Who evaluates evaluators?

Assessing cryptography evaluators assessing a secure messaging application security

Marion VIDEAU

Workshop on Randomness and Arithmetics for Cryptographic Hardware, WRACH 2023

Quarkslab

Overview

- General considerations about security and cryptography a.k.a. old people rambles
- Small recap on ANSSI/CCN and ITSEF (CESTI) and security evaluations
- Secure messaging security challenges
- The example app under cryptographic evaluation: a modified matrix/element a.k.a. CRY.ME
- Evaluation on Quarkslab's side
- Conclusion

Our everyday challenge

$$\mathbf{a}_L \in \{0,1\}^n \text{ s.t. } \langle \mathbf{a}_L, \mathbf{2}^n \rangle = v \tag{36}$$

$$\mathbf{a}_R = \mathbf{a}_L - \mathbf{1}^n \qquad \in \mathbb{Z}_p^n \tag{37}$$

$$\alpha \xleftarrow{\$} \mathbb{Z}_p \tag{38}$$

$$A = h^\alpha \mathbf{g}^{\mathbf{a}_L} \mathbf{h}^{\mathbf{a}_R} \qquad \in \mathbb{G} \tag{39}$$

$$\mathbf{s}_L, \mathbf{s}_R \xleftarrow{\$} \mathbb{Z}_p^n \tag{40}$$

$$\rho \xleftarrow{\$} \mathbb{Z}_p \tag{41}$$

$$S = h^\rho \mathbf{g}^{\mathbf{s}_L} \mathbf{h}^{\mathbf{s}_R} \qquad \in \mathbb{G} \tag{42}$$

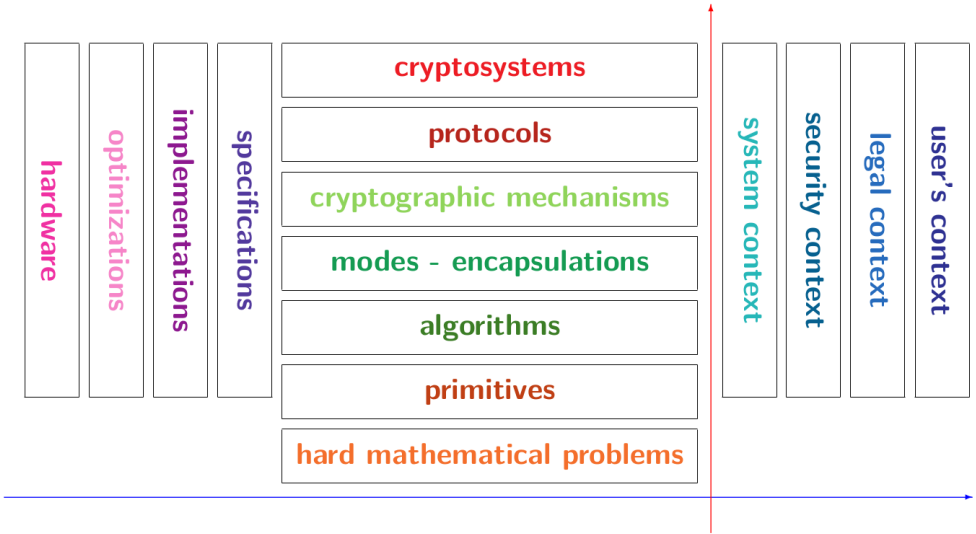
$$\mathcal{P} \to \mathcal{V} : A, S \tag{43}$$

