Cryptology

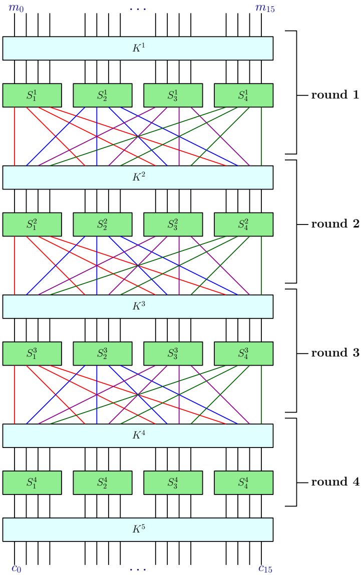
Sabyasachi Karati

Assistant Professor
Cryptology and Security Research Unit (C.S.R.U)
R. C. Bose Centre for Cryptology and Security
Indian Statistical Institute (ISI)
Kolkata, India

Lecture 07

Linear Cryptanalysis

SPN Network



$\ell = 4$, $l = 4$, and $m = 4$

Some Comments

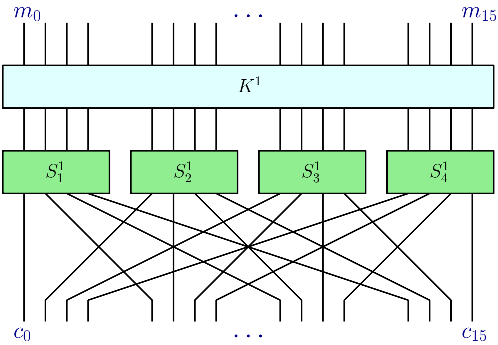
- Experience, indicates that SPNs are a good choice for constructing PRP as long as care is taken to choose the S-boxes, the mixing permutations, and the key schedule.

Some Comments

- Experience, indicates that SPNs are a good choice for constructing PRP as long as care is taken to choose the S-boxes, the mixing permutations, and the key schedule.
- The strength of a cipher $\mathcal{E}$ constructed in this way depends heavily on the *# rounds*.

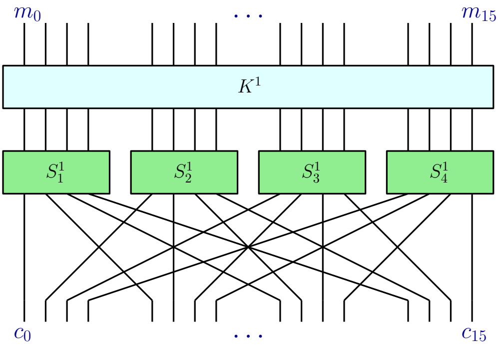
A Trivial Case

- Assume that $\mathcal{E}$ consists of one full round and no final key-mixing step.



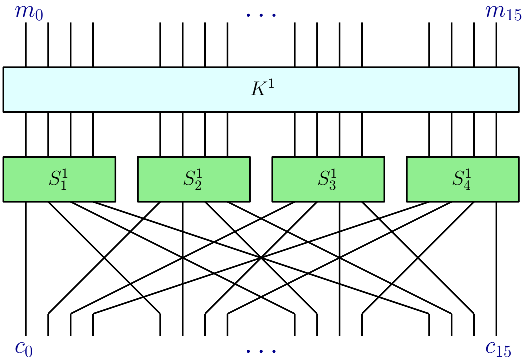
A Trivial Case

- Assume that $\mathcal{E}$ consists of one full round and no final key-mixing step.

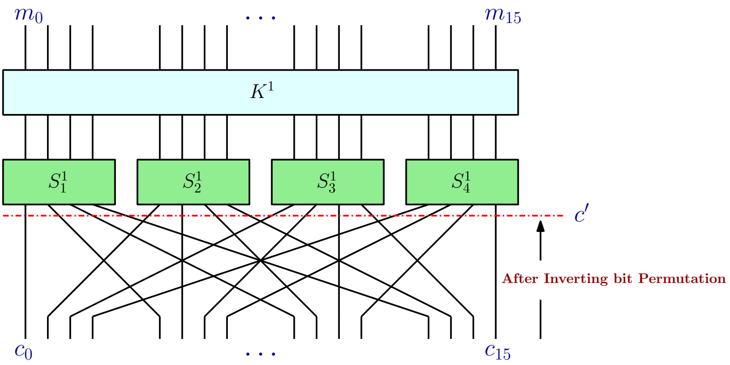


- Attack: An adversary given only a single input/output pair (m, c) can easily learn the secret key k for which $c = \mathcal{E}(k, x)$.

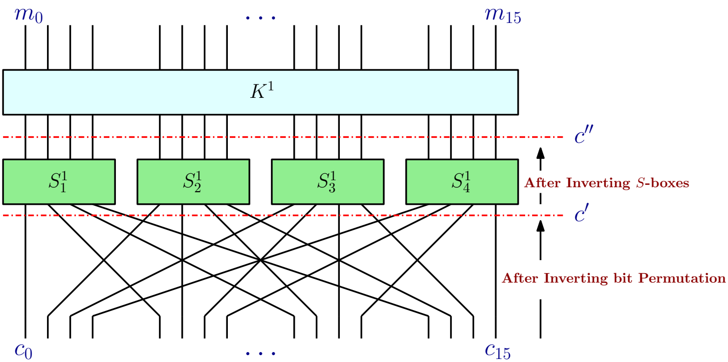
A Trivial Case



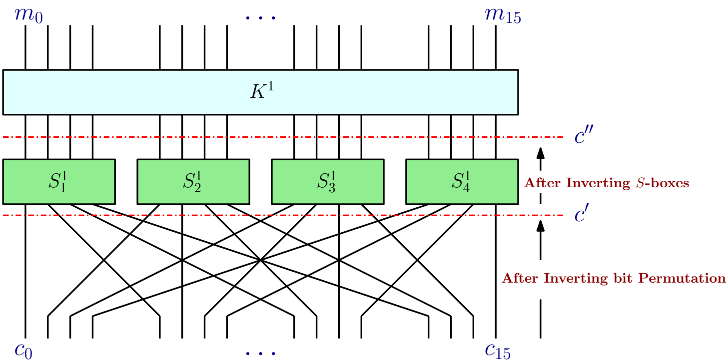
A Trivial Case



A Trivial Case

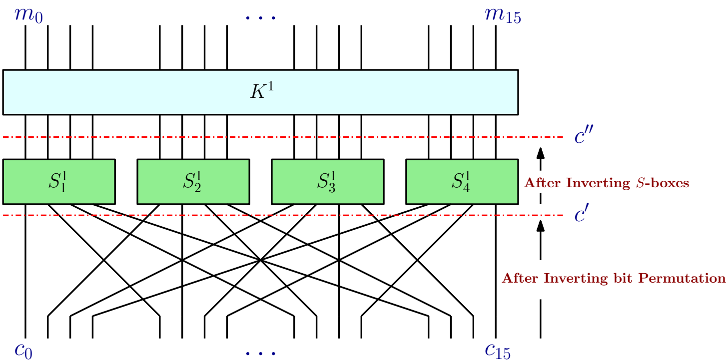


A Trivial Case



- $k = K^1 = m \oplus c''$.

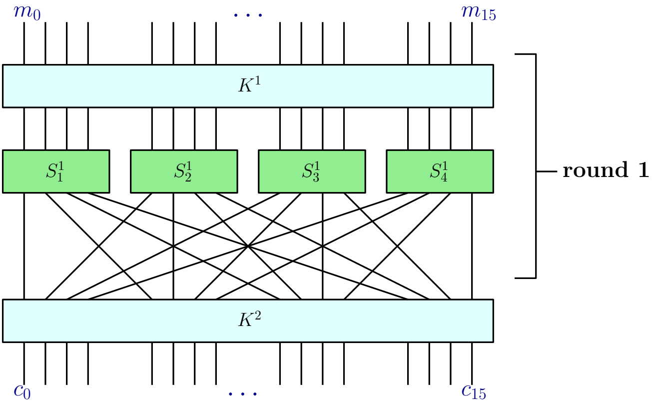
A Trivial Case



- $k = K^1 = m \oplus c''$.
- No security gained by performing S-box substitution or applying a mixing permutation after the final round-key mixing.

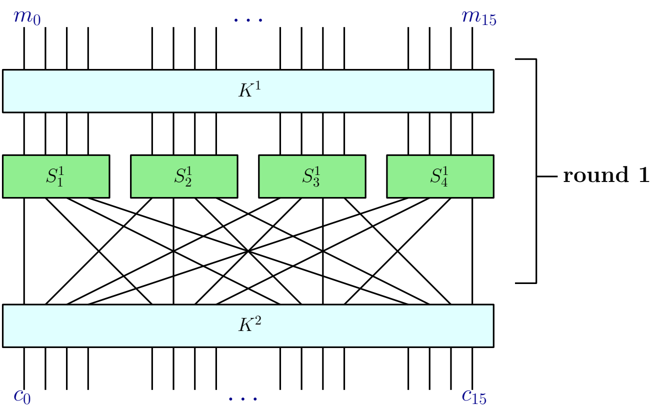
Attacking a 1-round SPN

- Consider one full round followed by a key-mixing step.



Attacking a 1-round SPN

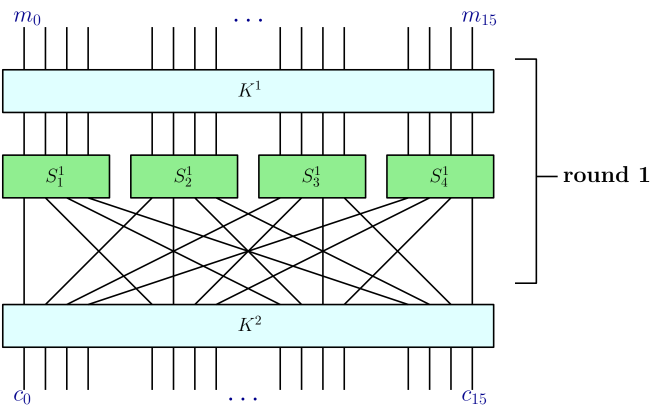
- Consider one full round followed by a key-mixing step.



- **For concreteness:** Assume a 16-bit block length, 4×4 S-boxes and independent 16-bit round-keys K^1, k^2.

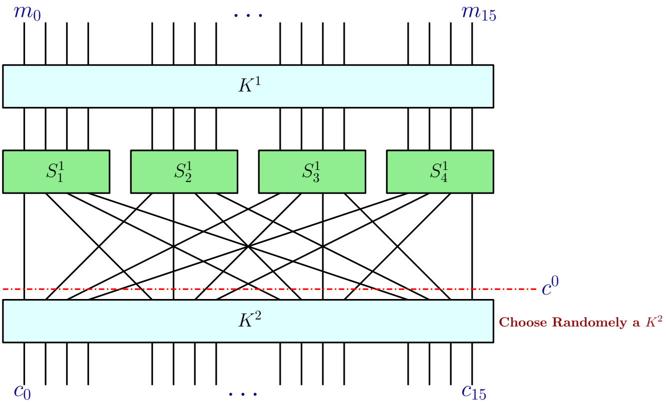
Attacking a 1-round SPN

- Consider one full round followed by a key-mixing step.



