Notes in Computer Science, vol. 10493, pp. 456–474. Springer (2017). https://doi.org/10.1007/978-3-319-66399-9_25, https://doi.org/10.1007/978-3-319-66399-9_25
75. Tang, G., Duong, D.H., Joux, A., Plantard, T., Qiao, Y., Susilo, W.: Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In: Dunkelman, O., Dziembowski, S. (eds.) 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. Lecture Notes in Computer Science, vol. 13277, pp. 582–612. Springer (2022). https://doi.org/10.1007/978-3-031-07082-2_21, https://doi.org/10.1007/978-3-031-07082-2_21
76. Tsang, P.P., Wei, V.K.: Short linkable ring signatures for e-voting, e-cash and attestation. In: Deng, R.H., Bao, F., Pang, H., Zhou, J. (eds.) Information Security Practice and Experience, First International Conference, ISPEC 2005, Singapore, April 11-14, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3439, pp. 48–60. Springer (2005). https://doi.org/10.1007/978-3-540-31979-5_5, https://doi.org/10.1007/978-3-540-31979-5_5
77. Unruh, D.: Quantum proofs of knowledge. In: Advances in Cryptology – Eurocrypt 2012. LNCS, vol. 7237, pp. 135–152. Springer (April 2012)
78. Unruh, D.: Computationally binding quantum commitments. In: Advances in Cryptology – Eurocrypt 2016. pp. 497–527. Springer (2016)

79. Unruh, D.: Post-quantum security of fiat-shamir. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 65–95. Springer (2017)
80. Yamakawa, T., Zhandry, M.: Classical vs quantum random oracles. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 568–597. Springer (2021)
81. Yuen, T.H., Esgin, M.F., Liu, J.K., Au, M.H., Ding, Z.: Dualring: Generic construction of ring signatures with efficient instantiations. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology – CRYPTO 2021. pp. 251–281. Springer International Publishing, Cham (2021)
82. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019. pp. 239–268. Springer International Publishing, Cham (2019)

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

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

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 supports this property.

A.2 Properties of the Σ-protocol based on abstract group actions

Completeness. It is clear that the honest prover with the statement and witness (x, w) following the $\alpha(\mathsf{G}, \mathsf{S})$-$\mathsf{GMW}$ protocol 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 both are uniform distributions 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 9. 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 6.1, 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 Proof of Theorem 2

To prove Theorem 2 we first need some preparations.

Post-Quantum 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 adversaries with eavesdropping attacks.

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*

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

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 [58, Theorem 1]. Since the perfect unique response is a stronger property than the weakly collapsing property, we can state the result in [58] as follows.

Theorem 5 ([58]). *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 $\alpha(\mathsf{G},\mathsf{S})$-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 5. □

Security of $\alpha(\mathsf{G},\mathsf{S})$-GMW-FS-$\mathcal{O}(s_0)$ signature. Liu and Zhandry [58, 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 [82]. 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 6 ([58], 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 6. □

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.□

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

C.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 the original challenge space is binary. One can observe that the response with challenge $\mathsf{cha} = 0$ is more costly than that challenge $\mathsf{cha} = 1$. Instead of choosing the challenge bit uniformly in each round, we execute OR sigma protocol $M > \lambda$ rounds and fix exactly K rounds with challenge $\mathsf{cha} = 0$. To satisfy the λ bits of security, we can choose proper parameters M, K such that $\binom{M}{K} \geq 2^{\lambda}$. Denote $C_{M,K}$ as the set of strings in $\{0,1\}^M$ with K-bits of 0.
2. With the unbalanced challenge space technique, we do M executions of OR sigma protocol and $M-K$ executions respond with random seeds. Instead of randomly sample M independent seeds, we can utilize seed tree to generate these seeds. Then prover can responsd with $\mathsf{seeds}_{\mathsf{internal}} \leftarrow \mathsf{ReleaseSeeds}(\mathsf{seed}_{\mathsf{root}}, \mathbf{c})$ instead of $M-K$ seeds, where $\mathbf{c}$ is randomly sampled from $C_{M,K}$. The verifier can use $\mathsf{seeds}_{\mathsf{internal}}$ and $\mathbf{c}$ to recover $M-K$ seeds. Note that here we divide M leaves into K parts, and put a leaf corresponding to $c_{i,i\in[M]} = 0$ in each part, which leads to a smaller upper bound $K \cdot \log_2(\frac{M}{K})$ for the internal seeds.
3. Adding salt is a well-known technique that allows us to have tighter security proofs for zero-knowledge. Also it avoids multi-target attacks, as in [34], without affecting too much efficiency.

