SECURE-IC

THE SECURITY SCIENCE COMPANY

October, 30th 2018 – Cybersecurity cooperation between France and Japan

Defensive and offensive AI for embedded security

Thomas PERIANIN

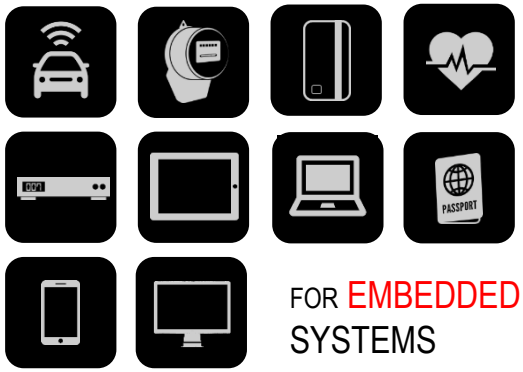
Embedded security engineer

thomas.perianin@secure-ic.com

Our activity

WHAT DO WE DO?

SECURITY TECHNOLOGIES



FOR EMBEDDED SYSTEMS

FOR WHOM?

- CHIPSET/DEVICE VENDORS
- IC DESIGN HOUSES
- CERTIFICATION LABS
- GOVERNMENTAL AGENCIES

FOR WHICH MARKETS?

OUR VISION

Going forward, there will be more and more interconnected devices or objects in various market verticals, this is what we call Internet of Things or Internet of Everything. All those objects being interconnected to the cloud, each and every object could be a threat for the whole network. Therefore the security of the objects or the devices is key. Even more, security will become one of the most important assets of the digital world.

BUSINESS LINES

PROTECT

THREAT PROTECTION Business Line

SECURYZR

COMBINATION OF **SMART UNITS** AND **EXPERTISE RESULTS**

EVALUATE

THREAT ANALYSIS Business Line

LABORYZR

READY-TO-USE **PRE** AND **POST-SILICON ANALYSIS PLATFORMS**

SERVICE & CERTIFY

THINK AHEAD Business Line

EXPERTYZR

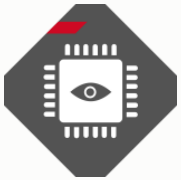
THE **NEXT STEPS** TOWARDS **SECURITY CHALLENGES**

OUTLINE

1. Defensive AI for cybersecurity: Smart Monitor
2. Offensive AI fo cybersecurity: ML approach for Cache-Timing Attacks

SECURE-IC
THE SECURITY SCIENCE COMPANY

3



Defensive AI: Smart Monitor

EMBEDDED CYBER-SECURITY POWERED BY AI

SECURE-IC

DIGITAL SENSOR

ALL-IN-ONE DIGITAL FAULT-INJECTION DETECTOR [1-2-3]

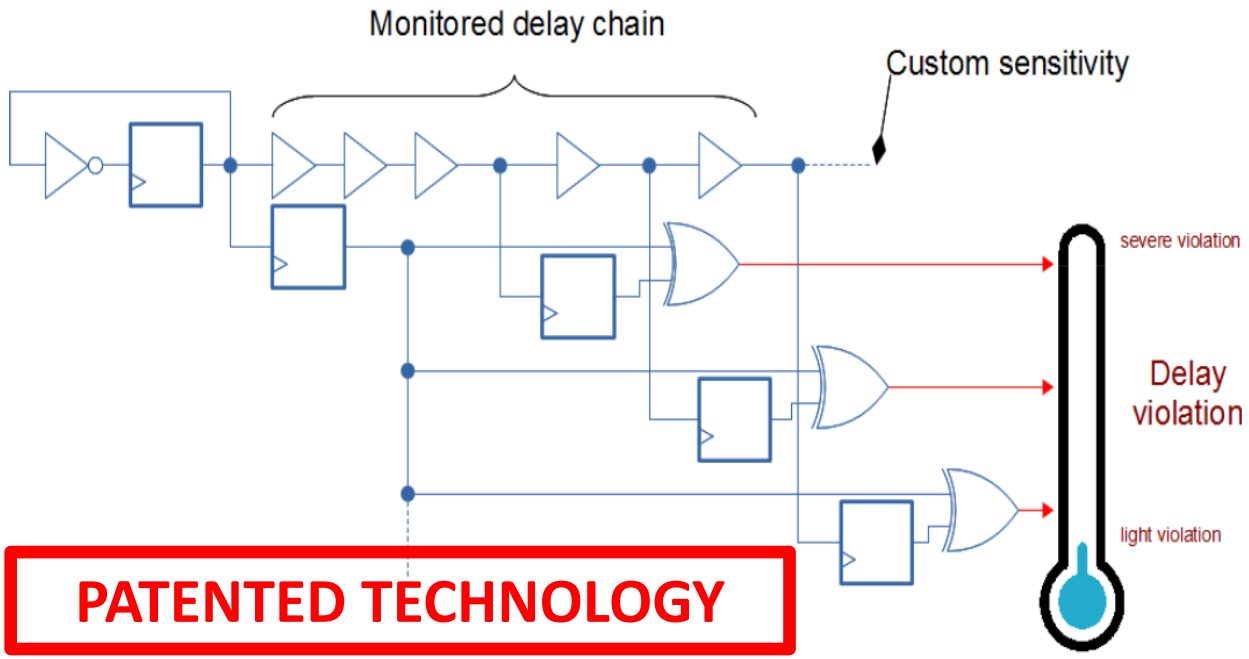
- **Monitors for abnormal operating conditions**
  - Small digital circuits monitoring behavior, conditions
  - Raises an alarm when situation becomes critical
  - System engineer decides action to perform w/alarm
- **Sensitive to the following**
  - Temperature
  - Voltage
  - Clock frequency
  - Laser exposure, EM exposure
- **"Global vs. localized" threats**
  - Global: Temperature, voltage, clock frequency (single-sensor) [4-5]
  - Local: EM [6] or surface-level laser attack (multi-sensor)
- **IP is completely Digital which makes it...**
  - Difficult to locate because it is melted in the circuit/logic/standard cells
  - Easier to port to a new technology
  - "True-time" hardware alarm (predictable latency)

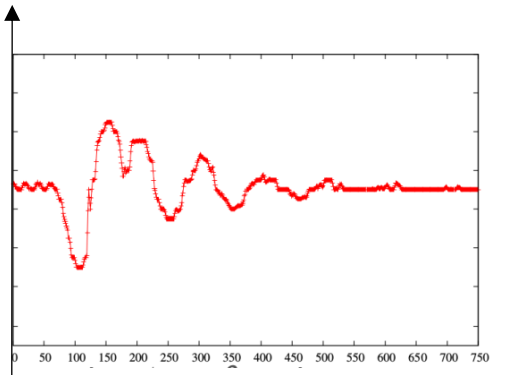
SECURE-IC

HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

ML-ENABLED CYBER-PHYSICAL SECURITY

- Digital Sensor: Fault Injection Detection
  - Detect variation of propagation time along a delay chain
  - ➔ Problem: false-positives





I	0	1	0	1	0	1	0	1	0	1	0
O_1	1	0	1	0	1	0	1	0	1	0	1
O_2	1	0	1	0	1	0	1	0	1	0	1
⋮	1	0	1	0	0	0	1	0	1	0	1
O_{th}	1	0	1	1	0	1	1	0	1	1	1
O_{th+1}	0	1	0	1	0	1	0	0	0	1	0
O_{th+2}	0	1	0	1	0	1	0	1	0	1	0
⋮	0	1	0	1	0	1	0	1	0	1	0
O_n	0	1	0	1	0	1	0	1	0	1	0

