On the Field-Based Division Property:

Applications to MiMC, Feistel MiMC and GMiMC

Jiamin Cui[1], Kai Hu[2], Meiqin Wang[1], Puwen Wei[1]

1. Shandong University, China
2. Nanyang Technological University, Singapore

ASIACRYPT 2022

Contents

1 Background

2 Field-Based Division Property

3 Detect the Upper Bound of the Algebraic Degree

4 Application

Symmetric-Key Primitives with New Cost Metrics

Algebraically simple symmetric-key primitives over large finite fields are efficient in MPC/FHE/ZK protocols.

- Optimized for a specific cost metric like low number of multiplications, low multiplicative depth, ...
- Described over $\mathbb{F}_{2^n}$ or $\mathbb{F}_p$ for large n and p.
- Non-linear layer with a simple algebraic description (e.g., power maps $x \mapsto x^d$ or $x \mapsto x^{-1}$).

Examples : MiMC&Feistel MiMC [Alb+16], GMiMC [Alb+19a], HadesMiMC [Gra+20], Vision&Rescue [Aly+20], Ciminion [Dob+21] ...

Motivation

Algebraic cryptanalysis most often determines the overall security of these novel symmetric-key designs with simple algebraic representation.

- Gröbner-basis attack on Jarvis and Friday [Alb+19b]
- Higher-order attack on full-round MiMC [Eic+20]
- Higher-order attack on full-round GMiMC [Bey+20]

A natural question

How to study the algebraic representation of the cipher?

Our Results

1. Propose general monomial prediction, a way of studying the polynomial representation for ciphers over $\mathbb{F}_{2^n}$.
2. Give a new framework of degree evaluation with general monomial prediction.
3. Analyze the security of MiMC, Feistel MiMC and GMiMC and present more accurate number of rounds necessary to guarantee the security level.

Polynomial Representation

Definition (Polynomial Representation)

Any function $F\colon \mathbb{F}_{2^n}^t \to \mathbb{F}_{2^n}$ can be uniquely expressed by a polynomial over $\mathbb{F}_{2^n}$, as

$$F(x_0, \cdots, x_{t-1}) = \sum_{\boldsymbol{u}=(u_0,\cdots,u_{t-1})\in\{0,1,\cdots,2^n-1\}^t} \varphi(\boldsymbol{u}) \cdot \pi_{\boldsymbol{u}}(\boldsymbol{x}), \varphi(\boldsymbol{u}) \in \mathbb{F}_{2^n}.$$

- $\pi_{\boldsymbol{u}}(\boldsymbol{x}) = x_0^{u_0} x_1^{u_1} \cdots x_{t-1}^{u_{t-1}}$
- If $\varphi(\boldsymbol{u}) \neq 0$, monomial $\pi_{\boldsymbol{u}}(\boldsymbol{x})$ is contained by F ($\pi_{\boldsymbol{u}}(\boldsymbol{x}) \to F$). Else, $\pi_{\boldsymbol{u}}(\boldsymbol{x}) \nrightarrow F$.
- **Example:** $F(x_0, x_1) = x_0^{13} x_1 + 2x_0^7 x_1^{10} + 1$

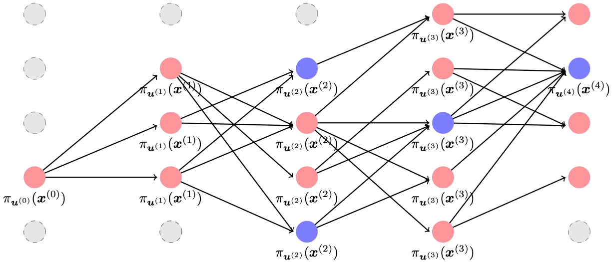
$$\rightsquigarrow x_0^7 x_1^{10} \to F,\ x_0^{11} x_1 \nrightarrow F$$

- **Question:** How to judge if $\boldsymbol{x}^{\boldsymbol{u}} \to \boldsymbol{y}^{\boldsymbol{v}}$ or not ?

General Monomial Prediction

Definition (General Monomial Trail)

Let $\boldsymbol{F}^{(i)}$ be a sequence of polynomials over $\mathbb{F}_{2^n}$, $\boldsymbol{x}^{(i+1)} = \boldsymbol{F}^{(i)}(\boldsymbol{x}^{(i)})$, $0 \leq i < r$. The transition $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \to \pi_{\boldsymbol{u}^{(1)}}(\boldsymbol{x}^{(1)}) \to \cdots \to \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$
is called an r-round general monomial trail, denoted by $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \rightsquigarrow \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$.



