NPTEL ONLINE CERTIFICATION COURSES

Course Name: Hardware Security

Faculty Name: Prof Debdeep Mukhopadhyay

Department : Computer Science and Engineering

Topic

Lecture 45: Power Analysis Countermeasures

CONCEPTS COVERED

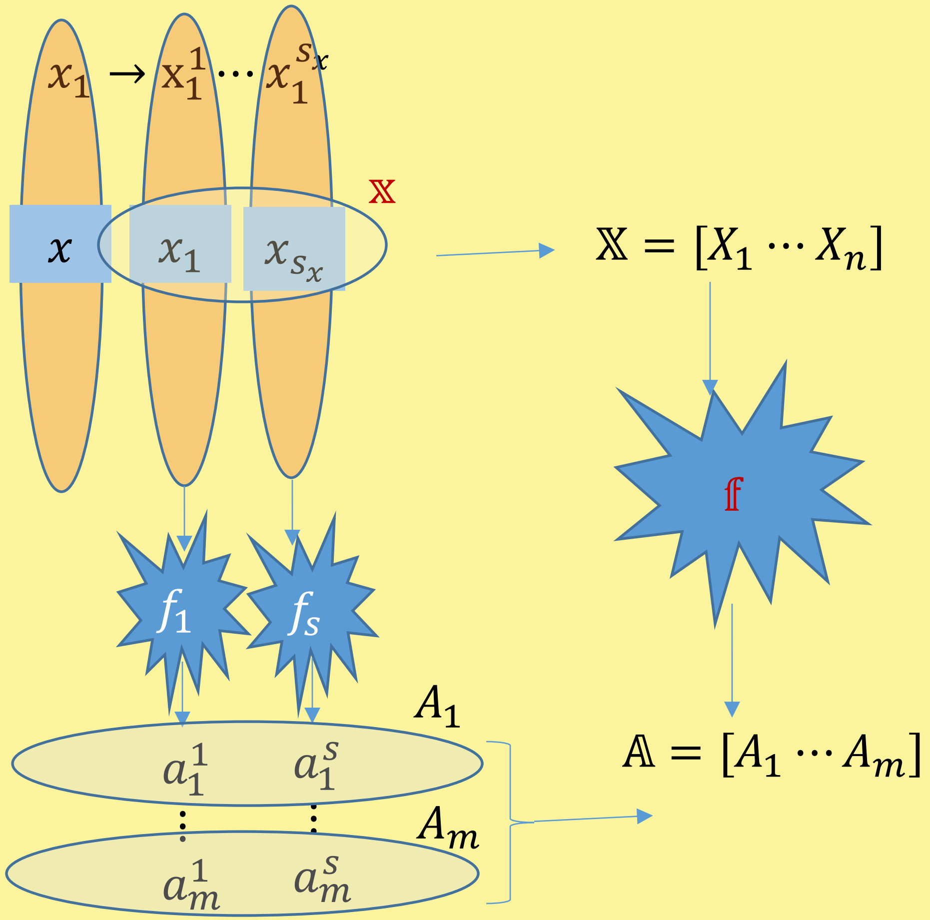
Concepts Covered:

- Properties of TI
- Some Constructions
- Experimental Evaluations and Results

Correctness

$$f(x_1, \cdots, x_n) \rightarrow (a_1, \cdots, a_m)$$

For all $a \in F_2^m, \mathbb{A} = \mathbb{f}(\mathbb{X})$, implies that $a = \Sigma_i a_i = \Sigma_i f_i(\mathbb{x})$, for all $\mathbb{x}$ satisfying $\Sigma x_i = x, x \in F_2^n$



Uniform Masking

- For all values with $\Pr[X = x] > 0$, let $Sh(x)$ denote the set of valid share vectors $\mathbb{x}$ for x:

$$Sh(x) = \left\{\mathbb{x} \in F_2^{ns_x} \middle| x_1 \oplus \cdots \oplus x_{s_x} = x\right\}$$

- $Pr[\mathbb{X} = \mathbb{x}|X = x]$ denotes the probability that $\mathbb{X} = \mathbb{x}$ when the unshared input is x, taken over all the auxiliary inputs of the masking.

