PyuQuMuQu: Attacks on MQ-Based Linkable Ring Signatures and a New 5-Pass Construction

Freeman Slaughter

University of South Florida, Tampa, FL, USA
fslaughter@usf.edu

Abstract. Linkable ring signatures (LRS) let a member sign on behalf of a group anonymously while ensuring that any two signatures by the same signer are publicly linkable, a major component in e-voting and cryptocurrencies. Random systems of multivariate quadratic (MQ) equations are one of the most conservative post-quantum assumptions, yet there are only two MQ-based LRS's in the literature: the first is due to Omar, Padhye, and Dey, and the second by Namdeo, Mishra, and Srivastava. Both of these schemes are built from Sakumoto-style identification protocols whose soundness for signatures is well-established, but in the ring setting was never re-examined. We present a sumset attack that lets a signer with no knowledge of an MQ solution universally forge accepting signatures in both protocols. In the same vein, we show that the four-challenge MQ protocol of Monteiro, Goya, and Terada (as transcribed in Namdeo, Mishra, and Srivastava) has soundness error 3/4 instead of the claimed 1/2, and this bound is tight. Its natural repair does achieve 1/2, but is only 3-special sound, so the two-transcript extraction argument upon which their LRS relies upon does not hold regardless.

We then build PyuQuMuQu, a plausibly post-quantum MQ-based LRS from a 5-pass proof with a d-dimensional vector first challenge and an additively split second challenge, whose soundness error is $\frac{1}{2} + \frac{N}{2(q^d-1)}$ for a ring with $N \leq q^d - 1$ members.

We demonstrate anonymity, linkability, and non-slanderability in the random-oracle model under explicitly stated assumptions involving random MQ maps. PyuQuMuQu attains 355 kB signature sizes for a ring with 4 members 128 bits of security.

1 Introduction

Ring signatures are an advanced cryptographic functionality which lets a signer prove that a message was signed by some member of a set without revealing which one and without any coordination with the other members. A linkable ring signature, introduced by Liu, Wei, and Wong [32], adds a linking tag: two

PyuQuMuQu: Pseudonymity Using Quantum-resistant Multivariate Quadratics.

This research was supported by the National Science Foundation (Grant Number DMS-2342254).

signatures by the same secret key are publicly recognizable as such, while signatures by different keys remain unlinkable. This is precisely the feature that anonymous e-voting and cryptocurrency transactions require. The standard security notions are anonymity, linkability, and non-slanderability, formalized by Liu, Au, Susilo, and Zhou [31], who also showed that in their model the last two imply existential unforgeability. There is a nuance with linkability: a recent analysis of Balla and Chaidos [6] showed that an LRS in which an adversary knows multiple keys can produce more unlinkable signatures than keys, so we demonstrate linkability against adversarially chosen keys.

Most post-quantum LRS proposals are lattice-based, from the one-time schemes of Torres et al. [1] to logarithmic-size constructions [10], with code-based [33] variants rather lagging behind. More recently, generic proof systems have been turned into LRS's: Xue, Lu, Au, and Zhang [43] outline how to build an LRS from any signature of knowledge and instantiate it with a STARK, Chiang et al. [16] obtain linkable and threshold ring signatures from VOLE-in-the-head with AES, and DualRing-PRF [44] uses MPC-in-the-head techniques with Legendre PRF's. The multivariate quadratic problem, which involves solving a random system of m quadratic equations in n variables over $\mathbb{F}_q$, is conspicuously underutilized in the literature. This is difficult to understand, because random MQ is an unusually straightforward post-quantum assumption: it has no structure to attack, its concrete hardness is well studied, and it underlies MQOM, one of the nine candidates that advanced to the third round of the May 2026 NIST additional signatures standardization effort [36]. The most advanced MQ ring signature is [23], which utilizes Threshold Computation in the Head to achieve very small signature sizes, but does not enjoy linkability – it additionally relies on MPC techniques, whereas ours does not.

The MQ-based LRS literature consists of two major schemes. Omar, Padhye, and Dey [39] gave the first, constructed on top of the 3-pass identification protocol of Sakumoto, Shirai, and Hiwatari [41], with reported signatures of about 1180 kB for 20 members at 128 bits of security. Namdeo, Mishra, and Srivastava [37] followed with a round-optimal variant built from the four-challenge protocol of Monteiro, Goya, and Terada [35], which boasts a soundness error of 1/2, down from 2/3.

1.1 Our Contributions

We present three main contributions.

Attacks: Section 3 presents a sumset attack on both existing MQ-based LRS schemes. These protocols distribute the verifier's challenge additively across the ring members, letting the signer select how the shares are split. We show that a signer who knows no MQ solution can prepare, for each ring member, a response that answers a fixed subset of sub-challenges, then use the freedom inherent in these shares (via Cauchy-Davenport for [39], or with direct computation for [37]) to force the challenge distribution into answerable ones. The result is a forgery that succeeds with probability 1, for any message, ring, and linking tag. Along the way, we show that the protocol of [35], as transcribed in Table 5 of [37],

is incomplete and has soundness error 3/4 rather than the stated 1/2: a cheating prover can answer three of the four challenges. Its natural repair restores completeness and error 1/2, but extraction necessitates three transcripts, which invalidates the two-transcript extraction lemma of [37] irregardless. We do not claim that [35] itself is flawed, rather the transcription that [37] builds on.

An MQ-based LRS: Section 4 proposes a 5-pass proof for an MQ relation whose first challenge is a vector $\boldsymbol{a} \in \mathbb{F}_q^d \setminus \{\mathbf{0}\}$ and whose second is a single bit $b \in \{0, 1\}$. The vector challenge makes this ring version work: Section 5 runs one instance for each of the N ring members, splits the bit challenge by XOR, and proves that a cheating prover can pass both bit challenges for at most one vector $\boldsymbol{a}$ per member – the result is a soundness error of $\frac{1}{2} + \frac{\min\{N,L\}}{2L}$ (Theorem 3), for $L = q^d - 1$, which is tight. The linking tag is $T = \mathcal{F}(s)$ for a second public quadratic map $\mathcal{F}$, and our proof works for the stacked relation $\mathcal{P}(s) = y_\pi$, $\mathcal{F}(s) = T$ at no extra soundness cost, though necessitates a careful parameter selection. The signature scheme (Section 6 onwards) follows from the standard Fiat-Shamir transform.

Secure MQ Assumptions: We prove our MQ LRS enjoys anonymity, linkability, and non-slanderability in the random-oracle model. Rather than simply assuming all MQ maps act as random oracles, we identify a minimal set of requirements:

1. the one-wayness of the stacked map $(\mathcal{P}, \mathcal{F})$ on planted inputs, which by Liu, Lu, and Yang [30], also supplies anonymity, and
2. key/tag consistency, the statement that no key y has two preimages with different tags, which permits linkability against malicious keys.

The second is not a standard MQ assumption: Section 5 shows it fails outright for $m_\mathcal{P} \leq n$ (Proposition 2) and gives the evidence for it when $m_\mathcal{P} = n + c$ with $c \geq \lambda / \log_2 q$.

2 Preliminaries

2.1 Notation

Let q be a prime power and λ the security parameter. The distinct and independent public membership and linking maps are

$$\mathcal{P} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{m_\mathcal{P}}, \quad \mathcal{F} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{m_\mathcal{F}},$$

both with only quadratic and linear terms, no constant terms. Each user samples their secret $s_i \in \mathbb{F}_q^n$ and publishes their public key $y_i = \mathcal{P}(s_i)$. The ring is then $R = (y_1, \ldots, y_N)$, and a signer with secret s prints the linking tag $T = \mathcal{F}(s) \in \mathbb{F}_q^{m_\mathcal{F}}$. The intended relation is

$$\mathcal{R}_{R,T} = \big\{(s, \pi) \mid \pi \in [N],\ \mathcal{P}(s) = y_\pi,\ \mathcal{F}(s) = T\big\}. \tag{1}$$

Given arbitrary quadratic maps, we can normalize them by

$$\mathcal{P}_0(x) = \mathcal{P}(x) - \mathcal{P}(0), \quad y_{i,0} = y_i - \mathcal{P}(0),$$
$$\mathcal{F}_0(x) = \mathcal{F}(x) - \mathcal{F}(0), \quad T_0 = T - \mathcal{F}(0),$$

which preserves the relation. We suppress subscripts for brevity.

For every such map A, define $G_A(u, v) = A(u + v) - A(u) - A(v)$. The map G_A is then bilinear.

Write, in stacked notation,

$$Q(x) = \begin{pmatrix} \mathcal{P}(x) \\ \mathcal{F}(x) \end{pmatrix}, \quad Y_i = \begin{pmatrix} y_i \\ T \end{pmatrix}, \quad G_Q = \begin{pmatrix} G_{\mathcal{P}} \\ G_{\mathcal{F}} \end{pmatrix}. \tag{2}$$

Thus $Q : \mathbb{F}_q^n \to \mathbb{F}_q^{m_Q}$, where $m_Q = m_{\mathcal{P}} + m_{\mathcal{F}}$.

2.2 Zero-Knowledge Proofs

Zero-knowledge proofs (ZKP's) [26] are a critical framework in privacy-oriented designs which permit a prover P to convince a verifier V that a statement is true, in a way that reveals no other information. For a relation $\mathcal{R}$, the prover wishes to convince the verifier that they know a witness w for a given statement x satisfying $(x; w) \in \mathcal{R}$. Since we only concern ourselves with 5-pass ZKP's, we adapt the traditional notion from [5]. All the algorithms we consider here are probabilistic polynomial-time (PPT).

Definition 1 (Zero-Knowledge Proof of Knowledge). A 5-pass interactive protocol is a ZKP proof of knowledge for a relation $\mathcal{R}$ with soundness error κ if it utilizes challenge spaces $\mathcal{C}_1, \mathcal{C}_2$, and the following hold:

1. **Completeness**: if the prover acts honestly and $(x; w) \in \mathcal{R}$, they get accepted,
2. **Soundness**: there exists a PPT extractor $\mathcal{E}$ such that for any prover P^* which V accepts with probability $\varepsilon > \kappa$, $\mathcal{E}$ outputs at witness w with $(x; w) \in \mathcal{R}$ in time that is polynomial in λ and $1/(\varepsilon - \kappa)$.
3. **Honest-verifier zero knowledge**: there exists a PPT simulator $\mathcal{S}$ which can generate an accepting transcript indistinguishable from an honest one, without w.

Repeating a (k_1, k_2)-special-sound protocol τ times in parallel reduces the knowledge error to κ^τ [3], and under the Fiat-Shamir paradigm [24] its non-interactive cost was analyzed in [4].

The protocols in this paper use a first challenge space of size $L = q^d - 1$, and a binary second challenge space, where $d = 1$ recovers the following notion [15].

Definition 2 ($(L, 2)$-Identification Scheme). An $(L, 2)$-identification scheme is a 5-pass interactive protocol where $\texttt{chal}_1$ is uniform from $\mathcal{C}_1$ and $\texttt{chal}_2$ is uniform from $\mathcal{C}_2$, where $|\mathcal{C}_1| = L$ and $|\mathcal{C}_2| = 2$. The natural choice is $\mathcal{C}_1 = \mathbb{F}_q^d \backslash \{\mathbf{0}\}$, so $L = q^d - 1$, and $\mathcal{C}_2 = \{0, 1\}$.

Schemes of this type enjoy (k_1, k_2)-out-of-$(L, 2)$ special soundness, wherein a witness can be computed efficiently from any $2k_1$ accepting transcripts with k_1 distinct first challenges, each one answered for both second challenges. It is well-known [2,4] that (k_1, k_2)-out-of-$(L, 2)$ special soundness protocol are proofs of knowledge with knowledge error

$$\kappa = 1 - \left(1 - \frac{k_1 - 1}{L}\right)\left(1 - \frac{k_2 - 1}{2}\right).$$

The relevant protocol in Section 4 is $(2, 2)$-special sound, meaning $\kappa = \frac{1}{2} + \frac{1}{2L}$, while the ring protocol of Section 5 is $(N + 1, 2)$-special sound, with $\kappa = \frac{1}{2} + \frac{N}{2L}$. In both cases, the soundness error κ is the probability that a cheating prover can successfully convince a verifier.

The Fiat-Shamir paradigm [24,22] exchanges the verifier's choices with a random oracle, so that $\texttt{chal}_1$ is a hash of the previous transcript, public data, and ID's, while $\texttt{chal}_2$ is the hash of the transcript before it, now including $\texttt{chal}_1$. This generally preserves soundness and zero knowledge in the random oracle model, but may sacrifice some tightness [4].

2.3 Linkable Ring Signatures

Ring signatures permit a member in a group sign a message for the entire group, yet hides their identity in that group and requires no discussion between the members [40]. Using the public keys of the other members, the signer produces a zero-knowledge proof of membership with their individual secret key. Linkable ring signatures additionally append a linking tag, so that if the same signing key is ever reused, the linking tags will match, broadcasting that the same user signed [32]. We consider the security model from [31,32,8], and let λ denote the security parameter.

