jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2025, VOL. 71, NO. 1, PP. 95–100
Manuscript received December 2, 2024; revised March, 2025. doi: 10.24425/ijet.2025.153550

Differential properties of LRX-analogues of small constant multiplication

Serhii Yakovliev

***Abstract*—In this work, we consider a class of mappings over bit vectors which imitate the multiplication by small constants with pure logic operations and non-cyclic shifts. Such mappings can provide non-linearity and strengthen the design of LRX-cryptosystems, which are widely used in lightweight cryptography, due to their apparent benefits: a simple implementation and the absence of internal rotational symmetry, which increases security against rotational attacks. We examine the security of these mappings against differential cryptanalysis. We provide an explicit easy-to-calculate expression of differential probabilities for several versions of LRX-analogues of small constant multiplication with different operations and shift values.**

***Keywords*—symmetric cryptography, ARX-cryptosystems, LRX-cryptosystems, differential cryptanalysis**

I. Introduction

An ARX-cryptosystem (from “Add-Rotation-XOR”) is a system which uses only elementary operations within its structure: additions modulo 2^n, bitwise additions (XOR), and rotations. Other elementary operations that can be easily implemented, e.g. non-cyclic shifts and logical operations, are also often used in ARX-cryptosystems. This approach allows the construction of highly efficient lightweight algorithms suitable for use in low-resource devices.

In certain instances, modular addition is substituted with some purely logic nonlinear mappings to achieve even greater efficiency. Such systems are often called LRX-cryptosystems, where “L” means “Logic”. In instances where the sole nonlinear operation is logical AND, the name “AND-RX” is used. Among the most reputed LRX-cryptosystems are the ciphers Simon [1], NORX [2] and Ascon [3].

The traditional approach to constructing nonlinear layers in ARX-cryptosystems involves the combination of nonlinear operations with rotations. However, when a nonlinear operation is bitwise, such constructions exhibit internal rotational symmetry. This may result some vulnerabilities and reduce the security of cryptosystems against rotational attacks — a specific form of cryptanalysis, applicable to ARX-cryptosystems [4], [5].

The use of multiplications by small constants represents an alternative approach for elementary nonlinear mappings in ARX-cryptosystems. We can select the hash function SHABAL as the most notable construction [6]. Such multiplication can be considered as a combination of nonlinear operation (modular addition) with non-cyclic shifts. This, among other effects, breaks the rotational symmetry. However, in the case of LRX-cryptosystems, where modular addition is not used, we cannot define multiplication by constant as well.

In this paper, we examine a family of LRX-mappings which imitate multiplications by small constants in different ways. We derive analytical expressions for the differential probabilities of these mappings, which are explicit and easy to calculate. We demonstrate that such mappings are comparable in terms of their cryptographic properties with better-known constructions, such as Simon’s internal function or Daemen’s S-box. Consequently, they can be considered as an alternative choice for the design of a secure LRX-cryptosystem.

The rest of the paper is organized as follows. Section II provides the necessary terms, notation, and definitions. Section III describes several approaches to constructing nonlinear ARX- and LRX-mappings and introduces the notion of the LRX-analogue of small constant multiplication. In Section IV we derive analytic expressions of differential probabilities for the LRX-analogue based on the AND operation, prove their correctness, and compare the obtained results with known results of Simon’s internal function. Section V expands the results of the previous section to other LRX-analogues with different logical operations, and section VI — to LRX-analogues with another form of non-cyclic shifts.

II. Terms and Notation

In this paper, we use the following notation.

Let $V_n = \{0,1\}^n$ be the set of all binary vectors of length n. An arbitrary n-bit binary vector $x \in V_n$ is considered as follows:

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

where $x_i \in \{0,1\}$. Every binary vector is also treated as a number modulo 2^n in natural representation:

$$x = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \dots + x_1 2 + x_0.$$

The symbol 0 is used to denote the zero vector (equivalent to the number 0), and the symbol 1^n — a vector $(1,1,\dots,1)$ (equivalent to the number -1 modulo 2^n).

The symbol $\star$ is used to denote any bitwise operation on V_n, so

$$x \star y = (x_{n-1} \star y_{n-1}, \dots, x_1 \star y_1, x_0 \star y_0).$$

S. Yakovliev is with Institute of Physics and Technology, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine (e-mail: yasv@rl.kiev.ua).

As such operations we consider

- $x \oplus y$ — bitwise addition (XOR),
- $x \sim y$ — logical equivalence,
- $x \,\&\, y$ — logical AND,
- $x \vee y$ — logical OR,
- $x \downarrow y$ — Peirce arrow (NOR),
- $x \uparrow y$ — Sheffer stroke (NAND),
- $x \Rightarrow y$, $x \Leftarrow y$ — an implication and converse implication correspondingly.[1]

The inversion of all bits in the vector x (logical NOT) is denoted as $\overline{x}$ or as $\neg x$.