$$\mathcal{V} : y, z \xleftarrow{\$} \mathbb{Z}_p^\star \tag{44}$$

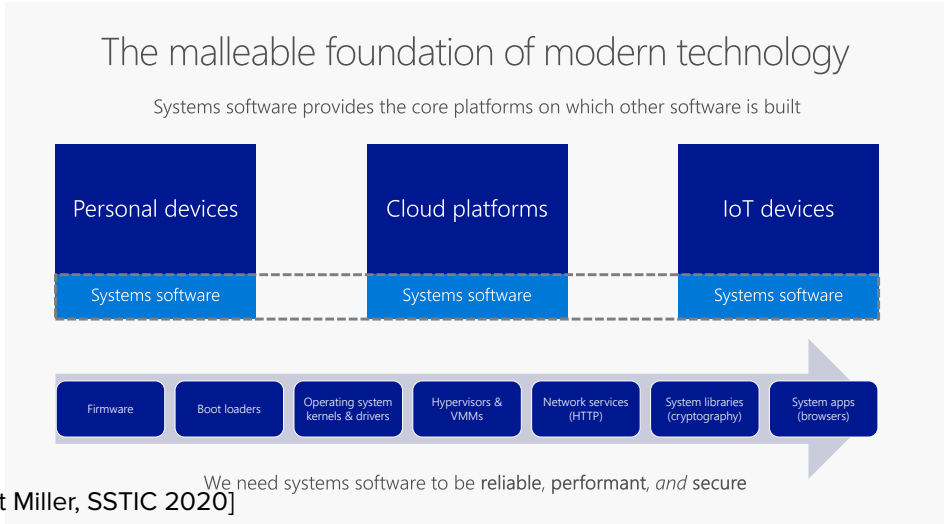
$$\mathcal{V} \to \mathcal{P} : y, z \tag{45}$$

```
725  // PAPER LINES 38-39
726  rct::key alpha = rct::skGen();
727  rct::key ve = vector_exponent(aL, aR);
728  rct::key A;
729  rct::addKeys(A, ve, rct::scalarmultBase(alpha));
730
731  // PAPER LINES 40-42
732  rct::keyV sL = rct::skvGen(MN), sR = rct::skvGen(MN);
733  rct::key rho = rct::skGen();
734  ve = vector_exponent(sL, sR);
735  rct::key S;
736  rct::addKeys(S, ve, rct::scalarmultBase(rho));
737
738  // PAPER LINES 43-45
739  rct::key y = hash_cache_mash(hash_cache, A, S);
740  rct::key z = hash_cache = rct::hash_to_scalar(y);
741
742  // Polynomial construction by coefficients
743  const auto zMN = vector_dup(z, MN);
744  rct::keyV l0 = vector_subtract(aL, zMN);
745  const rct::keyV &l1 = sL;
746
747  // This computes the ugly sum/concatenation from PAPER LINE 65
748  rct::keyV zero_twos(MN);
749  const rct::keyV zpow = vector_powers(z, M+2);
750  for (size_t i = 0; i < MN; ++i)
751  {
```

Cryptographic abstraction layers



System Software



[Matt Miller, SSTIC 2020]

Small recall on ANSSI/CCN and ITSEF

ANSSI - French certification center

- Implements the certification scheme
- Licenses the ITSEFs (Information Technology Security Evaluation Facilities) which conduct the evaluations
  - Audit (preliminary and follow-up)
  - Follow-up of their technical skills through evaluations
  - Mandatory participation to technical challenges
- Supervises the evaluation projects

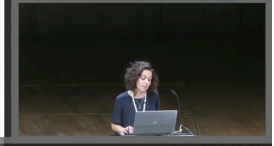
2022: CRY.ME challenge for all ITSEFs and only for cryptographic analysis

