Cryptanalysis of Block Ciphers: Lecture 1

Nilanjan Datta

IAI, TCG CREST

tcg crest
Inventing Harmonious Future

Contents

Cryptanalysis

Kerckhoffs' Principle

- The cryptosystem is known to the adversary.
- But the key is not known to the attacker.
- The secrecy of the cryptosystem lies in the key.

Goals of Cryptanalysis

Assumptions

Cryptanalyst has access to black-box implementation of the block cipher with secret key K.

Aims of Cryptanalyst

- Key Recovery: Find the key K.
- Plaintext Recovery: Find M corresponding to C such that $E_K(M) = C$ for unknown K.
- Distinguishing: Distinguish member of block ciphers from a random permutation.

Models for Cryptanalysis

The model essentially tells you the power of the adversary.

Attack Scenarios

- Ciphertext Only Attack (CA).
- Known Plaintext Attack (KPA).
- Chosen Plaintext Attack (CPA).
- Chosen Ciphertext Attack (CCA).

Models for Cryptanalysis

The model essentially tells you the power of the adversary.

Attack Scenarios

- Ciphertext Only Attack (CA).
- Known Plaintext Attack (KPA).
- Chosen Plaintext Attack (CPA).
- Chosen Ciphertext Attack (CCA).

- Increasing order of strength: $CA < KPA < CPA < CCA$.
- The adversary may be adaptive as well.

Complexity of Cryptanalysis

Data

Data is measured by the number of queries.

Time

Time is measured by computational cost (cost of one execution of E_K or D_K) executed by an attacker offline.

Memory

Memory is measured by the memory required to store plaintext, ciphertext, intermediate values to mount an attack.

Complexity of Cryptanalysis

Attack Complexity

(D, T, M) Attack complexity of an attack against some security notion under some attack model:

- Attacker can ask D queries to the oracle.
- Attacker can spend the cost of E_K or D_K T times.
- Attacker has enough memory to store M data.

Generic Brute Force Attacks

Block size: n, Key size: k.

Key Recovery Attack: Exhaustive Key Search

- Try all the keys, one by one.
- Attack complexity: $(k/n, 2^k, negl)$.

Plaintext Recovery: Codebook/Dictionary Attack

- Query all 2^n plaintext and stores the corresponding ciphertexts.
- Attack complexity: $(2^n, negl, 2n.2^n)$.

Shortcut Attacks

Attacks exploiting the intrinsic properties of the block cipher.

Popular Shortcut Attacks

- Differential Cryptanalysis
- Impossible Differential Cryptanalysis
- Linear Cryptanalysis
- Integral Attacks
- Related key Attacks
- Boomerang Attacks

Differential Cryptanalysis

Proposed by Biham and Shamir

Goal of the Attacker

- Distinguishing Attack
- Key Recovery Attack

Attack Model

Chosen Plaintext Attack (CPA)

Differential Cryptanalysis

Difference of Two Values

$\Delta x = x \oplus x'$

Difference processed by a Function

$\Delta y = F(x) \oplus F(x')$

- Difference Propagation: $\Delta x \rightarrow \Delta y$
- Propagation Ratio: $\Pr[\Delta x \rightarrow \Delta y]$

Motivation

Analysis with Single Value

$$S = P \oplus K$$

K is secret $\Rightarrow$ Attacker have no idea about the state

Analysis with Difference of Two Values

$$S = P \oplus K, \qquad S' = P' \oplus K$$

Motivation

Analysis with Single Value

$$S = P \oplus K$$

K is secret $\Rightarrow$ Attacker have no idea about the state

Analysis with Difference of Two Values

$$S = P \oplus K, \qquad S' = P' \oplus K$$
$$\Delta S = S \oplus S' = (P \oplus K) \oplus (P' \oplus K) = P \oplus P'$$

Attacker knows the state difference irrespective of key value K

Basic Concept

- Given an iterative cipher $\mathcal{E}$ composed of r rounds

Main Idea

Try to exploit high propagation ratio $\Pr[\Delta x \xrightarrow{\mathcal{E}} \Delta y]$ for r rounds

Distinguishing Attack

- Attacker has a large set of tuples (x, x', y, y') with fixed input xor $\Delta x = x \oplus x'$
- Verify whether $y \oplus y' = \Delta y$ occurs with significantly high probability

Basic Concept

- Given an iterative cipher $\mathcal{E}$ composed of r rounds

Main Idea

Try to exploit high propagation ratio $\Pr[\Delta x \xrightarrow{\mathcal{E}} \Delta y]$ for $(r-1)$ rounds

