MITSUBISHI ELECTRIC
Changes for the Better

COSADE2015

# Two Operands of Multipliers in Side-Channel Attack

Takeshi Sugawara, Daisuke Suzuki, and Minoru Saeki

Mitsubishi Electric Corp.

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

MITSUBISHI ELECTRIC
Changes for the Better

# Overview

- The recent single-shot internal-collision attack is studied focusing on operand order of multipliers
  - The operand order divides success/failure of the attack
  - The causes of the difference are analyzed
    - Integer multipliers
    - Long-integer multiplication algorithm
  - Designing operand order can be a cost-effective way to suppress side-channel leakage

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

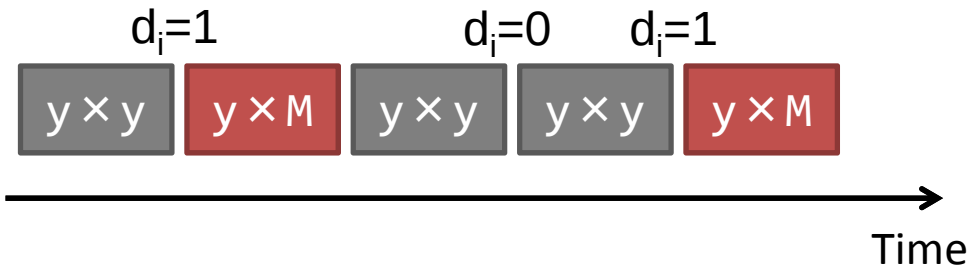
MITSUBISHI ELECTRIC
Changes for the Better

# Background

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# A classical SCA on RSA*

- Distinguish square and multiply to decode the secret key $d_i$




- Example
  - In typical compiler-generated code, "if" branch is faster than "for" branch, and thus they are distinguishable

- Data-dependent branch should be avoided

Binary method

```
y <- 1;
for(i=0; i<N; ++i){
    y <- y×y;
    if(d_i==1){
        y <- y×M;
    }
}
return y;
```

Multiply-always method

```
y[2] <- {1, 1};
for(i=0; i<N; ++i){
    y[1] <- y[1]×y[1];
    y[d_i] <- y[1]×M;
}
return y[1];
```

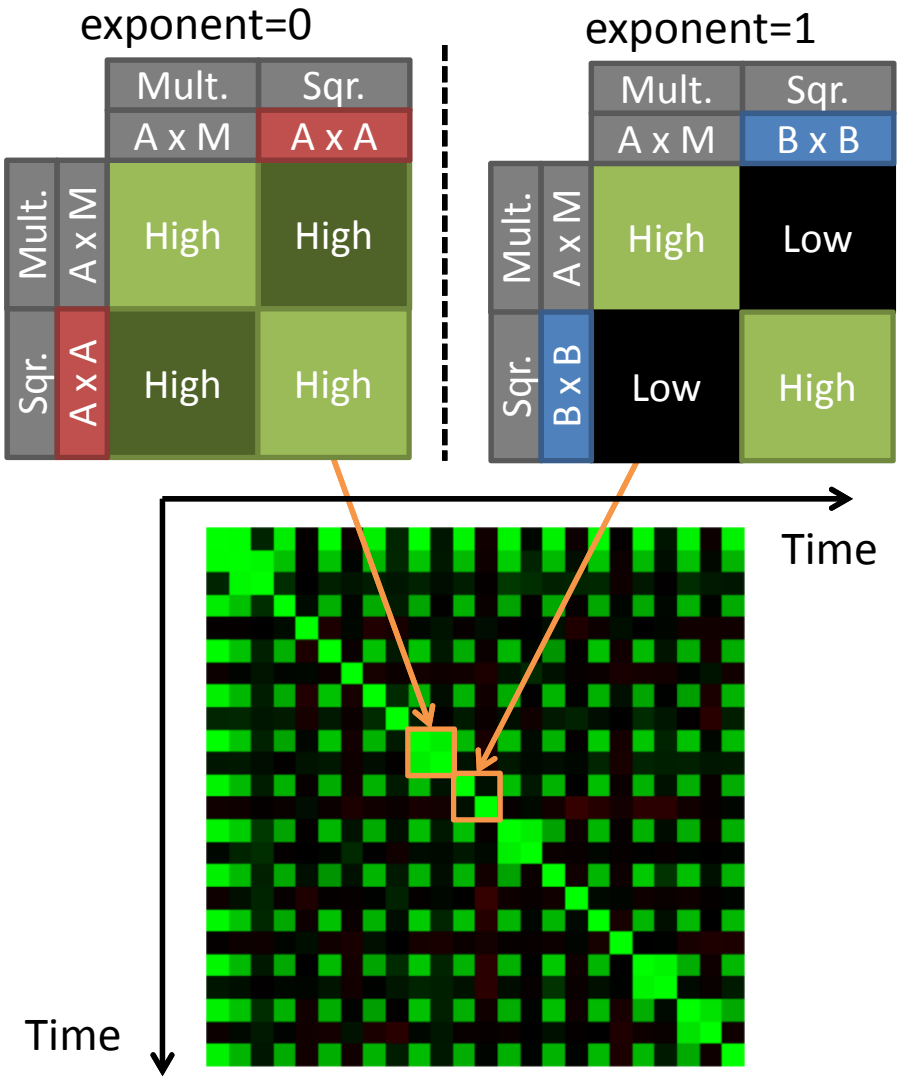
*P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", CRYPTO 1999

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Internal collision attack by Witteman et al.*

- Attacking the multiply-always method
- Idea
  - Consecutive multiply & squaring has exponent-dependent collision
  - The collision is found by looking at the correlation matrix

- The matrix requires multiple RSA calls with the same exponent
  - DPA countermeasures are effective