$\mathcal{P}_1(s_1, \ldots, s_N)$

1 : $\mathsf{seed} \xleftarrow{\$} \{0,1\}^\lambda$
2 : $(h, \mathsf{bits}_1, \ldots, \mathsf{bits}_N) \leftarrow \mathsf{PRG}(\mathsf{seed})$
3 : **for** i from 1 to N **do**
4 : $\quad t_i \leftarrow \alpha(h, s_i)$
5 : $\quad \mathsf{C}_i \leftarrow \mathsf{Com}(t_i, \mathsf{bits}_i)$
6 : $(\mathsf{root}, \mathsf{tree}) \leftarrow \mathsf{MerkleTree}(\mathsf{C}_1, \ldots, \mathsf{C}_N)$
7 : $\mathsf{com} \leftarrow \mathsf{root}$
8 : The prover $\mathcal{P}$ sends the commitment com to the verifier $\mathcal{V}$

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

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

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

1 : $c \leftarrow \mathsf{cha}$
2 : **if** $c = 0$ **then**
3 : $\quad f \leftarrow h * g_I$
4 : $\quad \mathsf{path} \leftarrow \mathsf{getMerklePath}(\mathsf{tree}, I)$
5 : $\quad \mathsf{rsp} \leftarrow (f, \mathsf{path}, \mathsf{bits}_I)$
6 : **else**
7 : $\quad \mathsf{rsp} \leftarrow \mathsf{seed}$
8 : The prover $\mathcal{P}$ sends the response rsp to the verifier $\mathcal{V}$

$\mathcal{V}_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, s_0, s_1, \ldots, s_N)$

1 : $(\mathsf{root}, c) \leftarrow (\mathsf{com}, \mathsf{cha})$
2 : **if** $c = 0$ **then**
3 : $\quad (f, \mathsf{path}, \mathsf{bits}) \leftarrow \mathsf{rsp}$
4 : $\quad \tilde{t} \leftarrow \alpha(f, s_0)$
5 : $\quad \tilde{\mathsf{C}} \leftarrow \mathsf{Com}(\tilde{t}, \mathsf{bits})$
6 : $\quad \widetilde{\mathsf{root}} \leftarrow \mathsf{ReconstructRoot}(\tilde{\mathsf{C}}, \mathsf{path})$
7 : $\quad$ The verifier $\mathcal{V}$ outputs accept if $\widetilde{\mathsf{root}} = \mathsf{root}$, else outputs reject
8 : **else**
9 : $\quad \mathsf{seed} \leftarrow \mathsf{rsp}$
10 : $\quad \widetilde{\mathsf{root}} \leftarrow \mathcal{P}_1((s_1, \ldots, s_N), \mathsf{seed})$
11 : $\quad$ The verifier $\mathcal{V}$ outputs accept if $\widetilde{\mathsf{root}} = \mathsf{root}$, else outputs reject

Fig. 4. OR-Sigma protocol.

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 $\mathcal{O}_{\mathsf{s}i}$.

