ASP-DAC 2016

Assessing CPA Resistance of AES with Different Fault Tolerance Mechanisms

Hoda Pahlevanzadeh, Jaya Dofe, and Qiaoyan Yu

University of New Hampshire

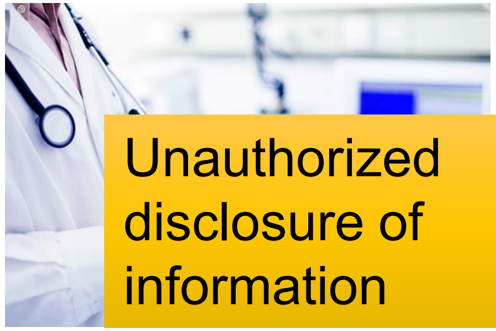
Durham, NH, USA 03824

Email: Qiaoyan.Yu@unh.edu

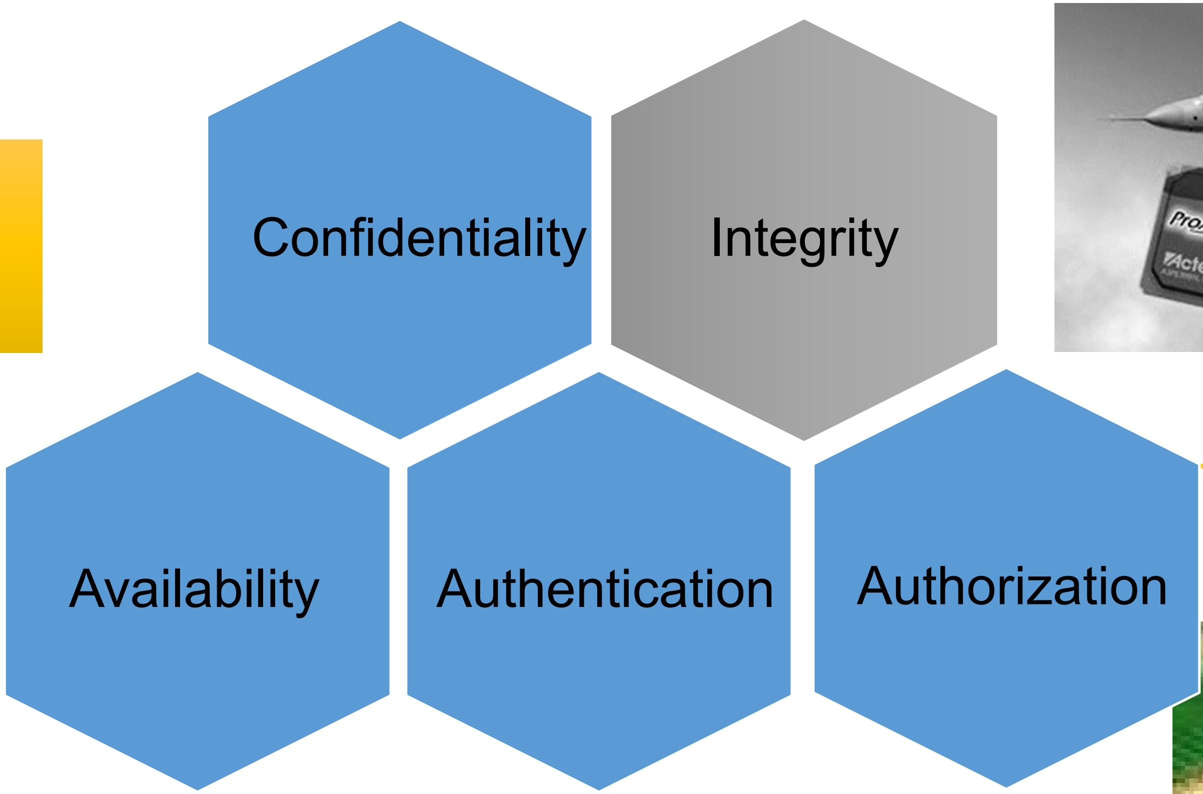
Outline

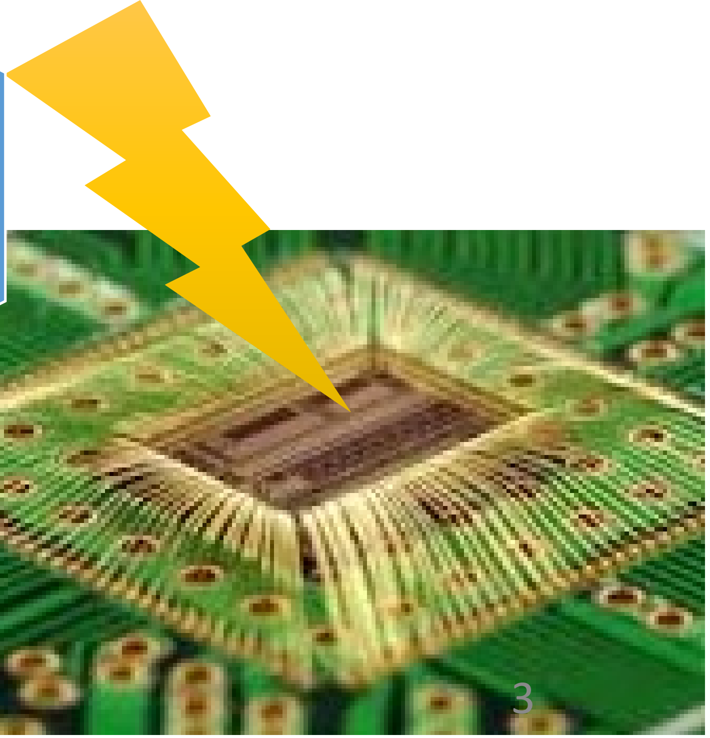
- Security threats on hardware
  - Fault attack
  - Side-channel attack (SCA)
  - Combined attack
- Impact of existing countermeasures for fault attack on cryptosystem against SCA
- Factors affect the efficiency of SCA

Security Challenges in IC



Unauthorized disclosure of information

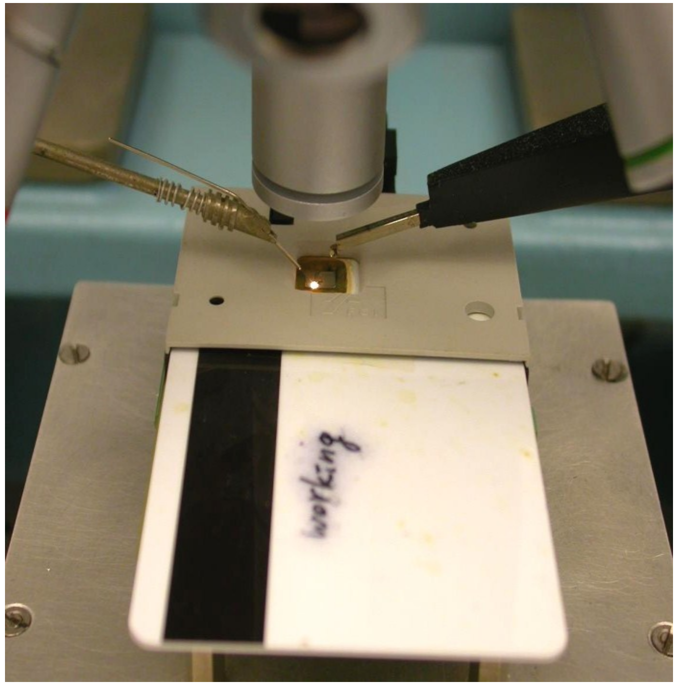




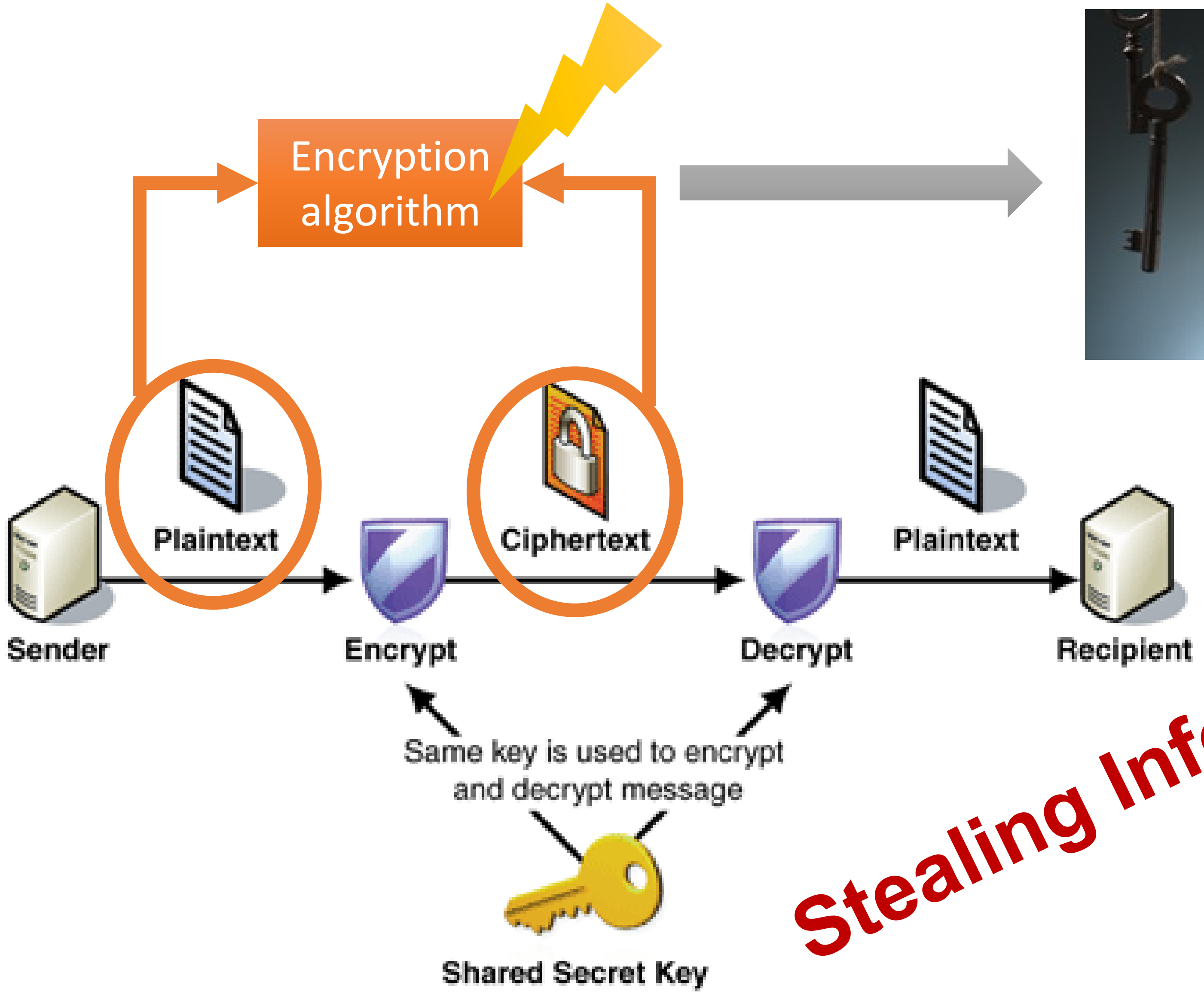
Unauthorized withholding of information

Unauthorized users access

IC Vulnerability to an Attack



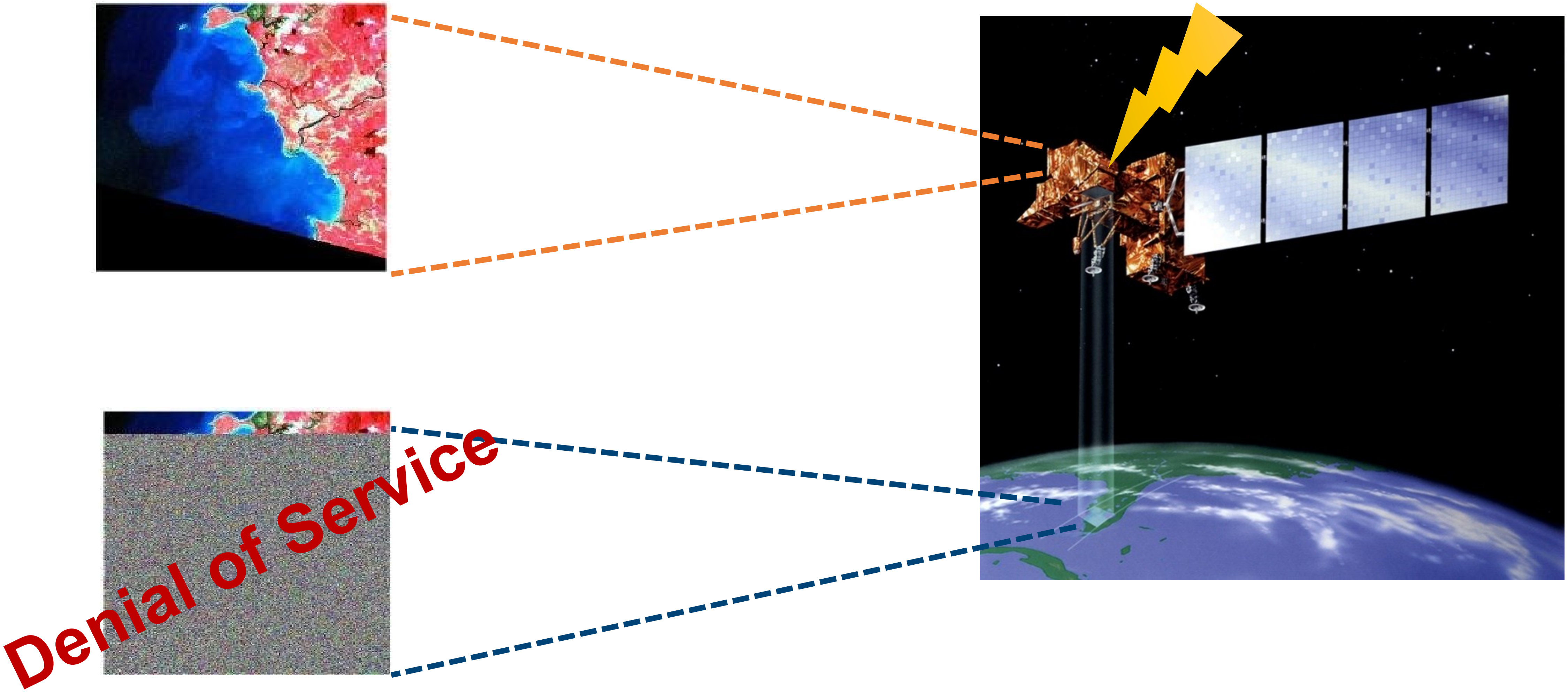
[1]



Stealing Information

[1] S. Skorobogatov, ECRYPT II, 2011.

