Japanese Standards Association (JSA)
Information Technology Research and Standardization Center (INSTAC)
Tamper-resistance Standardization Research Committee (TSRC)

# Experimental Results of Attacks Against Ciphers Implemented on INSTAC-8 Compliant Board

Yukiyasu Tsunoo (*3,4), Toru Hisakado (*4),
Etsuko Tsujihara (*5), Tsutomu Matsumoto (*1,6),
Shinichi Kawamura (*2,7), Koichi Fujisaki (*7)

*1:TSRC Chair, *2:TSRC Secretary, *3:TSRC member, *4: NEC Corporation,
*5: YDK Co.,Ltd., *6: Yokohama National University, *7: Toshiba Corporation

# Table of Contents

- Introduction
- Development of the evaluation platform
- DPA on DES
- EMA on Mini cipher model
- SPA on A5/1
- Conclusion

# Side Channel Attacks

Example :

An attack based on measurement of instantaneous power consumption of a device while it runs a cryptographic algorithm.

- Execution Time
  - → Timing Attack
- Power Consumption
  - →Power Analysis
    - Simple Power Analysis (SPA)
    - Differential Power Analysis (DPA)
- Electromagnetic radiation
  - →ElectroMagnetic Analysis (EMA)

# Tamper Resistance Techniques

Any kind of technique that adds resistance to ciphers so that they might not be broken easily by side channel attack.

- Blockage of attacks
- Detection of attacks
- Trace of attacks

## Problems

- Common evaluation environment is required, where we can verify the newly proposed technique.
- Standardization of requirements for the level and quality of tamper resistance

# INSTAC
## (Information Technology Research and Standardization Center)

- INSTAC is a division of Japanese standard association to develop and encourage standardization in information technology.
- INSTAC established a task group on tamper-resistance standardization, to promote sound development and normal usage of tamper-resistance techniques.

# Activities of INSTAC

- To establish the foundations for secure implementation of information technologies from a viewpoint of standardization, INSTAC has been conducting following studies and researches:

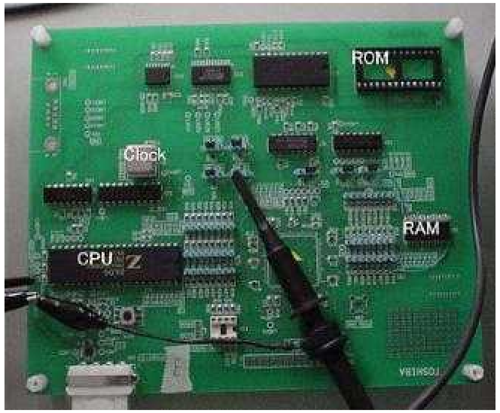
  - Systematic study on various tampering techniques
    - ✓ Development of specified standard evaluation platform

  - Development of the methods to describe requirements for tamper-resistance

  - International standardization with respect to tamper-resistance

# Developing Evaluation Platforms

- INSTAC-8 (2003)
  - Equipped with 8bit CPU
  - SW implementation is supported
  - Suitable for common key cipher because of the limitation of memory



- INSTAC-32 (due for release in 2005 winter)
  - Equipped with 32bit CPU & FPGA
  - SW/HW implementation is supported
  - The public key cryptosystem can be processed.

# Attack on Ciphers on the Evaluation Platform

## (1) DPA : DES (Block Cipher)

- ➢ Without countermeasure
- ➢ With countermeasure to DPA
  - - one proposed by Akkar and Giraud (CHES2001)
  - - one proposed by Goubin and Patarin (CHES1999)

Fujisaki, Tomoeda, Miyake, Komano, Shimbo, Kawamura [ISEC2004]

## (2) EMA : Mini cipher model (Block Cipher)

Takahashi, Fukunaga, Ootsuka, Kanda [ISEC2004]

## (3) SPA : A5/1 (Stream Cipher)

Tsunoo, Hisakado, Tsujihara, Issiki, Minematsu[to appear]

# Outline of Experimental Attack

- Purpose: Design verification of INSTAC-8 compliant evaluation board

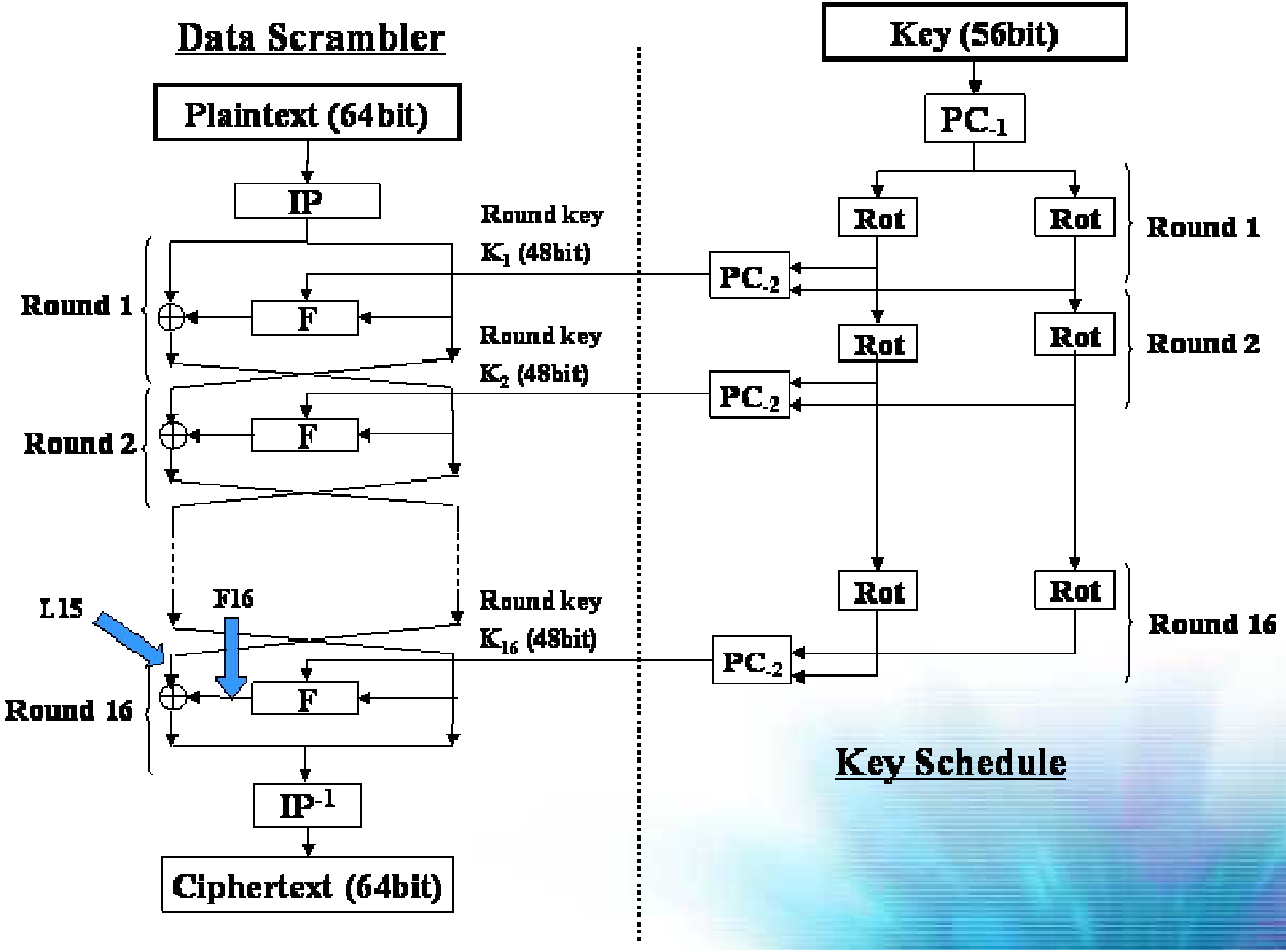
- Outline: DPA was made on DES and tamper-resistance techniques were evaluated, to verify the ability of the board to evaluate the tamper resistance techniques.

- Applied on DES (Block Cipher)

- Attack technique: DPA

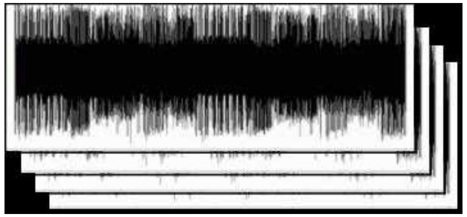
- Tamper-resistance technique: (1) technique proposed by Akkar et al. (2) technique proposed by Goubin et al.

