CYBERNETICS and COMPUTER TECHNOLOGIES

УДК 004.056.55:512.6 DOI:10.34229/2707-451X.25.3.9

S. YAKOVLIEV

SOME ALGEBRAIC PROPERTIES OF RX-DIFFERENTIAL PROBABILITIES OF BOOLEAN MAPPINGS

Analytical expressions were obtained for the transformation of RX-differential probabilities for Boolean mappings under linear shifts of inputs and outputs. This made it possible to demonstrate the relationships between the security parameters against differential and rotational cryptanalysis for special classes of ARX-mappings.

Keywords: *symmetric cryptography, ARX-cryptosystems, differential cryptanalysis, rotational cryptanalysis, RX-analysis.*

Introduction. ARX-cryptosystems are based on a set of extremely simple operations available at the level of computing processor instructions, such as modular addition, bitwise addition, cyclic shifts, etc. LRX-cryptosystems use non-linear logic operations, such as logical AND, instead of modular addition to improve implementation efficiency. Due to their simple implementation and ultra-high speed, ARX and LRX cryptosystems have become an important part of so-called lightweight cryptography – a field dedicated to the development of reliable algorithms for low-resource devices and the Internet of Things.

The development of methods for the differential cryptanalysis of ARX-cryptosystems began with the work [1], in which analytical, computationally efficient expressions for the probabilities of modular addition differentials were obtained for the first time. The algebraic structure of ARX systems gave rise a specific type of cryptanalysis known as rotational cryptanalysis [2, 3], which examines the behaviour of pairs of texts that differ in cyclic shift during computations. Finally, a combined attacking method for ARX-systems was proposed in [4]: differential-rotational cryptanalysis (RX-analysis).

This paper considers the algebraic properties of the probabilities of RX-differentials of Boolean functions, focusing on transformations during linear shifts of inputs and outputs. These properties simplify the analysis of ARX-cryptosystems by providing analytical expressions for the differential and rotation pair probabilities, derived from the corresponding RX-differential expressions.

The results presented in this paper were first reported at the XIII International Scientific and Practical Conference “Glushkov Readings. Modern Cybernetics 2024” (December 6, 2024, Kyiv, Ukraine).

Required terms and definitions. Let $V_n = \{0,1\}^n$. Each element $x \in V_n$ is considered as a binary vector $x = (x_{n-1}, x_{n-2}, \dots, x_1, x_0)$, $x_i \in \{0,1\}$, and as a binary representation of a certain non-negative integer from the interval 0 до $2^n - 1$. The symbol 0 denotes the zero vector (equivalent to the number 0).

We use the standard notation for logic operation: & for logical AND, ∨ for logical OR and $\oplus$ for bitwise addition (XOR); all of these operations are applied to vectors bitwise. The symbol + denotes addition modulo 2^n. The inversion of all the bits in the vector x (logical NOT) is denoted by either $\overline{x}$ or $\neg x$.

The symbols $\lll$ and $\ggg$ denote cyclic shifts (rotations) of vectors. For a vector $x \in V_n$, denote its rotation by r positions to the left as

$$x^r = x \lll r = (x_{n-r-1}, x_{n-r-2}, \dots, x_1, x_0, x_{n-1}, x_{n-2}, \dots, x_{n-r}).$$

Note that the following relationships are valid in the introduced notation: $x^{-r} = x \ggg r \equiv x^{n-r}$ and $x^n = x$.

Consider an arbitrary Boolean binary mapping $f: V_n \times V_n \to V_n$. This paper will focus on ARX- and LRX-mappings, i.e., mappings constructed as compositions of additions modulo 2^n, bitwise additions, cyclic and non-cyclic shifts and logic operations (AND, OR, etc.).

