Cryptanalysis of AES

Dept. of Computer Science & Engg.
IIT Kharagpur, India

Types of Cryptanalysis/Attacks

- Algebraic Analysis

  Linear Cryptanalysis, Differential Cryptanalysis

- Algorithmic / Structural Analysis

  Man-in-the-Middle Attack, Related Key Attack

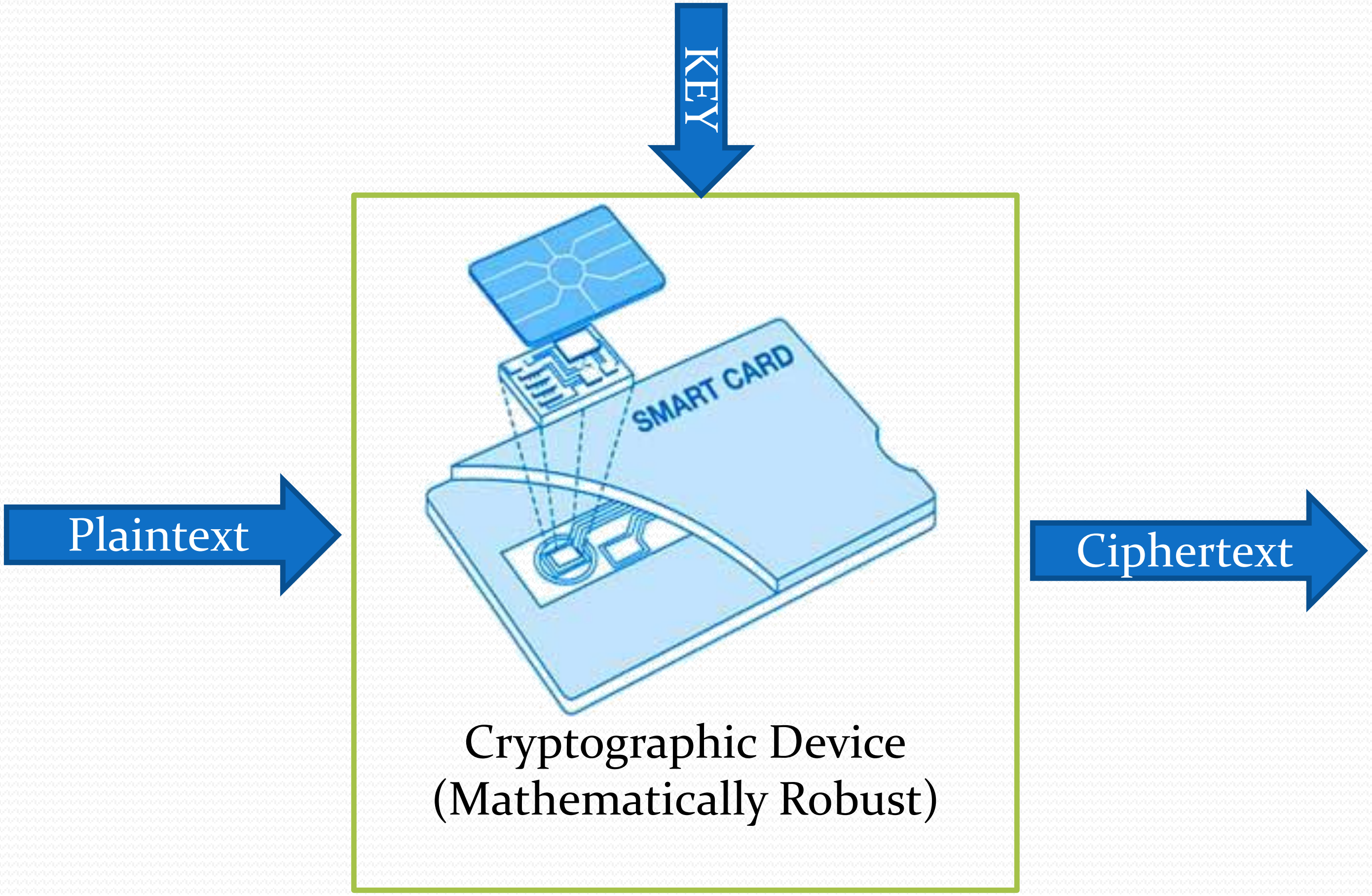
- Side Channel Analysis

  Power Attack, Timing Attack, Fault Analysis etc.

What is a Side Channel Attack(SCA)?

- Most cryptographic algorithms are theoretically or computationally secure but their implementations may be vulnerable
- A 'side channel' is a source of information that is inherent to the physical implementation of a primitive viz, light, sound, power, etc.
- SCA exploits such vulnerabilities
- Implementation based attacks

Conventional Viewpoint



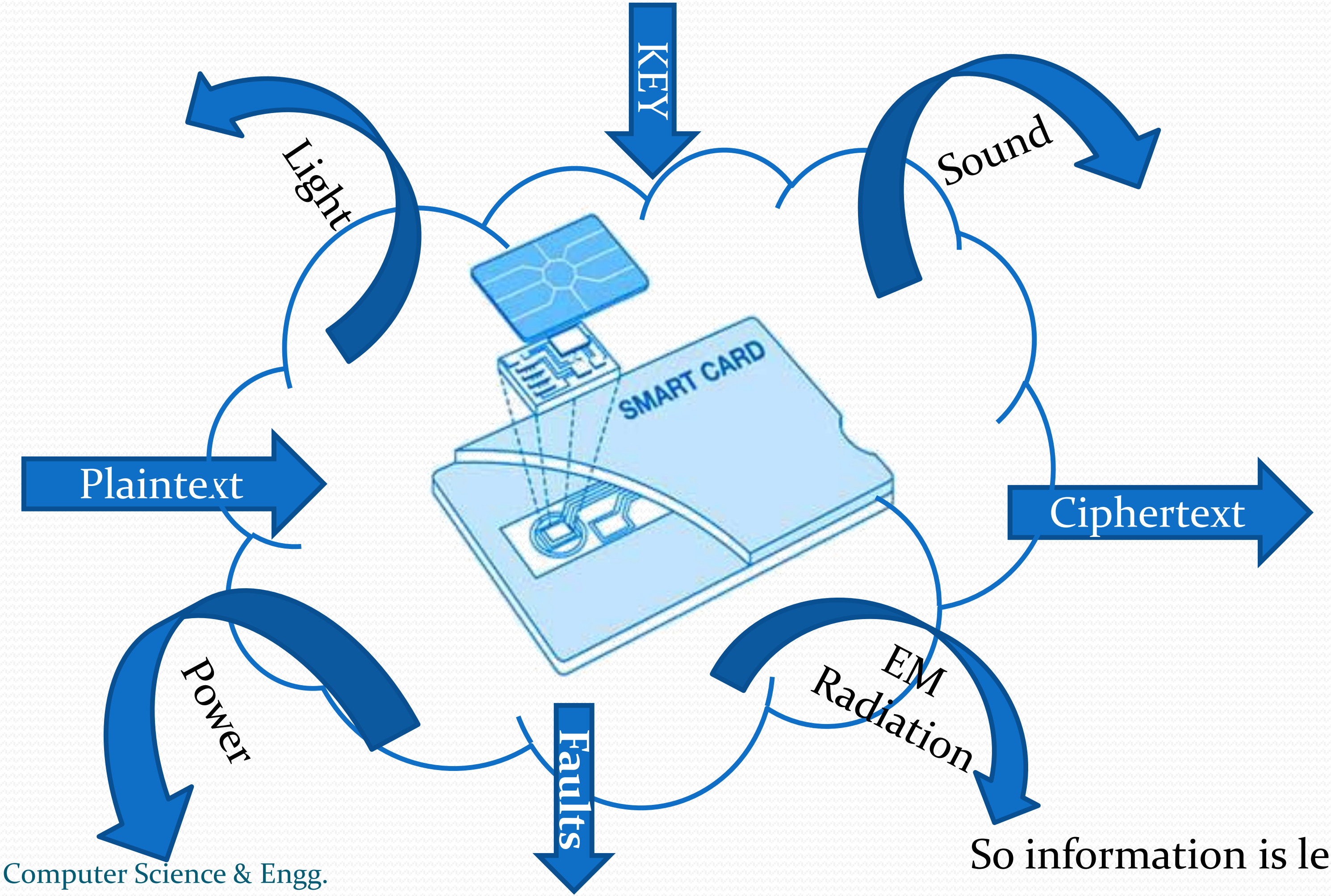
KEY

Plaintext

Ciphertext

Cryptographic Device
(Mathematically Robust)

Side Channel Viewpoint



So information is leaking.

Types of SCA

- Power Attacks
- Radiation Monitoring Attacks
- Acoustic Attacks
- Scan-Chain Based Attacks
- Fault Attacks

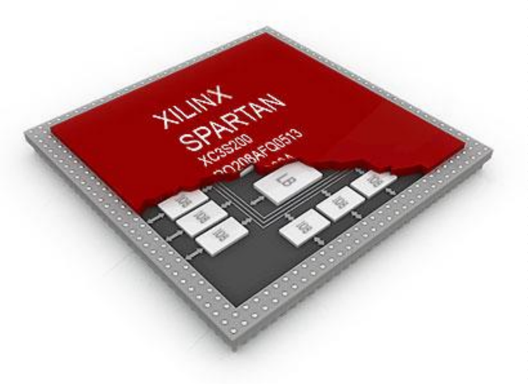
Our Focus

Underlying Idea:
Information leaked by these side channels can give useful information about the secret key

Hardware targets

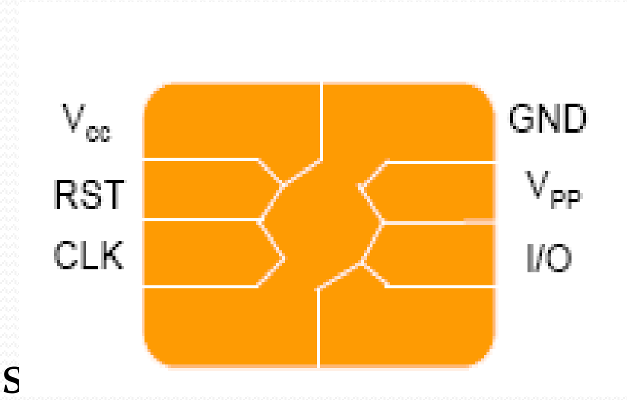
- The most common hardware that are targetted are
  - the smart cards (SC)

  - The FPGAs



Smart Cards

- It has a small processor (8bit or 32bit) long with ROM, EEPROM and a small RAM



- There are eight wires connecting the process
- Power supply: SCs have no internal batteries, the current provided by the reader
- Clock: SCs do not have an internal clock

Type of Attack classification

- Many possible attacks, the attacks are often not mutually exclusive
- Invasive vs. noninvasive attacks
- Active vs. passive
  - Active attacks tamper with device's proper functionality, either temporary or permanently
- Passive, Non-invasive attacks and relatively inexpensive

