ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

2023 Математические методы криптографии № 60

УДК 519.7 DOI 10.17223/20710410/60/5

ON ADDITIVE DIFFERENTIAL PROBABILITIES OF A COMPOSITION OF BITWISE XORS[1]

I. A. Sutormin*, N. A. Kolomeec**

*_Novosibirsk State University, Novosibirsk, Russia_
**_Sobolev Institute of Mathematics, Novosibirsk, Russia_

E-mail: ivan.sutormin@gmail.com, kolomeec@math.nsc.ru

We study the additive differential probabilities $\mathrm{adp}_k^{\oplus}$ of compositions of $k-1$ bitwise XORs. For vectors $\alpha^1,\ldots,\alpha^{k+1} \in \mathbb{Z}_2^n$, it is defined as the probability of transformation input differences $\alpha^1,\ldots,\alpha^k$ to the output difference α^{k+1} by the function $x^1 \oplus \ldots \oplus x^k$, where $x^1,\ldots,x^k \in \mathbb{Z}_2^n$ and $k \geqslant 2$. It is used for differential cryptanalysis of symmetric-key primitives, such as Addition-Rotation-XOR constructions. Several results which are known for $\mathrm{adp}_2^{\oplus}$ are generalized for $\mathrm{adp}_k^{\oplus}$. Some argument symmetries are proven for $\mathrm{adp}_k^{\oplus}$. Recurrence formulas which allow us to reduce the dimension of the arguments are obtained. All impossible differentials as well as all differentials of $\mathrm{adp}_k^{\oplus}$ with the probability 1 are found. For even k, it is proven that $\max\limits_{\alpha^1,\ldots,\alpha^k} \mathrm{adp}_k^{\oplus}(\alpha^1,\ldots,\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(0,\ldots,0,\alpha^{k+1} \to \alpha^{k+1})$. Matrices that can be used for efficient calculating $\mathrm{adp}_k^{\oplus}$ are constructed. It is also shown that the cases of even and odd k differ significantly.

Keywords: _ARX, XOR, additive differential probabilities, differential cryptanalysis._

РАЗНОСТНЫЕ ХАРАКТЕРИСТИКИ ПО МОДУЛЮ 2^n КОМПОЗИЦИИ НЕСКОЛЬКИХ ПОБИТОВЫХ ИСКЛЮЧАЮЩИХ ИЛИ

И. А. Сутормин*, Н. А. Коломеец**

*_Новосибирский государственный университет, г. Новосибирск, Россия_
**_Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия_

Исследуются разностные характеристики $\mathrm{adp}_k^{\oplus}$ по модулю 2^n композиции $k-1$ побитовых XOR. Для векторов $\alpha^1,\ldots,\alpha^{k+1} \in \mathbb{Z}_2^n$ они определяются как вероятность преобразования функцией $x^1 \oplus \ldots \oplus x^k$ входных разностей $\alpha^1,\ldots,\alpha^k$ в выходную разность α^{k+1}, где $x^1,\ldots,x^k \in \mathbb{Z}_2^n$ и $k \geqslant 2$. Данные характеристики используются при разностном криптоанализе симметричных алгоритмов, в том числе ARX-конструкций, использующих только три операции: сложение по модулю 2^n, побитовый XOR и циклический сдвиг битов. Показано, что многие свойства, известные для $\mathrm{adp}_2^{\oplus}$, обобщаются на $\mathrm{adp}_k^{\oplus}$. Доказаны симметрии аргументов $\mathrm{adp}_k^{\oplus}$. Получены рекуррентные формулы, позволяющие уменьшить на 1 размерность аргументов n. Найдены все несовместные разности и все разности, при которых $\mathrm{adp}_k^{\oplus}$ равна 1. Для чётного k доказано, что $\max\limits_{\alpha^1,\ldots,\alpha^k \in \mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(\alpha^1,\ldots,\alpha^k \to \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(0,\ldots,0,\alpha^{k+1} \to \alpha^{k+1})$. Построены матрицы, которые можно

[1] The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. FWNF–2022–0018).

использовать для вычисления $\mathrm{adp}_k^{\oplus}$ за линейное по n время. Показано, что случаи чётного и нечётного k существенно различаются.

Ключевые слова: *ARX, XOR, разностные характеристики, сложение по модулю, разностный криптоанализ.*

1. Introduction

Symmetric cryptography is used in many areas in the modern world: for fast data encryption (block and stream ciphers), for checking data integrity, for creating an electronic signature (cryptographic hash functions), etc. ARX is one of the constructions being used to develop these algorithms. All cryptographic primitives of this architecture use only three operations: addition modulo 2^n (Addition, $\boxplus$), circular shift (Rotation, $\lll$) and bitwise addition modulo 2 (XOR, $\oplus$). Examples of ARX-based ciphers include the block ciphers FEAL [1], Threefish [2], one of the eSTREAM winners, the stream cipher Salsa20 [3] and its modification ChaCha20 [4] (it is a part of TLS 1.3), as well as SHA-3 finalists hash functions BLAKE [5] and Skein [2]. One of the well known problems of ARX ciphers is the complexity of their differential cryptanalysis.

Differential cryptanalysis is a statistical method for the analysis of symmetric-key primitives. It was proposed by E. Biham and A. Shamir in [6]. This attack uses pairs of the input differences ΔP and output differences ΔC with a high probability of ccurrence. The ordered pair (ΔP, ΔC) is called a differential. A common way to find such differential with a high probability is to construct a differential trail, i.e., a sequence ($\Delta P = \Delta X_0$, $\Delta X_1, \ldots, \Delta X_p$, $\Delta C = \Delta X_{p+1}$), where $\Delta X_1, \ldots, \Delta X_p$ are some intermediate values that would occur after some operations. A common technique to construct a differential trail is to use a “greedy” strategy to pick the intermediate differences ΔX_{i+1} which have the highest probability of occurring for fixed ΔX_i. Under some assumptions, we can multiply all the probabilities of a differential trail and obtain an estimation for the probability of the differential $(\Delta P, \Delta C)$.

As for ARX ciphers, the difference Δ is typically one of their basic operations (addition or XOR). There are also approaches that use other Δ or even several different Δ, see, for instance, [7–10]. If we express the differences using addition modulo 2^n, the additive differential probabilities are what we need. For an arbitrary function $f : (\mathbb{Z}_2^n)^k \to \mathbb{Z}_2^n$ the probability $\mathrm{adp}^f(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$, where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$, is defined as

$$\frac{1}{2^{nk}} \left|\{x^1, \ldots, x^k \in \mathbb{Z}_2^n : f(x^1 \boxplus \alpha^1, \ldots, x^k \boxplus \alpha^k) = f(x^1, \ldots, x^k) \boxplus \alpha^{k+1}\}\right|.$$

However, the probability obtained by “greedy” strategy may be significantly different from the real one. For instance, even simple composition $x \oplus y \oplus z$ can produce a high error. Let us choose the input differences α, 0, 0 for the first, second and third arguments respectively. Then the “greedy” strategy gives us

$$\mathrm{P} = \mathrm{adp}^{\oplus}(\alpha, 0 \to \Delta X_1) \cdot \mathrm{adp}^{\oplus}(\Delta X_1, 0 \to \Delta X_2).$$

It is known [11] that $\max\limits_{\gamma} \mathrm{adp}^{\oplus}(\alpha, 0 \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, 0 \to \alpha)$. Thus, we should choose $\Delta X_1 = \alpha$ and then $\Delta X_2 = \alpha$ and obtain the result $P = (\mathrm{adp}^{\oplus}(\alpha, 0 \to \alpha))^2$. At the same time, the function is symmetric, i.e., we can swap the first and the last arguments without changing the value/probabilities:

$$\mathrm{P} = \mathrm{adp}^{\oplus}(0, 0 \to \Delta X_1) \cdot \mathrm{adp}^{\oplus}(\Delta X_1, \alpha \to \Delta X_2).$$

But $\mathrm{adp}^{\oplus}(0,0 \to 0) = 1$ is obviously the maximum value and $\max\limits_{\beta,\gamma} \mathrm{adp}^{\oplus}(\beta,\alpha \to \gamma) = = \mathrm{adp}^{\oplus}(0,\alpha \to \alpha) = \mathrm{adp}^{\oplus}(\alpha,0 \to \alpha)$. In this case, the "greedy" strategy gives us a different result: $\mathrm{P} = \mathrm{adp}^{\oplus}(\alpha,0 \to \alpha)$.

Thus, if we apply this for the function $x^1 \oplus x^2 \oplus \ldots \oplus x^k$, we obtain two different results: $\mathrm{P} = (\mathrm{adp}^{\oplus}(\alpha,0 \to \alpha))^k$ and $\mathrm{P} = \mathrm{adp}^{\oplus}(\alpha,0 \to \alpha)$. We can make the difference between them as big as we want by choosing α and k. Similar examples for other compositions can be found in [12].

One of the possible ways to reduce the error is to use the differential probabilities for the whole composition $x^1 \oplus \ldots \oplus x^k$:

$$\mathrm{adp}^{\oplus}_k(\alpha^1,\ldots,\alpha^k \to \alpha^{k+1}) = \frac{1}{2^{nk}} \left| \{x^1,\ldots,x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k}(\alpha^i \boxplus x^i) = \alpha^{k+1} \boxplus \bigoplus_{i=1}^{k} x^i\} \right|,$$

where $\alpha^1,\ldots,\alpha^{k+1} \in \mathbb{Z}_2^n$. Though it is difficult to meet this operation for large k in real ciphers, at least $x^1 \oplus x^2 \oplus x^3$ is used, for instance, in EDON-R [13].

