Niu *et al. J Surveill Secur Saf* 2023;4:94-111
DOI: 10.20517/jsss.2023.09

Journal of Surveillance, Security and Safety

Original Article

Open Access

On the additive differential probability of ARX construction

Zhongfeng Niu[1], Siwei Sun[1,2], Lei Hu[3,4]

[1]School of Cryptology, University of Chinese Academy of Sciences, Beijing 100049, China.
[2]State Key Laboratory of Cryptology, Beijing 5159, China.
[3]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 10009, China.
[4]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China.

Correspondence to: Prof. Siwei Sun, School of Cryptology, University of Chinese Academy of Sciences, 19 Yuquan Road, Beijing 100049, China. E-mail: sunsiwei@ucas.ac.cn.

How to cite this article: Niu Z, Sun S, Hu L. On the additive differential probability of ARX construction. *J Surveill Secur Saf* 2023;4:94-111. http://dx.doi.org/10.20517/jsss.2023.09

Received: 27 Mar 2023 **First Decision:** 28 Aug 2023 **Revised:** 21 Oct 2023 **Accepted:** 1 Nov 2023 **Published:** 29 Nov 2023

Academic Editor: Josef Pieprzyk **Copy Editor:** Dan Zhang **Production Editor:** Dan Zhang

Abstract

Aim: The additive differential cryptanalysis is a significant technique used in the analysis of ARX ciphers. In this paper, we will focus on accurately and efficiently calculating the additive differential probability of $x \lll d \oplus y \lll e$.

Methods: Inspired by the work of Niu *et al.* at Crypto 2022, we use a delicate partition of $\mathbf{F}_2^n \times \mathbf{F}_2^n$ into subsets.

Result: We derive an algorithm that can calculate it with linear time complexity. Compared with our algorithm, the one proposed by Velichkov *et al.* is only suitable when $e = 0$.

Conclusion: For the ARX construction: $(x \boxplus y) \lll d \oplus y \lll e$, which appears in Alzette, Speck, *etc.*, our algorithm can find more accurate additive differential characteristics for such ARX constructions. It is essential to evaluate the resistance of such ARX primitives against Additive differential cryptanalysis.

Keywords: Additive differential probability, ARX construction, Alzette, Speck

INTRODUCTION

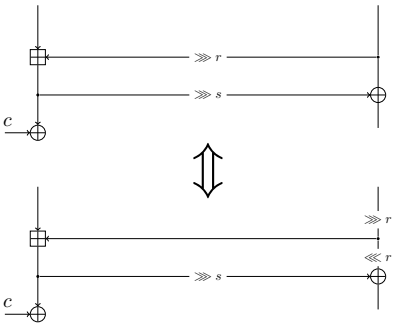
ARX ciphers are constructed by the modular addition, bit rotation, and XOR operations (ARX). Examples include the block cipher SPECK[1], Sparx[2], the stream cipher Salsa20[3], ChaCha20[4], the cryptographic permutations Alzette[5], Sparkle[6], the MAC (Message Authentication Code) Chaskey[7], the PRF (Pseudo-random function) Siphash[8], the SHA-3 finalists BLAKE[9], and Skein[10]. The ARX design has the following three advantages. Firstly, diffusion and confusion can be provided by the modulo additions, making it possible to avoid the table look-ups to look up the table compared with the S-box based SPN designs, which strengthens the resilience against timing side-channel attacks. Secondly, since modulo additions can be natively supported in modern CPUs, the ARX ciphers have fast software implementations due to the native support of the modulo additions in modern CPUs. Finally, the code size of describing an ARX primitive is very simple and small,incurring minimal costs, making it suitable for application scenarios the cases where the memory footprint is highly constrained.

Differential Cryptanalysis of ARX Primitives. Among all the cryptanalyses[11–17] for symmetric cryptography, Differential Cryptanalysis[16,17] is one of the most important techniques to analyze the cryptographic primitives. Thus, both in the design and cryptanalysis of ARX ciphers, the differential properties of ARX constructions are of great importance. The first algorithm for computing the differential probabilities of modulo additions efficiently was first proposed in 2001[18]. Later, for the additive differential probabilities of XOR, Lipmaa *et al.*[19] give the first algorithm for computing it efficiently. In 2011, Velichkov *et al.*[20] presented an algorithm for computing the additive differential probabilities of ARX constructions efficiently. However, the algorithm is only suitable for some ARX constructions involving only one bit rotation, such as Skein[3]. For other ARX constructions, such as Alzette[5] (see Figure 1), we must consider a new algorithm.

Contribution. Inspired by the work of Niu *et al.*[21] on calculating the rotational differential-linear correlation of the modulo addition for modulo additions, we use a delicate artful partition of $\mathbf{F}_2^m \times \mathbf{F}_2^m$ into subsets, where the elements in each subset fulfill certain equations. The method is extremely efficient, and the. The time complexity of computing the additive differential probabilities of ARX constructions: $(x \boxplus y) \lll d \oplus y \lll e$ is, can be estimated by the complexity of $4n$ n 8×8 matrix multiplications. It can be summarized as follows, with factor 4.

Theorem Organization. For $\alpha', \beta, \gamma \in \mathbf{F}_2^n$ and ARX construction $ARX(x, y, d, e)$, which is illustrated in Fig 5, if we let $\alpha = \alpha' \boxplus^n \beta$, then $\Pr[(\alpha', \beta) \to \gamma]^{ARX}$ can be calculated as:

$$\sum_{a,b\in\mathbf{F}_2} C^T_{a,b} \prod_{i=d}^{n-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i} \; R_2 \prod_{i=e}^{d-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i} \; R_1 \prod_{i=0}^{e-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i} \; \mathbf{e_{4+2b+a}}$$



$$x \leftarrow x \boxplus (y \ggg r), y \leftarrow y \boxplus (x \ggg s), x \leftarrow x \oplus c$$

Figure 1. The round function of Alzette, where x is the input of the left branch, and y is the input of the right branch

.

where $\mathbf{e}_i$ denotes the i-th unit vector,

$$M_{000} = \frac{1}{4}\begin{pmatrix} 01100000 \\ 01000000 \\ 00100000 \\ 00000000 \\ 01104001 \\ 01000001 \\ 00100001 \\ 00000001 \end{pmatrix} M_{001} = \frac{1}{4}\begin{pmatrix} 40010110 \\ 00010100 \\ 00010010 \\ 00010000 \\ 00000110 \\ 00000100 \\ 00000010 \\ 00000000 \end{pmatrix} M_{010} = \frac{1}{4}\begin{pmatrix} 10000000 \\ 00000000 \\ 10010000 \\ 00010000 \\ 10000100 \\ 00000100 \\ 10010140 \\ 00010100 \end{pmatrix} M_{011} = \frac{1}{4}\begin{pmatrix} 01001000 \\ 01000000 \\ 01401001 \\ 01000001 \\ 00001000 \\ 00000000 \\ 00001001 \\ 00000001 \end{pmatrix}$$

$$M_{100} = \frac{1}{4}\begin{pmatrix} 10000000 \\ 10010000 \\ 00000000 \\ 00010000 \\ 10000010 \\ 10010410 \\ 00000010 \\ 00010010 \end{pmatrix} M_{101} = \frac{1}{4}\begin{pmatrix} 00101000 \\ 04101001 \\ 00100000 \\ 00100001 \\ 00001000 \\ 00001001 \\ 00000000 \\ 00000001 \end{pmatrix} M_{110} = \frac{1}{4}\begin{pmatrix} 00000000 \\ 01000000 \\ 00100000 \\ 01100000 \\ 00001000 \\ 01001000 \\ 00101000 \\ 01101004 \end{pmatrix} M_{111} = \frac{1}{4}\begin{pmatrix} 10000000 \\ 10000100 \\ 10000010 \\ 10040110 \\ 00000000 \\ 00000100 \\ 00000010 \\ 00000110 \end{pmatrix}$$

and

$$R_1 = \sum_{c,h,v \in \mathbf{F}_2} \mathbf{e}_{\mathbf{4c+h}}\, \mathbf{e}^{\mathbf{T}}_{\mathbf{4c+2v+h}}$$

$$R_2 = \sum_{w,z,u \in \mathbf{F}_2} \mathbf{e}_{\mathbf{4z+2w}}\, \mathbf{e}^{\mathbf{T}}_{\mathbf{4z+2w+u}}$$

$$C_{a,b} = \sum_{s \in \mathbf{F}_2} \mathbf{e}^{\mathbf{T}}_{\mathbf{4s+2b+a}}$$

Section 2 briefly introduces some notations and preliminaries on modulo addition, ARX structures, and additive differential probability. The partition of $\mathbf{F}_2^n \times \mathbf{F}_2^n$ and its properties are described in section 3. In section 4, we show that the calculation of additive differential probability of ARX structures can be divided into three parts. Then, in section 5, we give the method to calculate the additive differential probability of ARX structures. Finally, we conclude our work in section 6.

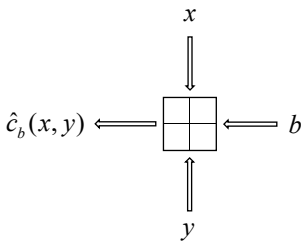


Figure 2. The $\hat{c}_b(\mathbf{x},\mathbf{y})$.

