UDC 004.056.53:512.6

Some Properties of RX-Differential Probabilities for an Operation that Approximates Modular Addition

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 RX-analysis for the NORX mixing operation, a logic-only surrogate for modular addition used in ARX/LRX designs. Given established closed-form RX-probability expressions and feasibility conditions, we characterize the distribution of RX-probabilities over random RX-differentials, provide a constructive algorithm that, for fixed input differences and rotation value, enumerates the admissible output differences and simultaneously yields their cardinality, together with a maximization method for identical-input cases.

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

Introduction

Cryptosystems of the ARX class (*Add–Rotation–XOR*) rely on a small set of elementary operations — addition modulo 2^n, bitwise exclusive-or (XOR), and cyclic rotations — and are therefore attractive for highly efficient, lightweight implementations on constrained platforms. In a number of modern designs, modular addition is reduced or replaced altogether by purely logical composition in order to further streamline hardware or constant-time software. We use the umbrella term *LRX* for such logic-centric patterns. Representative examples often discussed in this context include Simon [1], NORX [2], and Ascon [3].

Rotational cryptanalysis, introduced by D. Khovratovich and I. Nikolić [4, 5], studies the evolution of *rotational pairs* — inputs related by a fixed cyclic rotation — through ARX round functions. It is well understood that injecting round or key-dependent constants typically destroys rotational symmetry and thus defeats plain rotational distinguishers [4, 5]. To address this barrier, Ashur and Liu proposed *differential-rotational* cryptanalysis (RX-analysis) [6], which augments rotational pairs with XOR differentials. RX-differentials restore analytical traction in the presence of constants and enable nontrivial propagation analyses across modular addition. In particular, [6] derived a closed-form expression for RX-probabilities at a single-bit rotation ($r = 1$) for modular addition and demonstrated a 7-round RX-distinguisher on Speck32/64 [1]. Since then, RX-style analyses have been adapted to several families, including Simon/Simeck via AND-RX modeling [7], Alzette and CHAM [8], and SipHash [9]. More recently, exact probability formulas for modular addition at *all* rotations have been obtained [10], and RX-probabilities for both modular addition and certain logical surrogates have been further systematized [11].

This paper investigates the RX-differential properties of the logic-only operation that approximates modular addition, proposed by the designers of the NORX cipher [2]. The distribution of RX-probabilities over random RX-differentials is characterized. Building on the closed-form RX-probability formula and the feasibility criterion from [11], an efficient algorithm is presented that, for fixed inputs and rotation, enumerates all admissible output differences and, as a by-product, yields the cardinality of the admissible set. A maximization method tailored to identical-input cases is introduced, selecting outputs that attain the maximum RX-probability for a fixed rotation. Finally, several structured families of RX-differentials are analyzed, with

compact closed-form characterizations that clarify boundary cases.

1. Notation and Definitions

Throughout, we follow the notation and definitions of [11]:

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

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

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

$x[i]$ — the i-th bit of the vector $x \in V_n$ (thus $x[i] = x_i$);

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

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 $x \ggg r$ denotes a cyclic right rotation of x by r bits; note that $x^{-r} \equiv x^{n-r}$;

$x \ll r$ — a non-cyclic left shift of x by r bits:

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

$x \vee y$ — 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 (Hamming) weight of x (the number of ones);

$\mu_{n,r}$ — an n-bit vector having zeros at positions $i = 0$ and $i = r$ and ones elsewhere; it is given by $\mu_{n,r} = 2^n - 2^r - 2$.

$b_k(N,p)$ — the binomial probability mass function:

$$b_k(N,p) := \binom{N}{k} p^k (1-p)^{N-k}.$$

Consider the mapping $f\colon V_n \times V_n \to V_n$. The *differential* $\omega = (\alpha, \beta \to \gamma)$ *of* f is any triple of vectors $\alpha, \beta, \gamma \in V_n$ describing the differences between two input (or output) values of f with respect to $\oplus$.

The *probability of the differential* $\omega = (\alpha, \beta \to \gamma)$ *for* f is defined as

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

The concept of rotational-differential (RX) analysis was introduced in [6]. We denote an *RX-differential* by

$$\theta = (r;\, \alpha, \beta \to \gamma),$$

which arises by composing the rotation $(x,y) \mapsto (x^r, y^r)$ with the differential $(\alpha, \beta \to \gamma)$. The *probability of an RX-differential* of f is defined as

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

We refer to the ordinary differential $(\alpha, \beta \to \gamma)$ and the RX-differential $(r; \alpha, \beta \to \gamma)$ as *corresponding differentials*.

