ALPEN-ADRIA UNIVERSITÄT KLAGENFURT

Solving Degree Bounds for Iterated Polynomial Systems

Matthias Johann Steiner

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

March 26, 2024

M. Steiner has been supported in part by the European Research Council

(ERC Grant No. 725042)

www.aau.at

Outline

Motivation

Many new MPC/ZK-friendly ciphers and hash functions:

- `MiMC` [AGR+16]
- `GMiMC` [AGP+19a]
- Hades [GLR+20]
- Poseidon [GKR+21]
- and many more...

Motivation

Many new MPC/ZK-friendly ciphers and hash functions:

- `MiMC` [AGR+16]
- `GMiMC` [AGP+19a]
- Hades [GLR+20]
- Poseidon [GKR+21]
- and many more...

- Defined over large finite fields $\mathbb{F}_q$, where $\log_2(q) \geq 64$.
- Low degree polynomials at round level.

Motivation

Many new MPC/ZK-friendly ciphers and hash functions:

- `MiMC` [AGR+16]
- `GMiMC` [AGP+19a]
- Hades [GLR+20]
- Poseidon [GKR+21]
- and many more...

- Defined over large finite fields $\mathbb{F}_q$, where $\log_2(q) \geq 64$.
- Low degree polynomials at round level.
- $\Rightarrow$ **Low degree polynomial models**.

Motivation: Gröbner Basis Attacks I

Standard Gröbner Basis Attack

1. Model the cipher function with a system of polynomials.
2. Compute a Gröbner basis with respect degree reverse lexicographic order (DRL) term order.
3. Perform a term order conversion to the lexicographic (LEX) term order.
4. Solve the univariate equation.

Motivation: Gröbner Basis Attacks II

$I \subset P = \mathbb{F}_q[x_1, \ldots, x_n]$ zero-dimensional, $d = \dim_{\mathbb{F}_q}(P/I)$

Term Order Conversion To LEX

Complexity of probabilistic FGLM [FGHR14]:

$$\mathcal{O}\left(n \cdot d^{\omega}\right),$$

where $2 \leq \omega \leq 3$.

Motivation: Gröbner Basis Attacks II

$I \subset P = \mathbb{F}_q[x_1, \ldots, x_n]$ zero-dimensional, $d = \dim_{\mathbb{F}_q}(P/I)$

Term Order Conversion To LEX

Complexity of probabilistic FGLM [FGHR14]:

$$\mathcal{O}\left(n \cdot d^{\omega}\right),$$

where $2 \leq \omega \leq 3$.

Univariate Factoring

- Compute GCD with field equation $f = x^q - x$.
- Complexity [BBLP22]:

$$\mathcal{O}\Big(d \cdot \log(d) \cdot \log\big(\log(d)\big) \cdot \big(\log(d) + \log(q)\big)\Big),$$

if $d \leq q$.

Motivation: Gröbner Basis Attacks III

$I \subset P = \mathbb{F}_q[x_1, \ldots, x_n]$ zero-dimensional

DRL Gröbner Basis Computation

- Typically assumed that I is **regular** or **semi-regular**.
- Degree of regularity d_{reg} can be read-off Hilbert series.
- Complexity [BFS04]:

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

Contributions

- Full characterization of polynomial systems in generic coordinates.
  - Efficient verification process.

Contributions

- Full characterization of polynomial systems in generic coordinates.
  - Efficient verification process.
- Proven DRL complexity estimates for attacks on:
  - `MiMC` [AGR+16]
  - `GMiMC` [AGP+19a]
  - Hades [GLR+20]

Contributions

- Full characterization of polynomial systems in generic coordinates.
  - Efficient verification process.
- Proven DRL complexity estimates for attacks on:
  - `MiMC` [AGR+16]
  - `GMiMC` [AGP+19a]
  - Hades [GLR+20]
- Limits of generic coordinates:
  - Sponge functions, e.g. Poseidon [GKR+21].
  - Non-affine key schedules.

Contributions

- Full characterization of polynomial systems in generic coordinates.
  - Efficient verification process.
- Proven DRL complexity estimates for attacks on:
  - `MiMC` [AGR+16]
  - `GMiMC` [AGP+19a]
  - Hades [GLR+20]
- Limits of generic coordinates:
  - Sponge functions, e.g. Poseidon [GKR+21].
  - Non-affine key schedules.
- Identification of degree fall polynomials for `MiMC` family.

Outline

Term Orders

$P = K[x_1, \ldots, x_n]$, $m = \prod_{i=1}^{n} x_i^{d_i}$, $\boldsymbol{d} = (d_1, \ldots, d_n)$

Term Order

1. $>$ is a total ordering on $\mathbb{Z}_{\geq 0}$.
2. If $\boldsymbol{a} > \boldsymbol{b}$ and $\boldsymbol{c} \in \mathbb{Z}_{\geq 0}^n$, then $\boldsymbol{a} + \boldsymbol{c} > \boldsymbol{b} + \boldsymbol{c}$.
3. $>$ is a well-ordering on $\mathbb{Z}_{\geq 0}^n$, i.e. every non-empty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element under $>$.

