Time Samples Correlation Attack

Olivier MEYNARD[1,2], Sylvain GUILLEY[1], Denis REAL[2] and Jean-Luc DANGER[1]

[1]TELECOM-ParisTech , CNRS – LTCI (UMR 5141),
[2]DGA/MI (French DoD, information superiority).

COSADE.
Darmsadt, Thursday, 24th February 2011.

Outline

Presentation Outline

Introduction to Side Channel Analysis (*aka* SCA)

Side Channel

Cryptographic devices leak sensitive information:

- Computation time,
- Power consumption,
- Electromagnetic radiation.

Exploitation of SCAs

The success of an attack depends on:

- A relevant partitioning with a suitable **leakage model**;
- **Distinguisher** including:
  covariance (DPA), *correlation* (CPA), *mutual information* (MIA), *maximum likelihood* (template and stochastic attacks).

Two research directions:

1. Comparison and research of new distinguishers:
   - **'Mutual Information Analysis: How, When and Why'**, *In CHES 2009, by Veyrat-Chatillon et. al*
2. How to make the most with the existing distinguisher?
   - **Combining time samples from an acquisition campaign**: *'Revisiting Higher-Order DPA attacks: Multivariate Mutual Information Analysis', Gierlichs et al.: CT-RSA 2010.*
   - **Combine Side Channel:** *'Multi-channel Attacks', Agrawal et al.:CHES 2003.*
   - **Combine Active and Passive attacks** *'Passive and Active Combined Attacks on AES.',Clavier et al.:FDTC 2010.*

Our contribution

Various Samples within a trace can carry information: POI Points Of Interests

We propose to:

1. *Study different methods to find out POI,*
2. *Combine multi-sample EM trace.*

Our contribution

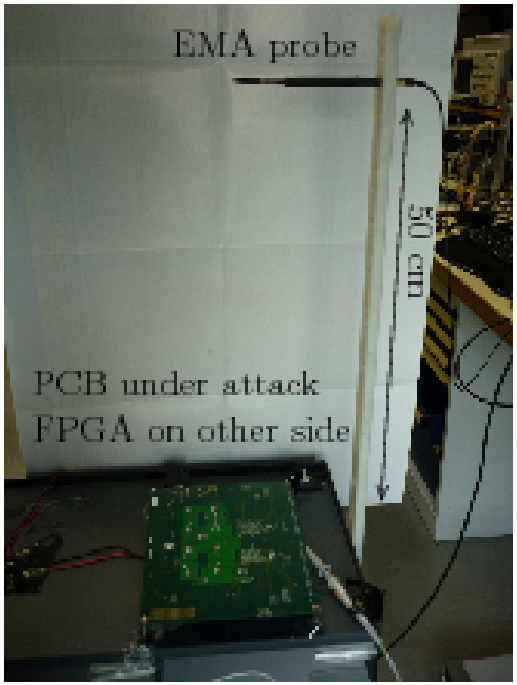
Various Samples within a trace can carry information:
POI Points Of Interests

We propose to:

1. *Study different methods to find out POI,*
2. *Combine multi-sample EM trace.*

Presentation Outline

Context of electromagnetic (EM) side-channel



- Use a SASEBO-G board,
- AES hardware implementation,
- Without any countermeasures.

The leakage evolves due to distortion into communication channel.

