NPTEL ONLINE CERTIFICATION COURSES

Course Name: Hardware Security

Faculty Name: Prof Debdeep Mukhopadhyay

Department : Computer Science and Engineering

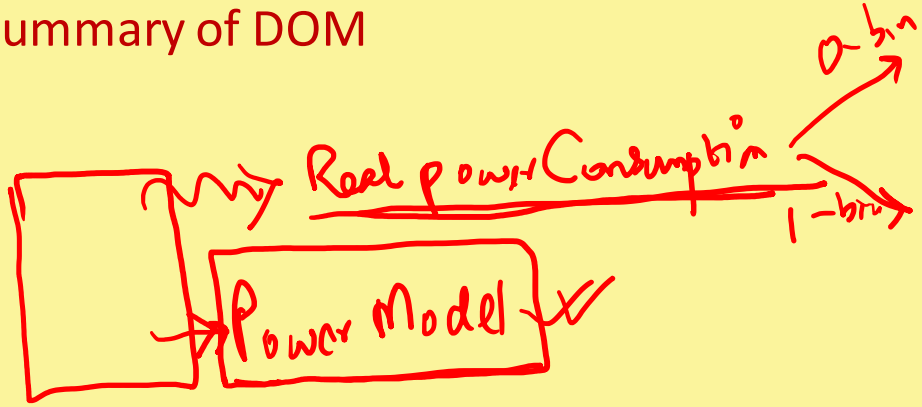
Topic

Lecture 26: Power Analysis-II

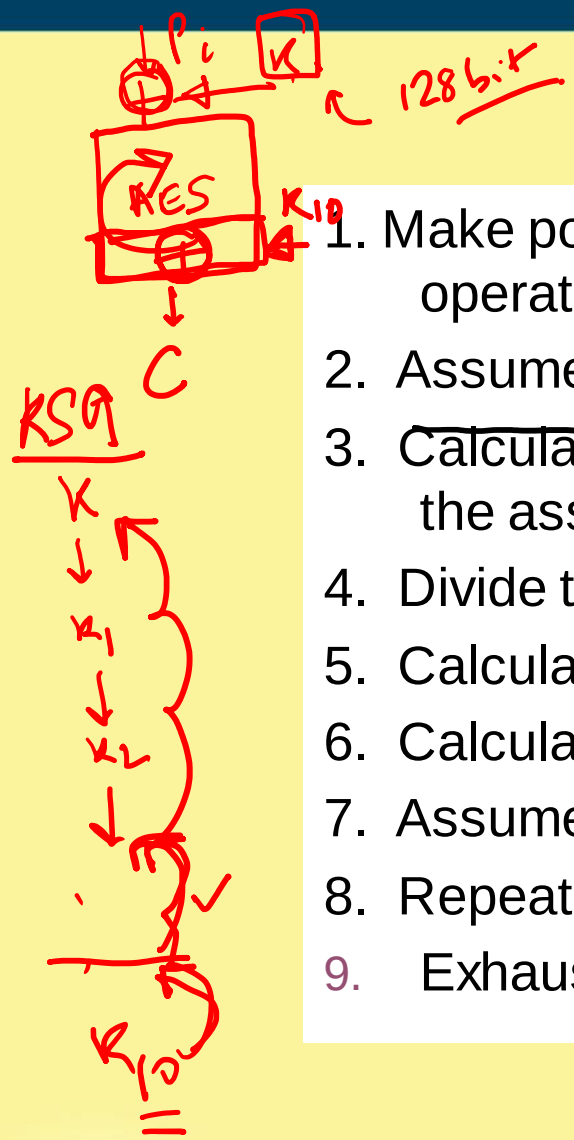
CONCEPTS COVERED

Concepts Covered:

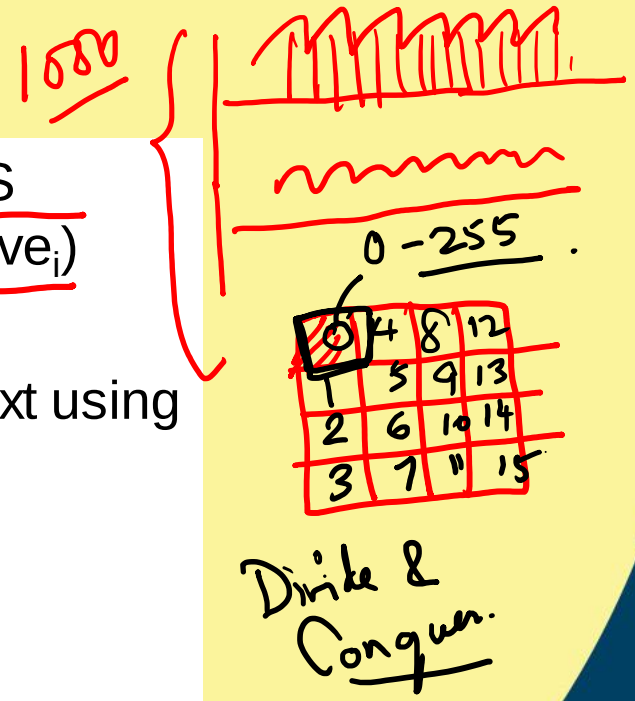
- Difference-of-Mean (DOM) Method
- DOM on AES
- Selection Function
- DOM on actual power traces on AES, DES, 3-DES
- Summary of DOM



