Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 18** : 1–15.
ISSN-0037-8712
doi:10.5269/bspm.82996

Security Analysis of the Extended Grendel Permutation Over $\mathbb{Z}_{pq}$

Abdelkarim Lkoaiza and Seddik Abdelalim

ABSTRACT: We study the security of the extended grendel permutation defined over the ring $\mathbb{Z}_{pq}$, where $p \equiv q \equiv 3 \pmod 4$. The construction combines an arithmetic S-box derived from the quadratic residue symbol through the Chinese remainder theorem (CRT) based map L_{pq}, together with an MDS diffusion layer and round constants. This work complements our previous paper [1], which focused on the construction itself, by providing a systematic cryptographic analysis. Using the wide-trail strategy together with a decomposition induced by the CRT, we derive bounds against linear and differential cryptanalysis, examine resistance to integral distinguishers, and study algebraic attacks, including interpolation and preimage attacks. We also outline a polynomial-system modeling approach, supported by gröbner basis techniques, to evaluate the complexity of symbolic attacks related to the L_{pq} layer. Our results indicate that no low-complexity classical distinguishers arise in the considered attack models.

Keywords: Extended grendel, arithmetic S-box, MDS diffusion, linear cryptanalysis, differential cryptanalysis, integral attacks, algebraic attacks, gröbner bases.

Contents

1. Introduction

Hash functions based on the *sponge* construction, popularized by the Keccak family [8] and standardized through SHA-3, are today a central tool for data integrity, authentication, and blockchain applications [15]. In this setting, the practical security of a sponge function essentially depends on the robustness of its internal permutation: it must behave like a random permutation, resist the main classical distinguishers, and maintain good diffusion even in the presence of structured inputs.

2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted March 25, 2026. Published June 22, 2026.

In our previous work, entitled *An extended grendel approach applied to blockchain signature as an alternative to Keccak permutation*, we introduced an alternative arithmetic permutation inspired by SPN (Substitution–Permutation Network) designs, replacing the usual binary components by operations over the ring $\mathbb{Z}_{pq}$, where p and q are two odd prime numbers. Nonlinearity is provided by an arithmetic S-box built from the symbol L_{pq}, which generalizes the use of quadratic symbols (Legendre/Jacobi) [4] in a composite setting, while diffusion is obtained by an MDS layer and the injection of round constants. This approach pursues a double objective: (i) to propose an "arithmetized" primitive, compatible with proof-oriented cryptographic frameworks, and (ii) to offer a conceptual alternative to the Keccak model while retaining the sponge structure (absorption, permutation, squeezing) [17].

The present article focuses on an indispensable step: the security analysis of this *extended grendel* permutation over $\mathbb{Z}_{pq}$. More precisely, we evaluate its resistance against several families of classical attacks on sponge/SPN-type permutations [5]. We first study linear and differential cryptanalysis by combining the *wide-trail* argument with bounds on biases/probabilities at the S-box level, which yields complexity estimates as a function of the number of rounds N and the arithmetic parameters. We then examine the presence of *integral* distinguishers (zero-sum and propagation of substructures), adapting known principles over finite fields to the case of $\mathbb{Z}_{pq}$ via the CRT, which decomposes the study into two components modulo p and modulo q. Finally, we address algebraic attacks, including interpolation attacks, root-finding, and polynomial modeling, and we discuss the feasibility of gröbner-basis attacks by making explicit the system of equations induced by the rounds and by providing Macaulay-type complexity bounds.

Our main contribution is therefore a structured, attack-centered evaluation, highlighting the resistance mechanisms provided by (i) the arithmetic nonlinearity related to L_{pq}, (ii) MDS diffusion and the injection of constants [7], and (iii) the CRT decomposition, which is crucial as soon as one reasons over a non-integral ring. Beyond the bound results and the considered attack models, this study provides a reusable methodological framework to analyze other arithmetic permutations defined over composite rings and intended for sponge constructions.

The paper is organized as follows. Section 2 collects the preliminaries: notations, CRT, quadratic residues, the definition of L_{pq}, the S-box over $\mathbb{Z}_{pq}$, MDS diffusion and the description of the extended grendel permutation, as well as a recall of the MELP/MEDP quantities used to bound correlations and probabilities. Section 3 addresses linear and differential cryptanalysis. Section 4 is devoted to integral attacks. Section 5 discusses algebraic attacks. Section 6 analyzes polynomial-system modeling and gröbner-basis attacks. Section 7 concludes and presents perspectives.

2. Preliminaries

2.1. Notations

We denote $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (similarly $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$).
For $a \in \mathbb{Z}_{pq}$, its reductions are denoted by $a_p := a \bmod p \in \mathbb{F}_p$ and $a_q := a \bmod q \in \mathbb{F}_q$.
For a vector $x \in (\mathbb{Z}_{pq})^m$, we write $x_p := x \bmod p \in (\mathbb{F}_p)^m$ and $x_q := x \bmod q \in (\mathbb{F}_q)^m$.

Chinese remainder theorem

Let p and q be two odd prime numbers, and fix integers $u, v \in \mathbb{Z}$ such that

$$up + vq = 1.$$

Define the CRT idempotents

$$e_p := vq \in Z_{pq}, \qquad e_q := up \in Z_{pq}.$$

Then

$$e_p \equiv 1 \pmod p, \qquad e_p \equiv 0 \pmod q, \qquad e_q \equiv 0 \pmod p, \qquad e_q \equiv 1 \pmod q,$$

and

$$e_p + e_q = 1.$$

Lemma 2.1 (CRT recombination) *For any $(a_p, a_q) \in F_p \times F_q$, the unique element $a \in Z_{pq}$ satisfying*

$$a \equiv a_p \pmod{p}, \qquad a \equiv a_q \pmod{q}$$

is given by

$$a = a_p e_p + a_q e_q \in Z_{pq}.$$

Likewise, for any $x \in (Z_{pq})^m$,

$$x = x_p e_p + x_q e_q \in (Z_{pq})^m,$$

where the equality is understood componentwise.

