Nástroje pro verifikaci bezpečnosti kryptografických zařízení s využitím AI
Projekt výzvy MVČR Impakt VJ02010010

Průběžná prezentace výsledků pro NUKIB, CRoCS@FI Masarykova univerzita

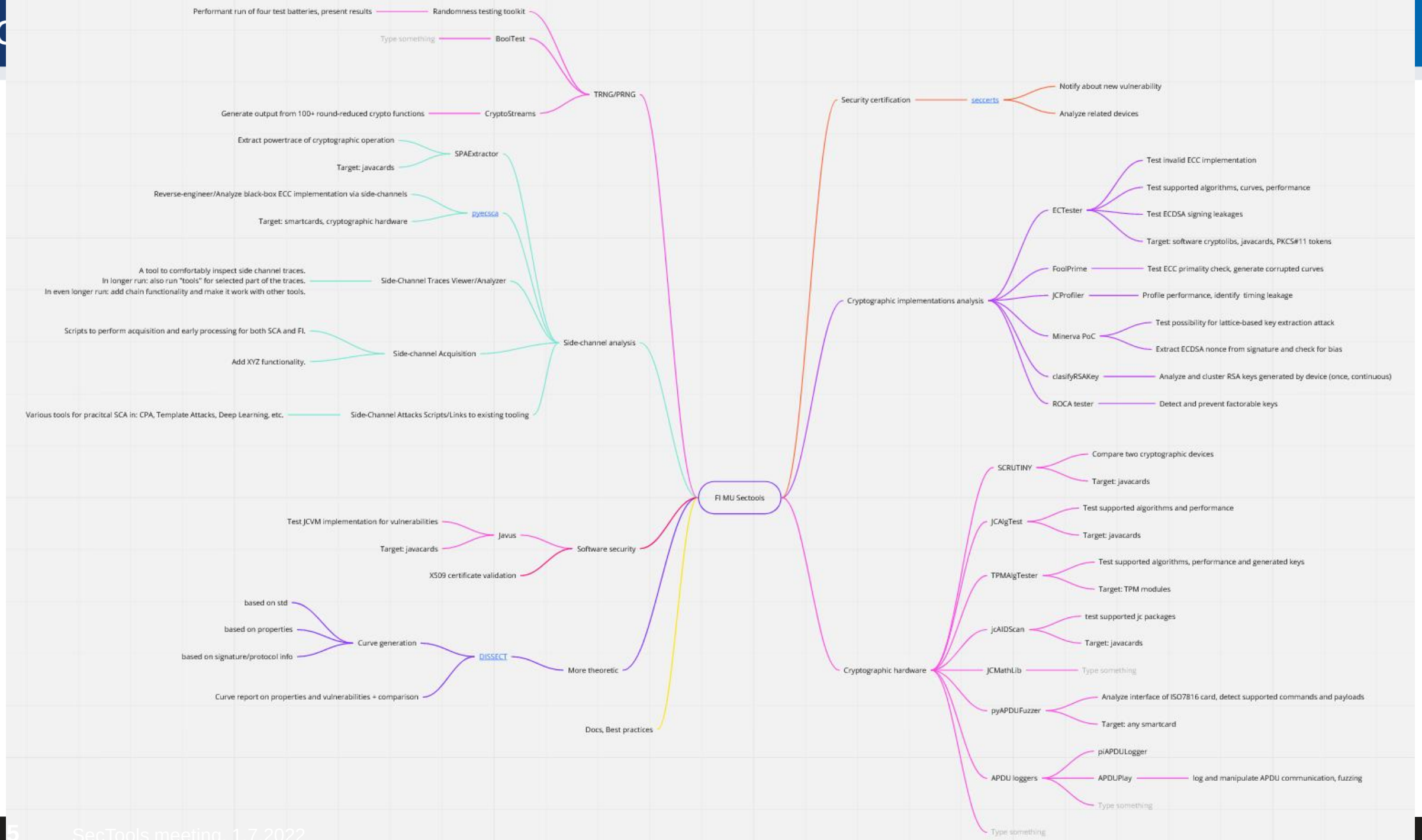
Praha 1.7.2022

CROCS
Centre for Research on Cryptography and Security

Rok 2022

#	Činnost	Odpovědná skupina	Délka činnosti											
			1	2	3	4	5	6	7	8	9	10	11	12
	2022													
3	Analýzu stávajících certifikačních reportů schémat Common Criteria a NIST FIPS 140-2/3	MU	×	×	×	×	×	×						
4	Analýza a volba kryptografických primitiv pro SW implementaci, návrh programového vybavení pro analýzu implementací kryptografických algoritmů pro SW čipových karet.	MU							×	×	×	×	×	×

