Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Finite Fields and Their Applications 13 (2007) 366–381
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Propagation characteristics of $x \mapsto x^{-1}$ and Kloosterman sums

Pascale Charpin [a,*], Tor Helleseth [b], Victor Zinoviev [c]

[a] *INRIA, Domaine de Voluceau-Rocquencourt, BP 105-78153, Le Chesnay, France*
[b] *Department of Informatics, University of Bergen, N-5020 Bergen, Norway*
[c] *Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, 101447 Moscow, Russia*

Received 12 October 2004; revised 17 August 2005

Available online 26 October 2005

Communicated by Gary L. Mullen

Abstract

We study the inverse permutation $\sigma : x \mapsto x^{-1}$ on the field of order 2^n by means of their component functions f_λ. We prove that the weights of derivatives of f_λ can be expressed in terms of Kloosterman sums. We are then able to compute some indicators of the propagation characteristics of σ. We can claim that σ, which is considered as a *good* cryptographic mapping regarding several criteria, is moreover such that the functions f_λ have good propagation properties with respect to these indicators.

We further deduce several new formulas on Kloosterman sums, by using classical formulas which link any Boolean function with its derivatives.

Keywords: Vectorial mapping; Inverse permutation; Melas codes; Boolean functions; Derivative; Cryptographic criterion; Propagation characteristics; Kloosterman sum

* Corresponding author.
E-mail address: pascale.charpin@inria.fr (P. Charpin).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2005.08.007

1. Introduction

The security of most conventional cryptographic systems is based on some properties of Boolean functions—currently called *cryptographic criteria*. In *iterated block ciphers*, the ciphertext is obtained by iteratively applying a keyed function, called the *round function*, to the plaintext. The design of such ciphers relies on the development of their cryptanalysis. It is particularly true since the publication of two generic attacks: the *differential* and the *linear* cryptanalysis. The ability to resist against differential cryptanalysis was notably described through specific criteria of Boolean functions (see, for instance, [1,2]). The *propagation criterion* (PC) was introduced by Preneel et al. [15], generalizing the *strict avalanche criterion* [16]. More generally, the *propagation characteristics* of any Boolean function refer to certain properties of its derivatives [17].

Let us denote by $\mathcal{B}_n$ the set of Boolean functions of n variables. Throughout the paper, $E^* = E \setminus \{0\}$ for any set E. For computing the spectrum of any $f \in \mathcal{B}_n$ we will use the notation:

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

The differential properties (sometimes called autocorrelation properties) measure the unbalancedness of the function's derivatives. More formally, for any Boolean function $f \in \mathcal{B}_n$, its derivative with respect to nonzero $a \in \mathbf{F}_2^n$ is the function of $\mathcal{B}_n$ defined as

$$D_a f(x) = f(x) + f(x + a), \quad x \in \mathbf{F}_2^n. \tag{2}$$

The worst case arises when $D_a f(x)$ is constant, that is $D_a f(x) = 0$ or 1, for some nonzero a. Such an a is called a *linear structure* of f. This feature should be avoided in a well-designed cipher and furthermore it is of interest to choose f such that the absolute value of the differential spectra,

$$M(f) = \max_{a \in \mathbf{F}_2^{n*}} \left|\mathcal{F}(D_a f)\right|, \tag{3}$$

is minimized. In [17], the authors propose another indicator, the second moment of the auto-correlation coefficients called the *sum-of-squares* indicator

$$\nu(f) = \sum_{a \in \mathbf{F}_2^n} \left(\mathcal{F}(D_a f)\right)^2, \tag{4}$$

where, by convention, $\mathcal{F}(D_0 f) = 2^n$. Note that obviously $2^{2n} \leqslant \nu(f) \leqslant 2^{3n}$ with equality if and only if f is bent[1] and f is constant, respectively. A function f is said to have

[1] f is bent if and only if all its derivatives are balanced, that is $\mathcal{F}(D_a f) = 0$ for any $a \neq 0$. Bent functions exist for even n only. They have the best possible nonlinearity which is $2^{n-1} - 2^{n/2-1}$.

good propagation characteristics with respect to the indicators $M(f)$ and $\nu(f)$ when these quantities are *small*.

In the case of vectorial functions, that is functions G with n binary inputs and m binary outputs, the derivatives of G may be defined with respect to the nonzero linear combinations of its coordinates, m Boolean functions $g_1, \ldots, g_m$ providing the m outputs. Hence, for any nonzero $b \in \mathbf{F}_2^m$ we consider the Boolean function $g^{(b)}(x) = \sum_{i=1}^m b_i g_i(x)$ and define $D_a g^{(b)}$ as in (2). Then similarly to the Boolean case we may look for the maximum absolute value of the spectra,

$$\mathcal{M}(G) = \max_{b \in \mathbf{F}_2^{m*}} M\big(g^{(b)}\big), \tag{5}$$

and also to

$$\mathcal{V}(G) = \max_{b \in \mathbf{F}_2^{m*}} \nu\big(g^{(b)}\big). \tag{6}$$

The $2^m - 1$ functions $g^{(b)}$ are usually called the *component* functions of G. In the case where $m = n$, G is generally a permutation on $\mathbf{F}_2^n$. Some *power permutations*, $x \mapsto x^d$, are used in DES-like cryptosystems, notably the *almost bent* functions [5] for odd n. For the study of power permutations it is usual to identify $\mathbf{F}_2^n$ with the field of order 2^n. The component functions of $x \mapsto x^d$ are the functions

$$x \mapsto \mathrm{Tr}\big(\lambda x^d\big), \quad \lambda \in \mathbf{F}_{2^n},$$

where Tr is the trace function, i.e., $\mathrm{Tr}(a) = a + a^2 + \cdots + a^{2^{n-1}}$ for any $a \in \mathbf{F}_{2^n}$.

The permutation $\sigma : x \mapsto x^{-1}$ appears in the design of the AES cryptosystem [8]. This permutation is considered as a *very good* cryptographic mapping. Notably, it opposes an high resistance against differential cryptanalysis [14]. Note that to compute the spectrum of any component function $x \mapsto \mathrm{Tr}(\lambda x^{-1})$ of σ is exactly to compute a *Kloosterman sum*.