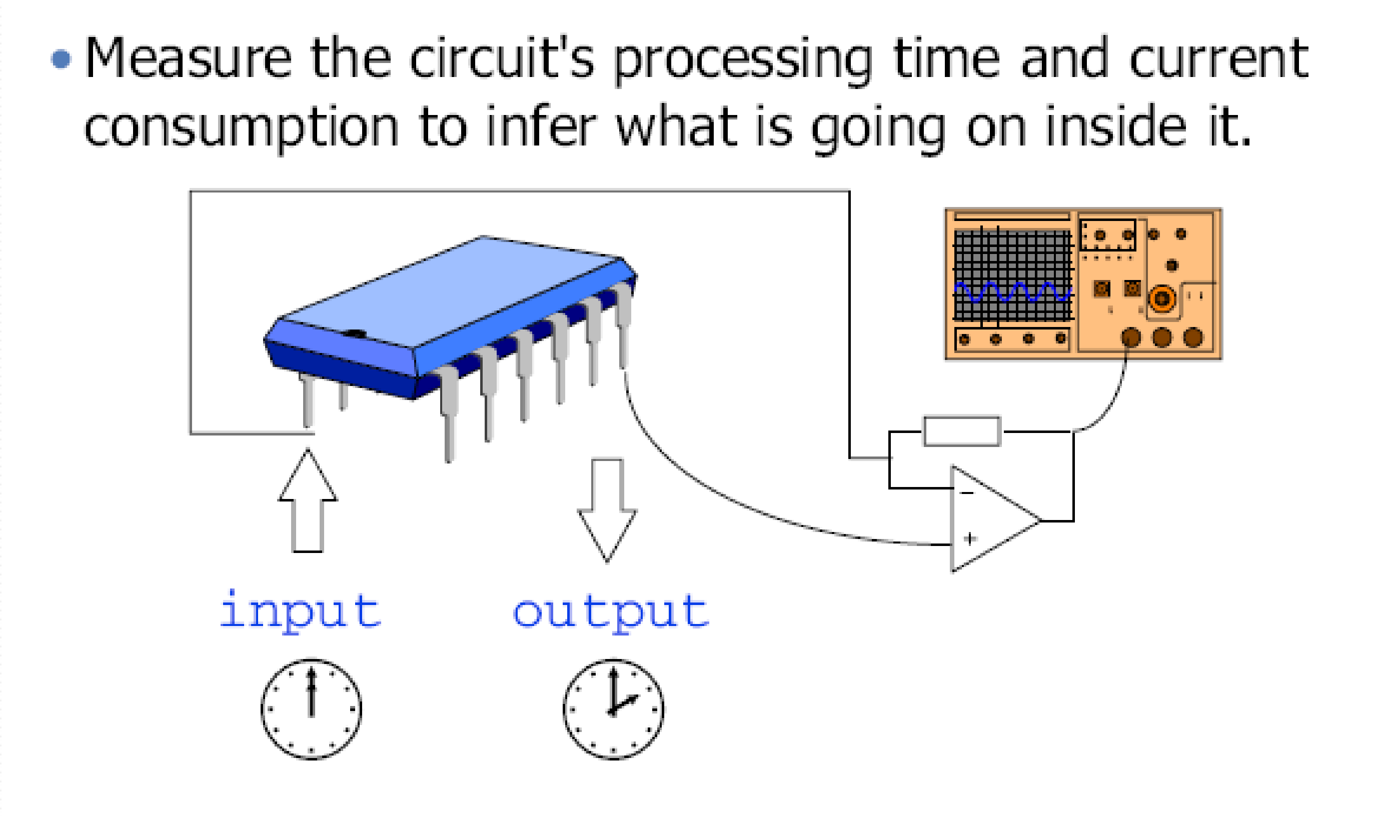
Major Attack Groups

- Probing attack (invasive)
- Fault injection attacks – active attacks , maybe invasive or noninvasive
- Timing attacks exploit device’s running time
- Power analysis attack
- Electromagnetic radiation attacks

Type of Side Channel Attacks

- **Power attacks**
- Electromagnetic Radiation attacks
- Timing attacks
- Fault attacks
- Scan Attack

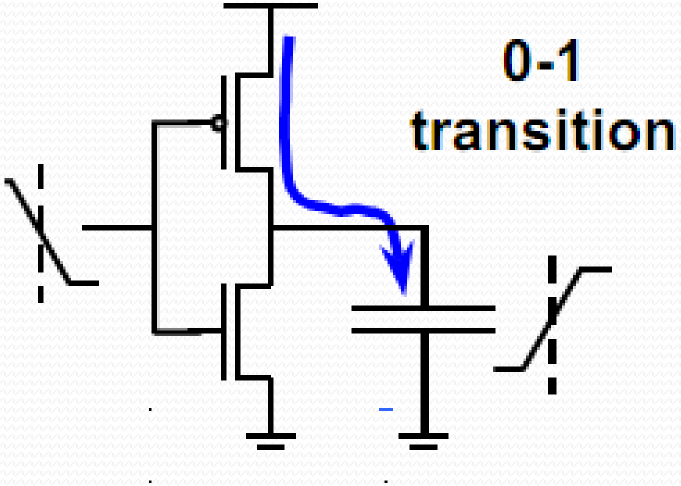
Power attacks



- Measure the circuit's processing time and current consumption to infer what is going on inside it.

Basic Principle of Power Analysis

Input	Output	Dynamic Power Consumption
0 → 0	1	No
0 → 1	1 →0	Discharge
1 → 0	0 →1	Charge
1 → 1	0	No



The CMOS Inverter

- ❖ CMOS – Most popular logic style
- ❖ CMOS inverter is the basic building block
- ❖ Consumes power from supply when there is a 0 →1 transition in the output
- ❖ Switching Activity – Number of times the output of a logic gate switches
- ❖ Basic assumption - Power dissipation is a function of the switching activity

Power Attacks

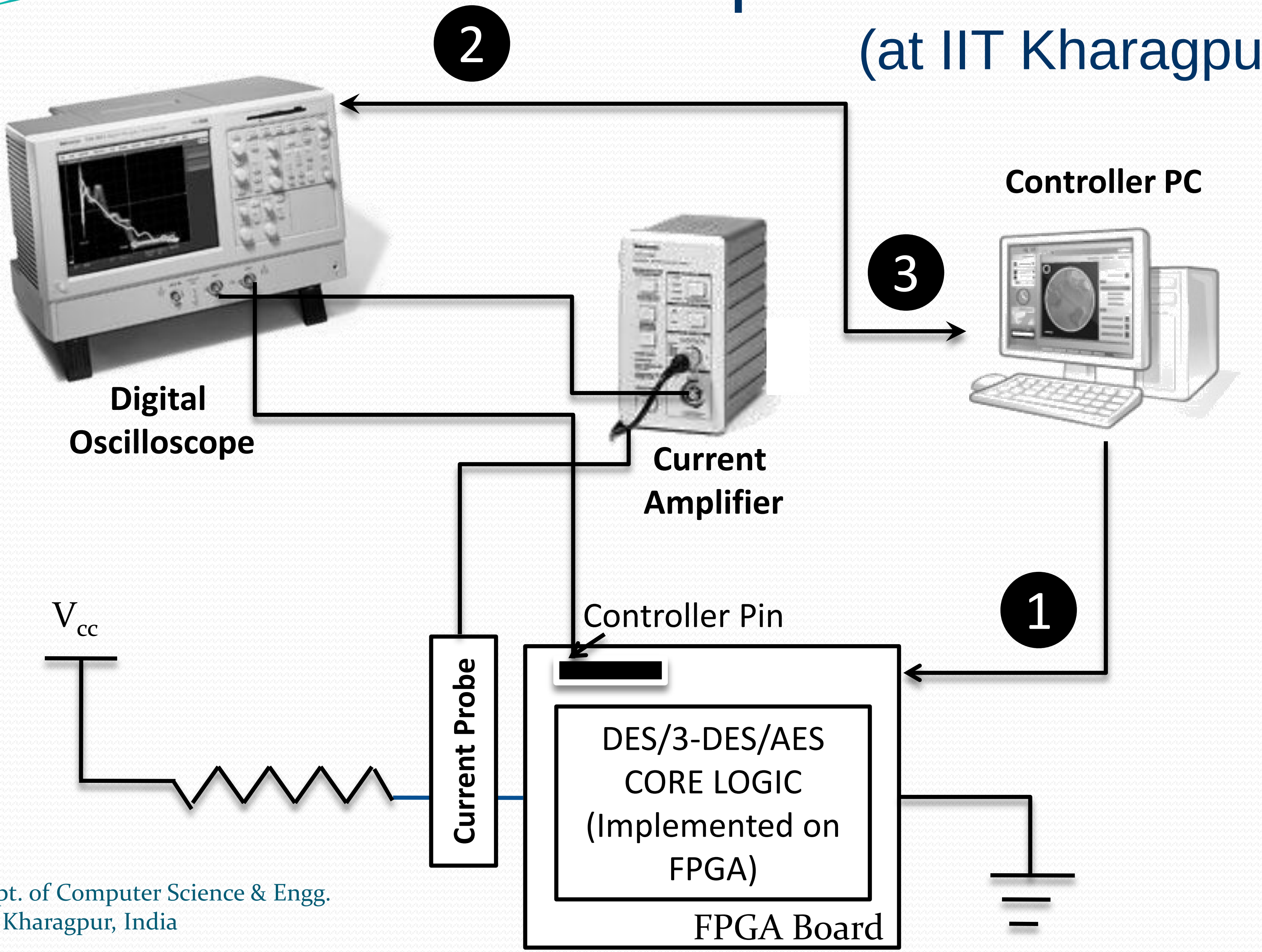
- SPA – Simple Power Analysis Attacks
  - Fact exploited - Power consumption at an instant of time is a function of the operation being carried out by the device
- DPA – Differential Power Analysis Attacks
  - Fact exploited - Power consumption of the same operation at different instants of time depends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

Power Attacks (PA)

- During the last few years (eight ?) lot of research has been conducted on Differential Power Attacks (DPA)
- Exploit the fact that (dynamic) power consumption of chip is correlated to intermediate results of the algorithm
- To measure a ckt's power, a small resistor (50 ohm) is inserted in series with the power or ground input

Experiment Set-up

(at IIT Kharagpur)



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
- As an example: 1 millisecond operation sampled at 5MHz yield a trace with 5000 points

Simple Power Analysis (SPA) of DES

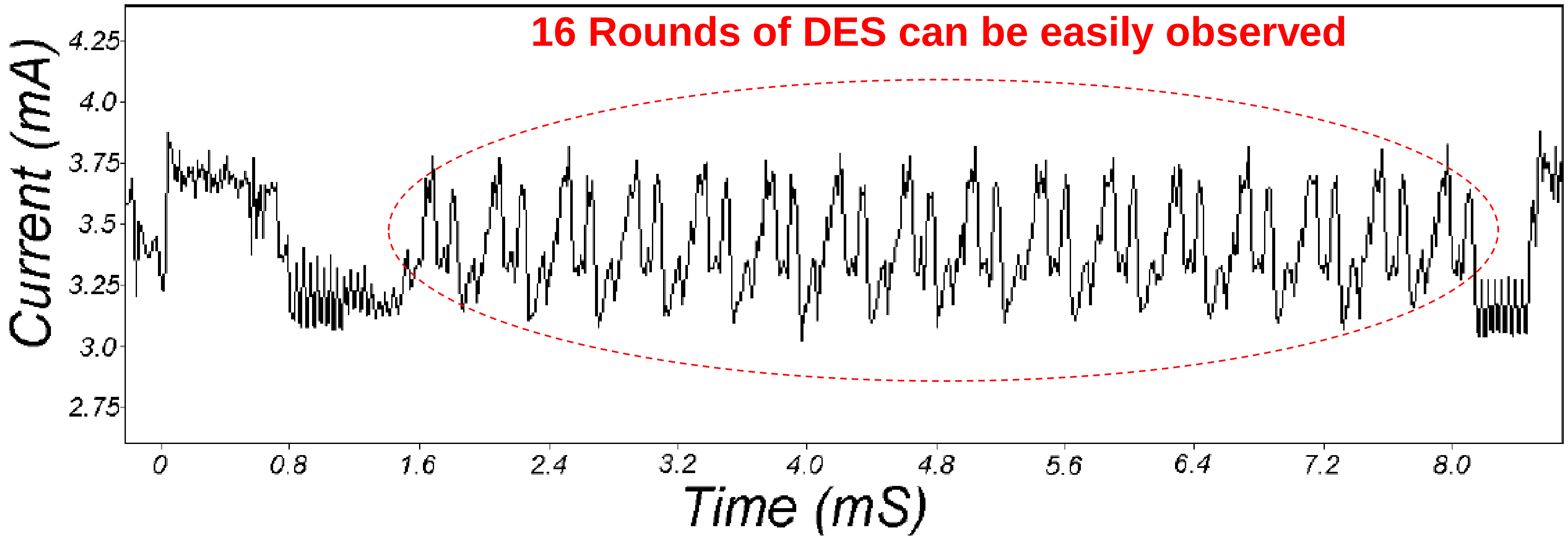
- Conditional branching in software or microcode can cause significant power consumption differences for “0" and “1" bits. Comparison operations typically perform a conditional branch when a mismatch is found. This conditional branching causes large SPA (and sometimes timing) characteristics.

Example - DES key schedule: involves rotating 28- bit key registers. A conditional branch is commonly used to check the bit shifted. The resulting power consumption traces for a ”1" bit and a “0" bit will contain different SPA features if the execution paths take different branches for each.