Definition 3 (Linkable Ring Signature). Given public parameters pp, a ring of users R, and a message M, an LRS is a set of PPT algorithms

$$\mathsf{Setup}(1^\lambda) \to \mathsf{pp}, \quad \mathsf{KeyGen}(\mathsf{pp}) \to (s, y),$$
$$\mathsf{Sign}(s, R, M) \to \sigma, \quad \mathsf{Verify}(R, M, \sigma) \to \{0, 1\},$$

along with a linking algorithm $\mathsf{Link}(\mathsf{pp}, R, M, \sigma, R', M', \sigma') \to \{0, 1\}$, such that: for signer at index π in R, we have

1. **Correctness**: $\mathsf{Verify}(R, M, \mathsf{Sign}(s_\pi, R, M)) = 1$ whenever $y_\pi \in R$.
2. **Linking Correctness**: honest signatures link if and only if they were signed with the same private key, except with probability $\mathsf{negl}(\lambda)$.

For each game below, the adversary $\mathcal{A}$ knows pp and the public keys of n_u honest users, then is granted access to a corruption oracle returning s_i and a signing oracle returning $\mathsf{Sign}(s_i, R, M)$ for honest $i \in R$. $\mathcal{A}$ may also place keys of its own choosing into rings.

1. **Anonymity**: $\mathcal{A}$ outputs (R, M, i_0, i_1) with $i_0, i_1 \in R$ uncorrupted and unqueried, receives $\sigma \xleftarrow{\$} \mathsf{Sign}(s_{i_\beta}, R, M)$ for a hidden bit β, and guesses β with advantage $\mathsf{negl}(\lambda)$.
2. **Linkability**: $\mathcal{A}$ cannot output $k+1$ valid signatures, none from the signing oracle, that are pairwise unlinked, from a set of k public keys.
3. **Non-Slanderability**: $\mathcal{A}$ cannot output a valid signature, not given to the signing oracle, that links to the oracle signature of an uncorrupted user.
4. **Unforgeability**: $\mathcal{A}$ cannot output a valid (R, M, σ), with R a ring of uncorrupted honest keys where (R, M) was never queried.

We exclude i_0, i_1 from the signing oracle in the anonymity game because of linkability: any earlier signature of i_β includes tag $\mathcal{F}(s_{i_\beta})$, which links to the challenge. Linkability and non-slanderability imply unforgeability [31,38], and Section 6 demonstrates these security properties.

3 MQ-Based LRS Forgery Attacks

We present a novel sumset attack method which we apply to the MQ LRS's of [39] and [37], resulting in a forgery attack which succeeds regardless of challenge, despite knowing no MQ preimage.

3.1 Omar, Padhye, Dey

In [39], the authors describe a LRS based on the hardness of the MQ problem, derived from Sakumoto et al. [41]. We construct a polynomial-time forgery attack that can successfully answer every verifier challenge without knowing any member's witness. We follow their notation for this section only.

Fix a ring component and suppress its index. Following the $ch^* = 0$ branch of the simulator argument in Theorem 3.4, select arbitrary $x^*, a_0, b_0 \in K^l$ and $d_0, d_0' \in K^v$, and set

$$\begin{aligned} a_1 &= x^* - a_0, \quad b_1 = a_0 - b_0, \\ d_1 &= y_1 - F_1(x^*) + F_1(a_0) - d_0, \\ d_1' &= y_2 - F_2(x^*) + F_2(a_0) - d_0'. \end{aligned}$$

No equation of the type $F_t(x^*) = y_t$ has been imposed. Compute

$$\begin{aligned} c_0 &= \mathrm{Com}\big(a_1, G_1(b_0, a_1) + d_0, G_2(b_0, a_1) + d_0'\big), \\ c_1 &= \mathrm{Com}(b_0, d_0, d_0'), \quad c_2 = \mathrm{Com}(b_1, d_1, d_1'). \end{aligned}$$

The same commitment $\mathrm{com} = (c_0, c_1, c_2)$ admits responses

$$\mathrm{rsp}^{(1)} = (a_1, b_1, d_1, d_1'), \quad \mathrm{rsp}^{(2)} = (a_1, b_0, d_0, d_0')$$

for challenges 1 and 2, respectively. Challenge 2 verifies directly; for challenge 1, using their $F_t(0) = 0$ convention and the bilinearity of G_t, we obtain

$$\begin{aligned} y_1 - F_1(a_1) - G_1(b_1, a_1) - d_1 &= F_1(x^*) - F_1(a_0) - F_1(a_1) - G_1(b_1, a_1) + d_0 \\ &= G_1(a_0, a_1) - G_1(b_1, a_1) + d_0 \\ &= G_1(b_0, a_1) + d_0. \end{aligned}$$

The same calculation holds for $F_2, G_2, y_2, d_0', d_1'$, hence both responses verify.

Consequently, an adversary can prepare such a commitment independently for each component before receiving Ch, and every component admits the challenge set $A_i = \{1, 2\} \subseteq \mathbb{Z}_3$. Since

$$A_1 + A_2 = \{1, 2\} + \{1, 2\} = \mathbb{Z}_3,$$

by Cauchy-Davenport [14,17], every challenge can be decomposed into answerable sub-challenges. To be specific, fix $ch_i = 1$ for $i > 2$, and let $D = Ch - (w-2) \pmod 3$ for w ring members, then based on its value pick

$$(ch_1, ch_2) = \begin{cases} (1, 2), & D = 0, \\ (2, 2), & D = 1, \\ (1, 1), & D = 2. \end{cases}$$

It then holds that $\sum_{i=1}^{w} ch_i = Ch \pmod 3$, and every verification succeeds.

Consequently, for all $w \geq 2$, we find that for this witness-agnostic adversary,

$$\Pr[w\text{-VSAK accepts}] = 1.$$

In particular, three accepting transcripts with distinct challenges do not necessarily reveal all three sub-challenges at any index.

Immediately after Protocol 3 in [39] it is asserted that w-VSAK inherits the 2/3 soundness error of VSAK, but the above shows this is false, and with it the 3-special soundness claimed in their Theorem 3.1.

The non-interactive MLRS from their Section 3.3 suffers from the same flaw. Select any message M and tag $z \in K^v$, derive F_2 from $H_1(R)$, and use the ring's public keys (y_i, z). Prepare all commitments for the r repetitions, evaluate the Fiat-Shamir hash $(Ch_1, \ldots, Ch_r) = H_2(\text{Commit} \mid\mid M)$, and answer each Ch_j with the attack above.

Thus an adversary can fabricate an accepting signature with probability 1 for any number of rounds r and any tag z, without any knowledge of the secret key, a universal forgery attack.

3.2 Namdeo, Mishra, and Srivastava

The MQ LRS by Namdeo, Mishra, and Srivastava [37] shares some superficial similarities with [39], though Cauchy-Davenport no longer applies, as this protocol considers the sum of the challenges modulo 4. Nonetheless, this scheme is

vulnerable to the same structural weakness as above, allowing a keyless adversary to forge proofs at-will. For this section only, we use their notation.

To be exact, the signer computes challenges $(Ch_1, \ldots, Ch_r) = H_2(\text{Commit} \,||\, M)$, then selects sub-challenges that satisfy

$$\sum_{i=1}^{w} ch_{i,j} = Ch_j \pmod 4.$$

Fix one component and suppress its index, so that we write $F = F_1$, $G = G_1$, and $y = y_i$. The intended witness satisfies $F(x) = y$, but our construction never uses such an x. Pick arbitrary $r_0, r_1, t_0, d_0 \in K^l$ and $e_0, w_0 \in K^v$, then set

$$t_1 = r_0 - t_0, \quad d_1 = r_1 - d_0, \quad e_1 = F(r_0) - e_0, \quad w_1 = F(r_1) - w_0.$$

Construct five of the six commitments as

$$c_0 = \text{Com}\big(r_0, G(t_0, d_1) + w_1\big), \quad c_2 = \text{Com}(t_0, e_0),$$
$$c_3 = \text{Com}(t_1, e_1), \quad c_4 = \text{Com}(d_0, w_0), \quad c_5 = \text{Com}(d_1, w_1).$$

Consider now the answer sets $A = \{1, 2\}$ and $B = \{0, 2\}$, which can be seen to satisfy $A + B = \mathbb{Z}_4$. For $A = \{1, 2\}$, set $c_1 = \text{Com}\big(r_1, G(t_0, r_1) + e_0\big)$. The prover commits to these values using the vector $\text{com}^A = \big(c_0, \ldots, c_5\big)$. Note that the responses

$$\text{Rsp}_1^A = \big(r_1, t_0, e_0, d_1, w_1, c_0, c_3\big),$$
$$\text{Rsp}_2^A = \big(r_0, t_0, e_0, d_1, w_1, c_1, c_4\big)$$

are exactly the responses specified for challenges 1 and 2.

For challenge 1 the verifier recomputes c_1, c_2, c_5 directly and c_4 from $r_1 - d_1 = d_0$, $F(r_1) - w_1 = w_0$. For challenge 2 it recomputes c_0, c_2, c_5 and c_3 from $r_0 - t_0 = t_1$, $F(r_0) - e_0 = e_1$. The two remaining commitments are supplied. Thusly, com^A answers $\{1, 2\}$ with no witness x, and without even using y.

For the answer set $B = \{0, 2\}$, the setup remains the same, except we now set

$$c_1 = \text{Com}\big(r_1, y - F(r_1) - G(t_1, r_1) - e_1\big),$$

which is the only commitment in either answer set that involves y at all. The prover commits like before using $\text{com}^B = \big(c_0, \ldots, c_5\big)$, with responses

$$\text{Rsp}_0^B = \big(r_1, t_1, e_1, d_0, w_0, c_0, c_2\big),$$
$$\text{Rsp}_2^B = \big(r_0, t_0, e_0, d_1, w_1, c_1, c_4\big).$$

For challenge 0, the verifier recovers c_1, c_3, c_4 as committed; c_5 may be reconstructed keeping in mind $r_1 - d_0 = d_1$, $F(r_1) - w_0 = w_1$, with c_0, c_2 handed to them by the prover. Thus, com^B is valid for challenges 0 and 2.

To close, we need only demonstrate that an adversary can always prepare an A answer for the first ring member and a B answer for the second. This can be accomplished using the modulo-4 choices in Table 1. Each row consists of

Ch	$ch_1 \in \{1,2\}$	$ch_2 \in \{0,2\}$
0	2	2
1	1	0
2	2	0
3	1	2

Table 1. Sub-challenge pairs for the four challenge possibilities.

sub-challenges that we demonstrated can be opened by the prover, and each row satisfies $ch_1 + ch_2 \equiv Ch \pmod 4$, therefore for $w \geq 2$, we have that

$$\Pr[\text{the verifier accepts a key-agnostic prover}] = 1.$$

This is apparent as we can perform the same procedure as in Section 3.1: fix the remaining arbitrary ch_i, absorb their sum into D, then note that the table covers every outcome.

From [37], their Lemma 5.3 claims that any two accepting transcripts with distinct sub-challenges to the same commitment imply extraction of a witness, then contrasts this with the three-transcript framework of Sakumoto [41]. The above construction contradicts this statement, with the meaningful result being that soundness error of $\frac{1}{2}$ does not imply extraction from any 2 challenges of 4.

3.3 Monteiro, Goya, and Terada

Monteiro, Goya, and Terada [35] present an improvement to Sakumoto et al. [41] which embiggens the verifier's challenge space from $\mathbb{Z}_3$ to $\mathbb{Z}_4$, with a claimed reduction of the soundness error from 2/3 to 1/2. We analyze only the version reproduced in Table 5 of Namdeo et al. [37], denoted Π^{pr}, and show that it is incomplete and has tight worst-case soundness error 3/4. We then provide the natural repair $\Pi^{\star}$, and show that it is 3-special sound instead of 2.

For only this section, we write in the notation of [37]. The prover knows $x \in \mathbb{K}^{\ell}$ with $F(x) = y$, samples $r_0, t_0, d_0 \in \mathbb{K}^{l}$ and $e_0, w_0 \in \mathbb{K}^{v}$, then sets $r_1 = x - r_0$, $t_1 = r_0 - t_0$, $d_1 = r_1 - d_0$, $e_1 = F(r_0) - e_0$, and $w_1 = F(r_1) - w_0$. The six commitments used in Π^{pr} are

$$c_0 = \text{Com}\big(r_0,\ G(t_0, d_1) + w_1\big), \quad c_1 = \text{Com}\big(r_1,\ G(t_0, r_1) + e_0\big),$$
$$c_2 = \text{Com}(t_0, e_0), \quad c_3 = \text{Com}(t_1, e_1), \quad c_4 = \text{Com}(d_0, w_0), \quad c_5 = \text{Com}(d_1, w_1).$$

The verifier, after providing the challenge ch, is given the openings of [37, Table 5], so they can recompute

- $ch = 0$: opens r_1, t_1, e_1, d_0, w_0, recomputes $c_1 = \text{Com}(r_1,\ y - F(r_1) - G(t_1, r_1) - e_1)$, c_3, c_4, and $c_5 = \text{Com}(r_1 - d_0,\ F(r_1) - w_0)$.
- $ch = 1$: opens r_1, t_0, e_0, d_1, w_1, recomputes $c_1 = \text{Com}(r_1,\ G(t_0, r_1) + e_0)$, c_2, c_5, and $c_4 = \text{Com}(r_1 - d_1,\ F(r_1) - w_1)$.
- $ch = 2$: opens r_0, t_0, e_0, d_1, w_1, recomputes $c_0 = \text{Com}(r_0,\ G(t_0, d_1) + w_1)$, c_2, c_5, and $c_3 = \text{Com}(r_0 - t_0,\ F(r_0) - e_0)$.