ANALYSIS OF CRYPTOGRAPHIC IMPLEMENTATIONS


FI MU Sectools
TRNG/PRNG
Randomness testing toolkit
Performant run of four test batteries, present results
BoolTest
Type something
CryptoStreams
Generate output from 100+ round-reduced crypto functions
Side-channel analysis
SPAExtractor
Extract powertrace of cryptographic operation
Target: javacards
pyecsca
Reverse-engineer/Analyze black-box ECC implementation via side-channels
Target: smartcards, cryptographic hardware
Side-Channel Traces Viewer/Analyzer
A tool to comfortably inspect side channel traces.
In longer run: also run "tools" for selected part of the traces.
In even longer run: add chain functionality and make it work with other tools.
Side-channel Acquisition
Scripts to perform acquisition and early processing for both SCA and FI.
Add XYZ functionality.
Side-Channel Attacks Scripts/Links to existing tooling
Various tools for pracitcal SCA in: CPA, Template Attacks, Deep Learning, etc.
Software security
Javus
Test JCVM implementation for vulnerabilities
Target: javacards
X509 certificate validation
More theoretic
DISSECT
Curve generation
based on std
based on properties
based on signature/protocol info
Curve report on properties and vulnerabilities + comparison
Docs, Best practices
Security certification
seccerts
Notify about new vulnerability
Analyze related devices
Cryptographic implementations analysis
ECTester
Test invalid ECC implementation
Test supported algorithms, curves, performance
Test ECDSA signing leakages
Target: software cryptolibs, javacards, PKCS#11 tokens
FoolPrime
Test ECC primality check, generate corrupted curves
JCProfiler
Profile performance, identify timing leakage
Minerva PoC
Test possibility for lattice-based key extraction attack
Extract ECDSA nonce from signature and check for bias
clasifyRSAKey
Analyze and cluster RSA keys generated by device (once, continuous)
ROCA tester
Detect and prevent factorable keys
Cryptographic hardware
SCRUTINY
Compare two cryptographic devices
Target: javacards
JCAlgTest
Test supported algorithms and performance
Target: javacards
TPMAlgTester
Test supported algorithms, performance and generated keys
Target: TPM modules
jcAIDScan
test supported jc packages
Target: javacards
JCMathLib
Type something
pyAPDUFuzzer
Analyze interface of ISO7816 card, detect supported commands and payloads
Target: any smartcard
APDU loggers
piAPDULogger
APDUPlay
log and manipulate APDU communication, fuzzing
Type something
Type something

Parameters to consider

- Development phase: new implementation, analysis of an existing one
- Analysis model: whitebox, graybox, blackbox
- Inspection setup: only software, hw probes, computational power
- Attacker model: logical, time/power side-channel, fault induction
- Target device: smartcard, MCU, SoC, CPU, FPGA
- User: product developer, (NUKIB) lab, third-party lab, end-user
- Cryptography targeted: symmetric, asymmetric, PQC, whole protocol

- Anything else?

Parameters to consider

- Development phase: new implementation, analysis of an existing one
- Analysis model: whitebox, graybox, blackbox
- Inspection setup: only software, hw probes, computational power
- Attacker model: logical, time/power side-channel, fault induction
- Target device: smartcard, MCU, SoC, CPU, FPGA
- User: product developer, (NUKIB) lab, third-party lab, end-user
- Cryptography targeted: symmetric, asymmetric, PQC, whole protocol

- Anything else?

