

TELECOM
ParisTech



Institut
Mines-Télécom

I. Side-Channel Analysis

from an electronic design perspective

Sylvain GUILLEY
Thursday, Sept. 5, 2013

Presentation Outline

Side-Channel Analysis

Attacks Classification

Countermeasures

Presentation Outline

Side-Channel Analysis

Attacks Classification

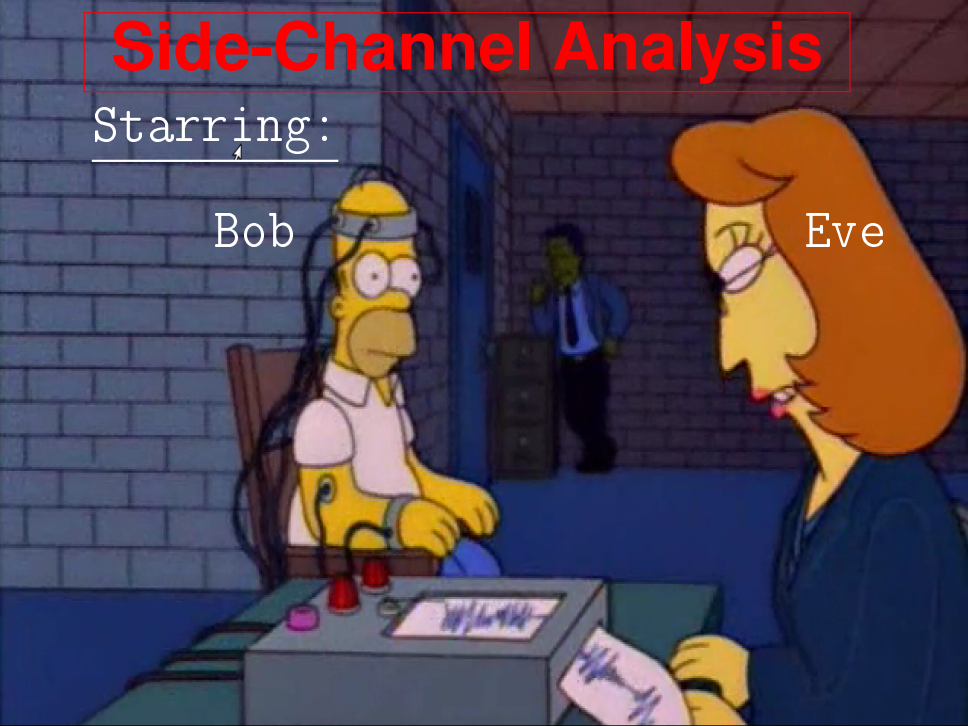
Countermeasures

Side-Channel Analysis

Starring:

