IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2021, No. 2, pp. 292–313. DOI:10.46586/tosc.v2021.i2.292-313

Maximums of the Additive Differential Probability of Exclusive-Or

Nicky Mouha[1], Nikolay Kolomeec[2], Danil Akhtiamov[3], Ivan Sutormin[2], Matvey Panferov[4], Kseniya Titova[4], Tatiana Bonich[4], Evgeniya Ishchukova[5], Natalia Tokareva[2] and Bulat Zhantulikov[4]

[1] Strativia, Largo, MD, USA, nicky@mouha.be
[2] Sobolev Institute of Mathematics, Novosibirsk, Russia, {kolomeec,tokareva}@math.nsc.ru
[3] The Hebrew University of Jerusalem, Jerusalem, Israel, akhtyamoff1997@gmail.com
[4] Novosibirsk State University, Novosibirsk, Russia, ivan.sutormin@gmail.com,sitnich@gmail.com,{m.panferov,t.bonich,b.zhantulikov}@g.nsu.ru
[5] Southern Federal University, Taganrog, Russia, uaishukova@sfedu.ru

Abstract. At FSE 2004, Lipmaa et al. studied the additive differential probability $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ of exclusive-or where differences $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ are expressed using addition modulo 2^n. This probability is used in the analysis of symmetric-key primitives that combine XOR and modular addition, such as the increasingly popular Addition-Rotation-XOR (ARX) constructions. The focus of this paper is on maximal differentials, which are helpful when constructing differential trails. We provide the missing proof for Theorem 3 of the FSE 2004 paper, which states that $\max_{\alpha,\beta} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ for all γ. Furthermore, we prove that there always exist either two or eight distinct pairs α, β such that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, and we obtain recurrence formulas for calculating $\mathrm{adp}^{\oplus}$. To gain insight into the range of possible differential probabilities, we also study other properties such as the minimum value of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, and we find all γ that satisfy this minimum value.

Keywords: Differential cryptanalysis · ARX · XOR · modular addition

1 Introduction

Differential cryptanalysis [BS91] is a well-known statistical method for the analysis of symmetric-key primitives. The main idea is to see how a difference ΔX between two inputs (e. g., plaintexts) propagates to a difference ΔY between the corresponding outputs (e. g., ciphertexts). The ordered pair $(\Delta X, \Delta Y)$ is referred to as a differential. A differential trail is defined as a sequence $(\Delta X, \Delta X_2, \ldots, \Delta X_{p-1}, \Delta Y)$ where $\Delta X_2, \ldots, \Delta X_{p-1}$ are some intermediate values that appear in the primitive.

A common technique to construct a differential trail is to use a "greedy" strategy to pick the intermediate differences that have the highest differential probability. Under some assumptions, the probabilities of a differential trail can be multiplied together to obtain a good estimate of the probability of a differential.

However, this presupposes that the maximal differential probabilities of elementary operations can be efficiently calculated. For ciphers based on S-boxes, this is rather straightforward: their size is usually small enough so that all input and output differences can be enumerated in a Difference Distribution Table (DDT).

However, this is often not the case for Addition-Rotation-XOR (ARX) constructions, where the addition modulo 2^n can have $n = 32$ or $n = 64$, thereby making it infeasible to

Received: 2020-11-23 Revised: 2021-03-01 Accepted: 2021-05-01 Published: 2021-06-11

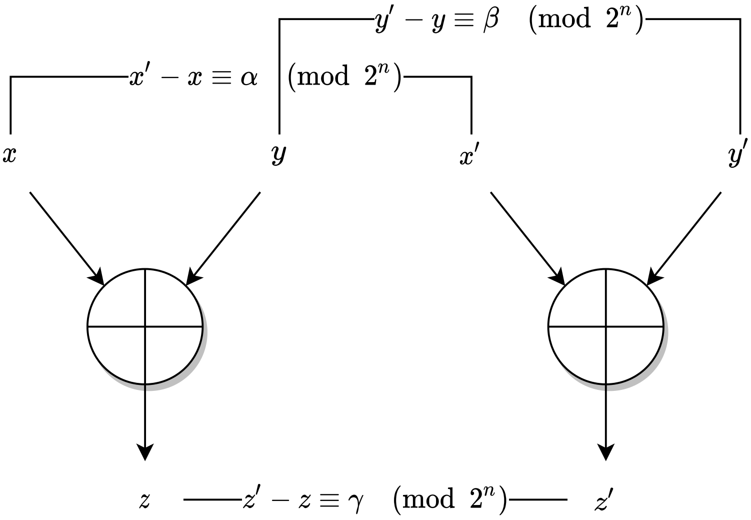
$y' - y \equiv \beta \pmod{2^n}$
$x' - x \equiv \alpha \pmod{2^n}$
x
y
x'
y'
z
$z' - z \equiv \gamma \pmod{2^n}$
z'

Figure 1: The differential probability $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ of exclusive-or when differences are represented using differences α, β, γ are expressed using addition modulo 2^n. The probability is obtained by averaging over all values of x and y.

construct a DDT. Two of the five finalists of the NIST SHA-3 hash function competition are ARX constructions: BLAKE [AMPH14] which uses either 32-bit or 64-bit additions (depending on the length of the hash value), and Skein [FLS+09] which uses 64-bit additions.

The differential probability $\mathrm{adp}^{\oplus}$ of exclusive-or (XOR) when differences are expressed using addition modulo 2^n was studied at FSE 2004 by Lipmaa et al. [LWD04]. It is defined as $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \Pr_{x,y \in \mathbb{F}_2^n}[(x + \alpha) \oplus (y + \beta) = \gamma + (x \oplus y)]$, and illustrated in Fig. 1.

Lipmaa et al. showed that $\mathrm{adp}^{\oplus}$ can be expressed as a rational series. That is, if we define $\omega_i = 4\alpha_i + 2\beta_i + \gamma_i$, then (as we will recall in Sect. 3) there are eight 8-dimensional square matrices A_j, a column vector C, and a row vector L, such that

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = L \cdot A_{\omega_{n-1}} \cdot \ldots \cdot A_{\omega_0} \cdot C,$$

here ω_i, i. e., which matrix is used as the i-th term of the product, depends on $\alpha_i, \beta_i, \gamma_i$. This formula allows us to easily calculate the probability given a differential $(\alpha, \beta \to \gamma)$.

Lipmaa et al. point out in their FSE 2004 paper [LWD04] that “many of the enumerative aspects of $\mathrm{adp}^{\oplus}$ seem infeasible,” but nevertheless provide a theorem related to the maximal differential probability when the output difference γ is fixed. More specifically, Theorem 3 of their paper states that for all output differences γ,

$$\max_{\alpha,\beta} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma).$$

Unfortunately, this theorem is not proven in the FSE 2004 paper, and communication with one of the authors revealed that the proof has been lost. Therefore, it is interesting to know whether the theorem is correct (or if there exists a counterexample), and the proof techniques may allow us to better understand $\mathrm{adp}^{\oplus}$ and help to prove other properties.

Outline. This paper is organized as follows. We give an overview of related work in Sect. 2. Sect. 3 provides some basic definitions. In Sect. 4, we give some useful argument symmetries for $\mathrm{adp}^{\oplus}$: the order of the arguments does not matter for $\mathrm{adp}^{\oplus}$, and the probability is unchanged under certain transformations of the arguments. In Sect. 5, we finally provide a proof of Theorem 3 of the FSE 2004 paper [LWD04]. Sect. 6 shows that there are either eight (if $\gamma \notin \{0, 2^{n-1}\}$) or two (otherwise) distinct pairs (α, β) such that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$. Recurrence formulas for an arbitrary $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ are obtained in Sect. 7. Sect. 8 focuses on properties of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$: a simplified matrix form by 2×2 matrices is proven; we find the minimum value of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, and obtain all γ that satisfy this minimum value. Lastly, we calculate the sum of all $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, and conclude the paper in Sect. 9 along with some suggestions for future work.

2 Related Work

At the Dagstuhl "Symmetric Cryptography" seminar in January 2009, Weinmann introduced the term AXR for symmetric-key primitives based on additions modulo 2^n, XORs and rotations. Later at the FSE 2009 rump session, he renamed the term to ARX. The design strategy, however, is much older: perhaps the earliest example of an ARX primitive is the block cipher FEAL [SM88] (Fast Data Encipherment Algorithm), introduced at EUROCRYPT 1987.

More recent examples of ARX ciphers include the eSTREAM finalist Salsa20 [Ber05], the ChaCha [Ber08] stream cipher included in the Transport Layer Security (TLS) protocol version 1.3, the block cipher Speck [BSS+13] (standardized as ISO/IEC 29167-22), the CHAM block cipher [KRK+17] (which has been revised to increase the number of rounds [RKJ+19]), and several submissions to the NIST lightweight cryptography project including COMET [GJN19] (which relies on SPECK and CHAM), SNEIK [Saa19], and Sparkle [BBCdS+20b].

To apply differential cryptanalysis to an ARX primitive, one approach is to use XOR differences: these differences pass through rotation and XOR operations with probability one, and formulas for the differential probability xdp^{+} of the modular addition were provided at FSE 2001 by Lipmaa et al. [LM01].

In this paper, however, we are interested in differences that are expressed using addition modulo 2^n. These differences go through the modular addition with probability one. The additive differential probability of rotation was studied by Berson [Ber92], and Lipmaa et al. [LWD04] provided a formula for $\mathrm{adp}^{\oplus}$, the additive differential probability of XOR.

Using Lipmaa et al.'s expression for $\mathrm{adp}^{\oplus}$, Velichkov et al. [VMDCP12, App. C] provided a search algorithm to list the output differences γ that maximize $\mathrm{adp}^{\oplus}$ for a given (α, β). Although this search algorithm can be very helpful, it cannot be used to provide general statements that hold for any value of n. At FSE 2011, Velichkov et al. [VMDCP11] explained how to calculate the additive differential probability of one ARX operation. Sun et al. [SHW+16] showed how to model $\mathrm{adp}^{\oplus}$ using the Mixed-Integer Linear Programming (MILP) approach for differential cryptanalysis [MWGP11].

Compared to additive differences, XOR differences not only propagate through two operations with probability one (XOR and rotation) instead of only one operation (addition). Another advantage of using XOR differences over additive differences is that the differential probabilities have simpler expressions (see Lipmaa et al. [LWD04, Table 3]). Lipmaa et al. [LWD04] pointed out that the number of possible differentials is larger for $\mathrm{adp}^{\oplus}$ than for xdp^{+}, but the average possible differential has a smaller probability.

