On the Algebraic Degree of Iterated Power Functions

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

[1] Sorbonne Université, France
[2] Inria, France
clemence.bouvier@inria.fr, anne.canteaut@inria.fr, leo.perrin@inria.fr

Abstract. New symmetric primitives intended to be run in abstract settings such as multi-party computations are being designed to use operations over large finite fields. In this work, we investigate the algebraic degree of one of the first such block ciphers, namely MiMC. It is composed of many iterations of a simple round function, which consists of an addition and of a low-degree power permutation applied to the full state, usually $x \mapsto x^3$ over a large field with characteristic 2. We show that, while the *univariate* degree increases predictably with the number of rounds, the *algebraic* degree has a much more complex behaviour, and simply stays constant during some rounds. We present a full investigation of such *plateaus* that slightly slow down the growth of the algebraic degree. Using these results, we slightly improve the higher-order differential attack presented by the authors of MiMC to cover one or two more rounds. More importantly, our results provide some precise guarantee on the algebraic degree of this cipher, and then on the minimal complexity for a higher-order differential attack.

1 Introduction

New computing environments are emerging, such as smart-contracts or zero-knowledge proofs, implementing Multi-Party Computation (MPC) protocols. The rise of these environments creates a new need since symmetric primitives are still needed in these contexts, in particular to ensure computation integrity [5]. However, the basic operations provided by these platforms correspond neither to the CPU instructions (bit-wise AND, rotations, etc.) nor to the hardware components (XNOR, wires, etc.) that are used to build symmetric primitives in the usual case. Instead, the core operations that implementers can use are finite-field operations over fields $\mathbb{F}_q$ of large size q, where q is typically bigger than 2^{64} and is usually either a prime number or a power of 2 [2,4]. Primitives that are designed using such operations only are called *arithmetization-friendly*, see e.g. [6] for a detailed survey on the arithmetization-friendly hash functions.

Designing arithmetization-friendly symmetric primitives is different from the "usual" case. Instead of using operations on $\mathbb{F}_{2^n}$ where n is a small even integer, typically $n = 4$ or 8, the underlying alphabet is now a large field whose cardinality is chosen according to some other parts in the protocol such as for instance the underlying field of a standard elliptic curve ($q \approx 2^{256}$), or, in some SNARK cases, a field of size $q = 2^{64}$. In order to optimize the multiplicative complexity of the circuit describing the encryption, the proposed constructions use non-linear functions but whose algebraic representations remain very simple on a large finite field. Indeed, several such proposals have been found to have significant flaws, from ad-hoc attacks relying on internal simplifications [1], to integral attacks [7]. Hence, it is necessary to better understand the behaviour of cryptanalysis techniques when they are applied to arithmetization-friendly designs.

Univariate and Algebraic Degrees. In this paper, we investigate the algebraic degree of an arithmetization-friendly block cipher. The complexity of so-called *higher-order differential attacks* [10] decreases with the algebraic degree, implying that it is important to understand how this quantity increases as a given round function is iterated. Let us first recall the two notions of degree which apply to a function over a finite field with characteristic 2.

Definition 1 (ANF and Algebraic Degree). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Its* Algebraic Normal Form (ANF) *is the representation of f as a multivariate polynomial with variables in $\mathbb{F}_2^n$, so that $f(x_0, ..., x_{n-1}) = \sum_{u \in \mathbb{F}_2^n} a_u x^u$, where $a_u \in \mathbb{F}_2$ for all u, and $x^u = \prod_{i=0}^{n-1} x_i^{u_i}$.*
The algebraic degree *of f is $\deg^a f = \max\left\{\mathrm{wt}(u) : u \in \mathbb{F}_2^n, a_u \neq 0\right\}$, where $\mathrm{wt}(u)$ is the Hamming weight of u. If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, then its algebraic degree, $\deg^a F$, is the maximal algebraic degree of the coordinates of F.*

Definition 2 (Univariate Representation and Degree). *Let $q > 1$ be a prime power and let F be a function from $\mathbb{F}_q$ to $\mathbb{F}_q$. Then the* univariate polynomial representation *of F is $F(x) = \sum_{i=0}^{q-1} u_i x^i$, where $u_i \in \mathbb{F}_q$ for all integers i. Its* univariate degree *$\deg^u F$ is the largest integer i for which $u_i \neq 0$.*