In this paper we essentially prove that the mapping $\sigma : x \mapsto x^{-1}$ has *good propagation characteristics* with respect to the indicators $\mathcal{M}(\sigma)$ and $\mathcal{V}(\sigma)$. We obtain this result by establishing a relation between the spectra of component functions and of its derivatives (Theorem 1). We give the exact values of $\mathcal{M}(\sigma)$ and $\mathcal{V}(\sigma)$ (Theorem 2). We then derive a number of new formulas on Kloosterman sums which make our's contribution to the theory of Kloosterman sums (Propositions 1–4).

2. Preliminaries

From now on, we identify $\mathbf{F}_2^n$ with the field of order 2^n, denoted $\mathbf{F}_{2^n}$. So the set $\mathcal{B}_n$ is the set of Boolean functions on $\mathbf{F}_{2^n}$. Recall that Tr is the trace-function on $\mathbf{F}_{2^n}$ and set $e(p(x)) = (-1)^{\mathrm{Tr}(p(x))}$ for any polynomial p on $\mathbf{F}_{2^n}$.

Let us denote by φ_a, $a \in \mathbf{F}_{2^n}$, the linear functions of $\mathcal{B}_n$. They are defined as follows: $\varphi_a(x) = \mathrm{Tr}(ax)$ for $x \in \mathbf{F}_{2^n}$. For any Boolean function $g \in \mathcal{B}_n$, the Fourier-transform of g in point $a \in \mathbf{F}_{2^n}$ is

$$\mathcal{F}(g + \varphi_a) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{g(x)+\mathrm{Tr}(ax)}. \tag{7}$$

The set $\{\mathcal{F}(g + \varphi_a) \mid a \in \mathbf{F}_{2^n}\}$ is usually called the *spectrum* of g. The Hamming weight of $g \in \mathcal{B}_n$, say $\mathrm{wt}(g)$, is the number of x such that $g(x) = 1$. The function g is said to be *balanced* when $\mathrm{wt}(g) = 2^{n-1}$. The *nonlinearity* $N(g)$ of g is the minimum value of $\mathrm{wt}(g + \varphi_a)$, when a runs through $\mathbf{F}_{2^n}$; it is quantified by

$$\mathcal{L}(g) = \max_{a \in \mathbf{F}_{2^n}} \left|\mathcal{F}(g + \varphi_a)\right|. \tag{8}$$

Recall that

$$N(g) = 2^{n-1} - \frac{\mathcal{L}(g)}{2}.$$

We will need some classical formulas on Boolean functions. First recall, for any $g \in \mathcal{B}_n$, Parseval's relation

$$\sum_{a \in \mathbf{F}_{2^n}} \mathcal{F}^2(g + \varphi_a) = 2^{2n} \tag{9}$$

and also the inverse formula of (7), for any $b \in \mathbf{F}_{2^n}$,

$$\sum_{a \in \mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(ab)} \mathcal{F}(g + \varphi_a) = 2^n (-1)^{g(b)}. \tag{10}$$

Basic properties on Boolean functions can be found, for instance, in [2,3,7] and in references therein.

Definition 1. The classical Kloosterman sum $K(a)$ on $\mathbf{F}_{2^n}$, for each $a \in \mathbf{F}_{2^n}$, is defined as follows:

$$K(a) = \sum_{x \in \mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(\frac{1}{x} + ax)}.$$

The *complete* Kloosterman sum is $\mathcal{K}(a) = K(a) + 1$, when taking the sum above on $\mathbf{F}_{2^n}$ (by convention $0^{-1} = 0$).

The set of values of $K(a)$ was determined by Lachaud and Wolfmann [12, Theorem 3.4]. In the next lemma, $K(a)$ is replaced by $\mathcal{K}(a) = K(a) + 1$.

Lemma 1. *The set* $\{\mathcal{K}(a) \mid a \in \mathbf{F}_{2^n}^*\}$ *is the set of all integers* s *such that*

$$s \equiv 0 \pmod 4 \quad \text{in the range } \left[-2^{(n/2)+1}+1,\ 2^{(n/2)+1}+1\right].$$

Consequently, the function $f \in \mathcal{B}_n$, defined by $f(x) = \mathrm{Tr}(x^{-1})$, satisfies:

$$\mathcal{L}(f) = \begin{cases} 2^{(n+2)/2} & \text{for even } n, \\ \max\{k \equiv 0 \pmod 4 \mid k < 2^{(n/2)+1}+1\} & \text{for odd } n. \end{cases} \tag{11}$$

Note that we have (where $x = ya$ and $z^2 = y$):

$$\sum_{x \in \mathbf{F}_{2^n}^*} e\left(\frac{a}{x} + ax\right) = \sum_{y \in \mathbf{F}_{2^n}^*} e\left(\frac{1}{y} + a^2 y\right) = \sum_{z \in \mathbf{F}_{2^n}^*} e\left(\frac{1}{z} + az\right).$$

Thus

$$K(a) = \sum_{x \in \mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(\frac{a}{x}+ax)} \quad \text{and} \quad \mathcal{K}(a) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(\frac{a}{x}+ax)}. \tag{12}$$

Note that $\mathcal{K}(0) = 0$ and, further, $\mathcal{K}(1/0) = 0$, since by convention $0^{-1} = 0$. The following result was previously proved by Helleseth and Zinoviev in [11]:

Lemma 2. *For any* $n \geqslant 3$,

$$\mathcal{K}(a) \equiv \begin{cases} 4 \pmod 8 & \text{if } \mathrm{Tr}(a) = 1, \\ 0 \pmod 8 & \text{if } \mathrm{Tr}(a) = 0. \end{cases}$$

3. Propagation characteristics of $x \mapsto x^{-1}$

From now on we denote by σ the permutation $x \mapsto x^{-1}$ on $\mathbf{F}_{2^n}$, and we assume that $n \geqslant 3$.