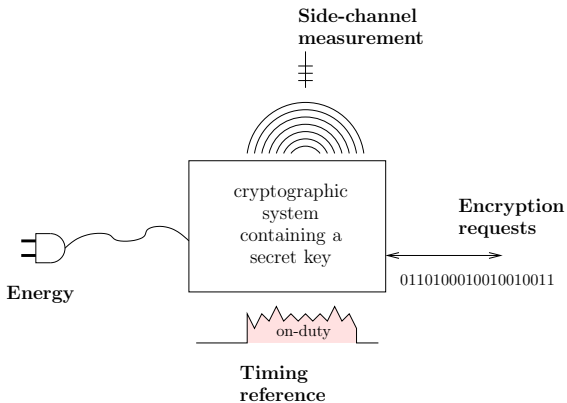
Bob

Eve



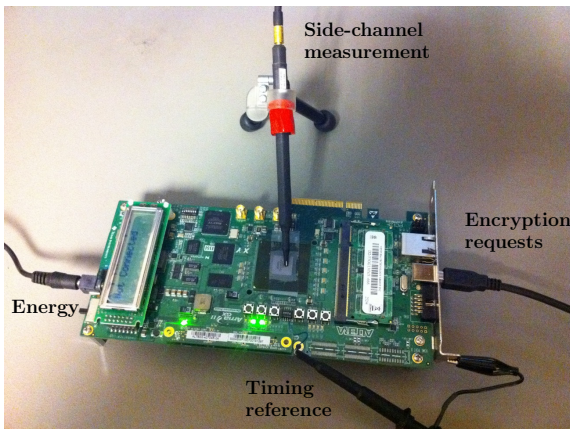
Side-Channel Analysis in Practice

1/3



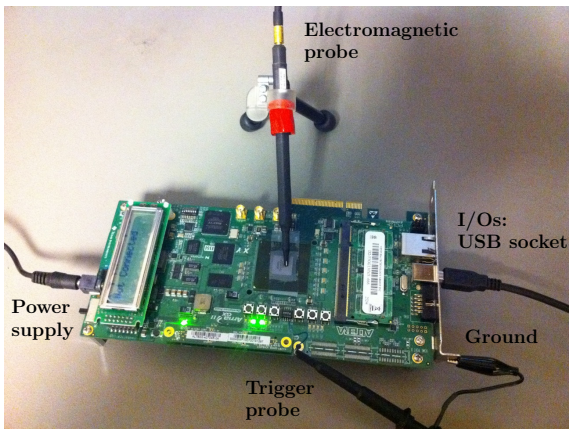
Side-Channel Analysis in Practice

2/3



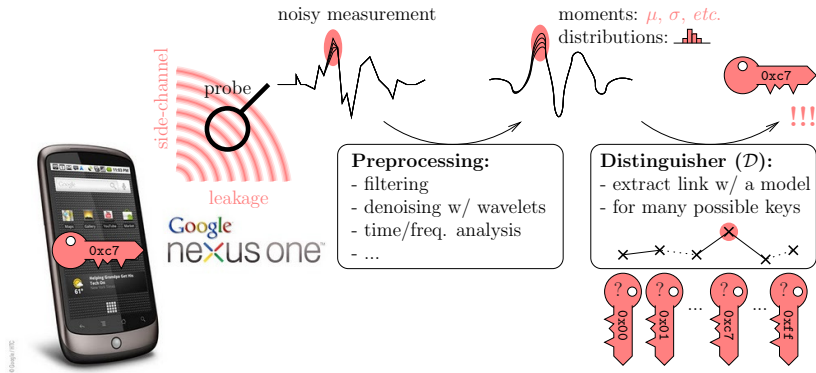
Side-Channel Analysis in Practice

3/3



Side-Channel Analysis on Embedded Systems

[GMN+11]



Sensitive Variables and Distinguishers

Definition (Sensitive variable)

A sensitive variable Z is an intermediate variable that :

- depends on some plaintext X , and
- depends on (*a few bits of*) the key k .

Definition (Distinguisher)

A distinguisher \mathcal{D} is a random variable with values in \mathbb{R} , that depend on two random variables Z and L .

Definition (Soundness)

A distinguisher \mathcal{D} is *sound* if $\operatorname{argmax}_{\hat{k}} \mathcal{D}(Z(\hat{k}), L) = k$.

Presentation Outline

Side-Channel Analysis

Attacks Classification

Countermeasures

Terminology

	Profiled	Non-profiled
Simple	SPA, SEMA	
Differential	Stochastic, Template	DPA, CPA, MIA, KSA

Definition (Profiled / Non-profiled Attacks)

The attack gets information from an **open device** / has **a priori** information (a *model*)

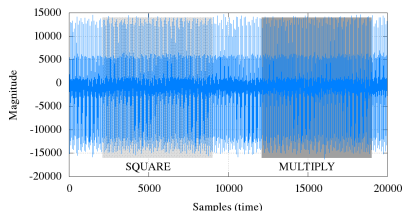
Definition (Simple / Differential Attacks)

One single query is enough / **Statistics on the queries** are required

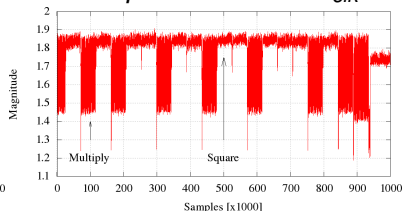
Simple Attacks

on digital signatures (DH, RSA, ECC, ...)

Profiling...
on raw traces



Attacking...
band-pass filtered at f_{clk}

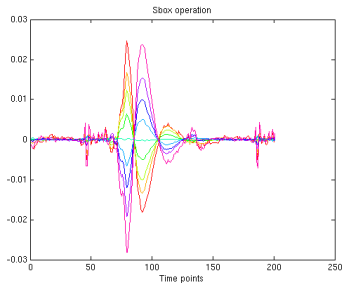


- **With profiling** : convolution product
- **Without profiling** : readout by an expert

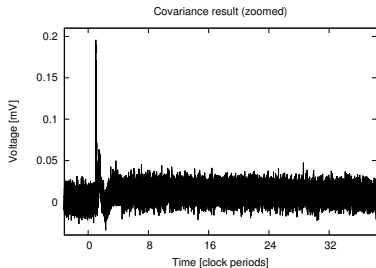
Differential Attacks

on encryption primitives (DES, RC5, AES, ...)