Term Orders

$P = K[x_1, \ldots, x_n]$, $m = \prod_{i=1}^{n} x_i^{d_i}$, $\boldsymbol{d} = (d_1, \ldots, d_n)$

Term Order

1. $>$ is a total ordering on $\mathbb{Z}_{\geq 0}$.
2. If $\boldsymbol{a} > \boldsymbol{b}$ and $\boldsymbol{c} \in \mathbb{Z}_{\geq 0}^n$, then $\boldsymbol{a} + \boldsymbol{c} > \boldsymbol{b} + \boldsymbol{c}$.
3. $>$ is a well-ordering on $\mathbb{Z}_{\geq 0}^n$, i.e. every non-empty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element under $>$.

Examples

1. $\boldsymbol{a} >_{LEX} \boldsymbol{b}$ if the first non-zero entry of $\boldsymbol{a} - \boldsymbol{b}$ is positive.
2. $\boldsymbol{a} >_{RLEX} \boldsymbol{b}$ if the last non-zero entry of $\boldsymbol{a} - \boldsymbol{b}$ is negative.
3. $\boldsymbol{a} >_{DRL} \boldsymbol{b}$ if $\sum_{i=1}^{n} a_i > \sum_{i=1}^{n} b_i$ or $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ and $\boldsymbol{a} >_{RLEX} \boldsymbol{b}$.

Gröbner Bases

$I = (f_1, \ldots, f_m) \subset P = K[x_1, \ldots, x_n]$ ideal,
$I = \{f \mid f = \sum_{i=1}^{m} h_i \cdot f_i,\ h_i \in P\}$

Gröbner Basis [Buc65]

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

Macaulay Matrices

$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$, $>$ term order on P

Macaulay Matrix $M_{\leq d}$

- $d \in \mathbb{Z}_{\geq 0}$:

Monomials: $s \in P,\ \deg(s) \leq d$

Polynomials:
$t \in P,\ f_i \in \mathcal{F},$
$\deg(t \cdot f_i) \leq d$

Solving Degree

$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$, $>$ term order on P

Solving Degree [CG21, Definition 6]

$\mathrm{sd}_>(\mathcal{F})$ least $d \in \mathbb{Z}_{\geq 0}$ such that Gaussian elimination on $M_{\leq d}$ produces $>$-Gröbner basis.

Solving Degree

$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$, $>$ term order on P

Solving Degree [CG21, Definition 6]

$\mathrm{sd}_>(\mathcal{F})$ least $d \in \mathbb{Z}_{\geq 0}$ such that Gaussian elimination on $M_{\leq d}$ produces $>$-Gröbner basis.

Have the complexity estimate [Sto00]

$$\mathcal{O}\left(m \cdot \mathrm{sd}_>(\mathcal{F}) \cdot \binom{n + \mathrm{sd}_>(\mathcal{F}) - 1}{\mathrm{sd}_>(\mathcal{F})}^{\omega}\right),$$

where $2 \leq \omega \leq 3$.

Outline

Generic Coordinates I

$$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$$

Highest Degree Component

- $f \in P$: $f = f_d + f_{d-1} + \ldots + f_0$, where f_i homogeneous of degree i.
- $f^{\text{top}} = f_d = f^{\text{hom}} \mod (x_0)$.

Generic Coordinates I

$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$

Highest Degree Component

- $f \in P$: $f = f_d + f_{d-1} + \ldots + f_0$, where f_i homogeneous of degree i.
- $f^{\text{top}} = f_d = f^{\text{hom}} \mod (x_0)$.

Theorem (Characterization of Generic Coordinates)

Equivalent are:

1. $\left(\mathcal{F}^{\text{hom}}\right)$ *is in generic coordinates.*
2. $\sqrt{\mathcal{F}^{\text{top}}} = (x_1, \ldots, x_n)$.
3. $(\mathcal{F}^{\text{top}})$ *is zero-dimensional in* $K[x_1, \ldots, x_n]$.
4. *For all* $1 \leq i \leq n$, $\exists d_i \in \mathbb{Z}_{\geq 1}$: $x_i^{d_i} \in \text{LM}_{DRL}\left(\mathcal{F}^{\text{hom}}\right)$.

Generic Coordinates II

$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$

Theorem ([CG21, Theorem 9, 10, Corollary 2])

- $\left(\mathcal{F}^{\text{hom}}\right)$ *in generic coordinates.*
- $\deg(f_1) \geq \ldots \geq \deg(f_m)$.
- $l \in \min\{n+1, m\}$.
- ***Then:***

$$\text{sd}_{DRL}(\mathcal{F}) \leq \sum_{i=1}^{l} (\deg(f_i) - 1) + 1.$$

Verifying Generic Coordinates

2. $\sqrt{\mathcal{F}^{\mathsf{top}}} = (x_1, \ldots, x_n)$.