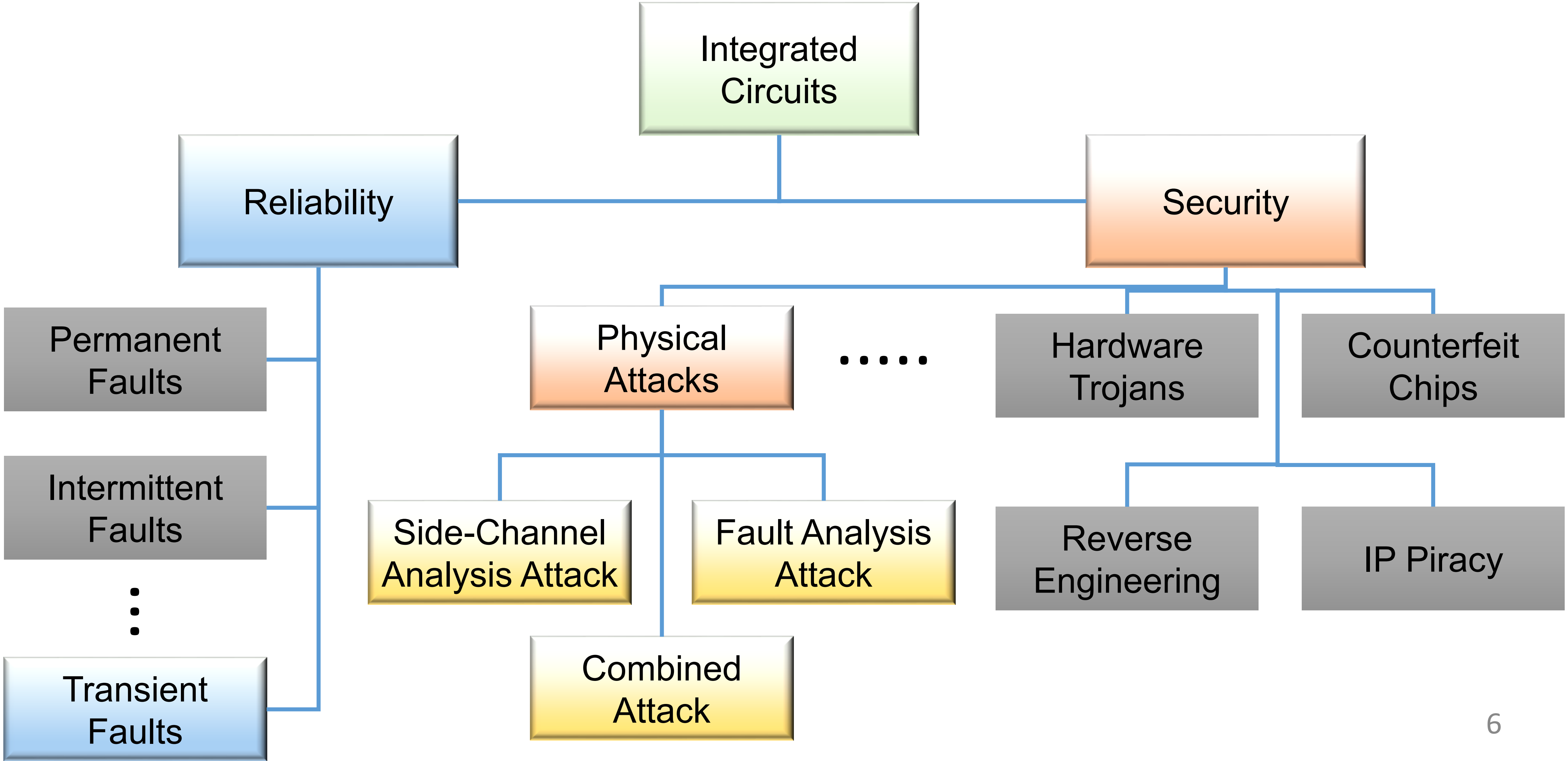
IC Vulnerability to Natural and Intentional Faults



Denial of Service

P. K. Singh, D. Patil, IJIIT, 2013

Unified Framework for Reliability and Security of IC



Integrated Circuits

Reliability

Security

Permanent Faults

Intermittent Faults

⋮

Transient Faults

Physical Attacks

.....

Hardware Trojans

Counterfeit Chips

Side-Channel Analysis Attack

Fault Analysis Attack

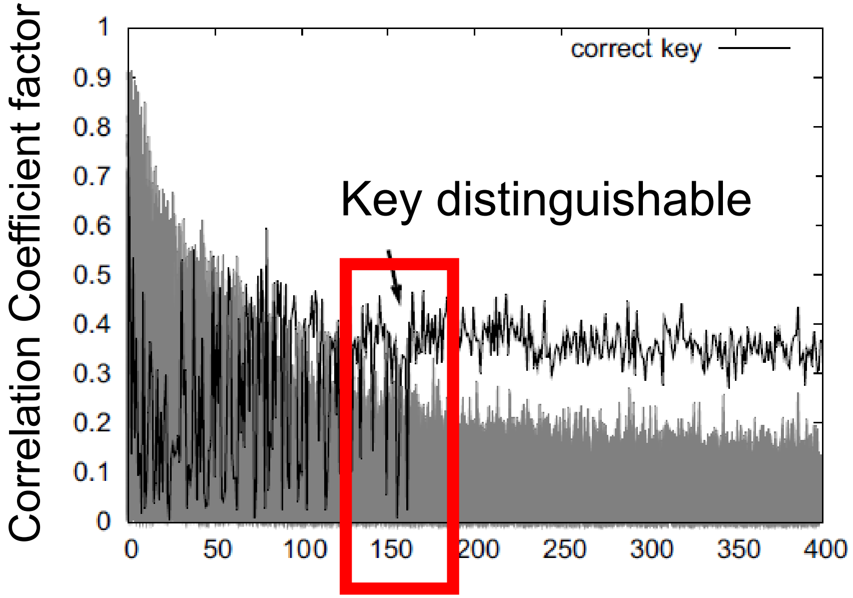
Combined Attack

Reverse Engineering

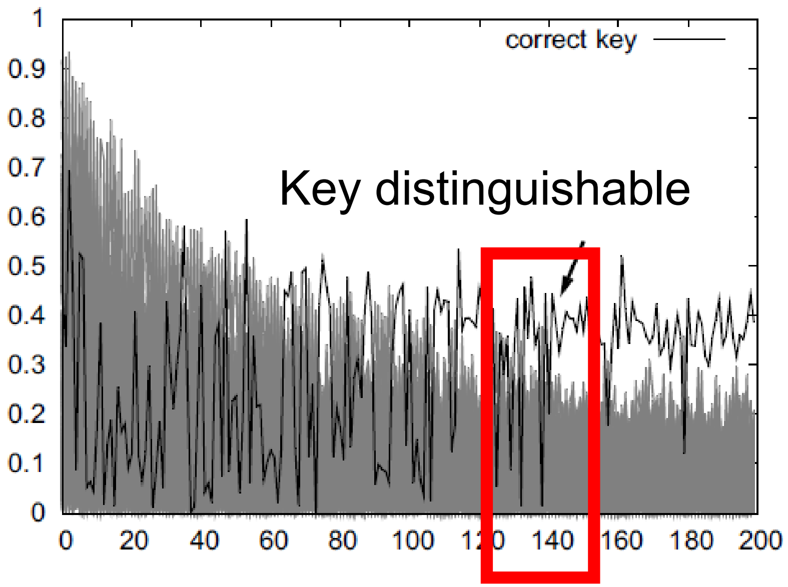
IP Piracy

IC Security Vulnerability to Protection Circuits

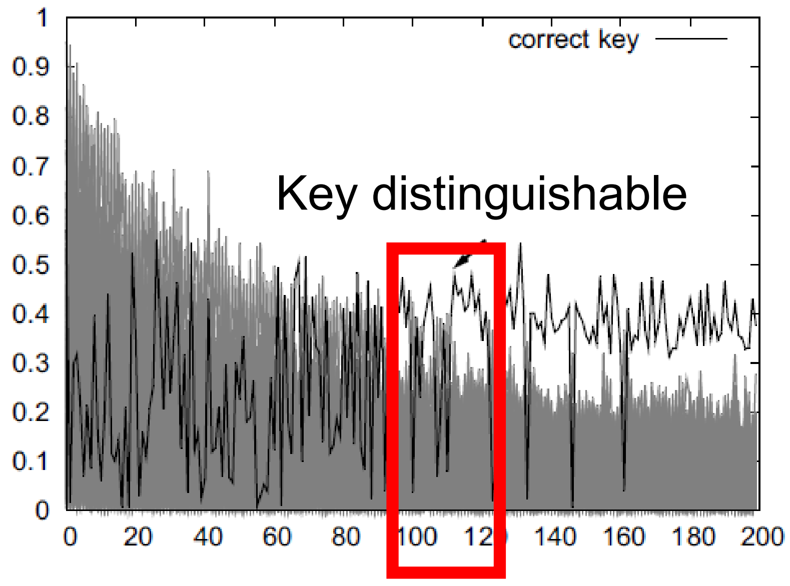
Attack on AES SBox, no fault detection method.

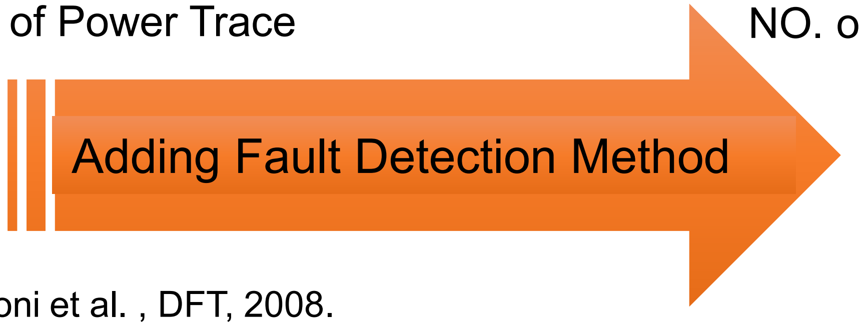


With parity based fault detection method.

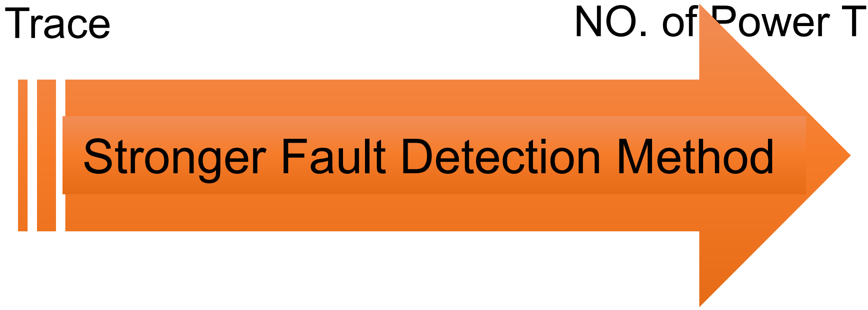


With residue code modulo 3 based fault detection method.





