Revealing the Weakness of Addition Chain Based Masked SBox Implementations

Jingdian Ming, Huizhong Li, Yongbin Zhou, Wei Cheng, Zehua Qiao

中国科学院 信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

中国科学院
CHINESE ACADEMY OF SCIENCES

南京理工大学
NANJING UNIVERSITY OF SCIENCE & TECHNOLOGY

INSTITUT
POLYTECHNIQUE
DE PARIS

CHES 2021

Outline

1. **Introduction and Previous Work**

2. **Resistance Measurement**

3. **Practical Experiments**

4. **Conclusion**

Outline

1. Introduction and Previous Work

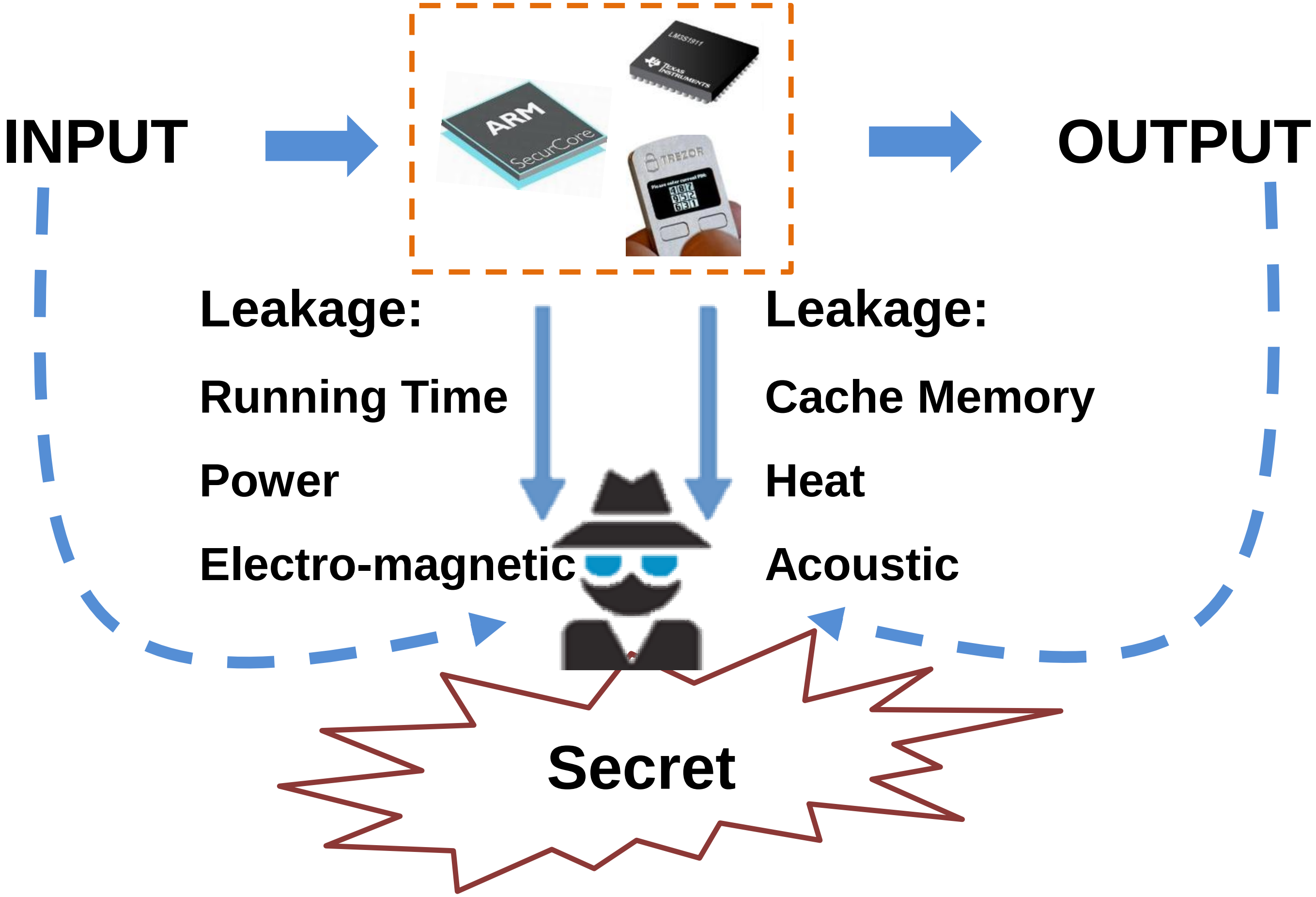
2. Resistance Measurement

3. Practical Experiments

4. Conclusion

Introduction and Previous Work

Side-channel attacks



INPUT

OUTPUT

Leakage:

Running Time

Power

Electro-magnetic

Leakage:

Cache Memory

Heat

Acoustic

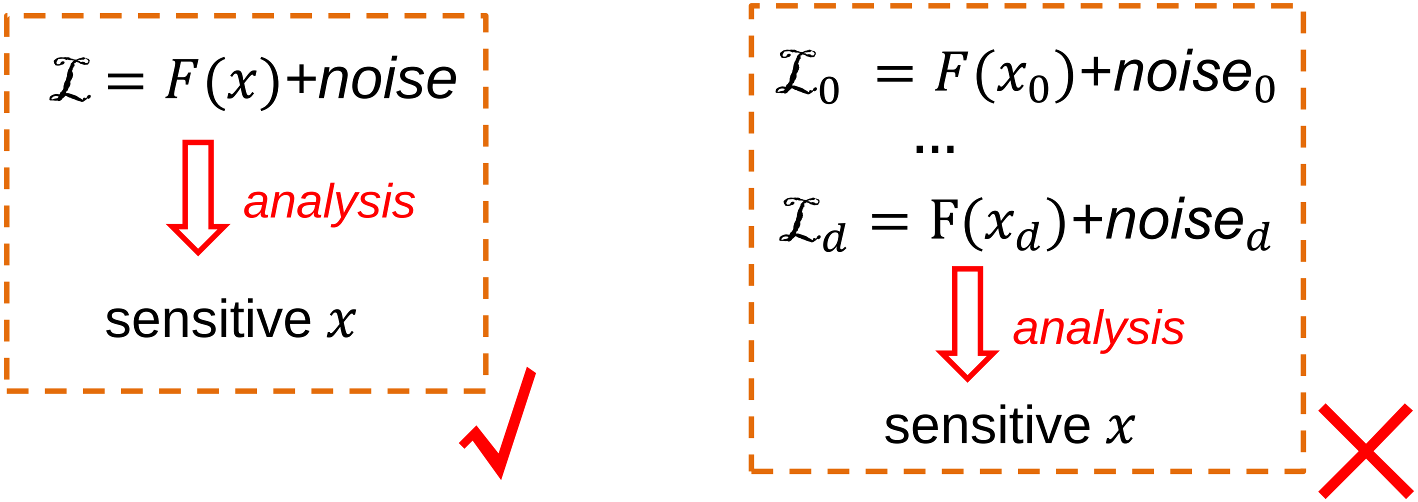
Secret

Introduction and Previous Work

Masking

Masking: randomize the dependency between sensitive intermediate and its corresponding leakages by splitting the sensitive values into *d+1* shares

$$x = x_0 \oplus x_1 \dots x_d$$



$\mathcal{L} = F(x)$+*noise*

analysis

sensitive x

✓

$\mathcal{L}_0 = F(x_0)$+*noise*$_0$

...

$\mathcal{L}_d = \mathrm{F}(x_d)$+*noise*$_d$

analysis

sensitive x

✗

[CJR+99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, Pankaj Rohatgi. Towards Sound Approaches to Counteract Power-Analysis Attacks. CRYPTO 1999: 398-412

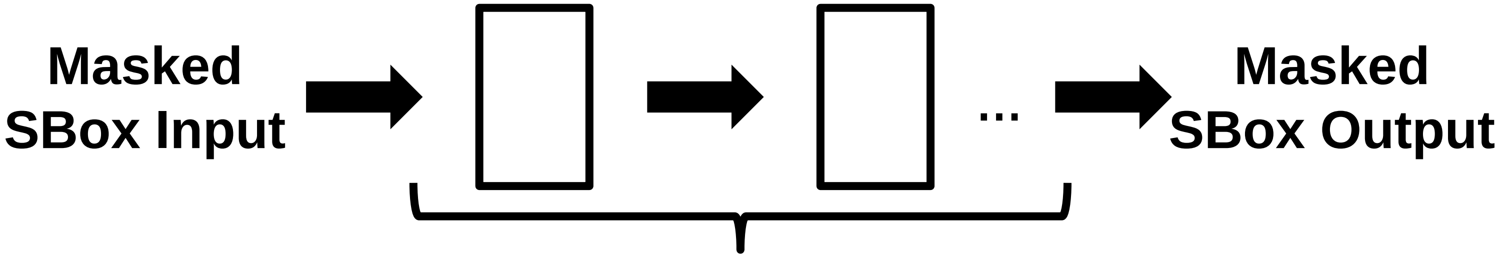
[Mes00] Thomas S. Messerges. Securing the AES Finalists against Power Analysis Attacks. FSE 2000: 150-164

Introduction and Previous Work

Masked Implementation for SBox

- Look-up table based implementation [CRZ18]

- Compute the unrolled functions over a finite field [RP10]



Several masked computations over a finite field

[CRZ18] Jean-Sébastien Coron, Franck Rondepierre, and Rina Zeitoun. High order masking of look-up tables with common shares. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018(1):40–72, 2018.

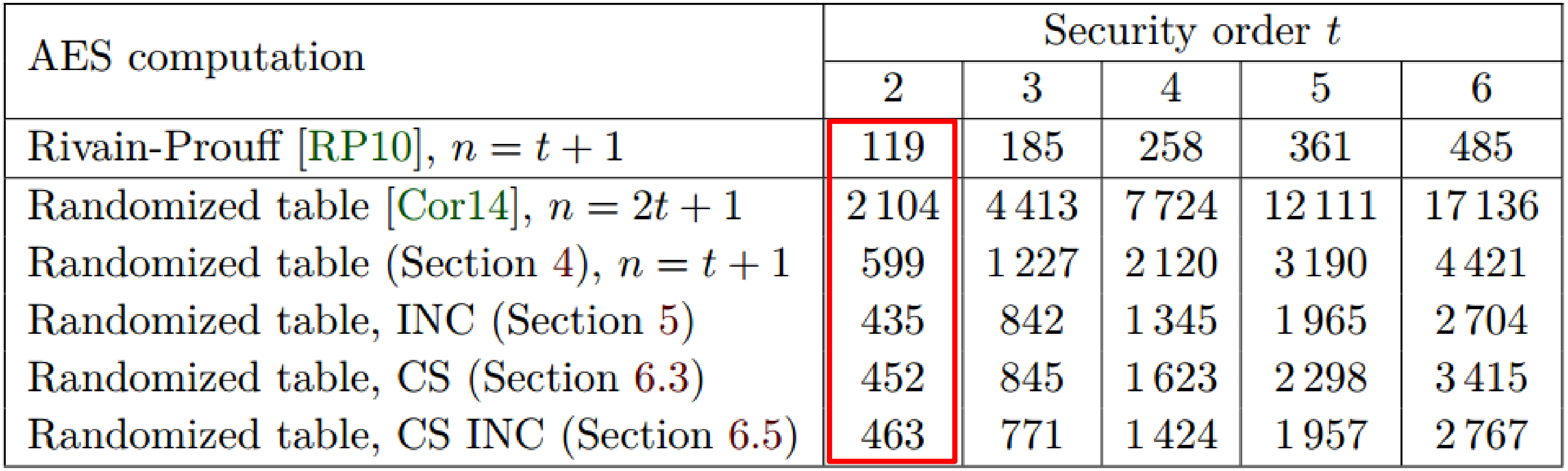
[RP10] Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of AES. In Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings, pages 413–427, 2010.

