NPTEL ONLINE CERTIFICATION COURSES

Course Name: Hardware Security

Faculty Name: Prof Debdeep Mukhopadhyay

Department : Computer Science and Engineering

Topic

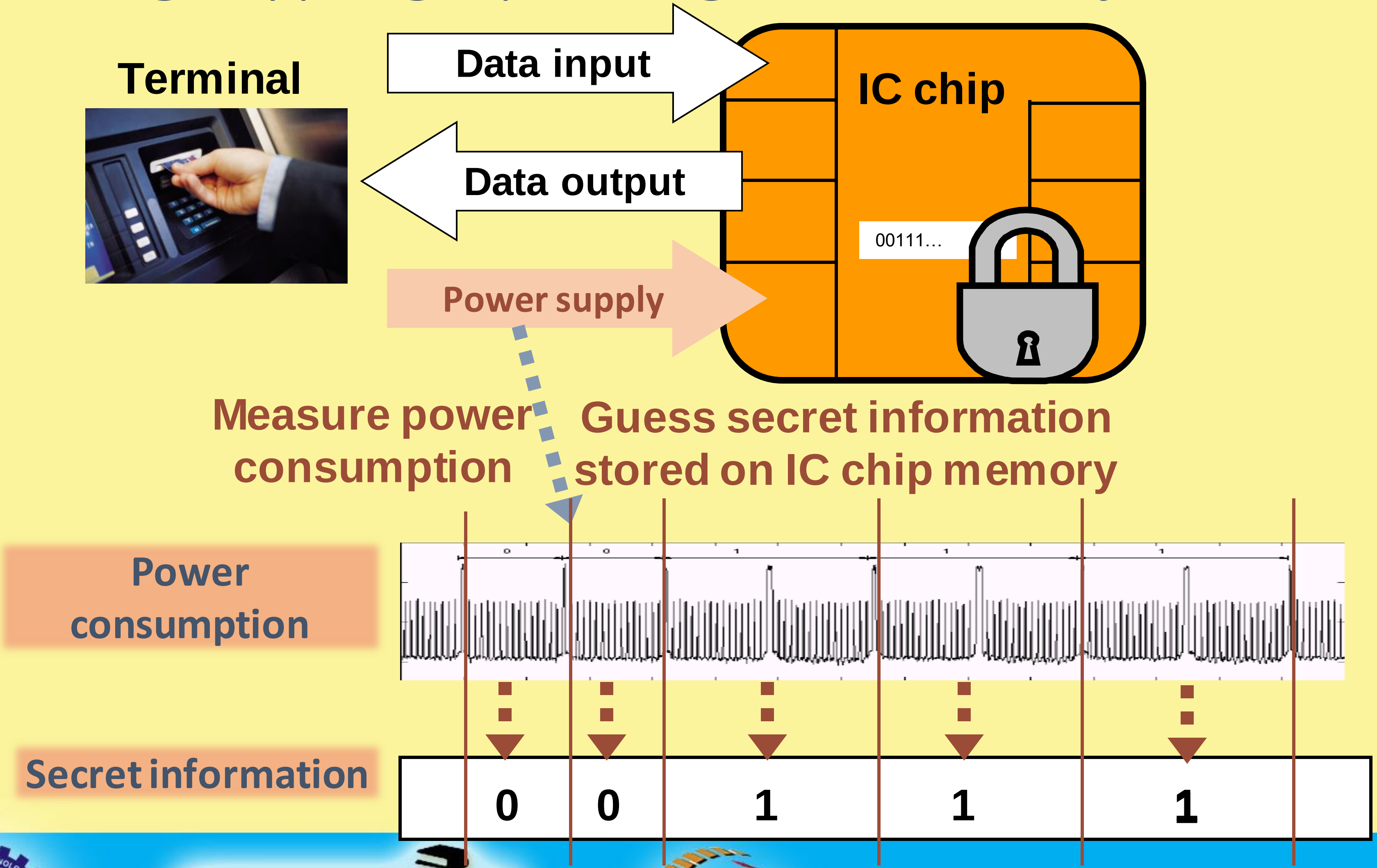
Lecture 24: Introduction to Side Channel Analysis

