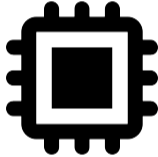




Thomas Roche  
NinjaLab

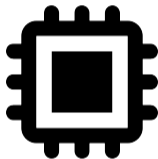
C&ESAR  
Rennes, FR – Nov. 20th, 2024

# Secure Elements



## Secure Elements

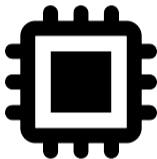
Generate/Store Keys  
Key Exch./Wrap.  
Signatures



## Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures

Remote Attacker

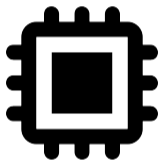


## Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



Remote Attacker



Simple HW  
Simple SW  
Simple I/O  
Formal Methods

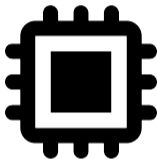
Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



Remote Attacker

$\varphi$  Attacker



Simple HW  
Simple SW  
Simple I/O  
Formal Methods

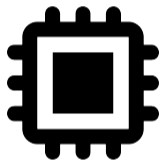
## Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



Remote Attacker

$\varphi$  Attacker



Side-Channel  
Fault Injection  
Invasive

Simple HW  
Simple SW  
Simple I/O  
Formal Methods

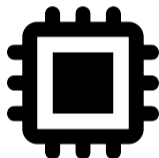
## Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



Remote Attacker

$\varphi$  Attacker



Side-Channel  
Fault Injection  
Invasive

Simple HW  
Simple SW  
Simple I/O  
Formal Methods  
HW CMs  
SW/Crypto CMs



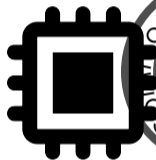
## Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



Remote Attacker

$\varphi$  Attacker



Side-Channel  
Fault Injection  
Invasive

Simple HW  
Simple SW  
Simple I/O  
Formal Methods  
HW CMs  
SW/Crypto CMs

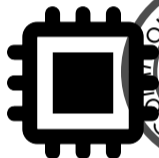
# Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



Remote Attacker

$\varphi$  Attacker



Side-Channel  
Fault Injection  
Invasive

Simple HW  
Simple SW  
Simple I/O

Formal Methods

HW CMs

SW/Crypto CMs

# Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures

Remote Attacker



$\varphi$  Attacker

Side-Channel  
Fault Injection  
Invasive

Simple SW  
Simple I/O  
Formal Methods

HW CMs  
SW/Crypto CMs

## Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



NXP

infineon

ST

SAMSUNG



- Sovereign Documents
- Access Control
- Bank Cards

Remote Attacker

$\varphi$  Attacker

Side-Channel  
Fault Injection  
Invasive

Simple SW  
Simple I/O  
Formal Methods  
HW CMs  
SW/Crypto CMs

## Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



NXP

infineon

ST

SAMSUNG



Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

$\varphi$  Attacker

- Bitcoin HW Wallets
- 2FA HW Tokens

Side-Channel  
Fault Injection  
Invasive

Simple SW  
Simple I/O  
Formal Methods  
HW CMs  
SW/Crypto CMs

## Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



NXP

infineon

ST

SAMSUNG



Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

$\varphi$  Attacker

- Bitcoin HW Wallets
- 2FA HW Tokens

Side-Channel  
Fault Injection  
Invasive

- SmartPhones
- Computers (TPMs)

Simple SW  
Simple I/O  
Formal Methods  
HW CMs  
SW/Crypto CMs

# Secure Elements

Generate/Store Keys  
Key Exch./Wrap.  
Signatures



Remote Attacker

$\varphi$  Attacker

Side-Channel  
Fault Injection  
Invasive

Simple SW  
Simple I/O  
Formal Methods  
HW CMs  
SW/Crypto CMs

- Sovereign Documents
- Access Control
- Bank Cards

- Bitcoin HW Wallets
- 2FA HW Tokens

- SmartPhones
- Computers (TPMs)

- Smart Cars
- Smart Homes

...

Generate/Store Keys  
Key Exch./Wrap.

Signatures



Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

NXP

infineon

ST

SAMSUNG



$\varphi$  Attacker

- Bitcoin HW Wallets
- 2FA HW Tokens

Side-Channel

Fault Injection

Invasive

Simple SW

Simple I/O

Formal Methods

HW CMs

SW/Crypto CMs

- SmartPhones
- Computers (TPMs)

- Smart Cars
- Smart Homes

...



# Agenda

## Introduction

- FIDO Hardware Tokens

- Infineon SLE 78

- FEITIAN A22 Open JavaCard

- Infineon ECDSA Observations

- The Extended Euclidean Algorithm

## A Side-Channel Vulnerability in EEA

- ECDSA Signature Verification

- Infineon ECDSA Signature Verification

- First Observations

- Summary

- A Masked Modular Inversion

## Full Reverse-Engineering of Infineon EEA

- Heuristical Approaches

- Summary of The Sensitive Leakage

## Yubikey 5C

- Aquisition Setup

- First Side-Channel Traces

- Attack in Practice

## Impact Analysis

- Infineon Security Microcontrollers

- Optiga Trust M

- Optiga TPM

## Conclusions

- Conclusions

- Mitigations

- Project Timeline

- Project Timeline

# Agenda

## Introduction

FIDO Hardware Tokens

Infineon SLE 78

FEITIAN A22 Open JavaCard

Infineon ECDSA Observations

The Extended Euclidean Algorithm

## A Side-Channel Vulnerability in EEA

ECDSA Signature Verification

Infineon ECDSA Signature Verification

First Observations

Summary

A Masked Modular Inversion

## Full Reverse-Engineering of Infineon EEA

Heuristical Approaches

Summary of The Sensitive Leakage



# FIDO Hardware Tokens



credits Yubico

- ▶ (2nd) Authentication Factor
- ▶ FIDO core crypto primitive is ECDSA:

*Elliptic Curve Digital Signature Algorithm*

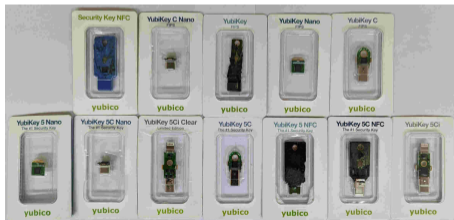
- ▶ Generate ECDSA key-pairs
  - ▶ ECDSA Sign challenges
- 
- ▶ Protect the ECDSA private keys
- ↔ *Secure Element*

# A Side Journey To Titan

- ▶ In 2021 NinjaLab published *A Side Journey to Titan* (Usenix Security'21)  
SCA vulnerability in NXP'P5x security MCU ECC cryptolib.
  - ↔ Side-Channel Key-Recovery Attack on ECDSA
  - ↔ Clone FIDO token *Google Titan Security Key*
- ▶ NXP'P5x security microcontrollers are already old devices (last CC certification in 2015)
  - ↔ Most common security microcontrollers in FIDO Tokens are Infineon SLE78.

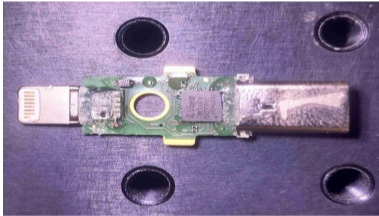
# A Side Journey To Titan

- ▶ In 2021 NinjaLab published *A Side Journey to Titan* (Usenix Security'21)  
SCA vulnerability in NXP'P5x security MCU ECC cryptolib.
  - ↪ Side-Channel Key-Recovery Attack on ECDSA
  - ↪ Clone FIDO token *Google Titan Security Key*
- ▶ NXP'P5x security microcontrollers are already old devices (last CC certification in 2015)
  - ↪ Most common security microcontrollers in FIDO Tokens are Infineon SLE78.

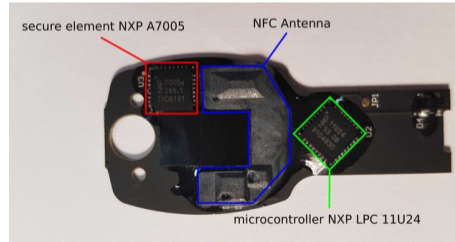


# Infineon SLE 78

The **SLE 78 USB** is a cache-based pure **16-bit security controller** family designed to meet all secure USB token design requirements. Its outstanding digital security concept Integrity Guard offers comprehensive error detection, a self-checking dual CPU and a fully encrypted data path including encrypted calculation in the CPU. It enables certification levels up to **Common Criteria EAL6+ (high) and EMVCo.**<sup>1</sup>



Yubikey 5Ci (SLE 78)



Google Titan Key (NXP A7005)

<sup>1</sup><https://www.infineon.com/cms/en/product/security-smart-card-solutions/security-controllers-for-usb-tokens/sle-78clufx5000ph/>

# FEITIAN A22 Open JavaCard

The screenshot shows the SmartCard Focus website. The main content area displays the product "JavaCOS A22 dual interface Java card - 150K". To the left is a navigation menu with categories like Products, Applications, and Manufacturers. To the right is a product detail box with a "Buy" button, a quantity selector, and a price table. Below the price table is a description of the card's features and specifications.

Smartcard Focus +44 (0)1429 629 250 ✓ stock ✓ service ✓ support

Home Shop Blog Resources About us Contact us

Products

- Cards
- Tags and tokens
- Starters/development kits
- Readers
- Software
- Accessories

Applications

- Logins/authentication
- NHS/Healthcare
- Digital tachographs
- NFC
- RFID/NFC app integration
- Door access control
- Mobile phone SIM

Manufacturers

- ACS
- BasicCard
- Cergate
- Dot Origin
- EasyTac
- Elatec
- Feitian

JavaCOS A22 dual interface Java card - 150K

Availability: In stock (0)

Buy £ 6.29  
Qty 1 (€ 7.55 inc VAT)

Units	Per Unit
T+	£ 6.29
T0+	£ 5.31
100+	£ 5.00
250+	Contact us

Prices shown are per unit, excluding VAT and delivery.  
Please contact us for volume and reseller pricing.

Descriptions Downloads

The JavaCOS dual interface card from Feitian is a FLASH-based Java Card with 150K of usable non-volatile storage, and 2.7K of user RAM. This card is designed for both contact and contactless functionality, supporting T-01 over ISO7816 and T-CL over ISO14443 A/B.

The JavaCOS A22 Java card is an implementation of the Java Card 2.2.2 and Global Platform 2.1.1 specifications, running on the Infineon SLE78 platform.

Supplied with standard default keys for easy use in both development and deployment environments, the card is also supported by a FREE Java card applet development environment, available on request.

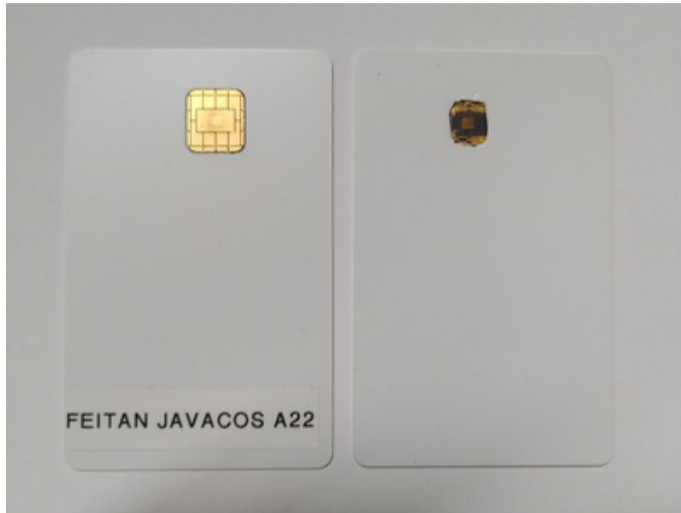
Supplied as plain white cards.

