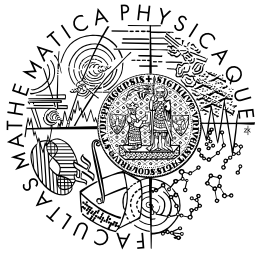

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Berenika Richterová

Cryptographic primitives in odd characteristic

Department of Algebra

Supervisor of the bachelor thesis: Dr. rer. nat. Faruk Göloglu

Study programme: Mathematics for Information Technologies

Study branch: Mathematics for Information Technologies

Prague 2022

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Author's signature

Dedication. To the thesis supervisor Dr. rer. nat. Faruk Gölogluu.

Title: Cryptographic primitives in odd characteristic

Author: Berenika Richterová

Department: Department of Algebra

Supervisor: Dr. rer. nat. Faruk Gölogl u, Department of Algebra

Abstract: In the thesis, we focus on the cryptanalytic techniques that can be used against the cryptographic primitives operating over odd characteristic finite fields. We introduce the GMiMC permutation, which belongs to such primitives. We describe an integral attack and generalize a certain type of this attack to finite fields of any characteristic. We also explain the notion of an impossible differential attack and then apply both the integral and the impossible differential attack to the GMiMC permutation.

Keywords: cryptanalysis, finite fields

Contents

Introduction

The majority of the symmetric cryptographic primitives operate over a finite field with a binary characteristic. Also most of the cryptanalysis techniques used against the symmetric primitives are based on binary finite fields and cannot be always straightforwardly applied to the case of a odd characteristic finite field. However, odd characteristic finite fields are recently also used for certain cryptographic primitives in the context of applications such as zero-knowledge proof systems (for instance STARKs).

In the thesis, based on Beyne et al. [2020] we analyze a permutation based on $\text{GMiMC}_{\text{erf}}$, which is a cipher designed to work over both binary and odd characteristic finite fields. We provide the description of the permutation as well as the necessary mathematical and cryptographic definitions and background. We describe an integral attack and then generalize this attack to the finite field of any characteristic. We also provide a formal explanation of the property used in integral attacks in binary characteristic, which is based on the theory presented in Lai [1994]. We apply the generalized attack to $\text{GMiMC}_{\text{erf}}$. In the last chapter of the thesis, we focus on a description of an impossible differential attack and show two versions of such attack against $\text{GMiMC}_{\text{erf}}$.

1. Preliminaries

In this chapter, we provide the mathematical notation used in the thesis, as well as important but more basic definitions and lemmas. In Section 1.2, we provide a cryptographic background of the topic of the thesis.

1.1 Notation and basics

Definition 1. *For a field F, we define* the characteristic of F *as a smallest $n \in \mathbb{N}$ such that*

$$\underbrace{1 + \cdots + 1}_{n} = 0$$

in F, if it exists. Otherwise, we define it as 0. *We write it* $\mathrm{char}(F)$.

Remark. It can be observed that every finite field is of positive characteristic. By field axioms, we have that the characteristic of a finite field is a prime. By algebra, we obtain that a number of elements of any finite field is a prime power. We also have that for every prime power, there exists a finite field with such number of elements. Moreover, by algebra we have that every finite field is unique up to isomorphism.

Notation.

- *In the thesis, we assume $k \in \mathbb{N}$.*
- *We denote by $\mathbb{F}_q$ a finite field with $q = p^s$ elements, for some prime p and $s \in \mathbb{N}$.*
- *By bold lowercase letters, we denote the row vectors. For instance by $\boldsymbol{x}$, we denote a vector of variables such that $\boldsymbol{x} = (x_1, \ldots, x_k)$ for some $k \in \mathbb{N}$.*
- *We denote by $\sqcup$ the disjoint union of two sets.*

1.1.1 Functions and polynomials over a finite field

In this section, we provide a formal description of an important connection between functions from $\mathbb{F}_q^k$ to $\mathbb{F}_q$ and polynomials in k variables. This connection is analogous to the connection of Boolean functions, that is to say functions from $\mathbb{F}_2^k$ to $\mathbb{F}_2$, which are in cryptanalysis widely analyzed, and polynomials over $\mathbb{F}_2$. In regard to the topic of the thesis which contains functions over $\mathbb{F}_q^k \to \mathbb{F}_q$ for a finite field of any characteristic, we find important to explicitly state the following lemmas and definitions. Lemma 2 and Lemma 3 are straightforward generalizations of their binary versions in Bashir [a]. Since the corresponding proofs directly follow the original proofs, we do not include them in the thesis. Note that we will refer to the following connection throughout the entire thesis.

Lemma 1. *For any function $f \colon \mathbb{F}_q^k \to \mathbb{F}_q$ there exists a polynomial P in the ring $\mathbb{F}_q[x_1, \ldots, x_k]/(x_1^q - x_1, \ldots, x_k^q - x_k)$, such that for all $\boldsymbol{v} = (v_1, \ldots, v_k) \in \mathbb{F}_q^k$ we have $P(\boldsymbol{v}) = f(\boldsymbol{v})$.*

Proof. We prove this by using a generalization of the Lagrange interpolating polynomial. For every $u_i \in \mathbb{F}_q$, let us set

$$p_{u_i}(x_i) = \prod_{\substack{a \in \mathbb{F}_q \\ a \neq v_i}} \frac{x_i - a}{u_i - a}.$$

It is clear that $p_{u_i}(w_i) = \delta_{u_i w_i}$, where $\delta_{u_i w_i}$ is Kronecker delta, that is to say a function with two arguments that gives 1 if the arguments are equal and 0 otherwise. For every $\boldsymbol{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$, set

$$p_{\boldsymbol{u}}(\boldsymbol{x}) = \prod_{i=1}^{k} p_{u_i}(x_i).$$

It holds for all $\boldsymbol{w} \in \mathbb{F}_q^k$ that $p_{\boldsymbol{u}}(\boldsymbol{w}) = \delta_{\boldsymbol{u}\boldsymbol{w}}$. Then

$$P(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_q^k} p_{\boldsymbol{u}}(\boldsymbol{x}) \cdot f(\boldsymbol{u})$$

is a polynomial in $x_1, \ldots, x_k$ of degree at most $q - 1$ in each variable. For all $\boldsymbol{v} \in \mathbb{F}_q^k$, we get $P(\boldsymbol{v}) = f(\boldsymbol{v})$. □

Lemma 2. *Let R_q^k denote a ring of functions from $\mathbb{F}_q^k$ to $\mathbb{F}_q$ with two operations defined for any $f, g \in R_q^k$ as follows*

$$\forall \boldsymbol{v} \in \mathbb{F}_q^k \colon (f + g)(\boldsymbol{v}) = f(\boldsymbol{v}) + g(\boldsymbol{v}),$$
$$(fg)(\boldsymbol{v}) = f(\boldsymbol{v})g(\boldsymbol{v})$$

Then

$$R_q^k \cong \mathbb{F}_q[x_1, \ldots, x_k]/(x_1^q - x_1, \ldots, x_k^q - x_k).$$

From Lemma 2 follows that one can view functions from the ring R_q^k and above described polynomials as the same objects. We now introduce the algebraic degree of a mapping $F \colon \mathbb{F}_q^k \to \mathbb{F}_q$ and the algebraic normal form of F. These notions are again analogous to the ones regarding Boolean functions.

Definition 2. *Consider a mapping $F \colon \mathbb{F}_q^k \to \mathbb{F}_q$.*

- *We define the* algebraic normal form of F *as a polynomial $P \in \mathbb{F}_q[x_1, \ldots, x_k]/(x_1^q - x_1, \ldots, x_k^q - x_k)$ of the form*

  $$P(\boldsymbol{x}) = \sum_{\boldsymbol{u}=(u_1,\ldots,u_k) \in \{0,\ldots,q-1\}^k} a_{\boldsymbol{u}} \prod_{i=1}^{k} x_i^{u_i}$$

  for some $a_{\boldsymbol{u}} \in \mathbb{F}_q$ such that

  $$\forall \boldsymbol{v} \in \mathbb{F}_q^k : F(\boldsymbol{v}) = P(\boldsymbol{v}).$$

  We denote it by $\mathrm{ANF}(F)$.

- *We define the* algebraic degree of F *as*

  $$\deg(F) = \begin{cases} -1 & \text{if } F(\boldsymbol{v}) = 0 \text{ for all } \boldsymbol{v} \in \mathbb{F}_q^k, \\ \max\limits_{\substack{\boldsymbol{u} \in \{0,\ldots,q-1\}^k \\ \text{such that } a_{\boldsymbol{u}} \neq 0}} \sum\limits_{i=1}^{k} u_i & \text{otherwise.} \end{cases}$$

- *We define the* algebraic degree of F in x_i *as*

$$\deg_{x_i}(F) = \begin{cases} -1 & \text{if } F(v) = 0 \text{ for all } v \in \mathbb{F}_q, \\ \max\limits_{\substack{\boldsymbol{u} \in \{0,\ldots,q-1\}^k \\ \text{such that } a_{\boldsymbol{u}} \neq 0}} u_i & \text{otherwise.} \end{cases}$$

Remark. For a function $F\colon \mathbb{F}_q^k \to \mathbb{F}_q$, we have by definition that $-1 \leq \deg(F) \leq k(q-1)$.

Lemma 3. *The algebraic degree of $F\colon \mathbb{F}_q^k \to \mathbb{F}_q$ is invariant under the affine permutation.*

1.2 Cryptographic background

In order to formally describe the topic of the thesis, we provide in this sections some important cryptographic definitions from Bashir [b].

1.2.1 Symmetric ciphers

Definition 3. *We define the* symmetric cipher *as a quintuple $\mathcal{S} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, e, d)$, for $\mathcal{P}$ a finite set of plaintexts, $\mathcal{C}$ a finite set of ciphertexts, $\mathcal{K}$ a finite set of keys and the functions $e\colon \mathcal{P} \times \mathcal{K} \to \mathcal{C}$ and $d\colon \mathcal{C} \times \mathcal{K} \to \mathcal{P}$ such that*

$$\forall k \in \mathcal{K}\ \forall m \in \mathcal{P} : d(e(m,k),k) = m.$$

For every $k \in \mathcal{K}$, we denote

$$\begin{aligned} e_k\colon \mathcal{P} &\to \mathcal{C} \\ m &\mapsto e(m,k) \end{aligned}$$

and

$$\begin{aligned} d_k\colon \mathcal{C} &\to \mathcal{P} \\ c &\mapsto d(c,k). \end{aligned}$$

Then we have for all $k \in \mathcal{K}$ that $d_k \circ e_k = \mathrm{id}_{\mathcal{P}}$. We call e an encryption function *and d a* decryption function.

Definition 4. *We define the* endomorphic cipher *$\mathcal{S}$ as a symmetric cipher with $\mathcal{P} = \mathcal{C}$ and $d_k = e_k^{-1}$ for all $k \in \mathcal{K}$. We write $\mathcal{S} = (\mathcal{P}, \mathcal{K}, e)$.*

Definition 5. *Let $\mathcal{S}' = (\mathcal{P}, \mathcal{K}', e')$ and $\mathcal{S} = (\mathcal{P}, \mathcal{K}, e)$ be two endomorphic ciphers and $n \in \mathbb{N}$. Consider a mapping $\mathcal{S}' \to \mathcal{S}$ determined by a mapping*

$$\begin{aligned} t\colon \mathcal{K}' &\to \mathcal{K}^N \\ k_M &\mapsto (k_1, \ldots, k_N) \end{aligned}$$

and $e'_k = e_{k_N} \circ \ldots \circ e_{k_1}$. We then call $\mathcal{S}'$ an iterative cipher*, $\mathcal{S}$ a* round *of $\mathcal{S}'$, t a* key schedule*, k_M a* master key *and k_i the i*th round key*.

