Quantum Communication
PAF Day 5

24 Juin 2022

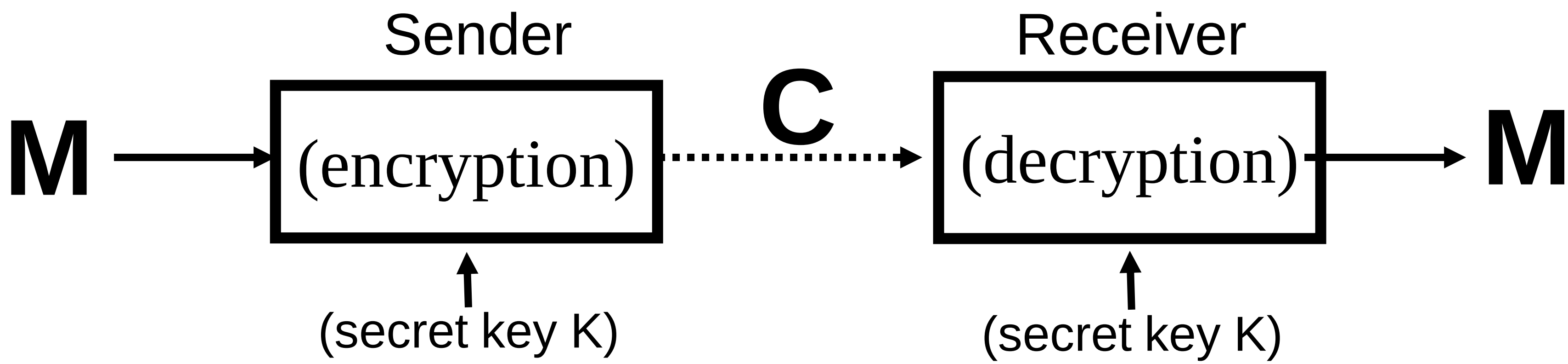
Francesco Mazzoncini
mazzoncini@telecom-paris.fr

Plan du cours

- Cryptographie quantique et cryptographie classique
- Principe de la Distribution Quantique de Clé (QKD)
- Real-World QKD

Cryptographie quantique et cryptographie classique

Symmetric-Key Cryptography



- Traditional (before 1970's) **private/secret/symmetric key** cryptography uses **one** key
- Same key shared by both sender and receiver => **Symmetric**

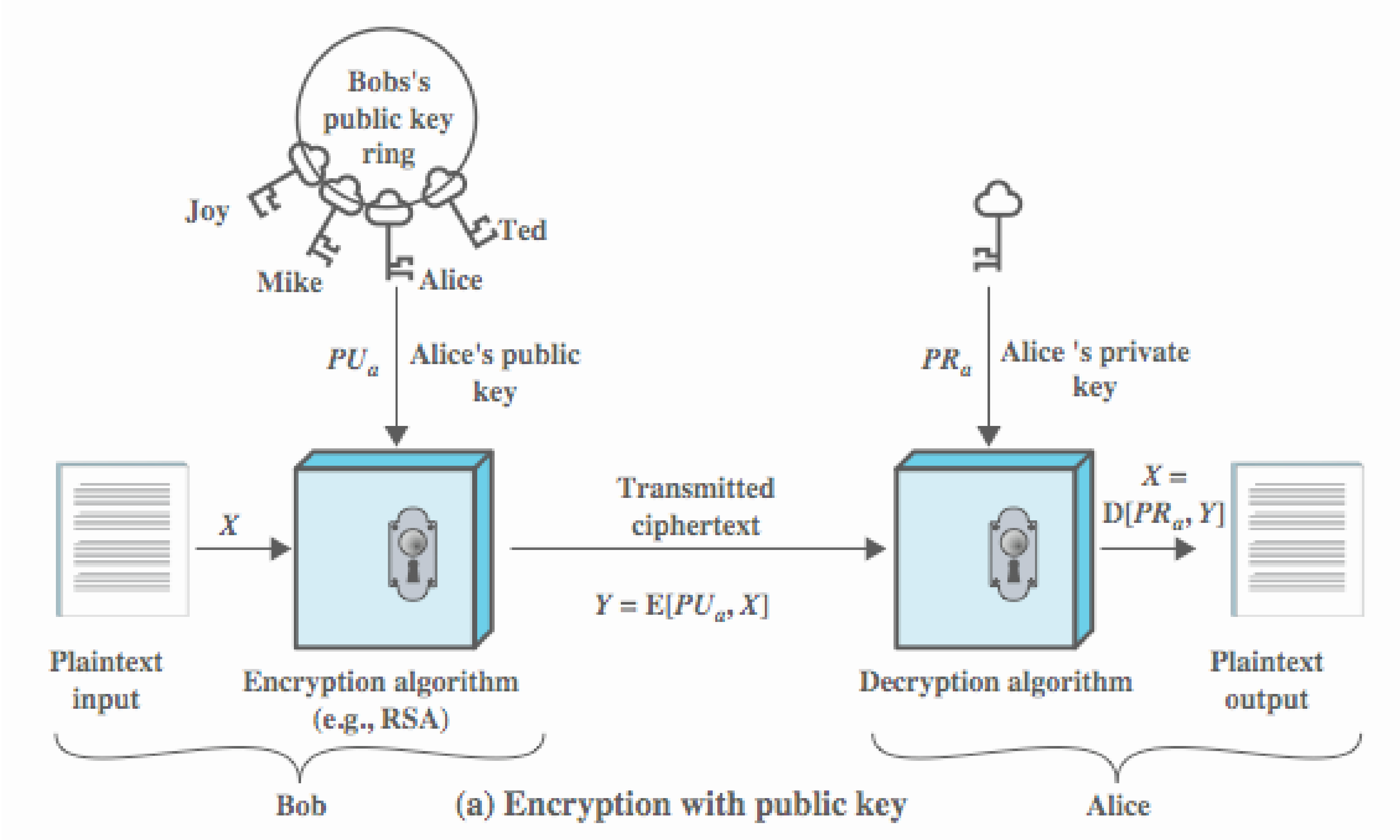
- *If this key is disclosed communications are compromised*
- *Does not protect sender from receiver forging a message & claiming is sent by sender (encryption ≠ authentication)*

