Practical Side-Channel Attacks on Real World Devices

Victor Lomné

NinjaLab

ICO – Demi-journée scientifique – Sécurité pour/par le Matériel

May 4, 2026 – Toulouse, France

NinjaLab : About us

- NinjaLab founded in 2017, based in Montpellier, France

- Team :
  - Dr. Thomas Roche (university of Grenoble, ANSSI, Apple)
  - Dr. Victor Lomné (university of Montpellier, ANSSI)
  - Malek Sfaxi (EURECOM, research engineer & PhD student)
  - Lucas Tabary-Maujean (ENS, PhD student – hosted)
  - Paul Martinez (INSA, intern)

- Our activities :
  - Penetration tests on embedded systems
  - Our speciality : **side-channel attacks** on crypto. implementations
    smartcard, MCU, SoC, FPGA, IoT, Smartphone, . . .



NinjaLab : Research Activities

- Participation to collaborative research projects :
  - Projet SCATTER : 2018 $\rightarrow$ 2022 – FUI
  - Projet VERISICC : 2019 $\rightarrow$ 2022 – RAPID
- Academic research in crypto. / HW security

  6 publications in top conferences
- 2 PhD students (with LIRMM) :
  - 2020 $\rightarrow$ 2024 : Camille Mutschler – SCA on PQCrypto
  - 2025 $\rightarrow$ 2028 : Malek Sfaxi – Physical attacks on SoCs
- Self-funded SCA pen. tests on commercial crypto. products :
  - 2018 : Ledger Nano S
  - 2021 : Google Titan Security Key
  - 2024 : Yubico Yubikeys (+ Infineon secure elements)

Agenda

Ledger Challenge 2018

A Side Journey to Titan

EUCLEAK

Agenda

Ledger Challenge 2018

A Side Journey to Titan

EUCLEAK

Ledger Challenge 2018

- **Ledger** : French startup selling hardware crypto-currency wallets
  8M+ products sold worldwide
- Ledger Nano S based on STMicroelectronics ST31H320 + Ledger SW
  ST31H320 : secure MCU, Common Criteria and EMVCo certified
- Special Ledger Nano S sent to all participants w. **private key**
- Goal : extract 256 bits ECC **private key**
  $\Rightarrow$ become owner of Bitcoin wallet with **2.3BTC** ($\approx$15k€)

- NinjaLab participated and won 

Ledger Challenge 2018 : Details

- Target crypto. operation :
  - ECC public key generation
    $\Rightarrow$ ECC scalar multiplication over secp256k1 (Bitcoin curve)
- SCA attack :
  - Develop custom app. $\rightarrow$ knowledge of private key
  - ElectroMagnetic Side-Channel Attack setup
  - Use of SCA leakage assessment tools (SNR, T-Test) for implem. RE
  - Scalar masked w. 32 bits mask $\rightarrow$ some scalar bits no masked
  - Template Attack (supervised SCA attack)
- Outputs :
  - Coordinated responsible disclosure with stakeholders
  - 8 months embargo
  - January 2019 : cryptolib patched (firmware version 1.5.5)
  - Scientific publication at CARDIS 2019

Agenda

Ledger Challenge 2018

A Side Journey to Titan

EUCLEAK

Google Titan Security Key

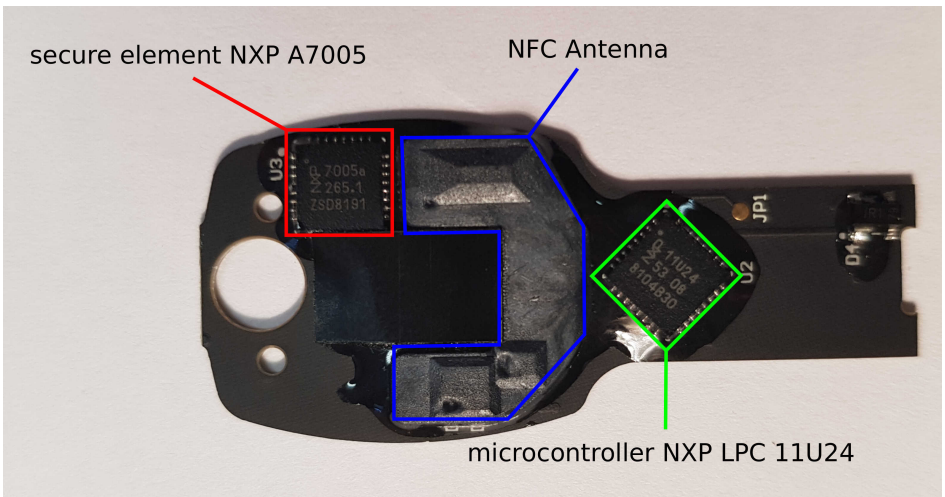
- Hardware token for **2FA** $\rightarrow$ **FIDO** protocol
  - Based on secure element NXP A7005
- Dev. of full attack allowing to **clone** Titan Key in less than 10 hours :
  - Blackbox ECDSA implem. reverse-engineered via side-channel
  - Machine learning SCA + lattice attack $\Rightarrow$ **ECDSA private key**
- Outputs :

