PROMETHEUS

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

PROMETHEUS overview and possible collaboration

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 768686.

PROMETHEUS Identity card

Who?

ENS Lyon (coordinator – Benoît Libert)
Orange (scientific leader – SC)

Centrum Wiskunde & Informatica
IDC Herzliya
Royal Holloway
Ruhr-Universität Bochum
Scytl
Thales
TNO
Universitat Politècnica de Catalunya
Université Rennes 1
Weizmann Institute of Science

What?

European Union H2020 project
Grant 780701
http://www.h2020prometheus.eu/

When?

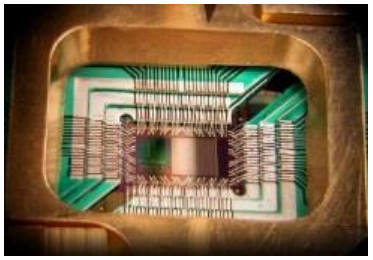
Starting date: January 2018
Duration: 4 years

How much?

Financial: 5.5 M€
Manpower: 790 m.m.

Quantum computers are coming

- Traditional vs. Quantum computers
  - Currently deployed computers have some restrictions
  - Quantum computers think differently
    - Can solve some of these limitations
    - Based on quantum superposition and quantum entanglement
- Recent advances in quantum computers
  - New funding coming from big actors
  - Implementation of simulators or true processors (analog or digital)
  - Research may go fast



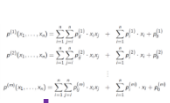
Impact on cryptography

- Secret key
  - Grover's algorithm in $O(\sqrt{n}) \Rightarrow$ faster exhaustive search $\Rightarrow$ Multiply by two the size of the secret key
  - Some existing cryptanalysis based on quantum algorithms
- Public key
  - Shor's algorithm $\Rightarrow$ RSA and ECC broken
- And even if quantum computers do not exist
  - RSA: key increase to have sufficient security
  - ECC: recent attacks on some (pairing-friendly) curves

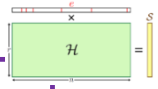
Post-quantum cryptography

- We need alternatives to currently deployed cryptography
- Practical solutions are known exist since mid 70

Multivariate polynomials

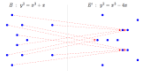


Codes

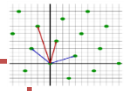


Hash tree

Isogenies



Euclidean Lattices



Quantum physics

Research is going on…

- NIST call for proposal
  - Signature schemes, KEM/encryption schemes

  Important to follow such competition

  - 8 proposals are from PROMETHEUS partners (among which 6 are lattice-based)
- Focus on basic cryptographic algorithms
  - Impact on TLS, SSH, PKI, Payment…

- What about other e-services?

Privacy is coming

- More and more e-services are using individuals' data ⇒ what about privacy?
- New European regulation: GDPR 2018
- GDPR's application necessitates relevant tools

Cryptography can certainly help!

⇒ Data confidentiality

⇒ Data minimisation

Cryptography and Privacy

- Data confidentiality
  - Encryption is there but does not permit data usability

A. We need advanced encryption schemes

- Data minimisation
  - Prove to have the right to do something…
  - While minimizing the quantity of personal information that are given to third parties

B. We need privacy-preserving authentication schemes

A. Versatile encryption

- Public key encryption scheme (most of the time)
  - A public key is used to encrypt some data
  - A private key is used to decrypt the data
- One can manipulate the ciphertext to obtain new properties
  - Such encryption schemes permit to perform some treatment over encrypted data
  - Different possibilities depending on
    - the treatment and the way to manage cryptographic keys
- Four main families

Unique treatment

Homomorphic encryption

Multiparty computation

Functional encryption

Example of such advanced tools

Homomorphic encryption

Searchable encryption

Multi Party Computation

Attribute based encryption

Functional encryption

Identity based encryption

Proxy Re-encryption

Broadcast encryption

…

Artificial Intelligence

- Ethics and responsibility
- Devise technical solutions to be GDPR compliant
- Machine learning algorithms in the encrypted domain

Cloud blind storage

- Data storage (cloud, safes)
- Date share and data treatment “in blind”
- Broadcast encryption, proxy re-encryption, attribute based encryption are suitable