Introduction and Previous Work

Masked Implementation for SBox

Computation based implementation is more efficient

- Running time in thousands of clock cycles of protected implementations of AES. The implementation was done in C on an iMac running a 3.2 GHz Intel processor [CRZ18]



AES computation	Security order t				
	2	3	4	5	6
Rivain-Prouff [RP10], $n = t + 1$	119	185	258	361	485
Randomized table [Cor14], $n = 2t + 1$	2 104	4 413	7 724	12 111	17 136
Randomized table (Section 4), $n = t + 1$	599	1 227	2 120	3 190	4 421
Randomized table, INC (Section 5)	435	842	1 345	1 965	2 704
Randomized table, CS (Section 6.3)	452	845	1 623	2 298	3 415
Randomized table, CS INC (Section 6.5)	463	771	1 424	1 957	2 767

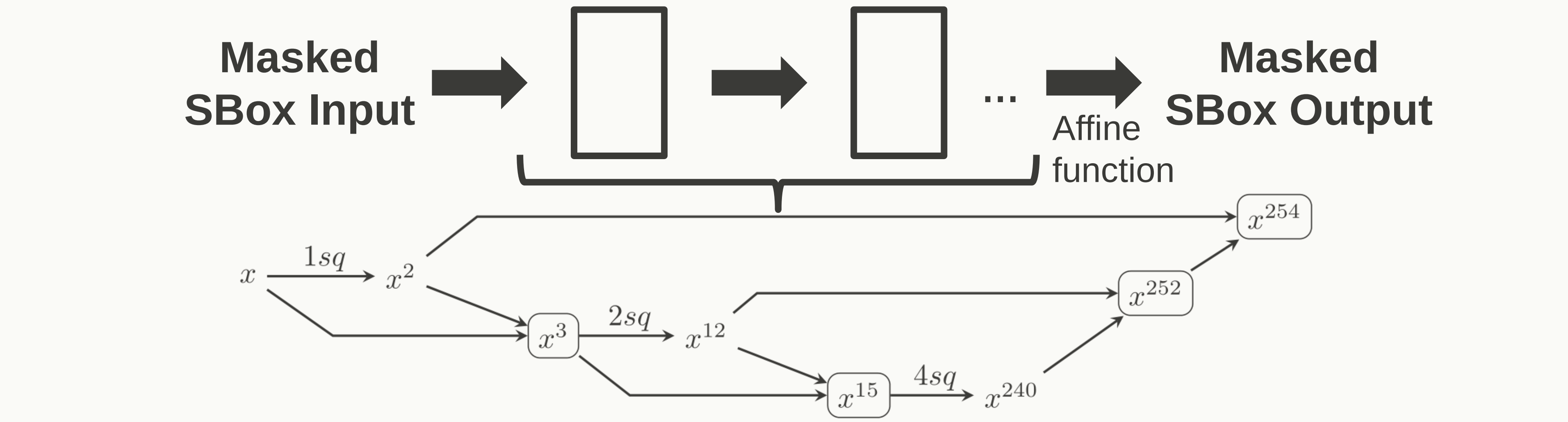
[CRZ18] Jean-Sébastien Coron, Franck Rondepierre, and Rina Zeitoun. High order masking of look-up tables with common shares. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018(1):40–72, 2018.

[RP10] Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of AES. In Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings, pages 413–427, 2010.

Introduction and Previous Work

Addition Chain based Masked Implementation

Core idea: The SBox is expressed as a sequence of squares and multiplications over a finite field. These non-linear multiplications can be then implemented using previously known schemes, such as ISW.



Masked SBox Input

…

Affine function

Masked SBox Output

e.g., one of the most popular addition chain for AES SBox

[ISW03] Yuval Ishai, Amit Sahai, and David A. Wagner. Private circuits: Securing hardware against probing attacks. In Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, pages 463–481, 2003.

[CGP+12] Claude Carlet, Louis Goubin, Emmanuel Prouff, Michaël Quisquater, and Matthieu Rivain. Higher-order masking schemes for s-boxes. In Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers, pages 366–384, 2012.

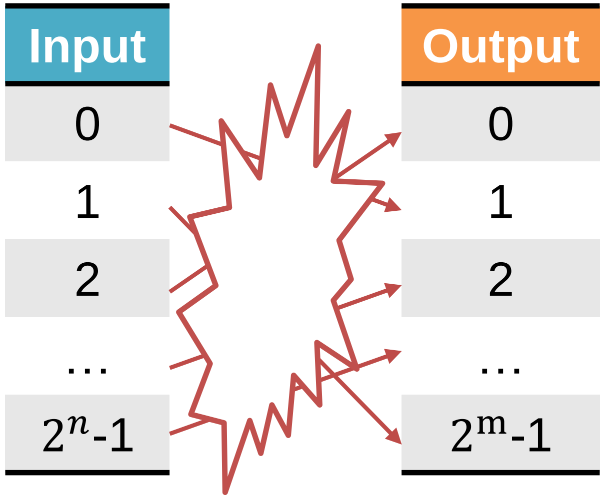
Introduction and Previous Work

Weakness of Addition Chain based Masked Implementation

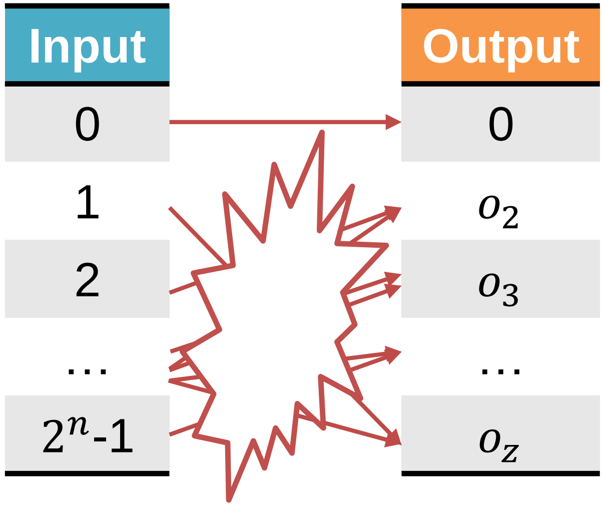
Most studies focus on the analyses on final SBox outputs

- What if the computations of some intermediate monomials leak more?

  (especially some unbalanced monomials)



Balanced (n,m)-function
(SBox is usually balanced)



Unbalanced exponent
over a finite field

Introduction and Previous Work

Weakness of Addition Chain based Masked Implementation

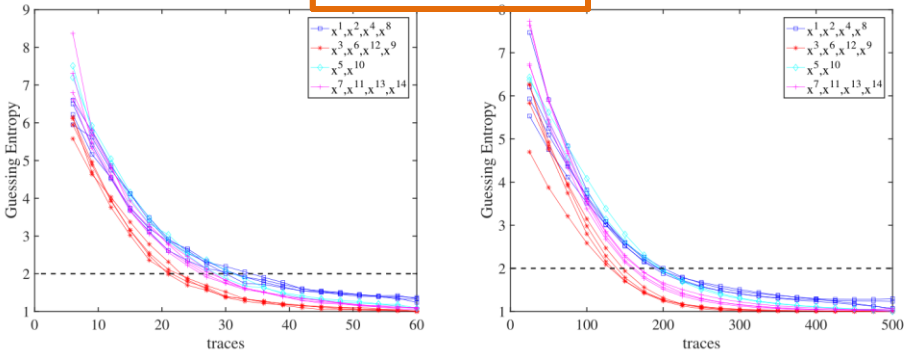
An example: 4-bit case

Simulated Higher-order attack

- Leakages of each share are under HW model
- The combined leakages are obtained by normalized product

Results are divided into 4 groups

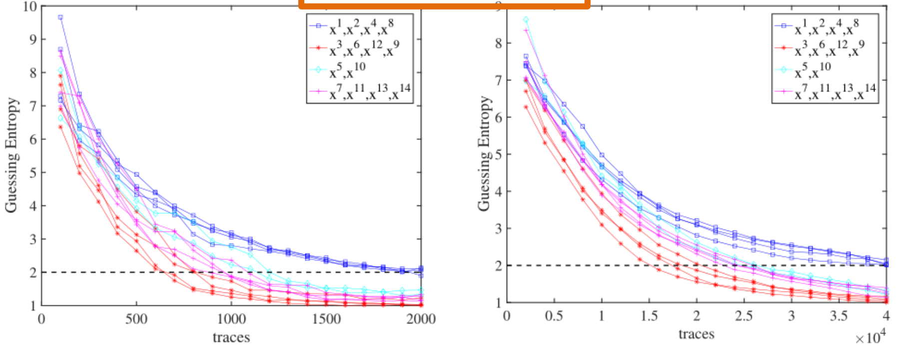
Low noise



(a) $d = 1$ (b) $d = 2$

Figure 2: The results of GE for $n = 4$ and $\sigma = 0.1$.

High noise



(a) $d = 1$ (b) $d = 2$

Figure 16: The results of GE for $n = 4$ and $\sigma = 2$.

Outline

1. Introduction and Previous Work
2. Resistance Measurement
3. Practical Experiments
4. Conclusion

Resistance Measurement

Related Work

Transparency order [Pro05] and its variants [CSM+17, LZM+20]

- The mathematical properties of the SBox
- Quantify the basic Differential Power Analysis (DPA) resilience

The distinguisher of DPA on *j*-th bit [KJJ99]

$$\Delta(j) = \mathbb{E}[\mathcal{L}|SBox_j = 1] - \mathbb{E}[\mathcal{L}|SBox_j = 0]$$

The expectation leakage when the *j*-th bit of *SBox* output is 1

The expectation leakage when the *j*-th bit of *SBox* output is 0

[KJJ99] P. C. Kocher, J. Jaffe, B. Jun. Differential Power Analysis. CRYPTO 1999, pp: 388-397, 1999.

[Pro05] Emmanuel Prouff. DPA attacks and s-boxes. In Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers, pages 424–441, 2005.

Resistance Measurement

Related Work

Differential Power Analysis (DPA)

- Leakages are assumed to follow Hamming weight model
- Analysis with N traces and plaintexts T
- $\dot{K}$ is the correct key while K is a key hypothesis

$$\Delta_{K,\dot{K}}(T,j) = \frac{\sum_{i=1}^{N} SBox_j(T_i \oplus K) \cdot HW[SBox(T_i, \dot{K})]}{\sum_{i=1}^{N} SBox_j(T_i \oplus K)} - \frac{\sum_{i=1}^{N} [1 - SBox_j(T_i \oplus K)] \cdot HW[SBox(T_i, \dot{K})]}{\sum_{i=1}^{N} [1 - SBox_j(T_i \oplus K)]}$$

[KJJ99] P. C. Kocher, J. Jaffe, B. Jun. Differential Power Analysis. CRYPTO 1999, pp: 388-397, 1999.

