When Polynomials Iterate: Structure and Security in Symmetric Cryptography

Arnab Roy
University of Innsbruck

Workshop on ZK, Succinct Proofs and Symmetric Cryptography
Wien, Feb 9, 2026

Outline

1. A Quick (Algebraic) Recall
2. Iterating Triangular Systems
3. Solving Iterative Triangular Systems (under Constraints)
4. Gröbner basis: A Method to Solve Polynomial Equations
5. Security of An Extended Feistel Family
(work under progress [Campa and Roy])

A Quick (Algebraic) Recall

Permutations over $\mathbb{F}_q$

- A fundamental function/primitive for *symmetric cryptography*
- May or may not have (secret) key
  - $F : \{0,1\}^n \mapsto \{0,1\}^n$
  - $F : \{0,1\}^\kappa \times \{0,1\}^n \mapsto \{0,1\}^n$
- All *symmetric key* permutations are iterative function
- In ZKP context: permutations defined over $\mathbb{F}_q$ gained attention
- Classical constructions: AES (over $\mathbb{F}_{2^8}$)
- What is new?
  - A polynomial based approach
  - Efficient polynomial evaluation/representation: multiplicative complexity
  - Example: bi-linear representation (in R1CS)

Classical Functions: A Polynomial Perspective

- Let $p : \mathbb{F}_q \mapsto \mathbb{F}_q$ be a permutation polynomial

$$S : \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}^\top \mapsto \begin{pmatrix} p(x_1) & \dots & p(x_n) \end{pmatrix}^\top$$

- $A : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ be a linear (or affine) transformation
- $F(x) := (S \circ A \circ \cdots S \circ A \circ S)(x)$ where $x \in \mathbb{F}_q^{n \cdot w}$
- The well-known **SPN**

- Let $f : \mathbb{F}_q \mapsto \mathbb{F}_q$

$$F : \begin{pmatrix} x_1 & x_2 \end{pmatrix}^\top \mapsto \begin{pmatrix} x_1 & x_2 + f(x_1) \end{pmatrix}^\top$$

- $A : \begin{pmatrix} x_1 & x_2 \end{pmatrix}^\top \mapsto \begin{pmatrix} x_{\sigma(1)} & x_{\sigma(2)} \end{pmatrix}^\top$ where $\sigma \in S_2$ (permutation group)
- $F(x) := (S \circ A \circ \cdots S \circ A \circ S)(x)$ where $x \in \mathbb{F}_q^{n \cdot w}$
- The well-known **Feistel Network** with two branches

Iterating Triangular Systems

A Starting Point

- Triangular dynamical system by Ostafe and Shparlinski (2010)

$$
\begin{aligned}
f_1(x_1, \dots, x_n) &= x_1 g_1(x_2, \dots, x_n) + h_1(x_2, \dots, x_n) \\
f_2(x_1, \dots, x_n) &= x_2 g_2(x_3, \dots, x_n) + h_2(x_3, \dots, x_n) \\
&\vdots \\
f_{n-1}(x_1, \dots, x_n) &= x_{n-1} g_{n-1}(x_n) + h_{n-1}(x_n) \\
f_n(x_1, \dots, x_n) &= x_n
\end{aligned}
$$

- TDS $\mathcal{F} = \{f_1, \dots, f_n\}$, where $f_i, g_i, h_i \in \mathbb{F}_q[x_1, \dots, x_n]$
- No invertibility

Triangular System for Cryptographic Permutation

- An invertible triangular system (Roy and Steiner, 2024)

$$
\begin{aligned}
f_1(x_1, \dots, x_n) &= p_1(x_1) \cdot g_1(x_2, \dots, x_n) + h_1(x_2, \dots, x_n) \\
f_2(x_1, \dots, x_n) &= p_2(x_2) \cdot g_2(x_3, \dots, x_n) + h_2(x_3, \dots, x_n) \\
&\vdots \\
f_{n-1}(x_1, \dots, x_n) &= p_{n-1}(x_{n-1}) \cdot g_{n-1}(x_n) + h_{n-1}(x_n) \\
f_n(x_1, \dots, x_n) &= p_n(x_n).
\end{aligned}
$$