Public-Key Cryptography

- Probably most significant advance in the 3000 year history of cryptography
- Uses **two** keys – a public & a private key
- **Asymmetric** since parties are **not** equal
- Uses clever application of number theoretic concepts to function
- Complements **rather than** replaces private key crypto

- Developed to address mainly two key issues:
  - **key distribution** – how to have secure communications in general without having to trust a KDC with your key
  - **digital signatures** – how to verify a message comes intact from the claimed sender

Example: RSA Public-Key encryption



Any person (here Bob), in posession of Alice public key can send confidential message to Alice

Asymmetric : B→ A

Cryptographie: Symétrique vs. asymétrique

Chiffrement symétrique (à clé secrète)

- Pros
  - Clé courte (~100 bits)
  - Chiffrement / déchiffrement rapide
- Cons
  - Distribution sécurisée de la clé
- Utilisation
  - Chiffrement de grand volume de données
- Exemples d'algorithmes
  - AES
  - DES

Chiffrement asymétrique (à clé publique)

- Pros
  - Pas nécessaire d'échanger la clé secrète (seule la clé publique est publiée)
- Cons
  - Clé longue (~ 1000 bits)
  - Calcul intensif
- Utilisation
  - Distribution de clés secrètes
  - Signature numérique
- Exemples d'algorithmes
  - RSA
  - Diffie-Helman

Modern cryptography : computational assumptions

Example1: Hardness of breaking AES128 encryption

Assumptions: AES (block cipher) is a secure one-way function

➔ Best attack is exhaustive search, requires 2^{128} operations

Example2: Hardness of factoring

Assumption: Best known factoring algorithm (General Field Number Sieve) is **sup-exponential**

Factoring large number N, requires Exp [O((ln n)$^{1/3}$)] operations

Remark: what about pratical computing power ?

(individu, ~10 k$)

1 GHz * 100 (parallélisation) * 1 an ~ 2^{52}

(grande organisation type NSA ~1000 M$)

10 Petaflops * 1 an ~ 2^{78}

One Time Pad OTP – Masque Jetable (Vernam 1917)

$M=C=K=\{0,1\}^n$

Chiffrement

$C = E(k, m) = k \oplus m$

Déchiffrement

$D(k, c) = k \oplus c$

Msg M:	0 1 1 0 1 1 1	$\oplus$
Key K:	1 0 1 1 0 1 0	
Ciphertext		
C:	1 1 0 1 1 0 1	

Shannon (1949): OTP vérifie la propriété de sécurité inconditionnelle

Key distribution problem and public-key crypto

Shannon positive result (1949):

- One-Time-Pad verifies the perfect secrecy condition

Shannon negative result (1949):

- Perfect secrecy condition requires $|K| \geq |M|$

➔ Secret-key distribution problem

➔ Information-theoretic security considered non-practical

Public-key cryptography

- Diffie-Hellman 1976
- RSA 1978

Current solution to the key distribution problem

Need for Quantum Resistant (Post-Quantum) Crypto

Threats on existing public-key cryptography

~~RSA, Elliptic Curve,~~

~~Discrete Log (DH,..)~~

If X+Y > Z ➔ PANIC (Mosca Th.)

NIST Call for Quantum Resistant

First call in 2017

➔ first standards in 2022/ 2024

Public-key cryptosystem	Example	Year
Code-based cryptography	McEliece encryption scheme	1978
Hash-based cryptography	Merkle's hash-tree signature system	1979
Lattice-based cryptography	NTRU encryption scheme	1996
Multivariate-quadratic-equations	HFE signature scheme	1996

Table 1.1: List of post-quantum cryptography

Principe de la QKD
(distribution quantique de clé)