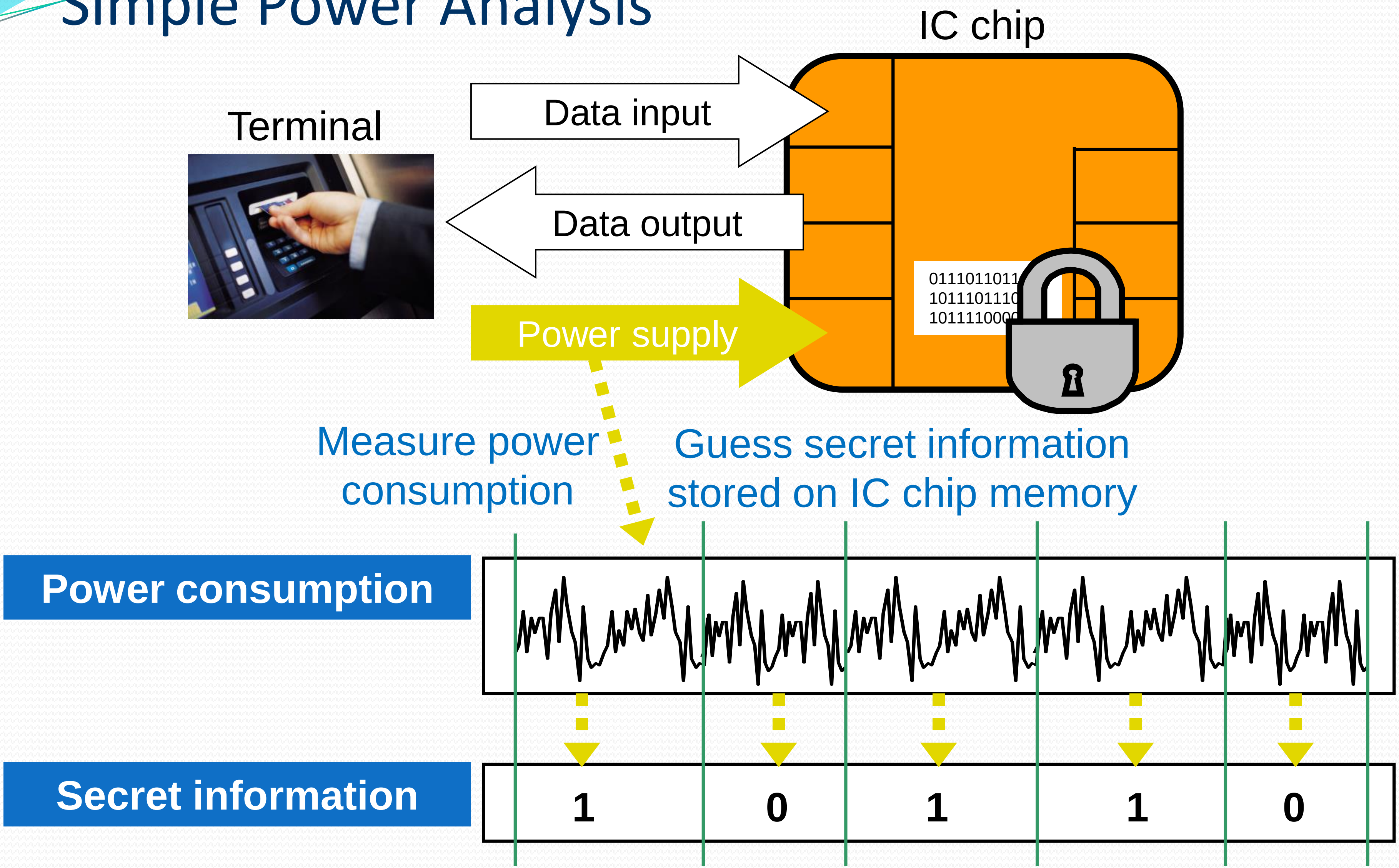
Simple Power Analysis (SPA)

- Multipliers: Modular multiplication circuits tend to leak a great deal of information about the data they process. The leakage functions are often strongly correlated to operand values and Hamming weights.
- Exponentiators: A simple modular exponentiation function scans across the exponent, performing a squaring operation in every iteration with an additional multiplication operation for each exponent bit that is equal to “1”. The exponent can be compromised if squaring and multiplication operations have different power consumption characteristics, take different amounts of time, or are separated by different code.

Power Traces of DES



Simple Power Analysis



IC chip

Terminal

Data input

Data output

Power supply

Measure power consumption

Guess secret information stored on IC chip memory

Power consumption

Secret information

1	0	1	1	0

Differential Power Analysis (DPA)

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)

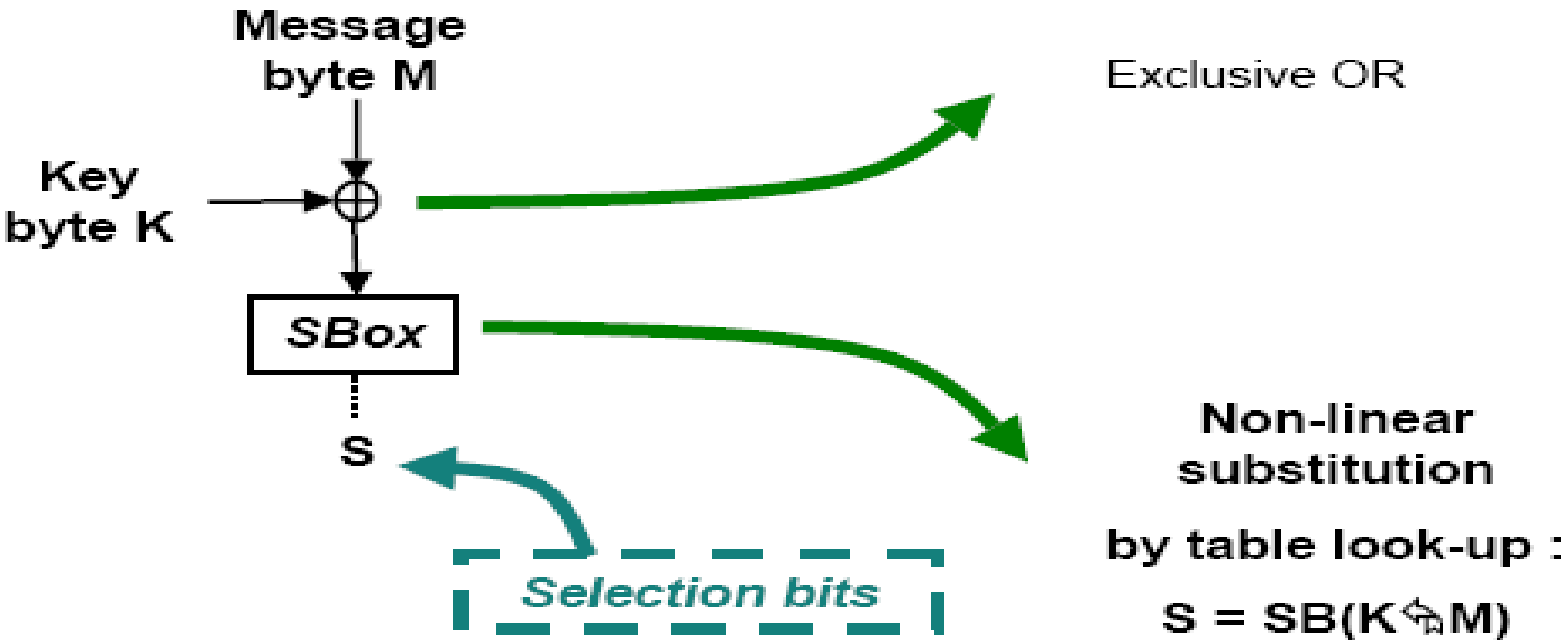
Data collection phase and data analysis phase

Procedure

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

Typical DPA Target

- Basic mechanism in Secret Key algorithms (AES, DES…)



Message byte M

Key byte K

SBox

S

Selection bits

Exclusive OR

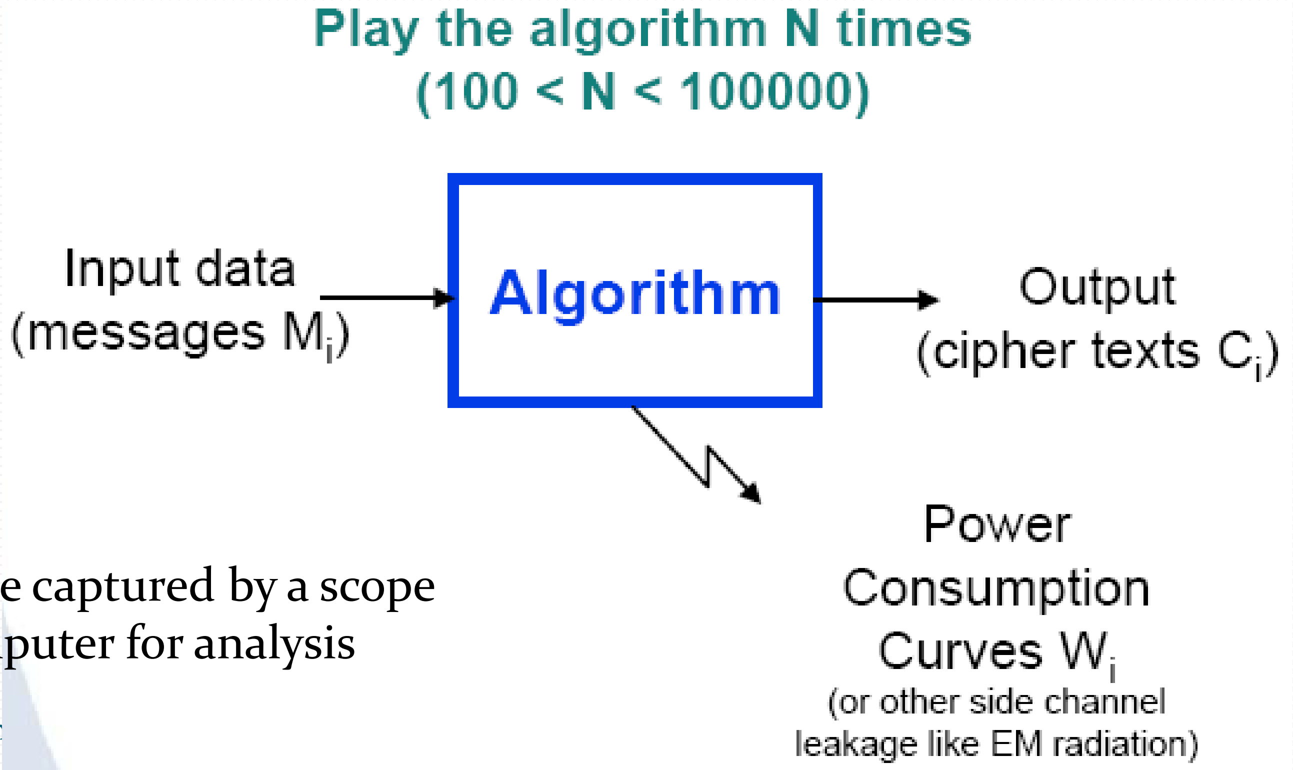
Non-linear substitution

by table look-up :

$S = SB(K \oplus M)$

DPA (cont'd)

- DPA can be performed in any algorithm that has the operation C=S(P⊕K),
  - P is known and K is the segment key



Play the algorithm N times

(100 < N < 100000)

Input data (messages M_i)

Algorithm

Output (cipher texts C_i)

Power Consumption Curves W_i

(or other side channel leakage like EM radiation)

The waveforms are captured by a scope and Sent to a computer for analysis

DPA Overview

The DPA selection function D(C; b; Ks) is defined.

If Ks is incorrect, evaluating D(C; b; Ks) will yield the correct value for bit b with probability P = 1/2 for each ciphertext.

Attacker observes m encryption operations and captures power traces T1::m[1::k] containing k samples each.

In addition, the attacker records the ciphertexts C1::m.

No knowledge of the plaintext is required.

DPA Overview

DPA analysis uses power consumption measurements to determine whether a key block guess Ks is correct.