- p_i is a permutation, g_i is irreducible; $p_i, g_i, h_i \in \mathbb{F}_q[x_1, \dots, x_n]$
- $F : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ is a bijection where $F := \begin{pmatrix} f_1 & f_2 & \dots & f_n \end{pmatrix}^\top$

Instances from Triangular System

- **SPN** and **partial SPN**: $g_i = 1, h_i = 0$ for all i
- **Generalised Feistel**
- **Balanced Feistel**: Can be composition of more than one F e.g. $F := F^{(p,g,h)} \circ F^{(p',g',h')}$
- All well-known invertible permutations in SKC (*to the best of my knowledge*)

- Gives the Horst scheme [GHRSWW '22, '23]

$$\begin{bmatrix} x_1 & x_2 \end{bmatrix}^\top \mapsto \begin{bmatrix} x_1 & x_1 g(x_2) + h(x_2) \end{bmatrix}^\top$$

- Horst variations: **Griffin** and **Reinforced Concrete** ($F : \mathbb{F}_p^3 \mapsto \mathbb{F}_p^3$)

$$\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \mapsto \begin{bmatrix} x_1^d & x_2 x_1 + a_1 x_1 + b_1 & x_3^2 + a_2 x_3 + b_2 \end{bmatrix}^\top$$

- p is prime; $d \in \mathbb{N}$ s.t. $\gcd(p, d-1) = 1$; a_i, b_i are integers such that $b_i^2 - 4a_i$ is non-square modulo p,

Cryptographic Functions from Triangular Polynomial System

Define a cryptographic permutation

- Choose an invertible linear (or affine) transformation $A : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$
- Define a cryptographic permutation: $P = (F \circ A \circ \cdots \circ A \circ F)(x)$
- p, g, h are characterised for cryptographic security, e.g.
  - degree (and structure/form) of permutation p_i
  - sparsity of g

Compression function $C : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ where $n > m$

- Sponge mode with P
- $C(x) = \text{Trunc}(P(x) + x)$ where Trunc chops off $n - m$ field elements
- In general $L(P(x) + x)$ where $L : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ is a linear transformation

Triangular Form, Inversion and Solving Polynomial Equation

- The triangular form results from **invertible** polynomial system
- Triangular form $\Longrightarrow$ decomposition

- Cryptanalytic security: polynomial system corresponding to the permutation or compression function derived from it

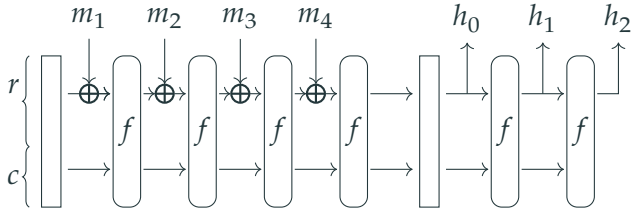
Solving Iterative Triangular Systems (under Constraints)

Constrained Polynomial Equations

- Constraints are due to **compression mode**
- Example: Constrained input constrained output (CICO) originates from Sponge mode

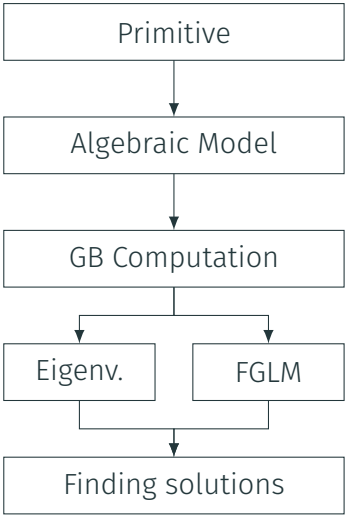
$$P(x_1, x_2, \ldots, x_\mu \| 0^{k_1}) = (y_1, \ldots, y_\nu \| 0^{k_2})$$

