Parity-Check Relations on Combination Generators

Anne Canteaut and María Naya-Plasencia

***Abstract*—A divide-and-conquer cryptanalysis can often be mounted against some keystream generators composed of several (possibly nonlinear) independent devices combined by a Boolean function. In particular, any parity-check relation derived from the periods of some constituent sequences usually leads to a distinguishing attack whose complexity is determined by the bias of the relation. However, estimating this bias is a difficult problem since the piling-up lemma cannot be used. Here, we give two exact expressions for this bias. Most notably, these expressions lead to a new algorithm for computing the bias of a parity-check relation, and they also provide some simple formulas for this bias in some particular cases which are commonly used in cryptography, namely resilient functions and plateaued functions. We also show how to build parity-check relations with the highest possible bias in some particularly relevant cases.**

***Index Terms*—Boolean functions, parity-check relations, stream ciphers.**

I. Introduction

PARITY-CHECK relations are extensively used in cryptanalysis for building statistical distinguishers. For instance, they can be exploited in divide-and-conquer attacks against some stream ciphers which consist of several independent devices whose output sequences are combined by a nonlinear function. Here, we focus on such keystream generators as depicted on Fig. 1. All the n constituent devices are updated independently from each other. The only assumption which will be used in the whole paper is that each sequence $\boldsymbol{x}_i = (x_i(t))_{t \geq 0}$ generated by the ith device is periodic with least period T_i.

The simplest case of a generator built according to the model depicted in Fig. 1 is the combination generator, where all devices are LFSRs. However, our work is of greater interest in the case where the next-state functions of the constituent devices are nonlinear. The eSTREAM candidate Achterbahn and its variants [3], [2], [4], [6], [5], designed by Gammel, Göttfert, and Kniffler, follow this design principle: all these ciphers are actually composed of several nonlinear feedback shift registers (NLFSRs) with maximal periods. This design is very attractive since the use of independent devices allows to accommodate a large internal state with a small hardware footprint.

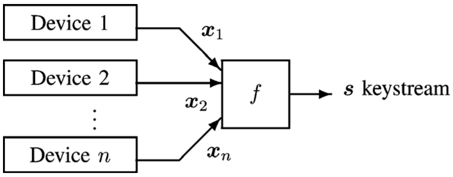

Fig. 1. Keystream generator composed of several independent devices combined by a Boolean function.

However, if the combining function f can be approximated by a function g depending on fewer variables (e.g., on the first m variables), the keystream $\boldsymbol{s} = f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ is correlated to a second sequence $\boldsymbol{\sigma} = g(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m)$ depending on the first m devices only. Exploiting such a correlation obviously requires the computation of the second sequence $\boldsymbol{\sigma}$. In the original attack proposed by Siegenthaler [16], a set including $\boldsymbol{\sigma}$ is computed by evaluating the sequences obtained for all possible initial states for the first m devices. Then, a distinguishing attack on the keystream can be performed if the attacker is able to detect the correlation between $\boldsymbol{\sigma}$ and the keystream, which corresponds to the correlation between f and g. The data complexity and the time complexity of the attack are then completely determined by the bias of the approximation of f by g, i.e., by the bias of $(f \oplus g)$.

But, an exhaustive search for the initial states of the first m devices is intractable as soon as the combining function f is well chosen. The use of parity-check relations proposed by Johansson, Meier, and Muller [11] then aims at eliminating the influences of some of these k devices in order to make the exhaustive search possible. For instance, if the approximation g is linear in the first k variables, the basic idea for eliminating the influences of the first k devices consists in summing the terms of $\boldsymbol{\sigma}$ at the 2^k instants defined by all possible combinations with $\{0,1\}$-coefficients of the periods of $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k$

$$\sigma'(t) = \bigoplus_{\tau \in \mathcal{T}} \sigma(t+\tau)$$

where $\mathcal{T} = \left\{ \sum_{i=1}^{k} c_i T_i, \quad c_i \in \{0,1\} \right\}$. Now, a set including this new sequence can be computed by an exhaustive search for the initial states of $(m-k)$ devices only. The attack then aims at detecting the correlation between the sequence obtained for the correct initial states, and the sequence $s'(t) = \sum_{\tau \in \mathcal{T}} s(t+\tau)$ derived from the keystream. Here, the correlation between both sequences plays a major role since it determines the complexity of the attack. It corresponds to the bias of

$$PC_{f \oplus g, \mathcal{T}}(t) = \bigoplus_{\tau \in \mathcal{T}} (f \oplus g)(x_1(t+\tau), \ldots, x_n(t+\tau)).$$

Several attacks exploiting parity-check relations [11], [9], [5] evaluate the bias of the parity-check relation with the so-called

Manuscript received December 17, 2010; revised September 28, 2011; accepted December 02, 2011. Date of publication January 18, 2012; date of current version May 15, 2012. This work was supported in part by the French Agence Nationale de la Recherche under Contract ANR-06-SETI-013-RAPIDE. This work was presented in part at the 2009 IEEE International Symposium on Information Theory.

A. Canteaut is with the INRIA Paris-Rocquencourt, Project-Team SECRET, 78153 Le Chesnay Cedex, France (e-mail: Anne.Canteaut@inria.fr).

M. Naya-Plasencia is with the FHNW Hochschule für Technik, CH-5210 Windisch, Switzerland (e-mail: maria.naya.plasencia@gmail.com).

Communicated by K. Martin, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2012.2184736

piling-up lemma [13]. They assume that the bias of $\boldsymbol{PC_{f\oplus g,\mathcal{T}}}$ corresponds to the bias of $(f\oplus g)$ raised to the power 2^k since $\mathcal{T}$ contains 2^k elements. But it clearly appears that this result does not apply since the terms $(f\oplus g)(x_1(t+\tau),\dots,x_n(t+\tau))$ for the different values of $\tau\in\mathcal{T}$ are not independent. Actually, Naya-Plasencia [14] and Hell and Johansson [10] have independently pointed out that the so-called *piling-up approximation* is far from being valid in some cases.

More surprisingly, since the first k constituent sequences do not influence $\boldsymbol{\sigma'}$, several approximations g of f may lead to the same sequence $\boldsymbol{\sigma'}$, and the piling-up lemma may give different values for the same bias. This situation occurred for instance in two attacks against Achterbahn-80 presented independently by Hell and Johansson [10] and Naya-Plasencia [14]. Both attacks exploit a correlation between the same pair of sequences $(\boldsymbol{s'},\boldsymbol{\sigma'})$ built from the same set $\mathcal{T}$. But, the first attack starts from a quadratic approximation g_1 of f with bias 2^{-5}, while the second one starts from an affine approximation g_2 of f with bias 2^{-3}. If the overall correlation between $\boldsymbol{s'}$ and $\boldsymbol{\sigma'}$ is evaluated with the piling-up lemma, it is concluded in the first case that the attack is infeasible since its data complexity exceeds the keystream length limitation. In the second case, the estimation of the bias concludes to a valid attack.

From this concrete example, it clearly appears that estimating the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$ may be a difficult problem. This issue has been raised in [14] and [7], which have identified some cases where the piling-up approximation holds. However, since these equality cases are quite rare, a much more extensive study is needed in order to evaluate the resistance of such keystream generators to distinguishing attacks. In this paper, we first emphasize that, even if most attacks based on parity-check relations use an explicit correspondence between the set $\mathcal{T}$ and an approximation g of f depending on k variables, the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$ does not depend directly on this approximation. Most notably, we show in Section II that the piling-up lemma applied to any approximation g compatible with $\mathcal{T}$ provides a lower bound on the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$. Then, Section IV gives two exact expressions for this bias, one involving the biases of some restrictions of f, and the other one by means of its Walsh coefficients. These expressions lead to an algorithm for computing the bias of a parity-check relation with a much lower complexity than the usual approach, and they also provide some simple formulas for this bias in some particular cases which are commonly used in cryptography: in Section V the case $k=t+1$ when f is t-resilient is treated and in Section VI the case where f is a plateaued function is considered. Most notably, in both cases, we show how the parity-check relations with the highest bias can be found.

II. Preliminaries on Parity-Check Relations

By analogy with coding theory, a *parity-check relation* for a binary sequence $\boldsymbol{x}=(x(t))_{t\geq 0}$ is a linear relation between some bits of $\boldsymbol{x}$ at different instants $(t+\tau)$ where τ varies in a fixed set and t takes any value

$$\bigoplus_{\tau\in\mathcal{T}} x(t+\tau)=0,\ \ \forall t\geq 0.$$

Then, the indexes τ corresponding to the nonzero coefficients of the characteristic polynomial of a linear recurring sequence provide a parity-check relation. A two-term parity-check relation

$$x(t)\oplus x(t+\tau)=0,\ \ \forall t\geq 0,$$

obviously corresponds to a period of the sequence.

The construction of parity-check relations mainly relies on the following simple lemma.