Quadratic residues and the symbol L_{pq}

We recall the legendre symbol

$$\left(\frac{\cdot}{p}\right) : F_p \longrightarrow \{-1, 0, 1\}.$$

In this work, for $p, q \equiv 3 \pmod 4$, we use a CRT-based representation that simultaneously encodes the quadratic-residue information modulo p and modulo q.

Definition 2.1 (The symbol L_{pq})
Let p and q be odd primes such that $p \equiv q \equiv 3 \pmod 4$, and let u, v satisfy 2.1. For any $a \in Z_{pq}$ such that $\gcd(a, pq) = 1$, we define

$$L_{pq}(a) := \left(\frac{a_p}{p}\right) e_p + \left(\frac{a_q}{q}\right) e_q \in Z_{pq}^{\times}.$$

Lemma 2.2 *For every $a \in \mathbb{Z}_{pq}^{\times}$, one has*

$$L_{pq}(a) \in \mathbb{Z}_{pq}^{\times}.$$

Proof: Since $a \in \mathbb{Z}_{pq}^{\times}$, its reductions $a_p \in \mathbb{F}_p^{\times}$ and $a_q \in \mathbb{F}_q^{\times}$ are nonzero. Hence

$$\left(\frac{a_p}{p}\right) \in \{\pm 1\}, \ \left(\frac{a_q}{q}\right) \in \{\pm 1\},$$

so both CRT components of $L_{pq}(a)$ are nonzero in $\mathbb{F}_p$ and $\mathbb{F}_q$. Therefore $L_{pq}(a)$ is invertible in $\mathbb{Z}_{pq}$. □

Remark 2.1 *Definition 2.1 is equivalent to the case-based form: $L_{pq}(a) = 1$ if a is a quadratic residue modulo p and q, $L_{pq}(a) = e_p - e_q$ (resp. $e_q - e_p$) if a is a residue modulo p but not modulo q (resp. modulo q but not modulo p), and $L_{pq}(a) = -1$ if a is a non-residue modulo p and q.*

2.2. Arithmetic S-box on the unit group of Z_{pq}

We construct a coordinate-wise substitution from L_{pq} on the set of invertible elements of Z_{pq}.

Definition 2.2 (S-box S) Let $p, q \equiv 3 \pmod 4$, and let $d \geq 1$ be such that $\gcd(d, (p-1)(q-1)) = 1$. We define the S-box

$$S : Z_{pq}^{\times} \to Z_{pq}^{\times} \qquad by \qquad S(x) := x^d L_{pq}(x).$$

Remark 2.2 The condition $\gcd\big(d, (p-1)(q-1)\big) = 1$ implies that the power map $x \longmapsto x^d$ is a permutation of $\mathbb{Z}_{pq}^{\times}$. Moreover, by lemma 2.2, $L_{pq}(x) \in \mathbb{Z}_{pq}^{\times}$ for every $x \in \mathbb{Z}_{pq}^{\times}$. Hence S is well defined on the unit group.

MDS diffusion and CRT lifting

In the permutation, diffusion is performed separately modulo p and modulo q, and then recombined through the CRT.

Definition 2.3 (CRT linear layer) *Let $M_p \in GL_m(F_p)$ and $M_q \in GL_m(F_q)$. We define the linear layer*

$$M : (Z_{pq})^m \to (Z_{pq})^m$$

by requiring that, for every $x \in (Z_{pq})^m$,

$$(M(x))_p = M_p(x_p), \qquad (M(x))_q = M_q(x_q).$$

The vector $M(x)$ is then uniquely determined by CRT recombination, applied componentwise, as in Lemma 2.1.

Remark 2.3 *If M_p and M_q are MDS matrices (with branch number $m+1$), then each projection achieves optimal diffusion. This is the standard assumption in wide-trail arguments.*

Extended grendel round function

Let $N \geq 1$ be the number of rounds. The construction combines a coordinate-wise nonlinear layer induced by S, a CRT-based linear diffusion layer, and the addition of round constants.

Definition 2.4 (Coordinate-wise nonlinear layer) *For a state $x = (x_0, \ldots, x_{m-1})$ whose coordinates belong to $Z_{pq}^{\times}$, we define*

$$S^{\|}(x) := (S(x_0), \ldots, S(x_{m-1})) \in (Z_{pq}^{\times})^m.$$

Definition 2.5 (One round function) *For a state x for which the coordinate-wise application $S^{\|}(x)$ is well defined, we define the i-th round function by*

$$\mathrm{Round}_i(x) := M\Big(S^{\|}(x)\Big) + C_i,$$

where M is the CRT linear layer from Definition 2.3 and $C_i \in (Z_{pq})^m$ is the round-constant vector at round i.

Definition 2.6 (N-round transformation) *The N-round transformation associated with the extended grendel construction is defined by*

$$T := \mathrm{Round}_{N-1} \circ \cdots \circ \mathrm{Round}_0.$$

Remark 2.4 Strictly speaking, the nonlinear layer $S^{\|}$ is naturally defined on $\left(\mathbb{Z}_{pq}^{\times}\right)^m$, whereas the CRT linear layer M acts on the full module $(\mathbb{Z}_{pq})^m$. Therefore, the iterated transformation T is formally defined on the set of states for which every intermediate round remains in the domain of the nonlinear layer. In the present work, the security analysis is carried out under this natural domain-of-definition restriction.

2.3. Sponge construction

We recall the sponge construction used to produce a hash function from a permutation.

Definition 2.7 (Sponge) *Let $b = r + c$ be the state size, where r is the rate and c is the capacity. The internal state is initialized to the all-zero state. After padding, the input message is split into blocks of r bits (or r symbols, depending on the encoding).*

During the absorption phase, for each message block M_i, we update the state by

$$state[0..r-1] \leftarrow state[0..r-1] \oplus M_i, \qquad state \leftarrow T(state).$$

Then, during the squeezing phase, we iteratively output

$$Z \leftarrow Z \,\|\, state[0..r-1], \qquad state \leftarrow T(state),$$

until the desired output length is reached.

MELP/MEDP quantities (recall)

In the linear and differential analysis, we use the classical bounds based on the maximum linear probability and the maximum differential probability at the S-box level, denoted by MELP and MEDP, respectively. Closed-form expressions for the S-box S and for the symbol L_{pq} were established in [1] and will be recalled when needed in the analysis sections.

