

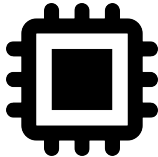


Illustration: Thomas Roche - NinjaLab / PHISIC 2025

Thomas Roche
NinjaLab

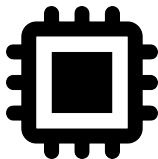
PHISIC 2025
Gardanne, FR – May 20th, 2025

Secure Elements



Secure Elements

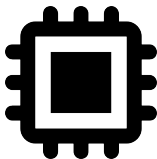
Generate/Store Keys
Key Exch./Wrap.
Signatures



Secure Elements

Generate/Store Keys
Key Exch./Wrap.
Signatures

Remote Attacker

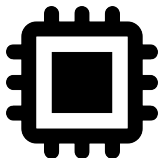


Secure Elements

Generate/Store Keys
Key Exch./Wrap.
Signatures



Remote Attacker



Simple HW
Simple SW
Simple I/O
Formal Methods

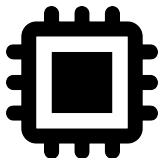
Secure Elements

Generate/Store Keys
Key Exch./Wrap.
Signatures



Remote Attacker

φ Attacker



Simple HW
Simple SW
Simple I/O
Formal Methods

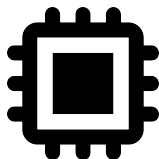
Secure Elements

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

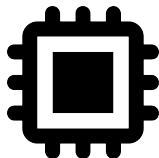
Secure Elements

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

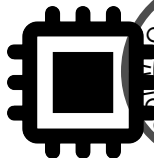
Secure Elements

Generate/Store Keys
Key Exch./Wrap.
Signatures



Remote Attacker

φ Attacker



Side-Channel
Fault Injection
Invasive

Simple HW
Simple SW
Simple I/O
Formal Methods

HW CMs
SW/Crypto CMs

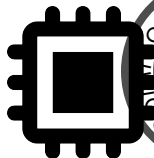
Secure Elements

Generate/Store Keys
Key Exch./Wrap.
Signatures



Remote Attacker

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



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

- Sovereign Documents
- Access Control
- Bank Cards

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

- Sovereign Documents
- Access Control
- Bank Cards
- Bitcoin HW Wallets
- 2FA HW Tokens

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

- Sovereign Documents
- Access Control
- Bank Cards
- Bitcoin HW Wallets
- 2FA HW Tokens
- 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

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

...

Generate/Store Keys
Key Exch./Wrap.

Signatures



Remote Attacker

NXP

infineon

ST

SAMSUNG



- 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

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

A Key-Recovery Attack

- In a Perfect World
- A Generic Attack

Full Reverse-Engineering of Infineon EEA

- Heuristical Approaches
- Summary of The Sensitive Leakage
- Full Nonce Recovery

Yubikey 5C

- Aquisition Setup
- First Side-Channel Traces
- Attack in Practice

Impact Analysis

- Infineon Security Microcontrollers
- Optiga Trust M
- Optiga TPM

Conclusions

- Summing up
- Mitigations
- Avenues Of Research
- 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

A Key-Recovery Attack

- In a Perfect World
- A Generic Attack



Conclusions

- Summing up
- Mitigations
- Avenues Of Research
- Project Timeline

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.

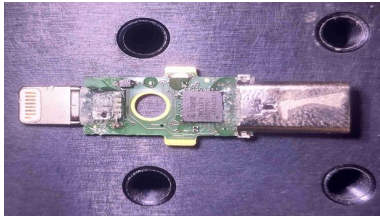
A Side Journey To Titan

- ▶ 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.

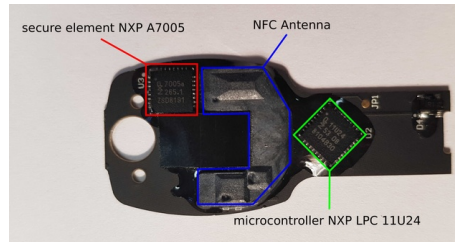


Infineon SLE 78

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.**¹



Yubikey 5Ci (SLE 78)



Google Titan Key (NXP A7005)

¹<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 header includes the company name, contact information (+44 (0)1428 688 250), and navigation links (Home, Shop, Blog, Resources, About us, Contact us). The left sidebar contains a 'Products' menu with categories like Cards, Tags and tokens, Starters/development kits, Readers, Software, and Accessories. Below this is an 'Applications' section with links to Login/authentication, NHS/Healthcare, Digital tachographs, NFC, RFID/NFC app integration, Door access control, and Mobile phone SIM. A 'Manufacturers' section lists ACS, BasicCard, Gemalto, Dot Origin, EasyTac, Elatec, and Feitian.

The main content area features the product 'JavaCOS A22 dual interface Java card - 150K'. It includes a small image of the card, a 'Buy' button, and a price table. The price is listed as £ 6.29 per unit, with a note that the price includes VAT (£ 7.55 inc VAT). A table shows the price per unit for different quantities: 10+, 100+, and 250+.

Units	Per Unit
10+	£ 6.29
100+	£ 5.91
250+	£ 5.60

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

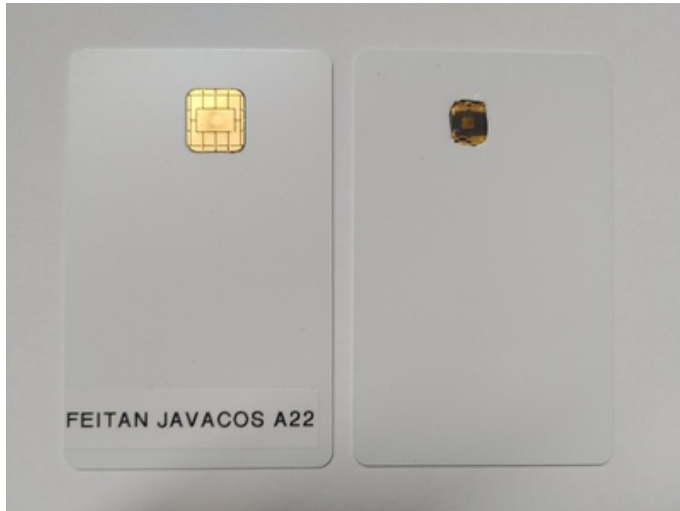
Below the price table, there is a 'Description' section with two paragraphs. The first paragraph states: 'The JavaCOS dual interface card from Feitian is a FLASH-based Java Card with 150K of usable non-volatile storage, and 2.7K of user RAM. This card is designed for both contact and contactless functionality, supporting T=0 over ISO7816 and T=CL over ISO14443 A/B.' The second paragraph states: '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.' There is also a 'Downloads' section with a link to 'Supplied as plain white cards.'

Figure: FEITIAN A22 – Screenshot from SmartCard Focus

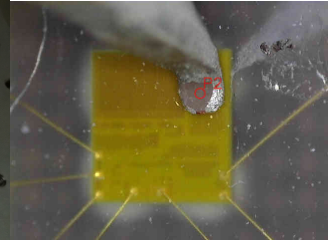
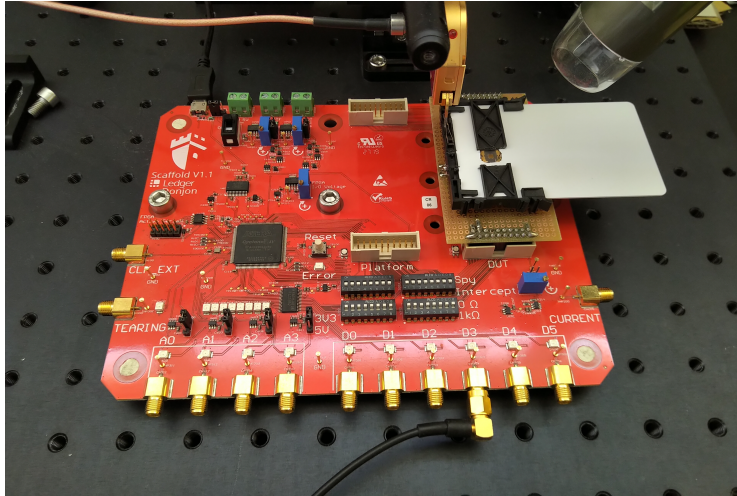
- ▶ Develop and push our own JavaCard applet
↳ ECDSA Signature & Verification
- ▶ certified EAL5+ under Common Criteria in 2018²
- ▶ Infineon asymmetric crypto lib version 1.02.013

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

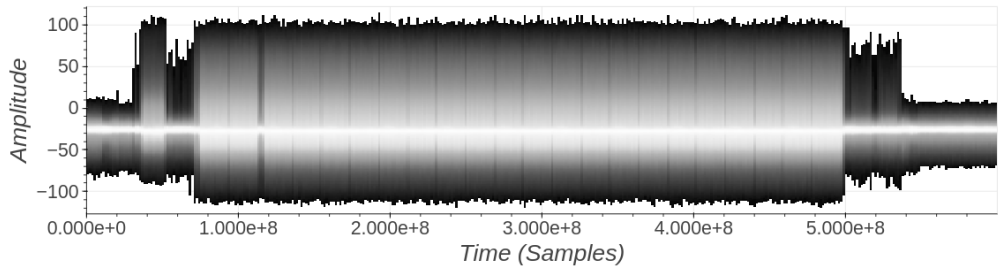
FEITIAN A22 Open JavaCard



FEITIAN A22 – EM Acquisitions



FEITIAN A22 – ECDSA Command – EM Radiations



ECDSA Signature Scheme

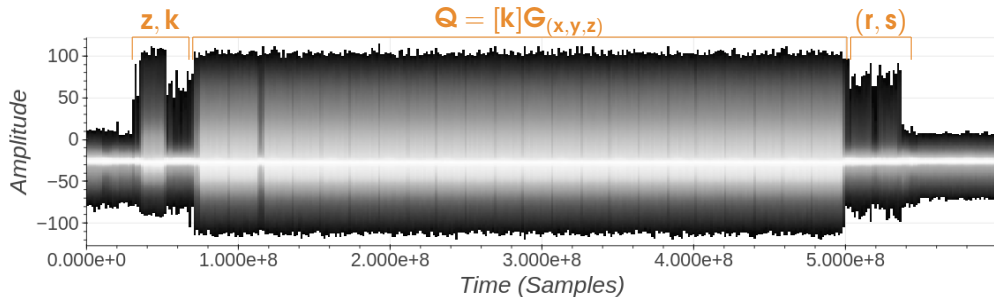
- ▶ Elliptic Curve E over \mathbb{F}_p (base point $G_{(x,y)}$, order is N)
- ▶ Inputs: **secret key** d , the input message to sign $h = H(m)$
- ▶ randomly **generate a nonce** k in $\mathbb{Z}/N\mathbb{Z}$
- ▶ compute $Q_{(x,y)} = [k]G_{(x,y)}$
- ▶ denote by r the x-coordinate of Q : $r = Q_x$
- ▶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

ECDSA Signature Scheme

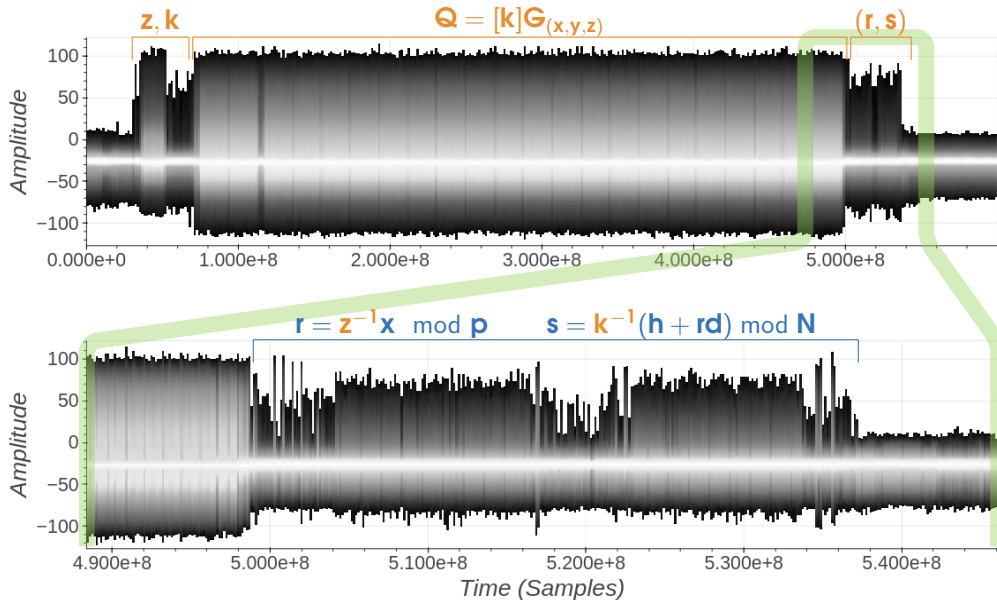
- ▶ Elliptic Curve E over \mathbb{F}_p (base point $G_{(x,y)}$, order is N)
- ▶ Inputs: **secret key** d , the input message to sign $h = H(m)$
- ▶ randomly **generate a nonce** k in $\mathbb{Z}/N\mathbb{Z}$
- ▶ compute $Q_{(x,y)} = [k]G_{(x,y)}$ —

- 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)

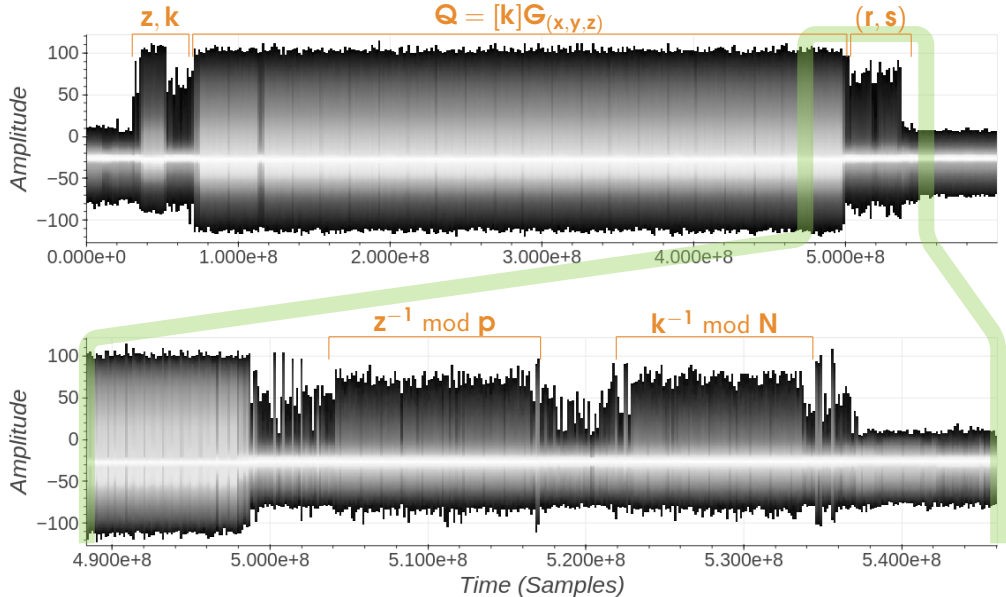
FEITIAN A22 – ECDSA Command – EM Radiations



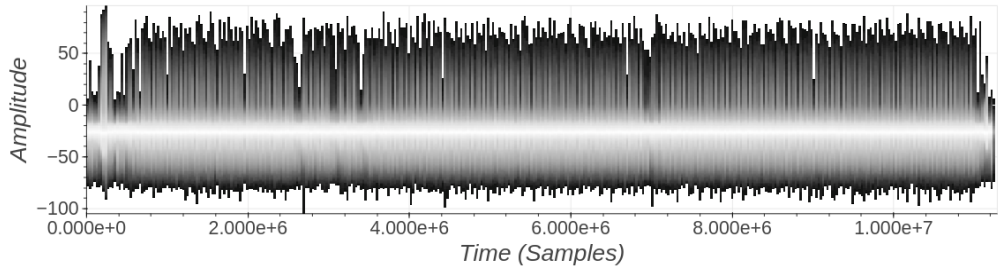
FEITIAN A22 – ECDSA Command – EM Radiations



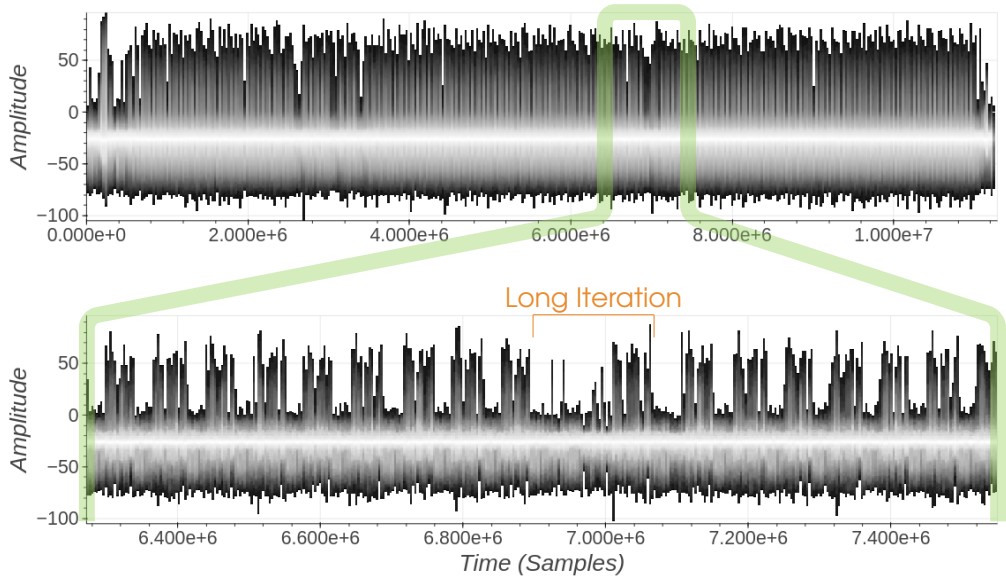
FEITIAN A22 – ECDSA Command – EM Radiations