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

In [2], the designers of NORX proposed the operation

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

which approximates addition modulo 2^n. This approximation is based on the well-known identity relating modular addition and logical operations [12]:

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

where the addition on the right-hand side is replaced by XOR.

The following theorem states the closed-form expression for the RX-differential probabilities of the operation $h(x,y)$ as established in prior work.

Theorem 1 ([11])**.** *For any fixed rotation value* r, $1 \le r \le n-1$, *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) $xrp^h(r; \alpha, \beta \to \gamma) \ne 0$ *iff*

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

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

$$xrp^h(r; \alpha, \beta \to \gamma) = \\ = \left(\frac{3}{4} - \frac{\delta[0]}{2}\right)\left(\frac{3}{4} - \frac{\delta[r]}{2}\right) 2^{-k}; \quad (2)$$

where $k = wt(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r})$ *and* $\delta = \alpha \oplus \beta \oplus \gamma$.

2. RX-Differential Probability Distribution for the Function $h(x,y)$

We now examine uniformly random RX-differentials: how often the probability is nonzero and, when it is, how it is distributed. The following theorem states the result.

Theorem 2. *Let r, $1 \le r \le n-1$, be fixed. An RX-differential $\theta = (r;\, \alpha, \beta \to \gamma)$ is called* random *when $\alpha, \beta, \gamma \in V_n$ are chosen independently and uniformly at random. Then the following results hold:*

1) $\Pr_\theta\{\, xrp^h(\theta) \neq 0 \,\} \;=\; \left(\frac{7}{8}\right)^{n-2}$.

2) Denote

$$\Pr(a) = \Pr_\theta\left\{\, xrp^h(\theta) = a \;\middle|\; xrp^h(\theta) \neq 0 \,\right\}.$$

Then

$$\Pr\left(\tfrac{9}{16}2^{-k}\right) = \tfrac{1}{4} b_k\big(n-2, \tfrac{6}{7}\big)$$
$$\Pr\left(\tfrac{3}{16}2^{-k}\right) = \tfrac{1}{2} b_k\big(n-2, \tfrac{6}{7}\big)$$
$$\Pr\left(\tfrac{1}{16}2^{-k}\right) = \tfrac{1}{4} b_k\big(n-2, \tfrac{6}{7}\big)$$

where $k \in \{0,1,\ldots,n-2\}$.

Proof. According to (1), an RX-differential $xrp^h(\theta)$ has nonzero probability if and only if

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

For each index $i \neq 0$, $i \neq r$ the only forbidden conjunction is

$$\alpha_{i-1} = \beta_{i-1} = 0 \quad \text{and} \quad \delta_i = 1.$$

Since

$$\Pr\{\alpha_{i-1} = \beta_{i-1} = 0\} = \tfrac{1}{4},\ \Pr\{\delta_i = 1\} = \tfrac{1}{2},$$

and δ_i depends only on $(\alpha_i, \beta_i, \gamma_i)$ (hence is independent of $\alpha_{i-1}, \beta_{i-1}$), the per-position acceptance probability equals $1 - \frac{1}{4}\cdot\frac{1}{2} = \frac{7}{8}$. Independence across the $n-2$ non-edge positions then yields

$$\Pr_\theta\{\, xrp^h(\theta) \neq 0 \,\} = \left(\tfrac{7}{8}\right)^{n-2}.$$

Assume that $xrp^h(\theta) \neq 0$. Then, by (2), we have $xrp^h(\theta) = s \cdot 2^{-k}$, where $k \in \{0, 1, \ldots, n-2\}$. The factor s depends only on $\delta[0]$ and $\delta[r]$ and takes values from $\{\frac{9}{16}, \frac{3}{16}, \frac{1}{16}\}$ with corresponding probabilities $\{\frac{1}{4}, \frac{1}{4}, \frac{1}{2}\}$, independently of k.

For every index $i \neq 0$, $i \neq r$, define the event A_i by $\alpha_{i-1} \vee \beta_{i-1} = 1$. By the proof of Theorem 1 (see [11]), for each index i where the condition A_i holds, the probability $xrp^h(\theta)$ acquires an additional multiplicative factor of $1/2$. Consequently, the overall factor contributed by the positions $i \neq 0$, $i \neq r$ equals 2^{-k}, where k is the number of successful events A_i.

