ON 3-SHARE THRESHOLD IMPLEMENTATIONS FOR 4-BIT S-BOXES

Sebastian Kutzner [1] Phuong Ha Nguyen [1,2] Axel Poschmann [1,2]
Huaxiong Wang [2]

[1]Temasek Lab@NTU

[2]MAS-SPMS-NTU, Singapore

7-March-2013

Outline

1. Introduction
2. Threshold Implementation
3. Design
4. Experiments
5. Conclusion

Outline

1. Introduction
2. Threshold Implementation
3. Design
4. Experiments
5. Conclusion

Motivation, Contributions

Motivation and Contributions

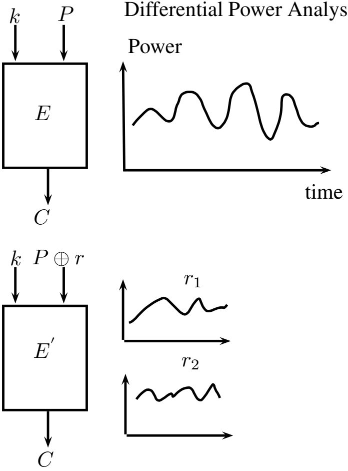
1. Reducing the hardware implementation of 3-share TI for a 4-bit S-box.
2. Implementation of improved 3-share TI of S-box of PRESENT.
3. Side Channel Attack experiments of improved approach.

So, what is TI or 3-share TI and why do we need it?

Outline

1. Introduction
2. Threshold Implementation
3. Design
4. Experiments
5. Conclusion

Threshold Implementations I



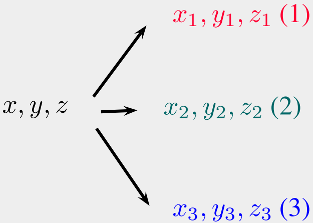
Differential Power Analysis (DPA)

2006, Nikova: Threshold Implementation Countermeasure.

Threshold Implementation II

3-share TI of function $f = z \oplus xy$

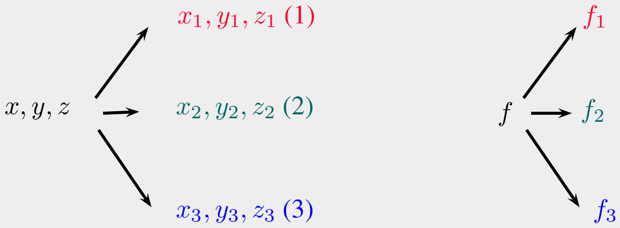
1. $x = x_1 \oplus x_2 \oplus x_3$
   $y = y_1 \oplus y_2 \oplus y_3$
   $z = z_1 \oplus z_2 \oplus z_3$



Threshold Implementation II

3-share TI of function $f = z \oplus xy$

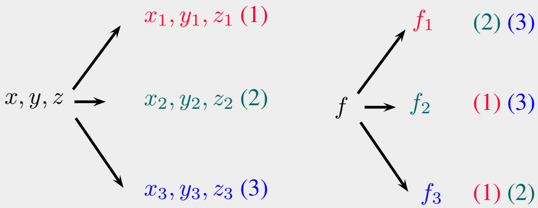
1. $x = x_1 \oplus x_2 \oplus x_3$
   $y = y_1 \oplus y_2 \oplus y_3$
   $z = z_1 \oplus z_2 \oplus z_3$
2. $f = f_1 \oplus f_2 \oplus f_3$



Threshold Implementation II

3-share TI of function $f = z \oplus xy$

1. $x = x_1 \oplus x_2 \oplus x_3$
   $y = y_1 \oplus y_2 \oplus y_3$
   $z = z_1 \oplus z_2 \oplus z_3$
2. $f = f_1 \oplus f_2 \oplus f_3$
3. $f_1 = z_2 \oplus x_2y_2 \oplus x_2y_3 \oplus x_3y_2$
4. $f_2 = z_3 \oplus x_3y_3 \oplus x_1y_3 \oplus x_3y_1$
5. $f_3 = z_1 \oplus x_1y_1 \oplus x_1y_2 \oplus x_2y_1$



x, y, z

x_1, y_1, z_1 (1)

x_2, y_2, z_2 (2)

x_3, y_3, z_3 (3)

f

f_1 (2) (3)

f_2 (1) (3)

f_3 (1) (2)