3. Linear and Differential Cryptanalysis

In this section, we analyze the resistance of the extended grendel construction against linear and differential cryptanalysis. We first derive bounds at the S-box level for the arithmetic map

$$S(x) = x^d L_{pq}(x),$$

namely an upper bound on the maximum linear probability (MELP) and an upper bound on the maximum differential probability (MEDP). We then extend these single-round estimates to N rounds by means of a wide-trail argument under the standard independence assumption. This yields explicit upper bounds on the success probabilities of linear and differential characteristics, together with the corresponding data-complexity estimates.

Definition 3.1 (Maximum linear probability) *Let $f : Z_{pq}^{\times} \to Z_{pq}$. The maximum linear probability of f is*

$$\mathrm{MELP}(f) := \max_{a,b \in Z_{pq}^{\times},\, c \in Z_{pq}} \Pr_{x \leftarrow Z_{pq}^{\times}} \big[ax + b\, f(x) = c\big].$$

Remark 3.1 *We recall that, in our previous work [1], the following bound was established for the S-box*

$$f(x) := x^d L_{pq}(x), \qquad \gcd(d, (p-1)(q-1)) = 1,$$

where p and q are odd primes such that $p \equiv q \equiv 3 \pmod 4$. Its maximum linear probability satisfies

$$\mathrm{MELP}(f) \le \frac{4d^2}{(p-1)(q-1)}.$$

Proposition 3.1 (Linear cryptanalysis) *Let p, q be two prime numbers such that $p \equiv q \equiv 3 \pmod 4$, and let $u, v \in \mathbb{Z}$ satisfy*

$$up + vq = 1.$$

Let $S(x) = x^d L_{pq}(x)$ with $\gcd\big(d, (p-1)(q-1)\big) = 1$.

Assume that the CRT linear layer satisfies the standard wide-trail diffusion hypothesis, and that the contributions of distinct active two-round blocks can be treated independently.

Then, for any linear trail over N rounds,

$$\Pr \le \left(\frac{4d^2}{(p-1)(q-1)}\right)^{\lfloor \frac{N}{2} \rfloor}, \qquad Q_{\mathrm{lin}} \ge \left(\frac{4d^2}{(p-1)(q-1)}\right)^{-\lfloor \frac{N}{2} \rfloor}.$$

Proof: By the *wide-trail* argument, for any linear trail T over N rounds, there exist at least $\lfloor \frac{N}{2} \rfloor$ disjoint two-round blocks $T_1, \ldots, T_{\lfloor N/2 \rfloor}$ such that each T_k crosses at least one nontrivial S layer. For each block,

$$\Pr[T_k] \le \mathrm{MELP}_S = \frac{4d^2}{(p-1)(q-1)}.$$

Under the independence assumption (wide-trail),

$$\Pr[T] = \prod_{k=1}^{\lfloor N/2 \rfloor} \Pr[T_k] \le \left(\frac{4d^2}{(p-1)(q-1)}\right)^{\lfloor N/2 \rfloor}.$$

Finally,

$$Q_{\text{lin}} \geq \frac{1}{\Pr[T]} \geq \left(\frac{4d^2}{(p-1)(q-1)}\right)^{-\lfloor N/2 \rfloor}.$$

□

Definition 3.2 (Maximum differential probability) *Let $f : Z_{pq}^{\times} \to Z_{pq}$. The maximum differential probability of f is defined by*

$$\text{MEDP}(f) := \max_{\Delta x \in Z_{pq}^{\times},\, \Delta y \in Z_{pq}} \Pr_{x \leftarrow Z_{pq}^{\times}} \big[f(x + \Delta x) - f(x) = \Delta y\big],$$

Remark 3.2 We recall that, in our previous work [1], the following bound was established for

$$f(x) := x^d L_{pq}(x), \qquad \gcd(d, (p-1)(q-1)) = 1,$$

where p and q are odd primes such that $p \equiv q \equiv 3 \pmod 4$. Its maximum differential probability satisfies

$$\text{MEDP}(f) = \frac{(4d-2)^2}{(p-1)(q-1)}.$$

This result will be used in the sequel to derive round-level and multi-round differential bounds.

Proposition 3.2 (Differential cryptanalysis) *Let p, q be two prime numbers such that $p \equiv q \equiv 3 \pmod 4$, and let $u, v \in \mathbb{Z}$ satisfy $up + vq = 1$. Let $S(x) = x^d L_{pq}(x)$ with $\gcd\big(d, (p-1)(q-1)\big) = 1$ and*

$$\text{MEDP}_S = \frac{(4d-2)^2}{(p-1)(q-1)}.$$

Then, for any differential characteristic over N rounds,

$$\Pr \leq \left(\frac{(4d-2)^2}{(p-1)(q-1)}\right)^{\lfloor \frac{N}{2} \rfloor}, \qquad Q_{\text{diff}} \geq \left(\frac{(4d-2)^2}{(p-1)(q-1)}\right)^{-\lfloor \frac{N}{2} \rfloor}.$$

Proof: By the *wide-trail* argument, for any differential characteristic T over N rounds, there exist at least $\lfloor \frac{N}{2} \rfloor$ disjoint two-round blocks $T_1, \ldots, T_{\lfloor N/2 \rfloor}$ such that each T_k crosses at least one nontrivial S layer. For each block,

$$\Pr[T_k] \leq \text{MEDP}_S = \frac{(4d-2)^2}{(p-1)(q-1)}.$$

Under the independence assumption (wide-trail),

$$\Pr[T] = \prod_{k=1}^{\lfloor N/2 \rfloor} \Pr[T_k] \leq \left(\frac{(4d-2)^2}{(p-1)(q-1)}\right)^{\lfloor \frac{N}{2} \rfloor}.$$

Finally,

$$Q_{\text{diff}} \geq \frac{1}{\Pr[T]} \geq \left(\frac{(4d-2)^2}{(p-1)(q-1)}\right)^{-\lfloor \frac{N}{2} \rfloor}.$$

□

4. Integral Attacks

In this section, we analyze *integral attacks* [11] against the extended grendel permutation over $\mathbb{Z}_{pq}$. The core idea is to sum the outputs of suitable polynomial functions over structured sets in order to obtain exact cancellations (zero-sum properties) over fields of odd characteristic. We first recall a standard lemma on polynomial sums over affine subspaces of $\mathbb{F}_p^t$ (with p odd), and then lift it via the CRT to derive zero-sum relations modulo pq. We also establish an analogous statement for multiplicative subgroups. Finally, we use these tools to obtain quantitative constraints on the minimal size of saturating sets when a nontrivial pattern crosses an MDS diffusion layer, yielding explicit lower bounds on the number of queries required by any saturation-type integral attack in our setting.

