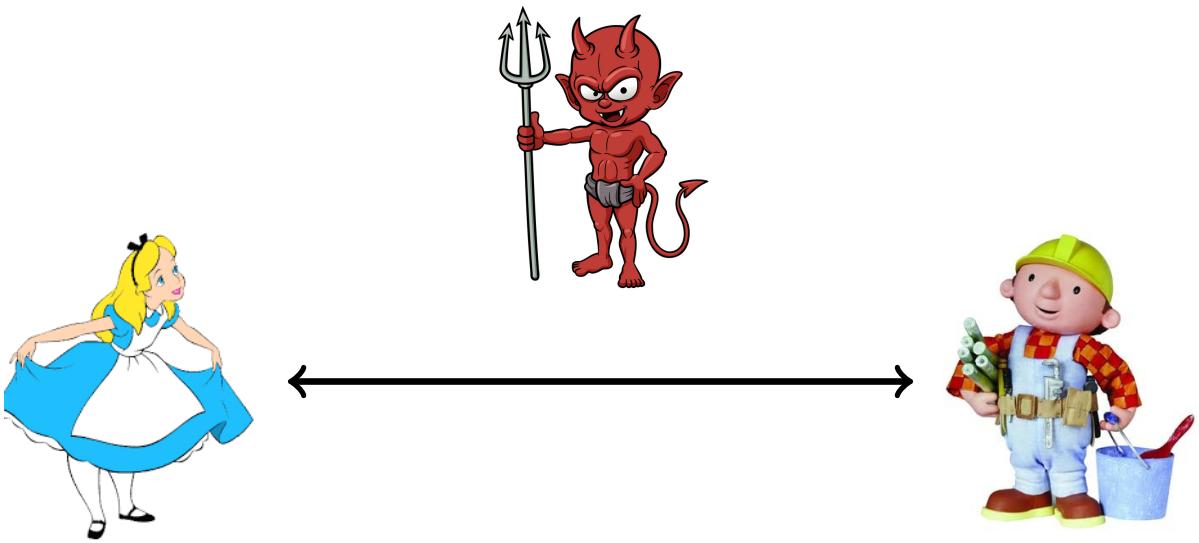
Cryptanalysis of Full Pyjamask-96

Christoph Dobraunig and Yann Rotella and Jan Schoone

