Auto-Aligned Remote Power Analysis through Ring Oscillator-based Sensors

XVII Reunión Española sobre Criptología y Seguridad de la Información. Santander, Spain. October 2022.

Lilian Bossuet, Anis Fellah-Touta, Carlos Andres Lara-Nino

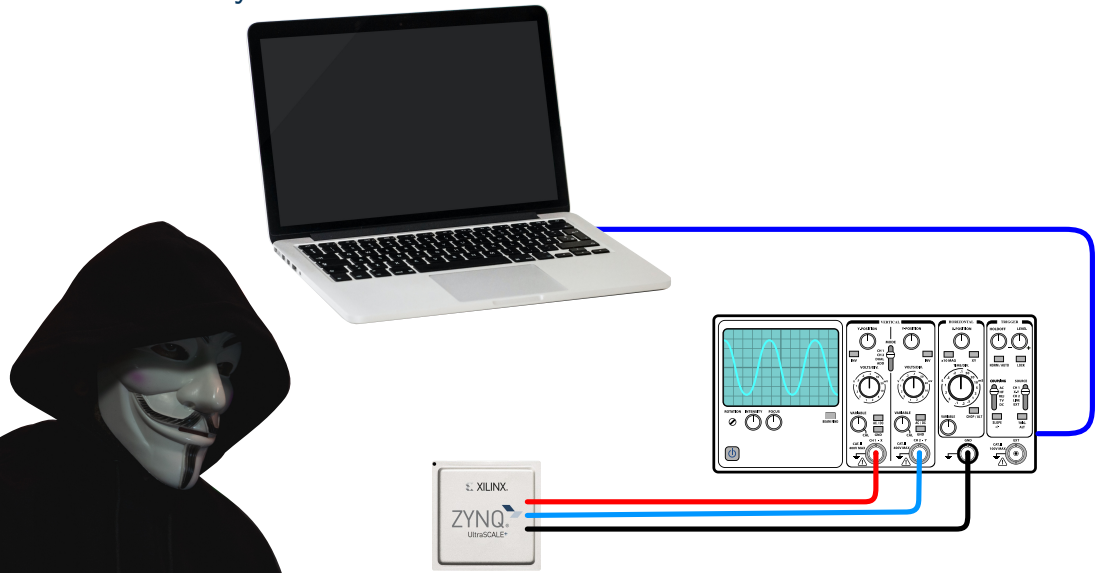
LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

In this talk:

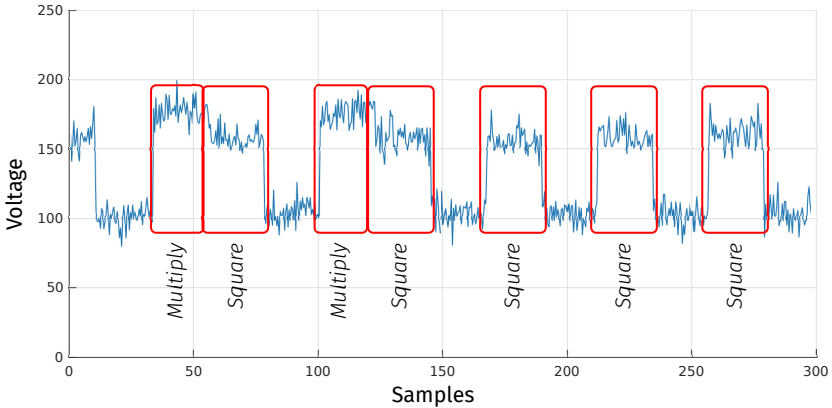
- Power Analysis
- Remote Power Analysis
- Covert channels
- Combined attacks

