# XS-circuits in block ciphers

**Sergey Agievich**

Research Institute for Applied Problems

of Mathematics and Informatics

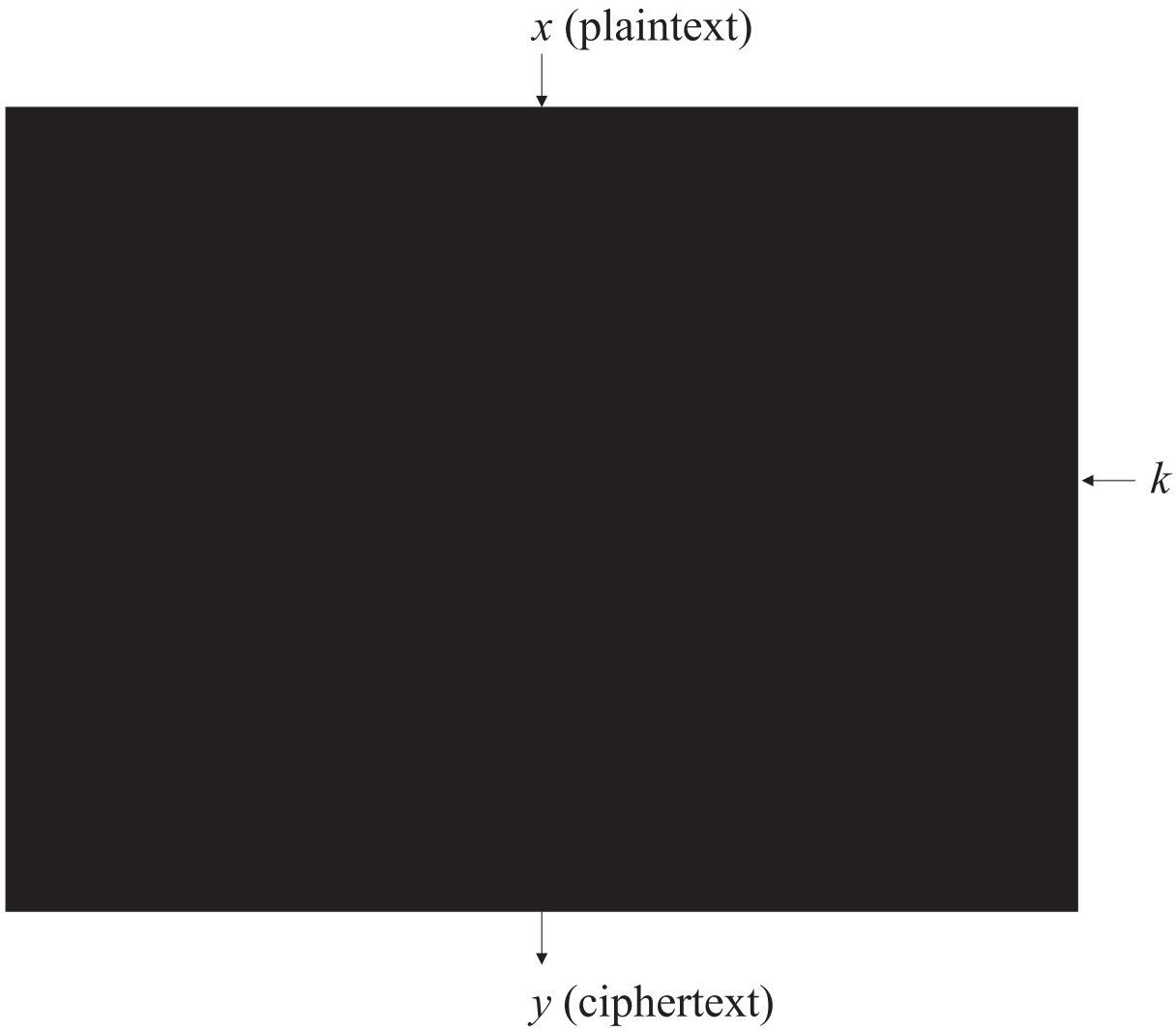
