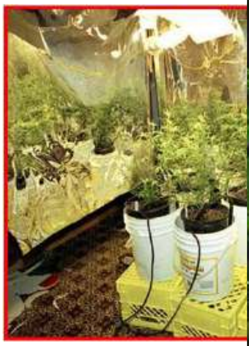
Revealing Secret Information via Emanated Side-Channel Information

Darshana Jayasinghe
Darshanaj@cse.unsw.edu.au

Sri Parameswaran

What is Side Channel?



- https://www.tele 402633/
Dutch-police-catc nl

Your Data is Protected

- All of us have been using cryptographic algorithms to protect sensitive data – knowingly or not

- We use different cryptographic methods to protect secret information
  - Most of the secret information is in 1's and 0's
  - Digital information can be copied and transmitted without loosing the original quality and information

Advanced Encryption Standard - AES

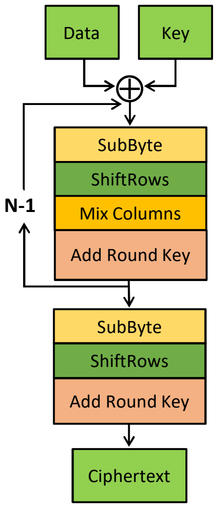
- Block cipher algorithm
- Plaintext (Data): 128 bits
- Key size: 128, 192 or 256 bits
  - Based on the key size, number of rounds will change

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

XOR

1) Initial round
2) (N – 1) rounds
3) Final round

AES - 128	N=10
AES - 192	N=12
AES - 256	N=14

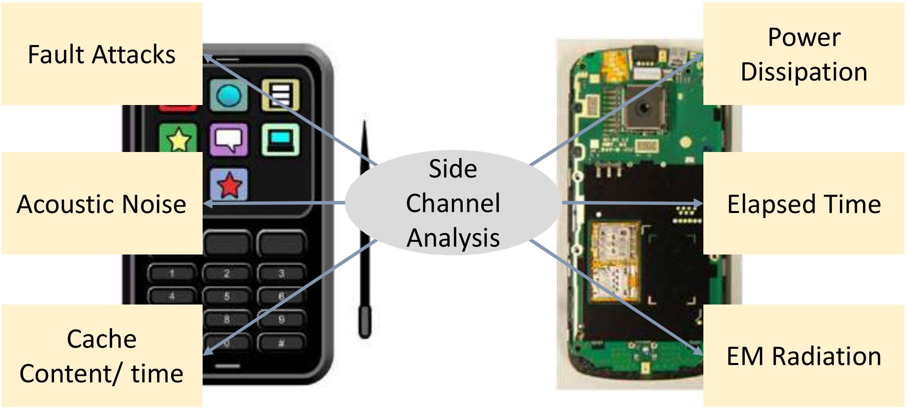


How Secure it is?

- Brute force a 128-bit key ?
- Assume
  - Every person on the planet owns 10 computers
  - Each computer can test 1 billion key combinations per second
  - There are 8 billion people on the planet
  - On average, we can crack the key after testing 50% of the possibilities
  - Then the earth's population can crack one 128-bit encryption key in ~67,000,000,000 years (67 billion years)!!

Age of the Earth: 4.54 ± 0.05 billion years
Age of the Universe: 13.799 ± 0.021 billion years