Lemma 1: Let $\boldsymbol{x}_1,\dots,\boldsymbol{x}_n$ be n sequences with periods $T_1,\dots,T_n$, and

$$\mathcal{T}=\Big\{\sum_{i=1}^{n} c_iT_i,\ \ c_i\in\{0,1\}\Big\}.$$

Then, the binary sequence $\boldsymbol{\sigma}$ defined by

$$\sigma(t)=\bigoplus_{i=1}^{n} x_i(t)$$

satisfies

$$\bigoplus_{\tau\in\mathcal{T}}\sigma(t+\tau)=0,\ \ \forall t\geq 0.$$

Proof: The influence of each sequence $\boldsymbol{x}_j$, $1\leq j\leq n$, in the sum vanishes. Indeed, the set $\mathcal{T}$ can be decomposed into two halves

$$\mathcal{T}_j=\Big\{\sum_{i\in\{1,\dots,n\}\setminus\{j\}} c_iT_i,\ \ c_i\in\{0,1\}\Big\}\text{ and }T_j+\mathcal{T}_j$$

such that $x_j(t+\tau)=x_j(t+\tau+T_j)$ for any t and any $\tau\in\mathcal{T}_j$. Therefore, for any j, $1\leq j\leq n$, we have

$$\bigoplus_{\tau\in\mathcal{T}} x_j(t+\tau)=\bigoplus_{\tau\in\mathcal{T}_j}(x_j(t+\tau)\oplus x_j(t+\tau+T_j))=0.$$

■

Such parity-check relations can then be generalized to the case of a sequence of the form $\sigma=f(\boldsymbol{x}_1,\dots,\boldsymbol{x}_n)$, where f is a nonlinear Boolean function.

Definition 2: Let $\boldsymbol{x}_1,\dots,\boldsymbol{x}_n$ be n sequences and let f be a Boolean function of n variables. Then, for any set

$$\mathcal{T}=\Big\{\sum_{i=1}^{s} c_iM_i,\ \ c_i\in\{0,1\}\Big\}$$

where $M_1,\dots,M_s$ are some non-negative integers, $\boldsymbol{PC_{f,\mathcal{T}}}$ is the binary sequence defined by

$$PC_{f,\mathcal{T}}(t)=\bigoplus_{\tau\in\mathcal{T}} f(x_1(t+\tau),\dots,x_n(t+\tau)),\ \forall t\geq 0.$$

In the whole paper, each M_i corresponds to a multiple of the least common multiple of the periods of some constituent sequences. Moreover, for the sake of simplicity, we will assume without loss of generality that the input variables are ordered in such a way that each integer M_i corresponds to a multiple of $\mathrm{lcm}(T_{\ell_i+1},\dots,T_{\ell_{i+1}})$ where T_i denotes the least period of $\boldsymbol{x}_i$, and $\ell_1,\dots,\ell_{s+1}$ is a strictly increasing sequence of integers with $\ell_1=0$ and $\ell_{s+1}=k$. This notably implies that $\mathcal{T}$ involves the periods of the first k sequences, $\boldsymbol{x}_1\dots,\boldsymbol{x}_k$.

Example: To illustrate our result, we will detail the following toy example in the whole paper. We consider $n=5$ sequences $\boldsymbol{x}_1,\dots,\boldsymbol{x}_5$ with least periods $T_1,\dots,T_5$, and the keystream sequence defined by $f(\boldsymbol{x}_1,\dots,\boldsymbol{x}_5)$ where f is the following balanced Boolean function of 5 variables

$$\begin{aligned}f(x_1,\dots,x_5) = {} & x_2+x_5+x_1x_4+x_3x_4+x_4x_5+x_1x_2x_3\\ & +x_1x_3x_4+x_1x_3x_5+x_2x_3x_5+x_3x_4x_5.\end{aligned}$$

Then, we want to determine the bias of the sequence defined by

$$PC_{f,\mathcal{T}}(t)=\bigoplus_{\tau\in\mathcal{T}} f(x_1(t+\tau),\dots,x_5(t+\tau))$$

where $\mathcal{T}=\{0,T_1T_2,T_3,T_1T_2+T_3\}$. The set $\mathcal{T}$ involves the period of $k=3$ sequences and has size $2^s=4$, i.e., $s=2$.

Proposition 3: Let $\boldsymbol{x}_1,\dots,\boldsymbol{x}_n$ be n sequences with least periods $T_1,\dots,T_n$ and

$$\mathcal{T}=\Big\{\sum_{i=1}^{s}c_iM_i,\ \ c_i\in\{0,1\}\Big\}$$

where $M_i=q_i\mathrm{lcm}(T_{\ell_i+1},\dots,T_{\ell_{i+1}})$ for some integer $q_i>0$ and $\ell_1=0$ and $\ell_{s+1}=k$. Let g be any Boolean function of k variables of the form

$$g(x_1,\dots,x_k)=\bigoplus_{i=1}^{s} g_i(x_{\ell_i+1},\dots,x_{\ell_{i+1}})$$

where each g_i is any Boolean function of $(\ell_{i+1}-\ell_i)$ variables. Then, for all $t\geq 0$, we have

$$PC_{g,\mathcal{T}}(t)=\bigoplus_{\tau\in\mathcal{T}} g(x_1(t+\tau),\dots,x_n(t+\tau))=0.$$

Proof: We first observe that, for any i, $1\leq i\leq s$, $M_i=q_i\mathrm{lcm}(T_{\ell_i+1},\dots,T_{\ell_{i+1}})$ is a period of all sequences $\boldsymbol{x}_{\ell_i+1},\dots,\boldsymbol{x}_{\ell_{i+1}}$, and therefore of any function g_i of $\boldsymbol{x}_{\ell_i+1},\dots,\boldsymbol{x}_{\ell_{i+1}}$. Then, the result directly follows from Lemma 1 applied to the sum of the s sequences $g_i(\boldsymbol{x}_{\ell_i+1},\dots,\boldsymbol{x}_{\ell_{i+1}})$ ■

In the whole paper, we use the following notation.

Definition 4: Let f be a Boolean function of n variables. Then, the *bias* of f is

$$\mathcal{E}(f)=2^{-n}\sum_{x\in\mathbf{F}_2^n}(-1)^{f(x)}.$$

This quantity is also called the imbalance of f (e.g., in [8] and [12]) or the correlation between f and the all-zero function (e.g., in [15]).

The underlying principle of the attack presented by Johansson, Meier, and Muller [11] consists in exhibiting a biased approximation g of the combining function f which involves k input variables, and a set of instants $\mathcal{T}$ such that the parity-check relation $\boldsymbol{PC_{g,\mathcal{T}}}$ vanishes. Then, the associated parity-check relation applied to $f(\boldsymbol{x}_1,\dots,\boldsymbol{x}_n)$ satisfies: for any $t\geq 0$

$$PC_{f,\mathcal{T}}(t)=PC_{f\oplus g,\mathcal{T}}(t)\oplus PC_{g,\mathcal{T}}(t)=PC_{f\oplus g,\mathcal{T}}(t).$$

It follows that the sequence $\boldsymbol{PC_{f,\mathcal{T}}}$ does not vanish but it may be biased in the sense that it is not uniformly distributed when the $T_1+\cdots+T_n$ bits $x_1(0),\dots,x_1(T_1-1),x_2(0),\dots,x_2(T_2-1),\dots,x_n(0),\dots x_n(T_n-1)$, corresponding to the concatenation of the periods of the constituent sequences, are randomly chosen. The bias of $\boldsymbol{PC_{f,\mathcal{T}}}$, denoted by $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$ is then defined as the bias of a Boolean function with $T_1+\cdots+T_n$ input variables. But, it is worth noticing that some of these $T_1+\cdots+T_n$ input variables are not involved in the algebraic normal form of the function. More precisely, when $\mathcal{T}$ contains 2^s elements, this Boolean function contains 2^s variables corresponding to each of the last $(n-k)$ sequences, and 2^{s-1} variables corresponding to each of the first k sequences. Moreover, all these variables are distinct when each M_i is coprime with all T_j with $j\notin[\ell_i+1;\ell_{i+1}]$. Therefore, the Boolean function depends on

$$k\times 2^{s-1}+(n-k)\times 2^s=(2n-k)2^{s-1}\text{ variables.}$$

Example: Let us consider $\mathcal{T}=\{0,T_1T_2,T_3,T_1T_2+T_3\}$ and

$$\begin{aligned}f(x_1,\dots,x_5) = {} & x_2+x_5+x_1x_4+x_3x_4+x_4x_5+x_1x_2x_3\\ & +x_1x_3x_4+x_1x_3x_5+x_2x_3x_5+x_3x_4x_5.\end{aligned}$$

Proposition 3 implies that the sequences $\boldsymbol{PC_{f\oplus g,\mathcal{T}}}$ are equal to $\boldsymbol{PC_{f,\mathcal{T}}}$ for all $g(x_1,x_2,x_3)=a_0x_1x_2+a_1x_1+a_2x_2+a_3x_3$ with $a_i\in\mathbf{F}_2$. It then appears that the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$ cannot be directly deduced from the bias of the chosen approximation, $\mathcal{E}(f\oplus g)$. Indeed, all possible approximations g do not have the same bias: we have $\mathcal{E}(f\oplus x_1)=0$, $\mathcal{E}(f\oplus x_1+x_2)=2^{-2}$ and $\mathcal{E}(f\oplus x_1x_2)=-2^{-3}$.

The bias of $\boldsymbol{PC_{f,\mathcal{T}}}$ corresponds to the bias of the following Boolean function:

$$\begin{aligned}pc(\xi_{1,0},\dots,\xi_{5,3}) = {} & f(\xi_{1,0},\xi_{2,0},\xi_{3,0},\xi_{4,0},\xi_{5,0})\\ & \oplus f(\xi_{1,0},\xi_{2,0},\xi_{3,1},\xi_{4,1},\xi_{5,1})\\ & \oplus f(\xi_{1,1},\xi_{2,1},\xi_{3,0},\xi_{4,2},\xi_{5,2})\\ & \oplus f(\xi_{1,1},\xi_{2,1},\xi_{3,1},\xi_{4,3},\xi_{5,3}).\end{aligned}$$

Therefore, pc is a Boolean function involving $(2\times 5-3)2^{2-1}=(2n-k)2^{s-1}=14$ variables.

