NPTEL ONLINE CERTIFICATION COURSES

Course Name: Hardware Security

Faculty Name: Prof Debdeep Mukhopadhyay

Department : Computer Science and Engineering

Topic

Lecture 25: Power Analysis-I

CONCEPTS COVERED

Concepts Covered:

- Working Principle of DPA
- Toy Example
- Difference-of-Mean (DOM) Method
- DOM on AES

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.

Simple Power Analysis (SPA)

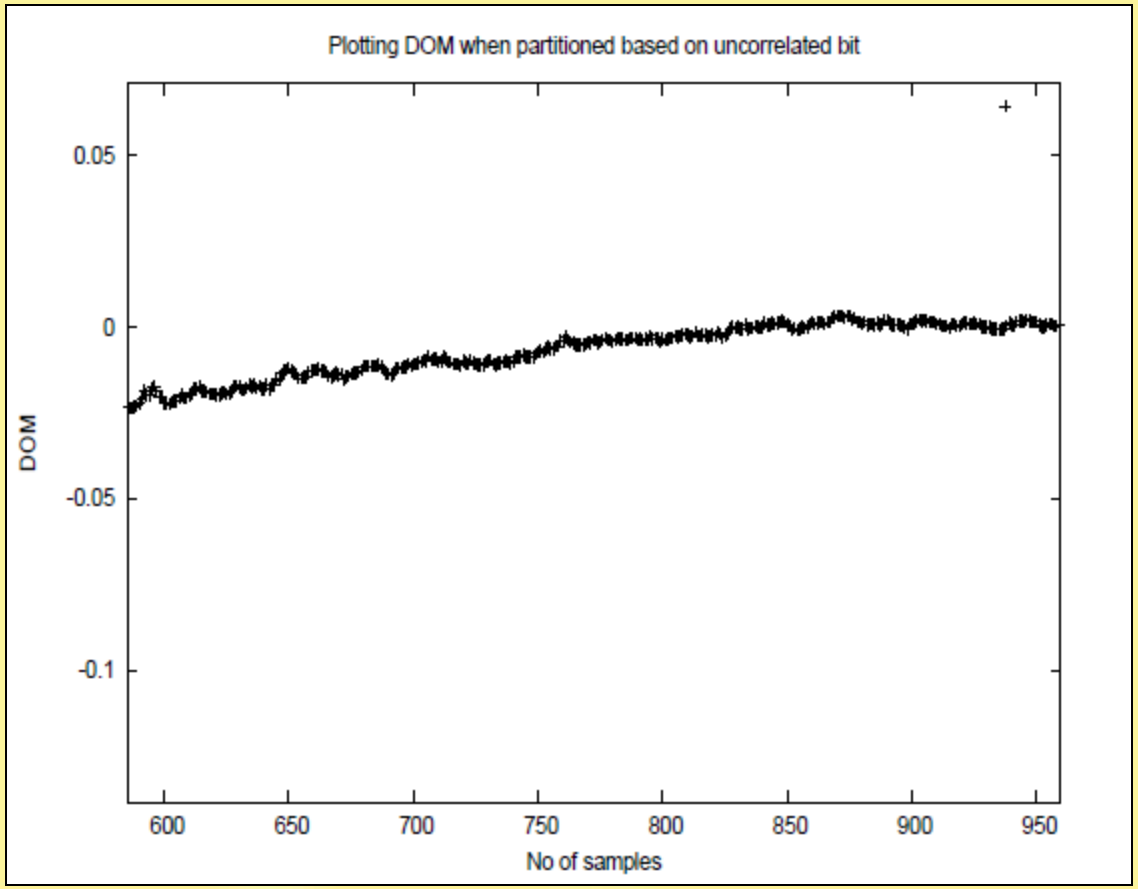
- Directly interprets the power consumption of the device
- Looks for the operations taking place and also the key!
- Trace: A set of power consumptions across a cryptographic process
- 1 millisecond operation sampled at 5MHz yield a trace with 5000 points

Principle of DPA

s	HW(s)	Target bit (LSB)
0000	0	0
0001	1	1
0010	1	0
0011	2	1
0100	1	0
0101	2	1
0110	2	0
0111	3	1
1000	1	0
1001	2	1
1010	2	0
1011	3	1
1100	2	0
1101	3	1
1110	3	0
1111	4	1

- Assume power leakage follows Hamming Weight.
- Divide the HW(s) into two bins:
  - 0 bin: when LSB is 0
  - 1 bin: when LSB is 1
- Difference-of-Mean (DoM)=20/8-12/8=1

When the partitioning is done wrt. an uncorrelated bit?



- Parititioning done by bits simulated using *rand* function in C.
- Observe the DoM is close to 0, as expected!