– $ch = 3$: opens r_0, t_1, e_1, d_0, w_0, recomputes $c_0 = \mathrm{Com}(r_0,\ y - F(r_0) - G(r_0, d_0) - w_0)$, c_3, c_4, and $c_2 = \mathrm{Com}(r_0 - t_1,\ F(r_0) - e_1)$,

where the two remaining commitments are communicated directly by the prover. Table 5 of [37] actually prints $t_1 = t_0 - d_0$ in the commitment phase, but based on the later reconstruction, we believe this to be in error.

Our goal is to attack the protocol's soundness, but first we must address a roadbump: the protocol as stated does not satisfy completeness, but we believe this to be a typo. First we show how to patch this scheme, and only then do we move to soundness.

Proposition 1. *Π^{pr} does not achieve the claimed completeness; namely an honest prover is rejected at challenge 3 unless $G(t_1, d_1) = 0$.*

Proof. For $ch = 3$, the verifier recomputes c_0 from $y - F(r_0) - G(r_0, d_0) - w_0$. Considering $y = F(r_0 + r_1) = F(r_0) + F(r_1) + G(r_0, r_1)$ and bilinearity, we see

$$y - F(r_0) - G(r_0, d_0) - w_0 = G(r_0, r_1 - d_0) + F(r_1) - w_0 = G(r_0, d_1) + w_1.$$

The honest c_0 commits to $G(t_0, d_1) + w_1$, so by binding, the check only passes if $G(r_0, d_1) = G(t_0, d_1)$; that is, if $G(r_0 - t_0, d_1) = G(t_1, d_1) = 0$.

The most obvious patch to the protocol is to replace c_0 with

$$c_0^\star = \mathrm{Com}\big(r_0,\ G(r_0, d_1) + w_1\big),$$

with the $ch = 2$ recomputation changed accordingly.

We write $\Pi^\star$ for the repaired protocol, which is now complete: the $ch = 3$ identity is the displayed in the proof of Proposition 1, the $ch = 0$ identity is Sakumoto's $y - F(r_1) - G(t_1, r_1) - e_1 = G(t_0, r_1) + e_0$, and the four consistency recomputations are the defining relations of t_1, e_1, d_1, w_1. We treat $\Pi^\star$ as a proposed repair of NMS's transcription, but cannot establish that it coincides with the original [35].

The situation is more dire even than this completeness analysis suggests: it is possible to generate false proofs for untrue statements, meaning the proving mechanism underlying Π^{pr} is not well-formed. Consider taking the specific $F : \mathbb{K}^2 \to \mathbb{K}^3$, in the notation of [37], given by $F(u_1, u_2) = (u_1^2, u_2^2, u_1 u_2)$, $y = (0, 0, 1)$. There exists no solution x to $F(x) = y$ over any field, by inspection. Nonetheless, for $a = (1, 0)$ and $b = (0, 1)$ we have

$$G(a, b) = F(a + b) - F(a) - F(b) = (0, 0, 1) = y,$$

thus the commitment above is accepting for any challenge in $\{0, 2, 3\}$, despite the fact that there exists no witness for this statement.

We now bring our attention to soundness. Let $F = F_1$, $G = G_1$, and assume $F(0) = 0$ with $G(u, v) = F(u + v) - F(u) - F(v)$. Suppose that one obtains $a, b \in \mathbb{K}^l$ such that $G(a, b) = y$ – note that this need not correspond to a witness

$F(x) = y$. We show that such vectors can be recovered by elementary linear algebra. Select

$$r_0 = r_1 = e_0 = e_1 = w_0 = w_1 = 0,$$
$$t_0 = a, \quad t_1 = -a, \quad d_0 = -b, \quad d_1 = b,$$

Before the challenge, where we suppress any random salt, set

$$c_0 = \mathrm{Com}(0, y), \qquad c_1 = \mathrm{Com}(0, y), \quad c_2 = \mathrm{Com}(a, 0)$$
$$c_3 = \mathrm{Com}(-a, 0), \quad c_4 = \mathrm{Com}(-b, 0), \quad c_5 = \mathrm{Com}(b, 0).$$

This permits responses

$$\mathrm{Rsp}_0 = \big(0, -a, 0, -b, 0, c_0, c_2\big),$$
$$\mathrm{Rsp}_2 = \big(0, a, 0, b, 0, c_1, c_4\big),$$
$$\mathrm{Rsp}_3 = \big(0, -a, 0, -b, 0, c_1, c_5\big).$$

Challenge 0*:* Using $y - F(r_1) - G(t_1, r_1) - e_1 = y - F(0) - G(-a, 0) = y$, the verifier reconstructs c_1, with c_5 following from $r_1 - d_0 = 0 - (-b) = b$, $F(r_1) - w_0 = 0$. They also can directly open c_3 and c_4, thus the 0 challenge is accepting.

Challenge 2*:* The verifier can reform c_0 by $G(t_0, d_1) + w_1 = G(a, b) = y$, and c_3 with $r_0 - t_0 = -a$, $F(r_0) - e_0 = 0$. Additionally, c_2 and c_5 agree with what the prover sent.

Challenge 3*:* Finally, for the challenge 3, the verifier can confirm c_0, since $y - F(r_0) - G(r_0, d_0) - w_0 = y - F(0) - G(0, -b) = y$. Seeing how $r_0 - t_1 = 0 - (-a) = a$, $F(r_0) - e_1 = 0$, c_2 matches. The verifier can directly open c_3 and c_4, thus the challenge 3 accepts as well.

For $y \neq 0$, the supplied challenge-1 response reconstructs $\mathrm{Com}(0, 0)$ rather than $\mathrm{Com}(0, y)$, so only admits answer set $\{0, 2, 3\}$ unless binding is violated. The consequence of this analysis is that

$$\Pr[\text{the verifier accepts a witness-less prover}] = \frac{3}{4}.$$

For the upper bound, consider accepting transcripts for $\{0, 1, 2\}$ under the same initial commitment – binding gives $t_0 + t_1 = r_0$ and $e_0 + e_1 = F(r_0)$. Comparing the challenge-0 and challenge-1 openings of c_1 gives

$$y = F(r_1) + G(t_0 + t_1, r_1) + e_0 + e_1 = F(r_0 + r_1).$$

Consequently, all four accepting challenges for a false statement would give a binding violation, so at most three challenges can accept, matching the claimed 3/4 lower bound. After the stated $r = 128$ parallel repetitions, the soundness error is $\left(\frac{3}{4}\right)^{128} \approx 2^{-53}$, far above the required 2^{-128} threshold which requires r to be at least 309.

Now, to show that finding valid a, b need not solve the MQ problem, fix b and consider the linear map $G(a, b) : \mathbb{K}^l \to \mathbb{K}^v$. Form the matrix $H = [G(e_1, b) \cdots G(e_l, b)]$, where the e_j are the standard basis vectors. Once $\text{rank}(H) = v$, the adversary can solve $Ha = y$ by Gaussian elimination, with no $F(x) = y$ solution required. At the paper's claimed parameters, with $(q, l, v) = (64, 72, 36)$, we have that the H matrix is overwhelmingly full-rank, so can be solved efficiently.

The claimed 3/4 bound is for Π^{pr} as printed, whose $ch = 2$ recomputation $G(t_0, d_1) + w_1$ can be exploited using $c_0 = \text{Com}(0, y)$. For the repaired $\Pi^\star$, the analysis is slightly different: every pair of challenges is answerable without a witness. For the pairs $\{0, 1\}$ and $\{2, 3\}$, one core commitment remains unopened, and the equation linking them

$$y = F(r_1) + G(t_0 + t_1, r_1) + e_0 + e_1 \text{ for } \{0, 1\}, \text{ or}$$
$$y = F(r_0) + G(r_0, d_0 + d_1) + w_0 + w_1 \text{ for } \{2, 3\},$$

can be solved for e_1 or w_1. Any three challenges, however, force $t_0 + t_1 = r_0$, $e_0 + e_1 = F(r_0)$, $d_0 + d_1 = r_1$, and $w_0 + w_1 = F(r_1)$ through the recomputed $c_2, \ldots, c_5$, so substituting these into the linking equation yields $y = F(r_0 + r_1)$. The consequence is that $\Pi^\star$ achieves the soundness error 1/2 that [35] claims, but is 3-special sound in lieu of 2-special sound. The attack of Section 3.2 works with c_0 replaced by $c_0^\star$, since $\{1, 2\}$ and $\{0, 2\}$ remain witness-free, thus Lemma 5.3 of [37] is false for both versions.

4 A 5-Pass MQ ZKP

For any given public constant-free quadratic map $A : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$, let $T \in \mathbb{F}_q^m$ be some element of the output space. A witness is $x \in \mathbb{F}_q^n$ with $A(x) = T$.

Fix the dimension of the challenge space as $d \geq 1$ and define the first-challenge set to be $\mathbb{F}_q^d \setminus \{\mathbf{0}\}$. Set $L = q^d - 1$, its cardinality. Then Figure 1 is a 5-pass MQ-based zero-knowledge proof, and an $(L, 2)$-identification scheme.

5 An MQ LRS

Let $N \leq q^d - 1$ be the number of ring members.

We present our interactive MQ linkable ring signature framework in Figure 2. Within each loop, the index i on masks, randomizers, and intermediate values are suppressed. Each $r_0, r_1, \rho_0, \rho_1, \rho_2, \varsigma_0, \varsigma_1$ should be thought of as independent values, which may differ in distinct loops.

The index i is suppressed for masks, commitments, and randomizers for brevity; on each fixed index i however, values are reused across all subsequent loops unless explicitly stated otherwise. All randomness sampling must be done independently and uniform at random.

5-Pass MQ Framework		
Public: $A : \mathbb{F}_q^n \to \mathbb{F}_q^m$ s.t. $A(0) = 0$, tag T, hash $\mathsf{com}(\cdot)$		
Prover: $x \in \mathbb{F}_q^n$ with $A(x) = T$		
PROVER		**VERIFIER**
Pick $r_0 \xleftarrow{\$} \mathbb{F}_q^n$, set $r_1 = x - r_0$		
For $\ell \in [d]$: $t_{0,\ell} \xleftarrow{\$} \mathbb{F}_q^n$, $E_{0,\ell} \xleftarrow{\$} \mathbb{F}_q^m$		
$V_\ell = G_A(t_{0,\ell}, r_1) + E_{0,\ell}$		
Sample $\rho_0, \rho_1 \xleftarrow{\$} \{0,1\}^{2\lambda}$		
$c_0 = \mathsf{com}(r_0, \{t_{0,\ell}, E_{0,\ell}\}_{\ell=1}^d;\ \rho_0)$		
$c_1 = \mathsf{com}(r_1, \{V_\ell\}_{\ell=1}^d;\ \rho_1)$	$\xrightarrow{c_0,\, c_1}$	
	$\xleftarrow{\boldsymbol{a}}$	$\boldsymbol{a} = (a_1, \ldots, a_d) \xleftarrow{\$} \mathbb{F}_q^d \setminus \{\mathbf{0}\}$
For $\ell \in [d]$: $t_{1,\ell} = a_\ell r_0 - t_{0,\ell}$		
$E_{1,\ell} = a_\ell A(r_0) - E_{0,\ell}$		
Sample $\rho_2 \xleftarrow{\$} \{0,1\}^{2\lambda}$		
$c_2 = \mathsf{com}(\{t_{1,\ell}, E_{1,\ell}\}_{\ell=1}^d;\ \rho_2)$	$\xrightarrow{c_2}$	
	$\xleftarrow{b}$	$b \xleftarrow{\$} \{0,1\}$
Set $\mathsf{rsp}_b = (r_b, \{t_{b,\ell}, E_{b,\ell}\}_{\ell=1}^d, \rho_b, \rho_2)$		
	$\xrightarrow{\mathsf{rsp}_b}$	
		If $b = 0$:
		$c_0 \overset{?}{=} \mathsf{com}(r_0, \{t_{0,\ell}, E_{0,\ell}\}_{\ell=1}^d;\ \rho_0)$
		For $\ell \in [d]$: $\widehat{t}_{1,\ell} = a_\ell r_0 - t_{0,\ell}$
		$\widehat{E}_{1,\ell} = a_\ell A(r_0) - E_{0,\ell}$
		$c_2 \overset{?}{=} \mathsf{com}(\{\widehat{t}_{1,\ell}, \widehat{E}_{1,\ell}\}_{\ell=1}^d;\ \rho_2)$
		If $b = 1$:
		$c_2 \overset{?}{=} \mathsf{com}(\{t_{1,\ell}, E_{1,\ell}\}_{\ell=1}^d;\ \rho_2)$
		For $\ell \in [d]$: $\widehat{V}_\ell = a_\ell T - a_\ell A(r_1)$
		$-G_A(t_{1,\ell}, r_1) - E_{1,\ell}$
		$c_1 \overset{?}{=} \mathsf{com}(r_1, \{\widehat{V}_\ell\}_{\ell=1}^d;\ \rho_1)$
		Accept iff every check passes.