Theorem 1. *Let* $\lambda \in \mathbf{F}_{2^n}^*$ *and define* $f_\lambda \in \mathcal{B}_n$ *as* $f_\lambda(x) = \mathrm{Tr}(\lambda x^{-1})$, $x \in \mathbf{F}_{2^n}$. *Recall that* $D_u f_\lambda(x) = f_\lambda(x) + f_\lambda(x+u)$ *and* $e(p(x)) = (-1)^{\mathrm{Tr}(p(x))}$. *Then for any* $u \neq 0$:

$$\mathcal{F}(D_u f_\lambda) = \mathcal{K}\left(\frac{\lambda}{u}\right) + 2\left(e\left(\frac{\lambda}{u}\right) - 1\right) = \sum_{x \in \mathbf{F}_{2^n}} e\left(\frac{\lambda}{u}\left(x^{-1} + x\right)\right) + 2\left(e\left(\frac{\lambda}{u}\right) - 1\right). \tag{13}$$

Proof. For any $u \in \mathbf{F}_{2^n}^*$, we compute $\mathcal{F}(D_u f_\lambda)$:

$$
\begin{aligned}
\mathcal{F}(D_u f_\lambda) &= \sum_{x\in\mathbf{F}_{2^n}} e\big(\lambda\big(x^{-1}+(x+u)^{-1}\big)\big)\\
&= \sum_{x\in\mathbf{F}_{2^n}\setminus\{0,u\}} e\left(\lambda\left(\frac{1}{x}+\frac{1}{x+u}\right)\right)+2e\left(\frac{\lambda}{u}\right)\\
&= \sum_{x\in\mathbf{F}_{2^n}\setminus\{0,u\}} e\left(\lambda\left(\frac{x+u+x}{x^2+ux}\right)\right)+2e\left(\frac{\lambda}{u}\right)\\
&= \sum_{x\in\mathbf{F}_{2^n}\setminus\{0,u\}} e\left(\lambda\left(\frac{u}{x^2+ux}\right)\right)+2e\left(\frac{\lambda}{u}\right)\\
&= \sum_{y\in\mathbf{F}_{2^n}\setminus\{0,1\}} e\left(\lambda\left(\frac{u}{(u/y)^2+(u^2/y)}\right)\right)+2e\left(\frac{\lambda}{u}\right)\\
&= \sum_{y\in\mathbf{F}_{2^n}\setminus\{0,1\}} e\left(\lambda\left(\frac{uy^2}{u^2(y+1)}\right)\right)+2e\left(\frac{\lambda}{u}\right)\\
&= \sum_{y\in\mathbf{F}_{2^n}\setminus\{0,1\}} e\left(\lambda\left(\frac{(y+1)^2+1}{u(y+1)}\right)\right)+2e\left(\frac{\lambda}{u}\right)\\
&= \sum_{y\in\mathbf{F}_{2^n}\setminus\{0,1\}} e\left(\frac{\lambda}{u}\left((y+1)+\frac{1}{y+1}\right)\right)+2e\left(\frac{\lambda}{u}\right)\\
&= \sum_{z\in\mathbf{F}_{2^n}\setminus\{0,1\}} e\left(\frac{\lambda}{u}\left(z+\frac{1}{z}\right)\right)+2e\left(\frac{\lambda}{u}\right).
\end{aligned}
$$

In the computation above we set first $y = u/x$, and later $z = y + 1$. Thus, using (12), we can express $\mathcal{F}(D_u f_\lambda)$ as follows:

$$\mathcal{F}(D_u f_\lambda) = \mathcal{K}\left(\frac{\lambda}{u}\right)+\left(2e\left(\frac{\lambda}{u}\right)-2\right). \qquad \square$$

The next property is easily proved; we indicate the proof for clarity.

Lemma 3. [7] *Let g be any function in $\mathcal{B}_n$, $n \geqslant 3$, such that* $\mathrm{wt}(g)$ *is even. Then for any $a \in \mathbf{F}_{2^n}$:*

$$\mathcal{F}(D_a g) \equiv 0 \pmod 8.$$

Proof. For any $a \neq 0$, we define the function $g_a : x \mapsto g(x + a)$. Then

$$\mathrm{wt}(D_a g) = \mathrm{wt}(g) + \mathrm{wt}(g_a) - 2\,\mathrm{wt}(g g_a) = 2\,\mathrm{wt}(g) - 2\,\mathrm{wt}(g g_a).$$

Now, we observe that x satisfies $g(x)g(x+a)=1$ if and only if $x+a$ satisfies this equation too. Thus $\mathrm{wt}(D_a g)$ is divisible by 4 or, equivalently, $\mathcal{F}(D_a g)$ is divisible by 8 since it is equal to $2^n - 2\,\mathrm{wt}(D_a g)$. □

Remark 1. It is easy to deduce Lemma 2 from the previous theorem. Indeed, according to Lemma 3, Theorem 1 implies, taking $u=1$ and any λ:

$$\mathcal{K}(\lambda) \equiv 2\big(1-(-1)^{\mathrm{Tr}(\lambda)}\big) \pmod 8.$$

Lemma 2 is obviously deduced, since the term above on the right equals 0 when $\mathrm{Tr}(\lambda)=0$ and 4 otherwise.

Theorem 1 extends, in a certain sense, Lemma 1. Recall that we assume that $n \geqslant 3$.

Corollary 1. *Let $f_\lambda \in \mathcal{B}_n$, $f_\lambda(x) = \mathrm{Tr}(\lambda x^{-1})$ with $\lambda \in \mathbf{F}_{2^n}^*$. Consider the derivatives of f_λ, with respect to $u \in \mathbf{F}_{2^n}^*$:*

$$D_u f_\lambda : x \mapsto \mathrm{Tr}\big(\lambda\big(x^{-1} + (x+u)^{-1}\big)\big).$$

Then $\mathcal{F}(D_u f_\lambda)$ takes any value s divisible by 8 in the range

$$\big[-2^{(n/2)+1} - 3,\ 2^{(n/2)+1} + 1\big] \quad \textit{when } u \textit{ runs through } \mathbf{F}_{2^n}^*.$$

Proof. Consider formula (13) for any fixed λ. We know from Lemma 1 that $\mathcal{K}(\lambda/u)$ takes any value s divisible by 4 in the range

$$\big[-2^{(n/2)+1} + 1,\ 2^{(n/2)+1} + 1\big] \quad \text{when } u \text{ runs through } \mathbf{F}_{2^n}^*.$$

Moreover, from Lemma 2, $\mathcal{K}(\lambda/u) \equiv 0 \pmod 8$ if and only if $\mathrm{Tr}(\lambda/u) = 0$.