Main focus domains + projects

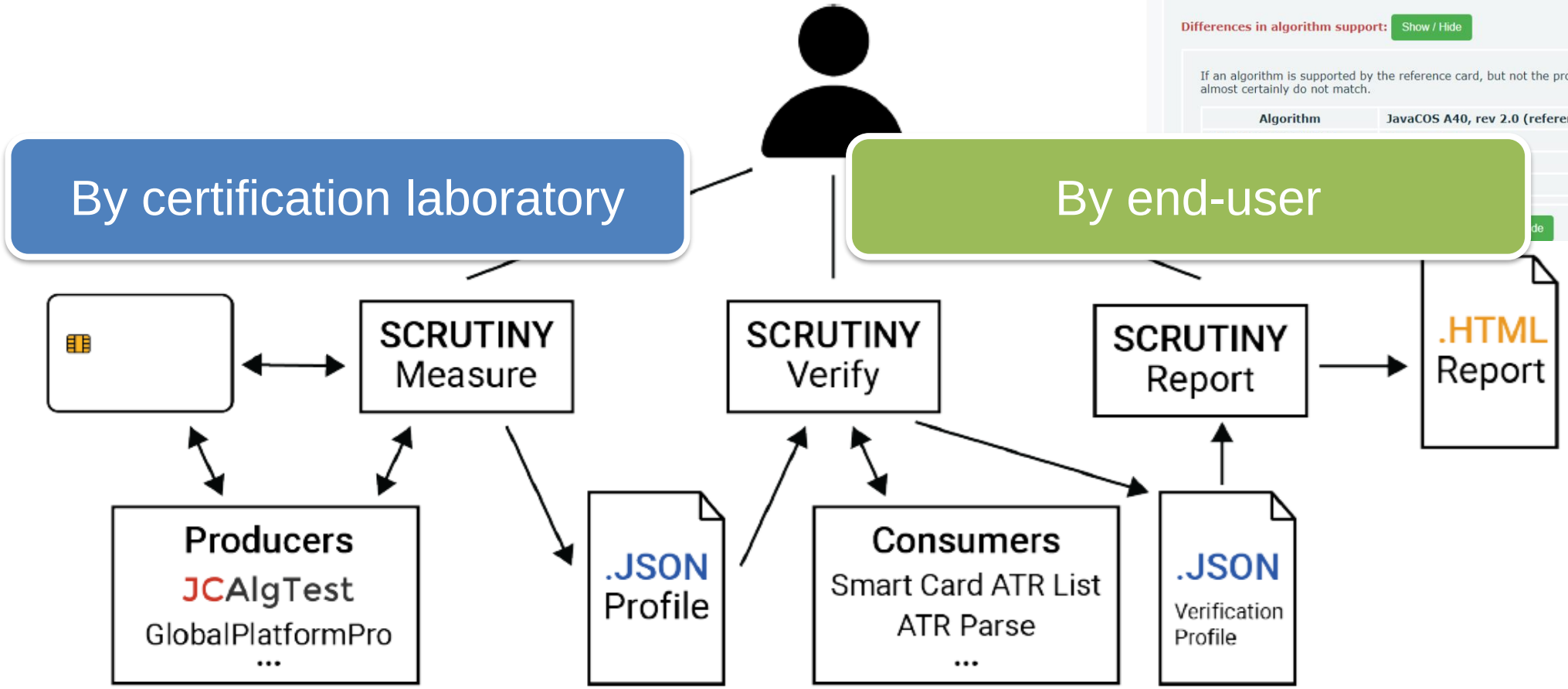
- Forensic profile of cryptographic device
  - SCRUTINY: Compare and visualize difference between target and expected profile
  - {JC/TPM}AlgTest: algs, performance and crypto assessment
  - SPAExtractor: Database of powertraces, pattern matching
  - co_template_finder: Finding (crypto) operation with repeating structure

- Analysis of cryptographic implementations
  - ECTester: EC implementation testsuit (cards+swlibs)
  - Javus: matrix testing of JavaCard VM security implementation
  - DISSECT: Verification of claimed EC curve selection process

Main focus domains + projects

- Randomness testing
  - BoolTest: new performant testing battery
  - RTT: distributed and high-performance RNG testing with unified interface for STS NIST, Dieharder, TestU01, BoolTest
- Analysis of cryptographic keys
  - Extraction of keys from real-world sources (TLS, CT, blockchain, hardware wallets)
  - ECC and RSA keys, bias detection, classification of source library
- Constant-time crypto analysis/verification tools
  - Survey on all existing tools, usability (developer) aspects (S&P 2022)
  - Application on cryptographic libraries (NSS)
  - JCProfiler: performance and constant-time analysis for JavaCards

https://github.com/crocs-muni/scrutiny/



Module: ATR

Show / Hide

Module: Algorithm Support

Algorithm Support comparison results

This module compares Java Card algorithm suppo

Overview:

The cards match in 4387 algorithms.

There are 2 algorithms with missing results for ei

There are 3 algorithms with different results.