Figure: FEITIAN A22 – Screenshot from SmartCard Focus

- ▶ Develop and push our own JavaCard applet  
↳ ECDSA Signature & Verification
- ▶ certified EAL5+ under Common Criteria in 2018<sup>2</sup>
- ▶ Infineon asymmetric crypto lib version 1.02.013

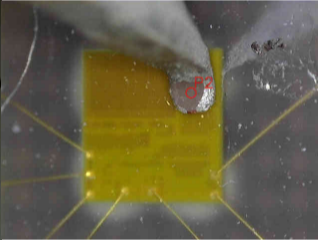
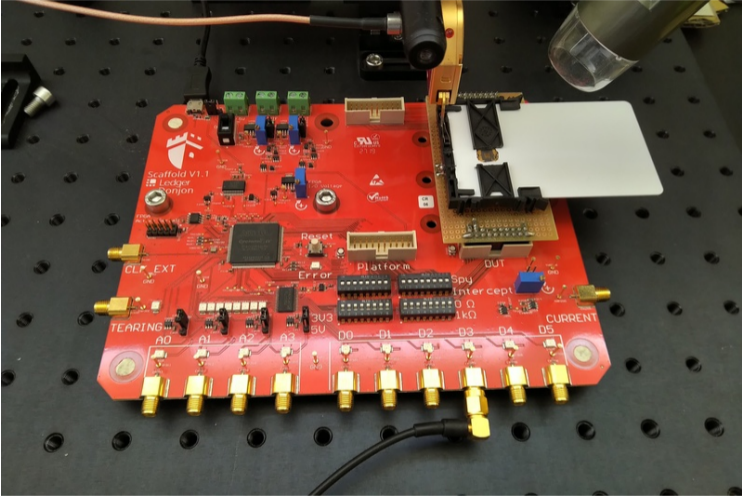
<sup>2</sup><https://www.commoncriteriaportal.org/files/epfiles/SERTIT-091CRFeitianv1.0.pdf>

# FEITIAN A22 Open JavaCard

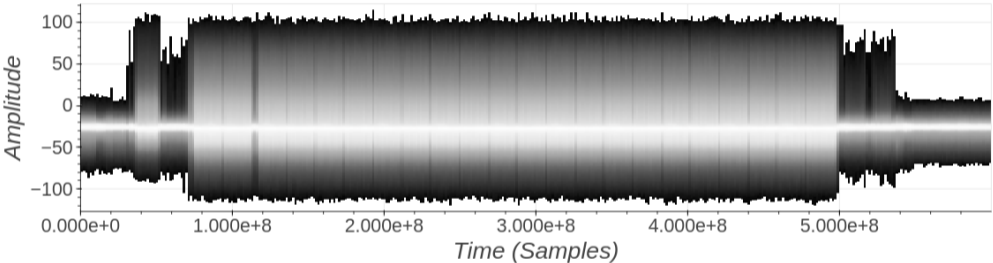




# FEITIAN A22 – EM Acquisitions



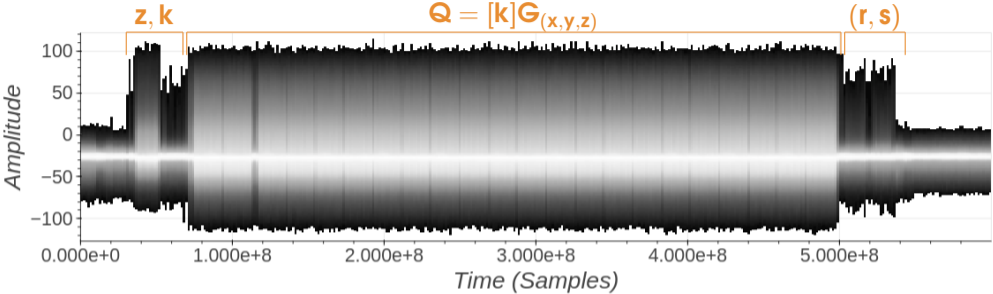
# FEITIAN A22 – ECDSA Command – EM Radiations



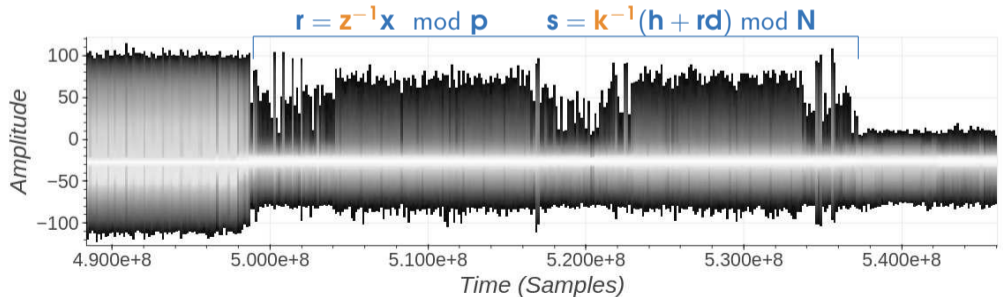
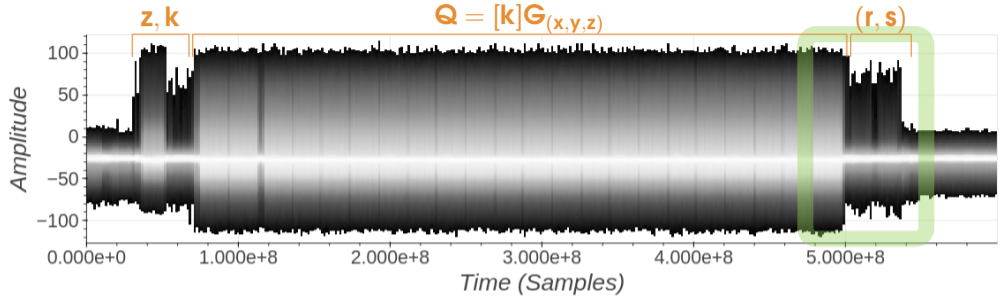
# ECDSA Signature Scheme

- ▶ Elliptic Curve  $E$  over  $\mathbb{F}_p$  (base point  $G_{(x,y)}$ , order is  $N$ )
- ▶ Inputs: **secret key**  $d$ , the input message to sign  $h = H(m)$
- ▶ randomly **generate a nonce**  $k$  in  $\mathbb{Z}/N\mathbb{Z}$
- ▶ randomly **generate a random**  $z$  in  $\mathbb{Z}/p\mathbb{Z}$
- ▶ random projection  $G_{(x,y)} \rightarrow G_{(xz,yz,z)}$
- ▶ compute  $Q_{(x,y,z)} = [k]G_{(x,y,z)}$
- ▶ inv projection  $Q_{(x,y,z)} \rightarrow Q_{(xz^{-1},yz^{-1})}$
- ▶ denote by  $r$  the  $x$ -coordinate of  $Q$ :  $r = Q_x$
- ▶ compute  $s = k^{-1}(h + rd) \bmod N$
- ▶ return  $(r, s)$

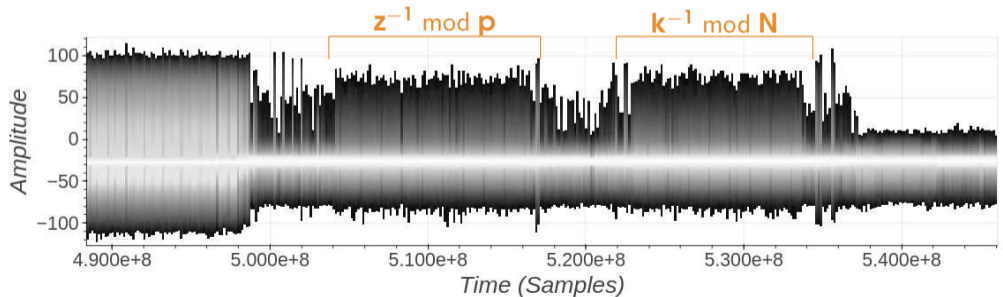
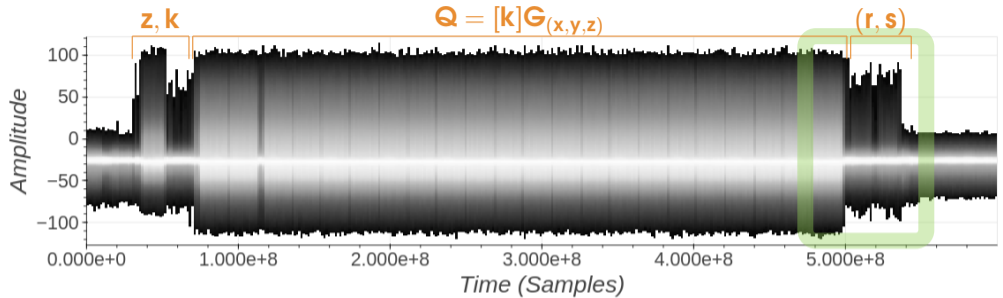
# FEITIAN A22 – ECDSA Command – EM Radiations



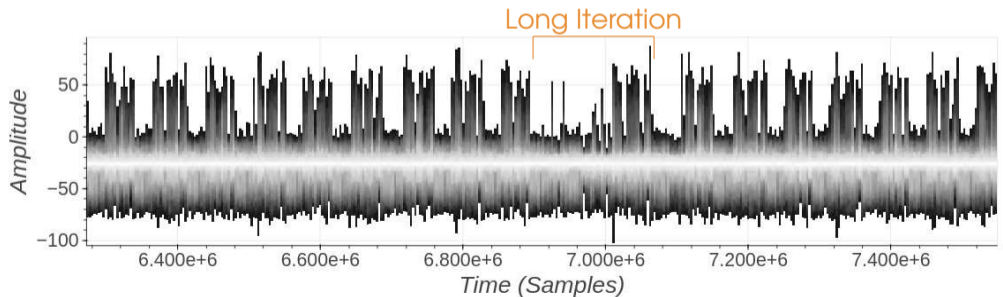
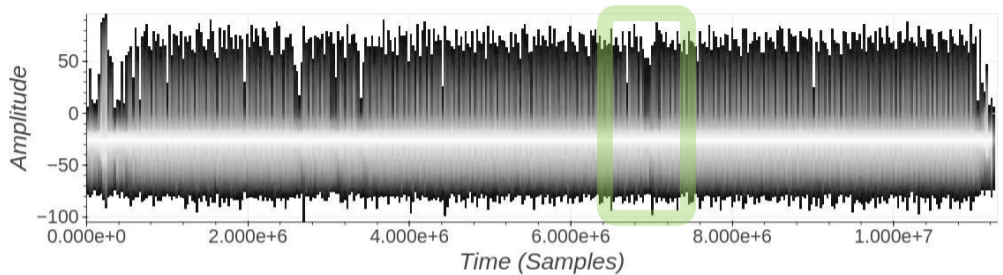
# FEITIAN A22 – ECDSA Command – EM Radiations



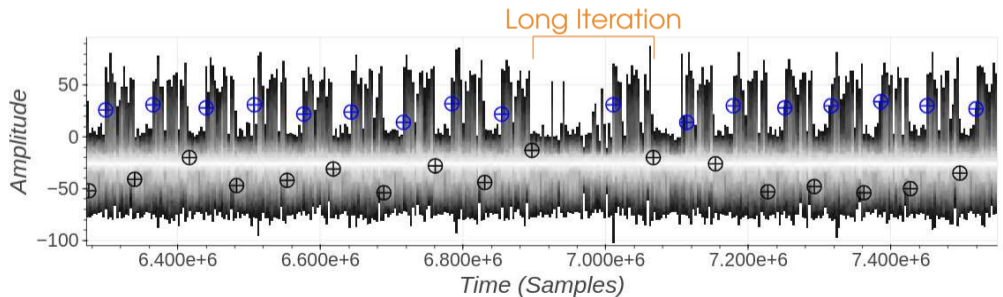
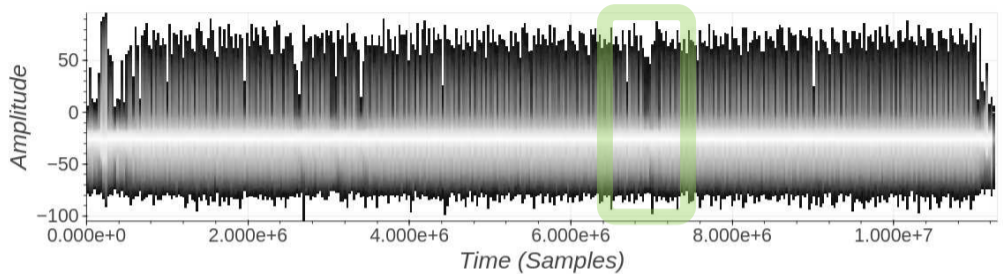
# FEITIAN A22 – ECDSA Command – EM Radiations



