UDC 004.056.53:512.6

Differential-Rotational Probabilities of Modular Addition and Its Approximations

Serhii Yakovliev[1], Nikita Korzh[1]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology*

Abstract

In this paper, we consider differential-rotational cryptanalysis, or RX-analysis, and its application to certain classes of ARX-cryptosystems. We provide exact analytical expressions for the RX-differential probabilities with arbitrary rotation values for modular addition. These expressions are described in terms of differential probabilities, which allows comparison of ordinary and RX-differential behaviour. Furthermore, we consider two operations that approximate modular addition, one of which comes from the NORX cipher. For these operations, we also provide exact analytical expressions for the RX-differential probabilities.

Keywords: symmetric cryptography, differential cryptanalysis, rotational cryptanalysis, RX-analysis, ARX, NORX

Introduction

ARX-cryptosystems (from "Add-Rotation-XOR") use only elementary operations within their structure, namely additions modulo 2^n, bitwise additions (XOR) and rotations. This approach enables the construction of highly efficient lightweight algorithms that are well-suited to low-resource devices.

In some cases, modular addition is replaced with some purely logical, non-linear mappings in order to achieve even greater efficiency. Such systems are informally designated as LRX-cryptosystems, where "L" stands for "Logic". Among the most famous LRX-cryptosystems are ciphers Simon [1], NORX [2] and Ascon [3].

Rotational cryptanalysis, first proposed by D. Khovratovich and I. Nikolić [4, 5], is a specific type of cryptanalysis that is exclusively applicable to ARX-cryptosystems. In this approach, an analyst considers so-called "rotation pairs" (pairs of messages, where the second message is a rotation of the first) and studies their transformations during the encryption process. It was found that the addition with constants (either modular or bitwise) effectively counters rotational cryptanalysis.

In [6], T. Ashur and Y. Liu proposed a combined approach, known as differential-rotational cryptanalysis (or RX-analysis), which integrates the ideas of both differential and rotational cryptanalysis. In this approach, rotation pairs are combined with ordinary differentials in what are known as RX-differentials. This allows to easily skip the bitwise addition with arbitrary constants in cryptanalysis. T. Ashur and Y. Liu provided an explicit formula for the RX-differential probabilities with rotation by one bit for modular addition, and set up a 7-round differential-rotational distinguisher on cipher Speck32/64 [1]. Subsequently, a number of successful differential-rotational attacks were proposed on modified Simon and Simeck [7], Alzette and CHAM [8], SipHash [9] etc.

In this work, we examine the properties of the RX-differentials with arbitrary rotation values. We present explicit expressions for the RX-differential probabilities of modular addition, which generalize the known results. We demonstrate the connection between corresponding ordinary and RX-differentials and compare their probabilities. Additionally, two operations which approximate modular addition with relatively short LRX-construction are considered. One of these operations was proposed in the

NORX cipher [2]. We present explicit expressions of RX-differential probabilities for these operations as well.

The rest of the paper is organized as follows. Section 1 provides all essential terms and definitions. Section 2 describes the notion of enhanced differential probabilities for modular addition and their algebraic properties. Section 3 provides explicit expressions of the RX-differential probabilities for modular addition and arbitrary rotation values, along with a complete proof of their correctness. It also compares the behaviour of ordinary and RX-differential probabilities. Section 4 provides explicit expressions of RX-differential probabilities for LRX-mappings that approximate modular addition.

1. Notation and Definitions

In this work, we will use the following notation:

V_n — the set of all binary vectors of length n: $V_n = \{0,1\}$;

$x \in V_n$ — an arbitrary n-bit binary vector

$x = (x_{n-1}, x_{n-2}, \ldots, x_1, x_0),\ x_i \in \{0,1\}$;

$x[k]$ — a sub-vector of last k bits of x:

$$x[k] = (x_{k-1}, x_{k-2}, \ldots, x_1, x_0).$$

$\oplus$ — the addition modulo 2 (XOR);

$+$ — the addition modulo 2^t when the arguments are t-bit vectors, or the usual addition of numbers;

x^r or $x \lll r$ — the rotation (cyclic shift) of the vector x by r bits to the left:

$$x^r = (x_{n-r-1}, \ldots, x_0, x_{n-1}, \ldots, x_{n-r});$$

x^{-r} or $x \ggg r$ — the rotation of the vector x by r bits to the right; note that $x^{-r} \equiv x^{n-r}$;

$x \ll r$ — the non-cyclic shift of the vector x by r bits to the left:

$$x \ll r = (x_{n-r-1}, \ldots, x_0, 0, \ldots, 0);$$

$x \vee y$ — the bitwise logical OR;

$x \wedge y$ or xy — the bitwise logical AND;

$\overline{x}$ — the inversion of all bits of x;

$wt(x)$ — the weight of the vector x (the number of ones);

$eq(x,y,z)$ — a function of bit equality: if $e = eq(x,y,z)$ then $e_i = 1$ iff $x_i = y_i = z_i$; this function can be calculated as

$$eq(x,y,z) = (x \oplus \overline{y})(x \oplus \overline{z});$$

$\mu_{n,r}$ — an n-bit vector with zeros at positions $i = 0$ and $i = r$ and ones at all other positions; it is computed as $\mu_{n,r} = 2^n - 2^r - 2$.

The sequence of carry bits (c_i), $c_i = c_i(x,y)$, associated with the addition of two vectors $x, y \in V_n$ is defined as

$$c_0 = 0, \quad c_{i+1} = x_i y_i \oplus x_i c_i \oplus y_i c_i, \quad i \geq 0.$$

We also define a vector function over carry bits

$$carry(x,y) = (c_{n-1}, \ldots, c_1, c_0) = \\ = (x+y) \oplus x \oplus y.$$

Note that the highest carry bit c_n is not included in $carry(x,y)$ because it is outside the vector.

Consider a mapping $f\colon V_n \times V_n \to V_n$. The *differential* $\omega = (\alpha, \beta \to \gamma)$ *of* f is an arbitrary triplet of vectors $\alpha, \beta, \gamma \in V_n$, representing the differences between two inputs (outputs) of f w.r.t. XOR operation $\oplus$. The *probability of the differential* $\omega = (\alpha, \beta \to \gamma)$ of f is defined as

$$xdp^f(\omega) = xdp^f(\alpha, \beta \to \gamma) = \\ = \Pr_{x,y}\{f(x \oplus \alpha, y \oplus \beta) = f(x,y) \oplus \gamma\}.$$

In the case $f(x,y) = (x+y) \bmod 2^n$ H. Lipmaa and Sh. Moriai [10] found an explicit analytical expression for differential probabilities. Their main result is given in the next theorem.

