Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Bi-Skew Generalized Triangular Matrix Rings and Their Applications in Post-Quantum Cryptography

Mohamed A. FARAHAT

mfarahat7923@gmail.com

Al-Azhar University

Refaat M. SALEM

Al-Azhar University

Hanan A. MOHAMED

Ain Shams University

Article

Keywords: Generalized triangular matrix ring, skew triangular matrix ring, post-quantum cryptography, canonical projection attack, idempotent confinement, nilpotent perturbation, Multivariate Quadratic problem, Radić inverse

Posted Date: November 10th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11213217/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Bi-Skew Generalized Triangular Matrix Rings and Their Applications in Post-Quantum Cryptography

Mohamed A. FARAHAT[1], **Refaat M. SALEM**[1], **Hanan A. MOHAMED**[2]

[1]Mathematics Department, Faculty of Science, Al-Azhar University, Cairo, Egypt.

[2]Mathematics Department, Faculty of Science, Ain Shams University, Cairo, Egypt.

mfarahat7923@gmail.com

Abstract

In this paper, we introduce a new algebraic structure called the *bi-skew generalized triangular matrix ring*, denoted by $(S, R, M, 0)_{\varphi,\psi}$, where S and R are associative rings with unity, ${}_SM_R$ is a unitary (S, R)-bimodule, φ is an endomorphism on S with $\varphi(1_S) = 1_S$, and ψ is an endomorphism on R with $\psi(1_R) = 1_R$. We rigorously determine the ideal structure of this ring by establishing a complete characterization of its Jacobson radical $J(A)$. Driven by the emerging vulnerabilities of classical public-key cryptosystems to quantum polynomial-time algorithms, we deploy this non-commutative framework to construct a post-quantum key exchange protocol inspired by the Stickel architecture. We demonstrate that while a naive pure-exponentiation protocol is vulnerable to a canonical projection homomorphism onto the diagonal subrings, this threat is completely neutralized within our protocol by integrating orthogonal idempotents (zero-divisor confinement) and ephemeral nilpotent perturbations drawn from $J(A)$. We prove that projection decoupling, centralizer decompositions, Shpilrain–Ushakov matrix inversions, and minimal polynomial linearizations are simultaneously obstructed by Frobenius non-linearity, idempotent singularity, and nilpotent masking. The security of the scheme is formulated under explicit multivariate quadratic (MQ) hardness conjectures against passive adversaries. Furthermore, as a second structural countermeasure against canonical projection, we construct an asymmetric data encapsulation mechanism (DEM) deploying Radić's right-invertibility over rectangular bimodules, confining the secret carrier entirely within the projection kernel and leveraging dimensional expansion from 2-vectors to 3-vectors for entropy hiding. Finally, two open cryptographic challenge problems are provided to facilitate community cryptanalysis.

2020 Mathematics Subject Classification: Primary 16D25, 16D90, 16S50; Secondary 11T71, 16W20, 16N20, 94A60.

Keywords and phrases: Generalized triangular matrix ring, skew triangular matrix ring, post-quantum cryptography, canonical projection attack, idempotent confinement, nilpotent perturbation, Multivariate Quadratic problem, Radić inverse.

1 Introduction

In this section, we review classical matrix ring extensions and define our new class of rings called a *bi-skew generalized triangular matrix ring*. Throughout this paper, R denotes an associative ring with identity and M_R is a unitary right R-module.

The anticipated realization of fault-tolerant quantum computational architectures poses a systemic challenge to ubiquitous public-key primitives founded upon the integer factorization problem and the discrete logarithm problem over finite fields and elliptic curves [8, 13]. In particular, Shor's algorithm polynomializes the abelian hidden subgroup problem, rendering conventional standards such as RSA and ECDSA asymptotically vulnerable. Additionally, passive adversarial surveillance models deploying "Store Now, Decrypt Later" (SNDL) strategies mandate the preemptive development of quantum-resistant cryptographic foundations [2]. Consequently, investigating non-commutative algebraic structures that naturally resist quantum Fourier transform linearizations has emerged as an active area of contemporary research.

Recall the following ring structures. In [5], Chen et al. investigated the skew triangular matrix ring $T_n(R, \sigma)$, where R is a ring with identity 1, σ is an endomorphism on R satisfying $\sigma(1_R) = 1_R$, and n is a positive integer. The skew upper triangular matrix ring of degree n is defined as:

$$W = \{(a_{ij}) \mid a_{ij} \in R \text{ and } a_{ij} = 0 \text{ for all } i > j\},$$

under componentwise addition and the multiplication rule:

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \quad \text{and} \quad (a_{ij})(b_{ij}) = (c_{ij}),$$

where $c_{ij} = 0$ for $i > j$ and

$$c_{ij} = \sum_{l=0}^{j-i} a_{i,i+l}\sigma^l(b_{i+l,j}) \quad \text{for } i \leq j.$$

Another classical extension is the generalized triangular matrix ring:

$$T = (S, R, M, 0) = \begin{pmatrix} S & M \\ 0 & R \end{pmatrix},$$

where S and R are rings and ${}_SM_R$ is an (S, R)-bimodule. The set T forms a ring under componentwise addition and standard block multiplication:

$$\begin{pmatrix} s_1 & m_1 \\ 0 & r_1 \end{pmatrix} \begin{pmatrix} s_2 & m_2 \\ 0 & r_2 \end{pmatrix} = \begin{pmatrix} s_1s_2 & s_1m_2 + m_1r_2 \\ 0 & r_1r_2 \end{pmatrix}$$

for all elements in T. Generalized triangular matrix rings of this form have been widely investigated in ring theory (see, e.g., [4]).

Motivated by these classical constructions, we introduce the central algebraic structure of this paper. The designation *bi-skew* reflects the bilateral twisting applied simultaneously to both constituent base rings S and R via the endomorphisms φ and ψ, in contrast to traditional skew extensions which twist only a single ring component.

Let S and R be associative rings with unity, ${}_SM_R$ a unitary (S, R)-bimodule, $\varphi \in \mathrm{End}(S)$ an endomorphism with $\varphi(1_S) = 1_S$, and $\psi \in \mathrm{End}(R)$ an endomorphism with $\psi(1_R) = 1_R$. The set

$$A = (S, R, M, 0)_{\varphi,\psi} = \left\{ \begin{pmatrix} s & m \\ 0 & r \end{pmatrix} \;\middle|\; s \in S,\, r \in R,\, m \in M \right\}$$

forms an associative ring under componentwise addition and the bi-skew multiplication defined by:

$$\begin{pmatrix} s_1 & m_1 \\ 0 & r_1 \end{pmatrix} \begin{pmatrix} s_2 & m_2 \\ 0 & r_2 \end{pmatrix} = \begin{pmatrix} s_1 s_2 & \varphi(s_1)m_2 + m_1\psi(r_2) \\ 0 & r_1 r_2 \end{pmatrix} \tag{1}$$

for all elements in A. Associativity of multiplication in A follows directly from the endomorphism properties of φ and ψ together with the bimodule associativity $(s \cdot m) \cdot r = s \cdot (m \cdot r)$. The ring possesses the identity element $I_A = \begin{pmatrix} 1_S & 0 \\ 0 & 1_R \end{pmatrix}$. We designate A as a *bi-skew generalized triangular matrix ring.*

Remark 1.
1. *If $\varphi = \mathrm{id}_S$ and $\psi = \mathrm{id}_R$, then $A = (S, R, M, 0) = T$, which recovers the classical generalized triangular matrix ring.*
2. *If $S = M = R$, $\varphi = \mathrm{id}_S$, and $\psi = \sigma$, then $A = (R, R, R, 0)_\sigma$ recovers the skew triangular matrix ring $W = T_n(R, \sigma)$ specifically for dimension $n = 2$, as the bi-skew construction is structured as a 2×2 block ring.*

Example 1 (Heterogeneous Bi-skew Generalized Triangular Matrix Ring)**.** *Let the left base ring be the finite field $S = \mathbb{F}_4 = \mathbb{F}_2[\alpha]/\langle \alpha^2 + \alpha + 1 \rangle$, endowed with the Frobenius automorphism $\varphi(s) = s^2$. Let the right base ring be $R = \mathbb{F}_{16} = \mathbb{F}_2[\beta]/\langle \beta^4 + \beta + 1 \rangle$, endowed with the Frobenius automorphism $\psi(r) = r^4$. The subfield $\mathbb{F}_2(\beta^5) = \mathbb{F}_2(\beta^2 + \beta) \subset R$ is canonically isomorphic to S via the embedding $\theta : S \hookrightarrow R$ defined by $\theta(\alpha) = \beta^5 = \beta^2 + \beta$. Reducing powers of β modulo the field polynomial $\beta^4 = \beta + 1$ yields: $\beta^5 = \beta^2 + \beta$ and $\beta^{10} = (\beta^2 + \beta)^2 = \beta^4 + \beta^2 = \beta^2 + \beta + 1$. Consequently, we verify the subfield embedding directly:*

$$\theta(\alpha)^2 + \theta(\alpha) + 1 = \beta^{10} + \beta^5 + 1 = (\beta^2 + \beta + 1) + (\beta^2 + \beta) + 1 = 0.$$

Define the bimodule ${}_S M_R = \mathbb{F}_{16} \times \mathbb{F}_{16}$, forming an elementary abelian 2-group of order 256. The left S-action is defined by $s(x, y) = (\theta(s)x, \theta(s)y)$ for all $s \in S$, and the right R-action is given by $(x, y)r = (xr, yr)$ for all $r \in R$. The resulting ring $A = (S, R, M, 0)_{\varphi,\psi}$ has order:

$$|A| = |S| \times |R| \times |M| = 4 \times 16 \times 256 = 16,384 \text{ elements.}$$

Consider two elements $P, Q \in A$ defined by:

$$P = \begin{pmatrix} \alpha & (1, \beta) \\ 0 & \beta^2 \end{pmatrix}, \quad Q = \begin{pmatrix} \alpha^2 & (\beta^3, 1) \\ 0 & \beta \end{pmatrix}.$$

Computing the bi-skew product yields $PQ = \begin{pmatrix} 1 & (\beta^{11}, 1) \\ 0 & \beta^3 \end{pmatrix}$, where the skew bimodule entry evaluates as:

$$\begin{aligned} m_{PQ} &= \varphi(s_P)m_Q + m_P\psi(r_Q) \\ &= \theta(\varphi(\alpha))(\beta^3, 1) + (1, \beta)\psi(\beta) \\ &= \theta(\alpha^2)(\beta^3, 1) + (1, \beta)\beta^4 \\ &= \beta^{10}(\beta^3, 1) + (\beta^4, \beta^5) \\ &= (\beta^{13} + \beta^4, \beta^{10} + \beta^5) = (\beta^{11}, 1). \end{aligned}$$

Here, reduction modulo $\beta^4 + \beta + 1 = 0$ gives $\beta^{13} + \beta^4 = (\beta^3 + \beta^2 + 1) + (\beta + 1) = \beta^3 + \beta^2 + \beta = \beta^{11}$ and $\beta^{10} + \beta^5 = (\beta^2 + \beta + 1) + (\beta^2 + \beta) = 1$.

