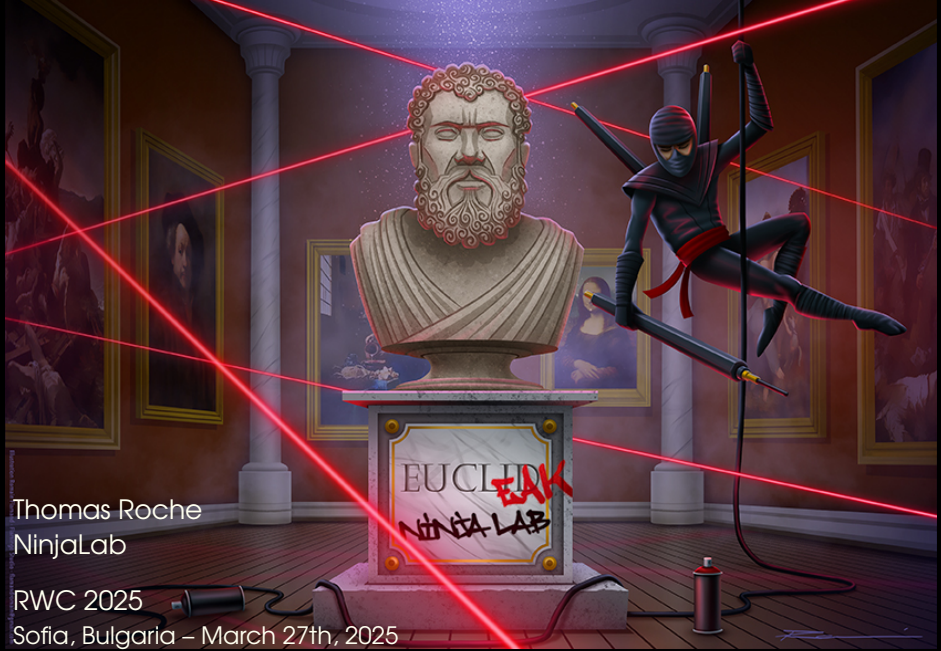


Thomas Roche
NinjaLab

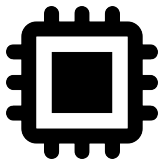
RWC 2025
Sofia, Bulgaria – March 27th, 2025