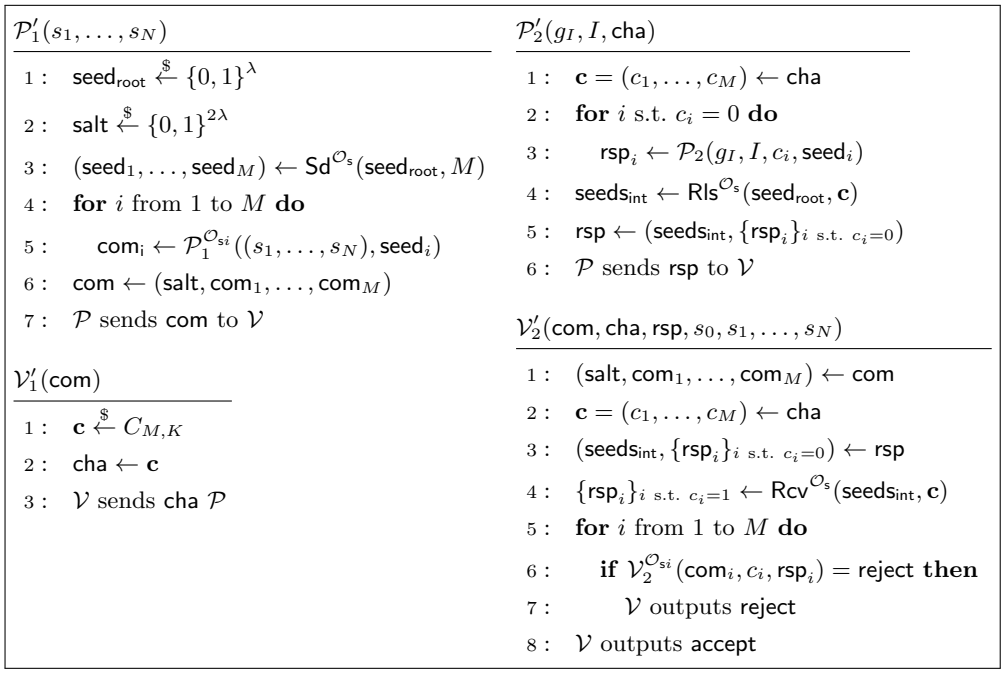

Fig. 5. Optimized OR sigma protocol.

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 shown in Figure 5 as follows.

Corollary 5. *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 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. □

C.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 λ.
Output: Public parameter: variable number $n \in \mathbb{N}$, a prime power q and an element $s_0 \in S$.

1 Choose $n \in \mathbb{N}$ and a prime power q corresponding to the security parameter λ.
2 Randomly sample an element s_0 from S.
3 **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 $s_i = \alpha(g_i, s_0)$.

1 Randomly sample a group element g_i from G.
2 Compute $s_i \leftarrow \alpha(g_i, s_0)$.
3 **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 10. Since the optimized base OR sigma protocol is proved to satisfy all properties in Corollary 5, and by Appendix A.1 in [12], the ring signature in Algorithm 1, 2, 3 and 4 has correctness, anonymity and unforgeability.

D Linkable ring signature from abstract group actions

D.1 Linkable ring signatures

We first review some basic notions related to linkable ring signatures.

A linkable ring signature is a variant of a 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 12 (Linkable ring signature). *A linkable ring signature scheme* Π_{LRS} *consists of three PPT algorithms in the ring signature in addition with a PPT algorithm such that:*

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

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

$\{\mathsf{vk}_i\}_{i\in D_b}$, it always holds that $\mathsf{LRS.Verify}(\mathsf{R},\mathsf{M},\sigma_b)=1$ and $\mathsf{LRS.Link}(\sigma_0,\sigma_1)=1$.

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

(1) The challenger runs $\mathsf{pp}\leftarrow\mathsf{LRS.SetUp}(1^\lambda)$ and send pp to $\mathcal{A}$.
(2) $\mathcal{A}$ generates public keys and secret keys $(\{\mathsf{vk}_i,\mathsf{sk}_i\})\leftarrow\mathsf{LRS.KeyGen}(\mathsf{pp}))$ for $i\in[N]$, and then produces a set $(\sigma_i,\mathsf{M}_i,\mathsf{R}_i)_{i\in[N+1]}$.
(3) We say $\mathcal{A}$ wins this game if all the following conditions are satisfied:
- $\forall i\in[N+1]$, have $\mathsf{R}_i\subseteq\mathsf{VK}$;
- $\forall i\in[N+1]$, have $\mathsf{LRS.Verify}(\mathsf{R}_i,\mathsf{M}_i,\sigma_i)=1$;
- $\forall i,j\in[N+1]$, where $i\neq j$, have $\mathsf{LRS.Link}(\sigma_i,\sigma_j)=0$.

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

(1) The challenger runs $\mathsf{pp}\leftarrow\mathsf{LRS.SetUp}(1^\lambda)$ generates public keys and secret keys $(\{\mathsf{vk}_i,\mathsf{sk}_i\})\leftarrow\mathsf{RS.KeyGen}(\mathsf{pp})$ for $i\in[N]$ and it also samples a ramdom bit $b\in\{0,1\}$. Then it sends the public keys $\mathsf{VK}=\{\mathsf{vk}_0,\ldots,\mathsf{vk}_N\}$ to $\mathcal{A}$.
(2) $\mathcal{A}$ sends two public keys $\mathsf{vk}_0',\mathsf{vk}_1'$ to the challenger, and we let $\mathsf{sk}_0',\mathsf{sk}_1'$ be the corresponding secret keys.
(3) The challenger outputs r_i of the corresponding $\mathsf{vk}_i\subseteq\mathsf{VK}\setminus\{\mathsf{vk}_0',\mathsf{vk}_1'\}$.
(4) $\mathcal{A}$ chooses a public key $\mathsf{vk}\in\{\mathsf{vk}_0',\mathsf{vk}_1'\}$ and provides a message M and a ring R that $\{\mathsf{vk}_0',\mathsf{vk}_1'\}\subseteq\mathsf{R}$ to query the challenger:
- If $\mathsf{vk}=\mathsf{vk}_0'$, the challenger outputs the signature $\mathsf{LRS.Sign}(sk_b,\mathsf{R},\mathsf{M})\rightarrow\sigma$.
- If $\mathsf{vk}=\mathsf{vk}_1'$, the challenger outputs the signature $\mathsf{LRS.Sign}(sk_{1-b},\mathsf{R},\mathsf{M})\rightarrow\sigma$.
(5) $\mathcal{A}$ check if $\mathsf{LRS.Verify}(\mathsf{R},\mathsf{M},\sigma)=1$, and if so outputs b'. If $b=b'$, we say $\mathcal{A}$ wins this game.