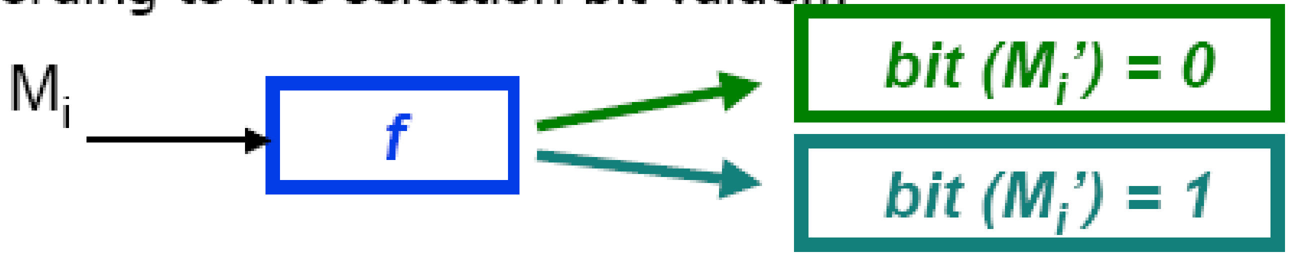
The attacker computes a k-sample differential trace D[1::k] by finding the difference between the average of the traces for which D(C; b; Ks) is one and

the average of the traces for which D(C; b; Ks) is zero.

Thus ∑W[j] is the average over C1::m due to the value represented by the selection function W on the power consumption measurements at point j.

DPA (cont'd)

- Partition the data and related curves into two packs, according to the selection bit value…



- … and assign -1 to pack 0 and +1 to pack 1

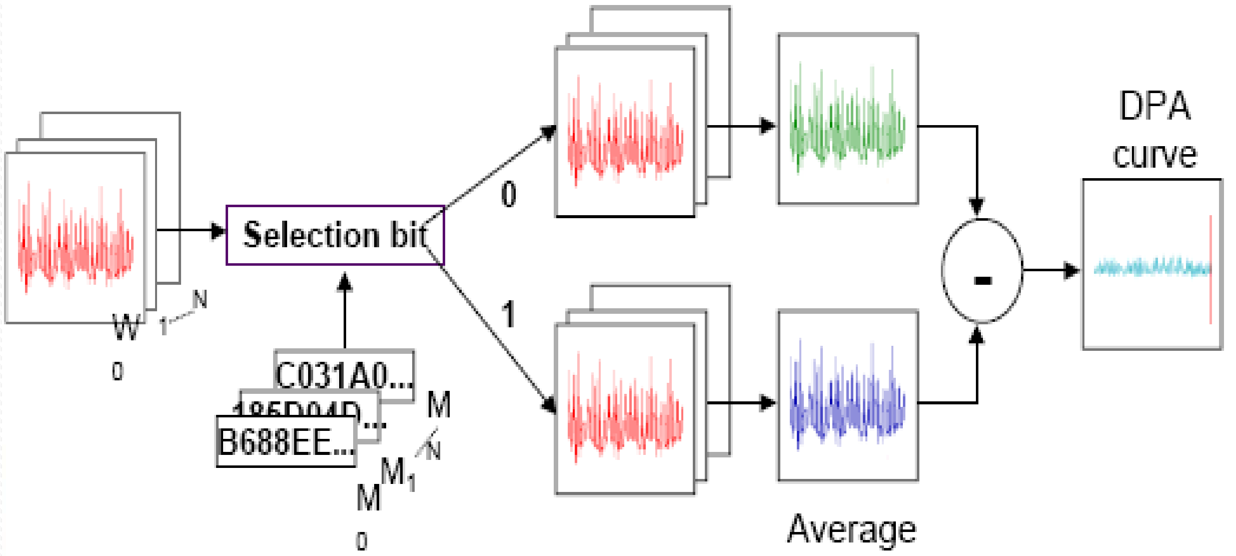
0	B688EE57BB63E03E	1	+1	
1	185D04D77509F36F	0	-1	
2	C031A0392DC881E6	1	+1	…

- Sum the signed consumption curves and normalise
- <=> Difference of averages

$(N_0 + N_1 = N)$

$$\boxed{DPA = \frac{\sum W_1}{N_1} - \frac{\sum W_0}{N_0}}$$

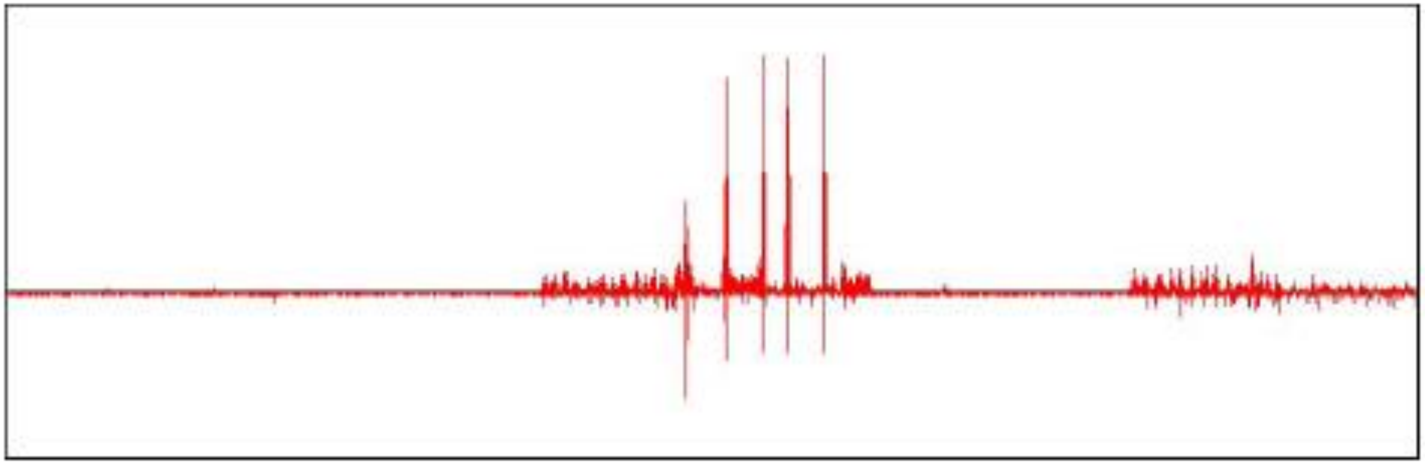
DPA (cont’d)



$$\Delta_n = \frac{\sum_{w_i \in S_0} w_i}{|S_0|} - \frac{\sum_{w_i \in S_1} w_i}{|S_1|}$$

DPA (cont'd)

- The DPA waveform with the highest peak will validate the hypothesis



DPA Procedure for DES

1. Make power consumption measurement of about 1000 DES operations, 100000 data points / curve, (Ciphertext$_i$, Curve$_i$)
2. Assume a key for a S-box of last round
3. Calculate first S-box first bit input 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

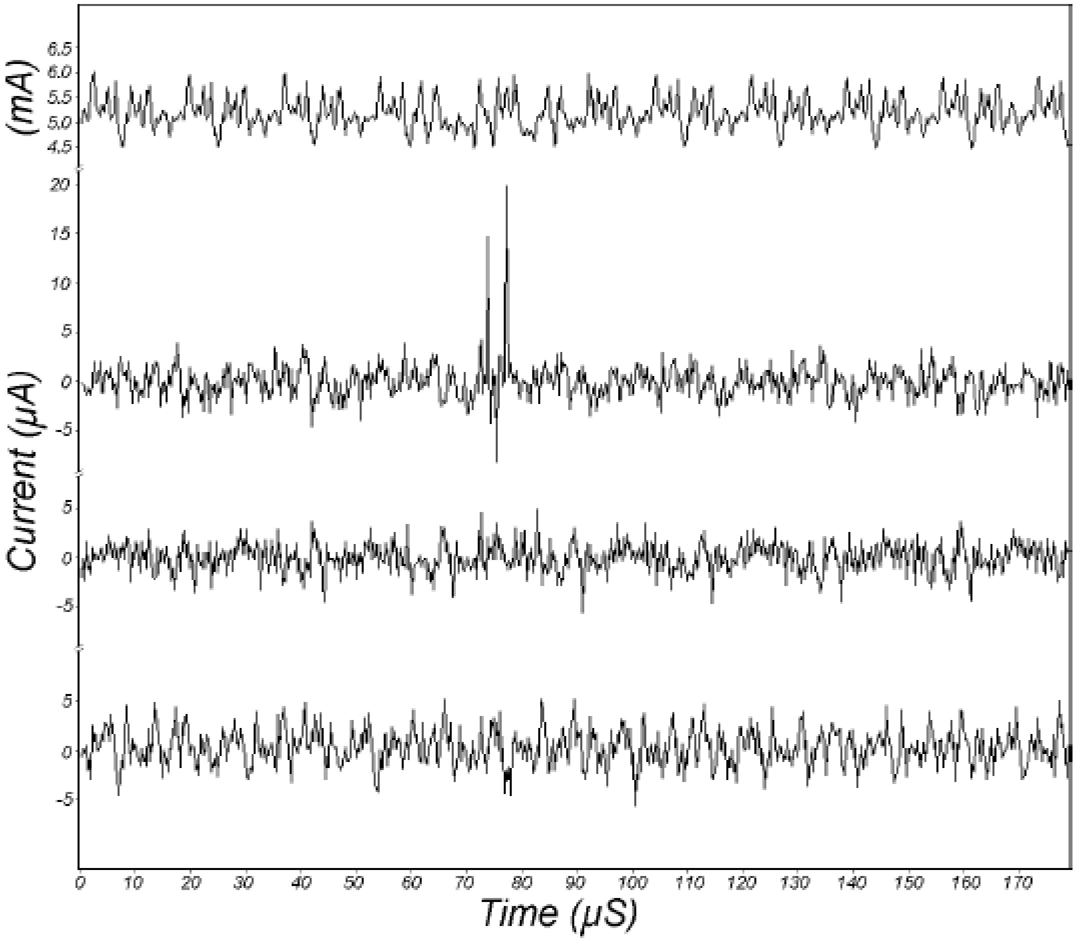
DPA Result Example

Average Power Consumption

Power Consumption Differential Curve With Correct Key Guess

Power Consumption Differential Curve With Incorrect Key Guess

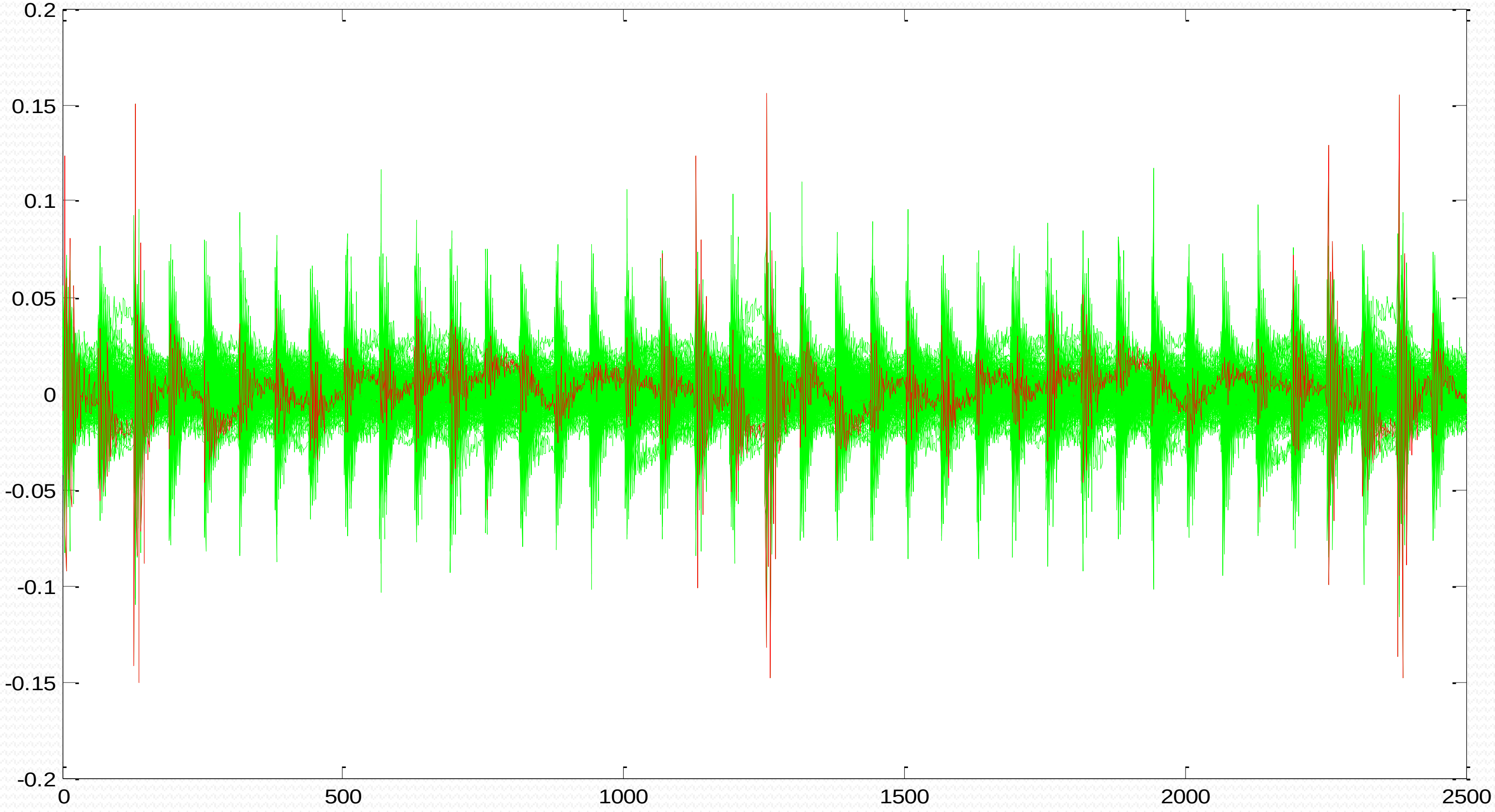
Power Consumption Differential Curve With Incorrect Key Guess