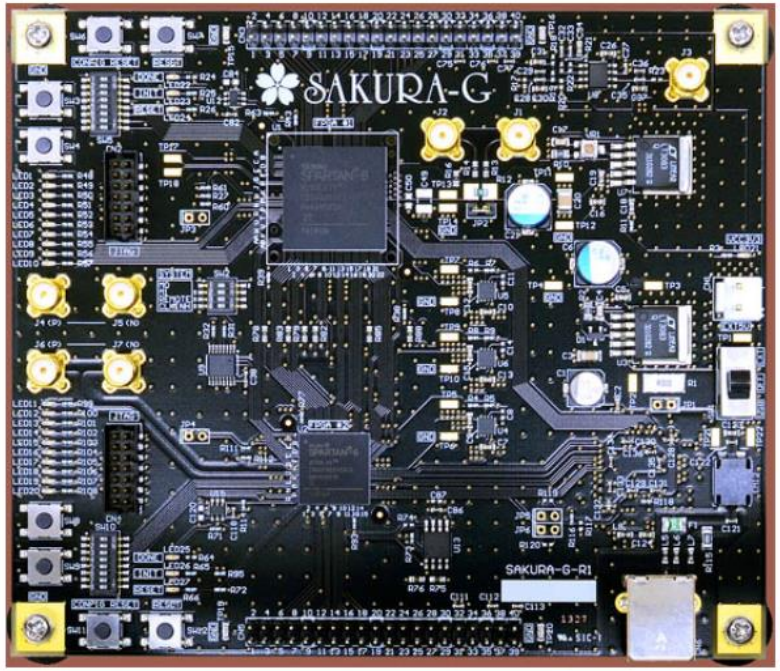
PATENTED TECHNOLOGY

SECURE-IC

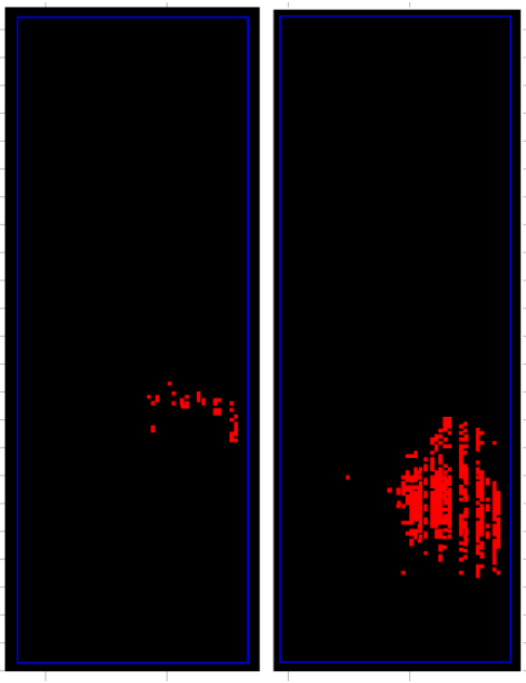
ARTIFICIAL INTELLIGENCE FOR CYBER-SECURITY

AI-ENABLED CYBER-PHYSICAL SECURITY

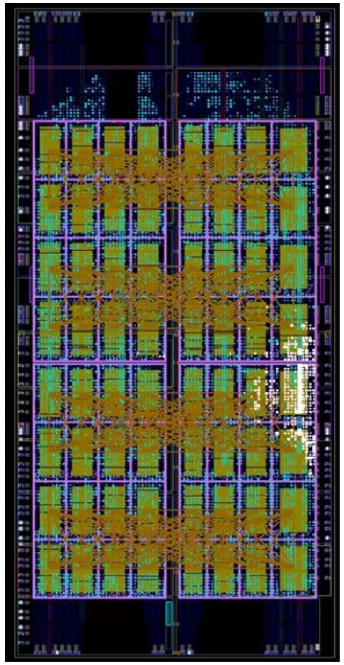
- Teaming Digital Sensors



FPGA board Sakura-G
(also on Xilink Ultrascale+)



Architecture 1:
4 DS - 50 LUTs for the delay chain (left) and an AES (right).



