UDC 004.056.55:512.6

Oblivious S-functions and Their Security against Rotational Cryptanalysis

Serhii Yakovliev[1], Ihor Voloshyn[1]

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

Abstract

This paper considers a specific class of ARX primitives: oblivious S-functions, which are distinguished by their computational states being independent of each other. We present generic analytical expressions for the rotation probabilities of oblivious S-functions, which characterize security against rotational cryptanalysis. We also examile particular classes of oblivious S-functions, including generalized NORX-like mappings and LRX-analogues for multiplication by three. For these mappings, we provide numerical values of the rotation probabilities.

Keywords: symmetric cryptography, ARX cryptosystems, rotational cryptanalysis, S-function

Introduction

ARX cryptosystems (from «Addition, Rotation, XOR») use only modular additions, bitwise additions, and cyclic shifts in their structure. Other operations are sometimes used as well, primarily those available at the processor instruction level, such as logical AND, logical OR, non-cyclic shifts etc. ARX systems without modular additions are often referred to as *LRX systems*, where L stands for "Logic".

ARX cryptosystems have gained popularity in recent years due to their speed and ease of implementation. These cryptosystems can be easily adapted to most hardware architectures. ARX cryptosystems are widely used for data encryption on cloud platforms, secure Internet connections, protecting bank card data, and ensuring fast cryptography in virtual private networks.

Rotational cryptanalysis [1, 2] is a specific cryptanalytic technique that is mostly suitable for ARX/LRX systems. It focuses on changes that occur during the calculation of ARX transformations in messages that differs by cyclic shifts. This method was applied to the Chaskey cipher [3], Salsa cipher [4], ChaCha cipher [5, 6], modified GOST cipher [7], MORUS cipher [8], and others.

In [9], the concept of *S-functions* was proposed: representation of ARX transformations as finite automata of a special type. S-functions enable the development of computationally efficient algorithms for evaluating outputs, distributions, and various statistics of ARX transformations. The analysis of S-functions and their applications for cryptographic purposes was further improved in [10, 11].

This paper considers a special class of S-functions: *oblivious S-functions*. We provide analytical expressions for the probabilities of rotation pairs in general and in specific cases. These expressions characterize the security of oblivious S-functions against rotational cryptanalysis.

The results obtained were partially presented at the International Conference on Innovative Solutions in Software Engineering (ICISSE 2023, Nov. 29–30, 2023, Ivano-Frankivsk, Ukraine) and at the XXIII Scientific and Practical Conference «Theoretical and Applied Problems of Physics, Mathematics, and Informatics» (May 14-17, 2025, Kyiv, Ukraine).

The rest of the paper is organized as follows. Section 1 provides the basic terms, definitions and notation. Section 2 introduces the concept of the oblivious S-function and presents analytical expressions for the rotation probabilities of the oblivious S-functions. The next sections are dedicated to specific cases of oblivious S-functions

and their rotation probabilities: Section 3 considers generalized NORX-like mappings; Section 4 considers LRX-analogues of multiplication by three; and Section 5 considers specific LRX mappings introduced in this paper.

1. Terms and Notation

This section introduces the necessary notation for the rest of the material.

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

$x \in V_n$ — an arbitrary vector whose bits are numbered in the following order:

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

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

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

$x \oplus y$ — bitwise addition operation (XOR);

$x \sim y$ — bitwise equivalence operation;

$x \wedge y$ — bitwise conjunction (logical AND);

$x \vee y$ — bitwise disjunction (logical OR);

$x \downarrow y$ — Pierce arrow (NOR);

$x \uparrow y$ — Sheffer stroke (NAND);

$x \to y$, $x \leftarrow y$ — implication and reverse implication;

$x \not\to y$, $x \not\leftarrow y$ — negation of implications.

We denote the set of all considered nonlinear bitwise logical operations by $\mathbb{O}$:

$$\mathbb{O} = \{\wedge, \vee, \downarrow, \uparrow, \to, \leftarrow, \not\to, \not\leftarrow\}.$$

V_n^m is the set of m-tuples of n-bit vectors. For each $X = (x^{(1)}, \ldots, x^{(m)}) \in V_n^m$ an *i-th slice* X_i is a vector of i-th coordinates:

$$X_i = \left(x_i^{(1)}, x_i^{(2)}, \ldots x_i^{(m)}\right) \in V_m.$$

The rotation for the tuple $X \in V_n^m$ is defined as the rotation of all its internal vectors:

$$X^r = \left(\left(x^{(1)}\right)^r, \left(x^{(2)}\right)^r, \ldots \left(x^{(m)}\right)^r\right).$$

Rotation-based cryptanalysis (or *rotational cryptanalysis*) is a method of cryptanalysis of ARX cryptosystems based on studying the properties of so-called *rotation pairs* — pairs of vectors $(X,\ X^r)$ that are passed through an ARX transformation, where r is an arbitrary but fixed value and X is a random value.