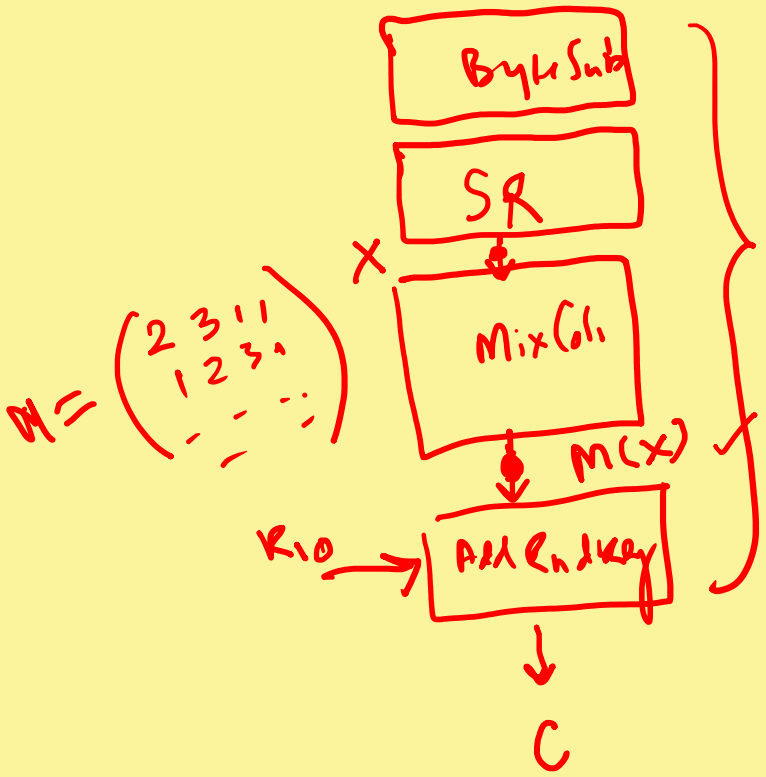
DPA Procedure for AES



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.



