A generalization of Linear Cryptanalysis

Diploma Work

Thomas Baignères (thomas.baigneres@epfl.ch)

Diploma Professor

Prof. Serge Vaudenay (serge.vaudenay@epfl.ch)

LASEC

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Contents

Contents

Contents

1. Presentation of the cipher
2. Linear Cryptanalysis of the cipher
3. Generalization of critical notions
    - Generalized *linear expressions*
    - Generalized *bias*

Contents

Contents

1. Presentation of the cipher
2. Linear Cryptanalysis of the cipher
3. Generalization of critical notions
   - Generalized *linear expressions*
   - Generalized *bias*
4. Generalized linear cryptanalysis of the cipher
5. Limitations, further improvements and conclusion.

Presentation of the cipher (1)

Presentation based on a symmetric-key block cipher.

Inspired from a tutorial from Howard M. Heys.

Presentation of the cipher (1)

Presentation based on a symmetric-key block cipher.
Inspired from a tutorial from Howard M. Heys.

Invertible function, mapping a 16-bits plaintext block P to a 16-bits ciphertext block C.

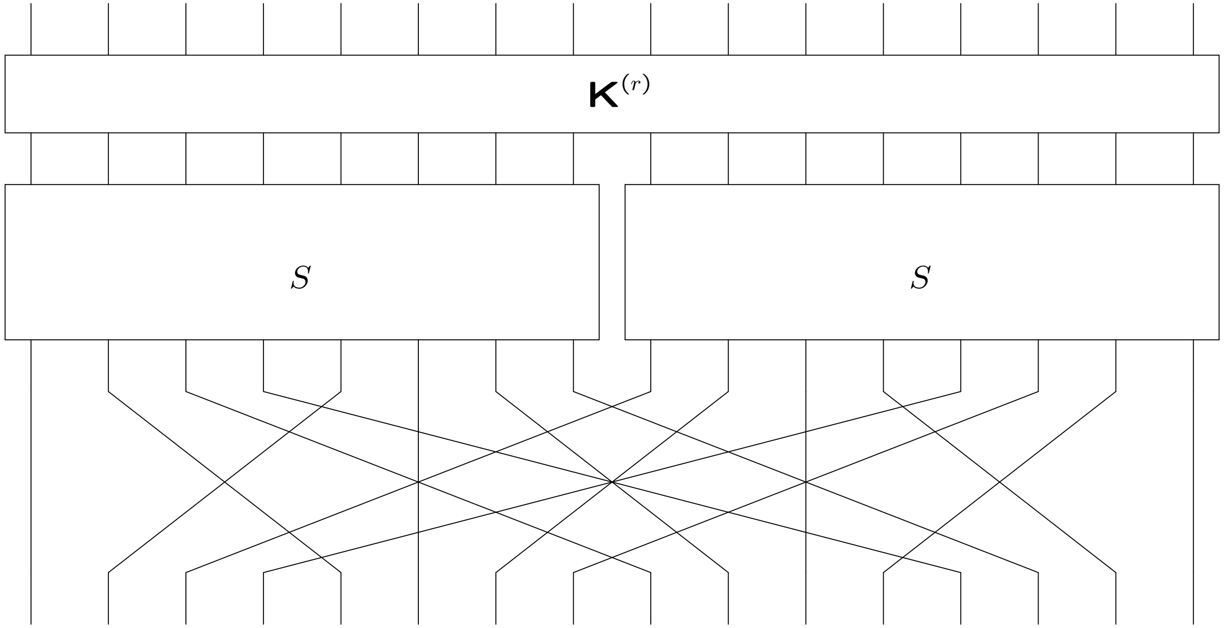
Presentation of the cipher (1)

Presentation based on a symmetric-key block cipher.
Inspired from a tutorial from Howard M. Heys.

Invertible function, mapping a 16-bits plaintext block P to a 16-bits ciphertext block C.

Our block cipher is a simple SPN, made of 3 identical rounds, followed by an additional round.

Presentation of the cipher (2)

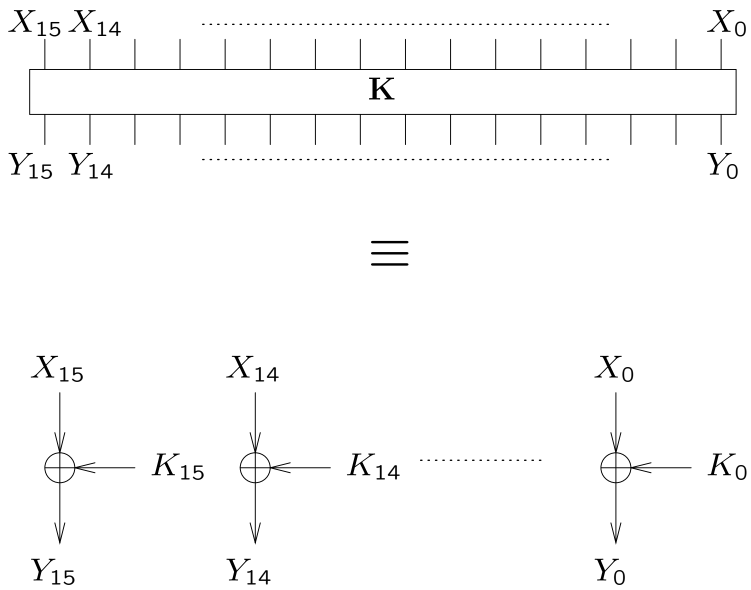


One round of the cipher:

- Key-xoring
- Substitution-box (from AES)
- Permutation

Presentation of the cipher (3)

Key xoring:



Presentation of the cipher (4)

Substitution Box:

Permutation applied to one byte.

$$
\begin{array}{ccc}
\texttt{0x00} & \xrightarrow{S} & \texttt{0x63} \\
\texttt{0x01} & \xrightarrow{S} & \texttt{0x7c} \\
\vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots \\
\texttt{0xff} & \xrightarrow{S} & \texttt{0x16}
\end{array}
$$

Presentation of the cipher (4)

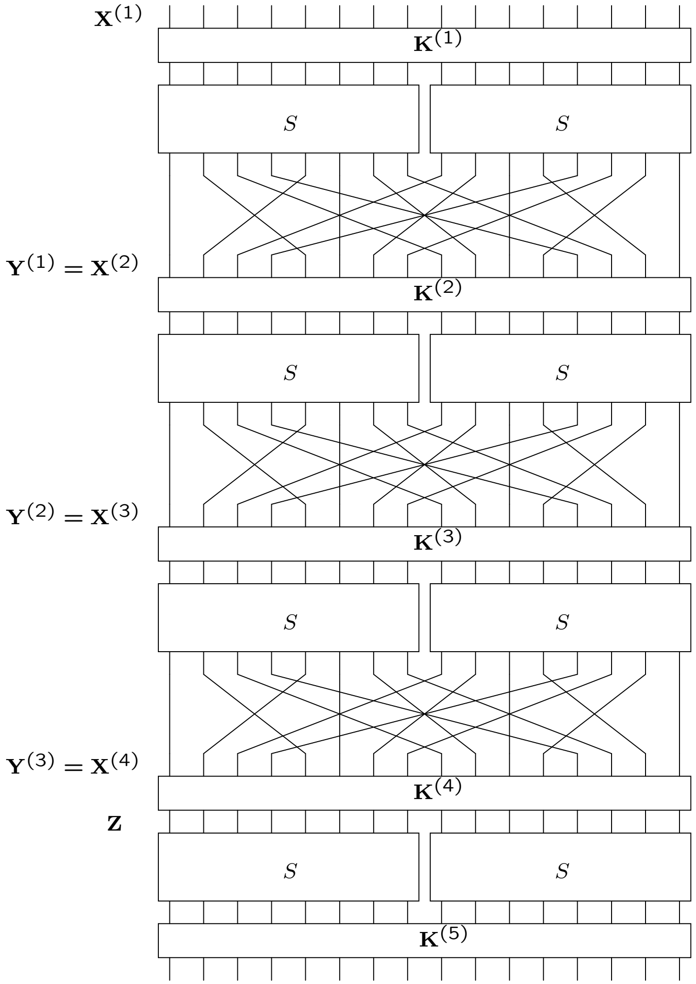
Substitution Box:

Permutation applied to one byte.

$$
\begin{array}{ccc}
\texttt{0x00} & \xrightarrow{S} & \texttt{0x63} \\
\texttt{0x01} & \xrightarrow{S} & \texttt{0x7c} \\
\vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots \\
\texttt{0xff} & \xrightarrow{S} & \texttt{0x16}
\end{array}
$$

This is the only non-linear transformation of the round.

Presentation of the cipher (5)



Linear Cryptanalysis of the cipher (1)

(Short) Historical review:

- Linear cryptanalysis is a statistical attack presented in 1993 by Matsui.

Linear Cryptanalysis of the cipher (1)

(Short) Historical review:

- Linear cryptanalysis is a statistical attack presented in 1993 by Matsui.
- It is a known-plaintext attack:

  The cryptanalyst has access to the ciphertext of several messages, and to the plaintext of those messages.

Linear Cryptanalysis of the cipher (1)

(Short) Historical review:

- Linear cryptanalysis is a statistical attack presented in 1993 by Matsui.
- It is a known-plaintext attack:

  The cryptanalyst has access to the ciphertext of several messages, and to the plaintext of those messages.

- Refined version in 1994 which allowed to break DES.

Linear Cryptanalysis of the cipher (1)

(Short) Historical review:

- Linear cryptanalysis is a statistical attack presented in 1993 by Matsui.
- It is a known-plaintext attack:

  The cryptanalyst has access to the ciphertext of several messages, and to the plaintext of those messages.

- Refined version in 1994 which allowed to break DES.
- Statistical part optimized by Pascal Junod and Serge Vaudenay in 2003.

Linear Cryptanalysis of the cipher (2) - First phase

Objective : Find an linear expression that approximates 3 rounds of the cipher.

Linear Cryptanalysis of the cipher (2) - First phase

Objective : Find an linear expression that approximates 3 rounds of the cipher.

$$\underbrace{\mathbf{a}\cdot \mathsf{P}}_{\text{one bit}} \oplus \underbrace{\mathbf{b}\cdot \mathbf{Z}}_{\text{one bit}} = 0 \qquad \mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{15} \end{pmatrix} \qquad \mathbf{b} = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{15} \end{pmatrix}$$

with $a_i \in \{0,1\}$ and $b_j \in \{0,1\}$ for all i, j.

The operator $\cdot$ is the inner-dot product:

$$\mathbf{a}\cdot \mathsf{P} = a_0\mathsf{P}_0 \oplus a_1\mathsf{P}_1 \oplus \cdots \oplus a_{15}\mathsf{P}_{15}$$

Linear Cryptanalysis of the cipher (3) - First phase

Objective : Find an effective linear expression that approximates 3 rounds of the cipher.

Linear Cryptanalysis of the cipher (3) - First phase

Objective : Find an effective linear expression that approximates 3 rounds of the cipher.

$$\underbrace{\mathbf{a} \cdot \mathsf{P}}_{\text{one bit}} \oplus \underbrace{\mathbf{b} \cdot \mathbf{Z}}_{\text{one bit}} = 0$$

If the linear expression holds with probability p, the value

$$\epsilon = \left| p - \frac{1}{2} \right|$$

must be far from 0. This is the bias of the linear expression.