Secure Elements

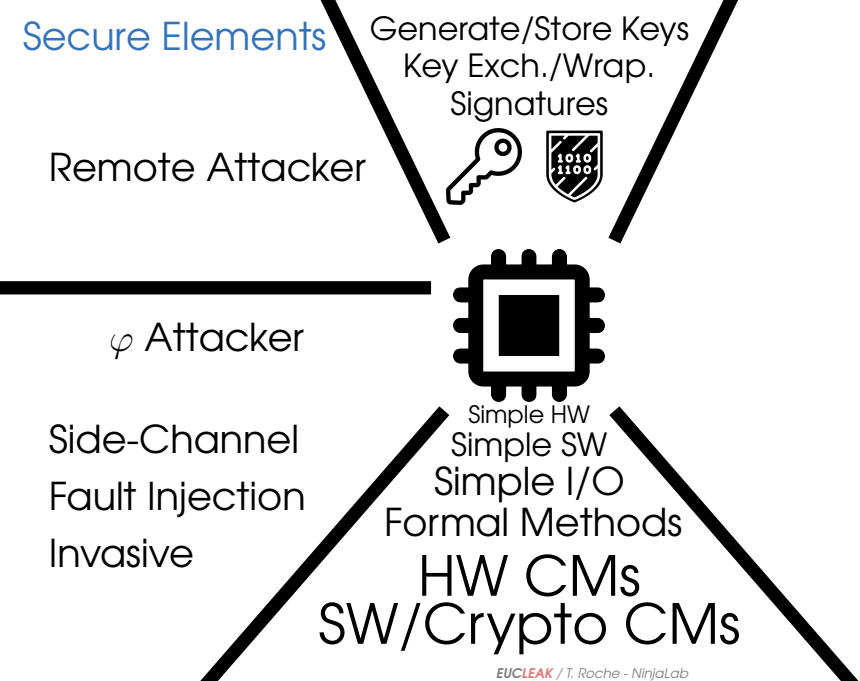
Secure Elements

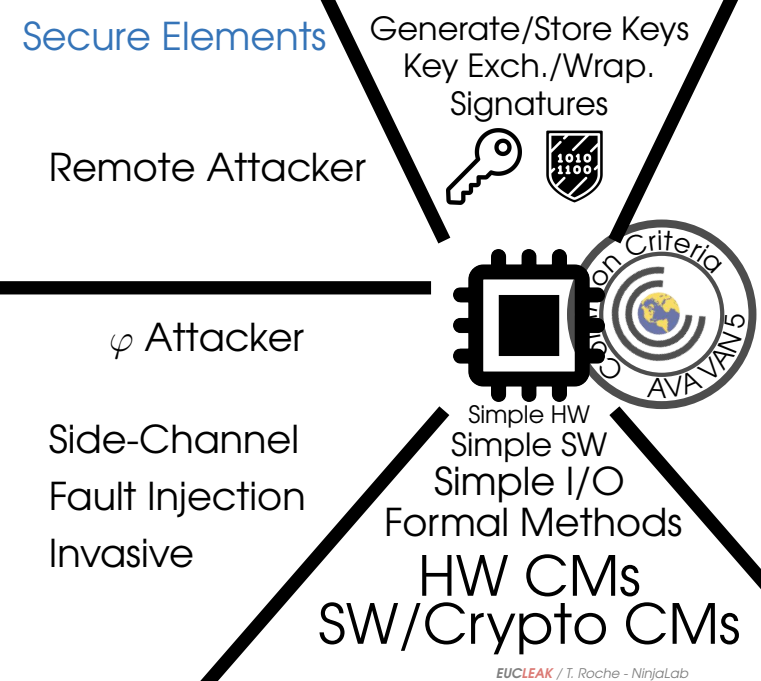
Generate/Store Keys
Key Exch./Wrap.
Signatures

