Algebraic properties of the MiMC block cipher

Clémence Bouvier[1,2]
Anne Canteaut[2] and Léo Perrin[2]

[1]Sorbonne Université

[2]Inria Paris, team COSMIQ

Seminar COSMIQ, december 16th, 2020

Content

Algebraic properties of the MiMC block cipher

1. Background
   - Emerging uses in symmetric cryptography
   - Definition of algebraic degree
   - Specification of MiMC
2. Study of MiMC and MiMC^{-1}
   - Algebraic degree of MiMC
   - Algebraic degree of MiMC^{-1}
3. Algebraic attack
   - Secret-key 0-sum distinguisher
   - Key-recovery
   - Known-key 0-sum distinguisher

1. Background
   - Emerging uses in symmetric cryptography
   - Definition of algebraic degree
   - Specification of MiMC
2. Study of MiMC and MiMC^{-1}
   - Algebraic degree of MiMC
   - Algebraic degree of MiMC^{-1}
3. Algebraic attack
   - Secret-key 0-sum distinguisher
   - Key-recovery
   - Known-key 0-sum distinguisher

Emerging uses in symmetric cryptography

Block ciphers : indistinguishable from a random permutation

Problem : Analyzing the security of new symmetric primitives

Protocols requiring new primitives :

- multiparty computation (MPC)
- homomorphic encryption (FHE)
- systems of zero-knowledge proofs (zk-SNARK, zk-STARK)

Deployment of the Blockchain

Primitives designed to minimize the number of multiplications in a finite field.
$\Rightarrow$ using nonlinear functions on a large finite field $\mathbb{F}_q$ (such as $\mathbb{F}_{2^n}$ where $n \sim 128$, or prime fields)

Algebraic degree

Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$, there is **one and only one univariate polynomial representation** on $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i ; b_i \in \mathbb{F}_{2^n}$$

Definition

Algebraic degree of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$:

$$\deg(F) = \max\{wt(i),\ 0 \leq i < 2^n,\ \text{and}\ \ b_i \neq 0\}$$

Proposition [BC13][1]

If $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is a permutation, then

$$\deg(F^{-1}) = n - 1 \iff \deg(F) = n - 1$$

[1] Boura, Canteaut (IEEE 2013)
On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$

The block cipher MiMC

Construction of MiMC [AGR+16][2] :

- n-bit blocks ($n \approx 127$)
- n-bit key k
- decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$

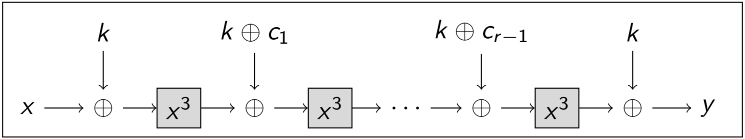


Figure: The MiMC encryption with r rounds

Security analysis of the encryption : Cryptanalysis

$\Rightarrow$ Study of the **algebraic degree**

[2] Albrecht et al. (Eurocrypt 2016)
MiMC : Efficient Encryption and Cryptographic with Minimal Multiplicative Complexity

Security analysis

A first plateau :

- Round 1 : deg $= 2$

$$\mathcal{P}_1(x) = (x+k)^3 = x^3 + kx^2 + k^2x + k^3$$

$1 = [1]_2$ $2 = [10]_2$ $3 = [11]_2$

- Round 2 : deg $= 2$

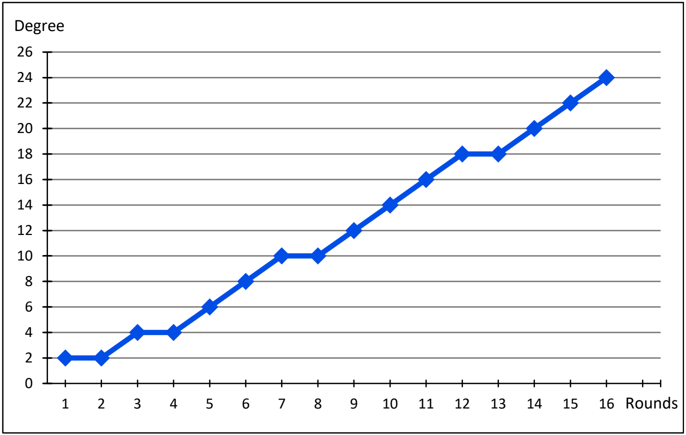
$$\begin{aligned}\mathcal{P}_2(x) &= ((x+k)^3 + k_1)^3 \\ &= x^9 + kx^8 + k_1x^6 + k^2k_1x^4 + k_1^2x^3 + (k^4k_1 + kk_1^2)x^2 \\ &+ (k^8 + k^2k_1^2)x + (k^3+k_1)^3 \qquad \text{where } k_1 = k + c_1\end{aligned}$$

