Algebraic Cryptanalysis of LOCKER and ROLLO

MiniMax

November 2026

Abstract

Ideal Low-Rank Parity-Check (LRPC) key encapsulation mechanisms replace Hamming weight with rank weight over a binary polynomial quotient ring. They were submitted to the first round of the NIST Post-Quantum Cryptography standardization process as Low-Rank Parity-Check Codes Encryption (LOCKER), Low-Rank Parity-Check Key Exchange (LAKE), and Rank-Ouroboros, and merged in the second round as Rank-Ouroboros, LAKE, and LOCKER (ROLLO). Because an irreducible binary modulus of degree n over $\mathbb{F}_{2^m}$ eliminates proper ideals when m and n are coprime, prior algebraic attacks unfold ring multiplication into a generic linear code of length $2n$ over $\mathbb{F}_{2^m}$, requiring hundreds of millions of minor variables and petabytes of memory on first-round parameters.

In this paper, we show that the irreducibility of the ring modulus enables a direct algebraic attack whenever the field extension degree m exceeds 2^r for error rank r or 2^d for secret key rank d. Because the binary quotient ring modulo the irreducible polynomial is itself the extension field $\mathbb{F}_{2^n}$, transposing the $n \times m$ binary coefficient matrix maps the scheme ring isomorphically onto a polynomial quotient ring over $\mathbb{F}_{2^n}$. Under this transposition, any subspace of the original base field $\mathbb{F}_{2^m}$ consists of polynomials with binary coefficients and is fixed pointwise by squaring coefficients in $\mathbb{F}_{2^n}$. Iterating this partial Frobenius automorphism generates an orbit of conjugate equations over the identical unknown support from a single passive ciphertext or public key with zero decapsulation queries. We derive polynomial-time ciphertext support recovery via local Schur elimination when $m > 2^r$, and direct public-key secret recovery via principal minors and a closed-form Moore-matrix gauge recursion when $m \geq 2^d$. Across all 27 published parameter sets (24 official NIST submission sets from 2017–2020 and 3 additional new2ROLLO-I sets), our attacks improve upon the best published complexities on 14 sets—recovering the shared secret of LOCKER-I in 1.15 s using 58 MB of memory on a 12-thread workstation and recovering the 2019 ROLLO-I-128 secret key in 5.97 s on a single core—while proving via exact Frobenius syzygy counts that the 2020 revised ROLLO and new2ROLLO-I parameter sets with $m \leq 2^r$ and $m < 2^d$ remain immune.

1 Introduction

1.1 Background and Design Rationale

Code-based public-key cryptosystems in the Hamming metric, such as Classic McEliece, require public keys of several hundred kilobytes because information-set decoding scales only linearly with the error weight in the exponent. Rank-metric cryptography replaces Hamming weight over $\mathbb{F}_2$ with the $\mathbb{F}_2$-rank of vectors over an extension field $K \cong \mathbb{F}_{2^m}$. Because generic Rank Syndrome Decoding (RSD) algorithms scale quadratically with m and the rank weight r in the exponent, rank-metric constructions achieve 128-bit security with public keys under one kilobyte.

Introduced by Gaborit, Murat, Ruatta, and Zémor [15], Ideal Low-Rank Parity-Check (LRPC) cryptosystems compress keys to a single ring element by operating in the polynomial quotient ring $R = K[X]/(P(X))$ of degree n. A secret key consists of a d-dimensional $\mathbb{F}_2$-subspace $F \subset K$ and two polynomials $x, y \in F^n$ whose coefficients lie in F, while the public

key is the quotient $h = x^{-1}y \bmod P(X)$ (747 bytes in LOCKER-I). Encapsulation samples an r-dimensional $\mathbb{F}_2$-subspace $E \subset K$ and error polynomials $e_1, e_2 \in E^n$, outputting the syndrome $u = e_1 + e_2 h \bmod P(X)$. Decapsulation computes $s = xu \equiv xe_1 + ye_2 \pmod{P(X)}$, whose coefficients lie in the product subspace $F \cdot E$ of dimension at most $rd < m$, and intersects $f_i^{-1} \operatorname{Supp}(s)$ across a basis of F to recover E.

Across the NIST Post-Quantum Cryptography standardization process and contemporaneous cryptanalytic literature, 27 Ideal-LRPC parameter sets (24 official submission sets and 3 literature sets) were specified across four parameter families. In November 2017 (NIST Round 1), Aragon et al. [3] submitted three sister schemes: LAKE (an ephemeral IND-CPA KEM), LOCKER (an IND-CCA2 KEM with nine parameter sets LOCKER-I..IX at $r \in \{5, 6\}$ and $d \in \{7, 8, 9\}$ designed for decryption failure rates below 2^{-64}), and Rank-Ouroboros. In March 2019 (NIST Round 2 [4]), the three submissions were merged into ROLLO-I (LAKE), ROLLO-II (LOCKER), and ROLLO-III (Rank-Ouroboros), comprising nine parameter sets with $r \in \{5, 6, 7\}, d \in \{6, 7, 8\}$ on ROLLO-I/II and secret-key rank $d = w \in \{5, 6, 7\}$, error rank $r = w_r \in \{6, 8, 8\}$ on ROLLO-III. Following the algebraic attacks of Bardet et al. [8, 9]—where [9] also proposed three illustrative large-m parameter sets new2ROLLO-I-128/192/256 ($m \in \{73, 89, 103\}$, $r \in \{7, 8, 9\}$, later re-evaluated in [10])—the April 2020 Round 2 revision [5] dropped ROLLO-III and raised (r, d) to 7–9 across six sets (ROLLO-I/II-128/192/256). In July 2020, NIST declined to advance ROLLO to Round 3 [20], citing rapid progress in algebraic cryptanalysis of rank-metric codes.

1.2 Prior Cryptanalysis

Prior cryptanalysis of Ideal-LRPC schemes follows four main directions, summarized in Table 1. First, Hauteville and Tillich [17] showed that when $P(X)$ factors over $\mathbb{F}_2$ (as in quasi-cyclic rings modulo $X^n - 1$), projecting modulo a proper factor shortens the code length while preserving the rank bound r. To block quotient-ring folding, all 27 published LOCKER and ROLLO parameter sets choose an irreducible binary polynomial $P(X) \in \mathbb{F}_2[X]$ with $\gcd(m, n) = 1$, so that $R \cong \mathbb{F}_{2^{mn}}$ is an extension field with no proper ideals. Chee et al. [12] separately analyzed a modified layered ROLLO-I variant with restricted error degrees $\deg(e_i) \ll n$, which does not apply to standard full-degree errors.

Second, combinatorial subspace-guessing attacks [15, 3] cost $\widetilde{O}(2^{(r-1)\lceil m(n+1)/(2n)\rceil})$ operations (2^{144} on LOCKER-I). Decryption-failure reaction attacks [21] require approximately $\mathrm{DFR}^{-1} \geq 2^{64}$ active decapsulation queries on LOCKER and do not apply to ephemeral ROLLO-I. Third, the structural dual-LRPC key recovery attack analyzed in the ROLLO specification [5, §6.2] and evaluated across the 2020 parameters by Song et al. [22] searches for rank-d multiples of $(y, -x)$ up to n ring shifts in $O((nm)^\omega 2^{d\lceil m/2\rceil - m - n})$ operations. This structural attack requires 2^{133} operations on LOCKER-I and reduces four 2020 sets below their claimed security ($2^{103.2}$–$2^{180.3}$), whereas 2020 ROLLO-I-128/256 and all new2ROLLO-I sets remain above claimed levels.

Fourth, the algebraic MaxMinors and Support-Minors attacks introduced by Bardet et al. [8, 9, 10] and further analyzed by Couvée et al. [11] and Esser, Verbel, and Villanueva-Polanco [14] expand multiplication modulo $P(X)$ into an $n \times n$ companion matrix over $K = \mathbb{F}_{2^m}$ and treat (e_1, e_2) as a generic $[2n, n]$ linear code over K. Even after optimal puncturing ($p = 17$ on LOCKER-I and $p = 9$ on 2019 ROLLO-I-128), linearizing $(r + 1) \times (r + 1)$ maximal minors requires $\binom{2n-p}{r} = \binom{149}{5} = 5.72 \times 10^8$ columns ($\approx$ 42 PB dense memory) on LOCKER-I and $\binom{85}{5} = 3.28 \times 10^7$ columns ($\approx$ 141 TB dense memory) on 2019 ROLLO-I-128. In the standard ring representation $R = K[X]/(P(X))$, one cannot generate extra equations over the same support $E = \langle b_1, \ldots, b_r \rangle_{\mathbb{F}_2} \subset K$ by squaring K-coefficients, because the Frobenius map on K

Table 1: Comparison of passive attacks (0 decapsulation queries) on LOCKER-I and 2019 ROLLO-I-128. Column counts give the number of linearized minor variables after optimal puncturing or Schur reduction; complexities are reported in $\log_2$ two-input gates.

Reference	Attack Method	Columns	Memory	Gates	Time
Target: LOCKER-I ($m = 71, n = 83, r = 5, d = 7$; *claimed* 128-*bit IND-CCA2)*					
Aragon et al. [3]	Combinatorial RSD	—	—	$2^{144.0}$	—
Hauteville–Tillich [17]	Quotient folding	—	—	N/A	—
Bardet et al. [9]	MaxMinors ($\omega = 2.81$)	5.72×10^8	42 PB	$2^{81.8}$	—
Esser et al. [14]	MaxMinors ($\omega = 2$)	5.72×10^8	42 PB	$2^{58.2}$	—
This Work (Sec. 5.2)	Schur TSM ($P = 9$)	2,240	58 MB	$2^{45.6\dagger}$	1.15 s
This Work (Sec. 5.4)	Sparse Lanczos TSM	4,032	18 MB	$2^{46.3}$	—
Target: 2019 ROLLO-I-128 ($m = 79, n = 47, r = 5, d = 6$; *claimed* 128-*bit IND-CPA)*					
Bardet et al. [9]	MaxMinors ($\omega = 2.81$)	3.28×10^7	141 TB	$2^{70.2}$	—
Esser et al. [14]	MaxMinors ($\omega = 2$)	3.28×10^7	141 TB	$2^{50.0}$	—
This Work (Sec. 5.2)	Schur TSM ($P = 8$)	1,120	48 MB	$2^{42.2}$	—
This Work (Sec. 6.1)	Direct key recovery	64	< 2 MB	$2^{31.3}$	5.97 s

†Evaluated in the $2n^2$ two-input gate model on the 2184×2240 Schur-reduced matrix over $\mathbb{F}_{2^{83}}$ ($2^{39.7}$ under the $n = \log_2 q$ field-operation metric of [14]).

sends

$$e_i(X) = \sum_{k=1}^{r} b_k\, a_{i,k}(X) \;\longmapsto\; \sum_{k=1}^{r} b_k^2\, a_{i,k}(X) \qquad (a_{i,k}(X) \in \mathbb{F}_2[X]/(P(X))),$$

which shifts E to a distinct subspace $E^{[1]} = \langle b_1^2, \ldots, b_r^2 \rangle_{\mathbb{F}_2} \neq E$. For this reason, the ROLLO specifications and subsequent rank-metric security analyses [5, 2, 6] concluded that choosing an irreducible modulus $P(X)$ prevents ideal structure from accelerating syndrome decoding.

1.3 Our Contributions

We show that the irreducibility of $P(X) \in \mathbb{F}_2[X]$—introduced specifically to defeat quotient-ring folding [17]—makes the binary quotient ring $L = \mathbb{F}_2[X]/(P(X)) \cong \mathbb{F}_{2^n}$ a field and unlocks a partial Frobenius action that preserves the secret support. Transposing the $n \times m$ binary coefficient matrix exchanges the roles of X and T, mapping $R = K[X]/(P(X))$ isomorphically onto $Q = L[T]/(g(T))$. In Q, each binary polynomial $a_{i,k}(X)$ becomes a field scalar in L, whereas each support basis element $b_k(T) \in K$ becomes a polynomial in T with $\{0, 1\}$ coefficients, fixed pointwise by squaring L-coefficients via $\rho(\sum_t \gamma_t T^t) = \sum_t \gamma_t^2 T^t$. Iterating ρ on a single passive ciphertext or public key generates up to n conjugate equations over the identical support basis:

1. **Transposed Partial Frobenius Orbit (Section 4, Lemma 2):** Building on the classical transposition duality of matrix codes [13], we prove that $\Phi : R \xrightarrow{\sim} Q = L[T]/(g(T))$ identifies $\Phi(K) = \mathbb{F}_2[T]/(g(T))$ with the fixed subring Q^ρ, satisfies $(L \otimes_{\mathbb{F}_2} E) \cap \Phi(K) = \Phi(E)$, and generates an orbit of conjugate syndrome equations $U_q = \rho^q(U_0)$ over the unchanged support $\Phi(E)$.
2. **Ciphertext Support Recovery for $m > 2^r$ (Section 5, Lemma 3, Propositions 4–8, Theorem 5):** Adapting the Support-Minors cofactor expansion of Bardet et al. [9, 10] to the commutative ring Q across $P \ll n$ Frobenius conjugates restricts the minor unknowns to $\binom{P}{r}2^r$ pair-transversal minors in L, where each non-pivot subset $0 \notin S_i$ forms a local $m \times 2^r$ block B_i. When $m > 2^r$ and $P \geq P_2^*(m, r) = \lceil (mr - 2^r)/(m - 2^r) \rceil \leq n$, local Schur elimination collapses LOCKER-I from 5.72×10^8 columns (42 PB) to 2,240 columns (58 MB),

recovering the shared secret in 1.15 s on a 12-thread CPU. For $r = 6$, retaining the unreduced block-staircase matrix yields constant row weight $w = (r+1)2^r = 448$, compressing LOCKER-III/VI/IX from 565–863 GB dense storage into 1.65–2.35 GB compressed sparse row (CSR) format ($2^{58.8}$–$2^{60.5}$ gates). We also prove that $X^n - 1$ quotients and non-coprime degrees $\gcd(m, n) > 1$ remain vulnerable via cyclotomic projection.

