Intra-Masking Dual-Rail Memory on LUT Implementation for Tamper-Resistant AES on FPGA

Ritsumeikan University, Japan

Hoang Anh Tuan
Fujino Takeshi

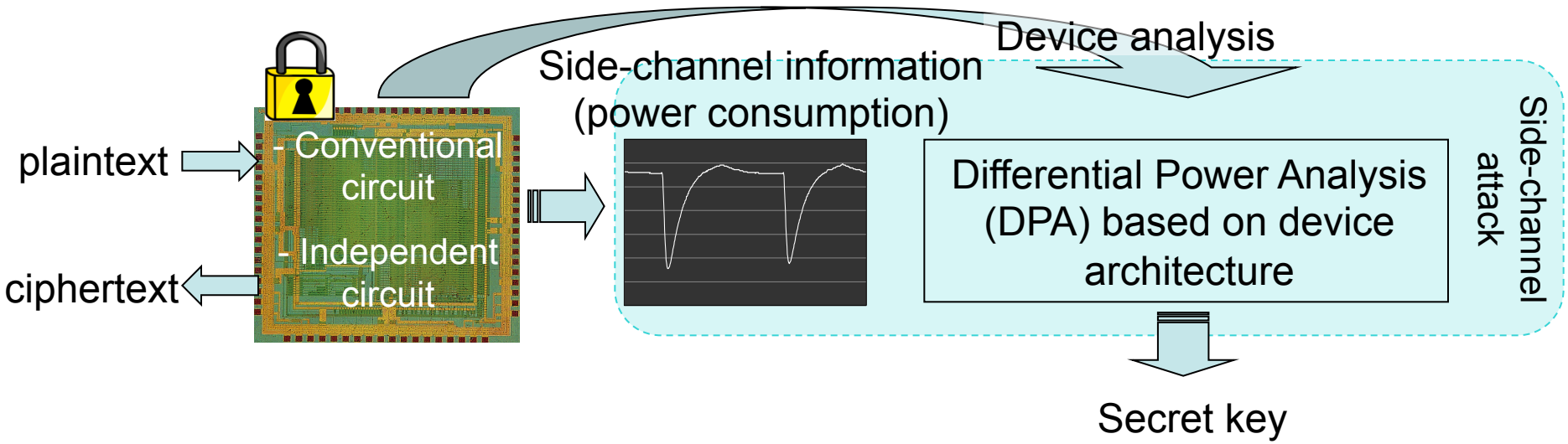
2012 / 02 / 23

Outline

- Background and objectives
- AES implementation and side-channel attack (SCA)
- Related work and motivation for dual-rail memory
- AES implementation using conceptual dual-rail memory and problems
- Intra-masking dual-rail memory
- Discussion, conclusion and future work

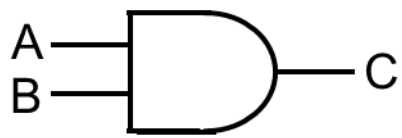
Background and Objectives

- Even the cryptographic algorithms such as AES and DES are safe, their implementations to devices are vulnerable under side-channel attack



- Introduce a SCA tamper resistant implementation using dual-rail memory and apply it to AES
- Evaluate the implementation on FPGA

Bases of side-channel attack



A1	B1	A2	B2	C1	C2	Trans
0	0	0	0	0	0	
0	0	0	1	0	0	
0	0	1	0	0	0	
0	0	1	1	0	1	1
0	1	0	0	0	0	
0	1	0	1	0	0	
0	1	1	0	0	0	
0	1	1	1	0	1	1
1	0	0	0	0	0	
1	0	0	1	0	0	
1	0	1	0	0	0	
1	0	1	1	0	1	1
1	1	0	0	1	0	1
1	1	0	1	1	0	1
1	1	1	0	1	0	1
1	1	1	1	1	1	

3/12

3/4

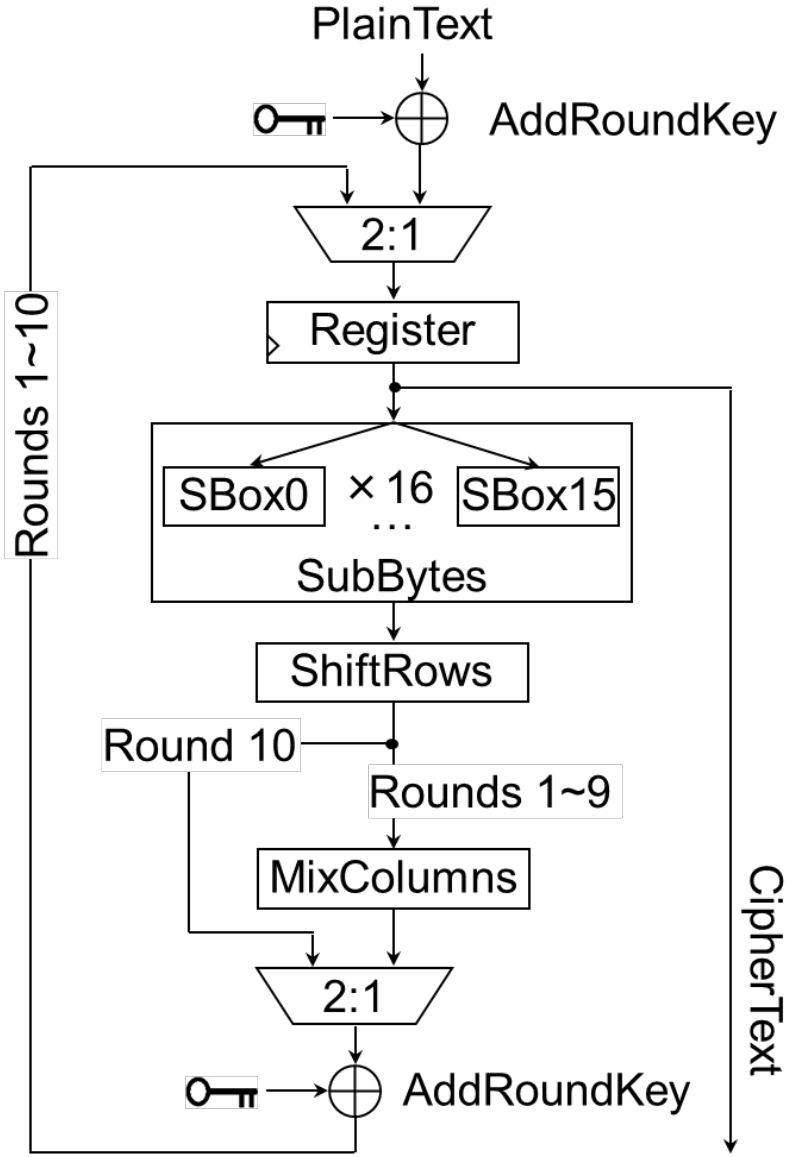
The difference in transition rate of non-linear logics can be used in side-channel attack