Architecture 2:
Matrix of 64 DS + AES + CyberEU

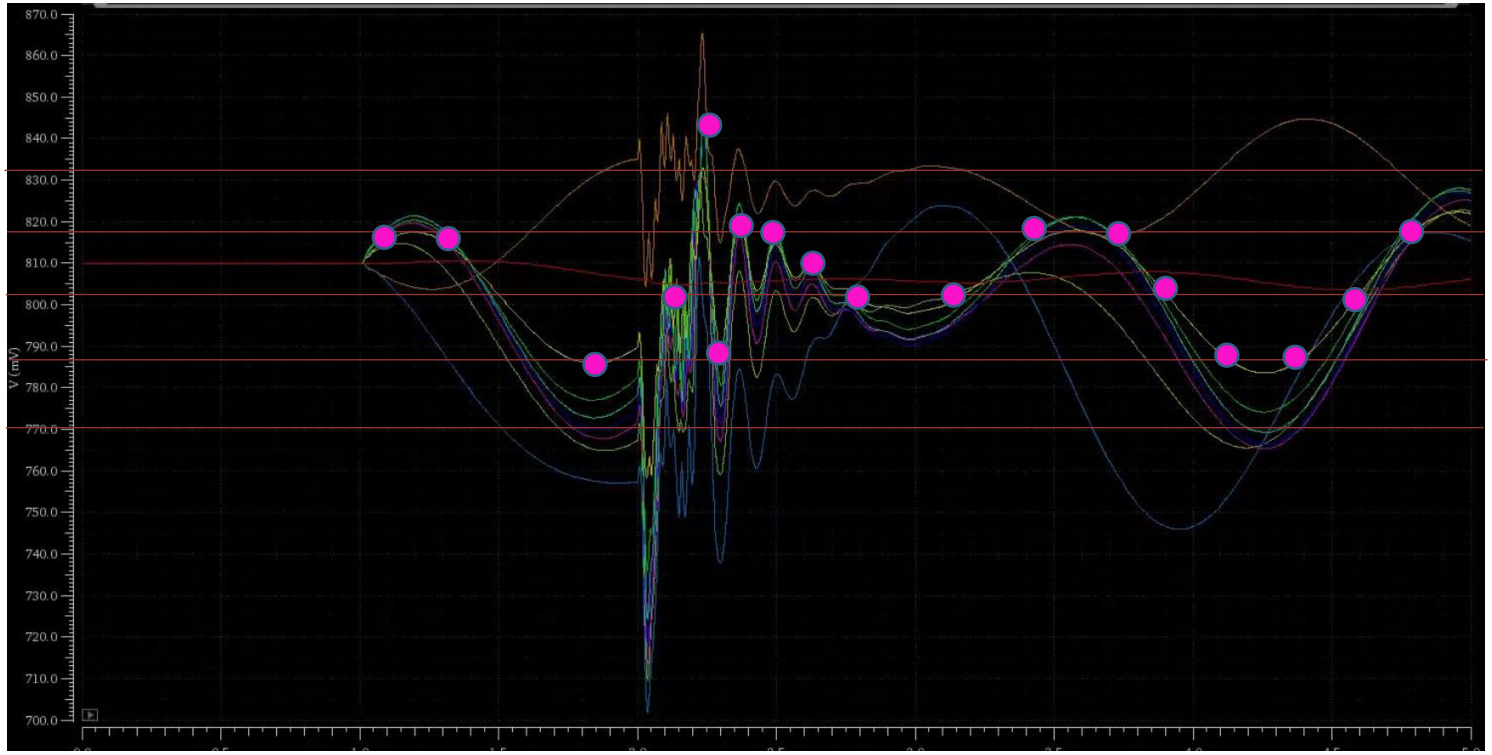
SECURE-IC

HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

ML-ENABLED CYBER-PHYSICAL SECURITY

- Digital Sensor: Fault Injection Detection

EMFI-specific Sensors thresholds

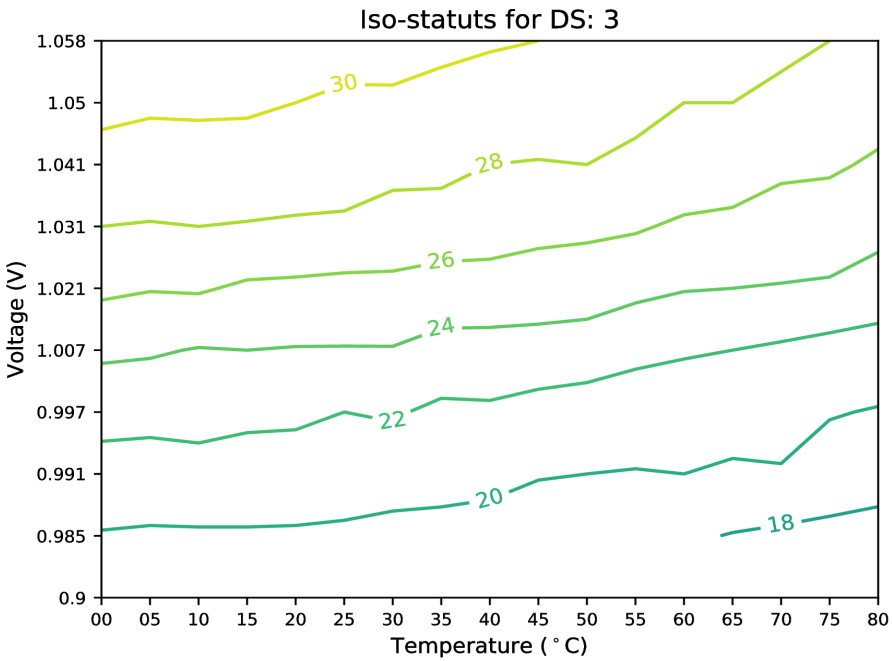


SECURE-IC

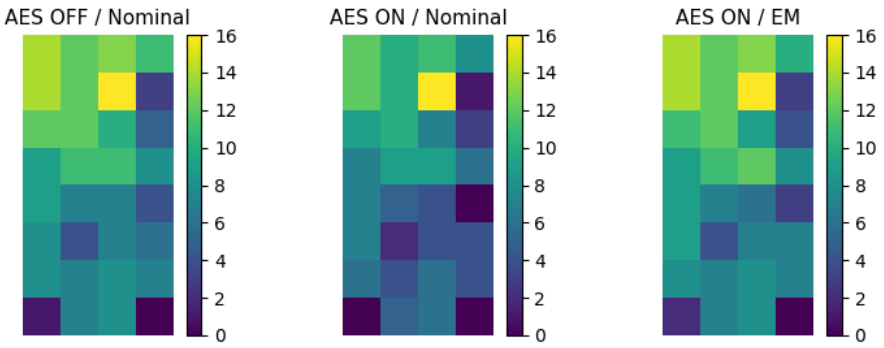
HARDWARE-ENABLED AI FOR EMBEDDED SECURITY

ML-ENABLED CYBER-PHYSICAL SECURITY

- Digital Sensor: Fault Injection Detection
  - **Enlarge Digital Sensor functionalities (Digital Voltmeter & Thermometer)**
  - **Pragmatic approach: On-chip characterization & threshold on OTP memory**

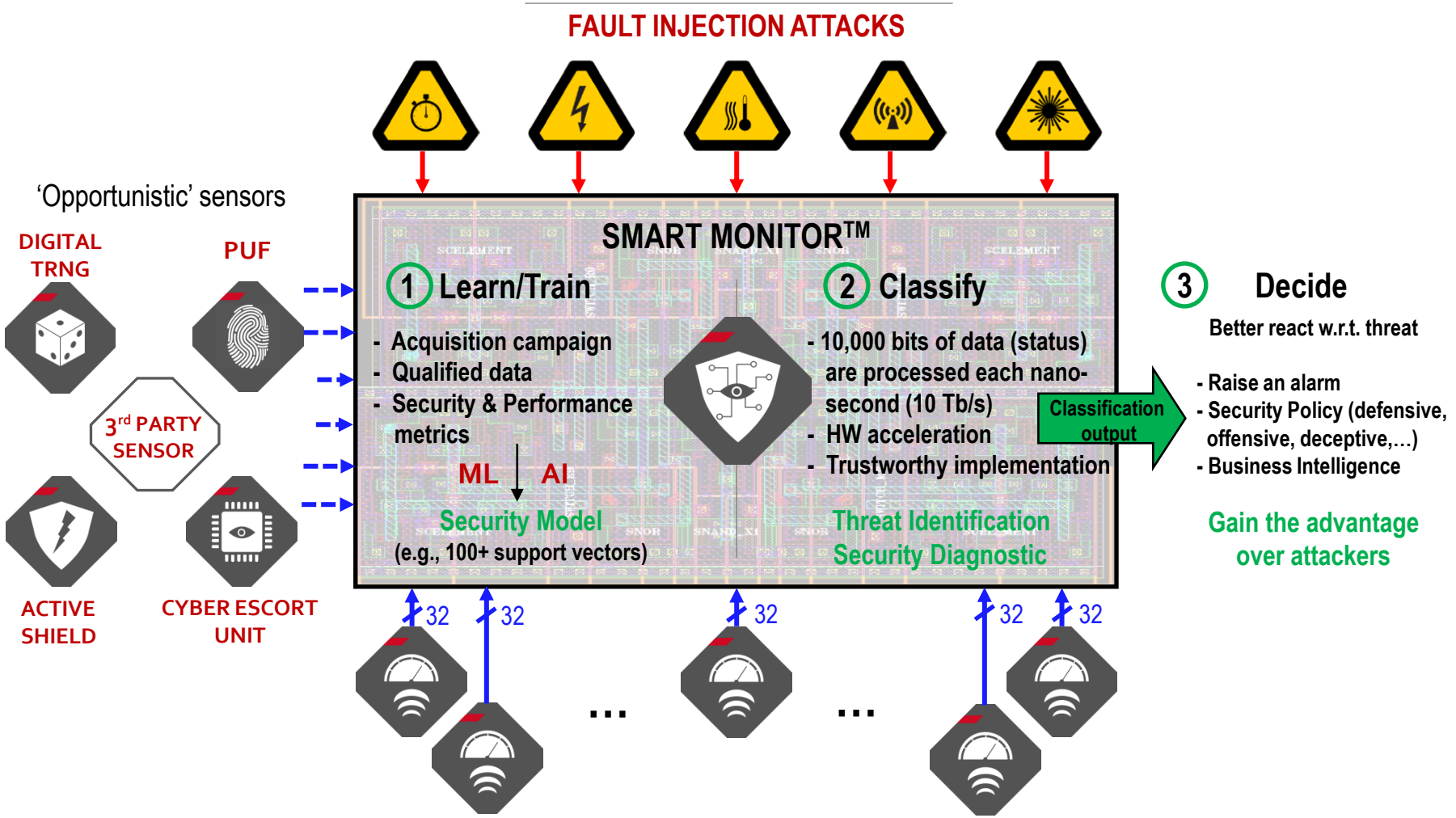


- Threshold setting highly impact sensitivity
- Hard to set with simulation
- Use of OTP to store individual DS threshold after characterization on test chip