Thus, when $\mathrm{Tr}(\lambda/u) = 0$ we get from (13):

$$\mathcal{F}(D_u f_\lambda) = \mathcal{K}(\lambda/u) \equiv 0 \pmod 8.$$

And we deduce that $\mathcal{F}(D_u f_\lambda)$ takes any value $\mathcal{K}(\lambda/u)$ which is divisible by 8 in the range $[-2^{(n/2)+1}+1,\ 2^{(n/2)+1}+1]$.

Assume now that $\mathrm{Tr}(\lambda/u) = 1$; thus $\mathcal{K}(\lambda/u)$ is congruent to 4 modulo 8. In this case, we have from (13) and using Lemma 3:

$$\mathcal{F}(D_u f_\lambda) = \mathcal{K}(\lambda/u) - 4 \equiv 0 \pmod 8.$$

Thus $\mathcal{F}(D_u f_\lambda)$ takes any value $\mathcal{K}(\lambda/u) - 4$, which is divisible by 8, in the range $[-2^{(n/2)+1} - 3, 2^{(n/2)+1} - 3]$, completing the proof. □

The functions f_λ, $\lambda \in \mathbf{F}_{2^n}^*$, are the component functions of the permutation σ. More precisely, taking any basis $\{\lambda_1, \ldots, \lambda_n\}$ in $\mathbf{F}_{2^n}$, σ can be represented as follows:

$$\sigma(x) = \begin{cases} f_{\lambda_1}(x), \\ \ldots \\ f_{\lambda_n}(x). \end{cases}$$

Using the previous theorem, we are going to compute the formulas (5) and (6) for σ. In the next corollary, we study the component functions of σ. Recall that $M(f)$ and $\nu(f)$, $f \in \mathcal{B}_n$, are respectively defined by (3) and (4).

Corollary 2. *Let $f_\lambda : x \mapsto \mathrm{Tr}(\lambda x^{-1})$, $f_\lambda \in \mathcal{B}_n$, with $\lambda \in \mathbf{F}_{2^n}^*$ ($n \geqslant 3$). Then $M(f_\lambda)$ and $\nu(f_\lambda)$ depend on n only. More precisely,*

$$M(f_\lambda) = \max_{a \in \mathbf{F}_{2^n}^*} \left| \mathcal{K}(a) + 2\left((-1)^{\mathrm{Tr}(a)} - 1\right) \right|. \tag{14}$$

That is, setting $\kappa_n = \max\{k \equiv 0 \pmod 4 \mid k < 2^{(n/2)+1} + 1\}$ for odd n,

$$M(f_\lambda) = \begin{cases} 2^{(n+2)/2} & \text{for even } n, \\ \kappa_n & \text{for odd } n \text{ such that } \kappa_n \equiv 0 \pmod 8, \\ \kappa_n \pm 4 & \text{for odd } n \text{ such that } \kappa_n \equiv 4 \pmod 8. \end{cases} \tag{15}$$

Moreover,

$$\nu(f_\lambda) = \begin{cases} 2^{2n+1} + 2^{n+3} & \text{if } n \text{ is even}, \\ 2^{2n+1} & \text{if } n \text{ is odd}. \end{cases}$$

Proof. By applying Theorem 1, formula (3) becomes

$$\begin{aligned} M(f_\lambda) &= \max_{u \in \mathbf{F}_{2^n}^*} \left| \mathcal{F}(D_u f_\lambda) \right| = \max_u \left| \mathcal{K}\left(\frac{\lambda}{u}\right) + 2\left((-1)^{\mathrm{Tr}(\lambda/u)} - 1\right) \right| \\ &= \max_{a \in \mathbf{F}_{2^n}^*} \left| \mathcal{K}(a) + 2\left((-1)^{\mathrm{Tr}(a)} - 1\right) \right|, \end{aligned}$$

by replacing $a = \lambda/u$. Note that λ and u are nonzero elements. Thus, (14) is proved.

From Lemma 1, we know the maximal absolute value of $\mathcal{K}(a)$, i.e., the nonlinearity of f_λ (see (11)). When n is even, it is exactly $2^{(n/2)+1}$ which is divisible by 8, since $n \geqslant 4$. Thus, we obtain this value for a such that $\mathrm{Tr}(a) = 0$ (Lemma 2); we further deduce from (14) that $M(f_\lambda) = 2^{(n+2)/2}$. For odd n, the maximal absolute value of $\mathcal{K}(a)$ equals κ_n. If κ_n is divisible by 8, we get as before $M(f_\lambda) = \kappa_n$. Otherwise, i.e., if $\kappa_n \equiv 4 \pmod 8$, assume that there is a such that $\mathcal{K}(a) = -\kappa_n$. For this a we have $\mathrm{Tr}(a) = 1$. Then, from (14),

$$M(f_\lambda) = |-\kappa_n - 4| = \kappa_n + 4.$$

If such a does not exist, we deduce that $\mathcal{K}(b)$, for $b \in \mathbf{F}_{2^n}$, takes all values divisible by 4 in the range $[-\kappa_n + 4,\ \kappa_n]$. Moreover, there is b such that $\mathcal{K}(b) = \kappa_n$ (with $\mathrm{Tr}(b) = 1$) and there is c such that $\mathcal{K}(c) = -\kappa_n + 4$ (with $\mathrm{Tr}(c) = 0$). Thus, according to (14), we get

$$M(f_\lambda) = \max\{|\kappa_n - 4|,\ |-\kappa_n + 4|\} = \kappa_n - 4,$$

completing the proof of (15). Now, using formulas (4) and (13), we have

$$\nu(f_\lambda) = \sum_{u \in \mathbf{F}_{2^n}} \big(\mathcal{F}(D_u f_\lambda)\big)^2 = 2^{2n} + \sum_{u \in \mathbf{F}_{2^n}^*} \left(\mathcal{K}\left(\frac{\lambda}{u}\right) + 2\big((-1)^{\mathrm{Tr}(\lambda/u)} - 1\big)\right)^2.$$