[Pro05] Emmanuel Prouff. DPA attacks and s-boxes. In Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers, pages 424–441, 2005.

Resistance Measurement

Related Work

Differential Power Analysis (DPA)

- Leakages are assumed to follow Hamming weight model
- Analysis with N traces and plaintexts T
- $\dot{K}$ is the correct key while K is a key hypothesis

$$\Delta_{K,\dot{K}}(T,j)=\frac{\sum_{i=1}^{N} SBox_j(T_i \oplus K)\cdot HW[SBox(T_i,\dot{K})]}{\sum_{i=1}^{N} \boxed{SBox}_j(T_i \oplus K)}-\frac{\sum_{i=1}^{N}[1-SBox_j(T_i \oplus K)]\cdot HW[SBox(T_i,\dot{K})]}{\sum_{i=1}^{N}[1-\boxed{SBox}_j(T_i \oplus K)]}$$

If it is replaced by an unbalanced function, the denominator might be ZERO

[KJJ99] P. C. Kocher, J. Jaffe, B. Jun. Differential Power Analysis. CRYPTO 1999, pp: 388-397, 1999.

[Pro05] Emmanuel Prouff. DPA attacks and s-boxes. In Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers, pages 424–441, 2005.

Resistance Measurement

New Notion: Polygon Degree

Revisited resistance measurement for a function F

- f_j is the j-th bit of F
- If $f_j \equiv 0 \; or \; 1$, it useless for distinguishing the secret key

So we have

$$\Delta_{K,\dot{K}}(F,T,j) = \begin{cases} 0, & \text{if } f_j \equiv 0 \text{ or } f_j \equiv 1 \\ \dfrac{\sum_{i=1}^{N} f_j(T_i \oplus K) \cdot HW[F(T_i \oplus \dot{K})]}{\sum_{i=1}^{N} f_j(T_i \oplus K)} - \dfrac{\sum_{i=1}^{N} [1 - f_j(T_i \oplus K)] \cdot HW[F(T_i \oplus \dot{K})]}{\sum_{i=1}^{N} [1 - f_j(T_i \oplus K)]}, & \text{otherwise} \end{cases}$$

Resistance Measurement

New Notion: Polygon Degree

- The equation can be derived as follows

$$\delta_\alpha(F,j) = \begin{cases} 0, & \text{if } f_j \equiv 0 \text{ or } f_j \equiv 1 \\ \dfrac{\sum_{i=0}^{2^n-1} f_j(i\oplus\alpha)\cdot HW[F(i)]}{m\sum_{i=0}^{2^n-1} f_j(i\oplus\alpha)} - \dfrac{\sum_{i=0}^{2^n-1}[1-f_j(i\oplus\alpha)]\cdot HW[F(i)]}{m\sum_{i=0}^{2^n-1}[1-f_j(i\oplus\alpha)]}, & \text{otherwise} \end{cases}$$

- We denote $\delta_\alpha(F)$ as the sum of $\delta_\alpha(F,j)$, then we introduce a new notion,

Definition 1 (Polygon Degree). *Let F denote a (n,m)-function, the polygon degree of F, denoted by $PD(F)$, is defined by:*

$$PD(F) = \frac{1}{2^n}\sum_{\alpha\in\mathbb{F}_{2^n}} \left(|\delta_0(F)| - |\delta_\alpha(F)|\right).$$

Resistance Measurement

New Notion: Polygon Degree

Three properties of polygon degree

- The smaller the PD of a function, the stronger it resists against SCAs
- For a function F, we have $0 \leq PD(F) < 1$
- PD is also valid in higher-order attacks (Thanks to Lemma 1)

Combined higher-order leakage: $\mathcal{C}_d(x) = \prod_{i=0}^{d}[\mathcal{L}(x_i) - \mathbb{E}(\mathcal{L}(x_i)]$

Then we have [RPD09] : $\mathbb{E}[\mathcal{C}_d(x)] = (-\frac{1}{2})^d(HW(x) - \frac{n}{2})$

[RPD09] Matthieu Rivain, Emmanuel Prouff, and Julien Doget. Higher-order masking and shuffling for software implementations of block ciphers. In Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings, pages 171–188, 2009.

Resistance Measurement

Soundness of Polygon Degree

How to verify the soundness of PD

1. Calculate the PD values of all exponents over a finite field

$$PD(F), \quad F(x) = x^{e} \quad over \quad \mathbb{F}_{2^n}$$

2. Perform higher-order CPA [PRB09] in simulation

Leakages are under HW model: $\mathcal{L}_i(x_i) = HW(x_i) + \mathcal{N}_i$

3. Match the PD values and simulated attack results

[RPD09] Matthieu Rivain, Emmanuel Prouff, and Julien Doget. Higher-order masking and shuffling for software implementations of block ciphers. In Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings, pages 171–188, 2009.

[PRB09] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan. Statistical analysis of second order differential power analysis. IEEE Trans. Computers, 58(6):799–811, 2009.

Resistance Measurement

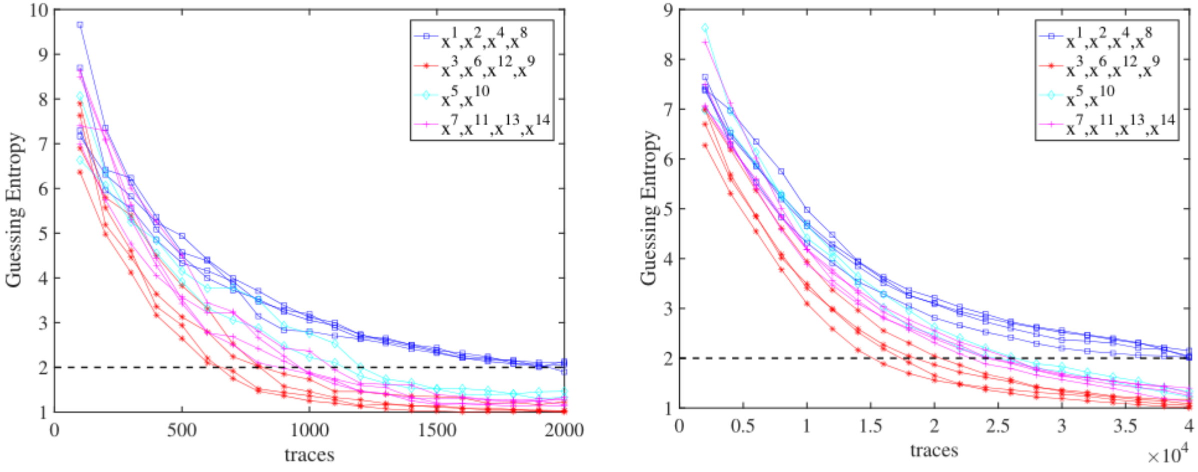
Soundness of Polygon Degree

Verification of the soundness of PD on 4-bit cases

Table 1. The PD of different exponents for $n = 4$.

$n = 4$			
classes	PD	classes	PD
x, x^2, x^4, x^8	0.1563	x^3, x^6, x^9, x^{12}	0.2984
x^5, x^{10}	0.1641	$x^7, x^{11}, x^{13}, x^{14}$	0.1836

Resistance: C3 🟥 < C7 🟪 < C5 🟦 < C1 🟦



(a) $d = 1$ (b) $d = 2$

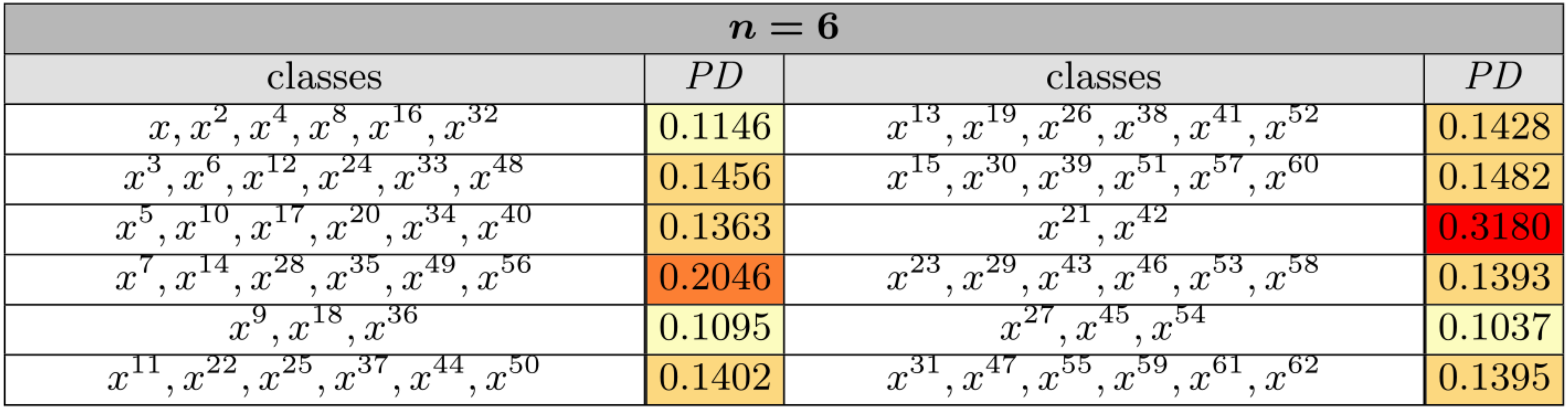
Figure 16: The results of GE for $n = 4$ and $\sigma = 2$.

Resistance Measurement

Soundness of Polygon Degree

Verification of the soundness of PD on 6-bit cases

Table 2. The PD of different cyclotomic classes for $n = 6$.



$n = 6$			
classes	PD	classes	PD
$x, x^2, x^4, x^8, x^{16}, x^{32}$	0.1146	$x^{13}, x^{19}, x^{26}, x^{38}, x^{41}, x^{52}$	0.1428
$x^3, x^6, x^{12}, x^{24}, x^{33}, x^{48}$	0.1456	$x^{15}, x^{30}, x^{39}, x^{51}, x^{57}, x^{60}$	0.1482
$x^5, x^{10}, x^{17}, x^{20}, x^{34}, x^{40}$	0.1363	x^{21}, x^{42}	0.3180
$x^7, x^{14}, x^{28}, x^{35}, x^{49}, x^{56}$	0.2046	$x^{23}, x^{29}, x^{43}, x^{46}, x^{53}, x^{58}$	0.1393
x^9, x^{18}, x^{36}	0.1095	x^{27}, x^{45}, x^{54}	0.1037
$x^{11}, x^{22}, x^{25}, x^{37}, x^{44}, x^{50}$	0.1402	$x^{31}, x^{47}, x^{55}, x^{59}, x^{61}, x^{62}$	0.1395

The powers x^a and x^b fall into a same PD value if a and b lie in a same cyclotomic class [CGP+12], namely $a = 2^i b$.