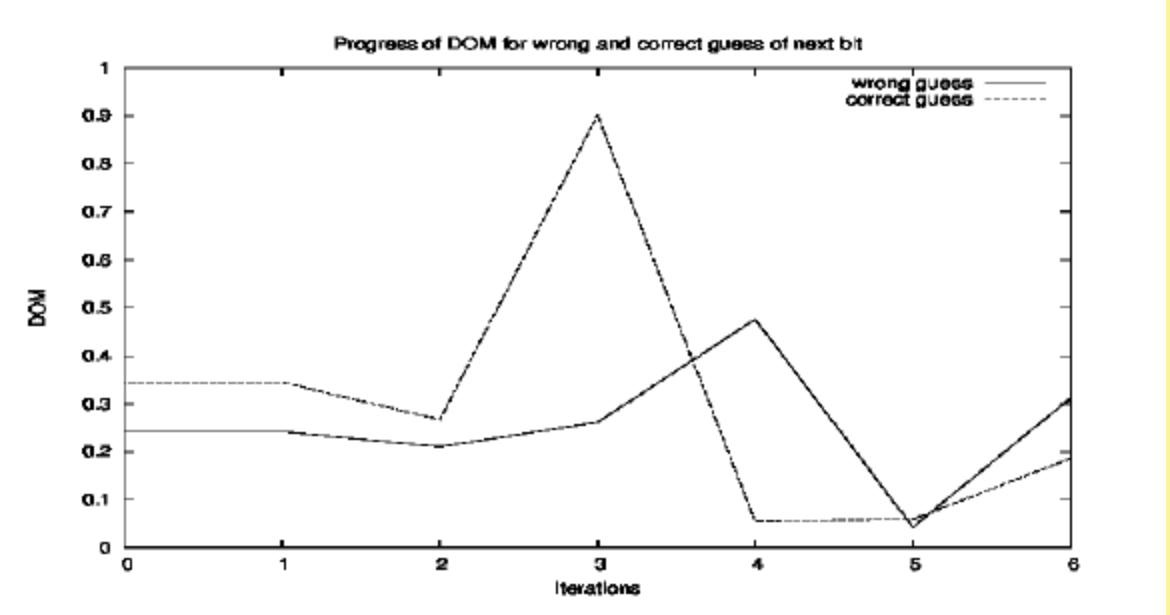
A Toy DPA

- Consider the operation $z=y^x \bmod 256$
- Assume attacker knows first 4 bits of the secret, x.
- Probability of guessing the next bit of x is ½ (with no side channel information).
- Now we assume, the attacker varies y and obtains several power traces.
  - We simulate them through Hamming Weights.

A Toy DPA

- For a given y, the attacker now guesses the next bit and computes the *probable* s after the 3rd iteration (note that square and multiply starts from bit 6 to bit 0).
- Based on the LSB of y, the corresponding trace is put into the 0 bin or 1 bin.
- For every guess (there are 2 guesses) the DoM is computed and plotted.
- The correct guess is expected to provide large DoM.

A Toy DPA



- Correct Key is 0x8F
- Next bit is thus 1.
- DoM computed after 2^{10} traces.
- Significant difference: 0.9 vs 0.2!

DPA Overview

Introduced by P. Kocher and colleagues

More powerful and more difficult to prevent than SPA

Different power consumption for different state (0 or 1)

Data collection phase and data analysis phase

Procedure

- Gather many power consumption curves
- Assume a key value
- Divide data into two groups(0 and 1 for chosen bit)
- Calculate mean value curve of each group
- Correct key assumption → not negligible difference

DPA Procedure for AES

1. Make power consumption measurement of about 1000 AES operations, 100000 data points / curve, ($Ciphertext_i$, $Curve_i$)
2. Assume a key for an S-box of last round
3. Calculate last round S-box first bit output for each ciphertext using the assumed key
4. Divide the measurement into 2 groups (output 0 and 1)
5. Calculate the average curve of each group
6. Calculate the difference of two curves
7. Assumed correct key → spikes in the differential curve
8. Repeat 2-7 for other S-boxes
9. Exhaustive search for 8 bits of key.

Difference-of-Mean (DOM) Method

- DPA selection function : $D(C,b,K_s)$ is defined as computing the value of the
  - b^{th} output bit, depending upon
    - C: Ciphertext
    - K_S is the guessed key (6 bits) for the S-Box
- **Note: If K_s is incorrect evaluating D(…) gives the correct bit in half of the cases for each of the ciphertexts.**

DOM (Contd.)

- Attacker obtains m encryption operations and capture power traces, $T_{1..m}[1..k]$, with k sample points each.
- An attacker records the m ciphertexts
- No knowledge of the plaintext is required

DOM (Contd.)