For every $f : V_n^m \to V_n$ the security of f against rotational cryptanalysis is determined by the *rotation probabilities* $rp^f(r)$,

$$rp^f(r) = \Pr_X\{f(X^r) = (f(X))^r\},$$

where X are randomly selected from V_n^m.

A function $f\colon V_n^m \to V_n$ is called an *S-function* [9] if there exist a set Q, mappings $\varphi\colon V_m \times Q \to \{0,1\}$ and $\psi\colon V_m \times Q \to Q$, a fixed value $S_0 \in Q$ and, for every $X \in V_n^m$, an additional sequence $S = (S_1, \ldots, S_{n-1})$, $S_i \in Q$, such that the calculation of the vector $z = f(X)$ can be represented as

$$\begin{aligned} z_i &= \varphi(X_i, S_i), \\ S_{i+1} &= \psi(X_i, S_i), \quad i = 0, 1, 2, \ldots \end{aligned}$$

The set Q must be finite and independent of n. The variables S_i are called *computational states* of the S-function, S_0 — *initial state*, φ — *output function*, ψ — *transition function*. We will further consider an arbitrary S-function as the tuple $\langle Q, \varphi, \psi, S_0\rangle$. As one can see, S-functions are special cases of Mealy automata.

2. Oblivious S-functions and Their Rotation Probabilities

In this paper, we introduce a special class of S-functions: oblivious S-functions, in which the value of the next state is determined only by the input bits. Formally, an *oblivious S-function* is the S-function of form $\langle Q, \varphi, \psi, S_0\rangle$, where

$$\forall i \geq 0\colon S_{i+1} = \psi(X_i).$$

Examples of oblivious S-functions include the family of mappings $f(x) = x \star (x \ll 1)$ studied in [12], where $\star$ denotes an arbitrary bitwise operation, and the function

$$\mathsf{H}(x, y) = x \oplus y \oplus (xy \ll 1),$$

proposed by the developers of the NORX cipher [13] as an approximation of modular addition.

For the oblivious S-functions, all rotation probabilities can be expressed in the general case. This result is formulated in the following theorem.

Theorem 1. *Let $f\colon V_n^m \to V_n$ be an oblivious S-function, with output function φ, transition function ψ, and initial state S_0. For $X \in V_n^m$ and $i \geq 1$, define $S_i := \psi(X_{i-1})$. Then*

$$\begin{aligned} rp^f(r) = \Pr\{&\varphi(X_0, S_0) = \varphi(X_0, S_n), \\ &\varphi(X_{n-r}, S_0) = \varphi(X_{n-r}, S_{n-r})\}. \end{aligned}$$

Proof. Assuming that $u := f(X^r)$, we have:

$$\begin{aligned} i = 0&: \ u_0 = \varphi(X_{n-r}, S_0), \\ 0 < i < r&: \ u_i = \varphi(X_{n-r+i}, S_{n-r+i}), \\ i = r&: \ u_r = \varphi(X_0, S_n), \\ r < i < n&: \ u_i = \varphi(X_{i-r}, S_{i-r}); \end{aligned}$$

Similarly, assuming that $v := (f(X))^r$, we have:

$$\begin{aligned} i = 0&: \ v_0 = \varphi(X_{n-r}, S_{n-r}), \\ 0 < i < r&: \ v_i = \varphi(X_{n-r+i}, S_{n-r+i}), \\ i = r&: \ v_r = \varphi(X_0, S_0), \\ r < i < n&: \ v_i = \varphi(X_{i-r}, S_{i-r}). \end{aligned}$$

Therefore, we have that $u_i = v_i$ for all $i \neq 0$, $i \neq r$; thus,

$$\begin{aligned} rp^f(r) = &\Pr\{u = v\} = \\ &= \Pr\{u_0 = v_0, u_r = v_r\}, \end{aligned}$$

from which, using the values u_0, u_r, v_0, and v_r, we obtain the statement of the theorem. □

Corollary 1. *For $2 \leq r \leq n-2$, it holds that*

$$rp^f(r) = \left(\Pr_{a,a'}\{\varphi(a, S_0) = \varphi(a, \psi(a'))\}\right)^2,$$

where a, a' are randomly selected from V_m.

Proof. Indeed, for $2 \leq r \leq n-2$, the equalities $u_0 = v_0$ and $u_r = v_r$ are determined by different slices of X, i.e. they are independent. Therefore, we can replace the specific slices of X with random variables from V_m. This implies the corollary's statement. □

Note that the rotation probabilities of oblivious S-functions do not depend on the length of the vectors. In particular, the values of $rp^f(r)$ are the same for all $2 \leq r \leq n-2$. The cases $r = 1$ and $r = n-1$ should be considered separately since the equations $u_0 = v_0$ and $u_r = v_r$ may be dependent in these cases.

