PROMETHEUS

PRivacy preserving pOst-quantuM systEms from
advanced crypTograpHic mEchanisms Using latticeS

Industrial Workshop
Technical overview

Sébastien Canard – Tuesday 28th June 2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780701. The contents of this workshop are the responsibility of the PROMETHEUS consortium, and do not necessarily reflect the official views of the European Union.

Context: quantum computing & cryptography

Quantum technologies

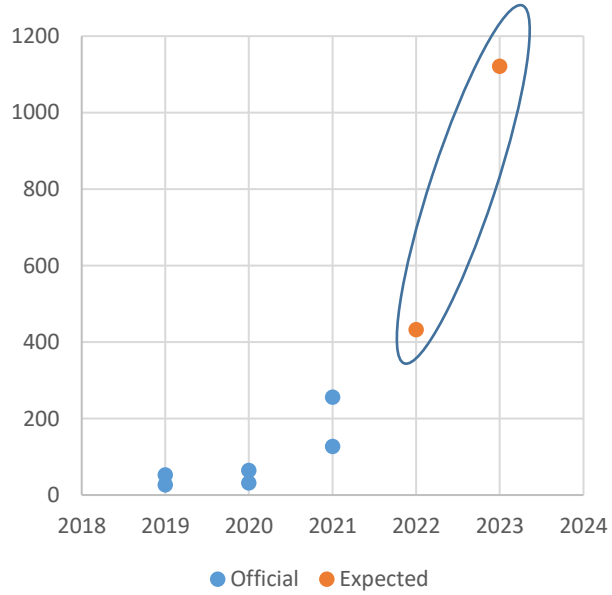
- Quantum superposition
  ⇒ more states are treated
  ⇒ qubits: 0, 1 or uncertain

- Quantum entanglement
  ⇒ linking distant objects

Quantum computing

- quantum computers think differently
- Quantum algorithms (Grover, Shor)

Evolution of quantum processors (in physical qubits) by year



Secret key cryptography

- Grover ⇒ better brute-force attack on the key
- 864 logical qubits to break AES-128

⇒ key lengths should be doubled

- Additional specific quantum attacks

Public key cryptography

- Shor's algorithm on factorization and discrete logarithm ⇒ full break
- 9217 logical qubits to break RSA-3072
- 2330 logical qubits to break ECC-256

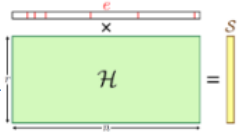
Quantum computers are not a threat now, but we need to be prepared as they could take off quickly

Long term confidentiality

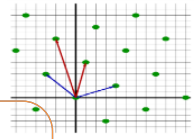
ANSSI BSI ENISA NCSC NSA

Post-Quantum Cryptography

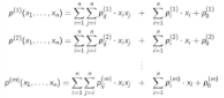
- Post-Quantum Cryptography is related to new mathematical problems for which quantum computers are not better than classical ones
- Several practical solutions are known exist since mid 70s



Codes

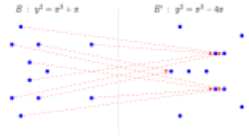


Euclidean lattices



Multivariate polynomials

Hash trees



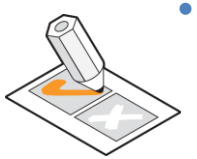
Isogenies

PROMETHEUS' identity card

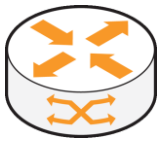
- PROMETHEUS: PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS
- H2020 project financed by the European Commission
- When?
  - Starting date: January 2018, duration: 4 years (1/2)
- Who?
  - Coordinator: ENS Lyon
  - Scientific leader: Orange
  - Academic partners: CWI, IDC, Royal Holloway, RUB, UPC, Université Rennes 1, Weizmann Institute
  - Industrial partners: SCYTL, Thales, TNO
- How much?
  - Grant amount: 5.5 M€, manpower: 790 p.m.

PROMETHEUS outline

- KEM and Encryption
  - Data confidentiality
  - Using additional secret key cryptography or not



- Digital signatures
  - Person/message authentication
  - Integrity and non-repudiation



- Advanced cryptography
  - Privacy-preserving techniques
  - Sensitive data protection

TLS, IPSEC, …

EMV, PKI, …

e-consumer, e-vote, anonymous authentication, end-to-end encryption, cloud outsourcing, …

