**PHISIC’22 – PROGRAM**

*Scientific & Program Committee.* Driss Aboulkassimi, Jean-Max Dutertre, Philippe Jaillon, Pierre-Alain Moëllic // *Organization Committee.* Bernard Dhalluin, Olivier Provitina, Raphaël Viera, Romain Wacquez

### TUESDAY, 17th MAY 2022

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30</td>
<td>Welcome</td>
<td></td>
</tr>
<tr>
<td>08:55</td>
<td>Coffee</td>
<td></td>
</tr>
<tr>
<td>09:00</td>
<td>Session Fault Injection Analysis</td>
<td>D. Aboulkassimi</td>
</tr>
<tr>
<td>10:15</td>
<td>Communication</td>
<td></td>
</tr>
<tr>
<td>10:45</td>
<td>Break / Poster Session / Demos</td>
<td>P-A. Moëllic</td>
</tr>
<tr>
<td>11:15</td>
<td>Session Security of Machine Learning</td>
<td></td>
</tr>
<tr>
<td>12:30</td>
<td>Lunch / Poster Session / Demos</td>
<td></td>
</tr>
<tr>
<td>14:00</td>
<td>Session RISCV (I)</td>
<td>O. Potin</td>
</tr>
<tr>
<td>14:50</td>
<td>Break / Poster Session / Demos</td>
<td></td>
</tr>
<tr>
<td>15:20</td>
<td>Session RISCV (II)</td>
<td>O. Potin</td>
</tr>
<tr>
<td>16:10</td>
<td>End + Social Event</td>
<td></td>
</tr>
</tbody>
</table>

### WEDNESDAY, 18th MAY 2022

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00</td>
<td>Session Cryptography</td>
<td>N. El Mrabet</td>
</tr>
<tr>
<td>10:40</td>
<td>Break / Poster Session / Demos</td>
<td></td>
</tr>
<tr>
<td>11:10</td>
<td>Session Defense : Resilience &amp; Detection</td>
<td>J-M. Dutertre</td>
</tr>
<tr>
<td>12:25</td>
<td>Lunch / Poster Session / Demos</td>
<td></td>
</tr>
<tr>
<td>15:45</td>
<td>Session Side-Channel Analysis</td>
<td>S. Pontie</td>
</tr>
<tr>
<td>17:00</td>
<td>Poster Session / DEMOS / END</td>
<td></td>
</tr>
</tbody>
</table>

**FAULT INJECTION ANALYSIS** (oral + poster) ...........................................................................................................2

**SECURITY OF MACHINE LEARNING** (oral + poster) ...........................................................................................................4

**RISCV** (oral + poster) .................................................................................................................................................5

**CRYPTOGRAPHY** (oral) .......................................................................................................................................................6

**DEFENSE : RESILIENCE & DETECTION** (oral) ........................................................................................................................8

**SIDE-CHANNEL ANALYSIS** (oral + poster) ..........................................................................................................................9

**EMBEDDED SYSTEMS** (poster) .............................................................................................................................................12
FAULT INJECTION ANALYSIS (oral + poster)

Software-based Fault Injection on Memory Transfers, Joseph GRAVELLIER, THALES

ABSTRACT
Today's integrated memory controllers use complex hardware such as delay-lines to monitor and control signal timings during external memory transfers. Because memory chips with different timing specifications may be used, delay-line tuning registers often remain accessible and programmable from the application processor. In this talk, we will introduce FaultLine and the concept of delay-line-based fault injection. We will show that by modifying the delay-line calibration value through a simple register access, a malware may induce faults in memory transfers and jeopardize the security of concurrently running assets. Then, we will present fault injection experiments conducted on an OS-capable system-on-chip that led to the extraction of cryptographic secrets.

Laser fault injection in NOR-Flash memories, mechanism, protections, Jean-Max DUTERTRE, Mines Saint-Etienne

ABSTRACT
The Flash memory of a Microcontroller Unit (MCU) is an important part of its attack surface as it contains its firmware and its security related data (e.g. passwords and cryptographic keys). Recent research works report the use of Laser Fault Injections (LFI) to corrupt the firmware at run time by targeting the Flash memory during its read operations (data reads from Flash were also faulted). These faults, induced on a single bit and following a bit-set fault model, were non-permanent: the data stored in Flash stayed unaltered while only their read copies were corrupted. Another work reports an extension of this fault model in the form of the ability to induce permanent faults by laser into a Flash memory. Single bit faults, that followed a bit-reset fault model, were induced during the Flash write operations. In this presentation we discuss these fault models and describe a hardware counter-measure that makes it possible to detect laser fault injection attempts.

