General Results of Linear Approximations over Finite Abelian Groups

Zhongfeng Niu[1], Siwei Sun[1, 4], Hanlun Yan[1], Qi Wang[2, 3]

[1]School of Cryptology, University of Chinese Academy of Sciences, Beijing, China

[2]Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen, 518055, China

[3] National Center for Applied Mathematics Shenzhen, Southern University of Science and Technology, Shenzhen, 518055, China

[4]State Key Laboratory of Cryptology, Beijing, 100878, China

niuzhongfeng1996@163.com, sunsiwei@ucas.ac.cn, hailun.yan@ucas.ac.cn, wangqi@sustech.edu.cn

Abstract

In recent years, progress in practical applications of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK) motivate people to explore symmetric-key cryptographic algorithms, as well as corresponding cryptanalysis techniques (such as differential cryptanalysis, linear cryptanalysis), over general finite fields $\mathbb{F}$ or the additive group induced by $\mathbb{F}^n$. This investigation leads to the break of some MPC/FHE/ZK-friendly symmetric-key primitives, the United States format-preserving encryption standard FF3-1 and the South-Korean standards FEA-1 and FEA-2. In this paper, we revisit linear cryptanalysis and give general results of linear approximations over arbitrary finite Abelian groups. We consider the *nonlinearity*, which is the maximal non-trivial linear approximation, to characterize the resistance of a function against linear cryptanalysis. The lower bound of the nonlinearity of a function $F : G \to H$ over an arbitrary finite Abelian group was first given by Pott in 2004. However, the result was restricted to the case that the size of G divides the size of H due to its connection to relative difference sets. We complete the generalization from $\mathbb{F}_2^n$ to finite Abelian groups and give the lower bound of λ_F for all different cases. Our result is deduced by the new links that we established between linear cryptanalysis and differential cryptanalysis over general finite Abelian groups.

Index Terms

Linear Cryptanalysis, Differential Cryptanalysis, Finite Abelien Groups, Linear Approximations.

I. Introduction

Linear cryptanalysis, which was first proposed by Matsui [1] in 1993, is one of the most powerful methods to evaluate the security of symmetric-key ciphers. The main idea of linear cryptanalysis is to find linear relations (called linear approximations) with high probability between parity bits of the plaintext, the ciphertext, and the secret key. Since Matsui's work, linear cryptanalysis has attracted intensive attention and has been developed to several extensions and variants [2]–[8].

In order to characterize the resistance of symmetric-key primitives against linear cryptanalysis, several metrics are proposed. Nyberg [9], Chabaud and Vaudenay [10] use the nonlinearity (linear-resistance) λ_F of Boolean vector functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ as

$$\lambda_F = \max_{a\in\mathbb{F}_2^n;\, b\neq 0^m,\, b\in\mathbb{F}_2^m} 2^{-n} \cdot | \sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x \oplus b\cdot F(x)} |,$$

with the following lower bound.

1) When $n > m$,

$$\lambda_F \geq 2^{-\frac{n}{2}};$$

2) When $n \leq m$,

$$\lambda_F \geq 2^{-n} \cdot \sqrt{3 \times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

The lower bound of linearity λ_F is related to the notion of bent functions and almost bent functions. A bent function is a Boolean function that can reach the lower bound of linearity λ_F under different cases. That is, a bent function is a special type of Boolean function with optimal nonlinearity.

The lower bound of linearity λ_F of the function $F : G \to H$ over an arbitrary finite Abelian group was first given by Pott in [11]. Pott generalized the main results on nonlinear functions from the case of $\mathbb{F}_2^n$ to those on arbitrary Abelian groups by using the discrete Fourier transform instead of the Walsh–Hadamard transforms (the main tool to investigate Boolean functions on $\mathbb{F}_2^n$). However, Pott only gave a lower bound of nonlinearity λ_F under certain conditions (when the size of the domain divides the size of the range of F, i.e., $|G| \mid |H|$). A more general result was missing.

When arguing why it should be interesting to consider Abelian groups, the reason is actually not very clear at the very beginning as most applications (in particular in cryptography) at that time exploit nonlinear functions on finite fields. Pott's pointed out that "there is no technical reason why you should restrict yourselves to this case" [11]. Until recent years, progress in practical applications of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK) motivate people to explore symmetric-key cryptographic algorithms over prime fields $\mathbb{F}_p$ for large p, such as MiMC [12], GMiMC [13], HadesMiMC [14], Poseidon [15] and other primitives [16], [17]. Moreover, this motivates us to reconsider traditional cryptanalysis techniques (such as differential cryptanalysis, linear cryptanalysis) for symmetric-key primitives working on prime fields $\mathbb{F}_p$ with large p. Although differential cryptanalysis (through the theory of Markov ciphers) can be specified over an arbitrary group, linear cryptanalysis is based on a metric (the linear probability) that sticks to bit strings. Applying it to a non-binary block cipher would at least require to generalize this notion.

In [18], Baignères et al. generalized the notion of linear distinguisher to arbitrary sets, which is considered as the most natural one. They got sharp estimates of the data complexity and cumulate characteristics in linear hulls. In their work, they used group characters: for the function $F : G \to H$ between finite Abelian group G and H, the "linear approximation" of F corresponds to a pair of group characters (ψ_1, ψ_2) of G and H. Namely, the correlation of the "linear approximation" (ψ_1, ψ_2) is equal to

$$C^F_{\psi_1,\psi_2} = \frac{1}{|G|} \sum_{x \in G} \psi_1(F(x)) \overline{\psi_2(x)},$$

where group characters ψ_1 and ψ_2 is a group homomorphism $\psi_1 : H \to \mathbb{C}^\times$ and a group homomorphism $\psi_2 : G \to \mathbb{C}^\times$, respectively, and $\overline{\psi_1}$ denotes the complex-conjugate of ψ_1. For example, for $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the linear approximation of F is

$$C^F_{u,v} = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot F(x)} (-1)^{v \cdot x},$$

which is exactly the case in [1]. For $F : \mathbb{Z}/N_1\mathbb{Z} \to \mathbb{Z}/N_2\mathbb{Z}$, the linear approximation of F is

$$C^F_{n_2,n_1} = \frac{1}{N_1} \sum_{x \in \mathbb{Z}/N_1\mathbb{Z}} e^{\frac{F(x) \cdot n_2 \cdot 2\pi i}{N_2}} e^{\frac{-x \cdot n_1 \cdot 2\pi i}{N_1}}.$$

For $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$, the linear approximation of F is

$$C^F_{u,v} = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} e^{\frac{<F(x),u> \cdot 2\pi i}{p}} e^{-\frac{<x,v> \cdot 2\pi i}{p}},$$

where $x \cdot v$ is the inner product of $x, v \in \mathbb{F}_p^n$.

At CRYPTO 2021, Beyne [19] considered the multidimensional case and applied it to the cryptanalysis of FF3-1. Later at ASIACRYPT 2021 [20], by using the notion of correlation matrix of linear approximation, which is similar to the notion in [21], Beyne showed the underlying link between the general linear approximation and many common cryptanalysis, such as invariant subspace attack, nonlinear invariants and integral attacks.

Our Contribution. In this paper, we give general results of linear approximations over finite Abelian groups, making Pott's work [11] more complete after nearly 20 years. Like [9], [10], for a function $F : G \to H$ mapping from finite Abelian group G to H, we use the "maximum value" of all non-trivial "linear approximation" λ_F, which is defined as

$$\lambda_F = \max_{\psi_1 \in \hat{G};\ \psi_2 \neq \hat{1},\ \psi_2 \in \hat{H}} |C^F_{\psi_1,\psi_2}|,$$

as the indicators to measure the resistance of linear cryptanalysis. First, we investigate the link between the linear cryptanalysis and differential cryptanalysis for the function $F : G \to H$ over finite Abelian groups. With the above link, we can deduce results of linear approximations by considering differentials, which is more natural over Abelian groups. Finally, we give the low bound of λ_F for all different cases ($\rho_{G,H}$ is defined in Definiton III.2)):

1) When $|G| \mid |H|$ and $\rho_{G,H} \leq \lfloor \frac{|G|}{|H|} \rfloor$

$$\lambda_F \geq |G|^{-\frac{1}{2}}.$$

2) When $|G| \nmid |H|$ and $\rho_{G,H} \leq \lceil \frac{|G|}{|H|} \rceil$

$$\lambda_F \geq \left(\frac{|H|(|G|-1)}{|G|^3(|H|-1)} \big(|H| \lceil \frac{|G|}{|H|} \rceil^2 + 2\, re \lceil \frac{|G|}{|H|} \rceil + re\big) + \frac{|H|-|G|}{|G|(|H|-1)} \right)^{\frac{1}{2}},$$

where $|G| = |H| \cdot \lceil \frac{|G|}{|H|} \rceil + re$, $0 < re < |H|$.

3) When $\rho_{G,H} > \lfloor \frac{|G|}{|H|} \rfloor$ and $|G| \mid \rho_{G,H}$

$$\lambda_F \geq \left(\frac{|H|(|G|-1)}{|G|^2(|H|-1)} \rho_{G,H} + \frac{|H|-|G|}{|G|(|H|-1)} \right)^{\frac{1}{2}}.$$

4) When $\rho_{G,H} > \lfloor \frac{|G|}{|H|} \rfloor$ and $|G| \nmid \rho_{G,H}$

$$\lambda_F \geq \left(\frac{|H|(|G|-1)}{|G|^3(|H|-1)} \big((m-h) \cdot c^2 + h \cdot (c+1)^2 \big) + \frac{|H|-|G|}{|G|(|H|-1)} \right)^{\frac{1}{2}},$$

where $|G| = m \cdot \rho_{G,H} + n$, $0 < n < \rho_{G,H}$ and $|G| = c \cdot m + h$, $0 < h < m$.

Note that in case 1), we get the same result as that in Pott's work [11] but with a different technique, and in case 3) the result is consistent with [10]'s result.

Organization. The remainder of the paper is organized as follows: Section II includes the notations and preliminaries. Section III generalizes the linearity of functions to Abelian Groups and gives its (trivial) lower bound. Section IV establishes new links between differential cryptanalysis and Linear cryptanalysis over finite Abelian groups. Section V gives some results of differential probability on finite Abelian groups. Section VI deduces a tighter lower bound of the nonlinearity λ_F by gathering the results in Section IV and Section V. The paper is concluded in Section VII.

II. Notations and Preliminaries

Let $\mathbb{F}_2 = \{0,1\}$ be the binary field and $\mathbb{F}_2^n = \{0,1\}^n$. Then, the set of n-bit binary strings $\mathbb{F}_2^n$ with the exclusive-or operation $\oplus$ forms an Abelian group. For x and y in $\mathbb{F}_2^n$, the inner product of x and y is denoted by $x \cdot y$. Let $\mathbb{C}$ be the set of complex numbers. Then, the set of nonzero complex numbers $\mathbb{C}^* = \mathbb{C} - \{0\}$ with the multiplication operation forms an Abelian group. For $z = a + bi \in \mathbb{C}$ with a and b being real numbers, its conjugate is denoted by $\bar{z} = a - bi$. The norm of z is defined as $\|z\| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$. For a finite set G, the number of elements in G is denoted by $|G|$.