In this paper, we study the properties of $\mathrm{adp}^{\oplus}_k$. As a rule, $n = 32$ is used in ARX constructions that makes an exhaustive search inefficient. We generalize results obtained in [11, 14] for $\mathrm{adp}^{\oplus} = \mathrm{adp}^{\oplus}_2$. Symmetries, impossible differentials, maximums, where one of the arguments is fixed, are considered. All these things are interesting for constructing differential trails. In [14] a way to compute $\mathrm{adp}^{\oplus}$ in linear time multiplying special matrices was proposed. It was also generalized in [15]. We describe special matrices that can be used for calculating $\mathrm{adp}^{\oplus}_k$.

The outline. Section 2 gives us necessary definitions. In Section 3, symmetries of $\mathrm{adp}^{\oplus}_k$ are proven (Theorem 1). Section 4 contains recurrence formulas that can be used to reduce the dimension of the arguments (Theorem 2). All impossible differentials (Theorem 3) and all differentials with the probability 1 (Theorem 4) are found in Section 5 (see also Remark 3). Section 6 provides maximums of the $\mathrm{adp}^{\oplus}_k$, where one of its argument is fixed and k is even (Theorem 5). In Section 7, matrices that allow us to calculate $\mathrm{adp}^{\oplus}_k$ are constructed (Theorem 6 and eq. (6)). We note that the cases of even and odd k significantly differ. Some operations are not symmetries for odd k. The structure of the matrices is a little bit more complex for odd k. The maximums for odd k do not generalize the maximums for $k = 2$.

2. Definitions

Let $\mathbb{Z}_2^n$ be a vector space of dimension n over a field consisting of two elements. Let $x = (x_1,\ldots,x_n)$ and $y = (y_1,\ldots,y_n)$ be elements of $\mathbb{Z}_2^n$. Then $x1$ and $x0$ are the vectors $(x_1,\ldots,x_n,1)$ and $(x_1,\ldots,x_n,0)$ from $\mathbb{Z}_2^{n+1}$ respectively. The bitwise XOR is denoted by $x \oplus y$. Also, $\overline{x} = (x_1 \oplus 1,\ldots,x_n \oplus 1) \in \mathbb{Z}_2^n$. We say that $y \preceq x$ if $y_i \leqslant x_i$ for all i, $1 \leqslant i \leqslant n$. We denote *the Hamming weight* of the vector x by $\mathrm{wt}(x)$. We associate the vector x with the integer $x_1 2^{n-1} + x_2 2^{n-2} + \ldots + x_n$. Thus, $x \boxplus y = (x+y) \bmod 2^n$, where x and y are considered as the corresponding integers. Also, $-x$ is the vector from $\mathbb{Z}_2^n$ whose corresponding integer is $-x \bmod 2^n$.

Additive differential probability of the function $f(x^1,\ldots,x^k) = x^1 \oplus \ldots \oplus x^k$, $x^1,\ldots,x^k \in \in \mathbb{Z}_2^n$, for *a differential* $\alpha^1,\ldots,\alpha^{k+1} \in \mathbb{Z}_2^n$ is defined as

$$\mathrm{adp}^{\oplus}_k(\alpha^1,\ldots,\alpha^k \to \alpha^{k+1}) = \frac{1}{2^{nk}} \left| \{x^1,\ldots,x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k}(\alpha^i \boxplus x^i) = \alpha^{k+1} \boxplus \bigoplus_{i=1}^{k} x^i\} \right|. \quad (1)$$

Also, we denote $\mathrm{adp}^{\oplus}_2$ by $\mathrm{adp}^{\oplus}$. Hereinafter we assume that $k \geqslant 2$.

3. Argument symmetries of $\mathrm{adp}_k^{\oplus}$

Argument symmetries were proven for $\mathrm{adp}^{\oplus}$ in [11]. In this Section, we generalize that result for $\mathrm{adp}_k^{\oplus}$, $k \geqslant 3$. It is straightforward that we can rearrange $\alpha^1,\dots,\alpha^k$ calculating $\mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^k \to \alpha^{k+1})$, see the definition of $\mathrm{adp}_k^{\oplus}$. Let us show that we can rearrange all $\alpha^1,\dots,\alpha^{k+1}$.

Proposition 1. For any $\alpha^1,\dots,\alpha^{k+1} \in \mathbb{Z}_2^n$ and $j \in \{1,\dots,k\}$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^j,\dots,\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^{k+1},\dots,\alpha^k \to \alpha^j).$$

In other words, $\mathrm{adp}_k^{\oplus}$ is symmetric.

Proof. Since we can rearrange the arguments $\alpha^1,\dots,\alpha^k$, we can only show that

$$\mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^{k+1},\alpha^2,\dots,\alpha^k \to \alpha^1).$$

Substituting in (1) $\bigoplus\limits_{i=1}^{k} x^i = y^1$, $x^i = y^i$ for all $i = 2,\dots,k$, we get that

$$\frac{1}{2^{nk}}\left|\left\{y^1,\dots,y^k \in \mathbb{Z}_2^n : \left(\left(\bigoplus_{i=1}^{k} y^i\right) \boxplus \alpha^1\right) \oplus \bigoplus_{i=2}^{k}(\alpha^i \boxplus y^i) = y^1 \boxplus \alpha^{k+1}\right\}\right|,$$

which is equivalent to

$$\frac{1}{2^{nk}}\left|\left\{y^1,\dots,y^k \in \mathbb{Z}_2^n : (y^1 \boxplus \alpha^{k+1}) \oplus \bigoplus_{i=1}^{k}(\alpha^i \boxplus y^i) = \left(\bigoplus_{i=1}^{k} y^i\right) \boxplus \alpha^1\right\}\right|.$$

We have the definition of $\mathrm{adp}_k^{\oplus}(\alpha^{k+1},\alpha^2,\dots,\alpha^k \to \alpha^1)$. ■

Proposition 2. For any $\alpha^1,\dots,\alpha^{k+1} \in \mathbb{Z}_2^n$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 2^{n-1},\alpha^2 \boxplus 2^{n-1},\alpha^3,\dots,\alpha^k \to \alpha^{k+1}).$$

Proof. It is not difficult to see that $a \boxplus 2^{n-1} = a \oplus 2^{n-1}$ since the vector $2^{n-1} \in \mathbb{Z}_2^n$ has 1 only in the most significant position. We can transform the condition from the definition of $\mathrm{adp}_k^{\oplus}$:

$$\begin{aligned}(\alpha^1 \boxplus x^1) \oplus (\alpha^2 \boxplus x^2) &= (\alpha^1 \boxplus x^1) \oplus 2^{n-1} \oplus (\alpha^2 \boxplus x^2) \oplus 2^{n-1} = \\ &= (\alpha^1 \boxplus x^1 \boxplus 2^{n-1}) \oplus (\alpha^2 \boxplus x^2 \boxplus 2^{n-1}) = \\ &= \big((\alpha^1 \boxplus 2^{n-1}) \boxplus x^1\big) \oplus \big((\alpha^2 \boxplus 2^{n-1}) \boxplus x^2\big).\end{aligned}$$

There is no need to change the terms containing $\alpha^3,\dots,\alpha^{k+1}$. ■

Proposition 3. For any $\alpha^1,\dots,\alpha^{k+1} \in \mathbb{Z}_2^n$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(-\alpha^1,\dots,-\alpha^k \to -\alpha^{k+1}).$$

Proof. By definition,

$$\begin{aligned}\mathrm{adp}_k^{\oplus}(\alpha^1,\dots,\alpha^k \to \alpha^{k+1}) &= \frac{1}{2^{nk}}\left|\left\{x^1,\dots,x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k}(\alpha^i \boxplus x^i) = \left(\bigoplus_{i=1}^{k} x^i\right) \boxplus \alpha^{k+1}\right\}\right| = \\ &= \frac{1}{2^{nk}}\left|\left\{x^1,\dots,x^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k} x^i = \bigoplus_{i=1}^{k}(\alpha^i \boxplus x^i) \boxplus -\alpha^{k+1}\right\}\right|.\end{aligned}$$

Substituting $y^i = x^i \boxplus \alpha^i$ for all $i = 1, \ldots, k$ and using $x^i = y^i \boxplus -\alpha^i$, we can rewrite the definition:

$$\frac{1}{2^{nk}} \left| \left\{ y^1, \ldots, y^k \in \mathbb{Z}_2^n : \bigoplus_{i=1}^{k} (-\alpha^i \boxplus y^i) = \left(\bigoplus_{i=1}^{k} y^i \right) \boxplus -\alpha^{k+1} \right\} \right|.$$

We have got exactly $\mathrm{adp}_k^{\oplus}(-\alpha^1, \ldots, -\alpha^k \to -\alpha^{k+1})$. ■

Proposition 4. For any $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(-\alpha^1, -\alpha^2, \alpha^3, \ldots, \alpha^k \to \alpha^{k+1}).$$