What are Side-Channel Analysis Attacks



Side Channel Analysis

Fault Attacks

Acoustic Noise

Cache Content/ time

Power Dissipation

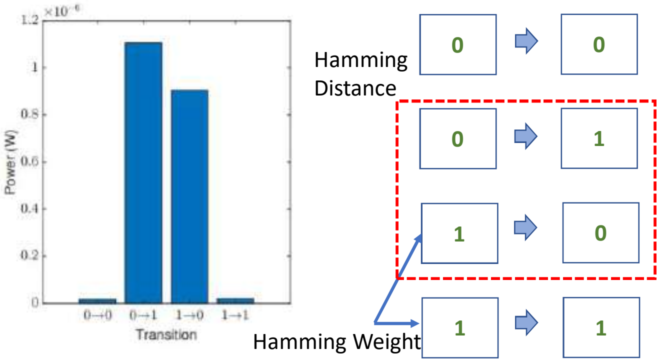
Elapsed Time

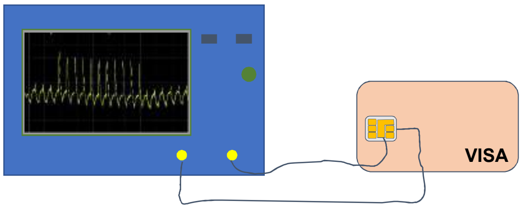
EM Radiation

Power Analysis Attacks

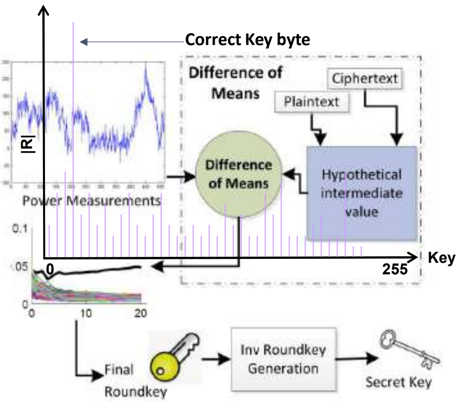
- Revealing the secret information via the power dissipation of the device
- Why?
    - CMOS gates are the most popular building blocks of IC manufacturing
    - Power dissipation of CMOS gates depend on inputs

1-bit Register





Differential Power Analysis Attacks - DPA



$M_0 = 34+32+27 = 93$

$M_1 = 50+36+25+20 = 131$

$R = \left|\frac{93}{3} - \frac{131}{4}\right|$

R = 1.75

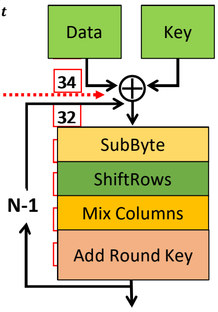
Difference of Means

If $b_0=0$; $M_0 = \sum_{n=1}^{N} P_n$

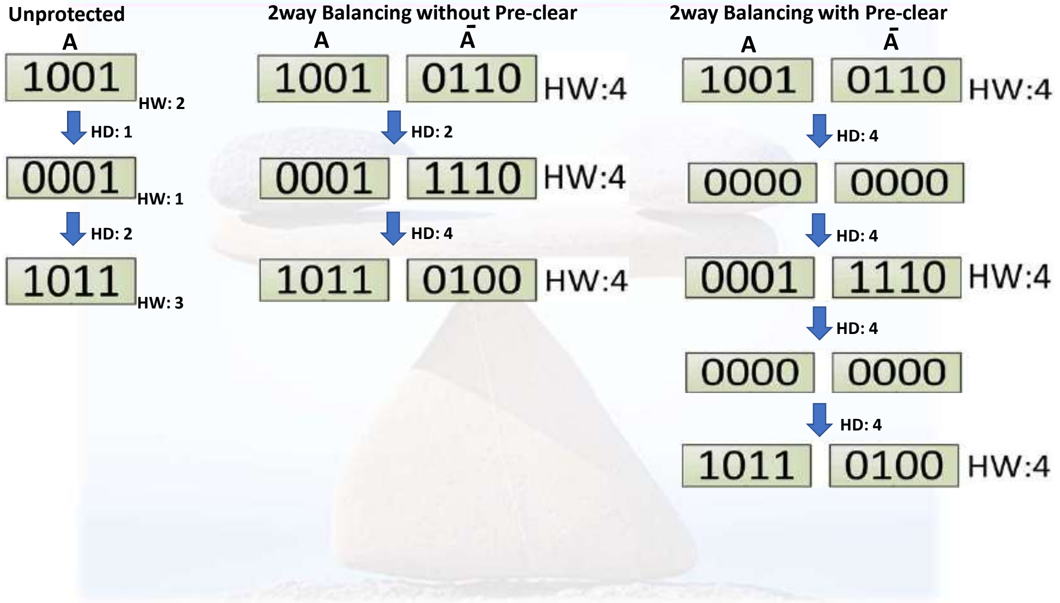
If $b_0=1$; $M_1 = \sum_{t=1}^{T} P_t$

Pt	Key	Pt⊕key	Binary	µW
3F	00	[illegible]	0011111 0	
6E	00	[illegible]	[illegible]0	34
06	00	[illegible]	[illegible]0	32
48	00	48	01001000	
29	00	28	00101000	
B3	00	B2	10110010	
83	00	82	10000010	

