Gröbner Bases For Feistel Designs With Application To GMiMC

Matthias Johann Steiner

mattsteiner@edu.aau.at

Alpen-Adria-Universität Klagenfurt, Klagenfurt am Wörthersee, Austria

Outline

1. Motivation
2. Gröbner Bases
3. $\texttt{GMiMC}_{\text{erf}}$
4. Constructing A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis
   - Examples
5. System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis
6. $\texttt{GMiMC}_{\text{erf}}$ Cryptanalysis
   - What went wrong?
7. Further Outlook
8. References

Motivation

- In past 10 years many novel symmetric designs for Homomorphic Encryption (HE), Multi-Party Computation (MPC) and Zero-Knowledge (ZK) have been introduced.
    - Native over prime field $\mathbb{F}_p$.
    - Multiplicative complexity one of the main performance metrics.
    - Often low degree polynomials at round level.
    - Compiled list of Arithmetization-Oriented (AO) Primitives: `https://stap-zoo.com/all-stap-primitives/`.
- Algebraic attacks major challenge in cryptanalysis.
    - Interpolation attacks.
    - Polynomial system solving.

Feistel Networks

- Long track record in the literature.
- Well-understood statistical properties.
- Very flexible.

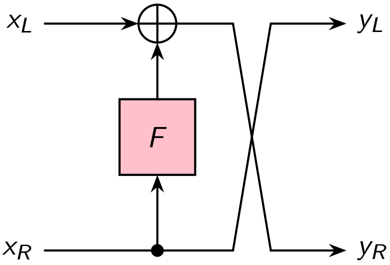


Figure: Classic two branch Feistel Network.

Arithmetization-Oriented Feistel Networks

Feistel Designs

- GMiMC (MPC, ZK) [AGP+19a].
- Ciminion (MPC) [GØSW23].
- Rubato (HE) [HKL+22].

Designs With Feistel Components

- Hydra (MPC) [GØSW23].
- Anemoi (ZK) [BBC+23].
- Monolith (ZK) [GKL+24].

Gröbner Bases I

- Invented by Austrian mathematician Bruno Buchberger in his PhD thesis at Universität Innsbruck [Buc65].
- Provides a general framework to solve fully determined polynomial systems.
- **Terminology:**
  - K a field, $\mathbb{F}_q$ a field with q elements.
  - $P = K[x_1, \ldots, x_n]$.
  - $I \subset P$ is an ideal if:
    - $0 \in I$.
    - $a, b \in I \Rightarrow a - b \in I$.
    - $r \in P,\ a \in I \Rightarrow a \cdot r \in I$.
  - We think of a polynomial system $\mathcal{F} \subset P$ as ideal $(\mathcal{F})$.

Gröbner Bases II

Term Orders on P

- A monomial $m = \prod_{i=1}^{n} x_i^{a_i} \in P$ can be identified with a vector $\boldsymbol{a} \in \mathbb{Z}_{\geq 0}^{n}$.
- A term order $>$ on P satisfies:
  - $>$ is a total ordering on $\mathbb{Z}_{\geq 0}^{n}$.
  - $\boldsymbol{a} > \boldsymbol{b}$ and $\boldsymbol{c} \in \mathbb{Z}_{\geq 0}$, then $\boldsymbol{a} + \boldsymbol{c} > \boldsymbol{b} + \boldsymbol{c}$.
  - $>$ is a well-ordering on $\mathbb{Z}_{\geq 0}^{n}$.
- $f \in P$, then $\mathrm{LM}_{>}(f)$ is the largest monomial in f under $>$.

Gröbner Bases III

Degree Reverse Lexicographic (DRL) Term Order

$\boldsymbol{a} >_{DRL} \boldsymbol{b}$ if either

- $\sum_{i=1}^{n} a_i > \sum_{i=1}^{n} b_i$, or
- $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ and right-most non-zero entry of $\boldsymbol{a} - \boldsymbol{b}$ is negative.

Gröbner Bases III

Degree Reverse Lexicographic (DRL) Term Order

$\boldsymbol{a} >_{DRL} \boldsymbol{b}$ if either

- $\sum_{i=1}^{n} a_i > \sum_{i=1}^{n} b_i$, or
- $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ and right-most non-zero entry of $\boldsymbol{a} - \boldsymbol{b}$ is negative.

Gröbner Basis

- $I \subset P$ ideal, $>$ term order on P.
- $\mathcal{G} \subset P$ is Gröbner basis if
  - $(\mathcal{G}) = I$, and
  - $(\mathrm{LM}_>(g) \mid g \in \mathcal{G}) = (\mathrm{LM}_>(f) \mid f \in I)$.

Gröbner Bases IV

Pairwise Coprime Leading Monomials

- $\mathcal{G} \subset P$, $>$ term order on P.
- $\forall f, g \in \mathcal{G}$, $f \neq g$,

$$\operatorname{gcd}\Big(\mathrm{LM}_>(f), \mathrm{LM}_>(g)\Big) = 1.$$

- $\Rightarrow \mathcal{G}$ is $>$-Gröbner basis [CLO15, Chapter 2 §9].

Gröbner Bases IV

Pairwise Coprime Leading Monomials

- $\mathcal{G} \subset P$, $>$ term order on P.
- $\forall f, g \in \mathcal{G}$, $f \neq g$,

$$\gcd \Big(\text{LM}_>(f), \text{LM}_>(g) \Big) = 1.$$

- $\Rightarrow \mathcal{G}$ is $>$-Gröbner basis [CLO15, Chapter 2 §9].

Example

- $\mathcal{F} = \{f_1, \ldots, f_n\} \subset K[x_1, \ldots, x_n]$ such that for all $1 \leq i \leq n$

$$\text{LM}_{DRL}(f_i) = x_i^d.$$

- $\Rightarrow \mathcal{F}$ is DRL Gröbner basis.

$\texttt{GMiMC}_{\text{erf}}$ I

- Operates on $\mathbb{F}_q^n$.
- Cubing as non-linear function.
- $c_i \in \mathbb{F}_q$ round constant.
- Two key sizes: $\boldsymbol{k} \in \mathbb{F}_q^n$ or $k \in \mathbb{F}_q$.
- Sponge mode for hash function.

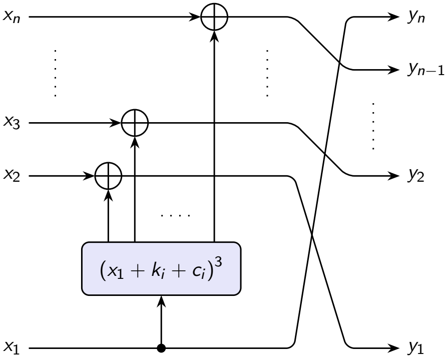


Figure: Keyed $\texttt{GMiMC}_{\text{erf}}$ round function.