- This is CICO-(k_1, k_2)



Gröbner basis: A Method to Solve Polynomial Equations

Cryptanalysis through GB Method



Gröbner basis computation

- Let $f_1, \dots, f_t$ be the polynomials representing a primitive; typically describing round functions
- Consider the ideal $I = \langle f_1, \dots, f_t \rangle$
- We want to find the variety of I i.e. $V(I) = \{a \in \mathbb{F}_q^s : a \text{ is common zero of } f_i\}$
- Gröbner basis $\mathcal{G} = \{g_1, \dots, g_s\}$ is such that $I = \langle g_1, \dots, g_s \rangle$

Basis conversion (obtain univariate polynomial)

- Obtain a "convenient" set of polynomial equations that is easy to solve
- Example: A **triangular** form

Basis conversion

- Common *modus operandi*: converting the GB from a graded monomial ordering to lexicographic
- In cryptanalysis, *Shape lemma is often assumed.*

Shape lemma

Let I be a zero-dimensional radical ideal such that the x_n coordinate of the points in $\mathbb{V}(I)$ are distinct. Let G be a reduced Gröbner basis for I relative to a LEX monomial order with x_n as the last variable. G consists of n polynomials

$$\{x_1 - g_1(x_n), x_2 - g_2(x_n), \dots, g_n(x_n)\}$$

where $\deg(g_i) < \deg(g_n)$ for each $1 \leq i < n$ and $\deg(g_n) = \dim_{\mathbb{K}}(\mathbb{K}[x_1, \dots, x_n]/I)$. We say, equivalently, that the ideal I has shape lemma or shape form.

Shape lemma for zero dimensional ideals

Theorem (Campa and Roy, 2025)

Let $I \subset \mathbb{K}[x_1, \dots, x_n]$ be a zero-dimensional ideal and let G be its Gröbner basis (w.r.t a generic monomial ordering $\prec$) which contains elements f_i such that $\mathrm{LM}(f_i) = x_i^{\alpha_i}$ for each $1 \leq i \leq n$. If I has no solutions at ∞, then the ideal I has a Shape Form in the reduced LEX Gröbner basis.

Gröbner basis: Monomial ordering

Every monomial $m = \prod_{i=1}^{n} x_i^{\alpha_i} \in R$ can be identified with the corresponding vector of exponents $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$.

DRL Monomial ordering

Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say $\alpha >_{\text{DRL}} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and } \alpha >_{\text{RLEX}} \beta.$$

We say $x^\alpha >_{\text{DRL}} x^\beta$ if $\alpha >_{\text{DRL}} \beta$.

Gröbner basis

Gröbner basis

Let $I = \langle f_1, \dots, f_s \rangle$ be an ideal in $\mathbb{K}[x_1, \dots, x_n]$ and let $\prec$ be a valid monomial ordering. A finite subset $G = \{g_1, \dots, g_t\}$ of I different from $\{0\}$ is said to be a **Gröbner Basis** (or Standard Basis) w.r.t. $\prec$ if

$$\langle \mathrm{LM}(g_1), \dots, \mathrm{LM}(g_t) \rangle = \langle \mathrm{LM}(I) \rangle.$$

Reduced Gröbner basis

Let G be a Gröbner basis for the ideal $I \subset \mathbb{K}[x_1, \dots, x_n]$ with respect to a monomial ordering $\prec$, if

- $\mathrm{LC}(g) = 1$ for all $g \in G$
- for all $g \in G$, no monomial of g lies in $\langle \mathrm{LT}(G \backslash \{g\}) \rangle$

G is said to be a **reduced Gröbner basis**.