# FEITIAN A22 – $k^{-1} \bmod N$ – EM Radiations

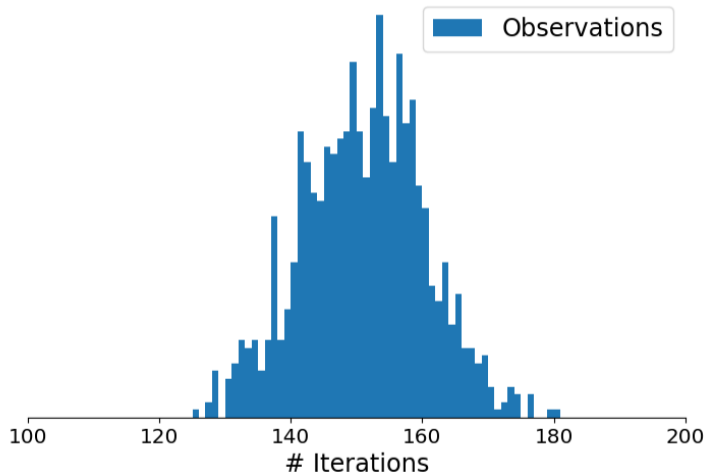


# FEITIAN A22 – $k^{-1} \bmod N$ – EM Radiations

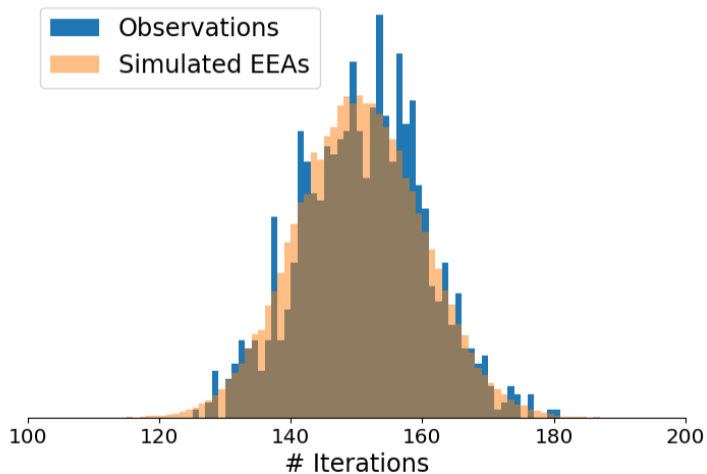




# FEITIAN A22 – $k^{-1} \bmod N$ – Iterations Count Distribution



# FEITIAN A22 – $k^{-1} \bmod N$ – Iterations Count Distribution



# Extended Euclidean Algorithm

---

**Input** :  $v, n$ : two positive integers with  $v \leq n$  and  $\gcd(v, n) = 1$

**Output**:  $v^{-1} \bmod n$ : the inverse of  $v$  modulo  $n$

```
1  $r_0, r_1 \leftarrow n, v$ 
2  $t_0, t_1 \leftarrow 0, 1$ 
3 while  $r_1 \neq 0$  do
4    $q \leftarrow \text{div}(r_0, r_1)$ 
5    $r_0, r_1 \leftarrow r_1, r_0 - q \cdot r_1$ 
6    $t_0, t_1 \leftarrow t_1, t_0 - q \cdot t_1$ 
7 if  $t_0 < 0$  then
8    $t_0 \leftarrow t_0 + n$ 
Return :  $t_0$ 
```

# Extended Euclidean Algorithm

---

**Input** :  $v, n$ : two positive integers with  $v \leq n$  and  $\gcd(v, n) = 1$

**Output**:  $v^{-1} \bmod n$ : the inverse of  $v$  modulo  $n$

1  $r_0, r_1 \leftarrow n, v$

2  $t_0, t_1 \leftarrow 0, 1$

3 **while**  $r_1 \neq 0$  **do**

4      $q \leftarrow \text{div}(r_0, r_1)$

5      $r_0, r_1 \leftarrow r_1, r_0 - q \cdot r_1$

6      $t_0, t_1 \leftarrow t_1, t_0 - q \cdot t_1$

7 **if**  $t_0 < 0$  **then**

8      $t_0 \leftarrow t_0 + n$

**Return** :  $t_0$

---

# Iterations does not match with  $k^{-1} \bmod N$

$\hookrightarrow$   $k$  might be masked

# Agenda

## Introduction

FIDO Hardware Tokens

Infineon SLE 78

FEITIAN A22 Open JavaCard

Infineon ECDSA Observations

The Extended Euclidean Algorithm

## A Side-Channel Vulnerability in EEA

ECDSA Signature Verification

Infineon ECDSA Signature Verification

First Observations

Summary

A Masked Modular Inversion

## Full Reverse-Engineering of Infineon EEA

Heuristical Approaches

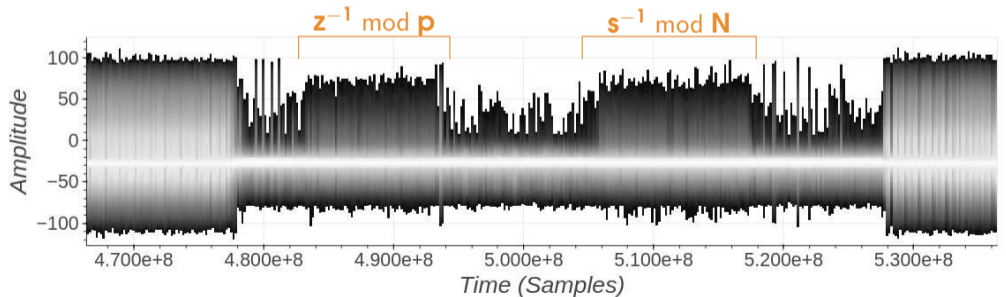
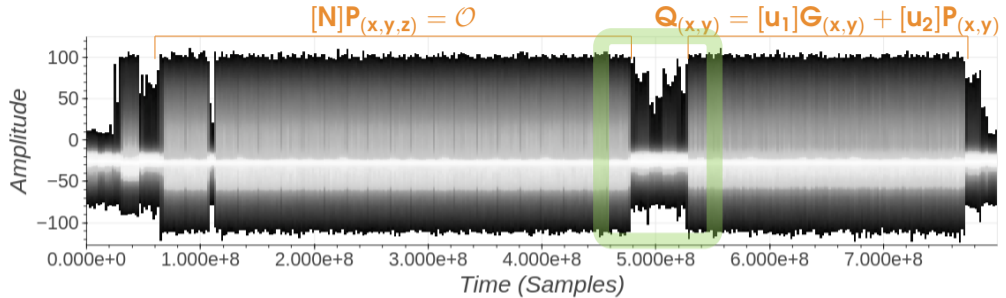
Summary of The Sensitive Leakage



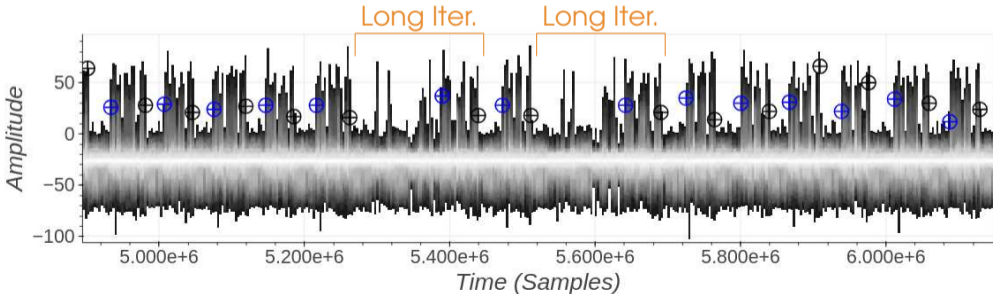
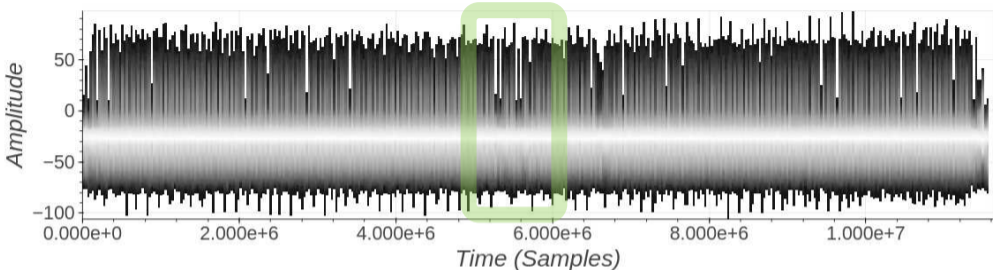
# ECDSA Signature Verification Scheme

- ▶ Elliptic Curve base point is  $G_{(x,y)}$ , Elliptic Curve order is  $N$
- ▶ Inputs: public key  $P_{(x,y)}$ , the input message  $h = H(m)$ , the signature  $(r, s)$
- ▶ check that  $P \neq \mathcal{O}$
- ▶ check that  $P \in E$
- ▶ check that  $[N]P = \mathcal{O}$
- ▶ Let  $u_1 = hs^{-1} \bmod N$ ,  $u_2 = rs^{-1} \bmod N$
- ▶ compute  $Q_{(x,y)} = [u_1]G_{(x,y)} + [u_2]P_{(x,y)}$
- ▶ return True iff  $r = Q_x \bmod N$

# FEITIAN A22 – ECDSA Verif Command – EM Radiations

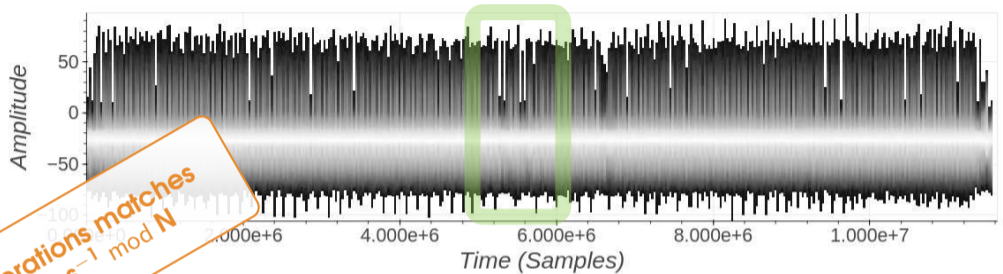


# FEITIAN A22 – $s^{-1} \bmod N$ – EM Radiations

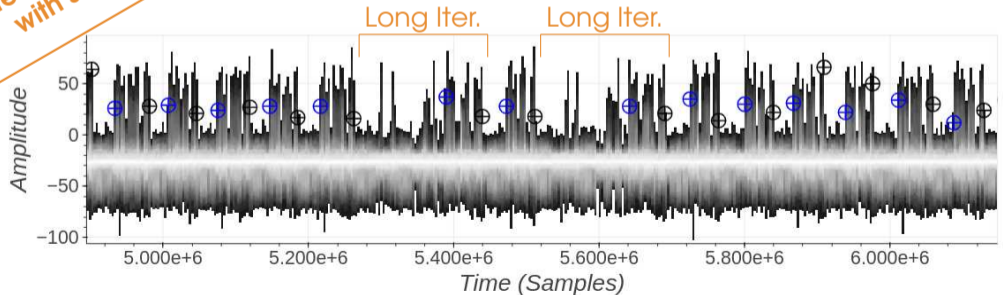




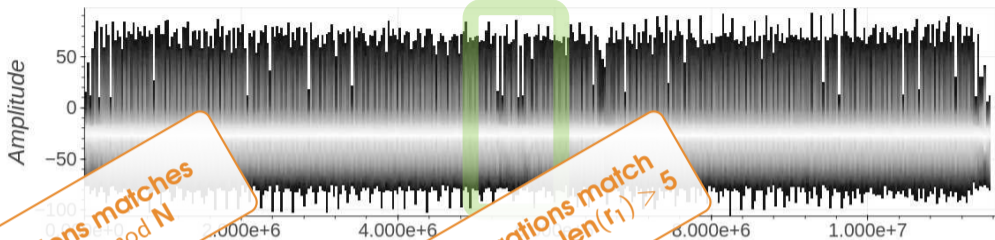
# FEITIAN A22 – $s^{-1} \bmod N$ – EM Radiations



# Iterations matches with  $s^{-1} \bmod N$

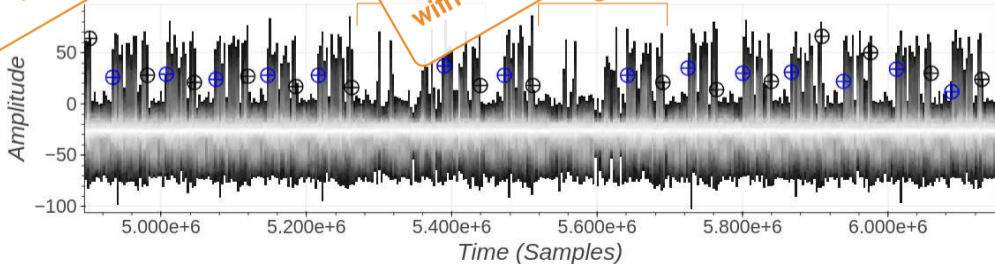


# FEITIAN A22 – $s^{-1} \bmod N$ – EM Radiations

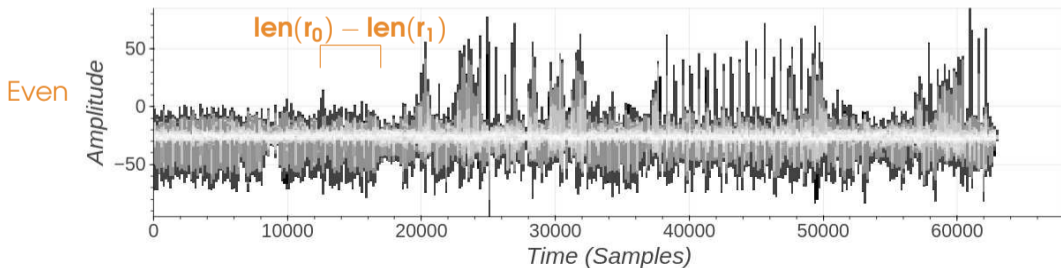
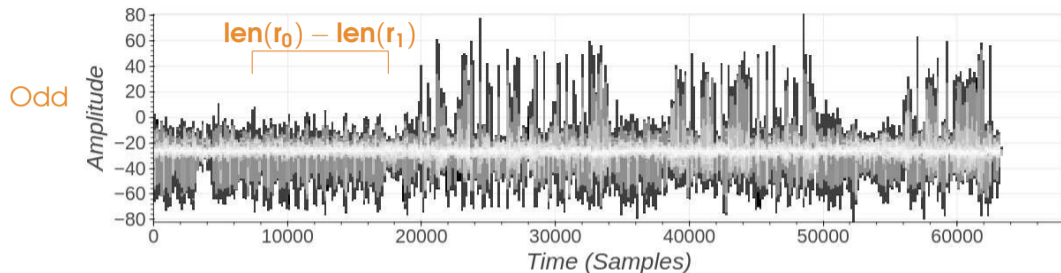