1.2.2 Feistel networks

A Feistel network is a design model commonly used for construction of iterative symmetric block ciphers (see for instance Biryukov [2005a]). The idea of encryption by this model for an input pair of a plaintext and a key k_M is iterating certain number of rounds that are described as follows.

First, an input vector $\boldsymbol{v} \in \mathbb{F}_2^t$ of a round of the Feistel network is divided into two parts $\boldsymbol{d_1} \in \mathbb{F}_2^{t/2}$ and $\boldsymbol{d_2} \in \mathbb{F}_2^{t/2}$, called branches. Let us denote by $p_l(v, j)$ a projection on the first $1 \leq j \leq t$ coordinates of the vector $\boldsymbol{v} = (v_1, \ldots, v_t)$, i.e. $p_l(\boldsymbol{v}, j) = (v_1, \ldots, v_m)$. Similarly, let $p_r(\boldsymbol{v}, j) = (v_{t-j+1}, \ldots, v_t)$ denote a projection on the last j coordinates of $\boldsymbol{v}$. Then, let $\boldsymbol{d_1} = p_l(\boldsymbol{v}, t/2)$, $\boldsymbol{d_2} = p_r(\boldsymbol{v}, t/2)$ and we denote by $\boldsymbol{d_1} \,||\, \boldsymbol{d_2}$ a concatenation of $\boldsymbol{d_1}$ and $\boldsymbol{d_2}$. By this notation, we have $\boldsymbol{v} = \boldsymbol{d_1} \,||\, \boldsymbol{d_2}$. One of the branches then serves as an input of a round function. The round function f is a function that in the ith round takes $\boldsymbol{d_1}$ and a round key k_i and returns an output $f(\boldsymbol{d}_1, k_i)$ of the same length as $\boldsymbol{d_1}$. The image of the round function is then added to the second branch and the branches then swap.

Together, the plaintext is encrypted by a fixed number of these rounds, in the ith round under the round-key k_i. The round-keys are obtained from the key schedule, which derives them from the master-key k_M.

We can describe the ith round of Feistel network graphically in Figure 1.1 and formally for $\boldsymbol{v} \in \mathbb{F}_2^t$ as

$$\mathcal{R}_i \colon \boldsymbol{v} \mapsto \Big(p_r(\boldsymbol{v}, t/2) + f(p_l(\boldsymbol{v}, t/2), k_i) \Big) \,||\, p_l(\boldsymbol{v}, t/2).$$

The round of the Feistel can be also descrbed The advantage of the design of the Feistel network is the fact that there exists an inverse of the round regardless of the round function being invertible. It is easily seen that the inverse of the ith round is as follows

$$\mathcal{R}_i^{-1} \colon \boldsymbol{v} \mapsto p_r(\boldsymbol{v}, t/2) \,||\, \Big(p_l(\boldsymbol{v}, t/2) + f(p_r(\boldsymbol{v}, t/2), k_i) \Big).$$

In general, the Feistel network can operate over $\mathbb{F}_q$, a finite field of any characteristic, and the lengths of $\boldsymbol{d_1}$ and $\boldsymbol{d_2}$ do not have to be equal (Schneier and Kelsey [1996]). We then call such a network unbalanced and formally describe the ith round as

$$\mathcal{R}_i \colon \boldsymbol{v} \mapsto \Big(p_r(\boldsymbol{v}, t-j) + f(p_l(\boldsymbol{v}, j), k_i) \Big) \,||\, p_l(\boldsymbol{v}, j)$$

for $\boldsymbol{v} \in \mathbb{F}_q^k$, some $1 \leq j \leq t-1$ and a round function $f \colon \mathbb{F}_q^j \times \mathcal{K} \to \mathbb{F}_q^{t-j}$ for a set of the round keys $\mathcal{K}$. An inverse of the ith round of this unbalanced Feistel network is as follows

$$\mathcal{R}^{-1} \colon \boldsymbol{v} \mapsto p_r(\boldsymbol{v}, j) \,||\, \Big(p_l(\boldsymbol{v}, t-j) - f(p_r(\boldsymbol{v}, j), k_i) \Big).$$

1.2.3 GMiMC

GMiMC is a family of symmetric block ciphers, introduced in Albrecht et al. [2019], that use different types of the Feistel network in their construction. They operate over a field $\mathbb{F}_q$ and implement a cube mapping over $\mathbb{F}_q$ as a round function.

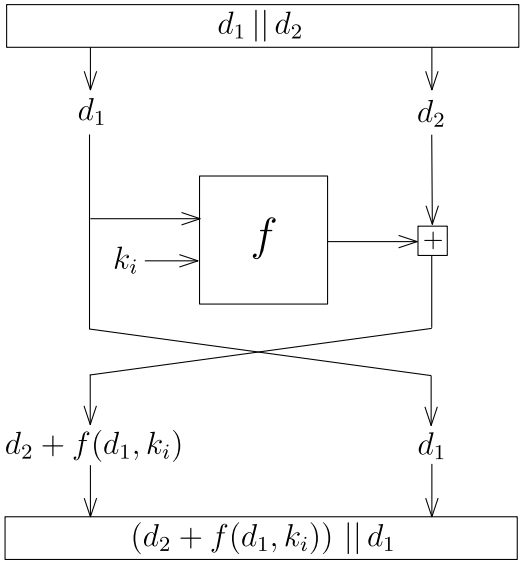

Figure 1.1: The ith round of a Feistel network.

Remark. We note that in the case of $\mathrm{char}(\mathbb{F}_q) = 3$, the mapping $x \mapsto x^3$ over $\mathbb{F}_q$ is by algebra an $\mathbb{F}_3$-automorphism. We can observe that the mapping $x \mapsto x^3$ is linear in this vector space. Thus, the mapping $x \mapsto x^3$ is not appropriate in characteristic 3 for cryptographic applications.

In what follows, we will consider one specific variant from the GMiMC family, called $\mathrm{GMiMC}_{\mathrm{erf}}$. As described in Albrecht et al. [2019], $\mathrm{GMiMC}_{\mathrm{erf}}$ operates over $\mathbb{F}_p$ or $\mathbb{F}_{2^s}$ for some p a prime and some $s \in \mathbb{N}$. In the thesis, we consider this variant over a general finite field $\mathbb{F}_q$ of any characteristic with the exception of $\mathrm{char}(\mathbb{F}_q) = 3$ because of the remark above. We also do not consider $\mathbb{F}_2$ since over this field we have that $x \mapsto x^3$ and $x \mapsto x$ are the same mappings. We denote by t the length of plaintexts and ciphertexts of $\mathrm{GMiMC}_{\mathrm{erf}}$. The set of plaintexts is then $\mathbb{F}_q^t$, the set of ciphertexts is $\mathbb{F}_q^t$ and the set of master-keys is $\mathbb{F}_q$. $\mathrm{GMiMC}_{\mathrm{erf}}$ is based on the unbalanced Feistel network with the ith round as follows

$$\mathcal{R}_i \colon \boldsymbol{v} \mapsto \Big((v_2, \ldots, v_t) + f(v_1, k_i) \Big) \,||\, v_1$$

for $\boldsymbol{v} = (v_1, \ldots, v_t) \in \mathbb{F}_q^t$ and a round function

$$\begin{aligned} f \colon \mathbb{F}_q \times \mathbb{F}_q &\to \mathbb{F}_q^{t-1} \\ (x, k_i) &\mapsto \Big((x + k_i)^3, \ldots, (x + k_i)^3 \Big) . \end{aligned}$$

We can rewrite the ith round of the Feistel network simply as

$$\mathcal{R}_i \colon \boldsymbol{v} \mapsto \Big(v_2 + (v_1 + k_i)^3, \ldots, v_t + (v_1 + k_i)^3, v_1 \Big) .$$

We will refer to the function

$$(v_1, k_i) \mapsto (v_1 + k_i)^3$$

as the *S-box*.

Encryption by $\text{GMiMC}_{\text{erf}}$ then consists of a fixed number of rounds of the Feistel network. For each round, the round-key $k_i \in \mathbb{F}_q$ is derived from the master key $k_M \in \mathbb{F}_q$ simply as

$$k_i = k_M + c_i,$$

where $c_i \in \mathbb{F}_q$ is a round constant.

Since each round of the Feistel network is invertible, the whole network is also invertible. Thus, if we replace the round-keys $k_i \in \mathbb{F}_q, i \geq 1$ by fixed independent and randomly chosen round-constants $\text{RC}_i \in \mathbb{F}_q, i \geq 1$, we obtain a permutation on $\mathbb{F}_q^t$. For brevity, we will from now on denote the permutation based on $\text{GMiMC}_{\text{erf}}$ by GMiMC. We will refer to a round of the corresponding Feistel network as a round of GMiMC. By Round i (of GMiMC) for $i \geq 1$, we will mean the ith round of the Feistel network in $\text{GMiMC}_{\text{erf}}$.

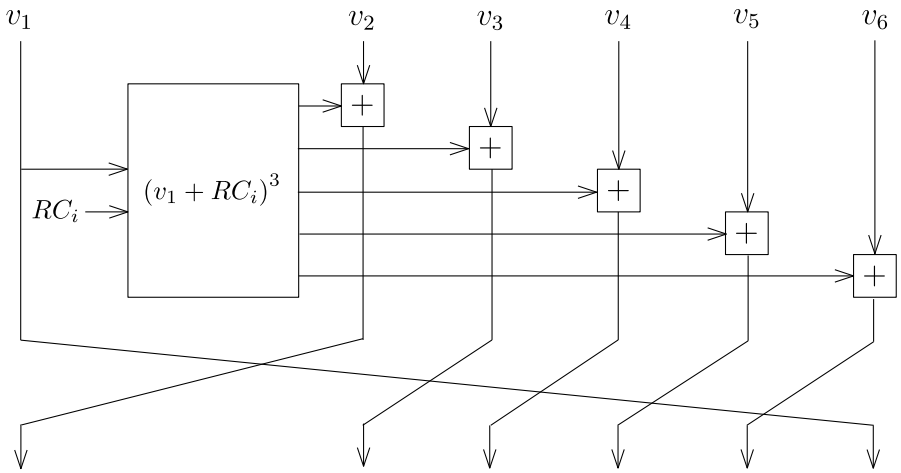

Figure 1.2: Round i of GMiMC permutation for $t = 6$.

1.2.4 Distinguishing attacks

The ciphers in the known-key setting are commonly used as permutations in the construction of the hash function, called the sponge construction. Even though it does not directly provide an attack on the hash function, being able to distinguish the *inner-permutation* from a random permutation is seen as a weakness of the hash function (Bertoni et al. [2008]). The distinguishing attack is a chosen plaintext attack model on the symmetric ciphers that finds an algorithm or a property of the cipher that can with some probability distinguish it from a random permutation. The algorithm or property is called the *distinguisher*. In the process of distinguishig when we yet do not know what the unidentified primitive is, we refer to it as a *black box*.

The complexity of the distinguisher refers to the amount of time or data that is needed to successfully verify if the property is satisfied. We choose for the unit of the time complexity to be an encryption of a plaintext.

The distinguishing attack on a concrete GMiMC is the attack that the thesis focuses on. In the next section, we describe a considered application of GMiMC permutation.