Evaluating iterated powers of P under this multiplication rule reveals:

$$P^2 = \begin{pmatrix} \alpha^2 & (\beta, \beta^2) \\ 0 & \beta+1 \end{pmatrix}, \quad P^3 = \begin{pmatrix} 1 & (\beta^3+\beta^2, \beta^3+\beta+1) \\ 0 & \beta^3+\beta^2 \end{pmatrix},$$

$$P^4 = \begin{pmatrix} \alpha & (\beta^3, \beta+1) \\ 0 & \beta^2+1 \end{pmatrix}, \quad \ldots, \quad P^{15} = \begin{pmatrix} 1 & (0,0) \\ 0 & 1 \end{pmatrix} = I_A.$$

By induction on k, the upper-right entry m_{P^k} has the structural form $x_k(1, \beta)$ for a field scalar $x_k \in \mathbb{F}_{16}$. The multiplicative orders satisfy $\mathrm{ord}(\alpha) = 3$ in $\mathbb{F}_4^\times$ and $\mathrm{ord}(\beta^2) = 15$ in $\mathbb{F}_{16}^\times$ (since β^2 generates $\mathbb{F}_{16}^\times$). Since $\gcd(13, 15) = 1$, the element β^{13} is a primitive generator of $\mathbb{F}_{16}^\times$. The scalar coefficient evaluates to:

$$x_k = \beta^{10(k-1)} \sum_{i=0}^{k-1} (\beta^{13})^i = \beta^{10(k-1)} \times \frac{\beta^{13k} - 1}{\beta^{13} - 1}.$$

Because $\beta^{13k} - 1 = 0$ if and only if $15 \mid k$, it follows that $x_k \neq 0$ for all $1 \leq k < 15$, and $x_{15} = 0$, confirming that the first simultaneous return to the identity $P^k = I_A$ occurs precisely at $k = 15$.

Theorem 1 (The Jacobson Radical of A)**.** *Let $A = (S, R, M, 0)_{\varphi,\psi}$ be a bi-skew generalized triangular matrix ring. Then the Jacobson radical of A is given by:*

$$J(A) = \begin{pmatrix} J(S) & M \\ 0 & J(R) \end{pmatrix}.$$

Proof. Recall that for any associative ring T with unity, an element $x \in J(T)$ if and only if $1_T - yx$ is invertible in T for all $y \in T$.

First, let $X = \begin{pmatrix} s & m \\ 0 & r \end{pmatrix} \in J(A)$. For an arbitrary $s' \in S$, consider $Y_1 = \begin{pmatrix} s' & 0 \\ 0 & 0 \end{pmatrix} \in A$. Then:

$$I_A - Y_1 X = \begin{pmatrix} 1_S - s's & -\varphi(s')m \\ 0 & 1_R \end{pmatrix}.$$

Because $X \in J(A)$, $I_A - Y_1 X$ is invertible in A. Its $(1,1)$-entry must therefore be invertible in S, meaning $1_S - s's \in U(S)$ for all $s' \in S$. Consequently, $s \in J(S)$. Similarly, choosing $Y_2 = \begin{pmatrix} 0 & 0 \\ 0 & r' \end{pmatrix} \in A$ for an arbitrary $r' \in R$ yields $1_R - r'r \in U(R)$, proving that $r \in J(R)$. Since M is the full bimodule, no constraint is imposed on the off-diagonal entry m, and it trivially lies in M. Hence:

$$J(A) \subseteq \begin{pmatrix} J(S) & M \\ 0 & J(R) \end{pmatrix}.$$

Conversely, let $X = \begin{pmatrix} s & m \\ 0 & r \end{pmatrix} \in \begin{pmatrix} J(S) & M \\ 0 & J(R) \end{pmatrix}$. For any arbitrary element $Y = \begin{pmatrix} s' & m' \\ 0 & r' \end{pmatrix} \in A$, we compute:

$$I_A - YX = \begin{pmatrix} 1_S - s's & -\varphi(s')m - m'\psi(r) \\ 0 & 1_R - r'r \end{pmatrix} = \begin{pmatrix} u & -v_0 \\ 0 & w \end{pmatrix},$$

where $u = 1_S - s's \in U(S)$, $w = 1_R - r'r \in U(R)$, and $v_0 = \varphi(s')m + m'\psi(r) \in M$. We construct the candidate inverse $Z = \begin{pmatrix} u^{-1} & v \\ 0 & w^{-1} \end{pmatrix} \in A$. Evaluating the right inverse condition $(I_A - YX)Z = I_A$:

$$\begin{pmatrix} u & -v_0 \\ 0 & w \end{pmatrix} \begin{pmatrix} u^{-1} & v \\ 0 & w^{-1} \end{pmatrix} = \begin{pmatrix} 1_S & \varphi(u)v - v_0\psi(w^{-1}) \\ 0 & 1_R \end{pmatrix}.$$

Setting $\varphi(u)v - v_0\psi(w^{-1}) = 0$ and noting that $\varphi(u) \in U(S)$ because $\varphi(u)\varphi(u^{-1}) = \varphi(uu^{-1}) = \varphi(1_S) = 1_S$, v is uniquely determined as:

$$v = \varphi(u^{-1})v_0\psi(w^{-1}).$$

Now evaluating the left inverse condition $Z(I_A - YX)$:

$$\begin{pmatrix} u^{-1} & v \\ 0 & w^{-1} \end{pmatrix} \begin{pmatrix} u & -v_0 \\ 0 & w \end{pmatrix} = \begin{pmatrix} 1_S & \varphi(u^{-1})(-v_0) + v\psi(w) \\ 0 & 1_R \end{pmatrix}.$$

Substituting $v = \varphi(u^{-1})v_0\psi(w^{-1})$ into the upper-right entry gives:

$$\begin{aligned} -\varphi(u^{-1})v_0 + [\varphi(u^{-1})v_0\psi(w^{-1})]\psi(w) &= -\varphi(u^{-1})v_0 + \varphi(u^{-1})v_0\psi(w^{-1}w) \\ &= -\varphi(u^{-1})v_0 + \varphi(u^{-1})v_0 = 0. \end{aligned}$$

Thus, Z is a strict two-sided inverse of $I_A - YX$ in A, proving that $X \in J(A)$. □

To prepare the algebraic foundation for our cryptographic constructions, we note two structural properties of A. First, A admits a natural canonical projection ring homomorphism onto its diagonal subrings:

$$\pi : A \longrightarrow S \times R, \quad \pi \begin{pmatrix} s & m \\ 0 & r \end{pmatrix} = (s, r), \tag{2}$$

whose kernel is precisely the nilpotent bimodule ideal $\ker(\pi) = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix} \subseteq J(A)$ satisfying $\ker(\pi)^2 = \{0\}$. Second, A possesses fundamental orthogonal idempotents $e_1 = \begin{pmatrix} 1_S & 0 \\ 0 & 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1_R \end{pmatrix}$ satisfying $e_1^2 = e_1$, $e_2^2 = e_2$, $e_1e_2 = e_2e_1 = 0$, and $e_1 + e_2 = I_A$, along with internal idempotents when S and R are matrix or decomposable rings. While base generators P, Q must satisfy $(P - I_A), (Q - I_A) \notin J(A)$ so that their multiplicative orbits do not collapse into trivial affine progressions $(I_A + N)^a = I_A + aN$, the interplay between $\ker(\pi) \subseteq J(A)$ and orthogonal idempotents provides the exact mechanism needed to immunize key exchange protocols against homomorphic projection attacks.

2 Bi-Skew Key Exchange Protocol and Projection Hardening

We now formulate an unauthenticated two-party key exchange protocol over $A = (S, R, M, 0)_{\varphi,\psi}$ inspired by the Stickel framework [15]. A rigorous design in triangular matrix rings must confront a fundamental structural threat: the canonical projection attack. In this section, we first expose how a naive pure-exponentiation protocol falls prey to diagonal projection, and then construct our hardened protocol deploying orthogonal idempotents and ephemeral nilpotent perturbations from $J(A)$.