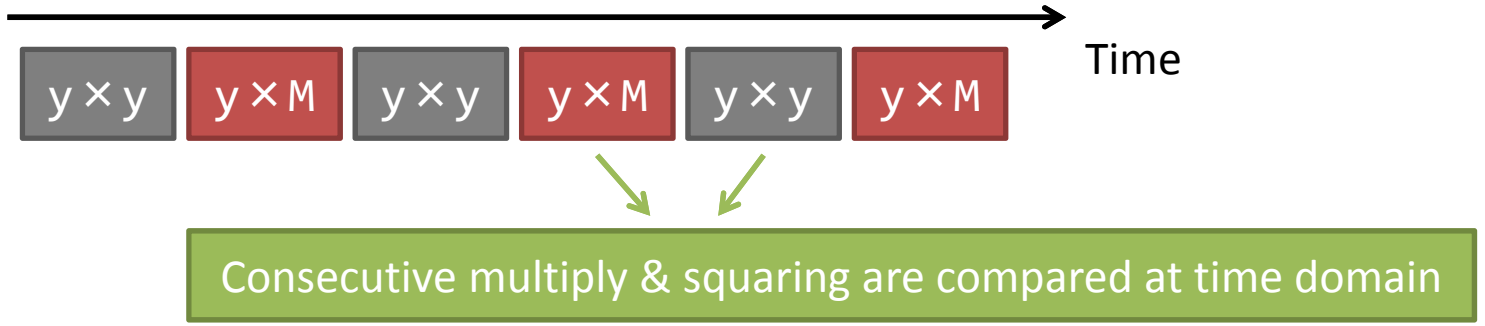



*M. F. Witteman, J.G.J. van Woudenberg, F. Menarini, "Defeating RSA Multiply-Always and Message Blinding Countermeasures," CT-RSA 2011

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Internal collision attack by Hanley et al.*

- Internal collision is detected using a single trace only



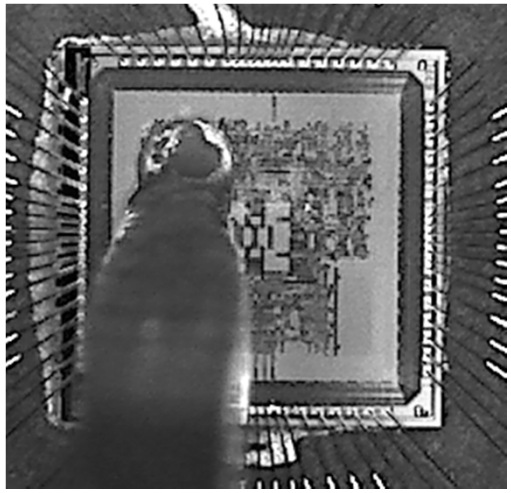

- Pro: defeats DPA countermeasures
- Con: available side-channel info. is limited
  - Feasibility heavily depends on SNR
  - Known results
    - 99% success in software
    - Unsuccessful for FPGA impl. with multiply-always method
      - Low SNR in FPGA

*N. Hanley, H. Kim, and M. Tunstall, "Exploiting Collisions in Addition Chain-based Exponentiation Algorithms Using a Single Trace," eprint 2012/485

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Our first attempt

- Improving the attack using the local-EM measurement
  - Very good SNR
  - Even transistor-level leak is measurable*
- Preliminary experiments
  - Local-EM traces are measured from multiple designs and analyzed with the method by Hanley et al.
  - Success rate greatly differ between the designs
    - We noticed that the operand order determines the difference



A tiny M-field probe on surface of a depackaged chip

T. Sugawara, et al., “On Measurable Side-Channel Leaks Inside ASIC Design Primitives,” CHES 2013

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

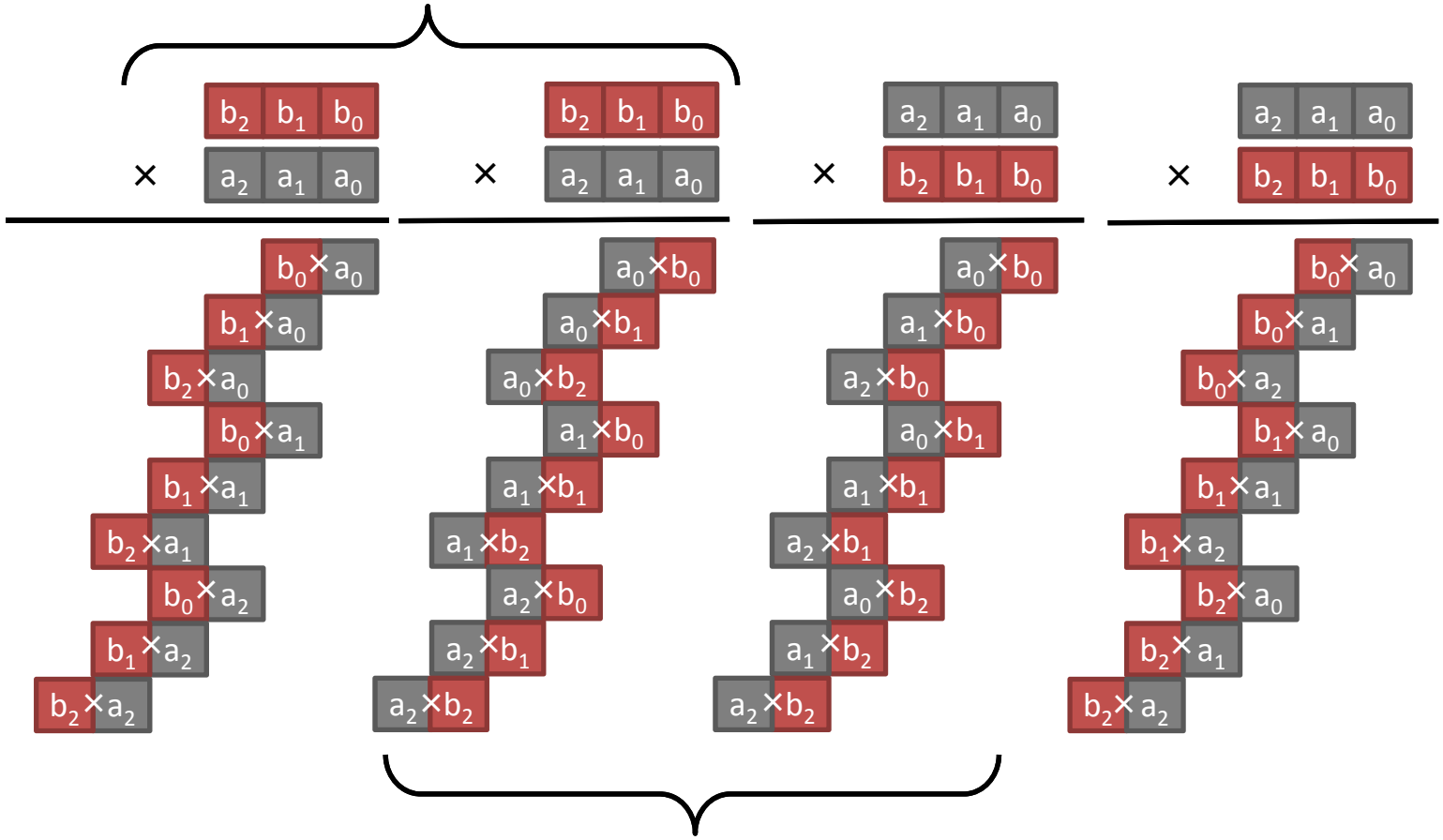
MITSUBISHI ELECTRIC
Changes for the Better