1.2.5 ZK-STARKs

ZK-STARKs (Zero-Knowledge Scalable Transparent ARguments of Knowledge) are *zero-knowledge proof systems*, which are systems that allow one party to verify the information of the second party without the necessity for the second party to reveal the information (Ben-Sasson et al. [2018]). These systems use collision-resistant hash functions. We want to consider hash functions that are *STARK-friendly*, that is to say they provide a certain level of security. In order to do that, we also need to analyze the inner-permutation of the considered hash function, in this case GMiMC permutation.

2. Integral attacks over finite fields of any characteristic

2.1 Integral attack

The umbrella term integral attack, first introduced by Knudsen and Wagner [2002], unifies several cryptanalytic techniques used against the symmetric-key primitives. In general, the integral attack is a chosen-plaintext attack that exploits a propagation of sums of values throughout the cipher. If the value of the sum after a certain number of encryption rounds can be predicted, then it is possible to recover key information.

Consider a symmetric iterative cipher $\mathcal{S} = (G^t, \mathcal{K}, e')$ for a finite commutative group $(G, +)$, where $G^t = \underbrace{G \times \cdots \times G}_{t}$. Let us denote the encryption function of one round by e. Then, $e' = e_{k_N} \circ \ldots \circ e_{k_1}$ for some $N \in \mathbb{N}$. Assume $N > 1$ and fix $i \in \{1, \ldots, t\}$. The idea of the attack is as follows. Suppose we find a multiset of plaintexts $V \subseteq G^t$ with a multiset of corresponding ciphetexts $W \subseteq G^t$ after $N - 1$ rounds such that we can predict the value

$$\Omega = \sum_{\boldsymbol{w}=(w_1,\ldots,w_t)\in W} w_i. \tag{2.1}$$

Then, we can guess the value k'_N of the Nth round key and compute

$$\boldsymbol{z}^{k'_N} = \sum_{\boldsymbol{v}\in V} e^{-1}_{k'_N} \circ e'(\boldsymbol{v}).$$

If

$$z_i^{k'_N} \neq \Omega$$

for $\boldsymbol{z}^{k'_N} = (z_1^{k'_N}, \ldots, z_t^{k'_N})$, we have a wrong value of the Nth round key.

For the attack, we usually prescribe the coordinates of the elements $\boldsymbol{v} \in V, \boldsymbol{v} = (v_1, \ldots, v_t)$ to be of one of the three following forms

$$\begin{aligned} v_i &= c_1, \quad \text{for all } \boldsymbol{v} \in V \\ \{v_i : \boldsymbol{v} \in V\} &= G \\ \sum_{\boldsymbol{v}\in V} v_i &= c_2, \end{aligned}$$

for some known and in advance fixed values $c_1, c_2 \in G$ and a fixed index $1 \leq i \leq t$. Each of these cases can be subsequently used in a prediction of Ω. In the first case, we fix a coordinate $1 \leq i \leq t$ and choose elements of V to be all equal in this coordinate. Assume that v_i serves as an input of a function $f\colon G \to G$ during the encryption. Then we have

$$\sum_{\boldsymbol{v}\in V} f(v_i) = |V|\, f(c_1).$$

In the second case, we choose for a fixed coordinate to vary in G, i.e. the ith coordinate of all elements of V differ. Then, if f is a bijection, all values $f(v_i) \in G$ differ. In particular,

$$\sum_{\boldsymbol{v}\in V} f(v_i) = \sum_{\boldsymbol{v}\in V} v_i.$$

In the setting where the round keys are replaced by the known round constants, a variant of the integral attack can be used to distinguish the primitive from a random permutation. Let us denote by π the black box. Suppose we can predict the value of Ω. Let z_i denote the value of the ith coordinate of $\sum_{\boldsymbol{v}\in V}\pi(\boldsymbol{v})$. If $z_i \neq \Omega$, then π is not the cipher. We can thus in this case distinguish $N-1$ rounds of $\mathcal{S}$. If Ω equals zero, we call the attack the *zero-sum distinguisher*.

Since we need to encrypt $|V|$ plaintexts in order to execute the attack, the time necessary for the $|V|$ summations is negligible in comparison. Therefore, the complexity of the attack depends on the cardinality of V, i.e. is $|V|$.

To determine the value of Ω for $G = \mathbb{F}_2$, the following property is usually exploited. For any multivariable function F over $\mathbb{F}_2$, we have that the sum of the images of F over elements of any affine subspace with the dimension larger than $\deg(F)$ equals zero. We provide a formal detailed explanation of this property in the following section.

2.2 Distinguishing property for a binary field

In majority of this section, we build a theoretical ground enabling the proof of the outlined property and we conclude the section with the very proof. The content of this section was first introduced in Lai [1994]. We expand the original proofs and in the case of Lemma 4, we provide our own.

Definition 6. *For a mapping* $F\colon \mathbb{F}_q^k \to \mathbb{F}_q$ *and an element* $\boldsymbol{a} \in \mathbb{F}_q^k$ *we define* the derivative of F at point $\boldsymbol{a}$ *as*

$$\partial_{\boldsymbol{a}}F(\boldsymbol{x}) = F(\boldsymbol{x}+\boldsymbol{a}) - F(\boldsymbol{a}).$$

For $i > 1$ *and* $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i) \in (\mathbb{F}_q^k)^i$ *we define* the i-th derivative of F at point $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i)$ *recursively as*

$$\partial^{(i)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_i}F(\boldsymbol{x}) = \partial_{\boldsymbol{a}_i}(\partial^{(i-1)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{i-1}}F(\boldsymbol{x})),$$

where

$$\partial^{(1)}_{\boldsymbol{a}_1}F(\boldsymbol{x}) = \partial_{\boldsymbol{a}_1}F(\boldsymbol{x}).$$

Lemma 4. *For any non-zero mapping* $F\colon \mathbb{F}_q^k \to \mathbb{F}_q$ *and any* $\boldsymbol{a} \in \mathbb{F}_q^k$,

$$\deg(\partial_{\boldsymbol{a}}F) \leq \deg(F) - 1.$$

Proof. Consider such a mapping F and some $\boldsymbol{a} = (a_1, \ldots, a_k) \in \mathbb{F}_q^k$. Set $d = \deg(F)$. Let us denote by Lemma 2

$$F(\boldsymbol{x}) = \sum_{\substack{i_1,\ldots,i_k\in\{0,\ldots,q-1\}\\ \text{such that}\sum_{j=1}^k i_j \leq d}} \alpha_{i_1,\ldots,i_k} x_1^{i_1}\ldots x_k^{i_k},$$

for some $\alpha_{i_1,\ldots,i_k} \in \mathbb{F}_q$. We compute

$$\begin{aligned}
F(\boldsymbol{x}+\boldsymbol{a}) &= \sum_{\substack{i_1,\ldots,i_k\in\{0,\ldots,q-1\}\\ \text{such that}\sum_{j=1}^{k} i_j\le d}} \alpha_{i_1,\ldots,i_k}(x_1+a_1)^{i_1}\ldots(x_k+a_k)^{i_k} \\
&= \sum_{\substack{i_1,\ldots,i_k\in\{0,\ldots,q-1\}\\ \text{such that}\sum_{j=1}^{k} i_j\le d}} \alpha_{i_1,\ldots,i_k}\left(x_1^{i_1}+\binom{i_1}{1}x_1^{i_1-1}a_1+\cdots+\binom{i_1}{i_1}a_1^{i_1}\right) \\
&\quad \ldots\left(x_k^{i_k}+\binom{i_k}{1}x_k^{i_k-1}a_k+\cdots+\binom{i_k}{i_k}a_k^{i_k}\right) \\
&= \sum_{\substack{i_1,\ldots,i_k\in\{0,\ldots,q-1\}\\ \text{such that}\sum_{j=1}^{k} i_j\le d}} \alpha_{i_1,\ldots,i_k}x_1^{i_1}\ldots x_k^{i_k} + g(\boldsymbol{x}) \\
&= F(\boldsymbol{x}) + g(\boldsymbol{x}),
\end{aligned}$$

where $g(\boldsymbol{x})$ is a polynomial in $x_1,\ldots,x_k$. It is easily seen that $\deg(g) < \deg(F)$. We obtain

$$\partial_{\boldsymbol{a}}F(\boldsymbol{x}) = F(\boldsymbol{x}+\boldsymbol{a}) - F(\boldsymbol{x}) = F(\boldsymbol{x}) + g(\boldsymbol{x}) - F(\boldsymbol{x}) = g(\boldsymbol{x}).$$

It follows

$$\deg(\partial_{\boldsymbol{a}}F) \le \deg(F) - 1.$$

□

Lemma 5. *For any mapping $F\colon \mathbb{F}_2^k \to \mathbb{F}_2$ and any linear subspace $V = \operatorname{span}\{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_i\} \le \mathbb{F}_2^k$ with $\dim(V) = i > 0$ we have,*

$$\partial^{(i)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_i}F(\boldsymbol{x}) = \sum_{\boldsymbol{c}\in V} F(\boldsymbol{x}+\boldsymbol{c}).$$

Proof. We prove it by induction. Let $i = 1$, then

$$\sum_{\boldsymbol{c}\in V} F(\boldsymbol{x}+\boldsymbol{c}) = F(\boldsymbol{x}+\boldsymbol{a}_1) + F(\boldsymbol{x}) = \partial_{\boldsymbol{a}_1}F(\boldsymbol{x}),$$

since we work with a binary finite field. Assume the formula holds for $i-1$, we will prove it for i. We have

$$\begin{aligned}
\partial^{(i)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_i}F(\boldsymbol{x}) &= \partial_{\boldsymbol{a}_i}\left(\partial^{(i-1)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{i-1}}F(\boldsymbol{x})\right) = \left(\partial^{(i-1)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{i-1}}F(\boldsymbol{x}+\boldsymbol{a}_i)\right) + \left(\partial^{(i-1)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{i-1}}F(\boldsymbol{x})\right) \\
&= \left(\sum_{\boldsymbol{c}\in\operatorname{span}\{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{i-1}\}} F(\boldsymbol{x}+\boldsymbol{a_i}+\boldsymbol{c})\right) + \left(\sum_{\boldsymbol{c}\in\operatorname{span}\{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{i-1}\}} F(\boldsymbol{x}+\boldsymbol{c})\right) \\
&= \sum_{\boldsymbol{c}\in V} F(\boldsymbol{x}+\boldsymbol{c}).
\end{aligned}$$

This follows from definition, inductive hypothesis and the fact that

$$\{\boldsymbol{c} \mid \boldsymbol{c}\in\operatorname{span}\{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{i-1}\}\} \sqcup \{\boldsymbol{c}+\boldsymbol{a}_i \mid \boldsymbol{c}\in\operatorname{span}\{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{i-1}\}\} = V.$$

□

Remark. Lemma 5 does not hold for a general $\mathbb{F}_q$. For instance, let $F\colon \mathbb{F}_3^2 \to \mathbb{F}_3$ be a mapping with

$$\mathrm{ANF}(F) = x_1 + x_2$$

in $\mathbb{F}_3[x_1, x_2]/(x_1^3 - x_1, x_2^3 - x_2)$ and $V = \mathrm{span}\{(1,0)\} \leq \mathbb{F}_3^2$. Then we have

$$\sum_{\boldsymbol{c}\in V} F(\boldsymbol{x}+\boldsymbol{c}) = (x_1+x_2) + (x_1+1+x_2) + (x_1+2+x_2) = 3x_1 + 3x_2 + 3 = 0$$

and

$$\partial_{(1,0)}F(\boldsymbol{x}) = F(\boldsymbol{x}+\boldsymbol{c}) - F(\boldsymbol{x}) = F(\boldsymbol{x}+(1,0)) - F(\boldsymbol{x}) = x_1+1+x_2-(x_1+x_2) = 1.$$

Finally, we formulate and prove the following distinguishing property.

