CASCADE Conference 03/04/2025

LIRMM

SERMA
SAFETY & SECURITY

Improving Leakage Exploitability in Horizontal Side Channel Attacks through Anomaly Mitigation with Unsupervised Neural Networks

Gauthier Cler, Sébastien Ordas, Philippe Maurine

Outline

Horizontal Attacks

Horizontal Attacks

- Single trace attack
- No profiling on open device possible, no leakage assessment.
- Usually on asymmetric implementations (RSA, ECC).
- Clustering approach:
  1. Divide trace into patterns
  2. Points of Interest (PoI) selection with univariate clustering
  3. Multidimensional clustering

Attack success highly relies on the quality of the trace.

Impact of anomalies on PoI selection

Anomalies in data

Outliers (interquantile range)

Distribution tails

$$x \notin [Q_1 - 1.5 \times IQR, Q_3 + 1.5 \times IQR]$$

Anomalies in data

Outliers (interquantile range)

Distribution tails

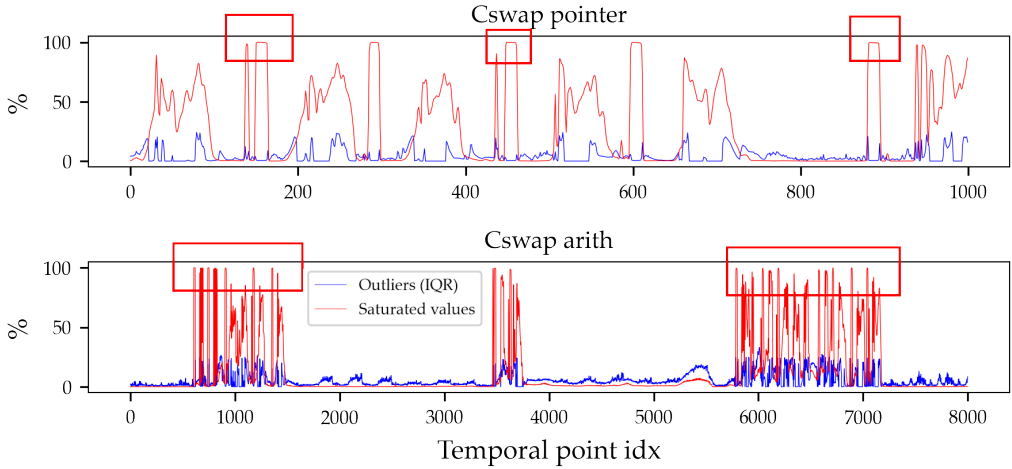
$$x \notin [Q_1 - 1.5 \times IQR, Q_3 + 1.5 \times IQR]$$

Saturated values

min/max values of digital sampling, for 8bit:

$$x = -128 \vee x = 127$$

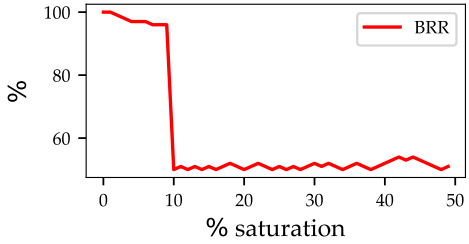
Anomalies in data

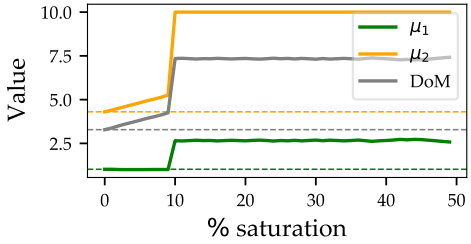


[1]Average anomalies Pointer:33.3%, Arith:16.5%

Impact of anomalies on PoI selection

- Clustering is **not robust** to anomalies in data
- Can cause centroids shift, singularities,...