Last Round of AES



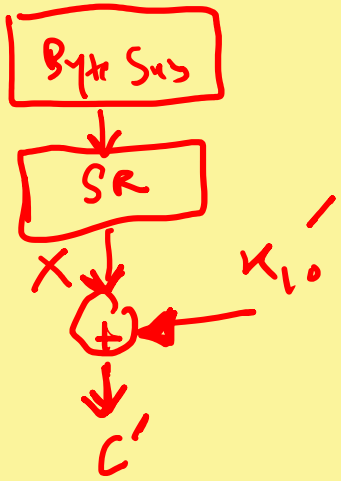
Key scheduling Rounds

1-9

Byte Sub.
Shift Row
Mix Columns.
Add Round key

Last Round | Byte Sub, Shift Row, Add Round key

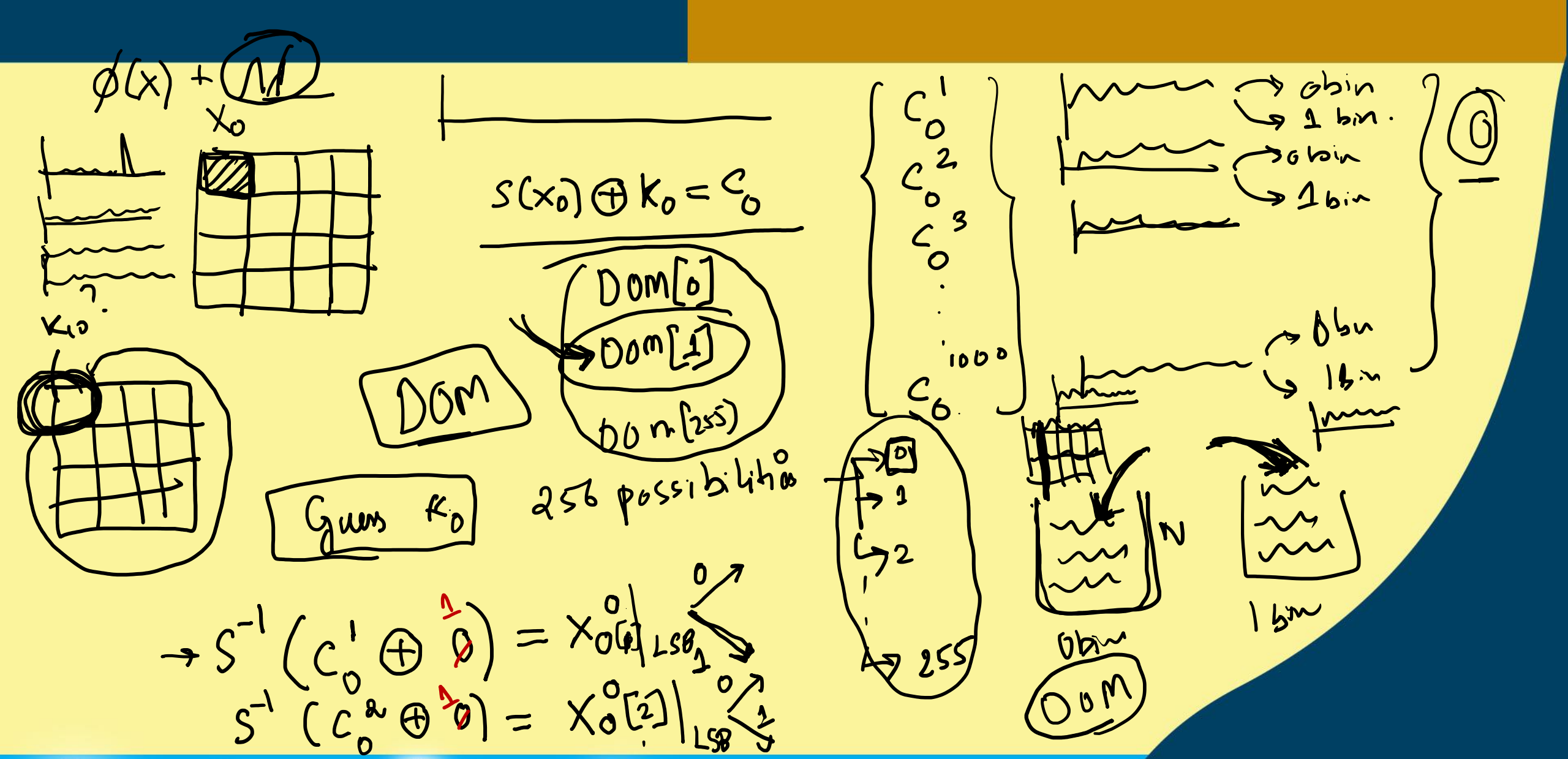
$\simeq$



Symmetry of Enc & Dec process we don't remove SR from the last Round

$$C = M(X) \oplus K_{10} = M(X \oplus M^{-1} K_{10}) \Rightarrow M^{-1} C = X \oplus M^{-1} K_{10}$$

or, $C' = X \oplus K_{10}$


$\phi(x)$ + M
x_0
k_0
$S(x_0) \oplus k_0 = c_0$
DOM
Dom[0]
Dom[1]
Dom[255]
Guess k_0
256 possibilities
c_0^1
c_0^2
c_0^3
c_0^{1000}
c_0
0bin
1 bin.
0 bin
1 bin
0
0bin
1bin
0
1
2
255
N
0bin
DOM
1bin
$S^{-1}(c_0^1 \oplus 0) = X_0^0[1]|_{LSB}$
$S^{-1}(c_0^2 \oplus 0) = X_0^0[2]|_{LSB}$

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.)

