Related-key attack on 5-round Kuznyechik

Vitaly Kiryukhin

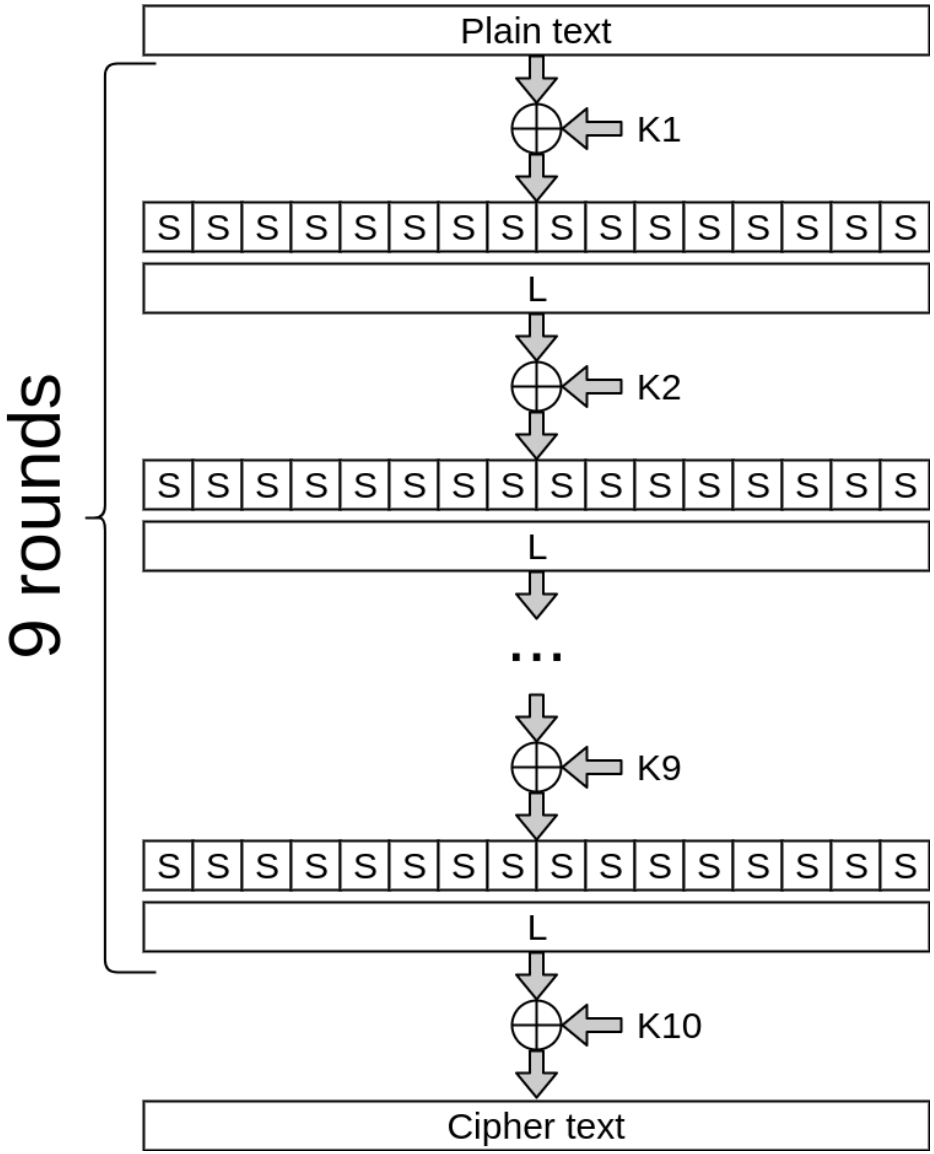
JSC «InfoTeCS»

CTCrypt'19

June 5, 2019

vitaly.kiryukhin@infotecs.ru

GOST 34.12-2015 – «Kuznyechik»



Kuznyechik is an LSX block cipher

Block size – 128 bit ($n = 16$ byte)

Key size – 256 bit

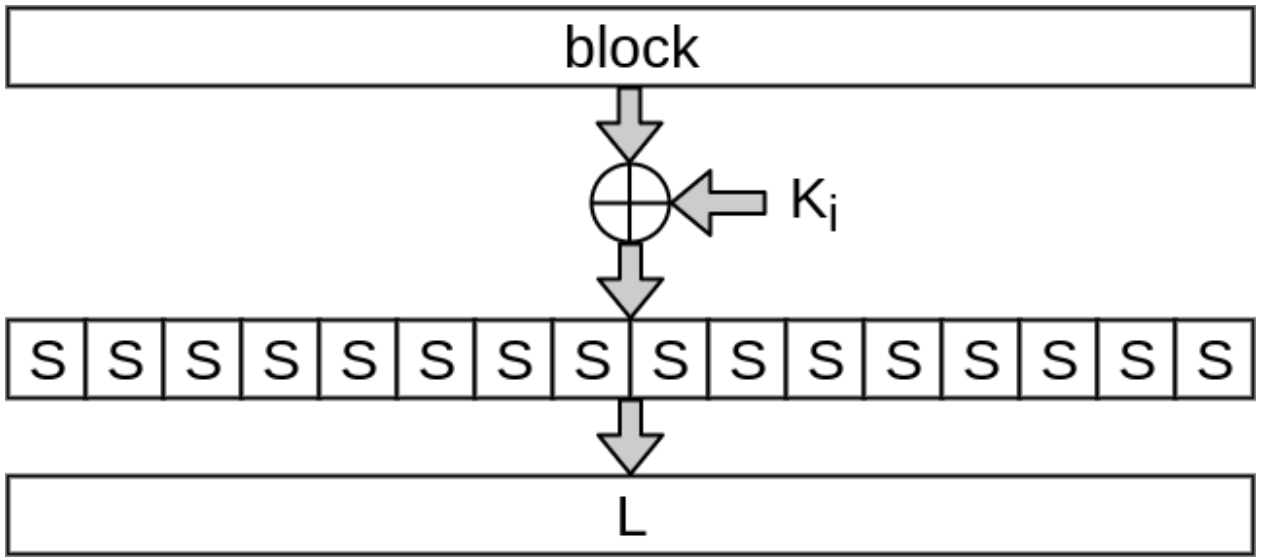
9 full rounds (10 round keys)

Round transformations

X – modulo 2 addition of an input block with an iterative key

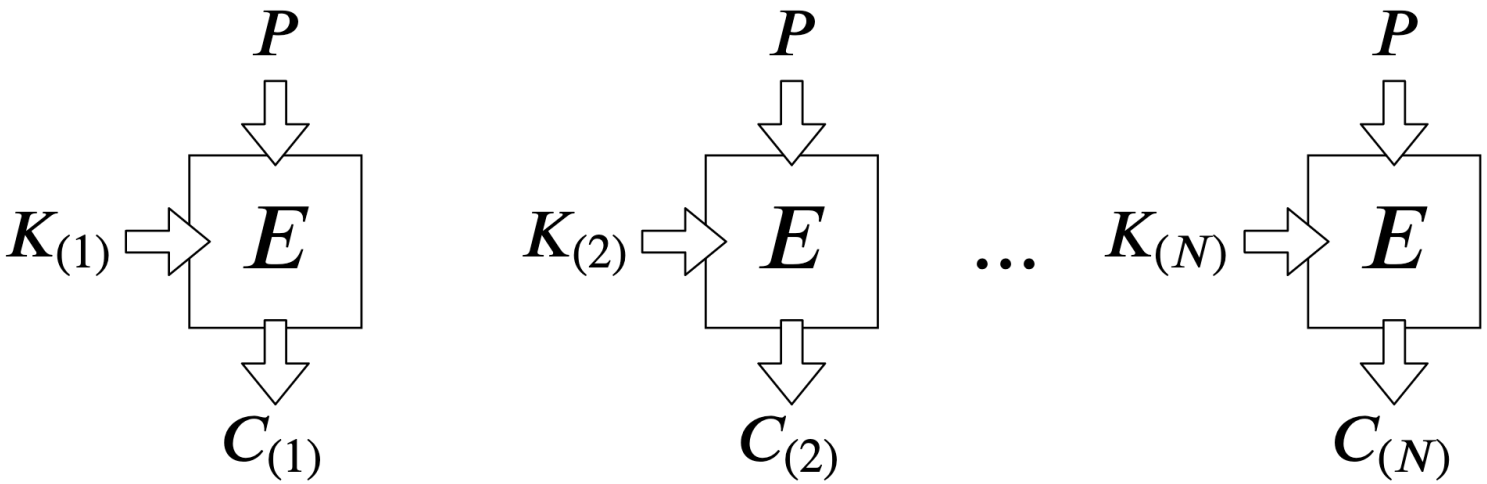
S – parallel application of a fixed bijective byte substitution

L – linear transformation – MDS(32, 16, 17), optimal diffusion operation, branch number (minimal code distance) $\mathcal{B} = 17$