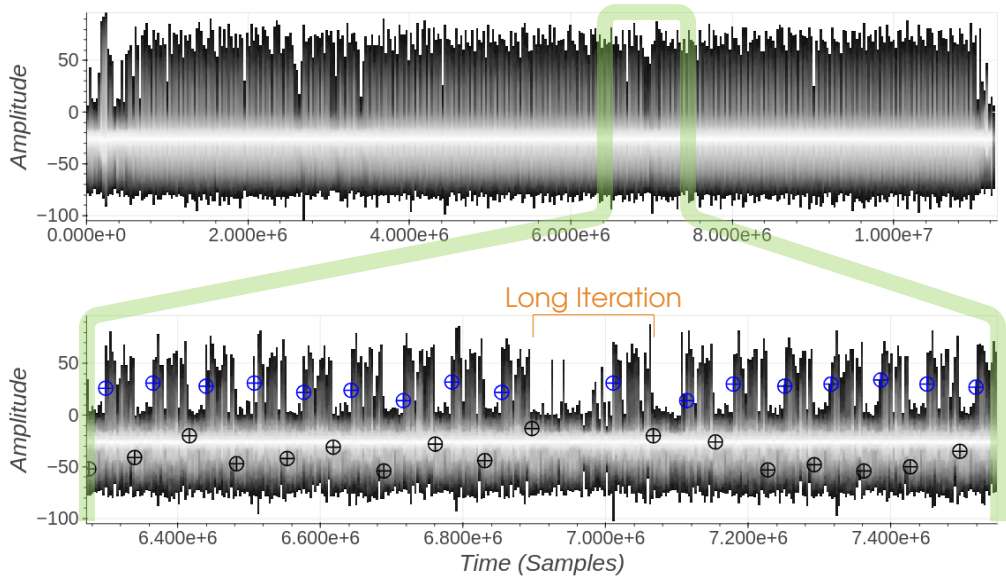
FEITIAN A22 – $k^{-1} \bmod N$ – EM Radiations



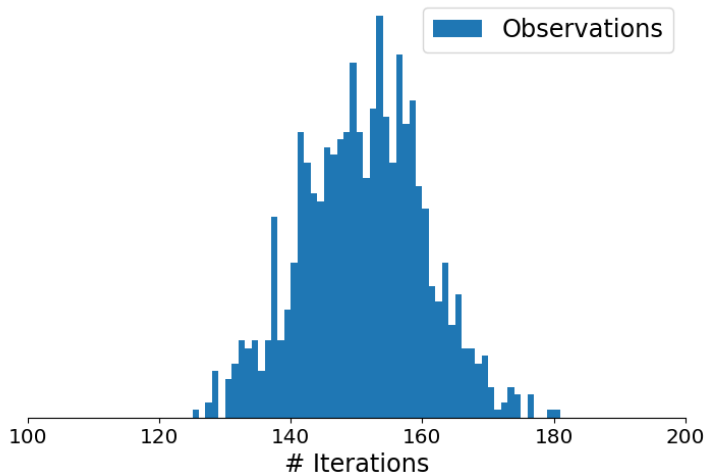
FEITIAN A22 – $k^{-1} \bmod N$ – EM Radiations



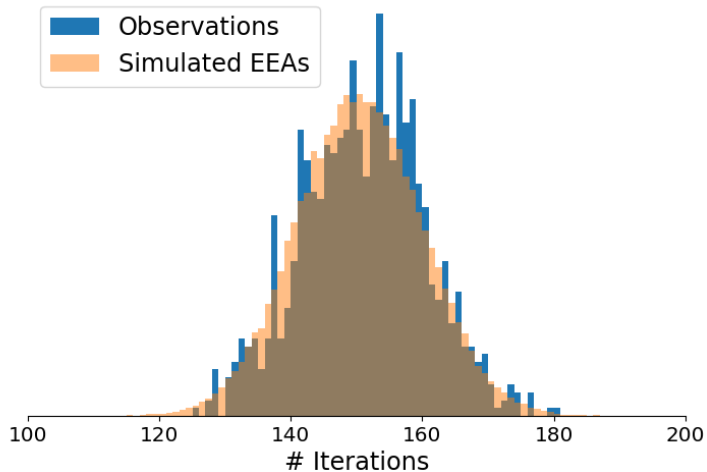
FEITIAN A22 – $k^{-1} \bmod N$ – EM Radiations



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

A Key-Recovery Attack

- In a Perfect World
- A Generic Attack



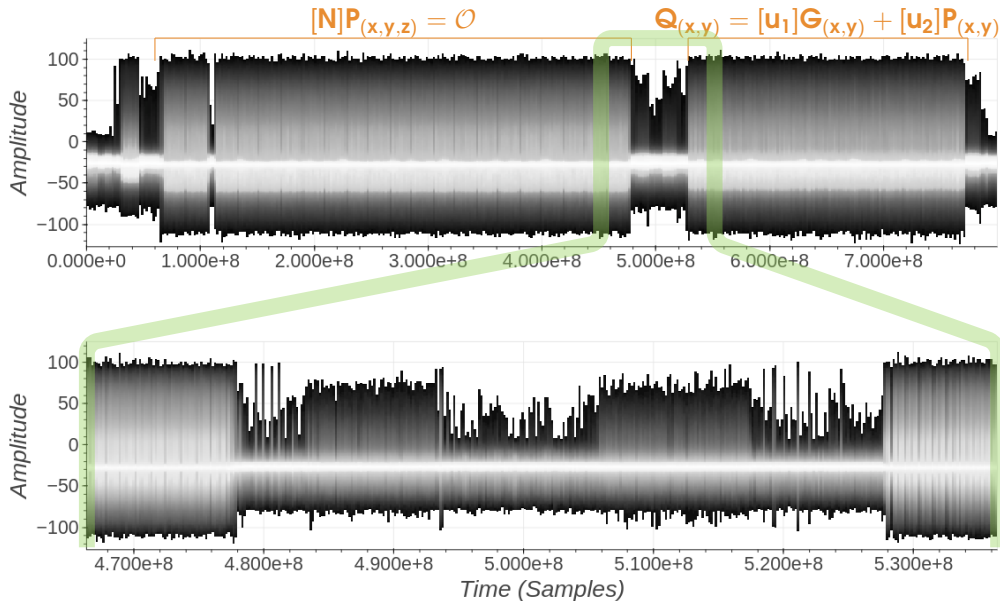
Conclusions

- Summing up
- Mitigations
- Avenues Of Research
- Project Timeline

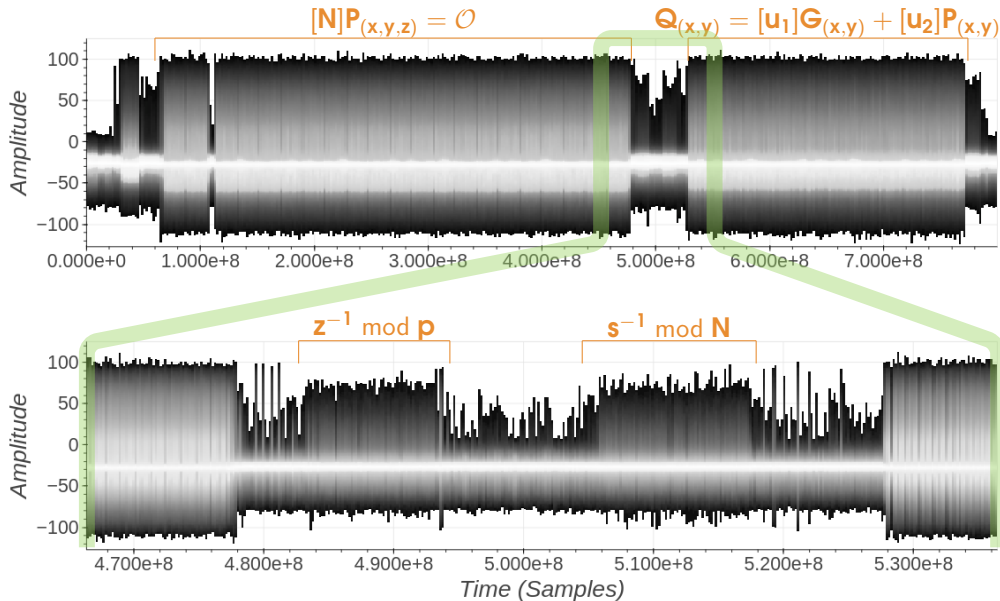
ECDSA Signature Verification Scheme

- ▶ 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 $r = Q_x \bmod N$

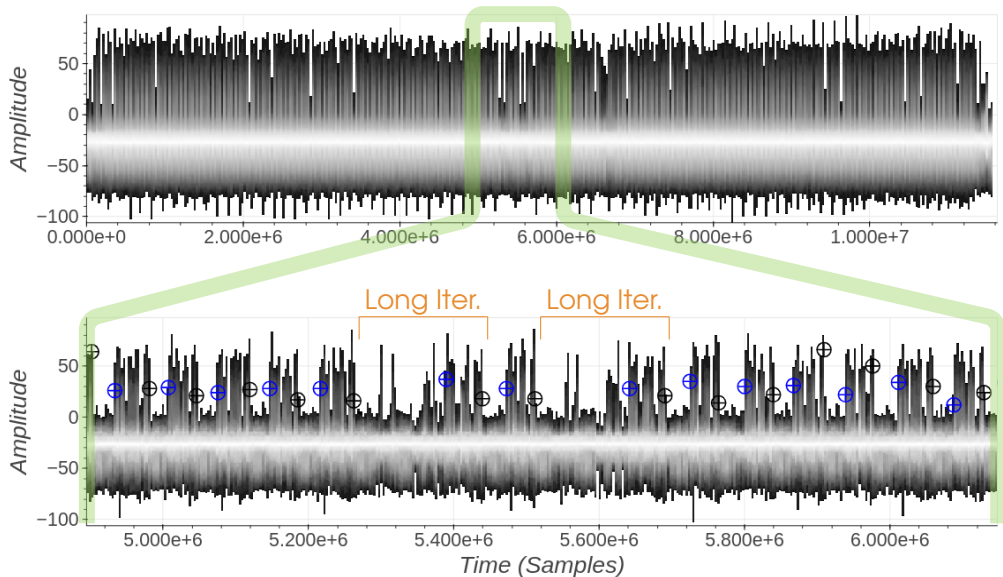
FEITIAN A22 – ECDSA Verif Command – EM Radiations



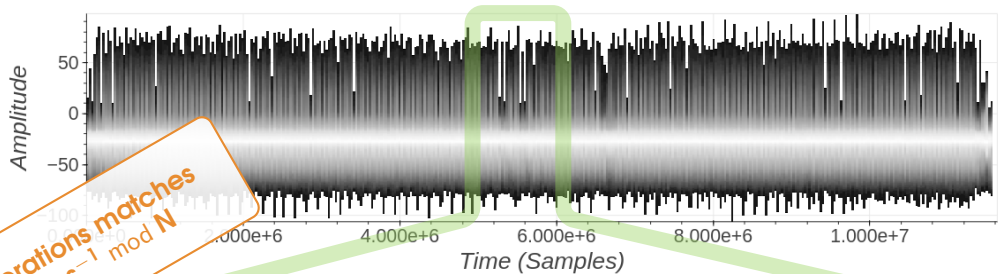
FEITIAN A22 – ECDSA Verif Command – EM Radiations



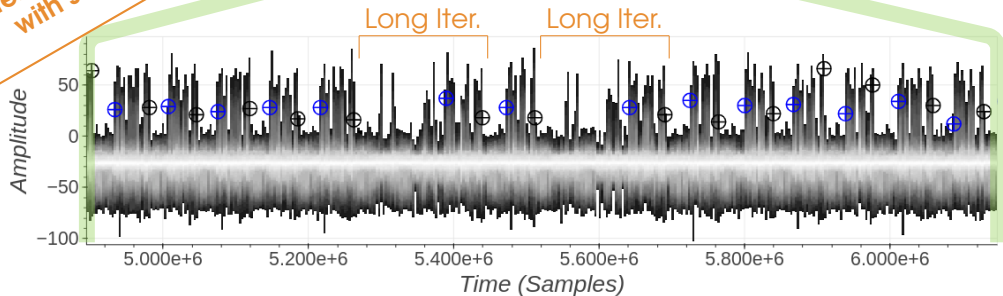
FEITIAN A22 – $s^{-1} \bmod N$ – EM Radiations



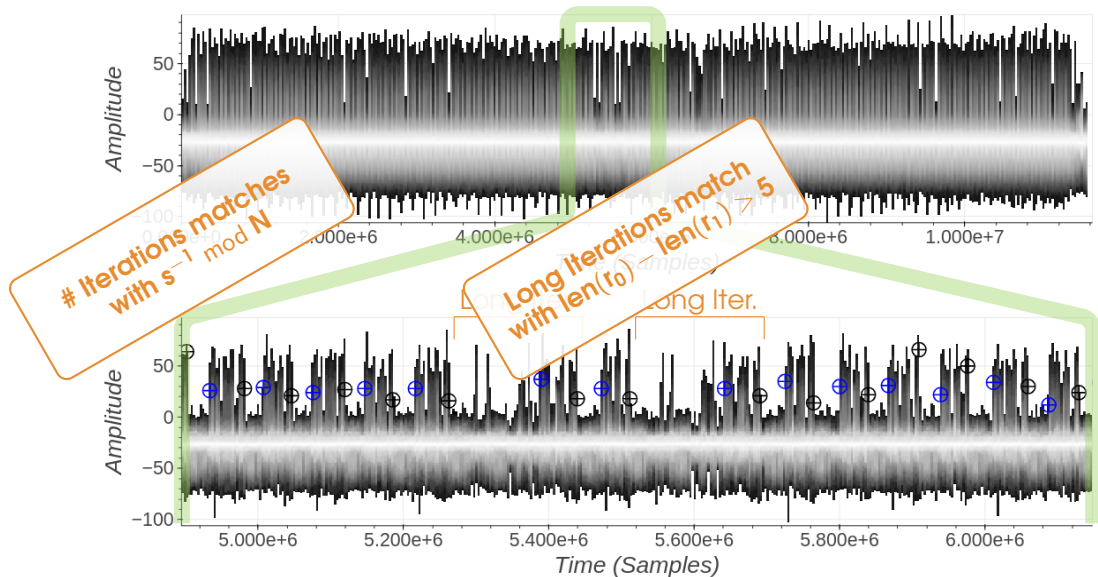
FEITIAN A22 – $s^{-1} \bmod N$ – EM Radiations



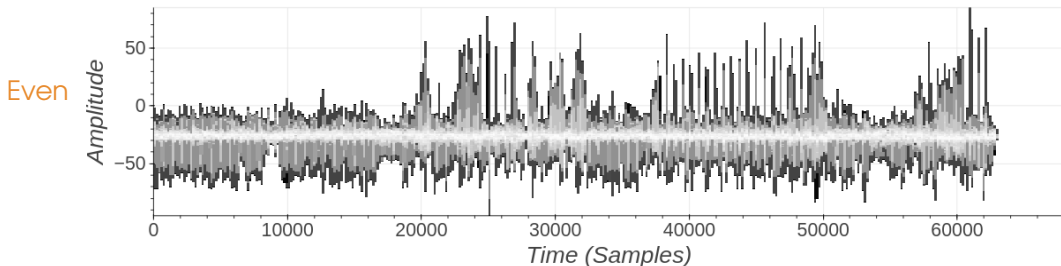
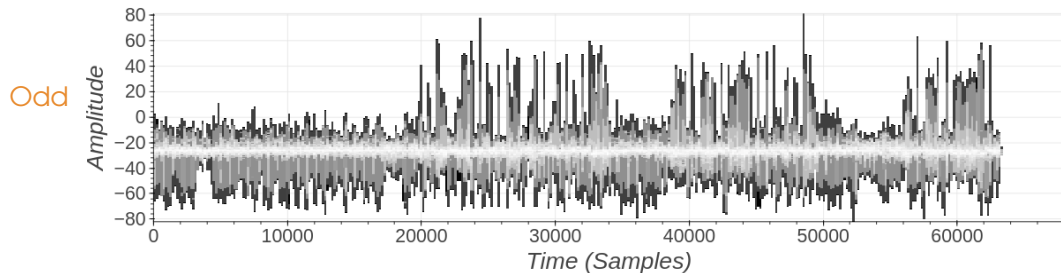
Iterations matches
with $s^{-1} \bmod N$



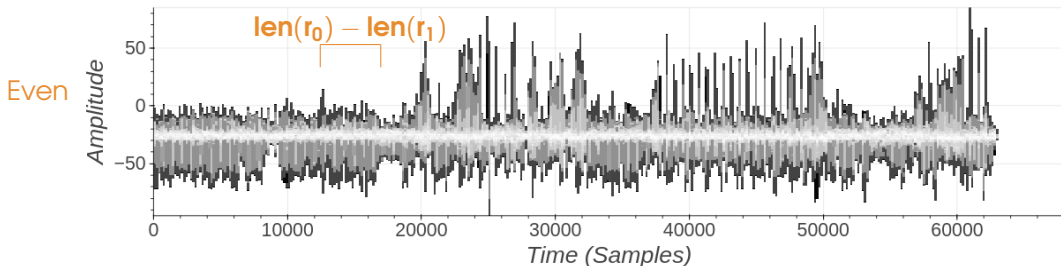
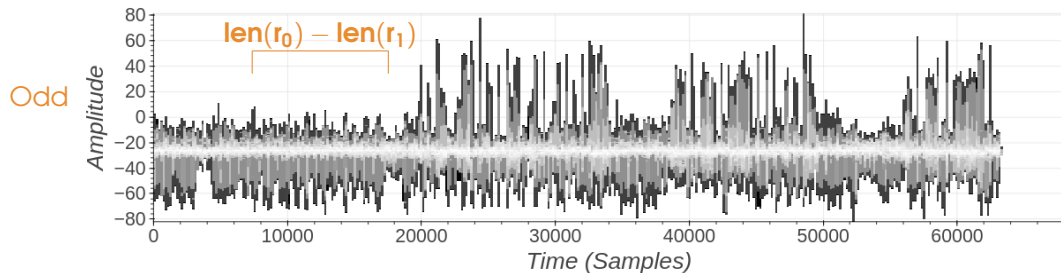
FEITIAN A22 – $s^{-1} \bmod N$ – EM Radiations