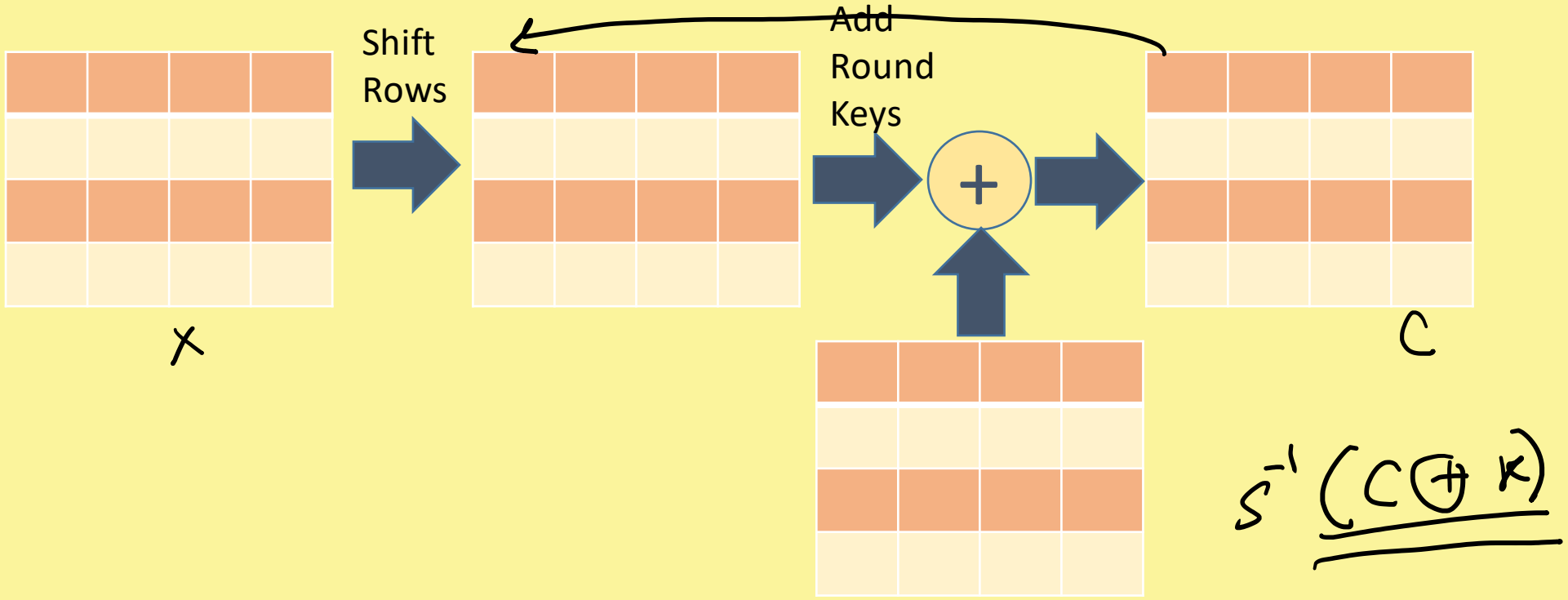
Sample Points

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 $\mathbb{D}$

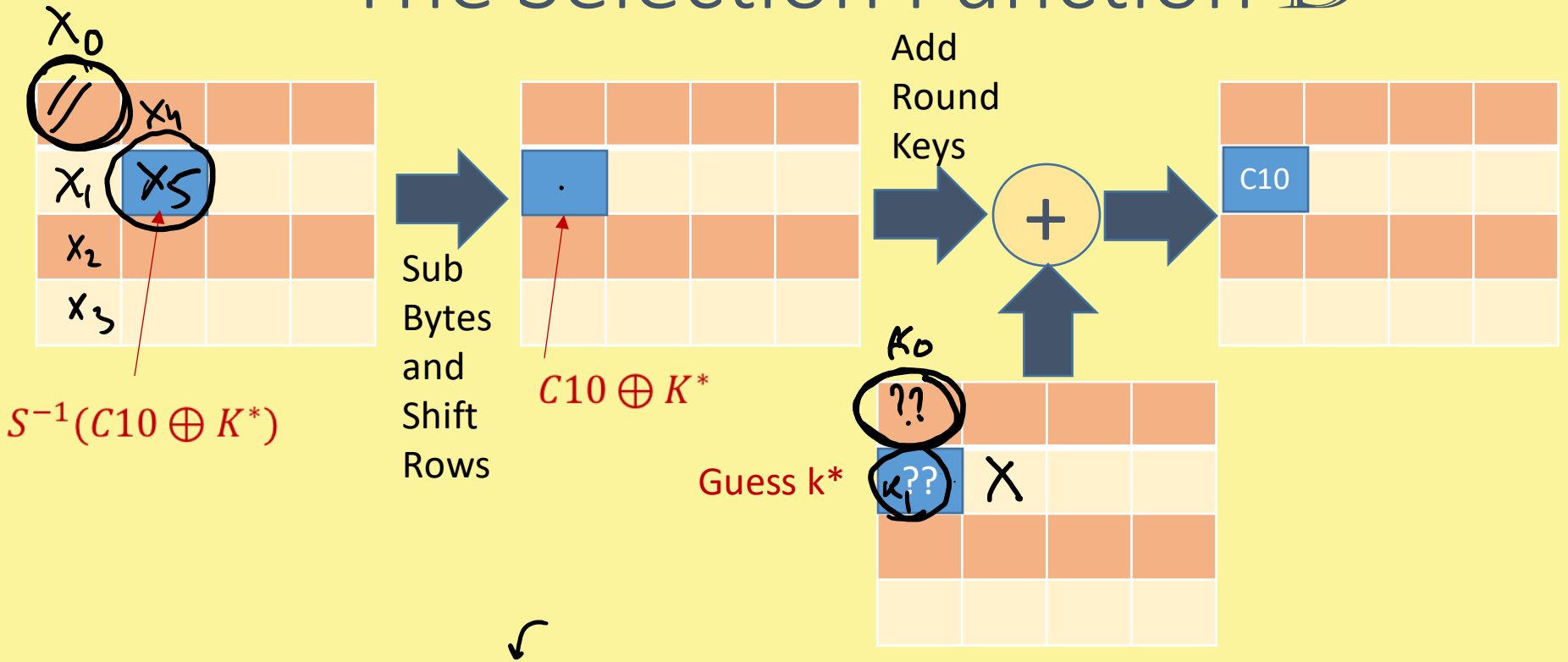


$S^{-1}(C \oplus K)$

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

DES

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.