# Algorithm


Data Scrambler
Plaintext (64bit)
IP
Round key
$K_1$ (48bit)
Round 1
F
Round key
$K_2$ (48bit)
Round 2
F
L15
F16
Round key
$K_{16}$ (48bit)
Round 16
F
$IP^{-1}$
Ciphertext (64bit)
Key (56bit)
$PC_{-1}$
Rot
Rot
Round 1
$PC_{-2}$
Rot
Rot
Round 2
$PC_{-2}$
Rot
Rot
Round 16
$PC_{-2}$
Key Schedule

# Algorithm for Attack

Measurement (3000)

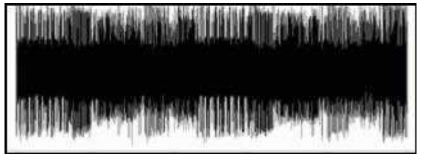


Distribution function

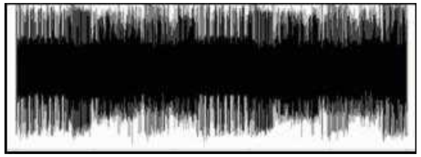
D( Ci, Ks) ∊ {0, 1}: Reference value in ciphertext Ci
Partial key candidate Ks

Distribution & average

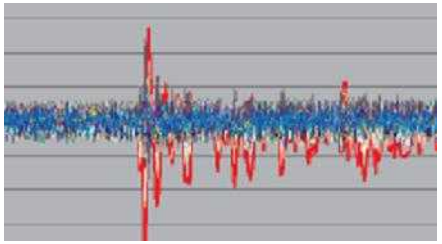
D(Ci,Ks) = 0



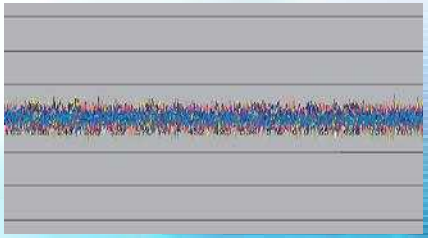
D(Ci,Ks) = 1



Difference

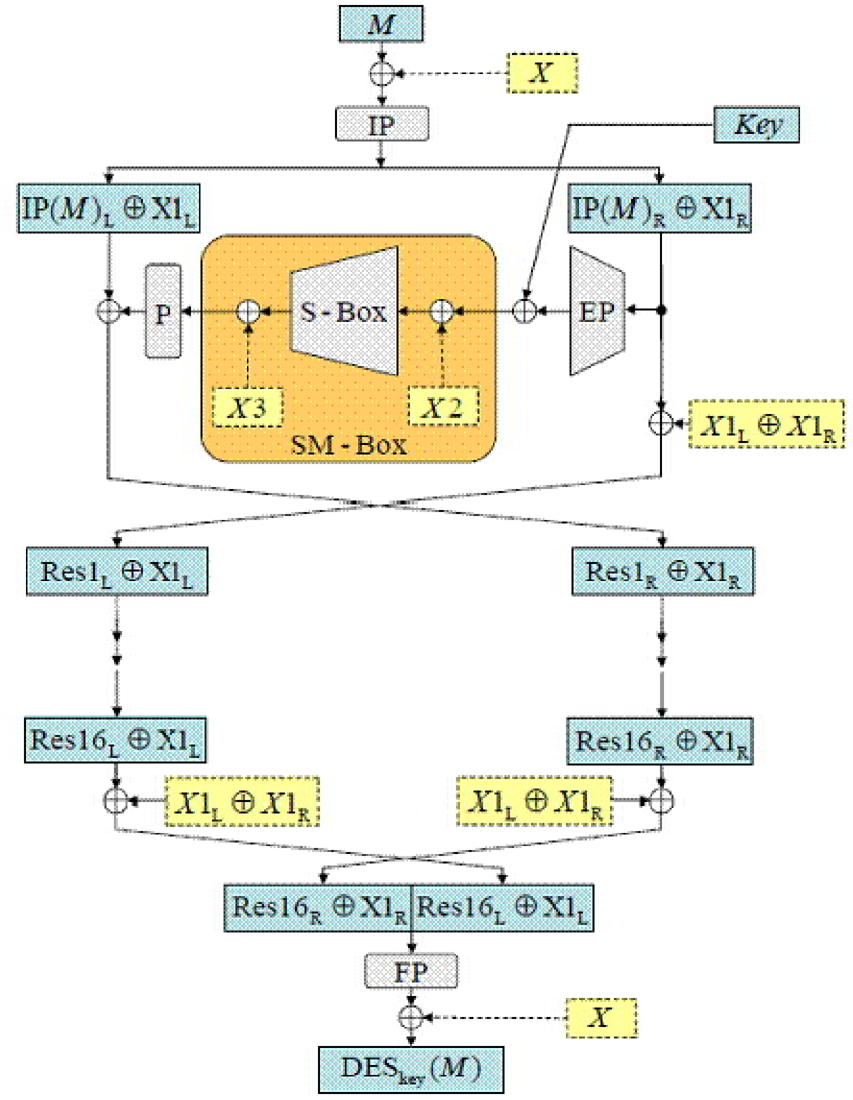


OK



NG

# If anti-DPA technique by Akkar et al. is taken


$M$
$X$
IP
$Key$
$\mathrm{IP}(M)_L \oplus X1_L$
$\mathrm{IP}(M)_R \oplus X1_R$
P
S-Box
EP
$X3$
$X2$
SM-Box
$X1_L \oplus X1_R$
$\mathrm{Res1}_L \oplus X1_L$
$\mathrm{Res1}_R \oplus X1_R$
$\mathrm{Res16}_L \oplus X1_L$
$\mathrm{Res16}_R \oplus X1_R$
$X1_L \oplus X1_R$
$X1_L \oplus X1_R$
$\mathrm{Res16}_R \oplus X1_R$
$\mathrm{Res16}_L \oplus X1_L$
FP
$X$
$\mathrm{DES}_{key}(M)$

As an anti-DPA technique, Akkar and Giraud proposed calculating the data masked with random numbers etc.

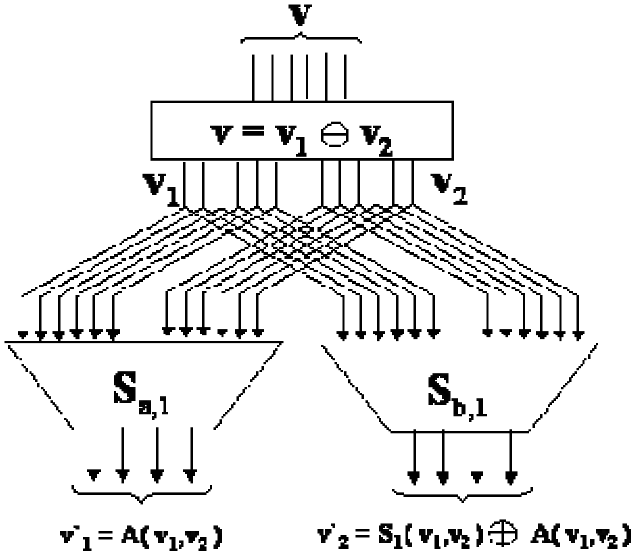
.

All the intermediate data are masked during calculation, and attackers cannot obtain correct intermediate data, unless they know the random numbers for masking.

# If anti-DPA technique by Goubin et al. is taken

## Improvement in algorithm

Improvements were made to DES algorithm to ensure that attackers cannot derive information, even if they make DPA on the weak points of DES, including the period of time during which S-box calculation is in process.



$$v = v_1 \oplus v_2$$
$$v' = S_1(v) = S_{a,1}(v_1,v_2) \oplus S_{b,1}(v_1,v_2)$$

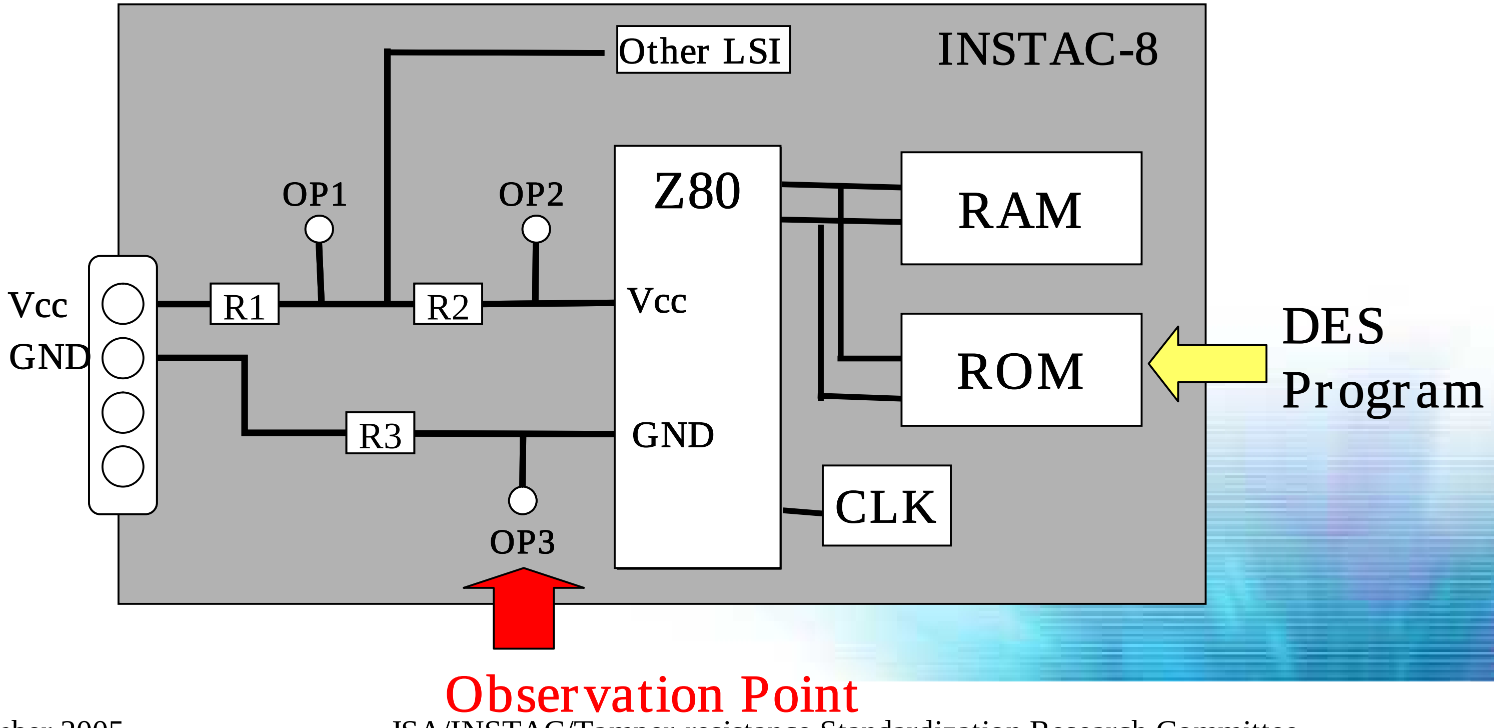
Normal input v is divided randomly, to generate $v_1$ and $v_2$, which fulfill $v = v_1$ xor $v_2$. Then, $v_1$ and $v_2$ are input to $S_{a,i}$ and $S_{b,i}$, respectively, for S-box calculation.