3. **Direct Public-Key Recovery for $m \geq 2^d$ (Section 6, Theorems 9–10, Proposition 11):** We prove that when $m \geq 2^d$, the $m \times 2^d$ matrix C_H formed by subset products of $H_0, \ldots, H_{d-1}$ has a one-dimensional L-kernel whose entries equal all 2^d principal minors of the Moore transition matrix $M = BA^{-1} \in \mathrm{GL}_d(L)$. Whereas classical principal-minor reconstruction [18, 16] determines $\tilde{M}$ only up to an unknown diagonal similarity $M = D\tilde{M}D^{-1}$ in $(L^\times)^{d-1}$ and transposition, we derive a closed-form Moore-row recursion for D from the uniqueness of the subspace annihilator polynomial $\mathcal{L}_\alpha(Z)$. On homogeneous Ideal-LRPC public keys $h = x^{-1}y \bmod P(X)$, this recovers the secret key (F, x, y) from h alone in 5.97 s on 2019 ROLLO-I-128 on a single core (whereas inhomogeneous 2019 ROLLO-III-128/192 public keys $\mathsf{pk} = (h, s = x + hy)$ are solved directly by Section 5 in $2^{39.3}$ and $2^{57.6}$ gates).
4. **Phase Transitions and 27-Set Security Ledger (Sections 7–8, Theorem 12):** We prove that in the sub-threshold regime $m \leq 2^r$, the exact $\mathbb{F}_2$-nullity is $\nu_{\mathbb{F}_2}(P) = n[2^r\binom{P-1}{r-1} - m\binom{P-2}{r-1}]$, which grows strictly with P and leaves quadratic Grassmannian Plücker relations underdetermined by factors of 6.5×10^3 to 1.07×10^5. Evaluating all 27 published parameter sets shows that our attacks improve upon published 2026 complexities on 14 sets (all 9 Round 1 LOCKER sets and 5 of 9 initial Round 2 ROLLO sets), while all 6 revised Round 2 ROLLO sets (2020) and all 3 new2ROLLO-I sets [9] satisfy $m < 2^r, 2^d$ and remain immune.

1.4 Paper Organization

Section 2 establishes our algebraic notation and reviews rank syndrome decoding, Ideal-LRPC codes, Support-Minors linearization, Moore matrices, and the Principal Minor Assignment Problem. Section 3 gives the formal specification of LOCKER and ROLLO across all four parameter generations. Section 4 introduces the transposed ring isomorphism Φ and proves support invariance under the partial Frobenius ρ. Section 5 develops our ciphertext support-recovery attacks. Section 6 presents our direct public-key recovery attack and transposed subspace search. Section 7 proves the exact nullity formula and quadratic Plücker barriers for $m \leq 2^r$. Section 8 presents the complete 27-set complexity ledger and experimental verification benchmarks.

2 Preliminaries

2.1 Finite Fields and Quotient Rings

Let $\mathbb{F}_2 = \{0, 1\}$ denote the binary field. Given an irreducible binary polynomial $g(T) \in \mathbb{F}_2[T]$ of degree m, we denote by $K \coloneqq \mathbb{F}_2[T]/(g(T)) \cong \mathbb{F}_{2^m}$ the degree-m extension field viewed as an m-dimensional vector space over $\mathbb{F}_2$ with power basis $(1, T, \ldots, T^{m-1})$. Let $P(X) \in \mathbb{F}_2[X]$ be a monic binary polynomial of degree n. The polynomial quotient ring over K is

$$R \coloneqq K[X]/(P(X)) = \left\{ \sum_{j=0}^{n-1} a_j X^j : a_j \in K \right\}.$$

Expanding each coefficient $a_j = \sum_{t=0}^{m-1} \mu_{j,t} T^t \in K$ ($\mu_{j,t} \in \mathbb{F}_2$) associates to every ring element $a \in R$ a unique binary coefficient matrix $M(a) \coloneqq (\mu_{j,t})_{0 \leq j < n,\, 0 \leq t < m} \in \mathbb{F}_2^{n \times m}$.

The *rank support* of $a \in R$, denoted $\mathrm{Supp}(a) \coloneqq \langle a_0, \ldots, a_{n-1} \rangle_{\mathbb{F}_2} \subseteq K$, is the $\mathbb{F}_2$-subspace of K spanned by the coefficients of $a(X)$. Its dimension $\mathrm{rank}_{\mathbb{F}_2}(a) \coloneqq \dim_{\mathbb{F}_2} \mathrm{Supp}(a) = \mathrm{rank}_{\mathbb{F}_2} M(a)$

is the rank weight of a. An element $e \in R$ satisfies $\mathrm{Supp}(e) \subseteq E$ for an r-dimensional subspace $E = \langle b_1, \ldots, b_r \rangle_{\mathbb{F}_2} \subset K$ if and only if $\mathrm{rank}_{\mathbb{F}_2} M(e) \leq r$, or equivalently if $e(X)$ admits the rank-r decomposition

$$e(X) = \sum_{k=1}^{r} b_k \, a_k(X), \qquad b_k \in K, \quad a_k(X) \in \mathbb{F}_2[X]/(P(X)). \tag{1}$$

In matrix terms, (1) expresses $M(e) \in \mathbb{F}_2^{n \times m}$ as a sum of r outer products of column vectors in $\mathbb{F}_2^n$ and row vectors in $\mathbb{F}_2^m$. By Delsarte's classical duality for matrix codes [13], transposing $M(e) \mapsto M(e)^\top \in \mathbb{F}_2^{m \times n}$ preserves the $\mathbb{F}_2$-rank r while exchanging the roles of the column space over $\mathbb{F}_2^n$ and the row space over $\mathbb{F}_2^m$.

We denote by $\mathrm{Gr}_{\mathbb{F}_2}(r, K)$ the Grassmannian of all r-dimensional $\mathbb{F}_2$-subspaces of K, whose cardinality is given by the Gaussian binomial coefficient

$$\left|\mathrm{Gr}_{\mathbb{F}_2}(r, K)\right| = \begin{bmatrix} m \\ r \end{bmatrix}_2 \coloneqq \prod_{i=0}^{r-1} \frac{2^m - 2^i}{2^r - 2^i}.$$

For any r-dimensional subspace $E \subset K$, we write $\mathrm{RREF}(E) \in K^r$ for the canonical basis of E whose $r \times m$ binary matrix in the basis $(1, T, \ldots, T^{m-1})$ is in reduced row-echelon form.

2.2 Rank Syndrome Decoding and Ideal-LRPC Codes

The security of LOCKER and ROLLO rests on the Rank Syndrome Decoding (RSD) problem and its ring-structured specialization to Ideal-LRPC codes [15, 3, 5].

Definition 1 (Ideal Rank Syndrome Decoding and Low-Rank Parity-Check Codes [15, 5])**.** Let $R = K[X]/(P(X))$ with $K = \mathbb{F}_{2^m}$ and $\deg P = n$. In the Ideal-RSD(m, n, r) distribution, a public polynomial $h \in R$ is given alongside a syndrome $u = e_1 + e_2 h \bmod P(X)$, where $E \xleftarrow{\$} \mathrm{Gr}_{\mathbb{F}_2}(r, K)$ is a uniform r-dimensional support and $e_1, e_2 \xleftarrow{\$} E^n$ are sampled uniformly among polynomials of full support $\mathrm{Supp}(e_1) = \mathrm{Supp}(e_2) = E$. An Ideal-LRPC$(m, n, d)$ public key replaces uniform $h \in R$ with $h = x^{-1} y \bmod P(X)$, where $F \xleftarrow{\$} \mathrm{Gr}_{\mathbb{F}_2}(d, K)$ is a secret d-dimensional support and $x, y \xleftarrow{\$} F^n$ with $x \in R^\times$.

For any two $\mathbb{F}_2$-subspaces $F, E \subset K$ of dimensions d and r, their product subspace $F \cdot E \coloneqq \langle fe : f \in F, e \in E \rangle_{\mathbb{F}_2} \subseteq K$ has dimension at most rd. When $rd < m$, multiplying the syndrome $u = e_1 + e_2 h$ by the secret polynomial $x \in F^n$ yields $s = xu \equiv xe_1 + ye_2 \pmod{P(X)}$ whose coefficients lie entirely in $F \cdot E$, enabling decoding by subspace intersection [15].

2.3 Support-Minors Modeling and Moore Matrices

Our cryptanalysis builds upon and extends three algebraic tools from rank-metric cryptanalysis and linear algebra:

Support-Minors and MaxMinors Linearization [9, 10]. In a generic $[N, k]$ linear code over $K = \mathbb{F}_{2^m}$ with parity-check matrix $H_{\mathrm{pub}} \in K^{(N-k) \times N}$, a rank-$r$ error vector $e = Cb^\top \in K^N$ factors through a basis $b \in K^r$ of E and a binary coordinate matrix $C \in \mathbb{F}_2^{N \times r}$ of rank r. Bardet et al. [9, 10] observed that for any syndrome equation, augmenting $C^\top$ with a syndrome-combination row produces an $(r+1) \times N$ matrix of rank r whose $(r+1) \times (r+1)$ maximal minors vanish. Expanding these determinants along the augmented row expresses every equation as a linear combination of the $\binom{N}{r}$ maximal minors (Plücker coordinates) of C. When applied directly to an Ideal-LRPC instance over $R = K[X]/(P(X))$ of length $N = 2n$, this modeling requires $\binom{2n-p}{r}$ minor columns after puncturing p positions.

Table 2: Summary of the three Ideal-LRPC KEM constructions over $R = \mathbb{F}_{2^m}[X]/(P(X))$ with hash function $H = \mathsf{SHA512}$. Here $x, y \in F^n$ have secret support $\dim_{\mathbb{F}_2} F = d$, and $e_1, e_2 \in E^n$ have ephemeral error support $\dim_{\mathbb{F}_2} E = r$.

Scheme (R1 / R2)	**Goal**	pk	**Ciphertext** ct **and Shared Secret** ss	$\log_2$ DFR
LAKE / ROLLO-I	CPA	$x^{-1}y$	$e_1 + e_2 h$; $ss = H(\mathrm{RREF}(E))$	$-28..-36$
LOCKER / ROLLO-II	CCA2	$x^{-1}y$	(u, v, d_{tag}); $ss = H(\mu \parallel u \parallel v)$	$-64..-128$
Ouroboros / ROLLO-III	CPA	$(h, s_{\mathrm{pk}})^{\mathrm{a}}$	$(r_0{+}r_1 h,\ e_0{+}r_1 s_{\mathrm{pk}})$; $ss = H(\mathrm{RREF}(E))$	$-28..-39$

[a]In ROLLO-III, $h \xleftarrow{\$} R$ is expanded uniformly from a public seed, $s_{\mathrm{pk}} = w_0 + w_1 h \bmod P(X)$ has secret-key support $\dim_{\mathbb{F}_2} \mathrm{Supp}(w_0, w_1) = d = w \in \{5, 6, 7\}$ ($1 \in \mathrm{Supp}(w_0, w_1)$), and $r_0, r_1, e_0 \in E^n$ share the rank-r error support E with $r = w_r \in \{6, 8, 8\}$.