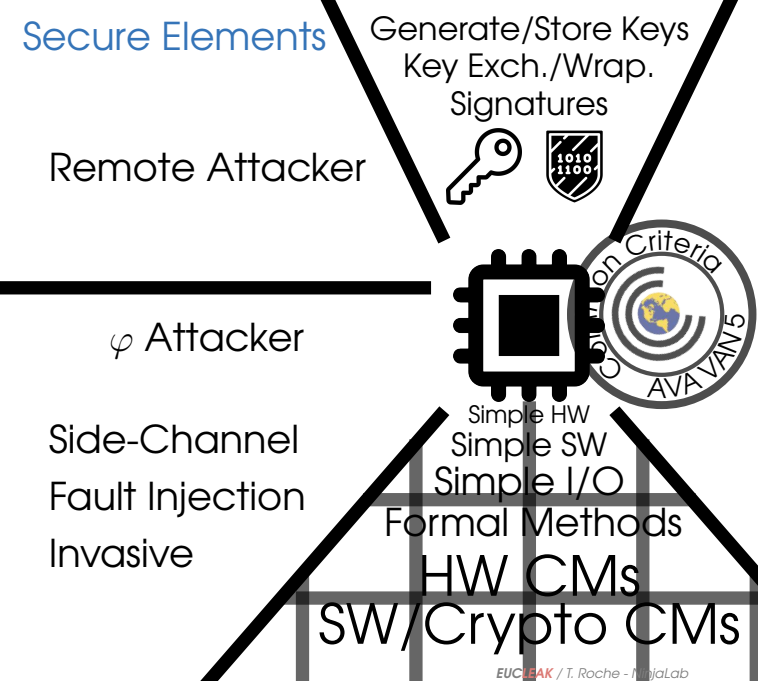
Remote Attacker

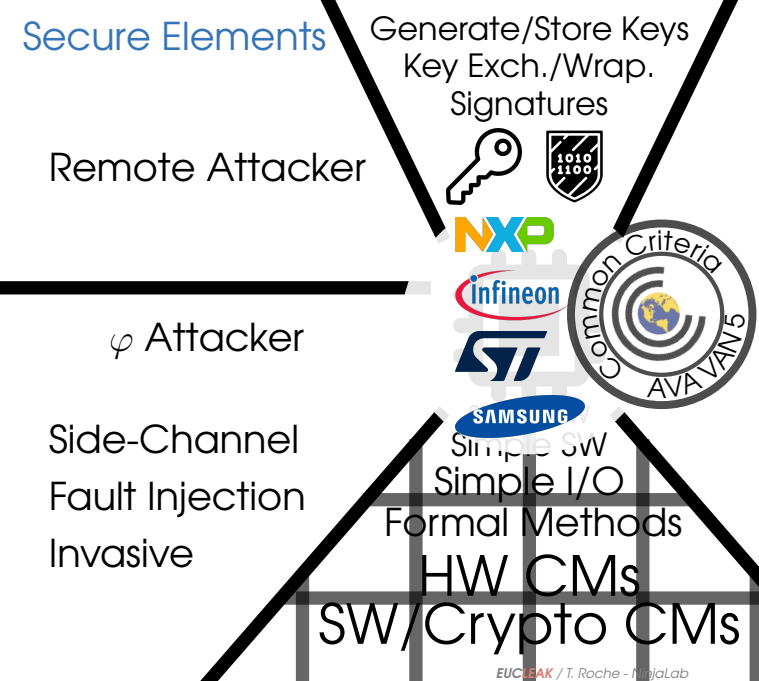


Simple HW
Simple SW
Simple I/O
Formal Methods


Secure Elements
Generate/Store Keys
Key Exch./Wrap.
Signatures
Remote Attacker
φ 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
1010
1100
Common Criteria
AVA VAN 5
φ Attacker
Simple HW
Simple SW
Simple I/O
Formal Methods
Side-Channel
Fault Injection
Invasive
HW CMs
SW/Crypto CMs


Secure Elements
Generate/Store Keys
Key Exch./Wrap.
Signatures
Remote Attacker
φ Attacker
Common Criteria
AVA VAN 5
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
NXP
infineon
SAMSUNG
Common Criteria
AVA VAN 5
φ 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

Remote Attacker

φ 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

...

EUCLEAK

Generate/Store Keys
Key Exch./Wrap.
Signatures

Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

- Bitcoin HW Wallets
- 2FA HW Tokens

- SmartPhones
- Computers (TPMs)

- Smart Cars
- Smart Homes

...

φ Attacker

Side-Channel
Fault Injection
Invasive

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

Agenda

Agenda

FIDO Hardware Tokens

credits Yubico

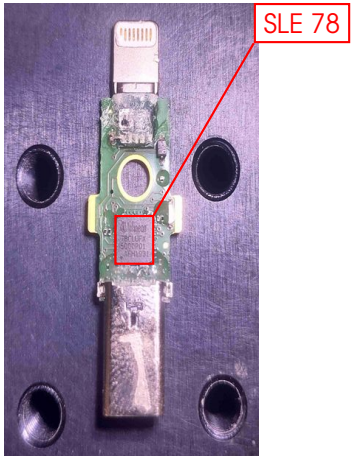
- (2nd) Authentication Factor
- FIDO core crypto primitive is ECDSA:

  Elliptic Curve Digital Signature Algorithm

  - Generate ECDSA key-pairs
  - ECDSA Sign challenges
- Protect the ECDSA private keys