Profiling...
on training traces



Attacking...
on matching traces



- **With profiling** : maximum likelihood
- **Without profiling** : correlation

Refined Classifications

... an open research topic !

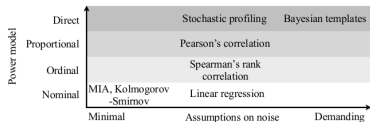


Fig. 1. Types of leakage model and the assumptions required by common distinguishers.

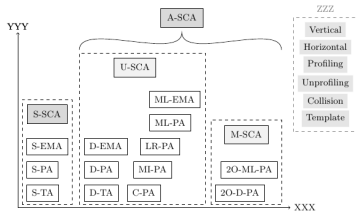


Fig. 2. Side-Channel Attacks

Using Stevens levels of measurement [Ste46].
(picture courtesy of [WOS12]).

Using a proposal for ISO 17825 “non-invasive attacks testing” [Eas12].
(picture courtesy of SGDSN/ANSSI).

Presentation Outline

Side-Channel Analysis

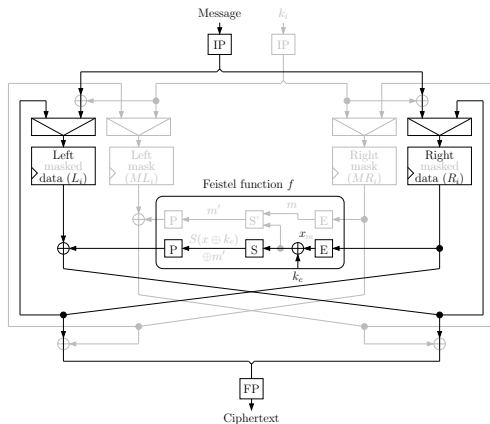
Attacks Classification

Countermeasures

Computing Masked DES

$Z \rightarrow (Z_0, Z_1)$, where $Z_0 \oplus Z_1 = Z$

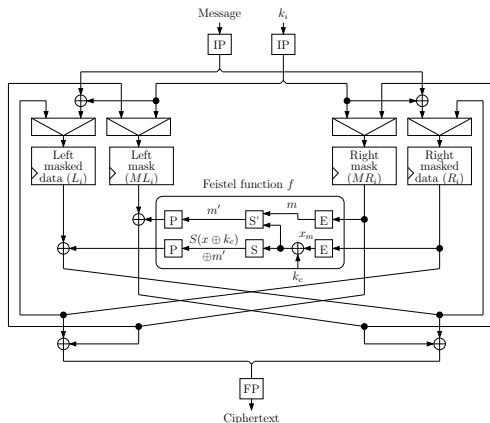
Everything is linear, but the sboxes.



Computing Masked DES

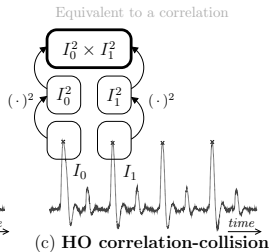
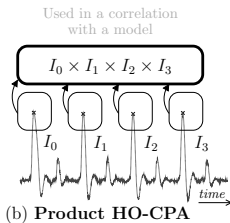
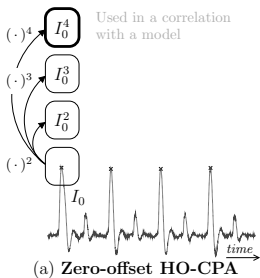
$Z \rightarrow (Z_0, Z_1)$, where $Z_0 \oplus Z_1 = Z$

Everything is linear, but the sboxes.



Vocabulary

Various order 4 attacks [BDGN13]



- **mono-** or **multi-**variate
- **degree** (*power at which traces are raised*) is also taken into account

References

- [BDGN13] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm.
A Low-Entropy First-Degree Secure Provable Masking Scheme for Resource-Constrained Devices.
In *Proceedings of the Workshop on Embedded Systems Security, WESS '13, New York, NY, USA, September 29 2013*. ACM.
Montreal, Canada.
- [Eas12] Randall J. Easter.
Text for ISO/IEC 1st WD 17825 – Information technology – Security techniques – Non-invasive attack mitigation test metrics for cryptographic modules, January 19 2012.
Prepared within ISO/IEC JTC 1/SC 27/WG 3. (Online).
- [GMN⁺11] Sylvain Guilley, Olivier Meynard, Maxime Nassar, Guillaume Duc, Philippe Hoogvorst, Housseem Maghrebi, Aziz Elaabid, Shivam Bhasin, Youssef Souissi, Nicolas Debande, Laurent Sauvage, and Jean-Luc Danger.
Vade Mecum on Side-Channels Attacks and Countermeasures for the Designer and the Evaluator.
In *DTIS (Design & Technologies of Integrated Systems)*, IEEE. IEEE, March 6-8 2011.
Athens, Greece. DOI : 10.1109/DTIS.2011.5941419 ; Online version :
<http://hal.archives-ouvertes.fr/hal-00579020/en/>.
- [Ste46] Stanley Smith Stevens.
On the theory of scales of measurement.
Science, 103(2684) :677–680, June 7 1946.
DOI : 10.1126/science.103.2684.677.
- [WOS12] Carolyn Whitnall, Elisabeth Oswald, and François-Xavier Standaert.
The myth of generic DPA...and the magic of learning.
Cryptology ePrint Archive, Report 2012/256, 2012.
<http://eprint.iacr.org/2012/256>.