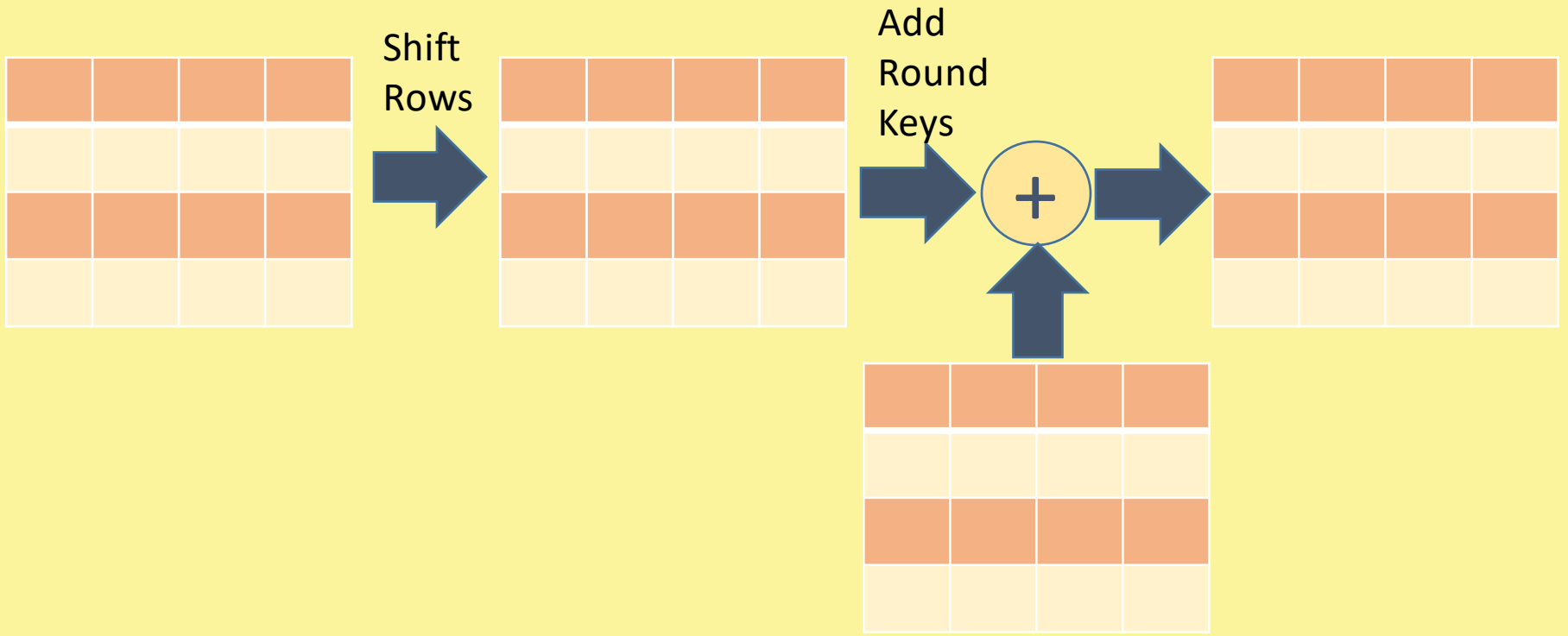
Sample Points

CIPHERTEXTS

T[1][1]	T[1][2]		T[1][k]
T[2][1]	T[2][2]		T[2][k]
T[m][1]	T[m][2]		T[2][k]