$1 = [1]_2$ $2 = [10]_2$ $3 = [11]_2$ $4 = [100]_2$ $6 = [110]_2$ $8 = [1000]_2$ $9 = [1001]_2$

1. Background
   - Emerging uses in symmetric cryptography
   - Definition of algebraic degree
   - Specification of MiMC
2. Study of MiMC and MiMC^{-1}
   - Algebraic degree of MiMC
   - Algebraic degree of MiMC^{-1}
3. Algebraic attack
   - Secret-key 0-sum distinguisher
   - Key-recovery
   - Known-key 0-sum distinguisher

Algebraic degree of MiMC

Figure: Algebraic degree of MiMC encryption



Algebraic degree of MiMC

Proposition

List of exponents that might appear in the polynomial :

$$\mathcal{M}_r = \{3j \bmod (2^n - 1) \text{ where } j \preceq i,\ i \in \mathcal{M}_{r-1}\}$$

If $3^r < 2^n - 1$:
upper bound $= 2 \times \lfloor \log_2(3^r)/2 \rfloor$
lower bound $= wt(3^r)$

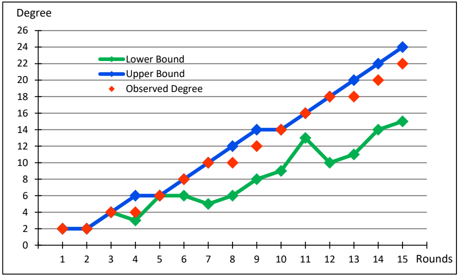


Figure: Comparison of the observed degree with bounds (for $n = 25$)

Algebraic degree of MiMC

Theorem

After r rounds of MiMC, the algebraic degree is

$$d \leq 2 \times \lceil \lfloor \log_2(3^r) \rfloor / 2 - 1 \rceil$$

Study of the missing monomials in the polynomial:

- no exponent $\equiv 5, 7 \mod 8$ so no exponent $2^{2k} - 1$
  Example $63 = 2^{2 \times 3} - 1 \notin \mathcal{M}_4 = \{0, 3, \ldots, 81\}$
  $\Rightarrow deg < 6 = wt(63)$
- if $k = \lfloor \log_2(3^r) \rfloor$, for all $r > 4$, $2^{k+1} - 5 > 3^r$
  Example $\lfloor \log_2(3^8) \rfloor = 12$ and $3^8 = 6561 < 8187 = 2^{13} - 5$
  $\Rightarrow deg < 12 = wt(8187)$

Algebraic degree of MiMC

Conjecture : After r rounds of MiMC, the algebraic degree is :

$$d = 2 \times \lceil \lfloor \log_2(3^r) \rfloor / 2 - 1 \rceil$$

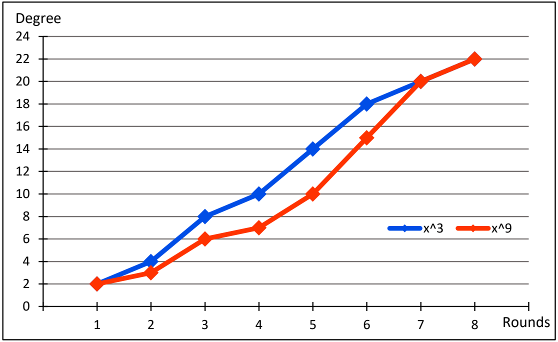
Study of maximum weight exponent monomials, present in polynomial:

- $2^{2k-1} - 5$ and $2^{2k} - 7$ if $\lfloor \log_2(3^r) \rfloor = 2k$
  Example $27 = 2^{2\times 3-1} - 5, 57 = 2^{2\times 3} - 7 \in \mathcal{M}_4 = \{0, 3, \ldots, 81\}$
  $\Rightarrow deg = 4 = wt(27) = wt(57)$
- $2^{2k+1} - 5$ if $\lfloor \log_2(3^r) \rfloor = 2k+1$
  Example $123 = 2^{2\times 3+1} - 5 \in \mathcal{M}_5 = \{0, 3, \ldots, 243\}$
  $\Rightarrow deg = 6 = wt(123)$

$\Rightarrow$ plateau when $\lfloor \log_2(3^r) \rfloor = 2k - 1$ and $\lfloor \log_2(3^{r+1}) \rfloor = 2k$

Form of coefficients

Figure: Comparison of algebraic degree for rounds r of MiMC with x^9 and for rounds $2r$ of MiMC with x^3 ($n = 23$)

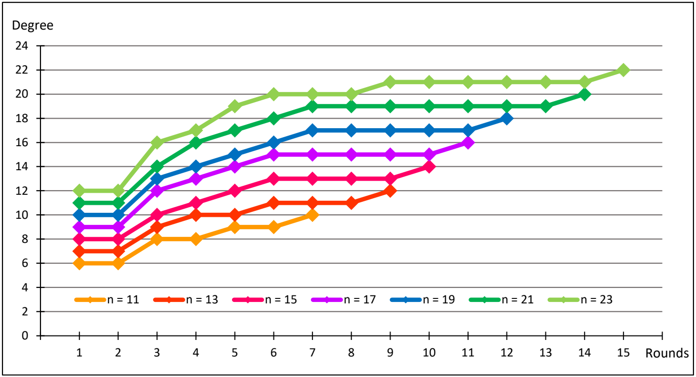


Exemple: coefficients of maximum weight exponent monomials at round 4

$$27 : c_1^{18} + c_3^2 \quad 30 : c_1^{17} \quad 51 : c_1^{10} \quad 54 : c_1^9 + c_3 \quad 57 : c_1^8 \quad 75 : c_1^2 \quad 78 : c_1$$

Study of MiMC^{-1}

Figure: Algebraic degree of MiMC decryption



Inverse function : $F : x \mapsto x^s, s = (2^{n+1} - 1)/3 = [101..01]_2$

Some ideas studied

plateau between round 1 and 2

- Round 1 : $deg = wt(s) = (n+1)/2$
- Round 2 : $deg = \max\{wt(js),\ \text{for } j \preceq s\} = (n+1)/2$

Proposition

for $j \preceq s$ such that $wt(j) \geq 2$:

$$wt(js) \in \begin{cases} [wt(j)-1, (n-1)/2] & \text{if } \ wt(j) \equiv 2 \mod 3 \\ [wt(j), (n+1)/2] & \text{else} \end{cases}$$

Some ideas studied

plateau between round 1 and 2

- Round 1 : $deg = wt(s) = (n+1)/2$
- Round 2 : $deg = \max\{wt(js),\ \text{for } j \preceq s\} = (n+1)/2$

Proposition

for $j \preceq s$ such that $wt(j) \geq 2$:

$$wt(js) \in \begin{cases} [wt(j)-1, (n-1)/2] & \text{if } \ wt(j) \equiv 2 \mod 3 \\ [wt(j), (n+1)/2] & \text{else} \end{cases}$$

Next rounds : another plateau at $n-2$?

$$\boxed{r_{n-2} \geq \left\lceil \frac{1}{\log_2 3} \left(2 \left\lceil \frac{n-5}{4} \right\rceil + 3\right) \right\rceil}$$

Study of MiMC^{-1}

Upper bound

Proposition

$\forall i \in [1, n-1]$, if the algebraic degree of encryption is $\deg(F) < (n-1)/i$, then the algebraic degree of decryption is $\deg(F^{-1}) < n - i$

Lower Bound

- Round 3 :
  $d \geq (n+1)/2 + \lfloor (n+1)/6 \rfloor$
- Round $r \geq 4$:
  $d \geq (n+1)/2 + \lfloor n/4 \rfloor$.