As a direct application of Theorem 1, one can construct an ARX-mapping that completely disrupts rotational pairs. For example, consider the following two functions:

$$\begin{aligned} \mathsf{A}(x, y) &= x \oplus y \oplus 1; \\ \mathsf{Neg}(x, y) &= x \oplus y \oplus (1 \ldots 10). \end{aligned}$$

They are both the oblivious S-functions with the set of states $Q = \{0, 1\}$ and output function $\varphi(x_i, y_i, S_i) = x_i \oplus y_i \oplus S_i$. Function A has the initial state $S_0 = 1$ and the transition function $\psi(x_i, y_i) = 0$. Function Neg has the initial state $S_0 = 0$ and the transition function $\psi(x_i, y_i) = 1$. From Theorem 1 we have

$$rp^{\mathsf{A}}(r) = rp^{\mathsf{Neg}}(r) = 0$$

for all $0 < r < n$. Therefore, these mappings do not transit rotation pairs at all. However, this simple security mechanism against rotational cryptanalysis can be bypassed with more sophisticated techniques, such as differential-rotational analysis [14].

3. Rotation Probabilities of NORX-like Functions

In [15], Aumasson *et al.* showed that the rotation probabilities of the function

$$\mathsf{H}(x, y) = x \oplus y \oplus (xy \ll 1),$$

the main nonlinear transformation of the NORX cipher, are equal to $9/16$, regardless of the rotation value r. This result can be generalized in several ways.

Claim 1. *The rotation probabilities $rp^{\mathsf{H}_\star}(r)$ of the generalized NORX-like operation*

$$\mathsf{H}_\star(x, y) = x \oplus y \oplus ((x \star y) \ll 1)$$

for all appropriate values of r are equal to

- $9/16$ *for* $\star \in \{\wedge, \downarrow, \not\rightarrow, \not\leftarrow\}$;
- $1/16$ *for* $\star \in \{\vee, \uparrow, \rightarrow, \leftarrow\}$;
- $1/4$ *for* $\star \in \{\oplus, \sim\}$.

Proof. The function $\mathsf{H}_\star(x, y)$ can be represented as an oblivious S-function as follows:

- the set of states: $Q = \{0, 1\}$;
- the initial state $S_0 = 0$;
- the transition function

$$S_{i+1} = \psi(x_i, y_i) = x_i \star y_i;$$

- the output function

$$z_i = \varphi(x_i, y_i, S_i) = x_i \oplus y_i \oplus S_i.$$

Therefore, from Theorem 1, we obtain for every value of r

$$\begin{aligned} rp^{\mathsf{H}_\star}(r) &= \Pr\{S_0 = S_n, S_0 = S_{n-r}\} = \\ &= \Pr\{x_{n-1} \star y_{n-1} = 0, x_{n-r-1} \star y_{n-r-1} = 0\}, \end{aligned}$$

and, hence bits at positions $n-1$ and $n-r-1$ are independent,

$$rp^{\mathsf{H}_\star}(r) = \left(\Pr_{a,b}\{a \star b = 0\}\right)^2,$$

where $a, b \in_R \{0, 1\}$. The statement of the theorem follows from direct calculations on truth tables for every operation. □

Another way to generalize the $\mathsf{H}(x, y)$ function is to combine of more than two arguments. There are two possible options.

Claim 2. *For $X \in V_n^m$, $X = (x^{(1)}, \ldots, x^{(m)})$ define the mapping*

$$\mathsf{HM}(X) = x^{(1)} \oplus \cdots \oplus x^{(m)} \oplus ((x^{(1)} \ldots x^{(m)}) \ll 1).$$

Then, for every appropriate value of r,

$$rp^{\mathsf{HM}}(r) = \left(1 - \frac{1}{2^m}\right)^2.$$

Proof. Again, we can represent the function $\mathsf{HM}(X)$ as the oblivious S-function as follows:

- the set of states: $Q = \{0, 1\}$;
- the initial state $S_0 = 0$;
- the transition function

$$S_{i+1} = \psi(X_i) = x_i^{(1)} x_i^{(2)} \ldots x_i^{(m)};$$

- the output function

$$z_i = \varphi(X_i, S_i) = x_i^{(1)} \oplus x_i^{(2)} \oplus \ldots \oplus x_i^{(m)} \oplus S_i.$$

Therefore, from Theorem 1, we obtain for every value of r

$$\begin{aligned} rp^{\mathsf{HM}}(r) &= \Pr\{S_0 = S_n, S_0 = S_{n-r}\} = \\ &= \Pr\{S_n = 0\} \Pr\{S_{n-r} = 0\}. \end{aligned}$$

As a result, we obtain

$$rp^{\mathsf{HM}}(r) = p^2,$$
$$p = \Pr_{a_1, a_2, \ldots, a_m}\{a_1 a_2 \ldots a_m = 0\},$$

where $a_1, a_2, \ldots, a_m \in_R \{0, 1\}$. The statement of claim comes from this and the properties of the logical AND operation. □