The *differential* of the mapping f is an arbitrary triple of vectors $(\alpha, \beta \to \gamma)$, where $\alpha, \beta, \gamma \in V_n$, which are interpreted as differences (with respect to the bitwise addition operation $\oplus$) between pairs of input and output values of the mapping f [1]. The *probability of the differential* $(\alpha, \beta \to \gamma)$ of the mapping f is defined as

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

The *rotation pair* (by *r* positions) is a pair of vectors (x, x^r), where $r \in \mathbb{Z}$, $0 \le r < n$, and $x \in V_n$ can be any vector [2]. If we consider a system of two vectors (x, y), the rotation pair is treated as $\big((x, y), (x^r, y^r)\big)$; similarly, rotation pairs are defined for larger tuples of vectors. The *probability of a rotation pair* passing through the mapping f is defined as

$$rp^f(r) = \Pr_{x,y}\Big\{f(x^r, y^r) = \big(f(x, y)\big)^r\Big\}.$$

The *generalized differential*, or the *RX-differential*, of the mapping f is a tuple $(r; \alpha, \beta \to \gamma)$ that combines rotation pairs and differentials [4]. The *probability of the RX-differential* $(r; \alpha, \beta \to \gamma)$ of the mapping f is defined as

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

The probabilities xdp^f, rp^f and xrp^f are the security parameters of the mapping f against differential, rotational and differential-rotational cryptanalyses, respectively. The complexity of each attack is inversely proportional to the maximum value of the corresponding probability.

Note that $rp^f(r) = xrp^f(r; 0,0 \to 0)$, meaning that rp^f can be considered a special case of xrp^f. Similarly, xdp^f can be considered a special case of xrp^f when $r = 0$.

Main results. This paper considers how linear shifts in inputs and outputs affect the RX-differential probabilities (and, as special cases, the differential and rotational probabilities). In many cases, linear shifts can be interpreted as the addition of constants or round keys, and they are often used as a mechanism to strengthen security of ARX-cryptosystems against rotational cryptanalysis.

The following theorem and its corollaries describe how the xrp probabilities change under linear shifts at the input and/or output of an arbitrary binary Boolean mapping.

Theorem 1. Suppose that $f: V_n \times V_n \to V_n$ is an arbitrary mapping and that $\Delta_x, \Delta_y, \Delta \in V_n$ are arbitrary vectors. Define a mapping $g(x, y)$ as

$$g(x, y) := f\big(x \oplus \Delta_x, y \oplus \Delta_y\big) \oplus \Delta.$$

Then, for all $\alpha, \beta, \gamma \in V_n$ and $r \in \mathbb{Z}_n$, the following relation holds true:

$$xrp^g(r; \alpha, \beta \to \gamma) = xrp^f\big(r; \alpha \oplus \Delta_x \oplus \Delta_x^r, \beta \oplus \Delta_y \oplus \Delta_y^r \to \gamma \oplus \Delta \oplus \Delta^r\big).$$

Proof. According to the definition of the probability xrp, we have:

$$xrp^g(r;\alpha,\beta\to\gamma)=\Pr_{x,y}\Big\{g(x^r\oplus\alpha,y^r\oplus\beta)=\big(g(x,y)\big)^r\oplus\gamma\Big\}=$$
$$=\Pr_{x,y}\Big\{f\big(x^r\oplus\alpha\oplus\Delta_x,y^r\oplus\beta\oplus\Delta_y\big)\oplus\Delta=\big(f\big(x\oplus\Delta_x,y\oplus\Delta_y\big)\oplus\Delta\big)^r\oplus\gamma\Big\}.$$

Introduce the substitutions $u:=x\oplus\Delta_x$ and $v:=y\oplus\Delta_y$; then $u^r:=x^r\oplus\Delta_x^r$, $v^r:=y^r\oplus\Delta_y^r$ and, correspondingly,

$$xrp^g(r;\alpha,\beta\to\gamma)=$$
$$=\Pr_{u,v}\Big\{f\big(u^r\oplus\alpha\oplus\Delta_x\oplus\Delta_x^r,v^r\oplus\beta\oplus\Delta_y\oplus\Delta_y^r\big)=\big(f(u,v)\big)^r\oplus\gamma\oplus\Delta\oplus\Delta^r\Big\}=$$
$$=xrp^f\big(r;\alpha\oplus\Delta_x\oplus\Delta_x^r,\beta\oplus\Delta_y\oplus\Delta_y^r\to\gamma\oplus\Delta\oplus\Delta^r\big),$$

which concludes the proof. □

Corollary 1. In the notation of Theorem 1, the following relations hold:

$$xdp^g(\alpha,\beta\to\gamma)=xdp^f(\alpha,\beta\to\gamma),$$
$$rp^g(r)=xrp^f\big(r;\Delta_x\oplus\Delta_x^r,\Delta_y\oplus\Delta_y^r\to\Delta\oplus\Delta^r\big).$$