Definition II.1. *Let $(G_1, +)$ and $(G_2, *)$ be two groups, if the function $f : G_1 \to G_2$ satifies*

$$f(g+h) = f(g) * f(h)$$

for all $g, h \in G_1$, the function f is called a homomorphism. Moreover, if f is bijection, we call it an isomorphism.

A. Group Characters

Definition II.2 (Group Characters [22])**.** *Let G be a finite Abelian group. A group homomorphism $h : G \to \mathbb{C}^*$ from G to $\mathbb{C}^*$ is called a group character of the finite Abelian group G. We denote by $\hat{G}$ the set of all characters of G.*

Example II.1. *The group homomorphism from $\mathbb{F}_2^n$ to $\mathbb{C}^*$ mapping $x \in \mathbb{F}_2^n$ to $(-1)^{a \cdot x}$ for some $a \in \mathbb{F}_2^n$ is a group character of $\mathbb{F}_2^n$. The group homomorphism from $\mathbb{Z}_n$ to $\mathbb{C}^*$ mapping $x \in \mathbb{Z}_n$ to $e^{-2\pi i a x/n}$ for some $a \in \mathbb{Z}_n$ is a group character of $\mathbb{Z}_n$.*

It is easy to check that the unit circle $\{z \in \mathbb{C} : \|z\| = 1\} \subseteq \mathbb{C}$ is a group with the multiplication in $\mathbb{C}$. The following lemma tells us that the group characters of G are group homomorphisms from G to the the unit circle in $\mathbb{C}$.

Lemma II.1. *Let G be a finite Abelian group. Then, For any $\chi \in \hat{G}$ and $g \in G$, $\|\chi(g)\| = 1$.*

Proof. For $g \in G$, there exists a positive integer N, such that $g^N = 1$. Then, for any $\chi \in \hat{G}$, $\|\chi(g)\|^N = \|(\chi(g))^N\| = \|\chi(g^N)\| = 1$, and thus $\|\chi(g)\| = 1$. □

Then, for $\psi \in \hat{G}$ and $\varphi \in \hat{G}$, the function mapping $x \in G$ to $\psi(x)\varphi(x) \in \mathbb{C}^*$ is the group homomorphism form G to $\mathbb{C}^*$ due to Definiton II.2. We denote the operator $\star$ over $\hat{G}$ such that for ψ and φ in $\hat{G}$, $\psi \star \varphi \in \hat{G}$ is mapping $x \in G$ to $\psi(x)\varphi(x) \in \mathbb{C}^*$.

Definition II.3. *Let $\mathbf{1}_G : G \to \mathbb{C}^*$ be the homomorphism from the finite Abelian group G to C^* such that for all $g \in G$, $\mathbf{1}_G(g) = 1$. Then, $\mathbf{1}_G$ is a group character of G.*

It is easy to check that $\hat{G}$ is also a finite Abelian group with the operation $\star$, where $\mathbf{1}_G \in \hat{G}$ is the identity element. The inverse element of ψ is denoted by ψ^{-1}, that is, $\psi \star \psi^{-1} = \psi^{-1} \star \psi = \mathbf{1}_G \in \hat{G}$. Note that the readers should not confuse ψ^{-1} with the inverse function of ψ, which may not exist at all. Let $\overline{\psi}$ be a function from G to $\mathbb{C}$ which maps $x \in G$ to $\overline{\psi(x)}$, where $\overline{z}$ is conjugate of z for $z \in \mathbb{C}$. Then, it is easy to check that $\overline{\psi}$ is also a group character.

Theorem II.1 ([22]). *The finite Abelian group $\hat{G}$ is isomorphic to G, which is denoted by $\hat{G} \cong G$. Therefore, $\hat{\hat{G}} \cong \hat{G} \cong G$.*

Theorem II.2 ([22]). *Let G, H be two finite Abelian group. Then χ is a character of (G, H) if and only if $\chi = \chi_1 \times \chi_2$ for some $\chi_1 \in \hat{G}$ and $\chi_2 \in \hat{H}$, where $\times$ is multiplication over $\mathbb{C}^*$.*

Theorem II.3 ([22]). *Different characters of G are "orthogonal", namely, for $\chi, \psi \in \hat{G}$,*

$$\sum_{x \in G} \overline{\chi(x)}\psi(x) = |G| \cdot \mathit{\Delta}_{\chi,\psi}, \tag{1}$$

where $\mathit{\Delta}_{\chi,\psi} = \begin{cases} 1, & \chi = \psi; \\ 0, & \chi \neq \psi. \end{cases}$

Theorem II.4. *let χ be a group character for the finite Abelian group G. Then, $\overline{\chi}(g) = \chi^{-1}(g)$ for all $g \in G$.*

Proof. According to the definition of "$\star$", $\mathbf{1}_G(g) = \chi \star (\chi^{-1})(g) = \chi(g)\chi^{-1}(g) = 1$. In addition, Lemma II.1 implies that $\|\chi(g)\|^2 = \chi(g)\overline{\chi}(g) = 1$. Thus, we have $\chi(g)\overline{\chi}(g) = \chi(g)\chi^{-1}(g)$, which in turn implies that $\overline{\chi}(g) = \chi^{-1}(g)$. □

B. Fourier Transformations over Finite Abelian Groups

Definition II.4 (Fourier Transformation)**.** *Let $f : G \to \mathbb{C}$ be a function from a finite Abelian group G to $\mathbb{C}$. Then, the function $\hat{f} : \hat{G} \to \mathbb{C}$ defined as $\hat{f} : \chi \mapsto \sum_{x \in G} f(x)\chi(x)$ is called a Fourier transformation of f.*

Example II.2. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function and $\chi \in \widehat{\mathbb{F}_2^n}$ be a group character such that $\chi(x) = (-1)^{a \cdot x}$ for some $a \in \mathbb{F}_2^n$. Then,*

$$\hat{f}(\chi) = \sum_{x \in \mathbb{F}_2^m} f(x)\chi(x) = \sum_{x \in \mathbb{F}_2^m} f(x)(-1)^{a \cdot x},$$

which corresponds to the Walsh-Hadamard transformation.

Definition II.5 (Inverse Fourier Transformation)**.** *Let $h : \hat{G} \to \mathbb{C}$ be a function, where G is a finite Abelian group. Then, the function $\tilde{h} : G \to \mathbb{C}$ defined as $\tilde{h} : x \mapsto \frac{1}{|G|} \sum_{\chi \in \hat{G}} h(x)\overline{\chi}(x)$ is called the inverse Fourier transformation of h.*

Theorem II.5. *Let $f : G \to \mathbb{C}$ be a function from a finite Abelian group G to $\mathbb{C}$. Then, $\tilde{\hat{f}} = f$.*

Next, we define the convolution operator "$*$", and the reader is kindly reminded that "$\star$" and "$*$" are different operators in this paper.

Definition II.6 (Convolution)**.** *Let f and g be functions from $(G, +)$ to $\mathbb{C}$. Then, the convolution $f * g$ of f and g is defined as*

$$(f * g)(x) = \sum_{y \in G} f(x - y)g(y).$$

Theorem II.6. *Let f and g be functions from $(G, +)$ to $\mathbb{C}$. Then, $\widehat{f * g}(\chi) = \hat{f}(\chi)\hat{g}(\chi)$.*

III. Differential Probability, Correlation of Linear Approximations and Linearity over Abelian Groups

In this section, we revisit the differential probability and the correlation of linear approximations over finite Abelian groups, based on which we give the definition and a (trivial) lower bound of the nonlinearity of functions over the Abelian Group.

Definition III.1. *Let $(G, +)$ and $(H, +)$ be two finite Abelian groups, and $F : G \to H$ be a function. The probability of the differential of F with input difference $g \in G$ and output difference $h \in H$ is defined as*

$$\Pr[g \xrightarrow{F} h] = \frac{\delta_F(g, h)}{|G|},$$

where $\delta_F(g, h) = |\{x \in G | F(x) - F(x - g) = h\}|$.

Example III.1. *For any function $F : G \to H$, $\delta_F(0, 0) = |G|$.*

Example III.2. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function. For $(\alpha, \beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. $\Pr[\alpha \xrightarrow{F} \beta] = 2^{-n}\delta_F(\alpha, \beta)$, where $\delta_F(\alpha, \beta) = |\{x \in \mathbb{F}_2^n | F(x) \oplus F(x \oplus \alpha) = \beta\}|$.*

Example III.3. *Let $F : G \to H$ be a function with $G = H = (\mathbb{Z}_{2^n}, \boxplus)$. For $a, b \in \mathbb{Z}_{2^n}$, we have*

$$\Pr[a \xrightarrow{F} b] = \frac{\delta_F(a,b)}{2^n},$$

where $\delta_F(a,b) = |\{x \in G | F(x) \boxplus (-F(x \boxplus (-a))) = b\}|$.

Let $S \subseteq \mathbb{Z}$ be a set of integers. We use $\min^+(S)$ to denote the minimum positive number in S. For example, $\min^+(S) = 2$ for $S = \{0, 3, 5, 5, 3, 0, 2\}$.

Definition III.2. *For a set $\mathscr{F}$ of functions from a finite Abelian group $(G, +)$ to another finite Abelian group $(H, +)$, we denote*

$$\rho_{G,H}^{\mathscr{F}} = \min{}^+\{\delta_F(a,b) : F \in \mathscr{F}, a \in G, b \in H\}.$$

When G, H, and $\mathscr{F}$ are clear from the context, we may omit the superscript and subscript for simplicity.

Example III.4. *Let $\mathscr{F}$ be the set of all vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then, $\rho_{\mathbb{F}_2^n,\mathbb{F}_2^n}^{\mathscr{F}} = 2$. For instance, for $(x_1, x_2, \cdots, x_n) \in \mathbf{F}_2^n$, the vectorial Boolean functions $f : \mathbb{F}_2^n \to \mathbf{F}_2^n$ is defined as*

$$(x_1, x_2, \cdots, x_n) \mapsto (x_1 \wedge x_n, x_2 \wedge x_1, \cdots, x_n \wedge x_{n-1}).$$

If we let $a = (1, 1, 1, \cdots, 1)$ and $b = (1, 1, 0, \cdots, 0)$, we have $\delta_f(a,b) = 2$ ([23] Theorem 2).