Despite the advantages of using XOR differences, there are ciphers for which additive differences may be more appropriate. For example, when Biryukov and Velichkov [BV14] provided a differential cryptanalysis using additive differences for TEA [WN94] and Raiden [PHCER08]; they argued that additive differences are more appropriate given that round keys and round constants are added (instead of XORed), and that there is a higher number of add operations compared to XOR operations in one round. In similar spirit, when Sparx and LAX were proposed by Dinu et al. [DPU+16], and when Beierle et al. [BBCdS+20a] introduced the ARX-based S-box called Alzette (used in CRAX, TRAX and Sparkle) [BBCdS+20a], they provided some rationale of why their designs resist differential attacks using additive differences.

Lastly, we would like to point out that care should be taken when multiplying probabilities of differentials. For example, in the differential cryptanalysis of XTEA [NW97] by Hong et al. [HHK+03] using XOR differences, the authors constructed a three-round iterative trail $(\alpha, 0) \to (\alpha, 0)$, where $\alpha = \texttt{0x80402010}$. The trail contains two consecutive addition operations, which separately have probabilities $\mathrm{xdp}^{+}(\alpha, 0 \to \alpha) = 2^{-3}$ and $\mathrm{xdp}^{+}(\alpha, \alpha \to 0) = 2^{-3}$. Hong et al. found that the joint probability $\mathrm{xdp}^{+}(\alpha, 0, \alpha \to 0)$ is higher than the product of the two probabilities $2^{-3} \cdot 2^{-3} = 2^{-6}$, and estimated the probability to be $2^{-4.755}$. Mouha et al. [MVDCP11, Sect. 3.6] revisited this problem by correctly calculating the XOR-differential probability of the three-input addition as 2^{-3}, which can be trivially confirmed using the commutative property of addition: $\mathrm{xdp}^{+}(\alpha, \alpha \to 0) \cdot \mathrm{xdp}^{+}(0, 0 \to 0) = 2^{-3} \cdot 1 = 2^{-3}$.

Mutatis mutandis, a similar observation also holds when analyzing, for example, the two consecutive XOR operations in one round of TEA using additive differences: calculating the differential probabilities of each XOR operation separately using the formulas in this paper and multiplying them, may not lead to a correct estimate. Therefore, some caution is needed when applying the results in this paper to differential trails of an ARX primitive. We consider these issues to be outside the scope of this paper, but we mention the analysis of larger components as a suggestion for future work in Sect. 9.

3 Definitions

Let G, H be abelian groups and $f : G \to H$ be a function. *A differential* of f is a pair $(\alpha, \beta) \in G \times H$ denoted by $\alpha \to \beta$, where f maps some $x, x + \alpha \in G$ to $f(x), f(x) + \beta \in H$ respectively. *The differential probability* is defined as

$$\mathrm{dp}^{f}(\alpha \to \beta) = \Pr_{x \in G}[f(x + \alpha) = f(x) + \beta].$$

In this work, we consider the additive differential probability $\mathrm{adp}^{\oplus}$ of exclusive-or, i. e., $G = H = \mathbb{Z}_{2^n}$ and the function $f(x, y) = x \oplus y$ in two arguments. In other words,

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \Pr_{x,y \in \mathbb{F}_2^n}[(x + \alpha) \oplus (y + \beta) = \gamma + (x \oplus y)].$$

For convenience, we denote that $x, y, \alpha, \beta, \gamma \in \mathbb{F}_2^n$, i. e., they are elements of the n-dimensional vector space over the two-element field. In this context, $x + y$, $x - y$ and $-x$ mean $x' + y' \mod 2^n$, $x' - y' \mod 2^n$ and $-x' \mod 2^n$ respectively, where $x' = x_0 + x_1 2^1 + ... + x_{n-1} 2^{n-1}$ (the same for y'), i. e., x is a binary representation of the integer $x' \in \{0, \dots, 2^n - 1\}$. Note that the coordinates of $x \in \mathbb{F}_2^n$ start with 0: $x = (x_0, x_1, \dots, x_{n-1})$.

Working with $\mathbb{F}_2^n$, we denote the XOR operation by $x \oplus y$. Also, we define

$$\overline{x} = (x_0 \oplus 1, x_1 \oplus 1, \dots, x_{n-1} \oplus 1).$$

By 0^n and 1^n we denote $(0, \dots, 0)$ and $(1, \dots, 1) \in \mathbb{F}_2^n$ respectively. We will often use integers, e. g., 0 and 2^{n-1}, instead of elements of $\mathbb{F}_2^n$ if n is clear from the context.

There is a matrix (or rational series) approach for calculating $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma), \alpha, \beta, \gamma \in \mathbb{F}_2^n$. Let $e_0, \dots, e_7$ be standard basis vectors of $\mathbb{Q}^8$ (they are vector-columns).

Theorem 1 (Lipmaa et al. [LWD04])**.** *Let* $L = (1, 1, 1, 1, 1, 1, 1, 1)$*,* $A_0, \dots, A_7$ *be* 8×8

matrices, where

$$A_0 = \frac{1}{4}\begin{pmatrix} 4 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and $A_k = ((A_k)_{i,j}) = ((A_0)_{i\oplus k, j\oplus k})$*, here* $i, j, k \in \mathbb{F}_2^3$*. Then*

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\omega) = L A_{\omega_{n-1}} A_{\omega_{n-2}} \ldots A_{\omega_0} e_0,$$

where the differential $(\alpha, \beta \to \gamma)$ *is written as the octal word* $\omega = \omega_{n-1} \ldots \omega_0$ *with* $\omega_i = \omega_i(\alpha, \beta, \gamma) = 4\alpha_i + 2\beta_i + \gamma_i$*. For convenience, the matrices* $A_0, ..., A_7$ *are given below.*

$$\begin{array}{cccc}
A_0 & A_1 & A_2 & A_3 \\
\frac{1}{4}\begin{pmatrix} 4&0&0&1&0&1&1&0\\0&0&0&1&0&1&0&0\\0&0&0&1&0&0&1&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&1&1&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0 \end{pmatrix} &
\frac{1}{4}\begin{pmatrix} 0&0&1&0&1&0&0&0\\0&4&1&0&1&0&0&1\\0&0&1&0&0&0&0&0\\0&0&1&0&0&0&0&1\\0&0&0&0&1&0&0&0\\0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1 \end{pmatrix} &
\frac{1}{4}\begin{pmatrix} 0&1&0&0&1&0&0&0\\0&1&0&0&0&0&0&0\\0&1&4&0&1&0&0&1\\0&1&0&0&0&0&0&1\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&1 \end{pmatrix} &
\frac{1}{4}\begin{pmatrix} 1&0&0&0&0&0&0&0\\1&0&0&0&0&1&0&0\\1&0&0&0&0&0&1&0\\1&0&0&4&0&1&1&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&1&1&0 \end{pmatrix} \\
A_4 & A_5 & A_6 & A_7 \\
\frac{1}{4}\begin{pmatrix} 0&1&1&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&1&1&0&4&0&0&1\\0&1&0&0&0&0&0&1\\0&0&1&0&0&0&0&1\\0&0&0&0&0&0&0&1 \end{pmatrix} &
\frac{1}{4}\begin{pmatrix} 1&0&0&0&0&0&0&0\\1&0&0&1&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\\1&0&0&0&0&0&1&0\\1&0&0&1&0&4&1&0\\0&0&0&0&0&0&1&0\\0&0&0&1&0&0&1&0 \end{pmatrix} &
\frac{1}{4}\begin{pmatrix} 1&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\1&0&0&1&0&0&0&0\\0&0&0&1&0&0&0&0\\1&0&0&0&0&1&0&0\\0&0&0&0&0&1&0&0\\1&0&0&1&0&1&4&0\\0&0&0&1&0&1&0&0 \end{pmatrix} &
\frac{1}{4}\begin{pmatrix} 0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&1&1&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&1&0&0&1&0&0&0\\0&0&1&0&1&0&0&0\\0&1&1&0&1&0&0&4 \end{pmatrix}
\end{array}$$

Note that we consider coordinates $\{0, \ldots, 7\}$ in terms of $\mathbb{Z}_{2^3}$ and $\mathbb{F}_2^3$ by their binary representations too. By the matrix approach it is easy to check (see [LWD04]) that

Lemma 1. *We have* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) > 0$ *if and only if the first (i. e., least significant) nonzero coordinate of* $\omega(\alpha, \beta, \gamma)$ *is equal to* $3, 5$ *or* 6*.*

Lemma 2. *We have* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ *equal to either* 0 *or* 1 *for* $\alpha, \beta, \gamma \in \mathbb{F}_2$ *and equal to either* 0 *or* $\frac{1}{2}$ *or* 1 *for* $\alpha, \beta, \gamma \in \mathbb{F}_2^2$*.*

Lemma 3. *We have* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = 1$ *if and only if* $\omega(\alpha, \beta, \gamma) = v0^*$*, where* $v \in \{0, 3, 5, 6\}$*.*

4 Argument Symmetries of $\mathrm{adp}^{\oplus}$

First, we list several argument symmetries of $\mathrm{adp}^{\oplus}$.

Proposition 1. *The function* $\mathrm{adp}^{\oplus}$ *is symmetric, i. e., for any* $\alpha, \beta, \gamma \in \mathbb{F}_2^n$*, it holds that*

$$\begin{aligned} &\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\beta, \alpha \to \gamma) = \mathrm{adp}^{\oplus}(\beta, \gamma \to \alpha) \\ = \ &\mathrm{adp}^{\oplus}(\gamma, \beta \to \alpha) = \mathrm{adp}^{\oplus}(\gamma, \alpha \to \beta) = \mathrm{adp}^{\oplus}(\alpha, \gamma \to \beta). \end{aligned}$$

Proof. We have $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\beta, \alpha \to \gamma)$ by definition. Furthermore,

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) &= \Pr_{x,y\in\mathbb{F}_2^n}[((x+\alpha)\oplus(y+\beta)) - (x\oplus y) = \gamma] \\
&= \Pr_{x,y\in\mathbb{F}_2^n}[((x+\alpha)\oplus(y+\beta)) = (x\oplus y) + \gamma] \\
&= \Pr_{x,y\in\mathbb{F}_2^n}[((x+\alpha)\oplus(y+\beta)) \oplus ((x\oplus y) + \gamma) = 0] \\
&= \Pr_{z=x\oplus y, y\in\mathbb{F}_2^n}[((z\oplus y)+\alpha)\oplus(y+\beta)\oplus(z+\gamma) = 0] \\
&= \Pr_{z,y\in\mathbb{F}_2^n}[(z+\gamma)\oplus(y+\beta) = (z\oplus y)+\alpha] \\
&= \Pr_{z,y\in\mathbb{F}_2^n}[(z+\gamma)\oplus(y+\beta) - (z\oplus y) = \alpha] \\
&= \mathrm{adp}^{\oplus}(\gamma, \beta \to \alpha).
\end{aligned}$$

Note that all other argument permutations are combinations of these two. □

Proposition 2. *For any $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ it holds that*

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha + 2^{n-1}, \beta + 2^{n-1} \to \gamma) = \mathrm{adp}^{\oplus}(\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1} \to \gamma),$$

in light of Proposition 1, we can add 2^{n-1} to any two arguments.