EMBEDDED CYBER- SECURITY POWERED BY AI

SMART MONITOR FOUNDATIONS

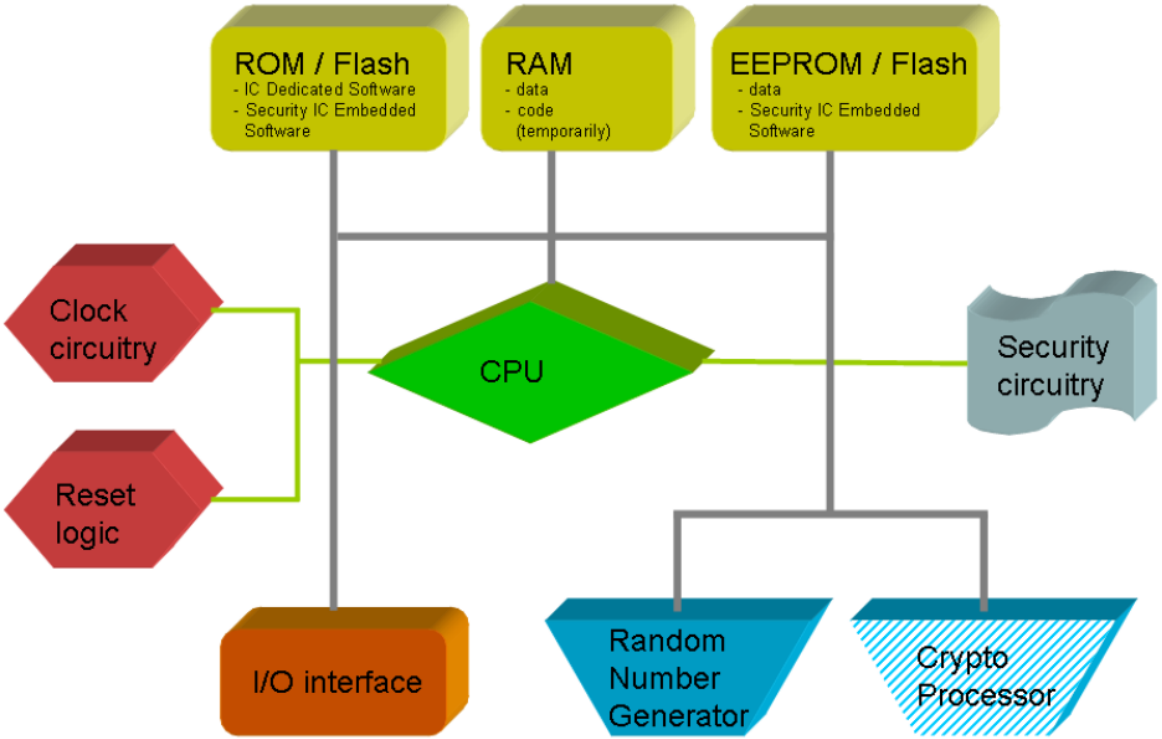


SECURE-IC

EMBEDDED CYBER- SECURITY POWERED BY AI

AI-ENABLED CYBER-PHYSICAL SECURITY

- Example of configuration



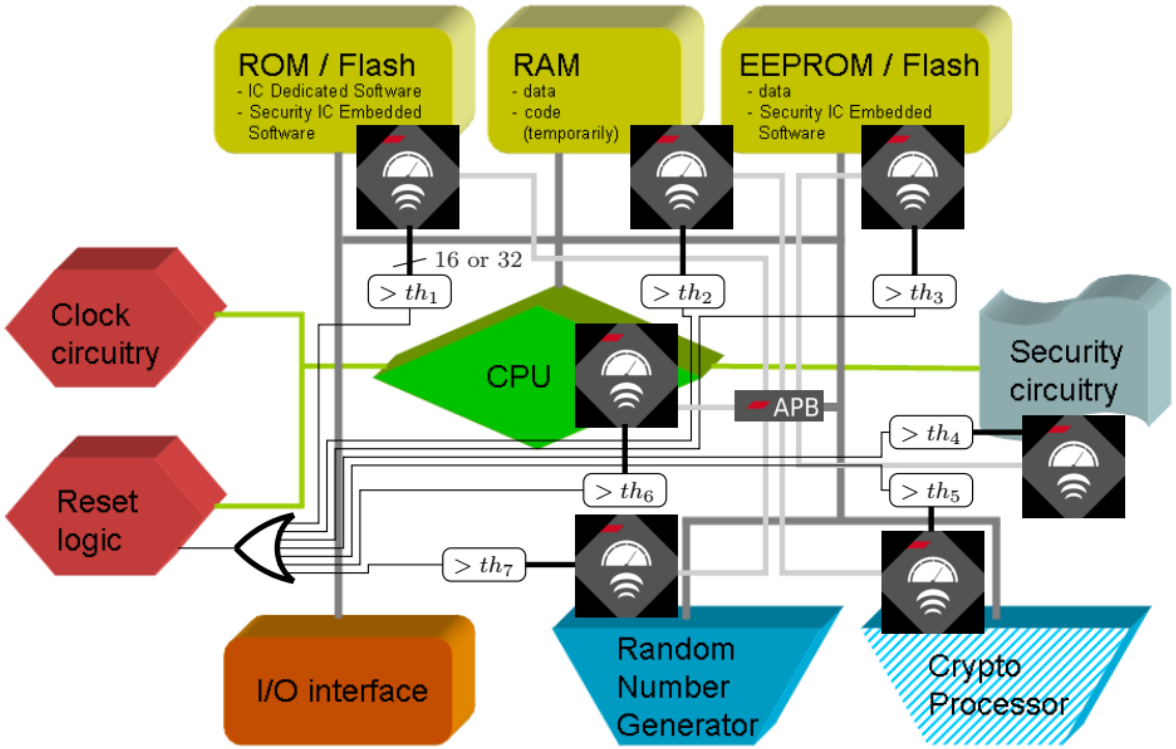
Unprotected SoC, according to PP 0084

SECURE-IC

EMBEDDED CYBER- SECURITY POWERED BY AI

AI-ENABLED CYBER-PHYSICAL SECURITY

- Example of configuration (increasing security)



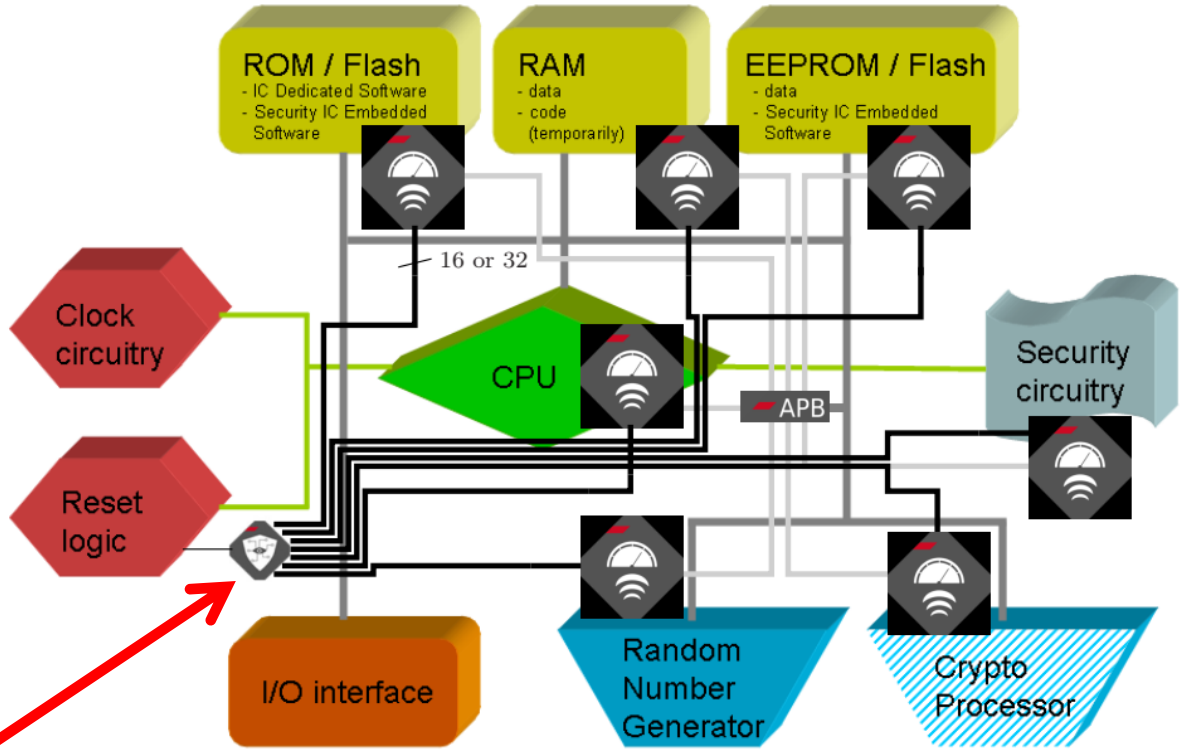
DSv2 without SM, fast

SECURE-IC

EMBEDDED CYBER- SECURITY POWERED BY AI

AI-ENABLED CYBER-PHYSICAL SECURITY

- Example of configuration (increasing security)



SMART MONITOR

DSv2 with SM, fast

SECURE-IC

EMBEDDED CYBER- SECURITY POWERED BY AI

AI-ENABLED CYBER-PHYSICAL SECURITY

- **SECURE-IC'S SMART MONITOR: AI FOR EMBEDDED SYSTEMS**

Create collective intelligence between IPs and other whistleblowers

- Sources of information are diverse, abundant
- Signals can come from on-chip analog sensors, digital sensors, software reports…
- … or from opportunistic media (weak signals) = Indice of Compromission (IoC)

By leveraging diversity and complementary

- Sensitive to physical vs logical malfunctions
- Able to detect permanent problems vs transient issues

SECURE-IC

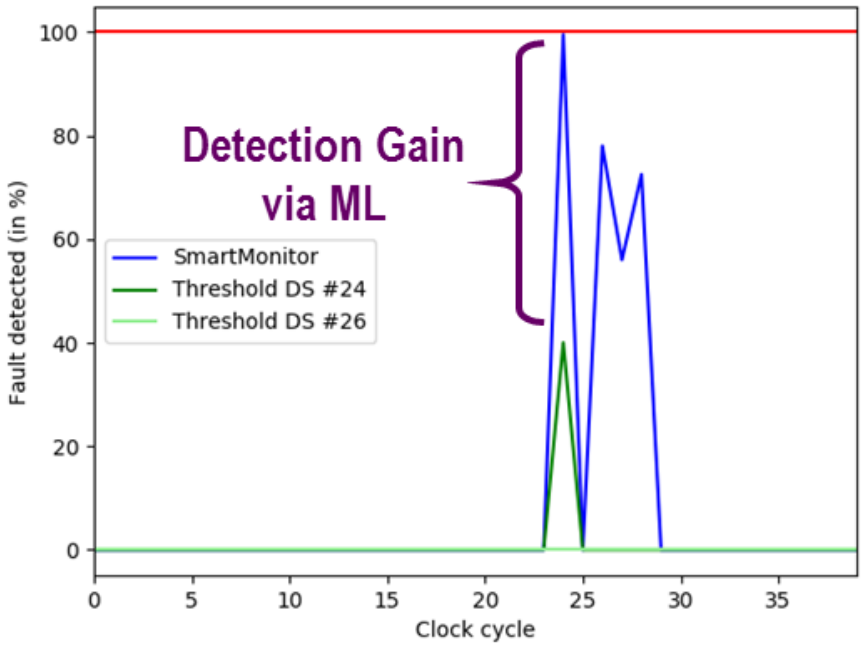
EMBEDDED CYBER- SECURITY POWERED BY AI

AI-ENABLED CYBER-PHYSICAL SECURITY

- Use-case : ML-enhanced EM Fault Injection Detection
  - A Fleet of Digital Sensors + Smart Monitor to:

    - Improves notably the global accuracy (detection efficiency and false-positive reduction)

  - Dateset generation:
    - EM Injection
    - Laser Injection
  - Training Support Vector Machines

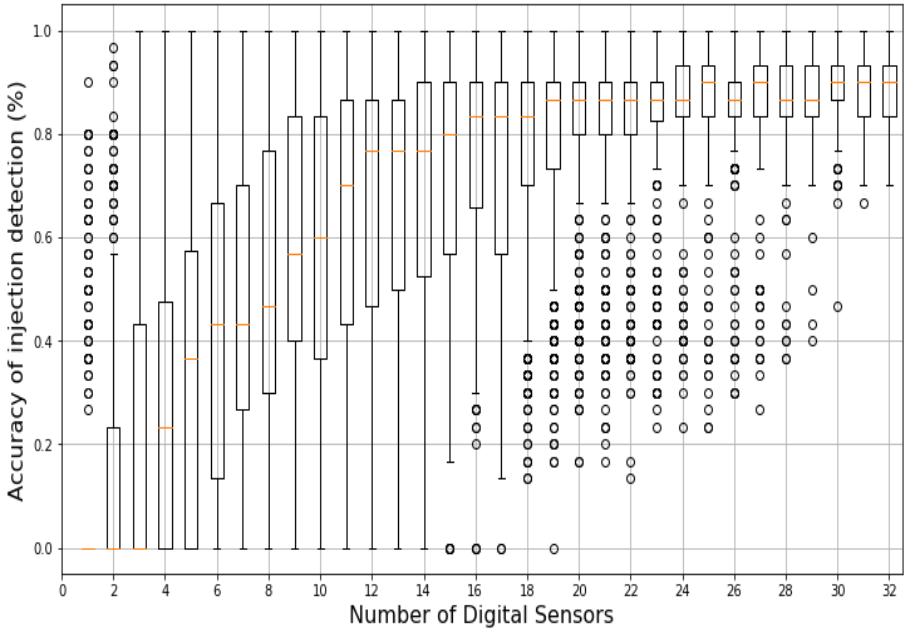


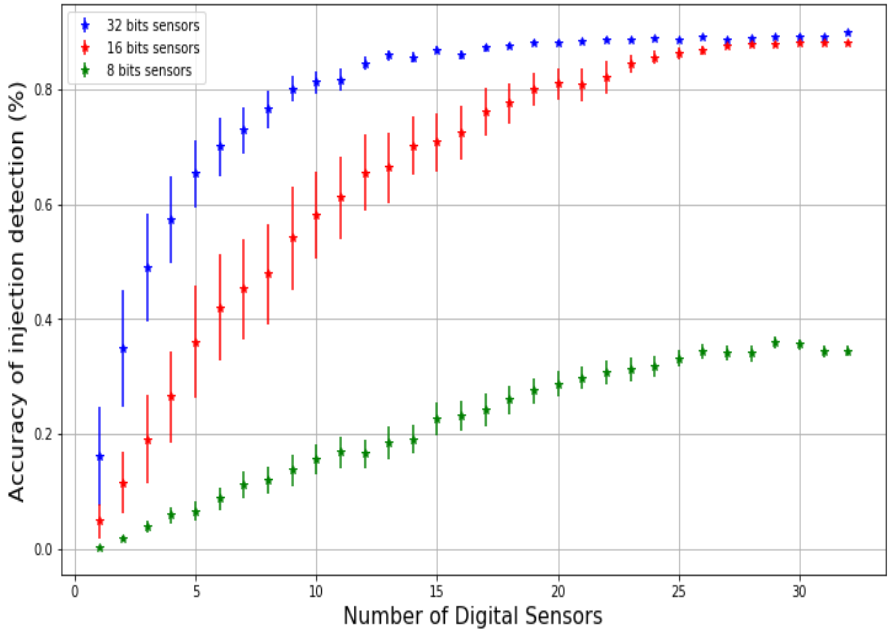
SECURE-IC

EMBEDDED CYBER- SECURITY POWERED BY AI

AI-ENABLED CYBER-PHYSICAL SECURITY

- Use-case : ML-enhanced EM Fault Injection Detection
  - A Fleet of Digital Sensors + Smart Monitor for a teaming strategy.





SECURE-IC

EMBEDDED CYBER- SECURITY POWERED BY AI

AI-ENABLED CYBER-PHYSICAL SECURITY

SECURE-IC'S SMART MONITOR: AI FOR EMBEDDED SYSTEMS

Gain assurance in Threat Detection

- Additional signals are aggregated for security event detection: multimodal analysis
- Learning phase to "lock down the perimeter" of attack
- Confidence & Robustness - Reduce false alarms and false positive event

The right decision at the right time in full knowledge

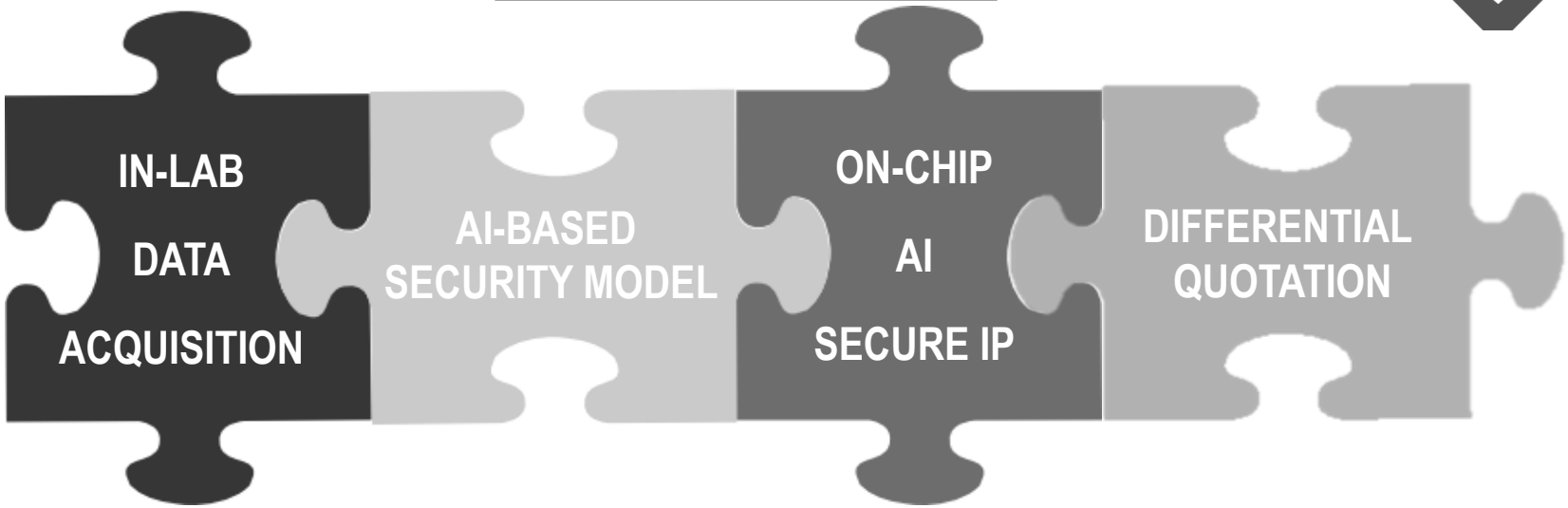
- Anatomy of an attack (nature, temporality, locality, intensity, attack phase…)
- Gain advantage over attackers (attack diagnosis): reverse the advantage
- Built an on-chip security Headquarter to react properly – Security strategy

Business Intelligence

- Know your device's every-day life
- Attack typology and statistics for ≠ device categories, geographic areas, technology nodes…

SMART MONITOR: ARTIFICIAL INTELLIGENCE FOR CYBER-SECURITY

PROGRAM FOUNDATIONS



EVALUATE	SERVICE	PROTECT	CERTIFY
Nominal Conditions	Data Processing	HW-Classifier	Security Audit
Real Attack	ML-algorithms	Secure Storage	Pre-quotation w/ & w/o AI
Collect Training Data	Model Generation	Trustworthy AI	CC Certification Scheme
Develop Guideline & Security Metrics	Performances	On-chip Security HQ	
	Topological invariant		

OFFER: GUI for Labs | Consulting Services | Hardware IP | Support to Certification

SECURE-IC

EMBEDDED CYBER- SECURITY POWERED BY AI

AI-ENABLED CYBER-PHYSICAL SECURITY

- **SMART MONITOR IMPROVEMENT PERSPECTIVES**
  - Trade-off between performances & security: RAM cost, input signal rate, #classes, code size, etc..
  - More diversity in the types of inputs of the Smart Monitor.
  - Security of the ML model (Integrity verification of the training data for ML)
  - Study differential ageing of sensors / effect of sensor breakdown: a model per year?
  - Dynamical feedback on the model: adaptive model.
  - Hardware, Software or a combination of both, depending whether reactivity or flexibility is most important
  - Use of dedicated memory to store history: should be protected.

