



SCRUTINY: more valuable and transparent security certifications

Open-source analysis tooling for crypto implementations
CHESS brokerage event, JIC, 5.2.2025

CRoCS team, [Petr Švenda](#)

Faculty of Informatics, Masaryk University, Czech Republic

CRoCS

Centre for Research on
Cryptography and Security



SCRUTINY: more valuable and transparent security certifications

Open-source analysis tooling for crypto implementations
CHES brokerage event, JIC, 5.2.2025

CRoCS team, [Petr Švenda](#)

Faculty of Informatics, Masaryk University, Czech Republic

Vendor



- Great understanding of target implementation (whitebox)
- Conflict between time-for-testing and time-to-market
- Motivated not-to-publish product details to protect own IP

Evallab



- Great knowledge in security testing, specialized equip., process knowledge
- But frequently unclear what exactly was tested and with what results
- Conflict between tough analysis and keeping vendor as a customer

Academia, security researchers



- Small understanding of target (blackbox)
- Great knowledge of *some* advanced attacks
- A lot of time, focus on publishable results
- Wide-scale testing, no single specific target

User



- Lack of knowledge, test outsourcing (certification)
- Do not know what was tested!

1. TRANSPARENCY PROBLEM

“How was the product tested, and with what results?”

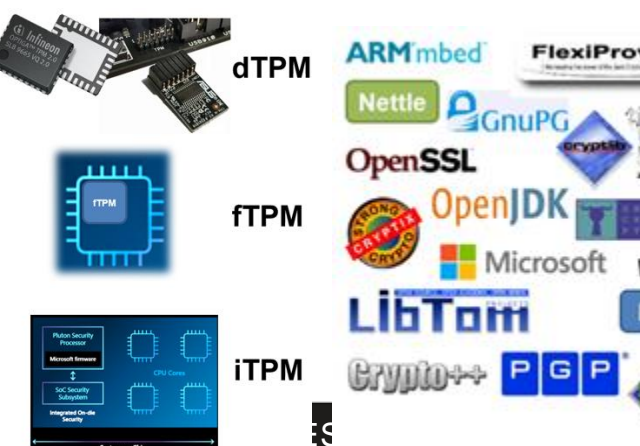
2. DISCOVERABILITY PROBLEM

“How to find the results relevant for given product?”

PRODUCTS FOR TESTING

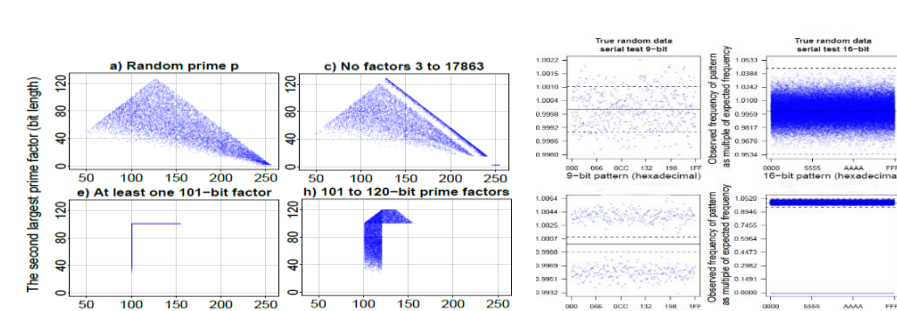
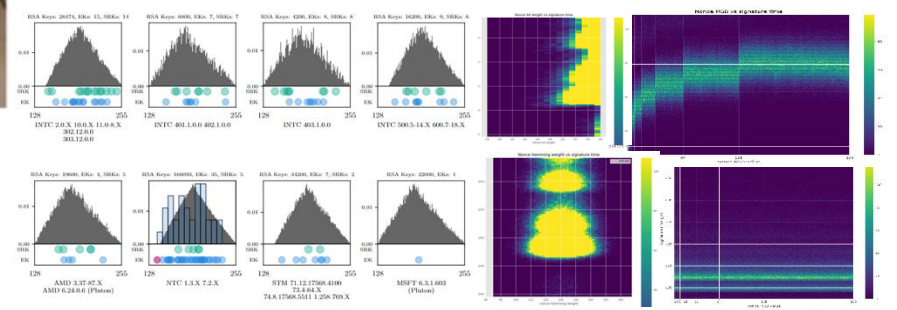
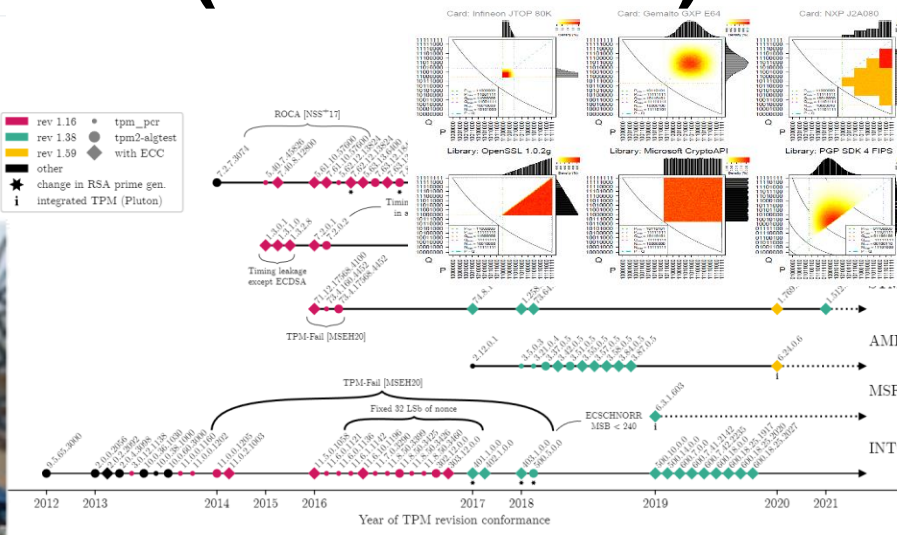
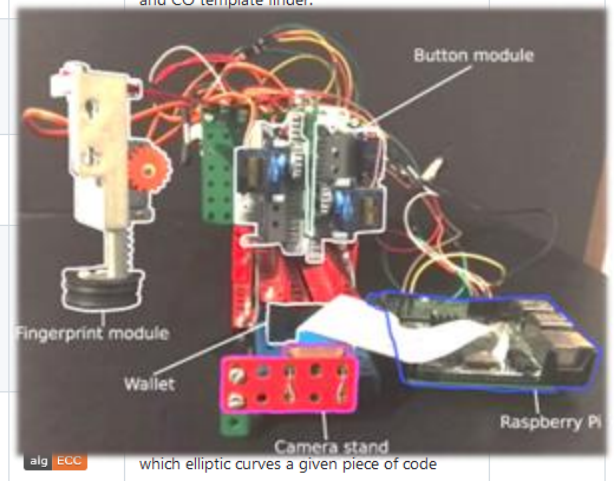
OPEN-SOURCE TOOLING