A challenge to test them all

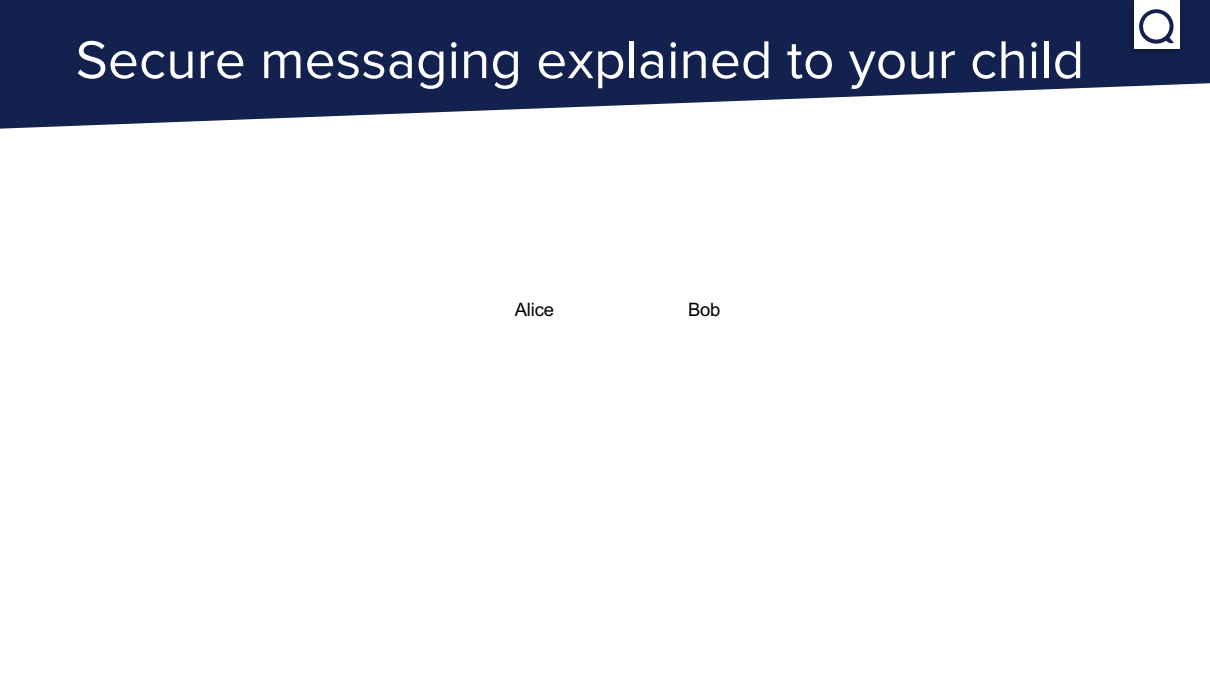
- Cryptographic analysis compliant to ANSSI's procedures[1, 2]
- Test vehicle common to all ITSEFs (software and hardware) but not only
  - **Open-source software product**
- Cover vulnerabilities of different types and levels of difficulty
  - **Several types of vulnerabilities:** conformance, symmetric crypto, asymmetric crypto, random number generation, protocols, implementation
  - **Three levels of difficulty:** not necessarily the same difficulty for identification and exploitation
  - **Various sources of errors:** weak choice of algorithms, design and/or implementation errors, differences between specifications and implementation, etc.

[1] ANSSI-CC-CRY-P-01 : https://www.ssi.gouv.fr/uploads/2014/11/anssi-cc-cry-p-01-modalites-pour-la-realisation-des-analyses-cryptographiques_v4.1.pdf

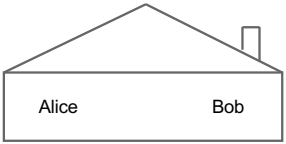
[2] ANSSI-PG-083 : https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf



Secure messaging explained to your child

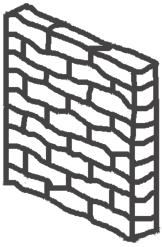


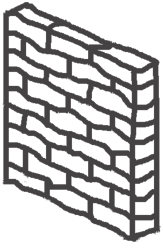
Alice wants to talk only to Bob



But they are separated

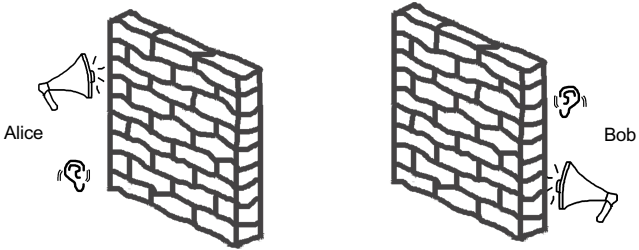
Alice



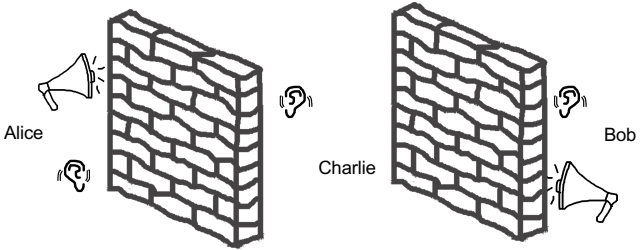


Bob

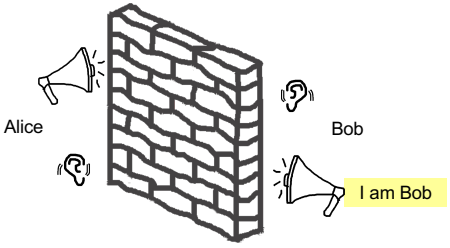
And they have to talk loud



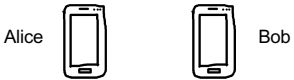
Others can hear them



Or even pretend to be Bob



Alice’s phone wants to talk to Bob’s phone



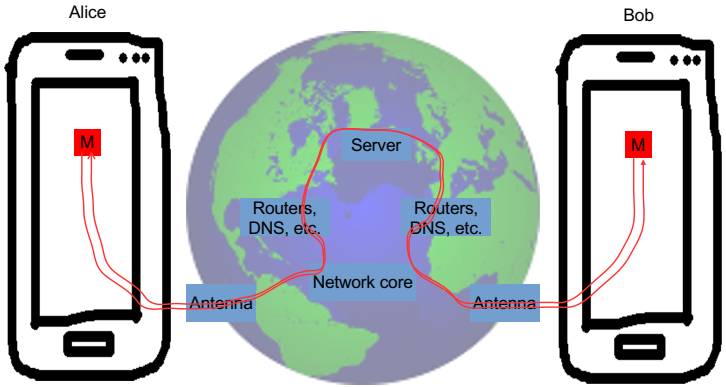
Through the vast Internet

Alice

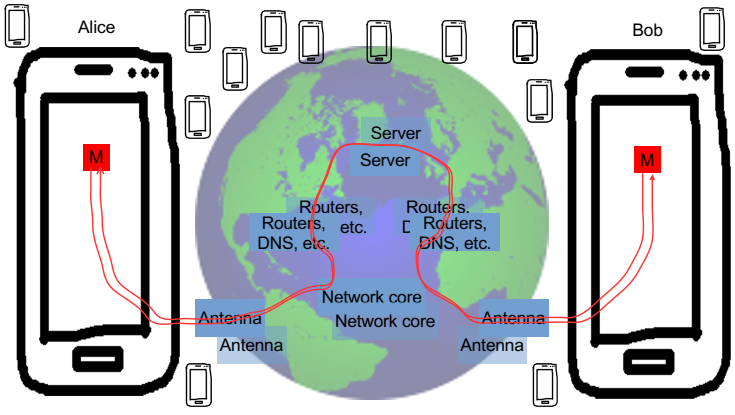
Bob

So it needs to talk loud...