If $q = 2^n$, then a function $F : \mathbb{F}_q \to \mathbb{F}_q$ can be seen both as a function defined over the finite field, and as a function defined over the vector space $\mathbb{F}_2^n$ using a simple isomorphism between $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$. For such a function, the algebraic degree is related to the univariate representation as follows: $\deg^a F = \max\{\mathrm{wt}(i) : i \in \mathbb{N}, u_i \neq 0\}$, where $\{u_i\}_{i \geq 0}$ is the set of all coefficients in the univariate representation of F.

Our Target. In this paper, we focus on the block cipher MiMC, introduced by Albrecht *et al.* [3], which operates on $\mathbb{F}_{2^n}$. It consists of r iterations of an extremely simple round function: round i, $0 \leq i < r$, corresponds to $x \mapsto x^d + c_{i+1}$, where d is coprime with $(2^n - 1)$ in order to ensure that the round function is bijective, and where $c = (c_1, \ldots, c_r)$ is a sequence of r round constants. As a consequence, the round function of a MiMC instance is fully specified by the exponent d and by the sequence c of all round constants, and we denote such a MiMC instance $\mathsf{MIMC}_{d,c}[r]$. It is worth noting that the key is omitted in this description: indeed, as far as the algebraic degree is concerned, it can be considered to be part of the round constants.

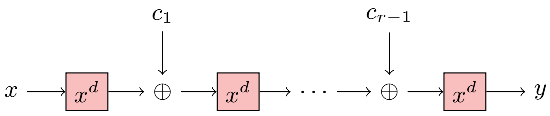

Fig. 1. $\mathsf{MIMC}_{d,c}$ with r rounds.

More precisely, our aim is to investigate the security of MiMC against integral attacks, and thus its algebraic degree. Let $(B_d^r)_{r>0}$ denote the sequence of the maximal degree of r rounds of MIMC_d, i.e., for any r, B_d^r is the degree of $\mathsf{MIMC}_{d,c}[r]$ for at least one sequence $c = (c_1, \dots, c_r)$ of constants:

$$B_d^r := \max_c \deg^a \mathsf{MIMC}_{d,c}[r] \ .$$

It may happen that this degree is not reached for some specific sets of round constants as we will point out in Sec. 5, hence the need to take the maximum over them. Our goal is then to find the exact value of B_d^r. Indeed, a (very expensive) attack on MIMC_3 has been exhibited in [9], exploiting the fact that the number of rounds proposed by the designers is not sufficient for achieving a maximal algebraic degree. However, this weakness is based on a simple upper-bound on B_d^r and any gap between this bound and the exact value of the degree would decrease the complexity of the attack (or increase the number of rounds covered for a given complexity). Our aim is therefore to determine the exact value of B_d^r, or equivalently the minimal complexity of any attack based on higher-order differentials as in [9].

A First Observation. A pattern of particular interest to us is what we call a *plateau*. To understand what it corresponds to, let us consider a simple example. For any input x, the output of the composition of the first two rounds is

$$(x^3 + c_1)^3 + c_2 = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3 + c_2 \ . \tag{1}$$

We deduce that this composition is quadratic as its algebraic degree is equal to $\max\{\mathrm{wt}(i),\ i \in \{0, 3, 6, 9\}\} = 2$. It is counter-intuitive: we would expect the algebraic degree to increase when a non-affine function is iterated.

Definition 3 (Plateau). *We say that there is a* plateau *whenever* $B_d^r = B_d^{r-1}$.

Since $(B_d^r)_{r\geq 1}$ is a non-decreasing sequence as proved later in Prop. 2, the existence and the frequency of plateaus are the most relevant elements when estimating the degree of MIMC_d after a large number of rounds.