- When C1 is “0”, the transition rate (to 1) is 3/12 = 1/4
- When C1 is “1”, the transition rate (to 0) is 3/4

Mean power consumption when C1 = “0” is smaller than mean power consumption when C1 = “1”

Categorize the processing data by groups “0” and “1” based on C1 and compare the mean power consumptions

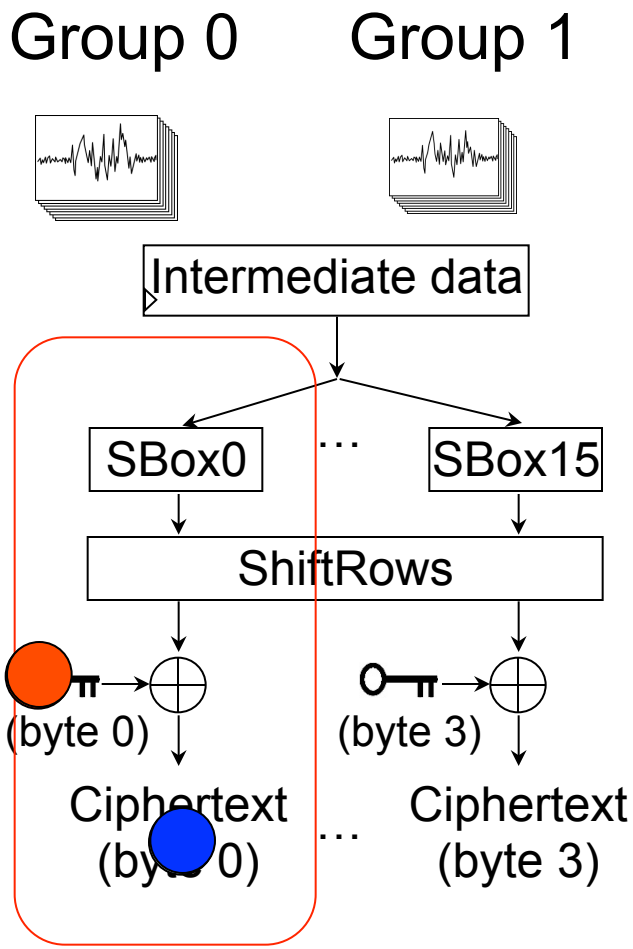
AES algorithm and implementation



- 128 bit data processing
- 128 bit key
- 10 rounds with 4 transformations
  - SubBytes
    - Multiplicative inverse
    - Affine transform
  - Shiftrows
  - Mixcolumns
  - Addroundkey

Linear operations with XOR gates

Leakage information and side-channel attack on AES



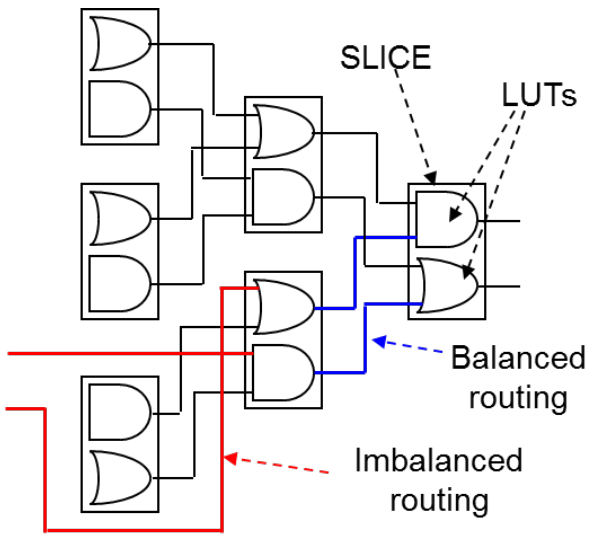
Processing at 10th round

Power consumption of the non-linear operation SBox can be used for side-channel attack

- Guess a byte-key and inversely compute the input of SBox (using know ciphertext)
- Group the power consumption based on the value of hypothesis input
- Compare the mean hypothesis power consumptions to find the correct byte-key

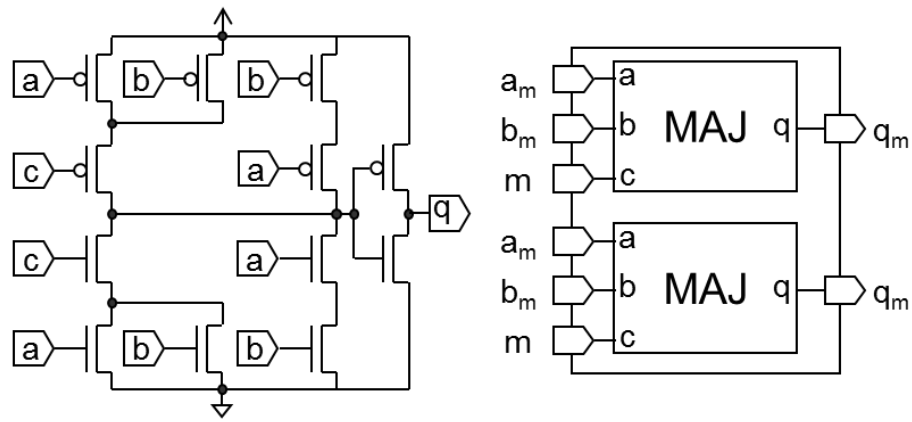
DPA countermeasures

Wave Dynamic Differential Logic (WDDL)



- Using dual-rail pre-charge logic to make power consumption uniform
- Load balancing is required in the pair wire
- Vulnerable under SCA due to the imbalance in the pair wire