1 | Power Analysis

Power Analysis

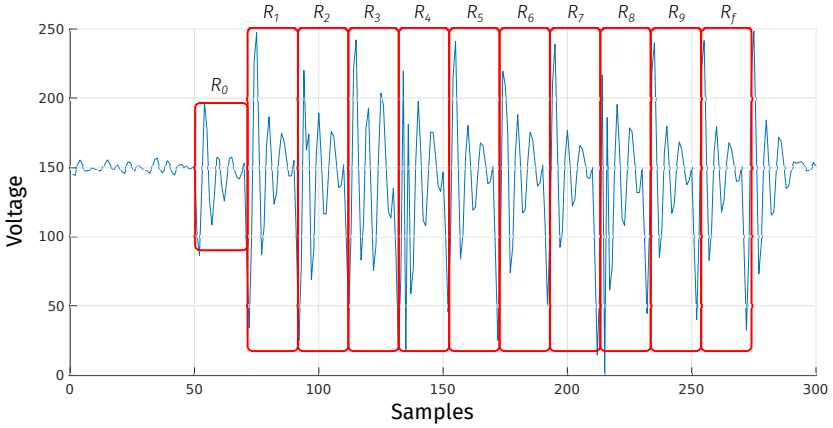


Simple Power Analysis



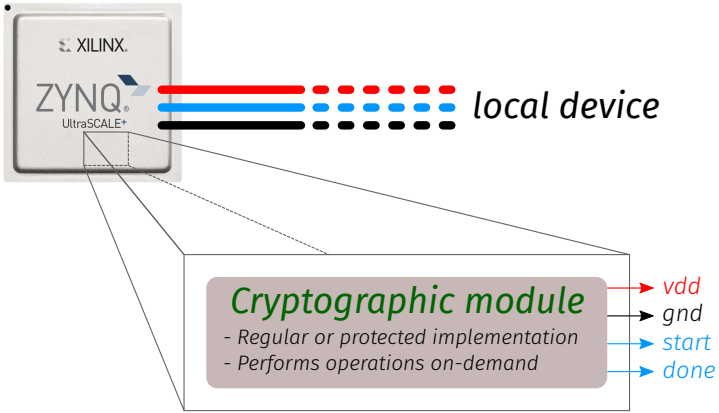
Courrège, JC., Feix, B., Roussellet, M., *Simple Power Analysis on Exponentiation Revisited*. In: Gollmann, D., Lanet, JL., Iguchi-Cartigny, J. (eds) Smart Card Research and Advanced Application. CARDIS 2010. Lecture Notes in Computer Science, vol 6035. Springer, Berlin, Heidelberg. 2010.

Differential Power Analysis, Correlation Power Analysis



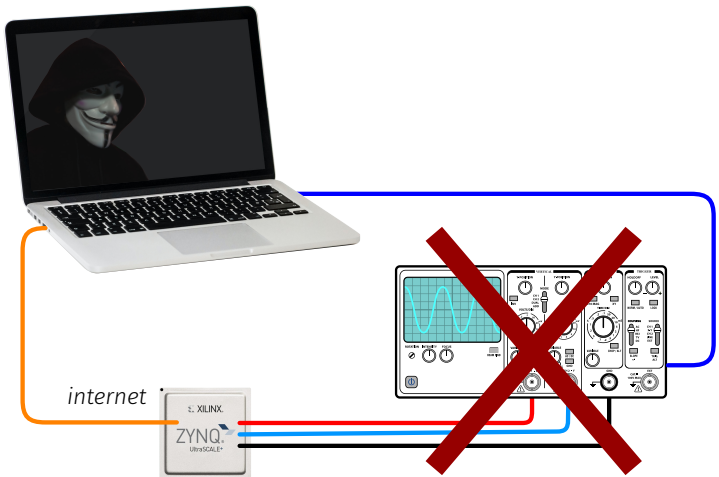
Owen Lo, William J. Buchanan, Douglas Carson, *Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)*, Journal of Cyber Security Technology, 1:2, 2017, pp. 88-107.

How are these traces captured?