- **For concreteness:** Assume a 16-bit block length, 4×4 S-boxes and independent 16-bit round-keys K^1, k^2.
- Therefore the master key $K^1 \| K^2$ is 32 bits long.

Attacking a 1-round SPN



Attacking a 1-round SPN

Trivial Attack

- Observation 1: The trivial attack can be extended to give a key-recovery attack using much less than 2^{32} work.
  - Given a single input/output pair (m, c), the attacker enumerates over all possible values for the second-round sub-key K^2.

Trivial Attack

- Observation 1: The trivial attack can be extended to give a key-recovery attack using much less than 2^{32} work.
  - Given a single input/output pair (m, c), the attacker enumerates over all possible values for the second-round sub-key K^2.
  - For each such value, invert the final key-mixing step to get a candidate intermediate value c^0.

Attacking a 1-round SPN

Trivial Attack

- Observation 1: The trivial attack can be extended to give a key-recovery attack using much less than 2^{32} work.
    - Given a single input/output pair (m, c), the attacker enumerates over all possible values for the second-round sub-key K^2.
    - For each such value, invert the final key-mixing step to get a candidate intermediate value c^0.
    - Use Trivial Attack to find the round-key k_1.

Attacking a 1-round SPN

Trivial Attack

- Observation 1: The trivial attack can be extended to give a key-recovery attack using much less than 2^{32} work.
  - Given a single input/output pair (m, c), the attacker enumerates over all possible values for the second-round sub-key K^2.
  - For each such value, invert the final key-mixing step to get a candidate intermediate value c^0.
  - Use Trivial Attack to find the round-key k_1.
  - For each $k^2 \in \{0, 1\}^{16}$, $K^1 \| K^2$ is a candidate master key.

Attacking a 1-round SPN

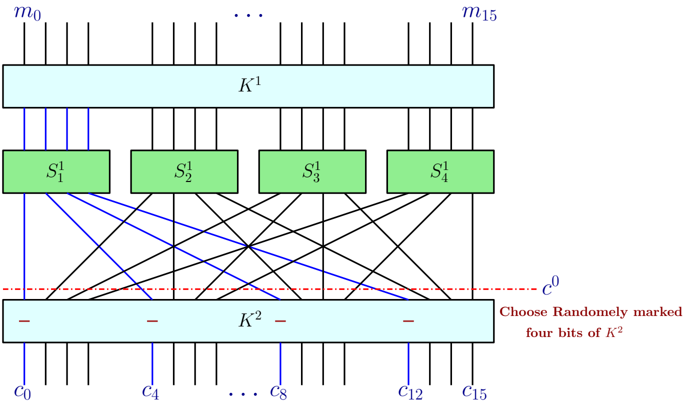
Trivial Attack

- Observation 1: The trivial attack can be extended to give a key-recovery attack using much less than 2^{32} work.
  - Given a single input/output pair (m, c), the attacker enumerates over all possible values for the second-round sub-key K^2.
  - For each such value, invert the final key-mixing step to get a candidate intermediate value c^0.
  - Use Trivial Attack to find the round-key k_1.
  - For each $k^2 \in \{0, 1\}^{16}$, $K^1 \| K^2$ is a candidate master key.
  - Therefore, in time 2^{16}, the attacker obtains a list of 2^{16} possibilities for the master key.

Trivial Attack

- Observation 1: The trivial attack can be extended to give a key-recovery attack using much less than 2^{32} work.
  - Given a single input/output pair (m, c), the attacker enumerates over all possible values for the second-round sub-key K^2.
  - For each such value, invert the final key-mixing step to get a candidate intermediate value c^0.
  - Use Trivial Attack to find the round-key k_1.
  - For each $k^2 \in \{0,1\}^{16}$, $K^1 \| K^2$ is a candidate master key.
  - Therefore, in time 2^{16}, the attacker obtains a list of 2^{16} possibilities for the master key.
  - Use an additional input/output pairs to find the key in roughly 2^{16} additional time.

Attacking a 1-round SPN



An Improved Attack

- Individual bits of the output depend on only part of the master key.

An Improved Attack

- Individual bits of the output depend on only part of the master key.
  - Enumerate over all possible values for the four bits $K^2_0, K^2_4, K^2_8, K^2_{12}$ of K^2.

An Improved Attack

- Individual bits of the output depend on only part of the master key.
  - Enumerate over all possible values for the four bits $K^2_0, K^2_4, K^2_8, K^2_{12}$ of K^2.
  - XOR it with the four bits c_0, c_4, c_8, c_{12} of c to obtain output of first S-box.

An Improved Attack

- Individual bits of the output depend on only part of the master key.
  - Enumerate over all possible values for the four bits $K_0^2, K_4^2, K_8^2, K_{12}^2$ of K^2.
  - XOR it with the four bits c_0, c_4, c_8, c_{12} of c to obtain output of first S-box.
  - Invert the S-box, to get the input to that S-box.

An Improved Attack

- Individual bits of the output depend on only part of the master key.
  - Enumerate over all possible values for the four bits $K^2_0, K^2_4, K^2_8, K^2_{12}$ of K^2.
  - XOR it with the four bits c_0, c_4, c_8, c_{12} of c to obtain output of first S-box.
  - Invert the S-box, to get the input to that S-box.
  - Since the input to that S-box is the XOR of first 4 bits of m and first 4 bits of K^1, this yields a candidate value for 4 bits of K^1.

Attacking a 1-round SPN

An Improved Attack

- We get 2^4 candidates for 8 bits of $K^1 \| K^2$.

Attacking a 1-round SPN

An Improved Attack

- We get 2^4 candidates for 8 bits of $K^1 \| K^2$.
- Repeat this process for remaing three sets of key bits of K^2.

Attacking a 1-round SPN

An Improved Attack

- We get 2^4 candidates for 8 bits of $K^1 \| K^2$.
- Repeat this process for remaing three sets of key bits of K^2.
- The attacker has thus reduced the number of possible master keys to $(2^4)^4 = 2^{16}$, as in the earlier attack.

An Improved Attack

- We get 2^4 candidates for 8 bits of $K^1 \| K^2$.
- Repeat this process for remaing three sets of key bits of K^2.
- The attacker has thus reduced the number of possible master keys to $(2^4)^4 = 2^{16}$, as in the earlier attack.
- Total time: $4 \cdot 2^4 = 2^6$, a dramatic improvement!

Attacking a 1-round SPN

Notes

- The attack is possible since different parts of the key can be isolated from other parts.

Notes

- The attack is possible since different parts of the key can be isolated from other parts.
- Further *diffusion* is needed to make sure that all the bits of the key affect all of the bits of the output.

Attacking a 1-round SPN

Notes

- The attack is possible since different parts of the key can be isolated from other parts.
- Further *diffusion* is needed to make sure that all the bits of the key affect all of the bits of the output.
- Multiple rounds are needed for this to take place.

Attacking a 1-round SPN

Notes

- The attack is possible since different parts of the key can be isolated from other parts.
- Further *diffusion* is needed to make sure that all the bits of the key affect all of the bits of the output.
- Multiple rounds are needed for this to take place.
- Attacking a two-round SPN: The above ideas can be extended to give a better-than-brute-force attack on a two-round SPN using independent round-keys.

Notes

- Algebraic Attacks
  - Buchberger's Algorithm
  - Linearization Technique
  - Relinearization Technique
  - The XL algorithm (XL - eXtended Linearization)

Notes

- Algebraic Attacks
  - Buchberger's Algorithm
  - Linearization Technique
  - Relinearization Technique
  - The XL algorithm (XL - eXtended Linearization)
- Structural Attacks
  - Slide Attack
  - Advanced Slide Attack

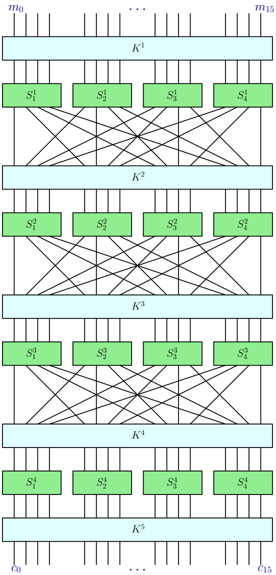
Notes

- Statistical Attacks
  - Distinguishing Attacks
  - Linear Cryptanalysis, and variants like
    - Zero-correlation attack

Notes

- Statistical Attacks
  - Distinguishing Attacks
  - Linear Cryptanalysis, and variants like
    - Zero-correlation attack
  - Differential Cryptanalysis, and variants like
    - Higher Order Differentials
    - Truncated Differential Cryptanalysis
    - Impossible Differential Cryptanalysis
    - Improbable Differential Cryptanalysis
    - Boomerang Attack
    - Cube Attack
- Other Attacks
  - Differential-linear attack
  - The Integral or Square attack and so on.

Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

Intuition

- Suppose that it is possible to find a probabilistic linear relationship between a subset of plaintext bits and a subset of state bits immediately preceding the substitutions performed in the last round.

Intuition

- Suppose that it is possible to find a probabilistic linear relationship between a subset of plaintext bits and a subset of state bits immediately preceding the substitutions performed in the last round.
- There exists a subset of bits whose XOR behaves in a non-random fashion.

Intuition

- Suppose that it is possible to find a probabilistic linear relationship between a subset of plaintext bits and a subset of state bits immediately preceding the substitutions performed in the last round.
- There exists a subset of bits whose XOR behaves in a non-random fashion.
- Consider a known-plaintext attack
  - An attacker has a large number of plaintext-ciphertext pairs under the same unknown key K

Intuition

- Suppose that it is possible to find a probabilistic linear relationship between a subset of plaintext bits and a subset of state bits immediately preceding the substitutions performed in the last round.
- There exists a subset of bits whose XOR behaves in a non-random fashion.
- Consider a known-plaintext attack
  - An attacker has a large number of plaintext-ciphertext pairs under the same unknown key K
- For each of the plaintext-ciphertext pairs, decrypt the ciphertext using all possible candidate keys for the last round of the cipher.

Linear Cryptanalysis

Intuition

- Suppose that it is possible to find a probabilistic linear relationship between a subset of plaintext bits and a subset of state bits immediately preceding the substitutions performed in the last round.
- There exists a subset of bits whose XOR behaves in a non-random fashion.
- Consider a known-plaintext attack
  - An attacker has a large number of plaintext-ciphertext pairs under the same unknown key K
- For each of the plaintext-ciphertext pairs, decrypt the ciphertext using all possible candidate keys for the last round of the cipher.
- For each candidate key, compute the values of the relevant state bits involved in the linear relationship, and determine if the above-mentioned linear relationship holds.