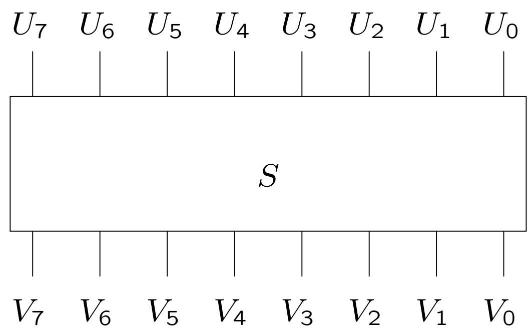
Linear Cryptanalysis of the cipher (4) - First phase

Question: How do we find such an expression ?

Linear Cryptanalysis of the cipher (4) - First phase

Question: How do we find such an expression ?

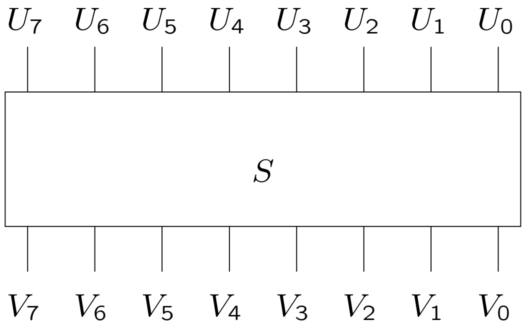
Non-linear transformations of the cipher: the substitution boxes.



Find a linear expression $\mathbf{a} \cdot \mathbf{U} \oplus \mathbf{b} \cdot \mathbf{V} = 0$ on the S-box, with a large bias.

Linear Cryptanalysis of the cipher (5) - First phase

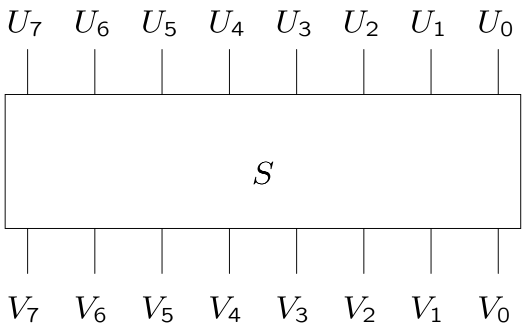
Example:



$$U_1 \oplus U_5 \oplus V_3 = 0$$

Linear Cryptanalysis of the cipher (5) - First phase

Example:



$$U_1 \oplus U_5 \oplus V_3 = 0$$

Set c to 0. For every input $\mathbf{U}$, increment c if the equation holds.

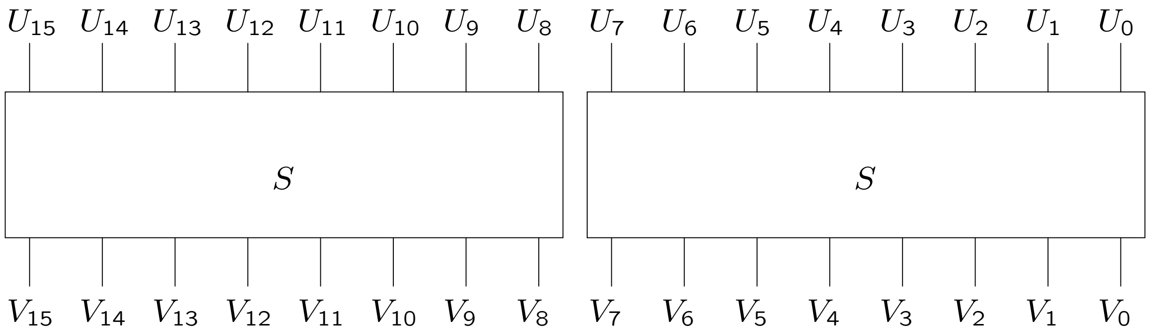
$$p = \frac{c}{2^8}$$

The equation is effective if $\epsilon = \left| p - \frac{1}{2} \right|$ is far from 0.

Linear Cryptanalysis of the cipher (6) - First phase

Suppose that the following equations have a large bias:

$$
\begin{aligned}
U_1 \oplus U_5 \oplus V_3 &= 0 \qquad \epsilon_1 \\
U_{12} \oplus V_{15} &= 0 \qquad \epsilon_2
\end{aligned}
$$

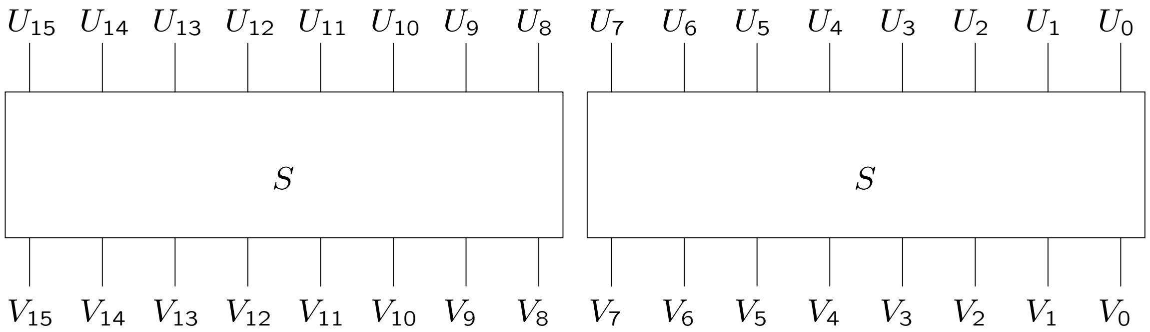


How do we find an expression on the whole S-box layer ?

Linear Cryptanalysis of the cipher (6) - First phase

Suppose that the following equations have a large bias:

$$U_1 \oplus U_5 \oplus V_3 = 0 \qquad \epsilon_1$$
$$U_{12} \oplus V_{15} = 0 \qquad \epsilon_2$$



How do we find an expression on the whole S-box layer ?

Using the piling-up lemma.

Linear Cryptanalysis of the cipher (7) - First phase

$$\begin{aligned} U_1 \oplus U_5 \oplus V_3 &= 0 \qquad \epsilon_1 \\ U_{12} \oplus V_{15} &= 0 \qquad \epsilon_2 \end{aligned}$$

Linear Cryptanalysis of the cipher (7) - First phase

$$\begin{aligned} U_1 \oplus U_5 \oplus V_3 &= 0 \qquad \epsilon_1 \\ U_{12} \oplus V_{15} &= 0 \qquad \epsilon_2 \end{aligned}$$

Then bias of

$$U_1 \oplus U_5 \oplus U_{12} \oplus V_3 \oplus V_{15} = 0$$

is

$$\epsilon = 2\epsilon_1\epsilon_2$$

Linear Cryptanalysis of the cipher (7) - First phase

$$\begin{aligned} U_1 \oplus U_5 \oplus V_3 &= 0 \qquad \epsilon_1 \\ U_{12} \oplus V_{15} &= 0 \qquad \epsilon_2 \end{aligned}$$

Then bias of

$$U_1 \oplus U_5 \oplus U_{12} \oplus V_3 \oplus V_{15} = 0$$

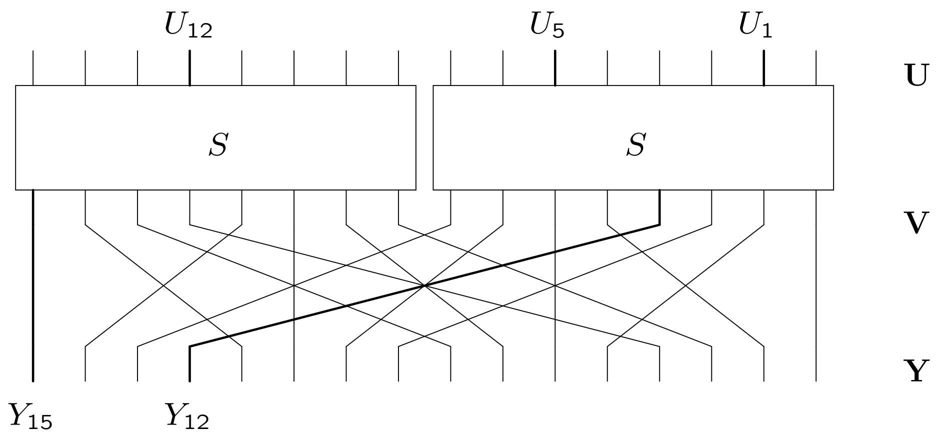
is

$$\epsilon = 2\epsilon_1\epsilon_2$$

We know how to find effective linear expressions on the S-box layer.

Linear Cryptanalysis of the cipher (8) - First phase

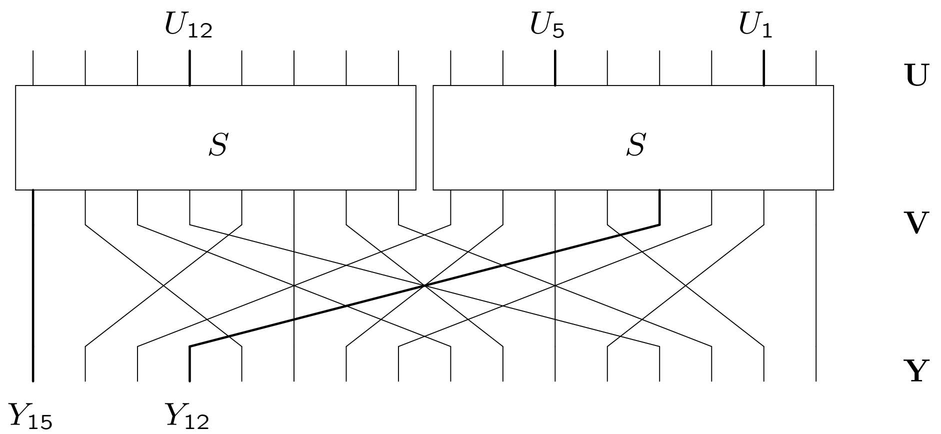
Going through the permutation is easy...



$$U_1 \oplus U_5 \oplus U_{12} \oplus V_3 \oplus V_{15} = 0 \qquad \epsilon$$

Linear Cryptanalysis of the cipher (8) - First phase

Going through the permutation is easy...