Claim 3. *Define the mapping*

$$\mathsf{Hm}(x, y, z) = x \oplus y \oplus z \oplus (maj(x, y, z) \ll 1),$$

where $maj(x, y, z)$ is a majority function:

$$maj(x, y, z) = xy \oplus yz \oplus xz.$$

Then for every appropriate value of r

$$rp^{\mathsf{Hm}}(r) = \frac{1}{4}.$$

Proof. As with previous claims, we can represent the function $\mathsf{Hm}(x, y, z)$ as the oblivious S-function as follows:

- the set of states: $Q = \{0, 1\}$;
- the initial state $S_0 = 0$;
- the transition function

$$S_{i+1} = \psi(x_i, y_i, z_i) = maj(x_i, y_i, z_i);$$

- the output function

$$u_i = \varphi(x_i, y_i, z_i, S_i) = x_i \oplus y_i \oplus z_i \oplus S_i.$$

Therefore, from Theorem 1, we obtain for every value of r

$$\begin{aligned} rp^{\mathsf{Hm}}(r) &= \Pr\{S_0 = S_n, S_0 = S_{n-r}\} = \\ &= \Pr\{maj(x_{n-1}, y_{n-1}, z_{n-1}) = 0\} \times \\ &\times \Pr\{maj(x_{n-r-1}, y_{n-r-1}, z_{n-r-1}) = 0\}. \end{aligned}$$

Hence maj is a balanced mapping, it takes zero value with probability 1/2; thus,

$$rp^{\mathsf{HM}}(r) = \left(\frac{1}{2}\right)^2 = \frac{1}{4},$$

which concludes the proof. □

As one can see, some of $\mathsf{H}_\star$ functions have very small rotation probabilities. However, they may lose some of the useful algebraic properties of the original H operation, such as regularity.

The function HM, thus highly nonlinear, has very high rotation probabilities. In contrast, the function Hm is quadratic and has moderate rotation probabilities. Therefore, for cryptographic purposes, the appropriate mappings must be chosen according to a wider set of criteria than just security against rotational cryptanalysis.

4. Rotation Probabilities of "Multiplication-by-3" Analogues

In this section, we consider mappings of the form $u_\star(x) = x \star (x \ll 1)$, where $\star$ is a bitwise operation. The functions $u_\star$ are LRX-analogues of multiplication by three:

$$3x \equiv x + 2x \equiv x + (x \ll 1) \pmod{2^n}.$$

In $u_\star$, modular addition is replaced with some simpler logical operation. The cryptographic properties of these mappings were studied in [16].

The following statements describe all the rotation probabilities of $u_\star(x)$. These results were obtained by first author and Denys Kobets [12].

Claim 4. *The following equations hold:*

$$\begin{aligned} rp^{u_\star}(1) &= \Pr\{x_{n-1} \star 0 = x_{n-1} \star x_{n-2}, \\ &\qquad x_0 \star 0 = x_0 \star x_{n-1}\}; \\ rp^{u_\star}(n-1) &= \Pr\{x_1 \star 0 = x_1 \star x_0, \\ &\qquad x_0 \star 0 = x_0 \star x_{n-1}\}; \\ rp^{u_\star}(r) &= \Pr\{x_{n-r} \star 0 = x_{n-r} \star x_{n-r-1}\} \times \\ &\times \Pr\{x_0 \star 0 = x_0 \star x_{n-1}\}. \end{aligned}$$

for every $2 \le r \le n - 2$.

Proof. First, we construct the following representation of $u_\star(x)$ as the oblivious S-function:

- the set of states: $Q = \{0, 1\}$;
- the initial state $S_0 = 0$;
- the transition function

$$S_{i+1} = \psi(x_i) = x_i;$$

- the output function

$$z_i = \varphi(x_i, S_i) = x_i \star S_i.$$

Therefore, from Theorem 1, we obtain

$$\begin{aligned} rp^f(r) = \Pr\{&\varphi(x_0, S_0) = \varphi(x_0, S_n),\\ &\varphi(x_{n-r}, S_0) = \varphi(x_{n-r}, S_{n-r})\} =\\ = \Pr\{&x_0 \star 0 = x_0 \star x_{n-1},\\ &x_{n-r} \star 0 = x_{n-r} \star x_{n-r-1}\}. \end{aligned}$$

Substituting r with 1, $n-1$, or an arbitrary value from 2 to $n-2$ implies the statement of the claim. □

Corollary 2. *For every operation $\star$, the rotation probabilities of $u_\star(x)$ are evaluated as*

$$rp^{u_\star}(1) = rp^{u_\star}(n-1) = q_\star, \quad rp^{u_\star}(r) = p_\star^2,$$

where

$$q_\star = \Pr_{a,b,c}\{a \star 0 = a \star b, b \star 0 = b \star c\},$$
$$p_\star = \Pr_{a,b}\{a \star 0 = a \star b\},$$

and $a, b, c \in_R \{0, 1\}$. The exact values are provided in the Table 1.

