Cryptography and Communications
https://doi.org/10.1007/s12095-024-00711-4

RESEARCH

Propagation properties of a non-linear mapping based on squaring in odd characteristic

Joan Daemen[1] · Daniël Kuijsters[1] · Silvia Mella[1] · Denise Verbakel[1]

Received: 28 November 2023 / Accepted: 18 March 2024

Abstract

Many modern cryptographic primitives for hashing and (authenticated) encryption make use of constructions that are instantiated with an iterated cryptographic permutation that operates on a fixed-width state consisting of an array of bits. Often, such permutations are the repeated application of a relatively simple round function consisting of a linear layer and a non-linear layer. These constructions do not require that the underlying function is a permutation and they can plausibly be based on a non-invertible transformation. Recently, Grassi proposed the use of non-invertible mappings operating on arrays of digits that are elements of a finite field of odd characteristic for so-called MPC-/FHE-/ZK-friendly symmetric cryptographic primitives. In this work, we consider a mapping that we call γ that has a simple expression and is based on squaring. We discuss, for the first time, the differential and linear propagation properties of γ and observe that these follow the same rules up to a relabeling of the digits. This is an intriguing property that, as far as we know, only exists for γ and the binary mapping χ_3 that is used in the cryptographic permutation XOODOO. Moreover, we study the implications of its non-invertibility on differentials with zero output difference and on biases at the output of the γ mapping and show that they are as small as they can possibly be.

Keywords Non-linear layer · Squaring · Finite fields

Mathematics Subject Classification (2010) 94A60 · 06E30

✉ Daniël Kuijsters
daniel.kuijsters@ru.nl

Joan Daemen
joan.daemen@ru.nl

Silvia Mella
silvia.mella@ru.nl

Denise Verbakel
denise.verbakel@ru.nl

[1] Digital Security, Radboud University, Toernooiveld 212, Nijmegen 6525 EC, The Netherlands

Published online: 26 April 2024

1 Introduction

The round functions in cryptographic permutations of the type Substitution-Permutation Networks (SPN) consist of a non-linear layer and a linear layer. These layers are chosen and combined so that there is no exploitable differential propagation from input to output or exploitable correlations between input and output when used in the context of a construction like the sponge or duplex construction [1], Farfalle [2] or Even-Mansour [3]. The relevant properties of these mappings over binary fields have been studied extensively, leading to solid designs. However, in the last years there has been a growing interest in similar functions operating on arrays of digits that are elements of a field of odd characteristic. For instance, Kölbl et al. designed a ternary cryptographic hash function called Troika [4]. Other examples are the symmetric primitives defined over $\mathbb{F}_p^n$ like MiMC [5], GMiMC [6], Poseidon [7], Ciminion [8], and many others. These are designed to be efficient in the context of Secure Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge proofs (ZK).

There are interesting differences between fields $\mathbb{F}_{2^d}$ of characteristic 2 and those of odd characteristic that we will denote by $\mathbb{F}_q$. For instance, addition and subtraction are the same in $\mathbb{F}_{2^d}$, but this is not the case in $\mathbb{F}_q$. In $\mathbb{F}_{2^d}$, squaring is a linear operation, whereas in $\mathbb{F}_q$ squaring is a non-linear operation. In $\mathbb{F}_2$, correlations between input and output bits have values that are rational and range from -1 to 1, but in $\mathbb{F}_p$, correlations are complex numbers inside the closed unit disk.

This work investigates a mapping over $\mathbb{F}_q^n$ that was recently proposed by Grassi [9] and that we call γ. This is the mapping defined over $\mathbb{F}_q^n$ by $\gamma_i(x) = x_i + x_{i+1}^2$ for $i \in \mathbb{Z}/n\mathbb{Z}$ and for all $x \in \mathbb{F}_q^n$.

The paper is organized as follows. Section 2 deals with commonly used notation and conventions that we follow. In Section 3 we recall the basic notions from differential cryptanalysis. An overview of correlation analysis is presented in Section 4. In Section 5 we apply this existing theory to the squaring transformation and derive its DP and LP values. Based on the squaring transformation, we motivate the choice for γ in Section 6. The main contribution of this paper lies in Sections 7 and 8, where we study the differential and linear propagation properties of γ, both in the forward and backward direction. Our results are useful in determining the maximum probabilities of differentials and differential trails over transformations making use of γ in their round function, as in computer-assisted trail search [10]. Moreover, as the differential and linear propagation properties of γ follow the same rules, our results are also useful to study the correlations of linear approximations and linear trails. In Section 9 we study the collision probability and bias of linear combinations of output digits of γ. Finally, we conclude in Section 10.

2 Notation and conventions

We denote by $\mathbb{F}_q$ the finite field of *odd* characteristic p, i.e., q is equal to p^d for some odd prime p and positive integer $d > 0$. Let $\mathbb{F}_q^n$ be the vector space of dimension n over the finite field $\mathbb{F}_q$. Given two vectors $x, y \in \mathbb{F}_q^n$, we denote their vector subtraction by $x - y$, i.e., $x - y = x + (-1)y$. A vector $x \in \mathbb{F}_q^n$ is indexed by the set $\mathbb{Z}/n\mathbb{Z}$. We denote its ith coordinate by x_i and call it a *digit*. The dot product between x and y is defined as $x^\top y = \sum_{i=0}^{n-1} x_i y_i$. We write e_i for the vector with all digits equal to 0, except for the digit that is indexed by i, which is equal to 1. The linear span of a set of vectors $S \subseteq \mathbb{F}_q^n$ is denoted by Span(S). A digit is said to be *active* if it is non-zero. The Hamming weight $\mathrm{HW}(x)$ of a vector $x \in \mathbb{F}_q^n$ is the number of active digits in the vector.

Let $z \in \mathbb{C}$ be a complex number. We denote its absolute value as $|z|$. We write $\overline{z}$ for its complex conjugate.