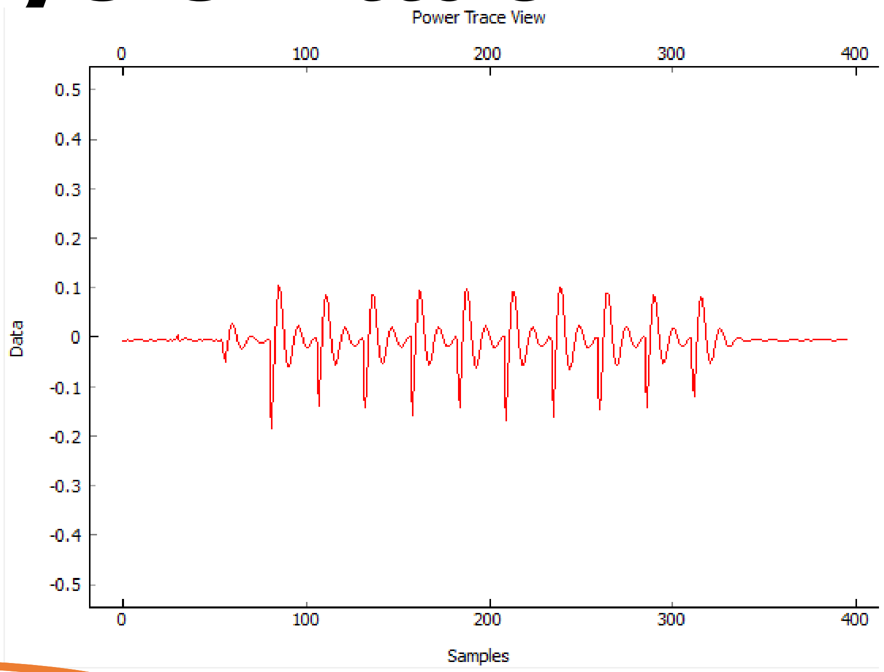
Adding Fault Detection Method

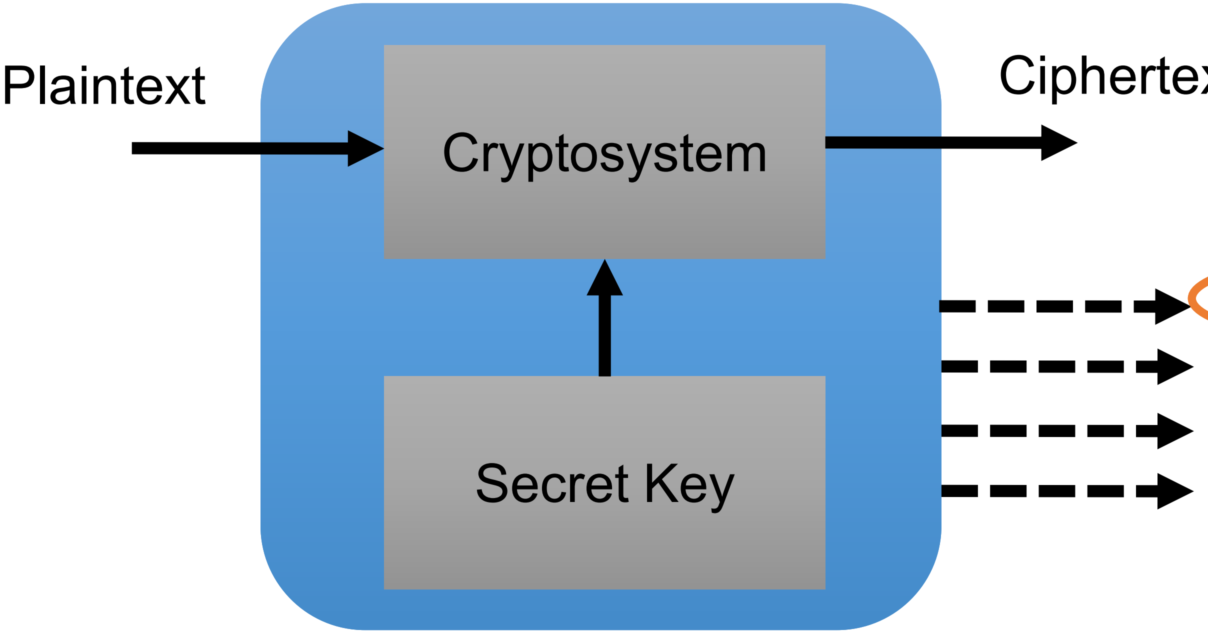


Stronger Fault Detection Method

F. Regazzoni et al. , DFT, 2008.

Side Channel Analysis Attack





Power consumption

Time variation

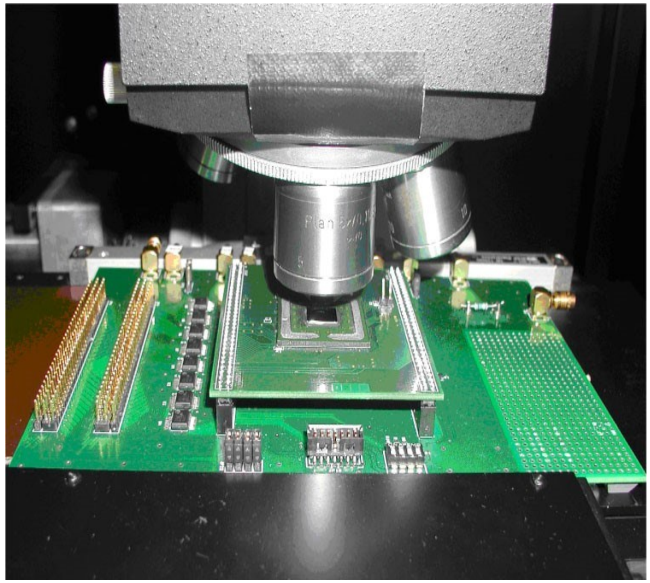
Electromagnetic radiation

Thermal radiation

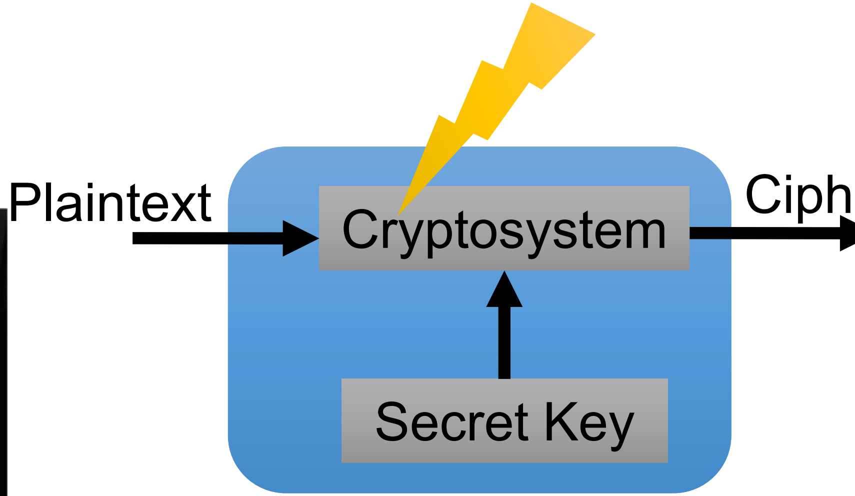
SCA Countermeasures

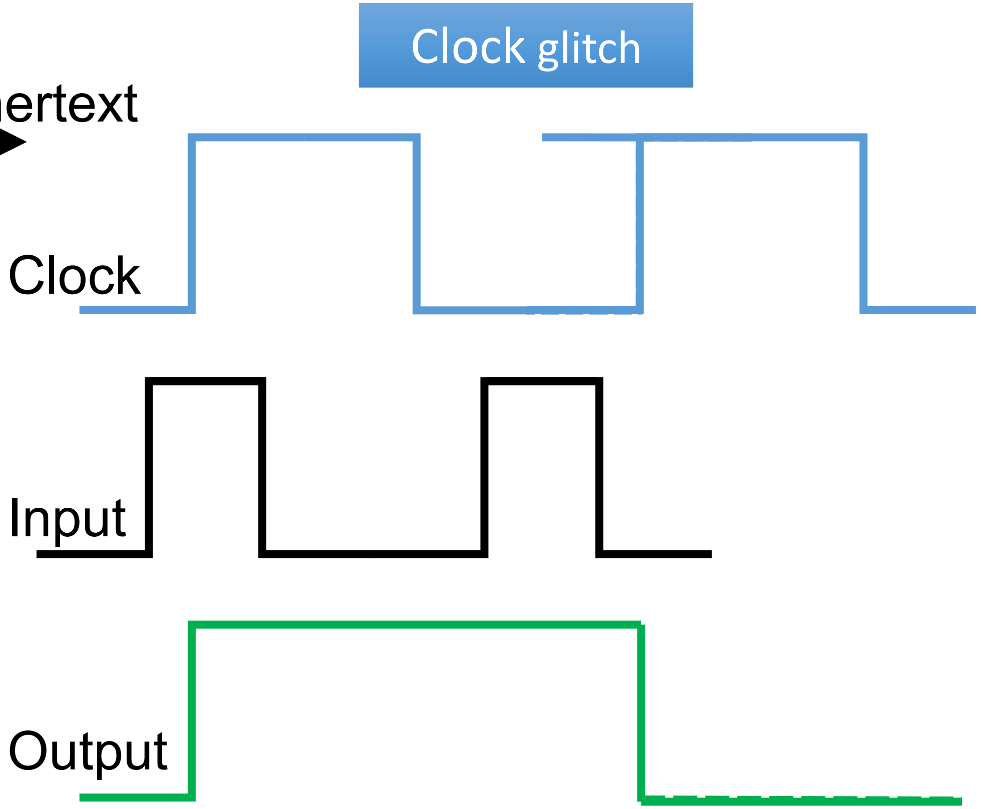
- Randomization (Masking)

Fault Analysis Attack



Laser fault injection equipment



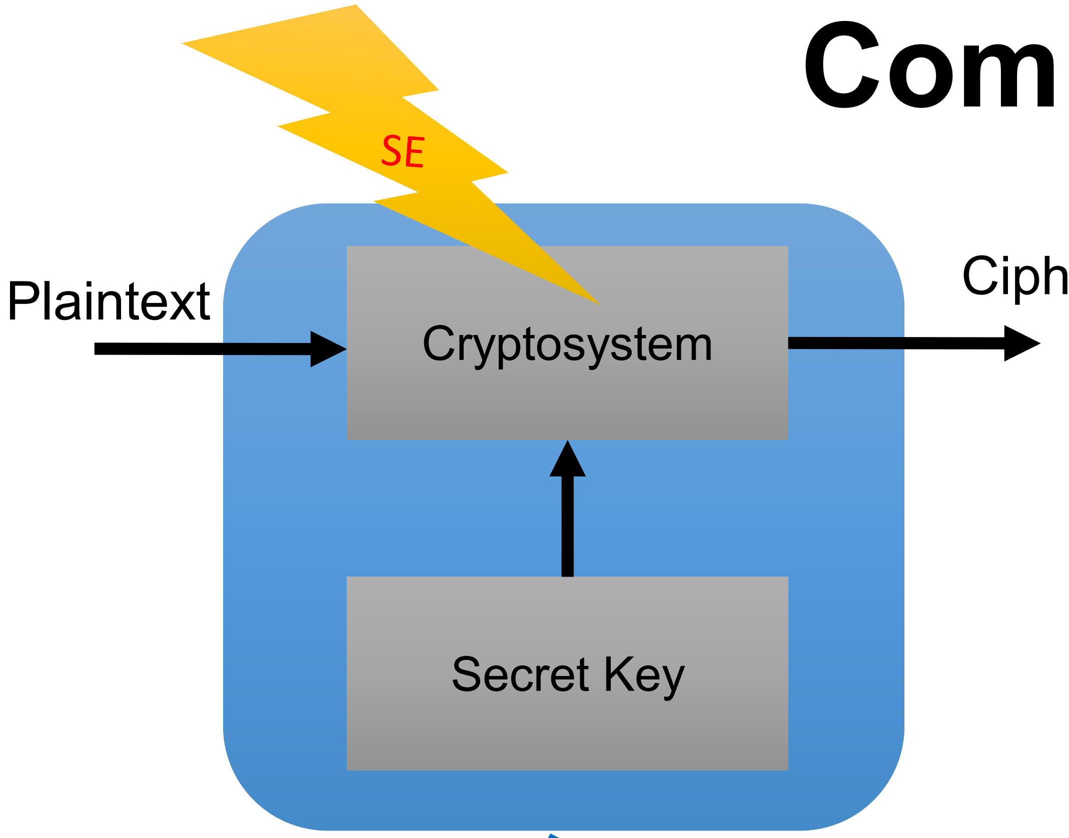


FA Countermeasures

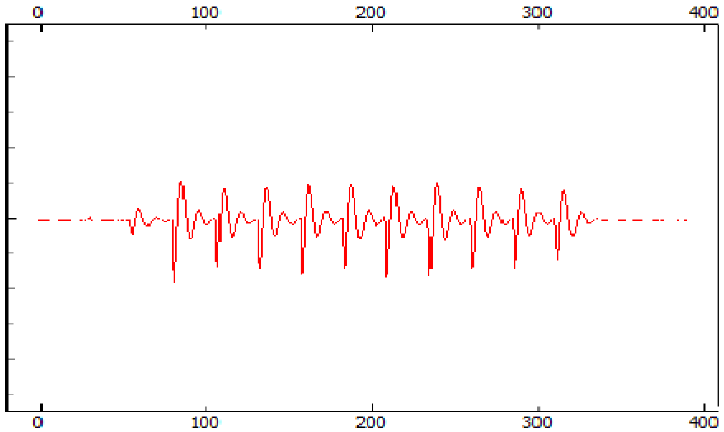
- DMR
- Inverse function
- ECC

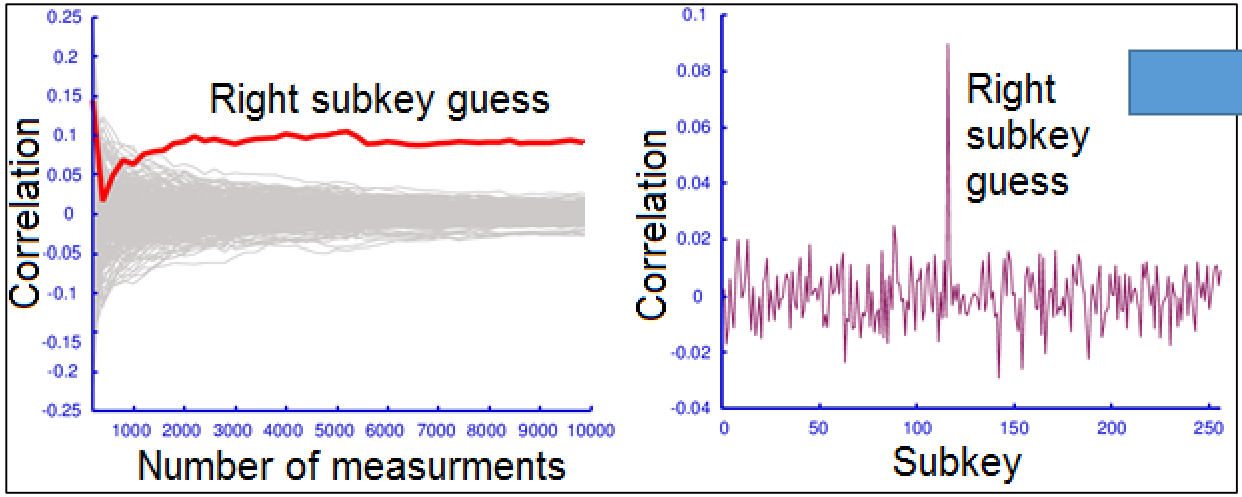
G. Canivet, et al., Journal of Cryptology, 2011.