  ↪ Secure Element

Yubikey 5Ci

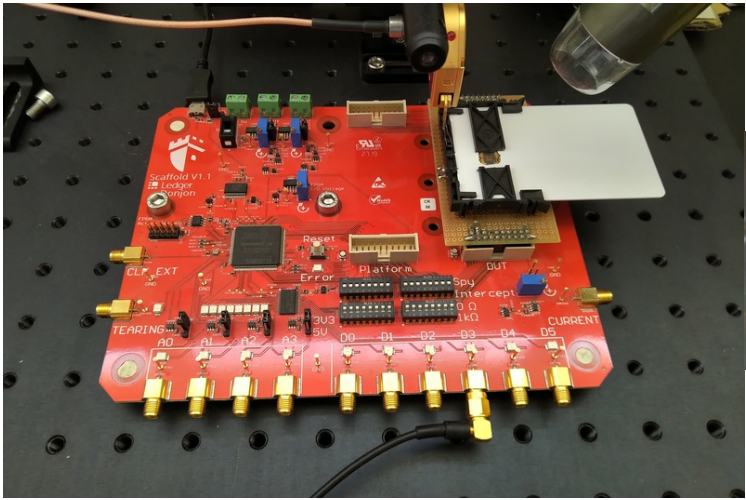


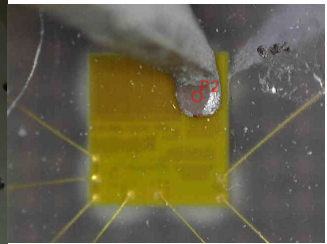
credits Yubico

Yubikey 5Ci – FEITIAN A22 Open JavaCard

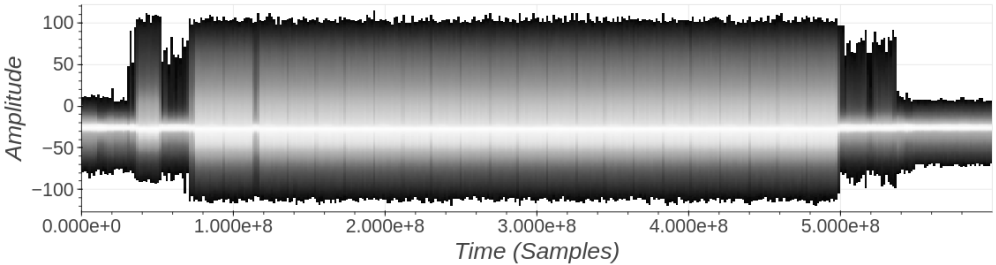
Agenda

FEITIAN A22 – EM Acquisitions





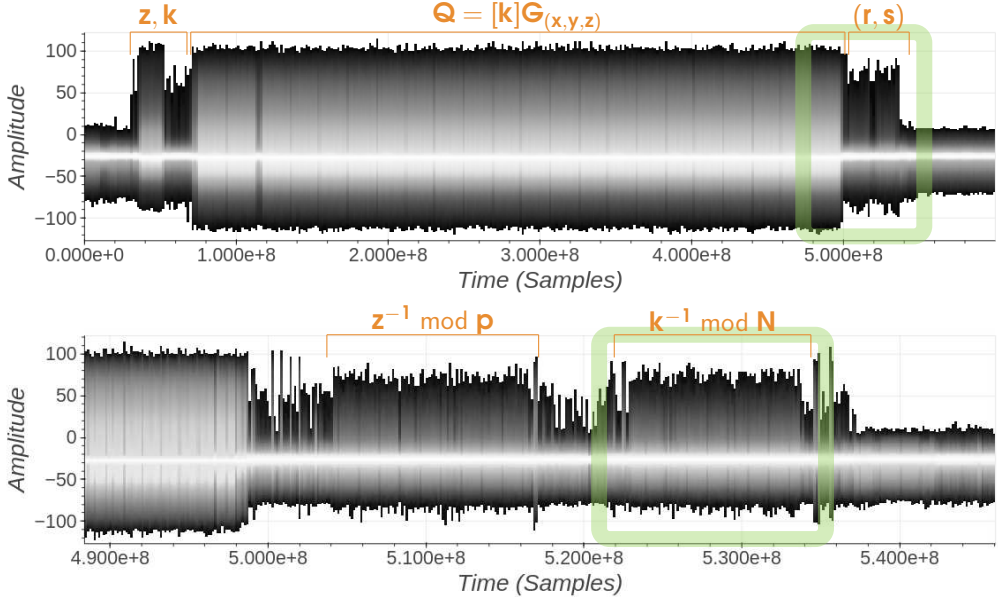
FEITIAN A22 – ECDSA Command – EM Radiations



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 $\mathbb{Z}/N\mathbb{Z}$
- compute $Q_{(x,y)} = [k]G_{(x,y)}$
  - 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



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 $\quad q \leftarrow \mathtt{div}(r_0, r_1)$
5 $\quad r_0, r_1 \leftarrow r_1, r_0 - q.r_1$
6 $\quad t_0, t_1 \leftarrow t_1, t_0 - q.t_1$
7 **if** $t_0 < 0$ **then**
8 $\quad t_0 \leftarrow t_0 + n$