Proof. The given statements follow from Theorem 1 for the edge values of $r=0$ (for xdp) and $a=b=c=0$ (for rp). In fact, when $r=0$ we have $a\oplus a^r=a\oplus a=0$ for any vector a. This implies that

$$xdp^g(\alpha,\beta\to\gamma)=xrp^g(0;\alpha,\beta\to\gamma)=xrp^f(0;\alpha,\beta\to\gamma)=xdp^f(\alpha,\beta\to\gamma).$$

Similarly, we have

$$rp^g(r)=xrp^g(r;0,0\to0)=xrp^f\big(r;\Delta_x\oplus\Delta_x^r,\Delta_y\oplus\Delta_y^r\to\Delta\oplus\Delta^r\big),$$

which concludes the proof. □

Corollary 2. Let $f\colon V_n\times V_n\to V_n$ be an arbitrary mapping. If a mapping g is described by one of the following forms:

1) $g(x,y)=f(\overline{x},\overline{y})$,
2) $g(x,y)=\neg f(x,y)$,
3) $g(x,y)=f^*(x,y)=\neg f(\overline{x},\overline{y})$ – the dual function of f,

then, for all $\alpha,\beta,\gamma\in V_n$ and $r\in\mathbb{Z}_n$, the following relations hold:

$$xdp^g(\alpha,\beta\to\gamma)=xdp^f(\alpha,\beta\to\gamma),$$
$$rp^g(r)=rp^f(r),$$
$$xrp^g(r;\alpha,\beta\to\gamma)=xrp^f(r;\alpha,\beta\to\gamma).$$

Proof. Let us use the fact that $\overline{x}=x\oplus11\ldots1$. For a vector $\Delta=11\ldots1$ we have $\Delta^r=\Delta$, or, in other words, $\Delta\oplus\Delta^r=0$. Accordingly, the statements of this corollary are obtained from Theorem 1 and Corollary 1 by substituting the following values:

1) for $g(x,y)=f(\overline{x},\overline{y})$: $\Delta_x=\Delta_y=11\ldots1$, $\Delta=0$;
2) for $g(x,y)=\neg f(x,y)$: $\Delta_x=\Delta_y=0$, $\Delta=11\ldots1$;
3) for $g(x,y)=\neg f(\overline{x},\overline{y})$: $\Delta_x=\Delta_y=\Delta=11\ldots1$;

which confirms the statement. □

Note that the statements of Theorem 1 (and Corollaries 1 and 2) are valid not only for mappings with two input arguments, but also for mappings with any number of arguments. In the latter case, however, the structure of differentials and rotation pairs requires clarification. For example, if $f:V_n\to V_n$ is an arbitrary mapping of one argument and $g(x)=f(x\oplus\Delta_x)\oplus\Delta$, then the following relations hold:

$$xrp^g(r;\alpha\to\beta)=xrp^f(r;\alpha\oplus\Delta_x\oplus\Delta_x^r\to\beta\oplus\Delta\oplus\Delta^r).$$
$$xdp^g(\alpha\to\beta)=xdp^f(\alpha\to\beta),$$
$$rp^g(r)=xrp^f(r;\Delta_x\oplus\Delta_x^r\to\Delta\oplus\Delta^r).$$

The equality of the xdp probabilities under linear shifts and inversion of the inputs and/or outputs was demonstrated in [5].

Application of the obtained results. Consider the modular addition function, the primary non-linear transformation in ARX-cryptosystems: $f(x,y) = (x+y) \ mod \ 2^n$. The cryptographic properties of modular addition have been studied extensively; in particular, [6, 7] provide exact formulas for the RX-differential probabilities of modular addition.

The following statement describes the dual function of modular addition.