Combined Attack



Power consumption





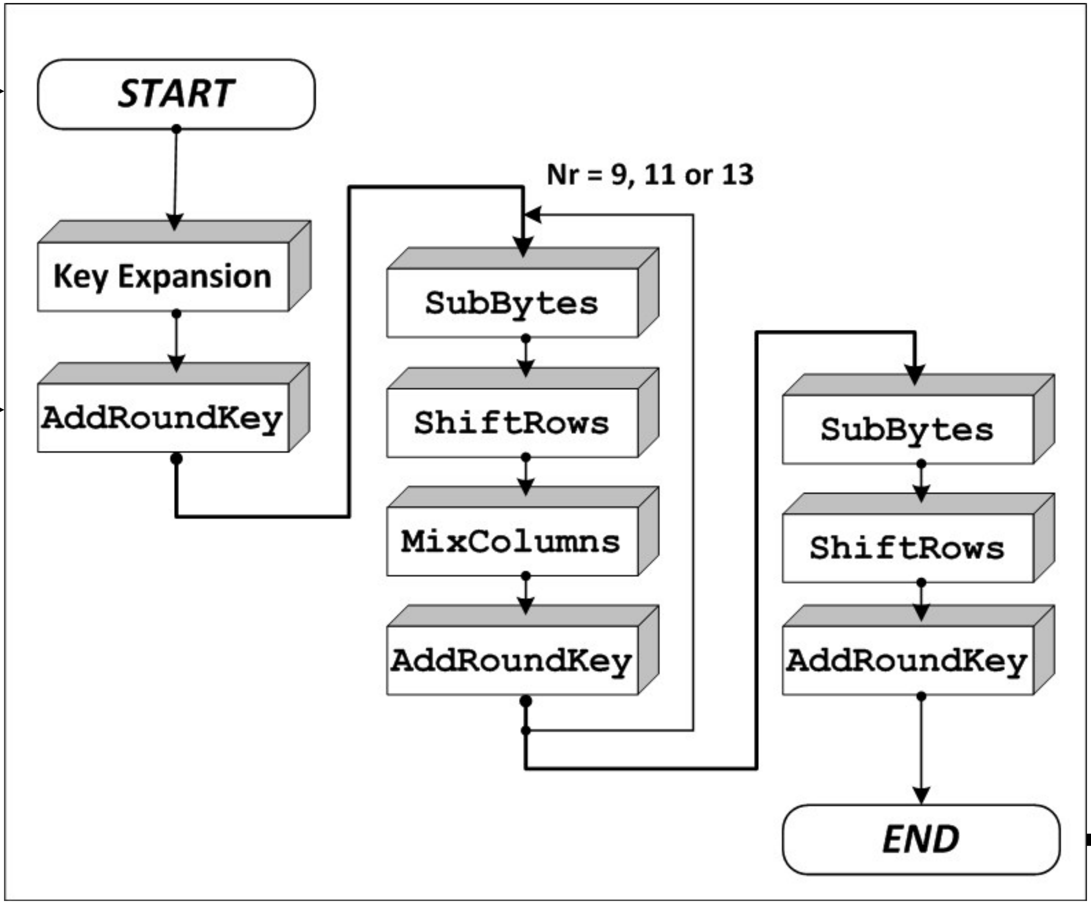
[REF]

[1] W. Hnath, J. Pettengill, *Major Qualifying Project, 2010.*

AES Cipher

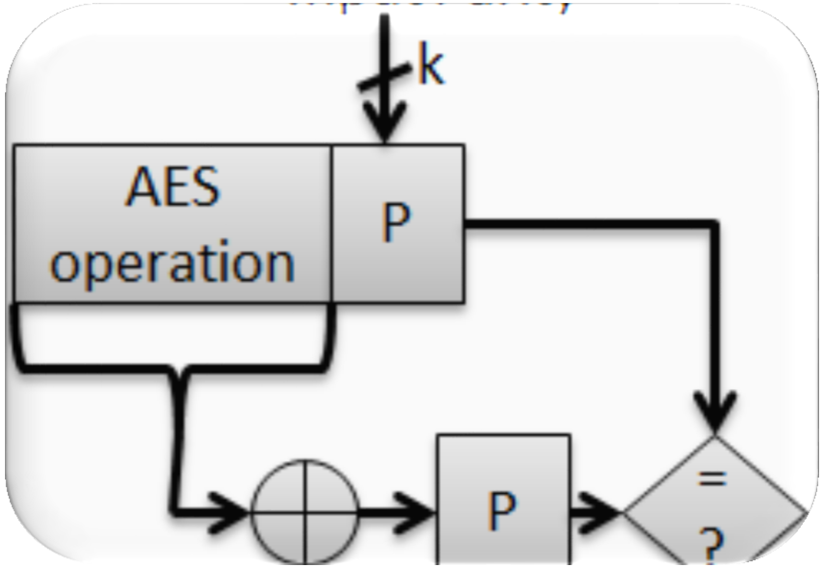
Plaintext

Key

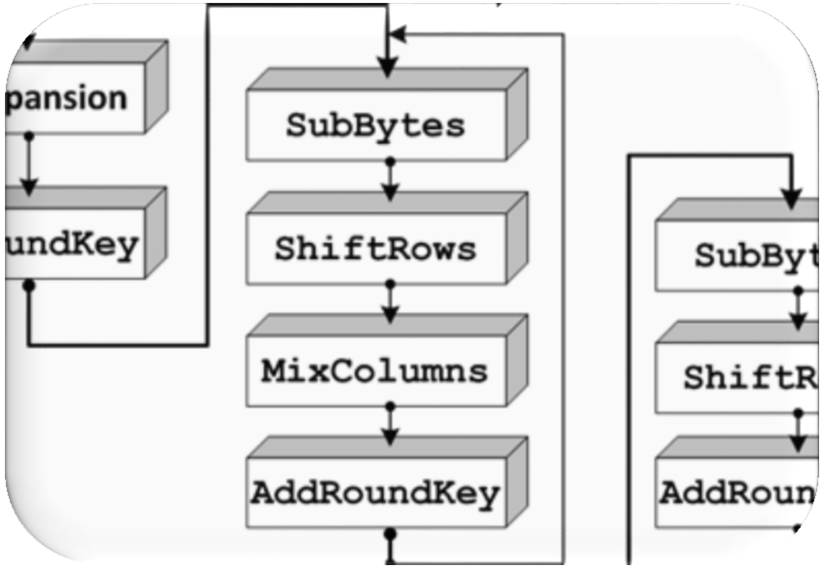


Ciphertext

Impact of existing countermeasures for fault attack on cryptosystem security

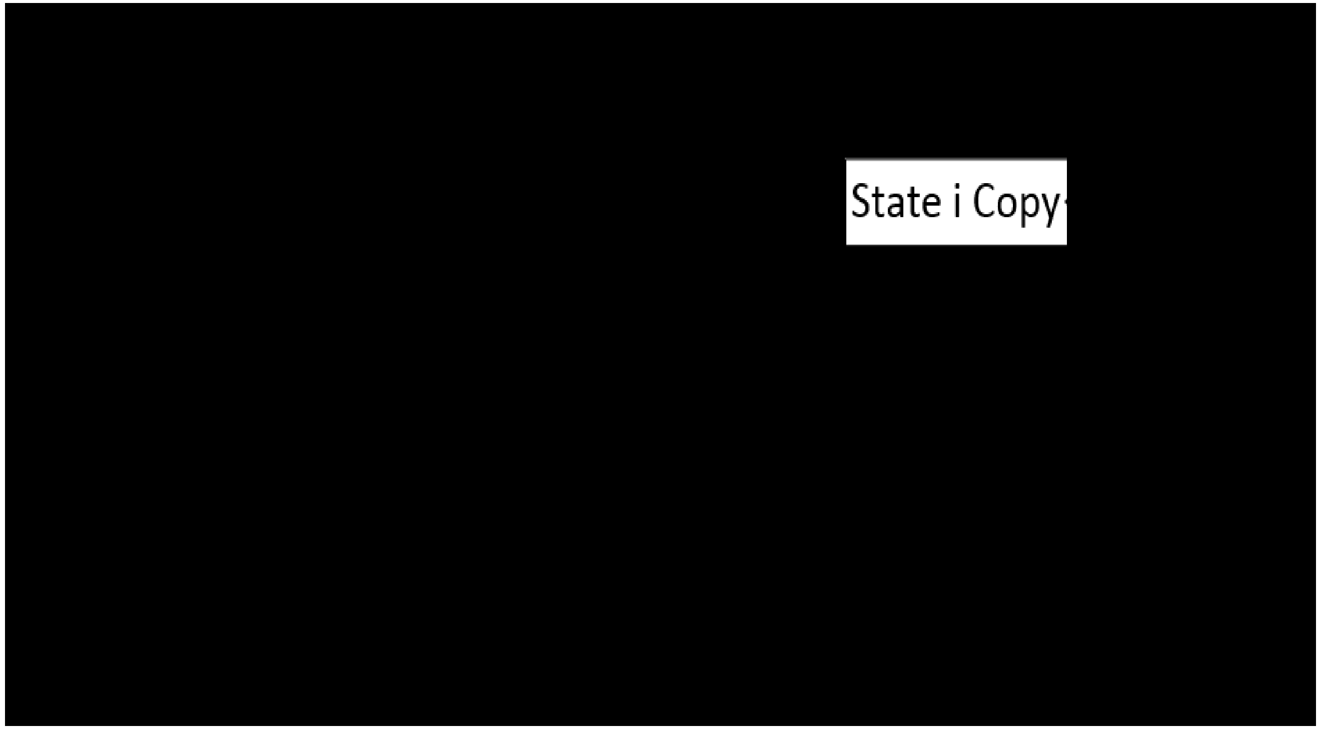


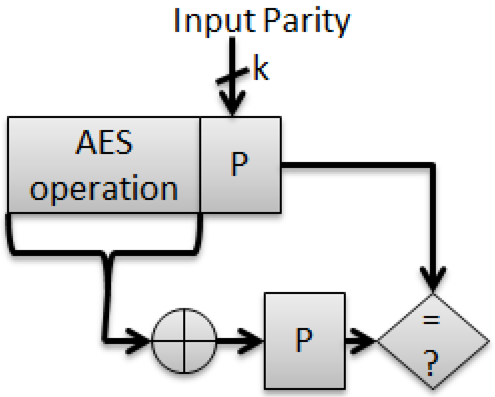
Different fault detection methods



Fault detection methods on different modules

Fault Detection Methods





[1] Double modular redundancy (DMR)

[2] Inverse function

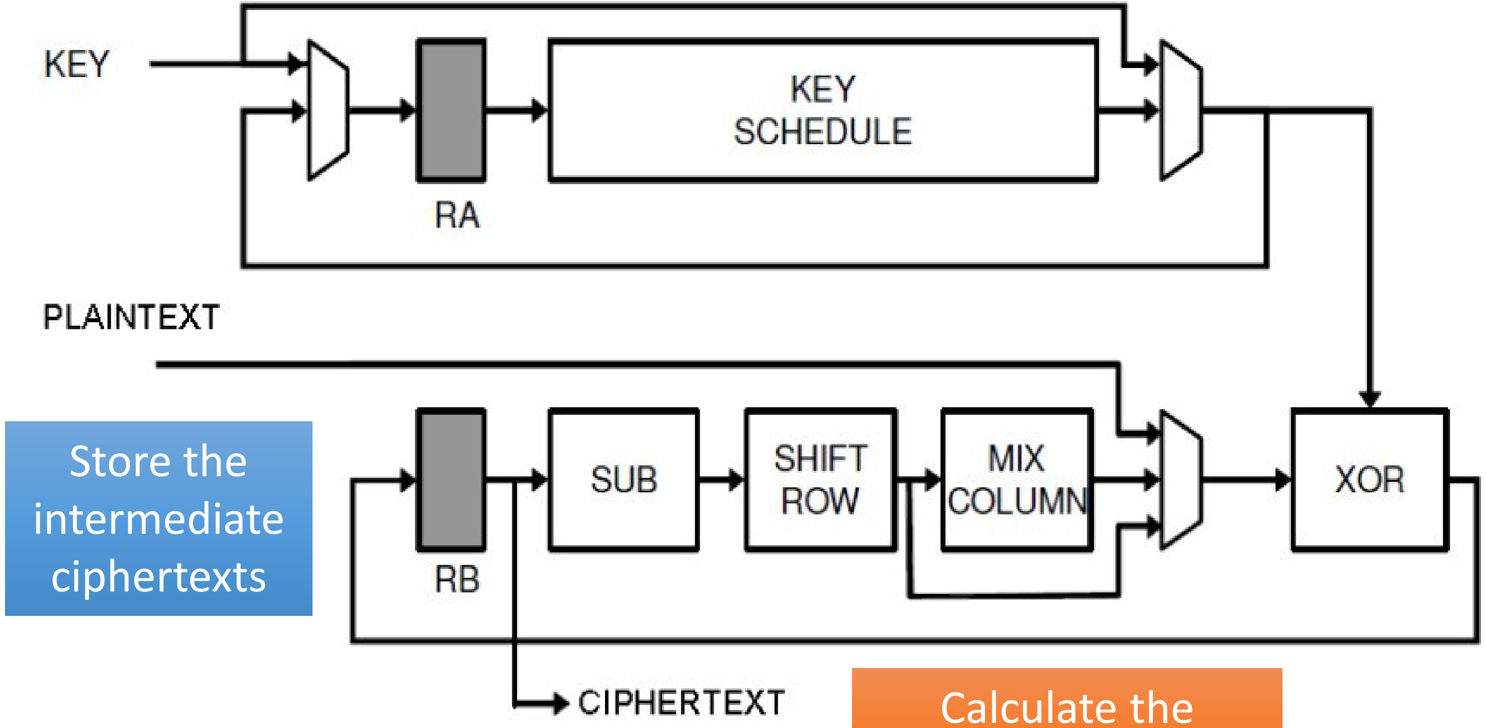
Parity check code

[1] G. Di Natale, et al., *JET*, 2009.