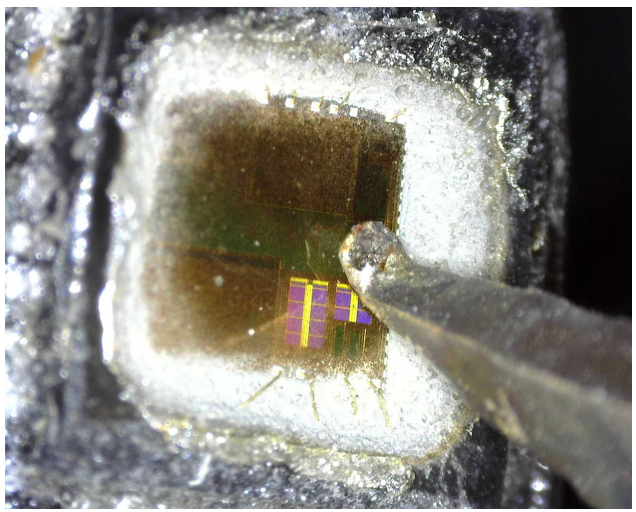
  $\Rightarrow$ Coordinated responsible disclosure with **Google** and **NXP**

  $\Rightarrow$ Scientific publication at USENIX Security Symposium 2021

Google Titan Security Key : Details (1/2)

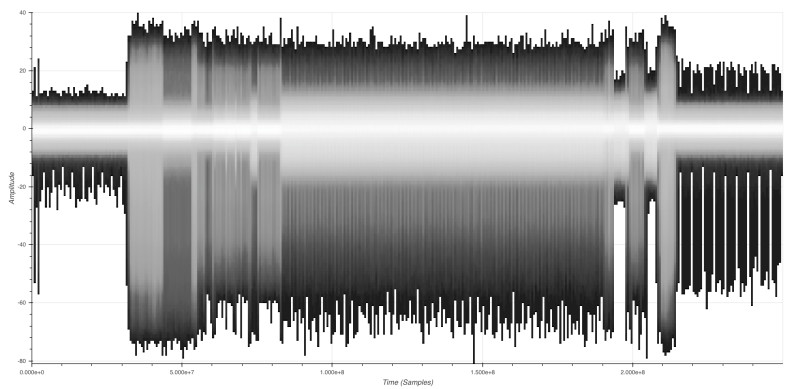
- Google Titan Security Key :
  - Hardware token for **2FA** $\rightarrow$ **FIDO** protocol
  - To be used as 2FA for your Google account
    and many other services supporting FIDO U2F protocol
  - Perform ECDSA signature over P256 for authentication
  - FIDO protocol $\rightarrow$ no way to extract ECDSA private key
    $\Rightarrow$ Full blackbox attack !





Google Titan Security Key : Details (2/2)

- SCA attack :
  - Use of NXP JavaCard w. similar crypto.lib. $\rightarrow$ knowledge of private key
  - ElectroMagnetic Side-Channel Attack setup
  - Use of SCA leakage assessment tools (SNR, T-Test) for implem. RE
  - Scalar multiplication not masked $\rightarrow$ Clustering based SCA attack
- Outputs :
  - Coordinated responsible disclosure with stakeholders
  - 3 months embargo
  - Scientific publication at USENIX Security Symposium 2021
  - CVE-2021-3011