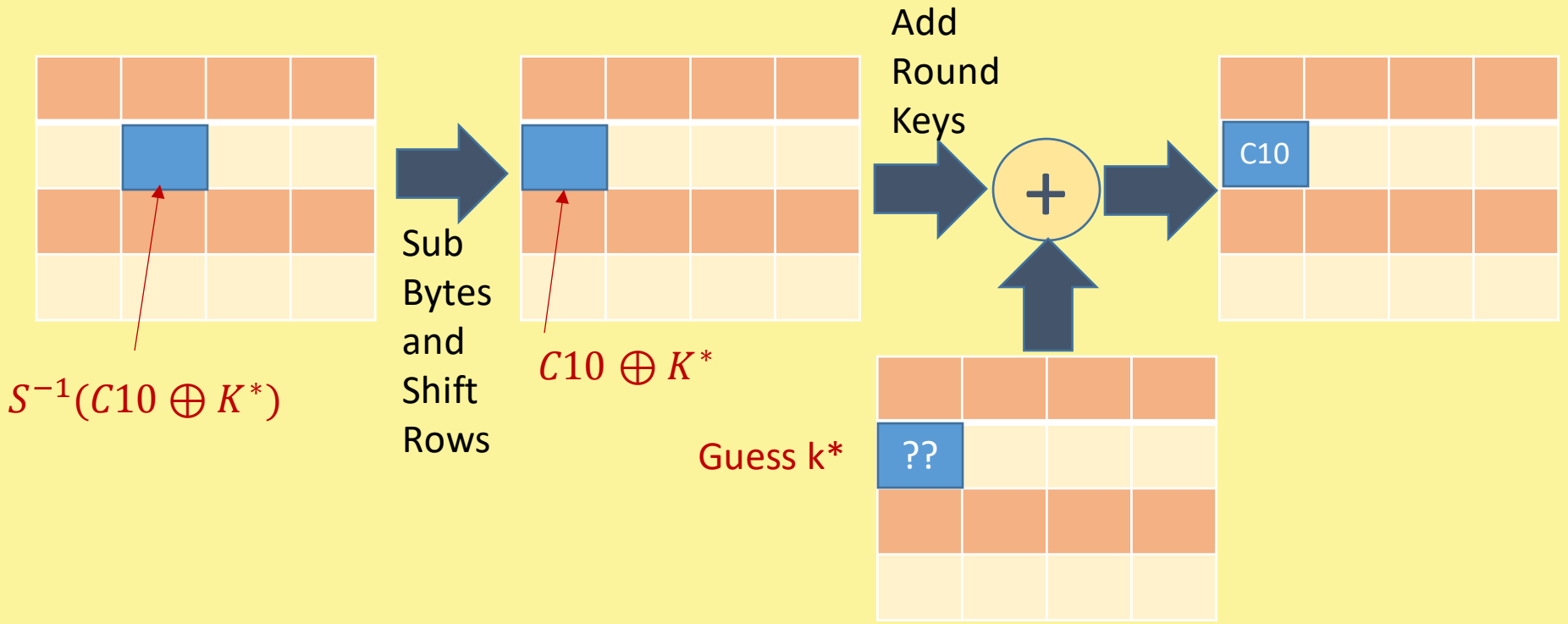
Tabular representation of power traces.

The Selection Function $\mathbb{D}$



$$f(R_{15}, K_{16}) = P(S(E(R_{15} \oplus K_{16})))$$

The Selection Function $\mathbb{D}$



D(C10,b=0,K10)=$S^{-1}(C10 \oplus K^*)|_{(b=0)}$

If the key guess is correct, this matches with the correct value for all ciphertexts collected. However, if wrong it matches roughly half times, assuming sufficiently large number of cipher samples have been collected.