There are 4 algorithms with suspicious difference

Differences in algorithm support: Show / Hid

If an algorithm is supported by the reference card, but n
almost certainly do not match.

Algorithm	JavaCOS A40, rev 2.0
ALG_DES_CBC_NOPAD	Unsupported
ALG_RSA_ISO14888	Unsupported
ALG_AES_CBC_ISO9797_M1	Supported

Differences in memory allocation during tests: Show /

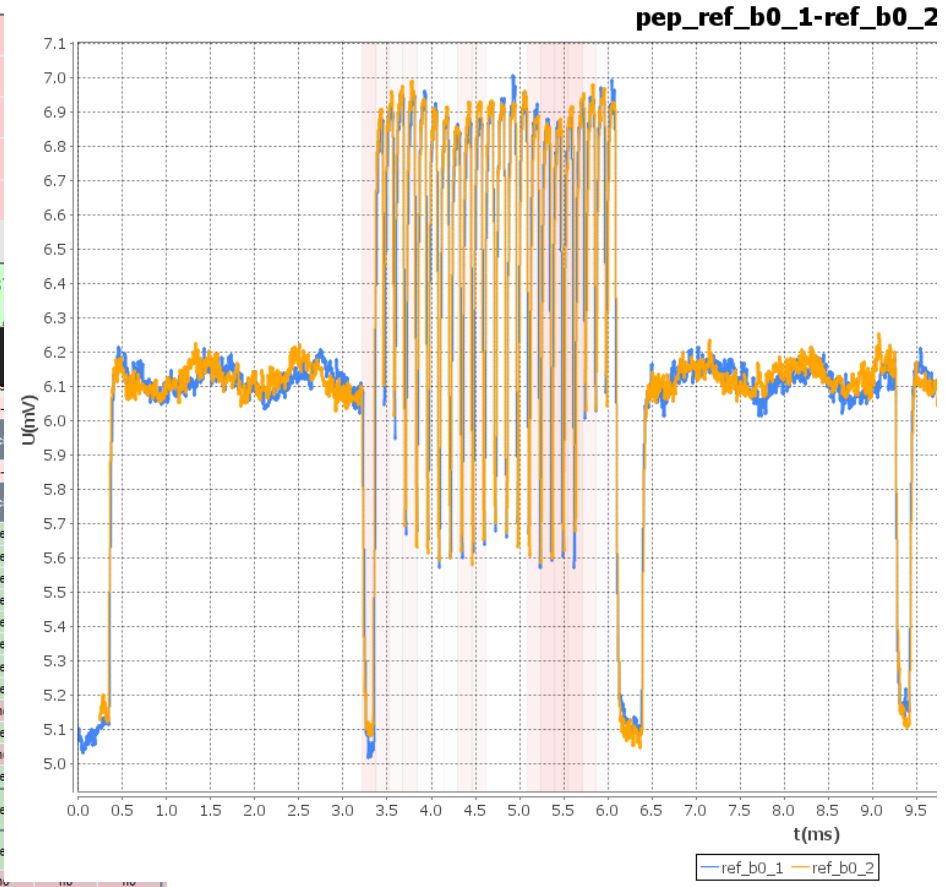
$\mathbb{F}_p$ performance

The following table shows performance of tested cards in ECDH and ECDSA over popular $\mathbb{F}_p$ curve sizes. Key generation performance is similar to ECDH performance. ECDSA timings are split for sign+verify operations. Times are in milliseconds.

Card‡	Type *	Type †	192b ECDH	192b ECDSA	256b ECDH	256b ECDSA	384b ECDH	384b ECDSA	521b ECDH	521b ECDSA
ACS ACOSJ 40K	1	a	172	254+257	209	311+315	360	503+536	✗	
	2	b	172	255+256	209	311+316	360	505+535	✗	
	3	c	172	254+257	209	311+315	360	505+537	✗	
	4	d	172	255+261	210	310+316	360	505+537	✗	
	5	e	✗	255+260	✗	311+315	✗	505+538	✗	
	6		✗		✗		✗		✗	
Athena IDProtect	1	a	147	110+163	209	148+228	448	279+473	937	53

