An Introduction to Quantum Computing

Lecture 11
Quantum Key Distribution

Paolo Zuliani

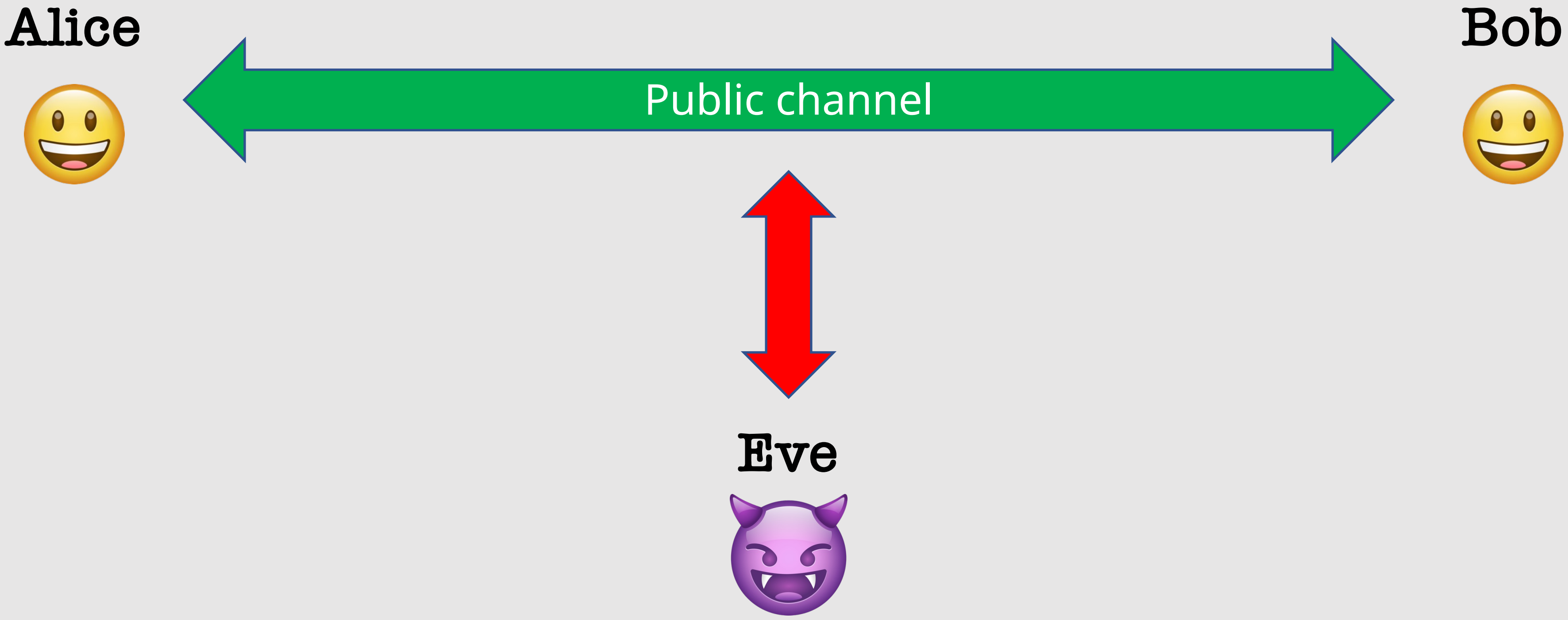
zuliani@di.uniroma1.it

Sapienza Università di Roma

Outline

- Communication context and problem
- One-time pad
- Privacy amplification
- Bennett & Brassard’s quantum key distribution (BB84)
- Post-quantum cryptography

Communication Context and Problem



Communication Context and Problem

Public-key cryptography:

- What are the prime factors of 4983749726021447820470189037 37?

- Best classical algorithms for integer factoring take time *exponential* in length of number.

- No one has showed that an efficient (*i.e.*, poly-time) algorithm cannot exist.