Moore Matrices and Subspace Annihilator Polynomials. For elements $\alpha_1, \ldots, \alpha_d$ in a characteristic-2 field L, the $d \times d$ Moore matrix is defined by $A \coloneqq (\alpha_k^{2^i})_{0 \le i < d,\, 1 \le k \le d}$. By Moore's determinant theorem, $\det(A) \neq 0$ if and only if $\alpha_1, \ldots, \alpha_d$ are linearly independent over $\mathbb{F}_2$. In that case, the d-dimensional $\mathbb{F}_2$-subspace $V_\alpha = \langle \alpha_1, \ldots, \alpha_d \rangle_{\mathbb{F}_2} \subset L$ is the root set of a unique monic 2-linearized annihilator polynomial of degree 2^d:

$$\mathcal{L}_\alpha(Z) \coloneqq \prod_{v \in V_\alpha} (Z + v) = Z^{2^d} + \sum_{j=0}^{d-1} c_j Z^{2^j} \in L[Z].$$

Principal Minor Assignment Problem [18, 16]. Given a matrix $M \in L^{d \times d}$ and a subset $Z \subseteq \{0, \ldots, d-1\}$, the principal minor $\Delta_Z(M) \coloneqq \det M[Z, Z]$ is the determinant of the $|Z| \times |Z|$ submatrix on row and column indices Z (with $\Delta_\emptyset(M) = 1$). Because $\det(D\tilde{M}D^{-1})[Z, Z] = \det \tilde{M}[Z, Z] = \det \tilde{M}^\top[Z, Z]$ for any invertible diagonal matrix $D = \mathrm{diag}(D_0, \ldots, D_{d-1}) \in (L^\times)^d$, the 2^d principal minors of M are invariant under both diagonal conjugation and transposition. Conversely, classical results on the Principal Minor Assignment Problem (PMAP) by Loewy [18] and Griffin and Tsatsomeros [16] establish that for a generic matrix M with nonzero off-diagonal entries, its principal minors of orders $1, 2$, and 3 uniquely determine M up to diagonal conjugation D and transposition $\tilde{M} \leftrightarrow \tilde{M}^\top$. In general, the $(d-1)$-dimensional diagonal gauge D cannot be recovered from the principal minors of M alone; in Section 6.1, we show that when $M = BA^{-1}$ links two Moore matrices A and B, the Frobenius shift structure of A and B uniquely determines D in closed form.

3 Specification of LOCKER and ROLLO

3.1 Key Generation, Encapsulation, and Decapsulation

Table 2 summarizes the three Ideal-LRPC KEM constructions over $R = K[X]/(P(X))$, Figure 1 illustrates their algebraic workflow, and Algorithms 1 and 2 specify their complete procedures [3, 4, 5].

While $e_1, e_2 \in E^n$ each have rank r, multiplying e_2 by the public polynomial $h \in R$ mixes elements across K, so the public syndrome $u = e_1 + e_2 h \bmod P(X)$ has full rank $\mathrm{rank}_{\mathbb{F}_2}(u) = m$. To decapsulate u, the receiver multiplies by $x \in F^n$ ($xh \equiv y \pmod{P(X)}$):

$$s(X) \coloneqq x(X)\, u(X) \equiv x(X)\, e_1(X) + y(X)\, e_2(X) \pmod{P(X)}.$$

Every coefficient of $s(X)$ belongs to the product space $F \cdot E$, which has dimension at most $rd < m$ ($35 < 71$ in LOCKER-I). Since $E \subseteq f_i^{-1}(F \cdot E)$ for each basis element f_i of F, the intersection $\bigcap_{i=1}^{d} f_i^{-1}\,\mathrm{Supp}(s)$ recovers E whenever $\mathrm{Supp}(s) = F \cdot E$ and random subspaces of dimension rd have trivial excess intersection. In LOCKER and ROLLO-II, Step 2 of RSR enlarges

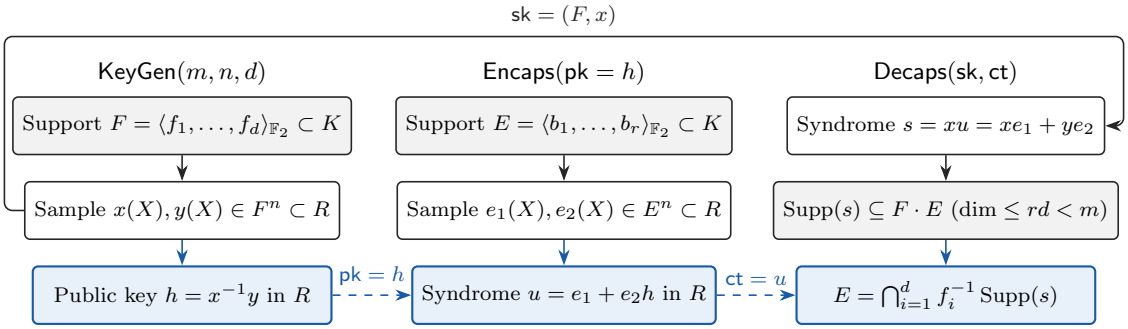

Figure 1: Architecture of Ideal-LRPC key encapsulation and decapsulation over $R = K[X]/(P(X))$. Multiplication by $h \in R$ scrambles $e_2 \in E^n$ to full rank $\mathrm{rank}_{\mathbb{F}_2}(u) = m$, whereas multiplying by $x \in F^n$ confines $\mathrm{Supp}(xu)$ to the product space $F \cdot E$ of dimension at most $rd < m$.

Algorithm 1: Key Generation (KeyGen) and Rank Support Recoverer (RSR)

KeyGen(m, n, d):

1. Sample $\sigma_{\mathrm{sk}} \xleftarrow{\$} \{0,1\}^{320}$ and expand a d-dimensional support $F = \langle f_1, \ldots, f_d \rangle_{\mathbb{F}_2} \subset K$ from $\mathsf{XOF}(\sigma_{\mathrm{sk}})$.
2. Sample full-rank $x(X), y(X) \in F^n \subset R$; restart at Step 1 if $x(X) \notin R^\times$.
3. $h(X) \leftarrow x(X)^{-1} y(X) \bmod P(X)$; **return** $\mathsf{pk} = h$, $\mathsf{sk} = (F, x, y, h)$.

RSR$(F = \langle f_1, \ldots, f_d \rangle,\ s \in R,\ r, \mathsf{expand} \in \{0,1\})$: ▷ $s = xu = xe_1 + ye_2 \in (F \cdot E)^n$

1. $S \leftarrow \mathrm{Supp}(s) \subseteq K$; $S_i \leftarrow f_i^{-1} S$ for $1 \le i \le d$.
2. **if** $\mathsf{expand} = 1$ **then for** $i = 1, \ldots, d-2$ **do** $U_i \leftarrow (S_i \cap S_{i+1}) + (S_{i+1} \cap S_{i+2}) + (S_i \cap S_{i+2})$; if $\dim_{\mathbb{F}_2}(S + F \cdot U_i) \le rd$, set $S \leftarrow S + F \cdot U_i$.
3. $E \leftarrow \bigcap_{i=1}^{d} f_i^{-1} S$; **return** $\mathrm{RREF}(E)$ if $\dim_{\mathbb{F}_2}(E) = r$ else $\perp$.

$S = \mathrm{Supp}(s)$ using pairwise intersections $f_i^{-1} S \cap f_{i+1}^{-1} S$ before taking the final intersection, reducing the decryption failure rate below 2^{-64} for IND-CCA2 security under the Fujisaki–Okamoto transform.

3.2 Evolution of Parameter Generations

In all 27 published parameter sets across the four families (listed in Table 5), both $g(T) \in \mathbb{F}_2[T]$ ($\deg g = m$) and $P(X) \in \mathbb{F}_2[X]$ ($\deg P = n$) are chosen as sparse irreducible binary polynomials (trinomials or pentanomials) with $\gcd(m, n) = 1$. In LOCKER-I $(m, n, r, d) = (71, 83, 5, 7)$, for example, $g(T) = T^{71} + T^6 + 1$ and $P(X) = X^{83} + X^7 + X^4 + X^2 + 1$; each coefficient $a_j \in K$ is serialized in $\lceil 71/8 \rceil = 9$ little-endian bytes, yielding $83 \times 9 = 747$ bytes per ring element. Across these families, the parameter regimes evolved from $m > 2^r$ in 2017 LOCKER ($m \in [71, 109]$, $r \in \{5, 6\}$, $2^r \in \{32, 64\}$) and 128/192-bit 2019 ROLLO ($m \in [79, 107]$, 2-IRSD rank in $\{5, 6\}$, with $m \ge 2^d = 64$ on homogeneous 2019 ROLLO-I-128) to the sub-threshold regime $m \le 2^r$ and $m < 2^d$ in 2020 ROLLO ($m \in [67, 97]$, $r \in \{7, 8, 9\}$, $2^r \in \{128, 256, 512\}$) and new2ROLLO-I [9] ($m \in \{73, 89, 103\}$, $r \in \{7, 8, 9\}$).

Algorithm 2: Encapsulation (Encaps) and Decapsulation (Decaps)

Encaps($\mathsf{pk} = h$):

1. *CPA (*ROLLO-I*):* Sample $E \subset K$ ($\dim_{\mathbb{F}_2} E = r$) and full-rank $e_1, e_2 \xleftarrow{\$} E^n$; set $u \leftarrow e_1 + e_2 h \bmod P(X)$; **return** $\mathsf{ct} = u, \quad ss = \mathsf{SHA512}(\mathrm{RREF}(E))$.
2. *CCA2 (*LOCKER / ROLLO-II*):* Sample $\mu \xleftarrow{\$} \{0,1\}^{512}$, set $\theta \leftarrow \mathsf{XOF}(\mu)$, and expand $E \subset K$ ($\dim_{\mathbb{F}_2} E = r$) and full-rank $e_1, e_2 \in E^n$ from $\mathsf{XOF}(\theta)$.
3. $u \leftarrow e_1 + e_2 h \bmod P(X); \quad v \leftarrow \mu \oplus \mathsf{SHA512}(\mathrm{RREF}(E)); \quad d_{\mathrm{tag}} \leftarrow \mathsf{SHA512}(\mu)$.
4. **return** $\mathsf{ct} = (u, v, d_{\mathrm{tag}}), \quad ss = \mathsf{SHA512}(\mu \parallel u \parallel v)$.

Decaps($\mathsf{sk} = (F, x, y, h)$, ct):

1. Verify canonical byte encoding of u; compute $s \leftarrow x \cdot u \bmod P(X)$.
2. *CPA:* $E' \leftarrow \mathsf{RSR}(F, s, r, 0)$; **return** $\mathsf{SHA512}(E')$ if $E' \neq \perp$ else $\perp$.
3. *CCA2:* $E' \leftarrow \mathsf{RSR}(F, s, r, 1)$; $\mu' \leftarrow v \oplus \mathsf{SHA512}(E')$ (0^{512} if $E' = \perp$).
4. Re-expand (E'', e_1', e_2') from $\mathsf{XOF}(\mathsf{XOF}(\mu'))$; set $u' \leftarrow e_1' + e_2' h \bmod P(X)$, $v' \leftarrow \mu' \oplus \mathsf{SHA512}(E')$, $d'_{\mathrm{tag}} \leftarrow \mathsf{SHA512}(\mu')$. **return** $\mathsf{SHA512}(\mu' \parallel u \parallel v)$ if $(u', v', d'_{\mathrm{tag}}) = (u, v, d_{\mathrm{tag}})$ else $\perp$.

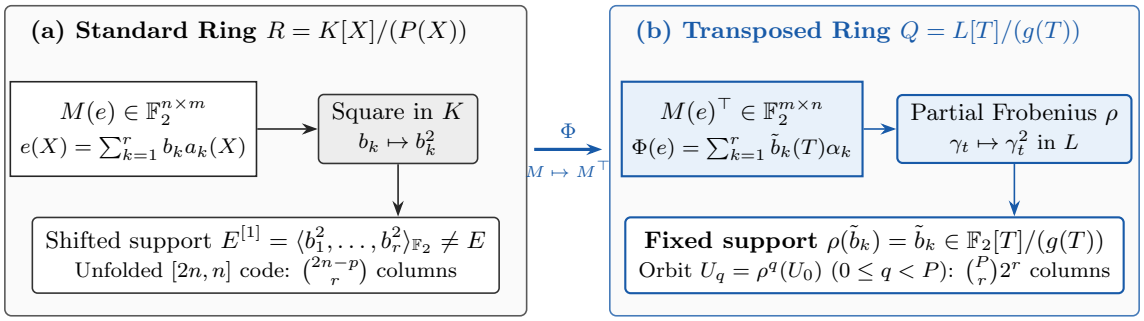

Figure 2: Comparison between (a) coefficient squaring in $R = K[X]/(P(X))$, which moves the unknown support $E \subset K$ to $E^{[1]} \neq E$, and (b) our transposed representation in $Q = L[T]/(g(T))$, where the partial Frobenius ρ squares scalars in $L = \mathbb{F}_2[X]/(P(X))$ while fixing $\Phi(E) \subset \mathbb{F}_2[T]/(g(T))$ pointwise.

4 Transposed Algebra and Partial Frobenius

4.1 Coefficient Matrix Transposition

Assume $P(X) \in \mathbb{F}_2[X]$ is irreducible of degree n, so that the binary quotient ring $L \coloneqq \mathbb{F}_2[X]/(P(X)) \cong \mathbb{F}_{2^n}$ is a field, and define the polynomial quotient ring $Q \coloneqq L[T]/(g(T)) \cong L \otimes_{\mathbb{F}_2} K$ (Section 5.5 relaxes irreducibility of P and coprimality of m and n). Transposing the $n \times m$ binary coefficient matrix $M(a) \in \mathbb{F}_2^{n\times m}$ into $M(a)^\top \in \mathbb{F}_2^{m\times n}$ exchanges the roles of X and T:

$$\begin{array}{ccc} R = K[X]/(P(X)) & \xrightarrow{\Phi:\, M(a)\mapsto M(a)^\top} & Q = L[T]/(g(T)) \\ b_k(T) \in K,\ a_k(X) \in \mathbb{F}_2[X]/(P(X)) & \longmapsto & \tilde{b}_k(T) \in \mathbb{F}_2[T]/(g(T)),\ \alpha_k \in L \end{array}$$

While matrix transposition of rank-metric codewords [13] and the tensor-product symmetry $K \otimes_{\mathbb{F}_2} L \cong L \otimes_{\mathbb{F}_2} K$ are classical, their cryptographic consequence for Ideal-LRPC codes over an irreducible modulus $P(X)$ has been overlooked: in $Q = L[T]/(g(T))$, the secret support elements $\tilde{b}_k(T) \in \mathbb{F}_2[T]/(g(T))$ have binary coefficients, whereas the ring coordinates $\alpha_k \in L$ lie in the extension field $L \cong \mathbb{F}_{2^n}$.

