Explicit Values of the Tables DDT, BCT, FBCT, and FBDT of the Inverse, the Gold, and the Bracken-Leander Functions

Said Eddahmani[*] and Sihem Mesnager[*,**]

[*]Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, Laboratory Geometry, Analysis and Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France
[**]LTCI, Telecom Paris, Polytechnic Institute of Paris, 91120 Palaiseau, France

Abstract

In cryptography, vectorial Boolean functions are crucial for building S-boxes with good cryptographic properties. Popular vectorial functions are the inverse, the Gold, and the Bracken-Leander functions. They have been intensively studied, and various properties related to standard attacks have been investigated. Thanks to novel advances in symmetric cryptography and, more precisely, those related to boomerang cryptanalysis, this article continues to follow this momentum and further examine these functions. More specifically, we revisit and bring new results about their Difference Distribution Table (DDT), their Boomerang Connectivity Table (BCT), their Feistel Boomerang Connectivity Table (FBCT), and their Feistel Boomerang Difference Table (FBDT). For each table, we give explicit values of all entries by solving specific systems of equations over the finite (binary) field $\mathbb{F}_{2^n}$ of order 2^n and give the precise cardinalities of their corresponding sets of such values.

1 Introduction

In symmetric cryptography, vectorial Boolean functions are called *S-boxes* (substitution-boxes). Our main reference in this context is the precious book of Carlet [6]. S-boxes are fundamental parts of block ciphers and essential component of symmetric key algorithms which performs substitutions. In a block cipher, the S-box over $\mathbb{F}_{2^n}$ is usually a permutation component that plays a central role in its security. The S-box should satisfy several criteria such as resistance against differential cryptanalysis [1] and resistance against linear cryptanalysis [10]. The differential uniformity δ_F of a permutation F (used as an S-box inside a cryptosystem) measures the resistance of the block cipher against the differential cryptanalysis. The differential uniformity is defined by

$$\delta_F = \max_{a,b\in\mathbb{F}_{2^n},a\neq 0} \mathrm{DDT}_F(a,b),$$

where $\mathrm{DDT}_F(a,b)$ is the entry at $(a,b) \in (\mathbb{F}_{2^n})^2$ of the difference distribution table

$$\mathrm{DDT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n},\ F(x+a)+F(x)=b\}.$$

When F is used as an S-box inside a cryptosystem, the smaller the value δ_F is, the better F to the resistance against differential attack.

Another important cryptanalytical technique on block ciphers is the boomerang attack, introduced by Wagner [12] in 1999, which is a variant of differential cryptanalysis. It can be adapted to vectorial Boolean functions that are permutations of $\mathbb{F}_{2^n}$ and can be measured through the boomerang uniformity β_F [3] defined by

$$\beta_F = \max_{a,b\in\mathbb{F}_{2^n},ab\neq 0} \mathrm{BCT}_F(a,b),$$

where $\mathrm{BCT}_F(a,b)$ is the entry at $(a,b) \in (\mathbb{F}_{2^n})^2$ of the Boomerang Connectivity Table (BCT) [7] of F,

$$\mathrm{BCT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n},\ F^{-1}(F(x)+b)+F^{-1}(F(x+a)+b)=a\}.$$

A block cipher that is secure against a boomerang attack must have a low boomerang uniformity (ideally 2 but 4 is acceptable as well).

Some variants of the DDT and the BCT for ciphers following a Feistel construction were presented very recently by Boukerrou et al. [2]. For a vectorial Boolean function F, the variant of the BCT is called the Feistel Boomerang Connectivity Table (FBCT). Its entry at a fixed $(a,b) \in (\mathbb{F}_{2^n})^2$ is defined by

$$\mathtt{FBCT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n},\ F(x)+F(x+a)+F(x+b)+F(x+a+b)=0\}.$$

The Feistel boomerang uniformity of F is defined by

$$\beta^F(F) = \max_{a,b\in\mathbb{F}_{2^n}, ab(a+b)\neq 0} \mathtt{FBCT}_F(a,b).$$