[2] R. Karri, et al., *DAC*, 2001.

CPA Attack on AES

Guess the first subkey

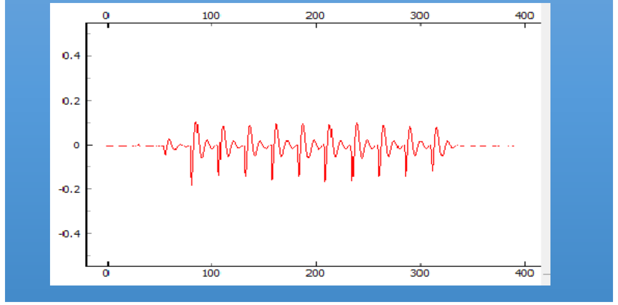


Store the intermediate ciphertexts

[1]

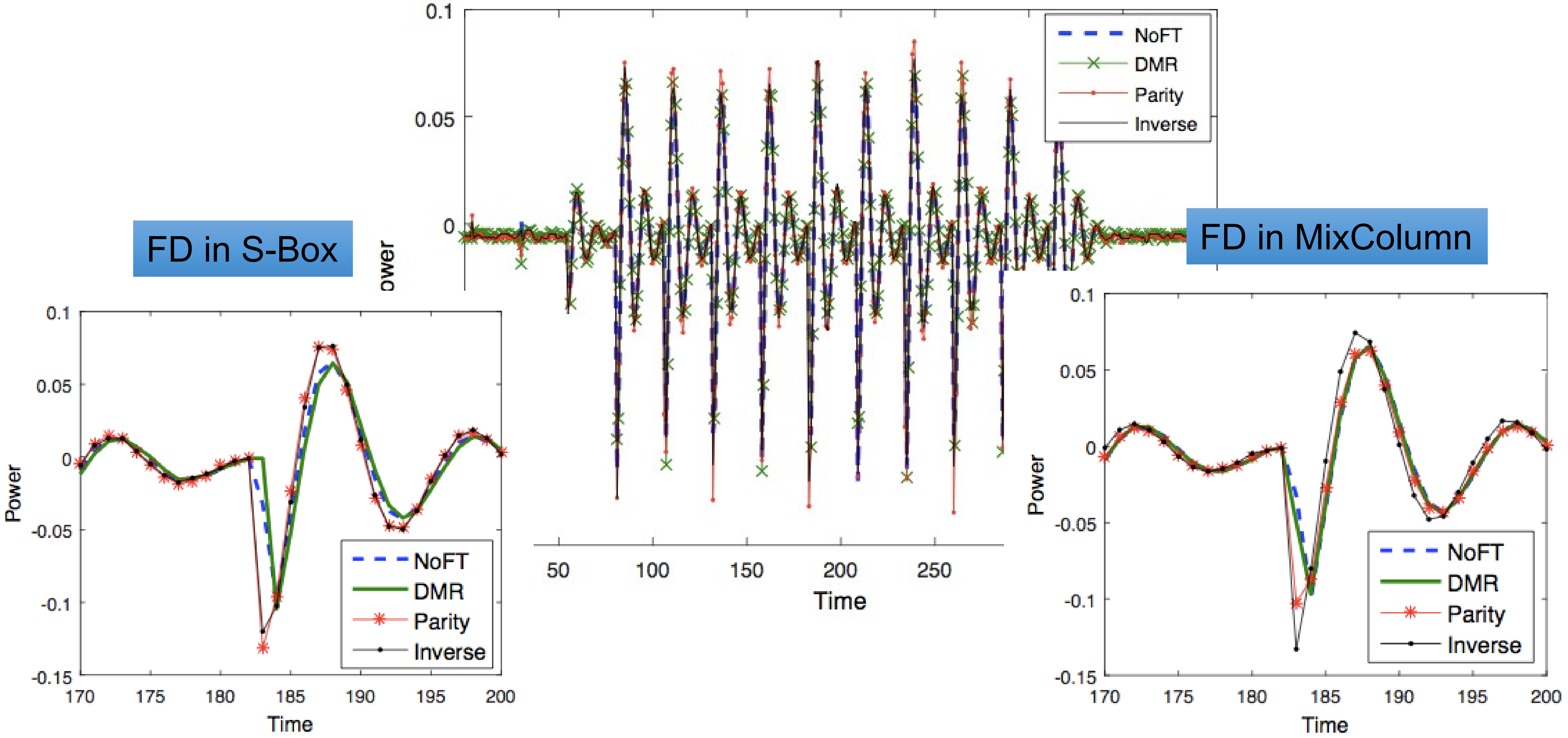
Calculate the ciphertext

Record the power consumption



[1] S. Shah, *ReConFig*, 2010.

CPA Attack on AES



FD in S-Box

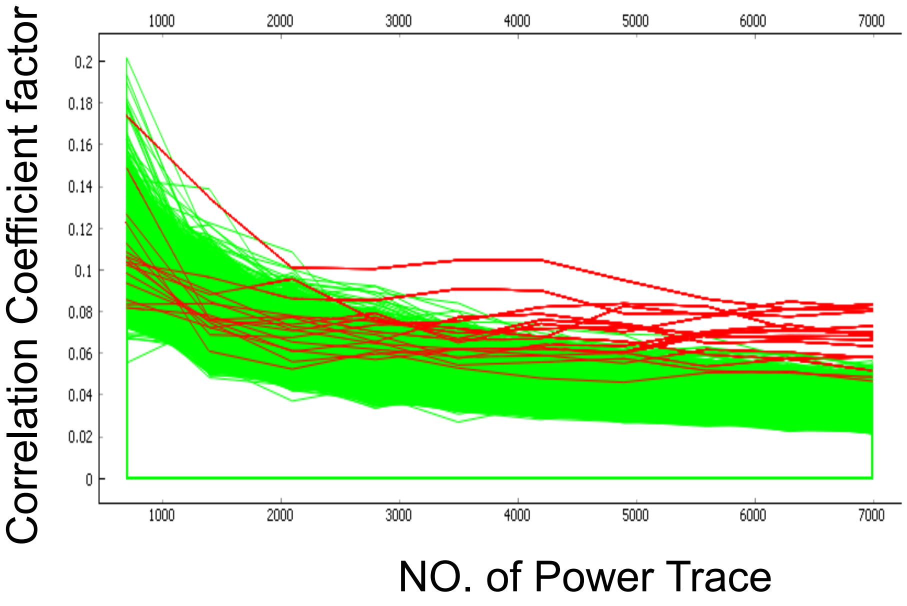
FD in MixColumn

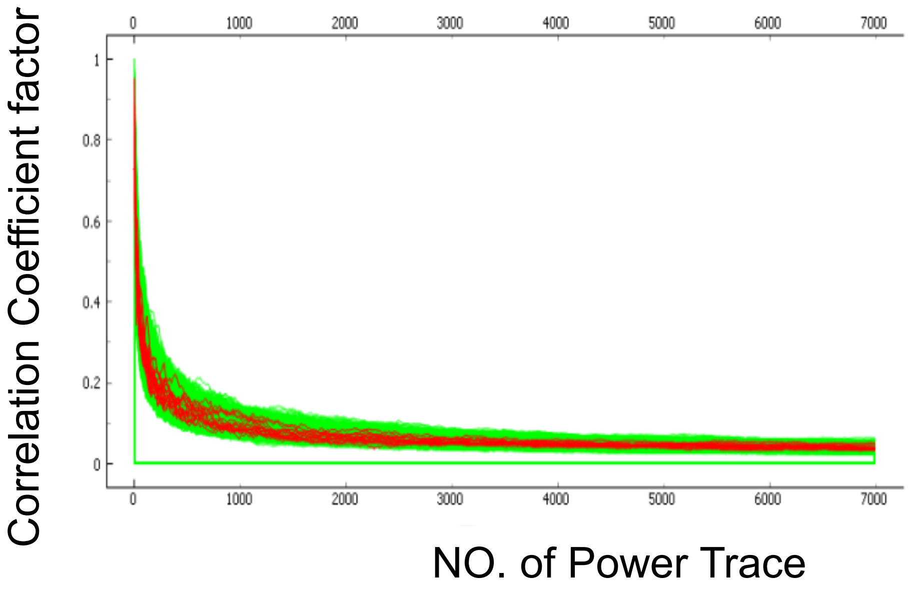
CPA Attack on AES

[1] $$r_{i,j} = \frac{D\sum_{d=1}^{D} h_{d,i}\, t_{d,j} - \sum_{d=1}^{D} h_{d,i} \sum_{d=1}^{D} t_{d,j}}{\sqrt{\left(\left(\sum_{d=1}^{D} h_{d,i}\right)^2 - D\left(\sum_{d=1}^{D} h_{d,i}^{2}\right)\right)\left(\left(\sum_{d=1}^{D} t_{d,j}\right)^2 - D\left(\sum_{d=1}^{D} t_{d,j}^{2}\right)\right)}}$$

