MUNI FI

CROCS

Centre for Research on Cryptography and Security

October 26, 2022

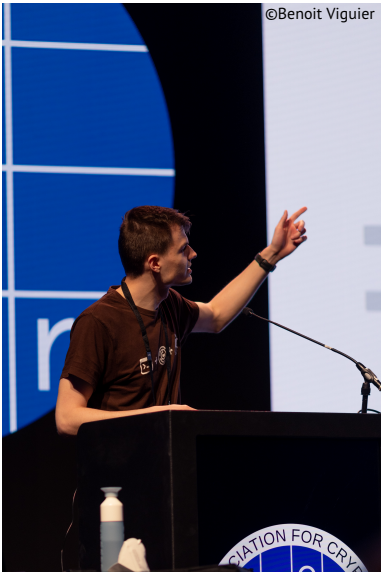
From Vulnerability to Impact - Automatically Analyzing the Security Certifications Landscape

Jan Jancar

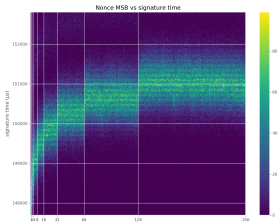
Petr Švenda, Adam Janovský,
Jiří Michalík, Stanislav Boboň
...

About me

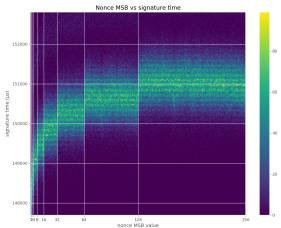
- PhD student @ Masaryk University
- Centre for Research on Cryptography and Security
- Focus:
  - Elliptic-curve cryptography
  - Side-channel attacks
  - Usable security
- Cycle alot



Outline


Nonce MSB vs signature time
152000
151000
150000
149000
140000
signature time (ps)
0
8
16
32
64
128
256
nonce MSB value
80
60
40
20
0

Outline


Nonce MSB vs signature time
signature time (µs)
nonce MSB value


Common Criteria


FIPS
VALIDATED
140-2
TM

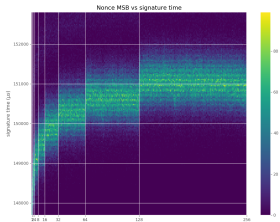

FIPS
140-3
TM

Outline


Common Criteria


FIPS
VALIDATED
140-2
TM


seccerts


Nonce MSB vs signature time
signature time (µs)
nonce MSB value


FIPS
140-3
TM

Minerva: a group of vulnerabilities

- **ECTester**: Testing elliptic-curve cryptography implementations

Minerva: a group of vulnerabilities

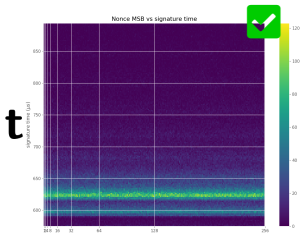
- **ECTester**: Testing elliptic-curve cryptography implementations
- Discovered a timing side-channel vulnerability in ECDSA in:
  - libgcrypt, wolfSSL, MatrixSSL, SunEC/Java, Crypto++
  - Athena IDProtect (CC and FIPS 140-2 certified)

Minerva: a group of vulnerabilities

- **ECTester**: Testing elliptic-curve cryptography implementations
- Discovered a timing side-channel vulnerability in ECDSA in:
  - libgcrypt, wolfSSL, MatrixSSL, SunEC/Java, Crypto++
  - Athena IDProtect (CC and FIPS 140-2 certified)
- ECDSA: random nonce k, scalar multiplication $[k]G$

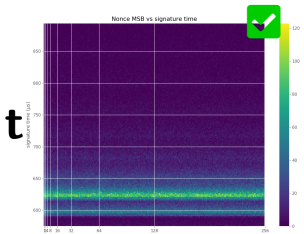
Minerva: a group of vulnerabilities

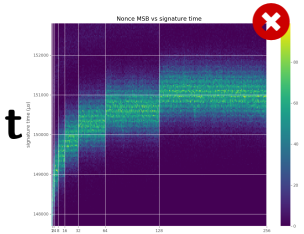
- **ECTester**: Testing elliptic-curve cryptography implementations
- Discovered a timing side-channel vulnerability in ECDSA in:
  - libgcrypt, wolfSSL, MatrixSSL, SunEC/Java, Crypto++
  - Athena IDProtect (CC and FIPS 140-2 certified)
- ECDSA: random nonce k, scalar multiplication $[k]G$



Minerva: a group of vulnerabilities

- **ECTester**: Testing elliptic-curve cryptography implementations
- Discovered a timing side-channel vulnerability in ECDSA in:
  - libgcrypt, wolfSSL, MatrixSSL, SunEC/Java, Crypto++
  - Athena IDProtect (CC and FIPS 140-2 certified)
- ECDSA: random nonce k, scalar multiplication $[k]G$





time
$\sim$
bit-length of k


Leaky loops
Ingredients: Athena IDProtect, Libgcrypt, SunEC, wolfSSL, MumbSSL. May contain traces of bee
Ján Jančár
Vladimír Sedláček
Petr Švenda
Marek Sys
9 780201 379624
CROCS
Centre for Research on Cryptography and Security
Minerva
Leaky loops

Minerva: a group of vulnerabilities

Responsible disclosure

Libraries

- [x] Analyze code for vulnerability
- [x] A few emails back and forth
  - Timelines for fix varied:
    6 days (WolfSSL),
    …
    11 months (MatrixSSL),
    never? (SunEC/Java)

Minerva: a group of vulnerabilities

Responsible disclosure

Libraries

- Analyze code for vulnerability
- A few emails back and forth
  - Timelines for fix varied:
    6 days (WolfSSL),
    …
    11 months (MatrixSSL),
    never? (SunEC/Java)

Smartcard

- No code available, can't debug
- Athena no longer exists, sold to NXP
- ???

