TOHOKU UNIVERSITY

GSIS
Graduate School of Information Sciences,
TOHOKU University

Fourth International Workshop on
Constructive Side-Channel Analysis and Secure Design (COSADE 2013)

Chosen-IV Correlation Power Analysis on KCipher-2 and a Countermeasure

Takafumi Hibiki*, Naofumi Homma*, Yuto Nakano†,
Kazuhide Fukushima†, Shinsaku Kiyomoto†,
Yutaka Miyake†, and Takafumi Aoki*

*Tohoku University, Japan
†KDDI R&D Laboratories, Inc., Japan

Introduction

- KCipher-2
  - ISO/IEC 18033-4 standard stream cipher
  - High throughput for encryption/decryption and high security against theoretical attacks
    - Dynamic Feedback Control (DFC) mechanism
      - Two FSRs (Feedback Shift Registers) with 32-bit word lengths similar to the SNOW2.0
    - Finite State Machine (FSM)
      - 32-bit integer addition
      - S-box and Permutation (S-box and Mixcolumns of AES)

Security evaluation against side-channel attacks has just begun

Side-channel attacks on KCipher-2

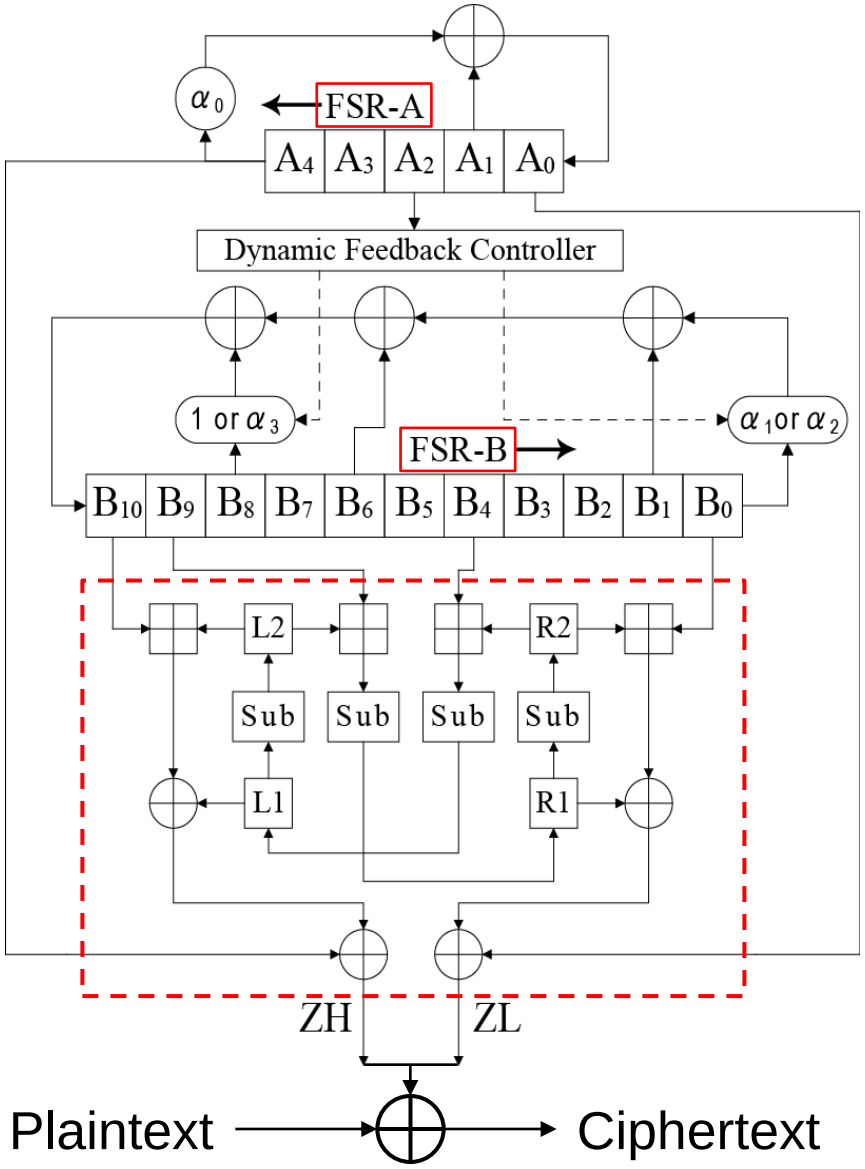
- Power Analysis on KCipher-2 [Henricksen]
  - Possibility of revealing only a 32-bit partial key out of 128-bit initial key
    - Previous study does not discuss any detailed attack scenario
  - Complexity to reveal the entire initial key: 2^{96}
    - It seems not to be a real threat
- Our contribution
  - Chosen Initial-Vector (IV) CPA on KCipher-2
    - Complexity to reveal the entire initial key: 2^{32}
  - Countermeasure based on random masking
    - Resistant to the above attack

[Henricksen] M. Henricksen, ACISP2010.

Outline

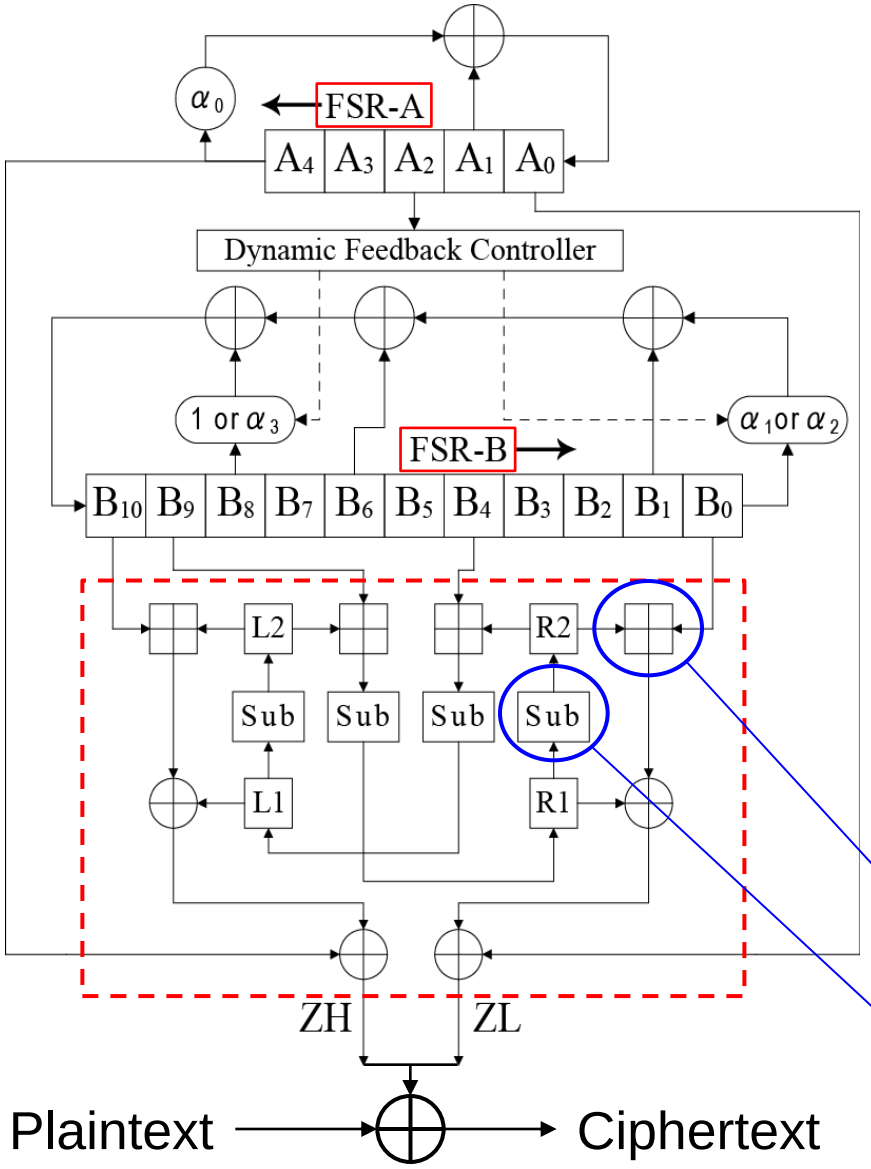
- Background
- KCipher-2
- Chosen-IV CPA on KCipher-2
- Countermeasure based on random masking
- Conclusions and future works

KCipher-2



- Input
  - 128-bit Initial Key (IK)
  - 128-bit Initial Vector (IV)
- Initialization process
  - Key loading step
  - Internal state initialization step (24 clock)
- Keystream output process
  - 64-bit keystream/cycle

KCipher-2

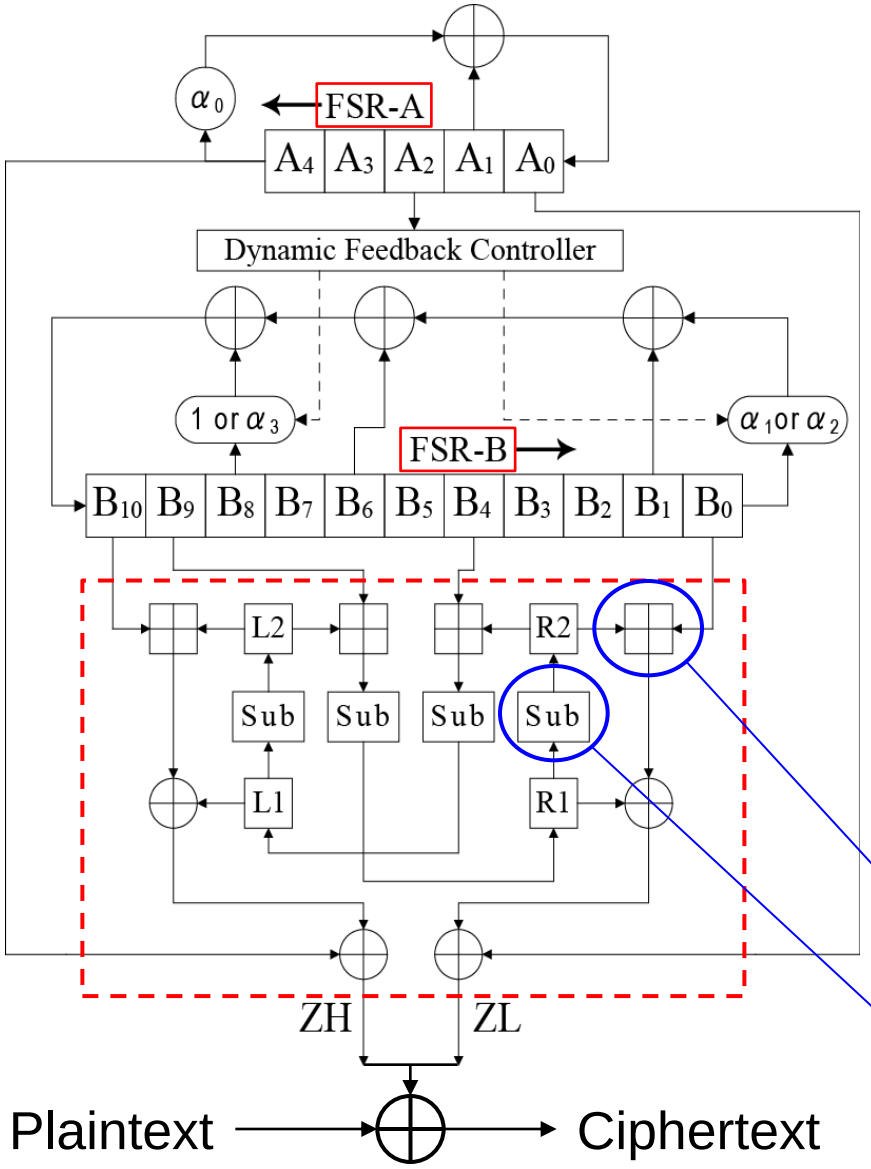


- Input
  - 128-bit Initial Key (IK)
  - 128-bit Initial Vector (IV)
- Initialization process
  - Key loading step
  - Internal state initialization step (24 clock)
- Keystream output process
  - 64-bit keystream/cycle