Context of electromagnetic (EM) side-channel

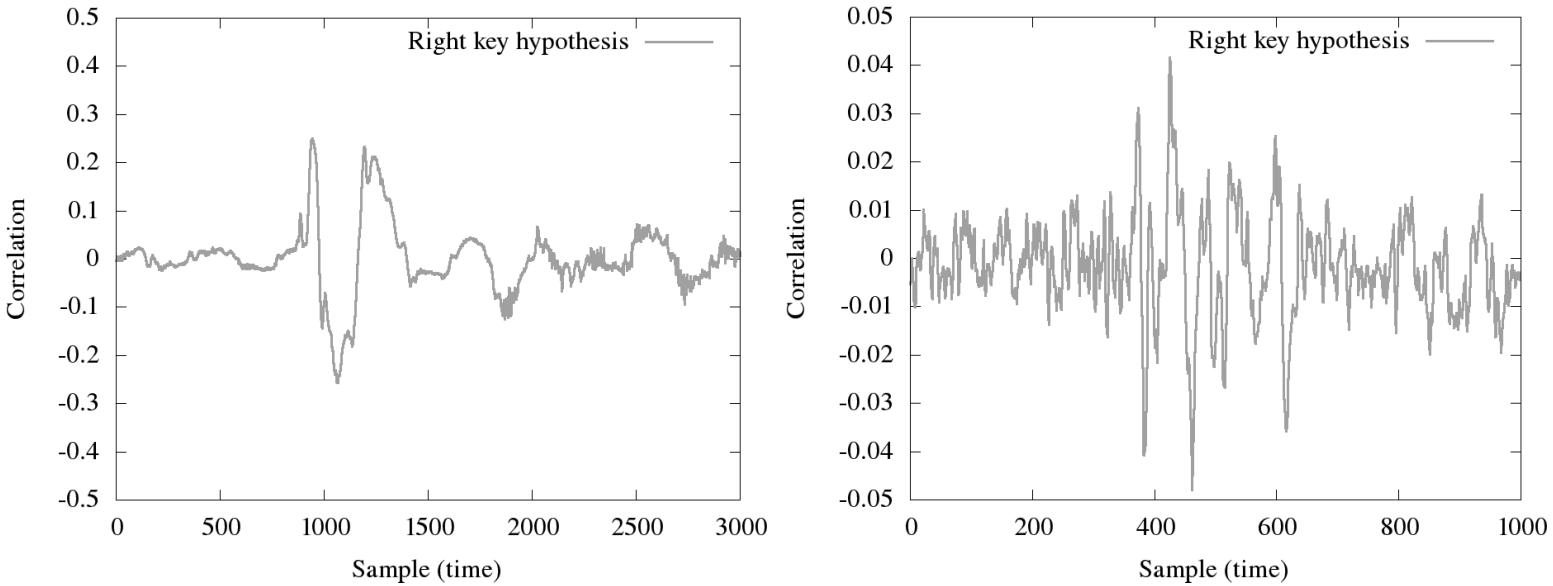


Figure 1: Differential trace for campaign at 0 cm and at 25 cm.

Context

- Two sets of measurements (short distance, and 25 cm).
- A CPA is successful for the two sets.
- the selection function: $\mathcal{L} = HW(\text{state}_9[sbox] \oplus \text{ciphertext}[sbox])$.

The *Sum Of Squared pairwise Differences* (sosd)

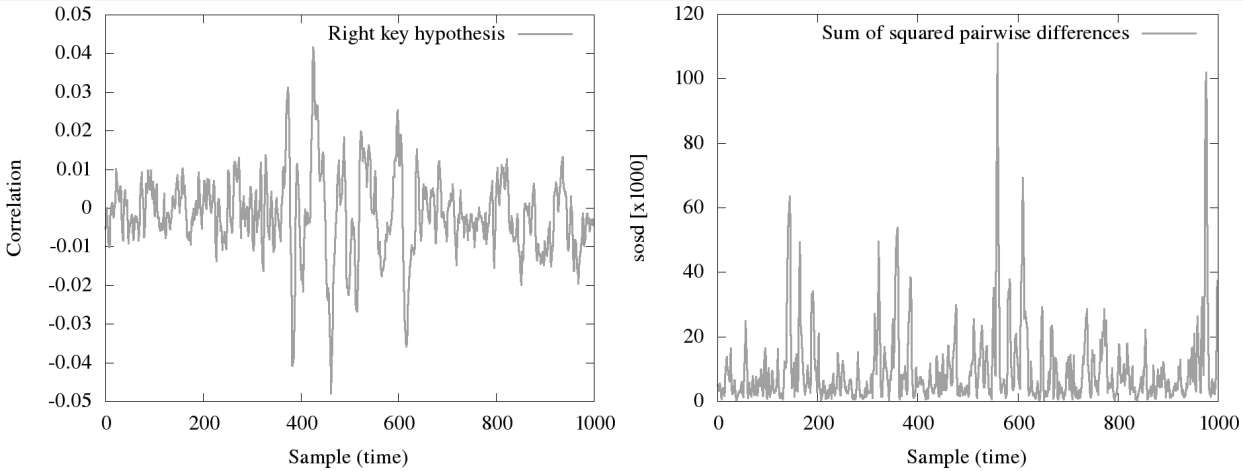


Figure 2: Differential trace and sosd for campaign at 25 cm.