Proof. It is easy to see that $\alpha + 2^{n-1} = \alpha \oplus 2^{n-1}$, therefore, $\alpha + x + 2^{n-1} = (\alpha + x) \oplus 2^{n-1}$, where $x \in \mathbb{F}_2^n$. Thus,

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) &= \Pr_{x,y\in\mathbb{F}_2^n}[((x+\alpha)\oplus(y+\beta)) - (x\oplus y) = \gamma] \\
&= \Pr_{x,y\in\mathbb{F}_2^n}[\big((x+\alpha)\oplus 2^{n-1}\oplus(y+\beta)\oplus 2^{n-1}\big) - (x\oplus y) = \gamma] \\
&= \Pr_{x,y\in\mathbb{F}_2^n}[\big((x+\alpha+2^{n-1})\oplus(y+\beta+2^{n-1})\big) - (x\oplus y) = \gamma] \\
&= \mathrm{adp}^{\oplus}(\alpha + 2^{n-1}, \beta + 2^{n-1} \to \gamma).
\end{aligned}$$

□

Proposition 3. *For any $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ it holds that* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \beta \to -\gamma)$. *In light of Proposition 1, we can replace by "$-$" any argument without changing the value of* $\mathrm{adp}^{\oplus}$.

Proof. First, we prove that

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) &= \Pr_{x,y\in\mathbb{F}_2^n}[((x+\alpha)\oplus(y+\beta)) - (x\oplus y) = \gamma] \\
&= \Pr_{x,y\in\mathbb{F}_2^n}[(x\oplus y) - ((x+\alpha)\oplus(y+\beta)) = -\gamma] \\
&= \Pr_{x'=x+\alpha, y'=y+\beta\in\mathbb{F}_2^n}[((x'-\alpha)\oplus(y'-\beta)) - (x'\oplus y') = -\gamma] \\
&= \mathrm{adp}^{\oplus}(-\alpha, -\beta \to -\gamma). \qquad (1)
\end{aligned}$$

For further calculations we will use that $\overline{x+y} = \overline{x} - y$. To confirm this, we have

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

Therefore, $\overline{x} = -x - 1$ and

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

Next, we prove that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(-\alpha, -\beta \to \gamma)$:

$$\begin{aligned}
\mathrm{adp}^{\oplus}(-\alpha, -\beta \to \gamma) &= \Pr_{x,y \in \mathbb{F}_2^n}[((x-\alpha) \oplus (y-\beta)) - (x \oplus y) = \gamma] \\
&= \Pr_{x'=\overline{x}, y'=\overline{y} \in \mathbb{F}_2^n}[\big((\overline{x'}-\alpha) \oplus (\overline{y'}-\beta)\big) - (\overline{x'} \oplus \overline{y'}) = \gamma] \\
&= \Pr_{x',y' \in \mathbb{F}_2^n}[\big(\overline{x'+\alpha} \oplus \overline{y'+\beta}\big) - (\overline{x'} \oplus \overline{y'}) = \gamma] \\
&\overset{u \oplus v = \overline{u} \oplus \overline{v}}{=} \Pr_{x',y' \in \mathbb{F}_2^n}[((x'+\alpha) \oplus (y'+\beta)) - (x' \oplus y') = \gamma] \\
&= \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma). \qquad (3)
\end{aligned}$$

Finally, we have

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha, \beta \to -\gamma) &\overset{(1)}{=} \mathrm{adp}^{\oplus}(-\alpha, -\beta \to -(-\gamma)) \\
&= \mathrm{adp}^{\oplus}(-\alpha, -\beta \to \gamma) \\
&\overset{(3)}{=} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma).
\end{aligned}$$

□

5 Maximum of $\mathrm{adp}^{\oplus}(x, y \to \gamma)$ for Fixed γ

In this section we give the missing proof of Theorem 3 from [LWD04]: we will prove that

$$\max_{\alpha,\beta \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma).$$

Let us define

$$A'_t = \begin{cases} A_0, & \text{if } t \text{ is even} \\ A_3, & \text{if } t \text{ is odd} \end{cases} \quad \text{and} \quad \overline{A'_t} = \begin{cases} A_3, & \text{if } t \text{ is even} \\ A_0, & \text{if } t \text{ is odd} \end{cases}.$$

Then

$$\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = LA'_{\omega_{n-1}} \ldots A'_{\omega_0} e_0 \text{ for any } \omega = \omega(\alpha, \beta, \gamma).$$

Lemma 4. *For any octal word $\omega_n \ldots \omega_0$, where $n \geq 0$, and $0 \leq k \leq 7$ the following holds:*

$$LA_{\omega_n} \ldots A_{\omega_0} e_k = LA_{\omega_n \oplus k} \ldots A_{\omega_0 \oplus k} e_0.$$

Proof. Let us denote by T_k the 8×8 involution matrix that swaps the i and $i \oplus k$ coordinates, $i = 0, \ldots, 7$. Then

$$\begin{aligned}
LA_{\omega_n} \ldots A_{\omega_0} e_k &= (LT_k) A_{\omega_n} \ldots A_{\omega_0} (T_k e_0) \\
&= L(T_k A_{\omega_n} T_k)(T_k A_{\omega_{n-1}} T_k) \ldots (T_k A_{\omega_0} T_k) e_0 \\
&= LA_{\omega_n \oplus k} \ldots A_{\omega_0 \oplus k} e_0,
\end{aligned}$$

since $(T_k A_m T_k)_{ij} = (A_m)_{i \oplus k, j \oplus k} = (A_0)_{i \oplus m \oplus k, j \oplus m \oplus k} = (A_{m \oplus k})_{ij}$ and T_k^2 is the identity matrix. □

Note that $A'_{\omega_i \oplus k} = A'_{\omega_i}$ for even k (as an integer number, i. e., for $k = 0, 2, 4, 6$) and $A'_{\omega_i \oplus k} = \overline{A'_{\omega_i}}$ for odd k.

Theorem 2. *For any $\gamma \in \mathbb{F}_2^n$, we have*

$$\max_{\alpha,\beta \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma).$$

Proof. Let us use induction by n. The base case of the induction, $n = 1$, follows from Lemma 2: it holds that $\mathrm{adp}^{\oplus}(0, 0 \to 0) = \mathrm{adp}^{\oplus}(0, 1 \to 1) = 1$.

Suppose that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leq \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ for any $\alpha, \beta, \gamma \in \mathbb{F}_2^n$. This means that

$$LA_{v_{n-1}} \ldots A_{v_0} e_0 \leq LA'_{v_{n-1}} \ldots A'_{v_0} e_0$$

for any octal word v of length n. Let us prove that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leq \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, where $\alpha, \beta, \gamma \in \mathbb{F}_2^{n+1}$, i. e.,

$$LA_{\omega_n} \ldots A_{\omega_0} e_0 \leq LA'_{\omega_n} \ldots A'_{\omega_0} e_0$$

for any octal word ω of length $n+1$. We consider four cases for A_{ω_0}, the first two of them are very easy.
Case $A_{\omega_0} \in \{A_1, A_2, A_4, A_7\}$:

$$LA_{\omega_n} \ldots A_{\omega_0} e_0 \overset{\text{Lemma 1}}{=} 0 < LA'_{\omega_n} \ldots A'_{\omega_0} e_0.$$

Case $A_{\omega_0} = A_0$, i. e., $A'_{\omega_0} = A_0$:

$$\begin{aligned} LA_{\omega_n} \ldots A_{\omega_0} e_0 &= LA_{\omega_n} \ldots A_{\omega_1} e_0 \\ &\overset{\text{induction}}{\leq} LA'_{\omega_n} \ldots A'_{\omega_1} e_0 \\ &= LA'_{\omega_n} \ldots A'_{\omega_0} e_0. \end{aligned}$$

Case $A_{\omega_0} = A_6$, i. e., $A'_{\omega_0} = A_0$. It is easy to see that

$$A_6 e_0 = \frac{1}{4} e_0 + \frac{1}{4} e_2 + \frac{1}{4} e_4 + \frac{1}{4} e_6.$$

Also, if $\omega_1 \in \{0, 3, 5, 6\}$, $LA_{\omega_n} \ldots A_{\omega_1}(e_2 + e_4) = 0$; otherwise $LA_{\omega_n} \ldots A_{\omega_1}(e_0 + e_6) = 0$. Indeed, $A_{\omega_1} e_2 = A_{\omega_1} e_4 = 0$ if $\omega_1 \in \{0, 3, 5, 6\}$ and $A_{\omega_1} e_0 = A_{\omega_1} e_6 = 0$ if $\omega_1 \in \{1, 2, 4, 7\}$. Thus, we can deduce that

$$LA_{\omega_n} \ldots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \ldots A_{\omega_1} e_{p_1} + \frac{1}{4} LA_{\omega_n} \ldots A_{\omega_1} e_{p_2},$$

where p_1 and p_2 are even. According to Lemma 4,

$$\begin{aligned} LA_{\omega_n} \ldots A_{\omega_0} e_0 &= \frac{1}{4} LA_{\omega_n \oplus p_1} \ldots A_{\omega_1 \oplus p_1} e_0 + \frac{1}{4} LA_{\omega_n \oplus p_2} \ldots A_{\omega_1 \oplus p_2} e_0 \\ &\overset{\text{induction}}{\leq} \frac{1}{4} LA'_{\omega_n \oplus p_1} \ldots A'_{\omega_1 \oplus p_1} e_0 + \frac{1}{4} LA'_{\omega_n \oplus p_2} \ldots A'_{\omega_1 \oplus p_2} e_0. \end{aligned}$$

Taking into account that both $\omega_i \oplus p_1$ and $\omega_i \oplus p_2$ are even if and only if ω_i is even (as an integer number), we have $A'_{\omega_i \oplus p_j} = A'_{\omega_i}$ (here $i \in \{1, \ldots, n\}$, $j \in \{1, 2\}$). Therefore,

$$\begin{aligned} LA_{\omega_n} \ldots A_{\omega_0} e_0 &\leq \frac{1}{4} LA'_{\omega_n} \ldots A'_{\omega_1} e_0 + \frac{1}{4} LA'_{\omega_n} \ldots A'_{\omega_1} e_0 \\ &= \frac{1}{2} LA'_{\omega_n} \ldots A'_{\omega_1} e_0. \end{aligned}$$

