# Analysis on Boolean function in a restricted (biased) domain

Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy and Pantelimon Stănică

***Abstract*—Boolean functions are usually studied under the assumption that each input bit is considered independent and identically distributed. However, in the case of some stream ciphers, a keystream bit is generated by using a nonlinear Boolean function with inputs from a restricted domain. At Eurocrypt 2016, one such stream cipher (FLIP) has been proposed, where a Boolean function on $n$ variables was exploited with inputs of weight $\frac{n}{2}$ only. Recently, Carlet et al. studied several properties of such functions and obtained certain bounds on linear approximations of direct sum in the restricted domain. In this paper, we observe that for a direct sum like $f = f_1 + f_2$, the inputs to each sub-function $f_1$, $f_2$ do not follow a uniform distribution in the restricted domain. In this regard, we study the properties of Boolean functions by considering a general probability distribution on the inputs. We further obtain several bounds related to the biases of direct sums. Finally, we obtain a lower bound on the bias of the nonlinear filter function of FLIP. Our results provide a general framework to study security parameters of ciphers over restricted domain.**

***Index Terms*—Bias, Boolean Function, FLIP, Pseudo-Randomness, Restricted Domain, Sequences, Stream Cipher,**

## I. Introduction

FINDING an efficient homomorphic encryption scheme using symmetric key cryptography is a current trend of research. In this direction, recent study shows that an efficient stream cipher can provide significant efficiency in homomorphic encryption. One important work that came in this direction is [1]. In 2017, Méaux [5] first presented the design specification of one stream cipher, which supports homomorphic encryption. The cipher, which is named FLIP, was cryptanalyzed by Duval et al. in Crypto 2016 [3]. Later, the modified design of FLIP (which resists the attack introduced at Crypto 2016) was proposed at Eurocrypt 2016 [6]. The keystream bit of the FLIP stream cipher is computed by using a nonlinear filter function defined over a restricted domain. A detailed study on Boolean functions over a restricted domain is done by Carlet et al. [2] and Mesnager et al. [8].

In this paper we observe that a different technique needs to be followed to study the Boolean function defined over restricted (or biased i.e., not uniform) domain. We first note that the design specification of a stream cipher, which supports homomorphic encryption, must be very simple to maintain error growth of the underlined homomorphic encryption scheme. To maintain the error growth the nonlinear filter function used in this kind of stream cipher has very simple Algebraic Normal Form (ANF). In fact the nonlinear filter function must have many linear terms and the degree of the function has to be quite low. From the design specification of the FLIP stream cipher it can be noticed that the intersection of variables' sets involved in any two monomials of the function is empty. With this kind of restrictions, this function does not carry good cryptographic properties. Hence, the cipher requires a large number of variables to provide a desirable security. Due to this, the state size of FLIP is very large and the nonlinear filter function has very simple ANF. Several properties of this kind of function can be easily checked if we assume that the inputs of the function follow a uniform distribution and they are mutually independent. However, in the case of the FLIP stream cipher this does not happen as the domain of the nonlinear filter function is restricted to a sub-domain. More specifically, each input point has a constant weight. Carlet et al. [2] and Mesnager et al. [8] have done mathematical analysis on this kind of function. Several theoretical bounds have been found in [2], [8]. Although specific numerical comparison is not available, in this paper, we try to fill this gap.

The design of a stream cipher is motivated towards generating pseudo-random (binary) sequence given a small initial seed. The general trend is to consider several linear or nonlinear feedback shift registers and to combine the outputs with certain nonlinear Boolean functions. The quality of the design is judged by how well a sequence close to uniform and true random stream can be simulated. While this field is already developed quite a bit, the present constraints arising out of homomorphic encryption opened up a new direction. The basic design ideas for such stream ciphers have been modified as we will explain in Section I-B. Based on that we need to study several components of the new design and analyse the quality of the sequence generated out of the evolution of such circuit. Our prime motivation here is to study the Boolean functions under a restricted scenario and the possibility of biases (this is related to non-randomness) in the output sequence due to that.

Now we would like to explain the problem in more technical point of view. The notations which are used for explanation are described in the Subsection I-A. In 2017, Carlet et al. [2] first observed that different cryptographic properties of a Boolean function change significantly when the domain of

S. Maitra is with Indian Statistical Institute, Kolkata, India.
E-mail: subho@isical.ac.in
B. Mandal is with CARAMBA, INRIA Nancy-Grand Est, France.
E-mail: bimal.mandal@inria.fr
T. Martinsen and P. Stănică are with Naval Postgraduate School, Monterey, USA; E-mail: {tmartins, pstanica}@nps.edu
D. Roy is with ERTL(E), STQC, Kolkata, India.
E-mail: roydibyendu.rd@gmail.com

This is a substantially revised and extended version of the paper [7] that appeared in the proceedings of Indocrypt 2018. This version includes additional results in Sections II-A III-A, III-B, III-C, III-D. Some results of [7] have been abridged and one may refer to [7] for other details. This paper has more than 50% new contributions over the conference version [7].

the function changes from $\mathbb{F}_2^n$ to a restricted subset $E \subset \mathbb{F}_2^n$. From the design specification of the FLIP stream cipher, it can be observed that the weight of the register (i.e., state) in each round remains fixed, due to the different state update function. Hence, the weight of the inputs of the nonlinear filter function remains constant. More specifically, if the size of the register (i.e., state) is $n$, then the weight of the inputs of the nonlinear filter function remains at $\frac{n}{2}$ for all rounds. Hence the nonlinear filter function always takes input from a restricted subset $E_{n,\frac{n}{2}} \subset \mathbb{F}_2^n$. From this observation, Carlet et al. [2] studied several cryptographic properties of Boolean functions on the restricted domain to provide the security parameters for FLIP. In 2018, Mesnager et al. [8] also investigated several properties of Boolean functions on restricted domain, although, the results proposed by Mesnager et al. [8] do not relate to the direct sum of Boolean functions. There is no numerical data related to the theoretical results available in the existing works [2], [8], and further, we would also like to mention that the results of [2], [8] are obtained by considering the complete function in the restricted domain.

In this paper, we look into the problem from a different direction. We first observe that if $\mathbf{x} \in E_{n,k}$ (see Section I-A for the definition) and $\mathbf{x} = \mathbf{x}_1||\mathbf{x}_2||\ldots||\mathbf{x}_n$ ($||$ denotes the concatenation) then $\mathbf{x}_1$, $\mathbf{x}_2$, …, $\mathbf{x}_n$ does not follow a uniform distribution. This motivates us to study the Walsh–Hadamard transform from a different perspective. We consider the exact probability distribution of each $\mathbf{x}_1$, $\mathbf{x}_2$, …, $\mathbf{x}_n$ to study the Walsh–Hadamard transform of each sub-function $f_i$, where $f(\mathbf{x}) = f_1(\mathbf{x}_1) + \ldots + f_n(\mathbf{x}_n)$. One may note that if the input $\mathbf{x}_i$ of $f_i$ does not follow a uniform distribution, then the cryptographic properties of $f_i$ differ significantly from the case when $\mathbf{x}_i$ follows uniform distribution. From this observation (considering the exact probability distribution), we expect to obtain tighter bound of the original bias of a Boolean function over a restricted domain as well as a tighter bound of the bias of nonlinear filter function of the FLIP stream cipher. A tighter bound definitely provide a better idea about the security parameters of the FLIP stream cipher.

**Contribution and Organization.** In our approach we consider the exact probability distributions of inputs of each sub-functions ($f_i$) of $f = \sum_i f_i$. With this consideration, we introduce our tools to analyse the properties of Boolean functions in Section II. In Section III we describe our prime motivation to obtain linear approximations of $n$-variable nonlinear Boolean functions whose domain is restricted to $E \subset \mathbb{F}_2^n$. The mathematical expressions we obtain in this direction are quite complicated to compare to the results obtain in [2], [8]. Note that the results obtain in [8] are not related to the direct sum of functions. We provide a clear numerical evidence for better understanding of our results in Section IV. The nonlinear filter function of $\text{FLIP}_{530}(42, 128, 360)$ is also considered to compare to the results of [2]. One can easily calculate that the maximum absolute Walsh–Hadamard transform value lies in the interval $[2^{-79}, 2^{-78}]$, when we assume that the inputs of the function follow a uniform distribution (i.e., the probability of each input is $\frac{1}{2^{530}}$). Hence, the original bias of the function in the uniform domain is quite low. However, our results show that when the inputs of the nonlinear filter function of $\text{FLIP}_{530}(42, 128, 360)$ is restricted to a subset $E_{530,265}$ (i.e., all points are of weight 265) then the restricted Walsh–Hadamard transform value is much higher. In fact, the maximum absolute value lies in $[2^{-18.49}, 2^{-13.59}]$. We obtain the upper bound of the bias (i.e., $2^{-13.59}$) by considering the theoretical results of [2] and the lower bound (i.e., $2^{-18.49}$) is obtained by using our tools. Our results fill the gap of the results obtained in [2] by calculating a lower bound of the bias of the function of the FLIP stream cipher on a large number of variables.

We first describe some background material, which are required for our work in the next section.

### A. Boolean functions

Let $\mathbb{F}_2$ be the two-element $\{0, 1\}$ field and $\mathbb{F}_2^n$ be the extension field over $\mathbb{F}_2$ of degree $n$. Let $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, x_2, \ldots, x_n) : \ x_i \in \mathbb{F}_2, \text{ for all } 1 \leq i \leq n\}$ be the vector space over $\mathbb{F}_2$ of dimension $n$. Let $\mathbf{x} = \mathbf{x}'||\mathbf{x}'' \in \mathbb{F}_2^n$ denotes the concatenation of $\mathbf{x}'$ and $\mathbf{x}''$. The total number of elements belonging to a set $S$ is known as the cardinality of the set and it is denoted by $|S|$. A Boolean function $f$ in $n$ variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ (i.e., $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$). The set of all Boolean functions in $n$ numbers of variables is denoted by $\mathcal{B}_n$. Any $n$-variable Boolean function $f$ has a unique polynomial representation, known as the *Algebraic Normal Form* (ANF) of $f$, namely

$$f(\mathbf{x}) = \sum_{\mathbf{a} \in \mathbb{F}_2^n} \mu_{\mathbf{a}} \left( \prod_{i=1}^{n} x_i^{a_i} \right), \text{ for all } \mathbf{x} \in \mathbb{F}_2^n, \text{ where } \mu_{\mathbf{a}} \in \mathbb{F}_2.$$

For any $\mathbf{x} \in \mathbb{F}_2^n$, the *Hamming weight* of $\mathbf{x}$ is denoted by $wt(\mathbf{x}) = \sum_{i=1}^{n} x_i$, where this sum is taken over the ring of integers. The *algebraic degree* of an $n$-variable Boolean function is defined as $\deg(f) = \max_{\mathbf{a} \in \mathbb{F}_2^n} \{wt(\mathbf{a}) : \ \mu_{\mathbf{a}} \neq 0\}$. The set of all elements $\mathbf{x} \in \mathbb{F}_2^n$ of weight $i$ is denoted by $E_{n,i}$, for all $0 \leq i \leq n$. The *support* of $f \in \mathcal{B}_n$ denoted by $\text{supp}(f)$ contains the set of all $\mathbf{x} \in \mathbb{F}_2^n$ such that $f(\mathbf{x}) = 1$. For an $n$-variable balanced Boolean function $|\text{supp}(f)| = 2^{n-1}$. A Boolean function $f \in \mathcal{B}_n$ is an *affine* function if the $deg(f)$ is at most 1. The set of all affine functions involving $n$ variables is denoted by $\mathcal{A}_n$ i.e., $\mathcal{A}_n = \{l_{\mathbf{a},\varepsilon} : \ \mathbf{a} \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2\}$, where $l_{\mathbf{a},\varepsilon}(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} + \varepsilon$, for all $\mathbf{x} \in \mathbb{F}_2^n$. An affine function is linear if $\varepsilon = 0$. The *Hamming distance* between any $f, g \in \mathcal{B}_n$ is denoted by $d_H(f, g)$ and defined as $d_H(f, g) = |\{\mathbf{x} \in \mathbb{F}_2^n : f(\mathbf{x}) \neq g(\mathbf{x})\}|$. The *correlation* between two $n$-variable Boolean functions $f$, $g$ is defined by

$$\mathsf{corr}(f, g) = \left| \frac{|\{\mathbf{x} : f(\mathbf{x}) = g(\mathbf{x})\}| - |\{\mathbf{x} : f(\mathbf{x}) \neq g(\mathbf{x})\}|}{2^n} \right|.$$

The correlation between an $n$-variable Boolean function $f$ and a linear function $l_{\mathbf{a},0}$ can be measured by *Walsh–Hadamard transform*, which is defined below,

$$\mathcal{W}_f(\mathbf{a}) = \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{a} \cdot \mathbf{x}}.$$

The correlation between the Boolean function $f$ and the linear function $l_{\mathbf{a},0}$ is the absolute value of the Walsh–Hadamard transform of $f \in \mathcal{B}_n$ at the point $\mathbf{a} \in \mathbb{F}_2^n$, i.e., $\mathsf{corr}(f, l_{\mathbf{a},0}) =$