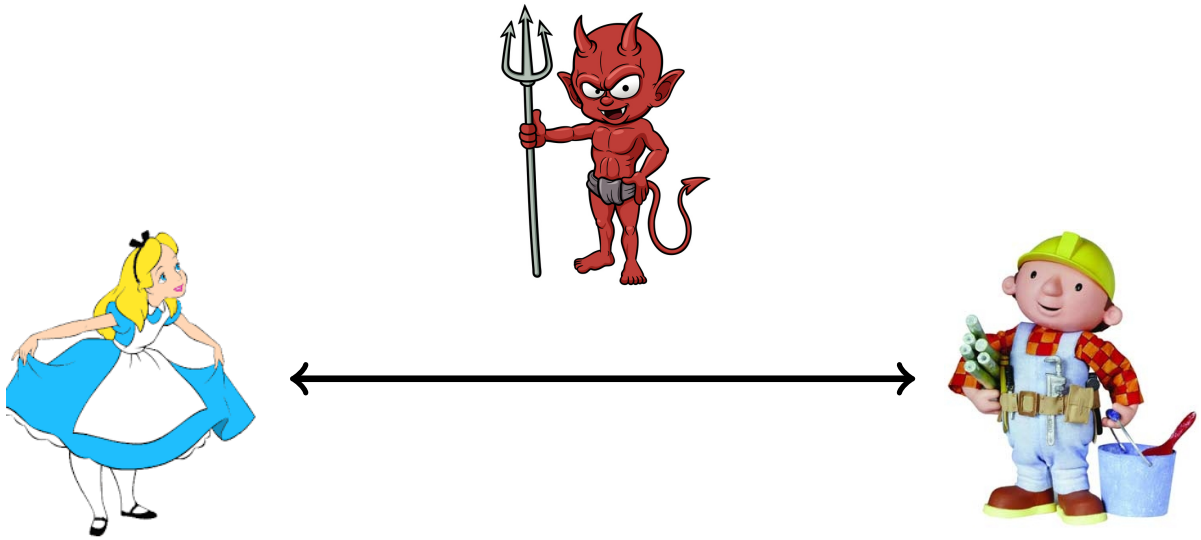
September 4, 2019

Cryptography



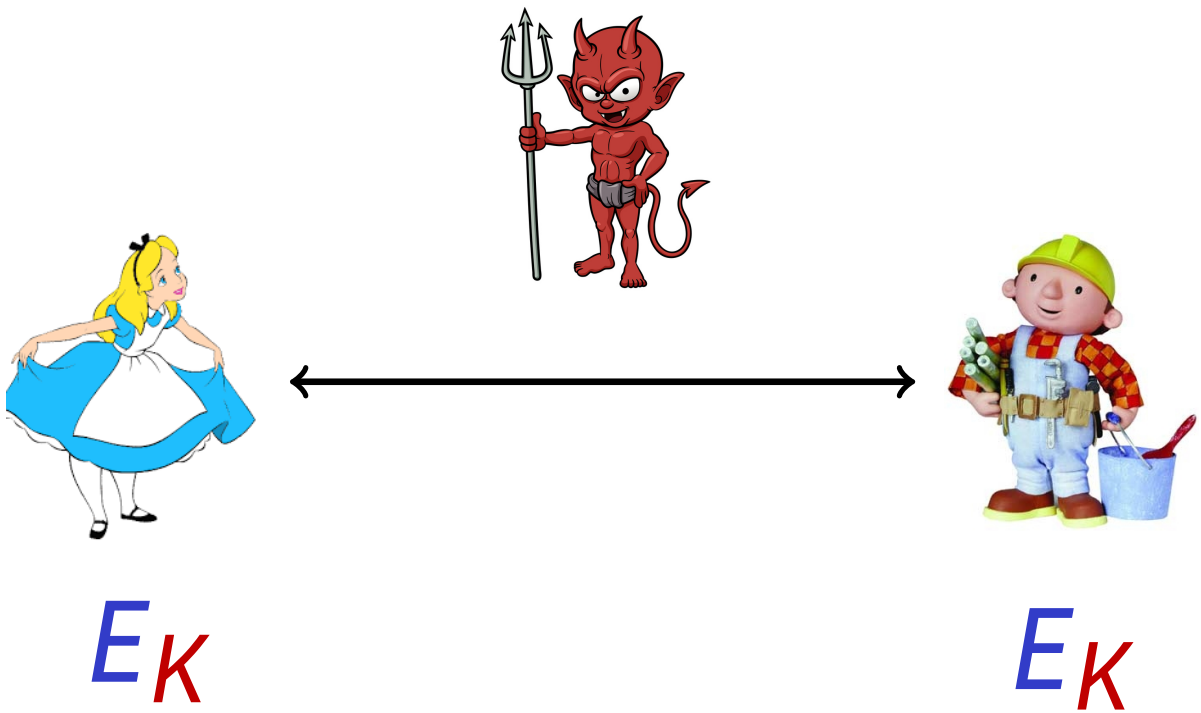
- Authenticity
- Integrity
- Confidentiality