CONCEPTS COVERED

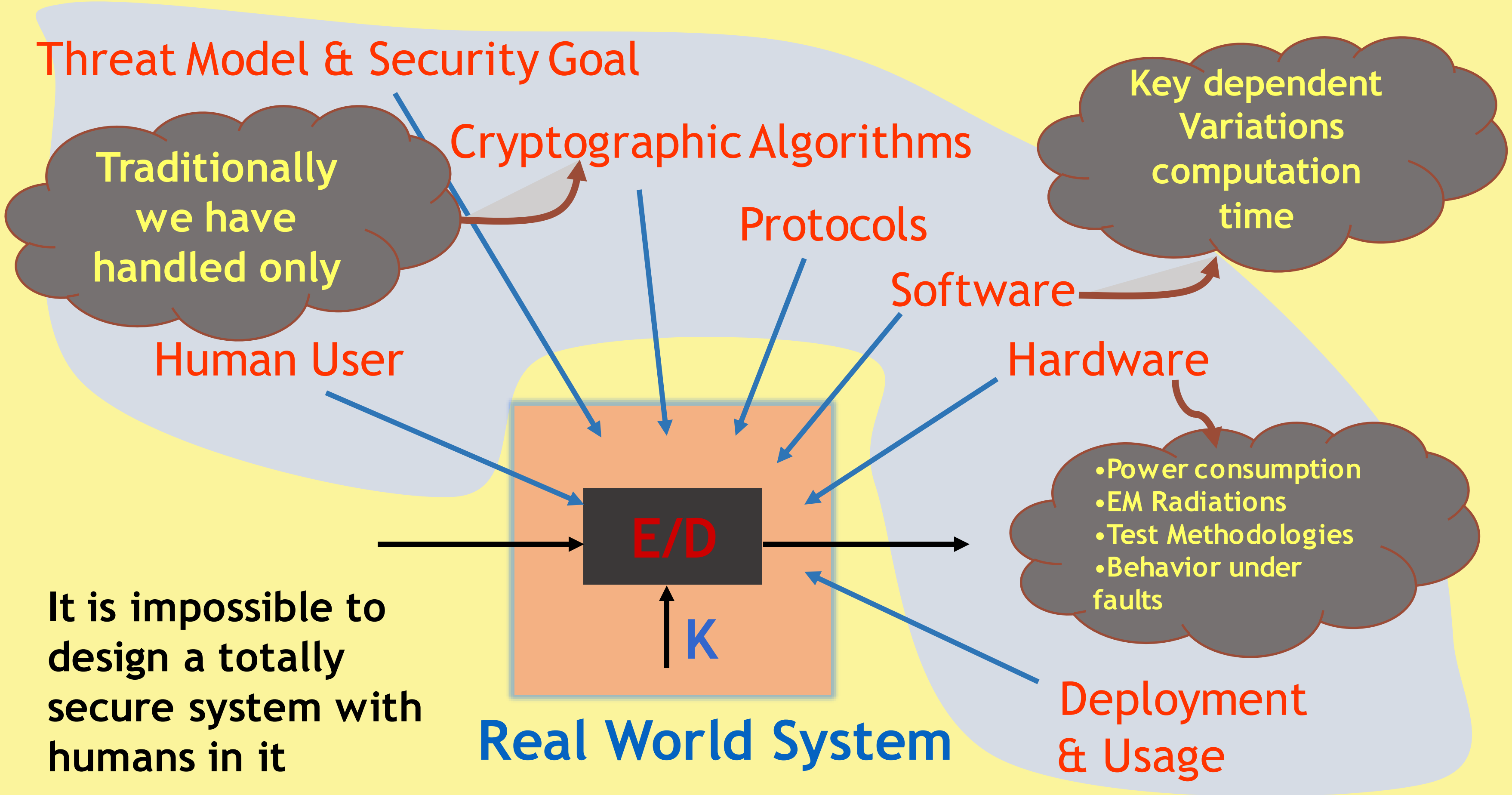
Concepts Covered:

- What is Side Channel Analysis?
- Types of Side Channel
- Brief History
- Timing Attack
- Power Analysis and Types

Strong cryptographic algorithms are just the beginning!



Side Channel Sources



It is impossible to design a totally secure system with humans in it

What are Side Channels?