Agenda

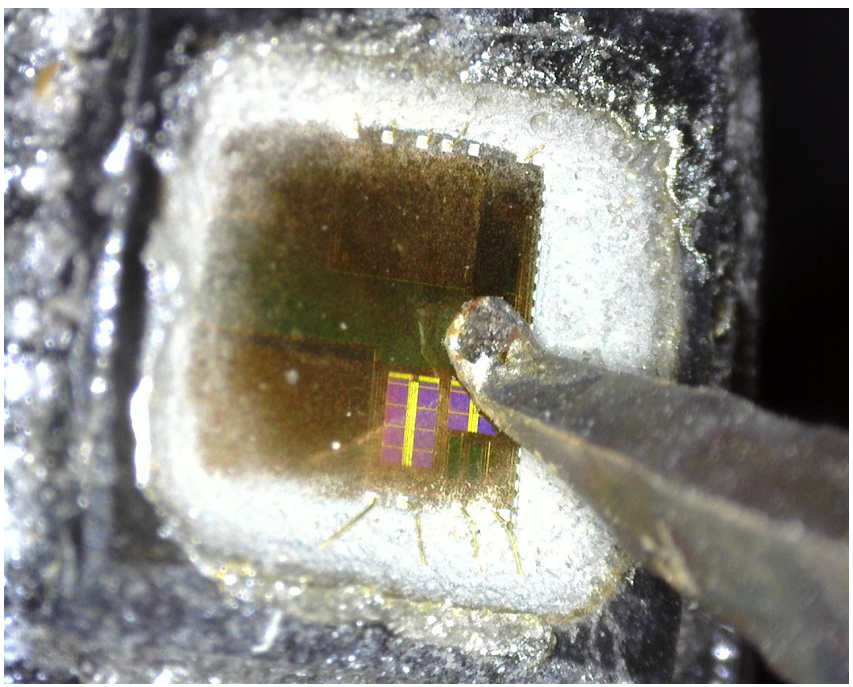
Ledger Challenge 2018

A Side Journey to Titan

EUCLEAK

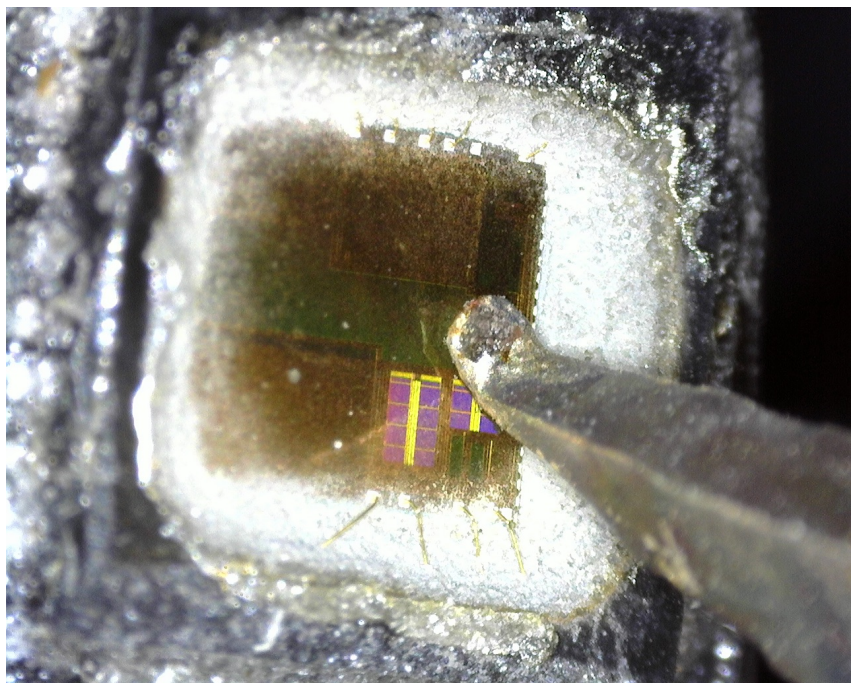
Root : A Side Journey to Titan

- January 2021 : we published **A Side Journey to Titan**



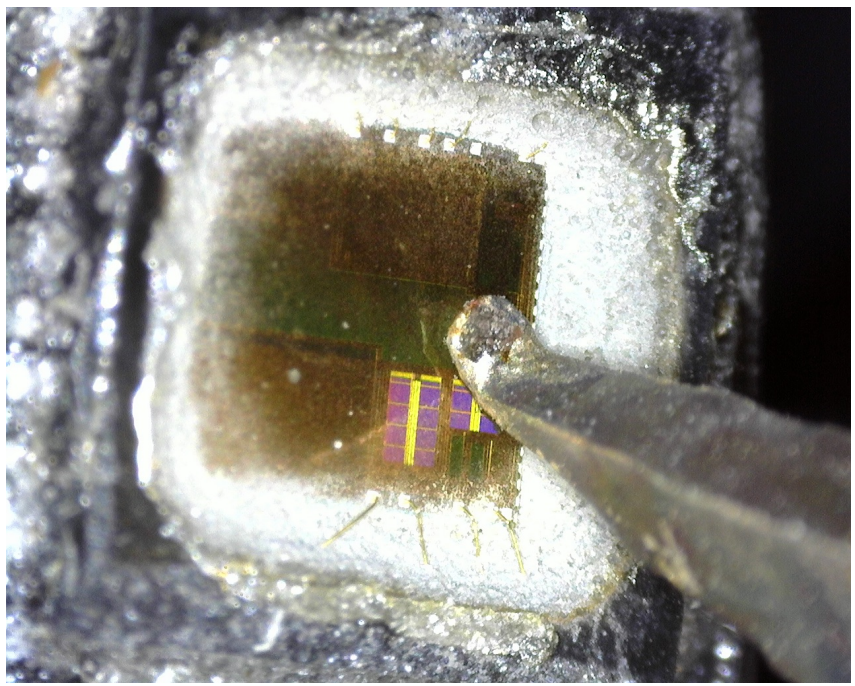
Root : A Side Journey to Titan

- January 2021 : we published **A Side Journey to Titan**
  - Side-channel vulnerability in **NXP P5x/A7x ECDSA** implementation



Root : A Side Journey to Titan

- January 2021 : we published **A Side Journey to Titan**
  - Side-channel vulnerability in **NXP P5x/A7x ECDSA** implementation
  - Attack applied on **Google Titan Security Key**
    Hardware FIDO token made by Google (HW subcontracted to Feitian)



Root : A Side Journey to Titan

- During Christmas 2020, we bought a lot (35!) of HW FIDO tokens :

Root : A Side Journey to Titan

- During Christmas 2020, we bought a lot (35!) of HW FIDO tokens :
  - Goal : check if NXP vulnerable secure element is used in other devices
    $\Rightarrow$ **Teardown** of each of the **35 FIDO devices**

Root : A Side Journey to Titan

- During Christmas 2020, we bought a lot (35!) of HW FIDO tokens :
  - Goal : check if NXP vulnerable secure element is used in other devices
    $\Rightarrow$ **Teardown** of each of the **35 FIDO devices**
  - Result : only 4 Feitian FIDO devices use a NXP A7005
    $\Rightarrow$ Throw 31 other FIDO devices ?

How to Re-Use Self-Funded Research ?

How to Re-Use Self-Funded Research ?

- Use these **FIDO devices teardowns** for a new **conference talk** !

On the Road Again ?

- Main observation : **Yubico** $\Rightarrow$ **40%** HW FIDO tokens market share !

Global FIDO Authentication Market 2024 Held the Largest Share in Upcoming Years by 2032

Research Reports World
24,610 followers

December 12, 2023

New 2023 Report on the Global "FIDO Authentication Market" | Information Technology Analysis | (110 Pages Report) -

Company Overview:

Yubico is one of the major players operating in the FIDO Authentication market, holding a share of 43.91% in 2021.

On the Road Again ?