For a vectorial Boolean function F, the variant of the DDT is the Feistel Boomerang Difference Table (FBDT). It is defined for $(a,c,b) \in (\mathbb{F}_2^n)^3$ by

$$\begin{aligned}\mathtt{FBDT}_F(a,c,b) = \#\{x \in \mathbb{F}_{2^n},\ & F(x)+F(x+a)+F(x+b)+F(x+a+b) = 0,\\ & F(x)+F(x+a) = c\}.\end{aligned}$$

In connection with the FBDT, we introduce the notion of Feistel boomerang difference uniformity γ_F of a function F as

$$\gamma_F = \max_{(a,c,b)\in\mathbb{F}_{2^n}^3, (a,c)\neq(0,0)} \mathtt{FBDT}_F(a,c,b).$$

One of the most studied power functions is the inverse function $S : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $S(x) = x^{2^n-2}$. It is used in the block cipher AES [8] and has been intensively studied. It is known that the inverse function is differentially 4-uniform when n is even, and differentially 2-uniform, that is Almost Perfect Nonlinear (APN) when n is odd [11]. Also, the BCT of the inverse function was studied by Boura and Canteaut [3]. When n is even, they showed that the possible values of the boomerang uniformity of the inverse function S are $\mathrm{BCT}_S = 4$ if $n \equiv 2 \pmod 4$, and $\mathrm{BCT}_S = 6$ if $n \equiv 0 \pmod 4$. Similarly, in [2], the FBCT of the inverse function was studied, and its Feistel boomerang uniformity was established as $\beta^F(F) = 4$ when n is even.

Another important power function is the Gold function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $G(x) = x^{2^k+1}$. It is a permutation if $\frac{n}{d}$ is odd, where $\gcd(k,n) = d$, and has also been intensively investigated. The Gold function is known to be differentially 4-uniform for n and k satisfying $\gcd(n,k) = 2$ and $n = 2m$ where m is odd. In [3], Boura and Canteaut showed that the Gold function have a boomerang uniformity equal to 4 when $n \equiv 2 \pmod 4$ and $\gcd(n,k) = 2$.

The Bracken-Leander function is defined over $\mathbb{F}_{2^n}$ by $F(x) = x^{2^{2k}+2^k+1}$ where $n = 4k$. When k is odd, and $\gcd\left(2^{4k}-1, 2^{2k}+2^k+1\right) = 1$, the function F is a permutation. In 2010, Bracken and Leander [4] showed that F has differential uniformity $\delta_F = 4$, and non-linear uniformity $\mathtt{NL}_F = 2^{n-1} - 2^{\frac{n}{2}}$. In [5], Calderini and Villa studied its boomerang uniformity and showed that it is upper bounded by 24. They performed extensive experiments for $3 \le k \le 15$ where k is odd, and found that the upper bound of $\beta_F = 24$ can be attained for certain values of k with $7 \le k \le 15$.

In this paper, we shall focus on the inverse, the Gold, and the Bracken-Leander functions over $\mathbb{F}_{2^n}$. More specifically, we accomplish the following assignment.

- For the inverse and the Gold functions, we give all explicit values of all entries in the DDT, the FBCT, and the FBDT. Also, for each entry, we give the number of couples $(a,b) \in (\mathbb{F}_{2^n})^2$ having such entry. We also show that the Feistel boomerang difference uniformity for the Gold function is $\gamma_F = 4$. For the inverse function, we show that $\gamma_F = 4$ if n is even, and $\gamma_F = 0$ if n is odd.
- For the inverse, the Gold, and the Bracken-Leander functions, we give all values of all entries in the FBCT. Moreover, we give the number of elements $(a,b) \in (\mathbb{F}_{2^n})^2$ with a possible value in the FBCT. Also, we consider the Feistel boomerang uniformity $\beta^F(F)$ and show that, for the inverse function, $\beta^F(F) = 4$ if n is even and $\beta^F(F) = 0$ if n is odd. We also show that $\beta^F(F) = 0$ for the Gold function and $\beta^F(F) = 2^k$ for the Bracken-Leander function with $n = 4k$.

