

More than two decades of attacks on the AES cryptosystem

Said Eddahmani

Department of Mathematics

Laboratory Geometry Analysis and Applications

University of Paris VIII

F-93526 Saint-Denis

France

and

University Sorbonne Paris Nord

CNRS, UMR 7539, F-93430

Villetaneuse

France

Abstract

In 2001, the National Institute for Standards and Technology (NIST) chose AES to secure sensitive information. Since then, AES has become the most widely used symmetric cryptosystem and has been intensively studied for vulnerabilities. In this survey, we celebrate twenty years of the AES by presenting an overview of cryptographers' work on it. We describe the main cryptanalytic techniques on AES, including linear cryptanalysis, differential cryptanalysis, boomerang cryptanalysis, differential-linear cryptanalysis cryptanalysis, and many other techniques of cryptanalysis.

Subject Classification: 94A60.

Keywords: Symmetric cryptography, AES cryptosystem, Cryptanalysis, Substitution boxes, Vectorial boolean function.

1. Introduction

The Advanced Encryption Standard (AES) [40], designed by Joan Daemen and Vincent Rijmen, was adopted by the National Institute of Standards and Technology (NIST) to secure classified digital government documents in 2001. Since then, AES has become a prominent symmetric

E-mail: said.eddahmani@etud.univ-paris8.fr

encryption algorithm to secure sensitive data and transactions. Meanwhile, many attacks have been developed to challenge the security of AES. An attack's efficiency is measured by comparing its complexity to the complexity of the brute force attack.

AES is a block cipher based on the substitution-permutation network (SPN) technique in which vectorial Boolean functions are intensively deployed. In symmetric cryptography, differential cryptanalysis [6] and linear cryptanalysis [35] are the two major techniques to attack a block cipher. Various criteria are used to measure the resistance of a block cipher when the S-Box is derived from a vectorial Boolean function. In general, the criteria are based on linear cryptanalysis [34], differential cryptanalysis [6], boomerang cryptanalysis [45], or some of their variants [29, 4]

AES has been designed to guarantee good resistance against both differential and linear cryptanalysis, and it is also resistant to all other known techniques of cryptanalysis. Its resistance is mainly guaranteed by the algebraic structure of its S-Box and by internal algorithms such as the MixColumns matrix and key schedule. There are no efficient differential or linear weaknesses for more than five rounds in AES, making it as one of the most secure cryptosystems in use today. Moreover, AES is believed to be resistant to quantum computers [11] and will remain secure in a post-quantum world.

2. Attacks on AES

Three complexities are used to test efficiency of an attack on a block cipher: time, data, and memory. The time complexity measures the time needed to perform the attack, the data complexity measures the amount of plaintexts-ciphertexts performed during the attack, while the memory complexity measures the quantity of storage needed to process the attack. In general, the efficiency of the attack is dominated by the time complexity. It is always compared to the time complexity of the direct attack, known as brute force.

- **Brute force attack.** It consists of decrypting a message by trying all the possible keys until the correct key is found. For AES-128, the time complexity of a brute force attack is 2^{128} . This makes brute force attacks not feasible, and consequently only theoretical.
- **Square attack.** One of the first attacks on AES was the Square attack, an attack presented by the designers of AES [18]. The square attack enables to break six rounds of AES-128 and has a complexity of

2^{48} . The first attack on AES-128 up to 7 rounds is a square attack presented in [24] which uses $2^{128} - 2^{119}$ chosen plaintexts and 2^{120} encryptions.