It follows from the previous discussion that, for an appropriate choice of $\mathcal{T}$, we have

$$\Pr[PC_{f,\mathcal{T}}(t)=0]=\frac{1}{2}(1+\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}))$$

with $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \mathcal{E}(\boldsymbol{PC_{f\oplus g,\mathcal{T}}}) \neq 0$. Actually, we will show in Section III that $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$ is always strictly positive when there exists some biased approximation g of f of the form $g(x_1, \dots, x_k) = \bigoplus_{i=1}^{s} g_i(x_{\ell_i+1}, \dots, x_{\ell_{i+1}})$. Then, computing

$$PC_{f,\mathcal{T}}(t) = \bigoplus_{\tau\in\mathcal{T}} s(t+\tau)$$

where $s(t) = f(x_1(t), \dots, x_n(t))$ is the keystream for different values of $t \geq 0$ enables the attacker to distinguish the keystream from a random sequence. The complexity of this distinguishing attack depends on the bias ε of $\boldsymbol{PC_{f,\mathcal{T}}}$. More precisely, the time complexity of the attack corresponds to $\varepsilon^{-2}2^s$ where 2^s is the number of elements in $\mathcal{T}$ since the bias ε can be detected from at least ε^{-2} occurrences of the biased relation. The data complexity, i.e., the number of consecutive keystream bits required for the attack is then the maximal value which must be considered for $(t+\tau)$, i.e.

$$\varepsilon^{-2} + \max \mathcal{T}.$$

III. A Lower Bound on the Bias of Parity-Check Relations

As previously explained, the piling-up lemma does not apply for estimating the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$. Otherwise, this bias would be derived from the biases of several approximations g of f. Indeed, it follows from Proposition 3 that, for a given set $\mathcal{T}$ and for any function g of the form

$$g(x_1, \dots, x_k) = \bigoplus_{i=1}^{s} g_i(x_{\ell_i+1}, \dots, x_{\ell_{i+1}})$$

we have

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \mathcal{E}(\boldsymbol{PC_{f\oplus g,\mathcal{T}}}).$$

However, we can prove that the piling-up approximation $[\mathcal{E}(f\oplus g)]^{2^s}$ provides a lower bound on the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$ for any such approximation g.

Theorem 5: Let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ be n sequences with least periods $T_1, \dots, T_n$, f a Boolean function of n variables and $\boldsymbol{s} = f(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$. Let

$$\mathcal{T} = \{\sum_{i=1}^{s} c_i M_i, \quad c_i \in \{0,1\}\}$$

where $M_i = q_i \mathrm{lcm}(T_{\ell_i+1}, \dots, T_{\ell_{i+1}})$ for some integer $q_i > 0$, $\ell_1 = 0$ and $\ell_{s+1} = k$. Assume that each M_i is coprime with all T_j with $j \notin [\ell_i + 1; \ell_{i+1}]$. Then, for any Boolean function g of k variables of the form

$$g(x_1, \dots, x_k) = \bigoplus_{i=1}^{s} g_i(x_{\ell_i+1}, \dots, x_{\ell_{i+1}}) \qquad (1)$$

where each g_i is a Boolean function of $(\ell_{i+1} - \ell_i)$ variables, we have

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) \geq [\mathcal{E}(f\oplus g)]^{2^s}.$$

Proof: First, we use the fact that, for any function g defined by (1)

$$PC_{f,\mathcal{T}}(t) = PC_{f\oplus g,\mathcal{T}}(t) \oplus PC_{g,\mathcal{T}}(t) = PC_{f\oplus g,\mathcal{T}}(t), \ \forall t \geq 0.$$

In the following, we extensively exploit the following result due to Nyberg, derived from [15, Cor. 6]. For any Boolean function h of n variables, we consider a decomposition of the input variables into two parts of respective sizes n_1 and n_2. For $v \in \mathbf{F}_2^{n_1}$, we denote by $\varphi_{(v,0)}$ the linear function of n variables defined by $\varphi_{(v,0)}(x,y) = v \cdot x$ and by pc_h the following Boolean function

$$\begin{array}{rccl} pc_h: & \mathbf{F}_2^{n_1} \times \mathbf{F}_2^{n_2} \times \mathbf{F}_2^{n_2} & \rightarrow & \mathbf{F}_2 \\ & (x,y,z) & \mapsto & h(x,y) \oplus h(x,z). \end{array}$$

Then, we compute

$$\begin{aligned} E &= \sum_{v\in\mathbf{F}_2^{n_1}} \left[2^n \mathcal{E}(h + \varphi_{(v,0)})\right]^2 \\ &= \sum_{v\in\mathbf{F}_2^{n_1}} \sum_{x\in\mathbf{F}_2^{n_1}, y\in\mathbf{F}_2^{n_2}} (-1)^{h(x,y)+v\cdot x} \sum_{x'\in\mathbf{F}_2^{n_1}, z\in\mathbf{F}_2^{n_2}} (-1)^{h(x',z)+v\cdot x'} \\ &= \sum_{x,x'\in\mathbf{F}_2^{n_1}} \sum_{y,z\in\mathbf{F}_2^{n_2}} (-1)^{h(x,y)+h(x',z)} \sum_{v\in\mathbf{F}_2^{n_1}} (-1)^{v\cdot(x+x')} \\ &= 2^{n_1} \sum_{x\in\mathbf{F}_2^{n_1}} \sum_{y,z\in\mathbf{F}_2^{n_2}} (-1)^{h(x,y)+h(x,z)} \\ &= 2^{2n} \mathcal{E}(pc_h). \end{aligned}$$

Therefore

$$\mathcal{E}(pc_h) = \sum_{v\in\mathbf{F}_2^{n_1}} \mathcal{E}(h + \varphi_{(v,0)})^2 \geq \mathcal{E}(h)^2. \qquad (2)$$

Now, we prove by induction on s that

$$\mathcal{E}(\boldsymbol{PC_{f\oplus g,\mathcal{T}}}) \geq [\mathcal{E}(f\oplus g)]^{2^s}.$$

- For $s = 1$, the result is a direct corollary of (2):

$$\mathcal{E}(PC_{f\oplus g,\mathcal{T}}) \geq [\mathcal{E}(f\oplus g)]^2.$$

- Induction step: Let us now consider

$$\mathcal{T}_s = \{\sum_{i=1}^{s-1} c_i M_i, \quad c_i \in \{0,1\}\}$$

and

$$g'(x_1, \dots, x_k) = \sum_{i=1}^{s-1} g_i(x_{\ell_i+1}, \dots, x_{\ell_{i+1}}).$$

Then,

$$\begin{aligned} PC_{f\oplus g,\mathcal{T}}(t) &= PC_{f\oplus g,\mathcal{T}_s}(t) \oplus PC_{f\oplus g,\mathcal{T}_s}(t+M_s) \\ &= PC_{(f\oplus g_s)\oplus g',\mathcal{T}_s}(t) \\ &\quad \oplus PC_{(f\oplus g_s)\oplus g',\mathcal{T}_s}(t+M_s). \end{aligned}$$

Therefore, (2) implies that

$$\begin{aligned} \mathcal{E}(\boldsymbol{PC_{f\oplus g,\mathcal{T}}}) &\geq \left[\mathcal{E}(PC_{(f\oplus g_s)\oplus g',\mathcal{T}_s})\right]^2 \\ &\geq \left[\mathcal{E}((f\oplus g_s)\oplus g')^{2^{s-1}}\right]^2 \geq \left[\mathcal{E}(f\oplus g)\right]^{2^s}. \end{aligned}$$

■

Example: The previous theorem provides a first explanation of the situation detailed in the example on Page 3: the bias of any approximation of the form $g(x_1,x_2,x_3) = a_0x_1x_2 + a_1x_1 + a_2x_2 + a_3x_3$ leads to a lower bound on the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$. We can check that the best approximation g is $x_1 + x_2$ and satisfies $\mathcal{E}(f \oplus x_1 + x_2) = 2^{-2}$. Therefore, we deduce that $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) \geq (2^{-2})^4 = 2^{-8}$.

The keypoint in the previous theorem is that $\mathcal{E}(f \oplus g)$ provides a lower bound on the bias on the parity-check relation for any choice of the approximation g of (1). The linear approximation of f by the sum of the first k input variables is usually considered, but any linear approximation involving these variables can be chosen, as stated in the next corollary. In the following, for any $\alpha \in \mathbf{F}_2^n$, φ_α denotes the linear function of n variables: $x \mapsto \alpha \cdot x$.

Corollary 6: With the notation of Theorem 5, we have

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) \geq \max_{\alpha\in V_k} \left[\mathcal{E}(f\oplus\varphi_\alpha)\right]^{2^s}$$

where V_k is the subspace spanned by the first k basis vectors. It is worth noticing that this corollary leads to a positive lower bound on the bias of the parity check relation even if the functions f and $x \mapsto x_1 \oplus \cdots \oplus x_k$ are not correlated (i.e., if the Walsh coefficient of f at point 1_k vanishes, where the first k coordinates of 1_k are 1 and the other $(n-k)$ are zero). This is the first known result in such a situation; the impossibility of deducing any estimation of the bias of the relation in such cases has been stressed in [7, Example 1]. However, some other approximations g with a higher degree may lead to a better bound. But, since any Boolean function is completely determined by its Walsh transform, i.e., by the biases of all its linear approximations, it appears that $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$ can be computed from the biases of the linear approximations of f only.