Definition III.3 ([18], [19])**.** *Let G and H be two finite Abelian groups, and $F : G \to H$ be a function. The correlation of the linear approximation of F with input character (or mask) $\psi \in \hat{G}$ and output character (or mask) $\chi \in \hat{H}$ is defined as*

$$\mathcal{C}_{\psi,\chi}^F = \frac{1}{|G|} \sum_{x \in G} \overline{\psi}(x) \chi(F(x)).$$

Example III.5. *The correlation $\mathcal{C}_{u,v}^F$ of the linear approximation of a vectorial boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with input mask $u \in \mathbb{F}_2^n$ (corresponding to the character $x \mapsto (-1)^{u \cdot x}$) and output mask $v \in \mathbb{F}_2^n$ (corresponding to the character $x \mapsto (-1)^{v \cdot x}$) is defined as*

$$\mathcal{C}_{u,v}^F = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} (-1)^{v \cdot F(x)} = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x \oplus v \cdot F(x)}.$$

Example III.6 ([18], [19])**.** *The correlation $\mathcal{C}_{a,b}^F$ of the linear approximation of a function $F : \mathbb{Z}_n \to \mathbb{Z}_m$ with input mask $a \in \mathbb{Z}_n$ (corresponding to the character $x \mapsto e^{2\pi iax/n}$) and output mask $b \in \mathbb{Z}_m$ (corresponding to the character $x \mapsto e^{2\pi ibx/m}$) is defined as*

$$\mathcal{C}_{a,b}^F = \frac{1}{n} \sum_{x \in \mathbb{Z}_n} e^{-2\pi iax/n} e^{2\pi ibF(x)/m}.$$

Example III.7 ([19])**.** *The correlation* $\mathcal{C}^{\boxplus}_{a,b}$ *of the modulo addition* $\boxplus$ *with input mask* $(a,b) \in (\mathbb{Z}_{2^n}, \mathbb{Z}_{2^n})$ *(corresponding to the character* $(x,y) \mapsto e^{2\pi iax/2^n} e^{2\pi iby/2^n}$*) and output mask* $c \in \mathbb{Z}_{2^n}$ *(corresponding to the character* $x \mapsto e^{2\pi icx/2^n}$*) can be calculated as:*

$$\begin{aligned}\mathcal{C}^F_{(a,b),c} =& 2^{-2n} \sum_{x,y\in\mathbb{Z}_{2^n}} e^{2\pi iax/2^n} e^{2\pi iby/2^n} e^{2\pi ic(x\boxplus y)/2^n} \\ =& 2^{-2n} \sum_{x,y\in\mathbb{Z}_{2^n}} e^{2\pi iax/2^n} e^{2\pi iby/2^n} e^{-2\pi icx/2^n} e^{-2\pi icy/2^n} \\ =& 2^{-n} \sum_{x\in\mathbb{Z}_{2^n}} e^{2\pi i(a-c)x/2^n}\, 2^{-n} \sum_{y\in\mathbb{Z}_{2^n}} e^{2\pi i(b-c)y/2^n} \\ =& \varDelta_{a,c}\ \varDelta_{b,c} = \begin{cases} 1, & a=b=c; \\ 0, & \textit{others.} \end{cases}\end{aligned}$$

For the correlation of Linear Approximations over a finite Abelian group, we have the following property:

Lemma III.1. *Let* ψ *and* χ *be characters of the finite Abelian groups* G *and* H *respectively, and* $F : G \to H$ *be a function. Then,* $\overline{\mathcal{C}^F_{\psi,\chi}} = \mathcal{C}^F_{\psi^{-1},\chi^{-1}}$.

Proof. According to Definition III.3 and Theorem II.4, we have

$$\begin{aligned}\overline{\mathcal{C}^F_{\psi,\chi}} =& \frac{1}{|G|} \sum_{x\in G} \overline{\overline{\psi}(x)\chi(F(x))} = \frac{1}{|G|} \sum_{x\in G} \overline{\overline{\psi}(x)}\,\overline{\chi}(F(x)) \\ =& \frac{1}{|G|} \sum_{x\in G} \overline{\psi^{-1}}(x)\chi^{-1}(F(x)) = \mathcal{C}^F_{\psi^{-1},\chi^{-1}}.\end{aligned}$$

□

In the following, we generalize the definition of the nonlinearity of functions to any finite Abelian groups and give its lower bound based on the Parseval equation which is the corollary of Lemma IV.3 in Section IV.

Definition III.4 (Linearity over Abelian Groups)**.** *Let* $(G,+)$ *and* $(H,+)$ *be two finite Abelian groups and* $F :$ $G \to H$ *be a Boolean function. The linearity* λ_F *of function* F *over finite Abelian groups is defined as:*

$$\lambda_F = \max_{(\psi,\chi)\in(\hat{G},\hat{H}),\chi\neq\boldsymbol{1}_H} \|\mathcal{C}_{\psi,\chi}\|. \tag{2}$$

Theorem III.1 (Parseval equation over Abelian Grounps)**.**

$$\sum_{\psi\in\hat{G}} \boldsymbol{C}_{\psi,\chi}\overline{\mathcal{C}_{\psi,\chi}} = \sum_{\psi\in\hat{G}} \|\mathcal{C}_{\psi,\chi}\|^2 = 1. \tag{3}$$

Proof. For $\delta_F(a,b)$, when $b \neq 0_H$, $\delta_F(0_G,b) = 0$ and $\delta_F(0_G,0_H) = |G|$. For any $\psi \in \hat{G}$, $\chi \in \hat{H}$, $\psi(0_G) = 1$, $\chi(0_H) = 1$.

Let $\delta_F(0_G,b) = f(b)$, for any $\chi \in \hat{H}$, we then have:

$$\hat{f}(\chi) = \sum_{g\in H} \chi(g)\delta_F(0_G,g) = \chi(0)\delta_F(0_G,0_H) = |G|.$$

From Lemma IV.3, it follows that:

$$f(b) = \frac{|G|}{|H|} \sum_{\psi \in \hat{G}, \chi \in \hat{H}} \chi(b)\, \mathcal{C}_{\psi,\chi}\overline{\mathcal{C}_{\psi,\chi}}.$$

Then,

$$\begin{aligned}\hat{f}(\chi) =& \frac{|G|}{|H|} \sum_{g \in H} \chi(g) \sum_{\chi_1 \in \hat{H}} \sum_{\psi \in \hat{G}} \chi_1(g)\, \mathcal{C}_{\psi,\chi_1}\overline{\mathcal{C}_{\psi,\chi_1}} \\ =& \frac{|G|}{|H|} \sum_{\chi_1 \in \hat{H}} \sum_{\psi \in \hat{G}} \mathcal{C}_{\psi,\chi_1}\overline{\mathcal{C}_{\psi,\chi_1}} \sum_{g \in H} \chi(g)\chi_1(g) \\ =& |G| \sum_{\chi_1 \in \hat{H}} \sum_{\psi \in \hat{G}} \mathcal{C}_{\psi,\chi_1}\overline{\mathcal{C}_{\psi,\chi_1}} \mathit{\Delta}_{\overline{\psi},\chi_1} \\ =& |G| \sum_{\psi \in \hat{G}} \mathcal{C}_{\psi,\overline{\chi}}\overline{\mathcal{C}_{\psi,\overline{\chi}}}.\end{aligned}$$

Thus,

$$\sum_{\psi \in \hat{G}} \mathcal{C}_{\psi,\chi}\overline{\mathcal{C}_{\psi,\chi}} = \sum_{\psi \in \hat{G}} \|\mathcal{C}_{\psi,\chi}\|^2 = 1.$$

□

According to the Parseval equation, we have $\lambda_F \geq |G|^{-\frac{1}{2}}$:

Corollary III.1. $\lambda_F \geq |G|^{-\frac{1}{2}}$.

Proof. Note that

$$\lambda_F = \max_{\chi \in \hat{H}, \chi \neq \mathbf{1}} \max_{\psi \in \hat{G}} (|\mathcal{C}_{\psi,\chi}|^2)^{\frac{1}{2}} = \max_{\chi \in \hat{H}, \chi \neq \mathbf{1}} (\max_{\psi \in \hat{G}} |\mathcal{C}_{\psi,\chi}|^2)^{\frac{1}{2}}.$$

For $\max_{\psi \in \hat{G}} |\mathcal{C}_{\psi,\chi}|^2$, we then have:

$$\max_{\psi \in \hat{G}} |\mathcal{C}_{\psi,\chi}|^2 \geq \frac{\sum_{\psi \in \hat{G}} |\mathcal{C}_{\psi,\chi}|^2}{|G|} = \frac{1}{|G|}.$$

Thus, $\lambda_F \geq |G|^{-\frac{1}{2}}$. □

IV. The Link between the Differential Cryptanalysis and Linear Cryptanalysis over Finite Abelian Groups

In this section, we establish new links between differential cryptanalysis and Linear cryptanalysis over finite Abelian group, which will be used in Section VI to deduce a tighter lower bound of λ_F.

We first define two special functions θ_F and θ_F^*.

Definition IV.1. *Let $(G,+)$ and $(H,+)$ be two finite Abelian groups, and $F : G \to H$ be a function. The functions $\theta_F : (G,H) \to \mathbb{R}$ and $\theta_F^* : (G,H) \to \mathbb{R}$ are defined as*

$$\theta_F(a,b) = \begin{cases} 1, & b = F(a) \\ 0, & b \neq F(a) \end{cases},$$

and

$$\theta_F^*(a,b) = \begin{cases} 1, & b = -F(-a) \\ 0, & b \neq -F(-a) \end{cases}.$$

For θ_F and θ_F^*, we have the following property.