Corollary 2 follows from Claim 4 and direct calculations.

Table 1
The rotation probabilities fop $u_\star(x)$

$\star$	$rp^{u_\star}(1)$, $rp^{u_\star}(n-1)$	$rp^{u_\star}(r)$, $2 \le r \le n-2$
$\wedge$	$5/8$	$9/16$
$\vee$	$1/2$	$9/16$
$\downarrow$	$1/2$	$9/16$
$\uparrow$	$5/8$	$9/16$
$\rightarrow$	$5/8$	$9/16$
$\leftarrow$	$1/2$	$9/16$
$\oplus$	$1/4$	$1/4$
$\sim$	$1/4$	$1/4$

As Table 1 shows, all operations $\star$ can be divided into two classes: nonlinear ($\star \in \mathbb{O}$) and linear ($\star \in \{\oplus, \sim\}$). The probability of that a rotation pair will pass through nonlinear transformations are between 0.5 and 0.625. Interestingly, both the smallest and largest probabilities are achieved for the smallest rotation value (one position to the left or right). For linear transformations, every rotation probability is equal to 0.25 for any rotation value.

The work [17] shows that the rotation probabilities of the function $f(x) = 3x \bmod 2^n$ for $r = 1$ depend on n, but tend to the value $1/3$. Accordingly, nonlinear LRX analogues of this mapping have higher rotation probabilities, which can be considered as a certain trade-off for a simpler and faster computable structure. Contrary to this, linear transformations have lower rotation probabilities and, consequently, provide better security against rotational cryptanalysis. However, it should be noted that linear transformations do not provide security against other types of cryptanalysis, such as differential and linear cryptanalysis. Therefore, when constructing ARX cryptosystems using constant multiplication analogues, combining nonlinear and linear operations is desirable in order to achieve the desired level of security against all types of cryptanalysis.

5. Rotation Probabilities of Specific Types of Oblivious S-functions

In this section, we consider two types of ARX transformations that combine the concepts of NORX-like mappings and multiplication-by-3 analogues:

$$f_\star(x, y) = x \oplus y \oplus (x \star (y \ll 1)) \oplus (y \star (x \ll 1));$$
$$g_\star(x, y) = x \oplus y \oplus (x \star (x \ll 1)) \oplus (y \star (y \ll 1)),$$

where $\star$ denotes some bitwise operation on binary vectors.

Claim 5. *The rotation probabilities for the functions $f_\star(x, y)$ and $g_\star(x, y)$, where $\star \in \mathbb{O}$, are equal to $3/8$, $7/16$ or $25/64$. The exact values are given in Table 2.*

Proof. The function $f_\star$ is an oblivious S-function. We construct the following representation:

- the set of states: $Q = V_2$, the states $S_i = (a_i, b_i)$;
- the initial state $S_0 = (0, 0)$;
- the transition function

$$S_{i+1} = \psi(x_i, y_i) = (x_i, y_i);$$

Table 2
The rotation probabilities for $f_\star(x,y)$ and $g_\star(x,y)$

$\star$	$rp(1)$, $rp(n-1)$	$rp(r)$, $2 \le r \le n-2$
$\wedge$	$7/16$	$25/64$
$\vee$	$3/8$	$25/64$
$\downarrow$	$3/8$	$25/64$
$\uparrow$	$7/16$	$25/64$
$\rightarrow$	$7/16$	$25/64$
$\leftarrow$	$3/8$	$25/64$
$\nrightarrow$	$7/16$	$25/64$
$\nleftarrow$	$3/8$	$25/64$

- the output function

$$z_i = \varphi(x_i, y_i, S_i) = x_i \oplus y_i \oplus (x_i \star b_i) \oplus (y_i \star a_i).$$

Therefore, according to Theorem 1, the probability $rp^{f_\star}(r)$ is equal to the probability that the next system of relations will be satisfied:

$$\begin{cases} \varphi(x_0, y_0, S_0) = \varphi(x_0, y_0, \psi(x_{n-1}, y_{n-1})), \\ \varphi(x_{n-r}, y_{n-r}, S_0) = \\ \qquad = \varphi(x_{n-r}, y_{n-r}, \psi(x_{n-r-1}, y_{n-r-1})). \end{cases}$$

After substituting the expressions φ and ψ, we obtain the following system of relations:

$$\begin{cases} (x_0 \star 0) \oplus (y_0 \star 0) \oplus \\ \quad \oplus (x_0 \star y_{n-1}) \oplus (y_0 \star x_{n-1}) = 0, \\ (x_{n-r} \star 0) \oplus (y_{n-r} \star 0) \oplus \\ \quad \oplus (x_{n-r} \star y_{n-r-1}) \oplus (y_{n-r} \star x_{n-r-1}) = 0. \end{cases}$$

For each operation $\star \in \mathbb{O}$ and for each value r, the probability that this system will be satisfied is found directly by constructing the corresponding truth tables.

