From Theory to Practice of Horizontal Attacks on Modular Exponentiation

DIOP Ibrahima, **LIARDET** Pierre-Yvan, **LINGE** Yanis,
ORDAS Thomas and **MAURINE** Philippe

Crypt-Archi Workshop,
Montpellier - La Grande-Motte
June 21-24, 2016.

life.augmented

cea

LIRMM

MINES Saint-Étienne

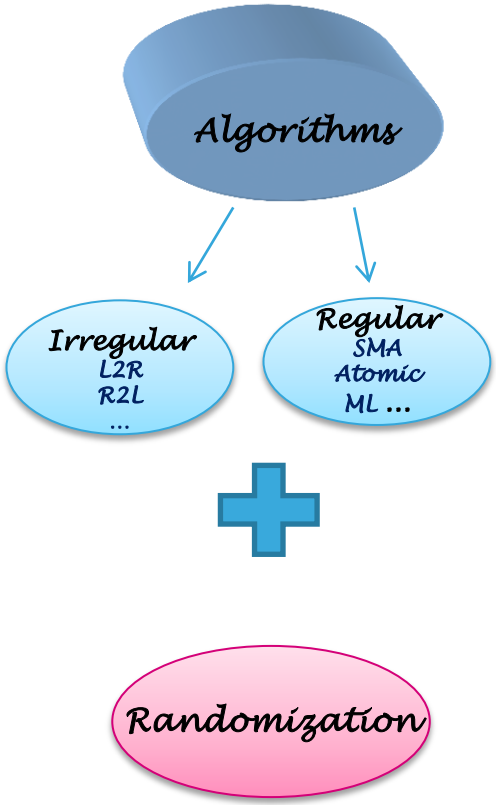
Introduction

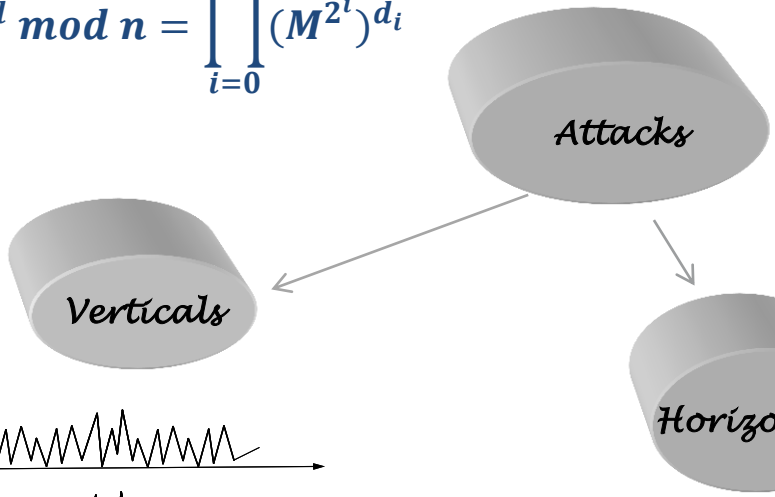
Horizontal Attacks in Practice

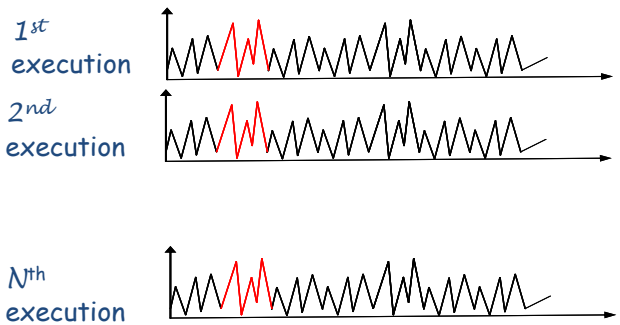
State of the Art

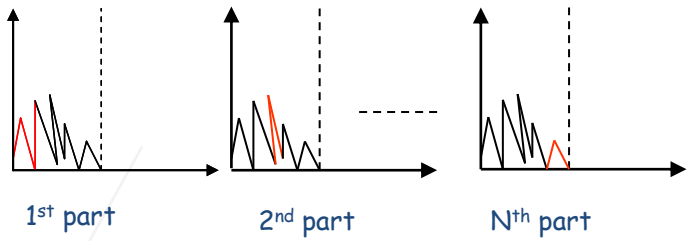
- ***Modular Exponentiation***:

$$M^d \bmod n = \prod_{i=0}^{k-1} (M^{2^i})^{d_i}$$



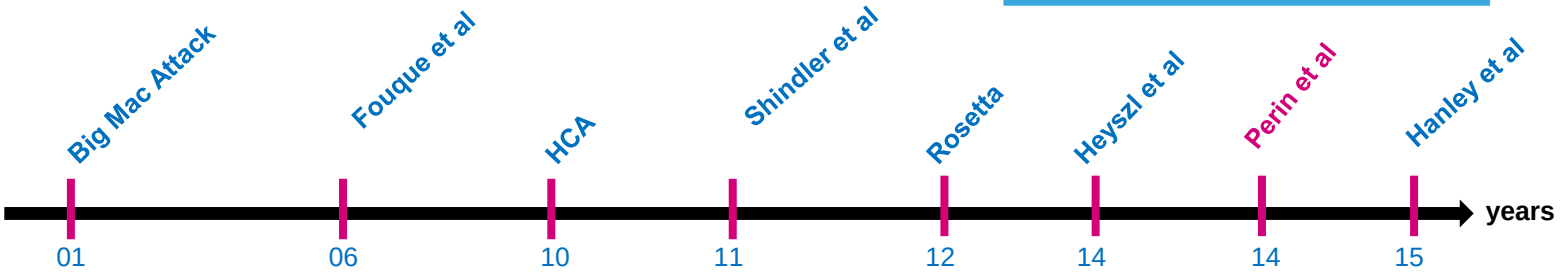






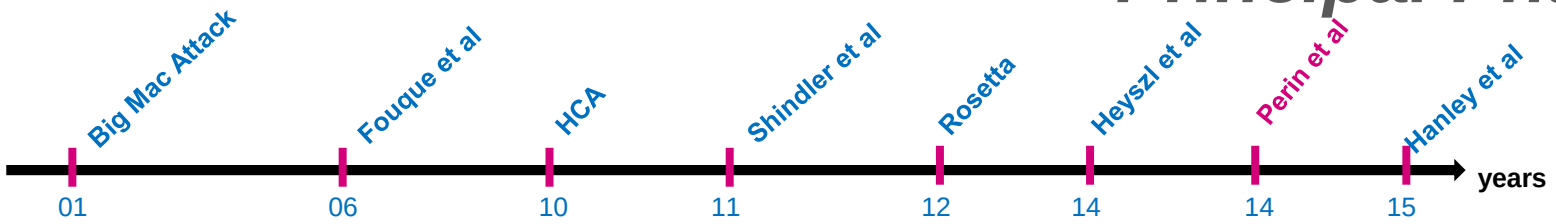
- Several Acquisitions
- Treatment : traces