- Main observation : **Yubico** $\Rightarrow$ **40%** HW FIDO tokens market share !
- Yubikey Series 5 secure element : **Infineon SLE78**

Global FIDO Authentication Market 2024 Held the Largest Share in Upcoming Years by 2032

Research Reports World
24,610 followers

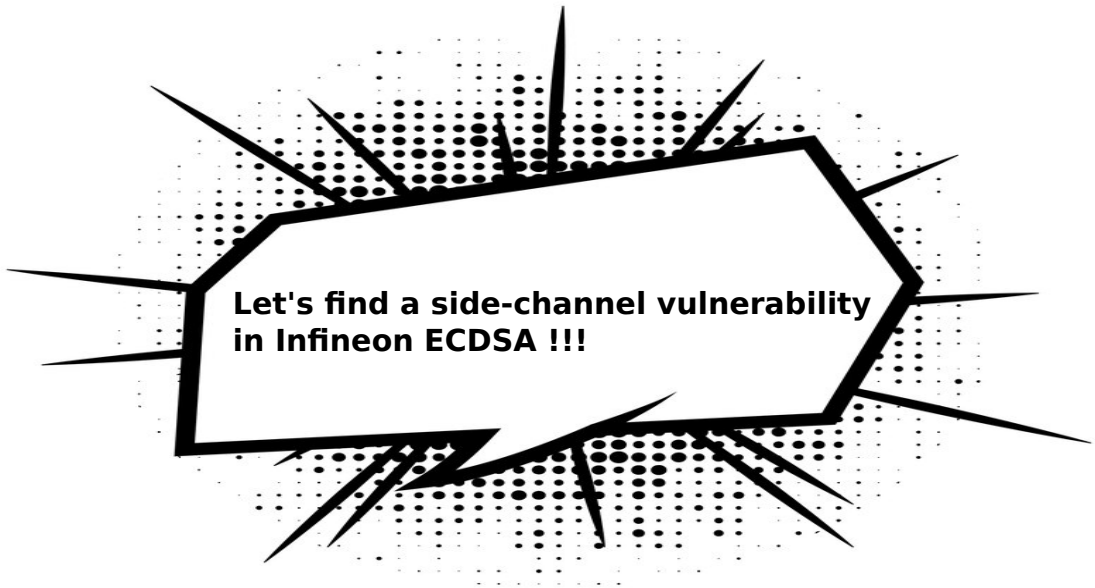
December 12, 2023

New 2023 Report on the Global "FIDO Authentication Market" | Information Technology Analysis | (110 Pages Report) -

Company Overview:

Yubico is one of the major players operating in the FIDO Authentication market, holding a share of 43.91% in 2021.

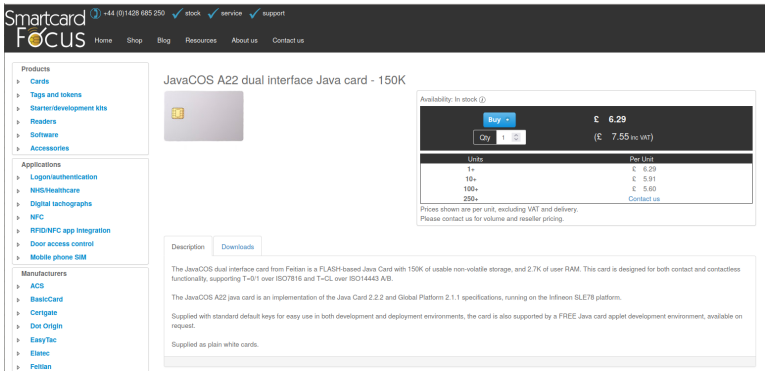
Thomas Mind



Side-Channel Hacking Tutorial

1. Find a **training device** similar to the device you want to hack

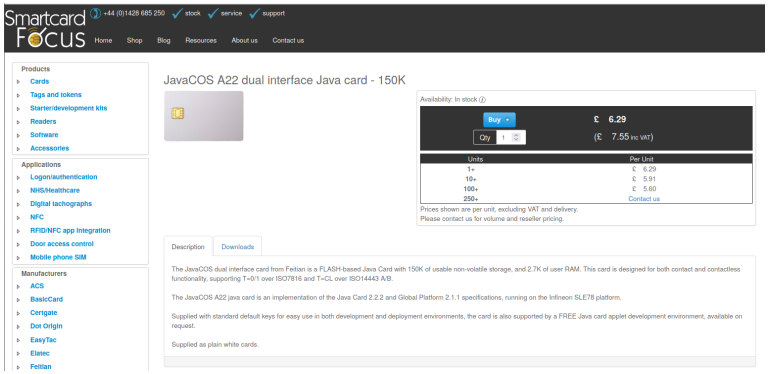
   Known key setup required !



Side-Channel Hacking Tutorial

1. Find a **training device** similar to the device you want to hack

   Known key setup required !

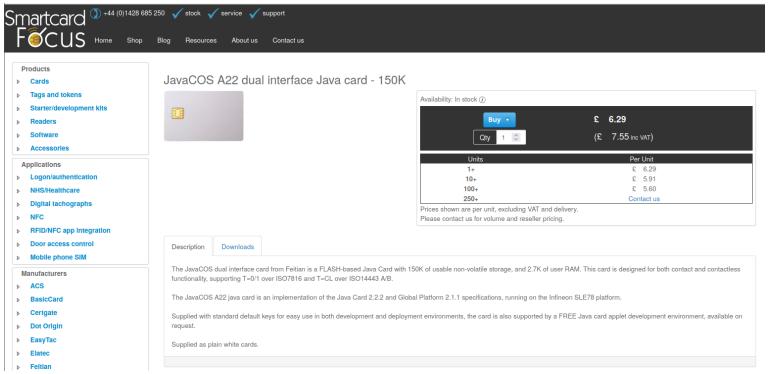


2. Give it to **Thomas**

Side-Channel Hacking Tutorial

1. Find a **training device** similar to the device you want to hack

   Known key setup required !

