XS-circuits in Block Ciphers *†

Sergey Agievich
Research Institute for Applied Problems of Mathematics and Informatics
Belarusian State University
agievich@{bsu.by,gmail.com}

Abstract

XS-circuits describe block ciphers that utilize 2 operations: X) bitwise modulo 2 addition of binary words and S) substitution of words using key-dependent S-boxes with possibly complicated internal structure. We propose a model of XS-circuits which, despite the simplicity, covers a rather wide range of block ciphers. In our model, several instances of a simple round circuit, which contains only one S operation, are linked together and form a compound circuit called a cascade. S operations of a cascade are interpreted as independent round oracles. We deal with diffusion characteristics of cascades. These characteristics are related to the cryptographic strength of corresponding block ciphers. We obtain results on invertibility, transitivity and 2-transitivity of mappings induced by round circuits and their cascades. We provide estimates on the first and second activation times where the ith activation time is the minimum number of rounds which guarantees that at least i round oracles get different queries while processing two different cascade's inputs. The activation times are related to differential cryptanalysis. We introduce the similarity and duality relations between round circuits. Cascades of related circuits have the same or dual diffusion characteristics. We find canonical representatives of classes of similar circuits and show that the duality between circuits is related to duality between differential and linear attacks against corresponding block ciphers. We discuss families of circuits with growing number of inputs. Such families can be used to build wide-block ciphers.

Keywords: block cipher, round permutation, S-box, circuit, diffusion, transitivity, 2-transitivity.

1 Introduction

A circuit is a directed acyclic graph that describes some algorithm. Leaves of the circuit are inputs of the algorithm, non-leaves are either intermediate results or outputs. Non-leaves are labeled by symbols of operations. The configuration when a vertex v with a label O receives arcs from vertices $u_1, u_2, \ldots$ means that $v = \mathsf{O}(u_1, u_2, \ldots)$.

Many symmetric cryptographic algorithms can be described by circuits in which vertices are binary words of particular length m and operations belong to the following set:

R) cyclic shift (rotation);

*This is an extended version of the paper submitted to the CTCrypt'18 workshop (May 28-30, 2018, Suzdal, Russia). Additionally contains Sections 8, 9, 10.

†Related programs and materials can be found here: https://github.com/agievich/xs.

X) bitwise modulo 2 addition;

A) addition of words as integers modulo 2^m;

L) bitwise logical AND and OR;

M) multiplication of words as elements of the field of order 2^m;

S) substitution of words with preservation of their length m.

Here R and S are unary operations, they are parametrized by a shift value and a substitution rule respectively. All other operations are binary. For small m, S is usually implemented using so-called table S-boxes through table lookup.

Different combinations of operations give different types of circuits. Some of them, for example, circuits of types ARX and LRX, have gained much attention in the last decade. In the circuits mentioned, the operation S is intentionally not used to avoid table lookup. That is because in modern processors the time of lookup can depend on the sequence of lookup queries and this dependence forms the basis for mounting timing attacks. But S should not only mean table S-boxes. The operation S can represent a complex cryptographic transformation, possibly built using another circuit with a smaller length of processing words. The internal circuit of S can be of type ARX or LRX and, therefore, be protected against timing attacks.

The simplest nontrivial circuits with the operation S are the circuits of type XS. They describe, for example, Feistel ciphers or encryption modes like CBC. In the first case, S is instantiated by round functions with (in general) different round keys. In the second case, S is itself a block cipher with some fixed key.

The examples above are typical. In the examples, S describes a key-dependent and therefore a priori secret transformation. Following the cryptographic tradition, we say that S is instantiated by an *oracle* S: its response $v = S(u)$ to a query u can be determined only by querying.

In most cases below we require that S is bijective. Responses of such an oracle are weakly connected with each other: S returns different v when processing different u. That is the only a priori information on responses. For bijective S, we allow access to the inverse oracle S^{-1} which on a query v gives a response u.

If a circuit contains several operations S, then they can be instantiated by independent oracles $S_1, S_2, \ldots$ or by multiple identical instances of a single oracle S. Feistel ciphers are described by circuits of the first type (call them *inhomogeneous*), encryptions modes by circuits of the second type (*homogeneous*).

A circuit of a block cipher usually contains multiple identical parts connected consecutively. These parts represent round permutations of the cipher. Further we consider the simplest round circuits which contain only one S operation. In Section 2 we provide a matrix model of such circuits. Similar models were proposed in [1, 3, 5, 16]. Our model is stricter, and due to this fact we obtain more targeting and precise results. In Section 4 we introduce cascades, that is, inhomogeneous compositions of round circuits. Sections 5, 6, 8 deal with diffusion characteristics of cascades. These characteristics are related to cryptographic strength of corresponding block ciphers. Sections 7 and 9 are devoted to the similarity and duality relations between round circuits. Cascades of related circuits have the same or dual diffusion characteristics. We find canonical representatives of classes of similar circuits and show that duality between circuits is related to duality between differential and linear attacks against

corresponding block ciphers. In Section 10 we discuss families of circuits with growing number of inputs. Such families can be used to build wide-block ciphers.

As a final remark, there is only one step from XS- to XMS-circuits. A circuit of the latter type is used, for example, in the AES block cipher. Usually XMS-circuits are classified as XLS where L stands not for logical operations but for linear transformations over tuples of underlying words. Actually, these transformations are described by circuits of type XM, so the overall XLS-circuit indeed has type XMS in our notations. It is interesting that XMS-circuits are also extensively used in message authentication algorithms like GCM [18]. In these algorithms, S is a block cipher with a fixed key (the homogeneous case).

2 Preliminaries

Consider a circuit with the same number n of inputs and outputs. Call n its *dimension*. Let $x_1, \ldots, x_n$ be inputs and $y_1, \ldots, y_n$ be outputs. They are binary words of length m which we interpret as elements of the field $\mathbb{F}_{2^m}$. In most cases, the specific value of m does not matter, so we usually write F instead of $\mathbb{F}_{2^m}$. Arrange inputs and outputs into the vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$.

Elements of F can be added together using the operation X and substituted separately using the operation S. To simplify notations for sums, we multiply each potential summand by zero or unity of the field F and sum all the resulting products. Multiplication by 1 means inclusion into the sum, multiplication by 0 means exclusion.

We call the number of S operations used in the circuit its *S-complexity*. Further we concentrate mainly on the circuits of S-complexity 1. From these simplest circuits a circuit of arbitrary complexity can be built.

For each instantiation of its S operations, the circuit induces a mapping $F^n \to F^n \colon x \mapsto y$. We are mainly interested in such a circuit that all these mappings are invertible. Two circuits of the same S-complexity are equivalent if their mappings are necessarily identical under identical instantiations. Among all pairwise equivalent circuits, find one which contains the minimum number of X operations. Call this number the *X-complexity* and assign it to all circuits of the equivalence class.

A circuit of dimension n and S-complexity 1 can be described by three parameters: a column vector $a = (a_1, \ldots, a_n)^T$, a matrix $B = (b_{ij})$, $i, j = 1, \ldots, n$, and a row vector $c = (c_1, \ldots, c_n)$. Coordinates of the vectors and elements of the matrix belong to the set $\{0, 1\} \subset F$. Despite binarity, a, B and c can be used in operations with arbitrary vectors and matrices over F.

The parameters (a, B, c) and an oracle S, some instantiation of S, describe the following mapping $x \mapsto y$:

1) $u \leftarrow a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$;

2) $v \leftarrow S(u)$;

3) for $i = 1, \ldots, n$: $y_i \leftarrow b_{1i} x_1 + b_{2i} x_2 + \ldots + b_{ni} x_n + c_i v$.

Denote this mapping by $(a, B, c)[S]$. It can be written in the matrix form:

$$(a, B, c)[S](x) = xB + S(xa)c.$$

Let us exclude from consideration zero vectors a and c, because with them the S-complexity actually reduces to 0. Indeed, if $a = 0$ then S gets only one (zero) query, and if $c = 0$ then S is not queried at all.

It is convenient to encode the parameters (a, B, c) by the matrix

$$\begin{pmatrix} B & a \\ c & 0 \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} & a_1 \\ b_{21} & b_{22} & \dots & b_{2n} & a_2 \\ \dots & \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nn} & a_n \\ c_1 & c_2 & \dots & c_n & 0 \end{pmatrix}.$$

Call it the *extended matrix* of the circuit. In Table 1 we provide extended matrices of some well-known circuits.

In each column of an extended matrix there is at least one unity (otherwise, either the corresponding circuit zeroizes some output coordinate or $a = 0$). Under direct implementation of the extended matrix, each next unity in the column requires an extra X addition. From here we obtain the upper bound on the X-complexity of (a, B, c): the number of unities in its extended matrix minus the number of columns.

Returning to Table 1, the Feistel, GFN1, Matsui and SkipjackX circuits all have X-complexity 1. The X-complexity of LaiMassey, SMS4 and MARS3 is equal to 3.

3 Invertibility

We have agreed to concentrate on circuits that induce invertible mappings. Let us give a formal definition.

Definition 1. A circuit (a, B, c) with nonzero a and c is *invertible* if the corresponding mapping $(a, B, c)[S]$ is invertible for any bijective oracle S over any field $F = \mathbb{F}_{2^m}$.

Theorem 1. A circuit (a, B, c) of dimension n is invertible if and only if one of the following cases holds:

1. The matrix B is invertible and $cB^{-1}a = 0$.
2. The matrices B, $(B\ a)$ and $\binom{B}{c}$ have ranks $n-1$, n and n respectively.

In the second case, the extended matrix of the circuit is invertible.

Proof. Let us consider 2 cases: B is invertible or not.