Masked Dual-rail Pre-charge Logic (MDPL)



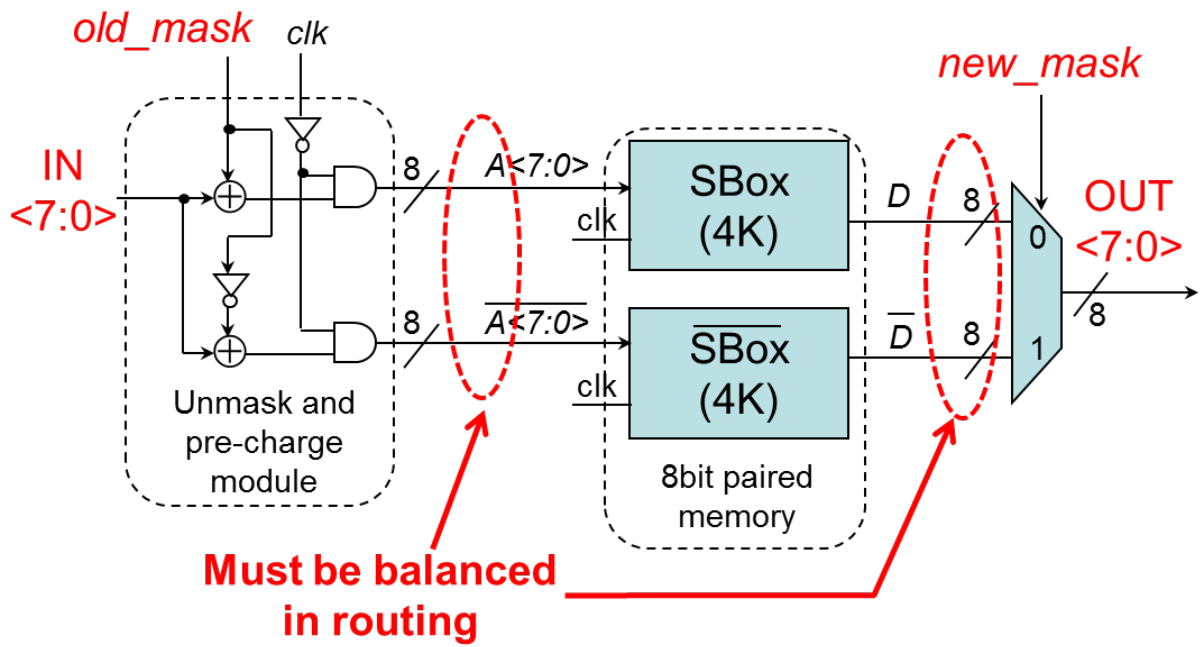
a. Schematic of a CMOS majority gates of MDPL (MAJ)

b. MDPL AND gate using the MAJ

- Using dual-rail logic based on masked data and its complement
- Load balancing is not required in the pair wire
- Vulnerable under SCA due to early propagation
- Large implementation and high power consumption

A countermeasure implementation method, which is independent with algorithms and can be implemented using standard design flow

Masked Dual-Rail Memory Concept



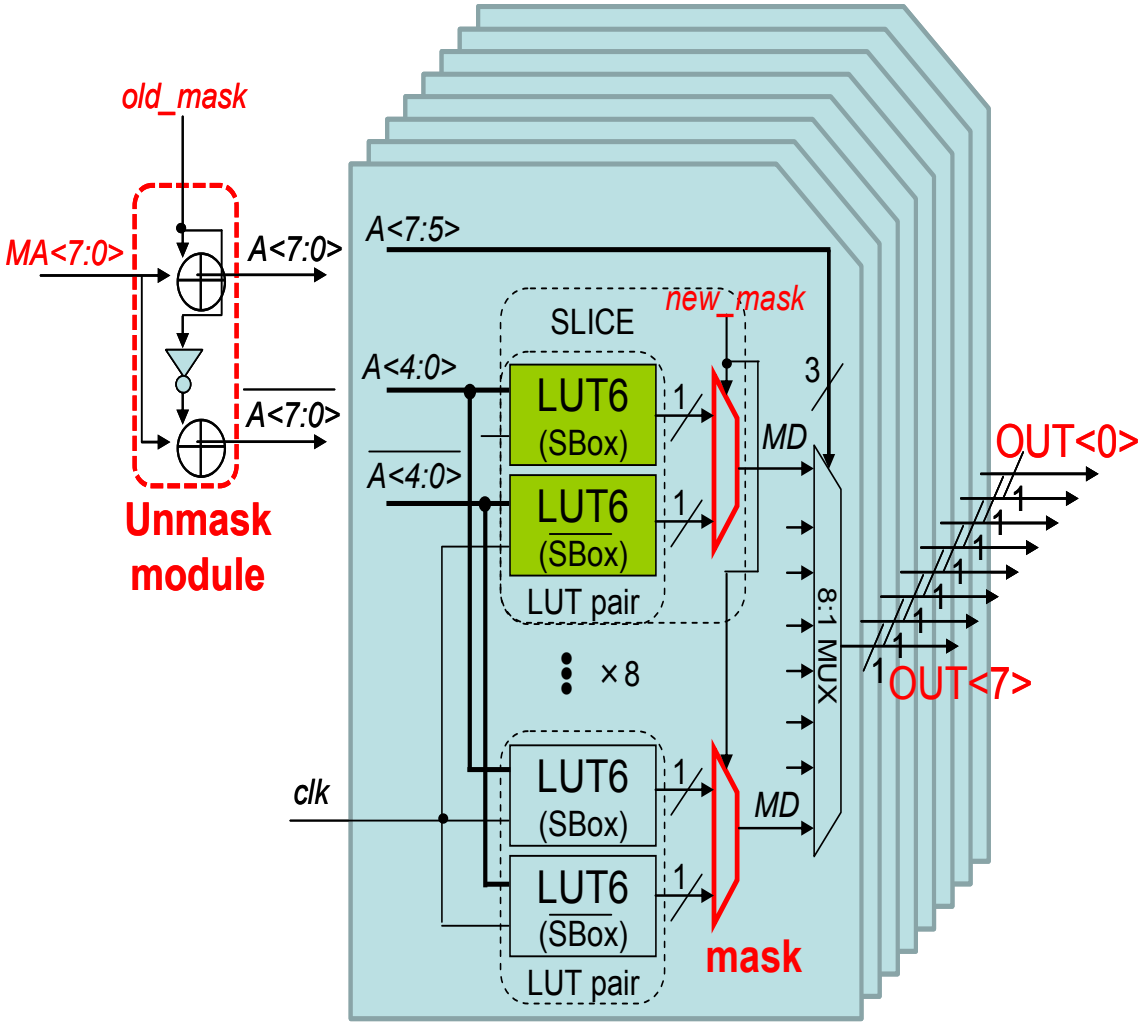
Truth table with pre-charge for SBox and /SBox