2.1 Naive Exponentiation and the Canonical Projection Vulnerability

Suppose Alice and Bob attempt a direct Stickel-type exchange using invertible public matrices $P, Q, X \in U(A)$ ($PQ \neq QP$) by selecting private integer exponents (a, b) and (u, v) and transmitting the pure product matrices:

$$U_{\text{Alice}}^{(0)} = P^a X Q^b, \quad U_{\text{Bob}}^{(0)} = P^u X Q^v. \tag{3}$$

While the upper-right bimodule entry of $U_{\text{Alice}}^{(0)}$ is heavily entangled via the bi-skew action (φ, ψ), an adversary does not need to attack the bimodule directly. Because the canonical projection $\pi : A \to S \times R$ defined in Equation (2) is a ring homomorphism, it preserves multiplication across the public transmission:

$$\pi\left(U_{\text{Alice}}^{(0)}\right) = \pi(P)^a \cdot \pi(X) \cdot \pi(Q)^b = \left(s_P^a s_X s_Q^b,\ r_P^a r_X r_Q^b\right).$$

This homomorphic projection completely decouples the diagonal components from the bimodule M, bypassing the non-commutative bi-skew polynomial expansion in $\ker(\pi)$. Moreover, because the transit matrix $X = \begin{pmatrix} s_X & m_X \\ 0 & r_X \end{pmatrix} \in U(A)$ is publicly known, its diagonal components $s_X \in U(S)$ and $r_X \in U(R)$ are public constants. The adversary simply multiplies the projected equations by s_X^{-1} and r_X^{-1} to obtain:

$$u_S \cdot s_X^{-1} = s_P^a s_Q^b \quad \text{in } S, \qquad u_R \cdot r_X^{-1} = r_P^a r_Q^b \quad \text{in } R. \tag{4}$$

When S and R are commutative finite fields, expressing the diagonal elements in terms of primitive root generators reduces Equation (4) via discrete logarithms to a 2×2 system of linear modular equations in the unknown exponents (a, b). Once (a, b) are recovered from the diagonal, the adversary substitutes them directly into the bi-skew power formula to reconstruct the entire secret matrix K.

2.2 Overcoming Projection Attacks via Idempotents and Nilpotent Perturbation

To neutralize the canonical projection attack at its root without sacrificing associative key agreement, we modify the protocol architecture using two complementary ring-theoretic tools:

1. **Idempotent Confinement (Zero-Divisor Singularity):** Observe that in a Stickel-like exchange, legitimate parties compute the shared key exclusively through *forward* matrix multiplications; neither Alice nor Bob ever inverts P^a, Q^b, P^u, or Q^v. Inversion is required *only* by the adversary (either to isolate diagonal components or to execute the Shpilrain–Ushakov inversion step Y_1^{-1}). We therefore incorporate non-trivial orthogonal idempotents $e_P, e_Q \in A$ ($e_P^2 = e_P$, $e_Q^2 = e_Q$, with complementary annihilating idempotents $\bar{e}_P = I_A - e_P$ and $\bar{e}_Q = I_A - e_Q$ satisfying $e_P \bar{e}_P = 0$ and $e_Q \bar{e}_Q = 0$) that commute with the base generators P and Q, respectively. By defining the active base generators as the idempotent-confined matrices $\tilde{P} = e_P P$ and $\tilde{Q} = e_Q Q$, all powers $\tilde{P}^a = e_P P^a$ and $\tilde{Q}^b = e_Q Q^b$ reside within a zero-divisor-dense subring where $\det(\tilde{P}^a) = 0$ and $\det(\tilde{Q}^b) = 0$. Consequently, any surrogate commuting matrix Y constructed by an adversary is strictly singular ($\det(Y) = 0$), rendering matrix inversion impossible.

2. **Ephemeral Nilpotent Perturbation via $J(A)$:** To break the multiplicative homomorphism of π, Alice selects ephemeral nilpotent elements $N_{A,1} \in \bar{e}_P J(A) \bar{e}_P$ and $N_{A,2} \in \bar{e}_Q J(A) \bar{e}_Q$ from the nilpotent radical ideal of index 2 (so that $N^2 = 0$ and $J(A)\bar{e} \cdot \bar{e}J(A) = 0$), and forms the perturbed secret operators:

$$\mathcal{A} = e_P P^a + N_{A,1}, \qquad \mathcal{B} = e_Q Q^b + N_{A,2}.$$

Similarly, Bob selects ephemeral nilpotent elements $N_{B,1} \in \bar{e}_P J(A) \bar{e}_P$ and $N_{B,2} \in \bar{e}_Q J(A) \bar{e}_Q$ and forms:

$$\mathcal{U} = e_P P^u + N_{B,1}, \qquad \mathcal{V} = e_Q Q^v + N_{B,2}.$$

When Alice transmits $U_{\text{Alice}} = \mathcal{A}X\mathcal{B}$, expanding the product yields:

$$U_{\text{Alice}} = \tilde{P}^a X \tilde{Q}^b + N_A, \quad \text{where } N_A = \tilde{P}^a X N_{A,2} + N_{A,1} X \tilde{Q}^b + N_{A,1} X N_{A,2} \in J(A). \tag{5}$$

Because the public transit matrix X mixes the Peirce components ($e_P X \bar{e}_Q \neq 0$ and $\bar{e}_P X e_Q \neq 0$), the composite perturbation $N_A \in J(A)$ is non-zero and satisfies $N_A^2 = 0$. This additive shift N_A destroys the pure multiplicativity of the public channel:

$$\pi(U_{\text{Alice}}) = \pi\left(\tilde{P}^a X \tilde{Q}^b\right) + \pi(N_A) \neq \pi(\tilde{P})^a \pi(X) \pi(\tilde{Q})^b,$$

contaminating both the diagonal and the bimodule block with unknown ephemeral radical variables and forcing the adversary to confront an entangled, non-homogeneous multivariate quadratic (MQ) system.

2.3 Hardened Protocol Specification

1. **Public Parameters:** Associative finite rings S, R (endowed with non-trivial radical/matrix structure over $\mathbb{F}_{p^k}$ and $\mathbb{F}_{p^t}$), unitary bimodule ${}_S M_R$, Frobenius endomorphisms $\varphi(x) = x^{p^c}$, $\psi(x) = x^{p^d}$, non-commuting base matrices $P, Q \in A$ ($PQ \neq QP$), commuting non-trivial idempotents e_P, e_Q defining $\tilde{P} = e_P P$ and $\tilde{Q} = e_Q Q$, and a public transit matrix $X \in A$.

2. **Key Exchange Phase:**

   - Alice picks private integers $a, b \in \mathbb{N}$ and ephemeral nilpotent matrices $N_{A,1} \in \bar{e}_P J(A) \bar{e}_P$, $N_{A,2} \in \bar{e}_Q J(A) \bar{e}_Q$, sets $\mathcal{A} = \tilde{P}^a + N_{A,1}$ and $\mathcal{B} = \tilde{Q}^b + N_{A,2}$, and transmits:
   $$U_{\text{Alice}} = \mathcal{A}X\mathcal{B} = \tilde{P}^a X \tilde{Q}^b + N_A.$$
   - Bob picks private integers $u, v \in \mathbb{N}$ and ephemeral nilpotent matrices $N_{B,1} \in \bar{e}_P J(A) \bar{e}_P$, $N_{B,2} \in \bar{e}_Q J(A) \bar{e}_Q$, sets $\mathcal{U} = \tilde{P}^u + N_{B,1}$ and $\mathcal{V} = \tilde{Q}^v + N_{B,2}$, and transmits:
   $$U_{\text{Bob}} = \mathcal{U}X\mathcal{V} = \tilde{P}^u X \tilde{Q}^v + N_B.$$

3. **Shared Secret Derivation:** Alice computes $K_{\text{Alice}} = \tilde{P}^a U_{\text{Bob}} \tilde{Q}^b$ (or $\mathcal{A}U_{\text{Bob}}\mathcal{B}$). Bob computes $K_{\text{Bob}} = \tilde{P}^u U_{\text{Alice}} \tilde{Q}^v$ (or $\mathcal{U}U_{\text{Alice}}\mathcal{V}$).

Theorem 2 (Correctness and Automatic Nilpotent Annihilation)**.** *Let $A = (S, R, M, 0)_{\varphi,\psi}$ be a bi-skew generalized triangular matrix ring. Under the hardened key exchange protocol, the ephemeral nilpotent perturbations $N_A, N_B \in J(A)$ vanish identically during shared secret derivation, yielding:*

$$K_{\text{Alice}} = K_{\text{Bob}} = \tilde{P}^{a+u} X \tilde{Q}^{b+v}.$$

Proof. Since $e_P^2 = e_P$ commutes with P and $\bar{e}_P = I_A - e_P$ satisfies $e_P\bar{e}_P = \bar{e}_P e_P = 0$, any element $N_1 \in \bar{e}_P J(A)\bar{e}_P$ satisfies $e_P N_1 = N_1 e_P = 0$. Furthermore, by the nilpotency of the radical sub-ideal, $N_{A,1}N_{B,1} = N_{B,1}N_{A,1} = 0$. Evaluating the left operator product $\mathcal{AU}$ yields:

$$\mathcal{AU} = (e_P P^a + N_{A,1})(e_P P^u + N_{B,1}) = e_P^2 P^{a+u} + e_P P^a N_{B,1} + N_{A,1} e_P P^u + N_{A,1}N_{B,1} = e_P P^{a+u} = \tilde{P}^{a+u}.$$

By symmetry, $\mathcal{UA} = e_P P^{u+a} = \tilde{P}^{a+u}$. Identically on the right, since $e_Q\bar{e}_Q = \bar{e}_Q e_Q = 0$ and $N_{A,2}N_{B,2} = N_{B,2}N_{A,2} = 0$, we have:

$$\mathcal{VB} = (e_Q Q^v + N_{B,2})\left(e_Q Q^b + N_{A,2}\right) = e_Q Q^{b+v} = \tilde{Q}^{b+v} = \mathcal{BV}.$$

By the associativity of multiplication in A, Alice's derivation evaluates to:

$$K_{\text{Alice}} = \mathcal{A}U_{\text{Bob}}\mathcal{B} = \mathcal{A}(\mathcal{U}X\mathcal{V})\mathcal{B} = (\mathcal{AU})X(\mathcal{VB}) = \tilde{P}^{a+u} X \tilde{Q}^{b+v},$$

and Bob's derivation evaluates to:

$$K_{\text{Bob}} = \mathcal{U}U_{\text{Alice}}\mathcal{V} = \mathcal{U}(\mathcal{A}X\mathcal{B})\mathcal{V} = (\mathcal{UA})X(\mathcal{BV}) = \tilde{P}^{a+u} X \tilde{Q}^{b+v}.$$

Thus, the nilpotent masks N_A and N_B vanish identically upon reconciliation, and $K_{\text{Alice}} = K_{\text{Bob}}$. □

Algorithm 1 Hardened Bi-Skew Non-Commutative Key Exchange Protocol

---

Require: Public parameters: Rings S, R, bimodule ${}_SM_R$, endomorphisms $\varphi \in \text{End}(S), \psi \in \text{End}(R)$, base matrices $P, Q, X \in A$, orthogonal idempotents e_P, e_Q with $\tilde{P} = e_P P$, $\tilde{Q} = e_Q Q$.