- These are covert channels which leak information which the designers of cryptographic algorithms did not consider.
- Information is leaked because of the implementation:
  - optimization leads to information leakage
  - example: **an if-else statement in a programming language**

A Brief History of Side Channels

- World War 1, telephones used in battle fields had just one wire and used the earth to carry the return current.
  - Spies would insert rod in the ground and connect them to amplifiers in order to pick up conversation.
- World War II, Bell Labs were the first to discover that electromagnetic emissions from devices could leak 75% of the plaintext that was sent securely from a distance of 80ft.
- During 1950s, Americans used radiations from encoding devices to spy on encrypted Russian message transmission.
- These attacks were studied by Americans, under the code named Tempest, to identify the shielding methods for equipments.
- In 1985, Win van Eck published the first unclassified report which showed how low cost equipments could be used to eavesdrop on messages from a distance of few hundred meters using the emanations from cathode ray tube monitors.
- More recent studies show how emissions from cables of LCD monitors, wireless keyboards, LED indicators can be picked up and decoded from several feet away.
- In the mid 1990s, two seminal papers by Paul C Kocher showed how execution time and power consumption can be used to easily retrieve secret keys from naïve implementations of ciphers.

Possible Side Channels

- Timing
- Power
- Electro-Magnetic radiations
- Faults
- Testability Features in Hardware

and may be many more…

Square and Multiply Algorithm

Input: $y, x, n,$
Output: $s \equiv y^x \bmod n$

$s = 1$
for $(i = n-1; i \geq 0; i--)$ **do**
    $bit = (x >> i)\&1$
    $s = s^2 \bmod n$
    if (bit) **then**
        $s = s \times y \bmod n$
    end
end
return s

We assume that the attacker knows the first b-1 bits, and wants to obtain the b-1th bit of the secret key.

Attacker knows x[0],…,x[b-2] and wants to determined x[b-1]

Paul C Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems, In Proceedings of Crypto, LNCS 1109, pgs 104-113, 1996.

Timing Measurement

- Assume that the attacker can measure time accurately for a function P.
- Compute the timestamp before and after calling a function P
- Then evaluate the difference between the timestamps.
- Note if there is no program between two timestamp calls, there is still a small time difference.
- This overhead should be appropriately deducted after computing the running time of the program P.

Timestamp Snippet

```
#include <time.h>

unsigned int timestamp(void)
{
    unsigned int bottom;
    unsigned int top;
    asm volatile("xorl %%eax,%%eax\n cpuid \n" ::: "%eax",
     "%ebx", "%ecx", "%edx"); // flush pipeline
    asm volatile("rdtsc\n" : "=a" (bottom), "=d" (top) );
                                    // read rdtsc
    asm volatile("xorl %%eax,%%eax\n cpuid \n" ::: "%eax",
    "%ebx", "%ecx", "%edx"); // flush pipeline again
    return bottom;
}
```

Attack Methodology

- Attacker measures the time required to perform the loop a large number of times by varying the value of *y*.
- Each observed timing can be denoted as $T_j = e + \sum_{i=0}^{w-1} t_i$, where t_i is the time required for performing multiplication and squaring for bit i.
- The measurement error, loop overhead are other sources of inaccuracies.
- We assume that the attacker knows or has correctly evaluated in the previous iterations the first (b-1) bits: x[0],…,x[b-2]
- Now the attacker guesses x[b-1]. Is it correct? 0 or 1?