$|\mathcal{W}_f(\mathbf{a})|$, for all $\mathbf{a} \in \mathbb{F}_2^n$. The set $\{|\mathcal{W}_f(\mathbf{a})| : \mathbf{a} \in \mathbb{F}_2^n\}$ provides the correlation between the Boolean function $f$ and the set of all possible linear functions $\{l_{\mathbf{a},0} : \mathbf{a} \in \mathbb{F}_2^n\}$. For any $f \in \mathcal{B}_n$, $\sum_{\mathbf{a}\in\mathbb{F}_2^n} \mathcal{W}_f(\mathbf{a})^2 = 1$, which is known as *Parseval's identity*. From this we obtain, $\max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f(\mathbf{a})| \geq \frac{1}{2^{n/2}}$. A Boolean function $f \in \mathcal{B}_n$ ($n$ even) is said to be bent if and only if the correlation between $f$ and $\{l_{\mathbf{a},0} | \mathbf{a} \in \mathbb{F}_2^n\}$ is $\frac{1}{2^{n/2}}$, i.e., $\mathsf{corr}(f, l_{\mathbf{a},0}) = |\mathcal{W}_f(\mathbf{a})| = 2^{-\frac{n}{2}}$, for all $\mathbf{a} \in \mathbb{F}_2^n$. Now to calculate the correlation between an $n$-variable Boolean function $f$ and an $n$-variable linear function $l_{\mathbf{a},0}$ over a restricted set $E \subset \mathbb{F}_2^n$, one needs to consider the inputs from the restricted set $E$. To define this notion over the restricted domain $E_{n,k}$, we consider a Boolean function $f \in \mathcal{B}_n$, which takes input from $E_{n,k}$. With this in mind, the (restricted domain) correlation between the Boolean function $f$ and a linear function $l_{\mathbf{a},0}$ is,

$$\mathsf{corr}^{(k)}(f, l_{\mathbf{a},0}) = \Big| \frac{|\{\mathbf{x} : f(\mathbf{x}) = l_{\mathbf{a},0}(\mathbf{x})\}| - |\{\mathbf{x} : f(\mathbf{x}) \neq l_{\mathbf{a},0}(\mathbf{x})\}|}{|E_{n,k}|} \Big|,$$

where $|E_{n,k}| = \binom{n}{k}$. To calculate the above mentioned correlation, we define the Walsh–Hadamard transform of an $n$-variable Boolean function in the restricted domain $E_{n,k}$, $0 \leq k \leq n$, as follows,

$$\mathcal{W}_f^{(k)}(\mathbf{a}) = \frac{1}{|E_{n,k}|} \sum_{\mathbf{x}\in E_{n,k}} (-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}}.$$

If $E$ is a subspace in $\mathbb{F}_2^n$, $\mathbf{b} \in \mathbb{F}_2^n$, then $E' = \mathbf{b} + E$ is a flat in $\mathbb{F}_2^n$. Also, $E^\perp = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{a} \cdot \mathbf{x} = 0, \text{ for all } \mathbf{x} \in E\}$ is the orthogonal complement of $E$. Further, we recall that for any $\mathbf{a} \in \mathbb{F}_2^n$, and subspace $E$ of $\mathbb{F}_2^n$ of dimension $\dim E$,

$$\sum_{\mathbf{x}\in E'} (-1)^{\mathbf{a}\cdot\mathbf{x}} = \begin{cases} 2^{\dim E}(-1)^{\mathbf{a}\cdot\mathbf{b}}, & \text{if } \mathbf{a} \in E^\perp; \\ 0, & \text{otherwise.} \end{cases} \quad (1)$$

Two more notations are defined here, which are used throughout the article.

**Definition 1.** *Let* $\mathbf{x} = (x_1, \ldots, x_n) \in E_{n,k}$ *and* $n = n_1 + n_2$, *and* $\mathbf{x}' = (x_1, \ldots, x_{n_1})$, $\mathbf{x}'' = (x_{n_1+1}, \ldots, x_n)$. *Then* $E_{n_1,i}^{n=n_1+n_2,k} = \{\mathbf{x}' \in \mathbb{F}_2^{n_1} \mid \mathbf{x} \in E_{n,k}, n = n_1 + n_2 \text{ and } wt(\mathbf{x}') = i\}$ *and* $E_{n_2,j}^{n=n_1+n_2,k} = \{\mathbf{x}'' \in \mathbb{F}_2^{n_2} \mid \mathbf{x} \in E_{n,k}, n = n_1 + n_2 \text{ and } wt(\mathbf{x}'') = j\}$.

Certainly, the above splitting process can be done for $n = n_1+n_2+n_3$, or, more generally, for $n = n_1+n_2+\cdots+n_q$, and so, $E_{n_1,i}^{n=n_1+n_2+n_3,k}$, $E_{n_2,j}^{n=n_1+n_2+n_3,k}$ and $E_{n_3,r}^{n=n_1+n_2+n_3,k}$, etc., can be inferred from Definition 1.

### *B. Design specification of the FLIP stream cipher*

In this section we describe a brief design specification of the FLIP stream cipher. More detailed design specification can be found in [6]. The FLIP cipher is based on three components: one register of length $n$, one pseudorandom number generator (PRNG), one nonlinear filter function $F$ involving $n$-variables. The register of the cipher is initialized by an $n$-bit secret key $K$ and a PRNG is initialized by an initialization vector $IV$. In each clock the PRNG generates a number which corresponds to a permutation. This permutation permutes the state bits of the register. Finally, the nonlinear filter function computes the keystream bit by taking the current state as input. The nonlinear filter function $F = f_1 + f_2 + f_3$ has three sub-functions $f_1$, $f_2$ and $f_3$, where $f_1$ is a linear function, $f_2$ is a quadratic bent function and $f_3$ is a special type of triangular function. The ANFs of $f_1$, $f_2$ are as follows: $f_1(x_0, x_1, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} x_i$, $f_2(x_0, x_1, \ldots, x_{2n-1}) = \sum_{i=0}^{n-1} x_{2i}x_{2i+1}$. The last function $f_3$ is the direct sum of $r$ many triangular function $T_k$, where each $T_k$ involves independent variables. The ANF of each triangular function is $T_k(x_0, x_1, \ldots, x_{\frac{k(k+1)}{2}-1}) = \sum_{i=1}^{k} \prod_{j=0}^{i-1} x_{j+\sum_{\ell=0}^{i-1}\ell}$. The final algebraic normal form of the nonlinear filter function $F$ is $F = f_1 + f_2 + \sum_{i=1}^{r} T_k$.

For our numerical analysis, we concentrate on the nonlinear filter function of FLIP(42, 128, ${}^8\Delta^9$) [6]. Here, $n = 530 = n_1 + n_2 + n_3$, $n_1 = 42$, $n_2 = 2 \times 64 = 128$ and $n_3 = 8 \cdot (1 + 2 + \cdots + 9) = 360$. The first sub-function $f_1$ contains 42 linear terms, the second sub-function $f_2$ contains 64 monomials of degree 2 and the last function $f_3$ is a direct sum of 8 triangular functions. Each triangular function has exactly one monomial of degree 1 to 9, i.e., each triangular function involves 45 variables.

The initial state of register of FLIP only takes an $n$-bit string of weight $\frac{n}{2}$. After that, in each round, the one permutation is generated by using a pseudorandom generator. This permutation permutes the index of state bits to update the state of the register. Then, the nonlinear filter function $F$ takes the updated state as input and generates keystream bit. Due to the update procedure of FLIP, the weight of the state of the register of FLIP remains fixed (i.e., $\frac{n}{2}$) in each round. So, every time, the keystream bit is computed by applying the nonlinear filter function $F$ on a state of weight $\frac{n}{2}$, i.e., $F(S_n^t) = z_t$, where $S_n^t$ is the $n$-bit state at $t$-th round and $wt(S_n^t) = \frac{n}{2}$.

An older version of FLIP [5] was cryptanalyzed by Duval et al. [3] at Crypto 2016. In that paper, two instances of FLIP stream cipher, namely, $n = 192$ ($n_1 = 47, n_2 = 40, n_3 = 105$) and $n = 400$ ($n_1 = 87, n_2 = 82, n_3 = 231$) were cryptanalyzed with the complexities $2^{54}$, $2^{68}$ respectively. Later in Eurocrypt 2016, Méaux et al. [6] proposed a modified design of FLIP, which prevents the attack proposed at Crypto 2016. Our work is based on the cipher proposed at Eurocrypt 2016.

## II. Tools for our analysis

Before describing our technical results, we first provide a brief overview on the existing results. The algebraic normal form of the nonlinear filter function ($F$) of FLIP is very simple. Due to this simplicity, the nonlinearity of the function $F$ can be easily calculated by using standard Walsh–Hadamard transform. It can be observed that in the uniform domain $2^{-79} < \max_{\mathbf{a}\in\mathbb{F}_2^{530}} |\mathcal{W}_F(\mathbf{a})| < 2^{-78}$. This is explained in the following section.

### *A. Walsh–Hadamard transform of the Boolean function in an instance of FLIP*

We compute the maximum value of the Walsh–Hadamard transform of the filter function in 530 variables, which is mentioned in [2, Table 1].

**Lemma 1.** *Let* $f \in \mathcal{B}_n$ *be defined by* $f(\mathbf{x}) = x_1x_2\cdots x_n$, *for all* $\mathbf{x} \in \mathbb{F}_2^n$. *Then* $\mathcal{W}_f(\mathbf{a}) = \delta_0(\mathbf{a}) - \frac{(-1)^{wt(\mathbf{a})}}{2^{n-1}}$, *for all* $\mathbf{a} \in \mathbb{F}_2^n$.

*Proof.* The Walsh–Hadamard transform of $f \in \mathcal{B}_n$ at $\mathbf{a} \in \mathbb{F}_2^n$ is

$$\begin{aligned}\mathcal{W}_f(\mathbf{a}) &= \frac{1}{2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} \\ &= \frac{1}{2^n}\Bigg(\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\mathbf{a}\cdot\mathbf{x}} - 2(-1)^{wt(\mathbf{a})}\Bigg) \\ &= \delta_0(\mathbf{a}) - \frac{(-1)^{wt(\mathbf{a})}}{2^{n-1}},\end{aligned}$$

and the lemma is shown. □

Using Lemma 1 and the Walsh–Hadamard spectrum of a bent function we get the next result.

**Theorem 1.** *Let $f \in \mathbb{F}_2^{530}$ be the direct sum $f(\mathbf{x}) = f_1(\mathbf{x}') + f_2(\mathbf{x}'') + f_3(\mathbf{x}''')$ of three functions $f_1 \in \mathcal{B}_{42}, f_2 \in \mathcal{B}_{128}, f_3 \in \mathcal{B}_{360}$, where $\mathbf{x} = \mathbf{x}'||\mathbf{x}''||\mathbf{x}'''$, $\mathbf{x}' \in \mathbb{F}_2^{42}, \mathbf{x}'' \in \mathbb{F}_2^{128}$ and $\mathbf{x}''' \in \mathbb{F}_2^{360}$, and $f_i$, $1 \le i \le 3$, are defined as in the FLIP cipher. Then, for any $\mathbf{a} \in \mathbb{F}_2^{530}$,*

$$\begin{aligned}\mathcal{W}_f(\mathbf{a}) = \frac{\delta_{\mathbf{1}}(\mathbf{a}')(-1)^{\tilde{f}_2(\mathbf{a}'')}}{2^{352}}\prod_{i=1}^{8}\delta_{\mathbf{1}}(\mathbf{a}'''_{i1})(-1)^{\mathbf{a}'''_{i21}\cdot\mathbf{a}'''_{i22}} \\ \left(4\delta_0(\mathbf{a}'''_{i3}) - (-1)^{wt(\mathbf{a}'''_{i3})}\right)\left(8\delta_0(\mathbf{a}'''_{i4}) - (-1)^{wt(\mathbf{a}'''_{i4})}\right)\cdots \\ \left(256\delta_0(\mathbf{a}'''_{i9}) - (-1)^{wt(\mathbf{a}'''_{i9})}\right),\end{aligned}$$

*where $\mathbf{a} = \mathbf{a}'||\mathbf{a}''||\mathbf{a}'''$, $\mathbf{a}' \in \mathbb{F}_2^{42}$, $\mathbf{a}'' \in \mathbb{F}_2^{128}$ and $\mathbf{a}''' \in \mathbb{F}_2^{360}$, and $\tilde{f}_2$ is the dual of $f_2$. Here, $\mathbf{a}''' = \mathbf{a}'''_1||\dots||\mathbf{a}'''_8$; $\mathbf{a}'''_i \in \mathbb{F}_2^{45}, 1 \le i \le 8$, $\mathbf{a}'''_i = \mathbf{a}'''_{i1}||\dots||\mathbf{a}'''_{i9}$; $\mathbf{a}'''_{ij} \in \mathbb{F}_2^j, 1 \le j \le 9$, and $\mathbf{a}'''_{i2} = \mathbf{a}'''_{i21}||\mathbf{a}'''_{i22}$.*

*Proof.* The first sub-function $f_1$ of the nonlinear filter function of the FLIP stream cipher is the linear function $f_1(\mathbf{x}') = \sum_{i=1}^{42} x_i$, for all $\mathbf{x}' \in \mathbb{F}_2^{42}$. The Walsh–Hadamard transform $f_1$ at the point $\mathbf{a}' \in \mathbb{F}_2^{42}$ is

$$\mathcal{W}_{f_1}(\mathbf{a}') = \frac{1}{2^{42}}\sum_{\mathbf{x}\in\mathbb{F}_2^{42}}(-1)^{(\mathbf{1}+\mathbf{a})\mathbf{x}} = \delta_{\mathbf{1}}(\mathbf{a}'),$$

where $\delta_{\mathbf{1}}(\mathbf{a}')$ is the Dirac function which is 1, if $\mathbf{a}' = \mathbf{1}$ and 0, otherwise. The second sub-function $f_2$ of the nonlinear filter function of the FLIP stream cipher is a bent function involving 128 variables (which can be found in Section I-B). The Walsh–Hadamard transform $f_2$ at the point $\mathbf{a}'' \in \mathbb{F}_2^{128}$ is, $\mathcal{W}_{f_2}(\mathbf{a}'') = 2^{-64}(-1)^{\tilde{f}(\mathbf{a}'')}$, where $\tilde{f}$ is the dual of $f$ and $\mathbf{a}'' \in \mathbb{F}_2^{128}$. The last function is a direct sum of 8 small triangular functions as in Section I-B. From Lemma 1 we get the Walsh–Hadamard transform values of all monomials of each of the triangular functions. Since, if $f(\mathbf{x}, \mathbf{y}) = f_1(\mathbf{x}) + f_2(\mathbf{y})$, for all $\mathbf{x} \in \mathbb{F}_2^{n_1}$ and $\mathbf{y} \in \mathbb{F}_2^{n_2}$, then $\mathcal{W}_f(\mathbf{a}, \mathbf{b}) = \mathcal{W}_{f_1}(\mathbf{a})\mathcal{W}_{f_2}(\mathbf{b})$, for all $\mathbf{a} \in \mathbb{F}_2^{n_1}$ and $\mathbf{b} \in \mathbb{F}_2^{n_2}$, the claim follows. □

From Theorem 1, we obtain the following consequence.