Proof. First of all, we show that $-x = \overline{x} \boxplus 1$ for any $x \in \mathbb{Z}_2^n$:

$$-x = (2^n - 1 - x) \boxplus 1 = \overline{x} \boxplus 1.$$

Therefore, $\overline{x} = -x \boxplus -1$ and for any $y \in \mathbb{Z}_2^n$

$$\overline{x \boxplus y} = -(x \boxplus y) \boxplus -1 = -x \boxplus -1 \boxplus -y = \overline{x} \boxplus -y.$$

It is easy to see that for any bits $x_i, y_i \in \mathbb{Z}_2$ the equality $\overline{x_i} \oplus \overline{y_i} = x_i \oplus y_i$ holds. Therefore, for any $x, y \in \mathbb{Z}_2^n$ it holds that $\overline{x} \oplus \overline{y} = x \oplus y$. Now, we transform the condition from the definition of $\mathrm{adp}_k^{\oplus}$:

$$(\alpha^1 \boxplus x^1) \oplus (\alpha^2 \boxplus x^2) = (\overline{\alpha^1 \boxplus x^1}) \oplus (\overline{\alpha^2 \boxplus x^2}) = (-\alpha^1 \boxplus \overline{x^1}) \oplus (-\alpha^2 \boxplus \overline{x^2}).$$

Using $y^i = \overline{x^i}$ for $i = 1, 2$, we obtain the following:

$$(-\alpha^1 \boxplus y^1) \oplus (-\alpha^2 \boxplus y^2).$$

We have got the condition from the definition of $\mathrm{adp}_k^{\oplus}(-\alpha^1, -\alpha^2, \alpha^3, \ldots, \alpha^k \to \alpha^{k+1})$. ■

Finally, Propositions 1–4 give us the following theorem.

Theorem 1. Let $k \geqslant 2$, $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ and $\beta^1, \ldots, \beta^{k+1} \in \mathbb{Z}_2^n$. Then

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\beta^1, \ldots, \beta^k \to \beta^{k+1})$$

if $\beta^1, \ldots, \beta^{k+1}$ are any of the following:

1) $\beta^i = \alpha^{\pi(i)}$ for all i, $1 \leqslant i \leqslant k+1$, where π is a permutation on the set $\{1, \ldots, k+1\}$;
2) for arbitrary $S \subseteq \{1, \ldots, k+1\}$, where $|S|$ is even,

$$\beta^i = \alpha^i \boxplus 2^{n-1} \text{ for all } i \in S \text{ and } \beta^i = \alpha^i \text{ for all } i \in \{1, \ldots, k+1\} \setminus S;$$

3) for arbitrary $S \subseteq \{1, \ldots, k+1\}$, where $|S|$ is even,

$$\beta^i = -\alpha^i \text{ for all } i \in S \text{ and } \beta^i = \alpha^i \text{ for all } i \in \{1, \ldots, k+1\} \setminus S;$$

4) if k is even, for arbitrary $S \subseteq \{1, \ldots, k+1\}$

$$\beta^i = -\alpha^i \text{ for all } i \in S \text{ and } \beta^i = \alpha^i \text{ for all } i \in \{1, \ldots, k+1\} \setminus S.$$

Proof. The first point directly follows from Proposition 1. To prove the second point, we just need to apply $|S|/2$ times Proposition 2 together with the first point. The same applies to the third point: it is sufficient to use Proposition 4 instead of Proposition 2. Let us prove the last point. Since k is even, the third point guaranties that

$$\mathrm{adp}_k^{\oplus}(\alpha^1,\ldots,\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(-\alpha^1,\ldots,-\alpha^k \to \alpha^{k+1}).$$

By Proposition 3,

$$\mathrm{adp}_k^{\oplus}(-\alpha^1,\ldots,-\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1,\ldots,\alpha^k \to -\alpha^{k+1}),$$

which implies that

$$\mathrm{adp}_k^{\oplus}(\alpha^1,\ldots,\alpha^k \to \alpha^{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha^1,\ldots,\alpha^k \to -\alpha^{k+1}).$$

Applying this equality $|S|$ times together with the first point gives us the last point. ■

4. Recurrence formulas for the $\mathrm{adp}_k^{\oplus}$

The recurrence formulas for the $\mathrm{adp}^{\oplus}$ obtained in [11] can be generalized for $\mathrm{adp}_k^{\oplus}$. Note that all our further results will use them.

Theorem 2. For all $\alpha^1,\ldots,\alpha^{k+1} \in \mathbb{Z}_2^n$, $k \geqslant 2$, and a vector of the least significant bits $A \in \mathbb{Z}_2^{k+1}$ the following holds:

1) if $\mathrm{wt}(A)$ is odd, then

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1,\ldots,\alpha^k A_k \to \alpha^{k+1}A_{k+1}) = 0; \tag{2}$$

2) if k is odd and $A = (1,\ldots,1) = 2^{k+1}-1$, then

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1,\ldots,\alpha^k A_k \to \alpha^{k+1}A_{k+1}) = \\ = \frac{1}{2^k} \sum_{\substack{B\in\mathbb{Z}_2^{k+1},\\ \mathrm{wt}(B)\text{ is even}}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1,\ldots,\alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}); \tag{3}$$

3) otherwise

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1,\ldots,\alpha^k A_k \to \alpha^{k+1}A_{k+1}) = \\ = \frac{1}{2^{\mathrm{wt}(A)}} \sum_{\substack{B\in\mathbb{Z}_2^{k+1},\\ B\preceq A}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1,\ldots,\alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}). \tag{4}$$

Note that $\alpha^i \boxplus B_i$ is the addition modulo 2^n, i.e., α^i determines n, $1 \leqslant i \leqslant k+1$.

Proof.

1) Let us prove that $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1,\ldots,\alpha^k A_k \to \alpha^{k+1}A_{k+1}) = 0$ if $\mathrm{wt}(A)$ is odd. First of all, we define $odd(x) = x_{n+1}$ for $x \in \mathbb{Z}_2^{n+1}$, i.e., $odd(x) = 1$ if and only if x is odd as integer. It is clear that $odd(x \boxplus y) = odd(x \oplus y) = odd(x) \oplus odd(y)$. By definition,

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1,\ldots,\alpha^k A_k \to \alpha^{k+1}A_{k+1}) = \\ = \frac{1}{2^{(n+1)k}} \left|\left\{x^1,\ldots,x^k \in \mathbb{Z}_2^{n+1} : \bigoplus_{i=1}^{k}(x^i \boxplus \alpha^i A_i) = \bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1}A_{k+1}\right\}\right|.$$

Since $\mathrm{wt}(A)$ is odd,

$$odd(\left(\bigoplus_{i=1}^{k}(x^i \boxplus \alpha^i A_i)\right) \oplus \left(\bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1} A_{k+1}\right)) = \bigoplus_{i=1}^{k} odd(x^i) \oplus \bigoplus_{i=1}^{k} odd(x^i) \oplus \bigoplus_{i=1}^{k+1} A_i = 1.$$

It implies that for any $x^1, \ldots, x^k \in \mathbb{Z}_2^{n+1}$

$$\bigoplus_{i=1}^{k}(x^i \boxplus \alpha^i A_i) \neq \bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1} A_{k+1}.$$

In other words, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 0$ since the condition from its definition cannot be satisfied.

2) Let us prove the equality (3). We rewrite the definition of $\mathrm{adp}_k^{\oplus}$ as

$$\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1) =$$
$$= \frac{1}{2^{(n+1)k}} \left| \left\{ x^1, \ldots, x^k \in \mathbb{Z}_2^n,\ a_1, \ldots, a_k \in \mathbb{Z}_2 : \bigoplus_{i=1}^{k}(\alpha^i 1 \boxplus x^i a_i) = \left(\bigoplus_{i=1}^{k} x^i a_i\right) \boxplus \alpha^{k+1} 1 \right\} \right|.$$

We fix a tuple $a_1, \ldots, a_k$. Using Proposition 1, we rearrange the $\mathrm{adp}_k^{\oplus}$ arguments so that $a_1 = a_2 = \ldots = a_j = 0$ and $a_{j+1} = \ldots = a_k = 1$ for some $j \leqslant k$. Then we rewrite the condition from the definition:

$$\bigoplus_{i=1}^{j}(\alpha^i 1 \boxplus x^i 0) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i 1 \boxplus x^i 1) = \left(\bigoplus_{i=1}^{j} x^i 0 \oplus \bigoplus_{i=j+1}^{k} x^i 1\right) \boxplus \alpha^{k+1} 1 =$$
$$= \left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i) 1\right) \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1) 0\right) = \left(\bigoplus_{i=1}^{j} x^i 0 \ \oplus \bigoplus_{i=j+1}^{k} x^i 1\right) \boxplus \alpha^{k+1} 1.$$

In the case of even j, we can rewrite the condition from the definition as

$$\left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i)\right) 0 \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1)\right) 0 = \left(\bigoplus_{i=1}^{j} x^i \ \oplus \bigoplus_{i=j+1}^{k} x^i\right) 1 \boxplus \alpha^{k+1} 1,$$
$$\left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i)\right) 0 \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1)\right) 0 = \left(\left(\bigoplus_{i=1}^{j} x^i \oplus \bigoplus_{i=j+1}^{k} x^i\right) \boxplus \alpha^{k+1} \boxplus 1\right) 0.$$

Now look at the corresponding condition from the definition of $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^j, \alpha^{j+1} \boxplus 1, \ldots, \alpha^k \boxplus 1 \to \alpha^{k+1} \boxplus 1)$:

$$\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1) = \left(\bigoplus_{i=1}^{j} x^i \oplus \bigoplus_{i=j+1}^{k} x^i\right) \boxplus \alpha^{k+1} \boxplus 1.$$

It is easy to see that if a tuple $x^1, \ldots, x^k$ satisfies one of these conditions, then it must also satisfy the other.