Exploit this operation



Balancing Bit Flips



Unprotected

A

1001 HW: 2

HD: 1

0001 HW: 1

HD: 2

1011 HW: 3

2way Balancing without Pre-clear

A $\bar{A}$

1001 0110 HW:4

HD: 2

0001 1110 HW:4

HD: 4

1011 0100 HW:4

2way Balancing with Pre-clear

A $\bar{A}$

1001 0110 HW:4

HD: 4

0000 0000

HD: 4

0001 1110 HW:4

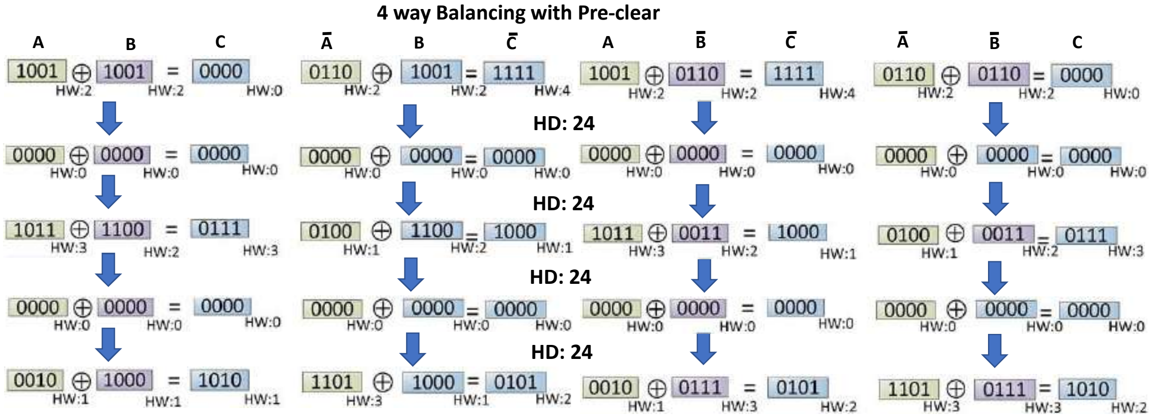
HD: 4

0000 0000

HD: 4

1011 0100 HW:4

Balancing Bit Flips



4 way Balancing with Pre-clear

A B C

1001 ⊕ 1001 = 0000 HW:2 HW:2 HW:0

0000 ⊕ 0000 = 0000 HW:0 HW:0 HW:0

1011 ⊕ 1100 = 0111 HW:3 HW:2 HW:3

0000 ⊕ 0000 = 0000 HW:0 HW:0 HW:0

0010 ⊕ 1000 = 1010 HW:1 HW:1 HW:1