DPA in details

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

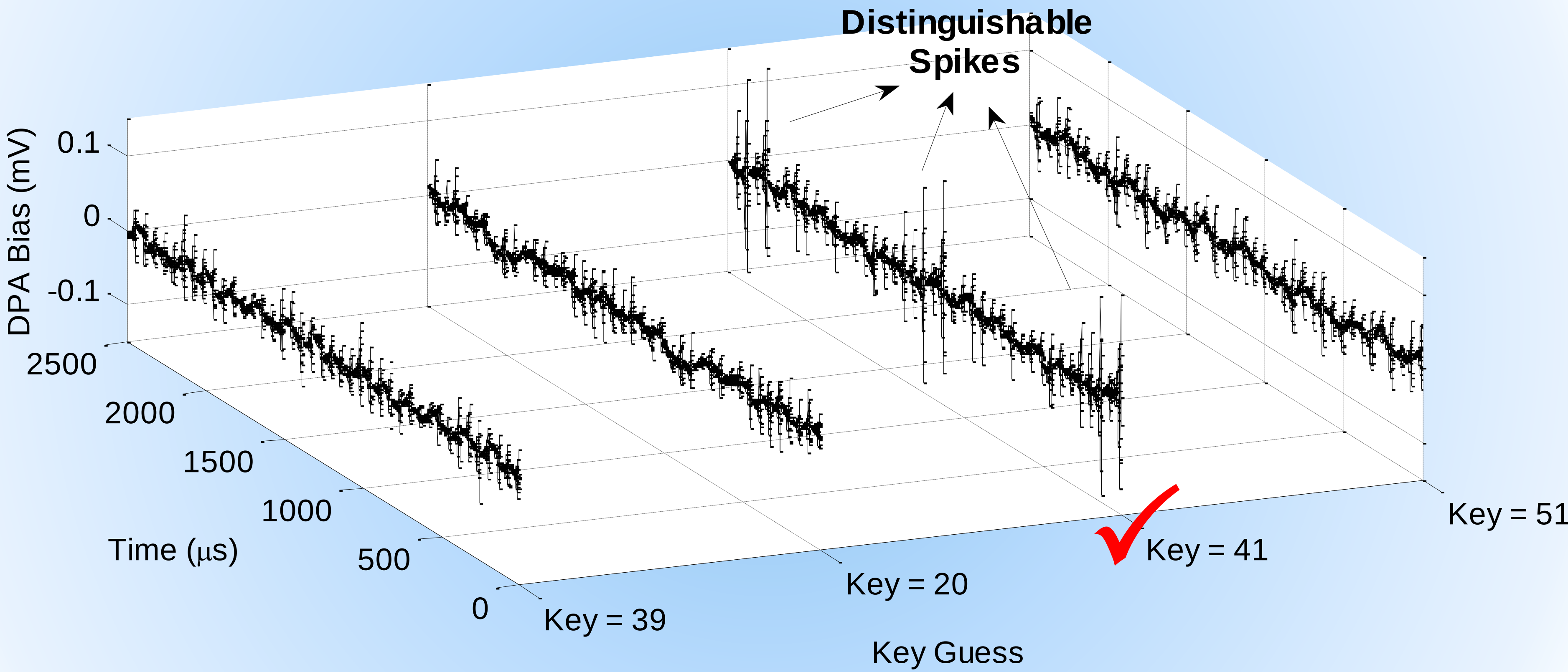
DPA Results - DES



2D Differential Plot

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

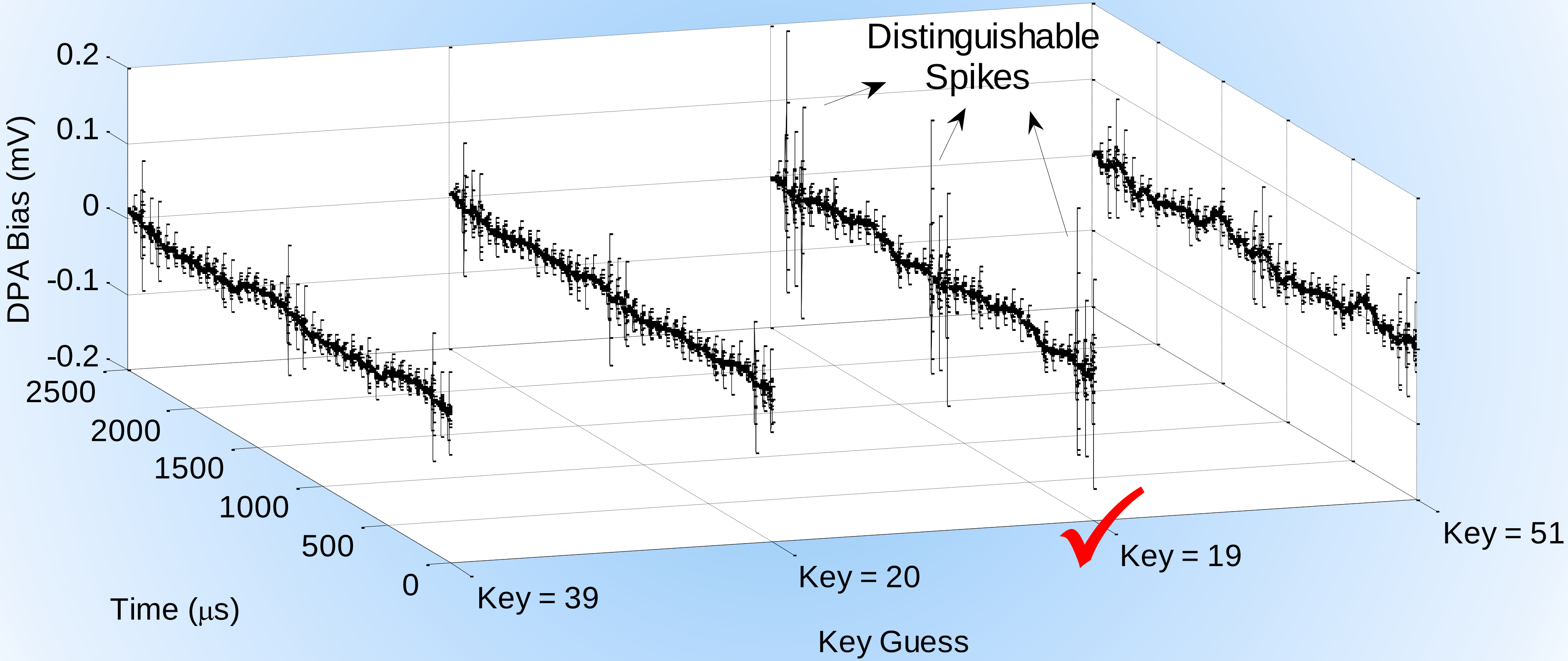
DPA Results - DES



3D Differential Plot

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

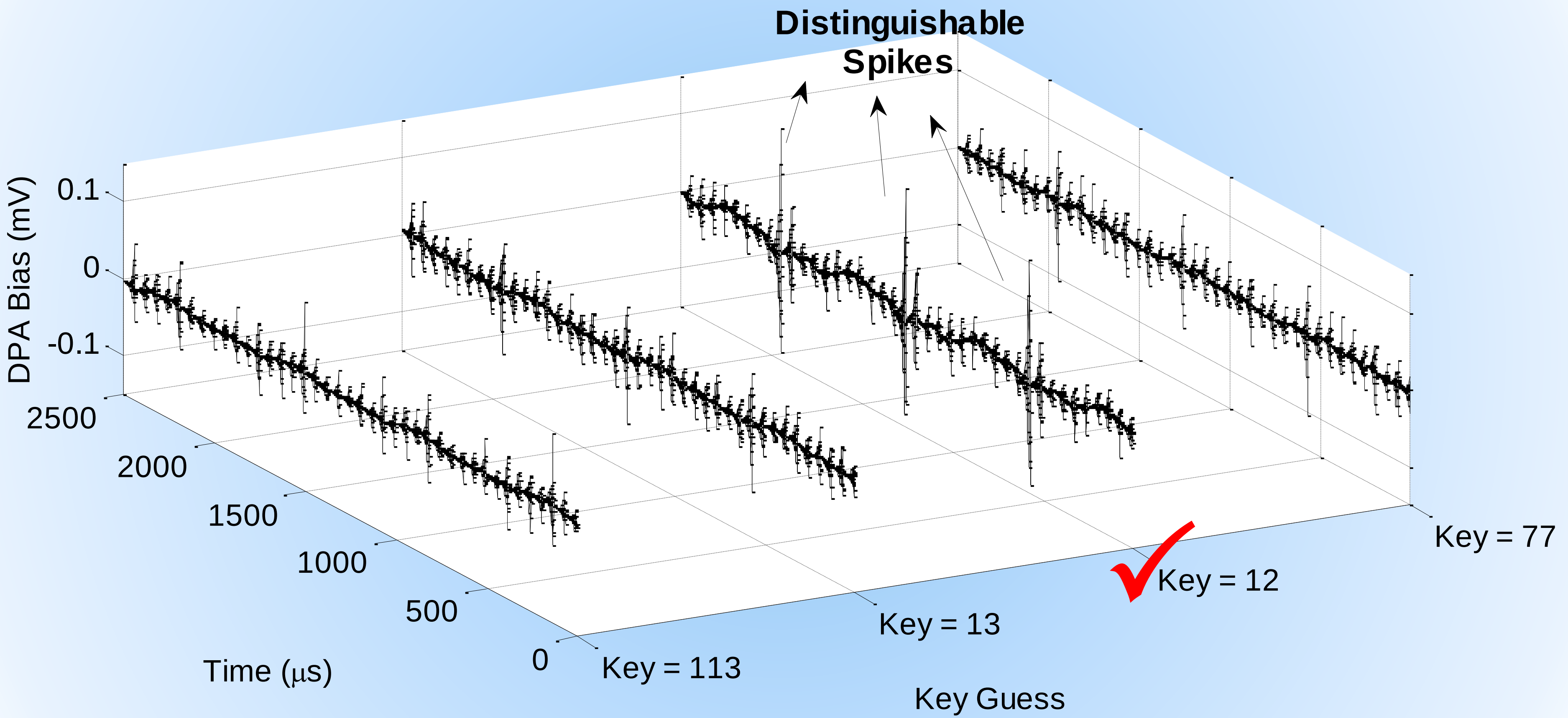
DPA Results - Triple-DES



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**

Probable Key Differential Power Analysis (PKDPA)

- Dhiman saha, D. Mukhopadhyay, D. Roy chowdhury, PKDPA: An Enhanced Probabilistic Differential Power Attack Methodologies, INDOCRYPT 2011
- Basic idea :
  - Don't look for the key with highest DPA Bias
  - Instead look at a fixed set of keys with high DPA biases
  - Do this for all target bits
  - Then perform a frequency analysis to get the correct key

DPA Vs PKDPA

- Perform Difference of Means(DoM) test
- Find key with highest DoM
- Repeat for all target bits
- If results of all bits be same, then conclude that to be the correct key
- Else repeat with higher # of power traces