In the case of odd j, we can rewrite the condition from the definition as

$$\left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i)\right) 1 \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1)\right) 0 = \left(\bigoplus_{i=1}^{j} x^i \ \oplus \bigoplus_{i=j+1}^{k} x^i\right) 0 \boxplus \alpha^{k+1} 1,$$
$$\left(\bigoplus_{i=1}^{j}(\alpha^i \boxplus x^i)\right) 1 \oplus \left(\bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i \boxplus 1)\right) 0 = \left(\left(\bigoplus_{i=1}^{j} x^i \oplus \bigoplus_{i=j+1}^{k} x^i\right) \boxplus \alpha^{k+1}\right) 1.$$

Now look at the corresponding condition from the definition of $\mathrm{adp}^{\oplus}_k(\alpha^1,\ldots,\alpha^j,\alpha^{j+1}\boxplus 1,\ldots,\alpha^k\boxplus 1\to\alpha^{k+1})$:

$$\bigoplus_{i=1}^{j}(\alpha^i\boxplus x^i)\oplus\bigoplus_{i=j+1}^{k}(\alpha^i\boxplus x^i\boxplus 1)=\left(\bigoplus_{i=1}^{j}x^i\oplus\bigoplus_{i=j+1}^{k}x^i\right)\boxplus\alpha^{k+1}.$$

It is easy to see that if a tuple $x^1,\ldots,x^k$ satisfies one of these conditions, then it must also satisfy the other.

The total number of tuples satisfying the conditions from the definitions for vectors of dimension $n+1$ is $2^{(n+1)k}\mathrm{adp}^{\oplus}_k(\alpha^1 1,\ldots,\alpha^k 1\to\alpha^{k+1}1)$, and for vectors of dimension n it is equal to $2^{nk}\mathrm{adp}^{\oplus}_k(\alpha^1,\ldots,\alpha^k\to\alpha^{k+1})$. For every fixed tuple $a_1,\ldots,a_k$, there is a unique $\mathrm{adp}^{\oplus}_k$ such that x^ia_i and x^i, $1\leqslant i\leqslant k$, satisfy the corresponding conditions. Choosing all possible combinations of $a_1,\ldots,a_k$, we obtain that

$$\begin{gathered}2^{(n+1)k}\mathrm{adp}^{\oplus}_k(\alpha^1A_1,\ldots,\alpha^kA_k\to\alpha^{k+1}A_{k+1})=\\=\sum_{\substack{B\in\mathbb{Z}_2^{k+1},\\ \mathrm{wt}(B)\text{ is even}}}2^{nk}\mathrm{adp}^{\oplus}_k(\alpha^1\boxplus B_1,\ldots,\alpha^k\boxplus B_k\to\alpha^{k+1}\boxplus B_{k+1}).\end{gathered}$$

We recall that after the rearranging $a_1,\ldots,a_k$ we have the following: $B_1,\ldots,B_j$ must be zero, $B_{j+1},\ldots,B_k$ must be one, and $B_{k+1}=1$ if and only if j is even. That is why we consider only B of even weight. The equality (3) is proven.

3) Now, we prove the equality (4). Since we exclude the previous cases, $\mathrm{wt}(A)$ is even and there exists i, $1\leqslant i\leqslant k+1$, such that $A_i=0$. Using Proposition 1, we rearrange the arguments of $\mathrm{adp}^{\oplus}_k$ so that $A_{j+1}=A_{j+2}=\ldots=A_{k+1}=0$, where $j\leqslant k$, and $A_1=\ldots=A_j=1$. We rewrite the definition of $\mathrm{adp}^{\oplus}_k(\alpha^1 1,\ldots,\alpha^j 1,\alpha^{j+1}0,\ldots,\alpha^k 0\to\alpha^{k+1}0)$:

$$\begin{gathered}\frac{1}{2^{n(k+1)}}\Bigg|\Big\{x^1,\ldots,x^k\in\mathbb{Z}_2^n,\ a_1,\ldots,a_k\in\mathbb{Z}_2^1:\\ \bigoplus_{i=1}^{j}(\alpha^i1\boxplus x^ia_i)\oplus\bigoplus_{i=j+1}^{k}(\alpha^i0\boxplus x^ia_i)=\Big(\bigoplus_{i=1}^{j}x^ia_i\ \oplus\bigoplus_{i=j+1}^{k}x^ia_i\Big)\boxplus\alpha^{k+1}0\Big\}\Bigg|.\end{gathered}$$

We also fix the first j elements from the tuple $a_1,\ldots,a_k$. Using Proposition 1, we rearrange the arguments of $\mathrm{adp}^{\oplus}_k$ so that $a_1=\ldots=a_q=1$ and $a_{q+1}=\ldots=a_j=0$ for some $q\leqslant j$. Then we can rewrite the condition from the definition as

$$\begin{gathered}\bigoplus_{i=1}^{q}(\alpha^i1\boxplus x^i1)\oplus\bigoplus_{i=q+1}^{j}(\alpha^i1\boxplus x^i0)\oplus\bigoplus_{i=j+1}^{k}(\alpha^i0\boxplus x^ia_i)=\\=\left(\bigoplus_{i=1}^{q}x^i1\ \oplus\bigoplus_{i=q+1}^{j}x^i0\ \oplus\bigoplus_{i=j+1}^{k}x^ia_i\right)\boxplus\alpha^{k+1}0,\\ \bigoplus_{i=1}^{q}(\alpha^i\boxplus x^i\boxplus 1)0\oplus\bigoplus_{i=q+1}^{j}(\alpha^i\boxplus x^i)1\oplus\bigoplus_{i=j+1}^{k}(\alpha^i\boxplus x^i)a_i=\\=\left(\bigoplus_{i=1}^{q}x^i\ \oplus\bigoplus_{i=q+1}^{j}x^i\ \oplus\bigoplus_{i=j+1}^{k}x^i\right)\left(\bigoplus_{i=1}^{q}1\oplus\bigoplus_{i=j+1}^{k}a_i\right)\boxplus\alpha^{k+1}0.\end{gathered}$$

Next, we rewrite it in the following way:

$$\left(\bigoplus_{i=1}^{q}(\alpha^i \boxplus x^i \boxplus 1) \oplus \bigoplus_{i=q+1}^{j}(\alpha^i \boxplus x^i) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i)\right)\left(\bigoplus_{i=q+1}^{j} 1 \oplus \bigoplus_{i=j+1}^{k} a_i\right) =$$
$$= \left(\bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1}\right)\left(\bigoplus_{i=1}^{q} 1 \oplus \bigoplus_{i=j+1}^{k} a_i\right).$$

Let us extract the condition for the least significant bit:

$$\bigoplus_{i=q+1}^{j} 1 \oplus \bigoplus_{i=j+1}^{k} a_i = \bigoplus_{i=1}^{q} 1 \oplus \bigoplus_{i=j+1}^{k} a_i, \text{which is equivalent to } \bigoplus_{i=1}^{j} 1 = 0.$$

It is always satisfied since $j = \mathrm{wt}(A)$ is even. Now we consider the transformed condition without the least significant bit:

$$\bigoplus_{i=1}^{q}(\alpha^i \boxplus x^i \boxplus 1) \oplus \bigoplus_{i=q+1}^{j}(\alpha^i \boxplus x^i) \oplus \bigoplus_{i=j+1}^{k}(\alpha^i \boxplus x^i) = \bigoplus_{i=1}^{k} x^i \boxplus \alpha^{k+1}.$$

It obviously matches the condition from the definition of

$$\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 1, \ldots, \alpha^q \boxplus 1, \alpha^{q+1}, \ldots, \alpha^k \to \alpha^{k+1}).$$

If the tuple $x^1, \ldots, x^k$ satisfies the condition from the definition, then the tuple consisting of vectors $x^i 1$ for all i, $i \leqslant q$, vectors $x^i 0$ for all i, $q < i \leqslant j$ and vectors $x^i a_i$ for all i, $j < i \leqslant k$, also satisfies the condition from the definition of $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to$ $\to \alpha^{k+1} A_{k+1})$ for all a_i, $j < i \leqslant k$. There are 2^{k-j} such solutions. We can also see that $\alpha_i \boxplus 1$ can occur only when $A_i = 1$. The total number of solutions of the conditions from the definitions for vectors of dimension $n+1$ is $2^{(n+1)k}\,\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1})$, and for vectors of dimension n it is equal to $2^{nk}\,\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$. Choosing all possible combinations of a_i, we obtain

$$2^{(n+1)k}\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \sum_{\substack{B \in \mathbb{Z}_2^{k+1},\\ B \preceq A}} 2^{nk} 2^{k-j} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}).$$

Since $j = \mathrm{wt}(A)$, the equality (4) is proven. ■

Remark 1. We can extend the recurrence formulas for “empty” $\alpha^1, \ldots, \alpha^{k+1}$, i.e., for $\alpha^i A_i \in \mathbb{Z}_2^1$. It is sufficient to assume that $\mathrm{adp}_k^{\oplus}(\varnothing, \ldots, \varnothing \to \varnothing) = 1$. Indeed, we obtain by the recurrence formulas exactly that $\mathrm{adp}_k^{\oplus}(A_1, \ldots, A_k \to A_{k+1}) = 1 \iff \mathrm{wt}(A_1, \ldots, A_{k+1})$ is even and $\mathrm{adp}_k^{\oplus}(A_1, \ldots, A_k \to A_{k+1}) = 0 \iff \mathrm{wt}(A_1, \ldots, A_{k+1})$ is odd.