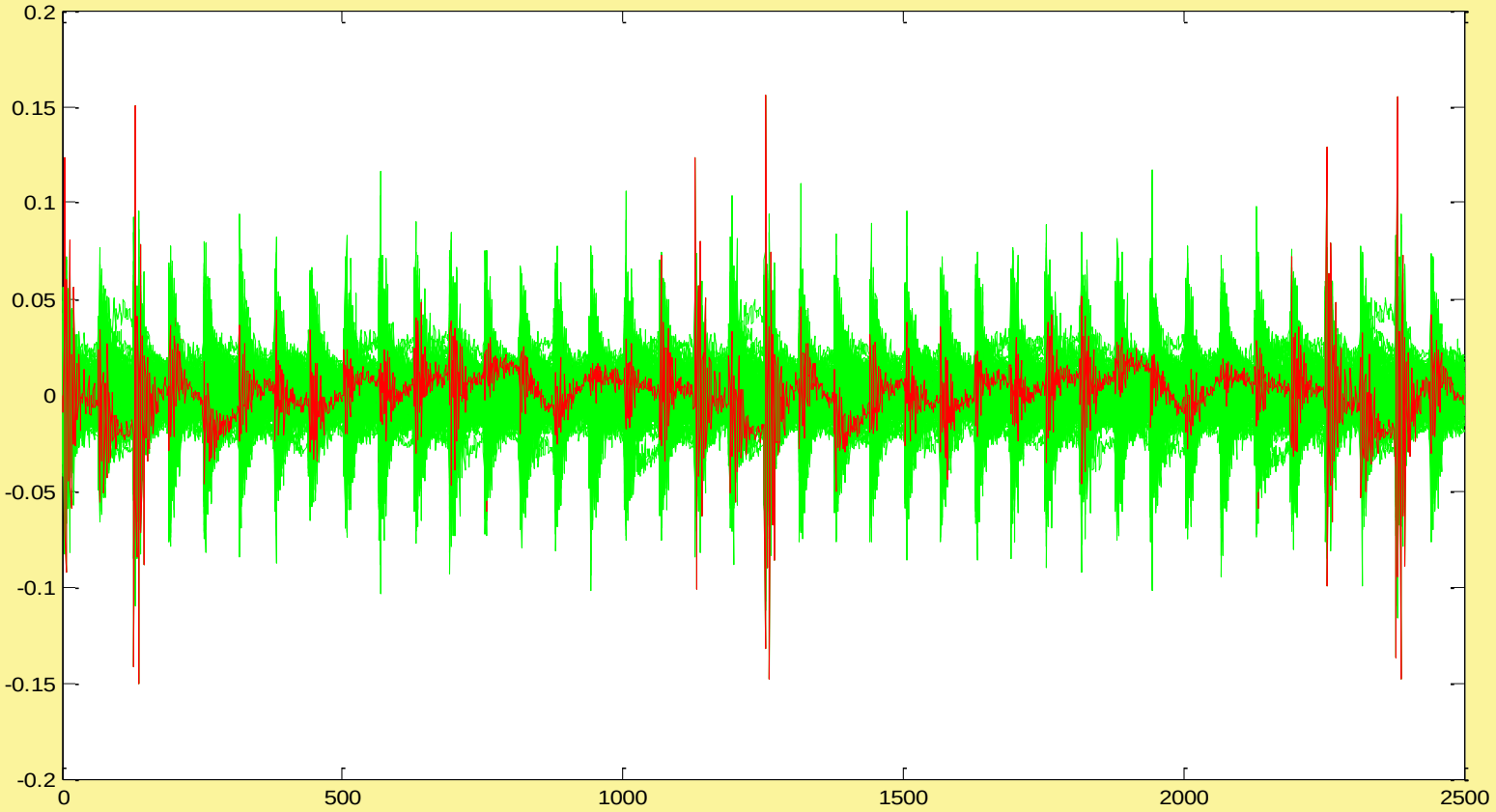
DPA Mathematically

- Attacker now computes a k-sample differential trace $\Delta_D[1..k]$ by finding the difference between the average of the traces for which D(…) is one and the average for which D(…) is zero.

$$\Delta_D = \frac{\sum_{i=1}^{m} D(C_i, b, K_s) T_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_s)} - \frac{\sum_{i=1}^{m} (1 - D(C_i, b, K_s)) T_i[j]}{\sum_{i=1}^{m} (1 - D(C_i, b, K_s))}$$

Principle: If K_s is wrongly guessed, D behaves like a random guess. Thus for a large number of sample points, ΔD[1..k] tends to zero. But if its correct, the differential will be non-zero and show spikes when D is correlated with the value being processed.