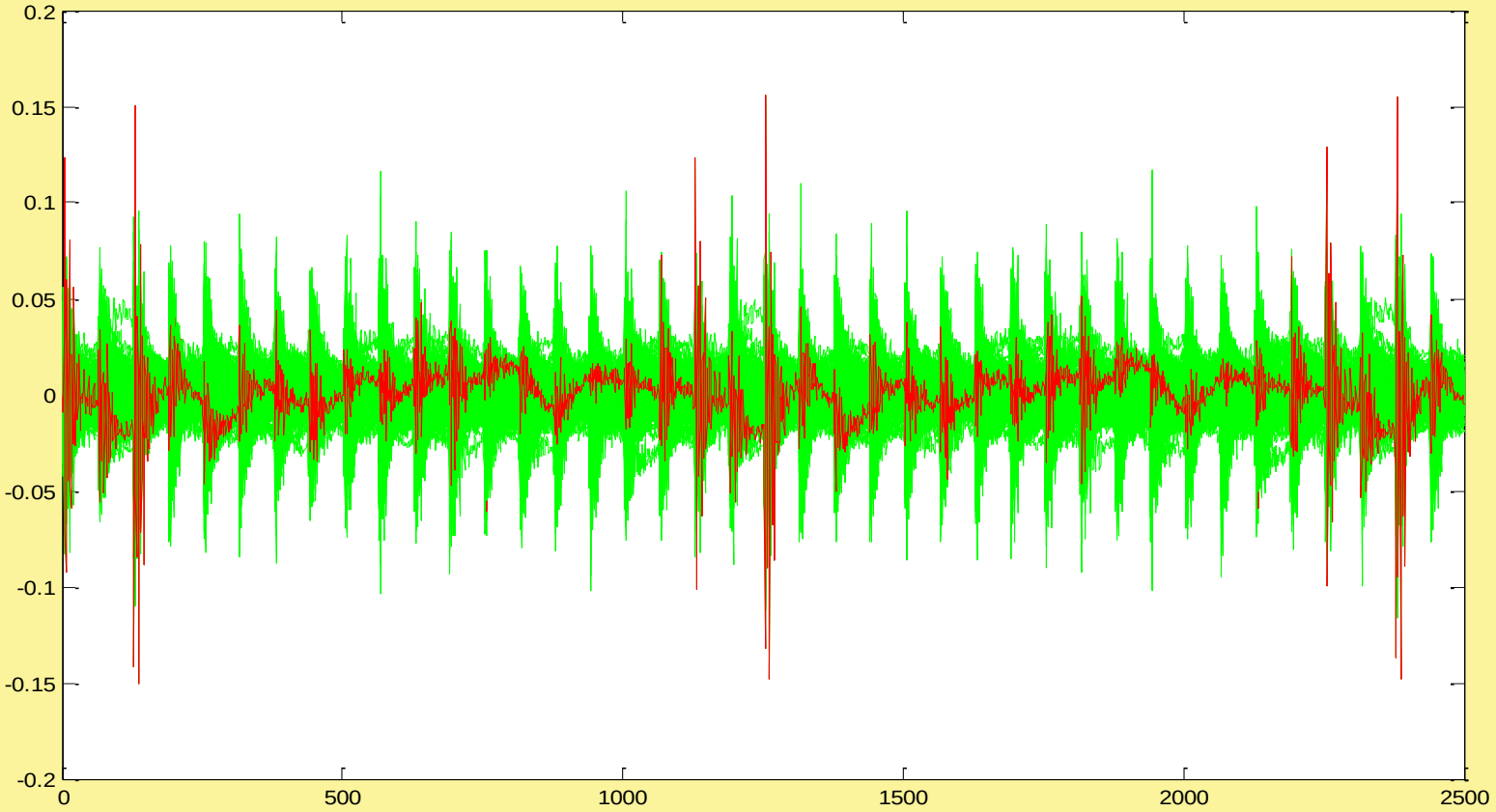
DPA Mathematically

- 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.