Remark 2. Using symmetries from Section 3 and the equality

$$\alpha \boxplus 1 = (2^n - 1) \boxplus -\overline{\alpha} \boxplus 1 = 2^n \boxplus -\overline{\alpha} \boxplus -1 \boxplus 1 = 2^n \boxplus -\overline{\alpha} = -\overline{\alpha},$$

we can replace $\alpha \boxplus 1$ with $\overline{\alpha}$ for a pair of arguments in the recurrence formulas (and for any argument if k is even). For instance,

$$\mathrm{adp}_3^{\oplus}(\alpha 1, \alpha 1, \alpha 1 \to \alpha 1) =$$
$$= \frac{1}{8}\mathrm{adp}_3^{\oplus}(\alpha, \alpha, \alpha \to \alpha) + \frac{3}{4}\mathrm{adp}_3^{\oplus}(\overline{\alpha}, \overline{\alpha}, \alpha \to \alpha) + \frac{1}{8}\mathrm{adp}_3^{\oplus}(\overline{\alpha}, \overline{\alpha}, \overline{\alpha} \to \overline{\alpha}).$$

5. Zeros and ones of the $\mathrm{adp}_k^{\oplus}$

For the purposes of cryptanalysis, it is important to distinguish the set of arguments on which $\mathrm{adp}_k^{\oplus}$ is equal to zero.

Theorem 3. For any $k \geqslant 2$ and any $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$, the equality $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = 0$ holds if and only if there exists i, $1 \leqslant i \leqslant n$, such that $(\alpha_i^1, \ldots, \alpha_i^{k+1}) \neq$ $\neq (0, \ldots, 0)$, $(\alpha_j^1, \ldots, \alpha_j^{k+1}) = (0, \ldots, 0)$ for all j, $i < j \leqslant n$, and one of the following conditions is true:

1) the vector $(\alpha_i^1, \ldots, \alpha_i^{k+1})$ has odd weight;

2) $(\alpha_i^1, \ldots, \alpha_i^{k+1}) = (1, \ldots, 1)$, k is odd, $i > 1$, and $(\alpha_{i-1}^1, \ldots, \alpha_{i-1}^{k+1})$ is of odd weight.

Proof. Let us use induction by n. For $n = 1$, $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$, where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2$, is equal to 0 if and only if $(\alpha^1, \ldots, \alpha^{k+1})$ is of odd weight. It is the base of the induction. Suppose that the statement holds for n. Let us prove that it is true for $n+1$. We represent elements from $\mathbb{Z}_2^{n+1}$ as $\alpha^1 A_1, \ldots, \alpha^{k+1} A_{k+1}$, where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ and $A = (A_1, \ldots, A_{k+1}) \in \mathbb{Z}_2^{k+1}$. First of all, we can assume that $A \neq (0, \ldots, 0)$. Indeed, $\mathrm{adp}_k^{\oplus}(\alpha^1 0, \ldots, \alpha^k 0 \to \alpha^{k+1} 0) = \mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$ by Theorem 2. Moreover, the statement of the theorem takes it into account. Next, we need to consider three cases.

1) $\mathrm{wt}(A)$ is odd. According to Theorem 2, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 0$. It proves that the first condition is sufficient.

2) $A = (1, \ldots, 1)$ and k is odd. In this case

$$\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1) =$$
$$= \frac{1}{2^k} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ \mathrm{wt}(B) \text{ is even}}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}).$$

The least significant bits of $\alpha^1 \boxplus B_1, \ldots, \alpha^{k+1} \boxplus B_{k+1}$ are $\alpha_n^1 \oplus B_1, \ldots, \alpha_n^{k+1} \oplus B_{k+1}$. Moreover, $\mathrm{wt}(B)$ is even. Thus, if $\mathrm{wt}(\alpha_n^1, \ldots, \alpha_n^{k+1})$ is odd, then $\mathrm{wt}(\alpha_n^1 \oplus B_1, \ldots, \alpha_n^{k+1} \oplus B_{k+1})$ is odd as well. It means that any of $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1})$ is equal to zero by induction.

Let $\mathrm{wt}(\alpha_n^1, \ldots, \alpha_n^{k+1})$ be even. Choosing $(0, \ldots, 0)$ or $(1, 1, 0, \ldots, 0)$ as B and taking into account that $k \geqslant 2$, we obtain that at least one of $(\alpha_n^1, \ldots, \alpha_n^{k+1})$ and $(\alpha_n^1 \oplus 1, \alpha_n^2 \oplus 1, \alpha_n^3, \ldots, \alpha_n^{k+1})$ does not belong to $\{(0, \ldots, 0), (1, \ldots, 1)\}$. Moreover, both of them are of even weight. It means that at least one of $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$ and $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 1, \alpha^2 \boxplus 1, \alpha^3, \ldots, \alpha^k \to \alpha^{k+1})$ is not zero by induction. Therefore, $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1)$ is not zero as well.

Thus, in this case $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1)$ is zero if and only if $\mathrm{wt}(\alpha_n^1, \ldots, \alpha_n^{k+1})$ is odd. It proves the correctness of the second condition.

3) $\mathrm{wt}(A)$ is even and $A \notin \{(0, \ldots, 0), (1, \ldots, 1)\}$. In this case

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \frac{1}{2^{\mathrm{wt}(A)}} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ B \preceq A}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}).$$

Without loss of generality we assume that $A_1 = A_2 = 1$, otherwise we can rearrange arguments by Theorem 1. Similarly to the previous point, at least one of $(\alpha_n^1, \alpha_n^2, \alpha_n^3, \ldots, \alpha_n^{k+1})$, $(\alpha_n^1 \oplus 1, \alpha_n^2, \alpha_n^3, \ldots, \alpha_n^{k+1})$, $(\alpha_n^1, \alpha_n^2 \oplus 1, \alpha_n^3, \ldots, \alpha_n^{k+1})$ and $(\alpha_n^1 \oplus 1, \alpha_n^2 \oplus 1, \alpha_n^3, \ldots, \alpha_n^{k+1})$ is of even weight and does not belong to $\{(0, \ldots, 0), (1, \ldots, 1)\}$. Thus, the corresponding

$\mathrm{adp}_k^{\oplus}$ is not zero by induction. Therefore, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1})$ is not zero as well.

It proves that the first condition is necessary, except for the cases $A = (0, \ldots, 0)$ and $A = (1, \ldots, 1)$ for odd k. ■

Note that the zeros of the function in the case of even k look similar to the zeros for $\mathrm{adp}^{\oplus}$. The second point appears only for odd k and generates an additional set of zeros.

The arguments on which $\mathrm{adp}_k^{\oplus}$ is equal to 1 are also interesting.

Theorem 4. For any $k \geqslant 2$ and any $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$, the equality $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = 1$ holds if and only if the vector $(\alpha_1^1, \ldots, \alpha_1^{k+1})$ has even weight, and one of the following conditions is true:

1) $(\alpha_i^1, \ldots, \alpha_i^{k+1}) = (0, \ldots 0)$ for all i, $2 \leqslant i \leqslant n$;
2) $(\alpha_2^1, \ldots, \alpha_2^{k+1}) = (1, \ldots, 1)$, k is odd, $n \geqslant 2$, and $(\alpha_i^1, \ldots, \alpha_i^{k+1}) = (0, \ldots 0)$ for all i, $3 \leqslant i \leqslant n$.

Proof. Let us use induction by n. For $n = 1$, $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$, where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2$, is equal to 1 if and only if $(\alpha^1, \ldots, \alpha^{k+1})$ is of even weight. It is the base of the induction. Suppose that the statement holds for n. Let us prove that it is true for $n+1$. We represent elements from $\mathbb{Z}_2^{n+1}$ as $\alpha^1 A_1, \ldots, \alpha^{k+1} A_{k+1}$, where $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ and $A = (A_1, \ldots, A_{k+1}) \in \mathbb{Z}_2^{k+1}$. Similarly to the proof of Theorem 3, we assume that $A \neq (0, \ldots, 0)$ (otherwise the statement is true by induction) and consider three cases.

1) $\mathrm{wt}(A)$ is odd, which means that $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 0 \neq 1$.

2) $A = (1, \ldots, 1)$ and k is odd. In this case

$$\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1) =$$
$$= \frac{1}{2^k} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ \mathrm{wt}(B) \text{ is even}}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}),$$

which implies that $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1) = 1$ if and only if $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}) = 1$ for all $B \in \mathbb{Z}_2^{k+1}$ of even weight.