Outline. Our work aims to provide a better understanding of these plateaus, first to identify them, and then to exploit them. In Sec. 2, we derive a simple method to generate the set of all exponents appearing in the univariate representation of $\mathsf{MIMC}_{3,c}[r]$ (Prop. 1). Then, we bound the algebraic degree of $\mathsf{MIMC}_{3,c}[r]$ in Sec. 3, and identify in Sec. 4 a sequence of exponents that reach the upper bound.

We then perform a similar analysis of two ciphers closely related to $\mathsf{MIMC}_{3,c}[r]$, namely its inverse and $\mathsf{MIMC}_{9,c}[r]$ (Sec. 5). Finally, in Sec. 6, we use our results on the algebraic degree of $\mathsf{MIMC}_{3,c}[r]$ to determine the best possible integral attacks, which slightly improve the first attacks presented by the designers in [9].

For the sake of compactness, the proofs are left out of this extended abstract.

2 Quantifying the Evolution of the Univariate Degree

In this section, we present a process that generates the set of all the exponents appearing in the univariate form of r rounds of MIMC_d (Prop. 1).

Recall that $\mathsf{MIMC}_{d,c}$ corresponds to the composition $F_{r-1} \circ \ldots \circ F_0$ where for any i, $0 \leq i < r$, $F_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $x \mapsto x^d \oplus c_{i+1}$, and the $c_{i+1} \in \mathbb{F}_{2^n}$ are arbitrary constants. Then, for the successive values of r, it is possible to recursively determine the list of monomials appearing in the univariate polynomial representing $\mathsf{MIMC}_{d,c}[r]$ for some c.

Proposition 1. *Let n and $d < 2^n-1$ be two positive integers such that $\gcd(d, 2^n-1) = 1$. Let $\mathcal{E}_r$ be the set of the exponents of all monomials appearing in the univariate polynomial $\mathsf{MIMC}_{d,c}[r]$ over $\mathbb{F}_{2^n}$ for at least one sequence c. Then, we have:*

$$\mathcal{E}_r = \{dj \bmod (2^n - 1) \textit{ where } j \preceq i,\ i \in \mathcal{E}_{r-1}\} ,$$

where, for x and y in $\mathbb{F}_2^n$, $y \preceq x$ means that $y_i \leq x_i$ for all i.

The maximum algebraic degree after r rounds, B_d^r, is then the maximal weight of the elements in $\mathcal{E}_r$. In particular, we have the following.

Proposition 2. *For any integer d, $(B_d^r)_{r\geq 1}$ is a non-decreasing sequence. Moreover, when d is odd, we have $\mathcal{E}_{r-1} \subseteq \mathcal{E}_r$, for all $r \geq 1$.*

By investigating exponents of $\mathcal{E}_r$, we can, for example, prove that there is always such a plateau between the first and second rounds for all d of the form $d = 2^k - 1$ for some k.

Proposition 3. *Let $F : x \mapsto x^d$ be a permutation of $\mathbb{F}_{2^n}$ where $d = 2^k - 1$, and $\gcd(k, n) = 1$, and let c be an arbitrary constant. Then, if $d^2 < 2^n - 1$, we have:*

$$\deg^a((x^d + c)^d) = \deg^a(F) .$$

Therefore, there is a plateau during the first two rounds, and actually, some other ones can be observed in the following rounds of MIMC_3, as seen on Figure 2 where we compare our result with the bound given in [9].

3 Bounding the Algebraic Degree of MIMC_3

We now mainly focus on the algebraic degree of MIMC_3 over $\mathbb{F}_{2^n}$, i.e., on the value of B_3^r. We also focus on the situation where the univariate degree of $\mathsf{MIMC}_3[r]$ does not exceed (2^n-1). Therefore, we implicitely assume in the rest of

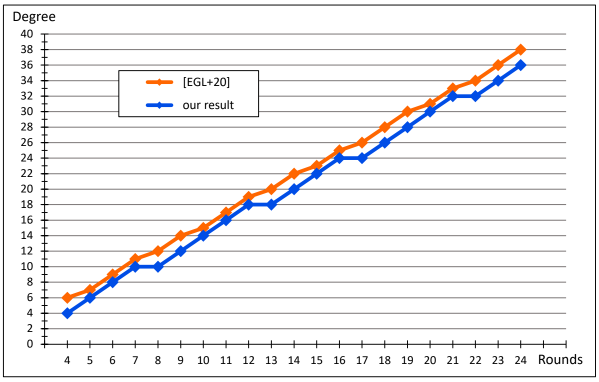

Fig. 2. Comparison of our result with previous work.

