Is information leakage spilling?

Lilian Bossuet, Vincent Grosso, Carlos Lara

19th International Workshop on Cryptographic Architectures Embedded in Logic Devices

Castro Urdiales, Spain

June 12, 2023

Université Jean Monnet Saint-Etienne, CNRS, Laboratoire Hubert Curien
UMR 5516, F-42023, SAINT-ETIENNE, France

Background

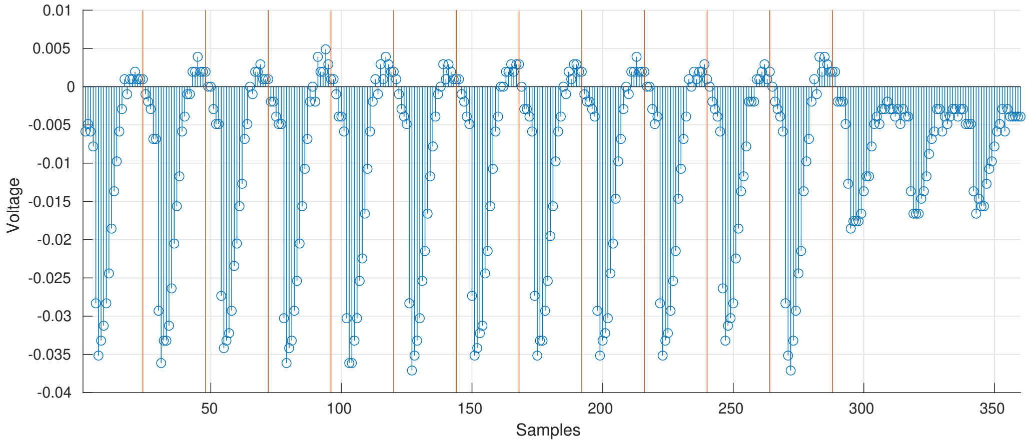
- Any computing device is, by nature, an agglomeration of physical phenomena
- there are magnitudes which can be seen and quantified when the system operates
- some of these measurements may be correlated with the data being processed[1]
  - power dissipation
  - electromagnetic emanation
  - clock frequency
  - heat dissipation
- these data can be leveraged by an attacker to compromise the security of the platform

[1] Mangard, S., Oswald, E., & Popp, T. Power analysis attacks: Revealing the secrets of smart cards (Vol. 31). Springer Science & Business Media.

- Electromagnetic and power traces are most commonly used to conduct SCAs on cryptographic algorithms[2]
- these magnitudes fluctuate quickly enough to give a good indicator of the status of the device
- sophisticated equipment is needed to capture the information

[2] Mangard, S., Oswald, E., & Popp, T. Power analysis attacks: Revealing the secrets of smart cards (Vol. 31). Springer Science & Business Media.

Power footprint



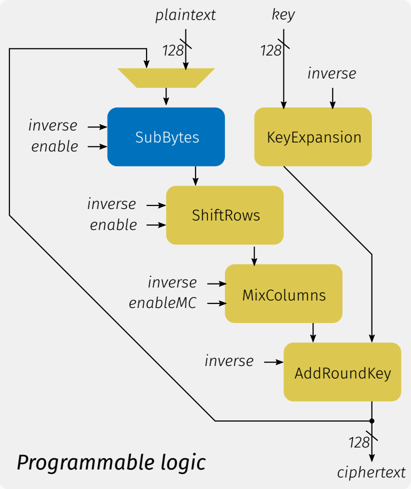
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7.

- The principle behind power analysis is to find a statistical relationship between an algorithm and a set of observations from its implementation[3]
- we assume that the data we seek to retrieve has an impact on the power footprint of the system
    - conditional operations
    - loads
    - stores

[3] Kocher, P., Jaffe, J., & Jun, B. Differential power analysis. In *Proceedings of the 19th Annual International Cryptology Conference* Santa Barbara, California, USA, August 15–19, 1999 (pp. 388-397). Springer Berlin Heidelberg.

Power Analysis Attacks (cont.)

- with a large set of observations we can test multiple hypotheses h_i and select the most likely to be correct
- to reduce the size of these hypotheses we target small fragments g_i of the secret data
- for example, an AES-128 key is divided into 16 8-bit fragments where each has 256 possible values
- there are multiple attacks which employ this strategy, but the best known ones are differential power analysis and correlation power analysis



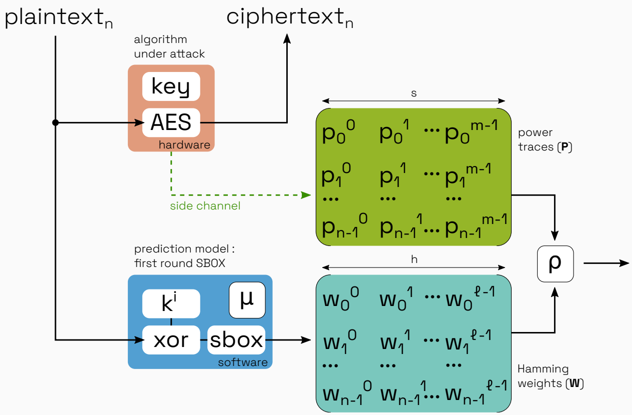
Require: M an array of n inputs/outputs processed with an algorithm under analysis E
Require: P an array $n \times m$ of power traces captured while processing of M
Ensure: G an array of guesses for the secret materials of E

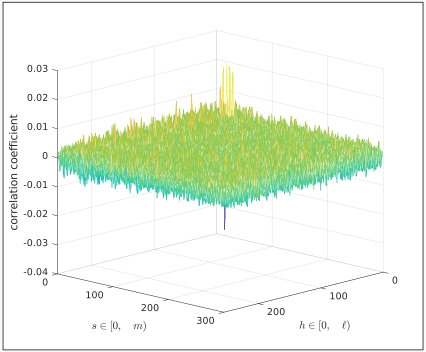
```
for g_i ∈ G do
    for h = 0 to ℓ − 1 do
        W^h = ω(μ(M^{g_i}, h))                {ω : Hamming weight; μ : Leakage model}
        for s = 0 to m − 1 do
            Q_s^h ← ρ(W^h, P^s)               {ρ : Correlation between two vectors of n elements}
        end for
    end for
    g_i ← max(|Q|)                            {Select the hypothesis with the greatest correlation coefficient in any sample}
end for
```

[4]