Example

Let $x_0, x_1, y, z \in \mathbb{F}_{2^3}$ with the irreducible polynomial $f(x) = x^3 + x + 1$. $z = 2y^3$, $y = x_0^3 \oplus 2x_0 \oplus x_1^2$. Considering the monomial x_0^5, we can calculate

$$\begin{aligned}
y^3 &\equiv 2x_0^7 \oplus x_0^6x_1^2 \oplus 4x_0^5 \oplus x_0^3x_1^4 \oplus 3x_0^3 \oplus 4x_0^2x_1^2 \oplus x_0^2 \oplus 2x_0x_1^4 \oplus x_1^6,\\
y^4 &\equiv x_0^5 \oplus 6x_0^4 \oplus x_1,\\
y^5 &\equiv 6x_0^7 \oplus 2x_0^6 \oplus x_0^5x_1^2 \oplus 7x_0^5 \oplus 6x_0^4x_1^2 \oplus x_0^3x_1 \oplus 2x_0x_1 \oplus x_0 \oplus x_1^3,\\
y^7 &\equiv 6x_0^7x_1^4 \oplus 4x_0^7x_1^2 \oplus 2x_0^7x_1 \oplus 2x_0^6x_1^4 \oplus x_0^6x_1^3 \oplus 6x_0^6x_1^2 \oplus 6x_0^6 \oplus x_0^5x_1^6 \oplus 7x_0^5x_1^4,\\
&\quad \oplus 4x_0^5x_1 \oplus 2x_0^5 \oplus 6x_0^4x_1^6 \oplus x_0^4x_1^2 \oplus 7x_0^4 \oplus x_0^3x_1^5 \oplus 6x_0^3x_1^2 \oplus 3x_0^3x_1 \oplus 4x_0^3\\
&\quad \oplus 4x_0^2x_1^3 \oplus x_0^2x_1 \oplus 6x_0^2 \oplus 2x_0x_1^5 \oplus x_0x_1^4 \oplus 3x_0 \oplus x_1^7.
\end{aligned}$$

Example

Similarly, we can compute the monomial of z as

$$z^1 \equiv \underline{2y^3}, z^4 \equiv 6y^{12} \equiv \underline{6y^5}, z^6 \equiv 5y^{18} \equiv \underline{5y^4}, z^7 \equiv y^{21} \equiv \underline{y^7}.$$

There are four monomial trails connecting x_0^5 and monomials of z :

$$x_0^5 \to y^3 \to z^1, \quad x_0^5 \to y^4 \to z^6, \quad x_0^5 \to y^5 \to z^4, \quad x_0^5 \to y^7 \to z^7.$$

Propagation Rules for Field-Based Operations

- Propagation rules : $\boldsymbol{u} \xrightarrow{f} \boldsymbol{v}$ if and only if $\boldsymbol{x}^{\boldsymbol{u}} \rightarrow \boldsymbol{y}^{\boldsymbol{v}}, \boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_{2^n}^t$

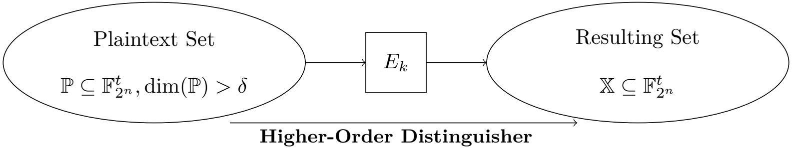
Operation	Propagation	Rule
$x_0 \oplus x_1 = y$	$(u_0, u_1) \xrightarrow{XOR} (v)$	$v = u_0 + u_1$ $v \succeq u_0$
$x_0 \cdot x_1 = y$	$(u_0, u_1) \xrightarrow{AND} (v)$	$v = u_0 = u_1$
$x = y_0 = y_1$	$(u) \xrightarrow{COPY} (v_0, v_1)$	$u = \mathsf{Mn}(v_0 + v_1, n)$
$x^d = y$	$(u) \xrightarrow{POWER} (v)$	$u = \mathsf{Mn}(d \cdot v, n)$

$$\mathsf{Mn}(u,n) = \begin{cases} 2^n - 1, & \text{if } 2^n - 1 \mid u, u \geq 2^n - 1 \\ u\%2^n - 1, & \text{else.} \end{cases}$$