NOTATIONS AND PRELIMINARIES

For a finite set $\mathbf{D}$, $\#\mathbf{D}$ denotes the number of elements. Let $\mathbf{F}_2 = \{0,1\}$ be the binary field. We denote by x_i the i-th bit of a vector $\mathbf{x} = (x_{n-1}, \cdots, x_0) \in \mathbf{F}_2^n$. In addition, $\lceil \mathbf{x} \rceil^{(t)} = (x_{n-1}, \cdots, x_{n-t})$ denotes the most significant t bits of $\mathbf{x}$. $\lfloor \mathbf{x} \rfloor^{(t)} = (x_{t-1}, \cdots, x_0)$ denotes the least significant t bits of $\mathbf{x}$. $[x]_a^b = (x_b, \cdots, x_a)$ denotes the substring of $\mathbf{x}$ form $(a-1)$-bit to $(b-1)$-bit. Concrete values in $\mathbf{F}_2^n$ are specified in hexadecimal or binary notations. For example, we use $\mathbf{0x3F21}$ to denote the binary string 0011111100100001. And let 1^n denote the binary string $111\cdots1111$, and 0^n denote the binary string $000\cdots000$. Rotation of $\mathbf{x}$ by t bits is denoted by $\mathbf{x} \lll t$. Let M_i for $0 \le i < n$ be the $k \times k$ matrices, and we use $\prod_{i=0}^{n} M_i$ to denote the product with the specified order $M_{n-1} \cdots M_0$. For any $n > 0$, the function $\delta : \mathbf{F}_2^n \to \{0,1\}$ is defined as $\delta^{(n)}(x) = \begin{cases} 1 & x = 0^n \\ 0 & others \end{cases}$. Let $\mathbf{e}_i$ denote the i-th unit vector.

Modulo Addition with an Initial Carry Bit and Additive Differential Probability

Let $\boxplus_b^{(n)} : \mathbf{F}_2^n \times \mathbf{F}_2^n \to \mathbf{F}_2^n$ be the operation mapping $(x,y) \in \mathbf{F}_2^n \times \mathbf{F}_2^n$ to

$$x \boxplus_b^{(n)} y = x + y + b \bmod 2^n$$

where $b \in \mathbf{F}_2$. For convenience, we use $x \boxplus y$ to denote $x + y \bmod 2^n$.

For $(x,y) \in \mathbf{F}_2^n \times \mathbf{F}_2^n$, the carry vector of (x,y) with initial carry bit $b \in \mathbf{F}_2$ is defined to be a $(n+1)$-bit vector $c_b(\mathbf{x},\mathbf{y}) = (c_n, c_{n-1}, \cdots, c_0)$ such that

$$c_i = \begin{cases} b, & i = 0 \\ x_{i-1}y_{i-1} \oplus x_{i-1}c_{i-1} \oplus y_{i-1}c_{i-1} & 1 \le i \le n. \end{cases}$$

We call $c_b(\mathbf{x},\mathbf{y})_n$ the most significant carry of $x \boxplus_b^{(n)} y$, denoted as $\hat{c}_b(\mathbf{x},\mathbf{y})$, which is illustrated in Figure 2. Under such notations, $x \boxplus_b^{(n)} y = x \oplus y \oplus \lfloor c_b(x,y) \rfloor^n$. Moreover,

$$c_b(\lfloor \mathbf{x} \rfloor^k, \lfloor \mathbf{y} \rfloor^k) = \lfloor c_b(\mathbf{x},\mathbf{y}) \rfloor^{k+1}$$

is a $(k+1)$-bit vector. Let $\boxminus^{(n)} : \mathbf{F}_2^n \times \mathbf{F}_2^n \to \mathbf{F}_2^n$ be the operation mapping $(x,y) \in \mathbf{F}_2^n \times \mathbf{F}_2^n$ to

$$x \boxminus^{(n)} y = x - y \bmod 2^n$$

Then, $\boxminus$ has the following relationship with $\boxplus_b^{(n)}$:

Theorem 0.1.

$$x \boxminus^{(n)} y = x \boxplus_1^{(n)} (y \oplus 1^n)$$

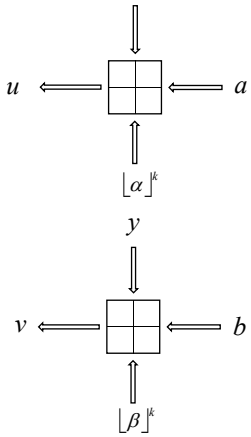


Figure 3. The equivalent form of the set $\mathbf{D}^{(k)}_{\substack{u\lhd a\\ v\lhd b}}(\alpha,\beta)$.

Partitions of $\mathbf{F}_2^k\times\mathbf{F}_2^k$

Definition 0.1. *Given* $(a,b)\in\mathbf{F}_2^2$, $(u,v)\in\mathbf{F}_2^2$, *and* $(\alpha,\beta)\in\mathbf{F}_2^n\times\mathbf{F}_2^n$, *for* $1\le k\le n$, *we use* $\mathbf{D}^{(k)}_{\substack{u\lhd a\\ v\lhd b}}(\alpha,\beta)\subseteqq\mathbf{F}_2^k\times\mathbf{F}_2^k$ *to denote the set*

$$\{(\mathbf{x},\mathbf{y})\in\mathbf{F}_2^k\times\mathbf{F}_2^k:\left(\hat{e}_a(\mathbf{x},\lfloor\alpha\rfloor^{(k)}),\hat{e}_b(\mathbf{y},\lfloor\beta\rfloor^{(k)})\right)=(u,v)\}.$$

In fact, it represents a solution set of some equations, which is illustrated in Figure 3.

Under the notation, we have

$$\mathbf{D}^{(n)}_{\substack{u\lhd a\\ v\lhd b}}(\alpha,\beta)=\{(\mathbf{x},\mathbf{y})\in\mathbf{F}_2^n\times\mathbf{F}_2^n:(\hat{e}_a(\mathbf{x},\alpha),\hat{e}_b(\mathbf{y},\beta))=(u,v)\}.$$

and $\mathbf{D}^{(1)}_{\substack{u\lhd a\\ v\lhd b}}(\alpha_i,\beta_i)=\{(x,y)\in\mathbf{F}_2\times\mathbf{F}_2:(\hat{e}_a(x,\alpha_i),\hat{e}_b(y,\beta_i))=(u,v)\}\subseteqq\mathbf{F}_2\times\mathbf{F}_2$, which is the solution of

$$\begin{cases}x\alpha_i\oplus\alpha_i a\oplus xa=u\\ y\beta_i\oplus\beta_i b\oplus yb=v\end{cases}.$$

The set $\mathbf{D}^{(n)}_{\substack{u\lhd a\\ v\lhd b}}(\alpha,\beta)$ has the following property:

Lemma 0.1. *For any fixed* $(a,b)\in\mathbf{F}_2^2$ *and* $(\alpha,\beta)\in\mathbf{F}_2^n\times\mathbf{F}_2^n$,

$$\mathbf{F}_2^n\times\mathbf{F}_2^n=\bigcup_{(u,v)\in\mathbf{F}_2^2}\mathbf{D}^{(n)}_{\substack{u\lhd a\\ v\lhd b}}(\alpha,\beta)$$

and $(u,v)=(u',v')$ *if and only if*

$$\mathbf{D}^{(n)}_{\substack{u\lhd a\\ v\lhd b}}(\alpha,\beta)\bigcap\mathbf{D}^{(n)}_{\substack{u'\lhd a\\ v'\lhd b}}(\alpha,\beta)\neq\varnothing.$$

 tp://dx.doi.org/10.20517/jsss.2023.09

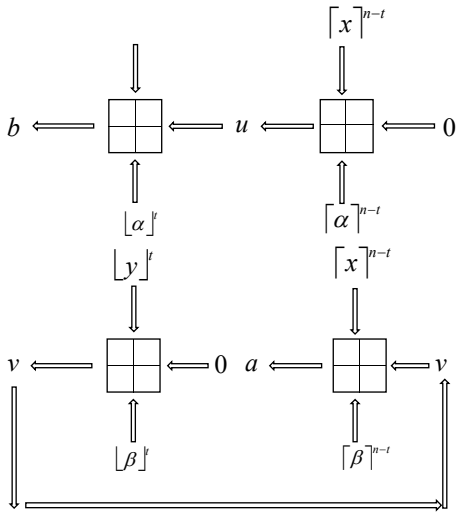


Figure 4. The equivalent form of the set $\mathbf{D}^{(t)}_{\substack{b \lhd u \\ v \lhd 0}} || \mathbf{D}^{(n-t)}_{\substack{u \lhd 0 \\ a \lhd v}}(\alpha, \beta)$.