Note that all known identities involving bit operations are also valid for bit vectors: $\overline{x} = x \oplus 1^n$, $x \vee y = x \oplus y \oplus xy$, $(x \sim y) = (x \oplus y \oplus 1^n)$, $(x \Rightarrow y) = \overline{x} \vee y$ etc.

The symbols $x \ll s$ and $x \lll s$ indicate non-cyclic shifts and cyclic shifts (rotations) of vector x by s bit to the left, whereas $x \gg s$ and $x \ggg s$ indicate shifts to the right:

$$\begin{aligned} x \ll s &= (x_{n-s-1}, x_{n-s-2}, \ldots, x_1, x_0, 0, \ldots, 0), \\ x \lll s &= (x_{n-s-1}, \ldots, x_0, x_{n-1}, \ldots, x_{n-s}), \\ x \gg s &= (0, \ldots, 0, x_{n-1}, x_{n-2}, \ldots, x_{s+1}, x_s), \\ x \ggg s &= (x_{s-1}, \ldots, x_0, x_{n-1}, \ldots, x_s). \end{aligned}$$

$wt(x)$ denotes the Hamming weight of a given vector x (i.e. the number of non-zero bits).

Consider an arbitrary mapping $f \colon V_n \to V_n$.

A *differential* $(\alpha \to \beta)$ is defined as an arbitrary pair of vectors $\alpha, \beta \in V_n$, which are considered as differences between the inputs (correspondingly, outputs) of mapping f. The *probability of a differential* $(\alpha \to \beta)$ for a given mapping f is defined as [7]

$$xdp^f(\alpha \to \beta) = \Pr_x \{ f(x \oplus \alpha) = f(x) \oplus \beta \}.$$

The probabilities of differentials determine the security against differential cryptanalysis.

III. LRX S-boxes and Small Constant Multiplication

Traditional approaches of introducing nonlinearity into the encryption process rely on the use of precomputed S-boxes, which can be randomly generated or implement a hard Boolean and/or algebraic function. However, the fundamental simplicity of ARX designs makes such approaches unsuitable. Low-resource devices may lack sufficient memory to store the S-box or enough computational resources to calculate its values. In classic ARX-systems, all nonlinearity is provided by modular additions; in LRX-systems, one has to use nonlinear Boolean operations (like AND) instead.

One of the most popular LRX nonlinear mappings is the so-called Daemen's S-box, which is used in the SHA-3 hash function [8] and (with certain modifications) in the Ascon cipher [3]:

$$S(x) = x \,\&\, (\overline{x} \lll 1) \oplus (x \ggg 1).$$

Originally based on cellular automata theory, this S-box can also be represented with the implication operation as follows:

$$S(x) = \neg(x \Rightarrow (x \lll 1)) \oplus (x \ggg 1). \tag{1}$$

Another example of the nonlinear LRX-mapping is an internal function of the block cipher Simon [1]:

$$F(x) = (x \lll 1) \,\&\, (x \lll 8) \oplus (x \lll 2).$$

These functions have been well studied and are widely used, but they possess rotational symmetry. A function $f \colon V_n \to V_n$ is said to be *rotational invariant*, if, for every r, $0 < r < n$,

$$f(x \lll r) = (f(x)) \lll r.$$

Any bitwise operation is rotational invariant. Furthermore, both Daemen's S-box and Simon's internal function are rotational invariant.

Rotation symmetry makes cryptosystem vulnerable to so-called rotational cryptanalysis — specific form of analysis of ARX-cryptosystems, first introduced by D. Khovratovich and I. Nicolić [4], [5]. Additionally, rotational invariant functions may exhibit other unfavorable properties. For example, it can be demonstrated that for a rotational invariant function f and every differential $(\alpha \to \beta)$ holds

$$xdp^f(\alpha \to \beta) = xdp^f((\alpha \lll r) \to (\beta \lll r));$$

therefore, differentials with non-zero probabilities are clustered by rotations (see, e.g., [9] for Simon-like functions).

The block cipher FEAL [10] and the TEA cipher family [11]–[13] implement non-cyclic shifts in their structure, which are equivalent to multiplication by a power of 2:

$$\begin{aligned} f(x) &= 2x \bmod 2^n = (x \ll 1) \bmod 2^n, \\ f(x) &= 2^s x \bmod 2^n = (x \ll s) \bmod 2^n. \end{aligned}$$

These functions are linear w.r.t. $\oplus$, but disrupt the internal rotational symmetry, which increases security against rotational attacks.

One of the SHA-3 candidates, the hash function SHABAL [6], uses multiplication by 3 and 5:

$$\begin{aligned} f_3(x) &= 3x \bmod 2^n = (x + (x \ll 1)) \bmod 2^n, \\ f_5(x) &= 5x \bmod 2^n = (x + (x \ll 2)) \bmod 2^n. \end{aligned}$$

These are simple transformations, linear w.r.t. $+$, but nonlinear w.r.t. $\oplus$, beginning with the second bit of the result. Additionally, they don't have rotational symmetry [14].