Fig. 1. One round of our MQ-based 5-pass zero-knowledge proof.

Choice of quadratic maps: We now describe the setup procedure, which for our LRS needs some slight modifications to ensure properties like linkability are practically feasible. At initialization, sample $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^{m_\mathcal{P}}$ and $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^{m_\mathcal{F}}$ independently from the constant-free MQ family. Namely, for each $A \in \{\mathcal{P}, \mathcal{F}\}$, let

$$A(x) = \sum_{1 \le u \le v \le n} \alpha_{uv}^{(A)} x_u x_v + \sum_{1 \le u \le n} \beta_u^{(A)} x_u, \text{ where } \alpha_{uv}^{(A)}, \beta_u^{(A)} \xleftarrow{\$} \mathbb{F}_q^{m_A}$$

with independent coefficient vectors. Equivalently, sample full MQ quadratic polynomials and subtract away their constant terms. These maps are public, sampled before any user interaction, and remain fixed. Honest users sample s_i uniformly, then can compute their public keys as $y_i = \mathcal{P}(s_i)$ and $T_i = \mathcal{F}(s_i)$.

Collision resistance and linkability: Linkability against malicious keys requires that nobody can find $s \neq s'$ with $\mathcal{P}(s) = \mathcal{P}(s')$ (collision resistance), but in the honest-key variant of Section 6 also second-preimage resistant. Injectivity of $\mathcal{P}$ would give this statistically, but only for $m_\mathcal{P} \geq 2n + \lambda/\log_2 q$, and requiring the same of $\mathcal{F}$ would give an attacker $4n + O(\lambda/\log_2 q)$ equations in n unknowns, a much easier problem than the standard square instances. Hence, we settle for computational, then bound the known attacks.

Fixed differences: For nonzero $\delta \in \mathbb{F}_q^n$, $\mathcal{P}(s+\delta) - \mathcal{P}(s) = \mathcal{P}(\delta) + G_\mathcal{P}(s, \delta)$ is affine, so $\mathcal{P}(s+\delta) = \mathcal{P}(s)$ when

$$G_\mathcal{P}(s, \delta) = -\mathcal{P}(\delta), \tag{3}$$

a system of $m_\mathcal{P}$ linear equations in the n unknowns s, the mechanism of Billet, Robshaw, and Peyrin [11]. Every collision $(s, s+\delta)$ solves (3) for its own δ, so the question is when the system is consistent. The matrix $G_\mathcal{P}(\cdot, \delta)$ depends only on the quadratic coefficients $\alpha^{(\mathcal{P})}$, whereas $\mathcal{P}(\delta)$ contains the term $\sum_u \beta_u^{(\mathcal{P})} \delta_u$ with $\beta^{(\mathcal{P})}$ uniform, hence for fixed δ the right-hand side is uniform in $\mathbb{F}_q^{m_\mathcal{P}}$ and independent of the matrix. For $m_\mathcal{P} > n$, the matrix has rank n except with probability $O(q^{n-m_\mathcal{P}})$, and a uniform vector lies in a fixed n-dimensional subspace of $\mathbb{F}_q^{m_\mathcal{P}}$ with probability $q^{n-m_\mathcal{P}}$. Then (3) is consistent for a $q^{n-m_\mathcal{P}}$ -fraction of the differences, hence an attacker who samples δ and performs Gaussian elimination needs $q^{m_\mathcal{P}-n}$ trials [11]. Consistency is conditional on δ alone, that $\mathcal{P}(\delta)$ lie in the column space of $G_\mathcal{P}(\cdot, \delta)$, which is the vanishing of $m_\mathcal{P} - n$ minors of degree about n in δ. We are aware of no method which computes δ faster than guessing, so we make this an explicit assumption in Section 6 (Assumption 3).

Considering (s, δ) jointly instead gives the underdetermined MQ system $\mathcal{P}(x) = \mathcal{P}(x')$ with $2n$ unknowns and $m_\mathcal{P}$ equations. The Thomae-Wolf reduction [42] maps an underdetermined system with $2n$ unknowns and $m_\mathcal{P}$ equations into a square instance of size about $m_\mathcal{P} - 1$, which for our parameters is harder than $q^{m_\mathcal{P}-n}$. Birthday search costs $q^{m_\mathcal{P}/2}$. We therefore take

$$m_\mathcal{P} = n + c, \quad c \geq \lceil \lambda/\log_2 q \rceil,$$

which gives $c = 19$ at $q = 128$. Our security estimates for the MQ instance in Section 8 are classical, following the convention of MQOM and MQDSS. Luckily, annealing against Grover costs only 18 further equations, so we take $c \geq \lceil 2\lambda / \log_2 q \rceil$ as a cheap hedge; a *provably* quantum-secure MQ instance would require arguments outside our scope.

Second preimages: For the honest-key variant, the attacker is given s and attempts to find $\delta \neq 0$ satisfying $\mathcal{P}(\delta) + G_{\mathcal{P}}(s, \delta) = 0$, an MQ system of $m_{\mathcal{P}}$ equations in n unknowns. An additional solution exists with probability about $q^{n-m_{\mathcal{P}}}$, and finding it is no easier than inverting $\mathcal{P}$.

The tag: The map $\mathcal{F}$ in fact need not be injective. It must be one-way: a framer who solves $\mathcal{F}(s') = T_*$ uses $y' = \mathcal{P}(s')$ to sign, which is the attack Assumption 4 excludes, so $m_{\mathcal{F}} \approx n$ gives standard MQ hardness to that instance. Two honest secrets $s \neq s'$ collide under $\mathcal{F}$ with probability $q^{-m_{\mathcal{F}}}$, since $\mathcal{F}(s) - \mathcal{F}(s')$ contains uniform $\beta^{(\mathcal{F})} \cdot (s - s')$, so among N users all tags are distinct except with probability $N^2 q^{-m_{\mathcal{F}}}$. Hence honest signers with different keys never link, and a witness for one key produces another key's tag only through a collision of $\mathcal{P}$. Linkability is only a meaningful notion within rings using the same maps, which reflects the case of real-world cryptocurrencies, where hash functions and elliptic curve generators must remain fixed.

Random MQ Maps: The stacked map $Q = (\mathcal{P}, \mathcal{F})$ is itself a random MQ map with m_Q outputs, and $\mathcal{P}$ is one with $m_{\mathcal{P}}$ outputs. Assume both are one-way on planted inputs, that is, on $(Q, Q(s))$ and $(\mathcal{P}, \mathcal{P}(s))$ for uniform s. Both are implied by Assumption 2 below. The reduction of Liu, Lu, and Yang [30, Propositions 2 and 5] turns one-wayness into image pseudorandomness, so when applied to Q,

$$(\mathcal{P}, \mathcal{F}, \mathcal{P}(s), \mathcal{F}(s)) \approx_c (\mathcal{P}, \mathcal{F}, U_{m_{\mathcal{P}}}, U_{m_{\mathcal{F}}}), \tag{4}$$

and applied to $\mathcal{P}$ alone, with the independent $\mathcal{F}$ and an independent $U_{m_{\mathcal{F}}}$ appended to both sides, we get

$$(\mathcal{P}, \mathcal{F}, \mathcal{P}(s), U_{m_{\mathcal{F}}}) \approx_c (\mathcal{P}, \mathcal{F}, U_{m_{\mathcal{P}}}, U_{m_{\mathcal{F}}}). \tag{5}$$

The right-hand sides of (4) and (5) coincide, so by transitivity

$$(\mathcal{P}, \mathcal{F}, \mathcal{P}(s), \mathcal{F}(s)) \approx_c (\mathcal{P}, \mathcal{F}, \mathcal{P}(s), U_{m_{\mathcal{F}}}).$$

Thus the tag is computationally hidden even given its membership image. Together with ROM simulation, this is the tag-hiding statement the anonymity proof invokes.

6 Security Proofs

Let λ be the security parameter and $d \in \mathbb{N}$ the dimension.

Multivariate Linkable Ring Signature

Public: $n, m_{\mathcal{P}}, m_{\mathcal{F}}, d \in \mathbb{N}$, $Q = (\mathcal{P}, \mathcal{F})$, ring $R = (y_1, \ldots, y_N)$, tag T, hash $\mathsf{com}(\cdot)$
Prover: (π, s_π) with $Q(s_\pi) = Y_\pi$

PROVER		**VERIFIER**
For $i \neq \pi$: $b_i \xleftarrow{\$} \{0,1\}$		
For $i \in [N]$: $\rho_0, \rho_1, \varsigma_0, \varsigma_1 \xleftarrow{\$} \{0,1\}^{2\lambda}$		
If $i = \pi$ or $b_i = 0$: $r_0 \xleftarrow{\$} \mathbb{F}_q^n$		
For $\ell \in [d]$: $t_{0,\ell} \xleftarrow{\$} \mathbb{F}_q^n$, $E_{0,\ell} \xleftarrow{\$} \mathbb{F}_q^{m_Q}$		
$c_{0,i} = \mathsf{com}(r_0, \{t_{0,\ell}, E_{0,\ell}\}_{\ell=1}^d;\ \rho_0)$		
If $i = \pi$: $r_1 = s_\pi - r_0$		
For $\ell \in [d]$: $V_\ell = G_Q(t_{0,\ell}, r_1) + E_{0,\ell}$		
$c_{1,i} = \mathsf{com}(r_1, \{V_\ell\}_{\ell=1}^d;\ \rho_1)$		
If $i \neq \pi$, $b_i = 0$: $c_{1,i} = \mathsf{com}(\varsigma_1;\ \rho_1)$		
If $i \neq \pi$, $b_i = 1$: $c_{0,i} = \mathsf{com}(\varsigma_0;\ \rho_0)$		
$r_1 \xleftarrow{\$} \mathbb{F}_q^n$, $\{V_\ell\}_{\ell=1}^d \xleftarrow{\$} (\mathbb{F}_q^{m_Q})^d$		
$c_{1,i} = \mathsf{com}(r_1, \{V_\ell\}_{\ell=1}^d;\ \rho_1)$		
$C_0 = (c_{0,i})_i$, $C_1 = (c_{1,i})_i$	$\xrightarrow{C_0, C_1}$	
	$\xleftarrow{\boldsymbol{a}}$	$\boldsymbol{a} = (a_1, \ldots, a_d) \xleftarrow{\$} \mathbb{F}_q^d \setminus \{\mathbf{0}\}$
For $i \in [N]$ and $\ell \in [d]$:		
If $i = \pi$ or $b_i = 0$: $t_{1,\ell} = a_\ell r_0 - t_{0,\ell}$		
$E_{1,\ell} = a_\ell Q(r_0) - E_{0,\ell}$		
If $i \neq \pi$, $b_i = 1$: $t_{1,\ell} \xleftarrow{\$} \mathbb{F}_q^n$		
$E_{1,\ell} = a_\ell Y_i - a_\ell Q(r_1)$ $-G_Q(t_{1,\ell}, r_1) - V_\ell$		
For $i \in [N]$: $\rho_2 \xleftarrow{\$} \{0,1\}^{2\lambda}$		
$c_{2,i} = \mathsf{com}(\{t_{1,\ell}, E_{1,\ell}\}_{\ell=1}^d;\ \rho_2)$		
$C_2 = (c_{2,i})_i$	$\xrightarrow{C_2}$	
	$\xleftarrow{b}$	$b \xleftarrow{\$} \{0,1\}$
Set $b_\pi = b \oplus \bigoplus_{i \neq \pi} b_i$,		
For $i \in [N]$:		
$R_i = (r_{b_i}, \{t_{b_i,\ell}, E_{b_i,\ell}\}_{\ell=1}^d, \rho_{b_i}, \rho_2)$		
	$\xrightarrow{(b_i, R_i)\ \forall i}$	
		$b \overset{?}{=} \bigoplus_{i=1}^N b_i$
		For $i \in [N]$:
		If $b_i = 0$:
		$c_{0,i} \overset{?}{=} \mathsf{com}(r_0, \{t_{0,\ell}, E_{0,\ell}\}_{\ell=1}^d;\ \rho_0)$
		For $\ell \in [d]$: $\widehat{t}_{1,\ell} = a_\ell r_0 - t_{0,\ell}$
		$\widehat{E}_{1,\ell} = a_\ell Q(r_0) - E_{0,\ell}$
		$c_{2,i} \overset{?}{=} \mathsf{com}(\{\widehat{t}_{1,\ell}, \widehat{E}_{1,\ell}\}_{\ell=1}^d;\ \rho_2)$
		If $b_i = 1$:
		For $\ell \in [d]$: $\widehat{V}_\ell = a_\ell Y_i - a_\ell Q(r_1)$ $-G_Q(t_{1,\ell}, r_1) - E_{1,\ell}$
		$c_{1,i} \overset{?}{=} \mathsf{com}(r_1, \{\widehat{V}_\ell\}_{\ell=1}^d;\ \rho_1)$
		$c_{2,i} \overset{?}{=} \mathsf{com}(\{t_{1,\ell}, E_{1,\ell}\}_{\ell=1}^d;\ \rho_2)$
		Accept iff every check passes

Fig. 2. One round of our MQ LRS.