Lemma 0.2. *Let* $\mathbf{D}^{(t)}_{\substack{b \lhd u \\ v \lhd 0}} || \mathbf{D}^{(n-t)}_{\substack{u \lhd 0 \\ a \lhd v}}(\alpha, \beta)$ *be the set of all* $(\mathbf{x}, \mathbf{y}) \in \mathbf{F}_2^n \times \mathbf{F}_2^n$ *such that*

$$\begin{cases} (\lfloor \mathbf{x} \rfloor^t, \lfloor \mathbf{y} \rfloor^t) \in \mathbf{D}^{(t)}_{\substack{b \lhd u \\ v \lhd 0}}(\lfloor \alpha \rfloor^t, \lfloor \beta \rfloor^t) \\ (\lceil \mathbf{x} \rceil^{n-t}, \lceil \mathbf{y} \rceil^{n-t}) \in \mathbf{D}^{(n-t)}_{\substack{u \lhd 0 \\ a \lhd v}}(\lceil \alpha \rceil^{n-t}, \lceil \beta \rceil^{n-t}) \end{cases} \tag{1}$$

which is illustrated in Figure 4. Then, the necessary and sufficient condition for

$$\mathbf{D}^{(t)}_{\substack{b \lhd u \\ v \lhd 0}} || \mathbf{D}^{(n-t)}_{\substack{u \lhd 0 \\ a \lhd v}}(\alpha, \beta) \bigcap \mathbf{D}^{(t)}_{\substack{b' \lhd u' \\ v' \lhd 0}} || \mathbf{D}^{(n-t)}_{\substack{u' \lhd 0 \\ a' \lhd v'}}(\alpha, \beta) \neq \varnothing \tag{2}$$

is $(u, v, a, b) = (u', v', a', b')$. *Moreover, we have*

$$\bigcup_{(a,b) \in \mathbf{F}_2^2} \bigcup_{(u,v) \in \mathbf{F}_2^2} \mathbf{D}^{(t)}_{\substack{b \lhd u \\ v \lhd 0}} || \mathbf{D}^{(n-t)}_{\substack{u \lhd 0 \\ a \lhd v}}(\alpha, \beta) = \mathbf{F}_2^n \times \mathbf{F}_2^n.$$

Proof. Equation 2 implies that

$$\begin{cases} \mathbf{D}^{(t)}_{\substack{b \lhd u \\ v \lhd 0}}(\lfloor \alpha \rfloor^t, \lfloor \beta \rfloor^t) \bigcap \mathbf{D}^{(t)}_{\substack{b' \lhd u' \\ v' \lhd 0}}(\lfloor \alpha \rfloor^t, \lfloor \beta \rfloor^t) \neq \varnothing \\ \mathbf{D}^{(n-t)}_{\substack{u \lhd 0 \\ a \lhd v}}(\lceil \alpha \rceil^{n-t}, \lceil \beta \rceil^{n-t}) \bigcap \mathbf{D}^{(n-t)}_{\substack{u' \lhd 0 \\ a' \lhd v'}}(\lceil \alpha \rceil^{n-t}, \lceil \beta \rceil^{n-t}) \neq \varnothing \end{cases}$$

which implies $v = v'$, $a = a'$ and $u = u'$, $b = b'$ according to 0.1.
The second part of the lemma comes from the fact that any elements in $\mathbf{F}_2^n \times \mathbf{F}_2^n$ must satisfy Equation 2 for some (u, v, a, b).

□

The ARX construction

The ARX construction $\mathbf{F}_2^{2n} \to \mathbf{F}_2^n$ is defined as:

$$ARX(x, y, d, e) = ((x \boxplus^n y) \lll d) \oplus y \lll e$$

which is illustrated in Figure 5, where $x, y \in \mathbf{F}_2^n, 0 \leq e,\ d < n$.

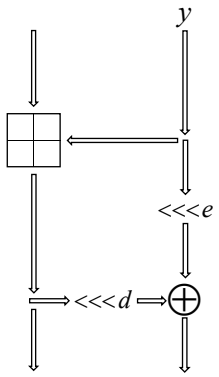


Figure 5. The ARX construction $ARX(x, y, d, e)$.

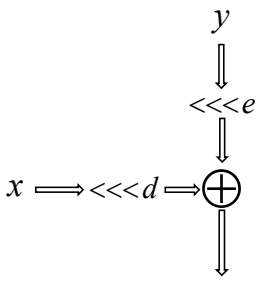


Figure 6. The function f.

Remark 0.1. *In FSE 2011[20], the ARX construction* $\mathbf{F}_2^{2n} \to \mathbf{F}_2^{2n}$ *is defined as:*

$$ARX(x, y, d, e) = ((x \boxplus^n y) \lll d) \oplus y$$

Compared with the ARX construction $ARX(x, y, d, e)$*, there are two rotations before* $\oplus$ *instead of one, namely* $ARX(x, y, d, 0)$*. We must point out that the ARX construction defined in FSE 2011[20] is not suitable for some ARX ciphers, such as Alzette[5] or Speck[1].*

The additive difference

Definition 0.2. *Given a vectorial Boolean function* $F : \mathbf{F}_2^n \to \mathbf{F}_2^m$*, the probability of additive difference with input difference* $\alpha \in \mathbf{F}_2^n$ *and output difference* $\beta \in \mathbf{F}_2^m$ *is defined as*

$$\Pr[\alpha \to \beta]^F = \frac{1}{2^n} \#\{x \in \mathbf{F}_2^n : F(x \boxplus^{(n)} \alpha) \boxminus^n F(x) = \beta\}$$

If we define the function $f : \mathbf{F}_2^{2n} \to \mathbf{F}_2^{2n}$ as:

$$f(x, y, d, e) = (x \lll d) \oplus (y \lll e)$$

which is illustrated in Figure 6. Then, for $ARX(x, y, d, e)$, its probability of additive difference with input difference $(\alpha, \beta) \in \mathbf{F}_2^{2n}$ and output difference $\gamma \in \mathbf{F}_2^n$ has the following relationship:

$$\Pr[(\alpha', \beta) \to \gamma]^{ARX} = \Pr[(\alpha, \beta) \to \gamma]^f$$

where $\alpha = \alpha' \boxplus^n \beta, 0 \le e \le d < n$.

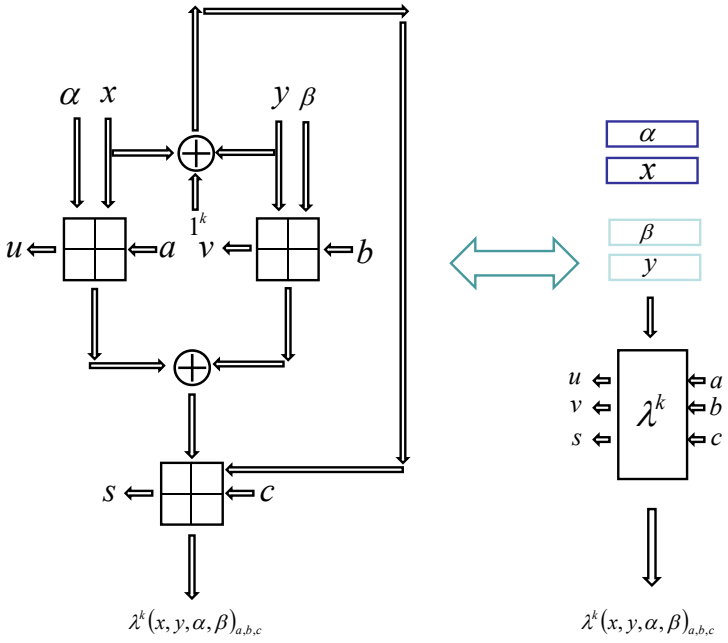


Figure 7. The function $\lambda^k(x, y, \alpha, \beta)_{a,b,c}$. On the right side, it is the simple form of $\lambda^k(x, y, \alpha, \beta)_{a,b,c}$, where α, x, β, y represent the input, a, b, c represent the three initial bits, and u, v, c represent three carry bits.

PARTITION OF $\mathbf{F}_2^n \times \mathbf{F}_2^n$

In order to know the probability of additive difference of the function $f(x, y)$ with input difference $(\alpha, \beta) \in \mathbf{F}_2^{2n}$ and output difference $\gamma \in \mathbf{F}_2^n$, we need to know the number of solutions of the equation:

$$f(x \boxplus^n \alpha, y \boxplus^n \beta, d, e) \boxminus^n f(x, y, d, e) = \gamma$$

Firstly, we define the function value $\lambda^k(x, y, \alpha, \beta)_{a,b,c} : \mathbf{F}_2^{4k} \to \mathbf{F}_2^k$ with three initial bits a, b, c as:

$$\lambda^k(x, y, \alpha, \beta)_{a,b,c} = \left(\left(x \boxplus_a^{(k)} \alpha\right) \oplus \left(y \boxplus_b^{(k)} \beta\right)\right) \boxplus_c^{(k)} \left(x \oplus y \oplus 1^k\right)$$

where $x, y, \alpha, \beta \in \mathbf{F}_2^k$, and it can generate three carry bits:

$$\begin{aligned} u &= \hat{c}_a(\mathbf{x}, \alpha) \\ v &= \hat{c}_b(\mathbf{y}, \beta) \\ s &= \hat{c}_c(\alpha \oplus \beta \oplus \mathbf{x} \oplus \mathbf{y} \oplus c_a(\mathbf{x}, \alpha) \oplus c_b(\mathbf{y}, \beta), \mathbf{x} \oplus \mathbf{y} \oplus 1^k) \end{aligned}$$

which is illustrated in Figure 7.