In this work, we consider *LRX-analogues of small constant multiplications*, which are defined as mappings of the form

$$f_\star(x) = x \star (x \ll s),$$

where $\star$ is an arbitrary nonlinear bitwise operation, such as logical AND. These mappings imitate the "multiplication" by a small constant of the form $2^s + 1$ (3, 5 etc.), since

$$(2^s + 1)x \equiv x + 2^s x \equiv x + (x \ll s) \pmod{2^n};$$

the modular addition is simply replaced by a bitwise logical operation. Moreover, the introduced functions also disrupt rotational symmetry.

We will restrict our consideration to the case $s \le \frac{n}{2}$. While the case $s > \frac{n}{2}$ is interesting from a mathematical point of view, it seems to be of little practical use.

[1] The traditional notation for bit implication is $x \to y$. However, we use the symbol "$\Rightarrow$" to avoid possible confusion with notation of differentials.

IV. Differential Probabilities for Logical AND "Multiplication" by a Small Constant

At first, we will consider the probability of differentials for the mapping $f_{\&}$. This mapping acts like the basic mapping for other $f_{\star}$, as it will be demonstrated in the section V.

The main result of this section is presented in the following theorem.

Theorem 1. *The probability of differential $(\alpha \to \beta)$ for the mapping $f_{\&}(x) = x \,\&\, (x \lll s)$ is described by the following relations:*

1) $xdp^{f_{\&}}(\alpha \to \beta) \neq 0$ iff

$$\begin{aligned}&(\beta \,\&\, (2^s - 1)) \vee\\ &\vee (\overline{\alpha} \,\&\, (\overline{\alpha} \lll s) \,\&\, \beta) \vee \\ &\vee (\alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\alpha \lll 2s) \,\&\, (\beta \oplus (\beta \lll s))) = 0,\end{aligned} \tag{2}$$

where $2^s - 1$ represents a vector with first $n - s$ zeroes and last s ones;

2) if $xdp^{f_{\&}}(\alpha \to \beta) \neq 0$, then $xdp^{f_{\&}}(\alpha \to \beta) = 2^{-w}$, where

$$w = wt((\alpha \lll s) \oplus (\alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\overline{\alpha} \lll 2s))). \tag{3}$$

Proof. Consider the equation $f_{\&}(x \oplus \alpha) = f_{\&}(x) \oplus \beta$, or

$$(x \oplus \alpha) \,\&\, ((x \oplus \alpha) \lll s) = (x \,\&\, (x \lll s)) \oplus \beta,$$

for each bit of vectors. After simple transformations we get

$$0 \le k \le s-1\colon 0 = \beta_k; \tag{4}$$

$$k \ge s\colon \alpha_k x_{k-s} \oplus \alpha_{k-s} x_k = \beta_k \oplus \alpha_k \alpha_{k-s}. \tag{5}$$

Denote the events (4) and (5), induced by random x, as A_k, and their probabilities as p_k. For $k < s$ we have $p_k = 1$ if $\beta_k = 0$, and vice versa. For $k \ge s$, the events A_k are not pairwise independent in general; thus, formally, $p_k = \Pr\{A_k \,|\, A_{k-1}, \ldots, A_s\}$ in this case. With this clarification, we can state that

$$xdp^{f_{\&}}(\alpha \to \beta) = \prod_{k=0}^{n-1} p_k.$$

We have the following cases for A_k.

1) $\alpha_{k-s} = 1$: A_k transforms to

$$x_k = \alpha_k x_{k-s} \oplus \beta_k \oplus \alpha_k \alpha_{k-s}.$$

Regardless of the value of the right side, x_k will be equal to this value with probability $p_k = \frac{1}{2}$.

2) $\alpha_{k-s} = 0$, $\alpha_k = 0$: A_k becomes $0 = \beta_k$, so $p_k = 1$ if $\beta_k = 0$ and $p_k = 0$ if $\beta_k = 1$.

3) $\alpha_{k-s} = 0$, $\alpha_k = 1$: A_k becomes $x_{k-s} = \beta_k$. As we can see, A_k does not depend on x_k, but depends on x_{k-s}. Consider the event A_{k-s}; in this case, A_{k-s} transforms to $\alpha_{k-2s} x_{k-s} = \beta_{k-s}$.

- If $\alpha_{k-2s} = 0$, then A_{k-s} doesn't depend on x_{k-s}, therefore, A_k and A_{k-s} are independent and $p_k = \frac{1}{2}$.
- If $\alpha_{k-2s} = 1$, then we have $x_{k-s} = \beta_k$ and $x_{k-s} = \beta_{k-s}$ simultaneously:
  - if $\beta_k = \beta_{k-s}$, then A_k is equal to A_{k-s}, so $p_k = 1$;
  - if $\beta_k \neq \beta_{k-s}$, then A_k is opposite to A_{k-s}, so $p_k = 0$.

In summary, there are three possible cases in which $xdp^{f_{\&}}(\alpha \to \beta) = 0$:

(a) $\exists k \le s-1\colon \beta_k = 1$;

(b) $\exists k \ge s\colon \alpha_k = 0, \alpha_{k-s} = 0, \beta_k = 1$;

(c) $\exists k \ge s\colon \alpha_k = 1, \alpha_{k-s} = 0, \alpha_{k-2s} = 1, \beta_k \neq \beta_{k-s}$.