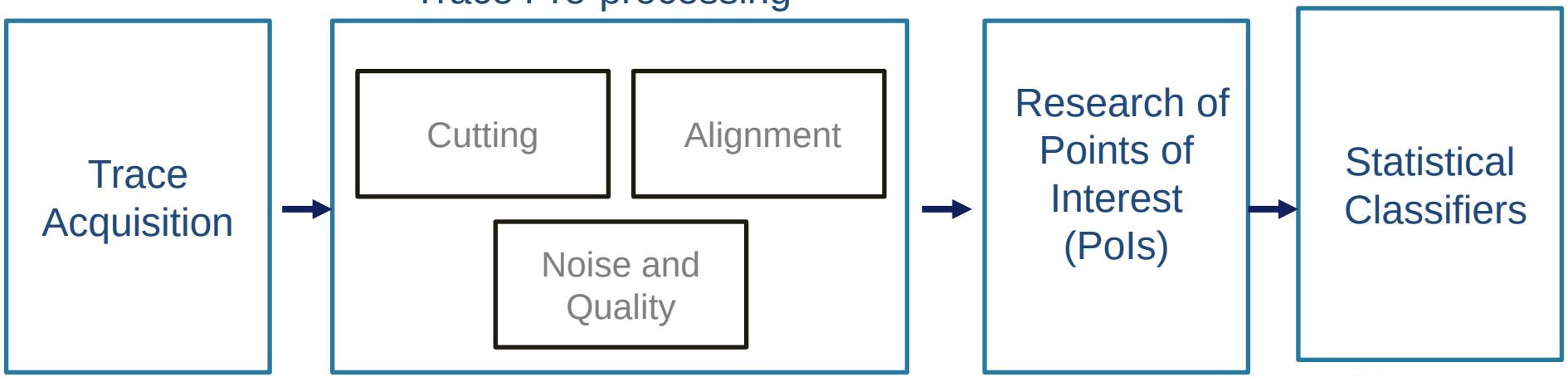
- Single Acquisition
- Treatment : parts of trace



Horizontal Attacks in Practice

Principal Phases

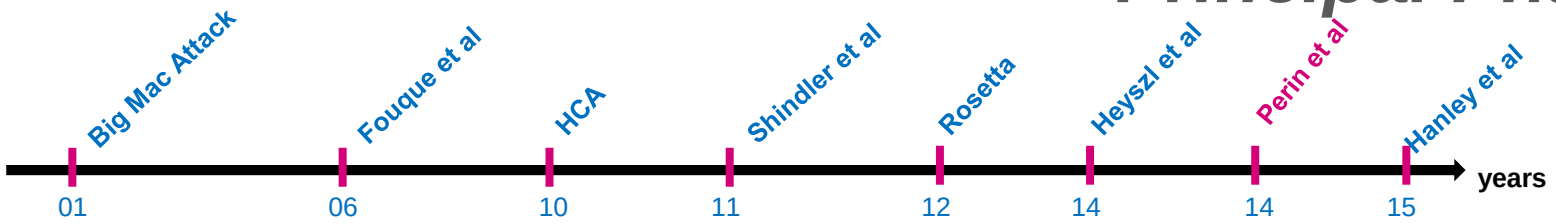


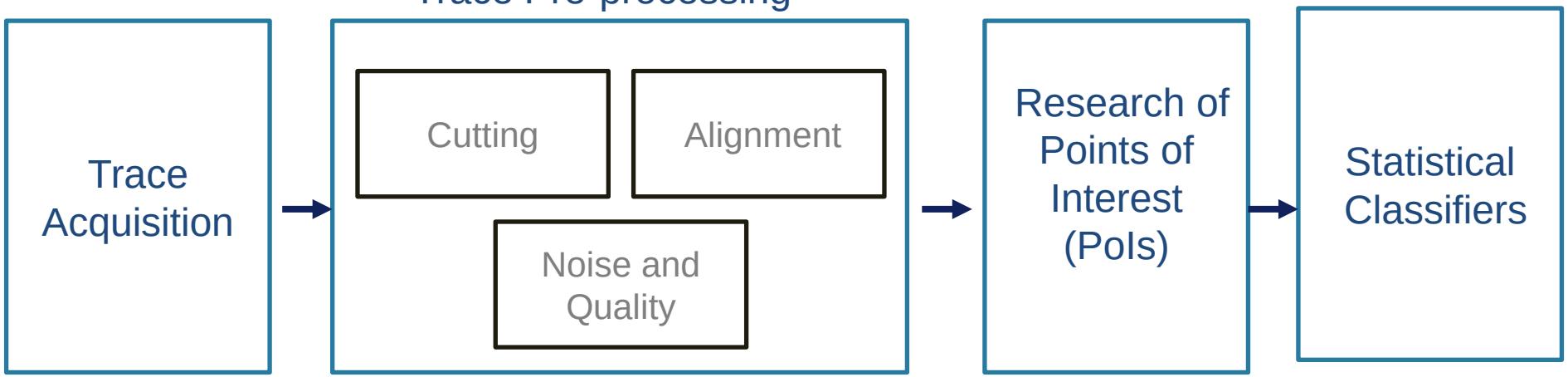


- Several works for each step in the literature

Horizontal Attacks in Practice

Principal Phases





- Several works for each step in the literature But …
  - Difficult in Practice

Trace Acquisition

Trace Pre-processing

Cutting

Alignment

Noise and Quality

Research of Points of Interest (PoIs)