- **Differential attack and its variants.** The differential cryptanalysis was presented by Biham and Shamir [5] in 1991 to attack DES [44]. It exploits the possible relationships between the input and the output data to find the subkeys related to the first or the last rounds. Since then, several variants of the differential attack have been proposed, such as the rectangle attack [7], the impossible differential attack [5], the truncated differential attack [30], the differential-linear attack [31], and the boomerang attack [45].
- **Linear attack.** The linear cryptanalysis was presented by Matsui [35] in 1993 to attack DES [44]. It uses the principles of finding significant probability occurrences of linear expressions relating the inputs and the outputs of any function.
- **Boomerang attack.** It is related to the differential cryptanalysis. It was introduced by Wagner [45] in 1999 and operated on quartets of data (P, P') and (Q, Q') with fixed differences, that is $P + P' = \delta$, and $Q + Q' = \Delta$ are fixed.
- **Impossible differential attack.** The impossible differential attack is another variant of differential attack that was presented by Biham, Biryukov, and Shamir [5] in 1999. It exploits differentials that never occur and have the probability of zero.
- **Side Channel attacks.** They are use various physical channels or electronic devices that may leak information about the processed data. Typically, side channel attacks exploits measurements of the running time, the amount of consumption, or the electromagnetic emissions during the implementation process rather than the algorithm itself. In [41, 1, 3], side channel attacks has been applied to successfully recover the secret key from a device running AES. To protect AES against attacks by side channels, various solutions have been studied, mainly in the implementation technique.
- **Quantum attacks.** In a post quantum world, Grover's algorithm [27] can be applied to attack symmetric primitives with small keys. Indeed, Grover's algorithm can perform a quantum search in a time which is the square root of the time of a non-quantum search. As a consequence, the actual recommendation for AES with a guaranteed post-quantum security is the version of AES-256 [11].

In addition to the former attacks, various cryptanalysis techniques on AES have been deployed such as partial-sum [24] attack, meet in the middle attack, bicliques attack [10], collision attack [25], and truncated differentials attack [30]. More attacks, tables and details can be found in [20, 27, 33, 11, 9, 21, 19].

3. Description of AES

The arithmetic of the AES algorithm is designed over the finite field $\mathbb{F}_{2^8}$. Each element of $\mathbb{F}_{2^8}$ or byte is presented as a list $b_7b_6 \dots b_1b_0$ of bits, which can be identified with a polynomial of the form $b_7x^7 + b_6x^6 + \dots + b_1x + b_0$. The multiplication and the inversion operations are performed in the finite field $\mathbb{F}_{2^8}$ with the polynomial $x^8 + x^4 + x^3 + x + 1$, with the convention that the inverse of 0 is 0.

The AES algorithm is designed to encrypt and to decrypt data blocs of size 128 bits by applying keys of size 128, 192, or 256 bits. Each block of 128 bits is structured as a byte string $B_0B_1 \dots B_{15}$ and is formulated as a matrix, known as the state matrix, of size 4×4 , which is numbered as follows

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

The encryption in AES uses 10 rounds of algorithms for keys of 128 bits, 12 rounds for keys of 192 bits, and 14 rounds for keys of 256 bits. All the rounds are composed of four algorithms, except the last one. The four algorithms are called SubBytes, ShiftRows, MixColumns, and AddRoundKey.

- SubBytes: This is a substitution function, and consists on applying the S-Box on the bytes. The S-Box is an 8×8 matrix. It is applied to the bytes of the state which operates on F_{2^8} by the mapping

$$S(x) = F(x^{-1}) + a,$$

where $0^{-1} = 0$, $a = (0, 1, 1, 0, 0, 0, 1, 1)^{\text{tr}}$ and F is the function defined by its matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- **ShiftRows:** it is a row-wise permutation step which consists in cyclically shifting the row number j , $j=0,1,2,3$, by j bytes to the left. More precisely, it proceeds as follows
 1. the first row of the state array is $j=0$, and remains unchanged,
 2. the next row is $j=1$ and is cyclically shifted by one byte,
 3. the third row is $j=2$ and is cyclically shifted by two bytes,
 4. the fourth row is $j=3$ and is cyclically shifted by three bytes.
- **MixColumns:** it consists in multiplying each column by the matrix

$$MC = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}.$$

The coefficients of the matrix MC used by MixColumns have been chosen to ensure a maximum distance separable (MDS) property, which guarantees the maximal possible diffusion between the input and the output [40].

- **AddRoundKey:** it is an operation that xors the state and the round subkey.

An algorithm AddRoundKey is performed at the beginning of the first round, while an algorithm MixColumns is not performed in the last round. The whole process of the AES algorithm can be described by Algorithm 1.

Algorithm 1: The AES-128 encryption algorithm.

Input: A plaintext block P of length 128 bits, and a key K of length $n \in \{128, 192, 256\}$ bits.

Output: The ciphertext block C with length 128 bits.