Related-key model

We have some number of encryptors

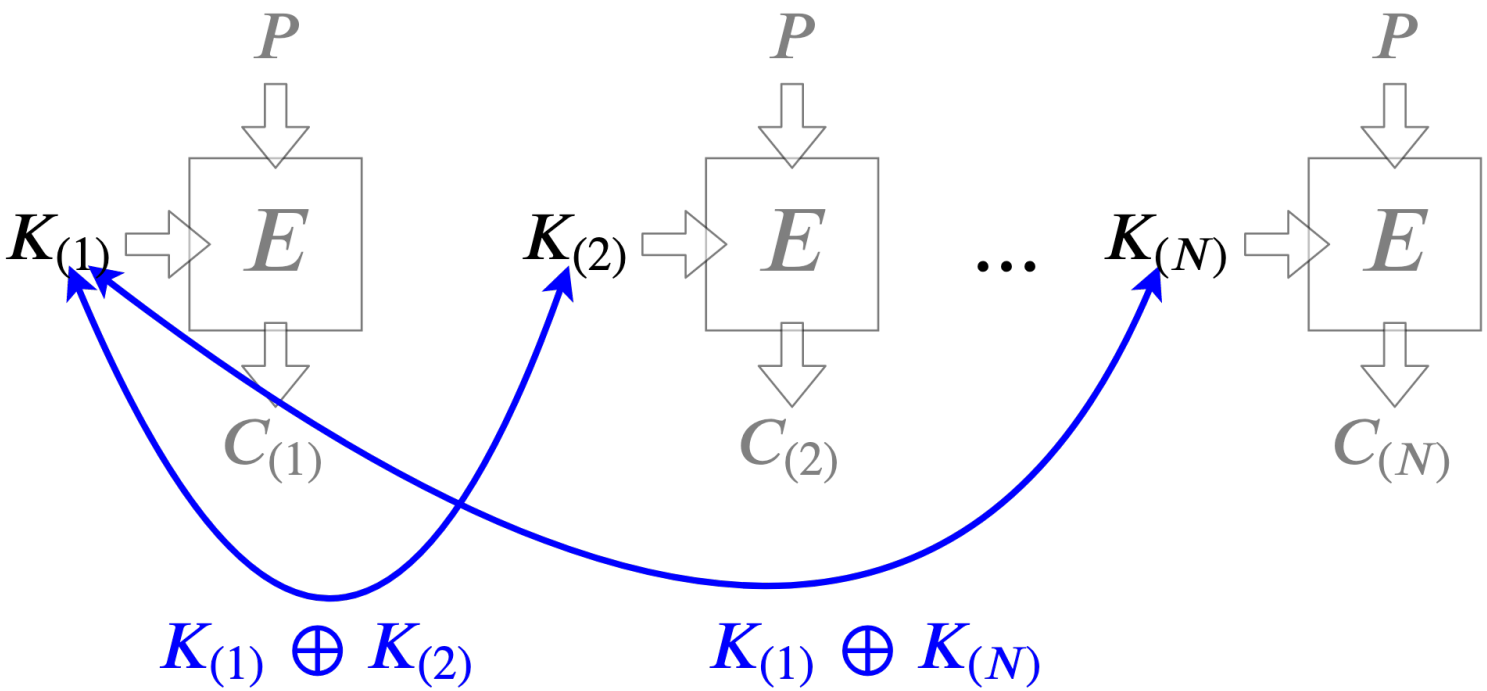


All keys $K_{(1)}, K_{(2)}, \ldots, K_{(N)}$ are secret and unknown

Related-key model

We know (or choose) the simple relations between the keys:

$$K_{(1)} \oplus K_{(2)}, \quad K_{(1)} \oplus K_{(3)}, \quad \ldots, \quad K_{(1)} \oplus K_{(N)}$$



Related-key attack on 3-round Kuznyechik

E.Alekseev, K.Goncharenko, G.Marshalko – *Provably Secure Counter Mode with Related Key-based Internal Re-keying* – CTCrypt'18

$$\mathsf{E}_{K_1,K_2}(A) = \mathsf{X}[K_4]\mathsf{LSX}[K_3]\mathsf{LSX}[K_2]\mathsf{LSX}[K_1](A)$$

$$(K_3, K_4) = \mathsf{F}[C_2]\mathsf{F}[C_1]\,(K_1, K_2)$$

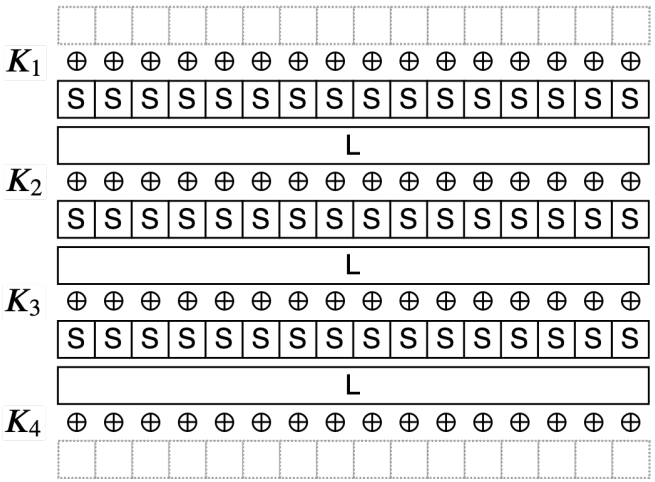
$$K_3 = K_1 \oplus \mathsf{LSX}[C_2](K_2 \oplus \mathsf{LSX}[C_1](K_1))$$

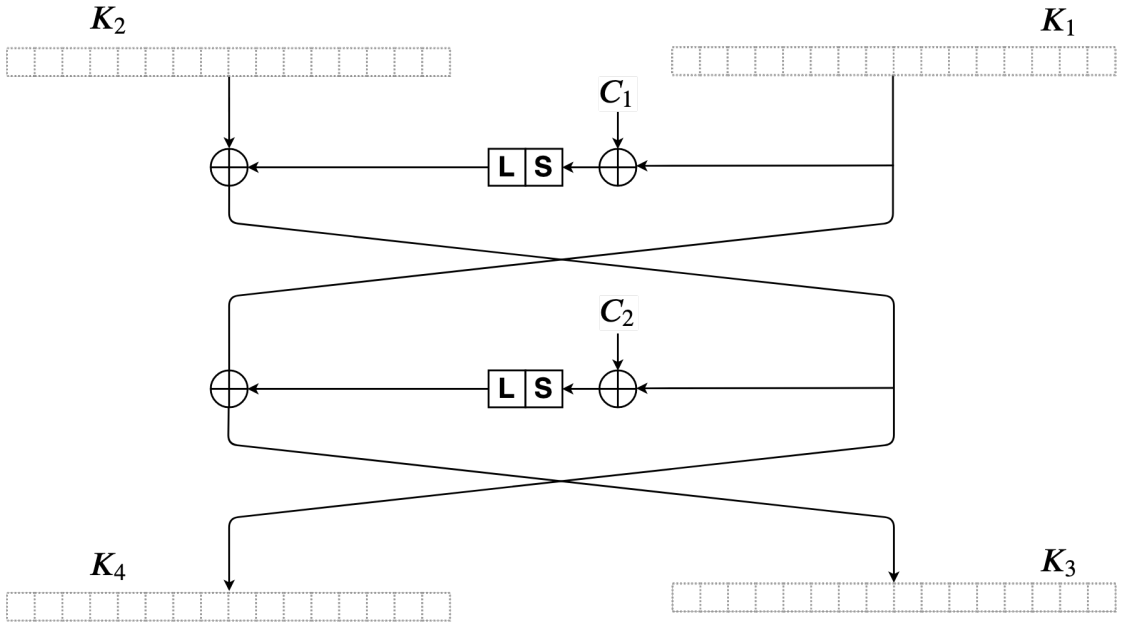
$$K_4 = K_2 \oplus \mathsf{LSX}[C_1](K_1)$$

Cipher rounds	Key schedule rounds	Operations	Keys
3	2	2^{12}	2^{12}

Related-key attack on 3-round Kuznyechik

$$\mathsf{E}_{K_1,K_2}(A) = \mathsf{X}[K_4]\mathsf{LSX}[K_3]\mathsf{LSX}[K_2]\mathsf{LSX}[K_1](A)$$