The least significant bits of $\alpha^1 \boxplus B_1, \ldots, \alpha^{k+1} \boxplus B_{k+1}$ are $\alpha_n^1 \oplus B_1, \ldots, \alpha_n^{k+1} \oplus B_{k+1}$. Choosing $(0, \ldots, 0)$ or $(1, 1, 0, \ldots, 0)$ as B and taking into account that $k \geqslant 2$, we obtain that at least one of $(\alpha_n^1, \ldots, \alpha_n^{k+1})$ and $(\alpha_n^1 \oplus 1, \alpha_n^2 \oplus 1, \alpha_n^3, \ldots, \alpha_n^{k+1})$ does not belong to $\{(0, \ldots, 0), (1, \ldots, 1)\}$. In other words, at least one of $\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$ and $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus 1, \alpha^2 \boxplus 1, \alpha^3, \ldots, \alpha^k \to \alpha^{k+1})$ is not equal to 1 if $n > 1$ by induction. If $n = 1$, then all $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}) = \mathrm{adp}_k^{\oplus}(\alpha_1^1 \oplus B_1, \ldots, \alpha_1^k \oplus B_k \to \alpha_1^{k+1} \oplus B_{k+1}) = 1$ if and only if $\mathrm{wt}(\alpha_1^1, \ldots, \alpha_1^{k+1})$ is even.

Thus, in this case $\mathrm{adp}_k^{\oplus}(\alpha^1 1, \ldots, \alpha^k 1 \to \alpha^{k+1} 1) = 1$ if and only if $n = 1$ and $\mathrm{wt}(\alpha_1^1, \ldots, \alpha_1^{k+1})$ is even. It proves the correctness of the second condition.

3) $\mathrm{wt}(A)$ is even and $A \notin \{(0, \ldots, 0), (1, \ldots, 1)\}$. In this case

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) =$$
$$= \frac{1}{2^{\mathrm{wt}(A)}} \sum_{\substack{B \in \mathbb{Z}_2^{k+1}, \\ B \preceq A}} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}).$$

This means that $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) = 1$ if and only if $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^k \boxplus B_k \to \alpha^{k+1} \boxplus B_{k+1}) = 1$ for all $B \in \mathbb{Z}_2^{k+1}$ such that $B \preceq A$.

Without loss of generality we assume that $A_1 = 1$, otherwise we can rearrange arguments by Theorem 1. Next, one of $(\alpha^1_n, \alpha^2_n, \ldots, \alpha^{k+1}_n)$ and $(\alpha^1_n \oplus 1, \alpha^2_n, \ldots, \alpha^{k+1}_n)$ is of odd weight. Thus, one of $\mathrm{adp}^{\oplus}_k(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$ and $\mathrm{adp}^{\oplus}_k(\alpha^1 \boxplus 1, \alpha^2, \ldots, \alpha^k \to \alpha^{k+1})$ is zero by Theorem 2 and $\mathrm{adp}^{\oplus}_k(\alpha^1 A_1, \ldots, \alpha^k A_k \to \alpha^{k+1} A_{k+1}) \neq 1$.

Together with the first point, it proves the correctness of the first condition. ■

Remark 3. The conditions from Theorems 3 and 4 for $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$ can be simplified. Let us define the following pattern symbols for elements of $\mathbb{Z}_2^{k+1}$:

— $*$ means any $x \in \mathbb{Z}_2^{k+1}$,

— $\mathtt{e}$ and $\mathtt{d}$ mean any $x \in \mathbb{Z}_2^{k+1}$ of even and odd weight respectively,

— $\mathbf{0}$ and $\mathbf{1}$ mean $(0, \ldots, 0)$ and $(1, \ldots, 1)$ from $\mathbb{Z}_2^{k+1}$ respectively.

Then $\mathrm{adp}^{\oplus}_k(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = 0$ if and only if the vector

$$\big((\alpha^1_1, \ldots, \alpha^{k+1}_1), \ldots, (\alpha^1_n, \ldots, \alpha^{k+1}_n)\big) \tag{5}$$

matches

$$(*, \ldots, *, \mathtt{d}, \mathbf{0}, \ldots, \mathbf{0}) \text{ for any } k \text{ or}$$
$$(*, \ldots, *, \mathtt{d}, \mathbf{1}, \mathbf{0}, \ldots, \mathbf{0}) \text{ for odd } k.$$

Similarly, $\mathrm{adp}^{\oplus}_k(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = 1$ if and only if the vector (5) matches

$$(\mathtt{e}, \mathbf{0}, \ldots, \mathbf{0}) \text{ for any } k \text{ or}$$
$$(\mathtt{e}, \mathbf{1}, \mathbf{0}, \ldots, \mathbf{0}) \text{ for odd } k.$$

6. Maximums of the $\mathrm{adp}^{\oplus}_k$

Also, for the purposes of cryptanalysis, the maximum values of $\mathrm{adp}^{\oplus}_k$ are of interest, where some argument (or arguments) is fixed. In the case of even k, it is not difficult to show that the maximum of the characteristic, where one its argument is fixed, is similar to the maximum for $k = 2$.

Theorem 5. Let $k \geqslant 2$ be even and $\gamma \in \mathbb{Z}_2^n$. Then

$$\max_{x^1, \ldots, x^k \in \mathbb{Z}_2^n} \mathrm{adp}^{\oplus}_k(x^1, \ldots, x^k \to \gamma) = \mathrm{adp}^{\oplus}_k(0, \ldots, 0, \gamma \to \gamma).$$

Proof. Let us use induction by n. If $n = 1$, $\mathrm{adp}^{\oplus}_k(0, \ldots, 0, \gamma \to \gamma) = 1$ for any $\gamma \in \mathbb{Z}_2$, see Theorem 4. It is the base of the induction.

Next, we assume that $\mathrm{adp}^{\oplus}_k(\beta^1, \ldots, \beta^k \to \gamma) \leqslant \mathrm{adp}^{\oplus}_k(0, \ldots, 0, \gamma \to \gamma)$ for any $\beta^1, \ldots, \beta^k, \gamma \in \mathbb{Z}_2^n$. Let $\alpha^1, \ldots, \alpha^k, \gamma \in \mathbb{Z}_2^n$, $A \in \mathbb{Z}_2^{k+1}$. We need to prove that $\mathrm{adp}^{\oplus}_k(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) \leqslant \mathrm{adp}^{\oplus}_k(0, \ldots, 0, \gamma A_{k+1} \to \gamma A_{k+1})$. We divide the proof into the following cases.

Case 1. $A = (0, \ldots, 0)$. According to Theorem 2, $\mathrm{adp}^{\oplus}_k(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) = \mathrm{adp}^{\oplus}_k(\alpha^1, \ldots, \alpha^k \to \gamma)$ and $\mathrm{adp}^{\oplus}_k(0, \ldots, 0, \gamma A_{k+1} \to \gamma A_{k+1}) = \mathrm{adp}^{\oplus}_k(0, \ldots, 0, \gamma \to \gamma)$. Thus, the induction hypothesis provides that $\mathrm{adp}^{\oplus}_k(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) \leqslant \mathrm{adp}^{\oplus}_k(0, \ldots, 0, \gamma A_{k+1} \to \gamma A_{k+1})$.

Case 2. $\mathrm{wt}(A)$ is odd. According to Theorem 2, $\mathrm{adp}^{\oplus}_k(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) = 0$. It proves the induction step.

Case 3. $\mathrm{wt}(A)$ is even and $A_{k+1} = 0$. Without loss of generality, we can assume that $A_1 = \ldots = A_w = 1$ and $A_{w+1} = \ldots = A_k = 0$, where $w = \mathrm{wt}(A)$. Indeed, Proposition 1 allows us to rearrange the arguments of $\mathrm{adp}_k^{\oplus}$. Then, Theorem 2 and the induction hypothesis give us that

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma 0) = 2^{-w} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma) \leqslant$$
$$\leqslant 2^{-w} \cdot 2^w \cdot \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma 0 \to \gamma 0).$$

Case 4. $\mathrm{wt}(A)$ is even and $A_{k+1} = 1$. Similarly to the previous case, we assume without loss of generality that $A_1 = \ldots = A_w = 1$ and $A_{w+1} = \ldots = A_k = 0$, where $w = \mathrm{wt}(A) - 1$. According to Theorem 2,

$$\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma A_{k+1}) =$$
$$= 2^{-w-1} \sum_{c \in \mathbb{Z}_2} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus c) =$$
$$= 2^{-w-1} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma) +$$
$$+ 2^{-w-1} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus 1).$$

Also, if the vector of the least significant coordinates has odd weight, i.e., $\mathrm{wt}(B) + c + \mathrm{wt}(\alpha_n^1, \ldots, \alpha_n^k, \gamma_n)$ is odd, then $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus c) = 0$. It means that at least half of $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma)$ are zero and at least half of $\mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus 1)$ are zero. At the same time,

$$\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma 1 \to \gamma 1) = \frac{1}{4}\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \boxplus 1 \to \gamma \boxplus 1),$$

since $\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma \boxplus 1) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \boxplus 1 \to \gamma) = 0$. Finally, by the induction hypothesis and due to the least significant vectors of odd weight, we obtain that

$$2^{-w-1} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma) \leqslant$$
$$\leqslant 2^{-w-1} \cdot 2^{w-1} \cdot \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma) = \frac{1}{4}\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma).$$

Similarly,

$$2^{-w-1} \sum_{B \in \mathbb{Z}_2^w} \mathrm{adp}_k^{\oplus}(\alpha^1 \boxplus B_1, \ldots, \alpha^w \boxplus B_w, \alpha^{w+1}, \ldots, \alpha^k \to \gamma \boxplus 1) \leqslant$$
$$\leqslant 2^{-w-1} \cdot 2^{w-1} \cdot \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \boxplus 1 \to \gamma \boxplus 1) = \frac{1}{4}\mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \boxplus 1 \to \gamma \boxplus 1).$$

Thus, $\mathrm{adp}_k^{\oplus}(\alpha^1 A_1, \ldots, \alpha^k A_k \to \gamma 1) \leqslant \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma 1 \to \gamma 1)$. ■

For odd k the maximum looks different.