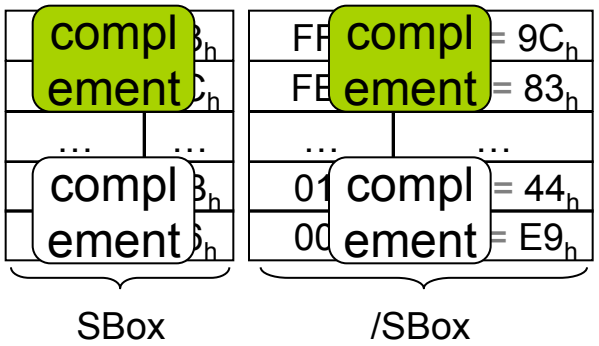
old_mask	IN<7:0>	clk	A<7:0>	D	/A<7:0>	/D	
x	xx_h	1	00_h	00_h	00_h	00_h	Pre-charge when *clk*=1
…	…	…	…	…	…	…	
x	xx_h	1	00_h	00_h	00_h	00_h	
0	00_h	0	00_h	63_h	FF_h	$/63_h = 9C_h$	Evaluate when *clk*=0
0	01_h	0	01_h	$7C_h$	FE_h	$/7C_h = 83_h$	
…	…	…	…	…	…	…	
0	FE_h	0	FE_h	BB_h	01_h	$/BB_h = 44_h$	
0	FF_h	0	FF_h	16_h	00_h	$/16_h = E9_h$	
			SBox		/SBox		

- Pre-charged dual-rail logic to make number of transitions balanced
- Complementary memories are used for complementary data
- Address and data buses work with their complementary buses

Same number of transitions inside the memory

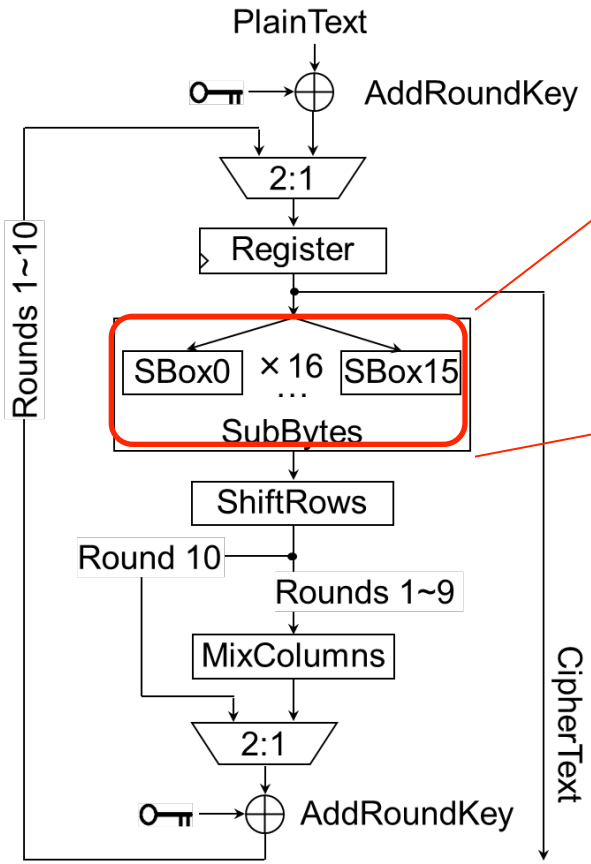
Conceptual dual-rail memory implementation





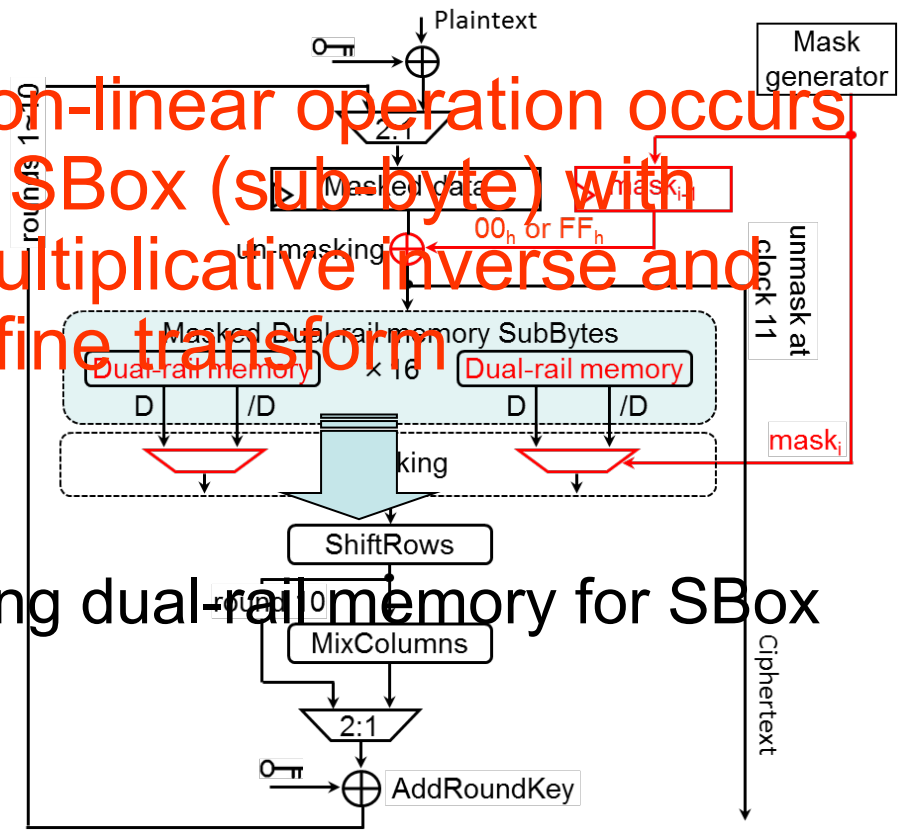
- A single unmask module is used for one SBox
- Memories for SBox and /SBox are divided into LUTs
- Two LUTs with complementary data are located in a slice