1. Let B be invertible. Then $yB^{-1} = x + S(xa)cB^{-1}$ and $yB^{-1}a = xa + S(xa)cB^{-1}a$.

1.1. If $cB^{-1}a \neq 0$ then

$$xa + S(xa) = yB^{-1}a.$$

For the circuit to be invertible it is necessary that for any $v = yB^{-1}a$ there exists a solution $u = xa$ of the equation $u + S(u) = v$. But the mapping $u \mapsto u + S(u)$ can be non-bijective (that is, S may not be a complete mapping), and the target equation may not have solutions for a certain v.

1.2. If $cB^{-1}a = 0$ then $xa = yB^{-1}a$ and inversion is defined by the equation

$$x = yB^{-1} + S(yB^{-1}a)cB^{-1}.$$

2. Let B be non-invertible. To determine x from $y = xB + S(xa)c$ it is necessary to get the response $S(xa)$ of S. This response can be obtained either directly from y or indirectly by determining xa from y and then using the query xa to S.

Table 1: Extended matrices of XS-circuits of S-complexity 1

Circuit	Extended matrix	Comments
Feistel	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	Used in the Lucifer and DES block ciphers which were developed under the direction of H. Feistel [11].
LaiMassey	$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$	Used by Lai X. and J. Massey in the IDEA block cipher [13].
Matsui	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	Used by M. Matsui in the MISTY2 block cipher [17].
SkipjackA	$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$	Used in the Skipjack block cipher [19]. Describes its first and third 8-round cascades.
SkipjackB	$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$	Describes the second and forth 8-round cascades of Skipjack.
MARS3	$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$	Used in the MARS block cipher [6]. In the specification of MARS the circuit is called the type-3 Feistel network. We modify the original circuit by replacing two operations A by X.
SMS4	$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$	Used in the SMS4 block cipher [10].
GFN1	$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 & 1 \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}$	The generalization of Feistel to an arbitrary dimension. Introduced in [24] under the name Generalized Feistel Network of type 1.
SkipjackG	$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 1 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}$	The generalization of the Skipjack circuits to an arbitrary dimension. Proposed in [22].

2.1. To determine xa from y there must exist a row vector $\alpha \in F^n$ such that $B\alpha = a$, $c\alpha = 0$ and consequently $xa = y\alpha$. After determining $u = xa$ we can find $v = S(u)$ and obtain the equation $x(B\ a) = (y + vc, u)$ in x. This equation can have more than one solution since the matrix $(B\ a)$ does not have full rank. Indeed, B is not invertible and $a = B\alpha$ is a linear combination of columns of B.

2.2. Suppose that $S(xa)$ can be determined by y. Then α has to satisfy the equations $B\alpha = 0$ and $c\alpha = 1$ which can be used to calculate $v = S(xa) = y\alpha$ and $u = xa = S^{-1}(v)$. After determining u, we again obtain the equation $x(B\ a) = (y + vc, u)$. In order that this equation has a unique solution, the matrix $(B\ a)$ has to have full rank. If $\operatorname{rank}(B\ a) = n$ then $\operatorname{rank} B = n - 1$. Therefore, all nonzero row vectors $\beta \in F^n$ such that $B\beta = 0$ are collinear to α. Since $c\alpha = 1$ and consequently $c\beta \neq 0$, $\operatorname{rank}\binom{B}{c} = n$.

3. If $\operatorname{rank} B = n - 1$ and $\operatorname{rank}(B\ a) = \operatorname{rank}\binom{B}{c} = n$ then the extended matrix $\left(\begin{smallmatrix} B & a \\ c & 0 \end{smallmatrix}\right)$ has full rank. Indeed, none of the rows of $(B\ a)$ can be expressed as a linear combination of other rows. In case the row $(c\ 0)$ is a linear combination of rows of $(B\ a)$, the vector c is a linear combination of rows of B. But it contradicts the fact that $\binom{B}{c}$ has full rank. □

We refer the circuits which correspond to the different cases of Theorem 1 as circuits of type I and type II respectively. From the proof above it follows that a type I circuit is invertible even if its oracle S is not bijective. In Table 1 only the SkipjackX and Matsui circuits are of type II.

Theorem 2. For an invertible circuit (a, B, c) with an oracle S the inverse mapping $(a, B, c)[S]^{-1}$ is again determined by an XS-circuit of S-complexity 1. This inverse circuit is defined as follows:

1. In the first case of Theorem 1 the inverse circuit uses the same oracle S and its description is $(B^{-1}a, B^{-1}, cB^{-1})$.

2. In the second case of Theorem 1 the inverse circuit uses the inverse oracle S^{-1} and its extended matrix is inverse of the extended matrix of (a, B, c).

Proof. Let us continue the previous proof. The inverse circuit of the first case was already described in clause 1.2. Consider the second case.

The left bottom element of the inverted extended matrix must be 0:

$$\begin{pmatrix} B & a \\ c & 0 \end{pmatrix}^{-1} = \begin{pmatrix} D & \alpha \\ \gamma & 0 \end{pmatrix}.$$

Indeed, otherwise $B\alpha = a$ which contradicts the fact that $(B\ a)$ has full rank.

Return to the equation $x(B\ a) = (y + vc, u)$ of clause 2.2. Multiplying both parts of this equation by the matrix $\binom{D}{\gamma}$ we obtain

$$x = yD + vcD + u\gamma.$$

The required result follows from the fact that $cD = 0$ and $u = S^{-1}(v) = S^{-1}(y\alpha)$. □

Further we denote the inverse of a circuit (a, B, c) by $(a, B, c)^{-1}$.

Example 1. The matrix B of the GFN1 circuit is a special circulant: multiplication of a row (column) vector on the right (left) by B causes left (right) cyclic shift of the vector. The matrix B^{-1} induces

cyclic shifts in the reverse direction. Therefore, the extended matrix $\left(\begin{smallmatrix} B^{-1} & B^{-1}a \\ cB^{-1} & 0 \end{smallmatrix}\right)$ of $\mathsf{GFN1}^{-1}$ has the form

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 1 & 0 & 0 & \dots & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

The extended matrix of $\mathsf{SkipjackG}^{-1}$:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 1 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 1 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

□

4 Regularity

Combine several instances of a circuit (a, B, c) by connecting one instance's output to the next instance's input. Call the resulting XS-circuit a *cascade*. Its dimension is the dimension of the underlying circuit (a, B, c). The cascade is invertible if (a, B, c) is invertible.

In cryptography, instances, parts of a cascade, are usually called *rounds*. We suppose that rounds use independent oracles $S_1, S_2, \dots$ or, in other words, cascades are inhomogeneous XS-circuits. Suppose also that round oracles are bijective.

Let $(a, B, c)^t$ be the t-round cascade. Its S-complexity equals t and X-complexity does not exceed the the total X-complexity of the rounds. If $(a, B, c)^t$ is invertible then its inverse is the t-round cascade $(a, B, c)^{-t}$ which contains t rounds of $(a, B, c)^{-1}$ and also has S-complexity t.

Setting some $y(0) \in F^n$ as the cascade input, we obtain $y(1) \in F^n$ after the first round, $y(2) \in F^n$ after the second one and so on. Let $(a, B, c)^t[S_1, \dots, S_t]$ be the mapping $y(0) \mapsto y(t)$ induced by the cascade $(a, B, c)^t$ with oracles $S_1, \dots, S_t$.

Round outputs satisfy the following equations:

$$y(t) = y(0)B^t + \sum_{\tau=1}^{t} S_\tau(y(\tau-1)a)cB^{t-\tau}, \quad t = 1, 2, \dots.$$

They can be rewritten as follows:

$$\begin{aligned} y(t) &= y(0)B^t + \sum_{\tau=1}^{t} v(\tau)cB^{t-\tau}, \\ v(t) &= S_t(u(t)), \\ u(t) &= y(0)B^{t-1}a + \sum_{\tau=1}^{t-1} v(\tau)cB^{t-1-\tau}a, \quad t = 1, 2, \dots. \end{aligned}$$

Here $u(1), \dots, u(t)$ is the *trace of queries* and $v(1), \dots, v(t)$ is the *trace of responses*. More precisely, we deal with *t-traces*. Since round oracles are independent, there exist $|F|^t$ different t-traces of each type.

In the cryptographic context, each cascade's round has to establish complex dependencies between certain coordinates of input and output vectors and simultaneously has to shuffle all the coordinates. Using related terms of Shannon, rounds are responsible for confusion and diffusion. In our case confusion is managed by round oracles, diffusion is maintained by the round circuit (a, B, c) itself.

Further we introduce several characteristics of diffusion. In particular, we will analyze how a cascade processes not one but two vectors: $y(0)$ and $y'(0)$. The additional vector $y'(0)$ produces an additional sequence $y'(1), y'(2), \ldots$ of round outputs. This sequence induces an additional trace of queries and is induced by an additional trace of responses. A query $u'(t)$ and, consequently, a corresponding response $v'(t)$ can differ from $u(t)$ and $v(t)$. Traces are *compatible*, that is, each oracle returns the same responses to the same queries and different responses to different queries.

We are interested in the dynamics of the *differences*

$$\Delta y(t) = y(t) + y'(t), \quad \Delta u(t) = u(t) + u'(t), \quad \Delta v(t) = v(t) + v'(t)$$

during the rounds. In the equations above $+$ can be replaced with $-$ (because F is a field of characteristic 2), that is why the term "difference" is relevant.

The difference $\Delta u(t)$ is the input difference of S_t, $\Delta v(t)$ is the output one. The relation between these differences can be written as follows:

$$\Delta v(t) = \Delta S_t(\Delta u(t)).$$

The compatibility of traces means that $\Delta v(t) = 0$ if and only if $\Delta u(t) = 0$.