SCI-FI: Control Signal, Code, and Control Flow Integrity against Fault Injection Attacks, Thomas CHAMELOT, CEA-LIST

ABSTRACT
Fault injection attacks are known to be able to tamper with the code and the control flow of a program. Several counter-measures have been proposed to thwart such attacks [1,2,4,5]. However, recent work highlights that some vulnerabilities exist in the micro-architecture [3]. As a consequence, the control signals involved in the whole pipelined execution of instructions inside the processor also needs to be protected. Such so-called execution integrity is not covered by state-of-the-art approaches. We present SCI-FI, a counter-measure against fault injection attacks that guarantees simultaneously code integrity, control-flow integrity and execution integrity. SCI-FI is a mixed hardware and software counter-measure. It combines sequentially two techniques: a signature-based approach and a duplication-based one. Code integrity and control flow integrity are ensured by the signature-based approach, which needs compiler support as well as additional custom instructions. The duplication-based approach guarantees execution integrity until the end of the execution pipeline. The security level provided by SCI-FI highly depends on the signature function as well as the size of the reference signatures. SCI-FI can be implemented with several signature functions, as the properties of the signature function imply a trade off between security (e.g., number of bit flips that can be detected) and silicon area overhead. It may also impact code size and code slowdown. We also illustrate how signature constructs based on cryptography can also support other security properties, such as authentication.
This talk will cover work already published [6, 7] regarding SCI-FI and its implementation in a RISC-V core, and in addition we will describe how SCIFI handles indirect branches regarding the CFI protection. We will present evaluation results regarding the overheads in terms of silicon area, code size and execution time. These results show that our countermeasure is competitive regarding existing code and control-flow integrity approaches, while also providing control signal integrity. To the best of our knowledge, our countermeasure is the first to cover fault injections targeting the processor microarchitecture.


**ABSTRACT**

Electromagnetic fault injection on a RISC-V processor targeting a FPGA: fault models and countermeasures, Amélie MAROTTA, INRIA

Electromagnetic Fault Injection (EMFI) attacks on microcontrollers have been the subject of many papers, describing its effect on the execution or data flow and how to exploit it. Furthermore, several models were proposed to explain how it affects the microarchitecture. How those two aspects are related is something that needs to be researched thoroughly.

Our goal is to develop efficient countermeasures against EMFI for a RISC-V processor implemented on a FPGA. To do so, we study the effect of EMFI on several levels. As a starting point, we are currently designing an experiment made of a set of hardware architecture microbenchmarks aiming at getting a better comprehension of the effect of EMFI on logic components (gate, flip-flop), depending on various parameters: the design in itself but also its size, placement and routing, the kind of probe used, etc. We will then take a look at how these effects propagate to the microarchitecture, and adapt countermeasures to the different vulnerable parts of the processor.

**ABSTRACT**

A CFI Verification System based on the RISC-V Trace Encoder, Anthony ZGHEIB, Mines Saint-Etienne

Control-Flow Integrity (CFI) is used to check a program execution flow and detect whether it is correctly executed and not altered by software or physical attacks. We present a CFI verification system for programs executed on RISC-V cores. Our solution is based on the RISC-V instruction Trace Encoder (TE). The TE provides information about the execution path of the user program. Two approaches are proposed. One is consistent with the RISC-V TE standard. It permits to detect instruction skip attacks on function calls, on their returns and on branch instructions. The second implies an evolution of the RISC-V TE specifications to detect more complex fault models as the corruption of any discontinuity instruction. We implemented both approaches on a RISC-V core and simulated their efficiency against Fault Injection Attacks (FIA). Compared to existing CFI solutions, our methodology does not modify the user application code nor the RISC-V compiler.
Concrete ML: A Data-Scientist-Friendly Toolkit for Machine Learning Over Encrypted Data, Jordan FRERY, ZAMA.IA

ABSTRACT
Privacy-preserving machine learning is a new technology that allows users to leverage intelligent cloud applications that process their personal data without revealing this data to any third party. In general, private computation using encrypted data aims to nullify the damage done by data leaks and reduce cybersecurity risks for cloud providers. In this work we introduce Concrete ML, a machine learning toolkit that data-scientists can use to create machine learning models that operate on encrypted data. Particular care was given to the simplicity of our python package, in order to make it usable by any data scientist, notably without any prior cryptography knowledge. Fully Homomorphic Encryption. Concrete ML is based on TFHE, which stands for Torus Fully-Homomorphic Encryption [CGGI20]. Thanks to the homomorphic property of the scheme, one can easily perform linear operations on ciphertexts (e.g., matrix multiplications and convolutions): such operations are often referred to as leveled operations. To perform non-linear operations which are typically activations (e.g., Relu or Sigmoid), we use fast Programmable BootStrapping (PBS) [CJL+20], which is a unique feature of TFHE.