We are going to compute the sum above on the right. We denote by $\ell(u)$ the expression $(-1)^{\mathrm{Tr}(\lambda/u)} - 1$. Further, we have

$$\sum_{u \in \mathbf{F}_{2^n}^*} \left(\mathcal{K}\left(\frac{\lambda}{u}\right) + 2\ell(u)\right)^2 = \sum_{u \in \mathbf{F}_{2^n}^*} \left(\mathcal{K}\left(\frac{\lambda}{u}\right)\right)^2 + 4\left(\sum_{u \in \mathbf{F}_{2^n}^*} \left(\big(\ell(u)\big)^2 + \ell(u)\mathcal{K}\left(\frac{\lambda}{u}\right)\right)\right).$$

Using (9) and the fact that $\mathcal{K}(0) = 0$, we get

$$\sum_{u \in \mathbf{F}_{2^n}^*} \left(\mathcal{K}\left(\frac{\lambda}{u}\right)\right)^2 = 2^{2n}.$$

We now apply (10) two times in the next computation, taking $g(x) = \mathrm{Tr}(x^{-1})$, $b = 1$ and $b = 0$:

$$\begin{aligned}\sum_{u \in \mathbf{F}_{2^n}^*} \ell(u)\mathcal{K}\left(\frac{\lambda}{u}\right) &= \sum_{u \in \mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(\lambda/u)}\mathcal{K}\left(\frac{\lambda}{u}\right) - \sum_{u \in \mathbf{F}_{2^n}^*} \mathcal{K}\left(\frac{\lambda}{u}\right)\\ &= \sum_{a \in \mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(a)}\mathcal{K}(a) - \sum_{a \in \mathbf{F}_{2^n}} \mathcal{K}(a)\\ &= 2^n\big((-1)^{\mathrm{Tr}(1)} - 1\big).\end{aligned}$$

Since $(\ell(u))^2$ equals 0 if $\mathrm{Tr}(\lambda/u) = 0$ and 4 otherwise, we have

$$\sum_{u \in \mathbf{F}_{2^n}^*} \big(\ell(u)\big)^2 = 2^{n-1} \times 4 = 2^{n+1}.$$

Finally, we obtain

$$\nu(f_\lambda) = 2^{2n+1} + 2^{n+2}\big((-1)^{\mathrm{Tr}(1)} - 1\big) + 2^{n+3}.$$

Thus $\nu(f_\lambda) = 2^{2n+1} + 2^{n+3}$ when $\mathrm{Tr}(1) = 0$ (n even). Otherwise, if n is odd then $\nu(f_\lambda) = 2^{2n+1}$, completing the proof. □

Theorem 2. *Let σ be the permutation $x \mapsto x^{-1}$ on $\mathbf{F}_{2^n}$; the functions f_λ are the component functions of σ. The values $M(f_\lambda)$ and $\nu(f_\lambda)$ are given by Corollary 2. Then for any $\lambda \in \mathbf{F}_{2^n}^*$:*

$$\mathcal{M}(\sigma) = M(f_\lambda) \quad \textit{and} \quad \mathcal{V}(\sigma) = \nu(f_\lambda).$$

Proof. As noticed in Corollary 2, the values $M(f_\lambda)$ and $\nu(f_\lambda)$ do not depend on λ. Thus, we directly compute the formulas (5) and (6) for σ:

$$\mathcal{M}(\sigma) = \max_{\lambda \in \mathbf{F}_{2^n}^*} M(f_\lambda) = M(f_\lambda) \quad \text{and} \quad \mathcal{V}(\sigma) = \max_{\lambda \in \mathbf{F}_{2^n}^*} \nu(f_\lambda) = \nu(f_\lambda),$$

completing the proof. □

To conclude this section, we want to replace the cryptographic properties of σ in a more general context. Let G be any permutation on $\mathbf{F}_{2^n}$ and denote by g_λ, $\lambda \in \mathbf{F}_{2^n}^*$, the component functions of G. The *nonlinearity* of G is quantified by means of the nonlinearities of its component functions. Precisely,

$$\Lambda(G) = \max_{\lambda \in \mathbf{F}_{2^n}^*} \mathcal{L}(g_\lambda),$$

where $\mathcal{L}(g_\lambda)$ is defined by (8). When n is odd then $\Lambda(G)$ is known to be greater than or equal to $2^{(n+1)/2}$. When n is even, it is known that $\Lambda(G)$ is strictly greater than $2^{n/2}$; the best known value is $\Lambda(G) = 2^{(n+2)/2}$ for some G. If G is of the form $x \mapsto x^d$, where d and $2^n - 1$ are coprime, then all g_λ have the same nonlinearity. This is because

$$\sum_{x \in \mathbf{F}_{2^n}} e\big(bx^d + ax\big) = \sum_{y \in \mathbf{F}_{2^n}} e\left(y^d + \frac{a}{b^{1/d}} y\right),$$

where $y = b^{1/d}x$. In particular, $\Lambda(\sigma) = \mathcal{L}(f)$ where $f(x) = \mathrm{Tr}(x^{-1})$. The value $\mathcal{L}(f)$, given by (11), is deduced from Lemma 1. One considers that the inverse permutation σ has a *good* nonlinearity. For even n, σ has the best known nonlinearity.

Generally, the indicators $\mathcal{M}(G)$ and $\mathcal{V}(G)$ are not known. They are, however, known for some (but few) special functions G. Consider for instance, for odd n, any *almost bent* function G[2]. For such G, all component functions g_λ have the same spectrum, the set $\{0, \pm 2^{(n+1)/2}\}$. In this case $\mathcal{V}(G)$ is considered as *small*: $\mathcal{V}(G) = \nu(g_\lambda) = 2^{2n+1}$ for any λ [4,18]. But, $\mathcal{M}(G)$ is not known unless G is quadratic. When G is quadratic $\mathcal{M}(G)$ and $\mathcal{V}(G)$ can be computed. But such G has some component functions g_λ which have at least one constant derivative, i.e., one linear structure. This fact provides $\mathcal{M}(G) = 2^n$ which is the worst value.