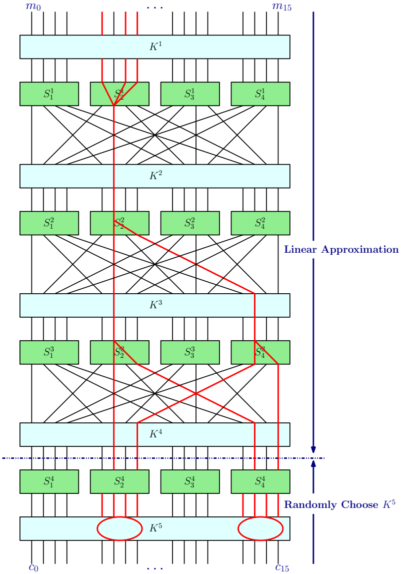
Intuition

- Suppose that it is possible to find a probabilistic linear relationship between a subset of plaintext bits and a subset of state bits immediately preceding the substitutions performed in the last round.
- There exists a subset of bits whose XOR behaves in a non-random fashion.
- Consider a known-plaintext attack
  - An attacker has a large number of plaintext-ciphertext pairs under the same unknown key K
- For each of the plaintext-ciphertext pairs, decrypt the ciphertext using all possible candidate keys for the last round of the cipher.
- For each candidate key, compute the values of the relevant state bits involved in the linear relationship, and determine if the above-mentioned linear relationship holds.
- Count frequencies of all the candidate keys that satisfies the linear relationship.

Intuition

- Suppose that it is possible to find a probabilistic linear relationship between a subset of plaintext bits and a subset of state bits immediately preceding the substitutions performed in the last round.
- There exists a subset of bits whose XOR behaves in a non-random fashion.
- Consider a known-plaintext attack
  - An attacker has a large number of plaintext-ciphertext pairs under the same unknown key K
- For each of the plaintext-ciphertext pairs, decrypt the ciphertext using all possible candidate keys for the last round of the cipher.
- For each candidate key, compute the values of the relevant state bits involved in the linear relationship, and determine if the above-mentioned linear relationship holds.
- Count frequencies of all the candidate keys that satisfies the linear relationship.
- Hope: The candidate key that has a frequency count furthest from 1/2 times the number of plaintext-ciphertext pairs contains the correct values for these key bits.

Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

Goal

- Main Aim: To find *linear approximations* of the form

$$\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0$$

  which have a high or low probability of occurrence.

Goal

- Main Aim: To find *linear approximations* of the form

$$\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0$$

  which have a high or low probability of occurrence.

- Let,

$$p_L = \Pr\left[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0\right],$$

Goal

- Main Aim: To find *linear approximations* of the form

$$\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0$$

  which have a high or low probability of occurrence.
- Let,

$$p_L = \Pr\left[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0\right],$$

- linear probability bias: $\epsilon_L = \mid p_L - \frac{1}{2} \mid .$

Goal

- Main Aim: To find *linear approximations* of the form

$$\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0$$

  which have a high or low probability of occurrence.
- Let,

$$p_L = \Pr\left[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0\right],$$

- linear probability bias: $\epsilon_L = \mid p_L - \frac{1}{2} \mid$.
- Tries to take advantage of high probability occurrences of linear approximations involving plaintext, ciphertext and sub-key bits.
- Mitsuru Matsui (EUROCRYPT, 1993): As an attack on DES.

Goal

- Main Aim: To find *linear approximations* of the form

$$\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0$$

  which have a high or low probability of occurrence.
- Let,

$$p_L = \Pr\left[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v} = 0\right],$$

- linear probability bias: $\epsilon_L = \mid p_L - \frac{1}{2} \mid .$
- Tries to take advantage of high probability occurrences of linear approximations involving plaintext, ciphertext and sub-key bits.
- Mitsuru Matsui (EUROCRYPT, 1993): As an attack on DES.
- It is a Known Plaintext Attack.

The Piling-up Lemma

- Let $\mathbf{X}_1, \mathbf{X}_2, \ldots$ be independent random variables taking on values from the set $\{0, 1\}$.
- Let $p_1, p_2, \ldots$ be real numbers such that $0 \leqslant p_i \leqslant 1$ for all i.
- Let $\forall i = 1, 2, \ldots$

$$\begin{aligned} \Pr[\mathbf{X}_i = 0] &= p_i, \text{ and} \\ \Pr[\mathbf{X}_i = 1] &= 1 - p_i \end{aligned}$$

The Piling-up Lemma

- Let $\mathbf{X}_1, \mathbf{X}_2, \ldots$ be independent random variables taking on values from the set $\{0, 1\}$.
- Let $p_1, p_2, \ldots$ be real numbers such that $0 \leqslant p_i \leqslant 1$ for all i.
- Let $\forall i = 1, 2, \ldots$

$$\begin{aligned} \Pr[\mathbf{X}_i = 0] &= p_i, \text{ and} \\ \Pr[\mathbf{X}_i = 1] &= 1 - p_i \end{aligned}$$

- For $i \neq j$

$$\begin{aligned} \Pr[\mathbf{X}_i = 0 \wedge \mathbf{X}_j = 0] &= p_i p_j, \\ \Pr[\mathbf{X}_i = 0 \wedge \mathbf{X}_j = 1] &= p_i(1 - p_j), \\ \Pr[\mathbf{X}_i = 1 \wedge \mathbf{X}_j = 0] &= (1 - p_i)p_j, \text{ and} \\ \Pr[\mathbf{X}_i = 1 \wedge \mathbf{X}_j = 1] &= (1 - p_i)(1 - p_j). \end{aligned}$$

The Piling-up Lemma

$$\begin{aligned}
\Pr[\mathbf{X}_i \oplus \mathbf{X}_j = 0] &= \Pr[\mathbf{X}_i = 0 \wedge \mathbf{X}_j = 0] + \Pr[\mathbf{X}_i = 1 \wedge \mathbf{X}_j = 1] \\
&= p_i p_j + (1 - p_i)(1 - p_j), \\
\Pr[\mathbf{X}_i \oplus \mathbf{X}_j = 1] &= \Pr[\mathbf{X}_i = 0 \wedge \mathbf{X}_j = 1] + \Pr[\mathbf{X}_i = 1 \wedge \mathbf{X}_j = 0] \\
&= p_i(1 - p_j) + (1 - p_i)p_j.
\end{aligned}$$

The Piling-up Lemma

- The bias of $\mathbf{X}_i$ is defined to be the quantity

$$\epsilon_i = p_i - \frac{1}{2}.$$

The Piling-up Lemma

- The bias of $\mathbf{X}_i$ is defined to be the quantity

$$\epsilon_i = p_i - \frac{1}{2}.$$

$$\begin{aligned} \Pr[\mathbf{X}_i = 0] &= p_i = \epsilon_i + \frac{1}{2}, \text{ and} \\ \Pr[\mathbf{X}_i = 1] &= 1 - p_i = \epsilon_i - \frac{1}{2} \end{aligned}$$

The Piling-up Lemma

- The bias of $\mathbf{X}_i$ is defined to be the quantity

$$\epsilon_i = p_i - \frac{1}{2}.$$

$$\begin{aligned}
\Pr[\mathbf{X}_i = 0] &= p_i = \epsilon_i + \frac{1}{2}, \text{ and} \\
\Pr[\mathbf{X}_i = 1] &= 1 - p_i = \epsilon_i - \frac{1}{2}
\end{aligned}$$

- $-\frac{1}{2} \leqslant \epsilon_i \leqslant \frac{1}{2}$.

The Piling-up Lemma

Let $\epsilon_{i_1,i_2,\ldots,i_k}$ denote the bias of the random variable $\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_k}$. Then

$$\epsilon_{i_1,i_2,\ldots,i_k} = 2^{k-1}\Pi_{j=1}^{k}\epsilon_{i_j}.$$

Proof

- Basis:

$$\Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} = 0] = \left(\frac{1}{2} + \epsilon_{i_1}\right)\left(\frac{1}{2} + \epsilon_{i_2}\right) + \left(\frac{1}{2} - \epsilon_{i_1}\right)\left(\frac{1}{2} - \epsilon_{i_2}\right) = \frac{1}{2} + 2\epsilon_{i_1}\epsilon_{i_2}$$

The Piling-up Lemma

Let $\epsilon_{i_1,i_2,\ldots,i_k}$ denote the bias of the random variable $\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_k}$. Then

$$\epsilon_{i_1,i_2,\ldots,i_k} = 2^{k-1}\Pi_{j=1}^{k}\epsilon_{i_j}.$$

Proof

- Basis:

$$\Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} = 0] = \left(\frac{1}{2} + \epsilon_{i_1}\right)\left(\frac{1}{2} + \epsilon_{i_2}\right) + \left(\frac{1}{2} - \epsilon_{i_1}\right)\left(\frac{1}{2} - \epsilon_{i_2}\right) = \frac{1}{2} + 2\epsilon_{i_1}\epsilon_{i_2}$$

- Induction:

$$\begin{aligned} & \Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_k} = 0] \\ = \quad & \Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_{k-1}} = 0 \wedge \mathbf{X}_{i_k} = 0] \\ & + \Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_{k-1}} = 1 \wedge \mathbf{X}_{i_k} = 1] \end{aligned}$$

The Piling-up Lemma

Let $\epsilon_{i_1,i_2,\ldots,i_k}$ denote the bias of the random variable $\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_k}$. Then

$$\epsilon_{i_1,i_2,\ldots,i_k} = 2^{k-1}\Pi_{j=1}^{k}\epsilon_{i_j}.$$

Proof

- Basis:

$$\Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} = 0] = \left(\frac{1}{2} + \epsilon_{i_1}\right)\left(\frac{1}{2} + \epsilon_{i_2}\right) + \left(\frac{1}{2} - \epsilon_{i_1}\right)\left(\frac{1}{2} - \epsilon_{i_2}\right) = \frac{1}{2} + 2\epsilon_{i_1}\epsilon_{i_2}$$

- Induction:

$$\begin{aligned}
& \Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_k} = 0] \\
= \; & \Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_{k-1}} = 0 \wedge \mathbf{X}_{i_k} = 0] \\
& + \Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_{k-1}} = 1 \wedge \mathbf{X}_{i_k} = 1] \\
= \; & \Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_{k-1}} = 0]\Pr[\mathbf{X}_{i_k} = 0] \\
& + \Pr[\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \oplus \mathbf{X}_{i_{k-1}} = 1]\Pr[\mathbf{X}_{i_k} = 1]
\end{aligned}$$

Proof

$$= \left(\frac{1}{2} + \epsilon_{i_1,i_2,\ldots,i_{k-1}}\right)\left(\frac{1}{2} + \epsilon_{i_k}\right) + \left(\frac{1}{2} - \epsilon_{i_1,i_2,\ldots,i_{k-1}}\right)\left(\frac{1}{2} - \epsilon_{i_k}\right)$$

Proof

$$\begin{aligned} &= \left(\frac{1}{2}+\epsilon_{i_1,i_2,\ldots,i_{k-1}}\right)\left(\frac{1}{2}+\epsilon_{i_k}\right)+\left(\frac{1}{2}-\epsilon_{i_1,i_2,\ldots,i_{k-1}}\right)\left(\frac{1}{2}-\epsilon_{i_k}\right) \\ &= \frac{1}{2}+2\epsilon_{i_1,i_2,\ldots,i_{k-1}}\epsilon_{i_k} \end{aligned}$$