⇩

This process makes it impossible for attackers to classify samples, because they cannot obtain the output from $S_{a,i}$ and $S_{b,i}$.

# Testing Bench

- Platform : INSTAC-8 compliant platform
- Algorithm : DES (Block Cipher)
- Attack : DPA (Differential Power Analysis)

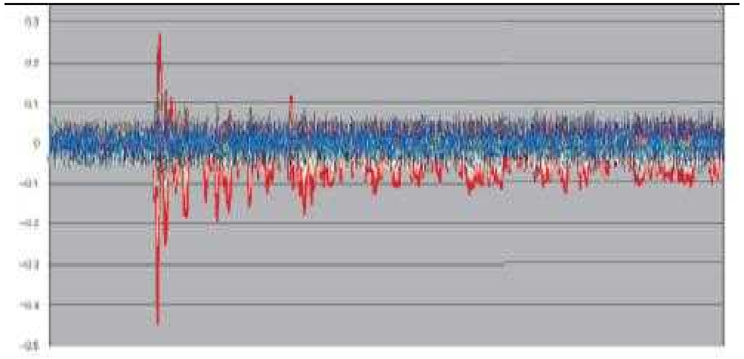


# Attack result

Condition
Time: 1ms
Resolution: 500MSample/Sec
Number of wave form: 3000

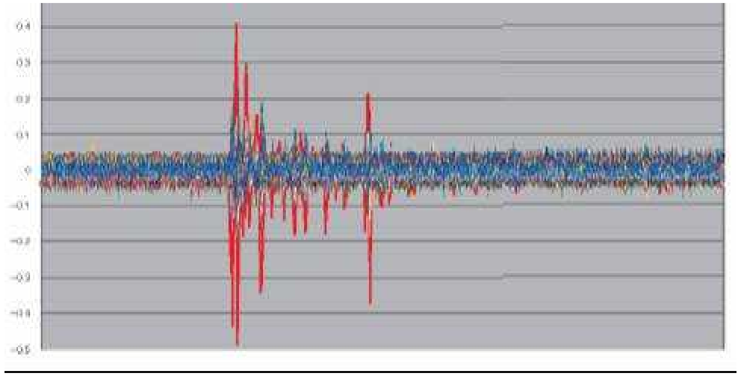
- Without Countermeasure for DPA

## Case of L15



| bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Decision | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| bit | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Decision | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| bit | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| Decision | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| bit | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Decision | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

## Case of F16



| bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Decision | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| bit | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Decision | ○ | ○ | ○ | ○ | ○ | ○ | × | × |
| bit | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| Decision | ○ | ○ | × | ○ | ○ | × | × | ○ |
| bit | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Decision | ○ | ○ | ○ | × | ○ | × | ○ | ○ |

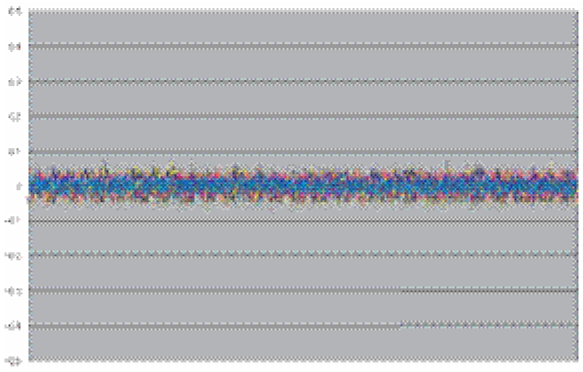
DPA on DES

# Attack result

Condition
Time: 1ms
Resolution: 500MSample/Sec
Number of wave form: 3000

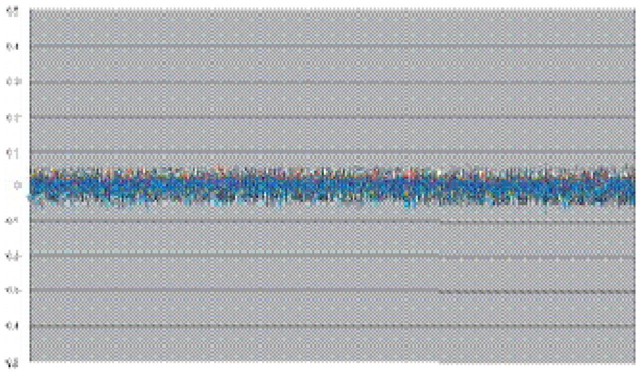
- With Countermeasure Proposed by Akkar and Giraud

## Case of L15



| bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Decision | × | × | × | × | × | × | × | × |
| bit | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Decision | × | × | × | × | × | × | × | × |
| bit | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| Decision | × | × | × | × | × | × | × | × |
| bit | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Decision | × | × | × | × | × | × | × | × |

## Case of F16



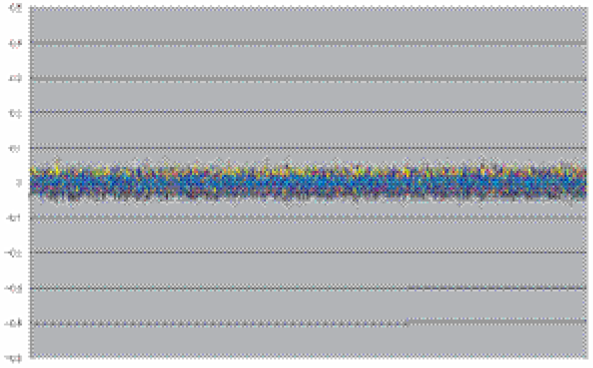
| bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Decision | × | × | × | × | × | × | × | × |
| bit | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Decision | × | × | × | × | × | × | × | × |
| bit | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| Decision | × | × | × | × | × | × | × | ○ |
| bit | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Decision | × | × | × | × | × | × | × | × |

# Attack result

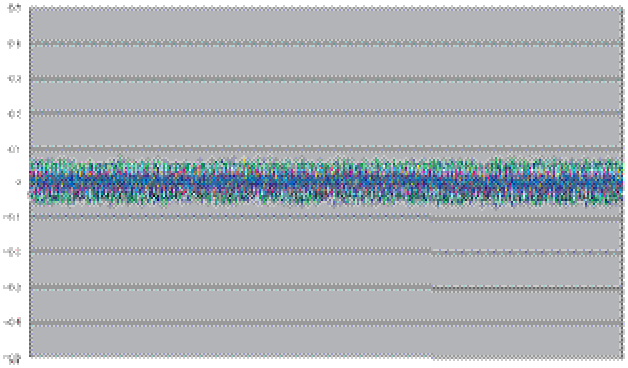
Condition
Time: 1ms
Resolution: 500MSample/Sec
Number of wave form: 3000

- With Countermeasure Proposed by Goubin and Patarin

Case of L15



Case of F16



| bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Decision | × | × | × | × | × | × | × | × |
| bit | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Decision | × | × | × | × | × | × | × | ○ |
| bit | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| Decision | × | × | × | × | × | × | × | × |
| bit | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Decision | × | × | × | × | × | × | × | × |

| bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Decision | × | × | × | × | × | × | × | × |
| bit | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Decision | × | × | × | × | × | × | × | × |
| bit | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| Decision | × | × | × | × | × | × | × | × |
| bit | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Decision | × | × | × | × | × | × | × | × |

# Conclusion

- ➢ DPA was conducted on the following three DES algorithm implemented on INSTAC-8
  - ✓ Without Countermeasure
  - ✓ With Countermeasure to DPA
    - - One proposed by Akkar and Giraud (CHES2001)
    - - One proposed by Goubin and Patarin (CHES1999)

- ➢ By 3000 wavy measurements, attackers could obtain secret key of DES without countermeasure to DPA at the success rate of 100% and 75% in L15 case and F16 case, respectively.