Traffic analysis

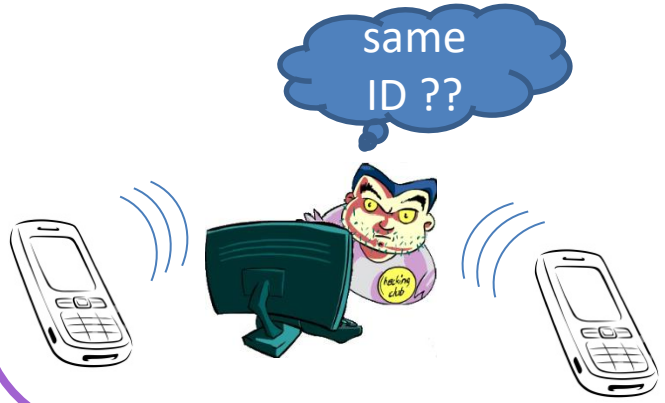
- Encrypted traffic ⇒ no traffic analysis
- IDS, parental control, SIEM, Quality service probes, …
- Needs adapted encrypted mechanisms

B. Authentication & Anonymity

- Having one communication log
- Infeasibility to link such communication with an identity

ANONYMITY

- Having 2 distinct communication logs
- Infeasibility to know whether both communications are related to the same identity



(NON) TRACEABILITY

Accountability

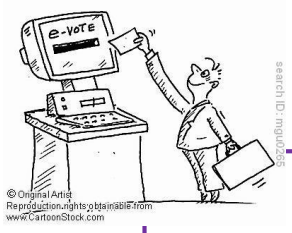
- Anonymity is a good point for privacy
  - Permits data minimization
  - “I belong to the group of authorized users”
- But anonymity should not lead to more fraud
  - Money laundering, anonymity of terrorists, etc.
- We also need accountability
  - The user should be authorized
  - Necessity to revoke the anonymity in case of fraud
    - By whom? when?
    - It depends on the use case and on legal restrictions
  - Pay attention to false accusations

Anonymity, accountability and standards

- ISO/IEC SC27 WG2
- Group signatures – ISO/IEC 20008-2
  - Each group member can sign messages
  - Each signature is anonymous, except for a designated opening manager
- Blind signatures – ISO/IEC 18370
  - A signer can sign documents that he does not know
  - The user who obtain the signature of his choice is anonymous in the group of users having obtain a signature from this signer
  - The user is authenticated by the signer when he obtains the signature

Anonymous credentials

- Authorization to access a place or a service
- Anonymity within the group of authorized entities
- Access control over attributes



e-vote systems

- A voter is a member of the group of authorized voters
- Anonymity of the votes
- (Without anonymity revocation)
- Related to additional tools

e-cash systems

- A coin is a member of a group of authorized coins
- Each spending corresponds to a group signature
- Double spending detection

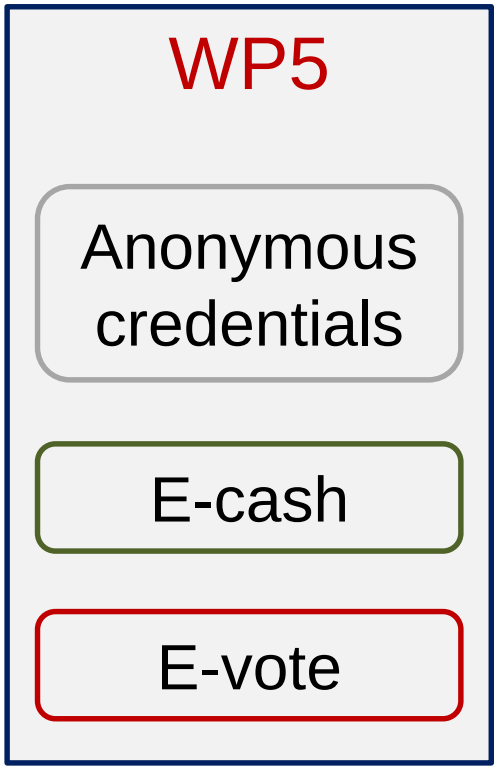
What about constructions?