$\texttt{GMiMC}_{\text{erf}}$ II

- Multivariate key $\boldsymbol{k} \in \mathbb{F}_q^n$.
  - Needs key schedule matrix $\boldsymbol{M}_{\mathcal{K}} \in \mathbb{F}_q^{n \times n}$ such that
    - $\det(\boldsymbol{M}_{\mathcal{K}}) \neq 0$, and
    - for all $1 \leq i \leq \left\lceil \frac{r}{n} \right\rceil$ all entries in $\boldsymbol{M}_{\mathcal{K}}^i$ are non-zero.
  - Set $\boldsymbol{K} = \left(\boldsymbol{M}_{\mathcal{K}} \boldsymbol{k}, \dots, \boldsymbol{M}_{\mathcal{K}}^{\left\lceil \frac{r}{n} \right\rceil} \boldsymbol{k} \right)^{\intercal} \in \mathbb{F}_q^{n \cdot \left\lceil \frac{r}{n} \right\rceil}$.
  - $k_i = K_i$.

$\texttt{GMiMC}_{\text{erf}}$ II

- Multivariate key $\boldsymbol{k} \in \mathbb{F}_q^n$.
    - Needs key schedule matrix $\boldsymbol{M}_{\mathcal{K}} \in \mathbb{F}_q^{n \times n}$ such that
        - $\det\left(\boldsymbol{M}_{\mathcal{K}}\right) \neq 0$, and
        - for all $1 \leq i \leq \left\lceil \frac{r}{n} \right\rceil$ all entries in $\boldsymbol{M}_{\mathcal{K}}^i$ are non-zero.
    - Set $\boldsymbol{K} = \left(\boldsymbol{M}_{\mathcal{K}} \boldsymbol{k}, \dots, \boldsymbol{M}_{\mathcal{K}}^{\left\lceil \frac{r}{n} \right\rceil} \boldsymbol{k}\right)^\intercal \in \mathbb{F}_q^{n \cdot \left\lceil \frac{r}{n} \right\rceil}$.
    - $k_i = K_i$.
- Univariate key $k \in \mathbb{F}_q$.
    - $k_i = k$ for all rounds.

UNIVERSITÄT KLAGENFURT

$\texttt{GMiMC}_{\mathsf{erf}}$ Polynomial System

- $\boldsymbol{p}, \boldsymbol{c} \in \mathbb{F}_q^n$ encrypted under key $\boldsymbol{k} \in \mathbb{F}_q^n$.

$\texttt{GMiMC}_{\text{erf}}$ Polynomial System

- $\boldsymbol{p}, \boldsymbol{c} \in \mathbb{F}_q^n$ encrypted under key $\boldsymbol{k} \in \mathbb{F}_q^n$.
- Introduce variables after every round function

$$\mathcal{F}_{\texttt{GMiMC}_{\text{erf}}} : \begin{cases} \mathcal{R}^{(1)} \left(\boldsymbol{p}, \boldsymbol{y} \right) - \boldsymbol{x}^{(1)} = 0, & \\ \mathcal{R}^{(i)} \left(\boldsymbol{x}^{(i-1)}, \boldsymbol{y} \right) - \boldsymbol{x}^{(i)} = 0, & 2 \leq i \leq r - 1, \\ \mathcal{R}^{(r)} \left(\boldsymbol{x}^{(r-1)}, \boldsymbol{y} \right) - \boldsymbol{c} = 0, & \end{cases}$$

where $\boldsymbol{y} = (y_1, \ldots, y_n)^\intercal$ and $\boldsymbol{x}^{(i)} = \left(x_1^{(i)}, \ldots, x_n^{(i)} \right)$.

$\texttt{GMiMC}_{\text{erf}}$ Polynomial System

- $\boldsymbol{p}, \boldsymbol{c} \in \mathbb{F}_q^n$ encrypted under key $\boldsymbol{k} \in \mathbb{F}_q^n$.
- Introduce variables after every round function

$$\mathcal{F}_{\texttt{GMiMC}_{\text{erf}}}: \begin{cases} \mathcal{R}^{(1)}\left(\boldsymbol{p}, \boldsymbol{y}\right) - \boldsymbol{x}^{(1)} = 0, & \\ \mathcal{R}^{(i)}\left(\boldsymbol{x}^{(i-1)}, \boldsymbol{y}\right) - \boldsymbol{x}^{(i)} = 0, & 2 \leq i \leq r-1, \\ \mathcal{R}^{(r)}\left(\boldsymbol{x}^{(r-1)}, \boldsymbol{y}\right) - \boldsymbol{c} = 0, & \end{cases}$$

where $\boldsymbol{y} = (y_1, \ldots, y_n)^\intercal$ and $\boldsymbol{x}^{(i)} = \left(x_1^{(i)}, \ldots, x_n^{(i)}\right)$.

- $\mathcal{F}_{\texttt{GMiMC}_{\text{erf}}} \subset \mathbb{F}_q\left[\boldsymbol{x}^{(i)}, \boldsymbol{y} \;\middle|\; 1 \leq i \leq r-1\right]$ consists of $r \cdot n$ equations in $r \cdot n$ variables.

Transforming The $\mathtt{GMiMC}_{\text{erf}}$ System I

- $\boldsymbol{Y} = \left(\boldsymbol{y}, \boldsymbol{M}_{\mathcal{K}}\boldsymbol{y}, \dots, \boldsymbol{M}_{\mathcal{K}}^{\lceil \frac{r}{n} \rceil - 1}\boldsymbol{y}\right)^{\intercal}$.
- For $1 < i < r$ let us take a closer look:

$$\begin{pmatrix} x_2^{(i-1)} + \left(x_1^{(i-1)} + Y_i + c_i\right)^3 \\ \vdots \\ x_n^{(i-1)} + \left(x_1^{(i-1)} + Y_i + c_i\right)^3 \\ x_1^{(i-1)} \end{pmatrix} = \begin{pmatrix} x_1^{(i)} \\ \vdots \\ x_n^{(i)} \end{pmatrix}.$$

Transforming The $\mathtt{GMiMC}_{\text{erf}}$ System II

- Transform to

$$\begin{pmatrix} x_2^{(i-1)} + \left(x_1^{(i-1)} + Y_i + c_i\right)^3 \\ -x_2^{(i-1)} + x_3^{(i-1)} \\ \vdots \\ -x_2^{(i-1)} + x_n^{(i-1)} \\ x_1^{(i-1)} \end{pmatrix} = \begin{pmatrix} x_1^{(i)} \\ -x_1^{(i)} + x_2^{(i)} \\ \vdots \\ -x_1^{(i)} + x_{n-1}^{(i)} \\ x_n^{(i)} \end{pmatrix}.$$