Institut Mines-Telecom

II. Side-Channel Mathematical Analysis

Olivier Rioul

Télécom ParisTech





Outline

Introduction

A mathematical theory of side-channel attacks?

Conclusion



Outline

Introduction

A mathematical theory of side-channel attacks?

Conclusion

Axiom 1: Mathematicians are smart.

Why?

- ▶ because they can built fast & arbitrarily secure encryption algorithms (e.g., AES 128, AES 256)

Who says this?

- ▶ the American government:



FACT SHEET

CNSS Policy No. 15, Fact Sheet No. 1

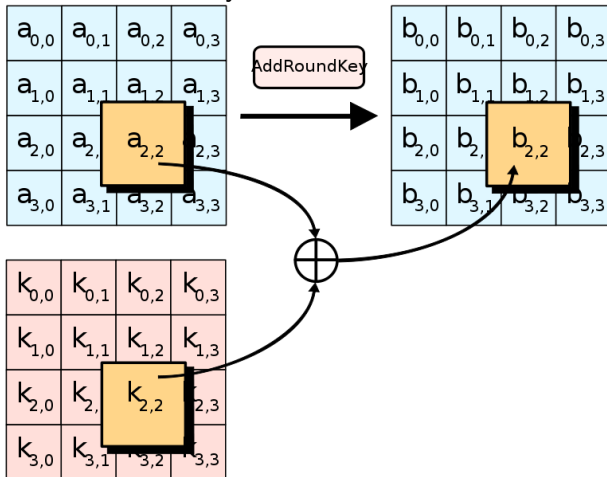
National Policy on the Use of the Advanced Encryption Standard (AES) to
Protect National Security Systems and National Security Information

June 2003

(6) The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.

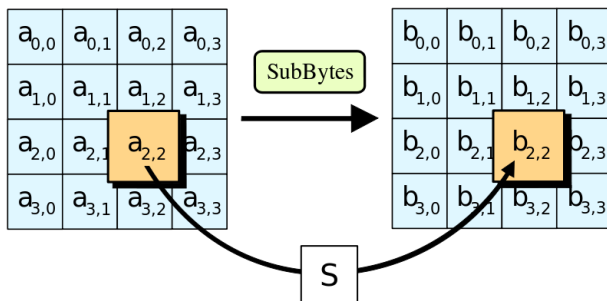
Axiom 1: Mathematicians are smart.

+ We know exactly how AES works !



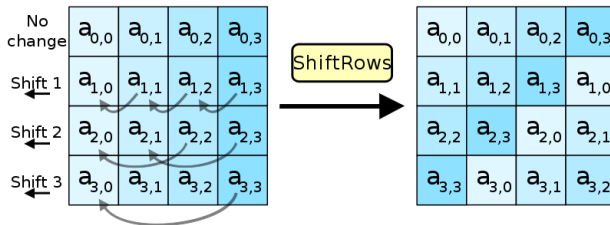
Axiom 1: Mathematicians are smart.

+ We know exactly how AES works !



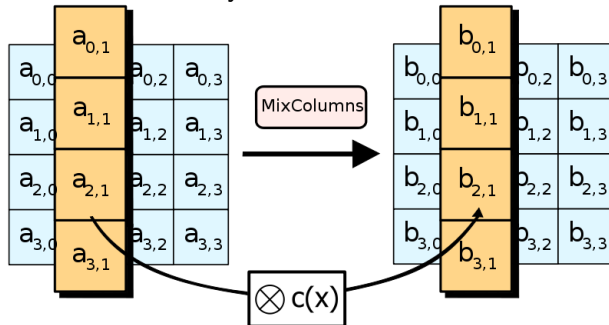
Axiom 1: Mathematicians are smart.

+ We know exactly how AES works !



Axiom 1: Mathematicians are smart.

+ We know exactly how AES works !