Similarly, the function $g_\star$ is also an oblivious S-function with the following representation:

- the set of states: $Q = V_2$,
  the states $S_i = (a_i, b_i)$;
- the initial state $S_0 = (0, 0)$;
- the transition function

$$S_{i+1} = \psi(x_i, y_i) = (x_i, y_i);$$

- the output function

$$z_i = \varphi(x_i, y_i, S_i) = x_i \oplus y_i \oplus (x_i \star a_i) \oplus (y_i \star b_i).$$

The probability $rp^{g_\star}(r)$ is equal to the probability that the next system of relations will be satisfied:

$$\begin{cases} \varphi(x_0, y_0, S_0) = \varphi(x_0, y_0, \psi(x_{n-1}, y_{n-1})), \\ \varphi(x_{n-r}, y_{n-r}, S_0) = \\ \qquad = \varphi(x_{n-r}, y_{n-r}, \psi(x_{n-r-1}, y_{n-r-1})). \end{cases}$$

After substituting the expressions for φ and ψ, we obtain the following system of relations that defines the probability $rp^{g_\star}(r)$:

$$\begin{cases} (x_0 \star 0) \oplus (y_0 \star 0) \oplus \\ \quad \oplus (x_0 \star x_{n-1}) \oplus (y_0 \star y_{n-1}) = 0, \\ (x_{n-r} \star 0) \oplus (y_{n-r} \star 0) \oplus \\ \quad \oplus (x_{n-r} \star x_{n-r-1}) \oplus (y_{n-r} \star y_{n-r-1}) = 0. \end{cases}$$

For each operation $\star \in \mathbb{O}$ and for each value r, the probability that this system will be satisfied is also found directly by constructing the corresponding truth tables. □

For illustrative purposes, we demonstrate the proper calculation of the rotation probabilities for the function

$$g_{\nrightarrow}(x,y) = x \oplus y \oplus (x \nrightarrow (x \ll 1)) \oplus (y \nrightarrow (y \ll 1)).$$

It is easy to verify that, for $a \in \{0,1\}$, the relation $a \nrightarrow 0 \equiv a$ holds. According to the proof of Claim 5, the probabilities $rp^{g_\nrightarrow}(r)$ are equal to the probability of satisfying the following system of equations:

$$\begin{cases} x_0 \oplus y_0 \oplus (x_0 \nrightarrow x_{n-1}) \oplus (y_0 \nrightarrow y_{n-1}) = 0, \\ x_{n-r} \oplus y_{n-r} \oplus (x_{n-r} \nrightarrow x_{n-r-1}) \oplus \\ \qquad \oplus (y_{n-r} \nrightarrow y_{n-r-1}) = 0. \end{cases}$$

For $2 \le r \le n-2$, we have $rp^{g_\nrightarrow}(r) = p^2$, where

$$p = \Pr\{a \oplus b \oplus (a \nrightarrow c) \oplus (b \nrightarrow d) = 0\}. \quad (1)$$

The truth table for calculating probability (1) is given in Table 3. From this table we have

$$rp^{g_\nrightarrow}(r) = \left(\frac{10}{16}\right)^2 = \frac{25}{64}.$$

For $r = 1$, the following system of equations is used to calculate $rp^{g_\nrightarrow}(1)$:

$$\begin{cases} x_0 \oplus y_0 \oplus (x_0 \nrightarrow x_{n-1}) \oplus (y_0 \nrightarrow y_{n-1}) = 0, \\ x_{n-1} \oplus y_{n-1} \oplus (x_{n-1} \nrightarrow x_{n-2}) \oplus \\ \qquad \oplus (y_{n-1} \nrightarrow y_{n-2}) = 0. \end{cases}$$

Therefore,

$$\begin{aligned} &rp^{g_\nrightarrow}(r) = \\ &\quad = \Pr\{a \oplus b \oplus (a \nrightarrow c) \oplus (b \nrightarrow d) = 0, \quad (2) \\ &\qquad c \oplus d \oplus (c \nrightarrow e) \oplus (d \nrightarrow f) = 0\}. \end{aligned}$$

Table 3
Truth table for calculating probability (1); here $B = a \nrightarrow c$, $C = b \nrightarrow d$, $A = a \oplus b \oplus B \oplus C$.
The probability p is calculated as $p = \Pr\{A = 0\}$

a	b	c	d	B	C	A
0	0	0	0	0	0	0
0	0	0	1	0	0	0
0	0	1	0	0	0	0
0	0	1	1	0	0	0
0	1	0	0	0	1	0
0	1	0	1	0	0	1
0	1	1	0	0	1	0
0	1	1	1	0	0	1
1	0	0	0	1	0	0
1	0	0	1	1	0	0
1	0	1	0	0	0	1
1	0	1	1	0	0	1
1	1	0	0	1	1	0
1	1	0	1	1	0	1
1	1	1	0	0	1	1
1	1	1	1	0	0	0

The truth table for calculating probability (2) is given in Table 4. From this table, we can see that

$$rp^{g\nrightarrow}(r) = \frac{28}{64} = \frac{7}{16}.$$

The case $r = n - 1$ is similar to the case $r = 1$.