Symmetric Cryptography

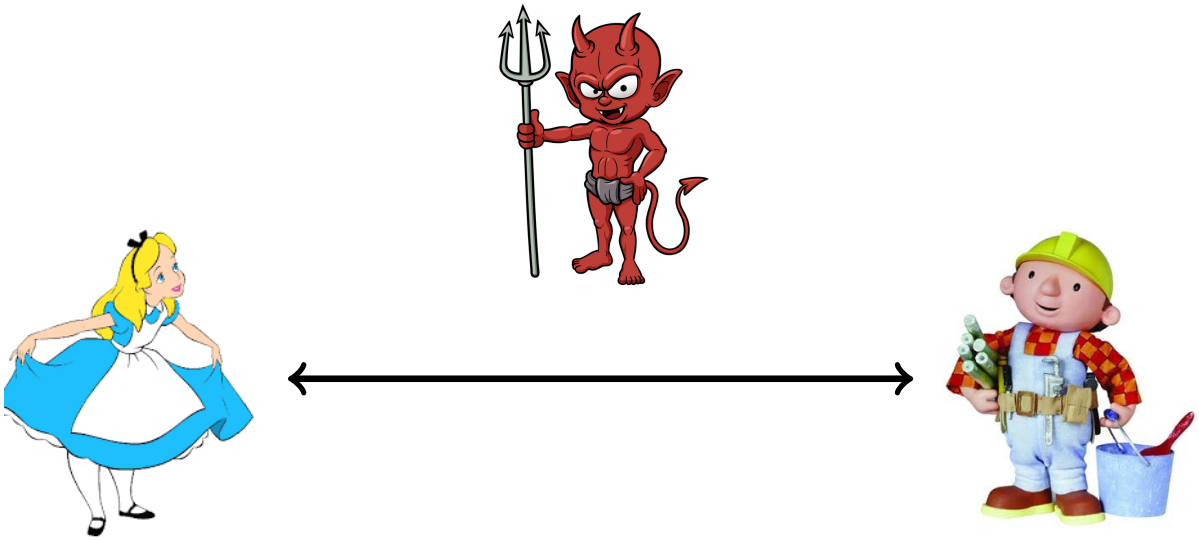


K K

Symmetric Cryptography



Symmetric Cryptography



$$c = E_K(m) \qquad m = E_K^{-1}(c)$$

NIST Competition

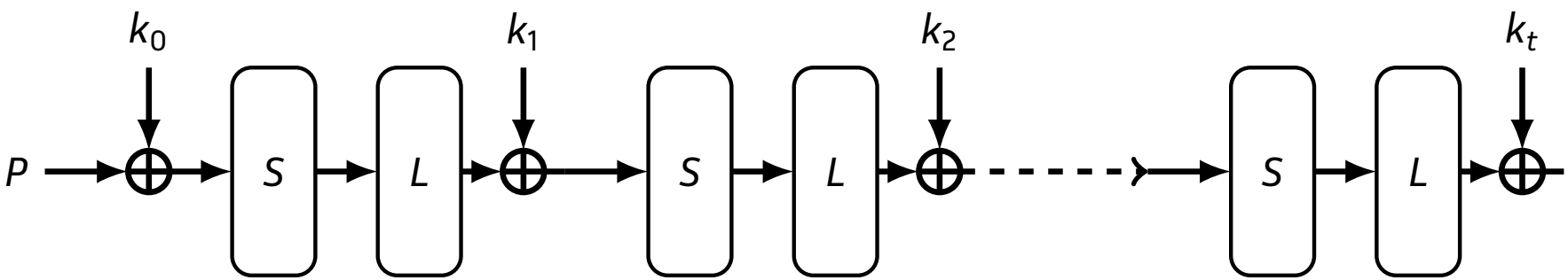
- 56 submissions: Permutation-based, Block-cipher based , Stream-cipher
- Some issues with domain separations
- Implementations issues found
- 15 attacks
- hardware, software, fault resistance, side channel resistance
- Round 2 announced on Friday: 32 candidates up to September 1, 2020

Structure of this Talk

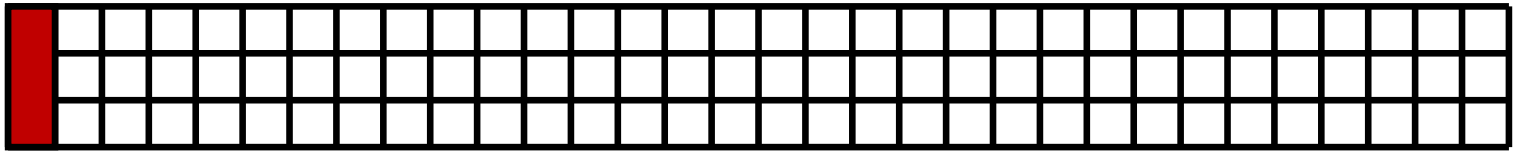
Plan of this Section

Description

- OCB
- SPN, with 96 and 128 bit length



The round function



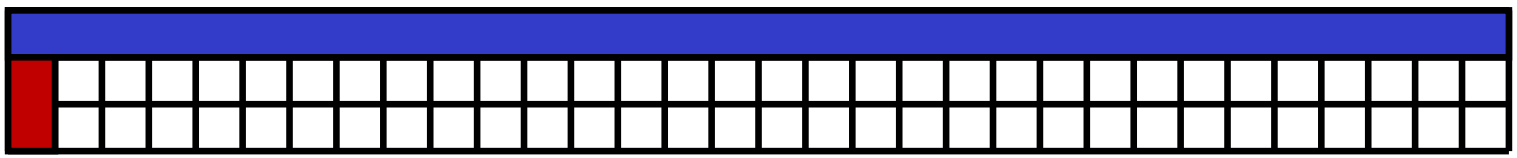
The S-box layer:

- 96-bit: quadratic S-box on 3 bits
- 128-bit: S-box of degree 3, on 4 bits

The linear layer:

- Circulant matrices of size 32 on each row
- vectors defining the matrices of weight 11 or 13

The round function



The S-box layer:

- 96-bit: quadratic S-box on 3 bits
- 128-bit: S-box of degree 3, on 4 bits

The linear layer:

- Circulant matrices of size 32 on each row
- vectors defining the matrices of weight 11 or 13

Plan of this Section

Degrees of Pyjamask [Boura, Canteaut IEEE-2013]

Round	1	2	3	4	5	6	7	8	9	10	11	12+
96-bit	2	4	8	16	32	64	80	88	92	**94**	95	95
128-bit	3	9	27	81	112	122	126	127	127	127	127	127

Integral property on 10 rounds

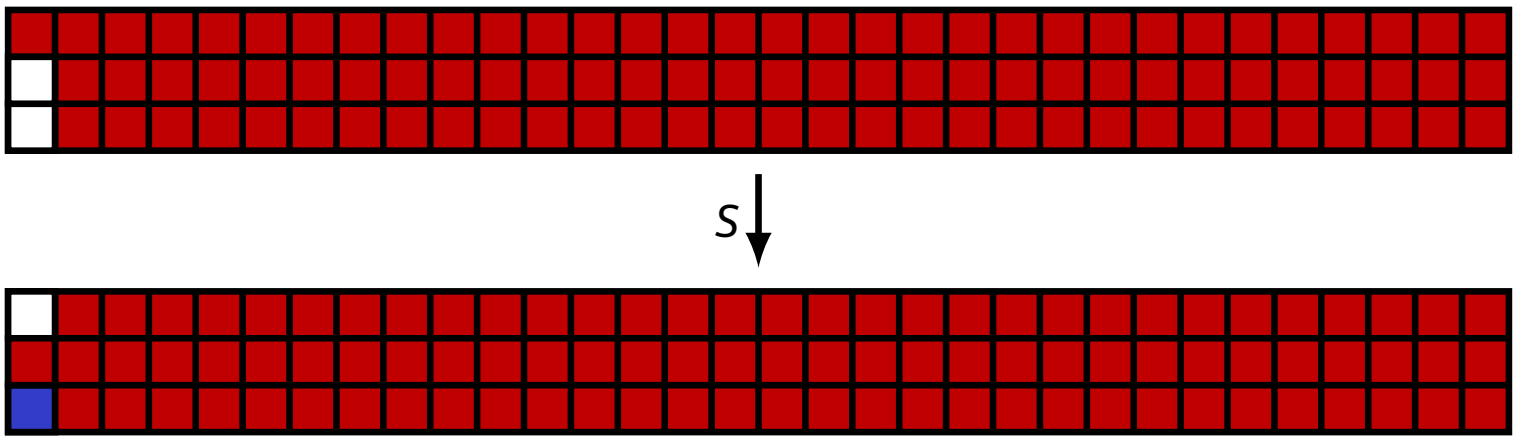
Definition (Higher-order derivative)

Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$.

$$\Delta_V F(x) = \Delta_{a_1}\Delta_{a_2}\cdots\Delta_{a_k}F(x) = \sum_{v\in V} F(x+v)\,, \forall x \in \mathbb{F}_2^n$$