Finally, let us calculate $LA'_{\omega_n} \ldots A'_{\omega_0} e_0$. Recall that $A'_{\omega_0} = A_0$ for the case that we are considering here, and that $A_0 e_0 = e_0$, so that:

$$\begin{aligned} LA'_{\omega_n} \ldots A'_{\omega_0} e_0 &= LA'_{\omega_n} \ldots A'_{\omega_1} e_0 \\ &> \frac{1}{2} LA'_{\omega_n} \ldots A'_{\omega_1} e_0 \\ &\geq LA_{\omega_n} \ldots A_{\omega_0} e_0. \end{aligned} \tag{4}$$

Case $A_{\omega_0} \in \{A_3, A_5\}$, i. e., $A'_{\omega_0} = A_3$. It is easy to see that

$$\begin{aligned} A_3 e_0 &= \frac{1}{4}e_0 + \frac{1}{4}e_1 + \frac{1}{4}e_2 + \frac{1}{4}e_3, \\ A_5 e_0 &= \frac{1}{4}e_0 + \frac{1}{4}e_1 + \frac{1}{4}e_4 + \frac{1}{4}e_5. \end{aligned}$$

Note that $LA_{\omega_n} \dots A_{\omega_1} e_j = 0$ for

- $\omega_1 \in \{0,3,5,6\}$ and $j \notin \{0,3,5,6\}$,
- $\omega_1 \notin \{0,3,5,6\}$ and $j \in \{0,3,5,6\}$,

since in these cases $A_{\omega_1} e_j = 0$. The latter was already noted by Lipmaa et al. [LWD04] when they showed by direct computation that the kernels are $\ker A_0 = \ker A_3 = \ker A_5 = \ker A_6 = \langle e_1, e_2, e_4, e_7 \rangle$ and $\ker A_1 = \ker A_2 = \ker A_4 = \ker A_7 = \langle e_0, e_3, e_5, e_6 \rangle$.

Thus, we can deduce that

$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_p + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_q,$$

where p is even and q is odd. Moreover, either $p, q \in \{0,3,5,6\}$ or $p, q \in \{1,2,4,7\}$. Indeed,

- if $\omega_1 \in \{0,3,5,6\}$ and $A_{\omega_0} = A_3$,
$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_0 + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_3, \text{ i. e., } p = 0 \text{ and } q = 3;$$
- if $\omega_1 \in \{0,3,5,6\}$ and $A_{\omega_0} = A_5$,
$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_0 + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_5, \text{ i. e., } p = 0 \text{ and } q = 5;$$
- if $\omega_1 \notin \{0,3,5,6\}$ and $A_{\omega_0} = A_3$,
$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_1 + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_2, \text{ i. e., } p = 2 \text{ and } q = 1;$$
- if $\omega_1 \notin \{0,3,5,6\}$ and $A_{\omega_0} = A_5$,
$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_1 + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_4, \text{ i. e., } p = 4 \text{ and } q = 1.$$

According to Lemma 4,

$$\begin{aligned} LA_{\omega_n} \dots A_{\omega_0} e_0 \quad &= \quad \frac{1}{4} LA_{\omega_n \oplus p} \dots A_{\omega_1 \oplus p} e_0 + \frac{1}{4} LA_{\omega_n \oplus q} \dots A_{\omega_1 \oplus q} e_0 \\ &\overset{\text{induction}}{\leq} \quad \frac{1}{4} LA'_{\omega_n \oplus p} \dots A'_{\omega_1 \oplus p} e_0 + \frac{1}{4} LA'_{\omega_n \oplus q} \dots A'_{\omega_1 \oplus q} e_0. \end{aligned} \tag{5}$$

Taking into account that $\omega_i \oplus p$ is even if and only if ω_i is even and $\omega_i \oplus q$ is even if and only if ω_i is odd, it is easy to see that $A'_{\omega_i \oplus p} = A'_{\omega_i}$ and $A'_{\omega_i \oplus q} = \overline{A'_{\omega_i}}$. Therefore,

$$LA_{\omega_n} \dots A_{\omega_0} e_0 \leq \frac{1}{4} LA'_{\omega_n} \dots A'_{\omega_1} e_0 + \frac{1}{4} L\overline{A'_{\omega_n}} \dots \overline{A'_{\omega_1}} e_0.$$

To complete the case, let us calculate $LA'_{\omega_n} \dots A'_{\omega_0} e_0$:

$$\begin{aligned} LA'_{\omega_n} \dots A'_{\omega_0} e_0 \quad &= \quad LA'_{\omega_n} \dots A'_{\omega_1} (\frac{1}{4}e_0 + \frac{1}{4}e_3) \\ &\overset{\text{Lemma 4}}{=} \quad \frac{1}{4} LA'_{\omega_n} \dots A'_{\omega_1} e_0 + \frac{1}{4} LA'_{\omega_n \oplus 3} \dots A'_{\omega_1 \oplus 3} e_0 \\ &= \quad \frac{1}{4} LA'_{\omega_n} \dots A'_{\omega_1} e_0 + \frac{1}{4} L\overline{A'_{\omega_n}} \dots \overline{A'_{\omega_1}} e_0 \\ &\geq \quad LA_{\omega_n} \dots A_{\omega_0} e_0. \end{aligned}$$

This completes the proof of the theorem. □

In light of Proposition 1, it does not matter which argument we fix: $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leq \mathrm{adp}^{\oplus}(\alpha, \alpha \to 0)$ and $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leq \mathrm{adp}^{\oplus}(\beta, \beta \to 0)$ hold too.

6 Number of Maximums of $\mathrm{adp}^{\oplus}$ for Fixed γ

Let us define

$$\mathrm{adpmax}(\gamma) = \{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \ : \mathrm{adp}^{\oplus}(x, y \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)\},\ \gamma \in \mathbb{F}_2^n.$$

Proposition 4. *Let $\gamma \in \mathbb{F}_2^n$, $\gamma \in \{0, 2^{n-1}\}$. Then $\#\mathrm{adpmax}(\gamma) = 2$. More precisely,*

$$\mathrm{adpmax}(0) = \{(0, 0), (2^{n-1}, 2^{n-1})\},$$
$$\mathrm{adpmax}(2^{n-1}) = \{(0, 2^{n-1}), (2^{n-1}, 0)\}.$$

Proof. According to Lemma 3, $\mathrm{adp}^{\oplus}(0, 0 \to 0) = \mathrm{adp}^{\oplus}(0, 2^{n-1} \to 2^{n-1}) = 1$. The lemma also provides the conditions for α, β, γ such that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = 1$:

$$4\alpha_i + 2\beta_i + \gamma_i = 0 \text{ for } 0 \leq i < n-1 \text{ and } 4\alpha_{n-1} + 2\beta_{n-1} + \gamma_{n-1} \in \{0, 3, 5, 6\},$$

i. e., $\alpha_i = \beta_i = \gamma_i = 0$ for $0 \leq i < n-1$ and $(\alpha_{n-1}, \beta_{n-1}, \gamma_{n-1})$ is either $(0, 0, 0)$ or $(1, 1, 0)$ or $(1, 0, 1)$ or $(0, 1, 1)$. □

Proposition 5. *Let $\gamma \in \mathbb{F}_2^n$, $\gamma \notin \{0, 2^{n-1}\}$. Then the following eight pairs are distinct and belong to* $\mathrm{adpmax}(\gamma)$*:*

$$\begin{array}{llll} (0, \gamma), & (0, -\gamma), & (2^{n-1}, \gamma \oplus 2^{n-1}), & (2^{n-1}, -\gamma \oplus 2^{n-1}), \\ (\gamma, 0), & (-\gamma, 0), & (\gamma \oplus 2^{n-1}, 2^{n-1}), & (-\gamma \oplus 2^{n-1}, 2^{n-1}). \end{array}$$

Proof. Theorem 2 gives us that $(0, \gamma) \in \mathrm{adpmax}(\gamma)$. The other pairs are provided by Propositions 1, 2 and 3, since $\mathrm{adp}^{\oplus}$ has the same value for these pairs with fixed γ.

Next, we know that $\gamma \notin \{0, 2^{n-1}\}$. Let us divide these pairs into two sets: $P = \{(0, \gamma), (0, -\gamma), (\gamma, 0), (-\gamma, 0)\}$ and P' contains the other pairs.

Any two pairs from P are distinct, since $\gamma \neq -\gamma$ and $\gamma, -\gamma \neq 0$. The same is true for P': indeed, any pair $(a, b) \in P'$ is equal to $(a' \oplus 2^{n-1}, b' \oplus 2^{n-1})$, where $(a', b') \in P$. This is why any two pairs from P' coincide if and only if the corresponding pairs from P coincide.

At the same time, a pair from P cannot be equal to a pair from P', since at least one coordinate of any pair from P' is equal to 2^{n-1}, but $0, \gamma, -\gamma \neq 2^{n-1}$. □

To prove auxiliary lemmas, we introduce the following notation: for $A \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n$, let us define $\mathrm{swap}(A) = \{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : (y, x) \in A\}$. It is clear that $\#\mathrm{swap}(A) = \#A$. Also,

$$\mathrm{perfmax}(\gamma) = \{(x, y) \in \mathrm{adpmax}(\gamma) : (x, \overline{y}) \in \mathrm{adpmax}(\overline{\gamma})\}. \tag{6}$$

Note that $\mathrm{swap}(\mathrm{adpmax}(\gamma)) = \mathrm{adpmax}(\gamma)$, since $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\beta, \alpha \to \gamma)$ by Proposition 1. Therefore,

$$\mathrm{swap}(\mathrm{perfmax}(\gamma)) = \{(x, y) \in \mathrm{adpmax}(\gamma) : (\overline{x}, y) \in \mathrm{adpmax}(\overline{\gamma})\}. \tag{7}$$

Let us list some of their straightforward properties.

Lemma 5. *The following statements hold:*

- $\#\mathrm{perfmax}(\gamma) \leq \min\{\#\mathrm{adpmax}(\gamma), \#\mathrm{adpmax}(\overline{\gamma})\}$*;*
- $(\alpha, \beta) \in \mathrm{perfmax}(\gamma)$ *if and only if* $(\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1}) \in \mathrm{perfmax}(\gamma)$.