In cryptography, the event $\Delta u(t) \neq 0$ is called the *activation* of S_t. In case of the activation, the output difference $\Delta v(t)$ is hard to predict during cryptanalysis. The more activations a cascade guarantees while processing different $y(0)$ and $y'(0)$, the higher quality of diffusion.

Relations between differences are derived from the previous equations by inserting the symbol Δ before the expressions $y(t)$, $y(0)$, $v(\tau)$, $v(t)$, S_t, $u(t)$, etc. For example,

$$\Delta u(t) = \Delta y(0) B^{t-1} a + \sum_{\tau=1}^{t-1} \Delta v(\tau) c B^{t-1-\tau} a.$$

Definition 2. The *lag* of a circuit (a, B, c) is the minimum positive integer l such that $cB^{l-1}a = 1$.

The lag l characterizes the relationship between a query $u(t)$ and previous responses $v(1), \ldots, v(t-1)$: For a suffuciently large t the query $u(t)$ depends on $v(t-l)$ but not on $v(t-l+1), \ldots, v(t-1)$. The smaller the lag, the higher quality of diffusion because unpredictable oracle's responses are used faster to create new queries. The lag also characterizes the relationship between $\Delta u(t)$ and $\Delta v(1), \ldots, \Delta v(t-1)$.

Circuits that provide reasonable (rational) diffusion are described by the following definitions. Further we justify the relevance of the requirements of these definitions.

Definition 3. An invertible circuit (a, B, c) of dimension n is *regular* if the following conditions hold:

1) the matrix $C = \begin{pmatrix} cB^{n-1} \\ \cdots \\ cB \\ c \end{pmatrix}$ is invertible;

Table 2: Lags of the regular standard circuits

Circuit	Lag	Inverse lag	Sum of lags
Feistel	1	1	2
Matsui	2	1	3
SkipjackA	1	4	5
SkipjackB	4	1	5
MARS3	1	1	2
SMS4	1	1	2
GFN1	1	$n-1$	n
SkipjackG	1	n	$n+1$

2) the matrix $A = \begin{pmatrix} a & Ba & \dots & B^{n-1}a \end{pmatrix}$ is invertible.

Definition 4. A circuit (a, B, c) of dimension n is *strongly regular* if it is regular and additionally

3) the matrix $C_l = \begin{pmatrix} cB^{(n-1)l} \\ \dots \\ cB^l \\ c \end{pmatrix}$ is invertible. Here l is the lag of (a, B, c).

The forthcoming Corollary 3 shows that the lag of a regular circuit doesn't exceed its dimension. Therefore, in the last definition, l is finite and the third condition is correct.

Trivially, if a regular circuit has lag 1 then this circuit is strongly regular. Further we prove more complicated facts, for example, the fact that mutually inverse circuits are both regular or both non-regular (Corollaries 1 and 2). Despite this fact, the following example shows that mutually inverse circuits are not necessarily strongly regular simultaneously.

Example 2. FourCell is a circuit proposed in [8]. Its extended matrix has the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

FourCell has lag 4. The circuit is regular but not strongly regular. The inverse circuit has lag 1 and therefore is strongly regular. □

All circuits of Table 1 except LaiMassey are strongly regular. In Table 2 we report their lags as well as *inverse lags*, that is, lags of inverse circuits. The lags of $\mathsf{GFN1}^{-1}$ and $\mathsf{SkipjackG}^{-1}$ are easily calculated using Example 1.

5 Transitivity

Definition 5. A cascade $(a, B, c)^t$ of dimension n is *transitive* if for any $\alpha, \beta \in F^n$ there exist round oracles $S_1, \dots, S_t$ such that

$$(a, B, c)^t[S_1, \dots, S_t](\alpha) = \beta.$$

A circuit (a, B, c) is *transitive* if $(a, B, c)^t$ is transitive for some t. The minimal such t is the *index of transititvity* of (a, B, c).

Transitivity indeed characterizes diffusion in the sense that for a sufficiently large t any $y(t)$ is reachable from any $y(0)$. The smaller the index of transitivity, the faster diffusion.

Example 3. The LaiMassey circuit maps $x = (x_1, x_2)$ to

$$y = (y_1 + S(x_1 + x_2), y_2 + S(x_1 + x_2)).$$

This mapping saves the sum of coordinates: $y_1 + y_2 = x_1 + x_2$. The sum is not being changed during all further rounds and therefore the circuit is not transitive. □

Theorem 3. The index of transitivity of a circuit (a, B, c) does not exceed its dimension n. The index equals n if and only if the first condition of regularity (invertibility of C) holds.

Proof. Let α, β be arbitrary elements of F^n. The number of vectors $y(t)$ reachable from $y(0) = \alpha$ does not exceed the number of t-traces of responses. With $t < n$ this number is less than $|F^n|$ and therefore there exists unreachable $y(t)$. Consequently, the index of transitivity cannot be less than n.

Let C be invertible. Then there exists a unique vector $v = (v(1), \ldots, v(n)) \in F^n$ such that

$$vC = \alpha B^n + \beta.$$

The responses $v(1), \ldots, v(n)$ transfer $y(0) = \alpha$ to $y(n) = \beta$:

$$y(n) = y(0)B^n + \sum_{\tau=1}^{n} v(\tau)cB^{n-\tau} = \alpha B^n + vC = \beta.$$

Therefore, $(a, B, c)^n$ is transitive.

Let $(a, B, c)^n$ be transitive. Suppose by contradiction that C is not invertible. Then there exist $\alpha, \beta \in F^n$ such that the equation $vC = \alpha B^n + \beta$ does not have solutions in v. It means that no trace of responses transfers $y(0) = \alpha$ to $y(n) = \beta$, a contradiction. □

Note that transitivity does not require invertibility. For example, a circuit of dimension 1 which maps x_1 to $x_1 + S(x_1)$ is transitive but not invertible. However, below we need invertibility.

Corollary 1. The first condition of regularity holds for an invertible circuit (a, B, c) if and only if it holds for the inverse circuit $(a, B, c)^{-1}$.

Proof. By definition, mutually inverse circuits are transitive simultaneously, their indices of transitivity coincide. The required result follows from the second part of Theorem 3. □

Call a binary operation *Latin* if its table is a Latin square or, in other words, if the operation induces a quasigroup on the underlying set. Latin operations are often used in cryptography, for example, to instantiate round oracles using round keys, as in the following theorem. The theorem means that a circuit which dimension n is equal to its index of transitivity can be used to extend a Latin operation on F to a Latin operation on F^n.

Theorem 4. Let a cascade $(a, B, c)^n$ of dimension n be transitive and use the oracles

$$S_t^k(u) = S(u * k_t), \quad u \in F, \quad t = 1, \ldots, n,$$

where $k = (k_1, \ldots, k_n) \in F^n$, S is a fixed permutation on F, and $*$ is a Latin operation on F. Then the operation

$$O\colon F^n \times F^n \to F^n,\ (\alpha, k) \mapsto (a, B, c)^n[S_1^k, \ldots, S_n^k](\alpha)$$

is Latin too.

Proof. Firstly, due to transitivity of $(a, B, c)^n$ there exists a unique n-trace of responses which transfers any given α to any given β. Since $*$ is Latin, this trace unambiguously determines k, that is, the equation $O(\alpha, k) = \beta$ has a unique solution in k. Secondly, due to invertibility any given β and k unambiguously determine α, that is, the equation $O(\alpha, k) = \beta$ has a unique solution in α. In result, O induces a quasigroup on F^n. □

6 2-transitivity

Definition 6. A cascade $(a, B, c)^t$ of dimension n is 2-*transitive* if for any distinct $\alpha, \alpha' \in F^n$ and any distinct $\beta, \beta' \in F^n$ there exist round oracles $S_1, \ldots, S_t$ such that

$$(a, B, c)^t[S_1, \ldots, S_t](\alpha) = \beta, \quad (a, B, c)^t[S_1, \ldots, S_t](\alpha') = \beta'.$$

2-transitivity is an important diffusion property of cascades. In particular, 2-transitivity of $(a, B, c)^t$ implies absence of so-called *impossible differentials*, that is, unrealizable transitions from some difference $\Delta y(0) = \Delta\alpha$ to some difference $\Delta y(t) = \Delta\beta$. Such transitions can be used to mount impossible differential attacks.

In addition, 2-transitivity helps to determine the permutation group generated by the mappings $(a, B, c)[S]$, where S runs over all bijections over F. Usually, 2-transitivity is a serious evidence that this group is the alternating group. It is the largest achievable group (for $n \geq 2$), its appearance demonstrates the welcomed diversity of the mappings $(a, B, c)[S]$.

Unfortunately, 2-transitivity is a rather complicated property which cannot be supported by such a simple criterion as in the case of transitivity (Theorem 3). Let us introduce a weakened version of 2-transitivity.

Definition 7. A cascade $(a, B, c)^t$ of dimension n is *weakly* 2-*transitive* if there do not exist nonzero $\Delta\alpha, \Delta\beta \in F^n$ such that $(a, B, c)^t[S_1, \ldots, S_t]$ necessarily, independently of the choice of the round oracles, tranfers the difference $\Delta y(0) = \Delta\alpha$ to the difference $\Delta y(t) = \Delta\beta$.

As before, a circuit (a, B, c) is *(weakly)* 2-*transitive* if $(a, B, c)^t$ is (weakly) 2-transitive for some t. The minimal such t is the *index of (weak)* 2-*transitivity.*

Example 4. Let us continue Example 3. The LaiMassey circuit is not weakly 2-transitive. Indeed, for any nonzero $\Delta\gamma \in F$ the difference $\Delta x = (\Delta\gamma, \Delta\gamma)$ goes to the difference $\Delta y = (\Delta\gamma, \Delta\gamma)$. This difference is being saved during all further rounds. □

Note that (weak) 2-transitivity, as well as transitivity, does not require invertibility.