The given conditions are equivalent to

(a) $\beta \,\&\, (2^s - 1) \neq 0$;

(b) $\overline{\alpha} \,\&\, (\overline{\alpha} \lll s) \,\&\, \beta \neq 0$;

(c) $\alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\alpha \lll 2s) \,\&\, (\beta \oplus (\beta \lll s)) \neq 0$.

This implies the first statement of the theorem.

If $xdp^{f_{\&}}(\alpha \to \beta) \neq 0$ then all p_k are equal to 1 or $\frac{1}{2}$ only, and $p_k = \frac{1}{2}$ when $k \ge s$ and one of two conditions is met:

(d) $\alpha_{k-s} = 1$;

(e) $\alpha_k = 1,\ \alpha_{k-s} = 0,\ \alpha_{k-2s} = 0$.

These conditions are mutually exclusive, given that α_{k-s} assumes opposing values. The number of cases (d) is equal to a weight of $(\alpha \lll s)$, and the number of cases (e) is equal to the weight of $\alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\overline{\alpha} \lll 2s)$. This implies the second statement of the theorem and concludes the proof. □

Corollary 1. For each fixed $\alpha \in V_n$ the probability of the differential $(\alpha \to \beta)$ for any $\beta \in V_n$ can be either 0 or 2^{-w}, where w is defined in (3). Therefore, for each fixed α there are precisely 2^w possible β's with non-zero (and equal) differential probability.

Corollary 2. For each fixed $\alpha \in V_n$ all possible β with non-zero probability of differential $(\alpha \to \beta)$ can be constructed with an algorithm below:

1) For every $i = 0, 1, \ldots, s-1$: $\quad \beta_i := 0$.
2) For every $i = s, s+1, \ldots, n-1$:
   - if $\alpha_i = 0$ and $\alpha_{i-s} = 0$ then $\beta_i := 0$
   - else if $\alpha_i = 1$, $\alpha_{i-s} = 0$ and $\alpha_{i-2s} = 1$ then $\beta_i := \beta_{i-s}$
   - else $\beta_i \in \{0, 1\}$.

Both Corollaries 1 and 2 directly follow from Theorem 1.

Note that in [15] Kölbl et al. considered mappings of the form $r_{\&}(x) = x \,\&\, (x \lll s)$ (as well as more generalized forms). They derived an analytic expression for the differential probabilities of such mappings, thereby clarifying the results of Biryukov et al. [16]. Their main result is presented in adapted notation in the following theorem.

Theorem 2 ([15]). *For the function $r_{\&}(x) = x \,\&\, (x \lll s)$, where $\gcd(n, s) = 1$, and arbitrary $\alpha, \beta \in V_n$ the probability of the differential $(\alpha \to \beta)$ can be expressed as follows:*

1) if $\alpha = 1^n$ and $wt(\beta)$ is even, then

$$xdp^{r_{\&}}(\alpha \to \beta) = 2^{1-n};$$

2) if $\alpha \neq 1^n$, $\beta \,\&\, \overline{\mu} = 0$ and $(\beta \oplus (\beta \lll s)) \,\&\, \delta = 0$, where $\mu = \alpha \vee (\alpha \lll s)$ and $\delta = \alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\alpha \lll 2s)$, then

$$xdp^{r_{\&}}(\alpha \to \beta) = 2^{-w}, \text{ where } w = wt(\mu \oplus \delta).$$

3) in all other cases $xdp^{r_\&}(\alpha \to \beta) = 0$.

Vectors μ and δ are addressed in [15] as `varibits` and `doublebits`, respectively. In the case $\gcd(n, s) > 1$, authors of [15] noted that it only makes expressions more complex and cumbersome due to the partitioning of bits into separate classes, and raises differential probabilities in general.

We can observe that

$$\beta \,\&\, \overline{\mu} = \beta \,\&\, \overline{(\alpha \vee (\alpha \lll s))} = \\ = \beta \,\&\, \overline{\alpha} \,\&\, \overline{(\alpha \lll s)} = \beta \,\&\, \overline{\alpha} \,\&\, (\overline{\alpha} \lll s).$$

Further, we can write

$$\mu \oplus \delta = (\alpha \vee (\alpha \lll s)) \oplus \alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\alpha \lll 2s) = \\ = (\alpha \lll s) \oplus \alpha \,\&\, (\overline{\alpha} \lll s) \oplus \alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\alpha \lll 2s) = \\ = (\alpha \lll s) \oplus \alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, ((\alpha \lll 2s) \oplus 1^n) = \\ = (\alpha \lll s) \oplus \alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\overline{\alpha} \lll 2s).$$