Theorem 1 ([10])**.** *For arbitrary vectors $\alpha, \beta, \gamma \in V_n$, the probability of the differential $(\alpha, \beta \to \gamma)$ of the modular addition can be evaluated as follows:*

1) $xdp^+(\alpha, \beta \to \gamma) \neq 0$ iff

$$e \wedge (\alpha \oplus \beta \oplus \gamma \oplus (\alpha \ll 1)) = 0;$$

2) if $xdp^+(\alpha, \beta \to \gamma) \neq 0$, then

$$xdp^+(\alpha, \beta \to \gamma) = 2^{-wt(\overline{e})},$$

where $e = eq(\alpha \ll 1, \beta \ll 1, \gamma \ll 1)$.

In [6] T. Ashur and Y. Liu generalized the concept of differential to unify differential and rotational cryptanalysis in one setting. We introduce it in the following manner. *RX-differential* $(r; \alpha, \beta \to \gamma)$ of the mapping f combines a pair of rotation $((x,y),(x^r,y^r))$ with a differential $(\alpha, \beta \to \gamma)$. The *probability of the RX-differential* $(r; \alpha, \beta \to \gamma)$ for the mapping f is defined as

$$xrp^f(r; \alpha, \beta \to \gamma) = \\ = \Pr_{x,y}\{f(x^r \oplus \alpha, y^r \oplus \beta) = (f(x,y))^r \oplus \gamma\}.$$

We use the term xrp^f from "XOR-rotational probability of f" similarly to the term xdp^f

("XOR-differential probability of f"). The ordinary differential $(\alpha, \beta \to \gamma)$ and the RX-differential $(r; \alpha, \beta \to \gamma)$ are referred to as the *corresponding differentials*.

The probabilities xdp^f characterize the security against differential cryptanalysis, and xrp^f — against differential-rotational cryptanalysis.

2. Enhanced Differential Probabilities of the Modular Addition

In this section, we consider some non-trivial differential properties of modular addition. With each differential $\omega = (\alpha, \beta \to \gamma) \in (V_n)^3$ we associate vectors

$$e = e(\omega) = eq(\alpha \ll 1, \beta \ll 1, \gamma \ll 1),$$
$$\delta = \delta(\omega) = \alpha \oplus \beta \oplus \gamma,$$
$$\tau = \tau(\omega) = \alpha \oplus \beta \oplus \gamma \oplus (\alpha \ll 1).$$

Define *enhanced probabilities* $xdp^+_{\kappa,\sigma}(\omega)$ of the differential ω for the modular addition:

$$xdp^+_{\kappa,\sigma}(\omega) =$$
$$= \Pr_{x,y}\{(x \oplus \alpha) + (y \oplus \beta) = (x + y + \kappa) \oplus \gamma, \quad c_n(x \oplus \alpha, y \oplus \beta) = \sigma\},$$

where $\kappa, \sigma \in \{0, 1\}$.

The motivation is as follows. As claimed in [10], the probability $xdp^+(\omega)$ can be expressed as

$$xdp^+(\omega) = \Pr_{x,y}\{c' \oplus c = \alpha \oplus \beta \oplus \gamma\},$$

where the vectors c and c' are carry bit vectors:

$$c' = carry(x \oplus \alpha, y \oplus \beta),$$
$$c = carry(x, y).$$

The parameter σ in enhanced probability allows to split xdp^+ into two subcases by the value of the highest carry bit c'_n, actually $c'_n = \sigma$. On the other hand, the parameter κ allows to extend the notion of xdp^+ to the case when the sequence of carry bits (c_i) starts from the value $c_0 = \kappa$. Both parameters affect the differential-rotational properties of modular addition, as will be demonstrated subsequently.

From the definition we have

$$xdp^+(\omega) = xdp^+_{0,0}(\omega) + xdp^+_{0,1}(\omega).$$

In particular, if $xdp^+(\omega)$ is zero, then both $xdp^+_{0,0}(\omega)$ and $xdp^+_{0,1}(\omega)$ are also zero. But finding the exact value of these enhanced probabilities is a much more complicated problem.

Theorem 2. *For each $\sigma \in \{0, 1\}$ and arbitrary differential $\omega = (\alpha, \beta \to \gamma)$, the following equality holds:*

$$xdp^+_{0,\sigma}(\omega) = \begin{cases} \frac{1}{2} xdp^+(\omega), & \delta \neq 0, \\ \frac{1}{2} xdp^+(\omega) + \frac{(-1)^\sigma}{2^{n+1}}, & \delta = 0, \end{cases}$$

where $\delta = \alpha \oplus \beta \oplus \gamma$.

Proof. For a given differential $\omega = (\alpha, \beta \to \gamma)$ introduce three sequences of partial differential probabilities:

$$U_k = xdp^+(\alpha[k], \beta[k] \to \gamma[k]),$$
$$P_k = xdp^+_{0,0}(\alpha[k], \beta[k] \to \gamma[k]),$$
$$Q_k = xdp^+_{0,1}(\alpha[k], \beta[k] \to \gamma[k]),$$

where $k = 0, 1, \ldots, n-1$.

From Theorem 1 it follows that the sequence U_k satisfies a recurrence relation

$$U_k = \begin{cases} 0, & (e_k = 1) \wedge (\tau_k = 1); \\ U_{k-1}, & (e_k = 1) \wedge (\tau_k = 0); \\ \frac{1}{2} U_{k-1}, & (e_k = 0); \end{cases}$$

with an initial value of $U_0 = 1$. Let's find similar recurrence relations for P_k and Q_k. Note that $c'_0 = 0$ by definition, so the initial values for these sequences are $P_0 = 1$, $Q_0 = 0$.

Consider bit by bit the event "$c' \oplus c = \delta$", where $c' = carry(x \oplus \alpha, y \oplus \beta)$, $c = carry(x, y)$. By the definition of carry bits, after some algebraic transformations, we have

$$k = 0\colon 0 = \delta_0;$$
$$k > 0\colon \alpha_{k-1} y_{k-1} \oplus \beta_{k-1} x_{k-1} \oplus \alpha_{k-1}\beta_{k-1} \oplus \oplus (x_{k-1} \oplus y_{k-1})\Delta c_{k-1} \oplus \oplus (\alpha_{k-1} \oplus \beta_{k-1}) c'_{k-1} = \delta_k,$$

where $\Delta c_{k-1} = c'_{k-1} \oplus c_{k-1} = \delta_{k-1}$ by the condition of the considered event. Therefore, the probability that the given equation is satisfied for $k > 0$ is affected by the independent values x_{k-1}, y_{k-1} and c'_{k-1}, and the probability $\Pr\{c'_{k-1} = \sigma\}$ is equal to P_{k-1} or Q_{k-1}, depending on the σ.

The Tables 1 and 2 give all variants of the equation $\Delta c_k = \delta_k$, their probabilities and the distribution of the carry bit c'_k for all possible values of α_{k-1}, β_{k-1}, δ_{k-1} and δ_k.

From these tables we can derive mutual recurrences for P_k and Q_k, divided by three cases:

Table 1
Table of equations and probabilities for the event $\Delta c_k = \delta_k$ in the case $c'_{k-1} = 0$.