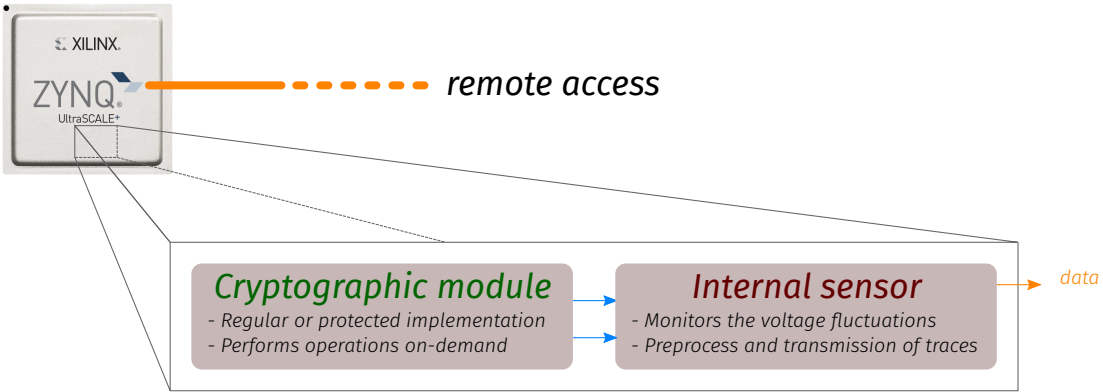


2 | Remote Power Analysis

Remote Power Analysis

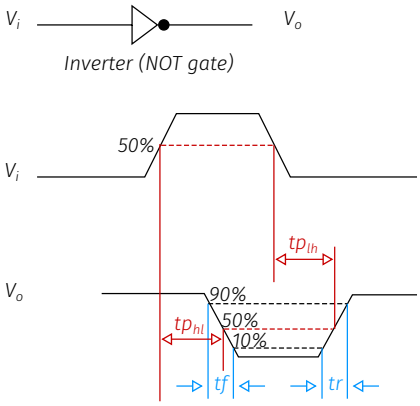


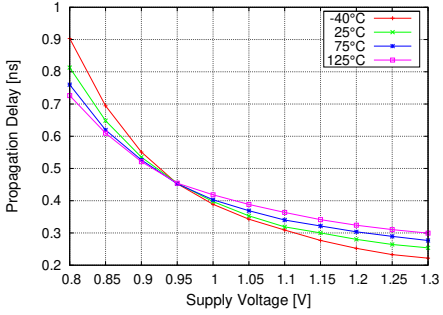
How are these traces captured?



F. Schellenberg, D. R. E. Gnad, A. Moradi and M. B. Tahoori, *An Inside Job: Remote Power Analysis Attacks on FPGAs*, in IEEE Design & Test, vol. 38, no. 3, pp. 58-66, June 2021.

Internal sensors

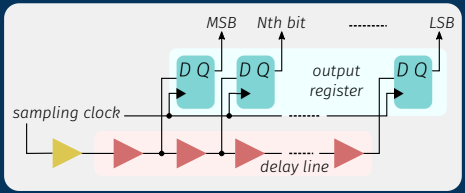




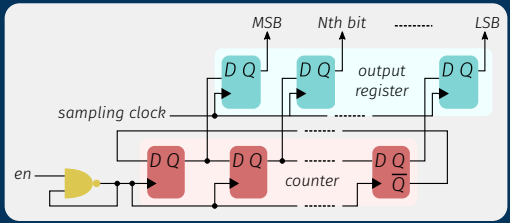
A. Sassone et al., *Investigating the effects of Inverted Temperature Dependence (ITD) on clock distribution networks*, 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012, pp. 165-166.