Lemma 6. *For any mapping $F\colon \mathbb{F}_2^k \to \mathbb{F}_2$ and any affine subspace $V \subset \mathbb{F}_2^k$ with $\deg(F) < \dim(V)$, we have*

$$\sum_{\boldsymbol{v}\in V} F(\boldsymbol{v}) = 0.$$

Proof. Let us have a mapping F and an affine subspace V satisfying the assumptions. Set $d = \dim(V)$. Assume that $d > 0$. Then, there exists a linear subspace $U \leq \mathbb{F}_2^k$ and an element $\boldsymbol{\alpha} \in \mathbb{F}_2^k$ such that $V = \boldsymbol{\alpha} + U$, where $U = \mathrm{span}\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d\}$ for some $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d \in \mathbb{F}_2^k$. By Lemma 5, we obtain

$$\partial^{(d)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_d} F(\boldsymbol{x}) = \sum_{\boldsymbol{c}\in U} F(\boldsymbol{x}+\boldsymbol{c}) = \sum_{\boldsymbol{v}\in V} F(\boldsymbol{x}+\boldsymbol{v}+\boldsymbol{\alpha}).$$

It follows for all $\boldsymbol{v} \in V, \boldsymbol{v} = \boldsymbol{\alpha} + \boldsymbol{u}$ for some $\boldsymbol{u} \in U$,

$$\begin{aligned}\sum_{\boldsymbol{v}'\in V} F(\boldsymbol{v}+\boldsymbol{v}'+\boldsymbol{\alpha}) &= \sum_{\boldsymbol{y}\in U} F(\boldsymbol{\alpha}+\boldsymbol{u}+\boldsymbol{\alpha}+\boldsymbol{y}+\boldsymbol{\alpha}) = \sum_{\boldsymbol{y}\in U} F(\boldsymbol{\alpha}+\boldsymbol{u}+\boldsymbol{y}) \\ &= \sum_{\boldsymbol{w}\in U} F(\boldsymbol{\alpha}+\boldsymbol{w}) = \sum_{\boldsymbol{v}'\in V} F(\boldsymbol{v}').\end{aligned}$$

Lemma 4 and the assumption $\deg(F) - \dim(V) < 0$ then give

$$\deg\left(\partial^{(d)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_d} F\right) \leq \deg(F) - \dim(V) < 0.$$

We obtain $\partial^{(d)}_{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_d} F(\boldsymbol{x}) = 0$ and consequently,

$$\sum_{\boldsymbol{v}\in V} F(\boldsymbol{v}) = 0.$$

For $d = 0$, we have by the assumptions that $\deg(F) = -1$. Then F is a zero mapping and we have

$$\sum_{\boldsymbol{v}\in V} F(\boldsymbol{v}) = 0.$$

□

2.3 Generalization to finite fields of any characteristic

Since Lemma 5 does not hold in a general finite field, we obtain a distinguishing property that can be exploited only over $\mathbb{F}_2$. In this section, we describe a different distinguishing property, presented in Beyne et al. [2020], that can be used in a finite field of any characteristic. We also provide more details on some of the original proofs.

Proposition 7. *For any* $F\colon \mathbb{F}_q \to \mathbb{F}_q$ *with* $\deg(F) < q-1$*, we have*

$$\sum_{x\in\mathbb{F}_q} F(x) = 0.$$

Proof. Let $F\colon \mathbb{F}_q \to \mathbb{F}_q$ be such a mapping. By Lemma 2 and our assumption that $\deg(F) < q-1$, we can write

$$F(x) = \sum_{i=0}^{q-2} a_i x^i,$$

for some $a_0, \ldots, a_{q-2} \in \mathbb{F}_q$. It then suffices to show that for $1 \le i \le q-2$,

$$\sum_{x\in\mathbb{F}_q} x^i = 0.$$

Since $\mathbb{F}_q$ is a finite field, we have $c\,\mathbb{F}_q = \mathbb{F}_q$ for any $c \in \mathbb{F}_q^*$.

For $q = 2$, it is clear that

$$\sum_{x\in\mathbb{F}_2} F(x) = \sum_{x\in\mathbb{F}_2} a_0 = 2a_0 = 0.$$

Assume $q > 2$. Since a multiplicative group of the finite field $\mathbb{F}_q$ is cyclic, there exists an element $c \in \mathbb{F}_q^*$, such that c generates $\mathbb{F}_q^*$. For $q > 2$, it is evident that $c \neq 1$. Let us compute

$$\sum_{x\in\mathbb{F}_q} x^i = \sum_{x\in\mathbb{F}_q} (cx)^i = \sum_{x\in\mathbb{F}_q} c^i x^i = c^i \sum_{x\in\mathbb{F}_q} x^i.$$

If $\sum_{x\in\mathbb{F}_q} x^i = d \neq 0$, then there exists an inverse of d in $\mathbb{F}_q^*$ and it follows that $c^i = 1$. However, c as a generator of $\mathbb{F}_q^*$ is of order $q-1$, therefore $c^i \neq 1$, for $1 \le i \le q-2$. This yields

$$\sum_{x\in\mathbb{F}_q} x^i = 0.$$

We thus have

$$\sum_{x\in\mathbb{F}_q} F(x) = \sum_{x\in\mathbb{F}_q} \sum_{i=0}^{q-2} a_i x^i = 0 + \sum_{x\in\mathbb{F}_q} a_0 = q a_0 = 0.$$

□

This distinguishing property can be generalized to the multivariable functions as follows.

Corollary 8. *For any mapping* $F\colon \mathbb{F}_q^k \to \mathbb{F}_q$ *with* $\deg(F) < d(q-1)$ *and any affine subspace* $V \subseteq \mathbb{F}_q^k$ *with* $\dim(V) \geq d$*, we have*

$$\sum_{\boldsymbol{v} \in V} F(\boldsymbol{v}) = 0.$$

Proof. Consider a mapping F and an affine subspace V satisfying the assumptions. Let us set $\delta = \dim(V) \geq d$. Consider $I_\delta \leq \mathbb{F}_q^k$ a vector space generated by the first δ vectors of the canonical basis of $\mathbb{F}_q^k$. By simple linear algebra, there exists an affine permutation $A\colon I_\delta \to V$. We have

$$\sum_{\boldsymbol{v} \in V} F(\boldsymbol{v}) = \sum_{\boldsymbol{v} \in I_\delta} F \circ A^{-1}(\boldsymbol{v}) = \sum_{y_1,\ldots,y_\delta \in \mathbb{F}_q} (F \circ A^{-1})(y_1, \ldots, y_\delta, 0, \ldots, 0).$$

By Lemma 3, we have that $\deg(F \circ A^{-1}) = \deg(F) < d(q-1)$. Similarly to Proposition 7, it thus suffices to show that

$$\sum_{y_1,\ldots,y_\delta \in \mathbb{F}_q} y_1^{i_1} \ldots y_\delta^{i_\delta} = 0,$$

for all values of i_j satisfying $\sum_{j=1}^{\delta} i_j < d(q-1)$. Since $\delta \geq d$, there exists an exponent i_j such that $i_j < q-1$ and it follows by Proposition 7, $\sum_{y_j \in \mathbb{F}_q} y_j^{i_j} = 0$. Consequently, the sum above equals zero, which concludes the proof. □

We now consider summing over elements of a multiplicative subgroup of $\mathbb{F}_q$ and generalize Proposition 7.

Proposition 9. *Let* G *be a multiplicative subgroup of* $\mathbb{F}_q^*$*. For any* $F\colon \mathbb{F}_q \to \mathbb{F}_q$ *such that* $\deg(F) < |G|$*,*

$$\sum_{x \in G} F(x) - F(0) \cdot |G| = 0.$$

Proof. By Lemma 2, we can write

$$F(x) = \sum_{i=0}^{|G|-1} a_i x^i,$$

for some $a_0, \ldots, a_{|G|-1} \in \mathbb{F}_q$. Similarly to the proof of Proposition 7, we have that it is sufficient to show that

$$\sum_{x \in G} x^i = 0,$$

for $1 \leq i \leq |G| - 1$. By algebra, we have that every subgroup of a cyclic group is cyclic. As in the proof of Proposition 7, we obtain

$$\sum_{x \in G} x^i = \sum_{x \in G} c^i x^i = c^i \sum_{x \in G} x^i,$$

for $c \in G$ such that $G = \langle c \rangle_{\mathbb{F}_q}$. We follow the proof analogically and get

$$\sum_{x \in G} F(x) = \sum_{x \in G} \sum_{i=0}^{|G|-1} a_i x^i = 0 + \sum_{x \in G} a_0 = |G| \cdot a_0.$$

Since $a_0 = F(0)$, it follows

$$\sum_{x \in G} F(x) - |G| \cdot F(0) = 0.$$

□

3. Integral distinguishers on GMiMC

In this chapter, we describe a construction of the integral distinguishers on the GMiMC permutation, presented in Beyne et al. [2020]. The construction uses the generalized distinguishing properties from Chapter 2. When choosing the input set, we *saturate* one or more branches of the permutation. That means that on certain coordinates of the inputs we choose the values to vary in $\mathbb{F}_q$. The rest of the coordinates either depend on the value of the saturated coordinate or are constants in $\mathbb{F}_q$. It implies that the number of the saturated coordinates determines the cardinality of the input set and therefore the complexity of the distinguisher.

3.1 Saturating a single branch

First, we construct a zero-sum distinguisher with one saturated coordinate. We divide the construction in two parts - forward and backward direction - and get a distinguisher that covers in total $(4t - 6 + 2\lfloor \log_3(q-2) \rfloor)$ rounds of GMiMC. Since we saturate a single branch of the permutation, i.e. a single coordinate of the input vector varies in $\mathbb{F}_q$, the distinguisher has complexity q.

3.1.1 Forward direction

The construction will be based on a set of q inputs in the form

$$\mathcal{X}_0 = \{(\alpha_1, \alpha_2, \ldots, \alpha_{t-2}, x, f(x)) \mid x \in \mathbb{F}_q\},$$

where $\alpha_1, \ldots, \alpha_{t-2} \in \mathbb{F}_q$ are arbitrary constants and f is a function defined as follows

$$f(x) = -\left(x + \sum_{i=1}^{t-2} \beta_i + \mathrm{RC}_{t-1}\right)^3 - x - 2\sum_{i=1}^{t-2} \beta_i - \mathrm{RC}_{t-1} - \mathrm{RC}_t.$$

We define

$$\beta_1 = (\alpha_1 + \mathrm{RC}_1)^3$$

and for $i = 1, \ldots, t-3$ we define β_{i+1} recursively as

$$\beta_{i+1} = \left(\alpha_{i+1} + \sum_{j=1}^{i} \beta_j + \mathrm{RC}_{i+1}\right)^3.$$

For $i = 1, \ldots, t-2$, the value of β_i depends only on fixed values $\alpha_1, \ldots, \alpha_i$ and known round-constants $\mathrm{RC}_1, \ldots, \mathrm{RC}_i$, all β_i are thus constants in $\mathbb{F}_q$.