Actually, little is known about $\mathcal{M}(G)$ and $\mathcal{V}(G)$ when G is any vectorial function, since there are few general results about the differential properties of Boolean functions. To find

[2] See [5] for more explanations on permutations and almost bent functions.

$M(g_\lambda)$ for any λ seems to be a very difficult problem, as well as to establish good bounds on these quantities.

To illustrate our purpose, we want to mention a recent work on $M(g)$, g being any Boolean function on $\mathbf{F}_{2^n}$, n odd. It was conjectured a long time that if g is balanced then $M(g) \geqslant 2^{(n+1)/2}$. Recently, Maitra and Sarkhar, in [13], proved that for $n = 15$, the Patterson–Wiedermann functions satisfy $M(g) = 160$ (while $2^{(n+1)/2} = 256$). Since these functions are not balanced, the authors derive from these functions a balanced function such that $M(g) = 216$, which disproves the conjecture.

Here we proved that any component function f_λ of σ is such that $M(f_\lambda)$ is close to $2^{n/2+1}$ and this is a *small* value. Note that, moreover, each f_λ is balanced. The indicator $\nu(f_\lambda)$ is also small comparing to the upper bound 2^{3m}. More precisely, it is small when we refer to Proposition V.2 of [3] which gives good upper bounds for functions g of high nonlinearity:

- if n is odd and $\mathcal{L}(g) \leqslant 2^{(n+1)/2}$ then $\nu(g) \leqslant 2^{2n+1}$;
- if n is even and $\mathcal{L}(g) \leqslant 2^{(n+2)/2}$ then $\nu(g) \leqslant 2^{2n+2}$.

Note that for n even $\mathcal{L}(f_\lambda) = 2^{(n+2)/2}$ and we proved that $\nu(f_\lambda) = 2^{2n+1} + 2^{n+3}$. For n odd we have $2^{(n+1)/2} \leqslant \mathcal{L}(f_\lambda) < 2^{n/2+1} + 1$, but we proved that $\nu(f_\lambda) = 2^{2n+1}$. Thus we can conclude:

Corollary 3. *The permutation $\sigma : x \mapsto x^{-1}$ has good propagation characteristics with respect to $\mathcal{M}(\sigma)$ and $\mathcal{V}(\sigma)$. In other terms, the indicators $\mathcal{M}(\sigma)$ and $\mathcal{V}(\sigma)$ (see respectively* (5) *and* (6)*) are small.*

4. New formulas on Kloosterman sums

In [3], several relations between the values $\mathcal{F}(g + \varphi_a)$ and $\mathcal{F}(D_u g)$, where $a \in \mathbf{F}_{2^n}$, $u \in \mathbf{F}_{2^n}^*$ and g is any function in $\mathcal{B}_n$, were studied. In this section, we consider the Boolean function $f : x \mapsto \mathrm{Tr}(x^{-1})$ on $\mathbf{F}_{2^n}$. Thus

$$(f + \varphi_a)(x) = \mathrm{Tr}\big(x^{-1} + ax\big) \quad \text{and} \quad \mathcal{F}(f + \varphi_a) = \mathcal{K}(a).$$

In the previous section, we proved that $\mathcal{F}(D_u f)$ can be expressed by means of $\mathcal{K}(1/u)$ (Theorem 1). We then deduced the value of $\nu(f)$. Using these results and classical formulas on Boolean functions, we will derive new formulas on Kloosterman sums. Recall that $n \geqslant 3$ as in the previous section.

Formulas (16)–(19) below are proved in [3] or usually known. First for any $g \in \mathcal{B}_n$:

$$\sum_{a \in \mathbf{F}_{2^n}} \mathcal{F}^4(g + \varphi_a) = 2^n \nu(g). \tag{16}$$

Thus, applying this to f and using Corollary 2, we obtain the following:

Proposition 1.

$$\sum_{a\in\mathbf{F}_{2^n}} \big(\mathcal{K}(a)\big)^4 = \begin{cases} 2^{3n+1}+2^{2n+3} & \text{if } n \text{ is even,} \\ 2^{3n+1} & \text{if } n \text{ is odd.} \end{cases}$$

Remark 2. By the previous proposition, we know the sum of the fourth powers of the $\mathcal{K}(a)$, $a \in \mathbf{F}_{2^n}$. Note that the sum of the third powers is known. It is given by

$$\sum_{a\in\mathbf{F}_{2^n}} \big(\mathcal{K}(a)\big)^3 = 2^{2n}N,$$

where N is the number of $x \in \mathbf{F}_{2^n}$ such that $1 + x^{-1} + (x+1)^{-1} = 0$ (see [10, Theorem 3.4]). It is easy to check that

$$1 + x^{2^{n-1}-1} + (x+1)^{2^{n-1}-1} = \frac{(x^{2^{n-2}}+x)^2}{x(1+x)}.$$

When $\gcd(n-2,n) = 1$ (i.e., n is odd) then $N = 2$. Otherwise, when n is even, $\gcd(n-2,n) = 2$ providing $N = 4$.

For any $g \in \mathcal{B}_n$ and $a \in \mathbf{F}_{2^n}$, we have this classical formula:

$$\mathcal{F}^2(g+\varphi_a) = \sum_{u\in\mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}(au)}\mathcal{F}(D_u g), \tag{17}$$

which leads to the next formula when applied to our function f.

Proposition 2. *For any $a \in \mathbf{F}_{2^n}$, $a \neq 0$:*

$$\big(\mathcal{K}(a)\big)^2 - 2\mathcal{K}(a) = 2^n + \sum_{u\in\mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(au)}\mathcal{K}\left(\frac{1}{u}\right).$$

Consequently, $\mathcal{K}(a) = 0$ if and only if the sum above on the right is equal to -2^n.