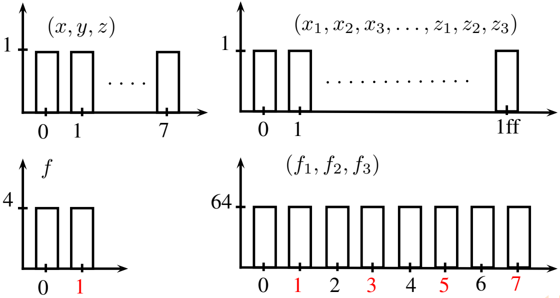
Threshold Implementation II

3-share TI of function $f = z \oplus xy$

1. $x = x_1 \oplus x_2 \oplus x_3$
   $y = y_1 \oplus y_2 \oplus y_3$
   $z = z_1 \oplus z_2 \oplus z_3$
2. $f = f_1 \oplus f_2 \oplus f_3$
3. $f_1 = z_2 \oplus x_2 y_2 \oplus x_2 y_3 \oplus x_3 y_2$
4. $f_2 = z_3 \oplus x_3 y_3 \oplus x_1 y_3 \oplus x_3 y_1$
5. $f_3 = z_1 \oplus x_1 y_1 \oplus x_1 y_2 \oplus x_2 y_1$

$$(x, y, z) \longrightarrow (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3)$$

$$f \longrightarrow (f_1, f_2, f_3)$$

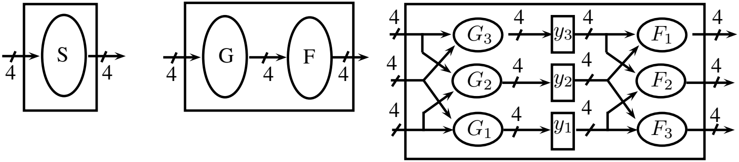


red: $f_1 \oplus f_2 \oplus f_3 = f = 1$

black: $f_1 \oplus f_2 \oplus f_3 = f = 0$

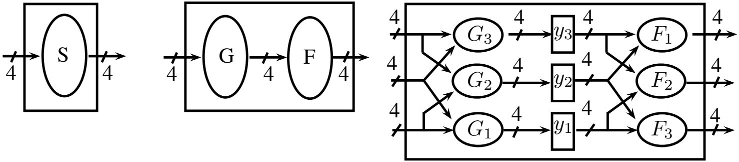
3-share TI to PRESENT S-BOX

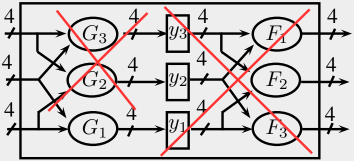
Since degree of S-box S is 3 → 4-share TI.
S=F(G()) where degrees of F and G are two.



3-share TI to PRESENT S-BOX

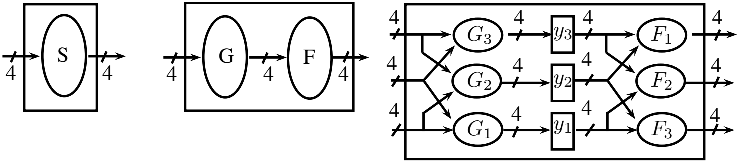
Since degree of S-box S is 3 → 4-share TI.
S=F(G()) where degrees of F and G are two.

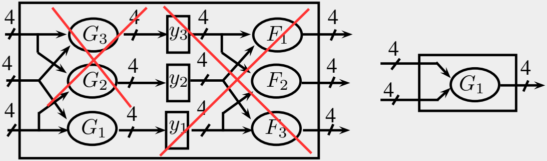




3-share TI to PRESENT S-BOX

Since degree of S-box S is 3 → 4-share TI.
S=F(G()) where degrees of F and G are two.