Let E denote the event that $xrp^h(\theta) \neq 0$. We now evaluate the conditional probability $\Pr\{A_i \mid E\}$. Since this probability depends only on the triple $(\alpha_{i-1}, \beta_{i-1}, \gamma_{i-1})$, there are $2^3 = 8$ possible assignments. Exactly one of them is ruled out by E; among the remaining seven, six satisfy A_i. Therefore,

$$\Pr\{A_i \mid E\} = \tfrac{6}{7}.$$

The events A_i are pairwise independent (each depends on different bits of α and β) and are identically distributed with $\Pr\{A_i \mid E\} = \frac{6}{7}$. Hence, across the indices $i \notin \{0, r\}$ we obtain a sequence of independent Bernoulli trials. Therefore, the probability that there are exactly k successful events (which yields the overall factor 2^{-k}) is given by the binomial law $b_k(n-2, \frac{6}{7})$.

Combining the two parts, we obtain the claimed distribution:

$$\Pr\left(\tfrac{9}{16}\, 2^{-k}\right) = \tfrac{1}{4}\, b_k\big(n-2, \tfrac{6}{7}\big)\,,$$
$$\Pr\left(\tfrac{3}{16}\, 2^{-k}\right) = \tfrac{1}{2}\, b_k\big(n-2, \tfrac{6}{7}\big)\,,$$
$$\Pr\left(\tfrac{1}{16}\, 2^{-k}\right) = \tfrac{1}{4}\, b_k\big(n-2, \tfrac{6}{7}\big)\,,$$

which concludes the proof. □

As the word size n grows, the share of triples $(r; \alpha, \beta \to \gamma)$ with nonzero RX-probability falls like $\frac{7}{8}^{n-2}$. Such triples still exist for every n, but they are rare. Given the probability is nonzero, it has the form $s\, 2^{-k}$. Here $k \in \{0, \ldots, n-2\}$ follows the binomial distribution $b_k(n-2, \frac{6}{7})$, and $s \in \{\frac{9}{16}, \frac{3}{16}, \frac{1}{16}\}$ with probabilities $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$. In typical cases, the nonzero RX-probability is about $2^{-\frac{6}{7}(n-2)}$, so large probabilities are rare.

3. Searching for Nonzero-Probability RX-Differentials of the Function $h(x,y)$

By equation (1), an RX–differential $xrp^h(r; \alpha, \beta \to \gamma)$ is feasible iff

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

The algorithm below lists exactly all γ satisfying this constraint: it leaves the positions 0 and

r unconstrained, and for each $i \notin \{0, r\}$ fixes $\gamma[i] = \alpha[i] \oplus \beta[i]$ whenever $\alpha[i-1] \vee \beta[i-1] = 0$; otherwise $\gamma[i]$ may be chosen freely (all indices modulo n).

Algorithm 1 (Enumerating all vectors $\boldsymbol{\gamma}$ with $\boldsymbol{xrp^h(r; \alpha, \beta \to \gamma) \neq 0}$).
Input: $\alpha, \beta \in V_n$, $r \in \mathbb{Z}$ *with* $1 \leq r \leq n-1$.
Output: *the set of vectors* $\gamma \in V_n$.

1) *For all* $i > 0$, *set* $A[i] = \alpha[i-1] \vee \beta[i-1]$.
2) *Initialize the bits singled out by condition* (1)*:*
$$\gamma[0] \leftarrow \{0,1\}, \qquad \gamma[r] \leftarrow \{0,1\}.$$
3) *For each* $i \in \{1, \ldots, n-1\} \setminus \{r\}$ *set*
   (i) *If* $A[i] = 1$, *then* $\gamma[i] \in \{0,1\}$ *(free choice);*
   (ii) *If* $A[i] = 0$, *then* $\gamma[i] \leftarrow \alpha[i] \oplus \beta[i]$.

Claim 1. *For the fixed inputs* $\alpha, \beta \in V_n$ *and rotation* r, *algorithm* (1) *correctly enumerates the set of all output differences* γ *for which* $xrp^h(\theta) \neq 0$.