$\bar{A}$ B $\bar{C}$

0110 ⊕ 1001 = 1111 HW:2 HW:2 HW:4

0000 ⊕ 0000 = 0000 HW:0 HW:0 HW:0

0100 ⊕ 1100 = 1000 HW:1 HW:2 HW:1

0000 ⊕ 0000 = 0000 HW:0 HW:0 HW:0

1101 ⊕ 1000 = 0101 HW:3 HW:1 HW:2

HD: 24

HD: 24

HD: 24

HD: 24

A $\bar{B}$ $\bar{C}$

1001 ⊕ 0110 = 1111 HW:2 HW:2 HW:4

0000 ⊕ 0000 = 0000 HW:0 HW:0 HW:0

1011 ⊕ 0011 = 1000 HW:3 HW:2 HW:1

0000 ⊕ 0000 = 0000 HW:0 HW:0 HW:0

0010 ⊕ 0111 = 0101 HW:1 HW:3 HW:2

$\bar{A}$ $\bar{B}$ C

0110 ⊕ 0110 = 0000 HW:2 HW:2 HW:0

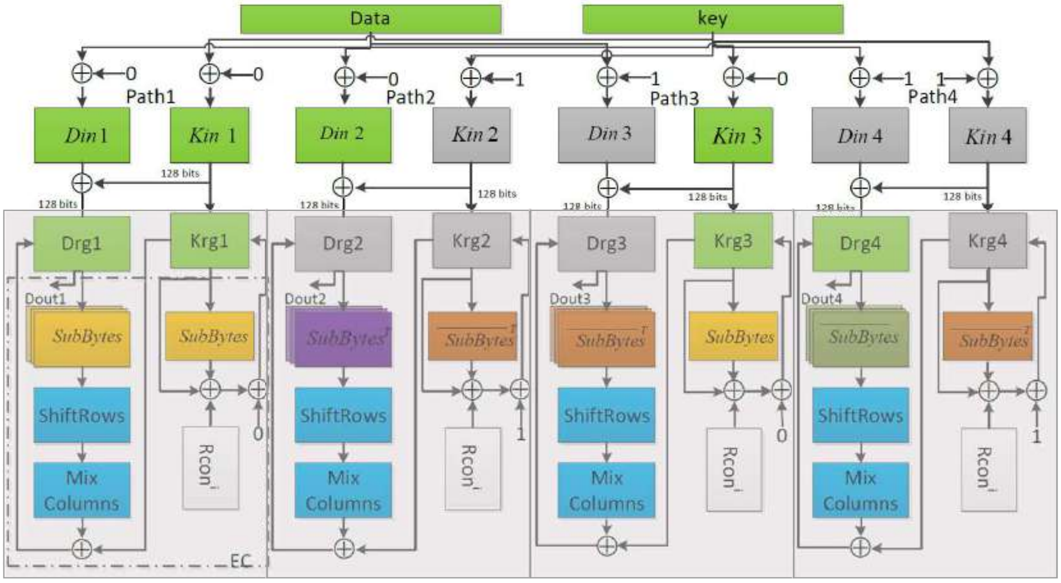
0000 ⊕ 0000 = 0000 HW:0 HW:0 HW:0

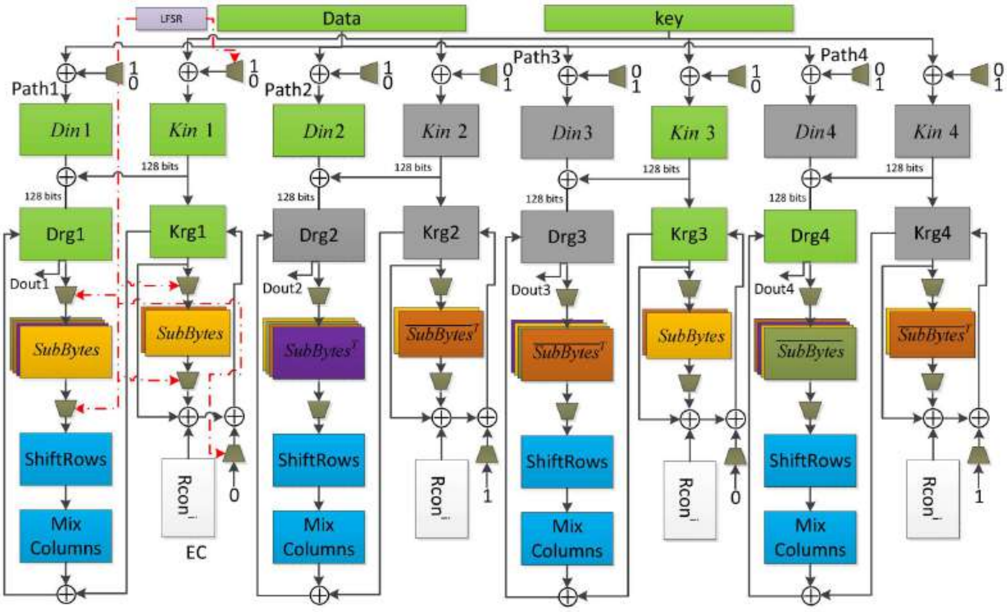
0100 ⊕ 0011 = 0111 HW:1 HW:2 HW:3