- Gierlichs *et.al* CHES'06.
- Partitioning in accordance with $\mathcal{L}$ in $[0, 8]$,

$$\text{sosd} \doteq \sum_{j,j'=0}^{8} \left(\mu_j - \mu_{j'}\right)^2$$

where $\mu_j(t)$ are the mean of observation in each class $j \in [0, 8]$.

At 25cm CPA doesn't success on the POI of sosd.

The *Sum Of Squared pairwise (T-)Differences* (sost)

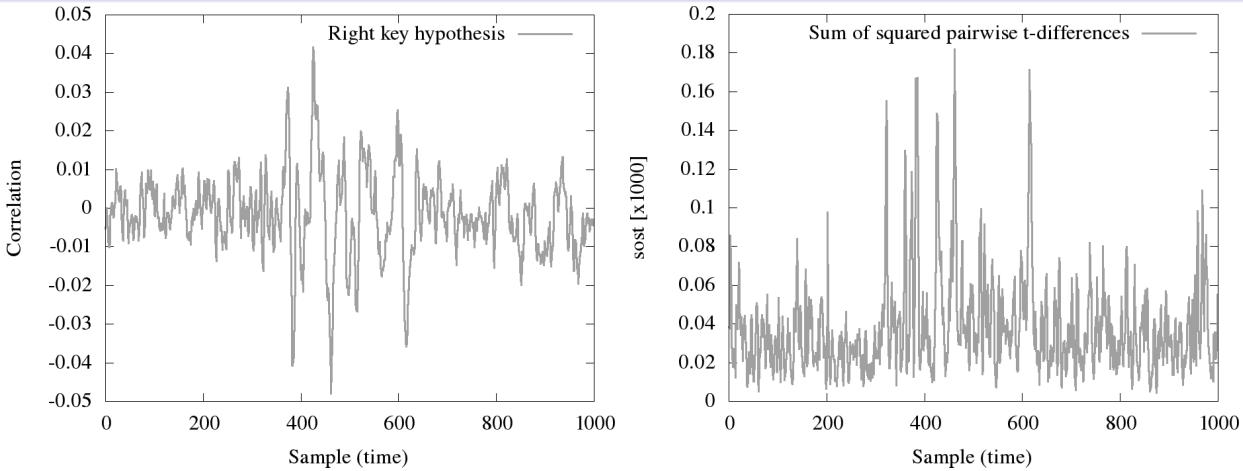


Figure 3: Differential trace and sost for campaign at 25 cm.

- Gierlichs *et.al* CHES'08.
- Based on T-Test (standard statistical test)
- Consider the variability $(\sigma_j^2, \sigma_{j'}^2)$ in relation to the number of samples $(n_j, n_{j'})$.

$$\text{sost} \doteq \sum_{j,j'=0}^{8} \left(\frac{\mu_j - \mu_{j'}}{\sqrt{\frac{\sigma_j^2}{n_j} + \frac{\sigma_{j'}^2}{n_{j'}}}} \right)^2$$

At 25cm sost is not optimal.

Techniques for Revealing the POIs

The Principal Component Analysis (PCA).