Proposition 1. The dual function of $f(x,y) = (x+y) \ mod \ 2^n$ is a mapping

$$f^*(x,y) = (x+y+1) \ mod \ 2^n.$$

Proof. Let us use the well-known fact that

$$\overline{x} \equiv 2^n - 1 - x \ (mod \ 2^n).$$

Therefore,

$$f^*(x,y) = \neg f(\overline{x},\overline{y}) = \neg(\overline{x}+\overline{y}) \equiv$$
$$\equiv 2^n - 1 - (2^n - 1 - x + 2^n - 1 - y) = x + y + 1 - 2^n \equiv x + y + 1 \ (mod \ 2^n),$$

which concludes the proof. □

According to Corollary 2, f and f^* have identical distributions of differential probabilities, as well as rotation pair probabilities. This result is somewhat counterintuitive since adding constants in ARX-transformations is a common tool for increasing security against rotational cryptanalysis [3]. Indeed, for the function $h(x) = x \oplus c$, the equality $h(x^r) = \big(h(x)\big)^r$ holds if and only if $c = c^r$. If the constant c is chosen such that $c \neq c^r$ for all r, then such a transformation will significantly complicate the passage of the rotation pair (if not make it impossible altogether). Clearly, the constant $c = 1$ satisfies this property. Adding the constant by more complex modular addition rather than bitwise addition should further enhance these effects. However, when adding two arguments, adding the constant 1 does not alter the probability distributions of RX-differentials and rotation pairs and therefore does not increase security against rotational cryptanalysis. Similarly, we can consider the sums of a larger number of arguments: for $x+y+z$, the dual function is $x+y+z+2$, for $x+y+z+t$ is, respectively, $x+y+z+t+3$, and so on. Therefore, the mere presence of constant addition does not guarantee protection against rotational cryptanalysis in itself, and the corresponding security evaluation must be obtained through careful analysis.

Let $f(x,y)$ be a *rotation-invariant mapping*, i.e. $f(x^r,y^r) = \big(f(x,y)\big)^r$ for arbitrary x,y. Examples of such mappings include bitwise operations, such as & or ∨, as well as arbitrary combinations of these with rotations of the arguments. Two transformations widely used in LRX cryptosystems are also rotation-invariant mappings: Daemen's S-box, which is used in the SHA-3 hash function [8] and the Ascon cipher [9]:

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

and the internal non-linear function of the Simon cipher [10]:

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

For rotation-invariant mappings, RX-analysis is equivalent to standard differential cryptanalysis, and rotational cryptanalysis does not yield meaningful results. The following statement formalizes these well-known observations.

Proposition 2. For a rotation-invariant mapping $f(x,y)$ and arbitrary $\alpha,\beta,\gamma \in V_n$, $r \in \mathbb{Z}_n$, the following relations hold:

$$xrp^f(r;\ \alpha,\beta \to \gamma) = xdp^f(\alpha^{-r},\beta^{-r} \to \gamma^{-r}), \qquad rp^f(r) = 1.$$

Proof. According to the definitions of xrp probabilities and rotation-invariant mappings, we have

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

The equality $rp^f(r)=1$ follows directly from the definitions of rp probabilities and rotation-invariant mappings. Therefore, the statement is proven. □

Consider the mapping $g(x,y):=f\left(x\oplus\Delta_x,y\oplus\Delta_y\right)\oplus\Delta$, which, in general, is not rotation-invariant. The following statement holds true for mappings of this type.

Proposition 3. If $f(x,y)$ is an arbitrary rotation-invariant mapping, $\Delta_x,\Delta_y,\Delta\in V_n$ are arbitrary vectors, and $g(x,y):=f\left(x\oplus\Delta_x,y\oplus\Delta_y\right)\oplus\Delta$, then

$$rp^g(r)=xdp^f\left(\Delta_x\oplus\Delta_x^{-r},\Delta_y\oplus\Delta_y^{-r}\to\Delta\oplus\Delta^{-r}\right).$$

Proof. From Theorem 1 and Corollary 1 we have

$$rp^g(r)=xrp^f\left(r;\Delta_x\oplus\Delta_x^r,\Delta_y\oplus\Delta_y^r\to\Delta\oplus\Delta^r\right).$$

By applying Proposition 2, we obtain

$$rp^g(r)=xdp^f\left((\Delta_x\oplus\Delta_x^r)^{-r},\left(\Delta_y\oplus\Delta_y^r\right)^{-r}\to(\Delta\oplus\Delta^r)^{-r}\right).$$

Since $(\Delta\oplus\Delta^r)^{-r}=\Delta^{-r}\oplus\Delta$, the proposition is proved. □

Proposition 3 reveals an unexpected connection between differentials and rotation pairs for rotation-invariant mappings with linear shifts.