Comparison with Word/Bit-Based Division Property

	Word-Based Division Property	**Bit-Based Division Property**	**General Monomial Prediction**
Variable	$\boldsymbol{X} = (x_0, \cdots, x_t)$ $x_i \in \mathbb{F}_2^N$	$\boldsymbol{X} = (X_0, \cdots, X_{Nt-1})$ $X_i \in \mathbb{F}_2$	$\boldsymbol{x} = (x_0, \cdots, x_t)$ $x_i \in \mathbb{F}_{2^n}$
Operation	word/bit-based	bit-based	field-based
Local Propagation	algebraic degree	ANF	polynomial representation

Higher-Order Differential Attack [Lai94]



- Suppose the algebraic degree of E_k is δ, for any vector space of dimension $\dim(\mathbb{P}) > \delta$, we have

$$\bigoplus_{\boldsymbol{p} \in \mathbb{P}} E_k(\boldsymbol{p}) = 0.$$

- Attackers need to detect the algebraic degree (over $\mathbb{F}_2$) of ciphers over $\mathbb{F}_{2^n}$.

(Algebraic) Degree over Different Fields

$\mathbb{F}_{2^n}[x_0, x_1, \cdots, x_{t-1}] \;/\; \langle {x_0}^{2^n} - x_0, {x_1}^{2^n} - x_1, \cdots, {x_{t-1}}^{2^n} - x_{t-1} \rangle$

$\mathbb{F}_2[X_0, X_1, \cdots, X_{nt-1}] \;/\; \langle {X_0}^2 - X_0, {X_1}^2 - X_1, \cdots, {X_{nt-1}}^2 - X_{nt-1} \rangle$

Corollary: For any $F(x_0, \cdots, x_{t-1}) = \sum_{\boldsymbol{u}} \varphi(\boldsymbol{u}) \cdot x_0^{u_0} \cdots x_{t-1}^{u_{t-1}}, x_i \in \mathbb{F}_{2^n}$

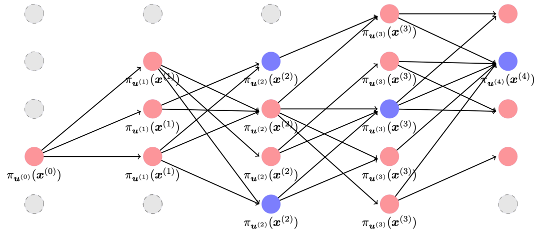
$$\deg(F) = \max\{\sum_{i=0}^{t-1} u_i \mid \varphi(\boldsymbol{u}) \neq 0\},\ \ \delta(F) = \max\{\sum_{i=0}^{t-1} HW(u_i) \mid \varphi(\boldsymbol{u}) \neq 0\}.$$

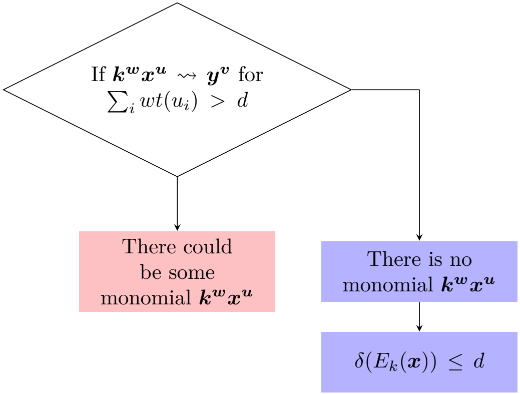
Example: $F(x_0, x_1) = x_0^{13} x_1 + x_0^7 x_1^{10} + 1$

$$\deg(F) = 17,\ \ \delta(F) = 5$$

Our Strategy

Goal is to check if $\boldsymbol{y}^{\boldsymbol{v}}$ has the monomial $\boldsymbol{k}^{\boldsymbol{w}}\boldsymbol{x}^{\boldsymbol{u}}$ with algebraic degree $\delta > d$ or not.





New Detection Algorithm

$$\boldsymbol{k}^{\boldsymbol{w}}\boldsymbol{x}^{\boldsymbol{u}} \rightsquigarrow \boldsymbol{y}^{\boldsymbol{v}} \text{ for } \sum_i wt(u_i) > d$$

Initial Constraints

- $\boldsymbol{u} = (u_0, u_1, \cdots, u_{t-1})$, each u_i is a bitvector with length n.
- $\sum_{i=0}^{t-1} \sum_{j=0}^{n-1} u_i[j] > d$.
- No constraints on $\boldsymbol{w}$.