    ➔ We are looking for PoC partners!

Bibliography

[1] Selmane, N., Bhasin, S., Guilley, S., & Danger, J. L. (2011). Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks. *IET information security*, *5*(4), 181-190.

[2] Guilley, S., Sauvage, L., Danger, J. L., Selmane, N., & Pacalet, R. (2008, August). Silicon-level solutions to counteract passive and active attacks. In *FDTC* (pp. 3-17). IEEE-CS.

[3] Luca, B., Shay, G., Israel, K., David, N., & Jean-Pierre, S. (2008). Fifth international workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2008, Washington, DC, USA, 10 August 2008.

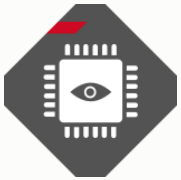
[4] Selmane, N., Guilley, S., & Danger, J. L. (2008, May). Practical setup time violation attacks on AES. In *Dependable Computing Conference, 2008. EDCC 2008. Seventh European* (pp. 91-96). IEEE.

[5] Bhasin, S., Selmane, N., Guilley, S., & Danger, J. L. (2009, July). Security evaluation of different AES implementations against practical setup time violation attacks in FPGAs. In *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on* (pp. 15-21). IEEE.

[6] Riviere, L., Najm, Z., Rauzy, P., Danger, J. L., Bringer, J., & Sauvage, L. (2015). High precision fault injections on the instruction cache of ARMv7-M architectures. *arXiv preprint arXiv:1510.01537*.

SECURE-IC
THE SECURITY SCIENCE COMPANY

3



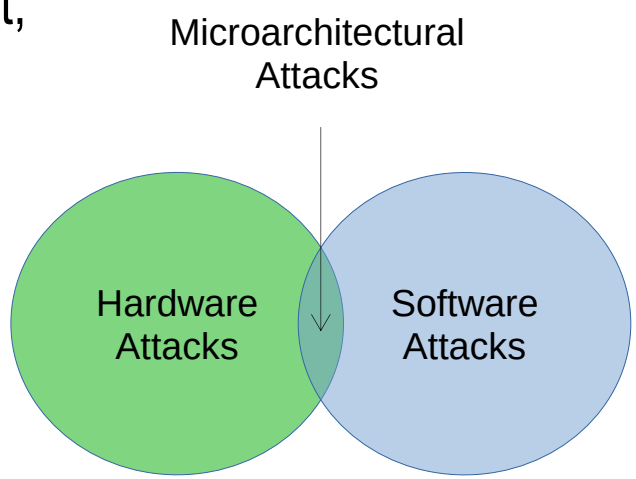
Offensive AI for embedded security

Machine learning approach for Cache Timing Attacks

Microarchitectural Attacks

INTRODUCTION

- Stealthy attacks have emerged, at the intersection of:
  - Hardware security: side-channel & fault injection
  - Software security: they can be perpetrated only by software:
    - Without the need for any equipment,
    - Whenever, even on the field!
- At the origin of recent Zero-day attacks such as Spectre & Meltdown



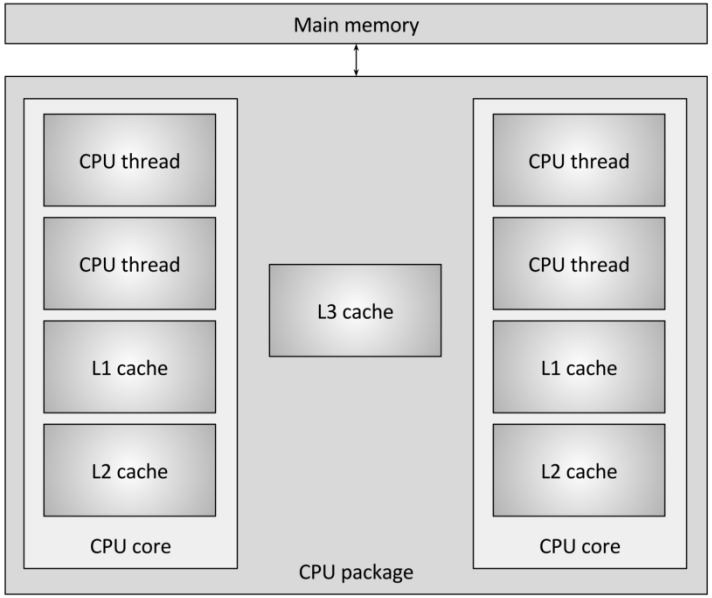
Microarchitectural Attacks

Cache-Timing Attacks

- **Malicious process spies L1I, L1D or LLC cache**
- **Cache-access patterns leak information about secret**

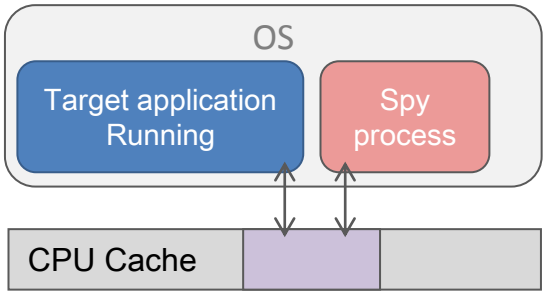
Causes of cache leakages:

- **Through control flow graph: conditional branching, loops**
- **Through accesses in tables**



Examples:

- **Spectre, CacheBleed (2017), Cache Attacks on Intel SGX (2017)**
- **Attacks on AES, RSA, ECC, Lattice-Based signatures…**
- **Cross VM / Cross Cores attacks**

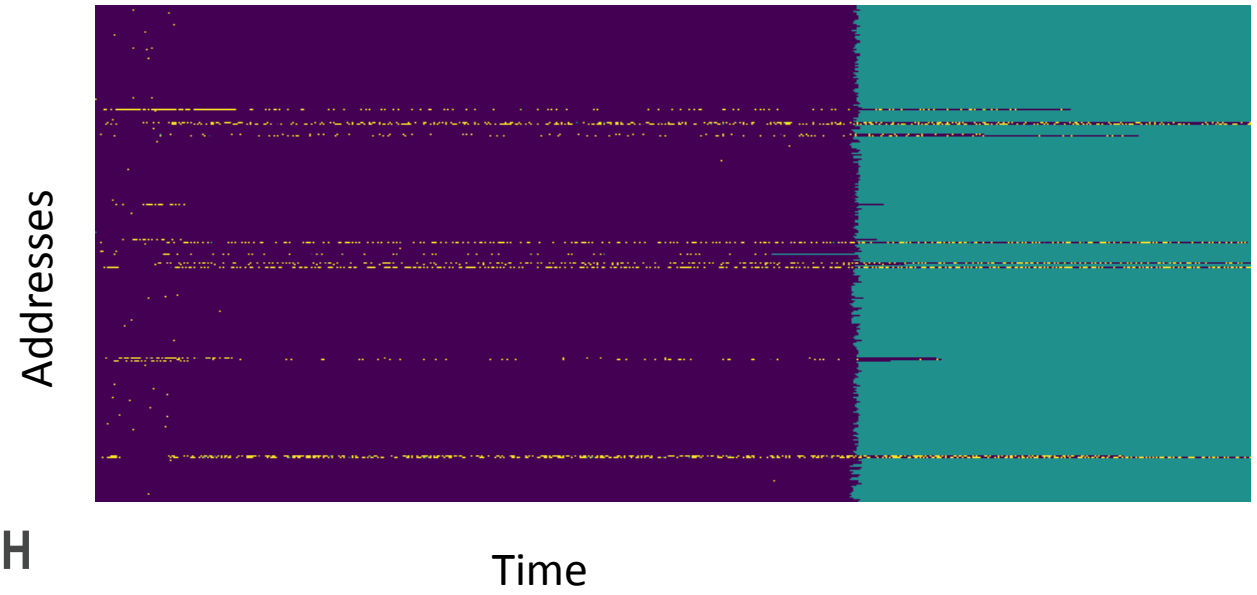


SECURE-IC

Microarchitectural Attacks

We measure the access time to the Cache through various strategies:

- EVICT + TIME
- PRIME + PROBE
- FLUSH + RELOAD
- FLUSH + TIME + FLUSH



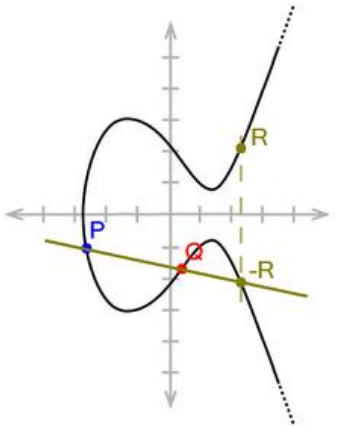
SECURE-IC

OpenSSL

Targeting OpenSSL

- ECDSA: Digital Signature Algorithm

- Ephemeral key – 256 bits Nonce: Sensitive information



- Multiplication computation

```
int ec_wNAF_mul(const EC_GROUP *group, EC_POINT *r, const BIGNUM *scalar,
                size_t num, const EC_POINT *points[], const BIGNUM *scalars[],
                BN_CTX *ctx)
```

- WNAF (W- Non Adjacent form)

WNAf: [0, 0, 0, 1, 0, 0, 0, 0, 3 …., 1, 0, 0, 0, 0, 3, 0, 0, 0]

SECURE-IC

Cache Timing Leakage

- Conditional Branch

→ Timing Leakage!!