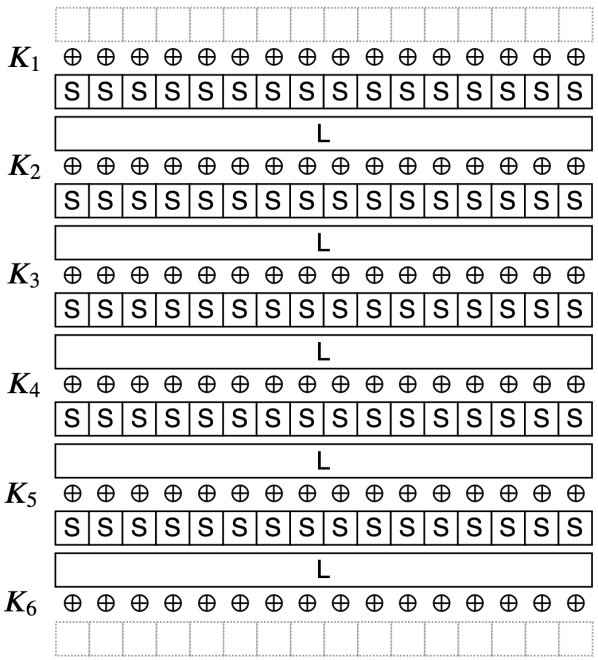
5-round Kuznyechik

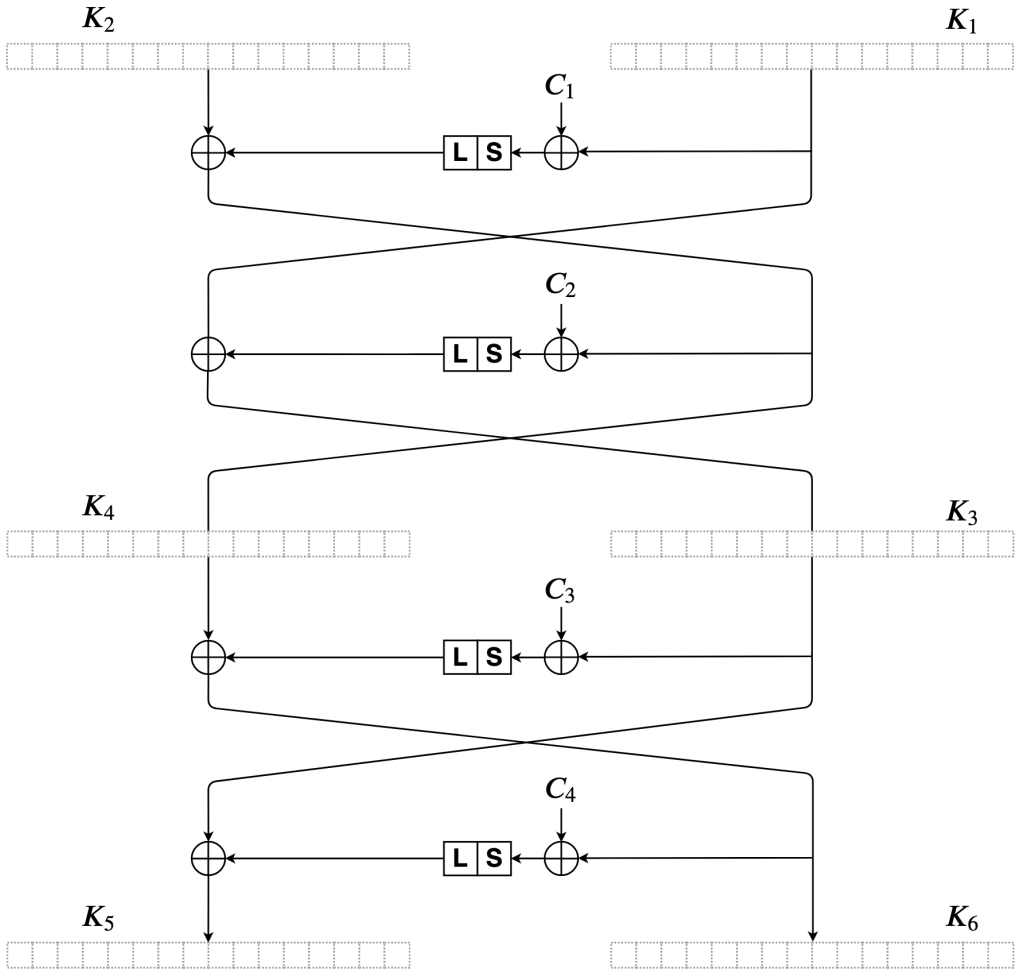
$$\mathsf{E}_{K_1,K_2}(A) = \mathsf{X}[K_6]\mathsf{LSX}[K_5]\mathsf{LSX}[K_4]\mathsf{LSX}[K_3]\mathsf{LSX}[K_2]\mathsf{LSX}[K_1](A)$$

$$(K_3, K_4) = \mathsf{F}[C_2]\mathsf{F}[C_1]\,(K_1, K_2)$$

$$(K_5, K_6) = \mathsf{F}[C_4]\mathsf{F}[C_3]\,(K_3, K_4)$$

5-round Kuznyechik





5-round Kuznyechik

Equivalent representation of the last two rounds

$$\mathsf{E}_{K_1,K_2}(A) = \mathsf{X}[\widetilde{K}_6]\mathsf{SLX}[\widetilde{K}_5]\mathsf{SX}[K_4]\mathsf{LSX}[K_3]\mathsf{LSX}[K_2]\mathsf{LSX}[K_1](A)$$

$$(K_3, K_4) = \mathsf{F}[C_2]\mathsf{F}[C_1]\,(K_1, K_2)$$

$$K_4 = K_2 \oplus \mathsf{LSX}[C_1](K_1)$$

$$K_3 = K_1 \oplus \mathsf{LSX}[C_2](K_4)$$

$$(K_5, K_6) = \mathsf{F}[C_4]\mathsf{F}[C_3]\,(K_3, K_4)$$

$$K_6 = K_4 \oplus \mathsf{LSX}[C_3](K_3)$$

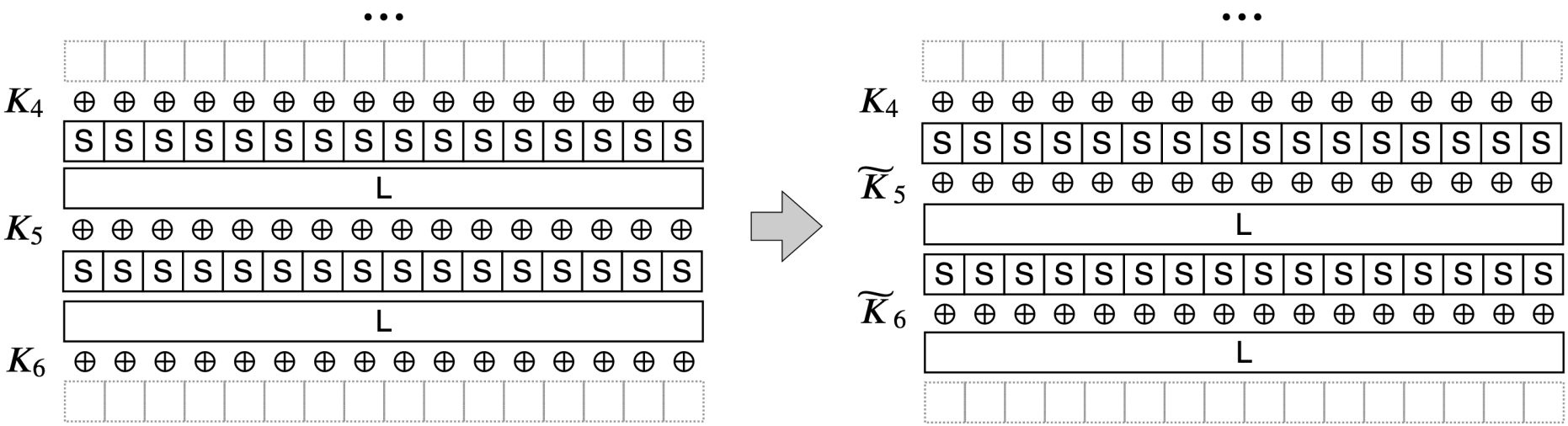
$$K_5 = K_3 \oplus \mathsf{LSX}[C_4](K_6)$$