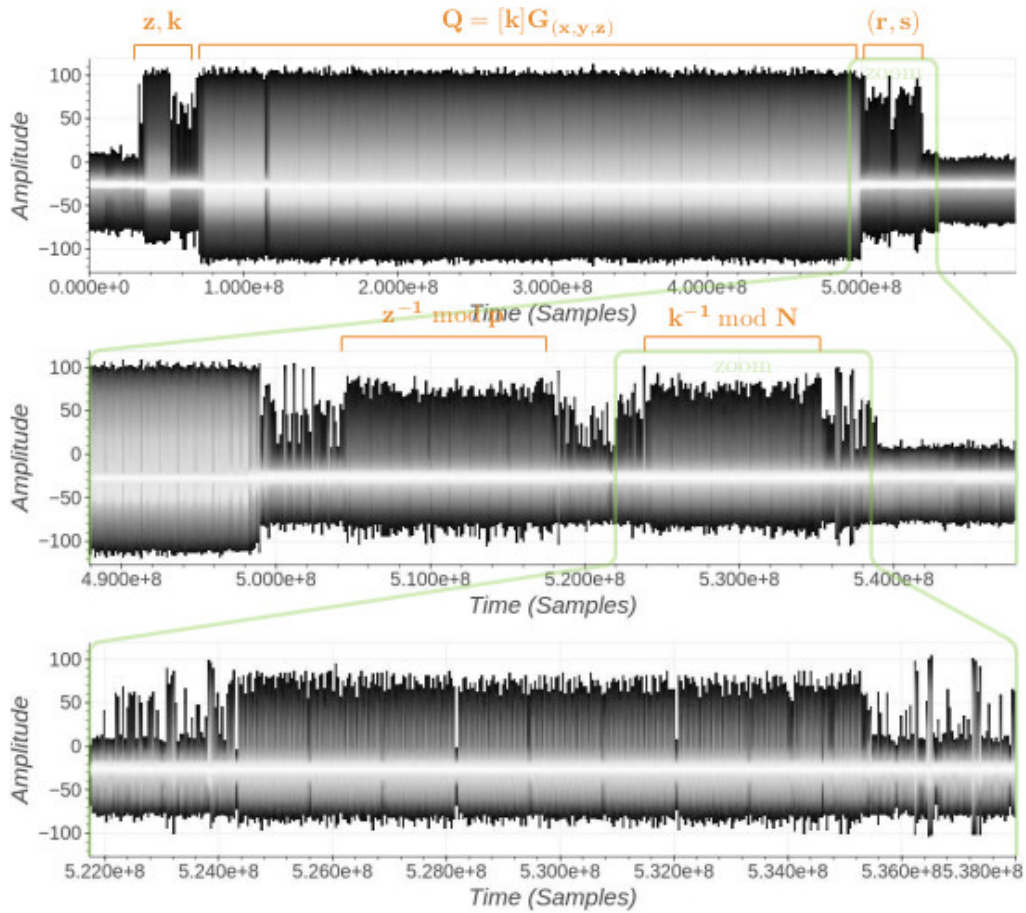


2. Give it to **Thomas**

3. Feed him with good coffee and wait for some time . . .

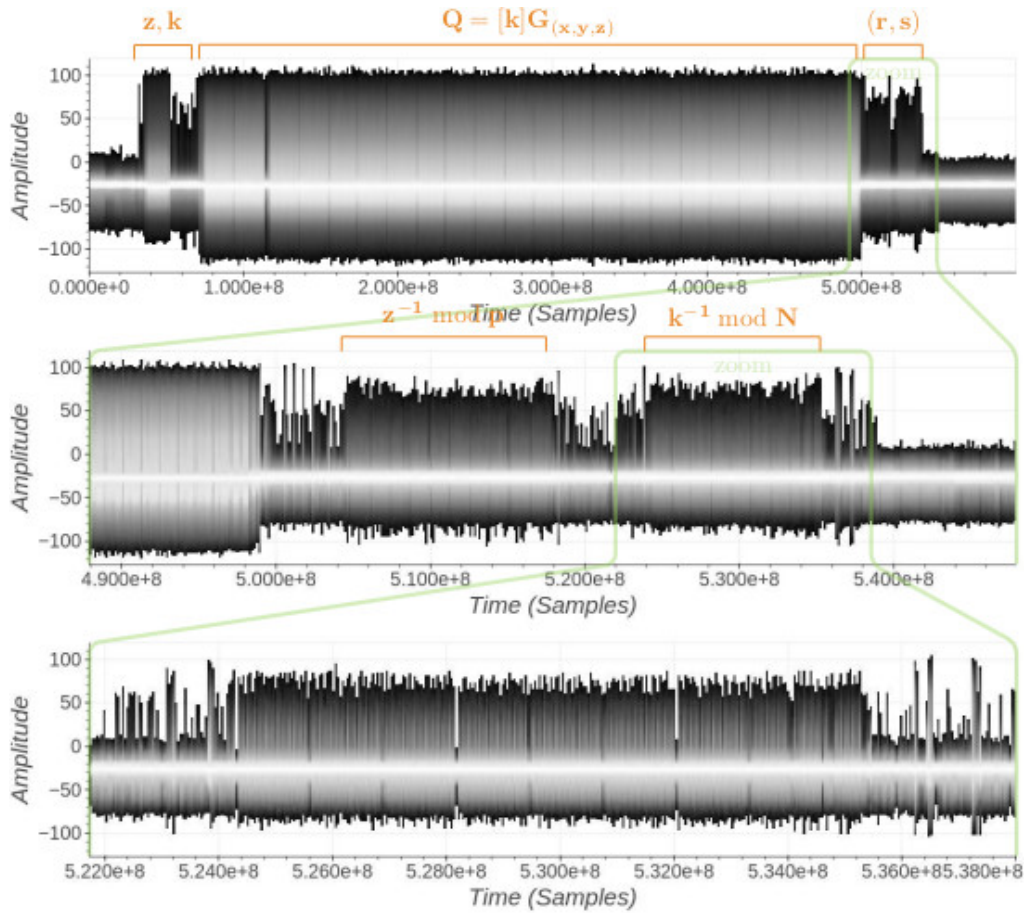
EUCLEAK : Vulnerability

- Side-channel vulnerability in **ECDSA nonce modular inversion**



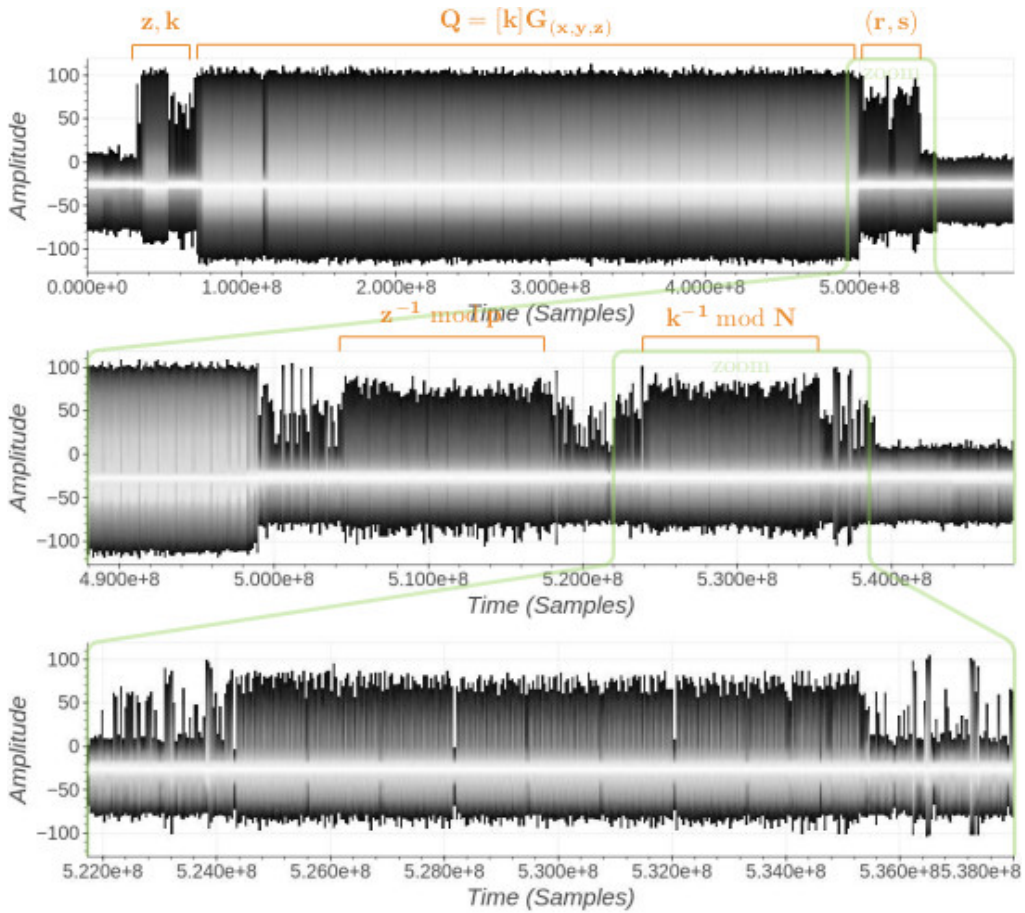
EUCLEAK : Vulnerability

- Side-channel vulnerability in **ECDSA nonce modular inversion**
- Modular inversion : **non constant time Extended Euclid Algorithm**



EUCLEAK : Vulnerability

- Side-channel vulnerability in **ECDSA nonce modular inversion**
- Modular inversion : **non constant time Extended Euclid Algorithm**
- Countermeasure : multiplicative mask of **32 bits**



EUCLEAK : Journey to an Attack

- **Side-channel reverse-engineering** of (masked) EEA

EUCLEAK : Journey to an Attack

- **Side-channel reverse-engineering** of (masked) EEA
- Understanding of timing leakages

EUCLEAK : Journey to an Attack

- **Side-channel reverse-engineering** of (masked) EEA
- Understanding of timing leakages
- Design of a **side-channel attack algorithm**