the paper that $n > \lfloor \log_2(3^r) \rfloor$. In this situation, the algebraic degree of r rounds of MIMC_3 is upper-bounded by $\lceil \log_2(3^r) \rceil = \lceil r \log_2 3 \rceil$, as observed in [9]. But this bound can be improved by showing that some exponents are missing in $\mathcal{E}_r$.

Lemma 1. *Let $\mathcal{E}_r$ be the set of exponents in the univariate form of $\mathsf{MIMC}_3[r]$, as defined in Prop. 1. Then, any $i \in \mathcal{E}_r$ satisfies*

$$i \bmod 8 \notin \{5, 7\} \ .$$

Proposition 4. *Let $k_r = \lfloor r \log_2 3 \rfloor$. For any $r \geq 4$, the algebraic degree after r rounds of MIMC_3 satisfies*

$$B_3^r \leq 2 \times \lceil k_r/2 - 1 \rceil \ .$$

Besides, if the univariate degree 3^r is lower than $2^n - 1$, then the monomial x^{3^r} appears in the polynomial. Since its coefficient is always 1, independently of the choice of the constants, this monomial never vanishes. This defines a trivial lower bound for B_3^r:

$$\mathrm{wt}(3^r) \ \leq \ B_3^r \ \leq \ 2 \times \lceil k_r/2 - 1 \rceil \ .$$

4 Exact Degree of MIMC_3

In this section, we show the tightness of the previously established bound. At this aim, we investigate the following conjecture, which exhibits a sequence of exponents in the univariate polynomial $\mathsf{MIMC}_{3,c}[r]$ for some c.

In what follows, $(k_r)_{r>0}$ and $(b_r)_{r>0}$ denote two sequences defined by

$$k_r = \lfloor r \log_2 3 \rfloor \ \text{ and } \ b_r = k_r \bmod 2 \ .$$

Conjecture 1. Let $(\omega_r)_{r>0}$ be the sequence of integers defined by

$$\omega_r = 2^{k_r} - \alpha_{b_r}, \quad \text{where} \quad \alpha_{b_r} = \begin{cases} 7 & \text{if } b_r = 0 \\ 5 & \text{if } b_r = 1 \ . \end{cases}$$

Then, for all $r > 0$, it holds that $\omega_r \in \mathcal{E}_r$.

While the most general case remains a conjecture at the time of writing, we show that the conjecture is true for all $r < 16265$, except for a few sporadic cases for which a proof still remains out of reach.

Theorem 1. *Conjecture 1 holds for all $r \in \{4, ..., 16265\}$ except maybe the values $r \in \mathcal{F}$, where*

$$\begin{aligned} \mathcal{F} &= \big((359 + R) \cup (665 + R) \cup (718 + R)\big) \backslash \mathcal{V} \\ \textit{with } R &= \{665\lambda + 53\mu,\ \ 0 \leq \lambda \leq 23, 0 \leq \mu \leq 5\} \\ \mathcal{V} &= \{359, 412, 518, 624, 665\} \ . \end{aligned}$$

To prove this theorem, we first need to investigate the sequence $(k_r)_{r>0}$.

Proposition 5. *Let $r \geq 3$, and let $(s_r)_{r>0}$ be the sequence of the* switches *from one parity to another for $(k_r)_{r>0}$, i.e. $s_1 = 0$ and $s_r = b_r \oplus b_{r-1}$. Then there exists $1 \leq \ell < r$ such that*

$$k_r - k_{r-\ell} = k_\ell$$

if and only if $(s_1 \dots s_r)$ is not a palindrome, i.e. if there exists i, $0 \leq i < r$ such that $s_{r-i} \neq s_{i+1}$.