JCAlgTest

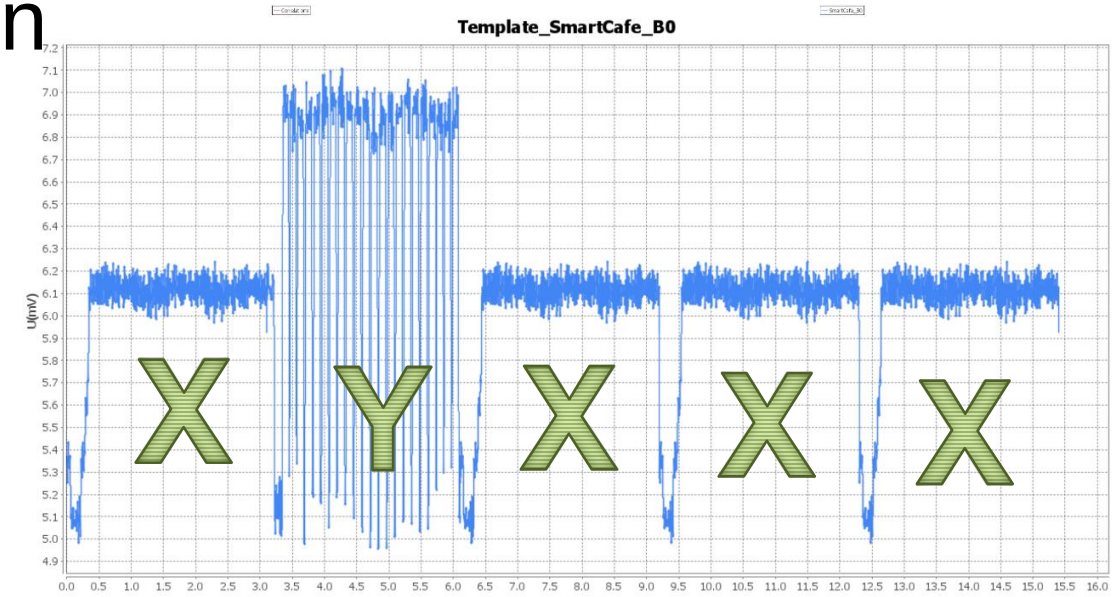
JCSystem.getMaxCommitCapacity()	2.1	-	-	-	-	-	-
javacardx.apdu.ExtendedLength	introduced in JC ver.	c0	c1	c2	c3	c4	c
Extended APDU	2.2.2	-	no	no	-	-	-
javacardx.crypto.Cipher	introduced in JC ver.	c0	c1	c2	c3	c4	c
ALG_DES_CBC_NOPAD	≤2.1	yes	yes	yes	yes	yes	ye
ALG_DES_CBC_ISO9797_M1	≤2.1	yes	yes	yes	yes	yes	ye
ALG_DES_CBC_ISO9797_M2	≤2.1	yes	yes	yes	yes	yes	ye
ALG_DES_CBC_PKCS5	≤2.1	no	no	no	yes	yes	ye
ALG_DES_ECB_NOPAD	≤2.1	yes	yes	yes	yes	yes	ye
ALG_DES_ECB_ISO9797_M1	≤2.1	yes	yes	yes	yes	yes	ye
ALG_DES_ECB_ISO9797_M2	≤2.1	yes	yes	yes	yes	yes	ye
ALG_DES_ECB_PKCS5	≤2.1	no	no	no	yes	yes	ye
ALG_RSA_ISO14888	≤2.1	no	no	no	no	no	n
ALG_RSA_PKCS1	≤2.1	yes	yes	yes	yes	yes	ye
ALG_RSA_ISO9796	≤2.1	no	no	no	no	no	n
ALG_RSA_NOPAD	2.1.1	yes	yes	yes	yes	yes	ye
ALG_AES_BLOCK_128_CBC_NOPAD	2.2.0	yes	no	suspicious yes	yes	yes	ye
ALG_AES_BLOCK_128_ECB_NOPAD	2.2.0	yes	no	suspicious yes	yes	yes	ye
ALG_RSA_PKCS1_OAEP	2.2.0	no	no	no	no	no	n
ALG_KOREAN_SEED_ECB_NOPAD	2.2.2	yes	no	no	yes	yes	yes	yes	yes
ALG_KOREAN_SEED_CBC_NOPAD	2.2.2	yes	no	no	yes	yes	yes	yes	yes
ALG_AES_BLOCK_192_CBC_NOPAD	3.0.1	no	-	-	no	no	no	no	no
ALG_AES_BLOCK_192_ECB_NOPAD	3.0.1	no	-	-	no	no	no	no	no
ALG_AES_BLOCK_256_CBC_NOPAD	3.0.1	no	-	-	no	no	no	no	no
ALG_AES_BLOCK_256_ECB_NOPAD	3.0.1	no	-	-	no	no	no	no	no