Ito *et al.* discovered a particular case of Proposition 3 during their analysis of the Friet-PC cryptographic LRX-permutation [11].This permutation uses the function

$$g(x,y)=(x\oplus\Delta_x)\&\left(y\oplus\Delta_y\right),$$

where Δ_x and Δ_y are constants defined by the specification.

The probabilities of the differentials for the bitwise AND operation (i.e. the mapping $f(x,y)=x\&y$) were found in [12]. In particular, the probability of the differential $(\alpha,\beta\to0)$ for arbitrary $\alpha,\beta\in V_n$ is

$$xdp^{\&}(\alpha,\beta\to0)=2^{-wt(\alpha\vee\beta)}.$$

As any bitwise logic operation describes a rotation-invariant mapping, applying Proposition 3 to the mapping $g(x,y)$ when $\Delta=0$ gives us

$$rp^g(r)=2^{-wt\left((\Delta_x^{-r}\oplus\Delta_x)\vee(\Delta_y^{-r}\oplus\Delta_y)\right)}=2^{-wt\left((\Delta_x\oplus\Delta_x^r)\vee(\Delta_y\oplus\Delta_y^r)\right)},$$

which was found in [11]. However, as can be seen, Proposition 3 can be applied to more complex rotation-invariant mappings and their modifications.

Conclusions. This paper presents analytical expressions for the probabilities of RX-differentials of Boolean mappings under linear shifts of inputs and/or outputs. It demonstrates that, for some classes of shifts (in particular, vector inversions), the distribution of differential probabilities and rotation pairs probabilities remains unchanged. Accordingly, some cases of adding constants in the nodes of ARX cryptosystems do not necessarily increase their security against rotational cryptanalysis. The relationship between differentials and rotation pairs is demonstrated for specific classes of rotation-invariant mappings and their modifications.

The obtained results could be useful for evaluating the cryptographic security of ARX-cryptosystems and for developing new secure cryptographic algorithms suitable for low-resource devices.

Funding. The author did not receive any funding for conducting research or writing the article.

References

1. Lipmaa H., Moriai S. Efficient Algorithms for Computing Differential Properties of Addition. *In: Matsui, M. (eds) Fast Software Encryption. FSE 2001. Lecture Notes in Computer Science*. Vol 2355. Springer, Berlin, Heidelberg, 2002. https://doi.org/10.1007/3-540-45473-X_28
2. Khovratovich D., Nikolić I. Rotational Cryptanalysis of ARX. *In: Hong, S., Iwata, T. (eds) Fast Software Encryption. FSE 2010. Lecture Notes in Computer Science*. Vol 6147. Springer, Berlin, Heidelberg, 2010. https://doi.org/10.1007/978-3-642-13858-4_19
3. Khovratovich D., Nikolic I., Pieprzyk J., Sokołowski P., Steinfeld R. Rotational Cryptanalysis of ARX Revisited. *Cryptology ePrint Archive*. Paper 2015/095. 2015. https://eprint.iacr.org/2015/095
4. Ashur T., Liu Yu. Rotational Cryptanalysis in the Presence of Constants. *Cryptology ePrint Archive*. Paper 2016/826. 2016. https://doi.org/10.46586/tosc.v2016.i1.57-70
5. Yakovliev S. Differential Properties of LRX-analogues of Small Constant Multiplication. *INTL Journal of Electronics and Telecommunications*. 2025. Vol. 71, No. 1. P. 95–100. http://dx.doi.org/10.24425/ijet.2025.153550
6. Biryukov A., Lambin B., Udovenko A. Exact Formula for RX-Differential Probability Through Modular Addition for All Rotations. *IACR Transactions on Symmetric Cryptology*. 2025. Vol. 2025, No. 1. P. 542–591. https://doi.org/10.46586/tosc.v2025.i1.542-591
7. Yakovliev S., Korzh N. Differential-Rotational Probabilities of Modular Addition and Its Approximations. *Theoretical and Applied CyberSecurity*. 2024. Vol. 6, No. 2. P. 5–15. https://doi.org/10.20535/tacs.2664-29132024.2.318611
8. NIST and Dworkin M.J. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. 2015. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=919061 (accessed: 22.06.2025)
9. Dobraunig C., Eichlseder M., Mendel F., Schlaffer M. Ascon v1.2: Lightweight Authenticated Encryption and Hashing. *Journal of Cryptology*. 2021. Vol. 34. https://doi.org/10.1007/s00145-021-09398-9
10. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. The SIMON and SPECK Families of Lightweight Block Ciphers. *Cryptology ePrint Archive*. Paper 2013/404. 2013. https://eprint.iacr.org/2013/404
11. Ito R., Shiba R., Sakamoto K., Liu F., Isobe T. Bit-wise Cryptanalysis on AND-RX Permutation Friet-PC. *Cryptology ePrint Archive*. Paper 2021/212. 2021. https://doi.org/10.1016/j.jisa.2021.102860
12. Biryukov A., Roy A., Velichkov V. Differential Analysis of Block Ciphers SIMON and SPECK. *Cryptology ePrint Archive*. Paper 2014/922. 2014. https://eprint.iacr.org/2014/922

