NPTEL ONLINE CERTIFICATION COURSES

Course Name: Hardware Security

Faculty Name: Prof Debdeep Mukhopadhyay

Department : Computer Science and Engineering

Topic

Lecture 43: Power Analysis Countermeasures

CONCEPTS COVERED

Concepts Covered:

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

Countering DPA

- Two broad *approaches* are taken
  - Make the power consumption of the device independent of the data processed
    - Detached power supplies
    - Logic styles with a data independent power consumption
    - Noise generators
    - Insertion of random delays
  - Methods are costly and not in tune with normal CAD methodologies

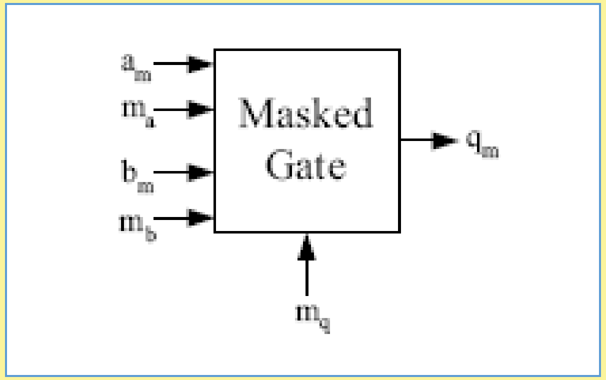
Countering DPA (Second Approach)

- *Second Approach* is to randomize the intermediate results
- Based on the principle that the power consumption of the device processing randomized data is uncorrelated to the actual intermediate results
- Masking: Can be applied at the algorithm level or at the gate level

Gate Level Masking

- No wire stores a value that is correlated to an intermediate result of the algorithm.
- Process of converting an unmasked digital circuit to a masked version can be automated

Masked AND Gate



$$a_m = a \oplus m_a$$
$$b_m = b \oplus m_b$$
$$q_m = q \oplus m_q$$
$$q = f(a,b)$$
$$q_m = \hat{f}(a_m, m_a, b_m, m_b, m_q)$$