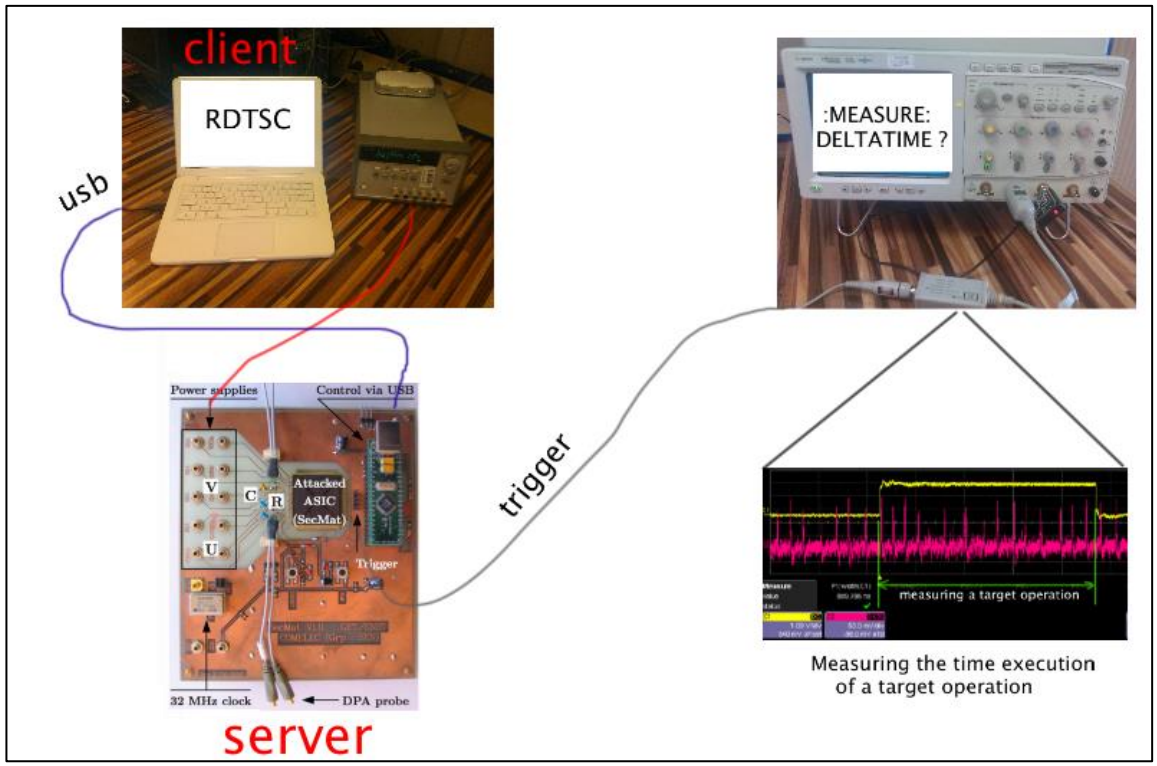
- Sequential multiplication

→ Can be spied

```
for (k = max_len - 1; k >= 0; k--) {
    if (!r_is_at_infinity) {
        if (!EC_POINT_dbl(group, r, r, ctx)) //Secure-IC comment : doubling function
            goto err;
    }

    for (i = 0; i < totalnum; i++) {
        if (wNAF_len[i] > (size_t)k) {
            int digit = wNAF[i][k];
            int is_neg;

            if (digit) {

                /*
                */

                if (r_is_at_infinity) {
                    /*
                    */
                } else {
                    if (!EC_POINT_add
                        (group, r, r, val_sub[i][digit >> 1], ctx)) //Secure-IC comment : addition function
                        goto err;
                }
```

WNAf: [0,0,0,1,0,0,0,0,3 …., 1, 0, 0, 0, 0, 3, 0, 0, 0]
=>
Multiplication: [D, D, D, A, D, D, D, D, A, …, A, D, D, D, A, D, D, D]

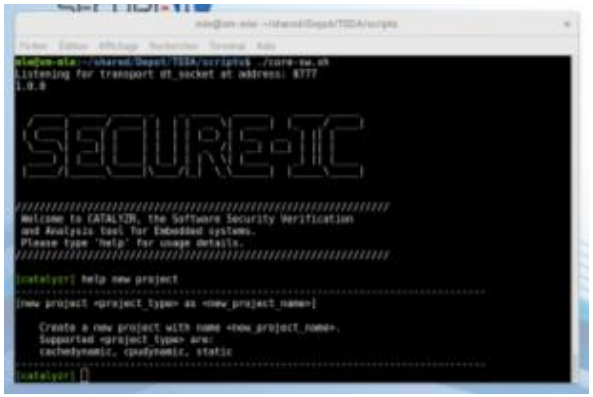
Architecture of Spying process

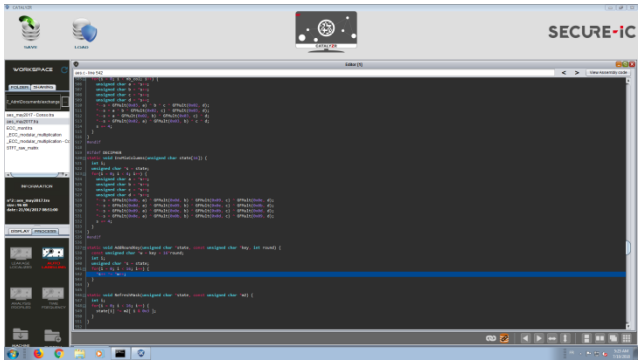


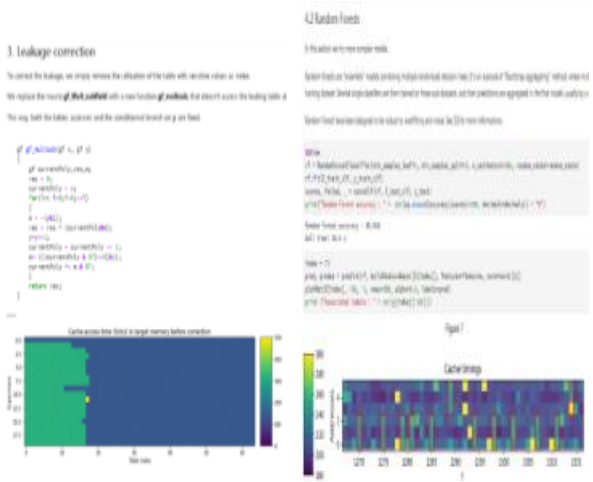
[Jean-Luc Danger, Nicolas Debande, Sylvain Guilley, Youssef Souissi: High-order timing attacks. CS2@HiPEAC 2014: 7-12]

Secure-IC Catalyzr

- Static analysis for leakage detection
- Cache spying and timing analysis
- All in one tool







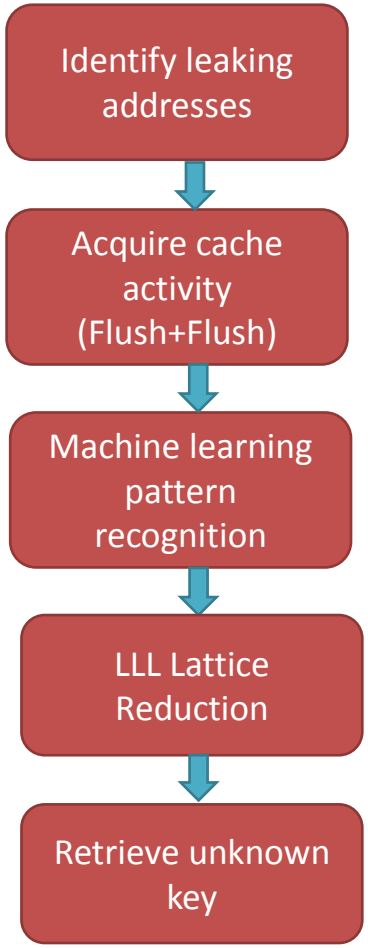
Screenshots of Catalyzr tool.