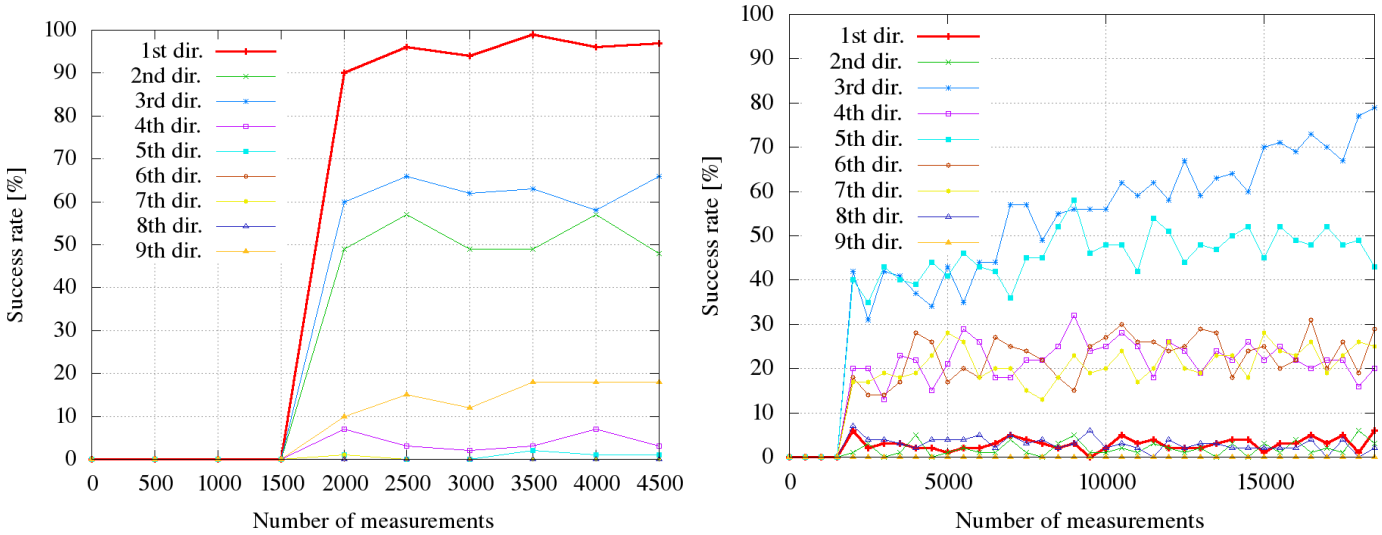


Figure 4: Success rate of the CPA after PCA pre-processing.

- The estimation for $l = 0$ or 8 is less accurate.
- Level of Noise is higher, since very less number of traces for these subsets.

Presentation Outline

Observations

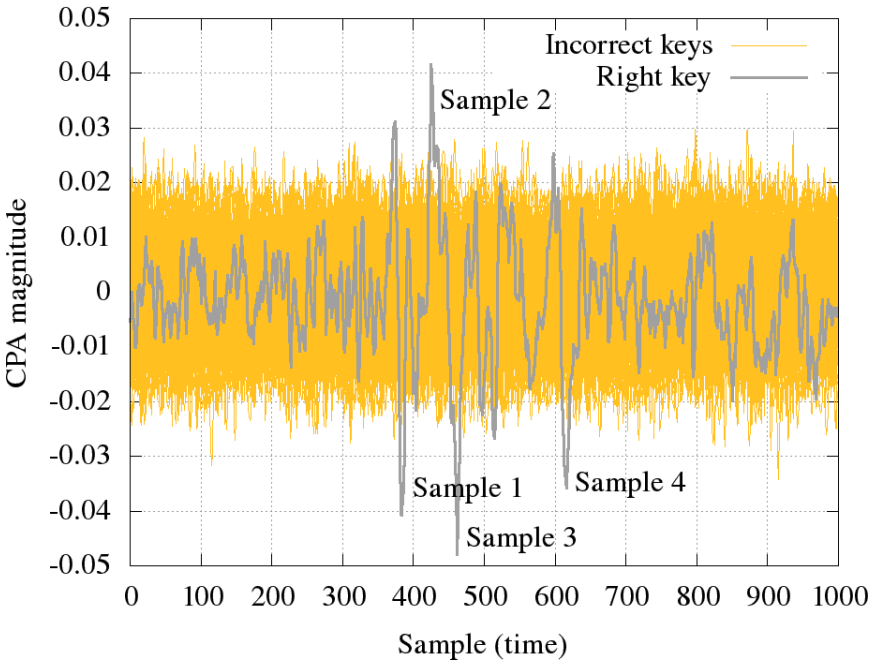


Figure 5: Correlation traces obtained for the right key hypotheses and for incorrect key hypotheses at 25 cm.

- Correlation traces are extremely noisy.
- Time Samples{1,2,3,4} magnitude of the correlation trace for right key is higher.
- Samples are located within the same clock period.
- They are carrying secret information.

Sample Combination Principle and Results

Principle

- Confirm that the 4 samples are POIs.
- Perform successful CPAs at these time samples.
- The new distinguisher we promote is thus:

$$\hat{\rho}_{\text{combined}} \doteq \prod_{t \in \text{Sample}\{1,2,3,4\}} \hat{\rho}_t \,,$$

where $\hat{\rho}_t$, is Pearson correlation coefficients.