Minerva: a group of vulnerabilities

Responsible disclosure

Sorry I spent all your money. Clumsy good-looking male shrugging and holding smartphone and credit card, feeling awkward

Smartcard

- No code available, can't debug
- Athena no longer exists, sold to NXP
- ???

Minerva: a group of vulnerabilities

Responsible disclosure cont.

- Notify NXP ☑

Minerva: a group of vulnerabilities

Responsible disclosure cont.

- Notify NXP ☑
- What about end users? Who are they?
  - NXP notified affected customers, but won't know about all

Minerva: a group of vulnerabilities

Responsible disclosure cont.

- Notify NXP ☑
- What about end users? Who are they?
  - NXP notified affected customers, but won't know about all
- Where is the vulnerability from? Do other implementations share it?
  - NXP pointed to the underlying ATMEL crypto library, but no details

Minerva: a group of vulnerabilities

Responsible disclosure cont.

- Notify NXP ☑
- What about end users? Who are they?
  - NXP notified affected customers, but won't know about all
- Where is the vulnerability from? Do other implementations share it?
  - NXP pointed to the underlying ATMEL crypto library, but no details
- Are certified products affected?

Minerva: a group of vulnerabilities

Responsible disclosure cont.

- Notify NXP ☑
- What about end users? Who are they?
  - NXP notified affected customers, but won't know about all
- Where is the vulnerability from? Do other implementations share it?
  - NXP pointed to the underlying ATMEL crypto library, but no details
- Are certified products affected?

Let's look to security certifications for more info

Security certifications

- How to have confidence in security?
  - Without trusting vendors?
- Security certifications!
- Common Criteria, FIPS 140, EMVCo

Security certifications

The process

Common Criteria

- Certification that product adheres to some *Security Target*
  - Vendor pays and provides materials
  - Independent lab evaluates
  - Certification body issues *Certificate* and *Certification Report*
  - Certificates released and internationally recognized
- Security target might point to a *Protection Profile* instead
  - Common set of requirements for a product class (e.g. a firewall PP)

FIPS 140

- Certification that product adheres to some *Security Policy*
  - Vendor pays and provides materials
  - Independent lab evaluates
  - Certification body issues *Certificate*
  - Certificates released

Security certifications

The process

Common Criteria

- Certification that product adheres to some *Security Target**
  - Vendor pays and provides materials
  - Independent lab evaluates
  - Certification body issues *Certificate* and *Certification Report*
  - Certificates released and internationally recognized
- Security target might point to a *Protection Profile* instead
  - Common set of requirements for a product class (e.g. a firewall PP)

FIPS 140

- Certification that product adheres to some *Security Policy*
  - Vendor pays and provides materials
  - Independent lab evaluates
  - Certification body issues *Certificate*
  - Certificates released

All of these are public!

Référence du rapport de certification

ANSSI-CC-2012/23

Nom du produit

Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU

Référence/version du produit

- **Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005**
- **Athena IAS-ECC applet : version 3, correctif F9, build 2**
- **Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G**
- **Inside Secure Toolbox version: 00.03.11.05**

Conformité à un profil de protection

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04
[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté
AVA_VAN.5

Développeurs

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Inside Secure S.A.
Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom

Commanditaire

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

1. ST Introduction

1.1. ST Identification

ST title	- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet
Authors	Athena Smartcard, Inc.
General Status	Final version
ST Version Number	1.2
Date of production	March 22, 2012
TOE Reference	Mask Reference: "IDProtect_AT90SC28872RCU_005" IASECC Applet Athena Smartcard Solutions, Inc. AID A000000164494153454343010101 Version F903 Build 0002 ROM Code reference: "v0003 b0002" EEPROM Code Reference: "vF903 b0002" IDProtect Athena Smartcard Solutions, Inc. Release Date 0352 Release Level 0005 ROM Code reference: "IDProtect_AT90SC28872RCU_005" AT90SC28872RCU Inside Secure Revision G Identification Number AT58U07 Certificate BSI-DSZ-CC-0421-2008 [8] Ad-X Inside Secure Version 00.03.11.05 Certificate ANSSI-CC-2009/11 [9]
Common Criteria	CC version 3.1 Part 1: CCMB 2009-07-001 revision 3 [1] Part 2: CCMB 2009-07-002 revision 3 [2] Part 3: CCMB 2009-07-003 revision 3 [3]
PP Claim	Protection Profile — Secure Signature-Creation Device Type 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0005b Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0006b

[8] BSI-DSZ-CC-0421-2008 "*Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "*Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

Référence du rapport de certification

ANSSI-CC-2012/23

Nom du produit

Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU

Référence/version du produit

- **Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005**
- **Athena IAS-ECC applet : version 3, correctif F9, build 2**
- **Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G**
- **Inside Secure Toolbox version: 00.03.11.05**

Conformité à un profil de protection

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04
[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté
AVA_VAN.5

Développeurs

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Inside Secure S.A.
Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom

Commanditaire

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

1. ST Introduction

1.1. ST Identification

ST title	- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet
Authors	Athena Smartcard, Inc.
General Status	Final version
ST Version Number	1.2
Date of production	March 22, 2012
TOE Reference	Mask Reference: "IDProtect_AT90SC28872RCU_005" IASECC Applet Athena Smartcard Solutions, Inc. AID A000000164494153454343010101 Version F903 Build 0002 ROM Code reference: "v0003 b0002" EEPROM Code Reference: "vF903 b0002" IDProtect Athena Smartcard Solutions, Inc. Release Date 0352 Release Level 0005 ROM Code reference: "IDProtect_AT90SC28872RCU_005" AT90SC28872RCU Inside Secure Revision G Identification Number AT58U07 Certificate BSI-DSZ-CC-0421-2008 [8] Ad-X Inside Secure Version 00.03.11.05 Certificate ANSSI-CC-2009/11 [9]
Common Criteria	CC version 3.1 Part 1: CCMB 2009-07-001 revision 3 [1] Part 2: CCMB 2009-07-002 revision 3 [2] Part 3: CCMB 2009-07-003 revision 3 [3]
PP Claim	Protection Profile — Secure Signature-Creation Device Type 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0005b Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0006b

[8] BSI-DSZ-CC-0421-2008 "*Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "*Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

Référence du rapport de certification

ANSSI-CC-2012/23

Nom du produit

Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU

Référence/version du produit

- **Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005**
- **Athena IAS-ECC applet : version 3, correctif F9, build 2**
- **Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G**
- **Inside Secure Toolbox version: 00.03.11.05**

Conformité à un profil de protection

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04
[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté
AVA_VAN.5

Développeurs

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Inside Secure S.A.
Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom

Commanditaire

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

1. ST Introduction

1.1. ST Identification

ST title	- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet
Authors	Athena Smartcard, Inc.
General Status	Final version
ST Version Number	1.2
Date of production	March 22, 2012
TOE Reference	Mask Reference: "IDProtect_AT90SC28872RCU_005" IASECC Applet Athena Smartcard Solutions, Inc. AID A000000164494153454343010101 Version F903 Build 0002 ROM Code reference: "v0003 b0002" EEPROM Code Reference: "vF903 b0002" IDProtect Athena Smartcard Solutions, Inc. Release Date 0352 Release Level 0005 ROM Code reference: "IDProtect_AT90SC28872RCU_005" AT90SC28872RCU Inside Secure Revision G Identification Number AT58U07 Certificate BSI-DSZ-CC-0421-2008 [8] Ad-X Inside Secure Version 00.03.11.05 Certificate ANSSI-CC-2009/11 [9]
Common Criteria	CC version 3.1 Part 1: CCMB 2009-07-001 revision 3 [1] Part 2: CCMB 2009-07-002 revision 3 [2] Part 3: CCMB 2009-07-003 revision 3 [3]
PP Claim	Protection Profile — Secure Signature-Creation Device Type 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0005b Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0006b

[8] BSI-DSZ-CC-0421-2008 "*Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "*Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

Référence du rapport de certification

ANSSI-CC-2012/23

Nom du produit

Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU

Référence/version du produit

- **Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005**
- **Athena IAS-ECC applet : version 3, correctif F9, build 2**
- **Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G**
- **Inside Secure Toolbox version: 00.03.11.05**

Conformité à un profil de protection

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04
[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté
AVA_VAN.5

Développeurs

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Inside Secure S.A.
Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom

Commanditaire

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

1. ST Introduction

1.1. ST Identification

ST title	- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet
Authors	Athena Smartcard, Inc.
General Status	Final version
ST Version Number	1.2
Date of production	March 22, 2012
TOE Reference	Mask Reference: "IDProtect_AT90SC28872RCU_005" IASECC Applet Athena Smartcard Solutions, Inc. AID A000000164494153454343010101 Version F903 Build 0002 ROM Code reference: "v0003 b0002" EEPROM Code Reference: "vF903 b0002" IDProtect Athena Smartcard Solutions, Inc. Release Date 0352 Release Level 0005 ROM Code reference: "IDProtect_AT90SC28872RCU_005" AT90SC28872RCU Inside Secure Revision G Identification Number AT58U07 Certificate BSI-DSZ-CC-0421-2008 [8] Ad-X Inside Secure Version 00.03.11.05 Certificate ANSSI-CC-2009/11 [9]
Common Criteria	CC version 3.1 Part 1: CCMB 2009-07-001 revision 3 [1] Part 2: CCMB 2009-07-002 revision 3 [2] Part 3: CCMB 2009-07-003 revision 3 [3]
PP Claim	Protection Profile — Secure Signature-Creation Device Type 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0005b Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0006b

[8] BSI-DSZ-CC-0421-2008 "*Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "*Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

Référence du rapport de certification

ANSSI-CC-2012/23

Nom du produit

Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU

Référence/version du produit

- **Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005**
- **Athena IAS-ECC applet : version 3, correctif F9, build 2**
- **Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G**
- **Inside Secure Toolbox version: 00.03.11.05**

Conformité à un profil de protection

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04
[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté
AVA_VAN.5

Développeurs

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Inside Secure S.A.
Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom

Commanditaire

Athena Smartcard Solutions Inc.
1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