Then, we use two ingredients allowing us to show that $\omega_r \in \mathcal{E}_r$. The first is MILP-based and computationnally intensive. The second is an inductive algorithm establishing that $\omega_r \in \mathcal{E}_r$ using the knowledge that $\omega_{r-\ell} \in \mathcal{E}_{r-\ell}$ for some $\ell < r$, such that Prop. 5 is satisfied. (see Fig. 3).

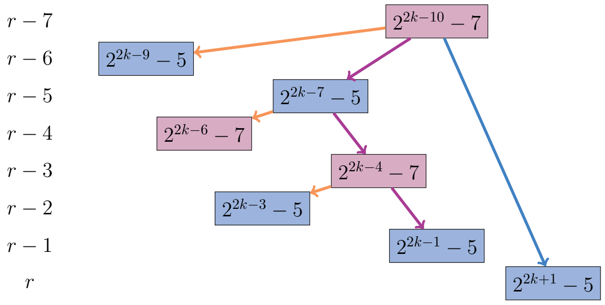

Fig. 3. Some steps of our inductive algorithm.

Although this second algorithm is more efficient than establishing the presence of exponents with the MILP-based algorithm for each round, we have identified two situations for which we need the MILP solver: when we have a palindromic sequence of (s_i), or when the value of ℓ satisfying Prop. 5 is too large. It follows that, with the MILP solver, Conjecture 1 can be proved for several more rounds. However, there are still some rounds that cannot be reached either by the recursive algorithm or by the MILP solver since the cost becomes too high to obtain a result.

Finally, we put together these results and algorithms using computer-assisted steps, to prove Theorem 1. Even if this method does not cover all the rounds, the number of rounds of MIMC_3 we are interested in is largely covered ($\simeq 80$).

As a consequence, we deduce the following corollary for Prop. 4.

Corollary 1. *Let $\boldsymbol{R} = \{4, ..., 16265\} \setminus \mathcal{F}$. For any $r \in \boldsymbol{R}$, the algebraic degree after r rounds of MIMC_3 satisfies:*

$$B_3^r = 2 \times \lceil k_r/2 - 1 \rceil \ .$$

We derive from Cor. 1 that there is a plateau between rounds r and $r+1$ when k_r is odd and k_{r+1} is even. Moreover, let $r \in \boldsymbol{R}$ s.t. $B_3^r = B_3^{r+1}$, we can also show that the next plateau is either $B_3^{r+4} = B_3^{r+5}$ or $B_3^{r+5} = B_3^{r+6}$.

It is worth noting that, for the sporadic cases $r \in \mathcal{F}$, we have both the upper bound of Prop. 4 and a lower bound derived from the fact that $(B_d^r)_{r \geq 1}$ is a non-decreasing sequence (Prop. 2). In most cases, there is a very small gap between the two values, e.g.

$$734 = B_3^{464} \leq B_3^{465} \leq 736 \ , \quad 902 = B_3^{570} \leq B_3^{571} \leq 904 \ .$$

5 Generalization to Other Permutations

5.1 Degree of MIMC_9 and the coefficients form

The set of exponents given by $\mathcal{E}_r$ is not always minimal, because the monomials coefficients can be cancelled for some constants choices, and this could cause the degree to drop at some rounds. The influence of the monomials coefficients can be observed for instance by comparing the algebraic degree of the transformation describing MIMC_9 and the one describing MIMC_3. Indeed, using x^9, as a round function, is equivalent to using x^3 with one constant out of two being equal to zero. On Fig. 4, we can thus see that the algebraic degree at round r for MIMC_9 is not always the algebraic degree at round $2r$ for MIMC_3.

Besides, we have already shown in Sec. 3 that for MIMC_3, the exponents equal to 5 and 7 modulo 8 are missing. For MIMC_d, where $d = 2^j + 1$ we have:

Proposition 6. *Let $\mathcal{E}_r$ be the set of exponents in the univariate form of $\mathsf{MIMC}_d[r]$, where $d = 2^j + 1$. Then, any $i \in \mathcal{E}_r$ satisfies: $i \bmod 2^j \in \{0, 1\}$.*

5.2 On the algebraic degree of MIMC_3^{-1}

We also study the algebraic degree of the inverse transformation. MIMC_3^{-1} is obtained by reversing the order of the round constants and by replacing the round function by $F^{-1}(x) = x^s$ where $s = (2^{n+1} - 1)/3$ (see e.g. [11, Prop. 5]). We first exhibit the following behavior, which can be observed on Fig. 5.