# Operands of multipliers

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Two levels of multiplication

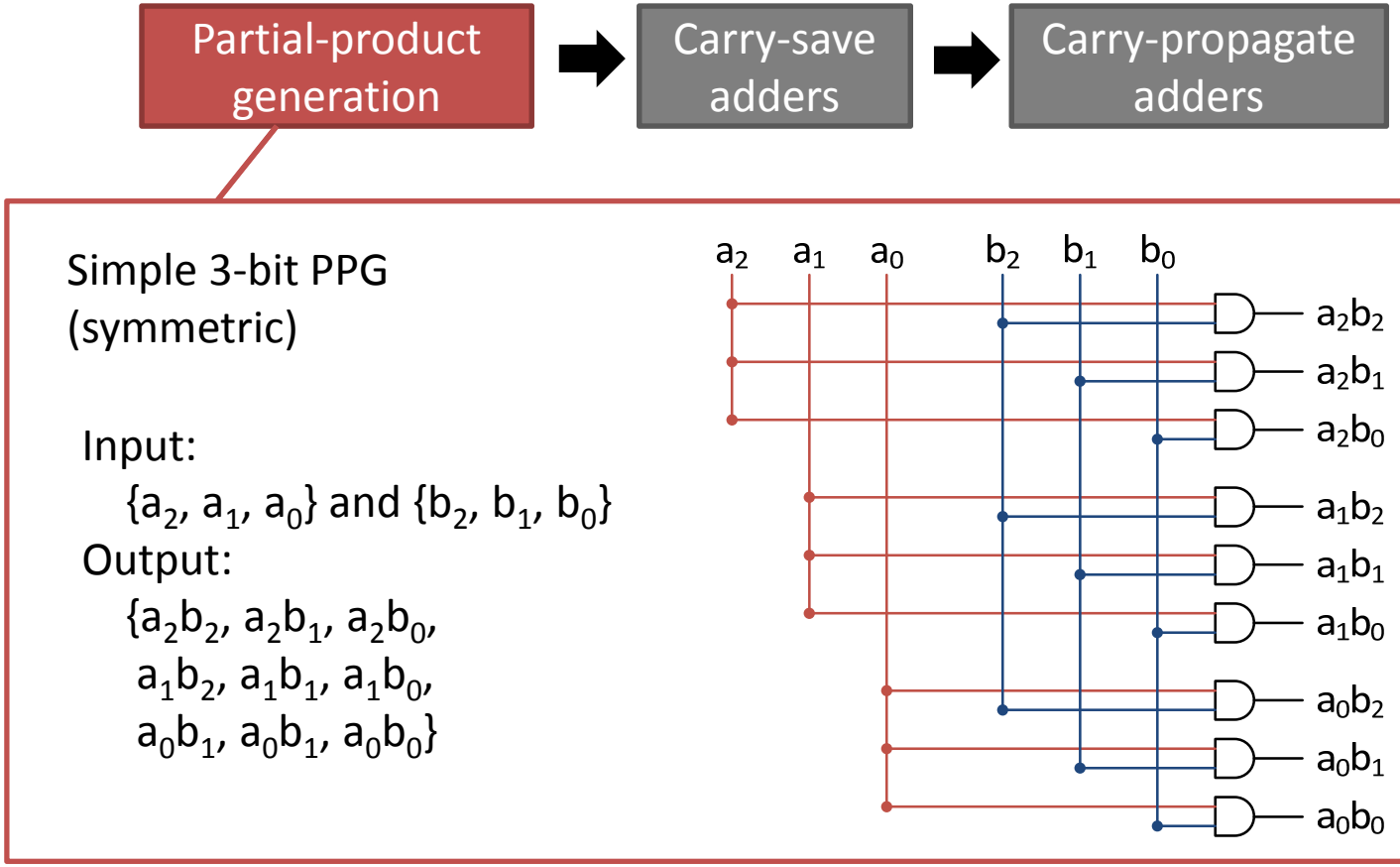
- 1st level: word-size integer multiplier
- 2nd level: long-integer multiplication
- 2x2 possible operand orders




COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Integer multipliers

- Two operands are mixed at the PPG stage
  - The simplest PPG is symmetric*



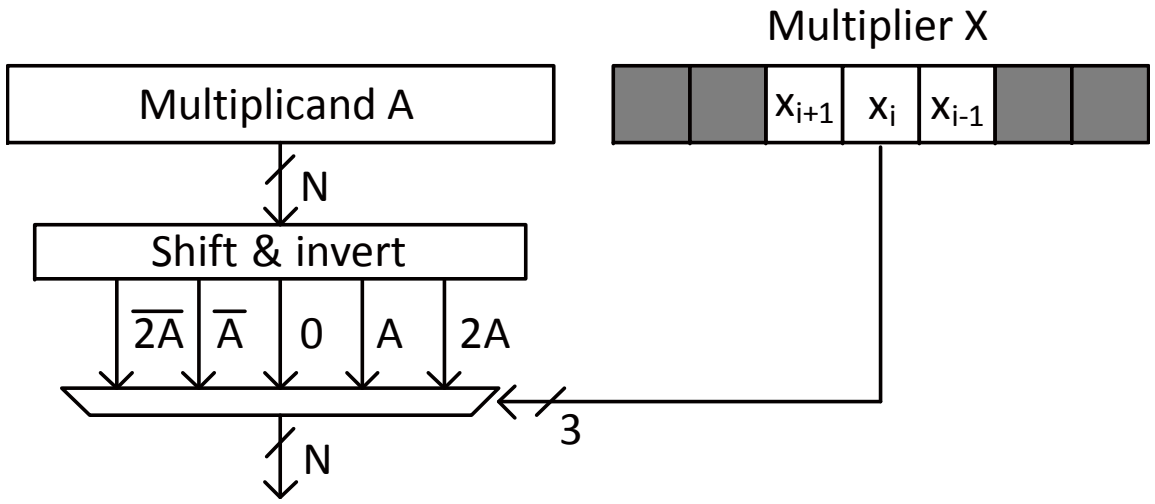

*C. D. Walter, "Sliding Windows Succumbs to Big Mac Attack.," CHES 2001

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Sophisticated PPG: Booth recoding

- Commonly used in commercial logic synthesizers
- Multiplier is recoded with {-2, -1, 0, 1, 2} instead of {0, 1}
  - The number of partial products is reduced
    - Similar idea to the non-adjacent form (NAF)
- The circuit is asymmetric between operands

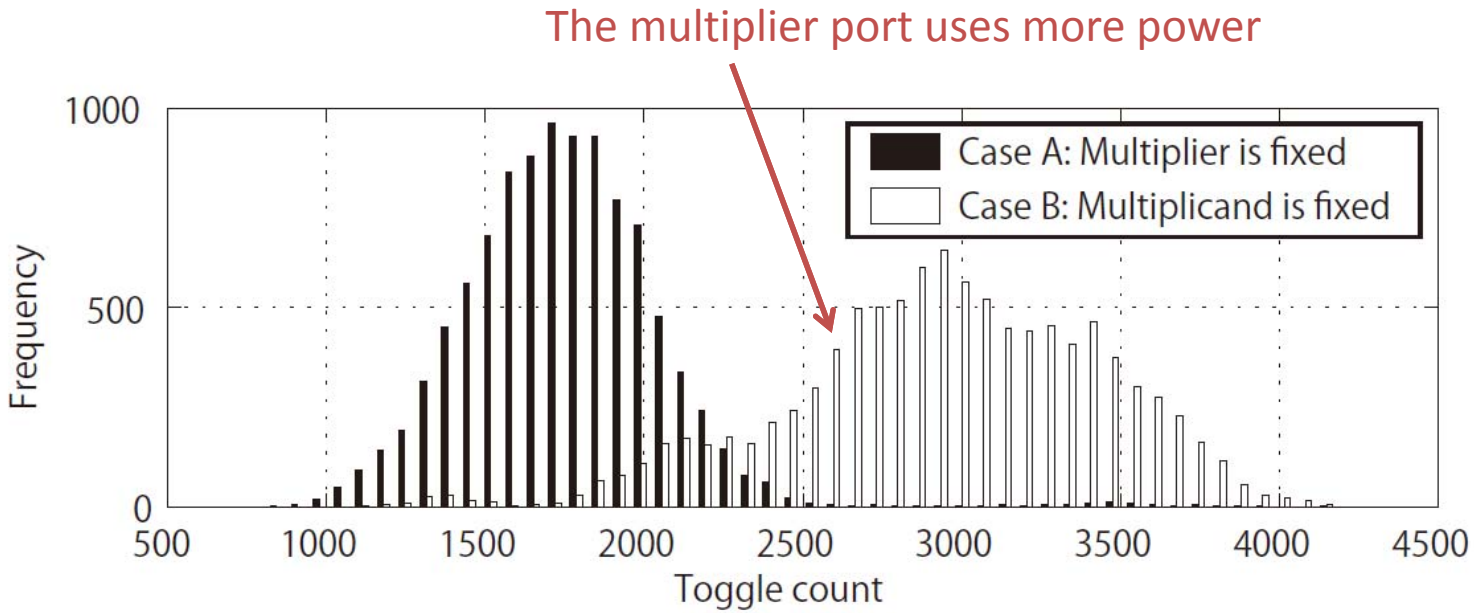
A circuit for generating one partial product with radix-4 Booth recoding




COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Simulating power consumption