Remark 4.1 We recall the following result, established in our previous [18].

Let F_p be a finite field, let $V \subseteq F_p^t$ be an affine subspace of dimension k, and let $F : F_p^t \to F_p$ be a polynomial function of total degree at most $k(p-1)$. Then

$$\sum_{v \in V} F(v) = 0.$$

This result will be used in the sequel to derive integral properties over affine subspaces.

Proposition 4.1 (Integral pattern over Z_{pq} via CRT) *Let p and q be two odd prime numbers. Let $V_p \subseteq (F_p)^t, V_q \subseteq (F_q)^t$ be two affine subspaces of dimensions k_p and k_q, respectively, and define*

$$V := \{x \in (Z_{pq})^t : x \bmod p \in V_p,\ x \bmod q \in V_q\}.$$

Let $F : (Z_{pq})^t \to Z_{pq}$, and let F_p and F_q denote its reductions modulo p and modulo q, respectively. Assume that F_p and F_q are polynomial functions satisfying:

$$\deg(F_p) \le k_p(p-1) \qquad \textit{and} \qquad \deg(F_q) \le k_q(q-1).$$

Then

$$\sum_{v \in V} F(v) \equiv 0 \pmod{pq}.$$

Proof: By Remark 4.1, applied over F_p and F_q, the degree assumptions imply

$$\sum_{a \in V_p} F_p(a) = 0 \quad \text{in } F_p, \qquad \sum_{b \in V_q} F_q(b) = 0 \quad \text{in } F_q.$$

Now, by CRT, the set V is in bijection with the product $V_p \times V_q$. Hence, reducing modulo p, we obtain

$$\sum_{v \in V} F(v) \equiv \sum_{(a,b) \in V_p \times V_q} F_p(a) = |V_q| \sum_{a \in V_p} F_p(a) \equiv 0 \pmod{p}.$$

Similarly, reducing modulo q gives

$$\sum_{v \in V} F(v) \equiv \sum_{(a,b) \in V_p \times V_q} F_q(b) = |V_p| \sum_{b \in V_q} F_q(b) \equiv 0 \pmod{q}.$$

Therefore,

$$\sum_{v \in V} F(v) \equiv 0 \pmod{p} \qquad \text{and} \qquad \sum_{v \in V} F(v) \equiv 0 \pmod{q}.$$

Since p and q are coprime, the CRT yields

$$\sum_{v \in V} F(v) \equiv 0 \pmod{pq}.$$

□

Remark 4.2 (Integral patterns for subgroups) We recall the following result, established in our previous [18]

Let $\mathbb{F}_p$ be a finite field and let $G \subset \mathbb{F}_p^\times$ be a (multiplicative) subgroup. Let $F : \mathbb{F}_p \to \mathbb{F}_p$ be a polynomial function such that $\deg(F) < |G|$. Then

$$\sum_{g \in G} F(g) = F(0)\,|G|.$$

Proposition 4.2 (CRT generalization over $\mathbb{Z}_{pq}$) *Let p, q be two odd prime numbers and let $G \subset (\mathbb{Z}_{pq})^\times$ be a (multiplicative) subgroup. Define*

$$G_p := \{\, g \bmod p : g \in G \,\} \subset \mathbb{F}_p^\times, \qquad G_q := \{\, g \bmod q : g \in G \,\} \subset \mathbb{F}_q^\times.$$

Let $F : \mathbb{Z}_{pq} \to \mathbb{Z}_{pq}$ and denote by F_p and F_q its reductions modulo p and q. Assume that F_p and F_q are polynomial and satisfy

$$\deg(F_p) < |G_p| \qquad \textit{and} \qquad \deg(F_q) < |G_q|.$$

Then we have simultaneously

$$\sum_{g \in G} F(g) \equiv F(0)\,|G| \pmod{p}, \qquad \sum_{g \in G} F(g) \equiv F(0)\,|G| \pmod{q},$$

and in particular

$$\sum_{g \in G} F(g) \equiv F(0)\,|G| \pmod{pq}.$$

Proof: Let $\pi_p : G \to G_p$ be the natural reduction map modulo p, which is surjective by definition of G_p. Set $K_p := \ker(\pi_p) = \{g \in G : \pi_p(g) = 1\}$. Then $|G| = |K_p|\,|G_p|$.
Reducing modulo p and grouping terms by the fibers of π_p, we obtain

$$\sum_{g \in G} F(g) \equiv \sum_{g \in G} F_p(g \bmod p) \pmod{p}$$

and hence

$$\sum_{g \in G} F(g) \equiv \sum_{h \in G_p} \sum_{\substack{g \in G \\ \pi_p(g) = h}} F_p(h) = |K_p| \sum_{h \in G_p} F_p(h) \pmod{p}.$$

By Remark 4.2, applied over F_p, we have

$$\sum_{h \in G_p} F_p(h) = F_p(0)|G_p| \quad \text{in } F_p.$$

Therefore,

$$\sum_{g \in G} F(g) \equiv |K_p|\,F_p(0)\,|G_p| = F_p(0)\,|G| \equiv F(0)\,|G| \pmod{p}.$$

The same argument modulo q yields

$$\sum_{g \in G} F(g) \equiv F(0)|G| \pmod{q}.$$

Since p and q are coprime, the CRT gives

$$\sum_{g \in G} F(g) \equiv F(0)|G| \pmod{pq}.$$

□

4.1. Integral patterns over F_p

Remark 4.3 We recall the following field-level observation from [4]. Consider an SPN-type permutation over F_p^m with a coordinate-wise S-box layer, addition of round constants, and an MDS linear layer of branch number $m+1$. If a nontrivial affine subspace $V \subseteq F_p^m$ supporting a zero-sum pattern propagates across at least one diffusion layer without collapsing to a trivial pattern, then its dimension must satisfy

$$\dim(V) \geq \left\lceil \frac{m+1}{2} \right\rceil.$$

Consequently, any saturation-type integral attack based on such a subspace requires at least

$$p^{\lceil \frac{m+1}{2} \rceil}$$

queries.