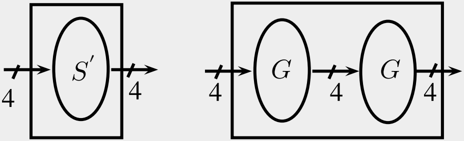




Reducing Hardware Implementation I

1st Observation

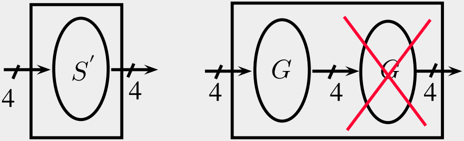
$$S^{'} = G(G())$$



Reducing Hardware Implementation I

1st Observation

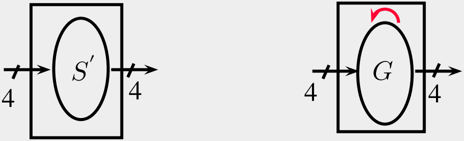
$$S^{'} = G(G())$$



Reducing Hardware Implementation I

1st Observation

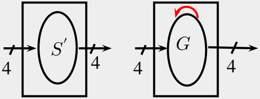
$$S^{'} = G(G())$$



Reducing Hardware Implementation I

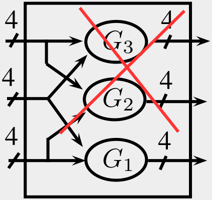
1st Observation

$S' = G(G())$



2nd Observation

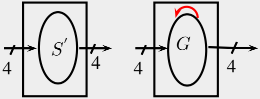
$G_1 \approx G_2 \approx G_3$



Reducing Hardware Implementation I

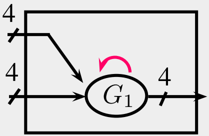
1st Observation

$S' = G(G())$



2nd Observation

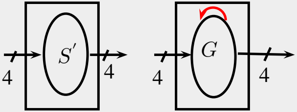
$G_1 \approx G_2 \approx G_3$



Reducing Hardware Implementation I

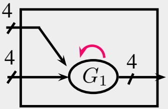
1st Observation

$S^{'} = G(G())$

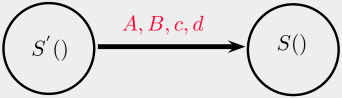


2nd Observation

$G_1 \approx G_2 \approx G_3$



3rd Observation

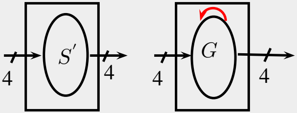


$$S^{'}() = G(G())$$
$$S(x) = A(S^{'}(Bx \oplus c) \oplus d)$$
$$S(x) = A(G(G(Bx \oplus c)) \oplus d)$$

Reducing Hardware Implementation I

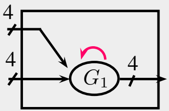
1st Observation

$S' = G(G())$

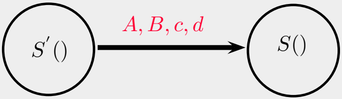


2nd Observation

$G_1 \approx G_2 \approx G_3$

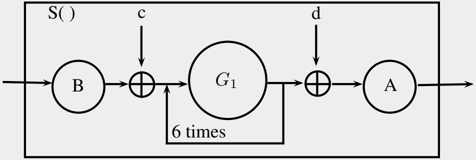


3rd Observation

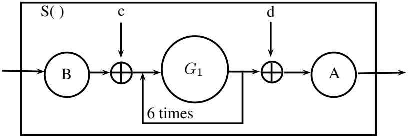


$$S'() = G(G())$$
$$S(x) = A(S'(Bx \oplus c) \oplus d)$$
$$S(x) = A(G(G(Bx \oplus c)) \oplus d)$$

Result



Reducing Hardware Implementation II



Improved 3-share TI to PRESENT S-BOX

1. S:=[12, 5, 6, 11, 9, 0, 10, 13, 3, 14, 15, 8, 4, 7, 1, 2]
2. G:=[0, 4 , 1, 5, 2, 15, 11, 6, 8, 12, 9, 13, 14, 3, 7, 10]
3. $$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$
4. $c = (0001)_2 = 1, \; d = (0101)_2 = 5$
5. $S(x) = A(S^{'}(Bx \oplus c) \oplus d) = A(G(G(Bx \oplus c)) \oplus d), \forall x \in \{0, \ldots, 15\}$