Proof. The first point directly follows from the definition. Next, Proposition 2 provides that

$$(\alpha, \beta) \in \mathrm{adpmax}(\gamma) \iff (\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1}) \in \mathrm{adpmax}(\gamma),$$
$$(\alpha, \overline{\beta}) \in \mathrm{adpmax}(\overline{\gamma}) \iff (\alpha \oplus 2^{n-1}, \overline{\beta} \oplus 2^{n-1}) \in \mathrm{adpmax}(\overline{\gamma}).$$

The equality $\overline{\beta \oplus 2^{n-1}} = \overline{\beta} \oplus 2^{n-1}$ completes the proof. □

Lemma 6. *Let* $\gamma \in \mathbb{F}_2^n$, $\#\mathrm{adpmax}(\gamma) \leq 8$ *and* $\#\mathrm{adpmax}(\overline{\gamma}) \leq 8$. *Then* $\#\mathrm{perfmax}(\gamma) \leq 2$.

Proof. Let $\gamma \in \{0, 2^{n-1}\}$. Lemma 5 provides that $\#\mathrm{perfmax}(\gamma) \leq \#\mathrm{adpmax}(\gamma)$. At the same time, $\#\mathrm{adpmax}(\gamma) = 2$ by Proposition 4. The case of $\overline{\gamma} \in \{0, 2^{n-1}\}$ is completely identical. Hence, the lemma is proven for these cases.

Let $\gamma, \overline{\gamma} \notin \{0, 2^{n-1}\}$. Note that this excludes the case of $n = 1$. Under the lemma assumption, Proposition 5 describes all 8 distinct pairs from $\mathrm{adpmax}(\gamma)$ (the same for $\mathrm{adpmax}(\overline{\gamma})$). In light of Lemma 5, it is sufficient to prove that at most one pair from $P = \{(0, \gamma), (0, -\gamma), (\gamma, 0), (-\gamma, 0)\} \subseteq \mathrm{adpmax}(\gamma)$ belongs to $\mathrm{perfmax}(\gamma)$, since any of the other four pairs from $\mathrm{adpmax}(\gamma)$ are equal to $(\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1})$, where $(\alpha, \beta) \in P$.

First, we consider $(\gamma, 0)$ and $(-\gamma, 0)$. Since $\gamma \notin \{0, 2^{n-1}\}$ and $n > 1$, we have $\gamma, -\gamma, \overline{0} \notin \{0, 2^{n-1}\}$. But one coordinate of any pair from $\mathrm{adpmax}(\overline{\gamma})$ is always equal to 0 or 2^{n-1}, i. e., both $(\gamma, \overline{0})$ and $(-\gamma, \overline{0})$ do not belong to $\mathrm{adpmax}(\overline{\gamma})$ and, as a consequence, they are not elements of $\mathrm{perfmax}(\gamma)$.

Next, we consider $(\alpha, \beta) = (0, -\gamma)$. Using (2), we obtain

$$\begin{aligned} (\alpha, \overline{\beta}) &= (0, \overline{-\gamma}) \\ &\overset{\overline{x} = -x-1}{=} (0, -(-\gamma) - 1) \\ &\overset{-x = \overline{x}+1}{=} (0, -(\overline{\gamma} + 1) - 1) \\ &= (0, -\overline{\gamma} - 2). \end{aligned}$$

Since $\alpha = 0$, let us consider the first elements of the pairs from $\mathrm{adpmax}(\overline{\gamma})$ described by Proposition 5: none of $\overline{\gamma}$, $-\overline{\gamma}$, $\overline{\gamma} \oplus 2^{n-1}$, $-\overline{\gamma} \oplus 2^{n-1}$, 2^{n-1} is equal to 0 due to $\overline{\gamma} \notin \{0, 2^{n-1}\}$. It means that $(\alpha, \overline{\beta})$ may only be equal to $(0, \overline{\gamma})$ or $(0, -\overline{\gamma})$ from $\mathrm{adpmax}(\overline{\gamma})$.

This implies that γ satisfies one of the two following equalities:

- $-\overline{\gamma} - 2 = -\overline{\gamma}$, which is inconsistent for $n > 1$;
- $-\overline{\gamma} - 2 = \overline{\gamma}$, i. e., $2\overline{\gamma} + k2^n = -2$, where $k \in \mathbb{Z}$ or, equivalently,

  $$\overline{\gamma} = -1 - k2^{n-1}, \text{ where } k = \{0, 1\}, \text{ since } k2^{n-1} \bmod 2^n \in \{0, 2^{n-1}\}.$$

  By again using (2), we have that $\overline{\gamma} = -1 - k2^{n-1} = \overline{k2^{n-1}}$. But $\overline{\gamma} = \overline{k2^{n-1}}$ (where $k = \{0, 1\}$) if and only if $\gamma \in \{0, 2^{n-1}\}$, which is a contradiction.

Thus, only $(0, \gamma)$ and $(2^{n-1}, \gamma \oplus 2^{n-1})$ belong to $\mathrm{perfmax}(\gamma)$. Thereby, the lemma is proven. □

Corollary 1. *Let* $\gamma \in \mathbb{F}_2^n$. *Then* $\#\mathrm{adpmax}(\gamma) \leq 8$.

Proof. Let us use induction by n. The base case of the induction, $n = 1$, is straightforward: the only possible values of γ are 0 and $2^{n-1} = 1$, for which Proposition 4 holds.

We suppose that $\#\mathrm{adpmax}(c) \leq 8$ for any $c \in \mathbb{F}_2^n$. Let us prove that $\#\mathrm{adpmax}(\gamma) \leq 8$ for $\gamma \in \mathbb{F}_2^{n+1}$. We denote $(x_0, \ldots, x_{n-1})$ by x' for $x \in \mathbb{F}_2^{n+1}$.

Case $\gamma_0 = 0$. Let us consider $(\alpha, \beta) \in \mathrm{adpmax}(\gamma)$. It is easy to see that $\omega_0(\alpha, \beta, \gamma) \notin \{2, 4\}$ (this follows from Case $A_{\omega_0} \in \{A_1, A_2, A_4, A_7\}$ of Theorem 2), and that $\omega_0(\alpha, \beta, \gamma) \neq 6$

(by (4) from the proof of Theorem 2). This means that $\alpha_0 = \beta_0 = 0$. Thus, $\#\mathrm{adpmax}(\gamma) = \#\mathrm{adpmax}(\gamma') \leq 8$ by induction.

Case $\gamma_0 = 1$. We rely on the case $A_{\omega_0} \in \{A_3, A_5\}$ of Theorem 2. Let us consider $(\alpha, \beta) \in \mathrm{adpmax}(\gamma)$. Like in the previous case, $\omega_0(\alpha, \beta, \gamma) \notin \{1, 7\}$, i. e., we have two variants: 3 or 5. Also, we have two distinct choices for $\omega_1(\alpha, \beta, \gamma)$: it can belong to either $\{0, 3, 5, 6\}$ or $\{1, 2, 4, 7\}$. Recall that p and q depend on this choice. Thus, we have $2 \cdot 2 = 4$ different "branches" for α, β. Let us consider any of them.

Let $p = 4p_1 + 2p_2$ (p is even), $q = 4q_1 + 2q_2 + 1$ (q is odd), where $p_1, p_2, q_1, q_2 \in \{0, 1\}$. Considering the sums $x \oplus p_i$, $x \oplus q_i$, where $x \in \mathbb{F}_2^n$, we mean $x \oplus 0^n$ for $p_i, q_i = 0$ and $x \oplus 1^n$ otherwise.

According to (5), $LA_{\omega_n} \dots A_{\omega_0} e_0 = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ is equal to $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ if and only if

- $LA_{\omega_n \oplus p} \dots A_{\omega_1 \oplus p} e_0 = \mathrm{adp}^{\oplus}(\alpha' \oplus p_1, \beta' \oplus p_2 \to \gamma')$ is equal to $\mathrm{adp}^{\oplus}(0, \gamma' \to \gamma')$ and
- $LA_{\omega_n \oplus q} \dots A_{\omega_1 \oplus q} e_0 = \mathrm{adp}^{\oplus}(\alpha' \oplus q_1, \beta' \oplus q_2 \to \gamma' \oplus 1^n)$ is equal to $\mathrm{adp}^{\oplus}(0, \overline{\gamma'} \to \overline{\gamma'})$.

It means that $(\alpha, \beta) \in \mathrm{adpmax}(\gamma)$ if and only if $(\alpha' \oplus p_1, \beta' \oplus p_2) \in \mathrm{adpmax}(\gamma')$ and $(\alpha' \oplus q_1, \beta' \oplus q_2) \in \mathrm{adpmax}(\gamma' \oplus 1) = \mathrm{adpmax}(\overline{\gamma'})$.

Since $p, q \in \{0, 3, 5, 6\}$ or $p, q \in \{1, 2, 4, 7\}$, $(p_1, p_2) \oplus (q_1, q_2) \in \{(0, 1), (1, 0)\}$. Thus, taking $a = \alpha' \oplus p_1$, $b = \beta' \oplus p_2$, we have $(\alpha' \oplus q_1, \beta' \oplus q_2) \in \{(a, \overline{b}), (\overline{a}, b)\}$. In other words, by (6) and (7),

$$\text{either } (a, b) \in \mathrm{perfmax}(\gamma') \text{ or } (a, b) \in \mathrm{swap}(\mathrm{perfmax}(\gamma')).$$

In light of the induction hypothesis, Lemma 6 provides that for the both cases

$$\#\mathrm{perfmax}(\gamma') = \#\mathrm{swap}(\mathrm{perfmax}(\gamma')) \leq 2,$$

i. e., there are at most two distinct pairs (a, b) satisfying the conditions. For any "branch" (a, b) uniquely determines (α, β). Therefore, we have at most $4 \cdot 2$ distinct choices for $(\alpha, \beta) \in \mathrm{adpmax}(\gamma)$. The statement is proven. □

7 Recurrence Formulas for $\mathrm{adp}^{\oplus}$

A matrix approach to calculate $\mathrm{adp}^{\oplus}$ and Lemma 4 allow us to obtain recurrence formulas for $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$. It is possible to rewrite the proof of Theorem 2 in terms of these formulas. First, let us denote the vector $(0, x_0, x_1, \dots, x_{n-1}) \in \mathbb{F}_2^{n+1}$ by $x0$, i. e., in terms of integers, $x0 = 2x$. We define $x1$: $x1 = 2x + 1$ in exactly the same way.

Let us prove an auxiliary lemma.

Lemma 7. *Let* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) > 0$. *Then* $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$.

Proof. By Lemma 1, $\omega_0 = 4\alpha_0 \oplus 2\beta_0 \oplus \gamma_0 \in \{0, 3, 5, 6\}$, which implies $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$. □

Now we can give the recurrence formulas for $\mathrm{adp}^{\oplus}$.