**Corollary 1.** *Let $\mathbf{x} \in \mathbb{F}_2^{530}$ and $f \in \mathcal{B}_{530}$ as in Theorem 1. Then:*

- *(i) the maximum absolute value of $\mathcal{W}_f(\mathbf{a})$ for some $\mathbf{a} \in \mathbb{F}_2^{530}$ is $2^{-79} < \frac{(19923090075)^8}{2^{352}} < 2^{-78}$.*
- *(ii) the maximum value is achieved at $\mathbf{a} = \mathbf{1}||\mathbf{a}''||\mathbf{a}'''$, $\mathbf{1} \in \mathbb{F}_2^{42}$, $\mathbf{a}'' \in \mathbb{F}_2^{128}$, and $\mathbf{a}''' \in \mathbb{F}_2^{360}$, such that $\mathbf{a}'''_{i1} = \mathbf{1} \in \mathbb{F}_2$, $\mathbf{a}'''_{i2} \in \mathbb{F}_2^2$, $1 \le i \le 8$, and $\mathbf{a}'''_{ij} = 0 \in \mathbb{F}_2^j$, $1 \le i \le 8, 3 \le j \le 9$.*
- *(iii) the maximum bias of the function $f$ from $l_{\mathbf{a},0} = \mathbf{a}\cdot\mathbf{x}$, where $\mathbf{a} \in \mathbb{F}_2^{530}$ is $2^{-79} < \max_{\mathbf{a}\in\mathbb{F}_2^{530}}|\mathcal{W}_f(\mathbf{a})| < 2^{-78}$.*

However, when we consider the same function in a restricted domain, then the scenario changes significantly. At the end of the paper, we will see that the maximum absolute restricted Walsh–Hadamard spectrum is indeed much higher in the restricted domain $E_{530,265}$, lying in $[\frac{1}{2^{18.49}}, \frac{1}{2^{13.59}}]$. The lower bound is obtained by using our results, and the upper bound is obtained by implementing the result of Carlet et al. [2]. Thus, the simple Walsh–Hadamard transform does not provide the correct value and it is much higher when the inputs are from a restricted domain $E_{530,265}$.

### *B. Our idea: Frequency distribution of concatenated sub-strings of a fixed weight bit string*

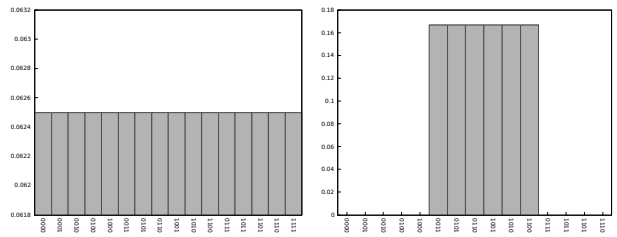
We first consider an $n$ bit string $\mathbf{x}$ with $wt(\mathbf{x}) = k$, i.e., $\mathbf{x} \in E_{n,k}$. In this $n$-bit string $\mathbf{x}$, if we consider the first $n_1$ bits, say $\mathbf{x}'$, then the weight distribution of $\mathbf{x}'$ may not be uniform. If the distribution of $\mathbf{x}'$ is different, then the cryptographic properties of the function defined over $\mathbf{x}'$ will be affected. In IACR ToSC, Carlet et al. [2] studied several cryptographic properties of the complete function $f = f_1 + f_2 + f_3$ (the direct sum of three functions $f_1$, $f_2$, $f_3$) without considering the exact probability distributions of the inputs of each sub-functions, $f_1$, $f_2$, $f_3$. To get the correct picture about the complete function $f$, one needs to study each function $f_i$ ($i = 1, 2, 3$) by considering the exact probability distribution of inputs of each of the $f_i$'s.

For the simplicity of our discussion, we first consider $n = n_1 + n_2$ and $\mathbf{x} \in \mathbb{F}_2^n$, which is the concatenation of $\mathbf{x}', \mathbf{x}''$ (i.e., $\mathbf{x} = \mathbf{x}'||\mathbf{x}''$), where $\mathbf{x}' \in \mathbb{F}_2^{n_1}$ and $\mathbf{x}'' \in \mathbb{F}_2^{n_2}$. Let $Pr(\mathbf{x}) = \frac{1}{2^n}$ denote the probability of picking $\mathbf{x} \in \mathbb{F}_2^n$. We recall that $E_{n,k}$ denotes the set of all $n$-bit strings of weight $k$. The cardinality of $E_{n,k}$ is $|E_{n,k}| = \binom{n}{k}$, $0 \le k \le n$. So, $Pr[\mathbf{x}]$, when $\mathbf{x} \in E_{n,k}$ is equal to $\frac{1}{\binom{n}{k}}$. Now if we consider $\mathbf{x}' \in E_{n_1,i}^{n=n_1+n_2,k}$, $0 \le i \le n_1$ then $Pr[\mathbf{x}']$ will be $\frac{\binom{n_2}{k-i}}{\binom{n}{k}}$. We consider the following example to explain it more clearly.

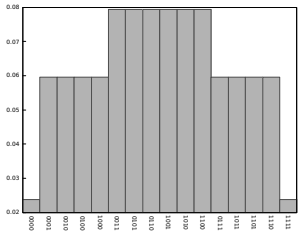
Consider the set $E_{4,2}$ (i.e., $|E_{4,2}| = 6$). Now, if we consider the first two bits of $\mathbf{x} \in E_{4,2}$ then $|E_{2,0}^{4=2+2,2}| = 1$, $|E_{2,1}^{4=2+2,2}| = 4$ and $|E_{2,2}^{4=2+2,2}| = 1$. So, $Pr(\mathbf{x}' = 00) = \frac{1}{6} = Pr(\mathbf{x}' = 11)$, $Pr(\mathbf{x}' = 01) = \frac{1}{3} = Pr(\mathbf{x}' = 10)$. The Figure 1 represents the probability distribution of points in the uniform case with $n = 4$, in the uniform case with $n = 4$, $k = 2$ and in restricted case with $n = 10$, $k = 5$ and $n_1 = 4$.

Let $\pi$ be any permutation on the set $\{1, 2, \dots, n\}$. Then $(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}) \in E_{n,k}$ for all $\mathbf{x} = (x_1, x_2, \dots, x_n) \in E_{n,k}$. We consider $\mathbf{x} = (x_1, x_2, \dots, x_n) \in E_{n,\frac{n}{2}}$ and $\mathbf{x}' = (y_1, y_2, \dots, y_{n_1}) \in \mathbb{F}_2^{n_1}$ where $y_i = x_i$, $1 \le i \le n_1$. We are now interested to calculate the frequency distributions of $\mathbf{x}'$.

**Case** 1: Consider the case when $n_1 = \frac{n}{2}$. It can be observed that all possible elements $\mathbf{x}'$ of $\mathbb{F}_2^{n_1}$ exist under this scenario. Here, $\binom{\frac{n}{2}}{i}\binom{\frac{n}{2}}{\frac{n}{2}-i}$ many elements of $\mathbf{x}'$ with $wt(\mathbf{x}') = i$, $0 \le i \le \frac{n}{2}$ exist and each bit pattern of the same weight occurs an equal number of times.



(a) All weight uniform case $n = 4$ (b) Weight 2 uniform case $n = 4$



(c) For restricted case $n = 10$, $k = 5$, $n_1 = 4$

Fig. 1: Probability distributions

**Case** 2: Consider the case when $n_1 < \frac{n}{2}$. Also, here, all possible elements $\mathbf{x}'$ of $\mathbb{F}_2^{n_1}$ exist, that is, $\binom{n_1}{i}\binom{n-n_1}{\frac{n}{2}-i}$ many elements $\mathbf{x}' \in \mathbb{F}_2^{n_1}$ with $wt(\mathbf{x}') = i$ are present, where $0 \le i \le n_1$.

**Case** 3: Consider the case when $n_1 > \frac{n}{2}$. Now we find the number of possible $\mathbf{x}'$ with $wt(\mathbf{x}') = i$, $n_1 - \frac{n}{2} \le i \le \frac{n}{2}$. One can observe that $\left|\{\mathbf{x}' \in \mathbb{F}_2^{n_1} |\ wt(\mathbf{x}') = \frac{n}{2}\}\right| = \binom{n_1}{\frac{n}{2}}$, where every such element occurs exactly once. In general, for each $i$, $0 \le i \le n - n_1$, such that $wt(\mathbf{x}') = \frac{n}{2} - i$, then $\mathbf{x}'$ occurs $\binom{n_1}{\frac{n}{2}-i}\binom{n-n_1}{i}$ times ($0 \le i \le n - n_1$).

In the rest of the paper, we consider $n_i < n$, $1 \le i \le 2$, and $\mathbf{x} \in E_{n,\frac{n}{2}}$.

## III. Biased Walsh–Hadamard transform

In this section, we define the Walsh–Hadamard transform of a Boolean function by considering the general probability distribution (not necessarily uniform) of input elements. For our convention, we shall name this as biased Walsh–Hadamard transform of a Boolean function (another definition can be found in [4]). Biased Walsh–Hadamard transform of a function at a point $\mathbf{a}$ is basically the bias between a Boolean function and a linear function $l_{\mathbf{a},0}$ over a non-uniform domain.

Let $p(\mathbf{a})$ be the probability of an input element $\mathbf{a} \in \mathbb{F}_2^n$ in $f \in \mathcal{B}_n$. Recall that $0 \le p(\mathbf{a}) \le 1$, for all $\mathbf{a} \in \mathbb{F}_2^n$, and $\sum_{\mathbf{a}\in\mathbb{F}_2^n} p(\mathbf{a}) = 1$. For any $f, g \in \mathcal{B}_n$, we let $\mathcal{S}(f,g) = \{\mathbf{x} \in \mathbb{F}_2^n :\ f(\mathbf{x}) \ne g(\mathbf{x})\}$ and $\bar{\mathcal{S}}(f,g) = \mathbb{F}_2^n \setminus \mathcal{S}(f,g) = \{\mathbf{x} \in \mathbb{F}_2^n :\ f(\mathbf{x}) = g(\mathbf{x})\}$.

Now we define the concept of Hamming distance between two functions in a non-uniform domain. We call this the *biased Hamming distance* between two functions $f$, $g$ and denote it by $d_H^B(f,g)$, where, $d_H^B(f,g) = \sum_{\mathbf{x}\in\mathcal{S}(f,g)} p(\mathbf{x})$. Further,

$$\begin{aligned} d_H^B(f,g) &= \frac{1}{2}\left\{\sum_{\mathbf{x}\in\bar{\mathcal{S}}(f,g)} p(\mathbf{x}) + \sum_{\mathbf{x}\in\mathcal{S}(f,g)} p(\mathbf{x})\right\} \\ &\quad - \frac{1}{2}\left\{\sum_{\mathbf{x}\in\bar{\mathcal{S}}(f,g)} p(\mathbf{x}) - \sum_{\mathbf{x}\in\mathcal{S}(f,g)} p(\mathbf{x})\right\} \\ &= \frac{1}{2} - \frac{1}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})+g(\mathbf{x})}. \end{aligned}$$

If $g$ is affine function (i.e., if $g = l_{\mathbf{a},\varepsilon}$), then $d_H^B(f, l_{\mathbf{a},\varepsilon}) = \frac{1}{2} - \frac{(-1)^\varepsilon}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} = \frac{1}{2} - \frac{(-1)^\varepsilon}{2}\mathcal{W}_f^B(\mathbf{a})$, where $\mathcal{W}_f^B(\mathbf{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}}$ is the *biased Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at $\mathbf{a} \in \mathbb{F}_2^n$. The *biased Walsh–Hadamard spectrum* of $f \in \mathcal{B}_n$ is the multiset $\left[\mathcal{W}_f^B(\mathbf{a}) :\ \mathbf{a} \in \mathbb{F}_2^n\right]$. It can be observed that $\mathcal{W}_{l_{\mathbf{a},0}}^B(\mathbf{a}) = 1$ and $\mathcal{W}_{l_{\mathbf{a},0}}^B(\mathbf{b})$ may or may not be zero for $\mathbf{a} \ne \mathbf{b}$, which differs from the uniform domain case.

Further, we define the correlation between two functions $f, g \in \mathcal{B}_n$ in a non-uniform domain, denoted by $\mathsf{corr}^B(f,g)$, which is defined by

$$\mathsf{corr}^B(f,g) = \left|\sum_{\mathbf{x}\in\bar{S}(f,g)} p(\mathbf{x}) - \sum_{\mathbf{x}\in S(f,g)} p(\mathbf{x})\right|.$$

It can be observed that $\mathsf{corr}^B(f, l_{\mathbf{a},0}) = \left|\mathcal{W}_f^B(\mathbf{a})\right|$.