IV. Exact Formulas for the Bias of the Parity-Check Relation

In some situations, especially when the designer of a generator has to guarantee that the system resists distinguishing attacks, the previous lower bound on the bias of a parity-check relation is not sufficient, and its exact value must be computed. However, since a parity-check relation with 2^s terms depending on k sequences involves $(2n-k)2^{s-1}$ variables where n is the number of variables of f, computing its bias requires $2^{(2n-k)2^{s-1}}$ evaluations of f, which is out of reach in many practical situations. For instance, Achterbahn-128 uses a combining function f of 13 variables, and the biases of parity-check relations with 8 terms (i.e., with $s = 3$) and $k = 10$ must be estimated; this requires 2^{64} operations. Here, we give two exact expressions of the bias of a parity-check relation, which can be computed with much fewer operations, e.g., with 2^{43} evaluations of f in the previous case. The first expression makes use of the biases of the restrictions of f when its first k inputs are fixed; the second one, which is related to a theorem due to Nyberg [15], is based on the Walsh coefficients of the combining function.

A. Expression by Means of the Restrictions of f

Definition 7: Let f be a Boolean function of n variables and let V_k and V_{n-k} be two subspaces such that $V_k \times V_{n-k} = \mathbf{F}_2^n$ and $\dim(V_k) = k$. Then, the restriction of f to the affine subspace $a + V_{n-k}$, $a \in V_k$, denoted by $f_{|a+V_{n-k}}$, is the Boolean function of $(n-k)$ variables defined by

$$f_{|a+V_{n-k}} : x \in V_{n-k} \mapsto f(x+a).$$

If there is no ambiguity on the choice of V_{n-k}, $f_{|a+V_{n-k}}$ will be denoted by $f_{|a}$.

We now assume that each M_i is coprime with all T_j with $j \notin [\ell_i + 1; \ell_{i+1}]$. For computing the exact value of $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$, we decompose $\boldsymbol{PC_{f,\mathcal{T}}}$ according to the values of the first k variables in f since the other $(n-k)$ sequences $\boldsymbol{x}_i$, $k+1 \leq i \leq n$, are supposed to be such that $x_i(t+\tau)$ is statistically independent from $x_i(t)$ for any $\tau \in \mathcal{T}$. Amongst the other $k2^s$ variables $x_i(t+\tau)$, $1 \leq i \leq k$ and $\tau \in \mathcal{T}$, we can easily see that each variable is repeated once. Indeed, for j such that $\ell_i < j \leq \ell_{i+1}$ we have $x_j(t+\tau) = x_j(t+\tau')$ for all t if and only if $(\tau - \tau') \equiv 0 \bmod M_i$. It follows that the values of $x_j(t+\tau)$, $1 \leq j \leq k$ and $\tau \in \mathcal{T}$ are determined by a $k \times 2^{s-1}$ binary matrix A in the following way. For each j, $1 \leq j \leq k$, we denote by $I(j)$ the integer in $\{1,\ldots,s\}$ such that $\ell_{I(j)} < j \leq \ell_{I(j)+1}$. The 2^{s-1} bits in the row A_j of A, $1 \leq j \leq k$, are then indexed by the elements $\tau \in \mathcal{T}_{I(j)}$ where

$$\mathcal{T}_{I(j)} = \Big\{ \sum_{i\in\{1,\ldots,s\}\setminus\{I(j)\}} c_iM_i,\ \ c_i \in \{0,1\} \Big\}.$$

It follows that the values of all $x_j(t+\tau)$ for $1 \leq j \leq k$ and $\tau \in \mathcal{T}$ can be arranged in a $k \times 2^s$ matrix $\chi(A)$ defined by

$$\chi(A)_{j,\tau} = \begin{cases} A_{j,\tau} & \text{if} \quad \tau \in \mathcal{T}_{I(j)} \\ A_{j,\tau - M_{I(j)}} & \text{if} \quad \tau \in M_{I(j)} + \mathcal{T}_{I(j)} \end{cases}. \tag{3}$$

Example: Let us consider a set $\mathcal{T}$ composed of 2^3 elements (i.e, $s = 3$) which involve the periods of $k = 4$ sequences

$$\mathcal{T} = \left\{ c_1T_1T_2 + c_2T_3 + c_3T_4,\ c_1, c_2, c_3 \in \{0,1\} \right\}.$$

Then, the elements of the 4×4 matrix A are numbered as follows:

$$\begin{pmatrix} A_{1,0} & A_{1,T_3} & A_{1,T_4} & A_{1,T_3+T_4} \\ A_{2,0} & A_{2,T_3} & A_{2,T_4} & A_{2,T_3+T_4} \\ A_{3,0} & A_{3,T_1T_2} & A_{3,T_4} & A_{3,T_1T_2+T_4} \\ A_{4,0} & A_{4,T_1T_2} & A_{4,T_3} & A_{4,T_1T_2+T_3} \end{pmatrix}$$

Each of the four rows of the matrix $\chi(A)$ corresponds to the eight values $x_j(t+\tau)$, $\tau \in \mathcal{T}$, deduced from A as described by (4) at the bottom of the page.

The definition of $\chi(A)$ enables us to express the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$ by means of the biases of the restrictions of f to all cosets of the subspace V_{n-k} spanned by the last $(n-k)$ basis vectors.

Theorem 8: Let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ be n sequences with least periods $T_1, \dots, T_n$, f a Boolean function of n variables and $\boldsymbol{s} = f(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$. Let

$$\mathcal{T} = \{\sum_{i=1}^{s} c_i M_i, \;\; c_i \in \{0,1\}\}$$

where $M_i = q_i \mathrm{lcm}(T_{\ell_i+1}, \dots, T_{\ell_{i+1}})$ for some integer $q_i > 0$, $\ell_1 = 0$ and $\ell_{s+1} = k$. Assume that each M_i is coprime with all T_j with $j \notin [\ell_i + 1; \ell_{i+1}]$. Then, we have

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \frac{1}{2^{k2^{s-1}}} \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \prod_{\tau \in \mathcal{T}} \mathcal{E}(f_{|\chi^\tau(A)})$$

where $f_{|\chi^\tau(A)}$ is the restriction of f when its first k inputs are fixed and equal to the column of index τ of matrix $\chi(A)$.

Proof: Since the variables $x_j(\tau)$ for $k < j \leq n$ and $\tau \in \mathcal{T}$ are all independent and also independent from the variables $x_j(\tau)$ for $1 \leq j \leq k$, we can compute

$$I = 2^{k2^{s-1}+(n-k)2^s} \mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$$

as follows:

$$\begin{aligned}
I &= \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \sum_{B \in \mathbf{F}_2^{(n-k) \times 2^s}} (-1)^{\bigoplus_{\tau \in \mathcal{T}} f(\chi(A)_{1,\tau}, \dots, \chi(A)_{k,\tau}, B_{1,\tau}, \dots, B_{n-k,\tau})} \\
&= \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \sum_{B \in \mathbf{F}_2^{(n-k) \times 2^s}} \prod_{\tau \in \mathcal{T}} (-1)^{f(\chi(A)_{1,\tau}, \dots, \chi(A)_{k,\tau}, B_{1,\tau}, \dots, B_{n-k,\tau})} \\
&= 2^{(n-k)2^s} \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \prod_{\tau \in \mathcal{T}} \left[2^{-(n-k)} \sum_{B \in \mathbf{F}_2^{(n-k) \times 2^s}} (-1)^{f(\chi(A)_{1,\tau}, \dots, B_{n-k,\tau})} \right] \\
&= 2^{(n-k)2^s} \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \prod_{\tau \in \mathcal{T}} \mathcal{E}(f_{|\chi^\tau(A)}).
\end{aligned}$$

■

This result leads to Algorithm 1 for computing the exact value of $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$.

Algorithm 1 Computing the exact value of the bias of $\boldsymbol{PC_{f,\mathcal{T}}}$

```
Require: $f$, an $n$-variable Boolean function and
    $\mathcal{T} = \{\sum_{i=1}^{s} c_i M_i, \;\; c_i \in \{0,1\}\}$
where $M_i = q_i \mathrm{lcm}(T_{\ell_i+1}, \dots, T_{\ell_{i+1}})$ for some integer $q_i > 0$, $\ell_1 = 0$, and $\ell_{s+1} = k$.
/* Precomputation*/
for all $a \in V_k$ do
    $E_a \leftarrow \mathcal{E}(f_{|a}) = \frac{1}{2^{n-k}} \sum_{y \in V_{n-k}} (-1)^{f(a+y)}$
end for
/* Computation of the bias*/
$\mathcal{E} \leftarrow 0$
for all $A \in \mathbf{F}_2^{k \times 2^{s-1}}$ do
    $\mathcal{A} \leftarrow 1$
    for all $c$ from 0 to $2^s - 1$ do
        $\tau \leftarrow \sum_{i=0}^{s} c_i M_{i+1}$
        $\mathcal{A} \leftarrow \mathcal{A} \times E_{\chi^\tau(A)}$
    end for
    $\mathcal{E} \leftarrow \mathcal{E} + \mathcal{A}$
end for
return $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \frac{1}{2^{k2^{s-1}}} \mathcal{E}$.
```

Example: Let us first compute the biases of all restrictions of $f(x_1, \dots, x_5) = x_2 + x_5 + x_1x_4 + x_3x_4 + x_4x_5 + x_1x_2x_3 + x_1x_3x_4 + x_1x_3x_5 + x_2x_3x_5 + x_3x_4x_5$ when the first three variables are fixed and equal to $a_1a_2a_3$: for $a_3 = 1$, we have that $\mathcal{E}(f_{|a}) = 0$ and, for $a_3 = 0$, we have

$$\mathcal{E}(f_{|000}) = \mathcal{E}(f_{|110}) = \frac{1}{2} \text{ and } \mathcal{E}(f_{|100}) = \mathcal{E}(f_{|010}) = -\frac{1}{2}.$$