Convert the ciphertext to power trace

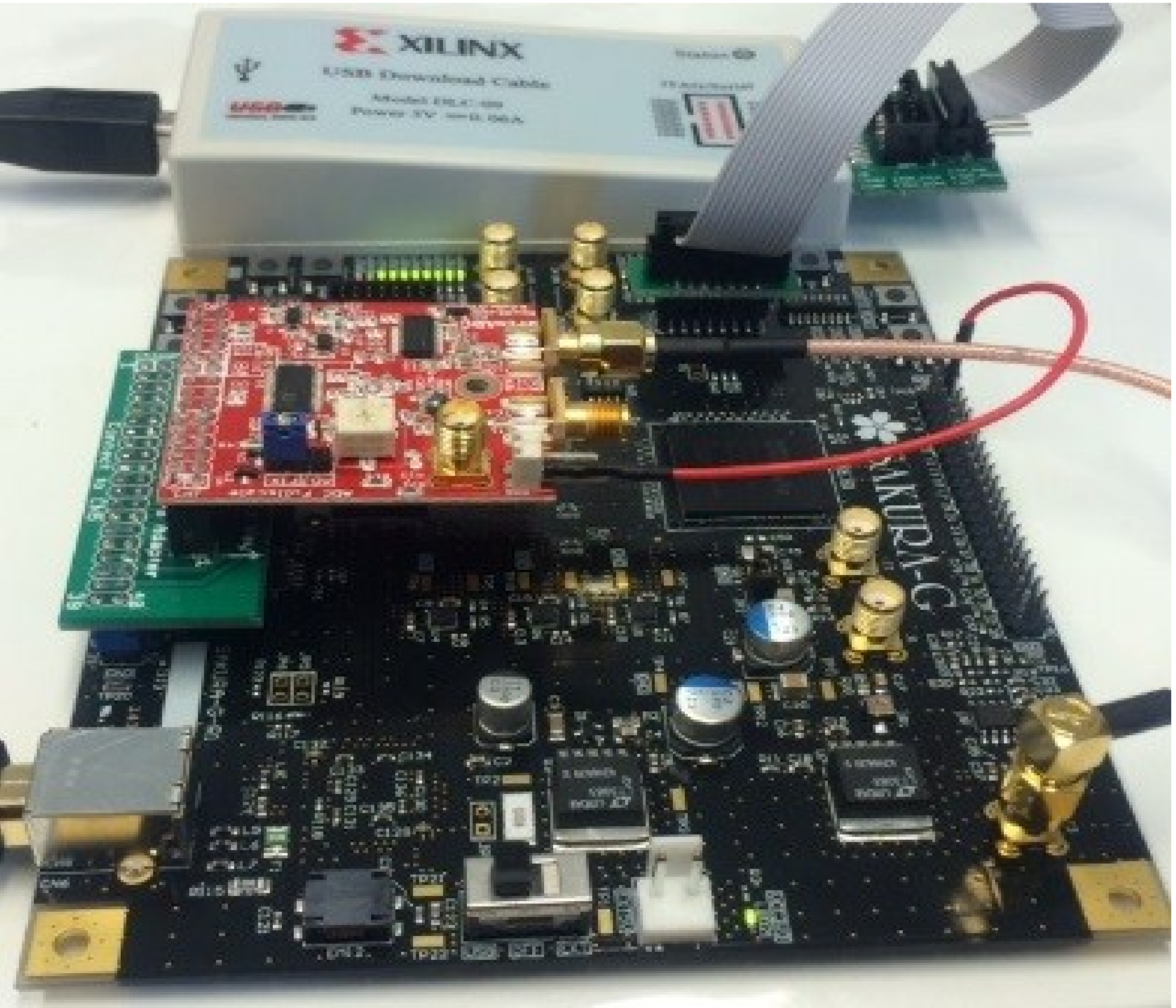
h = aH(D) + b



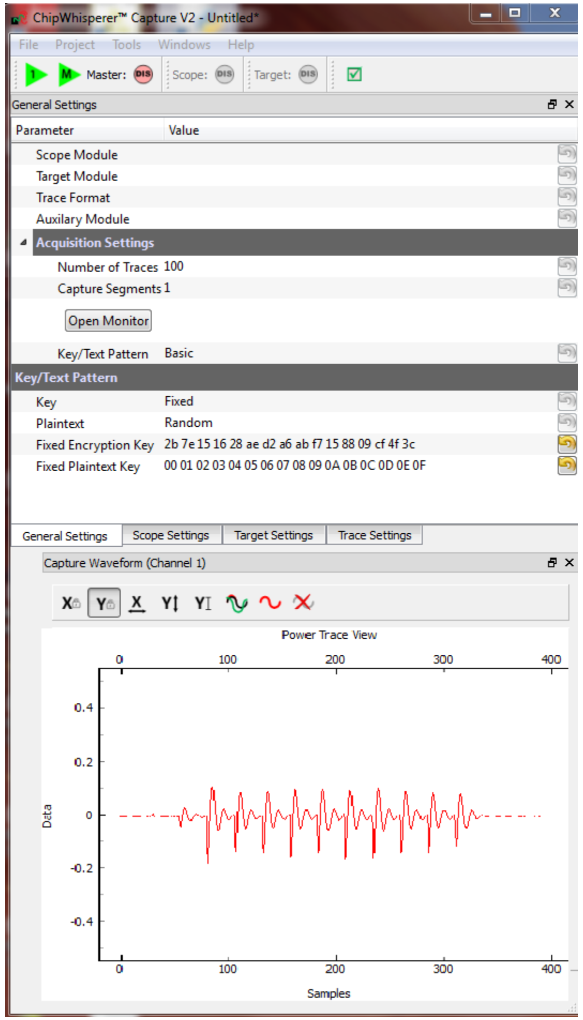


[1] E. Brier et al., Lecture Notes in Computer Science, 2004.

Experimental Setup

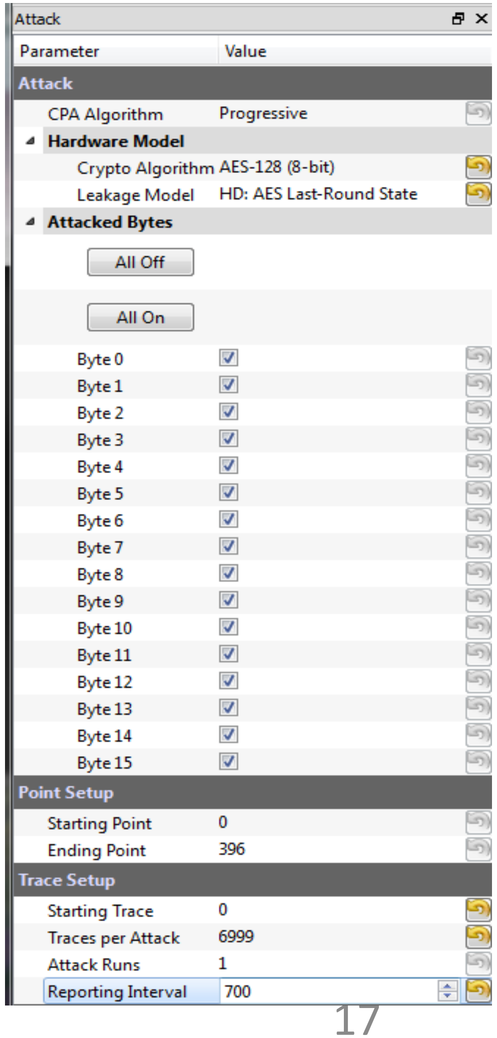


Capture



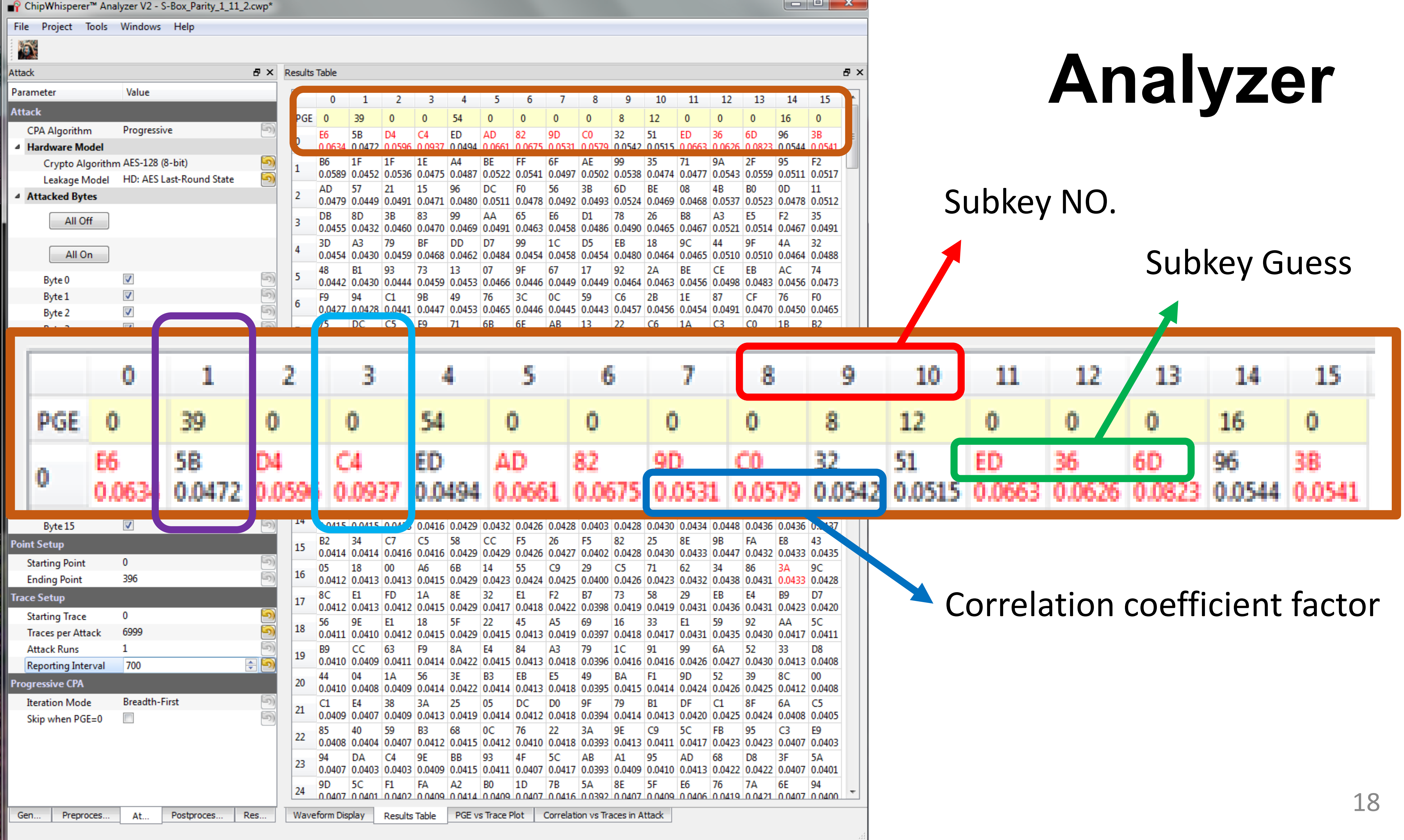
Parameter	Value
Scope Module	
Target Module	
Trace Format	
Auxilary Module	
Acquisition Settings	
Number of Traces	100
Capture Segments	1
Key/Text Pattern	Basic
Key/Text Pattern	
Key	Fixed
Plaintext	Random
Fixed Encryption Key	2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
Fixed Plaintext Key	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Analyzer



Parameter	Value
Attack	
CPA Algorithm	Progressive
Hardware Model	
Crypto Algorithm	AES-128 (8-bit)
Leakage Model	HD: AES Last-Round State
Attacked Bytes	
Byte 0	☑
Byte 1	☑
Byte 2	☑
Byte 3	☑
Byte 4	☑
Byte 5	☑
Byte 6	☑
Byte 7	☑
Byte 8	☑
Byte 9	☑
Byte 10	☑
Byte 11	☑
Byte 12	☑
Byte 13	☑
Byte 14	☑
Byte 15	☑
Point Setup	
Starting Point	0
Ending Point	396
Trace Setup	
Starting Trace	0
Traces per Attack	6999
Attack Runs	1
Reporting Interval	700

Analyzer

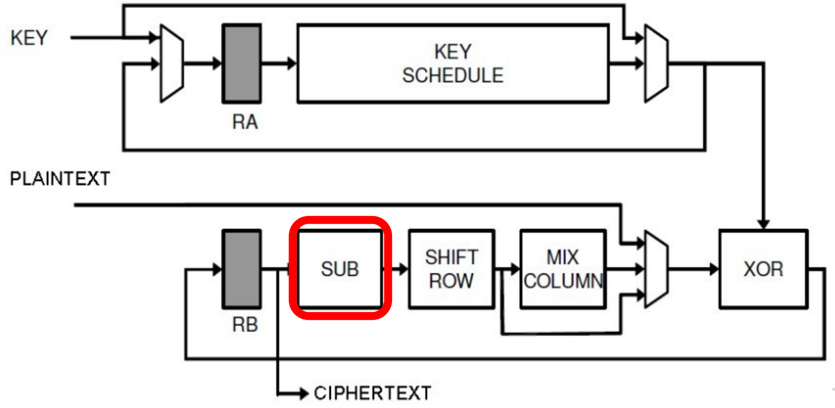


Parameter	Value
Attack	
CPA Algorithm	Progressive
Hardware Model	
Crypto Algorithm	AES-128 (8-bit)
Leakage Model	HD: AES Last-Round State
Attacked Bytes	
Byte 0	☑
Byte 1	☑
Byte 2	☑
Byte 15	☑
Point Setup	
Starting Point	0
Ending Point	396
Trace Setup	
Starting Trace	0
Traces per Attack	6999
Attack Runs	1
Reporting Interval	700
Progressive CPA	
Iteration Mode	Breadth-First
Skip when PGE=0	☐