Belarusian State University

agievich@{bsu.by|gmail.com}

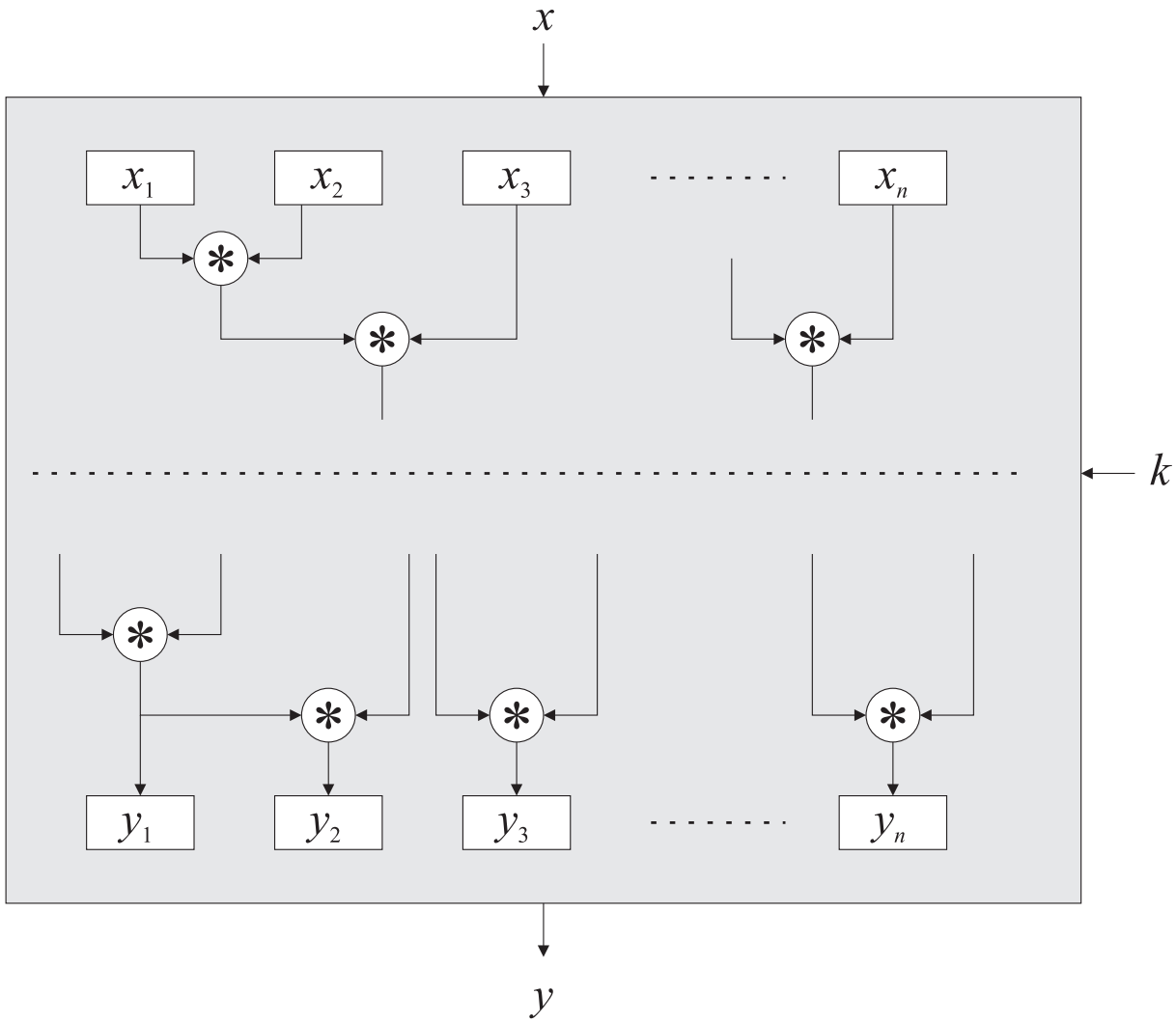
CTCrypt-2018

[Suzdal, 2018.05.28]