Statistical Classifiers

life.augmented

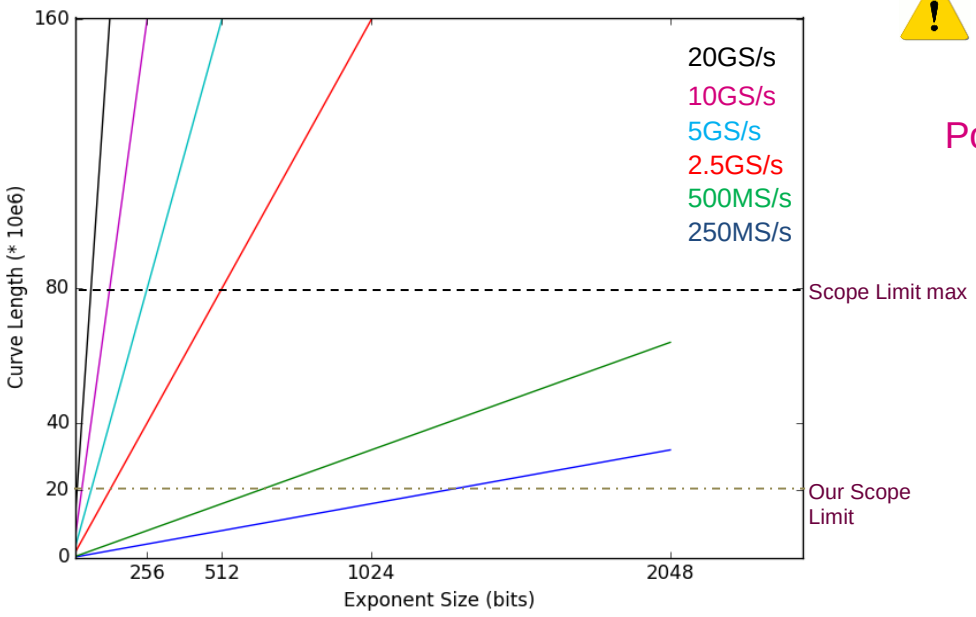
cea

LIRMM

MINES Saint-Étienne

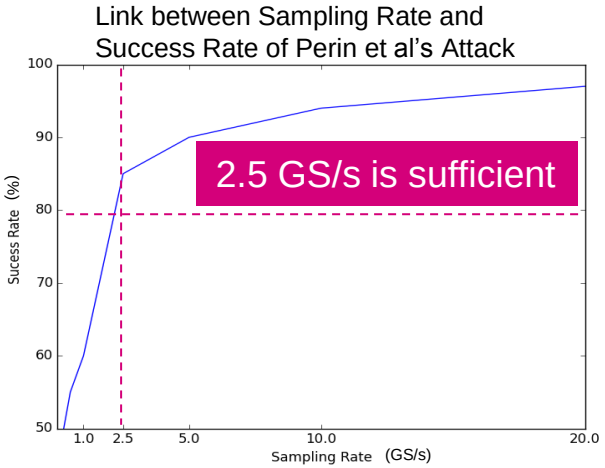
Horizontal Attacks in Practice
Trace Aquisition

- Example of Perin et al's Attack
  - Setup
    - Sampling Rate: 20GS/s ➔ > 1 billion Samples for an 1024-bits Exponent and Data (Message, Modulo)



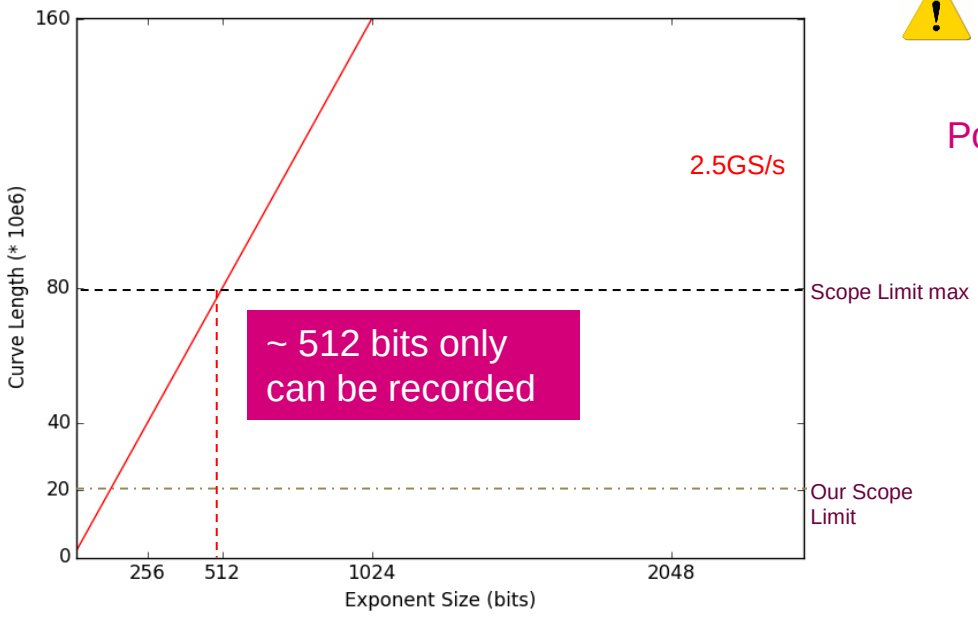
⚠ ➔ Scope Limitation (Only 40 bits can be recorded)

➔ Possible Solution: Decrease the sampling rate



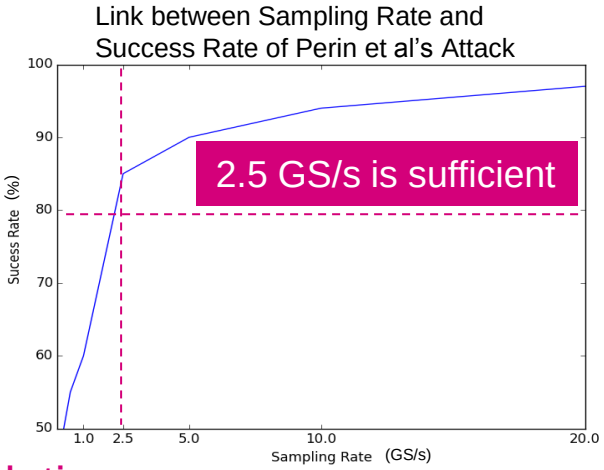
Horizontal Attacks in Practice
Trace Aquisition

- Example of Perin et al's Attack
  - Setup
    - Sampling Rate: 20GS/s ➔ > 1 billion Samples for an 1024-bits Exponent and Data (Message, Modulo)



⚠ ➔ Scope Limitation (Only 40 bits can be recorded)

Possible Solution: Decrease the sampling rate



⚠ Size Exponent must be greater or equal to 1024

- Solution:
  - Scope in Parallel
  - Smart Triggering

life.augmented

LIRMM

MINES Saint-Étienne

Trace Pre-processing

Trace Acquisition

Cutting

Alignment

Noise and Quality

Research of Points of Interest (PoIs)

