Quantum Computing
and
Quantum Cryptography

Thierry Sans

Quantum Computing

A quantum computer uses **quantum bits** and relies on of **quantum-mechanical phenomena** to perform computation

1. Brute-forcing n-bits key with Grover's algorithm would take $\mathbf{2^{n/2}}$
   - ➡ Using symmetric encryption is still doable

2. Factoring prime numbers with Shor's algorithm would be done in polynomial time
   - ➡ Using asymmetric encryption is at risk
   - ➡ Problem for key exchange

Post-quantum Cryptography

Cryptographic schemes that can defeat quantum computers

➡ Still in research (started around 2006)

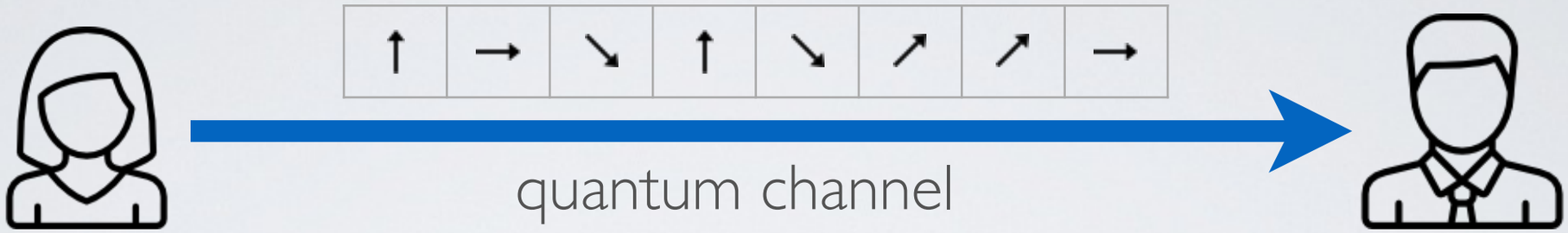
https://en.wikipedia.org/wiki/Post-quantum_cryptography

Quantum Cryptography

The use uses quantum bits and quantum-mechanical phenomena to realize cryptographic tasks

➡ Example : Quantum Key Distribution - use a quantum channel to establish a shared key to use on a public channel

Quantum Key Distribution - step 1

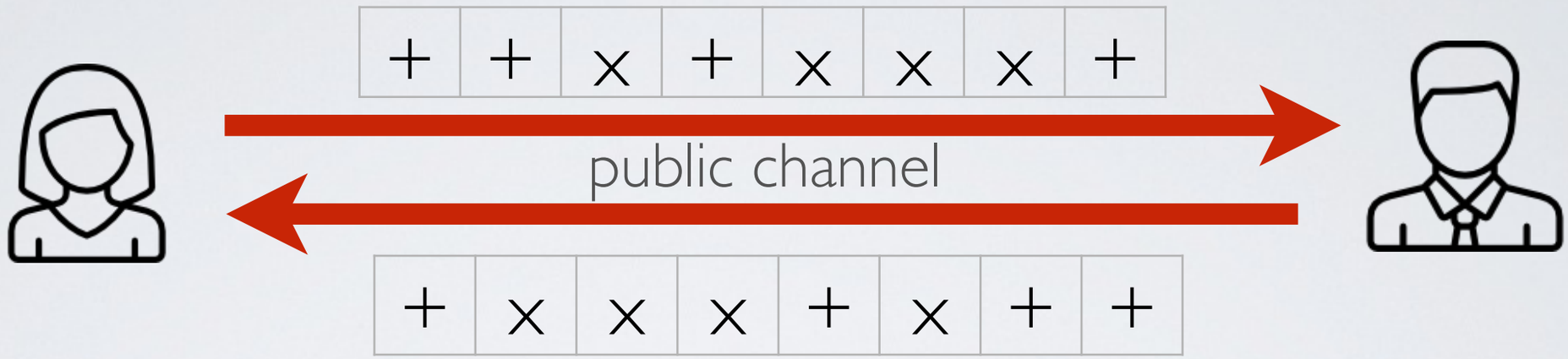


0	I	I	0	I	0	0	I
+	+	×	+	×	×	×	+
↑	→	↘	↑	↘	↗	↗	→

+	×	×	×	+	×	+	+
↑	↗	↘	↗	→	↗	→	→

1. Alice creates:
   I. a sequence of random sequence of bits
   II. a sequence of random sequence of basis
   III. a sequence of random sequence of polarized photons corresponding to the basis
2. Alice sends the photon sequence to Bob over the quantum channel
3. Bob selects a random sequence of basis
4. Bob measures Alice's sequence of photons using his basis

Quantum Key Distribution - step 2



0		I			0		I

0		I			0		I

5. Alice and Bob exchange their sequence of basis on the public channel

6. The basis that are commonly correct are used to generate the key

Quantum Key Distribution - step 3

0	I	0	I

0	I	0	I

0	I

public channel

0	I

Has Eve eavesdrop on the quantum Channel ?

➡ Eavesdropping the quantum channel modifies the polarization of the photons

7. Alice and Bob spare and exchange a sub sequence of their shared secret key
8. If this subsequence match, it means that nobody has eavesdrop the quantum channel. If not, the key is invalid.