Ensure: Identical shared secret key $K = K_{\text{Alice}} = K_{\text{Bob}} \in A$. **Phase 1: Perturbed Ephemeral Key Generation**

1: **Alice:** Selects private exponents $a, b \in \mathbb{N}$ and nilpotents $N_{A,1}, N_{A,2} \in J(A)$ with $N^2 = 0$.

2: **Alice:** Computes perturbed matrix $U_{\text{Alice}} = (\tilde{P}^a + N_{A,1})X(\tilde{Q}^b + N_{A,2}) = \tilde{P}^a X \tilde{Q}^b + N_A$.

3: **Alice** $\xrightarrow{U_{\text{Alice}}}$ **Bob**

4: **Bob:** Selects private exponents $u, v \in \mathbb{N}$ and nilpotents $N_{B,1}, N_{B,2} \in J(A)$ with $N^2 = 0$.

5: **Bob:** Computes perturbed matrix $U_{\text{Bob}} = (\tilde{P}^u + N_{B,1})X(\tilde{Q}^v + N_{B,2}) = \tilde{P}^u X \tilde{Q}^v + N_B$.

6: **Bob** $\xrightarrow{U_{\text{Bob}}}$ **Alice Phase 2: Shared Secret Derivation (Nilpotent Annihilation)**

7: **Alice:** Computes $K_{\text{Alice}} = (\tilde{P}^a + N_{A,1})U_{\text{Bob}}(\tilde{Q}^b + N_{A,2}) = \tilde{P}^{a+u} X \tilde{Q}^{b+v}$.

8: **Bob:** Computes $K_{\text{Bob}} = (\tilde{P}^u + N_{B,1})U_{\text{Alice}}(\tilde{Q}^v + N_{B,2}) = \tilde{P}^{u+a} X \tilde{Q}^{v+b}$.

9: **return** $K = K_{\text{Alice}} = K_{\text{Bob}}$.

Open Cryptographic Challenge 1 (Hardened Bi-Skew Key Exchange Challenge)**.** *Let $A = (S, R, M, 0)_{\varphi,\psi}$ be instantiated over heterogeneous finite extensions with coprime Galois degrees: let S be a 2×2 upper-triangular/decomposable ring over $\mathbb{F}_{2^{15}}$ with Frobenius automorphism $\varphi(s) = s^{2^1}$ ($\mathrm{ord}(\varphi) = 15$), and let R be defined over $\mathbb{F}_{2^{16}}$ with Conway polynomial $f(x) = x^{16} + x^5 + x^3 + x + 1$ and automorphism $\psi(r) = r^{2^1}$ ($\mathrm{ord}(\psi) = 16$). Let $M = \mathbb{F}_{2^{240}}^{2\times 2}$ act as a compatible unitary (S, R)-bimodule. Since $\gcd(15, 16) = 1$, Asymmetric Orbit Disjointness is strictly fulfilled. Given public parameters (P, Q, X, e_P, e_Q) and nilpotent-perturbed exchange matrices $U_{\text{Alice}} = \tilde{P}^a X \tilde{Q}^b + N_A$ and $U_{\text{Bob}} = \tilde{P}^u X \tilde{Q}^v + N_B$ where $N_A, N_B \in J(A)$ satisfy $N^2 = 0$, recover the shared key $K = \tilde{P}^{a+u} X \tilde{Q}^{b+v} \in A$ or the private tuples (a, b, N_A) in time strictly faster than $\mathcal{O}(2^{128})$ operations.*

3 Practical Implementation: Hybrid Key Encapsulation and Payload Encryption

In modern cryptographic infrastructures, asymmetric algebraic structures are deployed as Key Encapsulation Mechanisms (KEM) to establish a shared secret K via Algorithm 1, which then seeds an ultra-fast symmetric cipher for bulk transmission.

3.1 Canonical Bit-Serialization of the Shared Matrix Key

Let $K = \begin{pmatrix} s & m \\ 0 & r \end{pmatrix} = \begin{pmatrix} 1 & (\beta^{11}, 1) \\ 0 & \beta^3 \end{pmatrix} \in A$ be the shared secret matrix established via the key exchange protocol over $A = (S, R, M, 0)_{\varphi,\psi}$, where the active components lie in $\mathbb{F}_4$, $\mathbb{F}_{16}$, and ${}_S M_R = \mathbb{F}_{16}^2$.

We define a canonical bit-serialization map $\tau : A \to \mathbb{F}_2^{14}$ by decomposing each component over its polynomial basis:

1. **Top-Left Entry** ($s \in \mathbb{F}_4$): Represented over $\{1, \alpha\}$ as $s = s_0 + s_1\alpha \mapsto (s_0, s_1) \in \mathbb{F}_2^2$. For $s = 1$, $\tau(s) = 01_2$.

2. **Bottom-Right Entry** ($r \in \mathbb{F}_{16}$): Represented over $\{1, \beta, \beta^2, \beta^3\}$ as $r = \sum_{i=0}^{3} r_i \beta^i \mapsto (r_0, r_1, r_2, r_3) \in \mathbb{F}_2^4$. For $r = \beta^3$, $\tau(r) = 1000_2$.

3. **Bimodule Component** ($m = (x, y) \in \mathbb{F}_{16}^2$): Each coordinate maps to a 4-bit vector:

$$x = \beta^{11} = \beta^3 + \beta^2 + \beta \mapsto 1110_2,$$
$$y = 1 = 1 + 0\beta + 0\beta^2 + 0\beta^3 \mapsto 0001_2.$$

   Thus, $\tau(m) = \tau(x) \parallel \tau(y) = 11100001_2 \in \mathbb{F}_2^8$.

Concatenating yields the 14-bit master key:

$$K_{\text{bits}} = \tau(s) \parallel \tau(r) \parallel \tau(x) \parallel \tau(y) = 01100011100001_2 \in \mathbb{F}_2^{14}.$$

3.2 Encryption and Numerical Verification

Let $(p_1, \ldots, p_N)$ denote plaintext bytes ($p_i \in \mathbb{F}_2^8$). The keystream $(k_1, \ldots, k_N)$ is generated via periodic concatenation seeded by K_{bits}. We verify this using the 11-byte ASCII

payload: `"ATTACK SOON"`.

$$\text{Ciphertext} = \texttt{22F1FA775B33C130EAE178}.$$

Decryption via $p_i = c_i \oplus k_i$ completely restores `"ATTACK SOON"`. This test serves as a proof-of-concept for the serialization pipeline.

4 Structural Security and Complexity Analysis

In this section, we present a comprehensive cryptanalytic and computational complexity evaluation of the hardened bi-skew key exchange protocol. We formally specify the adversarial threat model under passive eavesdropping conditions, prove the structural immunity of the scheme against canonical projection, centralizer-based decomposition, and minimal polynomial linearization attacks, and formulate the algebraic intractability of private key extraction via multivariate quadratic (MQ) systems.

4.1 Threat Model

We evaluate the protocol in the standard passive eavesdropper model (honest-but-curious adversary). The goal of the adversary is to compute the shared secret matrix $K = \tilde{P}^{a+u} X \tilde{Q}^{b+v}$ from the public transcript $(P, Q, X, e_P, e_Q, U_{\text{Alice}}, U_{\text{Bob}})$, where $U_{\text{Alice}} = \tilde{P}^a X \tilde{Q}^b + N_A$ and $U_{\text{Bob}} = \tilde{P}^u X \tilde{Q}^v + N_B$.

4.2 Resistance to Projection and Classical Linearization Attacks

Proposition 1 (Obstruction of Canonical Projection Decoupling)**.** *Under Algorithm 1, the canonical projection homomorphism $\pi : A \to S \times R$ fails to decouple the private exponents (a, b) from the radical perturbation $N_A \in J(A)$, and the transit matrix X cannot be eliminated by diagonal division.*

Proof. Applying π to the perturbed transmission $U_{\text{Alice}} = (\tilde{P}^a + N_{A,1}) X (\tilde{Q}^b + N_{A,2}) = \tilde{P}^a X \tilde{Q}^b + N_A$ yields:

$$\pi(U_{\text{Alice}}) = \pi(\tilde{P}^a X \tilde{Q}^b) + \pi(N_A).$$

First, because $N_A = \tilde{P}^a X N_{A,2} + N_{A,1} X \tilde{Q}^b + N_{A,1} X N_{A,2}$ couples the unknown ephemeral matrices $N_{A,1}, N_{A,2} \in J(A)$ with the private powers $\tilde{P}^a, \tilde{Q}^b$ across the off-diagonal blocks of X, $\pi(N_A)$ injects unknown bilinear terms into the diagonal projection. Second, because $\tilde{P} = e_P P$ and $\tilde{Q} = e_Q Q$ are confined by non-trivial orthogonal idempotents, $\pi(\tilde{P})$ and $\pi(\tilde{Q})$ are zero-divisors in $S \times R$ with vanishing determinants. Thus, multiplicative inversion and discrete logarithm reductions over $U(S) \times U(R)$ are algebraically undefined, forcing the adversary to solve the coupled polynomial equations over the full ring A. □