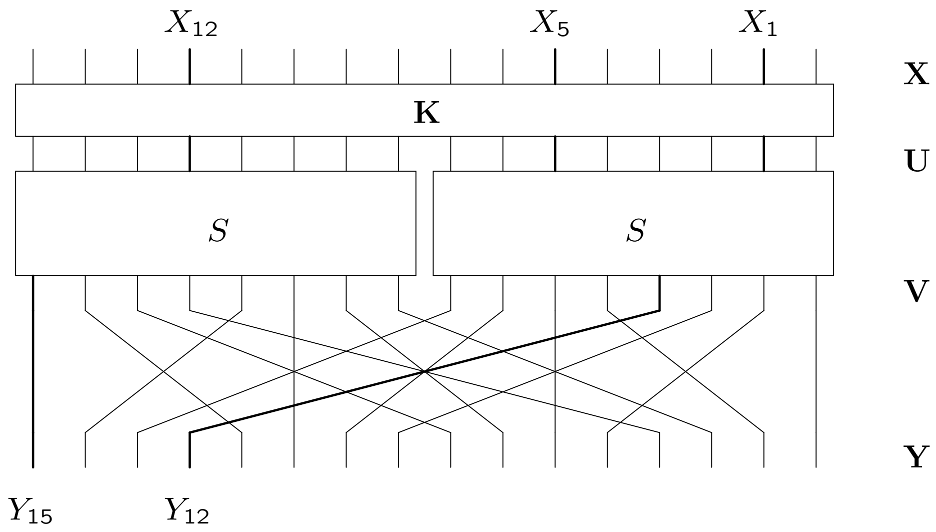
$$U_1 \oplus U_5 \oplus U_{12} \oplus V_3 \oplus V_{15} = 0 \qquad \epsilon$$

becomes

$$U_1 \oplus U_5 \oplus U_{12} \oplus Y_{12} \oplus Y_{15} = 0 \qquad \epsilon$$

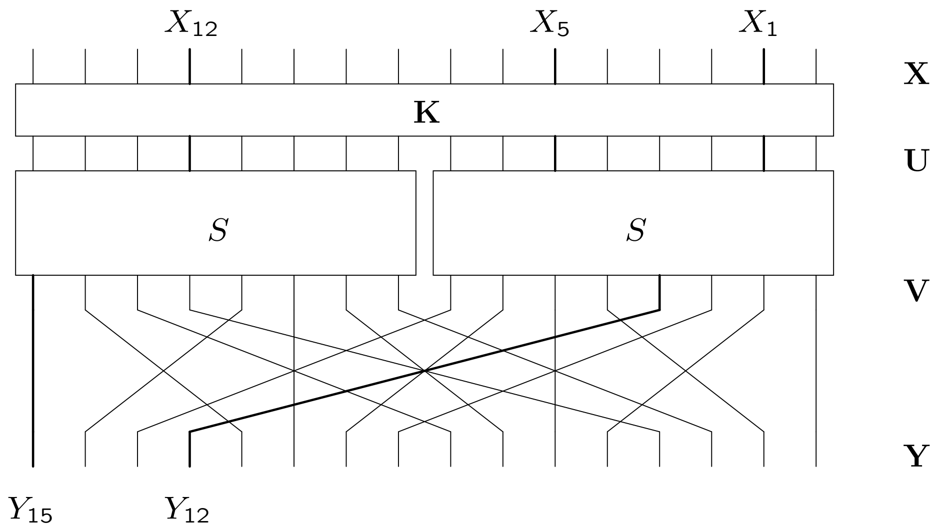
Linear Cryptanalysis of the cipher (9) - First phase

Going through the subkey layer...



Linear Cryptanalysis of the cipher (9) - First phase

Going through the subkey layer...

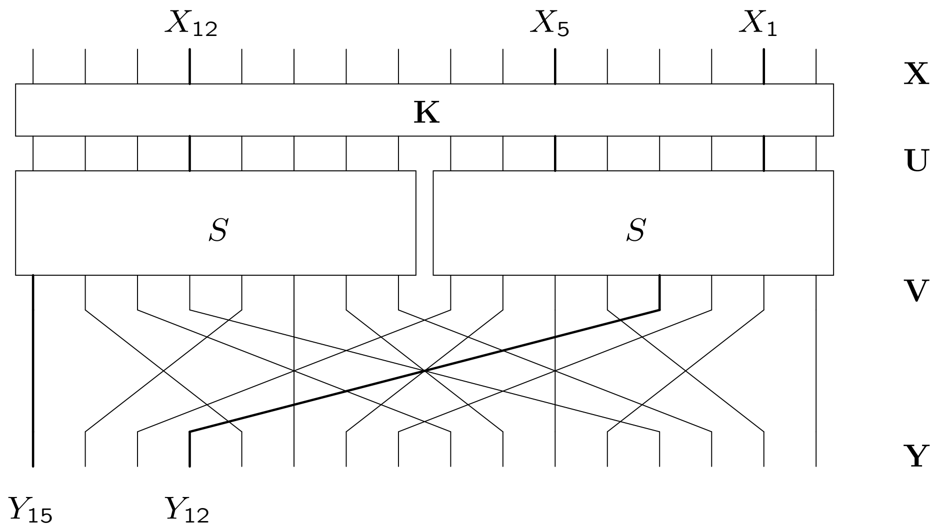


$$U_1 \oplus U_5 \oplus U_{12} \oplus Y_{12} \oplus Y_{15} = 0 \qquad \epsilon$$

$$\Rightarrow \quad X_1 \oplus X_5 \oplus X_{12} \oplus Y_{12} \oplus Y_{15} = K_1 \oplus K_5 \oplus K_{12} \qquad \epsilon$$

Linear Cryptanalysis of the cipher (9) - First phase

Going through the subkey layer...



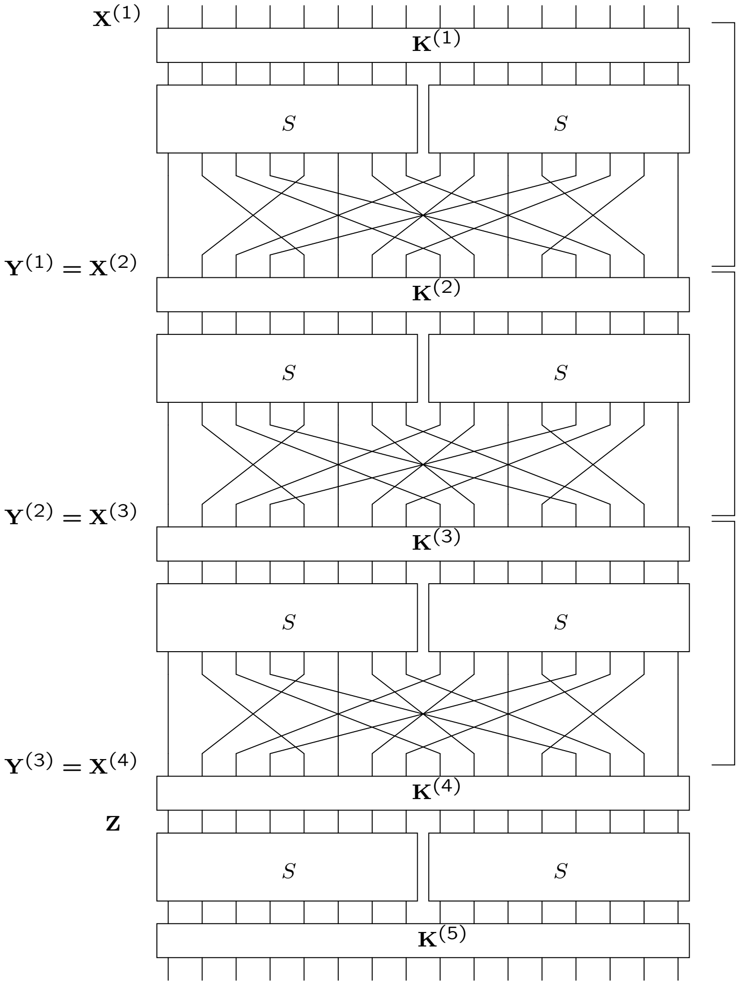
$$U_1 \oplus U_5 \oplus U_{12} \oplus Y_{12} \oplus Y_{15} = 0 \qquad \epsilon$$

$$\Rightarrow \quad X_1 \oplus X_5 \oplus X_{12} \oplus Y_{12} \oplus Y_{15} = K_1 \oplus K_5 \oplus K_{12} \qquad \epsilon$$

$$\Rightarrow \quad X_1 \oplus X_5 \oplus X_{12} \oplus Y_{12} \oplus Y_{15} = 0 \qquad \epsilon$$

as $\epsilon = \left|p - \frac{1}{2}\right| = \left|(1-p) - \frac{1}{2}\right|$.

Linear Cryptanalysis of the cipher (10) - First phase



$\mathbf{a}^{(1)} \cdot \mathsf{P} \oplus \mathbf{b}^{(1)} \cdot \mathbf{Y}^{(1)} = 0 \qquad \epsilon^{(1)}$

$\mathbf{a}^{(2)} \cdot \mathbf{X}^{(2)} \oplus \mathbf{b}^{(2)} \cdot \mathbf{Y}^{(2)} = 0 \qquad \epsilon^{(2)}$

$\mathbf{a}^{(3)} \cdot \mathbf{X}^{(3)} \oplus \mathbf{b}^{(3)} \cdot \mathbf{Y}^{(3)} = 0 \qquad \epsilon^{(3)}$

Linear Cryptanalysis of the cipher (11) - First phase

If $b^{(1)} = a^{(2)}$ and $b^{(2)} = a^{(3)}$ we can add the 3 linear equations:

$$\mathbf{a}^{(1)} \cdot \mathsf{P} \oplus \mathbf{b}^{(3)} \cdot \mathbf{Y}^{(3)} = 0$$

Linear Cryptanalysis of the cipher (11) - First phase

If $b^{(1)} = a^{(2)}$ and $b^{(2)} = a^{(3)}$ we can add the 3 linear equations:

$$\mathbf{a}^{(1)} \cdot \mathsf{P} \oplus \mathbf{b}^{(3)} \cdot \mathbf{Y}^{(3)} = 0$$

Using the piling-up lemma :

$$\epsilon = 4\ \epsilon^{(1)}\ \epsilon^{(2)}\ \epsilon^{(3)}$$

Linear Cryptanalysis of the cipher (11) - First phase

If $b^{(1)} = a^{(2)}$ and $b^{(2)} = a^{(3)}$ we can add the 3 linear equations:

$$\mathbf{a}^{(1)} \cdot \mathsf{P} \oplus \mathbf{b}^{(3)} \cdot \mathbf{Y}^{(3)} = 0$$

Using the piling-up lemma :

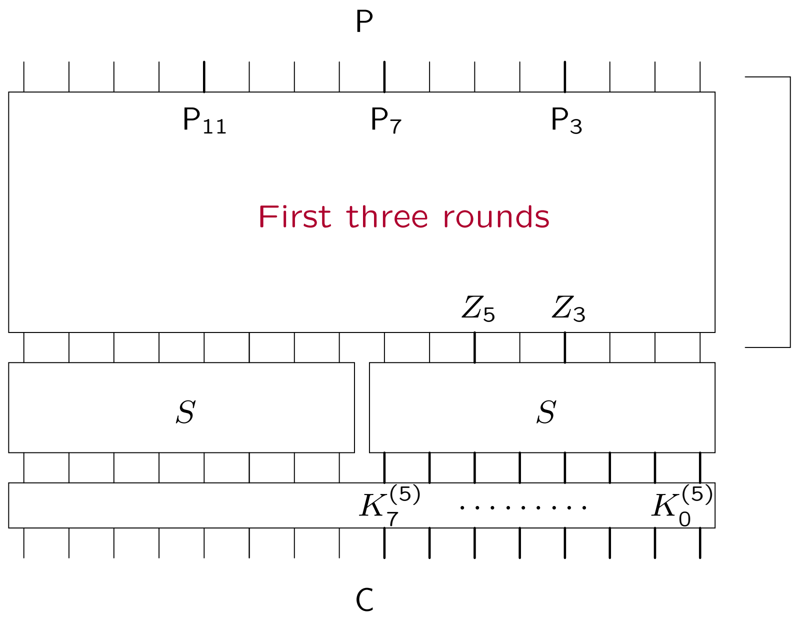
$$\epsilon = 4\, \epsilon^{(1)}\, \epsilon^{(2)}\, \epsilon^{(3)}$$