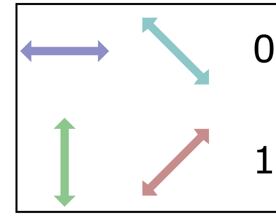
Protocole BB84

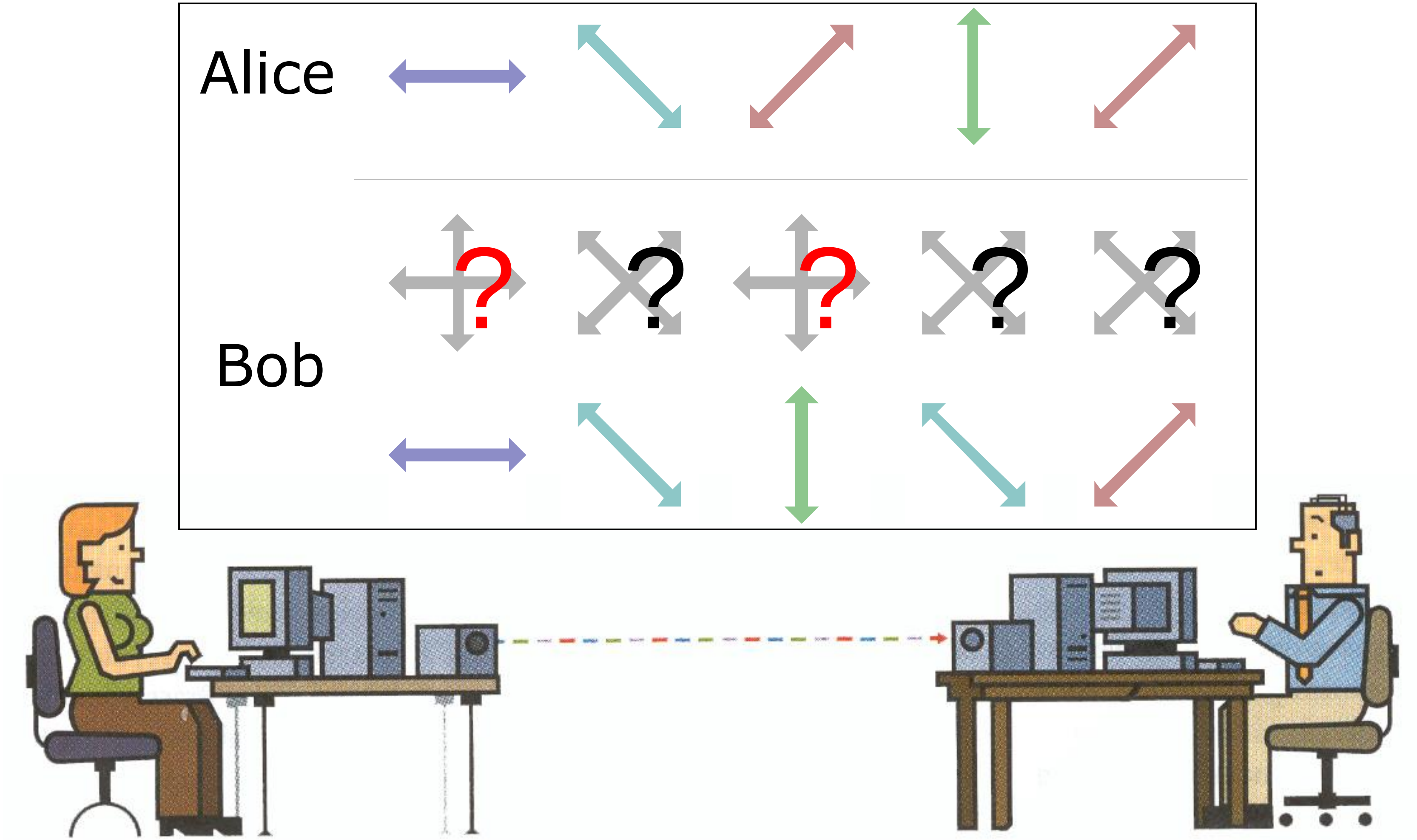
Precursor of quantum crypto: Quantum Money

Uncloneable Quantum Banknotes
Wiesner, 1969 .. Published 1983

Crucial ideal: Conjugate Coding
Encode 1 bit into 1 qubit using 2 complementary basis