Outline

1 Introduction

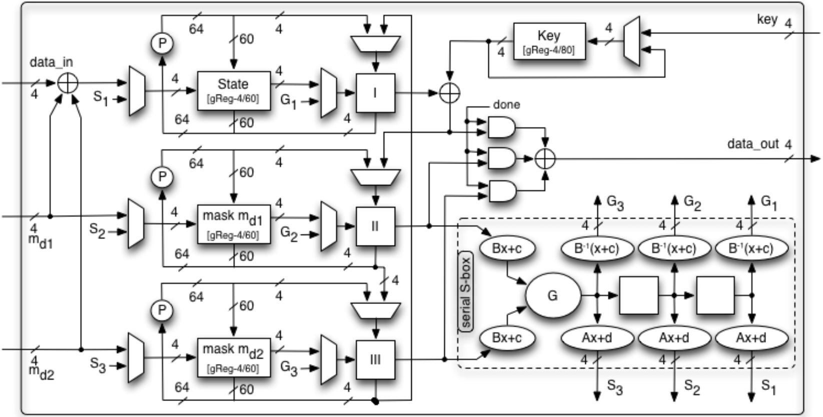
2 Threshold Implementation

3 Design

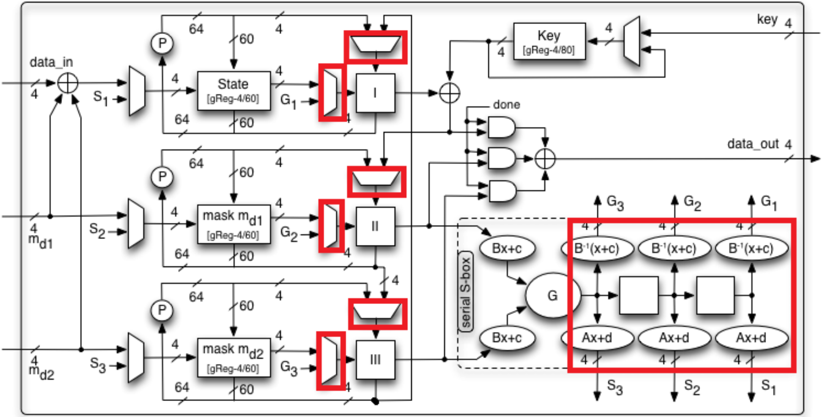
4 Experiments

5 Conclusion

Improved Design I



Improved Design I



Improved Design II

Table : Area savings for different implementation strategies.

Architecture Strategy	S-box Savings	Storage Strategy	S-box Area share	Overall Savings	Time Overhead
serial	-37.0%	D-FF + en	11.4%	-4.2%	
		s-FF + cg	15.7%	-5.8%	5.2
round-based	-40.6%	D-FF + en	61.8%	-25.1%	
		s-FF + cg	67.9%	-27.6%	3

Outline

1 Introduction

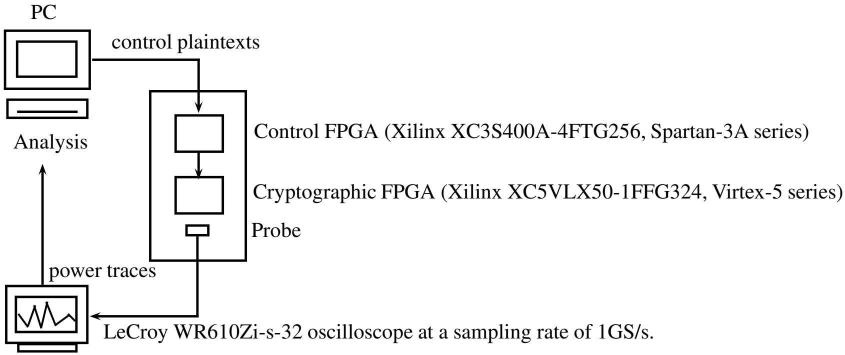
2 Threshold Implementation

3 Design

4 Experiments

5 Conclusion

Experiment setup



PC

control plaintexts

Control FPGA (Xilinx XC3S400A-4FTG256, Spartan-3A series)

Analysis

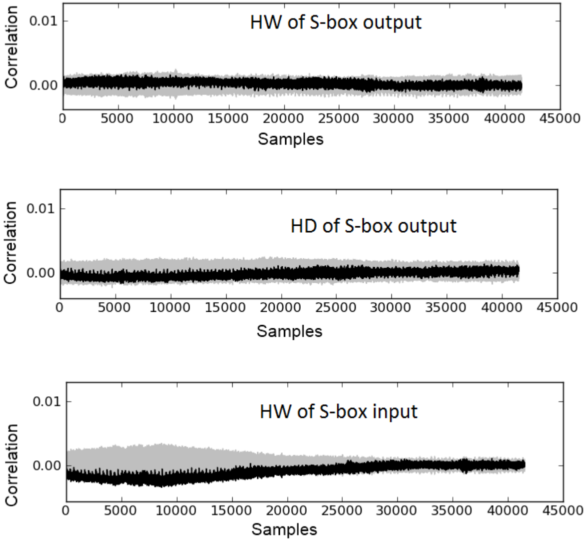
Cryptographic FPGA (Xilinx XC5VLX50-1FFG324, Virtex-5 series)

Probe

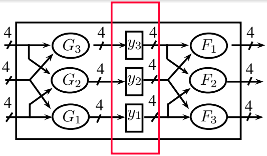
power traces

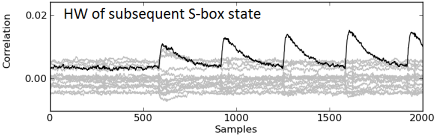
LeCroy WR610Zi-s-32 oscilloscope at a sampling rate of 1GS/s.