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

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

(1) The challenger 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 $\mathsf{LRS.Sign}(\mathsf{sk}_i,\mathsf{R},\mathsf{M})\rightarrow\sigma$ to $\mathcal{A}$ and adds $(i,\mathsf{R},\mathsf{M})$ to SL.
- $(\mathsf{corrupt},i)$: The challenger sends the random bits r_i to $\mathcal{A}$ and adds vk_i to CL.

(3) We say $\mathcal{A}$ wins this game if $\mathcal{A}$ outputs $(\mathsf{R}', \mathsf{M}', \sigma')$ such that $(\cdot, \mathsf{M}', \mathsf{R}') \notin \mathsf{SL}$, $\mathsf{LRS.Verify}(\mathsf{R}', \mathsf{M}', \sigma') = 1$, and for some query $(i, \mathsf{R}, \mathsf{M}) \in \mathsf{SL}$ where the identity i satisfies $\mathsf{vk}_i \in \mathsf{VK} \setminus \mathsf{CL}$, the challenger outputs a signature σ that $\mathsf{LRS.Link}(\sigma', \sigma) = 1$ holds.

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

D.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 [5,28].

Definition 13. *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 14 (Pair-pseudorandom). *The pseudorandom pairs equivalence under group action problem with 2 pairs of elements ask 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 [4].

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

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

for the relaxed special soundness.

$\mathcal{P}_1(s_1, \ldots, s_N, r)$

1 : $\mathsf{seed} \xleftarrow{\$} \{0,1\}^\lambda$
2 : $(h, \mathsf{bits}_1, \ldots, \mathsf{bits}_N) \leftarrow \mathsf{PRG}(\mathsf{seed})$
3 : $r' \leftarrow \beta(h, r)$
4 : **for** i from 1 to N **do**
5 : $\quad t_i \leftarrow \alpha(h, s_i)$
6 : $\quad \mathsf{C}_i \leftarrow \mathsf{Com}(t_i, \mathsf{bits}_i)$
7 : $(\mathsf{root}, \mathsf{tree}) \leftarrow \mathsf{MerkleTree}(\mathsf{C}_1, \ldots, \mathsf{C}_N)$
8 : $h \leftarrow \mathcal{H}_{\mathsf{Coll}}(r', \mathsf{root})$
9 : $\mathsf{com} \leftarrow h$
10 : $\mathcal{P}$ sends com to $\mathcal{V}$

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

1 : $c \xleftarrow{\$} \{0,1\}$
2 : $\mathsf{cha} \leftarrow c$
3 : $\mathcal{V}$ sends cha to $\mathcal{P}$

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

1 : $c \leftarrow \mathsf{cha}$
2 : **if** $c = 0$ **then**
3 : $\quad f \leftarrow h * g_I$
4 : $\quad \mathsf{path} \leftarrow \mathsf{getMerklePath}(\mathsf{tree}, I)$
5 : $\quad \mathsf{rsp} \leftarrow (f, \mathsf{path}, \mathsf{bits}_I)$
6 : **else**
7 : $\quad \mathsf{rsp} \leftarrow \mathsf{seed}$
8 : $\mathcal{P}$ sends rsp to $\mathcal{V}$

$\mathcal{V}_2(\mathsf{com}, \mathsf{cha}, \mathsf{rsp}, s_0, s_1, \ldots, s_N, r_0, r)$