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



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

$$\begin{aligned} m &\stackrel{\$}{\leftarrow} \mathbb{Z}/N\mathbb{Z}^* \\ k' &= k \times m \bmod N \\ k'^{-1} &= \text{EEA}(k', N) \\ k^{-1} &= k'^{-1} \times m \bmod N \end{aligned}$$

A Masked Modular Inversion

$$\begin{aligned} m &\stackrel{\$}{\leftarrow} \mathbb{Z}/2^{32}\mathbb{Z}^* \\ k' &= k \times m \bmod N \\ k'^{-1} &= \text{EEA}(k', N) \\ k^{-1} &= k'^{-1} \times m \bmod N \end{aligned}$$

- Hypothesis: the mask can be brute-forced
(otherwise there is no reason to continue the investigation)

A Masked Modular Inversion

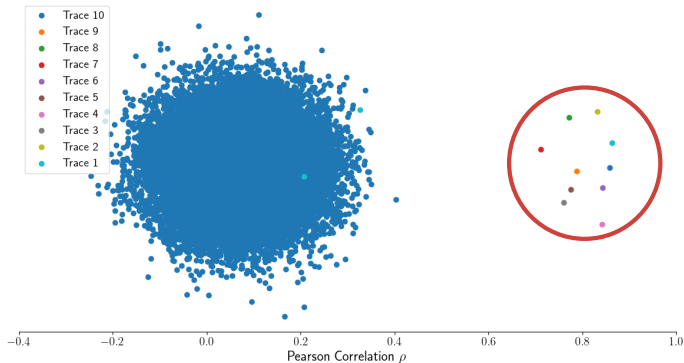
$$\begin{aligned} m &\stackrel{\$}{\leftarrow} \mathbb{Z}/2^{32}\mathbb{Z}^* \\ k' &= k \times m \bmod N \\ k'^{-1} &= \text{EEA}(k', N) \\ k^{-1} &= k'^{-1} \times m \bmod N \end{aligned}$$

- ▶ 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 leakages in ECDSA's nonce modular inversion.

Extended Euclidean Algorithm

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

blinded nonce \rightarrow nonce \rightarrow private key

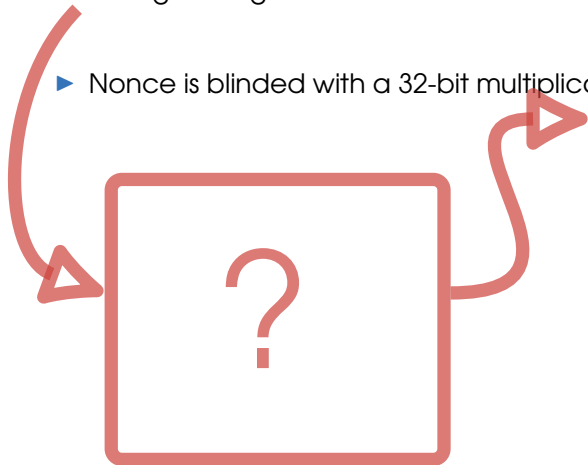
Let's sum up

- ▶ Timing leakages in ECDSA's nonce modular inversion.

Extended Euclidean Algorithm

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

blinded nonce \rightarrow nonce \rightarrow private key



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

A Key-Recovery Attack

- In a Perfect World
- A Generic Attack

- Full Reverse-Engineering of Infineon EEA
- Heuristics for Key-Recovery
- Summary of Key-Recovery
- Key-Recovery
- Prerequisites
- First Side-Channel Attack in EEA
- Impact
- Infineon Security Controllers
- Optiga Trust
- Optiga TPM
- Conclusions
- Summing up
- Mitigations
- Avenues Of Research
- Project Timeline



Simple Attack

From the observation of

$$k'^{-1} = EEA(k', N)$$

Get the leaked information for each iteration:

$$\{\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_n\}$$

Deduce the list of successive quotients:

$$\{q_1, q_2, \dots, q_n\}$$

And we are done:

$$\begin{pmatrix} N \\ k' \end{pmatrix} = \prod_{i=1}^n \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Simple Attack

From the observation of

$$k'^{-1} = EEA(k', N)$$

Get the leaked information for each iteration:

$$\{\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_n\}$$

Deduce the list of successive quotients:

$$\{q_1, q_2, \dots, q_n\}$$

And we are done:

$$\begin{pmatrix} N \\ k' \end{pmatrix} = \prod_{i=1}^n \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Simple Attack

From the observation of

$$k'^{-1} = EEA(k', N)$$

Get the leaked information for each iteration:

$$\{\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_n\}$$

Deduce the list of successive quotients:

$$\{q_1, q_2, \dots, q_n\}$$



And we are done:

$$\begin{pmatrix} N \\ k' \end{pmatrix} = \prod_{i=1}^n \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

1111111111111111100001111010100111001001000011001

0

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

111111111111111100001111010100111001001000011001

0

110110111100110100111110100011111001101101101110

1

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

111111111111111100001111010100111001001000011001

110110111100110100111110100011111001101101101110



0

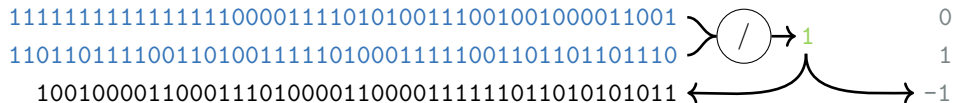
1

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$



A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

111111111111111100001111010100111001001000011001

110110111100110100111110100011111001101101101110

100100001100011101000011000011111101101010101011



0

1

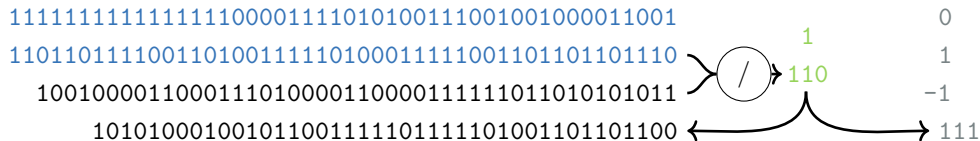
-1

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$



A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

111111111111111100001111010100111001001000011001

110110111100110100111110100011111001101101101110

100100001100011101000011000011111101101010101011

101010001001011001111101111101001101101100

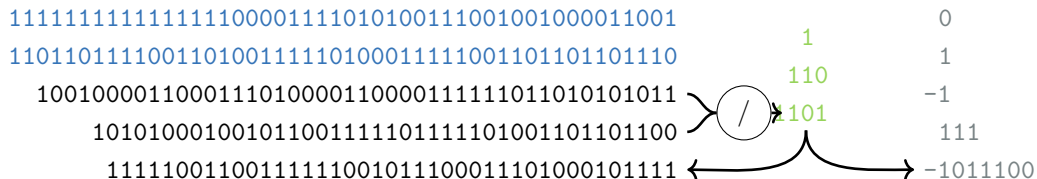
 1 110 101 0 1 -1 111

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$



A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

111111111111111100001111010100111001001000011001

110110111100110100111110100011111001101101101110

100100001100011101000011000011111101101010101011

101010001001011001111101111101001101101100

11111001100111111001011100011101000101111



0

1

-1

111

-1011100

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
 1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        101011100011010110010011001100100111101
```

```

  1      0
110     1
1101    -1
  1     111
      -1011100
        1100011
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
  1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100111101
```

```

  1      0
110     1
1101    -1
      111
      1    -1011100
      10   1100011
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
  1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100111101
          1001010100001001100110110000011110110101
```

```

  1      0
 10     1
110    -1
1101   111
  1    -1011100
 10    1100011
      -100100010
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
 1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100111101
          1001010100001001100110110000011110110101
```

```

  1      0
110     1
1101    -1
      111
      1    -1011100
      10   1100011
      1   -100100010
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
 1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100111101
          1001010100001001100110110000011110110101
            1101000010001001011101001000110001000
```

```

  1      0
 10     1
110    -1
1101   111
  1   -1011100
 10   1100011
  1  -100100010
      110000101
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
  1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100111101
          1001010100001001100110110000011110110101
            1101000010001001011101001000110001000
```

```

  1      0
 10     1
110    -1
1101   111
  1   -1011100
 10   1100011
  1   -100100010
101   110000101
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
 1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100111101
          1001010100001001100110110000011110110101
            1101000010001001011101001000110001000
              1001010110011101100100011000000001101
```

```

  1      0
110     1
1101    -1
      111
      1
      -1011100
      1100011
      1
      -100100010
      110000101
      101    -100010111011
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
 1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100111101
          1001010100001001100110110000011110110101
            1101000010001001011101001000110001000
              1001010110011101100100011000000001101
```

q	
	0
1	1
110	-1
1101	111
1	-1011100
10	1100011
1	-100100010
101	110000101
1	-100010111011

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
 1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100100111101
          1001010100001001100110110000011110110101
            1101000010001001011101001000110001000
              1001010110011101100100011000000001101
                11101011101011111000110000101111011
```

```

0
1
-1
111
-1011100
1100011
-100100010
110000101
-100010111011
101001000000
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
 1001000011000111010000110000111111011010101011
    101010001001011001111101111101001101101100
      11111001100111111001011100011101000101111
        1010111100011010110010011001100100111101
          1001010100001001100110110000011110110101
            1101000010001001011101001000110001000
              1001010110011101100100011000000001101
                11101011101011111000110000101111011
```

```

  1      0
110     1
1101    -1
      111
      1
      -1011100
      1100011
      1
      -100100010
      110000101
      1
      -100010111011
      10
      101001000000
```

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
1111111111111100001111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011		101001000000
1111111000101110010110110100010111		-1110100111011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
1111111111111100001111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
1111111000101110010110110100010111		-1110100111011

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

```

1111111111111111100001111010100111001001000011001
11011011110011010011111010001111001101101101110
1001000011000111010000110000111111011010101011
1010100010001011001111101111101001101101100
111110011001111110010111000011101000101111
10101111000011010110010011001100100111101
1001010100001001100110110000011110110101
1101000010001001011101001000110001000
1001010110011101100100011000000001101
1110101110101111000110000101111011
11111110000101110010110110100001011
1101100100110000101111010001100100

```

```

      0
      1
110  -1
1101 111
      1
10  -1011100
      1
101 1100011
      1
10  -100100010
      1
101 110000101
      1
10  -100010111011
      1
101 101001000000
      1
10  -1110100111011
      1
101 10011101111011

```

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

```

1111111111111111100001111010100111001001000011001
11011011110011010011111010001111001101101101110
1001000011000111010000110000111111011010101011
101010001001011001111101111101001101101100
11111001100111111001011100001101000010111
1010111100011010110010011001100100111101
1001010100001001100110110000011110110101
1101000010001001011101001000110001000
1001010110011101100100011000000001101
1110101110101111000110000101111011
11111110000101110010110110100001011
110110010011000010111100001100101

```

```

      0
      1
110   -1
1101  111
      1
      10  -1011100
      1    1100011
101     -100100010
      1    110000101
10     -100010111011
      1    101001000000
      1   -1110100111011
      1    1001101110111

```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
1111111111111111100001111010100111001001000011001
110110111100110100111110100011111001101101101110
1001000011000111010000110000111111011010101011
101010001001011001111101111101001101101100
11111001100111111001011100011101000101111
1010111100011010110010011001100100100111101
1001010100001001100110110000011110110101
1101000010001001011101001000110001000
1001010110011101100100011000000001101
111010111010111110001100001011111011
1111111000101110010110110100010111
1101100100110000101111010001100100
10010011111101100111100010110011
```

```
0
1
110
-1
111
-1011100
1100011
-100100010
110000101
-100010111011
101001000000
-1110100111011
10011101111011
-100010010110110
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

```

111111111111111100001111010100111001001000011001
11011011110011010011111010001111001101101101110
100100001100011101000011000011111101101010101
101010001001101101111101111010011010101100
11111001100111111001011100011101000101111
1010111100011010110010011001100100111101
1001010100001001100110110000011110110101
1101000010001001011101001000110001000
1001010110011101100100011000000001101
11101011101011111000110000101111011
1111111000101110010110110100001011
11011001001100001011111010001100100
1001001111110110100111100010110011

```

```

      0
1      1
110    -1
1101   111
      1  -1011100
10     1100011
      1  -100100010
101    110000101
      1  -100010111011
10     101001000000
      1  -1110100111011
      1  10011101111011
101    -100010010110110

```


A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
11111111111111110000111010100111001001000011001
1101101111001101001111010001111001101101101110
100100001100011101000011000011111011010101011
101010001001011001111101111101001101101100
11111001100111111001011100011101000101111
1010111100011010110010011001100100111101
1001010100001001100110110000011110110101
1101000010001001011101001000110001000
1001010110011101100100011000000001101
11101011101011111000110000101111011
111111100010111001011011010001011
1101100100110000101111010001100100
10010011111101100111100010110011
10000000111100101001100011100101
```

```
0
1
-1
111
-1011100
1100011
-100100010
110000101
-100010111011
101001000000
-1110100111011
10011101111011
-100010010110110
10111111100001001
```

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$
[illegible]

```

      0
      1
110   -1
1101  11
      1
      10  -1011100
      1    1100011
101     -100100010
      1    110000101
      10  -100010111011
      1    101001000000
      1   -1110100111011
      1    10011101111011
101     -100010010110110
      1    1011111100001001

```

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

```

1111111111111111100001111010100111001001000011001
11011011110011010011111010001111001101101101110
100100001100011101000011000011111101101010101
1010100010010110011111011111011001101101100
1111100110011111100111100011101000101111
1010111100011010110010011001100100111101
1001010100001001100110110000011110110101
11010000100010010111101001000110001000
100101011001110110010001100000001101
1110101110101111000110000101111011
111111100010111001011011010001011
1101100100110000101111010001100100
1001001111101100111100010110011
100000001111001010011000111100101
1001100000011101111111111100111

```

```

      0
      1
110  -1
1101 111
      1
      -1011100
10    1100011
      1
      -100100010
101   110000101
      1
      -100010111011
10    101001000000
      1
      -1110100111011
      1
      10011101111011
101   -100010010110110
      1
      1011111100001001
      -1100001110111111

```

A Generic Attack

$$R_0 = N, R_1 = k'$$

 q

$$U_0 = 0, U_1 = 1$$

```
111111111111111100001111010100111001001000011001
11011011110011010011111010001111001101101101110
 100100001100011101000011000011111011010101011
   101010001001011001111101111101001101101100
    11111001100111111001011100011101000101111
     1010111100011010110010011001100100111101
      1001010100001001100110110000011110110101
       1101000010001001011101001000110001000
        1001010110011101100100011000000001101
         11101011101011111000110000101111011
          1111111000101110010110110100010111
           1101100100110000101111010001100100
            1001001111101100111100010110011
             10000000111100101001100011100101
              10011000000111101111111001110
```

```

  1      0
 10      1
110     -1
1101    111
  1    -1011100
 10    1100011
  1    -100100010
101    110000101
  1    -100010111011
 10    101001000000
  1    -1110100111011
  1    10011101111011
101    -100010010110110
  1    10111111100001001
110    -11100001110111111
```

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
1111111111111100001111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110		-11100001110111111
1110110110110101101000010001		11000001010110000011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
1111111111111100001111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110101101000010001		11000001010110000011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
1111111111111100001111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
111011011011010101101000010001		11000001010110000011
100001010001000010110111101		-11011101100101000010

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
1111111111111100001111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
111011011011010101101000010001	11	11000001010110000011
100001010001000010110111101		-11011101100101000010

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
1001001111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
111011011011010101101000010001	11	11000001010110000011
100001010001000010110111101		-11011101100101000010
10011000011100100011011010		1101011010000101001001

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
111011011011010101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010		1101011010000101001001

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
10010011111101100111100010110011	101	-100010010110110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
111011011011010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
1001100001110010001101101010	1	1101011010000101001001
1110001101011110011100011		-10000110111101010001011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
1111111111111100001111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
10010011111101100111100010110011	101	-100010010110110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
111011011011010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
1001100001110010001101101010	1	1101011010000101001001
1110001101011110011100011	1	-10000110111101010001011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
1001001111101100111100010110011	101	-10001001010110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
111011011011010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
1110001101011110011100011	1	-10000110111101010001011
100110110000101111110111		11110010001101111010100

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
10010011111101100111100010110011	101	-10001001010110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
111011011011010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
1110001101011110011100011	1	-100001101111010100001011
100110110000101111110111	10	11110010001101111010100

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
10010011111101100111100010110011	101	-100010010110110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
11101101101101010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	1	-10000110111101010001011
100110110000101111110111	10	11110010001101111010100
100100001010010011110101		-1001101011011001000110011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
10010011111101100111100010110011	101	-100010010110110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
11101101101101010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	1	-10000110111101010001011
100110110000101111110111	10	11110010001101111010100
100100001010010011110101	1	-1001101011011001000110011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
1101101111001101001111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
1001001111101100111100010110011	101	-10001001010110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
11101101101101010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
1001100001110010001101101010	1	1101011010000101001001
11100011010111100011100011	1	-10000110111101010001011
100110110000101111110111	10	11110010001101111010100
100100001010010011110101	1	-1001101011011001000110011
10100110011100000010		1101011101100111000000111

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
10010011111101100111100010110011	101	-10001001010110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
111011011011010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	1	-10000110111101010001011
100110110000101111110111	10	11110010001101111010100
100100001010010011110101	1	-1001101011011001000110011
10100110011100000010	1101	1101011101100111000000111

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
111011011011010101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
1110001101011110011100011	10	-10000110111101010001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000100011
10100110011100000010		1101011101100111000000111
10010110100111011011		-10111000101100010100010001110

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
111011011011010101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
1110001101011110011100011	10	-100001101111010100001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011		-10111000101100010100010001110

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
111011011011010101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000100011
10100110011100000010	1	1101011101100111000000111
10010110100111011011		-10111000101100010100010001110
1111110100100111		110001100010011111011010010101

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$
[illegible]

1
110
1101
1
10
1
101
1
10
1
1
101
1
110
1
11
1
1
10
1
1101
1
1001