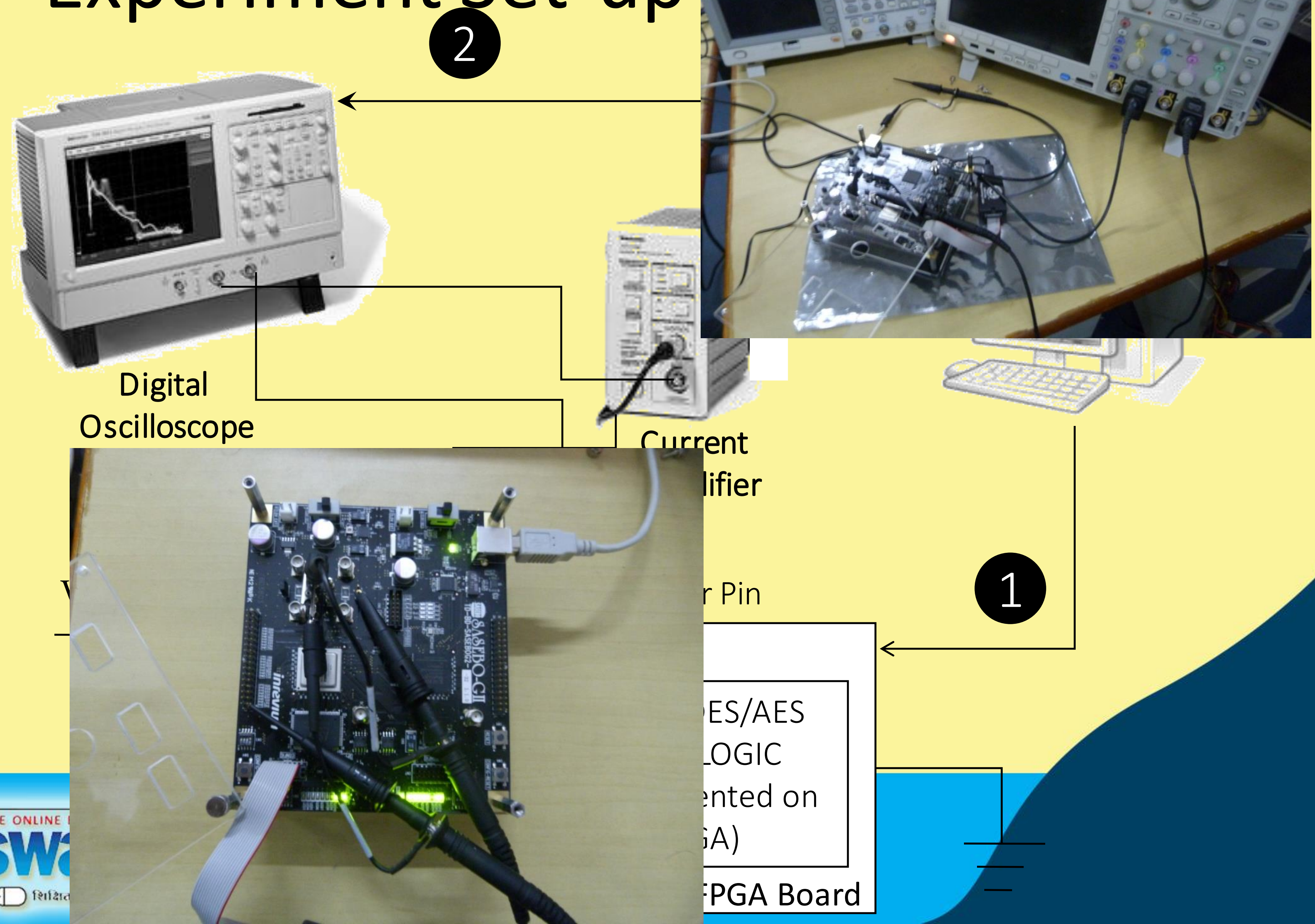
Attack Methodology (contd.)

- If the guess is correct, subtracting from T yields

$$
\begin{aligned}
T_r &= e + \Sigma_{i=0}^{w-1} t_i - \Sigma_{i=0}^{b-1} t_i \\
&= e + \Sigma_{i=b}^{w-1} t_i + (t_{b-1} - t_{b-1}^{*}) \\
&= e + \Sigma_{i=b}^{w-1} t_i + \Delta t_{b-1}
\end{aligned}
$$

- Attacker obtains a distribution by varying the value of y and observing the above timing T_r.
- Assuming that the measurement error and the individual timings for the modular multiplier are independent, the variance of this distribution is:
  - If the guess is correct: $Var(T_r) = Var(e) + (w-b)Var(t)$
  - If the guess is wrong: $Var(T_r) = Var(e) + (w-b)Var(t) + 2Var(t)$