Proposition 2 (Obstruction of Centralizer Linearization and Shpilrain–Ushakov Inversion)**.** *Let $A = (S, R, M, 0)_{\varphi,\psi}$ be a bi-skew generalized triangular matrix ring with non-trivial automorphisms $\varphi \neq \mathrm{id}_S$ and $\psi \neq \mathrm{id}_R$. The centralizer $\mathrm{Cent}_A(\tilde{P}) = \{Y \in A \mid Y\tilde{P} = \tilde{P}Y\}$ is a non-linear algebraic variety rather than a linear subspace, and any idempotent-confined surrogate matrix $Y_1 \in e_P \mathrm{Cent}_A(\tilde{P}) e_P$ satisfies $\det(Y_1) = 0$, completely disabling Shpilrain and Ushakov's decomposition attack [14].*

Proof. Let $Y = \begin{pmatrix} s_Y & m_Y \\ 0 & r_Y \end{pmatrix}$ and $\tilde{P} = \begin{pmatrix} s_{\tilde{P}} & m_{\tilde{P}} \\ 0 & r_{\tilde{P}} \end{pmatrix}$. The commuting condition $Y\tilde{P} = \tilde{P}Y$ under Equation (1) implies:

$$\varphi(s_Y)m_{\tilde{P}} + m_Y\psi(r_{\tilde{P}}) = \varphi(s_{\tilde{P}})m_Y + m_{\tilde{P}}\psi(r_Y). \tag{6}$$

Because $\varphi(s_Y) = s_Y^{p^c}$ and $\psi(r_Y) = r_Y^{p^d}$ are non-linear for $c, d \geq 1$, Equation (6) contains terms of degree p^c and p^d in the coordinates of s_Y and r_Y. Thus, $\mathrm{Cent}_A(\tilde{P})$ is not a linear subspace.

Furthermore, Shpilrain and Ushakov's attack requires finding surrogate matrices Y_1, Y_2 satisfying $Y_1XY_2 = U_{\text{Alice}} - N_A$ and subsequently computing Y_1^{-1} to recover K. Due to the unknown nilpotent shift $N_A \in J(A)$, expanding the bimodule block of $Y_1XY_2 + N_A = U_{\text{Alice}}$ yields:

$$m_U = \varphi(s_{Y_1})\big(\varphi(s_X)m_{Y_2} + m_X\psi(r_{Y_2})\big) + m_{Y_1}\psi(r_Xr_{Y_2}) + m_{N_A},$$

which couples non-linear automorphism powers with unknown nilpotent coordinates m_{N_A}, defeating Gaussian elimination. Crucially, even if an adversary could solve this non-linear system to obtain $Y_1 \in e_PAe_P$, the orthogonality relation $e_P\bar{e}_P = 0$ ensures that $Y_1\bar{e}_P = 0$. Hence, Y_1 is a strict zero-divisor with $\det(Y_1) = 0$, and the required inverse Y_1^{-1} does not exist in A. □

Proposition 3 (Obstruction of Minimal Polynomial Linearization)**.** *The minimal polynomial attack developed by Mullan [9] against Stickel schemes cannot efficiently compute K in $A = (S, R, M, 0)_{\varphi,\psi}$ without solving an entangled, underdetermined multivariate system.*

Proof. In classical matrix rings over commutative fields, an adversary computes the minimal polynomial $\mu_P(\lambda)$ of P, expressing P^a as a linear combination $\sum_{i=0}^{d_P-1} c_iP^i$, where $d_P = \deg(\mu_P) \leq \dim(A)$. In the original Stickel scheme, this allows rewriting $U_{\text{Alice}} = P^aXQ^b$ as a purely linear system:

$$U_{\text{Alice}} = \sum_{i=0}^{d_P-1}\sum_{j=0}^{d_Q-1} c_ie_j(P^iXQ^j),$$

from which the scalar coefficients can be recovered via standard Gaussian elimination.

In contrast, within the bi-skew ring A under Algorithm 1, matrix multiplication twists entries by φ and ψ and adds the nilpotent mask $N_A \in J(A)$. Computing $\tilde{P}^iX\tilde{Q}^j$ in A involves the recursive bi-skew bimodule mapping:

$$(\tilde{P}^iX\tilde{Q}^j)_{12} = \varphi(s_{\tilde{P}}^i)\left[\varphi(s_X)m_{\tilde{Q}^j} + m_X\psi(r_{\tilde{Q}}^j)\right] + m_{\tilde{P}^i}\psi(r_Xr_{\tilde{Q}}^j).$$

When substituting the polynomial representation into $U_{\text{Alice}} = \tilde{P}^aX\tilde{Q}^b + N_A$, the unknowns c_i and e_j cannot be factored out linearly because the outer multiplication in A applies φ non-trivially across linear combinations:

$$\varphi\left(\sum_i c_is_{\tilde{P}}^i\right) = \sum_i c_i^{p^c}\varphi(s_{\tilde{P}}^i) \neq \sum_i c_i\varphi(s_{\tilde{P}}^i),$$

and the unknown coordinates of $N_{A,1}, N_{A,2}$ introduce additional bilinear cross-terms $c_i^{p^c}n_{A,2}$ and $n_{A,1}e_j^{p^d}$. Consequently, the system in terms of $(c_i, e_j, N_{A,1}, N_{A,2})$ transforms into a high-degree, heavily underdetermined multivariate polynomial system over $\mathbb{F}_{p^k}$, completely obstructing Mullan's linearization. □

4.3 Endomorphism Parameterization and Resistance against Gröbner Basis Attacks

The algebraic security of the proposed scheme critically hinges on the hardness of solving the underlying multivariate quadratic (MQ) system generated within the bimodule M and radical $J(A)$. In general, an algebraic adversary attempting to solve the non-linear key relation:

$$(U_{\text{Alice}})_M = \varphi^2(U_S)\varphi(X_S)V_M + \varphi(U_S)X_M\psi(V_R) + U_M\psi(X_R)\psi^2(V_R) + (N_A)_M \tag{7}$$

by deploying exact Gröbner basis algorithms such as Faugère's F_4 or F_5 faces an arithmetic complexity governed by the degree of regularity (D_{reg}) of the polynomial ideal, scaling as:

$$\mathcal{O}\left(\binom{N_v + D_{\text{reg}}}{D_{\text{reg}}}^{\omega}\right) \tag{8}$$

where N_v denotes the total number of unknown variables (combining exponent bits and nilpotent perturbation coordinates) over the base field, and $2 \leq \omega \leq 3$ is the linear algebra constant.

To enforce generic non-linear behavior, prevent low-degree Syzygies, and maximize D_{reg}, the endomorphisms $\varphi \in \text{End}(S)$ and $\psi \in \text{End}(R)$ must be strictly parameterized under the following algebraic constraints:

1. **Proper Galois Extension Condition:** Let $S = M_n(\mathbb{F}_{p^k})$ and $R = M_m(\mathbb{F}_{p^t})$, where the endomorphisms act entrywise via Frobenius powers $\varphi = \sigma^{r_1}$ and $\psi = \sigma^{r_2}$ with $\sigma(x) = x^p$. We strictly require:

$$\gcd(r_1, k) = 1 \quad \text{and} \quad \gcd(r_2, t) = 1. \tag{9}$$

   This prevents the existence of proper intermediate subfields $\mathbb{F}_{p^d} \subsetneq \mathbb{F}_{p^k}$ that remain pointwise fixed under φ or ψ ($\text{Fix}(\varphi) = \mathbb{F}_p$). Consequently, the adversary is barred from applying fixed-point or subfield-trace attacks to project the MQ system into lower-dimensional quotient rings.

2. **Asymmetric Orbit Disjointness:** In the heterogeneous setting where S and R are defined over coprime Galois extensions (i.e., $[\mathbb{F}_{p^k} : \mathbb{F}_p]$ and $[\mathbb{F}_{p^t} : \mathbb{F}_p]$ with $\gcd(k, t) = 1$), we strictly enforce $\gcd(\text{ord}(\varphi), \text{ord}(\psi)) = 1$. In the homogeneous setting ($S \cong R$), we enforce independent generator selection such that $\langle\varphi\rangle \cap \langle\psi\rangle = \{\text{id}\}$ is avoided unless φ and ψ generate non-conjugate cyclic subactions with disparate Frobenius shift parameters, precluding simultaneous diagonalization via twisted Kronecker linearization.

3. **Suppression of Dembowski-Ostrom Differentials:** To thwart differential algebraic attacks, the characteristic p is chosen odd, or, in case $p = 2$, the extension degree k must be a prime ≥ 127 with $r_i \geq 3$. This constraint avoids low Hamming weight Frobenius automorphisms which inherently produce linear Lie derivatives of the form $D_a f(x) = f(x + a) - f(x) - f(a)$, thereby preserving the non-linearity of the system.

4. **Radical Isolation of Base Generators:** While ephemeral masks N_A, N_B are drawn from $J(A)$, the active base components $\tilde{P}$ and $\tilde{Q}$ must strictly satisfy:

$$(\tilde{P} - e_P) \notin J(A) \quad \text{and} \quad (\tilde{Q} - e_Q) \notin J(A), \tag{10}$$

guaranteeing that their multiplicative powers within $e_P A e_P$ and $e_Q A e_Q$ achieve maximal exponential period and do not collapse into linear modular expressions.