# 1. Block ciphers



# 2. . . . into block ciphers



# 3. Circuits

- $x$ is divided into fragments
- fragments are elements of $\{0,1\}^m \sim F = \mathbb{F}_{2^m} \sim \mathbb{F}_2^m \sim \mathbb{Z}_{2^m}$
- fragments are processed using operations (binary or unary)
  - $k$ adjusts operations (key-dependent operations) or
  - $k$ is divided into fragments which become operands

**A circuit** (informally) — a graph which describes the operations and their sequence

# 4. Operations

## Binary

**X**: addition in $\mathbb{F}_2^m \sim \mathbb{F}_{2^m}$ (XOR, $\oplus$, $+$)

**A**: addition / subtraction in $\mathbb{Z}_{2^m}$ ($\boxplus$, $\boxminus$)

**M**: multiplication in $\mathbb{F}_{2^m}$

**L**: componentwise logical AND or OR ($\wedge$, &, $\vee$)

## Unary

**R**: cyclic shift (rotation: $\lll$, $\ggg$)

**S**: substitution ($S$-box)*

*it might be a circuit with a smaller $m$!

# 5. Stable designs

**LRX**: Simon ($m = 16, 24, 32, 48, 64$)

**ARX**: Speck ($m = 16, 24, 32, 48, 64$)

**ARXS**: GOST, Belt ($m = 32$; with extended $S$-boxes $\in \mathbf{S}$)

**XMS**: AES, Kuznechyk* ($m = 8$)

*usually classified as **XLS**, where L stands for "linear"

# 6. XS-circuits

**Operations**: **X** ($+$) and **S** (key dependent $S$-boxes, oracles)

**S-complexity**: the number of **S** nodes

**X-complexity**: the minimum number of **X** nodes

# 7. XS-circuits of S-complexity 1

**Parameters**:

- $a \in \mathbb{F}_2^n$ (column)
- $B = (b_{ij})$ — a matrix of order $n$ over $\mathbb{F}_2$
- $c \in \mathbb{F}_2^n$ (row)

**The mapping** $x \mapsto y$ $(x, y \in F^n)$:

1) $u \leftarrow a_1x_1 + a_2x_2 + \ldots + a_nx_n$;
2) $v \leftarrow S(u)$ [$S$ is an instantiation of **S**];
3) for $i = 1, \ldots, n$: $y_i \leftarrow b_{1i}x_1 + b_{2i}x_2 + \ldots + b_{ni}x_n + c_iv$.

$$\boxed{y = (a, B, c)[S](x)}$$

**In the matrix form**:

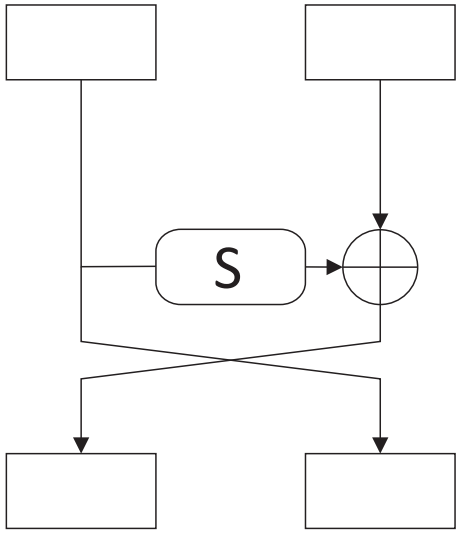
$$\boxed{y = xB + S(xa)c}$$

# 8. The extended matrix

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

fully describes the circiut!