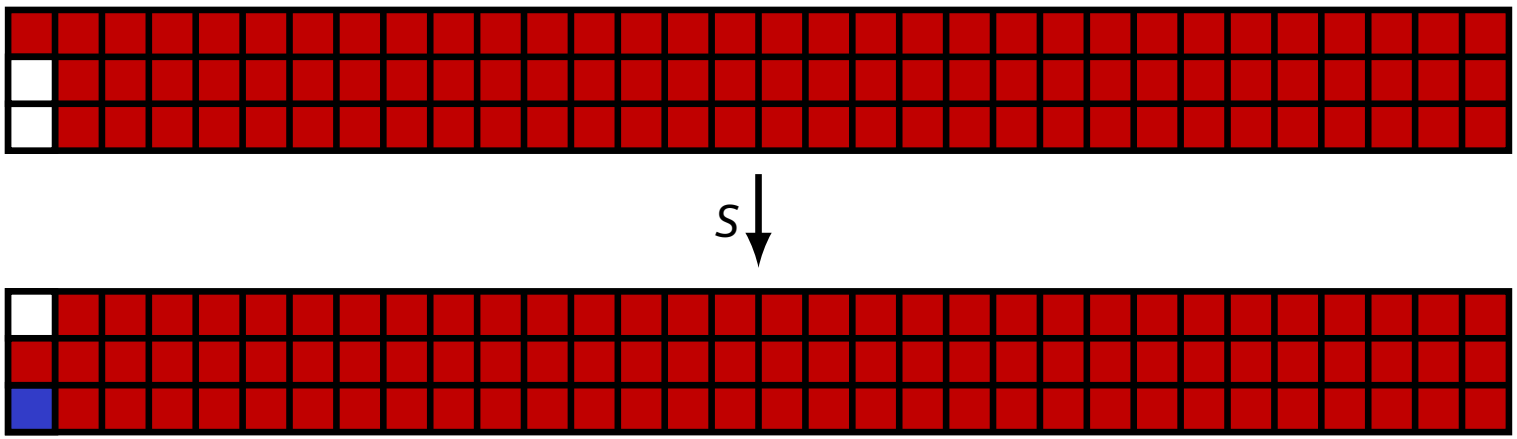
- Put an affine space of dimension 94 -> Get a constant after 10 rounds.

Extend to 11 rounds



- Value in blue depends on three key bits;
- For one input affine space we recover 3 equations;

Extend to 11 rounds

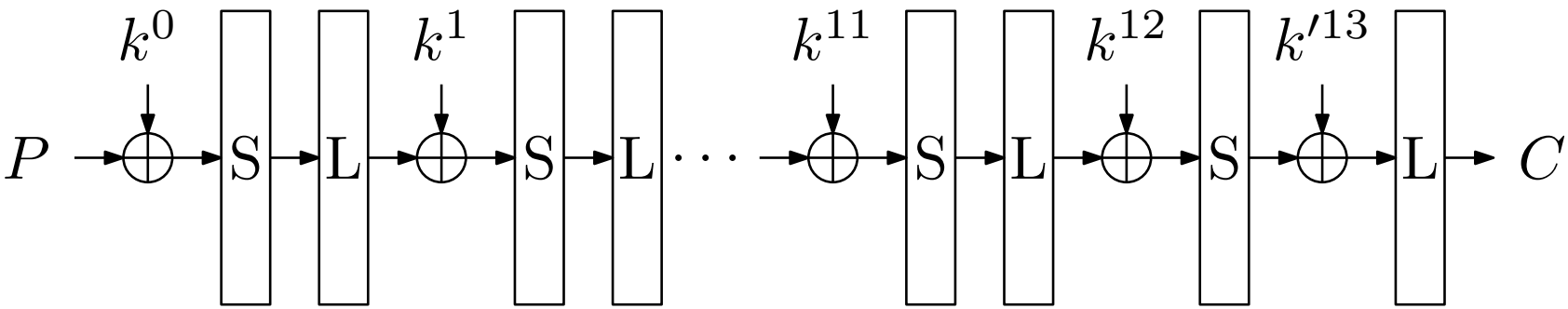


- Value in blue depends on three key bits;
- For one input affine space we recover 3 equations;
- 7 different affine spaces and 32 S-boxes;
- Gives $(3 \cdot 7 - 7) \cdot 32 = 448$ equations.

Remaining work

Precompute $f_i(k_0'^{13}, k_1'^{13}, k_3'^{13})$ for fixed vectorspace

Evaluate $\sum_j \left(g_i(k^0, k^1, P_j)\right)$



Plan of this Section

Classical algebraic cryptanalysis

Integral distinguisher on 11 rounds gives 448 equations.