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 $\quad q \leftarrow \mathtt{div}(r_0, r_1)$
5 $\quad r_0, r_1 \leftarrow r_1, r_0 - q.r_1$
6 $\quad t_0, t_1 \leftarrow t_1, t_0 - q.t_1$
7 **if** $t_0 < 0$ **then**
8 $\quad t_0 \leftarrow t_0 + n$
Return : t_0

k is blinded with a 32-bit mask

$$m \xleftarrow{\$} \mathbb{Z}/2^{32}\mathbb{Z}^\star$$
$$k' = k \times m \bmod N$$
$$k'^{-1} = \mathtt{EEA}(k', N)$$
$$k^{-1} = k'^{-1} \times m \bmod N$$

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 $\quad q \leftarrow \texttt{div}(r_0, r_1)$
5 $\quad r_0, r_1 \leftarrow r_1, r_0 - q.r_1$
6 $\quad t_0, t_1 \leftarrow t_1, t_0 - q.t_1$
7 **if** $t_0 < 0$ **then**
8 $\quad t_0 \leftarrow t_0 + n$
Return : t_0

Input : a, b: two positive integers
Output : q: the quotient of the division of a by b

$r \leftarrow a$
$\ell \leftarrow len(r) - len(b)$
$q \leftarrow 0$
while $\ell \geq 0$ **do**
$\quad g \leftarrow \texttt{sign}(r).2^{\ell}$
$\quad r \leftarrow r - g.b$
$\quad q \leftarrow q + g$
$\quad \ell \leftarrow len(r) - len(b)$
if $r < 0$ **then**
$\quad q \leftarrow q - 1$
$\quad r \leftarrow r + b$
Return : q

Let's sum up

- Timing leakages in the EEA implementation that inverse ECDSA's nonce k.

Let's sum up

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

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

Let's sum up

- Timing leakages in the EEA implementation that inverse ECDSA's nonce k.
- 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

Let's sum up

- Timing leakages in the EEA implementation that inverse ECDSA's nonce k.
- 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

Agenda

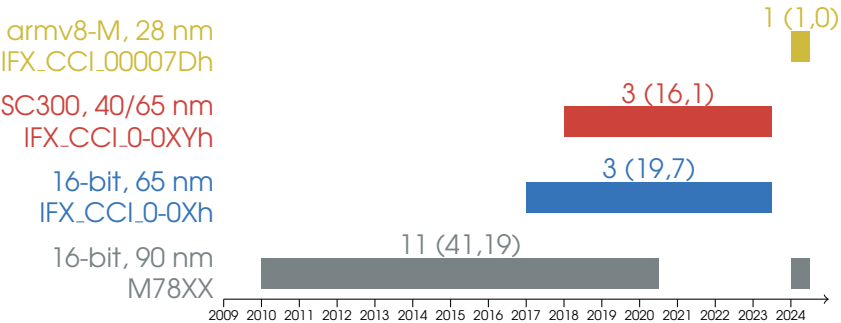
Introduction
- FIDO Ha…
- Yubikey …

A Side-Chann… …bility
- Infineon ECDS… …s
- The Extended … …gorithm
- Summary

Impact Analysis
- Infineon Security Microcontrollers

Conclusions
- Summing up
- Mitigations
- Project Timeline

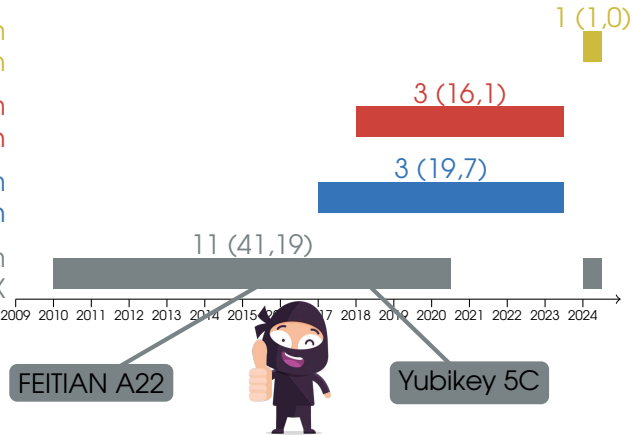
Infineon Security Microcontrollers (IC CC Certifications)