Conclusions

This paper introduces a new ARX primitive: the oblivious S-function. The computation states of such S-functions depend only on the input arguments and not on previous states. Thus, oblivious S-functions have a simplified computation scheme, increasing their implementation efficiency.

For the oblivious S-functions, we obtained general analytical expressions for the rotation probabilities, which characterize security against rotational cryptanalysis. We demonstrate that the rotation probability values do not depend on the input vector lengths and only take two different values, depending on the rotation parameter. Numerical values of rotation probabilities have been thoroughly obtained for several classes of oblivious S-functions, including generalized NORX-like operations and multiplication-by-3 analogues.

These results can be used to construct new ARX/LRX cryptosystems with provable security against rotational analysis and other types of cryptanalysis.

Table 4
Truth table for calculating probability (2); here $C = a \nrightarrow c$, $D = b \nrightarrow d$, $E = c \nrightarrow e$, $F = d \nrightarrow f$, $A = a \oplus b \oplus C \oplus D$, $B = c \oplus d \oplus E \oplus F$.
The lines that determine the probability $\Pr\{A = 0, B = 0\}$ are marked in bold

a	b	c	d	e	f	C	D	E	F	A	B
0	0	0	0	0	0	0	0	0	0	**0**	**0**
0	0	0	0	0	1	0	0	0	0	**0**	**0**
0	0	0	0	1	0	0	0	0	0	**0**	**0**
0	0	0	0	1	1	0	0	0	0	**0**	**0**
0	0	0	1	0	0	0	0	0	1	**0**	**0**
0	0	0	1	0	1	0	0	0	0	0	1
0	0	0	1	1	0	0	0	0	1	**0**	**0**
0	0	0	1	1	1	0	0	0	0	0	1
0	0	1	0	0	0	0	0	1	0	**0**	**0**
0	0	1	0	0	1	0	0	1	0	**0**	**0**
0	0	1	0	1	0	0	0	0	0	0	1
0	0	1	0	1	1	0	0	0	0	0	1
0	0	1	1	0	0	0	0	1	1	**0**	**0**
0	0	1	1	0	1	0	0	1	0	0	1
0	0	1	1	1	0	0	0	0	1	0	1
0	0	1	1	1	1	0	0	0	0	**0**	**0**
0	1	0	0	0	0	0	1	0	0	**0**	**0**
0	1	0	0	0	1	0	1	0	0	**0**	**0**
0	1	0	0	1	0	0	1	0	0	**0**	**0**
0	1	0	0	1	1	0	1	0	0	**0**	**0**
0	1	0	1	0	0	0	0	0	1	1	1
0	1	0	1	0	1	0	0	0	0	1	0
0	1	0	1	1	0	0	0	0	1	1	1
0	1	0	1	1	1	0	0	0	0	1	0
0	1	1	0	0	0	0	1	1	0	**0**	**0**
0	1	1	0	0	1	0	1	1	0	**0**	**0**
0	1	1	0	1	0	0	1	0	0	0	1
0	1	1	0	1	1	0	1	0	0	0	1
0	1	1	1	0	0	0	0	1	1	1	0
0	1	1	1	0	1	0	0	1	0	1	1
0	1	1	1	1	0	0	0	0	1	1	1
0	1	1	1	1	1	0	0	0	0	1	0
1	0	0	0	0	0	1	0	0	0	**0**	**0**
1	0	0	0	0	1	1	0	0	0	**0**	**0**
1	0	0	0	1	0	1	0	0	0	**0**	**0**
1	0	0	0	1	1	1	0	0	0	**0**	**0**
1	0	0	1	0	0	1	0	0	1	**0**	**0**
1	0	0	1	0	1	1	0	0	0	0	1
1	0	0	1	1	0	1	0	0	1	**0**	**0**
1	0	0	1	1	1	1	0	0	0	0	1
1	0	1	0	0	0	0	0	1	0	1	0
1	0	1	0	0	1	0	0	1	0	1	0
1	0	1	0	1	0	0	0	0	0	1	1
1	0	1	0	1	1	0	0	0	0	1	1
1	0	1	1	0	0	0	0	1	1	1	0
1	0	1	1	0	1	0	0	1	0	1	1
1	0	1	1	1	0	0	0	0	1	1	1
1	0	1	1	1	1	0	0	0	0	1	0
1	1	0	0	0	0	1	1	0	0	**0**	**0**
1	1	0	0	0	1	1	1	0	0	**0**	**0**
1	1	0	0	1	0	1	1	0	0	**0**	**0**
1	1	0	0	1	1	1	1	0	0	**0**	**0**
1	1	0	1	0	0	1	0	0	1	1	0
1	1	0	1	0	1	1	0	0	0	1	1
1	1	0	1	1	0	1	0	0	1	1	0
1	1	0	1	1	1	1	0	0	0	1	1
1	1	1	0	0	0	0	1	1	0	1	0
1	1	1	0	0	1	0	1	1	0	1	0
1	1	1	0	1	0	0	1	0	0	1	1
1	1	1	0	1	1	0	1	0	0	1	1
1	1	1	1	0	0	0	0	1	1	**0**	**0**
1	1	1	1	0	1	0	0	1	0	0	1
1	1	1	1	1	0	0	0	0	1	0	1
1	1	1	1	1	1	0	0	0	0	**0**	**0**