- Effectively: security based on unproven computational assumptions…

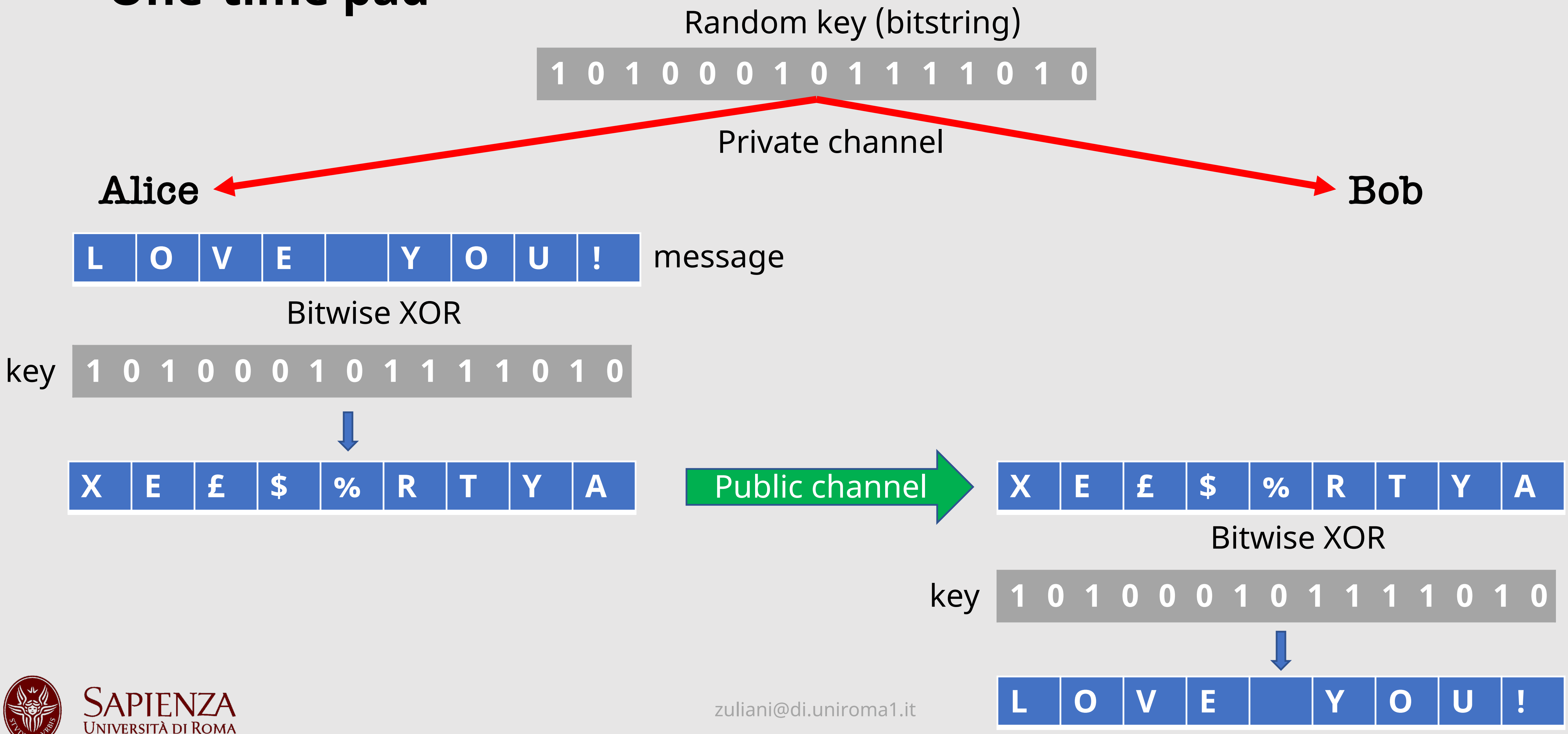
Communication Context and Problem

Private-key cryptography:

- Parties must share a *private* key.
- Benefit: can be *perfectly* secure!
- Effectively: security based on privacy.
- Disadvantage: how to share a private key?
  - Trusted couriers
  - Private communication lines (*e.g.*, red phone between USA – USSR)
  - Covert operations
  - *etc* …

Private-key Cryptography

One-time pad



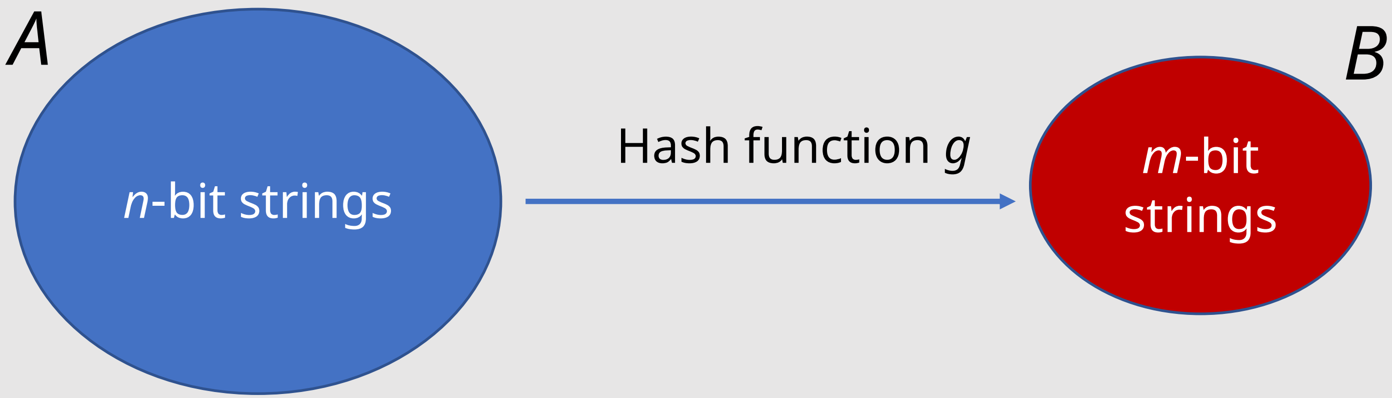
Private-key Cryptography

- Key and message must have the ***same length*** ⇒ the only perfectly secure cryptosystem!!
- Keys should be guarded at *all times*.
- Keys should be *destroyed after use*; else reduced privacy.
- How to distribute random keys securely? BB84!

Privacy Amplification

- Alice and Bob share a bitstring, but Eve has some knowledge of it.
- Can Alice and Bob “distil” a more secure key that reduces Eve’s knowledge of the key?

Universal Hash Functions



$$\forall a_1, a_2 \in A, \quad g \text{ randomly chosen hash function} \Longrightarrow \mathrm{Prob}(g(a_1) = g(a_2)) \leq \frac{1}{|B|}$$

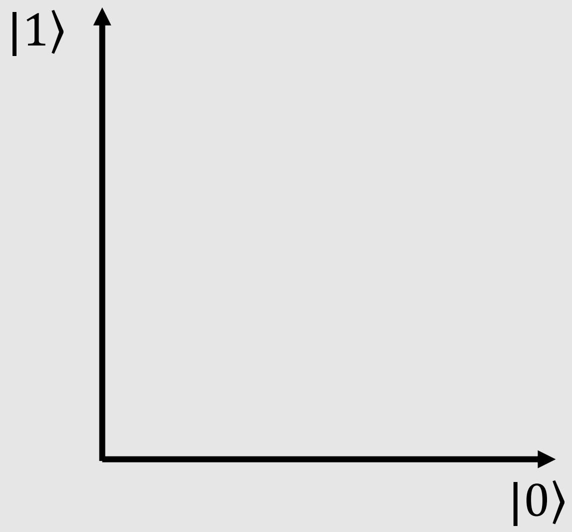
Privacy Amplification

- Alice and Bob *publicly* select a universal hash function g.
- They apply g to their shared bitstring W – the output $g(W)$ will be their secret key S.
- It can be shown that if Eve's entropy (knowledge) on $W > d$, then

Eve's entropy on $S \geq m - 2^{m-d}$

The BB84 QKD Protocol

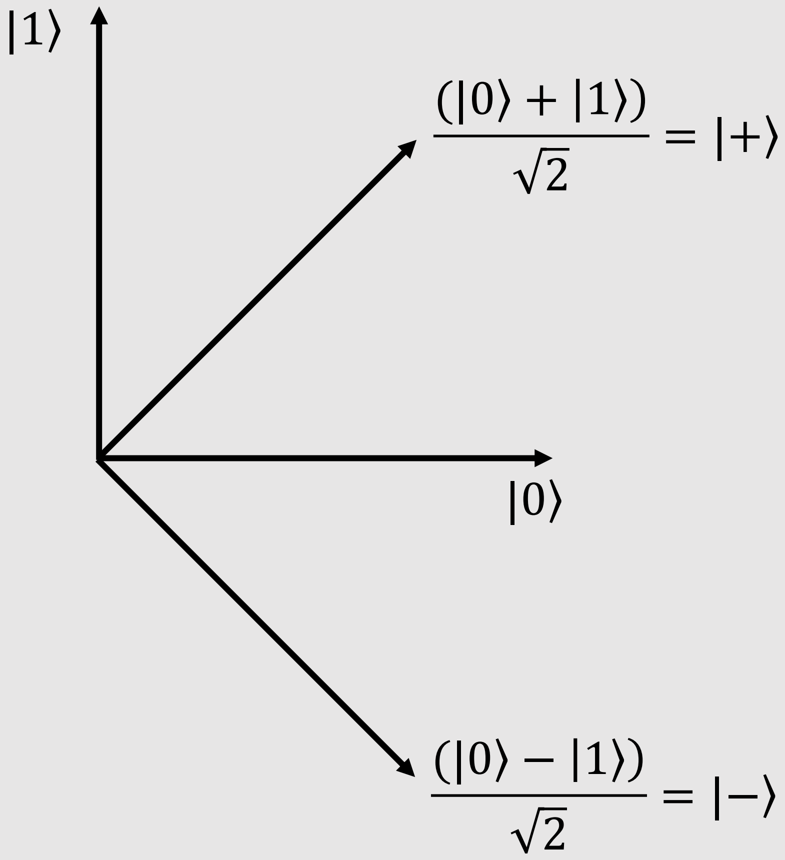
- Enables Alice and Bob to share a random bitstring (key) over ***public quantum/classical channels***
- Security based on the validity of Quantum Physics only. (Philosophy mode off!)
- **Main idea**: trying to distinguish two *non-orthogonal quantum states* implies disturbance!



Suppose you know a qubit is either in state $|0\rangle$ or $|1\rangle$. (These two states are orthogonal.)

By measuring it you can learn ***precisely*** its state.

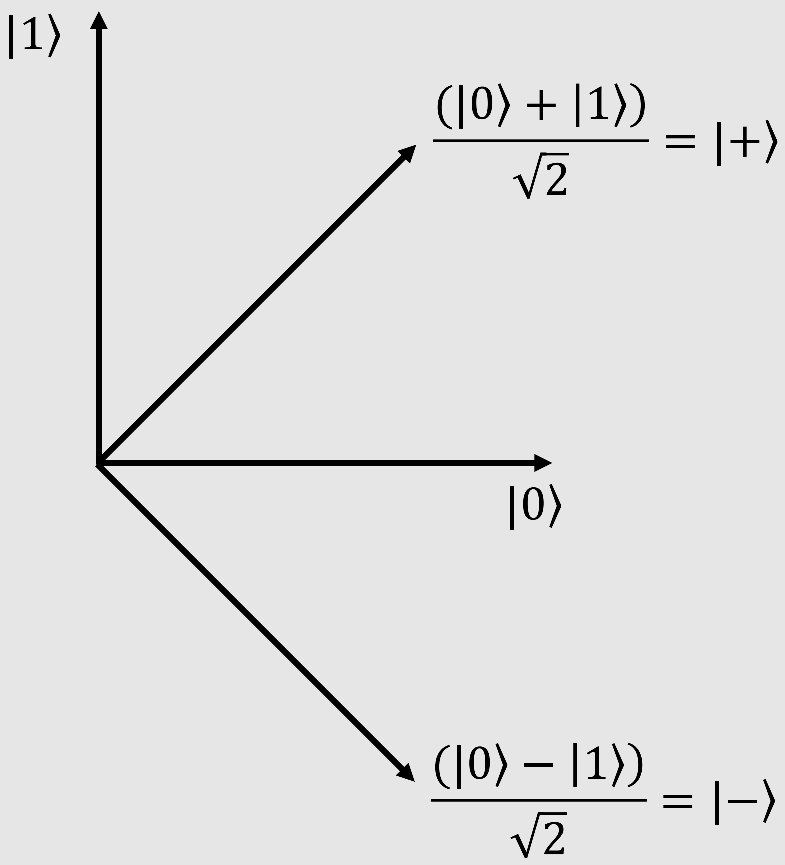
The BB84 QKD Protocol



Suppose your qubit is either in state $|+\rangle$ or $|-\rangle$.
(These two states are again orthogonal.)

By rotating it and then measuring it you can learn ***precisely*** its state.

The BB84 QKD Protocol



Suppose your qubit is either $|0\rangle, |1\rangle, |+\rangle$ or $|-\rangle$. These states are no longer orthogonal!

Distinguishing is now trickier …

One measurement is definitely not sufficient! (It will destroy the state.)

The BB84 QKD Protocol

Alice **Bob** time

Choose random bitstrings *a*, *b* of length *N* ‘big enough’

Produce *N* qubits $Q = \otimes_{i=1}^{N} |q_{a_i b_i}\rangle$

$$|q_{00}\rangle = |0\rangle$$
$$|q_{10}\rangle = |1\rangle$$
$$|q_{01}\rangle = |+\rangle$$
$$|q_{11}\rangle = |-\rangle$$

Send Q to Bob

Public quantum channel

$Q' = \otimes_{i=1}^{N} |q_{a_i b_i}\rangle$

The BB84 QKD Protocol

Alice | **Bob** | time

Choose random bitstring b' of length N 'big enough'

Measure each qubit in Q' with basis $|0\rangle, |1\rangle$ or $|+\rangle, |-\rangle$ depending on b'

Store measurement results in bitstring a'

Publish bitstring b — Public classical channel — Publish bitstring b'

The BB84 QKD Protocol

time

Alice

Store in *W* the bits of *a* for which *b*=*b′*

Select a random substring of *W* and compare with Bob

Check fails → **Abort**

OK ↓

Privacy amplification on remaining *W* bits

Highly secure key

Public classical channel

Bob

Store in *W′* the bits of *a′* for which *b*=*b′*

Select a random substring of *W′* and compare with Alice

Check fails → **Abort**

OK ↓

Privacy amplification on remaining *W′* bits

Highly secure key

Post-Quantum Cryptography

- Quantum computers can (in principle) break factoring-based crypto.
- Probably still 1-2 decades away but getting too close for comfort.
- Stored data (might?) need re-encoding with longer keys.
- Cryptosystems that are quantum-safe: lattice based?
  - A putative quantum-safe cryptosystem was recently broken on a laptop
  - April 2024: mistake found in quantum algo for breaking lattice-based cryptosystem …
- Currently, no quantum-secure cryptosystem is available.
- Links:
  - https://csrc.nist.gov/projects/post-quantum-cryptography
  - https://ianix.com/pqcrypto/pqcrypto-deployment.html