Received 22.06.2025

Serhii Yakovliev,
Ph.D., Head of the Department of Mathematical Methods of Information Security,
Institute of Physics and Technology, Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine.
https://orcid.org/0000-0002-5647-5043
yasv@rl.kiev.ua

УДК 004.056.55:512.6

С.В. Яковлєв

Деякі алгебраїчні властивості імовірностей RX-диференціалів булевих відображень

Навчально-науковий фізико-технічний інститут, КПІ ім. Ігоря Сікорського, Київ
Листування: yasv@rl.kiev.ua

Вступ. ARX- та LRX-криптосистеми будуються на основі виключно простих операцій, доступних на рівні інструкцій обчислювальних процесорів: модульного додавання, побітового додавання, циклічних зсувів тощо. Через просту реалізацію та надвисоку швидкість роботи ARX- та LRX-криптосистеми стали важливою частиною так званої «легкої криптографії» (lightweight cryptography) – напрямку, присвяченому розробці надійних алгоритмів для малоресурсних пристроїв та Інтернету речей. Однак простота структури спрощує побудову атак, тому створення таких систем вимагає ретельного аналізу та оцінювання криптографічної стійкості до відомих методів атак, таких як RX-аналіз.

У даній роботі розглядаються перетворення імовірностей RX-диференціалів булевих функцій під час лінійних зсувів входів та виходів. Властивості таких перетворень дозволяють спростити аналіз ARX-

криптосистем, зокрема, одержувати аналітичні вирази для імовірностей диференціалів та пар обертання через відповідні вирази для RX-диференціалів.

Мета роботи – отримати точні аналітичні вирази для імовірностей RX-диференціалів булевих відображень із лінійними зсувами, які дозволять провадити більш тонкий аналіз криптографічних властивостей таких відображень.

Результати. Отримано точні аналітичні вирази для імовірностей RX-диференціалів (а також звичайних диференціалів та пар обертання) для бінарних булевих відображень із лінійними зсувами. Доведено, що RX-диференціали для заданих відображень та їх двоїстих функцій матимуть однакові імовірності. Показано, що додавання із константами, поширений метод підвищення стійкості до обертального криптоаналізу, не завжди дає бажаний ефект. Для обертально-інваріантних відображень зі зсувами продемонстровано несподіваний зв'язок між імовірностями пар обертання та імовірностями диференціалів.

Висновки. Отримані результати можуть бути використані при аналізі криптографічної стійкості ARX-криптосистем та розробці нових надійних криптографічних алгоритмів, придатних для застосування у малоресурсних пристроях.

Ключові слова: симетрична криптографія, ARX-криптосистеми, дифереціальний криптоаналіз, обертальний криптоаналіз, RX-криптоаналіз.