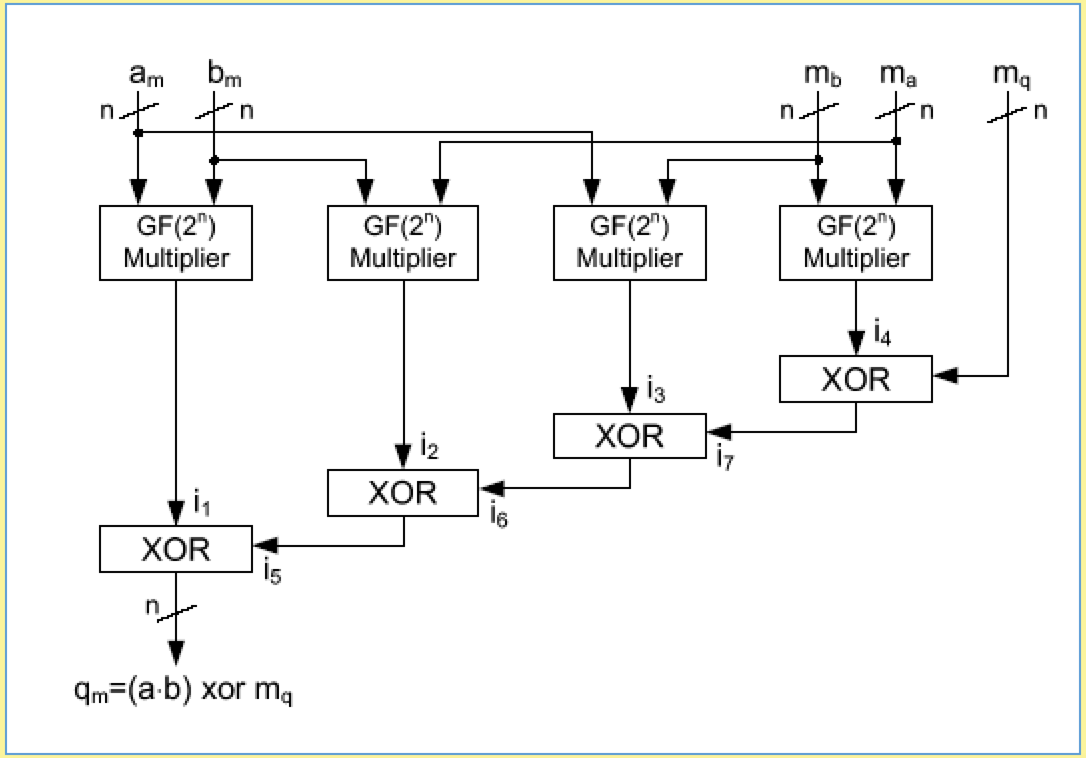
Masked AND Gate

$$
\begin{aligned}
q_m &= (a \cdot b) \oplus m_q \\
&= (a_m \oplus m_a).(b_m \oplus m_b) \oplus m_q \\
&= (((a_m.b_m \oplus b_m.m_a) \oplus (m_b \cdot a_m)) \oplus m_a.m_b) \oplus m_q
\end{aligned}
$$

Masked AND Gate

- There are 4^5=1024 possible input transmissions that can occur.
- It turns out that the expected value of the energy required for the processing of q=0 and q=1 are identical.
- Thus protected against DPA, under the assumption that the CMOS ***gates switch only once in one clock cycles.***
- But we know there are glitches, and so the output of gates swing a number of times before reaching a steady state. Hence... the argument continues.

Masked Multiplier



Same Principle may be applied for multiplier circuits.

Masking and 1st order Analysis

- In these masking designs, the intermediate variable X is split into two random variables X_1 and X_2, st. $X_1 \oplus X_2 = X$.
- Assume the leakage $L(X) = HW(X_1, X_2)$, we have the following:

x	x_1	x_2	$L(X)$	Mean($L(X)$)	Var($L(X)$)
0	0	0	0	1	1
0	1	1	2		
1	0	1	1	1	0
1	1	0	1		

Masking does not reveal any information from 1st-order analysis, as the mean is constant for different values of x. However, a 2nd –order analysis can reveal because of the dependence of variance on x.

Higher Order Masking

- Thus in a dth order masking aims to randomize intermediate sensitive data X by splitting into d+1 uniformly distributed variables $X_1, \cdots, X_d, X_{d+1}$, st:

$$X = X_1 \perp X_2 \perp \cdots \perp X_d \perp X_{d+1}$$

- Depending on the exact $\perp$ operator, we can have multiplicative, additive masking.
- When the $\perp$ operator is XORing, we call it Boolean Masking.
- Each variable X_i is referred to as a secret share and the secret sharing can be done by randomly generating $X_1, X_2, \cdots, X_d$, and calculating X_{d+1}.

Hiding within the Mask

- Given an input sharing, all the cipher operations are done inside a mask:
  - Linear Transformations
  - S-Box computations
- Linear transformations are easy:
  - Thus, $l(X) = l(X_1 \oplus X_2 \oplus \cdots \oplus X_{d+1}) = l(X_1) \oplus \cdots \oplus l(X_{d+1})$
- So, we can perform the linear operations on the masks.

Nonlinear Masking

- It is challenging for nonlinear functions.
- Example: $f(X, Y) = Z \oplus XY$
- Masked Circuit:
  - $f_1(X_1, Y_1) = Z_1 \oplus X_1Y_1$
  - $f_2(X_1, X_2, Y_1, Y_2) = \big((Z_2 \oplus X_1Y_2) \oplus X_2Y_1\big) \oplus X_2Y_2$
- Note again the ordering of the operations is very important!
  - Don't do, $f_2(X_1, X_2, Y_1, Y_2) = (Z_2 \oplus X_1Y_2) \oplus (X_2Y_1 \oplus X_2Y_2)$ …as the second parenthesis is dependent on Y
- However, this is not secure against higher order attacks.
- Actually, not even 1st order attacks if there are glitches.

NPTEL ONLINE CERTIFICATION COURSES

Thank you!