4.4 Heuristic Complexity and Cryptographic Assumptions

Lemma 1 (Power Formula in Bi-Skew Rings)**.** *Let* $P = \begin{pmatrix} s_P & m_P \\ 0 & r_P \end{pmatrix} \in A$*. For any positive integer* $n \geq 1$*, the* n*-th power of* P *under the bi-skew multiplication rule is:*

$$P^n = \begin{pmatrix} s_P^n & \mu_n \\ 0 & r_P^n \end{pmatrix}, \quad \text{where} \quad \mu_n = \sum_{i=0}^{n-1} s_P^{(n-1-i)p^c} m_P r_P^{ip^d}. \tag{11}$$

Proof. We proceed by induction on n. For $n = 1$, $\mu_1 = s_P^0 m_P r_P^0 = m_P$, which holds. Assume the formula holds for $n = k$:

$$P^k = \begin{pmatrix} s_P^k & \mu_k \\ 0 & r_P^k \end{pmatrix}.$$

Then by the bi-skew multiplication rule (1):

$$\begin{aligned} P^{k+1} = P \cdot P^k &= \begin{pmatrix} s_P & m_P \\ 0 & r_P \end{pmatrix} \begin{pmatrix} s_P^k & \mu_k \\ 0 & r_P^k \end{pmatrix} \\ &= \begin{pmatrix} s_P^{k+1} & \varphi(s_P)\mu_k + m_P \psi(r_P^k) \\ 0 & r_P^{k+1} \end{pmatrix}. \end{aligned}$$

Since $\varphi(x) = x^{p^c}$ and $\psi(y) = y^{p^d}$, substituting $\mu_k = \sum_{i=0}^{k-1} s_P^{(k-1-i)p^c} m_P r_P^{ip^d}$ yields:

$$\begin{aligned} \varphi(s_P)\mu_k + m_P \psi(r_P^k) &= s_P^{p^c} \left(\sum_{i=0}^{k-1} s_P^{(k-1-i)p^c} m_P r_P^{ip^d} \right) + m_P r_P^{kp^d} \\ &= \sum_{i=0}^{k-1} s_P^{(k-i)p^c} m_P r_P^{ip^d} + s_P^0 m_P r_P^{kp^d} = \sum_{i=0}^{k} s_P^{(k-i)p^c} m_P r_P^{ip^d} = \mu_{k+1}. \end{aligned}$$

This completes the induction. □

Decomposing private exponents $a = \sum_{j=0}^{n-1} x_j 2^j$ ($x_j \in \{0, 1\}$) together with the unknown entries of the nilpotent perturbations $N_A, N_B \in J(A)$ yields a multivariate polynomial system over $\mathbb{F}_{p^k}$. While the general decision Multivariate Quadratic (MQ) problem over finite fields is NP-complete [6], average-case hardness is a standard cryptographic intractability assumption:

Hardness Assumption 1 (Hardened Bi-Skew Key Extraction Hardness)**.** *Given public parameters* $A = (S, R, M, 0)_{\varphi,\psi}$*,* $P, Q, X \in A$*, orthogonal idempotents* e_P, e_Q*, and nilpotent-perturbed exchange matrices* $U_{\text{Alice}} = \tilde{P}^a X \tilde{Q}^b + N_A$ *and* $U_{\text{Bob}} = \tilde{P}^u X \tilde{Q}^v + N_B$*, there exists no probabilistic polynomial-time (PPT) classical or quantum algorithm that computes* $K = \tilde{P}^{a+u} X \tilde{Q}^{b+v}$ *with non-negligible probability.*

Gröbner Basis Asymptotics: Under the conservative heuristic assumption that the non-linear algebraic system generated by the Frobenius cross-terms in μ_n and the nilpotent perturbation variables in N_A behaves like a semi-regular sequence, computing a Gröbner basis via Faugère's F_4/F_5 algorithms [7] requires:

$$T_{\text{Gröbner}} = \mathcal{O}\left(\binom{n + d_{\text{reg}}}{d_{\text{reg}}}^{\omega} \right)$$

where $n = 256$ is the number of boolean variables representing key and perturbation bits, $\omega \approx 2.81$ is the linear algebra exponent, and $d_{\text{reg}} \geq \frac{n}{2} + 1 = 129$ denotes the generic degree of regularity. Evaluating the precise empirical degree of regularity under structured Frobenius endomorphisms remains an open problem.

Quantum Bounds: Shor's algorithm [13] is inapplicable because A is non-commutative, the idempotent-confined generators are non-invertible zero-divisors, and the underlying bilateral action is non-abelian. Under Grover's search, the BBBV theorem [3] establishes a lower query bound of $\Omega(\sqrt{|\mathcal{K}|}) = \Omega(2^{128})$ operations for $|\mathcal{K}| \geq 2^{256}$.

Table 1: Parameter Specifications and Cryptographic Security Levels.

Security Level	p	k	**Key Size**	**Space** $\lvert\mathcal{K}\rvert$	**Classical Hardness**	**Quantum Queries**
Toy (Illustration)	2	16	16 bits	2^{16}	$\mathcal{O}(2^{16})$	$\mathcal{O}(2^{8})$
NIST Category 1	2	128	128 bits	2^{256}	$\mathcal{O}(2^{143})$	$\Omega(2^{64})$
NIST Category 5	2	256	256 bits	2^{512}	$\mathcal{O}(2^{285})$	$\Omega(2^{128})$

Table 2: Qualitative Comparison with Standard Post-Quantum Cryptographic Families.

Scheme Family	**Underlying Hard Problem**	**Key Size**	**Linearization / Projection Risk**	**Shor Immunity**
Lattice-based (ML-KEM)	Module-LWE / Module-SIS	Medium	Low	Yes
Code-based (McEliece)	Syndrome Decoding	Very Large	Low	Yes
Multivariate (Rainbow)	Multivariate Quadratic (MQ)	Large	High (Oil-Vinegar breaks)	Yes
Isogeny-based (CSIDH)	Group Action on Elliptic Curves	Compact	Medium (Kuperberg attacks)	Yes
Bi-Skew Ring (Ours)	**Perturbed Bi-Skew Non-Abelian CDH**	**Compact**	**Resistant (Idempotent +** $J(A)$ **Masking)**	**Yes**

Prototype Implementation and Computational Benchmarks: To validate execution practicality, the hardened protocol was implemented in a reference Python/SageMath prototype on a standard workstation (Intel Core i7-11800H @ 2.30 GHz, 16 GB RAM). For dimension $n = 256$ bits over Galois extensions, the ephemeral key generation $(U_{\text{Alice}}, U_{\text{Bob}})$ including nilpotent masking executed in an average of 4.4 ms, while shared secret derivation required 6.9 ms. Total key agreement exchange completes in under 12 ms, demonstrating minimal computational overhead. To empirically corroborate Propositions 1–3, we conducted experimental cryptanalytic benchmarks using a reference SageMath implementation comparing the classical Stickel key exchange against our hardened bi-skew formulation under identical field parameters ($\mathbb{F}_{16}$). Under Mullan's minimal polynomial linearization attack, the classical scheme was completely compromised in under 2 ms via standard Gaussian elimination. In contrast, when evaluated against our hardened bi-skew structure, the Frobenius automorphisms (φ, ψ) and nilpotent radical shifts $N_A \in J(A)$ systematically corrupt the linear independence of the evaluated terms, yielding an inconsistent linear system (0 valid key reconstructions).

5 Concealed Data Encapsulation (DEM) via Radić's Right-Invertibility: A Kernel-Confined Countermeasure to Canonical Projection

While Section 2 neutralizes the canonical projection homomorphism $\pi : A \to S \times R$ during key exchange through idempotent confinement and nilpotent masking, the internal ideal structure of $A = (S, R, M, 0)_{\varphi,\psi}$ offers a second, even more direct architectural

countermeasure for payload transmission. Specifically, because the kernel of the canonical projection is the upper-right bimodule ideal:

$$\ker(\pi) = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix} \subseteq J(A),$$

any cryptographic primitive that embeds its secret carrier exclusively within the upper-right bimodule component M is inherently invisible to π.

In this section, we construct a lightweight, high-throughput Data Encapsulation Mechanism (DEM) that exploits this kernel confinement over rectangular bimodules ${}_SM_R$. By utilizing Radić's right-invertibility over modular matrix rings, the shared rectangular bimodule block $m \in M$ acts as a private dimension-expanding trapdoor, enabling deterministic message unmasking while presenting both an annihilated projection image and an algebraically intractable kernel barrier to unauthorized eavesdroppers.

5.1 The Secret-Carrier DEM Framework, Kernel Confinement, and Dimensional Expansion

The rectangular key $m \in M_{a\times b}(T)$ is extracted directly as the upper-right bimodule block of the shared secret matrix $K = \tilde{P}^{a+u} X \tilde{Q}^{b+v} \in A$:

$$K = \begin{pmatrix} s_K & m \\ 0 & r_K \end{pmatrix}, \quad m \in M_{a\times b}(T).$$

Because K is established via the hardened bi-skew key exchange of Algorithm 1, the rectangular matrix m is entirely secret and unobservable by passive eavesdroppers.

Proposition 4 (Kernel Confinement and Absolute Projection Immunity)**.** *Let* $K = \begin{pmatrix} s_K & m \\ 0 & r_K \end{pmatrix} \in A$ *be the master secret matrix and let* $Z = \begin{pmatrix} s_Z & C_i \\ 0 & r_Z \end{pmatrix} \in A$ *be any matrix representation encapsulating the ciphertext block* $C_i = P_i m$ *in the bimodule component. Applying the canonical projection homomorphism* $\pi : A \to S \times R$ *annihilates both the secret rectangular key* m *and the encapsulated payload* C_i *identically to zero.*

Proof. Decompose $K = D_K + M_K$, where $D_K = \begin{pmatrix} s_K & 0 \\ 0 & r_K \end{pmatrix}$ is the diagonal component and $M_K = \begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix} = e_1 K e_2$ is the bimodule carrier. Since $M_K \in \ker(\pi) = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix}$, evaluating π yields:

$$\pi(K) = \pi(D_K) + \pi(M_K) = (s_K, r_K) + (0, 0) = (s_K, r_K).$$

Similarly, for any matrix Z carrying $C_i = P_i m$ in its $(1,2)$-entry, $\pi(Z) = (s_Z, r_Z)$, mapping C_i identically to zero. Consequently, homomorphic projection onto $S \times R$ strips away the entire secret carrier and yields zero mutual information regarding m or P_i. The adversary is therefore forced to attack the bimodule equation $C_i = P_i m$ directly within $\ker(\pi)$. □

Beyond its immunity to canonical projection, a distinctive cryptographic feature of this construction is its dimensional expansion: the encryption function maps an a-dimensional plaintext vector $P_i \in M_{1\times a}(T)$ ($a = 2$) into a higher b-dimensional ciphertext vector $C_i = P_i m \in M_{1\times b}(T)$ ($b = 3$). This transformation injects structured algebraic redundancy, expanding two plaintext characters into three ciphertext characters.