# Iterations matches with  $s^{-1} \bmod N$

Long Iterations match with  $\text{len}(r_0) - \text{len}(r_1) > 5$



# FEITIAN A22 – $s^{-1} \bmod N$ – Single Iteration



# Extended Euclidean Algorithm – Summary

---

**Input** :  $v, n$ : two positive integers with  $v \leq n$  and  $\gcd(v, n) = 1$

**Output**:  $v^{-1} \bmod n$ : the inverse of  $v$  modulo  $n$

```
1  $r_0, r_1 \leftarrow n, v$ 
2  $t_0, t_1 \leftarrow 0, 1$ 
3 while  $r_1 \neq 0$  do
4    $q \leftarrow \text{div}(r_0, r_1)$ 
5    $r_0, r_1 \leftarrow r_1, r_0 - q \cdot r_1$ 
6    $t_0, t_1 \leftarrow t_1, t_0 - q \cdot t_1$ 
7 if  $t_0 < 0$  then
8    $t_0 \leftarrow t_0 + n$ 
Return :  $t_0$ 
```

# Extended Euclidean Algorithm – Summary

---

**Input** :  $v, n$ : two positive integers with  $v \leq n$  and  $\gcd(v, n) = 1$

**Output**:  $v^{-1} \bmod n$ : the inverse of  $v$  modulo  $n$

1  $r_0, r_1 \leftarrow n, v$

2  $t_0, t_1 \leftarrow 0, 1$

3 **while**  $r_1 \neq 0$  **do**

4      $q \leftarrow \text{div}(r_0, r_1)$

5      $r_0, r_1 \leftarrow r_1, r_0 - q \cdot r_1$

6      $t_0, t_1 \leftarrow t_1, t_0 - q \cdot t_1$

7 **if**  $t_0 < 0$  **then**

8      $t_0 \leftarrow t_0 + n$

**Return** :  $t_0$

---

# Iterations does match with  $s^{-1} \bmod N$

Timing Leakage on  $\text{len}(r_0) - \text{len}(r_1)$

Odd iterations  $\neq$  Even iterations

# A Masked Modular Inversion

$$\begin{aligned}k' &= k \times m \bmod N \\k'^{-1} &= \text{EEA}(k', N) \\k^{-1} &= k'^{-1} \times m \bmod N\end{aligned}$$

# A Masked Modular Inversion

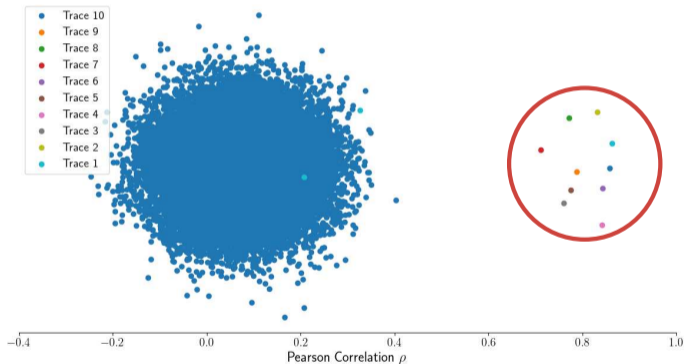
$$\begin{aligned}k' &= k \times m \bmod N \\k'^{-1} &= \text{EEA}(k', N) \\k^{-1} &= k'^{-1} \times m \bmod N\end{aligned}$$

- ▶ Hypothesis: the mask can be brute-forced  
(otherwise there is no reason to continue the investigation)
- ▶ Brute-force the mask:
  - ▶ For each value  $\hat{m}$ , compute  $\hat{k}' = k \times \hat{m} \bmod N$
  - ▶ Predict the sequence of  $\{\hat{\ell}_i = \text{len}(r_0) - \text{len}(r_1)\}_i$
  - ▶ compare  $\{\hat{\ell}_i\}$  with  $\{\ell_i\}_i$  (the observations)
  - ▶ Keep  $\hat{m}$  if the sequences match well enough

# A Masked Modular Inversion – Brute-Force Results

For the selected masks  $\hat{m}$

Pearson Correlation between  $\{\hat{\ell}_i = \text{len}(r_0) - \text{len}(r_1)\}_i$  and  $\{\ell_i\}_i$



$m$  is always a 32-bit odd integer!



## Let's sum up

- ▶ Timing leakage in the EEA implementation that inverse ECDSA's nonce.

## Let's sum up

- ▶ Timing leakage in the EEA implementation that inverse ECDSA's nonce.
- ▶ Nonce is blinded with a 32-bit multiplicative mask.

blinded nonce  $\rightarrow$  nonce  $\rightarrow$  private key

## Let's sum up

▶ Timing leakage in the EEA implementation that inverse ECDSA's nonce.

▶ Nonce is blinded with a 32-bit multiplicative mask.

blinded nonce  $\rightarrow$  nonce  $\rightarrow$  private key

▶ The timing leakage **might be enough information** to guess the blinded nonce.

Theoretically

## Let's sum up

▶ Timing leakage in the EEA implementation that inverse ECDSA's nonce.

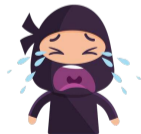
▶ Nonce is blinded with a 32-bit multiplicative mask.

blinded nonce  $\rightarrow$  nonce  $\rightarrow$  private key

▶ The timing leakage **might be enough information** to guess the blinded nonce.

Theoretically

# No Key-Recovery Attack Was Found!



# Agenda

## Introduction

FIDO Hardware Tokens

Infineon SLE 78

FEITIAN A22 Open JavaCard

Infineon ECDSA Observations

The Extended Euclidean Algorithm

## A Side-Channel Vulnerability in EEA

ECDSA Signature Verification

Infineon ECDSA Signature Verification

First Observations

Summary

A Masked Modular Inversion

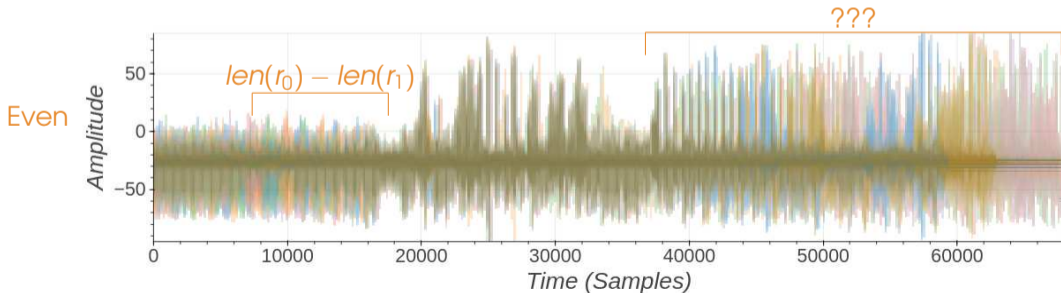
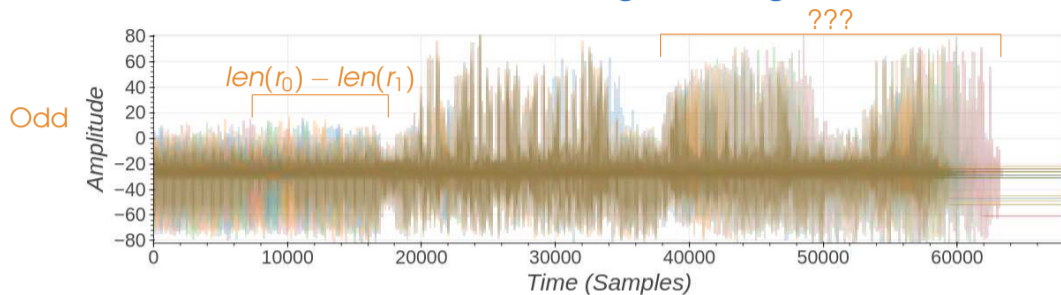
## Full Reverse-Engineering of Infineon EEA

Heuristical Approaches

Summary of The Sensitive Leakage



# FEITIAN A22 – $s^{-1} \bmod N$ – More Timing Leakages



# A Weird Euclidean Division Algorithm

---

**Input** :  $a, b$ : two positive integers

**Output**:  $q$ : the quotient of the division of  $a$  by  $b$

```
1  $r \leftarrow a$ 
2  $\ell \leftarrow \text{len}(r) - \text{len}(b)$ 
3  $q \leftarrow 0$ 
4 while  $\ell \geq 0$  do
5    $g \leftarrow \text{sign}(r) \cdot 2^\ell$ 
6    $r \leftarrow r - g \cdot b$ 
7    $q \leftarrow q + g$ 
8    $\ell \leftarrow \text{len}(r) - \text{len}(b)$ 
9 if  $r < 0$  then
10   $q \leftarrow q - 1$ 
11   $r \leftarrow r + b$ 
    // q is the quotient
    // r is the remainder
Return :  $q$ 
```

---

# Summary of The Sensitive Leakage

---

**Input** :  $a, b$ : two positive integers

**Output**:  $q$ : the quotient of the division of  $a$  by  $b$

```
1  $r \leftarrow a$ 
2  $\ell \leftarrow \text{len}(r) - \text{len}(b)$             $\ell = \text{len}(r_0) - \text{len}(r_1)$  leaks
3  $q \leftarrow 0$ 
4 while  $\ell \geq 0$  do                   # Loop Iter. leaks
5    $g \leftarrow \text{sign}(r).2^\ell$           $\ell = 0$  leaks
6    $r \leftarrow r - g.b$ 
7    $q \leftarrow q + g$ 
8    $\ell \leftarrow \text{len}(r) - \text{len}(b)$ 
9 if  $r < 0$  then
10   $q \leftarrow q - 1$ 
11   $r \leftarrow r + b$ 
Return :  $q$                                // q is the quotient
                                           // r is the remainder
```



## Let's sum up

- ▶ Timing leakage in the EEA implementation that inverse ECDSA's nonce.

## Let's sum up

- ▶ Timing leakage in the EEA implementation that inverse ECDSA's nonce.
- ▶ Nonce is blinded with a 32-bit multiplicative mask.

blinded nonce  $\rightarrow$  nonce  $\rightarrow$  private key

## Let's sum up

- ▶ Timing leakage in the EEA implementation that inverse ECDSA's nonce.
- ▶ Nonce is blinded with a 32-bit multiplicative mask.  
blinded nonce  $\rightarrow$  nonce  $\rightarrow$  private key
- ▶ The timing leakage is **enough information** to guess the blinded nonce.



Side-Channel Attack  
on Ext. Euclidean Alg.

[ninjalab.io/eucleak](https://ninjalab.io/eucleak)

# Let's sum up

- ▶ Timing leakage in the EEA implementation that inverse ECDSA's nonce.
- ▶ Nonce is blinded with a 32-bit multiplicative mask.  
blinded nonce  $\rightarrow$  nonce  $\rightarrow$  private key
- ▶ The timing leakage is **enough information** to guess the blinded nonce.



Side-Channel Attack  
on Ext. Euclidean Alg.