1. $r \leftarrow 6 + \frac{n}{32}$
 2. $C \leftarrow \text{AddRoundKey}(P, K)$
 3. **for** $i = 1$ to r **do**
 4. $C \leftarrow \text{SubBytes}(C)$
 5. $C \leftarrow \text{ShiftRows}(C)$
 6. **if** $i \leq r - 1$ **then**
 7. $C \leftarrow \text{MixColumns}(C)$
 8. **end if**
 9. $C \leftarrow \text{AddRoundKey}(C, K)$
 10. **end for**
 11. Return C .
-

4. Boolean and vectorial (Boolean) functions

Let n and m be two positive integers. Vectorial Boolean functions are functions from the finite field $\mathbb{F}_{2^n}$ to the finite field $\mathbb{F}_{2^m}$. They are intensively used to design cryptographical block ciphers, especially for creating substitution-boxes or S-boxes. This section presents a list of basic definitions related to Boolean functions. An excellent book on Boolean and vectorial functions for symmetric cryptography is [16].

For a positive integer n , $\mathbb{F}_{2^n}$ denotes the finite field of 2^n elements and $\mathbb{F}_2^n$ denotes the n -dimensional vector space over $\mathbb{F}_2$.

Definition 1: For a positive integer n , a Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is a mapping that satisfies

$$f(x) = g(x_1, x_2, \dots, x_n).$$

Definition 2: For two positive integers n and m , an (n, m) - vectorial Boolean function is a mapping $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ satisfying

$$F(x) = F(x_1, x_2, \dots, x_n) = (f_1(x), f_2(x), \dots, f_m(x)),$$

where each f_i , $1 \leq i \leq m$, is a Boolean function.

5. Linear Cryptanalysis

Linear cryptanalysis of symmetric ciphers was introduced in 1994 by Matsui [35] to attack DES. Linear cryptanalysis exploits approximate

linear relationships that exist between inputs and outputs. The goal is to find a valid relationship more significant than usual, and this will constitute a linear approximation that can be employed to find some bits of the key. The Walsh transform [15, 2] of the round function of any cipher is then involved in measuring its resistance against linear attacks.

Definition 3: For a positive integer n , let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a Boolean function. The Walsh transform W_f of f is a function $W_f : \mathbb{F}_2^n \rightarrow \mathbb{Z}$, and is defined by

$$W_f(x) = \sum_{u \in \mathbb{F}_2^n} (-1)^{x \cdot u + f(u)},$$

where $x \cdot u$ is the inner product of x and u on $\mathbb{F}_2^n$, and is defined by $x \cdot u = \sum_{i=1}^n x_i u_i$.

The Walsh transform has various properties such as Parseval's relation.

Proposition 1: For a positive integer n , let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a Boolean function. The Walsh transform W_f of f satisfies

$$\sum_{x \in \mathbb{F}_2^n} W_f(x)^2 = 2^{2n}.$$

The notion of Walsh transform for (n, m) -vectorial Boolean functions depends on linear approximations.

Definition 4: Let F be an (n, m) -vectorial Boolean function. For $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, a linear approximation of F with the masks u and v is the following relation

$$u \cdot x = v \cdot F(x), \text{ for } x \in \mathbb{F}_2^n.$$

For (n, m) -vectorial Boolean functions, the following definition extends the notion of Walsh transform.

Definition 5: For positive integers m and n , let F be a (n, m) -Boolean function. The Walsh transform W_F of F is a function $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^{m*} \rightarrow \mathbb{Z}$, and is defined by

$$W_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot F(x)}.$$

There is also a Parseval relation for Walsh transform.

Proposition 2: For positive integers m and n , let F be an (n, m) -vectorial Boolean function. For every $v \in \mathbb{F}_2^m$, the Walsh transform W_F of F satisfies

$$\sum_{u \in \mathbb{F}_2^n} (W_F(u, v))^2 = 2^{2^n}.$$

To each (n, m) -vectorial Boolean function F corresponds a specific table LAT_F , called the linear approximation table. It is a $2^n \times 2^m$ table, where the entry at $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ is

$$LAT_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot F(x)}, u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m.$$

For a Boolean function $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, the maximum of $|W_f(x)|$ for all $x \in \mathbb{F}_2^n$ is related the linearity and to the non-linearity of f . It serves to measure the distance between the Boolean function f and the set composed by the linear functions.