Basic Concept

- Given an iterative cipher $\mathcal{E}$ composed of r rounds

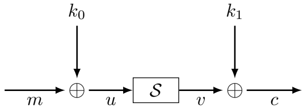
Main Idea

Try to exploit high propagation ratio $\Pr[\Delta x \xrightarrow{\mathcal{E}} \Delta y]$ for $(r-1)$ rounds

Sub-key Recovery Attack

- Attacker has a large set of tuples (x, x', y, y') with fixed input xor $\Delta x = x \oplus x'$
- For each candidate keys
  - decrypt (y, y') and compute the xor of certain state bits
  - if the xor is Δy, increment a counter for the candidate key
- Report the candidate key with highest counter

First Toy Cipher: Cipher1

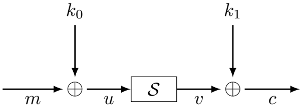


x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	6	4	C	5	0	7	2	E	1	F	3	D	8	A	9	B

Table: Sample S-Box

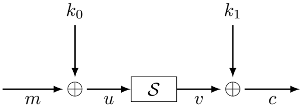
- Can you mount a key-recovery attack?
- Assume that you know two (plaintext-ciphertext) pairs: $(A, 9)$ and $(5, 6)$.

Differential Cryptanalysis of Cipher1



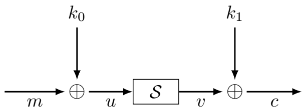
- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known (use of differential)

Differential Cryptanalysis of Cipher1



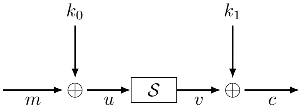
- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known (use of differential)
- Guess the Key k_1 and obtain v_0 and v_1
- Verify whether $S^{-1}(v_0) \oplus S^{-1}(v_1) \stackrel{?}{=} \Delta u$

Differential Cryptanalysis of Cipher1



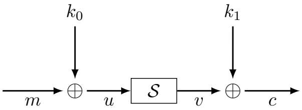
- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known (use of differential)
- Guess the Key k_1 and obtain v_0 and v_1
- Verify whether $S^{-1}(v_0) \oplus S^{-1}(v_1) \stackrel{?}{=} \Delta u$
- If verified for multiple keys, consider another pair messages and continue.

Differential Cryptanalysis of Cipher1



- We know two (plaintext-ciphertext) pairs: $(A, 9)$ and $(5, 6)$.
- $\Delta u = u_0 \oplus u_1 = A \oplus 5 = F$.
- Guess the Key k_1 and verify whether $S^{-1}(k_1 \oplus 9) \oplus S^{-1}(k_1 \oplus 6) \stackrel{?}{=} F$.
- Satisfies for $k_1 = 7,\ 8$.

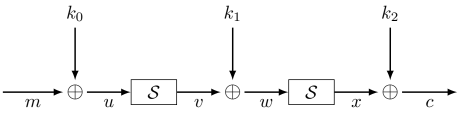
Differential Cryptanalysis of Cipher1



- Consider encryption of two messages 9 and 8. Let the ciphertexts are 7 and 0 resp.
- $\Delta u = u_0 \oplus u_1 = 9 \oplus 8 = 1$.
- Guess the Key k_1 and verify whether $S^{-1}(k_1 \oplus 7) \oplus S^{-1}(k_1 \oplus 0) \stackrel{?}{=} 1$.
- Satisfies for $k_1 = 0,\ 7$.

Conclusion: $k_1 = 7$ should be the key.

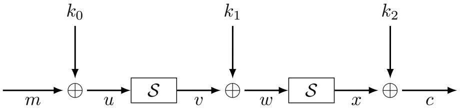
Second Toy Cipher: Cipher2



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

Table: Sample S-Box

Differential Cryptanalysis of Cipher2



- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known
- Guess the Key k_2 and obtain x_0 and x_1. Compute $w_0 = S^{-1}(x_0)$ and $w_1 = S^{-1}(x_1)$
- $\Delta v = v_0 \oplus v_1 = w_0 \oplus w_1$ is known

Need to find Δu such that the propagation ratio $\Delta u \to \Delta v$ is high

High Differential Characteristic for Sample S-Box

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

i	j	$S(i) \oplus S(j)$
0	F	D
1	E	D
2	D	6
3	C	D
4	B	D
5	A	4
6	9	D
7	8	F
8	7	F
9	6	D
A	5	4
B	4	D
C	3	D
D	2	6
E	1	D
F	0	D

