Quantum Computing
Post-Quantum Cryptography
Quantum Cryptography

Thierry Sans

Quantum Computing
Post-Quantum Cryptography

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 safe**

2. Factoring prime numbers with Shor's algorithm would be done in polynomial time
   ➡ **Using asymmetric encryption (key exchange and digital signatures) is at risk**

Post-Quantum Cryptography

Cryptographic schemes that can defeat quantum computers

➡ Still in research (started around 2006)

➡ On August 2024, the NIST released final versions of the first three Post Quantum Crypto Standards

➡ On November 2024, the NIST has announced prohibiting classical cryptography (RSA, DSA, ECDSA, ECDH) after 2035

	ML-KEM (Module-Lattice Key Encapsulation)	**ML-DSA** (Module-Lattice Digital Signature)	**SLH-DSA** (Stateless Hash-Based Signature)
Standard	FIPS-203	FIPS-204	FIPS-205
Purpose	**Key Exchange** to generate a 256-bits shared key	**Digital Signature Scheme** that offers a good balance of performance relative to signature sizes	**Digital Signature Scheme** designed as a fallback / conservative option with smaller public keys but large signatures and slower performances
Description	Exists in three versions ML-KEM-512 ML-KEM-768 ML-KEM-1024	Exists in three versions ML-DSA-44 ML-DSA-65 ML-DSA-87	Exists in 12 variants as combinations of different key sizes (128, 192, 256), different hash (Sha2, Shake) and different algorithm trade-off (small vs fast)
Algorithm and Mathematical Foundation	Module Learning With Errors (MLWE) based on a lattice approach	CRYSTALS-Dilithium based on lattice signature	SPHINCS+ a purely hash-based signature scheme, does not rely on a lattice approach

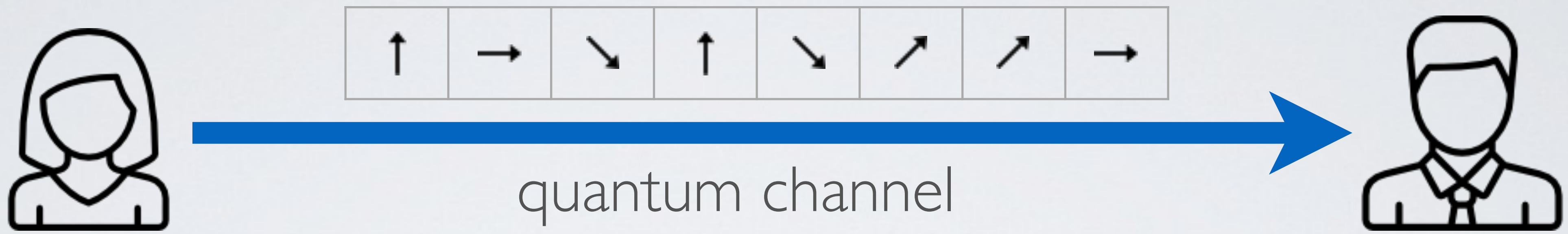
Quantum Cryptography

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

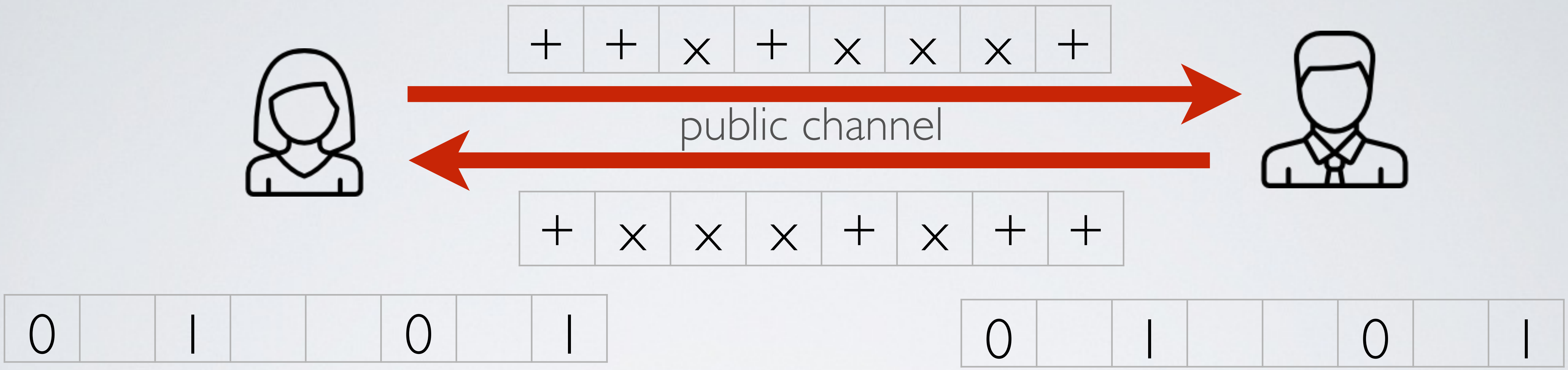


0	1	1	0	1	0	0	1
+	+	×	+	×	×	×	+
↑	→	↘	↑	↘	↗	↗	→

+	×	×	×	+	×	+	+
↑	↗	↘	↗	→	↗	→	→

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

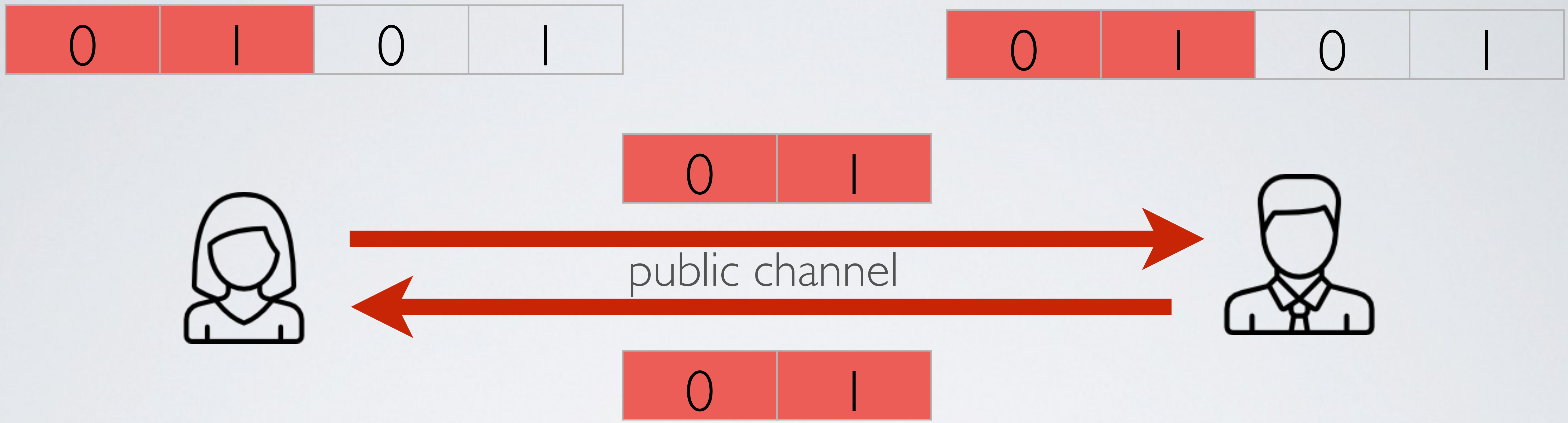
Quantum Key Distribution - step 2



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



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.