Remark 4.4 We also recall from [4] that multiplicative-subgroup patterns over $F_p^\times$ do not yield long integral propagations through such SPN structures. More precisely, although a subgroup may remain stable through the nonlinear layer in special cases, the affine part of the round function, in particular the addition of round constants and the MDS diffusion, breaks the subgroup structure. Hence subgroup-based zero-sum patterns do not propagate across more than a very limited number of rounds.

4.2. CRT lifting of integral constraints

Proposition 4.3 *Let p and q be two odd prime numbers, and let $m \geq 1$. Consider a round function over $(Z_{pq})^m$ whose reductions modulo p and modulo q define SPN-type transformations over F_p^m and F_q^m, respectively, each with an MDS diffusion layer of branch number $m+1$.*

Let $V_p \subseteq F_p^m$ and $V_q \subseteq F_q^m$ be two projected patterns, and define

$$V := \{x \in (Z_{pq})^m : \ x \bmod p \in V_p, \ x \bmod q \in V_q\}.$$

Assume that both V_p and V_q support nontrivial affine zero-sum patterns that propagate across at least one diffusion layer without collapsing to a trivial pattern. Then

$$|V_p| \geq p^{\lceil \frac{m+1}{2} \rceil}, \qquad |V_q| \geq q^{\lceil \frac{m+1}{2} \rceil},$$

and therefore

$$|V| = |V_p|\,|V_q| \geq (pq)^{\lceil \frac{m+1}{2} \rceil}.$$

Proof: By Remark 4.3, any nontrivial affine zero-sum pattern over F_p^m propagating through at least one MDS diffusion layer must have dimension at least

$$\left\lceil \frac{m+1}{2} \right\rceil.$$

Hence

$$|V_p| \geq p^{\lceil \frac{m+1}{2} \rceil}.$$

By the same argument over F_q^m, we obtain

$$|V_q| \geq q^{\lceil \frac{m+1}{2} \rceil}.$$

Finally, by CRT, the global pattern V is in bijection with the product $V_p \times V_q$. Hence

$$|V| = |V_p|\,|V_q| \geq (pq)^{\lceil \frac{m+1}{2} \rceil}.$$

□

4.3. Consequence for the hash construction

Proposition 4.4 *Under the assumptions of Proposition 4.3, any nontrivial affine zero-sum saturation-type integral distinguisher compatible with the CRT structure of the construction requires at least*

$$(pq)^{\lceil \frac{m+1}{2} \rceil}$$

queries.

Proof: Proposition 4.3. shows that any propagated nontrivial affine zero-sum pattern compatible with the CRT projections must have cardinality at least

$$(pq)^{\lceil \frac{m+1}{2} \rceil}.$$

Therefore, any saturation-type integral distinguisher based on such a pattern requires at least that many chosen queries. □

5. Algebraic Attacks

In this section, we discuss algebraic attack strategies against the extended grendel construction over $\mathbb{Z}_{pq}$. Owing to the CRT decomposition

$$\mathbb{Z}_{pq} \simeq \mathbb{F}_p \times \mathbb{F}_q,$$

algebraic questions over $\mathbb{Z}_{pq}$ naturally split into two component problems over $\mathbb{F}_p$ and $\mathbb{F}_q$. [3] Over $\mathbb{Z}_{pq}$, algebraic analysis is naturally carried out through the CRT. Indeed, the ring isomorphism $\mathbb{Z}_{pq} \simeq \mathbb{F}_p \times \mathbb{F}_q$ induces, for any map $f : (\mathbb{Z}_{pq})^m \to \mathbb{Z}_{pq}$, two component maps

$$f_p : (\mathbb{F}_p)^m \to \mathbb{F}_p, \qquad f_q : (\mathbb{F}_q)^m \to \mathbb{F}_q,$$

obtained by reduction modulo p and q. Consequently, an interpolation [19] or root-finding attack over $\mathbb{Z}_{pq}$ decomposes into two corresponding attacks modulo p and modulo q, followed by CRT recombination. Throughout this section, we measure complexity in terms of oracle evaluations of f.

5.1. Field-level recalled facts

We recall the following standard observations on algebraic attacks from [4]. First, an interpolation attack over a finite field is effective only when the attacked primitive admits a representation by a polynomial of sufficiently low degree. By contrast, if the reduced coordinate functions already have maximal, or near-maximal, degree in each variable, then exact interpolation requires a number of input-output pairs comparable to the full size of the domain, and therefore does not provide a practical low-complexity distinguisher.

We also recall that the classical GCD attack [4] is mainly relevant in keyed algebraic settings, where the attacked primitive can be described by a bivariate polynomial

$$F(X, K),$$

with low degree in an unknown key variable K. In such a situation, two input-output pairs may yield two polynomials in K whose common root reveals the secret key. This attack model is therefore specific to primitives involving a hidden algebraic variable.

Finally, a root-finding, or preimage attack [4] may be formulated whenever one output coordinate can be expressed as a univariate polynomial

$$f(x)$$

of the input. For a known output value y, the preimage problem then reduces to solving

$$f(x) - y = 0.$$

Its practical complexity depends on the degree of the resulting polynomial and on the algebraic modeling assumptions. In particular, when auxiliary symbolic choices must be guessed in advance, the total complexity acquires the corresponding multiplicative guessing factor.