Proof. By equation (1), $xrp^h(\theta)$ is nonzero exactly when
$$\overline{((\alpha \vee \beta) \ll 1)} \wedge \delta \wedge \mu_{n,r} = 0,$$
where $\delta = \alpha \oplus \beta \oplus \gamma$ and $A[i] = \alpha[i-1] \vee \beta[i-1]$. The mask $\mu_{n,r}$ has $\mu_{n,r}[0] = \mu_{n,r}[r] = 0$ and $\mu_{n,r}[i] = 1$ for all other positions.

At positions 0 and r the mask is 0, so the condition holds regardless of $\gamma[0]$ and $\gamma[r]$; the algorithm therefore leaves these two bits free. For any other index i, we must satisfy $\overline{A}[i] \wedge \delta[i] = 0$. If $A[i] = 0$, then $\delta[i] = 0$, i.e., $\gamma[i] = \alpha[i] \oplus \beta[i]$. If $A[i] = 1$, there is no restriction on $\gamma[i]$. This is exactly what the algorithm enforces, so every output γ satisfies equation (1).

Conversely, take any γ that satisfies equation (1). For each $i \notin \{0, r\}$ with $A[i] = 0$ it must hold that $\gamma[i] = \alpha[i] \oplus \beta[i]$, and for $i \in \{0, r\}$ or $A[i] = 1$ the bit $\gamma[i]$ may be chosen freely. The algorithm enumerates exactly these choices, so every feasible γ appears in its output.

Therefore Algorithm 1 correctly lists precisely all γ with $xrp^h(\theta) \neq 0$. □

Corollary 1. *The cardinality of the set of vectors* $\gamma \in V_n$ *for which the RX-probability of the differential* $(r;\, \alpha, \beta \to \gamma)$ *is nonzero equals*
$$\big|\{\gamma :\, xrp^h(r; \alpha, \beta \to \gamma) \neq 0\}\big| = \\ = 4 \cdot 2^{wt\left(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r}\right)}.$$

Proof. By equation (1) and Algorithm 1, the bits $\gamma[0]$ and $\gamma[r]$ are unconstrained, contributing a factor $2^2 = 4$.

For every other index $i \neq 0, i \neq r$, the bit $\gamma[i]$ is free exactly when $((\alpha \vee \beta) \ll 1)[i] = 1$ and $\mu_{n,r}[i] = 1$; otherwise $\gamma[i]$ is forced to $\alpha[i] \oplus \beta[i]$. The number of free positions among $i \notin \{0, r\}$ is therefore
$$wt(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r}),$$
and each such position contributes a factor 2. Multiplying the independent choices gives
$$\big|\{\gamma :\, xrp^h(r; \alpha, \beta \to \gamma) \neq 0\}\big| = \\ = 4 \cdot 2^{wt\left(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r}\right)}.$$
Thus we obtain the claimed count. □

Note that in view of the closed-form expression for xrp, it is natural to focus the search for maximum-probability RX-differentials on the subclass of vectors satisfying
$$\delta[0] = \delta[r] = 0, \qquad \delta = \alpha \oplus \beta \oplus \gamma.$$
Under this condition, the multiplicative factor in (2) attains its largest possible value $9/16$, thereby maximizing the RX-differential probability.

To describe the set of vectors γ for which the RX-differential $(r; \alpha, \beta \to \gamma)$ has nonzero probability and the factor in (2) equals $9/16$, it suffices to replace Step 2 of Algorithm 1 with
$$\gamma[0] \leftarrow \alpha[0] \oplus \beta[0], \qquad \gamma[r] \leftarrow \alpha[r] \oplus \beta[r].$$

4. Analysis of Special Forms of RX-Differentials

Below we study three structured families of RX-differentials with clean, closed-form descriptions that are useful for automated search: $(r; \alpha, \alpha \to \alpha)$, $(r; \alpha, \alpha \to \gamma)$ and $(r; \alpha, \beta \to \alpha \oplus \beta)$.