Sample Combination Principle and Results

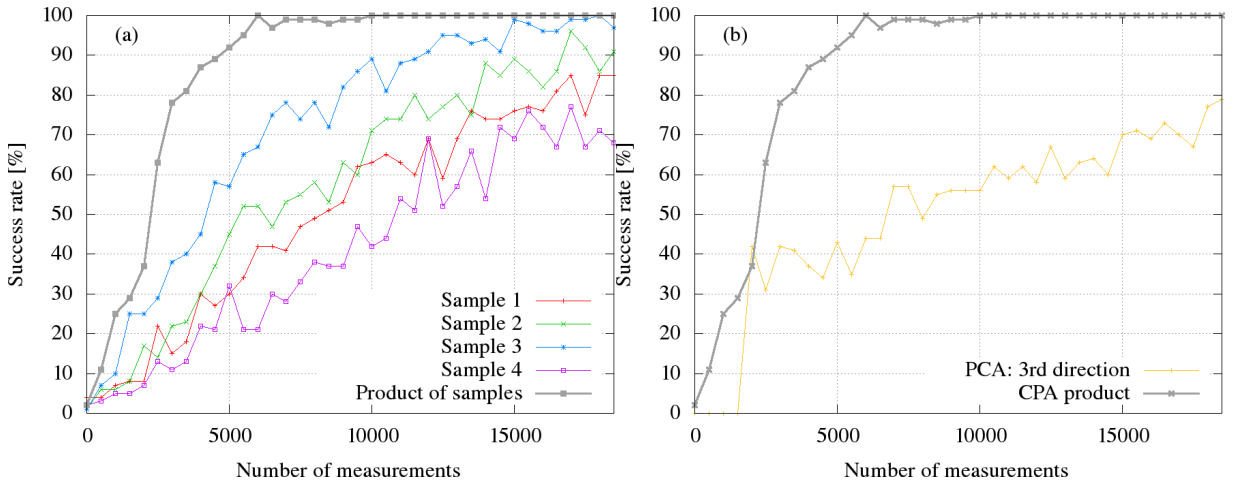


Figure 6: (a)–*left*: Success rate of the mono-sample attack, and product of correlations attack; (b)–*right*: Comparison between a CPA using the pre-treatment by PCA and our product of correlation.

How to best combine Samples ?