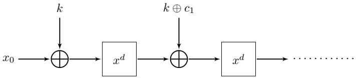
Stopping Rules

- Consider the algebraic degree of the i'th output word

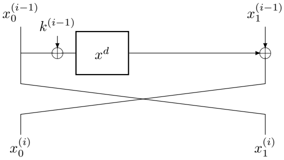
$$\begin{cases} v_i = 1, & \text{if } i = i', \\ v_i = 0, & \text{if } i \neq i'. \end{cases}$$

MiMC Family Specification [Alb+16; Alb+19a]

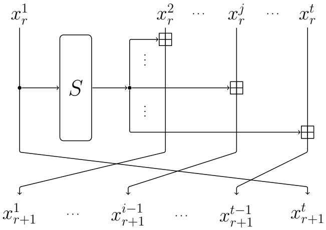
- Use $x \mapsto x^d$ as round function.



MiMC

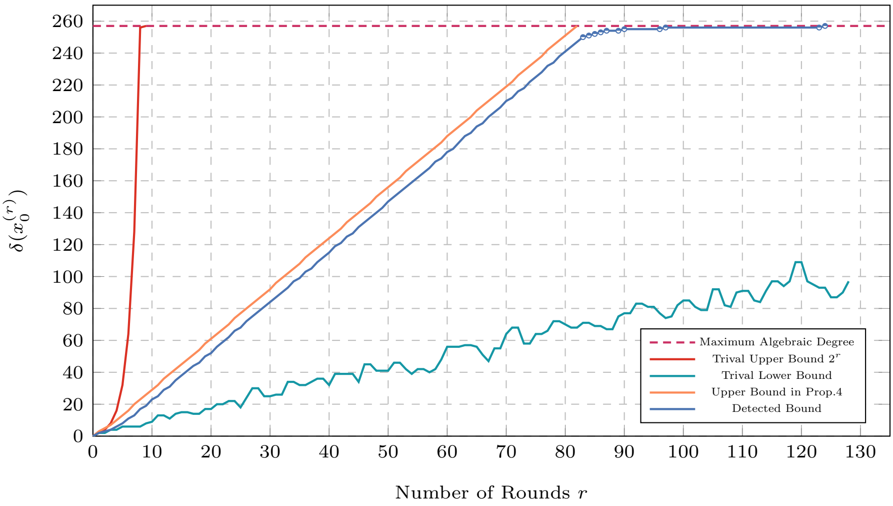


Feistel MiMC



GMiMC-erf

Our Results : Feistel MiMC



Results from Our New Algorithm

MiMC

- Exact algebraic degree for $d = 3$ [BCP22].
- One or two more rounds higher-order distinguisher for $d = 2^l - 1$ (previous best [Eic+20]).
- Higher-order distinguisher with lower data for $d = 2^l + 1$.

Feistel MiMC

- A 124-round higher-order distinguisher (previous best 83 rounds [Bey+20]).
- A full-round known-key higher-order distinguisher (previous best 164 rounds [Bey+20]).

GMiMC$_{\texttt{erf}}$

- A 50-round higher-order distinguisher for GMiMC$_{\texttt{erf}}[33, 8]$ (previous best 40 rounds [Bey+20]).

Results from Our New Algorithm

Primitive	Type	#Rounds	Attack		Source
			#Rounds	Cost	
MiMC ($d = 3$)	Integral distinguisher	82	81	2^{127}	This Work
MiMC ($d = 7$)		46	46	2^{127}	This Work
MiMC ($d = 9$)		41	41	2^{127}	This Work
Feistel MiMC	Integral distinguisher	166	124	2^{257}	This Work
	ZS distinguisher	166	166	2^{251}	This Work
	ZS distinguisher	166	248	2^{257}	This Work
$\text{GMiMC}_{\texttt{erf}}$ [33,8]	Integral distinguisher	56	50	2^{263}	This Work

Conclusion

- Propose general monomial prediction, a way of studying the polynomial representation for ciphers over $\mathbb{F}_{2^n}$.
- Give a new framework of degree evaluation and we no longer only rely on the theoretical proof to estimate the algebraic degree over finite fields.
- Give best degree evaluation and distinguishers for MiMC, Feistel MiMC and GMiMC.
- Open questions:
  - Optimization of the performance?
  - The number of general monomial trails?
  - More about the structure?

Thank you.