α_{k-1}	β_{k-1}	δ_{k-1}	equation	$\Pr\{\Delta c_k{=}\delta_k\}$, $\delta_k{=}0$	$\Pr\{c'_k{=}0\}$, $\delta_k{=}0$	$\Pr\{\Delta c_k{=}\delta_k\}$, $\delta_k{=}1$	$\Pr\{c'_k{=}0\}$, $\delta_k{=}1$
0	0	0	$0 = \delta_k$	1	$\frac{3}{4}$	0	0
0	0	1	$x_k \oplus y_k = \delta_k$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
0	1	0	$x_k = \delta_k$	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$
0	1	1	$y_k = \delta_k$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	0	0	$y_k = \delta_k$	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$
1	0	1	$x_k = \delta_k$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	0	$x_k \oplus y_k \oplus 1 = \delta_k$	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$
1	1	1	$1 = \delta_k$	0	0	1	$\frac{3}{4}$

Table 2
Table of equations and probabilities for the event $\Delta c_k = \delta_k$ in the case $c'_{k-1} = 1$.

α_{k-1}	β_{k-1}	δ_{k-1}	equation	$\Pr\{\Delta c_k{=}\delta_k\}$, $\delta_k{=}0$	$\Pr\{c'_k{=}0\}$, $\delta_k{=}0$	$\Pr\{\Delta c_k{=}\delta_k\}$, $\delta_k{=}1$	$\Pr\{c'_k{=}0\}$, $\delta_k{=}1$
0	0	0	$0 = \delta_k$	1	$\frac{1}{4}$	0	0
0	0	1	$x_k \oplus y_k = \delta_k$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	0
0	1	0	$x_k = \delta_k$	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
0	1	1	$y_k = \delta_k$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	0
1	0	0	$y_k = \delta_k$	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	1	$x_k = \delta_k$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	0
1	1	0	$x_k \oplus y_k \oplus 1 = \delta_k$	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	1	1	$1 = \delta_k$	0	0	1	$\frac{1}{4}$

(1) if $(e_k = 1) \wedge (\tau_k = 1)$, then

$$P_k = 0, \qquad Q_k = 0.$$

(2) if $(e_k = 1) \wedge (\tau_k = 0)$, then

$$P_k = \frac{3}{4}P_{k-1} + \frac{1}{4}Q_{k-1},$$

$$Q_k = \frac{1}{4}P_{k-1} + \frac{3}{4}Q_{k-1};$$

(3) if $(e_k = 0)$, then

$$P_k = \frac{q_k}{2}P_{k-1} + \frac{(1-q_k)}{2}Q_{k-1},$$

$$Q_k = \frac{(1-q_k)}{2}P_{k-1} + \frac{q_k}{2}Q_{k-1},$$

where $q_k = 2^{-(\delta_k \oplus \delta_{k-1})}$. From these recurrences we can obtain the statement of the theorem by induction.

It should first be noted that $xdp^+(\omega)$ cannot be zero if $\delta = 0$ (or, equivalently, $\gamma = \alpha \oplus \beta$): from Theorem 1 it's easy to see that the probability $xpd^+(\alpha, \beta \to \alpha \oplus \beta)$ is non-zero for every α and β. Thus, if $xdp^+(\omega) = 0$, then $\delta \neq 0$ and $xdp^+_{0,\sigma}(\omega) = 0 = \frac{1}{2}xdp^+(\omega)$, which is the statement of the theorem. For the remainder of this proof, we will consider only the case $xdp^+(\omega) \neq 0$.

Since $e_0 = 1$ in every case, if $xdp^+(\omega) \neq 0$ then $\delta_0 = 0$, so the initial values must correspond to the second case of the theorem's statement. Indeed,

$$P_0 = 1 = \frac{1}{2}U_0 + \frac{1}{2},$$

$$Q_0 = 0 = \frac{1}{2}U_0 - \frac{1}{2}.$$

This forms the basis of induction.

Consider the case $\delta[k] = 0$. By the assumption of induction we have

$$P_{k-1} = \frac{1}{2}U_{k-1} + \frac{1}{2^k},$$

$$Q_{k-1} = \frac{1}{2}U_{k-1} - \frac{1}{2^k}.$$

Then in the case (2) we have $U_k = U_{k-1}$ and

$$P_k = \frac{3}{4}P_{k-1} + \frac{1}{4}Q_{k-1} = \\ = \frac{3}{4}\left(\frac{1}{2}U_{k-1} + \frac{1}{2^k}\right) + \frac{1}{4}\left(\frac{1}{2}U_{k-1} - \frac{1}{2^k}\right) = \\ = \frac{1}{2}U_k + \frac{1}{2^{k+1}},$$

From the other hand, in the case (3) we have $q_k = 1$, $U_k = \frac{1}{2}U_{k-1}$ and

$$P_k = \frac{1}{2}P_{k-1} = \frac{1}{2}\left(\frac{1}{2}U_{k-1} + \frac{1}{2^k}\right) = \\ = \frac{1}{2}U_k + \frac{1}{2^{k+1}},$$

Thereby, in both cases

$$Q_k = U_k - P_k = \frac{1}{2}U_k - \frac{1}{2^{k+1}}.$$

So, if $\delta = 0$, it follows by induction that

$$xdp^+_{0,\sigma}(\omega) = \frac{1}{2}xdp^+(\omega) + \frac{(-1)^\sigma}{2^{n+1}}.$$

Then consider the case $\delta[k-1] = 0$, $\delta_k = 1$. Note that in this case the condition $(e_k = 1) \wedge (\tau_k = 0)$ is unachievable: if $e_k = 1$, then $\alpha_{k-1} = \beta_{k-1} = \gamma_{k-1}$ and, since $\delta_{k-1} = 0$, all these bits are zero. But then the value $\tau_k = \delta_k \oplus \alpha_{k-1} = 1$. Thus, under these conditions the case (2) of recurrence has no place. Then in the case (3) we have $q_k = \frac{1}{2}$ and

$$P_k = \frac{1}{4}P_{k-1} + \frac{1}{4}Q_{k-1} = \\ = \frac{1}{4}\left(\frac{1}{2}U_{k-1} + \frac{1}{2^k}\right) + \frac{1}{4}\left(\frac{1}{2}U_{k-1} - \frac{1}{2^k}\right) = \\ = \frac{1}{4}U_{k-1} = \frac{1}{2}U_k,$$

and, from this point,

$$P_k = Q_k = \frac{1}{2}U_k.$$

Therefore, in the case (2) for any $t > k$ we have

$$P_t = \frac{3}{4}P_{t-1} + \frac{1}{4}Q_{t-1} = \\ = \frac{3}{4}\cdot\frac{1}{2}U_{t-1} + \frac{1}{4}\cdot\frac{1}{2}U_{t-1} = \frac{1}{2}U_t,$$

and in the case (3)

$$P_t = \frac{q_t}{2}P_{t-1} + \frac{(1-q_t)}{2}Q_{t-1} = \\ = \frac{q_t}{2}\cdot\frac{1}{2}U_{t-1} + \frac{(1-q_k)}{2}\cdot\frac{1}{2}U_{t-1} = \frac{1}{2}U_t.$$

So, if $\delta \neq 0$, it follows by induction that

$$xdp^+_{0,\sigma}(\omega) = \frac{1}{2}xdp^+(\omega),$$

which concludes the proof. □

The Theorem 2 completely describes the probabilities $xdp^+_{0,\sigma}$. Further we demonstrate that the probabilities $xdp^+_{1,\sigma}$ are also expressed through $xdp^+_{0,\sigma}$. The properties of $xdp^+_{1,\sigma}$ are given in the next two lemmas.