32-bit integer addition

32-bit Sub function
(S-box and Permutation)

KCipher-2



- Input
  - 128-bit Initial Key (IK)
  - 128-bit Initial Vector (IV)
- Initialization process
  - Key loading step
  - Internal state initialization step (24 clock)
- Keystream output process
  - 64-bit keystream/cycle

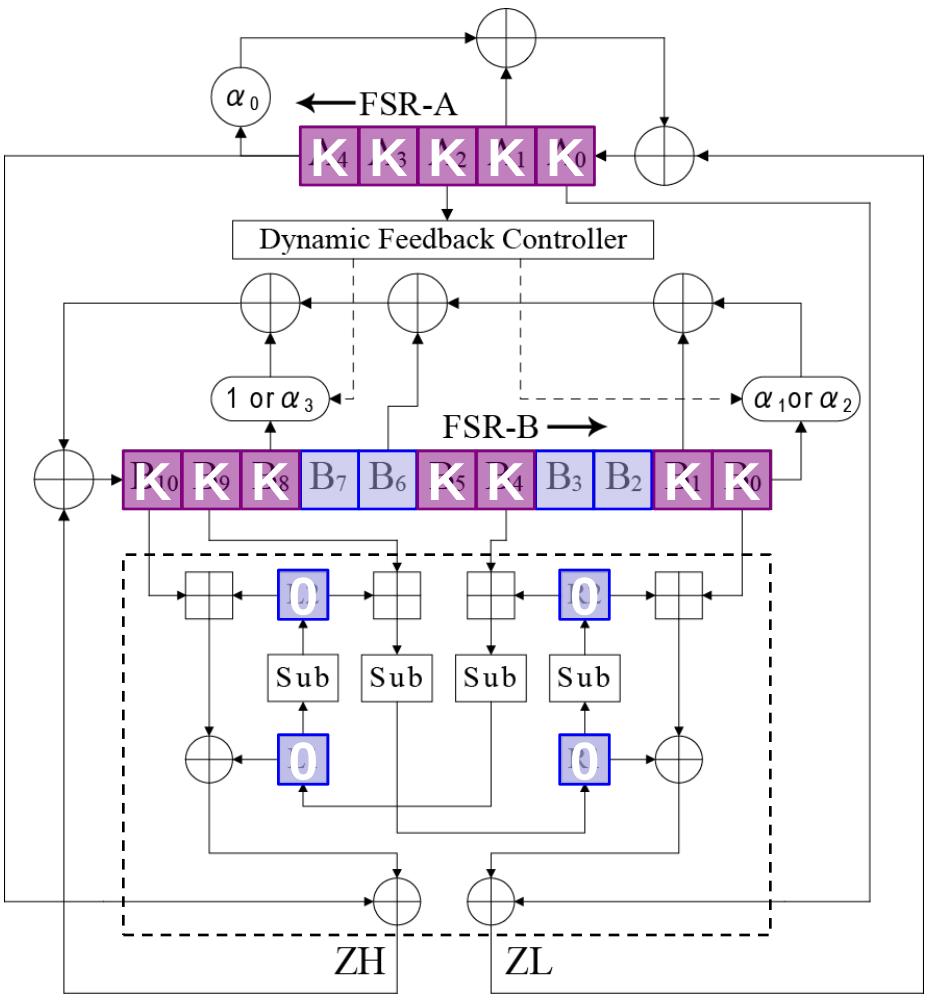
32-bit integer addition

32-bit Sub function
(S-box and Permutation)

Outline of attack to recover 128-bit initial key

- Recover 128-bit initial key from three 32-bit internal keys with a 32-bit brute-force search
  - Proposed CPAs provides three 32-bit internal keys
    - Start by estimating the lowest byte for each 32-bit internal key
    - Use recovered bytes to estimate higher bytes sequentially
    - Complexity: 2^{10} ($=2^8 \times 4$)
  - With 96-bit internal keys revealed, 32-bit partial initial key is recovered by a 32-bit brute-force search
    - Complexity: 2^{32}

Target values used in our CPA



: IV and 0 : 0 Known

K : K (Internal key) Unknown

! : Targetable

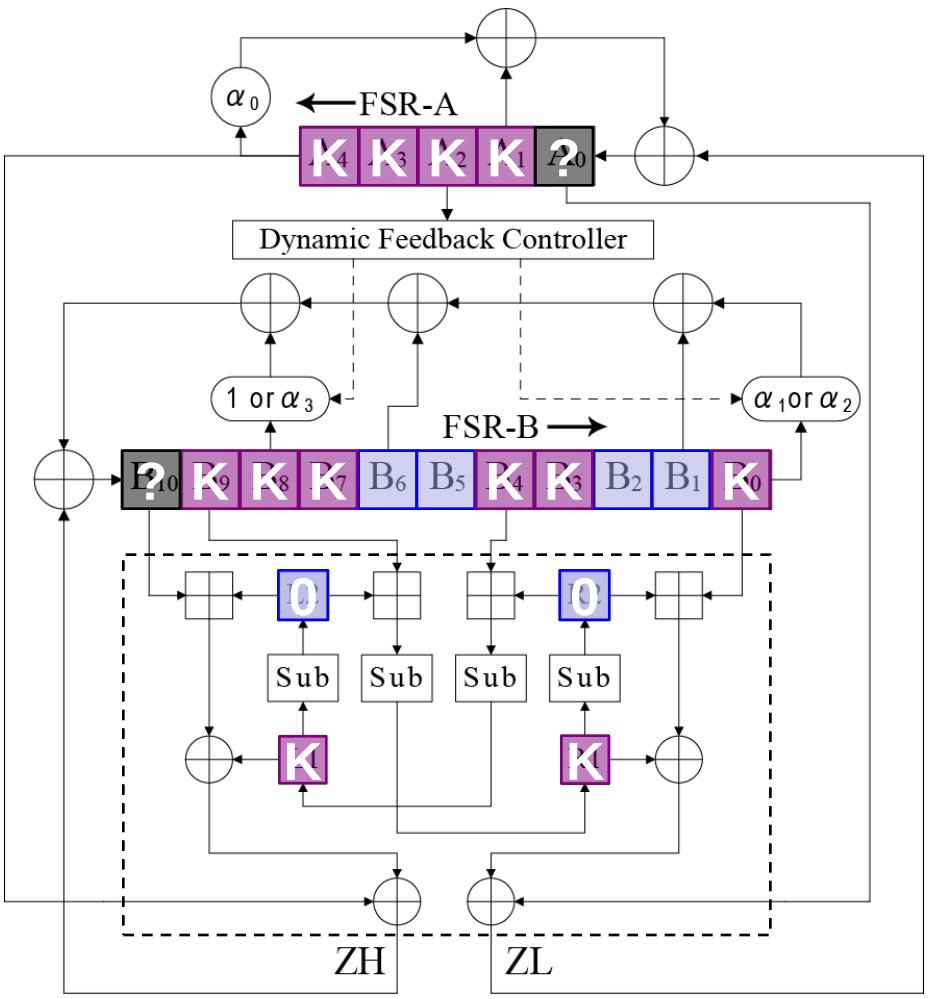
? : Untargetable

Internal state initialization step

Clock 0 (Initial state)

- Initial vector (IV) and Internal key (K) are stored in FSRs
- Registers (L1, L2, R1, R2) are set to be zero.

Target values used in our CPA



: IV and 0 : 0 Known

K : K (Internal key) Unknown

! : Targetable

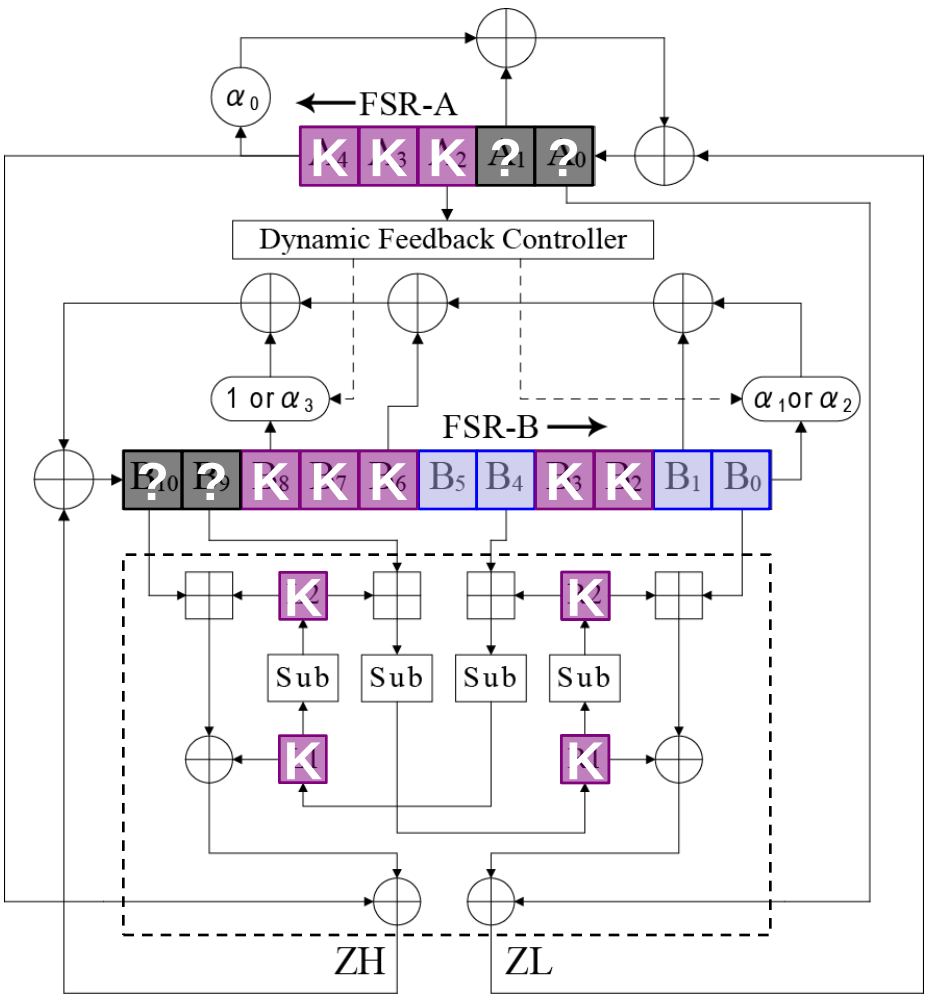
? : Untargetable

Internal state initialization step

Clock 1

- Values given by only internal key or initial vector
- Untargetable values given by more than 64-bit internal keys