Algorithm 2: A Generic Attack Algorithm

Input : $\{m_{start}, m_{next}\}$: a pair of brute-force parameters,
Input : $\{\mathcal{L}_i\}_{0 \leq i < n}$: the leaked information from the execution of $\texttt{EEA}(k', N)$
Input : $f(.)$: the leakage function
Output: c: a candidate for k or Error if none found

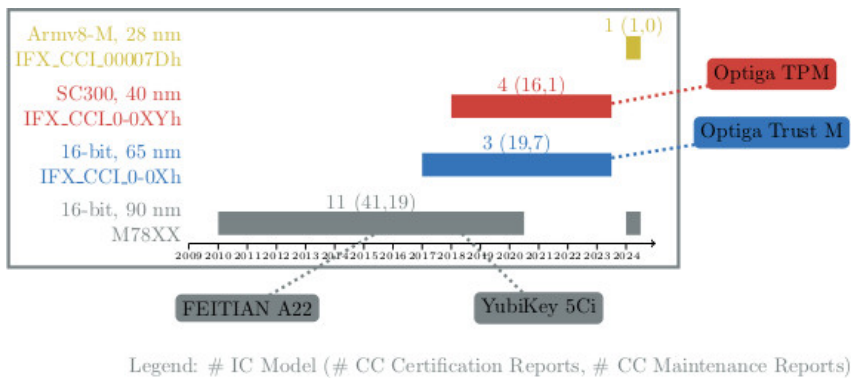
$L \leftarrow \{(0, 0, -1)\}$
while *True* **do**
  $(c, t, q) \leftarrow L.pop()$ // pop the first element of the list L
  if $t = len(N)$ **then** // $len(x)$ returns the binary length of x
    return c
  else if $t = 0$ **then**
    $s, m \leftarrow 1, m_{start}$
  else
    $s, m \leftarrow 0, min(m_{next}, len(N) - t)$
  end
  $N_{t+m} \leftarrow msb_{t+m}(N)$ // $t+m$ msb of N
  for $x \in [start, 2^m]$ **do**
    $v \leftarrow c.2^m + x$
    $success, \hat{q} \leftarrow \texttt{TEEA}(v, N_{t+m}, \{\mathcal{L}_i\}_{0 \leq i < n}, f)$ // call to Algorithm 3
    if *success* **then**
      Add tuple $(v, t + m, \hat{q})$ to L such that L stays sorted *w.r.t.* last element of the tuple $(\hat{q})$.
    end
  end
end
return Error