UNIVERSITÄT KLAGENFURT

Transforming The $\texttt{GMiMC}_{\text{erf}}$ System II

- Transform to

$$\begin{pmatrix} x_2^{(i-1)} + \left(x_1^{(i-1)} + Y_i + c_i\right)^3 \\ -x_2^{(i-1)} + x_3^{(i-1)} \\ \vdots \\ -x_2^{(i-1)} + x_n^{(i-1)} \\ x_1^{(i-1)} \end{pmatrix} = \begin{pmatrix} x_1^{(i)} \\ -x_1^{(i)} + x_2^{(i)} \\ \vdots \\ -x_1^{(i)} + x_{n-1}^{(i)} \\ x_n^{(i)} \end{pmatrix}.$$

- Transform $\mathcal{F}_{\texttt{GMiMC}_{\text{erf}}}$ to r cubic polynomials $\mathcal{F}_{\text{cub}}$ and $r \cdot (n-1)$ affine polynomials $\mathcal{F}_{\text{lin}}$.

Transforming The $\texttt{GMiMC}_{\text{erf}}$ System II

- Transform to

$$\begin{pmatrix} x_2^{(i-1)} + \left(x_1^{(i-1)} + Y_i + c_i\right)^3 \\ -x_2^{(i-1)} + x_3^{(i-1)} \\ \vdots \\ -x_2^{(i-1)} + x_n^{(i-1)} \\ x_1^{(i-1)} \end{pmatrix} = \begin{pmatrix} x_1^{(i)} \\ -x_1^{(i)} + x_2^{(i)} \\ \vdots \\ -x_1^{(i)} + x_{n-1}^{(i)} \\ x_n^{(i)} \end{pmatrix}.$$

- Transform $\mathcal{F}_{\texttt{GMiMC}_{\text{erf}}}$ to r cubic polynomials $\mathcal{F}_{\text{cub}}$ and $r \cdot (n-1)$ affine polynomials $\mathcal{F}_{\text{lin}}$.
- If $\text{rank}\left(\mathcal{F}_{\text{lin}}\right) = r \cdot (n-1)$, then reduce to r cubic equations in r variables.

Transforming The $\texttt{GMiMC}_{\text{erf}}$ System III

- What happens to the cubic term $\left(x_1^{(i-1)} + Y_i + c_i\right)^3$?
  - $x_1^{(i-1)} + Y_i \mod (\mathcal{F}_{\text{lin}}) = \mathcal{L}_i + a_i$, where $\mathcal{L}_i$ is a linear polynomial and $a_i \in \mathbb{F}_q$.

Transforming The $\mathtt{GMiMC}_{\mathrm{erf}}$ System III

- What happens to the cubic term $\left(x_1^{(i-1)} + Y_i + c_i\right)^3$?
  - $x_1^{(i-1)} + Y_i \mod (\mathcal{F}_{\mathrm{lin}}) = \mathcal{L}_i + a_i$, where $\mathcal{L}_i$ is a linear polynomial and $a_i \in \mathbb{F}_q$.
  - $\Rightarrow \left(x_1^{(i-1)} + Y_i + c_i\right)^3 \mod (\mathcal{F}_{\mathrm{lin}}) = (\mathcal{L}_i + a_i + c_i)^3$.

Transforming The $\texttt{GMiMC}_{\mathsf{erf}}$ System III

- What happens to the cubic term $\left(x_1^{(i-1)} + Y_i + c_i\right)^3$?
  - $x_1^{(i-1)} + Y_i \mod (\mathcal{F}_{\mathrm{lin}}) = \mathcal{L}_i + a_i$, where $\mathcal{L}_i$ is a linear polynomial and $a_i \in \mathbb{F}_q$.
  - $\Rightarrow \left(x_1^{(i-1)} + Y_i + c_i\right)^3 \mod (\mathcal{F}_{\mathrm{lin}}) = (\mathcal{L}_i + a_i + c_i)^3$.
  - All cubic monomials in round i come from $(\mathcal{L}_i)^3$.

Transforming The $\mathtt{GMiMC}_{\mathsf{erf}}$ System III

- What happens to the cubic term $\left(x_1^{(i-1)} + Y_i + c_i \right)^3$?
    - $x_1^{(i-1)} + Y_i \mod (\mathcal{F}_{\text{lin}}) = \mathcal{L}_i + a_i$, where $\mathcal{L}_i$ is a linear polynomial and $a_i \in \mathbb{F}_q$.
    - $\Rightarrow \left(x_1^{(i-1)} + Y_i + c_i \right)^3 \mod (\mathcal{F}_{\text{lin}}) = (\mathcal{L}_i + a_i + c_i)^3$.
    - All cubic monomials in round i come from $(\mathcal{L}_i)^3$.
- If we can perform a change of variables $\hat{x}_i = \mathcal{L}_i$, then

$$\mathcal{F}_{\text{cub}} \mapsto \left\{ \hat{x}_i^3 + \alpha_i \cdot \hat{x}_i^2 + \mathcal{A}_i = 0, \qquad 1 \leq i \leq r, \right.$$

where $\mathcal{A}_i \in \mathbb{F}_q\left[\hat{x}_i \;\middle|\; 1 \leq i \leq r\right]$ is affine.

Transforming The $\texttt{GMiMC}_{\text{erf}}$ System III

- What happens to the cubic term $\left(x_1^{(i-1)} + Y_i + c_i\right)^3$?
    - $x_1^{(i-1)} + Y_i \mod (\mathcal{F}_{\text{lin}}) = \mathcal{L}_i + a_i$, where $\mathcal{L}_i$ is a linear polynomial and $a_i \in \mathbb{F}_q$.
    - $\Rightarrow \left(x_1^{(i-1)} + Y_i + c_i\right)^3 \mod (\mathcal{F}_{\text{lin}}) = (\mathcal{L}_i + a_i + c_i)^3$.
    - All cubic monomials in round i come from $(\mathcal{L}_i)^3$.
- If we can perform a change of variables $\hat{x}_i = \mathcal{L}_i$, then

$$\mathcal{F}_{\text{cub}} \mapsto \left\{\hat{x}_i^3 + \alpha_i \cdot \hat{x}_i^2 + \mathcal{A}_i = 0, \qquad 1 \leq i \leq r,\right.$$

where $\mathcal{A}_i \in \mathbb{F}_q\left[\hat{x}_i \;\middle|\; 1 \leq i \leq r\right]$ is affine.