- Perform Difference of Means(DoM) test
- Find n keys with high DoMs
- Repeat for all target bits
- Perform frequency analysis
- Key with $f \geq$ ½ (# of target bits) = correct key
- Else repeat with higher # of power traces

The Probable Key Matrix

Target Bit

B1	B2	B3	B4	B5	B6	B7	B8
180	30	101	41	93	197	26	182

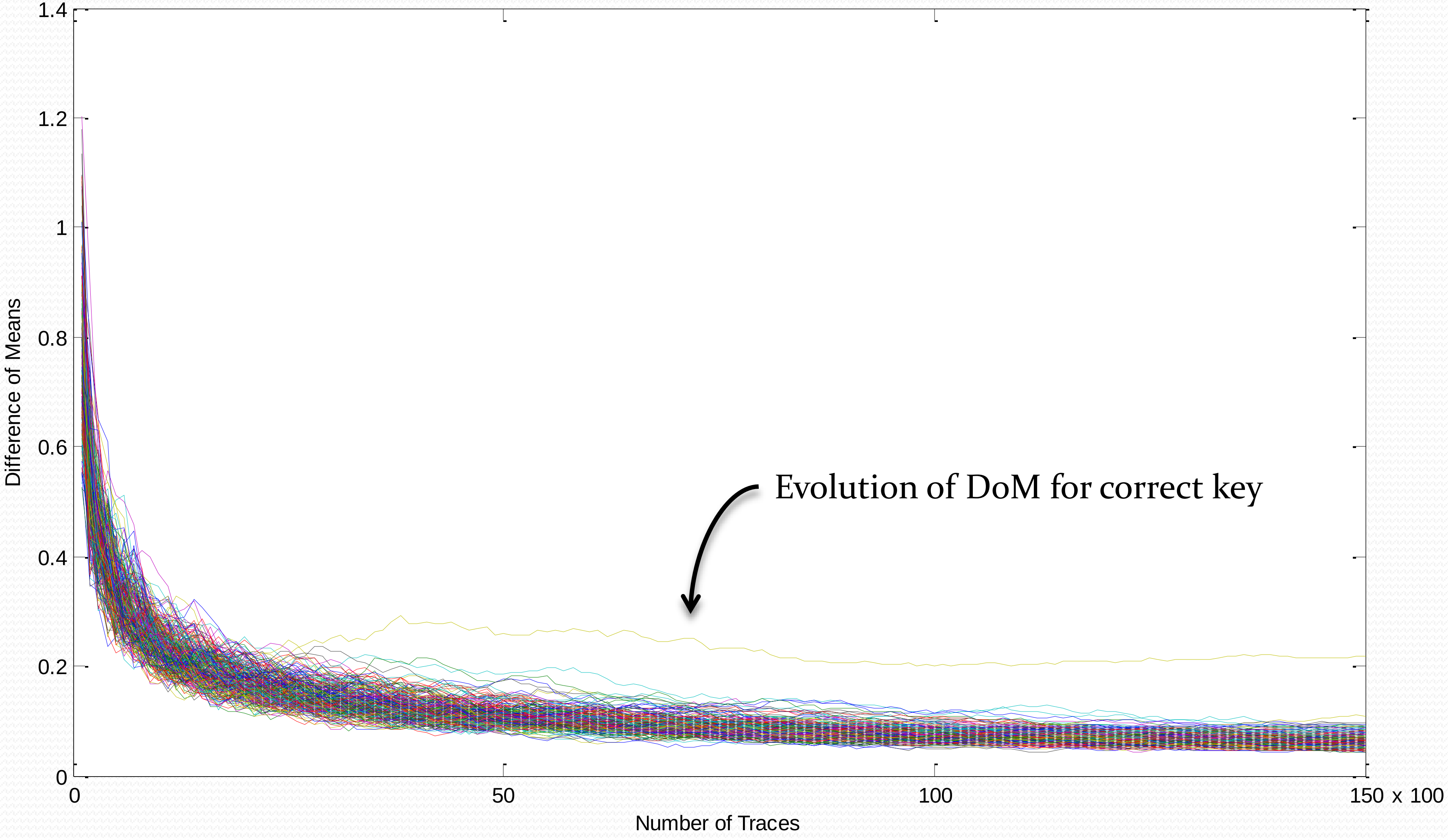
First row represents keys with highest DoM values i.e., DPA keys

Each column represents a probable key set for the related target bit

Keys arranged in descending order of DoM for every target bit

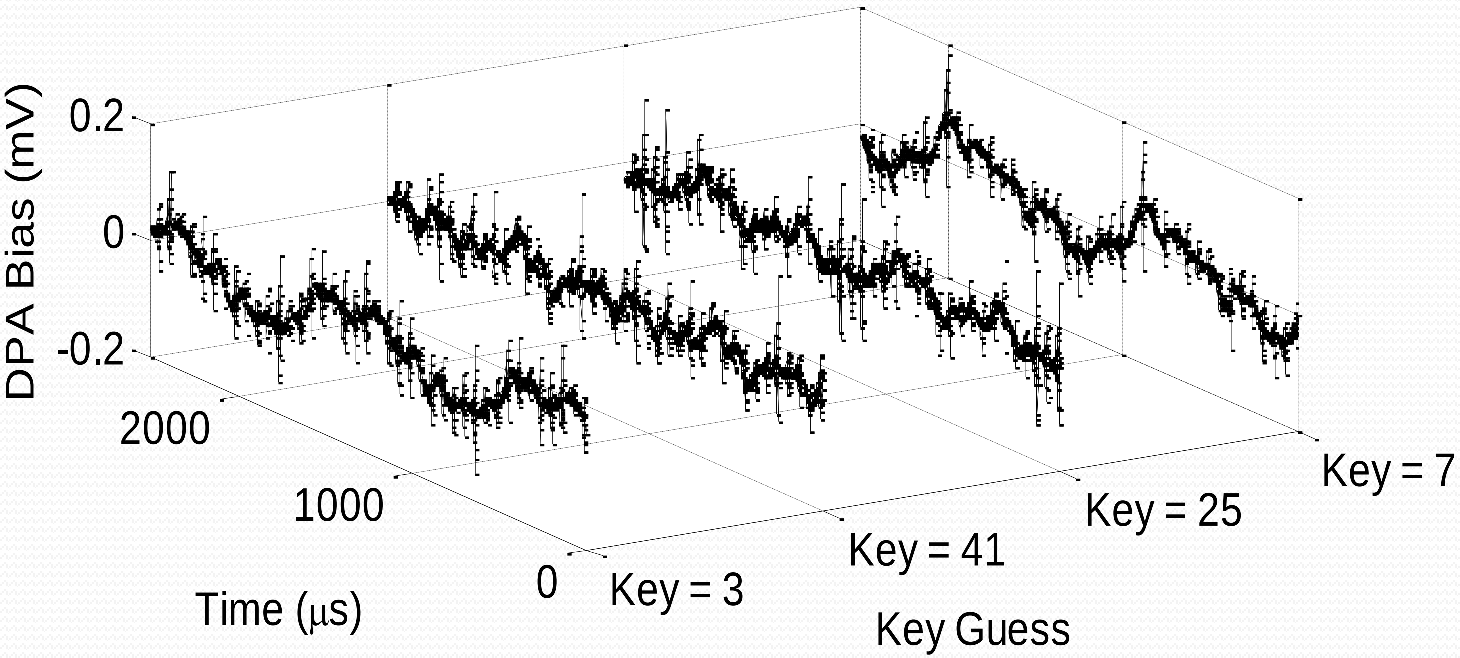
Probable Key Matrix for AES
Sbox – 13, Traces 2,500, Window-Size = 10

Probable Key Progression



Evolution of DoM for correct key

PKDPA Results - DES



Bit	Key Returned
1	37
2	22
3	34
4	7

DPA Keys

3D Differential Plot

SBOX – 7 **BIT – 4** **TRACE COUNT = 900**

?

Correct Key = 25

Cannot be Distinguished

Classical DPA fails for 900 Traces

PKDPA Results - DES

SBOX – 7

TRACE COUNT = 900

Window-Size = 5

Most Frequent Key = 25

Frequency = 3

B1	B2	B3	B4
37	22	34	7
12	40	31	41
25	42	25	3
46	10	60	9
61	20	44	25

Probable Key Matrix

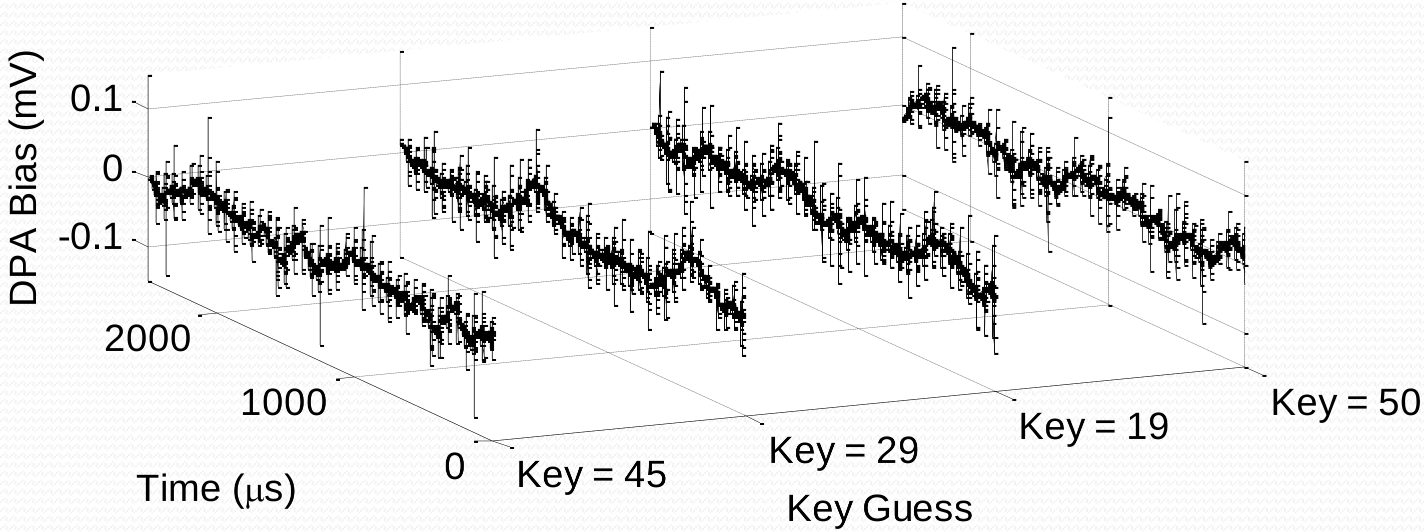
✓

Correct Key = 25

By PKDPA Principle

PKDPA succeeds for 900 Traces

PKDPA Results - TripleDES



Bit	Key Returned
1	6
2	19
3	45
4	30

DPA Keys

3D Differential Plot

SBOX – 4 **BIT – 3** **TRACE COUNT = 3,200**

?