Let F be a field, then we write F^* for its multiplicative group $F \setminus \{0\}$.

3 Differential analysis

First published by Biham and Shamir in [11], *differential cryptanalysis* is a chosen-plaintext attack that exploits the non-uniformity of the distribution of differences at the output of a transformation when it is applied to pairs of inputs with a fixed difference.

Any successful theory of cryptanalysis needs to address the problem of secret key translation. Differential cryptanalysis deals with this problem by considering differences, which are invariant under translation. Let $x \in \mathbb{F}_q^n$ and $x^* \in \mathbb{F}_q^n$ be inputs of a transformation $\alpha \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ and let their difference be $a = x^* - x$. Likewise, let $y \in \mathbb{F}_q^n$ and $y^* \in \mathbb{F}_q^n$ be outputs of α and let their difference be $b = y^* - y$. The (ordered) pair $(a, b) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ containing the input and output difference is called a *differential* over α. The differential $(0, 0)$ is called *trivial*. The *differential probability (DP)* of a differential (a, b) over the transformation α is defined as

$$\mathrm{DP}_\alpha(a, b) = q^{-n} \left|\{x \in \mathbb{F}_q^n : \alpha(x + a) - \alpha(x) = b\}\right| .$$

If $\mathrm{DP}_\alpha(a, b) > 0$, we say that a and b are *compatible* differences over α. For compatible differences a and b, we define the weight of a differential (a, b) over α as

$$\mathrm{w}_\alpha(a, b) = -\log_q(\mathrm{DP}_\alpha(a, b)) .$$

A non-trivial differential (a, b) over α can only lead to a distinguisher if $\mathrm{DP}_\alpha(a, b)$ differs significantly from q^{-n}, which is the expected DP of any non-trivial differential over a randomly selected transformation of $\mathbb{F}_q^n$.

4 Correlation analysis

Correlation analysis of cryptographic primitives effectively is Fourier analysis on finite abelian groups. As such, the theory is well-understood and this section serves as a recap. The ideas that we present here are based on the works of Daemen [12], Baignères et al. [13], and Daemen and Rijmen [14]. Many of the proofs can be found in the book by Hou [15].

4.1 Characters

Let $(G, +)$ be a finite abelian group and let e be the (finite) exponent of G, i.e., the smallest integer n such that $na = 0$ for all $a \in G$.

A *character* of G is a homomorphism from G into the subgroup of $\mathbb{C}^*$ consisting of the eth roots of unity. The set of characters of G is denoted by $\hat{G}$ and it forms a group under the multiplication defined by $(\chi\chi')(a) = \chi(a)\chi'(a)$ for all $a \in G$ and $\chi, \chi' \in \hat{G}$. The groups G and $\hat{G}$ are isomorphic, but this isomorphism is not canonical.

For a fixed isomorphism between G and $\hat{G}$ and for each $a \in G$, we write χ_a for the image of a under this isomorphism. In particular, the character χ_0 that is defined by $\chi_0(a) = 1$ for all $a \in G$ is called the *trivial character* and it is the identity element of the group $\hat{G}$.

Now, let $(G, +, \cdot)$ be the commutative ring that is obtained by introducing a multiplicative structure on G. This is always possible by the fundamental theorem of finite abelian groups. A character $\chi \in \hat{G}$ is called a *generating character* for G if $\chi_a(b) = \chi(ab)$ for all $a, b \in G$. If a commutative ring has a generating character for its additive group, then $\chi_a(b) = \chi(ab) = \chi(ba) = \chi_b(a)$. In the case that G is the direct sum of n copies of a commutative ring R and if R has a generating character, say ϕ, then we obtain a generating character χ for G by setting $\chi(a_1, \ldots, a_n) = \phi(a_1) \cdots \phi(a_n)$. It holds that $\chi_a(b) = \chi(ab) = \phi(a^\top b)$, where the multiplication in G is defined component-wise.

As an example, consider G equal to $\mathbb{F}_q$ and put $\omega = e^{2\pi i/p}$. Let $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ be the absolute trace function that is defined by $\mathrm{Tr}(x) = \sum_{i=0}^{d-1} x^{p^i}$. This is a linear mapping. Each $u \in \mathbb{F}_q$ defines a generating character χ_u for $\mathbb{F}_q$ that is defined by

$$\chi_u(x) = \omega^{\mathrm{Tr}(ux)}, \qquad x \in \mathbb{F}_q .$$

As a second example, consider G equal to $\mathbb{F}_q^n$, which is a direct sum of n copies of $\mathbb{F}_q$. Hence, each $u \in \mathbb{F}_q^n$ gives a generating character χ_u for $\mathbb{F}_q^n$ that is defined by

$$\chi_u(x) = \omega^{\mathrm{Tr}(u^\top x)}, \qquad x \in \mathbb{F}_q^n .$$

4.2 The Fourier transform

Consider the set $L^2(G)$ of functions $f\colon G \to \mathbb{C}$. Fix an ordering of the elements of G, e.g., $G = \{a_0, \ldots, a_{n-1}\}$. We write $\upsilon_f = (f(a_0), \ldots, f(a_{n-1}))$ for the finite sequence of the output values of f. By identifying a function f with the vector $\upsilon_f \in \mathbb{C}^{|G|}$, $L^2(G)$ can be seen as a finite-dimensional complex inner product space with inner product

$$\langle f, g\rangle = \sum_{a\in G} f(a)\overline{g(a)}, \qquad f, g \in L^2(G) .$$

For any $f \in L^2(G)$, the inner product induces a norm by setting

$$\|f\| = \langle f, f\rangle^{\frac{1}{2}} .$$

The standard basis of $L^2(G)$ is formed by the set of Dirac delta functions $\{\delta_a \in L^2(G) : a \in G\}$, which are defined by

$$\delta_a(b) = \begin{cases} 1 & \text{if } a = b\,, \\ 0 & \text{if } a \neq b\,. \end{cases}$$