Axiom 1: Mathematicians are smart.

+ We know exactly how AES works !

- ▶ 10 to 14 rounds of such computation
- ▶ computation on 8-bit chunks (algebraic properties of \mathbb{F}_{2^8})
- ▶ $S(X \oplus k)$ (AddRoundKey + SubBytes) within each round (where X is inductively known but cannot always be chosen)
- ▶ S resists to cryptanalysis (differential attack):

$$\Delta_S = \max_{k,a} |\{x \in \mathbb{F}_{2^8} \mid S(x) \oplus S(x \oplus k) = a\}|$$

+ AES has *not* been broken yet

- ▶ Best attack so far : \approx brute force (2^{128} to 2^{256} tries)

Axiom 1: Mathematicians are smart.

+ We know exactly how AES works !

- ▶ 10 to 14 rounds of such computation
- ▶ computation on 8-bit chunks (algebraic properties of \mathbb{F}_{2^8})
- ▶ $S(X \oplus k)$ (AddRoundKey + SubBytes) within each round (where X is inductively known but cannot always be chosen)
- ▶ S resists to cryptanalysis (differential attack):

$$\Delta_S = \max_{k,a} |\{x \in \mathbb{F}_{2^8} \mid S(x) \oplus S(x \oplus k) = a\}|$$

+ AES has (**almost**) *not* been broken yet

- ▶ Best attack so far : \approx brute force ($2^{126.1}$ to $2^{254.4}$ tries)

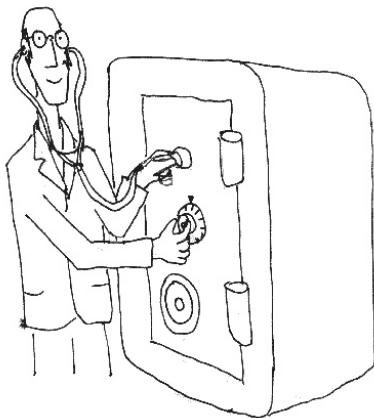
Axiom 1: Mathematicians are smart.

85070591730234615865843651857942052864 to
115792089237316195423570985008687907853269984665640564039457584007913129639936 tries...



Axiom 2: Physicists are smarter.

Physical (non invasive) attack



Axiom 2: Physicists are smarter.

Safe box attack

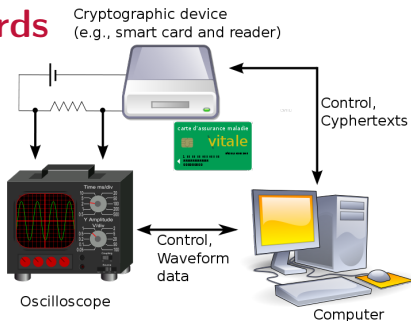
A simple attack (e.g., 16-byte key or 4-digit PIN)

```
for i in [0..3]: # or 0..15
    if private_key[i] is input_key[i]:
        continue # lock click heard!
    else:
        return NOK
return OK
```

$\leq 4 \times 10$ tries (instead of 10^4)

$\leq 16 \times 256$ tries (instead of 2^{128})

Keywords



- ▶ measuring *power traces*: output from a noisy *side channel*
- ▶ using noisy data *statistics* (DPA vs. SPA)
- ▶ *profiling* or not profiling the device
- ▶ modeling *intermediate values* within cryptographic operations (e.g., byte by byte recovery for each AES round 16 down to 1)
- ▶ *univariate* ou *multivariate* sampling
- ▶ hiding, shuffling, masking... as *countermeasures*



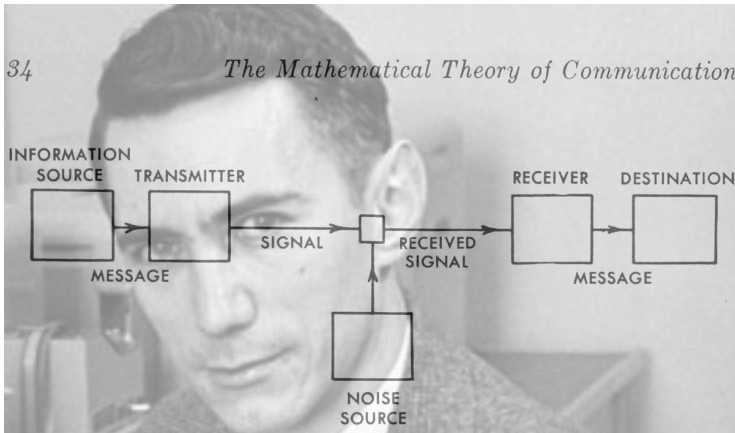
Outline

Introduction

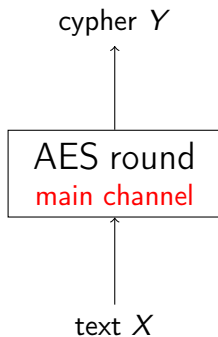
A mathematical theory of side-channel attacks?