Verifying Generic Coordinates

2. $\sqrt{\mathcal{F}^{\mathrm{top}}} = (x_1, \ldots, x_n)$.

Radical Ideal

- $I \subset P$ ideal.
- $\sqrt{I} = \{f \in P \mid \exists n \geq 1 \colon f^n \in I\}$.

Verifying Generic Coordinates

2. $\sqrt{\mathcal{F}^{\text{top}}} = (x_1, \ldots, x_n)$.

Radical Ideal

- $I \subset P$ ideal.
- $\sqrt{I} = \{f \in P \mid \exists n \geq 1 \colon f^n \in I\}$.

Verification Process

1. $\mathcal{F}^{\text{top}} = \mathcal{F}^{\text{hom}} \mod (x_0)$, $\sqrt{\mathcal{F}^{\text{top}}} = (0)$.
2. For x_i: find $f \in (\mathcal{F}^{\text{top}})$ such that $f = x_i^d$.
3. Set $\mathcal{F}^{\text{top}} = \mathcal{F}^{\text{top}} \mod (x_i)$, $\sqrt{\mathcal{F}^{\text{top}}} = \sqrt{\mathcal{F}^{\text{top}}} + (x_i)$, return to 2.
4. If $\sqrt{\mathcal{F}^{\text{top}}} = (x_1, \ldots, x_n)$, then $\left(\mathcal{F}^{\text{hom}}\right)$ in generic coordinates.

Outline

Applications: MiMC

MiMC [AGR+16]

- Univariate cipher for MPC.
- Defined over finite fields $\mathbb{F}_p$ such that $\gcd(3, p-1) = 1$.
- Let $k \in \mathbb{F}_p$ denote a secret key, and let $c_1, \ldots, c_r \in \mathbb{F}_p$ be constants.

$$\mathcal{R}_{i,k}(x) = \begin{cases} (x + k + c_i)^3, & 1 \leq i \leq r-1, \\ (x + k + c_r)^3 + k, & i = r. \end{cases}$$

- MiMC cipher:

$$\mathcal{C}_{\mathtt{MiMC}}(x, k) = \mathcal{R}_{r,k} \circ \cdots \circ \mathcal{R}_{1,k}(x).$$

MiMC Polynomial Model

- Given a plain/ciphertext $p, c \in \mathbb{F}_p$ MiMC sample:

$$\mathcal{F}_{\texttt{MiMC}}: \begin{cases} (p + y + c_1)^3 - x_1 = 0, \\ (x_{i-1} + y + c_i)^3 - x_i = 0, \quad 2 \leq i \leq r-1, \\ (x_{r-1} + y + c_r)^3 + y - c = 0. \end{cases}$$

MiMC Polynomial Model

- Given a plain/ciphertext $p, c \in \mathbb{F}_p$ MiMC sample:

$$\mathcal{F}_{\texttt{MiMC}}: \begin{cases} (p + y + c_1)^3 - x_1 = 0, \\ (x_{i-1} + y + c_i)^3 - x_i = 0, \quad 2 \leq i \leq r-1, \\ (x_{r-1} + y + c_r)^3 + y - c = 0. \end{cases}$$

Theorem

Equivalent are:

1. $\left(\mathcal{F}^{\mathsf{hom}}\right)$ *is in generic coordinates.*
2. $\sqrt{\mathcal{F}^{\mathsf{top}}} = (x_1, \ldots, x_n)$.

MiMC Polynomial Model

- Given a plain/ciphertext $p, c \in \mathbb{F}_p$ MiMC sample:

$$\mathcal{F}_{\texttt{MiMC}}: \begin{cases} (p + y + c_1)^3 - x_1 = 0, \\ (x_{i-1} + y + c_i)^3 - x_i = 0, \quad 2 \leq i \leq r-1, \\ (x_{r-1} + y + c_r)^3 + y - c = 0. \end{cases}$$

Theorem

Equivalent are:

1. $\left(\mathcal{F}^{\text{hom}}\right)$ *is in generic coordinates.*
2. $\sqrt{\mathcal{F}^{\text{top}}} = (x_1, \ldots, x_n)$.

- MiMC highest degree components:

$$\mathcal{F}^{\text{top}}_{\texttt{MiMC}}: \begin{cases} y^3 = 0, \\ (x_{i-1} + y)^3 = 0, \quad 2 \leq i \leq r. \end{cases}$$

Gröbner Basis Attack on MiMC I

- $\mathcal{F}_{\texttt{MiMC}}$ already a DRL Gröbner basis under $x_{r-1} > \ldots > x_1 > y$.
  - $\dim_{\mathbb{F}_p}(\mathcal{F}_{\texttt{MiMC}}) = 3^r$.