Completeness:

Theorem 1 (Perfect Completeness). *An honest execution of Figure 1 accepts for every $\boldsymbol{a} \in \mathbb{F}_q^d \setminus \{\mathbf{0}\}$ and every $b \in \{0,1\}$.*

Proof. The $b = 0$ challenge checks the values used to generate the commitments, so this passes upon an honest execution. In the $b = 1$ branch, for each ℓ,

$$\begin{aligned}\widehat{V}_\ell &= a_\ell A(r_0 + r_1) - a_\ell A(r_1) - G_A(a_\ell r_0 - t_{0,\ell}, r_1) - a_\ell A(r_0) + E_{0,\ell} \\ &= a_\ell G_A(r_0, r_1) - a_\ell G_A(r_0, r_1) + G_A(t_{0,\ell}, r_1) + E_{0,\ell} \\ &= V_\ell.\end{aligned}$$

Both commitment therefore verify, hence completeness.

Soundness:

Lemma 1. *Suppose both b challenges have accepting responses for the same initial transcript $(c_0, c_1, \boldsymbol{a}, c_2)$. Unless a hash collision is obtained, there exist common inputs $r_0, r_1, t_{0,\ell}, E_{0,\ell}, V_\ell$ satisfying, for all $\ell \in [d]$,*

$$a_\ell(T - A(r_0 + r_1)) = V_\ell - G_A(t_{0,\ell}, r_1) - E_{0,\ell}. \tag{6}$$

Proof. For the $b = 0$ challenge, the prover supplies an opening of c_0, which certifies the validity of

$$\begin{aligned}t_{1,\ell} &= a_\ell r_0 - t_{0,\ell}, \\ E_{1,\ell} &= a_\ell A(r_0) - E_{0,\ell}.\end{aligned}$$

The $b = 1$ response provides an opening of c_1, which authenticates

$$V_\ell = a_\ell T - a_\ell A(r_1) - G_A(t_{1,\ell}, r_1) - E_{1,\ell}.$$

The two openings of c_2 must have the same input, or violate binding, hence substitute the above values into

$$V_\ell = a_\ell T - a_\ell A(r_1) - G_A(a_\ell r_0 - t_{0,\ell}, r_1) - (a_\ell A(r_0) - E_{0,\ell})$$

for each $\ell \in [d]$, which after applying the polar identity provides the lemma.

Theorem 2. *Given two distinct vectors $\boldsymbol{a}, \boldsymbol{a}' \in \mathbb{F}_q^d \setminus \{\mathbf{0}\}$ which share initial commitments (c_0, c_1) and accepting responses for both b challenges for each vector, one can efficiently output either a hash collision or a witness x such that $A(x) = T$.*

Proof. Compare openings of c_0, c_1 across both pairs: either the inputs are the same, or one obtains a collision otherwise. The corresponding c_2 commitments for $\boldsymbol{a}$ and $\boldsymbol{a}'$ do not need to be equal, just accepting. Applying Lemma 1 independently to the two pairs gives for all $\ell \in [d]$

$$a_\ell \Delta = a'_\ell \Delta,$$

where $\Delta = T - A(r_0 + r_1)$. Some index in $a_\ell - a'_\ell$ is nonzero, and by distinctness, it is invertible, so subtraction necessitates $\Delta = 0$. With this, one can extract $x = r_0 + r_1$.

Corollary 1. *One straightforward corollary of the above Theorem 2 is that once the initial commitments (c_0, c_1) have been sent, for an adversary attempting to prove without a witness, there is at most a unique challenge $\boldsymbol{a} \in \mathbb{F}_q^d \setminus \{\mathbf{0}\}$ in which the adversary can pass both b branches.*

Theorem 3. *Set $L = q^d - 1$. For a ring with N members, Figure 2 achieves a knowledge error of*

$$\varepsilon_{N,d} = \frac{1}{2} + \frac{\min\{N, L\}}{2L}. \tag{7}$$

Moreover, this bound is tight.

Proof. By Corollary 1, at most one $\boldsymbol{a}$ challenge permits an adversarial prover to pass both b challenges. Apply this to each index, a total of $\min\{N, L\}$ times – outside of this exceptional event, each index can be answered only for a single b challenge, which the prover must guess in advance and cannot change after sending c_2. Averaging yields the equation.

Formally, Theorem 2, together with a pigeonhole argument, turns Figure 2 an $(N+1, 2)$-special-sound 5-pass protocol. Since the knowledge error of a (k_1, k_2)-special-sound protocol with challenge spaces of sizes L and 2 respectively is $1 - (1 - \frac{k_1 - 1}{L})(1 - \frac{k_2 - 1}{2}) = \frac{1}{2} + \frac{N}{2L}$ [4,2] (i.e.: it is an $(L, 2)$-identification scheme [15]), we recover the formula stated.

For tightness, select N distinct guesses $\boldsymbol{\alpha}$. Define $S = \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_N\}$, so that $|S| = \min\{N, L\}$. Prepare each response with the expectation of receiving the $b = 0$ challenge, which can be answered correctly without fail. In the event they guessed the second challenge incorrectly and the verifier sends $b = 1$, they succeed only if $\boldsymbol{a} \in S$, so the total probability of success is $\frac{L + |S|}{2L}$, which simplifies to what was given.

A consequence of Theorem 2 is that an accepting transcript with $N + 1$ distinct $\boldsymbol{a}$ first challenges and both second b challenge responses for each vector permits efficient extraction of a witness $(s, \pi) \in \mathcal{R}_{R,T}$, or else a hash collision: for a fixed $\boldsymbol{a}$, the two b challenge bits have different parity, so some index i opens both branches, and $N + 1$ vectors over N indices cause two distinct vectors to overlap on one index. A second repercussion is that N cannot grow without bound for fixed d; for now, we assume that N is small compared to L.

Honest Verifier Zero-Knowledge:

Theorem 4. *Figure 2 achieves computational honest-verifier zero knowledge. When $\mathsf{com}(\cdot)$ is a random oracle, this gets upgraded to statistical.*

Proof. Given only the public values, the simulator algorithm $\mathcal{S}$ selects the challenges it expects, $\boldsymbol{a} \xleftarrow{\$} \mathbb{F}_q^d \setminus \{\mathbf{0}\}$, $b \xleftarrow{\$} \{0, 1\}$, then samples uniform $(b_1, \ldots, b_N) \in \{0, 1\}^N$ such that $\bigoplus_i b_i = b$.

For $b_i = 0$, it samples $r_0, t_{0,\ell} \xleftarrow{\$} \mathbb{F}_q^n$ and $E_{0,\ell} \xleftarrow{\$} \mathbb{F}_q^{m_Q}$, then sets

$$c_{0,i} = \mathsf{com}(r_0, \{t_{0,\ell}, E_{0,\ell}\}_{\ell=1}^d;\ \rho_0), \quad c_{1,i} = \mathsf{com}(\varsigma_1;\ \rho_1),$$
$$t_{1,\ell} = a_\ell r_0 - t_{0,\ell}, \quad E_{1,\ell} = a_\ell Q(r_0) - E_{0,\ell},$$

where $\varsigma_1 \in \{0,1\}^{2\lambda}$ is a random string.

For $b_i = 1$, it picks $r_1, t_{1,\ell} \xleftarrow{\$} \mathbb{F}_q^n$ and $V_\ell \xleftarrow{\$} \mathbb{F}_q^{m_Q}$, then defines

$$c_{0,i} = \mathsf{com}(\varsigma_0; \rho_0), \quad c_{1,i} = \mathsf{com}(r_1, \{V_\ell\}_{\ell=1}^d;\ \rho_1),$$
$$E_{1,\ell} = a_\ell Y_i - a_\ell Q(r_1) - G_Q(t_{1,\ell}, r_1) - V_\ell,$$

where $\varsigma_0 \in \{0,1\}^{2\lambda}$ is as before.

In either case, it can compute

$$c_{2,i} = \mathsf{com}(\{t_{1,\ell}, E_{1,\ell}\}_{\ell=1}^d;\ \rho_2), \quad R_i = (r_{b_i}, \{t_{b_i,\ell}, E_{b_i,\ell}\}_{\ell=1}^d, \rho_{b_i}, \rho_2).$$

Upon publishing the transcript $(C_0, C_1, \boldsymbol{a}, C_2, b, \{b_i, R_i\}_{i=1}^N)$, each verification check holds by construction.

It remains to compare distributions. In a genuine execution, conditioned on b, the individual challenges appear uniform, independent of the signer index. The opened values have identical distributions: for $b_i = 0$, both open to uniform $(r_0, t_{0,\ell}, E_{0,\ell})$, while for $b_i = 1$, both open to $(r_1, t_{1,\ell}, E_{1,\ell})$ with V_ℓ uniform. In the honest interaction, $V_\ell = G_Q(t_{0,\ell}, r_1) + E_{0,\ell}$ is masked by $E_{0,\ell}$, which is never revealed. The only difference lies in the unopened commitment at each index: the signer's is $\mathsf{com}(r_1, \{V_\ell\};\ \rho_1)$ or $\mathsf{com}(r_0, \{t_{0,\ell}, E_{0,\ell}\};\ \rho_0)$, while the simulator's is $\mathsf{com}(\varsigma;\ \rho)$. Each uses a new random $\rho \in \{0,1\}^{2\lambda}$ that is never revealed, so with a random-oracle commitment the two are identically distributed unless the distinguisher guesses ρ, a negligible outcome. Hence, the simulated and genuine interactions are computationally indistinguishable, despite $\mathcal{S}$ not knowing any witness (π, s_π).

7 Formalizing PyuQuMuQu-LRS

We adopt the security model of [31], in the form given by [32,8], so in this section we show anonymity, unforgeability, linkability, and non-slanderability. Linkability and non-slanderability together imply existential unforgeability [31,38]; we nonetheless prove it directly, since its reduction to Assumption 2 is the format the other two proofs follow.

Define the context as $\mathsf{ctx} = \mathsf{com}(\texttt{PyuQuMuQu-v1}, \mathsf{IDs}, \mathsf{params}, R, T, M, \mathsf{salt})$ for message M. We use domain separation tags $\texttt{com0}, \texttt{com1}, \texttt{com2}, \texttt{init}, \texttt{FS1}, \texttt{FS2}$ to keep hash functions distinct. The Fiat-Shamir challenge functions are

$$\begin{aligned}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_\tau) &= \mathsf{FS}_1(h, \mathsf{ctx}) \in \left(\mathbb{F}_q^d \setminus \{\mathbf{0}\}\right)^\tau, \\ (b_1, \ldots, b_\tau) &= \mathsf{FS}_2(h, \mathsf{ctx}, \{\boldsymbol{a}_j\}_{j=1}^\tau, C_2) \in \{0,1\}^\tau.\end{aligned} \tag{8}$$

We assume the ideal model, in which they have independent uniform outputs. The transmitted local bits (the sub-challenges) are denoted $b_{i,j}$, to distinguish them from the global bits (the challenges) b_j.

Figure 3 showcases our non-interactive MQ-based linkable ring signature generation procedure, with Figure 4 the corresponding verification process.