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

Credits: `www.bsi.bund.de`, `www.sec-certs.org`

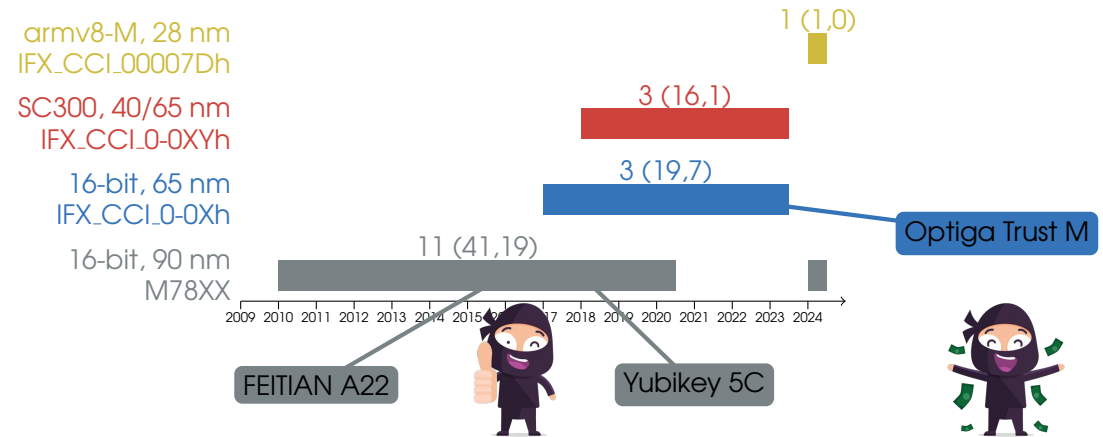
Infineon Security Microcontrollers (IC CC Certifications)



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

Credits: `www.bsi.bund.de`, `www.sec-certs.org`

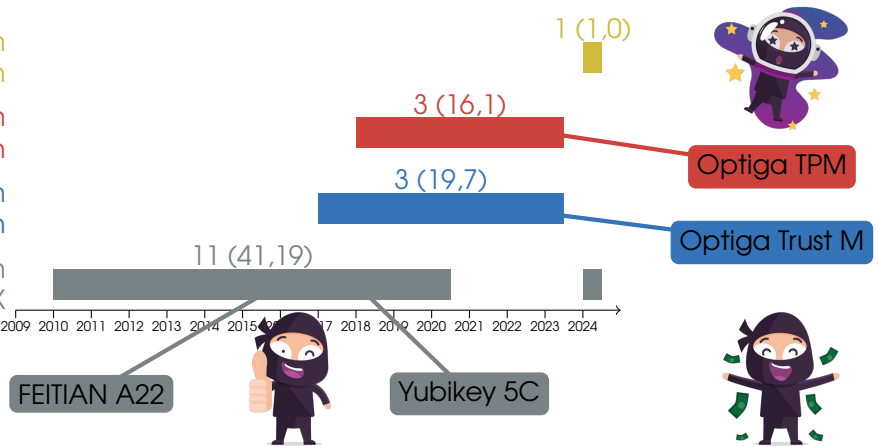
Infineon Security Microcontrollers (IC CC Certifications)



