Post-Quantum Digital Signatures

QuData Project Kick-Off

Dominik Leichtle

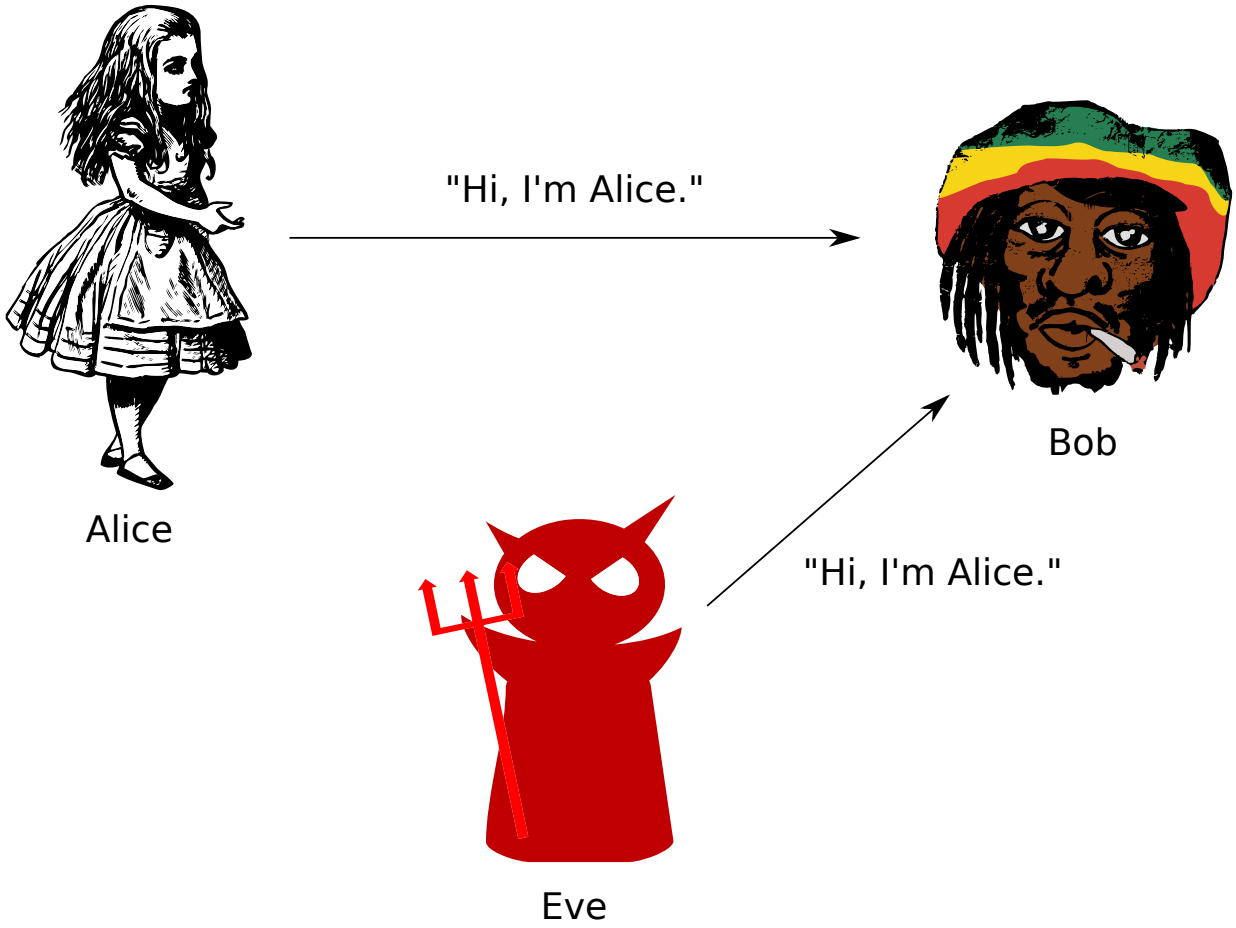
Sorbonne Université

January 10, 2019

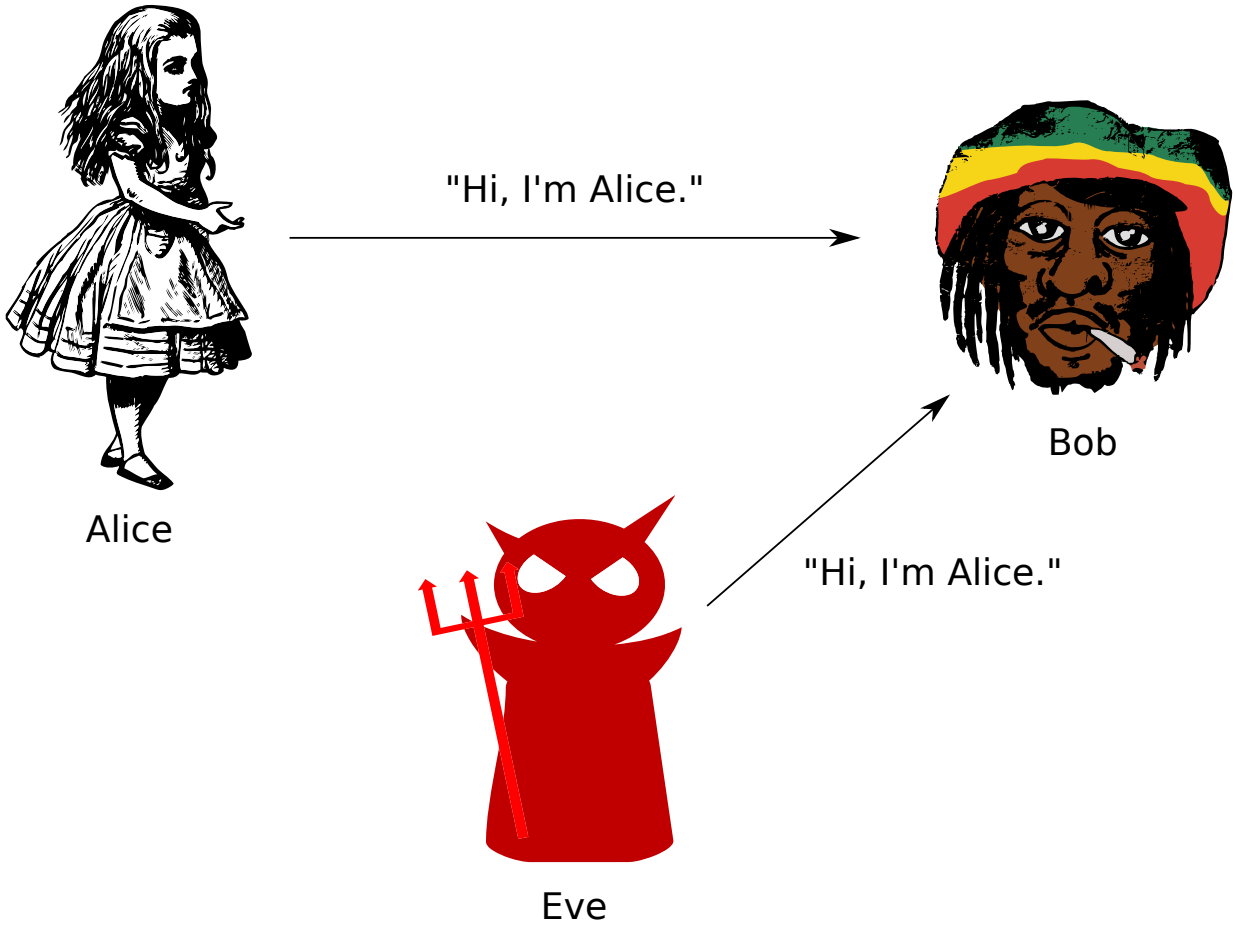
Alice

"Hi, I'm Alice."

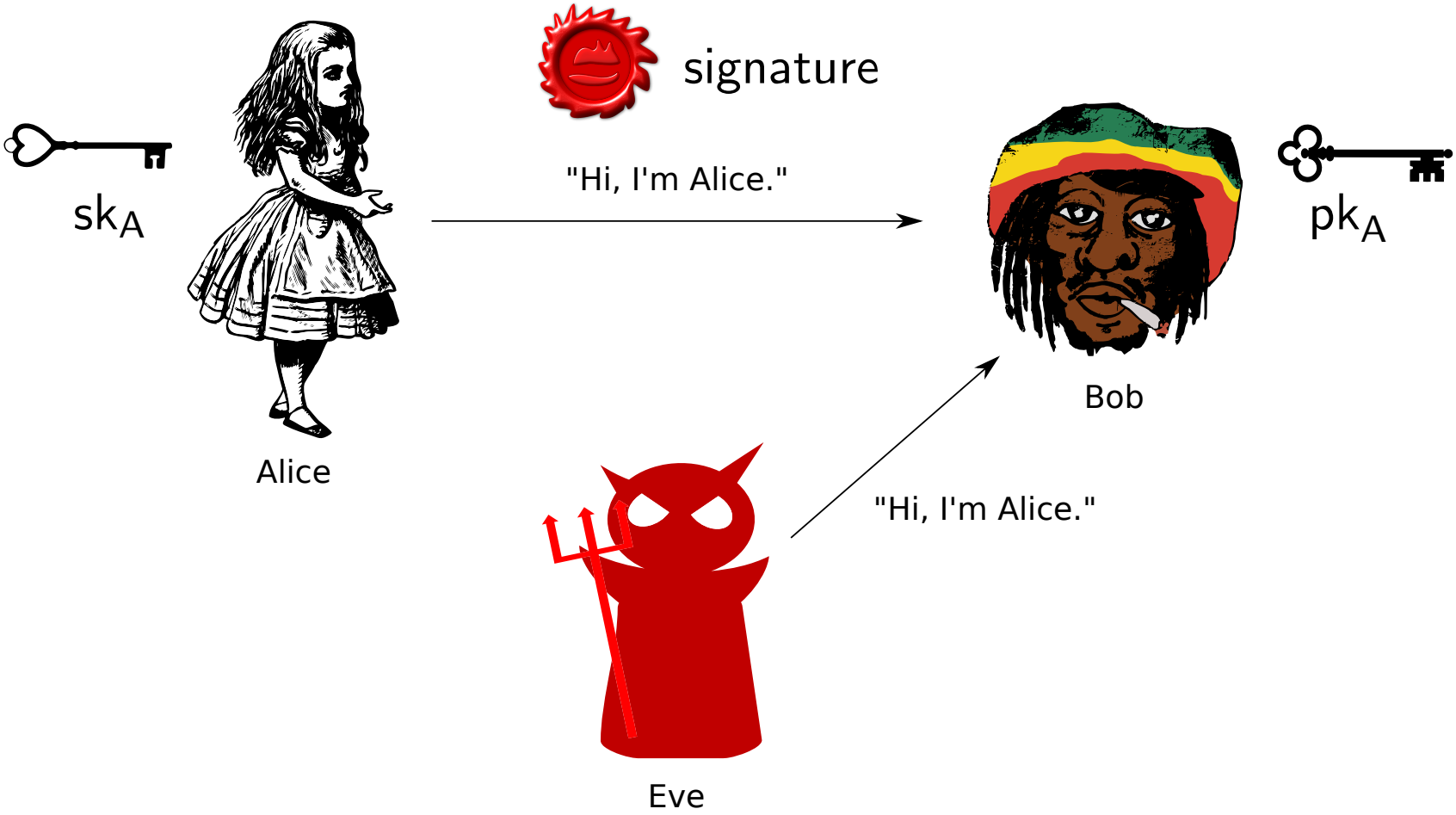
Bob


"Hi, I'm Alice."
Alice
Bob
"Hi, I'm Alice."
Eve

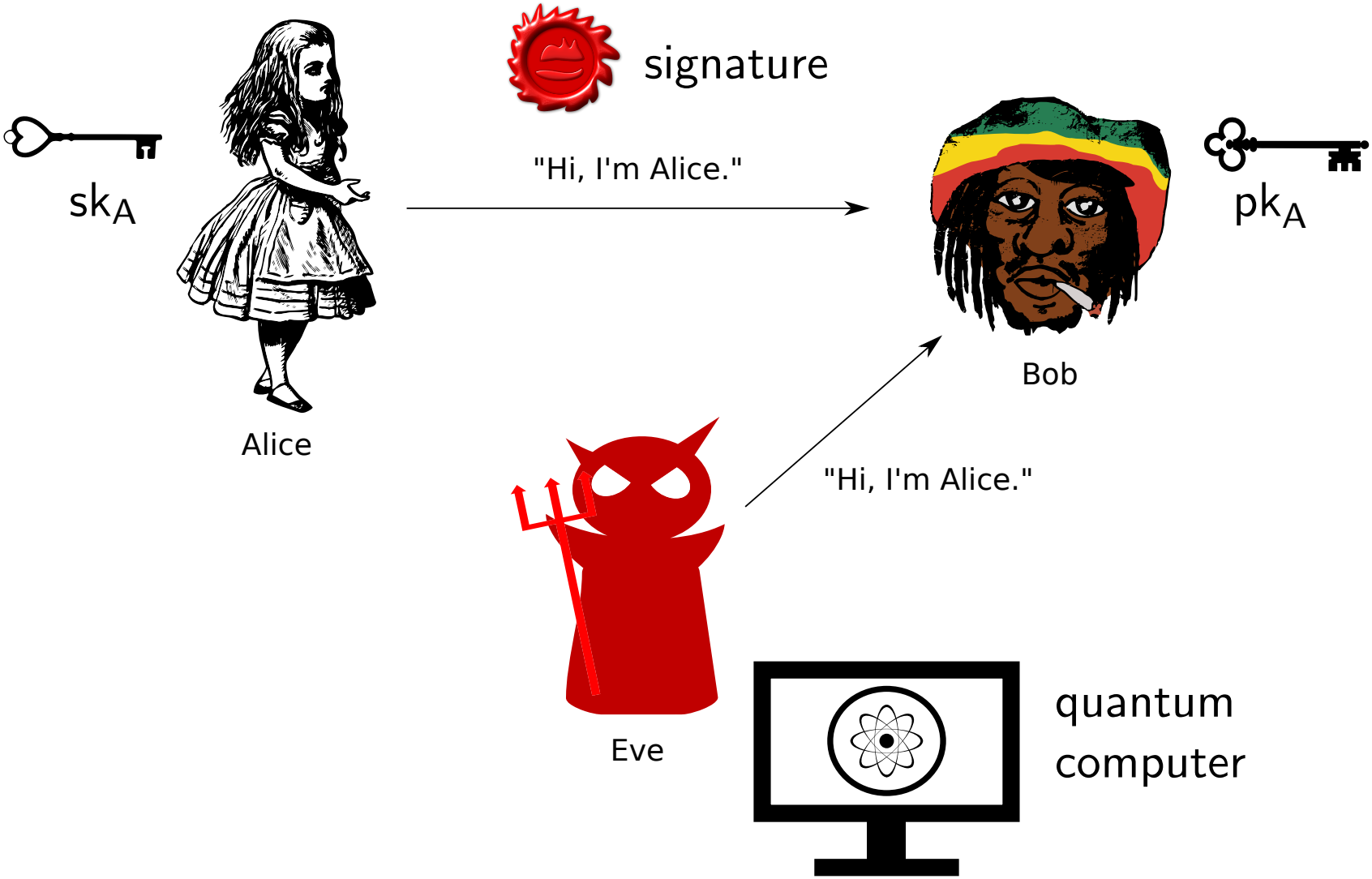
Authenticity and Integrity



Authenticity and Integrity



Authenticity and Integrity



Hard number-theoretic problems

Easy for quantum computers:

- Factoring
- Discrete logarithms

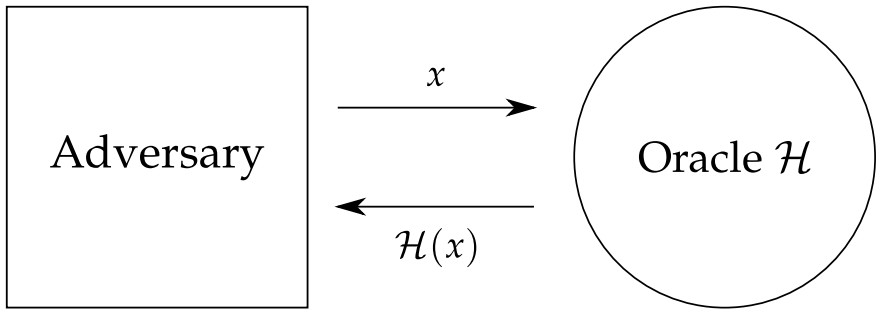
Problems assumed to be hard even for quantum computers based on:

- Coding theory
- Lattices
- Multivariate equations
- Isogenies between supersingular elliptic curves
- Mersenne primes
- ...

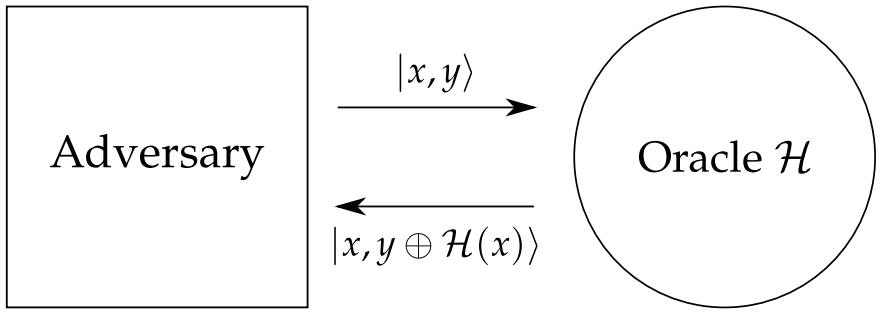
(Quantum) random oracle model

Hash functions have public descriptions: everybody can locally implement them

Classical ROM:



Quantum ROM:



(Quantum) random oracle model

How do quantum computers make the life of cryptographers harder?

- Quantum computers allow for faster attacks on symmetric cryptography, e.g.
  - Grover search for pre-image finding
  - Quantum collision search
- Some classical proof strategies in security reductions do not directly translate to the QROM, e.g.
  - Rewinding the adversary
  - Storing the state of an adversary

3-pass identification schemes

sk_A

Prover(sk) **Verifier**(pk)

$\mathsf{com} \leftarrow \mathcal{P}_0^{\mathsf{sk}}()$

com $\longrightarrow$

$\mathsf{ch} \leftarrow\!\!\$\ \mathit{ChSet}$

ch $\longleftarrow$

$\mathsf{resp} \leftarrow \mathcal{P}_1^{\mathsf{sk}}(\mathsf{ch})$

resp $\longrightarrow$

$\mathcal{V}^{\mathsf{pk}}(\mathsf{com}, \mathsf{ch}, \mathsf{resp})$?

pk_A

From ID to signature schemes

- 1987: Fiat-Shamir transform [FS87]
  - Security proof (only) in the Classical ROM
- 2014: Unruh transform [Unr14]
  - Security proof in the Quantum ROM
  - Large signatures
- 2017: Lossy Fiat-Shamir transform [KLS17]
  - Security proof in the Quantum ROM
  - Smaller signatures (than Unruh transform)
  - Additional requirement: lossy key generator

State of the art

128-bit post-quantum security level (all sizes in bytes)

Signature scheme	based on	sig size	sk size	pk size
Lossy-Stern-FS	**codes**	**218,485**	**32**	**218**
SOFIA-4-128	multivariate	126,176	32	64
Picnic-10-38	purely symmetric	195,458	32	64
SPHINCS$^+$-256f	hash-based	16,976	64	32
Elliptic Curve DSA	*pre-quantum*	*64*	*32*	*64*

Future work

Design shorter and more efficient signatures!
(without losing security)

Come visit: Campus UPMC, Lip6

Email: dominik.leichtle@lip6.fr