SCIENCE
PASSION
TECHNOLOGY

An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC

Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, **Markus Schofnegger**, Qingju Wang

November 23, 2020

Background

- Algebraically simple designs are becoming increasingly popular
  - Proof systems like SNARKs, STARKs, ...
- Certain metrics are more important than others
  - – Plain efficiency
  - + Algebraic representation of the construction
  - + Number of multiplications (also in e.g. MPC)
- MiMC [2] a benchmark since 2016 in some of these settings
  - And basis for follow-up designs (e.g., GMiMC [1] and HadesMiMC [5])

Summary of the Attacks

Type	n	Rounds	Time	Data
SK	129	80	2^{128}	2^{128}
SK	n	$\lceil \log_3(2^{n-1} - 1) \rceil - 1$	2^{n-1}	2^{n-1}
KK	129	160 ($\approx 2 \times$ full)	–	2^{128}
KK	n	$2 \cdot \lceil \log_3(2^{n-1} - 1) \rceil - 2$	–	2^{n-1}
KR	129	82 (full)	$2^{122.64}$	2^{128}
KR	255	161 (full)	$2^{246.67}$	2^{254}
KR	n	$\lceil n \cdot \log_3(2) \rceil$ (full)	$\leq 2^{n-\log_2(n)+1}$	2^{n-1} CC

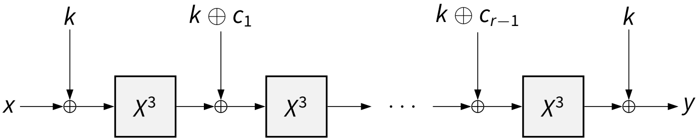
Overview

- Specification of the MiMC block cipher
  - Round function
  - Number of rounds
  - Degree of the round function
- Distinguishers for MiMC
- Key-Recovery Attack on MiMC
- Summary and Future Work

Specification of MiMC

MiMC – Specification

- MiMC works over $\mathbb{F}_p$ or $\mathbb{F}_{2^n}$
  - Attack works over $\mathbb{F}_{2^n}$
- Simple construction:



- Round function in round i:

$$R_i(x) = (x + k + c_i)^3$$

MiMC – Specification cont.

- Every round key k the same (no key schedule)
- Round constants c_i chosen randomly from $\mathbb{F}_{2^n}$
- n is odd to achieve a permutation
- How many rounds are secure?
- Approach by the designers
  - Best known non-random property as reference, add one more round
  - $r = \lceil n / \log_2(3) \rceil$ rounds (for example, 82 rounds for $n = 129$)
- Due to this new result, a few more rounds are needed

MiMC – Round Function Degree

- Word-level degree of round function is 3
  - Upper bound for degree of whole construction is 3^r after r rounds
  - Complexity of factorization, interpolation, ...
  - Number of rounds chosen w.r.t. this analysis
- Bit-level degree (*algebraic degree*) of round function is $\mathrm{hw}(3) = 2$
  - Upper bound for degree of whole construction is 2^r after r rounds
  - For example, $2^{82} \gg 128$ for $r = 82$ and $n = 129$
  - Most likely, security is easily reached here...

Distinguishers for MiMC

Higher-Order Differentials [7, 6]

- Exploit low algebraic degrees
- Distinguishers if this degree is sufficiently low
  - Algebraic degree of $f(\cdot)$ is δ, vector space $V \oplus c$ of dimension $\delta + 1$:

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

  - Results in a *zero-sum* distinguisher
- What do we need for protection?
  - Reach max. algebraic degree ($n - 1$ for permutation with block size n)
  - Vector space needs then dimension n (i.e., full space)

Algebraic Degree of Key-Alternating Ciphers

- Consider a key-alternating cipher $E_k^r : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

$$E_k^r(x) := k_r \oplus R(\cdots R(k_1 \oplus R(k_0 \oplus x))\cdots)$$

- Each round function $R(\cdot)$ has degree d
- We want to reach algebraic degree $n-1$
- Focus on the smallest word-level degree $\overline{d}$ with $\mathrm{hw}(\overline{d}) = n-1$
  - $\overline{d} = 2^{n-1} - 1$
- When does a monomial of degree $\geq \overline{d}$ appear?
  - For example, $x^{2^{n-1}-1}$ in the univariate description of MiMC

Algebraic Degree of Key-Alternating Ciphers cont.