- We have to solve a system of 448 equations, but we have 3 rounds to pass.
- Three rounds is of degree 8.
- linearization technique:

$$\sum_{i=1}^{8} \binom{96+128}{i} \approx 2^{47}.$$

Counting number of monomials

- add ciphertext and key -> gives 2 monomials
- S-box layer -> gives $2^2 + 6 = 10$ monomials
- Linear layer -> gives $13 \cdot 10 = 130$ monomials
- add key -> gives 92 monomials
- S-box -> $130^2 + 3 \cdot 130$ monomials

This gives 2^{37} monomials

Finding and solving the system

$$\sum_{x \in V} f(x, k) = 0$$

where $|V| = 2^{94}$ and $c \in \mathcal{C}$.
For example:

Finding and solving the system

$$\sum_{x \in V} f(x, k) = 0$$

where $|V| = 2^{94}$ and $c \in \mathcal{C}$.
For example:

$$f(x,k) = x_0x_1k_0 + x_1x_2k_1k_2 + x_0k_1k_2 + x_0x_1k_3 + x_3k_3 + x_0k_0$$

Finding and solving the system

$$\sum_{x \in V} f(x, k) = 0$$

where $|V| = 2^{94}$ and $c \in \mathcal{C}$.
For example:

$$f(x,k) = x_0x_1k_0 + x_1x_2k_1k_2 + x_0k_1k_2 + x_0x_1k_3 + x_3k_3 + x_0k_0$$

$$[x_0x_1, x_1x_2, x_0, x_3]$$

Finding and solving the system

$$\sum_{x \in V} f(x, k) = 0$$

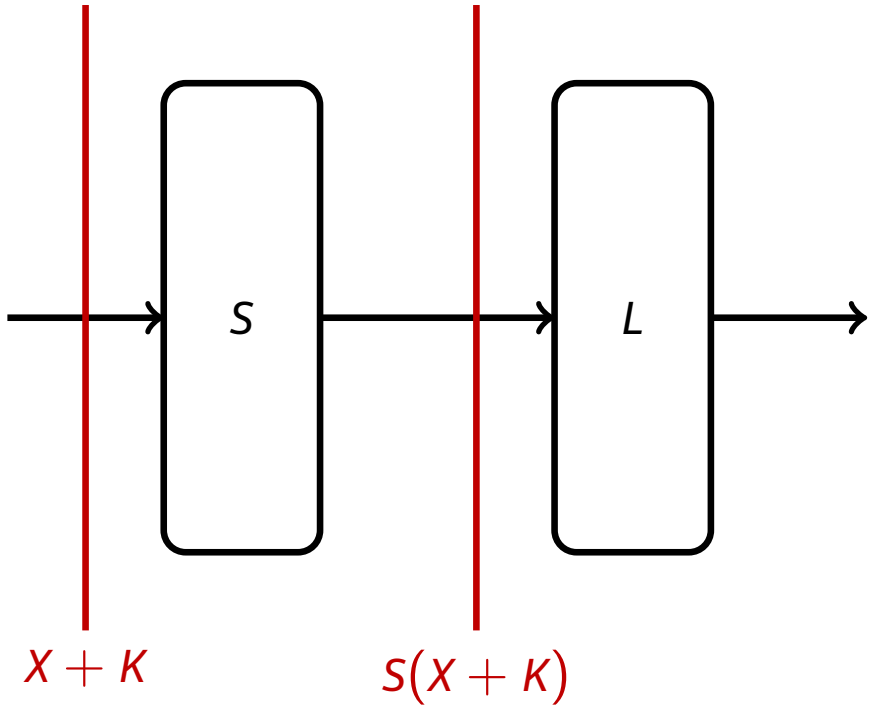
where $|V| = 2^{94}$ and $c \in \mathcal{C}$.
For example:

$$f(x,k) = x_0x_1k_0 + x_1x_2k_1k_2 + x_0k_1k_2 + x_0x_1k_3 + x_3k_3 + x_0k_0$$

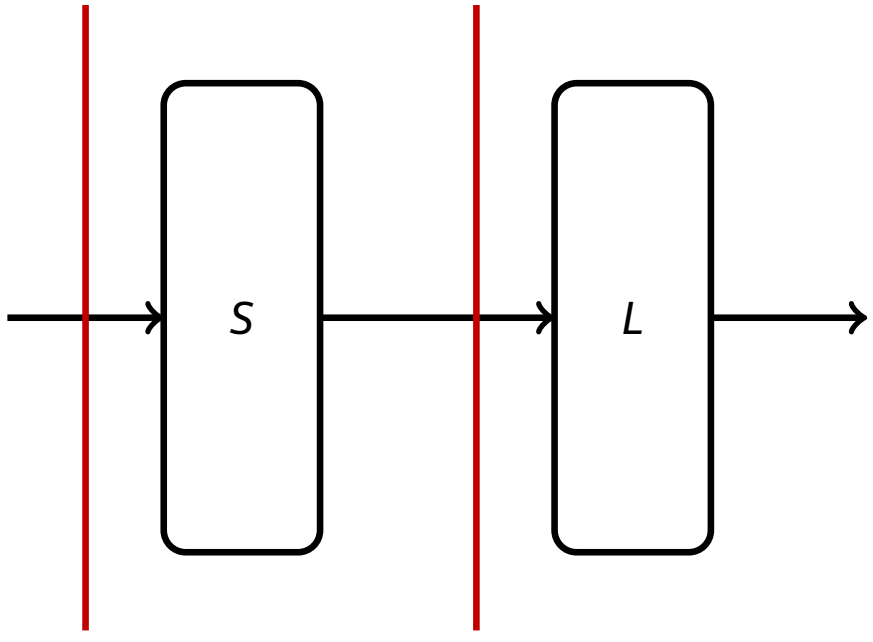
$$[x_0x_1, x_1x_2, x_0, x_3]$$

$$[k_0, k_1k_2, k_3]$$

Using quadratic properties

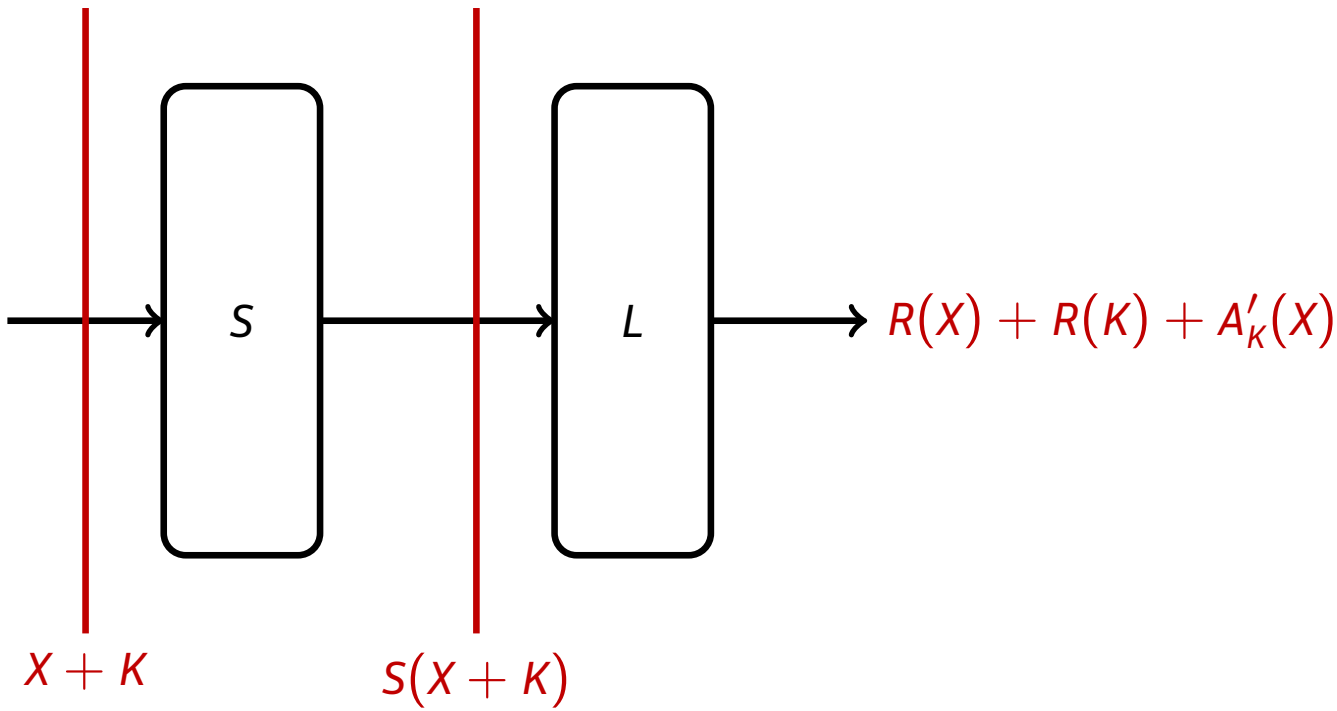


Using quadratic properties



$$= S(X) + S(K) + A_K(X)$$

Using quadratic properties



Plan of this Section

Conclusion

- Full-round attack: 2^{113}
- Huge data complexity: 2^{96}
- Very small memory complexity: 2^{20}

Thanks!
Questions?