0000 ⊕ 0000 = 0000 HW:0 HW:0 HW:0

1101 ⊕ 0111 = 1010 HW:3 HW:3 HW:2

QuadSeal





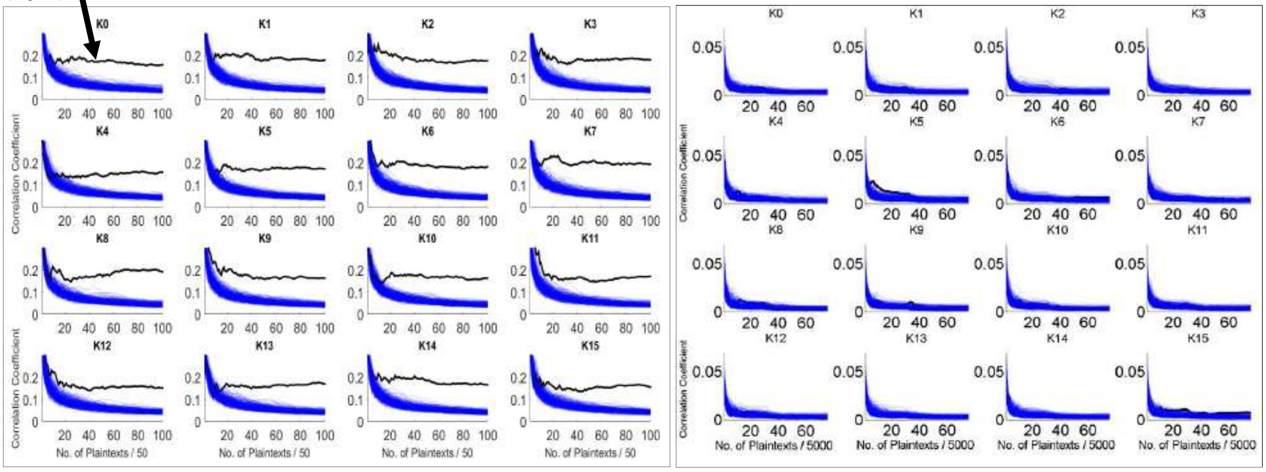
D. Jayasinghe, A. Ignjatovic, J. A. Ambrose, R. Ragel and S. Parameswaran, "QuadSeal: Quadruple algorithmic symmetrizing countermeasure against power based side-channel attacks," *2015 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)*, Amsterdam, 2015, pp. 21-30.

Power Analysis Attack Results

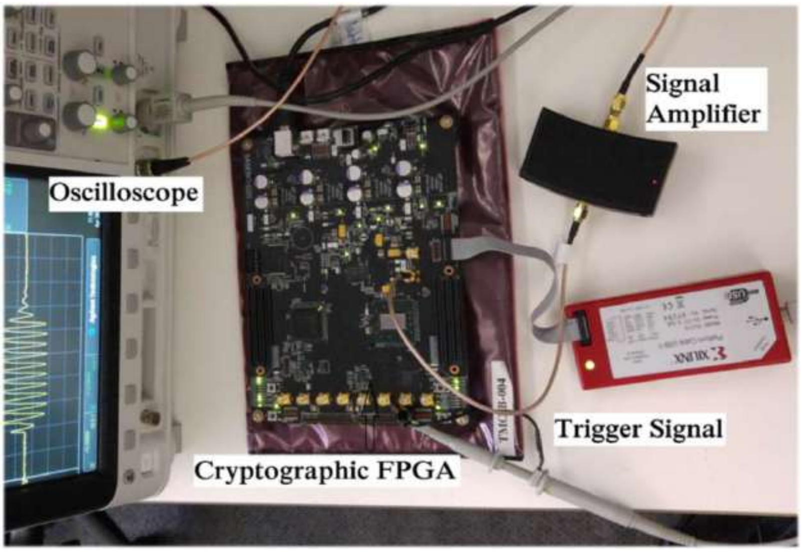
Correct Secret Key (Byte)

Unprotected AES

QuadSeal AES



Experimental Setup



Thank you…

- I explained very little, feel free to ask any question.

Image Courtesy: www.oceanservice.noaa.gov