Definition 6: For a positive integer n , let $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a Boolean function. The linearity of f is denoted $\mathcal{L}(f)$, and is defined by

$$\mathcal{L}(f) = \max_{x \in \mathbb{F}_2^n} |W_f(x)|.$$

The non-linearity of f is denoted $\mathcal{NL}(f)$ and satisfies

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{x \in \mathbb{F}_2^n} |W_f(x)|.$$

Applying the Parseval relation, the non-linearity of a Boolean function satisfies the following result [15].

Lemma 1: For a positive integer n , let $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a Boolean function. The non-linearity of f is upper bounded as follows

$$\mathcal{NL}(f) \leq \begin{cases} 2^{n-1} - 2^{\frac{n-1}{2}} & \text{if } n \text{ is odd,} \\ 2^{n-1} - 2^{\frac{n}{2}-1} & \text{if } n \text{ is even.} \end{cases}$$

Boolean functions satisfying $\mathcal{NL}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ are called *Bent functions* [36, 17, 46].

A generalization of the notion of non-linearity to (n, m) -Boolean functions was introduced by Nyberg [37]. It corresponds to the minimum non-linearity of all partial functions $F_v: \mathbb{F}_2^n \rightarrow \mathbb{Z}$ defined for all $v \in \mathbb{F}_2^m$ with $v \neq 0$ by $F_v(x) = v \cdot F(x)$.

Definition 7: For positive m and n , let F be an (n, m) -vectorial Boolean function. The linearity of F is defined by

$$\mathcal{L}(F) = \max_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m, v \neq 0} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot F(x)} \right|,$$

and its non-linearity is defined by

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m, v \neq 0} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot F(x)} \right|.$$

Example 1: For AES, the linearity and the non-linearity of the S box are

$$\mathcal{L}(S) = 32, \quad \mathcal{NL}(S) = 2^7 - \frac{32}{2} = 112.$$

6. Differential Cryptanalysis

Differential attacks are statistical chosen plaintext attacks introduced in 1990 by Biham and Shamir [6] for the cryptanalysis of DES. The differential cryptanalysis studies the evolution of the differences from round to round in a cipher with relatively high probability. More specifically, it considers pairs composed by inputs having a fixed difference and analyzes the difference of the outputs that can be used to find some parts of the secret key.

Definition 8: For a positive integer n , let $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a vectorial Boolean function. A differential (δ, Δ) is any couple where δ is a fixed difference of two inputs, and Δ is the difference of the correspondent outputs such that there exist a pair $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ satisfying the system of equations

$$x + y = \delta, S(x) + S(y) = \Delta.$$

A set $E(\delta, \Delta)$ can then be defined in connection with any differential (δ, Δ) .

Definition 9: Let (δ, Δ) be a differential of a vectorial Boolean function S . The set of pairs satisfying (δ, Δ) is

$$E(\delta, \Delta) = \{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n, x + y = \delta, S(x) + S(y) = \Delta\}.$$

The differential is called impossible if $\#E(\delta, \Delta) = 0$ and possible if $\#E(\delta, \Delta) \neq 0$.

To resist differential attacks, a Boolean function should possess relatively small values of $E(\delta, \Delta)$.

If m and n are small enough, it is useful to build and store a table, called differential distribution table, or DDT for short.

Definition 10: The differential distribution table (DDT) of a vectorial Boolean function $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is a $2^n \times 2^m$ table where the entry at $(\delta, \Delta) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ is defined by

$$\text{DDT}(\delta, \Delta) = \#\{x \in \mathbb{F}_2^n, S(x) + S(\delta + x) = \Delta\}.$$

Example 2: For AES, the DDT is an $2^8 \times 2^8$ table. For all $\delta, \Delta \in \mathbb{F}_2^8$, we have $\text{DDT}(\delta, \Delta) \in \{0, 2, 4, 256\}$. The distribution of the values is presented in Table 1.

Table 1
Distribution of DDT for AES

$\text{DDT}(\delta, \Delta)$	0	2	4	256
$\#\{\delta, \Delta\}$	33150	32130	255	1

The maximum in the DDT plays an important role in differential cryptanalysis and is called *differential uniformity* [37].