- Change of variables possible if $\operatorname{rank}(\mathcal{L}_1, \dots, \mathcal{L}_r) = r$.

Transforming The $\texttt{GMiMC}_{\text{erf}}$ System III

- What happens to the cubic term $\left(x_1^{(i-1)} + Y_i + c_i \right)^3$?
  - $x_1^{(i-1)} + Y_i \mod (\mathcal{F}_{\text{lin}}) = \mathcal{L}_i + a_i$, where $\mathcal{L}_i$ is a linear polynomial and $a_i \in \mathbb{F}_q$.
  - $\Rightarrow \left(x_1^{(i-1)} + Y_i + c_i \right)^3 \mod (\mathcal{F}_{\text{lin}}) = (\mathcal{L}_i + a_i + c_i)^3$.
  - All cubic monomials in round i come from $(\mathcal{L}_i)^3$.
- If we can perform a change of variables $\hat{x}_i = \mathcal{L}_i$, then

$$\mathcal{F}_{\text{cub}} \mapsto \left\{ \hat{x}_i^3 + \alpha_i \cdot \hat{x}_i^2 + \mathcal{A}_i = 0, \qquad 1 \leq i \leq r, \right.$$

where $\mathcal{A}_i \in \mathbb{F}_q \left[\hat{x}_i \;\middle|\; 1 \leq i \leq r \right]$ is affine.

  - Change of variables possible if $\text{rank}\left(\mathcal{L}_1, \ldots, \mathcal{L}_r \right) = r$.
  - For DRL pairwise coprime leading monomials ⇒ DRL Gröbner basis.

Efficient Testing For A DRL Gröbner Basis

- For change of variables we must have that $\text{rank}\left(\mathcal{F}_{\text{lin}}\right) = r \cdot (n - 1)$ and $\text{rank}\left(\mathcal{L}_1, \dots, \mathcal{L}_r\right) = r$.
  - For efficient verification we can delete constant terms in $\mathcal{F}_{\text{lin}}$.
  - Add the linear equations from the cubic terms.

Efficient Testing For A DRL Gröbner Basis

- For change of variables we must have that $\operatorname{rank}(\mathcal{F}_{\mathrm{lin}}) = r \cdot (n-1)$ and $\operatorname{rank}(\mathcal{L}_1, \dots, \mathcal{L}_r) = r$.
    - For efficient verification we can delete constant terms in $\mathcal{F}_{\mathrm{lin}}$.
    - Add the linear equations from the cubic terms.
- E.g., for $1 < i < r$ this yields

$$\left\{ \begin{array}{r} x_1^{(i-1)} + Y_i, \\ \left(-x_2^{(i-1)} + x_{j+1}^{(i-1)}\right) - \left(-x_1^{(i)} + x_j^{(i)}\right), \\ x_1^{(i-1)} - x_n^{(i)} \end{array} \right\}_{2 \leq j \leq n-1} .$$

Efficient Testing For A DRL Gröbner Basis

- For change of variables we must have that $\operatorname{rank}(\mathcal{F}_{\text{lin}}) = r \cdot (n-1)$ and $\operatorname{rank}(\mathcal{L}_1, \dots, \mathcal{L}_r) = r$.
    - For efficient verification we can delete constant terms in $\mathcal{F}_{\text{lin}}$.
    - Add the linear equations from the cubic terms.
- E.g., for $1 < i < r$ this yields

$$\left\{ \begin{array}{r} x_1^{(i-1)} + Y_i, \\ \left(-x_2^{(i-1)} + x_{j+1}^{(i-1)}\right) - \left(-x_1^{(i)} + x_j^{(i)}\right), \\ x_1^{(i-1)} - x_n^{(i)} \end{array} \right\}_{2 \leq j \leq n-1}.$$

- Implement computer algebra program of your choice.

Examples

Example 1

- $q = 2^{64} - 2^{32} + 1$, $n = 3$, $\boldsymbol{M}_{\mathcal{K}} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$.
- Change of variables works for all integers $r \in [5, 100]$ with $r \not\equiv -1 \mod 6$.

Examples

Example 1

- $q = 2^{64} - 2^{32} + 1$, $n = 3$, $\boldsymbol{M}_{\mathcal{K}} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$.
- Change of variables works for all integers $r \in [5, 100]$ with $r \not\equiv -1 \mod 6$.

Example 2

- $q = 2^{31} - 1$, $n = 4$, $\boldsymbol{M}_{\mathcal{K}} = \begin{pmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{pmatrix}$.
- Change of variables works for all integers $r \in [5, 100]$.

Outline

1 Motivation

2 Gröbner Bases

3 $\texttt{GMiMC}_{\text{erf}}$

4 Constructing A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis
- Examples

5 System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis

6 $\texttt{GMiMC}_{\text{erf}}$ Cryptanalysis
- What went wrong?

7 Further Outlook

8 References

UNIVERSITÄT KLAGENFURT

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis I

$P = \mathbb{F}_q \left[\hat{x}_i \;\middle|\; 1 \leq i \leq r \right]$

- Want to solve the `GMiMC` DRL Gröbner basis for the key

$$\mathcal{G}_{\texttt{GMiMC}_{\text{erf}}} \colon \left\{ \hat{x}_i^3 + \alpha_i \cdot \hat{x}_i^2 + \mathcal{A}_i = 0, \qquad 1 \leq i \leq r. \right.$$

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis I

$P = \mathbb{F}_q \left[\hat{x}_i \;\middle|\; 1 \leq i \leq r \right]$

- Want to solve the $\texttt{GMiMC}$ DRL Gröbner basis for the key

$$\mathcal{G}_{\texttt{GMiMC}_{\text{erf}}} \colon \left\{ \hat{x}_i^3 + \alpha_i \cdot \hat{x}_i^2 + \mathcal{A}_i = 0, \qquad 1 \leq i \leq r. \right.$$

- As $\mathbb{F}_q$-vector spaces

$$R := P / \left(\mathcal{G}_{\texttt{GMiMC}_{\text{erf}}} \right) \cong P / \left(\hat{x}_i^3 \mid 1 \leq i \leq r \right),$$

$$\dim_{\mathbb{F}_q} (R) = 3^r.$$

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis I

$P = \mathbb{F}_q \left[\hat{x}_i \;\middle|\; 1 \leq i \leq r \right]$

- Want to solve the $\texttt{GMiMC}$ DRL Gröbner basis for the key

$$\mathcal{G}_{\texttt{GMiMC}_{\text{erf}}} \colon \left\{ \hat{x}_i^3 + \alpha_i \cdot \hat{x}_i^2 + \mathcal{A}_i = 0, \qquad 1 \leq i \leq r. \right.$$

- As $\mathbb{F}_q$-vector spaces

$$R := P / \left(\mathcal{G}_{\texttt{GMiMC}_{\text{erf}}} \right) \cong P / \left(\hat{x}_i^3 \;\middle|\; 1 \leq i \leq r \right),$$

$$\dim_{\mathbb{F}_q} (R) = 3^r.$$

- For every $f \in P$, the multiplication map

$$\theta_f : R \to R, \qquad x \mapsto x \cdot f$$

is $\mathbb{F}_q$-linear $\Rightarrow$ *Multiplication Matrix* $\boldsymbol{M}_f \in \mathbb{F}_q^{3^r \times 3^r}$.