AES implementation with masked dual-rail memory



Normal AES implementation

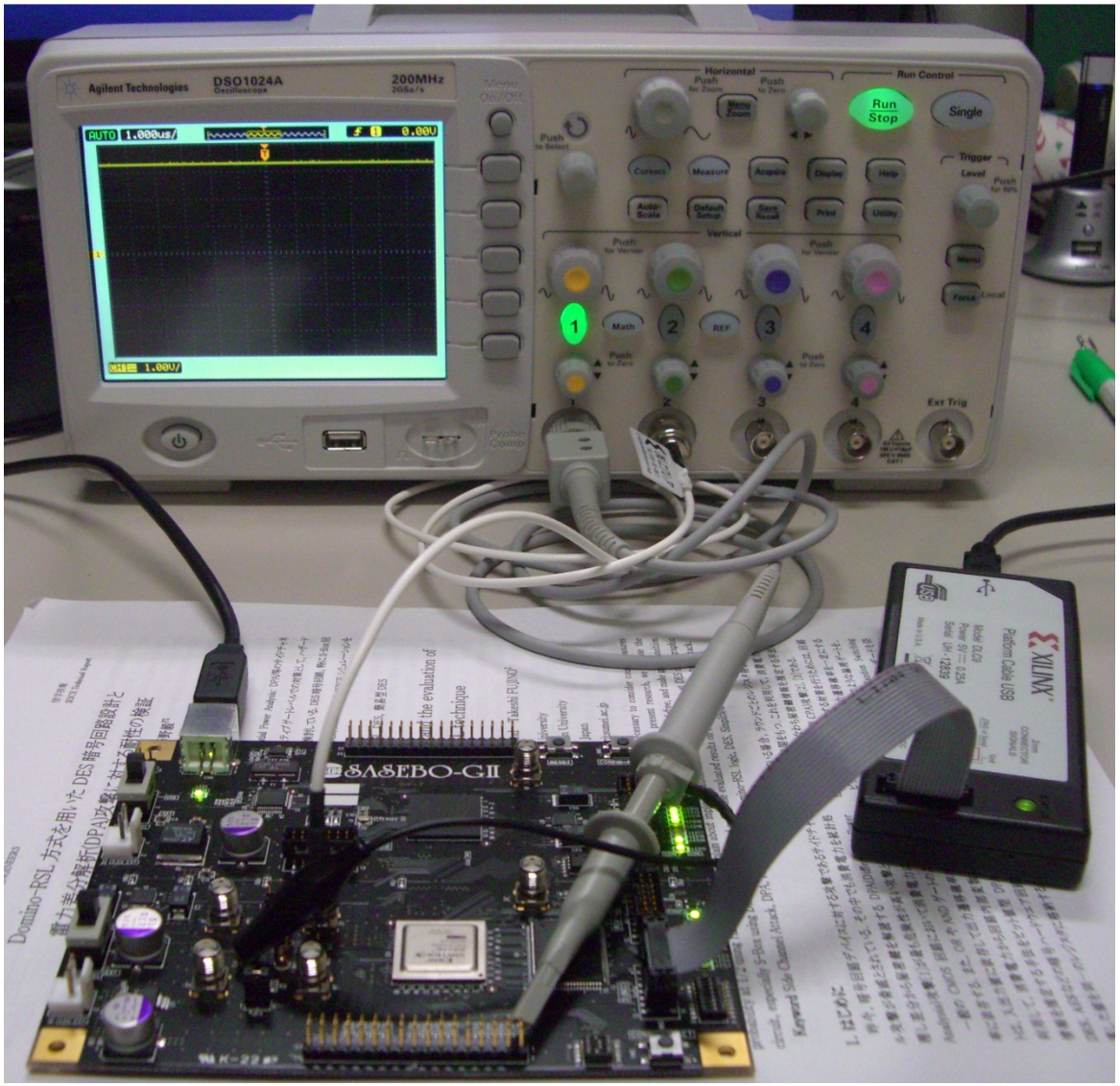
- Non-linear operation occurs in SBox (sub-byte) with multiplicative inverse and affine transform