Lemma IV.1. *$\hat{\theta}_F(\psi,\chi) = |G|\mathcal{C}_{\psi^{-1},\chi}$, and $\hat{\theta}_F^*(\psi,\chi) = \hat{\theta}_F(\psi^{-1},\chi^{-1})$.*

Proof. For $\hat{\theta}_F(\psi,\chi)$, we have

$$\begin{aligned}\hat{\theta}_F(\psi,\chi) =& \sum_{(a,b)\in(G,H)} \chi(b)\ \psi(a)\ \theta_F(a,b) = \sum_{a\in G} \chi(F(a))\ \psi(a) \\ =& \sum_{a\in G} \chi(F(a))\ \overline{\overline{\psi(a)}} = \sum_{a\in G} \chi(F(a))\ \overline{\psi^{-1}(a)} \\ =& |G|\mathcal{C}_{\psi^{-1},\chi}.\end{aligned}$$

For $\hat{\theta}_F^*(\psi,\chi)$, we have

$$\begin{aligned}\hat{\theta}_F^*(\psi,\chi) =& \sum_{(a,b)\in(G,H)} \chi(b)\psi(a)\ \theta_F^*(a,b) \\ =& \sum_{a\in G} \chi(-F(-a))\ \psi(a).\end{aligned}$$

Since for any $g \in G$ and $h \in H$, $\chi(g)\chi(-g) = 1$ and $\psi(h)\psi(-h) = 1$, $\chi(-g) = \chi^{-1}(g)$, and $\psi^{-1}(h) = \psi(-h)$. Consequently,

$$\begin{aligned}\hat{\theta}_F^*(\psi,\chi) =& \sum_{a\in G} \chi(-F(-a))\psi(-(-a)) \\ =& \sum_{-a\in G} \chi^{-1}(F(-a))\psi^{-1}(-a) = \hat{\theta}_F(\psi^{-1},\chi^{-1}).\end{aligned}$$

□

Lemma IV.2. *$(\theta_F^* * \theta_F)(a,b) = \delta_F(a,b)$.*

Proof. According to Definition II.6, we have

$$\begin{aligned}(\theta_F^* * \theta_F)(a,b) =& \sum_{(x,y)\in(G,H)} \theta_F^*(a-x,b-y)\theta_F(x,y) \\ =& \sum_{(x,y)\in(G,H)} \theta_F^*(a-x,b-F(x)) \\ =& |\{x \in G : b - F(x) = -F(-(a-x))\}| \\ =& |\{x \in G : F(x) - F(a-x) = b\}| \\ =& \delta_F(a,b).\end{aligned}$$

□

Lemma IV.3. *Let G and H be finite Abelian groups, and $F : G \to H$ be a function. Then, we have*

$$\delta_F(a,b) = \frac{|G|}{|H|} \sum_{\chi \in \hat{H}, \psi \in \hat{G}} \overline{\psi}(a)\chi(b)\mathcal{C}^F_{\psi,\chi}\overline{\mathcal{C}^F_{\psi,\chi}},$$

or equivalently,

$$\mathcal{C}^F_{\psi,\chi}\overline{\mathcal{C}^F_{\psi,\chi}} = \frac{1}{|G|^2} \sum_{a \in G, b \in H} \psi(a)\overline{\chi}(b)\delta_F(a,b).$$

Proof. According to the Lemma IV.2, we have

$$\begin{aligned}
\delta_F(a,b) =& (\theta^*_F * \theta_F)(a,b) = (\widetilde{\widehat{\theta^*_F * \theta_F}})(a,b) = (\widetilde{\hat{\theta^*_F} \times \hat{\theta}_F})(a,b) \\
=& \frac{1}{|G|}\frac{1}{|H|} \sum_{\psi \in \hat{G}, \lambda \in \hat{H}} \overline{\psi(a)}\ \overline{\lambda(b)}\ \hat{\theta}^*_F(\psi,\lambda)\hat{\theta}_F(\psi,\lambda) \\
=& \frac{|G|}{|H|} \sum_{\psi \in \hat{G}, \lambda \in \hat{H}} \overline{\psi(a)}\ \overline{\lambda(b)}\ \mathcal{C}_{\psi,\lambda^{-1}}\mathcal{C}_{\psi^{-1},\lambda} \\
=& \frac{|G|}{|H|} \sum_{\psi \in \hat{G}, \chi \in \hat{H}} \overline{\psi(a)}\chi(b)\ \mathcal{C}_{\psi,\chi}\mathcal{C}_{\psi^{-1},\chi^{-1}} \\
=& \frac{|G|}{|H|} \sum_{\psi \in \hat{G}, \chi \in \hat{H}} \overline{\psi(a)}\ \chi(b)\ \mathcal{C}_{\psi,\chi}\overline{\mathcal{C}_{\psi,\chi}}.
\end{aligned}$$

Equivalently, we can see that:

$$\begin{aligned}
&\sum_{a \in G, b \in H} \psi(a)\overline{\chi(b)}\delta_F(a,b) \\
=& \frac{|G|^2}{|G||H|} \sum_{a \in G, b \in H} \psi(a)\overline{\chi(b)} \sum_{\sigma \in \hat{G}, \tau \in \hat{H}} \overline{\sigma(a)}\ \tau(b)\ \mathcal{C}_{\sigma,\tau}\overline{\mathcal{C}_{\sigma,\tau}} \\
=& \sum_{\sigma \in \hat{G}, \tau \in \hat{H}} \mathcal{C}_{\sigma,\tau}\overline{\mathcal{C}_{\sigma,\tau}} \sum_{a \in G} \psi(a)\overline{\sigma(a)} \sum_{b \in H} \tau(b)\overline{\chi(b)} \\
=& |G|^2\mathcal{C}^F_{\psi,\chi}\overline{\mathcal{C}^F_{\psi,\chi}}.
\end{aligned}$$

□

Gathering Lemma IV.1, Lemma IV.2 and Lemma IV.3, we finally draw the conclusion in Theorem IV.1, which gives the relationship between the differential probability and correlation of linear approximations:

Theorem IV.1. *Let G and H be finite Abelian groups, and $F : G \to H$ be a function. Then, we have*

$$\sum_{\psi \in \hat{G}} \sum_{\chi \in \hat{H}, \chi \neq \mathbf{1}} \|\mathcal{C}^F_{\psi,\chi}\|^4 = \frac{|H|}{|G|^3} \sum_{a \in G, a \neq 0} \sum_{b \in H} \delta_F(a,b)^2 + \frac{|H|}{|G|} - 1.$$

In addition, we call $\sum_{a \in G, a \neq 0} \sum_{b \in H} \delta_F(a,b)^2$ as the square sum of Differential Probability.

Proof. According to Lemma IV.3, $\|\mathcal{C}^F_{\psi,\chi}\|^2 = \mathcal{C}^F_{\psi,\chi}\overline{\mathcal{C}^F_{\psi,\chi}} = \frac{1}{|G|^2}\widehat{\delta}_F(\overline{\psi},\chi)$. Therefore, we have

$$
\begin{aligned}
&\sum_{\psi\in\hat{G}}\sum_{\chi\in\hat{H},\chi\neq\mathbf{1}_H}\|\mathcal{C}^F_{\psi,\chi}\|^4\\
=&\sum_{\psi\in\hat{G}}\sum_{\chi\in\hat{H}}\|\mathcal{C}^F_{\psi,\chi}\|^4-\sum_{\psi\in\hat{G}}\|\mathcal{C}^F_{\psi,\mathbf{1}}\|^4\\
=&\frac{1}{|G|^4}\sum_{\psi\in\hat{G}}\sum_{\chi\in\hat{H}}(\widehat{\delta}_F(\overline{\psi},\chi))^2-\sum_{\psi\in\hat{G}}\|\mathcal{C}^F_{\psi,\mathbf{1}}\|^4\\
=&\frac{1}{|G|^4}\sum_{\psi\in\hat{G}}\sum_{\chi\in\hat{H}}\widehat{\delta_F*\delta_F}(\overline{\psi},\chi)-\sum_{\psi\in\hat{G}}\|\mathcal{C}^F_{\psi,\mathbf{1}}\|^4\\
=&\frac{1}{|G|^4}\sum_{\psi\in\hat{G}}\sum_{\chi\in\hat{H}}\widehat{\delta_F*\delta_F}(\psi,\chi)-\sum_{\psi\in\hat{G}}\|\mathcal{C}^F_{\psi,\mathbf{1}}\|^4\\
=&\frac{|H|}{|G|^3}\frac{1}{|G||H|}\sum_{\psi\in\hat{G}}\sum_{\chi\in\hat{H}}\overline{\psi}(0)\overline{\chi}(0)\widehat{\delta_F*\delta_F}(\psi,\chi)-\sum_{\psi\in\hat{G}}\|\mathcal{C}^F_{\psi,\mathbf{1}}\|^4\\
=&\frac{|H|}{|G|^3}(\delta_F*\delta_F)(0,0)-\sum_{\psi\in\hat{G}}\|\mathcal{C}^F_{\psi,\mathbf{1}}\|^4.
\end{aligned}
$$

Due to the fact that $\mathcal{C}^F_{\psi,\mathbf{1}_H} = \begin{cases}1,\ \psi=\mathbf{1}_G\\ 0,\ \text{otherwise}\end{cases}$, it follows that

$$\sum_{\psi\in\hat{G}}\sum_{\chi\in\hat{H},\chi\neq\mathbf{1}_H}\|\mathcal{C}^F_{\psi,\chi}\|^4=\frac{|H|}{|G|^3}\sum_{a\in G,a\neq0}\sum_{b\in H}\delta_F(a,b)^2+\frac{|H|}{|G|}-1.$$

□

Example IV.1. *Applying Theorem IV.1 to a vectorial Boolean function $F:\mathbb{F}_2^n\to\mathbb{F}_2^m$, we have*

$$\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^m,v\neq0}\|\mathcal{C}^F_{u,v}\|^4=2^{m-3n}\sum_{\substack{a\in\mathbb{F}_2^n\\ a\neq0}}\sum_{b\in\mathbb{F}_2^m}\delta_F(a,b)^2+2^{m-n}-1.$$

This is consistent with the result derived in [10].

V. On the lower bound of the square sum of Differential Probability

In this section, we consider $\sum_{a\in G,a\neq0}\sum_{b\in H}\delta_F(a,b)^2$ (the right part) in the equation in Theorem IV.1. We calculate its lower bound so that we can get the lower bound of the linear approximations (the left part), which will be directly used to deduce a tighter lower bound of λ_F in Section VI.

Let $G=\{a_1,\cdots,a_{|G|-1},a_{|G|}\}$ and $H=\{b_1,\cdots,b_{|H|-1},b_{|H|}\}$ with $a_{|G|}=0$. Then,

$$\sum_{a\in G,a\neq0}\sum_{b\in H}\delta_F(a,b)^2=\sum_{i=1}^{|G|-1}\sum_{j=1}^{|H|}\delta_F(a_i,b_j)^2. \tag{4}$$

Let $\boldsymbol{d} = (d_1, \cdots, d_H)$, $\mathbb{D}_{G,H} = \{\boldsymbol{d} \in \mathbb{Z}^{|H|} : d_i = 0 \text{ or } d_i \geq \rho^{\mathscr{F}}_{G,H}, \text{ for } 0 \leq i \leq |H|, \text{ and } \sum_{i=1}^{|H|} d_i = |G|\}$, and $\xi_{G,H} = \min_{\boldsymbol{d} \in \mathbb{D}_{G,H}} \sum_{j=1}^{|H|} d_j$. It is easy to see that for any $i \in \{1, 2, \cdots, |G| - 1\}$, $\sum_{j=1}^{|H|} \delta_F(a_i, b_j) = |G|$, and for $1 \leq j \leq |H|$, $\delta_F(a_i, b_j) = 0$ or $\rho^{\mathscr{F}}_{G,H} \leq \delta_F(a_i, b_j) \leq |G|$. Therefore, for any $i \in \{1, \cdots, |G| - 1\}$,

$$\sum_{j=1}^{|H|} \delta_F(a_i, b_j)^2 \geq \xi_{G,H}. \tag{5}$$

Consequently, $\sum_{i=1}^{|G|-1} \sum_{j=1}^{|H|} \delta_F(a_i, b_j)^2$ is lower bounded by $(|G| - 1)\xi_{G,H}$. Next, we derive $\xi_{G,H}$.