Conclusion

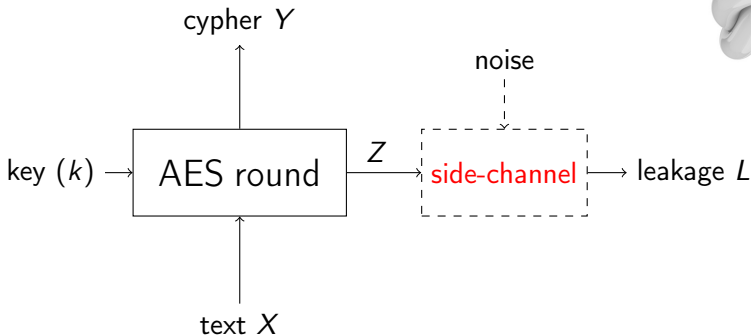
A mathematical theory of SCA?



A communication problem?



A communication problem?

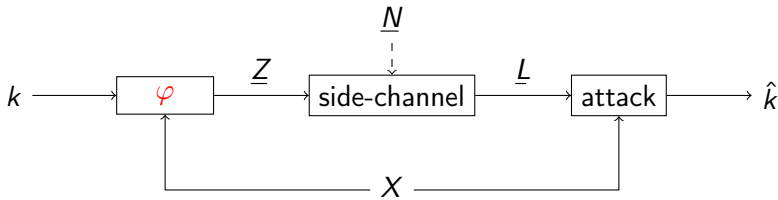


- ▶ input: n -bit key k (fixed but unknown)
- ▶ sensitive variable Z (depends on k and X (or Y))
- ▶ (noisy) leakage L

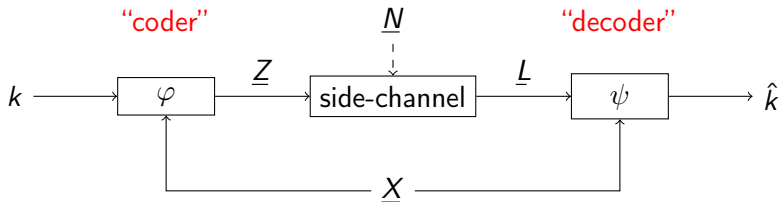
A communication problem?



- ▶ m measures (channel uses)
- ▶ text $\underline{X} = (X_1, X_2, \dots, X_m)$ chosen or i.i.d.
- ▶ sensitive variable $\underline{Z} = (Z_1, Z_2, \dots, Z_m)$ i.i.d.
- ▶ memoryless side-channel
- ▶ noisy leakage $\underline{L} = (L_1, L_2, \dots, L_m)$ i.i.d.



A communication problem?



- ▶ looks like a communication problem ;)
- ▶ (with common side information \underline{X})
- ▶ the "coder" may be (partially) unknown (model discrepancy)
- ▶ the side-channel may be also (partially) unknown
- ▶ k is *fixed* (huge repetition code $(m, 1)$)

The attacker will eventually succeed! (if m is large enough, unless φ is constant or side-capacity=0).

The detection problem



Criterion

“success rate”, or mathematically:

$$\max \mathbb{P}_s = \mathbb{P}\{\hat{k} = k\}$$

(related criterion: min guessing entropy $\sum_k k \cdot p_{(k)}$ where $p_{(k)} \searrow$)

- ▶ frequentist approach: $\mathbb{P}_{s|k} = \mathbb{P}\{\hat{k}(\underline{X}, \underline{L}) = k\}$
- ▶ Bayesian approach: $\mathbb{P}_s = \mathbb{E}\{\mathbb{P}_{s|K}\}$ where prior K is uniform.