EUCLEAK : Impact

- All **Yubikey 5 Series** (up to firmware 5.7) impacted !

EUCLEAK : Impact

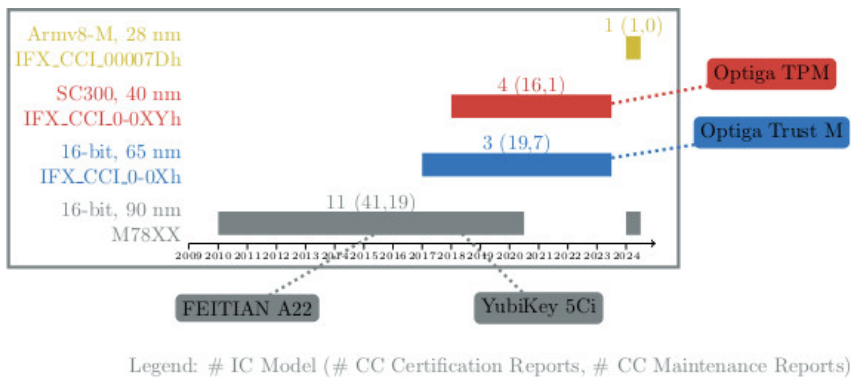
- All **Yubikey 5 Series** (up to firmware 5.7) impacted !
- All **Infineon secure elements since 14 years** impacted !



Legend: # IC Model (# CC Certification Reports, # CC Maintenance Reports)

EUCLEAK : Impact

- All **Yubikey 5 Series** (up to firmware 5.7) impacted !
- All **Infineon secure elements since 14 years** impacted !
- CVE-2024-45678



EUCLEAK : Patches

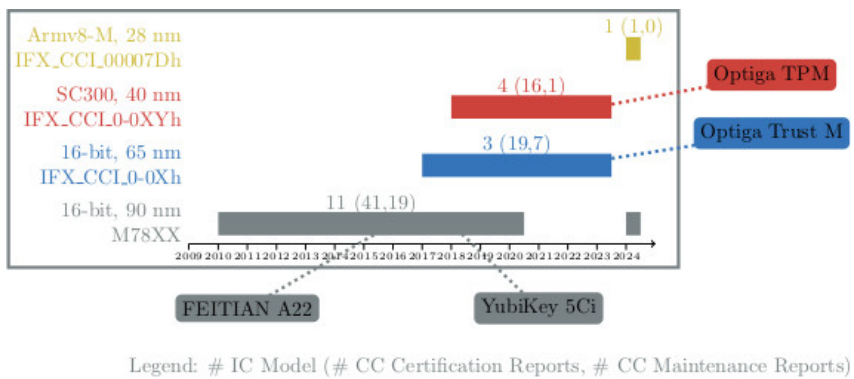
- Coordinated responsible disclosure of 4.5 months

EUCLEAK : Patches

- Coordinated responsible disclosure of 4.5 months
- Yubikey 5 Series :
  - Release of their own cryptolib (from firmware 5.7)
  - Security advisory pyblished by Yubico