Target values used in our CPA



: IV and 0 : 0 Known

K : K (Internal key) Unknown

! : Targetable

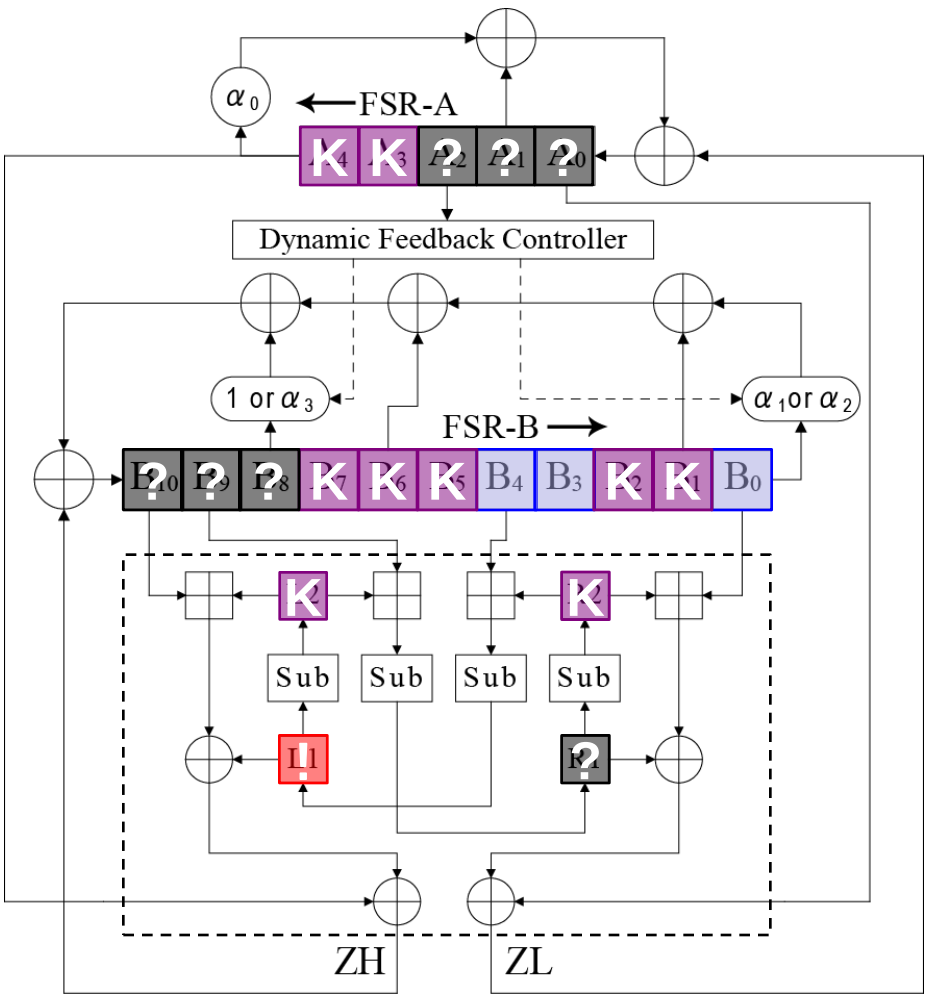
? : Untargetable

Internal state initialization step

Clock 2

- Values given by only internal key or initial vector
- More untargetable values given by more than 64-bit internal keys

Target values used in our CPA



: IV and 0 : 0 Known

K : K (Internal key) Unknown

! : Targetable

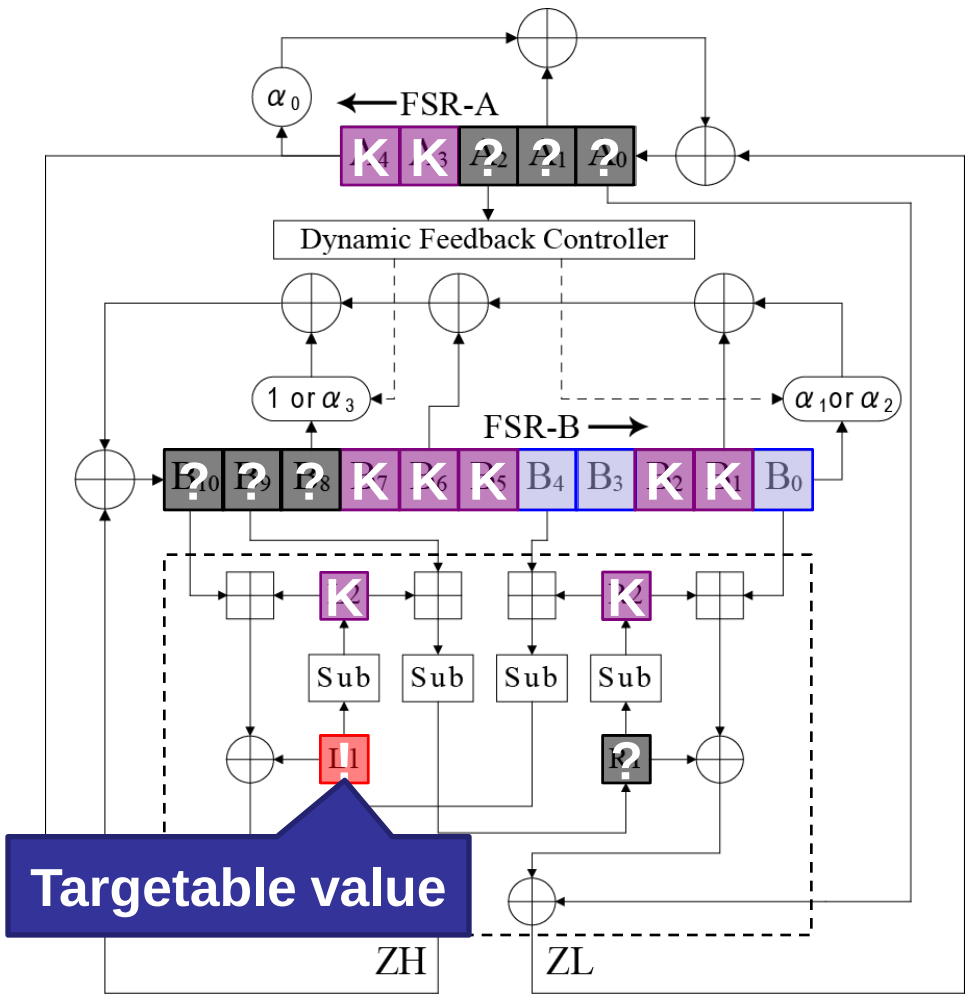
? : Untargetable

Internal state initialization step

Clock 3

- Targetable value given by initial vector and 32-bit internal key
  - Stored in Register L1

Target values used in our CPA



: IV and 0 : 0 Known

K : K (Internal key) Unknown

! : Targetable

? : Untargetable

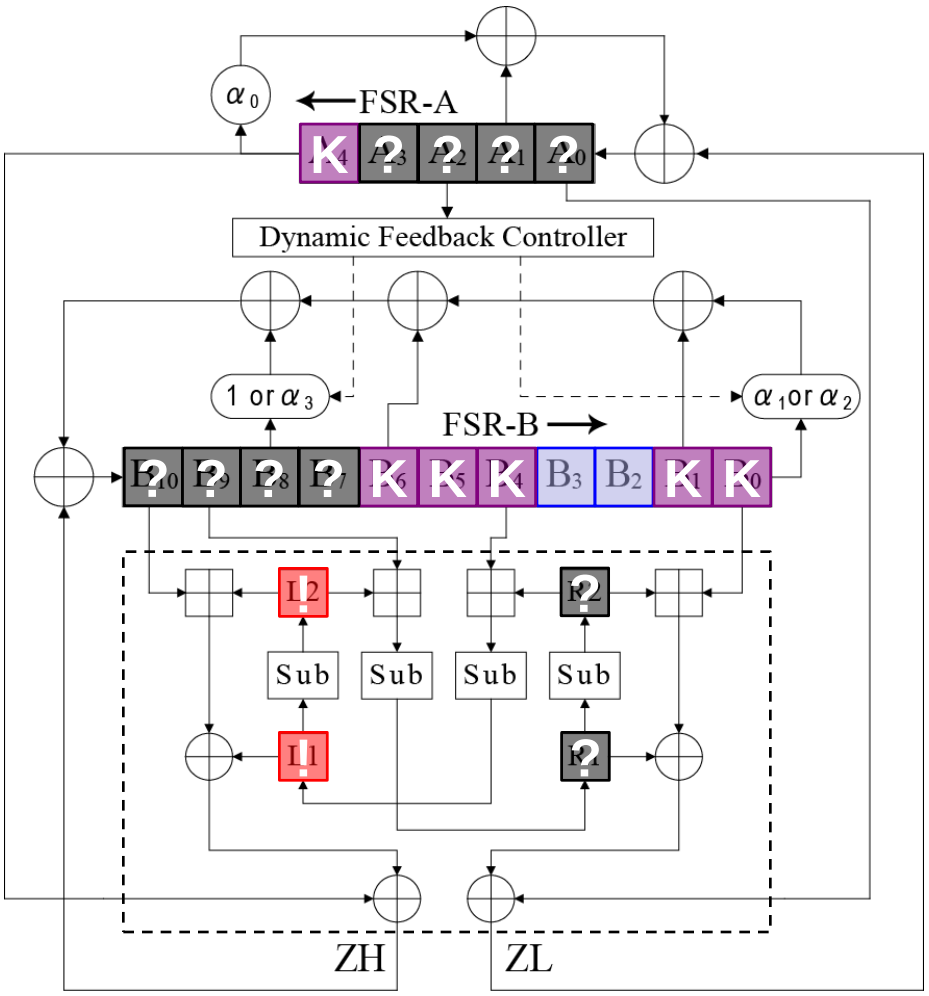
Internal state initialization step

Clock 3

- Targetable value given by initial vector and 32-bit internal key
  - Stored in Register L1

$L1^{(3)}$ = Sub(IV + Sub(Sub(K)))

Target values used in our CPA



: IV and 0 : 0 Known

K : K (Internal key) Unknown

! : Targetable

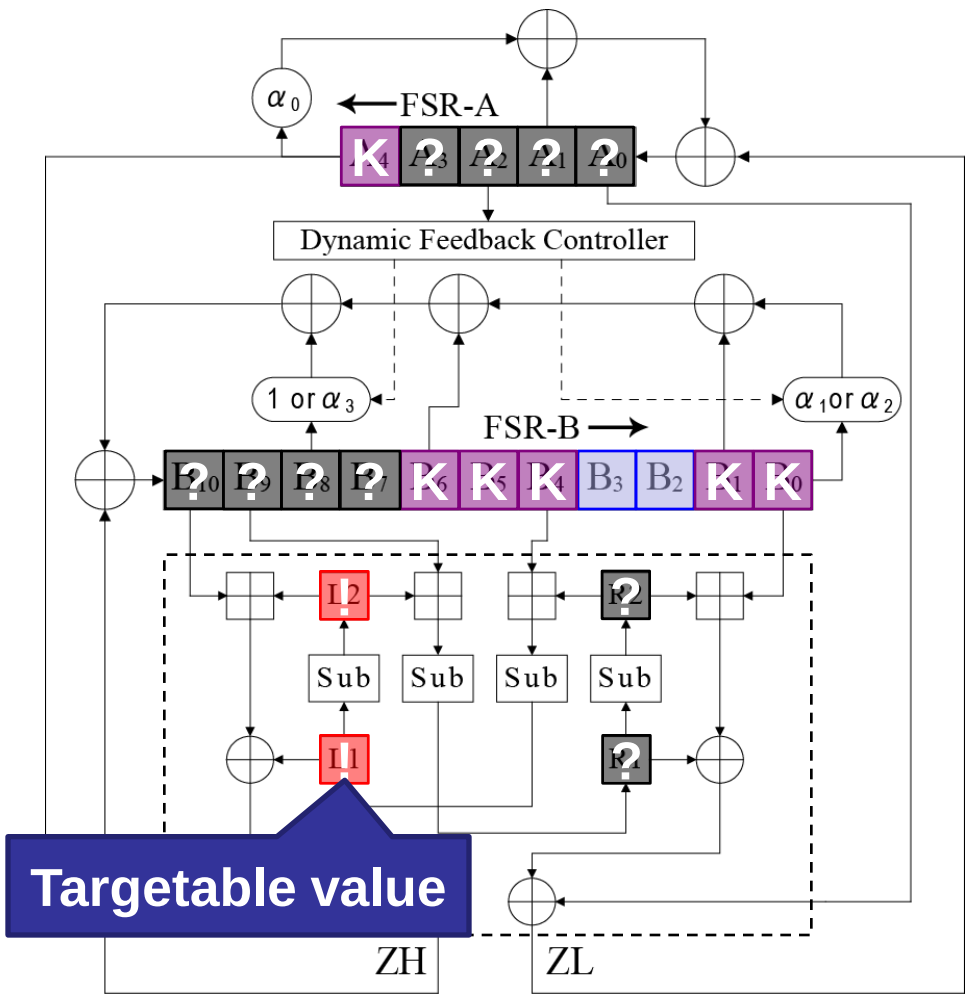
? : Untargetable

Internal state initialization step

Clock 4

- Targetable value given by initial vector and 32-bit internal key
  - Stored in Register L1