References

[1] D. Khovratovich and I. Nikolić, "Rotational Cryptanalysis of ARX," in Fast Software Encryption FSE 2010, Lecture Notes in Computer Science, vol. 6147, pp. 333–346, Springer, 2010. DOI: 10.1007/978-3-642-13858-4_19.

[2] D. Khovratovich, I. Nikolić, J. Pieprzyk, P. Sokołowski, and R. Steinfeld, "Rotational Cryptanalysis of ARX Revisited," in Fast Software Encryption, p. 519–536, Springer Berlin Heidelberg, 2015. DOI: 10.1007/978-3-662-48116-5_25.

[3] L. Kraleva, T. Ashur, and V. Rijmen, "Rotational Cryptanalysis on MAC Algorithm Chaskey," in Applied Cryptography and Network Security (M. Conti, J. Zhou, E. Casalicchio, and A. Spognardi, eds.), (Cham), pp. 153–168, Springer International Publishing, 2020. DOI: 10.1007/978-3-030-57808-4_8.

[4] R. Ito, "Rotational Cryptanalysis of Salsa Core Function," in Information Security (W. Susilo, R. H. Deng, F. Guo, Y. Li, and R. Intan, eds.), (Cham), pp. 129–145, Springer International Publishing, 2020. DOI: 10.1007/978-3-030-62974-8_8.

[5] S. Barbero, E. Bellini, and R. Makarim, "Rotational analysis of ChaCha permutation," 2020. https://arxiv.org/abs/2008.13406.

[6] S. Barbero, D. Bazzanella, and E. Bellini, "Rotational Cryptanalysis on ChaCha Stream Cipher," Symmetry, vol. 14, p. 1087, 2022. DOI: 10.3390/sym14061087.

[7] P. Zajac and M. Ondroš, "Rotational Cryptanalysis of GOST with Identical S-boxes," Tatra Mountains Mathematical Publications, vol. 57, no. 1, pp. 1–19, 2013. DOI: 10.2478/tmmp-2013-0032.

[8] A. D. Dwivedi, P. Morawiecki, and S. Wójtowicz, "Differential and Rotational Cryptanalysis of Round-reduced MORUS," in International Conference on Security and Cryptography, 2017. DOI: 10.5220/0006411502750284.

[9] N. Mouha, V. Velichkov, C. De Cannière, and B. Preneel, "The Differential Analysis of S-Functions," in Selected Areas in Cryptography (A. Biryukov, G. Gong, and D. Stinson, eds.), pp. 36–56, Springer, 2011. DOI: 10.1007/978-3-642-19574-7_3.

[10] V. Velichkov, N. Mouha, C. De Cannière, and B. Preneel, "The additive differential probability of arx," in Fast Software Encryption (A. Joux, ed.), (Berlin, Heidelberg), pp. 342–358, Springer Berlin Heidelberg, 2011. DOI: 10.1007/978-3-642-21702-9_20.

[11] A. Biryukov and V. Velichkov, "Automatic search for differential trails in arx ciphers," in Topics in Cryptology – CT-RSA 2014 (J. Benaloh, ed.), pp. 227–250, Springer International Publishing, 2014. DOI: 10.1007/978-3-319-04852-9_12.

[12] S. Yakovliev and D. Kobets, "Rotational Cryptanalysis of Some Complication Functions of ARX Cryptosystems," in Proceedings of International Conference on Innovative Solutions in Software Engineering (ICISSE 2023, Nov. 29–30, 2023, Ivano-Frankivsk, Ukraine), pp. 101–104, Vasyl Stefanyk Precarpathian National University, 2023. [in Ukrainian].

[13] 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.

[14] T. Ashur and Y. Liu, "Rotational Cryptanalysis in the Presence of Constants," IACR Transactions on Symmetric Cryptology, vol. 2016, p. 57–70, Dec. 2016. DOI: 10.13154/tosc.v2016.i1.57-70.

[15] 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.

[16] S. Yakovliev, "Differential Properties of LRX-analogues of Small Constant Multiplication," International Journal of Electronics and Telecommunications, vol. 71, no. 1, pp. 95–100, 2025. DOI: 10.24425/ijet.2025.153550.

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