Table 3: Summary of ciphertext support-recovery variants over $L = \mathbb{F}_2[X]/(P(X))$, where $\nu_L = \max(1, \binom{P}{r}2^r - \binom{P-1}{r}m)$ denotes the Stage 1 L-kernel dimension.

Variant	**Threshold**	**Matrix Dimension Over L**	**Target Regime**
Schur (Sec. 5.2)	$m > 2^r,\ P = P_2^*$	$\binom{P-1}{r}(m-2^r) \times \binom{P-1}{r-1}2^r$	$r \le 5$ dense Schur
Overdet. (Sec. 5.3)	$m > 2^r,\ P = P_1^*$	$\binom{P-1}{r}m \times \binom{P}{r}2^r$ ($\nu_L = 1$)[a]	Single-stage (L only)
Sparse Krylov (Sec. 5.4)	$m > 2^r,\ P = P_2^*$	$\binom{P-1}{r}m \times \binom{P}{r}2^r$ ($w = (r+1)2^r$)	$r = 6$ sparse Lanczos
Projection (Sec. 5.5)	$\deg P_1 \ge P_2^*$	$\binom{P-1}{r}(m-2^r) \times \binom{P-1}{r-1}2^r$ over L_1	$X^n - 1$, $\gcd(m,n) > 1$

[a]Reduces to $\binom{P-1}{r}(m-2^r) \times \binom{P-1}{r-1}2^r$ with $\nu_L = 1$ if local Schur elimination is applied before solving.

4.2 Support Invariance Under Partial Frobenius

Figure 2 illustrates how the transposed representation isolates the unknown support inside the fixed subring of the partial Frobenius automorphism ρ.

Lemma 2. *For $a = \sum_{j=0}^{n-1}(\sum_{t=0}^{m-1}\mu_{j,t}T^t)X^j \in R$, the transpose map*

$$\Phi(a) \coloneqq \sum_{t=0}^{m-1}\left(\sum_{j=0}^{n-1}\mu_{j,t}X^j\right)T^t \in Q = L[T]/(g(T))$$

is an $\mathbb{F}_2$-algebra isomorphism, and $\rho : Q \to Q$ defined by $\rho(\sum_{t=0}^{m-1}\gamma_t T^t) \coloneqq \sum_{t=0}^{m-1}\gamma_t^2 T^t$ ($\gamma_t \in L$) is a ring automorphism of order n with fixed subring $Q^\rho = \Phi(K) = \mathbb{F}_2[T]/(g(T))$. For any r-dimensional subspace $E = \langle b_1, \dots, b_r\rangle_{\mathbb{F}_2} \subset K$:

1. *$W \coloneqq \mathrm{span}_L(\Phi(E)) \subset Q$ is a free L-submodule of rank r satisfying $W \cap \Phi(K) = \Phi(E)$.*
2. *Setting $U_0 = \Phi(u)$, $H_0 = \Phi(h)$, $\tilde{b}_k = \Phi(b_k) \in Q^\rho$, and $\alpha_k = \Phi(a_k), \beta_k = \Phi(c_k) \in L$ for $e_1 = \sum_{k=1}^r b_k a_k$ and $e_2 = \sum_{k=1}^r b_k c_k$, applying ρ^q ($q \ge 0$) to $u = e_1 + e_2 h$ yields*

$$U_q(T) = \sum_{k=1}^{r}\tilde{b}_k(T)\left(\alpha_k^{2^q} + H_q(T)\,\beta_k^{2^q}\right) \quad \text{in } Q, \qquad U_q = \rho^q(U_0),\ H_q = \rho^q(H_0). \tag{2}$$

Proof. Both R and Q identify canonically with $\mathbb{F}_2[X,T]/(P(X), g(T))$; Φ exchanges the order of summation and is therefore a ring isomorphism. Because $\mathrm{char}\, L = 2$ and $g(T)$ has coefficients in $\mathbb{F}_2 = L^{\sigma_L}$, squaring L-coefficients respects addition, multiplication, and reduction modulo $g(T)$, with fixed subring $\mathbb{F}_2[T]/(g(T)) = \Phi(K)$. In $Q = L \otimes_{\mathbb{F}_2} \Phi(K)$, $\mathbb{F}_2$-linearly independent elements $\tilde{b}_1, \dots, \tilde{b}_r \in \Phi(K)$ remain L-linearly independent, and expanding $\sum_{k=1}^r \lambda_k \tilde{b}_k \in \Phi(K)$ over an $\mathbb{F}_2$-basis of L forces $\lambda_k \in \mathbb{F}_2$, proving $W \cap \Phi(K) = \Phi(E)$. Applying ρ^q to $U_0 = \sum_{k=1}^r \tilde{b}_k(\alpha_k + H_0\beta_k)$ fixes $\tilde{b}_k$ pointwise and squares $\alpha_k, \beta_k \in L$ q times, yielding (2). □

5 Ciphertext Support Recovery

Given a public key h and ciphertext syndrome $u = e_1 + e_2 h \bmod P(X)$ with error support $\dim_{\mathbb{F}_2} E = r$, we fix a window size $P \in \{r+1, \dots, n\}$ and evaluate (2) for $0 \le q < P$. Table 3 summarizes the four ciphertext support-recovery variants developed in this section.

5.1 Ring-Valued Support-Minors Linearization

Following the Support-Minors cofactor strategy of Bardet et al. [9, 10], we eliminate the unknown basis elements $\tilde{b}_1, \dots, \tilde{b}_r \in Q^\rho$ by taking $(r+1) \times (r+1)$ determinants, but we carry out the expansion inside the commutative polynomial ring $Q = L[T]/(g(T))$ across the P Frobenius

conjugates rather than over an unfolded length-$2n$ code. Write $Z_{q,k}(T) \coloneqq \alpha_k^{2^q} + H_q(T)\beta_k^{2^q} \in Q$ and collect the $2P$ scalar columns in L^r into the coordinate matrix

$$G \coloneqq \begin{pmatrix} A_0 & B_0 & \cdots & A_{P-1} & B_{P-1} \end{pmatrix} \in L^{r\times 2P}, \qquad A_{q,k} = \alpha_k^{2^q}, \quad B_{q,k} = \beta_k^{2^q}.$$

For any $(r+1)$-subset $S' \subseteq \{0,\dots,P-1\}$, the $(r+1)\times(r+1)$ matrix $M_{S'} = [U_q \mid Z_{q,1}\cdots Z_{q,r}]_{q\in S'}$ over Q satisfies $M_{S'}(1,\tilde{b}_1,\dots,\tilde{b}_r)^\top = 0$, so $\det_Q(M_{S'}) = 0$. Expanding $\det_Q(M_{S'})$ along column 0 in characteristic 2 (where $+1 = -1$) gives

$$\sum_{a\in S'} U_a(T) \det_Q\big[A_s^\top + H_s(T)B_s^\top\big]_{s\in S'\setminus\{a\}} = 0 \quad \text{in } Q.$$

By multilinearity of the determinant in each of the r rows $s_1 < \cdots < s_r$ of $S = S'\setminus\{a\}$, choosing either $A_{s_i}^\top$ ($\mu_i = 0$) or $H_{s_i}(T)B_{s_i}^\top$ ($\mu_i = 1$) in row i expands this $r\times r$ cofactor in Q into 2^r terms:

$$E_{S'} \coloneqq \sum_{a\in S'} U_a(T)\,\gamma_{S'\setminus\{a\}}(T) = 0 \quad \text{in } Q, \qquad \gamma_S(T) \coloneqq \sum_{\mu\in\{0,1\}^r} p_{S,\mu} \prod_{\substack{i=1\\ \mu_i=1}}^{r} H_{s_i}(T), \tag{3}$$

where $p_{S,\mu} \coloneqq \det_L G[:,(2s_i+\mu_i)_{i=1}^r] \in L$ are the $N_{\mathrm{col}} = \binom{P}{r}2^r$ pair-transversal minors of G selecting one column from each conjugate pair $\{A_{s_i}, B_{s_i}\}$ ($s_i \in S$). Extracting the m coefficients of $1, T, \dots, T^{m-1}$ in (3) yields m homogeneous L-linear equations per subset S'.

The next lemma lifts the standard MaxMinors pivot-syzygy reduction [9, 10] from a field to the commutative ring $Q = L[T]/(g(T))$.

Lemma 3. *If $U_0 \in Q^\times$, every equation $E_{S''}$ with $0 \notin S'' \subseteq \{1,\dots,P-1\}$ ($|S''| = r+1$) is a Q-linear combination of $\{E_{\{0\}\cup S} : S \subseteq \{1,\dots,P-1\}, |S| = r\}$. Retaining only the $\binom{P-1}{r}$ subsets containing 0 yields $N_{row} = \binom{P-1}{r}m$ scalar L-equations without changing the right kernel.*

Proof. For any r-subset $S \subseteq \{1,\dots,P-1\}$, $E_{\{0\}\cup S} = 0$ rearranges in characteristic 2 to $U_0\gamma_S = \sum_{x\in S} U_x\gamma_{\{0\}\cup(S\setminus\{x\})}$. Multiplying $E_{S''}$ by U_0 and substituting $S = S''\setminus\{a\}$ gives

$$U_0 E_{S''} = \sum_{a\in S''} U_a(U_0\gamma_{S''\setminus\{a\}}) = \sum_{a\in S''}\sum_{x\in S''\setminus\{a\}} U_aU_x\,\gamma_{\{0\}\cup(S''\setminus\{a,x\})} \equiv 0 \quad \text{in } Q,$$

since each unordered pair $\{a,x\} \subset S''$ appears twice and cancels modulo 2. Because $U_0 \in Q^\times$, $E_{S''} = 0$. □

5.2 Local Schur Elimination and Frobenius Threshold

Partition the $\binom{P}{r}$ minor blocks of width 2^r into the $\binom{P-1}{r-1}$ core blocks with $0 \in S$ ($N'_{\mathrm{col}} = \binom{P-1}{r-1}2^r$ columns) and the $K_{\mathrm{blk}} = \binom{P-1}{r}$ non-pivot blocks with $0 \notin S$. In the 0-anchored equation $E_{\{0\}\cup S_i} = U_0\gamma_{S_i} + \sum_{x\in S_i} U_x\gamma_{\{0\}\cup(S_i\setminus\{x\})}$, every summand except $U_0\gamma_{S_i}$ contains 0 in its index set. Consequently, unlike systematic MaxMinors over a field where each non-pivot subset contributes a single scalar column, the 2^r columns of $S_i \subseteq \{1,\dots,P-1\}$ appear exclusively in the i-th m-row block $B_i \in L^{m\times 2^r}$:

$$\mathcal{M} = \begin{pmatrix} C_1 & B_1 & 0 & \cdots & 0 \\ C_2 & 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C_{K_{\mathrm{blk}}} & 0 & 0 & \cdots & B_{K_{\mathrm{blk}}} \end{pmatrix} \in L^{N_{\mathrm{row}}\times N_{\mathrm{col}}}, \qquad C_i \in L^{m\times N'_{\mathrm{col}}}, \quad B_i \in L^{m\times 2^r}. \tag{4}$$

Figure 3 illustrates the block-staircase structure of $\mathcal{M}$ and the resulting two-stage recovery pipeline.

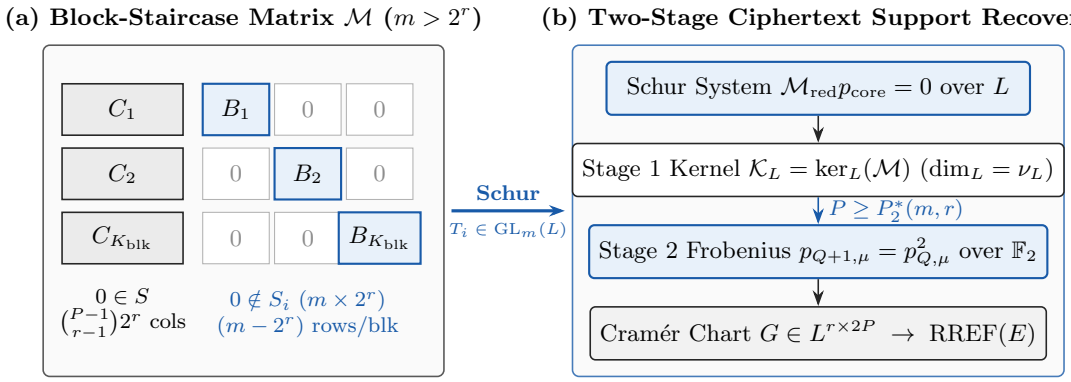

Figure 3: Structure of the 0-anchored Support-Minors system in $Q = L[T]/(g(T))$: (a) each non-pivot subset $S_i \subseteq \{1, \ldots, P-1\}$ forms an isolated $m \times 2^r$ block B_i that is eliminated locally with zero fill-in whenever $m > 2^r$; (b) the resulting two-stage solver extracts $\ker_L(\mathcal{M}_{\text{red}})$, enforces $p_{Q+1,\mu} = p_{Q,\mu}^2$ over $\mathbb{F}_2$, and reconstructs G and E.