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis II

- If $\boldsymbol{a} \in \overline{\mathbb{F}_q}^r$ is root of $(\mathcal{G}_{\texttt{GMiMC}_{\text{erf}}}) \Rightarrow f(\boldsymbol{a})$ is eigenvalue of $\boldsymbol{M}_f$ [KR16, Proposition 6.2.1].

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis II

- If $\boldsymbol{a} \in \overline{\mathbb{F}_q}^r$ is root of $\left(\mathcal{G}_{\texttt{GMiMC}_{\text{erf}}}\right) \Rightarrow f(\boldsymbol{a})$ is eigenvalue of $\boldsymbol{M}_f$ [KR16, Proposition 6.2.1].
- Let $\mathcal{B}' \subset \mathbb{F}_q\left[\hat{x}_i \;\middle|\; 2 \leq i \leq r\right] / \left(\hat{x}_i^3 \;\middle|\; 2 \leq i \leq r\right)$ be a vector space basis, then

$$\mathcal{B} = \mathcal{B}' \cup \hat{x}_1 \cdot \mathcal{B}' \cup \hat{x}_1^2 \cdot \mathcal{B}'$$

is vector space basis of $\mathcal{R}$.

UNIVERSITÄT KLAGENFURT

System Solving With A `GMiMC`$_{\text{erf}}$ Gröbner Basis III

- Then for $f = \hat{x}_1$ [BBL$^+$24, Lemma 2]

$$\boldsymbol{M}_{\hat{x}_1} = \begin{array}{cc} \begin{array}{ccc} \mathcal{B}' & \hat{x}_1 \cdot \mathcal{B}' & \hat{x}_1^2 \cdot \mathcal{B}' \end{array} & \\ \begin{pmatrix} 0 & \boldsymbol{I} & 0 \\ 0 & 0 & \boldsymbol{I} \\ \boldsymbol{M}_0 & \boldsymbol{M}_1 & \boldsymbol{M}_2 \end{pmatrix} & \begin{array}{c} \hat{x}_1 \cdot \mathcal{B}' \\ \hat{x}_1^2 \cdot \mathcal{B}' \\ \hat{x}_1^3 \cdot \mathcal{B}' \end{array} \end{array},$$

$$\begin{aligned} \chi_{\hat{x}_1}(x) &= \det \left(\boldsymbol{I} \cdot x - \boldsymbol{M}_{\hat{x}_1} \right) \\ &= \pm \det \left(\boldsymbol{I} \cdot x^3 - \boldsymbol{M}_2 \cdot x^2 - \boldsymbol{M}_1 \cdot x - \boldsymbol{M}_0 \right). \end{aligned}$$

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis III

- Then for $f = \hat{x}_1$ [BBL$^+$24, Lemma 2]

$$\begin{array}{cc} & \begin{array}{ccc} \mathcal{B}' & \hat{x}_1 \cdot \mathcal{B}' & \hat{x}_1^2 \cdot \mathcal{B}' \end{array} & \\ \boldsymbol{M}_{\hat{x}_1} = & \begin{pmatrix} 0 & \boldsymbol{I} & 0 \\ 0 & 0 & \boldsymbol{I} \\ \boldsymbol{M}_0 & \boldsymbol{M}_1 & \boldsymbol{M}_2 \end{pmatrix} & \begin{array}{c} \hat{x}_1 \cdot \mathcal{B}' \\ \hat{x}_1^2 \cdot \mathcal{B}' \\ \hat{x}_1^3 \cdot \mathcal{B}' \end{array} \end{array},$$

$$\begin{aligned} \chi_{\hat{x}_1}(x) &= \det\left(\boldsymbol{I} \cdot x - \boldsymbol{M}_{\hat{x}_1}\right) \\ &= \pm \det\left(\boldsymbol{I} \cdot x^3 - \boldsymbol{M}_2 \cdot x^2 - \boldsymbol{M}_1 \cdot x - \boldsymbol{M}_0\right). \end{aligned}$$

- Characteristic polynomial can be computed in [BBL$^+$24, §3.2]

$$\mathcal{C}_{\text{char-poly}} = \mathcal{O}\left(3 \cdot \log_2(3)^2 \cdot \left(1 + \log_2\left(\log_2(3)\right)\right) \cdot 3^{\omega \cdot (r-1)}\right)$$

field operations, where $2 \leq \omega < 2.371552$ [WXXZ24].

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis IV

$\texttt{GMiMC}_{\text{erf}}$ Gröbner basis

$$\begin{aligned}
\hat{x}_1^3 + \alpha_1 \cdot \hat{x}_1^2 + \mathcal{A}_1 &= 0, \\
\hat{x}_2^3 + \alpha_2 \cdot \hat{x}_2^2 + \mathcal{A}_2 &= 0, \\
&\vdots \\
\hat{x}_n^3 + \alpha_n \cdot \hat{x}_n^2 + \mathcal{A}_n &= 0.
\end{aligned}$$

$\texttt{GMiMC}_{\text{erf}}$ substitution variables

$$\begin{aligned}
\hat{x}_1 &= y_1, \\
\hat{x}_2 &= x_1^{(1)} + y_2, \\
&\vdots \\
\hat{x}_n &= x_1^{(n-1)} + y_n,
\end{aligned}$$

- Characteristic polynomial for $\hat{x}_1$ $\Rightarrow$ Key guess for y_1.

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis IV

$\texttt{GMiMC}_{\text{erf}}$ Gröbner basis

$$\begin{gathered}\hat{x}_1^3 + \alpha_1 \cdot \hat{x}_1^2 + \mathcal{A}_1 = 0,\\ \hat{x}_2^3 + \alpha_2 \cdot \hat{x}_2^2 + \mathcal{A}_2 = 0,\\ \vdots \\ \hat{x}_n^3 + \alpha_n \cdot \hat{x}_n^2 + \mathcal{A}_n = 0.\end{gathered}$$

$\texttt{GMiMC}_{\text{erf}}$ substitution variables

$$\begin{aligned}\hat{x}_1 &= y_1,\\ \hat{x}_2 &= x_1^{(1)} + y_2,\\ &\vdots\\ \hat{x}_n &= x_1^{(n-1)} + y_n,\end{aligned}$$

- Characteristic polynomial for $\hat{x}_1 \Rightarrow$ Key guess for y_1.
- Substitute $\hat{x}_1 = y_1$ back into system to eliminate $\hat{x}_1$.