Target values used in our CPA



: IV and 0 : 0 Known

K : K (Internal key) Unknown

! : Targetable

? : Untargetable

Internal state initialization step

Clock 4

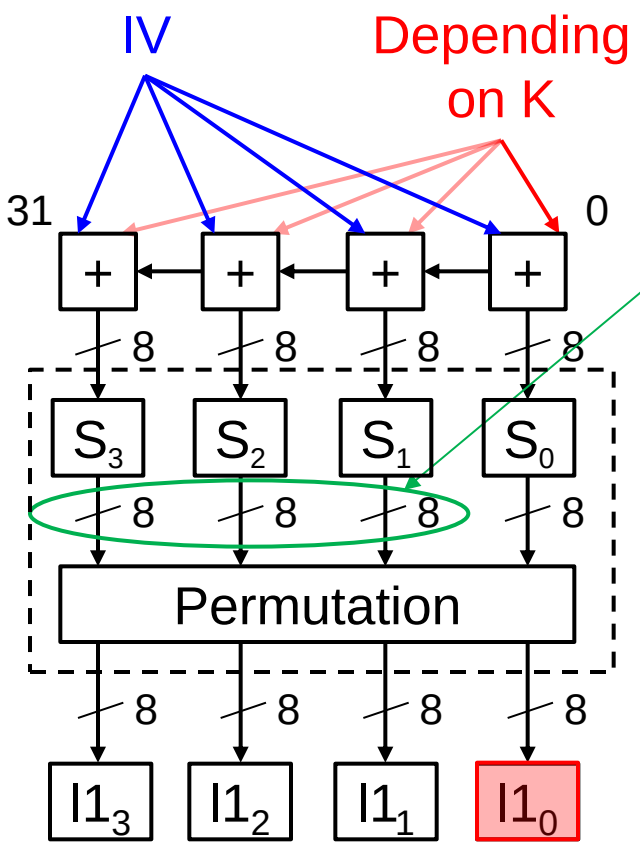
- Targetable value given by initial vector and 32-bit internal key
  - Stored in Register L1

After Clock 4: Untargetable

$L1^{(4)}$= Sub(IV + Sub(Sub(K + Sub(0))))

Chosen-IV method to calculate each byte in L1

- Each byte of internal key can be estimated by each byte in L1

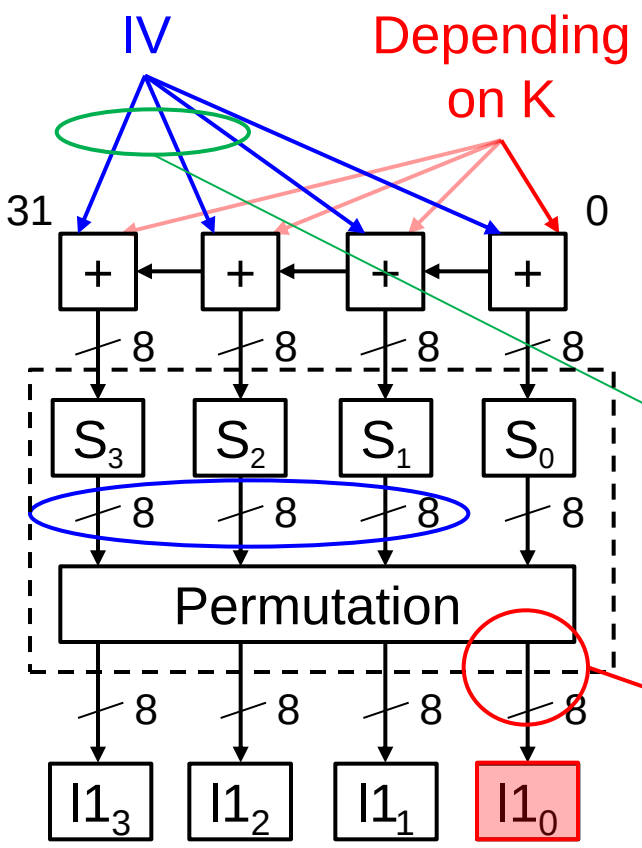


- Difficulties
  - Carry propagation in integer addition
  - Permutation

$$I1_0 = s_0 \otimes (02)_{16} \oplus s_1 \otimes (03)_{16} \oplus s_2 \oplus s_3 \quad ?$$

Chosen-IV method to calculate each byte in L1

- Each byte of internal key can be estimated by each byte in L1



- Difficulties
  - Carry propagation in integer addition
  - Permutation

$$I1_0 = s_0 \otimes (02)_{16} \oplus s_1 \otimes (03)_{16} \oplus s_2 \oplus s_3 \quad ?$$

- Choose IV with zeros as all elements except for the byte of interest
  - Carry propagation does not occur
  - Output of Permutation can be approximated

$$I1_0 \simeq s_0 \otimes (02)_{16}$$

Power model

- Use 1-bit Hamming Weight model (HW)
  - It is difficult to use Hamming Distance model
    - $L1^{(2)}$ (= Sub (K + Sub(0))) is unknown constant value
  - 1-bit HW model is equivalent to 1-bit HD model close to real power consumption

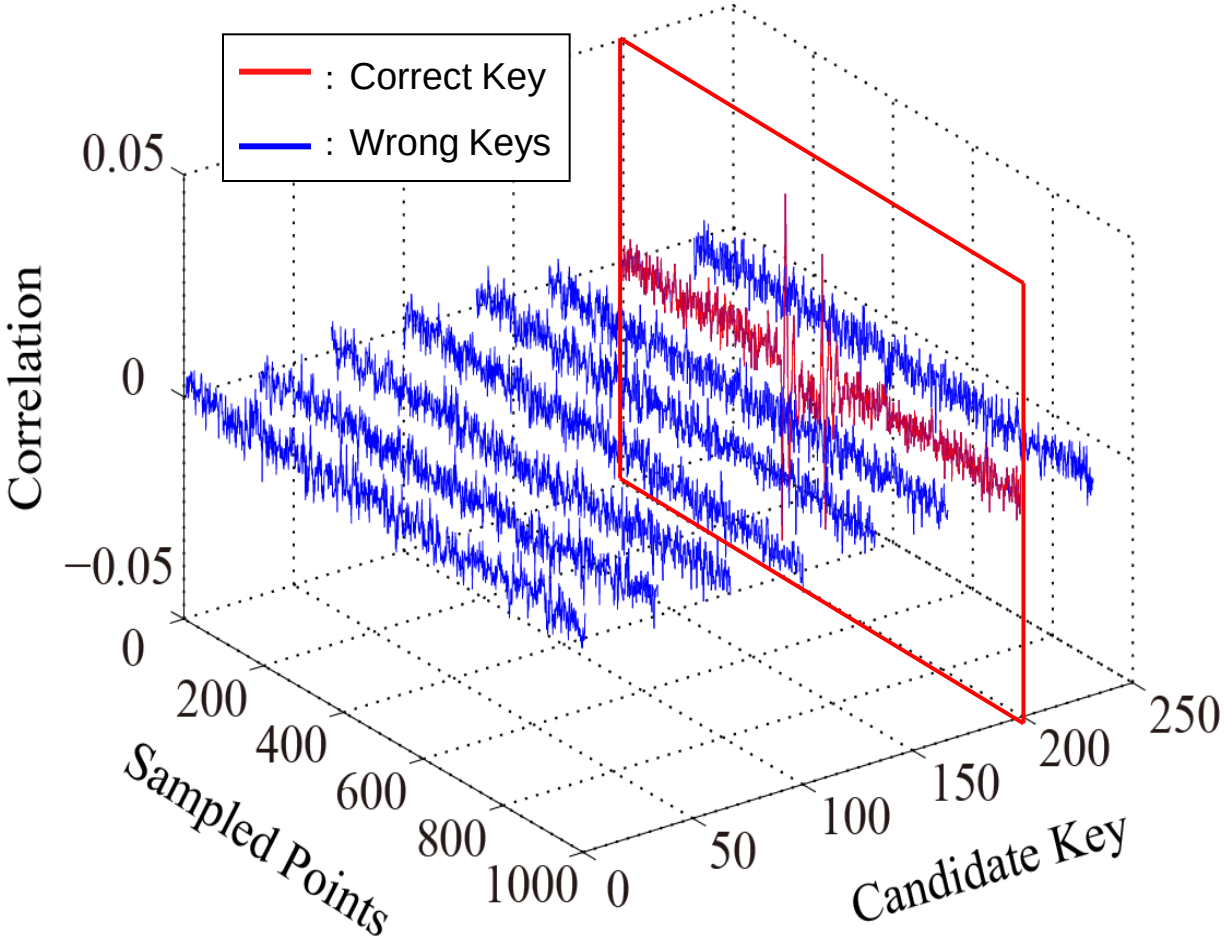
$L1^{(2)}$	$L1^{(3)}$	HD ($L1^{(2)}$, $L1^{(3)}$) ≈Real	HW ($L1^{(3)}$)
0	0	$P_{0\rightarrow 0}=0$	$P_0=0$
0	1	$P_{0\rightarrow 1}=1$	$P_1=1$
1	0	$P_{1\rightarrow 0}=1$	$P_0=0$
1	1	$P_{1\rightarrow 1}=0$	$P_1=1$

  - Sign of correlation peak can be used for estimating the value of $L1^{(2)}$

Estimation of keys

Chosen-IV CPAs at Clocks 3 and 4:

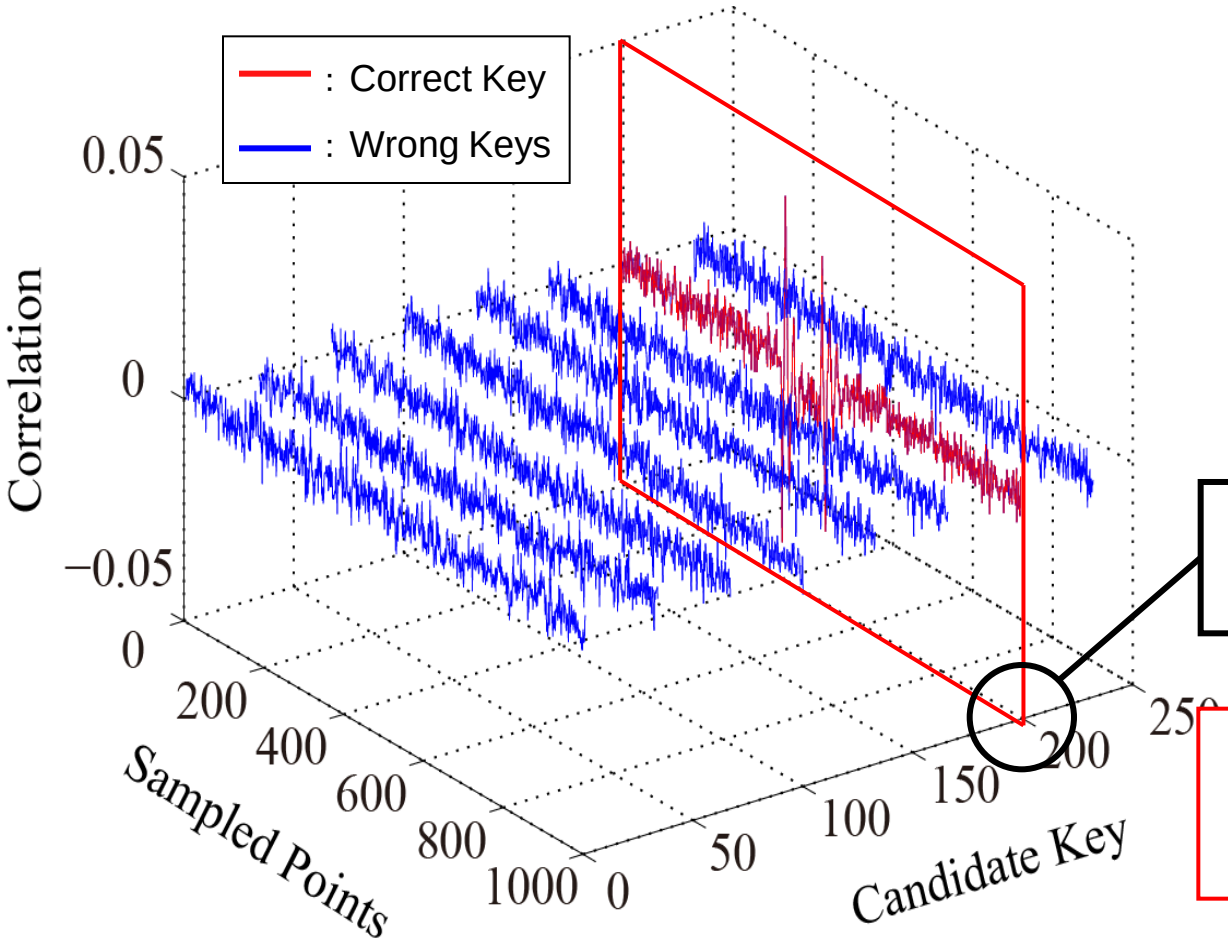
Key estimation by correlation peak and its sign