Now, we compute $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$ for $\mathcal{T} = \{0, T_1T_2, T_3, T_1T_2 + T_3\}$ with Theorem 8:

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \frac{1}{2^6} \sum_{A \in \mathbf{F}_2^{3 \times 2}} \prod_{\tau \in \mathcal{T}} \mathcal{E}(f_{|\chi^\tau(A)}).$$

$$\begin{array}{llcccccccccl}
\mathcal{T} & = \{ & 0 & T_1T_2 & T_3 & T_1T_2 + T_3 & T_4 & T_1T_2 + T_4 & T_3 + T_4 & T_1T_2 + T_3 + T_4 & \} \\
\chi_1(A) & = (& A_{1,0} & A_{1,0} & A_{1,T_3} & A_{1,T_3} & A_{1,T_4} & A_{1,T_4} & A_{1,T_3+T_4} & A_{1,T_3+T_4} &) \\
\chi_2(A) & = (& A_{2,0} & A_{2,0} & A_{2,T_3} & A_{2,T_3} & A_{2,T_4} & A_{2,T_4} & A_{2,T_3+T_4} & A_{2,T_3+T_4} &) \\
\chi_3(A) & = (& A_{3,0} & A_{3,T_1T_2} & A_{3,0} & A_{3,T_1T_2} & A_{3,T_4} & A_{3,T_1T_2+T_4} & A_{3,T_4} & A_{3,T_1T_2+T_4} &) \\
\chi_4(A) & = (& A_{4,0} & A_{4,T_1T_2} & A_{4,T_3} & A_{4,T_1T_2+T_3} & A_{4,0} & A_{4,T_1T_2} & A_{4,T_3} & A_{4,T_1T_2+T_3} &)
\end{array} \quad (4)$$

The elements of the 3 × 2 matrix A are numbered as follows

$$\begin{pmatrix} A_{1,0} & A_{1,T_3} \\ A_{2,0} & A_{2,T_3} \\ A_{3,0} & A_{3,T_1T_2} \end{pmatrix}$$

and Matrix $\chi(A)$ is defined from A by

$$\begin{pmatrix} A_{1,0} & A_{1,0} & A_{1,T_3} & A_{1,T_3} \\ A_{2,0} & A_{2,0} & A_{2,T_3} & A_{2,T_3} \\ A_{3,0} & A_{3,T_1T_2} & A_{3,0} & A_{3,T_1T_2} \end{pmatrix}$$

Since $\mathcal{E}(f_{|a}) = 0$ when $a_3 = 1$, the product

$$\prod_{\tau \in \mathcal{T}} \mathcal{E}(f_{|\chi^\tau(A)})$$

is equal to zero except if the last row of A is zero. And it can be checked that, for the 16 possible matrices A which may lead to a nonzero product, we have

$$\prod_{\tau \in \mathcal{T}} \mathcal{E}(f_{|\chi^\tau(A)}) = (2^{-1})^4.$$

Therefore, we deduce that

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \frac{1}{2^6}\left(16 \times 2^{-4}\right) = 2^{-6}.$$

The precomputation step in Algorithm 1 consists in computing and storing in a table the 2^k values of

$$\mathcal{E}(f_{|a}) = \frac{1}{2^{n-k}} \sum_{y \in V_{n-k}} (-1)^{f(a+y)}, \ \forall\, a \in V_k$$

where V_k (respectively, V_{n-k}) denotes the linear subspace spanned by the first k basis vector (respectively, by the last $(n-k)$ basis vector). This step requires 2^n evaluations of f. Then, for computing the bias of the parity-check relation, we need to compute, for all $A \in \mathbf{F}_2^{k \times 2^{s-1}}$, the product of 2^s precomputed values whose indexes are determined by the columns of $\chi(A)$. This requires $2^{k2^{s-1}} \times 2^s$ operations over integers. This leads to an overall complexity of $2^{k2^{s-1}+s} + 2^n$ which is much lower than the complexity of the trivial computation, $2^{(2n-k)2^{s-1}}$ evaluations of f. For instance, the 13-variable function in Achterbahn-128 is 8-resilient. Estimating the bias of a parity-check relation involving 10 input variables with 8 terms (i.e., with $s = 3$) then requires 2^{43} operations.

B. *Expression by Means of the Walsh Coefficients of f*

A similar exact expression for the bias of $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$ can be obtained from the Walsh coefficients of f, i.e., from all biases $\mathcal{E}(f + \varphi_a)$, $a \in V_k$ where V_k is the subspace spanned by the first k basis vectors. As previously, for any $a \in \mathbf{F}_2^n$, φ_a denotes the n-variable linear function defined by $\varphi_a(x) = a \cdot x$.

Theorem 9: Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ be n sequences with least periods $T_1, \ldots, T_n$, f a Boolean function of n variables and $\boldsymbol{s} = f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$. Let

$$\mathcal{T} = \{\sum_{i=1}^{s} c_i M_i, \ \ c_i \in \{0,1\}\}$$

where $M_i = q_i \mathrm{lcm}(T_{\ell_i+1}, \ldots, T_{\ell_{i+1}})$ for some integer $q_i > 0$, $\ell_1 = 0$ and $\ell_{s+1} = k$. Assume that each M_i is coprime with all T_j with $j \notin [\ell_i + 1; \ell_{i+1}]$. Then, we have

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \prod_{\tau \in \mathcal{T}} \mathcal{E}(f + \varphi_{(\chi^\tau(A),0)}).$$

Proof: As previously, we denote by M^τ the column of index τ of any matrix M. Let us compute

$$\begin{aligned} I = & \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \prod_{\tau \in \mathcal{T}} \mathcal{E}(f + \varphi_{(\chi^\tau(A),0)}) \\ = & \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \prod_{\tau \in \mathcal{T}} 2^{-n} \sum_{X^\tau \in \mathbf{F}_2^k} \sum_{Y^\tau \in \mathbf{F}_2^{n-k}} (-1)^{f(X^\tau, Y^\tau) + \chi^\tau(A) \cdot X^\tau} \\ = & 2^{-n2^s} \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} \sum_{X \in \mathbf{F}_2^{k \times 2^s}} \sum_{Y \in \mathbf{F}_2^{(n-k) \times 2^s}} (-1)^{\bigoplus_{\tau \in \mathcal{T}} f(X^\tau, Y^\tau) + \chi^\tau(A) \cdot X^\tau} \\ = & 2^{-n2^s} \sum_{Y \in \mathbf{F}_2^{(n-k) \times 2^s}} \sum_{X \in \mathbf{F}_2^{k \times 2^s}} (-1)^{\bigoplus_{\tau \in \mathcal{T}} f(X^\tau, Y^\tau)} \\ & \times \left[\sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} (-1)^{\bigoplus_{\tau \in \mathcal{T}} \chi^\tau(A) \cdot X^\tau} \right]. \end{aligned}$$

Now, from the definition of $\chi(A)$ [see (3)], we can write

$$\begin{aligned} \bigoplus_{\tau \in \mathcal{T}} \chi^\tau(A) \cdot X^\tau &= \bigoplus_{j=1}^{k} \bigoplus_{\tau \in \mathcal{T}} \chi(A)_{j,\tau} \cdot X_{j,\tau} \\ &= \bigoplus_{j=1}^{k} \bigoplus_{\tau \in \mathcal{T}_{I(j)}} \chi(A)_{j,\tau} \cdot \left(X_{j,\tau} + X_{j,\tau+M_{I(j)}}\right) \end{aligned}$$

where

$$\mathcal{T}_{I(j)} = \Big\{ \sum_{i \in \{1,\ldots,s\} \setminus \{I(j)\}} c_i M_i, \ \ c_i \in \{0,1\} \Big\}.$$

Since the set $\{\chi(A)_{j,\tau}, \ \tau \in \mathcal{T}_{I(j)}\}$ depends on the row A_j only, it follows that

$$\begin{aligned} & \sum_{A \in \mathbf{F}_2^{k \times 2^{s-1}}} (-1)^{\bigoplus_{\tau \in \mathcal{T}} \chi^\tau(A) \cdot X^\tau} = \\ & \prod_{j=1}^{k} \sum_{A_j \in \mathbf{F}_2^{2^{s-1}}} (-1)^{\bigoplus_{\tau \in \mathcal{T}_{I(j)}} \chi(A)_{j,\tau} \cdot \left(X_{j,\tau} + X_{j,\tau+M_{I(j)}}\right)}. \end{aligned}$$

Then, we deduce

$$\sum_{A\in\mathbf{F}_2^{k\times 2^{s-1}}} (-1)^{\bigoplus_{\tau\in\mathcal{T}} \chi^\tau(A)\cdot X^\tau} = \begin{cases} (2^{2^{s-1}})^k, & \text{if } X_{j,\tau} = X_{j,\tau+M_{I(j)}} \text{ for all } 1\le j\le k \\ & \quad \text{and } \tau\in\mathcal{T}_{I(j)} \\ 0, & \text{otherwise.}\end{cases}$$

Therefore, the matrices $X \in \mathbf{F}_2^{k\times 2^s}$ for which the previous sum does not vanish are exactly those which can be written as $X = \chi(M)$ for some $M\in\mathbf{F}_2^{k\times 2^{s-1}}$. We deduce from (5) that

$$\begin{aligned}&\sum_{A\in\mathbf{F}_2^{k\times 2^{s-1}}}\prod_{\tau\in\mathcal{T}}\mathcal{E}(f+\varphi_{(\chi^\tau(A),0)})\\ &= 2^{-n2^s}\sum_{Y\in\mathbf{F}_2^{(n-k)\times 2^s}}\ \sum_{M\in\mathbf{F}_2^{k\times 2^{s-1}}} 2^{k2^{s-1}}(-1)^{\bigoplus_{\tau\in\mathcal{T}} f(\chi^\tau(M),Y^\tau)}\\ &= \mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}).\end{aligned}$$

■

This expression leads to an algorithm for computing the bias which is very similar to the one based on the biases of the restrictions of f. But, we need to precompute and to store the Walsh coefficients of f corresponding to all elements in V_k.