- ➢ It was confirmed that the countermeasures proposed by Akkar and Goubin are effective to DPA on INSTAC-8.

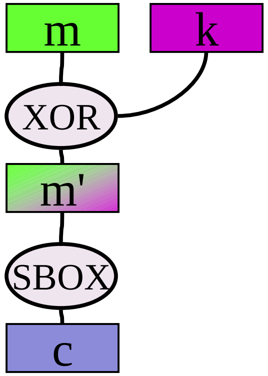
# Outline of Experimental Attack

- **Purpose:** Study on techniques to obtain implementation information, including hamming weight.
- **Outline:** Linear correlation between hamming weight and voltage changes detected by EMA was found.
- Applied on Mini cipher model (Block Cipher)
- Attack technique: EMA
- Tamper-resistance technique: None

# Algorithm

Code of mini cipher model

```
7:   XOR  A,(HL)     ; Load from HL and XOR with A
4:   LD   C,A        ; Move A to register C
7:   LD   A,(BC)     ; Load from BC and move to A
4:   LD   C,A        ; Move A to register C
```



Execution : Execute mini cipher model while Input m and key k are changed from 0 to 255

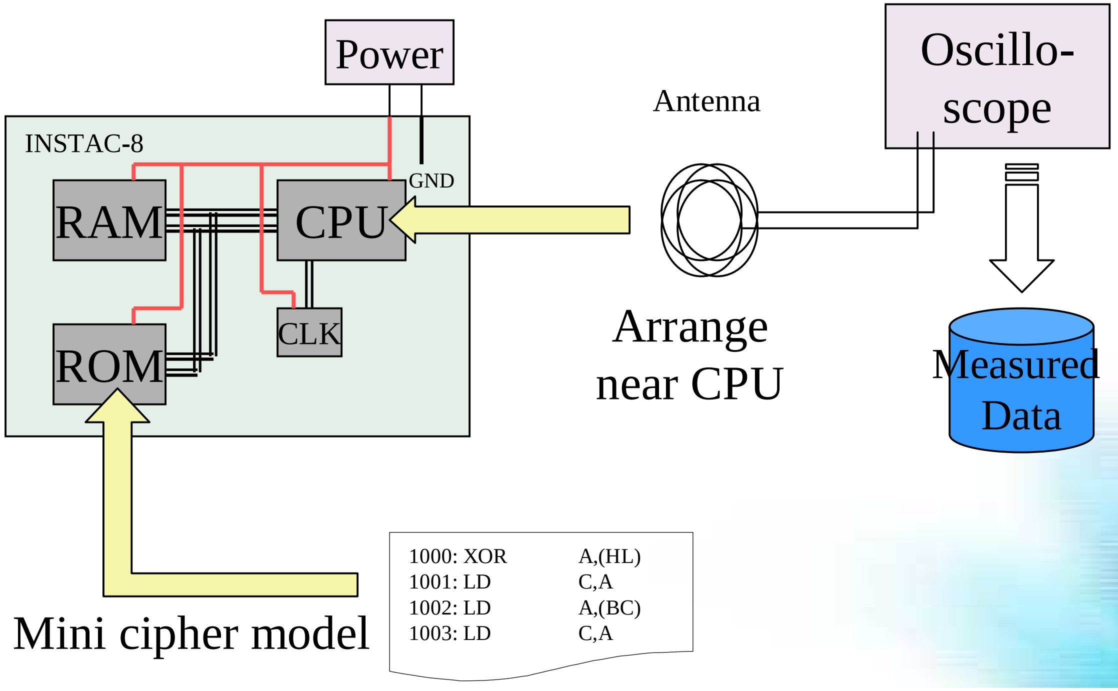
```
for A=0..255 do begin
     for (*HL) = 0..255 do begin
        mini cipher model
 end;
```

- Repeat the above-mentioned processing six times and obtain 256*256*6 data.

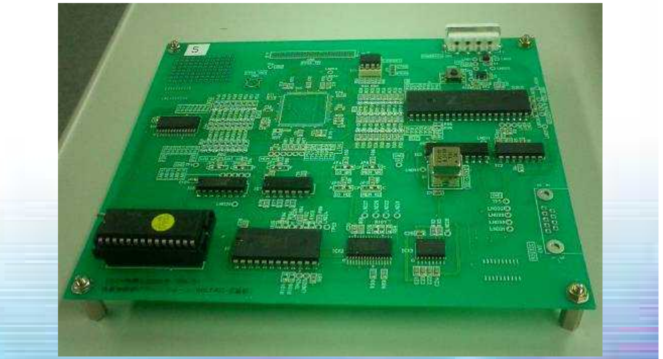
EMA on Mini cipher model

# Testing Bench

- Platform : INSTAC-8 compliant platform
- Algorithm : Mini cipher model (Block Cipher)
- Attack : EMA (ElectroMagnetic Analysis )



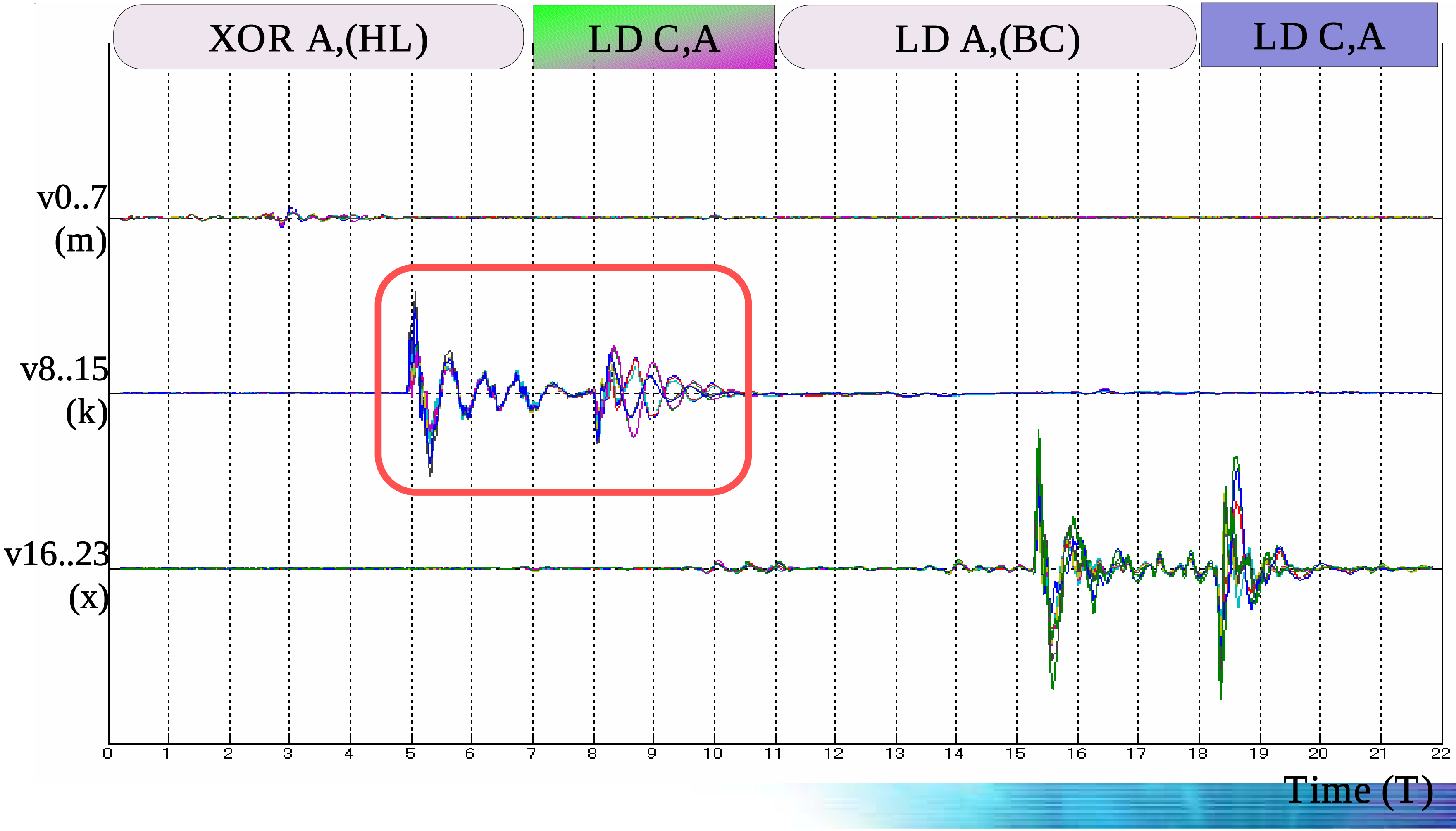
```
1000: XOR     A,(HL)
1001: LD      C,A
1002: LD      A,(BC)
1003: LD      C,A
```