Going through $\mathbf{K}^{(4)}$, we finally obtain an expression like:

$$\boxed{\mathbf{a} \cdot \mathsf{P} \oplus \mathbf{b} \cdot \mathbf{Z} = 0}$$

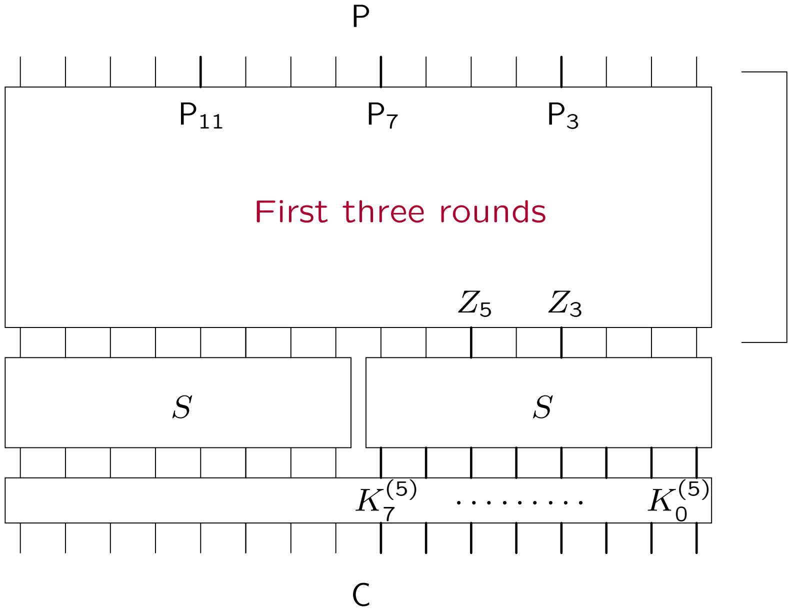
with a large bias ϵ.

Linear Cryptanalysis of the cipher (12) - Second phase



$P_3 \oplus P_7 \oplus P_{11} \oplus Z_3 \oplus Z_5 = 0 \qquad \epsilon$

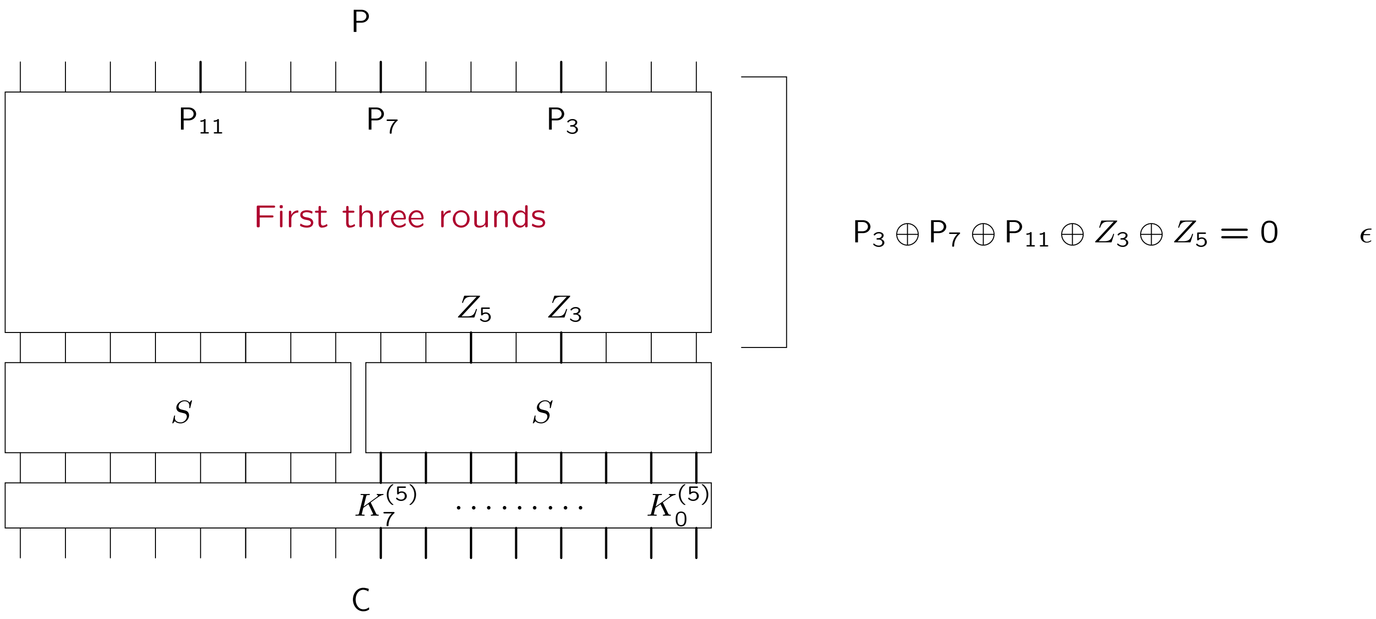
Linear Cryptanalysis of the cipher (12) - Second phase



$\mathsf{P}_3 \oplus \mathsf{P}_7 \oplus \mathsf{P}_{11} \oplus Z_3 \oplus Z_5 = 0 \qquad \epsilon$

1: For every possible $K_7^{(5)}, \ldots, K_0^{(5)}$ do

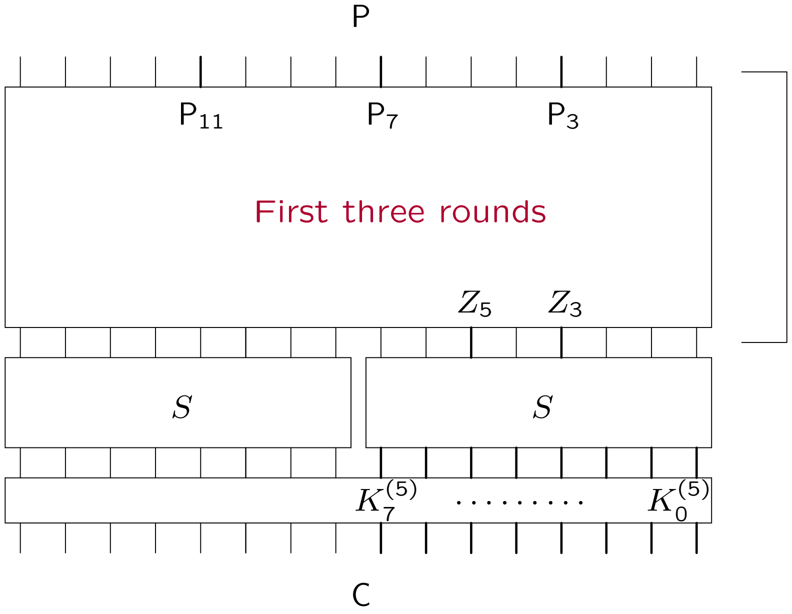
Linear Cryptanalysis of the cipher (12) - Second phase



1: For every possible $K_7^{(5)}, \ldots, K_0^{(5)}$ do

2: Set c to 0. For every (P, C), compute $\mathbf{Z}$ and increment c if equation holds.

Linear Cryptanalysis of the cipher (12) - Second phase



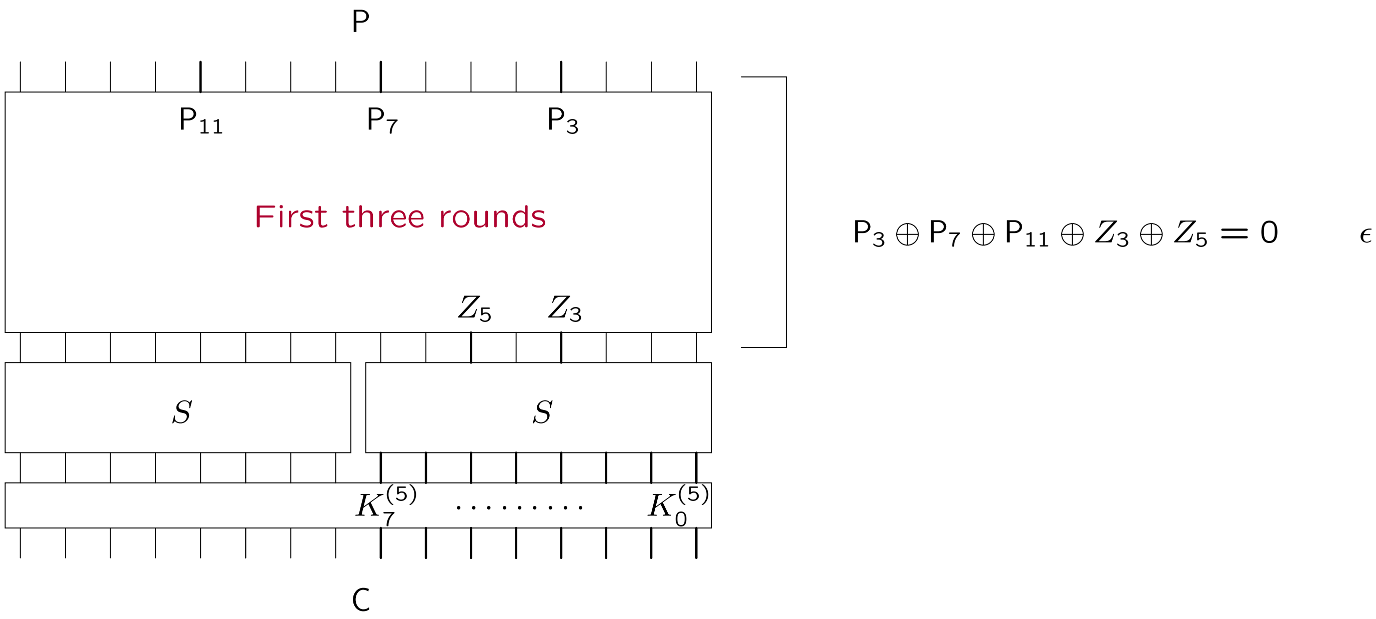
$P_3 \oplus P_7 \oplus P_{11} \oplus Z_3 \oplus Z_5 = 0 \qquad \epsilon$

1: For every possible $K_7^{(5)}, \ldots, K_0^{(5)}$ do

2: Set c to 0. For every (P, C), compute $\mathbf{Z}$ and increment c if equation holds.

3: $\epsilon_{K_7^{(5)}, \ldots, K_0^{(5)}} = \left| \frac{c}{n} - \frac{1}{2} \right|$

Linear Cryptanalysis of the cipher (12) - Second phase



1: For every possible $K_7^{(5)}, \ldots, K_0^{(5)}$ do

2: Set c to 0. For every (P, C), compute $\mathbf{Z}$ and increment c if equation holds.

3: $\epsilon_{K_7^{(5)},\ldots,K_0^{(5)}} = \left|\frac{c}{n} - \frac{1}{2}\right|$

4: Output the subkey bits corresponding to the largest bias.