Estimation of keys

Chosen-IV CPAs at Clocks 3 and 4:

Key estimation by correlation peak and its sign



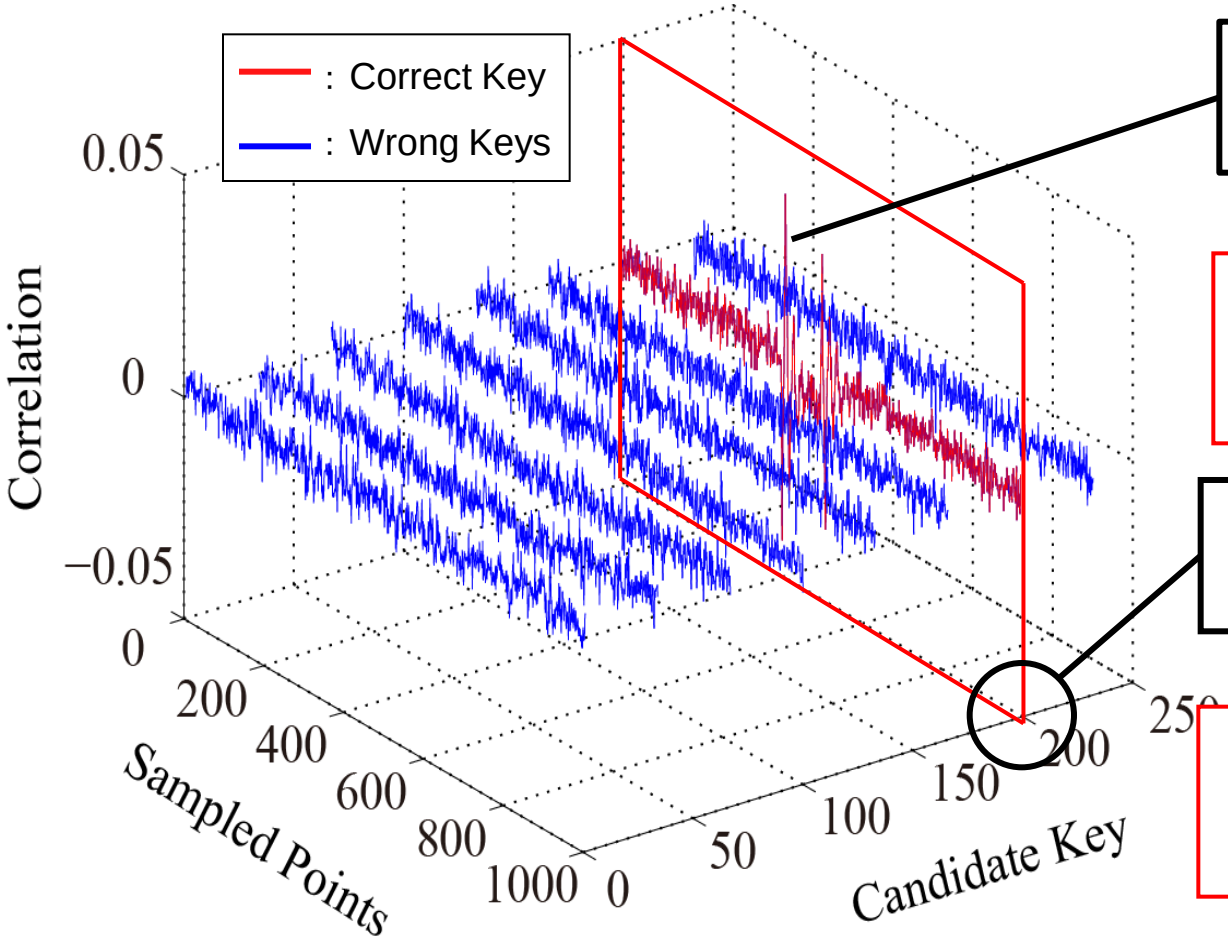
Correlation peak position

32-bit internal key x2 (at Clocks 3 and 4)

Estimation of keys

Chosen-IV CPAs at Clocks 3 and 4:

Key estimation by correlation peak and its sign



Sign of correlation peak

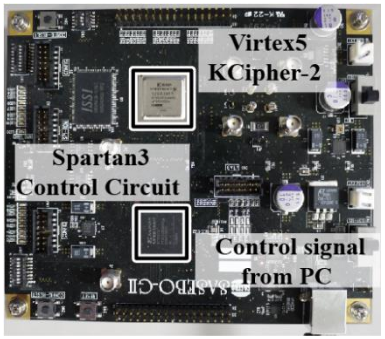
32-bit internal key (from value of $L1^{(2)}$)

Correlation peak position

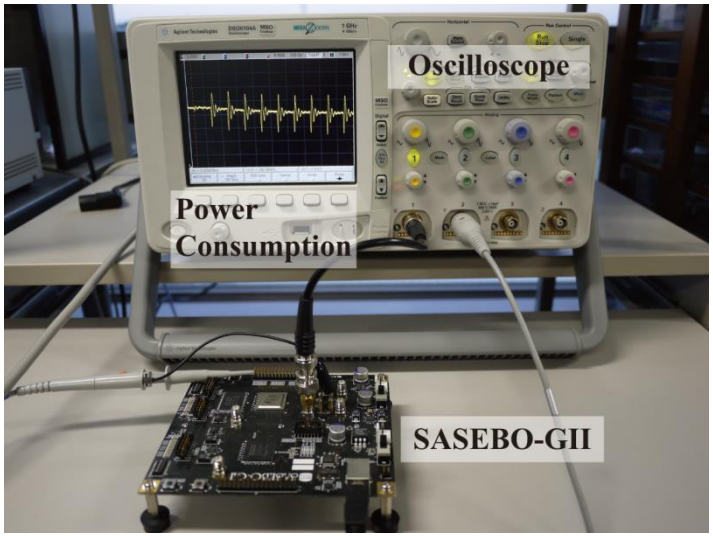
32-bit internal key x2 (at Clocks 3 and 4)

Experimental setup

- KCipher-2 in FPGA (SASEBO-GII)
  - Number of chosen IVs: 100,000
  - Clock frequency: 2.0 MHz
  - Sampling rate: 200 MSample/s