For each differential $\omega = (\alpha, \beta \to \gamma)$, we denote the differential of the bitwise inverted differences as $\overline{\omega}$: $\overline{\omega} = (\overline{\alpha}, \overline{\beta} \to \overline{\gamma})$.

Lemma 1. *For arbitrary $\alpha, \beta, \gamma \in V_n$ the following equality holds:*

$$\Pr_{x,y}\{(x \oplus \alpha) + (y \oplus \beta) = (x + y + 1) \oplus \gamma\} = \\ = xdp^+(\overline{\alpha}, \overline{\beta} \to \overline{\gamma}).$$

Moreover, for each $\sigma \in \{0, 1\}$

$$xdp^+_{1,\sigma}(\alpha, \beta \to \gamma) = xdp^+_{0,\sigma}(\overline{\alpha}, \overline{\beta} \to \overline{\gamma}).$$

Proof.[1] It's well known that the following equalities hold for any $u, v \in V_n$ [11]:

$$\overline{u} \oplus \overline{v} = u \oplus v,$$
$$\overline{u} \oplus v = u \oplus \overline{v},$$
$$\overline{u} = -u - 1.$$

Therefore, we have

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

With these facts, we can perform equivalent transformations:

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y + 1) \oplus \gamma,$$
$$(\overline{x} \oplus \overline{\alpha}) + (\overline{y} \oplus \overline{\beta}) = (x + y + 1) \oplus \gamma,$$
$$(\overline{x} \oplus \overline{\alpha}) + (\overline{y} \oplus \overline{\beta}) = \overline{(\overline{x} + \overline{y})} \oplus \gamma,$$
$$(\overline{x} \oplus \overline{\alpha}) + (\overline{y} \oplus \overline{\beta}) = (\overline{x} + \overline{y}) \oplus \overline{\gamma},$$

where the probability of the last equality is, by definition, equal to $xdp^+(\overline{\alpha}, \overline{\beta} \to \overline{\gamma})$. This proves the first statement of the lemma.

The second statement comes from the previous arguments and an equation

$$c_n(x \oplus \alpha, y \oplus \beta) = c_n(\overline{x} \oplus \overline{\alpha}, \overline{y} \oplus \overline{\beta}),$$

so a substitution of the variables $x, y \mapsto \overline{x}, \overline{y}$ transforms the internal event of $xdp^+_{1,\sigma}(\omega)$ into the internal event of $xdp^+_{0,\sigma}(\overline{\omega})$. □

[1] The first statement of Lemma 1 was introduced in [6, Lemma 2] in a different formulation and with a completely different proof.

Lemma 2. *For any $\omega = (\alpha, \beta \to \gamma)$ only one of the differentials ω and $\overline{\omega}$ can have a non-zero xdp^+ probability.*

Proof. From Theorem 1 we know that $xdp^+(\omega) \neq 0$ iff $e(\omega) \wedge \tau(\omega) = 0$. But if $\alpha_i = \beta_i = \gamma_i$, then $\overline{\alpha_i} = \overline{\beta_i} = \overline{\gamma_i}$, so $e(\omega)_i = e(\overline{\omega})_i$ for all i. Similarly, $\tau(\omega)_i = \tau(\overline{\omega})_i$ for all $i > 0$. For $i = 0$ we have

$$\begin{aligned}\tau(\omega)_0 &= \alpha_0 \oplus \beta_0 \oplus \gamma_0,\\ \tau(\overline{\omega})_0 &= \overline{\alpha_0} \oplus \overline{\beta_0} \oplus \overline{\gamma_0} = \\ &= \alpha_0 \oplus \beta_0 \oplus \gamma_0 \oplus 1 = \tau(\omega)_0 \oplus 1.\end{aligned}$$

Since $e(\omega)_0 = e(\overline{\omega})_0 = 1$, we can conclude that the vectors $e(\omega) \wedge \tau(\omega)$ and $e(\overline{\omega}) \wedge \tau(\overline{\omega})$ differ only at position $i = 0$, where they equal to $\alpha_0 \oplus \beta_0 \oplus \gamma_0$ and $\alpha_0 \oplus \beta_0 \oplus \gamma_0 \oplus 1$ respectively. So we have the following cases:

$$\begin{aligned}\alpha_0 \oplus \beta_0 = \gamma_0 \quad &\Rightarrow \quad xdp^+(\overline{\omega}) = 0,\\ \alpha_0 \oplus \beta_0 \neq \gamma_0 \quad &\Rightarrow \quad xdp^+(\omega) = 0.\end{aligned}$$

This concludes the proof. □

Corollary 1. For any differential $\omega = (\alpha, \beta \to \gamma)$ and $\sigma \in \{0, 1\}$ only one of the probabilities $xdp^+_{0,\sigma}(\omega)$ and $xdp^+_{1,\sigma}(\omega)$ can be non-zero. In particular, $xdp^+_{\kappa,\sigma}(\omega) = 0$ if $\delta_0 = \kappa \oplus 1$.

Proof. This follows directly from Lemma 2 and the equality $xdp^+_{1,\sigma}(\omega) = xdp^+_{0,\sigma}(\overline{\omega})$ (from Lemma 1). □

In summary, we can transform the enhanced probability $xdp^+_{1,\sigma}$ into the probability $xdp^+_{0,\sigma}$ of the bitwise inverse differential, and we can efficiently compute all probabilities $xdp^+_{0,\sigma}$ with the Theorems 2 and 1.

3. The Probabilities of RX-differentials for the Modular Addition

T. Ashur and Y. Liu in [6] provided the explicit formula of RX-differential probabilities for modular addition in the case $r = 1$, which this margin is too narrow to contain. In [8] M. Huang *et al.* gave the ponderous expression for these probabilities with an arbitrary rotation value of r, which combines at least four parts with four probabilities of sub-events in each. In this section we present a much simpler evaluation expression for RX-differential probabilities for any value of r in terms of enhanced differential probabilities of modular addition.