Gröbner Basis Attack on MiMC I

- $\mathcal{F}_{\texttt{MiMC}}$ already a DRL Gröbner basis under $x_{r-1} > \ldots > x_1 > y$.
  - $\dim_{\mathbb{F}_p}(\mathcal{F}_{\texttt{MiMC}}) = 3^r$.
- Two possible attack strategies:
  - Term order conversion to LEX and GCD with field equation $y^p - y$:

$$\mathcal{O}\left(3^{\omega \cdot r} + \text{GCD complexity}\right).$$

Gröbner Basis Attack on MiMC I

- $\mathcal{F}_{\texttt{MiMC}}$ already a DRL Gröbner basis under $x_{r-1} > \ldots > x_1 > y$.
  - $\dim_{\mathbb{F}_p}(\mathcal{F}_{\texttt{MiMC}}) = 3^r$.
- Two possible attack strategies:
  - Term order conversion to LEX and GCD with field equation $y^p - y$:

$$\mathcal{O}\left(3^{\omega \cdot r} + \text{GCD complexity}\right).$$

  - Recompute DRL Gröbner basis $(\mathcal{F}_{\texttt{MiMC}}) + (y^p - y)$:

$$\mathcal{O}\left(\binom{3 \cdot r + \deg(r_y)}{2 \cdot r + \deg(r_y)}^{\omega}\right).$$

Gröbner Basis Attack on MiMC II

- MiMC requires that $r \geq \log_3(p)$.
- Assume that $\deg(r_y) \leq 2 \cdot \lceil \log_3(p) \rceil$.

Table: MiMC complexity estimates with $\omega = 2$.

$\log_2(p)$	r	DRL Complexity (bits)	Term Order Conversion (bits)
64	50	338	165
128	81	527	264
256	162	1157	521

Gröbner Basis Attack on MiMC II

- MiMC requires that $r \geq \log_3(p)$.
- Assume that $\deg(r_y) \leq 2 \cdot \lceil \log_3(p) \rceil$.

Table: MiMC complexity estimates with $\omega = 2$.

$\log_2(p)$	r	DRL Complexity (bits)	Term Order Conversion (bits)
64	50	338	165
128	81	527	264
256	162	1157	521

- Analog you can obtain proven complexity estimates:
  - MiMC two plain/ciphertext attack.
  - Feistel-MiMC: $\begin{pmatrix} x_L \\ x_R \end{pmatrix}, k \mapsto \begin{pmatrix} x_R + (x_L + k + c_i)^3 \\ x_L \end{pmatrix}$.
  - Feistel-MiMC-Hash.

Applications: Hades

Hades [GLR+20]

- SPN cipher for MPC.

Applications: Hades

Hades [GLR+20]

- SPN cipher for MPC.
- Defined over prime fields $\mathbb{F}_p$ with $d \in \mathbb{Z}_{>1}$ such that $\gcd(d, p-1) = 1$.

Applications: Hades

Hades [GLR+20]

- SPN cipher for MPC.
- Defined over prime fields $\mathbb{F}_p$ with $d \in \mathbb{Z}_{>1}$ such that $\gcd(d, p-1) = 1$.
- Full SPN rounds: $\mathcal{S} : (\boldsymbol{x}, \boldsymbol{k}) \mapsto \boldsymbol{M} \begin{pmatrix} x_1^d \\ \vdots \\ x_n^d \end{pmatrix} + \boldsymbol{k} + \boldsymbol{c}_i$.

Applications: Hades

Hades [GLR+20]

- SPN cipher for MPC.
- Defined over prime fields $\mathbb{F}_p$ with $d \in \mathbb{Z}_{>1}$ such that $\gcd(d, p-1) = 1$.
- Full SPN rounds: $\mathcal{S} : (\boldsymbol{x}, \boldsymbol{k}) \mapsto \boldsymbol{M} \begin{pmatrix} x_1^d \\ \vdots \\ x_n^d \end{pmatrix} + \boldsymbol{k} + \boldsymbol{c}_i$.
- Partial SPN rounds: $\mathcal{P} : (\boldsymbol{x}, \boldsymbol{k}) \mapsto \boldsymbol{M} \begin{pmatrix} x_1^d \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \boldsymbol{k} + \boldsymbol{c}_i$.

Applications: Hades

Hades [GLR+20]

- SPN cipher for MPC.
- Defined over prime fields $\mathbb{F}_p$ with $d \in \mathbb{Z}_{>1}$ such that $\gcd(d, p-1) = 1$.
- Full SPN rounds.
- Partial SPN rounds.