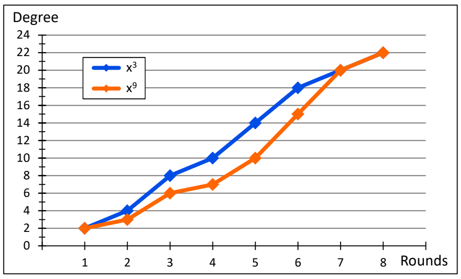

Fig. 4. Algebraic degree for r rounds of MIMC_9 and $2r$ rounds of MIMC_3 $(n = 23)$.

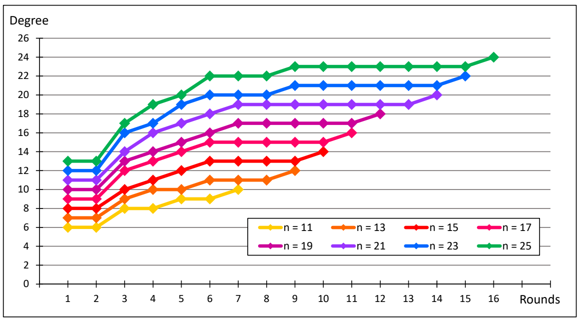

Fig. 5. Algebraic degree of MIMC_3^{-1}.

Proposition 7. *There is a plateau between the first two rounds of* MIMC_3^{-1}*:*

$$B_s^1 = B_s^2 = \frac{n+1}{2} \ .$$

Since the algebraic degree is already high in the first round, this plateau is counter-intuitive, and we explain this behavior by bounding the Hamming weight of the exponents $js \bmod 2^n - 1$. In Sec. 2, we have also proved that $B_d^1 = B_d^2$, when $d = 2^k - 1$. However, a similar plateau does not always exist for MIMC_d^{-1}, as observed for instance when $(n, d) = (11, 15)$.

Moreover, we also try to explain the large plateaus that increase with the size of the field on the last rounds. The degree of the round function being higher than x^3, studying the algebraic degree of MIMC_3^{-1} over the iterations is much more difficult. In [8] the authors show how the encryption degree influences the decryption degree, so that we can deduce the following corollary.

Corollary 2. *Let r_{n-i} be the first round of* MIMC_3^{-1} *where the algebraic degree reaches $n - i$. Then, we have:*

$$r_{n-i} \geq \left\lceil \frac{1}{\log_2 3} \left(2 \left\lceil \left\lceil \frac{n-1}{i} \right\rceil /2 - 1 \right\rceil + 3 \right) \right\rceil \ .$$

So in particular:

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

6 Higher-order Differential Attacks

Finally, we use our study of the algebraic degree to improve integral attacks presented in [9] and determine their best possible variants. High-order differential attacks exploit the low algebraic degree of a construction. Indeed, if the degree is sufficiently low then we can construct a 0-sum, using that $\bigoplus_{x \in \mathcal{V}} F(x) = 0$ for any affine subspace $\mathcal{V} \subset \mathbb{F}_{2^n}$, such that $\dim \mathcal{V} \geq \deg^a(F) + 1$.

Since a randomly selected permutation on $\mathbb{F}_2^n$ has maximum degree $n-1$ with a very high propability, an iterated cipher needs to reach the maximal algebraic degree in order to be indistinguishable from a random permutation. Besides we can also extend this distinguisher to a key-recovery attack using the rounds which are not covered by the 0-sum.

In Tab. 1, we compare our results with those by Eichlseder *et al.* [9] using the same notation: "KR" for Key-Recovery, "KK" for Known-Key distinguisher, and "SK" for Secret-Key distinguisher. Rather than proposing a new attack strategy, we show instead that their attack can cover one or two more rounds, thanks to our more precise evaluation of the algebraic degree. And we also derive from our results that our improved secret-key distinguishers are optimal in the sense that no such distinguisher based on the algebraic degree of the cipher can cover more rounds.