We use the following notation throughout this section: each vector $x \in V_n$ is represented as a concatenation $x = x^* \| x'$, where

$$\begin{aligned}x^* &= (x_{n-1}, x_{n-2}, \ldots, x_r),\\ x' &= (x_{r-1}, x_{r-2}, \ldots, x_0) = x[r],\end{aligned}$$

so $|x^*| = n - r$ and $|x'| = r$. In parallel, x is represented as $x = x'' \| x^{**}$, where

$$\begin{aligned}x'' &= (x_{n-1}, x_{n-2}, \ldots, x_{n-r}),\\ x^{**} &= (x_{n-r-1}, x_{n-r-2}, \ldots, x_0) = x[n-r],\end{aligned}$$

and $|x''| = r$, $|x^{**}| = n - r$. Note that x^r is expressed as $x^r = x^{**} \| x''$.

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

Theorem 3. *For any fixed rotation value r, $1 \leq r \leq n-1$, and arbitrary vectors $\alpha, \beta, \gamma \in V_n$, the probability of the RX-differential $(r; \alpha, \beta \to \gamma)$ of the modular addition is evaluated as follows:*

$$xrp^+(r; \alpha, \beta \to \gamma) = xdp^+_{\delta_r,\delta_0}(\omega^*) xdp^+_{\delta_0,\delta_r}(\omega'),$$

where $\omega^* = (\alpha^*, \beta^* \to \gamma^*)$, $\omega' = (\alpha', \beta' \to \gamma')$, and $\delta = \alpha \oplus \beta \oplus \gamma$.

Proof. Consider the equation

$$(x^r \oplus \alpha) + (y^r \oplus \beta) = (x + y)^r \oplus \gamma.$$

Denote its left part by $w = w(x, y)$ and its right part by $u = u(x, y)$. Then we can say that

$$\begin{aligned}u^* &= (x^{**} + y^{**}) \oplus \gamma^*,\\ u' &= (x'' + y'' + C_{n-r}) \oplus \gamma',\\ w^* &= (x^{**} \oplus \alpha^*) + (y^{**} \oplus \beta^*) + C_r,\\ w' &= (x'' \oplus \alpha') + (y'' \oplus \beta'),\end{aligned}$$

where C_r and C_{n-r} are the highest carry bits:

$$\begin{aligned}C_r &= c_r(x'' \oplus \alpha', y'' \oplus \beta'),\\ C_{n-r} &= c_{n-r}(x^{**}, y^{**}).\end{aligned}$$

The variables C_r and C_{n-r} are independent because they are determined by independent parts of the vectors x and y.

From the equations $u^* = w^*$ and $u' = w'$ we get the system of equations

$$\begin{cases}(x'' \oplus \alpha') + (y'' \oplus \beta') = \\ \qquad = (x'' + y'' + C_{n-r}) \oplus \gamma',\\ (x^{**} \oplus \alpha^*) + (y^{**} \oplus \beta^*) + C_r = \\ \qquad = (x^{**} + y^{**}) \oplus \gamma^*.\end{cases}$$

Let $x^{***} = x^{**} \oplus \alpha^*$, $y^{***} = y^{**} \oplus \beta^*$; then the obtained system can be written as

$$\begin{cases} (x'' \oplus \alpha') + (y'' \oplus \beta') = \\ \qquad = (x'' + y'' + C_{n-r}) \oplus \gamma', \\ (x^{***} \oplus \alpha^*) + (y^{***} \oplus \beta^*) = \\ \qquad = (x^{***} + y^{***} + C_r) \oplus \gamma^*. \end{cases}$$

These equations describe dependent events, since C_{n-r} is a function of x^{***}, y^{***}, and C_r is a function of x'', y''. From this we have that the probability of the first equation is $xdp^+_{C_{n-r},C_r}(\omega')$, and the probability of the second equation is $xdp^+_{C_r,C_{n-r}}(\omega^*)$ for all possible values of C_{n-r}, C_r. Therefore,

$$\begin{aligned} xrp^+(r;\alpha,\beta\to\gamma) = {} & xdp^+_{0,0}(\omega^*)\cdot xdp^+_{0,0}(\omega') + \\ & + xdp^+_{0,1}(\omega^*)\cdot xdp^+_{1,0}(\omega') + \\ & + xdp^+_{1,0}(\omega^*)\cdot xdp^+_{0,1}(\omega') + \\ & + xdp^+_{1,1}(\omega^*)\cdot xdp^+_{1,1}(\omega'). \end{aligned}$$

But from Lemma 2 it follows that we can specify all guaranteed zero terms in the xrp^+ expression with the values of the bits δ_r and δ_0 (computed from the last bits of the differentials ω^* and ω'):

$$\begin{aligned} \delta_0 = 0\colon &\quad xdp^+_{1,\sigma}(\omega') = 0; \\ \delta_r = 0\colon &\quad xdp^+_{1,\sigma}(\omega^*) = 0; \\ \delta_r = 1\colon &\quad xdp^+_{0,\sigma}(\omega^*) = 0; \\ \delta_0 = 1\colon &\quad xdp^+_{0,\sigma}(\omega') = 0. \end{aligned}$$

Thus, for any value of (δ_0, δ_r), only one listed term in the xrp^+ expression can possibly be non-zero. This concludes the proof of the theorem. □

Theorem 3 can also be expressed in Lipmaa-Moriai style, which allows to compare ordinary and RX-differentials. This expressions follow directly from the statement of the Theorems 3 and the Theorems 2 and 1.

Corollary 2. For any fixed rotation value r and vectors $\alpha, \beta, \gamma \in V_n$, the probability of the RX-differential $(r;\alpha,\beta \to \gamma)$ of the modular addition can be evaluated as follows:

1) $xrp^+(r;\alpha,\beta\to\gamma) \neq 0$ iff

$$e \wedge (\alpha \oplus \beta \oplus \gamma \oplus (\alpha \ll 1)) \wedge \mu_{n,r} = 0;$$

2) if $xrp^+(r;\alpha,\beta\to\gamma) \neq 0$, then

$$\begin{aligned} & xrp^+(r;\alpha,\beta\to\gamma) = \\ & \quad = \frac{1}{4}\Bigg(2^{-wt(\overline{e}^*)-wt(\overline{e}')} + \\ & \qquad + [\delta'=0]\frac{(-1)^{\delta_r}\cdot 2^{-wt(\overline{e}^*)}}{2^r} + \\ & \qquad + [\delta^*=0]\frac{(-1)^{\delta_0}\cdot 2^{-wt(\overline{e}')}}{2^{n-r}} + \\ & \qquad + [\delta^*=0][\delta'=0]\frac{(-1)^{\delta_r\oplus\delta_0}}{2^n}\Bigg), \end{aligned}$$

where $\delta = \alpha \oplus \beta \oplus \gamma$, $[\dots]$ denotes an indicator function (Iverson brackets), and

$$\begin{aligned} e &= eq(\alpha \ll 1, \beta \ll 1, \gamma \ll 1), \\ e^* &= eq(\alpha^* \ll 1, \beta^* \ll 1, \gamma^* \ll 1), \\ e' &= eq(\alpha' \ll 1, \beta' \ll 1, \gamma' \ll 1). \end{aligned}$$

Corollary 2 allows us to compare the behaviour of the xdp^+ and xrp^+ probabilities of the corresponding differentials. In fact, xrp^+ has softer requirements for RX-differentials to have non-zero probability than xdp^+ for the corresponding ordinary differential: the conditions are identical to xdp^+ except for bit positions 0 and r, which are excluded from consideration. Therefore, there are approximately four times more RX-differentials with non-zero probability than ordinary ones.