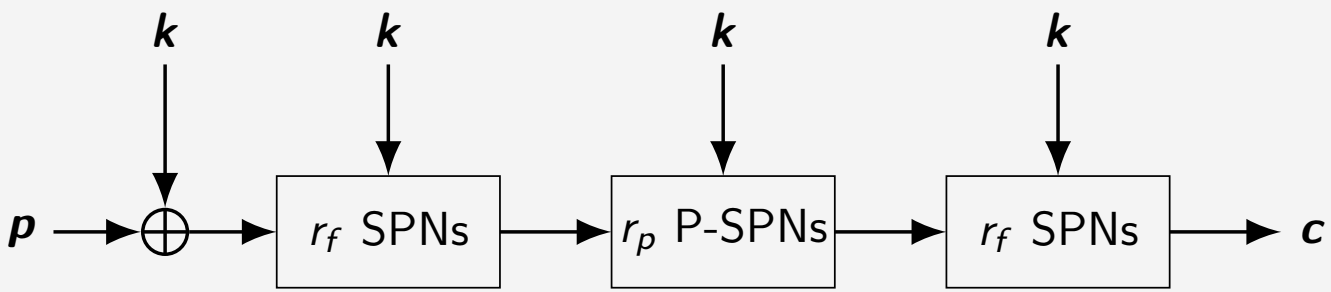

Figure: Hades strategy.

Hades Polynomial model

Given a plain/ciphertext $\boldsymbol{p}, \boldsymbol{c} \in \mathbb{F}_p^n$ Hades sample:

- Can set up iterated Hades polynomial system:

$$\mathcal{F}_{\text{Hades}}: \begin{cases} \boldsymbol{M}\mathcal{S}\left(\boldsymbol{p}+\boldsymbol{y}\right)+\boldsymbol{y}+\boldsymbol{c}_1-\boldsymbol{x}^{(1)}=0, \\ \boldsymbol{M}\mathcal{S}\left(\boldsymbol{x}^{(i-1)}\right)+\boldsymbol{y}+\boldsymbol{c}_i-\boldsymbol{x}^{(i)}=0, \\ \boldsymbol{M}\mathcal{P}\left(\boldsymbol{x}^{(i-1)}\right)+\boldsymbol{y}+\boldsymbol{c}_i-\boldsymbol{x}^{(i)}=0, \\ \boldsymbol{M}\mathcal{S}\left(\boldsymbol{x}^{(2\cdot r_f+r_p-1)}\right)+\boldsymbol{y}+\boldsymbol{c}_{2\cdot r_f+r_p}-\boldsymbol{c}=0. \end{cases}$$

Hades Polynomial model

Given a plain/ciphertext $\boldsymbol{p}, \boldsymbol{c} \in \mathbb{F}_p^n$ Hades sample:

- Can set up iterated Hades polynomial system:

$$\mathcal{F}_{\text{Hades}}: \begin{cases} \boldsymbol{M}\mathcal{S}\left(\boldsymbol{p}+\boldsymbol{y}\right)+\boldsymbol{y}+\boldsymbol{c}_1-\boldsymbol{x}^{(1)}=0, \\ \boldsymbol{M}\mathcal{S}\left(\boldsymbol{x}^{(i-1)}\right)+\boldsymbol{y}+\boldsymbol{c}_i-\boldsymbol{x}^{(i)}=0, \\ \boldsymbol{M}\mathcal{P}\left(\boldsymbol{x}^{(i-1)}\right)+\boldsymbol{y}+\boldsymbol{c}_i-\boldsymbol{x}^{(i)}=0, \\ \boldsymbol{M}\mathcal{S}\left(\boldsymbol{x}^{(2\cdot r_f+r_p-1)}\right)+\boldsymbol{y}+\boldsymbol{c}_{2\cdot r_f+r_p}-\boldsymbol{c}=0. \end{cases}$$

- $\boldsymbol{M}^{-1}\mathcal{F}_{\text{Hades}}$ zero-dimensional DRL Gröbner basis for $\boldsymbol{x}^{(1)} > \ldots > \boldsymbol{x}^{(2\cdot r_f+r_p-1)} > \boldsymbol{y}$.

Hades Polynomial model

Given a plain/ciphertext $\boldsymbol{p}, \boldsymbol{c} \in \mathbb{F}_p^n$ Hades sample:

- Can set up $\mathcal{F}_{\text{Hades}}$.
- $\boldsymbol{M}^{-1}\mathcal{F}_{\text{Hades}}$ zero-dimensional DRL Gröbner basis for $\boldsymbol{x}^{(1)} > \ldots > \boldsymbol{x}^{(2\cdot r_f + r_p - 1)} > \boldsymbol{y}$.

Corollary

$\mathcal{F}$ zero-dimensional DRL Gröbner basis $\Rightarrow \left(\mathcal{F}^{\text{hom}}\right)$ in generic coordinates.

Hades Polynomial model

Given a plain/ciphertext $\boldsymbol{p}, \boldsymbol{c} \in \mathbb{F}_p^n$ Hades sample:

- Can set up $\mathcal{F}_{\text{Hades}}$.
- $\boldsymbol{M}^{-1}\mathcal{F}_{\text{Hades}}$ zero-dimensional DRL Gröbner basis for $\boldsymbol{x}^{(1)} > \ldots > \boldsymbol{x}^{(2\cdot r_f + r_p - 1)} > \boldsymbol{y}$.

Corollary

$\mathcal{F}$ zero-dimensional DRL Gröbner basis $\Rightarrow \left(\mathcal{F}^{\text{hom}}\right)$ in generic coordinates.