EMA on Mini cipher model

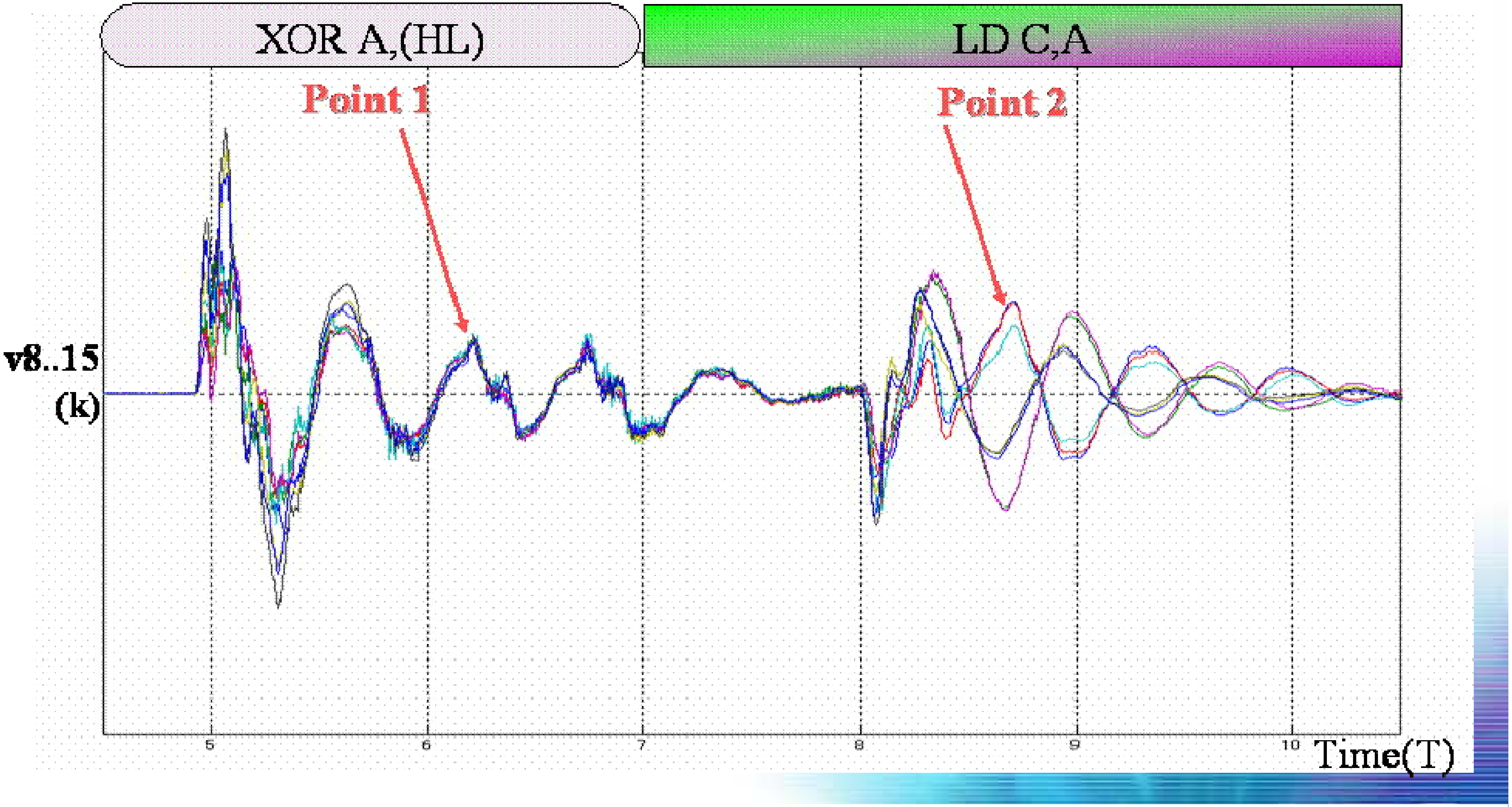
# Measured Data

- The whole of difference graph (T=0 ~ 22)



# Measured Data

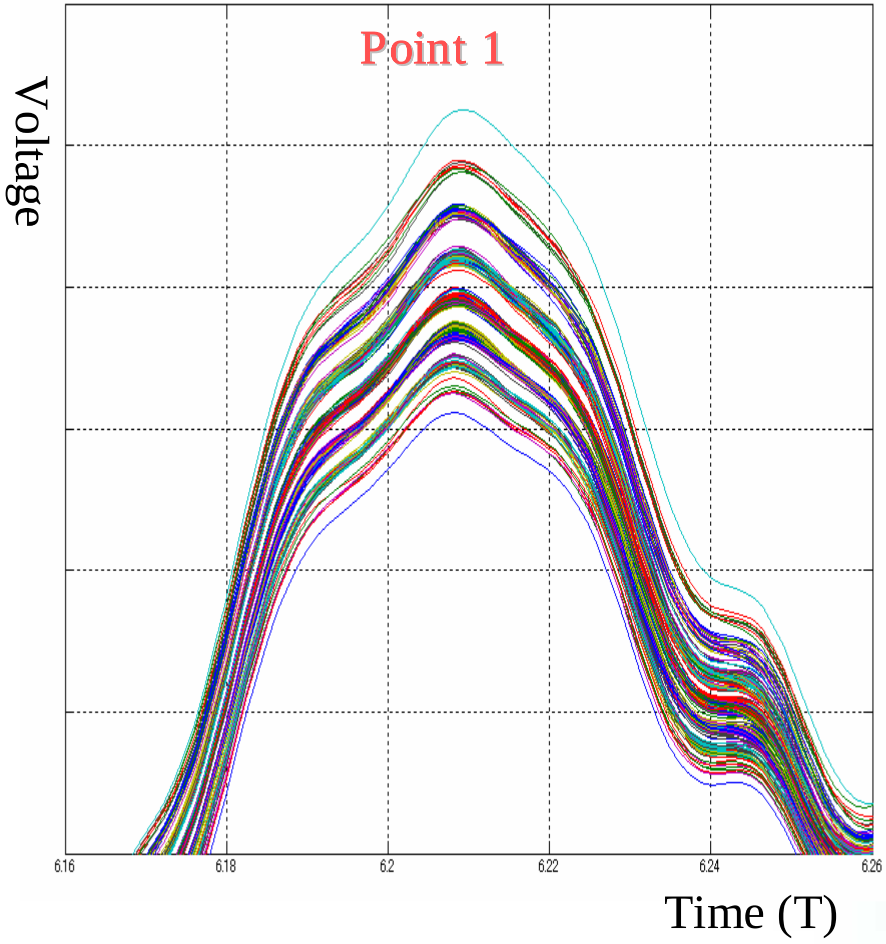
- The difference graph about k (T=5 ~ 10)

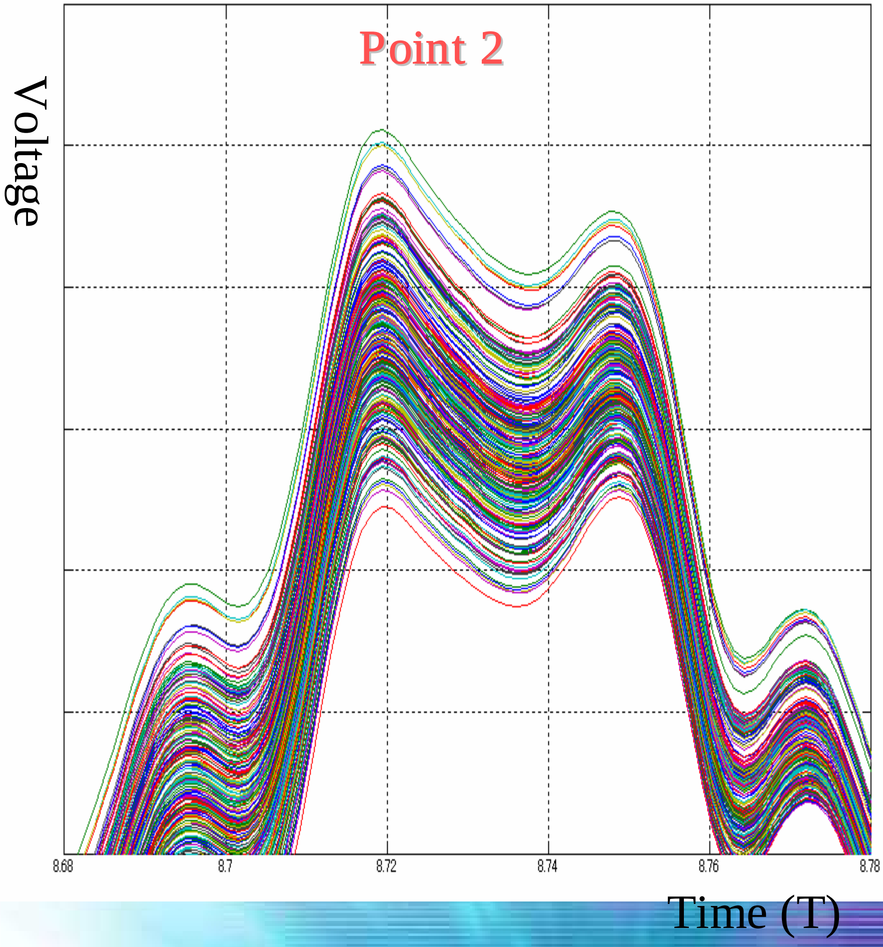


EMA on Mini cipher model

# Measured Data

- ➢ Wave forms at point 1 and 2 (grouped by the value of k and its average) $g_{s_k} := \sum_{n} (w_{w_n,i}) / \sum_{n} (1)$