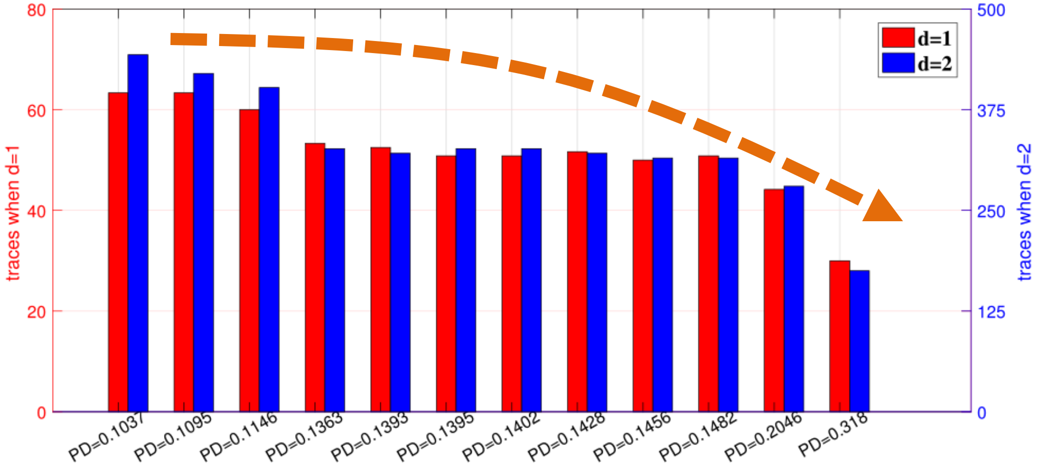
[CGP+12] Claude Carlet, Louis Goubin, Emmanuel Prouff, Michaël Quisquater, and Matthieu Rivain. Higher-order masking schemes for s-boxes. In Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers, pages 366–384, 2012.

Resistance Measurement

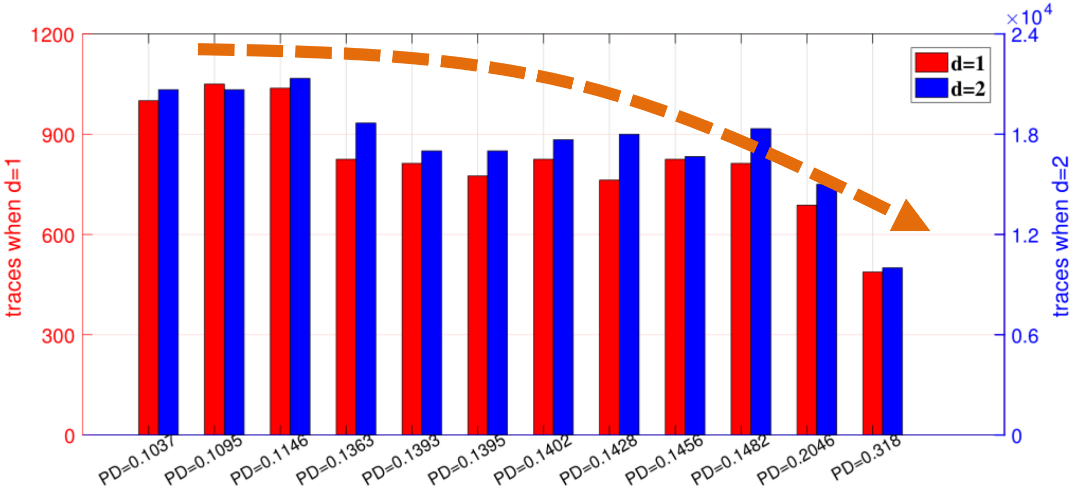
Soundness of Polygon Degree

Verification of the soundness of PD on 6-bit cases

Low noise
(σ=0.1)



High noise
(σ=2)



Resistance Measurement

Soundness of Polygon Degree

Verification of the soundness of PD on 8-bit cases

- We use inverse functions $Num = a / PD + b$ to fit the results.

Low noise
(σ=0.1)

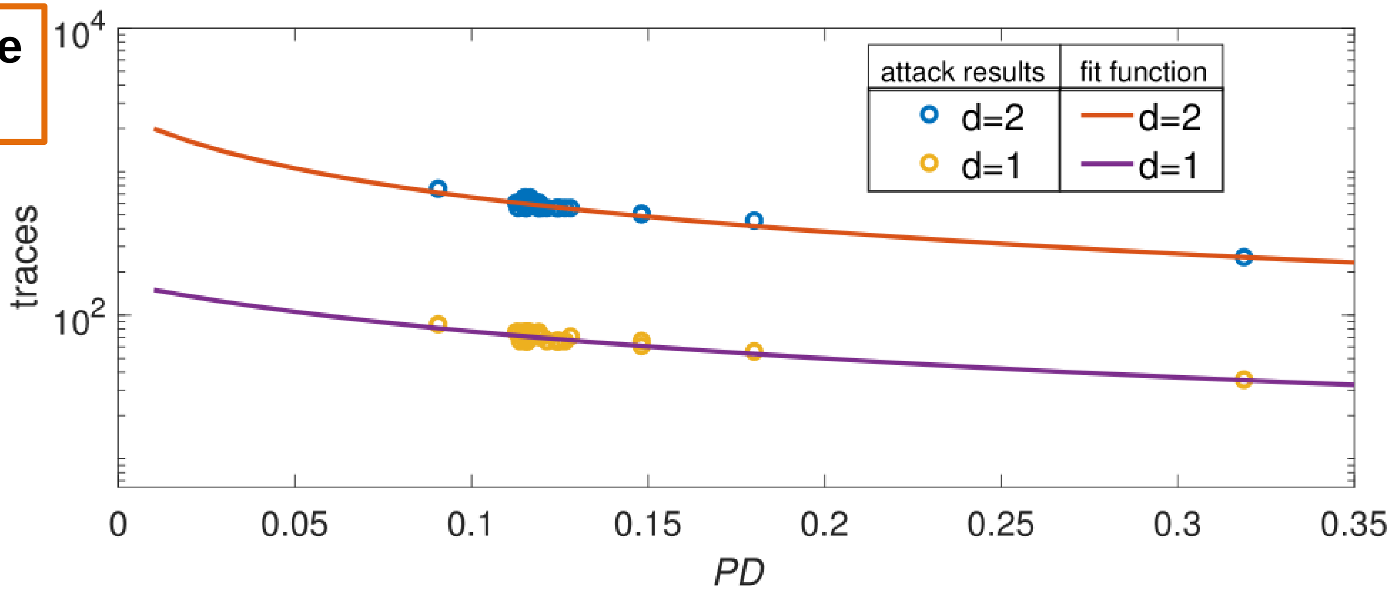


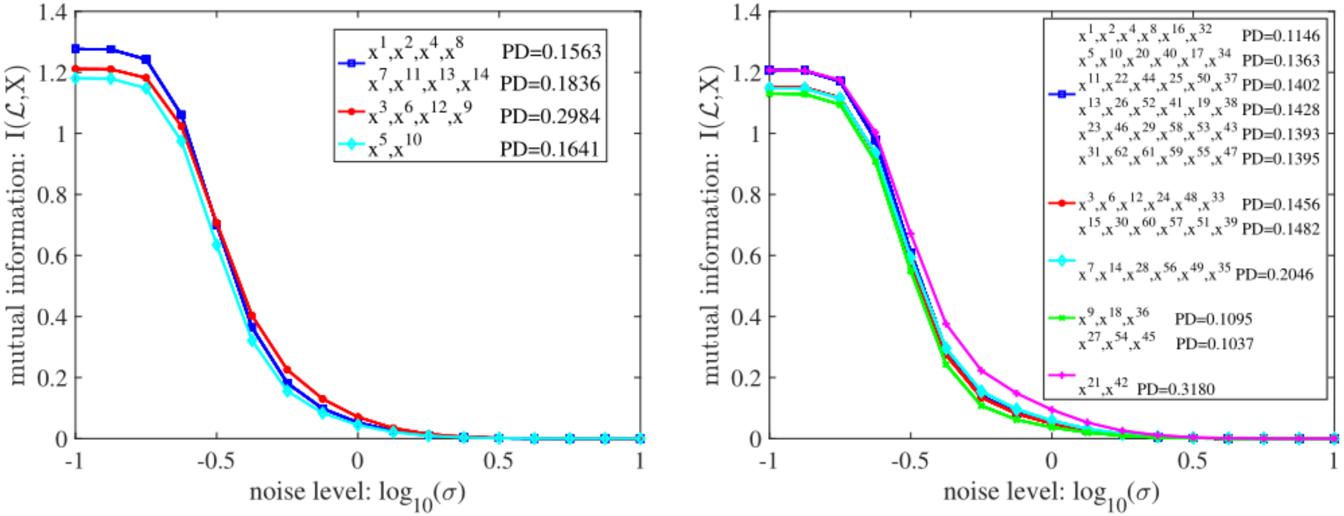
Figure 4: Number of traces for the GE to be below 10 (in y-axis) versus the different PD (in x-axis) for $n = 8$ and $\sigma = 0.1$.

Resistance Measurement

Information-Theoretic Evaluation

Mutual information (MI), as a well-known Information-Theoretic metric [CS19]

- Let $\mathcal{L} = (\mathcal{L}_0, \ldots, \mathcal{L}_d)$ be the multivariate leakage, then I denotes the MI.



(a) $n = 4$

(b) $n = 6$

Figure 5: Mutual information of monomial functions for $d = 1$.

1. The monomial with the same output size fall into a same class
2. MI metric does not match the results well as the PD does

[CS19] Gaëtan Cassiers and François-Xavier Standaert. Towards globally optimized masking: From low randomness to low noise rate or probe isolating multiplications with reduced randomness and security against horizontal attacks. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2019(2):162–198, 2019.

Outline

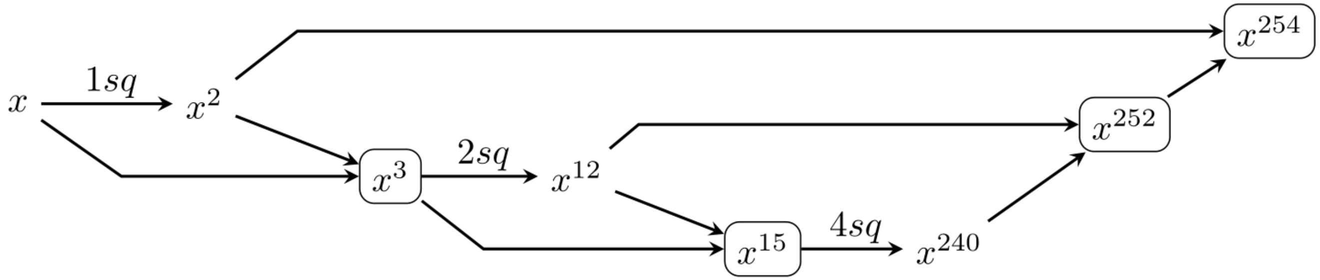
1. Introduction and Previous Work
2. Resistance Measurement
3. Practical Experiments
4. Conclusion

Practical Experiments

Application of Polygon Degree in Addition Chain

AES SBox as a study case

- One of the most popular block cipher
- Simple expression over the finite field



- Many public masked implementations

[CRZ18] Jean-Sébastien Coron, Franck Rondepierre, and Rina Zeitoun. High order masking of look-up tables with common shares. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018(1):40–72, 2018.

Practical Experiments

Application of Polygon Degree in Addition Chain

How to find all feasible and the most efficient addition chains?