[1] BRR: Bit Recovery Rate

Anomalies mitigation

Limits of simple mitigation

Mitigation by ablation

- Remove time points based on anomalies threshold
- Possibly loosing information about the leakage

Limits of simple mitigation

Mitigation by ablation

- Remove time points based on anomalies threshold
- Possibly loosing information about the leakage

Mitigation by replacement

- Replace anomalies points with mean/median of non anomalies for each time point
- Decrease separability of mixture components

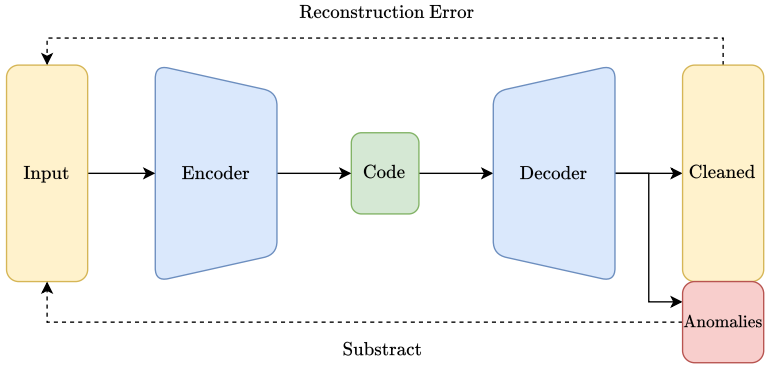
Contribution - Mitigation with neural networks

Consider alternative methods

- Able to be trained in an unsupervised manner
- Leakage/information conservation
- Two approaches:
  - Robust auto-encoder
  - CycleGAN

Robust auto-encoder unsupervised mitigation

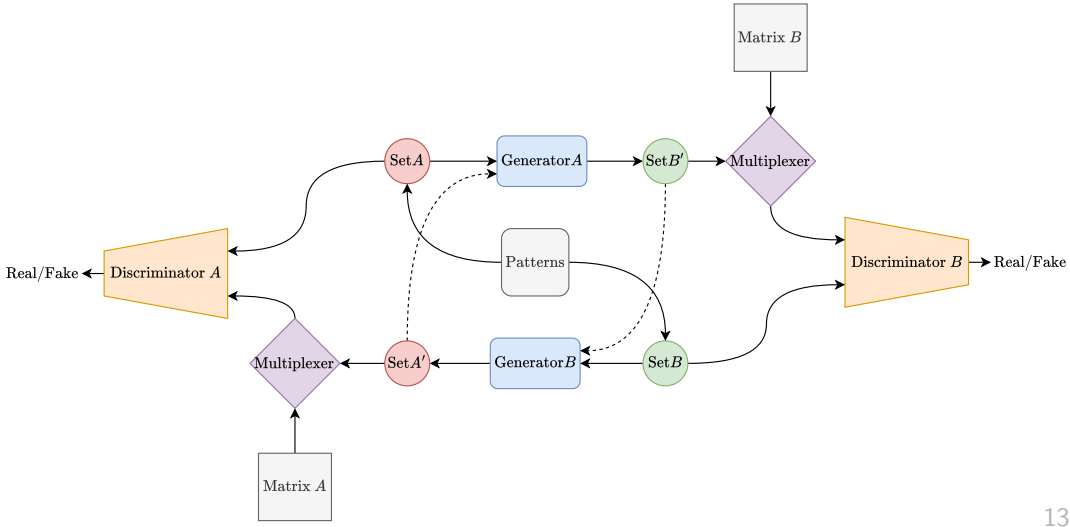
Decomposition of input data to **cleaned** and **anomalies** matrices.



Limits

- RAE Generate new synthetic patterns $\rightarrow$ Can cause side effects on non anomalies.
- RAE does not exploit the anomalies model.