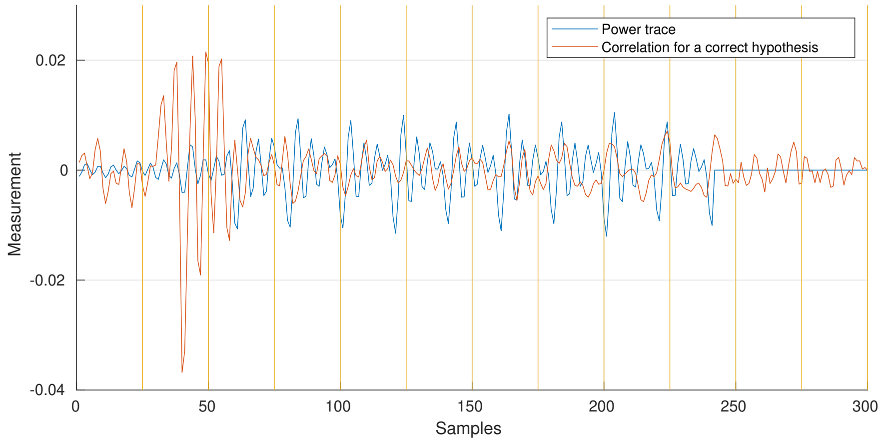
[4] Brier, E., Clavier, C., & Olivier, F. Correlation power analysis with a leakage model. In *Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems* Cambridge, MA, USA, August 11-13, 2004. (pp. 16-29). Springer Berlin Heidelberg.

Correlation Power Analysis : first round SBOX



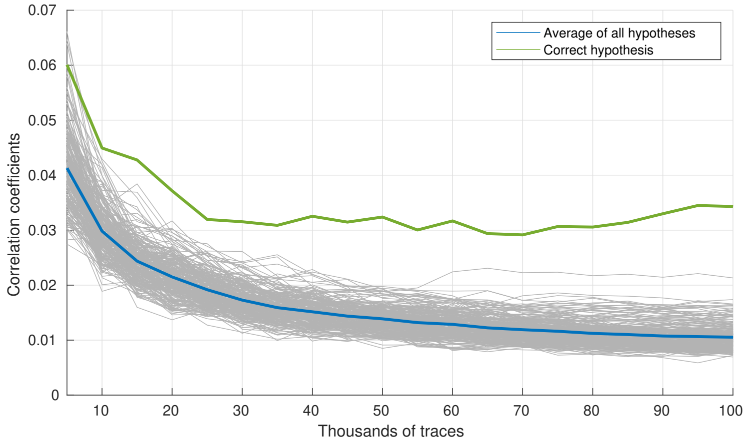


Correlation Power Analysis : first round SBOX



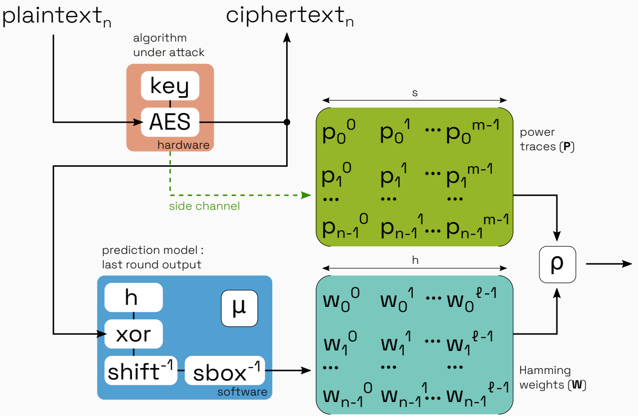
Setup : TDC @ 250 MHz, iterative AES @ 10 MHz, Zynq-7000, 100K traces.

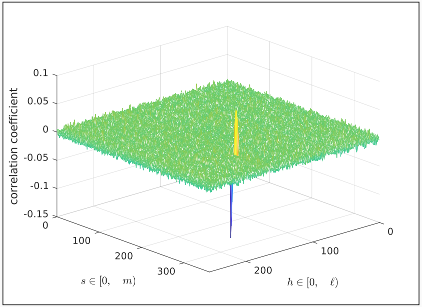
Correlation Power Analysis : first round SBOX

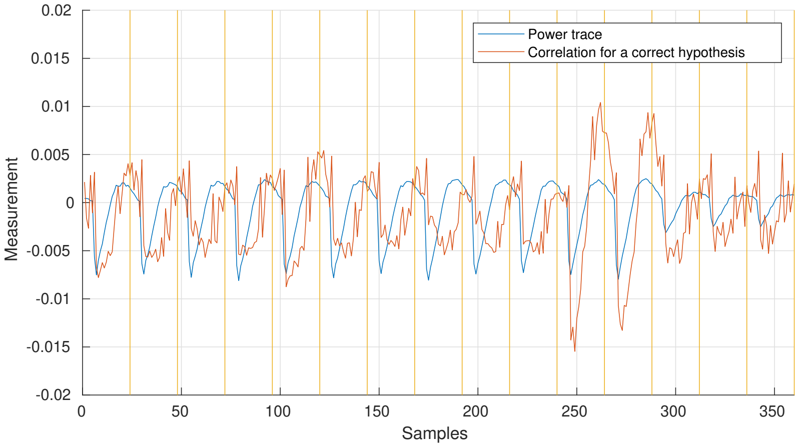


Setup : TDC @ 250 MHz, iterative AES @ 10 MHz, Zynq-7000.

Correlation Power Analysis : last round output

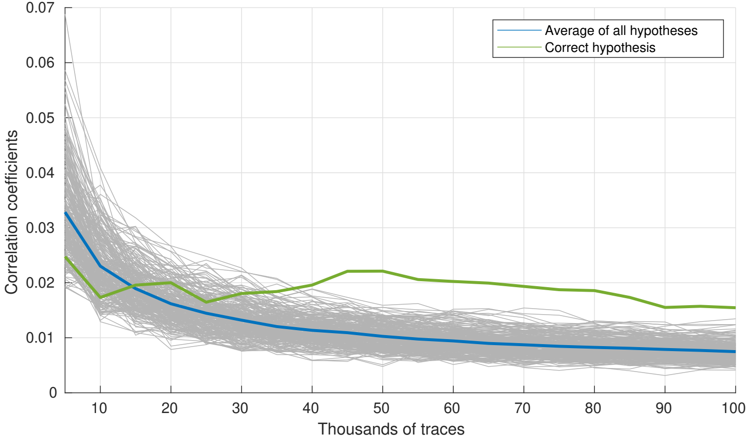






Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 100K traces.