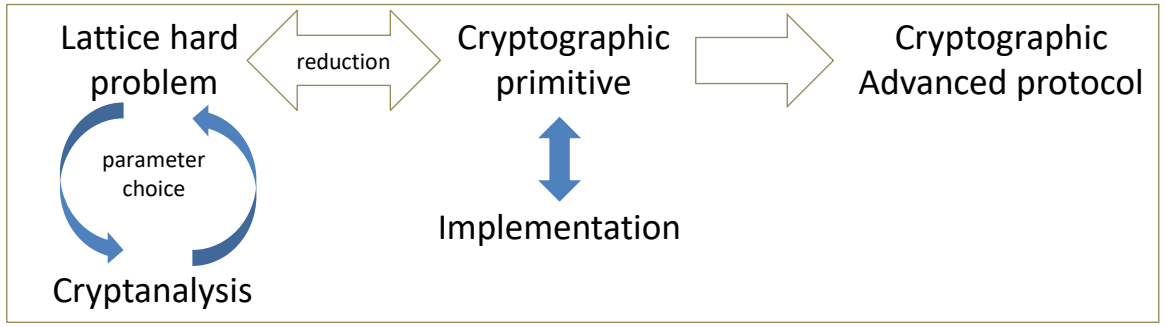
PROMETHEUS

Propose post-quantum solutions using lattices

- Objective 1: Build a complete study of the foundations of lattice-based cryptography
- Objective 2: Provide innovative lattice-based cryptographic primitives
- Objective 3: Protect the privacy of individuals in a post-quantum era

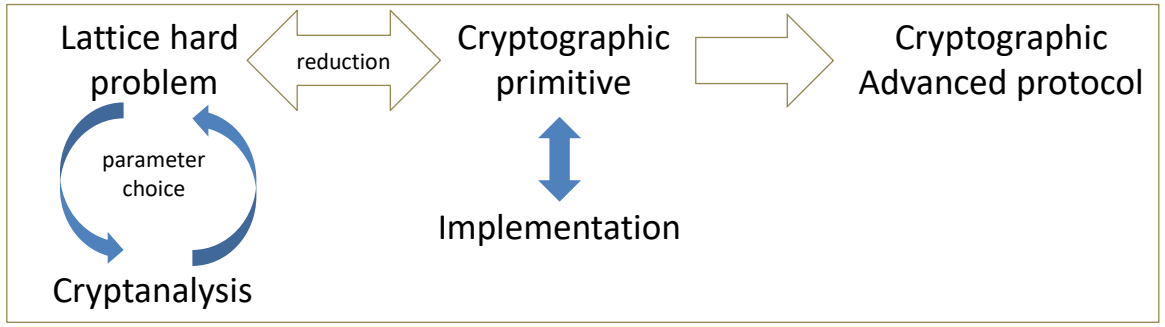
PROMETHEUS' result

Research (118 published papers)



PROMETHEUS' result

Research (118 published papers)

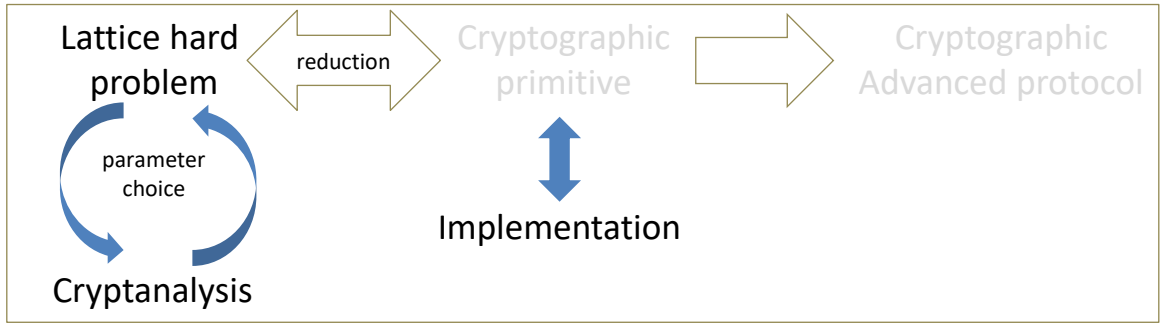


- Foundations ⇒ Objective 1
- Primitives ⇒ Objective 2
- Advanced protocols ⇒ Objective 3