- Generalizes to any affine key schedule.
- Have baseline solving degree:

$$\text{sd}_{DRL}\left(\boldsymbol{M}^{-1}\mathcal{F}_{\text{Hades}}\right) \leq (d-1)\cdot(2\cdot n\cdot r_f + r_p) + 1.$$

Gröbner Basis Attack on Hades

- Complexity estimate after variable elimination in partial rounds:

$$\mathcal{O}\left(\binom{d \cdot (2 \cdot n \cdot r_f + r_p)}{(d-1) \cdot (2 \cdot n \cdot r_f + r_p) + 1}^{\omega}\right).$$

- Same complexity as in Hades proposal [GLR+19, §E.3] under regularity assumption.

Gröbner Basis Attack on Hades

- Complexity estimate after variable elimination in partial rounds:

$$\mathcal{O}\left(\binom{d \cdot (2 \cdot n \cdot r_f + r_p)}{(d-1) \cdot (2 \cdot n \cdot r_f + r_p) + 1}^{\omega}\right).$$

- Same complexity as in Hades proposal [GLR+19, §E.3] under regularity assumption.

Table: Hades complexity estimation with $n = 2$ and $\omega = 2$ over a finite field $\mathbb{F}_q$ such that $\gcd(d, q-1) = 1$.

	$d = 3$		$d = 5$	
r_f	3	4	3	4
r_p	10	10	10	10
κ (bits)	142.4	164.6	191.6	220.8

Applications: $\texttt{GMiMC}_{\text{erf}}$

$\texttt{GMiMC}_{\text{erf}}$ [AGP+19a]

- Feistel cipher with expanding round function (erf) for MPC.
- Defined over prime fields $\mathbb{F}_p$.
- Uses cubing in Feistel, i.e. $f(x) = x^3$.
- Round function:

$$(\boldsymbol{x}, \boldsymbol{k}) \mapsto \begin{pmatrix} x_n \\ x_1 + x_n^3 \\ \vdots \\ x_{n-1} + x_n^3 \end{pmatrix} + \boldsymbol{k} + \boldsymbol{c}.$$

Gröbner Basis Attack on $\texttt{GMiMC}_{\text{erf}}$ I

- Generic coordinates verification for $\texttt{GMiMC}_{\text{erf}}$ via rank of linear system.
  - Solving degree:

$$\text{sd}_{DRL}\left(\mathcal{F}_{\texttt{GMiMC}_{\text{erf}}}\right) \leq r \cdot (d-1) + 1.$$

  - Complexity estimate:

$$\mathcal{O}\left(\binom{r \cdot d}{r \cdot (d-1) + 1}^{\omega}\right).$$

Gröbner Basis Attack on $\texttt{GMiMC}_{\text{erf}}$ I

- Generic coordinates verification for $\texttt{GMiMC}_{\text{erf}}$ via rank of linear system.
  - Solving degree:

$$\mathrm{sd}_{DRL}\left(\mathcal{F}_{\texttt{GMiMC}_{\text{erf}}}\right) \leq r \cdot (d-1) + 1.$$

  - Complexity estimate:

$$\mathcal{O}\left(\binom{r \cdot d}{r \cdot (d-1)+1}^{\omega}\right).$$

- In GMiMC proposal [AGP+19a] only polynomial model in n key variables was analyzed.
  - Complexity estimate [AGP+19b, §C.3]:

$$\mathcal{O}\left(\binom{n+3^{r-n}}{3^{r-n}}^{\omega}\right).$$

Gröbner Basis Attack on $\texttt{GMiMC}_{\text{erf}}$ II

Table: $\texttt{GMiMC}_{\text{erf}}$ complexity estimation with $n = 3$ and $\omega = 2$ over a finite field $\mathbb{F}_q$.

	Iterated Model		Full Model	
r	10	25	10	25
κ (bits)	49	130	62	204

- Other Feistel types can be analyzed analog.

Summary & Open Problems

Summary

- Full characterization of generic coordinates.
  - Efficient criterion.
- Proven DRL complexity estimates for `MiMC` and Hades.
- Efficient criteria for `GMiMC` family to be in generic coordinates.
  - Better complexity estimate than in `GMiMC` cryptanalysis.

Summary & Open Problems

Summary

- Full characterization of generic coordinates.
  - Efficient criterion.
- Proven DRL complexity estimates for `MiMC` and Hades.
- Efficient criteria for `GMiMC` family to be in generic coordinates.
  - Better complexity estimate than in `GMiMC` cryptanalysis.

Open Problems

- Cover more designs.
- Generic coordinates criterion fails for:
  - Sponge functions (Poseidon [GKR+21]).
    - Poseidon Gröbner basis via weight order [Ste24].
  - Non-affine key schedules.
- Improve upon Macaulay bound for overdefined systems.