$$\widetilde{K}_6 = \mathsf{L}^{-1}(K_6)$$

$$\widetilde{K}_5 = \mathsf{L}^{-1}(K_5)$$

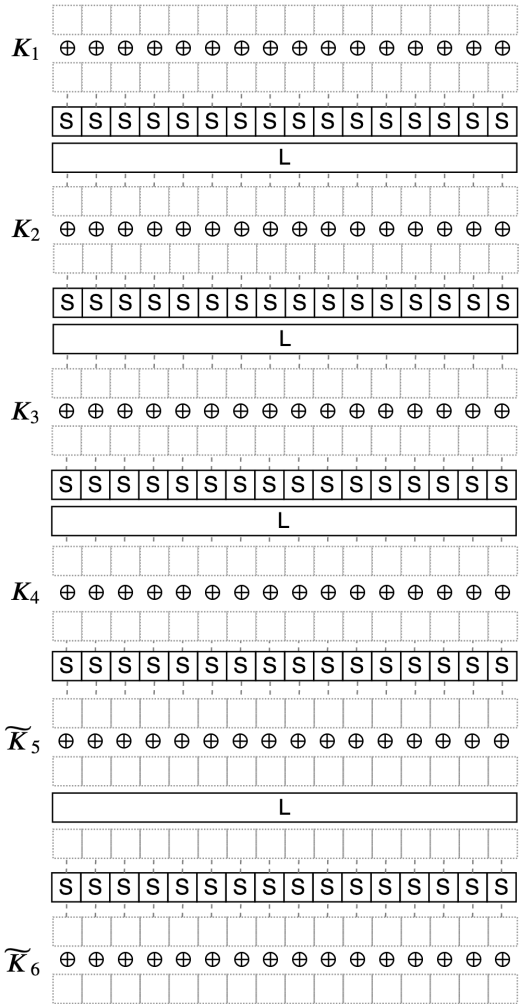
5-round Kuznyechik

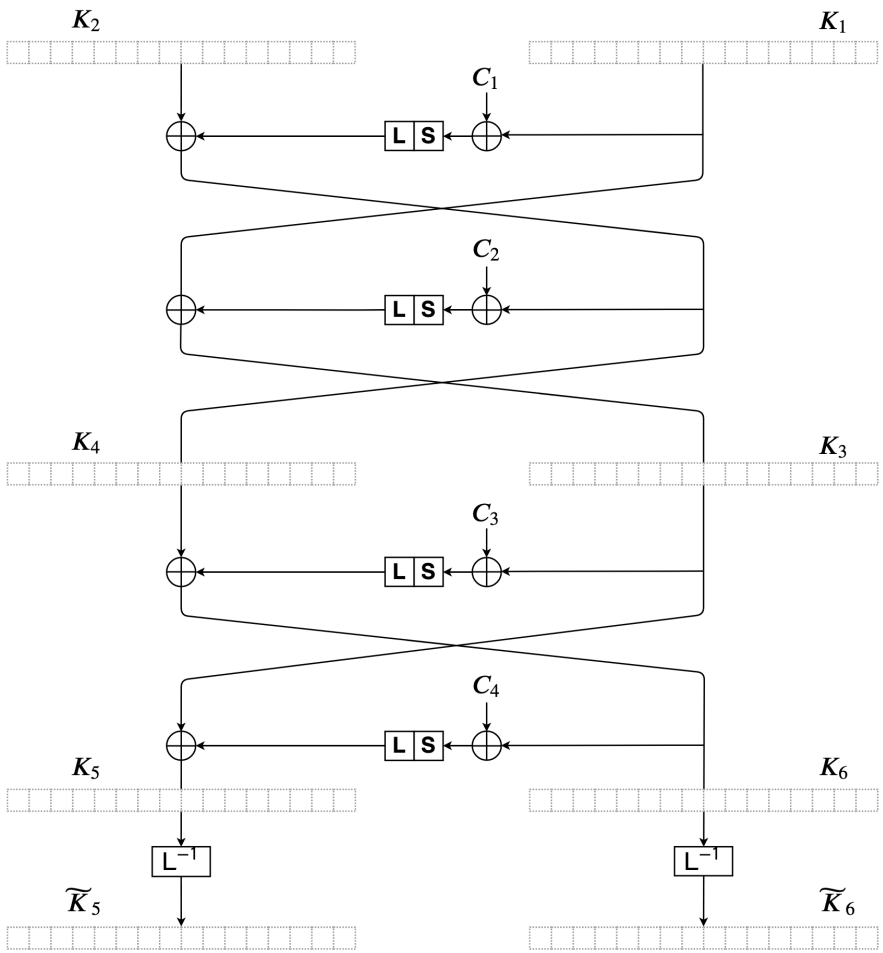
Equivalent representation of the last two rounds



5-round Kuznyechik

Equivalent representation of the last two rounds





Polytopic notation

Let we have a sequence of blocks

$$P_0, ..., P_d \in \mathbb{F}_{2^8}^n,$$

then we refer to sequence

$$\boldsymbol{\Delta P} = (P_0 \oplus P_1, P_0 \oplus P_2, ..., P_0 \oplus P_d) \in \left(\mathbb{F}_{2^8}^n\right)^d$$

as a difference (or d-difference).

We always use $d = 2^8 - 1 = 255$.

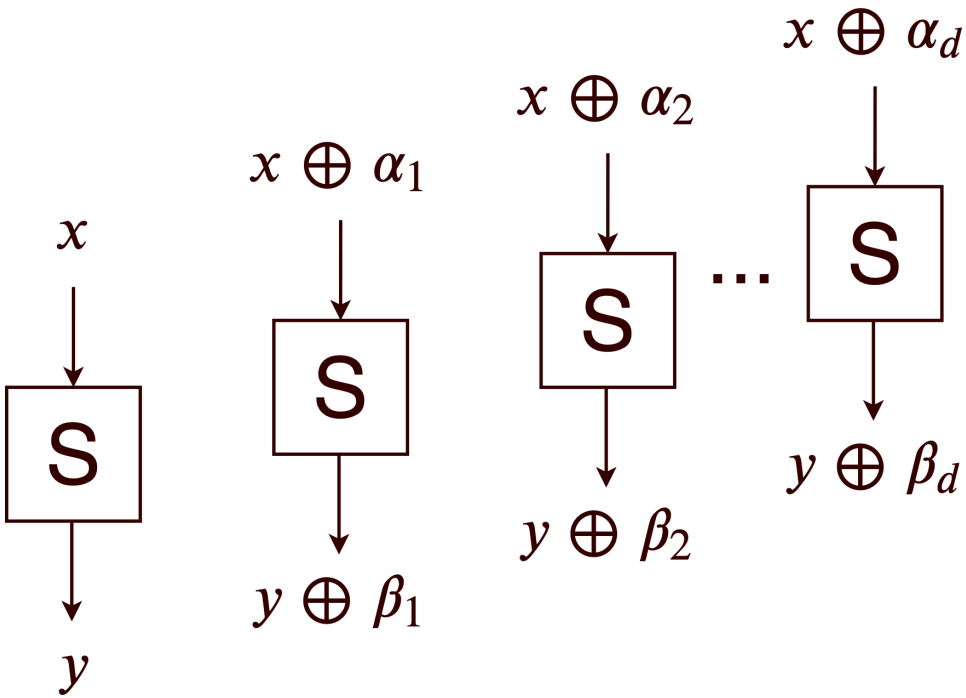
Polytopic notation

$$\boldsymbol{\Delta P} = \underbrace{\begin{pmatrix} b_{1,1} & b_{1,2} & \dots & \dots & b_{1,n} \\ b_{2,1} & b_{2,2} & \dots & \dots & b_{d,n} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ b_{d,1} & b_{d,2} & \dots & \dots & b_{d,n} \end{pmatrix}}_{n=16} = \begin{pmatrix} P_0 \oplus P_1 \\ P_0 \oplus P_2 \\ \vdots \\ \vdots \\ P_0 \oplus P_d \end{pmatrix}$$

$$b_{i,j} \in \mathbb{F}_{2^8}, \;\; P_0, ..., P_d \in \mathbb{F}_{2^8}^n$$

Polytopic notation

S-layer



The differences $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ and $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_d)$.

After S-box we have no more than 2^8 possible differences.

Polytopic notation

S-layer

$$\Delta P = \underbrace{\begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} & \dots & \dots & b_{1,n} \\ b_{2,1} & b_{2,2} & b_{2,3} & \dots & \dots & b_{d,n} \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \vdots \\ b_{d,1} & b_{d,2} & b_{d,3} & \dots & \dots & b_{d,n} \end{pmatrix}}_{n=16}$$

Each «**column**» will be transformed independently of the others.

Polytopic notation

L-layer

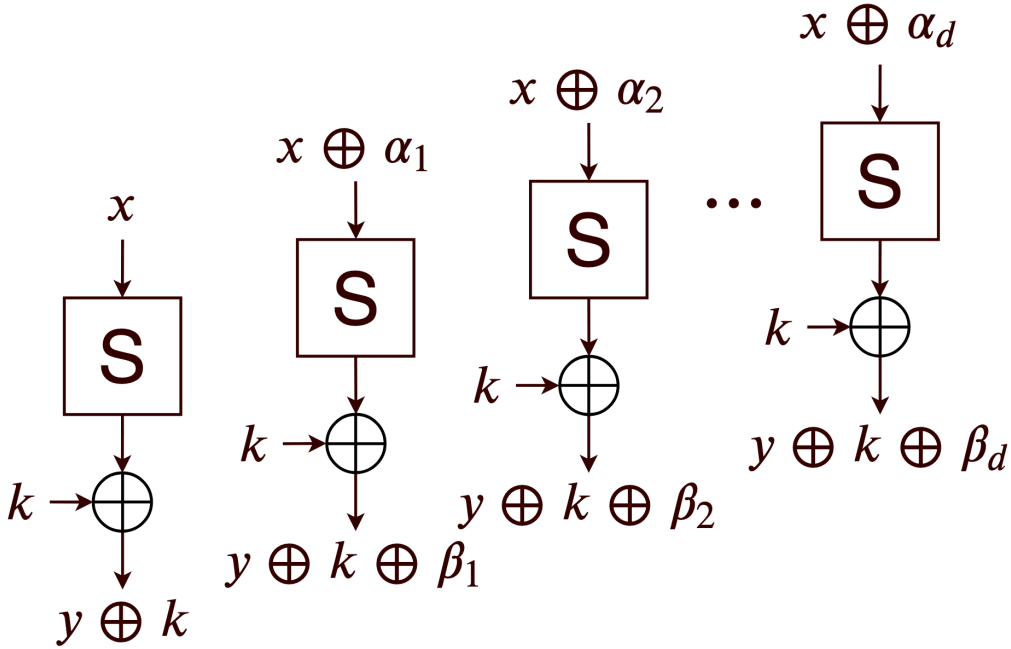
The L-transformation bijectively maps one difference to another.

Each «**row**» will be transformed independently of the others.

$$\mathsf{L}(\boldsymbol{\Delta P}) = \begin{pmatrix} \mathsf{L}(P_0 \oplus P_1) \\ \mathsf{L}(P_0 \oplus P_2) \\ \vdots \\ \vdots \\ \mathsf{L}(P_0 \oplus P_d) \end{pmatrix}$$

Polytopic notation

Round key recovery



If we know $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ and $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_d)$ then we know the unique pair $(x, y \oplus k)$.