Using dual-rail memory for SBox

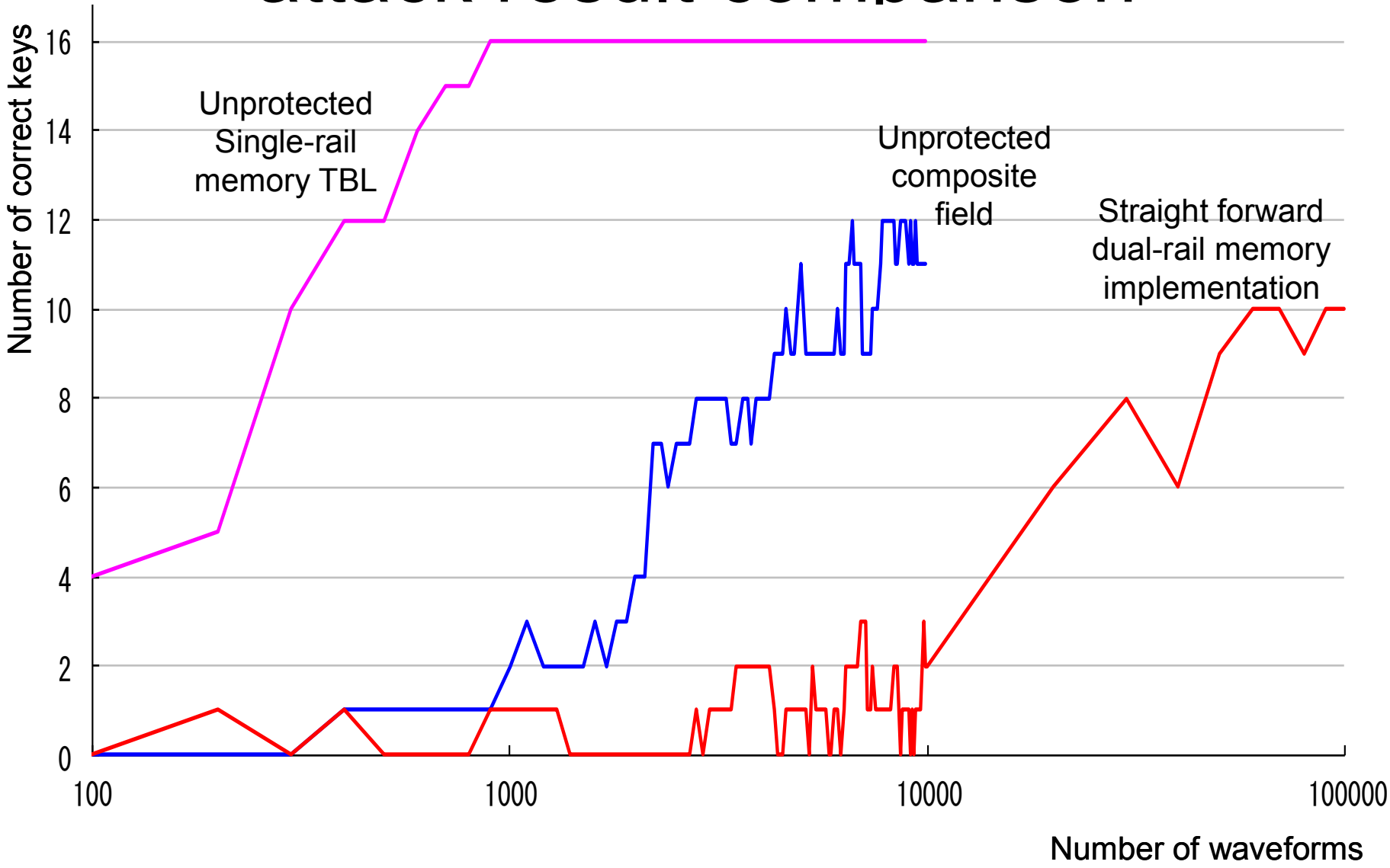
AES implementation with additive mask on dual-rail memory

Experiment conditions

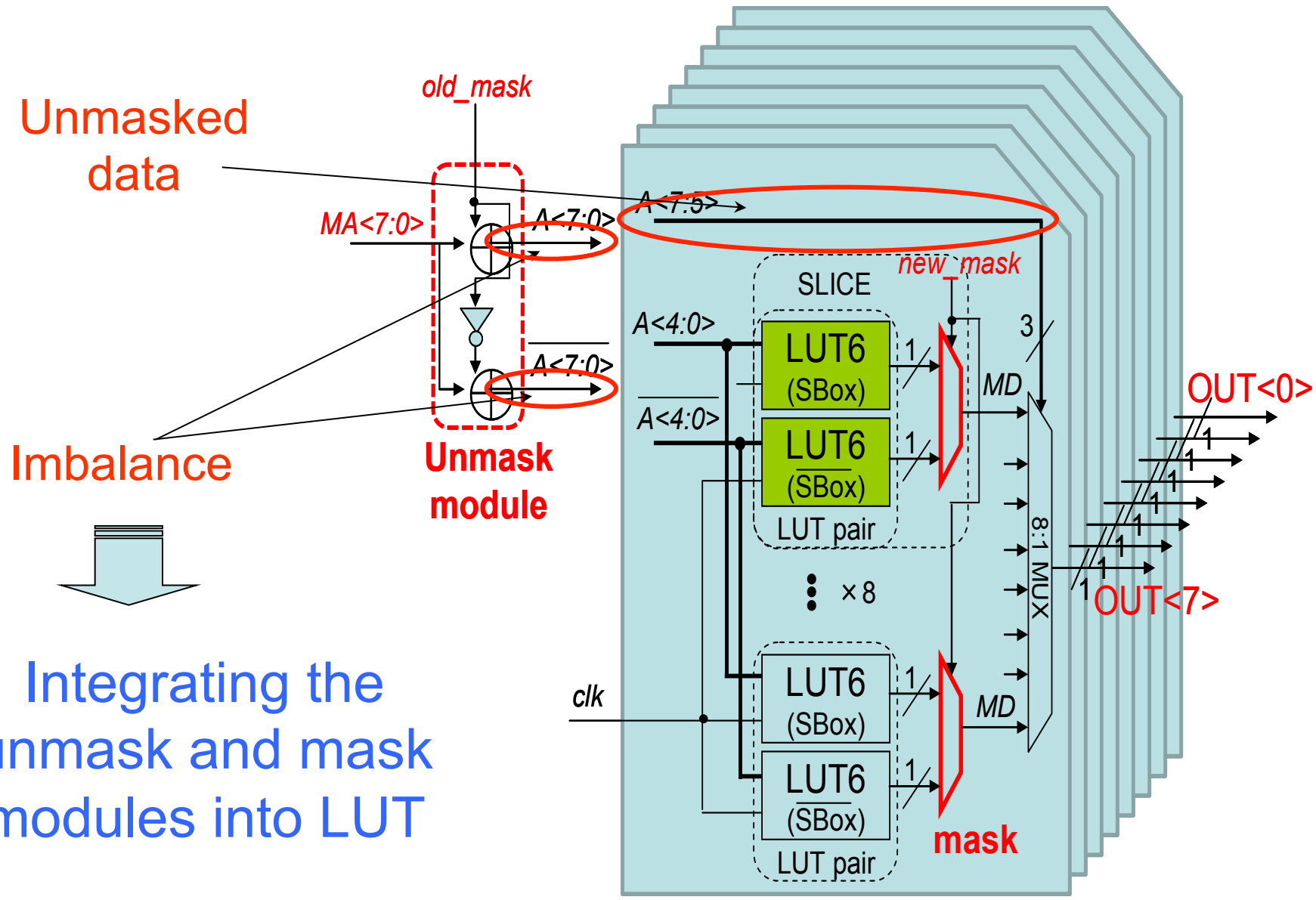


- SASEBO GII board with two FPGAs, one for controller and the other for AES (Virtex-5 XC5vlx30)
- Oscilloscope
- Attack with 1,000,000 traces
- HWCPA attacks