In the context of correlation analysis, the solution to the problem of secret key translation lies in changing the basis of $L^2(G)$ to the set of characters of G. For any $a, b \in G$, the corresponding characters satisfy $\langle \chi_a, \chi_b\rangle = |G|\delta_a(b)$. By normalizing the characters, we obtain an orthonormal basis

$$\Phi_G = \{\phi_a : a \in G\} ,$$

where $\phi_a = |G|^{-\frac{1}{2}}\chi_a$. By projecting f onto Φ_G, we find that

$$f = \sum_{a \in G} \langle f, \phi_a \rangle \phi_a \,.$$

The operator $\mathcal{F} \colon L^2(G) \to L^2(G)$ that is defined by $\mathcal{F}(f)(a) = \langle f, \phi_a \rangle$ for all $a \in G$ is called the *Fourier transform*. By identifying a function f with υ_f, the Fourier transform is best described as assigning to f its coordinates in the normalized character basis. The *Plancherel theorem* asserts that the Fourier transform is unitary, i.e., we have

$$\langle \mathcal{F}(f), \mathcal{F}(g) \rangle = \langle f, g \rangle, \qquad f, g \in L^2(G) \,.$$

Let us return to the question of how to address the problem of secret key translation. Let $b \in G$. We define the translation operator $T_b \colon L^2(G) \to L^2(G)$ by $(T_b f)(a) = f(a+b)$ for all $a \in G$. Moreover, we define the modulation operator $M_b \colon L^2(G) \to L^2(G)$ by $(M_b f)(a) = \phi_b(a) f(a)$ for all $a \in G$. The big insight is that translation turns into modulation when changing from the standard basis to the normalized character basis, i.e.,

$$T_b = \mathcal{F}^{-1} \circ M_b \circ \mathcal{F}, \qquad b \in G \,.$$

Let H be a finite abelian group and let $F \colon G \to H$ be a mapping between G and H. We want a representation of F in $L^2(G)$. To that end, let χ be any character of H. We take as representation the function $\chi \circ F \in L^2(G)$.

4.3 Correlation

We now specialize to the case that G and H are each equal to the vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$.

Let $\alpha \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a transformation of $\mathbb{F}_q^n$. We consider pairs $(u, v) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ that we call *linear approximations* of α. We refer to u as the *output mask* and to v as the *input mask*. The linear approximation $(0, 0)$ is called *trivial*. The *correlation* of the linear approximation is defined as

$$\mathrm{C}_\alpha(u, v) = q^{-\frac{n}{2}} \mathcal{F}(\chi_u \circ \alpha)(v) \,.$$

We call the masks u and v *compatible* over α if $\mathrm{C}_\alpha(u, v)$ is nonzero. In general, correlations are complex numbers. The *linear potential (LP)* is a real number and related to a correlation by

$$\mathrm{LP}_\alpha(u, v) = \mathrm{C}_\alpha(u, v)\overline{\mathrm{C}_\alpha(u, v)} \,.$$

If u and v are compatible over α, then we can define the *weight* of the linear approximation (u, v) as

$$\mathrm{w}_\alpha(u, v) = -\log_q(\mathrm{LP}_\alpha(u, v)) \,.$$

5 The squaring transformation

The squaring transformation $\beta \colon \mathbb{F}_q \to \mathbb{F}_q$ is defined by $x \mapsto x^2$ for all $x \in \mathbb{F}_q$. Because we study the case of odd characteristic, β is non-linear. We show that β has the property that the maximal DP over all non-trivial differentials is q^{-1}, which is the smallest possible value. A similar property holds for the maximal LP over all non-trivial linear approximations. In other words, we show that β is a *bent* polynomial [16]. Note that this is an improvement from the case of characteristic 2, for which these values are both equal to $2q^{-1}$ and are obtained by, respectively, almost perfect nonlinear and bent functions [17].

First, by applying Theorem 5.33 from [18], we obtain that the correlation of any linear approximation $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$ with $u \neq 0$ of β is equal to

$$\begin{aligned} \mathrm{C}_\beta(u, v) &= q^{-\frac{1}{2}} \mathcal{F}(\chi_u \circ \beta)(v) \\ &= q^{-1} \sum_{x \in \mathbb{F}_q} \chi_1(ux^2 - vx) \\ &= \begin{cases} q^{-\frac{1}{2}} (-1)^{d-1} \chi_1(-v^2(4u)^{-1}) \eta(u) & \text{if } p \equiv 1 \pmod 4\,, \\ q^{-\frac{1}{2}} (-1)^{d-1} i^d \chi_1(-v^2(4u)^{-1}) \eta(u) & \text{if } p \equiv 3 \pmod 4\,, \end{cases} \end{aligned}$$

where $\eta(u) = 1$ if u is a square in $\mathbb{F}_q$ and -1 otherwise. It follows that for all $u, v \in \mathbb{F}_q$ with $u \neq 0$ we have $\mathrm{LP}_\beta(u, v) = q^{-1}$. In particular, choosing v equal to zero shows that any linear combination of output digits of β is imbalanced, i.e., the distribution of this linear combination is non-uniform. If u is 0, then for all nonzero $v \in \mathbb{F}_q$ we have $\mathrm{LP}_\beta(0, v) = 0$, and $\mathrm{LP}_\beta(0, 0) = 1$.

Second, consider the equation that relates the input $x \in \mathbb{F}_q$, the input difference $a \in \mathbb{F}_q$, and the output difference $b \in \mathbb{F}_q$, i.e.,

$$\begin{aligned} b &= \beta(x + a) - \beta(x) \\ &= (x + a)^2 - x^2 \\ &= x^2 + 2ax + a^2 - x^2 \\ &= 2ax + a^2\,. \end{aligned}$$

Assuming that $a \neq 0$ and because the characteristic of $\mathbb{F}_q$ is odd, we can solve for x to find that $x = (2a)^{-1}(b - a^2)$. Hence, there is exactly one solution to this equation. Dividing by the domain size, q, then shows that $\mathrm{DP}_\beta(a, b) = q^{-1}$. In particular, any nonzero input difference can propagate to a zero output difference. If a is 0, then for all nonzero $b \in \mathbb{F}_q$, we have $\mathrm{DP}_\beta(0, b) = 0$ and $\mathrm{DP}_\beta(0, 0) = 1$.