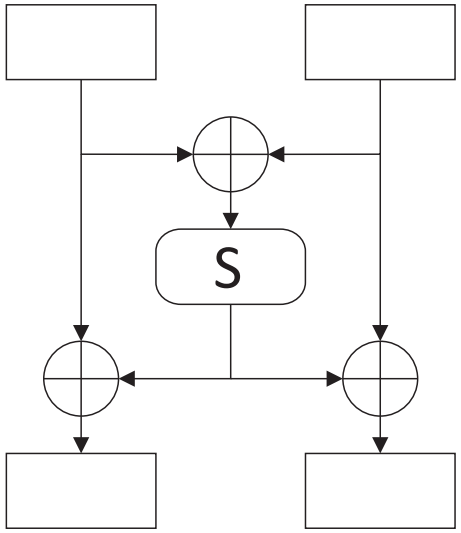
# 9. XS-circuits: Feistel




[H. Feistel, 1975; LUCIFER; **X**-complexity 1]

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

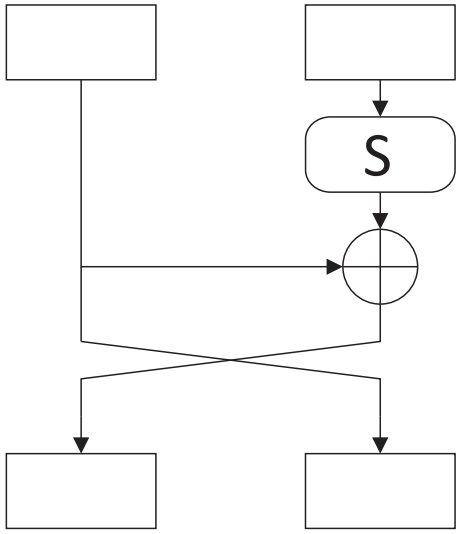
# 10. XS-circuits: LaiMassey




[Lai + Massey, 1991; into IDEA; **X**-complexity 3]

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

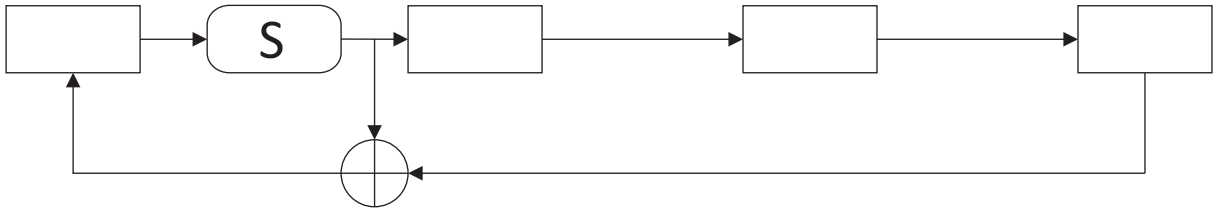
# 11. XS-circuits: Matsui




[M. Matsui, 1997; MISTY2; **X**-complexity 1]

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

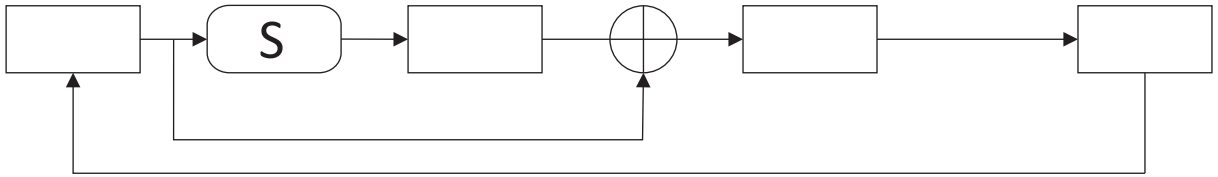
# 12. XS-circuits: SkipjackA




[NSA, 1998; SKIPJACK; **X**-complexity 1]