Then, we define a subset of $\mathbf{D}^{(k)}_{\substack{u \lhd a \\ v \lhd b}}(\alpha, \beta)$:

Definition 0.3. *Given* $(a, b, c) \in \mathbf{F}_2^3$, $(u, v, s) \in \mathbf{F}_2^3$, *and* $(\alpha, \beta) \in \mathbf{F}_2^n \times \mathbf{F}_2^n$, *for* $1 \le k \le n$, *we use* $\mathbf{S}^{(k)}_{\substack{u \lhd a \\ v \lhd b \\ s \lhd c}}(\alpha, \beta) \subseteq \mathbf{D}^{(k)}_{\substack{u \lhd a \\ v \lhd b}}(\alpha, \beta)$ *to denote the set*

$$\{(\mathbf{x}, \mathbf{y}) \in \mathbf{F}_2^k \times \mathbf{F}_2^k : \begin{array}{c} \left(\hat{c}_a(\mathbf{x}, \lfloor \alpha \rfloor^{(k)}), \hat{c}_b(\mathbf{y}, \lfloor \beta \rfloor^{(k)})\right) = (u, v) \\ \hat{c}_c(\lfloor \alpha \rfloor^{(k)} \oplus \lfloor \beta \rfloor^{(k)} \oplus \mathbf{x} \oplus \mathbf{y} \oplus \lfloor c_a(\mathbf{x}, \alpha) \rfloor^k \oplus \lfloor c_b(\mathbf{y}, \beta) \rfloor^k, \mathbf{x} \oplus \mathbf{y} \oplus 1^k) = s \end{array} \}.$$

For the set $\mathbf{S}^{(k)}_{\substack{u \lhd a \\ v \lhd b \\ s \lhd c}}(\alpha, \beta)$, we have the following property:

Lemma 0.3. *For any fixed* $(a,b,u,v) \in \mathbf{F}_2^4$, $c \in \mathbf{F}_2$ *and* $(\alpha,\beta) \in \mathbf{F}_2^n \times \mathbf{F}_2^n$,

$$\mathbf{D}^{(n)}_{\substack{u \lhd a \\ v \lhd b}}(\alpha,\beta) = \bigcup_{s \in \mathbf{F}_2} \mathbf{S}^{(n)}_{\substack{u \lhd a \\ v \lhd b \\ s \lhd c}}(\alpha,\beta)$$

and $s = s'$, $v = v'$, $u = u'$ *if and only if*

$$\mathbf{S}^{(n)}_{\substack{u \lhd a \\ v \lhd b \\ s \lhd c}}(\alpha,\beta) \bigcap \mathbf{S}^{(n)}_{\substack{u' \lhd a \\ v' \lhd b \\ s' \lhd c}}(\alpha,\beta) \neq \varnothing.$$

For the function $g(x,y)^{(\alpha,\beta)} = f(x \boxplus^n \alpha, y \boxplus^n \beta, d, e) \boxminus^n f(x,y,d,e)$, it can be repressed as bit level:

$$g(x,y)_i^{(\alpha,\beta)} = \alpha_{(i-d) \bmod n} \oplus \beta_{(i-e) \bmod n} \oplus 1 \oplus \mathcal{C}_0(x,\alpha)_{(i-d) \bmod n} \oplus \mathcal{C}_0(y,\beta)_{(i-e) \bmod n} \oplus g_i$$

where $g_0 = 1$ and for $1 \le i \le n$, g_i is defined as:

$$\begin{aligned} g_i = &\left((x \boxplus^n \alpha)_{(i-1-d) \bmod n} \oplus (y \boxplus^n \beta)_{(i-1-e) \bmod n}\right)\left(x_{(i-1-d) \bmod n} \oplus y_{(i-1-e) \bmod n} \oplus 1\right) \\ &\oplus \left((x \boxplus^n \alpha)_{(i-1-d) \bmod n} \oplus (y \boxplus^n \beta)_{(i-1-e) \bmod n}\right) g_{i-1} \oplus \left(x_{(i-1-d) \bmod n} \oplus y_{(i-1-e) \bmod n} \oplus 1\right) g_{i-1} \end{aligned}$$

Then, according to the expression of $g(x,y)^{(\alpha,\beta)}$ in bit level, we have:

Lemma 0.4.

$$g(x,y)^{(\alpha,\beta)} = \Delta_3 || \Delta_2 || \Delta_1$$

where

$$\begin{cases} \Delta_1 = \lambda^e([x]_{n-d}^{n-d-e}, \lceil y \rceil^e, [\alpha]_{n-d}^{n-d-e}, \lceil \beta \rceil^e)_{a,b,1} \\ \Delta_2 = \lambda^{d-e}(\lceil x \rceil^{d-e}, \lfloor y \rfloor^{d-e}, \lceil \alpha \rceil^{d-e}, \lfloor \beta \rfloor^{d-e})_{h,0,c} \\ \Delta_3 = \lambda^{n-d}(\lfloor x \rfloor^{n-d}, [y]_{d-e}^{n-e}, \lfloor \alpha \rfloor^{n-d}, [\beta]_{d-e}^{n-e})_{0,w,z} \end{cases}$$

and

$$\begin{cases} a = \hat{\mathcal{C}}_0(\lfloor x \rfloor^{n-d}, \lfloor \alpha \rfloor^{n-d}) \\ h = \hat{\mathcal{C}}_a([x]_{n-d}^{n-d-e}, [\alpha]_{n-d}^{n-d-e}) \\ w = \hat{\mathcal{C}}_0(\lfloor y \rfloor^{d-e}, \lfloor \beta \rfloor^{d-e}) \\ b = \hat{\mathcal{C}}_w([y]_{d-e}^{n-e}, [\beta]_{d-e}^{n-e}) \\ c = \hat{\mathcal{C}}_1([\alpha \oplus x]_{n-d}^{n-d-e} \oplus \lceil \beta \oplus y \rceil^e \oplus \lfloor \mathcal{C}_a([x]_{n-d}^{n-d-e}, [\alpha]_{n-d}^{n-d-e}) \rfloor^e \oplus \lfloor \mathcal{C}_b(\lceil y \rceil^e, \lceil \beta \rceil^e) \rfloor^e, [x]_{n-d}^{n-d-e} \oplus \lceil y \rceil^e \oplus 1^e) \\ z = \hat{\mathcal{C}}_c(\lceil \alpha \oplus x \rceil^{d-e} \oplus \lfloor \beta \oplus y \rfloor^{d-e} \oplus \lfloor \mathcal{C}_h(\lceil x \rceil^{d-e}, \lceil \alpha \rceil^{d-e}) \rfloor^{d-e} \oplus \lfloor \mathcal{C}_0(\lfloor y \rfloor^{d-e}, \lfloor \beta \rfloor^{d-e}) \rfloor^{d-e}, \lceil x \rceil^{d-e} \oplus \lfloor y \rfloor^{d-e} \oplus 1^{d-e}) \end{cases}$$

It is illustrated in Figure 8:

Lemma 0.5. *For* $d \ge e$, *let* $\mathbf{S}^{(n-d)}_{\substack{a \lhd 0 \\ b \lhd w \\ s \lhd z}} || \mathbf{S}^{(d-e)}_{\substack{u \lhd h \\ w \lhd 0 \\ z \lhd c}} || \mathbf{S}^{(e)}_{\substack{h \lhd a \\ v \lhd b \\ c \lhd 1}}(\alpha,\beta)$ *be the set of all* $(\mathbf{x},\mathbf{y}) \in \mathbf{F}_2^n \times \mathbf{F}_2^n$ *such that*

$$\begin{cases} (\lfloor \mathbf{x} \rfloor^{n-d}, [\mathbf{y}]_{d-e}^{n-e}) \in \mathbf{S}^{(t)}_{\substack{a \lhd 0 \\ b \lhd w \\ s \lhd z}}(\lfloor \alpha \rfloor^{n-d}, [\beta]_{d-e}^{n-e}) \\ (\lceil \mathbf{x} \rceil^{d-e}, \lfloor \mathbf{y} \rfloor^{d-e}) \in \mathbf{S}^{(d-e)}_{\substack{u \lhd h \\ w \lhd 0 \\ z \lhd c}}(\lceil \alpha \rceil^{d-e}, \lfloor \beta \rfloor^{d-e}) \\ ([\mathbf{x}]_{n-d}^{n-d-e}, \lceil \mathbf{y} \rceil^e) \in \mathbf{S}^{(e)}_{\substack{h \lhd a \\ v \lhd b \\ c \lhd 1}}([\alpha]_{n-d}^{n-d-e}, \lceil \beta \rceil^e) \end{cases} \tag{3}$$

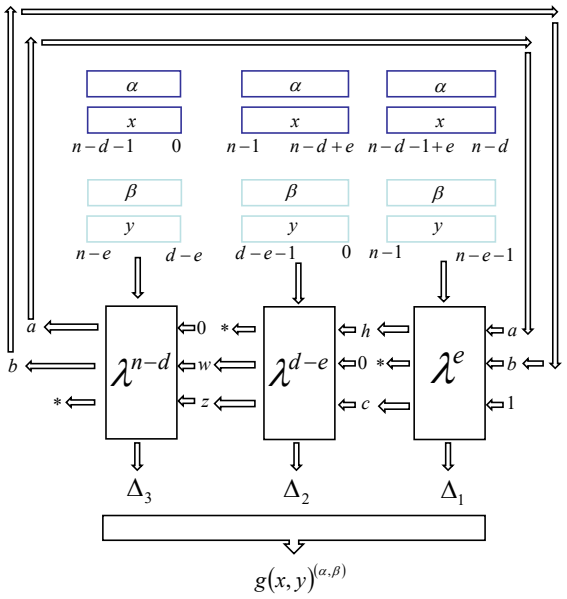


Figure 8. The equivalent form of $g(x, y)^{(\alpha,\beta)}$. For instance, 0, $n-d-1$ behind the α and x represent the substring of α and x from 1-bit to $n-d$ bit.