```

0
1
-1
111
-1011100
1100011
-100100010
110000101
-100010111011
101001000000
-1110100111011
10011101111011
-100010010110110
10111111100001001
-11100001110111111
11000001010110000011
-11011101100101000010
1101011010000101001001
-10000110111101010001011
11110010001101111010100
-1001101011011001000110011
1101011101100111000000111
-10111000101100010100010001110
1100011000100111101101001010

```

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111111110000111010100111001001000011001	1	0
110110111100110100111110100011111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
101011110001101011001001100110010010011101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
11011001001100001011111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110110101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-100001101111010100001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111		110001100010011111011010010101
1000001101111100		-11110110000000101101001111001011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110110101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
1110001101011110011100011	10	-10000110111101010001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	110001100010011111011010010101
1000001101111100		-11110110000000101101001111001011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
110110111100110100111110100011111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
11011001001100001011111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110110101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
1001100001110010001101101010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	110001100010011111011010010101
1000001101111100		-11110110000000101101001111001011
111100110101011		100001110110001111100101001100000

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
110110111100110100111110100011111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110110101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	110001100010011111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011		100001110110001111100101001100000
100111010001		-1000000100110010101001111000101011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111111110000111010100111001001000011001	1	0
110110111100110100111110100011111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
11111110001011100101101101010001011	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110110101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
1110001101011110011100011	10	-10000110111101010001011
10011011000010111111011	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	110001100010011111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001		-1000000100110010101001111000101011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-10001001010110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
11101101101101010110101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001		-1000000100110010101001111000101011
1111011111		1100101001000010001110011010001100100

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

111111111111110000111010100111001000011001	0
1101101111001101001111101000111110011011011110	1
1001000011000111010000110000111111011010101011	-1
101010001001011001111101111101001101101100	111
11111001100111111001011100011101000101111	-1011100
1010111100011010110010011001100100111101	1100011
1001010100001001100110110000011110110101	-100100010
1101000010001001011101001000110001000	110000101
1001010110011101100100011000000001101	-100010111011
111010111010111110001100001011111011	101001000000
1111111000101110010110110100001011	-1110100111011
1101100100110000101111010001100100	10011101111011
10010011111101100111100010110011	-100010010110110
10000000111100101001100011100101	10111111100001001
1001100000011101111111001110	-11100001110111111
1110110110110101101000010001	11000001010110000011
100001010001000010110111101	-11011101100101000010
10011000011100100011011010	1101011010000101001001
1110001101011110011100011	-10000110111101010001011
10011011000010111111011	11110010001101111010100
1001000010100100111110101	-1001101011011001000110011
10100110011100000010	110101110110011100000011
10010110100111011011	-10111000101100010100010001110
1111110100100111	11000110001001111011010010101
1000001101111100	-11110110000000101101001111001011
111100110101011	100001110110001111100101001100000
100111010001	-1000000100110010101001111000101011
1111011111	1100101001000010001110011010001100101

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111111110000111010100111001001000011001	1	0
110110111100110100111110100011111001101101101110	110	1
1001000011000111010000110000111111011010101011	1101	-1
101010001001011001111101111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110110101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
1001100001110010001101101010	1	1101011010000101001001
11100011010111100011100011	10	-100001101111010100001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	110001100010011111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111		1100101001000010001110011010001100100
1000010011		-11010010010101010110010000011011110011

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

111111111111111111000011110100111001001000011001	0	
1101101111001101001111110100011111001101101101110	1	
100100001100011101000011000011111101101010101011	-1	
101010001001011001111101111101001101101100	111	
111110011001111111001011100011101000101111	-1011100	
1010111100011010110010011001100100111101	1100011	
1001010100001001100110110000011110110101	-100100010	
11010000100010010111101001000110001000	110000101	
1001010110011101100100011000000001101	-100010111011	
11101011101011111000110000101111011	101001000000	
111111100010111001011011010100010111	-111010011011	
1101100100110000101111010001100100	10011101111011	
10010011111101100111100010110011	-100010010110110	
10000000111100101001100011100101	10111111100001001	
10011000000111101111111001110	-11100001110111111	
1110110110110101101101000010001	11000001010110000011	
100001010001000010110111101	-11011101100101000010	
10011000011100100011011010	1101011010000101001001	
1110001101011110011100011	-100001101111010001011	
100110110000101111110111	11110010001101111010100	
100100001010010011110101	-1001101011011001000110011	
10100110011100000010	1101011101100111000000111	
10010110100111011011	-10111000101100010100010001110	
1111110100100111	11000110001001111011010010101	
1000001101111100	-11110110000000101101001111001011	
111100110101011	10000110110001111100101001100000	
100111010001	-1000000100110010101001111000101011	
1111011111	1100101001000010001110011010001100100	
1000010011	-11010010010101010110010000001011110011	

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
1111100110011111001011100011101000101111	1	-1011100
1010111100011010110010011001100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
11111110001011100101101101010001011	1	-1110100111011
1101100100110000101111010001100100	1	10011101111011
1001001111101100111100010110011	101	-100010010110110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
111011011011010101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	1	-10000110111101010001011
10011011000010111111011	10	11110010001101111010100
100100001010010011110101	1	-1001101011011001000110011
10100110011100000010	1101	1101011101100111000000111
10010110100111011011	1	-10111000101100010100010001110
1111110100100111	1001	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1	100001110110001111100101001100000
100111010001	1100	-1000000100110010101001111000101011
1111011111	10	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100		100110111011101101000000011101101010111

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
11111110001011100101101101010001011	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
1001001111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
11101101101101010110101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-1000011011110101010001011
10011011000010111111011	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111	1	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100	1	100110111011101101000000011101101010111

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
1001001111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
11101101101101010110101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-1000011011110101010001011
10011011000010111111011	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111	1	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100		10011011101110110101000000011101101010111
1000111		-1000001001110010111110010100001001001010

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
111111100010111001011011010100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
1001001111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
11101101101101010110101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
10011011000010111111011	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111	1	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100	110	100110111011101101000000011101101010111
1000111		-1000001001110010111110010100001001001010

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001		0
11011011110011010011111010001111001101101101110	1	1
100100001100011101000011000011111011010101011	110	-1
10101000100101100111110111101001101101100	1101	111
11111001100111111001011100011101000101111	1	-1011100
1010111100011010110010011001100100111101	10	1100011
1001010100001001100110110000011110110101	1	-100100010
1101000010001001011101001000110001000	101	110000101
1001010110011101100100011000000001101	1	-100010111011
111010111010111110001100001011111011	10	101001000000
111111100010111001011011010100010111	1	-110100111011
1101100100110000101111010001100100	1	10011101111011
1001001111101100111100010110011	101	-10001001010110
10000000111100101001100011100101	1	10111111100001001
10011000000111101111111001110	110	-11100001110111111
1110110110110101101101000010001	1	11000001010110000011
100001010001000010110111101	11	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
1110001101011110011100011	1	-10000110111101010001011
10011011000010111111011	10	11110010001101111010100
100100001010010011110101	1	-1001101011011001000110011
10100110011100000010	1101	1101011101100111000000111
10010110100111011011	1	-10111000101100010100010001110
1111110100100111	1001	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1	100001110110001111100101001100000
100111010001	1100	-1000000100110010101001111000101011
1111011111	10	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100	1	10011011101110101000000011101101010111
1000111	110	-1000001001110010111110010100001001010
100010		110101110010001111011101111100100100010011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
1111111000101110010110110100010111	1	-110100111011
1101100100110000101111010001100100	101	10011101111011
1001001111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110101101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
10011011000010111111011	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111	1	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100	110	10011011101110101000000011101101010111
1000111	10	-1000001001110010111110010100001001001010
100010		110101110010001111011101111100100100010011

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
1111111000101110010110110100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
1001001111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110101101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
10011011000010111111011	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111	1	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100	110	1001101110111011010000000011101101010111
1000111	10	-1000001001110010111110010100001001001010
100010		11010111001000111101101111100100100010011
11		-1110011101110010001111010001101010001110000

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
1111111000101110010110110100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
1001001111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110101101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111	1	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100	110	1001101110111011010000000011101101010111
1000111	10	-1000001001110010111110010100001001001010
100010	1011	110101110010001111011101111100100100010011
11		-1110011101110010001111010001101010001110000

A Generic Attack

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
11011011110011010011111010001111001101101101110	110	1
100100001100011101000011000011111011010101011	1101	-1
10101000100101100111110111101001101101100	1	111
11111001100111111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
1111111000101110010110110100010111	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
111011011011010101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
100110110000101111110111	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111	1	1100101001000010001110011010001100100
1000010011	1	-110100100101010101100100000011011110011
111001100	110	1001101110111011010000000011101101010111
1000111	10	-1000001001110010111110010100001001001010
100010	1011	110101110010001111011101111100100100010011
11		-1110011101110010001111010001101010001110000
1		10100101110101111010100011110001110100111100011

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

```

11111111111111110000111010100111001001000011001
1101101111001101001111010001111001101101101110
100100001100011101000011000011111101101010101
10101000100101100111101111010011011011000
11111001100111111001011100011101000101111
1010111100011010110010011001100100111101
1001010100001001100110110000011110110101
110100010001001011101001000110001000
1001010110011101100100011000000001101
111010111010111110001100001011111011
1111111000101110010110110100010111
1101100100110000101111010001100100
10010011111101100111100010110011
1000000011100101001100011100101
10011000000111011111111001110
1110110110110101101000010001
100001010001000010110111101
10011000011100100011011010
1110001101011110011100011
100110110000101111110111
100100001010010011110101
10100110011100000010
10010110100111010111
1111110100100111
1000001101111100
111100110101011
100111010001
111011111
1000010011
111001100
1000111
100010
11

```

[illegible]

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

11111111111111110000	111010100111001001000011001	1	0
11011011110011010011	110100011111001101101101110	110	1
100100001100011101000011000011111011010101011	101	-1	111
10101000100101001111101111101001101101100	1	-1011100	1100011
11111001100111111001011100011101000101111	10	-100100010	110000101
1010111100011010110010011001100100111101	101	-100010111011	101001000000
1001010100001001100110110000011110110101	1	-110100111011	10011101111011
1101000010001001011101001000110001000	10	-10001001010110	1011111100001001
1001010110011101100100011000000001101	1	-1110000111011111	11000001010110000011
111010111010111110001100001011111011	1	-11011101100101000010	1101011010000101001001
1111111000101110010110110100010111	101	-10000110111101010001011	1111001000101111010100
1101100100110000101111010001100100	1	-10011010110010001000110011	1101011101100111000000111
10010011111101100111100010110011	110	-10111000101100010100010001110	11000110001001111011010010101
10000000111100101001100011100101	1	-11110110000000101101001111001011	10000111011000111100101001100000
10011000000111101111111001110	11	-1000000100110010101001111000101011	1100101001000010001110011010001100100
11101101011010110101101000010001	1	1000011101100011110010100001001010	-110100100101010110010000011011110011
100001010001000010110111101	1	1111001000101111010100	10011011101110110101000000011101101010111
10011000011100100011011010	10	1000011011001011110010100001001010	-100000100111001011110010100001001001010
11100011010111100011100011	1	110101100100011110111100100100010011	11010111001000111101111100100100010011
100110110000101111110111	1101	-10111000101100010100010001110	-1110011101110010001111010001110000
100100110100111011011	1	11000110001001111011010010101	1100101001000010001110011010001100100
1111110100100111	1001	-11110110000000101101001111001011	-100000100111001011110010100001001010
1000001101111100	1	1000011101100011110010100010010000	11010111001000111101110111100100100010011
111100110101011	1100	-1000000100110010101001111000101011	1100101001000010001110011010001100100
100111010001	10	11000110010101010110010000011011110011	-11010010010101010110010000011011110011
1111011111	1	10011011101110110101000000011101101010111	100001100111001011110010100001001010
1000010011	1	-100000100111001011110010100001001010	110101110010001111011101111100100100010011
111001100	110	-111001110111001000111101000111010001110000	-1110011101110010001111010001101010001110000
1000111	10	1010011001000111101110111100100100010011	1010011001000111101110111100100100010011
100010	1011	-1110011101110010001111010001101010001110000	1010011001000111101110111100100100010011
11			
1			

A Generic Attack

(Jebelean95)

$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111110000111010100111001001000011001	1	0
1101101111001101001111010001111101101101110	110	1
10010000110001110100001100001111110110101011	101	-1
10101000100101001111110111101001101101100	1	111
1111100110011111001011100011101000101111	10	-1011100
1010111100011010110010011001100100111101	1	1100011
1001010100001001100110110000011110110101	101	-100100010
1101000010001001011101001000110001000	1	110000101
1001010110011101100100011000000001101	10	-100010111011
111010111010111110001100001011111011	1	101001000000
1111111000101110010110110100001011	1	-1110100111011
1101100100110000101111010001100100	101	10011101111011
10010011111101100111100010110011	1	-100010010110110
10000000111100101001100011100101	110	10111111100001001
10011000000111101111111001110	1	-11100001110111111
1110110110110101101101000010001	11	11000001010110000011
100001010001000010110111101	1	-11011101100101000010
10011000011100100011011010	1	1101011010000101001001
11100011010111100011100011	10	-10000110111101010001011
10011011000010111111011	1	11110010001101111010100
100100001010010011110101	1101	-1001101011011001000110011
10100110011100000010	1	1101011101100111000000111
10010110100111011011	1001	-10111000101100010100010001110
1111110100100111	1	11000110001001111011010010101
1000001101111100	1	-11110110000000101101001111001011
111100110101011	1100	100001110110001111100101001100000
100111010001	10	-1000000100110010101001111000101011
1111011111	1	1100101001000010001110011010001100100
1000010011	1	-11010010010101010110010000011011110011
111001100	110	100110111011101101000000011101101010111
1000111	10	-10000010011100101111100101000010010101
100010	1011	11010111001000111101101111100100100010011
11		-1110011101110010001111010001101010001110000
1		10100101110101111010100011110001110100111100011

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

```

1111111111111111100001111010100111001001000011001
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
        XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
          XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
            XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
              XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
                XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
                  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
                    XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
                      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
                        XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
                          XXXXXXXXXXXXXXXXXXXXXXXXXXXX
                            XXXXXXXXXXXXXXXXXXXXXXXXXX
                              XXXXXXXXXXXXXXXXXXXXXXXX
                                XXXXXXXXXXXXXXXXXXXXXX
                                  XXXXXXXXXXXXXXXXXXXX
                                    XXXXXXXXXXXXXXXXXX
                                      XXXXXXXXXXXXXXXX
                                        XXXXXXXXXXXXXX
                                          XXXXXXXXXX
                                            XXXXXX
                                              XX

```

X
XXX
XXXX
X
XX
X
XXX
X
XX
X
X
XXX
X
XXX
X
XX
X
X
XX
X
XXXX
X
XXXX
X
XXXX
XX
X
X
XXX
XX
XXXX

[illegible]

A Generic Attack

	$R_0 = N, R_1 = k'$	q	$U_0 = 0, U_1 = 1$
111111111111111100001111010100111001001000011001			0
110110111100110100111XXXXXXXXXXXXXXXXXXXXXXXX		1	1
1001000011000111010XXXXXXXXXXXXXXXXXXXXXXXX		110	-1
101010001001011XXXXXXXXXXXXXXXXXXXXXXXX		1101	111
1111100110XXXXXXXXXXXXXXXXXXXXXXXX		1	-1011100
1010111XXXXXXXXXXXXXXXXXXXXXXXX		10	1100011
10010XXXXXXXXXXXXXXXXXXXXXXXX		1	-100100010
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		XXX	XXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	-XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		XX	XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	-XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		XXX	-XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		XXX	-XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		XX	-XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	-XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		XX	XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	-XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		XXX	XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		X	-XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX		XXX	XXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX		X	-XXXXXXXXXXXX
XXXXXXXXXXXX		XX	XXXXXXXXXXXX
XXXXXXXXXXXX		X	-XXXXXXXXXXXX
XXXXXX		XXX	XXXXXXXXXXXX
XXXXXX		XX	-XXXXXXXXXXXX
XXXXXX		XXX	XXXXXXXXXXXX
XX		XXX	-XXXXXXXXXXXX
X			XXXXXXXXXXXX

 $P \sim L$

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$
[illegible]

1	110	1101	1	10	1	101	1	10	1	1	101	1	XXX	X	XX	X	X	XX	X	XXXX	X	XXXX	X	X	XXXX	XX	X	X	XXX	XX	XXXX
---	-----	------	---	----	---	-----	---	----	---	---	-----	---	-----	---	----	---	---	----	---	------	---	------	---	---	------	----	---	---	-----	----	------

[illegible]

$\mathcal{P} \stackrel{?}{\sim} \mathcal{L}$

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$
[illegible]

1	110
1101	1
1	10
1	101
1	10
1	1
101	1
1	110
1	11
X	X
XX	X
XXXX	X
X	XX
XXXX	X
X	XXX
XXXX	XX
XXXX	XXXX

[illegible]

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