4.1. RX-differentials with identical arguments ($\alpha = \beta = \gamma$)

We apply Theorem 1 to identify RX-differentials of the form $(r, \alpha, \alpha \to \alpha)$ with nonzero probability. The RX-differential has nonzero probability precisely when the following condition holds:
$$\overline{(\alpha \ll 1)} \wedge \alpha \wedge \mu_{n,r} = 0.$$

Accordingly, the set of admissible vectors α is defined by the following condition

$$\mathcal{A}_{n,r} = \Big\{ \alpha \in V_n \;\Big|\; \overline{(\alpha \ll 1)} \wedge \alpha \wedge \mu_{n,r} = 0 \Big\}.$$

Denote

$$\mathcal{M} = \Big\{ (s,t) \in \mathbb{Z}^2 \;\Big|\; \begin{matrix} 0 \le s \le r, \\ 1 \le t \le n-r \end{matrix} \Big\}.$$

Lemma 1. *For any n and any rotation value r with $1 \le r \le n-1$, the set $\mathcal{A}_{n,r}$ equals*

$$\mathcal{A}_{n,r} = \Big\{ \big(2^s{-}1\big) + \big(\big(2^t{-}1\big) \ll r\big) \;\Big|\; (s,t) \in \mathcal{M} \Big\}.$$

Proof. According to (1), for every i with $1 \le i \le n-1$ and $i \ne r$, the pattern

$$\overline{\alpha[i-1]} \wedge \alpha[i] = 1$$

is forbidden; that is, a one cannot immediately follow a zero unless $i = r$. Consequently, the only permitted starting positions of runs of consecutive ones are 0 and r.

Partition $\mathcal{A}_{n,r}$ by the values of $\alpha[0]$ and $\alpha[r]$. For $\varepsilon, \delta \in \{0,1\}$ define

$$\mathcal{A}_{n,r}^{(\varepsilon,\delta)} = \{\alpha \in \mathcal{A}_{n,r} \mid \alpha[r] = \varepsilon,\ \alpha[0] = \delta\}.$$

Then $\mathcal{A}_{n,r} = \mathcal{A}_{n,r}^{(0,0)} \cup \mathcal{A}_{n,r}^{(0,1)} \cup \mathcal{A}_{n,r}^{(1,0)} \cup \mathcal{A}_{n,r}^{(1,1)}$, And these subsets are pairwise disjoint.

We describe each subset in turn:

1) $\alpha[0] = 0$, $\alpha[r] = 0$. No run of ones appears, hence $\mathcal{A}_{n,r}^{(0,0)}$ contains only the all-zero vector.
2) $\alpha[0] = 1$, $\alpha[r] = 0$. A single run $1 \ldots 1$ starts at position 0 and ends at one of the positions $1, \ldots, r-1$. Thus
$$\alpha \;=\; 2^k - 1, \qquad 0 < k \le r.$$
3) $\alpha[0] = 0$, $\alpha[r] = 1$. Here a run of ones starts at position r and ends at one of the positions $r+1, \ldots, n-1$, i.e., it has length t with $0 < t \le n-r$:
$$\alpha \;=\; \big(2^t - 1\big) \ll r, \qquad 0 < t \le n-r.$$
4) $\alpha[0] = 1$, $\alpha[r] = 1$. This yields two runs of ones, the first starting at position 0 and the second at position r:
$$\alpha \;=\; \big(2^k - 1\big) \;+\; \big(\big(2^t - 1\big) \ll r\big),$$
where $0 < k < r$ and $0 < t \le n-r$.

These cases can be unified as

$$\mathcal{A}_{n,r} = \Big\{ \big(2^s{-}1\big) + \big(\big(2^t{-}1\big) \ll r\big) \;\Big|\; (s,t) \in \mathcal{M} \Big\},$$

as claimed. □

Corollary 2. *For any fixed r, the number of vectors $\alpha \in V_n$ satisfying $\overline{(\alpha \ll 1)} \wedge \alpha \wedge \mu_{n,r} = 0$ equals*

$$|\mathcal{A}_{n,r}| = (r+1)(n-r+1).$$

Proof. With the notation from the proof of Lemma 1, we have

$$\begin{aligned} |\mathcal{A}_{n,r}| &= |\mathcal{A}_{n,r}^{(0,0)}| + |\mathcal{A}_{n,r}^{(0,1)}| + |\mathcal{A}_{n,r}^{(1,0)}| + |\mathcal{A}_{n,r}^{(1,1)}| = \\ &= 1 + (n-r) + r + (n-r)r = \\ &= n + 1 + nr - r^2 = \\ &= n(r+1) - (r^2 - 1) = \\ &= (r+1)(n-r+1), \end{aligned}$$

as required. □

4.2. RX-differentials with identical input differences

Consider RX-differentials of the form $(r;\, \alpha, \alpha \to \gamma)$. We focus on those with the largest multiplicative factor in (2). Accordingly, we restrict to differentials satisfying

$$\delta[0] = 0, \qquad \delta[r] = 0, \qquad \delta = \gamma.$$

The set of admissible output vectors for this RX-differential with $\gamma[0] = \gamma[r] = 0$ is

$$\mathcal{B}_{n,r}(\alpha) = \Big\{ \gamma \in V_n \;\Big|\; \overline{(\alpha \ll 1)} \wedge \gamma \wedge \mu_{n,r} = 0 \Big\}.$$