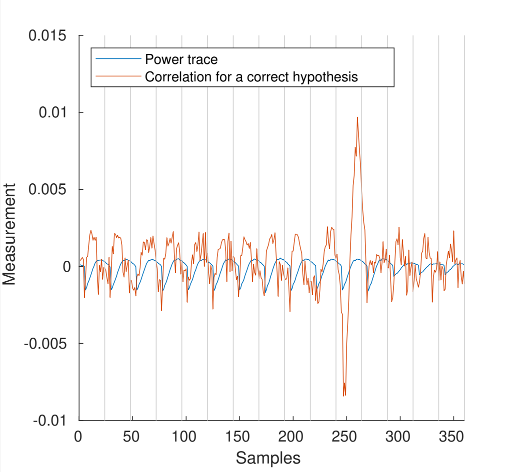
Correlation Power Analysis : last round output

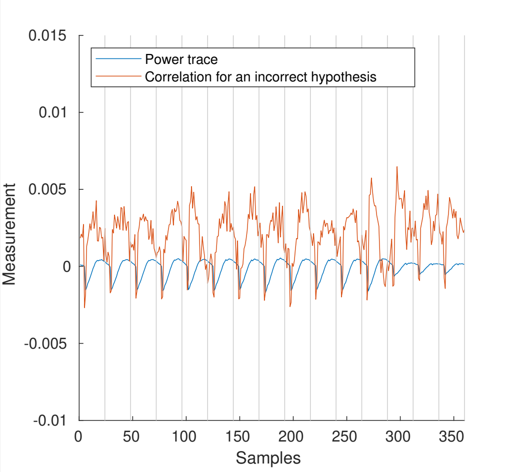


Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7.

A: An area estimator for CPA

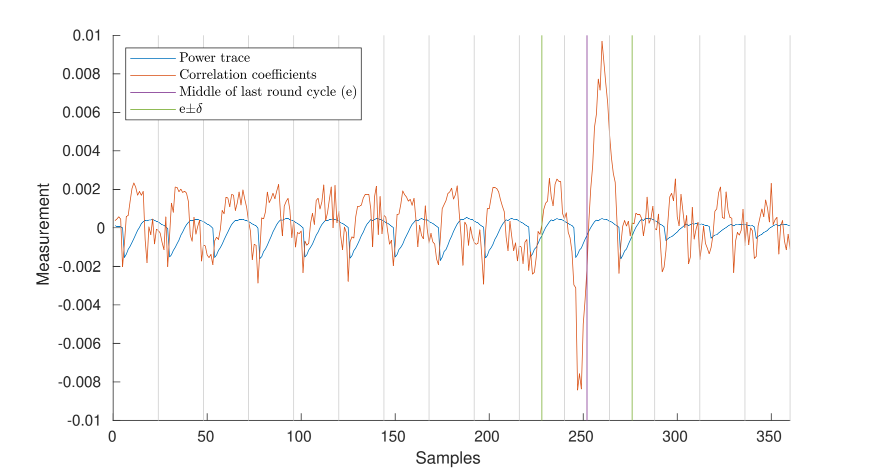
Looking closer at the hypotheses





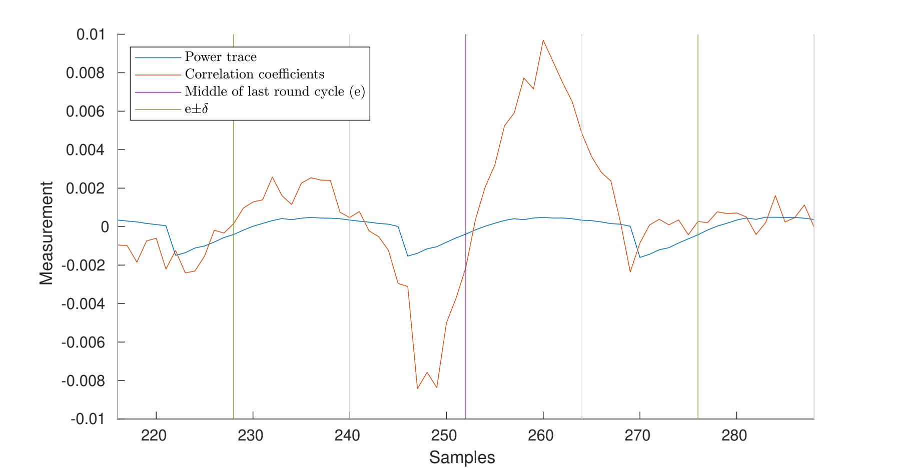
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces.

Correlation behavior for a correct hypothesis



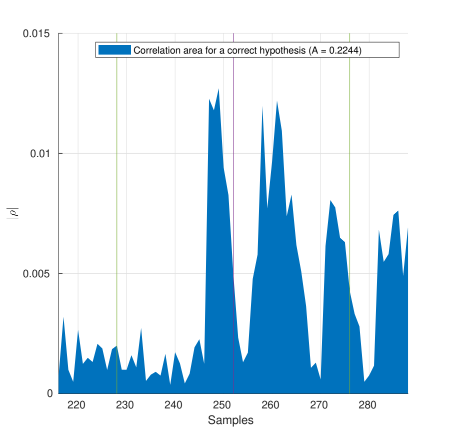
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces.

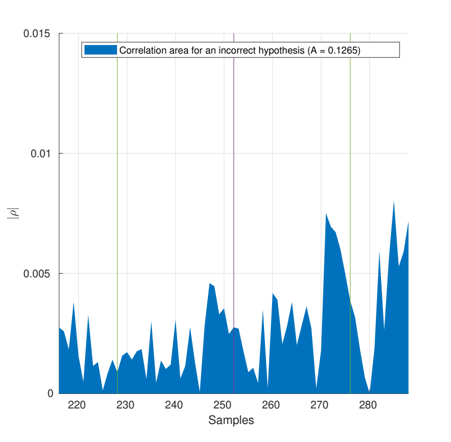
Enhance!



Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces.

Looking closer at the hypotheses (cont.)





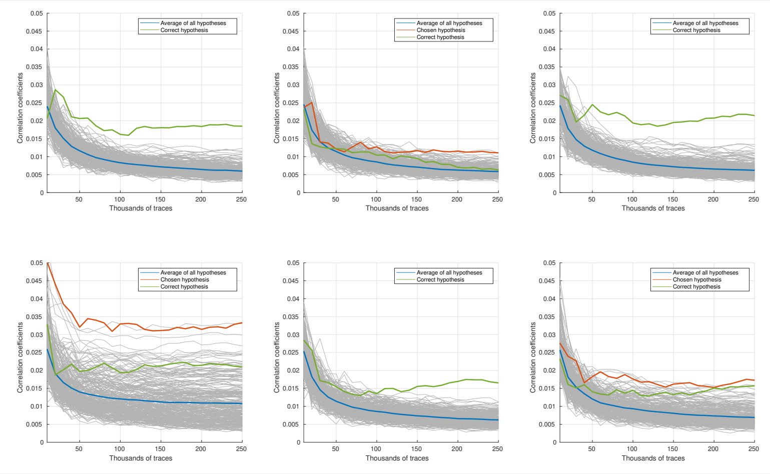
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces.