In contrast to Beyne et al. [2020], we implement a formal notation of the sets of the internal states of GMiMC. Since each coordinate of elements of the set $\mathcal{X}_0$ is an univariate polynomial in x, we can write

$$\mathcal{X}_0 = \{(\phi_0^{(1)}(x), \ldots, \phi_0^{(t)}(x)) \mid x \in \mathbb{F}_q\},$$

where by Lemma 2, $\phi_0^{(1)}, \ldots, \phi_0^{(t)}$ are elements of $\mathbb{F}_q[x]/(x^q - x)$. For $i \geq 1$, let us denote by

$$\mathcal{X}_i = \{(\phi_i^{(1)}(x), \ldots, \phi_i^{(t)}(x)) \mid x \in \mathbb{F}_q\},$$

where $\phi_i^{(j)}$ is an element of $\mathbb{F}_q[x]/(x^q - x)$, the set of outputs of i rounds of GMiMC permutation applied to $\mathcal{X}_0$. Let us further denote the vector function $(\phi_i^{(1)}, \ldots, \phi_i^{(t)})$ by Φ_i.

In the first part of the construction of the distinguisher, we monitor the transformation of the set $\mathcal{X}_0$ moving forward through rounds of GMiMC. Let us focus on the first $(t-2)$ rounds of GMiMC. Considering the design of GMiMC permutation, we can observe that in these rounds the value of the image of the S-box does not depend on the value of x. The image of the S-box in the first round is equal to $(\alpha_1 + \mathrm{RC}_1)^3$, which we previously denoted by β_1. This value is then added to all the other coordinates. After the first round we therefore obtain the following set of outputs

$$\mathcal{X}_1 = \{(\alpha_2 + \beta_1, \alpha_3 + \beta_1, \ldots, \alpha_{t-2} + \beta_1, x + \beta_1, f(x) + \beta_1, \alpha_1) \mid x \in \mathbb{F}_q\}.$$

We can see by definition of β_i for $1 \leq i \leq t-2$, that the image of the S-box in the i-th round corresponds exactly to β_i. This gives us the set of outputs of Round $(t-2)$ as follows

$$\mathcal{X}_{t-2} = \{(x + \sum_{i=1}^{t-2} \beta_i, f(x) + \sum_{i=1}^{t-2} \beta_i, \alpha_1 + \sum_{\substack{i=1 \\ i \neq 1}}^{t-2} \beta_i, \alpha_2 + \sum_{\substack{i=1 \\ i \neq 2}}^{t-2} \beta_i, \ldots, \alpha_{t-2} + \sum_{\substack{i=1 \\ i \neq t-2}}^{t-2} \beta_i) \mid x \in \mathbb{F}_q\}.$$

For brevity let $x' = x + \sum_{i=1}^{t-2} \beta_i$. Since $\phi_{t-2}^{(3)}, \ldots, \phi_{t-2}^{(t)}$ are constant functions, let us denote their image values by $\gamma_1, \ldots, \gamma_{t-2}$, respectively. Now $\phi_{t-2}^{(2)}(x)$ for $x \in \mathbb{F}_q$ can be written as follows

$$\begin{aligned}
\phi_{t-2}^{(2)}(x) &= f(x) + \sum_{i=1}^{t-2} \beta_i = f\left(x' - \sum_{i=1}^{t-2} \beta_i\right) + \sum_{i=1}^{t-2} \beta_i \\
&= -\left(x' - \sum_{i=1}^{t-2} \beta_i + \sum_{i=1}^{t-2} \beta_i + \mathrm{RC}_{t-1}\right)^3 - \left(x' - \sum_{i=1}^{t-2} \beta_i\right) - 2\sum_{i=1}^{t-2} \beta_i \\
&\quad - \mathrm{RC}_{t-1} - \mathrm{RC}_t + \sum_{i=1}^{t-2} \beta_i \\
&= -\left(x' + \mathrm{RC}_{t-1}\right)^3 - x' - \mathrm{RC}_{t-1} - \mathrm{RC}_t.
\end{aligned}$$

The derivation of x' from x is a translation, therefore it is a bijection on $\mathbb{F}_q$ and we can thus rewrite the set $\mathcal{X}_{t-2}$ depending on x' in the form

$$\mathcal{X}_{t-2} = \{(x', -\left(x' + \mathrm{RC}_{t-1}\right)^3 - x' - \mathrm{RC}_{t-1} - \mathrm{RC}_t, \gamma_1, \ldots, \gamma_{t-2}) \mid x' \in \mathbb{F}_q\}.$$

This set is then transformed after one more round into

$$\begin{aligned}
\mathcal{X}_{t-1} = \{(&-x' - \mathrm{RC}_{t-1} - \mathrm{RC}_t, \\
&\gamma_1 + \left(x' + \mathrm{RC}_{t-1}\right)^3, \ldots, \gamma_{t-2} + \left(x' + \mathrm{RC}_{t-1}\right)^3, x') \mid x' \in \mathbb{F}_q.\}
\end{aligned}$$

The image of the S-box in Round t equals

$$\left(\phi_{t-1}^{(1)}(x) + \mathrm{RC}_t\right)^3 = (-x' - \mathrm{RC}_{t-1} - \mathrm{RC}_t + \mathrm{RC}_t)^3 = -(x' + \mathrm{RC}_{t-1})^3,$$

we therefore obtain

$$\mathcal{X}_t = \{(\gamma_1, \ldots, \gamma_{t-2}, x' - (x' + \mathrm{RC}_{t-1})^3, -x' - \mathrm{RC}_{t-1} - \mathrm{RC}_t) \mid x' \in \mathbb{F}_q\}.$$

Fixed values $\gamma_1, \ldots, \gamma_{t-2}$ do not depend on the value of x' and therefore the images of the S-box in the following $(t-2)$ rounds are constants. It follows that the set of outputs after $t + (t-2) = (2t-2)$ rounds is of the form

$$\mathcal{X}_{2t-2} = \{(x' - (x' + \mathrm{RC}_{t-1})^3 + \delta_1, -x' + \delta_2, \delta_3, \ldots, \delta_t) \mid x' \in \mathbb{F}_q\},$$

for some constants $\delta_1, \ldots, \delta_t \in \mathbb{F}_q$.

Now, we observe that each coordinate of Φ_{2t-2} is of degree at most 3. It follows that the coordinates of $\Phi_{(2t-2)+1}$ are of degree at most 3^2, since the first coordinate of Φ_{2t-2} serves as an input to the cube mapping in a round of GMiMC. In the same manner, we can give an upper bound on the degree of the coordinates of $\Phi_{(2t-2)+r}$, that is 3^{1+r}. By Proposition 7, for each coordinate function $\sum \phi_{(2t-2)+r}^{(i)}(x')$ sums to zero when x' varies in $\mathbb{F}_q$ if the degree of the coordinate is less then $q-1$. We thus can use the distinguishing property from Proposition 7 for $(2t-2)+r$ rounds of GMiMC if $3^{1+r} < q-1$, i.e., if $r \leq \lfloor \log_3(q-2) \rfloor - 1$. We choose the maximal such r and set $r = \lfloor \log_3(q-2) \rfloor - 1$.

We obtain a zero-sum distinguisher on altogether $(2t-2)+r = (2t-3+\lfloor \log_3(q-2) \rfloor)$ rounds of GMiMC with the distinguishing property

$$\forall i \in \{1, \ldots, t\} \colon \sum_{x' \in \mathbb{F}_q} \phi_{2t-2+r}^{(i)}(x') = 0.$$

The constructed distinguisher can be further extended in the forward direction. We exploit the following lemma presented in Beyne et al. [2020].

Lemma 10. *Let us denote by $(x_1, \ldots, x_t)$ and $(y_1, \ldots, y_t)$ the input and output of $(t-1)$ rounds of GMiMC, respectively. It follows*

$$\sum_{i=2}^{t} y_i - (t-2)y_1 = \sum_{i=1}^{t-1} x_i - (t-2)x_t.$$

Proof. Let us denote by $(x_1^m, \ldots, x_t^m)$ the input of the mth round of GMiMC. For $m > 1$ and any $i, j \in \{1, \ldots, t-1\}$ we have by the design of GMiMC

$$x_i^m = x_{i+1}^{m-1} + \left(x_j^m - x_{j+1}^{m-1}\right)$$

and

$$x_t^m = x_1^{m-1}.$$

Then for any $j \in \{1, \ldots, t-1\}$ we have

$$\begin{aligned}\sum_{i=1}^{t} x_i^m - (t-1)x_j^m = \sum_{i=1}^{t-1} \left(x_i^m - x_j^m\right) + x_t^m &= \sum_{i=1}^{t-1} \left(x_{i+1}^{m-1} - x_{j+1}^{m-1}\right) + x_1^{m-1} \\ &= \sum_{i=1}^{t} x_i^{m-1} - (t-1)x_{j+1}^{m-1}.\end{aligned}$$

By applying

$$\sum_{i=1}^{t} x_i^m - (t-1)x_j^m = \sum_{i=1}^{t} x_i^{m-1} - (t-1)x_{j+1}^{m-1}$$

$(t-1)$ times, we obtain the requested equality. □

Lemma 10 implies that we can add $(t-1)$ more rounds to the previous distinguisher as follows. Let us set

$$R = (2t - 3 + \lfloor \log_3(q-2) \rfloor) + (t-1) = 3t - 4 + \lfloor \log_3(q-2) \rfloor .$$

By Lemma 10 for all $x \in \mathbb{F}_q$, elements of $\mathcal{X}_R$ satisfy the following property

$$\sum_{i=2}^{t} \phi_R^{(i)}(x) - (t-2)\phi_R^{(1)}(x) = \sum_{i=1}^{t-1} \phi_{2t-2+r}^{(i)}(x) - (t-2)\phi_{2t-2+r}^{(t)}(x).$$

We have

$$\sum_{x\in\mathbb{F}_q} \left(\sum_{i=1}^{t-1} \phi_{2t-2+r}^{(i)}(x) - (t-2)\phi_{2t-2+r}^{(t)}(x) \right) = \sum_{i=1}^{t-1} \sum_{x\in\mathbb{F}_q} \phi_{2t-2+r}^{(i)}(x) - (t-2) \sum_{x\in\mathbb{F}_q} \phi_{2t-2+r}^{(t)}(x) = 0.$$

Therefore we obtain

$$\sum_{x\in\mathbb{F}_q} \left(\sum_{i=2}^{t} \phi_R^{(i)}(x) - (t-2)\phi_R^{(1)}(x) \right) = 0. \tag{3.1}$$

This results in a zero-sum distinguisher on R rounds of GMiMC. For the input set of the form $\mathcal{X}_0$ w have that the outputs after R rounds, i.e. elements of the form $\Phi_R(x)$ for $x \in \mathbb{F}_q$, satisfy 3.1.

The construction of the integral distinguisher is summarized in Figure 3.1.

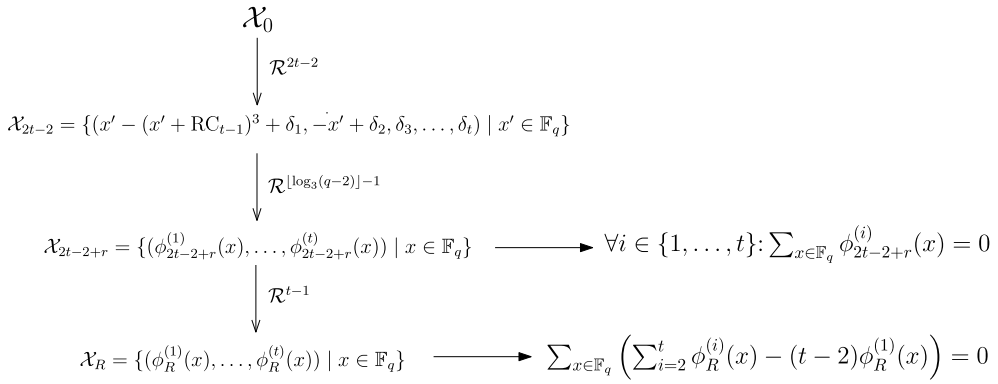

Figure 3.1: Forward direction of a construction of a zero-sum distinguisher with one saturated branch.