1. ST Introduction

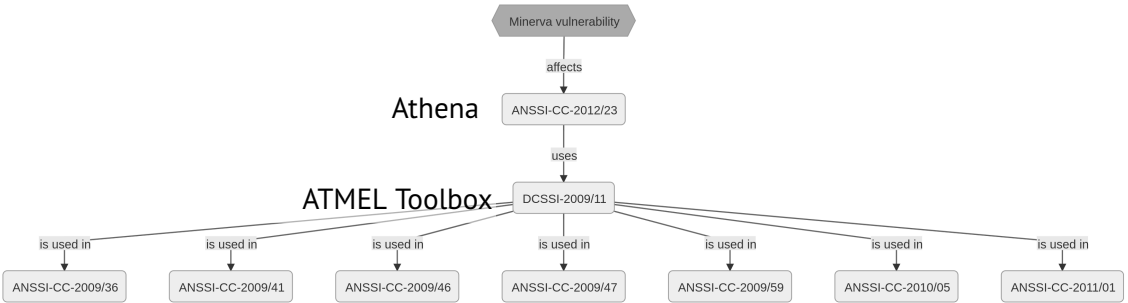
1.1. ST Identification

ST title	- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet
Authors	Athena Smartcard, Inc.
General Status	Final version
ST Version Number	1.2
Date of production	March 22, 2012
TOE Reference	Mask Reference: "IDProtect_AT90SC28872RCU_005" IASECC Applet Athena Smartcard Solutions, Inc. AID A000000164494153454343010101 Version F903 Build 0002 ROM Code reference: "v0003 b0002" EEPROM Code Reference: "vF903 b0002" IDProtect Athena Smartcard Solutions, Inc. Release Date 0352 Release Level 0005 ROM Code reference: "IDProtect_AT90SC28872RCU_005" AT90SC28872RCU Inside Secure Revision G Identification Number AT58U07 Certificate BSI-DSZ-CC-0421-2008 [8] Ad-X Inside Secure Version 00.03.11.05 Certificate ANSSI-CC-2009/11 [9]
Common Criteria	CC version 3.1 Part 1: CCMB 2009-07-001 revision 3 [1] Part 2: CCMB 2009-07-002 revision 3 [2] Part 3: CCMB 2009-07-003 revision 3 [3]
PP Claim	Protection Profile — Secure Signature-Creation Device Type 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0005b Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0006b

[8] BSI-DSZ-CC-0421-2008 "*Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "*Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices*". CC v2.3, EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

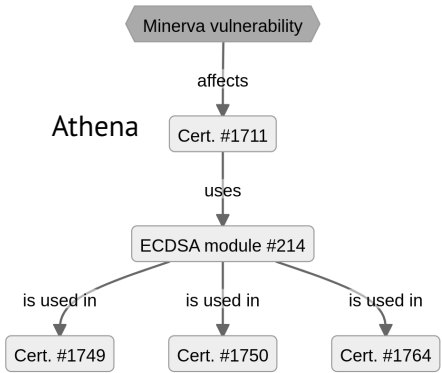
Back to Minerva: CC



Note

* The **Fast** functions of M10.3, M10.4, M10.5, M10.7, M10.8, M10.9, do not offer any DPA/SPA protection and **must** not be used for secure data.

Back to Minerva: FIPS 140



Manual labor?

Volume

- CC $\sim$ 5k certificates
- FIPS 140 $\sim$ 4k certificates

Issues

- **No common format, written by people for people**
- No search
- Typos
- PDFs that are not PDFs
- Errors in data
- Scanned documents

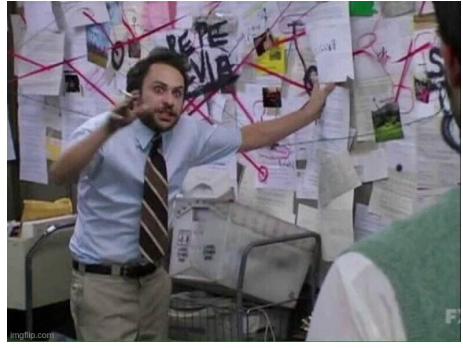
Manual labor?

Volume

- CC $\sim$ 5k certificates
- FIPS 140 $\sim$ 4k certificates

Issues

- **No common format, written by people for people**
- No search
- Typos
- PDFs that are not PDFs
- Errors in data
- Scanned documents

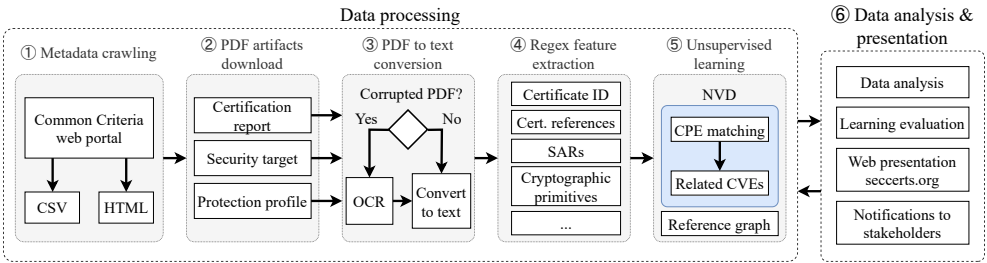


"There is no ~~Pepe Silvia~~."
Security Target

Automate!