Correlation Power Analysis revisited

Require: M an array n of inputs/outputs processed with an algorithm under analysis E
Require: P an array $n \times m$ of power traces captured while processing of M
Require: e the sample with the expected greater correlation
Require: f, f_s the frequencies of the target and the sensor, respectively
Ensure: G an array of guesses for the secret materials of E

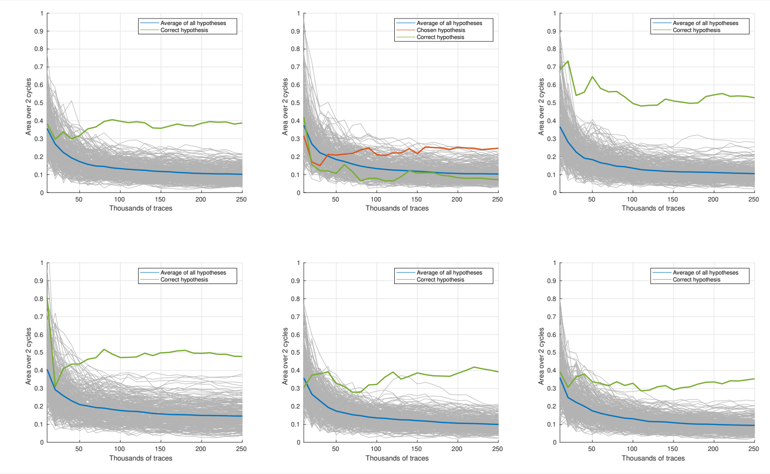
```
δ ← f_s/f                                {δ : Samples per cycle of the target}
for g_i ∈ G do
    for h = 0 to ℓ do
        W^h = ω(μ(M^{g_i}, h))           {ω : Hamming weight; μ : Leakage model}
        for s = e − δ to e + δ do
            Q^s ← ρ(W^h, P^s)            {ρ : Correlation between two vectors of n elements}
        end for
        A^h ← Σ(|Q^s − Q̄^s|)            {Center and solve as a Riemann sum}
    end for
    g_i ← max(A)                         {Select the hypothesis with the greatest area}
end for
```

Demo 1 : CPA results



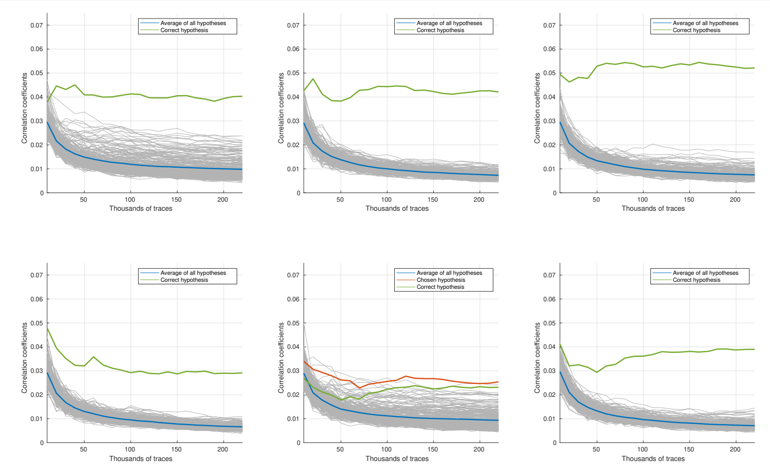
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces, LRM.

Demo 1 : improved CPA results



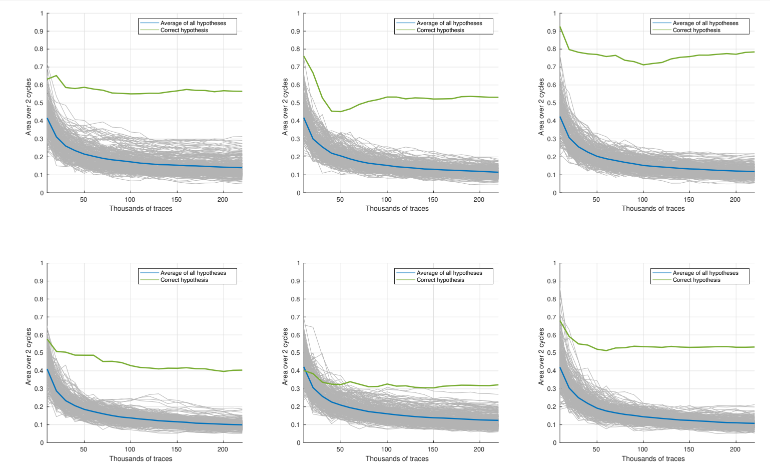
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces, LRM.

Demo 2 : CPA results (different sensor, different target)



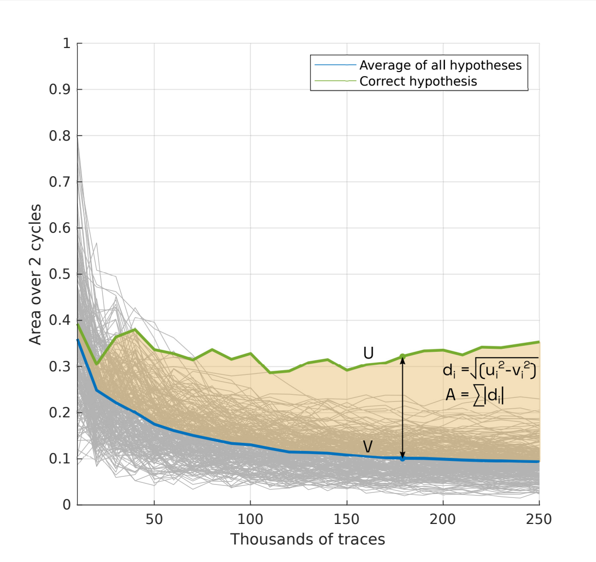
Setup : TDC @ 250 MHz, iterative AES @ 10 MHz, Zynq-7000, 220k traces, LRM.

Demo 2 : improved CPA results (different sensor, different target)

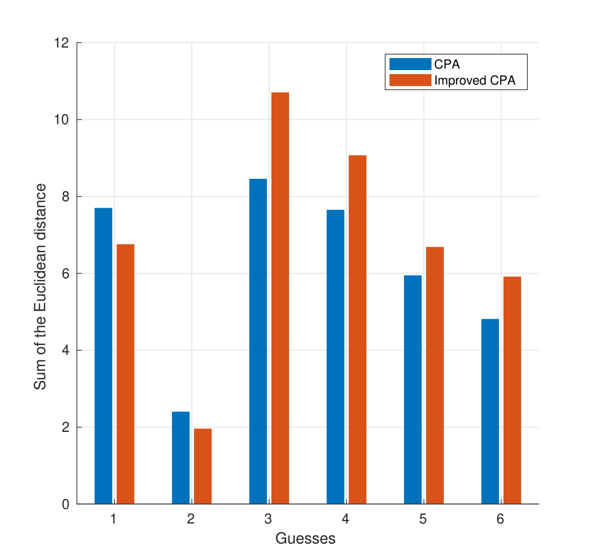


Setup : TDC @ 250 MHz, iterative AES @ 10 MHz, Zynq-7000, 220k traces, LRM.