We summarize these properties to make the symmetry between the differential and linear case apparent:

- For all $a, u \in (\mathbb{F}_q)^*$ and $b, v \in \mathbb{F}_q$, we have $\mathrm{DP}_\beta(a, b) = \mathrm{LP}_\beta(u, v) = q^{-1}$;
- For all $b, v \in (\mathbb{F}_q)^*$, we have $\mathrm{DP}_\beta(0, b) = \mathrm{LP}_\beta(0, v) = 0$;
- We have $\mathrm{DP}_\beta(0, 0) = \mathrm{LP}_\beta(0, 0) = 1$.

6 The γ mapping

Some modern block cipher modes, like GCM [19], CTR and OFB [20], do not use the inverse block cipher. Similarly, constructions like sponge [21], duplex [1], and Farfalle [2], which are generally based on permutations, do not use their inverse. Therefore, in such constructions permutations can be replaced by transformations. An example is the GLUON family of lightweight hash functions [22], which makes use of the sponge construction on top of a non-invertible map.

A cryptographic transformation can be used as long as collisions and imbalances in the output cannot be exploited. This can be tackled by either ensuring that such imbalance is very small or by limiting the attacker's access to the input and output of the transformation by construction. For instance, in the sponge and duplex constructions the attacker has control of only the outer part of the state and not of its inner part. Therefore, if a collision requires a difference in the inner part of the state at the input of the transformation, the attacker cannot inject it with input messages. Similarly, the attacker has no visibility of the inner bits or digits of any output mask. As another example, whitening keys can be added at input and output, like in Farfalle [2], Even-Mansour [3], and Elephant [23].

We consider the problem of building a non-invertible mapping based on squaring that can be used as non-linear layer in the round function of cryptographic transformations. When such transformations are used in constructions that are usually instantiated with permutations, the non-invertibility of the mapping should be difficult to exploit.

By definition, such a non-linear layer has pairs of distinct inputs that are mapped to the same output, i.e., collisions. A naive idea would be to apply β to each digit of the state independently. The problem with this approach is that each collision for β is trivially extended to a collision for the entire non-linear layer, giving rise to differentials with DP as high as q^{-1}. They are easy to exploit as the adversary needs access to only a single input digit to generate a local collision. Similarly, any bias in the output of β is trivially present in the output of the non-linear layer, giving rise to linear approximations with LP as high as q^{-1}. They are easy to exploit as the adversary needs access to only a single output digit to exploit them. The measure of both is inversely proportional to the order of the field. Hence, unless the order of the field is very large, this leads to unacceptable weaknesses in the cryptographic transformation.

Compared to the above, the non-linear layer in the round function of a cryptographic transformation should have lower DP and LP and there should not exist local properties that can be extended to global properties. We achieve this by making the DP of differentials of the form $(a, 0)$ and the LP of linear approximations of the form $(u, 0)$ small, i.e., equal to the inverse of the domain size. Moreover, any differential over or linear approximation of the non-linear layer requires access to every digit of the state.

The work by Grassi [9] presents an analysis of a number of mappings based on β that minimize the probability of a collision in their output. We consider one of these mappings and call it γ. Concretely, the mapping $\gamma : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is defined, for all $x \in \mathbb{F}_q^n$, by

$$\gamma_i(x) = x_i + x_{i+1}^2, \qquad i \in \mathbb{Z}/n\mathbb{Z}\,.$$

The remainder of this text is concerned with an analysis of the differential and linear propagation properties of γ.

7 Differential propagation properties of γ

Let $(a, b) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ be a differential over γ and let $x \in \mathbb{F}_q^n$ be an input of γ. The equations that relate the input difference a and the output difference b are of the form

$$b_i = a_i + a_{i+1}^2 + 2a_{i+1}x_{i+1}, \qquad i \in \mathbb{Z}/n\mathbb{Z}\,. \tag{1}$$

We consider two cases in the analysis of these equations. In the first case, we fix the input difference a and give a description of the set of compatible output differences b. From this, we are able to deduce that $\mathrm{DP}_\gamma(a, b)$ depends only on a and whether b is compatible with a or not.

In the second, reverse case, we fix the output difference b and present an algorithm for the computation of the set of compatible input differences a. We then derive an expression of the so-called minimum reverse weight of this set. All these results can be directly applied to perform computer-aided trail search, as described in [10], in cryptographic transformations instantiated with γ as the non-linear layer.

7.1 Forward propagation from a given input difference

We observe that for an input difference a, the equations of (1) are linear in the digits of x. We make this explicit by writing them as a matrix equation of the form

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-2} \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 + a_1^2 \\ a_1 + a_2^2 \\ a_2 + a_3^2 \\ \vdots \\ a_{n-2} + a_{n-1}^2 \\ a_{n-1} + a_0^2 \end{pmatrix} + \begin{pmatrix} 0 & 2a_1 & 0 & 0 & \cdots 0 & 0 \\ 0 & 0 & 2a_2 & 0 & \cdots 0 & 0 \\ 0 & 0 & 0 & 2a_3 & \cdots 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & 0 & \cdots 0 & 2a_{n-1} \\ 2a_0 & 0 & 0 & 0 & \cdots 0 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{n-2} \\ x_{n-1} \end{pmatrix} .$$