Proposition 4. *Suppose $m > 2^r$ and $\operatorname{rank}_L(B_i) = 2^r$ for all $1 \leq i \leq K_{blk}$. Left-multiplying row block i by $T_i \in \mathrm{GL}_m(L)$ such that $T_i \begin{pmatrix} C_i & B_i \end{pmatrix} = \begin{pmatrix} \widetilde{C}_i & I_{2^r} \\ \mathcal{M}_{red,i} & 0 \end{pmatrix}$ eliminates $B_1, \ldots, B_{K_{blk}}$ locally with zero fill-in, yielding*

$$\mathcal{M}_{red} = \begin{pmatrix} \mathcal{M}_{red,1} \\ \vdots \\ \mathcal{M}_{red,K_{blk}} \end{pmatrix} \in L^{N'_{row} \times N'_{col}}, \qquad N'_{row} = \binom{P-1}{r}(m - 2^r), \quad N'_{col} = \binom{P-1}{r-1}2^r,$$

with $\dim_L \ker(\mathcal{M}_{red}) = \dim_L \ker(\mathcal{M})$ and $N'_{col} - N'_{row} = N_{col} - N_{row}$.

Proof. Applying $\operatorname{diag}(T_1, \ldots, T_{K_{\text{blk}}})$ to $\mathcal{M}p = 0$ decouples $p_{S_i} = \widetilde{C}_i p_{\text{core}}$ and leaves $\mathcal{M}_{\text{red}} p_{\text{core}} = 0$. By Pascal's identity $\binom{P}{r} - \binom{P-1}{r} = \binom{P-1}{r-1}$, we have $N'_{\text{col}} - N'_{\text{row}} = N_{\text{col}} - N_{\text{row}}$. □

When Stage 1 leaves kernel dimension $\nu_L = N_{\text{col}} - N_{\text{row}} > 1$ with basis $\{v^{(1)}, \ldots, v^{(\nu_L)}\} \subset L^{N_{\text{col}}}$, Stage 2 enforces the Frobenius shift relation $A_{q+1} = A_q^{[1]}, B_{q+1} = B_q^{[1]}$ on minors:

$$p_{Q+1,\mu} = (p_{Q,\mu})^2 \qquad \forall\, Q \subseteq \{0, \ldots, P-2\},\ |Q| = r,\ \mu \in \{0,1\}^r. \tag{5}$$

Writing $p = \sum_{f=1}^{\nu_L} \theta_f v^{(f)}$ with $\theta_f = \sum_{j=0}^{n-1} \vartheta_{f,j} X^j \in L$ ($\vartheta_{f,j} \in \mathbb{F}_2$) turns (5) into a homogeneous $\mathbb{F}_2$-linear system $\mathcal{F}\vartheta = 0$ in $\nu_L n$ binary variables.

Theorem 5. *On a Stage 1 kernel $\mathcal{K}_L = \ker_L(\mathcal{M})$ of rank $N_{row} = \binom{P-1}{r}m$, the Frobenius operator $\mathcal{F}|_{\mathcal{K}_L}$ satisfies $\binom{P-2}{r}mn$ $\mathbb{F}_2$-linear syzygies, so*

$$\operatorname{rank}_{\mathbb{F}_2}\left(\mathcal{F}\big|_{\mathcal{K}_L}\right) \leq n\left[\binom{P-1}{r}2^r - \binom{P-2}{r}m\right]. \tag{6}$$

Two-stage TSM *determines a unique solution ($\dim_{\mathbb{F}_2} \ker(\mathcal{F}|_{\mathcal{K}_L}) = 1$ when $\nu_L > 1$, or $\nu_L = 1$ up to $L^\times$) if and only if $m > 2^r$ and*

$$P \geq P_2^*(m, r) := \left\lceil \frac{mr - 2^r}{m - 2^r} \right\rceil \leq n, \tag{7}$$

with strict inequality $m(P-r) > 2^r(P-1)$ when requiring positive excess rank over $\mathbb{F}_2$.

Algorithm 3: Two-Stage Ciphertext Support Recovery ($m > 2^r$, $P = P_2^*(m, r) \le n$)

1. Compute $U_q = \rho^q(\Phi(u))$ and $H_q = \rho^q(\Phi(h))$ in $Q = L[T]/(g(T))$ for $0 \le q < P$.
2. For each r-subset $S_i \subseteq \{1, \dots, P-1\}$, form $\begin{pmatrix} C_i & B_i \end{pmatrix}$ from $E_{\{0\}\cup S_i}$ and eliminate B_i into $\mathcal{M}_{\mathrm{red},i}$.
3. Compute $\ker_L(\mathcal{M}_{\mathrm{red}})$ of dimension ν_L and back-substitute $p_{S_i} = \widetilde{C}_i p_{\mathrm{core}}$.
4. If $\nu_L > 1$, solve $p_{Q+1,\mu} + p_{Q,\mu}^2 = 0$ over $\mathbb{F}_2$ on $\ker_L(\mathcal{M})$ to obtain p.
5. Normalize a non-singular chart $[B_0 \cdots B_{r-1}] = I_r$ and reconstruct $G \in L^{r\times 2P}$ via Cramér minor ratios.
6. Solve $[G_{k,2q} + H_q G_{k,2q+1}]_{q\in I,\, 1\le k\le r} \cdot \tilde{b} = (U_q)_{q\in I}$ over Q ($|I| = r$); set $E \leftarrow \mathrm{RREF}(\mathrm{Supp}(\Phi^{-1}(\tilde{b})))$.
7. In CCA2 mode, set $\mu' = v \oplus \mathsf{SHA512}(E)$, verify $\mathsf{SHA512}(\mu') = d_{\mathrm{tag}}$, and **return** $\mathsf{SHA512}(\mu' \parallel u \parallel v)$.

Proof. For each of the $\binom{P-2}{r}$ subsets $S' \subseteq \{0, \dots, P-2\}$ containing 0 and any $p \in \mathcal{K}_L$, Lemma 3 gives $E_{S'+1}(p) = 0$ in addition to $\rho(E_{S'}(p)) = 0$. Subtracting the two identities yields

$$\sum_{a\in S'} U_{a+1}(T) \sum_{\mu\in\{0,1\}^r} (p_{Q_a+1,\mu} + p_{Q_a,\mu}^2) \prod_{\mu_i=1} H_{(Q_a)_i+1}(T) \equiv 0 \quad \text{in } Q \qquad (Q_a = S' \setminus \{a\}),$$

which imposes $\binom{P-2}{r}mn$ linear dependencies over $\mathbb{F}_2$ among the $\binom{P-1}{r}2^r n$ bit-components of $(p_{Q+1,\mu} + p_{Q,\mu}^2)$ and proves (6). Because (5) restricts $L^\times$-scaling to $\lambda^2 = \lambda$ ($\lambda = 1$), unique recovery requires $n[\binom{P-1}{r}2^r - \binom{P-2}{r}m] \ge n[\binom{P}{r}2^r - \binom{P-1}{r}m]$, which simplifies via Pascal's identity to $\binom{P-2}{r-1}m \ge \binom{P-1}{r-1}2^r$, or equivalently $m(P-r) \ge 2^r(P-1)$ and (7). □

Reconstructing G and E from Pair-Transversal Minors. Once the minor vector p is known, we adapt the chart-normalization procedure of [9, 10] to our pair-transversal minors $(p_{S,\mu})$. Choose a non-singular chart (for instance $B_0, \dots, B_{r-1}$, corresponding to $S_0 = \{0, \dots, r-1\}$ and $\mu_0 = 1^r$) and normalize G under its left $\mathrm{GL}_r(L)$-action so that $[B_0 \cdots B_{r-1}] = I_r$. Every column $c = 2q + \mu$ outside pairs $0, \dots, r-1$ ($q \ge r$) and every diagonal entry $A_{i,i}$ ($0 \le i < r$) is recovered by a single-column Cramér replacement in I_r:

$$G_{i,2q+\mu} = \frac{p_{\mathrm{chart}(i\leftarrow 2q+\mu)}}{p_{S_0,1^r}} \quad (q \ge r), \qquad A_{i,i} = \frac{p_{S_0,1^r\oplus e_i}}{p_{S_0,1^r}} \quad (0 \le i < r).$$

For off-diagonal entries $A_{i,k}$ ($k \ne i$, $0 \le i, k < r$), pick any external column $v = G[:, 2q+\mu]$ ($q \ge r$) with $v_i \ne 0$; replacing columns i and k of I_r by A_i and v gives a 2×2 determinant $p/p_{S_0,1^r} = A_{i,i}v_k + A_{i,k}v_i$, whence $A_{i,k} = (p/p_{S_0,1^r} + A_{i,i}v_k)/v_i$. Solving r independent rows of (2) over Q then yields $(\tilde{b}_1, \dots, \tilde{b}_r)$ and $E = \mathrm{RREF}(\mathrm{Supp}(\Phi^{-1}(\tilde{b})))$ (Algorithm 3).

5.3 Overdetermined Single-Stage Recovery

Corollary 6. *For $m > 2^r$, choosing $P \ge P_1^*(m, r) := \lceil mr/(m-2^r)\rceil \le n$ (or $mr/(m-2^r)+1$ when $(m-2^r) \mid mr$) gives $N_{row} \ge N_{col} - 1$ and $\nu_L = \dim_L \ker(\mathcal{M}_{red}) = 1$, recovering p up to $L^\times$-scaling in Stage 1 without forming the binary Frobenius matrix $\mathcal{F}$.*

On LOCKER-I ($m = 71, n = 83, r = 5$), setting $P = P_1^*(71, 5) = 10$ gives an unreduced $8{,}946 \times 8{,}064$ system ($4{,}914 \times 4{,}032$ after local Schur reduction) of rank $N_{\mathrm{col}} - 1$ ($\nu_L = 1$). On $r = 6, m = 107$ (LOCKER-III/VI), increasing P from $P_2^* = 14$ to $P_1^* = 15$ eliminates the Stage 2 binary matrix of 869–1,164 GiB altogether.

5.4 Sparse Krylov Solving

At $r = 6$, dense storage of the unreduced matrix $\mathcal{M}$ requires 565–863 GB of memory (97–508 GB after local Schur reduction). Retaining the unreduced matrix $\mathcal{M}$ in (4) preserves exact constant row weight for sparse Krylov solvers such as Wiedemann [23] and Block-Lanczos [19].

Proposition 7. *Every row of $\mathcal{M} \in L^{N_{row} \times N_{col}}$ contains at most $w = (r+1)2^r$ non-zero entries across the $r+1$ disjoint 2^r-column blocks $S' \setminus \{a\}$ $(a \in S')$. Compressed sparse row (CSR) storage uses $N_{row}w(4+8\lceil n/64\rceil)+8(N_{row}+1)$ bytes, and Block-Lanczos on $\mathcal{M}^\top\mathcal{M}$ followed by Stage 2 requires*

$$C_{CT}(m,n,r) = 4N_{col}N_{row}wn^2 + \frac{(\nu_L n)^{\omega_0}}{7} + \binom{P-1}{r} 2^r \nu_L n^2 \quad \text{gates} \quad (\omega_0 = \log_2 7), \tag{8}$$

at $2n^2$ two-input gates per $\mathbb{F}_{2^n}$ multiply-accumulate.

Proof. For fixed $S' = \{0\} \cup S$, the $r+1$ subsets $S' \setminus \{a\}$ $(a \in S')$ are distinct, so their 2^r-column blocks do not overlap. Block-Lanczos [19] with block width β performs $\lceil N_{\mathrm{col}}/\beta \rceil$ iterations of β-wide multiplications by $\mathcal{M}$ and $\mathcal{M}^\top$, totaling $2N_{\mathrm{col}}N_{\mathrm{row}}w$ scalar $\mathbb{F}_{2^n}$ multiply-adds ($4N_{\mathrm{col}}N_{\mathrm{row}}wn^2$ gates), plus $\mathbb{F}_2$ elimination on $\nu_L n$ columns. □

5.5 Reducible Quotients and Non-Coprime Degrees

Proposition 8. *1. If $P(X) \in \mathbb{F}_2[X]$ has an irreducible divisor $P_1(X) \mid P(X)$ of degree $n_1 \geq P_2^*(m,r)$ (in particular, the cyclotomic polynomial $\Phi_n(X)$ of degree $n-1$ inside $X^n - 1 = (X+1)\Phi_n(X)$ when $\mathrm{ord}_n(2) = n-1$), projecting to $K[X]/(P_1(X))$ and running TSM over $L_1 = \mathbb{F}_2[X]/(P_1(X))$ recovers E with probability at least $1 - 2^{-(n_1-r)}$. Running TSM on $K[X]/(X^n-1)$ directly fails because $\rho = \mathrm{id}$ on $K[X]/(X+1)$ produces identical rows in $M_{S'}$.*

2. If $P(X)$ is $\mathbb{F}_2$-irreducible and $k = \gcd(m,n) > 1$, then $Q \cong (\mathbb{F}_{2^{\mathrm{lcm}(m,n)}})^k$ contains zero divisors, yet $L = \mathbb{F}_{2^n}$ remains a field, $(L \otimes_{\mathbb{F}_2} E) \cap \Phi(K) = \Phi(E)$, and (3)–(5) hold over L and $\mathbb{F}_2$ whenever $U_0 \in Q^\times$ (which occurs with probability $(1 - 2^{-\mathrm{lcm}(m,n)})^k$).