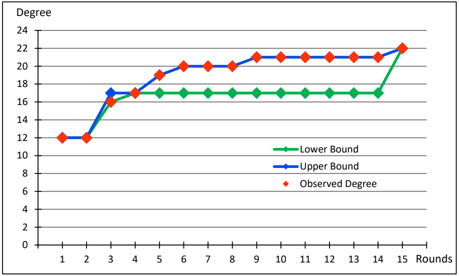


Figure: Bounds on algebraic degree of MiMC decryption (for $n = 23$)

Other permutations

Other permutations with a plateau between rounds 1 and 2 :

Proposition

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto x^d$ where $d = 2^k - 1$. If $d^2 < 2^n - 1$, then :

$$deg((x^d + c)^d) = deg(x^d) \quad \text{where } c \text{ is a constant}$$

BUT no plateau between rounds 1 and 2 for decryption !

Example (with $\mathbb{F}_{2^{11}}$)

- encryption : $15 = 2^4 - 1 \Rightarrow$ plateau
- decryption : $15^{-1} = 273$ so
  - algebraic degree at round 1 : $3 = wt(273)$
  - algebraic degree at round 2 : $5 = wt(273 \times 273 \mod 2^{11} - 1)$

1. Background
   - Emerging uses in symmetric cryptography
   - Definition of algebraic degree
   - Specification of MiMC

2. Study of MiMC and MiMC^{-1}
   - Algebraic degree of MiMC
   - Algebraic degree of MiMC^{-1}

3. Algebraic attack
   - Secret-key 0-sum distinguisher
   - Key-recovery
   - Known-key 0-sum distinguisher

Higher-order differential attacks

Higher-order differentials :

Exploiting a low algebraic degree
If $\deg(f) = d$, then for a vector space $\mathcal{V}$ such that $\dim \mathcal{V} \geq d + 1$

$$\bigoplus_{x \in \mathcal{V}} f(x) = 0.$$

$\Rightarrow$ set up a 0-sum distinguisher

Random permutation : maximal degree $= n - 1$

Secret-key 0-sum distinguisher

Proposition

The number of rounds of MiMC$_k$ (or MiMC$_k^{-1}$) necessary for the algebraic degree to reach its maximum is : $r \geq \lceil \log_3 2^n \rceil$.

Full MiMC$_k$: $R = \lceil \log_3 2^n \rceil$

Corollary

Let $\mathcal{V}$ be a $(n-1)$-dimensional subspace of $\mathbb{F}_{2^n}$. We can set up a 0-sum distinguisher for $R-1$ rounds of MiMC$_k$ (or MiMC$_k^{-1}$).
$\Rightarrow$ 1 round of security margin.

Let $f^r(x,k)$ be the function corresponding to r rounds of MiMC$_k$

$$\bigoplus_{x \in \mathcal{V}} f^{R-1}(x,k) = 0 = \bigoplus_{x \in \mathcal{V}} f^{-(R-1)}(x,k) \ .$$

Secret-key 0-sum distinguisher

Proposition

$\forall r \leq R - 1$, the algebraic degree of MiMC satisfies : $d \leq n - 3$.

Corollary

Let $\mathcal{V}$ be a $(n-2)$-dimensional subspace of $\mathbb{F}_{2^n}$. We can set up a 0-sum distinguisher for $R-1$ rounds of MiMC$_k$

Secret-key 0-sum distinguisher

Proposition

$\forall r \leq R-1$, the algebraic degree of MiMC satisfies : $d \leq n-3$.

Corollary

Let $\mathcal{V}$ be a $(n-2)$-dimensional subspace of $\mathbb{F}_{2^n}$. We can set up a 0-sum distinguisher for $R-1$ rounds of MiMC$_k$

Example

r	78	79	80	81	82
d	122	124	124	126	128

Table: Degree in the last rounds for $n = 129$

Algebraic degree of MiMC at $r = R-2$: $d \leq n-3$ or $d \leq n-5$.
$\Rightarrow$ 0-sum distinguisher for $R-2$ rounds of MiMC$_k$, for a $(n-2)$ or $(n-4)$-dimensional subspace of $\mathbb{F}_{2^n}$.