PyuQuMuQu Linkable Ring Signature Generation

Public: $q, n, m_{\mathcal{P}}, m_{\mathcal{F}}, d, \tau, \lambda \in \mathbb{N}$, $Q = (\mathcal{P}, \mathcal{F})$, ring $R = (y_1, \ldots, y_N)$, message M
Private: (π, s_π) with $\mathcal{P}(s_\pi) = y_\pi$

Set $T = \mathcal{F}(s_\pi)$ and $Y_i = (y_i, T)$ for $i \in [N]$
Sample $\mathsf{salt} \xleftarrow{\$} \{0,1\}^\lambda$ and form ctx
For $j \in [\tau]$: for $i \neq \pi$, sample $b_{i,j} \xleftarrow{\$} \{0,1\}$
For $j \in [\tau]$ and $i \in [N]$:
  Sample $\rho_0, \rho_1, \varsigma_0, \varsigma_1 \xleftarrow{\$} \{0,1\}^{2\lambda}$
  If $i = \pi$ or ($i \neq \pi$ and $b_{i,j} = 0$): $r_0 \xleftarrow{\$} \mathbb{F}_q^n$
    For $\ell \in [d]$: sample $t_{0,\ell} \xleftarrow{\$} \mathbb{F}_q^n$, $E_{0,\ell} \xleftarrow{\$} \mathbb{F}_q^{m_Q}$
    $c_{0,i,j} = \mathsf{com}(r_0, \{t_{0,\ell}, E_{0,\ell}\}_{\ell=1}^d;\ \rho_0)$
  If $i = \pi$: $r_1 = s_\pi - r_0$
    For $\ell \in [d]$, set $V_\ell = G_Q(t_{0,\ell}, r_1) + E_{0,\ell}$
    $c_{1,i,j} = \mathsf{com}(r_1, \{V_\ell\}_{\ell=1}^d;\ \rho_1)$
  If $i \neq \pi$ and $b_{i,j} = 0$: $c_{1,i,j} = \mathsf{com}(\varsigma_1;\ \rho_1)$
  If $i \neq \pi$ and $b_{i,j} = 1$:
    $c_{0,i,j} = \mathsf{com}(\varsigma_0;\ \rho_0)$; sample $r_1 \xleftarrow{\$} \mathbb{F}_q^n$, $\{V_\ell\}_{\ell=1}^d \xleftarrow{\$} (\mathbb{F}_q^{m_Q})^d$
    $c_{1,i,j} = \mathsf{com}(r_1, \{V_\ell\}_{\ell=1}^d;\ \rho_1)$
Set $C_0 = \mathsf{com}(\mathtt{com0}, \mathsf{ctx}, \{c_{0,i,j}\}_{j,i})$, $C_1 = \mathsf{com}(\mathtt{com1}, \mathsf{ctx}, \{c_{1,i,j}\}_{j,i})$
Set $h = \mathsf{com}(\mathtt{init}, \mathsf{ctx}, C_0, C_1)$
Generate $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_\tau) = \mathsf{FS}_1(h, \mathsf{ctx})$, where $\boldsymbol{a}_j = (a_{j,1}, \ldots, a_{j,d})$
For $j \in [\tau]$ and $i \in [N]$:
  For $\ell \in [d]$:
    If $i = \pi$ or ($i \neq \pi$ and $b_{i,j} = 0$):
      $t_{1,\ell} = a_{j,\ell} r_0 - t_{0,\ell}$, $E_{1,\ell} = a_{j,\ell} Q(r_0) - E_{0,\ell}$
    If $i \neq \pi$ and $b_{i,j} = 1$: sample $t_{1,\ell} \xleftarrow{\$} \mathbb{F}_q^n$
      $E_{1,\ell} = a_{j,\ell} Y_i - a_{j,\ell} Q(r_1) - G_Q(t_{1,\ell}, r_1) - V_\ell$
  Sample $\rho_2 \xleftarrow{\$} \{0,1\}^{2\lambda}$, set $c_{2,i,j} = \mathsf{com}(\{t_{1,\ell}, E_{1,\ell}\}_{\ell=1}^d;\ \rho_2)$
Set $C_2 = \mathsf{com}(\mathtt{com2}, \mathsf{ctx}, \{c_{2,i,j}\}_{j,i})$
Generate $(b_1, \ldots, b_\tau) = \mathsf{FS}_2(h, \mathsf{ctx}, \{\boldsymbol{a}_j\}_{j=1}^\tau, C_2)$
For $j \in [\tau]$: set $b_{\pi,j} = b_j \oplus \bigoplus_{i \neq \pi} b_{i,j}$
For $j \in [\tau]$ and $i \in [N]$: $R_{i,j} = \big(r_{b_{i,j}}, \{t_{b_{i,j},\ell}, E_{b_{i,j},\ell}\}_{\ell=1}^d, \rho_{b_{i,j}}, \rho_2, c_{1-b_{i,j},i,j}\big)$
Output $\sigma = \big(T, \mathsf{salt}, h, C_2, \{b_{i,j}, R_{i,j}\}_{j,i}\big)$

Fig. 3. PyuQuMuQu linkable ring signature generation.

PyuQuMuQu Linkable Ring Signature Verification
Public: $Q = (\mathcal{P}, \mathcal{F})$, ring $R = (y_1, \ldots, y_N)$, message M **Input:** $\sigma = \big(T, \mathsf{salt}, h, C_2, \{b_{i,j}, R_{i,j}\}_{j,i}\big)$

Set $Y_i = (y_i, T)$, and reconstruct ctx
Generate $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_\tau) = \mathsf{FS}_1(h, \mathsf{ctx})$
Generate $(b_1, \ldots, b_\tau) = \mathsf{FS}_2(h, \mathsf{ctx}, \{\boldsymbol{a}_j\}_{j=1}^{\tau}, C_2)$
For $j \in [\tau]$: $b_j \stackrel{?}{=} \bigoplus_{i=1}^{N} b_{i,j}$
For $j \in [\tau]$ and $i \in [N]$:
  If $b_{i,j} = 0$: Parse $R_{i,j} = (r_0, \{t_{0,\ell}, E_{0,\ell}\}_{\ell=1}^{d}, \rho_0, \rho_2, c)$
  $\widehat{c}_{0,i,j} = \mathsf{com}(r_0, \{t_{0,\ell}, E_{0,\ell}\}_{\ell=1}^{d};\ \rho_0)$, $\widehat{c}_{1,i,j} = c$
  For $\ell \in [d]$: $\widehat{t}_{1,\ell} = a_{j,\ell} r_0 - t_{0,\ell}$, $\widehat{E}_{1,\ell} = a_{j,\ell} Q(r_0) - E_{0,\ell}$
  $\widehat{c}_{2,i,j} = \mathsf{com}(\{\widehat{t}_{1,\ell}, \widehat{E}_{1,\ell}\}_{\ell=1}^{d};\ \rho_2)$
  If $b_{i,j} = 1$: parse $R_{i,j} = (r_1, \{t_{1,\ell}, E_{1,\ell}\}_{\ell=1}^{d}, \rho_1, \rho_2, c)$, $\widehat{c}_{0,i,j} = c$
  For $\ell \in [d]$: $\widehat{V}_\ell = a_{j,\ell} Y_i - a_{j,\ell} Q(r_1) - G_Q(t_{1,\ell}, r_1) - E_{1,\ell}$
  $\widehat{c}_{1,i,j} = \mathsf{com}(r_1, \{\widehat{V}_\ell\}_{\ell=1}^{d};\ \rho_1)$, $\widehat{c}_{2,i,j} = \mathsf{com}(\{t_{1,\ell}, E_{1,\ell}\}_{\ell=1}^{d};\ \rho_2)$
Set $\widehat{C}_0 = \mathsf{com}(\mathtt{com0}, \mathsf{ctx}, \{\widehat{c}_{0,i,j}\}_{j,i})$,
  $\widehat{C}_1 = \mathsf{com}(\mathtt{com1}, \mathsf{ctx}, \{\widehat{c}_{1,i,j}\}_{j,i})$, $\widehat{C}_2 = \mathsf{com}(\mathtt{com2}, \mathsf{ctx}, \{\widehat{c}_{2,i,j}\}_{j,i})$
Accept iff $h \stackrel{?}{=} \mathsf{com}(\mathtt{init}, \mathsf{ctx}, \widehat{C}_0, \widehat{C}_1)$ and $C_2 \stackrel{?}{=} \widehat{C}_2$

Fig. 4. PyuQuMuQu linkable ring signature verification.

7.1 Anonymity

From the discussion about random MQ maps at the beginning of Section 5, we argued that:

Assumption 1. *For an honest setup, assume that for any two distinct challenge users i_0, i_1, and with aux defined as the secret keys of all other users, we have the following indistinguishability:*

$$(\mathcal{P}, \mathcal{F}, R, \mathsf{aux}, \mathcal{F}(s_{i_0})) \approx_c (\mathcal{P}, \mathcal{F}, R, \mathsf{aux}, \mathcal{F}(s_{i_1})). \tag{9}$$

Theorem 5. *If Assumption 1 holds, Figures 3-4 are anonymous.*

Proof. In the anonymity game, $\mathcal{A}$ receives all public keys, may corrupt users and ask for signatures, then identifies a ring R, a message M, and two uncorrupted members $i_0, i_1 \in R$ for which it has requested no signatures.

The challenger returns $\sigma \stackrel{\$}{\leftarrow} \mathsf{Sign}(s_{i_\beta}, R, M)$ for a hidden bit β, and $\mathcal{A}$ guesses β. We link $\beta = 0$ to $\beta = 1$ through a chain of indistinguishable games.

Game G_0: The real game with $\beta = 0$.

Game G_1: The challenge signature is produced by the simulator of Theorem 4, run on the statement (R, T) with the true tag $T = \mathcal{F}(s_{i_0})$ but without s_{i_0}. The simulator fixes the challenges $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_\tau$ and $b_1, \ldots, b_\tau$ up front, builds the $N\tau$ transcripts exactly as in that proof, and then programs the Fiat-Shamir hashes $\mathsf{FS}_1(h, \mathsf{ctx})$ and $\mathsf{FS}_2(h, \mathsf{ctx}, \{\boldsymbol{a}_j\}_j, C_2)$ to return them. Programming fails only if

$\mathcal{A}$ has already queried one of these points. Both contain ctx, hence the fresh salt, so over Q_H oracle queries this happens with probability at most $Q_H 2^{-\lambda}$. When it succeeds, the opened part of every local transcript is distributed exactly as in an honest signature, each unopened uniform commitment is masked by a fresh $\rho \in \{0,1\}^{2\lambda}$, and the second challenge bits are uniform subject to $\bigoplus_i b_{i,j} = b_j$. Nothing in σ reveals the the witness index, so G_0 and G_1 differ by at most the negligible simulation error $\varepsilon_{\mathrm{zk}} = \mathsf{negl}(\lambda)$.

Game G_2: The same as G_1, but the simulator is given the tag $T = \mathcal{F}(s_{i_1})$. The simulator knows no secret key, so a distinguisher between G_1 and G_2 is a distinguisher for (9). The reduction receives $(\mathcal{P}, \mathcal{F}, R, \mathsf{aux}, T^*)$, where aux holds the secret keys of every user besides i_0, i_1. It answers all corruption and signing queries with those keys (except involving i_0, i_1), simulates the challenge signature on T^*, and forwards $\mathcal{A}$'s guess. It acts as G_1 when $T^* = \mathcal{F}(s_{i_0})$, and G_2 when $T^* = \mathcal{F}(s_{i_1})$. For random maps, (9) is two applications of the tag-hiding statement of Section 5, with a uniform tag, as aux is independent of s_{i_0} and s_{i_1}.

Game G_3: The real game with $\beta = 1$. This is G_2 but with the simulator replaced by honest signing with s_{i_1}. We apply the same indistinguishability argument of $\mathsf{G}_0 \approx \mathsf{G}_1$.

Summing the gaps, the anonymity advantage of $\mathcal{A}$ is at most $2\varepsilon_{\mathrm{zk}} + \varepsilon_{\mathrm{tag}}$, where $\varepsilon_{\mathrm{tag}}$ is the distinguishing advantage in (9), both terms of which are negligible.

7.2 Unforgeability, Linkability, Non-Slanderability

Unforgeability:

Lemma 2. *Let $\mathcal{A}$ be an algorithm making at most Q_H random-oracle queries that outputs an accepting signature σ on (R, M) with probability ε, where the challenges of σ are from $\mathsf{FS}_1, \mathsf{FS}_2$. Figure 2 is $(N+1, 2)$-special sound by Theorem 3, so by [3] and the bound of [4], there is an extractor running in expected time $\mathrm{poly}(\lambda, Q_H)/(\varepsilon - \eta)$ that outputs either a witness $(s, i) \in \mathcal{R}_{R,T}$ or a collision in $\mathsf{com}(\cdot)$, where*

$$\eta = (Q_H + 1)^2 \varepsilon_{N,d}^{\tau} + Q_H^2 2^{-2\lambda} + Q_H 2^{-\lambda}$$

collects the knowledge error, commitment collisions, and simulator programming failures.

We choose τ in Section 8 so that η is negligible, and the proofs below invoke Lemma 2 for every extraction.

Assumption 2. *Sample the maps as specified per protocol, and pick $s_* \xleftarrow{\$} \mathbb{F}_q^n$. Given maps $\mathcal{P}, \mathcal{F}$, with*

$$\mathcal{P}(s_*) = y_*, \quad \mathcal{F}(s_*) = T_*,$$

we assume it is computationally difficult to find s with $\mathcal{P}(s) = y_*$, where this preimage need not have tag T_*.

Theorem 6. *Under Assumption 2, Figure 3 is existentially unforgeable.*

Proof. Plant the instance (y_*, T_*) of Assumption 2 at a uniformly guessed honest index. Generate the remaining keys honestly, and simulate signatures for the embedded user using the supplied T_* with the zero-knowledge simulator of Theorem 4, programming the Fiat-Shamir hashes $\mathsf{FS}_1, \mathsf{FS}_2$ as in the anonymity proof. If the guessed user is corrupted, abort. From an accepted forgery, Lemma 2 yields (s, i) with $\mathcal{P}(s) = y_i$ and $\mathcal{F}(s) = T$, or a collision, which we discard. If i is the embedded user, output s. Guessing among polynomially many keys loses at most a polynomial factor; on the event that the extracted user was guessed, it is guaranteed that they were not corrupted. Any forgery success probability above negligible therefore violates Assumption 2, excepting for the bounded simulation/extraction events.

Linkability: For maliciously chosen public keys, a sufficient property of the maps is that it is hard to find s, s' such that

$$\mathcal{P}(s) = \mathcal{P}(s'), \quad \text{but} \quad \mathcal{F}(s) \neq \mathcal{F}(s'). \tag{10}$$

This key/tag consistency is distinct from standard MQ preimage resistance.