Proof. In (1), the natural projection $\pi_1 : R \twoheadrightarrow K[X]/(P_1(X))$ is K-linear, so $\mathrm{Supp}(\pi_1(e_i)) \subseteq E$ and $\pi_1(e_2)$ has full rank r modulo $\Phi_n(X)$ whenever $(e_{2,j} + e_{2,n-1})_{0 \leq j < n-1}$ spans E. In (2), Laplace expansion holds over any commutative ring Q, while all entries of $\mathcal{M}$ and $\mathcal{F}$ lie in the fields L and $\mathbb{F}_2$. □

6 Public-Key Secret Recovery

In LOCKER, ROLLO-I, and ROLLO-II, the public key $h = x^{-1}y \bmod P(X)$ satisfies the homogeneous rank-d relation

$$x(X)\,h(X) + y(X) \equiv 0 \pmod{P(X)}, \qquad \mathrm{Supp}(x), \mathrm{Supp}(y) \subseteq F = \langle f_1, \ldots, f_d \rangle_{\mathbb{F}_2} \subset K.$$

Recovering any nonzero $K^\times$-multiple $(\gamma F, \gamma x, \gamma y)$ $(\gamma \in K^\times)$ yields a functionally equivalent secret key for decapsulation. (For ROLLO-III, where $h \xleftarrow{\$} R$ is uniform and $\mathsf{pk} = (h, s = x + hy \bmod P(X))$ is inhomogeneous of secret rank $d = w$, Algorithm 3 of Section 5 applies directly to (h,s) to recover (F,x,y).)

6.1 Principal Minors From Partial-Frobenius Products

Write $\Phi(x) = \sum_{k=1}^{d} \tilde{f}_k(T)\alpha_k$ and $\Phi(y) = \sum_{k=1}^{d} \tilde{f}_k(T)\beta_k$ ($\tilde{f}_k \in Q^\rho$, $\alpha_k, \beta_k \in L$). Applying ρ^q for $0 \le q < d$ gives d homogeneous equations in Q:

$$\sum_{k=1}^{d} \tilde{f}_k(T)\left(\alpha_k^{2^q} H_q(T) + \beta_k^{2^q}\right) = 0 \quad \text{in } Q \qquad (0 \le q < d). \tag{9}$$

Define the Moore matrices $A = (\alpha_k^{2^q})_{0\le q<d,\,1\le k\le d} \in \mathrm{GL}_d(L)$ and $B = (\beta_k^{2^q})_{0\le q<d,\,1\le k\le d} \in \mathrm{GL}_d(L)$ (both invertible because $\mathrm{rank}_{\mathbb{F}_2}(x) = \mathrm{rank}_{\mathbb{F}_2}(y) = d$), and set $M \coloneqq BA^{-1} \in \mathrm{GL}_d(L)$.

Theorem 9. *Let $C_H \in L^{m\times 2^d}$ be the matrix whose column $\mu \in \{0,1\}^d$ holds the m T-coefficients of $\prod_{q:\,\mu_q=1} H_q(T) \in Q$. Every valid keypair (x, y) defines a right kernel vector $p \in \ker_L(C_H)$ with $p_{1\ldots1} = \det(A) \neq 0$ and*

$$\frac{p_\mu}{p_{1\ldots1}} = \Delta_{Z(\mu)}(M) \coloneqq \det M[Z(\mu), Z(\mu)], \qquad Z(\mu) \coloneqq \{0 \le q < d : \mu_q = 0\}.$$

When $m \ge 2^d$, C_H has generic rank $2^d - 1$, so one $m \times 2^d$ elimination over L yields all 2^d principal minors of M.

Proof. Since $\tilde{f}_1, \ldots, \tilde{f}_d$ are L-linearly independent, (9) implies $\det_Q[\alpha_k^{2^q} H_q(T) + \beta_k^{2^q}] = 0$. Expanding row q into $\mu_q = 1$ ($\alpha_k^{2^q} H_q$) and $\mu_q = 0$ ($\beta_k^{2^q}$) gives $C_H p = 0$, where $p_\mu = \det N_\mu$ takes row q from A if $\mu_q = 1$ and from $B = MA$ if $\mu_q = 0$. Right-multiplying N_μ by A^{-1} places unit rows $e_q^\top$ at $q \notin Z(\mu)$ and rows of M at $q \in Z(\mu)$, giving $\det(N_\mu A^{-1}) = \det M[Z(\mu), Z(\mu)]$. □

6.2 Closed-Form Moore-Matrix Gauge Recursion

Once all 2^d principal minors $\Delta_Z(M)$ are extracted from $\ker_L(C_H)$, the classical PMAP reduction [18, 16] reconstructs a representative $\tilde{M}$ up to diagonal conjugation $M = D\tilde{M}D^{-1}$ ($D = \mathrm{diag}(D_0, \ldots, D_{d-1}) \in (L^\times)^d$) and transposition $\tilde{M} \leftrightarrow \tilde{M}^\top$. Imposing the row-0 gauge $\tilde{M}_{0,j} = 1$ ($1 \le j < d$) immediately gives the diagonal $\tilde{M}_{i,i} = \Delta_{\{i\}}$, the 2-cycle products $\pi_{i,j} \coloneqq M_{i,j}M_{j,i} = \Delta_{\{i\}}\Delta_{\{j\}} + \Delta_{\{i,j\}}$, and column 0 as $\tilde{M}_{j,0} = \pi_{0,j}$. Expanding any 3×3 principal minor $\Delta_{\{i,j,k\}}$ isolates the 3-cycle sum

$$\tilde{M}_{i,j}\tilde{M}_{j,k}\tilde{M}_{k,i} + \tilde{M}_{i,k}\tilde{M}_{k,j}\tilde{M}_{j,i} = T_{i,j,k} \coloneqq \Delta_{\{i,j,k\}} + \Delta_{\{i\}}\Delta_{\{j\}}\Delta_{\{k\}} + \Delta_{\{i\}}\pi_{j,k} + \Delta_{\{j\}}\pi_{i,k} + \Delta_{\{k\}}\pi_{i,j}.$$

Setting $(i, j, k) = (0, 1, j)$ ($2 \le j < d$) with $\tilde{M}_{0,1} = \tilde{M}_{0,j} = 1$ and $\tilde{M}_{j,1} = \pi_{1,j}/\tilde{M}_{1,j}$ yields $d - 2$ univariate quadratics $\pi_{0,j}\tilde{M}_{1,j}^2 + T_{0,1,j}\tilde{M}_{1,j} + \pi_{0,1}\pi_{1,j} = 0$ over L (solved via half-traces for odd n). Once row 1 and column 1 are fixed, $(T_{0,i,j}, T_{1,i,j})$ form a 2×2 linear system in $(\tilde{M}_{i,j}, \tilde{M}_{j,i})$ for every $2 \le i < j < d$, leaving at most two consistent candidates $\{\tilde{M}, \tilde{M}^\top\}$.

In a general PMAP instance, the diagonal gauge $D \in (L^\times)^d$ cannot be recovered from principal minors alone. Theorem 10 resolves this gauge ambiguity in closed form without searching $(L^\times)^{d-1}$ by exploiting the Frobenius row-shift structure of the Moore matrices A and B.

Theorem 10. *For Moore matrices $A_{i,k} = \alpha_k^{2^i}$ and $B_{i,k} = \beta_k^{2^i} = (MA)_{i,k}$ with $M = D\tilde{M}D^{-1}$ and $\tilde{M}_{0,j} = 1$ ($j \ge 1$), rescaling $(x, y) \mapsto (\delta x, \delta y)$ ($\delta \in L^\times$) fixes $D_0 = D_1 = 1$, and $D_2, \ldots, D_{d-1}$ satisfy*

$$D_{i+1} = D_i^2 \cdot \frac{\tilde{M}_{1,0}\,\tilde{M}_{i,d-1}^2}{\tilde{M}_{0,d-1}^2\,\tilde{M}_{i+1,0}} \qquad (1 \le i \le d-2). \tag{10}$$

The secret subspace $\langle \alpha_1, \ldots, \alpha_d \rangle_{\mathbb{F}_2} \subset L$ equals $\ker_{\mathbb{F}_2}(\mathcal{L}_\alpha)$ for

$$\mathcal{L}_\alpha(Z) = Z^{2^d} + \sum_{j=1}^{d-1} \frac{M_{0,j-1}^2 + M_{1,j}}{M_{0,d-1}^2} Z^{2^j} + \frac{M_{1,0}}{M_{0,d-1}^2} Z, \tag{11}$$

with total gate complexity $C_{PK}(m, n, d) = (2^d - d - 1) \cdot 2m^2n^2 + m \cdot 2^{2d}n^2 + \frac{1}{2}d^2m^3n$.

Algorithm 4: Direct Public-Key Secret Recovery ($m \geq 2^d$)

1. Compute $H_q = \rho^q(\Phi(h))$ $(0 \leq q < d)$ and form $C_H \in L^{m\times 2^d}$ with columns $\prod_{\mu_q=1} H_q(T)$.
2. Find $p \in \ker_L(C_H) \setminus \{0\}$ and normalize $\Delta_{Z(\mu)} \leftarrow p_\mu / p_{1\ldots1}$ for all $\mu \in \{0,1\}^d$.
3. Reconstruct $\tilde{M}$ ($\tilde{M}_{0,j} = 1$) from the $d-2$ quadratics on $(0,1,j)$ and 2×2 linear systems on $(0,i,j),(1,i,j)$.
4. For $\hat{M} \in \{\tilde{M}, \tilde{M}^\top\}$ (re-gauged to $\hat{M}_{0,j} = 1$), compute D via (10), $M = D\hat{M}D^{-1}$, $\langle \alpha_1, \ldots, \alpha_d \rangle_{\mathbb{F}_2} = \ker_{\mathbb{F}_2}(\mathcal{L}_\alpha)$ via (11), and $\beta = M_{0,\cdot}A$; solve $\sum_{k=1}^{d} \tilde{f}_k(T)(\alpha_k H_0(T) + \beta_k) = 0$ over $\mathbb{F}_2$ and **return** $\Phi^{-1}(\tilde{f}, \Phi(x), \Phi(y))$.

Proof. Squaring row i of $B = MA$ $(0 \leq i \leq d-2)$ gives $\beta_k^{2^{i+1}} = M_{i,d-1}^2 \alpha_k^{2^d} + \sum_{j=1}^{d-1} M_{i,j-1}^2 \alpha_k^{2^j}$, whereas row $i+1$ of $B = MA$ gives $\beta_k^{2^{i+1}} = \sum_{j=0}^{d-1} M_{i+1,j} \alpha_k^{2^j}$. Subtracting the two expressions shows that

$$\mathcal{L}^{(i)}(Z) \coloneqq Z^{2^d} + \sum_{j=1}^{d-1} \frac{M_{i,j-1}^2 + M_{i+1,j}}{M_{i,d-1}^2} Z^{2^j} + \frac{M_{i+1,0}}{M_{i,d-1}^2} Z$$

vanishes on $V_\alpha = \langle \alpha_1, \ldots, \alpha_d \rangle_{\mathbb{F}_2}$ for every $0 \leq i \leq d-2$ ($M_{i,d-1} \neq 0$ since $|V_\alpha| = 2^d$). Because the monic degree-2^d annihilator $\prod_{v\in V_\alpha}(Z+v)$ is unique, $\mathcal{L}^{(i)} = \mathcal{L}^{(0)}$ for all i, so $M_{i+1,0}/M_{i,d-1}^2 = M_{1,0}/M_{0,d-1}^2$. Rescaling $(\alpha_k, \beta_k) \mapsto (\delta\alpha_k, \delta\beta_k)$ maps $D_i \mapsto \delta^{2^i-1} D_i$, so $\delta = D_1^{-1}$ sets $D_0 = D_1 = 1$. Substituting $M_{i,j} = (D_i/D_j)\tilde{M}_{i,j}$ gives

$$\frac{(D_{i+1}/D_0)\,\tilde{M}_{i+1,0}}{(D_i/D_{d-1})^2\,\tilde{M}_{i,d-1}^2} = \frac{(D_1/D_0)\,\tilde{M}_{1,0}}{(D_0/D_{d-1})^2\,\tilde{M}_{0,d-1}^2},$$

where D_{d-1}^2 cancels from both denominators, yielding (10) and (11) (Algorithm 4). □

6.3 Transposed Subspace Search for Small Field Degrees

When $m < 2^d$, $C_H \in L^{m\times 2^d}$ has an underdetermined kernel of dimension at least $2^d - m > 1$. In this regime, the classical structural dual-LRPC subspace search [15, 17, 5] tests whether a candidate D-dimensional subspace $W \subset K$ $(d \leq D < m)$ contains a $K^\times$-multiple γF of the secret support by solving an $n(m-D) \times nD$ binary system in $O((m-D)D^2n^3)$ bit operations. Working over the field $L = \mathbb{F}_2[X]/(P(X))$ reduces each window test by a factor of n to an $(m-D)\times D$ matrix over L, while confirming that the exponential Grassmannian covering factor keeps $m < 2^d$ parameters secure.