Proof

$$
\begin{aligned}
&= \left(\frac{1}{2}+\epsilon_{i_1,i_2,\ldots,i_{k-1}}\right)\left(\frac{1}{2}+\epsilon_{i_k}\right)+\left(\frac{1}{2}-\epsilon_{i_1,i_2,\ldots,i_{k-1}}\right)\left(\frac{1}{2}-\epsilon_{i_k}\right) \\
&= \frac{1}{2}+2\epsilon_{i_1,i_2,\ldots,i_{k-1}}\epsilon_{i_k} \\
&= \frac{1}{2}+2\left(2^{k-2}\Pi_{j=1}^{k-1}\epsilon_{i_j}\right)\epsilon_{i_k}
\end{aligned}
$$

Proof

$$
\begin{aligned}
&= \left(\frac{1}{2}+\epsilon_{i_1,i_2,\ldots,i_{k-1}}\right)\left(\frac{1}{2}+\epsilon_{i_k}\right)+\left(\frac{1}{2}-\epsilon_{i_1,i_2,\ldots,i_{k-1}}\right)\left(\frac{1}{2}-\epsilon_{i_k}\right)\\
&= \frac{1}{2}+2\epsilon_{i_1,i_2,\ldots,i_{k-1}}\epsilon_{i_k}\\
&= \frac{1}{2}+2\left(2^{k-2}\Pi_{j=1}^{k-1}\epsilon_{i_j}\right)\epsilon_{i_k}\\
&= \frac{1}{2}+2^{k-1}\Pi_{j=1}^{k}\epsilon_{i_j}.
\end{aligned}
$$

The Piling-up Lemma

Corollary. Let $\epsilon_{i_1}, \epsilon_{i_2}, \ldots$ denote the bias of the random variable $\mathbf{X}_{i_1}, \mathbf{X}_{i_2}, \cdots$. Suppose that $\epsilon_{i_j} = 0$ for some j. Then $\epsilon_{i_1, i_2, \ldots, i_k} = 0$.

The Piling-up Lemma

Corollary. Let $\epsilon_{i_1}, \epsilon_{i_2}, \ldots$ denote the bias of the random variable $\mathbf{X}_{i_1}, \mathbf{X}_{i_2}, \cdots$. Suppose that $\epsilon_{i_j} = 0$ for some j. Then $\epsilon_{i_1, i_2, \ldots, i_k} = 0$.

Note

- Let $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ be three independent random variables with $\epsilon_1 = \epsilon_2 = \epsilon_3 = \frac{1}{4}$.

The Piling-up Lemma

Corollary. Let $\epsilon_{i_1}, \epsilon_{i_2}, \ldots$ denote the bias of the random variable $\mathbf{X}_{i_1}, \mathbf{X}_{i_2}, \cdots$. Suppose that $\epsilon_{i_j} = 0$ for some j. Then $\epsilon_{i_1, i_2, \ldots, i_k} = 0$.

Note

- Let $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ be three independent random variables with $\epsilon_1 = \epsilon_2 = \epsilon_3 = \frac{1}{4}$.
- $\epsilon_{1,2} = \epsilon_{2,3} = \epsilon_{1,3} = \frac{1}{8}$.

The Piling-up Lemma

Corollary. Let $\epsilon_{i_1}, \epsilon_{i_2}, \ldots$ denote the bias of the random variable $\mathbf{X}_{i_1}, \mathbf{X}_{i_2}, \cdots$. Suppose that $\epsilon_{i_j} = 0$ for some j. Then $\epsilon_{i_1, i_2, \ldots, i_k} = 0$.

Note

- Let $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ be three independent random variables with $\epsilon_1 = \epsilon_2 = \epsilon_3 = \frac{1}{4}$.
- $\epsilon_{1,2} = \epsilon_{2,3} = \epsilon_{1,3} = \frac{1}{8}$.
- $\mathbf{X}_1 \oplus \mathbf{X}_3 = (\mathbf{X}_1 \oplus \mathbf{X}_2) \oplus (\mathbf{X}_2 \oplus \mathbf{X}_3)$.

The Piling-up Lemma

Corollary. Let $\epsilon_{i_1}, \epsilon_{i_2}, \ldots$ denote the bias of the random variable $\mathbf{X}_{i_1}, \mathbf{X}_{i_2}, \cdots$. Suppose that $\epsilon_{i_j} = 0$ for some j. Then $\epsilon_{i_1, i_2, \ldots, i_k} = 0$.

Note

- Let $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ be three independent random variables with $\epsilon_1 = \epsilon_2 = \epsilon_3 = \frac{1}{4}$.
- $\epsilon_{1,2} = \epsilon_{2,3} = \epsilon_{1,3} = \frac{1}{8}$.
- $\mathbf{X}_1 \oplus \mathbf{X}_3 = (\mathbf{X}_1 \oplus \mathbf{X}_2) \oplus (\mathbf{X}_2 \oplus \mathbf{X}_3)$.
  - $\epsilon'_{1,3} = 2 \times \frac{1}{8} \times \frac{1}{8} = \frac{1}{32}$

The Piling-up Lemma

Corollary. Let $\epsilon_{i_1}, \epsilon_{i_2}, \ldots$ denote the bias of the random variable $\mathbf{X}_{i_1}, \mathbf{X}_{i_2}, \cdots$. Suppose that $\epsilon_{i_j} = 0$ for some j. Then $\epsilon_{i_1, i_2, \ldots, i_k} = 0$.

Note

- Let $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ be three independent random variables with $\epsilon_1 = \epsilon_2 = \epsilon_3 = \frac{1}{4}$.
- $\epsilon_{1,2} = \epsilon_{2,3} = \epsilon_{1,3} = \frac{1}{8}$.
- $\mathbf{X}_1 \oplus \mathbf{X}_3 = (\mathbf{X}_1 \oplus \mathbf{X}_2) \oplus (\mathbf{X}_2 \oplus \mathbf{X}_3)$.
  - $\epsilon'_{1,3} = 2 \times \frac{1}{8} \times \frac{1}{8} = \frac{1}{32}$
  - $(\mathbf{X}_1 \oplus \mathbf{X}_2)$ and $(\mathbf{X}_2 \oplus \mathbf{X}_3)$ are not independent random variables.

The Piling-up Lemma

Corollary. Let $\epsilon_{i_1}, \epsilon_{i_2}, \ldots$ denote the bias of the random variable $\mathbf{X}_{i_1}, \mathbf{X}_{i_2}, \cdots$. Suppose that $\epsilon_{i_j} = 0$ for some j. Then $\epsilon_{i_1, i_2, \ldots, i_k} = 0$.

Note

- Let $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ be three independent random variables with $\epsilon_1 = \epsilon_2 = \epsilon_3 = \frac{1}{4}$.
- $\epsilon_{1,2} = \epsilon_{2,3} = \epsilon_{1,3} = \frac{1}{8}$.
- $\mathbf{X}_1 \oplus \mathbf{X}_3 = (\mathbf{X}_1 \oplus \mathbf{X}_2) \oplus (\mathbf{X}_2 \oplus \mathbf{X}_3)$.
  - $\epsilon'_{1,3} = 2 \times \frac{1}{8} \times \frac{1}{8} = \frac{1}{32}$
  - $(\mathbf{X}_1 \oplus \mathbf{X}_2)$ and $(\mathbf{X}_2 \oplus \mathbf{X}_3)$ are not independent random variables.
- In Linear Cryptanalysis:
  - $(\mathbf{X}_1 \oplus \mathbf{X}_2 = 0)$ and $(\mathbf{X}_2 \oplus \mathbf{X}_3 = 0)$ are analogus to linear approximations of S-boxes.

The Piling-up Lemma

Corollary. Let $\epsilon_{i_1}, \epsilon_{i_2}, \ldots$ denote the bias of the random variable $\mathbf{X}_{i_1}, \mathbf{X}_{i_2}, \cdots$. Suppose that $\epsilon_{i_j} = 0$ for some j. Then $\epsilon_{i_1, i_2, \ldots, i_k} = 0$.

Note

- Let $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ be three independent random variables with $\epsilon_1 = \epsilon_2 = \epsilon_3 = \frac{1}{4}$.
- $\epsilon_{1,2} = \epsilon_{2,3} = \epsilon_{1,3} = \frac{1}{8}$.
- $\mathbf{X}_1 \oplus \mathbf{X}_3 = (\mathbf{X}_1 \oplus \mathbf{X}_2) \oplus (\mathbf{X}_2 \oplus \mathbf{X}_3)$.
  - $\epsilon'_{1,3} = 2 \times \frac{1}{8} \times \frac{1}{8} = \frac{1}{32}$
  - $(\mathbf{X}_1 \oplus \mathbf{X}_2)$ and $(\mathbf{X}_2 \oplus \mathbf{X}_3)$ are not independent random variables.
- In Linear Cryptanalysis:
  - $(\mathbf{X}_1 \oplus \mathbf{X}_2 = 0)$ and $(\mathbf{X}_2 \oplus \mathbf{X}_3 = 0)$ are analogus to linear approximations of S-boxes.
  - $(\mathbf{X}_1 \oplus \mathbf{X}_3 = 0)$ is analogous to a cipher approximation where the intermediate bit $\mathbf{X}_2$ is eliminated.

Linear Approximations of S-boxes

- How do we construct expressions which are highly linear and, hence, can be exploited?

Linear Approximations of S-boxes

- How do we construct expressions which are highly linear and, hence, can be exploited?
- Can be done by considering the properties of the cipherâs only nonlinear component: the S-box.

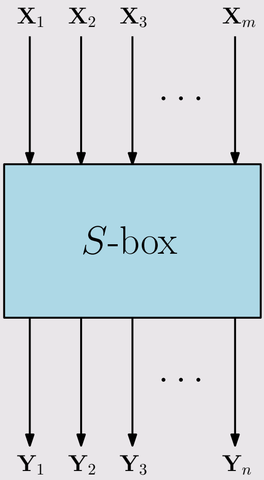
Linear Approximations of S-boxes

- How do we construct expressions which are highly linear and, hence, can be exploited?
- Can be done by considering the properties of the cipherâs only nonlinear component: the S-box.
- The nonlinearity properties of the S-box are enumerated, it is possible to develop linear approximations between sets of input and output bits in the S-box.

Linear Approximations of S-boxes

- How do we construct expressions which are highly linear and, hence, can be exploited?
- Can be done by considering the properties of the cipherâs only nonlinear component: the S-box.
- The nonlinearity properties of the S-box are enumerated, it is possible to develop linear approximations between sets of input and output bits in the S-box.
- Possible to concatenate linear approximations of the S-boxes.

Linear Approximations of S-boxes



Linear Approximations of S-boxes

- Consider S-box $\pi_S : \{0,1\}^m \longrightarrow \{0,1\}^n$.

Linear Approximations of S-boxes

- Consider S-box $\pi_S : \{0,1\}^m \longrightarrow \{0,1\}^n$.
- $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m$ are input random variable.
- $\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_n$ are output random variable.