Statistical Classifiers

life.augmented

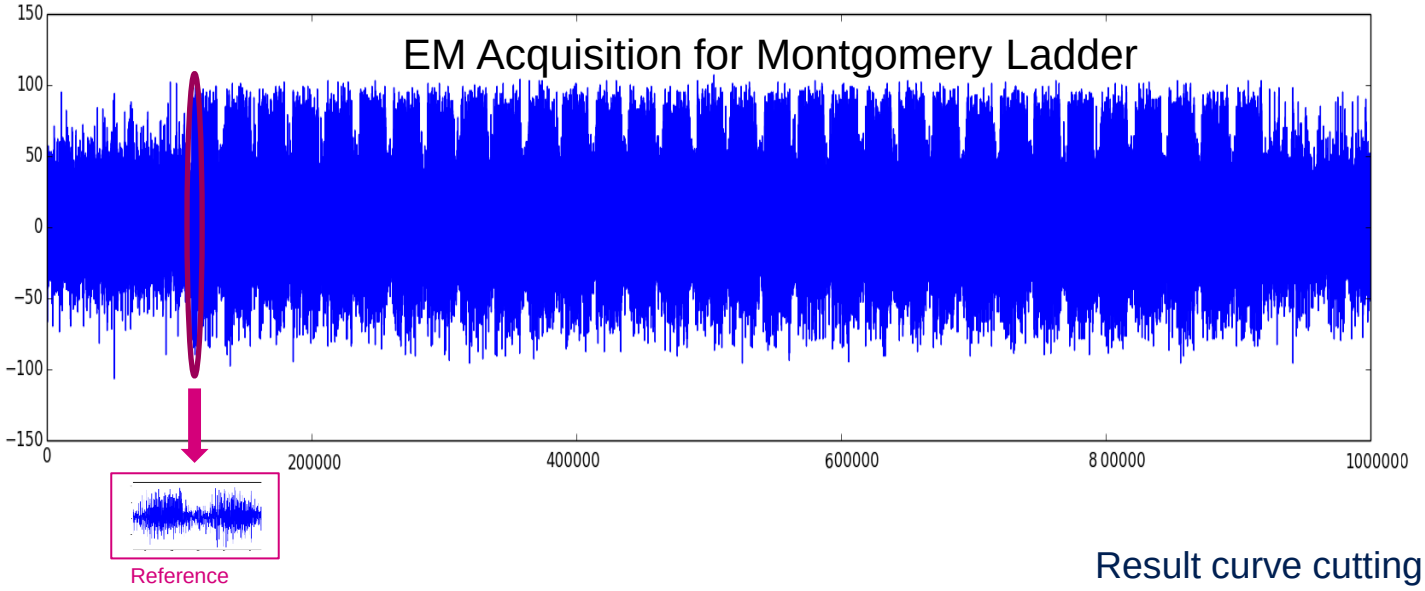
cea

LIRMM

MINES Saint-Étienne

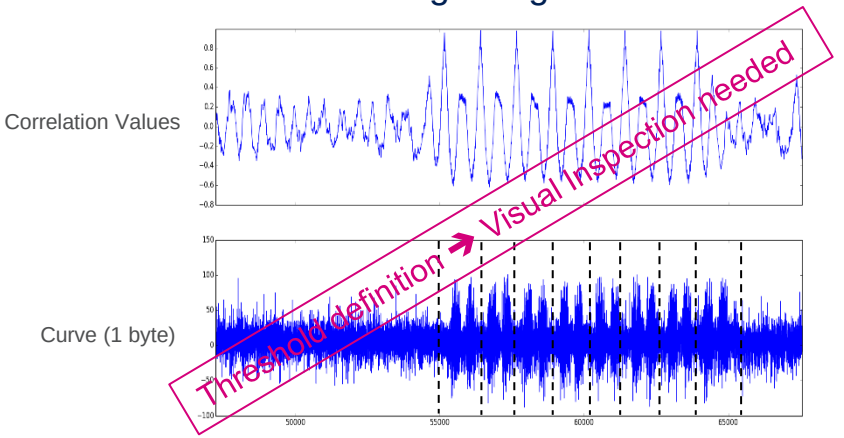
Horizontal Attacks in Practice

Curve Cutting



- Example of Perin et al's Attack
  - Use Cross Correlation
    - Define a reference pattern of length t
    - Compute the correlation coefficient values by sliding windows

Result curve cutting using Cross-Correlation



Horizontal Attacks in Practice

Curve Cutting

- The Bounded Collision Detection Criterion (BCDC) [1] :

$$0 < BCDC(T_1, T_2) = \frac{1}{\sqrt{2}} \frac{\sigma_{(T_1 - T_2)}}{\sigma_{(T_1)}} \leq 1$$

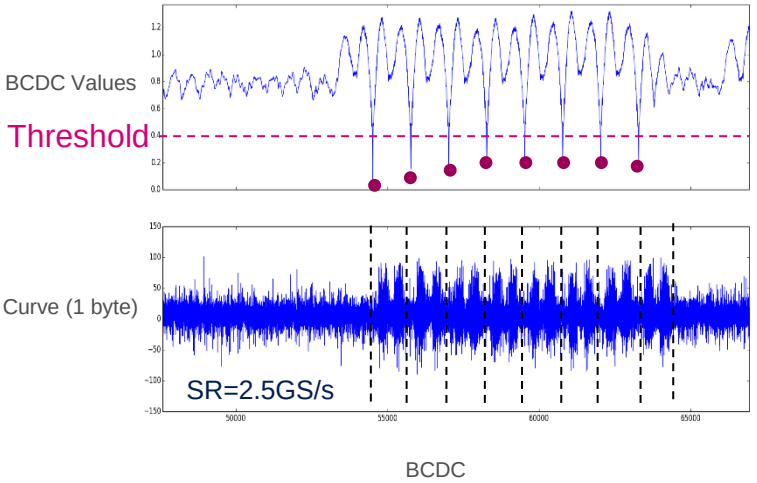
  - In the case of collision:

$$BCDC(T_1, T_2) \rightarrow 0$$

[1] I. Diop et al. ***Collision Based Attacks in Practice***. DSD 2015

- Solution: Curve Cutting using BCDC instead Cross Correlation
  - Define a reference pattern of length t
  - Compute BCDC values by sliding window

Result curve cutting using BCDC



Conclusion

- Similar Results as cross correlation
- But BCDC allows to define automatically a threshold ([1])

Trace Pre-processing

Trace Acquisition

Cutting

Alignment

Noise and Quality

Research of Points of Interest (PoIs)

Statistical Classifiers

life.augmented

cea

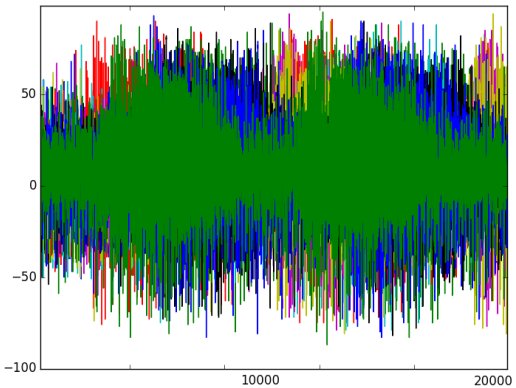
LIRMM

MINES Saint-Étienne

Horizontal Attacks in Practice

Resynchronization

- Example of Perin et al's Attack
  - FPGA ➔ No resynchronization problems



Patterns after curve cutting

Problem in real circuit: Due to the environmental countermeasures the patterns are misaligned despite the curve cutting method…