$F \rightarrow D$ has high propagation ratio: $\frac{10}{16}$

Differential Uniformity

Difference Distribution Table (DDT)

$2^n \times 2^n$ table to capture the distribution of the difference:

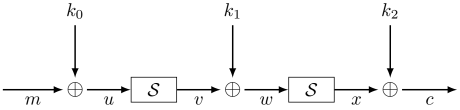
$$D_S(a,b) = |\{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus a) = b\}|.$$

Differential Uniformity

Maximum value in the DDT table (non-zero difference propagation):

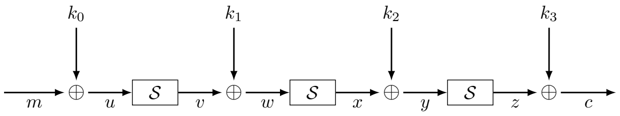
$$D_S = max_{a,b \neq 0} D_S(a,b).$$

Differential Cryptanalysis of Cipher2



- Set $m_0 \oplus m_1 = F$
- We have $\Delta u = F$ is known
- Guess the Key k_2 and obtain x_0 and x_1. Compute $w_0 = S^{-1}(x_0)$ and $w_1 = S^{-1}(x_1)$
- Verify whether $\Delta v = D$
- For the correct key, above holds with high probability

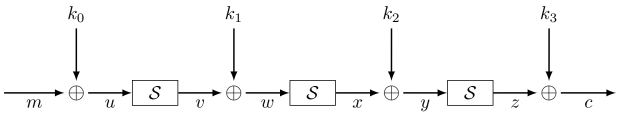
Third Toy Cipher: Cipher3



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

Table: Sample S-Box

Differential Cryptanalysis of Cipher3



- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known
- Guess the Key k_3 and obtain z_0 and z_1. Compute $y_0 = S^{-1}(z_0)$ and $y_1 = S^{-1}(z_1)$
- $\Delta x = x_0 \oplus x_1 = y_0 \oplus y_1$ is known

Need to find Δu such that propagation ratio $\Delta u \rightarrow \Delta x$ is high

High Propagation ratio for Sample S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
2	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
3	0	0	0	6	0	2	0	0	2	0	0	0	4	0	2	0
4	0	0	0	2	0	2	4	0	0	2	2	2	0	0	2	0
5	0	2	2	0	4	0	0	4	2	0	0	2	0	0	0	0
6	0	0	2	0	4	0	0	2	2	0	2	2	2	0	0	0
7	0	0	0	0	0	4	4	0	2	2	2	2	0	0	0	0
8	0	0	0	0	0	2	0	2	4	0	0	4	0	2	0	2
9	0	2	0	0	0	2	2	2	0	4	2	0	0	0	0	2
A	0	0	0	0	2	2	0	0	0	4	4	0	2	2	0	0
B	0	0	0	2	2	0	2	2	2	0	0	4	0	0	2	0
C	0	4	0	2	0	2	0	0	2	0	0	0	0	0	6	0
D	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
E	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
F	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

Table: DDT Corresponding to the S-Box

$F \rightarrow D \rightarrow C$ has high propagation ratio:

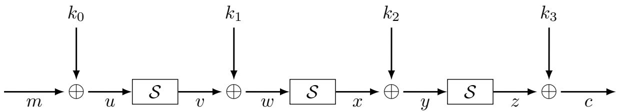
High Propagation ratio for Sample S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
2	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
3	0	0	0	6	0	2	0	0	2	0	0	0	4	0	2	0
4	0	0	0	2	0	2	4	0	0	2	2	2	0	0	2	0
5	0	2	2	0	4	0	0	4	2	0	0	2	0	0	0	0
6	0	0	2	0	4	0	0	2	2	0	2	2	2	0	0	0
7	0	0	0	0	0	4	4	0	2	2	2	2	0	0	0	0
8	0	0	0	0	0	2	0	2	4	0	0	4	0	2	0	2
9	0	2	0	0	0	2	2	2	0	4	2	0	0	0	0	2
A	0	0	0	0	2	2	0	0	0	4	4	0	2	2	0	0
B	0	0	0	2	2	0	2	2	2	0	0	4	0	0	2	0
C	0	4	0	2	0	2	0	0	2	0	0	0	0	0	6	0
D	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
E	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
F	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