Uniform Masking: A masking X is uniform if and only if there exists a constant p such that $\forall x$ we have: if $\mathbb{x} \in Sh(x)$, then $Pr[\mathbb{X} = \mathbb{x}|X = x] = p$, else $Pr[\mathbb{X} = \mathbb{x}|X = x] = 0$, *and* $\Sigma_{\mathbb{x} \in Sh(x)} \Pr[\mathbb{X} = \mathbb{x}] = \Pr[X = x]$

Uniformity of a masking implies that the independence of the combination of any $s_x - 1$ shares, satisfying an (s_x, s_x) secret sharing scheme.

Proof

- Define, $\mathbb{X}_i$ as the r.v denoting the i^th share. Then $\mathbb{X}_{\bar{i}}$ denotes the vector without the i^th share
- If masking is uniform$\Rightarrow$ $\mathbb{x}_{\bar{i}}$ and x are independent for any i.
- $Pr[\mathbb{X} = \mathbb{x} | X = x] = \Pr[\mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}}, \mathbb{X}_i = \mathbb{x}_i | X = x] = \frac{\Pr[\mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}}, \mathbb{X}_i = \mathbb{x}_i, X = x]}{\Pr[X = x]} = \frac{\Pr[\mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}}, \mathbb{X}_i = \mathbb{x}_i, X = x]}{\Pr[X = x, \mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}}]} \frac{\Pr[\mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}}, X = x]}{\Pr[X = x]}$

$$= \Pr[\mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}} | X = x] \Pr[\mathbb{X}_i = \mathbb{x}_i | X = x, \mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}}]$$

The last factor equals 1 when $\mathbb{x} \in Sh(x)$ and zero otherwise.

Thus, $\forall x, \Pr[\mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}} | X = x] = p.$

$\therefore \Pr[\mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}}] = \Sigma_x \Pr[\mathbb{X}_{\bar{i}} = \mathbb{x}_{\bar{i}} | X = x] \Pr[X = x] = p = 2^{n(1-s_x)}$

Non-Completeness

- Masked Circuit:
  - $f_1(X_1, Y_1) = Z_1 \oplus X_1Y_1$
  - $f_2(X_1, X_2, Y_1, Y_2) = \left((Z_2 \oplus X_1Y_2) \oplus X_2Y_1\right) \oplus X_2Y_2$
  - Note, f_2 depends on all the 2 shares. Therefore an attacker probing the corresponding wire can observe all the information required.
  - A TI on the other hand ensures that if the attacker probes d wires, it can only provide information for at most $s_{in} - 1$ shares, which is independent of the sensitive data.
- d-th order Non-completeness: Any combination of up to d component functions f_i of $\mathbb{f}$ *must be independent of at least one input share.*

Security Guarantee

- If the input mask $\mathbb{X}$ of the shared function $\mathbb{f}$ is a uniform masking and $\mathbb{f}$ is a d-th order TI then the d-th order analysis on the power consumptions of a circuit implementing $\mathbb{f}$ does not reveal the unmasked input value x even if the inputs are delayed or glitches occur in the circuit.

Sharing of Affine Functions

- An affine function $f(X) = A$ can be implemented with $s \geq d + 1$ component functions to thwart d-th order attacks.
- Construction:

$$f_1(X_1) = A_1 = f(X_1),$$

For $2 \leq i \leq s, f_i(X_i) = A_i$, where f_i is f without constant terms.

  - Eg, $f(X) = 1 \oplus X \Rightarrow f_1(X_1) = 1 \oplus X_1, f_i(X_i) = X_i, 2 \leq i \leq s$

What if the input is not uniform?