The Problem with Sponge Functions

- Sponge construction [BDPV07, BDPV08]:

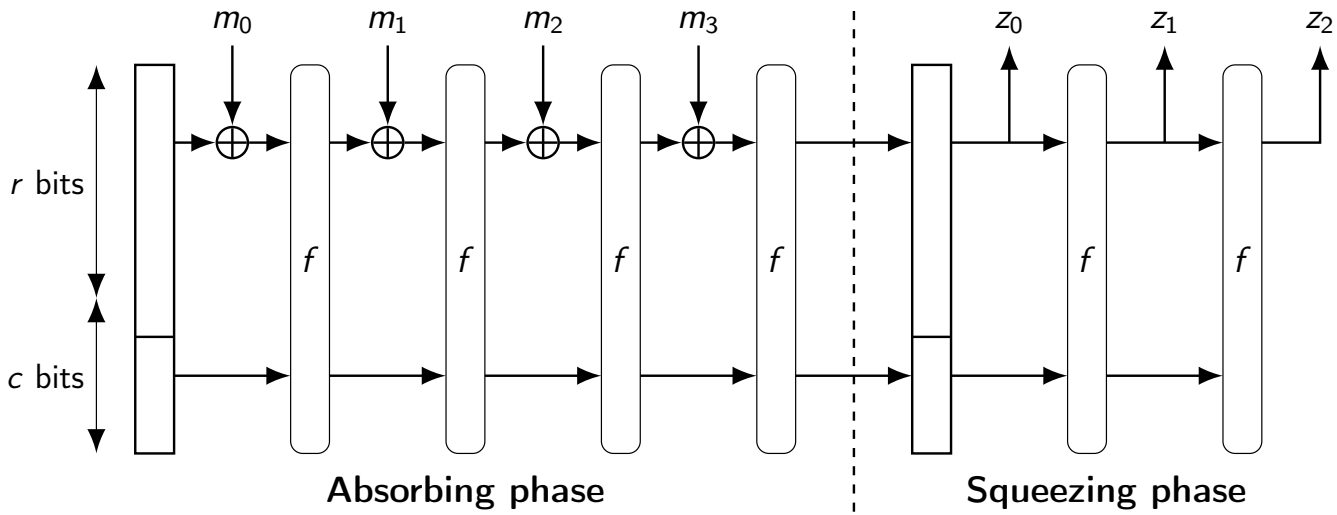

Figure: Sponge illustration by [Jea16].

The Problem with Sponge Functions

- Preimage problem for sponge function:

$$\mathcal{P}\begin{pmatrix} \boldsymbol{x}_{in} \\ \mathtt{IV} \end{pmatrix} = \begin{pmatrix} \mathtt{hash} \\ \boldsymbol{x}_{out} \end{pmatrix}.$$

The Problem with Sponge Functions

- Preimage problem for sponge function:

$$\mathcal{P}\begin{pmatrix} \boldsymbol{x}_{in} \\ \mathtt{IV} \end{pmatrix} = \begin{pmatrix} \mathtt{hash} \\ \boldsymbol{x}_{out} \end{pmatrix}.$$

- Poseidon [GKR+21] (Hades permutation in sponge mode).

The Problem with Sponge Functions

- Preimage problem for sponge function:

$$\mathcal{P}\begin{pmatrix} \boldsymbol{x}_{in} \\ \mathtt{IV} \end{pmatrix} = \begin{pmatrix} \mathtt{hash} \\ \boldsymbol{x}_{out} \end{pmatrix}.$$

- Poseidon [GKR+21] (Hades permutation in sponge mode).
  - Consider last round in iterated polynomial model:

$$\boldsymbol{f}^{(r)} = \boldsymbol{M}\mathcal{S}_d\left(\boldsymbol{x}^{(r-1)}\right) + \boldsymbol{c}_r - \begin{pmatrix} \mathtt{hash} \\ \boldsymbol{x}_{out} \end{pmatrix}.$$

The Problem with Sponge Functions

- Preimage problem for sponge function:

$$\mathcal{P}\begin{pmatrix} \boldsymbol{x}_{in} \\ \mathtt{IV} \end{pmatrix} = \begin{pmatrix} \mathtt{hash} \\ \boldsymbol{x}_{out} \end{pmatrix}.$$

- Poseidon [GKR+21] (Hades permutation in sponge mode).
  - Consider last round in iterated polynomial model:

$$\boldsymbol{f}^{(r)} = \boldsymbol{M}\mathcal{S}_d\left(\boldsymbol{x}^{(r-1)}\right) + \boldsymbol{c}_r - \begin{pmatrix} \mathtt{hash} \\ \boldsymbol{x}_{out} \end{pmatrix}.$$

  - Then ${\boldsymbol{f}^{(r)}}^{\mathsf{top}} = \boldsymbol{M}\mathcal{S}_d\left(\boldsymbol{x}^{(r-1)}\right)$.
  - $\boldsymbol{x}_{out}$ not present in $\left(\mathcal{F}^{\mathsf{top}}_{\mathsf{Poseidon}}\right) \Rightarrow$ **Cannot be in generic coordinates.**