Table: DDT Corresponding to the S-Box

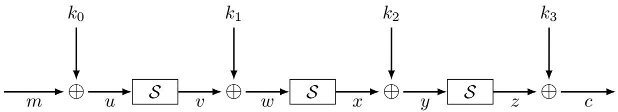
$F \rightarrow D \rightarrow C$ has high propagation ratio: $\frac{10}{16} \cdot \frac{6}{16}$

Differential Cryptanalysis of Cipher3



- Set $m_0 \oplus m_1 = F$
- We have $\Delta u = F$ is known

Differential Cryptanalysis of Cipher3



- Set $m_0 \oplus m_1 = F$
- We have $\Delta u = F$ is known
- Guess the Key k_3 and obtain z_0 and z_1. Compute $y_0 = S^{-1}(z_0)$ and $y_1 = S^{-1}(z_1)$
- Verify whether $\Delta x = \Delta y = C$
- For the correct key, above holds with high probability

Impossible Differential Cryptanalysis: Basic Concept

- Independently found by Knudsen, Biham and Shamir
- Exploits a differential Propagation that is never satisfied

Basic Concept

Impossible Differential Characteristic

- Δx: Input difference of function F
- Δy: Output difference of function F

The pair $(\Delta x, \Delta y)$ is an impossible differential characteristic with respect to F if

$$\Pr[\Delta x \rightarrow \Delta y] = 0$$

Basic Concept

Impossible Differential Characteristic

- Δx: Input difference of function F
- Δy: Output difference of function F

The pair $(\Delta x, \Delta y)$ is an impossible differential characteristic with respect to F if

$$\Pr[\Delta x \rightarrow \Delta y] = 0$$

Example

Let F be a bijective function. Then following are trivial impossible diffential characteristic:

- $0 \rightarrow y \ (y \neq 0)$
- $x \rightarrow 0 \ (x \neq 0)$

Comparison with Differential Cryptanalysis

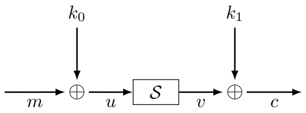
Differential Cryptanalysis

- Construct a differential characteristic with a high probability.
- Detect the right key from the obtained key suggestions.

Impossible Differential Cryptanalysis

- Construct a differential characteristic that has probability 0.
- Discard all the wrong key guesses from the obtained key suggestions.

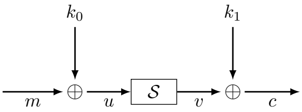
First Toy Cipher: Cipher1



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

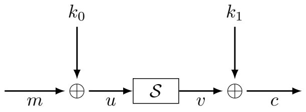
Table: Sample S-Box

Impossible Differential Cryptanalysis of Cipher1



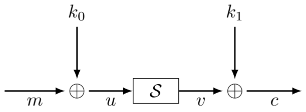
- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known
- Guess the Key k_1 and obtain v_0 and v_1

Impossible Differential Cryptanalysis of Cipher1



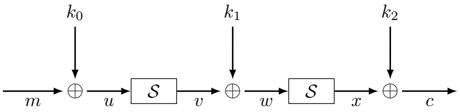
- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known
- Guess the Key k_1 and obtain v_0 and v_1
- Verify whether $S^{-1}(v_0) \oplus S^{-1}(v_1) \overset{?}{\neq} \Delta u$

Impossible Differential Cryptanalysis of Cipher1



- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known
- Guess the Key k_1 and obtain v_0 and v_1
- Verify whether $S^{-1}(v_0) \oplus S^{-1}(v_1) \overset{?}{\neq} \Delta u$
- If the above holds, discard the key. Continue with another pair messages and continue until only one key remains.

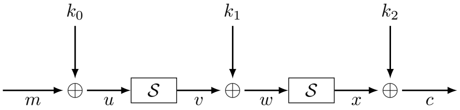
Second Toy Cipher: Cipher2



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

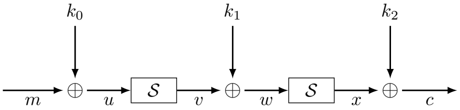
Table: Sample S-Box

Impossible Differential Cryptanalysis of Cipher2



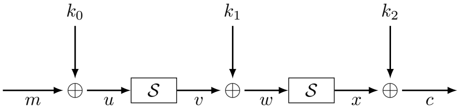
- Consider encryption of two messages m_0 and m_1