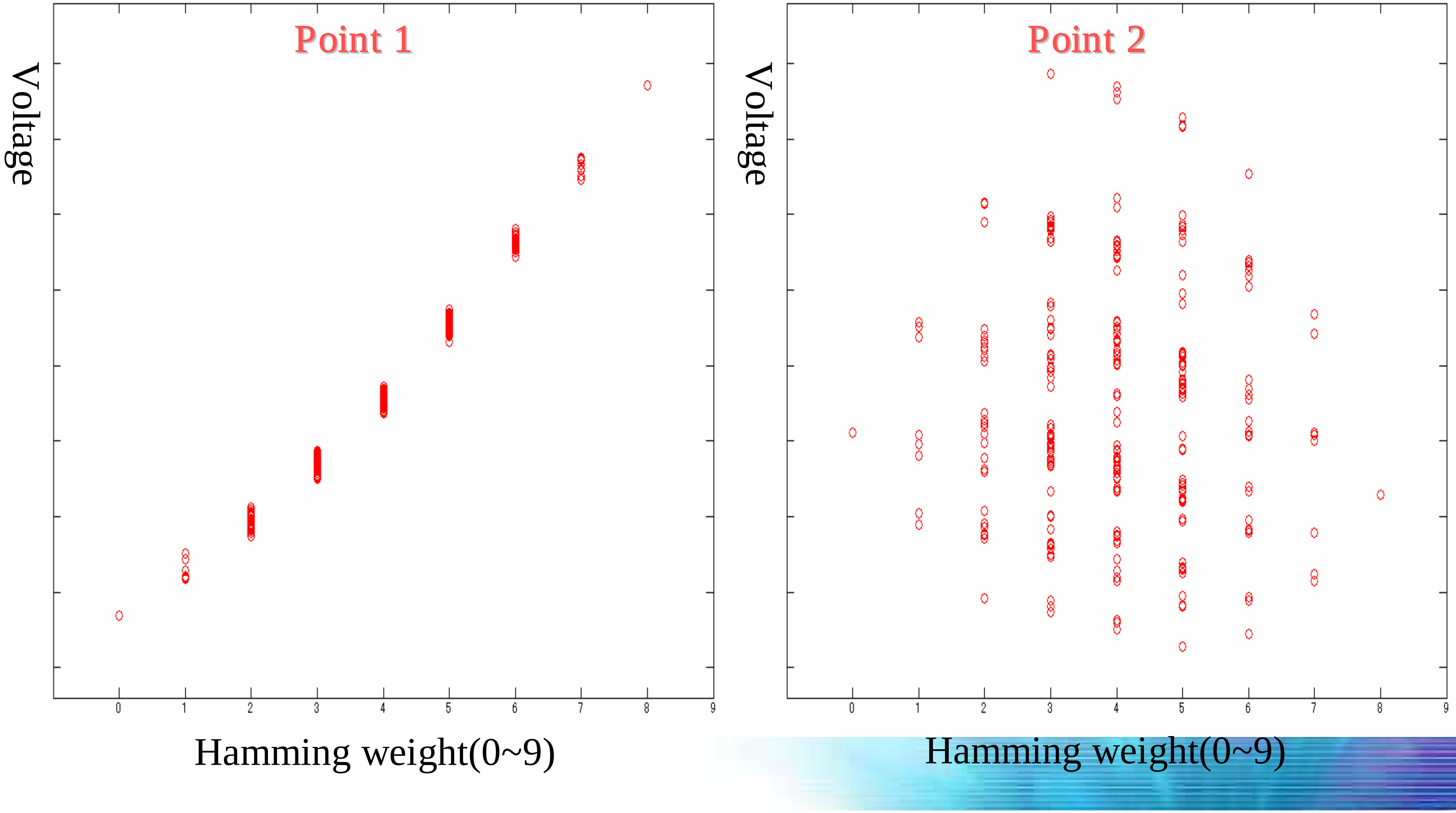




EMA on Mini cipher model

# Measurement data

- The relation ship between the waveforms and hamming weight of data



# Conclusion

- The way of obtaining information about implementation necessary for the analysis was examined.
- The section where information of the hamming weight etc. appear was specified by installing mini cipher model on INSTAC-8 and analyzing the measured data.

# Outline of Experimental Attack

- **Purpose:** To examine the effectiveness of proposed attack technique against A5/1
- **Outline:** Information necessary for the cryptanalysis was estimated, based on power consumption data, to verify the effectiveness of the attack technique.
- Applied on A5/1 (Stream Cipher)
- Attack technique: SPA
- Tamper-resistance technique: None

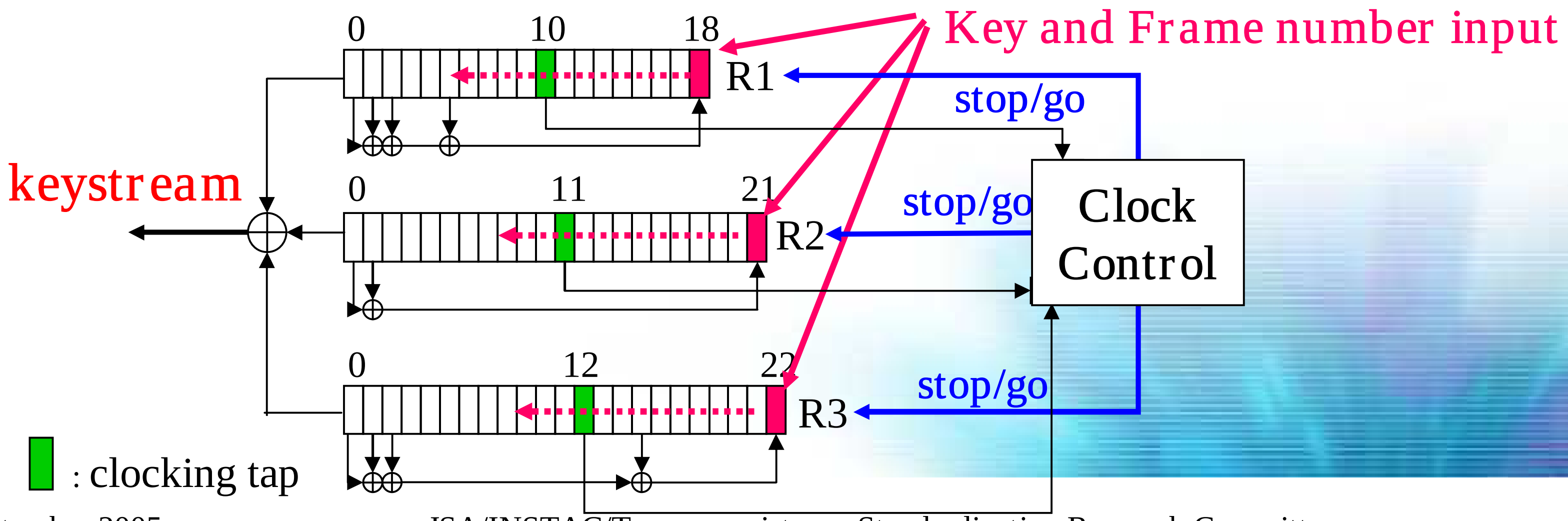
# Algorithm : A5/1

1. All 3 registers are zeroed
2. 64 cycles (without the stop/go clock):
   Each bit of Key is XORed and put into the LSB of the register
3. 22cycles(without the stop/go clock):
   Each bit of Frame number is XORed and put into the LSB of the register
4. 100 cycles with the stop/go clock control, discarding the output

} Keysetup

5. 228 cycles with the stop/go clock control which produce the output bit sequence
   → We use this operation for attack