Linear Cryptanalysis of the cipher (14) - Recap'

Linear cryptanalysis in two phases:

1. Find an effective linear expression

2. Find the last subkey bits

Linear Cryptanalysis of the cipher (14) - Recap'

Linear cryptanalysis in two phases:

1. Find an effective linear expression
   - $\rightsquigarrow$ Generalise linear expression
   - $\rightsquigarrow$ Generalise bias
   - $\rightsquigarrow$ Generalise piling-up lemma

2. Find the last subkey bits

Generalization of critical notions (1) - linear expressions

We will can consider $\mathbf{a}, \mathsf{P}, \mathbf{b}, \mathsf{C}, \mathbf{Z}, \ldots$ as elements of the finite field $\mathsf{F}_{2^{16}}$.

Generalization of critical notions (1) - linear expressions

We will can consider $\mathbf{a}, \mathsf{P}, \mathbf{b}, \mathsf{C}, \mathbf{Z}, \ldots$ as elements of the finite field $\mathsf{F}_{2^{16}}$.

The trace function defines a linear mapping from $\mathsf{F}_{2^{16}}$ onto one of its subfields. (e.g. F_2):

$$\begin{array}{rcccl} \textbf{Tr} & : & \mathsf{F}_{2^{16}} & \longrightarrow & \mathsf{F}_2 \\ & & \mathbf{X} & \longmapsto & \textbf{Tr}(\mathbf{X}) \end{array}$$

Generalization of critical notions (1) - linear expressions

We will can consider $\mathbf{a}, \mathsf{P}, \mathbf{b}, \mathsf{C}, \mathbf{Z}, \ldots$ as elements of the finite field $\mathsf{F}_{2^{16}}$.

The trace function defines a linear mapping from $\mathsf{F}_{2^{16}}$ onto one of its subfields. (e.g. F_2):

$$\begin{array}{rcccl} \mathbf{Tr} & : & \mathsf{F}_{2^{16}} & \longrightarrow & \mathsf{F}_2 \\ & & \mathbf{X} & \longmapsto & \mathbf{Tr}(\mathbf{X}) \end{array}$$

We can replace the inner-dot product by the trace function:

$$\mathbf{a} \cdot \mathsf{P} \quad \rightsquigarrow \quad \mathbf{Tr}(\mathbf{a}\mathsf{P})$$

Generalization of critical notions (1) - linear expressions

We will can consider $\mathbf{a}, \mathsf{P}, \mathbf{b}, \mathsf{C}, \mathbf{Z}, \ldots$ as elements of the finite field $\mathsf{F}_{2^{16}}$.

The trace function defines a linear mapping from $\mathsf{F}_{2^{16}}$ onto one of its subfields. (e.g. F_2):

$$\begin{array}{rcrcl} \mathbf{Tr} & : & \mathsf{F}_{2^{16}} & \longrightarrow & \mathsf{F}_2 \\ & & \mathbf{X} & \longmapsto & \mathbf{Tr}(\mathbf{X}) \end{array}$$

We can replace the inner-dot product by the trace function:

$$\mathbf{a} \cdot \mathsf{P} \quad \rightsquigarrow \quad \mathbf{Tr}(\mathbf{a}\mathsf{P})$$

A linear expression becomes:

$$\mathbf{a} \cdot \mathsf{P} \oplus \mathbf{b} \cdot \mathbf{Z} = 0 \quad \rightsquigarrow \quad \mathbf{Tr}(\mathbf{a}\mathsf{P} \oplus \mathbf{b}\mathbf{Z}) = 0$$

Generalization of critical notions (2) - linear expressions

We denoted p the probability that

$$\mathbf{a} \cdot \mathsf{P} \oplus \mathbf{b} \cdot \mathbf{Z} = 0$$

holds. We now denote p the probability that

$$\mathbf{Tr}\left(\mathbf{a}\mathsf{P} \oplus \mathbf{b}\mathbf{Z}\right) = 0$$

holds.

Generalization of critical notions (2) - linear expressions

We denoted p the probability that

$$\mathbf{a} \cdot \mathsf{P} \oplus \mathbf{b} \cdot \mathbf{Z} = 0$$

holds. We now denote p the probability that

$$\mathbf{Tr}\left(\mathbf{a}\mathsf{P} \oplus \mathbf{b}\mathbf{Z}\right) = 0$$

holds.

It can be shown that:

$$p = \mathbf{Pr}\left[\mathbf{Tr}\left(\mathbf{b}\mathbf{Z}\right) = 0 \mid \mathbf{Tr}\left(\mathbf{a}\mathsf{P}\right) = 0\right] .$$

Generalization of critical notions (2) - linear expressions

We denoted p the probability that

$$\mathbf{a} \cdot \mathsf{P} \oplus \mathbf{b} \cdot \mathbf{Z} = 0$$

holds. We now denote p the probability that

$$\mathbf{Tr}\left(\mathbf{a}\mathsf{P} \oplus \mathbf{b}\mathbf{Z}\right) = 0$$

holds.
It can be shown that:

$$p = \mathbf{Pr}\left[\mathbf{Tr}\left(\mathbf{b}\mathbf{Z}\right) = 0 \mid \mathbf{Tr}\left(\mathbf{a}\mathsf{P}\right) = 0\right] \ .$$

We define a linear transition matrix:

$$\mathbf{LT}\left(\mathbf{a}, \mathbf{b}\right) = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$$

which can replace linear expression.

Generalization of critical notions (3) - bias

Bias matrix associated to the transition matrix:

$$\mathbf{LB}(\mathrm{a},\mathrm{b}) = \mathbf{LT}(\mathrm{a},\mathrm{b}) - \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} \varepsilon & -\varepsilon \\ -\varepsilon & \varepsilon \end{pmatrix}$$

where the bias of the (old) linear expressions is $\epsilon = |\varepsilon|$.

Generalization of critical notions (3) - bias

Bias matrix associated to the transition matrix:

$$\mathsf{LB}\,(\mathbf{a},\mathbf{b}) = \mathsf{LT}\,(\mathbf{a},\mathbf{b}) - \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} \varepsilon & -\varepsilon \\ -\varepsilon & \varepsilon \end{pmatrix}$$

where the bias of the (old) linear expressions is $\epsilon = |\varepsilon|$.

A linear expression is effective if its bias

$$\epsilon = \left| p - \frac{1}{2} \right|$$

is large.

Generalization of critical notions (3) - bias

Bias matrix associated to the transition matrix:

$$\mathbf{LB}(\mathrm{a},\mathrm{b}) = \mathbf{LT}(\mathrm{a},\mathrm{b}) - \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} \varepsilon & -\varepsilon \\ -\varepsilon & \varepsilon \end{pmatrix}$$

where the bias of the (old) linear expressions is $\epsilon = |\varepsilon|$.

A linear expression is effective if its bias

$$\epsilon = \left| p - \frac{1}{2} \right|$$

is large.

A linear transition matrix is effective if its bias

$$\| \mathbf{LB}(\mathrm{a},\mathrm{b}) \|_2^2 = \sum_{i,j} \varepsilon_{i,j}^2$$

is large.

Generalization of critical notions (4) - Recap'

- Linear expression $\rightsquigarrow$ **LT**
- $\epsilon = \left|p - \frac{1}{2}\right| \rightsquigarrow \| \mathbf{LB} \|_2$

Generalization of critical notions (4) - Recap'

- Linear expression $\rightsquigarrow$ **LT**

- $\epsilon = \left| p - \frac{1}{2} \right| \rightsquigarrow \| \mathbf{LB} \|_2$

Where is the generalization ?!?

Generalization of critical notions (4) - Recap'

- Linear expression $\rightsquigarrow$ **LT**

- $\epsilon = \left|p - \frac{1}{2}\right| \rightsquigarrow \| \mathbf{LB} \|_2$

Where is the generalization ?!?

We can choose:

- F_{2^4} as departure field for the trace,

- and F_{2^2} as arrival field,

both seen as vector spaces over $F_{2^{16}}$.

Generalization of critical notions (5) - Recap'

For example, if $\mathbf{Tr} : \mathsf{F}_{2^4} \longrightarrow \mathsf{F}_{2^2}$ we obtain:

$$[\mathbf{LT}\,(a,b)]_{i,j} = \mathbf{Pr}\,[\mathbf{Tr}\,(\mathbf{b}\cdot\mathbf{Z}) = j \mid \mathbf{Tr}\,(\mathbf{a}\cdot\mathsf{P}) = i]$$

with

$$\mathbf{b}\cdot\mathbf{Z} = b_0Z_0 \oplus b_1Z_1 \oplus b_2Z_2 \oplus b_3Z_3\ .$$

where $b_0, b_1, Z_0, \cdots \in \mathsf{F}_{2^4}$.

Generalization of critical notions (5) - Recap'

For example, if $\textbf{Tr} : \mathsf{F}_{2^4} \longrightarrow \mathsf{F}_{2^2}$ we obtain:

$$[\textbf{LT}\,(a,b)]_{i,j} = \textbf{Pr}\,[\textbf{Tr}\,(\mathbf{b}\cdot\mathbf{Z}) = j \mid \textbf{Tr}\,(\mathbf{a}\cdot\mathsf{P}) = i]$$

with

$$\mathbf{b}\cdot\mathbf{Z} = b_0 Z_0 \oplus b_1 Z_1 \oplus b_2 Z_2 \oplus b_3 Z_3 \ .$$

where $b_0, b_1, Z_0, \cdots \in \mathsf{F}_{2^4}$.

The bias matrix is simply

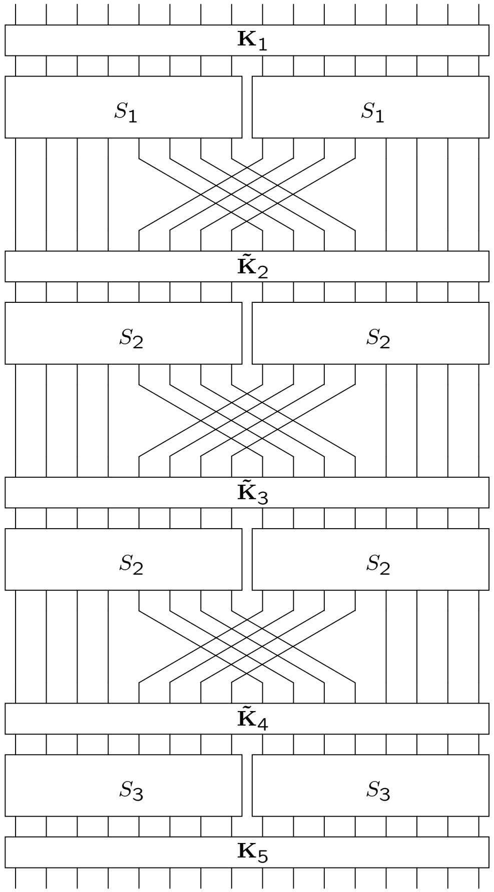
$$\textbf{LB}\,(a,b) = \textbf{LT}\,(a,b) - \begin{pmatrix} 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

The matrix is effective if $\| \textbf{LB}\,(a,b) \|_2$ is large.

Generalized cryptanalysis of the cipher (1) - Prologue

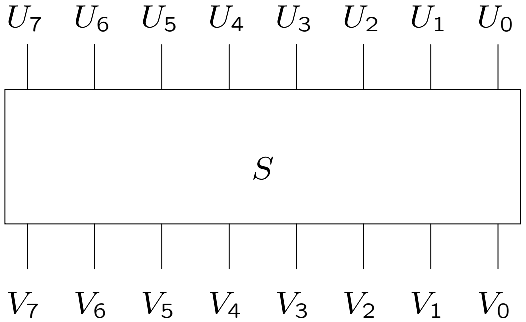
Generalized cryptanalysis in F_4.