Our study of the exact entries and the cardinalities in each table is aimed to facilitate the analysis of differential and boomerang cryptanalysis of S-boxes when studying distinguishers and trails.

2 The DDT of the inverse function

The entries of the DDT of the inverse function form the set $\{0, 2, 2^n\}$ if n is odd, and the set $\{0, 4, 2^n\}$ if n is even. Depending on the structure of each fixed $(a,b) \in (\mathbb{F}_{2^n})^2$, we give the explicit value of $\mathtt{DDT}_S(a,b)$. Moreover, we give the number of couples (a,b) having a prescribed value in the DDT. For all n, we have $\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{DDT}_S(a,b) = 2^n\right\} = 1$. For an even integer n, we have

$$\begin{aligned}\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{DDT}_S(a,b) = 4\right\} &= 2^n - 1,\\ \#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{DDT}_S(a,b) = 2\right\} &= \left(2^{n-1}-2\right)\left(2^n-1\right),\\ \#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{DDT}_S(a,b) = 0\right\} &= \left(2^{n-1}+2\right)\left(2^n-1\right),\end{aligned}$$

and, for an odd integer n, we have

$$\#\left\{(a,b)\in\mathbb{F}_{2^n}^2 : \mathtt{DDT}_S(a,b)=2\right\} = 2^{n-1}\left(2^n-1\right),$$
$$\#\left\{(a,b)\in\mathbb{F}_{2^n}^2 : \mathtt{DDT}_S(a,b)=0\right\} = \left(2^{n-1}+1\right)\left(2^n-1\right).$$

3 The DDT of the Gold Function

For the Gold function defined over $\mathbb{F}_{2^n}$ by $G(x)=x^{2^k+1}$, we prove the following result when $d=\gcd(k,n)$, and $m=\frac{n}{d}$,

$$\mathtt{DDT}_G(a,b)=\begin{cases}2^n & \text{if } a=0 \text{ and } b=0,\\ 2^d & \text{if } a\neq 0, \text{ and } \mathrm{Tr}_d^n\left(\frac{b}{a^{2^k+1}}\right)=m \pmod 2,\\ 0 & \text{if } a=0 \text{ and } b\neq 0, \text{ or } a\neq 0 \text{ and } \mathrm{Tr}_d^n\left(\frac{b}{a^{2^k+1}}\right)\neq m \pmod 2.\end{cases}$$

For each $\delta\in\left\{0,2^d,2^n\right\}$, we give the number of couples $(a,b)\in\left(\mathbb{F}_{2^n}\right)^2$ such that $\mathrm{DDT}_G(a,b)=\delta$,

$$\#\left\{(a,b)\in\mathbb{F}_{2^n}^2 : \mathtt{DDT}_G(a,b)=2^n\right\}=1,$$
$$\#\left\{(a,b)\in\mathbb{F}_{2^n}^2 : \mathtt{DDT}_G(a,b)=2^d\right\}=2^{n-d}\left(2^n-1\right),$$
$$\#\left\{(a,b)\in\mathbb{F}_{2^n}^2 : \mathtt{DDT}_G(a,b)=0\right\}=\left(2^n-1\right)\left(2^n-2^{n-d}+1\right).$$

4 The BCT of the Inverse Function

The values of the BCT of the inverse function S form the set $\{0,2,4,6,2^n\}$ if $n\equiv 0 \pmod 4$, the set $\{0,2,4,2^n\}$ if $n\equiv 2 \pmod 4$, and the set $\{0,2,2^n\}$ if n is odd. We give the explicit value of all entries of the BCT, as well as the number of couples (u,v) having the same BCT. Specifically, we show that $\#\left\{(u,v)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_S(u,v)=2^n\right\}=2^{n+1}-1$, and when n is odd, we have

$$\#\left\{(u,v)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_S(u,v)=2\right\}=2^{n-1}\left(2^n-1\right),$$
$$\#\left\{(u,v)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_S(u,v)=0\right\}=\left(2^{n-1}-1\right)\left(2^n-1\right).$$