} Run

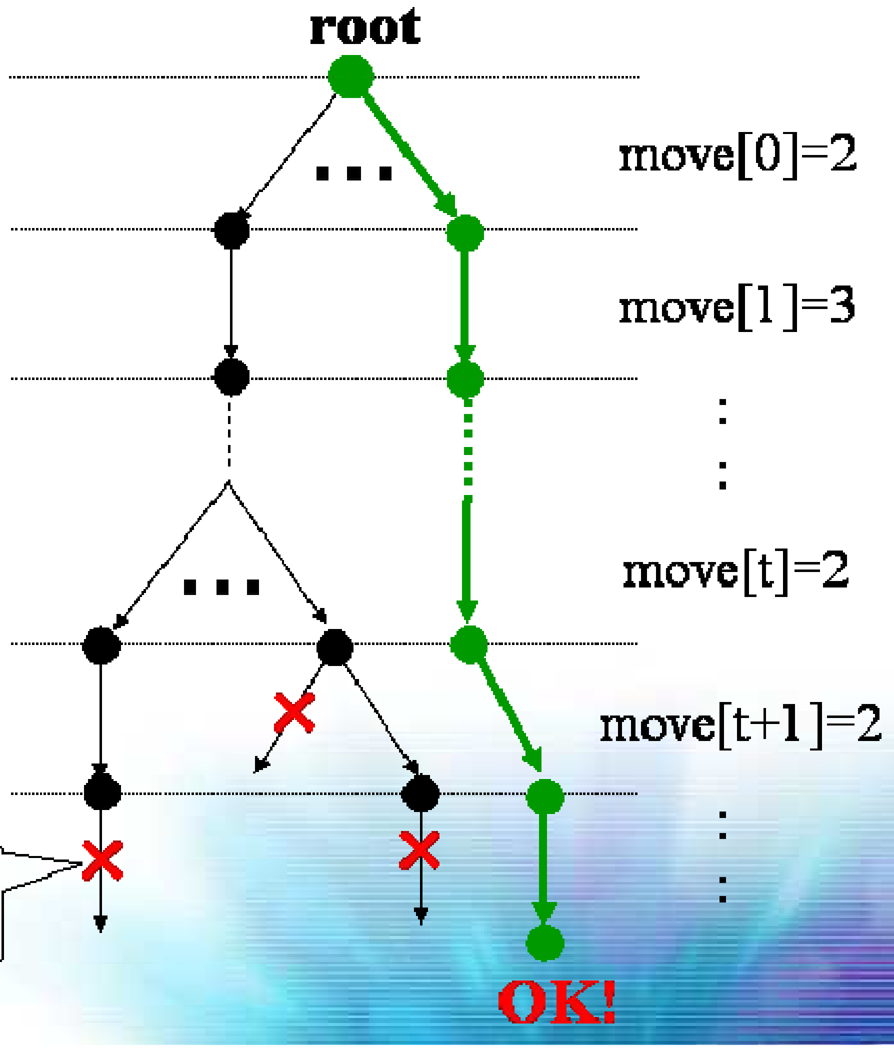


# Algorithm for Attack : A5/1

Input: Key stream
Frame number
move information

Output: 64-bit Key

Operation: Tree search algorithm
(depth-first search )
each of nodes are clocking
tap value at each time t



Contradiction check by key stream

# Computation Costs for Attack : A5/1

- Before contradiction check by key stream

$$(2\times\frac{1}{4}+6\times\frac{3}{4})\times 3^{\frac{14\times 9}{16}}\times 1^{\frac{14\times 3}{16}}\times 6^{\frac{14\times 3}{16}}\times 2^{\frac{14\times 1}{16}}\approx 2^{22.46}$$

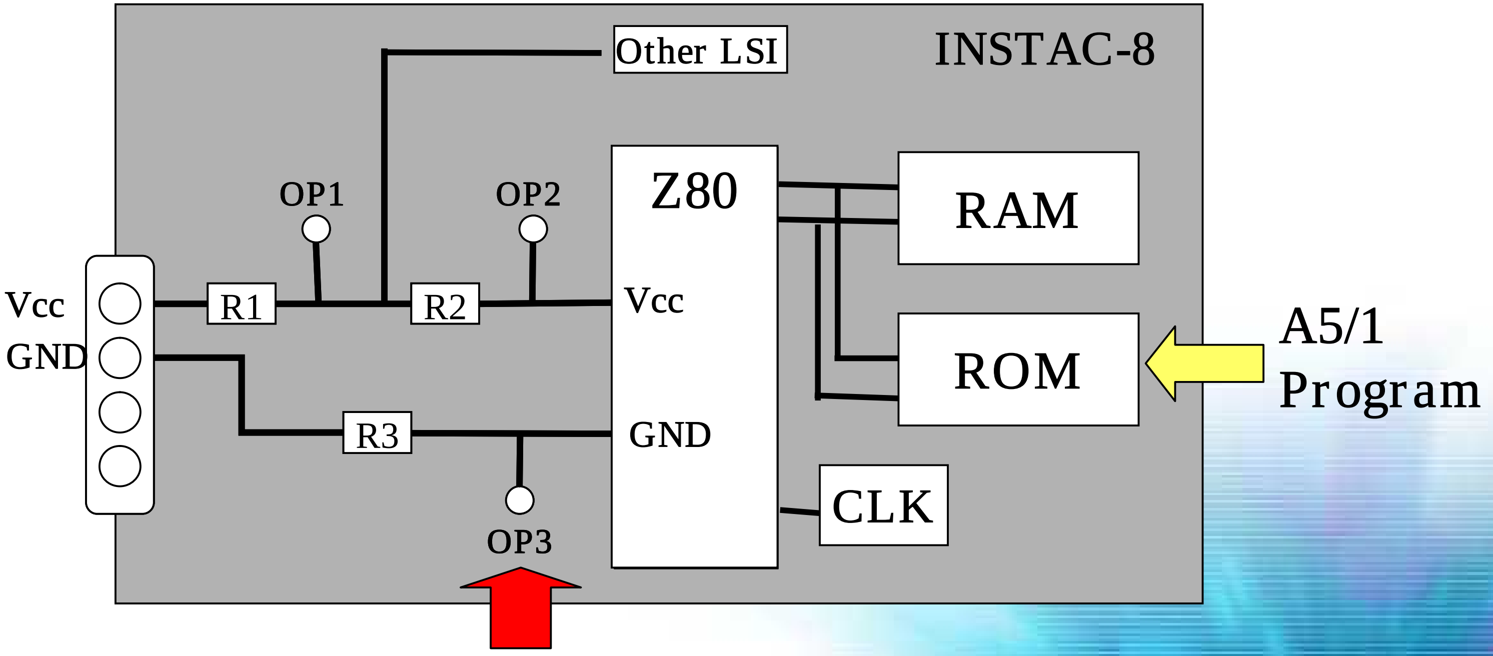
- The maximum width of the search tree

$$2^{22.46}\times(\frac{3}{2})^{\frac{15\times 9}{16}}\times(\frac{1}{2})^{\frac{15\times 3}{16}}\times(\frac{6}{2})^{\frac{15\times 3}{16}}\times(\frac{2}{2})^{\frac{15\times 1}{16}}\approx 2^{29.04}$$

- The maximum width of the search tree by experiment: $2^{26.84}$
- Computation time : 13.2min (Pentium4, 2.0GHz)
- Key stream, move information: 47 bit

# Testing Bench

- Platform : INSTAC-8 compliant platform
- Algorithm : A5/1(Stream Cipher)
- Attack : SPA (Simple Power Analysis)



Observation Point

# Functions of A5/1 (Only Run state)

| Operation | clock | Time (ms) |
|---|---|---|
| Run | 6464440 | 808.06 |
| Clock (move=2/3) | 27852 / 34419 | 3.48 / 4.20 |
| Majority | 4355 | 0.54 |
| Clockone | 7772 | 0.97 |
| Parity | 5978 | 0.75 |
| Getbit | 6814 | 0.85 |

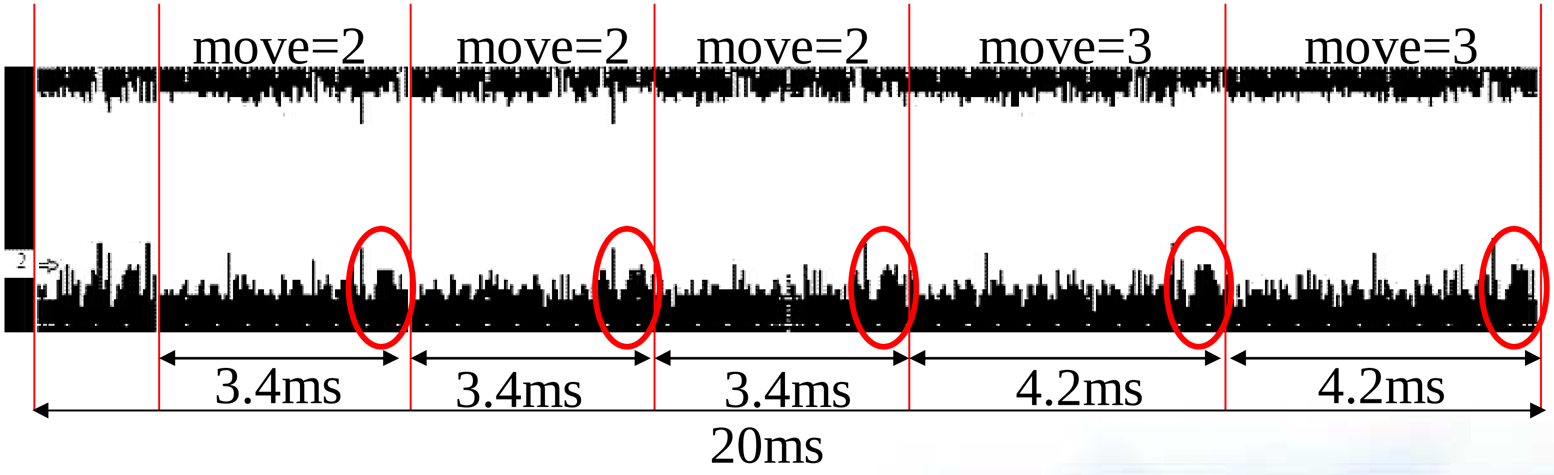
A5/1 program: http://cryptome.org/gsm-a512.htm