Key-recovery

Let $\mathcal{V}$ be a $(n-1)$-dimensional subspace of $\mathbb{F}_{2^n}$.
$\Rightarrow$ 0-sum distinguisher for $R-1$ rounds of MiMC_k^{-1}.
So

$$F(k) = \bigoplus_{x \in \text{MiMC}_k^{-1}(\mathcal{V}+v)} f(x,k) = 0 \; .$$

1 round of MiMC_k is described by :

$$(x \oplus k)^3 = k^3 \oplus k^2 \cdot x \oplus k \cdot x^2 \oplus x^3$$

Let $\mathcal{W} = \text{MiMC}_k^{-1}(\mathcal{V}+v)$:

$$\begin{aligned} F(k) &= \bigoplus_{x \in \mathcal{W}} (k^3 \oplus k^2 \cdot x \oplus k \cdot x^2 \oplus x^3) \\ &= \left(k^2 \cdot \bigoplus_{x \in \mathcal{W}} x \right) \oplus \left(k \cdot \bigoplus_{x \in \mathcal{W}} x^2 \right) \oplus \left(\bigoplus_{x \in \mathcal{W}} x^3 \right) \end{aligned}$$

Known-key 0-sum distinguisher

0-sum distinguisher for $R - 1$ rounds of MiMC_k and MiMC_k^{-1}.
So with a known-key : 0-sum distinguisher for $2R - 2$ rounds

Impact on hash functions ?

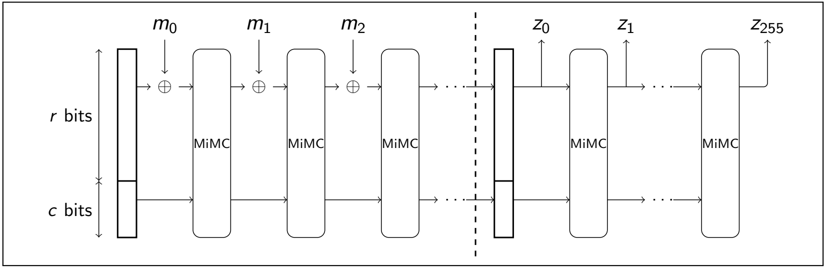


Figure: Sponge hash function

Known-key 0-sum distinguisher

MiMC with $n = 1025$ (647 rounds).

- rate : 512 bits
- capacity : 513 bits
- plateau on rounds $R-4$ and $R-3$ (equals to $n-7$) for MiMC encryption
- $r_{n-2} \geq 324$, so the degree at round $r < r_{n-2}$ satisfies : $d \leq n-3$.

$$\begin{tikzcd}
x & \boxed{f^{-(R-1)}(y,0)} \arrow[l] & y \arrow[l] \arrow[r] & \boxed{f^{R-1}(y,0)} \arrow[r] & z \\
 & d \leq n-2 & & d \leq n-3 &
\end{tikzcd}$$

$dim(\mathcal{V}) = n-1$ $\quad 2R-2$ rounds

$$\begin{tikzcd}
x & \boxed{f^{-323}(y,0)} \arrow[l] & y \arrow[l] \arrow[r] & \boxed{f^{R-1}(y,0)} \arrow[r] & z \\
 & d \leq n-3 & & d \leq n-3 &
\end{tikzcd}$$

$dim(\mathcal{V}) = n-2$ $\quad \sim \frac{3}{2}R$ rounds

$$\begin{tikzcd}
x & \boxed{f^{-216}(y,0)} \arrow[l] & y \arrow[l] \arrow[r] & \boxed{f^{R-2}(y,0)} \arrow[r] & z \\
 & d \leq n-4 & & d \leq n-5 &
\end{tikzcd}$$

$dim(\mathcal{V}) = n-3$ $\quad \sim \frac{4}{3}R$ rounds

Known-key 0-sum distinguisher

MiMC with $n = 769$ (486 rounds).