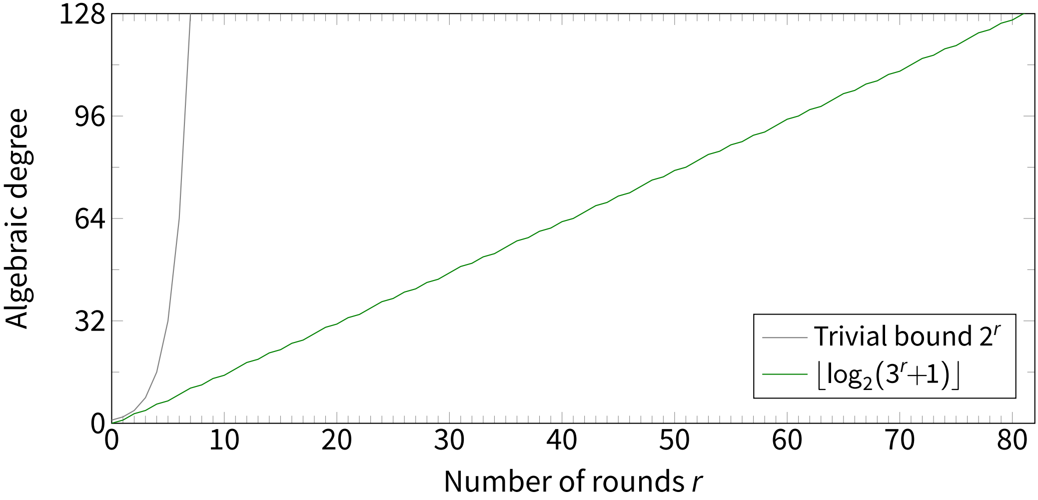
- To make such a monomial appear, we need

$$d^r \geq 2^{n-1} - 1$$

- This implies $r \geq \lceil \log_d(2^{n-1} - 1) \rceil$
- For $d = 3$, this is *very* close to the number of rounds of MiMC
  - Indeed, it's at most 2 off

$\rightarrow$ Growth is linear in the number of rounds

Algebraic Degree Growth – Concrete Example MiMC



Higher-Order (Secret-Key) Distinguisher

- Following the previous results:
  - Higher-order distinguisher on $\lceil \log_3(2^{n-1} - 1) \rceil - 1$ rounds
  - Number of rounds not covered by distinguisher

$$1 \leq \lceil n \cdot \log_3(2) \rceil - \left(\left\lceil \log_3(2^{n-1} - 1) \right\rceil - 1 \right) \leq 2$$

- Examples for various block sizes:
  - Distinguisher covers $r - 1$ rounds for $n \in \{33, 63, 255\}$
  - Distinguisher covers $r - 2$ rounds for $n \in \{31, 65, 129\}$

Known-Key Distinguisher

- Attacker knows the key
- Discover property that holds with a probability higher than that for an ideal permutation
  - Find set of inputs and outputs whose sums are equal to zero
  - Exploit the inside-out approach

$$\underbrace{\bigoplus_{w \in \mathcal{V} \oplus v} R^{-(r_{dec}-1)}(w) = 0}_{\text{Zero sum}} \xleftarrow{R^{-(r_{dec}-1)}} \mathcal{V} \oplus v \xrightarrow{R^{r_{enc}-1}} \underbrace{0 = \bigoplus_{w \in \mathcal{V} \oplus v} R^{r_{enc}-1}(w)}_{\text{Zero sum}}$$

- We know $R^{r_{enc}-1} \approx$ full MiMC, but what about $R^{-(r_{dec}-1)}$?

Known-Key Distinguisher cont.

Proposition (Corollary 3 of [3])

Let F be a permutation of $\mathbb{F}_2^n$. The algebraic degree of the inverse F^{-1} is $n-1$ if and only if the algebraic degree of F is $n-1$.

If we use a subspace of dimension $n-1$, the number of rounds we can distinguish is the same for MiMC and MiMC^{-1}!

- $R^{r_{\text{enc}}-1} \approx$ full MiMC *and* $R^{-(r_{\text{dec}}-1)} \approx$ full MiMC^{-1}
- Known-key zero-sum distinguisher on almost *double* the number of rounds

Key-Recovery Attack on MiMC

Ingredients

- Distinguisher with dimension $n - 1$ works in both directions
- Secret-key distinguisher on almost the full round number
  - Usually exactly what we need for an attack …
- Some major problems here
  - We need a high data complexity
  - The final subkey has a size of n bits
  - Full diffusion at bit level, high-degree inverse $\rightarrow$ guessing not an option
  - Interpolation like [4]? Many monomials, more data $\rightarrow$ not possible

Ingredients cont.

How to break the final round?