```

11111111111111111100001111010100111001001000011001
11011011110011010011111010001111001101101101110
1001000011000111010000110000111111011010101011
10101000100101100111110111101001101101100
111110011001111111001011100011101000101111
1010111100011010110010011001100100111101
1001010100001001100110110000011110110101
11010000100010010111101001000110001000
1001010110011101100100011000000001111
11101011101011111000110000101111011
1111111000101110010110110100010111
1101100100110000101111010001100100
10010011111101100111100010110011
10000000111100101001100011100101
10011000000111101111111001110
1110110110110101101000010001
100001010001000010110111101
10011000011100100011011010
1110001101011110011100011
100110110000101111110111
100100001010010011110101
10100110011100000010
10010110100111011011
1111110100100111
1000001101111100
111100110101011
100111010001
1111011111
1000010011
111001100
1000111
100010
11

```

```

0
1
110 -1
1101 111
1 -1011100
10 1100011
1 -100100010
101 110000101
1 -100010111011
10 101001000000
1 -1110100111011
1 10011101111011
101 -100010010110110
1 1011111100001001
110 -11100001110111111
1 11000001010110000011
11 -11011101100101000010
1 1101011010000101001001
1 -10000110111101010001011
10 11110010001101111010100
1 -1001101011011001000110011
1101 1101011101100111000000111
1 -10111000101100010100010001110
1001 11000110001001111011010010101
1 -11110110000000101101001111001011
1 100001110110001111100101001100000
1100 -1000000100110010101001111000101011
10 1100101001000010001110011010001100100
1 -110100100101010101100100000011011110011
1 100110111011101101010000000111011010111
110 -10000010011110010111110010100001001001010
10 110101110010001111011101111100100100010011
1011 -1110011101110010001111010001101010001110000
1010010111010111101010001111000111010011110001

```

A Generic Attack

$$R_0 = N, R_1 = k'$$

q

$$U_0 = 0, U_1 = 1$$

1
110
1101
1
10
1
101
1
0
1
110
1
1
1
10
1
1101
1
1001
1
1
1100
10
1
1
11
10
101

```

0
1
-1
111
-1011100
1100011
-100100010
110000101
-100010111011
101001000000
-1110100111011
10011101111011
-100010010110110
10111111100001001
-1110000111011111
11000001010110000011
-11011101100101000010
1101011010000101001001
-10000110111101010001011
11110010001101111010100
-1001101011011001000110011
1101011101100111000000111
-10111000101100010100010001110
11000110001001111011010010101
-1111011000000010110100111100111
100001110110001111100101001100000
-1000000100110010101001111000101011
1100101001000010001110011010001100100
110110110101010110010000011011110011
1101101111011101101000000011101101010111
-1000001001110010111110010100001001001010
1101011110010001111011101111100100100010011
-1110011101110010001111010001101010001110000
101001011101011110101000111000111010011110001
101001011101011110101000111000111010011110001

```



$\mathcal{P} \sim \mathcal{L}$

with $\mathcal{L} = \text{len}(r_0) - \text{len}(r_1)$

the candidate list has exponential growth

Agenda

Introduction

FIDO Hardware

Infineon SLE

FEITIAN A22 Or

Infineon ECDSA

The Extended



A Side-Channel Attack Only in EEA

ECDSA Signature V

Infineon ECDSA Si

First Observations

Summary

A Masked Modular Inversion

A Key-Recovery Attack

In a Perfect World

A Generic Attack

Full Reverse-Engineering of Infineon EEA

Heuristical Approaches

Summary of The Sensitive Leakage

Full Nonce Recovery

Yubikey 5C

Aquisition Setup

First Side-Channel Traces

Attack in Practice

Impact Analysis

Infineon Security Microcontrollers

Optiga Trust M

Optiga TPM

Conclusions

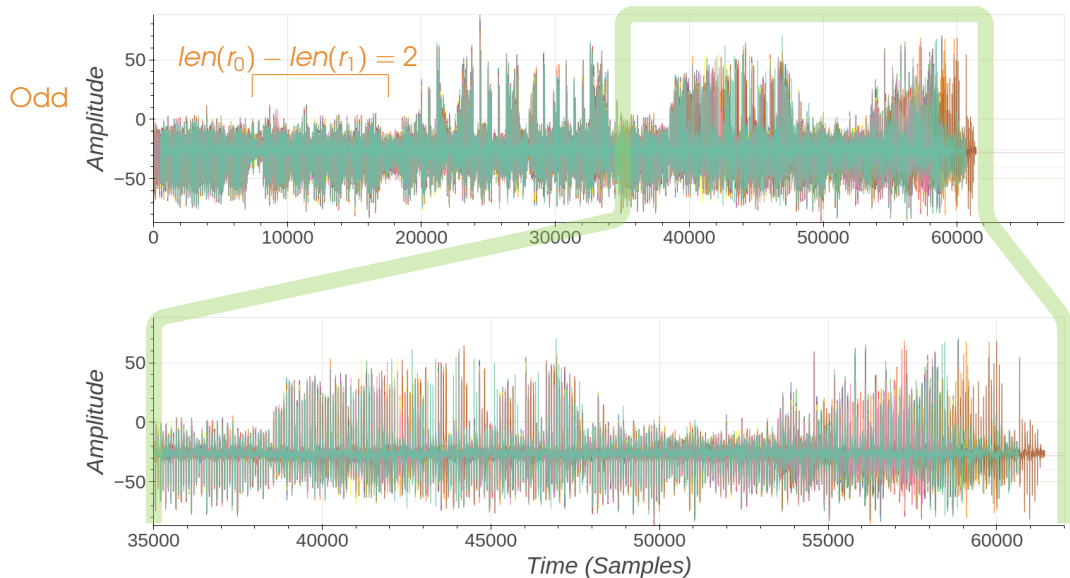
Summing up

Mitigations

Avenues Of Research

Project Timeline

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



A Weird Euclidean Division 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    $r_0, r_1 \leftarrow r_1, r_0 - q.r_1$ 
6    $t_0, t_1 \leftarrow t_1, t_0 - q.t_1$ 
7 if  $t_0 < 0$  then
8    $t_0 \leftarrow t_0 + n$ 
Return :  $t_0$ 
```

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

```
 $r \leftarrow a$ 
 $\ell \leftarrow \text{len}(r) - \text{len}(b)$ 
 $q \leftarrow 0$ 
while  $\ell \geq 0$  do
   $g \leftarrow \text{sign}(r).2^\ell$ 
   $r \leftarrow r - g.b$ 
   $q \leftarrow q + g$ 
   $\ell \leftarrow \text{len}(r) - \text{len}(b)$ 
if  $r < 0$  then
   $q \leftarrow q - 1$ 
   $r \leftarrow r + b$ 
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  $\ell \leftarrow \text{len}(r) - \text{len}(b)$ 
3  $q \leftarrow 0$ 
4 while  $\ell \geq 0$  do
5    $g \leftarrow \text{sign}(r).2^\ell$ 
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

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
5    $g \leftarrow \text{sign}(r).2^\ell$            Long Division
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
```

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  $q \leftarrow 0$                          # Loop Iter. leaks
4 while  $\ell \geq 0$  do                    $\ell = 0$  leaks
5    $g \leftarrow \text{sign}(r).2^\ell$ 
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
```

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  $\ell \leftarrow \text{len}(r) - \text{len}(b)$ 
3  $q \leftarrow 0$ 
4 while  $\ell \geq 0$  do
5    $g \leftarrow \text{sign}(r).2^\ell$ 
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 :  $q$ 
```

$\ell = \text{len}(r_0) - \text{len}(r_1)$ leaks

Loop Iter. leaks

$\ell = 0$ leaks

Odd: $\text{sign}(r)$ leaks

Even: $\text{sign}(r)$ leaks iff $\ell > 0$

// q is the quotient

// r is the remainder

Let's sum up

- ▶ Timing leakages in ECDSA's nonce modular inversion.

Extended Euclidean Algorithm

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

blinded nonce \rightarrow nonce \rightarrow private key

Let's sum up

- ▶ Timing leakages in ECDSA's nonce modular inversion.

Extended Euclidean Algorithm

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

blinded nonce \rightarrow nonce \rightarrow private key



Side-Channel Attack
on Ext. Euclidean Alg.

ninjalab.io/eucleak

Let's sum up

- ▶ Timing leakages in ECDSA's nonce modular inversion.

Extended Euclidean Algorithm

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

blinded nonce \rightarrow nonce \rightarrow private key



Side-Channel Attack
on Ext. Euclidean Alg.

ninjalab.io/eucleak



From Blinded Nonce to ECDSA Private Key

- ▶ From k' compute $Q_{(x,y)} = [k']G_{(x,y)} = [m][k]G_{(x,y)}$
- ▶ From the signature (r, s) , find the opposite points $A = -B$ such that $A_x = B_x = r$:

$$A = [k]G_{(x,y)} \text{ or } B = [k]G_{(x,y)}$$

- ▶ finally we have $[m]A = Q$ or $[m]B = Q$

From Blinded Nonce to ECDSA Private Key

- ▶ From k' compute $Q_{(x,y)} = [k']G_{(x,y)} = [m][k]G_{(x,y)}$
- ▶ From the signature (r, s) , find the opposite points $A = -B$ such that $A_x = B_x = r$:

$$A = [k]G_{(x,y)} \text{ or } B = [k]G_{(x,y)}$$

- ▶ finally we have $[m]A = Q$ or $[m]B = Q$

\hookrightarrow find m with Pollard's kangaroo algorithm in $O(2^{\frac{\text{len}(m)}{2}})$

From Blinded Nonce to ECDSA Private Key

- ▶ From k' compute $Q_{(x,y)} = [k']G_{(x,y)} = [m][k]G_{(x,y)}$
- ▶ From the signature (r, s) , find the opposite points $A = -B$ such that $A_x = B_x = r$:

$$A = [k]G_{(x,y)} \text{ or } B = [k]G_{(x,y)}$$

- ▶ finally we have $[m]A = Q$ or $[m]B = Q$

\hookrightarrow find m with Pollard's kangaroo algorithm in $O(2^{\frac{\text{len}(m)}{2}})$

- ▶ $k = k' / m \bmod N$

From Blinded Nonce to ECDSA Private Key

- ▶ From k' compute $Q_{(x,y)} = [k']G_{(x,y)} = [m][k]G_{(x,y)}$
- ▶ From the signature (r, s) , find the opposite points $A = -B$ such that $A_x = B_x = r$:

$$A = [k]G_{(x,y)} \text{ or } B = [k]G_{(x,y)}$$

- ▶ finally we have $[m]A = Q$ or $[m]B = Q$

\hookrightarrow find m with Pollard's kangaroo algorithm in $O(2^{\frac{\text{len}(m)}{2}})$

- ▶ $k = k' / m \bmod N$
- ▶ $d = r^{-1}(ks - h) \bmod N$

Agenda

Introduction

- FIDO Hardware
- Infineon SLE 70
- FEITIAN A22 C
- Infineon ECD
- The Extended

A Side-Channel Attack on the Security in EEA

- ECDSA Signatures
- Infineon ECD
- First Observations
- Summary
- A Masked Module

A Key-Recovery Attack

- In a Perfect World
- A Generic Attack



Full Reverse-Engineering of Infineon EEA

- Heuristical Approaches
- Summary of The Sensitive Leakage
- Full Nonce Recovery

Yubikey 5C

- Aquisition Setup
- First Side-Channel Traces
- Attack in Practice

Impact Analysis

- Infineon Security Microcontrollers
- Optiga Trust M
- Optiga TPM

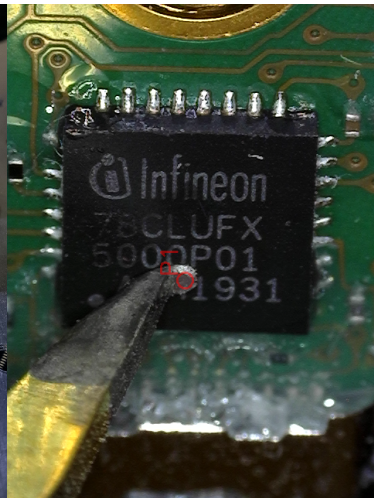
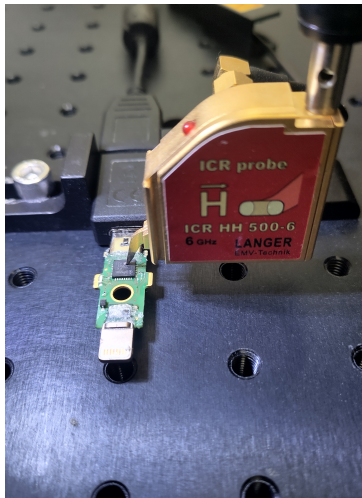
Conclusions

- Summing up
- Mitigations
- Avenues Of Research
- Project Timeline

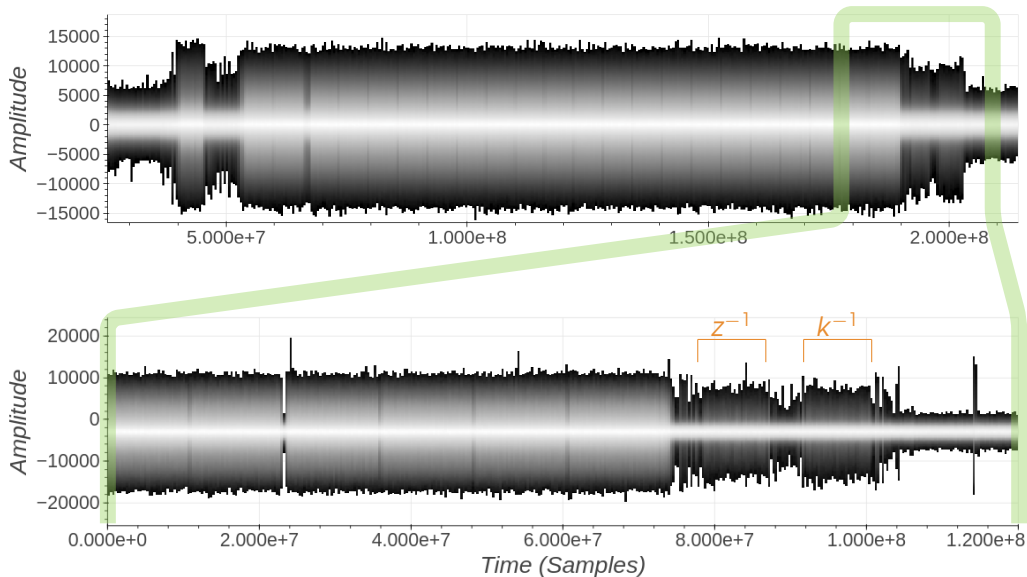
Yubikey 5Ci – EM Acquisitions



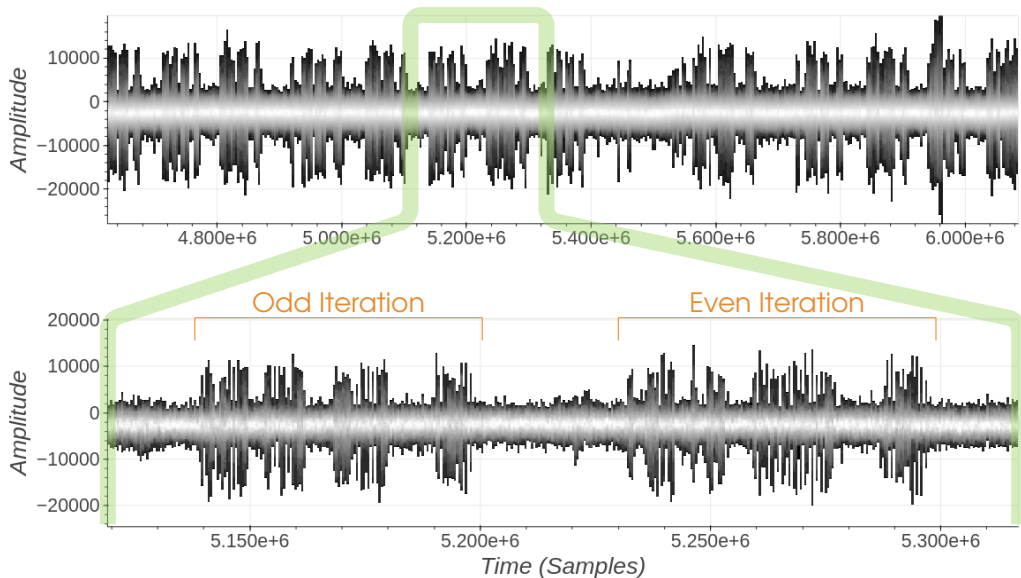
credits Yubico



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 $\text{len}(r_0) - \text{len}(r_1) \leq 5$ 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 $\text{len}(r_0) - \text{len}(r_1) \leq 5$ 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 Hardware Token