Corollary 1. For any odd $k \geqslant 3$ and $\gamma = 2^{n-1} + 2^{n-2} \in \mathbb{Z}_2^n$ the following holds:

$$\mathrm{adp}_k^{\oplus}(\gamma, \gamma, 0, \ldots, 0 \to 0) < 1 = \mathrm{adp}_k^{\oplus}(\gamma, \ldots, \gamma \to \gamma).$$

It directly follows from Theorem 4. However, for some cases we can generalize results of Theorem 5.

Corollary 2. Let $k \geqslant 3$ be odd. Then for any $\gamma \in \mathbb{Z}_2^n$ the following holds:

$$\max_{x^1,\ldots,x^{k-1}\in\mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(0, x^1, \ldots, x^{k-1} \to \gamma) = \mathrm{adp}_k^{\oplus}(0, \ldots, 0, \gamma \to \gamma).$$

Indeed, the proof of Theorem 5 is correct for this case since the first argument is zero. Thus, we will never use the case $(1, \ldots, 1)$ in the recurrence formulas which is the only difference between even and odd k. At the same time, we believe that for an arbitrary odd k the following holds.

Hypothesis 1. Let $k \geqslant 3$ be odd and $\gamma \in \mathbb{Z}_2^n$. Then

$$\max_{x^1,\ldots,x^k\in\mathbb{Z}_2^n} \mathrm{adp}_k^{\oplus}(x^1, \ldots, x^k \to \gamma) = \mathrm{adp}_k^{\oplus}(\gamma, \ldots, \gamma \to \gamma).$$

Note that a problem connected with the values $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ can be found in [16]. NSUCRYPTO-2014 [17] also included a problem related to ARX constructions.

7. A matrix approach for calculating $\mathrm{adp}_k^{\oplus}$

The section is devoted to a generalization of the approach proposed in [14] for calculating $\mathrm{adp}^{\oplus}$, i.e., $\mathrm{adp}_2^{\oplus}$. There is also the S-function technique [15], which provides a matrix calculation algorithm that help to compute values of any S-function (including $\mathrm{adp}_k^{\oplus}$). However, it does not allow us to obtain analytic expressions for the matrix elements, as well as relationship between matrices.

In this section, we will consider a vector space $\widehat{\mathbb{Q}}^{2^{k+1}}$ over rationals. We assume that the coordinates of the vectors from $\widehat{\mathbb{Q}}^{2^{k+1}}$ start with zero and for coordinate $x_1 2^k + x_2 2^{k-1} + \ldots + x_{k+1}$ we use both integer and binary vectors $(x_1, \ldots, x_{k+1})$ representations, $x \in \mathbb{Z}_2^{k+1}$. Let $A \in \mathbb{Z}_2^{k+1}$ and $k \geqslant 2$. We define matrices M_A^k of size $2^{k+1} \times 2^{k+1}$ in the following way:

$$(M_A^k)_{y,x} = \begin{cases} 2^{-k}, & \text{if } x = \overline{A}, k \text{ is odd and } \mathrm{wt}(y) \text{ is even,} \\ 2^{-\mathrm{wt}(x\oplus A)}, & \text{if } \mathrm{wt}(x \oplus A) \text{ is even and } y \oplus A \preceq x \oplus A, \\ 0, & \text{otherwise,} \end{cases} \tag{6}$$

where $x, y \in \mathbb{Z}_2^{k+1}$. Similarly to the elements of $\widehat{\mathbb{Q}}^{2^{k+1}}$, we use both integer (starting with 0) and binary vector notations for the matrix indexes.

The next theorem follows from the Theorem 2 and gives us a way to calculate $\mathrm{adp}_k^{\oplus}$.

Theorem 6. Let $k \geqslant 2$ and $\alpha^1, \ldots, \alpha^{k+1} \in \mathbb{Z}_2^n$. Then

$$\mathrm{adp}_k^{\oplus}(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = (1, \ldots, 1) M^k_{(\alpha^1_1,\ldots,\alpha^{k+1}_1)} \cdot \ldots \cdot M^k_{(\alpha^1_n,\ldots,\alpha^{k+1}_n)} (1, 0, \ldots, 0)^{\mathrm{T}}.$$

Proof. We use the recurrence formulas obtained in Theorem 2. First of all, we define $[\beta]_m = (\beta_1, \ldots, \beta_m)$ for any $\beta \in \mathbb{Z}_2^n$ and $1 \leqslant m \leqslant n$. Also, $[\beta]_m \boxplus a$ means $[\beta]_m + a \bmod 2^m$, where $a \in \mathbb{Z}_2$. Let $x \in \mathbb{Z}_2^{k+1}$. We apply Theorem 2 to $\mathrm{adp}_k^{\oplus}([\alpha^1]_{m+1} \boxplus x_1, \ldots, [\alpha^k]_{m+1} \boxplus x_k \to [\alpha^{k+1}]_{m+1} \boxplus x_{k+1})$. Let $A = (\alpha^1_{m+1}, \ldots, \alpha^{k+1}_{m+1})$. Then the vector of the least significant bits of the arguments is $x \oplus A$. After applying the recurrence formulas, we obtain a sum of

$$\mathrm{adp}_k^{\oplus}([[\alpha^1]_{m+1} \boxplus x_1]_m \boxplus y_1, \ldots, [[\alpha^k]_{m+1} \boxplus x_k]_m \boxplus y_k \to [[\alpha^{k+1}]_{m+1} \boxplus x_{k+1}]_m \boxplus y_{k+1})$$

for some $y \in \mathbb{Z}_2^{k+1}$, $y \preceq x \oplus A$. Let us show that

$$[[\alpha^i]_{m+1} \boxplus x_i]_m \boxplus y_i = [\alpha^i]_m \boxplus (y_i \oplus x_i \cdot A_i), \tag{7}$$

where $i = 1, \ldots, k+1$ and $y \preceq x \oplus A$. Indeed, if $(A_i, x_i) = (\alpha^i_{m+1}, x_i) \neq (1,1)$, i.e., $x_i \cdot A_i = 0$, then the addition of x_i to $[\alpha^i]_{m+1}$ may change only its least significant bit. Thus, $[[\alpha^i]_{m+1} \boxplus x_i]_m = [\alpha^i]_m$. If $(A_i, x_i) = (1,1)$, then $y_i = 0$ since $x_i \oplus A_i = 0$ and $y \preceq x \oplus A$. Thus, $[[\alpha^i]_{m+1} \boxplus x_i]_m \boxplus y_i = [[\alpha^i]_{m+1} \boxplus 1]_m = [\alpha^i]_m \boxplus 1 = [\alpha^i]_m \boxplus (y_i \oplus x_i \cdot A_i)$.

Next, we denote by $x \cdot A$ the vector $(x_1 \cdot A_1, \ldots, x_{k+1} \cdot A_{k+1})$. Let us show that

$$\{y \oplus (x \cdot A) : y \in \mathbb{Z}_2^{k+1} \text{ and } y \preceq x \oplus A\} = \{z \in \mathbb{Z}_2^{k+1} : z \oplus A \preceq x \oplus A\}. \tag{8}$$

Indeed, $\{y \oplus (x \cdot A) : y \in \mathbb{Z}_2^{k+1} \text{ and } y \preceq x \oplus A\} = \{z \in \mathbb{Z}_2^{k+1} : z \oplus (x \cdot A) \preceq x \oplus A\}$. At the same time, $z \oplus (x \cdot A) \preceq x \oplus A \iff z \oplus A \preceq x \oplus A$ since for any $i = 1, \ldots, k+1$ we have the following: $x_i \neq A_i$ (i.e., $x_i \oplus A_i = 1$) implies that both $z_i \oplus (x_i \cdot A_i) \leqslant 1$ and $z_i \oplus A_i \leqslant 1$ always hold for any $z_i \in \mathbb{Z}_2$; also, $x_i = A_i$ implies that $z_i \oplus (x_i \cdot A_i) = z_i \oplus A_i$.

Moreover, the following holds for $x = \overline{A}$:

$$\{y \oplus (x \cdot A) : y \in \mathbb{Z}_2^{k+1},\ \mathrm{wt}(y) \text{ is even}\} = \{z \in \mathbb{Z}_2^{k+1} : \mathrm{wt}(z) \text{ is even}\}. \tag{9}$$

It is straightforward since in this case $x \oplus A = (1, \ldots, 1)$ and $x \cdot A = (0, \ldots, 0)$.