Theorem 5. The index of weak 2-transitivity of a circuit (a, B, c) does not exceed its dimension n. The index equals n if and only if the second condition of regularity (invertibility of A) holds.

Proof. A cascade $(a, B, c)^t$ is not weakly 2-transitive if and only if there exists a nonzero input difference $\Delta y(0)$ which induces the zero vector $\Delta u = (\Delta u(1), \ldots, \Delta u(t))$ of internal differences between queries to the round oracles. The vector Δu must exist because once two queries to some oracle S_τ are distinct, the corresponding responses are distinct too and the output difference $\Delta y(t)$ depends on the difference $\Delta v(\tau)$ between these responses. Note that if $\Delta u = 0$, then the differences $\Delta v(1), \ldots, \Delta v(t)$ are zero too. This fact can be written as

$$\Delta y(0) \begin{pmatrix} a & Ba & \ldots & B^{t-1}a \end{pmatrix} = 0.$$

If $t < n$, then the last equation has a nonzero solution in $\Delta y(0)$. This solution induces zero Δu and $(a, B, c)^t$ is not weakly 2-transitive. This proves the first part of the theorem.

If $A = \begin{pmatrix} a & Ba & \ldots & B^{n-1}a \end{pmatrix}$ is invertible then $(a, B, c)^n$ is weakly 2-transitive. Indeed, otherwise $\Delta y(0)A = 0$ for some nonzero $\Delta y(0)$, which is impossible.

Conversely, if $(a, B, c)^n$ is weakly 2-transitive then A is invertible. Indeed, otherwise there exists a nonzero $\Delta y(0)$ which induces $\Delta u = 0$. □

Corollary 2. The second condition of regularity holds for an invertible circuit (a, B, c) if and only if it holds for the inverse circuit $(a, B, c)^{-1}$.

Proof. By definition, mutually inverse circuits are weakly 2-transitive simultaneously, their indices of weak 2-transitivity coincide. The required result follows from the second part of Theorem 5. □

Theorem 6. Let circuits (a, B, c) and $(a, B, c)^{-1}$ of dimension n be strongly regular and

$$\left(1 - \frac{2}{|F|}\right)^{n-1} \left(1 - \frac{1}{|F|}\right) > \frac{1}{2}.$$

Then the circuits are 2-transitive and their indices of 2-transitivity do not exceed

$$2n + (n-1)(l + l'),$$

where l is the lag of (a, B, c) and l' is the lag of $(a, B, c)^{-1}$.

Proof. From the proof of Theorem 5 it follows that for any nonzero input difference $\Delta y(0)$ there exists $r \leq n$ such that $\Delta u(r)$, the difference between queries to S_r, is nonzero. The corresponding difference $\Delta v(r) = \Delta \mathsf{S}_r(\Delta u(r))$ between responses is nonzero too.

Let r be the first round when $\Delta u(r) \neq 0$. By definition of lag

$$\begin{aligned} \Delta u(r+l) &= \Delta v(r) + \Delta y(0) B^{r+l-1} a + \sum_{\tau=1}^{r-1} \Delta v(\tau) c B^{r+l-1-\tau} a \\ &= \Delta v(r) + \Delta y(0) B^{r+l-1} a. \end{aligned}$$

Manipulating responses of S_r (round oracles are free to choose which response to give), we obtain different $\Delta v(r)$. At least $|F| - 2$ of them provide $\Delta u(r+l) \neq 0$.

Having a nonzero $\Delta u(r+l)$, we tune a nonzero $\Delta v(r+l)$ to achieve a nonzero $\Delta u(r+2l)$. Continue in such a manner until the round number $r + (n-1)l$. In this round, we do not require that $\Delta u(r+nl) \neq 0$ and have $|F| - 1$ ways to choose $\Delta v(r + (n-1)l)$.

Thus, there exist at least $(|F| - 2)^{n-1}(|F| - 1)$ vectors

$$\Delta v = (\Delta v(r), \Delta v(r+l), \ldots, \Delta v(r + (n-1)l))$$

Table 3: Bounds on the indices of 2-transitivity

Circuit	Upper bound (Theorem 6)	Lower bound
Feistel	6	6 [12]
Matsui	7	
SkipjackA	22	17 [3]
SkipjackB	22	17 [3]
MARS3	14	12 [15]
SMS4	14	12 [15]
GFN1 ($n = 4$)	20	20 [9]
SkipjackG ($n = 4$)	22	17 [15]

with nonzero coordinates.

Let the oracles S_t, $t \neq r + il$, implement the identity mapping, that is, they output input queries. Then

$$\Delta y(r + (n-1)l) = \Delta y(0)M + \Delta v C_l,$$

where M is some matrix of order n, C_l is the matrix of the definition of strong regularity. Due to the invertibility of C_l, different Δv induce different $\Delta y(r + (n-1)l)$. Therefore, the difference $\Delta y(r + (n-1)l)$ can take at least $(|F| - 2)^{n-1}(|F| - 1)$ distinct values.

To provide the required difference $\Delta v(t)$, $t = r + il$, the oracle S_t first returns an arbitrary $\mathsf{S}_t(u(t))$ and then the specific $\mathsf{S}_t(u'(t)) = \mathsf{S}_t(u(t)) + \Delta v(t)$. By choosing a vector $v = (v(r), v(r + l), \ldots, v(r + (n-1)l))$ of the first responses, achieve that the vector

$$y(r + (n-1)l) = y(0)M + vC_l$$

takes a fixed value $\gamma \in F^n$.

In sum, applying the circuit $(a, B, c)^{r+(n-1)l}$ to a given pair (α, α'), $\alpha \neq \alpha'$, and running over all possible round oracles, we obtain at least $(|F| - 2)^{n-1}(|F| - 1)$ different pairs (γ, z), $z \in F^n$.

The same holds for the inverse circuit $(a, B, c)^{-1}$: The circuit $(a, B, c)^{-r'-(n-1)l'}$, $r' \leq n$, with various round oracles transfers a given pair (β, β'), $\beta \neq \beta'$, to at least $(|F|-2)^{n-1}(|F|-1)$ different pairs (γ, z'), $z' \in F^n$.

Under conditions of the theorem,

$$2(|F| - 2)^{n-1}(|F| - 1) > |F|^n$$

and there must exist a collision $z = z'$. This collision means that the pair (α, α') can be transferred to the pair (β, β') by the circuit $(a, B, c)^{r+r'+(n-1)(l+l')}$. This implies the required result. □

The additional condition of Theorem 6 is not burdensome. It holds for example if $|F| = 2^m > 4n$. In practice, $m \geq 16$, $n \leq 8$ and the condition indeed satisifies.

In Table 3 we present bounds on the indices of 2-transitivity of the standard circuits. Upper bounds are built using Theorem 6 and Table 2. Lower bounds are the quantities $d+1$, where d is the maximum known number of rounds such that an impossible differential for $(a, B, c)^d$ exists.

Note that the upper bounds for SkipjackA and SkipjackB presented in Table 3 should not be transferred on the Skipjack cipher itself. In this cipher 8 SkipjackA rounds are followed by 8 SkipjackB rounds, then again by 8 SkipjackA and 8 SkipjackB rounds.

The proof of Theorem 6 can be easily extended to the case when the last rounds of a cascade differ from the first ones. In particular, using the fact that SkipjackA and $\mathsf{SkipjackB}^{-1}$ both have lag 1, the cascade of first 7 SkipjackA and then 7 SkipjackB rounds is 2-transitive.

It is interesting that although the 14-round cascade $\mathsf{SkipjackA}^7\mathsf{SkipjackB}^7$, as well as 22-round cascades $\mathsf{SkipjackA}^{22}$ and $\mathsf{SkipjackB}^{22}$ are 2-transitive (we multiply round circuits from left to right), the 24-round cascade

$$\mathsf{SkipjackA}^4\mathsf{SkipjackB}^8\mathsf{SkipjackA}^8\mathsf{SkipjackB}^4$$

is not (see [2] for details).

7 Similarity

Definition 8. Circuits (a, B, c) and (a', B', c') of dimension n are *similar* if there exists an invertible $(0,1)$-matrix P of order n such that $a' = P^{-1}a$, $B' = P^{-1}BP$, $c' = cP$.

Similarity means that if $y = (a, B, c)[S](x)$ and $x' = xP$, $y' = yP$ then $y' = (a, B, c)[S](x')$. Indeed, from $y = xB + S(xa)c$ it follows that

$$yP = xPP^{-1}BP + S(xPP^{-1}a)cP$$

or

$$y' = x'B' + S(x'a')c'.$$

The conclusion above is easily extended to several rounds: If $(a, B, c)^t[S_1, S_2, \ldots, S_t]$ transfers $y(0)$ to $y(t)$ then $(a', B', c')^t[S_1, S_2, \ldots, S_t]$ transfers $y'(0) = y(0)P$ to $y'(t) = y(t)P$. It means that similar circuits have the same cryptographic quality. In particular, they have the same type, lag, indices of transitivity and (weak) 2-transitivity, they are (strongly) regular simultaneously. At the same time, mutually similar circuits can have different X-complexity. To reduce the number of X operations, a circuit can be replaced by a similar one.

Similarity is an equivalence relation. It is natural to pose the problem of determining canonical representatives of equivalence classes as well as other classification problems.