(4 multiplications and 7 squares are the most efficient for AES SBox)

Step.1 Find the addition chains including 4 multiplications

Exponential set {1, 2, 4,…, 128}

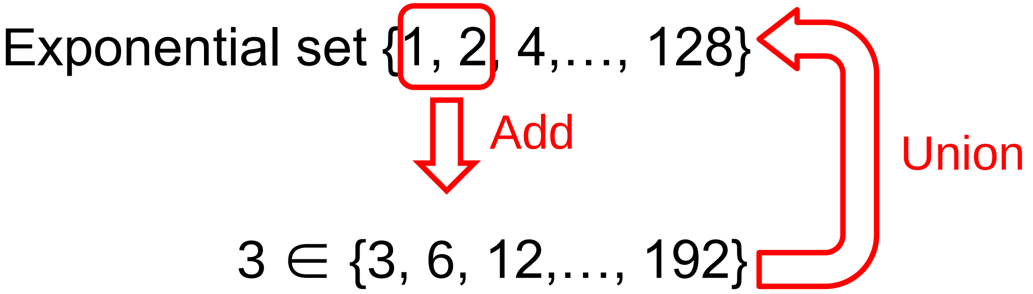
Practical Experiments

Application of Polygon Degree in Addition Chain

How to find all feasible and the most efficient addition chains?

(4 multiplications and 7 squares are the most efficient for AES SBox)

Step.1 Find the addition chains including 4 multiplications



Exponential set $\{\boxed{1, 2}, 4, \ldots, 128\}$

$3 \in \{3, 6, 12, \ldots, 192\}$

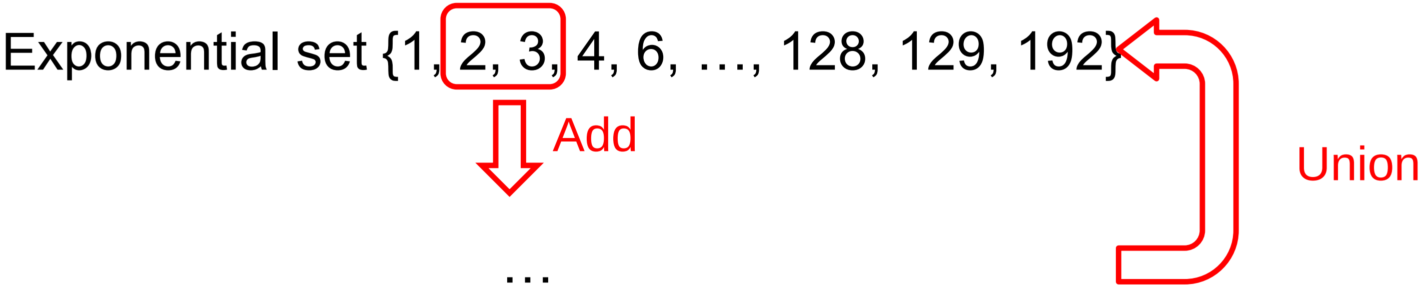
Practical Experiments

Application of Polygon Degree in Addition Chain

How to find all feasible and the most efficient addition chains?

(4 multiplications and 7 squares are the most efficient for AES SBox)

Step.1 Find the addition chains including 4 multiplications



Exponential set {1, 2, 3, 4, 6, …, 128, 129, 192}

Add

Union

…

After 4 additions, does 254 belongs to the final exponential set?

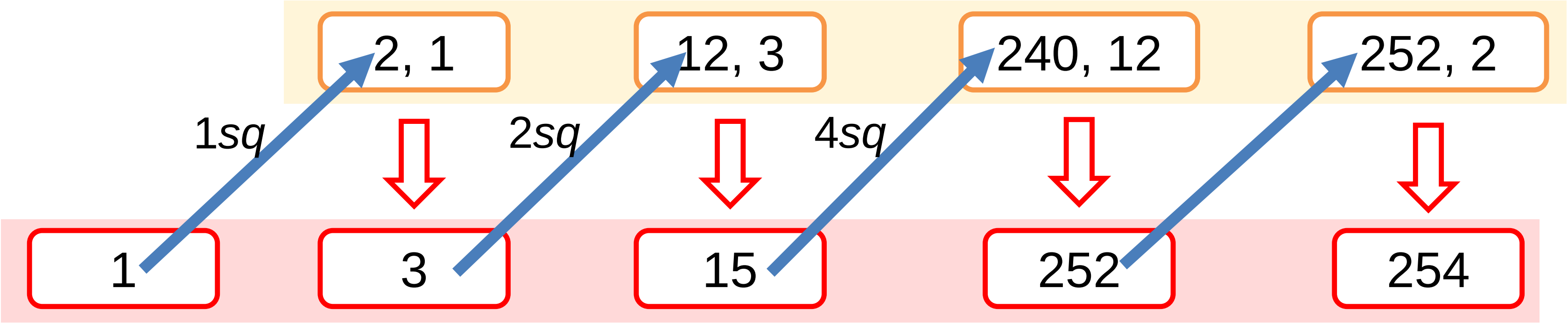
Practical Experiments

Application of Polygon Degree in Addition Chain

How to find all feasible and the most efficient addition chains?

(4 multiplications and 7 squares are the most efficient)

Step.2 Count the number of squares in these addition chains



Sum the square number from red to orange in each cyclotomic class, we get 1,330 addition chains with 7 squares (none with lower square number)

Practical Experiments

Application of Polygon Degree in Addition Chain

Two instantiated adversaries

- $\mathcal{A}_1$ has limited computational resources, so he is only able to find leakages corresponding to one sensitive intermediate.

  Measurement: Max$[PD(F)]$

- $\mathcal{A}_2$ has enough computational resources. So he is able to launch higher-order attacks on all sensitive intermediates, then sums the results together to achieve a higher success rate.

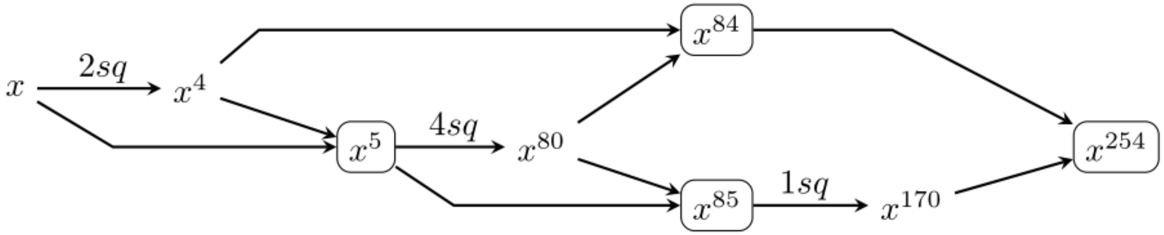
  Measurement: $\sum[PD(F)]$

Practical Experiments

Application of Polygon Degree in Addition Chain

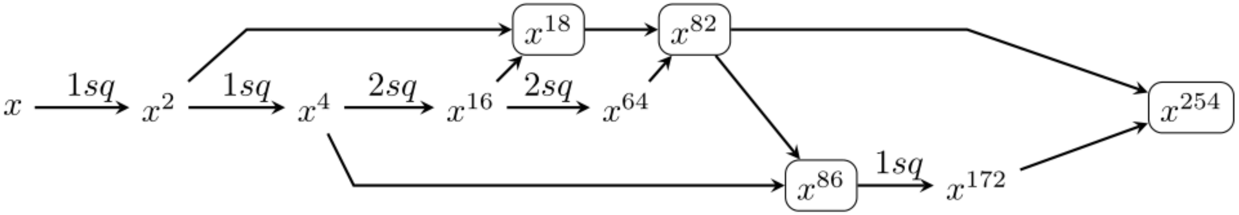
Three typical addition chains

Weakest



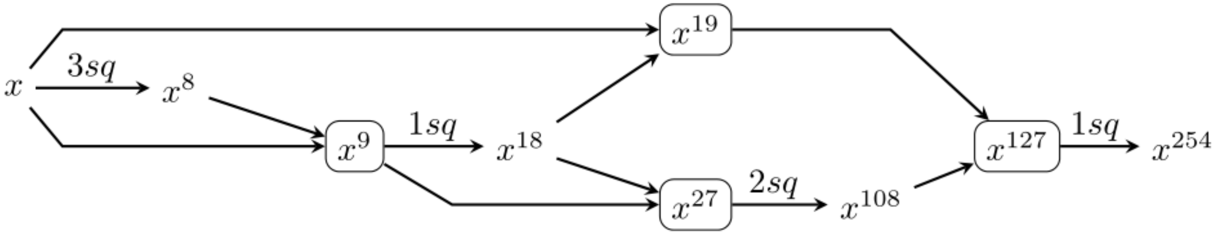
(a) One of the weakest addition chains $\mathcal{F}_c$ for x^{254} against both $\mathcal{A}_1$ and $\mathcal{A}_2$

Strongest



(b) One of the strongest addition chains $\mathcal{F}_b$ for x^{254} against both $\mathcal{A}_1$ and $\mathcal{A}_2$

Strong and Parallelizable

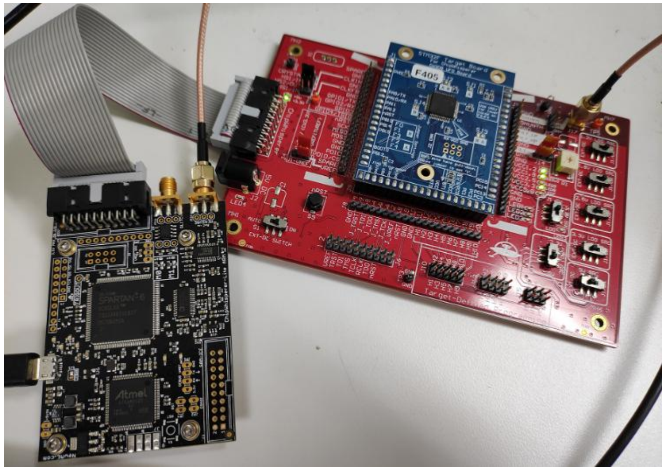


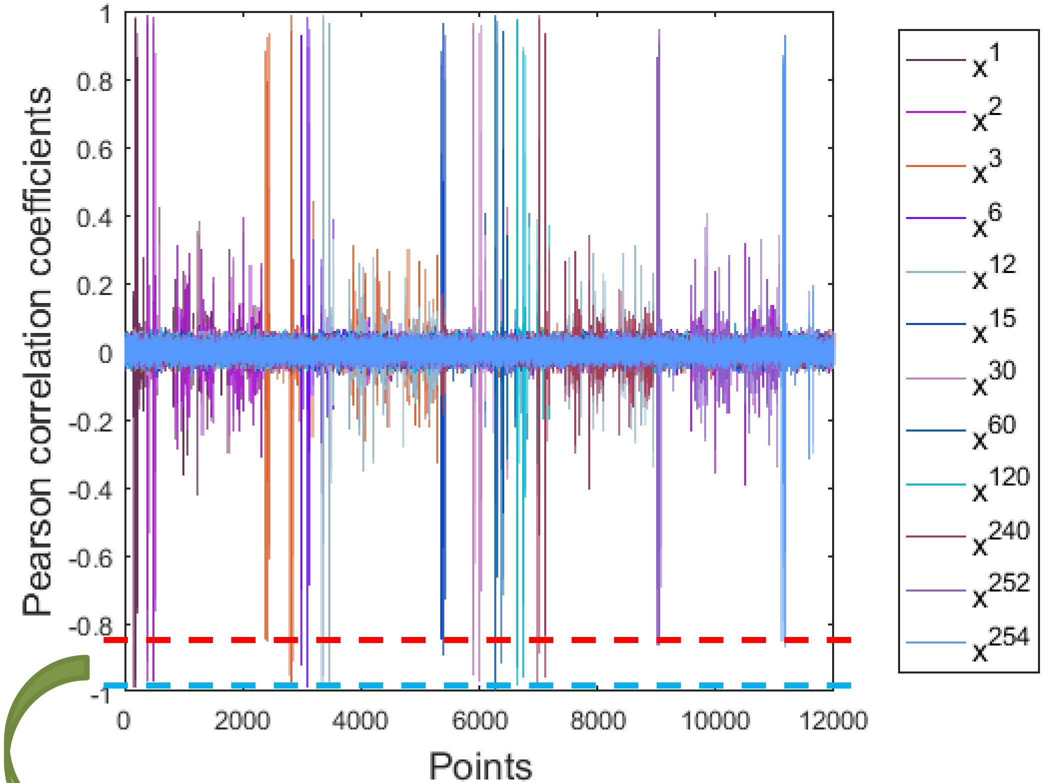
(c) One recommended computation $\mathcal{F}_c$ for x^{254} ($x^{18} \cdot x$ and $x^{18} \cdot x^9$ can be proceeded in parallel [CGPZ16])