Related Work. Several companies or researchers have worked on FHE libraries or privacy-preserving machine learning. We can notably mention Seal [SEA], HELib [HEL], Palisade [Pal] and Lattigo [Lat]. More information can be found in the respective repositories or papers, as well as on fhe.org.


Subverting Facial Recognition Systems, Richard MARRIOTT, IDEMIA

ABSTRACT
Facial recognition is an open-set problem, i.e. facial recognition systems must be adaptable for identification and verification of previously unknown groups of people. This adaptation stage – enrolment – provides an additional point at which an attacker might target a facial recognition system. For this reason, amongst others, facial recognition warrants particular attention when considering potential threats to deployed systems. A review of the attack-focused facial recognition literature was performed at IDEMIA as part of the initial stages of project PICTURE (Physical and Intrinsic Security of Embedded Neural Networks) with the intention of characterizing all potential forms of threat to deployed systems. This talk summarizes the literature-review, discussing topics such as the vulnerability of facial recognition systems to adversarial attacks (both digital and physical), face-morphing attacks, obfuscation attacks, and the poisoning of training data.

Fooling a Neural Network with Laser Fault Injection, Mathieu DUMONT, CEA-LETI / Mines Saint-Etienne

ABSTRACT
For many domains, machine learning proposes very efficient solutions to handle complex data and performs challenging and critical tasks. However, the growing popularity of edge-deployed neural networks in large
variety of embedded systems brings new security challenges for the AI community. Indeed, physical access to the integrated circuit constitutes a real threat against the integrity, confidentiality and accessibility of neural network models. In the same way that a cryptographic key could be recovered, an attacker could steal IP model or personal data. Among physical attacks, Fault Injection are known to be very powerful with a wide spectrum of attack vectors as the Laser beam injection. Here, we evaluate the vulnerabilities of embedded neural networks with state-of-the-art laser equipment. By targeting the Flash memory of a typical 32-bits microcontroller, transient mono-bit faults are induced on neurons weight values, leading to a misclassification of the neural network. Those works show that Fault Injection attacks constitute a real threat for embedded machine learning models, testifying a significant need from a security point of view.

Poster

Neural Network Model Extraction with Side-Channel Analysis, Raphaël JOUD, CEA-LETI / Mines Saint-Etienne

Abstract

Embedded Deep Neural Network models play an increasingly important role in several domains, especially IoT-related. However, embedded DNN suffer from broad spectrum of attacks threatening their integrity, confidentiality and availability. We focus on fidelity-oriented side-channel-based extraction of DNN weights values. We present a method based on electromagnetic (EM) emanation statistical analysis rather than timing variations and raise several challenges related to the complexity of an embedded inference process.

Poster

Parameter-based Attacks Against Neural Network Models, Kevin HECTOR, CEA-LETI / Mines Saint-Etienne

Abstract

An important evolution about AI concerns the deployment of machine learning models on a large variety of devices. However, this deployment raises many security issues affecting integrity, confidentiality and availability. Leveraging these weaknesses, powerful algorithmic (API-based) attacks like adversarial examples have been proposed. These threats do not target the model implementation and its intrinsic parameters. This work is focused on fault injection methods that target the parameters (weights) of a deep neural network model. A first step is a simulation-based analysis of state-of-the-art attacks, such as Bit-Flip Attack (BFA), to better understand model’s flaws as well as design adapted defense schemes.

RISCV (oral + poster)

Protecting a RISCV core against fault and side channel attacks, Gaëtan LEPLUS, CA-LETI / Laboratoire Hubert Curien

Abstract

Because of their diametrically opposite countermeasure, it is difficult to handle the problems of side channels and fault injection at the same time. We propose countermeasures for increasing security against these two attacks while keeping costs to a minimum, by masking instructions with previously executed instructions and by hardware insertion of dummy instructions. We also protect the execution stage at every moment of computation by adding to the data an authenticity tag which is homomorphic to binary logic and arithmetic operations and which depends on a secret key.