Manipulating P and replacing B by $P^{-1}BP$, we can bring B to a convenient matrix canonical form. Let us use the Frobenius normal form:

$$B = \operatorname{diag}(B_1, B_2, \ldots, B_k).$$

Here B_i are Frobenius cells, that is, companion matrices of polynomials $f_{B_i}(\lambda) \in \mathbb{F}_2[\lambda]$. The polynomials divide each other: $f_{B_1}(\lambda) \mid f_{B_2}(\lambda) \mid \ldots \mid f_{B_k}(\lambda)$.

The condition $k = 1$ is necessary for regularity of a circuit. Indeed, by the Cayley–Hamilton theorem the matrix B is a root of f_{B_k}. If $k > 1$, then $\deg f_{B_k} < n$ and some nonzero linear combination of the matrix powers $B^0, B^1, \ldots, B^{n-1}$ drops to zero. But it means that the matrices C and A of the definition of regularity do not have full rank, that is, regularity does not hold.

Further we consider only single-cell canonical matrices B. Such a matrix has the form:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & b_1 \\ 1 & 0 & \dots & 0 & 0 & b_2 \\ 0 & 1 & \dots & 0 & 0 & b_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & b_{n-1} \\ 0 & 0 & \dots & 0 & 1 & b_n \end{pmatrix}.$$

Its characteristic polynomial $f_B(\lambda) = \lambda^n + b_n\lambda^{n-1} + \ldots + b_1$. The coefficient b_1 equals 1 for circuits of type I and 0 for circuits of type II.

Theorem 7. Let (a, B, c) be a circuit of dimension n in which B is a Frobenius cell with a characteristic polynomial $\lambda^n + b_n\lambda^{n-1} + \ldots + b_1$. The circuit is invertible if and only if one of the following cases holds:

1) $b_1 = 1$ and $a_1(b_2c_1 + b_3c_2 + \ldots + b_nc_{n-1} + c_n) + a_2c_1 + a_3c_2 + \ldots + a_nc_{n-1} = 0$;

2) $b_1 = 0$, $a_1 = 1$ and $b_2c_1 + b_3c_2 + \ldots + b_nc_{n-1} + c_n = 1$.

There exist $2^{2n-1} - 3 \cdot 2^{n-1} + 1$ suitable pairs (a, c) in the first case and 2^{2n-2} in the second.

Proof. Let us apply Theorem 1. If $b_1 = 1$ then the invertibility requires that $cB^{-1}a = 0$. The stated result follows from the fact that

$$B^{-1} = \begin{pmatrix} b_2 & 1 & 0 & \dots & 0 \\ b_3 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ b_n & 0 & 0 & \dots & 1 \\ b_1 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

If $b_1 = 0$ then the matrices $(B\ a)$ and $\binom{B}{c}$ must have full rank n. For the first matrix, it is true if and only if $a_1 = 1$. The second matrix has full rank if and only if c cannot be expressed linearly through the last $n-1$ rows of B. It is equivalent to the inequality $b_2c_1 + b_3c_2 + \ldots + b_nc_{n-1} \neq c_n$ written in the statement of the theorem in a slightly different form.

The second case of the last part of the theorem is obvious. To treat the first case, we have to determine the number of pairs (a, c) which make the quadratic form $g(a, c) = cB^{-1}a$ equal to 0. The form g is linearly equivalent to $a_1c_n + a_2c_1 + \ldots + a_nc_{n-1}$ and the required number of pairs is $2^{2n-1} + 2^{n-1}$ (see, for example, [14, Theorem 6.32]). From this number we have to subtract $2^{n+1} - 1$, the number of pairs (a, c) such that $a = 0$ or $c = 0$. □

Let P be a $(0, 1)$-normalizer of B, that is, an invertible matrix such that $P^{-1}BP = B$. Using P, we can bring (a, B, c) to the form $(P^{-1}a, B, cP)$ in which, generally, the vectors a and c are changed but the matrix B is not. In other words, we can refine the canonical form of not only the matrix but also the vectors of circuit's description.

Let $p_1, p_2, \ldots, p_n$ be consecutive rows of P. From the equality $PB = BP$ it follows that

$$\begin{aligned} p_nB &= p_{n-1} + b_np_n, \\ p_{n-1}B &= p_{n-2} + b_{n-1}p_n, \\ &\dots \\ p_2B &= p_1 + b_2p_n. \end{aligned}$$

These equations mean that all rows of P can be expressed through p_n:

$$P = P(p_n) = \begin{pmatrix} p_n M_1 \\ p_n M_2 \\ \cdots\cdots \\ p_n M_n \end{pmatrix}.$$

Here $M_n = E$ and $M_i = BM_{i+1} + b_{i+1}E = B^{n-i} + b_n B^{n-i-1} + \ldots + b_{i+1}E$, $i = n-1, \ldots, 2, 1$, where E is the identity matrix.

Multiplying $P(p_n)$ on the left by an invertible matrix, we can bring it to the form

$$\begin{pmatrix} p_n B^{n-1} \\ p_n B^{n-2} \\ \cdots\cdots\cdots \\ p_n E \end{pmatrix}.$$

With $p_n = c$ this is the matrix C of the definition of regularity. Thus, $P(p_n)$ is invertible if and only if the first condition of regularity holds with $c = p_n$. Moreover, there exists a bijective correspondence between acceptable vectors c of regular circuits (a, B, c) and normalizers P of the matrix B: $c \leftrightarrow P(c)$.

The vector $c = (0, 0, \ldots, 0, 1)$ is acceptable because in the corresponding matrix C the main diagonal contains only unities, all elements above the diagonal are zero and, therefore, C is invertible. A normalizer $P(c')$ transfers a regular circuit (a, B, c) to the similar circuit (a', B, c'). Indeed, $cP(c')$ is the last row of $P(c')$ which is c'. Moreover, only one $P(c')$ transfers c to c' and $a' = P(c')^{-1}a$ is uniquely determined.

This reasoning can be inverted: We can bring a regular circuit (a', B, c') to the form (a, B, c) in which $c = (0, 0, \ldots, 0, 1)$ and a is uniquely determined. Simultaneously, acting in same manner, we can bring (a', B, c') to the form (a, B, c) in which $a = (1, 0, \ldots, 0, 0)^T$ and c is uniquely determined. The chosen a is acceptable because the corresponding matrix A of the definition of regularity equals E.

Gathering all, we obtain the following result.

Theorem 8. A regular circuit is similar to each of the following circuits:

1) $((1, 0, 0, \ldots, 0)^T, B, c)$;

2) $(a, B, (0, 0, \ldots, 0, 1))$.

Here B is a uniquely determined Frobenius cell. The vectors a and c are also uniquely determined.

Theorem 8 provides two canonical forms of regular circuits. These forms are represented schematically in Figures 1 and 2.

Corollary 3. The lag of a regular circuit does not exceed its dimension.

Proof. Since similar circuits have the same lag, it is sufficient to consider a circuit of the first canonical form. If its lag is greater than its dimension n then the first coordinates of $c, cB, \ldots, cB^{n-1}$ are zero. Therefore, C is not invertible which contradicts regularity. $\square$

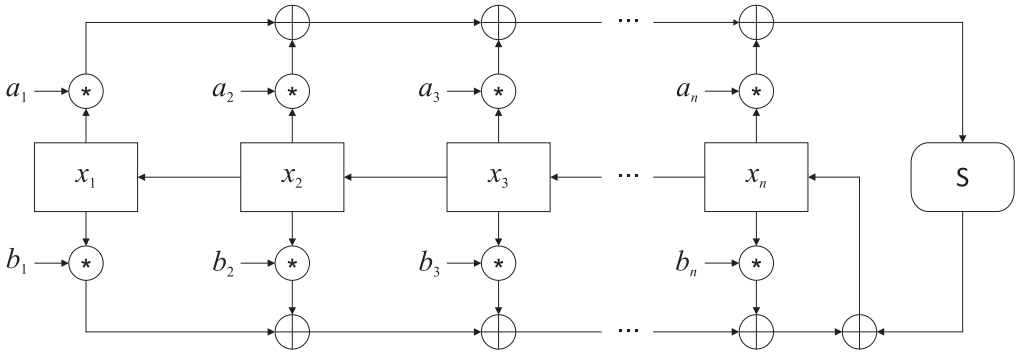

Figure 1: The first canonical form

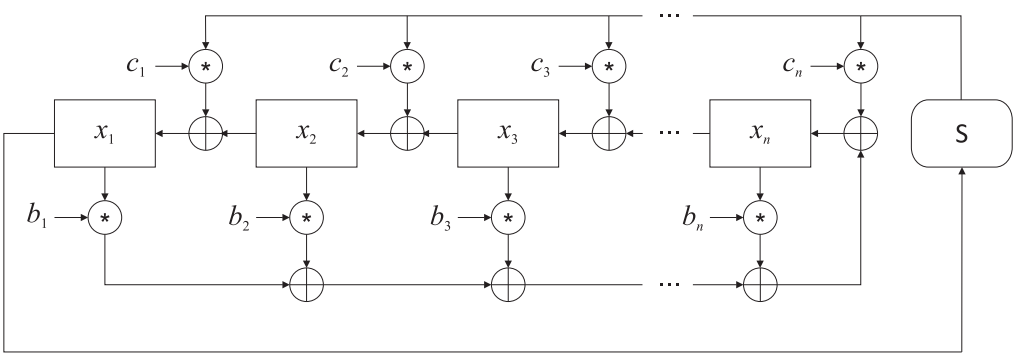

Figure 2: The second canonical form

Let us refine the vectors a and c which can appear in Theorem 8. The number of acceptable vectors a (vectors c) is the number of equivalence classes of regular circuits with similar matrices B.