### A. Theoretical estimates of biases in non-uniform domain

**Theorem 2** (Biased Parseval's Identity)**.** *Let $f \in \mathcal{B}_n$, and $p(\mathbf{x})$ be the probability of $\mathbf{x} \in \mathbb{F}_2^n$. Then*

$$\sum_{\mathbf{a}\in\mathbb{F}_2^n} \mathcal{W}_f^B(\mathbf{a})^2 = 2^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})^2.$$

*Proof.* The identity follows using Equation (1), and writing

$$\begin{aligned} &\sum_{\mathbf{a}\in\mathbb{F}_2^n} \mathcal{W}_f^B(\mathbf{a})^2 \\ &= \sum_{\mathbf{a}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}}\right) \\ &\qquad\qquad \left(\sum_{\mathbf{y}\in\mathbb{F}_2^n} p(\mathbf{y})(-1)^{f(\mathbf{y})+\mathbf{a}\cdot\mathbf{y}}\right) \\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^n} p(\mathbf{x})p(\mathbf{y})(-1)^{f(\mathbf{x})+f(\mathbf{y})} \sum_{\mathbf{a}\in\mathbb{F}_2^n}(-1)^{\mathbf{a}\cdot(\mathbf{x}+\mathbf{y})} \\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{z}\in\mathbb{F}_2^n} p(\mathbf{x})p(\mathbf{x}+\mathbf{z})(-1)^{f(\mathbf{x})+f(\mathbf{x}+\mathbf{z})} \sum_{\mathbf{a}\in\mathbb{F}_2^n}(-1)^{\mathbf{a}\cdot\mathbf{z}}, \\ &\qquad\qquad\qquad\qquad \text{where } \mathbf{z} = \mathbf{x}+\mathbf{y} \\ &= 2^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})^2, \end{aligned}$$

and the result is shown. □

**Theorem 3.** *Let* $p := \sqrt{\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})^2}$ *and* $a := \min_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})$ *(we assume* $a > 0$*),* $A := \max_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})$*. Then* $\max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^B(\mathbf{a})| \geq p$ *and* $1 \leq \sum_{\mathbf{a}\in\mathbb{F}_2^n} \mathcal{W}_f^B(\mathbf{a})^2 \leq \frac{(a+A)^2}{4aA}$*, where the lower bound becomes equality if and only if for all* $\mathbf{x}$*,* $p(\mathbf{x}) = 2^{-n}$ *(uniform domain) and the upper bound is an equality if and only if there exists* $2^{n-1} \leq \alpha \in \mathbb{Z}$ *such that exactly* $\alpha$ *of the* $p(\mathbf{x})$ *are equal to* $a = \frac{1}{2\alpha}$*, and exactly* $2^n - \alpha$ *of the* $p(\mathbf{x})$ *are equal to* $A = \frac{1}{2(2^n-\alpha)}$*.*

*Proof.* From Theorem 2, we get $\max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^B(\mathbf{a})| \geq p$, otherwise, if $\max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^B(\mathbf{a})| < p$, then

$$\sum_{\mathbf{a}\in\mathbb{F}_2^n} \mathcal{W}_f^B(\mathbf{a})^2 < \sum_{\mathbf{a}\in\mathbb{F}_2^n} p^2 = 2^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})^2,$$

which is a contradiction. So, we must have $\max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^B(\mathbf{a})| \geq p$.

Next, we recall the Cauchy-Schwarz inequality

$$\left(\sum_{i=1}^N x_i y_i\right)^2 \leq \left(\sum_{i=1}^N x_i^2\right)\left(\sum_{i=1}^N y_i^2\right),$$

with equality if and only if $x_i, y_i$ are proportional; as well as Pólya-Szegö (sometimes called Kantorovich) inequality [9]

$$\left(\sum_{i=1}^N x_i^2\right)\left(\sum_{i=1}^N y_i^2\right) \leq \frac{(ab+AB)^2}{4abAB}\left(\sum_{i=1}^N x_i y_i\right)^2,$$
$$0 < a \leq x_i \leq A,\ 0 < b \leq y_i \leq B,$$

with equality if and only if $\alpha := N \cdot \frac{A}{a} \big/ \left(\frac{A}{a} + \frac{B}{b}\right) \in \mathbb{Z}$, $\beta := N \cdot \frac{B}{b} \big/ \left(\frac{A}{a} + \frac{B}{b}\right) \in \mathbb{Z}$ and $\alpha$ of the numbers $x_1, \ldots, x_N$ are equal to $a$ and $\beta$ of these numbers are equal to $A$, and if the corresponding numbers $y_i$ are equal to $B$ and $b$, respectively.

To get the lower bound in the second claim, we apply Cauchy-Schwarz inequality with $N := 2^n, x_i := p(\mathbf{i}), y_i := 1$, where $\mathbf{i}$ is the $n$-bit vector obtained from the binary expansion of $i$, and observe that $\sum_{i=1}^N x_i y_i = 1$. The equality will happen if $x_i/y_i$ is constant, and since $\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x}) = 1$, we get that $p(\mathbf{x}) = 2^{-n}$ for all $\mathbf{x} \in \mathbb{F}_2^n$ (uniform domain).

To get the upper bound in the second claim, we apply Pólya-Szegö inequality with $N := 2^n, x_i := p(\mathbf{i}), y_i := 1, b = B := 1$. The equality will happen if and only if $\alpha := \frac{A\,2^n}{a+A}, \beta := \frac{a\,2^n}{a+A} \in \mathbb{Z}$ and exactly $\alpha$ of the $p(\mathbf{x})$ are equal to $a$, and exactly $\beta$ of the $p(\mathbf{x})$ are equal to $A$. Observe that $a\alpha = A\beta$, $\beta = 2^n - \alpha$, and since $\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x}) = 1$, then $a\alpha + A\beta = 1$, which renders $a\alpha = A\beta = \frac{1}{2}$, so $a = \frac{1}{2\alpha}, A = \frac{1}{2(2^n-\alpha)}$, $\alpha \geq 2^{n-1}$. The theorem is shown. □

Based on this result, we may require to redefine several existing characteristics of a Boolean function, for example balancedness or bentness in restricted domain. Certain results in this direction are presented in the subsection III-B.

### *B. Properties of Boolean functions in biased domain*

A Boolean function $f \in \mathcal{B}_n$ is said to be (biased) *bent* in the non-uniform domain if the absolute value of the biased Walsh–Hadamard transform at any point is $p = \sqrt{\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})^2}$. Next, we say that a function $f \in \mathcal{B}_n$ is (biased) *balanced* in the non-uniform domain (of probability function $p$) if and only if

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})} = 0,\ i.e.,\ \sum_{\mathbf{x}\in\mathrm{supp}(f)} p(\mathbf{x}) = \sum_{\mathbf{x}\notin\mathrm{supp}(f)} p(\mathbf{x}).$$

**Remark 1.** *Let* $p(\mathbf{x})$ *be the probability of* $\mathbf{x} \in \mathbb{F}_2^n$*. Since for* $f \in \mathcal{B}_n$*, we have*

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})} &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(1-2f(\mathbf{x})) \\ &= 1 - 2\sum_{\mathbf{x}\in\mathrm{supp}(f)} p(\mathbf{x}),\end{aligned}$$

*then a Boolean function* $f \in \mathcal{B}_n$ *is balanced if and only if* $\sum_{\mathbf{x}\in\mathrm{supp}(f)} p(\mathbf{x}) = \frac{1}{2}$.

**Example 1.** *Let* $f, g \in \mathcal{B}_4$ *be two Boolean functions as in Table I. In the uniform domain,* $f$ *is balanced but* $g$ *is not balanced, however, both* $f$ *and* $g$ *are balanced in the biased domain with the fixed input probability from Table* I*, since* $\sum_{\mathbf{x}\in\mathrm{supp}(f)} p(\mathbf{x}) = \frac{1}{2} = \sum_{\mathbf{x}\in\mathrm{supp}(g)} p(\mathbf{x})$ *:*

| $x_4x_3x_2x_1$ | $p(\mathbf{x})$ | $f(\mathbf{x})$ | $g(\mathbf{x})$ |
|---|---|---|---|
| 0000 | $\frac{1}{42}$ | 0 | 1 |
| 0001 | $\frac{5}{84}$ | 0 | 1 |
| 0010 | $\frac{5}{84}$ | 1 | 1 |
| 0011 | $\frac{5}{63}$ | 1 | 0 |
| 0100 | $\frac{5}{84}$ | 1 | 1 |
| 0101 | $\frac{5}{63}$ | 0 | 0 |
| 0110 | $\frac{5}{63}$ | 0 | 0 |
| 0111 | $\frac{5}{84}$ | 0 | 1 |
| 1000 | $\frac{5}{84}$ | 0 | 1 |
| 1001 | $\frac{5}{63}$ | 0 | 0 |
| 1010 | $\frac{5}{63}$ | 1 | 0 |
| 1011 | $\frac{5}{84}$ | 1 | 1 |
| 1100 | $\frac{5}{63}$ | 1 | 0 |
| 1101 | $\frac{5}{84}$ | 0 | 1 |
| 1110 | $\frac{5}{84}$ | 1 | 1 |
| 1111 | $\frac{1}{42}$ | 1 | 0 |

TABLE I: Biased balanced Boolean functions

We now calculate the number of maximum possible distinct values of the biased Walsh–Hadamard transform of a symmetric Boolean function.

Recall that $K_i(m,n) = \sum_{j=0}^{i} (-1)^j \binom{m}{j}\binom{n-m}{i-j}$ is the Krawtchouk polynomial of degree $i$. Let $f \in \mathcal{B}_n$ be a symmetric Boolean function and $f(\mathbf{x}) = \varepsilon_i \in \mathbb{F}_2$ if $wt(\mathbf{x}) =$

$i,\ 0 \le i \le n$. The Walsh–Hadamard transform of $f$ at $\mathbf{a} \in \mathbb{F}_2^n$ can be written as

$$\begin{aligned}\mathcal{W}_f(\mathbf{a}) &= \sum_{i=0}^{n}(-1)^{\varepsilon_i}\sum_{\mathbf{x}\in E_{n,i}}(-1)^{\mathbf{a}\cdot\mathbf{x}}\\ &= \sum_{i=0}^{n}(-1)^{\varepsilon_i}\sum_{j=0}^{i}(-1)^j\binom{wt(\mathbf{a})}{j}\binom{n-wt(\mathbf{a})}{i-j}\\ &= \sum_{i=0}^{n}(-1)^{\varepsilon_i}K_i(wt(\mathbf{a}),n).\end{aligned}$$

**Theorem 4.** *Let $\mathbf{x} \in \mathbb{F}_2^n$ with probability $p(\mathbf{x})$. We assume that if $wt(\mathbf{x}) = wt(\mathbf{y})$, then $p(\mathbf{x}) = p(\mathbf{y})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. Then there exist at most $n+1$ distinct values of the biased Walsh–Hadamard transform of a symmetric function $f \in \mathcal{B}_n$.*

*Proof.* We have $p(\mathbf{x}) = p(\mathbf{y})$ when $wt(\mathbf{x}) = wt(\mathbf{y})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. Let $p_{n,i} = p(\mathbf{x})$ and $f(\mathbf{x}) = \varepsilon_i \in \mathbb{F}_2$, for all $\mathbf{x} \in \mathbb{F}_2^n$ with $wt(\mathbf{x}) = i$, $0 \le i \le n$. For any $\mathbf{a} \in \mathbb{F}_2^n$,

$$\begin{aligned}\mathcal{W}_f^B(\mathbf{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}p(\mathbf{x})(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}}\\ &= \sum_{i=0}^{n}\sum_{\mathbf{x}\in E_{n,i}}p(\mathbf{x})(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}}\\ &= \sum_{i=0}^{n}p_{n,i}(-1)^{\varepsilon_i}\sum_{\mathbf{x}\in E_{n,i}}(-1)^{\mathbf{a}\cdot\mathbf{x}}\\ &= \sum_{i=0}^{n}p_{n,i}(-1)^{\varepsilon_i}K_i(wt(\mathbf{a}),n),\end{aligned}$$

where $K_i(wt(\mathbf{a}), n)$ is the Krawtchouk polynomial of degree $i$, $0 \le i \le n$, computed at $wt(\mathbf{a})$. Since for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ with $wt(\mathbf{a}) = wt(\mathbf{b})$, $K_i(wt(\mathbf{a}), n) = K_i(wt(\mathbf{b}), n)$, $0 \le i \le n$, the result is shown. □

The first sub-function of the nonlinear filter function of the FLIP stream cipher is a symmetric function involving 42 variables in the uniform domain, so it will have at most 43 distinct biased Walsh–Hadamard coefficients. The next section describes the nature of the biased Walsh–Hadamard transform of a linear function.

### C. Biased Walsh–Hadamard transform of an affine function

Let $n = n_1 + n_2$ and $\mathbf{x} = \mathbf{x}'||\mathbf{x}'' \in \mathbb{F}_2^n$ such that $\mathbf{x}' \in \mathbb{F}_2^{n_1}$ with probability $p(\mathbf{x}')$. Assume that if $wt(\mathbf{x}') = wt(\mathbf{y}')$, then $p(\mathbf{x}') = p(\mathbf{y}')$, $\mathbf{x}', \mathbf{y}' \in \mathbb{F}_2^{n_1}$.