(The difference $\boldsymbol{\alpha}$ must contain at least 8 different bytes)

We know ciphertext $y \oplus k$ and $\mathsf{S}(x) \Rightarrow$ it is easy to find the key k.

Polytopic notation

We denote

$$\mathsf{f}(\boldsymbol{\Delta P})$$

– the set of differences after transformation f.

For example:

– the set $\mathsf{L}(\boldsymbol{\Delta P})$ contains only one difference;

– the set $\mathsf{S}(\boldsymbol{\Delta P})$ contains no more than $(2^8)^t$ differences, where t is the number of active S-boxes.

Integral properties

$$\boldsymbol{\Delta P} = \underbrace{\begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} & \dots & \dots & b_{1,n} \\ b_{2,1} & b_{2,2} & b_{2,3} & \dots & \dots & b_{d,n} \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \vdots \\ b_{d,1} & b_{d,2} & b_{d,3} & \dots & \dots & b_{d,n} \end{pmatrix}}_{n=16} = \begin{pmatrix} P_0 \oplus P_1 \\ P_0 \oplus P_2 \\ \vdots \\ \vdots \\ P_0 \oplus P_d \end{pmatrix}$$

All (**A**) – *i*-th «**column**» contains all different non-zero bytes

Balanced (**B**) – xor of all bytes from *i*-th «**column**» is equal to zero

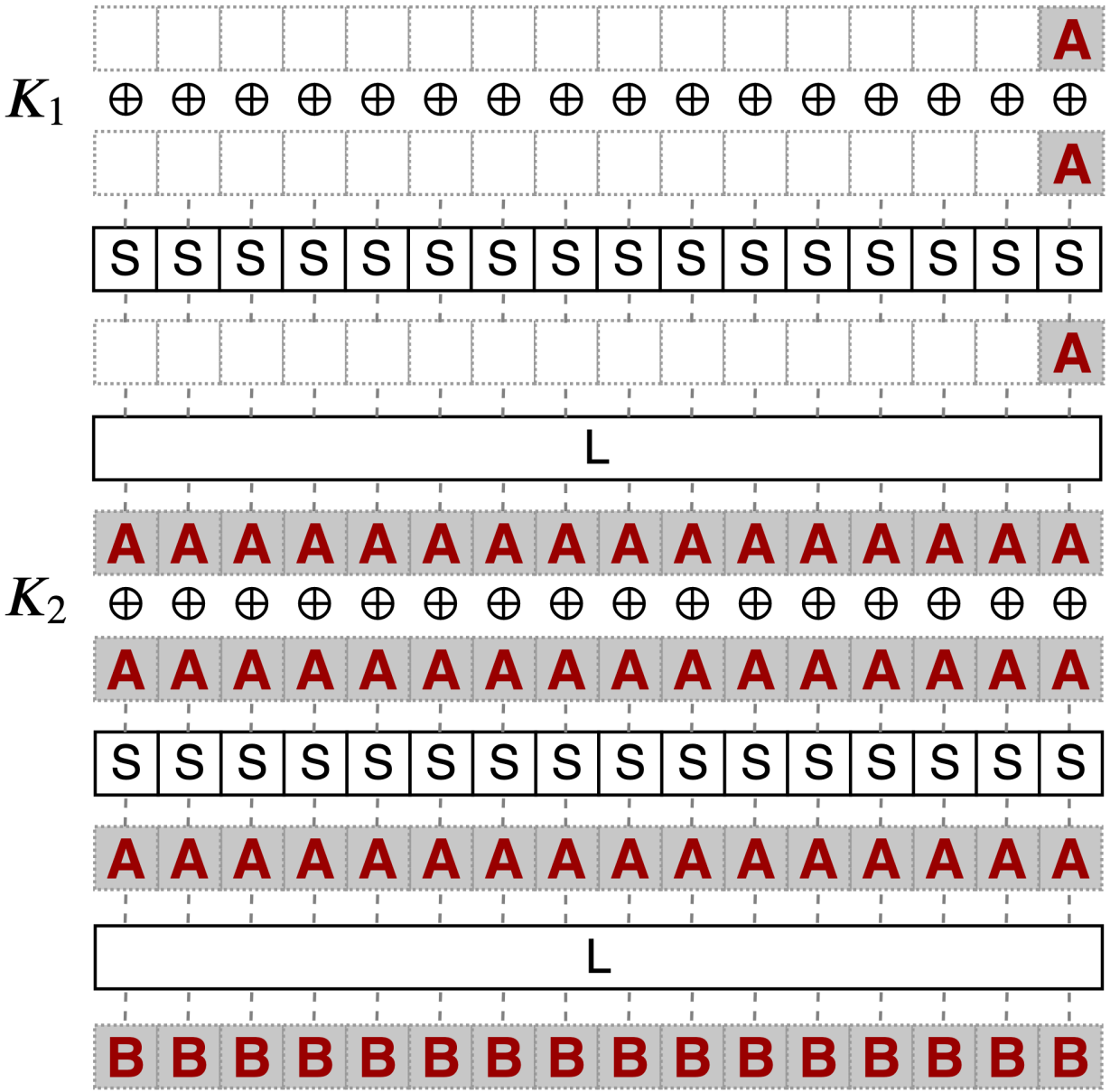
LSXLSX integral property

Let one position in the difference

$$\boldsymbol{\delta} = \left(\underbrace{\begin{matrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 0 & 2 \\ \dots & \dots & \ddots & \dots & \dots \\ 0 & 0 & \dots & 0 & 255 \end{matrix}}_{n=16} \right)$$

has integral property **A** and all other positions are inactive. Then any difference from LSXLSX($\boldsymbol{\delta}$) has the integral property **B**.

LSXLSX integral property



Main steps of the related-key attack

1. Adversary chooses 2^8 collections of related keys, 2^8 keys in each collection. One plaintext C_1 will be used.
2. For one of these collections, the special easy verifiable property (integral distinguisher) is true.
3. The round keys K_6, K_5 are recovered by using integral and polytopic properties.

Key collections

The difference

$$\boldsymbol{\kappa} = \left(\underbrace{\begin{matrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 0 & 2 \\ \dots & \dots & \ddots & \dots & \dots \\ 0 & 0 & \dots & 0 & 255 \end{matrix}}_{n=16} \right)$$

The collection of the related keys:

$$(K_1, K_2) \text{ and set } \left(K_1 \oplus \boldsymbol{\kappa}, K_2 \oplus \boldsymbol{\kappa''}\right), \text{ where } \boldsymbol{\kappa''} \in \mathsf{LS}(\boldsymbol{\kappa})$$

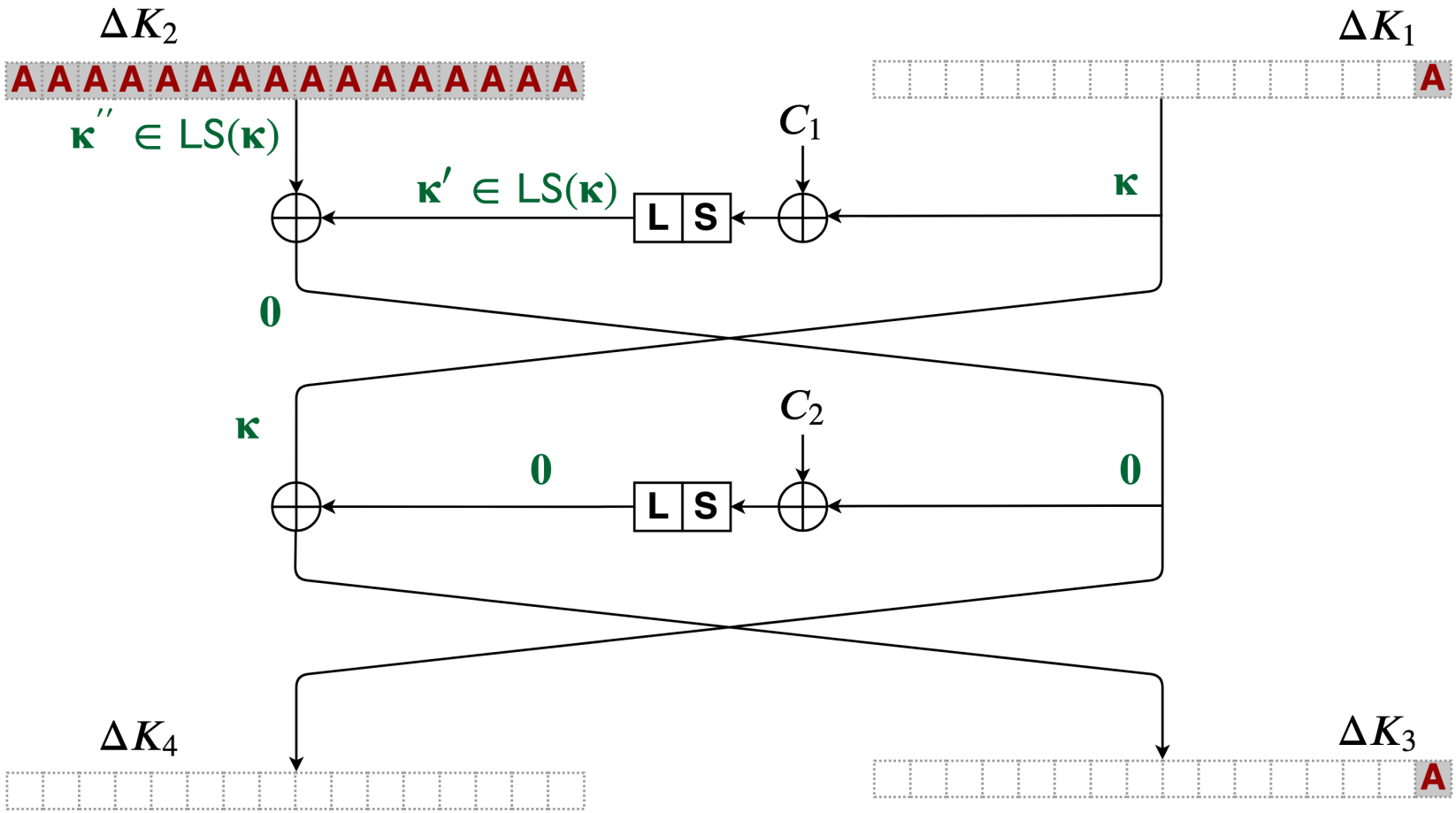
«Main» key and a set of $d = 255$ related keys.