Definition V.1. *Let $(G, +)$ and $(H, +)$ be two finite Abelian groups, and*

$$\zeta_{G,H} = \min_{\boldsymbol{d} \in \mathbb{D}_{G,H}} \sum_{i=1}^{|H|} \left(d_i - \frac{|G|}{|H|} \right)^2 \tag{6}$$

where $\boldsymbol{d} = (d_1, \cdots, d_H)$ and

$$\mathbb{D}_{G,H} = \{\boldsymbol{d} \in \mathbb{Z}^{|H|} : d_i = 0 \text{ or } d_i \geq \rho, \text{ for } 0 \leq i \leq |H|, \text{ and } \sum_{i=1}^{|H|} d_i = |G|\}.$$

We can see the following relationship between $\xi_{G,H}$ and $\zeta_{G,H}$.

Lemma V.1.

$$\zeta_{G,H} + \frac{|G|^2}{|H|} = \xi_{G,H}.$$

Proof. For $\boldsymbol{d} = (d_1, \cdots, d_H) \in S$, we can see that

$$\begin{aligned}
&\sum_{i=1}^{|H|} \left(d_i - \frac{|G|}{|H|} \right)^2 + \frac{|G|^2}{|H|} \\
=& \left(\sum_{i=1}^{|H|} {d_i}^2 - 2\frac{|G|}{|H|} \sum_{i=1}^{|H|} d_i + \frac{|G|^2}{|H|^2} \sum_{i=1}^{|H|} 1 \right) + \frac{|G|^2}{|H|} \\
=& \left(\sum_{i=1}^{|H|} {d_i}^2 - 2\frac{|G|^2}{|H|} + \frac{|G|^2}{|H|} \right) + \frac{|G|^2}{|H|} \\
=& \sum_{i=1}^{|H|} {d_i}^2.
\end{aligned}$$

Thus, we have

$$\zeta_{G,H} + \frac{|G|^2}{|H|} = \xi_{G,H}.$$

□

Obviously, according to the Lemma V.1, if we know the value of $\zeta_{G,H}$, then we can get $\xi_{G,H}$ immediately. Next, we will give the value of $\zeta_{G,H}$ under different cases.

A. $|H| \mid |G|$ and $\rho \leq \lfloor \frac{|G|}{|H|} \rfloor$

Setting $d_i = \frac{|G|}{|H|}$, we get $\zeta_{G,H} = 0$, and thus $\xi_{G,H} = \frac{|G|^2}{|H|}$ according to Lemma V.1.

B. $|H| \nmid |G|$ and $\rho \leq \lfloor \frac{|G|}{|H|} \rfloor$

Under such cases, we can see that the $\zeta_{G,H}$ can be reached over a subset of $\mathbb{D}_{G,H}$:

Lemma V.2. *Let $(G,+)$ and $(H,+)$ be two finite Abelian groups with $|H| \nmid |G|$ and $\rho \leq \lfloor \frac{|G|}{|H|} \rfloor$. Then*

$$\zeta_{G,H} = \min_{\boldsymbol{d} \in \mathbb{D}_{G,H}} \sum_{i=1}^{|H|} \left(d_i - \frac{|G|}{|H|} \right)^2 = \min_{\boldsymbol{d} \in \mathbb{B}_{G,H}} \sum_{i=1}^{|H|} \left(d_i - \frac{|G|}{|H|} \right)^2$$

where $\boldsymbol{d} = (d_1, \cdots, d_H)$,

$$\mathbb{D}_{G,H} = \{\boldsymbol{d} \in \mathbb{Z}^{|H|} : d_i = 0 \text{ or } d_i \geq \rho, \text{ for } 0 \leq i \leq |H|, \text{ and } \sum_{i=1}^{|H|} d_i = |G|\},$$

$$\mathbb{B}_{G,H} = \{\boldsymbol{d} \in \mathbb{Z}^{|H|} : d_i \geq \lfloor \frac{|G|}{|H|} \rfloor, \text{ for } 0 \leq i \leq |H|, \text{ and } \sum_{i=1}^{|H|} d_i = |G|\},$$

and $\mathbb{B}_{G,H}$ is a subset of $\mathbb{D}_{G,H}$.

Proof. See Appendix A. □

Then, when $|H| \nmid |G|$ and $\rho \leq \lfloor \frac{|G|}{|H|} \rfloor$, we can get $\xi_{G,H}$.

Lemma V.3. *For the two finite Abelian groups $(G,+)$ and $(H,+)$, when $|H| \nmid |G|$ and $\rho \leq \lfloor \frac{|G|}{|H|} \rfloor$, we have:*

$$\zeta_{G,H} = r \cdot \left(\lfloor \frac{|G|}{|H|} \rfloor + 1 - \frac{|G|}{|H|} \right)^2 + (|H| - r) \cdot \left(\lfloor \frac{|G|}{|H|} \rfloor - \frac{|G|}{|H|} \right)^2$$

Accordingly,

$$\xi_{G,H} = \left(r \cdot \left(\lfloor \frac{|G|}{|H|} \rfloor + 1 \right)^2 + (|H| - r) \cdot \lfloor \frac{|G|}{|H|} \rfloor^2 \right)$$

where $r = |G| - |H| \cdot \lfloor \frac{|G|}{|H|} \rfloor$ and $r < |H|$.

Proof. For a given $\boldsymbol{d} = (d_1, \cdots, d_{|H|}) \in \mathbb{B}_{G,H}$, we assume that there are k entries of $\boldsymbol{d}$ strictly larger than $\lfloor \frac{|G|}{|H|} \rfloor$. Without loss of generality, we may assume that the k entries are $d_1, \cdots, d_k$, and thus $d_{k+1} = \cdots = d_{|H|} = \lfloor \frac{|G|}{|H|} \rfloor$. Let

$$d_1 = \lfloor \frac{|G|}{|H|} \rfloor + \epsilon_1, \ \cdots, \ d_k = \lfloor \frac{|G|}{|H|} \rfloor + \epsilon_k$$

with $\epsilon_1, \cdots, \epsilon_k \geq 1$, and $r = \sum_{j=1}^{k} \epsilon_j$. Then

$$|G| = d_1 + \cdots + d_k + d_{k+1} + \cdots + d_{|H|} = r + |H| \lfloor \frac{|G|}{|H|} \rfloor. \tag{7}$$

Therefore, $r = |G| - |H| \cdot \lfloor \frac{|G|}{|H|} \rfloor$. Note that $r < |H|$, otherwise $r + |H| \lfloor \frac{|G|}{|H|} \rfloor \geq |H|(1 + \lfloor \frac{|G|}{|H|} \rfloor) > |H| \frac{|G|}{|H|} = |G|$.

Since $|H| - k > r - k = \sum_{j=1}^{k} (\epsilon_j - 1)$, for each $j \in \{1, \cdots, k\}$, we can select a new set of $\epsilon_j - 1$ entries of $\boldsymbol{d}$ (denoted as $d_{j_1}, \cdots, d_{j_{\epsilon_j - 1}}$) whose values are all $\lfloor \frac{|G|}{|H|} \rfloor$. Then we set the values of these entries and d_j to $\lfloor \frac{|G|}{|H|} \rfloor + 1$. We call the new vector $\boldsymbol{d}'$, and it is easy to see that $\boldsymbol{d}' \in \mathbb{B}_{G,H}$. It satisfies that r components are equal to $\lfloor \frac{|G|}{|H|} \rfloor + 1$ and the remaining $|H| - r$ components are equal to $\lfloor \frac{|G|}{|H|} \rfloor$.

Let $m = \lfloor \frac{|G|}{|H|} \rfloor + 1 - \frac{|G|}{|H|}$, for any positive integer a, the following inequality holds:

$$(m + a - 1)^2 + (a - 1)(m - 1)^2 \geq am^2$$

And it's easy to verify that the inequality is equivalent to the inequality $a^2 \geq a$ where $a \geq 1$.

Because of the above inequality, for each $j \in \{1, \cdots, k\}$, we can see that

$$\begin{aligned}
&\left(d_j - \frac{|G|}{|H|}\right)^2 + \sum_{i=1}^{\epsilon_j - 1} \left(d_{j_i} - \frac{|G|}{|H|}\right)^2 \\
=&(m + \epsilon_j - 1) + (\epsilon_j - 1)(m-1) \\
\geq& \epsilon_j m^2 = \left(d'_j - \frac{|G|}{|H|}\right)^2 + \sum_{i=1}^{\epsilon_j - 1} \left(d'_{j_i} - \frac{|G|}{|H|}\right)^2
\end{aligned}$$

where $m = \lfloor \frac{|G|}{|H|} \rfloor + 1 - \frac{|G|}{|H|}$.

Thus, for all $\boldsymbol{d} = (d_1, \cdots, d_{|H|}) \in \mathbb{D}_{G,H}$ such that $d_i \geq \lfloor \frac{|G|}{|H|} \rfloor$ where $1 \leq i \leq |H|$,

$$\begin{aligned}
&\sum_{j=1}^{|H|} \left(d_j - \frac{|G|}{|H|}\right)^2 \\
\geq& \sum_{j=1}^{|H|} \left(d'_j - \frac{|G|}{|H|}\right)^2 \\
=& r \cdot \left(\lfloor \frac{|G|}{|H|} \rfloor + 1 - \frac{|G|}{|H|}\right)^2 + (|H| - r) \cdot \left(\lfloor \frac{|G|}{|H|} \rfloor - \frac{|G|}{|H|}\right)^2 .
\end{aligned}$$

In summary, we know that

$$\zeta_{G,H} = r \cdot \left(\lfloor \frac{|G|}{|H|} \rfloor + 1 - \frac{|G|}{|H|}\right)^2 + (|H| - r) \cdot \left(\lfloor \frac{|G|}{|H|} \rfloor - \frac{|G|}{|H|}\right)^2$$

where $r = |G| - |H| \cdot \lfloor \frac{|G|}{|H|} \rfloor$, $r < |H|$. □

C. $\rho > \lfloor \frac{|G|}{|H|} \rfloor$ and $\rho \mid |G|$

Under such cases, we have:

Lemma V.4. *For the two finite Abelian groups $(G, +)$ and $(H, +)$, when $\rho > \lfloor \frac{|G|}{|H|} \rfloor$ and $\rho \mid |G|$, we have:*

$$\zeta_{G,H} = |G|\rho - \frac{|G|^2}{|H|}.$$

Accordingly,

$$\xi_{G,H} = |G|\rho.$$

Proof. For any $\boldsymbol{d} = (d_1, \cdots, d_{|H|}) \in \mathbb{D}_{G,H}$, for $1 \leq i \leq |H|$, due to $d_i \geq \rho$ or $d_i = 0$, we have:

$$\left(d_i - \frac{|G|}{|H|}\right)^2 \geq \left(\rho - 2\frac{|G|}{|H|}\right) \cdot q + \frac{|G|^2}{|H|^2},$$

where $q = 0$ or $q = \rho$.