Proposition 11. *Let $W \subset K$ be a D-dimensional $\mathbb{F}_2$-subspace $(d \leq D < m)$ extended to a basis $(w_0, \ldots, w_{m-1})$ of K with $\mathbb{F}_2$-dual basis $(\omega_0, \ldots, \omega_{m-1})$, and define $M_W \in L^{(m-D)\times D}$ by*

$$(M_W)_{k,j} \coloneqq \sum_{i=0}^{n-1} \langle \omega_{D+k},\, w_j h_i \rangle\, X^i \in L \qquad (0 \leq k < m-D,\ 0 \leq j < D).$$

Then $\ker_L(M_W) \cong \{x \in R : \mathrm{Supp}(x) \subseteq W \text{ and } \mathrm{Supp}(xh) \subseteq W\}$. One $O((m-D)D^2n^2)$ elimination over L tests whether $\gamma F \subseteq W$ for any $\gamma \in K^\times$, covering a multiplicative orbit of size $2^m - 1$; covering the full keyspace requires at least $\begin{bmatrix} m \\ d \end{bmatrix}_2 / \left((2^m-1)\begin{bmatrix} D \\ d \end{bmatrix}_2\right)$ subspaces ($\geq 2^{406.8}$ at $D = 8$, $\geq 2^{397.8}$ at $D = 9$, and $\geq 2^{205.0}$ at $D = 33$ on 2020 ROLLO-I-128).

Proof. Every $x \in R$ with $\mathrm{Supp}(x) \subseteq W$ writes uniquely as $x = \sum_{j=0}^{D-1} w_j \lambda_j(X)$ $(\lambda_j \in L)$, and its w_{D+k}-component after multiplying by $h \bmod P(X)$ equals $\sum_{j=0}^{D-1} (M_W)_{k,j} \lambda_j$. If $\gamma F \subseteq W$, then $\gamma x \in \ker_L(M_W) \setminus \{0\}$. On 2020 ROLLO-I-128 ($m = 67, n = 83, d = 8$) at $D = 33$, a single 34×33 window test over $\mathbb{F}_{2^{83}}$ executes in 0.29 s on one core, but requires $\geq 2^{205.0}$ windows to cover $\mathrm{Gr}_{\mathbb{F}_2}(8, K)$. □

Table 4: Exact binary nullity $\nu_{\mathbb{F}_2}(P)$ and quadratic Grassmannian Plücker relation deficit across representative $m \le 2^r$ parameter sets. Here $\binom{\nu_{\mathbb{F}_2}+1}{2}$ counts quadratic binary monomials on the kernel, and $N_{\mathrm{Pl}} = \binom{2P}{r-1}\binom{2P-r+1}{r+1}$ counts quadratic Plücker generators over L.

Parameter Set	(m, n, r)	P	$\nu_{\mathbb{F}_2}(P)$	$\binom{\nu_{\mathbb{F}_2}+1}{2}$	$N_{\mathbf{Pl}}$	$nN_{\mathbf{Pl}}$
2019 ROLLO-I-256	$(113, 67, 7)$	7	8.58×10^3	3.68×10^7	3.00×10^3	2.01×10^5
2019 ROLLO-II-256	$(127, 157, 7)$	9	4.23×10^5	8.95×10^{10}	9.19×10^6	1.44×10^9
2020 ROLLO-I-128	$(67, 83, 7)$	8	6.88×10^4	2.37×10^9	3.60×10^5	2.99×10^7
2020 ROLLO-I-192	$(79, 97, 8)$	8	2.48×10^4	3.08×10^8	1.14×10^4	1.11×10^6
2020 ROLLO-I-256	$(97, 113, 9)$	9	5.79×10^4	1.67×10^9	4.38×10^4	4.94×10^6
2020 ROLLO-II-128	$(83, 189, 7)$	8	1.54×10^5	1.18×10^{10}	3.60×10^5	6.81×10^7
2020 ROLLO-II-192	$(97, 193, 8)$	8	4.94×10^4	1.22×10^9	1.14×10^4	2.21×10^6
2020 ROLLO-II-256	$(97, 211, 8)$	9	4.12×10^5	8.47×10^{10}	1.75×10^6	3.69×10^8
new2ROLLO-I-128 [9]	$(73, 83, 7)$	8	6.83×10^4	2.33×10^9	3.60×10^5	2.99×10^7
new2ROLLO-I-256 [9]	$(103, 113, 9)$	9	5.79×10^4	1.67×10^9	4.38×10^4	4.94×10^6

7 Phase Transitions and Impossibility Barriers

7.1 Exact Binary Nullity Below Threshold

In the sub-threshold regime $m \le 2^r$ (2019 ROLLO-I/II-256, 2020 ROLLO, and new2ROLLO-I), neither increasing the number of Frobenius conjugates $P \le n$ nor adjoining quadratic Grassmannian Plücker relations closes the system.

Theorem 12. *Over $Q = L[T]/(g(T))$ with authentic conjugates $H_q = \rho^q(H_0)$ and $U_q = \rho^q(U_0)$:*

1. *Because ρ is an automorphism of Q fixing $\Phi(K)$ pointwise, equation q of (2) is the ρ^q-image of equation 0. The solution set $\{E' \in \mathrm{Gr}_{\mathbb{F}_2}(r, K) : U_0 \in W_{E'} + H_0 W_{E'}\}$ is independent of P, with expected spurious count $\begin{bmatrix} m \\ r \end{bmatrix}_2 2^{-n(m-2r)}$.*

2. *Eliminating shifted variables via $p_{Q+1,\mu} = p_{Q,\mu}^2$ leaves $2^r\binom{P-1}{r-1}n$ binary unknowns, while $\binom{P-2}{r}$ of the $\binom{P-1}{r}$ 0-anchored equations become redundant via $E_{S'+1} = \rho(E_{S'})$, leaving only the $\binom{P-2}{r-1}$ blocks with $\{0,1\} \subseteq S'$. For all $m \le 2^r$ and $r+1 \le P \le n$ ($d > r$), the exact $\mathbb{F}_2$-nullity is*

$$\nu_{\mathbb{F}_2}(P) = n\left[2^r\binom{P-1}{r-1} - m\binom{P-2}{r-1}\right], \tag{12}$$

which grows strictly with P.

Proof. Part (1) follows from bijectivity of ρ^q on Q and $\rho^q(\tilde{b}_k) = \tilde{b}_k$. For Part (2), under $p_{Q+1,\mu} = p_{Q,\mu}^2$, every r-subset $Q \subseteq \{0, \dots, P-1\}$ is determined by the unique shifted subset $Q - \min Q \ni 0$ when anchored from below, or equivalently $Q + (P - 1 - \max Q) \ni P-1$ within $\{0, \dots, P-1\}$; there are $\binom{P-1}{r-1}$ such orbits, giving $2^r\binom{P-1}{r-1}n$ independent binary variables. Among the $\binom{P-1}{r}$ 0-anchored equations $E_{S'}$, every subset $S' \subseteq \{0, \dots, P-2\}$ containing 0 ($\binom{P-2}{r}$ subsets) satisfies $\rho(E_{S'}) = E_{S'+1}$, which already lies in the Q-span of $\{E_{\{0\}\cup S}\}$ by Lemma 3. Subtracting these $\binom{P-2}{r}$ redundant Q-equations leaves $\binom{P-1}{r} - \binom{P-2}{r} = \binom{P-2}{r-1}$ independent Q-equations (mn bits each), yielding (12). When $m \le 2^r$, $\nu_{\mathbb{F}_2}(P+1) - \nu_{\mathbb{F}_2}(P) = n[2^r\binom{P-1}{r-2} - m\binom{P-2}{r-2}] > 0$. □

7.2 Quadratic Plücker Deficit and Scope Boundaries

Table 4 compares the number of quadratic binary monomials $\binom{\nu_{\mathbb{F}_2}(P)+1}{2}$ on this kernel against the total number of quadratic Plücker generators $N_{\mathrm{Pl}} = \binom{2P}{r-1}\binom{2P-r+1}{r+1}$ of $\mathrm{Gr}_L(r, 2P)$: quadratic

unknowns exceed L-relations by factors of 6.5×10^3 to 1.07×10^5, and exceed the bit bound nN_{Pl} by factors of 62 to 553. In addition, since $\rho^n = \mathrm{id}_Q$, solvability on the inhomogeneous public key of 2019 ROLLO-III-256 ($d = w = 7$, while $r = w_r = 8$ already satisfies $m < 2^r$) requires $P_2^*(m, d) \leq n$, which fails because $m = 131 > 2^7 = 128$ requires $P \geq 264 > n = 67$ for positive excess rank ($P_2^* = 263 > 67$). Hybrid sub-support guessing of an a-dimensional subspace $E_0 \subset E$ via quotient projection $K \twoheadrightarrow K/E_0$ [9, 11] also fails because the product $e_2 h$ uses field multiplication in K and E_0 is an $\mathbb{F}_2$-subspace rather than an ideal of K. Finally, unstructured rank-metric signature schemes such as RYDE [7] and Mirath [1] have no polynomial quotient modulus $P(X)$ and admit no $\Phi(K)$-fixing automorphism ρ.

8 Complexity Ledger and Experimental Evaluation

8.1 Gate Complexity Across All Twenty-Seven Sets

Table 5 evaluates all 27 published parameter sets (24 official NIST sets and 3 new2ROLLO-I sets [9]) in $\log_2$ two-input gates against the minimum published complexity across MaxMinors (MM), Support-Minors (SM) [10, 14], and structural Dual-LRPC (DL) [5, §6.2], [22]. Our methods improve upon the best published complexities through 2026 on 14 of the 27 sets: all 9/9 Round 1 LOCKER sets by 10.3–23.1 bits, and 5/9 initial Round 2 ROLLO sets by 5.1–20.6 bits. Because the required conjugate count $P_2^*(m, r) = \lceil (mr - 2^r)/(m - 2^r) \rceil$ decreases as m increases at fixed r, the 192-bit sets LOCKER-II/VIII ($m = 101, P = 7$, unreduced size 606×672) require smaller matrices and solve faster than 128-bit LOCKER-I ($m = 71, P = 9$, unreduced size 3976×4032).

8.2 Experimental Verification and Runtime Benchmarks

Table 6 reports measured matrix dimensions, Stage 1 kernel nullities ν_L, memory footprints, and wall-clock runtimes from our C++17 and Python implementations. On LOCKER-I at $P = 9$, our 12-thread C++17 Schur-reduced solver constructs the 2184×2240 matrix in 0.35 s, extracts the 56-dimensional L-kernel in 1.50 s, solves the binary Frobenius system in 0.15 s, and recovers the exact 64-byte shared secret ss in 1.15–2.15 s wall-clock using 58 MB of RAM. Our parameterized dense solver solves all five $r = 5$ LOCKER parameter sets (LOCKER-I, II, IV, VII, VIII, where LOCKER-VII shares the $(m, n, r, d) = (83, 149, 5, 8)$ parameters of 2019 ROLLO-II-128), and cyclotomic $\Phi_n(X)$ projection solves the canonical $X^{83} - 1$ and $X^{107} - 1$ ring variants in 1.19 s and 1.29 s.

On $r = 6$ LOCKER-III $(107, 89, 6, 8)$ at $P = 14$, our sparse Krylov engine constructs the full 183,612 × 192,192 CSR matrix (82,258,176 non-zeros, constant row weight $w = 448$) in 1.65 GB of RAM versus 565 GB dense, executing sparse matrix-vector products at 8.33 ns per $\mathbb{F}_{2^{89}}$ multiply-accumulate ($\beta = 4$, 8 threads) and matching the gate cost model (8) within 1.0% on LOCKER-I. For direct public-key recovery, our single-core solver recovers the secret key (F, x, y) up to $K^\times$-scaling in 5.97 s on 2019 ROLLO-I-128.