- Let, $(X, Y) \in F_2^2, A = f(X, Y) = XY$.
- Following is a 1st order TI:
  - $A_1 = f_1(X_2, X_3, Y_2, Y_3) = X_2Y_2 \oplus X_2Y_3 \oplus X_3Y_2$
  - $A_2 = f_2(X_1, X_3, Y_1, Y_3) = X_3Y_3 \oplus X_1Y_3 \oplus X_3Y_1$
  - $A_3 = f_3(X_1, X_2, Y_1, Y_2) = X_1Y_1 \oplus X_1Y_2 \oplus X_2Y_1$

Uniformity Analysis

$$X = 0 \Rightarrow X = X_1 \oplus X_2 \oplus X_3 = 0$$
$$Y = 0 \Rightarrow Y = Y_1 \oplus Y_2 \oplus Y_3 = 0$$

Distribution of (A_1, A_2, A_3)

	000	011	101	110
000	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)
011	(0,0,0)	(1,1,0)	(1,0,1)	(0,1,1)
101	(0,0,0)	(1,0,1)	(0,1,1)	(1,1,0)
110	(0,0,0)	(0,1,1)	(1,1,0)	(1,0,1)

Uniformity Analysis

	a_1, a_2, a_3							
(x, y)	000	011	101	110	001	010	100	111
$(0, 0)$	7	3	3	3	0	0	0	0
$(0, 1)$	7	3	3	3	0	0	0	0
$(1, 0)$	7	3	3	3	0	0	0	0
$(1, 1)$	0	0	0	0	5	5	5	1

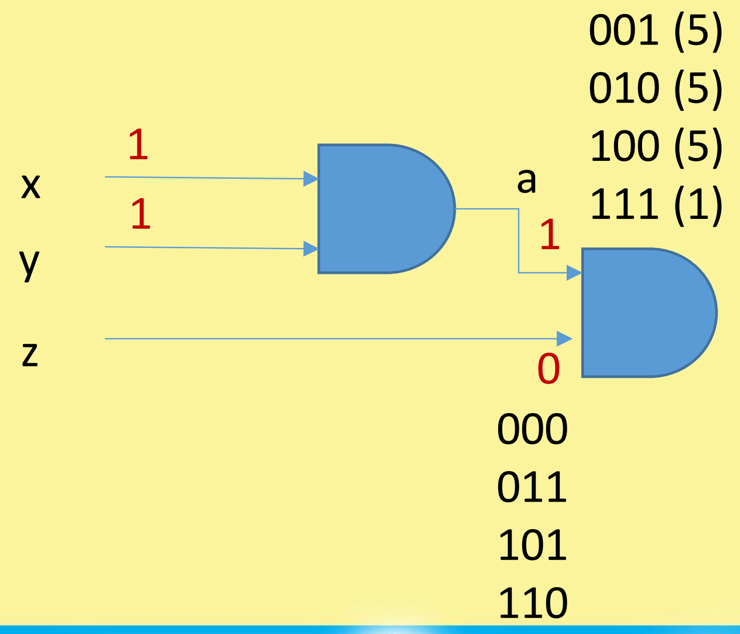
As the input masking (X,Y) is uniform, and the circuit is a first order TI, the circuit itself does not leak vs a 1st order DPA adversary.

The average Hamming weights does not depend on (x,y).
For example, if (x,y)=(0,1), average HW=(3x2)x3/16=18/16. If (x,y)=(1,1), average HW=((5x1)x3+3x1)/16=18/16

But what if this circuit is fed as an input to a second circuit?

Uniformity Analysis

- Let B=g(Z,A)=ZA, and this multiplication is implemented with similar equations.
- Assume Z is uniform, and A is the output of the previous circuit.