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis IV

$\texttt{GMiMC}_{\text{erf}}$ Gröbner basis

$$\begin{aligned} \hat{x}_1^3 + \alpha_1 \cdot \hat{x}_1^2 + \mathcal{A}_1 &= 0, \\ \hat{x}_2^3 + \alpha_2 \cdot \hat{x}_2^2 + \mathcal{A}_2 &= 0, \\ &\vdots \\ \hat{x}_n^3 + \alpha_n \cdot \hat{x}_n^2 + \mathcal{A}_n &= 0. \end{aligned}$$

$\texttt{GMiMC}_{\text{erf}}$ substitution variables

$$\begin{aligned} \hat{x}_1 &= y_1, \\ \hat{x}_2 &= x_1^{(1)} + y_2, \\ &\vdots \\ \hat{x}_n &= x_1^{(n-1)} + y_n, \end{aligned}$$

- Characteristic polynomial for $\hat{x}_1 \Rightarrow$ Key guess for y_1.
- Substitute $\hat{x}_1 = y_1$ back into system to eliminate $\hat{x}_1$.
- Ignore first polynomial $\Rightarrow$ DRL Gröbner basis in $r - 1$ variables.

System Solving With A $\texttt{GMiMC}_{\mathrm{erf}}$ Gröbner Basis IV

$\texttt{GMiMC}_{\mathrm{erf}}$ Gröbner basis

$$\begin{aligned} \hat{x}_1^3 + \alpha_1 \cdot \hat{x}_1^2 + \mathcal{A}_1 &= 0, \\ \hat{x}_2^3 + \alpha_2 \cdot \hat{x}_2^2 + \mathcal{A}_2 &= 0, \\ &\vdots \\ \hat{x}_n^3 + \alpha_n \cdot \hat{x}_n^2 + \mathcal{A}_n &= 0. \end{aligned}$$

$\texttt{GMiMC}_{\mathrm{erf}}$ substitution variables

$$\begin{aligned} \hat{x}_1 &= y_1, \\ \hat{x}_2 &= x_1^{(1)} + y_2, \\ &\vdots \\ \hat{x}_n &= x_1^{(n-1)} + y_n, \end{aligned}$$

- Characteristic polynomial for $\hat{x}_1$ ⇒ Key guess for y_1.
- Substitute $\hat{x}_1 = y_1$ back into system to eliminate $\hat{x}_1$.
- Ignore first polynomial ⇒ DRL Gröbner basis in $r - 1$ variables.
- Characteristic polynomial for $\hat{x}_2$ ⇒ Key guess for y_2.

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis IV

$\texttt{GMiMC}_{\text{erf}}$ Gröbner basis

$$\begin{aligned}
\hat{x}_1^3 + \alpha_1 \cdot \hat{x}_1^2 + \mathcal{A}_1 &= 0, \\
\hat{x}_2^3 + \alpha_2 \cdot \hat{x}_2^2 + \mathcal{A}_2 &= 0, \\
&\vdots \\
\hat{x}_n^3 + \alpha_n \cdot \hat{x}_n^2 + \mathcal{A}_n &= 0.
\end{aligned}$$

$\texttt{GMiMC}_{\text{erf}}$ substitution variables

$$\begin{aligned}
\hat{x}_1 &= y_1, \\
\hat{x}_2 &= x_1^{(1)} + y_2, \\
&\vdots \\
\hat{x}_n &= x_1^{(n-1)} + y_n,
\end{aligned}$$

- Characteristic polynomial for $\hat{x}_1$ ⇒ Key guess for y_1.
- Substitute $\hat{x}_1 = y_1$ back into system to eliminate $\hat{x}_1$.
- Ignore first polynomial ⇒ DRL Gröbner basis in $r - 1$ variables.
- Characteristic polynomial for $\hat{x}_2$ ⇒ Key guess for y_2.
- Iterate.

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis V

- Dominating complexity for iterated solving

$$
\begin{aligned}
&\mathcal{O} \left(\sum_{i=1}^{n} N^{i-1} \cdot \mathcal{C}_{\text{char-poly}}(r - i + 1, \omega) \right) \\
&\in \mathcal{O} \left(3 \cdot \log_2(3)^2 \cdot \Big(1 + \log_2 \big(\log_2(3) \big) \Big) \cdot \frac{3^{\omega \cdot r} - N^n}{3^{\omega} - N} \right),
\end{aligned}
$$

where N is a bound on the $\mathbb{F}_q$-valued solutions in each iteration.

System Solving With A $\texttt{GMiMC}_{\mathrm{erf}}$ Gröbner Basis V

- Dominating complexity for iterated solving

$$\mathcal{O}\left(\sum_{i=1}^{n} N^{i-1} \cdot \mathcal{C}_{\text{char-poly}}(r - i + 1, \omega)\right)$$
$$\in \mathcal{O}\left(3 \cdot \log_2(3)^2 \cdot \Big(1 + \log_2\big(\log_2(3)\big)\Big) \cdot \frac{3^{\omega \cdot r} - N^n}{3^\omega - N}\right),$$

  where N is a bound on the $\mathbb{F}_q$-valued solutions in each iteration.

- N a priori unknown but can be avoided with additional plain/ciphertext samples.

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis V

- Dominating complexity for iterated solving

$$\mathcal{O}\left(\sum_{i=1}^{n} N^{i-1} \cdot \mathcal{C}_{\text{char-poly}}(r - i + 1, \omega)\right)$$
$$\in \mathcal{O}\left(3 \cdot \log_2(3)^2 \cdot \Big(1 + \log_2\big(\log_2(3)\big)\Big) \cdot \frac{3^{\omega \cdot r} - N^n}{3^\omega - N}\right),$$

  where N is a bound on the $\mathbb{F}_q$-valued solutions in each iteration.
- N a priori unknown but can be avoided with additional plain/ciphertext samples.
  - Compute DRL Gröbner bases in parallel.

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis V

- Dominating complexity for iterated solving

$$\mathcal{O} \left(\sum_{i=1}^{n} N^{i-1} \cdot \mathcal{C}_{\text{char-poly}}(r - i + 1, \omega) \right)$$
$$\in \mathcal{O} \left(3 \cdot \log_2(3)^2 \cdot \Big(1 + \log_2 \big(\log_2(3) \big) \Big) \cdot \frac{3^{\omega \cdot r} - N^n}{3^{\omega} - N} \right),$$

  where N is a bound on the $\mathbb{F}_q$-valued solutions in each iteration.