Correct Key = 19

Cannot be Distinguished

Classical DPA fails for 3,200 Traces

PKDPA Results - TripleDES

SBOX – 4

TRACE COUNT = 3,200

Window-Size = 5

Most Frequent Key = 19

Frequency = 3

B1	B2	B3	B4
6	19	45	30
32	24	22	45
5	20	29	19
38	7	38	25
19	54	50	3

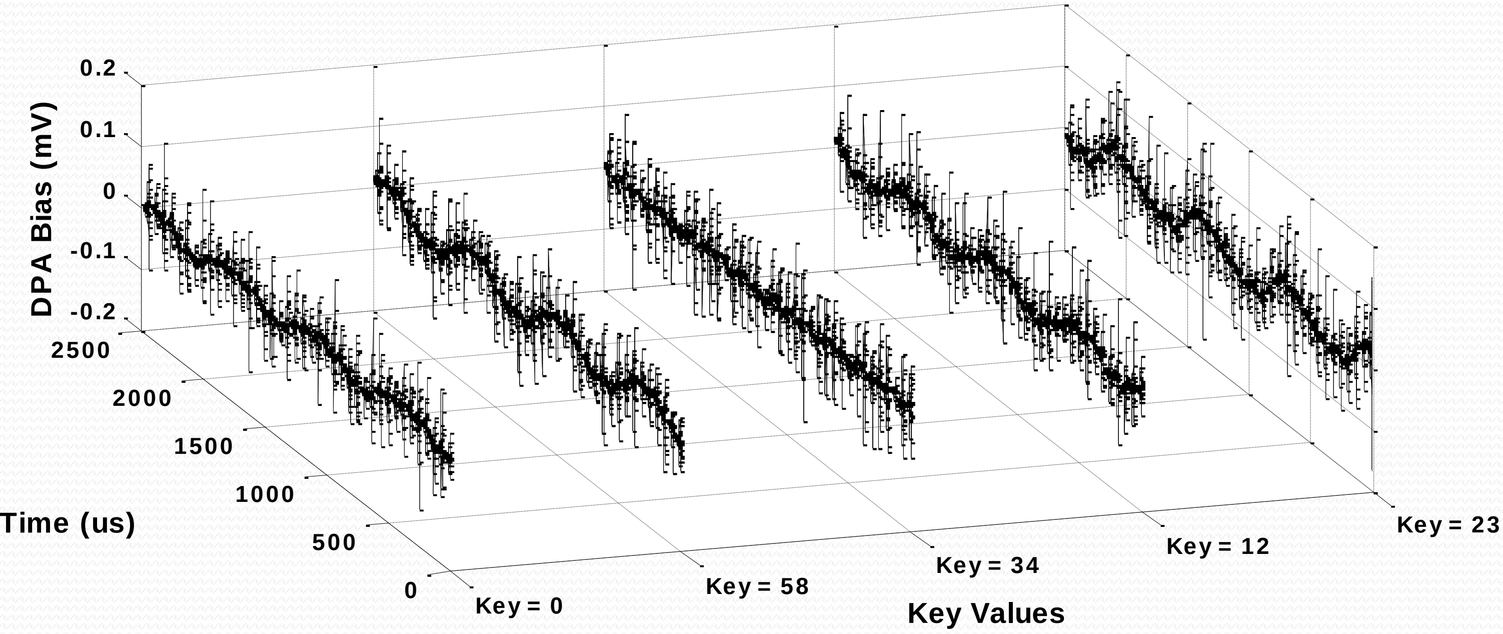
Probable Key Matrix

Correct Key = 19

By PKDPA Principle

PKDPA succeeds for 3,200 Traces

PKDPA Results - AES



3D Differential Plot

SBOX – 15 BIT – 4 TRACE COUNT = 2,500

Bit	Key Returned
1	11
2	12
3	244
4	124
5	86
6	244
7	242
8	147

DPA Keys

?

Correct Key = 12

Cannot be Distinguished

Classical DPA fails for 2,500 Traces

PKDPA Results - AES

SBOX – 15

TRACE COUNT = 2,500

Window-Size = 10

Most Frequent Key = 12

Frequency = 4

B1	B2	B3	B4	B5	B6	B7	B8
11	12	244	124	86	244	242	147
23	86	76	95	64	38	143	107
61	227	58	244	69	67	128	42
133	19	217	12	210	17	44	88
197	161	164	142	127	124	174	137
35	38	69	139	60	103	41	12
22	191	52	117	218	61	36	122
220	164	123	74	193	196	68	125
238	105	12	73	18	82	133	159
178	26	193	147	89	78	202	96

Probable Key Matrix

PKDPA succeeds for 2,500 Traces

✓ Correct Key = 12
By PKDPA Principle

Masked AES

- Most popular counter-measure against DPA attacks is masking

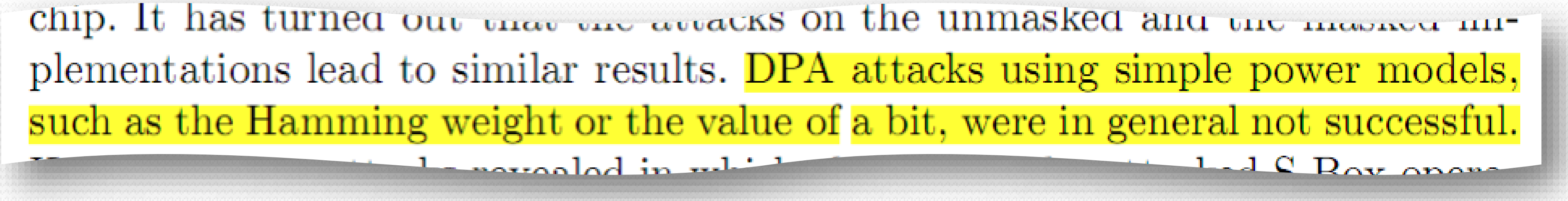
- Using PKDPA attacked AES implementation protected by masking technique by Oswald *et al.* [18]

- The bit model of power analysis was used to attack masked Sbox during the encryption of 13, 000 random plaintexts.

- A randomly generated mask was used for each of these encryptions

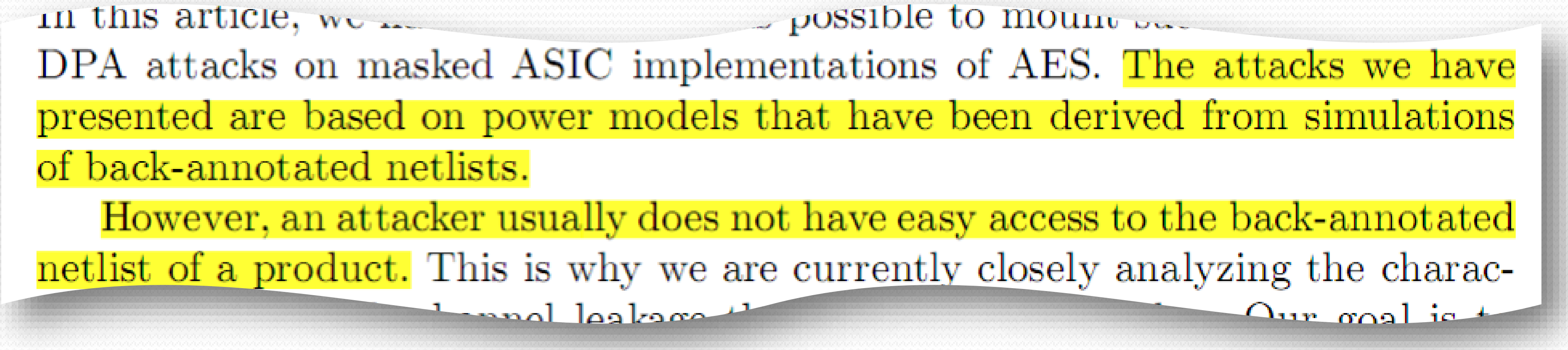
A Related Result

- Mangard *et al.* attacked the same masked AES implemented on an ASIC in [19]



chip. It has turned out that the attacks on the unmasked and the masked implementations lead to similar results. DPA attacks using simple power models, such as the Hamming weight or the value of a bit, were in general not successful.

- Power models based on simulation required 30,000 traces to attack the masked design



In this article, we ... possible to mount suc... DPA attacks on masked ASIC implementations of AES. The attacks we have presented are based on power models that have been derived from simulations of back-annotated netlists.

However, an attacker usually does not have easy access to the back-annotated netlist of a product. This is why we are currently closely analyzing the charac-

PKDPA Results – Masked AES

SBOX – 15

TRACE COUNT = 13,000

Window-Size = 15

Most Frequent Key = 12

Frequency = 6

RECALL

PKDPA is based on "bit" model

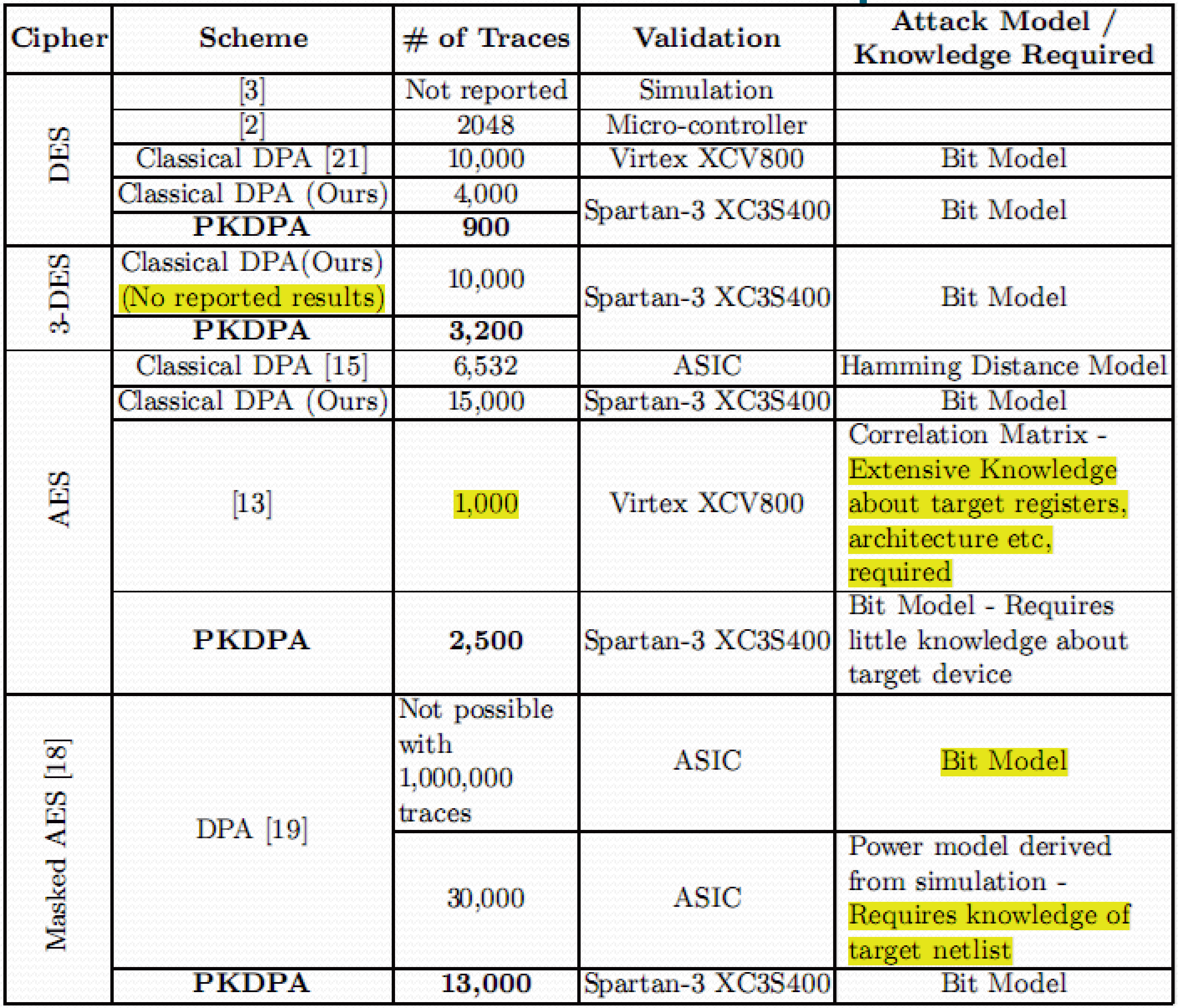
B1	B2	B3	B4	B5	B6	B7	B8
111	163	196	12	129	42	130	125
12	215	239	147	12	76	16	0
216	54	62	169	113	218	139	143
94	22	249	200	13	37	98	126
139	181	86	87	244	58	10	2
172	50	113	67	30	22	176	225
160	226	169	97	218	97	116	73
57	194	240	250	183	117	146	178
11	137	76	81	145	230	244	200
110	42	137	201	35	173	158	90
44	162	102	180	182	138	44	83
233	72	176	0	216	227	245	22
237	12	55	142	67	56	12	145
208	253	12	94	93	155	236	13
103	73	19	84	203	191	147	111

Probable Key Matrix

Correct Key = 12
By PKDPA Principle

PKDPA succeeds for 13,000 Traces

A Comparative Study



Cipher	Scheme	# of Traces	Validation	Attack Model / Knowledge Required
DES	[3]	Not reported	Simulation	
	[2]	2048	Micro-controller	
	Classical DPA [21]	10,000	Virtex XCV800	Bit Model
	Classical DPA (Ours)	4,000	Spartan-3 XC3S400	Bit Model
	PKDPA	**900**		
3-DES	Classical DPA(Ours) (No reported results)	10,000	Spartan-3 XC3S400	Bit Model
	PKDPA	**3,200**		
AES	Classical DPA [15]	6,532	ASIC	Hamming Distance Model
	Classical DPA (Ours)	15,000	Spartan-3 XC3S400	Bit Model
	[13]	1,000	Virtex XCV800	Correlation Matrix - Extensive Knowledge about target registers, architecture etc, required
	PKDPA	**2,500**	Spartan-3 XC3S400	Bit Model - Requires little knowledge about target device
Masked AES [18]	DPA [19]	Not possible with 1,000,000 traces	ASIC	Bit Model
		30,000	ASIC	Power model derived from simulation - Requires knowledge of target netlist
	PKDPA	**13,000**	Spartan-3 XC3S400	Bit Model

