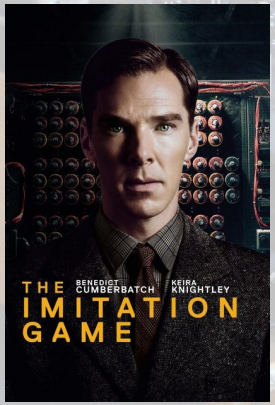
Radboud University

A Panorama on Classical Cryptography

Benoît Viguier

December 13th, 2021

What is cryptography?



What is cryptography?

Cryptography is about communication in the presence of adversaries.

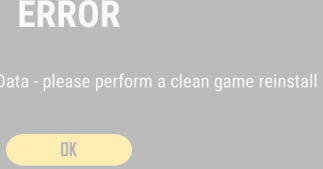
Ron Rivest

What do we want to protect?

- **Confidentiality**
- Data Integrity
- Data origin authentication
- Entity authentication

What do we want to protect?

- Confidentiality
- **Data Integrity**
- Data origin authentication
- Entity authentication



What do we want to protect?

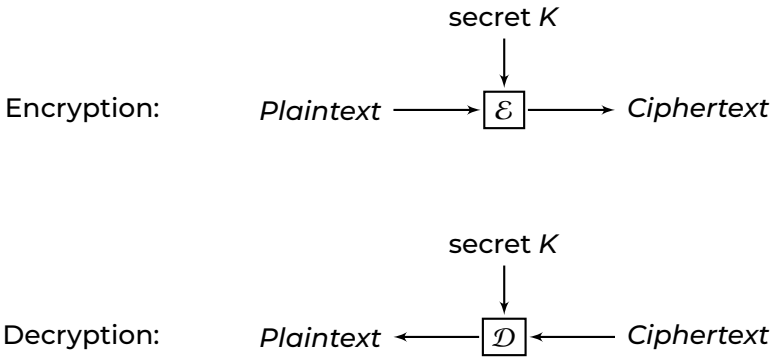
- Confidentiality
- Data Integrity
- **Data origin authentication**
- Entity authentication

What do we want to protect?

- Confidentiality
- Data Integrity
- Data origin authentication
- **Entity authentication**

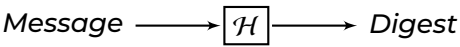
Crypto in our everyday life.

Symmetric encryption scheme

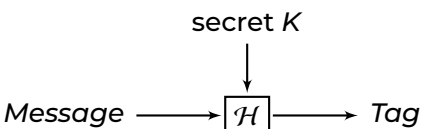


Crypto 101.

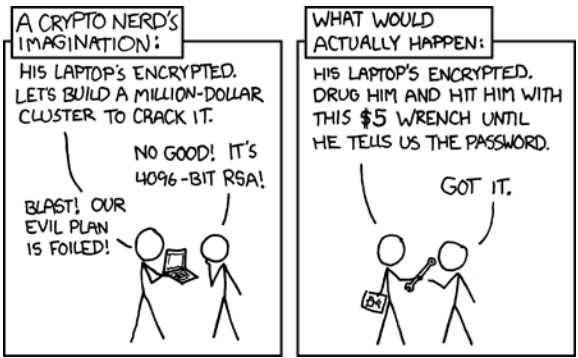
Hashing function



Message Authentication Code (MAC)



What my thesis is about.



https://xkcd.com/538/

- Designing
- Implementing
- Breaking
- Verifying
- Standardizing

... cryptography.

Designing.

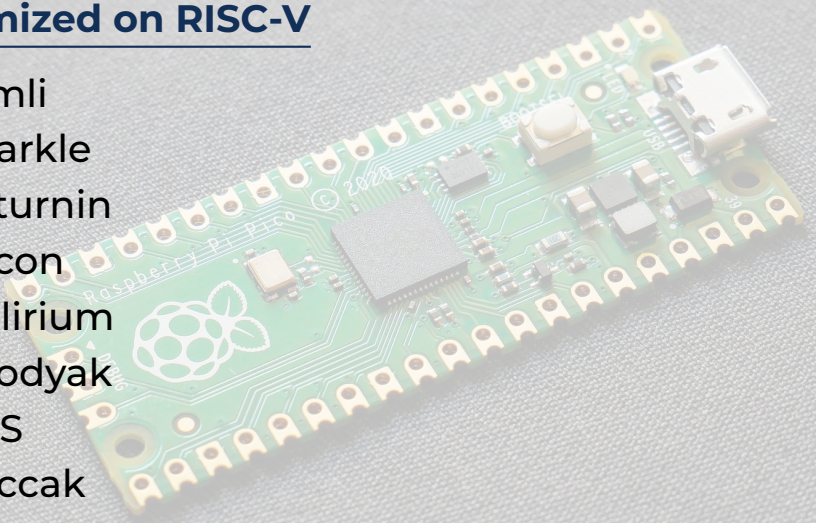
Gimli

- Authenticated-Encryption scheme (AE)
- Cross-platform and Lightweight
- High performances & secure

Implementing.