Experiment Set-up



Power Attacks

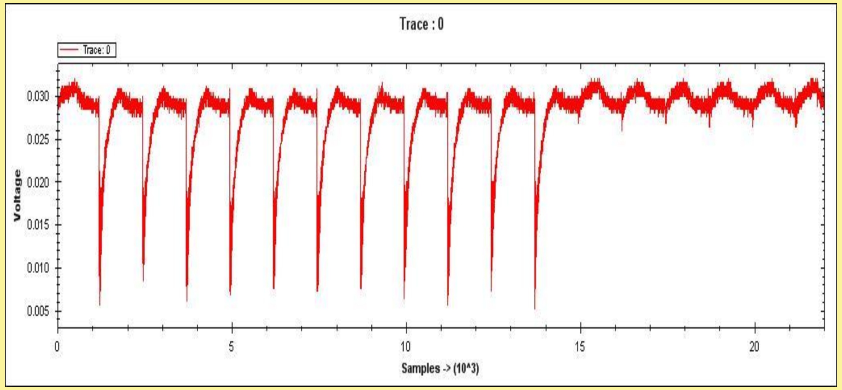
- SPA – Simple Power Analysis attacks
  - Fact exploited - Power consumption at an instant of time is a function of the operation being carried out by the device
- DPA – Differential Power Analysis
  - Fact exploited - Power consumption of the same operation at different instants of time depends on the data being processed.

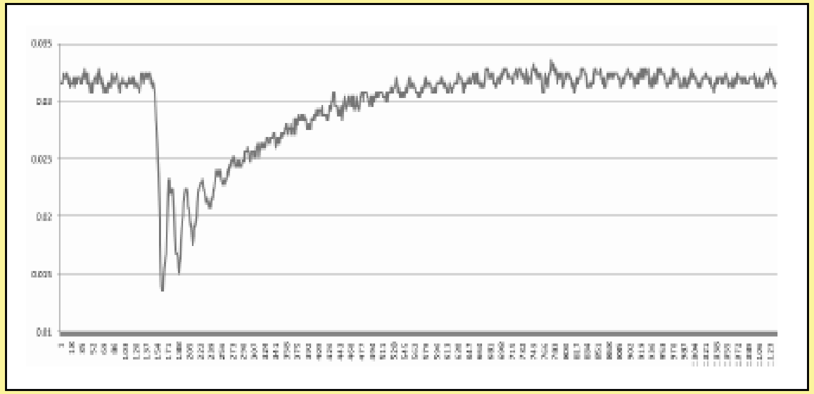
Paul C. Kocher, Joshua Jaffe, Benjamin Jun:Differential Power Analysis. CRYPTO 1999: 388-397

Simple Power Analysis (SPA)

- Directly interprets the power consumption of the device
- Looks for the operations taking place and also the key!
- Trace: A set of power consumptions across a cryptographic process
- 1 millisecond operation sampled at 5MHz yield a trace with 5000 points

A Power Trace



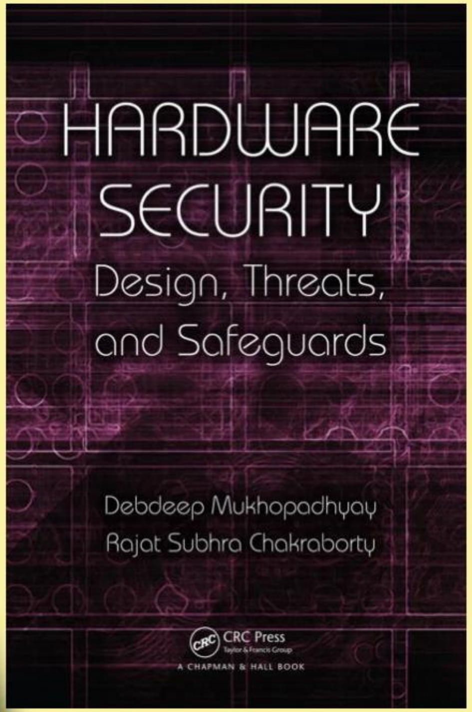


- Power Trace of a round of AES.
- Observe the variation of power values.
- The variations occur because of the operation dependence of power: leads to SPA.
- The variations also occur because of data dependence of power: leads to DPA.

References

References:

- Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, Hardware Security: Design, Threats and Safeguards, CRC Press



D. Stinson, Cryptography: Theory and Practice, Chapman & Hall/CRC

Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman & Hall/CRC

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, An Introduction to Mathematical Cryptography, Springer.

FREE ONLINE EDUCATION swayam

Conclusion:

Definition of Side Channel Analysis

Brief History

Types of Side Channel Analysis

Kocher's Timing Attacks

Power Analysis and Types

NPTEL ONLINE CERTIFICATION COURSES

Thank you!