Definition 11: Let $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be a vectorial Boolean function. The differential uniformity of S is defined by

$$\text{DU}(S) = \max_{(\delta, \Delta) \in \mathbb{F}_2^n \times \mathbb{F}_2^m, \delta \neq 0} \text{DDT}(\delta, \Delta).$$

Example 3: Using Table 1, we see that the S-Box of AES has differential uniformity $\text{DU}(\text{AES}) = 4$.

An important family of vectorial Boolean functions is the family of *almost perfect nonlinear (APN) functions* [28]. They are vectorial Boolean functions with differential uniformity 2. They have been proposed for designing ciphers resistant against differential cryptanalysis [38, 39].

7. Differential-Linear Cryptanalysis

In 1994, Langford and Hellman [31] showed that by combining differential and linear cryptanalysis, one could mount a new attack on block ciphers, called *differential-linear cryptanalysis*.

If E is a block cipher, the differential-linear cryptanalysis splits E into two parts F_0 and F_1 so that $E = F_1 \circ F_0$. In the original work [31], the part F_0 is based on a truncated differential $\alpha_0 \rightarrow \beta_0$ with probability $p = 1$,

and the part F_1 , is based on a linear approximation $\lambda_l \rightarrow \lambda_o$ that predicts $\lambda_l \cdot P = \lambda_o \cdot F_1(P)$ with bias ε , that is with probability $\frac{1}{2} + \varepsilon$. In 2002, Biham et al. [8] extended this technique to differentials for F_1 with probability $p < 1$. The differential-linear cryptanalysis was applied to 8-round DES in [31], to the 7-round and 9-round reduced versions of DES in [8], the COCONUT98 in [8], the 10 round of the CTC2 block cipher in [33], and the 32-round SHACAL-2 in [42].

8. Boomerang Cryptanalysis

Introduced in 1999 by Wagner [45], the boomerang attack is an adaptive chosen plaintext attack based on differential cryptanalysis. It can be applied to study the differential behaviour of certain parts of the cipher when a high-probability trail for the entire cipher is challenging to find.

The starting point of a boomerang attack when applied to a cipher E is to compose E as $E = F_1 \circ F_0$ with two sub-ciphers F_0 and F_1 . If there exists a differential characteristics (α_0, β_0) for F_0 , with probability p_0 and if there exists a differential characteristics (α_1, β_1) for F_1 with probability p_1 , then it E can be distinguished from a random permutation. The method is optimised when $p_0 p_1$ is much larger than 2^{-k} where k is the length of the blocks in the underlying cipher.

When a cipher is represented by its S-Box, a convenient way to evaluate its resistance to the boomerang attack is to consider the *Boomerang Connectivity Table*, introduced by Cid et al. [14] (see also [13, 32]).

Definition 12: For a positive integer n , let $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation, and S^{-1} the inverse permutation of S . The boomerang connectivity table, or BCT for short, is a table of dimension $2^n \times 2^n$, where the entry at $(a_0, a_1) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ is

$$\text{BCT}_S(a_0, a_1) = \#\{x \in \mathbb{F}_2^n, S^{-1}(S(x) + a_1) + S^{-1}(S(x + a_0) + a_1) = a_0\}.$$

Example 4: In AES, for all $a_0, a_1 \in \mathbb{F}_2^n$, we have $\text{BCT}_S(a_0, a_1) \in \{0, 2, 4, 6, 256\}$. The frequencies are listed in Table 2.

Table 2
Distribution of BCT values for AES

$\text{BCT}_S(a_0, a_1)$	0	2	4	6	256
$\#\{(a_0, a_1)\}$	32640	31620	255	510	511

The non-trivial maximum of the BCT table is called the *boomerang uniformity*.

Definition 13: For a positive integer n , let $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation. The boomerang uniformity of S is defined by

$$BU(S) = \max_{\substack{(a_0, a_1) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \\ a_0, a_1 \neq 0}} BCT_S(a_0, a_1).$$

The boomerang uniformity is used to measure the resistance of a block cipher to the boomerang attacks.

Example 5: For AES, the boomerang uniformity is $BU(AES) = 6$ as it appears in Table 2.