Identify vectors (row and column) with polynomials: both a vector $w = (w_1, w_2, \ldots, w_n)$ and its transpose are associated with the polynomial $w(\lambda) = w_1 + w_2\lambda + \ldots + w_n\lambda^{n-1}$. In particular, $f_B(\lambda) = \lambda^n + b(\lambda)$, where b is the last column of B.

Theorem 9. Let (a, B, c) be an invertible circuit of dimension n in which B is a Frobenius cell. The circuit is regular if and only if both the polynomials $a(\lambda)$ and $(cP)(\lambda)$ are coprime with $f_B(\lambda)$. Here $P = (p_{ij})$, $1 \le i, j \le n$, where

$$p_{ij} = \begin{cases} b_{i+j}, & i + j \le n, \\ 1, & i + j = n + 1, \\ 0, & i + j > n + 1. \end{cases}$$

Proof. Columns of A are described by the polynomials

$$(B^i a)(\lambda) = \lambda^i a(\lambda) \bmod f_B(\lambda), \quad i = 0, 1, \ldots, n-1.$$

The matrix A is invertible if and only if any nonzero linear combination of its columns is nonzero. In other words, if and only if

$$g(\lambda)a(\lambda) \not\equiv 0 \pmod{f_B(\lambda)}$$

for any nonzero $g(\lambda) \in \mathbb{F}_2[\lambda]$, $\deg g \le n$. It is equivalent to coprimeness of $a(\lambda)$ and $f_B(\lambda)$.

In [20] it was proved that $B = PB^TP^{-1}$. From this fact, taking into account the symmetry of P, it follows that columns of PC^T have the form

$$P(cB^i)^T = P(cP(B^T)^iP^{-1})^T = B^i(cP)^T.$$

Processing PC^T in the same way as A, we conclude the proof. □

Example 5. Let $n \geq 2$ and $f_B(\lambda)$ be irreducible. Then there are $2^{n-1} - 1$ equivalence classes of regular circuits which matrices are similar to B. Indeed, let such a circuit has the first canonical form. By Theorem 7, the circuit is invertible if and only if $c_n = b_2c_1 + b_3c_2 + \ldots + b_nc_{n-1}$. There are $2^{n-1} - 1$ acceptable nonzero c and they all satisfy the conditions of Theorem 9.

It is interesting that if $f_B(\lambda)$ is irreducible then the set of normalizers of B augmented with the zero matrix forms the field of order 2^n. In particular, the sum of distinct normalizers is again a normalizer. □

Example 6. Let $f_B(\lambda) = \lambda^n + 1$. This is the case of the Feistel, SMS4, MARS3 and GFN1 circuits. Normalizers of B are all invertible circulants. In the most interesting case $n = 2^k$, acceptable a, c are those that contain an odd number of unities and both the number of normalizers and equivalence classes is 2^{n-1}.

The SMS4 circuit has the first canonical form, MARS3 has the second one. These circuits are similar: MARS3 can be converted to SMS4 using the normalizer

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

□

Example 7. Let (a, B, c) be a circuit of type II. Bring it to the second canonical form. For invertibility, it is sufficient and necessary that $a(0) = 1$. For regularity, $a(\lambda)$ must additionally be coprime to $f_B(\lambda)$. If $f_B(\lambda) = \lambda^n$ (SkipjackA, SkipjackG) then the last condition holds for every $(a_2, \ldots, a_n)$ and consequently there are 2^{n-1} equivalence classes.

It is interesting that SkipjackB does not belong to the equivalence class of SkipjackA because its polynomial $f_B(\lambda) = \lambda^4 + \lambda \neq \lambda^4$. □

8 Activations

In differential cryptanalysis, differences $\Delta y(0), \Delta y(1), \ldots, \Delta y(t)$ into a cascade $(a, B, c)^t$ are investigated. if for a given $\Delta y(0) = \Delta\alpha(0)$ there exist oracles $S_1, \ldots, S_t$ such that $\Delta y(1) = \Delta\alpha(1), \ldots, \Delta y(t) = \Delta\alpha(t)$ then $\Delta\alpha(0), \Delta\alpha(1), \ldots, \Delta\alpha(t)$ is the (*differential*) *characteristic* of $(a, B, c)^t$.

Let us specify the relationship between adjacent differences of a characteristic. To do this, recall the transfer from $\Delta y(\tau-1)$ to $\Delta y(\tau)$ described in Section 4. If $\Delta y(\tau-1)a = 0$ then the oracle S_τ is not activated. Its input difference $\Delta u(\tau)$ is zero, the output difference $\Delta v(\tau)$ is also zero and $\Delta y(\tau) = \Delta y(\tau-1)B$. If $\Delta y(\tau-1)a \neq 0$ then S_τ is active, its output difference $\Delta v(\tau)$ can take an arbitrary nonzero value $\Delta\delta(\tau)$ and $\Delta y(\tau) = \Delta y(\tau-1)B + \Delta\delta(\tau)c$.

Thus, the differences $\Delta\alpha(0), \Delta\alpha(1), \ldots, \Delta\alpha(t)$ form a characteristic if

$$\Delta\alpha(\tau) = \begin{cases} \Delta\alpha(\tau-1)B, & \Delta\alpha(\tau-1)a = 0, \\ \Delta\alpha(\tau-1)B + \Delta\delta(\tau)c, & \Delta\alpha(\tau-1)a \neq 0, \end{cases} \tag{1}$$

for $\tau = 1, 2, \ldots, t$ and some nonzero $\Delta\delta(\tau) \in F$.

Definition 9. The ith *activation time* of a circuit (a, B, c) is the minimum number of rounds t such that $(a, B, c)^t$ guarantees i activations, that is, each nonzero characteristic $\Delta\alpha(0)$, $\Delta\alpha(1), \ldots, \Delta\alpha(t)$ of $(a, B, c)^t$ contains at least i differences $\Delta\alpha(\tau - 1)$, $1 \le \tau \le t$, such that $\Delta\alpha(\tau - 1)a \neq 0$.

Denote the ith activation time of a circuit (a, B, c) by $\rho_i(a, B, c)$ or simply ρ_i if the circuit is clear from the context.

Weak 2-transitivity of a cascade $(a, B, c)^t$ can be interpreted as a guarantee of 1 activation. Therefore, the index of weak 2-transitivity of (a, B, c) coincides with $\rho_1(a, B, c)$. If (a, B, c) has dimension n and satisfies the second condition of regularity then, by Theorem 5, $\rho_1(a, B, c) = n$. Moreover, if (a, B, c) is invertible then the inverse circuit $(a, B, c)^{-1}$ also satisfies the second condition (Corollary 2) and $(a, B, c)^{-n}$ also guarantees 1 activation. It means that the cascade $(a, B, c)^{2n}$ guarantees 2 activations and $\rho_2(a, B, c) \le 2n$.

The last bound can be refined.

Theorem 10. Let a circuit (a, B, c) of dimension n satisfy the second condition of regularity (invertibility of A). Let $\gamma_t = cB^{t-1}a$, $t = 1, 2, \ldots$. Then

$$\rho_2(a, B, c) = n + \max_{r=1,2,\ldots,n} \tau(r),$$

where $\tau(r)$ is the mininum positive integer τ such that

$$(\underbrace{0, \ldots, 0}_{r-1}, 1, \gamma_1, \ldots, \gamma_{n-r})A^{-1}B^{n+\tau-1}a \neq \gamma_{n-r+\tau}. \tag{2}$$

Proof. Suppose that the first activation occurs in the rth round:

$$\Delta u(1) = \ldots = \Delta u(r-1) = 0, \quad \Delta u(r) = \alpha\beta, \quad \Delta v(r) = \beta, \quad \alpha, \beta \neq 0.$$

The arguments above yield $r \le n$.

To avoid activations during the next $n-r$ rounds, the differences $\Delta u(r+\tau)$, $\tau = 1, \ldots, n-r$, must be zero, thus having the form

$$\Delta u(r + \tau) = \Delta y(0)B^{r+\tau-1}a + \gamma_\tau\beta.$$

It is achieved by choosing $\Delta y(0)$ as a solution of the linear equation

$$\Delta y(0)A = \beta(\underbrace{0, 0, \ldots, 0}_{r-1}, \alpha, \gamma_1, \ldots, \gamma_{n-r}).$$

Since A is invertible, a solution exists and is unique.

In the rounds $n + \tau$, $\tau = 1, 2, \ldots$, the differences between queries to round oracles have the form

$$\Delta u(n + \tau) = \beta(\underbrace{0, 0, \ldots, 0}_{r-1}, \alpha, \gamma_1, \ldots, \gamma_{n-r})A^{-1}B^{n+\tau-1}a + \gamma_{n-r+\tau}\beta.$$

As soon as a nonzero difference is encountered, we get the second activation. Therefore,

$$\rho_2 = n + \max_{r=1,2,\ldots,n} \min_{\alpha \in F \setminus \{0\}} \tau(r, \alpha),$$

where $\tau(r, \alpha)$ is the minimal positive integer τ such that

$$(0, \ldots, 0, \alpha, \gamma_1, \ldots, \gamma_{n-r})A^{-1}B^{n+\tau-1}a \neq \gamma_{n-r+\tau}.$$

To complete the proof, it is sufficient to say that $\tau(r, \alpha) \ge \tau(r, 1) = \tau(r)$. Indeed, if the product of a row vector $(0, \ldots, 0, \alpha, \gamma_1, \ldots, \gamma_{n-r})$ by a column $(0, 1)$-vector $A^{-1}B^{n+\tau-1}a$ is equal to $\gamma_{n-r+\tau} \in \{0, 1\}$ for $\alpha \neq 1$, then this product stays the same for $\alpha = 1$. $\square$

Example 8. Apply Theorem 10 to determine the time ρ_2 of the GFN1 circuit of dimension n. For this circuit, $A = B^n = E$ and the sequence (γ_t) consists of repetitions of the n-fragment $(1, 0, \ldots, 0)$.