000	5+5+5+5+5+5+1=31
011	5+5+1=11
101	5+5+1=11
110	5+5+1=11

Uniformity Analysis

	b_1, b_2, b_3							
(x, y, z)	000	011	101	110	001	010	100	111
$(0, 0, 0)$	37	9	9	9	0	0	0	0
$(0, 0, 1)$	37	9	9	9	0	0	0	0
$(0, 1, 0)$	37	9	9	9	0	0	0	0
$(0, 1, 1)$	37	9	9	9	0	0	0	0
$(1, 0, 0)$	37	9	9	9	0	0	0	0
$(1, 0, 1)$	37	9	9	9	0	0	0	0
$(1, 1, 0)$	31	11	11	11	0	0	0	0
$(1, 1, 1)$	0	0	0	0	21	21	21	1

Note, for (x,y,z)=(1,1,0), Average Hamming Weight=11x2x3/64=33/32 ,while for first 6 rows it is 27/32.
These deviations of means with inputs lead to a 1st-order DPA attack.

Note also if the function g was linear and was shared in the manner as seen previously, then circuit is still secure. The output distribution of f is carried to output of g.

Uniform Sharing of a Function

- We need to make sure that the input of a sharing $\mathbb{g}$ **which follows** $\mathbb{f}$ is also uniform masking.
- **Uniform Sharing of a Function:** The d-th order sharing $\mathbb{f}$ is uniform if and only if:

$$\forall x \in F_2^n, \forall a \in F_2^m, with\ f(x) = a, \forall \mathbb{a} \in Sh(a), and\ s_{out} \geq d + 1:$$

$$|\{\mathbb{x} \in Sh(x) | f(\mathbb{x}) = \mathbb{a}\}| = \frac{\mathbf{2^{n(s_{in}-1)}}}{\mathbf{2^{n(s_{out}-1)}}}$$

Proof

- If the masking $\mathbb{X}$ is uniform and the circuit $\mathbb{f}$ is uniform, then the masking $\mathbb{A}$ of $a = f(x)$, defined by $\mathbb{A}= \mathbb{f}(\mathbb{X})$ is uniform.
- We show: $\Pr([\mathbb{A} = \mathbb{a} | A = a]) = \Sigma_{\substack{\mathbb{x} \in Sh(x) \\ x, f(x) = a}} \Pr[\mathbb{A} = \mathbb{f}(\mathbb{x}) | A = f(x)] \Pr(\mathbb{X} = \mathbb{x}, X = x)$
- The inner probability in the summation term=$2^{n(s_{in}-1)-m(s_{out}-1)} \Pr(\mathbb{X} = \mathbb{x} | X = x) \Pr[X = x] = 2^{n(s_{in}-1)-m(s_{out}-1)} 2^{-n(s_{in}-1)} = 2^{-m(s_{out}-1)} \Pr[X = x]$
- Thus, we have $\Pr[\mathbb{A} = \mathbb{a} | A = a) = \mathrm{p} = 2^{-m(s_{out}-1)}$, if $\mathbb{a} \in Sh(a)$, and 0 otherwise.