Therefore, case 2) of Theorem 2 can be expressed as follow: for $\alpha \neq 1^n$ the probability $xdp^{r_\&}(\alpha \to \beta) \neq 0$ iff

$$(\overline{\alpha} \,\&\, (\overline{\alpha} \lll s) \,\&\, \beta) \vee \\ \vee (\alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\alpha \lll 2s) \,\&\, (\beta \oplus (\beta \lll s))) = 0, \tag{6}$$

and if $xdp^{r_\&}(\alpha \to \beta) \neq 0$, then $xdp^{r_\&}(\alpha \to \beta) = 2^{-w}$, where

$$w = wt((\alpha \lll s) \oplus (\alpha \,\&\, (\overline{\alpha} \lll s) \,\&\, (\overline{\alpha} \lll 2s))). \tag{7}$$

Formulas (6) and (7) are evidently analogous with (2) and (3), which emphases the resemblance of statements of Theorem 1 and Theorem 2. But the dissimilarities are also important.

- Theorem 1 is valid for any appropriate value of s, not only for mutually prime values with n. There are no separate classes of bits and possible probability rising for specific values of s.
- The function $r_\&(x)$ always possesses a special class of differentials with $\alpha = 1^n$ and arbitrary β of even weight. The probability of these differentials is equal to $\frac{2}{2^n}$ and is therefore fixed (thus very small). The function $f_\&(x)$ does not possess any special classes of differentials.
- Since w in (7) calculated over all bits of α and in (3) — only over first $n - s$ bits, the differential probabilities of $f_\&$ are expected to be slightly higher than the probabilities of $r_\&$. However, exact comparison requires a more rigorous analysis.

The aforementioned differences can be explained as consequences of the disruption of rotational symmetry in $f_\&(x)$.

At last, we should note that the results of Theorems 1 and 2 were obtained through disparate methodologies: Kölbl et al. used linear algebra techniques, while our analysis is based on discrete probabilities over Boolean equations.

V. Differential Probabilities for Other Logical "Multiplication" Analogues

For every other nonlinear bitwise logical operation $\star$ it is possible to express the differential probabilities of $f_\star$ through $xdp^{f_\&}$ (in this sense $f_\&$ acts like a "basic" mapping). These results are summarized in the following theorem.

Theorem 3. *For every differential* $(\alpha \to \beta)$ *the next equities are hold:*

$$xdp^{f_\vee}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta \oplus \alpha \oplus (\alpha \ll s)); \\ xdp^{f_\uparrow}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta); \\ xdp^{f_\downarrow}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta \oplus \alpha \oplus (\alpha \ll s)); \\ xdp^{f_\Rightarrow}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta \oplus \alpha); \\ xdp^{f_\Leftarrow}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta \oplus (\alpha \ll s)).$$

The proof of Theorem 3 requires some auxiliary statements, which are given in the following lemmas.

Lemma 1. *Let* $f \colon V_n \to V_n$ *be an arbitrary mapping and* $\Delta_x, \Delta_y \in V_n$ *be arbitrary vectors. Define the function*

$$h(x) = f(x \oplus \Delta_x) \oplus \Delta_y.$$

Then the probabilities of each differential $(\alpha \to \beta)$ *for* $f(x)$ *and* $h(x)$ *are equal:*

$$xdp^h(\alpha \to \beta) = xdp^f(\alpha \to \beta).$$

Proof. From the definition we have

$$xdp^h(\alpha \to \beta) = \Pr_x\{h(x \oplus \alpha) = h(x) \oplus \beta\} = \\ = \Pr_x\{f(x \oplus \alpha \oplus \Delta_x) \oplus \Delta_y = f(x \oplus \Delta_x) \oplus \Delta_y \oplus \beta\} = \\ = \Pr_x\{f(x \oplus \alpha \oplus \Delta_x) = f(x \oplus \Delta_x) \oplus \beta\};$$

define substitution $u := x \oplus \Delta_x$, then

$$xdp^h(\alpha \to \beta) = \Pr_u\{f(u \oplus \alpha) = f(u) \oplus \beta\} = \\ = xdp^f(\alpha \to \beta),$$

which concludes the proof. □

Corollary 3. If $h(x)$ has one of the following form:

1) $h(x) = f(\overline{x})$,
2) $h(x) = \neg f(x)$,
3) $h(x) = \neg f(\overline{x})$ — dual function of f,

then for each differential $(\alpha \to \beta)$

$$xdp^h(\alpha \to \beta) = xdp^f(\alpha \to \beta).$$

Proof. Since $\overline{a} = a \oplus 1^n$ for every $a \in V_n$, this corollary follows directly from Lemma 1 by setting values:

1) $\Delta_x = 1^n$, $\Delta_y = 0$;
2) $\Delta_x = 0$, $\Delta_y = 1^n$;
3) $\Delta_x = 1^n$, $\Delta_y = 1^n$.