Example: The Walsh coefficients of $f(x_1,\dots,x_5) = x_2 + x_5 + x_1x_4 + x_3x_4 + x_4x_5 + x_1x_2x_3 + x_1x_3x_4 + x_1x_3x_5 + x_2x_3x_5 + x_3x_4x_5$ involving the first three variables all vanish except

$$\mathcal{E}(f+x_1+x_2) = \mathcal{E}(f+x_1+x_2+x_3) = +2^{-2}.$$

We compute $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$ for $\mathcal{T} = \{0, T_1T_2, T_3, T_1T_2+T_3\}$ with Theorem 9

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \sum_{A\in\mathbf{F}_2^{3\times 2}}\prod_{\tau\in\mathcal{T}}\mathcal{E}(f+\varphi_{(\chi^\tau(A),0)}).$$

Matrix $\chi(A)$ is defined from the 3×2 matrix A by

$$\begin{pmatrix} A_{1,0} & A_{1,0} & A_{1,T_3} & A_{1,T_3}\\ A_{2,0} & A_{2,0} & A_{2,T_3} & A_{2,T_3}\\ A_{3,0} & A_{3,T_1T_2} & A_{3,0} & A_{3,T_1T_2}\end{pmatrix}. \qquad (5)$$

Then, we have to determine all A such that all columns of $\chi(A)$ are such that $\varphi_{(\chi^\tau(A),0)}$ is a biased approximation of f. This condition equivalently means that all coefficients in the first two rows of A must be equal to 1. Since the last row of A can take any value, we deduce that there are exactly four matrices A such that

$$\prod_{\tau\in\mathcal{T}}\mathcal{E}(f+\varphi_{(\chi^\tau(A),0)})\neq 0.$$

Moreover, since the biases of all involved approximations are equal (i.e., have same sign and magnitude), the previous product is always equal to $(2^{-2})^4 = 2^{-8}$. We eventually deduce that

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = 4\times 2^{-8} = +2^{-6}.$$

C. Combining Both Methods

By using the equivalence of previous results, we obtain the following equality.

Proposition 10: With the notation of Theorem 8, we have

$$\begin{aligned}2^{k\cdot 2^{s-1}}&\sum_{A\in\mathbf{F}_2^{k\times 2^{s-1}}}\prod_{\tau\in\mathcal{T}}\mathcal{E}(f\oplus\varphi_{(\chi^\tau(A),0)})\\ &= \sum_{A\in\mathbf{F}_2^{k\times 2^{s-1}}}\prod_{\tau\in\mathcal{T}}\mathcal{E}(f_{|\chi^\tau(A)})\end{aligned}$$

We can now combine both techniques for computing the bias of a parity-check relation. If we build a parity-check relation with k variables, we can divide k in k_1 and k_2, where k_1 represents the variables which will be fixed by considering the restrictions of f and k_2 the variables involved in the linear approximations. In this case, by using the vectors $\chi(A)$ and considering the first k_1 associated vectors to the k_1 fixed variables, and the last k_2 vectors associated to the variables used for the approximations, we find the following.

Proposition 11:

$$\begin{aligned}&\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})\\ &\quad= \frac{1}{2^{k_1\cdot 2^{s-1}}}\sum_{A\in\mathbf{F}_2^{k\times 2^{s-1}}}\prod_{\tau\in\mathcal{T}}\mathcal{E}\left((f\oplus\varphi_{(0,\chi_2^\tau(A),0)})_{|\chi_1^\tau(A)}\right)\end{aligned}$$

where $\chi^\tau(A) = (\chi_1^\tau(A), \chi_2^\tau(A))$ and $\chi_1^\tau(A)$ represents the first k_1 variables while $\chi_2^\tau(A)$ represents the next k_2 ones.

V. Computing the Bias When $k = t+1$

As a direct corollary of Theorem 9, we obtain the following theorem which shows that equality holds in Corollary 6 when, amongst all linear functions depending on the k variables involved in $\mathcal{T}$, a single one corresponds to a biased approximation of f. With this theorem, we recover the value of the bias of a parity-check relation involving the periods of k input sequences when the resiliency order of f is equal to $(k-1)$. This particular case of our theorem corresponds to the case identified in [14], [7] where the piling-up approximation holds.

Theorem 12: With the notation of Theorem 9, suppose that there exists at most one linear function φ_u with $u\in V_k$ such that $\mathcal{E}(f+\varphi_u)\neq 0$. Then, we have

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \left[\mathcal{E}(f+\varphi_u)\right]^{2^s}.$$

In particular, if f is $(k-1)$-resilient, then

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = \left[\mathcal{E}(f+\varphi_{1_k})\right]^{2^s}.$$

where 1_k is the n-bit word whose first k coordinates are equal to 1 and the other ones are equal to 0.

Proof: Assume that u is the only element in V_k such that $\mathcal{E}(f+\varphi_u)$ may differ from zero. Then, the product involved in Theorem 9

$$\prod_{\tau\in\mathcal{T}}\mathcal{E}(f+\varphi_{(\chi^\tau(A),0)})$$

does not vanish if and only if $(\chi^\tau(A),0)=u$ for all $\tau\in\mathcal{T}$. Therefore, the only matrix A which satisfies this condition is defined by $A_{i,\tau}=u_i$ for all $1\leq i\leq k$ and for all τ. In particular, when f is $(k-1)$-resilient, the only vector $u\in V_k$ such that $\mathcal{E}(f+\varphi_u)$ may be nonzero is $u=1_k$. ■

For a t-resilient function, the bias of a parity-check relation involving any $(t+1)$ inputs is given by Theorem 12 but, as pointed out in [7], this result does not hold anymore when $\mathcal{T}$ involves $(t+2)$ sequences.

VI. When f is a t-Resilient Plateaued Function

We dedicate one section to t—resilient plateaued functions because, thanks to their particular form, they allow us to compute the bias of parity-check relations in a very efficient way even when $k=t+2$. We will also show how to build the parity-check relations with the highest possible bias. We will provide an upper bound on this bias when $k=t+v$, $\forall v$, and we will finally give some illustrative examples. The notion of plateaued functions was first defined in [17] using the Walsh coefficients, but here we will use the following equivalent formulation.

Definition 13: [17] A Boolean function f is a plateaued function if the biases of all its linear approximations belongs to $\{0,\pm\varepsilon\}$.

We can then prove [1] that the bias ε of any biased linear approximation of an n-variable plateaued function is of the form $\pm 2^{i-n}$ for some integer i. This type of function is widely used in cryptography. For instance, the Boolean functions used in both versions of Achterbahn are plateaued. The parity-check relations built from plateaued functions are particularly easy to study as the bias of all their biased linear approximations have the same magnitude.

A. How to Efficiently Compute the Bias When $k=t+2$

We are going to consider t-resilient plateaued functions.

Proposition 14: Let f be a t-resilient plateaued function with $\mathcal{E}(f+\varphi_a)\in\{0,\pm\varepsilon\}$ for all $a\in\mathbf{F}_2^n$. Let $k=t+2$. Then, with the notation and hypotheses of Theorem 9, we define

$$\nu=\#\{A\in\mathbf{F}_2^{k\times 2^{s-1}}\ :\mathcal{E}(f\oplus\varphi_{(\chi^\tau(A),0)})\neq 0 \text{ for all } \tau\in\mathcal{T}\}.$$

Then, we have

$$\mathcal{E}(PC_{f,\mathcal{T}})=\nu\varepsilon^{2^s}.$$

Proof: We use the expression of the bias of parity-check relations which has been introduced in Theorem 9

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})=\sum_{A\in\mathbf{F}_2^{k\times 2^{s-1}}}\prod_{\tau\in\mathcal{T}}\mathcal{E}(f\oplus\varphi_{(\chi^\tau(A),0)})\qquad(6)$$

where all the nonzero $\mathcal{E}(f+\varphi_{(u,0)})$, $u\in\mathbf{F}_2^k$ have the same absolute value. For a given A, the value of the product will be 0 if at least one of the $\mathcal{E}(f+\varphi_{(u,0)})$ appearing in it is zero, and will be $\pm\varepsilon^{2^s}$ if none of them is zero. Now, we will show that, in the case where we build parity-check relations with $t+2$ variables, this product cannot equal $-\varepsilon^{2^s}$. As previously explained, when the product

$$\prod_{\tau\in\mathcal{T}}\mathcal{E}(f\oplus\varphi_{(\chi^\tau(A),0)})$$

is not zero, none $\mathcal{E}(f\oplus\varphi_{(u,0)})$ is zero, implying that the Hamming weight of $\chi^\tau(A)$ satisfies $wt(\chi^\tau(A))\geq t+1$ for all $\tau\in\mathcal{T}$. Otherwise, as f is t—resilient, the bias of the corresponding approximation would be zero.