SPA on A5/1

# Characteristic Power Wave Form Pattern

Condition

| | |
|---|---|
| Time: | 20ms |
| Resolution: | 1.25GSample/Sec |
| Number of wave form: | 1 |

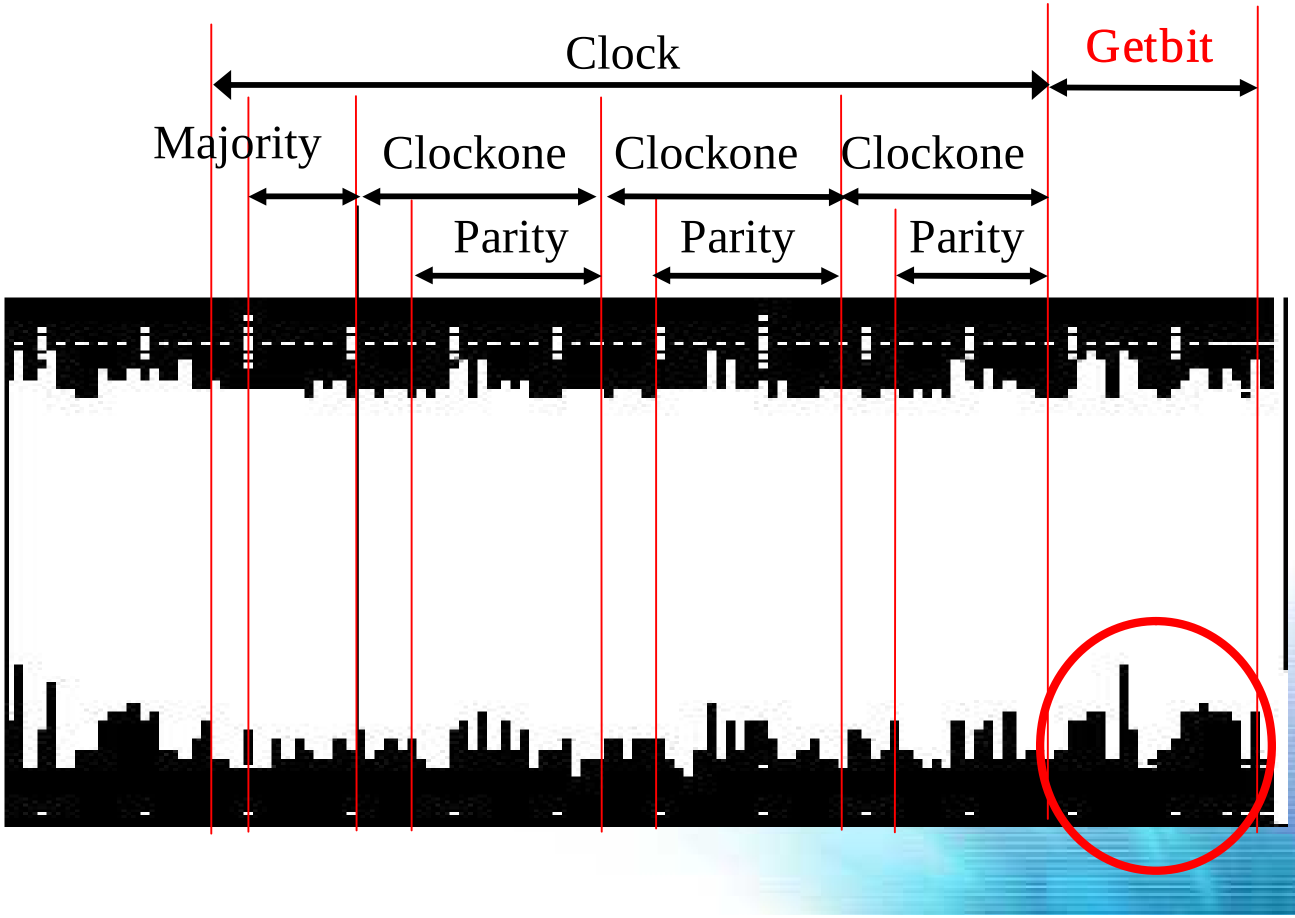


Move information could be obtained from power waveforms.

SPA on A5/1

# The Characteristic is Getbit

| Condition | |
|---|---|
| Time: | 20ms |
| Resolution: | 1.25GSample/Sec |
| Number of wave form: | 1 |



# Conclusion : A5/1

- A side channel attack was performed against A5/1
  - Condition: Attackers can obtain the number of LFSRs which shift at each time, based on side channel information
  - The maximum width of the search tree : $2^{26.84}$
  - Computation time: 13.2min (Pentium 4, 2.0GHz)
  - Side channel information: 47 bit (1 frame)
- It was confirmed that attackers can obtain the number of shifted LFSRs from power consumption waveforms detected by INSTAC-8.

# Conclusion

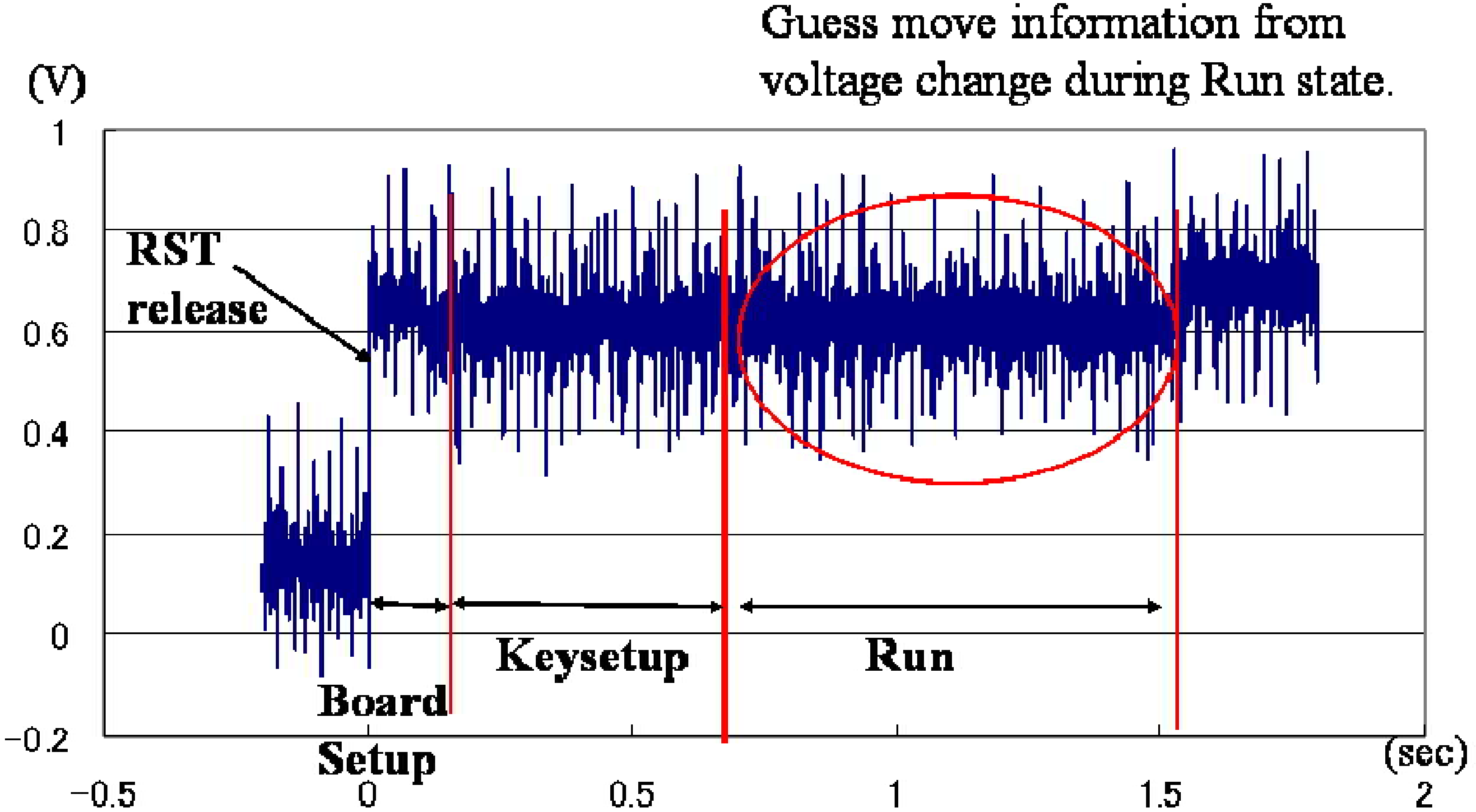
- Three kinds of side channel attack were performed against ciphers implemented on evaluation platform, INSTAC-8

- For DES, the effectiveness of existing DPA and counter-measures to it was demonstrated. The effectiveness of the new attacks, SPA against A5/1 and EMA against the mini cipher model, were also shown.

- The key was recovered successfully by each of the three kinds of attacks at high success rate. This shows that INSTAC-8 is an effective platform for evaluating attacks and their countermeasures.

Thank you.

# Outline of experiment : A5/1


Guess move information from
voltage change during Run state.
(V)
RST
release
Board
Setup
Keysetup
Run
(sec)