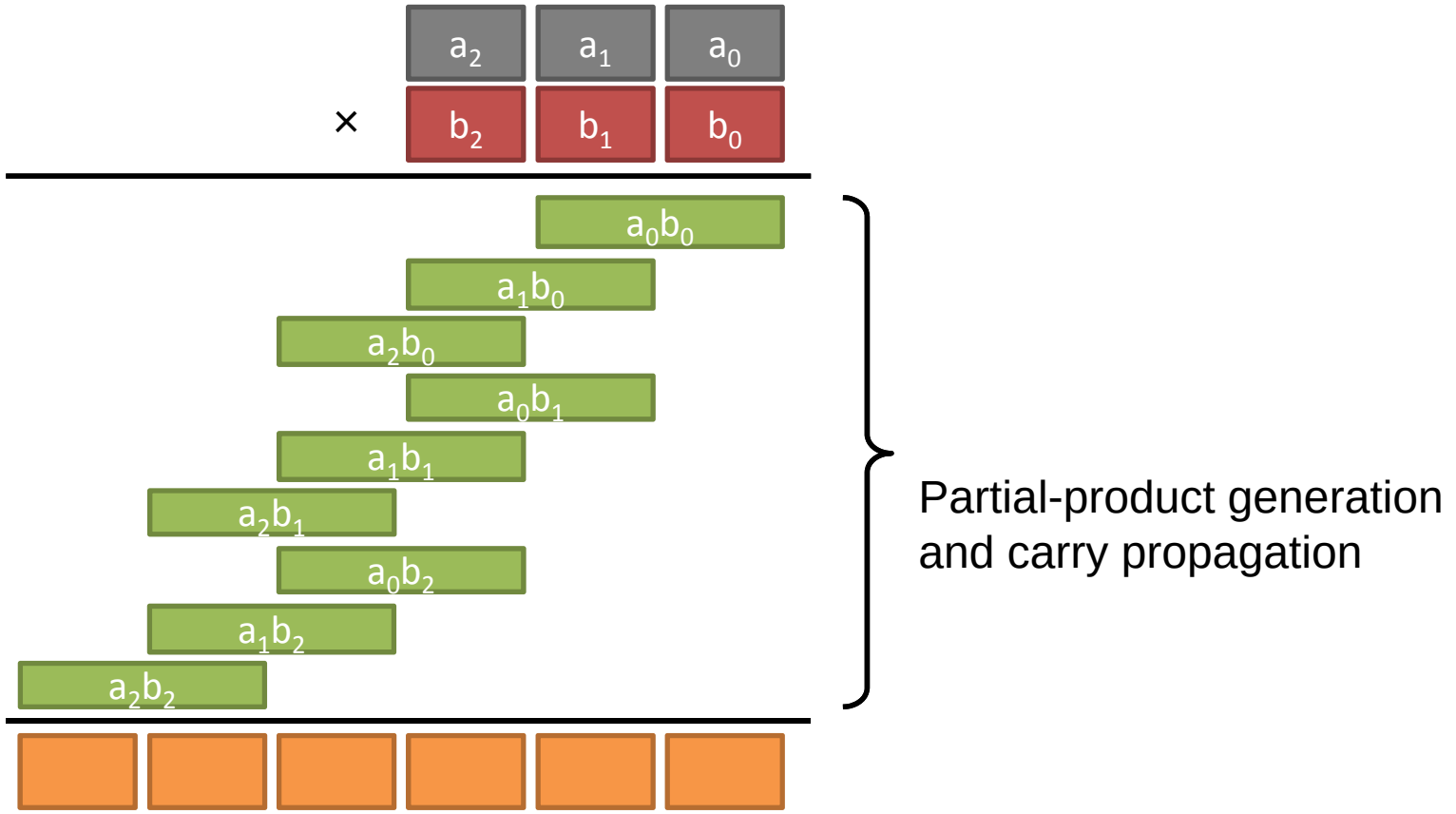
- A 32-bit multiplier with the radix-4 Booth recoding is made
- Post-synthesis logic simulation is conducted while counting the number signal-changing events (i.e., toggles)
- Two types of test vectors
  - $a_i$ x const
  - const x $a_i$
- The multiplier uses more power than the multiplicand




COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Long integer multiplication (LIM)

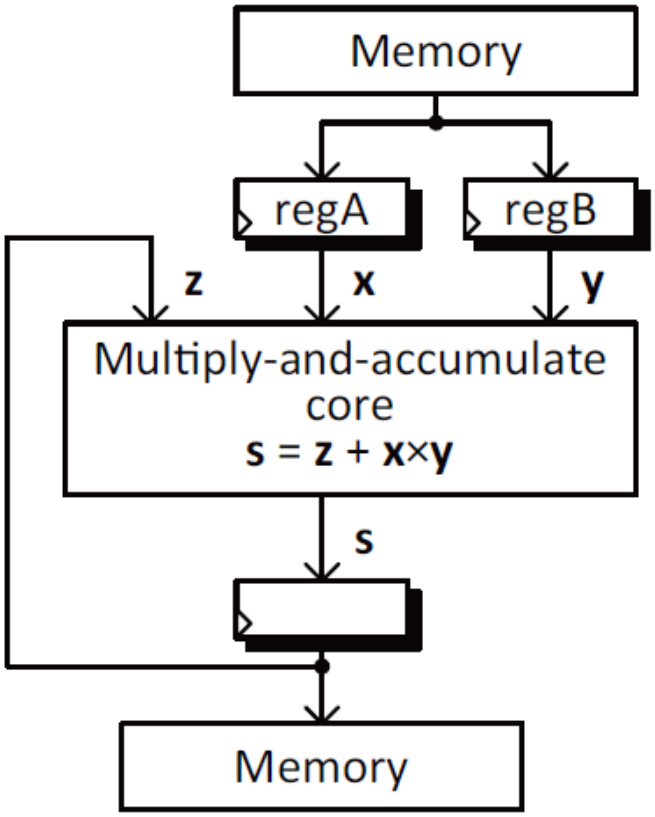
- Varieties
  - Operand scanning
  - Integration with modular reduction (e.g., Montgomery multiplication)

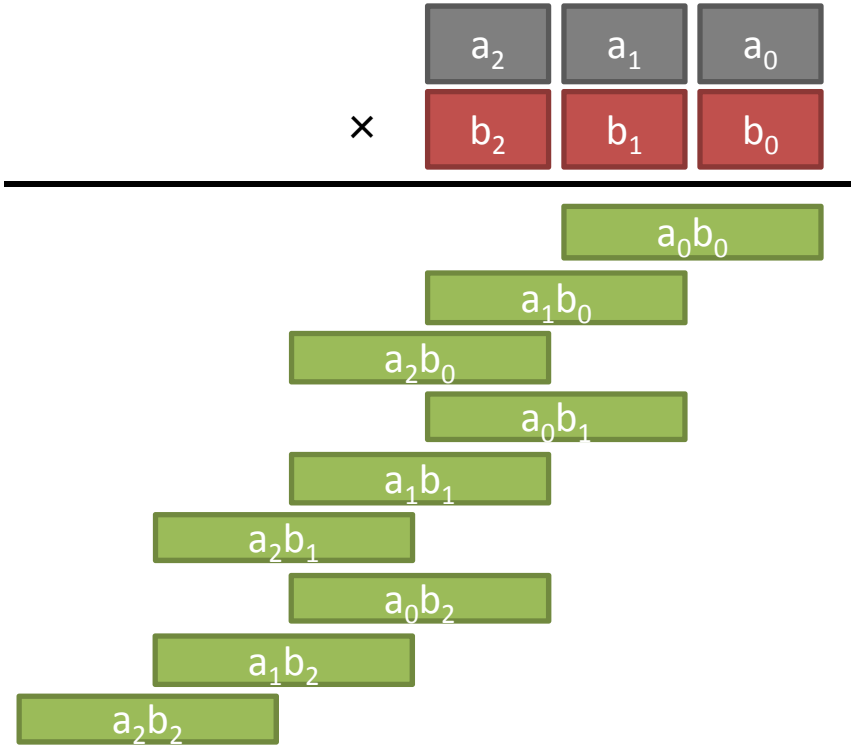



COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Common circuit architecture for LIM