Practical Experiments

Experiment Setup

Power traces





- ChipWhisperer-Lite board
- 32-bit ARM Cortex-M4 CPU
- Low noise scenario

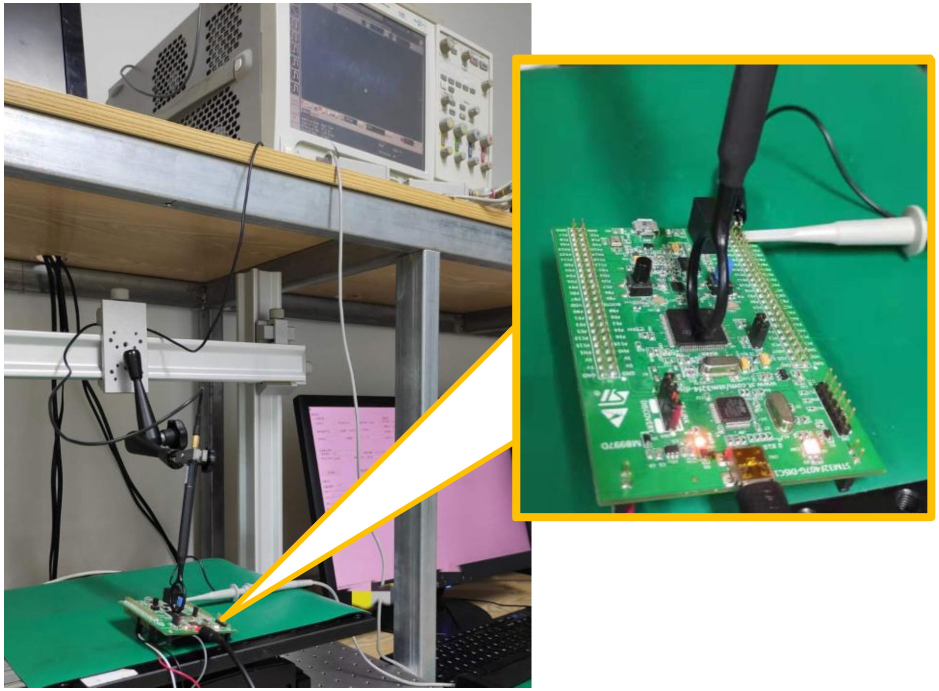
Noise level for monomials are different

[CRZ18] Jean-Sébastien Coron, Franck Rondepierre, and Rina Zeitoun. High order masking of look-up tables with common shares. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018(1):40–72, 2018.

Practical Experiments

Experiment Setup

EM traces



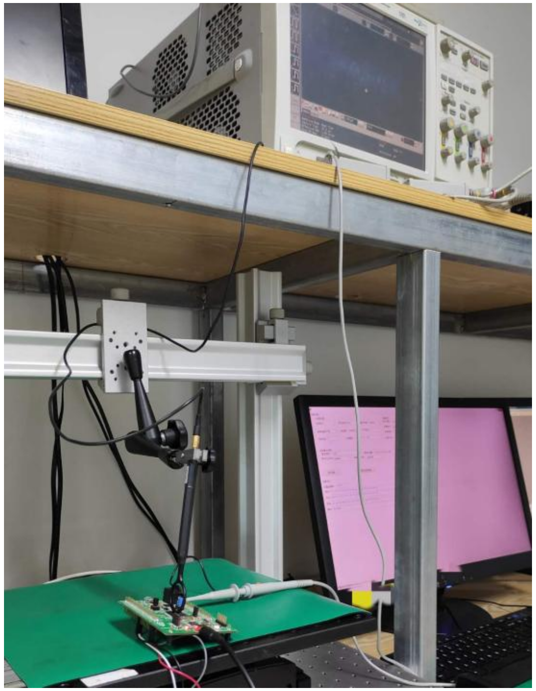
- Agilent DSO90404A Oscilloscope
- EM near field probe
- 32-bit ARM Cortex-M4 CPU
- High noise scenario

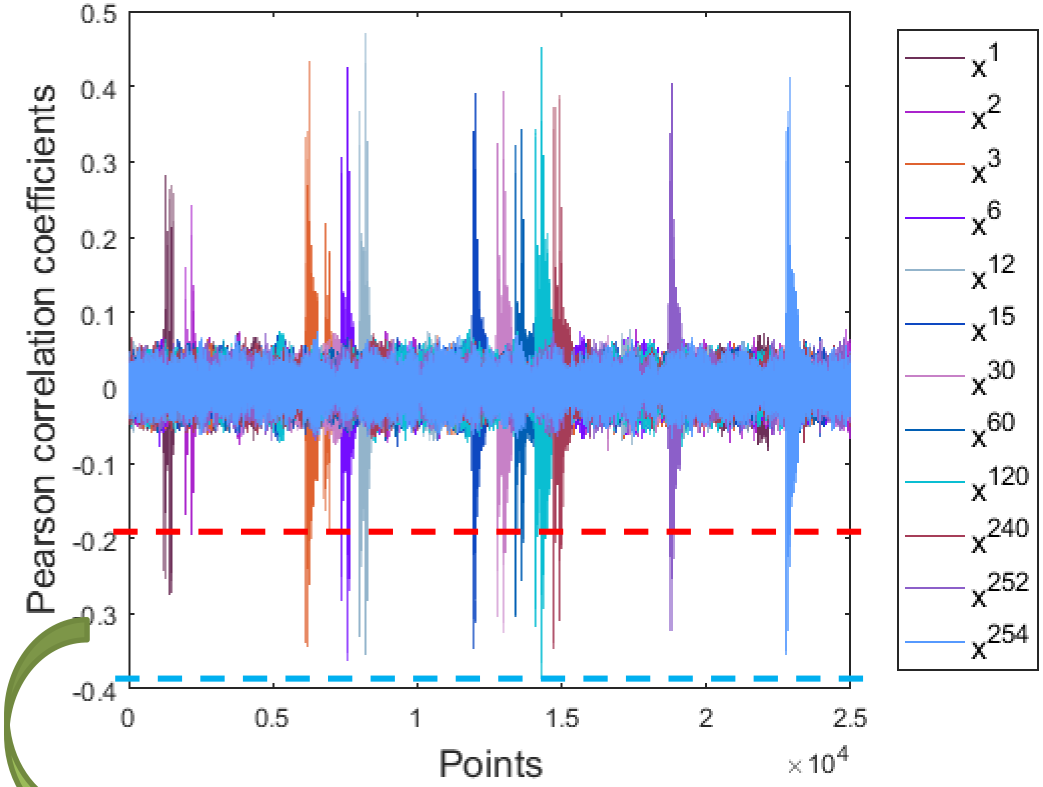
[CRZ18] Jean-Sébastien Coron, Franck Rondepierre, and Rina Zeitoun. High order masking of look-up tables with common shares. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018(1):40–72, 2018.

Practical Experiments

Experiment Setup

EM traces





Difference gets more obvious

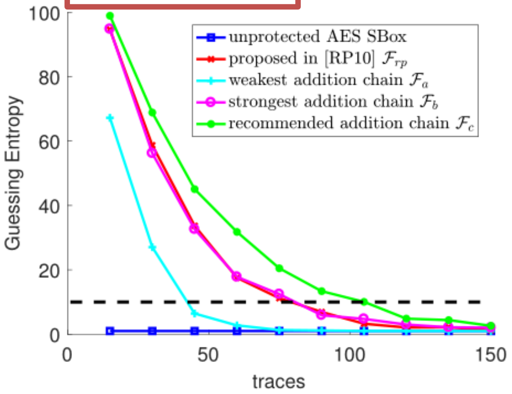
Practical Experiments

Experimental Results

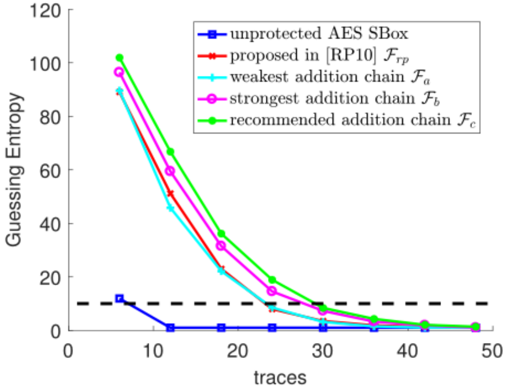
Power analysis

- Broken within a small amount of traces
- Two strong addition chains are better than others
- In the worst case, its resistance is closed to that of unprotected AES SBox