Similarly, when n is even, we have.

$$\#\left\{(u,v)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_S(u,v)=6\right\}=\begin{cases}2^{n+1}-2 & \text{if } n=4m,\\ 0 & \text{if } n=4m+2,\end{cases}$$

$$\#\left\{(u,v)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_S(u,v)=4\right\}=\begin{cases}2^n-1 & \text{if } n=4m,\\ 3\left(2^n-1\right) & \text{if } n=4m+2,\end{cases}$$

$$\#\left\{(u,v)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_S(u,v)=2\right\}=\begin{cases}\left(2^n-1\right)\left(2^{n-1}-4\right) & \text{if } n=4m,\\ \left(2^{n-1}-2\right)\left(2^n-1\right) & \text{if } n=4m+2.\end{cases}$$

$$\#\left\{(u,v)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_S(u,v)=0\right\}=\begin{cases}2^{n-1}\left(2^n-1\right) & \text{if } n=4m,\\ \left(2^n-1\right)\left(2^{n-1}-2\right) & \text{if } n=4m+2.\end{cases}$$

5 The BCT of the Gold Function

Recall that the Gold function is defined over on $\mathbb{F}_{2^n}$ by $G(x)=x^{2^k+1}$. When G is a permutation of $\mathbb{F}_{2^n}$, that is when $m=\frac{n}{d}$ is odd where $d=\gcd(k,n)$, we give all entries of the BCT of G at $(a,b)\in\left(\mathbb{F}_{2^n}\right)^2$,

$$\mathtt{BCT}_G(a,b)=\begin{cases}2^n & \text{if } a=0 \text{ or } b=0,\\ 2^d & \text{if } a\neq 0 \text{ and } \mathrm{Tr}_d^n\left(\dfrac{b}{a^{2^k+1}}\right)\neq 0,\\ 0 & \text{if } a\neq 0 \text{ and } \mathrm{Tr}_d^n\left(\dfrac{b}{a^{2^k+1}}\right)=0,\end{cases}$$

where $\mathrm{Tr}_d^n(x)=\sum_{i=0}^{\frac{n}{d}-1}x^{2^{ir}}$. For each admissible value $\beta\in\left\{0,2^d,2^n\right\}$ of the BCT of the Gold function, we give the explicit number of couples $(a,b)\in\left(\mathbb{F}_{2^n}\right)^2$ such that $\mathrm{BCT}_G(a,b)=\beta$,

$$\#\left\{(a,b)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_G(a,b)=2^n\right\}=2^{n+1}-1,$$
$$\#\left\{(a,b)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_G(a,b)=2^d\right\}=2^{n-d}\left(2^d-1\right)\left(2^n-1\right),$$
$$\#\left\{(a,b)\in\mathbb{F}_{2^n}^2 : \mathtt{BCT}_G(a,b)=0\right\}=\left(2^n-1\right)\left(2^{n-d}-1\right).$$

6 The FBCT of the Inverse Function

We present a detailed study of the FBCT of the inverse function over the finite field $\mathbb{F}_{2^n}$. Our results are obtained by direct calculation, while the results in [2] are obtained by considering the DDT. We show that the set of the FBCT values is $\{0, 4, 2^n\}$ when n is even, and $\{0, 2^n\}$ when n is odd. When n is even, we have

$$\begin{aligned}
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 2^n\right\} = 3 \times 2^n - 2,\\
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 4\right\} = 2\left(2^n - 1\right),\\
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 0\right\} = \left(2^n - 4\right)\left(2^n - 1\right).
\end{aligned}$$

Similarly, when n is odd, we have

$$\begin{aligned}
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 2^n\right\} = 3 \times 2^n - 2,\\
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 0\right\} = \left(2^n - 2\right)\left(2^n - 1\right).
\end{aligned}$$

Consequently, the Feistel boomerang uniformity of the inverse function is $\beta^F(F) = 4$ if n is even, and $\beta^F(F) = 0$ if n is odd.