**Proposition 1.** *Let $n = n_1 + n_2$, $n_1 < \frac{n}{2}$ and $\mathbf{x} = \mathbf{x}'||\mathbf{x}'' \in \mathbb{F}_2^n$ such that $\mathbf{x}' \in \mathbb{F}_2^{n_1}$ with probability $p(\mathbf{x}')$. Let $\mathbf{u}' \in \mathbb{F}_2^{n_1}, \varepsilon \in \mathbb{F}_2$, and $f(\mathbf{x}') = \mathbf{u}'\cdot\mathbf{x}' + \varepsilon$, for all $\mathbf{x}' \in \mathbb{F}_2^{n_1}$. Then*

$$\mathcal{W}_f^B(\mathbf{a}') = \begin{cases}(-1)^{\varepsilon}, & \text{if } \mathbf{a}' = \mathbf{u}';\\ \sum_{i=0}^{n_1} q_{n_1,i}K_i(wt(\mathbf{a}'+\mathbf{u}'),n_1), & \text{otherwise},\end{cases}$$

*where $q_{n_1,i} = p(\mathbf{x}')$ if $wt(\mathbf{x}') = i$ and $K_i(wt(\mathbf{a}'+\mathbf{u}'), n_1)$ is the Krawtchouk polynomial of degree $i$, where $0 \le i \le n_1$, computed at $wt(\mathbf{a}'+\mathbf{u}')$, i.e., $K_i(wt(\mathbf{a}'+\mathbf{u}'), n_1) = \sum_{\mathbf{x}'\in E_{n_1,i}}(-1)^{(\mathbf{a}'+\mathbf{u}')\cdot\mathbf{x}'}$.*

*Proof.* For any $\mathbf{a}' \in \mathbb{F}_2^{n_1}$,

$$\begin{aligned}\mathcal{W}_f^B(\mathbf{a}') &= \sum_{\mathbf{x}'\in\mathbb{F}_2^{n_1}}p(\mathbf{x}')(-1)^{f(\mathbf{x}')+\mathbf{a}'\cdot\mathbf{x}'}\\ &= (-1)^{\varepsilon}\sum_{\mathbf{x}'\in\mathbb{F}_2^{n_1}}p(\mathbf{x}')(-1)^{(\mathbf{a}'+\mathbf{u}')\cdot\mathbf{x}'}\\ &= (-1)^{\varepsilon}\sum_{i=0}^{n_1}q_{n_1,i}\sum_{\mathbf{x}'\in E_{n_1,i}}(-1)^{(\mathbf{a}'+\mathbf{u}')\cdot\mathbf{x}'},\end{aligned}$$

and the proposition follows. □

From Proposition 1 we get the biased Walsh–Hadamard transform of the linear function $f_1 \in \mathcal{B}_{n_1}$, $f_1(\mathbf{x}) = \sum_{j=1}^{n_1} x_j = \mathbf{1}\cdot\mathbf{x}$, which is used in the FLIP cipher.

**Corollary 2.** *Let $n = n_1 + n_2 + n_3$ and $f_1(\mathbf{x}) = \sum_{j=1}^{n_1} x_j = \mathbf{1}\cdot\mathbf{x}$, for all $\mathbf{x} \in \mathbb{F}_2^{n_1}$, which is used in the FLIP cipher. Then the biased Walsh–Hadamard transform of $f_1$ at $\mathbf{a} \in \mathbb{F}_2^{n_1}$ is equal to*

$$\mathcal{W}_{f_1}^B(\mathbf{a}) = \begin{cases}1, & \text{if } \mathbf{a} = \mathbf{1};\\ \sum_{i=0}^{n_1} q_{n_1,i}K_i(wt(\bar{\mathbf{a}}),n_1), & \text{otherwise},\end{cases}$$

*where $\bar{\mathbf{a}} = \mathbf{a} + \mathbf{1}$, the complement of $\mathbf{a}$, and $K_i(wt(\bar{\mathbf{a}}), n_1)$ is the Krawtchouk polynomial of degree $i$, computed at $\bar{\mathbf{a}}$.*

It can be observed that the properties of a linear function change significantly in a biased domain.

**Example 2.** *Let $n = 10$ and $n_1 = 4$. The total number of bit strings of length 10 and weight 5 is $|E_{10,5}| = \binom{10}{5} = 252$. Let $f(\mathbf{x}) = \mathbf{1}\cdot\mathbf{x}$, for all $\mathbf{x} \in \mathbb{F}_2^4$, which is the parity of the weight of $\mathbf{x}$. The probability of a bit pattern $\mathbf{x}' \in \mathbb{F}_2^4$ having weight $i$ and the biased Walsh–Hadamard transform of $f$ are given in Table* II. *We know that for any $\mathbf{a} \in \mathbb{F}_2^4$,*

$$\begin{aligned}\mathcal{W}_f^B(\mathbf{a}) &= \sum_{i=0}^{4}q_{4,i}\sum_{\mathbf{x}\in E_{4,i}}(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}}\\ &= \sum_{i=0}^{4}q_{4,i}\sum_{\mathbf{x}\in E_{4,i}}(-1)^{(1+\mathbf{a})\cdot\mathbf{x}}\\ &= q_{4,0} + q_{4,1}\sum_{\mathbf{x}\in E_{4,1}}(-1)^{\bar{\mathbf{a}}\cdot\mathbf{x}} + q_{4,2}\sum_{\mathbf{x}\in E_{4,2}}(-1)^{\bar{\mathbf{a}}\cdot\mathbf{x}}\\ &\quad + q_{4,3}\sum_{\mathbf{x}\in E_{4,3}}(-1)^{\bar{\mathbf{a}}\cdot\mathbf{x}} + q_{4,4}(-1)^{wt(\bar{\mathbf{a}})}.\end{aligned}$$

*Thus, the sum of the squares of the biased Walsh–Hadamard coefficients is equal to 1.076, and so there is a bias with respect to the other linear functions (we could infer the sum of the squares of the biased Walsh–Hadamard coefficients $> 1$ from Theorem 3, which also gives the upper bound of the sum of the squares of the biased of Walsh–Hadamard coefficients $\frac{(\frac{1}{42}+\frac{1}{84})^2}{4\cdot\frac{1}{42}\cdot\frac{1}{84}} = \frac{9}{8} = 1.125$).*

### D. Biased Walsh–Hadamard transforms of some Boolean functions

In this section we study the biased Walsh–Hadamard transforms of some particular functions. We first observe that, it is

| $x_4x_3x_2x_1$ | $p(\mathbf{x})$ | $f(\mathbf{x})$ | $\mathcal{W}_f(\mathbf{a})$ | $\mathcal{W}_f^B(\mathbf{a})$ |
|---|---|---|---|---|
| 0000 | $\frac{1}{42}$ | 0 | 0 | $\frac{1}{21}$ |
| 0001 | $\frac{5}{84}$ | 1 | 0 | 0 |
| 0010 | $\frac{5}{84}$ | 1 | 0 | 0 |
| 0011 | $\frac{5}{63}$ | 0 | 0 | $\frac{1}{9}$ |
| 0100 | $\frac{5}{84}$ | 1 | 0 | 0 |
| 0101 | $\frac{5}{63}$ | 0 | 0 | $\frac{1}{9}$ |
| 0110 | $\frac{5}{63}$ | 0 | 0 | $\frac{1}{9}$ |
| 0111 | $\frac{5}{84}$ | 1 | 0 | 0 |
| 1000 | $\frac{5}{84}$ | 1 | 0 | 0 |
| 1001 | $\frac{5}{63}$ | 0 | 0 | $\frac{1}{9}$ |
| 1010 | $\frac{5}{63}$ | 0 | 0 | $\frac{1}{9}$ |
| 1011 | $\frac{5}{84}$ | 1 | 0 | 0 |
| 1100 | $\frac{5}{63}$ | 0 | 0 | $\frac{1}{9}$ |
| 1101 | $\frac{5}{84}$ | 1 | 0 | 0 |
| 1110 | $\frac{5}{84}$ | 1 | 0 | 0 |
| 1111 | $\frac{1}{42}$ | 0 | $\frac{1}{16}$ | 1 |

TABLE II: Biased Walsh–Hadamard spectrum of linear Boolean function

difficult to calculate the biased Walsh–Hadamard transform of a bent or triangular function, in arbitrary number of variables, directly. To tackle this, we first compute the biased Walsh–Hadamard transform values of monomials Boolean functions, and then, we derive an iterative formula to calculate the biased Walsh–Hadamard spectrum.

**Theorem 5.** *Let $f \in \mathcal{B}_n$. The following are true:*

(i) *Let $E_{n,k}$ be the set of vectors of weight $k$ in $\mathbb{F}_2^n$. The (unnormalized) restricted nonlinearity of $f$ at $\mathbf{c} \in \mathbb{F}_2^n$ can be computed by*

$$\sum_{\mathbf{x}\in E_{n,k}} (-1)^{f(\mathbf{x})+\mathbf{c}\cdot\mathbf{x}} = K_k(wt(\mathbf{c}),n) - 2\sum_{\mathbf{x}\in E_{n,k}\cap \mathrm{supp}(f)} (-1)^{\mathbf{c}\cdot\mathbf{x}}.$$

(ii) *If $f(\mathbf{x}) = x_1x_2\cdots x_n$ and $\mathbf{x} \in \mathbb{F}_2^n$ with probability $p(\mathbf{x})$, then the biased Walsh–Hadamard transform of $f$ at $\mathbf{a} \in \mathbb{F}_2^n$ is equal to*

$$\mathcal{W}_f^B(\mathbf{a}) = 1 - 2\left(p(\mathbf{1})(-1)^{wt(\mathbf{a})} + \sum_{\mathbf{x}\in \mathrm{supp}(l_{\mathbf{a},0})} p(\mathbf{x})\right),$$

*where $l_{\mathbf{a},0}(\mathbf{x}) = \mathbf{a}\cdot\mathbf{x}$, $\mathbf{x} \in \mathbb{F}_2^n$, is a linear function.*

*Proof.* We write

$$\begin{aligned}
&\sum_{\mathbf{x}\in E_{n,k}} (-1)^{f(\mathbf{x})+\mathbf{c}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}\in E_{n,k}\cap \mathrm{supp}(f)} (-1)^{f(\mathbf{x})+\mathbf{c}\cdot\mathbf{x}} + \sum_{\mathbf{x}\in E_{n,k}\cap \overline{\mathrm{supp}(f)}} (-1)^{f(\mathbf{x})+\mathbf{c}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}\in E_{n,k}\cap \mathrm{supp}(f)} (-1)^{1+\mathbf{c}\cdot\mathbf{x}} + \sum_{\mathbf{x}\in E_{n,k}\cap \overline{\mathrm{supp}(f)}} (-1)^{f(\mathbf{x})+\mathbf{c}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}\in E_{n,k}} (-1)^{\mathbf{c}\cdot\mathbf{x}} - 2\sum_{\mathbf{x}\in E_{n,k}\cap \mathrm{supp}(f)} (-1)^{\mathbf{c}\cdot\mathbf{x}} \\
&= K_k(wt(\mathbf{c}),n) - 2\sum_{\mathbf{x}\in E_{n,k}\cap \mathrm{supp}(f)} (-1)^{\mathbf{c}\cdot\mathbf{x}}.
\end{aligned}$$

We now prove the second claim. Observe that $(-1)^{\varepsilon} = 1-2\varepsilon$, $\varepsilon \in \mathbb{F}_2$. Also, it is clear that $f(\mathbf{x}) = 1$ only when $\mathbf{x} = \mathbf{1} = (1,1,\ldots,1)$. For any $\mathbf{a} \in \mathbb{F}_2^n$,

$$\begin{aligned}
\mathcal{W}_f^B(\mathbf{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\{\mathbf{1}\}} p(\mathbf{x})(-1)^{\mathbf{a}\cdot\mathbf{x}} - p(\mathbf{1})(-1)^{wt(\mathbf{a})} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{\mathbf{a}\cdot\mathbf{x}} - 2p(\mathbf{1})(-1)^{wt(\mathbf{a})} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(1-2\mathbf{a}\cdot\mathbf{x}) - 2p(\mathbf{1})(-1)^{wt(\mathbf{a})} \\
&= 1 - 2\left(p(\mathbf{1})(-1)^{wt(\mathbf{a})} + \sum_{\mathbf{x}\in\mathrm{supp}(l_{\mathbf{a},0})} p(\mathbf{x})\right),
\end{aligned}$$

where $\mathrm{supp}(l_{\mathbf{a},0})$ is defined as in Section I-A, and our theorem is shown. □

From Theorem 5, we get the following corollary.

**Corollary 3.** *Let $\mathbf{x} \in \mathbb{F}_2^n$ with probability $p(\mathbf{x})$ as defined above, and let $f \in \mathcal{B}_n$ be defined by $f(\mathbf{x}) = x_1x_2\cdots x_n$, for all $\mathbf{x} \in \mathbb{F}_2^n$. Then:*

*(i) $\mathcal{W}_f^B(0,0,\ldots,0) = 1 - 2p(\mathbf{1})$.*

*(ii) If $\mathbf{a} \neq \mathbf{0}, \mathbf{1}$ and $l_{\mathbf{a},0}$ is a biased balanced linear function, then $\mathcal{W}_f^B(\mathbf{a}) = -2p(\mathbf{1})(-1)^{wt(\mathbf{a})}$.*

*Proof.* The first claim follows directly from Theorem 5 when $\mathbf{a} = \mathbf{0}$. If $\mathbf{a} \in \mathbb{F}_2^n$, such that $l_{\mathbf{a},0}$ is balanced in biased domain, i.e., $\sum_{\mathbf{x}\in\mathrm{supp}(l_{\mathbf{a},0})} p(\mathbf{x}) = \frac{1}{2}$, the second claim follows. □

In Section III-C, we saw that the behavior of a linear function in the biased domain is different than its behavior in the uniform domain. This is also true for bent functions, so in the biased domain, a bent function may not remain bent. For example, let $n = 10$ and $f \in \mathcal{B}_4$ be the bent function $f(\mathbf{x}) = x_1x_2 + x_3x_4$. The biased Walsh–Hadamard transform of $f$ is given in Table III. Also, the sum of the squares of the biased Walsh–Hadamard coefficients of $f$ is 1.0763.