BB84: Transmission

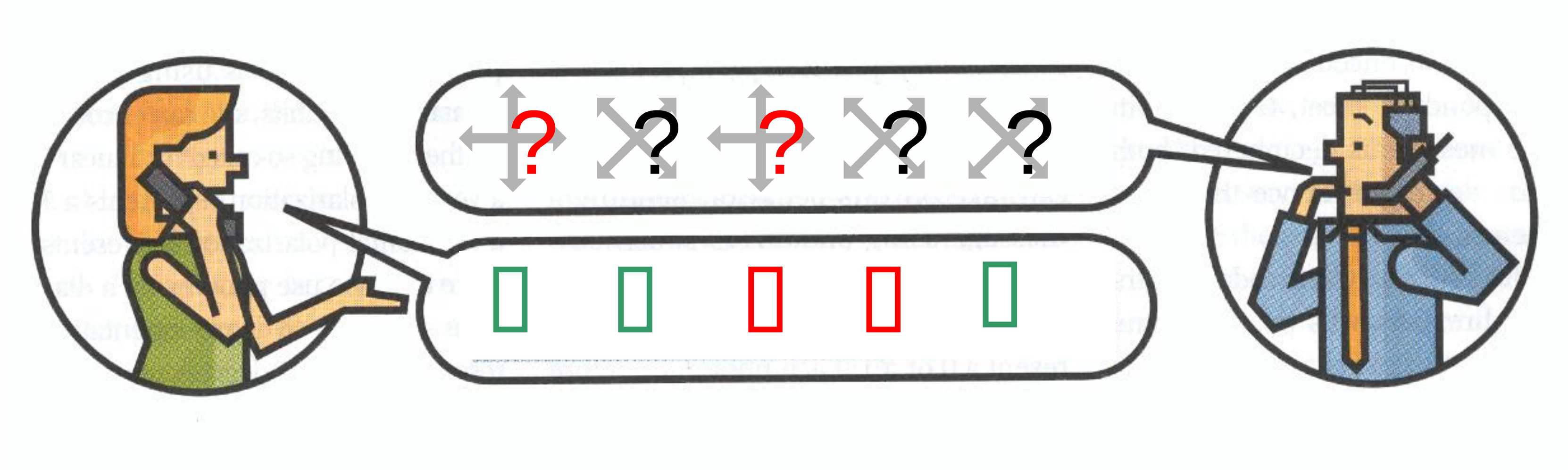




Dessins issus de IEEE Spectrum

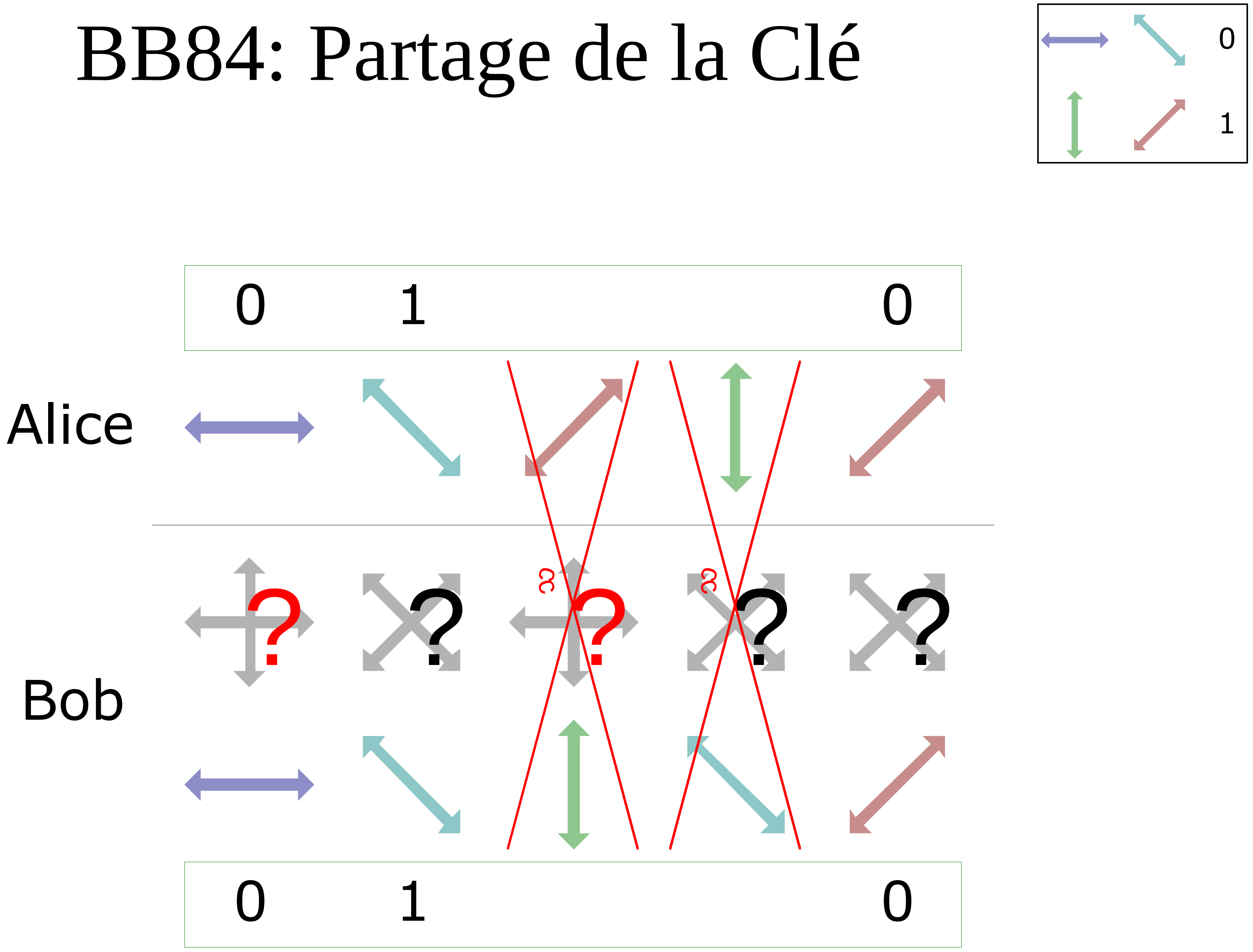
BB84: Tamisage/ Sifting

- Eliminer les mesures qui ne correspondent pas
  - Utilisation d’un canal **public**



Dessins issus de IEEE Spectrum

BB84: Partage de la Clé



Nécessite d'étapes supplémentaire pour "fabriquer une clé"

Données initiales (clé brute)

- **contiennent des erreurs**
- **Peuvent donc aussi être correlées à l'espion Eve**