3.1.2 Backward direction and the full distinguisher

Integral distinguisher stated above can be extended even more. We can take advantage of the fact that GMiMC permutation does not work with any secret material and the computing in a round is dependent only on the known round-constant and an input. This give us an advantage when choosing a starting set in the construction of the integral distinguisher. We do not have to start with a set of inputs of Round 1, we can build the distinguisher from an internal state and monitor rounds of GMiMC backwards. We can see that the inverse of a round of GMiMC is a round of an unbalanced Feistel network with the same S-box $x \to x^3$ over $\mathbb{F}_q$. More precisely, the inverse of the ith round of GMiMC is as follows

$$\mathcal{R}_i^{-1}\colon (x_1, x_2, \ldots, x_t) \mapsto \left(x_t, x_1 - (x_t + \mathrm{RC}_i)^3, \ldots, x_{t-1} - (x_t + \mathrm{RC}_i)^3\right).$$

We can now start building the integral distinguisher backwards. We choose a set of the internal states of GMiMC after $m = (t-2+\lfloor \log_3(q-2) \rfloor)$ rounds to be of the form of $\mathcal{X}_0$, where we substitute RC_i by $\mathrm{RC}_{i+t-2+\lfloor \log_3(q-2) \rfloor}$ for $i = 1, \ldots, t$. From now on, $\mathcal{X}_0$ denotes such set. Based on the notation in the previous section, $\mathcal{X}_r$ still denotes the output of r rounds of GMiMC applied to $\mathcal{X}_0$. Since $\mathcal{X}_0$ is now a set of internal states after m rounds, $\mathcal{X}_r$ denotes a set of outputs of Round $m+r$ of GMiMC. We can now extend the notation for $-m \leq i \leq -1$. Let us denote by

$$\mathcal{X}_i = \{(\phi_i^{(1)}(x), \ldots, \phi_i^{(t)}(x)) \mid x \in \mathbb{F}_q\}$$

the output set of $|i|$ inverse rounds of GMiMC applied to $\mathcal{X}_0$. In other words, $\mathcal{X}_{-m}$ denotes the set of inputs of Round 1 and for $i > -m$, $\mathcal{X}_i$ denotes a set of outputs after Round $m + i$ of GMiMC.

By definition, each coordinate of Φ_0 is a polynomial of degree at most 3. Since the inverse of a round of GMiMC preserves the S-box, it implies that the coordinates of $\Phi_{-r'}$ for $r' \geq 0$ are polynomials of degree at most $3^{1+r'}$. In the same manner as in the forward direction, we desire of the degree of $\Phi_{-r'}$ to be less then $q-1$. This holds if $r' \leq \lfloor \log_3(q-2) \rfloor - 1$. We again choose the maximal $r' = \lfloor \log_3(q-2) \rfloor - 1$. Then Proposition 7 gives for all $i \in \{1, \ldots, t\}$

$$\sum_{x \in \mathbb{F}_q} \phi_{-r'}^{(i)}(x) = 0. \tag{3.2}$$

It is easily seen that $\mathcal{X}_{-r'}$ also denotes the internal state after Round $m - r' = (t - 2 + \lfloor \log_3(q-2) \rfloor) - (\lfloor \log_3(q-2) \rfloor - 1) = t - 1$ of GMiMC.

Subsequently, we use Lemma 10, since it shows a relation between an input and an output of $t-1$ rounds of GMiMC. We obtain

$$\sum_{i=2}^{t} \phi_{-r'}^{(i)}(x) - (t-2)\phi_{-r'}^{(1)}(x) = \sum_{i=1}^{t-1} \phi_{-m}^{(i)}(x) - (t-2)\phi_{-m}^{(t)}(x)$$

for all $x \in \mathbb{F}_q$. We have by (3.2) that

$$\sum_{x \in \mathbb{F}_q} \left(\sum_{i=2}^{t} \phi_{-r'}^{(i)}(x) - (t-2)\phi_{-r'}^{(1)}(x) \right) = 0,$$

therefore we obtain

$$\sum_{x \in \mathbb{F}_q} \left(\sum_{i=1}^{t-1} \phi_{-m}^{(i)}(x) - (t-2)\phi_{-m}^{(t)}(x) \right) = 0.$$

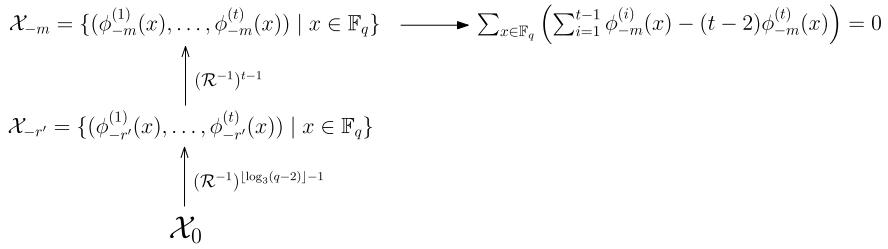

Figure 3.2: Backward direction of a construction of a zero-sum distinguisher with one saturated branch.

The distinguisher constructed in Section 3.1.1 can be built similarly by substituting RC_i by RC_{i+m} for $i = 1, \ldots, t$ and starting with Round $m+1$ of GMiMC. Combining the distinguishers in the forward and backward direction gives a zero-sum distinguisher on

$$R' = 4t - 6 + 2\left\lfloor \log_3(q-2) \right\rfloor$$

rounds of GMiMC with complexity q. As depicted in Figure 3.3, the set of inputs of GMiMC $\mathcal{X}_{-m}$ transforms after R' rounds into the set of outputs $\mathcal{X}_R$, which then satisfies property (3.1).

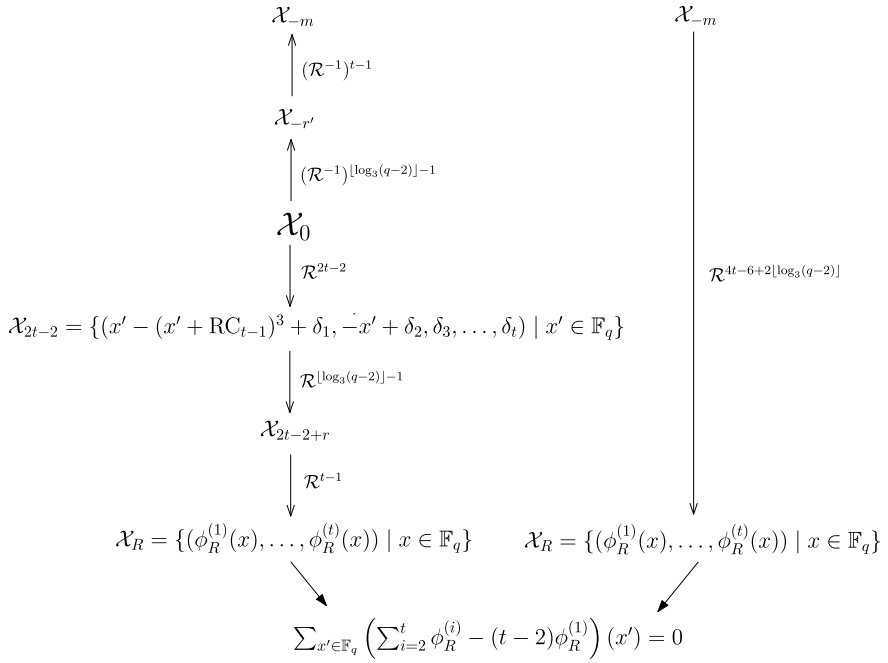

Figure 3.3: The construction of the full zero-sum distinguisher with one saturated branch.

3.2 Saturating two branches

We now turn to the construction of the zero-sum distinguisher by saturating two branches of the permutation. This distinguisher covers even more rounds than the distinguisher in the previous section, specifically $5t - 8 + 2\left\lfloor \log_3(q-2) \right\rfloor$ rounds of GMiMC. However, it has complexity q^2 and can be exhibited for $t > 4$. We

proceed with the construction similarly as above and divide it to forward and backward direction.

3.2.1 Forward direction

Set

$$\mathcal{Y}_0 = \{(\alpha_1, \ldots, \alpha_{t-4}, x, f(x), g(y), y) \mid x, y \in \mathbb{F}_q\},$$

where

$$f(x) = -\left(x + \sum_{i=1}^{t-4} \beta_i + \mathrm{RC}_{m+t-3}\right)^3 - x - 2\sum_{i=1}^{t-4} \beta_i - \mathrm{RC}_{m+t-3} - \mathrm{RC}_{m+t-2},$$
$$g(y) = (y + \mathrm{RC}_m)^3 - y - \mathrm{RC}_m - \mathrm{RC}_{m-1},$$

$\alpha_1, \ldots, \alpha_{t-4}$ are arbitrary constants in $\mathbb{F}_q$, $m = 2t - 2 + \lfloor \log_3(q-2) \rfloor$ and $\beta_1, \ldots, \beta_{t-4}$ are defined as in the section 3.1.1 by replacing RC_i by RC_{m+i}. Let us consider $\mathcal{Y}_0$ a set of internal states after Round m of GMiMC, in other words a set of outputs of the mth round.

Let us set

$$\mathcal{Y}_i = \{(\phi_i^{(1)}(x,y), \ldots, \phi_i^{(t)}(x,y)) \mid x, y \in \mathbb{F}_q\},$$

for $i \geq -m$, where $\phi_i^{(j)}$ is an element of $\mathbb{F}_q[x,y]/(x^q - x, y^q - y)$. Consider $\mathcal{Y}_i$ a set of outputs of next i rounds of GMiMC applied to $\mathcal{Y}_0$ for $i \geq 1$ and for $-m \leq i \leq -1$ a set of outputs of $|i|$ inverse rounds of GMiMC applied to $\mathcal{Y}_0$. It follows that $\mathcal{Y}_{-m}$ is then a set of inputs of Round 1 of GMiMC permutation. As previously, we denote the vector function $(\phi_i^{(1)}, \ldots, \phi_i^{(t)})$ by Φ_i.

Firstly, we focus on the transformation of $\mathcal{Y}_0$ through next $(t-4)$ rounds. Since $\alpha_1, \ldots, \alpha_{t-4}$ are constants, the input of the S-box does not depend on values of x and y in these rounds. By definition of β_i for $i = 1, \ldots, t-4$, we get that the image of the S-box in Round $(m+i)$ is equal to β_i, therefore we obtain

$$\mathcal{Y}_{t-4} = \left\{ \left(x + \sum_{i=1}^{t-4} \beta_i, f(x) + \sum_{i=1}^{t-4} \beta_i, g(y) + \sum_{i=1}^{t-4} \beta_i, y + \sum_{i=1}^{t-4} \beta_i, \right.\right.$$
$$\left.\left. \alpha_1 + \sum_{\substack{i=1 \\ i \neq 1}}^{t-4} \beta_i, \ldots, \alpha_{t-4} + \sum_{\substack{i=1 \\ i \neq t-4}}^{t-4} \beta_i \right) \;\middle|\; x, y \in \mathbb{F}_q \right\}$$

as a set of outputs of Round $(m+t-4)$. We again set $x' = x + \sum_{i=1}^{t-4} \beta_i$. Since $\phi_{t-4}^{(3)}, \ldots \phi_{t-4}^{(t)}$ are polynomials only in y, we denote them by $\gamma_1(y), \ldots, \gamma_{t-2}(y)$, respectively. Let us now compute

$$\begin{aligned}
\phi_{t-4}^{(2)}(x,y) = f(x) + \sum_{i=1}^{t-4} \beta_i &= f\left(x' - \sum_{i=1}^{t-4} \beta_i\right) + \sum_{i=1}^{t-4} \beta_i \\
&= -\left(x' - \sum_{i=1}^{t-4} \beta_i + \sum_{i=1}^{t-4} \beta_i + \mathrm{RC}_{m+t-3}\right)^3 - \left(x' - \sum_{i=1}^{t-4} \beta_i\right) - 2\sum_{i=1}^{t-4} \beta_i \\
&\quad - \mathrm{RC}_{m+t-3} - \mathrm{RC}_{m+t-2} + \sum_{i=1}^{t-4} \beta_i \\
&= -\left(x' + \mathrm{RC}_{m+t-3}\right)^3 - x' - \mathrm{RC}_{m+t-3} - \mathrm{RC}_{m+t-2}.
\end{aligned}$$

Together we have a set of outputs of Round $(m+t-4)$ depending on x' and y of the form

$$\mathcal{Y}_{t-4} = \{(x', -(x'+\mathrm{RC}_{m+t-3})^3 - x' - \mathrm{RC}_{m+t-3} - \mathrm{RC}_{m+t-2}, \\ \gamma_1(y), \ldots, \gamma_{t-2}(y)) \mid x', y \in \mathbb{F}_q\}.$$

The images of the S-box in next two rounds are $(x'+\mathrm{RC}_{m+t-3})^3$ and $-(x'+\mathrm{RC}_{m+t-3})^3$. We thus obtain

$$\mathcal{Y}_{t-2} = \{(\gamma_1(y), \ldots, \gamma_{t-2}(y), \\ x' - (x'+\mathrm{RC}_{m+t-3})^3, -x' - \mathrm{RC}_{m+t-3} - \mathrm{RC}_{m+t-2}) \mid x', y \in \mathbb{F}_q\}.$$

Since $\gamma_1, \ldots, \gamma_{t-2}$ do not depend on the value of x', we have $\deg_{x'}\left(\phi^{(i)}_{2t-4}\right) \leq 3$ for every $i \in \{1, \ldots, t\}$. The derivation of x' clearly does not change the degree of the polynomial, therefore we have $\deg_x\left(\phi^{(i)}_{2t-4}\right) \leq 3$ for every $i \in \{1, \ldots, t\}$. To use Corollary 8, we need to verify that $\deg(\phi^{(i)}_{2t-4+r}) < 2(q-1)$ for every $i \in \{1, \ldots, t\}$. Since we consider $\phi^{(i)}_{2t-4+r}$ a polynomial in $\mathbb{F}_q[x,y]/(x^q - x, y^q - y)$, we have that $\deg(\phi^{(i)}_{2t-4+r}) \leq 2(q-1)$. We need to show that $\deg(\phi^{(i)}_{2t-4+r}) \neq 2(q-1)$. Clearly, $\deg(\phi^{(i)}_{2t-4+r}) = 2(q-1)$ if and only if $\deg_x(\phi^{(i)}_{2t-4+r}) = q-1$ and $\deg_y(\phi^{(i)}_{2t-4+r}) = q-1$. Therefore it suffices to show that the degree of $\phi^{(i)}_{2t-4+r}$ in x or in y is less than $q-1$. As explained in the previous section, $\deg_x(\phi^{(i)}_{2t-4+r}) < q-1$ holds if $3^{1+r} \leq q-2$, i.e. if $r \leq \lfloor \log_3(q-2) \rfloor - 1$. Let us set $r = \lfloor \log_3(q-2) \rfloor - 1$. Corollary 8 then gives

$$\forall i \in \{1, \ldots, t\}\colon \sum_{x,y \in \mathbb{F}_q} \phi^{(i)}_{2t-4+r}(x,y) = 0.$$

Similarly to the previous section, we obtain by Lemma 10

$$\sum_{i=2}^{t} \phi^{(i)}_{3t-5+r}(x,y) - (t-2)\phi^{(1)}_{3t-5+r}(x,y) = \sum_{i=1}^{t-1} \phi^{(i)}_{2t-4+r}(x,y) - (t-2)\phi^{(t)}_{2t-4+r}(x,y)$$

for every $x, y \in \mathbb{F}_q$ We again choose $R = 3t-5+r = 3t-6+\lfloor \log_3(q-2) \rfloor$. We then obtain similarly to the previous sections

$$\sum_{x,y \in \mathbb{F}_q} \left(\sum_{i=2}^{t} \phi^{(i)}_R(x,y) - (t-2)\phi^{(1)}_R(x,y) \right) = 0. \tag{3.3}$$

3.2.2 Backward direction and the full distinguisher

Analogically to the zero-sum distinguisher in Section 3.1, we consider a transformation of $\mathcal{Y}_0$ through some inverse rounds of GMiMC. By the definition of an inverse round of GMiMC, $\mathcal{Y}_0$ transforms after one such round into

$$\begin{aligned}\mathcal{Y}_{-1} &= \{(y, \alpha_1 - (y+\mathrm{RC}_m)^3, \ldots, \alpha_{t-4} - (y+\mathrm{RC}_m)^3, \\ &\quad x - (y+\mathrm{RC}_m)^3, f(x) - (y+\mathrm{RC}_m)^3, g(y) - (y+\mathrm{RC}_m)^3) \mid x, y \in \mathbb{F}_q\} \\ &= \{(y, \alpha_1 - (y+\mathrm{RC}_m)^3, \ldots, \alpha_{t-4} - (y+\mathrm{RC}_m)^3, \\ &\quad x - (y+\mathrm{RC}_m)^3, f(x) - (y+\mathrm{RC}_m)^3, -y - \mathrm{RC}_m - \mathrm{RC}_{m-1}) \mid x, y \in \mathbb{F}_q\}.\end{aligned}$$

The image of the S-box of the next inverse round is

$$\left(\phi_{-1}^{(t)}(x,y)+\mathrm{RC}_{m-1}\right)^3=(-y-\mathrm{RC}_m-\mathrm{RC}_{m-1}+\mathrm{RC}_{m-1})^3=-(y+\mathrm{RC}_m)^3,$$

therefore we get

$$\mathcal{Y}_{-2}=\{(-y-\mathrm{RC}_m-\mathrm{RC}_{m-1},y+(y+\mathrm{RC}_m)^3,\alpha_1,\ldots,\alpha_{t-4},x,f(x))\mid x,y\in\mathbb{F}_q\}.$$

We observe that since the images of $\phi_{-2}^{(3)},\ldots,\phi_{-2}^{(t)}$ do not depend on the value of y, neither does the image of the S-box in the next $t-2$ rounds. Therefore, all coordinates of Φ_{-t} are polynomials in x and y with $\deg_y\left(\phi_{-t}^{(i)}\right)\leq 3$, $i\in\{1,\ldots,t\}$. We now consider r' more inverse rounds of GMiMC as follows. By the explanation in Section 3.2.1, we have the following. To satisfy the assumptions in Corollary 8, it suffices to constrict r' so that $\deg_y(\phi_{-t-r'})<q-1$. This holds if $3^{1+r'}\leq q-2$, thus if $r'\leq\lfloor\log_3(q-2)\rfloor-1$. For $r'=\lfloor\log_3(q-2)\rfloor-1$, we obtain by Corollary 8,

$$\forall i\in\{1,\ldots,t\}\colon\sum_{x,y\in\mathbb{F}_q}\phi_{-t-r'}^{(i)}(x,y)=0.$$

As previously, we use Lemma 10 to extend the distinguisher by $t-1$ more inverse rounds to altogether $t+r'+(t-1)=2t-2+\lfloor\log_3(q-2)\rfloor=m$ rounds of GMiMC. We then have

$$\sum_{x,y\in\mathbb{F}_q}\left(\sum_{i=1}^{t-1}\phi_{-m}^{(i)}(x,y)-(t-2)\phi_{-m}^{(t)}(x,y)\right)=0.$$

We obtain a zero-sum distinguisher on

$$R'=m+R=5t-8+2\lfloor\log_3(q-2)\rfloor$$

rounds GMiMC with complexity q^2 such that for the set of inputs of the form $\mathcal{Y}_{-m}$, the outputs after R' rounds are of the form $\Phi_R^{(i)}(x,y)$ for $x,y\in\mathbb{F}_q$ and hold (3.3).

3.3 Exploiting integral distinguishers over multiplicative subgroups

The complexity of the constructed zero-sum distinguishers over $\mathbb{F}_q$ for "larger" q can be too high, in other words number of encryptions needed for the attack in some cases exceeds some requested threshold. In these cases, the distinguisher as described would be inefficient. However, for a multiplicative group $G\leq\mathbb{F}_q$, we can derive similar distinguishers with lower complexity. We modify the distinguisher from Section 3.1.1 by saturating the coordinate only over the elements of $G\cup\{0\}$ and we obtain by Proposition 9 a zero-sum distinguisher with complexity $|G|+1$ for

$$4t-6+2\lfloor\log_3(|G|-1)\rfloor$$

rounds of GMiMC. Similarly, we obtain from Section 3.1.2 a similar zero-sum distinguisher on

$$3t-6+\lfloor\log_3(|G|-1)\rfloor$$

rounds of GMiMC also with the complexity $|G| + 1$.

Consider a concrete setting of GMiMC over $\mathbb{F}_q$ with N rounds for some $N \in \mathbb{N}$. Exploiting the distinguishers over multiplicative subgroups can be also beneficial when for instance the distinguisher from Section 3.1.1 covers more than N rounds of GMiMC over $\mathbb{F}_q$. If there exists a multiplicative subgroup $G \leq \mathbb{F}_q$ such that

$$4t - 6 + 2\left\lfloor \log_3(|G| - 1) \right\rfloor \geq N,$$

then we obtain a distinguisher that covers all N rounds, but complexity of such distinguisher, i.e. $|G| + 1$, is (for some cases significantly) lower.

4. Impossible differential attacks on GMiMC

4.1 Impossible differential attacks

The impossible differential attack was first introduced in Biham et al. [1999b]. It is a chosen plaintext attack on the block ciphers. The attack exploits propagation of differences of pairs of plaintexts through a cipher.

Let $\mathcal{S} = (\mathcal{P}, \mathcal{K}, e)$ be an iterative cipher. For a function $F\colon \mathcal{P} \to \mathcal{P}$, we say that $\boldsymbol{\alpha}$ *propagates over* F *to* $\boldsymbol{\beta}$ *with probability* p if for a random pair of input vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{P}$ with the input difference $\boldsymbol{u} - \boldsymbol{v} = \boldsymbol{\alpha}$ we obtain the output difference $F(\boldsymbol{u}) - F(\boldsymbol{v}) = \boldsymbol{\beta}$ with probability p. We denote this by

$$\boldsymbol{\alpha} \xrightarrow[p]{F} \boldsymbol{\beta}.$$

We refer to the pair $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ as the *differential* with probability p. For functions $F, F'\colon \mathcal{P} \to \mathcal{P}$ we can build a longer propagation over $F \circ F'$

$$\boldsymbol{\alpha} \xrightarrow[p]{F} \boldsymbol{\beta} \xrightarrow[p']{F'} \boldsymbol{\gamma}$$

with probability pp' (one usually assume that the propagations $\boldsymbol{\alpha} \xrightarrow[p]{F} \boldsymbol{\beta}$ and $\boldsymbol{\beta} \xrightarrow[p']{F'} \boldsymbol{\gamma}$ are independent). In the same manner, we can build a propagation over the whole cipher (or at least a number of rounds).