Solution: Hierarchical Synchronization

⬇

- Resynchronization Method
  1. Global Alignment :
     - Apply the POC [2] between a pattern reference and other patterns to determine the displacement value
  2. Local Alingment:
     - Elastic Alignment [3]

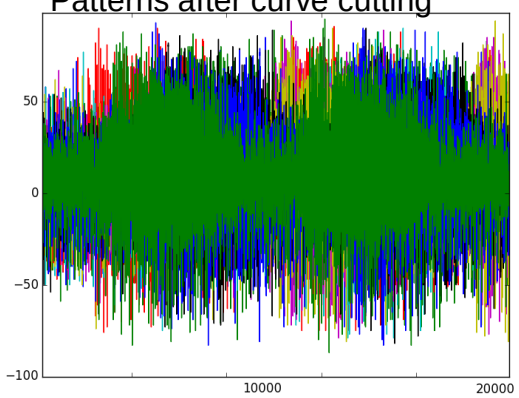
[2] N. Homma et al. ***High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching. CHES 2006***

[3] M. Witteman et al. ***Improving Differential Power Analysis by Elastic Alignment. CT-RSA 2011***

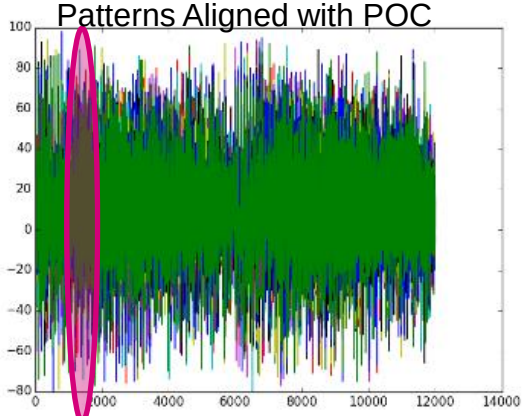
Horizontal Attacks in Practice

Resynchronization-Results

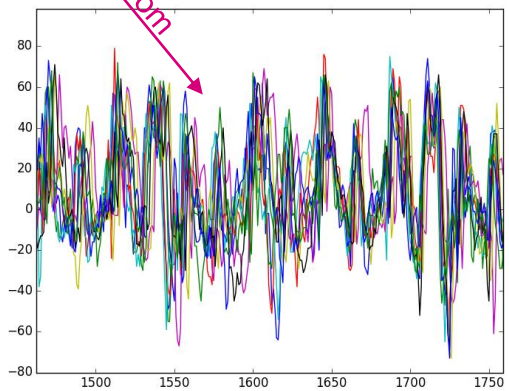
Patterns after curve cutting



Patterns Aligned with POC

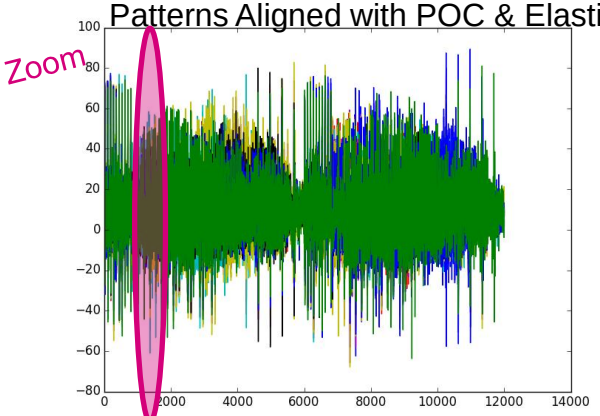


Zoom

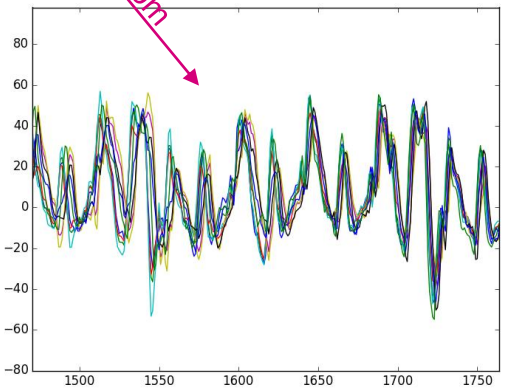


Zoom on Patterns Aligned with POC

Patterns Aligned with POC & Elastic



Zoom



Zoom on Patterns Aligned with POC & Elastic

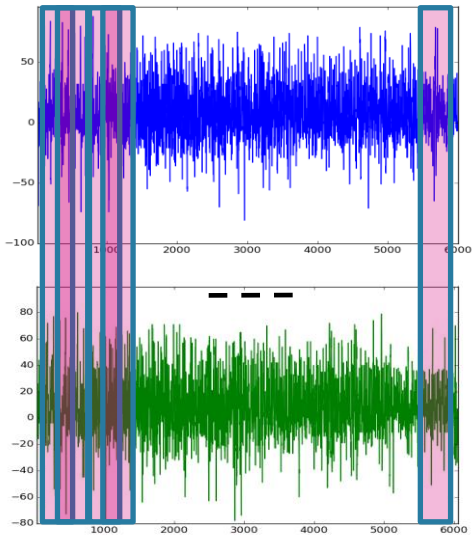
The proposed method seems to work well but…

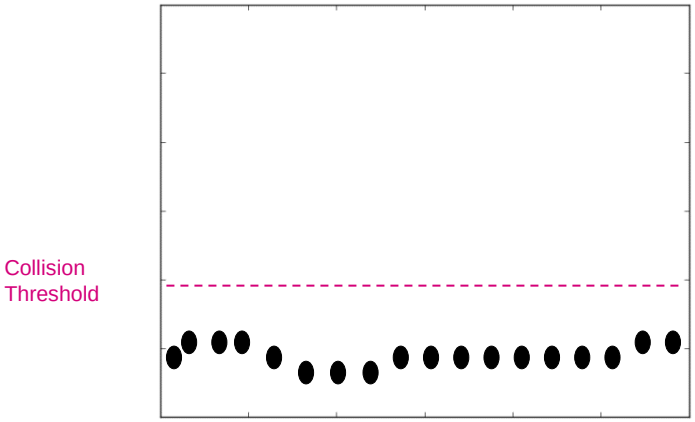
How can we validate this??