Proof. We apply (17) to the function f, where $f(x) = \mathrm{Tr}(x^{-1})$ so that $\mathcal{F}(f+\varphi_a) = \mathcal{K}(a)$. Using (13), we obtain

$$\begin{aligned} \mathcal{F}^2(f+\varphi_a) &= 2^n + \sum_{u\in\mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(au)}\mathcal{F}(D_u f) \\ &= 2^n + \sum_{u\in\mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(au)}\left(\mathcal{K}\left(\frac{1}{u}\right) + 2(-1)^{\mathrm{Tr}(1/u)} - 2\right) \end{aligned}$$

$$= 2^n + \sum_{u\in\mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(au)}\mathcal{K}\left(\frac{1}{u}\right) - 2\sum_{u\in\mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(au)} + 2\sum_{u\in\mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(1/u+au)}$$

$$= 2^n + \sum_{u\in\mathbf{F}_{2^n}^*} (-1)^{\mathrm{Tr}(au)}\mathcal{K}\left(\frac{1}{u}\right) + 2\mathcal{K}(a).$$

Noticing that one cannot have $\mathcal{K}(a) = 2$, the proof is completed. □

We will obtain another expression of $\mathcal{K}^2(a) - 2\mathcal{K}(a)$ as an instance of another general formula (see Proposition 3 later). Let V be a subspace of $\mathbf{F}_{2^n}$ of dimension k and denote by $V^\perp$ the dual of V. Then any $g \in \mathcal{B}_n$ satisfies

$$\sum_{a\in V} \mathcal{F}^2(g+\varphi_a) = 2^k \sum_{u\in V^\perp} \mathcal{F}(D_u g) \tag{18}$$

and

$$\sum_{a\in V} \mathcal{F}(g+\varphi_a) = 2^k \sum_{u\in V^\perp} (-1)^{g(u)}. \tag{19}$$

Note that in this paper

$$V^\perp = \big\{y \mid \mathrm{Tr}(yx) = 0 \text{ for all } x \in V\big\}.$$

Proposition 3. *For any subspace V of $\mathbf{F}_{2^n}$ of dimension k, $1 \leqslant k \leqslant n-1$:*

$$\sum_{a\in V}\big(\mathcal{K}^2(a) - 2\mathcal{K}(a)\big) = 2^{n+1}\big(2^{k-1}-1\big) + 2^k \sum_{u\in V^\perp} \mathcal{K}\left(\frac{1}{u}\right). \tag{20}$$

In particular, if $V = \{0, v\}^\perp$ for some $v \in \mathbf{F}_{2^n}^*$ then

$$\sum_{a,\ \mathrm{Tr}(av)=0}\big(\mathcal{K}^2(a) - 2\mathcal{K}(a)\big) = 2^{n+1}\big(2^{n-2}-1\big) + 2^{n-1}\mathcal{K}\left(\frac{1}{v}\right).$$

If $V = \{0, a\}$ then

$$\big(\mathcal{K}(a)\big)^2 - 2\mathcal{K}(a) = 2\sum_{u,\ \mathrm{Tr}(au)=0} \mathcal{K}\left(\frac{1}{u}\right). \tag{21}$$

Proof. Recall that $\mathcal{K}(1/u) = 0$ for $u = 0$. We compute the sum on V by applying (18) and (19) to the function f, where $f(x) = \mathrm{Tr}(x^{-1})$ so that $\mathcal{F}(f+\varphi_a) = \mathcal{K}(a)$. According to (13), with $\lambda = 1$, we have

$$\sum_{a\in V}\mathcal{K}^2(a) = 2^k \sum_{u\in V^\perp} \mathcal{F}(D_u f) \quad \big(\text{using (18)}\big)$$

$$= 2^{k+n} + 2^k \sum_{u\in V^\perp\setminus\{0\}} \left(\mathcal{K}\left(\frac{1}{u}\right) + 2(-1)^{\mathrm{Tr}(1/u)} - 2\right)$$

$$= 2^{k+n} - 2^{k+1}\big(2^{n-k}-1\big) + 2^k \sum_{u\in V^\perp} \mathcal{K}\left(\frac{1}{u}\right)$$

$$+ 2^{k+1}\left(\sum_{u\in V^\perp} (-1)^{\mathrm{Tr}(1/u)} - 1\right)$$

$$= 2^{k+n} - 2^{n+1} + 2^k \sum_{u\in V^\perp} \mathcal{K}\left(\frac{1}{u}\right) + 2^{k+1} \sum_{u\in V^\perp} (-1)^{\mathrm{Tr}(1/u)}.$$

Now we apply (19) to f:

$$\sum_{a\in V}\mathcal{K}(a) = 2^k \sum_{u\in V^\perp} (-1)^{\mathrm{Tr}(1/u)}$$

and then obtain (20). The other formulas are instances of (20) for particular V, noticing the $\{0, v\}^\perp$ is the kernel of φ_v. □

When $n = 2t$ we derive another interesting formula.

Proposition 4. *Let $n = 2t$ with $t \geqslant 2$. Consider the Kloosterman sums $\mathcal{K}(a)$ on $\mathbf{F}_{2^n}$. Then*

$$\sum_{a\in\mathbf{F}_{2^t}}\mathcal{K}^2(a) = 2^{n+t+1}.$$

There are at most 2^{t-1} elements $a \in \mathbf{F}_{2^t}$ such that $\mathcal{K}(a) = 0$.

Proof. Assume that $n = 2t$ and $V = \mathbf{F}_{2^t}$. Then $V^\perp = V$ since $\mathrm{Tr}(xy) = 0$ for all $x \in \mathbf{F}_{2^t}$ and all $y \in \mathbf{F}_{2^t}$. We apply (19) to f, where $f(x) = \mathrm{Tr}(x^{-1})$ so that $\mathcal{F}(f + \varphi_a) = \mathcal{K}(a)$:

$$\sum_{a\in\mathbf{F}_{2^t}}\mathcal{K}(a) = 2^t \sum_{u\in\mathbf{F}_{2^t}} (-1)^{\mathrm{Tr}(1/u)} = 2^n.$$