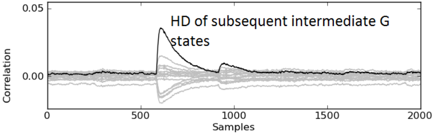
The same security level: 5 million traces

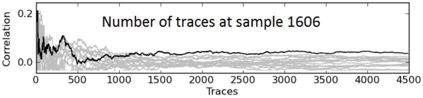


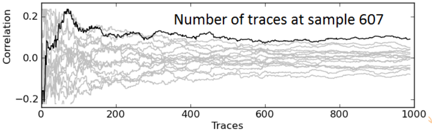
Higher sensitive point for attack





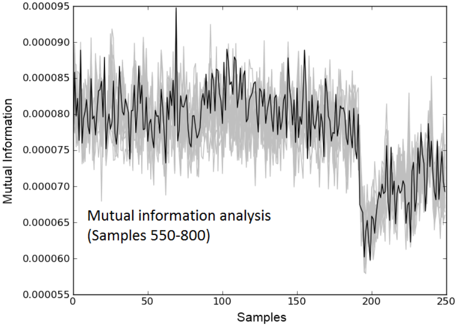


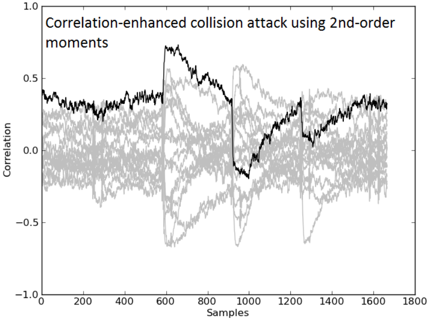




MIA and correlation-enhanced collision attack I

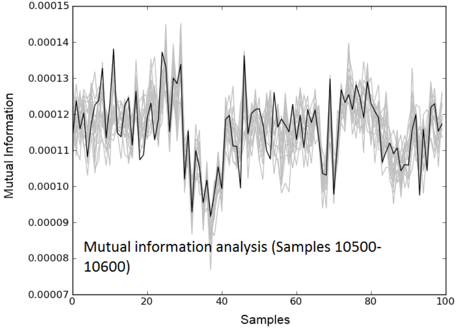
1) 10,000,000 traces of this implementation and mounted both attacks targeting HD of consecutive outputs of the *G*-stage of original approach.
2) First successful practical MIA on TI.
3) Correlation-enhanced collision attack requires less traces than MIA.

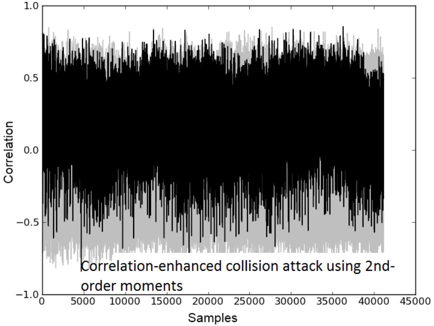




MIA and correlation-enhanced collision attack II

1) Sources for univariate leakage, e.g. the state update.
2) must be carefully serialized for every clock cycle, which is ongoing work.


Mutual information analysis (Samples 10500-10600)


Correlation-enhanced collision attack using 2nd-order moments

Wagner's zero-offset attack

1. Only works against the two-share masking scheme for the simulation.
2. Does not work against TI.
3. In order to attack against TI, the attack should be modified, i.e., by raising the mean-free measurement values to the power of three instead of squaring.
4. 100 times worse than MIA (in simulation), which shows how sensitive this attack is against noise and why it does not work in practice.

Outline

1 Introduction

2 Threshold Implementation

3 Design

4 Experiments

5 Conclusion

1. Two methodologies reducing the hardware implementation of TI are introduced.
2. A new design of 3-share TI for PRESENT's S-box is suggested.
3. Practical experiments show the security level of the new approach.

THANK YOU FOR LISTENING.