7 The FBCT of the Gold Function

For the Gold function defined over $\mathbb{F}_{2^n}$ by $G(x) = x^{2^k+1}$, we show that its FBCT is very simple, explicitly,

$$\mathtt{FBCT}_G(a,b) = \begin{cases} 2^n & \text{if } b = 0 \text{ or } a \in b \cdot \mathbb{F}_{2^d},\\ 0 & \text{if } a \notin b \cdot \mathbb{F}_{2^d}. \end{cases}$$

We also give the explicit cardinalities of the sets of FBCT with the same entry,

$$\begin{aligned}
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 2^n\right\} = 2^{n+d} + 2^n - 2^d,\\
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 0\right\} = \left(2^n - 1\right)\left(2^n - 2^d\right).
\end{aligned}$$

The former result shows that the Feistel boomerang uniformity of the Gold function is $\beta^F(F) = 0$.

8 The FBCT of the Bracken-Leander Function

Recall that the Bracken-Leander function over $\mathbb{F}_{2^n}$ for $n = 4k$ is defined by $F(x) = x^{2^{2k}+2^k+1}$. We show how to compute all explicit values of its FBCT,

$$\mathtt{FBCT}_F(a,b) = \begin{cases} 2^n & \text{if } ab(a+b) = 0,\\ 2^{2k} & \text{if } \dfrac{a}{b} \in \mathbb{F}_{2^{2k}} \backslash \mathbb{F}_{2^k},\\ 0 & \text{if } \dfrac{a}{b} \in \mathbb{F}_{2^k} \backslash \{0,1\}, \text{ or if } \dfrac{a}{b} \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^{2k}}. \end{cases}$$

Moreover, we give the number of couples $(a,b) \in \mathbb{F}_{2^n}$ having a prescribed entry in the FBCT,

$$\begin{aligned}
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 2^n\right\} = 3 \times 2^n - 2,\\
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 2^{2k}\right\} = 2^k\left(2^k - 1\right)\left(2^n - 1\right),\\
&\#\left\{(a,b) \in \mathbb{F}_{2^n}^2 : \mathtt{FBCT}_F(a,b) = 0\right\} = \left(2^n - 1\right)\left(2^n - 2^{2k} + 2^k - 2\right).
\end{aligned}$$

The former result shows that the Feistel boomerang uniformity is $\beta^F(F) = 2^k$.

9 The FBDT of the Inverse Function

For the inverse function, we show that the set of the possible values of the entries of the FBDT is $\{0, 2, 4, 2^n\}$. Also, we have $\#\left\{(a,c,b) \in \mathbb{F}_{2^n}^3 : \mathtt{FBDT}_S(a,c,b) = 2^n\right\} = 2^n$, and when n is even, we have

$$\begin{aligned}
&\#\left\{(a,c,b) \in \mathbb{F}_{2^n}^3 : \mathtt{FBDT}_S(a,c,b) = 4\right\} = 4\left(2^n - 1\right),\\
&\#\left\{(a,c,b) \in \mathbb{F}_{2^n}^3 : \mathtt{FBDT}_S(a,c,b) = 2\right\} = 2\left(2^{n-1} - 2\right)\left(2^n - 1\right),\\
&\#\left\{(a,c,b) \in \mathbb{F}_{2^n}^3 : \mathtt{FBDT}_S(a,c,b) = 0\right\} = 2^{2n}\left(2^n - 1\right).
\end{aligned}$$

Similarly, when n is odd, we have

$$\#\left\{(a,c,b)\in\mathbb{F}_{2^n}^3 : \texttt{FBDT}_S(a,c,b)=2\right\} = 2^{2n}\left(2^n-1\right),$$
$$\#\left\{(a,c,b)\in\mathbb{F}_{2^n}^3 : \texttt{FBDT}_S(a,c,b)=0\right\} = 2^{n}\left(2^n-1\right).$$

We notice that the Feistel boomerang difference uniformity is $\gamma_S = 4$ if n is even and $\gamma_S = 2$ if n is odd.