seccerts

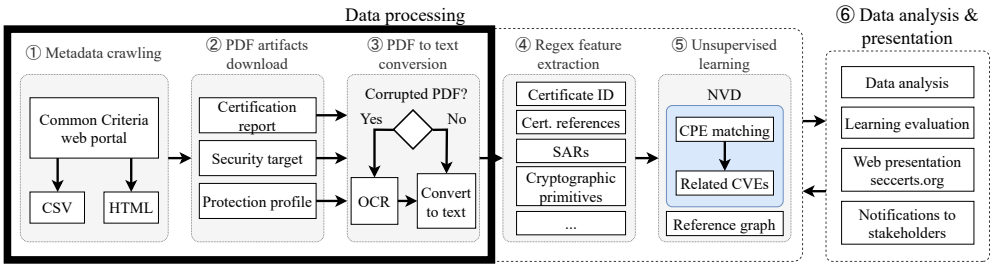
seccerts.org



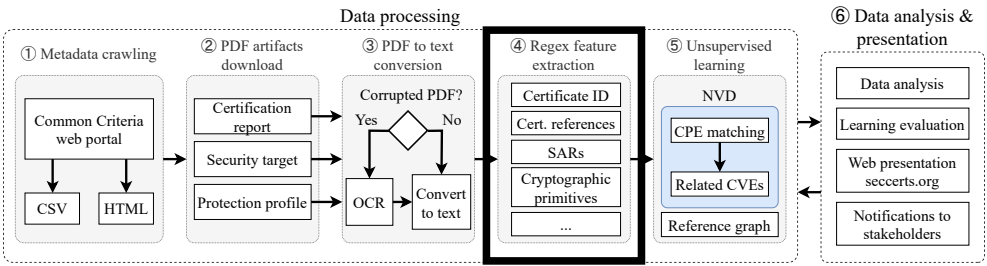
Automate!

seccerts

seccerts.org



Feature extraction



Feature extraction

Regular expressions

- Certification ID
- References to other certificates
- Security assurance requirements
- Security levels
- References to standards (ISO/IEC, ...)
- Cryptographic algorithms
- Elliptic curves
- Cryptographic libraries
- ...

PDF file metadata

Web metadata

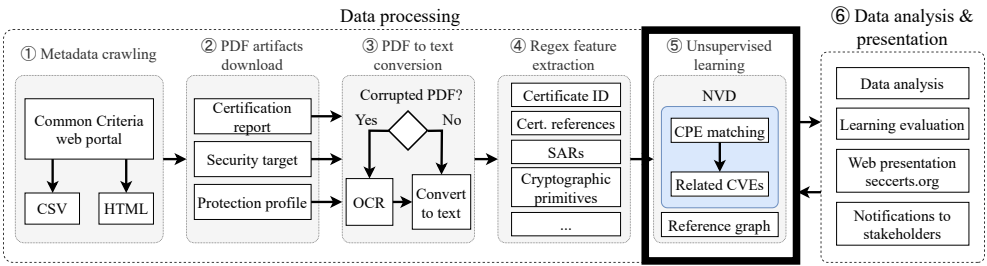
Limitations

- No context

Future work

- Try Natural Language Processing

Mapping of vulnerabilities



Mapping of vulnerabilities

- **Question**: Which certified products are affected by a given vulnerability?
- **Solution**: Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*

Mapping of vulnerabilities

- **Question**: Which certified products are affected by a given vulnerability?
- **Solution**: Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:
  `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`

Mapping of vulnerabilities

- **Question**: Which certified products are affected by a given vulnerability?
- **Solution**: Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:
  `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Example certificate name:
  `Infineon Technologies Security Controller M7793 A12 and G12 with optional RSA2048/4096 v1.02.010 or v1.02.013, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 libraries and with specific IC-dedicated software`

Mapping of vulnerabilities

- **Question**: Which certified products are affected by a given vulnerability?
- **Solution**: Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:
  `cpe:2.3:a:`**`infineon`**`:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Example certificate name:
  `Infineon` `Technologies Security Controller M7793 A12 and G12 with optional RSA2048/4096 v1.02.010 or v1.02.013, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 libraries and with specific IC-dedicated software`

Mapping of vulnerabilities

- **Question**: Which certified products are affected by a given vulnerability?
- **Solution**: Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:
  `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Example certificate name:
  Infineon Technologies Security Controller M7793 A12 and G12 with optional **RSA**2048/4096 v1.02.010 or v1.02.013, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 libraries and with specific IC-dedicated software

Mapping of vulnerabilities

- **Question**: Which certified products are affected by a given vulnerability?
- **Solution**: Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:
  `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Example certificate name:
  Infineon Technologies Security Controller M7793 A12 and G12 with optional **RSA**2048/4096 v1.02.010 or v1.02.013, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 **libraries** and with specific IC-dedicated software

Mapping of vulnerabilities

- **Question**: Which certified products are affected by a given vulnerability?
- **Solution**: Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:
  `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Example certificate name:
  Infineon Technologies Security Controller M7793 A12 and G12 with optional **RSA**2048/4096 v1.02.010 or **v1.02.013**, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 **libraries** and with specific IC-dedicated software

Mapping of vulnerabilities

- **Question**: Which certified products are affected by a given vulnerability?
- **Solution**: Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:
  `cpe:2.3:a:`**`infineon`**`:`**`rsa_library`**`:`**`1.02.013`**`:*:*:*:*:*:*:*`
- Example certificate name:
  `Infineon` `Technologies Security Controller M7793 A12 and G12 with optional` **`RSA`**`2048/4096 v1.02.010 or` **`v1.02.013`**`, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013` **`libraries`** `and with specific IC-dedicated software`
- *"…using token-set-ratio and partial-ratio metrics from RapidFuzz."*

Mapping of vulnerabilities

Evaluation

- Vulnerabilities: 376 out of 5129 CC certificates
- Vulnerabilities: 278 out of 4342 FIPS 140 certificates
- Manually evaluated precision $\sim$ 89%
- Limitations:
  - CPE <-> Name match only
  - No configuration details
  - Noisy data

Mapping of vulnerabilities

Security

- **Question**: Do certifications help security?

Mapping of vulnerabilities

- **Question**: Do certifications help security?
- **Easier question**: Do higher assurance levels lead to less (severe) vulnerabilities?

Mapping of vulnerabilities

- **Question**: Do certifications help security?
- **Easier question**: Do higher assurance levels lead to less (severe) vulnerabilities?
- **Easier question**: Do higher assurance levels correlate with less (severe) vulns?