EUCLEAK : Patches

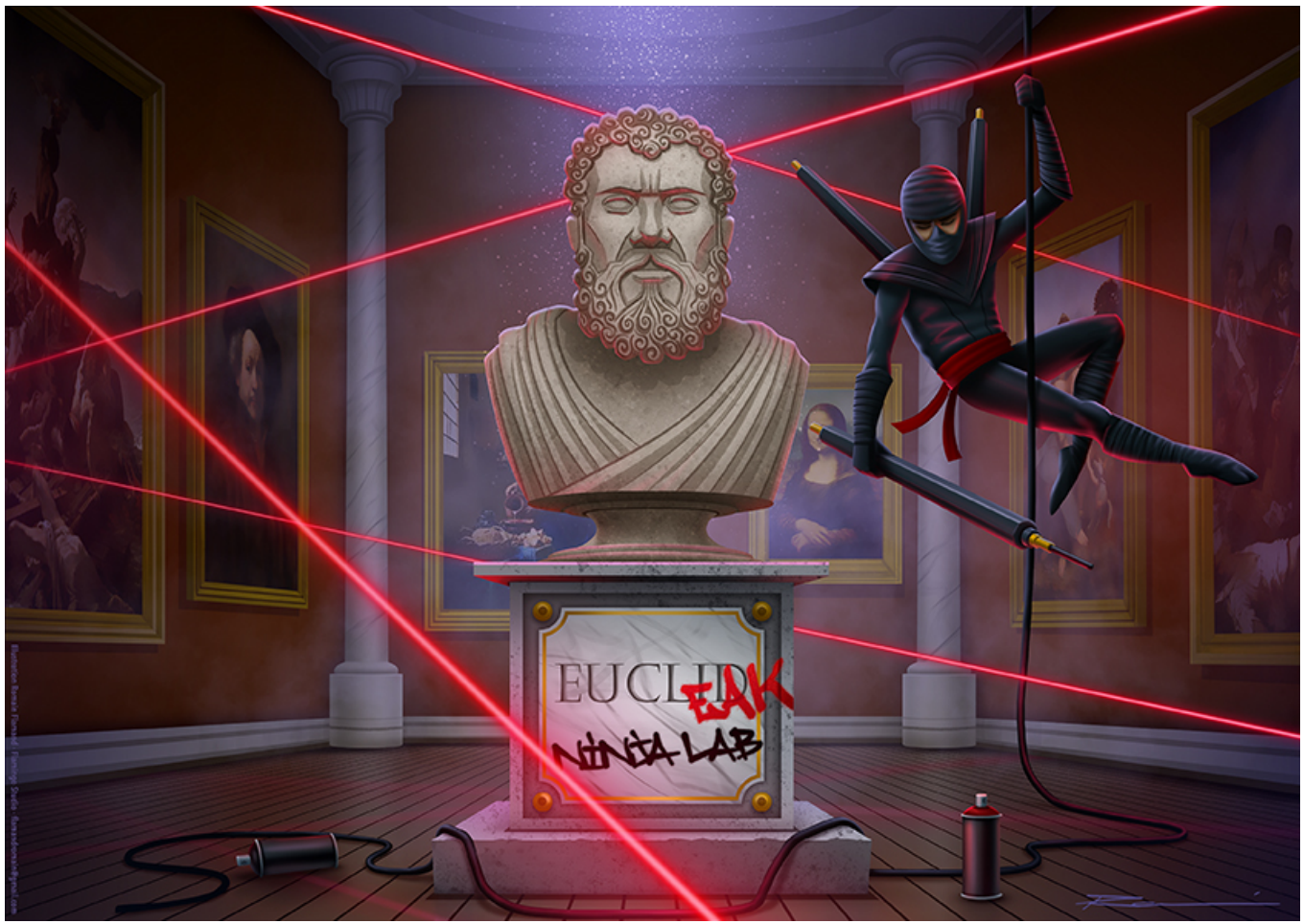
- Coordinated responsible disclosure of 4.5 months
- Yubikey 5 Series :
  - Release of their own cryptolib (from firmware 5.7)
  - Security advisory pyblished by Yubico
- Infineon secure elements :
  - Cryptolib patched by Infineon but no public statement
  - Re-certification of chips (80 certifications over 14 years impacted !)



Legend: # IC Model (# CC Certification Reports, # CC Maintenance Reports)

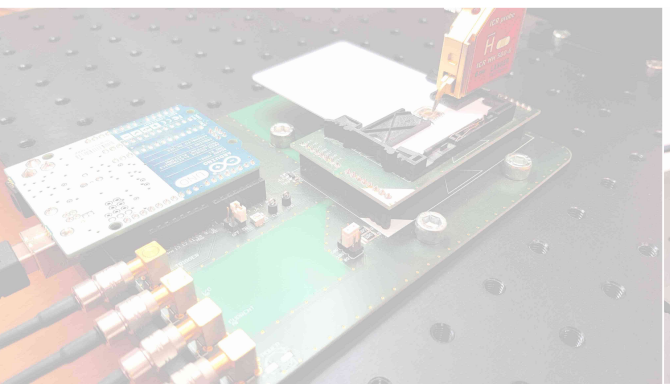
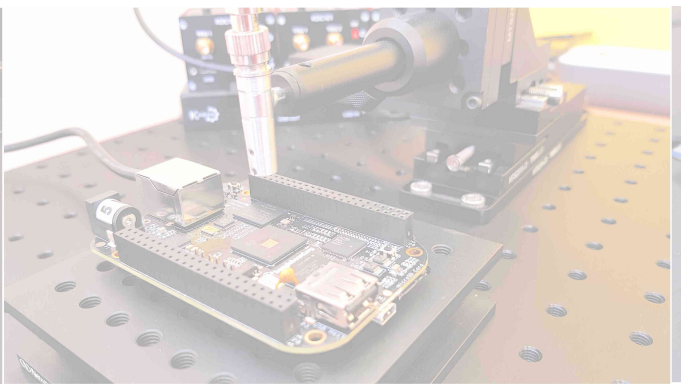
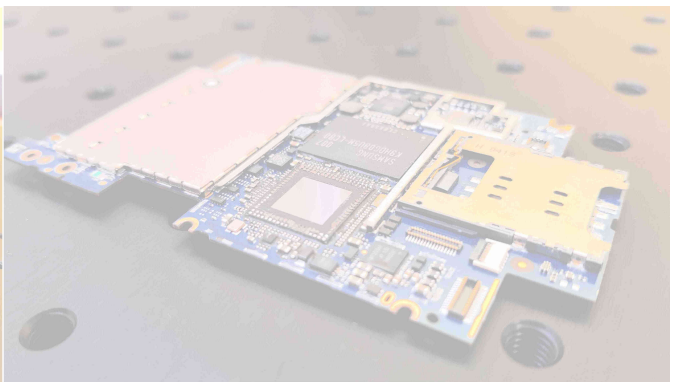
EUCLEAK : More Reading !

- Dedicated webpage on **NinjaLab website**
- Technical **write-up** by **Thomas** (88 pages !)
- Scientific publication at IEEE S&P 2025



NinjaLab

Improve the Security of your Cryptographic Implementation

https://ninjalab.io
contact@ninjalab.io

NinjaLab
12 rue Boussairolles
34000 MONTPELLIER
FRANCE