Recovering Information on a RISC-V CPU with a Baremetal Micro-Architectural Covert Channel, Valentin MARTINOLI, THALES

Abstract
We propose to study the micro architectural vulnerabilities of the open-source RISC-V CPU named CVA6. We have built a realistic scenario for extracting information and propose an analysis on how to reduce the impact of noise on the attack, while staying as close as possible to hardware level through baremetal simulations. Micro architectural attacks take advantage of optimization mechanisms inside recent CPUs to cause information leakages. Competitive access to limited and shared hardware resources is the root cause of micro architectural covert channels. We used this behavior to implement a Prime + Probe micro architectural covert channel, and we simulated the extraction of secret information through the L1 data cache of the CVA6, a 64-bit open-source application class RISC-V processor. This constitutes a proof of concept that RISC-V cores are not immune by design to these threats. We propose to look at the different challenges that need to be taken up to adapt a well-known micro architectural covert channel to a specific attack scenario. We also experimented the implications that adding an Operating System might have on the said attack by adding a scheduling mechanism and generating noise. This enabled us to study the impact of scheduling and multiprocessing on our micro architectural timing covert channel.

**Protected Extension of Lightweight Cryptographic Algorithms on RISC-V**, Jean-Luc DANGER, Telecom Paris

**ABSTRACT**

Lightweight Cryptography (LWC) proposes interesting candidates for securing the communications in constrained environments. As many lightweight cryptographic algorithms have been, the features of agility and genericity have to be be considered. A high robustness against side-channel analysis (SCA) is also required when the connected object executes sensitive applications or manipulates private data. In this talk, a extended instruction set of the RISC-V ISA is presented. It is able to be executed in a robust manner against first-order SCA by using the Rotating S-Box Masking (RSM) protection. This extension takes advantage of instructions which are common to most LWC algorithms, thus provide agility in addition to security with only 40% of extra combinatorial logic. It has been implemented and validated on the VexRisc core processor. The security analysis showed that SCA on PRESENT were impossible with up to 1 million traces.

**Tightly and Loosely Coupled RISC-V Accelerators for Post-Quantum Cryptography**, Georg SIGL, Technische Universität München (TUM)

**ABSTRACT**

Hardware Acceleration of PQC is accompanying the NIST standardization process. We have contributed to this process tightly coupled accelerators into a RISC-V 32-bit processor, which combine medium performance and power gain with low resource overhead and high flexibility. This enables lattice based PQC schemes even on low cost and low performance microcontrollers. SIKE has been proposed as alternate candidate. Its advantage are short key and message lengths, but it suffers from high computation times. This forces the use of hardware accelerators. The talk presents results of our chip designs in 65nm and gives an outlook at our new design in 22nm.

**CRYPTOGRAPHY (oral)**

**TPMs (Trusted Platform Modules) : Where we are now?,** Julien FRANCOQ, NAVAL GROUP

**ABSTRACT**

TPMs have been imagined more than 15 years ago to protect the integrity of PCs and servers. However, it took a long time to definitelty integrate and adopt them in different applications and markets (IoT, industrial
systems, etc.). This talk will give some technical insights on TPMs, particularly their architectures, their usage, their benefits, but also the published and fixed attacks on them.

*The Hidden Parallelepiped Is Back Again: Power Analysis Attacks on Falcon, Melissa Rossi, ANSSI*

**ABSTRACT**

Falcon is a very efficient and compact lattice-based signature finalist of the NIST’s Post-Quantum standardization campaign. This work assesses Falcon’s side-channel resistance by analyzing two vulnerabilities, namely the pre-image computation and the trapdoor sampling. The first attack is an improvement of Karabulut and Aysu (DAC 2021). It overcomes several difficulties inherent to the structure of the stored key like the Fourier representation and directly recovers the key with a limited number of traces and a reduced complexity. The main part of this paper is dedicated to our second attack: we show that a simple power analysis during the signature execution could provide the exact value of the output of a subroutine called the base sampler. This intermediate value does not directly lead to the secret and we had to adapt the so-called hidden parallelepiped attack initially introduced by Nguyen and Regev in Eurocrypt 2006 and reused by Ducas and Nguyen in Asiacrypt 2012. We extensively quantify the resources for our attacks and experimentally demonstrate them with Falcon’s reference implementation on the ELMO simulator (McCann, Oswald and Whitnall USENIX 2017) and on a ChipWhisperer Lite with STM32F3 target (ARM Cortex M4). While the success of these attacks may be unsurprising because the reference implementation does not claim any side-channel protection, these new attacks highlight the need for side-channel protection for one of the three finalists of NIST’s standardization campaign by pointing out the vulnerable parts and quantifying the resources of the attacks.