⬇

Il faut corriger les erreurs

Il faut distiller une clé totalement inconnue d'Eve

➔ *Etapes de reconciliation (canal Classique)*

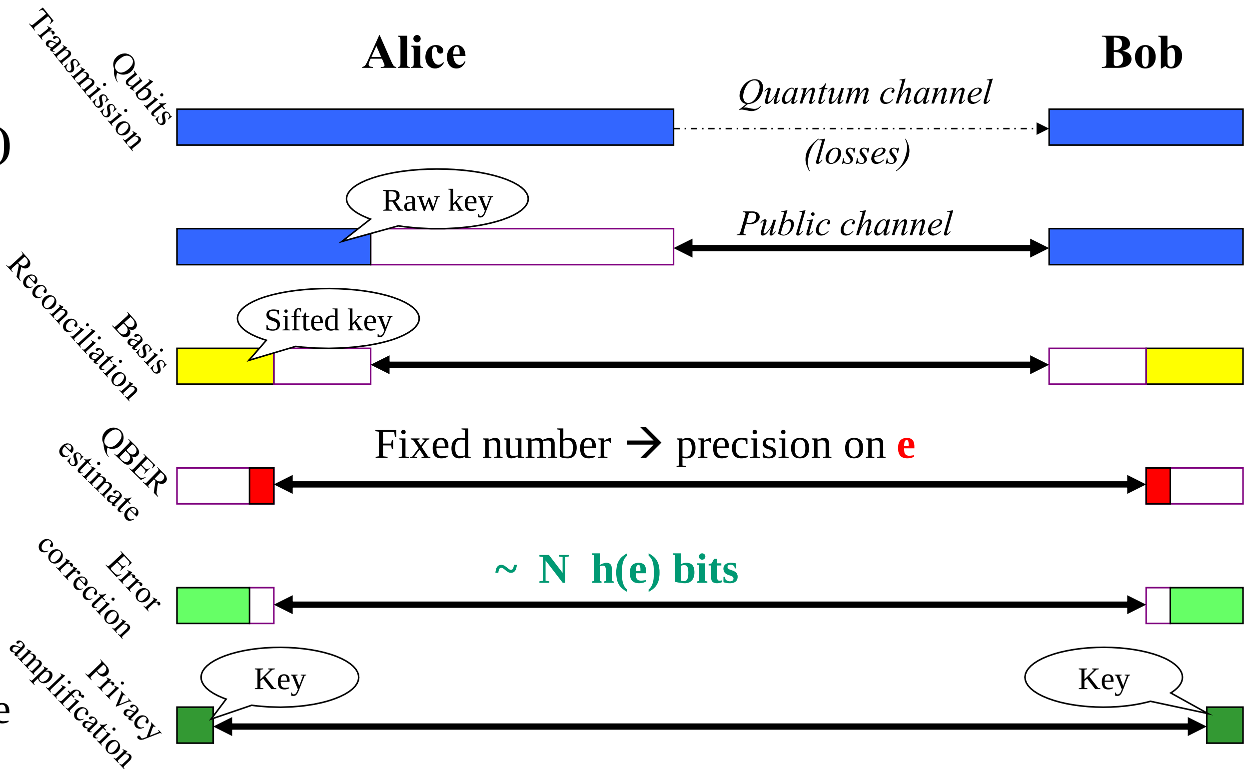
The steps to a secret key

~ **M signals** **(channel uses)**

~ **MT signals**

~ **MT/2 = N signals**

Need to remove
~ **N h(e) bits**
(security proof)



~ **MT signals received**

N bits (BB84)

+ Authentication!!!

Key Rate $_{\text{BB84}}$ per ch.use ~ T (1-2 h(e))

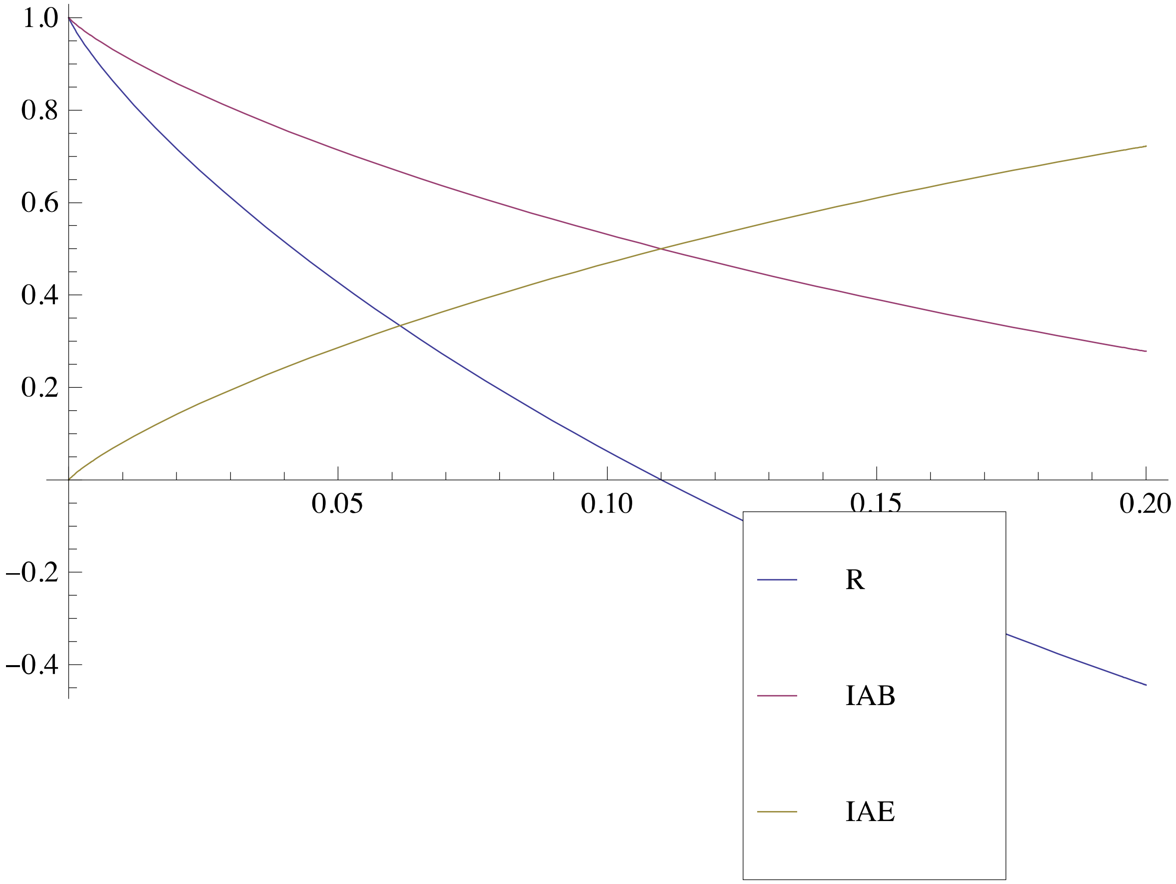
Secure key rate: (depends on Eve attack power)

Main idea: Csiszar Körner, (for classical correlated data $X_{A,}$ $X_{B,}$ X_E)$_,$

$$R(XA\,;\,XB\,||\,X_E\,)\ \geq \max[\,I(X_A\,;\,X_B)\,-\,I(X_A\,;\,X_E)\,,$$
$$I(X_B\,;\,X_A) - \,I(X_B\,;\,X_E)\,]$$

- **Direct reconcilation: R$\geq$ I(X_A ; X_B) - I(X_A ; X_E)**
- Reverse reconciliation: R $\geq$ I(X_B ; X_A) - I(X_B ; X_E)