Correlation power analysis (CPA) attack result comparison

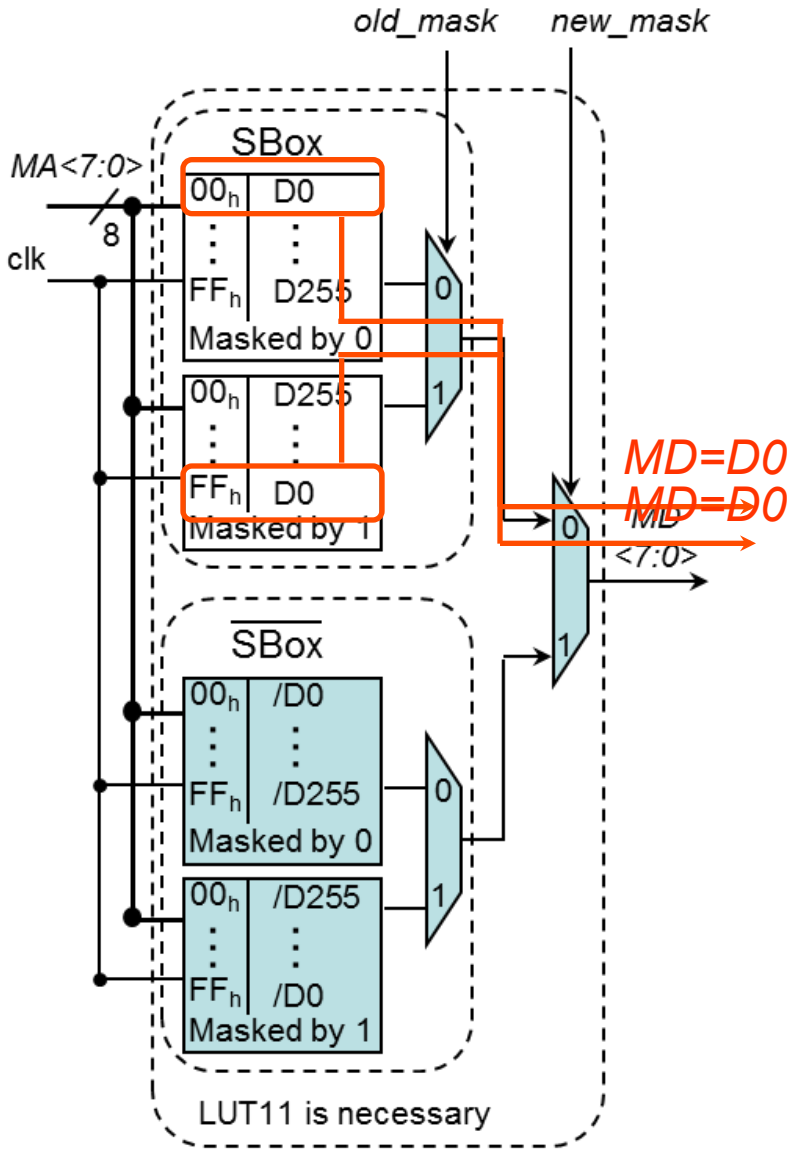


Leakage information and solution



Integrating the unmask and mask modules into LUT

Memory duplication for one-bit unmasking



Intra unmasking: Memories for SBox and /SBox are copied and stored in reversed order