[ninjalab.io/eucleak](http://ninjalab.io/eucleak)



# Agenda



## Introduction

FIDO Hardware

Infineon SLE

FEITIAN A22 C

Infineon EC

The Extended Elliptic Curve Algorithm

## A Side-Channel Vulnerability in EEA

ECDSA Signature Generation

Infineon ECDSA Signature Verification

First Observations

Summary

A Masked Modular Inversion

## Full Reverse-Engineering of Infineon EEA

Heuristical Approaches

Summary of The Sensitive Leakage

## Yubikey 5C

Aquisition Setup

First Side-Channel Traces

Attack in Practice

## Impact Analysis

Infineon Security Microcontrollers

Optiga Trust M

Optiga TPM

## Conclusions

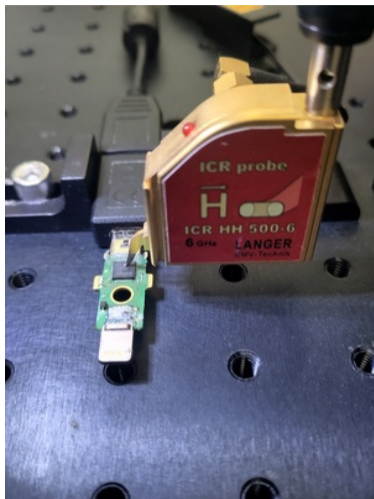
Conclusions

Mitigations

Project Timeline

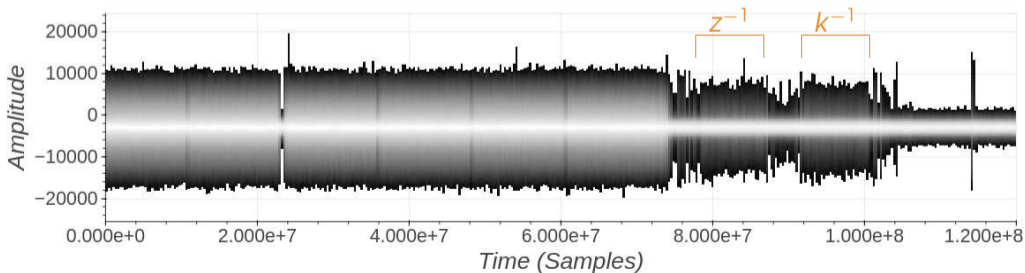
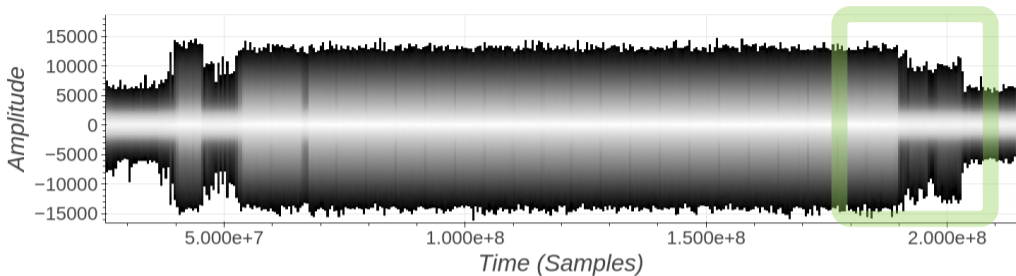
Project Timeline

# Yubikey 5Ci – EM Acquisitions

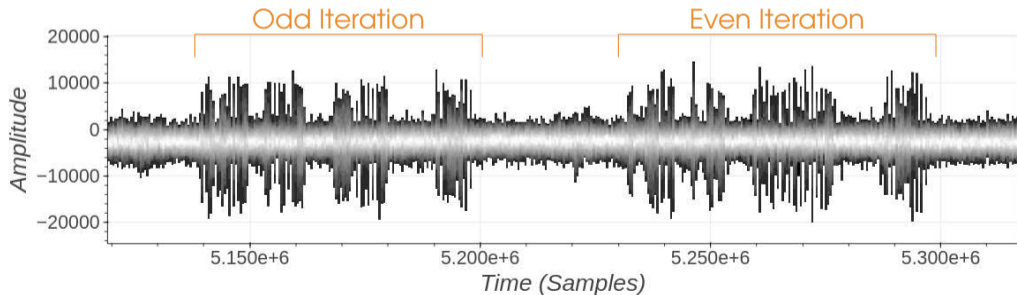
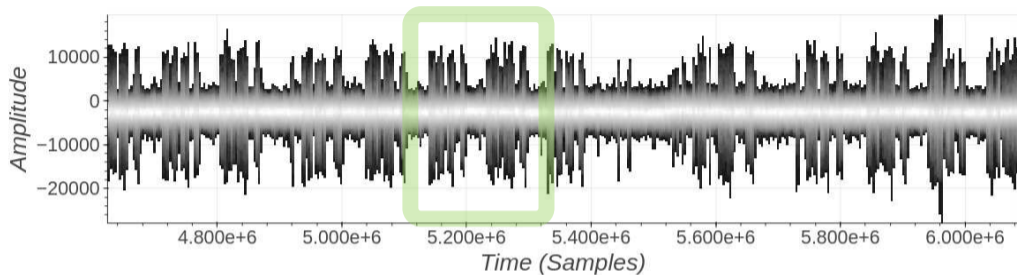


credits Yubico

# Yubikey 5Ci – ECDSA Command – EM Radiations



# Yubikey 5Ci – $k^{-1} \bmod N$ – EM Radiations





# Attack in Practice

- ▶ Secret key  $d$  is unknown
- ▶ Select EEA executions where  $len(r_0) - len(r_1) \leq 5$  for the first half of the EEA  
↳ from 200 side-channel traces, 6 are selected
- ▶ From all iterations of the 6 side-channel traces, the leakage is extracted.  
semi-automated
- ▶ The attack is successful for 5 out of the 6 EEA traces.



# Attack in Practice

- ▶ Secret key  $d$  is unknown
- ▶ Select EEA executions where  $len(r_0) - len(r_1) \leq 5$  for the first half of the EEA  
↳ from 200 side-channel traces, 6 are selected
- ▶ From all iterations of the 6 side-channel traces, the leakage is extracted.  
semi-automated
- ▶ The attack is successful for 5 out of the 6 EEA traces.
- ▶ The pruning step can be avoided with more effort on the learning phase.
- ▶ The leakage extraction could be improved in both
  - ▶ Automation
  - ▶ Robustness



# Agenda



Introduction  
FIDO H...  
Infineon SL...  
FEITIAN A22...  
Infineon T...  
The Extended  
Algorithm  
A Side-Channel  
ECDSA Signa...  
Infineon ECDSA...  
Verification  
First Observations  
Summary  
A Masked Modular Inversion  
Full Reverse-Engineering of Infineon EEA  
Heuristical Approaches  
Summary of The Sensitive Leakage

Yubikey 5C  
Aquisition Setup  
First Side-Channel Traces  
Attack in Practice  
Impact Analysis  
Infineon Security Microcontrollers  
Optiga Trust M  
Optiga TPM  
Conclusions  
Conclusions  
Mitigations  
Project Timeline  
Project Timeline

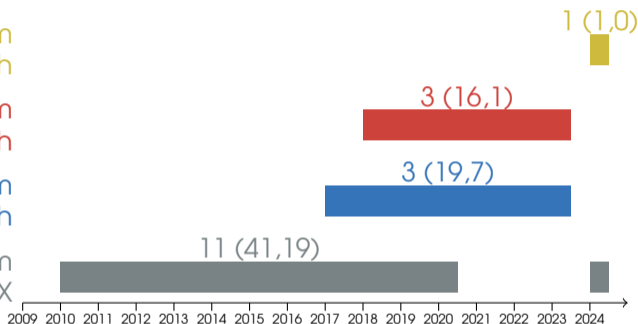
# Infineon Security Microcontrollers (IC CC Certifications)

armv8-M, 28 nm  
IFX\_CCI\_00007Dh

SC300, 40/65 nm  
IFX\_CCI\_0-0XYh

16-bit, 65 nm  
IFX\_CCI\_0-0Xh

16-bit, 90 nm  
M78XX



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

Credits: [www.bsi.bund.de](http://www.bsi.bund.de), [www.sec-certs.org](http://www.sec-certs.org)

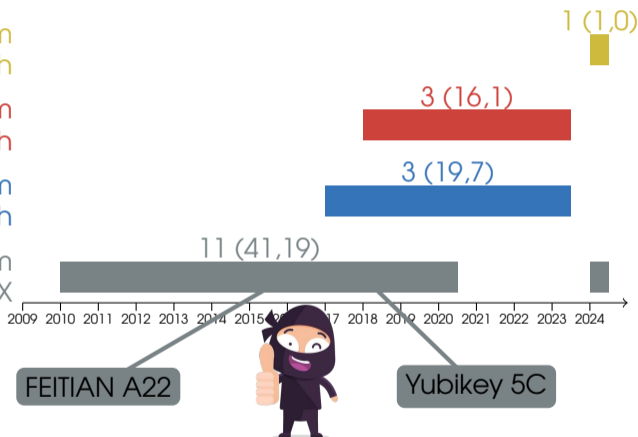
# Infineon Security Microcontrollers (IC CC Certifications)

armv8-M, 28 nm  
IFX\_CCI\_00007Dh

SC300, 40/65 nm  
IFX\_CCI\_0-0XYh

16-bit, 65 nm  
IFX\_CCI\_0-0Xh

16-bit, 90 nm  
M78XX



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

Credits: [www.bsi.bund.de](http://www.bsi.bund.de), [www.sec-certs.org](http://www.sec-certs.org)

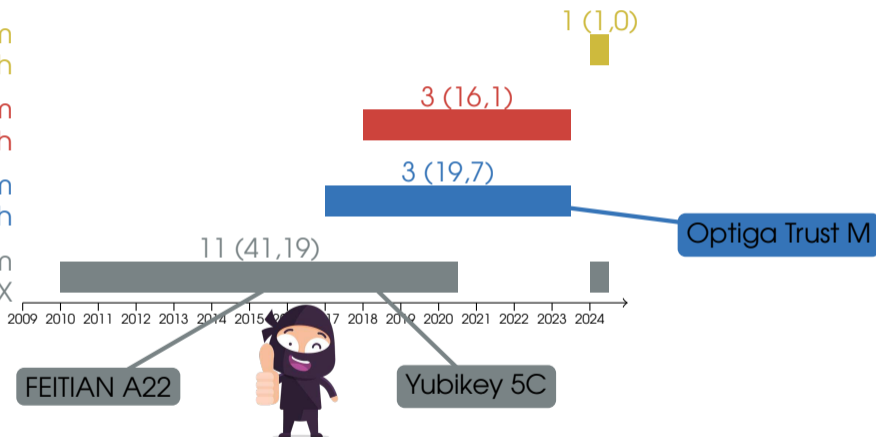
# Infineon Security Microcontrollers (IC CC Certifications)

armv8-M, 28 nm  
IFX\_CCI\_00007Dh

SC300, 40/65 nm  
IFX\_CCI\_0-0XYh

16-bit, 65 nm  
IFX\_CCI\_0-0Xh

16-bit, 90 nm  
M78XX



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

Credits: [www.bsi.bund.de](http://www.bsi.bund.de), [www.sec-certs.org](http://www.sec-certs.org)

# Optiga Trust M – Evaluation Kit



All Search

Newsletter Contact Where to Buy English myInfineon Cart

Products Applications Design Support Community About Infineon Careers

Home Products Evaluation Boards CY8CEVAL-062S2

## CY8CEVAL-062S2

- Overview
- Documents
- Order
- Design Support
- Support

The PSoC™ 62S2 evaluation kit (CY8CEVAL-062S2) enables you to evaluate and develop applications using the **PSoC™ 62 MCU**. The kit features the PSoC™ 62 MCU (CY8C624ABZI-S2D44): 150-MHz Arm® Cortex®-M4 and 100-MHz Arm® Cortex®-M0+ cores, 2MB of Flash, 1MB of SRAM, hardware crypto accelerator, rich analog and digital peripherals, audio and communication interfaces, and industry-leading capacitive-sensing with CAPSENSE™ technology.

This kit features an M.2 interface that enables you to connect the supported M.2 radio modules based on AIROC™ Wi-Fi/Bluetooth® combo devices. This feature enables flexible evaluation of the radio module that best suits your wireless connectivity requirements. With PSoC™ 62 MCU as the Wi-Fi host MCU, and the AIROC™ device enabling Wi-Fi and Bluetooth® connectivity, you can easily prototype and evaluate embedded IoT applications using this kit. In addition, the kit also features an OPTIGA™ Trust-M security controller for secured cloud device provisioning.