- Most of existing standards and implementations are based on RSA and ECC
  - Broken by quantum computers or by cryptanalysis
  - Inefficient using RSA
  - Some exceptions in the case of versatile encryption
- Post-quantum constructions are not mature
  - Some open problems remain, solutions are inefficient
  - NIST CfP is an answer, but will not solve that problems
  - Lattice-based cryptography is the more mature solution

Here comes PROMETHEUS!

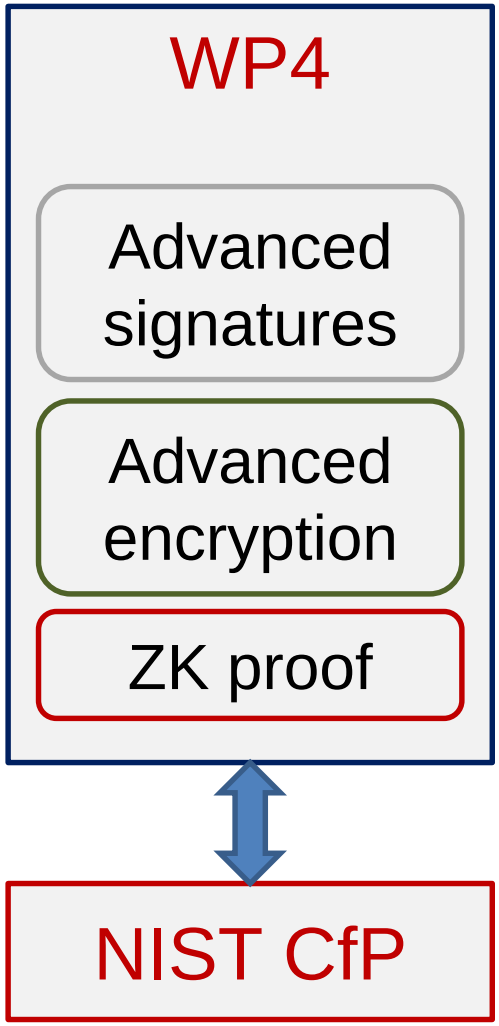
Privacy-preserving protocols

- Main problems to solve
  - Obtain better flexibility
  - Improve efficiency
- Two main approaches
  - Explore new paradigms fitting lattices
  - Build systems based on usual building blocks



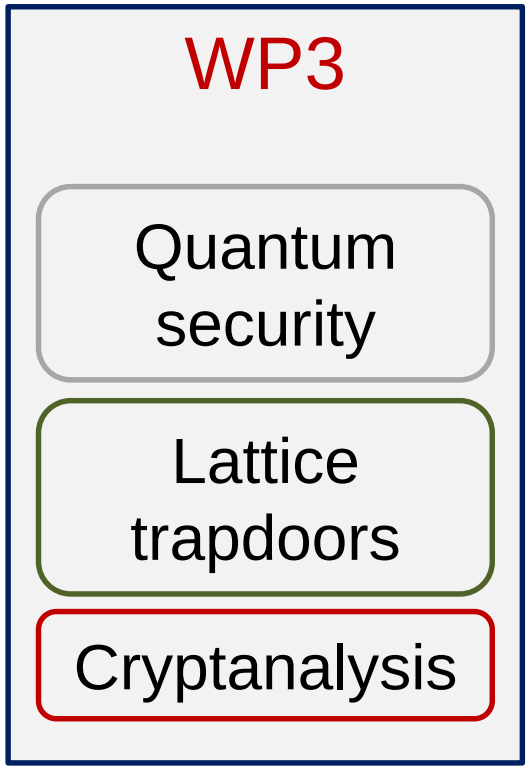
Building blocks

- Main problems to solve
  - Find constructions related to blocks for which no solution exists
  - Improve efficiency
  - Improve security
- In relation with
  - Security assumptions
  - Security proofs
  - And possibly lattice trapdoors