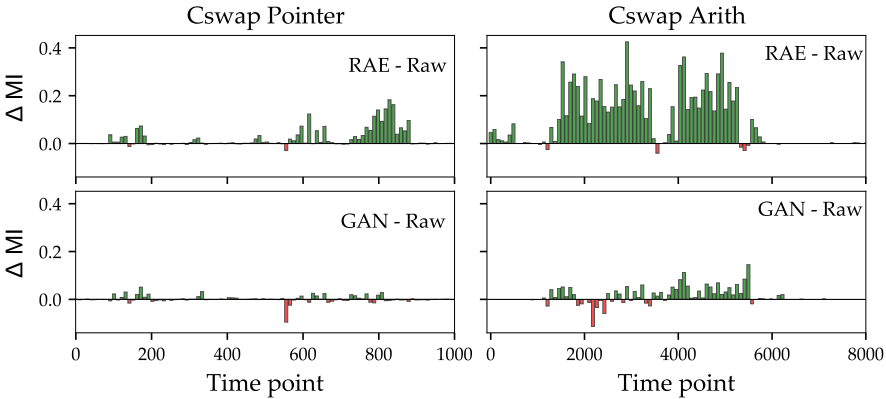
Multiplexer CycleGAN self-supervised mitigation



Results

Information conservation

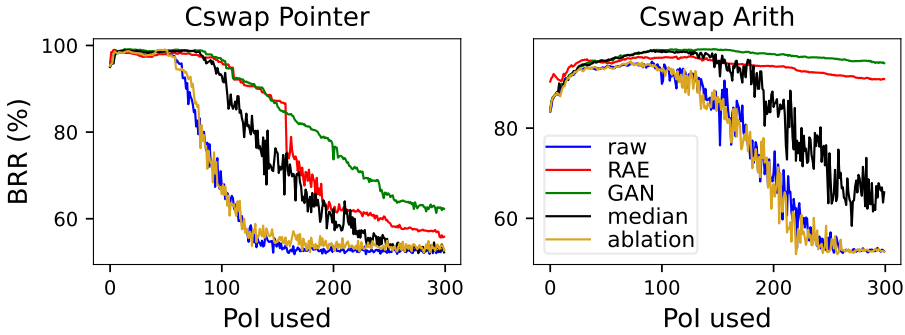
No change in the global MI. [1]



[1] Estimated with MINE.

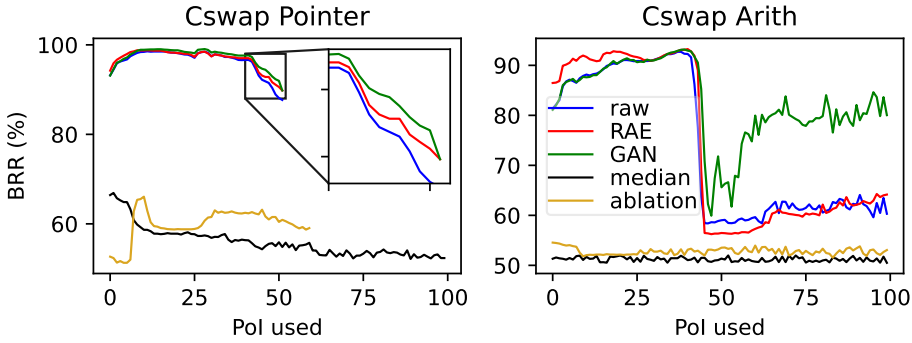
Supervised selection - upper bound

Select k PoI with highest t-values and apply multidimensional clustering.



Unsupervised selection

Multidimensional clustering on the best k PoI from Cler *et al.* 2023 unsupervised selection.



Conclusion

Conclusion

Benefits

- Anomalies mitigation **improves leakage exploitability**
- Methods are applicable in a completely unsupervised context

Conclusion

Benefits

- Anomalies mitigation **improves leakage exploitability**
- Methods are applicable in a completely unsupervised context

Limitations

- Architecture choice and parameters tuning can be hard in practice
- Attack success **still** depends on the exploitation method

Conclusion

Benefits

- Anomalies mitigation **improves leakage exploitability**
- Methods are applicable in a completely unsupervised context

Limitations

- Architecture choice and parameters tuning can be hard in practice
- Attack success **still** depends on the exploitation method

Future work

- Consider additional anomalies models
- Generalize on other targets/algorithms

Thank you for your attention.

Do you have any question?

SERMA
SAFETY & SECURITY

14, rue Galilée
33600 PESSAC
05 57 26 08 88
contact-s3@serma.com

Bonus