OPEN TEST RESULTS (METADATA)



README MIT license

Tool	Repo stats	Target domain	Info	Notes
JCAIqTest	Stars: 115 Contributors: 16	platform: javacard alg: RSA alg: ECC	Automated testing tool for algorithms from JavaCard API supported by particular smart card. Performance testing of almost all available methods. The results for more than 1000 smart cards.	
jcAIDScan	Stars: 8 Contributors: 3			
GlobalPlatformPro tool	Stars: 730 Contributors: 30			
TPMAIqTest	Stars: 6 Contributors: 8			
scrutiny-power-traces-analyzer	Stars: 3 Contributors: 2			
JCMathLib - ECPoint library	Stars: 86 Contributors: 6			
ECTester	Stars: 66 Contributors: 7			
pyecdsa	Stars: 56 Contributors: 9			
ec-detector	Stars: 1 Contributors: 5	alg: ECC	which elliptic curves a given piece of code	



1. TRANSPARENCY PROBLEM

“How was the product tested, and with what results?”

2. DISCOVERABILITY PROBLEM

“How to find the results relevant for a given product?”

PRODUCTS

BINDINGS

METADATA

Infineon M7794A12
 BSI-DSZ-CC-0814-2012
 CC EAL4+




CSV information

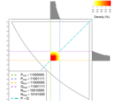

Status	archived
Valid from	26.07.2012
Valid until	01.09.2019
Scheme	DE
Manufacturer	Infinion Technologies AG
Category	ICs, Smart Cards and Smart Card-Related Devices and Systems
Security level	AVA_VAN.5, EAL4+, ATE_DPT.2, ALC_DVS.2
Protection profiles	SECURITY_IC_V1.0_PKISKPP
Maintenance updates	Infinion smartcard IC (Security Controller) M7794 A12 with optional RSA2048/4096 v1.02.013, EC v1.02.013 and Toolbox v1.02.013 (15.03.2013) Certification report

● Binding ● 

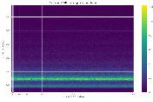

● Binding ● 

● Binding ● 



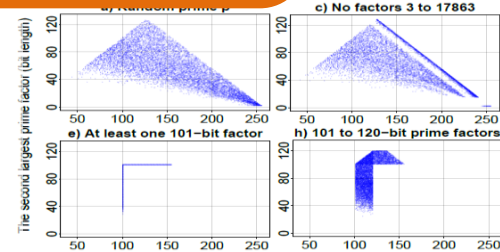
RSA keypairs
 Distribution of primes P and Q

ECDSA signature
 Dependency of sig time on private key

CVE-2017-15361
 Vulnerability in keygen (ROCA)

JSON blobs for products/metadata/bindings
 Filtering based on trust to signer
 NOSTR for format and propagation network



SCRUTINY: more valuable and transparent security certifications



Open-source analysis tooling for crypto implementations
CHES brokerage event, JIC, 5.2.2025

CRoCS team, [Petr Švenda](#)

Faculty of Informatics, Masaryk University, Czech Republic