Complexity

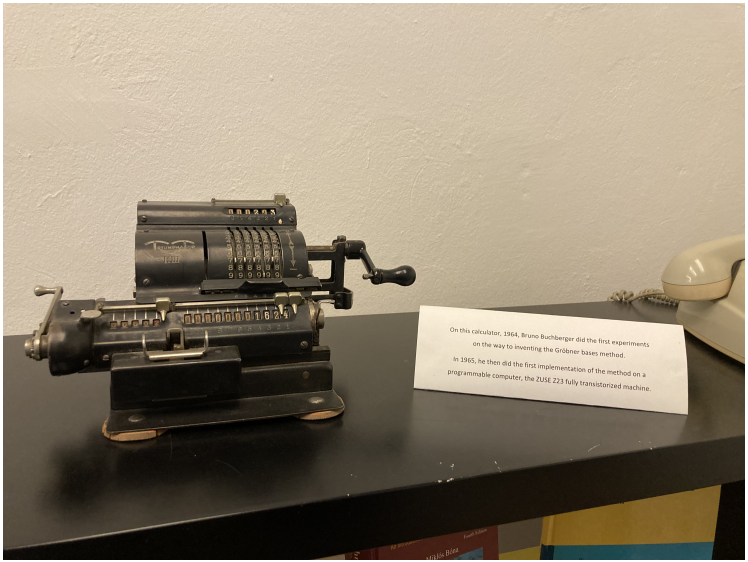
Gröbner basis computation/method

- Is it easy (polynomial time complexity) to compute the GB?
- Can we prove the complexity for a (generic) class of functions/permutations?
- What is the complexity of basis conversion?

Quotient ring dimension

- Decides the complexity of solving the polynomial equations.

Talking about Complexity



Security of An Extended Feistel Family
(work under progress [Campa and Roy])

Iterative Polynomial Instances: Feistel and Extended Feistel

- We consider 4 family of instances that are cryptographically important:
  - Instance-1: known as Unbalanced Feistel Network 1 (UFN-1)
  - Instance-2: known as Unbalanced Feistel Network 2 (UFN-2)
  - Instance-3: known as Balanced Feistel (BFN)
  - Instance-4: known as (multi) rotating Feistel network

Notation:

- R: number of iterations
- Degree d is small (e.g. $d = 3, 5, 7$)

Instance-1

- $g_j = 1$ for all $1 \leq j \leq n$
- $\deg(p_j) = 1$ for all $1 \leq j \leq n$
- if h_j is not a constant polynomial, $\deg(h_j) = d$ for all $1 \leq j \leq n$
- $\mathcal{L}(x_1, \dots, x_n) = (x_2, \dots, x_n, x_1)$
- We employ DRL.

$$\mathcal{L}(\mathcal{F}(\mathbf{x}_i)) = \begin{cases} x_{i,2} \\ x_{i,3} \\ \vdots \\ x_{i,n} \\ x_{i,1} + h(\ell_i(\mathbf{x}_{i,2:n})) \end{cases}$$

where $\ell_i(\mathbf{x}_{i,2:n})$ is a linear combination of the input variables.

Theorem (Gröbner basis for Instance-1)

Let R, n denote the number of rounds and the number of branches respectively. The GB $\mathcal{G}_{DRL}$ for the polynomial system that represents the CICO-$(n-k, k)$ problem of Instance-1 is composed by

- $R - n$ *polynomials of degree* d
- $R - n$ *polynomials of degree* 1.
- $\mathrm{LM}(p_i) = x_{i+n,1}^d$ *for* $1 \leq i \leq R - n$
- $\mathrm{LM}(p_{i+R-n}) = y_{i+n,1}$ *for* $1 \leq i \leq R - n$

where $p_j \in \mathcal{G}$. The defined GB is a reduced GB for Instance-1 and it contains $2(R-n)$ polynomials in $2(R-n)$ variables.

The associated quotient ring dimension is d^{R-n}.

Proof idea

- Stitch together the triangular form to establish the final triangular form
  - Use the linear transformation A in between two consecutive iterations
  - Here it is circular shift of variables
- Shape lemma (Campa and Roy, 2025)) follows by establishing the structures of the polynomials in Gröbner basis
- Prove the quotient ring dimension

Thank you!

Questions?