Non-completeness: Example

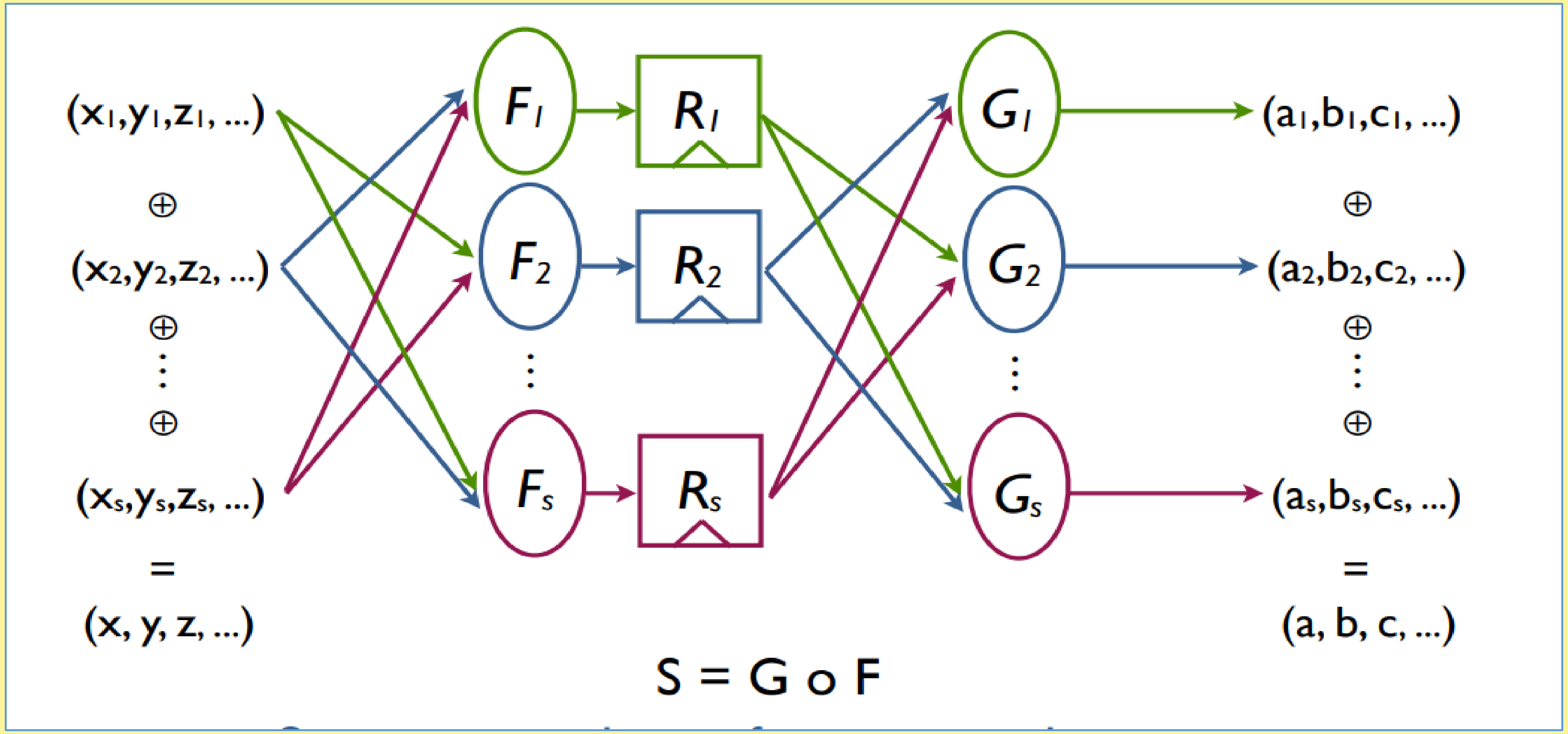
$$S(x,y,z) = x \oplus yz$$
$$= (x_1 \oplus x_2 \oplus x_3) \oplus (y_1 \oplus y_2 \oplus y_3)(z_1 \oplus z_2 \oplus z_3)$$

$$S_1(x_2,x_3,y_2,y_3,z_2,z_3) = x_2 \oplus y_2z_2 \oplus y_2z_3 \oplus y_3z_2$$
$$S_2(x_1,x_3,y_1,y_3,z_1,z_3) = x_3 \oplus y_3z_3 \oplus y_3z_1 \oplus y_1z_3$$
$$S_3(x_1,x_2,y_1,y_2,z_1,z_2) = x_1 \oplus y_1z_1 \oplus y_1z_2 \oplus y_2z_1$$

First order non-complete: Any one sub-function is independent of at least one share. We shall be dealing with First order TI throughout this presentation.