### Kit Features

- PSoC™ 62 MCU (CY8C624ABZI-S2D44)
- M.2 interface connector to connect the M.2 radio modules OPTIGA™ Trust-M security controller

Follow

Buy online

PSoC™ 62S2 evaluation kit (CY8CEVAL-062S2)

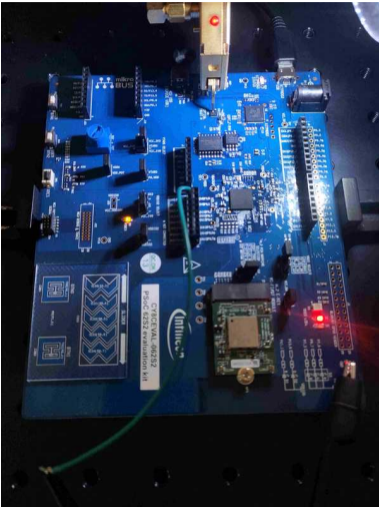


Download User Manual

<https://github.com/Infineon/optiga-trust-m>

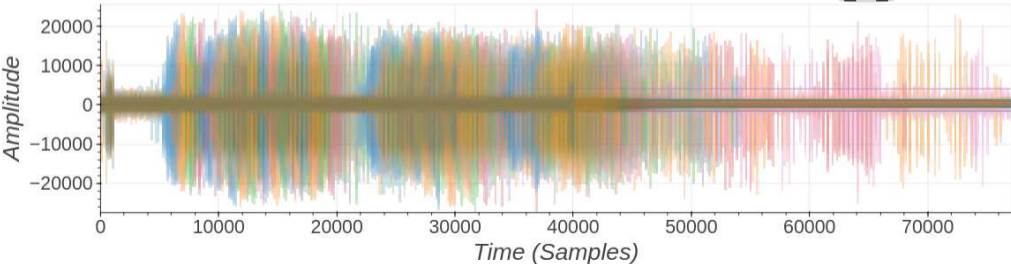
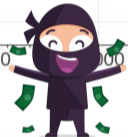
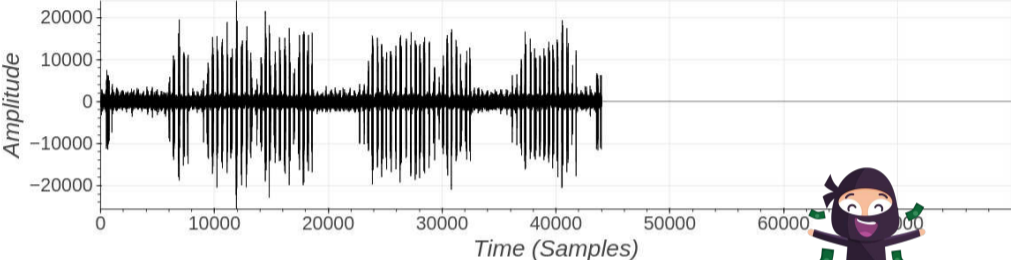
<https://github.com/Infineon/mtb-example-optiga-crypto>

# Optiga Trust M – Side-channel Setup





# Optiga Trust M – $s^{-1} \bmod N$ – Single Iteration



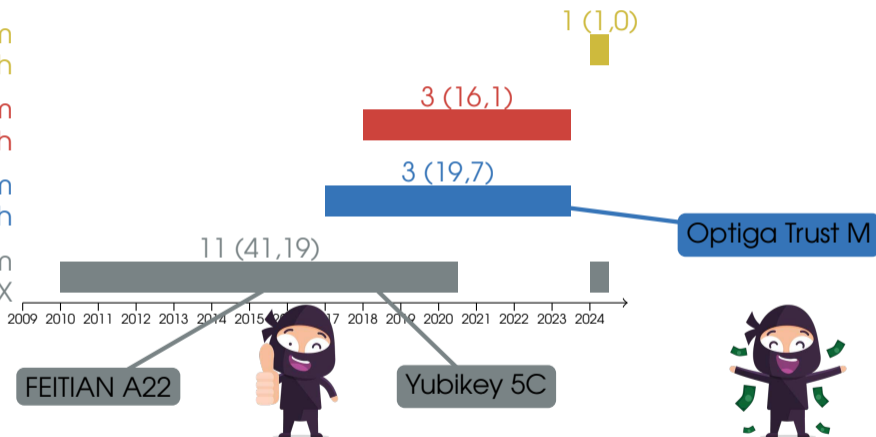
# Infineon Security Microcontrollers (IC CC Certifications)

armv8-M, 28 nm  
IFX\_CCI\_00007Dh

SC300, 40/65 nm  
IFX\_CCI\_0-0XYh

16-bit, 65 nm  
IFX\_CCI\_0-0Xh

16-bit, 90 nm  
M78XX



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

Credits: [www.bsi.bund.de](http://www.bsi.bund.de), [www.sec-certs.org](http://www.sec-certs.org)

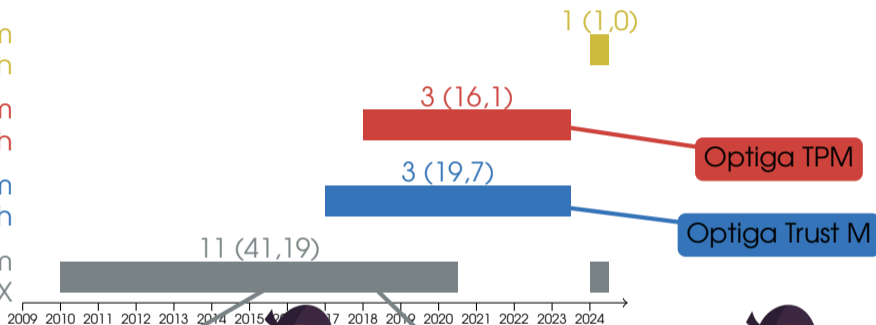
# Infineon Security Microcontrollers (IC CC Certifications)

armv8-M, 28 nm  
IFX\_CCI\_00007Dh

SC300, 40/65 nm  
IFX\_CCI\_0-0XYh

16-bit, 65 nm  
IFX\_CCI\_0-0Xh

16-bit, 90 nm  
M78XX



FEITIAN A22

Yubikey 5C

Optiga TPM

Optiga Trust M

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

Credits: [www.bsi.bund.de](http://www.bsi.bund.de), [www.sec-certs.org](http://www.sec-certs.org)

# Optiga TPM – Evaluation Kit



Tout ▼ Numéro de référence/Mot-clé

Produits ▼ Fabricants Services et outils Ressources techniques Aide

Tous les produits > Solutions intégrées > Calcul > HAT/cartes complémentaires Raspberry Pi > Infineon Technologies TPM9673FW2613RPIEBTOBO1

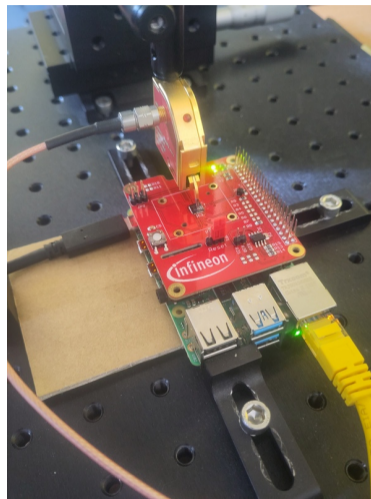
## TPM9673FW2613RPIEBTOBO1



Les images sont fournies à titre indicatif  
Voir les caractéristiques du produit

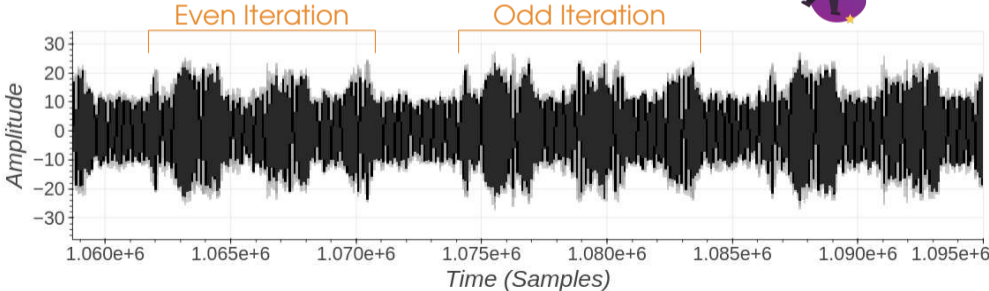
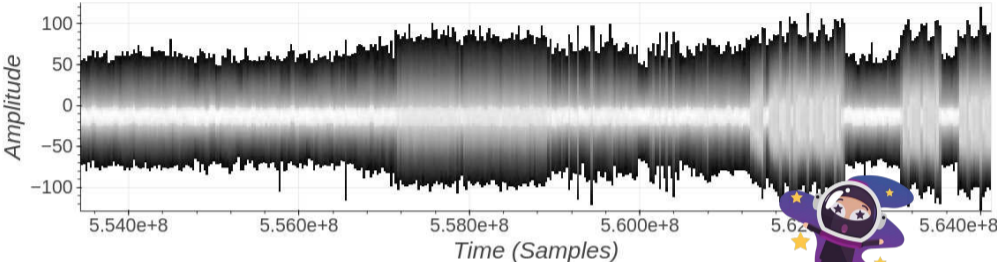
Partager

N° Mouser :	726-TPM9673FW2613RPI
N° de fab. :	TPM9673FW2613RPIEBTOBO1
Fab. :	Infineon Technologies
N° client:	<input type="text" value="N° client"/>
Description :	HAT/cartes complémentaires Raspberry Pi
Cycle de vie:	<b>NEW</b> Nouveau produit: Nouveau chez ce fabricant.
Fiche technique:	<a href="#">TPM9673FW2613RPIEBTOBO1 Fiche technique (PDF)</a>
Plus d'informations	<a href="#">En savoir plus à propos de Infineon Technologies TPM9673FW2613RPIEBTOBO1</a>



<https://github.com/Infineon/optiga-tpm>

# Optiga TPM – $s^{-1} \bmod N$ – EM Radiations



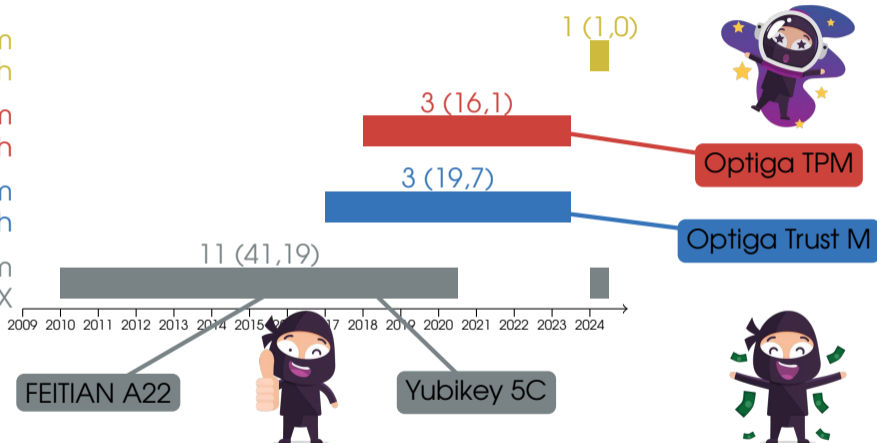
# Infineon Security Microcontrollers (IC CC Certifications)

armv8-M, 28 nm  
IFX\_CCI\_00007Dh

SC300, 40/65 nm  
IFX\_CCI\_0-0XYh

16-bit, 65 nm  
IFX\_CCI\_0-0Xh

16-bit, 90 nm  
M78XX



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

Credits: [www.bsi.bund.de](http://www.bsi.bund.de), [www.sec-certs.org](http://www.sec-certs.org)

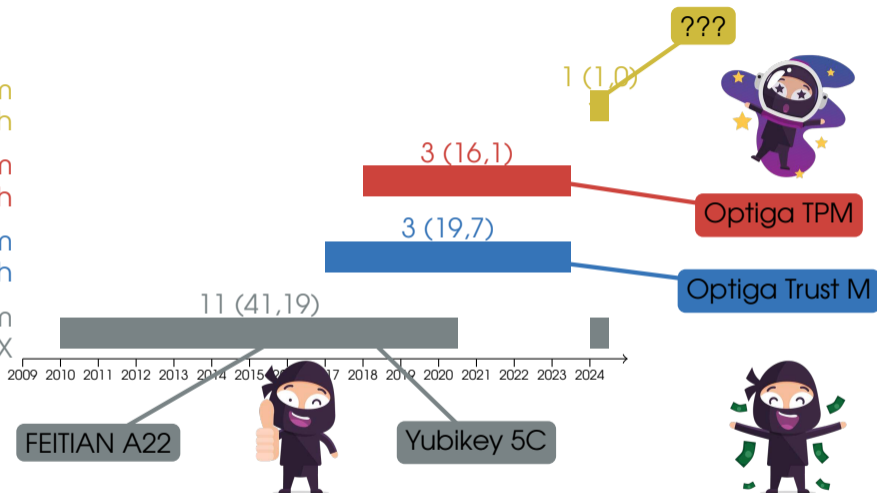
# Infineon Security Microcontrollers (IC CC Certifications)

armv8-M, 28 nm  
IFX\_CCI\_00007Dh

SC300, 40/65 nm  
IFX\_CCI\_0-0XYh

16-bit, 65 nm  
IFX\_CCI\_0-0Xh

16-bit, 90 nm  
M78XX



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

Credits: [www.bsi.bund.de](http://www.bsi.bund.de), [www.sec-certs.org](http://www.sec-certs.org)