5.2. CRT lifting of algebraic attack constraints

Proposition 5.1 *Let p and q be two odd prime numbers, and let $m \geq 1$. Let*

$$f : (Z_{pq})^m \to Z_{pq},$$

and let f_p and f_q denote its reductions modulo p and modulo q, respectively:

$$f_p : (F_p)^m \to F_p, \qquad f_q : (F_q)^m \to F_q.$$

Then the following statements hold.

(i) ***Interpolation.*** *Assume that f_p and f_q are represented by reduced multivariate polynomials in m variables, with partial degrees at most $p-1$ and $q-1$, respectively. Then exact interpolation of f requires at least*

$$Q_{\text{int}} \geq \max\{p^m, q^m\}$$

oracle evaluations.

(ii) ***Root-finding / preimage search.*** *Let $y \in Z_{pq}$, and write*

$$y_p := y \bmod p, \qquad y_q := y \bmod q.$$

Then solving

$$f(x) = y \pmod{pq}$$

is equivalent, via CRT, to solving simultaneously

$$f_p(x_p) = y_p \quad \text{over } F_p, \qquad f_q(x_q) = y_q \quad \text{over } F_q.$$

Hence any preimage attack over Z_{pq} decomposes into two component solving problems followed by CRT recombination. If an algebraic model introduces T binary unknowns to be guessed in advance, and if the corresponding solving costs after fixing these unknowns are C_p and C_q, then a standard guess-and-solve strategy has average complexity at least

$$Q_{\text{root}} \gtrsim 2^T \cdot \max\{C_p, C_q\}.$$

(iii) ***GCD attack.*** *The classical GCD attack applies only when the attacked primitive depends on an unknown algebraic variable, typically a secret key. Therefore, in the present public-permutation setting with no hidden key variable, this attack model does not apply.*

Proof: (i) Over F_p, the vector space of reduced multivariate polynomials in m variables with partial degrees at most $p-1$ has dimension

$$p^m,$$

with basis

$$\{x_1^{a_1} \cdots x_m^{a_m} : 0 \leq a_i \leq p-1\}.$$

Therefore, exact determination of f_p requires at least p^m independent constraints, and hence at least p^m evaluations. The same argument modulo q gives the lower bound q^m. Since one evaluation of f simultaneously provides one value modulo p and one value modulo q, exact interpolation of f requires at least

$$\max\{p^m, q^m\}$$

queries.

(ii) By the CRT, the map

$$(Z_{pq})^m \longrightarrow (F_p)^m \times (F_q)^m, \qquad x \longmapsto (x_p, x_q),$$

is a bijection. Under this correspondence, the equation

$$f(x) = y \pmod{pq}$$

is equivalent to the pair of equations

$$f_p(x_p) = y_p, \qquad f_q(x_q) = y_q.$$

Hence the preimage problem over Z_{pq} decomposes into two solving problems over F_p and F_q, followed by CRT recombination. If the algebraic model contains T binary choices to be guessed in advance, then a guess-and-solve strategy incurs an average multiplicative factor 2^T, and the total cost is dominated by the more expensive of the two component solves. This yields

$$Q_{\text{root}} \gtrsim 2^T \cdot \max\{C_p, C_q\}.$$

(iii) The classical GCD attack requires a hidden algebraic variable, such as a secret key, appearing in a low-degree bivariate model. Since no such unknown key variable is present here, this attack model is not applicable. □

6. Grobner Basis Attacks

In this section, we investigate algebraic attacks based on gröbner [9] bases against the extended grendel permutation over $\mathbb{Z}_{pq}$. Such attacks model a target instance (preimage, collision, or distinguisher) as a system of multivariate polynomial equations. Since $\mathbb{Z}_{pq}$ is not a field, the analysis is naturally carried out through the CRT, which reduces algebraic problems over $\mathbb{Z}_{pq}$ to two corresponding systems over $\mathbb{F}_p$ and $\mathbb{F}_q$. We first show that the coordinate-wise CRT recombination induces two independent evolutions modulo p and modulo q, yielding an immediate lower bound on the gröbner-basis complexity. We then consider the setting where the L_{pq} symbols at S-box inputs are known, in which case the nonlinear layer simplifies to monomial terms up to known scalars. This enables Macaulay/F4–F5-type complexity estimates over each field and leads to an additional multiplicative factor under a guess-and-solve strategy when the symbols must be guessed.

6.1. CRT Reduction and Modeling Framework

Proposition 6.1 (CRT reduction for a gröbner attack) *Let p, q be two odd prime numbers and let $u, v \in \mathbb{Z}$ satisfy $up + vq = 1$. Consider one round of the extended grendel permutation on $(\mathbb{Z}_{pq})^m$ of the following form:*

$$\textit{(S-box)} \quad x \mapsto S^{\|}(x), \qquad \textit{(diffusion)} \quad y = M_1 S^{\|}(x),\ z = M_2 S^{\|}(x),$$

followed by coordinate-wise CRT recombination

$$x' \;=\; (vq)\, y + (up)\, z \;+\; C,$$

where M_1 and M_2 are matrices, C is a round constant, and $S^{\|}$ acts coordinate-wise.

Then the reductions $x_p := x \bmod p$ and $x_q := x \bmod q$ evolve according to two rounds over fields:

$$x'_p \;=\; M_{1,p}\, S_p^{\|}(x_p) + C_p \quad \textit{in } (\mathbb{F}_p)^m, \qquad x'_q \;=\; M_{2,q}\, S_q^{\|}(x_q) + C_q \quad \textit{in } (\mathbb{F}_q)^m,$$

where $M_{1,p}$ (resp. $M_{2,q}$) is the reduction of M_1 modulo p (resp. of M_2 modulo q), and S_p, S_q are the reductions of the S-box.