PROMETHEUS' result

See Eamonn's presentation

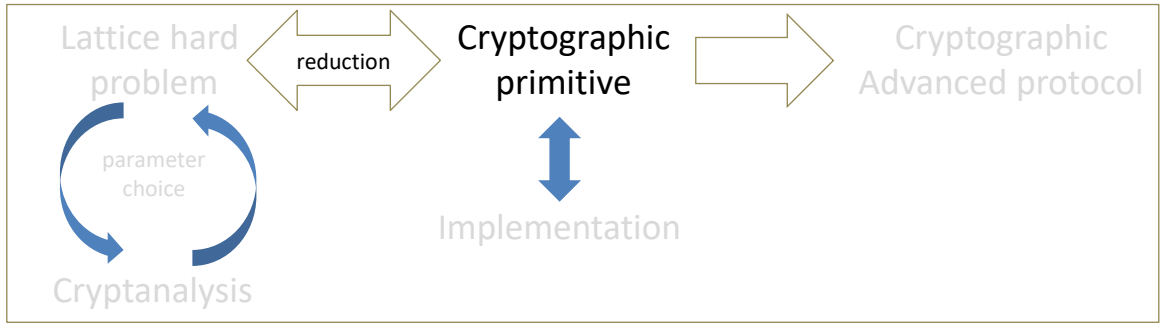
Research (118 published papers)



- Foundations ⇒ Objective 1
  - Better understanding of (structured) lattice-related hard problems and security proofs/reductions in the quantum setting
  - Better control of concrete security
  - More efficient and secure lattice basic algorithms
  - Better comprehension of side-channel attacks on implementations and countermeasure techniques
- Primitives ⇒ Objective 2
- Advanced protocols ⇒ Objective 3

PROMETHEUS' result

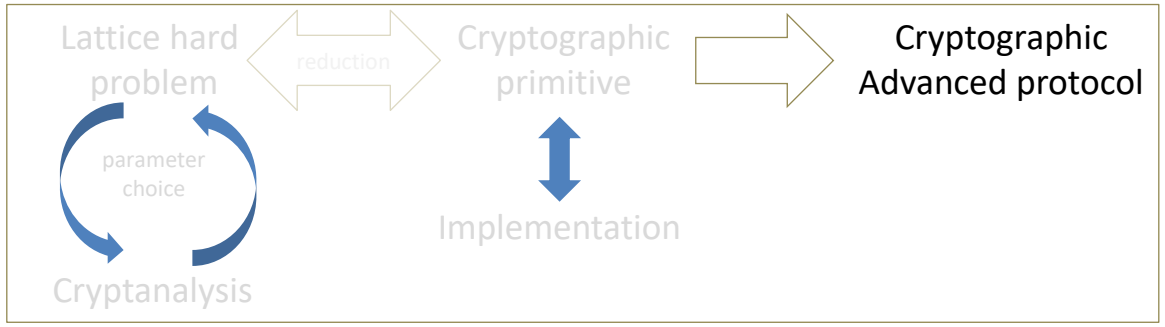
Research (118 published papers)



- Foundations ⇒ Objective 1
- Primitives ⇒ Objective 2
  - Evaluation and defense of NIST competitors on lattice-based signatures and Key Encapsulation Mechanisms
  - Building blocks for use cases: better design of signature schemes with efficient protocols, full redesign of lattice-based blind signatures, many zero-knowledge proofs of knowledge, several improvements on homomorphic encryption
- Advanced protocols ⇒ Objective 3

PROMETHEUS' result

Research (118 published papers)



- Foundations ⇒ Objective 1
- Primitives ⇒ Objective 2
- Advanced protocols ⇒ Objective 3
  - First secure lattice-based e-cash system
  - Several frameworks for lattice-based e-voting
  - First implementation of lattice-based anonymous credentials

PROMETHEUS' result

Research

Standardization

See Damien's presentation

NIST

- PROMETHEUS' members are implied in several finalists
- Strong participation to NIST discussions

ISO/IEC

- Strong involvement in WG2 - Cryptography and security mechanisms
- See ISO/IEC standards on blind and group signatures
- Participation in the vote for a new ISO/IEC standard on FHE

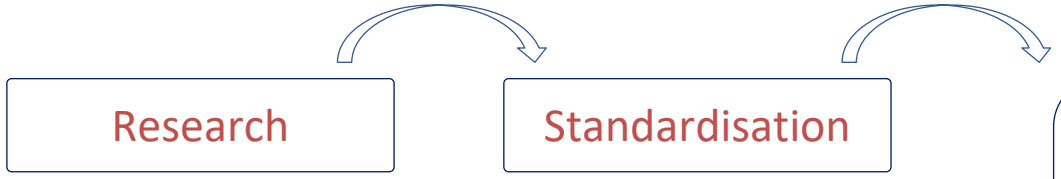
ETSI

- Strong involvement in TC Cyber
- Contribution to a report on PQ signatures

IETF

- Follow-up of internal studies

PROMETHEUS' result



See Georg's presentation

Implementation

- Lattice foundations
  - (Leaky)-LWE Estimator: open-source software for estimating the security of lattice-based cryptography (in presence of side channels for the "Leaky" version)
- Basic primitives
  - Several implementations of NIST competitors
  - Taking into account side-channel attacks
  - Crysalid: quantum resistant hybrid cryptographic library for signature and key-exchange functions
  - Other primitives: blind signatures, ZKPK, homomorphic encryption
- Advanced protocols
  - Implementation related to our use cases