Quantifying the improvement



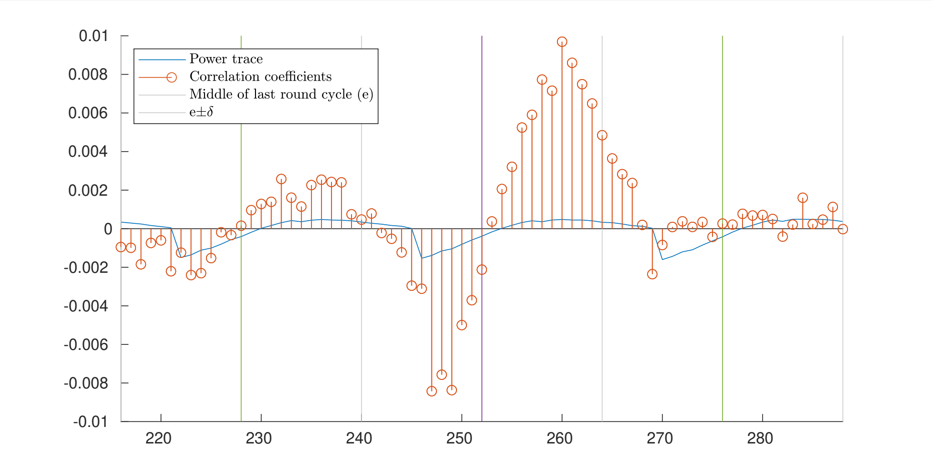
Quantifying the improvement (cont.)



B: Bolstering the correlation area

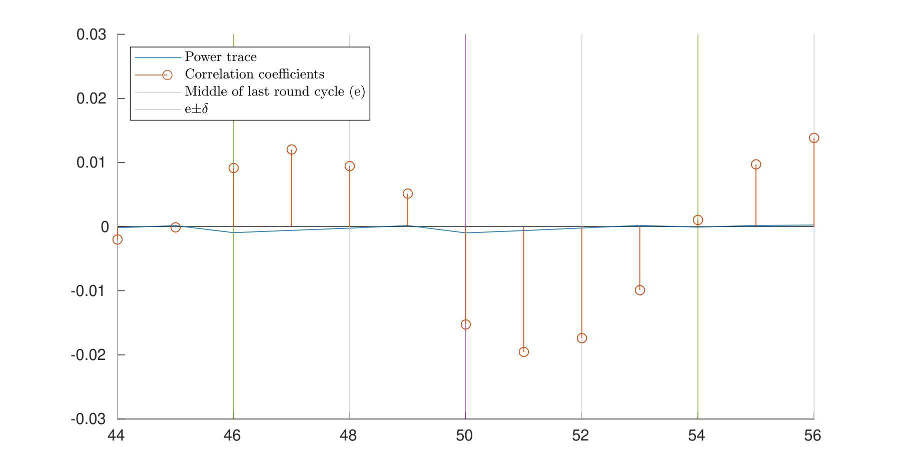
Effects of the sampling frequency

24 samples per cycle



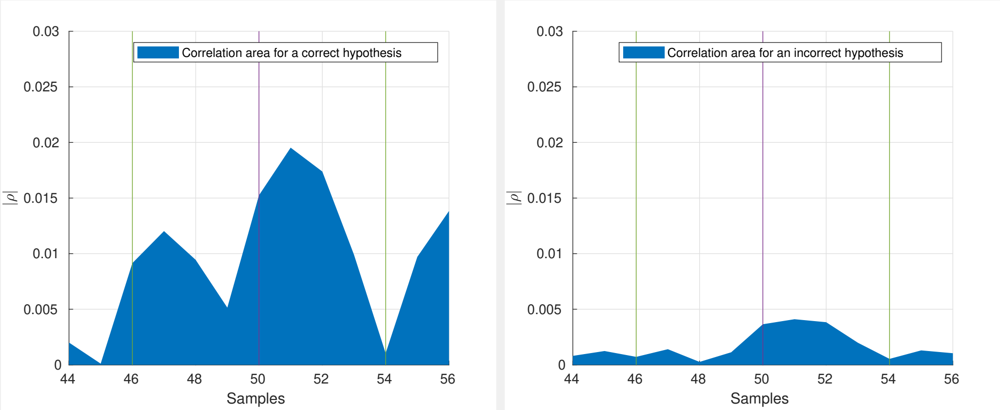
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces.

4 samples per cycle



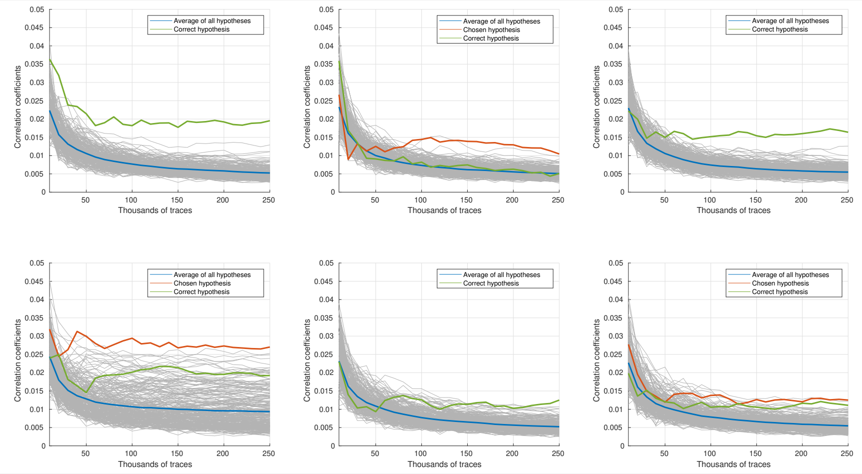
Setup : ChipWhisperer Lite @ 40 MHz, iterative AES @ 10 MHz, Artix-7, 250k traces.

4 samples per cycle



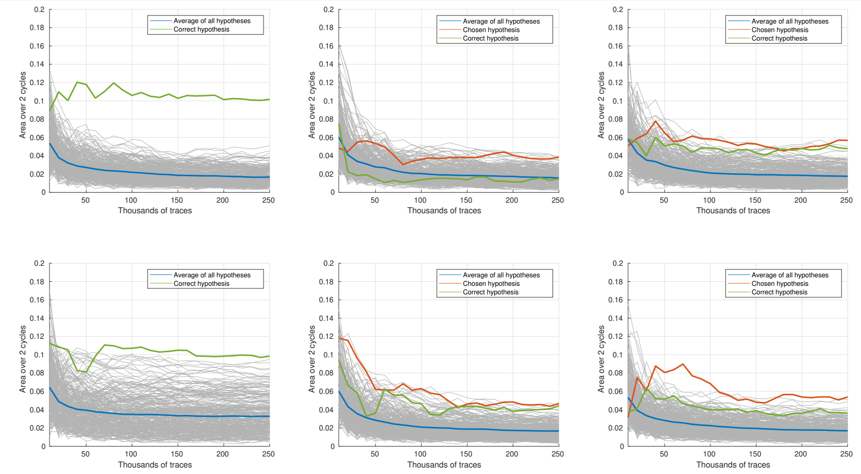
Setup : ChipWhisperer Lite @ 40 MHz, iterative AES @ 10 MHz, Artix-7, 250k traces.