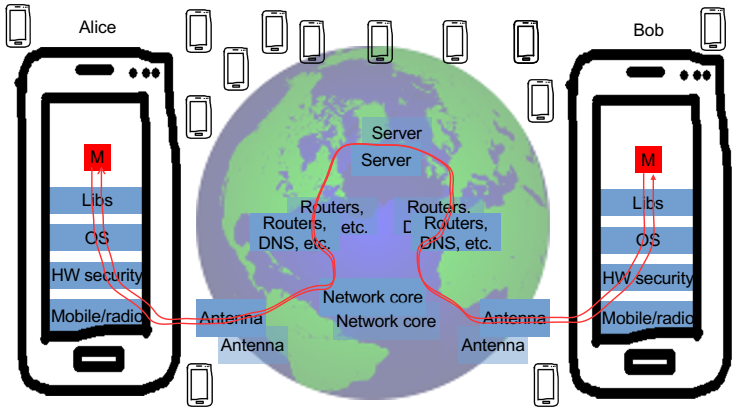
Very loud


Alice
Bob
M
M
Server
Routers,
DNS, etc.
Routers,
DNS, etc.
Network core
Antenna
Antenna

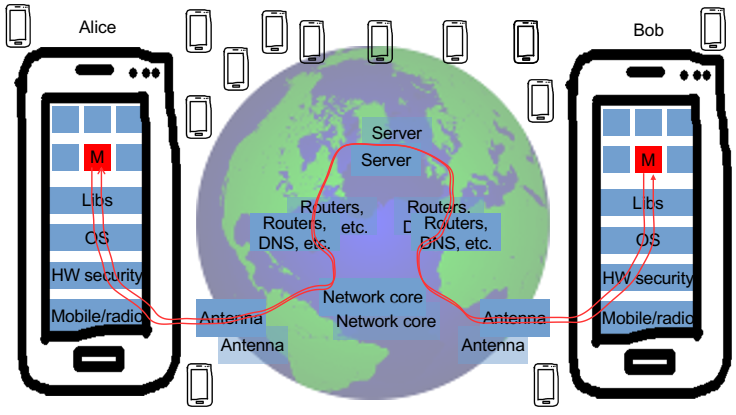
Others could hear them



What to trust?



You are not alone



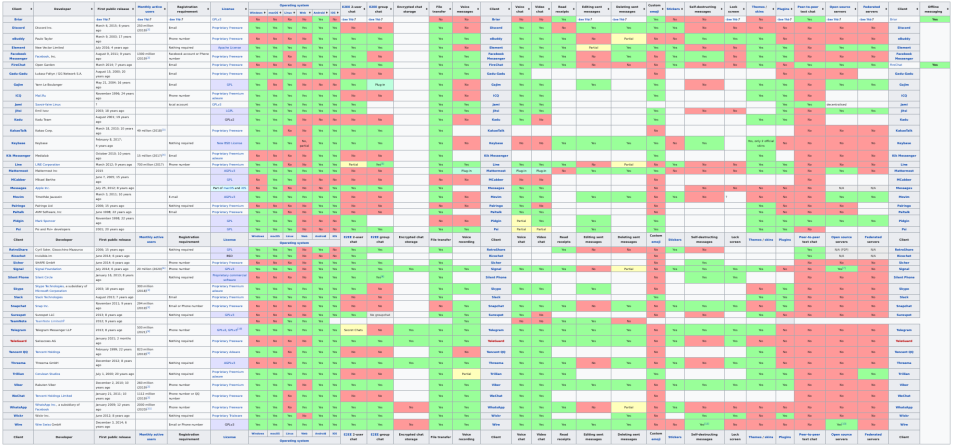
You are not your phone

phone lost

Who said it looks simple?