It's easy to describe a set of RX-differentials with non-zero probability in terms of xdp^+: $xrp^+(r;\alpha,\beta\to\gamma) \neq 0$ if

$$xdp^+(\alpha \wedge \mu_{n,r}, \beta \wedge \mu_{n,r} \to \gamma \wedge \mu_{n,r}) \neq 0,$$

even if $xdp^+(\alpha,\beta\to\gamma)$ is zero.

Consider the case where both xdp^+ and xrp^+ probabilities are non-zero. Then the xrp^+ probabilities are generally expected to be smaller than the corresponding xdp^+ probabilities, but there are differentials with the opposite relationship. Consider the next example: $n = 4$ and differential

$$\alpha = 0001,\ \beta = 1111,\ \gamma = 1110.$$

Direct calculations show that

$$\begin{aligned} xdp^+(\alpha,\beta\to\gamma) &= \frac{1}{8}, \\ xrp^h(r;\alpha,\beta\to\gamma) &= \frac{9}{64} > \frac{1}{8}, \quad r = 1,2,3. \end{aligned}$$

4. Probabilities of RX-differentials for Operations that Approximate Addition

In [2], the developers of the NORX cipher introduced the operation[2]

$$h(x,y) = x \oplus y \oplus ((x \wedge y) \ll 1),$$

which approximates addition modulo 2^n. In [12], another approximation operation for modular addition was introduced:

$$v(x,y) = x \oplus y \oplus ((x \vee y) \ll 1) \oplus 1.$$

Both approximations are based on well-known equations for modular addition and logical operations [11]:

$$x + y = (x \oplus y) + ((x \wedge y) \ll 1),$$
$$x + y = ((x \vee y) \ll 1) - (x \oplus y),$$

where the addition (subtraction) on the right has been replaced by XOR.

The cryptographic properties of these operations, including the values of the XOR-differential probabilities, have been researched in [13, 12]. These results are given in the next two theorems.

Theorem 4 ([13])**.** *For arbitrary vectors $\alpha, \beta, \gamma \in V_n$, the probability of the differential $(\alpha, \beta \to \gamma)$ for the function $h(x,y)$ can be evaluated as follows:*

1) $xdp^h(\alpha, \beta \to \gamma) \neq 0$ iff

$$(\overline{(\alpha \vee \beta) \ll 1}) \wedge \delta = 0;$$

2) if $xdp^h(\alpha, \beta \to \gamma) \neq 0$, then

$$xdp^h(\alpha, \beta \to \gamma) = 2^{-wt((\alpha \vee \beta) \ll 1)};$$

where $\delta = \alpha \oplus \beta \oplus \gamma$.

Theorem 5 ([12])**.** *For arbitrary vectors $\alpha, \beta, \gamma \in V_n$, the probability of the differential $(\alpha, \beta \to \gamma)$ for the function $v(x,y)$ can be evaluated as follows:*

1) $xdp^v(\alpha, \beta \to \gamma) \neq 0$ iff

$$(\overline{(\alpha \vee \beta) \ll 1}) \wedge \delta = 0;$$

2) if $xdp^v(\alpha, \beta \to \gamma) \neq 0$, then

$$xdp^v(\alpha, \beta \to \gamma) = 2^{-wt((\alpha \vee \beta) \ll 1)};$$

where $\delta = \alpha \oplus \beta \oplus \gamma$.

[2] This operation was denoted as $x\mathsf{H}y$ and $\mathsf{H}(x,y)$ in [2] since the symbol H resembles $+$ in some way. We use the more functional notation $h(x,y)$.

It is worth noting that the statements of the Theorems 4 and 5 are identical, so for any differential ω the equality $xdp^h(\omega) = xdp^v(\omega)$ holds.

The next two theorems provide analytic expressions for the RX-differential probabilities of given operations $h(x,y)$ and $v(x,y)$.

Theorem 6. *For any fixed rotation value r, $1 \leq r \leq n-1$, and arbitrary vectors $\alpha, \beta, \gamma \in V_n$, the probability of the RX-differential $(r; \alpha, \beta \to \gamma)$ for the function $h(x,y)$ can be evaluated as follows:*

1) $xrp^h(r; \alpha, \beta \to \gamma) \neq 0$ iff

$$(\overline{(\alpha \vee \beta) \ll 1}) \wedge \delta \wedge \mu_{n,r} = 0;$$

2) if $xrp^h(r; \alpha, \beta \to \gamma) \neq 0$, then

$$xrp^h(r; \alpha, \beta \to \gamma) =$$
$$= \left(\frac{3}{4} - \frac{\delta_0}{2}\right)\left(\frac{3}{4} - \frac{\delta_r}{2}\right) 2^{-wt(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r})};$$

where $\delta = \alpha \oplus \beta \oplus \gamma$.

Proof. Consider the equation

$$h(x^r \oplus \alpha, y^r \oplus \beta) = (h(x,y))^r \oplus \gamma.$$

It's easy to show that this equation is equal to $u \oplus w = \delta$, where two vectors $u = u(x,y)$, $w = w(x,y)$ are introduced as

$$u = ((xy) \ll 1)^r,$$
$$w = ((x^r \oplus \alpha)(y^r \oplus \beta) \ll 1).$$

The following relations describe each bit of u:

$$\begin{cases} u_i = x_{i+n-r-1} y_{i+n-r-1}, & 0 \leqslant i < r; \\ u_r = 0, & i = r; \\ u_i = x_{i-r-1} y_{i-r-1}, & i > r; \end{cases}$$

and a similar system of relations describes every bit of w:

$$\begin{cases} w_0 = 0, & i = 0; \\ w_i = (x_{i+n-r-1} \oplus \alpha_{i-1})(y_{i+n-r-1} \oplus \beta_{i-1}), & 0 < i \leqslant r; \\ w_i = (x_{i-r-1} \oplus \alpha_{i-1})(y_{i-r-1} \oplus \beta_{i-1}), & i > r. \end{cases}$$

Consider the equation $u \oplus w = \delta$ bit by bit. There are the following possible cases for this.