Demo 3 : CPA results (4 samples per cycle)



Setup : ChipWhisperer @ 40 MHz, iterative AES @ 10 MHz, Artix-7, 250k traces, LRM.

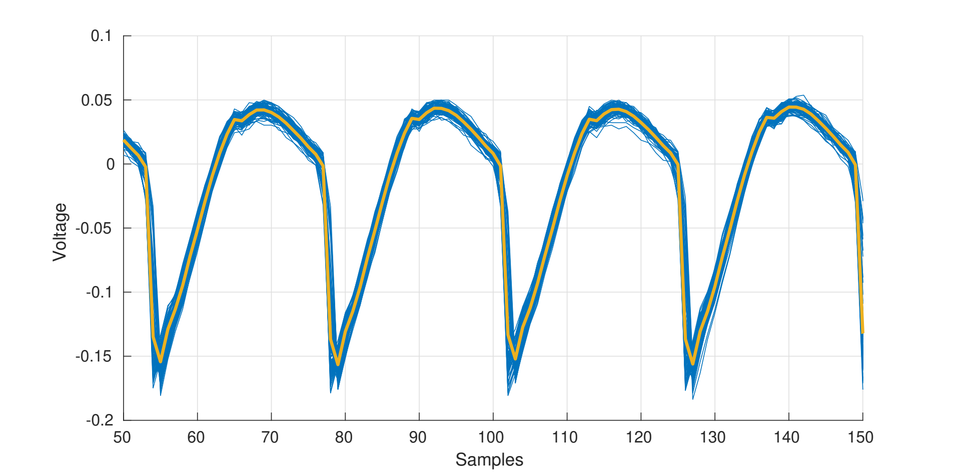
Demo 3 : improved CPA results (4 samples per cycle)



Setup : ChipWhisperer @ 40 MHz, iterative AES @ 10 MHz, Artix-7, 250k traces, LRM.

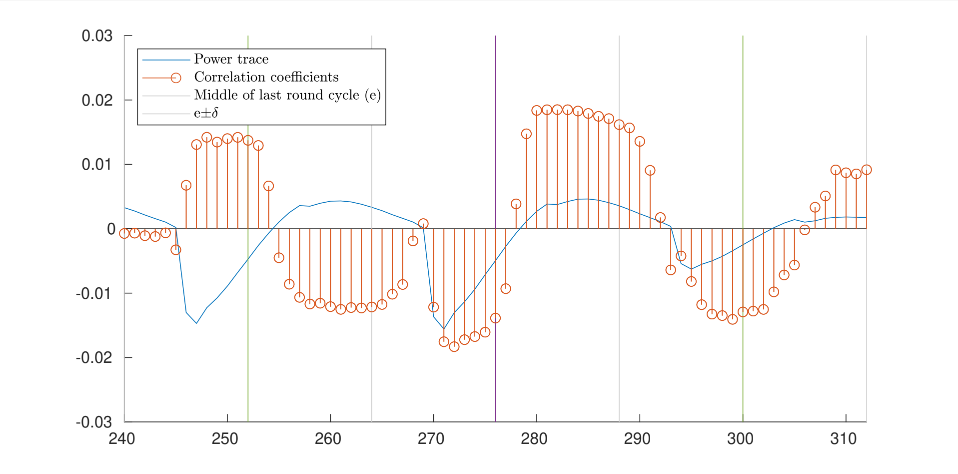
Effects of the noise

Averaging 100 traces



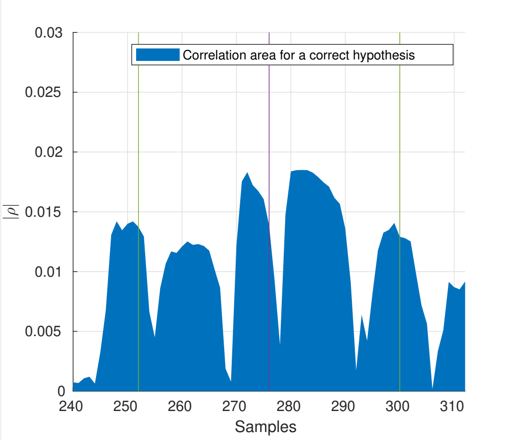
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces.

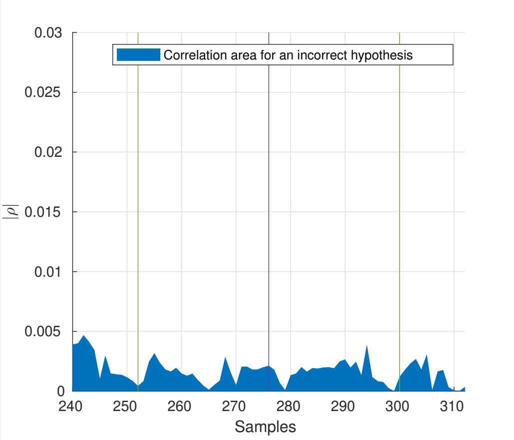
Averaging 100 traces



Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces.