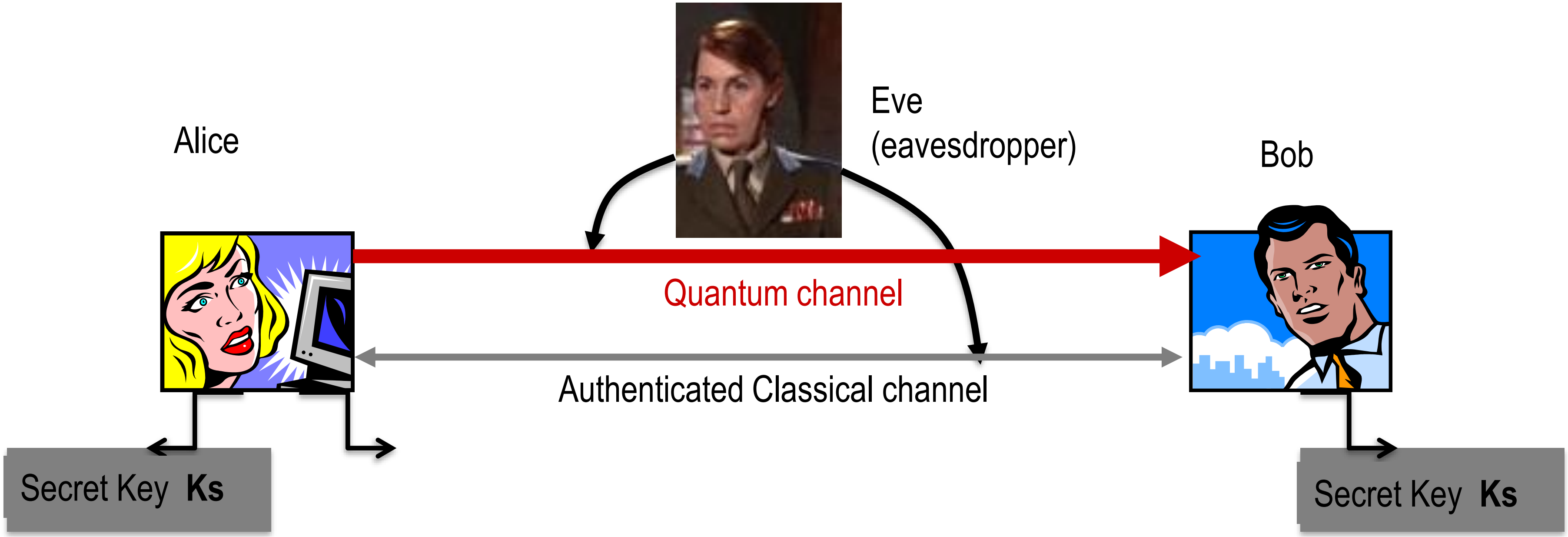
BB84 Secure key rate against collective and coherent attacks



BB84 : $R_{\text{(secure key rate)}}$ ~n (1-2 h(QBER))

Taux d’erreur tolérable maximal ~11 %

Quantum Key Distribution (QKD): general setting



- Intuition for security:
  Any measurement by Eve leads to detectable perturbation by Alice/Bob

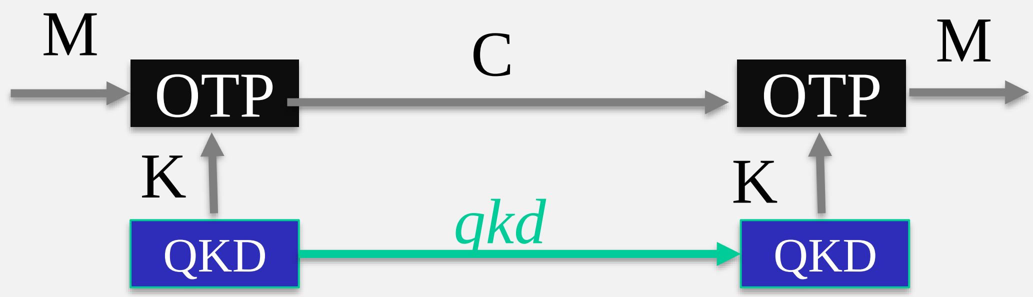
- **Specificity: Information-Theoretic Security (ITS)** [Unconditional Security]
  - No assumption about Eve computational power
  - « Future-proof »

QKD combined with encryption: Secure Communication

One-Time Pad rekeying

☺ ITS

➔ Perfect Secrecy

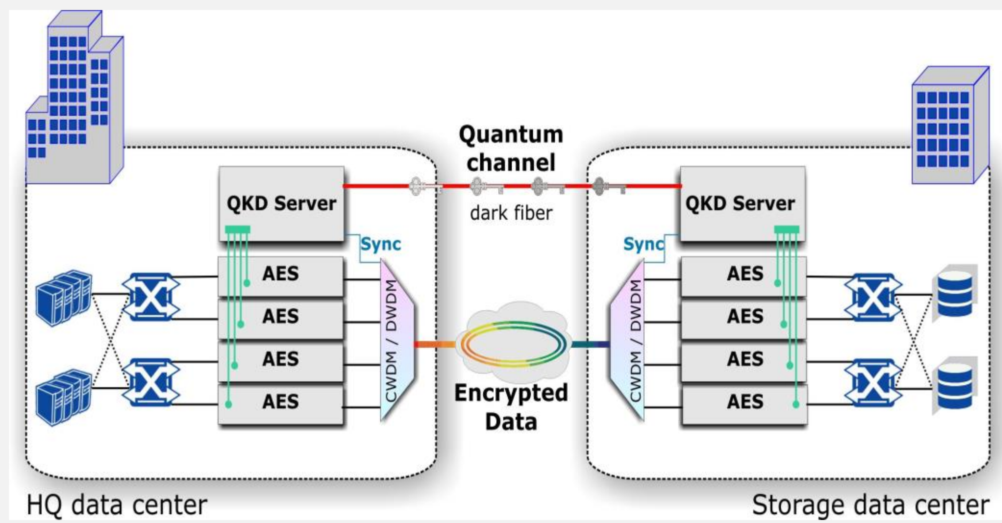


☹ Rate = QKD Rate ≤ 1Mb/s

AES Rekeying

☺ High Rate ~ 10 Gb/s

☹ Less Security Gain



QKD mostly useful when long-term security is needed

Long-term secrets
- Industry, IP
- Military
- Governmental

Personal Data
- Medical record
- Genomic
- Private

Computational Cryptography
Based on hardness of mathematical problems

Generic Vulnerability (incl. PQC)