Then, noticing that $u^{-1} \in \mathbf{F}_{2^t}$ if and only if $u \in \mathbf{F}_{2^t}$, (20) becomes

$$\sum_{a\in\mathbf{F}_{2^t}}\mathcal{K}^2(a) = 2^{n+1}\big(2^{t-1}-1\big) + 2^t \sum_{u\in\mathbf{F}_{2^t}} \mathcal{K}\left(\frac{1}{u}\right) + 2\sum_{a\in\mathbf{F}_{2^t}}\mathcal{K}(a)$$

$$= 2^{n+1}\big(2^{t-1}-1\big) + \big(2^t+2\big)\sum_{a\in\mathbf{F}_{2^t}}\mathcal{K}(a)$$

$$= 2^{n+t} - 2^{n+1} + 2^n\big(2^t+2\big) = 2^{n+t+1}.$$

We know from (11) that $\mathcal{L}^2(f) = 2^{n+2}$, i.e., $\mathcal{L}(f) = 2^{t+1}$. Consequently, $2^{n+t+1} \leqslant 2^{n+2}X$ where X is the number of $a \in \mathbf{F}_{2^t}$ such that $\mathcal{K}^2(a) \neq 0$. Hence $2^{t-1} \leqslant X$, implying that there are at most 2^{t-1} elements a such that $\mathcal{K}(a) = 0$. Note that if $a \in \mathbf{F}_{2^t}$ then $\mathrm{Tr}(a) = 0$ implying that $\mathcal{K}(a)$ is divisible by 8 (Lemma 2). This does not contradict $\mathcal{K}(a) = \pm 2^{t+1}$. □

5. Conclusion

A Boolean function is said to be *good*, cryptographically speaking, when it is efficient regarding several criteria. So, such a function is generally almost good for each criterion. This concept is simply generalized to vectorial functions, by considering the properties of the component functions. The functions $f_\lambda \in \mathcal{B}_n$, which we study in this paper, are balanced, have high degree and high nonlinearity. We proved that moreover the indicators $M(f_\lambda)$ and $\nu(f_\lambda)$ are small for any λ. And this holds, as a direct consequence, for the permutation $\sigma : x \mapsto x^{-1}$ on $\mathbf{F}_{2^n}$. This kind of result seems difficult to obtain for other permutations. Such indicators are generally not known for any permutation which is neither quadratic nor almost bent.

On the other hand, Kloosterman sums appear in many problems and any new property could have interesting applications (see, for instance, the recent works [6,9]). The crucial problem is the determination of $\mathcal{K}(a)$ for specific values of a. In this paper, we propose a list of new formulas which could be useful in this context. For instance, Proposition 4 leads to this open problem:

Open problem. Let $n = 2t$ and consider the Kloosterman sums $\mathcal{K}(a)$ on $\mathbf{F}_{2^n}$. Which values takes $\mathcal{K}(a)$ for $a \in \mathbf{F}_{2^t}$?

Acknowledgments

The authors thank Anne Canteaut for helpful discussions on cryptographic criteria, and the anonymous reviewer who, by a number of comments, contributed to improving the manuscript.

References

[1] A. Canteaut, Cryptographic functions and design criteria for block ciphers, in: Progress in Cryptology, INDOCRYPT 2001, in: Lecture Notes in Comput. Sci., vol. 2247, Springer-Verlag, 2001, pp. 1–16.
[2] A. Canteaut, P. Charpin, M. Videau, Cryptanalysis of block ciphers and weight divisibility of some binary codes, in: M. Blaum, P.G. Farrell, H. van Tilborg (Eds.), Information, Coding and Mathematics, Kluwer Academic, 2002, pp. 75–97.
[3] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of $R(1, m)$, IEEE Trans. Inform. Theory 47 (4) (2001) 1494–1513.
[4] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, Propagation characteristics and correlation–immunity of highly nonlinear Boolean functions, in: Advances in Cryptology, EUROCRYPT 2000, in: Lecture Notes in Comput. Sci., vol. 1807, Springer-Verlag, Berlin, 2000, pp. 507–522.

[5] C. Carlet, P. Charpin, V.A. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Des. Codes Cryptogr. 15 (2) (1998) 125–156.
[6] P. Charpin, T. Helleseth, V.A. Zinoviev, On cosets of weight 4 of binary BCH codes with minimal distance 8 and exponential sums, Prob. Inf. Transm., in press.
[7] P. Charpin, E. Pasalic, On propagation characteristics of resilient functions, in: Selected Areas in Cryptography, SAC 2002, in: Lecture Notes in Comput. Sci., vol. 2595, Springer-Verlag, 2003, pp. 356–365.
[8] J. Daemen, V. Rijmen, AES proposal: The Rijndael block cipher, available at http://csrc.nist.gov/encryption/aes/rijndael/, 1999.
[9] H. Dobbertin, P. Felke, T. Helleseth, P. Rosendalh, Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums, IEEE Trans. Inform. Theory, in press.
[10] T. Helleseth, Some results about the crosscorrelation function between two maximal linear sequences, Discrete Math. 16 (1976) 209–232.
[11] T. Helleseth, V.A. Zinoviev, On Z_4-linear Goethals codes and Kloosterman sums, Des. Codes Cryptogr. 17 (1–3) (1999) 246–262.
[12] G. Lachaud, J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. Inform. Theory 36 (3) (1990) 686–692.
[13] S. Maitra, P. Sarkhar, Modifications of Patterson–Wiedemann functions for cryptographic applications, IEEE Trans. Inform. Theory 48 (1) (2002) 278–284.
[14] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptology, EUROCRYPT '93, in: Lecture Notes in Comput. Sci., vol. 765, Springer-Verlag, 1993, pp. 55–64.
[15] B. Preneel, W.V. Leekwijck, L.V. Linden, R. Govaerts, J. Vandewalle, Propagation characteristics of Boolean functions, in: Advances in Cryptology, EUROCRYPT '90, in: Lecture Notes in Comput. Sci., vol. 437, Springer-Verlag, 1991, pp. 155–165.
[16] A.F. Webster, S.E. Tavares, On the design of S-boxes, in: Advances in Cryptology, CRYPTO '85, in: Lecture Notes in Comput. Sci., vol. 219, Springer-Verlag, 1986, pp. 523–534.
[17] X.-M. Zhang, Y. Zheng, GAC—the criterion for global avalanche characteristics of cryptographic functions, J. Universal Comput. Sci. 1 (5) (1995) 320–337.
[18] Y. Zheng, X.-M. Zhang, Plateaued functions, in: Information and Communication Security, ICICS '99, in: Lecture Notes in Comput. Sci., vol. 1726, Springer-Verlag, 1999, pp. 224–300.