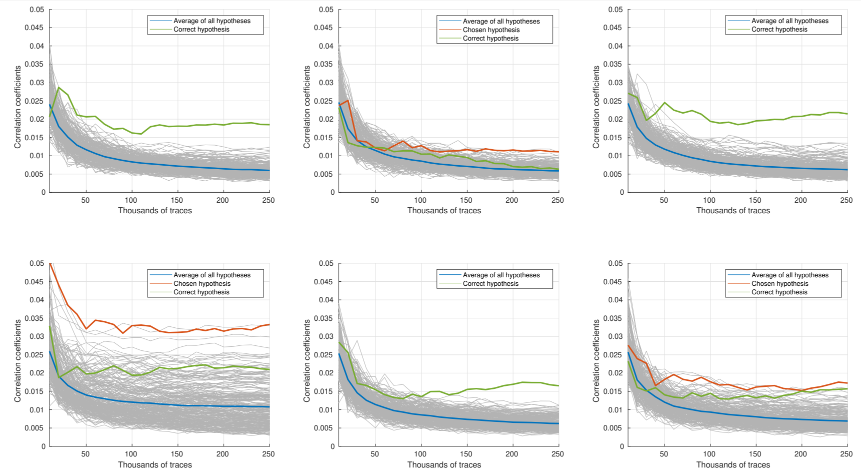
Averaging 100 traces





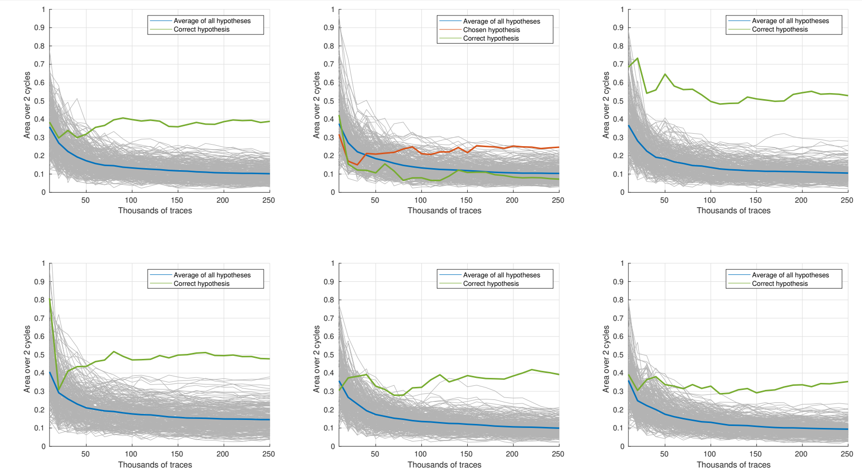
Setup : ChipWhisperer Lite @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces.

Demo 4 : CPA results (average of 100 traces)



Setup : ChipWhisperer @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces, LRM, average of 100 traces.

Demo 4 : improved CPA results (average of 100 traces)



Setup : ChipWhisperer @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces, LRM, average of 100 traces.

Effects of the jitter

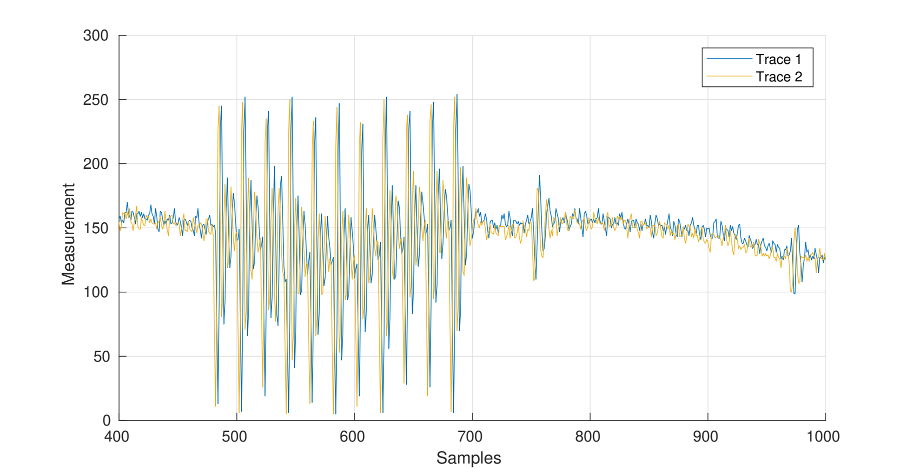
Miss-aligned traces

- Under certain scenarios the acquisition of traces is not perfectly synchronized[5]
- This introduces a jitter in the traces which affects CPA
- However, we suspect that this phenomenon can be leveraged to increase the correlation area
- Miss-aligned traces are bound to bundle together and produce a spill in the correlation matrix

---

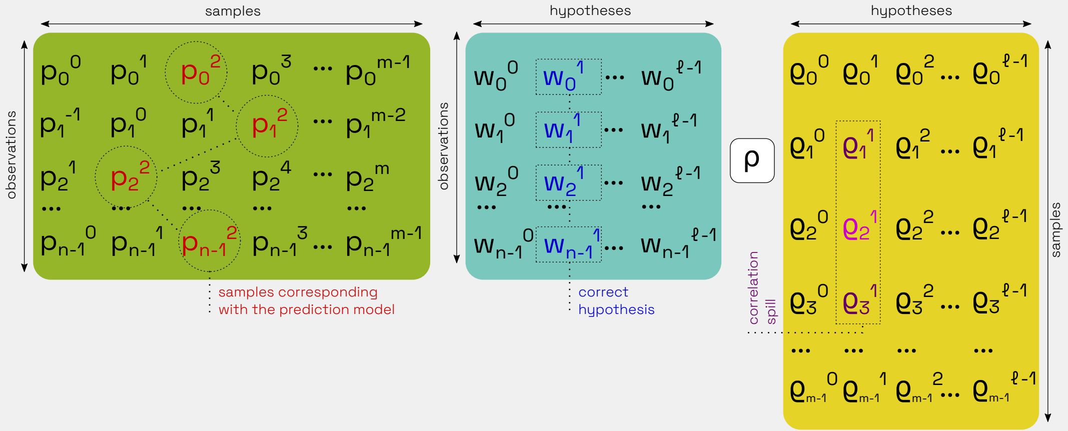
[5] Fellah-Touta, A., Bossuet, L. & Lara-Nino, C. A. Combined Internal Attacks on SoC-FPGAs: Breaking AES with Remote Power Analysis and Frequency-based Covert Channels. To appear in *Proceedings of the 8th IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Delft, The Netherlands, July 3, 2023. (pp. 1–7). IEEE.

Miss-aligned traces (cont.)



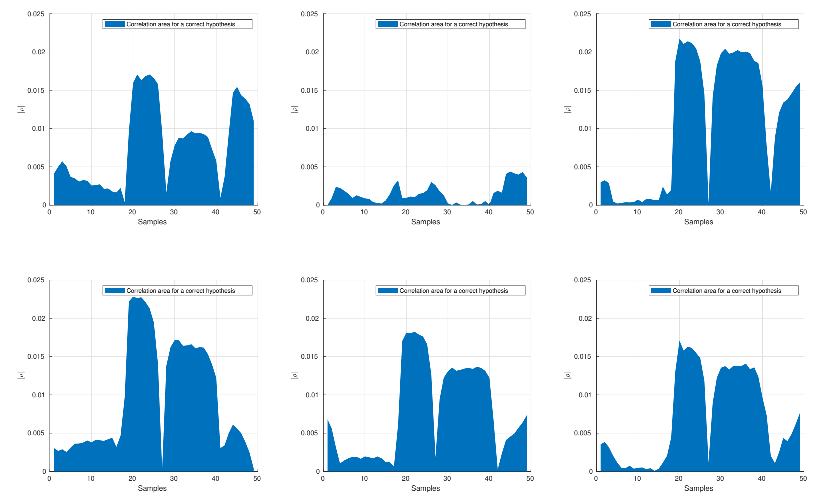
Setup : TDC @ 200 MHz, iterative AES @ 10 MHz, Zynq-7000.