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

# 13. XS-circuits: SkipjackB




[NSA, 1998; SKIPJACK; **X**-complexity 1]

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

# 14. XS-circuits: MARS3

[IBM, 1998; MARS (candidate of the AES contest); **X**-complexity 3]

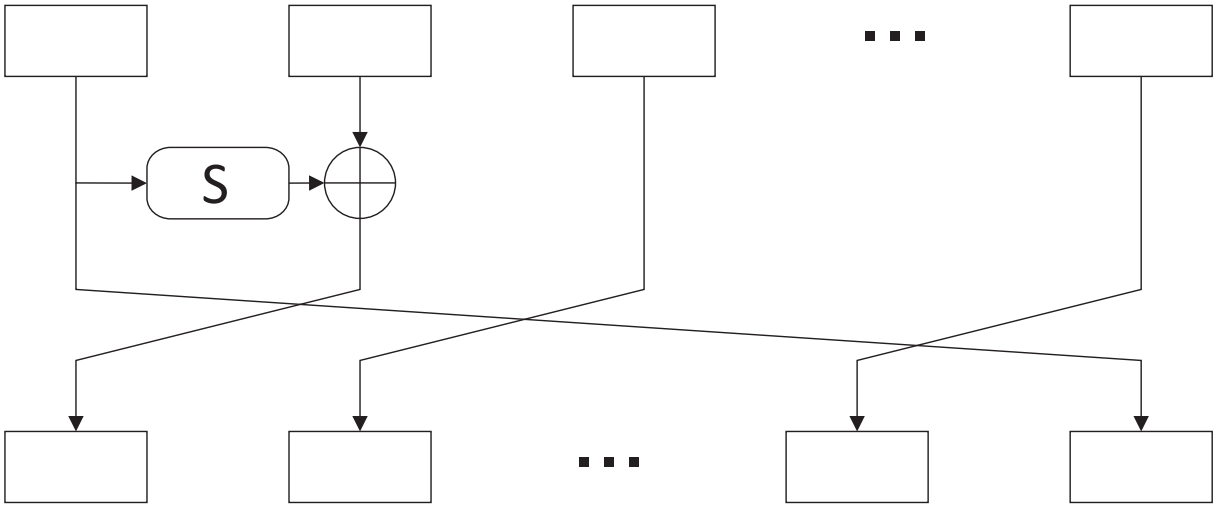
$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

# 15. XS-circuits: SMS4

[Chinese Government, 2006; SMS4; **X**-complexity 3]