- N a priori unknown but can be avoided with additional plain/ciphertext samples.
  - Compute DRL Gröbner bases in parallel.
  - Compute characteristic polynomials in parallel.

System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis V

- Dominating complexity for iterated solving

$$\mathcal{O} \left(\sum_{i=1}^{n} N^{i-1} \cdot \mathcal{C}_{\text{char-poly}}(r - i + 1, \omega) \right)$$
$$\in \mathcal{O} \left(3 \cdot \log_2(3)^2 \cdot \Big(1 + \log_2 \big(\log_2(3) \big) \Big) \cdot \frac{3^{\omega \cdot r} - N^n}{3^\omega - N} \right),$$

  where N is a bound on the $\mathbb{F}_q$-valued solutions in each iteration.

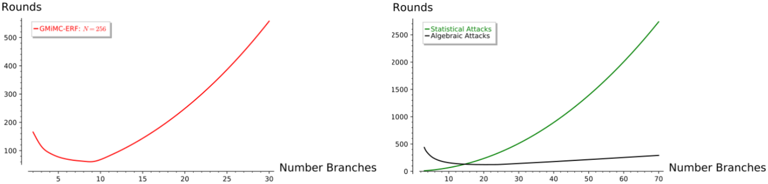
- N a priori unknown but can be avoided with additional plain/ciphertext samples.
  - Compute DRL Gröbner bases in parallel.
  - Compute characteristic polynomials in parallel.
  - Filter key guesses via GCD.

Outline

1. Motivation
2. Gröbner Bases
3. $\texttt{GMiMC}_{\text{erf}}$
4. Constructing A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis
   - Examples
5. System Solving With A $\texttt{GMiMC}_{\text{erf}}$ Gröbner Basis
6. $\texttt{GMiMC}_{\text{erf}}$ Cryptanalysis
   - What went wrong?
7. Further Outlook
8. References

GMiMC$_{\text{erf}}$ Cryptanalysis I

- GMiMC team claimed there is trade-off between algebraic and statistical cryptanalysis.



(a) $\kappa = 256$.

(b) $\kappa = 1024$.

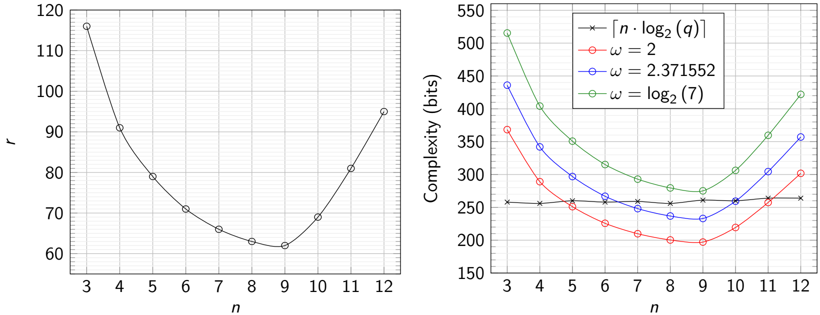
Figure: Figrues from [AGP$^+$19b, Fig. 5, 7].

$\texttt{GMiMC}_{\text{erf}}$ Cryptanalysis II

- For Gröbner basis cryptanalysis of $\texttt{GMiMC}_{\text{erf}}$:
  - Fix security level κ.
  - Increase $n \in \mathbb{Z}_{\geq 0}$ and set $\log_2(q) = \left\lceil \frac{\kappa}{n} \right\rceil$.
  - Multivariate key $\boldsymbol{k} \in \mathbb{F}_q^n$.
  - Compute round number r for (q, n, κ) for $\texttt{GMiMC}_{\text{erf}}$ with round numbers tool.[1]
  - Assume that we can construct DRL Gröbner basis via substitution.
  - Use $N = 1$ in $\mathcal{O}\left(3 \cdot \log_2(3)^2 \cdot \Big(1 + \log_2\big(\log_2(3)\big)\Big) \cdot \frac{3^{\omega \cdot r} - N^n}{3^\omega - N}\right)$.

[1] https://extgit.iaik.tugraz.at/krypto/gmimc-implementation

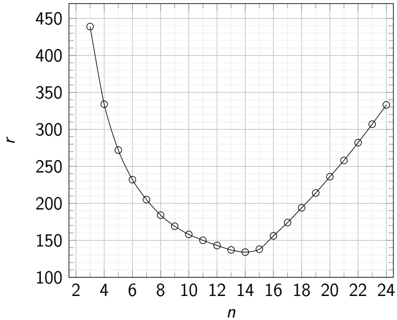
$\mathtt{GMiMC}_{\text{erf}}$, $\kappa = 256$



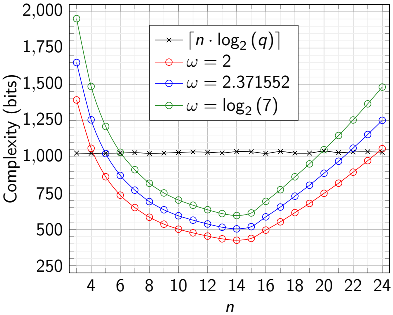
(a) Round numbers, $\kappa = 256$.

(b) Complexities, $\kappa = 256$.

$\texttt{GMiMC}_{\text{erf}}$, $\kappa = 1024$

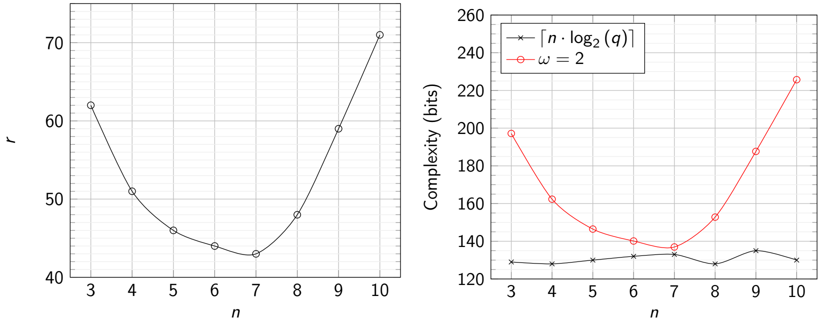


(a) Round numbers, $\kappa = 1024$.



(b) Complexities, $\kappa = 1024$.

$\texttt{GMiMC}_{\text{erf}}$, $\kappa = 128$



(a) Round numbers, $\kappa = 128$.