Find an equivalent cipher: permutation has to be linear in F_{2^4}.



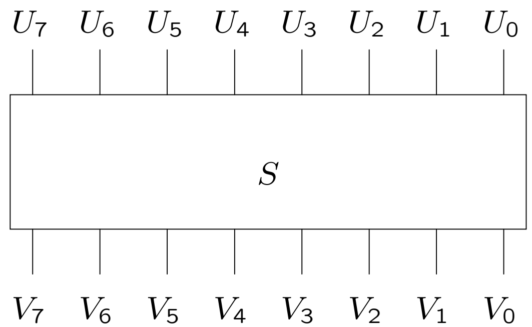
Generalized cryptanalysis of the cipher (2) - First phase

Step 1: Find an effective transition matrix on the substitution box.



Generalized cryptanalysis of the cipher (2) - First phase

Step 1: Find an effective transition matrix on the substitution box.



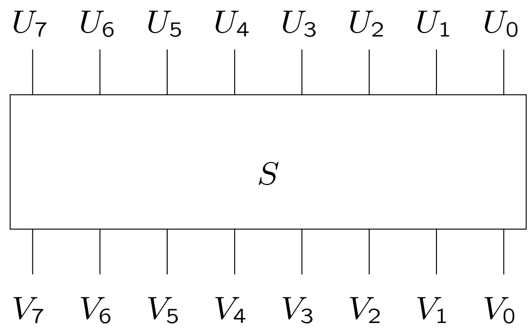
Set **LT** (a, b) to 0. For every input $\mathbf{U}$, increment $[\mathbf{LT}\,(\mathbf{a}, \mathbf{b})]_{i,j}$ where

$$i = \mathbf{Tr}\,(\mathbf{a} \cdot \mathbf{U})$$
$$j = \mathbf{Tr}\,(\mathbf{b} \cdot \mathbf{V})$$

Compute $\mathbf{LT}\,(\mathbf{a}, \mathbf{b}) \leftarrow \frac{2^2}{2^8}\mathbf{LT}\,(\mathbf{a}, \mathbf{b})$ and $\mathbf{LB}\,(\mathbf{a}, \mathbf{b})$.

Generalized cryptanalysis of the cipher (2) - First phase

Step 1: Find an effective transition matrix on the substitution box.



Set $\mathbf{LT}(a,b)$ to 0. For every input $\mathbf{U}$, increment $[\mathbf{LT}(\mathbf{a},\mathbf{b})]_{i,j}$ where

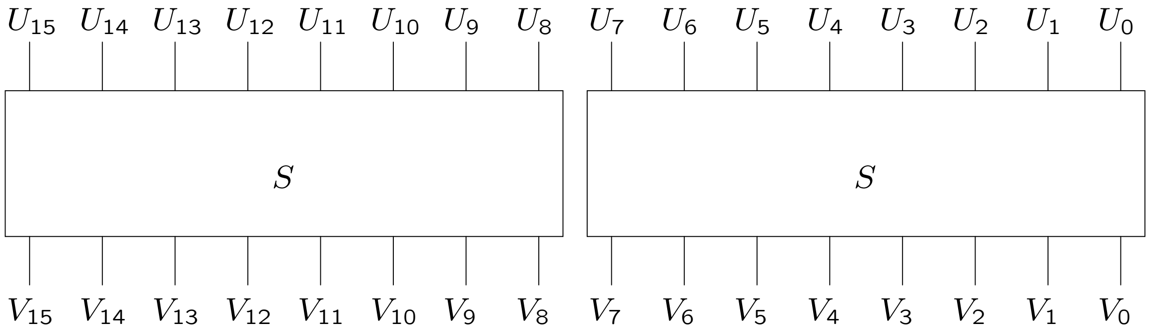
$$\begin{aligned} i &= \mathbf{Tr}(\mathbf{a}\cdot\mathbf{U}) \\ j &= \mathbf{Tr}(\mathbf{b}\cdot\mathbf{V}) \end{aligned}$$

Compute $\mathbf{LT}(\mathbf{a},\mathbf{b}) \leftarrow \frac{2^2}{2^8}\mathbf{LT}(\mathbf{a},\mathbf{b})$ and $\mathbf{LB}(\mathbf{a},\mathbf{b})$.

If $\| \mathbf{LB}(\mathbf{a},\mathbf{b}) \|_2$ is large, the matrix is effective.

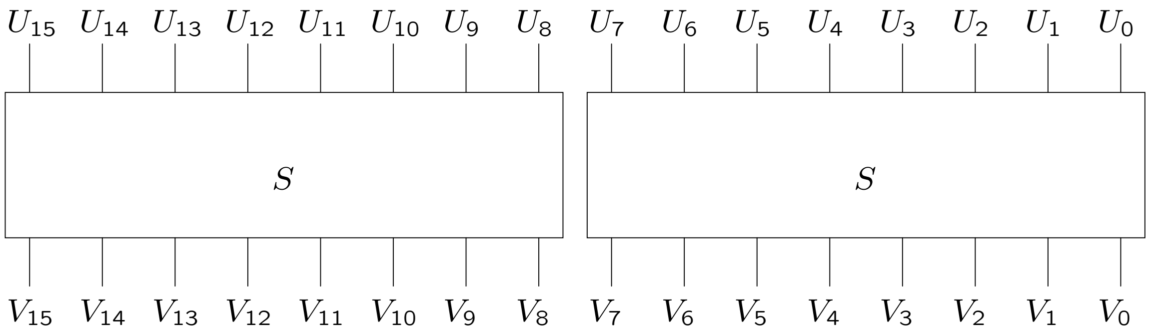
Generalized cryptanalysis of the cipher (3) - First phase

Step 2: Find transition matrix on the S-box layer.



Generalized cryptanalysis of the cipher (3) - First phase

Step 2: Find transition matrix on the S-box layer.



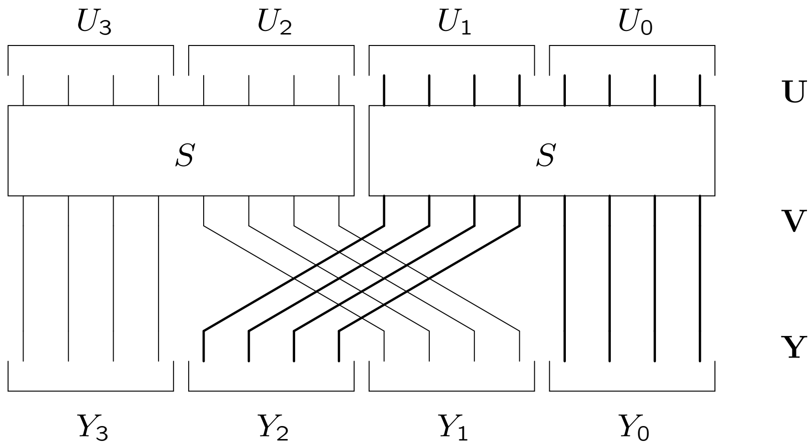
We suppose that only one S-box is active, i.e.

$$\mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} b_0 \\ b_1 \\ 0 \\ 0 \end{pmatrix}$$

Transition matrix on S-box layer = Transition matrix on S-box.

Generalized cryptanalysis of the cipher (4) - First phase

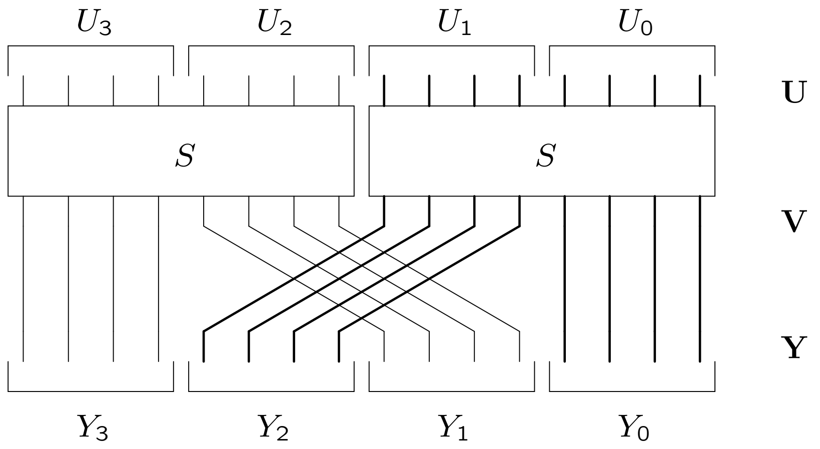
Step 3: Going through the permutation.



$$[\mathsf{LT}(\mathrm{a}, \mathrm{b})]_{i,j} = \mathsf{Pr}[\mathsf{Tr}(\mathrm{b} \cdot \mathbf{V}) = j \mid \mathsf{Tr}(\mathbf{a} \cdot \mathbf{U}) = i]$$

Generalized cryptanalysis of the cipher (4) - First phase

Step 3: Going through the permutation.



$$[\textsf{LT}\,(\mathbf{a},\mathbf{b})]_{i,j} = \textsf{Pr}\,[\textsf{Tr}\,(\mathbf{b}\cdot\mathbf{V}) = j \mid \textsf{Tr}\,(\mathbf{a}\cdot\mathbf{U}) = i]$$

becomes

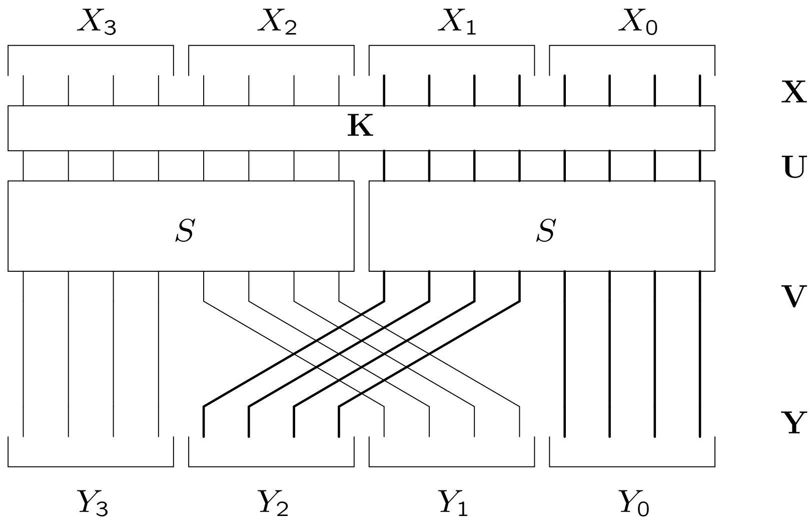
$$[\textsf{LT}\left(\mathbf{a},\tilde{\mathbf{b}}\right)]_{i,j} = \textsf{Pr}\left[\textsf{Tr}\left(\tilde{\mathbf{b}}\cdot\mathbf{Y}\right) = j \mid \textsf{Tr}\,(\mathbf{a}\cdot\mathbf{U}) = i\right]$$

with

$$\mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \tilde{\mathbf{b}} = \begin{pmatrix} b_0 \\ 0 \\ b_1 \\ 0 \end{pmatrix}$$

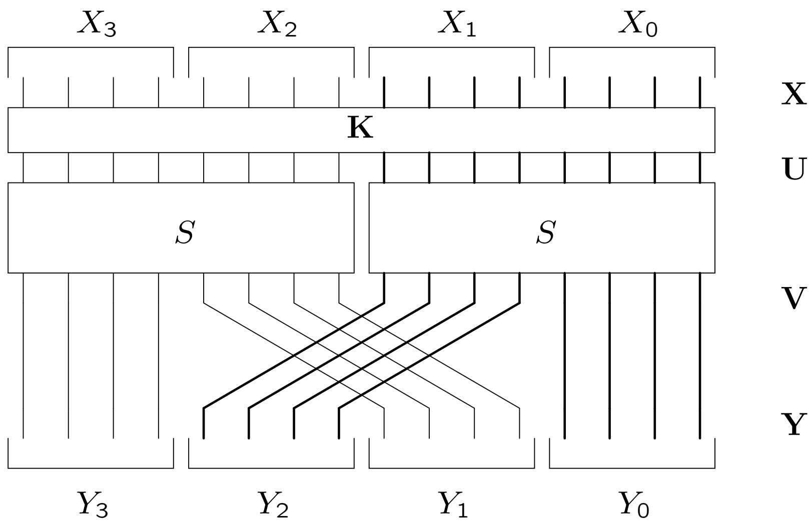
Generalized cryptanalysis of the cipher (5) - First phase

Step 4: Going through the key layer.