Theorem 2 allows us to express $r = \mathrm{adp}^{\oplus}_k([\alpha^1]_{m+1} \boxplus x_1, \ldots, [\alpha^k]_{m+1} \boxplus x_k \to [\alpha^{k+1}]_{m+1} \boxplus x_{k+1})$ in the following way:

1) If $\mathrm{wt}(x \oplus A)$ is odd, then $r = 0$.
2) If $x \oplus A = (1, \ldots, 1)$ and k is odd, then according to (7) and (9) the following holds:

$$r = 2^{-k} \sum_{z\colon \mathrm{wt}(z) \text{ is even}} \mathrm{adp}^{\oplus}_k([\alpha^1]_m \boxplus z_1, \ldots, [\alpha^k]_m \boxplus z_k \to [\alpha^{k+1}]_m \boxplus z_{k+1}).$$

3) Otherwise, due to (7) and (8) we have that

$$r = 2^{-\mathrm{wt}(x \oplus A)} \sum_{z\colon z \oplus A \preceq x \oplus A} \mathrm{adp}^{\oplus}_k([\alpha^1]_m \boxplus z_1, \ldots, [\alpha^k]_m \boxplus z_k \to [\alpha^{k+1}]_m \boxplus z_{k+1}).$$

At the same time, we know how the matrix M^k_A transforms the standard basis $\widehat{e}^{\mathrm{T}}_x$ (it has 1 in the coordinate x and 0 in all other coordinates) for all $x \in \mathbb{Z}_2^{k+1}$: $(M^k_A)_{y,x}$ is the y-th coordinate of $M^k_A \widehat{e}^{\mathrm{T}}_x$, where $y \in \mathbb{Z}_2^{k+1}$, which is equal to

$$\begin{cases} 2^{-k}, & \text{if } x = \overline{A},\ k \text{ is odd and } \mathrm{wt}(y) \text{ is even},\\ 2^{-\mathrm{wt}(x \oplus A)}, & \text{if } \mathrm{wt}(x \oplus A) \text{ is even and } y \oplus A \preceq x \oplus A,\\ 0 & \text{otherwise.} \end{cases}$$

It is not difficult to see that the mapping M^k_A completely corresponds to the points 1, 2, and 3. It other words, we can consider it as a "state" transformation: it maps all multipliers of $\mathrm{adp}^{\oplus}_k([\alpha^1]_{m+1} \boxplus x_1, \ldots, [\alpha^k]_{m+1} \boxplus x_k \to [\alpha^{k+1}]_{m+1} \boxplus x_{k+1})$ (for all $x \in \mathbb{Z}_2^{k+1}$) to all multipliers of $\mathrm{adp}^{\oplus}_k([\alpha^1]_m \boxplus y_1, \ldots, [\alpha^k]_m \boxplus y_k \to [\alpha^{k+1}]_m \boxplus y_{k+1})$ (for all $y \in \mathbb{Z}_2^{k+1}$). Since we start with $\mathrm{adp}^{\oplus}_k(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1})$, it corresponds to the "state" $\widehat{e}^{\mathrm{T}}_0$. Thus, the final multipliers are

$$s = M^k_{(\alpha^1_1, \ldots, \alpha^{k+1}_1)} \cdots M^k_{(\alpha^1_n, \ldots, \alpha^{k+1}_n)} \widehat{e}^{\mathrm{T}}_0,$$

see Remark 1 for the case $n = 1$. Finally, $\mathrm{adp}^{\oplus}_k(\alpha^1, \ldots, \alpha^k \to \alpha^{k+1}) = (1, \ldots, 1) \cdot s$. ■

Corollary 3. If k is even, then $(M^k_A)_{y,x} = (M^k_0)_{y \oplus A, x \oplus A}$, $A, x, y \in \mathbb{Z}_2^{k+1}$. It means that all M^k_A can be obtained from each other using some permutations of rows and columns.

This does not hold for odd k. However, almost the same thing is true: we swap x and $x \oplus A$ columns, after that we swap y and $y \oplus A$ rows of M^k_0 except for the rows $\overline{A}$ and $(1, \ldots, 1)$.

The proof follows directly from the definition of M_A^k. Thus, the difference in recurrence formulas gives us some difference in the calculation of the $\mathrm{adp}_k^{\oplus}$ for odd and even k.

Some matrices for $k = 3$ are presented bellow:

$$\overset{8\cdot M^3_{(0,0,0,0)}}{\begin{pmatrix}
8&0&0&2&0&2&2&0&0&2&2&0&2&0&0&1\\
0&0&0&2&0&2&0&0&0&2&0&0&0&0&0&0\\
0&0&0&2&0&0&2&0&0&0&2&0&0&0&0&0\\
0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&2&2&0&0&0&0&0&2&0&0&0\\
0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&2&2&0&2&0&0&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}},\quad
\overset{8\cdot M^3_{(0,0,0,1)}}{\begin{pmatrix}
0&0&2&0&2&0&0&0&2&0&0&0&0&0&1&0\\
0&8&2&0&2&0&0&2&2&0&0&2&0&2&0&0\\
0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&2&0&0&0&0&2&0&0&0&2&0&0&1&0\\
0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&2&0&0&2&0&0&0&0&0&2&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&2&0&0&2&0&2&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{pmatrix}},\quad
\overset{8\cdot M^3_{(1,1,1,1)}}{\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0\\
0&0&0&2&0&2&2&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0\\
0&0&0&2&0&0&0&0&2&2&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0\\
0&0&0&0&0&2&0&0&0&2&0&0&2&0&0&0\\
0&0&0&0&0&0&2&0&0&0&2&0&2&0&0&0\\
1&0&0&2&0&2&2&0&0&2&2&0&2&0&0&8
\end{pmatrix}}.$$

For instance, if $\alpha^1 = (0,0,1)$, $\alpha^2 = (0,0,1)$, $\alpha^3 = (0,0,1)$, and $\alpha^4 = (0,1,1)$, we obtain that

$$\mathrm{adp}_3^{\oplus}(\alpha^1,\alpha^2,\alpha^3 \to \alpha^4) = (\underbrace{1,\dots,1}_{16})M^3_{(0,0,0,0)}M^3_{(0,0,0,1)}M^3_{(1,1,1,1)}(\underbrace{1,0,\dots,0}_{16})^{\mathrm{T}}.$$

8. Conclusion

We have generalized some properties of $\mathrm{adp}^{\oplus}$ to $\mathrm{adp}_k^{\oplus}$. The results obtained show us that there is the difference between odd and even k, it looks like the case of odd k is more complicated. A generalization of other properties such as maximum for odd k is a topic for future research.

The authors would like to thank Nicky Mouha for interesting discussions and valuable advice.

REFERENCES

1. *Shimizu A. and Miyaguchi S.* Fast Data Encipherment Algorithm (FEAL). LNCS, 1988, vol. 304, pp. 267–278.
2. *Ferguson N., Lucks S., Schneier B., et al.* `http://www.skein-hash.info` — The Skein Hash Function Family, 2009.
3. *Bernstein D. J.* `https://cr.yp.to/snuffle/spec.pdf` — Salsa20 specification, 2005.
4. *Bernstein D. J.* `https://cr.yp.to/chacha/chacha-20080128.pdf` — ChaCha, a variant of Salsa20, 2008.
5. *Aumasson J.-P., Meier W., Phan R. C.-W., and Henzen L.* The Hash Function BLAKE. Berlin; Heidelberg, Springer, 2014.
6. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems. J. Cryptology, 1991, vol. 4, no. 1, pp. 3–72.
7. *Malyshev F. M.* Veroyatnostnye kharakteristiki raznostnykh sootnosheniy dlya neodnorodnoy lineynoy sredy [Probabilistic characteristics of differential and linear relations for nonhomogeneous linear medium]. Matematicheskie Voprosy Kriptografii, 2019, vol. 10, no.1, pp. 41–72. (in Russian)
8. *Malyshev F. M.* Raznostnye kharakteristiki osnovnykh operatsiy ARX-shifrov [Differential characteristics of base operations in ARX-ciphers]. Matematicheskie Voprosy Kriptografii, 2020, vol. 11, no.4, pp. 97–105. (in Russian)
9. *Leurent G.* Analysis of differential attacks in ARX constructions. LNCS, 2012, vol. 7658, pp. 226–243.

10. *Leurent G.* Construction of differential characteristics in ARX designs application to Skein. LNCS, 2013, vol. 8042, pp. 241–258.
11. *Mouha N., Kolomeec N., Tokareva N., et al.* Maximums of the additive differential probability of exclusive-or with one fixed argument. IACR Trans. Symmetric Cryptology, 2021, vol. 2021, no. 2, pp. 292–313.
12. *Velichkov V., Mouha N., De Canniére C., and Preneel B.* The additive differential probability of ARX. LNCS, 2011, vol. 6733, pp. 342–358.
13. *Gligoroski D., Ødegărd R. S., Mihova M., et al.* Cryptographic hash function Edon-R'. Proc. 1st Intern. Workshop on Security and Communication Networks, Trondheim, Norway, 2009, pp. 1–9.
14. *Lipmaa H., Wallén J., and Dumas P.* On the additive differential probability of Exclusive-Or. LNCS, 2004, vol. 3017, pp. 317–331.
15. *Mouha N., Velichkov V., De Canniére C., and Preneel B.* The differential analysis of S-functions. LNCS, 2011, vol. 6544, pp. 36–56.
16. *Gorodilova A., Tokareva N., Agievich S., et al.* An overview of the eight international olympiad in cryptography "Non-Stop University Crypto". Siberian Electronic Math. Reports, 2022, vol. 19, no. 1, pp. A9–A37.
17. *Agievich S. V., Gorodilova A. A., Tokareva N. N., et al.* Problems, solutions and experience of the first international student's Olympiad in cryptography. Prikladnaya Diskretnaya Matematika, 2015, no. 3, pp. 41–62.