*Post-Quantum Crypto Deployment on Smartcard/Secure Element, Aurélien Greuet, IDEMIA*

**ABSTRACT**

The NIST has launched a Post-Quantum Cryptography (PQC) standardization process. The goal is to update their crypto standards to include Post-Quantum algorithms. They are expected to be safe against a quantum attacker, but they can be more memory consuming and slower than classical crypto, like RSA or algorithms based on elliptic curves. Smartcard and secure elements are used in secure products like bank cards, SIM cards, passports, ID cards, etc. Hence, demand for PQC on these devices will probably begin as soon as the standards are released. To anticipate this demand, PQC deployment must start as soon as possible, on today’s chips. However, smartcards are very limited in terms of RAM capacity, CPU features and frequency. In addition, smartcard implementations must be secure against a large set of side-channel attacks like power/electromagnetic correlation attacks, template attacks, fault attacks, etc. This makes implementations slower and even more memory consuming. Nevertheless, strong constraints on execution time and memory usage must be fulfilled, making PQC deployment a tricky challenge on smartcard. We present an overview of these constraints, the impact on the deployment of PQC on smartcard and some ideas to make the transition easier.

*SIKE Channels: Zero-Value Side-Channel Attacks on SIKE, Elise Tasso, CEA-LETI / Mines Saint-Etienne*

**ABSTRACT**

Starting in 1994 with Shor’s factorization algorithm, quantum computers have been shown to threaten classic asymmetric cryptography. Thus the National Institute of Standards and Technology launched the Post-Quantum Cryptography Standardization Process in December 2016 for research teams worldwide to propose algorithms that can be implemented on classical computers but resist quantum computer attacks. There are protocols for encryption and key encapsulation and protocols for signature. They are based on various mathematical tools. We will focus here on the Supersingular Isogeny Key Encapsulation (SIKE),
the only candidate based on isogenies. It is now an alternate candidate in the third round of the standardization process, meaning that it is deemed promising enough by the NIST to pursue research on it. Like the other candidates, SIKE is believed to be mathematically secure, but vulnerabilities may appear in its implementations. Both active and passive hardware attacks have been found to affect it. We present here new side-channel attacks on SIKE. Previous works had shown that SIKE is vulnerable to differential power analysis and pointed to coordinate randomization as an effective countermeasure. We show that coordinate randomization alone is not sufficient, as SIKE is vulnerable to a class of attacks similar to refined power analysis in elliptic curve cryptography, named zero-value attacks. We describe and confirm in the lab two such attacks leading to full key recovery, and analyze their countermeasures.

**DEFENSE : RESILIENCE & DETECTION (oral)**

*Monitoring and Analysis of Electromagnetic Emanation from Malware Execution*, Damien MARION, IRISA

**ABSTRACT**
Research about IoT malware and tools developed for automated IoT malware classification are limited. IoT and embedded technologies use numerous customized firmware and hardware, without taking into consideration security issues, which make them an attractive attack surface for cybercriminals, especially malware authors. Various types of state-of-the-art malware on Microsoft Windows took decades from the first known malicious software to happen in the wild, now start emerging on IoT devices in a shorter time. We present a novel, robust and promising approach of leveraging electromagnetic emanations to identify the kinds of malware that are targeting the Raspberry Pi device. Using our approach, malware analysts can obtain accurate information about the type and identity of IoT malware, even with obfuscation techniques that can prevent static and symbolic binary analysis. We recorded traces of more than 100K measurements from IoT devices infected with various malware samples and realistic benign activity. Our method allows deployment independent of available resources with no overhead. Moreover, our approach has the advantage that malware authors are less likely to detect and bypass. In our experiments, we were able to predict three common types of malware vs. benign activities with 99.82% accuracy.