1 : $(h, c) \leftarrow (\mathsf{com}, \mathsf{cha})$
2 : **if** $c = 0$ **then**
3 : $\quad (f, \mathsf{path}, \mathsf{bits}) \leftarrow \mathsf{rsp}$
4 : $\quad \tilde{t} \leftarrow \alpha(f, s_0)$
5 : $\quad \tilde{\mathsf{C}} \leftarrow \mathsf{Com}(\tilde{t}, \mathsf{bits})$
6 : $\tilde{r'} \leftarrow \beta(f, r_0)$
7 : $\quad \widetilde{\mathsf{root}} \leftarrow \mathsf{ReconstructRoot}(\tilde{\mathsf{C}}, \mathsf{path})$
8 : $\quad$ **if** $h = \mathcal{H}_{\mathsf{Coll}}(\tilde{r'}, \widetilde{\mathsf{root}})$ **then**
9 : $\quad\quad \mathcal{V}$ outputs accept
10 : $\quad$ **else**
11 : $\quad\quad \mathcal{V}$ outputs reject
12 : **else**
13 : $\quad \mathsf{seed} \leftarrow \mathsf{rsp}$
14 : $\quad \widetilde{\mathsf{root}} \leftarrow \mathcal{P}_1((s_1, \ldots, s_N), \mathsf{seed})$
15 : $\quad$ **if** $h = \mathcal{H}_{\mathsf{Coll}}(\tilde{r'}, \widetilde{\mathsf{root}})$ **then**
16 : $\quad\quad \mathcal{V}$ outputs accept
17 : $\quad$ **else**
18 : $\quad\quad \mathcal{V}$ outputs reject

Fig. 6. Linkable OR sigma protocol.

Theorem 7. *Assume the stabilizers* $\mathrm{Stab}(s_0)$ *and* $\mathrm{Stab}(r_0)$ *are trivial and the pair-pseudorandom problem defined in Definition 14 is hard. The linkable OR sigma protocol shown in Figure 6 after the optimization satisfies the properties defined in Definition 13.*

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

Proof. By Theorem 7 and [12, Theorem 4.5,Theorem 4.6], our OR sigma protocol satisfies correctness, relaxed special soundness and honest-verifier zero-knowledge. □

D.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 to a link algorithm.

Algorithm 5: Set Up

Input: The security parameter λ.
Output: Public parameter: variable number $n \in \mathbb{N}$, a prime power q and elements $s_0, r_0 \in S$.

1 Choose $n \in \mathbb{N}$ and a prime power q corresponding to the security parameter λ.
2 Randomly sample elements s_0, r_0 from S.
3 **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 $s_i = \alpha(g_i, s_0)$.

1 Randomly sample a group element g_i from G.
2 Compute $s_i \leftarrow \alpha(g_i, s_0)$.
3 **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 the same secret key. "No" otherwise.

```
if r = r' then
    return Yes
else
    return No
```

Algorithm 8: Linkable signing procedure

Input: The public key: $s_0, \ldots, s_N$. The private key: g_I. The security parameter λ. The message msg. The commitment scheme $\mathsf{Com} : \{0,1\}^* \to \{0,1\}^\lambda$. A hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$.

Output: The signature Sig on msg.

$r \leftarrow \beta(g_I, r_0)$

$\mathsf{com} = (\mathsf{salt}, (\mathsf{com}_i)_{i\in[M]}) \leftarrow \mathcal{P}_1'(s_0, s_1, \ldots, s_N, r)$

$\mathsf{cha} \leftarrow \mathcal{H}(\mathsf{msg}||s_1||\cdots||s_N||r||\mathsf{com})$

$\mathsf{rsp} \leftarrow \mathcal{P}_2'(g_I, I, \mathsf{cha})$

return $\mathsf{Sig} = (\mathsf{salt}, r, \mathsf{cha}, \mathsf{rsp})$

Algorithm 9: Linkable verification procedure

Input: The public key $s_0, \ldots, s_N \in S$. The signature $\mathsf{Sig} = (\mathsf{salt}, r, \mathsf{cha}, \mathsf{rsp})$. 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.

$\mathsf{com} \leftarrow \mathsf{RecoverCom}(s_0, \ldots, s_N, r, \mathsf{salt}, \mathsf{cha}, \mathsf{rsp})$

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 11. Since the linkable OR sigma protocol is proved to satisfy all conditions in Corollary 6, 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 12. The above security proof is derived from the rewinding technique, but its security reduction is non-tight due to the loss of *forking lemma*[43]. Beullens et.al. proposed a new property called online extractability [10], which is used to obtain an almost tight security reduction of ring signature. Further they use some techniques including the Katz-Wang technique [54] to obtain the

tight security. Since our ring signature follows their construction, if append the above property and techniques to our ring signature, we can get a tight security reduction as well.