The detection problem



$$\mathbb{P}_s = \sum_{\underline{x}} \mathbb{P}\{\underline{x}\} \int_{\underline{\ell}} p(\underline{\ell}|\underline{x}) \cdot \mathbb{P}\{k = \psi(\underline{x}, \underline{\ell})|\underline{x}, \underline{\ell}\} d\underline{\ell}$$

MAP maximum a posteriori

$$\hat{k} = \arg \max_k \log \mathbb{P}\{k|\underline{x}, \underline{\ell}\}$$

Now $\mathbb{P}\{k|\underline{x}, \underline{\ell}\} = \mathbb{P}\{k\}p\{\underline{x}, \underline{\ell}|k\}/p\{\underline{x}, \underline{\ell}\}$, where $\underline{X} \perp k$:

$$p\{\underline{x}, \underline{\ell}|k\} = \mathbb{P}\{\underline{x}|k\}p(\underline{\ell}|\underline{x}, k) = \mathbb{P}\{\underline{x}\}p(\underline{\ell}|\underline{x}, k)$$

ML maximum likelihood

$$\hat{k} = \arg \max_k \log p(\underline{\ell}|\underline{x}, k)$$



Template attack



Apply the optimal rule!

$$\hat{k} = \arg \max_k \log p(\underline{\ell} | \underline{x}, k)$$



Template attack

Apply the (well, quasi-) optimal rule!

$$\hat{k} = \arg \max_k \log \hat{p}(\underline{\ell} | \underline{x}, k)$$

profiling phase estimate the pdf $\hat{p}\{\ell | x, k\}$ for **every** x and k

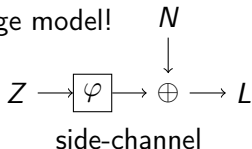
attacking phase given $\underline{\ell} = (\ell_1, \ell_2, \dots, \ell_m)$ and $\underline{x} = (x_1, \dots, x_m)$,
compute $\hat{L}\{\underline{\ell} | \underline{x}, k\} = \sum_{i=1}^m \log \hat{p}\{\ell_i | x_i, k\}$ for each k
and select the maximum.

“Optimal” ... but practical?

- ▶ requires an exact copy of the device, where k can be chosen
- ▶ $2^{2n} = 65536$ templates (pdfs)....
- ▶ sufficient statistics $Z = S(X \oplus k) : (X, k) \rightarrow Z \rightarrow L$ is Markov
- ▶ reduces to $2^n = 256$ densities $p(\ell | x, k) = p(\ell | z)$

Stochastic model attack

It's best to use a leakage model!



Example: additive model

$$L = \underbrace{\varphi(Z)}_{\text{deterministic}} + \underbrace{N}_{\text{stochastic}}$$

where

- ▶ $Z = S(X \oplus k)$, let $Z' = \varphi(Z)$
- ▶ $\varphi : \mathbb{F}_2^n \rightarrow \mathbb{R}$
- ▶ N AWGN (measurement noise)

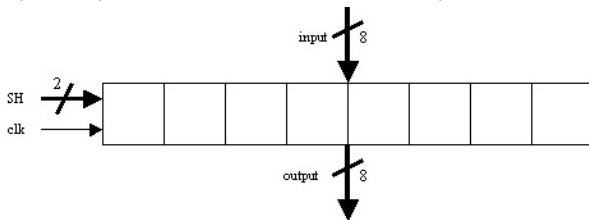


Interlude



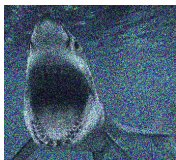
Where do physical leakages come from?

- ▶ no direct access to $S(X \oplus k)$: noisy values
- ▶ when $S(X \oplus k)$ is wrote in a byte register (with initial state 0),



$$\text{consumed power for each } i\text{th bit} = \begin{cases} 0 & \text{if } [S(X \oplus k)]_i = 0 \\ \varepsilon & \text{if } [S(X \oplus k)]_i = 1 \end{cases}$$

- ▶ total power $\approx \varepsilon \cdot w_H(S(X \oplus k))$
- ▶ HW model: sensitive variable $Z' = w_H\{S(X \oplus k)\}$.



Stochastic model attack: AWGN

Since $(X, k) - Z' - L$ is Markov and $N \perp\!\!\!\perp Z'$:

$$p(\ell|x, k) = p(\ell|z') = p(n = \ell - z'|z') = p_N(\ell - z')$$

ML detection becomes: $\hat{k} = \arg \max_k \log p_N(\underline{\ell} - \underline{z}')$ where

$$\log p_N(\underline{\ell} - \underline{z}') = -\frac{1}{2\sigma_N^2} \|\underline{\ell} - \underline{z}'\|^2 + \text{Cst.}$$

expanding $\|\cdot\|^2$ gives...