# Infineon Security Microcontrollers (IC CC Certifications)

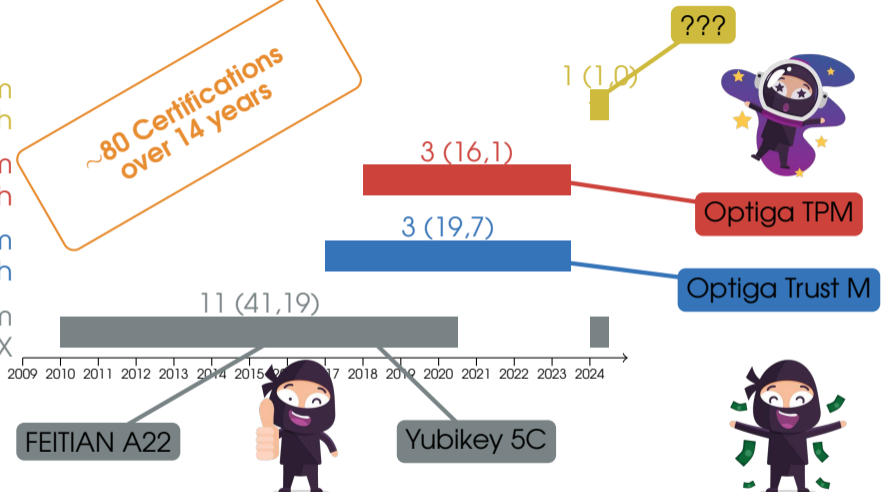
armv8-M, 28 nm  
IFX\_CCI\_00007Dh

SC300, 40/65 nm  
IFX\_CCI\_0-0XYh

16-bit, 65 nm  
IFX\_CCI\_0-0Xh

16-bit, 90 nm  
M78XX

~80 Certifications  
over 14 years



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

Credits: [www.bsi.bund.de](http://www.bsi.bund.de), [www.sec-certs.org](http://www.sec-certs.org)



# Agenda



## Introduction

FIDO Hardware

Infineon LE

FEITIAN Attack

Infineon ECDSA

The Extended

## A Side-Channel Attack on the Stability in EEA

ECDSA Signature Verification

Infineon ECDSA Signature Verification

First Observations

Summary

A Masked Modular Inversion

## Full Reverse-Engineering of Infineon EEA

Heuristical Approaches

Summary of The Sensitive Leakage

## Yubikey 5C

Aquisition Setup

First Side-Channel Traces

Attack in Practice

## Impact Analysis

Infineon Security Microcontrollers

Optiga Trust M

Optiga TPM

## Conclusions

Conclusions

Mitigations

Project Timeline

Project Timeline

# Let's sum up: Attack Requirements

- ▶ *Infineon security microcontroller with Infineon cryptlib*
- ▶ modular inversion of a secret (eg. ECDSA).
- ▶ The attacker must have physical access to the device:
  - ▶ open the device to access to the Infineon chip package;
  - ▶ EM probe + oscillo to capture the EM side-channel signal (few minutes).
- ▶ Later, the offline phase will take one hour to one day to retrieve the private key.

Generate/Store Keys  
Key Exch./Wrap.

Signatures



Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

NXP

infineon



$\varphi$  Attacker

- Bitcoin HW Wallets
- 2FA HW Tokens

Side-Channel

Fault Injection

Invasive

Simple SW  
Simple I/O  
Formal Methods

- SmartPhones
- Computers (TPMs)

HW CMs

SW/Crypto CMs

- Smart Cars
- Smart Homes

...

Generate/Store Keys  
Key Exch./Wrap.

Signatures



Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

NXP



$\varphi$  Attacker



- Bitcoin HW Wallets
- 2FA HW Tokens

Side-Channel

Fault Injection

Invasive

Simple SW  
Simple I/O  
Formal Methods

- SmartPhones
- Computers (TPMs)

HW CMs

SW/Crypto CMs

- Smart Cars
- Smart Homes

...

Generate/Store Keys  
Key Exch./Wrap.

Signatures



Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

NXP



≥ 14 years



$\varphi$  Attacker

- Bitcoin HW Wallets
- 2FA HW Tokens

Side-Channel

Fault Injection

Invasive

Simple SW  
Simple I/O  
Formal Methods

HW CMs

SW/Crypto CMs

- SmartPhones
- Computers (TPMs)

- Smart Cars
- Smart Homes

...

# Mitigations

## At Infineon Level:

- ▶ Increase the size of the multiplicative mask to Elliptic Curve size
- ▶ Use a *constant time* algorithm for inversion

eg. BEEA or ModExp

## At Application Level:

- ▶ Avoid ECDSA

eg. EdDSA or RSA

- ▶ Defense in Depth

eg. Activate PIN (or any biometrics) on the device

- ▶ Protocol Specific Mitigations

eg. Activate Counter in FIDO

# Project Timeline



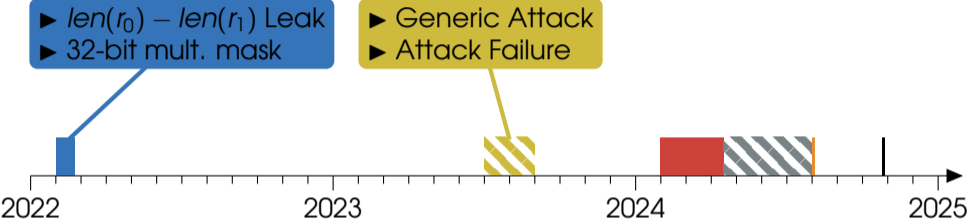
# Project Timeline

- ▶  $len(r_0) - len(r_1)$  Leak
- ▶ 32-bit mult. mask

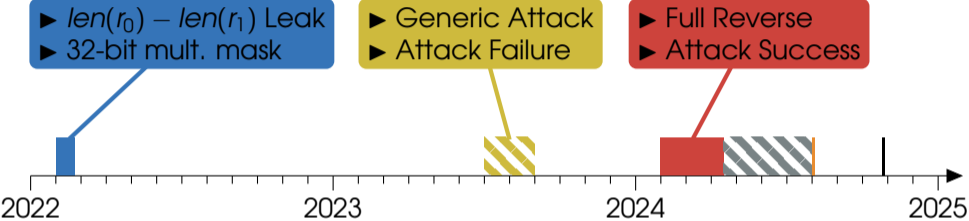




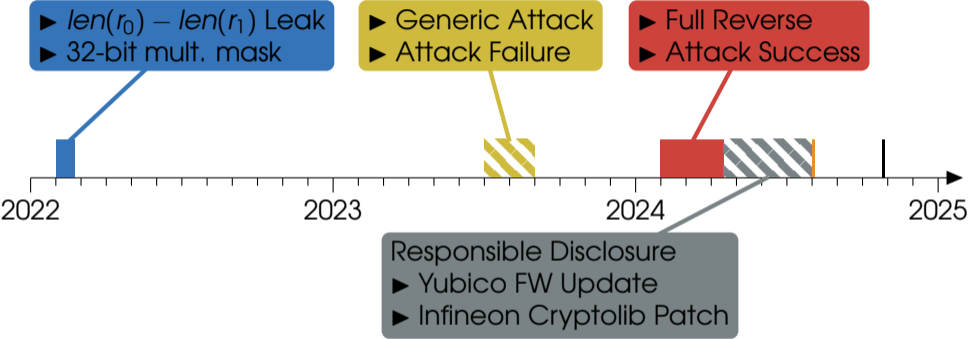
# Project Timeline



# Project Timeline



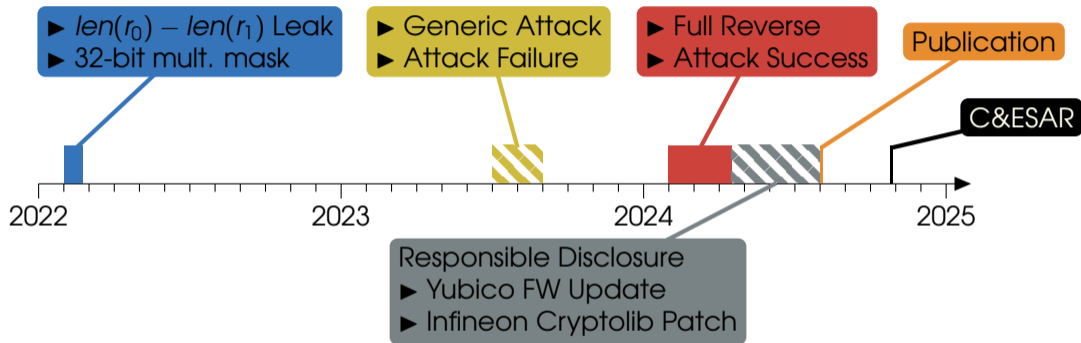
# Project Timeline



# Project Timeline



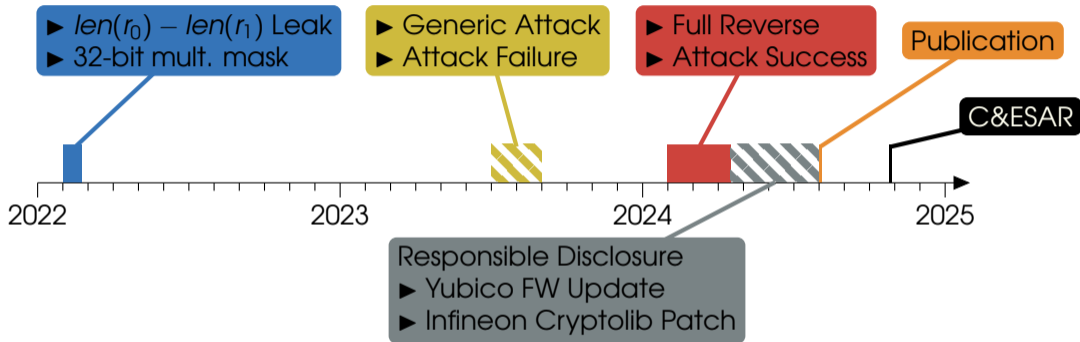
[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)



# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)

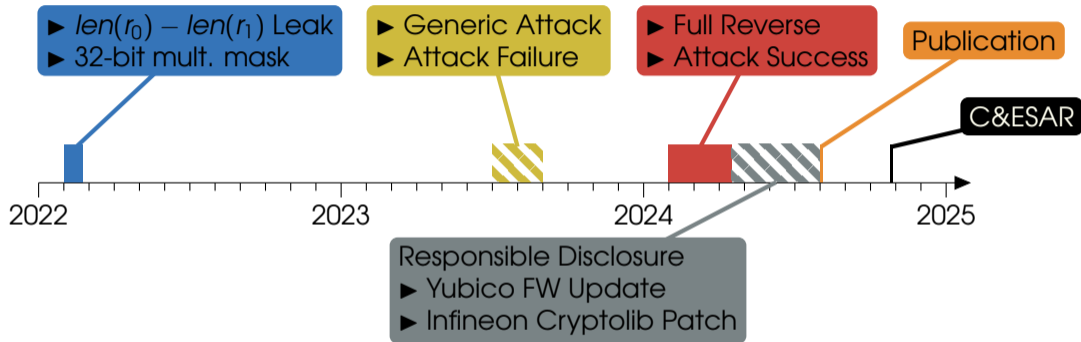


- Sept. 3rd 2024: Yubico Releases a Security Advisory

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)

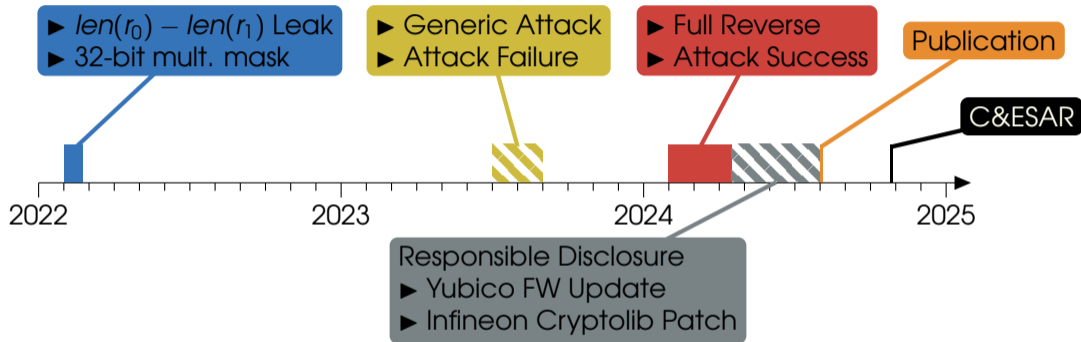


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)