Two shares

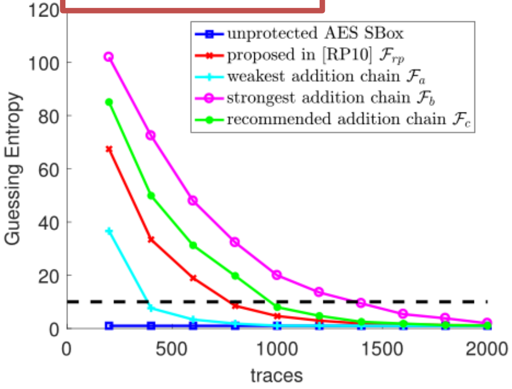


(a) Guessing entropy for $\mathcal{A}_1$

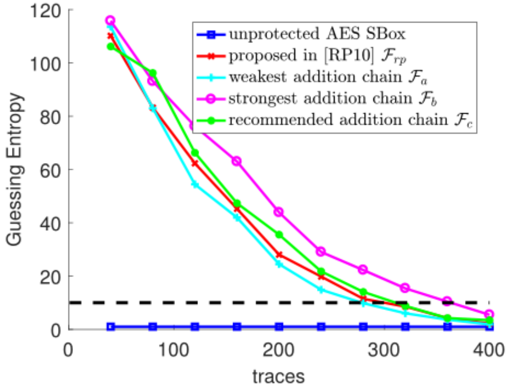


(b) Guessing entropy for $\mathcal{A}_2$

Three shares



(a) Guessing entropy for $\mathcal{A}_1$



(b) Guessing entropy for $\mathcal{A}_2$

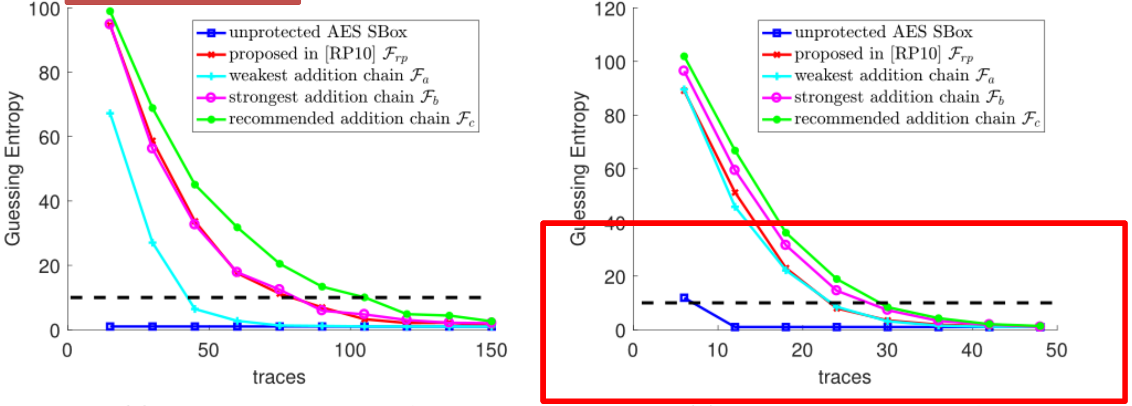
Practical Experiments

Experimental Results

Power analysis

- Broken within a small amount of traces
- Two strong addition chains are better than others
- In the worst case, its resistance is closed to that of unprotected AES SBox

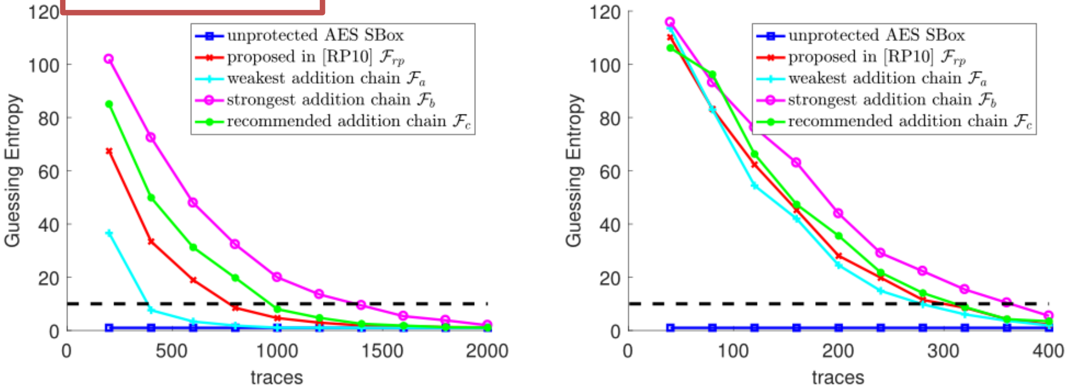
Two shares



(a) Guessing entropy for $\mathcal{A}_1$

(b) Guessing entropy for $\mathcal{A}_2$

Three shares



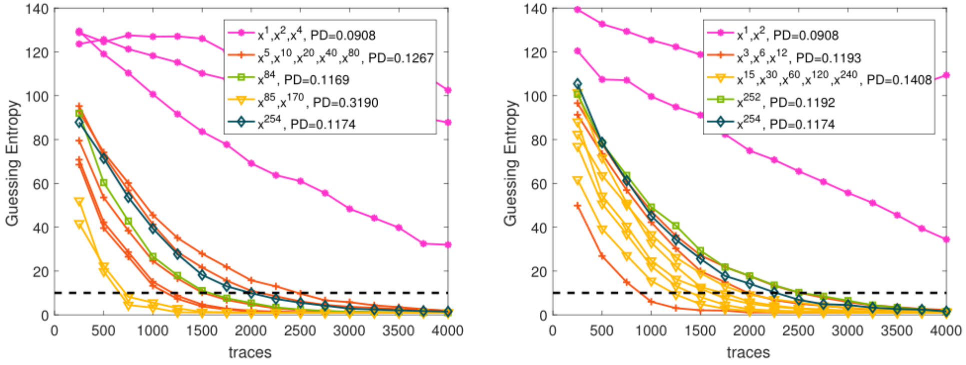
(a) Guessing entropy for $\mathcal{A}_1$

(b) Guessing entropy for $\mathcal{A}_2$

Practical Experiments

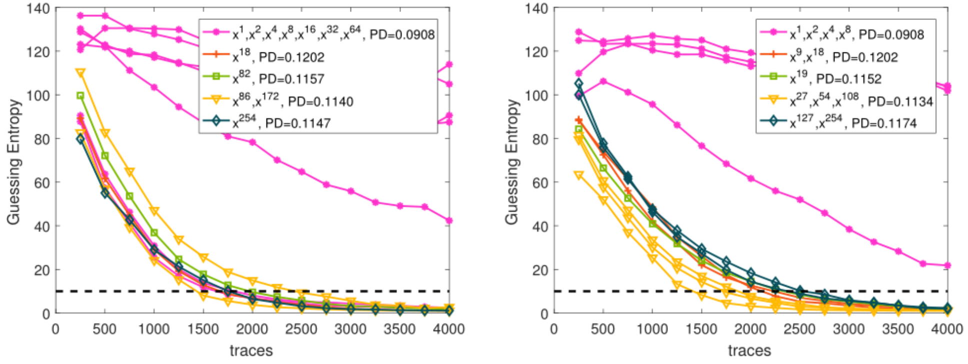
Experimental Results

EM analysis



(a) The addition chain $\mathcal{F}_a$ with the weakest resistance

(b) The addition chain proposed in [RP10] $\mathcal{F}_{rp}$



(c) The addition chain $\mathcal{F}_b$ with the strongest resistance

(d) The addition chain $\mathcal{F}_c$ with strong resistance and parallel feasibility

Adversary $\mathcal{A}_1$

Two shares

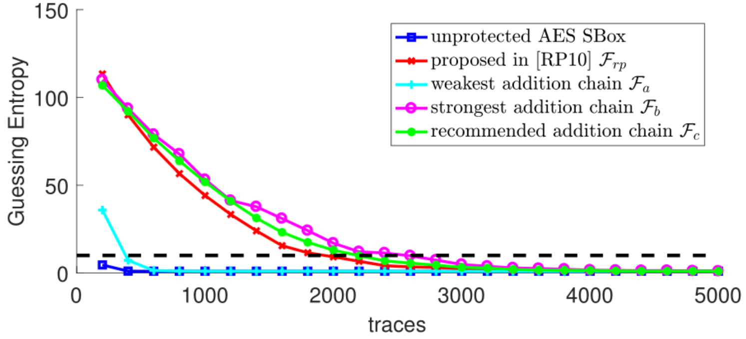


Figure 11: The combined results of second-order CEMA on four typical masked addition chain implementations.

Adversary $\mathcal{A}_2$

Practical Experiments

Experimental Results

EM analysis

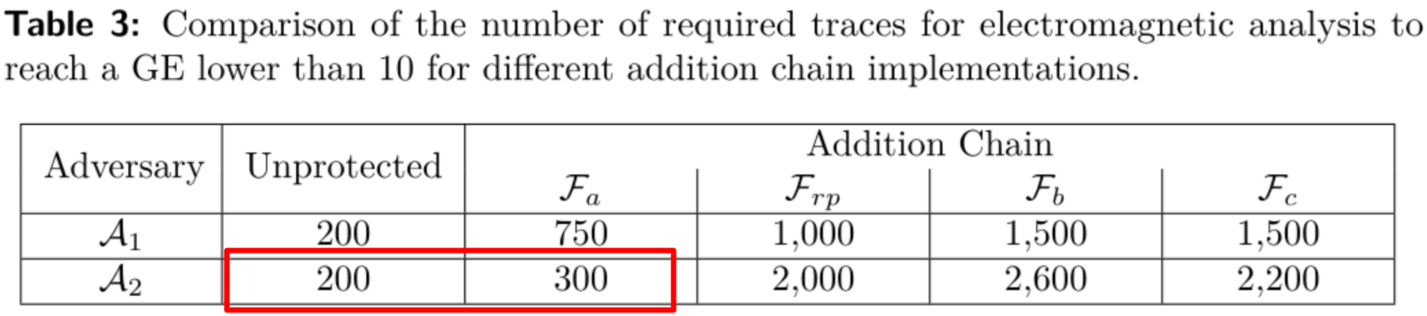


Table 3: Comparison of the number of required traces for electromagnetic analysis to reach a GE lower than 10 for different addition chain implementations.

Adversary	Unprotected	Addition Chain			
		$\mathcal{F}_a$	$\mathcal{F}_{rp}$	$\mathcal{F}_b$	$\mathcal{F}_c$
$\mathcal{A}_1$	200	750	1,000	1,500	1,500
$\mathcal{A}_2$	200	300	2,000	2,600	2,200

In the worst case, its resistance is also closed to that of **unprotected implementation**

Practical Experiments

Experimental Results

EM analysis

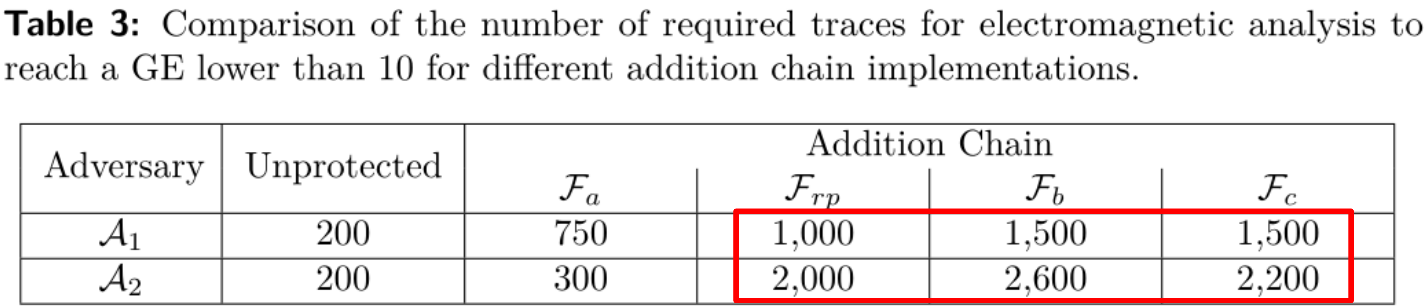


Table 3: Comparison of the number of required traces for electromagnetic analysis to reach a GE lower than 10 for different addition chain implementations.