PROMETHEUS' result

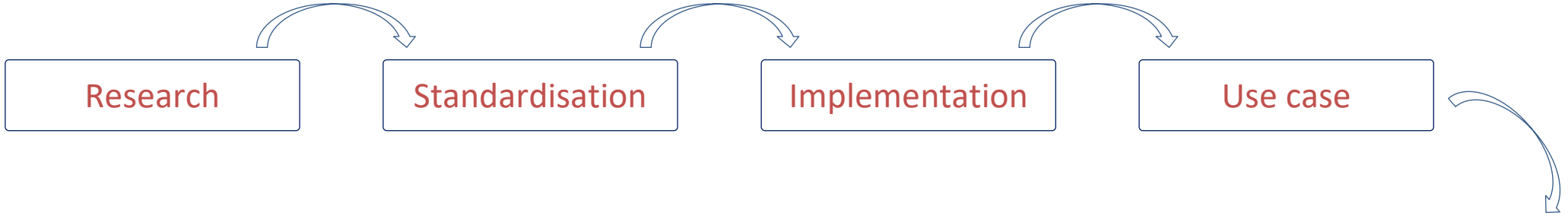
See Aleix's presentation

See Gabriele's presentation

Use cases

- Individual as a consumer
  - Quantum resistant e-payment
- Individual as a citizen
  - Quantum resistant e-voting
- Personal data minimization in proximity services
  - Quantum resistant Identity wallet
- Cyber threat intelligence to protect companies' data

PROMETHEUS' result



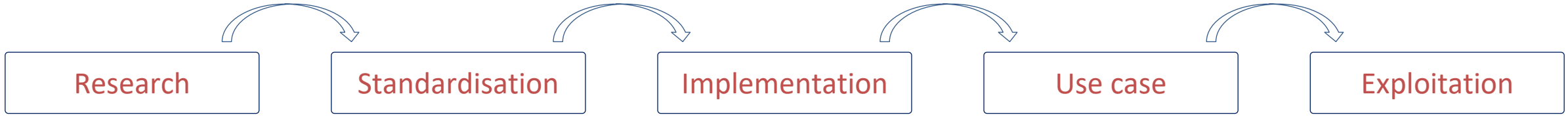
See Jean-Michel's presentation

See Thomas's presentation

Exploitation

- Short-term exploitation of lattice-based signatures and encryption (see security agencies' positions)
  - Transition to post-quantum cryptography should be thought today ⇒ efficiency is there!
  - Hybrid systems
  - Crypto agility
- Middle to long-term exploitation of advanced use cases
  - Maturity is sometimes very far from what can be done using classical cryptography

Key results and takeaways



Quantum computers are not a threat now, but we need to be prepared as they could take off quickly

Importance to design alternatives to historical cryptography

PROMETHEUS' outcomes

- Give to the community a large number of improvements related to lattice-based cryptography, from foundations to advanced protocols
- Thoroughly assess the exact maturity level of lattice-based cryptography
- Share our conclusions to academic, industry and authorities (https://www.h2020prometheus.eu/ and https://twitter.com/h2020prometheus)

Today’s agenda

Tuesday, 28 June 2022			
From	**To**	Topic	Speakers
10:00	10:15	Welcome and introduction	Jean Bolot - Orange
10:15	10:45	PROMETHEUS project technical overview	Sébastien Canard - Orange
10:45	**11:00**	Status of NIST standardization process on post-quantum	Damien Stehlé - ENS de Lyon
11:00	**11:45**	PQ implementation on hardware and side-channels attacks	Georg Land - University of Bochum
11:45	**12:30**	Overview of the impacts of post-quantum cryptography for an operator's IP network	Jean Michel Combes - Orange
12:30	**14:00**	**Buffet**	
14:00	**14:30**	Quantum-safe cryptography for Cyber-Threat Intelligence sharing	Gabriele Spini - TNO
14:30	**15:00**	Presentation of the different tools for parameters selection and their usage	Eamonn Postlethwaite - CWI
15:00	**15:45**	Impact of the transition to post-quantum cryptography on space and defence systems	Thomas Ricosset - Thales
15:45	**16:30**	Quantum-resistant mixnet prototype for e-voting systems	Aleix Amill - Scytl
16:30	**17:00**	**Informal discussions**	

Thank you