Lemma 2. *For any fixed r and any $\alpha \in V_n$, the number of vectors γ satisfying $\overline{(\alpha \ll 1)} \wedge \gamma \wedge \mu_{n,r} = 0$ with $\gamma[0] = \gamma[r] = 0$ equals*

$$|\mathcal{B}_{n,r}(\alpha)| \;=\; 2^{\,wt(\alpha \ll 1) \,-\, \alpha[r-1]}.$$

Proof. Coordinates 0 and r are fixed by $\gamma[0] = \gamma[r] = 0$. For all other positions, $\overline{(\alpha \ll 1)} \wedge \gamma = 0$, i.e.,

$$\gamma[i] = \begin{cases} 0, & \text{if } (\alpha \ll 1)[i] = 0, \\ 0 \text{ or } 1, & \text{if } (\alpha \ll 1)[i] = 1. \end{cases}$$

Thus the free bits of γ occur exactly where $i \ne 0, i \ne 1$ and $(\alpha \ll 1)[i] = 1$. Their number therefore is

$$wt(\alpha \ll 1) - \alpha[r-1]$$

since $(\alpha \ll 1)[0] = 0$ and $(\alpha \ll 1)[r] = \alpha[r-1]$. Each free bit is chosen independently, giving

$$|\mathcal{B}_{n,r}(\alpha)| = 2^{\,wt(\alpha \ll 1) - \alpha[r-1]}.$$

This completes the proof. □

Algorithm 2 (Finding γ that maximize the probability of $(r;\, \alpha, \alpha \to \gamma)$).
Input: *$\alpha \in V_n$, fixed rotation r with $1 \le r \le n-1$.*
Output: *the set $\mathcal{B}_{n,r}(\alpha)$.*

1) Fix the bits to maximize the factor in (2)*:*

$$\gamma[0] \leftarrow 0, \qquad \gamma[r] \leftarrow 0.$$

2) For each $i \in \{1, \dots, n-1\} \setminus \{r\}$ do
   (i) *If $\alpha[i-1] = 1$, set $\gamma[i] \in \{0,1\}$ (free choice);*
   (ii) *if $\alpha[i-1] = 0$, set $\gamma[i] \leftarrow 0$.*

It follows that the cardinality of $\mathcal{B}_{n,r}(\alpha)$, describing all possible output differences of RX-differentials of the form $(r; \alpha, \alpha \to \gamma)$ under $\gamma[0] = \gamma[r] = 0$. The algorithm enumerates the entire set $\mathcal{B}_{n,r}(\alpha)$ in total time $O\big(n\, 2^k\big)$, where

$$k = wt(\alpha \lll 1) - \alpha[r-1],$$

i.e., 2^k vectors with $O(n)$ work per vector. This yields a provably minimal exhaustive search and enables exact RX-probability evaluation, substantially narrowing the search space in the analysis of ARX- and LRX-constructions.

4.3. RX-differentials of the form $(r;\, \alpha, \beta \to \alpha \oplus \beta)$

We now determine the RX-differential probabilities of $h(x,y)$ for differentials $(r; \alpha, \beta \to \alpha \oplus \beta)$. From Theorem 1, the RX-differential $(r; \alpha, \beta \to \gamma)$ has nonzero probability precisely when

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

Here $\delta = \alpha \oplus \beta \oplus (\alpha \oplus \beta) = 0$, so the condition is satisfied trivially and every such RX-differential has nonzero probability given by

$$xrp^h(r; \alpha, \beta \to \alpha \oplus \beta) = \tfrac{9}{16}\, 2^{-k},$$

where $k = wt\big(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r}\big)$. The maximum probability is reached when $k = 0$.