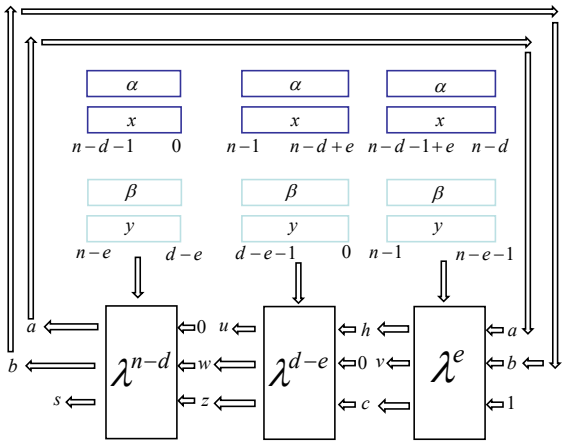


Figure 9. The equivalent form of the set $\mathbf{S}^{(n-d)}_{\substack{a\lhd 0\\ b\lhd w\\ s\lhd z}}||\mathbf{S}^{(d-e)}_{\substack{u\lhd h\\ w\lhd 0\\ z\lhd c}}||\mathbf{S}^{(e)}_{\substack{h\lhd a\\ v\lhd b\\ c\lhd 1}}(\alpha,\beta)$.

which is illustrated in Figure 9. Then, the necessary and sufficient condition for

$$\mathbf{S}^{(n-d)}_{\substack{a\lhd 0\\ b\lhd w\\ s\lhd z}}||\mathbf{S}^{(d-e)}_{\substack{u\lhd h\\ w\lhd 0\\ z\lhd c}}||\mathbf{S}^{(e)}_{\substack{h\lhd a\\ v\lhd b\\ c\lhd 1}}(\alpha,\beta)\bigcap\mathbf{S}^{(n-d)}_{\substack{a'\lhd 0\\ b'\lhd w'\\ s'\lhd z'}}||\mathbf{S}^{(d-e)}_{\substack{u'\lhd h'\\ w'\lhd 0\\ z'\lhd c'}}||\mathbf{S}^{(e)}_{\substack{h'\lhd a'\\ v'\lhd b'\\ c'\lhd 1}}(\alpha,\beta)\neq\varnothing \tag{4}$$

is $(a,h,u,b,v,w,c,z,s)=(a',h',u',b',v',w',c',z',s')$. *Moreover, we have*

$$\bigcup_{(a,h,u)\in\mathbf{F}_2^3}\bigcup_{(b,v,w)\in\mathbf{F}_2^3}\bigcup_{(c,z,s)\in\mathbf{F}_2^3}\mathbf{S}^{(n-d)}_{\substack{a\lhd 0\\ b\lhd w\\ s\lhd z}}||\mathbf{S}^{(d-e)}_{\substack{u\lhd h\\ w\lhd 0\\ z\lhd c}}||\mathbf{S}^{(e)}_{\substack{h\lhd a\\ v\lhd b\\ c\lhd 1}}(\alpha,\beta)=\mathbf{F}_2^n\times\mathbf{F}_2^n.$$

Proof. Equation 4 implies that

$$\begin{cases} \mathbf{S}^{(n-d)}_{\substack{a\lhd 0\\ b\lhd w\\ s\lhd z}}(\lfloor\alpha\rfloor^{n-d},[\beta]^{n-e}_{d-e})\cap \mathbf{S}^{(n-d)}_{\substack{a'\lhd 0\\ b'\lhd w'\\ s'\lhd z'}}(\lfloor\alpha\rfloor^{n-d},[\beta]^{n-e}_{d-e})=\varnothing \\ \mathbf{S}^{(d-e)}_{\substack{u\lhd h\\ w\lhd 0\\ z\lhd c}}(\lceil\alpha\rceil^{d-e},\lfloor\beta\rfloor^{d-e})\cap \mathbf{S}^{(d-e)}_{\substack{u'\lhd h'\\ w'\lhd 0\\ z'\lhd c'}}(\lceil\alpha\rceil^{d-e},\lfloor\beta\rfloor^{d-e})=\varnothing \\ \mathbf{S}^{(e)}_{\substack{h\lhd a\\ v\lhd b\\ c\lhd 1}}([\alpha]^{n-d-e}_{n-d},\lceil\beta\rceil^{e})\cap \mathbf{S}^{(e)}_{\substack{h'\lhd a'\\ v'\lhd b'\\ c'\lhd 1}}([\alpha]^{n-d-e}_{n-d},\lceil\beta\rceil^{e})=\varnothing \end{cases}$$

According to Lemma 0.2, we have $(h,u,w,v)=(h',u',w',v')$. And $a=a'$, $b=b'$ according to Definition 0.2. Furthermore, $(c,z,s)=(c',z',s')$.

The second part of the lemma comes from the fact that any elements in $\mathbf{F}_2^n\times\mathbf{F}_2^n$ must satisfy Equation 4 for some (a,h,u,b,v,w,c,z,s). □

METHODS

Lemma 0.6. *For the probability of additive difference of the function $f(x,y)$ with input difference $(\alpha,\beta)\in\mathbf{F}_2^{2n}$ and output difference $\gamma\in\mathbf{F}_2^n$, $d\geq e$, we have*

$$\begin{aligned}\Pr[(\alpha,\beta)\to\gamma]^f=&\frac{1}{2^{2n}}\sum_{(x,y)\in\mathbf{F}_2^n\times\mathbf{F}_2^n}\delta^n(f(x\boxplus^n\alpha,y\boxplus^n\beta,d,e)\boxminus^n f(x,y,d,e)\oplus\gamma)\\ =&\frac{1}{2^{2n}}\sum_{(a,h,b,w,c,z)\in\mathbf{F}_2^6}\Psi(a,b,w,z)\Phi(w,z,h,c)\chi(h,c,a,b)\end{aligned}$$

where

$$\begin{cases}\Psi(a,b,w,z)=\frac{1}{2^{2(n-d)}}\sum_{s\in\mathbf{F}_2}\sum_{(\lfloor\mathbf{x}\rfloor^{n-d},[\mathbf{y}]^{n-e}_{d-e})\in\mathbf{S}^{(n-d)}_{\substack{a\lhd 0\\ b\lhd w\\ s\lhd z}}(\lfloor\alpha\rfloor^{n-d},[\beta]^{n-e}_{d-e})}\delta^{(n-d)}(\Delta_3\oplus\lceil\gamma\rceil^{n-d})\\ \Phi(w,z,h,c)=\frac{1}{2^{2(d-e)}}\sum_{u\in\mathbf{F}_2}\sum_{(\lceil\mathbf{x}\rceil^{d-e},\lfloor\mathbf{y}\rfloor^{d-e})\in\mathbf{S}^{(d-e)}_{\substack{u\lhd h\\ w\lhd 0\\ z\lhd c}}(\lceil\alpha\rceil^{d-e},\lfloor\beta\rfloor^{d-e})}\delta^{(d-e)}(\Delta_2\oplus[\gamma]^d_e)\\ \chi(h,c,a,b)=\frac{1}{2^{2e}}\sum_{v\in\mathbf{F}_2}\sum_{([\mathbf{x}]^{n-d-e}_{n-d},\lceil\mathbf{y}\rceil^{e})\in\mathbf{S}^{(e)}_{\substack{h\lhd a\\ v\lhd b\\ c\lhd 1}}([\alpha]^{n-d-e}_{n-d},\lceil\beta\rceil^{e})}\delta^{(e)}(\Delta_1\oplus\lfloor\gamma\rfloor^{e})\end{cases}$$

and

$$\begin{cases}\Delta_1=\lambda^e([x]^{n-d-e}_{n-d},\lceil y\rceil^e,[\alpha]^{n-d-e}_{n-d},\lceil\beta\rceil^e)_{a,b,1}\\ \Delta_2=\lambda^{d-e}(\lceil x\rceil^{d-e},\lfloor y\rfloor^{d-e},\lceil\alpha\rceil^{d-e},\lfloor\beta\rfloor^{d-e})_{h,0,c}\\ \Delta_3=\lambda^{n-d}(\lfloor x\rfloor^{n-d},[y]^{n-e}_{d-e},\lfloor\alpha\rfloor^{n-d},[\beta]^{n-e}_{d-e})_{0,w,z}\end{cases}$$

Proof. According to Lemma 0.5, the $g(x,y)^{(\alpha,\beta)}$ can be divided into three parts, which is illustrated in Figure 10.