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

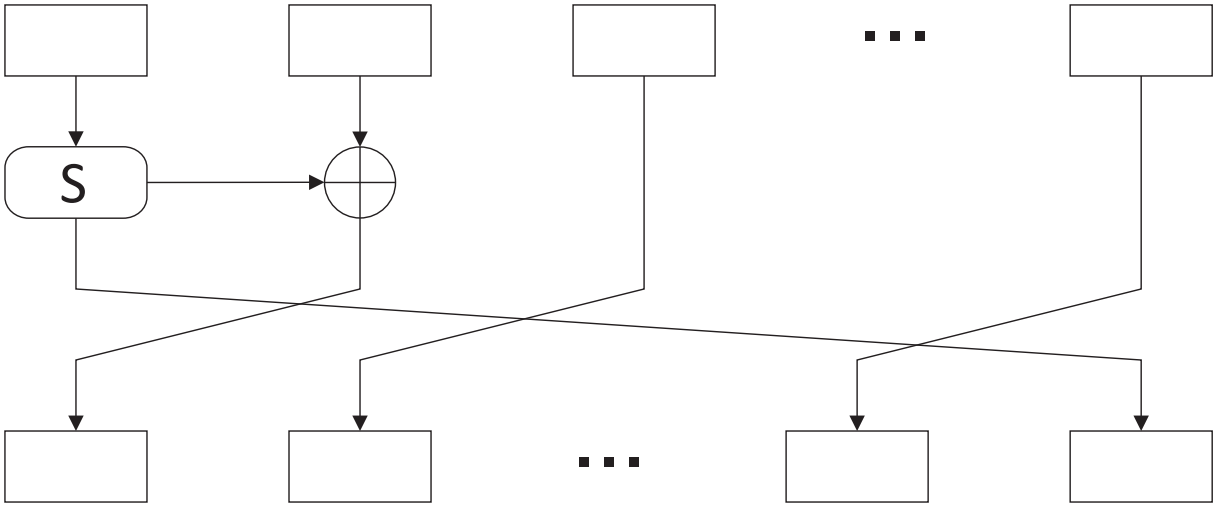
# 16. XS-circuits: GFN1




[Zheng + Matsumoto + Imai, 1989; a generalization of Feistel; **X**-complexity 1]

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

# 17. XS-circuits: SkipjackG




[Sung + Lee + Lim + Hong + Park, 2000; a generalization of Skipjack; **X**-complexity 1]

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

# 18. Invertibility

**Definition**. 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 iff one of the following cases holds:

I. $B$ is invertible and $cB^{-1}a = 0$.

II. $\operatorname{rank} B = n - 1$, $\operatorname{rank}(B\ a) = n$ and $\operatorname{rank}\binom{B}{c} = n$ (it yields that the extended matrix is invertible).

**Case I**: Feistel, LaiMassey, MARS3, SMS4, GFN1

**Case II**: Matsui, SkipjackX

# 19. Inversion

$((a, B, c)[S])^{-1} = (a, B, c)^{-1}[S']$, where
$(a, B, c)^{-1}$ is the **inverse circuit**

**Case I**:

- $(a, B, c)^{-1} = (B^{-1}a, B^{-1}, cB^{-1})$
- $S' = S$

**Case II**:

- ext. matrix of $(a, B, c)^{-1}$ = (ext. matrix of $(a, B, c)$)$^{-1}$
- $S' = S^{-1}$

**Example**:

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

# 20. Cascades

**A cascade** $(a, B, c)^t$: a composition of $t$ instances (**rounds**) of $(a, B, c)$

**An instantiation**: $(a, B, c)^t[S_1, \ldots, S_t]$

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

# 21. Regularity

**Definition**. A circuit $(a, B, c)$ is regular if

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

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

**Definition**. A lag of $(a, B, c)$ is the minimal positive integer $l$ such that $cB^{l-1}a = 0$.

**Definition**. A circuit $(a, B, c)$ is strongly regular if it is regular and

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

# 22. Lags

| $(a, B, c)$ | Lag of $(a, B, c)$ | Lag of $(a, B, c)^{-1}$ | 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 | $n$ | $n+1$ |

# 23. Transitivity

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

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

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 $(a, B, c)$.

**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.

# 24. 2-Transitivity

**Definition**. 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

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

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 $(a, B, c)$.

**Motivation**. 2-transitivity provides protection against impossible differential attacks (IDA) and helps to determine the permutation group generated by the mappings $(a, B, c)[S]$, where $S$ runs over all bijections over $F$.

**Weak** 2-**transitivity**: a weaken form, supported by the second condition of regularity (invertibility of $A$).

# 25. Index of 2-transitivity

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

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

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 $(a, B, c)^{-1}$.