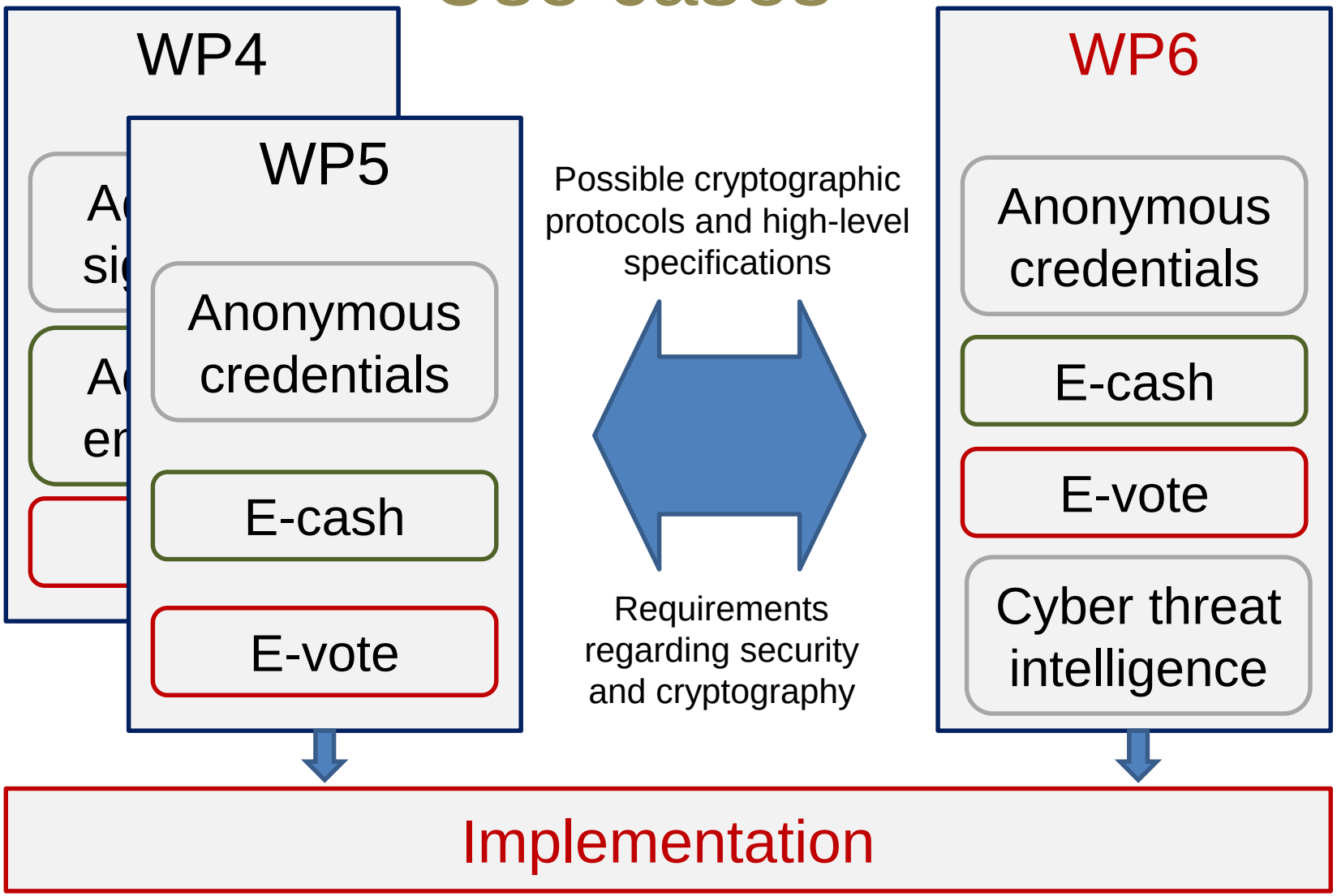


Problems, Cryptanalysis, Tools

- Main problems to work on
  - Quantum reductions and hardness
  - Better understanding and manipulation of lattice trapdoors
  - Concrete and quantum cryptanalysis
  - Side-channel attacks



Use cases


WP4
WP5
Anonymous credentials
E-cash
E-vote
Possible cryptographic protocols and high-level specifications
Requirements regarding security and cryptography
WP6
Anonymous credentials
E-cash
E-vote
Cyber threat intelligence
Implementation

FutureTPM and PROMETHEUS

- Basic signature/encryption mechanisms
  - Basic building block in both projects
  - Particular focus on lattice-based in PROMETHEUS
- Group signature and DAA
  - Direct Anonymous Attestations (DAA) are some special kinds of group signatures
  - Special traceability, TPM/Host interactions
  - DAA can also be used in e-voting
- Side channel attacks
  - Important to be taken into account in a TPM

Thank you