Linear Approximations of S-boxes

- Consider S-box $\pi_S : \{0,1\}^m \longrightarrow \{0,1\}^n$.
- $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m$ are input random variable.
- $\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_n$ are output random variable.
- $\mathbf{X}_i$s are independent, and $\epsilon_i = 0$.

Linear Approximations of S-boxes

- Consider S-box $\pi_S : \{0,1\}^m \longrightarrow \{0,1\}^n$.
- $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m$ are input random variable.
- $\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_n$ are output random variable.
- $\mathbf{X}_i$s are independent, and $\epsilon_i = 0$.
- $\mathbf{Y}_j$s are not independent from other $\mathbf{Y}_j$s and $\mathbf{X}_i$s.

Linear Approximations of S-boxes

- Consider S-box $\pi_S : \{0,1\}^m \longrightarrow \{0,1\}^n$.
- $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m$ are input random variable.
- $\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_n$ are output random variable.
- $\mathbf{X}_i$s are independent, and $\epsilon_i = 0$.
- $\mathbf{Y}_j$s are not independent from other $\mathbf{Y}_j$s and $\mathbf{X}_i$s.
- If $(y_1 \cdots y_n) \neq \pi_S(x_1 \cdots x_m)$,

$$\Pr[\mathbf{X}_1 = x_1, \ldots, \mathbf{X}_m = x_m, \mathbf{Y}_1 = y_1, \ldots, \mathbf{Y}_n = y_n] = 0.$$

Linear Approximations of S-boxes

- Consider S-box $\pi_S : \{0,1\}^m \longrightarrow \{0,1\}^n$.
- $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m$ are input random variable.
- $\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_n$ are output random variable.
- $\mathbf{X}_i$s are independent, and $\epsilon_i = 0$.
- $\mathbf{Y}_j$s are not independent from other $\mathbf{Y}_j$s and $\mathbf{X}_i$s.
- If $(y_1 \cdots y_n) \neq \pi_S(x_1 \cdots x_m)$,

$$\Pr[\mathbf{X}_1 = x_1, \ldots, \mathbf{X}_m = x_m, \mathbf{Y}_1 = y_1, \ldots, \mathbf{Y}_n = y_n] = 0.$$

- if $(y_1 \cdots y_n) = \pi_S(x_1 \cdots x_m)$,

$$\Pr[\mathbf{X}_1 = x_1, \ldots, \mathbf{X}_m = x_m, \mathbf{Y}_1 = y_1, \ldots, \mathbf{Y}_n = y_n] = 2^m.$$

Linear Approximations of S-boxes

input	0	1	2	3	4	5	6	7
output	E	4	D	1	2	F	B	8

input	8	9	A	B	C	D	E	F
output	3	A	6	C	5	9	0	7

Linear Approximations of S-boxes

input	0	1	2	3	4	5	6	7
output	E	4	D	1	2	F	B	8
input	8	9	A	B	C	D	E	F
output	3	A	6	C	5	9	0	7

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4
0	0	0	0	1	1	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	0	0	0	1	0
0	1	0	1	1	1	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	0	0	0
0	0	0	0	0	0	1	1
0	0	0	1	1	0	1	0
0	0	1	0	0	1	1	0
0	0	1	1	1	1	0	0
0	1	0	0	0	1	0	1
0	1	0	1	1	0	0	1
0	1	1	0	0	0	0	0
0	1	1	1	0	1	1	1

Linear Approximations of S-boxes

- Straightforward to compute the bias of a random variable of the form

$$\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v}.$$

Linear Approximations of S-boxes

- Straightforward to compute the bias of a random variable of the form

$$\mathbf{X}_{i_1} \oplus \mathbf{X}_{i_2} \oplus \cdots \mathbf{X}_{i_u} \oplus \mathbf{Y}_{j_1} \oplus \mathbf{Y}_{j_2} \oplus \cdots \oplus \mathbf{Y}_{j_v}.$$

- A linear cryptanalytic attack can potentially be mounted when a random variable of this form has a bias that is bounded away from zero.

Linear Approximations of S-boxes

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
0	0	0	0	0	0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	1	0	0	0	0	0	1	1
0	0	1	0	0	1	1	0	1	1	1	1	1	0
0	0	1	1	1	1	0	0	1	1	0	1	0	1
0	1	0	0	0	1	0	1	1	1	1	1	0	1
0	1	0	1	1	0	0	1	1	0	0	0	1	0
0	1	1	0	0	0	0	0	0	0	1	0	1	0
0	1	1	1	0	1	1	1	0	0	0	1	0	1

Linear Cryptanalysis

Linear Approximations of S-boxes

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
0	0	0	0	0	0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	1	0	0	0	0	0	1	1
0	0	1	0	0	1	1	0	1	1	1	1	1	0
0	0	1	1	1	1	0	0	1	1	0	1	0	1
0	1	0	0	0	1	0	1	1	1	1	1	0	1
0	1	0	1	1	0	0	1	1	0	0	0	1	0
0	1	1	0	0	0	0	0	0	0	1	0	1	0
0	1	1	1	0	1	1	1	0	0	0	1	0	1

- $\Pr[\mathbf{X}_2 \oplus \mathbf{X}_3 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_3 \oplus \mathbf{Y}_4 = 0] = \frac{3}{4}$

Linear Approximations of S-boxes

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
0	0	0	0	0	0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	1	0	0	0	0	0	1	1
0	0	1	0	0	1	1	0	1	1	1	1	1	0
0	0	1	1	1	1	0	0	1	1	0	1	0	1
0	1	0	0	0	1	0	1	1	1	1	1	0	1
0	1	0	1	1	0	0	1	1	0	0	0	1	0
0	1	1	0	0	0	0	0	0	0	1	0	1	0
0	1	1	1	0	1	1	1	0	0	0	1	0	1

- $\Pr[\mathbf{X}_2 \oplus \mathbf{X}_3 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_3 \oplus \mathbf{Y}_4 = 0] = \frac{3}{4}$
- $\Pr[\mathbf{X}_1 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_2 = 0] = \frac{1}{2}$

Linear Approximations of S-boxes

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
0	0	0	0	0	0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	1	0	0	0	0	0	1	1
0	0	1	0	0	1	1	0	1	1	1	1	1	0
0	0	1	1	1	1	0	0	1	1	0	1	0	1
0	1	0	0	0	1	0	1	1	1	1	1	0	1
0	1	0	1	1	0	0	1	1	0	0	0	1	0
0	1	1	0	0	0	0	0	0	0	1	0	1	0
0	1	1	1	0	1	1	1	0	0	0	1	0	1

- $\Pr[\mathbf{X}_2 \oplus \mathbf{X}_3 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_3 \oplus \mathbf{Y}_4 = 0] = \frac{3}{4}$
- $\Pr[\mathbf{X}_1 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_2 = 0] = \frac{1}{2}$
- $\Pr[\mathbf{X}_3 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_4 = 0] = \frac{1}{8}$

Linear Approximations of S-boxes

- Any random variable can be written as

$$\left(\bigoplus_{i=1}^{m} a_i \mathbf{X}_i\right) \oplus \left(\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j\right).$$

Linear Approximations of S-boxes

- Any random variable can be written as

$$\left(\bigoplus_{i=1}^{m} a_i \mathbf{X}_i\right) \oplus \left(\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j\right).$$

- Input sum a is the binary vector $(a_1, a_2, \ldots, a_m)$.

Linear Approximations of S-boxes

- Any random variable can be written as

$$\left(\bigoplus_{i=1}^{m} a_i \mathbf{X}_i\right) \oplus \left(\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j\right).$$

- Input sum a is the binary vector $(a_1, a_2, \ldots, a_m)$.
- Output sum b is the binary vector $(b_1, b_2, \ldots, b_n)$.

Linear Cryptanalysis

Linear Approximations Table of S-boxes $N_L(a,b)$

a \ b	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	-2	-2	0	0	-2	+6	+2	+2	0	0	+2	+2	0	0
2	0	0	-2	-2	0	0	-2	-2	0	0	+2	+2	0	0	-6	+2
3	0	0	0	0	0	0	0	0	+2	-6	-2	-2	+2	+2	-2	-2
4	0	+2	0	-2	-2	-4	-2	0	0	-2	0	+2	+2	-4	+2	0
5	0	-2	-2	0	-2	0	+4	+2	-2	0	-4	+2	0	-2	-2	0
6	0	+2	-2	+4	+2	0	0	+2	0	-2	+2	+4	-2	0	0	-2
7	0	-2	0	+2	+2	-4	+2	0	-2	0	+2	0	+4	+2	0	+2
8	0	0	0	0	0	0	0	0	-2	+2	+2	-2	+2	-2	-2	-6
9	0	0	-2	-2	0	0	-2	-2	-4	0	-2	+2	0	+4	+2	-2
A	0	+4	-2	+2	-4	0	+2	-2	+2	+2	0	0	+2	+2	0	0
B	0	+4	0	-4	+4	0	+4	0	0	0	0	0	0	0	0	0
C	0	-2	+4	-2	-2	0	+2	0	+2	0	+2	+4	0	+2	0	-2
D	0	+2	+2	0	-2	+4	0	+2	-4	-2	+2	0	+2	0	0	+2
E	0	+2	+2	0	-2	-4	0	+2	-2	0	0	-2	-4	+2	-2	0
F	0	-2	-4	-2	-2	0	+2	0	0	-2	+4	-2	-2	0	+2	0

Linear Approximations Table of S-boxes $N_L(a,b)$

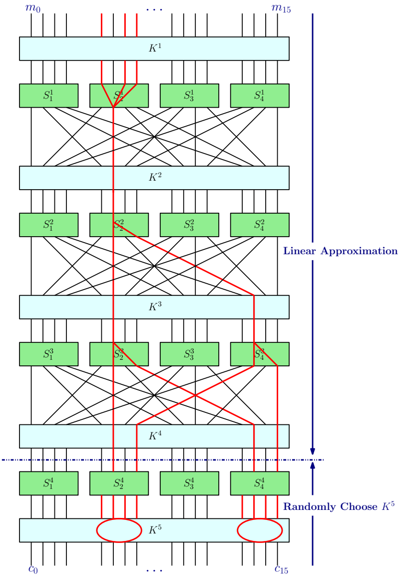
	b															
a	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	-2	-2	0	0	-2	+6	+2	+2	0	0	+2	+2	0	0
2	0	0	-2	-2	0	0	-2	-2	0	0	+2	+2	0	0	-6	+2
3	0	0	0	0	0	0	0	0	+2	-6	-2	-2	+2	+2	-2	-2
4	0	+2	0	-2	-2	-4	-2	0	0	-2	0	+2	+2	-4	+2	0
5	0	-2	-2	0	-2	0	+4	+2	-2	0	-4	+2	0	-2	-2	0
6	0	+2	-2	+4	+2	0	0	+2	0	-2	+2	+4	-2	0	0	-2
7	0	-2	0	+2	+2	-4	+2	0	-2	0	+2	0	+4	+2	0	+2
8	0	0	0	0	0	0	0	0	-2	+2	+2	-2	+2	-2	-2	-6
9	0	0	-2	-2	0	0	-2	-2	-4	0	-2	+2	0	+4	+2	-2
A	0	+4	-2	+2	-4	0	+2	-2	+2	+2	0	0	+2	+2	0	0
B	0	+4	0	-4	+4	0	+4	0	0	0	0	0	0	0	0	0
C	0	-2	+4	-2	-2	0	+2	0	+2	0	+2	+4	0	+2	0	-2
D	0	+2	+2	0	-2	+4	0	+2	-4	-2	+2	0	+2	0	0	+2
E	0	+2	+2	0	-2	-4	0	+2	-2	0	0	-2	-4	+2	-2	0
F	0	-2	-4	-2	-2	0	+2	0	0	-2	+4	-2	-2	0	+2	0

$$\Pr\left[\left(\bigoplus_{i=1}^{m} a_i \mathbf{X}_i\right) \oplus \left(\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j\right)\right] = \frac{8 + N_L(a,b)}{16}.$$

A Linear Attack on SPN

- $\mathbf{U}^i$: The input to the i^{th} round S-box.
- $\mathbf{U}^i_j$: The j^{th} bit of block $\mathbf{U}^{(i)}$.
- $\mathbf{V}^i$: The output of the i^{th} round S-box.
- $\mathbf{V}^i_j$: The j^{th} bit of block $\mathbf{V}^{(i)}$.
- $\mathbf{K}^i$: The i^{th} round key.