For $\boldsymbol{d}' \in \mathbb{D}_{G,H}$, we suppose that $d_i' = \rho$ for $1 \le i \le \frac{|G|}{\rho}$ and $d_i' = 0$ for $\frac{|G|}{\rho} + 1 \le i \le |H|$. Thus, according to the above inequality for any $\boldsymbol{d} \in \mathbb{D}_{G,H}$, we have:

$$\begin{aligned}\sum_{i=1}^{|H|} \left(d_i - \frac{|G|}{|H|}\right)^2 \ge& \sum_{i=1}^{|H|} \left(\rho - 2\frac{|G|}{|H|}\right) \cdot d_i' + \sum_{i=1}^{|H|} \frac{|G|^2}{|H|^2} \\ =& \sum_{i=1}^{|G|/\rho} \left(\rho^2 - \frac{|G|}{|H|}\rho\right) + \frac{|G|^2}{|H|} \\ =& |G|\rho - \frac{|G|^2}{|H|}.\end{aligned}$$

□

D. $\rho > \lfloor \frac{|G|}{|H|} \rfloor$ *and* $\rho \nmid |G|$

Under such cases, we can see that the $\zeta_{G,H}$ can be reached over a subset of $\mathbb{D}_{G,H}$:

Lemma V.5. *Let $(G,+)$ and $(H,+)$ be two finite Abelian groups with $\rho > \lfloor \frac{|G|}{|H|} \rfloor$ and $\rho \nmid |G|$. Then*

$$\zeta_{G,H} = \min_{\boldsymbol{d} \in \mathbb{D}_{G,H}} \sum_{i=1}^{|H|} \left(d_i - \frac{|G|}{|H|}\right)^2 = \min_{\boldsymbol{d} \in \mathbb{B}_{G,H}} \sum_{i=1}^{|H|} \left(d_i - \frac{|G|}{|H|}\right)^2$$

where $\boldsymbol{d} = (d_1, \cdots, d_H)$, $m \cdot \rho = |G| - n$,

$$\mathbb{D}_{G,H} = \{\boldsymbol{d} \in \mathbb{Z}^{|H|} : d_i = 0 \text{ or } d_i \ge \rho, \text{ for } 0 \le i \le |H|, \text{ and } \sum_{i=1}^{|H|} d_i = |G|\},$$

$$\mathbb{B}_{G,H} = \{\boldsymbol{d} \in \mathbb{Z}^{|H|} : \text{ for } 0 \le i \le |H|, \text{ the number of } d_i \text{ such that } d_i > 0 \text{ is } m\}.$$

and $\mathbb{B}_{G,H}$ is a subset of $\mathbb{D}_{G,H}$.

Proof. See Appendix A. □

Then, when $\rho > \lfloor \frac{|G|}{|H|} \rfloor$ and $\rho \nmid |G|$, we can get $\xi_{G,H}$.

Lemma V.6. *For the two finite Abelian groups $(G,+)$ and $(H,+)$, when $\rho > \lfloor \frac{|G|}{|H|} \rfloor$ and $\rho \nmid |G|$, we have:*

$$\zeta_{G,H} = \left((m-h) \cdot \left(c - \frac{|G|}{|H|}\right)^2 + h \cdot \left(c + 1 - \frac{|G|}{|H|}\right)^2\right)$$

Accordingly,

$$\xi_{G,H} = (m-h) \cdot c^2 + h \cdot (c+1)^2$$

where $m \cdot \rho = |G| - n$, $n < \rho$ and $h = |G| - c \cdot m$, $h < m$.

Proof. For any $\boldsymbol{d} = (d_1, \cdots, d_{|H|}) \in \mathbb{B}_{G,H}$, for convenience, we can let $d_i = \rho + r_i$ for $1 \le i \le m$ and $d_i = 0$ for $m + 1 \le i \le |H|$. In addition, $\sum_{i=1}^{|H|} r_i = n$, where $n = |G| - m \cdot \rho$.

Let $w = \rho - \frac{|G|}{|H|}$, then we can see that, for any $z, j \in \{1, \cdots, m\}$ such that $r_z > r_j$, we have

$$(w + r_z)^2 + (w + r_j)^2 \ge (w + r_z - 1)^2 + (w + r_j + 1)^2$$

if and only if $r_z - r_j = 1$, the equation holds.

For $\boldsymbol{d'} = (d'_1, \cdots, d'_{|H|}) \in \mathbb{B}_{G,H}$, we let $d'_i = d_i$, $i \in \{1, \cdots, m\}$ except for z, j and $r'_z = r_z - 1$, $r'_j = r_j + 1$. Then, from above inequality, we have

$$\sum_{i=0}^{|H|}(d_i - \frac{|G|}{|H|})^2 \geq \sum_{i=0}^{|H|}(d'_i - \frac{|G|}{|H|})^2$$

if and only if $r_z - r_j = 1$. Therefore the equation holds.

Thus, for $\boldsymbol{d'} = (d'_1, \cdots, d'_{|H|}) \in \mathbb{B}_{G,H}$ such that $d'_z, d'_j \geq \rho$ and $|d'_z - d'_j| \leq 1$ holds for any $z, j \in \{1, \cdots, |H|\}$, we have

$$\begin{aligned}
&\sum_{i=1}^{|H|}\left(d'_i - \frac{|G|}{|H|}\right)^2 \\
&= \left((m-h) \cdot \left(c - \frac{|G|}{|H|}\right)^2 + h \cdot \left(c + 1 - \frac{|G|}{|H|}\right)^2\right) \\
&= \min_{\boldsymbol{d} \in \mathbb{B}_{G,H}} \sum_{i=1}^{|H|}\left(d_i - \frac{|G|}{|H|}\right)^2,
\end{aligned}$$

where $m \cdot \rho = |G| - n$, $n < \rho$ and $h = |G| - c \cdot m$, $h < m$.

According to the Lemma V.5,

$$\zeta_{G,H} = \left((m-h) \cdot \left(c - \frac{|G|}{|H|}\right)^2 + h \cdot \left(c + 1 - \frac{|G|}{|H|}\right)^2\right)$$

where $m \cdot \rho = |G| - n$, $n < \rho$ and $h = |G| - c \cdot m$, $h < m$. □

VI. A Tighter bound of λ_F

In this section, we give a tighter lower bound of the linearity λ_F by gathering the results in the previous two sections Section IV and Section V. Note that we already give a lower bound of λ_F in Section IV, but we must point out that such a lower bound is meaningful only when $\rho^{\mathscr{F}}_{G,H} \leq \lfloor \frac{|G|}{|H|} \rfloor$, $|G| \mid |H|$ (see [11]). The bound of the linearity given in this section is reasonable under different cases.

According to the Parseval equation, we can drive a relationship between λ_F and $\sum_{\psi \in \hat{G}} \sum_{\chi \in \hat{H}, \chi \neq \mathbf{1}_H} \|\mathcal{C}^F_{\psi,\chi}\|^4$:

Lemma VI.1.

$$(\lambda_F)^2 \cdot (|H| - 1) \geq \sum_{\psi \in \hat{G}} \sum_{\chi \in \hat{H}, \chi \neq \boldsymbol{1}_H} \|\mathcal{C}^F_{\psi,\chi}\|^4$$

if and only if the equation holds when $\|\mathcal{C}^F_{\psi,\chi}\| = \lambda_F$ or $\|\mathcal{C}^F_{\psi,\chi}\| = 0$, for all $\psi \in \hat{G}$, $\chi \in \hat{H}$, $\chi \neq \boldsymbol{1}_H$.

Proof. For any $\psi \in \hat{G}$,$\chi \in \hat{H}$ and $\chi \neq \mathbf{1}_H$, we have:

$$(\lambda_F)^2 \cdot \|\mathcal{C}^F_{\psi,\chi}\|^2 \geq \|\mathcal{C}^F_{\psi,\chi}\|^4$$

if and only if the equation holds when $\|\mathcal{C}^F_{\psi,\chi}\| = \xi_{G,H}$ or $\|\mathcal{C}^F_{\psi,\chi}\| = 0$. Thus,

$$(\lambda_F)^2 \cdot \sum_{\psi \in \hat{G}} \sum_{\chi \in \hat{H}, \chi \neq \mathbf{1}_H} \|\mathcal{C}^F_{\psi,\chi}\|^2 \geq \sum_{\psi \in \hat{G}} \sum_{\chi \in \hat{H}, \chi \neq \mathbf{1}_H} \|\mathcal{C}^F_{\psi,\chi}\|^4.$$

By combining Theorem III.1, we get the inequality. □

Combing with Lemma IV.1 and Lemma V.1, we get:

Lemma VI.2. *Let $(G,+)$ and $(H,+)$ be two finite Abelian groups and $F : G \to H$ be a function. For a set $\mathscr{F}$ of functions from a finite Abelian group $(G,+)$ to another finite Abelian group $(H,+)$, we have:*

$$\sum_{\psi \in \hat{G}} \sum_{\chi \in \hat{H}, \chi \neq \mathbf{1}_H} \|\mathcal{C}^F_{\psi,\chi}\|^4 \geq \frac{|H|(|G|-1)}{|G|^3} \cdot \xi_{G,H} + \frac{|H|}{|G|} - 1,$$

where the value of $\xi_{G,H}$ can be obtained in Table I

Then, by gathering Lemma VI.1, Lemma VI.2, Lemma V.3, Lemma V.4 , Lemma V.6, according to $|G|$, $|H|$ and $\rho^{\mathscr{F}}_{G,H}$, we get the lower bound of λ_F:

Theorem VI.1. *Let $(G,+)$ and $(H,+)$ be two finite Abelian groups and $F : G \to H$ be a function. For a set $\mathscr{F}$ of functions from a finite Abelian group $(G,+)$ to another finite Abelian group $(H,+)$, we have:*

$$\lambda_F \geq \sqrt{\frac{1}{|H|-1}\left(\frac{|H|(|G|-1)}{|G|^3} \cdot \xi_{G,H} + \frac{|H|}{|G|} - 1\right)},$$

where the value of $\xi_{G,H}$ can be obtained in Table I, and the low bound of λ_F is summarized as Table II.