*Side Channel and Fault Injection Analysis of Physical Unclonable Functions*, Michael PEHL, Technische Universität München (TUM)

**ABSTRACT**
Physical Unclonable Functions (PUFs) have become a raising technology for small, resource-constrained devices as they are used, e.g., in the internet of things. The main applications are authentication and to store a cryptographic key securely. However, with the increasing interest in this technology, also attacks on PUFs raise increasingly attention. Modeling-attacks are the main threat when using PUFs for authentication with challenge-response protocols. For key-storage scenarios, hardware-related attacks, like side channel attacks (SCA) and fault injection attacks (FIA) are of higher relevance. This presentation discusses two possible attack points for such systems: First, it demonstrates SCA on an oscillator based PUF primitive as well as protection mechanisms. In particular, the presentation shows as attacks and corresponding counter measures for the Loop PUF, a highly promising PUF primitive for key-storage, when using it in combination with different schemes for bit derivation. Second, the presentation introduces findings from attacks on the PUF post-processing. It shows that a well-protected design requires consideration of SCA as well as of FIA on the error correction needed to derive a stable cryptographic key from a PUF. It also suggests possible solution for the presented weaknesses. The analysis results and countermeasures presented in this talk have been published in [1-4].
Active shielding against physical attacks by observation and fault injection: ChaXa, Clément GAINÉ, CEA-LETI / Mines Saint-Etienne

ABSTRACT
Electronic components may contain sensitive data, either on the storage chip or on the microprocessor. Deliberate and precise perturbation of their operation or measurement of their activity through auxiliary channels can be used to extract the secrets they contain. For these reasons, it is important that the integrity of the integrated circuit is ensured. It is therefore necessary to implement protection mechanisms against threats such as physical attacks. In this talk, we present a new device for protection against and supervision of fault injection and electromagnetic listening attacks. Patented by the CEA in January 2021, ChaXa aims to address the security of both EM fault injection and EM side-channel attacks. It allows the detection of several types of physical attacks and provides an appropriate response for each type of threat. A layer of ferrite particles, deposited on the surface of the chip, forms a first level of protection by passive shielding. It attenuates the signals emitted by the chip (thus preventing malicious interception) as well as those produced in the event of attacks by injection of electromagnetic faults. Coils are arranged on either side of the chip and form an active magnetic barrier capable of detecting electromagnetic listening probes or of generating random electromagnetic noise intended to prevent side-channel attacks.

SIDE-CHANNEL ANALYSIS (oral + poster)

Information Bounds and Convergence Rates of Profiling Attacks for Side-Channel Security Evaluators, Loïc MASURE, Université Catholique de Louvain

ABSTRACT
Current side-channel evaluation methodologies exhibit a gap between inefficient tools offering strong theoretical guarantees and efficient tools only offering heuristic (sometimes case-specific) guarantees. Profiled attacks based on the empirical leakage distribution correspond to the first category. Bronchain et al. showed at Crypto 2019 that they allow bounding the worst-case security level of an implementation, but the bounds become loose as the leakage dimensionality increases. Template attacks and machine learning models are examples of the second category. In view of the increasing popularity of such parametric tools in the literature, a natural question is whether the information they can extract (with a given choice of set of models) can be bounded. In this paper, we first show that a metric conjectured to be useful for this purpose, the hypothetical information, does not offer such a general bound. It only does when the assumptions exploited by a parametric model match the true leakage distribution. We therefore introduce a new metric, the training information, that provides the guarantees that were conjectured for the hypothetical information for practically-relevant models. We next initiate a study of the convergence rates of profiled side-channel distinguishers which clarifies, to the best of our knowledge for the first time, the parameters that influence the complexity of a profiling. On the one hand, the latter has practical consequences for evaluators as it can guide them in choosing the appropriate modeling tool depending on the implementation (e.g., protected or not) and contexts (e.g., granting them access to the countermeasures’ randomness or not). It also allows anticipating the amount of measurements needed to guarantee a sufficient model quality. On the other
hand, our results connect and exhibit differences between side-channel analysis and statistical learning theory.

References:
Efficient Profiled Side-Channel Analysis of Masked Implementations, Extended, [eprint.iacr.2022.158]
Information Bounds and Convergence Rates for Side-Channel Security Evaluators [coming soon on eprint].

A Side Journey to Titan, Thomas ROCHE, Victor LOMNE, NINJA LAB

ABSTRACT
The Google Titan Security Key is a FIDO U2F hardware device proposed by Google (available since July 2018) as a two-factor authentication token to sign in to applications (e.g. your Google account). Our work describes a side-channel attack that targets the Google Titan Security Key's secure element (the NXP A700X chip) by the observation of its local electromagnetic radiations during ECDSA signatures (the core cryptographic operation of the FIDO U2F protocol). In other words, an attacker can create a clone of a legitimate Google Titan Security Key.