Let us consider a value of $\tau\in\mathcal{T}$, such that the corresponding vector $\chi^\tau(A)$ has Hamming weight $t+1$. Let i be the position in $\{1,\ldots t+2\}$ which does not belong to the support of $\chi^\tau(A)$. If τ lies in $\mathcal{T}_{I(i)}$ where

$$\mathcal{T}_{I(i)}=\Big\{\sum_{j\in\{1,\ldots,s\}\setminus\{I(i)\}}c_jM_j,\ \ c_j\in\{0,1\}\Big\}$$

then $\chi^{\tau+M_{I(i)}}(A)=\chi^\tau(A)$, as the bit i of $\chi^\tau(A)$ is unchanged and the others are necessarily 1. Similarly, if $\tau\in M_{I(i)}+\mathcal{T}_{I(i)}$, we have $\chi^{\tau-M_{I(i)}}(A)=\chi^\tau(A)$. We then deduce that, if $wt(\chi^\tau(A))=t+1$, the associated approximation appears twice in the product of biases, and so the signs will be equal two by two. As each element $\chi^\tau(A)$ of weight $(t+1)$ appears an even number of times in the product and the product has 2^s terms, the element $\chi^\tau(A)$ of weight $(t+2)$ appears also an even number of times. Therefore, the product is always positive. ■

Let us recall that the variables involved in $\mathcal{T}$ are distributed in s groups, $[\ell_i+1;\ell_{i+1}]$ determined by the periods appearing in M_i, $1\leq i\leq s$ where $\mathcal{T}=\big\{\sum_{i=1}^s c_iM_i,\ \ c_i\in\{0,1\}\big\}$. When $k=t+2$, the biased linear approximations of f correspond to the sum of all the k variables of indexes $\{1,\ldots,k\}$ or of all of them but one. Let I be the set of index $i\in\{1,\ldots,n\}$ such that $\mathcal{E}\left[f\oplus\bigoplus_{1\leq j\leq k,j\neq i}x_j\right]=\pm\varepsilon\neq 0$. Then, we are able to compute the exact value of $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$ when this set I is included in one of the s intervals $[\ell_i+1;\ell_{i+1}]$.

Proposition 15: Let f be a t-resilient plateaued function with $\mathcal{E}(f+\varphi_a)\in\{0,\pm\varepsilon\}$ for all $a\in\mathbf{F}_2^n$. Let $k=t+2$ and

$$I=\Big\{i,\ 1\leq i\leq k,\mathcal{E}\left[f\oplus\bigoplus_{1\leq j\leq k,j\neq i}x_j\right]\neq 0\Big\}.$$

With the notation and hypotheses of Theorem 9, we assume that I is included in an interval $[\ell_i+1;\ell_{i+1}]$ for some $1\leq i\leq s$. Then, we have

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})=N^{2^{s-1}}\varepsilon^{2^s}$$

when N is the number of biased linear approximations of f involving its first k variables.

Proof: From Proposition 14, we have to compute the number ν of matrices A in $\mathbf{F}_2^{k\times 2^{s-1}}$ for which we obtain ε^{2^s} since the value of the product in (6) is determined by the number of possible $\chi(A)$ whose all columns $\chi^{\tau}(A)$ correspond to biased linear approximations of f.

If the linear approximations defined by the 2^s values of τ are biased, then all $\chi^{\tau}(A)$ equal 1 on all the positions in $\{1,\dots,k\}\setminus[\ell_i+1;\ell_{i+1}]$. Now, the 2^{s-1} vectors formed by the restrictions of $\chi^{\tau}(A)$ to $[\ell_i+1;\ell_{i+1}]$ can correspond to the restrictions on $[\ell_i+1;\ell_{i+1}]$ of any biased linear approximation of f. The number of possibilities for each of these restrictions is then exactly the number N of restrictions to $[\ell_i+1;\ell_{i+1}]$ of biased linear approximations of f. Therefore, we have

$$\nu = N^{2^{s-1}}$$

implying that the bias of the parity-check relation is $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = N^{2^{s-1}}\varepsilon^{2^s}$. ■

Example: The function $f(x_1,\dots,x_5) = x_2 + x_5 + x_1x_4 + x_3x_4 + x_4x_5 + x_1x_2x_3 + x_1x_3x_4 + x_1x_3x_5 + x_2x_3x_5 + x_3x_4x_5$ considered in the previous examples is a 1-resilient plateaued with $\mathcal{E}(f+\varphi_a) \in \{0, \pm 2^{-2}\}$ for all $a \in \mathbf{F}_2^5$. And only $N = 2$ linear approximations of f involving the first three variables are biased: $x_1 + x_2$ and $x_1 + x_2 + x_3$. Then, Proposition 15 applies since

$$\begin{aligned} I = &\{i,\ 1 \le i \le 3, \mathcal{E}\left[f \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_i\right] \neq 0\} \\ &= \{3\} \subset [\ell_2+1;\ell_3]. \end{aligned}$$

Then, we have

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = 2^2(2^{-2})^4 = 2^{-6}.$$

More generally, we conjecture that $\nu = N^{2^{s-1}}$ is the highest value we can get for any possible decomposition of I with respect to the intervals $[\ell_i+1;\ell_{i+1}]$. The following example shows that this conjecture holds for $s \le 3$.

Example: We now give an exact formula for ν for $s = 3$ in the case of any decomposition of I and any Boolean function f. Here

$$\mathcal{T} = \{c_1M_1 + c_2M_2 + c_3M_3,\ c_1, c_2, c_3 \in \{0,1\}\}.$$

We decompose the rows of matrix $\chi(A)$ into three blocks corresponding to the three intervals $[\ell_i+1, \ell_{i+1}]$, $1 \le i \le 3$ as shown by (7) at the bottom of the page, where each element $A_{i,\tau}$ is a column vector of size $(\ell_{i+1} - \ell_i)$.

- Suppose that the variables in the set I, which defines the biased approximations, belong to two intervals, namely $[\ell_2+1;\ell_3]$ and $[\ell_3+1;\ell_4]$. Then, we can see that the only possible correct value for all $A_{1,\tau}$ is the all-1 vector. However, any value different from the all-one vector on $[\ell_3+1;\ell_4]$ imposes that the corresponding element in $[\ell_2+1;\ell_3]$ equals the all-1 vector. For instance, any value of $A_{3,0}$ different from the all-one vector determines the values of $A_{2,0}$ and of A_{2,M_3}. Then, in this case we deduce:

$$\nu = N^{2^{3-2}} = N^2.$$

- Suppose now that the variables from I are distributed into the three intervals. Then, we have

$$\nu = N.$$

Example: Let us consider $f = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$, which is a plateaued function with 3 variables and 0-resilient. Its biased linear approximations are x_1, x_2, x_3 (with bias $\frac{1}{2}$) and $x_1 + x_2 + x_3$ (with bias $-\frac{1}{2}$). We want to compute the bias $\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}})$ for $\mathcal{T} = \{0, T_1, T_2, T_1 + T_2\}$. Using the same notation as in the previous example, we have

$$A = \begin{pmatrix} A_{1,0} & A_{1,T_2} \\ A_{2,0} & A_{2,T_1} \end{pmatrix}$$

implying that the $\chi^{\tau}(A)$ correspond to

$$\begin{aligned} \chi^{0}(A) &= (A_{1,0}, A_{2,0}) \\ \chi^{T_1}(A) &= (A_{1,0}, A_{2,T_1}) \\ \chi^{T_2}(A) &= (A_{1,T_2}, A_{2,0}) \\ \chi^{T_1+T_2}(A) &= (A_{1,T_2}, A_{2,T_1}). \end{aligned}$$

We need to compute the number ν of matrices A such that all four $\chi^{\tau}(A)$ corresponds to a biased approximation of f. In our case, this equivalently means that all $\chi^{\tau}(A)$ have Hamming weight 1. Then, only the two matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } A = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

satisfy the condition. We recover the previously obtained formula:

$$\nu = 2^{2^{2-2}} = 2.$$

The bias will then be

$$\mathcal{E}(\boldsymbol{PC_{f,\mathcal{T}}}) = 2\varepsilon^{2^2} = 2^{-3}.$$

Based on many simulation results, we also conjecture that the fact that $N^{2^{s-1}}\varepsilon^{2^s}$ is the maximal possible bias is valid for any k and not only for $k = t + 2$.

Conjecture 16: Let f be a t-resilient plateaued function. The bias of any parity check relation with 2^s terms involving k variables is at most $N^{2^{s-1}}\varepsilon^{2^s}$ where N is the number of biased

$$\begin{pmatrix} A_{1,0} & A_{1,0} & A_{1,M_2} & A_{1,M_2} & A_{1,M_3} & A_{1,M_3} & A_{1,M_2+M_3} & A_{1,M_2+M_3} \\ A_{2,0} & A_{2,M_1} & A_{2,0} & A_{2,M_1} & A_{2,M_3} & A_{2,M_1+M_3} & A_{2,M_3} & A_{2,M_1+M_3} \\ A_{3,0} & A_{3,M_1} & A_{3,M_2} & A_{3,M_1+M_2} & A_{3,0} & A_{3,M_1} & A_{3,M_2} & A_{3,M_1+M_2} \end{pmatrix} \tag{7}$$

linear approximations of f involving those k variables and ε is the associated bias.

B. Example: How to Build the Best Parity-Check Relation With 8 Variables for a 6-resilient Plateaued Function and Compute its Bias

We are going to consider the plateaued function G of 11 variables used in Achterbahn-80, which is 6-resilient. All its biased linear approximations have bias $\pm 2^{-3}$. We want to build parity-check relations with $k = 8$ variables. We consider all possible subsets with 8 variables, and, for each of them, we determine the number of linear approximations can be build with these variables, i.e., the number of subsets of 7 or 8 variables of the considered set of 8 variables correspond to a biased linear approximation.