Remark VI.1. *1. For the condition $|G| \mid |H|$ and $\rho^{\mathscr{F}}_{G,H} \leq \lfloor \frac{|G|}{|H|} \rfloor$, [11] has proved that the optimal function against differential cryptanalysis satisfies $\lambda_F = (\sqrt{|G|})^{-1}$.*
2. If we consider the set $\mathscr{F}$ of functions from finite Abelian group $(G,+)$ to another finite Abelian group $(H,+)$ such that $\rho^{\mathscr{F}}_{G,H} = |G|$ (The set contains all "affine" functions from a finite Abelian group $(G,+)$ to another finite Abelian group $(H,+)$), then we have $\lambda_F \geq 1$ from Theorem VI.1.
3. Likely, for the function set $\mathscr{F}$ such that $\rho^{\mathscr{F}}_{G,H} > \frac{|G|}{2}$, according to Theorem VI.1, we can get $\lambda_F \geq 1$.

Example VI.1. *We use the function $f(x) = \left((-1)^{x \bmod 2} \cdot x^2\right) \bmod p$ (p is a prime number), which was proposed in [16] (see the fifth row of Table 1 in [16]), to demonstrate the correctness of Theorem VI.1. The input domain is set as $\mathbb{F}_p$, which has good properties against the algebraic attack [16]. And for all possible prime numbers not greater than 100, we calculate the λ_f of $f(x)$. Then, we do a comparison with the lower bound in Theorem VI.1 (See Table III). If the input domain is set as $\mathbb{F}_q$, where $q > p$, the result is shown in Table IV. And if the input domain is set as $\mathbb{F}_q$, where $q < p$, the result is shown in Table V.*

VII. Conclusion and Future Work

For the lower bound of the linearity λ_F of a function $F : G \to H$ mapping from finite Abelian group G to H, we complete the generalization from $\mathbf{F}_2^n$ to finite Abelian groups according to the links we established between linear cryptanalysis and differential cryptannlysis. Compared with Pott's work [11], we give more general results.

On the functions the function from $\mathbb{F}_2^m$ to $\mathbb{F}_2^n$, some works [24] [25] [26] [27] [28] constructed a series of functions that can reach the low bound of λ_F, which are called bent functions ($m > n$) or almost bent functions ($m \leq n$). Such (almost) bent functions can be used to construct DES-like block cipher that are resistant to differential attacks and linear attacks. Likely, for some specific finite Abelian groups G and H, can we construct a series of functions that can reach the low bound of λ_F? We left it as an open problem. In addition, the notion of differential probability can be extended into finite groups [29]. In such a case, can we obtain same result?

References

[1] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings* (T. Helleseth, ed.), vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397, Springer, 1993. 1, 3

[2] B. S. K. Jr. and M. J. B. Robshaw, "Linear cryptanalysis using multiple approximations," in *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings* (Y. Desmedt, ed.), vol. 839 of *Lecture Notes in Computer Science*, pp. 26–39, Springer, 1994. 1

[3] A. Bogdanov, G. Leander, K. Nyberg, and M. Wang, "Integral and multidimensional linear distinguishers with correlation zero," in *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings* (X. Wang and K. Sako, eds.), vol. 7658 of *Lecture Notes in Computer Science*, pp. 244–261, Springer, 2012. 1

[4] M. Hermelin, J. Y. Cho, and K. Nyberg, "Multidimensional linear cryptanalysis of reduced round Serpent," in *Information Security and Privacy, 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings* (Y. Mu, W. Susilo, and J. Seberry, eds.), vol. 5107 of *Lecture Notes in Computer Science*, pp. 203–215, Springer, 2008. 1

[5] A. Biryukov, C. D. Cannière, and M. Quisquater, "On multiple linear approximations," in *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings* (M. K. Franklin, ed.), vol. 3152 of *Lecture Notes in Computer Science*, pp. 1–22, Springer, 2004. 1

[6] J. A. Davis and L. Poinsot, "G-perfect nonlinear functions," *Des. Codes Cryptogr.*, vol. 46, no. 1, pp. 83–96, 2008. 1

[7] M. Hermelin, J. Y. Cho, and K. Nyberg, "Multidimensional extension of Matsui's algorithm 2," in *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers* (O. Dunkelman, ed.), vol. 5665 of *Lecture Notes in Computer Science*, pp. 209–227, Springer, 2009. 1

[8] A. Bogdanov and M. Wang, "Zero correlation linear cryptanalysis with reduced data complexity," in *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers* (A. Canteaut, ed.), vol. 7549 of *Lecture Notes in Computer Science*, pp. 29–48, Springer, 2012. 1

[9] K. Nyberg, "Perfect nonlinear S-Boxes," in *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings* (D. W. Davies, ed.), vol. 547 of *Lecture Notes in Computer Science*, pp. 378–386, Springer, 1991. 2, 3

[10] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," in *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pp. 356–365, 1994. 2, 3, 4, 12

[11] A. Pott, "Nonlinear functions in Abelian groups and relative difference sets," *Discret. Appl. Math.*, vol. 138, no. 1-2, pp. 177–193, 2004. 2, 3, 4, 17, 18

[12] M. R. Albrecht, L. Grassi, C. Rechberger, A. Roy, and T. Tiessen, "MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity," in *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I* (J. H. Cheon and T. Takagi, eds.), vol. 10031 of *Lecture Notes in Computer Science*, pp. 191–219, 2016. 2

[13] M. R. Albrecht, L. Grassi, L. Perrin, S. Ramacher, C. Rechberger, D. Rotaru, A. Roy, and M. Schofnegger, "Feistel structures for MPC, and more," in *Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security, Luxembourg, September 23-27, 2019, Proceedings, Part II* (K. Sako, S. A. Schneider, and P. Y. A. Ryan, eds.), vol. 11736 of *Lecture Notes in Computer Science*, pp. 151–171, Springer, 2019. 2

[14] L. Grassi, R. Lüftenegger, C. Rechberger, D. Rotaru, and M. Schofnegger, "On a generalization of substitution-permutation networks: The HADES design strategy," in *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II* (A. Canteaut and Y. Ishai, eds.), vol. 12106 of *Lecture Notes in Computer Science*, pp. 674–704, Springer, 2020. 2

[15] L. Grassi, D. Khovratovich, C. Rechberger, A. Roy, and M. Schofnegger, “Poseidon: A new hash function for zero-knowledge proof systems,” in *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021* (M. Bailey and R. Greenstadt, eds.), pp. 519–535, USENIX Association, 2021. 2

[16] L. Grassi, D. Khovratovich, S. Rønjom, and M. Schofnegger, “The Legendre Symbol and the Modulo-2 operator in Symmetric Schemes over $\mathbb{F}_p^n$ preimage attack on full Grendel,” *IACR Trans. Symmetric Cryptol.*, vol. 2022, no. 1, pp. 5–37, 2022. 2, 18

[17] L. Grassi, S. Onofri, M. Pedicini, and L. Sozzi, “Invertible quadratic non-linear layers for MPC-/FHE-/ZK-friendly schemes over fnp application to poseidon,” *IACR Trans. Symmetric Cryptol.*, vol. 2022, no. 3, pp. 20–72, 2022. 2

[18] T. Baignères, J. Stern, and S. Vaudenay, “Linear cryptanalysis of non-binary ciphers,” in *Selected Areas in Cryptography, 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17, 2007, Revised Selected Papers* (C. M. Adams, A. Miri, and M. J. Wiener, eds.), vol. 4876 of *Lecture Notes in Computer Science*, pp. 184–211, Springer, 2007. 2, 7

[19] T. Beyne, “Linear cryptanalysis of FF3-1 and FEA,” in *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I* (T. Malkin and C. Peikert, eds.), vol. 12825 of *Lecture Notes in Computer Science*, pp. 41–69, Springer, 2021. 3, 7, 8

[20] T. Beyne, “A geometric approach to linear cryptanalysis,” in *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I* (M. Tibouchi and H. Wang, eds.), vol. 13090 of *Lecture Notes in Computer Science*, pp. 36–66, Springer, 2021. 3

[21] J. Daemen, R. Govaerts, and J. Vandewalle, “Correlation matrices,” in *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings* (B. Preneel, ed.), vol. 1008 of *Lecture Notes in Computer Science*, pp. 275–285, Springer, 1994. 3

[22] A. Terras, *Fourier analysis on finite groups and applications*. Cambridge University Press, 1999. 4, 5

[23] S. Kölbl, G. Leander, and T. Tiessen, “Observations on the SIMON block cipher family,” vol. 9215, pp. 161–185, 2015. 7

[24] A. Canteaut, P. Charpin, and H. Dobbertin, “Binary m-sequences with three-valued crosscorrelation: A proof of welch’s conjecture,” *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 4–9, 2000. 18

[25] A. Canteaut, P. Charpin, and H. Dobbertin, “A new characterization of almost bent functions,” in *Fast Software Encryption, 6th International Workshop, FSE ’99, Rome, Italy, March 24-26, 1999, Proceedings* (L. R. Knudsen, ed.), vol. 1636 of *Lecture Notes in Computer Science*, pp. 186–200, Springer, 1999. 18

[26] H. Dobbertin, “Almost perfect nonlinear power functions on GF(2^n): The welch case,” *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1271–1275, 1999. 18

[27] K. Nyberg, “Differentially uniform mappings for cryptography,” in *Advances in Cryptology - EUROCRYPT ’93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings* (T. Helleseth, ed.), vol. 765 of *Lecture Notes in Computer Science*, pp. 55–64, Springer, 1993. 18

[28] H. Dobbertin, “Almost perfect nonlinear power functions on GF(2^n): The niho case,” *Inf. Comput.*, vol. 151, no. 1-2, pp. 57–72, 1999. 18

[29] L. Poinsot, “Non Abelian bent functions,” *Cryptogr. Commun.*, vol. 4, no. 1, pp. 1–23, 2012. 19

Appendix

Appendix Proof of Lemma V.2

Proof. Firstly, for $\boldsymbol{d} \in \mathbb{D}_{G,H}$, we show that if $\min(\boldsymbol{d}) < \lfloor\frac{|G|}{|H|}\rfloor$, then $\max(\boldsymbol{d}) > \lfloor\frac{|G|}{|H|}\rfloor$, or $\max(\boldsymbol{d}) \geq \lfloor\frac{|G|}{|H|}\rfloor + 1$, where $\min(\boldsymbol{d})$ ($\max(\boldsymbol{d})$) denotes the minimum (maximum) component of vector $\boldsymbol{d}$. Otherwise, we have

$$\sum_{i=1}^{|H|} d_i < \lfloor\frac{|G|}{|H|}\rfloor + (|H|-1)\cdot\lfloor\frac{|G|}{|H|}\rfloor = |H|\lfloor\frac{|G|}{|H|}\rfloor < |H|\frac{|G|}{|H|} = |G|.$$