- Use of multiply-and-accumulate (MAC) unit

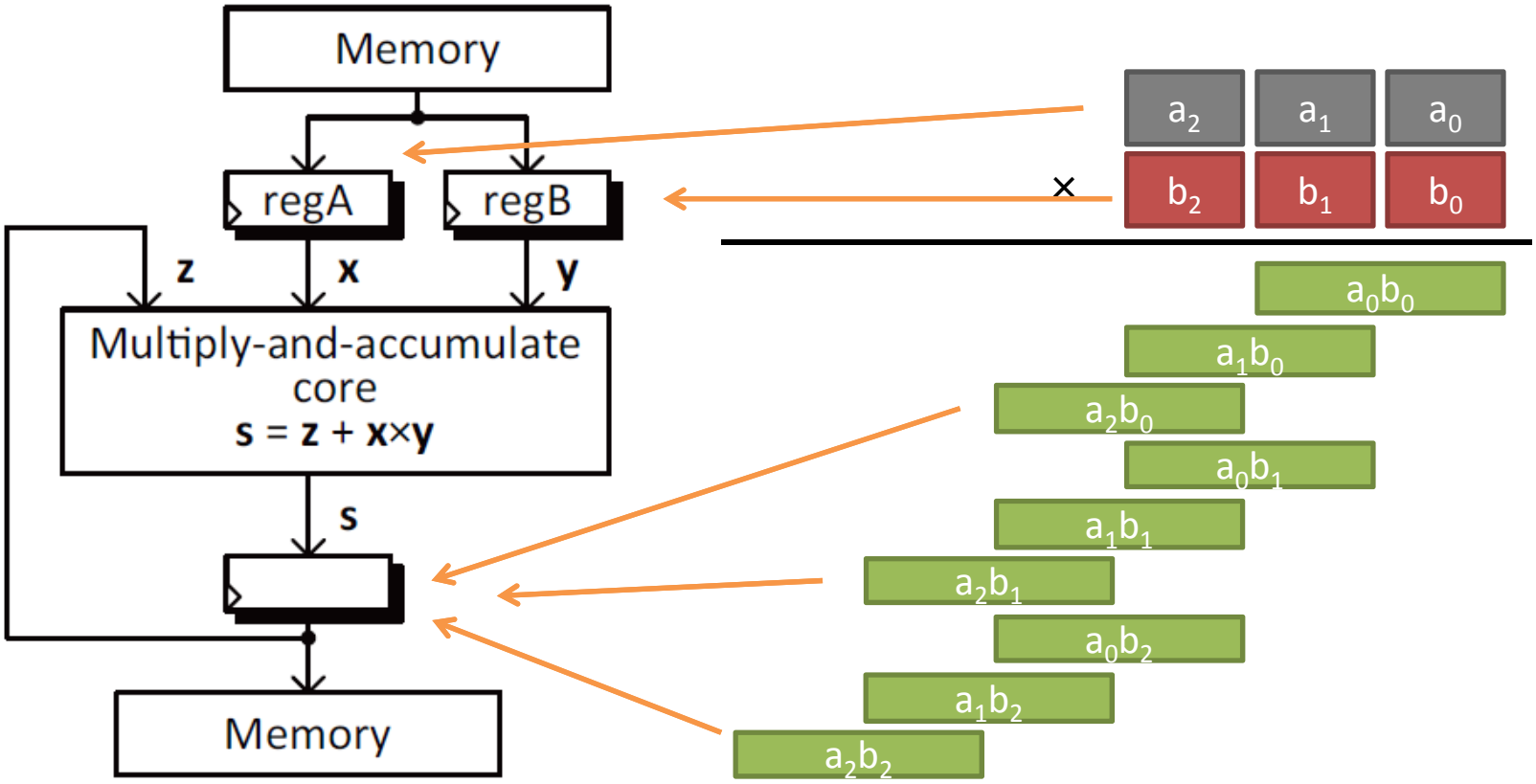



COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Common circuit architecture for LIM

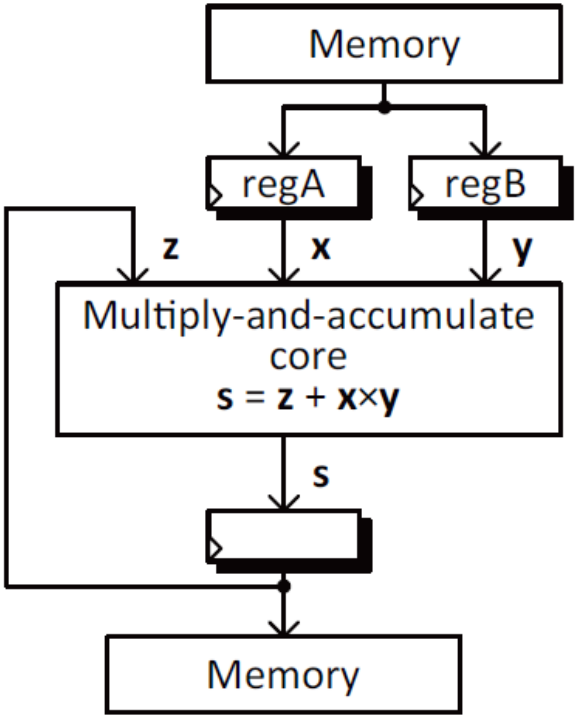
- Use of multiply-and-accumulate (MAC) unit




COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Operand scanning in LIM

- Reading from memory is a common performance bottle neck
  - An operand is cached if possible
  - regB is updated less frequently thus smaller leakage is expected