The number of distinct $\boldsymbol{\kappa''}$ is $2^8 \Rightarrow$ we have 2^8 collections.

Integral distinguisher

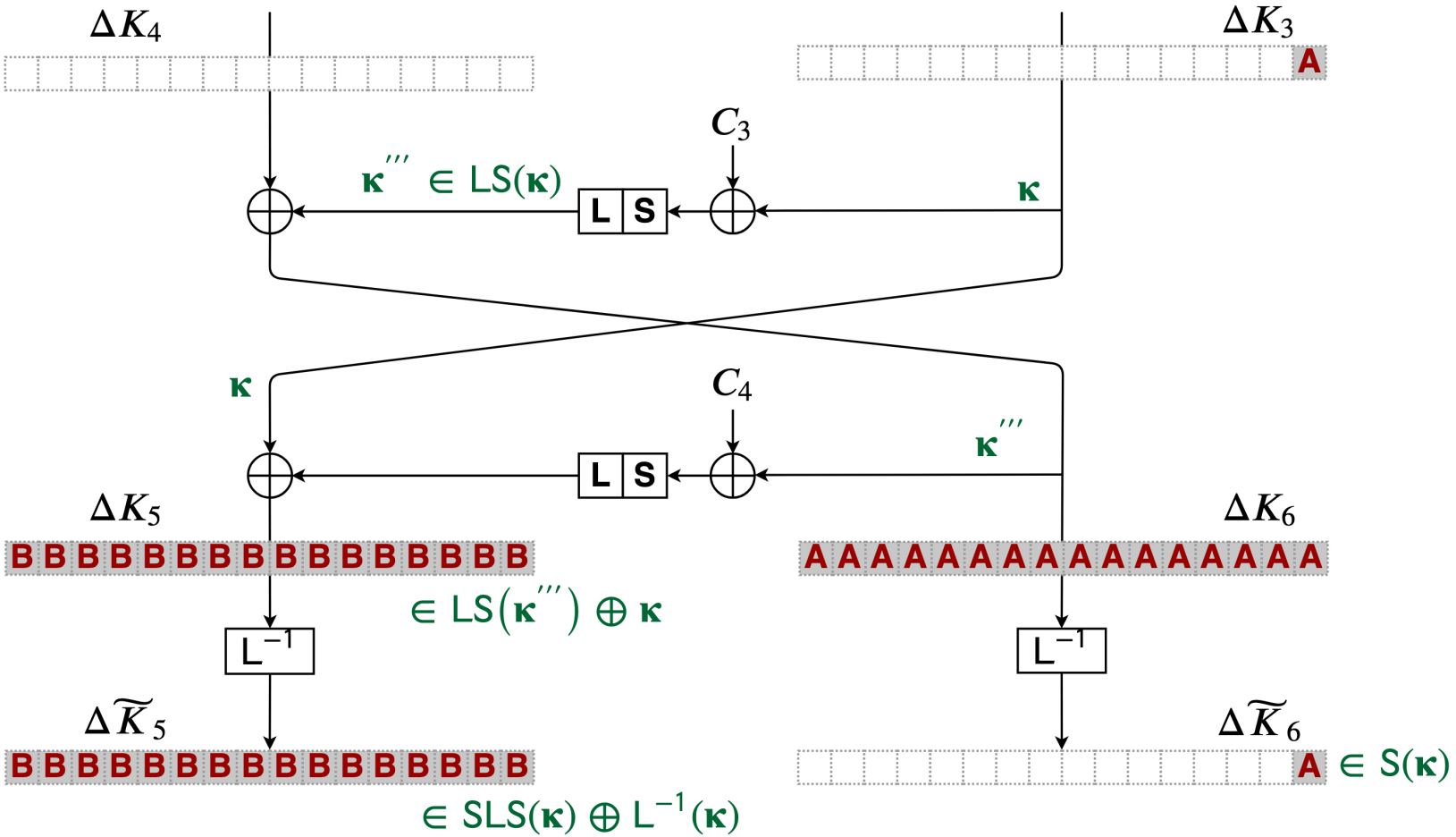
Key schedule

For one collection only $\kappa' = \kappa''$



Integral distinguisher

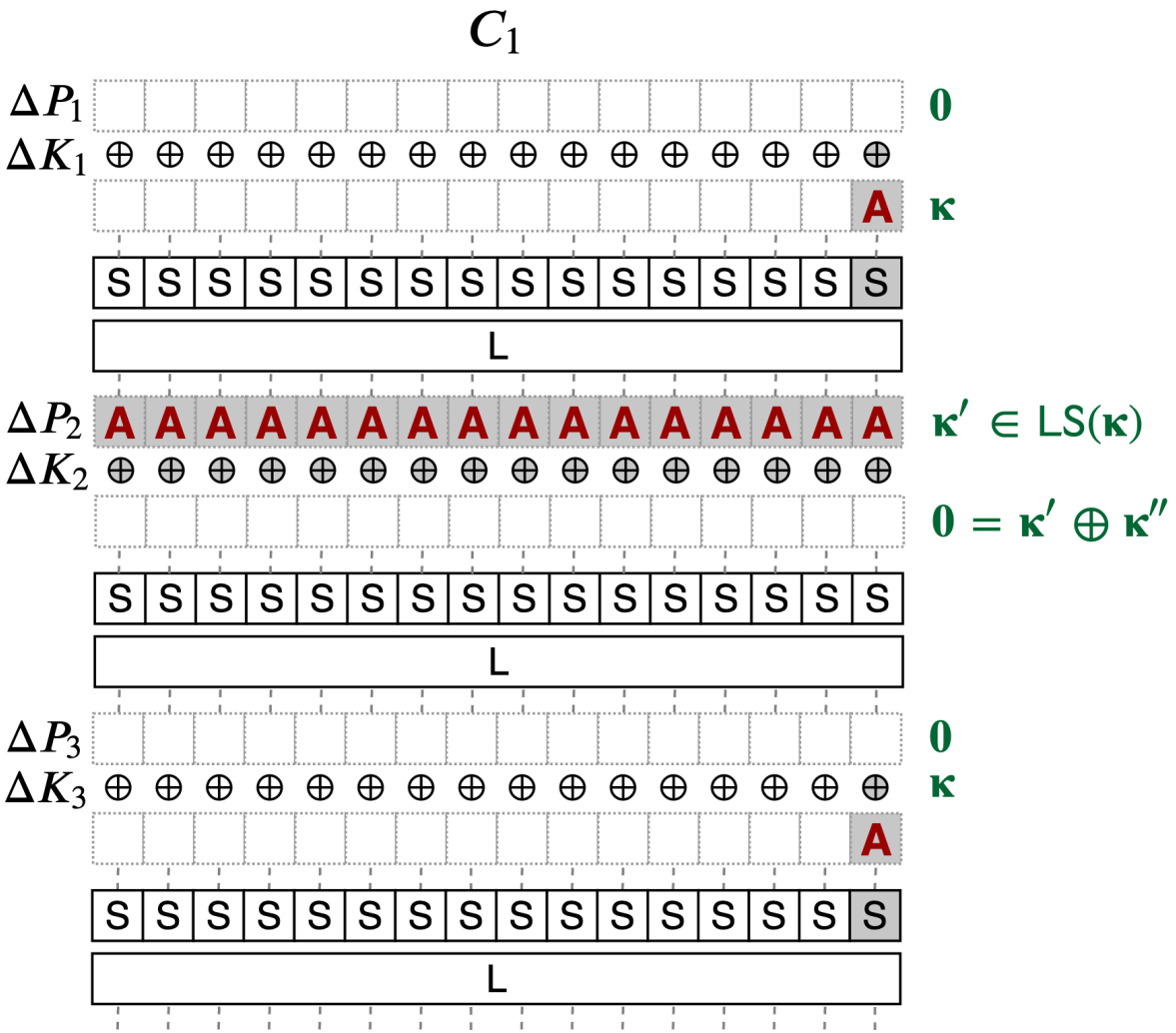
Key schedule



Integral distinguisher

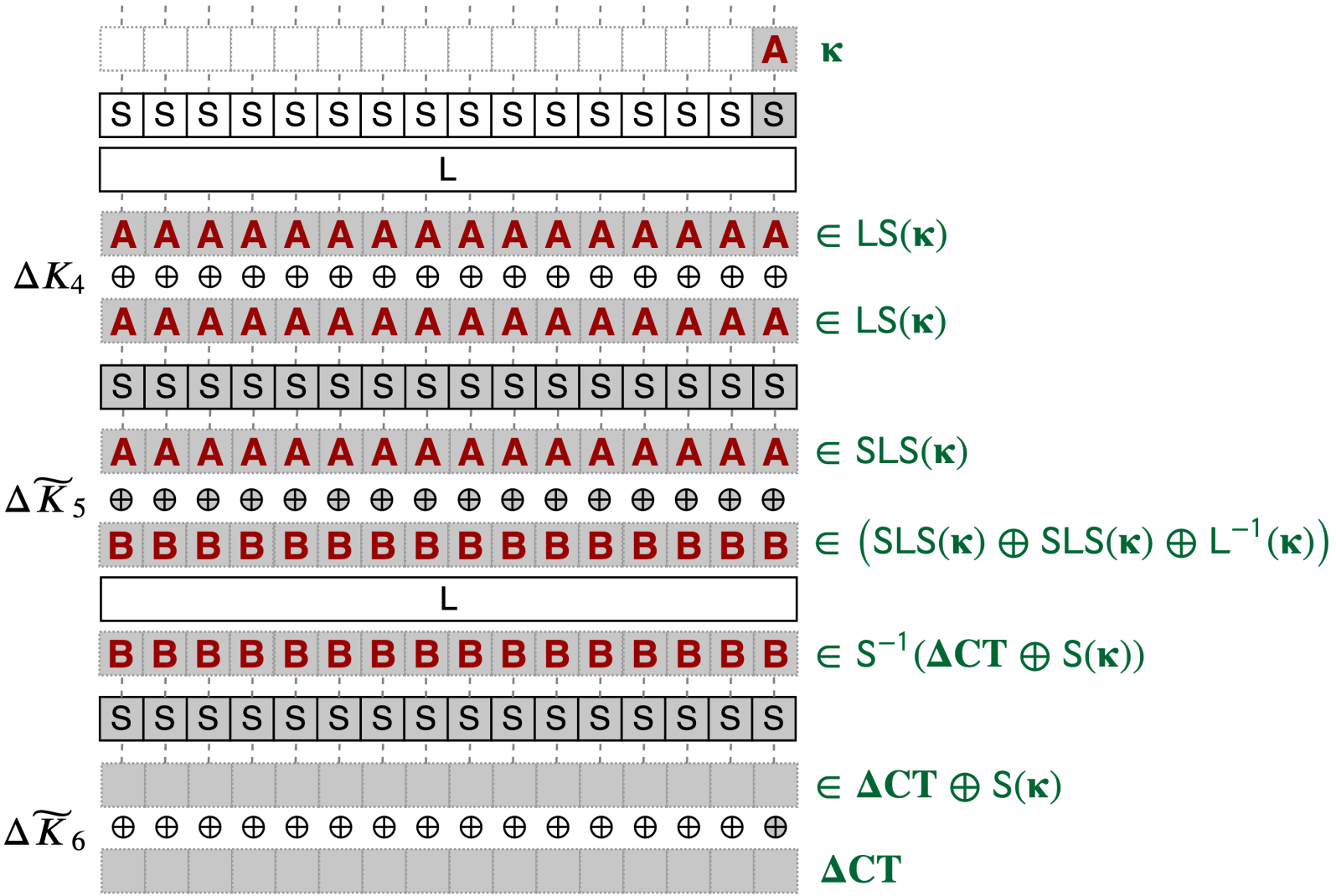
Encryption

$\kappa' = \kappa''$ in key schedule $\Leftrightarrow$ $\kappa' = \kappa''$ in encryption