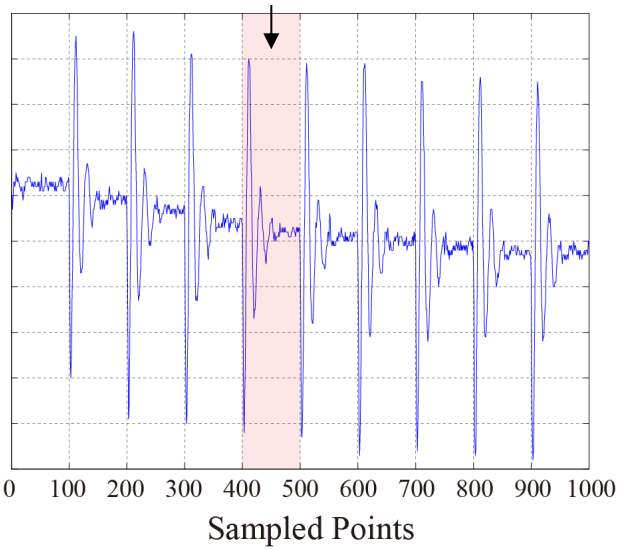


SASEBO-GII



(a) Overview of setup

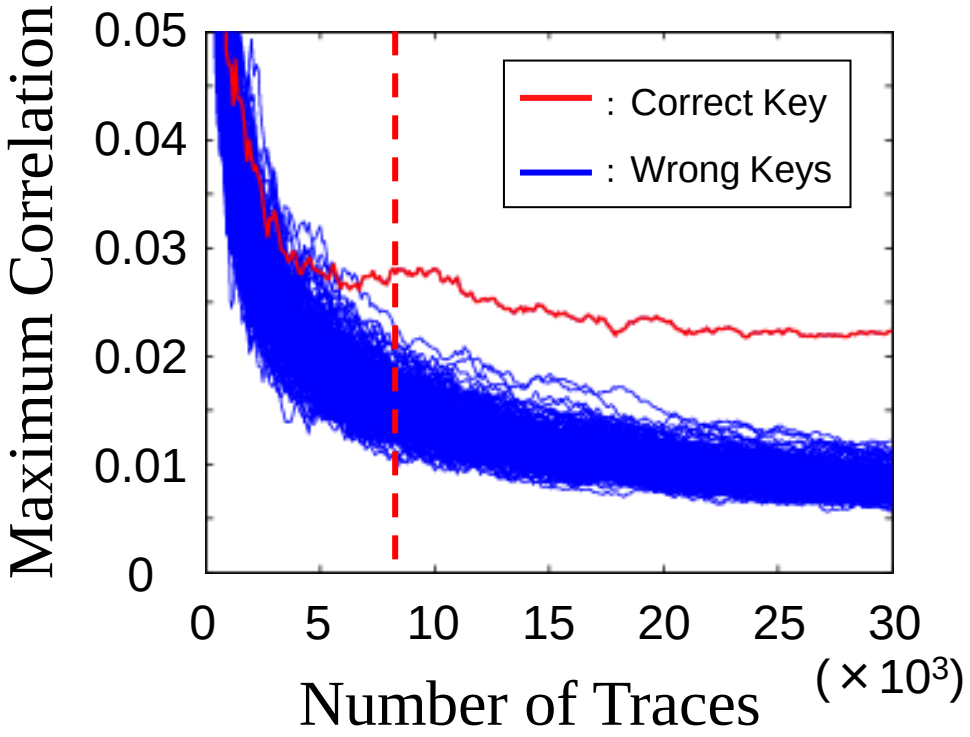
Clock 3 in initialization step



(b) Power trace

Estimation result by correlation peak position

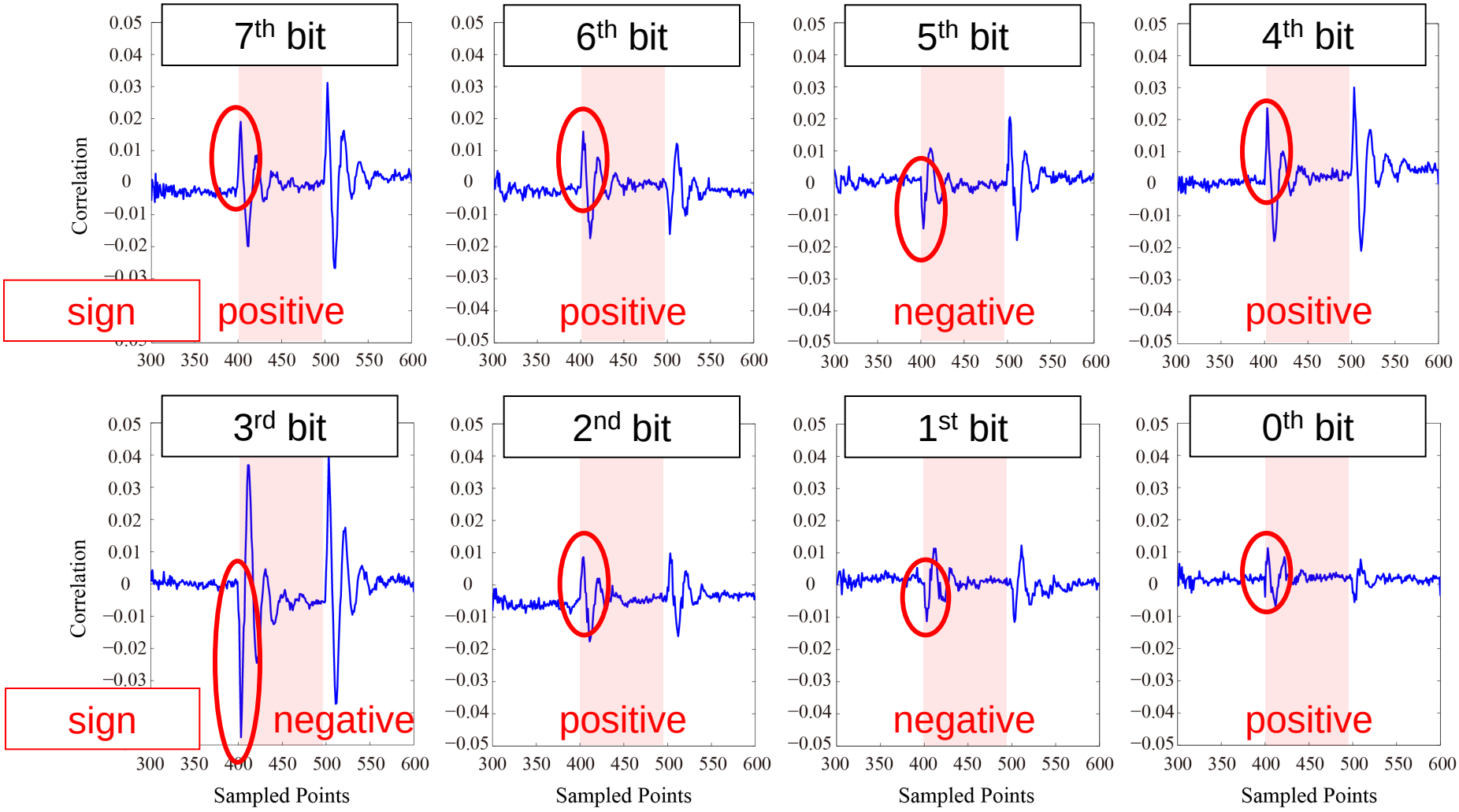
- Key estimation by correlation peak
  - evaluation of peak values by MTD*
    - Successful estimation of the correct key from 10,000 power traces



*Measurements To Disclosure

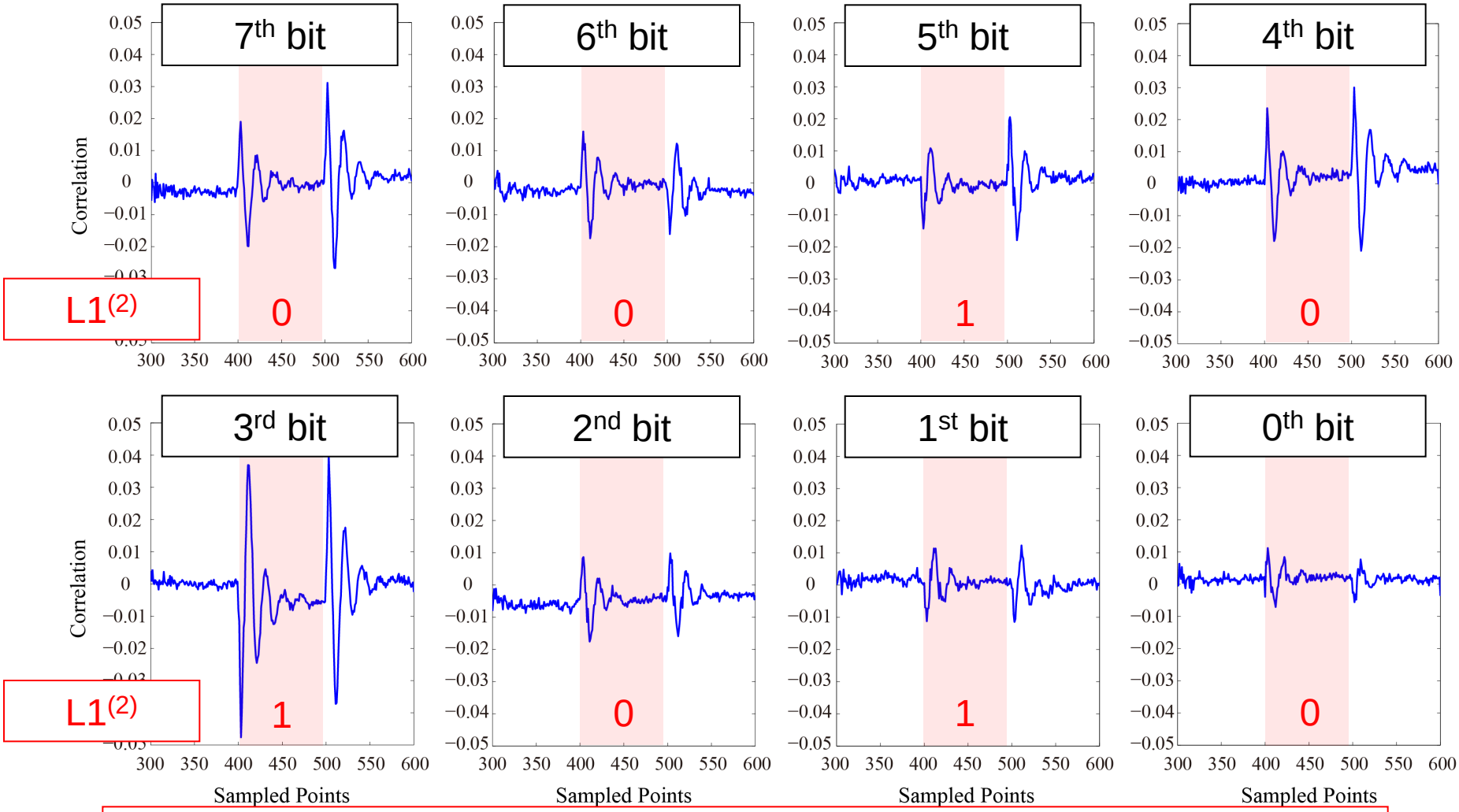
Estimation result by sign of correlation peak

Correlations for the correct key obtained in the clock 3 CPA



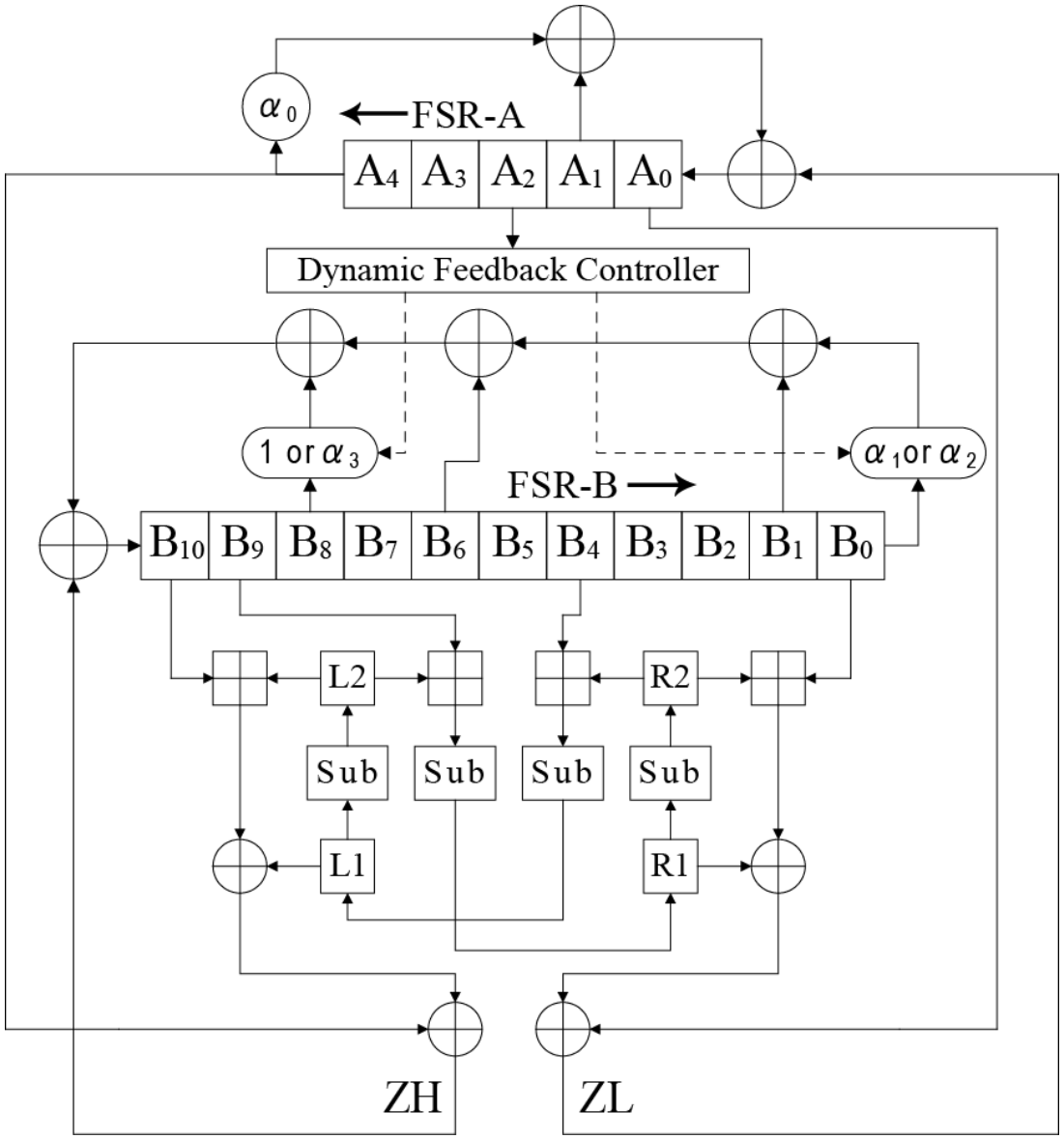
Estimation result by sign of correlation peak