Theorem 3. *For all $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ the following equalities hold.*

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 0) = {} & \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma),\\
\mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 0) = {} & \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\overline{\alpha}, \overline{\beta} \to \gamma)\\
& + \frac{1}{4}\mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma),\\
\mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 1) = {} & \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \overline{\gamma})\\
& + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}) + \frac{1}{4}\mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \gamma),\\
\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) = {} & \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma})\\
& + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}),\\
\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 1) = {} & \mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 0)\\
= {} & \mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 1) = 0.
\end{aligned}$$

Note 1. Any of $\overline{\alpha}$, $\overline{\beta}$ and $\overline{\gamma}$ can be replaced by $\alpha + 1$, $\beta + 1$ and $\gamma + 1$, respectively. Indeed, $\overline{\alpha} \overset{(2)}{=} -\alpha - 1 = -(\alpha + 1)$, that we can transform to $\alpha + 1$ by Proposition 3, the same is true for $\overline{\beta}$ and $\overline{\gamma}$.

Proof. First, $\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ easily follows from the matrix representation. Next, $\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 1) = \mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 1) = 0$ since the sum of the least significant bits is odd, see Lemma 7.

In light of Proposition 1, it is sufficient to prove that

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) = {} & \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma})\\
& + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}).
\end{aligned}$$

By the matrix approach, $\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) = LA_{w_n} \ldots A_{w_0} e_0$, where $w_{i+1} = 4\alpha_i + 2\beta_i + \gamma_i$ and $w_0 = 4 \cdot 0 + 2 \cdot 1 + 1 \cdot 1 = 3$, next,

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) \quad & = \quad LA_{w_n} \ldots A_{w_0} e_0\\
& = \quad \frac{1}{4}LA_{w_n} \ldots A_{w_1} e_0 + \frac{1}{4}LA_{w_n} \ldots A_{w_1} e_1\\
& \qquad + \frac{1}{4}LA_{w_n} \ldots A_{w_1} e_2 + \frac{1}{4}LA_{w_n} \ldots A_{w_1} e_3\\
& \overset{\text{Lemma 4}}{=} \frac{1}{4}LA_{w_n} \ldots A_{w_1} e_0 + \frac{1}{4}LA_{w_n \oplus 1} \ldots A_{w_1 \oplus 1} e_0\\
& \qquad + \frac{1}{4}LA_{w_n \oplus 2} \ldots A_{w_1 \oplus 2} e_0 + \frac{1}{4}LA_{w_n \oplus 3} \ldots A_{w_1 \oplus 3} e_0,
\end{aligned}$$

At the same time,

$$\begin{aligned}
LA_{w_n} \ldots A_{w_1} e_0 & = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma),\\
LA_{w_n \oplus 1} \ldots A_{w_1 \oplus 1} e_0 & = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma \oplus 1^n) && = \mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}),\\
LA_{w_n \oplus 2} \ldots A_{w_1 \oplus 2} e_0 & = \mathrm{adp}^{\oplus}(\alpha, \beta \oplus 1^n \to \gamma) && = \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma),\\
LA_{w_n \oplus 3} \ldots A_{w_1 \oplus 3} e_0 & = \mathrm{adp}^{\oplus}(\alpha, \beta \oplus 1^n \to \gamma \oplus 1^n) && = \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma}),
\end{aligned}$$

which completes the proof. □

Corollary 2. *For any $\gamma \in \mathbb{F}_2^n$, we have*

$$\mathrm{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) = \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}).$$

Proof. Since $0 \oplus \overline{\gamma}_0 \oplus \gamma_0 = 1$, Lemma 7 provides that

$$\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \overline{\gamma}) = 0.$$

Therefore, $\mathrm{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) = \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma})$ by Theorem 3. □

Corollary 3. *For any of $\mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 0)$, $\mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 1)$, and $\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1)$, at least two terms of the corresponding sum in Theorem 3 are zero.*

Proof. In light of Proposition 1, it is sufficient to prove the statement for $\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1)$.

Since $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = \alpha_0 \oplus \overline{\beta}_0 \oplus \overline{\gamma}_0$ and $\alpha_0 \oplus \overline{\beta}_0 \oplus \gamma_0 = \alpha_0 \oplus \beta_0 \oplus \overline{\gamma}_0 = \alpha_0 \oplus \beta_0 \oplus \gamma_0 \oplus 1$, Lemma 7 provides that either

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma}) = 0 \text{ or}$$
$$\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}) = 0. \qquad \square$$

The recurrence formulas help to determine the minimum nonzero value of $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$:

Corollary 4. *Let $n > 1$. Then the minimum nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$, $\alpha, \beta, \gamma \in \mathbb{F}_2^n$, is equal to $8 \cdot 4^{-n}$.*

Note 2. The formula for $n = 1$ differs: Lemma 2 shows us that either $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = 0$ or $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = 1$ for $\alpha, \beta, \gamma \in \mathbb{F}_2$.

Proof. Let us denote this minimum nonzero value by m_n. Applying to a nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$, $\alpha, \beta, \gamma \in \mathbb{F}_2^{n+1}$, a recurrence formula from Theorem 3, it is easy to see that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \geq \frac{1}{4}m_n$, which implies $m_{n+1} \geq \frac{1}{4}m_n$.

Let us consider $\gamma_{10}^n = (1, 0, 1, 0, \ldots) \in \mathbb{F}_2^n$ (i. e., the least significant bit is 1 and each next bit is the negation of the previous bit), e. g., $\gamma_{10}^3 = (1, 0, 1)$. Also, $\alpha 1 = (1, \alpha_0, \alpha_1, ..., \alpha_{n-1})$ by definition, where α_0 is the least significant bit of α. Then, by the recurrence formulas,

$$\begin{aligned}
\mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1}) &= \mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \overline{\gamma_{10}^n}1) \\
&= \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \overline{\gamma_{10}^n}) + \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 0^n \to \gamma_{10}^n) \\
&\quad + \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 0^n \to \overline{\gamma_{10}^n}) + \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n) \\
&\overset{\text{Lemma 7}}{=} \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 0^n \to \overline{\gamma_{10}^n}) + \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n).
\end{aligned} \tag{8}$$

Moreover, the first (i. e., least significant) and the second bits of $\overline{\gamma_{10}}$ are 0 and 1 respectively, which implies that $\mathrm{adp}^{\oplus}(0^n, 0^n \to \overline{\gamma_{10}^n}) = 0$ for $n > 1$. Indeed, it holds by Lemma 1 since $\omega_0 = 4 \cdot 0 + 2 \cdot 0 + 0 = 0$ and $\omega_1 = 4 \cdot 0 + 2 \cdot 0 + 1 = 1 \notin \{0, 3, 5, 6\}$. Therefore, (8) provides that

$$\mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1}) = \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n) \text{ for } n > 1. \tag{9}$$

Let us prove by induction that

$$m_n = \mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n).$$

The base case of the induction is $n = 2$. According to (8) and Note 2, the minimum nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_2^2$ is $\mathrm{adp}^{\oplus}(0^2, 1^2 \to \gamma_{10}^2) = \frac{1}{2}$. Note that this is consistent with Lemma 2.

Now, we prove that if the minimum nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ is m_n, then the minimum nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_2^{n+1}$ is m_{n+1}.

$$\mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1}) \overset{(9)}{=} \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n) \overset{\text{induction}}{=} \frac{1}{4}m_n.$$

Note that $\mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1})$ is nonzero. Moreover, it is also the minimum nonzero value. This can be seen as follows. Clearly, there must exist some $\alpha, \beta, \gamma \in \mathbb{F}_2^{n+1}$ that corresponds to the minimum nonzero value, and therefore one of the eight recurrence formulas of Theorem 3 applies. As the value of $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ is nonzero, at least one term in the recurrence formulas must be nonzero, and therefore $m_{n+1} \geq \frac{1}{4}m_n$. We found this smallest nonzero value: $m_{n+1} = \mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1}) = \frac{1}{4}m_n$, thereby proving the induction step.

Finally, we can now express m_n in terms of n: $m_n = \frac{1}{2} \cdot (\frac{1}{4})^{n-2} = 8 \cdot 4^{-n}$ for $n > 1$ by (9). □

8 Properties of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$

8.1 Simplified Matrix Form for $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$

When calculating $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ using Theorem 1, we only need A_0 (for bit positions where $\gamma_i = 0$) and A_3 (for bit positions where $\gamma_i = 1$). These matrices can be minimized to size 3×3 using the S-function toolkit of Mouha et al. [MVDCP11]: applying the software toolkit to remove non-accessible states and to merge indistinguishable states leads to:

$$A_0'' = \frac{1}{4}\begin{pmatrix} 4 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_3'' = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 0 & 4 \end{pmatrix},$$

where A_0'' and A_3'' can be obtained from A_0 and A_3 by removing the last four columns (the non-accessible states) and rows, and by merging the middle two remaining rows and columns (which correspond to indistinguishable states).

Note that $(1,1,1)A_0'' = (1,1,1)A_3'' = (1,0,1)$, which will help us to minimize the size of the matrices to 2×2 if we "cheat" by excluding the most significant bit from the matrix product. More formally, we can obtain matrices B_0 and B_1 by removing all rows and columns from A_0 and A_3 except 0 and 3, and calculate $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ as follows:

Proposition 6. *Let $\gamma \in \mathbb{F}_2^n$. Then*

$$\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = (1,1)B_{\gamma_{n-2}}B_{\gamma_{n-3}} \dots B_{\gamma_0}(1,0)^T,$$

where

$$B_0 = \frac{1}{4}\begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_1 = \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 1 & 4 \end{pmatrix}.$$

Proof. According to Theorem 1, we can calculate $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ by matrices A_0 and A_3. First, A_0x^T and A_3x^T depend only on x_0, x_3, x_5, x_6, where $x \in \mathbb{Q}^8$. Secondly, they have a block structure

$$\begin{pmatrix} P_i & Q_i \\ 0 & Q_i \end{pmatrix},$$

where P_i and Q_i are matrices of size 4×4. In addition, coordinates $\{4, 5, 6, 7\}$ of e_0 are zero. This means that coordinates 5 and 6 of the vector $A_{\omega_i}A_{\omega_{i-1}} \dots A_{\omega_0}e_0$, where $\omega_i = 3\gamma_i$,

$i = 0, \dots, n-1$, are zero. Thus, we can consider only coordinates 0 and 3. It is easy to see that

$$(A_0x^T)_0 = x_0 + \frac{1}{4}x_3, \quad (A_0x^T)_3 = \frac{1}{4}x_3, \tag{10}$$

and

$$(A_3x^T)_0 = \frac{1}{4}x_0, \quad (A_3x^T)_3 = \frac{1}{4}x_0 + x_3. \tag{11}$$

Thus,

$$LA_0x^T = LA_3x^T = x_0 + x_3 + x_5 + x_6 = x_0 + x_3$$

for $x^T = A_{\omega_i}A_{\omega_{i-1}} \dots A_{\omega_0}e_0$ due to the block structure.