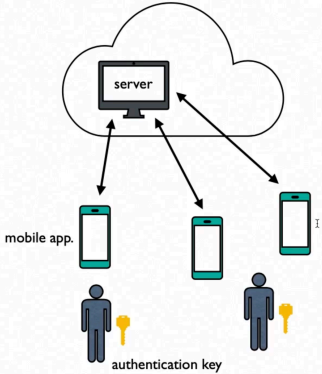
Features

Apps



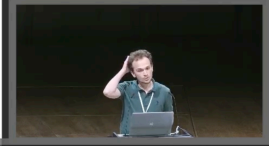
https://en.wikipedia.org/wiki/Comparison_of_cross-platform_instant_messaging_clients

The example app: a modified matrix a.k.a CRY.ME

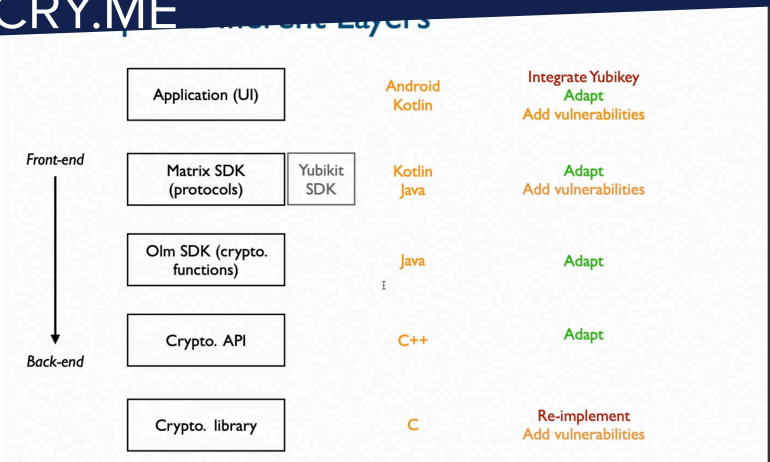


Functionalities

- Create account
- Login / Logout
- Send / Receive messages (1-to-1 or group)
- Send / Receive attachments
- Secure backup storage on the server
- Out-of-band verification between users



The example app: a modified matrix a.k.a CRY.ME



Evaluation on Quarkslab's side

Big steps:

- Meetings
- Analysis of security and environment issues
- Analysis of product implementation
- Compliance and resistance — Compliance, resistance and vulnerability analysis
- Compliance and resistance — Cryptography analysis
- Exploitation of the results
- Synthesis and report redaction

Total duration: 30 person.days

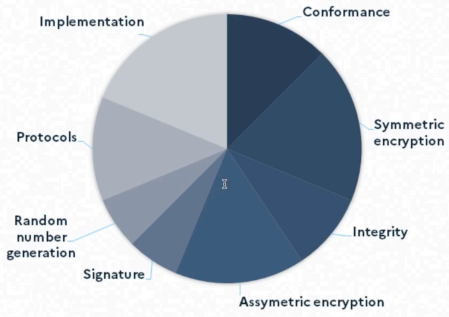
Evaluation on Quarkslab's side

Big steps:

- Meetings
- Analysis of security and environment issues
- Analysis of product implementation
- Compliance and resistance — Compliance, resistance and vulnerability analysis
- Compliance and resistance — Cryptography analysis
- Exploitation of the results
- Synthesis and report redaction

Total duration: 30 person.days of Angèle Bossuat and Philippe Teuwen with Matthieu Ramtine Tofighi Shirazi as head of CESTI

Vuln categories (no spoil)



Vuln categories (spoil)

Vuln categories (spoil)

- Classical theoretical vulns and attacks: LCG, ECDRBG
- Implementation issues: unfortunate typos on AES and PBKDF2, padding oracle
- Not-on-purpose vulns: Message replay, random generation OOM, Yubikey default PUK and management key

Bridging the gap between paper and exploit

as fast as possible... On the importance of tools

- IDE for code review and navigation
- diffing different version of codes
- HTTP Toolkit for intercepting and manipulating HTTP(S) communications
- RsaCtfToolkit, Pananoid Crypto
- Faas, CADO-NFS

Conclusion

- ”a mega crypto CTF”
- Challenges encourage learning by doing
- Team work for expertise coverage: learn how to speak sufficiently a different language
- CRY.ME is available in open-source as a pedagogical platform:
  `https://github.com/ANSSI-FR/cry-me`