- rate : 512 bits
- capacity : 257 bits
- plateau on rounds $R-2$ and $R-1$ (equals to $n-3$) for MiMC encryption
- $r_{n-2} \geq 243$, so the degree at round $r < r_{n-2}$ satisfies : $d \leq n-3$.

$$\begin{tikzcd} x & \underset{d \leq n-2}{\boxed{f^{-(R-1)}(y,0)}} \arrow[l] & y \arrow[l] \arrow[r] & \underset{d \leq n-3}{\boxed{f^{R-1}(y,0)}} \arrow[r] & z \end{tikzcd}$$

$dim(\mathcal{V}) = n-1$ $\quad 2R-2$ rounds

$$\begin{tikzcd} x & \underset{d \leq n-3}{\boxed{f^{-242}(y,0)}} \arrow[l] & y \arrow[l] \arrow[r] & \underset{d \leq n-3}{\boxed{f^{R-1}(y,0)}} \arrow[r] & z \end{tikzcd}$$

$dim(\mathcal{V}) = n-2$ $\quad \sim \frac{3}{2}R$ rounds

$$\begin{tikzcd} x & \underset{d \leq n-4}{\boxed{f^{-162}(y,0)}} \arrow[l] & y \arrow[l] \arrow[r] & \underset{d \leq n-5}{\boxed{f^{R-3}(y,0)}} \arrow[r] & z \end{tikzcd}$$

$dim(\mathcal{V}) = n-3$ $\quad \sim \frac{4}{3}R$ rounds

Comparison to previous work

Type	n	Rounds	Time	Data	Source
SK[3]	129	80	2^{128}XOR	2^{128}	[EGL+20][4]
SK	n	$\lceil \log_3(2^{n-1}-1)\rceil - 1$	2^{n-1}XOR	2^{n-1}	[EGL+20]
SK	129	81	2^{128}XOR	2^{128}	Slide 20
SK	n	$\lceil \log_3 2^n \rceil - 1$	2^{n-1}XOR	2^{n-1}	Slide 20
SK	129	81 (MiMC)	2^{127}XOR	2^{127}	Slide 21
SK	n	$\lceil \log_3 2^n \rceil - 1$ (MiMC)	2^{n-2}XOR	2^{n-2}	Slide 21
SK	129	80 (MiMC)	2^{125}XOR	2^{125}	Slide 21
SK	n	$\lceil \log_3 2^n \rceil - 2$ (MiMC)	2^{n-2} ou 2^{n-4}XOR	2^{n-2} ou 2^{n-4}	Slide 21
KK	129	160	-	2^{128}	[EGL+20]
KK	n	$2 \cdot \lceil \log_3(2^{n-1}-1)\rceil - 2$	-	2^{n-1}	[EGL+20]
KK	129	162	-	2^{128}	Slide 23
KK	n	$2 \cdot \lceil \log_3 2^n \rceil - 2$	-	2^{n-1}	Slide 23
KR	129	82	$2^{122.64}$	2^{128}	[EGL+20]
KR	n	$\lceil n \cdot \log_3 2 \rceil$	$2^{n-1-(\log_2\lceil n \log_3 2\rceil)}$ ou $2^{n-(\log_2\lceil n \log_3 2\rceil)}$	2^{n-1}	[EGL+20]
KR	129	82	$2^{121.64}$	2^{128}	Slide 22
KR	n	$\lceil n \cdot \log_3 2 \rceil$	$2^{n-1-(\log_2\lceil n \log_3 2\rceil)}$	2^{n-1}	Slide 22

Table: Attack complexity on MiMC

[3] SK : Secret-key distinguisher, KK : Known-key distinguisher, KR : Key-recovery

[4] Eichlseder et al. (Asiacrypt 2020)
An Algebraic Attack on Ciphers with Low-Degree Round Functions

Conclusion

MiMC study :

- steps in the evolution of the degree of the MiMC encryption function

$$2 \times \lceil \lfloor \log_2(3^r) \rfloor / 2 - 1 \rceil$$

- inverse transformation
  - plateau between rounds 1 and 2
  - next rounds ?
    plateau at $n-2$ in the last rounds ?

Attacks

- 0-sum distinguishers
- key-recovery

⇒ limited by the high degree of the inverse in the last rounds

$\boxed{\text{Other types of attacks ?}}$

Thanks for your attention