Consider the inequality (2). If $r < n$ and τ runs from 1 to n then the left and right parts of the inequiality take the values

$$\underbrace{0, \ldots, 0}_{r-1}, 1, 1, \underbrace{0, \ldots, 0}_{n-r-1} \quad \text{and} \quad \underbrace{0, \ldots, 0}_{r}, 1, \underbrace{0, \ldots, 0}_{n-r-1}$$

respectively. The parts differ for the first time at $\tau = r$. If $r = n$ then the inequality occurs immediately at $\tau = 1$. Consequently,

$$\tau(r) = \begin{cases} r, & r < n, \\ 1, & r = n, \end{cases}$$

and $\rho_2 = n + \max_r \tau(r) = 2n - 1$.

SkipjackG has the same characteristics $\tau(r)$ and ρ_2. We have rediscovered results of [23]. □

Theorem 11. Let (a, B, c) be a regular circuit of dimension n. Then $\rho_2(a, B, c) \leq 2n - 1$.

Proof. Let us continue the previous proof. The sequence (γ_t) is a linear recurrence sequence (LRS) over F with the characteristic polynomial f_B. Another LRS with the same characteristic polynomial is the sequence $z_t = \Delta y(0) B^{t-1} a$, $t = 1, 2, \ldots$. To justify the estimate $\rho_2 \leq 2n - 1$, it is sufficent to show that if $z_r = 1$ then all the equalities $z_{r+1} = \gamma_1, \ldots, z_{r+n} = \gamma_n$ cannot hold simultaneously. Let us prove this fact by contradiction.

Without loss of generality, let (a, B, c) have the first canonical form. Then $\gamma_1 = z_{r+1} = c_1, \ldots, \gamma_n = z_{r+n} = c_n$. The sequences (γ_t) and (z_{t+r}) coincide as LRS with the same characteristic polynomial of order n and the same initial prefixes of length n.

If the circuit has type I then (γ_t) and (z_{t+r}) are purely periodic. Therefore, $z_r = \gamma_0$, where $\gamma_0 = cB^{-1}a = 0$. By Theorem 1, $\gamma_0 = 0$ which contradicts the fact that $z_r = 1$.

If the circuit has type II then $b_1 = 0$ and

$$z_{r+n} = b_2 z_{r+1} + b_3 z_{r+2} + \ldots + b_n z_{r+n-1} = b_2 c_1 + b_3 c_2 + \ldots + b_n c_{n-1}.$$

By Theorem 7, $z_{r+n} \neq c_n$, again a contradiction. □

In Table 4 we report the second activation times of standard regular circuits. Only the times of MARS3 and SMS4 are strictly less than the bound of Theorem 11.

It is interesting that the time ρ_2(Feistel) fully determines all other times ρ_i(Feistel), $i \geq 3$. Indeed, the fact that $\rho_3 = 2$ means that in 3 consecutive Feistel rounds there must be at least 2 activations. This is the only restriction on differential characteristics of Feistel cascades. Therefore, 3 activations are guaranteed by 5 rounds, 4 activations — by 6 rounds, and so on: $\rho_3 = 5$, $\rho_4 = 6$, $\rho_5 = 8$, $\rho_6 = 9, \ldots$.

9 Duality

Definition 10. For a circuit (a, B, c), its *dual* is the circuit (c^T, B^T, a^T).

Let us list obvious facts regarding duality.

1. Mutually dual circuits have mutually transposed extended matrices.

Table 4: The 2nd activation times

Circuit	ρ_2
Feistel	3
Matsui	3
SkipjackA	7
SkipjackB	7
MARS3	5
SMS4	5
GFN1	$2n-1$
SkipjackG	$2n-1$

2. Mutually dual circuits are invertible simultaneously.

3. Invertible mutually dual circuits have the same type (I or II).

4. A circuit is transitive if and only if its dual is weakly 2-transitive.

5. Mutually dual circuits are regular simultaneously.

6. Mutually dual circuits have the same lag.

More sophisticated facts are related to differential and linear attacks against corresponding block ciphers. It is well-known (see, for example, [4, 7, 16]) that these attacks are dual in the sense of similarity and complementarity. Further we show their duality in a more specific sense: Linear attacks against ciphers which use (a, B, c) as the round circuit are connected with differential attacks against ciphers which use (c^T, B^T, a^T). Our results correlate with results of the paper [3] where mirror round functions, an analogue of dual circuits, are introduced.

Consider an invertible cascade $(a, B, c)^t$. In linear cryptanalysis, the correlations between adjacent vectors of the sequence $y(0), y(1), \ldots, y(t)$ are exploited. These correlations are described by column vectors $\beta(0), \beta(1), \ldots, \beta(t) \in F^n$ called *masks*. Suppose that $y(0)$ is chosen uniformly at random from F^n. Due to invertibility of (a, B, c), each induced vector $y(\tau)$, $\tau = 1, \ldots, t$, is also uniformly distributed over F^n under any choice of round oracles $S_1, S_2, \ldots, S_\tau$.

Let us say that $y(\tau)$ *correlates* with $y(\tau - 1)$ if there exists S_τ such that

$$\mathsf{P}\left\{\mathrm{Tr}(y(\tau)\beta(\tau)) = \mathrm{Tr}(y(\tau-1)\beta(\tau-1))\right\} \neq \frac{1}{2}.$$

A sequence of masks which provides correlations between all adjacent vectors is called the *linear characteristic* of $(a, B, c)^t$.

Above, Tr is the trace function $F \ni u \mapsto u + u^2 + u^4 + \ldots + u^{2^{m-1}} \in \{0, 1\}$. Any linear function $L\colon F \to \{0, 1\}$ can be written as $L(u) = \mathrm{Tr}(\gamma u)$ under an appropriate choice of $\gamma \in F$. The transition $y(\tau) \mapsto \mathrm{Tr}(y(\tau)\beta(\tau))$ is a linear compression of $y(\tau)$ up to one bit. The mask $\beta(\tau)$ regulates the compression rule.

Consider the relationship between adjacent masks of a linear characteristic. Let x be chosen uniformly at random from F^n, $y = xB + S(xa)c$ and $\alpha, \beta \in F^n$ be nonzero masks. The vectors x and y correlate if

$$\mathsf{P}\left\{\mathrm{Tr}(xB\beta + S(xa)c\beta) = \mathrm{Tr}(x\alpha)\right\} \neq \frac{1}{2}.$$

With $c\beta = 0$ the correlation is possible if and only if $\alpha = B\beta$. Let $c\beta = \gamma \neq 0$. Then the correlation condition is refined as follows:

$$\mathsf{P}\left\{\mathrm{Tr}(x(B\beta + \alpha)) = \mathrm{Tr}(S(xa)\gamma)\right\} \neq \frac{1}{2}.$$

The correlation appears with some S if and only if $u = xa$ and $v = x(B\beta + \alpha)$ are related linearly, that is, $v = u\delta$ for some nonzero $\delta \in F$. It means that

$$\alpha = B\beta + \delta a.$$

Gathering all, masks $\beta(0), \beta(1), \ldots, \beta(t)$ form a characteristic if

$$\beta(\tau - 1) = \begin{cases} B\beta(\tau), & c\beta(\tau) = 0, \\ B\beta(\tau) + \delta(\tau)a, & c\beta(\tau) \neq 0. \end{cases} \tag{3}$$

for $\tau = t, \ldots, 2, 1$ and some nonzero $\delta(\tau) \in F$.

Comparing the equations (1) and (3), we immediately obtain the following result.

Theorem 12. Let $\beta(0), \beta(1), \ldots, \beta(t)$ be a linear characteristic of an invertible cascade $(a, B, c)^t$. Then $\Delta\alpha(0), \Delta\alpha(1), \ldots, \Delta\alpha(t)$, where $\Delta\alpha(\tau) = \beta(t - \tau)^T$, is the differential characteristic of the dual cascade $(c^T, B^T, a^T)^t$. The converse is also true.

Recall that the condition $\Delta\alpha(\tau - 1)a \neq 0$ in (1) is called the activation. The dual condition $c\beta(\tau) \neq 0$ in (3) is also the activation, only linear not differential. Theorem 12 means that the minimum number of linear activations in some cascade is equal to the minimum number of differential activations in the dual cascade. This fact helps to switch from linear attacks to differential ones during security evaluation of block ciphers.

10 Expandability

The GFN1 and SkipjackG circuits are actually families of circuits of growing dimension n. We can easily switch from one dimension to another because the parameters (a, B, c) of the circuits are simply described depending on n. We call this property *expandability*.

Expandable circuits can be used to build variable input length (VIL) or wide-block (WBL) ciphers. To support cryptographic strength and effectiveness of these ciphers, an underlying circuit must be regular, has to have small X-complexity, direct and inverse lags.

Both GFN1 and SkipjackG satisfy all these properties except the last one: Their inverse lags are close to their dimensions (see Table 2). That is why the circuits have rather large indices of 2-transitivity (see Table 3) and hypothetical VIL- or WBL-ciphers should involve a rather large number of rounds to achieve cryptographic strength.

Further we discuss one possible expandable circuit with better diffusion properties. This circuit, called BeltWBL, has already been used in [21] where symmetric cryptographic algorithms based on the block cipher Belt are standardized. More precisely, BeltWBL is the core of the `belt-keywrap` algorithm which provides confidentiality and integrity control of variable length keys. In general, BeltWBL can be used to construct WBL-ciphers, that is why the name. The idea of BeltWBL belongs to Andrey Afonenko.