Correlations for the correct key obtained in the clock 3 CPA

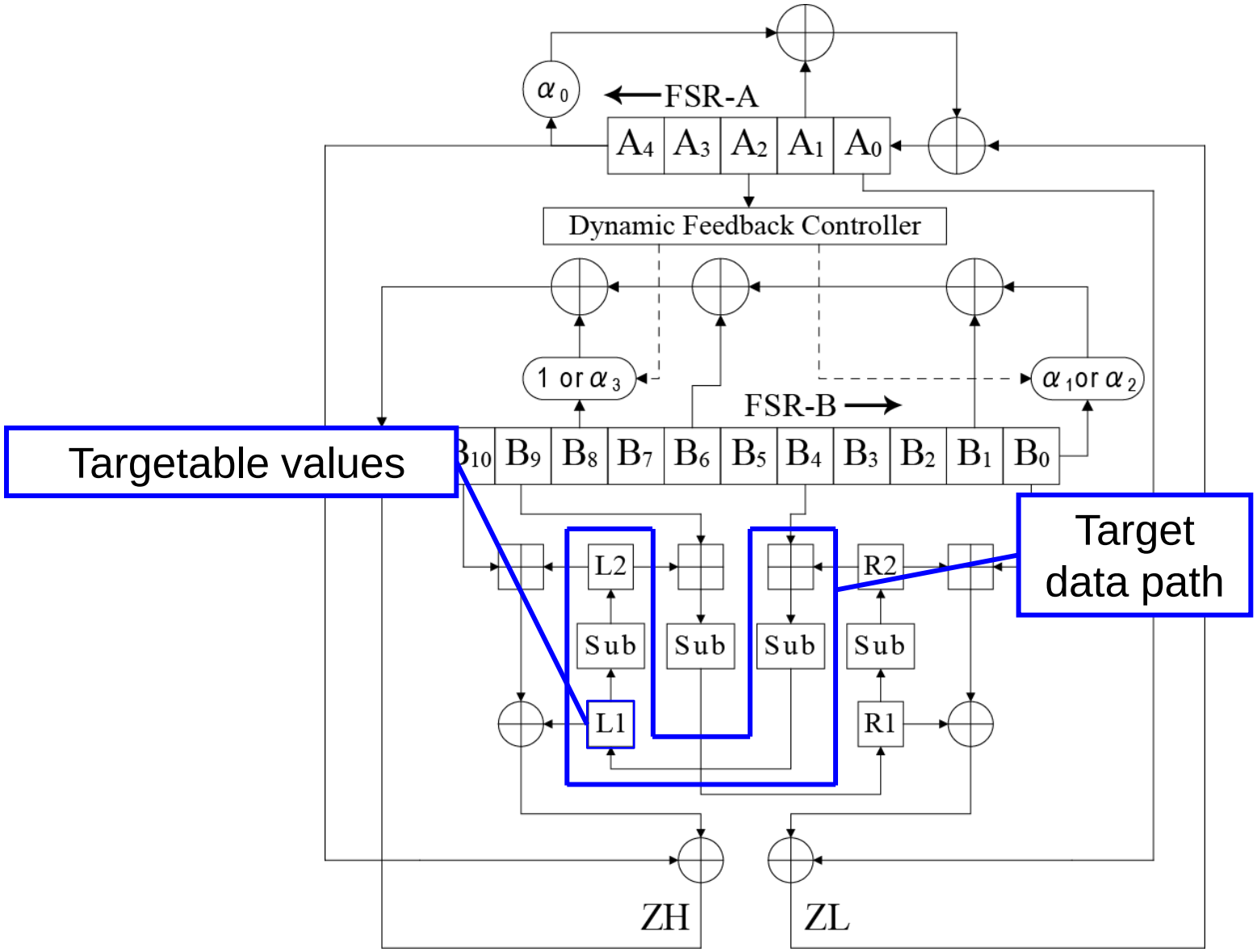


Three 32-bit internal keys were successfully obtained

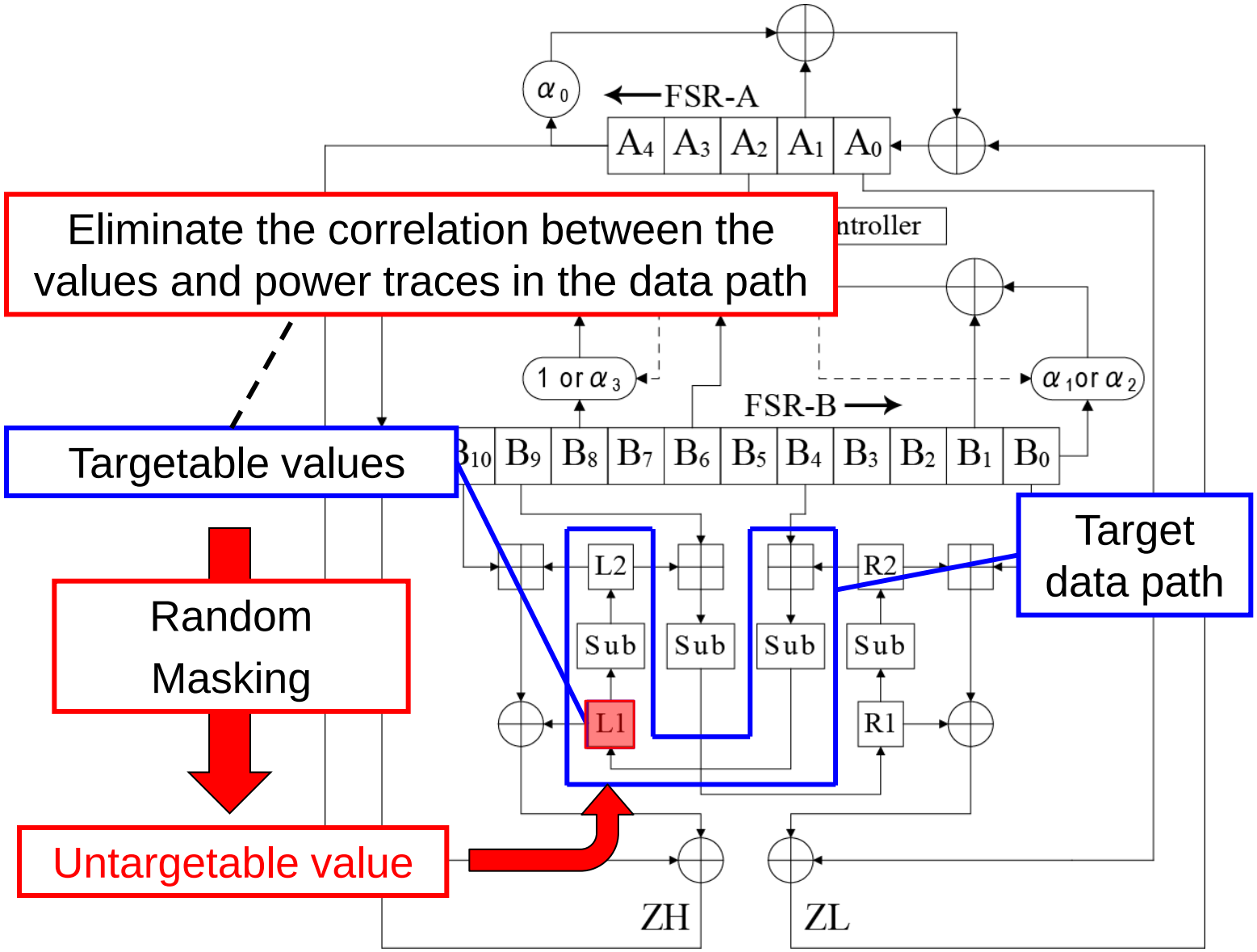
Countermeasure against proposed CPA



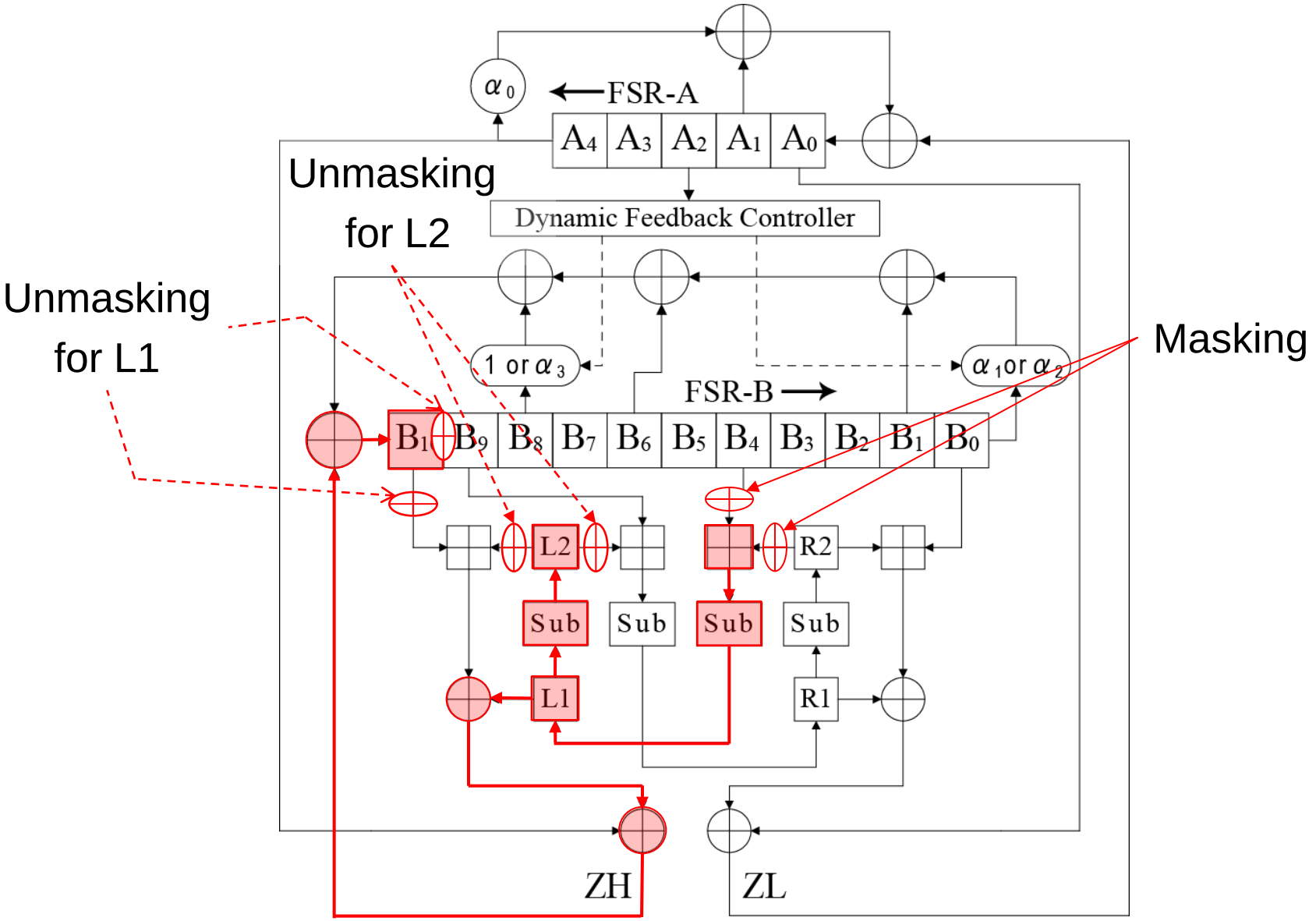
Countermeasure against proposed CPA



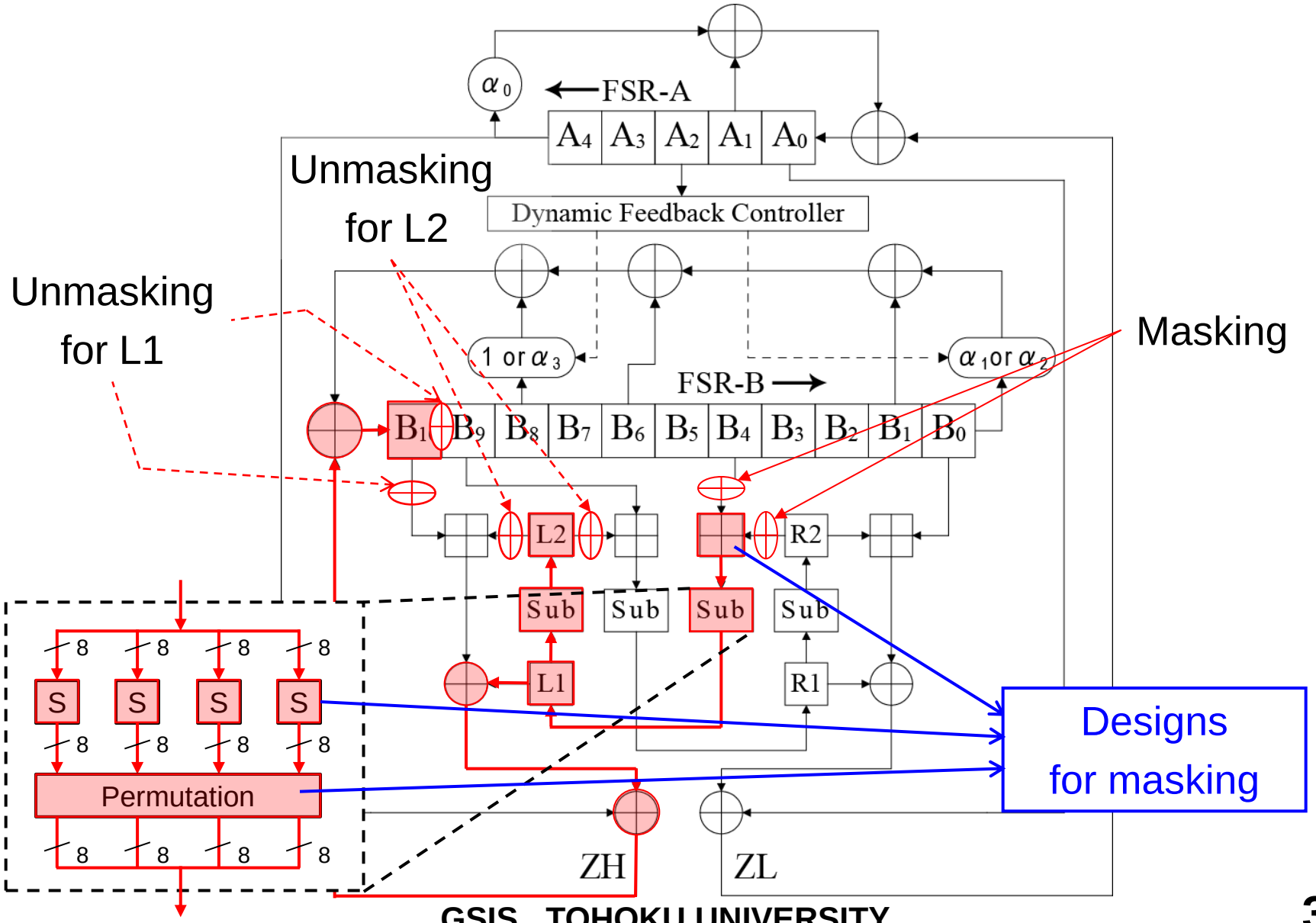
Countermeasure against proposed CPA



Countermeasure based on random masking



Countermeasure based on random masking



Masking of integer addition

- Apply Golic's masked AND operation [Golic] to the masking of integer addition
  - MUX-based masked AND ($\wedge$')
    - $X \wedge' Y = (x \oplus mx) \wedge' (y \oplus my)$

      $= \mathrm{MUX}(\mathrm{MUX}(mx, X; my), \mathrm{MUX}(X, mx; my); Y)$

      $= (x \wedge y) \oplus mx$
    - Unmask value given by a mask value mx or my
  - Application to integer addition algorithms
    - Ripple Carry Adder (RCA)
    - Kogge-Stone Adder (KSA)

[Golic] J. D. Golic, IEEE Trans., 2007

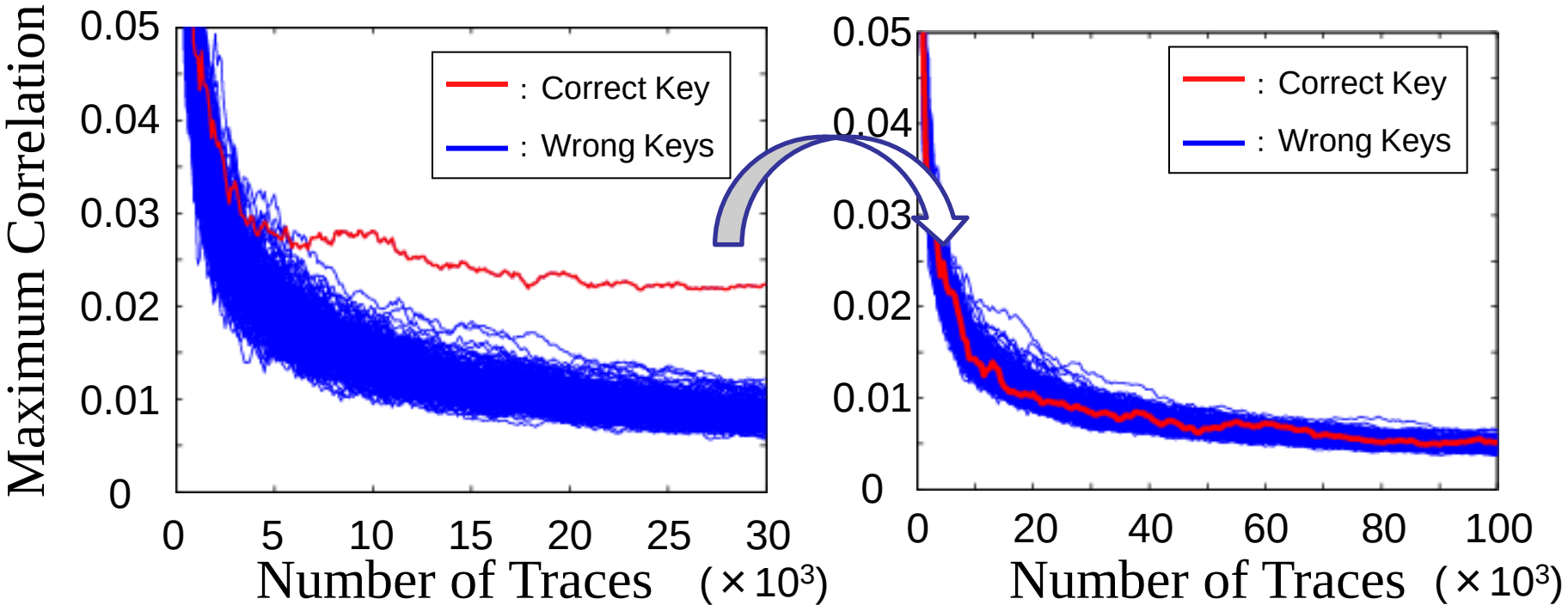
Masking of sub function

- Masked S-box
  - Additive masking [Oswald] for composite-field (Comp) structure
    - In GF(2^2), additive mask value can be separable from the true output value
  - Multiplicative masking [Akkar] for table (TBL) structure
    - Multiplicative mask can be separable from the output of multiplicative inversion in GF(2^8)
- Permutation (P)
  - Unmask value is easily calculated on the fly by the duplication of this function
    - $P\,(x \oplus mx) = P\,(x) \oplus P\,(mx)$

[Oswald] E. Oswald, FSE, 2005
[Akkar] M. Akkar, CHES, 2001

Evaluation of countermeasure

- Estimation by correlation peaks
  - Results of proposed CPA