Internal sensors

Time-to-Digital Converters

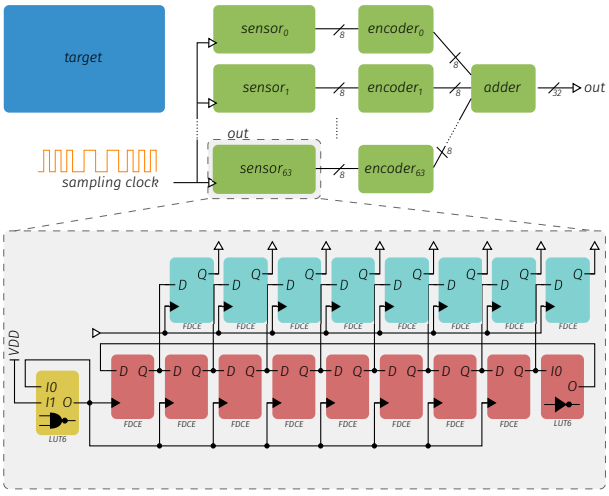


Based on ring oscillators

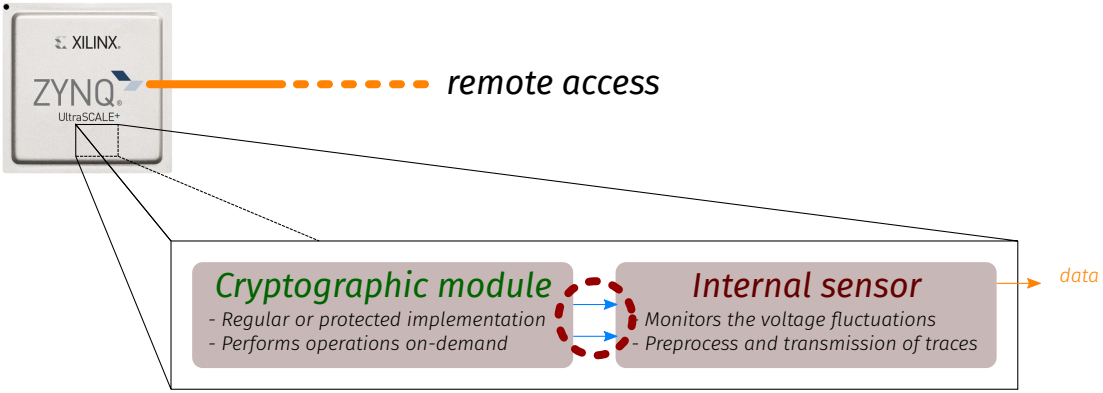


Gravellier, Joseph. *Remote Hardware Attacks on Connected Devices*. Dissertation. École des Mines de Saint-Étienne, 2021.

Ring Oscillator-based Sensors



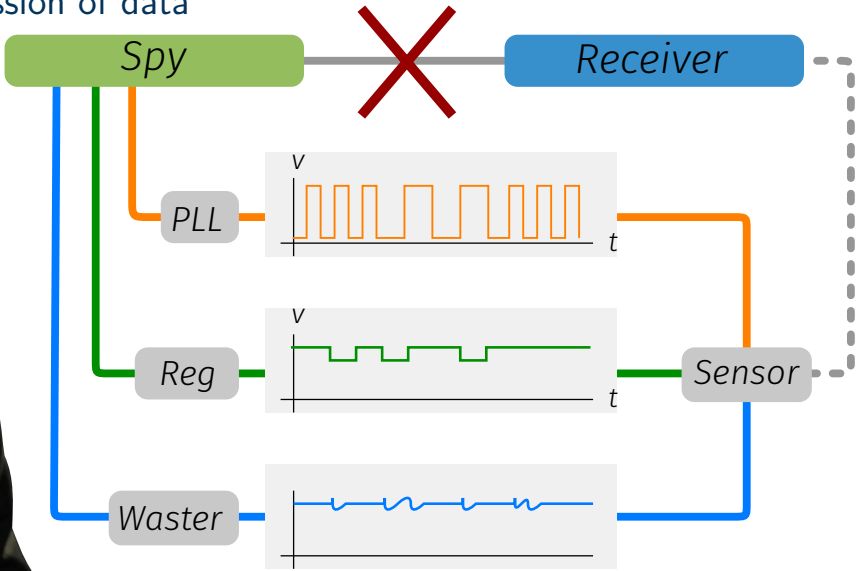
How are these traces captured?