Lemma 3. *For fixed r with $1 \le r \le n-1$, there are exactly 16 distinct pairs $(\alpha, \beta) \in V_n^2$ that achieve the maximal RX-probability $9/16$ for the differential $(r;\, \alpha, \beta \to \alpha \oplus \beta)$.*

Proof. Since $\delta = 0$, the prefactor in (2) equals $(3/4) \cdot (3/4) = 9/16$. Maximization thus requires $wt\big(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r}\big) = 0$, where $\mu_{n,r}$ has zeros at positions 0 and r (and ones elsewhere). Equivalently, $((\alpha \vee \beta) \ll 1)[i] = 0$ for all $i \notin \{0, r\}$. Because the shift is non-cyclic, this forces $\alpha \vee \beta$ to be zero at every position except possibly $n-1$ (which is discarded by the shift) and $r-1$ (which shifts into position r). Hence α and β may independently choose bits at positions $n-1$ and $r-1$, and must be zero elsewhere, giving $2^4 = 16$ admissible pairs. □

All differentials in this class are captured by the template

$$\alpha, \beta \in \{\, \star, 0, \dots, 0, \star, 0, \dots, 0 \,\},$$

where $\star \in \{0,1\}$ occupies positions $n-1$ and $r-1$. These results provide tight upper bounds on the computational complexity of RX-based attacks and a complete description of the extremal pairs (α, β) attaining the maximal RX-probability. This, in turn, supplies the foundation for formal RX-differential analyses of ARX- and LRX-cryptosystems and for optimizing associated automated search procedures.

Conclusions

This work examined the RX-differential behavior of the NORX mixing operation used as a logical surrogate for modular addition. The main outcomes are both statistical and algorithmic.

On the statistical side, the distribution of RX-probabilities over random RX-differentials was characterized: the share of feasible triples equals $\left(\frac{7}{8}\right)^{n-2}$, and conditioned on feasibility the probability takes values $s \cdot 2^{-k}$ with binomial distribution probabilities $b_k(n-2, \frac{6}{7})$ and weights $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$ in correspondence with the respective values of $s \in \frac{9}{16}, \frac{3}{16}, \frac{1}{16}$. Thus, feasible RX-differentials become exponentially rare as n grows, and large probabilities are outliers.

On the algorithmic side, the feasibility condition leads to a constructive enumeration routine that, for fixed inputs and rotation, outputs exactly the set of admissible output differences and, as a by-product, yields its cardinality $4 \cdot 2^{\,wt(((\alpha \vee \beta) \ll 1) \wedge \mu_{n,r})}$. A maximization procedure tailored to identical-input cases selects outputs attaining the maximum RX-probability for a fixed rotation. Several structured families were analyzed in closed form, including $(r; \alpha, \alpha \to \alpha)$ with $|\mathcal{A}_{n,r}| = (r+1)(n-r+1)$, $(r; \alpha, \alpha \to \gamma)$ with $|\mathcal{B}_{n,r}(\alpha)| = 2^{\,wt(\alpha \lll 1) - \alpha[r-1]}$, and $(r; \alpha, \beta \to \alpha \oplus \beta)$ where the maximum $\frac{9}{16}$ is achieved by exactly 16 input pairs.

These results enable principled pruning in RX-based trail search for LRX/ARX designs that replace modular addition with logical operations: enumeration avoids brute-force over 2^n outputs, while the distributional picture highlights the scarcity of large-probability events and pinpoints the corner cases where they occur.

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

[2] J.-P. Aumasson, P. Jovanovic, and S. Neves, "NORX V3.0: Submission to the CAESAR Competition," 2015. URL: 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. DOI: 10.1007/s00145-021-09398-9.

[4] D. Khovratovich and I. Nikolić, "Rotational Cryptanalysis of ARX," in *Fast Software Encryption*, pp. 333–346, Springer Berlin Heidelberg, 2010. DOI: 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. URL: 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, pp. 57–70, Dec. 2016. DOI: 10.13154/tosc.v2016.i1.57-70.

[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] A. Biryukov, B. Lambin, and A. Udovenko, "Exact formula for rx-differential probability through modular addition for all rotations," *IACR Transactions on Symmetric Cryptology*, vol. 2025, p. 542–591, Mar. 2025. DOI: 10.46586/tosc.v2025.i1.542-591.

[11] S. Yakovliev and N. Korzh, "Differential-Rotational Probabilities of Modular Addition and Its Approximations," *Theoretical and Applied Cyber Security*, vol. 6, no. 2, pp. 5–15, 2024. DOI: 10.20535/tacs.2664-29132024.2.318611.

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