An interesting property property relates the tables BCT_S and $BCT_{S^{-1}}$.

Proposition 3: [12] For a positive integer n , let $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation, and S^{-1} the inverse permutation of S . Then BCT_S and $BCT_{S^{-1}}$ satisfy

$$BCT_{S^{-1}}(a_0, a_1) = BCT_S(a_1, a_0) \text{ for all } a_0, a_1 \in \mathbb{F}_2^n.$$

Other properties and applications of boomerang attacks and BCTs can be found in [14, 12, 43, 22, 26].

9. Differential-Linear Connectivity Table of Vectorial Boolean Functions

In 2018, Kim et al. [29] and at Eurocrypt'19, Bar-On et al. [4] introduced a new tool, called the differential-linear connectivity table (DLCT) to improve the differential-linear attacks.

Definition 14: Let $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be a (n, m) -vectorial Boolean function. The differential-linear connectivity table, or DLCT for short of S is an $2^n \times 2^m$ table whose entry at row a and column b is

$$DLCT_S(a, b) = \#\{x \in \mathbb{F}_2^n : b \cdot S(x) = b \cdot S(x + a)\} - 2^{n-1},$$

where a is the difference and b is the mask.

Example 6: In AES, the DLCT is a $2^8 \times 2^8$ table where the entries are composed by elements in $\{-16, -12, -8, -4, 0, 4, 8, 12, 16, 128\}$. The frequencies of DLCT table are listed in Table 3.

Table 3
Distribution of DLCT values for AES

$\text{DLCT}_S(u, u)$	-16	-12	-8	04	0	4	8	12	16	128
$\#\{(u, v)\}$	2040	6120	10710	12240	8160	9180	8160	7140	1275	511

The non-trivial maximum of the values $|\text{DLCT}_S(u, v)|$ is called the *differential-linear uniformity* of the Boolean function S .

Definition 15: For positive integers m and n , let $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be an (n, m) -vectorial Boolean function. The differential-linear uniformity of S is

$$\text{DLU}(S) = \max_{\substack{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m \\ a, b \neq 0}} |\text{DLCT}_S(a, b)|.$$

To evaluate the resistance of a block cipher with S-Box function S to the differential-linear attack [31, 23, 33], it is convenient to find its differential-linear uniformity $\text{DLU}(S)$. If $\text{DLU}(S)$ is sufficiently high, this can be used by an attacker to mount differential-linear attacks.

Example 7: For AES, the differential-linear uniformity is $\text{DLU}(S) = 16$.

10. Conclusion

In this paper, we reviewed the main techniques that are used to attack block ciphers, with specific applications to the AES cryptosystem. Our study focused mainly on the linear, the differential, the differential-linear, and the boomerang cryptanalysis as well as the DLCT cryptanalysis. We detailed the definitions and the main properties of the vectorial Boolean functions involved in each technique and exhibited the corresponding tables and the optimal values for AES. All experiments show that AES is secure against all the cryptanalytic attacks studied in this paper.

References

- [1] C. Ashokkumar, R. P. Giri, and B. Menezes, “Highly efficient algorithms for AES key retrieval in cache access attacks,” in Proc. 2016 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 261-275 (2016).