Infineon ECD

FEITIAN

Infineon EC

The Extended

A Side-Channel Attack on Infineon ECD

ECDSA Signature Verification

Infineon ECDSA Signature Verification

First Observation

Summary

A Masked Modular Inversion

A Key-Recovery Attack

In a Perfect World

A Generic Attack



Full Reverse-Engineering of Infineon EEA

Heuristical Approaches

Summary of The Sensitive Leakage

Full Nonce Recovery

Yubikey 5C

Aquisition Setup

First Side-Channel Traces

Attack in Practice

Impact Analysis

Infineon Security Microcontrollers

Optiga Trust M

Optiga TPM

Conclusions

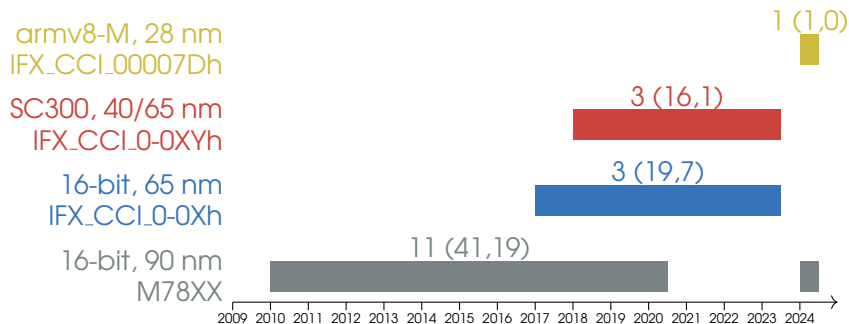
Summing up

Mitigations

Avenues Of Research

Project Timeline

Infineon Security Microcontrollers (IC CC Certifications)



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

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

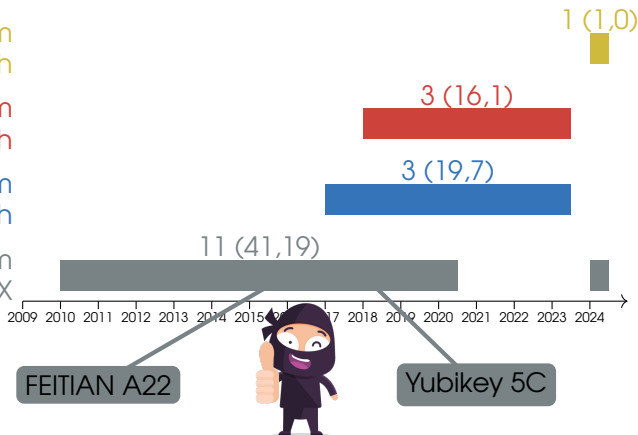
Infineon Security Microcontrollers (IC CC Certifications)

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, www.sec-certs.org

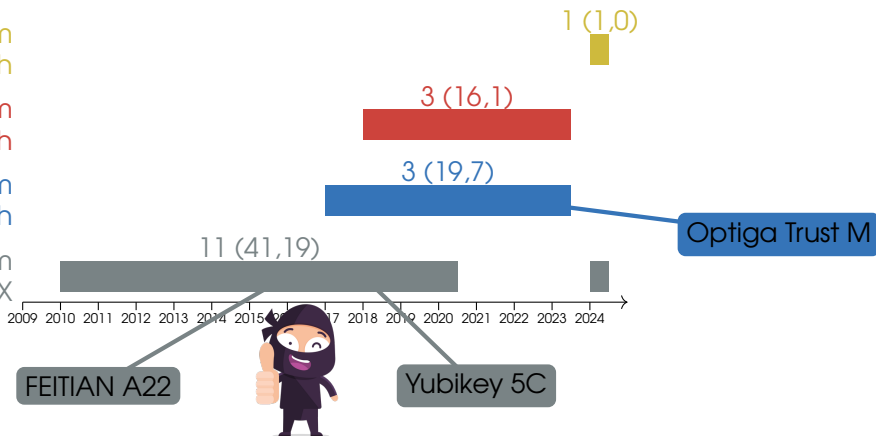
Infineon Security Microcontrollers (IC CC Certifications)

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, 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)

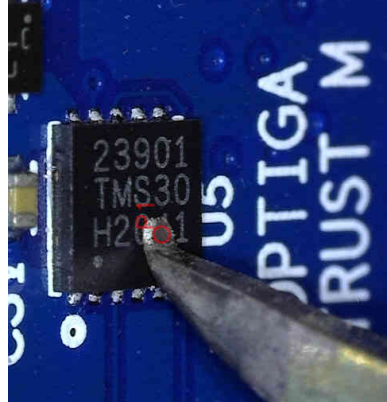
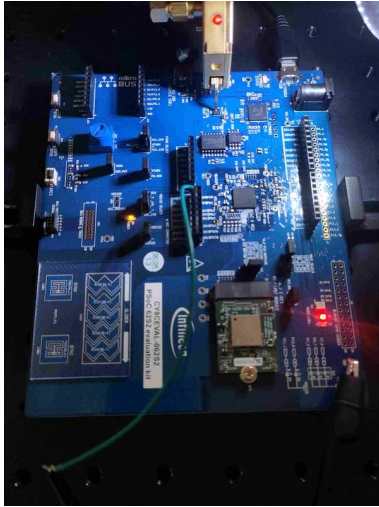


Download User
Manual

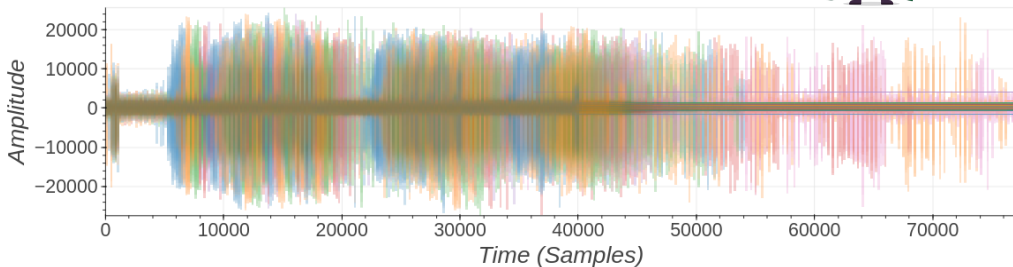
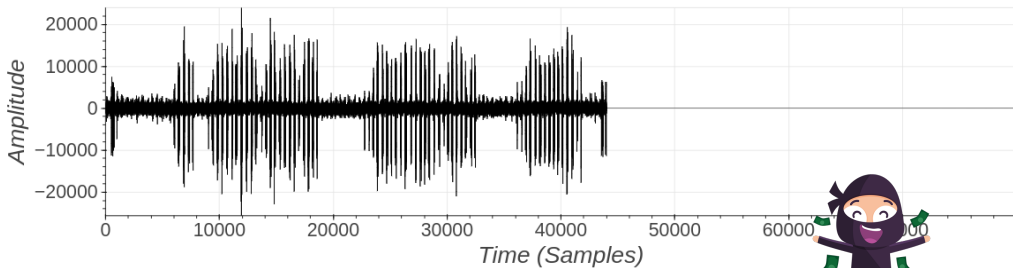
<https://github.com/Infineon/optiga-trust-m>

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

Optiga Trust M – Side-channel Setup



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



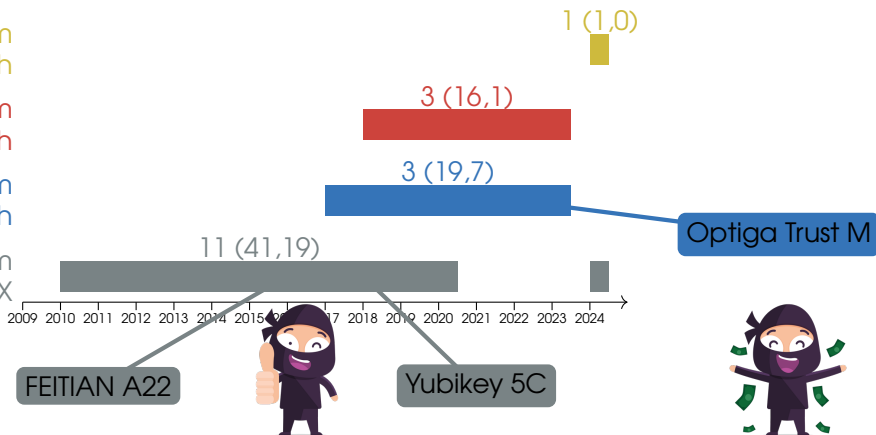
Infineon Security Microcontrollers (IC CC Certifications)

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, www.sec-certs.org

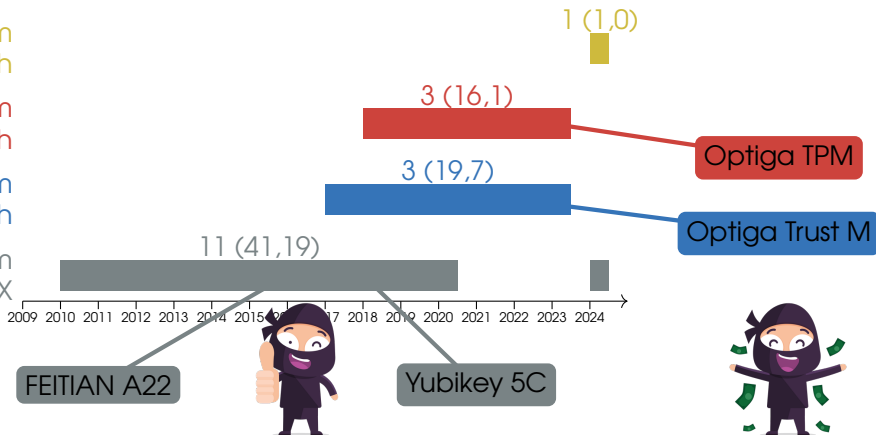
Infineon Security Microcontrollers (IC CC Certifications)

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, 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 TPM9673FW2613RPIEBTOB01

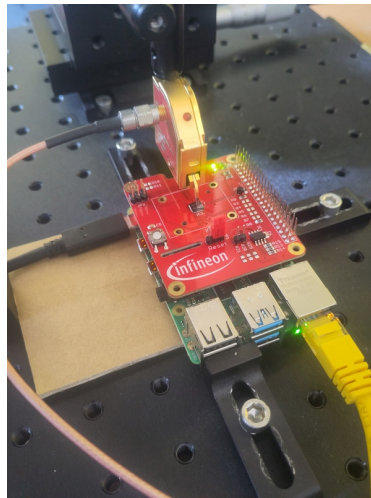
TPM9673FW2613RPIEBTOB01



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

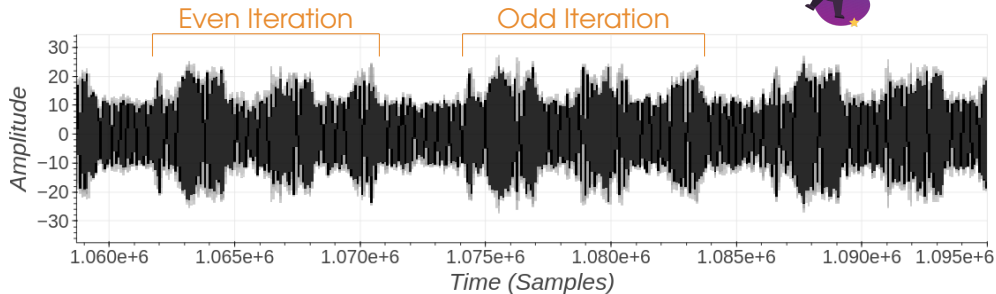
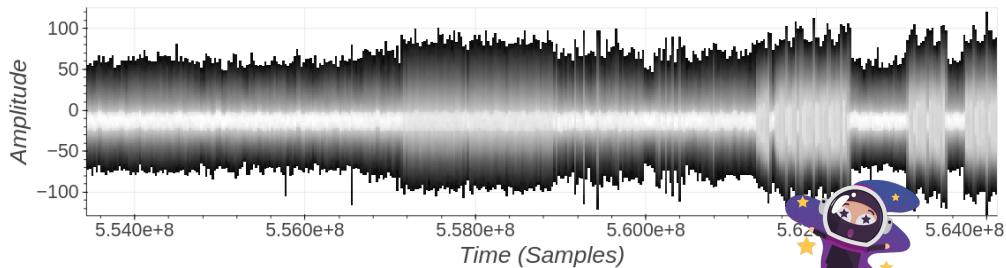
Partager

N° Mouser :	726-TPM9673FW2613RPI
N° de fab. :	TPM9673FW2613RPIEBTOB01
Fab. :	Infineon Technologies
N° client:	<input type="text" value="N° client"/>
Description :	HAT/cartes complémentaires Raspberry Pi
Cycle de vie:	 Nouveau produit: Nouveau chez ce fabricant.
Fiche technique:	 TPM9673FW2613RPIEBTOB01 Fiche technique (PDF)
Plus d'informations	En savoir plus à propos de Infineon Technologies TPM9673FW2613RPIEBTOB01



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

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



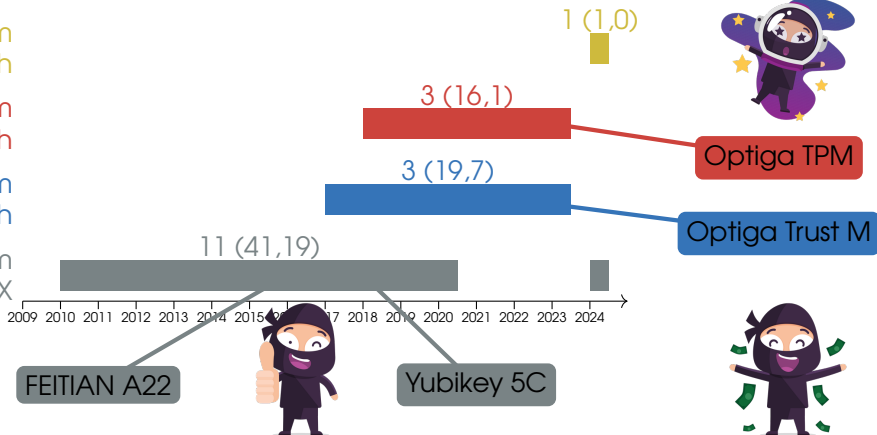
Infineon Security Microcontrollers (IC CC Certifications)

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



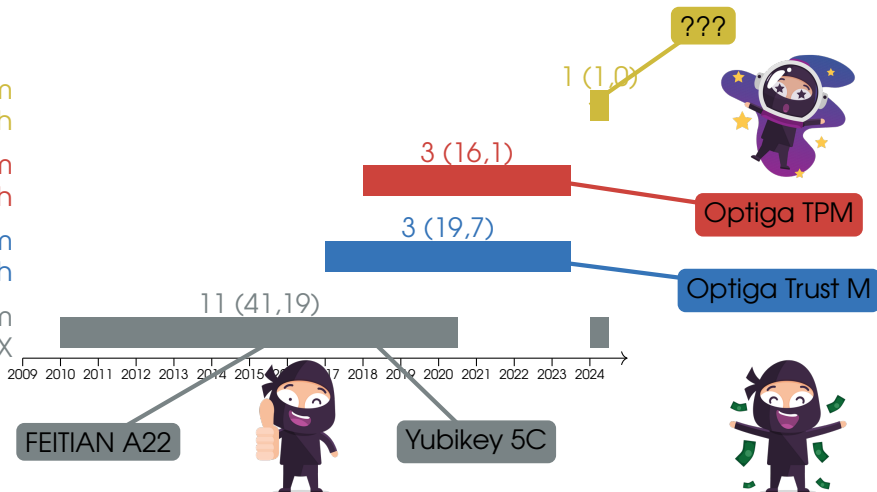
Infineon Security Microcontrollers (IC CC Certifications)

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, www.sec-certs.org

Infineon Security Microcontrollers (IC CC Certifications)

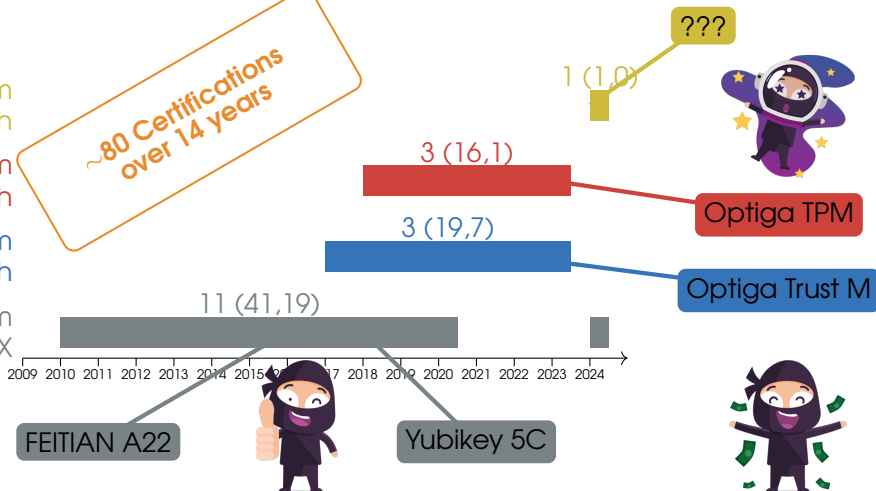
armv8-M, 28 nm
IFX_CCI_00007Dh

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, www.sec-certs.org

Agenda

Introduction

FIDO Hardware
Infineon SLE
FEITIAN A22
Infineon CCD
The External

A Side-Channel Attack on Infineon EEA

ECDSA Signature Verification
Infineon ECDSA Verification
First Observation
Summary

A Masked Modular Inversion

A Key-Recovery Attack

In a Perfect World
A Generic Attack



Full Reverse-Engineering of Infineon EEA

Heuristical Approaches
Summary of The Sensitive Leakage
Full Nonce Recovery

Yubikey 5C

Aquisition Setup
First Side-Channel Traces
Attack in Practice

Impact Analysis

Infineon Security Microcontrollers
Optiga Trust M
Optiga TPM

Conclusions

Summing up
Mitigations
Avenues Of Research
Project Timeline

Let's sum up: Attack Steps

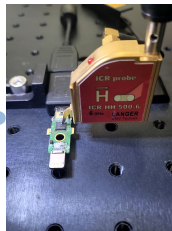
Infineon SE
running ECDSA



Chip
Physical Access



SCA Bench
few mins



Offline
Key-Recovery
few hours



Re-Packaging

Generate/Store Keys
Key Exch./Wrap.

Signatures



Remote Attacker

NXP

infineon



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

...

Generate/Store Keys
Key Exch./Wrap.