Thus, negating the input and/or output of the function will not affect the differential probabilities. □

Lemma 2. *Let* $f \colon V_n \to V_n$ *be an arbitrary mapping and* $\ell \colon V_n \to V_n$ *be a linear mapping (not necessarily bijective). Then the following equality holds for the function* $g(x) = f(x) \oplus \ell(x)$ *and any differential* $(\alpha \to \beta)$*:*

$$xdp^g(\alpha \to \beta) = xdp^f(\alpha \to \beta \oplus \ell(\alpha)).$$

Proof. Again, from the definition we have

$$\begin{aligned} &xdp^g(\alpha \to \beta) = \\ &= \Pr_x\{g(x \oplus \alpha) = g(x) \oplus \beta\} = \\ &= \Pr_x\{f(x \oplus \alpha) \oplus \ell(x \oplus \alpha) = f(x) \oplus \ell(x) \oplus \beta\} = \\ &= \Pr_x\{f(x \oplus \alpha) \oplus \ell(x) \oplus \ell(\alpha) = f(x) \oplus \ell(x) \oplus \beta\} = \\ &= \Pr_x\{f(x \oplus \alpha) = f(x) \oplus \beta \oplus \ell(\alpha)\} = \\ &= xdp^f(\alpha \to \beta \oplus \ell(\alpha)), \end{aligned}$$

which concludes the proof. □

Now we can proceed with the proof of Theorem 3.

Proof. We will proceed each operation individually.

1) $f_\vee(x)$: since $a \vee b = a \oplus b \oplus (a \,\&\, b)$, we have

$$f_\vee(x) = x \vee (x \ll s) = x \oplus (x \ll s) \oplus f_\&(x).$$

The function $\ell_1(x) = x \oplus (x \ll s)$ is linear, so from Lemma 2 it follows that

$$xdp^{f_\vee}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta \oplus \ell_1(\alpha)).$$

2) $f_\uparrow(x)$: since $a \uparrow b = \neg(a \,\&\, b)$, we have $f_\uparrow(x) = \neg f_\&(x)$ and the statement follows from Corollary 3.

3) $f_\downarrow(x)$: since $a \downarrow b = \neg(a \vee b)$, we have $f_\downarrow(x) = \neg f_\vee(x)$ and the statement follows from Corollary 3 and the first point of this proof.

4) $f_\Rightarrow(x)$: since $(a \Rightarrow b) = \overline{a} \vee b = \overline{a} \oplus b \oplus (\overline{a} \,\&\, b)$, and $\overline{a} = a \oplus 1^n$, we can write

$$\begin{aligned} f_\Rightarrow(x) &= (x \Rightarrow (x \ll s)) = \\ &= (x \oplus 1^n) \oplus (x \ll s) \oplus (x \oplus 1^n) \,\&\, (x \ll s) = \\ &= 1^n \oplus x \oplus (x \ll s) \oplus x \& (x \ll s) \oplus 1^n \& (x \ll s), \end{aligned}$$

and, hence $a \,\&\, 1^n = a$ for each $a \in V_n$,

$$f_\Rightarrow(x) = 1^n \oplus x \oplus x \,\&\, (x \ll s) = \neg f_\&(x) \oplus x.$$

Since $\ell_2(x) = x$ is obviously linear, from Lemma 2 and Corollary 3 follows

$$xdp^{f_\Rightarrow}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta \oplus \ell_2(\alpha)).$$

5) $f_\Leftarrow(x)$: similarly to previous point, we have $(a \Leftarrow b) = a \vee \overline{b} = a \oplus \overline{b} \oplus (a \,\&\, \overline{b})$, and

$$\begin{aligned} f_\Leftarrow(x) &= (x \Leftarrow (x \ll s)) = \\ &= x \oplus ((x \ll s) \oplus 1^n) \oplus x \,\&\, ((x \ll s) \oplus 1^n) = \\ &= 1^n \oplus x \oplus (x \ll s) \oplus x \,\&\, (x \ll s) \oplus 1^n \,\&\, x, \end{aligned}$$

and, finally,

$$\begin{aligned} f_\Leftarrow(x) &= 1^n \oplus (x \ll s) \oplus x \,\&\, (x \ll s) = \\ &= \neg f_\&(x) \oplus (x \ll s). \end{aligned}$$

Since $\ell_3(x) = (x \ll s)$ is also linear, from Lemma 2 and Corollary 3 follows

$$xdp^{f_\Leftarrow}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta \oplus \ell_3(\alpha)).$$

This concludes the proof of theorem. □

Interestingly, the function $f_\Rightarrow(x)$ allows another representation, namely $f_\Rightarrow(x) = f_\&(x) \oplus \overline{x}$, which implies

$$xdp^{f_\Rightarrow}(\alpha \to \beta) = xdp^{f_\&}(\alpha \to \beta \oplus \overline{\alpha}) = xdp^{f_\&}(\alpha \to \overline{\beta} \oplus \alpha),$$

and, therefore,

$$xdp^{f_\Rightarrow}(\alpha \to \beta) = xdp^{f_\Rightarrow}(\alpha \to \overline{\beta}).$$

Finally, as a side effect, the same approach can be used to express the differential probabilities of functions $r_\star(x) = x \star (x \lll s)$ through the differential probabilities of $r_\&(x)$, which are given by Theorem 2.