Impossible Differential Cryptanalysis of Cipher2



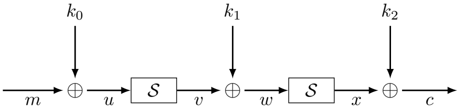
- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known

Impossible Differential Cryptanalysis of Cipher2



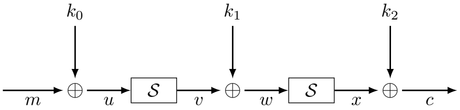
- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known
- Guess the Key k_2 and obtain x_0 and x_1. Compute $w_0 = S^{-1}(x_0)$ and $w_1 = S^{-1}(x_1)$

Impossible Differential Cryptanalysis of Cipher2



- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known
- Guess the Key k_2 and obtain x_0 and x_1. Compute $w_0 = S^{-1}(x_0)$ and $w_1 = S^{-1}(x_1)$
- $\Delta v = v_0 \oplus v_1 = w_0 \oplus w_1$ is known

Impossible Differential Cryptanalysis of Cipher2



- Consider encryption of two messages m_0 and m_1
- $\Delta u = u_0 \oplus u_1 = m_0 \oplus m_1$ is known
- Guess the Key k_2 and obtain x_0 and x_1. Compute $w_0 = S^{-1}(x_0)$ and $w_1 = S^{-1}(x_1)$
- $\Delta v = v_0 \oplus v_1 = w_0 \oplus w_1$ is known

Need to find Δu such that the propagation ratio $\Delta u \rightarrow \Delta v$ is zero

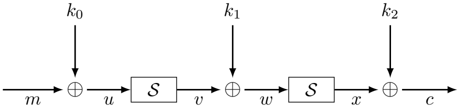
Zero Differential Characteristic for Sample S-Box

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

i	j	$S(i) \oplus S(j)$
0	F	D
1	E	D
2	D	6
3	C	D
4	B	D
5	A	4
6	9	D
7	8	F
8	7	F
9	6	D
A	5	4
B	4	D
C	3	D
D	2	6
E	1	D
F	0	D

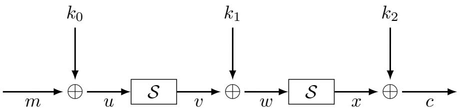
$F \rightarrow \{0, 1, 2, 3, 5, 7, 8, A, B, C, E\}$ has propagation ratio 0

Impossible Differential Cryptanalysis of Cipher2



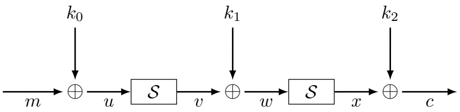
- Set $m_0 \oplus m_1 = F$

Impossible Differential Cryptanalysis of Cipher2



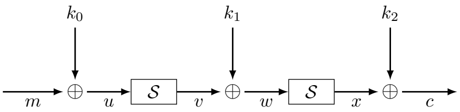
- Set $m_0 \oplus m_1 = F$
- We have $\Delta u = F$ is known

Impossible Differential Cryptanalysis of Cipher2



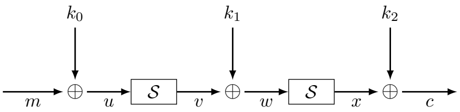
- Set $m_0 \oplus m_1 = F$
- We have $\Delta u = F$ is known
- Guess the Key k_2 and obtain x_0 and x_1. Compute $w_0 = S^{-1}(x_0)$ and $w_1 = S^{-1}(x_1)$

Impossible Differential Cryptanalysis of Cipher2



- Set $m_0 \oplus m_1 = F$
- We have $\Delta u = F$ is known
- Guess the Key k_2 and obtain x_0 and x_1. Compute $w_0 = S^{-1}(x_0)$ and $w_1 = S^{-1}(x_1)$
- Verify whether $\Delta v \in \{0, 1, 2, 3, 5, 7, 8, A, B, C, E\}$

Impossible Differential Cryptanalysis of Cipher2



- Set $m_0 \oplus m_1 = F$
- We have $\Delta u = F$ is known
- Guess the Key k_2 and obtain x_0 and x_1. Compute $w_0 = S^{-1}(x_0)$ and $w_1 = S^{-1}(x_1)$
- Verify whether $\Delta v \in \{0, 1, 2, 3, 5, 7, 8, A, B, C, E\}$
- If the above holds for a key, discard it

References

Kazuo Sakiyama, Yu Sasaki and Yang Li, *"Security of Block Ciphers: From Algorithm Design to Hardware Implementation"*

Thank You..!!!