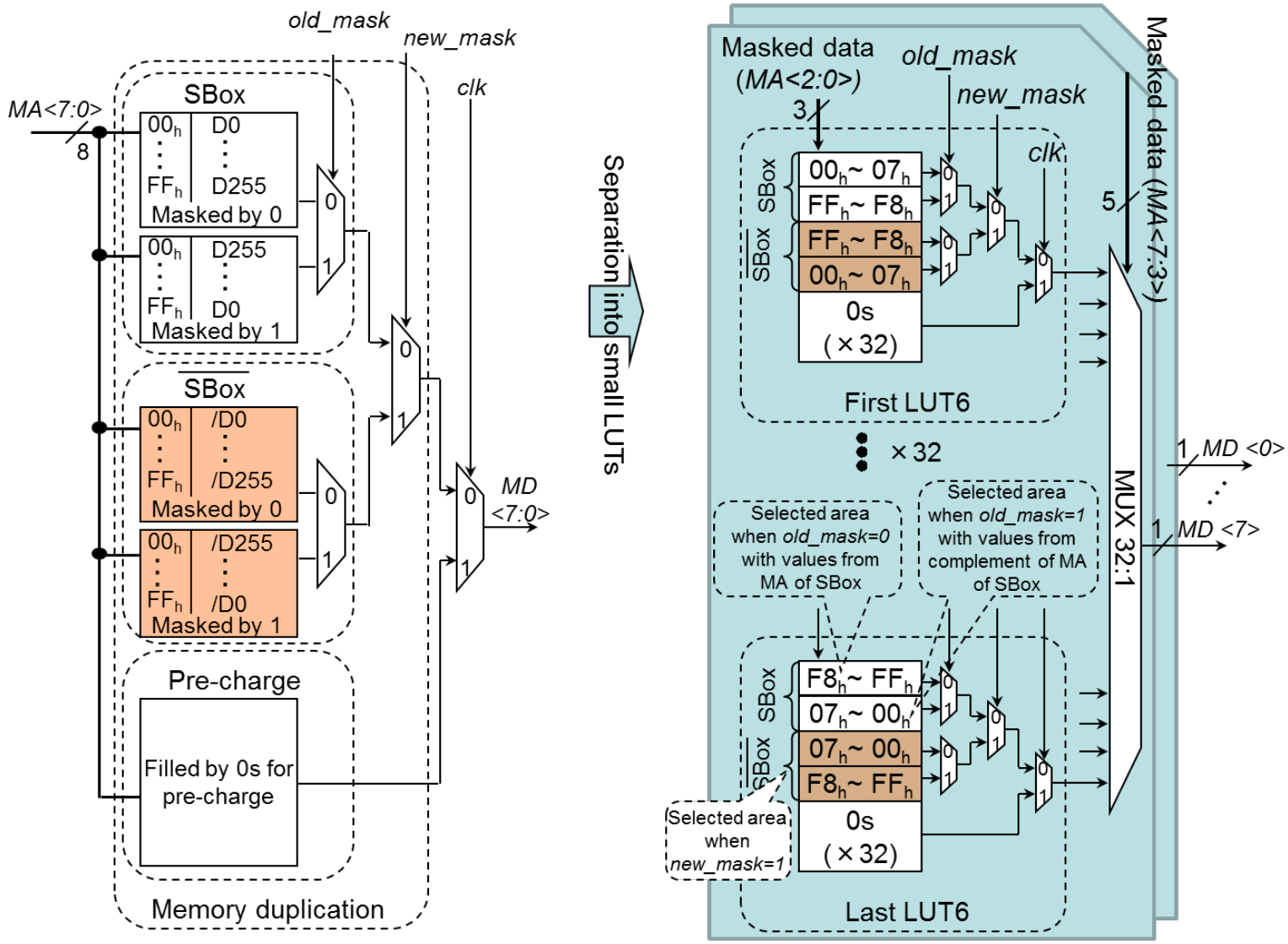
When $A=00_h$ and *old_mask*=0

$MA=00_h$

When $A=00_h$ and *old_mask*=1

$MA=FF_h$

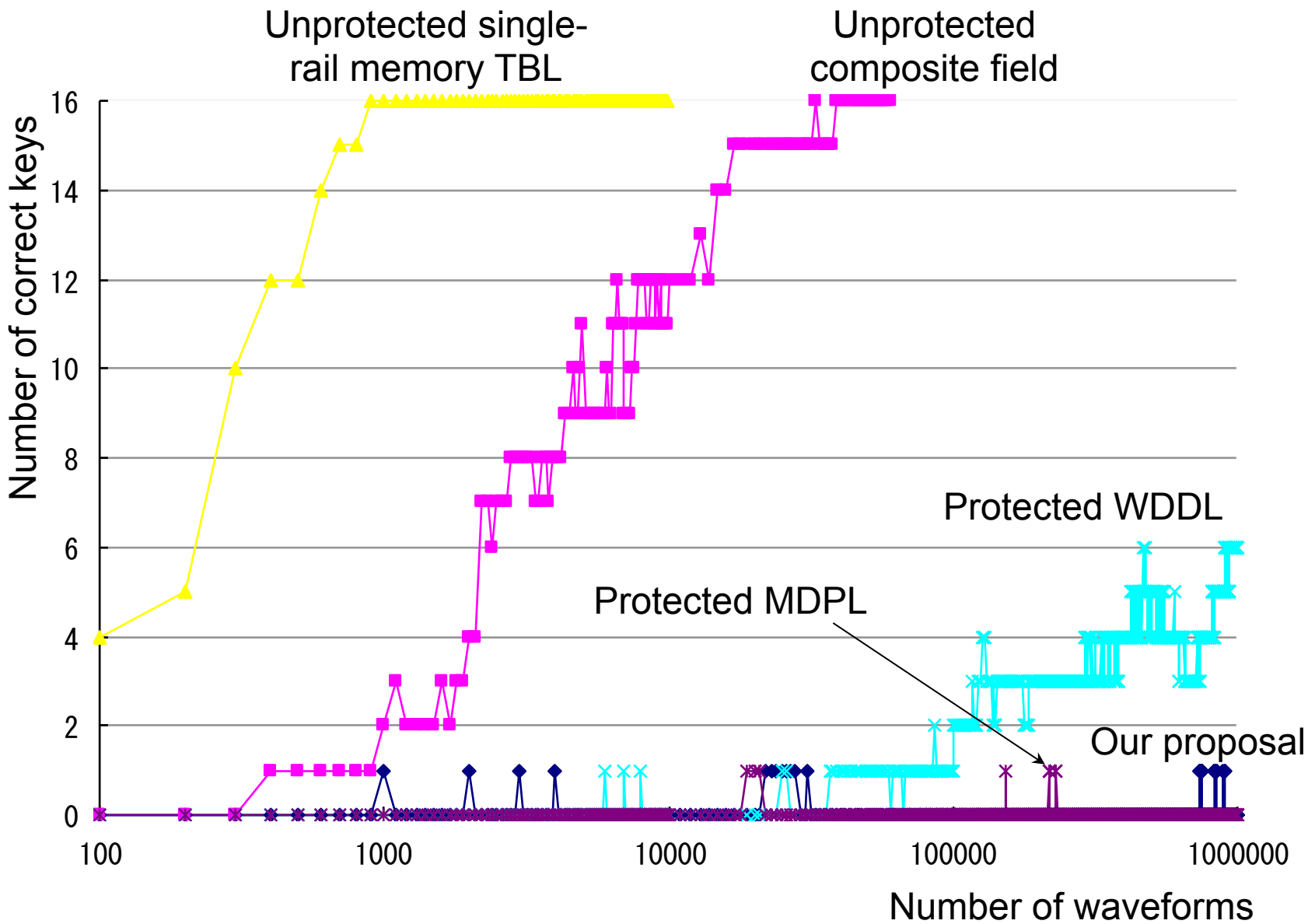
Distributed intra-additive masking dual-rail memory on LUT6



a. Ideally memory with pre-charge, unmask for input and re-mask for output inside

b. Implementation of memory with unmask for input and re-mask for output inside into multi LUTs

HWCPA attack comparison



Hardware size comparison

Implementation methods	No. of slice registers	No. of slice LUTs	Freq (MHz)	Throughput (Mbps)
TBL	405	891	220.1	2,817
Composite	397	1,890	138.9	1,777.8
WDDL	1,160	7,292	56.3	360
MDPL	1,205	12,140	44.4	284
Threshold	1,438	12,627	78.6	503
Dual-rail memory	546	5,898	141.2	1,643

Discussion

- Dual-rail memory implementation is independent with the cryptographic algorithms, so can be used in various non-linear logic
- Standard design flow can be used in the implementation
- AES implementation using dual-rail memory achieves higher throughput but occupies smaller hardware size than other countermeasure methods
- The proposed design is resistant with first order CPA attack

Conclusion and future work

- The conceptual dual-rail memory and its implementation on FPGA
- First-order CPA attack resistant AES implementation on FPGA

Future work

- Verify the implementation using BRAM
- Verify on ASIC

Thank you