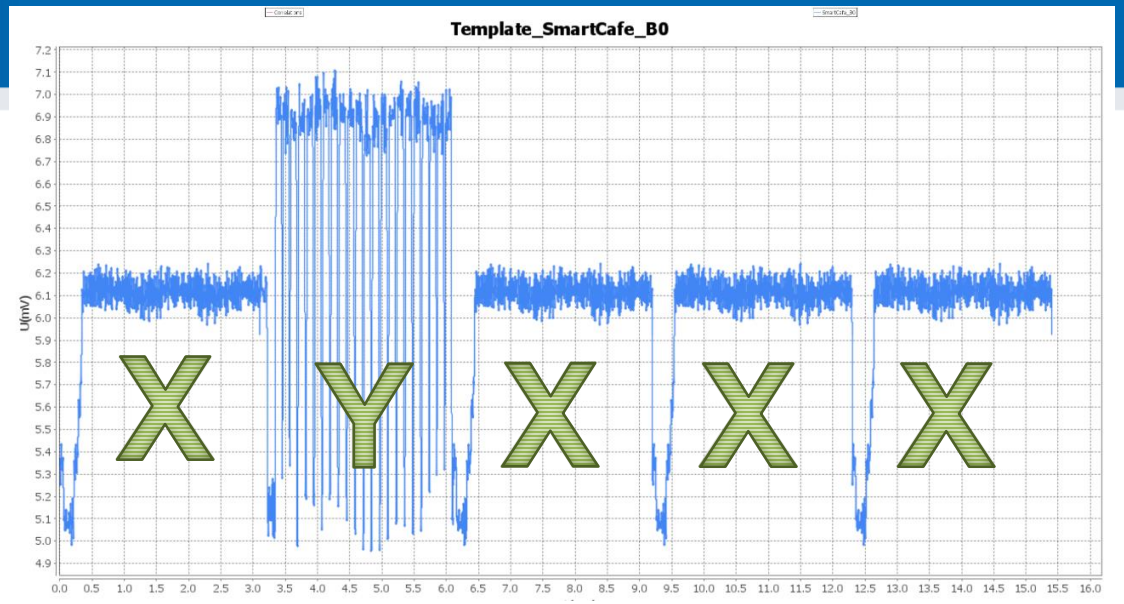
TRAUTMANN, Jens; BECKERS, Arthur; WOUTERS, Lennert; WILDERMANN, Stefan; VERBAUWHEDE, Ingrid; TEICH, Jürgen. Semi-Automatic Locating of Cryptographic Operations in Side-Channel Traces. *IACR Transactions on Cryptographic Hardware and Embedded Systems*. 2022, pp. 345–366. Available from DOI: 10.46586/tches.v2022.i1.345-366.