SECURE-IC

Microarchitectural Attack on ECDSA

OpenSSL

- Machine Learning enhanced attack on ECDSA of OpenSSL 1.1.0.
- Cryptographic nonce wNaf form: conditional branch testing the nonce digit value.
- Addresses of ec_GFp_simple_add and ec_GFp_simple_dbl: spied with FLUSH+FLUSH.
- Statistical profiling of cache addresses to select most relevant leakage points for attack.
- Pattern recognition (Intel i7-6700 CPU@3.40GHz) with e.g. Random Forest: 95% acuracy.
- ECDSA key fully recovered from nonce bits with LLL Latice reduction algorithm.
- Highly discreet and fully automated key recovery.

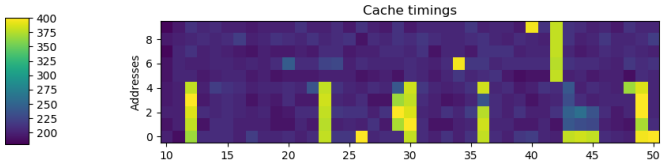


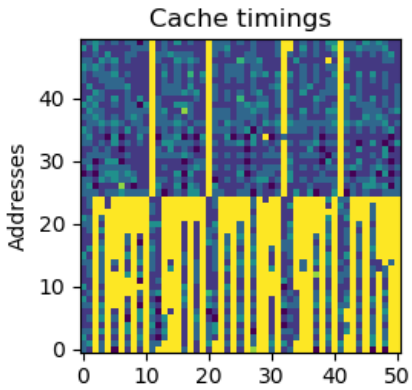
SECURE-IC

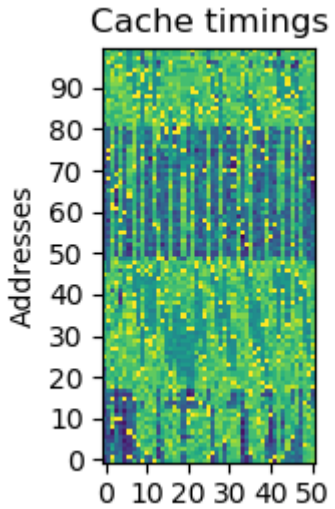
CATALYZR

Profiling Module

- The number of addresses to probe is limited!





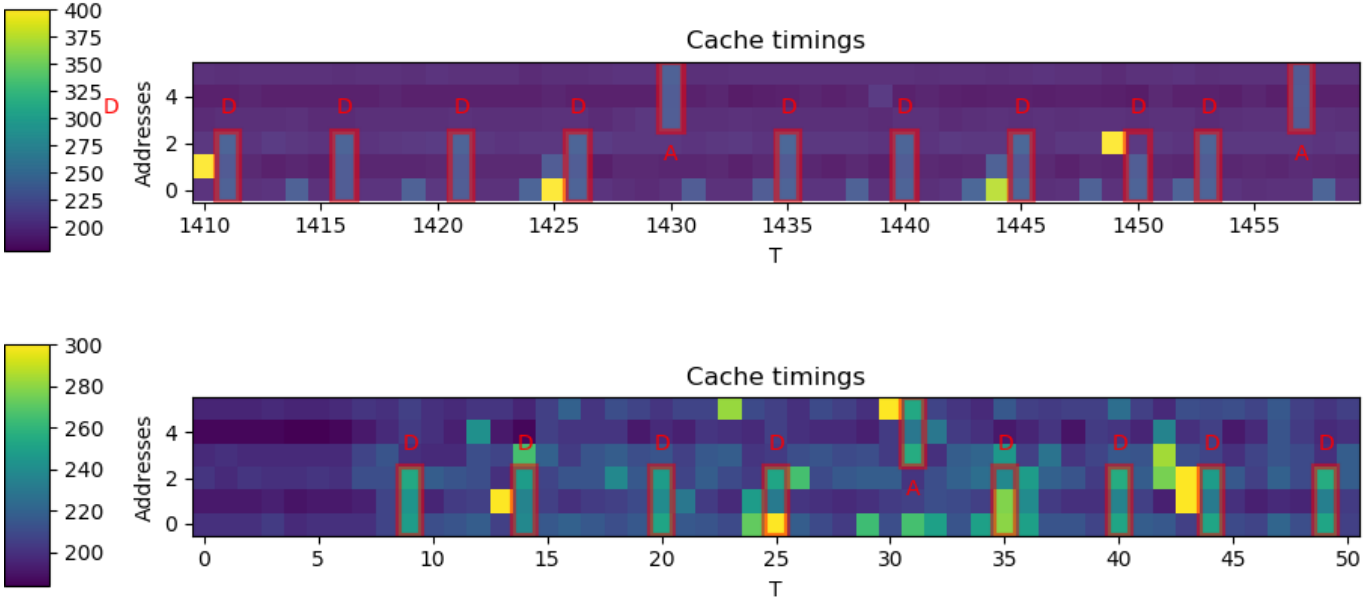


- What addresses to use for probing?
  - Over several hundreds.
  - Low noise.
  - Combination of addresses?

- Statistical profiling module : Unsupervised Learning (eg PCA)
- Automatic selection of informative addresses

Pattern recognition

- Supervised sequence generation with misaligned labels
- Allows to consider different aspects of the problem
- Practical and easy way to implement pattern recognition

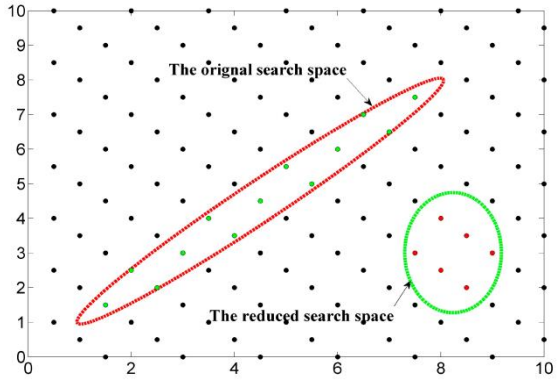


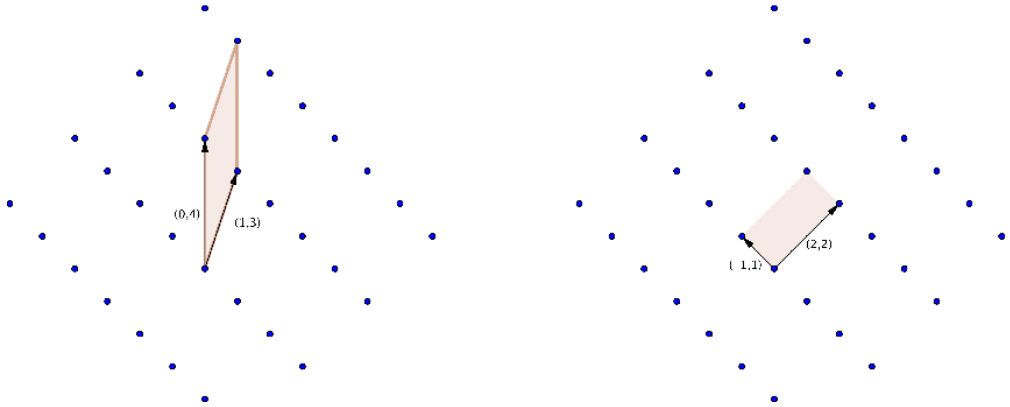
SECURE-IC

CATALYZR

Lattice reduction

- Reduce the search space of the nonce
- Lattice reduction algorithm
- Shortest Vector Problem
- Polynomial complexity
- Inputs: nonce bits
- Output: private key





Computation of LLL-reduced lattice basis

Conclusion

- Machine Learning is a practical way:
  - To select interest points
  - To implement pattern recognition
- Machine Learning provides confidence indicators
- Limitations:
  - Machine Learning metric => Accuracy (often)
  - Efficiency of an attack = different metrics
  - The quality of a model is not always reflected in the deployed attack
  - Cross architecture models

SECURE-IC

THE SECURITY SCIENCE COMPANY

THANKS FOR YOUR ATTENTION

CONTACT

EUROPE	sales-EU@secure-IC.com
APAC	sales-APAC@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com