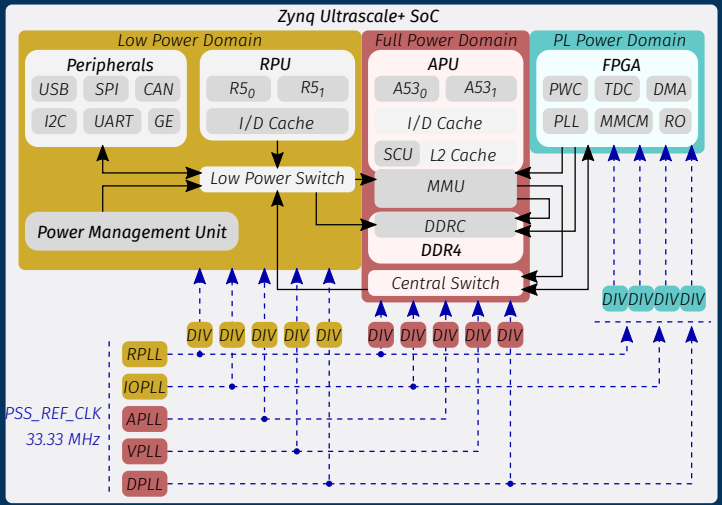
J. Gravellier, J. -M. Dutertre, Y. Teglia and P. Loubet-Moundi, *High-Speed Ring Oscillator based Sensors for Remote Side-Channel Attacks on FPGAs*, 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2019, pp. 1-8, doi: 10.1109/ReConFig48160.2019.8994789

3 | Covert Channels

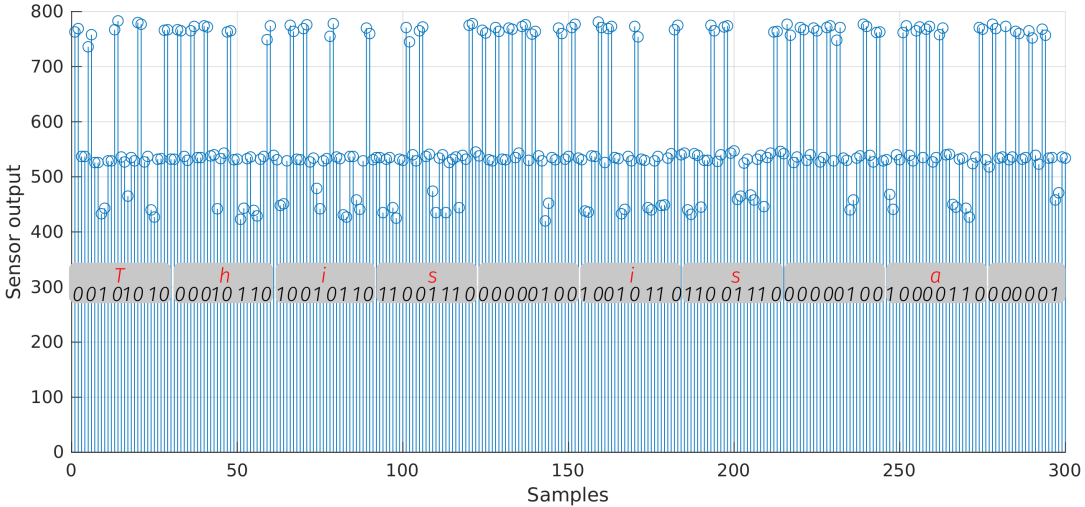
Covert transmission of data



Modifying the voltage and frequency of a chip

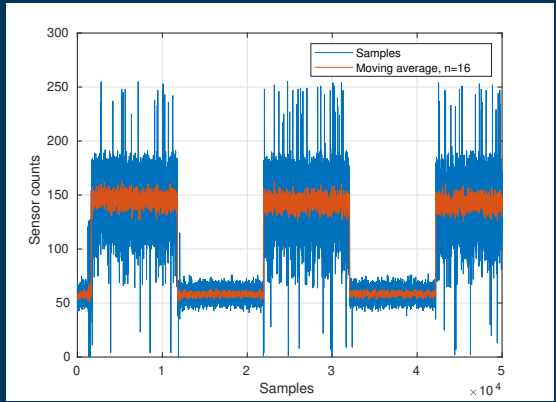


Frequency-based covert channels



How to use these covert channels in practice?