Optimized on RISC-V

- Gimli
- Sparkle
- Saturnin
- Ascon
- Delirium
- Xoodyak
- AES
- Keccak

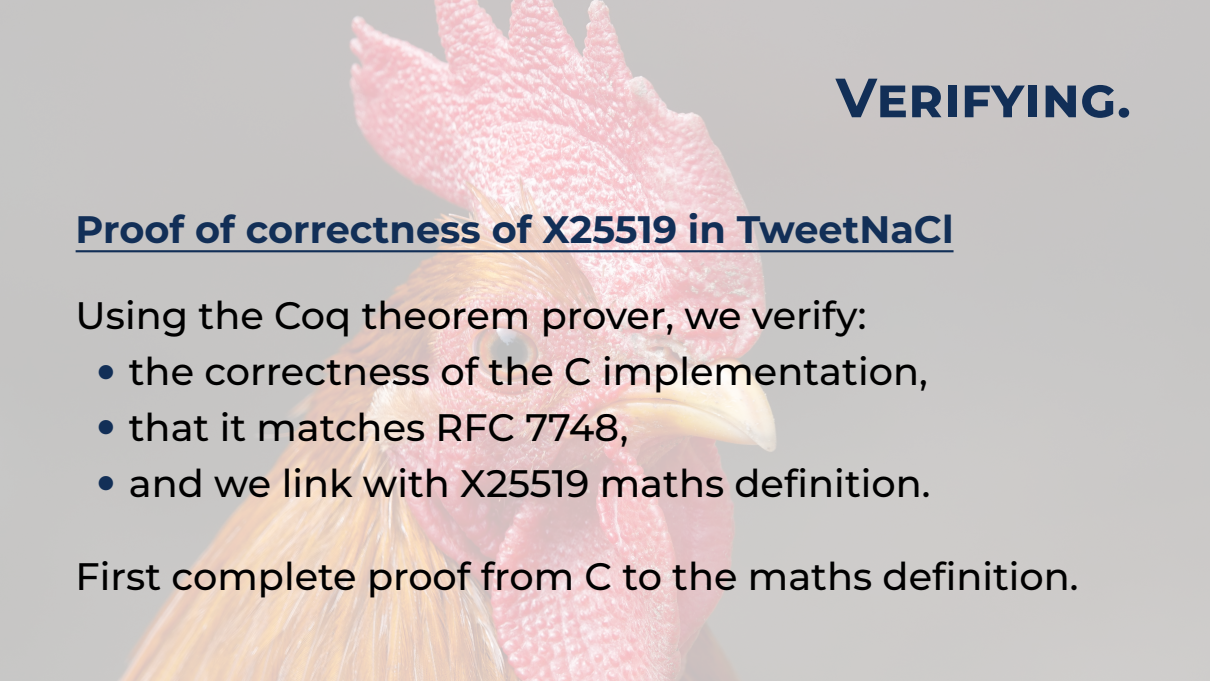


BREAKING.

Cryptanalysis of Morus

- Morus is a high-performances AE scheme.

	complexity claim	our result
Morus-640	2^{128}	2^{146}
Morus-1280	2^{256}	2^{152}



Verifying.

Proof of correctness of X25519 in TweetNaCl

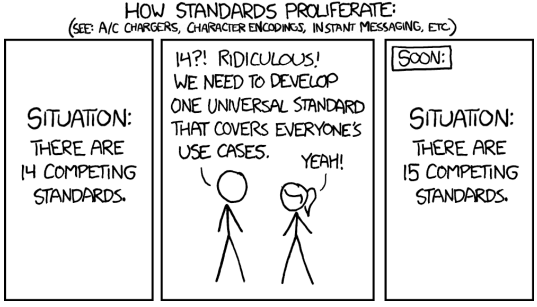
Using the Coq theorem prover, we verify:

- the correctness of the C implementation,
- that it matches RFC 7748,
- and we link with X25519 maths definition.

First complete proof from C to the maths definition.

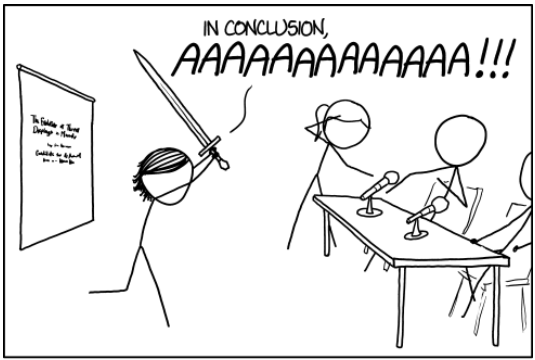
Standardizing.

- KangarooTwelve (SHA-3 *on steroids*)
- 1st Draft in January 2017,
- Still not accepted...
- CFRG is very slow.



https://xkcd.com/927/

Thank you for your attention.



THE BEST THESIS DEFENSE IS A GOOD THESIS OFFENSE.

https://xkcd.com/1403/