Theorem 4. *For each differential $(\alpha \to \beta)$, the following equations are satisfied:*

$$\begin{aligned} xdp^{r_\vee}(\alpha \to \beta) &= xdp^{r_\&}(\alpha \to \beta \oplus \alpha \oplus (\alpha \lll s)); \\ xdp^{r_\uparrow}(\alpha \to \beta) &= xdp^{r_\&}(\alpha \to \beta); \\ xdp^{r_\downarrow}(\alpha \to \beta) &= xdp^{r_\&}(\alpha \to \beta \oplus \alpha \oplus (\alpha \lll s)); \\ xdp^{r_\Rightarrow}(\alpha \to \beta) &= xdp^{r_\&}(\alpha \to \beta \oplus \alpha); \\ xdp^{r_\Leftarrow}(\alpha \to \beta) &= xdp^{r_\&}(\alpha \to \beta \oplus (\alpha \lll s)). \end{aligned}$$

The proof is similar to the proof of Theorem 3.

To illustrate the application of Theorem 4, consider Daemen's S-box (1):

$$S(x) = \neg r_\Rightarrow(x) \oplus (x \ggg 1),$$

with $s = 1$. From Lemma 2, Corollary 3 and Theorem 4 we obtain the formula for the probability of arbitrary differential $(\alpha \to \beta)$:

$$xdp^S(\alpha \to \beta) = xdp^{r_\&}(\alpha \to \beta \oplus \alpha \oplus (\alpha \ggg 1)),$$

where $xdp^{r_\&}$ is calculated as in Theorem 2.

VI. Differential Probabilities of Small Constant "Division" Analogues

In the context of this research, it is also natural to consider mappings of the form $g_\star(x) = x \star (x \gg s)$. These mappings can be seen as imitations of "division" by a small constant (or, more precisely, "multiplication" by a rational number), since

$$\left(1 + \frac{1}{2^s}\right) x \equiv x + \frac{x}{2^s} \equiv x + (x \gg s) \pmod{2^n};$$

but first of all, $g_\star$ is simply an alternative version of $f_\star$ with expectedly similar properties.

Let $\rho(x)$ be the reverse of the bits of x:

$$\begin{aligned} x &= (x_{n-1}, \ldots, x_1, x_0), \\ \rho(x) &= (x_0, x_1, \ldots, x_{n-1}). \end{aligned}$$

The most important properties of $\rho(x)$ are listed below:

- $\rho(x)$ is linear w.r.t. XOR: $\rho(x \oplus y) = \rho(x) \oplus \rho(y)$;
- more generally, $\rho(x)$ is automorphic w.r.t. any bitwise operation $\star$: $\rho(x \star y) = \rho(x) \star \rho(y)$;
- $\rho(x)$ is involutive: $\rho(\rho(x)) = x$, or $\rho^{-1} \equiv \rho$.

Lemma 3. *For every bitwise operation $\star$, the mapping $g_\star(x)$ can be expressed as*

$$g_\star(x) = \rho(f_\star(\rho(x))).$$

Proof. From the definition it follows that

$$\rho(x \gg s) = \rho(x) \ll s.$$

Therefore,

$$\rho(g_\star(x)) = \rho(x \star (x \gg s)) = \rho(x) \star \rho(x \gg s) = \\ = \rho(x) \star (\rho(x) \ll s) = f_\star(\rho(x)),$$

and, finally,

$$g_\star(x) = \rho(\rho(g_\star(x))) = \rho(f_\star(\rho(x))),$$

which concludes the proof. □

Theorem 5. *For each $\alpha, \beta \in V_n$, the probability of the differential $(\alpha \to \beta)$ of $g_\star$ is equal to*

$$xdp^{g_\star}(\alpha \to \beta) = xdp^{f_\star}(\rho(\alpha) \to \rho(\beta)).$$

Proof. From the definition of xdp, Lemma 3 and properties of $\rho(x)$ we have

$$\begin{aligned} &xdp^{g_\star}(\alpha \to \beta) = \\ &\quad = \Pr_x \{g_\star(x \oplus \alpha) = g_\star(x) \oplus \beta\} = \\ &\quad = \Pr_x \{\rho(f_\star(\rho(x \oplus \alpha))) = \rho(f_\star(\rho(x))) \oplus \beta\} = \\ &\quad = \Pr_x \{f_\star(\rho(x) \oplus \rho(\alpha)) = f_\star(\rho(x)) \oplus \rho(\beta)\}, \end{aligned}$$

and, with substitution $u := \rho(x)$,

$$\begin{aligned} &xdp^{g_\star}(\alpha \to \beta) = \\ &\quad = \Pr_u \{f_\star(u \oplus \rho(\alpha)) = f_\star(u) \oplus \rho(\beta)\} = \\ &\quad = xdp^{f_\star}(\rho(\alpha) \to \rho(\beta)), \end{aligned}$$

which concludes the proof. □

In this way we can express the differential probabilities of $g_\star$ in terms of the differential probabilities of $f_\star$, which are fully described in Theorems 1 and 3.