| $x_4x_3x_2x_1$ | $p(\mathbf{x})$ | $f(\mathbf{x})$ | $\mathcal{W}_f(\mathbf{a})$ | $\mathcal{W}_f^B(\mathbf{a})$ |
|---|---|---|---|---|
| 0000 | $\frac{1}{42}$ | 0 | $\frac{1}{4}$ | $\frac{13}{63}$ |
| 0001 | $\frac{5}{84}$ | 0 | $\frac{1}{4}$ | $\frac{2}{21}$ |
| 0010 | $\frac{5}{84}$ | 0 | $\frac{1}{4}$ | $\frac{2}{21}$ |
| 0011 | $\frac{5}{63}$ | 1 | $-\frac{1}{4}$ | $-\frac{2}{7}$ |
| 0100 | $\frac{5}{84}$ | 0 | $\frac{1}{4}$ | $\frac{2}{21}$ |
| 0101 | $\frac{5}{63}$ | 0 | $\frac{1}{4}$ | $\frac{13}{63}$ |
| 0110 | $\frac{5}{63}$ | 0 | $\frac{1}{4}$ | $\frac{13}{63}$ |
| 0111 | $\frac{5}{84}$ | 1 | $-\frac{1}{4}$ | $-\frac{2}{21}$ |
| 1000 | $\frac{5}{84}$ | 0 | $\frac{1}{4}$ | $\frac{2}{21}$ |
| 1001 | $\frac{5}{63}$ | 0 | $\frac{1}{4}$ | $\frac{13}{63}$ |
| 1010 | $\frac{5}{63}$ | 0 | $\frac{1}{4}$ | $\frac{13}{63}$ |
| 1011 | $\frac{5}{84}$ | 1 | $-\frac{1}{4}$ | $-\frac{2}{21}$ |
| 1100 | $\frac{5}{63}$ | 1 | $-\frac{1}{4}$ | $-\frac{2}{7}$ |
| 1101 | $\frac{5}{84}$ | 1 | $-\frac{1}{4}$ | $-\frac{2}{21}$ |
| 1110 | $\frac{5}{84}$ | 1 | $-\frac{1}{4}$ | $-\frac{2}{21}$ |
| 1111 | $\frac{1}{42}$ | 0 | $\frac{1}{4}$ | $\frac{13}{63}$ |

TABLE III: Biased Walsh–Hadamard spectrum of a bent function

### *E. The biased Walsh–Hadamard transform of a direct sum of Boolean functions*

In this section, we consider the direct sum of two Boolean functions $f_1$ and $f_2$ (i.e., $f = f_1 + f_2$) in a biased domain. Firstly, we prove the convolution theorem in the biased domain. Further, we present several results related to bound on

bias of direct sum of Boolean functions. Let $n = n_1+n_2$, and $\mathbf{x} = \mathbf{x}'||\mathbf{x}'' \in \mathbb{F}_2^n$, where $\mathbf{x}' \in \mathbb{F}_2^{n_1}$ and $\mathbf{x}'' \in \mathbb{F}_2^{n_2}$. Then, it can be observed that $Pr[\mathbf{x}] = Pr[\mathbf{x}', \mathbf{x}''] = Pr[\mathbf{x}'/\mathbf{x}'']Pr[\mathbf{x}''] = Pr[\mathbf{x}''/\mathbf{x}']Pr[\mathbf{x}']$, for any $\mathbf{x} \in \mathbb{F}_2^n$. The biased Walsh–Hadamard transform of $f(\mathbf{x}) = f_1(\mathbf{x}')+f_2(\mathbf{x}'')$ at $\mathbf{a} = \mathbf{a}'||\mathbf{a}''$ will be equal to

$$\begin{aligned}\mathcal{W}_f^B(\mathbf{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} \\ &= \sum_{\mathbf{x}''\in\mathbb{F}_2^{n_2}} p(\mathbf{x}'')(-1)^{f_2(\mathbf{x}'')+\mathbf{a}''\cdot\mathbf{x}''} \\ &\qquad \sum_{\mathbf{x}'\in\mathbb{F}_2^{n_1}} p(\mathbf{x}'/\mathbf{x}'')(-1)^{f_1(\mathbf{x}')+\mathbf{a}'\cdot\mathbf{x}'},\end{aligned} \tag{2}$$

where $p(\mathbf{x}'/\mathbf{x}'') = Pr[\mathbf{x}'/\mathbf{x}'']$. From Equation (2), it can be observed that it is difficult to calculate biased Walsh–Hadamard transform of $f = f_1 + f_2$, even though we have the biased Walsh–Hadamard transform of two sub-functions $f_1$, $f_2$, due to the fact in general $Pr[\mathbf{x}'/\mathbf{x}''] \neq Pr[\mathbf{x}']$.

Let us consider $n = n_1+n_2$ and $f(\mathbf{x}) = f_1(\mathbf{x}')+f_2(\mathbf{x}'')$ on $\mathbb{F}_2^n$, where $f_1(\mathbf{x}')$ depends on the first $n_1$ number of variables of $\mathbf{x}$ and $f_2(\mathbf{x}'')$ depends on last $n_2$ number of variables. Here $\mathbf{x} = \mathbf{x}'||\mathbf{x}''$. If the domain of $f$ is the uniform domain, then one can calculate the Walsh–Hadamard transform of $f$ at the point $\mathbf{a}$ by calculating the Walsh–Hadamard transform of $f_1$ and $f_2$ at the points $\mathbf{a}'$ and $\mathbf{a}''$, respectively, where $\mathbf{a} = \mathbf{a}'||\mathbf{a}''$. Thus, only two independent tables of size $1\times 2^{n_1}$ and $1\times 2^{n_2}$ are required to calculate the Walsh–Hadamard spectrum of $f$. However, this is not the scenario for the biased Walsh–Hadamard transform. From Theorem 6 and Corollary 4 it can be observed that we need more information to calculate the biased Walsh–Hadamard transform of $f$ at a point $\mathbf{a}$. In fact we need three probability tables $P_1, P_2$ and $P_3$ of sizes $1\times(n+1)$, $1\times(n_1+1)$ and $1\times(n_2+1)$ corresponding to $\mathbf{x}\in\mathbb{F}_2^n$, $\mathbf{x}'\in\mathbb{F}_2^{n_1}$ and $\mathbf{x}''\in\mathbb{F}_2^{n_2}$, respectively, and we also need two more tables $T_{f_1}$ and $T_{f_2}$ of sizes $2^{n_1}\times(n_1+1)$ and $2^{n_2}\times(n_2+1)$ (in the worst case) corresponding to the biased Walsh–Hadamard transform values of $f_1$ and $f_2$, respectively. Certainly, the computation complexity will increase when the there are many terms in the direct sum.

Next, we present a convolution theorem over the inputs of fixed weight. We are interested to compute $\mathcal{W}_f^{B(k)}$ (as defined in Equation (2), but here the sum is over $\mathbf{x}\in E_{n,k}$) for $f = f_1 + f_2$, where $0\le k\le n$. One may note that if $\mathbf{x},\mathbf{y}\in\mathbb{F}_2^m$ and $wt(\mathbf{x}) = wt(\mathbf{y})$, then $Pr[\mathbf{x}] = Pr[\mathbf{y}]$. We use the notation $p_{m,i}$ to denote $Pr[\mathbf{x}]$, for all $\mathbf{x}\in E_{m,i}$, where $0\le i\le m$. In Equation (3), we show a relation between the Walsh–Hadamard transform of a Boolean function in the uniform and non-uniform domain:

$$\mathcal{W}_f^{B(k)}(\mathbf{a}) = p\binom{n}{k}\mathcal{W}_f^{(k)}(\mathbf{a}), \quad \forall\,\mathbf{a}\in\mathbb{F}_2^n, \tag{3}$$

where $0\le k\le n$ and $p = Pr[\mathbf{x} : wt(\mathbf{x}) = k]$.

**Theorem 6** (Restricted Domain Convolution)**.** *Let $n = n_1+n_2$ and $f = f_1 + f_2$, where $f_i\in\mathcal{B}_{n_i}$, $i\in\{1,2\}$. Then, for any $\mathbf{a} = \mathbf{a}'||\mathbf{a}''\in\mathbb{F}_2^n$ and $0\le k\le n$,*

$$\begin{aligned}\mathcal{W}_f^{B(k)}(\mathbf{a}) &= p_{n,k}\sum_{i=0}^{k}\binom{n_1}{i}\binom{n_2}{k-i}\mathcal{W}_{f_1}^{(i)}(\mathbf{a}')\mathcal{W}_{f_2}^{(k-i)}(\mathbf{a}'') \\ &= \sum_{i=0}^{k}\frac{p_{n,k}}{q_{n_1,i}q_{n_2,k-i}}\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}')\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}''),\end{aligned}$$

*where $q_{n_1,i} = \frac{\binom{n_2}{k-i}}{\binom{n}{k}}, q_{n_2,k-i} = \frac{\binom{n_1}{i}}{\binom{n}{k}}$.*

*Proof.* For any $\mathbf{a} = \mathbf{a}'||\mathbf{a}''\in\mathbb{F}_2^n$ and $0\le k\le n$, we have

$$\begin{aligned}&\mathcal{W}_f^{B(k)}(\mathbf{a}) \\ &= \sum_{\mathbf{x}\in E_{n,k}} Pr[\mathbf{x}](-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} \\ &= p_{n,k}\sum_{\mathbf{x}\in E_{n,k}}(-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}} \\ &= p_{n,k}\sum_{i=0}^{k}\sum_{\mathbf{x}'\in E_{n_1,i}^{n=n_1+n_2,k}}\sum_{\mathbf{x}''\in E_{n_2,k-i}^{n=n_1+n_2,k}}(-1)^{f_1(\mathbf{x}')+\mathbf{a}'\cdot\mathbf{x}'} \\ &\qquad\qquad (-1)^{f_2(\mathbf{x}'')+\mathbf{a}''\cdot\mathbf{x}''} \\ &= p_{n,k}\sum_{i=0}^{k}\sum_{\mathbf{x}'\in E_{n_1,i}^{n=n_1+n_2,k}}(-1)^{f_1(\mathbf{x}')+\mathbf{a}'\cdot\mathbf{x}'} \\ &\qquad\qquad \sum_{\mathbf{x}''\in E_{n_2,k-i}^{n=n_1+n_2,k}}(-1)^{f_2(\mathbf{x}'')+\mathbf{a}''\cdot\mathbf{x}''} \\ &= p_{n,k}\sum_{i=0}^{k}\binom{n_1}{i}\binom{n_2}{k-i}\mathcal{W}_{f_1}^{(i)}(\mathbf{a}')\mathcal{W}_{f_2}^{(k-i)}(\mathbf{a}'').\end{aligned}$$

The above relation can also be rewritten in terms of the biased Walsh–Hadamard transform. From Equation (3), we obtain,

$$\mathcal{W}_f^{B(k)}(\mathbf{a}) = \sum_{i=0}^{k}\frac{p_{n,k}}{q_{n_1,i}q_{n_2,k-i}}\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}')\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}'').$$

Hence, we obtain both the relations in terms of the Walsh–Hadamard transform in the uniform and non-uniform domains. □

The following corollary follows from Theorem 6.

**Corollary 4.** *Let $n = n_1 + n_2$ and $f = f_1 + f_2$, where $f_i\in\mathcal{B}_{n_i}$, $i\in\{1,2\}$. For any $\mathbf{a} = \mathbf{a}'||\mathbf{a}''\in\mathbb{F}_2^n$,*

$$\begin{aligned}\mathcal{W}_f^B(\mathbf{a}) &= \sum_{k=0}^{n}\mathcal{W}_f^{B(k)}(\mathbf{a}) \\ &= \sum_{k=0}^{n}p_{n,k}\sum_{i=0}^{k}\binom{n_1}{i}\binom{n_2}{k-i}\mathcal{W}_{f_1}^{(i)}(\mathbf{a}')\mathcal{W}_{f_2}^{(k-i)}(\mathbf{a}'') \\ &= \sum_{k=0}^{n}\sum_{i=0}^{k}\frac{p_{n,k}}{q_{n_1,i}q_{n_2,k-i}}\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}')\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}'').\end{aligned}$$

We have already observed that it is indeed difficult to compute the biased Walsh–Hadamard transform of $f = f_1+f_2$ over a biased domain with a large number of variables. So we continue computing an appropriate bound for the biased

Walsh–Hadamard transform of $f \in \mathcal{B}_n$, where $f = f_1 + f_2 \in \mathcal{B}_n$, with $f_i \in \mathcal{B}_{n_i},\ i = 1, 2$.

In 2017, Carlet et al. [2] proved the following lemma.

**Lemma 2** ([2]). *If $n = n_1 + n_2$ and $f = f_1 + f_2,\ f_i \in \mathcal{B}_{n_i}$, $i \in \{1, 2\}$, then*

$$\max_{\mathbf{a}} \left|\mathcal{W}_f^{(k)}(\mathbf{a})\right| \le \sum_{i=0}^{k} p_{n,k} \Big\{ \max_{\mathbf{a}_1} \left| \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{a}_1\cdot\mathbf{x}_1} \right| \max_{\mathbf{a}_2} \left| \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_1(\mathbf{x}_2)+\mathbf{a}_2\cdot\mathbf{x}_2} \right| \Big\}.$$

The following theorem shows that using biased Walsh–Hadamard transform we may get an improved bound.

**Theorem 7** ([7]). *For all $0 \le k \le n$, the following inequality holds*

$$\sum_{i=0}^{k} p_{n,k} \max_{\mathbf{a}_1 \in \mathbb{F}_2^{n_1}} \left| \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{a}_1\cdot\mathbf{x}_1} \right| \max_{\mathbf{a}_2 \in \mathbb{F}_2^{n_2}} \left| \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_1(\mathbf{x}_2)+\mathbf{a}_2\cdot\mathbf{x}_2} \right| \ge \sum_{i=0}^{k} \max_{\mathbf{a}_1 \in \mathbb{F}_2^{n_1}} \left|\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}_1)\right| \max_{\mathbf{a}_2 \in \mathbb{F}_2^{n_2}} \left|\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}_2)\right|.$$

From the Theorem 7 it can be observed that the upper bound provided by Carlet et al. [2] (see Lemma 2) is much higher than

$$G = \sum_{i=0}^{k} \max_{\mathbf{a}_1 \in \mathbb{F}_2^{n_1}} |\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}_1)| \max_{\mathbf{a}_2 \in \mathbb{F}_2^{n_2}} |\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}_2)|.$$

One may think that $G$ can be smaller than $\max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^{(k)}(\mathbf{a})|$. In fact, we have observed that in some cases $G \le \max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^{(k)}(\mathbf{a})|$ but under some specific conditions $G \ge \max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^{(k)}(\mathbf{a})|$. To prove both the inequalities we start with the following lemma.