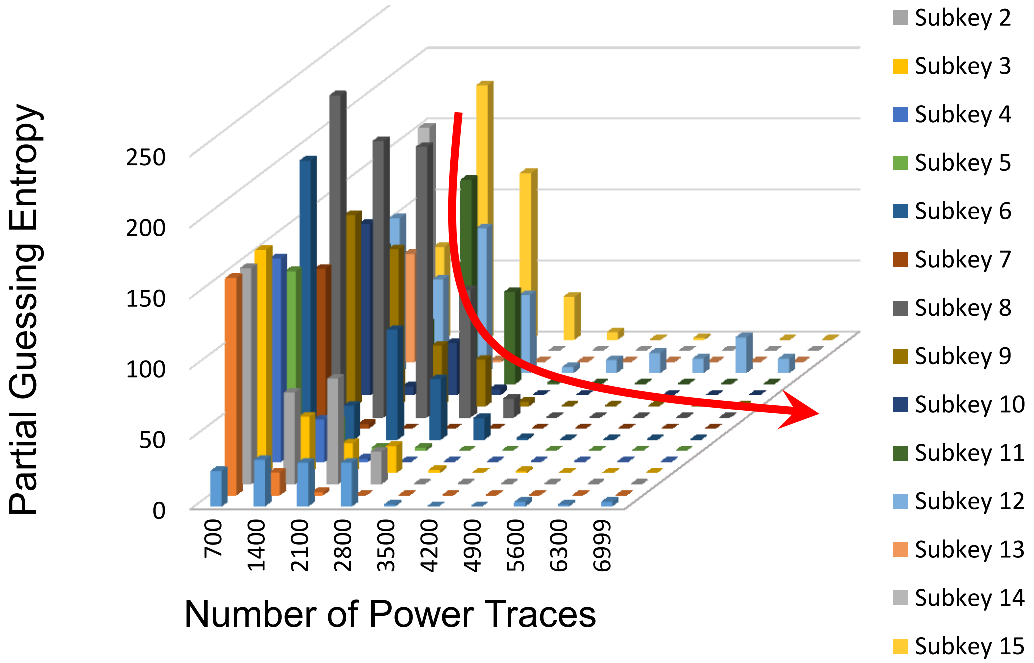
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE	0	39	0	0	54	0	0	0	0	8	12	0	0	0	16	0
0	E6 0.0634	5B 0.0472	D4 0.0596	C4 0.0937	ED 0.0494	AD 0.0661	82 0.0675	9D 0.0531	C0 0.0579	32 0.0542	51 0.0515	ED 0.0663	36 0.0626	6D 0.0823	96 0.0544	3B 0.0541
1	B6 0.0589	1F 0.0452	1F 0.0536	1E 0.0475	A4 0.0487	BE 0.0522	FF 0.0541	6F 0.0497	AE 0.0502	99 0.0538	35 0.0474	71 0.0477	9A 0.0543	2F 0.0559	95 0.0511	F2 0.0517
2	AD 0.0479	57 0.0449	21 0.0491	15 0.0471	96 0.0480	DC 0.0511	F0 0.0478	56 0.0492	3B 0.0493	6D 0.0524	BE 0.0469	08 0.0468	4B 0.0537	B0 0.0523	0D 0.0478	11 0.0512
3	DB 0.0455	8D 0.0432	3B 0.0460	83 0.0470	99 0.0469	AA 0.0491	65 0.0463	E6 0.0458	D1 0.0486	78 0.0490	26 0.0465	B8 0.0467	A3 0.0521	E5 0.0514	F2 0.0467	35 0.0491
4	3D 0.0454	A3 0.0430	79 0.0459	BF 0.0468	DD 0.0462	D7 0.0484	99 0.0454	1C 0.0458	D5 0.0454	EB 0.0480	18 0.0464	9C 0.0465	44 0.0510	9F 0.0510	4A 0.0464	32 0.0488
5	48 0.0442	B1 0.0430	93 0.0444	73 0.0459	13 0.0453	07 0.0466	9F 0.0446	67 0.0449	17 0.0449	92 0.0464	2A 0.0463	BE 0.0456	CE 0.0498	EB 0.0483	AC 0.0456	74 0.0473
6	F9 0.0427	94 0.0428	C1 0.0441	9B 0.0447	49 0.0453	76 0.0465	3C 0.0446	0C 0.0445	59 0.0443	C6 0.0457	2B 0.0456	1E 0.0454	87 0.0491	CF 0.0470	76 0.0450	F0 0.0465
	75	DC	C5	F9	71	6B	6E	AB	13	22	C6	1A	C3	C0	1B	B2
14	0.0415	0.0415	[illegible]	0.0416	0.0429	0.0432	0.0426	0.0428	0.0403	0.0428	0.0430	0.0434	0.0448	0.0436	0.0436	[illegible]
15	B2 0.0414	34 0.0414	C7 0.0416	C5 0.0416	58 0.0429	CC 0.0429	F5 0.0426	26 0.0427	F5 0.0402	82 0.0428	25 0.0430	8E 0.0433	9B 0.0447	FA 0.0432	E8 0.0433	43 0.0435
16	05 0.0412	18 0.0413	00 0.0413	A6 0.0415	6B 0.0429	14 0.0423	55 0.0424	C9 0.0425	29 0.0400	C5 0.0426	71 0.0423	62 0.0432	34 0.0438	86 0.0431	3A 0.0433	9C 0.0428
17	8C 0.0412	E1 0.0413	FD 0.0412	1A 0.0415	8E 0.0429	32 0.0417	E1 0.0418	F2 0.0422	B7 0.0398	73 0.0419	58 0.0419	29 0.0431	EB 0.0436	E4 0.0431	B9 0.0423	D7 0.0420
18	56 0.0411	9E 0.0410	E1 0.0412	18 0.0415	5F 0.0429	22 0.0415	45 0.0413	A5 0.0419	69 0.0397	16 0.0418	33 0.0417	E1 0.0431	59 0.0435	92 0.0430	AA 0.0417	5C 0.0411
19	B9 0.0410	CC 0.0409	63 0.0411	F9 0.0414	8A 0.0422	E4 0.0415	84 0.0413	A3 0.0418	79 0.0396	1C 0.0416	91 0.0416	99 0.0426	6A 0.0427	52 0.0430	33 0.0413	D8 0.0408
20	44 0.0410	04 0.0408	1A 0.0409	56 0.0414	3E 0.0422	B3 0.0414	EB 0.0413	E5 0.0418	49 0.0395	BA 0.0415	F1 0.0414	9D 0.0424	52 0.0426	39 0.0425	8C 0.0412	00 0.0408
21	C1 0.0409	E4 0.0407	38 0.0409	3A 0.0413	25 0.0419	05 0.0414	DC 0.0412	D0 0.0418	9F 0.0394	79 0.0414	B1 0.0413	DF 0.0420	C1 0.0425	8F 0.0424	6A 0.0408	C5 0.0405
22	85 0.0408	40 0.0404	59 0.0407	B3 0.0412	68 0.0415	0C 0.0412	76 0.0410	22 0.0418	3A 0.0393	9E 0.0413	C9 0.0411	5C 0.0417	FB 0.0423	95 0.0423	C3 0.0407	E9 0.0403
23	94 0.0407	DA 0.0403	C4 0.0403	9E 0.0409	BB 0.0415	93 0.0411	4F 0.0407	5C 0.0417	AB 0.0393	A1 0.0409	95 0.0410	AD 0.0413	68 0.0422	D8 0.0422	3F 0.0407	5A 0.0401
24	9D 0.0407	5C 0.0401	F1 0.0402	FA 0.0409	A2 0.0414	B0 0.0409	1D 0.0407	7B 0.0416	5A 0.0392	8E 0.0407	5F 0.0409	E6 0.0406	76 0.0419	7A 0.0421	6E 0.0407	94 0.0400

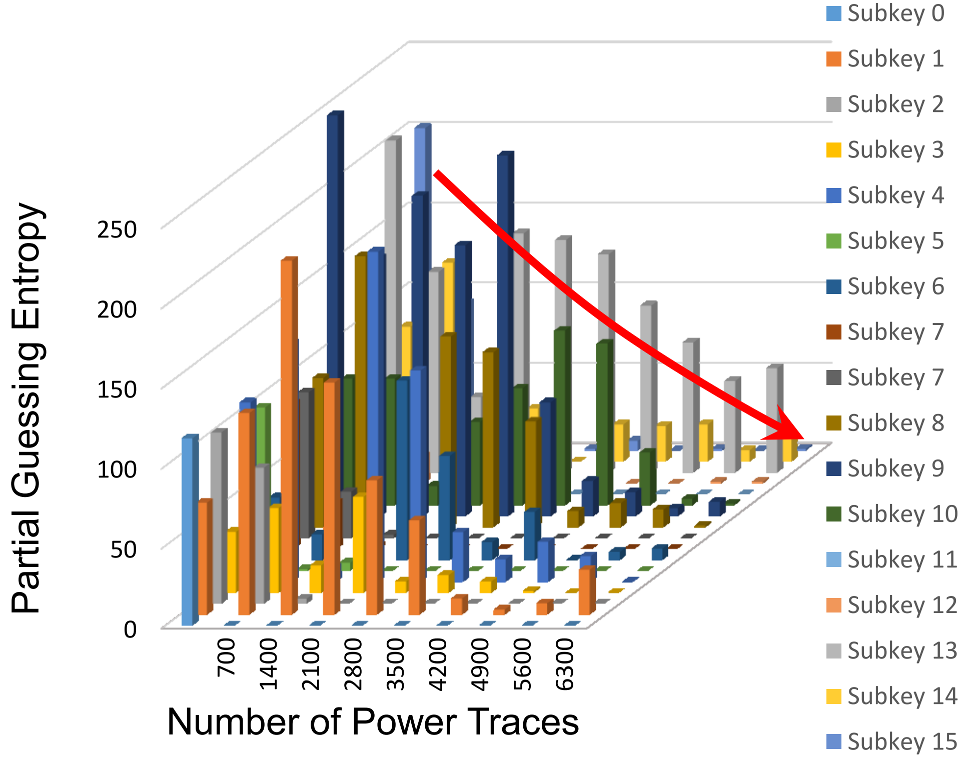
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE	0	39	0	0	54	0	0	0	0	8	12	0	0	0	16	0
0	E6 0.0634	5B 0.0472	D4 0.0596	C4 0.0937	ED 0.0494	AD 0.0661	82 0.0675	9D 0.0531	C0 0.0579	32 0.0542	51 0.0515	ED 0.0663	36 0.0626	6D 0.0823	96 0.0544	3B 0.0541

Impact of FD on SCA Attack

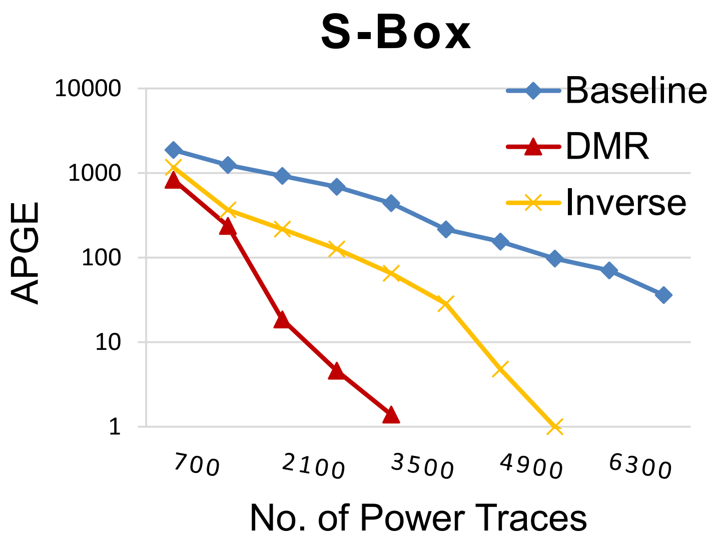


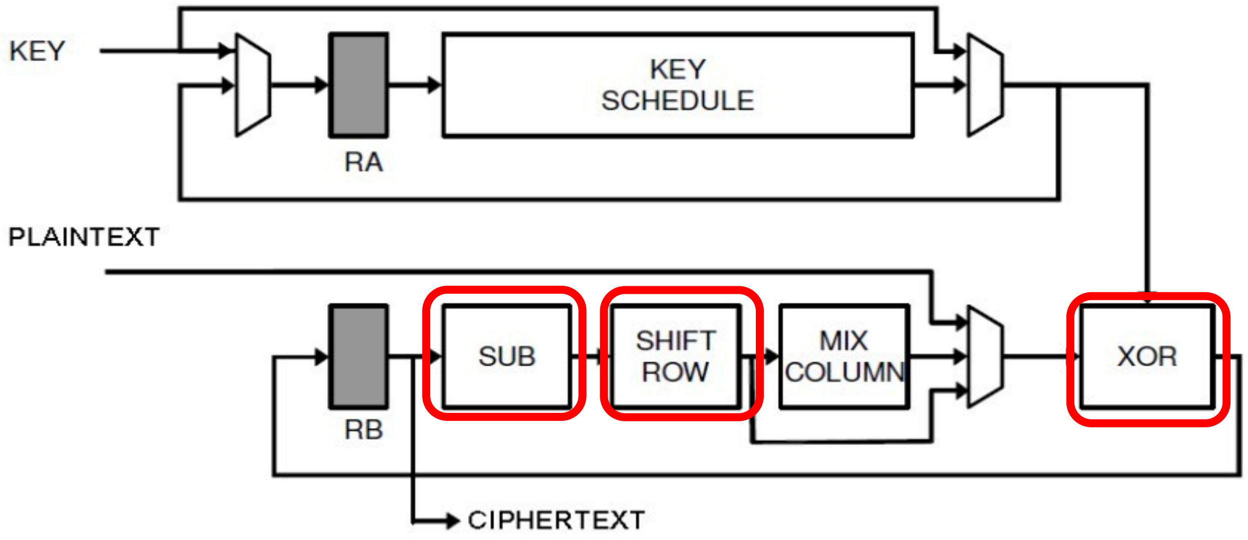
FD: Parity check code





Impact of Different Hardware Redundancy-Based FD Methods on SCA Attack





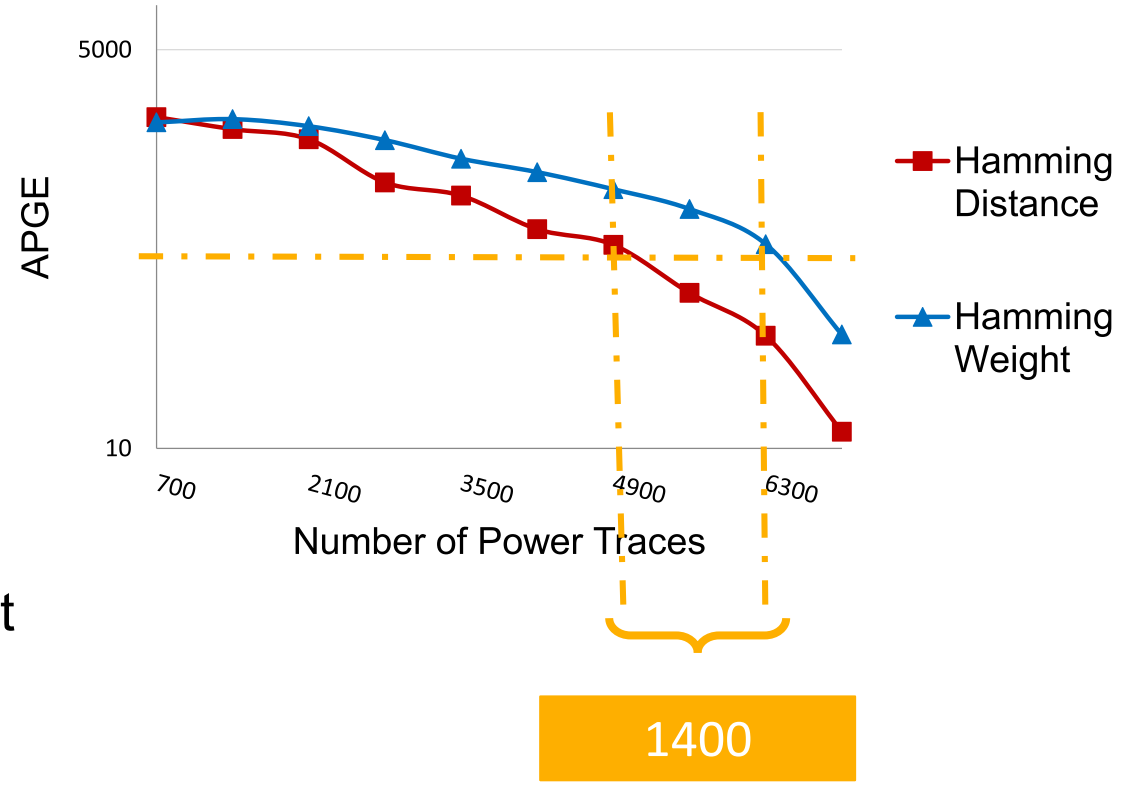
Existence of hardware redundancy-based FD increase the efficiency of CPA