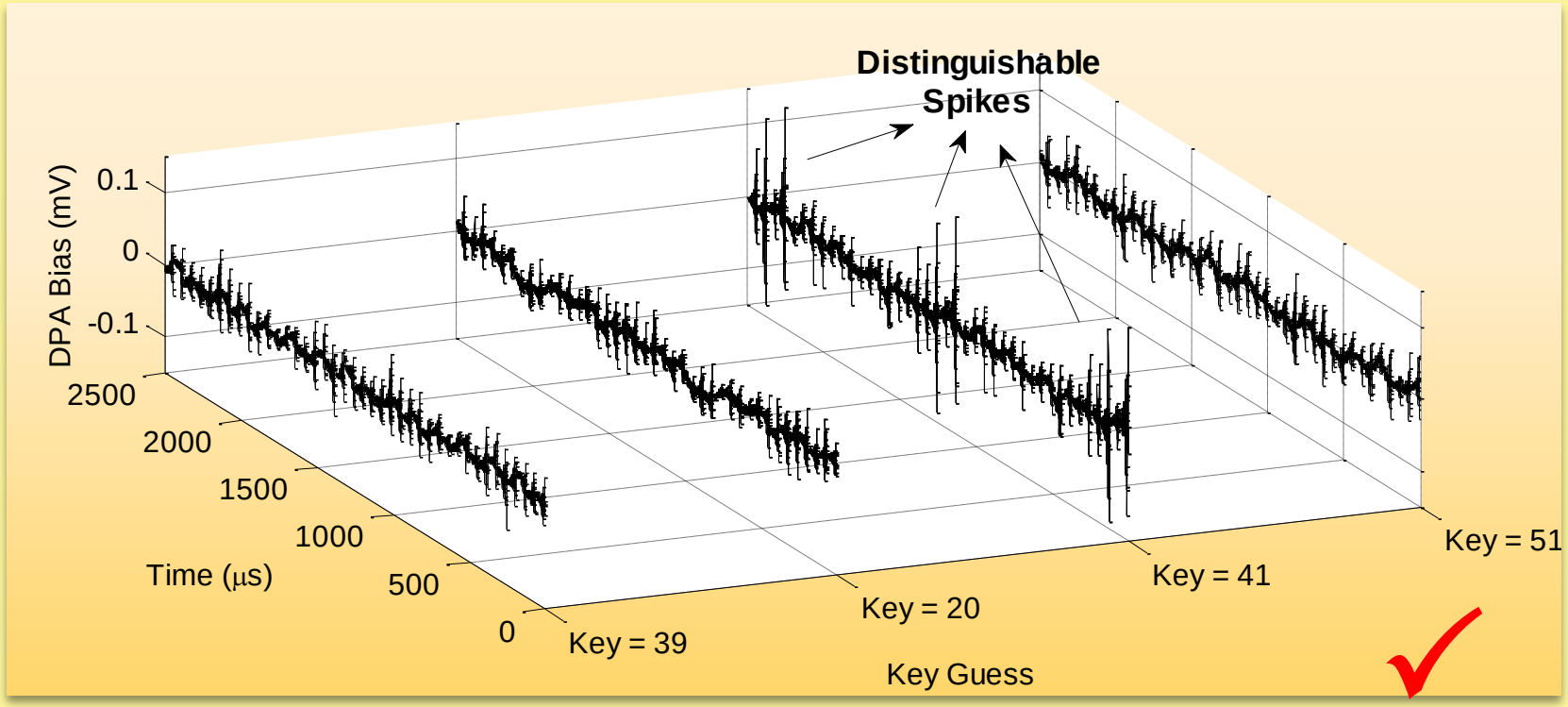
DPA Results - DES



2D Differential Plot

SBOX – 3 **BIT – 3** **TRACE COUNT = 4,000**

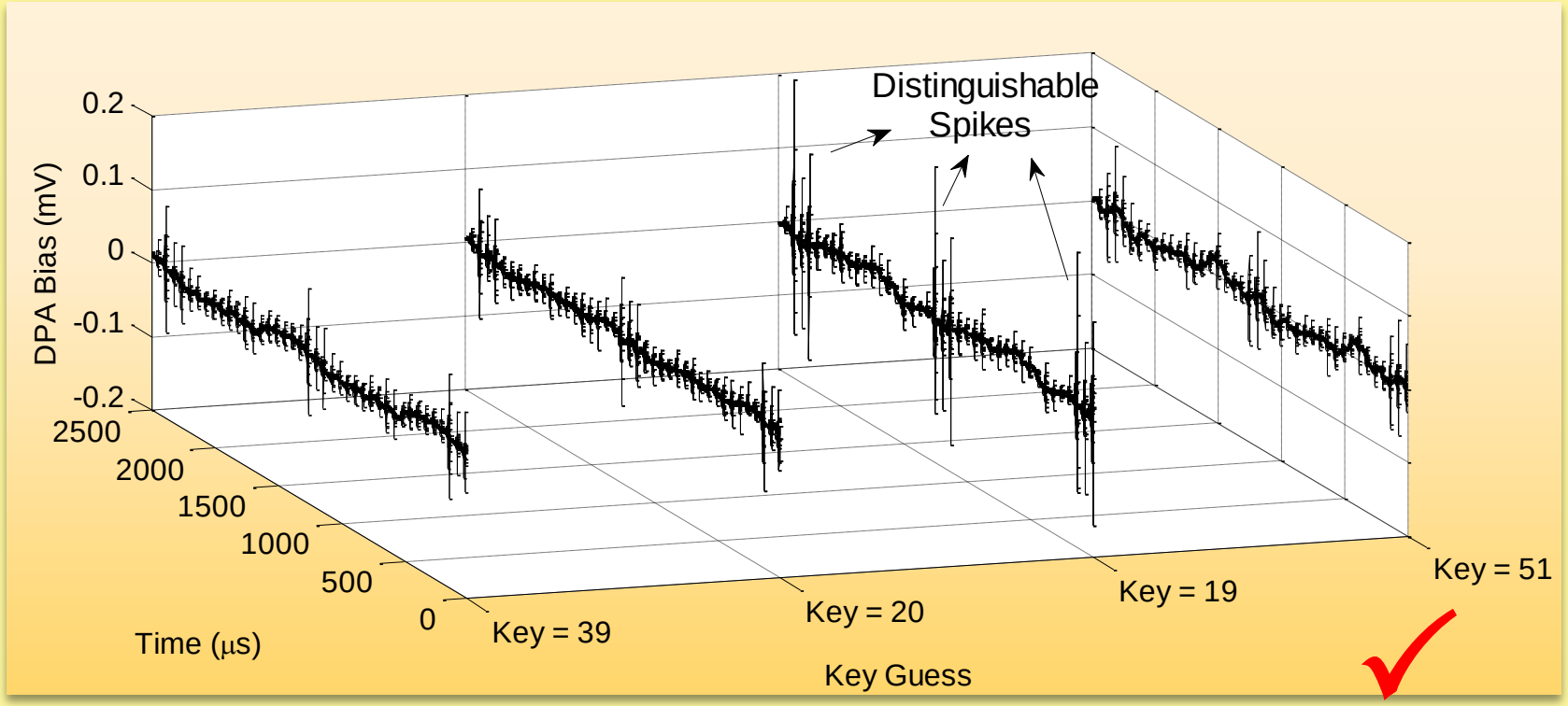
DPA Results - DES



3D Differential Plot

SBOX – 3 **BIT – 3** **TRACE COUNT = 4,000**

DPA Results - Triple-DES

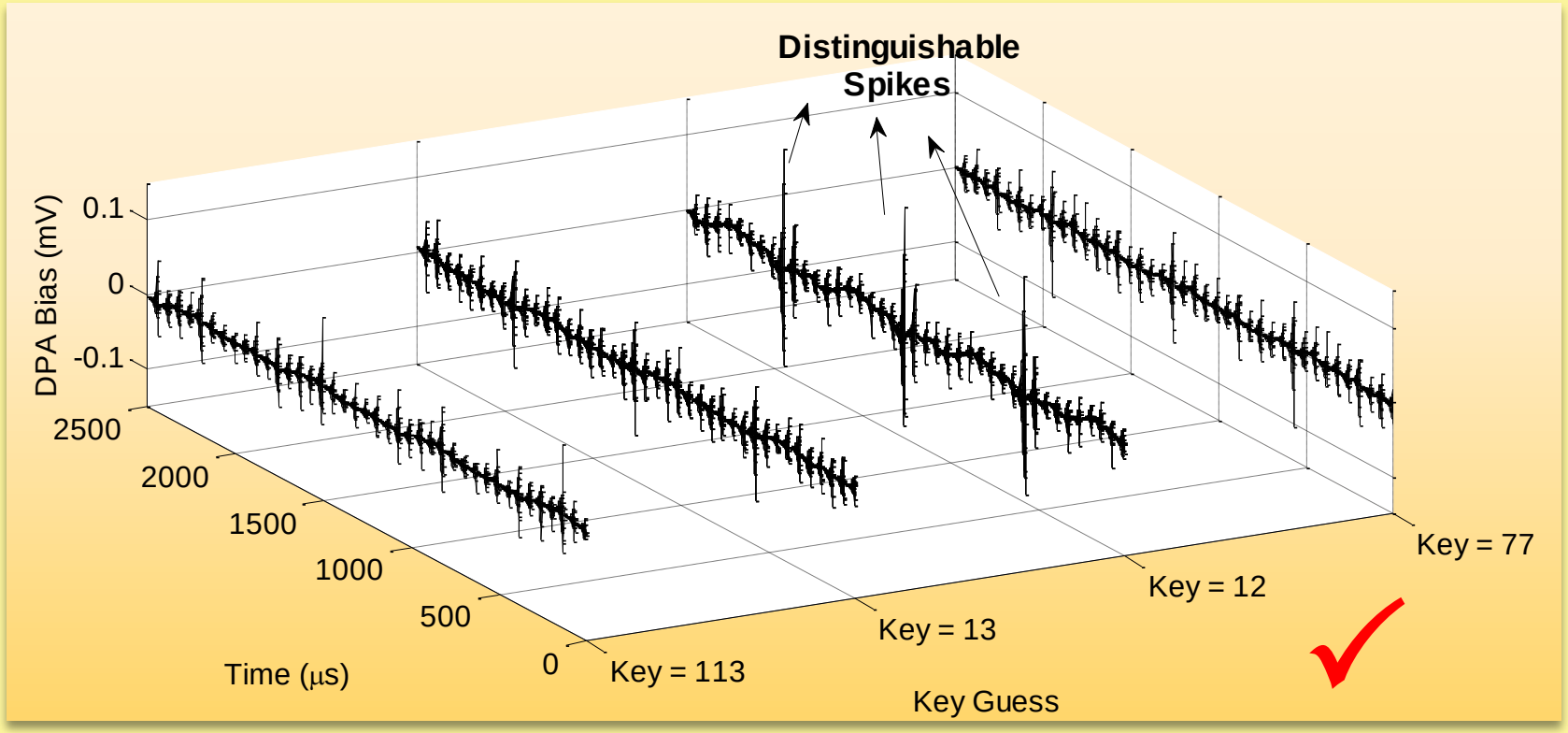