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

Credits: `www.bsi.bund.de`, `www.sec-certs.org`

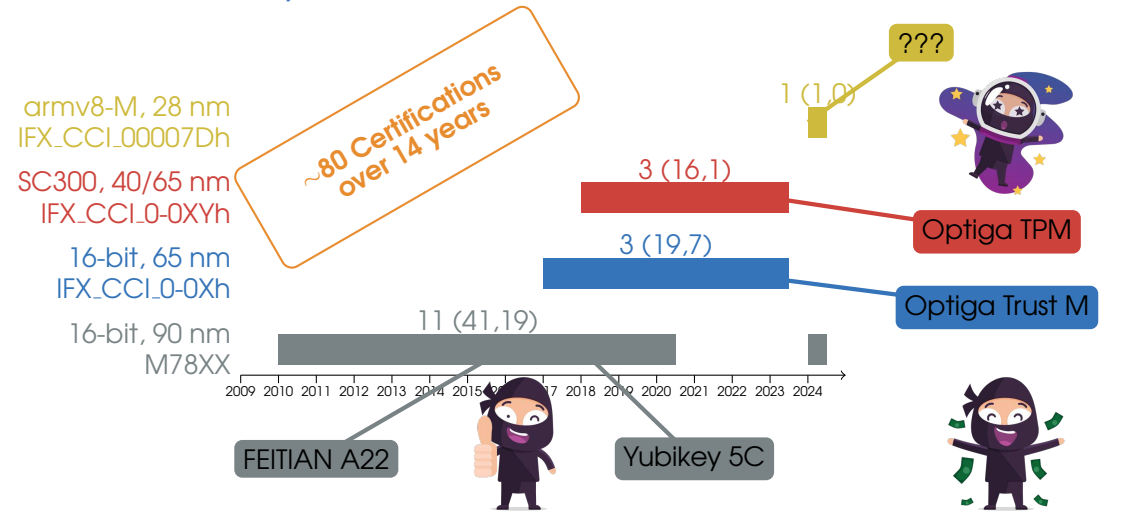
Infineon Security Microcontrollers (IC CC Certifications)



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

Credits: `www.bsi.bund.de`, `www.sec-certs.org`

Infineon Security Microcontrollers (IC CC Certifications)



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

Credits: `www.bsi.bund.de`, `www.sec-certs.org`

Agenda

Introduction
- FIDO Hard
- Yubikey 5 Series

A Side-Channel Lab
- Infineon ECDSA
- The Extended Euclidean Algorithm
- Summary

Impact Analysis
- Infineon Security Microcontrollers

Conclusions
- Summing up
- Mitigations
- Project Timeline

Let's sum up: Attack Requirements

- *Infineon security microcontroller* with *Infineon cryptolib*
- 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.

EUCLEAK

Generate/Store Keys
Key Exch./Wrap.
Signatures

Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

- Bitcoin HW Wallets
- 2FA HW Tokens

- SmartPhones
- Computers (TPMs)

- Smart Cars
- Smart Homes

...

φ Attacker

Side-Channel
Fault Injection
Invasive

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

EUCLEAK

Generate/Store Keys
Key Exch./Wrap.
Signatures

Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

- Bitcoin HW Wallets
- 2FA HW Tokens

- SmartPhones
- Computers (TPMs)

- Smart Cars
- Smart Homes

...

φ Attacker

Side-Channel
Fault Injection
Invasive

Infineon
$\geq$ 14 years

Common Criteria
AVA VAN.5

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

EUCLEAK

Generate/Store Keys
Key Exch./Wrap.
Signatures

Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

- Bitcoin HW Wallets
- 2FA HW Tokens

- SmartPhones
- Computers (TPMs)

- Smart Cars
- Smart Homes

...