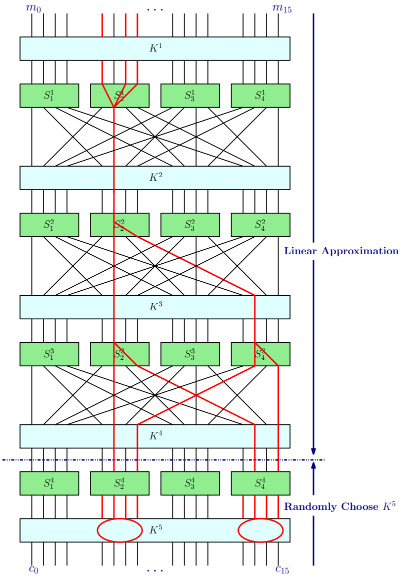
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

- S_2^1: $\mathbf{T}_1 = \mathbf{U}_4^1 \oplus \mathbf{U}_6^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{V}_5^1$, bias = $\frac{1}{4}$

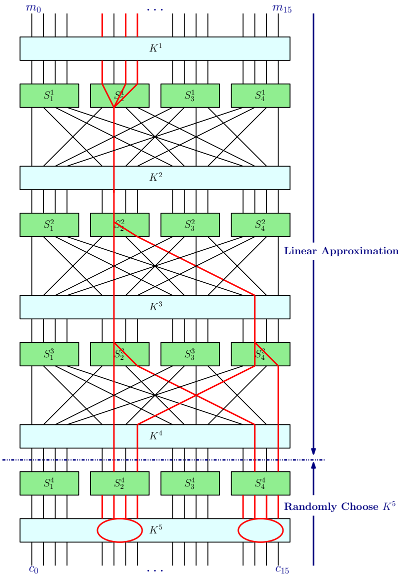
Linear Cryptanalysis



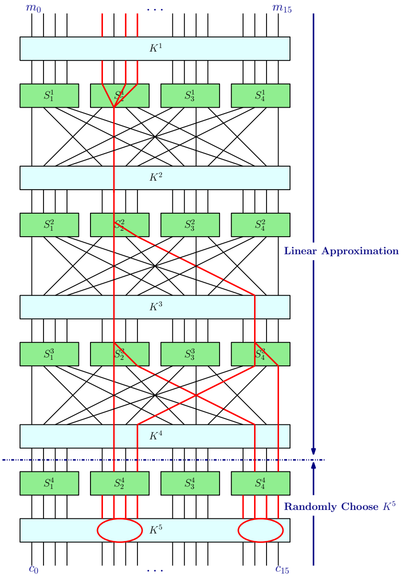
$\ell = 4$, $l = 4$, and $m = 4$

- S_2^1: $\mathbf{T}_1 = \mathbf{U}_4^1 \oplus \mathbf{U}_6^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{V}_5^1$, bias = $\frac{1}{4}$
- S_2^2: $\mathbf{T}_2 = \mathbf{U}_5^2 \oplus \mathbf{V}_5^2 \oplus \mathbf{V}_7^2$, bias = $-\frac{1}{4}$

Linear Cryptanalysis



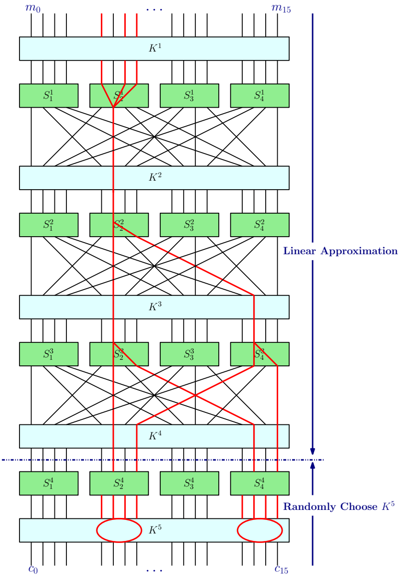
- S_2^1: $\mathbf{T}_1 = \mathbf{U}_4^1 \oplus \mathbf{U}_6^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{V}_5^1$, bias = $\frac{1}{4}$
- S_2^2: $\mathbf{T}_2 = \mathbf{U}_5^2 \oplus \mathbf{V}_5^2 \oplus \mathbf{V}_7^2$, bias = $-\frac{1}{4}$
- S_2^3: $\mathbf{T}_3 = \mathbf{U}_5^3 \oplus \mathbf{V}_5^3 \oplus \mathbf{V}_7^3$, bias = $-\frac{1}{4}$



$\ell = 4$, $l = 4$, and $m = 4$

- S_2^1: $\mathbf{T}_1 = \mathbf{U}_4^1 \oplus \mathbf{U}_6^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{V}_5^1$, bias = $\frac{1}{4}$
- S_2^2: $\mathbf{T}_2 = \mathbf{U}_5^2 \oplus \mathbf{V}_5^2 \oplus \mathbf{V}_7^2$, bias = $-\frac{1}{4}$
- S_2^3: $\mathbf{T}_3 = \mathbf{U}_5^3 \oplus \mathbf{V}_5^3 \oplus \mathbf{V}_7^3$, bias = $-\frac{1}{4}$
- S_4^3: $\mathbf{T}_4 = \mathbf{U}_{13}^3 \oplus \mathbf{V}_{13}^3 \oplus \mathbf{V}_{15}^3$, bias = $-\frac{1}{4}$

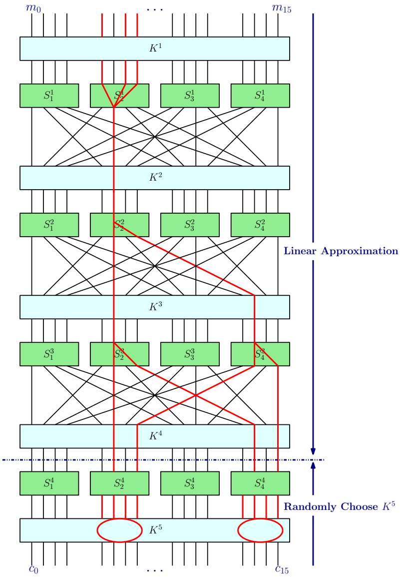
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

- $\mathbf{T}_1 = \left(m_4 \oplus \mathbf{K}^1_4\right) \oplus \left(m_6 \oplus \mathbf{K}^1_6\right) \oplus \left(m_7 \oplus \mathbf{K}^1_7\right) \oplus \mathbf{V}^1_5$

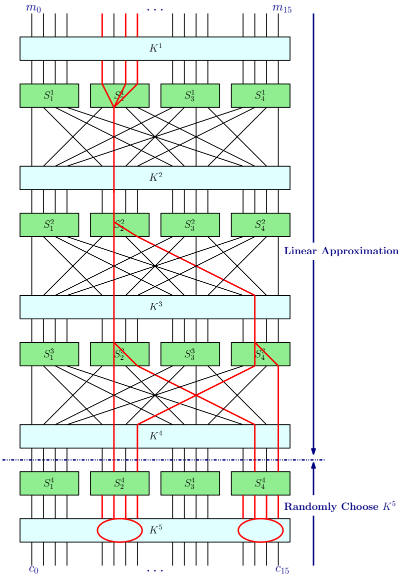
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

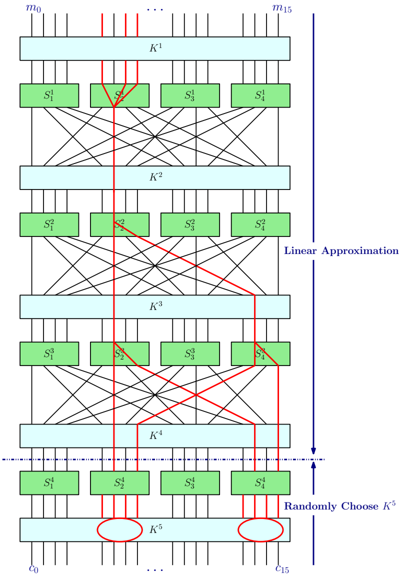
- $\mathbf{T}_1 = \left(m_4 \oplus \mathbf{K}_4^1\right) \oplus \left(m_6 \oplus \mathbf{K}_6^1\right) \oplus \left(m_7 \oplus \mathbf{K}_7^1\right) \oplus \mathbf{V}_5^1$
- $\mathbf{T}_2 = \left(\mathbf{V}_5^1 \oplus \mathbf{K}_5^2\right) \oplus \mathbf{V}_5^2 \oplus \mathbf{V}_7^2$

Linear Cryptanalysis



- $\mathbf{T}_1 = \left(m_4 \oplus \mathbf{K}_4^1\right) \oplus \left(m_6 \oplus \mathbf{K}_6^1\right) \oplus \left(m_7 \oplus \mathbf{K}_7^1\right) \oplus \mathbf{V}_5^1$
- $\mathbf{T}_2 = \left(\mathbf{V}_5^1 \oplus \mathbf{K}_5^2\right) \oplus \mathbf{V}_5^2 \oplus \mathbf{V}_7^2$
- $\mathbf{T}_3 = \left(\mathbf{V}_5^2 \oplus \mathbf{K}_5^3\right) \oplus \mathbf{V}_5^3 \oplus \mathbf{V}_7^3$