(b) Complexities, $\kappa = 128$.

What went wrong? I

- `GMiMC`$_{\text{erf}}$ team modeled `GMiMC`$_{\text{erf}}$ as n polynomials in n key variables of degrees $\leq 3^r$.
    - Complexity under regularity assumption: $\approx \mathcal{O}\left(\binom{n+r^{r-n}}{3^{r-n}}^{\omega}\right)$.

What went wrong? I

- $\texttt{GMiMC}_{\text{erf}}$ team modeled $\texttt{GMiMC}_{\text{erf}}$ as n polynomials in n key variables of degrees $\leq 3^r$.
    - Complexity under regularity assumption: $\approx \mathcal{O}\left(\binom{n+r^{r-n}}{3^{r-n}}^{\omega}\right)$.
- Computing $\texttt{GMiMC}_{\text{erf}}$ Gröbner basis for r cubic polynomials.
    - Complexity under regularity assumption: $\mathcal{O}\left(\binom{3 \cdot r+1}{2 \cdot r+1}^{\omega}\right)$.

What went wrong? I

- $\texttt{GMiMC}_{\mathsf{erf}}$ team modeled $\texttt{GMiMC}_{\mathsf{erf}}$ as n polynomials in n key variables of degrees $\leq 3^r$.
  - Complexity under regularity assumption: $\approx \mathcal{O}\left(\binom{n+r^{r-n}}{3^{r-n}}^{\omega}\right)$.
- Computing $\texttt{GMiMC}_{\mathsf{erf}}$ Gröbner basis for r cubic polynomials.
  - Complexity under regularity assumption: $\mathcal{O}\left(\binom{3 \cdot r+1}{2 \cdot r+1}^{\omega}\right)$.
- Solving $\texttt{GMiMC}_{\mathsf{erf}}$ system after change of variables.
  - Complexity: $\approx \mathcal{O}\left(3^{\omega \cdot r}\right)$.

UNIVERSITÄT KLAGENFURT

What went wrong? II

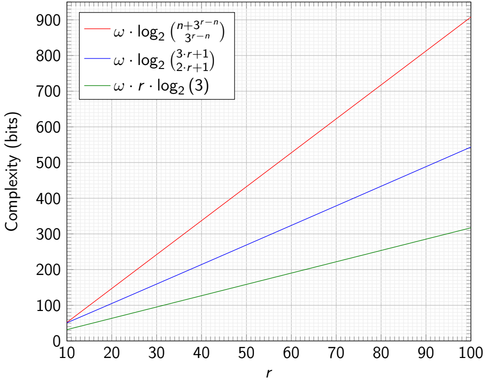


Figure: $\texttt{GMiMC}_{\text{erf}}$ complexity gap with $n = 3$ and $\omega = 2$.

Further Outlook

- "Variable elimination + change of coordinates ⇒ Gröbner basis" can be applied to other Feistel designs too.
    - Other members of `GMiMC` family (`GMiMCHash`, $\texttt{GMiMC}_{\mathsf{crf}}$).
    - Hydra [Ste24].
- Can be used at design stage to have Gröbner basis from the start.
- When is the `GMiMC` analysis going to be public?
    - In my PhD thesis: soon.
    - In a paper: later.

References I

Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger.
Feistel structures for MPC, and more.
In Kazue Sako, Steve Schneider, and Peter Y. A. Ryan, editors, *ESORICS 2019: 24th European Symposium on Research in Computer Security, Part II*, volume 11736 of *Lecture Notes in Computer Science*, pages 151–171, Luxembourg, September 23–27, 2019. Springer, Cham, Switzerland.
doi:10.1007/978-3-030-29962-0_8.

References II

Martin R. Albrecht, Lorenzo Grassi, Leo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger.
Feistel structures for MPC, and more.
Cryptology ePrint Archive, Report 2019/397, 2019.
URL: `https://eprint.iacr.org/2019/397`.

Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems.
New design techniques for efficient arithmetization-oriented hash functions: Anemoi permutations and Jive compression mode.
In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 507–539, Santa

References III

Barbara, CA, USA, August 20–24, 2023. Springer, Cham, Switzerland. doi:10.1007/978-3-031-38548-3_17.

Augustin Bariant, Aurélien Boeuf, Axel Lemoine, Irati Manterola Ayala, Morten Øygarden, Léo Perrin, and Håvard Raddum. The algebraic FreeLunch: Efficient Gröbner basis attacks against arithmetization-oriented primitives. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024, Part IV*, volume 14923 of *Lecture Notes in Computer Science*, pages 139–173, Santa Barbara, CA, USA, August 18–22, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-68385-5_5.

References IV

Bruno Buchberger.
Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.
PhD thesis, Universität Innsbruck, 1965.

David A. Cox, John Little, and Donal O'Shea.
Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.
Undergraduate Texts in Mathematics. Springer International Publishing, 4 edition, 2015.
doi:10.1007/978-3-319-16721-3.

References V

- Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch.
  Monolith: Circuit-friendly hash functions with new nonlinear layers for fast and constant-time implementations.
  IACR Transactions on Symmetric Cryptology, 2024(3):44–83, 2024.
  doi:10.46586/tosc.v2024.i3.44-83.

- Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, and Roman Walch.
  From farfalle to megafono via ciminion: The PRF hydra for MPC applications.
  In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part IV*, volume 14007 of

References VI

Lecture Notes in Computer Science, pages 255–286, Lyon, France, April 23–27, 2023. Springer, Cham, Switzerland. doi:10.1007/978-3-031-30634-1_9.

📄 Jincheol Ha, Seongkwang Kim, ByeongHak Lee, Jooyoung Lee, and Mincheol Son.
Rubato: Noisy ciphers for approximate homomorphic encryption.
In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022, Part I*, volume 13275 of *Lecture Notes in Computer Science*, pages 581–610, Trondheim, Norway, May 30 – June 3, 2022. Springer, Cham, Switzerland.
doi:10.1007/978-3-031-06944-4_20.

References VII

Martin Kreuzer and Lorenzo Robbiano.
Computational Linear and Commutative Algebra.
Springer International Publishing, Cham, 1 edition, 2016.
doi:10.1007/978-3-319-43601-2.

Matthias Johann Steiner.
Gröbner basis cryptanalysis of ciminion and hydra, 2024.
arXiv:2405.05040.

Virginia Vassilevska Williams, Yinzhan Xu, Zixuan Xu, and Renfei Zhou.
New bounds for matrix multiplication: from alpha to omega.
In David P. Woodruff, editor, *35th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 3792–3835, Alexandria, VA, USA, January 7–10, 2024. ACM-SIAM.
doi:10.1137/1.9781611977912.134.

References VIII