Mapping of vulnerabilities

Security

- **Question**: Do certifications help security?
- **Easier question**: Do higher assurance levels lead to less (severe) vulnerabilities?
- **Easier question**: Do higher assurance levels correlate with less (severe) vulns?
- Luckily they do (slightly):

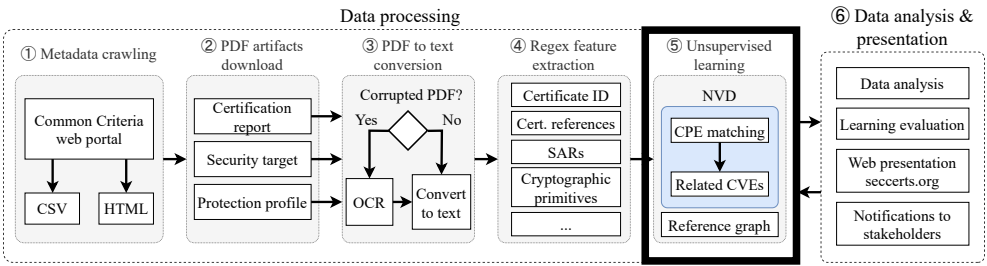
Common Criteria EAL

- $\rho = -0.03$ ( ) with number
- $\rho = -0.35$ (*) with severity

FIPS 140-2 Level

- $\rho = -0.70$ (*) with number
- $\rho = -0.36$ (*) with severity

Certificate references



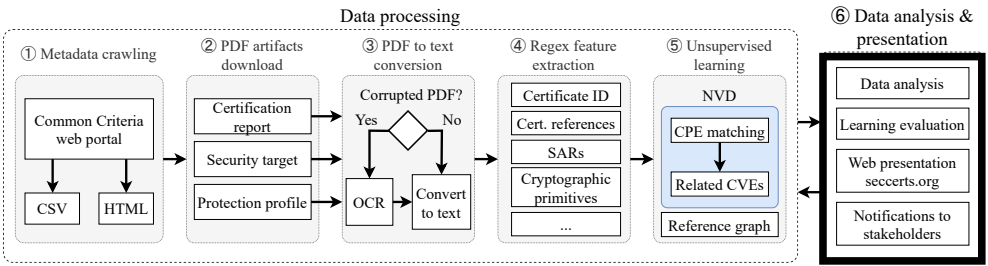
Certificate references

- **Question**: What (and why do) certificates refer to other certificates?
- **Solution** (partial): Extract certificate IDs via regex, canonicalize

Certificate references

- **Question**: What **(and why do)** certificates refer to other certificates?
- **Solution** (partial): Extract certificate IDs via regex, canonicalize
- The **reasons** are a hard problem
  - Component
  - Re-certification
  - Simultaneous certification
  - …
- **Future work**: Try Natural Language Processing

Data analysis



Data analysis

Temporal evolution

CC

FIPS 140

In process

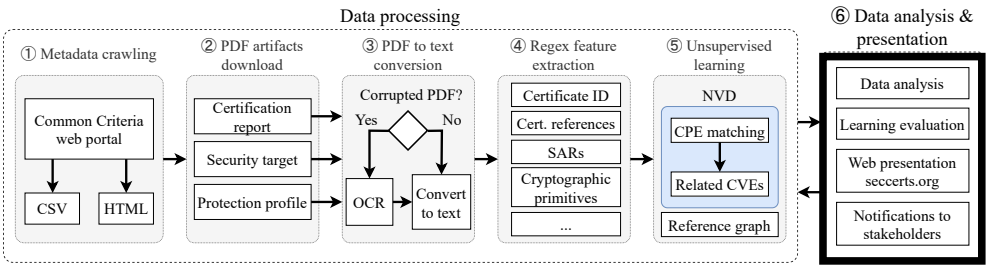
FIPS 140
MIP & IUT

Vulnerabilities

CC

FIPS 140

Web frontend



Web frontend

seccerts.org

- Browsing
  - CC and FIPS 140 certificates
- Search and filtering
  - Full-text search of certification documents
- Data
  - Daily updates
  - JSON export available
- Notifications
  - Subscribe via email
  - Notified on changes
  - Notified on new vulnerabilities

DEMO

Certificate

References

Use-cases

Vulnerability researchers

- Information on certified products

Use-cases

Vulnerability researchers

- Information on certified products

Evaluation labs

- Where the space is moving

Use-cases

Vulnerability researchers

- Information on certified products

Evaluation labs

- Where the space is moving

Vendors

- What competitors are doing

Use-cases

Vulnerability researchers

- Information on certified products

Evaluation labs

- Where the space is moving

Vendors

- What competitors are doing

End-users

- Notification for vulnerabilities

Takeaways

- Our tooling can do a lot of things
  - Vulnerability mapping & notification
  - Data analysis, Web frontend, …

Takeaways

- Our tooling can do a lot of things
  - Vulnerability mapping & notification
  - Data analysis, Web frontend, …
- We want your input on what it should do
  - Insight from "insiders" of certification ecosystem is priceless
  - We are all outsiders

Takeaways

- Our tooling can do a lot of things
  - Vulnerability mapping & notification
  - Data analysis, Web frontend, …
- We want your input on what it should do
  - Insight from "insiders" of certification ecosystem is priceless
  - We are all outsiders
- We have some input too
  - Assign robust cert IDs
  - Specify evaluated product boundaries more clearly
  - Pre-assign platform records to certificates (CPEs)
  - Create a component structure for composite products
  - Improve data quality & provide machine readable data

seccerts.org

Thanks!