Assumption 3. *For $\mathcal{P}, \mathcal{F}$ sampled as in Section 5 with $m_{\mathcal{P}} = n + c$, no PPT algorithm can output $s \neq s'$ from $(\mathcal{P}, \mathcal{F})$ satisfying* (10)*, except with probability* $\mathsf{negl}(\lambda)$*. The honest-key variant is the same statement when the algorithm is additionally given an honestly sampled s and must output s' for the key $\mathcal{P}(s)$.*

The property is necessary, as for quadratic maps, a single key can have two witnesses: since $G_{\mathcal{P}}(\cdot, \delta)$ is linear for fixed nonzero $\delta \in \mathbb{F}_q^n$, the collision $\mathcal{P}(s+\delta) = \mathcal{P}(s)$ is the linear system (3) with $m_{\mathcal{P}}$ equations in n unknowns, recalling the fixed-difference property of [11] in Section 5. For $m_{\mathcal{P}} \leq n$, this is solvable for effectively every δ, an issue for the linkability game in Theorem 7.

Proposition 2. *Suppose (s, δ) solves* (3)*, with $\mathcal{F}(s + \delta) \neq \mathcal{F}(s)$. Then a user with the key $y = \mathcal{P}(s)$ can produce two valid signatures on y that do not link.*

Proof. The user signs once with s and $s + \delta$ for y, publishing the tags $\mathcal{F}(s)$ and $\mathcal{F}(s + \delta)$. Both signatures verify, since each witness satisfies (1) for its own tag, but the tags differ.

Section 5 gives the evidence for Assumption 3: with $m_{\mathcal{P}} = n+c$, the system (3) is consistent for a q^{-c}-fraction of differences – trying differences is the best known method, with the joint and birthday attacks costlier. For a strictly honest-key paradigm with only later corruptions, a weaker yet sufficient assumption is that, given an honestly sampled s and its key, one cannot find such an s' for that key.

Theorem 7. *Suppose Assumption 3 holds. An adversary cannot produce $k + 1$ pairwise-unlinked accepted signatures using rings contained in a set of k distinct public keys. If these rings contain uncorrupted honest keys, we also suppose Assumption 2 holds.*

Proof. In the linkability game, $\mathcal{A}$ may register public keys of its own choosing, corrupt honest users, and ask for signatures. It wins by outputting $k+1$ valid signatures $\sigma_1, \ldots, \sigma_{k+1}$, none of which were queried by the signing oracle, with pairwise distinct tags $T_1, \ldots, T_{k+1}$ whose rings are in a set K of k public keys.

Apply Lemma 2 to each σ_j in turn. None was produced by the signing oracle, so none has programmed challenges. Up to η per signature, this yields witnesses (s_j, i_j) such that

$$\mathcal{P}(s_j) = y_{i_j} \in K, \quad \mathcal{F}(s_j) = T_j.$$

The rewinding costs a polynomial factor of runtime, and the failure probability is part of η. Since the tags are pairwise distinct, so are the witnesses $s_1, \ldots, s_{k+1}$.

Some extracted key y_{i_j} is honest and uncorrupted. Then σ_j is a forgery on behalf of y_{i_j}, and (10) is not even needed. The reduction guesses in advance which honest key will be hit, and plants the instance (y_*, T_*) of Assumption 2 there. They then answer that user's signing queries with the simulator of Theorem 4 on tag T_*, aborts if the user is corrupted, and outputs s_j. With polynomial-reciprocal probability, the guess is right and s_j inverts $\mathcal{P}$ at y_*.

Every extracted key is either registered by $\mathcal{A}$ or corrupted. Then the $k+1$ distinct witnesses map via $\mathcal{P}$ into a set of at most k keys, so by pigeonhole there exists some pair $j \neq h$ which satisfies

$$\mathcal{P}(s_j) = \mathcal{P}(s_h), \quad \mathcal{F}(s_j) = T_j \neq T_h = \mathcal{F}(s_h),$$

which is exactly the pair forbidden by (10). If y was generated honestly with secret s and corrupted later, the honest-key variant of Assumption 3 suffices: s_j and s_h have different tags, so at least one of them, say s_j, has $\mathcal{F}(s_j) \neq \mathcal{F}(s)$ while $\mathcal{P}(s_j) = \mathcal{P}(s)$. That s_j is precisely the forbidden honest key second preimage.

Non-Slanderability:

Assumption 4. *Given an honestly generated pair $y_* = \mathcal{P}(s_*), T_* = \mathcal{F}(s_*)$, the public maps, and all auxiliary information, we assume it is hard to find s such that $\mathcal{F}(s) = T_*$.*

Theorem 8. *Under Assumption 4, Figure 3 is nonslanderable.*

Proof. In the non-slanderability game, $\mathcal{A}$ receives all public keys, may corrupt users and ask for signatures, and wins by outputting a valid signature σ that was not returned by the signing oracle but links to one that was, say σ^*, signed on behalf of a user $*$ that $\mathcal{A}$ never corrupted. Linking means that σ and σ^* have the same tag T_*.

The reduction $\mathcal{B}$ receives $(\mathcal{P}, \mathcal{F}, y_*, T_*)$ from Assumption 4 and must find a preimage of T_* under $\mathcal{F}$. It guesses the framed user among the polynomially many honest users, places y_* at that position, then generates every other key honestly. Signing queries for other users are also answered honestly. Each signing query for the target is answered by the simulator of Theorem 4 for tag T_*, with $\mathsf{FS}_1, \mathsf{FS}_2$ programmed exactly as in the anonymity proof. If $\mathcal{A}$ corrupts the target, the guess was wrong and $\mathcal{B}$ aborts.

Let $\mathcal{A}$ output σ with tag T_*. Because σ is not an oracle output, its Fiat-Shamir challenges can be thought of as genuine queries; that is, a signature matching a simulated one must either be the result of a collision, or it must change C_2 and thereby draw fresh bits b_j, which $\mathcal{A}$ can only answer by reusing every local bit $b_{i,j}$ it already holds, since the other commitment at each index is never opened – an event of probability $2^{-\tau}$. A signature that shares ctx but not h with a simulated signature simply queries FS_1 at a new value. Both are absorbed into η. Lemma 2 therefore returns, up to η, a witness (s, i) with $Q(s) = Y_i = (y_i, T_*)$, or more exactly, $\mathcal{P}(s) = y_i$ and $\mathcal{F}(s) = T_*$, so $\mathcal{B}$ outputs s.

The index i is not important. A framing signature need not identify the target's key, only reproduce its tag, and s is a preimage of T_* regardless of whichever ring member it is a witness for. $\mathcal{B}$ succeeds with probability at least $\mathrm{Adv}_{\mathcal{A}}/\mathrm{poly}(\lambda) - \eta$, which contradicts Assumption 4 whenever the advantage of $\mathcal{A}$ is non-negligible.

8 Parameters and Costs

8.1 Parameters

Recall we require the number of ring members N to be less than $q^d - 1$ to bound the knowledge error, per Theorem 3. We take $m_{\mathcal{P}} = n + c$ with $c \geq \lceil 2\lambda / \log_2 q \rceil$ and $m_{\mathcal{F}} \approx n$, so that $m_Q = m_{\mathcal{P}} + m_{\mathcal{F}}$ is about $2n + 2\lambda / \log_2 q$. The factor 2 is the Grover insurance of Section 5; classically, $c \geq \lceil \lambda / \log_2 q \rceil$ suffices, which for the parameter set below would reduce $m_{\mathcal{P}}$ by 18. Note that while Crossbred and the hybrid algorithms guess variables, so a Grover speedup is possible in principle, we follow [36] and the MQOM specification in discounting it at security level I. Additionally, the estimator's best classical attack, BooleanSolve at $k = 0$, has no enumeration component for Grover to accelerate. Recall that m_Q is the number of equations an attacker can use to solve, so for the parameter set in Table 2 below, $(q, n, m_Q) = (128, 110, 257)$ corresponds to $(m_{\mathcal{P}}, m_{\mathcal{F}}) = (147, 110)$ with $c = 37$.

Assumptions 2 and 4 give the attacker two instances they can leverage, $y_* = \mathcal{P}(s_*)$ and $T_* = \mathcal{F}(s_*)$. Since s_* satisfies all m_Q equations, the relevant parameters for unforgeability and non-slanderability are (n, m_Q) – we tailor Table 2 for these. Overdetermined systems become easier to solve as the number of equations increases, which is why $\mathcal{F}$ need not be injective and $m_{\mathcal{P}}$ exceeds n by only c. Anonymity relies on tag-hiding of Section 5, which uses one-wayness of both Q and $\mathcal{P}$. A distinguisher may simply attempt to invert Q on (y, T), so the binding instance for anonymity is again (n, m_Q), not the harder $(n, m_{\mathcal{P}})$.

Choice of τ: The Fiat-Shamir transform of a 5-pass protocol does not inherit the knowledge error $\varepsilon^{\tau}_{N,d}$ of its underlying ZKP. Kales and Zaverucha [29] grind the first challenge separately: with $p = N/L$ the per-repetition probability that $\boldsymbol{a}_j$ happens to land in the cheater's prepared set, an attacker who obtains k such repetitions from FS_1 only has to guess the remaining $\tau - k$ bits from FS_2, at a

cost of

$$C(\tau, p) = \min_{0 \le k \le \tau} \Big(\Pr[\mathrm{Bin}(\tau, p) \ge k]^{-1} + 2^{\tau - k} \Big).$$

Its counterpart is [4], which bounds the multi-round knowledge error above by $(Q_H + 1)^2 \varepsilon_{N,d}^{\tau}$, for Q_H hash queries, plus the collision terms – this is η in Lemma 2. We take τ so that $C(\tau, N/L) \ge 2^{\lambda}$, which is standard in MQDSS-type schemes. Larger d shrinks p, but does not prevent this attack, while each increase of d adds $n + m_Q$ field elements per index. For $q = 128$, the smallest τ with $C(\tau, N/L) \ge 2^{128}$ is recorded in our parameter selection Table 3

We estimate the security of our MQ instance against known attacks in Table 2, using BS to denote BooleanSolveFXL [7], C for Crossbred [28], F5 [21], HybridF5 [9], and PXL [25]. Algorithms like Dinur [18,19], Bjorklund [12], Hashimoto [27], Lokshtanov [34], or ExhaustiveSearch [13] do not apply. We obtained these estimates using CryptographicEstimators[1] [20]. For some, we have extra details which provide algorithm-specific parameters, such as the Crossbred degrees D and d_{C}, or the number of coordinates in an exhaustive search k. For our estimations, we take the matrix multiplication constant to be the conservative $\omega = 2$. The best classical attack uses $k = 0$ guessed variables, so Grover search offers it no speedup – the quantum cost of this instance is, to our knowledge, its classical cost.

λ	q	n	m_Q	BS(k)	C(D, d_{C}, k)	F5	HF5(k)	PXL(k)
128	128	110	257	**133**(0)	139(13, 1, 96)	172	170(1)	158(2)

Table 2. Estimated security of parameter sets for $\lambda = 128$, assuming $\omega = 2$.

8.2 Sizes

Define $f = n + d(n + m_Q)$, which represents $r_{b_{i,j}} \in \mathbb{F}_q^n$, d vectors $t_{b_{i,j},\ell} \in \mathbb{F}_q^n$, and d vectors $E_{b_{i,j},\ell} \in \mathbb{F}_q^{m_Q}$. For each ring position in each repetition, Figure 3 communicates one bit $b_{i,j}$, two λ-length blinders, and one 2λ-length commitment, together with f field elements. The total cost of the signature is then

$$|\sigma| = \underbrace{m_{\mathcal{F}} \lceil \log_2(q) \rceil}_{T} + \underbrace{5\lambda}_{\mathsf{salt}+h+C_2} + N\tau \Big(\underbrace{1}_{b_{i,j}} + \underbrace{4\lambda}_{\rho_{b_{i,j}}, \rho_2, c_{1-b_{i,j},i,j}} + f \lceil \log_2(q) \rceil \Big) \text{ bits.}$$

The cost of communicating the coefficients of the MQ maps in (5) is $m_Q n(n + 3)/2 \lceil \log_2(q) \rceil$ bits [15], but we sample them from a seed. The cost of the public key is then

$$\underbrace{4\lambda}_{\mathcal{P},\mathcal{F}} + \underbrace{N m_{\mathcal{P}} \lceil \log_2(q) \rceil}_{R} \text{ bits.}$$

We record the signature and public key sizes in Table 3, with N the number of ring members and τ the minimal number of rounds so $C(\tau, N/L) \ge 2^{\lambda}$.

[1] `https://github.com/Crypto-TII/CryptographicEstimators`

λ	d	N	τ	Sig	PubKey
	1	4	184	355 kB	578 B
	1	8	204	786 kB	1.09 kB
128	1	16	240	1.85 MB	2.12 kB
	2	32	152	3.90 MB	4.18 kB
	2	64	156	8.01 MB	8.30 kB

Table 3. Signature and public key sizes using parameters of Table 2.