Finally, let us associate the first coordinate of a $v \in \mathbb{Q}^2$ with x_0 and the second coordinate with x_3. Then,

$$B_0v^T = \begin{pmatrix} v_0 + \frac{1}{4}v_1 \\ \frac{1}{4}v_1 \end{pmatrix}, \text{ which completely corresponds (10), and}$$

$$B_1v^T = \begin{pmatrix} \frac{1}{4}v_0 \\ \frac{1}{4}v_0 + v_1 \end{pmatrix}, \text{ which completely corresponds (11).}$$

Also, e_0 and $LA_0x^T = LA_3x^T = x_0 + x_3$ correspond $(1,0)^T$ and $(1,1)v^T = v_0 + v_1$ respectively, i. e.,

$$\begin{aligned} \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) &= (LA_{\omega_{n-1}})(A_{\omega_{n-2}} \dots A_{\omega_0}e_0) \\ &= (1,1)B_{\gamma_{n-2}}B_{\gamma_{n-3}} \dots B_{\gamma_0}(1,0)^T. \end{aligned}$$

□

8.2 Minimum of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$

Let us calculate the minimum value among $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$. We will start with the following lemma.

Lemma 8. *Let* $\gamma \in \mathbb{F}_2^n$. *Then* $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) < 3\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma})$.

Proof. By induction: for $n = 1$ the statement holds. Suppose that for any $\gamma \in \mathbb{F}_2^n$, it holds that $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) < 3\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma})$. Let us prove that the statement holds for $\gamma' \in \mathbb{F}_2^{n+1}$. We have two cases:

1. $\gamma' = \gamma 0$, $\gamma \in \mathbb{F}_2^n$. Then, using the recurrence formula for $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, we obtain

$$\mathrm{adp}^{\oplus}(0, \gamma 0 \to \gamma 0) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \frac{3}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma).$$

At the same time,

$$3\mathrm{adp}^{\oplus}(0, \overline{\gamma 0} \to \overline{\gamma 0}) = 3\mathrm{adp}^{\oplus}(0, \overline{\gamma}1 \to \overline{\gamma}1) = \frac{3}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{3}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}).$$

It completes the case, since $\frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) < \frac{3}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma})$ by the induction hypothesis.

2. $\gamma' = \gamma 1$, $\gamma \in \mathbb{F}_2^n$. Like for the previous point,

$$\mathrm{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}).$$

The induction hypothesis completes the proof, since

$$3\mathrm{adp}^{\oplus}(0, \overline{\gamma 1} \to \overline{\gamma 1}) = 3\mathrm{adp}^{\oplus}(0, \overline{\gamma}0 \to \overline{\gamma}0) = \frac{11}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}).$$

□

Corollary 5. *Let $\gamma \in \mathbb{F}_2^n$. Then* $\operatorname{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) < \operatorname{adp}^{\oplus}(0, \gamma 0 \to \gamma 0)$.

Proof. Indeed, $\operatorname{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) = \frac{1}{4}\operatorname{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\operatorname{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}) < \frac{1}{4}\operatorname{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{3}{4}\operatorname{adp}^{\oplus}(0, \gamma \to \gamma) = \operatorname{adp}^{\oplus}(0, \gamma \to \gamma) = \operatorname{adp}^{\oplus}(0, \gamma 0 \to \gamma 0)$. □

Theorem 4. *Let $m_n^d = \min\limits_{\gamma \in \mathbb{F}_2^n} \operatorname{adp}^{\oplus}(0, \gamma \to \gamma)$. Then for any n, we have*

$$m_{n+2}^d = \frac{1}{4} m_{n+1}^d + \frac{1}{4} m_n^d.$$

Moreover, $\operatorname{adp}^{\oplus}(0, \gamma \to \gamma) = m_n^d$, where $\gamma \in \mathbb{F}_2^n$, if and only if $\gamma_0 = 1$ (only if $n > 1$) and $\gamma_{i+1} = \overline{\gamma_i}$ for any $i = 1, \dots, n-3$. This means that γ_{n-1} and γ_1 can be arbitrary, and $\gamma_2, \dots, \gamma_{n-2}$ depend on γ_1.

Note 3. Note that we have no restrictions for $\gamma \in \mathbb{F}_2$. Also, if $n = 2, 3$, we have only one restriction: $\gamma_0 = 1$, i. e., the value of $\operatorname{adp}^{\oplus}(0, \gamma \to \gamma)$ is the same for any $\gamma \in \mathbb{F}_2^2, \mathbb{F}_2^3$ where $\gamma_0 = 1$.

Proof. Let us use induction by n. The statement of the theorem holds for $n = 1$ and $n = 2$ by Lemmas 2 and 3.

Let us suppose that the theorem holds for n. Now we will prove that it is true for $n + 1$. Let $\gamma \in \mathbb{F}_2^{n+1}$. We consider first two bits γ_0 and γ_1 of γ: first of all, Corollary 5 provides that $\gamma_0 = 1$ for the minimum of $\operatorname{adp}^{\oplus}(0, \gamma \to \gamma)$. Next, let

$$c = \begin{cases} (\gamma_2, \dots, \gamma_n) & \text{if } \gamma_1 = 0, \\ (\overline{\gamma}_2, \dots, \overline{\gamma}_n) & \text{if } \gamma_1 = 1, \end{cases}$$

where $c \in \mathbb{F}_2^{n-1}$. Then

$$\{\gamma', \overline{\gamma'}\} = \{c0, \overline{c0}\} \text{ for } \gamma' = (\gamma_1, \gamma_2, \dots, \gamma_n). \tag{12}$$

Indeed, $\gamma' = c0$ if $\gamma_1 = 0$, otherwise $\gamma' = (1, \overline{\overline{\gamma_2}}, \dots, \overline{\overline{\gamma_n}}) = (\overline{0}, \overline{c_0}, \dots, \overline{c_{n-1}}) = \overline{c0}$.

Since $\gamma_0 = 1$, Corollary 2 give us

$$\begin{aligned} \operatorname{adp}^{\oplus}(0, \gamma \to \gamma) &= \frac{1}{4}\operatorname{adp}^{\oplus}(0, \gamma' \to \gamma') + \frac{1}{4}\operatorname{adp}^{\oplus}(0, \overline{\gamma'} \to \overline{\gamma'}) \\ &\overset{(12)}{=} \frac{1}{4}\operatorname{adp}^{\oplus}(0, c0 \to c0) + \frac{1}{4}\operatorname{adp}^{\oplus}(0, \overline{c0} \to \overline{c0}) \\ &\overset{\text{Theorem 3}}{=} \frac{1}{4}\operatorname{adp}^{\oplus}(0, c \to c) + \frac{1}{4}\operatorname{adp}^{\oplus}(0, \overline{c}1 \to \overline{c}1). \end{aligned}$$

Since $\operatorname{adp}^{\oplus}(0, c \to c) \geq m_{n-1}^d$ and $\operatorname{adp}^{\oplus}(0, \overline{c}1 \to \overline{c}1) \geq m_n^d$, we have

$$m_{n+1}^d \geq \frac{1}{4} m_n^d + \frac{1}{4} m_{n-1}^d.$$

Moreover, $\operatorname{adp}^{\oplus}(0, \gamma \to \gamma) = \frac{1}{4} m_n^d + \frac{1}{4} m_{n-1}^d$ if and only if $\operatorname{adp}^{\oplus}(0, \overline{c}1 \to \overline{c}1) = m_n^d$, which gives us by the induction hypothesis the restriction

$$\begin{aligned} &c_{i+1} = \overline{c_i} \text{ for any } i = 0, \dots, n-4, \text{ or, equivalently,} \\ &\gamma_{i+1} = \overline{\gamma_i} \text{ for any } i = 2, \dots, n-2, \end{aligned} \tag{13}$$

and $\operatorname{adp}^{\oplus}(0, c \to c) = m_{n-1}^d$, which has for $n - 1 > 1$ one additional restriction: $c_0 = 1$. Since $c_0 = \gamma_1 \oplus \gamma_2$ by the definition of c, we have $\gamma_2 = \overline{\gamma_1}$ and extend (13) to $i = 1$.

Note that for the case $n-1=1$ (which excludes $c_0=1$) the theorem gives no $\gamma_{i+1}=\overline{\gamma_i}$. Indeed, $n+1=3$ and i should satisfy $1 \le i \le (n+1)-3$, but $1 > (n+1)-3 = 0$.

These restrictions for γ with $\gamma_0 = 1$ always guarantee that such a γ exists and, therefore, it holds that

$$\frac{1}{4}m_n^d + \frac{1}{4}m_{n-1}^d = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) \ge m_{n+1}^d \ge \frac{1}{4}m_n^d + \frac{1}{4}m_{n-1}^d.$$

It implies that $\mathrm{adp}^{\oplus}(0,\gamma \to \gamma) = m_{n+1}^d = \frac{1}{4}m_n^d + \frac{1}{4}m_{n-1}^d$ and makes the induction step proven. □

The numbers m_n^d, $n = 1, 2, \ldots$, form a Horadam sequence $H(1, \frac{1}{2}, \frac{1}{4}, -\frac{1}{4})$ — a generalization of the Fibonacci numbers. A sequence $H_1, H_2, H_3, \ldots$ is a Horadam sequence $H(a, b, p, q)$ if $H_1 = a$, $H_2 = b$ and $H_{n+2} = pH_{n+1} - qH_n$. Horadam [Hor65a, Hor65b] provides information on Horadam sequences and properties of sequence members, which help to obtain the following result.

Corollary 6. *The following formula holds:*

$$m_n^d = \frac{1}{34 \cdot 8^n}\Big((17+7\sqrt{17})(1+\sqrt{17})^n + (17-7\sqrt{17})(1-\sqrt{17})^n\Big).$$

Proof. According to [Hor65a, p. 161],[1]

$$H_n = A\alpha^{n-1} + B\beta^{n-1},$$

where α and β are roots of the polynomial $x^2 - px + q = 0$, $\beta \le \alpha$ for real roots, and

$$A = \frac{b - a\beta}{\alpha - \beta},\ B = \frac{a\alpha - b}{\alpha - \beta}.$$

Since $p = \frac{1}{4}, q = -\frac{1}{4}$,

$$\alpha = \frac{1}{8}(1+\sqrt{17}),\ \beta = \frac{1}{8}(1-\sqrt{17}),\ \alpha - \beta = \frac{\sqrt{17}}{4}.$$

Taking $a = 1$, $b = \frac{1}{2}$, we have

$$A = \frac{17+3\sqrt{17}}{34},\ B = \frac{17-3\sqrt{17}}{34}.$$

Finally, it is not difficult to check that

$$A = \frac{(17+7\sqrt{17})(1+\sqrt{17})}{34 \cdot 8},\ B = \frac{(17-7\sqrt{17})(1-\sqrt{17})}{34 \cdot 8}.$$

□

8.3 Results about $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$

It is easy to see that Propositions 2 and 3 provide

Proposition 7. *Let* $a, u, v \in \mathbb{F}_2^n$. *Then* $\mathrm{adp}^{\oplus}(a, u \to u) = \mathrm{adp}^{\oplus}(a, v \to v)$ *if* $u + v = 0 \pmod{2^{n-1}}$.