Generalized cryptanalysis of the cipher (5) - First phase

Step 4: Going through the key layer.

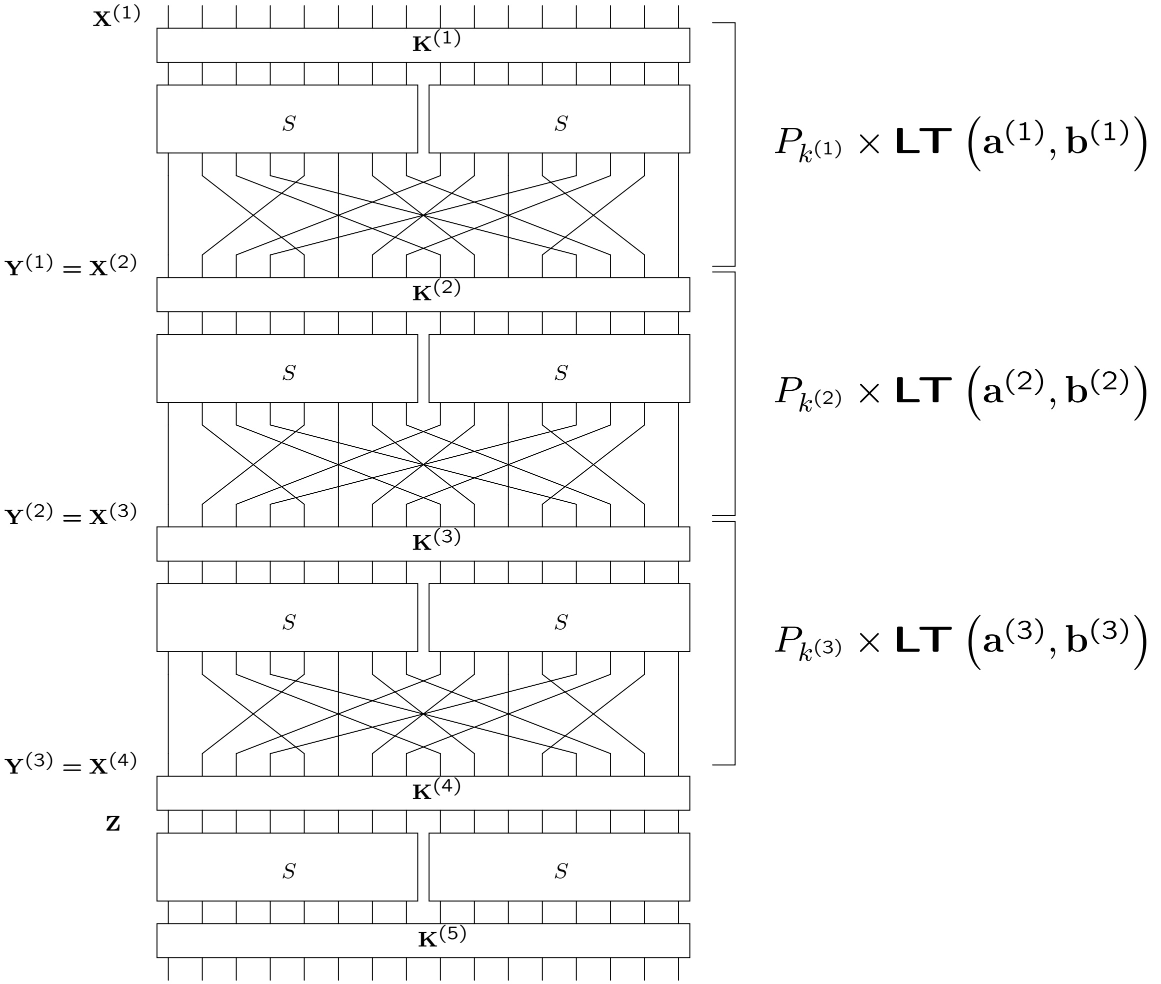


The transition matrix on one full round is:

$$P_k \times \mathbf{LT}\left(\mathbf{a}, \tilde{\mathbf{b}}\right)$$

where P_k is a permutation matrix depending on $k = \mathbf{Tr}\left(\mathbf{a} \cdot \mathbf{K}\right)$.

Generalized cryptanalysis of the cipher (6) - First phase



Generalized cryptanalysis of the cipher (7) - First phase

Step 5: Finding a transition matrix on the first three rounds.

If $b^{(1)} = a^{(2)}$ and $b^{(2)} = a^{(3)}$ we can find the transition matrix on the first three rounds (including $\mathbf{K}^{(4)}$):

Generalized cryptanalysis of the cipher (7) - First phase

Step 5: Finding a transition matrix on the first three rounds.

If $b^{(1)} = a^{(2)}$ and $b^{(2)} = a^{(3)}$ we can find the transition matrix on the first three rounds (including $\mathbf{K}^{(4)}$):

$$\left(\prod_{r=1}^{3} P_{k^{(r)}} \times \mathsf{LT}\left(\mathbf{a}^{(r)}, \mathbf{b}^{(r)}\right) \right) \times P_{k^{(4)}}$$

Generalized cryptanalysis of the cipher (7) - First phase

Step 5: Finding a transition matrix on the first three rounds.

If $b^{(1)} = a^{(2)}$ and $b^{(2)} = a^{(3)}$ we can find the transition matrix on the first three rounds (including $\mathbf{K}^{(4)}$):

$$\left(\prod_{r=1}^{3} P_{k^{(r)}} \times \textsf{LT}\left(\mathbf{a}^{(r)}, \mathbf{b}^{(r)}\right) \right) \times P_{k^{(4)}}$$

One can show that the corresponding bias matrix is:

$$\left(\prod_{r=1}^{3} P_{k^{(r)}} \times \textsf{LB}\left(\mathbf{a}^{(r)}, \mathbf{b}^{(r)}\right) \right) \times P_{k^{(4)}}$$

Generalized cryptanalysis of the cipher (8) - First phase

Step 5 - cont': Finding a transition matrix on the first three rounds.

The generalized piling-up lemma gives the bias of the last equation:

Generalized cryptanalysis of the cipher (8) - First phase

Step 5 - cont': Finding a transition matrix on the first three rounds.

The generalized piling-up lemma gives the bias of the last equation:

$$\| \left(\prod_{r=1}^{3} P_{k^{(r)}} \times \mathrm{LB}\left(\mathbf{a}^{(r)}, \mathbf{b}^{(r)}\right) \right) \times P_{k^{(4)}} \|_2 \approx \frac{1}{9} \prod_{r=1}^{3} \| \mathrm{LB}\left(\mathbf{a}^{(r)}, \mathbf{b}^{(r)}\right) \|_2$$

Generalized cryptanalysis of the cipher (8) - First phase

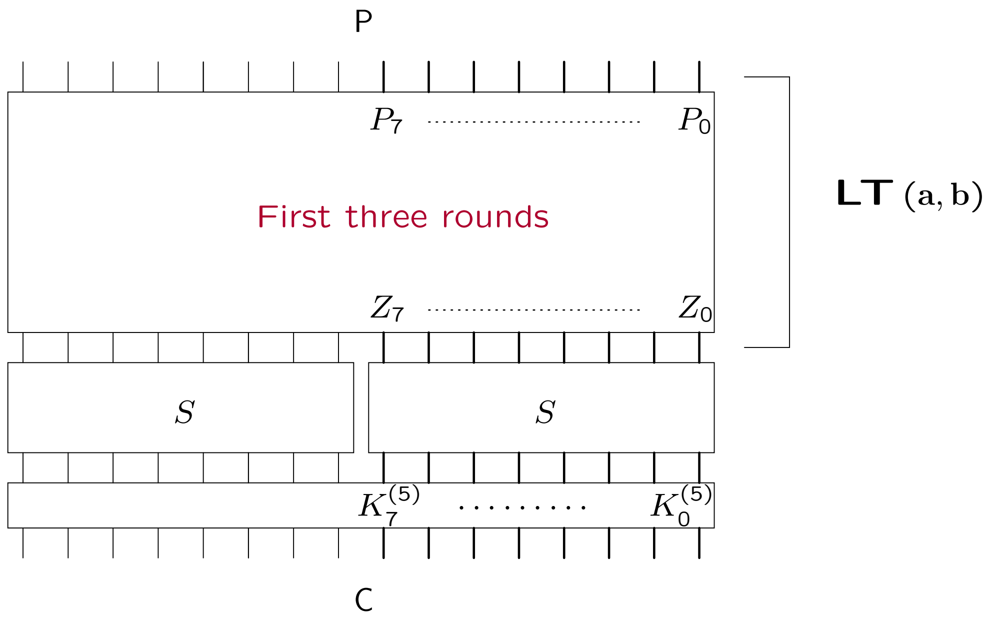
Step 5 - cont': Finding a transition matrix on the first three rounds.