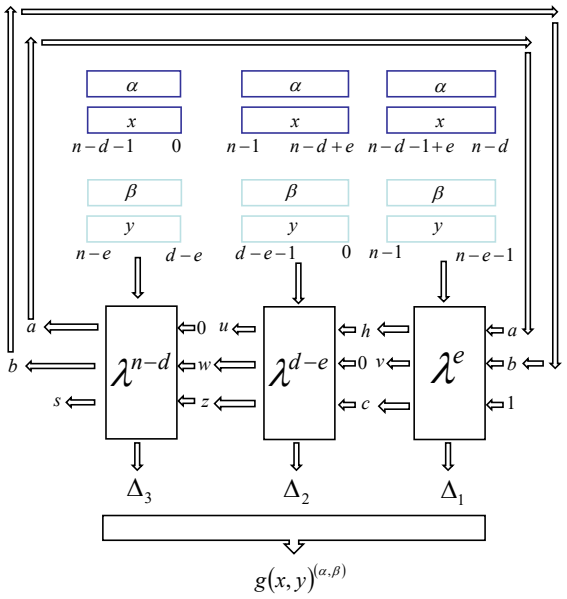


Figure 10. $g(x,y)^{(\alpha,\beta)}$.

Then, we have:

$$\frac{1}{2^{2n}}\sum_{(x,y)\in\mathbf{F}_2^n\times\mathbf{F}_2^n}\delta^n(f(x\boxplus^n\alpha,y\boxplus^n\beta,d,e)\boxminus^n f(x,y,d,e)\oplus\gamma)$$

$$=\frac{1}{2^{2n}}\sum_{(a,h,b,w,c,z,u,v,s)\in\mathbf{F}_2^9}\ \sum_{(x,y)\in\mathbf{S}^{(n-d)}_{\substack{a\lhd 0\\ b\lhd w\\ s\lhd z}}||\mathbf{S}^{(d-e)}_{\substack{u\lhd h\\ w\lhd 0\\ z\lhd c}}||\mathbf{S}^{(e)}_{\substack{h\lhd a\\ v\lhd b\\ c\lhd 1}}(\alpha,\beta)}\delta^n(f(x\boxplus^n\alpha,y\boxplus^n\beta,d,e)\boxminus^n f(x,y,d,e)\oplus\gamma)$$

Due to Lemma 0.3, it can be written as

$$\frac{1}{2^{2n}}\sum_{(a,h,b,w,c,z,u,v,s)\in\mathbf{F}_2^9}\ \sum_{(x,y)\in\mathbf{S}^{(n-d)}_{\substack{a\lhd 0\\ b\lhd w\\ s\lhd z}}||\mathbf{S}^{(d-e)}_{\substack{u\lhd h\\ w\lhd 0\\ z\lhd c}}||\mathbf{S}^{(e)}_{\substack{h\lhd a\\ v\lhd b\\ c\lhd 1}}(\alpha,\beta)}\delta^{(n-d)}(\Delta_3\oplus\lceil\gamma\rceil^{n-d})\,\delta^{(d-e)}(\Delta_2\oplus\lceil\gamma\rceil_e^d)\,\delta^{(e)}(\Delta_1\oplus\lfloor\gamma\rfloor^e)$$

$$=\sum_{(a,h,b,w,c,z,u,v,s)\in\mathbf{F}_2^9}\frac{1}{2^{2(n-d)}}\sum_{(\lfloor\mathbf{x}\rfloor^{n-d},\lfloor\mathbf{y}\rfloor_{d-e}^{n-e})\in\mathbf{S}^{(t)}_{\substack{a\lhd 0\\ b\lhd w\\ s\lhd z}}(\lfloor\alpha\rfloor^{n-d},\lfloor\beta\rfloor_{d-e}^{n-e})}\delta^{(n-d)}(\Delta_3\oplus\lceil\gamma\rceil^{n-d})$$

$$\frac{1}{2^{2(d-e)}}\sum_{(\lceil\mathbf{x}\rceil^{d-e},\lfloor\mathbf{y}\rfloor^{d-e})\in\mathbf{S}^{(d-e)}_{\substack{u\lhd h\\ w\lhd 0\\ z\lhd c}}(\lceil\alpha\rceil^{d-e},\lfloor\beta\rfloor^{d-e})}\delta^{(d-e)}(\Delta_2\oplus\lceil\gamma\rceil_e^d)\ \frac{1}{2^{2e}}\sum_{([\mathbf{x}]_{n-d}^{n-d-e},\lceil\mathbf{y}\rceil^e)\in\mathbf{S}^{(e)}_{\substack{h\lhd a\\ v\lhd b\\ c\lhd 1}}([\alpha]_{n-d}^{n-d-e},\lceil\beta\rceil^e)}\delta^{(e)}(\Delta_2\oplus\lfloor\gamma\rfloor^e)$$

$$=\sum_{(a,h,b,w,c,z)\in\mathbf{F}_2^6}\Psi(a,b,w,z)\Phi(w,z,h,c)\chi(h,c,a,b)$$

□

How to calculate the $\Psi(a,b,w,z)$, $\Phi(w,z,h,c)$ and $\chi(h,c,a,b)$

In this part, we will demonstrate how to calculate the $\Psi(a,b,w,z)$, $\Phi(w,z,h,c)$ and $\chi(h,c,a,b)$.

For $(s, v, u, c, b, a) \in \mathbf{F}_2^6$, let

$$\pi(\alpha_t, \beta_t, \gamma_t)_{4s+2v+u,4c+2b+a} = \sum_{(x,y)\in \mathbf{S}^{(1)}_{\substack{u\lhd a\\ v\lhd b\\ s\lhd c}}(\alpha_t,\beta_t)} \delta^{(1)}(\alpha_t\oplus\beta_t\oplus a\oplus b\oplus c\oplus\gamma_t\oplus 1) = \delta^{(1)}(\alpha_t\oplus\beta_t\oplus a\oplus b\oplus c\oplus\gamma_t\oplus 1)\,\#\mathbf{S}^{(1)}_{\substack{u\lhd a\\ v\lhd b\\ s\lhd c}}(\alpha_t,\beta_t)$$

and matrix $M_{\alpha_t,\beta_t,\gamma_t} = (d'_{4s+2v+u,\ 4c+2b+a})_{8\times 8}$ where

$$d'_{4s+2v+u,\ 4c+2b+a} = \frac{1}{4}\pi(\alpha_t, \beta_t, \gamma_t)_{4s+2v+u,\ 4c+2b+a}.$$

Then, there are eight possible matrices:

$$M_{000} = \frac{1}{4}\begin{pmatrix}01100000\\01000000\\00100000\\00000000\\01104001\\01000001\\00100001\\00000001\end{pmatrix} M_{001} = \frac{1}{4}\begin{pmatrix}40010110\\00010100\\00010010\\00010000\\00000110\\00000100\\00000010\\00000000\end{pmatrix} M_{010} = \frac{1}{4}\begin{pmatrix}10000000\\00000000\\10010000\\00010000\\10000100\\00000100\\10010140\\00010100\end{pmatrix} M_{011} = \frac{1}{4}\begin{pmatrix}01001000\\01000000\\01401001\\01000001\\00001000\\00000000\\00001001\\00000001\end{pmatrix}$$

$$M_{100} = \frac{1}{4}\begin{pmatrix}10000000\\10010000\\00000000\\00010000\\10000010\\10010410\\00000010\\00010010\end{pmatrix} M_{101} = \frac{1}{4}\begin{pmatrix}00101000\\04101001\\00100000\\00100001\\00001000\\00001001\\00000000\\00000001\end{pmatrix} M_{110} = \frac{1}{4}\begin{pmatrix}00000000\\01000000\\00100000\\01100000\\00001000\\01001000\\00101000\\01101004\end{pmatrix} M_{111} = \frac{1}{4}\begin{pmatrix}10000000\\10000100\\10000010\\10040110\\00000000\\00000100\\00000010\\00000110\end{pmatrix}$$

In addition, let

$$F^{(k)}_{(a,b,c)}(\lfloor\alpha\rfloor^k, \lfloor\beta\rfloor^k, \lfloor\gamma\rfloor^k, \lfloor x\rfloor^k, \lfloor y\rfloor^k) = \delta^{(k)}\left(\lambda^k(\lfloor x\rfloor^k, \lfloor y\rfloor^k, \lfloor\alpha\rfloor^k, \lfloor\beta\rfloor^k)_{(a,b,c)} \oplus \lfloor\gamma\rfloor^k\right)$$

For $1 \le k \le n$, let $\mathbf{V}^k = (d^k_{4s+2v+u})_{1\times 8}$ be the column vector, where

$$d_{4s+2v+u} = \frac{1}{2^{2k}} \sum_{(\lfloor x\rfloor^k,\lfloor y\rfloor^k)\in \mathbf{S}^{(k)}_{\substack{u\lhd a\\ v\lhd b\\ s\lhd c}}(\lfloor\alpha\rfloor^k,\lfloor\beta\rfloor^k)} F^{(k)}_{(a,b,c)}(\lfloor\alpha\rfloor^k, \lfloor\beta\rfloor^k, \lfloor\gamma\rfloor^k, \lfloor x\rfloor^k, \lfloor y\rfloor^k)$$

Lemma 0.7. *For* $1 \le k \le n$, $\mathbf{V}^{k+1} = M_{\alpha_k,\beta_k,\gamma_k}\,\mathbf{V}^k$ *and* $\mathbf{V}^1 = M_{\alpha_0,\beta_0,\gamma_0}\mathbf{e}_{4c+2b+a}$.