An operation sequence when s=3

| Seq. no. | regA | regB |
|---|---|---|
| 0 | $a_0$ | $b_0$ |
| 1 | $a_1$ | $b_0$ |
| 2 | $a_2$ | $b_0$ |
| 3 | $a_0$ | $b_1$ |
| 4 | $a_1$ | $b_1$ |
| 5 | $a_2$ | $b_1$ |
| 6 | $a_0$ | $b_2$ |
| 7 | $a_1$ | $b_2$ |
| 8 | $a_2$ | $b_2$ |

scanned at inner loop

scanned at outer loop

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

MITSUBISHI ELECTRIC
Changes for the Better

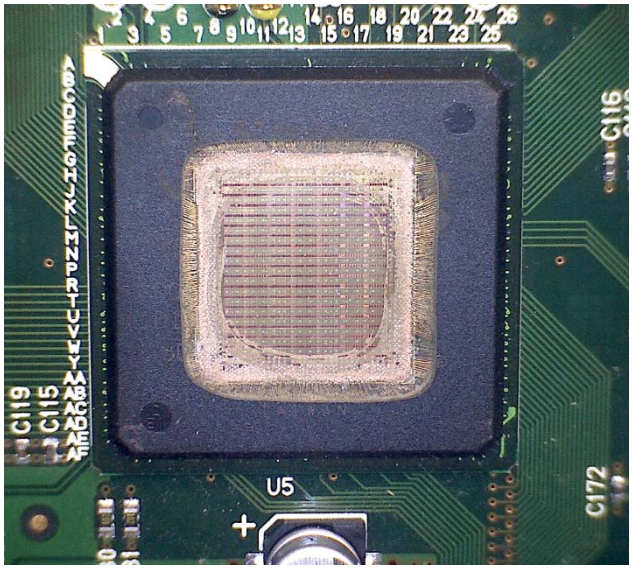
# Experiment

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

MITSUBISHI ELECTRIC
Changes for the Better

# Experiment

- 1024-bit Montgomery multiplier
  - CIOS operand scanning
  - MAC-based architecture with a 64-bit integer multiplier
  - Two operands to the 64-bit integer multiplier are swappable by an external switch
- The circuit is loaded to FPGA and its local-EM traces are measured