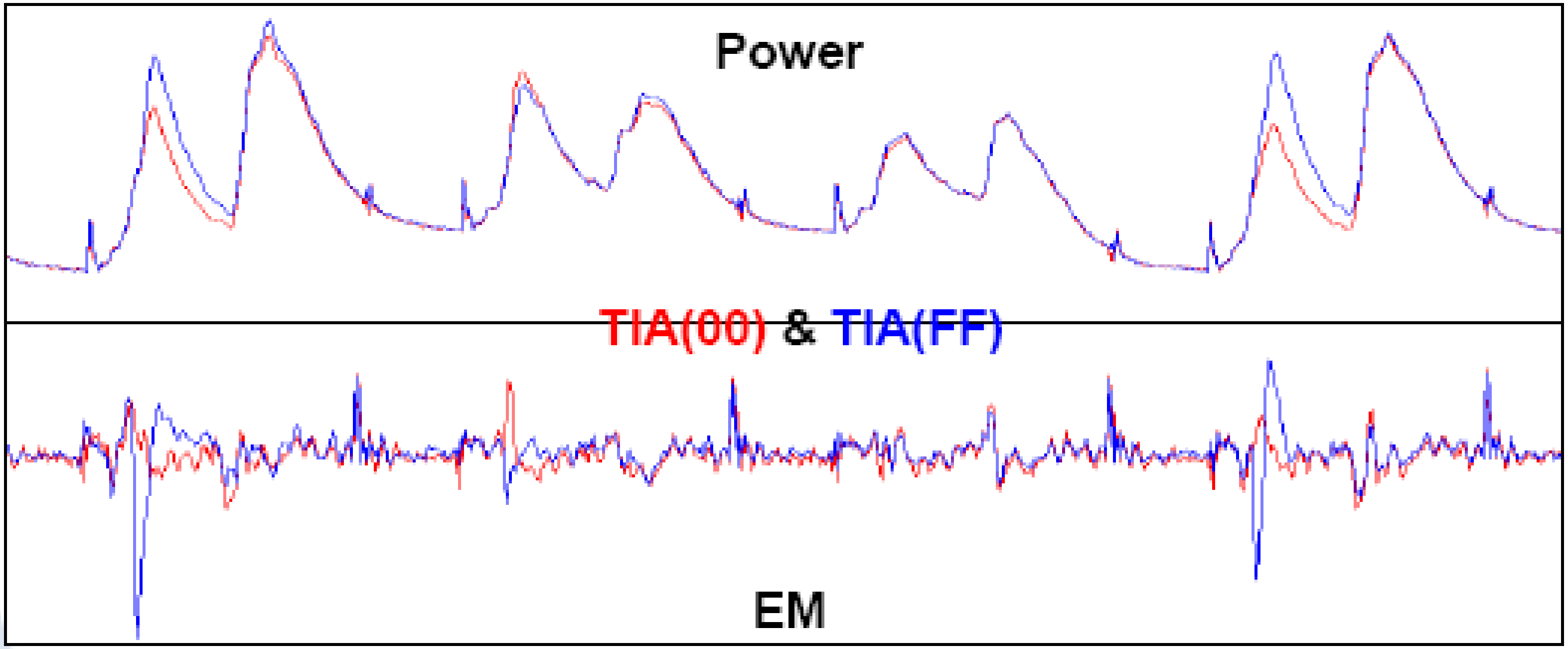
Outline

- Introduction
- Type of Side Channel Attacks
- Power attacks
- **Electromagnetic Radiation attacks**
- Fault attacks

Electromagnetic power analysis

EMA signal

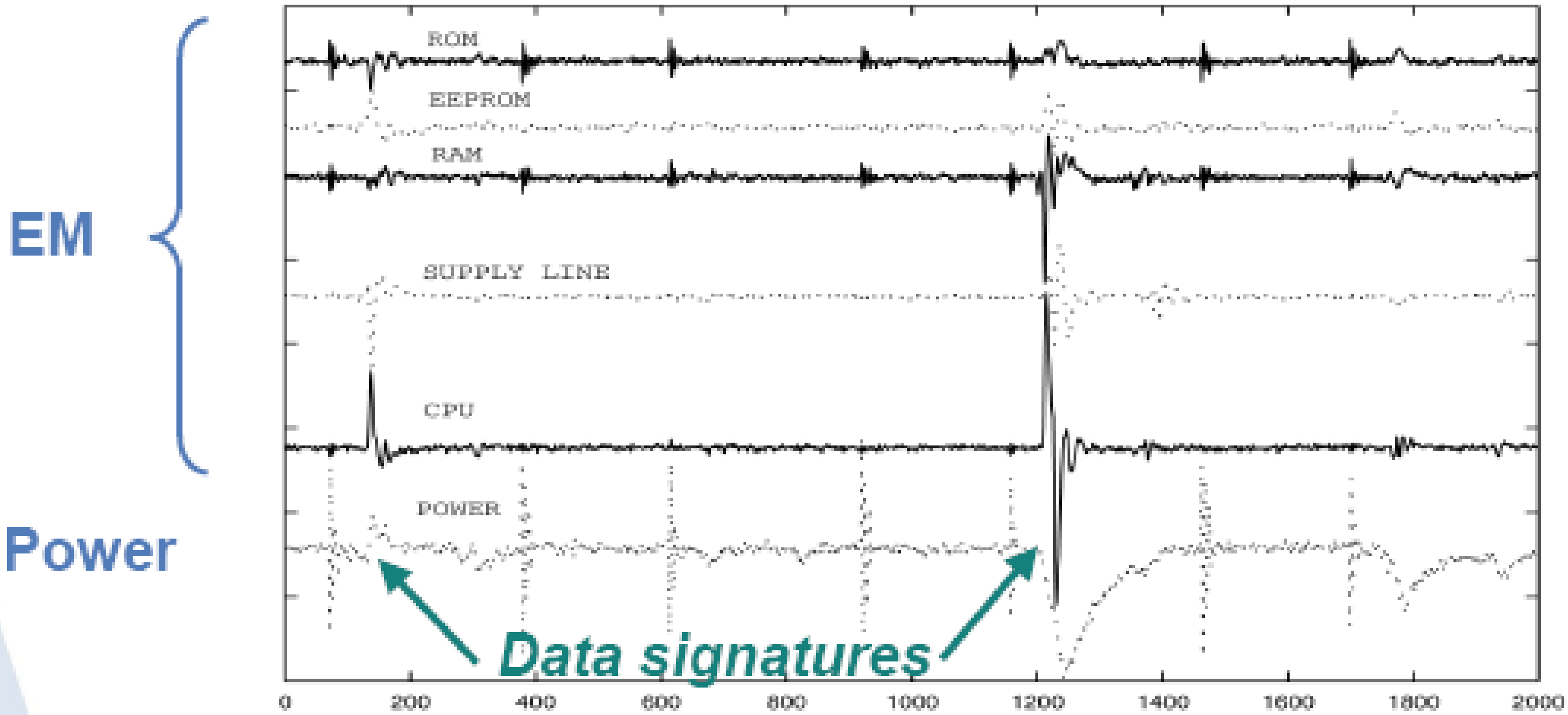
- Raw signals (TIA : transfer into accumulator instruction)
  - Power is less noisy
  - But EM signatures are sharper !



Spatial positioning

- EM signals versus XY probe position

Differential traces between (00h ⊕ 00h) and (FFh ⊕ 00h) picked up at different locations

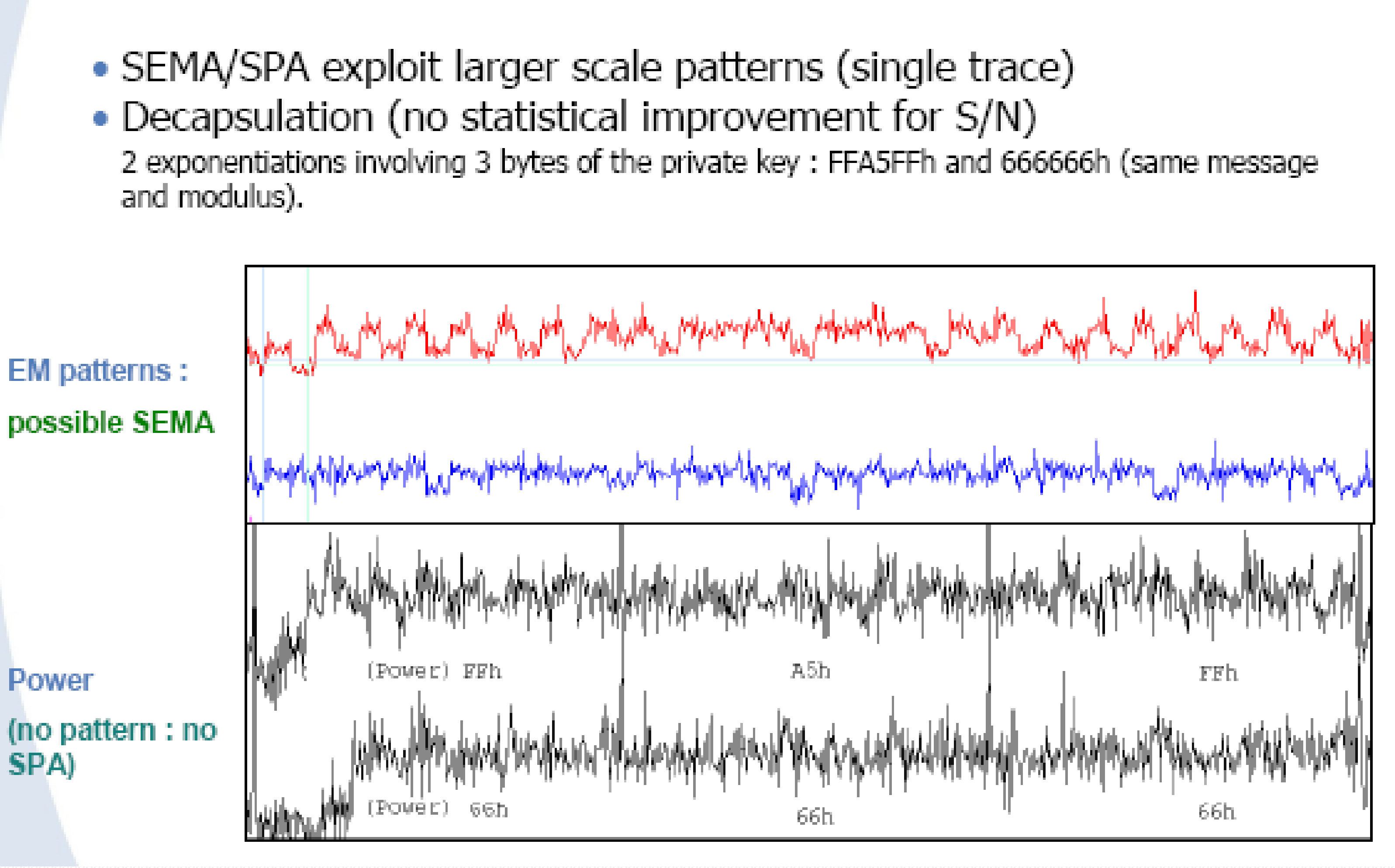


EM

Power

Data signatures

Example: SEMA on RSA



- SEMA/SPA exploit larger scale patterns (single trace)
- Decapsulation (no statistical improvement for S/N)

2 exponentiations involving 3 bytes of the private key : FFA5FFh and 666666h (same message and modulus).

EM patterns :

possible SEMA

Power

(no pattern : no SPA)

References

1. Paul C. Kocher et. al., Introduction to Differential Power Analysis, Journal of Cryptographic Engineering, 2011.

2.Dhiman Saha, Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury, **PKDPA: An Enhanced Probabilistic Differential Power Attack Methodology.** INDOCRYPT 2011, pp 3-21, India