Proof. For $a', b', c' \in \mathbf{F}_2$, we have:

$$\sum_{(\lfloor x\rfloor^{k+1},\lfloor y\rfloor^{k+1})\in \mathbf{S}^{(k+1)}_{\substack{a'\lhd a\\ b'\lhd b\\ c'\lhd c}}(\lfloor\alpha\rfloor^{k+1},\lfloor\beta\rfloor^{k+1})} F^{(k+1)}_{(a,b,c)}(\lfloor\alpha\rfloor^{k+1}, \lfloor\beta\rfloor^{k+1}, \lfloor\gamma\rfloor^{k+1}, \lfloor x\rfloor^{k+1}, \lfloor y\rfloor^{k+1})$$

$$= \sum_{i,j,z\in\mathbf{F}_2} \sum_{(\lfloor x\rfloor^{k+1},\lfloor y\rfloor^{k+1})\in \mathbf{S}^{(1)}_{\substack{a'\lhd i\\ b'\lhd j\\ c'\lhd z}}(\alpha_{k+1},\beta_{k+1})\|\mathbf{S}^{(k)}_{\substack{i\lhd a\\ j\lhd b\\ z\lhd c}}(\lfloor\alpha\rfloor^k,\lfloor\beta\rfloor^k)} F^{(k+1)}_{(a,b,c)}(\lfloor\alpha\rfloor^{k+1}, \lfloor\beta\rfloor^{k+1}, \lfloor\gamma\rfloor^{k+1}, \lfloor x\rfloor^{k+1}, \lfloor y\rfloor^{k+1})$$

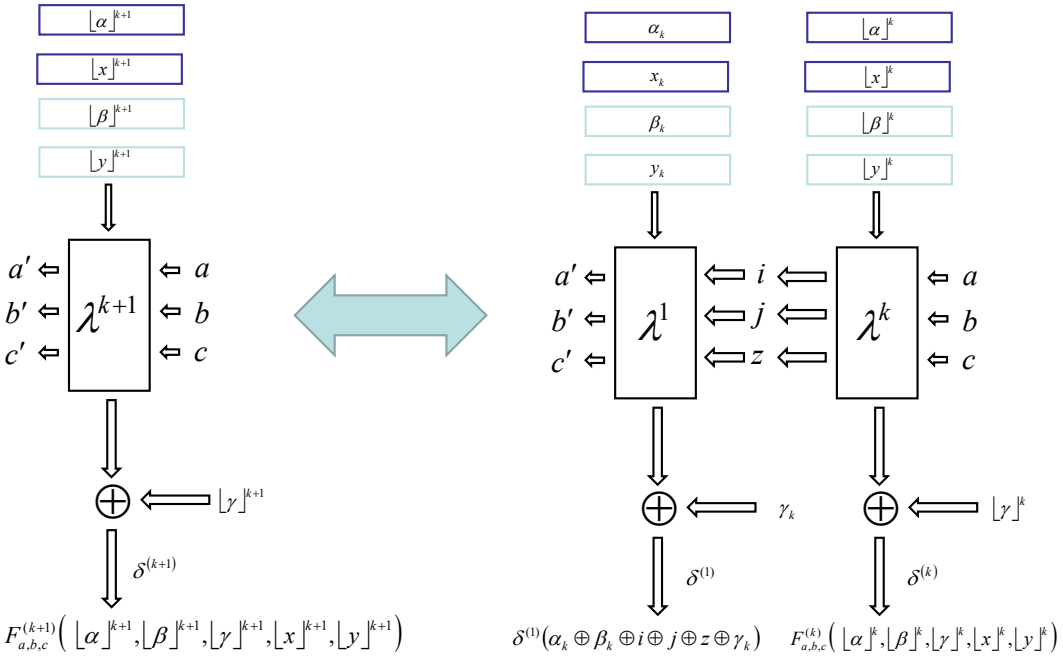


Figure 11. $F^{(k+1)}_{(a,b,c)}(\lfloor\alpha\rfloor^{k+1},\lfloor\beta\rfloor^{k+1},\lfloor\gamma\rfloor^{k+1},\lfloor x\rfloor^{k+1},\lfloor y\rfloor^{k+1})$.

And the $F^{(k+1)}_{(a,b,c)}(\lfloor\alpha\rfloor^{k+1},\lfloor\beta\rfloor^{k+1},\lfloor\gamma\rfloor^{k+1},\lfloor x\rfloor^{k+1},\lfloor y\rfloor^{k+1})$ can be divided into two parts, which is illustrated in Figure 11.

Thus,

$$\sum_{(\lfloor x\rfloor^{k+1},\lfloor y\rfloor^{k+1})\in\mathbf{S}^{(k+1)}_{\substack{a'\lhd a\\ b'\lhd b\\ c'\lhd c}}(\lfloor\alpha\rfloor^{k+1},\lfloor\beta\rfloor^{k+1})} F^{(k+1)}_{(a,b,c)}(\lfloor\alpha\rfloor^{k+1},\lfloor\beta\rfloor^{k+1},\lfloor\gamma\rfloor^{k+1},\lfloor x\rfloor^{k+1},\lfloor y\rfloor^{k+1})$$

$$=\sum_{i,j,z\in\mathbf{F}_2}\left(\sum_{(x,y)\in\mathbf{S}^{(1)}_{\substack{a'\lhd i\\ b'\lhd j\\ c'\lhd z}}(\alpha_k,\beta_k)}\delta^{(1)}(\alpha_k\oplus\beta_k\oplus i\oplus j\oplus z\oplus\gamma_k)\right)\cdot\left(\sum_{(\lfloor x\rfloor^k,\lfloor y\rfloor^k)\in\mathbf{S}^{(k)}_{\substack{i\lhd a\\ j\lhd b\\ z\lhd c}}(\lfloor\alpha\rfloor^k,\lfloor\beta\rfloor^k)}F^{(k)}_{(a,b,c)}(\lfloor x\rfloor^k,\lfloor y\rfloor^k,\lfloor\alpha\rfloor^k,\lfloor\beta\rfloor^k,\lfloor\gamma\rfloor^k)\right)$$

$$=2^{k+1}\sum_{i,j,z\in\mathbf{F}_2}\pi(\alpha_k,\beta_k,\gamma_k)_{4c'+2b'+a',\,4z+2j+i}\cdot d^k_{4z+2j+i}$$

Thus, for $1\le k\le n$, we have $\mathbf{V}^{k+1}=M_{\alpha_k,\beta_k,\gamma_k}\mathbf{V}^k$.

For $\mathbf{V}^1=M_{\alpha_0,\beta_0,\gamma_0}\mathbf{e}_{4c+2b+a}$, it holds from the definition of $\mathbf{V}^1$ and $M_{\alpha_0,\beta_0,\gamma_0}$. □

Then, according to Lemma 0.7, we have:

Lemma 0.8.

$$\psi(a,b,w,z)=\sum_{s\in\mathbf{F}_2}\mathbf{e}^{\mathbf{T}}_{\mathbf{4s+2b+a}}\prod_{i=d}^{n-1}M_{\alpha_{n-d+i\bmod n},\beta_{n-e+i\bmod n},\gamma_i}\,\mathbf{e}_{\mathbf{4z+2w}}$$

Lemma 0.9.

$$\psi(w,z,h,c) = \sum_{u\in\mathbf{F}_2} \mathbf{e}^{\mathbf{T}}_{\mathbf{4z+2w+u}} \prod_{i=e}^{d-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4c+h}}$$

Lemma 0.10.

$$\chi(h,c,a,b) = \sum_{v\in\mathbf{F}_2} \mathbf{e}^{\mathbf{T}}_{\mathbf{4c+2v+h}} \prod_{i=0}^{e-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4+2b+a}}$$

RESULT

According to the lemma in the previous section, we can get the calculation of additive differential probability of ARX construction $\Pr[(\alpha',\beta)\to\gamma]^{ARX}$, which is the main result of our paper:

Theorem 0.2. *For $\alpha,\beta,\gamma\in\mathbf{F}_2^n$, when $d\geq e$, the $\Pr[(\alpha,\beta)\to\gamma]^f$ ($\Pr[(\alpha',\beta)\to\gamma]^{ARX}$, $\alpha=\alpha'\boxplus^n\beta$) can be calculated as:*

$$\sum_{a,b\in\mathbf{F}_2} C^T_{a,b} \prod_{i=d}^{n-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, R_2 \prod_{i=e}^{d-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, R_1 \prod_{i=0}^{e-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4+2b+a}},$$

when $d\leq e$, the $\Pr[(\alpha,\beta)\to\gamma]^f$ ($\Pr[(\alpha',\beta)\to\gamma]^{ARX}$, $\alpha=\alpha'\boxplus^n\beta$) can be calculated as:

$$\sum_{a,b\in\mathbf{F}_2} C^T_{a,b} \prod_{i=e}^{n-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, R_1 \prod_{i=d}^{e-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, R_2 \prod_{i=0}^{d-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4+2b+a}},$$

where

$$R_1 = \sum_{c,h,v\in\mathbf{F}_2} \mathbf{e}_{\mathbf{4c+h}}\, \mathbf{e}^{\mathbf{T}}_{\mathbf{4c+2v+h}}$$
$$R_2 = \sum_{w,z,u\in\mathbf{F}_2} \mathbf{e}_{\mathbf{4z+2w}}\, \mathbf{e}^{\mathbf{T}}_{\mathbf{4z+2w+u}}$$
$$C_{a,b} = \sum_{s\in\mathbf{F}_2} \mathbf{e}_{\mathbf{4s+2b+a}}$$

Proof. When $d \geq e$, according to Lemma 0.6, Lemma 0.8, Lemma 0.9, and Lemma 0.10, we have:

$$
\begin{aligned}
&\Pr[(\alpha,\beta) \to \gamma]^f \\
=& \sum_{(a,h,b,w,c,z)\in\mathbf{F}_2^6} \Psi(a,b,w,z)\Phi(w,z,h,c)\chi(h,c,a,b) \\
=& \sum_{(a,h,b,w,c,z)\in\mathbf{F}_2^6} \sum_{s,u,v\in\mathbf{F}_2} \mathbf{e}_{\mathbf{4s+2b+a}}^{\mathbf{T}} \prod_{i=d}^{n-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4z+2w}}\mathbf{e}_{\mathbf{4z+2w+u}}^{\mathbf{T}} \prod_{i=e}^{d-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4c+h}} \\
&\quad \mathbf{e}_{\mathbf{4c+2v+h}}^{\mathbf{T}} \prod_{i=0}^{e-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4+2b+a}} \\
=& \sum_{a,b\in\mathbf{F}_2} \left(\sum_{s\in\mathbf{F}_2} \mathbf{e}_{\mathbf{4s+2b+a}}^{\mathbf{T}} \right) \prod_{i=d}^{n-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i} \left(\sum_{w,z,u\in\mathbf{F}_2} \mathbf{e}_{\mathbf{4z+2w}}\mathbf{e}_{\mathbf{4z+2w+u}}^{\mathbf{T}} \right) \prod_{i=e}^{d-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i} \\
&\quad \left(\sum_{c,h,v\in\mathbf{F}_2} \mathbf{e}_{\mathbf{4c+h}}\, \mathbf{e}_{\mathbf{4c+2v+h}}^{\mathbf{T}} \right) \prod_{i=0}^{e-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4+2b+a}} \\
=& \sum_{a,b\in\mathbf{F}_2} C_{a,b}^T \prod_{i=d}^{n-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, R_2 \prod_{i=e}^{d-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, R_1 \prod_{i=0}^{e-1} M_{\alpha_{n-d+i \bmod n},\beta_{n-e+i \bmod n},\gamma_i}\, \mathbf{e}_{\mathbf{4+2b+a}}
\end{aligned}
$$

When $d \leq e$, the proof is similarity. □

DISCUSSION

In this paper, we study the additive differential probabilities of ARX construction: $(x \boxplus y) \lll d \oplus y \lll e$. By using an artful partition of $\mathbf{F}_2^m \times \mathbf{F}_2^m$ into subsets, where the elements in each subset fulfill certain equations, we give a method for calculating the additive differential probabilities of ARX constructions. The time complexity of this method is equal to the complexity of $4n$ 8×8 matrix multiplications.

DECLARATIONS

Authors' contributions

Made substantial contributions to the conception and design of the study: Sun S, Hu L
Complete the proof of Theorem 0.2: Niu Z

Availability of data and materials

Not applicable.

Financial support and sponsorship

This work is supported by the National Key Research and Development Program of China (2022YFB2701900), the Natural Science Foundation of China (62032014), and the Fundamental Research Funds for the Central Universities.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

REFERENCES

1. Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK families of lightweight block ciphers. *IACR Cryptol ePrint Arch* 2013:404. Available from: http://eprint.iacr.org/2013/404.
2. Dinu D, Perrin L, Udovenko A, et al. Design strategies for ARX with provable bounds: sparx and LAX. In: Cheon JH, Takagi T, editors. Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I. vol. 10031 of Lecture Notes in Computer Science; 2016. pp. 484–513. DOI
3. Bernstein DJ. The Salsa20 family of stream ciphers. *Lectu Note Comput Sci* 2008;4986:179–90. Available from: http://dx.doi.org/10.1007/978-3-540-68351-3_8
4. Bernstein DJ. ChaCha, a variant of Salsa20. Available from: https://cr.yp.to/chacha/chacha-20080120.pdf.
5. Beierle C, Biryukov A, dos Santos LC, et al. Alzette: A 64-Bit ARX-box - (Feat. CRAX and TRAX). In: Micciancio D, Ristenpart T, editors. Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III. vol. 12172 of Lecture Notes in Computer Science. Springer; 2020. pp. 419–48. DOI
6. Beierle C, Biryukov A, dos Santos LC, et al. Lightweight AEAD and Hashing using the Sparkle Permutation Family. *IACR Trans Symmetric Cryptol* 2020;2020:208–61. DOI
7. Mouha N, Mennink B, Herrewege AV, et al. Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In: Joux A, Youssef AM, editors. Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers. vol. 8781 of Lecture Notes in Computer Science. Springer; 2014. pp. 306–23. DOI
8. Aumasson J, Bernstein DJ. SipHash: A fast short-input PRF. In: Galbraith SD, Nandi M, editors. Progress in Cryptology - INDOCRYPT 2012, 13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012. Proceedings. vol. 7668 of Lecture Notes in Computer Science. Springer; 2012. pp. 489–508. DOI
9. Aumasson JP, Henzen L, Meier W, Phan CW. SHA3 proposal BLAKE, 2008. Available from: https://www.scinapse.io/papers/200599792
10. Callas J, Com J, Walker J. The Skein Hash Function Family 2010. Available from: https://www.schneier.com/academic/skein/
11. Velichkov V, Mouha N, Cannière CD, Preneel B. UNAF: A special set of additive differences with application to the differential analysis of ARX. In: Canteaut A, editor. Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers. vol. 7549 of Lecture Notes in Computer Science. Springer; 2012. pp. 287–305. DOI
12. Lipmaa H. On differential properties of pseudo-hadamard transform and related mappings. In: Menezes A, Sarkar P, editors. Progress in Cryptology - INDOCRYPT 2002, Third International Conference on Cryptology in India, Hyderabad, India, December 16-18, 2002. vol. 2551 of Lecture Notes in Computer Science. Springer; 2002. pp. 48–61. DOI
13. Wallén J. Linear approximations of addition modulo 2^n. In: Johansson T, editor. Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers. vol. 2887 of Lecture Notes in Computer Science. Springer; 2003. pp. 261–73. DOI
14. Ashur T, Liu Y. Rotational cryptanalysis in the presence of constants. *IACR Trans Symmetric Cryptol* 2016;2016:57–70. DOI
15. Mouha N, Velichkov V, Cannière CD, Preneel B. The differential analysis of S-functions. In: Biryukov A, Gong G, Stinson DR, editors. Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers. vol. 6544 of Lecture Notes in Computer Science. Springer; 2010. pp. 36–56. DOI
16. Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. In: Menezes A, Vanstone SA, editors. Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings. vol. 537 of Lecture Notes in Computer Science. Springer; 1990. pp. 2–21. DOI
17. Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. *J Cryptol* 1991;4:3–72. DOI
18. Lipmaa H, Moriai S. Efficient algorithms for computing differential properties of addition. In: Matsui M, editor. Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers. vol. 2355 of Lecture Notes in Computer Science. Springer; 2001. pp. 336–50. DOI
19. Lipmaa H, Wallén J, Dumas P. On the additive differential probability of exclusive-or. In: Roy BK, Meier W, editors. Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers. vol. 3017 of Lecture Notes in Computer Science. Springer; 2004. pp. 317–31. DOI
20. Velichkov V, Mouha N, Cannière CD, Preneel B. The additive differential probability of ARX. In: Joux A, editor. Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers. vol. 6733 of Lecture Notes in Computer Science. Springer; 2011. pp. 342–58. DOI

21. Niu Z, Sun S, Liu Y, Li C. Rotational differential-linear distinguishers of ARX ciphers with arbitrary output linear masks. In: Dodis Y, Shrimpton T, editors. Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I. vol. 13507 of Lecture Notes in Computer Science. Springer; 2022. pp. 3–32. DOI