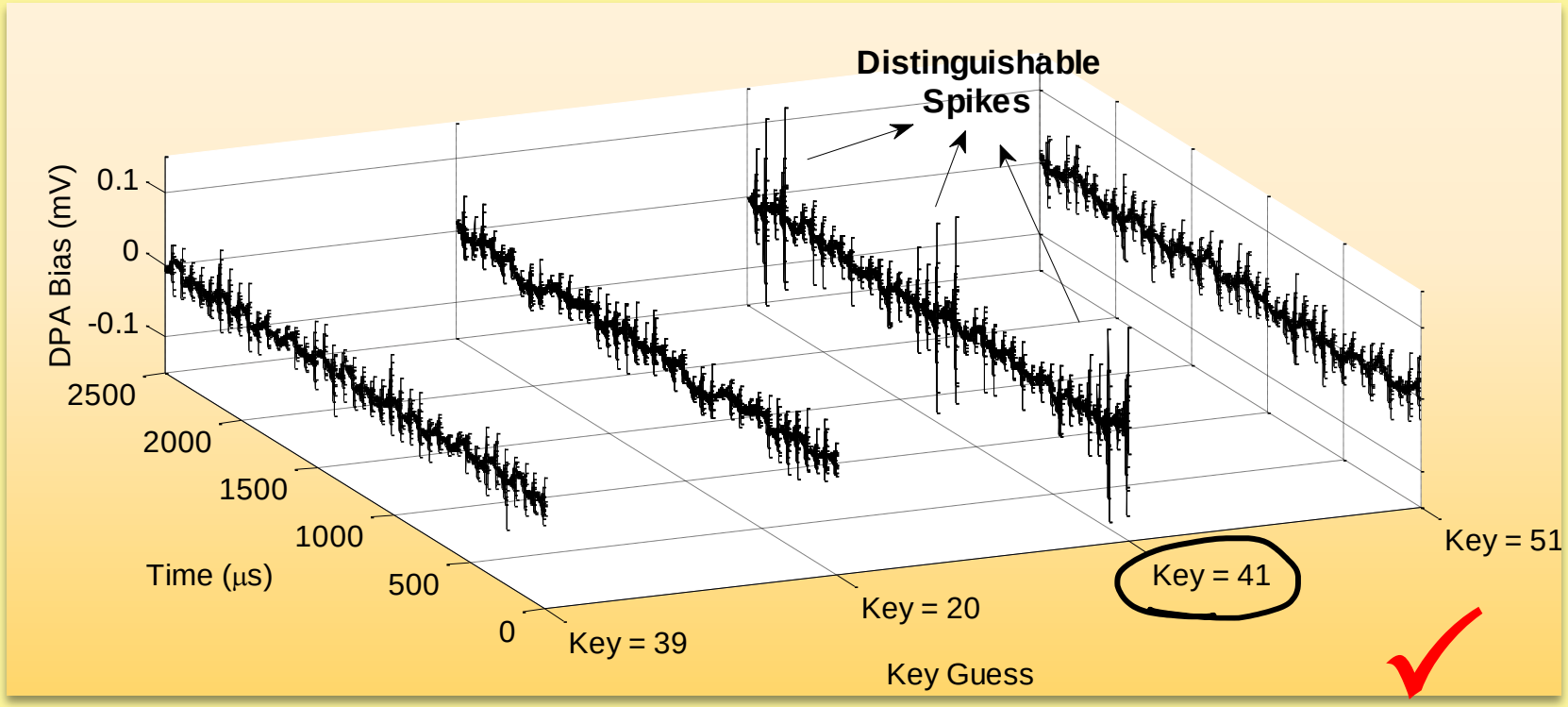
DPA Results - DES



2D Differential Plot

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

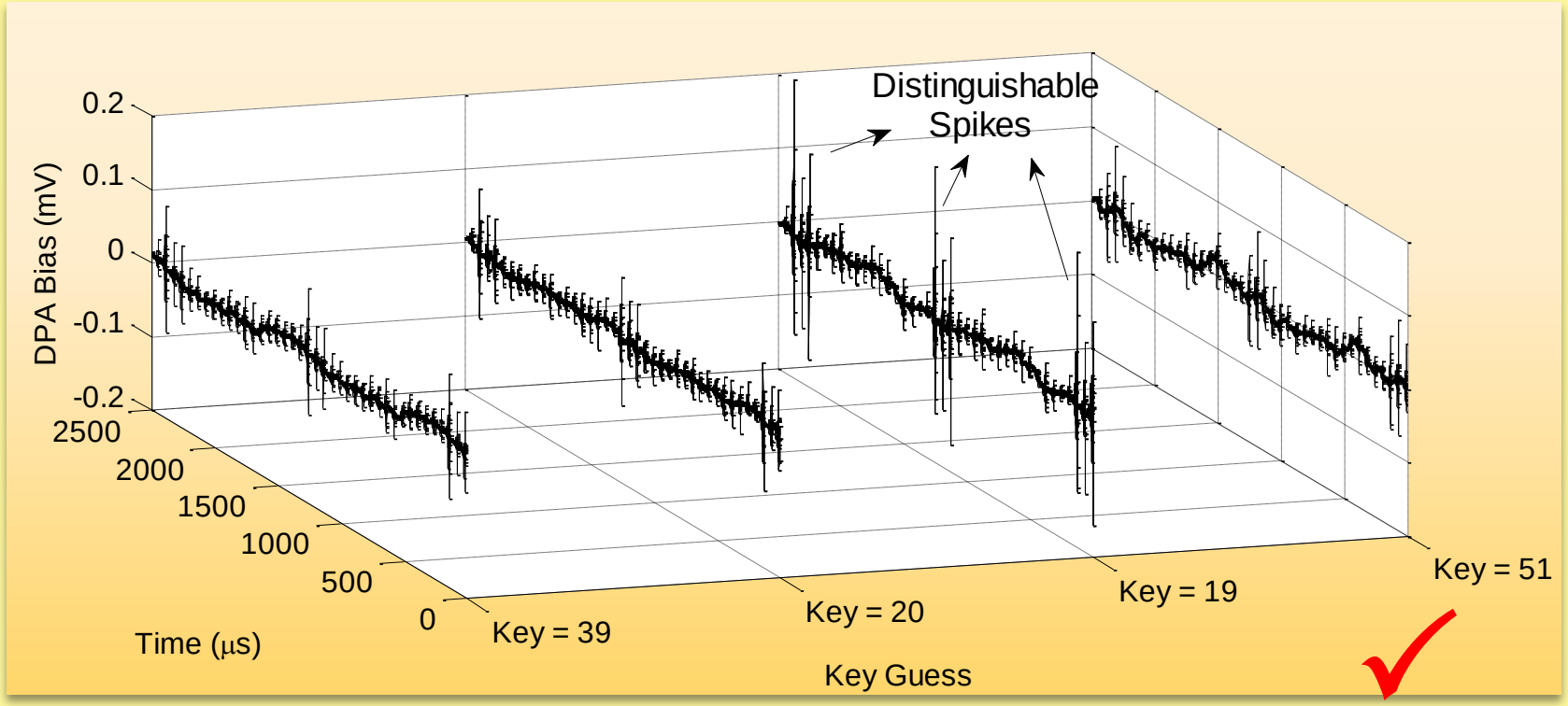
DPA Results - DES



3D Differential Plot