Key-Recovery Attack

- Both encryption function and decryption function reach maximum degree only in last 1 or 2 rounds
- Can we build an efficient equation system for the remaining few rounds?
  - Encryption function has much smaller degree (cheaper to evaluate)

$$R_1(x) = (x+k)^3 = x^3 + x^2k + xk^2 + k^3 \quad (\text{over } \mathbb{F}_{2^n})$$

- Request plaintexts (chosen ciphertexts)
- "Fill in" and sum over the values of $R_1(x)$ with each received plaintext x
- Solve the remaining univariate polynomial in k

Key-Recovery Attack cont.

- Generate symbolic expression:

$$R_1(x, k) = (x + k)^3 = x^3 + x^2k + xk^2 + k^3$$

- Request texts, compute values, start solving:

$$\underbrace{\{\text{MiMC}^{-1}(w) \mid w \in \mathbb{F}_{2^{n-1}}\}}_{\text{Plaintexts requested by oracle}} \xrightarrow{\text{Key solving}} \underbrace{0 = \bigoplus_{w \in \mathbb{F}_{2^{n-1}}} R^{-(r-1)}(w)}_{\text{Higher-order distinguisher}}$$

Key-Recovery Attack Complexity

- Complexity for computing $(x+k)^3 = x^3 + x^2k + xk^2 + k^3$
  - 2^{n-1} multiplications for x^3 (squarings are linear)
  - $2^{n-1} + 1$ squarings for x^3 and final x^2
  - $2^n + 1$ n-bit `XOR` additions for x, x^3, and final representation
- Complexity of solving $F(K) = K^2 \cdot \mathscr{P}_1 \oplus K \cdot \mathscr{P}_2 \oplus \mathscr{P}_3$ for K is negligible
  - $\mathscr{P}_i$ are the sums computed before
- Advantage w.r.t. exhaustive search is $\approx \log_2(n)$
- Memory cost is negligible

Key-Recovery Attack Impact

- Verified practically on toy versions[1]
  - Only 1 round for solving step in tested versions
  - Analysis and implementation also cover the case of two rounds
- New recommendation for number of rounds of MiMC
  - Based on number of multiplications necessary for attack and MiMC

[1] https://github.com/IAIK/mimc-analysis

New Recommendation for Number of Rounds

- Assume $\lceil n \log_3(2) \rceil - 1$ rounds can be covered by zero sum
- Cost dominated by number of operations needed to compute $F(K)$
- Around $((3^{\mathrm{KR}} - 1)/2) \cdot 2^{n-1}$ multiplications required
- $\lceil n \cdot \log_3(2) \rceil$ multiplications for MiMC encryption
- Number of extra rounds ρ has to satisfy

$$(3^{\rho+1} - 1) \cdot 2^{n-2} \geq 2^n \cdot (\lceil n \cdot \log_3(2) \rceil + \rho)$$

- For example, 87 rounds for $n = 129$ (instead of 82)

Key-Recovery Attack Generalization

- Straight-forward generalization from $\mathbb{F}$ to $\mathbb{F}^t$
- Final solving step with Gröbner basis
  - Multivariate system of equations
- Complete definition available in full paper
  - Pseudo code
  - Complexity estimation

Summary and Future Work

- New bound for degree growth of key-alternating ciphers
- First key-recovery attack on full MiMC over $\mathbb{F}_{2^n}$
- Complexity high, but strictly below exhaustive search
- New attack approach
  - Applicable to other low-degree constructions?
- Better analysis of inverse degree
  - Possible to reduce data complexity?

Questions

?

Bibliography I

[1] Martin R. Albrecht et al. **Feistel Structures for MPC, and More.** Computer Security - ESORICS 2019. Vol. 11736. LNCS. 2019, pp. 151–171.

[2] Martin R. Albrecht et al. **MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity.** ASIACRYPT 2016. Vol. 10031. LNCS. 2016, pp. 191–219.

[3] Christina Boura and Anne Canteaut. **On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$.** IEEE Trans. Information Theory 59.1 (2013), pp. 691–702.

[4] Itai Dinur et al. **Optimized Interpolation Attacks on LowMC.** Advances in Cryptology – ASIACRYPT 2015. Ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9453. LNCS. Springer, 2015, pp. 535–560. DOI: 10.1007/978-3-662-48800-3_22.

[5] Lorenzo Grassi et al. **On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy.** EUROCRYPT (2). Vol. 12106. LNCS. Springer, 2020, pp. 674–704.

Bibliography II

[6] Lars R. Knudsen. **Truncated and Higher Order Differentials.** FSE 1994. Vol. 1008. LNCS. 1994, pp. 196–211.

[7] Xuejia Lai. **Higher Order Derivatives and Differential Cryptanalysis.** Communications and Cryptography: Two Sides of One Tapestry. Springer US, 1994, pp. 227–233.