This dimensional mismatch diffuses statistical character frequencies across higher dimensions, introduces non-linear coordinate diffusion, and establishes an affine kernel coset $|\ker(m)| = (p^e)^{a(b-a)}$ that prevents direct inversion without the private Radić trapdoor m_R.

Definition 1 (Radić's Right-Invertibility over Modular Rings [11, 12])**.** *An $a \times b$ matrix $m \in M_{a\times b}(T)$ with $a < b$ over a commutative ring with unity T admits a Radić right inverse $m_R \in M_{b\times a}(T)$ satisfying $mm_R = I_a$ provided $\det(mm^T) \in U(T)$, given explicitly by:*

$$m_R = m^T(mm^T)^{-1}. \tag{12}$$

5.2 Encryption and Decryption Cycle

Let $T = \mathbb{Z}_{27}$, $a = 2$, and $b = 3$. Characters are mapped via the standard encoding:

$$\text{Space} \mapsto 0, \quad \text{A} \mapsto 1, \quad \text{B} \mapsto 2, \quad \ldots, \quad \text{Z} \mapsto 26.$$

Plaintext is partitioned into 2-dimensional row vectors $P_i \in M_{1\times 2}(\mathbb{Z}_{27})$.

- **Encryption (Dimensional Expansion $2 \to 3$):**

$$C_i = P_i m \in M_{1\times 3}(\mathbb{Z}_{27}). \tag{13}$$

- **Decryption (Dimensional Collapse $3 \to 2$):**

$$C_i m_R = P_i(mm_R) = P_i I_2 = P_i.$$

Example 2. *Let the secret upper-right block derived from K be:*

$$m = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \in M_{2\times 3}(\mathbb{Z}_{27}).$$

We compute $mm^T = \begin{pmatrix} 5 & 4 \\ 4 & 6 \end{pmatrix}$, $\det(mm^T) \equiv 14 \pmod{27}$. Since $\gcd(14, 27) = 1$, $14 \in U(\mathbb{Z}_{27})$ with $14^{-1} \equiv 2 \pmod{27}$, and the Radić inverse evaluates to:

$$m_R = m^T(mm^T)^{-1} = \begin{pmatrix} 16 & 21 \\ 23 & 12 \\ 19 & 10 \end{pmatrix} \in M_{3\times 2}(\mathbb{Z}_{27}).$$

Encrypting `"ATTACK SOON"` under Equation (13) partitions the 11-character string (padded to 12 characters with an additional space: `"ATTACK SOON "`) into 6 pairs of 2-dimensional row vectors, producing 6 triplets of ciphertext characters (18 characters total):

$$\textit{Ciphertext} = \texttt{VNTNV_AQYKN_ANZGW_}.$$

Multiplying each 3-dimensional block C_i by m_R from the right collapses the dimension back to 1×2, restoring P_i with zero decryption error.

Remark 2 (Real-World Deployment Scaling)**.** *The choice $a = 2$, $b = 3$ over $\mathbb{Z}_{27}$ in Example 2 is strictly pedagogical. In production deployments, parameters must satisfy $(p^e)^{a(b-a)} \geq 2^{256}$ (e.g., $a = 16$, $b = 32$ over $\mathbb{Z}_{256}$) to ensure the affine kernel coset $|\ker(m)|$ is intractable against underdetermined algebraic reconstruction [1].*

Open Cryptographic Challenge 2 (Open Rectangular Ciphertext Pedagogical Micro-Benchmark)**.** *Let $T = \mathbb{Z}_{27}$, $a = 2$, and $b = 3$. An authentic payload has been encrypted under an unknown private rectangular block $m \in M_{2\times 3}(\mathbb{Z}_{27})$ confined within* $\ker(\pi)$*, yielding the 18-character ciphertext stream:*

`STPEDSG_WPU_UNTAU_`

This challenge is provided strictly as a pedagogical micro-benchmark for algorithmic validation and character-frequency diffusion testing. (For production deployment parameters resisting algebraic brute-force, refer to Remark 2 with $a \geq 16, b \geq 32$ over $\mathbb{Z}_{256}$). We invite researchers to formulate linear programming or kernel-coset search routines to recover m without prior access to the master key K.

Algorithm 2 Secret-Carrier DEM via Radić Right-Invertibility

Require: Master secret matrix $K = \begin{pmatrix} s_K & m \\ 0 & r_K \end{pmatrix} \in A$, plaintext blocks $P_i \in M_{1\times a}(T)$.

Ensure: Decrypted plaintext blocks identical to P_i. **Trapdoor Derivation (Off-line within** $\ker(\pi)$**):**

1: Extract rectangular bimodule key $m \in M_{a\times b}(T)$ $(a < b)$ via $e_1 K e_2$.
2: Compute Gram-type matrix $G = mm^T \in M_{a\times a}(T)$.
3: Verify $\det(G) \in U(T)$; abort if non-invertible.
4: Compute private Radić right inverse: $m_R = m^T(mm^T)^{-1} \in M_{b\times a}(T)$. **Encryption (Dimensional Expansion $a \to b$):**
5: **for** each plaintext block $P_i \in M_{1\times a}(T)$ **do**
6: Transmit ciphertext block: $C_i = P_i m \in M_{1\times b}(T)$.
7: **end forDecryption (Dimensional Collapse $b \to a$):**
8: **for** each ciphertext block $C_i \in M_{1\times b}(T)$ **do**
9: Recover: $P_i' = C_i m_R = P_i(mm_R) = P_i I_a = P_i$.
10: **end for**
11: **return** Recovered payload $\{P_i\}$.

6 Conclusion and Future Perspectives

In this paper, we introduced Bi-Skew Generalized Triangular Matrix Rings $A = (S, R, M, 0)_{\varphi,\psi}$ and established a complete characterization of their Jacobson radical $J(A)$. Recognizing that naive exponentiation in triangular rings is susceptible to canonical projection attacks onto the diagonal subrings, we developed two complementary ring-theoretic countermeasures: (1) In Section 2, we hardened the Stickel-type key exchange protocol directly by integrating orthogonal idempotents (e_P, e_Q) and ephemeral nilpotent perturbations ($N \in J(A)$ with $N^2 = 0$), proving that the nilpotent masks vanish identically for legitimate parties while simultaneously destroying homomorphic projection, centralizer linearization, Shpilrain–Ushakov matrix inversion, and Mullan's minimal polynomial attack; and (2) In Section 5, we formulated a Data Encapsulation Mechanism (DEM) via Radić's right-invertibility that embeds the secret rectangular carrier completely inside the projection kernel $\ker(\pi)$, combining absolute projection immunity with dimensional expansion ($2 \to 3$ vector mapping). Finally, we posed two open cryptographic challenge problems to stimulate community cryptanalysis.

6.1 Limitations and Open Questions

While our structural analysis establishes resistance to existing projection and linearization attacks, several open questions remain: (1) The empirical degree of regularity of the derived MQ systems under nilpotent perturbation requires extensive computer-algebra benchmarking across small-field instances. (2) Establishing an average-case reduction from a standard lattice or generic non-abelian group problem remains an open theoretical goal. (3) Active security (IND-CCA2) requires integrating Fujisaki-Okamoto transform variants over A.

Epilogue: An Algebraic Bridge to Applied Cryptography

The theoretical constructs and structural theorems articulated throughout this work reflect the authors' primary grounding and perspective within pure abstract algebra and ring theory. It is not our intention to present this framework as a monolithic or production-ready cryptographic standard; rather, our objective has been to erect a rigorous, non-commutative algebraic foundation—the bi-skew generalized triangular matrix ring—and to reveal how its bilateral twisting dynamics, idempotent decompositions, and Jacobson radical ideal structure inherently frustrate traditional linearization, homomorphic projection, centralizer decompositions, and minimal polynomial attacks.

In formalizing these primitives and introducing our open challenges, we extend a sincere invitation to the applied cryptography and post-quantum security communities. Transformative scientific progress is seldom realized in isolation; it thrives at the fertile intersection of disciplines, where abstract algebraic paradigms are scrutinized, challenged, and refined by algorithmic cryptanalysts. We submit this work not as a final pronouncement, but as an open conduit for interdisciplinary collaboration. It is our earnest hope that this algebraic architecture serves as a catalyst for future joint inquiry, offering a resilient stepping stone toward post-quantum frameworks designed for the enduring protection of humanity's collective computational and communications infrastructure.

Author Contributions

M.A.F. and R.M.S. conceptualized the study and developed the mathematical methodology. M.A.F. wrote the main manuscript text and implemented the computational verification in SageMath. H.A.M. and R.M.S. performed the formal algebraic analysis and contributed to the design of the cryptographic protocol. All authors reviewed and approved the final manuscript.

Declaration of Generative AI and AI-Assisted Technologies

During the preparation of this work, the authors utilized Gemini (Google DeepMind) as an advanced AI collaborator to assist in verifying combinatorial equations and refining the academic English phrasing. All ring-theoretic proofs, the definition of the bi-skew generalized triangular matrix ring, and the overarching cryptographic protocol were independently conceptualized and authored by the human researchers, who assume full academic responsibility for the integrity and validity of the published results.

Funding Declaration

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data Availability

All data generated or analyzed during this study, including the executable SageMath verification scripts and cryptographic benchmark parameters, are included in this published article.

A SageMath Verification of Linearization Obstruction

To uphold the highest standards of scientific reproducibility and provide concrete empirical verification for the theoretical claims established in Propositions 1–3, this appendix provides a self-contained reference implementation in SageMath.