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

DPA Results - Triple-DES

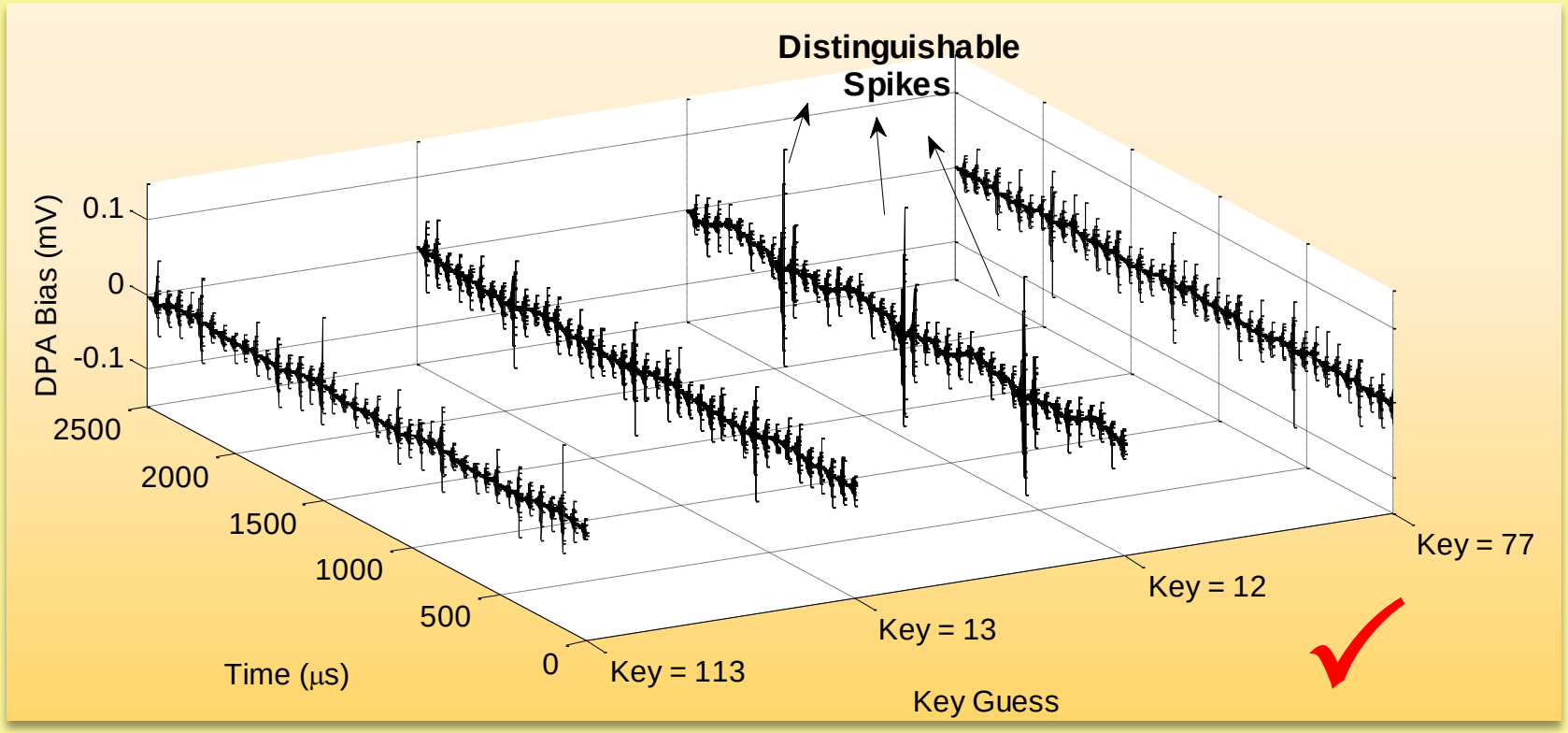


3D Differential Plot

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

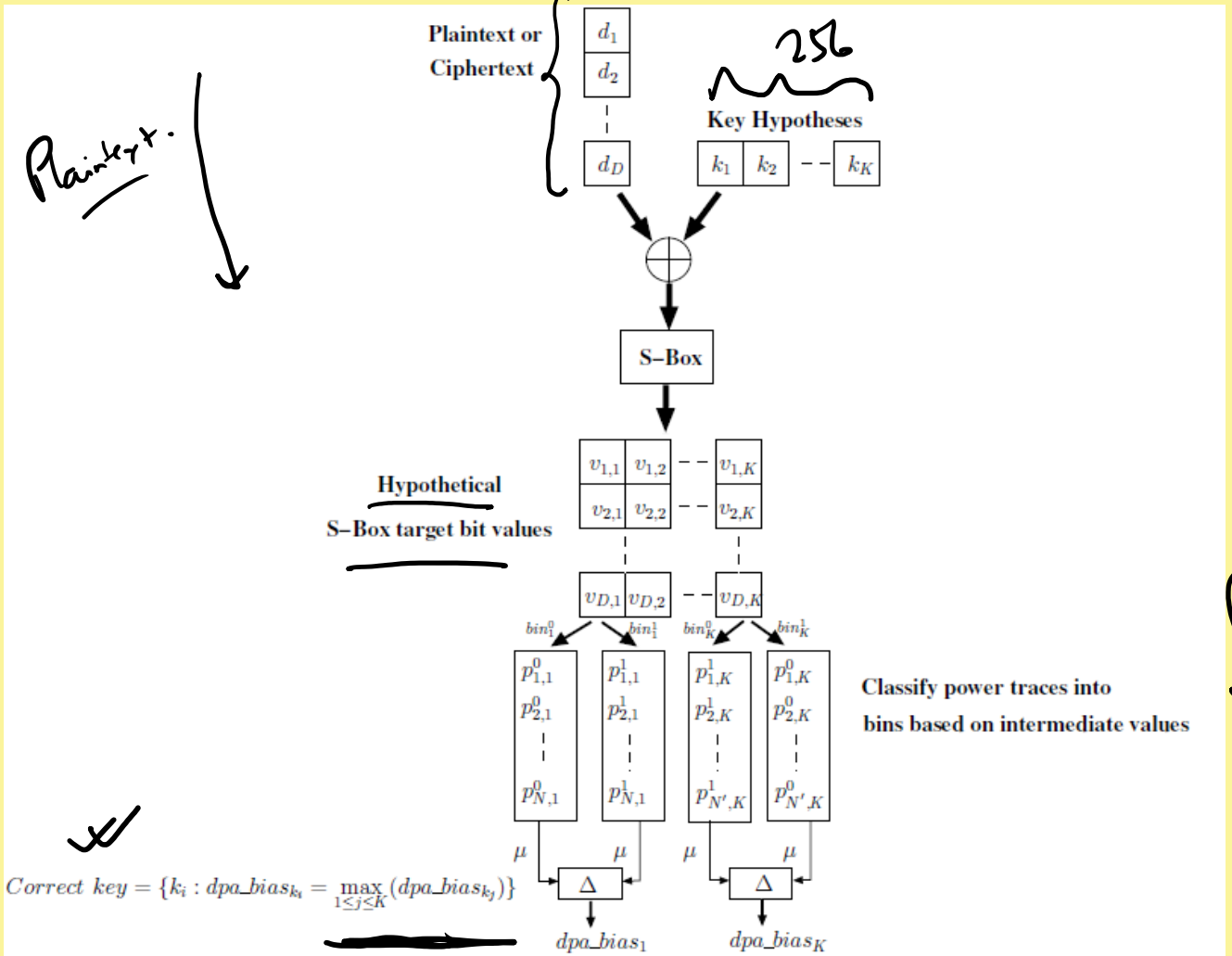
DPA Results - AES

3D Differential Plot



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

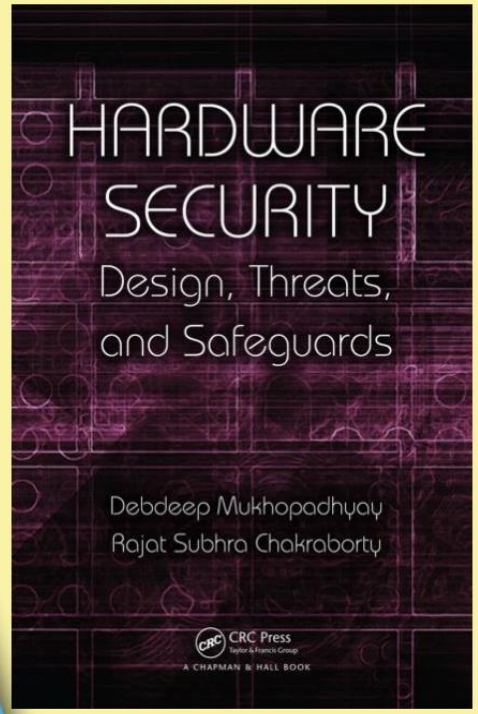
Summary of the DOM based Differential Power Analysis



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!