Signatures



Remote Attacker

- Sovereign Documents
- Access Control
- Bank Cards

NXP

infineon

≥ 14 years



φ 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

...

Generate/Store Keys
Key Exch./Wrap.

Signatures



Remote Attacker

NXP



≥ 14 years



SAMSUNG

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

...

φ Attacker

Side-Channel

Fault Injection

Invasive

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

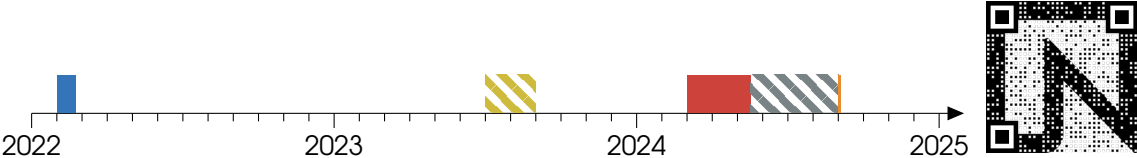
- ▶ Protocol Specific Mitigations

eg. Activate Counter in FIDO

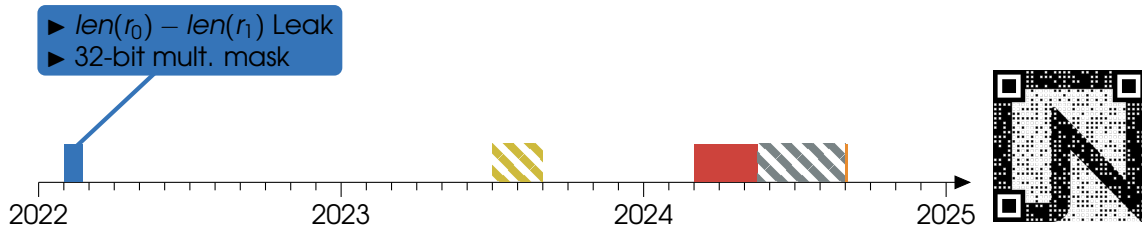
Avenues Of Research

- ▶ Extend this work to RSA (eg. key generation)
- ▶ Theoretical Analysis of the **EUCLEAK** generic attack
- ▶ Improve the attack in practice
eg. single-trace attack or improve EM acquisitions
- ▶ Extend the generic attack to the Binary EEA case.

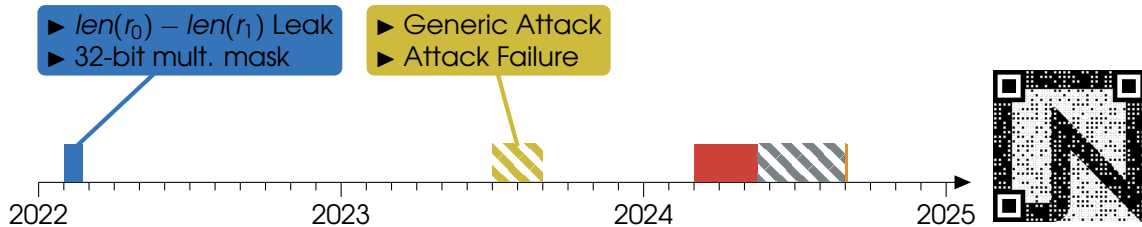
Project Timeline



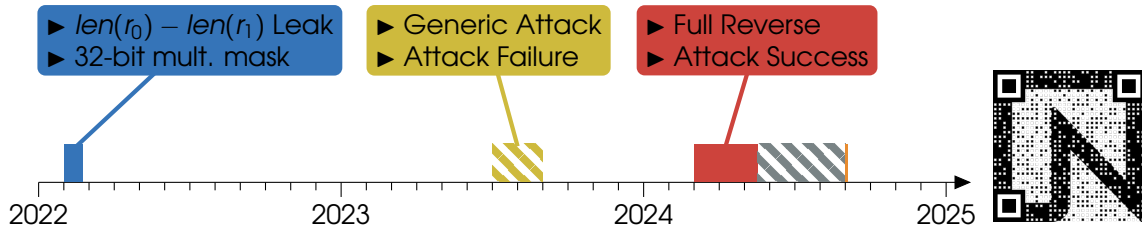
Project Timeline



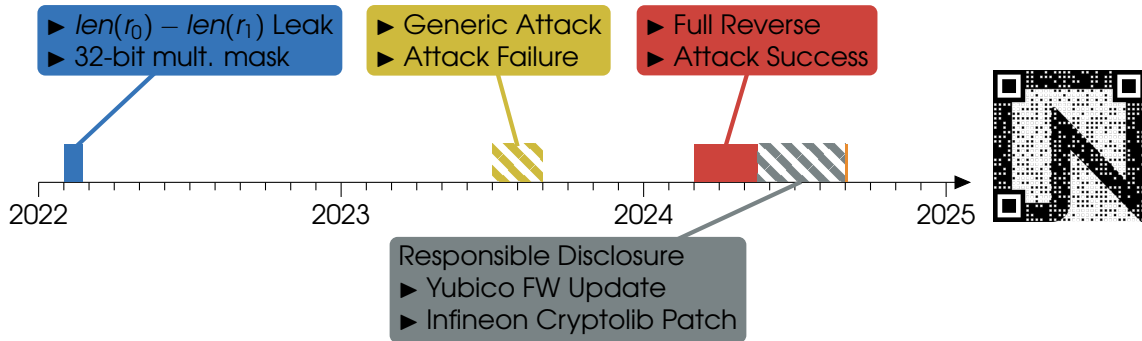
Project Timeline



Project Timeline



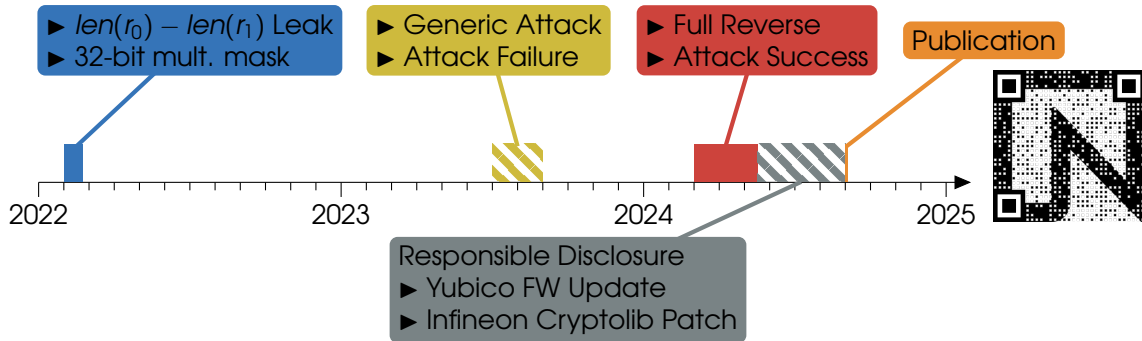
Project Timeline



Project Timeline



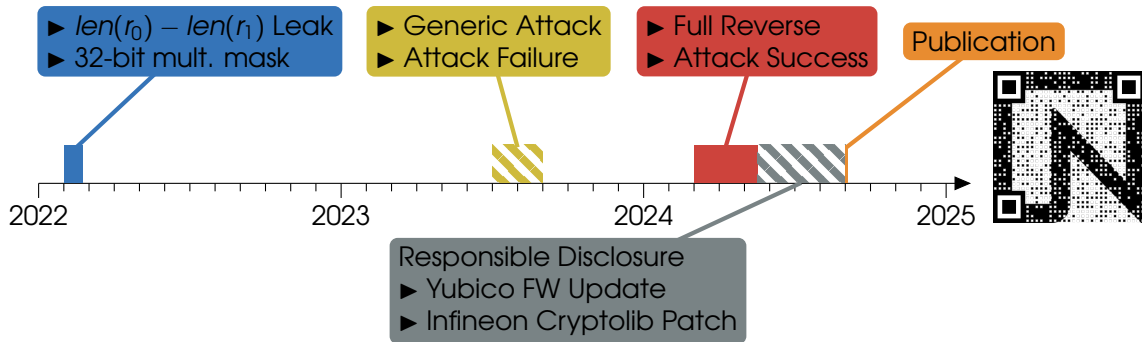
ninjalab.io/eucleak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



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

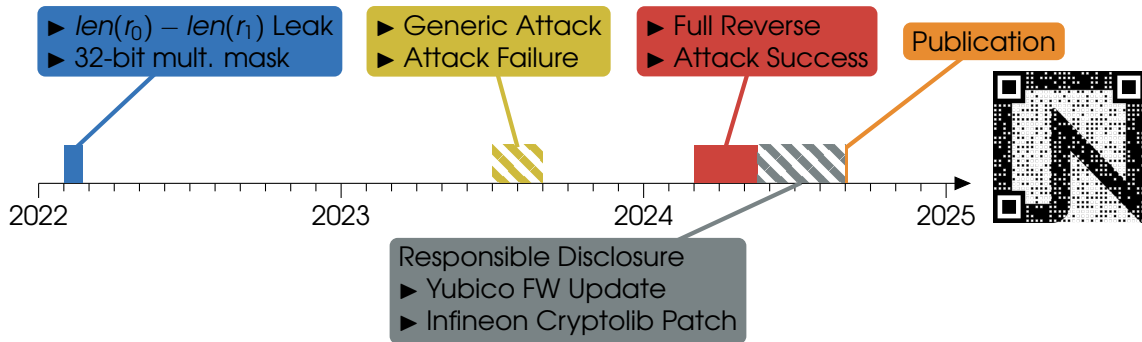


- Sept. 3rd 2024: Yubico Releases a Security Advisory

Project Timeline



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

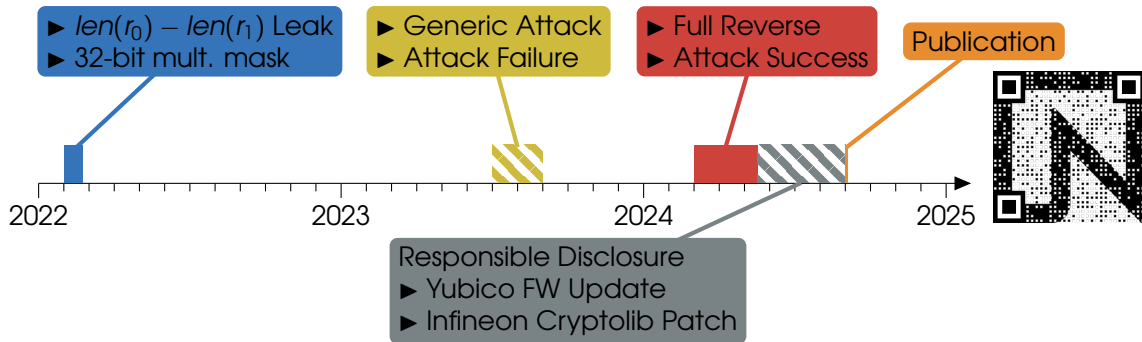


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)

Project Timeline



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

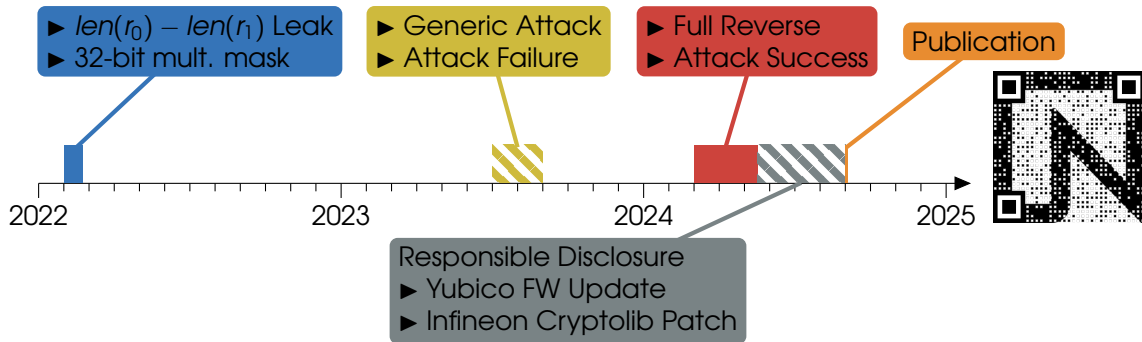


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**

Project Timeline



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

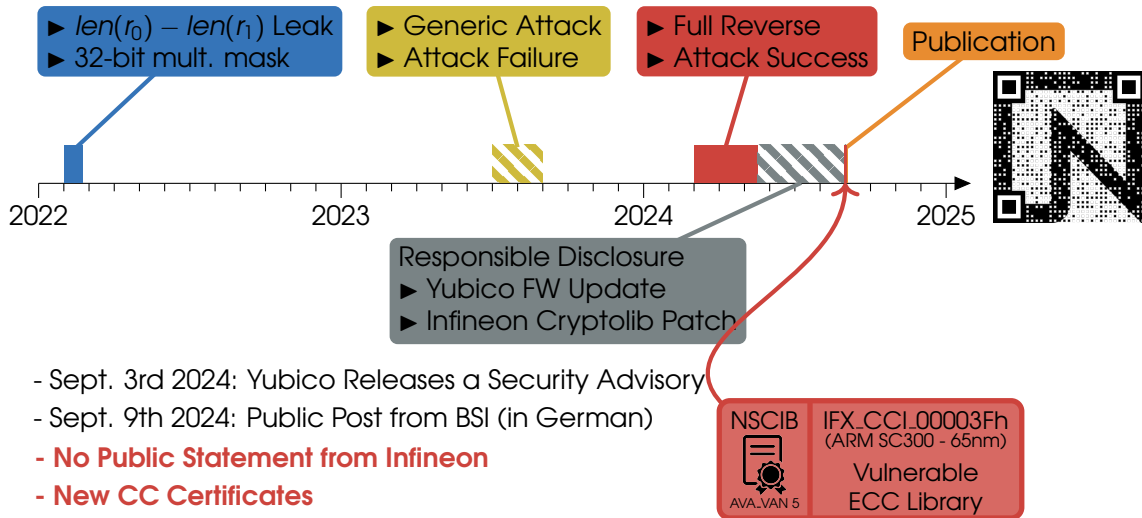


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

Project Timeline



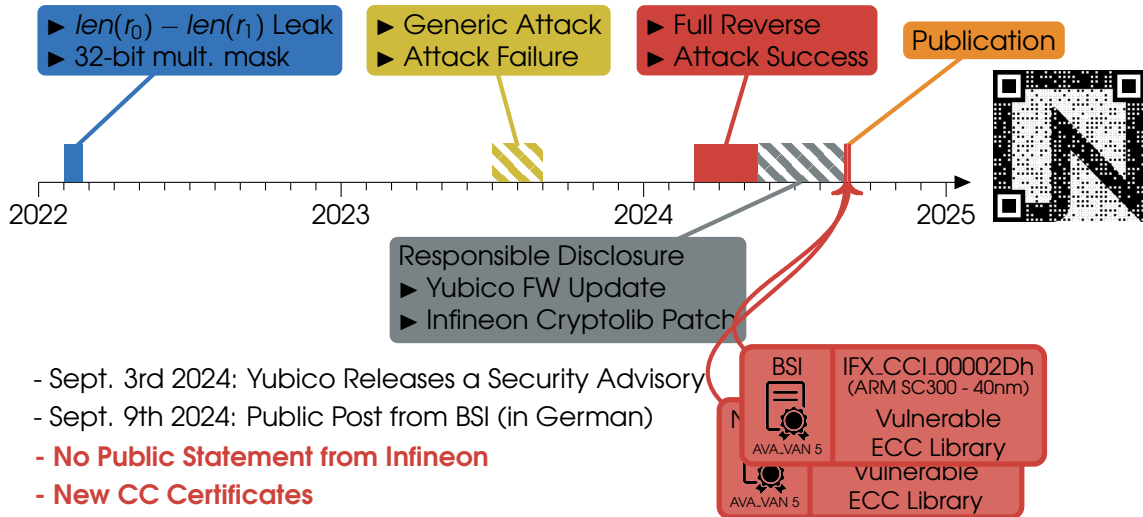
ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025