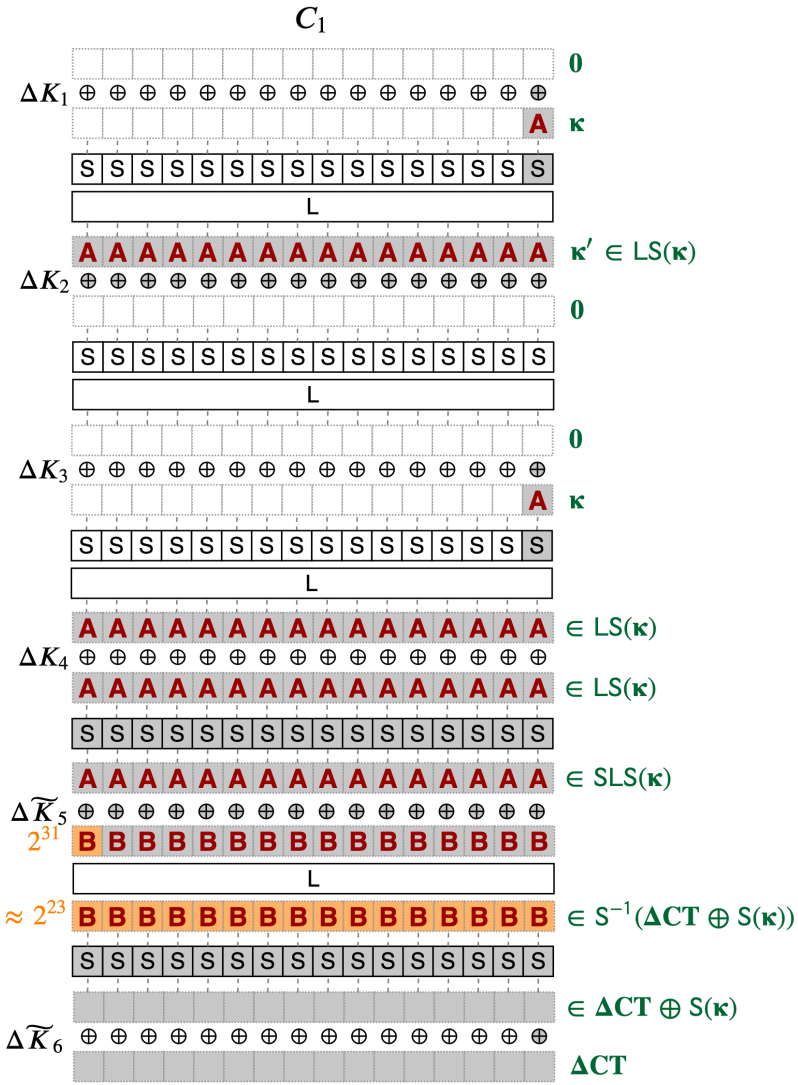


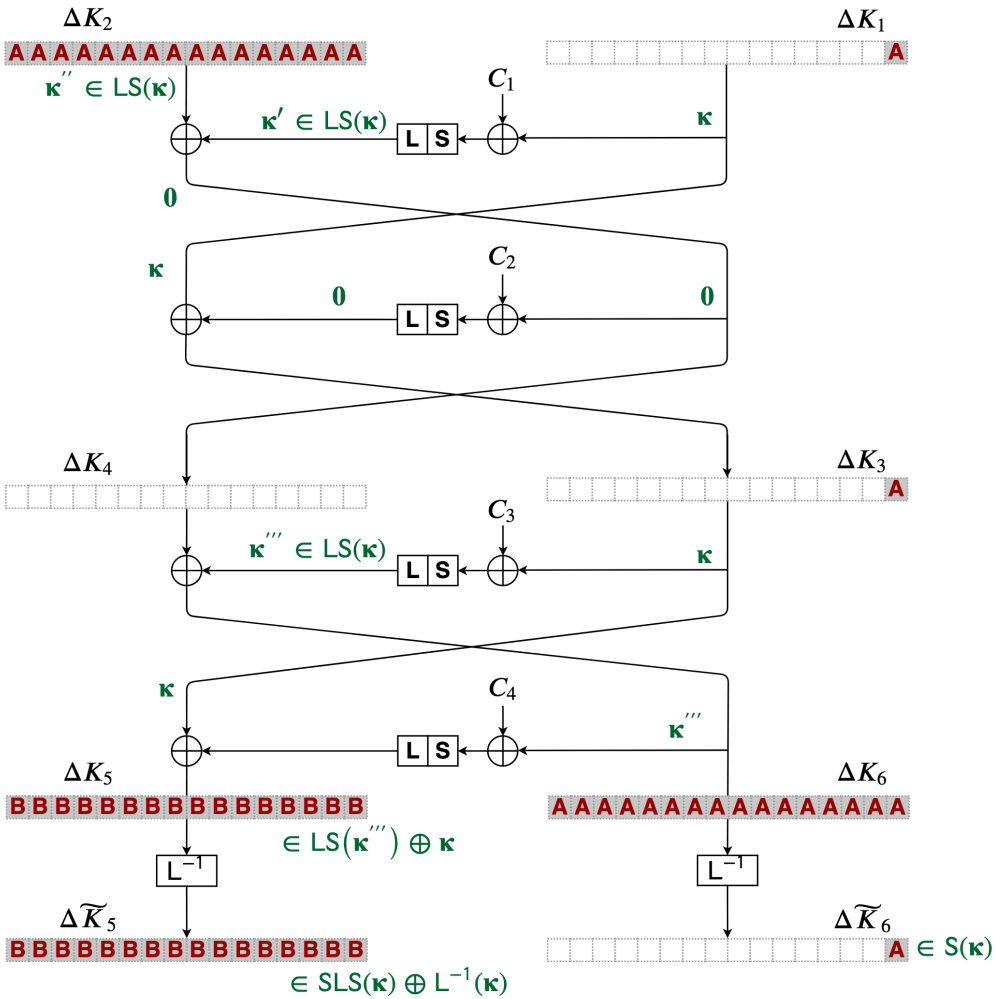
Integral distinguisher

Encryption



Integral distinguisher





Integral distinguisher

Thus, we have

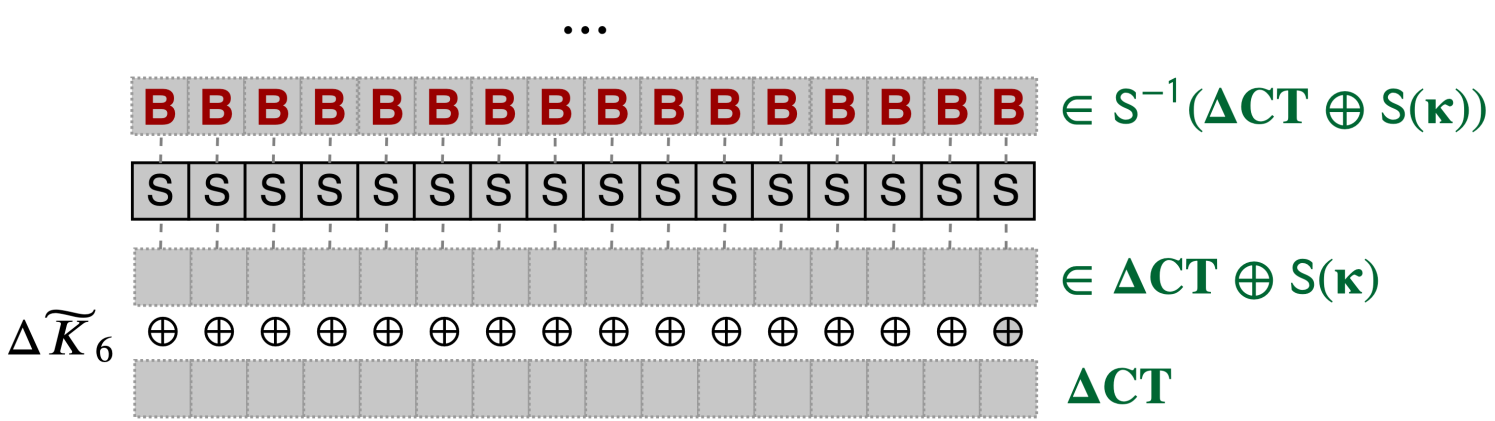
Lemma

*If $\boldsymbol{\kappa}' = \boldsymbol{\kappa}''$ then d-difference before last S-layer has the integral property **B**.*

Recovering of the round keys

1) propagate all differences from $\boldsymbol{\Delta CT} \oplus \mathrm{S}(\boldsymbol{\kappa})$ through S^{-1}

2) check the integral property **B** for each Sbox



If we correctly guessed $\boldsymbol{\kappa''}$, then there must be at least one such difference for each Sbox. Otherwise, we try next collection of the related-keys.

The set $\mathrm{S}^{-1}(\boldsymbol{\Delta CT} \oplus \mathrm{S}(\boldsymbol{\kappa}))$ will contain $\approx 2^{15} \cdot 2^8 = 2^{23}$ differences.

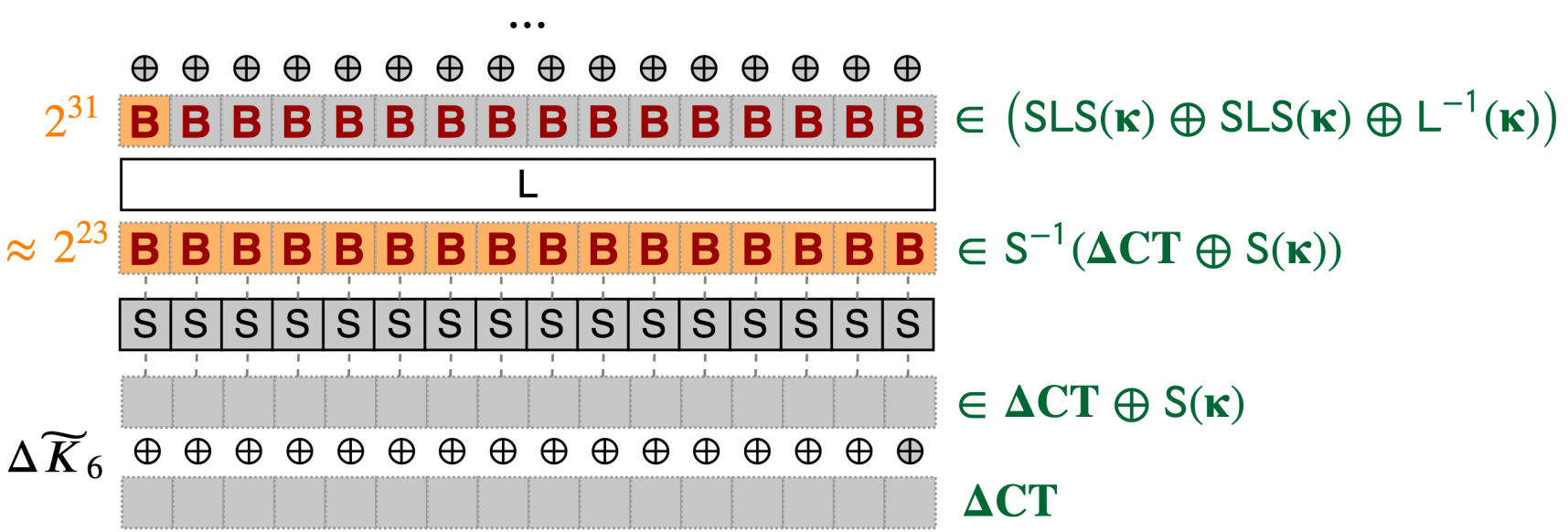
Recovering of the round keys

3) construct the set $(\mathsf{SLS}(\boldsymbol{\kappa}) \oplus \mathsf{SLS}(\boldsymbol{\kappa}) \oplus \mathsf{L}^{-1}(\boldsymbol{\kappa}))$ only for one Sbox

4) find intersection of sets

$$(\mathsf{SLS}(\boldsymbol{\kappa}) \oplus \mathsf{SLS}(\boldsymbol{\kappa}) \oplus \mathsf{L}^{-1}(\boldsymbol{\kappa})) \cap \mathsf{L}^{-1}\mathsf{S}^{-1}(\boldsymbol{\Delta CT} \oplus \mathsf{S}(\boldsymbol{\kappa}))$$

$$\left\{\boldsymbol{\delta_1} \oplus \boldsymbol{\delta_2} \oplus \mathsf{L}^{-1}(\boldsymbol{\kappa}),\ \boldsymbol{\delta_1} \in \mathsf{SLS}(\boldsymbol{\kappa}),\ \boldsymbol{\delta_2} \in \mathsf{SLS}(\boldsymbol{\kappa})\right\} \cap \mathsf{L}^{-1}\mathsf{S}^{-1}(\boldsymbol{\Delta CT} \oplus \mathsf{S}(\boldsymbol{\kappa}))$$