In a nutshell, the FIDO protocol works as follows:

- The user first performs a registration phase with his FIDO U2F token for every application using the FIDO U2F protocol as two-factor authentication, which generates an ECDSA key pair, and sends the key handle and the public key to the application's server.
- Then, for each authentication request, the application's server sends a challenge to the user device, which transfers it to the FIDO U2F token. The FIDO U2F token uses the associated ECDSA private key to sign the challenge and sends back the result to the server.

In a first phase of our study, we performed a teardown of the Titan Key, and figured out that the secure element performing the cryptographic operations is the NXP A700X. As there is no way in the FIDO protocol to extract the ECDA private key from a FIDO U2F token, we began our study in full blackbox with an unknown key context.

To understand the NXP ECDSA implementation, find a vulnerability and design a key-recovery attack, we had to make a quick stop on Rhea (NXP J3D081 JavaCard smartcard). Freely available on the web, this product looks very much like the NXP A700X chip and uses the same cryptographic library. Rhea, as an open JavaCard platform, gives us more control to study the ECDSA engine.

We could then show that the electromagnetic side-channel signal bears partial information about the ECDSA ephemeral key. The sensitive information is recovered with a non-supervised machine learning method and plugged into a customized lattice-based attack scheme. Note that we used a side-channel platform which costs about 10k euros for performing the side-channel measurements.

Finally, 4000 ECDSA observations were enough to recover the (known) secret key on Rhea and validate our attack process. It was then applied on the Google Titan Security Key with success (this time by using 6000 observations) as we were able to extract the long term ECDSA private key linked to a FIDO U2F account created for the experiment.

As a side observation, we identified a novel correlation between the elliptic curve group order and the lattice-based attack success rate. In short, contiguous blocks of zeros or ones in the binary representation of the elliptic curve group order favorably impacts lattice attack success rate.

Previous Communications of this work:
- This work has been published in Usenix Security 2021
- Workshop WAC4 (co-located with CRYPTO 2021)
- Hardwear.io NL 2021 (physical conference)

Simulating and interpreting EM side-channel attacks at chip level prior to fabrication, Davide POGGI, STMicroelectronics

ABSTRACT
EM side-channel attacks (SCA), which exploit essentially the magnetic field generated by ICs, are commonly used by adversaries to retrieve secret information manipulated by integrated circuits. Due to the increasing resolution and effectiveness of EM equipment used to perform these attacks, it is becoming increasingly difficult to design secure circuits robust enough to resist these attacks. One reason is that there is no CAD tool in literature allowing to check the robustness of ICs against EM SCA prior to fabrication. The first contribution of this work is the development of a simulation flow able to reproduce the magnetic field radiated by ICs. This flow is based on ANSYS RedHawk, an industrial voltage drop tool. The second contribution is a methodology to localize the root cause of leakages in ICs as well as EM hotspots, i.e., positions above the IC surface where an adversary can place an EM probe to capture secrets. The latter contribution is based on the concept of Noise-to-Add which is introduced in order to overcome the absence of noise in simulations (noise which is omnipresent in practice) that limits their interpretability. The soundness of the developed simulation flow is demonstrated by confronting, for the first time, experimental and simulated correlation maps.

Neural Estimation of the Mutual Information and its Application to Side-Channel Analysis, Valence CRISTIANI, CEA-LETI

ABSTRACT
A large variety of side-channel attacks have been developed to extract secrets from electronic devices through their physical leakages. Whatever the utilized strategy, the amount of information one could gain from a side-channel trace is always bounded by the Mutual Information (MI) between the secret and the trace. This makes it, all punning aside, a key quantity for leakage evaluation. Unfortunately, traces are usually of too high dimension for existing statistical estimators to stay sound when computing the MI over full traces. However, recent works from the machine learning community have shown that it is possible to evaluate the MI in high dimensional space thanks to newest deep learning techniques. This talk will explores how this new estimator could impact the side-channel domain both for leakage assessment and for unsupervised mutual information based attacks.