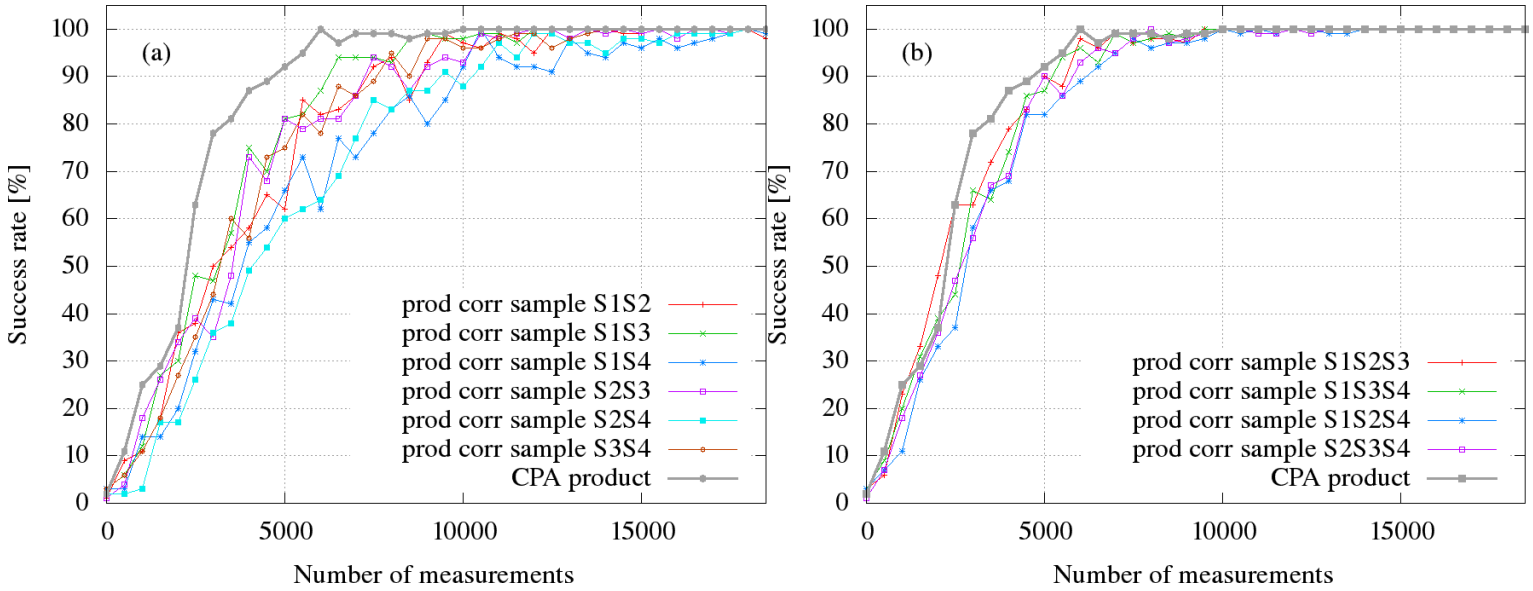


Figure 7: (a): Success rate of product of 2-samples correlation attack, and product of 4-samples of correlations attack; (b): Success rate of product of 3-samples correlation attack, and product of 4-samples of correlations attack.

How to locate POIs without knowing the key or without conducting an attack ?

⇓

One suggestion: Pre characterization assuming that the position of POIs do not depend on secret key

How to best combine Samples ?

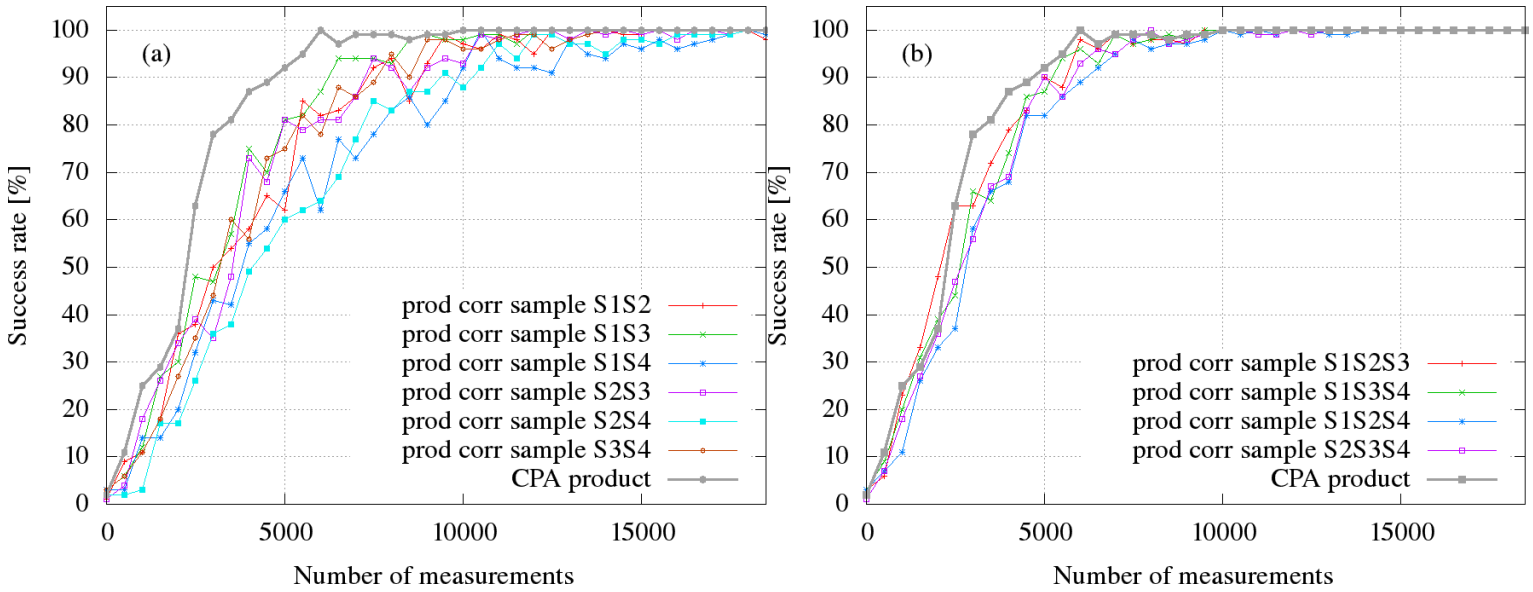


Figure 7: (a): Success rate of product of 2-samples correlation attack, and product of 4-samples of correlations attack; (b): Success rate of product of 3-samples correlation attack, and product of 4-samples of correlations attack.