J08nY | neuromancer.sk | jan@neuromancer.sk

Icons from **Font Awesome**

Photos from Unsplash

Resources

- https://unsplash.com/photos/9V5GssdEG-4
- https://unsplash.com/photos/snNHKZ-mGfE
- https://imgflip.com/memegenerator/74331809/Pepe-Silvia
- https://unsplash.com/photos/pAyN5zqdqDo
- https://www.dreamstime.com/sorry-i-spent-all-your-money-clumsy-good-looking-male-shrugging-holding-smartphone-credit-card-feeling-awkward-smiling-image113566709
- https://github.com/maxbachmann/RapidFuzz

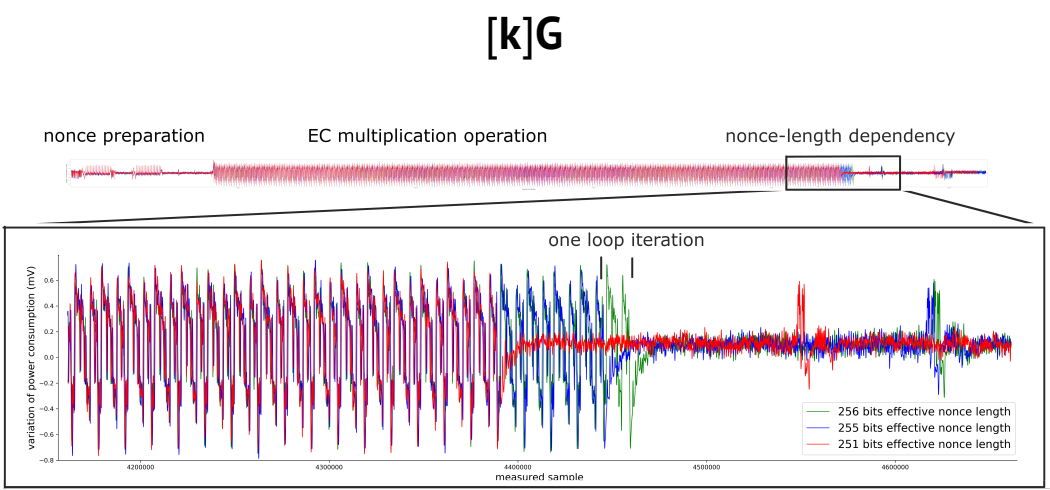
Minerva

Tested implementations

Type	Name	Version/Model	Scalar multiplier	Leakage
Library	OpenSSL	1.1.1d	Montgomery ladder	no
	BouncyCasle	1.58	Comb method	no
	SunEC	JDK 7 - JDK 12	Window-NAF	no
			Lopez-Dahab ladder	yes*
	WolfSSL	4.0.0	Sliding window	yes
	BoringSSL	974f4dddf	Window method	no
	libtomcrypt	v1.18.2	Sliding window	no
	libgcrypt	1.8.4	Double-and-add	yes*
	Botan	2.11.0	Window method	no
	Microsoft CNG	10.0.17134.0	Window method	no
	mbedTLS	2.16.0	Comb method	no
	MatrixSSL	4.2.1	Sliding window	yes
	Intel PP Crypto	2020	Window-NAF	no
	Crypto++	8.2	unknown	yes
Card	Athena IDProtect	010b.0352.0005	unknown	yes*
	NXP JCOP3	J2A081, J2D081, J3H145	unknown	no
	Infineon JTOP	52GLA080AL, SLE78	unknown	no
	G+D SmartCafe	v6, v7	unknown	no

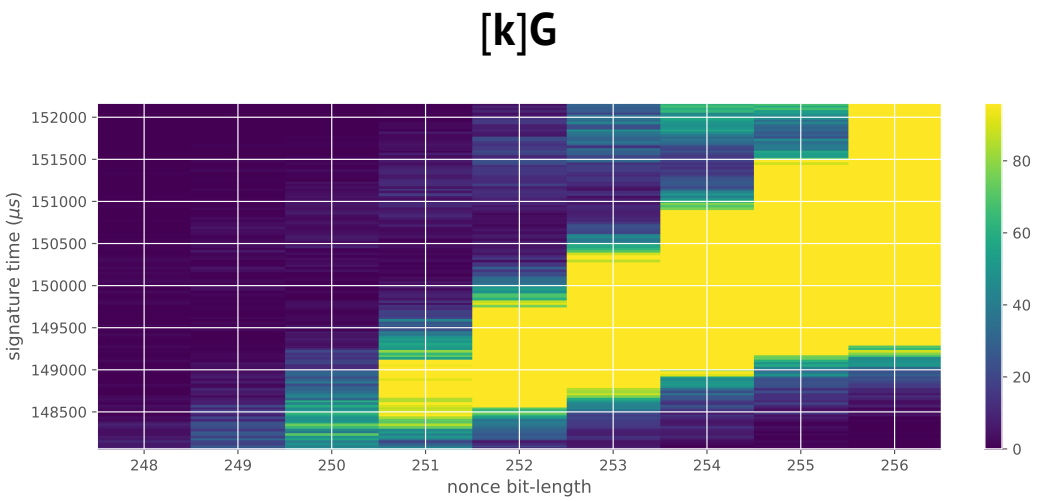
Minerva

Leak



Minerva

Leak



Minerva

Hidden Number Problem

- Average 1 LZB per signature
- There is noise

Minerva

Hidden Number Problem

- Average 1 LZB per signature
- There is noise

Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes

(Extended Abstract)

[1]

Dan Boneh[1]
Princeton University

Ramarathnam Venkatesan[2]
Bellcore

Minerva

Hidden Number Problem

- Average 1 LZB per signature
- There is noise

Hidden Number Problem (HNP) [1]

Given an oracle computing:

$$\mathcal{O}_{b,t}() = \mathrm{MSB}_l(at + b \bmod n)$$

with t u.i.d. in $\mathbb{Z}_n^*$, find a.