Correlation spill

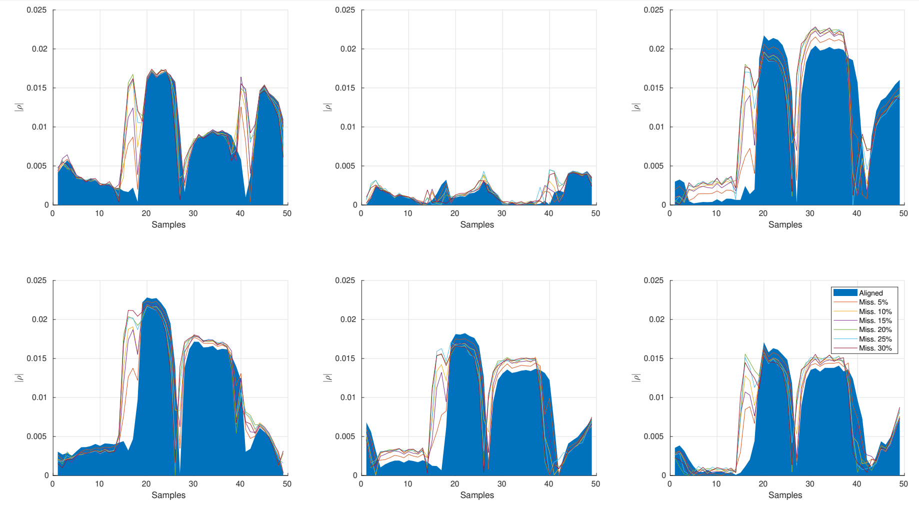


s

Average of 100 traces

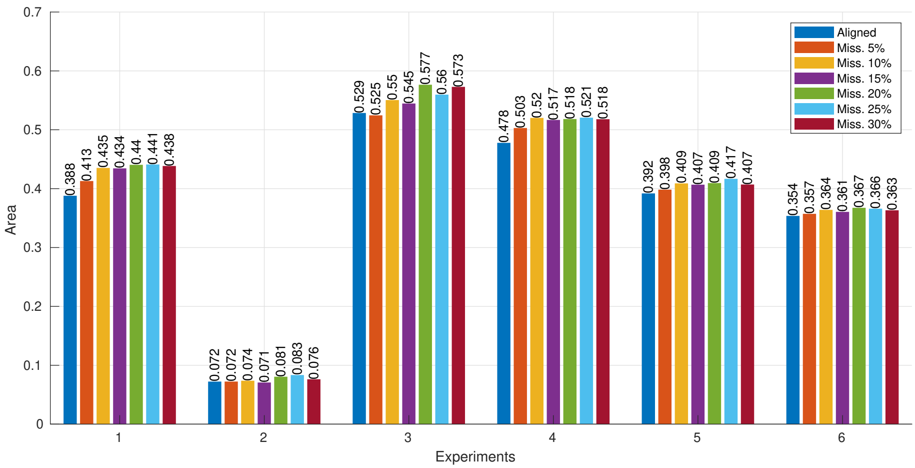


Intentionally miss-aligning some traces (by 4 samples)



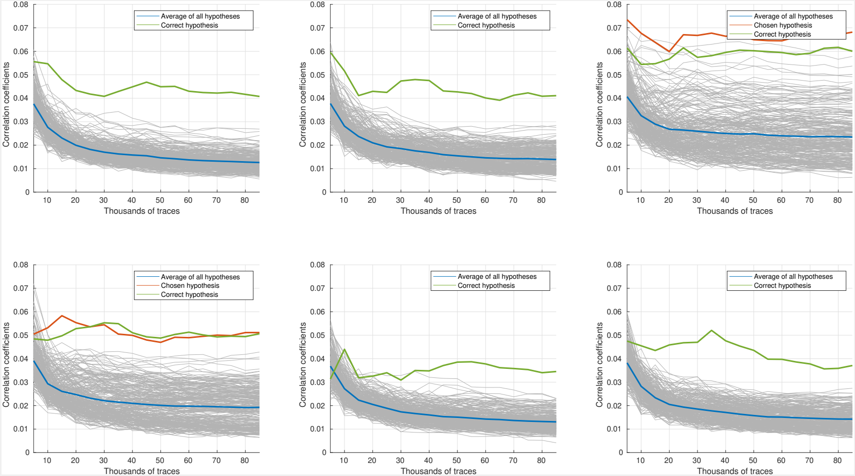
Setup : ChipWhisperer @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces, average of 100 traces.

Intentionally miss-aligning some traces (by 4 samples)



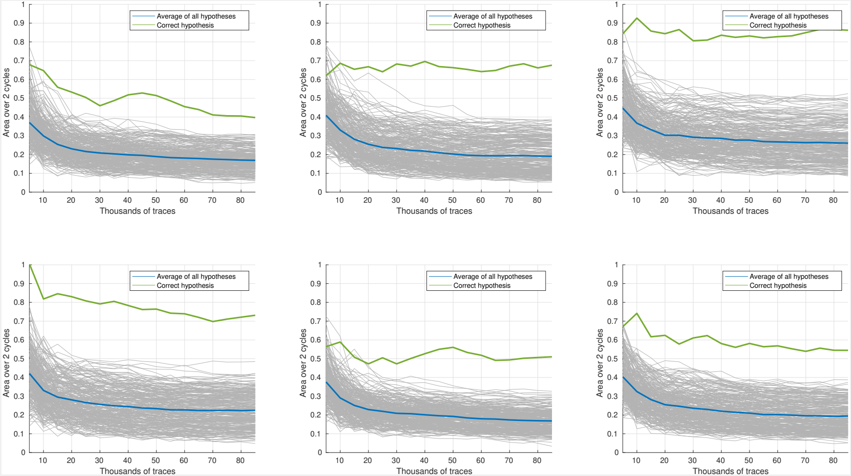
Setup : ChipWhisperer @ 96 MHz, iterative AES @ 4 MHz, Artix-7, 250k traces, average of 100 traces.

Demo 5 : CPA results (trigger-less traces)



Setup : TDC @ 200 MHz, iterative AES @ 10 MHz, Zynq-7000, 85k traces, FRM, average of 100 traces.

Demo 5 : improved CPA results (trigger-less traces)



Setup : TDC @ 200 MHz, iterative AES @ 10 MHz, Zynq-7000, 85k traces, FRM, average of 100 traces.

Final remarks

- We have proposed a new estimator for improving the performance of CPA
- Our approach relies on leveraging the information from lateral samples in the correlation matrix
- Pros : Improve the selection of the correct hypotheses
- Cons : If CPA does not work, it will not work. If CPA is good enough, you don't need this.

Acknowledgments

This work has been supported by the French government through the *Agence Nationale de la Recherche* in the framework of the *France 2030* initiative under project ARSENE (ANR-22-PECY-0004).

Thanks !