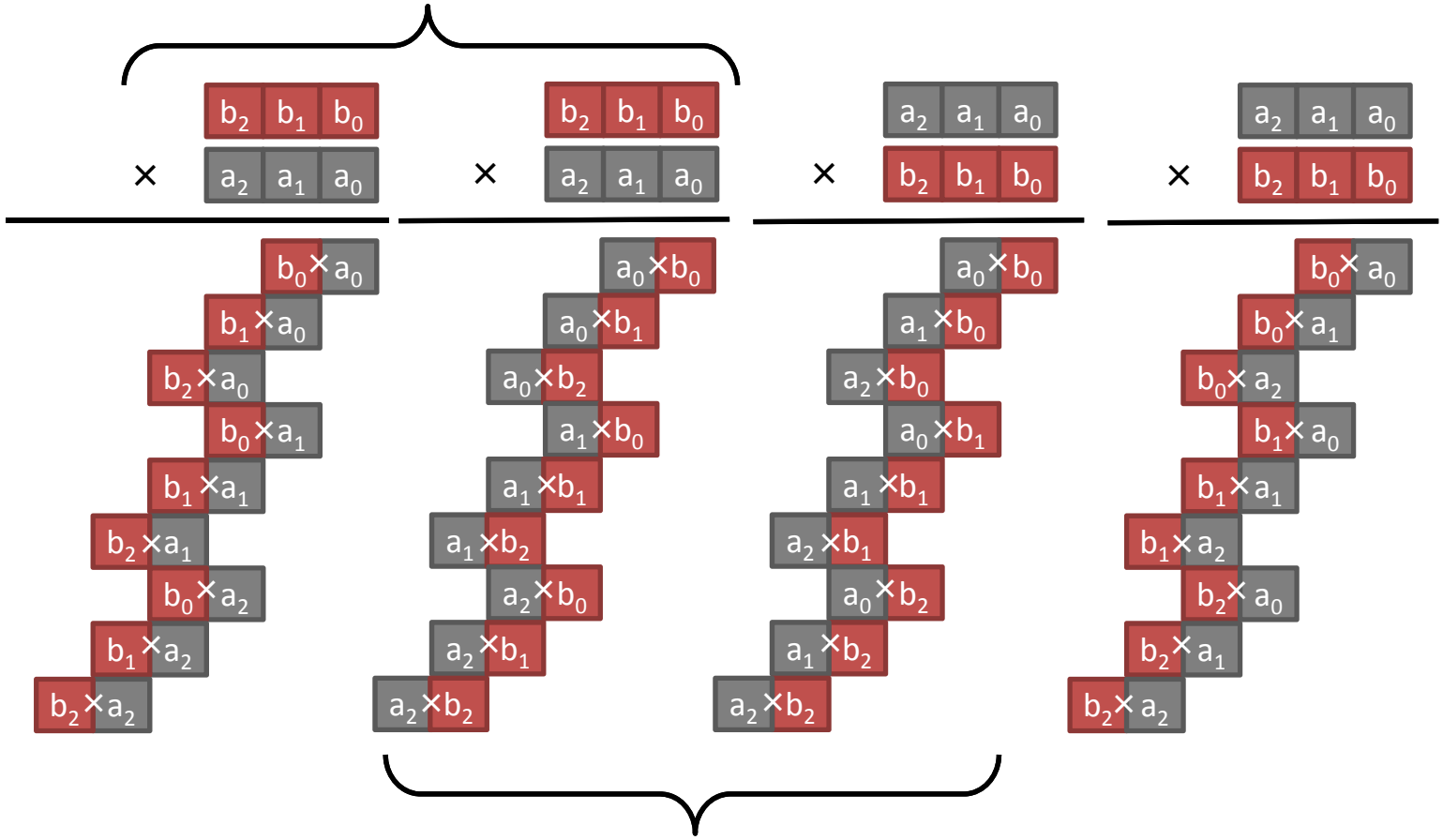

Depackaged FPGA
on SASEBO

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

MITSUBISHI ELECTRIC
Changes for the Better

# Measured cases

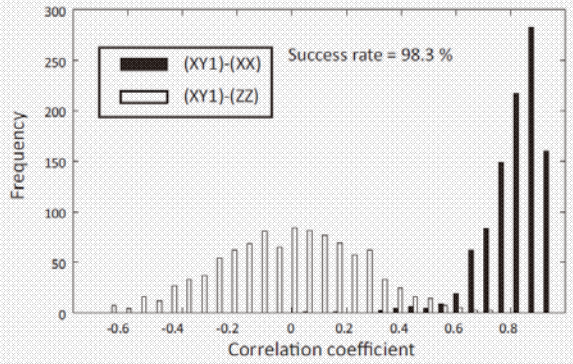
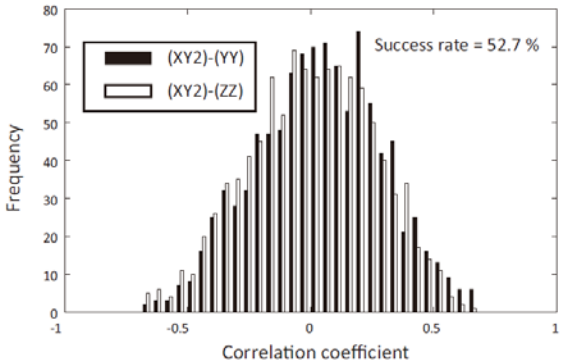
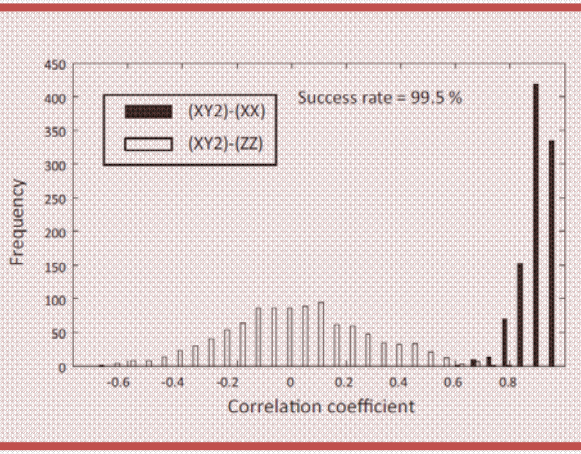
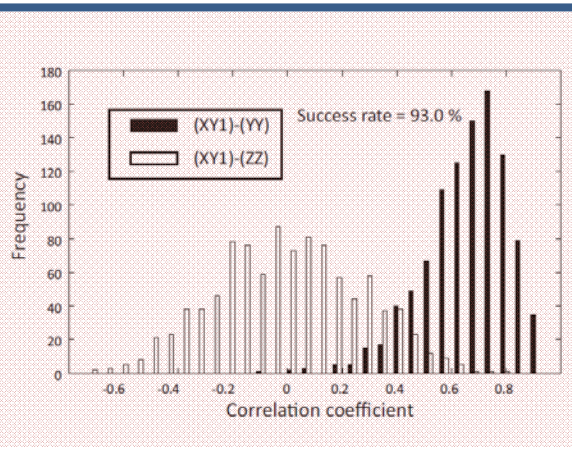
- Test vectors to the Montgomery multiplication is designed to emulate the internal-collision attack of the multiply-always method
- All the possible 2x2 cases are examined




COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

# Result

- The attack results are shown as histograms of correlation coefficients
  - Black bars: correlation with collision, white bars: correlation without collision

| | LIM: collision at inner loop | LIM: collision at outer loop |
|---|---|---|
| integer mult.: collision at multiplicand |  |  |
| integer mult.: collision at multiplier |  |  |







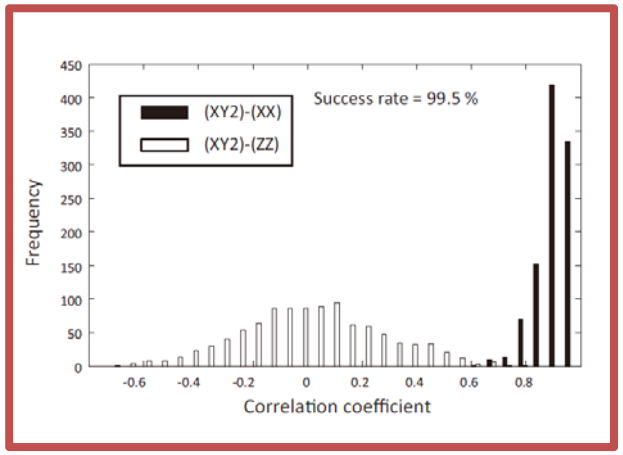


COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

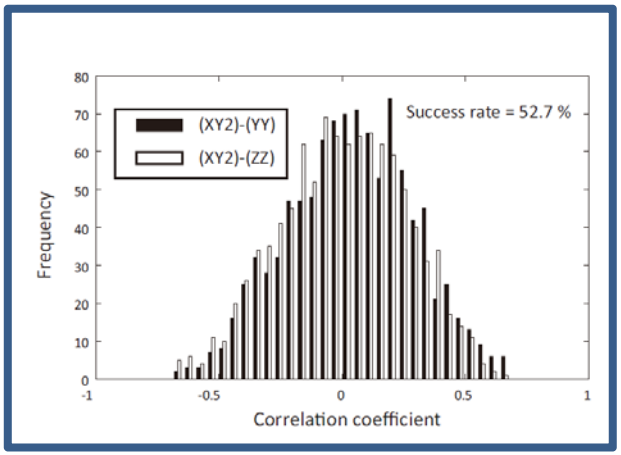
# Countermeasure

- The operand order divided success/failure of the attack

The best: 99.5% success




The worst: 52.7% success




- Designing operand order can be a cost-effective way to suppress side-channel leakage
  - Operand order can be changed for almost no cost
    - The good configuration can be predicted with simulation
  - Reconfiguring operand order after fabrication is also possible at low cost
  - Easy integration with other countermeasures

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.

MITSUBISHI ELECTRIC
Changes for the Better

# Conclusion

- Conclusion
  - Single-shot internal-collision is effective to hardware implementations
    - especially when combined with local EM measurement
  - Small difference like operand order divides success/failure
    - Understanding of low-layer circuits is useful for efficient countermeasures

- Further study
  - How much success rate of the exponent recovery is acceptable?
    - Say, for 80-bit security
  - Randomized operand scanning
  - Collision between input and output?
    - We have never seen exploitable (pure) input-to-output collision so far
    - Sometimes, an input-to-output collision becomes input-to-input collision
      - E.g., an output is immediately read back for the final subtraction

COPYRIGHT © 2014 MITSUBISHI ELECTRIC CORPORATION. ALL RIGHTS RESERVED.