Hence, the set of compatible output vectors b, which we denote by $\mathcal{A}(a)$, forms an affine subspace of $\mathbb{F}_q^n$. By affine subspace we mean the following. Let W be a linear subspace of $\mathbb{F}_q^n$ and let $u \in \mathbb{F}_q^n$. The coset $u + W = \{u + w : w \in W\}$ is called an affine subspace of $\mathbb{F}_q^n$ and u is called an offset. The affine subspace $\mathcal{A}(a)$ can be described by

$$\mathcal{A}(a) = \gamma(a) + \text{Span}\{2a_i e_{i-1} : i \in \mathbb{Z}/n\mathbb{Z}\} .$$

Two cosets $u + W$ and $v + W$ are equal if and only if $u - v \in W$. Therefore, we may add any linear combination of the basis vectors to the offset without it changing the affine subspace that is defined. Moreover, we may scale the basis vectors by any nonzero constant. Hence, a description of $\mathcal{A}(a)$ in which the offset has minimal Hamming weight is given by

$$\mathcal{A}(a) = a' + \text{Span}\{e_i : i \in \mathbb{Z}/n\mathbb{Z} \text{ and } a_{i+1} \neq 0\} ,$$

where

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

Clearly, the dimension of $\mathcal{A}(a)$, which is defined as the dimension of the associated vector space, is equal to the Hamming weight of a.

We are now ready to give a complete characterization of the distribution of differentials over γ.

Proposition 1 *Let $(a, b) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ be a differential over γ. Then b is compatible with a, i.e., $b \in \mathcal{A}(a)$, if and only if, for all $i \in \mathbb{Z}/n\mathbb{Z}$, we have $b_i = a_i$ or $a_{i+1} \neq 0$, in which case b_i can take on any value. Hence,*

$$\text{DP}_\gamma(a, b) = \begin{cases} q^{-\text{HW}(a)} & \textit{if } b \in \mathcal{A}(a) , \\ 0 & \textit{if } b \notin \mathcal{A}(a) . \end{cases}$$

In other words, the DP of a valid differential, and thus its differential weight, is a constant that depends only on the input difference.

7.2 Backward propagation from a given output difference

For a given output difference b, the compatible input differences do not form an affine space. However, we will show in this section how to efficiently generate all compatible input differences a with $\mathrm{w}_\gamma(a, b) \leq W$ for some weight limit W. To this end, we introduce the concept of compatible activity pattern. Given a vector $x \in \mathbb{F}_q^n$, its activity pattern $\widetilde{x}$ is a vector in $\mathbb{F}_q^n$ with $\widetilde{x}_i$ equal to 1 if $x_i \neq 0$ and 0 otherwise.

Definition 1 An activity pattern is compatible with b if there exists an input difference a that is compatible with b and for which $\widetilde{a}$ equals this activity pattern.

The generation of all compatible input differences is done in two phases: in the first phase, we generate the set of activity patterns compatible with b, and in the second phase, we determine for each compatible activity pattern the set of compatible input differences with that pattern.

We generate the compatible activity patterns in a recursive way in Algorithm 1, making use of the following proposition.

Proposition 2 *Given a differential (a, b) over γ, the following properties hold:*

1. *if $a_i = 0$ and $b_{i-1} = 0$ then $a_{i-1} = 0$;*
2. *if $a_i = 0$ and $b_{i-1} \neq 0$ then $a_{i-1} \neq 0$.*

Proof The two properties immediately follow from (1). We have

$$b_{i-1} = a_{i-1} + a_i^2 + 2a_i x_i \ ,$$

and $a_i = 0$ implies $b_{i-1} = a_{i-1}$. □

In Algorithm 1, we start with an empty list of compatible activity patterns L (line 4) and a fully unspecified activity pattern $\widetilde{a}$ (line 6). Then we specify whether $\widetilde{a}_{n-1} = 0$ (line 6) or 1 (line 7) (and thus whether a_{n-1} is active or not) and based on this we incrementally determine the activity of all other digits from a_{n-2} to a_0 using the procedure buildActivity. In this procedure, when $\widetilde{a}_i = 0$ we use Proposition 2 to determine whether $\widetilde{a}_{i-1} = 1$ or 0, otherwise we consider both possibilities (lines 16 and 17). When a compatible activity pattern is fully determined (i.e., when $i = 0$ is reached) then it is added to list L (line 12).

Given an output difference b and a compatible input activity pattern $\widetilde{a}$, we generate all compatible differences with activity $\widetilde{a}$ in Algorithm 2, making use of the following proposition.

Proposition 3 *Given a differential (a, b) over γ, the following properties hold:*

1. *if $\widetilde{a}_i = 0$, then $a_i = 0$;*
2. *if $\widetilde{a}_i = 1$ and $\widetilde{a}_{i+1} = 0$, then $a_i = b_i$;*
3. *if $\widetilde{a}_i = 1$ and $\widetilde{a}_{i+1} = 1$, then a_i can be any value in $\mathbb{F}_q$.*

Proof The first property follows from the definition of activity pattern. The other two properties immediately follow from (1). □

In Algorithm 2, we start with an empty list of compatible input differences L (line 4) and a fully unspecified difference a (line 5). We use the symbol $*$ when the activity of a digit is unspecified. Then we incrementally determine the value of all digits from a_0 to a_{n-1} using the procedure buildDifference. In this procedure, we use Proposition 3 to determine whether $a_i = 1$ or 0 (lines 10-12 and 16-18). When a compatible difference is fully determined (i.e., when $i = n - 1$ is reached) then it is added to list L (line 10-12).