- [2] S. Bajrić, "Infinite families of five-valued Walsh spectrum Boolean functions," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 5, pp. 1303-1320 (2022), doi: 10.1080/09720529.2020.1756043.
- [3] U. Banerjee, L. Ho, and S. Koppula, "Power-based side-channel attack for AES key extraction on the ATmega328 Microcontroller," arXiv preprint arXiv:2203.08220 (2022).
- [4] A. Bar-On, O. Dunkelman, N. Keller, and A. Weizman, "DLCT: A new tool for differential-linear cryptanalysis," in EUROCRYPT 2019, Y. Ishai and V. Rijmen, Eds., vol. 11476 of Lecture Notes in Computer Science, pp. 313-342 (2019).
- [5] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials," *J. Cryptology*, vol. 18, no. 4, pp. 291-311 (2005).
- [6] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3-72 (1991).
- [7] E. Biham, O. Dunkelman, and N. Keller, "The rectangle attack - rectangling the Serpent," in EUROCRYPT 2001, B. Pfitzmann, Ed., vol. 2045 of Lecture Notes in Computer Science, pp. 340-357, Springer (2001).
- [8] E. Biham, O. Dunkelman, and N. Keller, "Enhancing differential-linear cryptanalysis," in Advances in Cryptology – ASIACRYPT 2002, vol. 2501 of Lecture Notes in Computer Science, pp. 254-266, Springer (2002).
- [9] A. Biryukov, "The Boomerang attack on 5 and 6-Round AES," in Advanced Encryption Standard - AES, H. Dobbertin, V. Rijmen, and A. Sowa, Eds., vol. 3373 of Lecture Notes in Computer Science, pp. 11-16, Springer, Heidelberg (2005).
- [10] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique cryptanalysis of the full AES," in Asiacrypt 2011, D. H. Lee and X. Wang, Eds., vol. 7073 of Lecture Notes in Computer Science, pp. 344-371, Springer (2011).
- [11] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum security analysis of AES," Cryptology ePrint Archive, Report 2019/272 (2019). [Online]. Available: <https://eprint.iacr.org/2019/272>.
- [12] C. Boura and A. Canteaut, "On the boomerang uniformity of cryptographic S-boxes," *IACR Transactions on Symmetric Cryptology*, Ruhr Universität Bochum, vol. 2018, no. 3, pp. 290-310 (2018).

- [13] A. Canteaut, L. Kölsch, C. Li, C. Li, K. Li, L. Qu, and F. Wiemer, "On the differential-linear connectivity table of vectorial Boolean functions," (2019). [Online]. Available: <https://arxiv.org/abs/1908.07445v1>.
- [14] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song, "Boomerang connectivity table: a new cryptanalysis tool," in *Advances in Cryptology - EUROCRYPT 2018 - Proceedings, Part II*, J. B. Nielsen and V. Rijmen, Eds., vol. 10821 of *Lecture Notes in Computer Science*, pp. 683-714, Springer (2018).
- [15] C. Carlet, "Boolean functions for cryptography and error-correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. L. Hammer, Eds., pp. 257-397, Cambridge University Press (2010).
- [16] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge (2021).
- [17] C. Carlet and S. Mesnager, "Four decades of research on bent functions," *Des. Codes Cryptogr.*, vol. 78, pp. 5-50 (2016).
- [18] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer Verlag (2002).
- [19] H. Demirci and A. A. Selçuk, "A meet-in-the-middle attack on 8-round AES," in *Proc. of Fast Software Encryption 15*, vol. 5806 of *Lecture Notes in Computer Science*, pp. 116-126, Springer (2008).
- [20] P. Derbez, P. Fouque, and J. Jean, "Improved key recovery attacks on reduced-round AES in the single-key setting," in *Advances in Cryptology - EUROCRYPT 2013*, T. Johansson and P. Q. Nguyen, Eds., vol. 7881 of *Lecture Notes in Computer Science*, pp. 371-387, Springer (2013).
- [21] O. Dunkelman, K. Keller, E. Ronen, and A. Shamir, "The retracing boomerang attack," *Cryptology ePrint Archive*, Report 2019/1154 (2019). [Online]. Available: <https://eprint.iacr.org/2019/1154>.
- [22] O. Dunkelman, S. Indesteege, and N. Keller, "A differential-linear attack on 12-round Serpent," in *Progress in Cryptology - INDOCRYPT 2008*, D. R. Chowdhury, V. Rijmen, and A. Das, Eds., vol. 5365 of *Lecture Notes in Computer Science*, pp. 174-188, Springer, Berlin, Heidelberg (2008).
- [23] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved cryptanalysis of Rijndael," in *Fast Software Encryption: FSE 2000*, G. Goos, J. Hartmanis, J. van Leeuwen, and B. Schneier, Eds., vol. 1978 of *Lecture Notes in Computer Science*, pp. 213-230, Springer, Berlin, Heidelberg (2001).