φ Attacker

Side-Channel
Fault Injection
Invasive

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

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

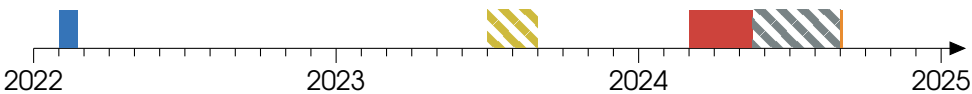
- Defense in Depth

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

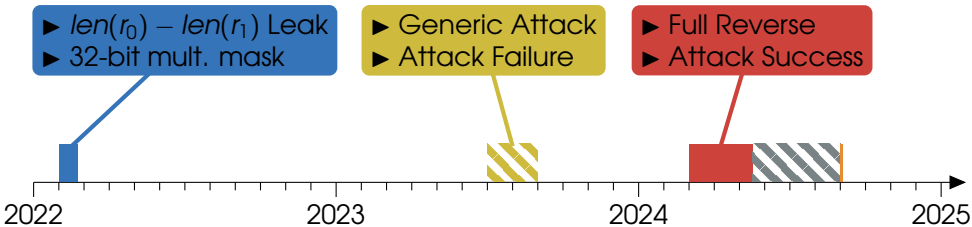
- Protocol Specific Mitigations

eg. Activate Counter in FIDO

Project Timeline

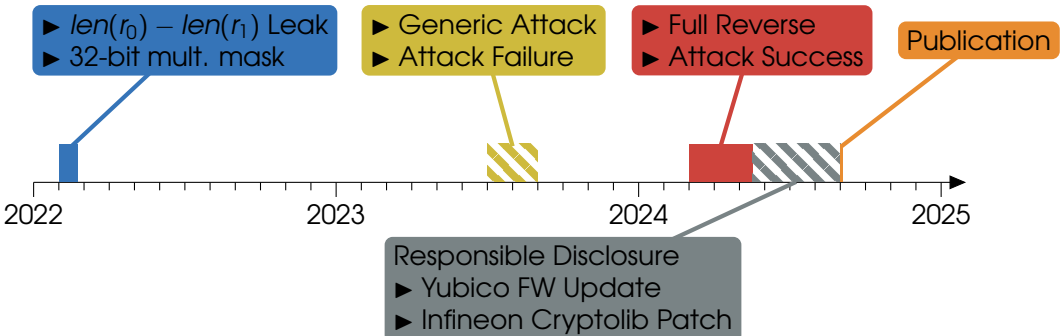


Project Timeline



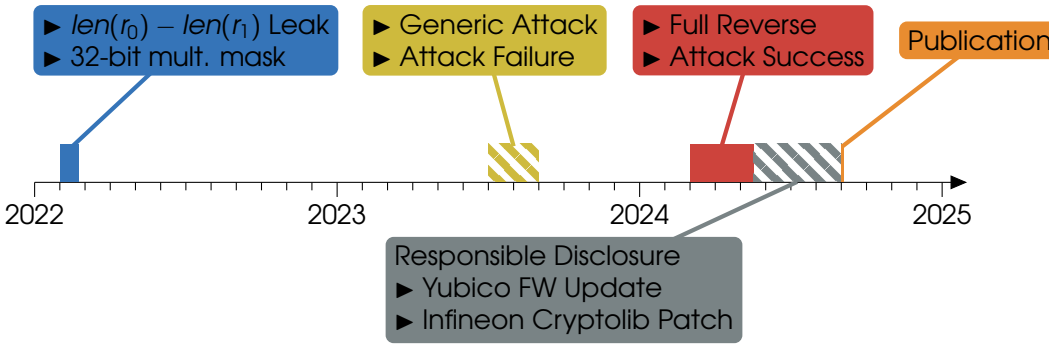
Project Timeline

ninjalab.io/eucleak
eprint.iacr.org/2024/1380
to appear in IEEE S&P 2025



Project Timeline

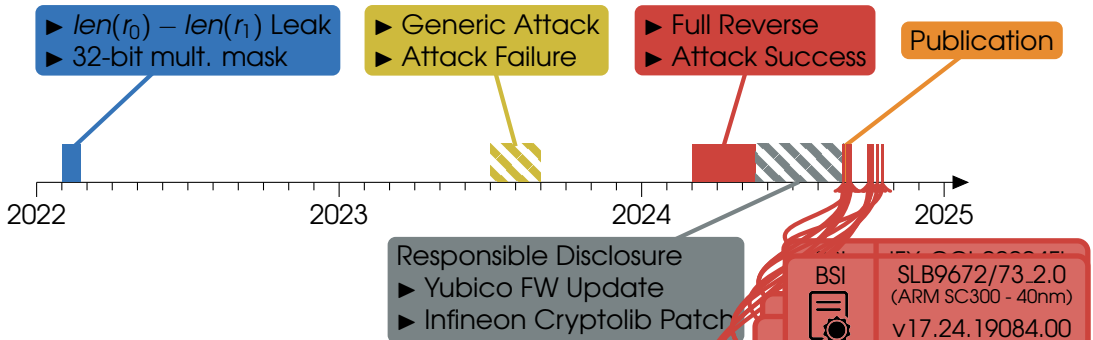
ninjalab.io/eucleak
eprint.iacr.org/2024/1380
to appear in IEEE S&P 2025



- 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
eprint.iacr.org/2024/1380
to appear in IEEE S&P 2025



- 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**

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, v3.02.000, 3.03.003, 3.04.001, v3.33.003, 3.34.000	3.05.002, v3.35.001
armv8-M, 28 nm	04.05.007,4.06.002	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