Horizontal Attacks in Practice

Resynchronization-Validation

- Validation
  - Validate the effectivness of the alignment method by using BCDC criterion
    - Do n measurement with the same data (exponent, message, modulo)
    - For each couple of measurements compute the BCDC by sliding windows
    - Compute the average BCDC for each window
    - If all BCDC values are inferior to 0.4 then ➔ The Synchronization is Successful

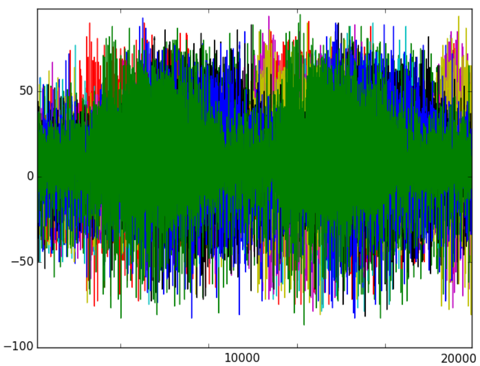


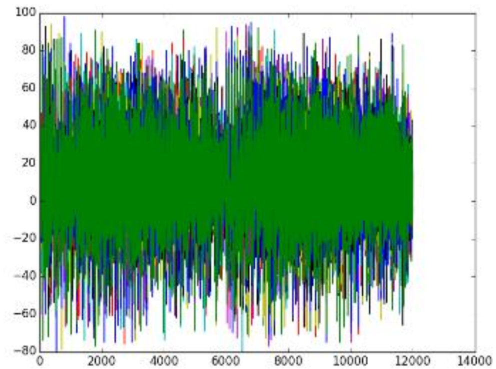


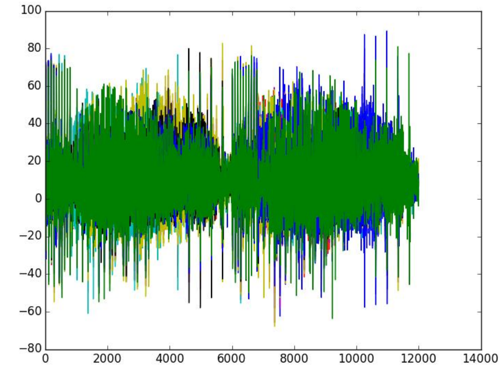
BCDC values

Horizontal Attacks in Practice

Resynchronization-Result Validation





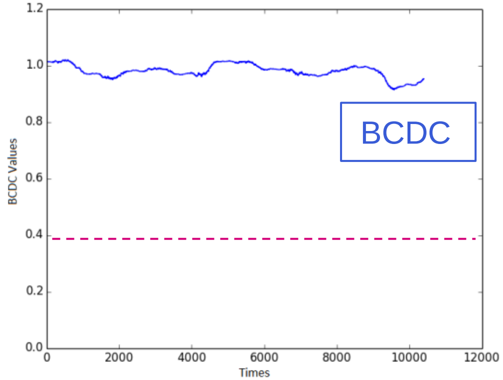


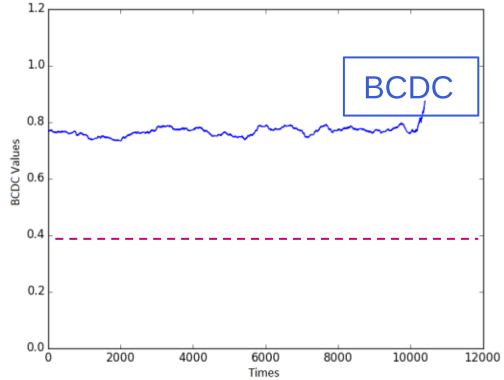
After curve cutting

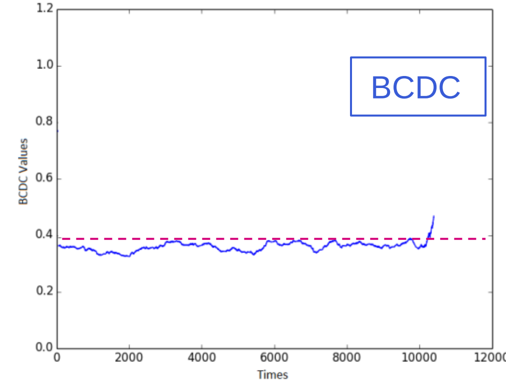
POC

POC & Elastic

Collision Threshold







Trace Pre-processing

Trace Acquisition

Cutting

Alignment

Noise and Quality

Research of Points of Interest (PoIs)

Statistical Classifiers

life.augmented

cea

LIRMM

MINES Saint-Étienne

Horizontal Attacks in Practice

Noise and Measurement Quality

- Example of Perin et al's Attack

  Compression technique to decrease noise in the patterns

  - Problem: Compression Suppose the knowledge of the exact number of cycles per bit treatment and so ➔ design knowledge …
  - Solution: Estimated SNR [4] (paper CARDIS 2015)
    - Take n Patterns $M_i = [\boldsymbol{m}^{\boldsymbol{i}}_{\boldsymbol{t_1}}, \dots, \boldsymbol{m}^{\boldsymbol{i}}_{\boldsymbol{t_w}}]$
    - Translate the Patterns in frequency domain using FFT
    - Compute for each couple (i, j) in frequency domain:
      $1 \leqslant i \prec j \leqslant \mathrm{n}$, with $l \geqslant 1$

[4] I. Diop et al. ***Collision for estimating SCA Measurement Quality and Related Application Attacks in Practice***. CARDIS 2015

$$\widehat{\boldsymbol{SNR}}(t_l, \dots, t_{l+p}) = \frac{1}{\boldsymbol{BCDC}^2\left(\left[\boldsymbol{m}^{\boldsymbol{i}}_{\boldsymbol{t_l}}, \dots, \boldsymbol{m}^{\boldsymbol{i}}_{\boldsymbol{t_{l+p}}}\right], \left[\boldsymbol{m}^{\boldsymbol{j}}_{\boldsymbol{t_l}}, \dots, \boldsymbol{m}^{\boldsymbol{j}}_{\boldsymbol{t_{l+p}}}\right]\right)} - \boldsymbol{1}$$

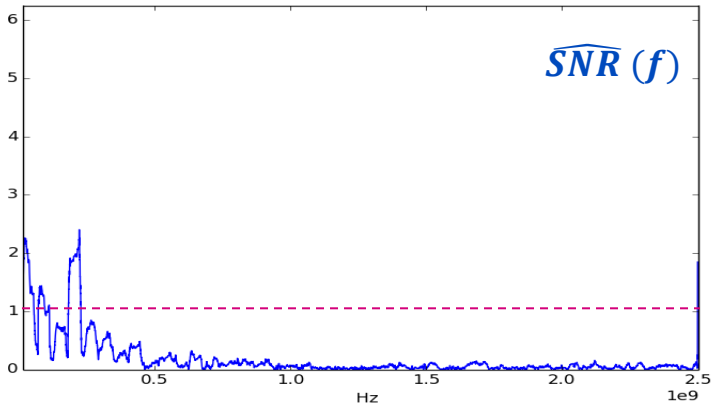
- Compute the average $\widehat{\boldsymbol{SNR}}$ values for each time windows $[t_l, \dots, t_{l+p}]$.
- Translate back the patterns in time domain after canceled the irrelevant frequencies