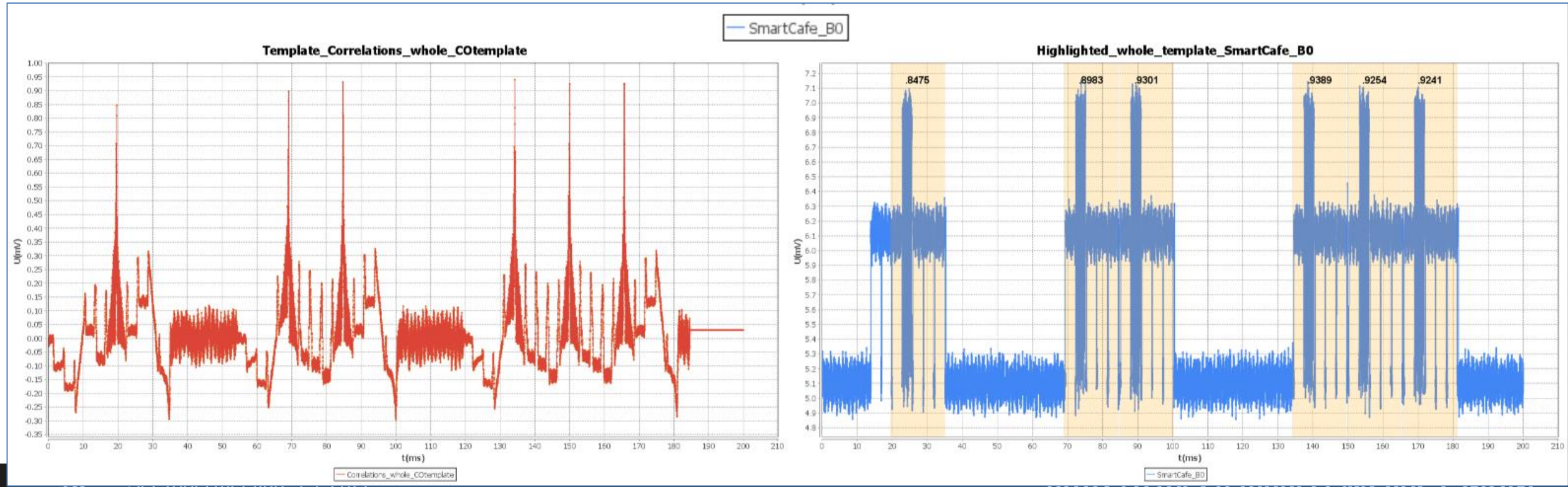
co_template_finder

- Search for specified repetition pattern
  - E.g., 10 rounds of AES,
  - No need for template operation
  - GPU speedup



(Master thesis, Martin Podhora)


Template_SmartCafe_B0
U(mV)
X Y X X X


SmartCafe_B0
Template_Correlations_whole_COtemplate
U(mV)
t(ms)
Correlations_whole_COtemplate
Highlighted_whole_template_SmartCafe_B0
.8475
.8983
.9301
.9389
.9254
.9241
U(mV)
t(ms)
SmartCafe_B0

Main focus domains: PA / EM

- (Lukasz Chmielewski, assistant prof @ FI, ex-Riscure SCA)
- Picoscope, XYZ stage, PA/EM probes
- Extension of open-source control scripts

Tentative proposal for the first phase

- We propose to focus on delivery of the following tools first:

- SCRUTINY: forensic profile of smartcard and comparison
- ECTester+DiSSECT: analysis of ECC implementation
- BoolTest: RNG randomness testing
- JCMathLib+JCProfiler: EC sw impl on JavaCard + on-card CT verif

SECCERTS.ORG PROJECT

Project discussion with application garant (NUKIB)

- 28.4.2022 Presentation for NUKIB in Prague
- 22.6.2022 Instruction to Python programmatic API (I. Trummova)
  - Importance of working with non-public documents
    - Solution: file specifying location of additional documents and pairing method
  - Importance of subset filtering (interest in selected products)

SECCERTS TOOL (OPEN-SOURCE)

1547 Certified Products by Category *		
Category	**Products**	**Archived**
Access Control Devices and Systems		
Biometric Systems and Devices	0	3
Boundary Protection Devices and Systems	40	184
Data Protection	61	139
Databases	12	75
Detection Devices and Systems	7	66
ICs, Smart Cards and Smart Card-Related Devices and Systems	560	913
Key Management Systems	6	46
Mobility		
Multi-Function Devices		
Network and Network-Related Devices and Systems		
Operating Systems		
Other Devices and Systems	233	523
Products for Digital Signatures	46	86
Trusted Computing	42	15
Totals:	**1547**	**3005**
Grand Total:		**4552**

** A Certified Product may have multiple Categories associated with it.*

Downloaded PDFs with reports, ST, updates

CC web (html)

CC web database (csv)

Frontpage (regex)

Keywords (regex)

Metadata (pdf)

Protection Profiles

Aggregate JSON with raw data

Pair corresponding data files

Normalize and clean data

Analysis and visualisations

Run custom analysis

- Processed data (json)
- Python SDK
- Web portal
- Reports

Plánované výstupy

- Analýza stávajících certifikačních reportů #3 (CC, FIPS140)
  - Primárním výsledkem je zpráva (**jaký jazyk?**)
    - Popis současného stavu Common Criteria a FIPS-140 certifikace, problémy
    - Identifikace zájmových oblastí (vývoj v čase, vliv zranitelností, notifikace)
  - Průběžně rozšiřovaný nástroj je již dostupný https://seccerts.org
- Výzkumný článek
  - **JCAlgTest: Robust identification metadata for certified smartcards**, Petr Svenda, Rudolf Kvasnovsky, Imrich Nagy, Antonin Dufka, SECRYPT 2022 (to appear), 2022.

MAPPING OF CC TO NATIONAL VULNERABILITY DATABASE - ADAM JANOVSKY