10 The FBDT of Gold Function

For the Gold function defined by $G(x) = x^{2^k+1}$ with $d = \gcd(n,k)$, we show that the FBDT satisfies

$$\texttt{FBDT}_F(a,c,b) = \begin{cases} 2^n & \text{if } a=0, c=0, \\ 2^d & \text{if } a\neq 0, b\in a\cdot\mathbb{F}_{2^d}, \mathrm{Tr}_d^n\left(\frac{c}{a^{2^k+1}}\right) = m \pmod 2, \\ 0 & \text{if } a=0, c\neq 0, \text{ or } a\neq 0, b\neq 0, a\notin b\cdot\mathbb{F}_{2^d}, \\ & \text{or } \mathrm{Tr}_d^n\left(\frac{c}{a^{2^k+1}}\right) \neq m \pmod 2. \end{cases}$$

Moreover, for $\delta\in\left\{0,2^d,2^n\right\}$, we show that the number of elements $(a,c,b)\in\left(\mathbb{F}_2^n\right)^3$ such that $\texttt{FBDT}_F(a,c,b) = \delta$ is as follows

$$\#\left\{(a,c,b)\in\mathbb{F}_{2^n}^3,\ \texttt{FBDT}_F(a,c,b)=2^n\right\} = 2^n,$$
$$\#\left\{(a,c,b)\in\mathbb{F}_{2^n}^3,\ \texttt{FBDT}_F(a,c,b)=2^d\right\} = 2^n\left(2^n-1\right),$$
$$\#\left\{(a,c,b)\in\mathbb{F}_{2^n}^3,\ \texttt{FBDT}_F(a,c,b)=0\right\} = 2^{2n}\left(2^n-1\right).$$

The former result shows that the Feistel boomerang difference uniformity for the Gold function is $\gamma_S = 2^d$.

References

[1] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, vol.4, no.1, pp.3-72, 1991.

[2] H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal and M. Minier., *On the Feistel Counterpart of the Boomerang Connectivity Table: Introduction and Analysis of the FBCT*, IACR Transactions on Symmetric Cryptology, Ruhr-University Bochum, 020, Issue 1, pp. 331-362, 2020.

[3] C. Boura and A. Canteaut., *On the Boomerang Uniformity of Cryptographic S-boxes.* IACR Transactions on Symmetric Cryptology, Ruhr Universität Bochum, 2018 (3), pp. 290–310, 2018.

[4] Bracken C., Leander G.: *A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree,* Finite Fields Appl. 16, pp. 231-242, 2010.

[5] M. Calderini, I. Villa, *On the boomerang uniformity of some permutation polynomials,* Cryptography and Communications (2020) 12: pp. 1161–1178

[6] C. Carlet., *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge, 2021.

[7] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song., *Boomerang Connectivity Table: A New Cryptanalysis Tool.* In Jesper Buus Nielsen and Vincent Rijmen, editors, Advances in Cryptology - EUROCRYPT 2018 -Proceedings, Part II, volume 10821 of Lecture Notes in Computer Science, pp. 683-714. Springer, 2018.

[8] J. Daemen and V. Rijmen., *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer, Heidelberg, 2002.

[9] R. Gold., *Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.)*, IEEE Transactions on Information Theory, vol.14, issue.1, pp. 154-156, 1968.

[10] M. Matsui., *Linear Cryptanalysis method for DES cipher*, Advances in Cryptology-EUROCRYPT'93, Springer-Verlag, Berlin, pp.386-397, 1994.

[11] K. Nyberg., *Differentially uniform mappings for cryptography.* In: Helleseth T. (eds) Advances in Cryptology - EUROCRYPT'93. Lecture Notes in Computer Science, vol 765. pp. 55-64, Springer, Berlin, Heidelberg, 1994.

[12] D. Wagner., *The Boomerang Attack.* In Lars R. Knudsen, editor, Fast Software Encryption, volume 1636 of Lecture Notes in Computer Science, pp. 156-170, Springer, 1999.