[1] Note that we use $n-1$ instead of n as the sequence starts with $n = 1$.

Proof. Let $u, v \in \mathbb{F}_2^n$. Since $2^{n-1} | 2^n$, we can correctly consider modulo 2^{n-1} operations.

Without loss of generality, we can assume that both $u, v < 2^{n-1}$. Otherwise, we can consider $u' = u \oplus 2^{n-1}$ instead of u, here $u' < 2^{n-1}$ and $u' = u \pmod{2^{n-1}}$, since Proposition 2 guarantees that $\mathrm{adp}^{\oplus}(a, u \to u) = \mathrm{adp}^{\oplus}(a, u' \to u')$ (and the same for v).

Thus, $v = 2^{n-1} - u$. Finally, by Propositions 2 and 3 we have

$$\mathrm{adp}^{\oplus}(a, u \to u) = \mathrm{adp}^{\oplus}(a, -u \to -u) = \mathrm{adp}^{\oplus}(a, 2^{n-1} - u \to 2^{n-1} - u) = \mathrm{adp}^{\oplus}(a, v \to v).$$

□

Computational experiments performed for n up to 32 show that there exist at most $32 = 2^5$ distinct γ with the same value $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, which implies that

$$\#\{\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) : \gamma \in \mathbb{F}_2^n\} \geq 2^{n-5}, \text{ where } n \leq 32.$$

Taking into account Theorem 4 (and Corollary 6), it looks like that the simplest way to calculate $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ is to use the recurrence formula (Corollary 2) and the minimized matrix representation (Proposition 6).

It is not difficult to compute the sum of all $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$:

Proposition 8. *For all n, we have*

$$\sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = 2 \left(\frac{3}{2}\right)^{n-1}.$$

Proof. For $n = 1$, the equality holds: $\mathrm{adp}^{\oplus}(0, 0 \to 0) + \mathrm{adp}^{\oplus}(0, 1 \to 1) = 1 + 1 = 2$. For all $n > 1$, the sum can be expressed using the sum for smaller n:

$$\begin{aligned}\sum_{\gamma \in \mathbb{F}_2^{n+1}} \mathrm{adp}^{\oplus}(0^{n+1}, \gamma \to \gamma) &= \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0^{n+1}, \gamma 0 \to \gamma 0) + \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0^{n+1}, \gamma 1 \to \gamma 1) \\ &= \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0^n, \gamma \to \gamma) \\ &\qquad + \frac{1}{4} \sum_{\gamma \in \mathbb{F}_2^n} \big(\mathrm{adp}^{\oplus}(0^n, \gamma \to \gamma)) + \mathrm{adp}^{\oplus}(0^n, \overline{\gamma} \to \overline{\gamma})\big) \\ &= \frac{3}{2} \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0^n, \gamma \to \gamma).\end{aligned}$$

□

9 Conclusion and Future Work

In this work we investigated some properties of $\mathrm{adp}^{\oplus}$ that are interesting for the differential cryptanalysis of ARX ciphers. We provide the missing proof of the theorem about $\max_{\alpha,\beta} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ from [LWD04], and established that there are either two (for $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = 1$) or eight (for any other cases) distinct pairs α, β on which $\mathrm{adp}^{\oplus}$ attains this maximum value. We obtained recurrence formulas for an arbitrary $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ which help to find minimum nonzero value of $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$, find all $\gamma \in \mathbb{F}_2^n$ for which $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \min_{c \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0, c \to c)$, and calculate this minimum value. As with any paper that analyzes the components of a primitive (e. g., additions, rotations, and XORs, but also S-boxes or matrix multiplications), some caution is necessary when extending the results to the analysis of a full primitive. We mention the analysis of larger components and the application to a full primitive as suggestions for future work.

Acknowledgments

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research. The authors are very grateful to organizers of The First Workshop at the Mathematical Center in Akademgorodok.

References

[AMPH14] Jean-Philippe Aumasson, Willi Meier, Raphael C.-W. Phan, and Luca Henzen. *The Hash Function BLAKE*. Information Security and Cryptography. Springer, 2014.

[BBCdS+20a] Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, and Qingju Wang. Alzette: A 64-bit ARX-box - (feat. CRAX and TRAX). In *CRYPTO 2020*, volume 12172 of *LNCS*, pages 419–448. Springer, 2020.

[BBCdS+20b] Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, and Qingju Wang. Lightweight AEAD and hashing using the Sparkle permutation family. *IACR Trans. Symmetric Cryptol.*, 2020(S1):208–261, 2020.

[Ber92] Thomas A. Berson. Differential cryptanalysis mod 2ˆ32 with applications to MD5. In *EUROCRYPT 1992*, volume 658 of *LNCS*, pages 71–80. Springer, 1992.

[Ber05] D.J. Bernstein. Salsa20 specification. https://cr.yp.to/snuffle/spec.pdf, April 2005.

[Ber08] D.J. Bernstein. ChaCha, a variant of Salsa20. https://cr.yp.to/chacha/chacha-20080128.pdf, January 2008.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, January 1991.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. https://eprint.iacr.org/2013/404.

[BV14] Alex Biryukov and Vesselin Velichkov. Automatic search for differential trails in ARX ciphers. In *CT-RSA 2014*, volume 8366 of *LNCS*, pages 227–250. Springer, 2014.

[DPU+16] Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov. Design strategies for ARX with provable bounds: Sparx and LAX. In *ASIACRYPT 2016*, volume 10031 of *LNCS*, pages 484–513. Springer, 2016.

[FLS+09] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family, 2009. http://www.skein-hash.info.

[GJN19] Shay Gueron, Ashwin Jha, and Mridul Nandi. COMET: COunter Mode Encryption with authentication Tag. Submission to the NIST Lightweight Cryptography Project (Round 2), September 2019.

[HHK$^+$03] Seokhie Hong, Deukjo Hong, Youngdai Ko, Donghoon Chang, Wonil Lee, and Sangjin Lee. Differential cryptanalysis of TEA and XTEA. In *ICISC 2003*, volume 2971 of *LNCS*, pages 402–417. Springer, 2003.

[Hor65a] Alwyn Francis Horadam. Basic properties of a certain generalised sequence of numbers. *The Fibonacci Quarterly*, 3(3):161–176, 1965.

[Hor65b] Alwyn Francis Horadam. Generating functions for powers of a certain generalised sequence of numbers. *Duke Mathematical Journal*, 32(3):437 – 446, 1965.

[KRK$^+$17] Bonwook Koo, Dongyoung Roh, Hyeonjin Kim, Younghoon Jung, Donggeon Lee, and Daesung Kwon. CHAM: A family of lightweight block ciphers for resource-constrained devices. In *ICISC 2017*, volume 10779 of *LNCS*, pages 3–25. Springer, 2017.

[LM01] Helger Lipmaa and Shiho Moriai. Efficient algorithms for computing differential properties of addition. In Mitsuru Matsui, editor, *FSE 2001*, volume 2355 of *LNCS*, pages 336–350. Springer, 2001.

[LWD04] Helger Lipmaa, Johan Wallén, and Philippe Dumas. On the additive differential probability of exclusive-or. In Bimal K. Roy and Willi Meier, editors, *FSE 2004*, volume 3017 of *LNCS*, pages 317–331. Springer, 2004.

[MVDCP11] Nicky Mouha, Vesselin Velichkov, Christophe De Cannière, and Bart Preneel. The differential analysis of S-functions. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *SAC 2010*, volume 6544 of *LNCS*, pages 36–56. Springer, 2011.

[MWGP11] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *Inscrypt 2011*, volume 7537 of *LNCS*, pages 57–76. Springer, 2011.

[NW97] Roger M. Needham and David J. Wheeler. Tea extensions. Technical report, Computer Laboratory, University of Cambridge, October 1997. http://www.cix.co.uk/~klockstone/xtea.pdf.

[PHCER08] Javier Polimón, Julio César Hernández Castro, Juan M. Estévez-Tapiador, and Arturo Ribagorda. Automated design of a lightweight block cipher with genetic programming. *Int. J. Knowl. Based Intell. Eng. Syst.*, 12(1):3–14, 2008.

[RKJ$^+$19] Dongyoung Roh, Bonwook Koo, Younghoon Jung, Ilwoong Jeong, Donggeon Lee, Daesung Kwon, and Woo-Hwan Kim. Revised version of block cipher CHAM. In *ICISC 2019*, volume 11975 of *LNCS*, pages 1–19. Springer, 2019.

[Saa19] Markku-Juhani O. Saarinen. SNEIKEN and SNEIKHA v1.1: Authenticated encryption and cryptographic hashing. Technical report, PQShield Ltd., May 2019. https://github.com/pqshield/sneik.

[SHW$^+$16] Siwei Sun, Lei Hu, Peng Wang, Meiqin Wang, Danping Shi, Xiaoshuang Ma, Qianqian Yang, and Kai Fu. Mixed integer programming models for finite automaton and its application to additive differential patterns of exclusive-or. Cryptology ePrint Archive, Report 2016/338, 2016. https://eprint.iacr.org/2016/338.

[SM88] Akihiro Shimizu and Shoji Miyaguchi. Fast data encipherment algorithm FEAL. In David Chaum and Wyn L. Price, editors, *EUROCRYPT 1987*, volume 304 of *LNCS*, pages 267–278. Springer, 1988.

[VMDCP11] Vesselin Velichkov, Nicky Mouha, Christophe De Cannière, and Bart Preneel. The additive differential probability of ARX. In *FSE 2011*, volume 6733 of *LNCS*, pages 342–358. Springer, 2011.

[VMDCP12] Vesselin Velichkov, Nicky Mouha, Christophe De Cannière, and Bart Preneel. UNAF: A special set of additive differences with application to the differential analysis of ARX. In *FSE 2012*, volume 7549 of *LNCS*, pages 287–305. Springer, 2012.

[WN94] David J. Wheeler and Roger M. Needham. TEA, a tiny encryption algorithm. In *FSE 1994*, volume 1008 of *LNCS*, pages 363–366. Springer, 1994.