In particular, for any instance of an algebraic attack (preimage, collision, distinguisher) modeled by a system E over $\mathbb{Z}_{pq}$, solving E is equivalent to simultaneously solving the two reduced systems E_p over $\mathbb{F}_p$ and E_q over $\mathbb{F}_q$, followed by CRT recombination. Therefore, a gröbner attack over $\mathbb{Z}_{pq}$ has complexity at least

$$C_{GB}(\mathbb{Z}_{pq}) \;\geq\; \max\big\{C_{GB}(\mathbb{F}_p),\, C_{GB}(\mathbb{F}_q)\big\}.$$

Proof: Since $vq \equiv 1 \pmod{p}$ and $up \equiv 0 \pmod{p}$, reducing the recombination modulo p yields

$$x'_p \equiv y + C \pmod{p}.$$

Moreover, $y = M_1 S^{\|}(x)$ implies $y \bmod p = M_{1,p} S_p^{\|}(x_p)$, hence

$$x'_p = M_{1,p} S_p^{\|}(x_p) + C_p \quad \text{in } (\mathbb{F}_p)^m.$$

Similarly, $vq \equiv 0 \pmod{q}$ and $up \equiv 1 \pmod{q}$, so modulo q we obtain

$$x'_q \equiv z + C \pmod{q},$$

and since $z = M_2 S^{\|}(x)$ we get $z \bmod q = M_{2,q} S_q^{\|}(x_q)$, hence

$$x'_q = M_{2,q} S_q^{\|}(x_q) + C_q \quad \text{in } (\mathbb{F}_q)^m.$$

Finally, solving a polynomial system over $\mathbb{Z}_{pq}$ is equivalent (via CRT) to solving its reductions modulo p and modulo q and recombining solutions coordinate-wise, which yields the stated complexity lower bound. □

6.2. Gröbner attack with known L_{pq} symbols (CRT viewpoint)

Assume that, for the considered instance, the attacker knows (or has correctly guessed) the values $L_{pq}(z_{i,j})$ at the inputs of the S-boxes. Then each nonlinear term

$$S(z) = z^d L_{pq}(z)$$

reduces to a known scalar multiple of z^d, and the associated polynomial modeling simplifies. Via the CRT isomorphism $\mathbb{Z}_{pq} \simeq \mathbb{F}_p \times \mathbb{F}_q$, the resulting system splits into two systems over $\mathbb{F}_p$ and $\mathbb{F}_q$.

Proposition 6.2 (Gröbner bounds with known L_{pq} symbols) *Let p, q be odd primes with $p \equiv q \equiv 3 \pmod{4}$, and let f be an SPN-type permutation on $(\mathbb{Z}_{pq})^m$ with N rounds, whose nonlinear layer is applied coordinate-wise as*

$$S(x) = x^d L_{pq}(x) \in \mathbb{Z}_{pq}.$$

Fix an algebraic attack model (e.g., one-absorb/one-squeeze preimage) which, after specializing the known inputs/outputs, leads to a system of n polynomial equations in n unknown state variables over $\mathbb{Z}_{pq}$. Assume that all values $L_{pq}(z_{i,j})$ at the S-box inputs occurring in the model are known.

Then the specialized system has total degree at most α (typically $\alpha = d$), and its CRT reductions yield two systems over fields,

$$E_p \subset \mathbb{F}_p[X_1, \ldots, X_n], \qquad E_q \subset \mathbb{F}_q[Y_1, \ldots, Y_n],$$

whose polynomials have the same degree bound α.

If the reduced systems behave as semi-regular (generic) sequences, the degree of regularity satisfies the Macaulay bound

$$d_{\text{reg}} \;\lesssim\; d_{\text{Mac}} \;:=\; 1 + \sum_{i=1}^{n} (\deg(p_i) - 1) \;\le\; 1 + n(\alpha - 1),$$

and a standard F4/F5-type solving cost over each field is dominated by linear algebra at degree d_{reg}, namely

$$C_{GB}(\mathbb{F}_p) \;\approx\; \binom{n + d_{\text{reg}}}{d_{\text{reg}}}^{\omega}, \qquad C_{GB}(\mathbb{F}_q) \;\approx\; \binom{n + d_{\text{reg}}}{d_{\text{reg}}}^{\omega},$$

for some linear-algebra exponent $\omega \in [2, 3]$.

Consequently, solving over $\mathbb{Z}_{pq}$ via CRT requires at least solving both reductions, and therefore

$$C_{GB}(\mathbb{Z}_{pq}) \;\gtrsim\; \max\{C_{GB}(\mathbb{F}_p),\, C_{GB}(\mathbb{F}_q)\} \quad (\textit{and typically } \approx C_{GB}(\mathbb{F}_p) + C_{GB}(\mathbb{F}_q)).$$

Finally, if the L_{pq} symbols are not given and must be guessed for t S-box inputs in the model, and if they are modeled as independent uniform variables taking 4 possible values, then a guess-and-solve strategy incurs an expected multiplicative factor 4^t, i.e.,

$$C_{GB}^{\text{guess}}(\mathbb{Z}_{pq}) \;\approx\; 4^t \cdot \max\{C_{GB}(\mathbb{F}_p),\, C_{GB}(\mathbb{F}_q)\}.$$

Proof: Under the *known-symbol* assumption, for each S-box input z occurring in the specialized model, the value $L_{pq}(z)$ is a known constant in $\mathbb{Z}_{pq}$, so $S(z) = z^d L_{pq}(z)$ becomes a monomial of degree d multiplied by a known scalar. Since each round equation is affine in the output and linear in the S-box layer, the specialized system consists of n equations of total degree at most α (typically $\alpha = d$).

Because $\mathbb{Z}_{pq} \simeq \mathbb{F}_p \times \mathbb{F}_q$, the system over $\mathbb{Z}_{pq}$ is equivalent to its two reductions modulo p and modulo q, yielding the field systems E_p and E_q. Assuming semi-regular behavior, the degree of regularity is (heuristically) upper-bounded by the Macaulay bound $d_{\text{Mac}} \leq 1 + n(\alpha - 1)$, and the dominant cost of F4/F5-type methods is the linear algebra at degree d_{reg}, with matrix dimension on the order of $\binom{n+d_{\text{reg}}}{d_{\text{reg}}}$, hence the stated estimates. The lower bound for $C_{GB}(\mathbb{Z}_{pq})$ follows since one must solve both reductions to reconstruct solutions via CRT.