**Lemma 3** ([7]). *Let $a_i$ be positive numbers and $b_i$ be any integer numbers (positive or negative), where $i = 0, 1, \ldots, k$. If $\left|\left|\sum_{i=0}^{k} a_i b_i\right| - \left|\sum_{i,j=0; i\neq j=0}^{k} a_i b_j\right|\right| \le \left|\sum_{i=0}^{k} a_i b_i\right|$, and the sums $\sum_{i=0}^{k} a_i b_i$, $\sum_{i,j=0;\ i\neq j}^{k} a_i b_j$ have opposite signs, then $\left|\sum_{i=0}^{k} a_i b_i\right| \ge \left(\sum_{i=0}^{k} a_i\right) \left|\sum_{j=0}^{k} b_j\right|$.*

We use the result of Lemma 3 to prove $G \ge \max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^{(k)}(\mathbf{a})|$. The proof of the the Theorem 8 can be found in [7].

**Theorem 8** ([7]). *Let $f = f_1 + f_2 \in \mathcal{B}_n,\ f_i \in \mathcal{B}_{n_i},\ i = 1, 2$, $A_i := q_{n_1,i} q_{n_2,k-i}$ and*

$$B_i := \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{a}_1\cdot\mathbf{x}_1} \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_2(\mathbf{x}_2)+\mathbf{a}_2\cdot\mathbf{x}_2},$$

*for all $0 \le i \le k$ (here $q_{n_1,i} = \frac{\binom{n_2}{k-i}}{\binom{n}{k}}$, $q_{n_2,k-i} = \frac{\binom{n_1}{i}}{\binom{n}{k}}$). Then*

$$\max_{\mathbf{a}\in\mathbb{F}_2^n} \left|\mathcal{W}_f^{(k)}(\mathbf{a})\right| \le \sum_{i=0}^{k} \max_{\mathbf{a}_1 \in \mathbb{F}_2^{n_1}} \left|\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}_1)\right| \max_{\mathbf{a}_2 \in \mathbb{F}_2^{n_2}} \left|\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}_2)\right|,$$

*if $\left|\left|\sum_{i=0}^{k} A_i B_i\right| - \left|\sum_{i=0}^{k} A_i B_i - p_{n,k} \sum_{j=0}^{k} B_j\right|\right| \le \left|\sum_{i=0}^{k} A_i B_i\right|$, where $p_{n,k} = \frac{1}{\binom{n}{k}}$, and, the expressions $\sum_{i=0}^{k} A_i B_i$, $p_{n,k} \sum_{j=0}^{k} B_j - \sum_{i=0}^{k} A_i B_i$ have opposite signs.*

Our next result shows that, under some specific conditions the lower bound of $\max_{\mathbf{a}\in\mathbb{F}_2^n} |\mathcal{W}_f^{(k)}(\mathbf{a})|$ can be achieved in terms of the biased Walsh–Hadamard transform.

**Theorem 9.** *Let $0 \le i \le k$, $\mathbf{c}_i \in \mathbb{F}_2^{n_1}$, $\mathbf{d}_i \in \mathbb{F}_2^{n_2}$, $q_{n_1,i} = \frac{\binom{n_2}{k-i}}{\binom{n}{k}}$, $q_{n_2,k-i} = \frac{\binom{n_1}{i}}{\binom{n}{k}}$, and*

$$\max_{\mathbf{a}_1 \in \mathbb{F}_2^{n_1}} \left|\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}_1)\right| = q_{n_1,i} \left| \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{c}_i\cdot\mathbf{x}_1} \right|,$$

$$\max_{\mathbf{a}_2 \in \mathbb{F}_2^{n_2}} \left|\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}_2)\right| = q_{n_2,k-i} \left| \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_2(\mathbf{x}_2)+\mathbf{d}_i\cdot\mathbf{x}_2} \right|.$$

*If $\sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{c}_i\cdot\mathbf{x}_1} \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_2(\mathbf{x}_2)+\mathbf{d}_i\cdot\mathbf{x}_2}$ has constant sign, for all $0 \le i \le k$, then,*

$$\sum_{i=0}^{k} \max_{\mathbf{a}_1 \in \mathbb{F}_2^{n_1}} \left|\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}_1)\right| \max_{\mathbf{a}_2 \in \mathbb{F}_2^{n_2}} \left|\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}_2)\right| \le \max_{\mathbf{a}\in\mathbb{F}_2^n} \left|\mathcal{W}_f^{(k)}(\mathbf{a})\right|.$$

*Proof.* We compute

$$\begin{aligned}
&\sum_{i=0}^{k} \max_{\mathbf{a}_1 \in \mathbb{F}_2^{n_1}} \left|\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}_1)\right| \max_{\mathbf{a}_2 \in \mathbb{F}_2^{n_2}} \left|\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}_2)\right| \\
&= \sum_{i=0}^{k} \left|\mathcal{W}_{f_1}^{B(i)}(\mathbf{c}_i) \mathcal{W}_{f_2}^{B(k-i)}(\mathbf{d}_i)\right| \\
&= \sum_{i=0}^{k} q_{n_1,i} q_{n_2,k-i} \Big| \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{c}_i\cdot\mathbf{x}_1} \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_2(\mathbf{x}_2)+\mathbf{d}_i\cdot\mathbf{x}_2} \Big| \qquad (4) \\
&\le \sum_{i=0}^{k} q_{n_1,i} q_{n_2,k-i} \sum_{i=0}^{k} \Big| \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{c}_i\cdot\mathbf{x}_1} \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_2(\mathbf{x}_2)+\mathbf{d}_i\cdot\mathbf{x}_2} \Big| \\
&= \frac{1}{\binom{n}{k}} \sum_{i=0}^{k} \Big| \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{c}_i\cdot\mathbf{x}_1} \qquad (5)
\end{aligned}$$

$$\left. \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_2(\mathbf{x}_2)+\mathbf{d}_i\cdot\mathbf{x}_2} \right|$$

$$= \frac{1}{\binom{n}{k}} \Big| \sum_{i=0}^{k} \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{c}_i\cdot\mathbf{x}_1} \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_2(\mathbf{x}_2)+\mathbf{d}_i\cdot\mathbf{x}_2} \Big|,$$

$$\leq \frac{1}{\binom{n}{k}} \max_{\mathbf{a}=\mathbf{b}_1||\mathbf{b}_2} \Big| \sum_{i=0}^{k} \sum_{\mathbf{x}_1 \in E_{n_1,i}} (-1)^{f_1(\mathbf{x}_1)+\mathbf{b}_1\cdot\mathbf{x}_1} \sum_{\mathbf{x}_2 \in E_{n_2,k-i}} (-1)^{f_2(\mathbf{x}_2)+\mathbf{b}_2\cdot\mathbf{x}_2} \Big|$$

$$\leq \max_{\mathbf{a}\in\mathbb{F}_2^n} \left| \mathcal{W}_f^{(k)}(\mathbf{a}) \right|,$$

and the theorem is shown. □

## IV. More accurate calculations of biases by our technique and comparisons with previous work

This section presents a numerical comparison between our bound and the bound proposed by Carlet et al. [2] (see Lemma 2). We first consider a 12-variable FLIP type function to provide a comparison, then we proceed further to compare the same for the nonlinear function of FLIP.

### A. Comparison for a small Boolean function

We consider a small Boolean function $f$ on 12 variables (FLIP type). The function $f$ is a direct sum of three functions $f_1$, $f_2$, $f_3$ (i.e., $f = f_1 + f_2 + f_3$), where $f_1(x_0, x_1) = x_0 + x_1$, $f_2(x_0, \ldots, x_3) = x_0x_1 + x_2x_3$ and $f_3(x_0, \ldots, x_5) = x_0 + x_1x_2 + x_3x_4x_5$. So, $f(x_0, \ldots, x_{11}) = f_1(x_0, x_1) + f_2(x_2, \ldots, x_5) + f_3(x_6, \ldots, x_{11})$. We assume that the function $f$ takes inputs from a restricted set $E_{12,6}$. We consider two types of Walsh–Hadamard transforms to compute bounds for bias of $f$. We first consider classical Walsh–Hadamard transform $\mathcal{W}_f$ (same as Carlet et al. [2]), and secondly, we consider our defined biased Walsh–Hadamard transform $\mathcal{W}_f^B$.

We first compute both types of Walsh–Hadamard transform values (classical and biased) of $f_1$, $f_2$, $f_3$ for all possible weights of the inputs of each function. Let $\mathbf{x} = \mathbf{x}_1||\mathbf{x}_2||\mathbf{x}_3$ and $f(\mathbf{x}) = f_1(\mathbf{x}_1) + f_2(\mathbf{x}_2) + f_3(\mathbf{x}_3)$. We compute the maximum absolute Walsh–Hadamard transform values of $f_1$, $f_2$, $f_3$ corresponding to each weight of $\mathbf{x}_1$, $\mathbf{x}_2$ and $\mathbf{x}_3$. From these maximum absolute Walsh–Hadamard transform values we compute the maximum absolute value of Walsh–Hadamard transform of $f(\mathbf{x}) = f_1(\mathbf{x}_1) + f_2(\mathbf{x}_2) + f_3(\mathbf{x}_3)$, when $\mathbf{x} \in E_{12,6}$. We multiply those maximum absolute Walsh–Hadamard transform values for which $wt(\mathbf{x}_1) + wt(\mathbf{x}_2) + wt(\mathbf{x}_3) = 6$. We further add these multiplied values. To compute the bias bound of $f$ in classical Walsh–Hadamard setup we divide the final value by $\binom{12}{6}$.

Here the domain of the function $f$ is $E_{12,6}$. We have observed that, the actual bias of the function $f$ in $E_{12,6}$ is $\approx 0.264069$. One may note that in uniform domain (i.e., $\mathbb{F}_2^{12}$) $l_1 = l_{\mathbf{a}_1,0} = x_0 + x_1 + x_6$ is the closest linear function to $f$ as the monomials of the form $x_ix_j$ or $x_ix_jx_k$ are always 0 unless all variables involved in the monomials are 1. It has been observed that, the biases between $f$ and $l_1$ in the domains $\mathbb{F}_2^{12}$ and $E_{12,6}$ are $|\mathcal{W}_f(\mathbf{a}_1)| = 0.09375$ and $|\mathcal{W}_f^{(6)}(\mathbf{a}_1)| = 0.099567$, respectively. If we restrict the domain of the function $f$ to $E_{12,6}$, then the bias between $f$ and a linear function is highest for $l_2 = l_{\mathbf{a}_2,0} = x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6$ instead of $l_1 = x_0 + x_1 + x_6$. The bias between $f$ and $l_2$ in restricted domain $E_{12,6}$ is $|\mathcal{W}_f^{(6)}(\mathbf{a}_2)| = 0.264069$, but the bias between $f$ and $l_1$ in the restricted domain $E_{12,6}$ is $|\mathcal{W}_F^{(6)}(\mathbf{a}_1)| = 0.099567$. The linear functions which are closest to $f$ in $E_{12,6}$ are provided below:

1) $l_{\mathbf{a}_2,0} = l_2 = x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6$: $|\mathcal{W}_f^{(6)}(\mathbf{a}_2)| = 0.264069$, $|\mathcal{W}_f(\mathbf{a}_2)| = 0.09375$.
2) $l_{\mathbf{a}_3,0} = l_3 = x_0 + x_1 + x_2 + x_3 + x_6 + x_7 + x_8$: $|\mathcal{W}_f^{(6)}(\mathbf{a}_3)| = 0.264069$, $|\mathcal{W}_f(\mathbf{a}_3)| = 0.09375$.
3) $l_{\mathbf{a}_4,0} = l_4 = x_0 + x_1 + x_4 + x_5 + x_6 + x_7 + x_8$: $|\mathcal{W}_f^{(6)}(\mathbf{a}_4)| = 0.264069$, $|\mathcal{W}_f(\mathbf{a}_4)| = 0.09375$.
4) $l_{\mathbf{a}_5,0} = l_5 = x_2 + x_3 + x_9 + x_{10} + x_{11}$: $|\mathcal{W}_f^{(6)}(\mathbf{a}_5)| = 0.264069$, $|\mathcal{W}_f(\mathbf{a}_5)| = 0$.
5) $l_{\mathbf{a}_6,0} = l_6 = x_4 + x_5 + x_9 + x_{10} + x_{11}$: $|\mathcal{W}_f^{(6)}(\mathbf{a}_6)| = 0.264069$, $|\mathcal{W}_f(\mathbf{a}_6)| = 0$.
6) $l_{\mathbf{a}_7,0} = l_7 = x_7 + x_8 + x_9 + x_{10} + x_{11}$: $|\mathcal{W}_f^{(6)}(\mathbf{a}_7)| = 0.264069$, $|\mathcal{W}_f(\mathbf{a}_7)| = 0$.