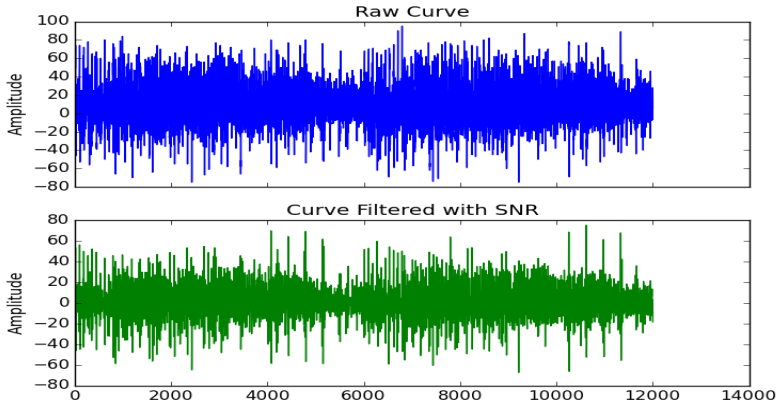
Horizontal Attacks in Practice

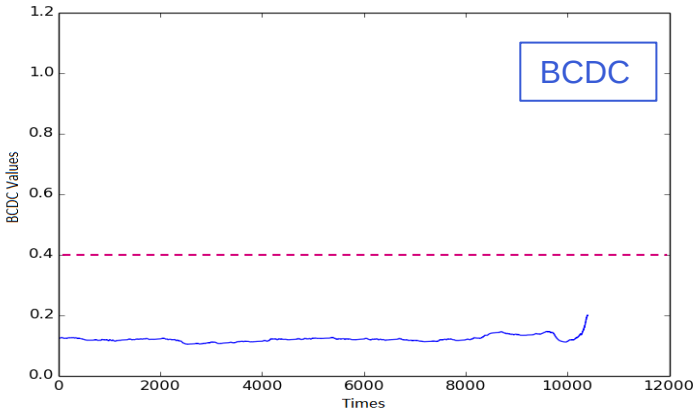
Noise and Measurement Quality

Setup:

- 20 patterns, Window lenght p = 200







Trace Pre-processing

Trace Acquisition

Cutting

Alignment

Noise and Quality

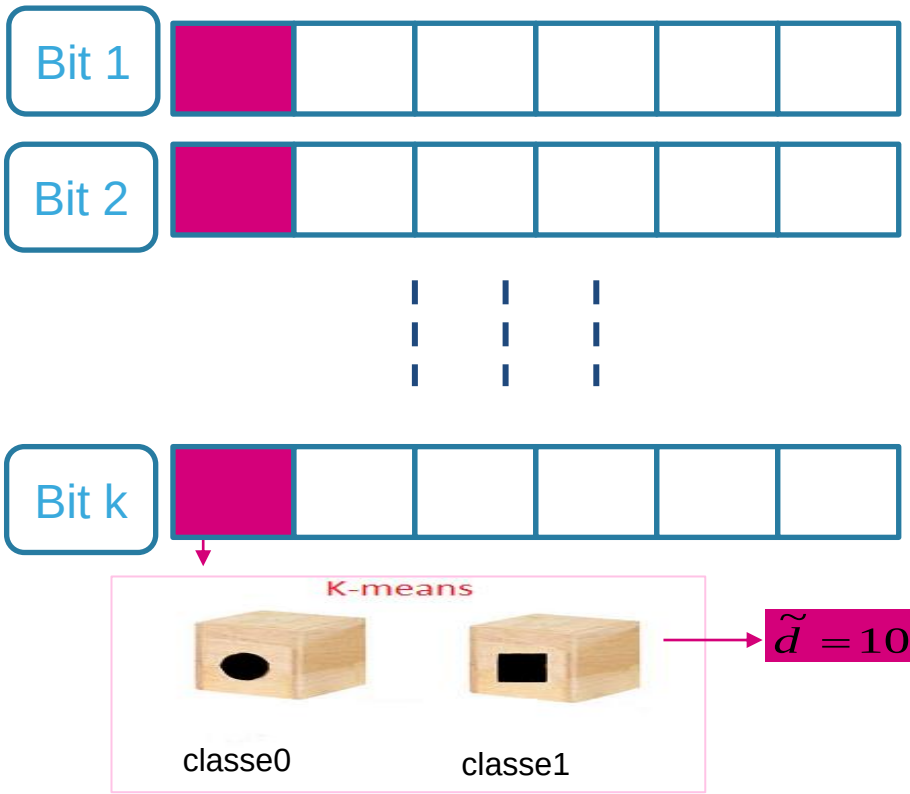
Research of Points of Interest (PoIs)

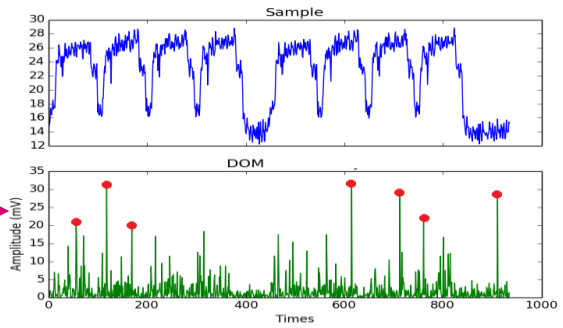
Statistical Classifiers

Horizontal Attacks in Practice

Perin et al. PoIs research method

- Example of Perin et al's Attack
  - The n operations $\langle MS \rangle_i$ are represented by a matrix T (k x L) and the k-means is applied over all columns of matrix T