    - Validity of proposed countermeasure was confirmed



(a) Without countermeasure
RCA, Comp

(b) With countermeasure
RCA, Comp

Performance of our architecture evaluated in ASIC

- Synopsys Design Compiler
- TSMC 65nm LP standard cell library

	Adder	S-box	Delay [ns]	Area [μm^2]
Without Counter-measure	RCA	Comp	6.50	30131
	KSA	TBL	2.27	56611
With Counter-measure	RCA	Comp	13.44	47930
	KSA	TBL	5.99	77621

Performance of our architecture evaluated in ASIC

- Synopsys Design Compiler
- TSMC 65nm LP standard cell library

	Adder	S-box	Delay [ns]	Area [μm^2]
Without Counter-measure	RCA	Comp	6.50	30131
	KSA	TBL	2.27	56611
With Counter-measure	RCA	Comp	13.44	47930
	KSA	TBL	5.99	77621

- Area overhead : 60%

Performance of our architecture evaluated in ASIC

- Synopsys Design Compiler
- TSMC 65nm LP standard cell library

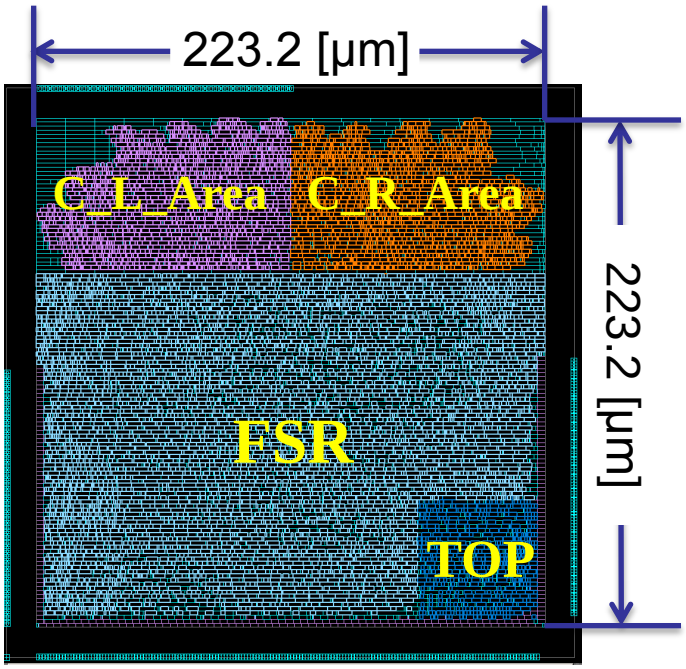
	Adder	S-box	Delay [ns]	Area [μm^2]
Without Counter-measure	RCA	Comp	6.50	30131
	KSA	TBL	2.27	56611
With Counter-measure	RCA	Comp	13.44	47930
	KSA	TBL	5.99	77621

- Area overhead : 60%
- Delay overhead : 160%

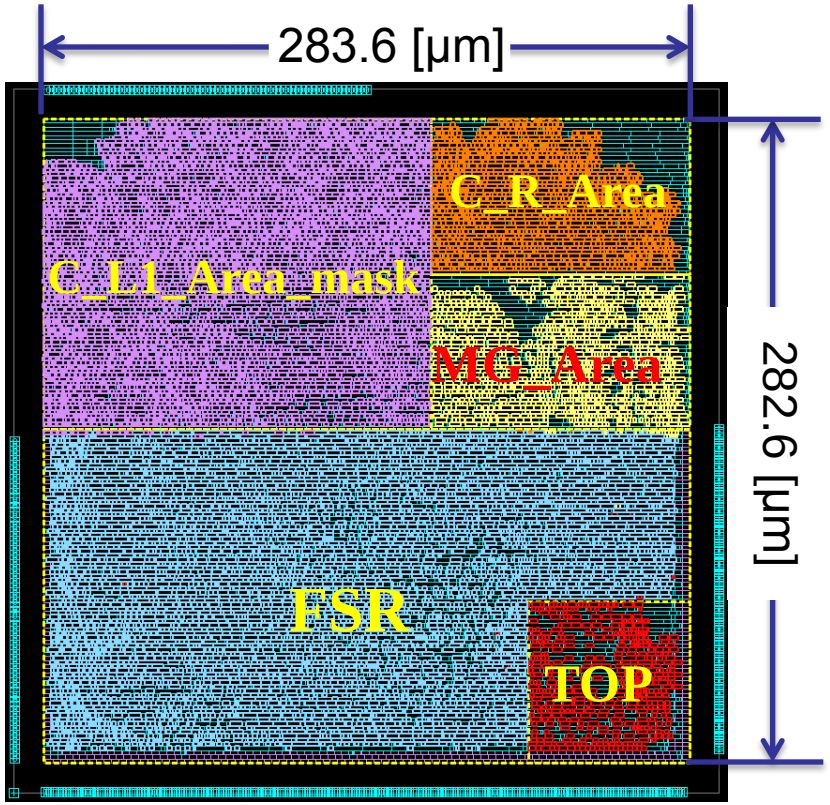
The layout of ASIC implementation

- TSMC 65nm LP standard cell library

Without countermeasure



With countermeasure



Conclusions and future works

- Chosen-IV CPA on KCipher-2 to reveal the entire 128-bit initial key
- Masking-based countermeasure resistant to proposed CPA
  - Area overhead: 60%, Delay overhead: 160%
- Future works
  - Other types of side-channel attacks
    - Advanced analysis defeating conventional countermeasure [Mangard]
    - Fault analysis
  - Attacks for other components
    - Attacks for FSR-A, B

[Mangard] S. Mangard, CHES, 2005

END

Thank you for your kind attention