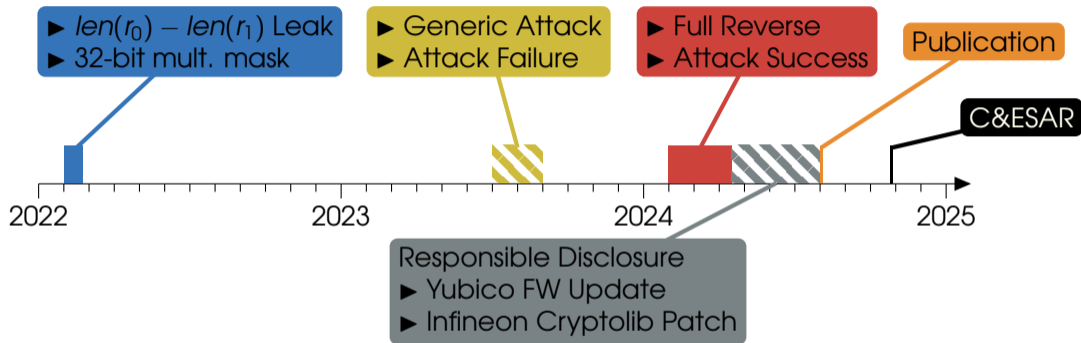


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)



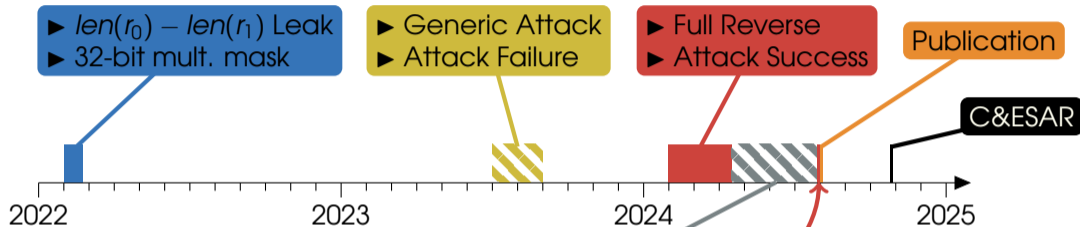
- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**



# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)



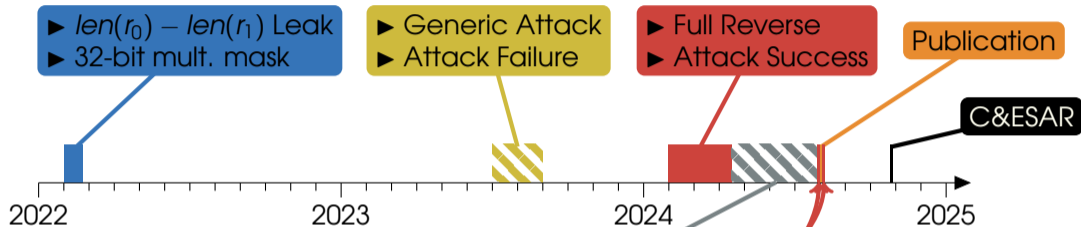
- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

NSCIB  AVA_VAN 5	IFX_CCI_0000XYh (ARM SC300 - 65nm)  Vulnerable ECC Library
------------------------	--

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)



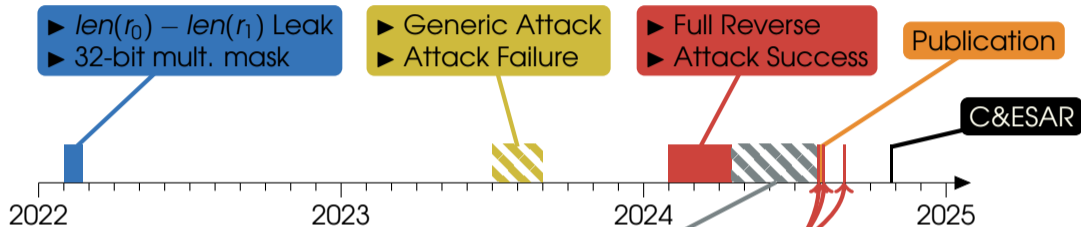
- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

BSI	IFX_CCI_00007Dh (Armv8-M - 28nm)
NSCIB	IFX_CCI_0000XYh (ARM SC300 - 65nm)
AVA_VAN 5	Vulnerable ECC Library

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)



- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

BSI IFX\_CCI\_000003h (16-bit - 65nm)

BSI IFX\_CCI\_00007Dh (Armv8-M - 28nm)

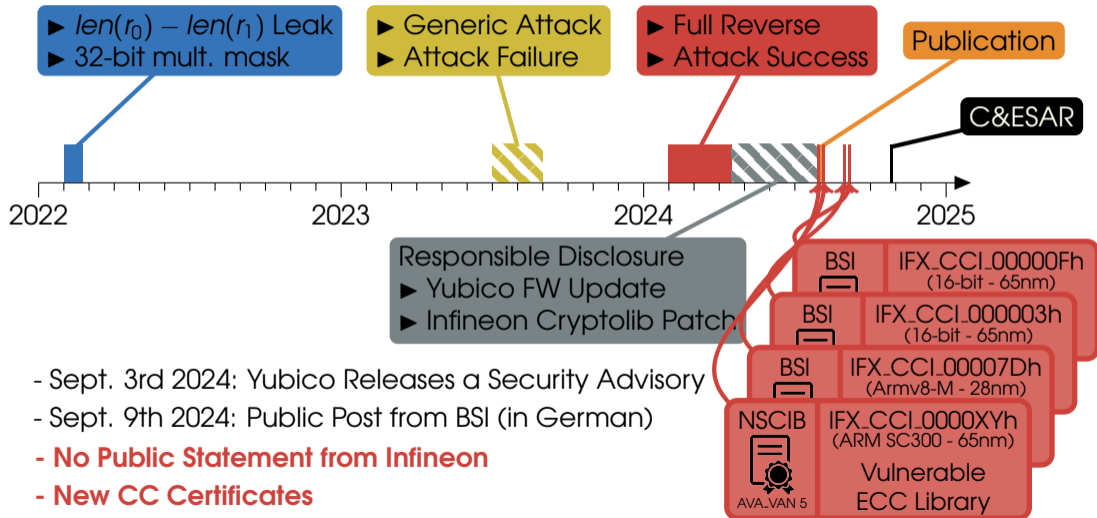
NSCIB IFX\_CCI\_0000XYh (ARM SC300 - 65nm)

AVA\_VAN 5 Vulnerable ECC Library

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)

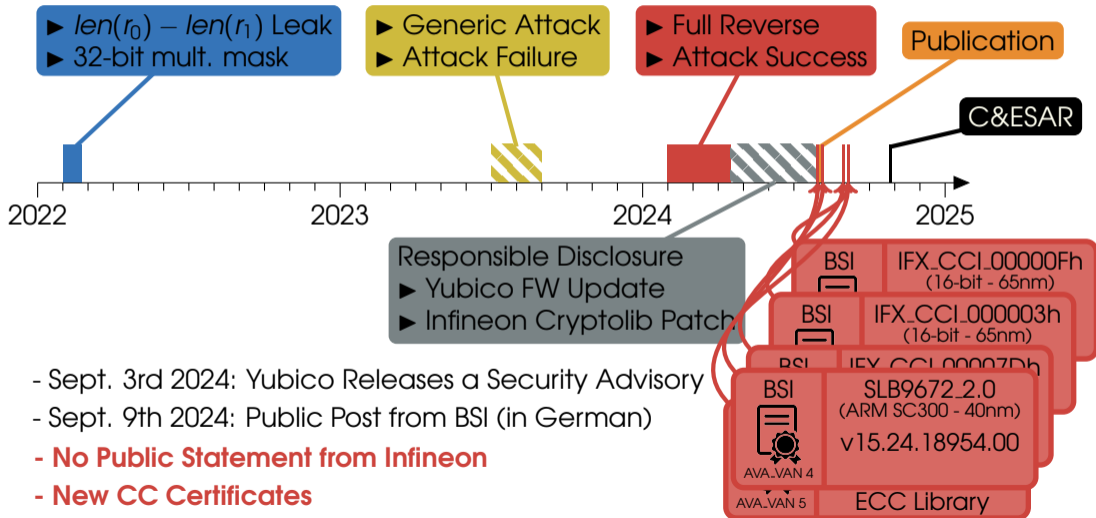


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)

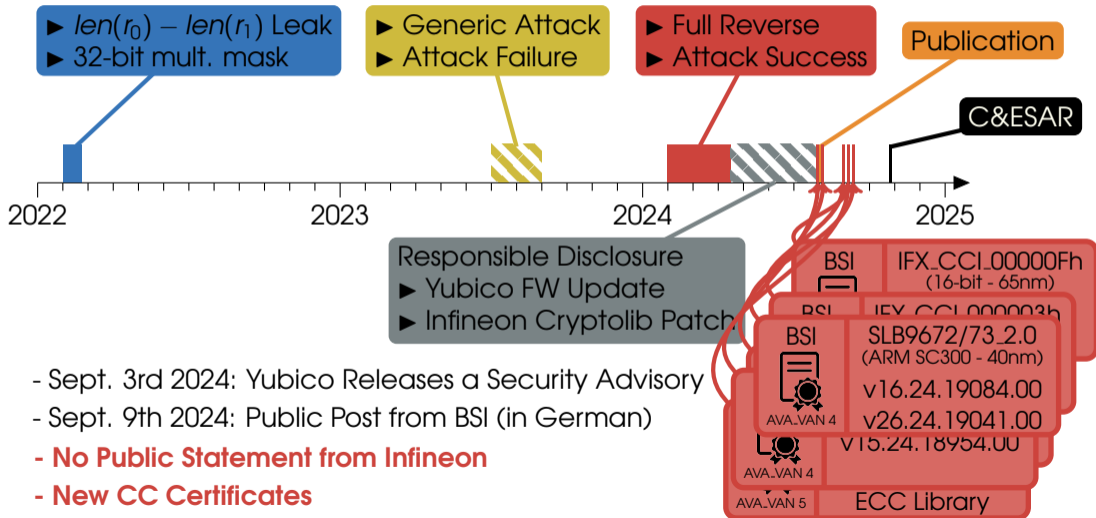


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)

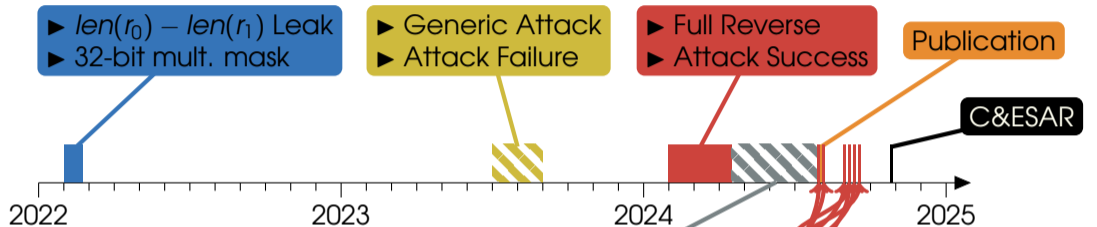


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

# Project Timeline



[ninjalab.io/eucleak](https://ninjalab.io/eucleak)  
[eprint.iacr.org/2024/1380](https://eprint.iacr.org/2024/1380)



- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

BSI  
SLB9672/73\_2.0  
(ARM SC300 - 40nm)  
v17.24.19084.00  
v27.24.19041.00  
AVA\_VAN 4

AVA\_VAN 4  
v16.24.19084.00  
v26.24.19041.00

AVA\_VAN 4  
v15.24.18954.00

AVA\_VAN 5  
ECC Library

# Infineon Security Microcontrollers – EC CryptoLibs – AFAWK

Family	Affected EC lib Versions	New EC lib versions
16-bit, 90 nm	1.1.18, 1.02.008, 1.02.013, 1.03.006, 2.03.008, 2.07.003	None
16-bit, 65 nm	2.06.003, 2.07.003, 2.08.007, 3.33.003	2.09.002
SC300, 40/65 nm	2.08.006, 3.03.003, 3.04.001	3.05.002
armv8-M, 28 nm	4.06.002	4.08.001
OptigaTPM	v15.20, v15.21, v15.22, v15.23, v16.10, v16.12, v26.10, v17.10, v17.12, v17.13, v27.10, v27.13	v15.24 v16.24, v26.24 v17.24, v27.24