To protect a function with degree d, at least d+1 shares are required

Composition of nonlinear functions



Separate non-linear functions with registers to prevent propagation of glitches

TI Example: TI of 2-input XOR Gate

- XOR is a linear function
- Let $c = a \oplus b$
- Let a_1, a_2, a_3 be the shares of a and b_1, b_2, b_3 be the shares of b i.e.
  - $a = a_1 \oplus a_2 \oplus a_3$
  - $b = b_1 \oplus b_2 \oplus b_3$
- Let c_1, c_2, c_3 be the output shares:
  - $c_1 = a_1 \oplus b_1$
  - $c_2 = a_2 \oplus b_2$
  - $c_3 = a_3 \oplus b_3$
- This is non-complete, uniform and correct
- In fact all the three properties can be achieved using just 2 shares!
- To summarize, TI design for linear functions are EASY!
- XOR + AND is functionally complete, so let us look into TI design of AND gate

TI Example: TI of 2-input AND Gate

- AND is not a linear function
- Let c = ab
- Lets first see whether we can design a 2-share TI
- Let a_1, a_2 be the shares of a and b_1, b_2 be the shares of b i.e.
  - $a = a_1 \oplus a_2$
  - $b = b_1 \oplus b_2$
- The two output shares must contain the following 4 terms:
  - a_1b_1
  - a_1b_2
  - a_2b_1
  - a_2b_2
- In no way can these 4 terms be combined into 2-shares without violating non-completeness.
- So, 2 share TI of AND gate is not possible
- We need to increase the number of shares

TI Example: TI of 2-input AND Gate

- With three shares even though non-completeness is satisfied, no three sharing can achieve uniformity without using extra randomness
- To achieve uniformity, non-completeness at the same time without using extra randomness, we need at least 4 shares
- Shown on the right is a uniform, non-complete sharing of the 2 input AND gate using 4 shares

$$A = X.Y$$

$$X = x_1 \oplus x_2 \oplus x_3 \oplus x_4$$

$$Y = y_1 \oplus y_2 \oplus y_3 \oplus y_4$$

$$A = a_1 \oplus a_2 \oplus a_3 \oplus a_4$$

$$a_1 = (x_2 \oplus x_3 \oplus x_4).(y_2 \oplus y_3) \oplus y_3$$

$$a_2 = ((x_1 \oplus x_3).(y_1 \oplus y_4)) \oplus (x_1.y_3) \oplus x_4$$

$$a_3 = (x_2 \oplus x_4).(y_1 \oplus y_4) \oplus x_4 \oplus y_4$$

$$a_4 = (x_1.y_2) \oplus y_3$$

TI Example: TI of 2-input AND Gate

- With three shares we can achieve uniformity using extra randomness
- The first example on the right uses 2-bits of randomness
- The second example uses one bit of randomness

$$A = X.Y$$
$$X = x_1 \oplus x_2 \oplus x_3$$
$$Y = y_1 \oplus y_2 \oplus y_3$$
$$A = a_1 \oplus a_2 \oplus a_3$$
$$a_1 = (x_2.y_2) \oplus (x_2.y_3) \oplus (x_3.y_2) \oplus \mathbf{r_1} \oplus \mathbf{r_2}$$
$$a_2 = (x_3.y_3) \oplus (x_1.y_3) \oplus (x_3.y_1) \oplus \mathbf{r_2}$$
$$a_3 = (x_1.y_1) \oplus (x_1.y_2) \oplus (x_2.y_1) \oplus \mathbf{r_1}$$

$\mathbf{r_1}$ and $\mathbf{r_2}$ are 2 bits of randomness

$$A = X.Y$$
$$X = x_1 \oplus x_2 \oplus x_3$$
$$Y = y_1 \oplus y_2 \oplus y_3$$
$$A = a_1 \oplus a_2 \oplus a_3$$
$$a_1 = (x_2.y_2) \oplus (x_2.y_3) \oplus (x_3.y_2) \oplus \mathbf{r}$$
$$a_2 = (x_3.y_3) \oplus (x_1.y_3) \oplus (x_3.y_1) \oplus (x_1.\mathbf{r}) \oplus (y_1.\mathbf{r})$$
$$a_3 = (x_1.y_1) \oplus (x_1.y_2) \oplus (x_2.y_1) \oplus (x_1.\mathbf{r}) \oplus (y_1.\mathbf{r}) \oplus \mathbf{r}$$