VII. Conclusion

In this paper, we consider a family of LRX-analogues of multiplication by small constants, constructed using various logical operations and non-cyclic shifts. These mappings have no rotational symmetry and are therefore less vulnerable to rotational cryptanalysis. We have obtained analytic expressions for the differential probabilities of LRX-analogues. Replacing multiplication by logical AND gives the basic LRX-analogue, which is comparable (but not identical) to the internal function of SIMON in terms of structure and security against differential cryptanalysis. The differential probabilities of all the other analogues are expressed in terms of the probabilities of the basic AND analogue, so they can all be considered as alternatives with roughly the same level of security.

The obtained results can be used to construct efficient LRX-cryptosystems and to evaluate their security against differential cryptanalysis.

Acknowledgment

Most of the results of this paper were presented at the Central European Conference on Cryptology CECC'24 (June 20–21, 2024, Warsaw, Poland) [17]. The author is thankful to the anonymous reviewers for their valuable comments.

References

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Families of Lightweight Block Ciphers," Cryptology ePrint Archive, Paper 2013/404, 2013. [Online]. Available: https://eprint.iacr.org/2013/404

[2] J.-P. Aumasson, P. Jovanovic, and S. Neves, "NORX V2.0," 2015. [Online]. Available: http://competitions.cr.yp.to/round2/norxv20.pdf

[3] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," *Journal of Cryptology*, vol. 34, 2021. [Online]. Available: https://doi.org/10.1007/s00145-021-09398-9

[4] D. Khovratovich and I. Nikolić, "Rotational Cryptanalysis of ARX," in *Fast Software Encryption*. Springer Berlin Heidelberg, 2010, pp. 333–346. [Online]. Available: https://doi.org/10.1007/978-3-642-13858-4_19

[5] D. Khovratovich, I. Nikolić, J. Pieprzyk, P. Sokołowski, and R. Steinfeld, "Rotational Cryptanalysis of ARX Revisited," Cryptology ePrint Archive, Paper 2015/095, 2015. [Online]. Available: https://eprint.iacr.org/2015/095

[6] E. Bresson, A. Canteaut, B. Chevallier-Mames, C. Clavier, T. Fuhr, A. Gouget, T. Icart, J.-F. Misarsky, M. Naya-Plasencia, P. Paillier, T. Pornin, J.-R. Reinhard, C. Thuillet, and M. Videau, "Shabal, a Submission to NIST's Cryptographic Hash Algorithm Competition," Submission to NIST, 2008.

[7] H. Lipmaa and S. Moriai, "Efficient Algorithms for Computing Differential Properties of Addition," in *Fast Software Encryption*, M. Matsui, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 336–350.

[8] NIST and M. J. Dworkin, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," 2015. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=919061

[9] S. Chen, M. Zhu, Z. Xiang, R. Xu, X. Zeng, and S. Zhang, "Rotational-XOR Differential Rectangle Cryptanalysis on Simon-like Ciphers," Cryptology ePrint Archive, Paper 2023/178, 2023. [Online]. Available: https://eprint.iacr.org/2023/178

[10] S. Miyaguchi, "The FEAL Cipher Family," in *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, ser. Lecture Notes in Computer Science, vol. 537. Springer, 1990, pp. 627–638. [Online]. Available: https://doi.org/10.1007/3-540-38424-3_46

[11] D. J. Wheeler and R. M. Needham, "TEA, a Tiny Encryption Algorithm," in *Fast Software Encryption*, B. Preneel, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 363–366.

[12] D. Wheeler and R. Needham, "TEA Extensions," Technical Report, Computer Laboratory, University of Cambridge, Cambridge, 1997. [Online]. Available: http://www.movable-type.co.uk/scripts/xtea.pdf

[13] R. Needham and D. Wheeler, "Correction to XTEA," Technical Report, Computer Laboratory, University of Cambridge, Cambridge, 1998. [Online]. Available: http://www.movable-type.co.uk/scripts/xxtea.pdf

[14] G. van Assche, "A Rotational Distinguisher on Shabal's Keyed Permutation and Its Impact on the Security Proofs," 2010. [Online]. Available: http://gva.noekeon.org/papers/ShabalRotation.pdf

[15] S. Kölbl, G. Leander, and T. Tiessen, "Observations on the SIMON Block Cipher Family," Cryptology ePrint Archive, Paper 2015/145, 2015. [Online]. Available: https://eprint.iacr.org/2015/145

[16] A. Biryukov, A. Roy, and V. Velichkov, "Differential Analysis of Block Ciphers SIMON and SPECK," Cryptology ePrint Archive, Paper 2014/922, 2014. [Online]. Available: https://eprint.iacr.org/2014/922

[17] S. Yakovliev, "Differential Probabilities for LRX-analogues of Small Constant Multiplication," in *Central European Conference on Cryptology CECC '24, Book of Abstracts*, M. Kutyłowski and J. Pomykała, Eds. Warsaw, Poland: Military University of Technology, NASK — National Research Institute, June 2024, pp. 78–81.