Minerva

Hidden Number Problem

- Average 1 LZB per signature
- There is noise

Hidden Number Problem (HNP) [1]

Given an oracle computing:

$$\mathcal{O}_{r,s}() = \mathrm{MSB}_l(k \bmod n)$$

Minerva

Hidden Number Problem

- Average 1 LZB per signature
- There is noise

Hidden Number Problem (HNP) [1]

Given an oracle computing:

$$\mathcal{O}_{r,s}() = \mathrm{MSB}_l(xs^{-1}r + H(m)s^{-1} \bmod n)$$

find x.

Minerva

Basic attack

- Collect N signatures, take d of the fastest

Minerva

Basic attack

- Collect N signatures, take d of the fastest
- Assume some bounds l_i: $|k_i| = |xt_i - u_i| = |xs_i^{-1}r_i + H(m_i)s_i^{-1}| < n/2^{l_i}$

Minerva

Basic attack

- Collect N signatures, take d of the fastest
- Assume some bounds l_i: $|k_i| = |xt_i - u_i| = |xs_i^{-1}r_i + H(m_i)s_i^{-1}| < n/2^{l_i}$
- Construct a lattice with basis $\mathbf{B}$ and reduce it:

$$\mathbf{B} = \begin{pmatrix} 2^{l_1}n & 0 & 0 & \dots & 0 & 0 \\ 0 & 2^{l_2}n & 0 & \dots & 0 & 0 \\ & \vdots & & & \vdots & \\ 0 & 0 & 0 & \dots & 2^{l_d}n & 0 \\ 2^{l_1}t_1 & 2^{l_2}t_2 & 2^{l_3}t_3 & \dots & 2^{l_d}t_d & 1 \end{pmatrix}$$

Minerva

Basic attack

- Collect N signatures, take d of the fastest
- Assume some bounds l_i: $|k_i| = |xt_i - u_i| = |xs_i^{-1}r_i + H(m_i)s_i^{-1}| < n/2^{l_i}$
- Construct a lattice with basis $\mathbf{B}$ and reduce it:

$$\mathbf{B} = \begin{pmatrix} 2^{l_1}n & 0 & 0 & \dots & 0 & 0 \\ 0 & 2^{l_2}n & 0 & \dots & 0 & 0 \\ & \vdots & & & \vdots & \\ 0 & 0 & 0 & \dots & 2^{l_d}n & 0 \\ 2^{l_1}t_1 & 2^{l_2}t_2 & 2^{l_3}t_3 & \dots & 2^{l_d}t_d & 1 \end{pmatrix}$$

- Construct a target $\mathbf{u} = (2^{l_1}u_1, \dots, 2^{l_d}u_d, 0)$

Minerva

Basic attack

- Collect N signatures, take d of the fastest
- Assume some bounds l_i: $|k_i| = |xt_i - u_i| = |xs_i^{-1}r_i + H(m_i)s_i^{-1}| < n/2^{l_i}$
- Construct a lattice with basis $\mathbf{B}$ and reduce it:

$$\mathbf{B} = \begin{pmatrix} 2^{l_1}n & 0 & 0 & \dots & 0 & 0 \\ 0 & 2^{l_2}n & 0 & \dots & 0 & 0 \\ & \vdots & & & \vdots & \\ 0 & 0 & 0 & \dots & 2^{l_d}n & 0 \\ 2^{l_1}t_1 & 2^{l_2}t_2 & 2^{l_3}t_3 & \dots & 2^{l_d}t_d & 1 \end{pmatrix}$$

- Construct a target $\mathbf{u} = (2^{l_1}u_1, \dots, 2^{l_d}u_d, 0)$
- Solve CVP($\mathbf{B}, \mathbf{u}$). The closest lattice point is often: $\mathbf{v} = (2^{l_1}t_1x, \dots, 2^{l_d}t_dx, x)$

Minerva

Basic attack

- Collect N signatures, take d of the fastest
- Assume some bounds l_i: $|k_i| = |xt_i - u_i| = |xs_i^{-1}r_i + H(m_i)s_i^{-1}| < n/2^{l_i}$
- Construct a lattice with basis $\mathbf{B}$ and reduce it:

$$\mathbf{B} = \begin{pmatrix} 2^{l_1}n & 0 & 0 & \dots & 0 & 0 \\ 0 & 2^{l_2}n & 0 & \dots & 0 & 0 \\ & \vdots & & & \vdots & \\ 0 & 0 & 0 & \dots & 2^{l_d}n & 0 \\ 2^{l_1}t_1 & 2^{l_2}t_2 & 2^{l_3}t_3 & \dots & 2^{l_d}t_d & 1 \end{pmatrix}$$

- Construct a target $\mathbf{u} = (2^{l_1}u_1, \dots, 2^{l_d}u_d, 0)$
- Solve CVP($\mathbf{B}, \mathbf{u}$). The closest lattice point is often: $\mathbf{v} = (2^{l_1}t_1x, \dots, 2^{l_d}t_dx, x)$
- Because $\forall i$: $(xt_i - u_i) \mod n$ is small