Algorithm 1 Generation of input activity patterns compatible with output difference b.

```
Input: difference $b \in \mathbb{F}_q^n$ at output of $\gamma$ and limit weight $W$
Output: list $L$ of activity patterns $\widetilde{a}$ compatible with $b$ at input of $\gamma$

$L \leftarrow$ empty
$\widetilde{a} \leftarrow *^n$
$\widetilde{a}_{n-1} \leftarrow 0$; buildActivity$(n-1, \widetilde{a}, b, W)$
$\widetilde{a}_{n-1} \leftarrow 1$; buildActivity$(n-1, \widetilde{a}, b, W)$

procedure buildActivity$(i, \widetilde{a}, b, W)$
    if $(\mathrm{HW}(\widetilde{a}) > W)$ then return        ▷ HW is computed on the specified part of $\widetilde{a}$
    if $(i = 0)$ then
        if $(\widetilde{a}_{n-1} = 1$ OR $\widetilde{b}_0 = \widetilde{a}_0)$ then add $\widetilde{a}$ to $L$
        return
    end if
    $\widetilde{a}' \leftarrow \widetilde{a}$
    if $(\widetilde{a}_i = 1$ OR $\widetilde{b}_{i-1} = 1)$ then $\widetilde{a}'_{i-1} \leftarrow 1$; buildActivity$(i-1, \widetilde{a}', b, W)$
    if $(\widetilde{a}_i = 1$ OR $\widetilde{b}_{i-1} = 0)$ then $\widetilde{a}'_{i-1} \leftarrow 0$; buildActivity$(i-1, \widetilde{a}', b, W)$
    return
end procedure
```

Algorithm 2 Generation of input differences compatible with output difference b and with activity pattern $\widetilde{a}$.

```
Input: difference $b \in \mathbb{F}_q^n$ at output of $\gamma$ and activity pattern $\widetilde{a}$
Output: list $L$ of input differences compatible with $b$ at input of $\gamma$ with activity pattern $\widetilde{a}$

$L \leftarrow$ empty
$a \leftarrow *^n$
buildDifference$(0, a, \widetilde{a}, b)$

procedure buildDifference$(i, a, \widetilde{a}, b)$
   if $(i = n-1)$ then
        if $(\widetilde{a}_i = 0)$ then $a'_i \leftarrow 0$; add $a$ to $L$
        elsif $(\widetilde{a}_i = 1$ AND $\widetilde{a}_0 = 0)$ then $a'_i \leftarrow b_i$; add $a$ to $L$
        else for each $k \in \mathbb{F}_q$ do $a'_i \leftarrow k$; add $a$ to $L$
        return
    end if
    $a' \leftarrow a$
    if $(\widetilde{a}_i = 0)$ then $a'_i \leftarrow 0$; buildDifference$(i+1, a', \widetilde{a}, b)$
    elsif $(\widetilde{a}_i = 1$ AND $\widetilde{a}_{i+1} = 0)$ then $a'_i \leftarrow b_i$; buildDifference$(i+1, a', \widetilde{a}, b)$
    else for each $k \in \mathbb{F}_q$ do $a'_i \leftarrow k$; buildDifference$(i+1, a', \widetilde{a}, b)$
end procedure
```

7.3 Computing the minimum reverse weight of an output difference

Given an output difference b, let $\Omega(b) = \{a \in \mathbb{F}_q^n : \mathrm{DP}_\gamma(a, b) > 0\}$ be the set of input differences that are compatible with b. The differentials (a, b) over γ with $a \in \Omega(b)$ can have different weights. Following [10], the *minimum reverse weight* of an output difference b is defined by

$$\mathrm{w}_\gamma^{\mathrm{rev}}(b) = \min_{a \in \Omega(b)} \mathrm{w}_\gamma(a, b)\,.$$

We notice that the minimum reverse weight of a difference b at the output of γ is fully determined by its activity pattern and its compatible activity patterns with minimum Hamming weight. In particular, it can be computed as in the following Proposition, which uses the notion of *run*.

Definition 2 Given $x \in \mathbb{F}_q^n$, a run of length ℓ in x is a sequence of ℓ active digits preceded and followed by non-active digits, i.e., it satisfies $x_i, x_{i+1}, \ldots, x_{i+\ell-1} \neq 0$ and $x_{i-1} = x_{i+\ell} = 0$ for some $i \in \mathbb{Z}/n\mathbb{Z}$.

Proposition 4 *Given a difference b at the output of γ composed by m runs of lengths ℓ_j, with $j = 0, \ldots, m-1$, then*

$$\mathrm{w}_\gamma^{rev}(b) = \sum_{j=0}^{m-1} \lceil \ell_j/2 \rceil \,.$$

Proof For a run starting in position i and of length ℓ in b, the digit $\widetilde{a}_{i+\ell-1}$ must be 1. There can be at most a single zero digit in between two active digits in the sequence $\widetilde{a}_i, \widetilde{a}_{i+1}, \ldots, \widetilde{a}_{i+\ell-1}$. It follows that for each run of length ℓ in b, a has at least $\ell/2$ active digits if ℓ is even and $(\ell+1)/2$ if ℓ is odd. □

8 Linear propagation properties of γ

In this section we analyze the correlation properties of the mapping γ, starting with the correlation of linear approximations of γ.

Proposition 5 *Let $(u, v) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ be a linear approximation of γ. We have*

$$\mathrm{C}_\gamma(u, v) = \prod_{i=0}^{n-1} \mathrm{C}_\beta(u_i - v_i, u_{i-1}) \,.$$