Harvesting Attack
”Intercept now, decrypt later ”

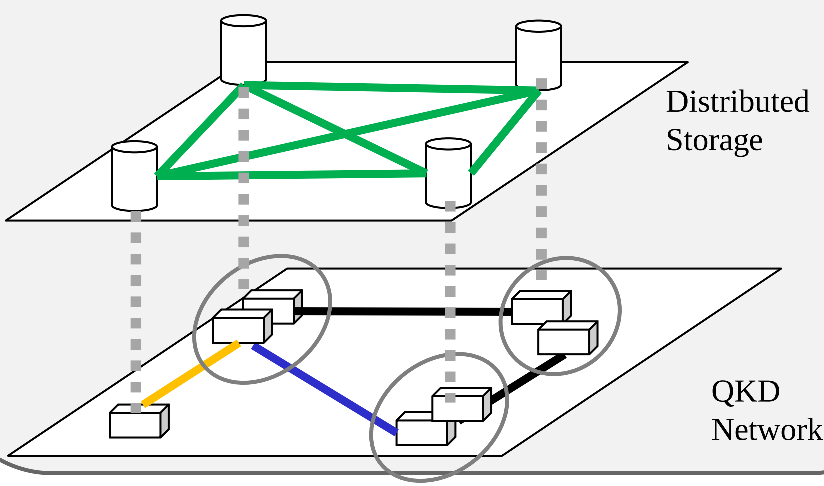
NSA Bullrun program

Long-Term Secure Storage

Need:
Confidentiality (integrity, availability) over 30+ years

Principle: Proactive Secret Sharing
➔ Protects against storage node corruption

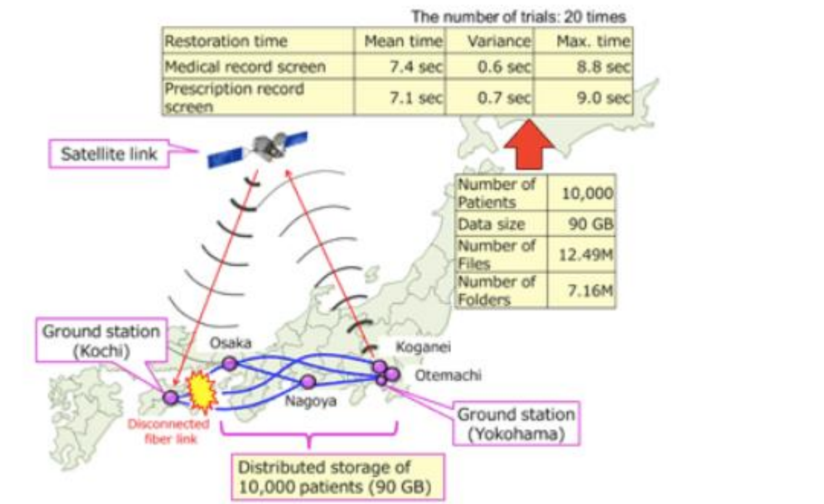
Requirements:
- Distributed Storage Infrastructure
- Secure Communication with ITS
    - *Impossible Classically*
    - ➔ ***QKD + OTP***



Initial demonstration

Braun, Johannes, J. Buchmann et al. "LINCOS: A storage system providing long-term integrity, authenticity, and confidentiality." *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. 2017.