How to locate POIs without knowing the key or without conducting an attack ?

⇓

One suggestion: Pre characterization assuming that the position of POIs do not depend on secret key

How to best combine Samples ?

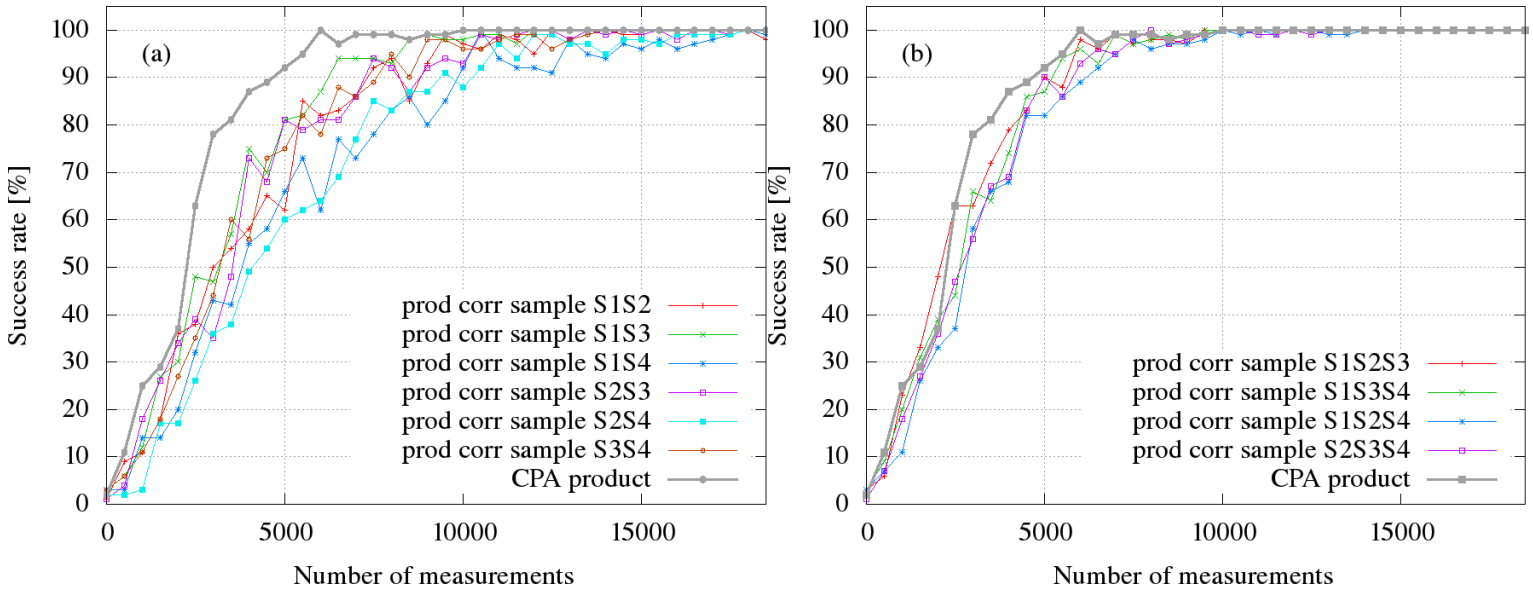


Figure 7: (a): Success rate of product of 2-samples correlation attack, and product of 4-samples of correlations attack; (b): Success rate of product of 3-samples correlation attack, and product of 4-samples of correlations attack.

How to locate POIs without knowing the key or without conducting an attack ?