Proof If we rewrite the correlation of a linear approximation of γ, we obtain

$$\begin{aligned}
\mathrm{C}_\gamma(u, v) &= q^{-n} \sum_{x \in \mathbb{F}_q^n} \omega^{\mathrm{Tr}\left(u^\top \gamma(x) - v^\top x\right)} \\
&= q^{-n} \sum_{x \in \mathbb{F}_q^n} \omega^{\mathrm{Tr}\left(\sum_{i=0}^{n-1} u_i(x_i + x_{i+1}^2) - v_i x_i\right)} \\
&= q^{-n} \sum_{x \in \mathbb{F}_q^n} \omega^{\mathrm{Tr}\left(\sum_{i=0}^{n-1} (u_i - v_i)x_i + u_{i-1}x_i^2\right)} \\
&= q^{-n} \sum_{x \in \mathbb{F}_q^n} \omega^{\sum_{i=0}^{n-1} \mathrm{Tr}\left((u_i - v_i)x_i + u_{i-1}x_i^2\right)} \\
&= q^{-n} \sum_{x \in \mathbb{F}_q^n} \prod_{i=0}^{n-1} \omega^{\mathrm{Tr}\left((u_i - v_i)x_i + u_{i-1}x_i^2\right)} \\
&= \prod_{i=0}^{n-1} q^{-1} \sum_{y \in \mathbb{F}_q} \omega^{\mathrm{Tr}\left((u_i - v_i)y + u_{i-1}y^2\right)} \\
&= \prod_{i=0}^{n-1} \mathrm{C}_\beta(u_i - v_i, u_{i-1}) \,.
\end{aligned}$$

□

The resulting product from Proposition 5 is non-zero if each of the factors is non-zero. Note that the correlation is non-zero if u_{i-1} is non-zero, as was discussed in Section 5. Additionally, if u_{i-1} is non-zero, then $v_i - u_i$ has to be equal to zero to get a non-zero correlation. In this case it should thus hold that $v_i = u_i$. From this reasoning, we can give a complete characterization of the distribution of linear approximations of γ.

Proposition 6 *Let $(u, v) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ be a linear approximation of γ. Then u is compatible with v, if and only if, for all $i \in \mathbb{Z}/n\mathbb{Z}$, we have $v_i = u_i$ or $u_{i-1} \neq 0$, in which case v_i can take on any value. Hence,*

$$\mathrm{LP}_\gamma(u, v) = \begin{cases} q^{-\mathrm{HW}(u)} & \text{if } v \text{ is compatible with } u\,, \\ 0 & \text{if } v \text{ is not compatible with } u\,. \end{cases}$$

Observe that Propositions 1 and 6 are very much alike. Indeed, propagation of differences and propagation of masks over γ follow similar rules. First, output masks play the role of input differences and input masks that of output differences. Second, indices are reversed, i.e., index i in a mask corresponds to index $n - i - 1$ in a difference, to account for this change in direction. The following proposition is an immediate consequence.

Proposition 7 *Let $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the mapping defined by $\pi_i(x) = x_{n-i-1}$ for all $i \in \mathbb{Z}/n\mathbb{Z}$. Let (u, v) be a linear approximation of γ. We have*

$$\mathrm{LP}_\gamma(u, v) = \mathrm{DP}_\gamma(\pi(u), \pi(v))\,.$$

From this, it follows that we can extend the results obtained in Section 7 to masks. For a given output mask $u \in \mathbb{F}_q^n$, we can build the affine subspace with dimension $\mathrm{HW}(u)$ of compatible input masks over γ as in Section 7.1. Moreover, for a given input mask $v \in \mathbb{F}_q^n$, the output activity patterns compatible with input masks over γ can be found by applying Algorithm 1. Using the resulting activity pattern $\widetilde{a}$ and the input mask v, all compatible output masks u can be obtained as described in Algorithm 2. Note that there can be several compatible output masks u for a given input mask v. Among them, there will be one realizing the minimum value of $\mathrm{w}(u, v)$. The *minimum reverse weight* of v is defined as

$$\mathrm{w}_\gamma^{\mathrm{rev}}(v) = \min_{u : \mathrm{LP}_\gamma(u,v) > 0} \mathrm{w}_\gamma(u, v)$$

and is determined by the decomposition of v in a sequence of runs, as explained in Section 7.3.

9 On collision probability and bias

A collision in the output of γ occurs when γ maps a pair of different inputs $(x, y) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ to the same output value. Assuming randomly and uniformly selected pairs of inputs, the probability of a collision is given by

$$\mathrm{CP}(\gamma) = q^{-2n} |\{(x, y) \in \mathbb{F}_q^n \times \mathbb{F}_q^n : x \neq y \text{ and } \gamma(x) = \gamma(y)\}|\,.$$

Translating this into the language of differential analysis, we find that

$$\mathrm{CP}(\gamma) = q^{-n} \sum_{a \in \mathbb{F}_q^n \setminus \{0\}} \mathrm{DP}_\gamma(a, 0)\,.$$

Proposition 8 *Let $a \in \mathbb{F}_q^n \setminus \{0\}$. If $(a, 0)$ is a differential with* $\mathrm{DP}_\gamma(a, 0) > 0$*, then all digits of a are active and* $\mathrm{DP}_\gamma(a, 0) = q^{-n}$.

Proof Let $a \in \mathbb{F}_q^n \setminus \{0\}$ be such that $\mathrm{DP}_\gamma(a, 0) > 0$. The input difference a is compatible with the output difference 0 if the latter is contained in the affine space $A(a)$. This is the case if and only if $a_i \neq 0$ for $i \in \mathbb{Z}/n\mathbb{Z}$. Hence, $\mathrm{DP}_\gamma(a, 0) = q^{-n}$ by Proposition 1. □

Clearly, there are $(q-1)^n$ input differences a for which this property holds. Therefore, we find that

$$\mathrm{CP}(\gamma) = (q-1)^n q^{-2n} .$$

Now, the collision probability of a function that is chosen randomly from the set of functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ is equal to q^{-n}. Hence, the ratio between the collision probability of γ and that of a random function is equal to $(1 - q^{-1})^n$. If the order of the field is large, then this quantity approximates 1.

By symmetry, we obtain a similar result for the bias of any linear combination of output digits of γ.

Proposition 9 *Let $u \in \mathbb{F}_q^n \setminus \{0\}$. If $(u, 0)$ is a linear approximation with* $\mathrm{LP}_\gamma(u, 0) > 0$*, then all digits of u are active and* $\mathrm{LP}_\gamma(u, 0) = q^{-n}$.

Clearly, if either q or n is large, then these quantities are very small and it becomes difficult to exploit them in practice.