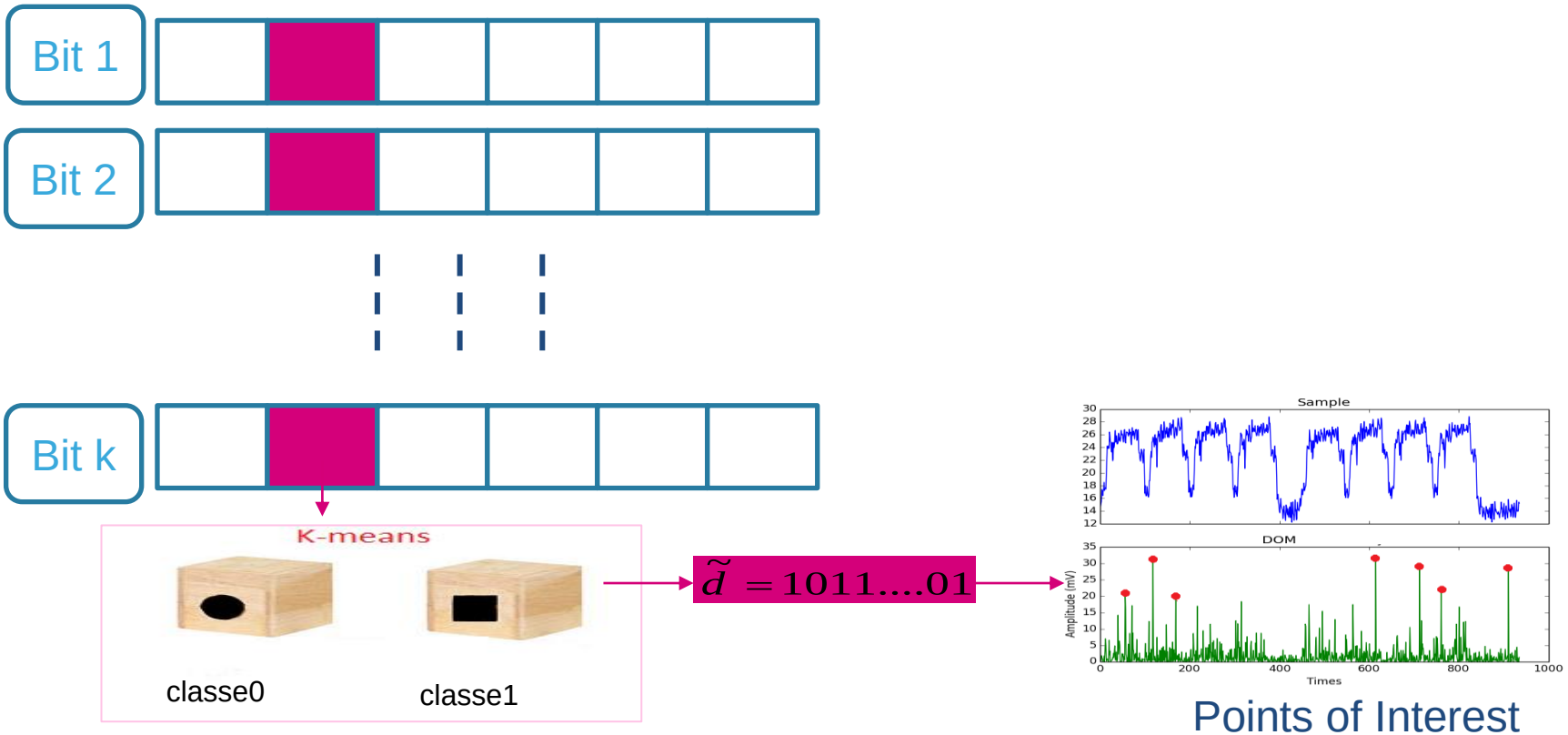


Points of Interest

Horizontal Attacks in Practice

Perin et al. PoIs research method

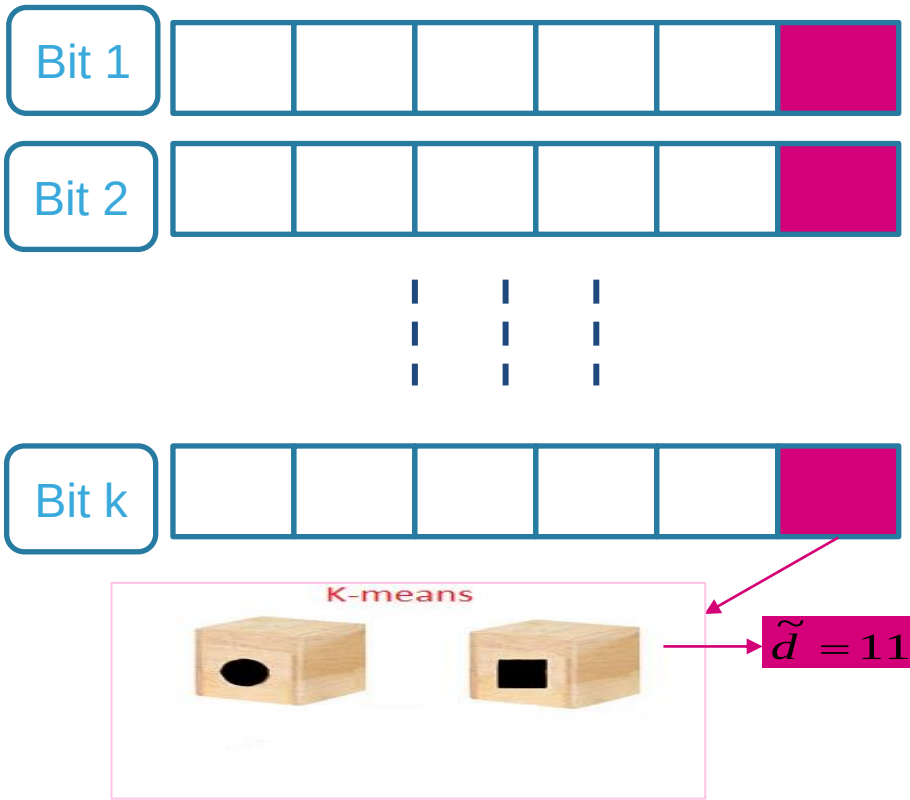
- Example of Perin et al's Attack
  - The n operations $\langle MS \rangle_i$ are represented by a matrix T (k x L) and the k-means is applied over all columns of matrix T



Horizontal Attacks in Practice

Perin et al. PoIs research method

- Example of Perin et al's Attack
  - The n operations $\langle MS \rangle_i$ are represented by a matrix T (k x L) and the k-means is applied over all columns of matrix T



Points of Interest

Trace Pre-processing

Trace Acquisition

Cutting

Alignment

Noise and Quality

Research of Points of Interest (PoIs)

Statistical Classifiers

life.augmented

cea

LIRMM

MINES Saint-Étienne

Horizontal Attacks in Practice

Distinguisher

- Exponent Recovery Using BDCD as Distinguisher

Let:

- P_1:The pattern corresponding to the MSB operation with only PoIs
- P_i: The pattern corresponding to the i^{th} bit exponent operation ($i \neq 1$) with only PoIs

- Compute $\rho_i = BCDC(P_1, P_i)$
  - If ρ_i is higher (or equal) than the collision threshold ➔ secret $bit_i = bit_1$
  - Else $bit_i \neq bit_1$

Horizontal Attacks in Practice

Distinguisher-Results

- Summarize of Results

Pre-processing Method	Distinguisher	
	Pearson	BCDC
Trace Misaligned	50.8%	50%
Aligned with POC only	53%	52.7%
Hierarchical Alignment	70%	84%
Hierarchical Alignment +Noise Reduction	82%	96%

Conclusion

Conclusion

Trace Acquisition (Smart Triggering)

Trace Pre-processing

- Cutting (BCDC)
- Alignment (POC & Elastic)
- Noise and Quality (SNR)

Research of Points of Interest (PoIs) (State of the art)

Statistical Classifiers (BCDC)

Questions