Generic Coordinates for Feistel ERF

- Iterated polynomial systems for Feistel with expanding round function (erf):

$$\boldsymbol{f}^{(i)} = \boldsymbol{M} \begin{pmatrix} x_1^{(i-1)} + h\left(x_n^{(i-1)}\right) \\ \vdots \\ x_{n-1}^{(i-1)} + h\left(x_n^{(i-1)}\right) \\ x_n^{(i-1)} \end{pmatrix} + \boldsymbol{c}_i + \boldsymbol{y} - \boldsymbol{x}^{(i)} = 0.$$

Generic Coordinates for Feistel ERF

- Iterated polynomial systems for Feistel with expanding round function (erf):

$$\boldsymbol{f}^{(i)} = \boldsymbol{M} \begin{pmatrix} x_1^{(i-1)} + h\left(x_n^{(i-1)}\right) \\ \vdots \\ x_{n-1}^{(i-1)} + h\left(x_n^{(i-1)}\right) \\ x_n^{(i-1)} \end{pmatrix} + \boldsymbol{c}_i + \boldsymbol{y} - \boldsymbol{x}^{(i)} = 0.$$

- Transform to:

$$\boldsymbol{g}^{(i)} = \begin{cases} \left(\boldsymbol{M}^{-1}\boldsymbol{f}^{(i)}\right)_j, & j = 1, n, \\ \left(\boldsymbol{M}^{-1}\boldsymbol{f}^{(i)}\right)_j - \left(\boldsymbol{M}^{-1}\boldsymbol{f}^{(i)}\right)_1, & 2 \le j \le n-1. \end{cases}$$

Polynomials with Degree Falls

$\mathcal{F} \subset P = K[x_1, \ldots, x_n]$

Degree Fall

- $d \in \mathbb{Z}$, $f \in (\mathcal{F})$.
- $\deg(f) < d$.
- $f \in \text{rowsp}(M_{\leq d})$.
- $f \notin \text{rowsp}(M_{\leq d-1})$.

- Leads to notion of last fall degree.
  - Last fall degree always finite for systems in generic coordinates.

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, Part II*, volume 11736 of *LNCS*, pages 151–171. Springer, Heidelberg, September 2019.
doi:10.1007/978-3-030-29962-0_8.

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.
https://eprint.iacr.org/2019/397.

References II

Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen.
MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity.
In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 191–219. Springer, Heidelberg, December 2016.
doi:10.1007/978-3-662-53887-6_7.

Augustin Bariant, Clémence Bouvier, Gaëtan Leurent, and Léo Perrin.
Algebraic attacks against some arithmetization-oriented primitives.
IACR Trans. Symm. Cryptol., 2022(3):73–101, 2022.
doi:10.46586/tosc.v2022.i3.73-101.

References III

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
Sponge functions.
Ecrypt Hash Workshop, 2007.
URL: https://keccak.team/files/SpongeFunctions.pdf.

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
On the indifferentiability of the sponge construction.
In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 181–197. Springer, Heidelberg, April 2008.
doi:10.1007/978-3-540-78967-3_11.

References IV

Magali Bardet, Jean-Charles Faugère, and Bruno Salvy.
On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations.
In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

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

References V

Alessio Caminata and Elisa Gorla.
Solving multivariate polynomial systems and an invariant from commutative algebra.
In Jean Claude Bajard and Alev Topuzoğlu, editors, *Arithmetic of Finite Fields*, pages 3–36, Cham, 2021. Springer International Publishing.
doi:10.1007/978-3-030-68869-1_1.

Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, and Guénaël Renault.
Sub-cubic change of ordering for Gröbner basis: A probabilistic approach.
In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, page

References VI

170–177, New York, NY, USA, 2014. Association for Computing Machinery.
doi:10.1145/2608628.2608669.

Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger.
Poseidon: A new hash function for zero-knowledge proof systems.
In Michael Bailey and Rachel Greenstadt, editors, *USENIX Security 2021*, pages 519–535. USENIX Association, August 2021.

References VII

Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger.
On a generalization of substitution-permutation networks: The HADES design strategy.
Cryptology ePrint Archive, Report 2019/1107, 2019.
https://eprint.iacr.org/2019/1107.

Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger.
On a generalization of substitution-permutation networks: The HADES design strategy.
In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 674–704. Springer, Heidelberg, May 2020.
doi:10.1007/978-3-030-45724-2_23.

References VIII


Jérémy Jean.
TikZ for Cryptographers.
https://www.iacr.org/authors/tikz/, 2016.


Matthias Johann Steiner.
A zero-dimensional gröbner basis for poseidon.
Cryptology ePrint Archive, Paper 2024/310, 2024.
URL: https://eprint.iacr.org/2024/310.


Arne Storjohann.
Algorithms for matrix canonical forms.
Doctoral thesis, ETH Zurich, Zürich, 2000.
Diss., Technische Wissenschaften ETH Zürich, Nr. 13922, 2001.
doi:10.3929/ethz-a-004141007.