Use information redundancy-based FD

Impact of Different Power Models in CPA Attack

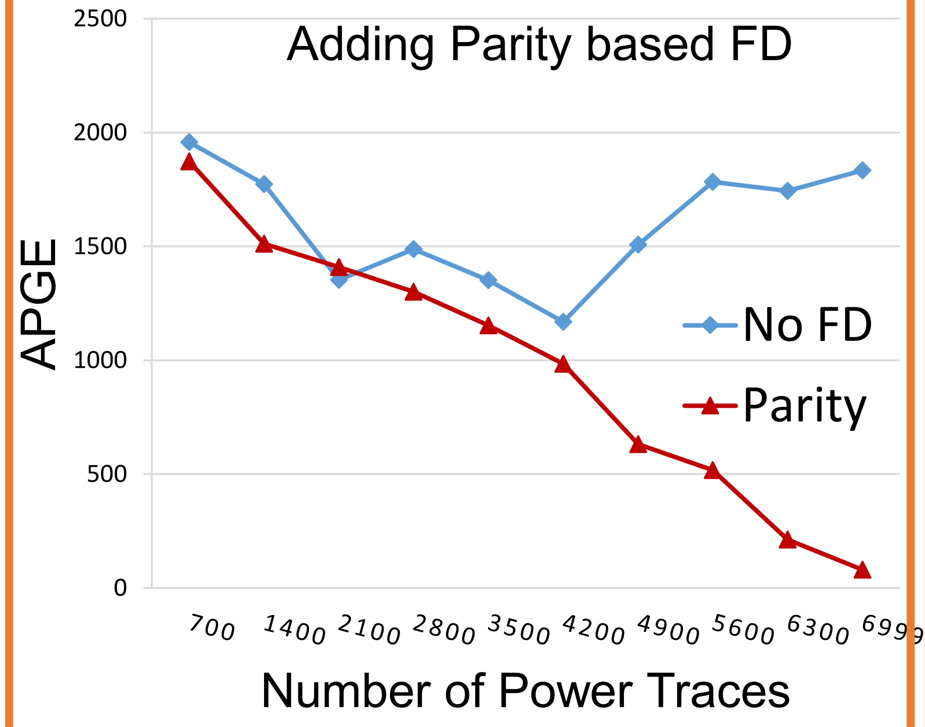
0	0	0	0	0	0	0	0	Ref. ciphertext
1	1	0	0	0	0	1	0	Real ciphertext
1	1	0	0	0	0	1	0	HW: 3

0	1	1	0	0	1	1	1	Previous ciphertext
1	1	0	1	1	0	1	0	Real ciphertext
1	0	1	1	1	1	0	1	HD: 6



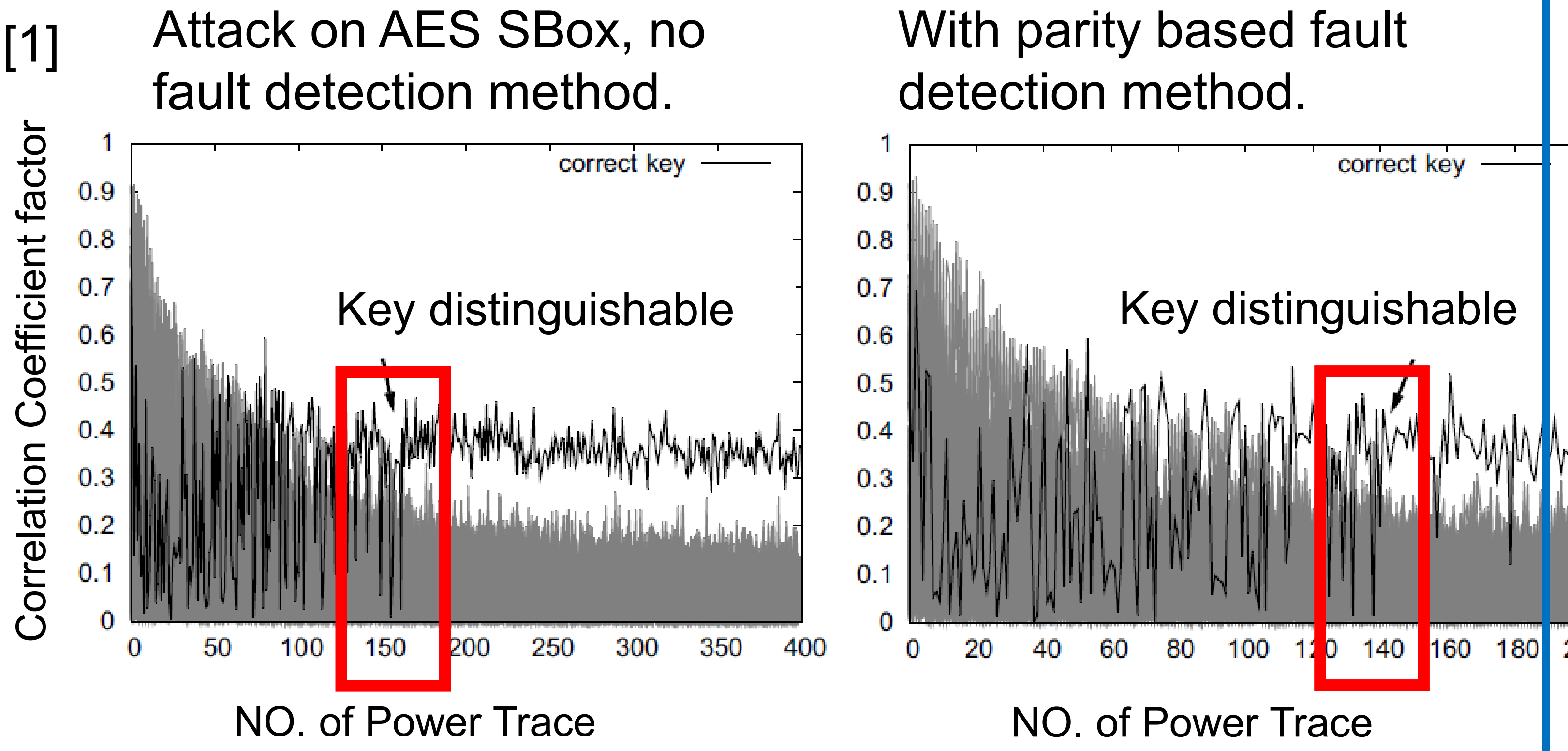
S-Box

Impact of Different Power Models in CPA Attack



Increases the robustness of the cryptographic algorithm

[1]


Attack on AES SBox, no fault detection method.

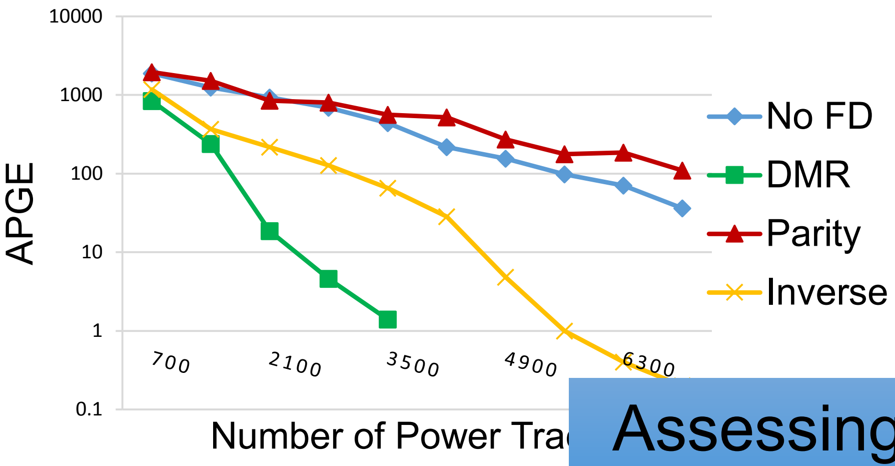
With parity based fault detection method.

Decreases the robustness of the cryptographic algorithm

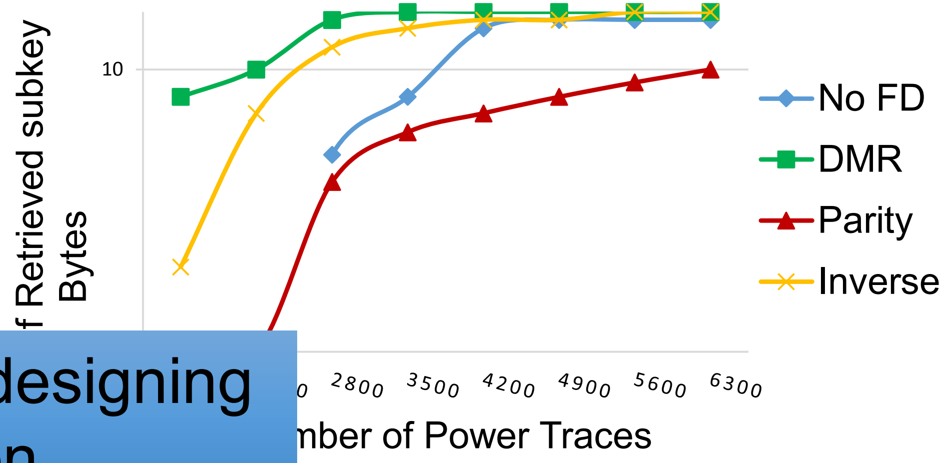
[1] F. Regazzoni et al. , DFT, 2008.

Two Approaches to Study the Impact of Different FDs

APGE for Different FDs on SBox

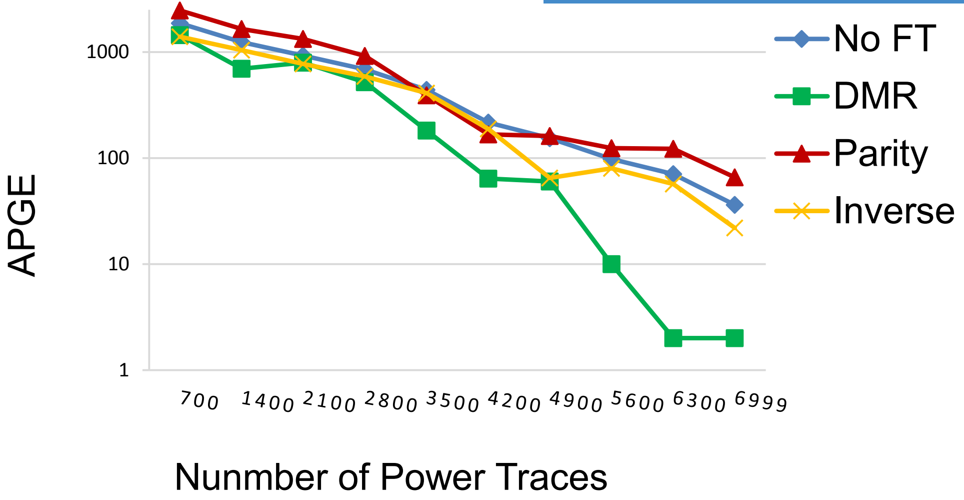


NO. of Retrieved Subkey Bytes for Different FDs on SBox

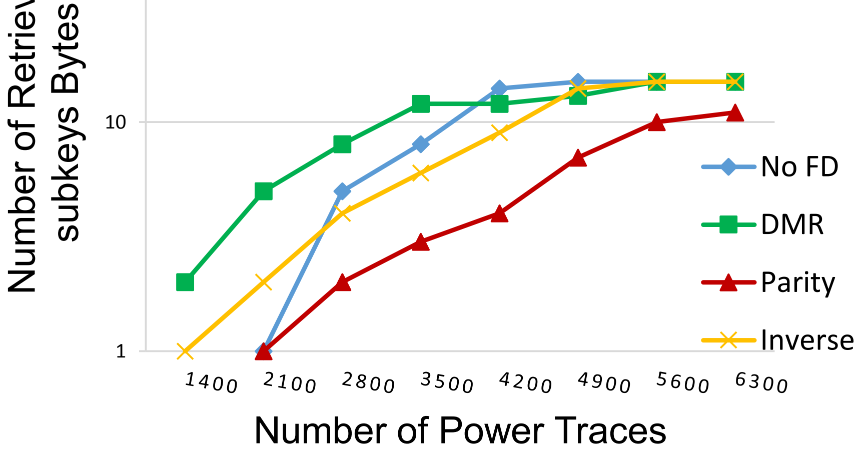


Assessing the process of designing a suitable protection

APGE For Different



NO. of Retrieved Subkey Bytes for Different FDs on Mixcolumn



Conclusion

- As the combination of FA and SCA attacks is emerging as an advanced attack, effective countermeasure for the combined attack is needed.
- One countermeasure for a particular attack can influence the other attack positively or negatively.
- Our experimental results indicate that the effective factors on CPA efficiency include
  - Type of redundancy
  - Module under protection
  - CPA attack power model

Thank you!

Any Questions?