Recovering of the round keys

3) construct the set $(\mathsf{SLS}(\boldsymbol{\kappa}) \oplus \mathsf{SLS}(\boldsymbol{\kappa}) \oplus \mathsf{L}^{-1}(\boldsymbol{\kappa}))$ only for one Sbox

4) find intersection of sets

$$(\mathsf{SLS}(\boldsymbol{\kappa}) \oplus \mathsf{SLS}(\boldsymbol{\kappa}) \oplus \mathsf{L}^{-1}(\boldsymbol{\kappa})) \cap \mathsf{L}^{-1}\mathsf{S}^{-1}(\boldsymbol{\Delta CT} \oplus \mathsf{S}(\boldsymbol{\kappa}))$$

First set contains

$$\frac{2^{16} \cdot (2^{16} - 1)}{2} + 1 < 2^{31}$$

differences.

We expect that the intersection contains no more than one difference.

If intersection is empty then we try next collection of the related-keys.

Recovering of the round keys

5) we know the difference before last S-layer $\Rightarrow$ we can compute keys $\widetilde{K}_6$

6) decrypt all ciphertexts with keys $\widetilde{K}_6$

7) the keys $\widetilde{K}_5$ can be found in the same way as $\widetilde{K}_6$

8) due to the reverse key schedule, the master key $K = K_1||K_2$ can be easily obtained

Complexity

The attack require:

- $1 + 2^8 \cdot \left(2^8 - 1\right) < 2^{16}$ related keys
- one chosen plaintext
- about 2^{32} memory access operations
- 2^{30} memory (in 16-byte blocks)

Conclusion

- Related-key attack on 5-round Kuznyehcik with 2-round key schedule
- Practical complexity: 2^{32} operations, 2^{30} memory, 2^{16} related keys
- Verification: about 5 minutes on a common PC
- Source codes https://gitlab.com/v.kir/rk-5R-kuznyechik

Thank you for attention!

Questions?