The BeltWBL circuit of dimension $n \geq 2$ is described as follows:

1) B is a Frobenius cell which last column is $b = (1, 1, \ldots, 1, 0)^T$;

2) $a = b$;

3) $c = (0, 0, \ldots, 1, 0)$.

It is interesting that the last two columns (rows) of the extended matrix are equal.

The circuit has type I. It coincides with Feistel for $n = 2$. The next theorem shows that BeltWBL is optimal with respect to the mentioned diffusion properties.

Theorem 13. The BeltWBL circuit of dimension $n \geq 2$ is regular. The lags of BeltWBL and $\mathsf{BeltWBL}^{-1}$ are both equal to 1.

Proof. Apply Theorem 9 to prove regularity. Firstly, the polynomial $f_B(\lambda) = \lambda^n + a(\lambda)$ is coprime to $a(\lambda) = 1+\lambda+\ldots+\lambda^{n-2}$. Secondly, the matrix P from the statement of Theorem 9 has the form:

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 0 & 1 \\ 1 & 1 & \ldots & 0 & 1 & 0 \\ 1 & 1 & \ldots & 1 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 1 & \ldots & 0 & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 & 0 \end{pmatrix}$$

Hence, $cP = (0, 1, 0, \ldots, 0)$ and the polynomial $(cP)(\lambda) = \lambda$ is also coprime to $f_B(\lambda)$. Conditions of Theorem 9 are satisfied and BeltWBL is regular.

Since $ca = 0$, the lag of BeltWBL is equal to 1. The lag of $\mathsf{BeltWBL}^{-1} = (B^{-1}a, B^{-1}, cB^{-1})$ is the minimum l such that

$$cB^{-1}(B^{-1})^{l-1}B^{-1}a = cB^{-1-l}a = 1.$$

We have $cB^{-1} = (0, 0, \ldots, 0, 1)$, $cB^{-2} = (1, 0, \ldots, 0, 0)$ and $cB^{-2}a = 1$. Thus, the inverse lag is also equal to 1. □

Finally, let us discuss the X-complexities of BeltWBL, $\mathsf{BeltWBL}^{-1}$ and their cascades.

The BeltWBL circuit induces the mapping

$$(x_1, x_2, \ldots, x_{n-2}, x_{n-1}, x_n) \mapsto (x_2, x_3, \ldots, x_{n-1}, x_n + S(u), u),$$

where $u = x_1 + x_2 + \ldots + x_{n-1}$. We need $n-2$ additions to calculate u and one more addition to calculate $x_n + S(u)$. Therefore, the X-complexity of BeltWBL is $n - 1$.

Fortunately, for large n the X-complexity of the cascade $\mathsf{BeltWBL}^t$ is considerably less than $(n-1)t$. Indeed, storing x_1, we can update u in the next round using only 2 additions. Moreover, in the second round we can use just 1 addition if we previously save the sum $x_2 + \ldots + x_{n-1}$. It means that the X-complexity of $\mathsf{BeltWBL}^t$ does not exceed $(n-2) + 3(t-1)$, that is, we need approximately 3 additions per round (this is the case of MARS3 and SMS4) as t grows.

The inverse mapping has the form:

$$(x_1, x_2, x_3, \ldots, x_{n-1}, x_n) \mapsto (u + x_n, x_1, x_2, \ldots, x_{n-2}, x_{n-1} + S(x_n)),$$

where $u = x_1 + x_2 + \ldots + x_{n-2}$. The X-complexity of $\mathsf{BeltWBL}^{-1}$ is again equal to $n - 1$. In the cascade $\mathsf{BeltWBL}^{-t}$ of large dimension n, we can again update u using 2 additions and, therefore, decrease the average X-complexity per round from $n - 1$ to approximately 4.

Acknowledgments: The author thanks Andrey Afonenko, Vadim Marchuk and Svetlana Mironovich who have been involved in XS-circuits-related projects and made a significant contribution to the overall understanding of the topic. The author also thanks Sugata Gangopadhyay, Nishant Sinha and Oleg Solovey for valuable discussions about future research directions.

References

[1] Berger T.P., Minier M., Thomas G. Extended Generalized Feistel Networks Using Matrix Representation. In: Lange, T., Lauter, K., Lisoněk, P. (eds) Selected Areas in Cryptography – SAC 2013. SAC 2013. Lecture Notes in Computer Science, vol 8282. Springer, Berlin, Heidelberg (2013).

[2] Biham E., Biryukov A., Shamir A. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. J. Cryptology, 18, 291-311 (2005).

[3] Blondeau C., Bogdanov A., Wang M. On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-type Ciphers. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds) Applied Cryptography and Network Security. ACNS 2014. Lecture Notes in Computer Science, vol 8479. Springer, Cham (2014).

[4] Blondeau C., Nyberg K. New Links between Differential and Linear Cryptanalysis. In: Johansson, T., Nguyen, P.Q. (eds) Advances in Cryptology – EUROCRYPT 2013. EUROCRYPT 2013. Lecture Notes in Computer Science, vol 7881. Springer, Berlin, Heidelberg (2013).

[5] Blondeau C., Wang M. Analysis of Impossible, Integral and Zero-Correlation Attacks on Type-II Generalized Feistel Networks using the Matrix Method. In: Leander, G. (eds) Fast Software Encryption. FSE 2015. Lecture Notes in Computer Science, vol 9054. Springer, Berlin, Heidelberg (2015).

[6] Burwick C., Coppersmith D., D'Avignon E., Gennaro R., Halevi S., Jutla C., Matyas Jr. S.M., O'Connor L., Peyravian M., Safford D., Zunic N. MARS: A Candidate Cipher for AES. In: AES – The First Advanced Encryption Standard Candidate Conference, Conference Proceedings (1998).

[7] Chabaud F., Vaudenay S. Links between differential and linear cryptanalysis. In: De Santis, A. (eds) Advances in Cryptology – EUROCRYPT'94. EUROCRYPT'94. Lecture Notes in Computer Science, vol 950. Springer, Berlin, Heidelberg (1995).

[8] Choy J., Chew G., Khoo K., Yap H. Cryptographic properties and application of a Generalized Unbalanced Feistel Network structure. Cryptogr. Commun. (2011) 3: 141. https://doi.org/10.1007/s12095-011-0042-6.

[9] Choy J., Yap H. Impossible Boomerang Attack for Block Cipher Structures. In: Takagi, T., Mambo, M. (eds) Advances in Information and Computer Security. IWSEC 2009. Lecture Notes in Computer Science, vol 5824. Springer, Berlin, Heidelberg (2009).

[10] Diffie W., Ledin G. SMS4 Encryption Algorithm for Wireless Networks. Cryptology ePrint Archive, Report 2008/329. https://eprint.iacr.org/2008/329 (2008). Accessed 8 June 2018.

[11] Feistel H., Notz W.A., Smith J.L. Some cryptographic techniques for machine-to-machine data communications. Proceedings of IEEE 63, 1545-1554 (1975).

[12] Knudsen L.R. DEAL – A 128-bit Block Cipher. Technical report, NIST AES Proposal. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.32.7982 (1998). Accessed 8 June 2018.

[13] Lai X., Massey J.L. A proposal for a new block encryption standard. In: Damgärd I.B. (eds) Advances in Cryptology – EUROCRYPT'90. EUROCRYPT 1990. Lecture Notes in Computer Science, vol 473. Springer, Berlin, Heidelberg (1991).

[14] Lidl R., Niederraiter H. Finite Fields. Cambridge University Press (1997).

[15] Luo Y., Wu Z., Lai X., Gong G. A unified method for finding impossible differentials of block cipher structures. Inform. Sci. 263, 211-220 (2014).

[16] Malyshev F.M. The duality of differential and linear methods in cryptography. Mat. Vopr. Kriptogr., Volume 5, Issue 3, 35–47 (2014).

[17] Matsui M. New block encryption algorithm MISTY. In: Biham, E. (eds) Fast Software Encryption. FSE 1997. Lecture Notes in Computer Science, vol 1267. Springer, Berlin, Heidelberg (1997).

[18] McGrew D.A., Viega J. The security and performance of the Galois / Counter Mode (GCM) of operation. In: Canteaut, A., Viswanathan, K. (eds) Progress in Cryptology – INDOCRYPT 2004. INDOCRYPT 2004. Lecture Notes in Computer Science, vol 3348. Springer, Berlin, Heidelberg (2004).

[19] National Institute of Standards and Technology (NIST). Skipjack and KEA Algorithm Specifications. Version 2.0. https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/skipjack/skipjack.pdf (1998). Accessed 8 June 2018.

[20] Solomon L. Similarity of the companion matrix and its transpose. Linear Algebra and Its Appl. 302-303, 555-561 (1999).

[21] STB 34.101.31-2011. Information Technology and Security. Data Encryption and Integrity Algorithms. Standard of Belarus. http://apmi.bsu.by/assets/files/std/belt-spec27.pdf (2011). In Russian. Accessed 8 June 2018.

[22] Sung J., Lee S., Lim J., Hong S., Park S. Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis. In: Okamoto, T. (eds) Advances in Cryptology – ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science, vol 1976. Springer, Berlin, Heidelberg (2000).

[23] Yap H. Impossible Differential Characteristics of Extended Feistel Networks with Provable Security against Differential Cryptanalysis. In: Kim, H., Kim, T., Kiumi, A. (eds) Advances in Security Technology. SecTech 2008. Communications in Computer and Information Science, vol 29. Springer, Berlin, Heidelberg (2009).

[24] Zheng Y., Matsumoto T., Imai H. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In: Brassard, G. (eds) Advances in Cryptology – CRYPTO'89. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. Springer, New York, NY (1990).