Empirical Evaluation of the Resilience of Novel Non-Algebraic AES S-Boxes to Power Side-Channel Attacks, Samuele Yves CERINI, CINI/Univ Turin

ABSTRACT
In the area of hardware security, the study of effective countermeasures against side-channel analysis is becoming increasingly crucial, as this class of attacks reaches higher rates of effectiveness with respect to classical cryptanalysis. While implementation-level countermeasures are achieving promising results, the academic community has recently focused on solutions that can reduce leakage from the cryptographic mathematical layer, regardless of the underlying hardware/software architecture. In the field of symmetric encryption schemes (such as AES), novel substitution structures have been proposed, claiming an improved side-channel resistance without any additional costs in terms of area, performance or power consumption. To the best of our knowledge, most of these solutions have been studied only from a mathematical point of view, and are still lacking practical experimentation on resource-constrained devices. This presentation provides insights on an empirical evaluation of the latest AES S-Box proposals. The necessary data has been collected in a reference scenario with limited noise effects, targeting an unprotected software implementation of the AES-128 algorithm running on an 8-bit microcontroller. The results show that despite claims of resistance to SCA, these new countermeasures do not provide significantly improved protection over the standard version of AES, let alone enough to thwart an attack.

POSTER A remote environment for education training on power side-channel analysis, Gianluca ROASCIO, CINI/Univ Turin

ABSTRACT
With the very rapid digital revolution we are experiencing, the presence of cybersecurity experts becomes critical in every organization and on multiple levels. However, classical and theory-oriented training seems
to lack effectiveness and power of attraction, while professional selection and training processes based on cybersecurity gamification are being successfully experimented, among which Capture-the-Flag (CTF) competitions certainly stand out. Nevertheless, careful analysis reveals that such initiatives have a major shortcoming in addressing security issues of the lowest level of IT systems: the hardware. This lack appears to be unjustified from the point of view of attack news and dangerousness, and it is probably due to an inadequate technical knowledge of the subject, as well as to an evident logistic problem deriving from the need to provide or make accessible a certain number of different devices to a number of people often wide and possibly remote. This presentation focuses on a platform able to provide interactive training lectures and CTF challenges on power side-channel analysis, leveraging real hardware physically connected to a server. The platform is presented from a technical perspective, and data on its efficiency, stability and scalability are offered.

**SCA**\textit{Lib}, Olivier Brochain, Gaëtan Cassiers, Université Catholique de Louvain

**ABSTRACT**

We describe an attack against the ANSSI Side-Channel Analysis Database (ASCAD), which recovers the full key using the leakage of a single masked block cipher execution. The attack uses a new open-source Side-Channel Analysis Library (SCA**Lib**), which allows running the leakage profiling and attacking in less than 5 minutes. It exploits well-known techniques, yet improves significantly over the best known attacks against ASCAD. We conclude by questioning the impact of these experimental findings for side-channel security evaluations.


**EMBEDDED SYSTEMS** (poster)

**POSTER** \textit{Multi-harvesting fully-integrated system architecture combining AC and DC sources}, Malek Teib, STM / IM2NP

**ABSTRACT**

Internet of Things and growing popularity of connected devices are emerging demand for wearables applications which is pushing ultra-low power secure systems development. Thus, having a system running at low voltage supply with low power consumption introduces the use of ambient energy harvesting. Besides, batteries have several limitations reducing their compatibility with wearables, such as periodical need for recharge, limited life-time, heavy and large form factor and non-eco-friendly life-cycle. Therefore ambient energy harvesting technology gives a promising alternative for self-powered wearables. The integration of these solutions on the same silicon support is a real technological and technical challenge. This presentation proposes a multi-harvesting fully-integrated system architecture combining AC and DC sources.

The proposed system is based on a MATLAB/Simulink model which allows the calibration of an optimal solution. Then, it is designed and simulated in 40 nm CMOS process, proving that using an AC source as second input, allows to start a harvesting system with very low DC source as main source.

**POSTER** Domain Adaptation & Pruning Techniques for Embedded Neural Networks, Baptiste Nguyen, CEA-LETI / Mines Saint-Etienne

**ABSTRACT**

The wide deployment of Machine Learning models is an essential evolution of Artificial Intelligence, predominantly by porting deep neural networks in constrained hardware platforms such as 32 bits
microcontrollers. For many IoT applications, the deployment of such complex models is hindered by two major issues that are usually handled separately. For supervised tasks, training a model requires a large quantity of labelled data which is expensive to collect or even intractable in many real-world applications. Furthermore, the inference process implies memory, computing and energy capacities that are not suitable for typical IoT platforms.

We jointly tackle these issues by investigating the efficiency of model pruning techniques under the scope of the single domain generalization problem. Our experiments show that a pruned neural network retains the benefit of the training with single domain generalization algorithms despite a larger impact of pruning on its performance. We emphasize the importance of the choice of the pruning method, more particularly between structured and unstructured pruning as well as the benefit of data-agnostic heuristics that preserve their properties in the single domain generalization setting.