$\Downarrow$

One suggestion: Pre characterization assuming that the position of POIs do not depend on secret key

POIs independence with the Key

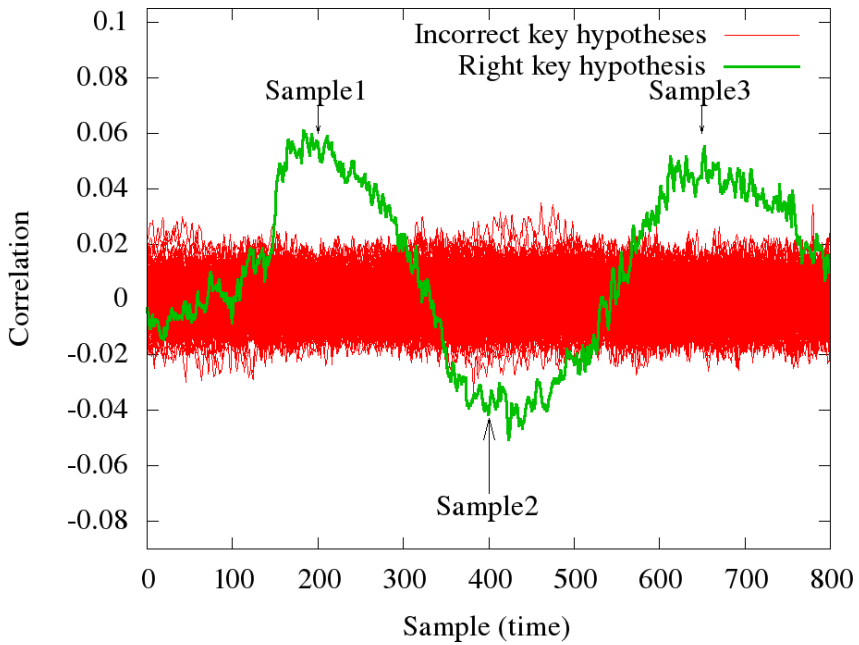


Figure 8: Differential traces obtained for the Sbox#2 using measurements from the DPA Contest v2 public database.

- traces of public database dpacontestv2.
- 32 different cipher keys, each one containing 20,000 random plain texts.
- Power measurement on SASEBO GII.

Results of the Attacks

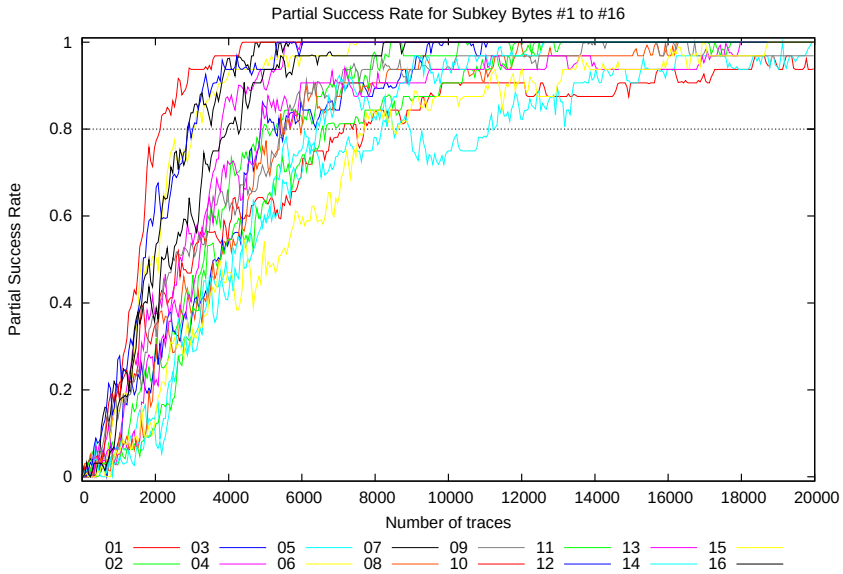


Figure 9: Success rate.

- We explore the richness of power consumption measurements.
- POI don't change with the Key and Sbox.
- We can break all the Sbox even if we change the key.

Presentation Outline

Conclusion

- Combine several timing samples in such a way to have an adaptive model.
- A better success rate obtained than a mono-model attack using a combination of samples (via PCA).
- We show how the leakage of each sample can be combined better than usual leakage reduction methods.
- This attack can be further enhanced by another method to select POIs.
- A proof of concept that the POI are independent of the Key and Sbox for power consumption measurement.

Thank you!
Any Questions?