For a given $\boldsymbol{d} \in \mathbb{D}_{G,H}$ with $\min(\boldsymbol{d}) < \lfloor\frac{|G|}{|H|}\rfloor$, we can transform it into another $\boldsymbol{d}' \in \mathbb{D}_{G,H}$ by increasing the smallest entry of $\boldsymbol{d}$ by 1 and decreasing the maximal entry of $\boldsymbol{d}$ by 1. Next, we show that

$$\sum_{i=1}^{|H|}\left(d_i - \frac{|G|}{|H|}\right)^2 \geq \sum_{i=1}^{|H|}\left(d_i' - \frac{|G|}{|H|}\right)^2. \tag{8}$$

Let $\min(\boldsymbol{d}) = \lfloor \frac{|G|}{|H|} \rfloor - \triangledown$ and $\max(\boldsymbol{d}) = \lfloor \frac{|G|}{|H|} \rfloor + \triangle$ with $\triangledown \geq 1$ and $\triangle \geq 1$, and $u = \frac{|G|}{|H|} - \lfloor \frac{|G|}{|H|} \rfloor$. Then,

$$\begin{aligned}
&\left(\min(\boldsymbol{d}) - \frac{|G|}{|H|}\right)^2 + \left(\max(\boldsymbol{d}) - \frac{|G|}{|H|}\right)^2 \\
&- \left(\min(\boldsymbol{d'}) - \frac{|G|}{|H|}\right)^2 - \left(\max(\boldsymbol{d'}) - \frac{|G|}{|H|}\right)^2 \\
=&(u - \triangledown)^2 + (u + \triangle)^2 - (u - \triangledown + 1)^2 - (u + \triangle - 1)^2 \\
=&2(\triangledown + \triangle) - 2 > 0.
\end{aligned}$$

Therefore, we can successively apply the above transformation until $\min(\boldsymbol{d}) \geq \lfloor \frac{|G|}{|H|} \rfloor$.

□

Appendix Proof of Lemma V.5

Proof. Supposed that $|G| = m \cdot \rho + n$, $n < \rho$. Then, we can see that the number of nonzero components is at most m . Else, it will be in contradiction to $n < \rho$.

And we define the set $\mathbb{D}'_{G,H}$ as

$$\begin{aligned}
\mathbb{D}'_{G,H} = \{\boldsymbol{h} \in \mathbb{Z}^{|H|} : h_i = 0 \text{ or } h_i \geq \rho, \text{ for } 0 \leq i \leq |H|, \\
\text{and } \sum_{i=1}^{|H|} h_i = |G| - n\},
\end{aligned}$$

where $\boldsymbol{d} = (d_1, \cdots, d_H)$, n= $|G| - m \cdot \rho$.

For $\boldsymbol{h'} = (h'_1, \cdots, h'_{|H|}) \in \mathbb{D}'_{G,H}$, we suppose that $h'_i = \rho$, $1 \leq i \leq m$ and $h'_i = 0$, $m + 1 \leq i \leq |H|$. Then, like Lemma V.4, using same technique, we get

$$\sum_{i=1}^{|H|} \left(h'_i - \frac{|G|}{|H|}\right)^2 = \min_{\boldsymbol{h} \in \mathbb{D}'_{G,H}} \sum_{i=1}^{|H|} \left(h_i - \frac{|G|}{|H|}\right)^2. \tag{9}$$

Next, for any $\boldsymbol{d} = (d_1, \cdots, d_H) \in \mathbb{D}_{G,H}$, we suppose that there are p ($p \leq m < |H|$) nonzero components. For convenience we denote it as the first p components. Then, we define $\boldsymbol{d'} \in \mathbb{D}'_{G,H}$ from $\boldsymbol{d}$, where $d_i^{'} = 0$ for $p + 1 \leq i \leq |H|$ and $d_i^{'} = d_i - r_i$, $d_i \geq \rho$, $0 \leq r_i \leq d_i - \rho$ for $1 \leq i \leq p$. In addition, $\sum_{i=0}^{p} r_i = n$.

And we also define $\boldsymbol{d}^b = (d_1^b, \cdots, d_{|H|}^b) \in \mathbb{B}_{G,H}$, where $d_i^b = h'_i + r_i = \rho + r_i$ for $1 \leq i \leq p$ and $d_i^b = h'_i$ for $p + 1 \leq i \leq |H|$.

Then, for $1 \leq i \leq p$, due to

$$(2d'_i + r_i - 2\frac{|G|}{|H|})\ r_i \geq (2\rho + r_i - 2\frac{|G|}{|H|})\ r_i,$$

we can see that

$$\begin{aligned}
&\left(d_i^{'} + r_i - \frac{|G|}{|H|}\right)^2 - \left(d_i^{'} - \frac{|G|}{|H|}\right)^2 \\
\geq &\left(\rho + r_i - \frac{|G|}{|H|}\right)^2 - \left(\rho - \frac{|G|}{|H|}\right)^2.
\end{aligned} \tag{10}$$

Finally, according to Equation (9) and Inequality (10), we have:

$$
\begin{aligned}
&\left(\sum_{i=0}^{p}\left(d_i^{'}+r_i-\frac{|G|}{|H|}\right)^2-\left(d_i^{'}-\frac{|G|}{|H|}\right)^2\right)+\sum_{i=0}^{|H|}\left(d_i^{'}-\frac{|G|}{|H|}\right)^2\\
=&\sum_{i=0}^{|H|}\left(d_i-\frac{|G|}{|H|}\right)^2\\
&\geq\left(\sum_{i=0}^{p}\left(\rho+r_i-\frac{|G|}{|H|}\right)^2-\left(\rho-\frac{|G|}{|H|}\right)^2\right)+\sum_{i=0}^{|H|}\left(h_i'-\frac{|G|}{|H|}\right)^2\\
&=\sum_{i=0}^{|H|}\left(d_i^b-\frac{|G|}{|H|}\right)^2.
\end{aligned}
$$

□

TABLE I: Summary of $\xi_{G,H}$

Cases		$\xi_{G,H}$
$\rho_{G,H} \leq \lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor$	$\lvert H\rvert \mid \lvert G\rvert$	$\frac{\lvert G\rvert^2}{\lvert H\rvert}$
	$\lvert H\rvert \nmid \lvert G\rvert$	$(\lvert H\rvert - r) \cdot \lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor^2 + r \cdot \left(\lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor + 1\right)^2, \;\; r = \lvert G\rvert - \lvert H\rvert \cdot \lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor, r < \lvert H\rvert$
$\rho_{G,H} > \lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor$	$\rho \mid \lvert G\rvert$	$\lvert G\rvert \cdot \rho$
	$\rho \nmid \lvert G\rvert$	$(m-h) \cdot c^2 + h \cdot (c+1)^2, \;\; \begin{cases} m \cdot \rho = \lvert G\rvert - n, n < \rho \\ h = \lvert G\rvert - c \cdot m, h < m \end{cases}$

TABLE II: Summary of the low bound of λ_F

Cases		The low bound of λ_F
$\rho^{\mathscr{F}}_{G,H} \leq \lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor$	$\lvert H\rvert \mid \lvert G\rvert$	$\lvert G\rvert^{-\frac{1}{2}}$
	$\lvert H\rvert \nmid \lvert G\rvert$	$\sqrt{\frac{\lvert H\rvert(\lvert G\rvert-1)}{\lvert G\rvert^3(\lvert H\rvert-1)}\left(\lvert H\rvert\cdot\lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor^2+2r\cdot\lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor+r\right)+\frac{\lvert H\rvert-\lvert G\rvert}{\lvert G\rvert(\lvert H\rvert-1)}}, \quad r=\lvert G\rvert-\lvert H\rvert\cdot\lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor, r<\lvert H\rvert$
$\rho^{\mathscr{F}}_{G,H} > \lfloor\frac{\lvert G\rvert}{\lvert H\rvert}\rfloor$	$\rho^{\mathscr{F}}_{G,H} \mid \lvert G\rvert$	$\sqrt{\frac{\lvert H\rvert(\lvert G\rvert-1)}{\lvert G\rvert^2(\lvert H\rvert-1)}\rho^{\mathscr{F}}_{G,H}+\frac{\lvert H\rvert-\lvert G\rvert}{\lvert G\rvert(\lvert H\rvert-1)}}$
	$\rho^{\mathscr{F}}_{G,H} \nmid \lvert G\rvert$	$\sqrt{\frac{\lvert H\rvert(\lvert G\rvert-1)}{\lvert G\rvert^3(\lvert H\rvert-1)}\left((m-h)\cdot c^2+h\cdot(c+1)^2\right)+\frac{\lvert H\rvert-\lvert G\rvert}{\lvert G\rvert(\lvert H\rvert-1)}}, \quad \begin{cases} m\cdot\rho=\lvert G\rvert-n, n<\rho \\ h=\lvert G\rvert-c\cdot m, h<m \end{cases}$

TABLE III: The λ_F of $f(x)$ and the lower bound in Theorem VI.1 under different p

p	3	5	7	11	13	17	19
λ_F	1.000	0.724	0.785	0.633	0.717	0.575	0.542
Lower bound	0.577	0.447	0.378	0.302	0.277	0.243	0.229
p	23	29	31	37	41	43	47
λ_F	0.532	0.531	0.498	0.432	0.412	0.418	0.393
Lower bound	0.209	0.186	0.180	0.164	0.156	0.152	0.146
p	53	59	61	67	71	79	83
λ_F	0.385	0.372	0.356	0.350	0.334	0.311	0.306
Lower bound	0.137	0.130	0.128	0.122	0.119	0.113	0.110

TABLE IV: The result of $q > p$

q	5	7	11	13	17	19	23
p	3	5	7	11	13	17	19
λ_F	0.833	0.565	0.640	0.587	0.481	0.500	0.496
Lower bound	0.482	0.411	0.325	0.295	0.262	0.240	0.222
q	29	31	37	41	43	47	53
p	23	29	31	37	41	43	47
λ_F	0.402	0.433	0.366	0.406	0.382	0.386	0.345
Lower bound	0.200	0.185	0.175	0.163	0.156	0.151	0.144
q	59	61	67	71	79	83	
p	53	59	61	67	71	79	
λ_F	0.328	0.378	0.320	0.336	0.294	0.294	
Lower bound	0.136	0.130	0.127	0.123	0.117	0.112	

TABLE V: The result of $q < p$

q	3	5	7	11	13	17	19
p	5	7	11	13	17	19	23
λ_F	0.832	0.749	0.692	0.533	0.601	0.634	0.538
Lower bound	0.667	0.503	0.438	0.324	0.308	0.255	0.248
q	23	29	31	37	41	43	47
p	29	31	37	41	43	47	53
λ_F	0.489	0.476	0.426	0.414	0.403	0.395	0.393
Lower bound	0.229	0.192	0.194	0.172	0.160	0.159	0.154
q	53	59	61	67	71	79	
p	59	61	67	71	79	83	
λ_F	0.370	0.339	0.348	0.339	0.326	0.313	
Lower bound	0.144	0.132	0.134	0.126	0.125	0.115	