**Remark**: $(\star)$ holds if, f.e., $|F| = 2^m > 4n$

# 26. Estimates on the index of 2-transitivity

| $(a, B, c)$ | Upper bound (Th. 6) | Lower bound* |
|---|---|---|
| Feistel | 6 | 6 (Knudsen, 1998) |
| Matsui | 7 | |
| SkipjackA | 22 | 17 (Blondeau et al., 2014) |
| SkipjackB | 22 | 17 (Blondeau et al., 2014) |
| MARS3 | 14 | 12 (Gong et al., 2014) |
| SMS4 | 14 | 12 (Gong et al., 2014) |
| GFN1 ($n = 4$) | 20 | 20 (Choy and Yap, 2009) |
| SkipjackG ($n = 4$) | 22 | 17 (Gong et al., 2014) |

* constructive — are based upon known impossible differentials

# 27. 2-transitivity: the Skipjack case

**This paper**:

SkipjackA$^{22}$ is 2-transitive

SkipjackB$^{22}$ is 2-transitive

SkipjackA$^{7}$SkipjackB$^{7}$ is 2-transitive

**Biham, Biryukov, Shamir (2005)**:

SkipjackA$^{4}$SkipjackB$^{8}$SkipjackA$^{8}$SkipjackB$^{4}$ isn't 2-transitive

(24 rounds!)

# 28. Simularity

**Definition**. 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 $a' = P^{-1}a$, $B' = P^{-1}BP$, $c' = cP$.

**Motivation**. 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.

$\boxed{(a, B, c) \sim (a', B', c')}$

**Examples**:

MARS $\sim$ SMS4

SkipjackA $\not\sim$ SkipjackB

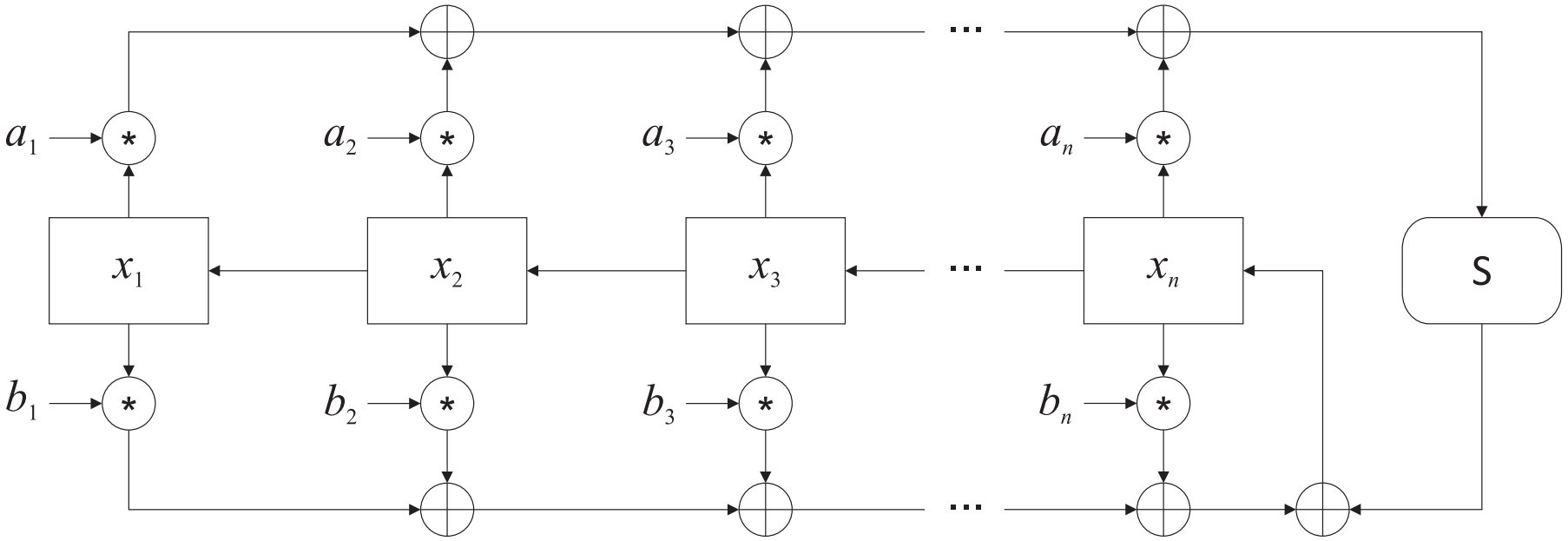
# 29. Canonical forms

**Theorem 8**. A regular circuit is similar to each of the following circuits:
1) $((1,0,0,\dots,0)^T, B, c)$;
2) $(a, B, (0,0,\dots,0,1))$.
Here $B$ is a uniquely determined Frobenius cell:

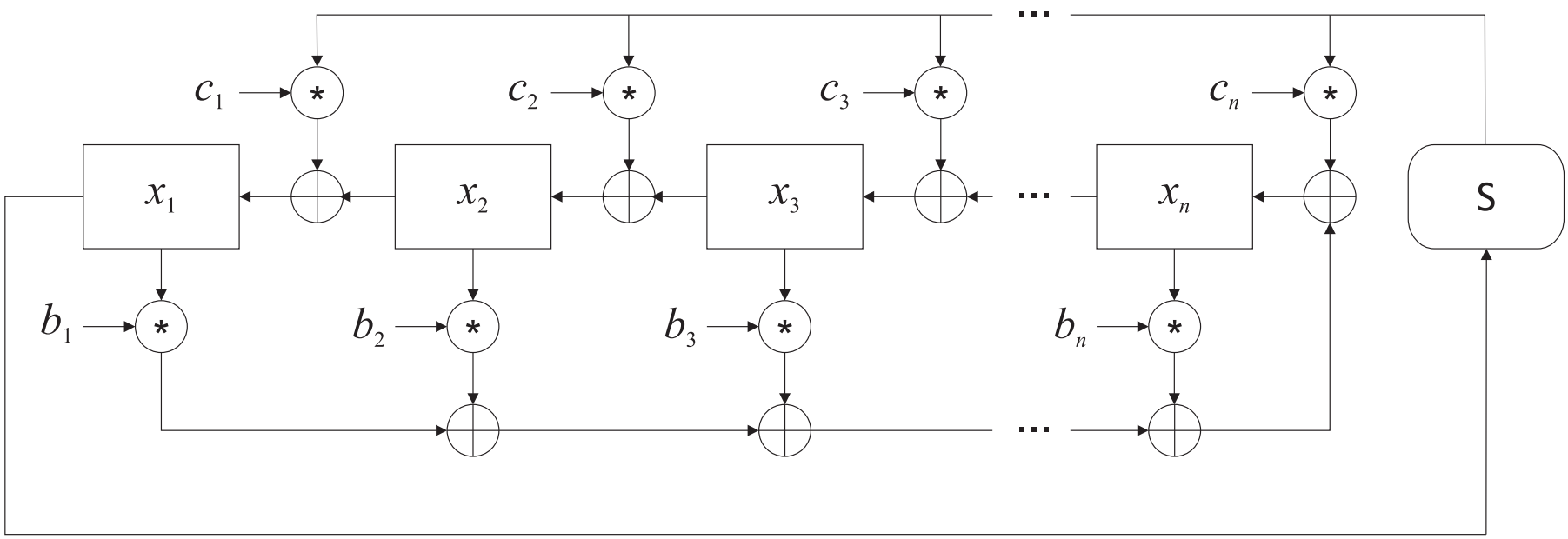
$$B = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & b_1 \\ 1 & 0 & \dots & 0 & 0 & b_2 \\ 0 & 1 & \dots & 0 & 0 & b_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & b_{n-1} \\ 0 & 0 & \dots & 0 & 1 & b_n \end{pmatrix}.$$

The vectors $a$ and $c$ are also uniquely determined.

# 30. The 1st canonical form



# 31. The 2nd canonical form



# 32. The roadmap

- Invertibility
- Regularity
- Transitivity
- 2-transitivity
- Weak 2-transitivity
- Similarity
- Duality [how to switch from linear to differential charactersitics]
- Activations [how to estimate the mimimum number of active $S$-boxes]
- Expandability [how to build wide-block ciphers]