Distinguisher attack

$\hat{k} = \arg \max_k \mathcal{D}(k)$ where

$$\mathcal{D}(k) = \langle \underline{\ell}; \underline{z}' \rangle - \frac{1}{2} \|\underline{z}'\|^2 \approx \boxed{\sum_{i=1}^m \ell_i z'_i}$$

This reduces to a **correlation** attack! (CPA/DPA/DoM)



Model discrepancy

It's best to use a leakage model... provided it is reliable!

$$L = \varphi(Z) + N \neq \hat{L} = \hat{\varphi}(Z) + \hat{N}$$

Remedies:

- ▶ model identification: $\hat{\varphi}(z) = \sum_i \alpha_i z_i + \sum_{i,j} z_i z_j + \dots$ instead of the linear $\sum_i z_i = w_H(z)$
- ▶ estimate $\hat{\varphi}(Z) = \mathbb{E}(L|Z)$ (optimal in the least squares sense)
- ▶ equivalent to applying *non linear* correlation attack
- ▶ use mutual information analysis (MIA) equivalent to MMI decoding

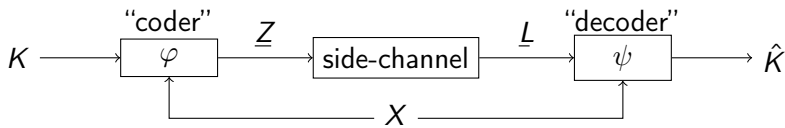
$$\hat{k} = \arg \max\{\mathcal{D}(k) = \hat{I}(L; Z)\}$$

which involves pdf estimation $p(\ell|z)$.



Postlude

What can be done against an almighty attacker?



- ▶ uniform prior: $n = H(K)$
- ▶ Fano's inequality: $H(K|\hat{K}) \leq H_2(\mathbb{P}_s) + n(1 - \mathbb{P}_s)$
- ▶ data processing inequality:
 $I(XK; X\hat{K}) \leq I(\underline{X}\underline{Z}; \underline{X}\hat{K}) \leq m \cdot I(XZ; XL)$
- ▶ Markov chain condition: $I(Z; L) - I(Z; X) = I(Z; L|X)$
common-randomness-does-not-help principle ;)

Theorem: for the best possible attacker,

$$n\mathbb{P}_s - H_2(\mathbb{P}_s) \leq m \cdot I(L; Z|X) \leq m \cdot C_{sc}$$

 Postlude

Conclusion for an AWGN channel :

$$n\mathbb{P}_s - H_2(\mathbb{P}_s) \leq \frac{m}{2} \cdot \log_2(1 + \text{snr})$$

where

- ▶ n is the number of key bits
- ▶ m is the number of traces
- ▶ \mathbb{P}_s is the success rate
- ▶ snr is the measurement signal-to-noise ratio

To avoid $\mathbb{P}_s \rightarrow 1$ rapidly:

- ▶ enlarge key chunks ($n \gg 1$)
- ▶ add noise ($\text{snr} \ll 1$)



Outline

Introduction

A mathematical theory of side-channel attacks?

Conclusion

Open problems

- ▶ How to evaluate **performance**?
 - ▶ asymptotically: $m \rightarrow +\infty$








$$1 - \mathbb{P}_s \doteq e^{-m \min_{k \neq k^*} \frac{\mathbb{E}\{\mathcal{D}(k^*) - \mathcal{D}(k)\}}{2 \text{Var}\{\mathcal{D}(k^*) - \mathcal{D}(k)\}}}$$

- ▶ or not: $\min\{m \mid P_s(m) > 90\%\} = ?$
- ▶ What is the impact of **pdf estimation** on performance?
- ▶ What is the impact of **model discrepancy** on performance?
What is the best distinguisher?
- ▶ What is the impact of **masking** on performance?
- ▶ What is an optimal **countermeasure**?
- ▶ How trade resistance to **cryptanalysis** vs. **side-channel analysis**?
- ▶ What is a **confusion** coefficient?
- ▶ etc., etc., etc.



Collected works...

Google compliant.

-  HM, OR, SG, JLD, “Comparison between side-channel analysis distinguishers”, ICICS’12 Hong Kong
-  **Annelie Heuser** (AH), SG, OR, “Practical vs. theoretical evaluation of DPA and CPA”, CrossFyre’13, Leuven
-  AH, SG, OR, “Revealing the secrets of success: Theoretical efficiency of side-channel distinguishers”, CryptArchi’13, Fréjus
-  AH, HM, OR, SG, JLD, “Mathematical and empirical comparison of information-theoretic side-channel distinguishers”, JCEN, rev.
-  AH, SG, OR, “Success metric: An all-in-one criterion for comparing side-channel distinguishers”, poster CHES’13, Santa Barbara
-  AH, SG, OR, “Theoretical study of one-bit Kolmogorov-Smirnov Side-Channel Analysis”, CARDIS’13, sub.
-  AH, SG, OR, “Distinguishing distinguishers...”, EUROCRYPT’14, sub.