10 Conclusion

When searching for trails over an iterated cryptographic transformation as described in [10], a number of tools are required. These include an efficient method to compute the minimum reverse weight of a given difference (resp. mask), and an efficient method to build all compatible input differences (resp. output masks) over the non-linear layer for a given output difference (resp. input mask) and vice versa. In this work we provided such tools for a mapping based on squaring that can be used as non-linear layer in the construction of cryptographic transformations of $\mathbb{F}_q^n$. Interestingly, it turns out that for this mapping, masks and differences follow the same propagation rules. This means that for a cryptographic transformation that uses this mapping as the non-linear layer in its round function, one would need to only perform either differential or linear trail search while obtaining insights and bounds for both.

Acknowledgements Joan Daemen and Daniël Kuijsters are supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA.
Silvia Mella is supported by the European Commission through the ERC Starting Grant 805031 (EPOQUE).

References

1. Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: Duplexing the sponge: singlepass authenticated encryption and other applications. Cryptology ePrint archive, paper 2011/499. (2011) https://eprint.iacr.org/2011/499
2. Bertoni, G., Daemen, J., Hoffert, S., Peeters, M., Assche, G.V., Keer, R.V.: Farfalle: parallel permutation-based cryptography. IACR Trans. Symmetric Cryptol. **2017**(4), 1–38 (2017)
3. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptol. **10**(3), 151–162 (1997). https://doi.org/10.1007/S001459900025
4. Kölbl, S., Tischhauser, E., Derbez, P., Bogdanov, A.: Troika: a ternary cryptographic hash function. Des. Codes Crypt. **88**(1), 91–117 (2019). https://doi.org/10.1007/s10623-019-00673-2
5. Albrecht, M.R., Grassi, L., Rechberger, C., Roy, A., Tiessen, T.: MiMC: efficient encryption and cryptographic hashing with minimal multiplicative complexity. Advances in cryptology - ASIACRYPT (2016)
6. Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schofnegger, M.: Feistel structures for MPC, and more. Computer security - ESORICS (2019)
7. Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., Schofnegger, M.: Poseidon: a new hash function for zero-knowledge proof systems. 30th USENIX security symposium (2021)
8. Dobraunig, C., Grassi, L., Guinet, A., Kuijsters, D.: Ciminion: symmetric encryption based on toffoli-gates over large finite fields. Advances in cryptology - EUROCRYPT (2021)
9. Grassi, L.: Bounded surjective quadratic functions over fnp for mpc-/zk-/fhefriendly symmetric primitives. IACR Trans. Symmetric Cryptol. **2023**(2), 94–131 (2023) https://doi.org/10.46586/TOSC.V2023.I2.94-131
10. Daemen, J., Assche, G.V.: Differential propagation analysis of keccak. In: Canteaut, A. (ed.) Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers. Lecture Notes in Computer Science, vol. 7549, pp. 422–441. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34047-5_24
11. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, august 11-15, 1990, Proceedings. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer, Berlin, Heidelberg (1990). https://doi.org/10.1007/3-540-38424-3_1
12. Daemen, J., Govaerts, R., Vandewalle, J.: Correlation matrices. In: Preneel, B. (ed.) Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings. Lecture Notes in Computer Science, vol. 1008, pp. 275–285. Springer, Berlin, Heidelberg (1994) https://doi.org/10.1007/3-540-60590-8_21
13. Baignères, T., Stern, J., Vaudenay, S.: Linear cryptanalysis of non binary ciphers. In: Adams, C., Miri, A., Wiener, M. (eds.) Selected Areas in Cryptography, pp. 184–211. Springer, Heidelberg, Germany (2007). https://doi.org/10.1007/978-3-540-77360-3_13
14. Daemen, J., Rijmen, V.: Correlation Analysis in GF(2n). In: the design of rijndael: the advanced encryption standard (AES), pp. 181–194. Springer, Heidelberg, Germany (2020). https://doi.org/10.1007/978-3-662-60769-5_12
15. Hou, X.-d.: Lectures on Finite Fields. American Mathematical Society, Providence, Rhode Island. Series: Graduate Studies in Mathematics, vol. 190 (2018)
16. Coulter, R.S., Matthews, R.W.: Bent polynomials over finite fields. Bull. Aust. Math. Soc. **56**(3), 429–437 (1997). https://doi.org/10.1017/S000497270003121X
17. Carlet, C. (ed.): Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, UK (2020). https://doi.org/10.1017/9781108606806
18. Lidl, R., Niederreiter, H.: Finite Fields vol. 20, 2nd edn. Cambridge University Press, Cambridge, United Kingdom (1997)
19. Standards, N.I., Technology: NIST SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (November 2007). https://csrc.nist.gov/pubs/sp/800/38/d/final
20. Standards, N.I., Technology: NIST SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques (November 2007). https://csrc.nist.gov/pubs/sp/800/38/a/final
21. Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: On the indifferentiability of the sponge construction. In: Smart, N.P. (ed.) Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13- 17, 2008. Proceedings. Lecture Notes in Computer Science, vol. 4965, pp. 181–197. Springer, Berlin, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_11
22. Berger, T.P., D'Hayer, J., Marquet, K., Minier, M., Thomas, G.: The GLUON family: a lightweight hash function family based on fcsrs. In: Mitrokotsa, A., Vaudenay, S. (eds.) Progress in Cryptology - AFRICACRYPT 2012 - 5th International Conference on Cryptology in Africa, Ifrance, Morocco, July

10- 12, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7374, pp. 306–323. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31410-0_19

23. Beyne, T., Chen, Y.L., Dobraunig, C., Mennink, B.: Dumbo, jumbo, and delirium: parallel authenticated encryption for the lightweight circus. IACR Trans. Symmetric Cryptol. **2020**(S1), 5–30 (2020) https://doi.org/10.13154/TOSC.V2020.IS1.5-30