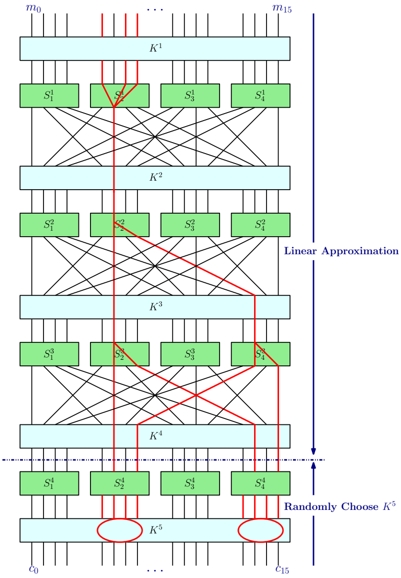
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

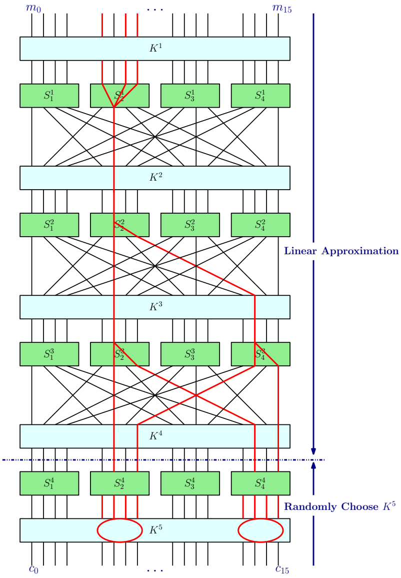
- $\mathbf{T}_1 = \left(m_4 \oplus \mathbf{K}_4^1\right) \oplus \left(m_6 \oplus \mathbf{K}_6^1\right) \oplus \left(m_7 \oplus \mathbf{K}_7^1\right) \oplus \mathbf{V}_5^1$
- $\mathbf{T}_2 = \left(\mathbf{V}_5^1 \oplus \mathbf{K}_5^2\right) \oplus \mathbf{V}_5^2 \oplus \mathbf{V}_7^2$
- $\mathbf{T}_3 = \left(\mathbf{V}_5^2 \oplus \mathbf{K}_5^3\right) \oplus \mathbf{V}_5^3 \oplus \mathbf{V}_7^3$
- $\mathbf{T}_4 = \left(\mathbf{V}_7^2 \oplus \mathbf{K}_{13}^3\right) \oplus \mathbf{V}_{13}^3 \oplus \mathbf{V}_{15}^3$

Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

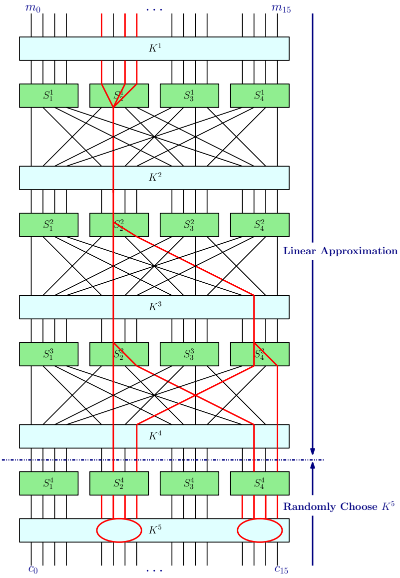
$$\mathbf{T} = \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4$$



$\ell = 4$, $l = 4$, and $m = 4$

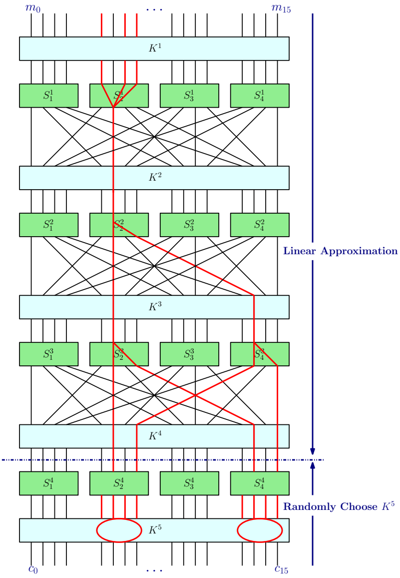
$$
\begin{aligned}
\mathbf{T} &= \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\quad \oplus \mathbf{V}_5^3 \oplus \mathbf{V}_7^3 \oplus \mathbf{V}_{13}^3 \oplus \mathbf{V}_{15}^3 \\
&\quad \oplus \mathbf{K}_4^1 \oplus \mathbf{K}_6^1 \oplus \mathbf{K}_7^1 \\
&\quad \oplus \mathbf{K}_5^2 \oplus \mathbf{K}_5^3 \oplus \mathbf{K}_{13}^3
\end{aligned}
$$

Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

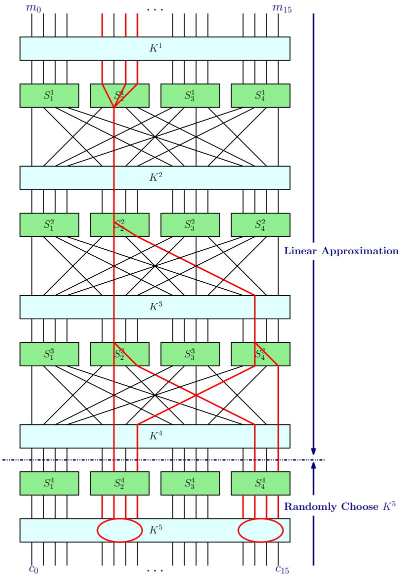
$$\mathbf{T} = \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4$$
$$= m_4 \oplus m_6 \oplus m_7$$



$\ell = 4$, $l = 4$, and $m = 4$

$$
\begin{aligned}
\mathbf{T} &= \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\quad \oplus \left(\mathbf{U}_5^4 \oplus \mathbf{K}_5^4\right) \oplus \left(\mathbf{U}_7^4 \oplus \mathbf{K}_7^4\right) \\
&\quad \oplus \left(\mathbf{U}_{13}^4 \oplus \mathbf{K}_{13}^4\right) \oplus \left(\mathbf{U}_{15}^4 \oplus \mathbf{K}_{15}^4\right)
\end{aligned}
$$

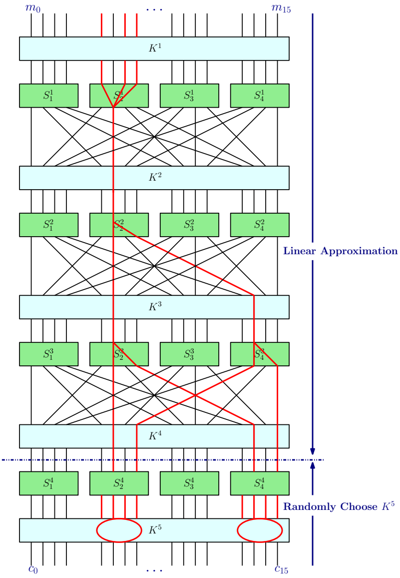
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

$$
\begin{aligned}
\mathbf{T} &= \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\oplus \left(\mathbf{U}^4_5 \oplus \mathbf{K}^4_5\right) \oplus \left(\mathbf{U}^4_7 \oplus \mathbf{K}^4_7\right) \\
&\oplus \left(\mathbf{U}^4_{13} \oplus \mathbf{K}^4_{13}\right) \oplus \left(\mathbf{U}^4_{15} \oplus \mathbf{K}^4_{15}\right) \\
&\oplus \mathbf{K}^1_4 \oplus \mathbf{K}^1_6 \oplus \mathbf{K}^1_7 \\
&\oplus \mathbf{K}^2_5 \oplus \mathbf{K}^3_5 \oplus \mathbf{K}^3_{13}
\end{aligned}
$$

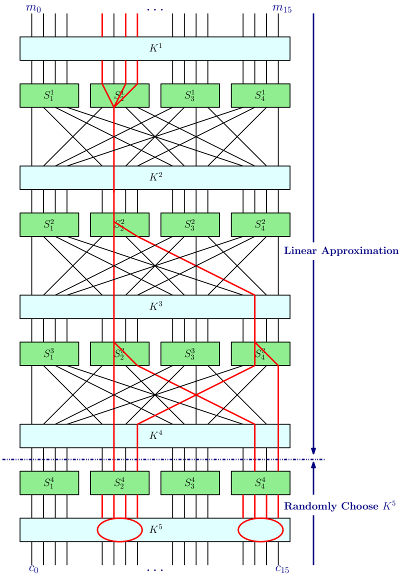
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

$$\mathbf{T} = \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4$$
$$= m_4 \oplus m_6 \oplus m_7$$

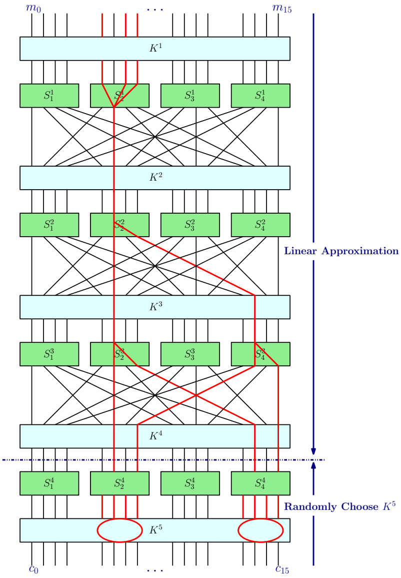
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

$$\begin{aligned}
\mathbf{T} &= \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\quad \oplus \mathbf{U}_5^4 \oplus \mathbf{U}_7^4 \oplus \mathbf{U}_{13}^4 \oplus \mathbf{U}_{15}^4
\end{aligned}$$

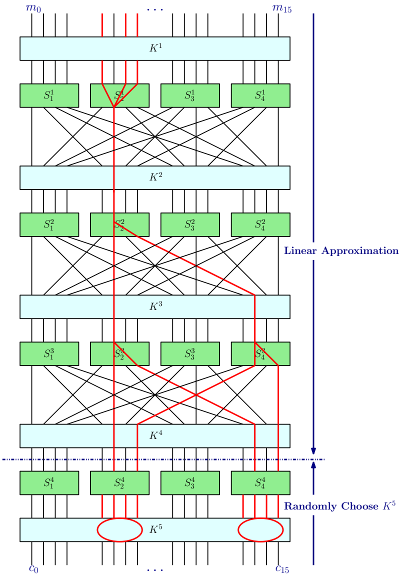
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

$$
\begin{aligned}
\mathbf{T} &= \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\quad \oplus \mathbf{U}_5^4 \oplus \mathbf{U}_7^4 \oplus \mathbf{U}_{13}^4 \oplus \mathbf{U}_{15}^4 \\
&\quad \oplus \mathbf{K}_4^1 \oplus \mathbf{K}_6^1 \oplus \mathbf{K}_7^1 \\
&\quad \oplus \mathbf{K}_5^2 \oplus \mathbf{K}_5^3 \oplus \mathbf{K}_{13}^3 \\
&\quad \oplus \mathbf{K}_5^4 \oplus \mathbf{K}_7^4 \oplus \mathbf{K}_{13}^4 \oplus \mathbf{K}_{15}^4
\end{aligned}
$$