3D Differential Plot

SBOX – 4 **BIT – 2** **TRACE COUNT = 10,000**

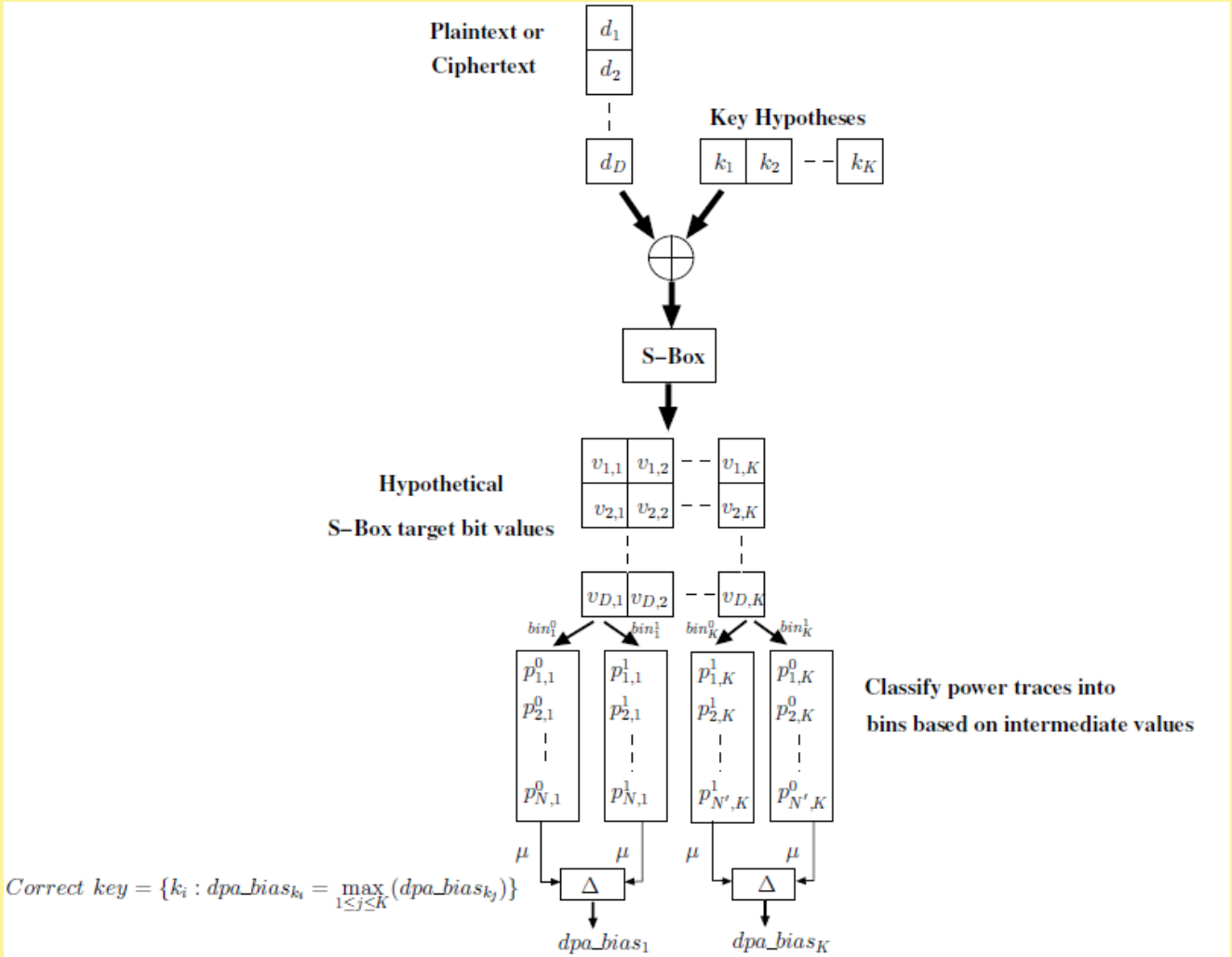
DPA Results - AES

3D Differential Plot



SBOX – 11 **BIT – 8** **TRACE COUNT = 15,000**

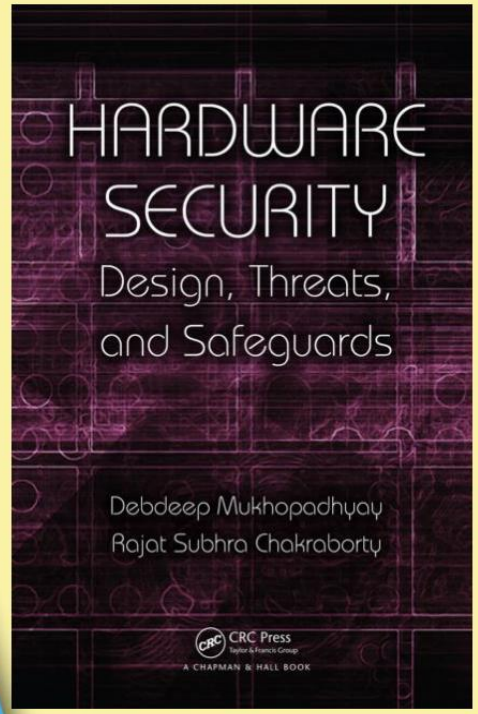
Summary of the DOM based Differential Power Analysis



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.

Conclusion:

DPA works because of the dependence of power consumption on state bits.

DPA works because of the fundamental way of computation

We discussed about DOM Method.

We applied DOM to a Toy cipher

Applying DOM for AES.

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!