- [24] H. Gilbert and M. Minier, "A collision attack on 7 rounds of Rijndael," in AES Candidate Conference, pp. 230-241 (2000).
- [25] M. Gorski and L. Lucks, "New related-key boomerang attacks on AES," in Progress in Cryptology - INDOCRYPT 2008, D. R. Chowdhury, V. Rijmen, and A. Das, Eds., vol. 5365 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg (2008).
- [26] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, USA, May 22-24, 1996, G. L. Miller, Ed., pp. 21-29 (1996).
- [27] J. Kim, S. Hong, and B. Preneel, "Related-key rectangle attacks on reduced AES-192 and AES-256," in Fast Software Encryption: FSE 2007, A. Biryukov, Ed., vol. 4593 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg (2007).
- [28] H. Kim, S. Kim, D. Hong, J. Sung, and S. Hong, "Improved differential-linear cryptanalysis using DLCT," *Journal of The Korean Institute of Information Security & Cryptology*, vol. 28, no. 6, pp. 733-748, Dec. (2018).
- [29] L. R. Knudsen, "Truncated and higher order differentials," in Fast Software Encryption, B. Preneel, Ed., vol. 1008 of Lecture Notes in Computer Science, pp. 196-211, Springer (1994).
- [30] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis," in CRYPTO, Y. Desmedt, Ed., vol. 839 of Lecture Notes in Computer Science, pp. 17-25, Springer (1994).
- [31] K. Li, L. Qu, B. Sun, and C. Li, "New results about the boomerang uniformity of permutation polynomials," *IEEE Transactions on Information Theory*, vol. 65, no. 11, pp. 7292-7303 (2019).
- [32] J. Lu, "A methodology for differential-linear cryptanalysis and its applications," *Des. Codes Cryptogr.*, vol. 77, no. 1, pp. 11-48 (2015).
- [33] J. Lu, O. Dunkelman, N. Keller, and J. Kim, "New Impossible Differential Attacks on AES," in Progress in Cryptology - INDOCRYPT 2008, D. R. Chowdhury, V. Rijmen, and A. Das, Eds., vol. 5365 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg (2008).
- [34] M. Matsui, "Linear cryptanalysis method for DES cipher," in Advances in Cryptology - EUROCRYPT '93, Springer-Verlag, Berlin, pp. 386-397 (1994).
- [35] S. Mesnager, *Bent Functions: Fundamentals and Results*, Springer, Switzerland (2016).

- [36] K. Nyberg, "Differentially uniform mappings for cryptography," in Proc. of EUROCRYPT '93, vol. 765 of Lecture Notes in Computer Science, pp. 55-64 (1994).
- [37] K. Nyberg and L. R. Knudsen, "Provable security against differential cryptanalysis," in Advances in Cryptology — CRYPTO '92, E. F. Brickell, Ed., vol. 740 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg (1992).
- [38] K. Nyberg and L. R. Knudsen, "Provable security against a differential attack," *Journal of Cryptology*, vol. 8, no. 1, pp. 27-37 (1995).
- [39] National Institute of Standards and Technology, Federal Information Processing Standards Publication 197: Announcing the Advanced Encryption Standard (AES). [Online]. Available: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [40] S. B. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-analysis attack on an ASIC AES implementation," in Proc. International Conference on Information Technology: Coding and Computing (ITCC 2004), vol. 2, pp. 546-552 (2004).
- [41] Y. Shin, J. Kim, G. Kim, S. Hong, and S. Lee, "Differential-linear type attacks on reduced rounds of SHACAL-2," in Proc. of ACISP '04, H. Wang, J. Pieprzyk, and V. Varadharajan, Eds., vol. 3108 of Lecture Notes in Computer Science, pp. 110-122, Springer-Verlag (2004).
- [42] L. Song, X. Qin, and L. Hu, "Boomerang connectivity table revisited," Cryptology ePrint Archive, Report 2019/146 (2019). [Online]. Available: <https://eprint.iacr.org/2019/146>.
- [43] U.S. National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publications No. 46 (1977).
- [44] D. Wagner, "The Boomerang attack," in Fast Software Encryption, L. R. Knudsen, Ed., vol. 1636 of Lecture Notes in Computer Science, pp. 156-170, Springer (1999).
- [45] G. Yellapu, "Improved lower bound for algebraic immunity of a subclass of MM bent Boolean functions," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 4, pp. 965-973 (2021), doi: 10.1080/09720529.2019.1701268.

Received February, 2023