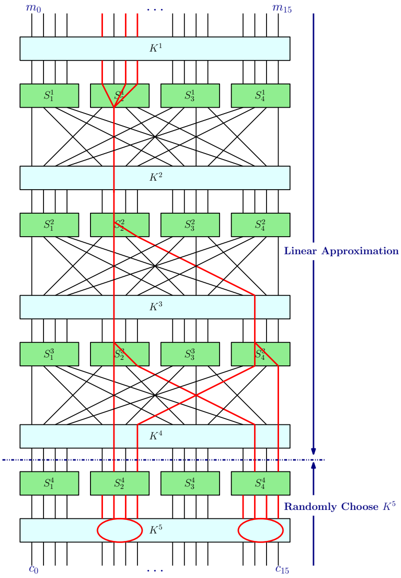
Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

$$
\begin{aligned}
\mathbf{T} &= \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\quad \oplus \mathbf{U}_5^4 \oplus \mathbf{U}_7^4 \oplus \mathbf{U}_{13}^4 \oplus \mathbf{U}_{15}^4 \\
&\quad \oplus \mathbf{K}_4^1 \oplus \mathbf{K}_6^1 \oplus \mathbf{K}_7^1 \\
&\quad \oplus \mathbf{K}_5^2 \oplus \mathbf{K}_5^3 \oplus \mathbf{K}_{13}^3 \\
&\quad \oplus \mathbf{K}_5^4 \oplus \mathbf{K}_7^4 \oplus \mathbf{K}_{13}^4 \oplus \mathbf{K}_{15}^4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\quad \oplus \mathbf{U}_5^4 \oplus \mathbf{U}_7^4 \oplus \mathbf{U}_{13}^4 \oplus \mathbf{U}_{15}^4
\end{aligned}
$$

Linear Cryptanalysis



$\ell = 4$, $l = 4$, and $m = 4$

$$
\begin{aligned}
\mathbf{T} &= \mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\quad \oplus \mathbf{U}_5^4 \oplus \mathbf{U}_7^4 \oplus \mathbf{U}_{13}^4 \oplus \mathbf{U}_{15}^4 \\
&\quad \oplus \mathbf{K}_4^1 \oplus \mathbf{K}_6^1 \oplus \mathbf{K}_7^1 \\
&\quad \oplus \mathbf{K}_5^2 \oplus \mathbf{K}_5^3 \oplus \mathbf{K}_{13}^3 \\
&\quad \oplus \mathbf{K}_5^4 \oplus \mathbf{K}_7^4 \oplus \mathbf{K}_{13}^4 \oplus \mathbf{K}_{15}^4 \\
&= m_4 \oplus m_6 \oplus m_7 \\
&\quad \oplus \mathbf{U}_5^4 \oplus \mathbf{U}_7^4 \oplus \mathbf{U}_{13}^4 \oplus \mathbf{U}_{15}^4 \\
&\quad \oplus \Sigma_K
\end{aligned}
$$

Bias of bT

- Bias of $\mathbf{T} = 2^{4-1} \times \frac{1}{4} \times (-\frac{1}{4})^2 = -\frac{1}{32}$

Bias of bT

- Bias of $\mathbf{T} = 2^{4-1} \times \frac{1}{4} \times (-\frac{1}{4})^2 = -\frac{1}{32}$
- Assume that all sub-key bits are fixed.
- $\Sigma_K = 0$ or 1.

Bias of bT

- Bias of $\mathbf{T} = 2^{4-1} \times \frac{1}{4} \times (-\frac{1}{4})^2 = -\frac{1}{32}$
- Assume that all sub-key bits are fixed.
- $\Sigma_K = 0$ or 1.
- Therefore, bias of $\mathbf{T}$ actually $\pm\frac{1}{32}$.

Bias of bT

- Bias of $\mathbf{T} = 2^{4-1} \times \frac{1}{4} \times (-\frac{1}{4})^2 = -\frac{1}{32}$
- Assume that all sub-key bits are fixed.
- $\Sigma_K = 0$ or 1.
- Therefore, bias of $\mathbf{T}$ actually $\pm\frac{1}{32}$.
- We assume that $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ and $\mathbf{T}_4$ are independent random variable.

Bias of bT

- Bias of $\mathbf{T} = 2^{4-1} \times \frac{1}{4} \times (-\frac{1}{4})^2 = -\frac{1}{32}$
- Assume that all sub-key bits are fixed.
- $\Sigma_K = 0$ or 1.
- Therefore, bias of $\mathbf{T}$ actually $\pm\frac{1}{32}$.
- We assume that $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ and $\mathbf{T}_4$ are independent random variable.
- But it reality they are not.

Bias of bT

- Bias of $\mathbf{T} = 2^{4-1} \times \frac{1}{4} \times (-\frac{1}{4})^2 = -\frac{1}{32}$
- Assume that all sub-key bits are fixed.
- $\Sigma_K = 0$ or 1.
- Therefore, bias of $\mathbf{T}$ actually $\pm\frac{1}{32}$.
- We assume that $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ and $\mathbf{T}_4$ are independent random variable.
- But it reality they are not.
- This approximation actually works in practice.

Attack

Input: A list $\mathcal{T}$ that contains T (m, c) pairs.

1. for $(L_1, L_2) \longleftarrow (0, 0)$ to (F, F) do
2. $\quad C[L_1, L_2] \longleftarrow 0$

Attack

Input: A list $\mathcal{T}$ that contains T (m,c) pairs.

1. for $(L_1, L_2) \longleftarrow (0,0)$ to (F,F) do
2. $\quad C[L_1, L_2] \longleftarrow 0$
3. for each $(m,c) \in \mathcal{T}$ do
4. $\quad v^4_{\langle 2 \rangle} \longleftarrow L_1 \oplus c_{\langle 2 \rangle}$
5. $\quad v^4_{\langle 4 \rangle} \longleftarrow L_2 \oplus c_{\langle 4 \rangle}$

Attack

Input: A list $\mathcal{T}$ that contains T (m,c) pairs.

1. for $(L_1, L_2) \longleftarrow (0,0)$ to (F,F) do
2. $\quad C[L_1, L_2] \longleftarrow 0$
3. for each $(m,c) \in \mathcal{T}$ do
4. $\quad v^4_{\langle 2 \rangle} \longleftarrow L_1 \oplus c_{\langle 2 \rangle}$
5. $\quad v^4_{\langle 4 \rangle} \longleftarrow L_2 \oplus c_{\langle 4 \rangle}$
6. $\quad u^4_{\langle 2 \rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 2 \rangle}\right)$
7. $\quad u^4_{\langle 4 \rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 4 \rangle}\right)$

Attack

Input: A list $\mathcal{T}$ that contains T (m,c) pairs.

1. for $(L_1,L_2) \longleftarrow (0,0)$ to (F,F) do
2. $\quad C[L_1,L_2] \longleftarrow 0$
3. for each $(m,c) \in \mathcal{T}$ do
4. $\quad v^4_{\langle 2\rangle} \longleftarrow L_1 \oplus c_{\langle 2\rangle}$
5. $\quad v^4_{\langle 4\rangle} \longleftarrow L_2 \oplus c_{\langle 4\rangle}$
6. $\quad u^4_{\langle 2\rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 2\rangle}\right)$
7. $\quad u^4_{\langle 4\rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 4\rangle}\right)$
8. $\quad z \longleftarrow m_4 \oplus m_6 \oplus m_7 \oplus u^4_5 \oplus u^4_7 \oplus u^4_{13} \oplus u^4_{15}$

Attack

Input: A list $\mathcal{T}$ that contains T (m, c) pairs.

1. for $(L_1, L_2) \longleftarrow (0,0)$ to (F, F) do
2. $\quad C[L_1, L_2] \longleftarrow 0$
3. for each $(m, c) \in \mathcal{T}$ do
4. $\quad v^4_{\langle 2 \rangle} \longleftarrow L_1 \oplus c_{\langle 2 \rangle}$
5. $\quad v^4_{\langle 4 \rangle} \longleftarrow L_2 \oplus c_{\langle 4 \rangle}$
6. $\quad u^4_{\langle 2 \rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 2 \rangle}\right)$
7. $\quad u^4_{\langle 4 \rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 4 \rangle}\right)$
8. $\quad z \longleftarrow m_4 \oplus m_6 \oplus m_7 \oplus u^4_5 \oplus u^4_7 \oplus u^4_{13} \oplus u^4_{15}$
9. $\quad$ if $z = 0$, $C[L_1, L_2] \longleftarrow C[L_1, L_2] + 1$

Attack

Input: A list $\mathcal{T}$ that contains T (m, c) pairs.

1. for $(L_1, L_2) \longleftarrow (0, 0)$ to (F, F) do
2. $\quad C[L_1, L_2] \longleftarrow 0$
3. for each $(m, c) \in \mathcal{T}$ do
4. $\quad v^4_{\langle 2 \rangle} \longleftarrow L_1 \oplus c_{\langle 2 \rangle}$
5. $\quad v^4_{\langle 4 \rangle} \longleftarrow L_2 \oplus c_{\langle 4 \rangle}$
6. $\quad u^4_{\langle 2 \rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 2 \rangle}\right)$
7. $\quad u^4_{\langle 4 \rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 4 \rangle}\right)$
8. $\quad z \longleftarrow m_4 \oplus m_6 \oplus m_7 \oplus u^4_5 \oplus u^4_7 \oplus u^4_{13} \oplus u^4_{15}$
9. $\quad$ if $z = 0$, $C[L_1, L_2] \longleftarrow C[L_1, L_2] + 1$
10. for $(L_1, L_2) \longleftarrow (0, 0)$ to (F, F) do
11. $\quad C[L_1, L_2] \longleftarrow \left| C[L_1, L_2] - \frac{T}{2} \right|$

Attack

Input: A list $\mathcal{T}$ that contains T (m, c) pairs.

1. for $(L_1, L_2) \longleftarrow (0,0)$ to (F, F) do
2. $\quad C[L_1, L_2] \longleftarrow 0$
3. for each $(m, c) \in \mathcal{T}$ do
4. $\quad v^4_{\langle 2 \rangle} \longleftarrow L_1 \oplus c_{\langle 2 \rangle}$
5. $\quad v^4_{\langle 4 \rangle} \longleftarrow L_2 \oplus c_{\langle 4 \rangle}$
6. $\quad u^4_{\langle 2 \rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 2 \rangle}\right)$
7. $\quad u^4_{\langle 4 \rangle} \longleftarrow \pi_S^{-1}\left(v^4_{\langle 4 \rangle}\right)$
8. $\quad z \longleftarrow m_4 \oplus m_6 \oplus m_7 \oplus u^4_5 \oplus u^4_7 \oplus u^4_{13} \oplus u^4_{15}$
9. $\quad$ if $z = 0$, $C[L_1, L_2] \longleftarrow C[L_1, L_2] + 1$
10. for $(L_1, L_2) \longleftarrow (0,0)$ to (F, F) do
11. $\quad C[L_1, L_2] \longleftarrow \left| C[L_1, L_2] - \frac{T}{2} \right|$
12. Let for (l_1, l_2), $C[l_1, l_2]$ has maximum. Then return (l_1, l_2).

End