Table IV provides a comparison between the original bias and the bounds obtained by using classical and biased Walsh–Hadamard transforms. From the Table IV it can be observed that our bound is much tighter than the bound proposed by Carlet et al. [2].

| | |
|---|---|
| Original bias | $\approx 0.264069$ |
| Carlet et al. [2] | $\leq 0.772727$ |
| This paper | $\geq 0.20857$ |

TABLE IV: Correlation bound comparison

### B. Comparison for the actual nonlinear filter function of FLIP

In this section, we provide a comparison of the bounds for the bias of the nonlinear filter function of the FLIP stream cipher. To compute the bounds we extend the ideas of Section IV-A. We consider the nonlinear filter function $F$ of $\text{FLIP}_{530}(42, 128, 360)$. This function is a direct sum of three Boolean functions $f_1$, $f_2$ and $f_3$ (i.e., $F = f_1 + f_2 + f_3$), where $f_1$ is a linear function involving 42 variables, $f_2$ is a quadratic bent function involving 128 variables and $f_3$ is a direct sum of 8 triangular functions. Here, each triangular function is of degree 9 and involving 45 variables. As each triangular function has one degree one term, so the final linear function of $F$ will involve 50 variables. Also each, triangular function has exactly one term of degree two. Hence $F$ will have 72 terms of degree 2, involving 144 variables.

We follow the same technique as in the toy example. We compute the bias bound by using classical and our biased Walsh–Hadamard transform. To compute the bounds, we first break the complete function $f$ into three parts. In the first part, we consider 5 linear Boolean functions, each involving 10 variables. The second part is based on 18 quadratic functions,

each involving 8 variables. The third part is based on eight degree 3 to degree 9 terms.

We follow a similar technique as in Section IV-A to compute the bias bound as in Lemma 2 of Carlet et al. [2] and the bound obtained through our study. The bias bound of Carlet et al.'s is $G_c = \frac{1}{2^{13.59}}$. The bias bound obtained using our biased Walsh–Hadamard transform is $G_o = \frac{1}{2^{18.49}}$. Lemma 2 clearly shows that $G_c$ will be an upper bound of the original bias (see Lemma 3 of [2] for more detail).

Our next goal is to show that $G_o$ is a lower bound of the original bias. We use Theorem 9 for this purpose. In the computation of $G_o$, the product of probabilities ($q_{n_1,i}q_{n_2,k-i}$ of Theorem 9) is the product of probabilities corresponding to the 5 linear functions each involving 10 variables, probabilities corresponding to 18 functions of degree 2 each involving 8 variables, and the probabilities corresponding to the eight degree $3, 4, \ldots, 9$ terms. Experimentally, we observed that the maximum of this product of probabilities is much smaller than $\frac{1}{\binom{530}{265}}$. We replace the product of probabilities by $\frac{1}{\binom{530}{265}}$ to achieve the inequality between Equations (4) and (5) from the proof of Theorem 9. Further, we observe that all functions, $f_1 = x_0+x_1+x_2+x_3+x_4+x_5+x_6+x_7+x_8+x_9$, $f_2 = x_0x_1+x_2x_3+x_4x_5+x_6x_7$, $f_3 = x_0x_1x_2$, $f_4 = x_0x_1x_2x_3$, $f_5 = x_0x_1x_2x_3x_4$, $f_6 = x_0x_1x_2x_3x_4x_5$, $f_7 = x_0x_1x_2x_3x_4x_5x_6$, $f_8 = x_0x_1x_2x_3x_4x_5x_6x_7$, $f_9 = x_0x_1x_2x_3x_4x_5x_6x_7x_8$ satisfy the condition of Theorem 9. In fact, there exists at least one point $\mathbf{b}$ for each function $f_j$ such that $\sum_{\mathbf{x}\in E_{n,i}}(-1)^{f_j(\mathbf{x})+\mathbf{b}\cdot\mathbf{x}}$ attains $\max_{\mathbf{a}}\left|\sum_{\mathbf{x}\in E_{n,i}}(-1)^{f_j(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}}\right|$ for all weights $i$.

The existence of a point $\mathbf{b}$ corresponding to each weight starting from weight zero to total weight is given below (points are provided in integer form)

1) For $f_1$, $\mathbf{b}$: $0, 1023, 0, 1023, 0, 1023, 0, 1023,\ 0, 1023, 0$.
2) For $f_2$, $\mathbf{b}$: $0, 0, 0, 63, 15, 3, 0, 255, 0$.
3) For $f_3$, $\mathbf{b}$: $0, 0, 0, 1$.
4) For $f_4$, $\mathbf{b}$: $0, 0, 0, 0, 1$.
5) For $f_5$, $\mathbf{b}$: $0, 0, 0, 0, 0, 1$.
6) For $f_6$, $\mathbf{b}$: $0, 0, 0, 0, 0, 0, 1$.
7) For $f_7$, $\mathbf{b}$: $0, 0, 0, 0, 0, 0, 0, 1$.
8) For $f_8$, $\mathbf{b}$: $0, 0, 0, 0, 0, 0, 0, 0, 1$.
9) For $f_9$, $\mathbf{b}$: $0, 0, 0, 0, 0, 0, 0, 0, 0, 1$.

Hence, from Theorem 9 we infer that $G_o = \frac{1}{2^{18.49}}$ will be a lower bound of the original bias of the nonlinear filter function of the FLIP stream cipher. This is summarized in Table V:

| | |
|---|---|
| Carlet et al. [2] | $\leq \frac{1}{2^{13.59}}$ |
| This paper | $\geq \frac{1}{2^{18.49}}$ |

TABLE V: Correlation comparison

Finally, let us summarize the theoretical results of our work and compare it to the existing results available in [2], [8]. Carlet et al. [2] first proved that the lower bound of the bias of a function in a restricted domain will be $\max_{\mathbf{a}\in\mathbb{F}_2^n}|\mathcal{W}_f^{(k)}(\mathbf{a})| \geq \frac{1}{\binom{n}{k}}\sqrt{\binom{n}{k}+\lambda}$ (the parameter $\lambda$ is defined in [2, Prop. 8, p. 207]). Later, Mesnager et al. [8] provided an improved lower bound of the original bias, $\max_{\mathbf{a}\in\mathbb{F}_2^n}|\mathcal{W}_f^{(k)}(\mathbf{a})| \geq \frac{1}{\binom{n}{k}}\sqrt{\binom{n}{k}+\lambda+\max\left(\theta, \frac{1}{\binom{n}{k}}\gamma-\lambda\right)}$ (the parameters $\lambda, \gamma, \theta$ are defined in [8, Thm. 16]). All these bounds are not related to the bias of direct sum of functions in restricted domain. In this paper, we have shown that the original bias of a direct sum of two functions (i.e., $f = f_1 + f_2$) in a restricted domain can be represented as the biased Walsh–Hadamard transform of $f_1$, $f_2$. We are able to find a lower bound of the original bias under some constraints, and the lower bound is $\max_{\mathbf{a}\in\mathbb{F}_2^n}\left|\mathcal{W}_{f_1+f_2}^{(k)}(\mathbf{a})\right| \geq \sum_{i=0}^{k}\max_{\mathbf{a}_1\in\mathbb{F}_2^{n_1}}\left|\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}_1)\right|\max_{\mathbf{a}_2\in\mathbb{F}_2^{n_2}}\left|\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}_2)\right|$. Carlet et al. [2] obtained an upper bound of the original bias of $f = f_1 + f_2$ in a restricted domain, and the bound is

$$\max_{\mathbf{a}\in\mathbb{F}_2^n}\left|\mathcal{W}_{f_1+f_2}^{(k)}(\mathbf{a})\right| \leq \frac{1}{\binom{n}{k}}\sum_{i=0}^{k}\Big(\max_{\mathbf{a}\in\mathbb{F}_2^{n_1}}\left|\sum_{\mathbf{x}\in E_{n_1,i}}(-1)^{f_1(\mathbf{x})+\mathbf{a}.\mathbf{x}}\right| \max_{\mathbf{b}\in\mathbb{F}_2^{n_2}}\left|\sum_{\mathbf{y}\in E_{n_2,k-i}}(-1)^{f_2(\mathbf{y})+\mathbf{b}.\mathbf{y}}\right|\Big).$$

We note that Mesnager et al. [8] do not provide any result related to the bias of direct sum of Boolean functions in a restricted domain. In this paper, we found (under some conditions) an upper bound of the bias of $f_1+f_2$ in a restricted domain in terms of the biased Walsh–Hadamard transform of sub-functions $f_1$ and $f_2$, namely, $\max_{\mathbf{a}\in\mathbb{F}_2^n}|\mathcal{W}_{f_1+f_2}^{(k)}(\mathbf{a})| \leq \sum_{i=0}^{k}\max_{\mathbf{a}_1\in\mathbb{F}_2^{n_1}}\left|\mathcal{W}_{f_1}^{B(i)}(\mathbf{a}_1)\right|\max_{\mathbf{a}_2\in\mathbb{F}_2^{n_2}}\left|\mathcal{W}_{f_2}^{B(k-i)}(\mathbf{a}_2)\right|$.

## V. Conclusion

In this paper, we have proposed a technique to study the cryptographic properties of Boolean function, whose inputs do not follow uniform distribution. In our study, we first define the notion of correlation between two Boolean functions in a non-uniform domain. Further, we show a relation between this correlation and our newly defined biased Walsh–Hadamard transform. We use the biased Walsh–Hadamard transform to study several cryptographic properties of a Boolean function, whose inputs follow a non-uniform distribution. We next show a convolution theorem for the biased Walsh–Hadamard transform. Due to the computation limitation for the convolution on a large number of variables, we proved several inequalities related to the bias of direct sum of functions. Consequently, we obtained a lower bound for the bias of the nonlinear filter function of FLIP by using biased Walsh–Hadamard transform. Further, we provide a comparison with the existing result. Certainly, our work provides a new direction to study several properties of Boolean function over a biased domain. Our results provide more accurate calculation of the biases of Boolean function over restricted domain, which help to determine the security parameter of FLIP type ciphers.

## REFERENCES


[1] A. Canteaut, S. Carpov, C. Fontaine, T. Lepoint, M. Naya-Plasencia, P. Paillier and R. Sirdey. Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression. *Journal of Cryptology* 31:3 (2018), https://doi.org/10.1007/s00145-017-9273-9 (earlier version in FSE 2016, LNCS 9783, pp. 313–333, Springer).

[2] C. Carlet, P. Méaux and Y. Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. *IACR Trans. Symmetric Cryptology* 3 (2017), pp. 192–227 (presented at FSE 2018).

[3] S. Duval, V. Lallemand and Y. Rotella. Cryptanalysis of the FLIP Family of Stream Ciphers. *Annual Cryptology Conference 2016 (CRYPTO, 2016)*, Springer, pp. 457–475, 2016.

[4] S. Gangopadhyay, A. K. Gangopadhyay, S. Pollatos and P. Stănică. Cryptographic Boolean functions with biased inputs. *Cryptography and Communications* 9:2 (2017), 301–314.

[5] P. Méaux. Symmetric Encryption Scheme adapted to Fully Homomorphic Encryption Scheme. *In: Journées Codage et Cryptographie - JC2 2015 - 12éme édition des Journées Codage et Cryptographie du GT C2, 5 au 9 octobre 2015, La Londeles-Maures, France (2015),* http://imath.univ-tln.fr/C2/.

[6] P. Méaux, A. Journault, F.-X. Standaert and C. Carlet. Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. *Advances in Cryptology-35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT, 2016)*, Springer, pp. 311–343, 2016.

[7] S. Maitra, B. Mandal, T. Martinsen, D. Roy and P. Stănică. Tools in analyzing linear approximation for Boolean functions related to FLIP *Proceeding of the 19th International Conference on Cryptology in India (Indocrypt 2018)*, Springer, pp. 282–303, 2018.

[8] S. Mesnager, Z. Zhou and C. Ding. On the nonlinearity of Boolean functions with restricted input. *Cryptography and Communications* (2018), 1–14.

[9] G. Pólya and G. Szegö. *Problems and Theorems in Analysis*. Classics in Mathematics Series, vol. I, Springer–Verlag, New York, 1976; original version *Aufgaben und Lehrsätze aus der Analysis* (Springer, 1925).



**Subhamoy Maitra** received his Bachelor of Electronics and Telecommunication Engineering degree in the year 1992 from Jadavpur University, Kolkata and Master of Technology in Computer Science in the year 1996 from Indian Statistical Institute, Kolkata. He has completed Ph.D. from Indian Statistical Institute in 2001. Currently he is a Professor at Indian Statistical Institute. His research interests are in Cryptology and Quantum Information.

**Bimal Mandal** received the Master of Science degree in Mathematics from Jadavpur University, India and the Ph.D. degree in Mathematics form Indian Institute of Technology Roorkee, India, in 2012 and 2018, respectively. From August, 2017 to October, 2018, he has been working as a visiting scientist at the Indian Statistical Institute, Kolkata, India. Currently, he is working as a post-doctoral fellow at the CARAMBA team, INRIA, France from November 2018. His research interests include cryptographic Boolean functions and cryptanalysis of block and stream ciphers.

**Thor Martinsen** (SM'13) received M.S. degrees in applied mathematics and computer science from the Naval Postgraduate School in Monterey, California in 2007. He subsequently earned his Ph.D. in applied mathematics from the Naval Postgraduate School in 2017. He is a Commander in the United States Navy and serves as Permanent Military Professor of applied mathematics and cyber security at the Naval Postgraduate School. Here he teaches and conducts research in mathematics, cryptology, cyber security, and electronic warfare.

**Dibyendu Roy** received his Master of Science in Mathematics degree in 2011 from Indian Institute of Technology Kharagpur, Kharagpur, India. He completed Ph.D. in Cryptology from Indian Institute of Technology Kharagpur, Kharagpur, India in 2016. Currently, he is a consultant at ERTL(E), STQC, Kolkata, India. His research interest is in Cryptology.

**Pantelimon Stănică** received his Master of Science in Mathematics degree in 1992 from University of Bucharest, Romania. He completed his Ph.D. in Mathematics at State University of New York at Buffalo in 1998. Currently, he is a Professor at the Naval Postgraduate School, in Monterey, California. His research interests are in Cryptology, Number Theory and Discrete Mathematics.