Adversary	Unprotected	Addition Chain			
		$\mathcal{F}_a$	$\mathcal{F}_{rp}$	$\mathcal{F}_b$	$\mathcal{F}_c$
$\mathcal{A}_1$	200	750	1,000	1,500	1,500
$\mathcal{A}_2$	200	300	2,000	2,600	2,200

The inefficient results on some monomials (e.g., x) are combined and negatively affect the final attack result

Practical Experiments

Experimental Results

Profiled Attack

☐ Template attack

1. Get the probability $P(X_i^j = x_i^j|\boldsymbol{\mathcal{L}_i^j}, \boldsymbol{M_i})$ utilizing profiled templates

2. Get the probability $P(x^j|\boldsymbol{\mathcal{L}^j}, \boldsymbol{M}) = \sum_{\mathcal{S}} \prod_{i=0}^{d} P(x_i^j|\boldsymbol{\mathcal{L}_i^j}, \boldsymbol{M_i})$ for each trace

☐ Deep learning based attack

1. Train using a CNN model

2. Last fully-connected layer contains $|F|$ neurons

[CK13] Omar Choudary and Markus G. Kuhn. Efficient template attacks. In Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers, pages 253–270, 2013.

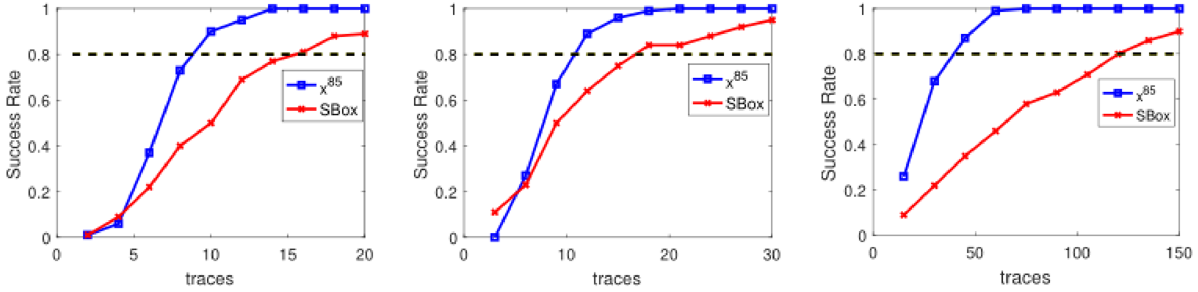
[CDP17] Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff. Convolutional neural networks with data augmentation against jitter-based countermeasures - profiling attacks without pre-processing. In Wieland Fischer and Naofumi Homma, editors, Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, volume 10529 of Lecture Notes in Computer Science, pages 45–68. Springer, 2017.

Practical Experiments

Experimental Results

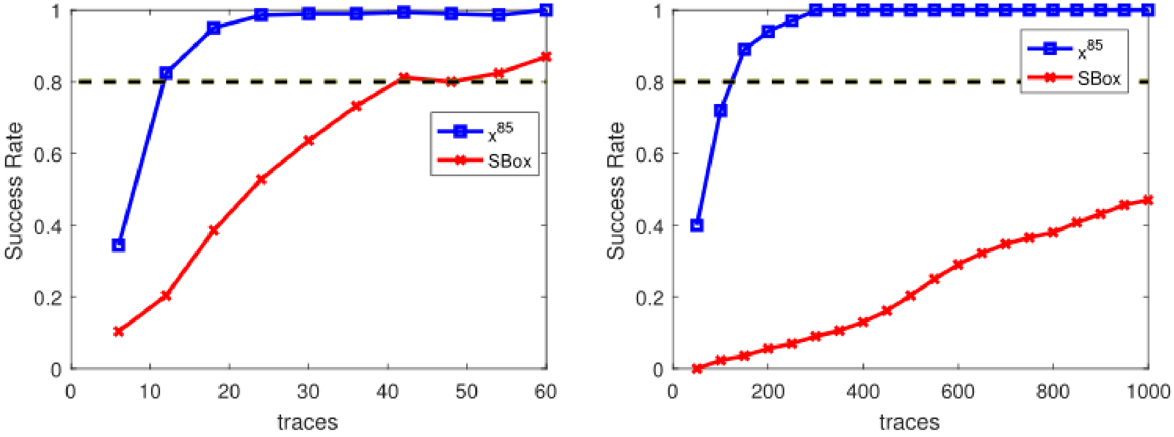
Template Attack

- With increasing noise, attacks on x^{85} become more efficient
- Since the smaller size of $F(x) = x^{85}$, the cost for storing templates and running attacks are lower



(a) $\sigma = 0.1$ (b) $\sigma = 1$ (c) $\sigma = 2$

Figure 12: The success rate for ETA on simulated protected leakages with different noise levels.



(a) Power leakages (b) Electromagnetic leakages

Figure 13: The success rate for ETA on practical leakages.

Practical Experiments

Experimental Results

DL based Attack

Experimental Environment

☐ **Operating System**

CentOS 6.1

☐ **CPU**

Intel(R) Xeon(R) CPU E5-2667 v3 @ 3.20GHz 32 core

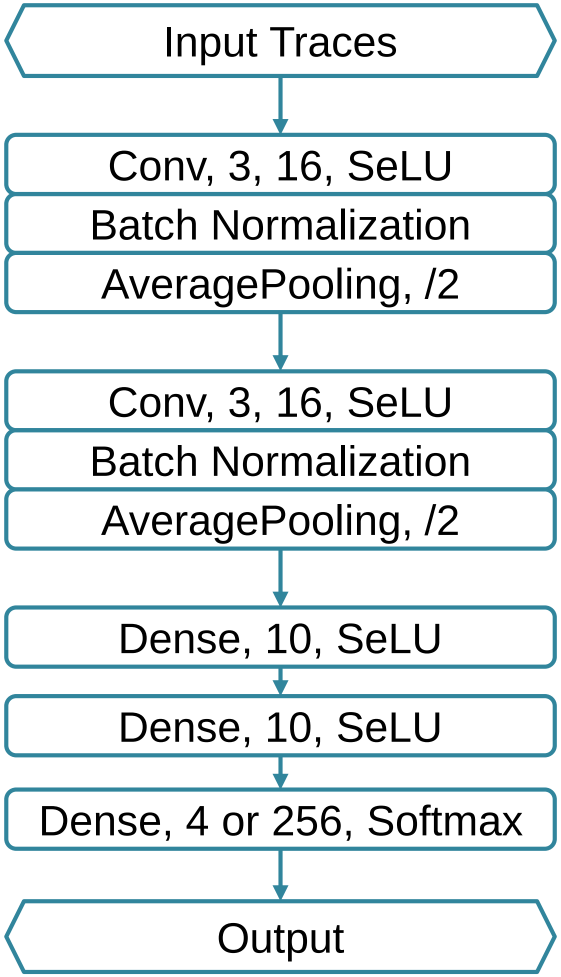
☐ **GPU**

Two NVIDIA Titan Xp GPUs

☐ **Deep Learning Framework**

Keras (version 2.2.2)+ TensorFlow (version 1.10.0)

CNN Architecture



Input Traces

Conv, 3, 16, SeLU

Batch Normalization

AveragePooling, /2

Conv, 3, 16, SeLU

Batch Normalization

AveragePooling, /2

Dense, 10, SeLU

Dense, 10, SeLU

Dense, 4 or 256, Softmax

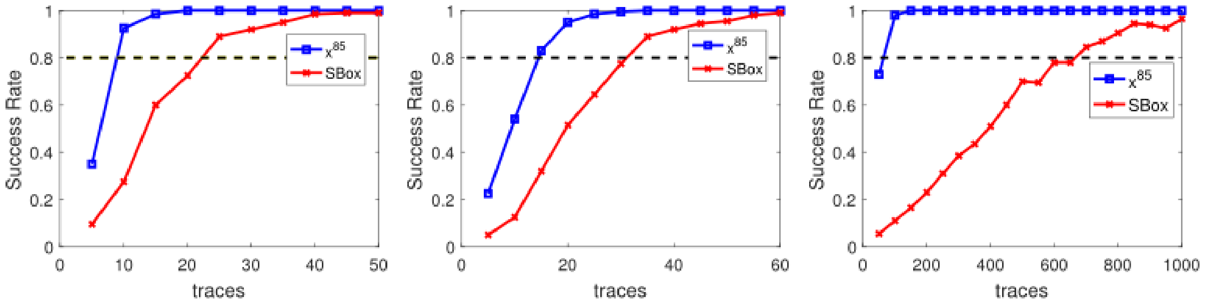
Output

Practical Experiments

Experimental Results

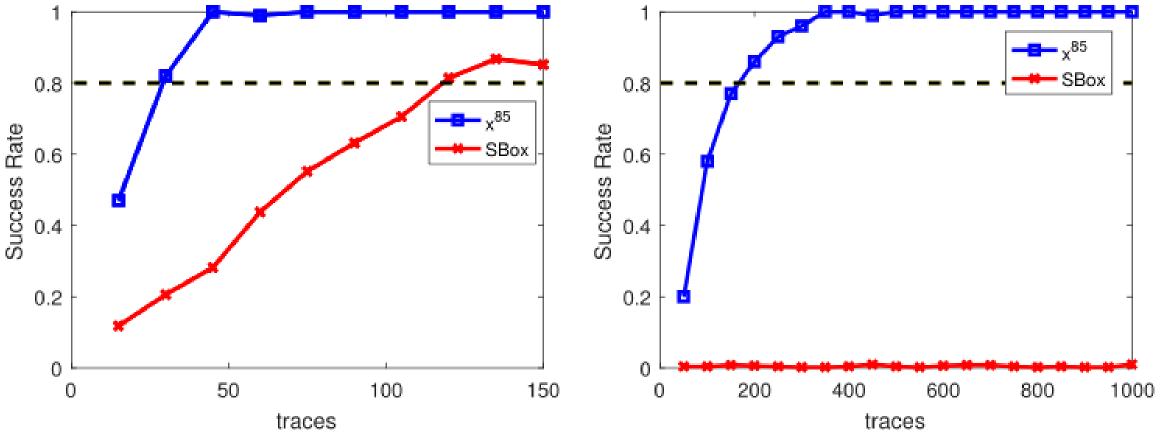
DL based Attack

- The network architectures may be not optimal, as our goal is to compare different addition chains, but not to find optimal parameters
- With increasing noise, attacks on x^{85} become more efficient as well



(a) $\sigma = 0.1$ (b) $\sigma = 1$ (c) $\sigma = 2$

Figure 14: The success rate of deep learning based profiling attacks on simulated leakages with different noise levels.



(a) Power leakages (b) Electromagnetic leakages

Figure 15: The success rate of deep learning based profiling attacks on practical leakages.

Outline

1. **Introduction and Previous Work**

2. **Resistance Measurement**

3. **Practical Experiments**

4. **Conclusion**

Conclusion

Our Work

Implementation	Masking Scheme	Metric	Distinguisher
Addition chain	Boolean Masking	Polygon Degree	Higher-order CPA
		Mutual information	Template Attack
			DL based Attack

Conclusion

Open Problem

Implementation	Masking Scheme	Metric	Distinguisher
Addition chain	Boolean Masking	Polygon Degree	Higher-order CPA
	Multiplicative masking	Mutual information	Template Attack
Other implementations? (unbalanced functions)	Inner product masking	Correlation coefficient	DL based Attack
	Shamir's secret sharing	Statistical distance	Mutual information analysis
	Other schemes?	Other Metrics?	Horizontal attack
			Other distinguishers?

THANKS

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS