Data Protection and Privacy in a Quantum World

Sébastien Canard
Journées Nationales du GDR Sécurité Informatique
June 2023

TELECOM Paris

INSTITUT POLYTECHNIQUE DE PARIS

Quantum computers and 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)

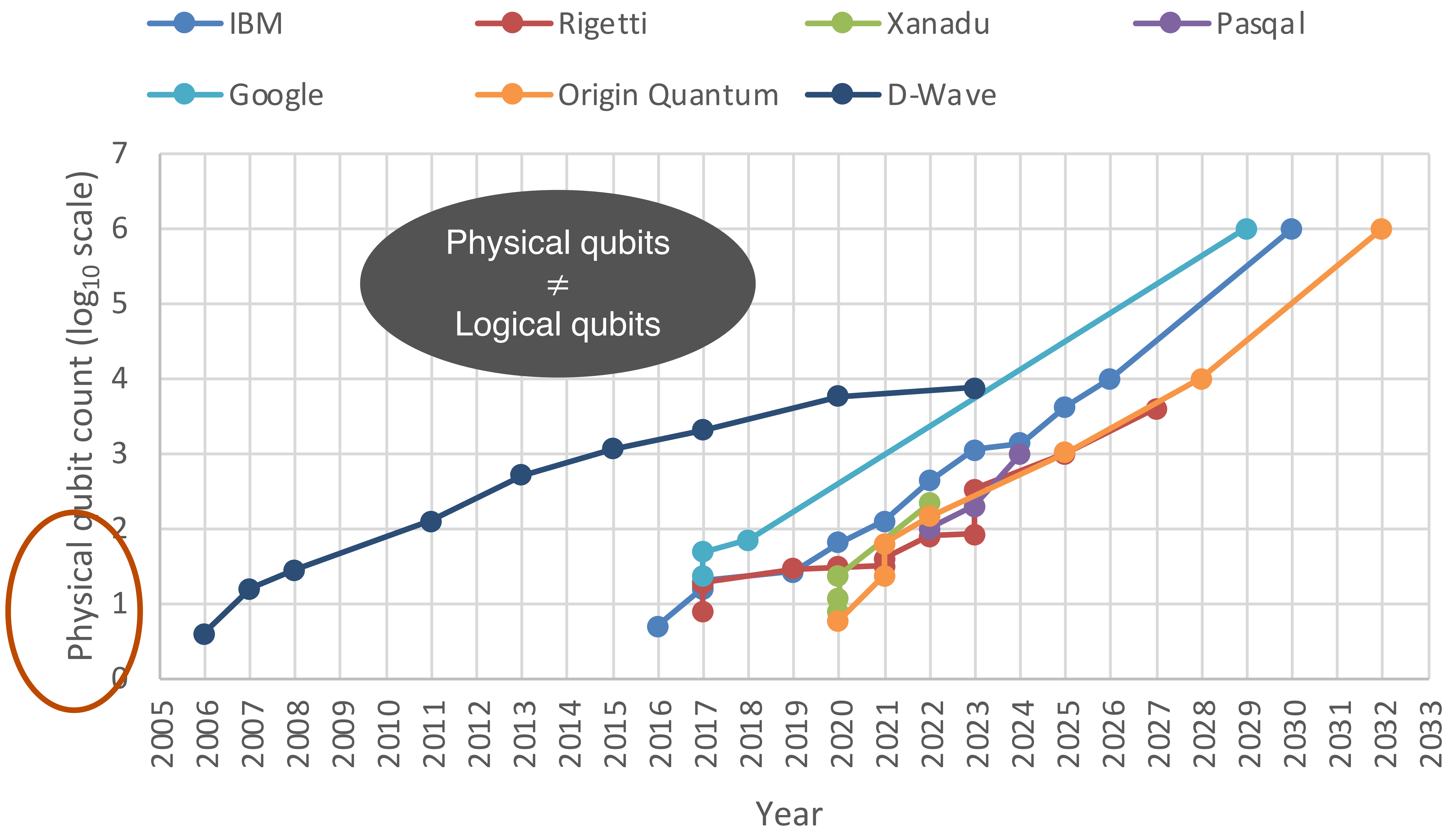
Secret key cryptography

- 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
- 6100 logical qubits to break RSA-3072
- 2330 logical qubits to break ECC-256

Availability of quantum computers



Not a threat now!

But « store now, decrypt later » paradigm

Recall:

AES	864 logical qubits
RSA	6100 logical qubits
ECC	2330 logical qubits

Impacted primitives

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

→ TLS, IPSEC, …

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

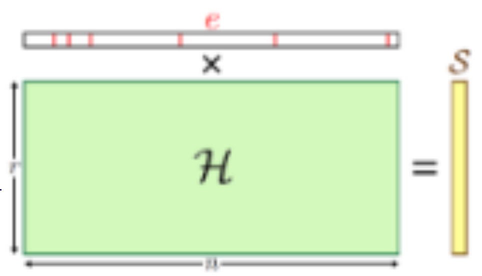
→ EMV, PKI, …

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

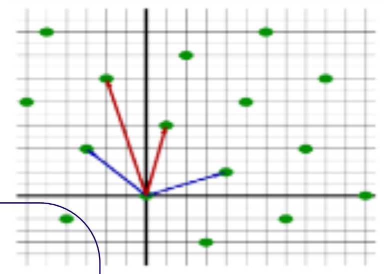
→ e-consumer, e-vote, anonymous authentication, end-to-end encryption, cloud outsourcing, …

Post-Quantum Cryptography

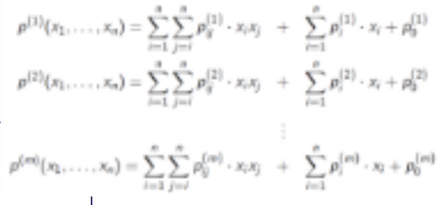
- Post-Quantum Cryptography is related to new mathematical problems for which quantum computers are not better than classical ones
- Several practical solutions are known exist since mid 70s



Codes

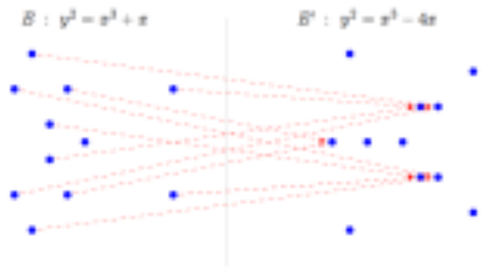


Euclidean lattices



Multivariate polynomials

Hash trees



Isogenies

NIST standardisation process on PQC

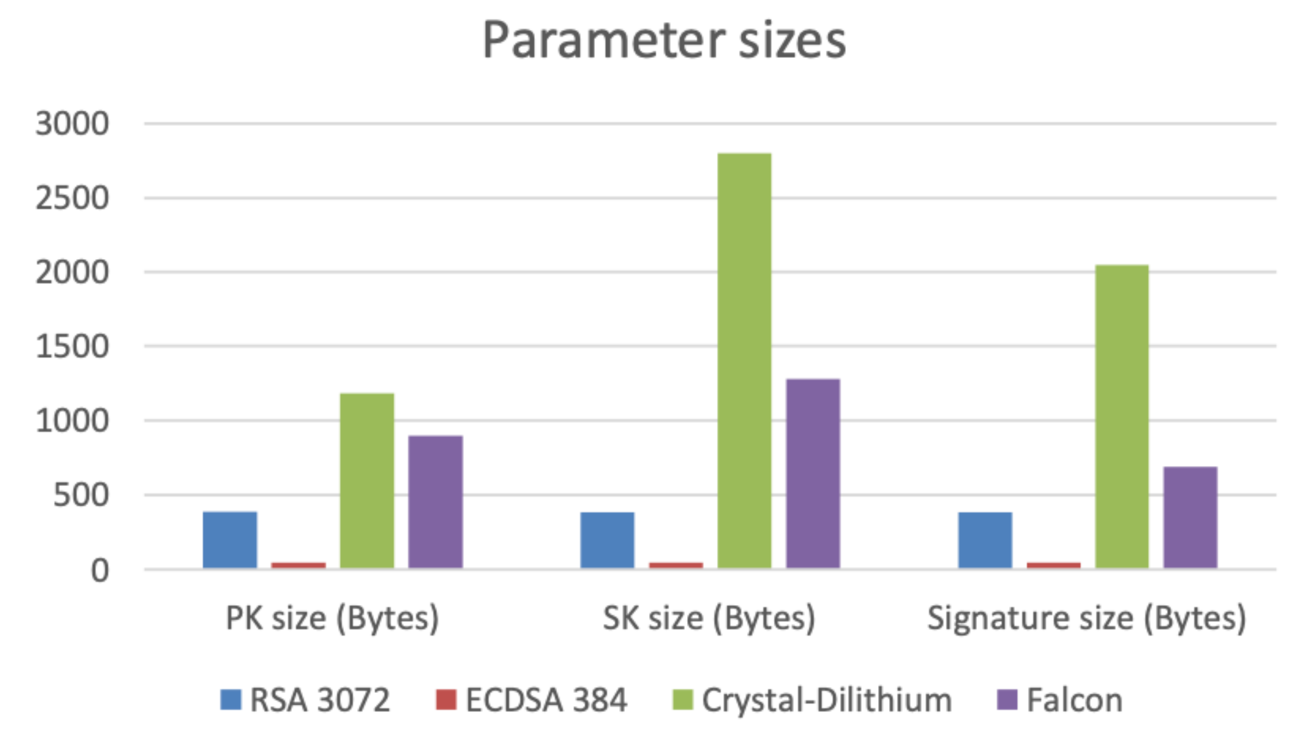
Whole process

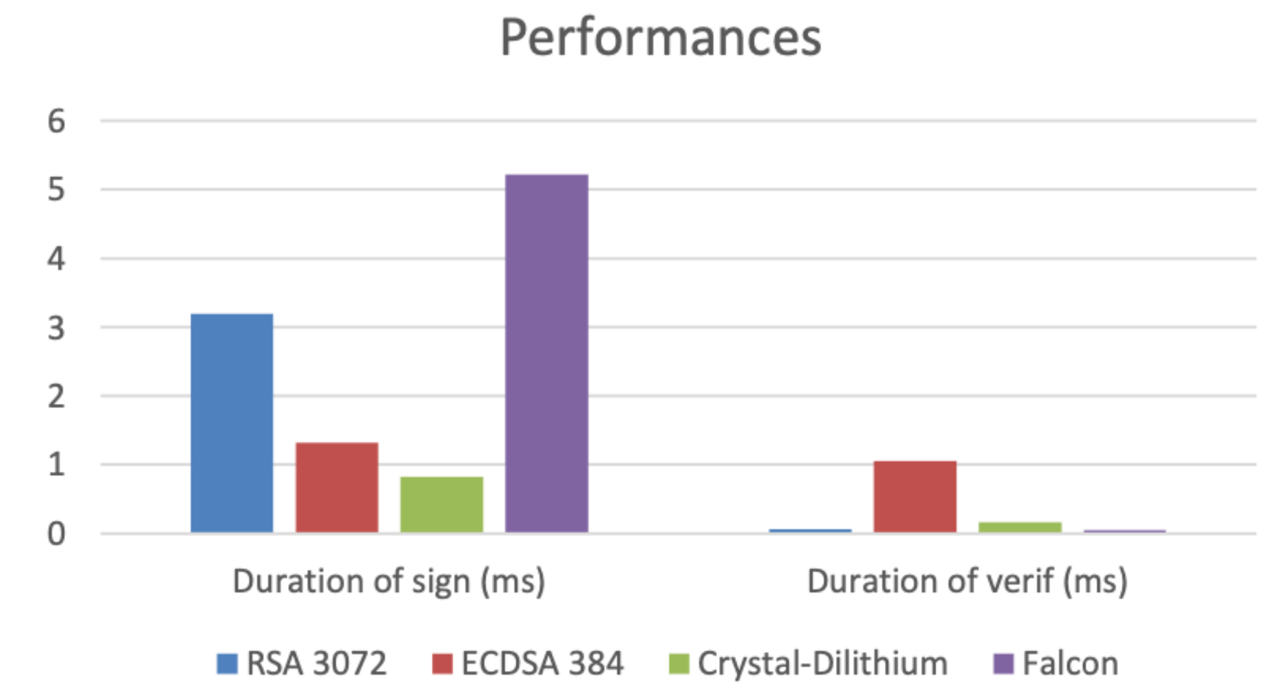
April 2015	Annoncement	NIST announces future standardisation		
December 2017	Submission	69 complete and proper submissions	49 PKE/KEM	20 SIG
January 2019	End 1st round	26 submissions	17 PKE/KEM	9 SIG
July 2020	End 2nd round	7 finalists, 8 alternates	4 (+5) PKE/KEM	3 (+3) SIG
July 2022	Winners	4 schemes selected for standardisation	1 PKE/KEM	3 SIG

Selected candidates

PKE/KEM	Kyber (lattices)		
SIG	Dilithium (lattices)	Falcon (lattices)	SPHINCS+ (hash functions)

+ New round (PKE/KEM)
+ New competition (SIG)





Standardisation of PQC

PQTN

Guidelines for telecommunication industry

Standardisation of PQ Key-Encapsulation Mechanisms including, but not-restricted to, NIST standards.

WG2

Survey of NIST candidates
Some advanced encryption mecanisms (e.g., IBE)

CYBER

SAGE

Standard Development Organisation

Upgrade and design of secret key algorithms supporting 256-bits key

SA3

Draft for first standards
New round for KEM
New competition for signatures

Post-quantum variant of major protocols (e.g., TLS, IKE)

What about advanced cryptographic mechanisms

Advanced encryption mechanisms		Advanced authentication mechanisms	
Privacy-preserving data treatment		Privacy-preserving authentication	Privacy-preserving payment
Fully homomorphic encryption	Other encryption with special features (e.g., IBE, ABE, FE)	Anonymous credentials/ attestations	E-cash
Inherently post-quantum secure (See next talk)	Hard to design post-quantum analogues at this stage	All those primitives are very good in the classical setting, leading to real products, or ready-to-market ones Not so easy in the post-quantum setting	

Our focus now

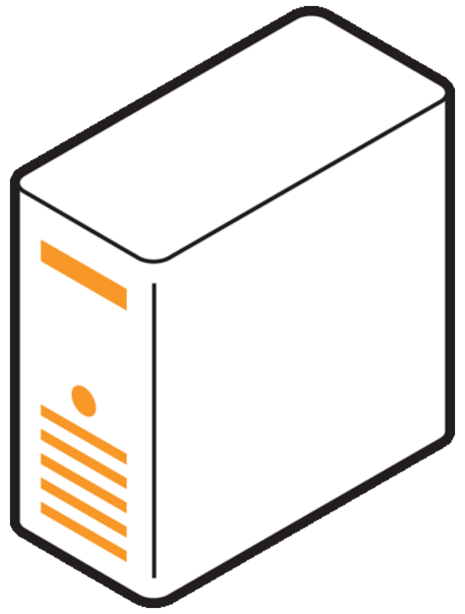
Anonymous credentials/attestations

- Advanced authentication mechanisms enable full leakage control
  - Blind Signature
  - Group Signature, DAA (Direct Anonymous Attestation), Enhanced Privacy ID (EPID)
  - Anonymous Credential
- Mechanisms widely deployed in billions of chips
  - Trusted Platform Module
  - Intel SGX enclaves
  - Willingness of the European Commission to deploy a privacy-preserving ID card…

- Standardised mechanisms
  - Blind signatures (ISO/IEC 18370)
  - Group signatures (ISO/IEC 20008)

Blind signature schemes

Message: m



Signing key: sk

Mask the message ⟷ Sign the masked message from Alice

Unmask the signature $\Longrightarrow\ \sigma$

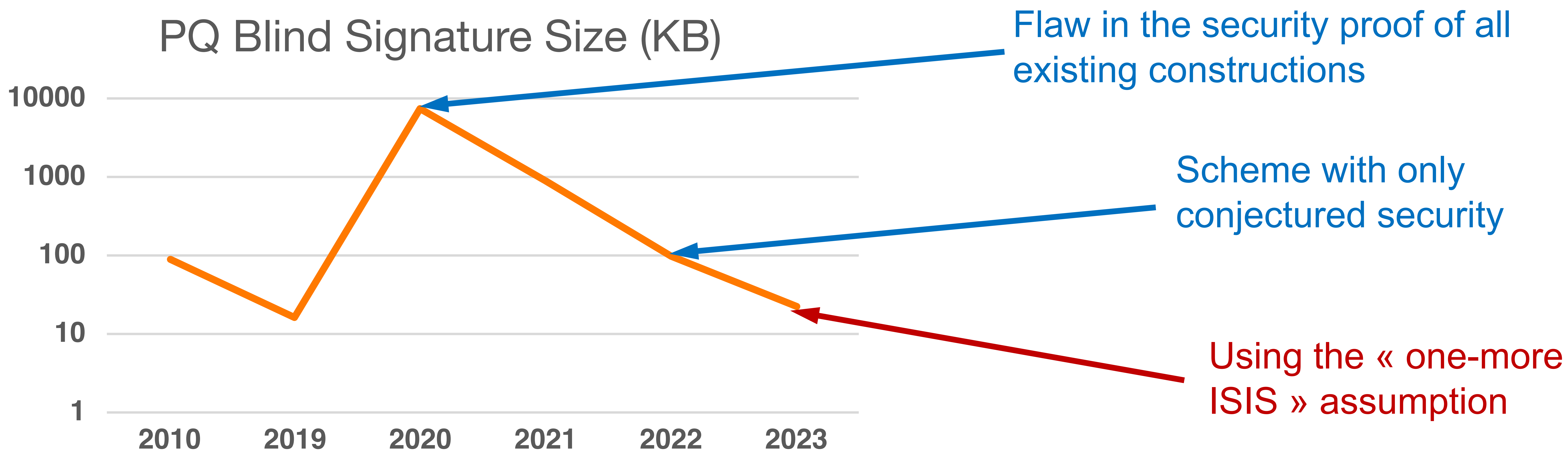
↓ (m, σ)

Verify validity of σ

- Unforgeability: infeasibility for Alice to create $l + 1$ message signature pairs after l interactions
- Blindness: infeasibity for signer to recognize the message signature pair

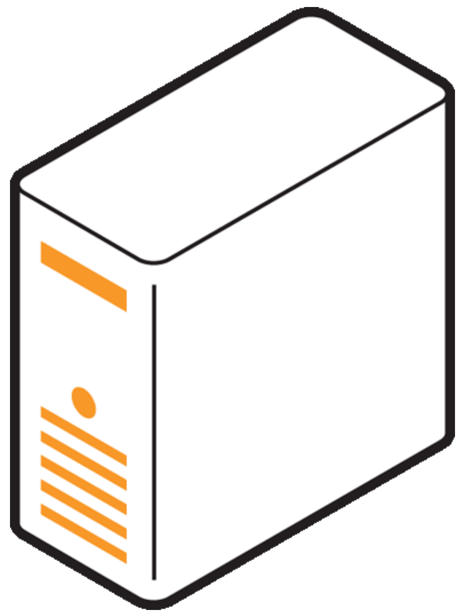
Post-quantum blind signatures

- Standardised blind signatures using classical cryptography
  - Based on RSA or Schnorr signatures
  - Size: 65 B
- Status on post-quantum constructions



Group signature schemes

Secret: x
Public ID: A



Signing key: sk

Obtain a signature on (x, A)

Sign (x, A)

Encrypt $A \Longrightarrow$ c
Compute $ZKPK(A, e, \sigma) \Longrightarrow \pi$

(c, π)

Verify validity of π
Ciphertext c can be sent for opening

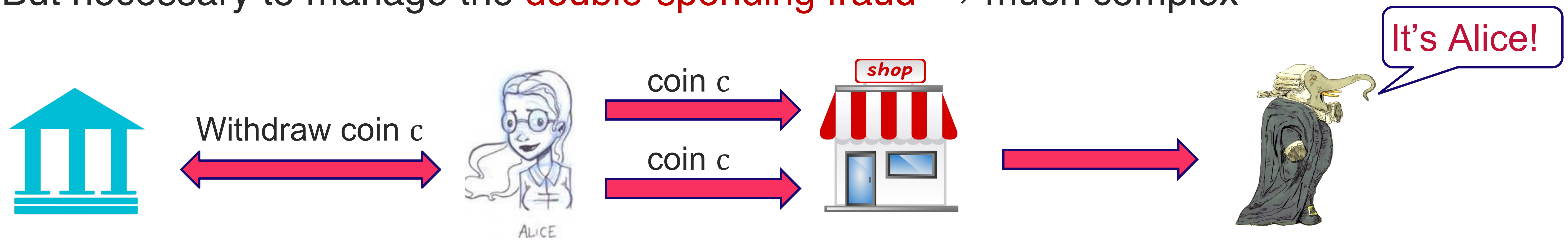
- Unforgeability: infeasibility to sign a message for non group members
- Unlinkability: infeasibity link two signatures from the same member
- Traceability: the opening of a valid signature should give the right member
- Non-frameability: infeasibity to falsely accuse a honest member

Post-quantum group signatures

- Basic tools to construct a group signature scheme
  - Signature scheme with advanced features + Encryption mechanisms
  - Zero-knowledge proof of knowledge (ZKPK)
- Standardised group signatures using classical cryptography
  - Based on pairings or on flexible RSA $\Longrightarrow$ Size: 160 B to 1 KB
- Status on post-quantum constructions
  - Hard to manage ZKPK efficiently compatible with signatures and encryption
  - Using a standard lattice assumption $\Longrightarrow$ Size: 600 KB
  - Using an interactive (stronger) version $\Longrightarrow$ Size: 30 KB

E-cash

- Main idea
  - Using group signatures: a wallet is a group member
  - But necessary to manage the double-spending fraud $\Longrightarrow$ much complex



- E-cash constructions using classical cryptography
  - Using pairings, implemented in a smart phone: payment $<$ 100 ms
- Status on post-quantum constructions
  - Security proof of most of the constructions has been invalidated
  - One generic scheme but no instantiation on post-quantum cryptography
  - One concrete scheme using lattices $\Longrightarrow$ Factor of 1 million compare to pairing-based solutions!

Conclusion

Quantum computers are not for now
But the threat is huge, and we need to be prepare

- Basic cryptography
  - NIST standards are in progress, other standards are working
  - Integration is the next steps $\Longrightarrow$ should be done by the industry
  - But research should continue
    - Cryptanalysis
    - Improve efficiency
    - Hardware implementation and security (SCA)

- Advanced cryptography
  - We are very far from what can be done using classical cryptography
  - One of the main research topic on privacy-preserving cryptography
    - Pairings look impossible
    - Use stronger assumptions to improve efficiency
    - Necessity to think differently

Thank you