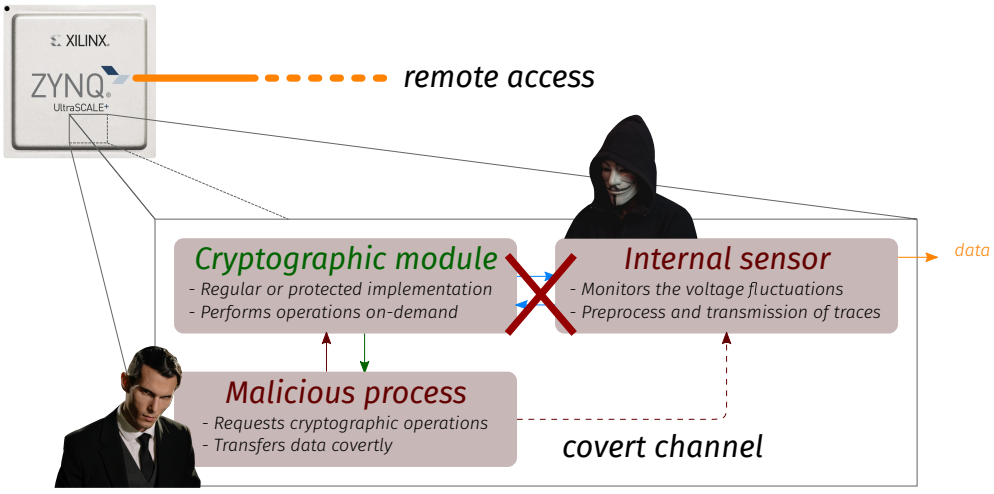
Require: f_1, f_2 a pair of sampling frequencies
  $f_{RO} = f_1$
  while TRUE **do**
    $f_{RO} \leftarrow f_{RO} = f_1 \quad ? \quad f_2 : f_1$
    `algorithm`(DATA)
  end while



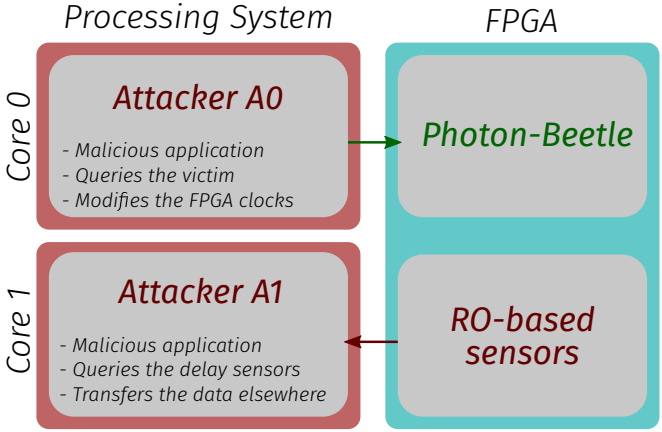
4 | Combined attacks

Remote Power Analysis + Covert Channel Attacks

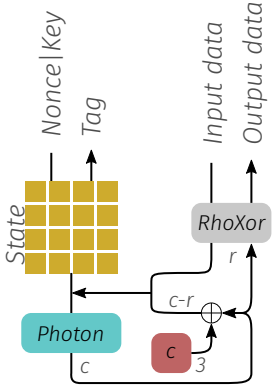
How are these traces captured?