The generalized piling-up lemma gives the bias of the last equation:

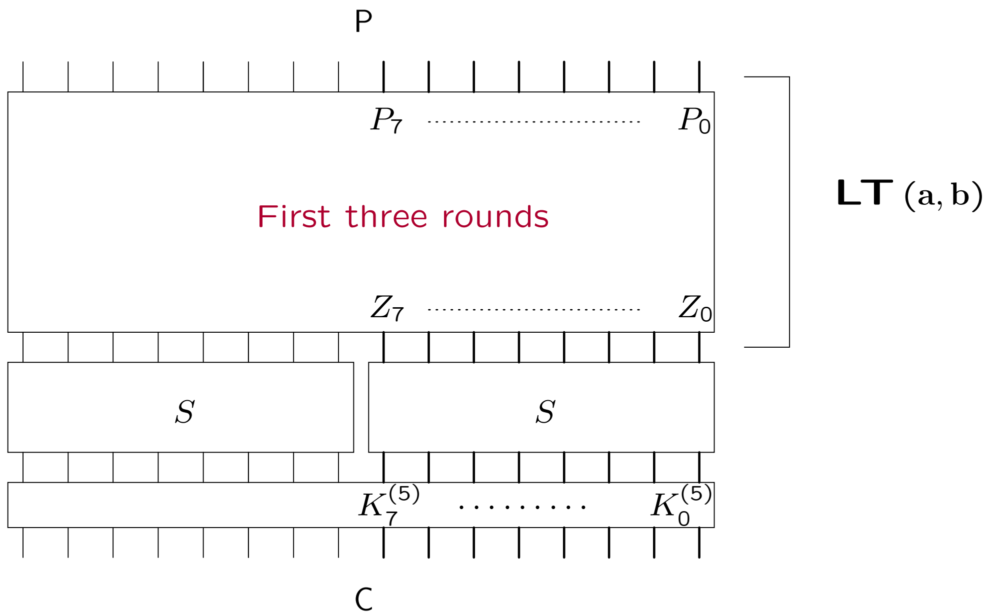
$$\| \left(\prod_{r=1}^{3} P_{k(r)} \times \mathrm{LB}\left(\mathbf{a}^{(r)}, \mathbf{b}^{(r)}\right) \right) \times P_{k(4)} \|_2 \approx \frac{1}{9} \prod_{r=1}^{3} \| \mathrm{LB}\left(\mathbf{a}^{(r)}, \mathbf{b}^{(r)}\right) \|_2$$

We finaly find a transition matrix on the first the rounds (i.e. in input/output mask $(\mathbf{a}, \mathbf{b})$) and its bias.

Generalized cryptanalysis of the cipher (9) - Second phase

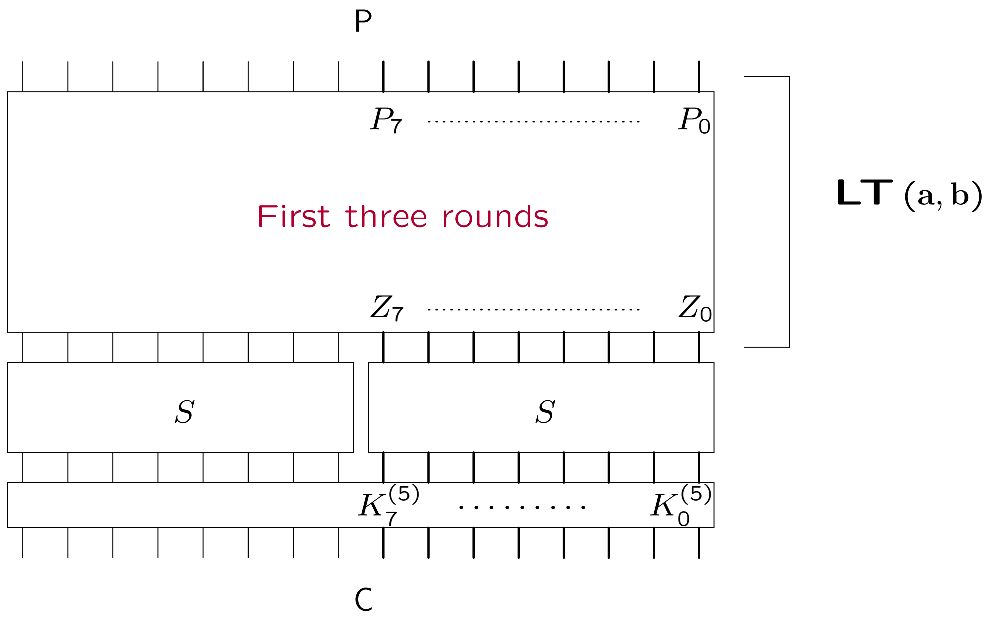


Generalized cryptanalysis of the cipher (9) - Second phase



1: For every possible $K_7^{(5)}, \ldots, K_0^{(5)}$ do

Generalized cryptanalysis of the cipher (9) - Second phase

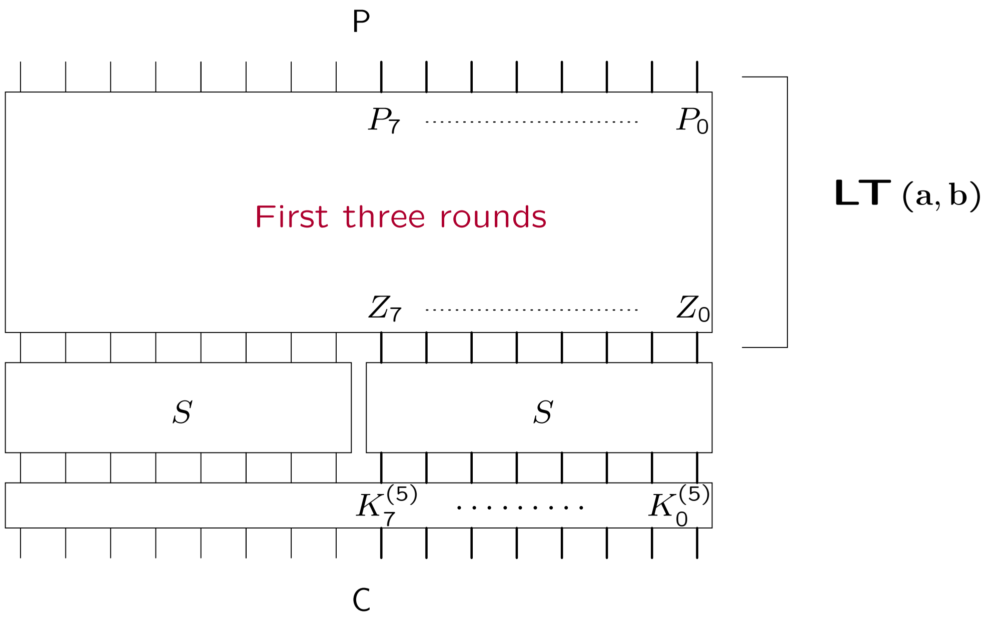


1: <u>For</u> every possible $K_7^{(5)}, \ldots, K_0^{(5)}$ <u>do</u>

2: Set matrix **LT** to 0. For every (P, C), compute $\mathbf{Z}$ and increment $[\mathbf{LT}]_{i,j}$ where

$$i = \mathbf{Tr}\,(\mathrm{a} \cdot \mathsf{P}) \quad \text{and} \quad j = \mathbf{Tr}\,(\mathrm{b} \cdot \mathbf{Z})$$

Generalized cryptanalysis of the cipher (9) - Second phase



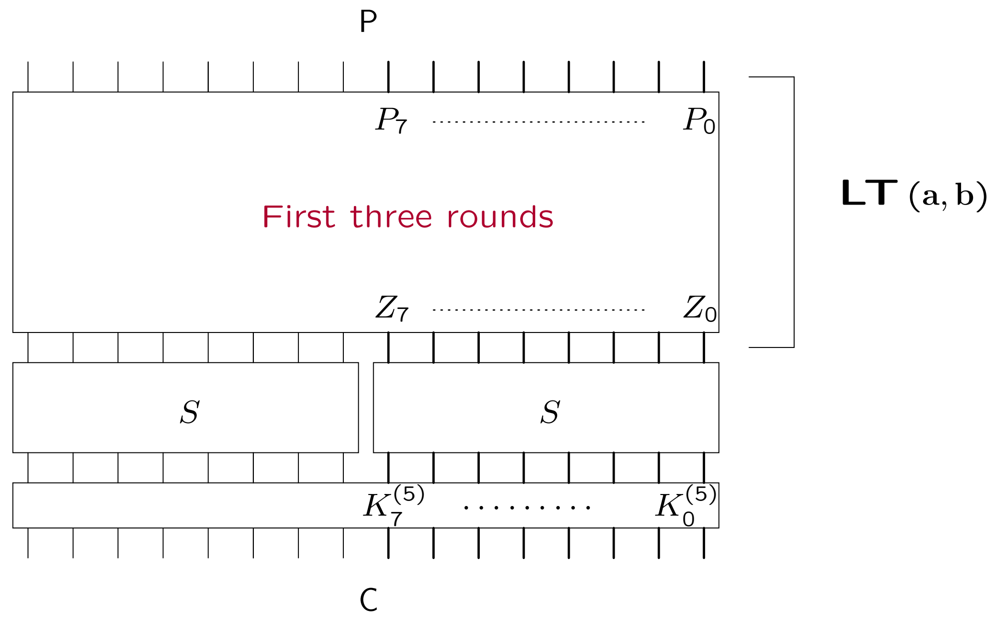
1: For every possible $K_7^{(5)}, \ldots, K_0^{(5)}$ do

2: Set matrix **LT** to 0. For every (P, C), compute **Z** and increment $[\mathbf{LT}]_{i,j}$ where

$$i = \mathbf{Tr}(\mathrm{a} \cdot \mathrm{P}) \quad \text{and} \quad j = \mathbf{Tr}(\mathrm{b} \cdot \mathbf{Z})$$

3: Compute $\mathbf{LT} \leftarrow 2^{-6}\mathbf{LT}$ and $\mathbf{LB}_{K_7^{(5)},\ldots,K_0^{(5)}}$

Generalized cryptanalysis of the cipher (9) - Second phase



1: For every possible $K_7^{(5)}, \ldots, K_0^{(5)}$ do

2: Set matrix **LT** to 0. For every (P, C), compute **Z** and increment $[\mathbf{LT}]_{i,j}$ where

$$i = \mathbf{Tr}(\mathrm{a} \cdot \mathrm{P}) \quad \text{and} \quad j = \mathbf{Tr}(\mathrm{b} \cdot \mathbf{Z})$$

3: Compute $\mathbf{LT} \leftarrow 2^{-6}\mathbf{LT}$ and $\mathbf{LB}_{K_7^{(5)},\ldots,K_0^{(5)}}$

4: Output the subkey bits corresponding to the largest $\| \mathbf{LB}_{K_7^{(5)},\ldots,K_0^{(5)}} \|_2$.

Limitations, further improvements and conclusion (1)

Theorem: Consider a permutation C over $\{0,1\}^n$. If for any $a,b \in F^*_{2^m}$ the bias matrix in F_2 is such that

$$\epsilon^2 \leq 4B$$

then, for any $a,b \in F^*_{2^m}$ the bias matrix in F_{2^n} is such that:

$$\sum_{i,j} \varepsilon^2_{i,j} \leq 2^{2n} B \; .$$

In other words. . .

Limitations, further improvements and conclusion (1)

Theorem: Consider a permutation C over $\{0,1\}^n$. If for any $a, b \in F^*_{2^m}$ the bias matrix in F_2 is such that

$$\epsilon^2 \leq 4B$$

then, for any $a, b \in F^*_{2^m}$ the bias matrix in F_{2^n} is such that:

$$\sum_{i,j} \varepsilon_{i,j}^2 \leq 2^{2n} B \ .$$

In other words...

If a cipher is very strong against linear cryptanalysis, it is strong against generalized linear cryptanalysis.

Limitations, further improvements and conclusion (2)

Theorem is true only when the transition matrix is defined with the trace function.

General definition:

$$[\mathbf{LT}\,(a,b)]_{i,j} = \mathbf{Pr}_X\left[\Phi(bC(X)) = j \;\mid\; \Psi(aX) = i\right] \;.$$

Thank you for your attention !