If t symbols L_{pq} must be guessed and each takes 4 values, a correct full guess occurs with probability 4^{-t}, so the expected number of trials is 4^t, which multiplies the expected cost by 4^t. □

7. Conclusion

We studied the security of the *extended grendel* permutation over $\mathbb{Z}_{pq}$ in the setting of a *sponge* construction. Our analysis covers linear and differential attacks (via a *wide-trail* reasoning and local MELP/MEDP bounds), integral attacks (adapted to the composite setting thanks to the CRT), as well as algebraic and gröbner-basis attacks (polynomial modeling and complexity discussion, with and without knowledge of the L_{pq} symbols). The obtained results provide explicit bounds as a function of the parameters (p, q) and the number of rounds N, and indicate that increasing N rapidly decreases the probability of observing distinguishable propagations. This study thus establishes a reusable evaluation framework for arithmetic permutations over composite rings and prepares parameter selection and large-scale experimental validations.

Acknowledgments

We thank the organizing committee of ICAME'25 for the announcement and the opportunity to submit our work within the framework of the special issue associated with the theme "Applied Mathematics, Modeling, and Engineering". We also express our gratitude to the journal *Boletim da Sociedade Paranaense de Matemáticas (BSPM)* for hosting this special issue, as well as to the editorial teams and the reviewers for their work in the selection and evaluation process.

References

1. A. Lkoaiza, S. Abdelalim, A. Cherkaoui, and I. Elmouki, *An Extended Grendel Approach Applied to Blockchain Signature as an Alternative to Keccak Permutation*, Statist. Optim. Inf. Comput., (2025).
2. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton Univ. Press, (2016).
3. A. Roy, E. Andreeva, and J. F. Sauer, *Interpolation cryptanalysis of unbalanced feistel networks with low degree round functions*, in *Selected Areas in Cryptography – SAC 2020*, Springer, (2020).
4. A. Szepieniec, *On the use of the Legendre symbol in symmetric cipher design*, Cryptology ePrint Arch., (2021).
5. A. Szepieniec, T. Ashur, and S. Dhooghe, *Rescue-Prime: A standard specification (SoK)*, IACR Cryptology ePrint Arch. 2020/1143, (2020).
6. C. Li and B. Prenel, *Improved interpolation attacks on cryptographic primitives of low algebraic degree*, in *Selected Areas in Cryptography – SAC 2019*, Lecture Notes in Comput. Sci. **11599**, 171–193, (2019).
7. F. Mattoussi, V. Roca, and B. Sayadi, *Complexity comparison of the use of Vandermonde versus Hankel matrices to build systematic MDS Reed–Solomon codes*, in *2012 IEEE 13th Int. Workshop on SPAWC*, IEEE, 344–348, (2012).
8. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, *The KECCAK SHA-3 submission, Version 3*, (2011).

9. J. F. Sauer and A. Szepieniec, *SoK: Gröbner basis algorithms for arithmetization-oriented ciphers*, Cryptology ePrint Arch. 2021/870, (2021).

10. J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM **27**, 701–717, (1980).

11. L. R. Knudsen and D. A. Wagner, *Integral cryptanalysis*, in *Fast Software Encryption – FSE 2002*, Lecture Notes in Comput. Sci. **2365**, 112–127, (2002).

12. L. Grassi, D. Khovratovich, S. Rønjom, and M. Schofnegger, *The legendre symbol and the modulo-2 operator in symmetric schemes over* $(\mathbb{F}_p)^n$, Cryptology ePrint Arch. 2021/1533, (2021).

13. M. Parmar and H. J. Kaur, *Comparative analysis of secured hash algorithms for blockchain technology and Internet of Things*, Int. J. Adv. Comput. Sci. Appl. **12**, (2021).

14. M. R. Albrecht, L. Grassi, C. Rechberger, A. Roy, and T. Tiessen, *MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity*, in *Advances in Cryptology – ASIACRYPT 2016*, Lecture Notes in Comput. Sci. **10031**, 191–219, (2016).

15. S. Abdelalim, A. Lkoaiza, A. Cherkaoui, I. Elmouki, and N. Abghour, *A Python Programming Initiative for Hash Construction through the Example of SHA-2*, in *Finite Abelian Groups, Elliptic Curves, Blockchain With Hashing and Graphs*, 264–278, (2025).

16. R. Zippel, *Probabilistic algorithms for sparse polynomials*, in *Symbolic and Algebraic Computation*, Lecture Notes in Comput. Sci. **72**, 216–226, (1979).

17. S. Abdelalim, A. Cherkaoui, A. Lkoaiza, I. Elmouki, and N. Abghour, *Advancing Blockchain Security Using Graph Theory: A Python Programming Perspective*, in *Finite Abelian Groups, Elliptic Curves, Blockchain With Hashing and Graphs*, 279–293, (2025).

18. T. Beyne, A. Canteaut, I. Dinur, I. Eichlseder, G. Leander, G. Leurent, M. Naya-Plasencia, L. Perrin, Y. Sasaki, Y. Todo, and F. Wiemer, *Out of oddity - new cryptanalytic techniques against symmetric primitives optimized for integrity proof systems*, in *Advances in Cryptology – CRYPTO 2020*, Lecture Notes in Comput. Sci. **12172**, 299–328, (2020).

19. T. Jakobsen and L. R. Knudsen, *The interpolation attack on block ciphers*, in *Fast Software Encryption – FSE 1997*, Lecture Notes in Comput. Sci. **1267**, 28–40, (1997).

20. Z. A. Kamal and R. Fareed, *A proposed hash algorithm to use for blockchain-based transaction flow system*, Period. Eng. Nat. Sci. **9**, 657–673, (2021).

Abdelkarim LKOAIZA,
Laboratory of Mathematical Analysis, Algebra and Applications (LAM2A),
Faculty of Sciences Ain Chock (FSAC)
, University Hassan II of Casablanca,
Casablanca, Morocco.
E-mail address: karimlkoaiza6@gmail.com

and

Seddik ABDELALIM,
Laboratory of Mathematical Analysis, Algebra and Applications (LAM2A),
Faculty of Sciences Ain Chock (FSAC)
, University Hassan II of Casablanca,
Casablanca, Morocco.
E-mail address: seddikabd@hotmail.com