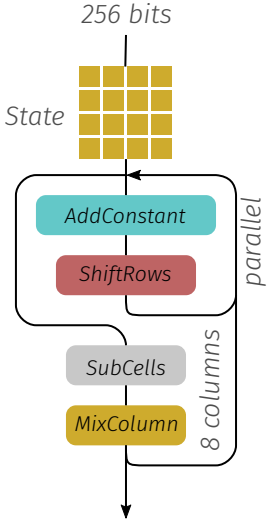


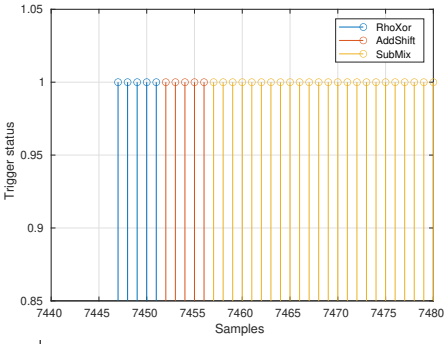
Threat model in practice



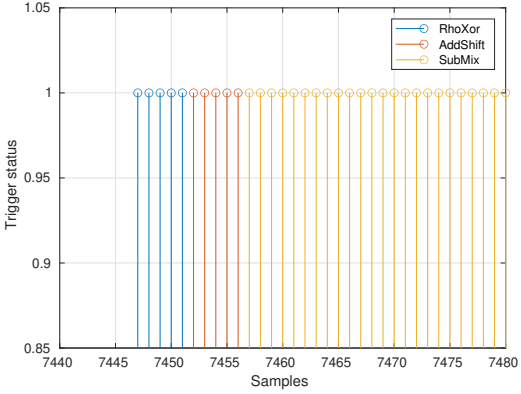
Case study: Photon-Beetle

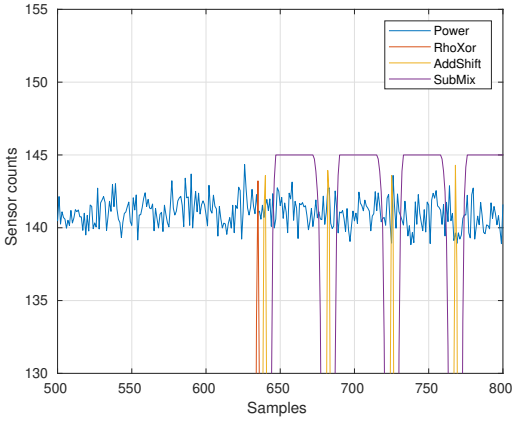




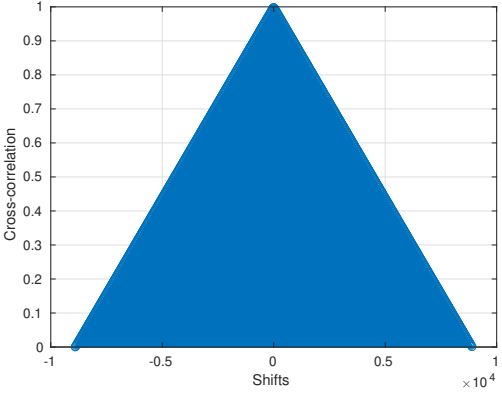


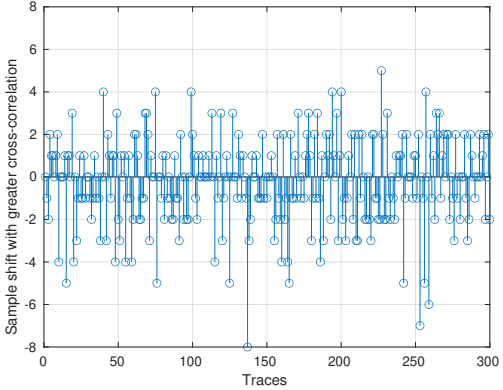
Automatic alignment of the signals





Is it really working?





5 | Conclusions and future work

In this work:

- We have proposed a novel approach to mitigate the need to use logical triggers in the acquisition of traces
- This improvement works towards demonstrating the factibility of remote power analysis attacks
- From our statistical analysis we have determined that the proposed technique achieves a correct alignment of 70-80% of the traces

Some things to come:

- Demonstrate that the proposed technique can be used in practical attacks
- Investigate covert channels under more strict threat models
- Improve the methodology to assess whether the traces are properly aligned (i.e. an exact method instead of cross-correlation)

UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

Laboratoire Hubert Curien

Lilian BOSSUET
Anis FELLAH-TOUTA
Carlos Andres LARA-NINO