The rationale for providing this computational artifact is twofold:

1. **Demonstration of the Classical Vulnerability:** We establish a concrete cryptanalytic baseline by implementing Mullan's minimal polynomial linearization attack [9] against the original, untwisted Stickel key exchange protocol [15] over the finite field $\mathbb{F}_{16}$. This confirms that under standard bilinear assumptions, the shared secret matrix is fully compromised via ordinary Gaussian elimination in less than 2 ms.

2. **Validation of the Hardened Bi-Skew Defense Mechanism:** Under identical field parameters and private exponents, we deploy the identical cryptanalytic routine against our proposed bi-skew generalized triangular matrix ring with radical perturbation. The script explicitly demonstrates how the bilateral Frobenius endomorphisms (φ, ψ) and radical shifts dismantle the scalar linearity of the evaluated powers, transforming the linear system into an overdetermined, inconsistent matrix over $\mathbb{F}_{16}$ (0 valid key solutions).

By publishing this executable benchmark, we bridge pure algebraic ring theory with applied algorithmic cryptanalysis, enabling independent researchers and referees to directly confirm that the obstruction to linearization is an active computational barrier rather than merely an asymptotic hypothesis.

```
# ============================================================================
# Simulation: Minimal Polynomial Linearization Attack (Mullan Attack)
# Comparing Classical Stickel Protocol vs. Hardened Bi-Skew Matrix Ring Protocol
# Authors: Mohamed A. Farahat, Refaat M. Salem, Hanan A. Mohamed
# ============================================================================

import time

print("=" * 70)
print("PHASE 1: SIMULATING THE CLASSICAL STICKEL SCHEME (NO TWIST)")
```

```
print("=" * 70)

# Base Field: F_16
F.<beta> = GF(2^4, modulus=x^4 + x + 1)
MS = MatrixSpace(F, 2, 2)

# Public invertible matrices P, Q, X (Non-commuting)
P_classical = MS([[beta, 1], [0, beta^2]])
Q_classical = MS([[beta^3, beta], [0, beta]])
X_classical = MS([[1, beta^2], [0, beta]])

# Alice and Bob private exponents
a_sec, b_sec = 5, 7
u_sec, v_sec = 3, 11

# Public exchange values
U_Alice_classical = (P_classical^a_sec) * X_classical * (Q_classical^b_sec)
U_Bob_classical   = (P_classical^u_sec) * X_classical * (Q_classical^v_sec)

# True Shared Secret Key
K_true_classical = (P_classical^a_sec) * U_Bob_classical * (Q_classical^b_sec)

deg_P = P_classical.minimal_polynomial().degree() # degree = 2
deg_Q = Q_classical.minimal_polynomial().degree() # degree = 2

# Linear System Setup: deg_P * deg_Q = 4 unknowns
A_matrix_rows = []
for i in range(deg_P):
    for j in range(deg_Q):
        basis_mat = (P_classical^i) * X_classical * (Q_classical^j)
        col = [basis_mat[0,0], basis_mat[0,1], basis_mat[1,0], basis_mat[1,1]]
        A_matrix_rows.append(col)

A_sys = Matrix(F, A_matrix_rows).transpose()
b_target = vector(F, [U_Alice_classical[0,0], U_Alice_classical[0,1],
                      U_Alice_classical[1,0], U_Alice_classical[1,1]])

z_solution = A_sys.solve_right(b_target)

# Key Reconstruction in Classical Scheme
K_attacker_classical = MS(0)
idx = 0
for i in range(deg_P):
    for j in range(deg_Q):
        K_attacker_classical += z_solution[idx] * ((P_classical^i) * U_Bob_classical
        idx += 1

print(f"Classical Attack Success: {K_attacker_classical == K_true_classical}")
```

```
assert K_attacker_classical == K_true_classical

print("=" * 70)
print("PHASE 2: SIMULATING THE HARDENED BI-SKEW GENERALIZED RING PROTOCOL")
print("=" * 70)

# Define Bi-Skew multiplication rule:
# (s1, m1, r1) * (s2, m2, r2) = (s1*s2, phi(s1)*m2 + m1*psi(r2), r1*r2)
def phi(s):
    return s^2  # Frobenius on F_4 (or left action)

def psi(r):
    return r^4  # Frobenius on F_16

def bi_skew_mult(M1, M2):
    s1, m1, r1 = M1[0], M1[1], M1[2]
    s2, m2, r2 = M2[0], M2[1], M2[2]
    s_new = s1 * s2
    m_new = phi(s1) * m2 + m1 * psi(r2)
    r_new = r1 * r2
    return (s_new, m_new, r_new)

def bi_skew_add(M1, M2):
    return (M1[0] + M2[0], M1[1] + M2[1], M1[2] + M2[2])

def bi_skew_pow(M, exp):
    res = (F(1), F(0), F(1))
    base = M
    for _ in range(exp):
        res = bi_skew_mult(res, base)
    return res

# Base elements and ephemeral nilpotent perturbations N_A, N_B in J(A)
P_biskew = (F(beta^5), F(1), F(beta^2))
Q_biskew = (F(beta^10), F(beta^3), F(beta))
X_biskew = (F(1), F(beta^2), F(beta))
N_A_mask = (F(0), F(beta^7), F(0))
N_B_mask = (F(0), F(beta^11), F(0))

# Key exchange under Bi-Skew action with nilpotent perturbation
P_a = bi_skew_pow(P_biskew, a_sec)
Q_b = bi_skew_pow(Q_biskew, b_sec)
U_Alice_core = bi_skew_mult(bi_skew_mult(P_a, X_biskew), Q_b)
U_Alice_biskew = bi_skew_add(U_Alice_core, N_A_mask)

P_u = bi_skew_pow(P_biskew, u_sec)
Q_v = bi_skew_pow(Q_biskew, v_sec)
U_Bob_core = bi_skew_mult(bi_skew_mult(P_u, X_biskew), Q_v)
```

```
U_Bob_biskew = bi_skew_add(U_Bob_core, N_B_mask)

# Derived shared secret key (after radical annihilation)
K_Alice_biskew = bi_skew_mult(bi_skew_mult(P_a, U_Bob_core), Q_b)
K_Bob_biskew   = bi_skew_mult(bi_skew_mult(P_u, U_Alice_core), Q_v)
assert K_Alice_biskew == K_Bob_biskew

# Attacker attempts Gaussian Elimination Linearization against Bi-Skew structure
A_biskew_rows = []
for i in range(deg_P):
    for j in range(deg_Q):
        P_i = bi_skew_pow(P_biskew, i)
        Q_j = bi_skew_pow(Q_biskew, j)
        term = bi_skew_mult(bi_skew_mult(P_i, X_biskew), Q_j)
        A_biskew_rows.append([term[0], term[1], term[2]])

A_biskew_sys = Matrix(F, A_biskew_rows).transpose()
b_biskew_target = vector(F, [U_Alice_biskew[0], U_Alice_biskew[1], U_Alice_biskew[2]]

attack_failed = False
try:
    z_biskew_sol = A_biskew_sys.solve_right(b_biskew_target)
    K_fake = (F(0), F(0), F(0))
    idx = 0
    for i in range(deg_P):
        for j in range(deg_Q):
            P_i = bi_skew_pow(P_biskew, i)
            Q_j = bi_skew_pow(Q_biskew, j)
            term = bi_skew_mult(bi_skew_mult(P_i, U_Bob_biskew), Q_j)
            K_fake = (K_fake[0] + z_biskew_sol[idx]*term[0],
                      K_fake[1] + z_biskew_sol[idx]*term[1],
                      K_fake[2] + z_biskew_sol[idx]*term[2])
            idx += 1
    if K_fake != K_Alice_biskew:
        attack_failed = True
except ValueError:
    attack_failed = True

print(f"Bi-Skew Linearization Attack Success: {not attack_failed}")
```

References

[1] R. B. Bapat, Outer inverses: determinants and linear equations, *Linear Algebra and its Applications*, 211:77–85, 1994.

[2] E. Barker, Recommendation for Key Management: Part 1 – General, *NIST Special Publication 800-57 Part 1 Rev. 5*, National Institute of Standards and Technology, 2020.

[3] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, Strengths and weaknesses of quantum computing, *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[4] G. F. Birkenmeier, J. K. Park, and S. T. Rizvi, *Extensions of Rings and Modules*, Springer, New York, 2013.

[5] J. Chen, X. Yang, and Y. Zhou, On strongly clean matrix and triangular matrix rings, *Communications in Algebra*, 34(10):3659–3674, 2006.

[6] J. Ding and B.-Y. Yang, Multivariate public key cryptography, in *Post-Quantum Cryptography*, D. J. Bernstein et al., Eds., Springer, Berlin, Heidelberg, pp. 193–241, 2009.

[7] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F_4), *Journal of Pure and Applied Algebra*, 139(1-3):61–89, 1999.

[8] M. Mosca, Cybersecurity in an era with quantum computers: will we be ready?, *IEEE Security & Privacy*, 16(5):38–41, 2018.

[9] C. Mullan, On the cryptanalysis of Stickel's key exchange scheme, *International Journal of Computer Mathematics*, 89(18):2454–2466, 2012.

[10] A. Myasnikov, V. Shpilrain, and A. Ushakov, *Noncommutative Cryptography and Complexity of Group Theoretic Problems*, American Mathematical Society, Providence, RI, 2008.

[11] M. Radić, A definition of the determinant of a rectangular matrix, *Glasnik Matematički*, 1(21):17–22, 1966.

[12] M. Radić, On the invertibility of rectangular matrices, *Linear Algebra and its Applications*, 143:247–254, 1991.

[13] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[14] V. Shpilrain and A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient, *Applicable Algebra in Engineering, Communication and Computing*, 17(3-4):285–289, 2006.

[15] E. Stickel, A new method for exchanging secret keys, in *Proc. 3rd Int. Conf. on Information Technology and Applications (ICITA'05)*, IEEE, vol. 2, pp. 426–430, 2005.