The idea of the impossible differential attack is, contrary to the traditional differential attack, to find and exploit the differentials with probability 0. If we obtain such a differential, we can many keys from a set of possible key candidates, since the key that enables the impossible propagation is obviously wrong. In the known-key setting, the attack distinguishes the cipher from a random permutation with a similar reasoning. If we find a pair of inputs of the black box satisfying the input and output difference required by the differential, it is clearly not possible for the primitive to be the cipher.

One method of constructing impossible differential is the *miss-in-the-middle* technique. This technique rely on constructing two differentials, each with probability 1, whose conditions can not be satisfied together.

Let t denote the length of the plaintext. In some cases, for the attack to be successful, one does not have to predict the exact values on all t coordinates of the output difference. If a differential predicts only some of the t coordinates of the output difference, it is called a *truncated differential*. This notion was introduced in Knudsen [1995].

4.2 Impossible differential attacks on GMiMC

The attack presented in Beyne et al. [2020] is an improvement of an attack presented in Albrecht et al. [2019], which we describe in the following section.

Let us denote by $\mathcal{R}$ a round of GMiMC permutation.

4.2.1 Original impossible differential attack on GMiMC

Let $\alpha \in \mathbb{F}_q$ be a non zero difference. The original attack uses the miss-in-the-middle technique and exploits the following propagation

$$(0, \ldots, 0, \alpha) \xrightarrow{\mathcal{R}^{t-1}} (\alpha, 0, \ldots, 0).$$

This propagation has probability 1, since in $(t-1)$ rounds, the difference α does not affect the image of the S-box. Similarly, we obtain for any difference $\beta \in \mathbb{F}_q$ a probability one propagation

$$(0, \ldots, 0, \beta) \xleftarrow{(\mathcal{R}^{-1})^{t-1}} (\beta, 0, \ldots, 0).$$

We also have

$$(\alpha, 0, \ldots, 0) \neq (0, \ldots, 0, \beta)$$

for $\alpha, \beta \neq 0$. Together, we construct the following impossible differential

$$(0, \ldots, 0, \alpha) \xrightarrow[1]{\mathcal{R}^{t-1}} (\alpha, 0, \ldots, 0) \neq (0, \ldots, 0, \beta) \xleftarrow[1]{(\mathcal{R}^{-1})^{t-1}} (\beta, 0, \ldots, 0).$$

We obtain an attack on $(2t-2)$ rounds of GMiMC exploiting

$$(0, \ldots, 0, \alpha) \xrightarrow[0]{\mathcal{R}^{2t-2}} (\beta, 0, \ldots, 0),$$

for any $\alpha \in \mathbb{F}_q, \alpha \neq 0$ and any $\beta \in \mathbb{F}_q$.

To distinguish GMiMC from a random permutation, by Biryukov [2005b] it is necessary to encrypt about $2^{t \log_2 q - \log_2 q}$ pairs of plaintexts with the differences of the form $(0, \ldots, 0, \alpha)$. Then, if one of the output differences of the pairs after $(2t-2)$ rounds is of the form $(\beta, 0, \ldots, 0)$, the black box is certainly not GMiMC. However as in Biham et al. [1999a], if none of the output differences is of such form, only with probability approximately e^{-1} is the black box the GMiMC permutation.

4.2.2 New impossible differential attack on GMiMC

The new impossible differential attack on $(3t-4)$ rounds of GMiMC, presented in Beyne et al. [2020], uses the the differential built in the previous section while adding $(t-2)$ rounds in the middle of the propagation. We obtain the impossible differential

$$(0 \ldots, 0, \alpha_1) \xrightarrow[0]{\mathcal{R}^{3t-4}} (\beta_1, 0 \ldots, 0)$$

for any $\alpha_1, \beta_1 \in \mathbb{F}_q, \alpha_1 \neq \beta_1$. The attack is applicable when t is even.

Let us denote by $\alpha_1 \xrightarrow{\mathcal{S}} \alpha_2$ the propagation of the difference α_1 through the S-box. For two inputs of the S-box a and $a + \alpha_1$, we have the images as follows

$$\begin{aligned}
&(a + \mathrm{RC}_i)^3, \\
&(a + \mathrm{RC}_i + \alpha_1) = (a + \mathrm{RC}_i)^3 + 3(a + \mathrm{RC}_i)^2\alpha_1 + 3(a + \mathrm{RC}_i)\alpha_1^2 + \alpha_1^2.
\end{aligned}$$

We obtain

$$\alpha_2 = 3(a + \mathrm{RC}_i)^2\alpha_1 + 3(a + \mathrm{RC}_i)\alpha_1^2 + \alpha_1^2.$$

Consider an input difference $(\alpha_1, 0, \ldots, 0)$ for any $\alpha_1 \in \mathbb{F}_q^*$. By the above, the output differences of the S-box in the next rounds are unpredictable, since they do not depend only on the input differences, but also on the exact values of the inputs. Let us denote the output difference of the S-box in the next $t/2-1$ rounds by $\alpha_2, \ldots, \alpha_{t/2}$. We can write

$$(\alpha_1, 0, \ldots, 0) \xrightarrow[1]{\mathcal{R}} (\alpha_2, \ldots \alpha_2, \alpha_1) \xrightarrow[1]{\mathcal{R}} (\alpha_2 + \alpha_3, \ldots, \alpha_2 + \alpha_3, \alpha_1 + \alpha_3, \alpha_2).$$

In the same manner, we have a probability one differential

$$(0, \ldots, 0, \alpha_1) \xrightarrow[1]{\mathcal{R}^{t-1}} (\alpha_1, 0, \ldots, 0)$$
$$\xrightarrow[1]{\mathcal{R}^{t/2-1}} \left(\sum_{i=2}^{t/2} \alpha_i, \ldots, \sum_{i=2}^{t/2} \alpha_i, \alpha_1 + \sum_{\substack{i=2 \\ i\neq 2}}^{t/2} \alpha_i, \sum_{\substack{i=2 \\ i\neq 3}}^{t/2} \alpha_i, \ldots, \sum_{\substack{i=2 \\ i\neq t/2}}^{t/2} \alpha_i \right).$$

Let us denote the last difference by Δ_1.

Similarly, for the input difference $(0, \ldots, 0, \beta_1), \beta_1 \in \mathbb{F}_q$ we denote the output differences of the S-box in the next $t/2 - 1$ inverse rounds by $\beta_2, \ldots, \beta_{t/2}$. It follows by the definition of the inverse round of GMiMC

$$(\beta_1, 0, \ldots, 0) \xrightarrow[1]{(\mathcal{R}^{-1})^{t-1}} (0, \ldots, 0, \beta_1)$$
$$\xrightarrow[1]{(\mathcal{R}^{-1})^{t/2-1}} \left(-\sum_{\substack{i=2 \\ i\neq t/2}}^{t/2} \beta_i, \ldots, -\sum_{\substack{i=2 \\ i\neq 3}}^{t/2} \beta_i, \beta_1 - \sum_{\substack{i=2 \\ i\neq 2}}^{t/2} \beta_i, -\sum_{i=2}^{t/2} \beta_i, \ldots, -\sum_{i=2}^{t/2} \beta_i \right)$$

with a probability 1. Let the last difference be denoted by Δ_2. We have a propagation

$$(0, \ldots, 0, \alpha_1) \xrightarrow[1]{\mathcal{R}^{3t/2-2}} \Delta \xleftarrow[1]{(\mathcal{R}^{-1})^{3t/2-2}} (\beta_1, 0, \ldots, 0).$$

To be a valid propagation, it must follow $\Delta_1 = \Delta = \Delta_2$, in other words, the differences Δ_1 and Δ_2 must equal in every coordinate. Thus, we obtain a system of t linear equations with $2(t/2 - 1) = t - 2$ variables. It follows by solving the system, that $\alpha_1 = \beta_1$ in order for the system to have a nontrivial solution. Thus, $(0, \ldots, 0, \alpha_1)$ never propagates to $(\beta_1, 0, \ldots, 0)$ after $3t - 4$ rounds for $\alpha_1 \neq \beta_1$.

Conclusion

In this thesis we presented GMiMC permutation and provided the cryptographic background necessary for its formal description. In Chapter 2, we described the concept of an integral attack and provided both the known distinguishing property in a binary finite field and the generalized distinguishing property in a finite field of any characteristic, introduced in Beyne et al. [2020]. We explained the theory and expended some of the proofs. In Chapter 3, we constructed the integral distinguishers on GMiMC using the generalized distinguishing property as presented in Beyne et al. [2020]. Finally, in Chapter 4 we described the impossible differential attack and provided two instances of the attack on GMiMC permutation.

Bibliography

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, Paper 2019/397, 2019. URL https://eprint.iacr.org/2019/397. https://eprint.iacr.org/2019/397.

Robert El Bashir. Matematická kryptografie a kryptoanalýza 1 - lecture notes on boolean functions, a. URL https://sent.cz/TK/booleovske_funkce-I.pdf.

Robert El Bashir. Matematická kryptografie a kryptoanalýza 1 - lecture notes on symmetric cryptosystems, b. URL https://sent.cz/TK/symetricke_kryptosystemy.pdf.

Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive, Paper 2018/046, 2018. URL https://eprint.iacr.org/2018/046. https://eprint.iacr.org/2018/046.

Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 181–197. Springer, 2008. doi: 10.1007/978-3-540-78967-3_11. URL https://iacr.org/archive/eurocrypt2008/49650180/49650180.pdf.

Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, and Friedrich Wiemer. Out of Oddity – New Cryptanalytic Techniques against Symmetric Primitives Optimized for Integrity Proof Systems. Cryptology ePrint Archive, Paper 2020/188, 2020. URL https://eprint.iacr.org/2020/188. https://eprint.iacr.org/2020/188.

Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *Advances in Cryptology — EUROCRYPT '99*, pages 12–23, Berlin, Heidelberg, 1999a. Springer Berlin Heidelberg. ISBN 978-3-540-48910-8.

Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In Jacques Stern, editor, *Advances in Cryptology — EUROCRYPT '99*, pages 12–23, Berlin, Heidelberg, 1999b. Springer Berlin Heidelberg. ISBN 978-3-540-48910-8.

Alex Biryukov. *Feistel Cipher*, pages 221–221. Springer US, Boston, MA, 2005a. ISBN 978-0-387-23483-0. doi: 10.1007/0-387-23483-7_159. URL https://doi.org/10.1007/0-387-23483-7_159.

Alex Biryukov. *Impossible Differential Attack*, pages 286–287. Springer US, Boston, MA, 2005b. ISBN 978-0-387-23483-0. doi: 10.1007/0-387-23483-7_197. URL https://doi.org/10.1007/0-387-23483-7_197.

Lars Knudsen and David Wagner. Integral cryptanalysis. In *Lecture notes in computer science*, pages 112–127, Berlin, 2002. Springer. ISBN 9783540440093.

Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *Fast Software Encryption*, pages 196–211, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg. ISBN 978-3-540-47809-6.

Xuejia Lai. *Higher Order Derivatives and Differential Cryptanalysis*, pages 227–233. Springer US, Boston, MA, 1994. ISBN 978-1-4615-2694-0. doi: 10.1007/978-1-4615-2694-0_23. URL https://doi.org/10.1007/978-1-4615-2694-0_23.

Bruce Schneier and John Kelsey. Unbalanced feistel networks and block cipher design. In Dieter Gollmann, editor, *Fast Software Encryption*, pages 121–144, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg. ISBN 978-3-540-49652-6.