+ 2 OpenQKD Use-Cases
& Pilot implementations in Japan



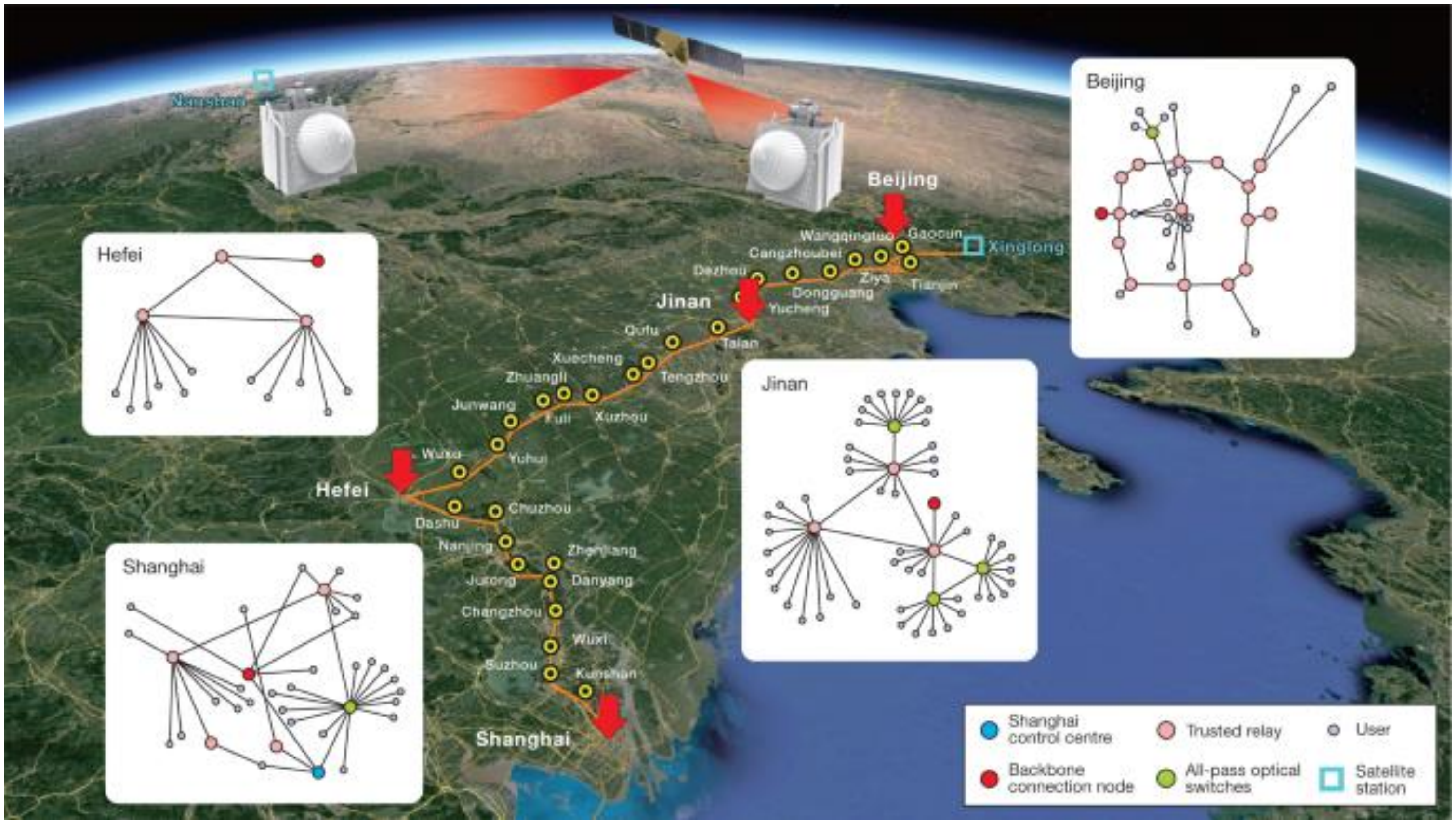
Restoration time	Mean time	Variance	Max. time
Medical record screen	7.4 sec	0.6 sec	8.8 sec
Prescription record screen	7.1 sec	0.7 sec	9.0 sec

Number of Patients	10,000
Data size	90 GB
Number of Files	12.49M
Number of Folders	7.16M

Figure 1: Network configuration of H-LINCOS and experimental results

Real-World QKD

QKD Networks – overview of major prototypes



- 4 metropolitan areas
- 32 trusted relays
- 150 users
- 700 fibre links

Span $\sim 4600\ km$

QKD Networks – overview of major prototypes

Initiated by the European Commission in 2019

Currently under negotiation

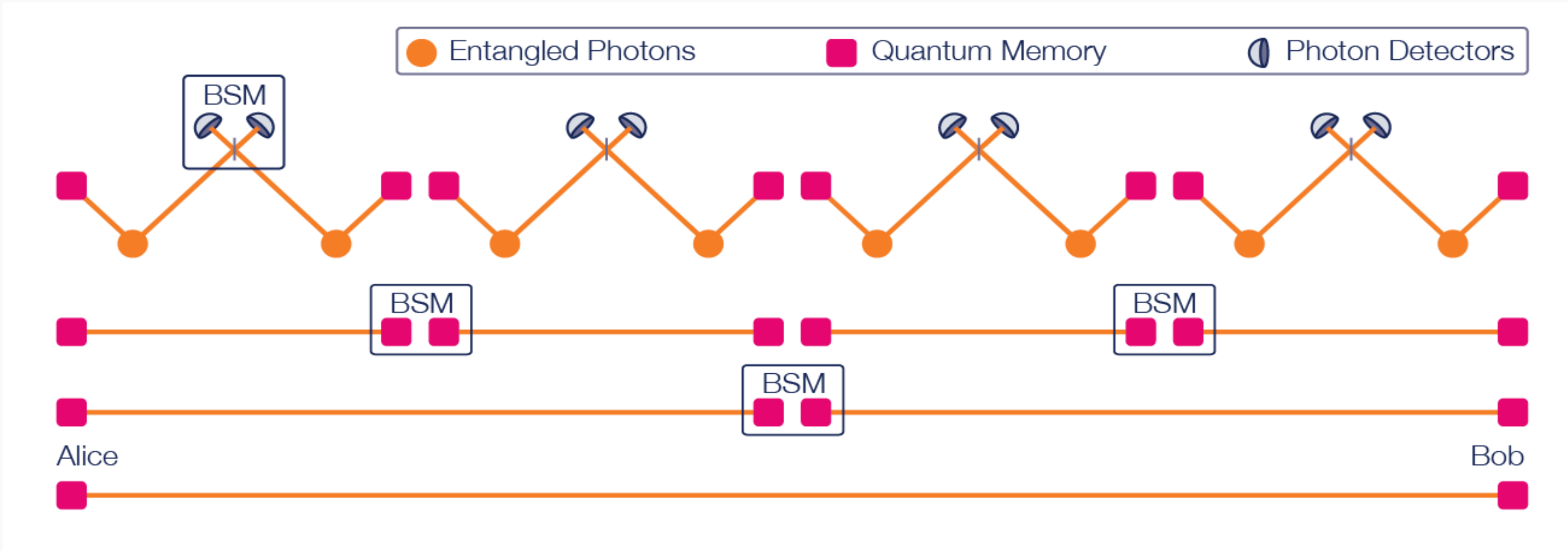
Aims at the **deployment**, by **2030**, of a pan-European **publicly controlled secure quantum communication infrastructure** linking selected EU strategic sites by using **both terrestrial and space links**.

Current signature of 24 countries (incl. France)

Large Industry Involvement – Important foreseen investment (1B€)

➔ Opportunities for Quantum Engineers and Researchers

Long-term vision for Q networks: Quantum Internet



Quantum Internet Alliance
Flagship Project