1. If $i = 0$, then

$$x_{n-r-1} y_{n-r-1} = \delta_0.$$

2. If $i = r$, then

$$(x_{n-1} \oplus \alpha_{r-1})(y_{n-1} \oplus \beta_{r-1}) = \delta_r.$$

3. If $0 < i < r$, then

$$x_{i+n-r-1}\beta_{i-1} \oplus \alpha_{i-1}y_{i+n-r-1} = \\ = \alpha_{i-1}\beta_{i-1} \oplus \delta_i.$$

4. If $i > r$, then

$$x_{i-r-1}\beta_{i-1} \oplus \alpha_{i-1}y_{i-r-1} = \alpha_{i-1}\beta_{i-1} \oplus \delta_i.$$

Let A_i be the event $u_i \oplus w_i = \delta_i$, and p_i be the probability of A_i. Since all events A_i depend on different bits of x and y, they are pairwise independent, therefore we have

$$xrp^h(r; \alpha, \beta \to \gamma) = \prod_{i=0}^{n-1} p_i.$$

Let's compute the probabilities p_i for each value of i.

1. In the case $i = 0$, if $\delta_0 = 0$, then

$$p_0 = \Pr\{x_{n-r-1}y_{n-r-1} = 0\} = \frac{3}{4},$$

and if $\delta_0 = 1$, then

$$p_0 = \Pr\{x_{n-r-1}y_{n-r-1} = 1\} = \frac{1}{4}.$$

Therefore, we have

$$p_0 = \left(\frac{3}{4} - \frac{\delta_0}{2}\right).$$

2. The case $i = r$ is considered similarly to the previous case; we have

$$p_r = \left(\frac{3}{4} - \frac{\delta_r}{2}\right).$$

3. Next we consider the case for all other values of i when $i \neq 0$ and $i \neq r$. All these cases are described by a general equation of the following form:

$$\delta_i \oplus \alpha_{i-1}\beta_{i-1} = x_*\beta_{i-1} \oplus y_*\alpha_{i-1},$$

where x_* and y_* are random independent bits.

The Table 3 shows the values of the probability p_i for all possible values of the parameters α_{i-1}, β_{i-1}, and δ_i.

From the Table 3 it is clear that there are specific values of the parameters $\alpha_{i-1}, \beta_{i-1}$, and δ_i, for which the probability $p_i = 0$, namely $\delta_i = 1$ and $\alpha_{i-1} = \beta_{i-1} = 0$ (the latter being equivalent to $\alpha_{i-1} \vee \beta_{i-1} = 0$), where $i \neq 0$, $i \neq r$. Clearly, if a vector

$$(\overline{(\alpha \vee \beta) \ll 1}) \wedge \delta \wedge \mu_{n,r}$$

has at least one non-zero bit, then $xrp^h(r; \alpha, \beta \to \gamma)$ is zero.

Table 3
The probabilities p_i in the general case of $i \neq 0, r$.

α_{i-1}	β_{i-1}	δ_i	equation of A_i	p_i
0	0	0	$0 = 0$	1
0	0	1	$1 = 0$	0
0	1	0	$0 = y_*$	$\frac{1}{2}$
0	1	1	$1 = y_*$	$\frac{1}{2}$
1	0	0	$0 = x_*$	$\frac{1}{2}$
1	0	1	$1 = x_*$	$\frac{1}{2}$
1	1	0	$1 = x_* \oplus y_*$	$\frac{1}{2}$
1	1	1	$0 = x_* \oplus y_*$	$\frac{1}{2}$

If the probability of the RX-differential is not zero, then for $\alpha_{i-1} = \beta_{i-1} = 0$ the probability p_i is one, and in all other cases where either one of the two bits α_{i-1}, β_{i-1} equals one, the probability p_i is $\frac{1}{2}$. Consequently, we have $p_i = \frac{1}{2}$ for every bit equal to one in the vector $(\alpha \oplus \beta) \ll 1$ (except for the positions $i = 0$ and $i = r$).

In summary, we have that non-zero probabilities of RX-differentials of $h(x, y)$ are equal to

$$xrp^h(r; \alpha, \beta \to \gamma) = \\ = \left(\frac{3}{4} - \frac{\delta_0}{2}\right)\left(\frac{3}{4} - \frac{\delta_r}{2}\right) 2^{-wt(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r})},$$

which concludes the proof. □

Theorem 7. *For any fixed rotation value r, $1 \leq r \leq n-1$, and arbitrary vectors $\alpha, \beta, \gamma \in V_n$, the probability of the RX-differential $(r; \alpha, \beta \to \gamma)$ for the function $v(x, y)$ can be evaluated as follows:*

1) $xrp^v(r; \alpha, \beta \to \gamma) \neq 0$ iff

$$(\overline{(\alpha \vee \beta) \ll 1}) \wedge \delta \wedge \mu_{n,r} = 0;$$

2) if $xrp^v(r; \alpha, \beta \to \gamma) \neq 0$, then

$$xrp^v(r; \alpha, \beta \to \gamma) = \\ = \left(\frac{3}{4} - \frac{\delta_0}{2}\right)\left(\frac{3}{4} - \frac{\delta_r}{2}\right) 2^{-wt(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r})}.$$

where $\delta = \alpha \oplus \beta \oplus \gamma$.

Proof. The proof is very similar to that of Theorem 6. Once again, consider the equation

$$v(x^r \oplus \alpha, y^r \oplus \beta) = (v(x, y))^r \oplus \gamma.$$

It's easy to show that this equation is equivalent to the equation $u \oplus w = \delta \oplus ((\alpha \oplus \beta) \ll 1)$,

where two vectors $u = u(x, y)$, $w = w(x, y)$ are introduced as

$$u = \big((x \ll 1) \oplus (y \ll 1) \oplus ((xy) \ll 1) \oplus 1\big)^r,$$
$$w = (x^r \ll 1) \oplus (y^r \ll 1) \oplus \\ \oplus ((x^r \oplus \alpha)(y^r \oplus \beta) \ll 1) \oplus 1.$$

Let A_i be the event $u_i \oplus w_i = \delta_i \oplus \alpha_{i-1} \oplus \beta_{i-1}$, and p_i be the probability of A_i, so that $xrp^v(r; \alpha, \beta \to \gamma)$ is a product of all p_i. Compute the probabilities p_i for each value of i.

1. For $i = 0$ we have

$$p_0 = \Pr\{\overline{x}_{n-r-1}\overline{y}_{n-r-1} = \delta_0\} = \left(\frac{3}{4} - \frac{\delta_0}{2}\right).$$

2. For $i = r$ we similarly have

$$p_r = \Pr\{(\overline{x_{n-1} \oplus \alpha_{r-1}})(\overline{y_{n-1} \oplus \beta_{r-1}}) = \delta_r\} = \\ = \left(\frac{3}{4} - \frac{\delta_r}{2}\right).$$

3. For all other values of $i \neq 0, r$, the events A_i are described by a general equation of the following form:

$$\delta_i \oplus \alpha_{i-1} \oplus \beta_{i-1} \oplus \alpha_{i-1}\beta_{i-1} = x_*\beta_{i-1} \oplus y_*\alpha_{i-1},$$

or, equivalently,

$$\delta_i \oplus \alpha_{i-1}\beta_{i-1} = \overline{x}_*\beta_{i-1} \oplus \overline{y}_*\alpha_{i-1},$$

where x_* and y_* are random independent bits. Clearly, a substitution $x_* \mapsto \overline{x}_*$, $y_* \mapsto \overline{y}_*$ allows us to describe all possible values of p_i with Table 3.