r is a unit of randomness

A Case Study of Lightweight TI based S-Box

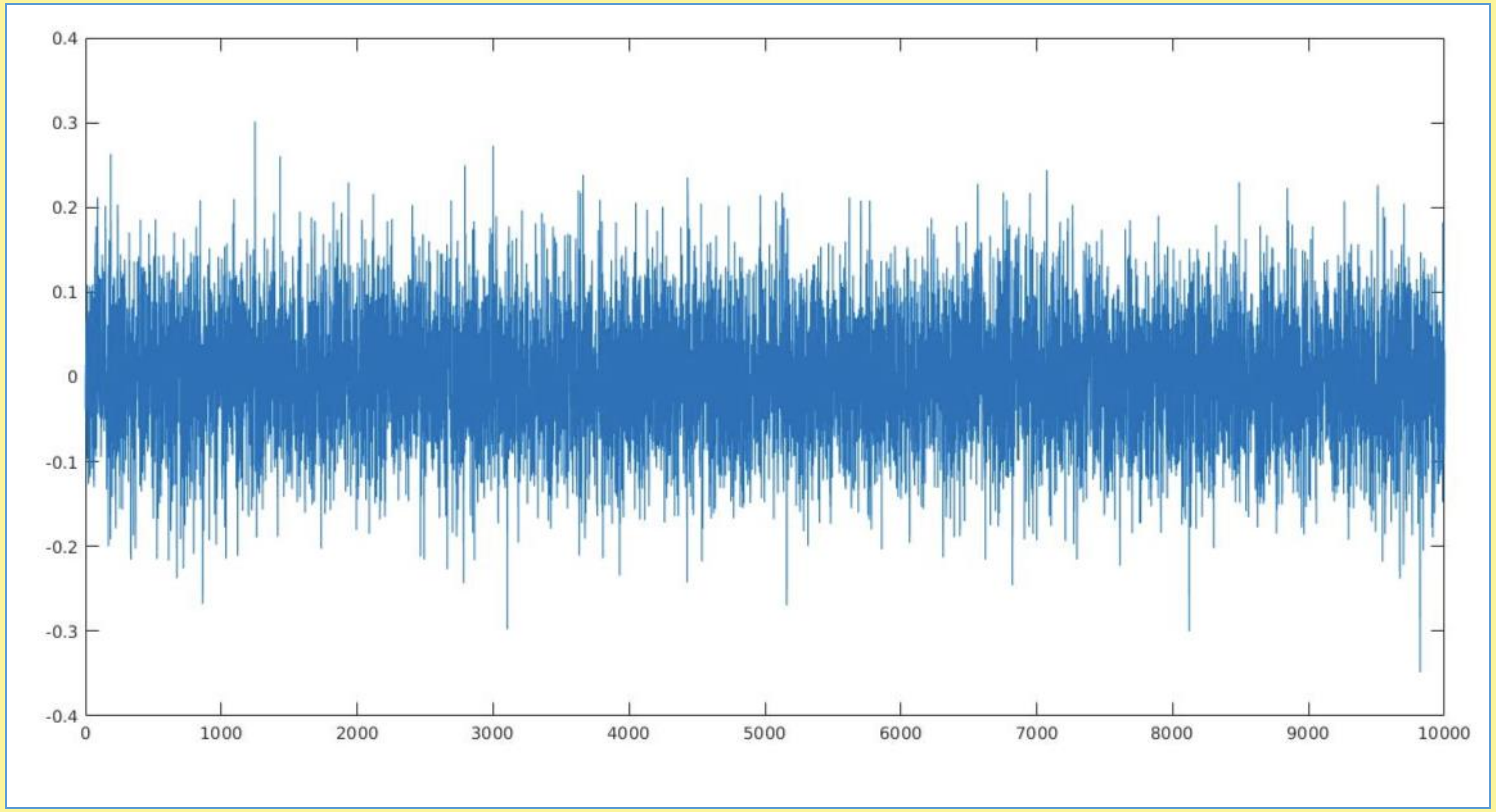
$$f = XZW \oplus YW \oplus XY \oplus Y \oplus Z$$