Type	n	Rounds	Time	Data	Source
SK	129	80	2^{128}XOR	2^{128}	[9]
	n	$\lceil \log_3(2^{n-1}-1) \rceil - 1$	2^{n-1}XOR	2^{n-1}	
	129	81	2^{128}XOR	2^{128}	New
	n	$\lceil \log_3 2^n \rceil - 1$	2^{n-1}XOR	2^{n-1}	
	129	81 (MIMC$_3$)	2^{127}XOR	2^{127}	New
	n	$\lceil \log_3 2^n \rceil - 1$ (MIMC$_3$)	2^{n-2}XOR	2^{n-2}	
	129	80 (MIMC$_3$)	2^{125}XOR	2^{125}	New
	n	$\lceil \log_3 2^n \rceil - 2$ (MIMC$_3$)	2^{n-2} or 2^{n-4}XOR	2^{n-2} or 2^{n-4}	
KK	129	160	-	2^{128}	[9]
	n	$2 \cdot \lceil \log_3(2^{n-1}-1) \rceil - 2$	-	2^{n-1}	
	129	162	-	2^{128}	New
	n	$2 \cdot \lceil \log_3 2^n \rceil - 2$	-	2^{n-1}	
KR	129	82	$2^{122.64}$	2^{128}	[9]
	n	$\lceil n \cdot \log_3 2 \rceil$	$2^{n-1-(\log_2 \lceil n \log_3 2 \rceil)}$ or $2^{n-(\log_2 \lceil n \log_3 2 \rceil)}$	2^{n-1}	
	129	82	$2^{121.64}$	2^{128}	New
	n	$\lceil n \cdot \log_3 2 \rceil$	$2^{n-1-(\log_2 \lceil n \log_3 2 \rceil)}$	2^{n-1}	

Table 1. Complexity of attacks on MIMC$_3$.

References

1. Albrecht, M.R., Cid, C., Grassi, L., Khovratovich, D., Lüftenegger, R., Rechberger, C., Schofnegger, M.: Algebraic cryptanalysis of STARK-friendly designs: Application to MARVELlous and MiMC. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part III. LNCS, vol. 11923, pp. 371–397. Springer, Heidelberg (Dec 2019)
2. Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schofnegger, M.: Feistel structures for MPC, and more. In: Sako, K., Schneider, S., Ryan, P.Y.A. (eds.) ESORICS 2019, Part II. LNCS, vol. 11736, pp. 151–171. Springer, Heidelberg (Sep 2019)
3. Albrecht, M.R., Grassi, L., Rechberger, C., Roy, A., Tiessen, T.: MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 191–219. Springer, Heidelberg (Dec 2016)
4. Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S., Szepieniec, A.: Design of symmetric-key primitives for advanced cryptographic protocols. IACR Trans. Symm. Cryptol. 2020(3), 1–45 (2020)
5. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive, Report 2018/046 (2018), https://eprint.iacr.org/2018/046
6. Ben-Sasson, E., Goldberg, L., Levit, D.: STARK friendly hash – survey and recommendation. Cryptology ePrint Archive, Report 2020/948 (2020), https://eprint.iacr.org/2020/948
7. Beyne, T., Canteaut, A., Dinur, I., Eichlseder, M., Leander, G., Leurent, G., Naya-Plasencia, M., Perrin, L., Sasaki, Y., Todo, Y., Wiemer, F.: Out of oddity - new cryptanalytic techniques against symmetric primitives optimized for integrity proof systems. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part III. LNCS, vol. 12172, pp. 299–328. Springer, Heidelberg (Aug 2020)
8. Boura, C., Canteaut, A.: On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$. IEEE Trans. Inf. Theory 59(1), 691–702 (2013)
9. Eichlseder, M., Grassi, L., Lüftenegger, R., Øygarden, M., Rechberger, C., Schofnegger, M., Wang, Q.: An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC. In: Advances in Cryptology ASIACRYPT 2020. pp. 477–506. Springer (2020)
10. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE'94. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (Dec 1995)
11. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT'93. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (May 1994)