Therefore, the probabilities p_i for xrp^v are the same as for xrp^h (see the proof of Theorem 6), from which the statement of the theorem follows. □

From the statements of the Theorems 6 and 7, it follows that the behaviour of the probabilities of RX-differentials for the functions $h(x, y)$ and $v(x, y)$ is described by identical expressions, so that their numerical values coincide. This allows us to conclude that both operations have the same level of security against RX-analysis and can be used as alternatives. It should be noted that, unlike the distribution of xrp^+, the distribution of xrp^h (xrp^v) values over all RX-differentials does not depend on r, so all possible values of r can be considered equally in cryptanalysis.

It's also interesting to compare the behaviour of the differential and RX-differential probabilities of $h(x, y)$, as well as $v(x, y)$. As we can see from the Theorems 4 and 6, similar to xrp^+ and xdp^+, xrp^h has softer requirements for RX-differential to have non-zero probability than xdp^h for the corresponding ordinary differential: the condition is identical, but bit positions 0 and r are also excluded from consideration. Thus, the number of RX-differential with non-zero probability is approximately four times higher than the number of ordinary differential, and, moreover, we can claim that $xrp^h(r; \alpha, \beta \to \gamma) \neq 0$ if

$$xdp^h(\alpha \wedge \mu_{n,r}, \beta \wedge \mu_{n,r} \to \gamma \wedge \mu_{n,r}) \neq 0.$$

Consider the case where both xdp^h and xrp^h probabilities of the corresponding differentials are non-zero. The value of xrp^h is multiplied by the factor $\frac{9}{16}$, $\frac{3}{16}$ or $\frac{1}{16}$ compared to the corresponding xdp^h value, and can also be multiplied by 2, depending on δ_0, δ_r and $\alpha_{i-1} \vee \beta_{i-1}$, so that in most cases xrp^h has less values than xdp^h. Interestingly, however, there are RX-differentials of h which have a higher probability than corresponding ordinary differentials. More precisely, if $\delta_0 = 0$, $\delta_r = 0$ and $\alpha_{r-1} \vee \beta_{r-1} = 1$ then

$$xrp^h(r; \alpha, \beta \to \gamma) \geq xdp^h(\alpha, \beta \to \gamma).$$

For $xdp^h \neq 0$ the ratio xrp^h/xdp^h is $\frac{9}{8}$ under the above conditions.

Consider the next example: $n \geq 3$, $r = 1$, and differential

$$\alpha = 0 \ldots 0011,\ \beta = 0 \ldots 0011,\ \gamma = 0 \ldots 0100;$$

then $\delta_0 = 0$, $\delta_1 = 0$, and

$$xdp^h(\alpha, \beta \to \gamma) = \frac{1}{4},$$
$$xrp^h(1; \alpha, \beta \to \gamma) = \frac{9}{32} > \frac{1}{4}.$$

From the Theorems 5 and 7 it follows that for xrp^v and xdp^v all the above considerations are the same.

Conclusions

In this work, we study the properties of the RX-differentials of modular addition and their LRX-approximations. We introduced the notion of enhanced differential probabilities for modular addition, which allow the differential properties to be considered from different angles, and provided explicit and simple analytic expressions for them. We then provided expressions for the probabilities of RX-differential with arbitrary

rotation values for modular addition in terms of enhanced differential probabilities and consequently in Lipmaa-Moriai style. These results generalize the pioneering results of T. Ashur and Yu. Liu, and are also much simpler than analogous results of M. Huang *et al.* Among other things, our results allow to compare the behaviour of the corresponding ordinary and RX-differentials, to effectively describe a set of RX-differentials with non-zero probabilities and to find RX-differentials with higher probability than the corresponding ordinary differentials. The latter, although interesting from a mathematical point of view, does not seem to be very useful since such differentials generally have relatively low probabilities.

We also considered two operations that approximate modular addition with purely logical functions. One of these operations is used in the NORX cipher. We provided explicit analytic expressions of the probabilities of RX-differentials for both operations in the Lipmaa-Moriai style, and showed that the behaviour of the RX-differentials of these operations is similar to that of modular addition.

We believe that the presented results advance the theory of differential-rotational cryptanalysis and allow the creation of new cryptographically secure ARX- and LRX-cryptosystems.

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. https://eprint.iacr.org/2013/404.

[2] J.-P. Aumasson, P. Jovanovic, and S. Neves, "NORX V3.0: Submission to the CAESAR Competition," 2015. https://competitions.cr.yp.to/round3/norxv30.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.

[4] D. Khovratovich and I. Nikolić, "Rotational Cryptanalysis of ARX," in *Fast Software Encryption*, pp. 333–346, Springer Berlin Heidelberg, 2010.

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

[6] T. Ashur and Y. Liu, "Rotational Cryptanalysis in the Presence of Constants," *IACR Transactions on Symmetric Cryptology*, vol. 2016, p. 57–70, Dec. 2016. https://tosc.iacr.org/index.php/ToSC/article/view/535.

[7] J. Lu, Y. Liu, T. Ashur, B. Sun, and C. Li, "Rotational-XOR Cryptanalysis of Simon-Like Block Ciphers," in *Information Security and Privacy* (J. K. Liu and H. Cui, eds.), pp. 105–124, Springer International Publishing, 2020.

[8] M. Huang, Z. Xu, and L. Wang, "On the Probability and Automatic Search of Rotational-XOR Cryptanalysis on ARX Ciphers," *Comput. J.*, vol. 65, pp. 3062–3080, 2021.

[9] W. Xin, Y. Liu, B. Sun, and C. Li, "Improved Cryptanalysis on SipHash," in *Cryptology and Network Security* (Y. Mu, R. H. Deng, and X. Huang, eds.), pp. 61–79, Springer International Publishing, 2019.

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

[11] H. Warren, *Hacker's Delight*. Always learning, Addison-Wesley, 2013.

[12] S. Yakovliev, "Cryptographic Properties of Operations Which Approximate Modular Addition," in *Information Technologies and Computer Modelling – ITCM'2022*, pp. 112–115, 2022. [in Ukrainian].

[13] J.-P. Aumasson, P. Jovanovic, and S. Neves, "Analysis of NORX: Investigating Differential and Rotational Properties," in *Progress in Cryptology – LATINCRYPT 2014* (D. F. Aranha and A. Menezes, eds.), pp. 306–324, Springer International Publishing, 2015.