$$b_1(X,Y,W) = X \oplus Y \oplus XW \oplus YW$$
$$b_2(X,Y,Z) = Z \oplus XY \oplus XZ$$
$$b_3(X,Z,W) = X \oplus W \oplus XZ \oplus ZW$$
$$f(X,Y,Z,W) = b_1 \oplus b_2 \oplus b_1b_3 \oplus b_2b_3 = b_1(b_1,b_2,b_3)$$

$$b_1 = b_{11} \oplus b_{12} \oplus b_{13}$$
$$b_2 = b_{21} \oplus b_{22} \oplus b_{23}$$
$$b_3 = b_{31} \oplus b_{32} \oplus b_{33}$$
$$X = X_1 \oplus X_2 \oplus X_3$$
$$Y = Y_1 \oplus Y_2 \oplus Y_3$$
$$Z = Z_1 \oplus Z_2 \oplus Z_3$$
$$W = W_1 \oplus W_2 \oplus W_3$$

$$b_{11} = X_1 \oplus Y_2 \oplus (Y_1W_1) \oplus (Y_1W_2) \oplus (Y_2W_1) \oplus (X_1W_1) \oplus (X_1W_2) \oplus (X_2W_1)$$
$$b_{12} = X_2 \oplus Y_3 \oplus (Y_2W_2) \oplus (Y_2W_3) \oplus (Y_3W_2) \oplus (X_2W_2) \oplus (X_2W_3) \oplus (X_3W_2)$$
$$b_{13} = X_3 \oplus Y_1 \oplus (Y_3W_3) \oplus (Y_3W_1) \oplus (Y_1W_3) \oplus (X_3W_3) \oplus (X_3W_1) \oplus (X_1W_3)$$
$$b_{21} = Z_1 \oplus (Z_1X_2) \oplus (Z_2X_1) \oplus (Y_1X_2) \oplus (Y_2X_1) \oplus (Z_1X_1) \oplus (Y_1X_1)$$
$$b_{22} = Z_2 \oplus (Z_2X_3) \oplus (Z_3X_2) \oplus (Y_2X_3) \oplus (Y_3X_2) \oplus (Z_2X_2) \oplus (Y_2X_2)$$
$$b_{23} = Z_3 \oplus (Z_1X_3) \oplus (Z_3X_1) \oplus (Y_1X_3) \oplus (Y_3X_1) \oplus (Y_3X_3) \oplus (Z_3X_3)$$
$$b_{31} = X_1 \oplus W_2 \oplus (Z_1W_1) \oplus (Z_1W_2) \oplus (Z_2W_1) \oplus (X_1Z_1) \oplus (X_1Z_2) \oplus (X_2Z_1)$$
$$b_{32} = X_2 \oplus W_3 \oplus (Z_2W_2) \oplus (Z_2W_3) \oplus (Z_3W_2) \oplus (X_2Z_2) \oplus (X_2Z_3) \oplus (X_3Z_2)$$
$$b_{33} = X_3 \oplus W_1 \oplus (Z_3W_3) \oplus (Z_3W_1) \oplus (Z_1W_3) \oplus (X_3Z_3) \oplus (X_3Z_1) \oplus (X_1Z_3)$$

TVLA Evaluation of the Design



Conclusions

Masking is a popular countermeasure

However susceptible to first order attacks due to glitches

TI gives a method based on secret sharing to alleviate this

We have seen properties and constructions on TI

References:

1. Begül Bilgin, Threshold Implementations As Countermeasure Against Higher-Order Differential Power Analysis, Phd Thesis.
2. Ashrujit Ghoshal, Rajat Sadhukhan, Sikhar Patranabis, Nilanjan Datta, Stjepan Picek, Debdeep Mukhopadhyay: Lightweight and Side-channel Secure 4 × 4 S-Boxes from Cellular Automata Rules. IACR Trans. Symmetric Cryptol. 2018(3): 311-334 (2018)

NPTEL ONLINE CERTIFICATION COURSES

Thank you!