Verification Against the Reference Implementation. Our cryptanalysis targets the mathematical specification of LOCKER and ROLLO directly and does not exploit any software defect. When generating benchmark instances from the unmodified NIST Round 1 LOCKER C/C++ submission package [3], we noted two upstream implementation defects: (i) across all 18 LOCKER-I..IX reference and optimized directories, `ffi_vec_add` zeroes its destination reference before addition, turning the in-place call $u \leftarrow u + e_1$ (where u initially holds $e_2 h$) into $u = e_1$ of rank r rather than full rank m (our fetch script strips this zeroing call across the reference directories); and (ii) the LOCKER-IX header lists modulus exponents $\{7, 9, 10\}$ copied from $n = 149$ instead of the specified irreducible exponents $\{2, 5, 6\}$ for $n = 157$. All experiments in

Table 5: Two-input gate complexities ($\log_2$ gates) across all 27 published LOCKER and ROLLO parameter sets. Column **Prior Best** takes the minimum published complexity across MaxMinors (MM), Support-Minors (SM) [10, 14], and Dual-LRPC (DL) [5, §6.2], [22]. Column **CT** evaluates the uniform sparse Block-Lanczos cost (8) at rank r, and **PK** evaluates direct key recovery via (11) on homogeneous $h = x^{-1}y$ (or inhomogeneous TSM (8) at rank $d = w$ on ROLLO-III public keys $\mathsf{pk} = (h, s)$); '—' indicates $m \le 2^r$, $P_2^* > n$, or $m < 2^d$.

Gen.	Parameter Set	(m, n, r, d)	Claim	Prior Best	CT	PK	Δ
2017	LOCKER-I	$(71, 83, 5, 7)$	128	58.2 (MM)	46.3	—	−11.9
	LOCKER-II	$(101, 83, 5, 7)$	192	57.5 (MM)	41.0	—	−16.6
	LOCKER-III	$(107, 89, 6, 8)$	256	69.6 (MM)	58.8	—	−10.8
	LOCKER-IV	$(79, 101, 5, 7)$	128	60.8 (MM)	44.4	—	−16.4
	LOCKER-V	$(97, 103, 6, 8)$	192	72.4 (MM)	62.1	—	−10.3
	LOCKER-VI	$(107, 103, 6, 8)$	256	72.1 (MM)	59.2	—	−12.9
	LOCKER-VII	$(83, 149, 5, 8)$	128	66.2 (MM)	45.6	—	−20.6
	LOCKER-VIII	$(101, 149, 5, 8)$	192	65.8 (MM)	42.7	—	−23.1
	LOCKER-IX	$(109, 157, 6, 9)$	256	79.3 (MM)	60.5	—	−18.8
2019	ROLLO-I-128	$(79, 47, 5, 6)$	128	50.0 (MM)	42.2	31.3	−18.7
	ROLLO-I-192	$(89, 53, 6, 7)$	192	61.4 (MM)	63.7	—	+2.3
	ROLLO-I-256	$(113, 67, 7, 8)$	256	127.7 (SM)	—	—	—
	ROLLO-II-128	$(83, 149, 5, 8)$	128	66.2 (MM)	45.6	—	−20.6
	ROLLO-II-192	$(107, 151, 6, 8)$	192	78.7 (MM)	60.3	—	−18.3
	ROLLO-II-256	$(127, 157, 7, 8)$	256	113.9 (SM)	—	—	—
	ROLLO-III-128	$(101, 47, 6, 5)$[a]	128	49.4 (MM)	58.4	39.3[b]	−10.1
	ROLLO-III-192	$(107, 59, 8, 6)$[a]	192	62.7 (MM)	—	57.6[b]	−5.1
	ROLLO-III-256	$(131, 67, 8, 7)$[a]	256	107.9 (SM)	—	—[c]	—
2020	ROLLO-I-128	$(67, 83, 7, 8)$	128	157.0 (DL)	—	—	—
	ROLLO-I-192	$(79, 97, 8, 8)$	192	180.3 (DL)	—	—	—
	ROLLO-I-256	$(97, 113, 9, 9)$	256	268.7 (DL)	—	—	—
	ROLLO-II-128	$(83, 189, 7, 8)$	128	103.2 (DL)	—	—	—
	ROLLO-II-192	$(97, 193, 8, 8)$	192	141.9 (DL)	—	—	—
	ROLLO-II-256	$(97, 211, 8, 9)$	256	173.2 (DL)	—	—	—
2020[d]	new2ROLLO-I-128	$(73, 83, 7, 8)$	128	175.3 (DL)	—	—	—
	new2ROLLO-I-192	$(89, 97, 8, 8)$	192	210.7 (DL)	—	—	—
	new2ROLLO-I-256	$(103, 113, 9, 9)$	256	290.0 (DL)	—	—	—

[a] In ROLLO-III, $r = w_r \in \{6, 8, 8\}$ is the ciphertext error rank and $d = w \in \{5, 6, 7\}$ is the secret-key rank in $\mathsf{pk} = (h, s = x + hy)$; **Prior Best** [9, 14] evaluates this rank-d $[2n, n]$ public-key instance. [b] Inhomogeneous TSM (8) applied to $\mathsf{pk} = (h, s)$ at rank $d = w$ (homogeneous Algorithm 4 does not apply as h is uniform). [c] Here $m = 131 > 2^7 = 128$ at $d = 7$, but $P_2^*(131, 7) = 263$ (264 for positive excess rank) exceeds $n = 67$. [d] Illustrative large-m parameter sets proposed in [9] and re-evaluated in [10].

Table 6: Measured matrix dimensions over $L = \mathbb{F}_2[X]/(P(X))$, Stage 1 nullity ν_L, memory usage, and wall-clock runtimes across our implemented solvers.

Instance	(m, n, r, d)	**Variant**	P	**Matrix Size**	ν_L	**Memory**	**Time**
LOCKER-I	$(71, 83, 5, 7)$	Schur TSM	9	2184×2240	56	58 MB	1.15 s[a]
LOCKER-I	$(71, 83, 5, 7)$	Overdet.	10	8946×8064	1	128 MB	14.2 s
LOCKER-II	$(101, 83, 5, 7)$	Dense TSM	7	606×672	66	12 MB	0.48 s[b]
LOCKER-IV	$(79, 101, 5, 7)$	Dense TSM	8	1659×1792	133	48 MB	6.05 s[b]
LOCKER-VII	$(83, 149, 5, 8)$	Dense TSM	8	1743×1792	49	72 MB	6.91 s[b]
LOCKER-VIII	$(101, 149, 5, 8)$	Dense TSM	7	606×672	66	16 MB	1.33 s[b]
LOCKER-I ($X^{83}-1$)	$(71, 82, 5, 7)$	Projection	9	2184×2240	56	58 MB	1.19 s
Split (m=n=15)	$(15, 15, 3, 5)$	Projection	6	150×160	10	< 1 MB	0.02 s
LOCKER-III (CSR)	$(107, 89, 6, 8)$	Lanczos	14	183612×192192	8580	1.65 GB	$2^{58.8}$ G[c]
2019 ROLLO-I-128	$(79, 47, 5, 6)$	Direct PK	6	79×64 (C_H)	1	< 2 MB	5.97 s

[a] 1.15 s wall-clock on 12-thread AVX-512 VPCLMULQDQ; 1.77–2.15 s on portable 12-thread PCLMULQDQ. [b] Stage 1–2 C++ linear-algebra time (12 threads) on the unreduced $\binom{P-1}{r}m \times \binom{P}{r}2^r$ system. [c] Measured CSR build ($w = 448$) and $\beta = 4$ sparse matrix-vector multiply benchmark (8.33 ns per multiply-add, 8 threads); total gate count from (8).

this paper use the specified irreducible modulus $P(X)$, compute the genuine non-aliased syndrome $u = e_1 + e_2 h \bmod P(X)$, and assert full rank $\mathrm{rank}_{\mathbb{F}_2}(u) = m$ and successful reference decapsulation on every trial.

Use of AI. The cryptanalytic results and artifacts were initially developed through an autonomous agent system powered by a MiniMax internal model. We validated the key technical claims and refined the presentation of the manuscript.

References

[1] G. Adj et al., "Mirath signature scheme: Algorithm specifications and supporting documentation (v2.1.0)," Submission to the NIST Post-Quantum Cryptography Additional Digital Signatures Process (Round 2), 2025.

[2] C. Aguilar-Melchor, N. Aragon, V. Dyseryn, P. Gaborit, and G. Zémor, "LRPC codes with multiple syndromes: Near ideal-size KEMs without ideals," in *Post-Quantum Cryptography – PQCrypto 2022*, LNCS, vol. 13512, pp. 45–68, Springer, 2022.

[3] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, and G. Zémor, "LOCKER – LOw rank parity ChecK codes EncRyption," Submission to the NIST Post-Quantum Cryptography Standardization Process (Round 1), Nov. 2017.

[4] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, G. Zémor, C. Aguilar Melchor, M. Bardet, S. Bettaieb, L. Bidoux, and A. Otmani, "ROLLO – Rank-Ouroboros, LAKE & LOCKER," Submission to the NIST Post-Quantum Cryptography Standardization Process (Round 2 Initial Specification), Mar. 2019.

[5] N. Aragon et al., "ROLLO – Rank-Ouroboros, LAKE & LOCKER (Updated Specification)," NIST Post-Quantum Cryptography Round 2 Revision, Apr. 21, 2020.

[6] N. Aragon, P. Briaud, V. Dyseryn, P. Gaborit, and A. Vinçotte, "The blockwise rank syndrome learning problem and its applications to cryptography," in *Post-Quantum Cryptography – PQCrypto 2024*, Part I, LNCS, vol. 14771, pp. 75–106, Springer, 2024. (IACR ePrint 2023/1875.)

[7] N. Aragon et al., "RYDE: Rank syndrome DEcoding signature scheme (v2.1.0)," Submission to the NIST Post-Quantum Cryptography Additional Digital Signatures Process (Round 2), 2025.

[8] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J.-P. Tillich, "An algebraic attack on rank metric code-based cryptosystems," in *Advances in Cryptology – EUROCRYPT 2020*, Part III, LNCS, vol. 12107, pp. 64–93, Springer, 2020.

[9] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.-P. Tillich, and J. Verbel, "Improvements of algebraic attacks for solving the rank decoding and MinRank problems," in *Advances in Cryptology – ASIACRYPT 2020*, Part I, LNCS, vol. 12491, pp. 507–536, Springer, 2020.

[10] M. Bardet, P. Briaud, M. Bros, P. Gaborit, and J.-P. Tillich, "Revisiting algebraic attacks on MinRank and on the rank decoding problem," *Designs, Codes and Cryptography*, vol. 91, no. 11, pp. 3671–3707, 2023. (IACR ePrint 2022/1031.)

[11] H. Beeloo-Sauerbier Couvée, A. Wachter-Zeh, and V. Weger, "Hybrid subsupport guessing: A new hybrid technique for the rank decoding problem," in *Post-Quantum Cryptography – PQCrypto 2026*, Part I, LNCS, vol. 16491, pp. 130–155, Springer, 2026. (IACR ePrint 2025/2168.)

[12] S. Chee, K. C. Jeong, T. Lange, N. Lee, A. Pellegrini, and H. Ryu, "Analysis of layered ROLLO-I: A BII-LRPC code-based KEM," *IACR Communications in Cryptology*, vol. 1, no. 3, art. 45, 2024. (IACR ePrint 2024/230.)

[13] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[14] A. Esser, J. A. Verbel, and R. Villanueva-Polanco, "Rank syndrome decoding estimator – An asymptotic and concrete analysis," Cryptology ePrint Archive, Paper 2026/082, 2026.

[15] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, "Low rank parity check codes and their application to cryptography," in *Proceedings of the Workshop on Coding and Cryptography (WCC 2013)*, pp. 168–180, 2013.

[16] K. E. Griffin and M. J. Tsatsomeros, "Principal minors, Part II: The principal minor assignment problem," *Linear Algebra and its Applications*, vol. 419, no. 1, pp. 125–171, 2006.

[17] A. Hauteville and J.-P. Tillich, "New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem," in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 2747–2751, IEEE, 2015.

[18] R. Loewy, "Principal minors and diagonal similarity of matrices," *Linear Algebra and its Applications*, vol. 78, pp. 23–64, 1986.

[19] P. L. Montgomery, "A block Lanczos algorithm for finding dependencies over GF(2)," in *Advances in Cryptology – EUROCRYPT '95*, LNCS, vol. 921, pp. 106–120, Springer, 1995.

[20] G. Alagic et al., "Status report on the second round of the NIST Post-Quantum Cryptography Standardization Process," National Institute of Standards and Technology, Internal Report NISTIR 8309, Jul. 2020.

[21] S. Samardjiska, P. Santini, E. Persichetti, and G. Banegas, "A reaction attack against cryptosystems based on LRPC codes," in *Progress in Cryptology – LATINCRYPT 2019*, LNCS, vol. 11774, pp. 197–216, Springer, 2019. (IACR ePrint 2019/845.)

[22] Y. Song, J. Zhang, X. Huang, and W. Wu, "Blockwise rank decoding problem and LRPC codes: Cryptosystems with smaller sizes," in *Advances in Cryptology – ASIACRYPT 2023*, Part VII, LNCS, vol. 14444, pp. 284–316, Springer, 2023. (Extended in *IEEE Trans. Inf. Theory*, vol. 71, no. 6, pp. 4806–4838, 2025; IACR ePrint 2023/1387.)

[23] D. H. Wiedemann, "Solving sparse linear equations over finite fields," *IEEE Transactions on Information Theory*, vol. 32, no. 1, pp. 54–62, 1986.