9 Conclusion

In this paper, we demonstrated that the multivariate quadratic linkable ring signatures of Omar, Padhye, and Dey [39], and by Namdeo, Mishra, and Srivastava [37] are unsound, by designing a sumset attack wherein an adversary can use the split nature of the challenges to force them into an admissible subset that they can always answer. We continue this attack to additionally show that the four-challenge protocol of Monteiro, Goya, and Terada [35], in the form transcribed by [37] and used as the foundation of their LRS, is incomplete and has soundness error 3/4, and that its natural repair – while achieving the desired soundness 1/2 – requires three transcripts to extract. The two-transcript lemma of [37] therefore fails in both cases.

We proceed to fill in the gap that we have created by proposing PyuQuMuQu, a plausibly post-quantum MQ-based linkable ring signature, built from a 5-pass zero-knowledge proof which enjoys a soundness error of $\frac{1}{2} + \frac{N}{2(q^d-1)}$, for d the challenge dimension and $N \leq q^d - 1$ the number of ring members. This protocol realizes ring signature sizes of 355 kB with a public key of 578 B for a ring with 4 members at 128-bit security.

Acknowledgments

This research was supported by the National Science Foundation (Grant Number DMS-2342254). There are no competing interests to declare. AI was used to assist in the polishing of this document by performing tasks like typesetting, identifying mistakes, and by cleaning up tables and figures. The resulting paper is an accurate representation of the author's work and intellectual contributions, so we accept all responsibility.

References

1. Alberto Torres, W.A., Steinfeld, R., Sakzad, A., Liu, J.K., Kuchta, V., Bhattacharjee, N., Au, M.H., Cheng, J.: Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0). In: Susilo, W., Yang, G. (eds.) Information Security and Privacy. pp. 558–576. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-93638-3_32

2. Attema, T., Cramer, R., Kohl, L.: A Compressed Σ-Protocol Theory for Lattices. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part II. pp. 549–579. Lecture Notes in Computer Science, Springer (2021). https://doi.org/10.1007/978-3-030-84245-1_19
3. Attema, T., Fehr, S.: Parallel Repetition of $(k_1, \ldots, k_\mu)$-Special-Sound Multi-Round Interactive Proofs. In: Advances in Cryptology – CRYPTO 2022 - 42nd Annual International Cryptology Conference, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13508, pp. 415–443. Springer (2022). https://doi.org/10.1007/978-3-031-15802-5_15, https://doi.org_15
4. Attema, T., Fehr, S., Klooß, M.: Fiat-Shamir Transformation of Multi-Round Interactive Proofs. Journal of Cryptology **36**(4), 36 (2023). https://doi.org/10.1007/s00145-023-09478-y
5. Babai, L.: Trading Group Theory for Randomness. In: Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing. p. 421–429. STOC '85, Association for Computing Machinery, New York, NY, USA (1985). https://doi.org/10.1145/22145.22192, https://doi.org/10.1145/22145.22192
6. Balla, D., Chaidos, P.: On the (Strong) Linkability of Linkable Ring Signatures. Cryptology ePrint Archive, Paper 2025/1375 (2025), https://eprint.iacr.org/2025/1375
7. Bardet, M., Faugère, J., Salvy, B., Spaenlehauer, P.: On the Complexity of Solving Quadratic Boolean Systems. J. Complex. **29**(1), 53–75 (2013). https://doi.org/10.1016/J.JCO.2012.07.001
8. Baum, C., Lin, H., Oechsner, S.: Towards Practical Lattice-Based One-Time Linkable Ring Signatures. In: Naccache, D., Xu, S., Qing, S., Samarati, P., Blanc, G., Lu, R., Zhang, Z., Meddahi, A. (eds.) Information and Communications Security - 20th International Conference, ICICS 2018, Lille, France, October 29-31, 2018, Proceedings. Lecture Notes in Computer Science, vol. 11149, pp. 303–322. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01950-1_18
9. Bettale, L., Faugère, J., Perret, L.: Hybrid Approach for Solving Multivariate Systems over Finite Fields. J. Math. Cryptol. **3**(3), 177–197 (2009). https://doi.org/10.1515/JMC.2009.009
10. 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. pp. 464–492. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-64834-3_16
11. Billet, O., Robshaw, M.J.B., Peyrin, T.: On Building Hash Functions from Multivariate Quadratic Equations. In: ACISP 2007. Lecture Notes in Computer Science, vol. 4586, pp. 82–95 (2007). https://doi.org/10.1007/978-3-540-73458-1_7
12. Björklund, A., Kaski, P., Williams, R.: Solving Systems of Polynomial Equations over GF(2) by a Parity-Counting Self-Reduction. In: Baier, C., Chatzigiannakis, I., Flocchini, P., Leonardi, S. (eds.) 46th International Colloquium on Automata, Languages, and Programming (ICALP 2019). Leibniz International Proceedings in Informatics (LIPIcs), vol. 132, pp. 26:1–26:13. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2019). https://doi.org/10.4230/LIPIcs.ICALP.2019.26
13. Bouillaguet, C., Chen, H.C., Cheng, C., Chou, T., Niederhagen, R., Shamir, A., Yang, B.: Fast Exhaustive Search for Polynomial Systems in F2. In: Mangard, S., Standaert, F. (eds.) Cryptographic Hardware and Embedded Systems - CHES

2010 (12th International Workshop, Santa Barbara CA, USA, August 17-20, 2010. Proceedings). pp. 203–218. Lecture Notes in Computer Science, Springer, Germany (2010). https://doi.org/10.1007/978-3-642-15031-9_14
14. Cauchy, A.L.: Recherches sur les Nombres. J. École Polytech. **9**, 99–116 (1813)
15. Chen, M., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: From 5-Pass MQ-Based Identification to MQ-Based Signatures. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 10032, pp. 135–165 (2016). https://doi.org/10.1007/978-3-662-53890-6_5
16. Chiang, J.H., Damgård, I., Duro, W.R., Engan, S., Kolby, S., Scholl, P.: Post-Quantum Threshold Ring Signature Applications from VOLE-in-the-Head. In: Huang, C., Chen, J., Shieh, S., Lie, D., Cortier, V. (eds.) Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, CCS 2025, Taipei, Taiwan, October 13-17, 2025. pp. 4664–4678. ACM (2025). https://doi.org/10.1145/3719027.3744854
17. Davenport, H.: On the Addition of Residue Classes. Journal of the London Mathematical Society **s1-10**(1), 30–32 (1935). https://doi.org/10.1112/jlms/s1-10.1.30
18. Dinur, I.: Cryptanalytic Applications of the Polynomial Method for Solving Multivariate Equation Systems over GF(2). In: Canteaut, A., Standaert, F.X. (eds.) Advances in Cryptology – EUROCRYPT 2021. pp. 374–403. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-77870-5_14
19. Dinur, I.: Improved Algorithms for Solving Polynomial Systems over GF(2) by Multiple Parity-Counting. In: Marx, D. (ed.) Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021, Virtual Conference, January 10 - 13, 2021. pp. 2550–2564. SIAM (2021). https://doi.org/10.1137/1.9781611976465.151
20. Esser, A., Verbel, J.A., Zweydinger, F., Bellini, E.: SoK: CryptographicEstimators - a Software Library for Cryptographic Hardness Estimation. In: Zhou, J., Quek, T.Q.S., Gao, D., Cárdenas, A.A. (eds.) Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2024, Singapore, July 1-5, 2024. ACM (2024). https://doi.org/10.1145/3634737.3645007
21. Faugère, J.C.: A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. p. 75–83. ISSAC '02, Association for Computing Machinery, New York, NY, USA (2002). https://doi.org/10.1145/780506.780516
22. Feige, U., Fiat, A., Shamir, A.: Zero-Knowledge Proofs of Identity. J. Cryptol. **1**(2), 77–94 (1988). https://doi.org/10.1007/BF02351717
23. Feneuil, T., Rivain, M.: Threshold Computation in the Head: Improved Framework for Post-Quantum Signatures and Zero-Knowledge Arguments. J. Cryptol. **38**(3), 28 (2025). https://doi.org/10.1007/S00145-025-09543-8
24. Fiat, A., Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Proceedings on Advances in Cryptology—CRYPTO '86. p. 186–194. Springer-Verlag, Berlin, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12
25. Furue, H., Kudo, M.: Polynomial XL: A Variant of the XL Algorithm Using Macaulay Matrices over Polynomial Rings. In: Post-Quantum Cryptography: 15th

International Workshop, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings, Part II. p. 109–143. Springer-Verlag, Berlin, Heidelberg (2024), https://doi.org/10.1007/978-3-031-62746-0_6
26. Goldwasser, S., Micali, S., Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing **18**(1), 186–208 (1989). https://doi.org/10.1137/0218012
27. Hashimoto, Y.: An Improvement of Algorithms to Solve Under-Defined Systems of Multivariate Quadratic Equations. Cryptology ePrint Archive, Paper 2021/1045 (2021), https://eprint.iacr.org/2021/1045
28. Joux, A., Vitse, V.: A Crossbred Algorithm for Solving Boolean Polynomial Systems. In: Kaczorowski, J., Pieprzyk, J., Pomykała, J. (eds.) Number-Theoretic Methods in Cryptology. pp. 3–21. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-76620-1_1
29. Kales, D., Zaverucha, G.: An Attack on Some Signature Schemes Constructed From Five-Pass Identification Schemes. In: CANS 2020. Lecture Notes in Computer Science, vol. 12579, pp. 3–22 (2020). https://doi.org/10.1007/978-3-030-65411-5_1
30. Liu, F.H., Lu, C.J., Yang, B.Y.: Secure PRNGs from Specialized Polynomial Maps over Any $\mathbb{F}_q$. In: Post-Quantum Cryptography – PQCrypto 2008. Lecture Notes in Computer Science, vol. 5299, pp. 181–202. Springer (2008). https://doi.org/10.1007/978-3-540-88403-3_13
31. Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Linkable Ring Signature with Unconditional Anonymity. IEEE Transactions on Knowledge and Data Engineering **26**(1), 157–165 (2014). https://doi.org/10.1109/TKDE.2013.17
32. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups. In: ACISP 2004. Lecture Notes in Computer Science, vol. 3108, pp. 325–335 (2004). https://doi.org/10.1007/978-3-540-27800-9_28
33. Liu, X., Wang, L.P.: A Postquantum Linkable Ring Signature Scheme from Coding Theory. Security and Communication Networks **2023**, 1–12 (12 2023). https://doi.org/10.1155/2023/1794053
34. Lokshtanov, D., Paturi, R., Tamaki, S., Williams, R.R., Yu, H.: Beating Brute Force for Systems of Polynomial Equations over Finite Fields. In: Klein, P.N. (ed.) Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19. pp. 2190–2202. SIAM (2017). https://doi.org/10.1137/1.9781611974782.143
35. Monteiro, F.S., Goya, D.H., Terada, R.: Improved Identification Protocol Based on the *MQ* Problem. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **98-A**(6), 1255–1265 (2015). https://doi.org/10.1587/TRANSFUN.E98.A.1255
36. Moody, D., Alagic, G., Bros, M., Ciadoux, P., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.K., Miller, C., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., Waller, N.: Status Report on the Second Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. Tech. Rep. NIST IR 8610, National Institute of Standards and Technology (2026). https://doi.org/10.6028/NIST.IR.8610
37. Namdeo, K., Mishra, D., Srivastava, N.: Round-Optimal Linkable Ring Signature Based on MQ Problem with Extended Linkability. J. Inf. Secur. Appl. **100**, 104483 (2026). https://doi.org/10.1016/J.JISA.2026.104483
38. Nguyen, K., Tang, H., Wang, H., Zeng, N.: New Code-Based Privacy-Preserving Cryptographic Constructions. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory

and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11922, pp. 25–55. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34621-8_2
39. Omar, S., Padhye, S., Dey, D.: Linkable Ring Signature Scheme Based on Multivariate Polynomial over Finite Field. Adv. Math. Commun. **19**(5), 1301–1319 (2025). https://doi.org/10.3934/AMC.2024055
40. 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. pp. 552–565. Lecture Notes in Computer Science, Springer (2001). https://doi.org/10.1007/3-540-45682-1_32
41. Sakumoto, K., Shirai, T., Hiwatari, H.: Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials. In: Rogaway, P. (ed.) Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6841, pp. 706–723. Springer (2011). https://doi.org/10.1007/978-3-642-22792-9_40
42. Thomae, E., Wolf, C.: Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) Public Key Cryptography – PKC 2012. pp. 156–171. Springer Berlin Heidelberg, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_10
43. Xue, Y., Lu, X., Au, M.H., Zhang, C.: Efficient Linkable Ring Signatures: New Framework and Post-Quantum Instantiations. In: Computer Security – ESORICS 2024. Lecture Notes in Computer Science, vol. 14985, pp. 435–456 (2024). https://doi.org/10.1007/978-3-031-70903-6_22
44. Zhang, X., Steinfeld, R., Liu, J.K., Esgin, M.F., Liu, D., Ruj, S.: DualRing-PRF: Post-quantum (Linkable) Ring Signatures from Legendre and Power Residue PRFs. In: Zhu, T., Li, Y. (eds.) Information Security and Privacy - 29th Australasian Conference, ACISP 2024, Sydney, NSW, Australia, July 15-17, 2024, Proceedings, Part II. Lecture Notes in Computer Science, vol. 14896, pp. 124–143. Springer (2024). https://doi.org/10.1007/978-981-97-5028-3_7