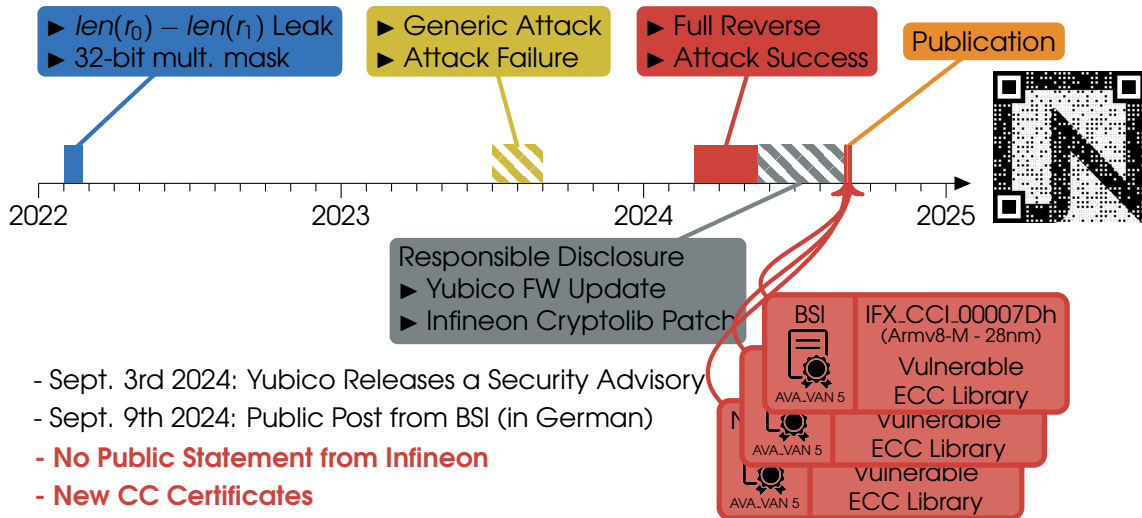


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

Project Timeline



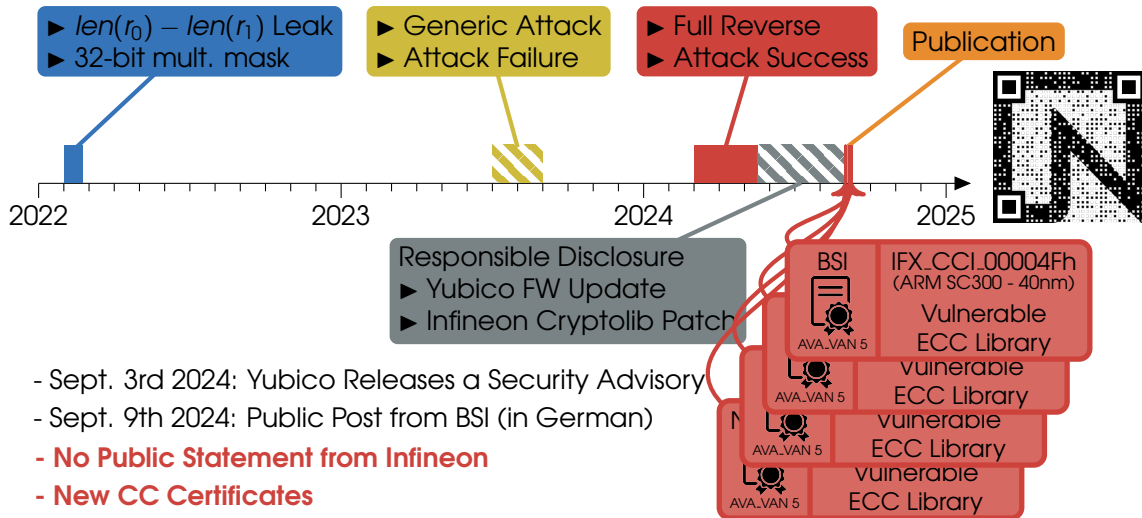
ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



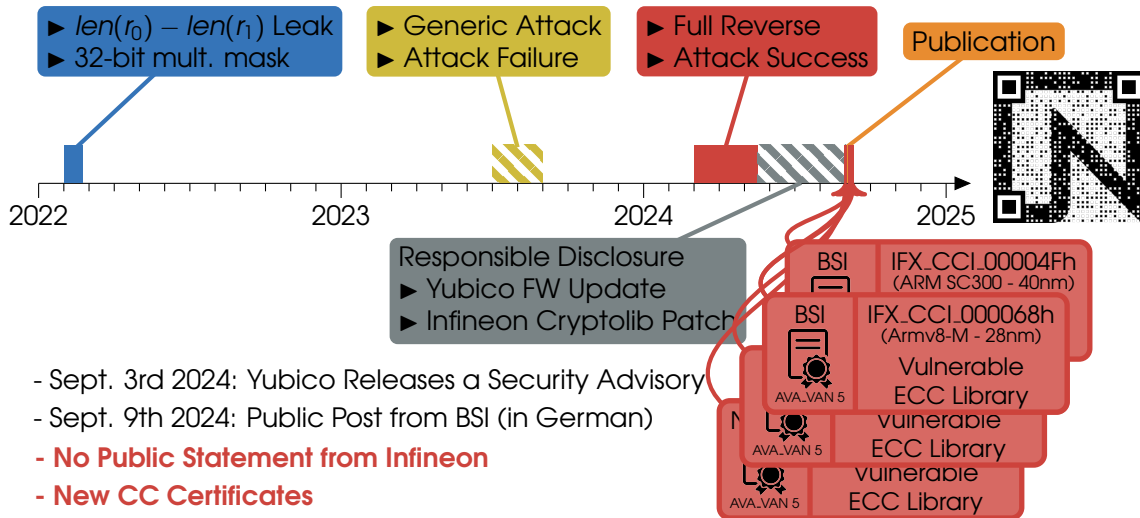
ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



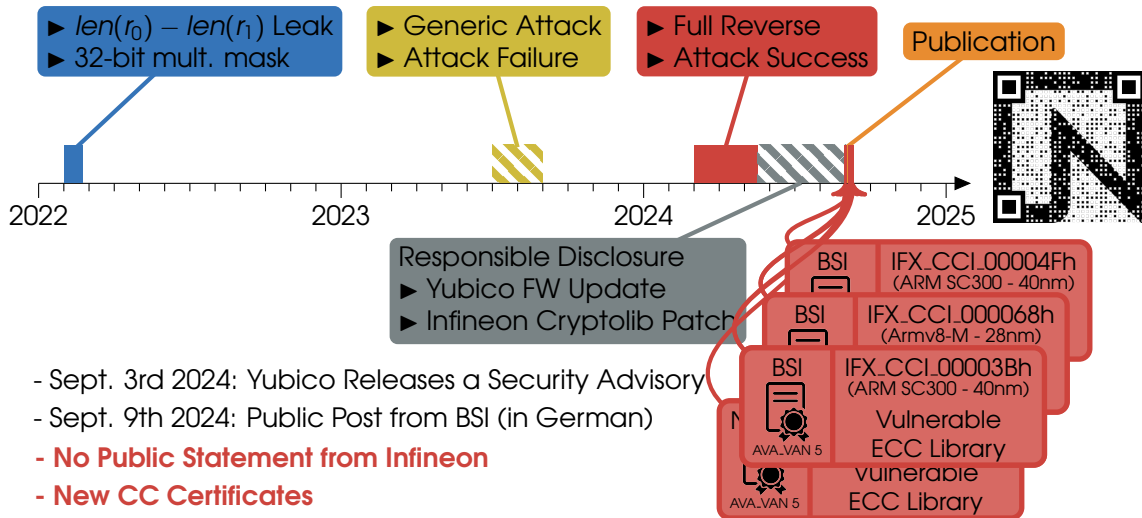
ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



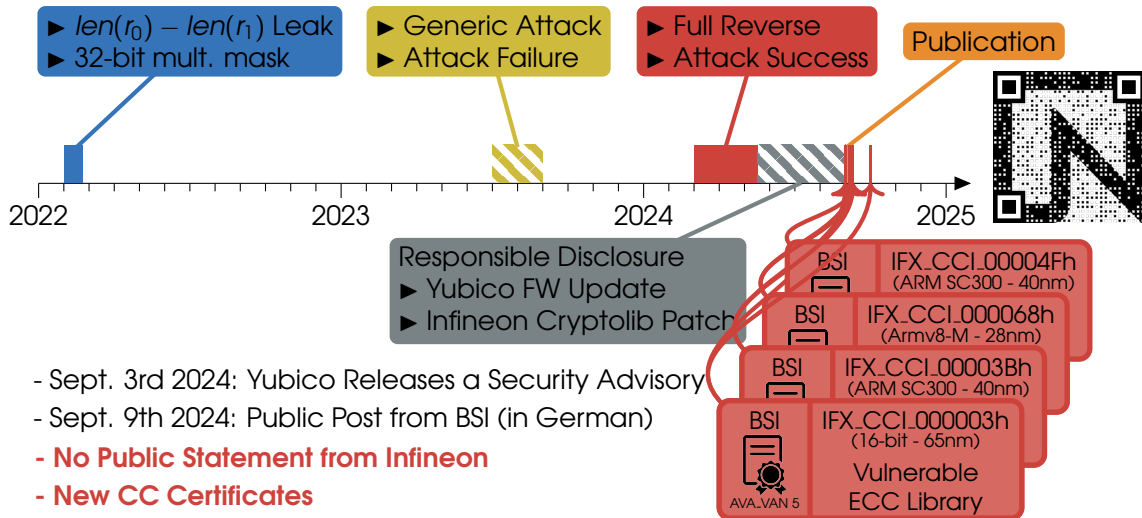
ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



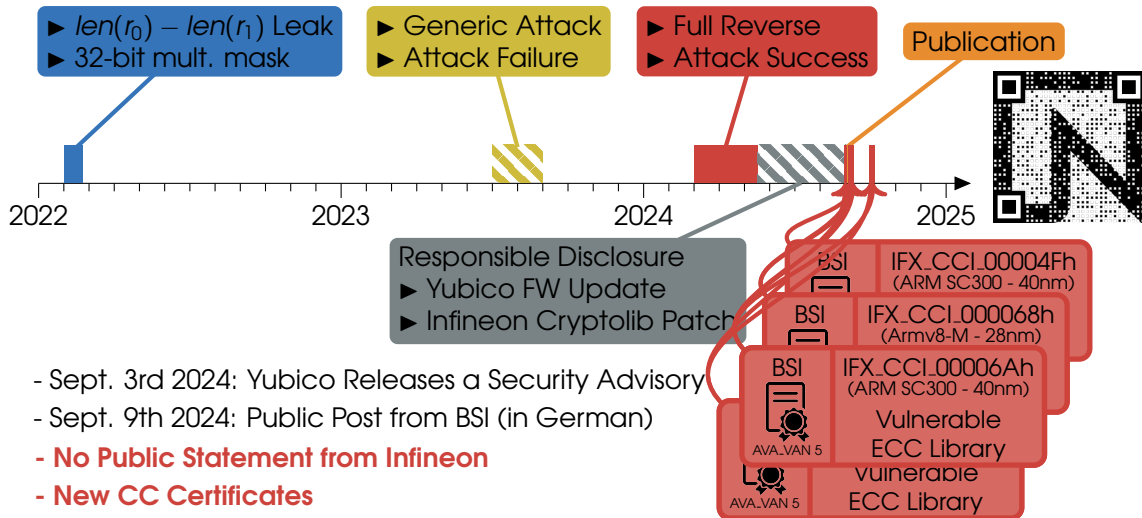
ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



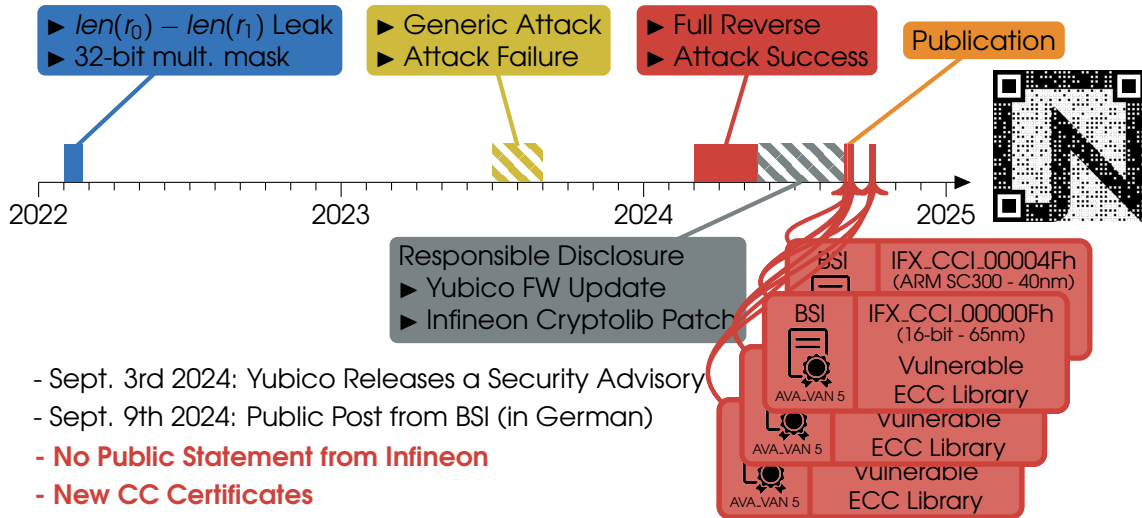
ninja1ab.io/eucleak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



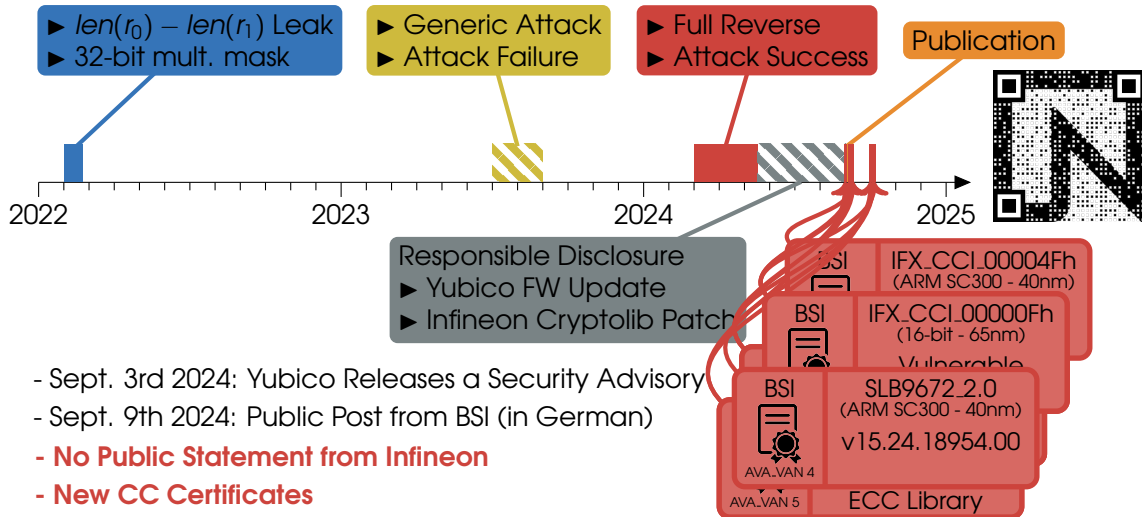
ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



Project Timeline



ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025

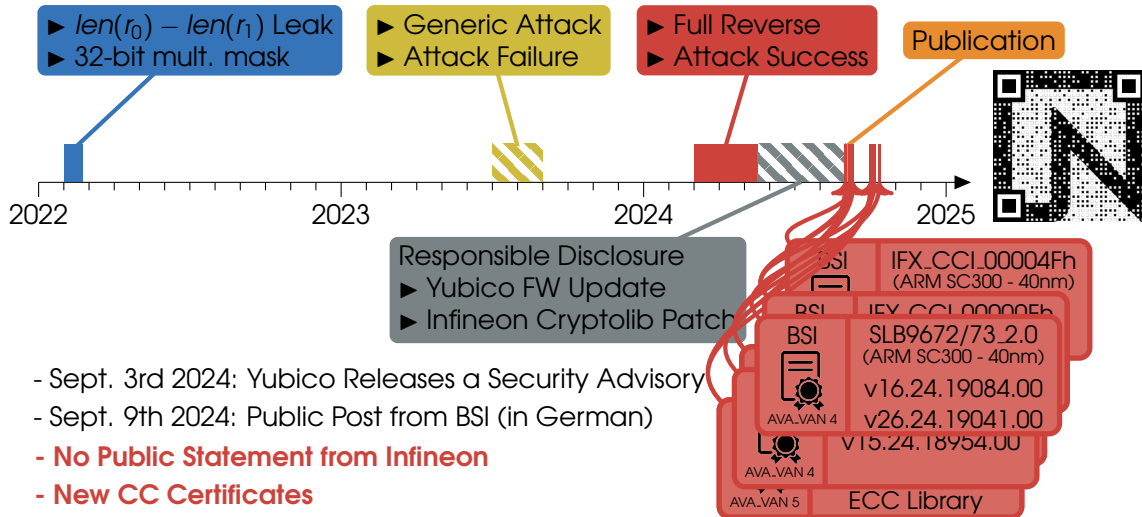


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

Project Timeline



ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025

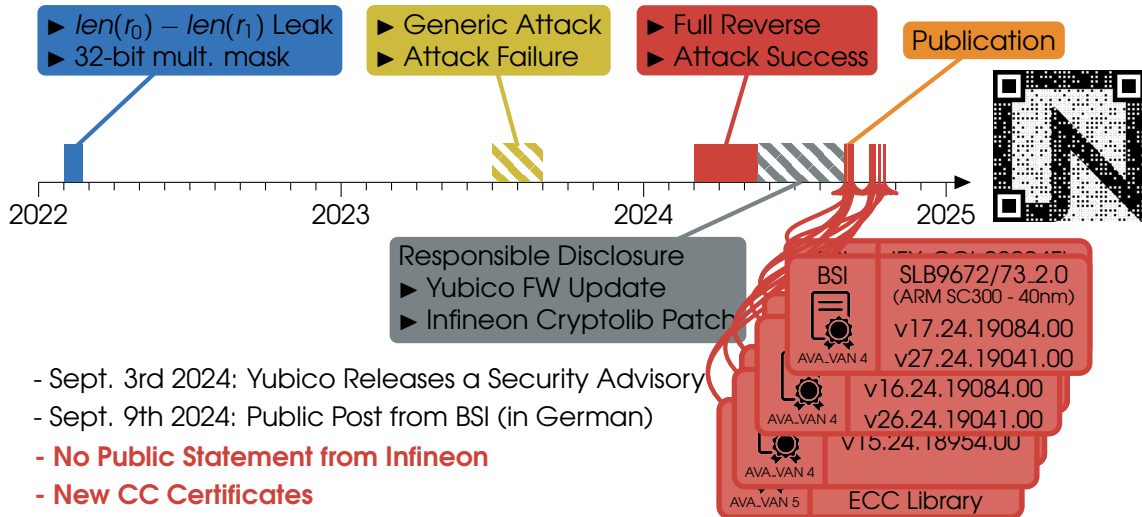


- Sept. 3rd 2024: Yubico Releases a Security Advisory
- Sept. 9th 2024: Public Post from BSI (in German)
- **No Public Statement from Infineon**
- **New CC Certificates**

Project Timeline



ninja1ab.io/euc1eak
eprint.iacr.org/2024/1380
published in IEEE S&P 2025



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