As an example, we choose the following set of 8 variables: $J = \{1, 4, 5, 6, 7, 9, 10, 11\}$. For the sake of simplicity, we are going to represent each subset of $\{1, \dots, 11\}$ by a vector in $\mathbf{F}_2^{11}$, here in hexadecimal, where the most right bit represents x_1 and the most left bit x_{11}. The set J corresponds then to `0x779`. In our case, with these variables we can build the following approximations:

$$x_1 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_9 \oplus x_{10} \oplus x_{11}, \text{ for } \texttt{0x779}.$$
$$x_1 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_9 \oplus x_{10} \oplus x_{11}, \text{ for } \texttt{0x769}.$$
$$x_1 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_9 \oplus x_{10} \oplus x_{11}, \text{ for } \texttt{0x771}.$$
$$x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_9 \oplus x_{10} \oplus x_{11}, \text{ for } \texttt{0x778}.$$

We can gather these 8 variables in 3 groups in two different ways, corresponding to two different 8-term parity-check relations:

- Let us first consider the following groups: $G_1 = \{1, 4, 5\}$, $G_2 = \{6, 7, 9\}$, and $G_3 = \{10, 11\}$.
  They define a parity-check relation built with

$$\mathcal{T} = \{c_1 T_1 T_4 T_5 + c_2 T_6 T_7 T_9 + c_3 T_{10} T_{11},\ c_1, c_2, c_3 \in \{0, 1\}\}.$$

  We observe that the variables from J missing in the 3 biased approximations with 7 variables always appear in the first group G_1. This means that the number of times ν where the product

$$\prod_{\tau \in \mathcal{T}} \mathcal{E}(f \oplus \varphi_{(\chi^\tau(A),0)})$$

  is not zero, is equal to $\nu = 4^{2^{s-1}}$. Here, $s = 3$, implying that the overall bias of this parity-check relation is

$$(2^{-3})^{2^s} \times 4^{2^{s-1}} = 2^{-16}$$

  which coincides with the bias computed with the algorithm described in Section VI-A. The previously used algorithm for computing the bias of this parity check requires 2^{56} computations, our algorithm computes it with a time complexity of 2^{35}, and in this particular case, we are able to deduce its value from a simple equation. This is the highest bias which can obtained for a parity-check relation build from 8 variables for the Achterbahn-80 combination function.

- Let us now consider the case where the groups are $G_1 = \{1, 9, 10\}$, $G_2 = \{5, 6, 7\}$ and $G_3 = \{4, 11\}$:
  They define a parity check equation built with

$$\mathcal{T} = \{c_1 T_1 T_9 T_{10} + c_2 T_5 T_6 T_7 + c_3 T_4 T_{11},\ c_1, c_2, c_3 \in \{0, 1\}\}.$$

  Here, the approximation `0x769` corresponds to a missing variable from G_2, `0x771` to a missing variable from G_3 and `0x778` to a missing variable from G_1. This will mean that the number of times that $\prod_{\tau \in \mathcal{T}} \mathcal{E}(f \oplus \varphi_{(\chi^\tau(A),0)}) \neq 0$ will be smaller than in the previous case. The final bias that we find is as follows:

$$(2^{-3})^{2^s} \times 108 = 2^{-17.25}.$$

  It coincides with the exact bias computed by the algorithm in Section VI-A.

  Let us now detail how we obtained $\nu = 108$. The main idea is to look at all possible cases for the vectors $\chi^\tau(A)$, by decomposing them into simpler cases. For example, we start by counting the number of cases where all the words $A_{1,0}, \dots, A_{1,M_1+M_3}$ corresponding to the first group differ from the all-one word. This number will be the first term of the sum (8) below. It equals 1 since all the words for the other groups are fixed determined if we impose that the product is not zero. Next, we count the number of cases where exactly three of the words $A_{1,0}, \dots, A_{1,M_1+M_3}$ differ from the all-one word. We have four possibilities for choosing which of the words equals the all-one word, but a single solution for each possibility, so the second term of the sum is 4. We continue this way. The most complex term, which is the fifth bracket, corresponds to the case where all the $A_{1,0}$, A_{1,M_2}, A_{1,M_3} and A_{1,M_2+M_3} are equal to the all-one word. In this case, we need to proceed recursively: we determine the number of cases where the four words $A_{2,0}$, A_{2,M_1}, A_{2,M_3} and $A_{2,M1+M_3}$ differ from the all-one word, where exactly three of them differ from the all-one word... This way, we can compute ν and we obtain

$$\nu = (1) + (4) + (18) + (27) + (1 + 4 + 12 + 16 + 16) = 108. \quad (8)$$

VII. Conclusion

Clearly, computing the accurate values of the biases of parity-check relations is of main importance for correctly estimating the complexity of some attacks on combination generators. The most direct impact of our results is the reduction of the complexity for computing these biases in any case. In some particular cases, this computation is even more simplified and it can be done with a simple formula, while the previously known methods had an unfeasible complexity. An important result is that the knowledge of only a few Walsh coefficients of the combination function is usually sufficient for estimating the bias of a parity-check relation. For instance, we have established a lower bound on the bias which provides some information even on parity-check relations built from non-biased approximations, and this is the first result in such a situation.

In the case of t-resilient functions, the bias of any relation built with $t+1$ variables exclusively depends on the bias of the associated linear approximation. This result can be extended to the case of plateaued functions: for parity-check relations involving $t+2$ variables, we have shown how the best parity-check relations involving $(t+2)$ variables can be easily determined and how their biases can be computed.

Acknowledgment

The authors would like to greatly thank the anonymous reviewers for their helpful comments which considerably improved the presentation of the technical material of the manuscript.

References

[1] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions," in *Proc. Adv. Cryptol. (EUROCRYPT'2000)*, 2000, vol. 1807, pp. 507–522.

[2] B. Gammel, R. Göttfert, and O. Kniffler, "An NLFSR-based stream cipher," in *Proc. ISCAS 2006—Int. Symp. Circuits Syst.*, 2006.

[3] B. Gammel, R. Göttfert, and O. Kniffler, The Achterbahn Stream Cipher Submitted to eSTREAM, 2005 [Online]. Available: http://www.ecrypt.eu.org/stream/

[4] B. Gammel, R. Göttfert, and O. Kniffler, Improved Boolean Combining Functions for Achterbahn eSTREAM Rep. 2005/072, 2005 [Online]. Available: http://www.ecrypt.eu.org/stream/papersdir/072.pdf

[5] B. Gammel, R. Göttfert, and O. Kniffler, Achterbahn-128/80 Submitted to eSTREAM, 2006 [Online]. Available: http://www.ecrypt.eu.org/stream/

[6] B. Gammel, R. Göttfert, and O. Kniffler, "Status of Achterbahn and tweaks," in *Proc. SASC 2006—Stream Ciphers Revisited*, 2006.

[7] R. Göttfert and B. Gammel, "On the frame length of Achterbahn-128/80," in *Proc. 2007 IEEE Inf. Theory Workshop on Inf. Theory for Wireless Netw.*, 2007, pp. 1–5.

[8] C. Harpes, G. Kramer, and J. L. Massey, "A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma," in *Proc. Adv. Cryptol. (EUROCRYPT'95)*, 1995, vol. 921, pp. 24–38.

[9] M. Hell and T. Johansson, "Cryptanalysis of Achterbahn-Version 2," in *Proc. Sel. Areas in Cryptogr. (SAC 2006)*, 2006, vol. 4356, pp. 45–55.

[10] M. Hell and T. Johansson, "Cryptanalysis of Achterbahn-128/80," *IET Inf. Secur.*, vol. 1, no. 2, pp. 47–52, 2007.

[11] T. Johansson, W. Meier, and F. Muller, "Cryptanalysis of Achterbahn," in *Proc. Fast Software Encrypt. (FSE 2006)*, 2006, vol. 4047, pp. 1–14.

[12] Z. Kukorelly*, On the Validity of Certain Hypotheses Used in Linear Cryptanalysis*, ser. ETH Ser. Inf. Process.. Konstanz: Hartung-Gorre Verlag, 1999, vol. 13.

[13] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Adv. Cryptolo. (EUROCRYPT'93)*, 1994, vol. 765.

[14] M. Naya-Plasencia, "Cryptanalysis of Achterbahn-128/80," in *Proc. Fast Software Encrypt. (FSE 2007)*, 2007, vol. 4593, pp. 73–86.

[15] K. Nyberg, "Correlation theorems in cryptanalysis," *Discr. Appl. Math.*, vol. 111, no. 1–2, pp. 177–188, 2001.

[16] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Trans. Inf. Theory*, vol. C-34, no. 1, pp. 81–84, 1985.

[17] Y. Zheng and X.-M. Zhang, "Plateaued functions," in *Proc. Inf. Commun. Secur. (ICICS'99)*, 1999, vol. 1726, pp. 224–300.

Anne Canteaut received the French engineer's degree from the École Nationale Supérieure de Techniques Avancées in 1993 and the Ph.D. degree in computer science from the University of Paris VI, France, in 1996.

Since 1997, she has been a researcher with the French National Research Institute in Computer Science (INRIA), Rocquencourt. She is currently Director of Research and the scientific head of the SECRET research team at INRIA. Her research interests include cryptography and coding theory.

Dr. Canteaut has served on program committees for several international conferences such as Crypto, FSE, and Eurocrypt. She served on the Editorial Board of the IEEE Transactions on Information Theory (2005 to 2008).

María Naya-Plasencia received the joint engineer's degree from the ETSIT of the Universidad Politécnica de Madrid, Spain, and the Institut National des Télécommunications Sud-Paris, France, in 2005 and the Ph.D. degree in computer science from the University of Paris VI, France, in 2009.

She is currently a Postdoctoral Fellow at the University of Versailles. Her main research interest is symmetric cryptography.

Dr. Naya-Plasencia has served on program committees for several international conferences such as FSE and SAC.