Lezione Crittografia

Type	Lesson

Crittografia con fotoni entangled

Riprendiamo la crittografia quantistica, e in particolare la distribuzione di chiavi, quasi sempre indicata con l'acronimo QKD (quantum key distribution). Dopo la proposta del protocollo BB84, basato su un solo fotone, vediamo ora la proposta di A. Ekert (1992), in cui si usa una coppia di fotoni entangled, nello stesso stato di Bell degli esperimenti di Clauser e Aspect.

Sorgente di fotoni entangled in stato di Bell

$$
\begin{aligned}
|\Psi^-\rangle &= \frac{1}{2\sqrt{2}}(|x\rangle + i\,|y\rangle) \otimes (-\,|x\rangle + i\,|y\rangle) - \frac{1}{2\sqrt{2}}\,(-\,|x\rangle + i\,|y\rangle) \otimes (|x\rangle + i\,|y\rangle) \\
&= \frac{i}{\sqrt{2}}\,(|x\rangle\,|y\rangle - |y\rangle\,|x\rangle) = \frac{i}{\sqrt{2}}\,(|H\rangle\,|V\rangle - |V\rangle\,|H\rangle) = \frac{i}{\sqrt{2}}\,(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle)
\end{aligned}
$$

Polarizzatore, operatore di proiezione:

$$
\begin{aligned}
\Pi_\theta &= |\theta\rangle\,\langle\theta| \\
|\theta\rangle &\equiv \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,|1\rangle \\
&= \cos(\theta/2)\,|x\rangle + \sin(\theta/2)\,|y\rangle
\end{aligned}
$$

Con i fotoni dello stato di Bell, Alice e Bob misurano trasmissione da polarizzatori ad angoli (α, β).

La probabilità di trasmissione congiunta è

$$
\begin{aligned}
P_{TT} =& |\,\langle\alpha,\beta|\,\Psi^-\rangle|^2 \\
=& \frac{1}{2}|\cos(\alpha/2)\sin(\beta/2) - \sin(\alpha/2)\cos(\beta/2)|^2 = \frac{1}{2}\sin^2(\alpha/2 - \beta/2)
\end{aligned}
$$

e analogamente

$$
\begin{aligned}
P_{RT} =& |\langle \alpha+\pi, \beta | \Psi^- \rangle|^2 = \frac{1}{2}\cos^2(\alpha/2 - \beta/2) \\
P_{TR} =& |\langle \alpha, \beta+\pi | \Psi^- \rangle|^2 = \frac{1}{2}\cos^2(\alpha/2 - \beta/2) \\
P_{RR} =& |\langle \alpha+\pi, \beta+\pi | \Psi^- \rangle|^2 = \frac{1}{2}\sin^2(\alpha/2 - \beta/2)
\end{aligned}
$$

Il coefficiente di correlazione, pari al valor medio del prodotto degli “spin”, ovvero degli osservabili valgono +1 per trasmissione e -1 per riflessione:

$$
\begin{aligned}
E(\alpha, \beta) =& (+1)(P_{TT} + P_{RR}) + (-1)(P_{RT} + P_{RT}) \\
=& \sin^2(\alpha/2 - \beta/2) - \cos^2(\alpha/2 - \beta/2) \\
=& -\cos(\alpha - \beta)
\end{aligned}
$$

Il protocollo prevede che Alice e Bob scelgano in maniera casuale l’angolo del polarizzatore tra 3 valori:

$$
\begin{aligned}
(\alpha_1, \alpha_2, \alpha_3) &= \left(0, \frac{\pi}{4}, \frac{\pi}{2}\right) \\
(\beta_1, \beta_2, \beta_3) &= \left(\frac{\pi}{4}, \frac{\pi}{2}, \frac{3}{4}\pi\right)
\end{aligned}
$$

Dopo aver eseguito N misure, Alice e Bob divulgano la direzione dei polarizzatori per tutte le misure, ma non il risultato delle singole misure, T o R, ovvero $(+1, -1)$.

1. Eliminano le occorrenze in cui uno dei due non ha rivelato fotone.
2. Usano il sottoinsieme di misure in cui hanno usato la stessa direzione, $\alpha_2 = \beta_1$ oppure $\alpha_3 = \beta_2$, per definire la chiave crittografica: in questi casi se Alice misura $(+1) = T$, Bob misura $(-1) = R$ e viceversa. Quindi Alice scrive 1 nella chiave per fotone trasmesso e Bob scrive 1 per fotone riflesso. Con questo sottoinsieme Alice e Bob hanno la stessa chiave, ma ciascuno l’ha derivata in proprio.
3. Usano il sottoinsieme complementare delle misure, quelle non utilizzate per la chiave, per verificare la sicurezza della trasmissione, ovvero un’eventuale intercettazione della spia Eve. Alice e Bob divulgano i risultati di queste misure, entrambi calcolano la combinazione lineare delle correlazioni

$$
\begin{aligned}
S =& E(\alpha_1, \beta_1) - E(\alpha_1, \beta_3) + E(\alpha_3, \beta_1) + E(\alpha_3, \beta_3) \\
=& -\cos(-\pi/4) + \cos(-3\pi/4) - \cos(\pi/4) - \cos(-\pi/4) \\
=& -2\sqrt{2}
\end{aligned}
$$

che vìola la disuguaglianza Clauser-Horne-Shimony-Holte (CHSH)

$$|S| > 2$$

$$S = -\cos(-\pi/4) + \cos(-3\pi/4) - \cos(\pi/4) - \cos(-\pi/4) = -2\sqrt{2}$$

In un'intercettazione Eve misura uno dei due fotoni, dopo aver scelto una sua base computazionale, ovvero una direzione del suo polarizzatore, e rinvia un nuovo fotone con la stessa polarizzazione di quello misurato. Eve deve eseguire quest'operazione in un numero sufficientemente alto di casi per estrarre informazione sulla chiave. Esattamente quante intercettazioni siano necessarie esula dai nostri scopi. Queste intercettazioni avvengono quindi anche nel sottoinsieme di misure di controllo che, di conseguenza, non vìola più la disuguaglianza CHSH. Quindi, se non è verificata la disuguaglianza, Alice e Bob rigettano la chiave generata.

Esperimento di Naik et al (2000)

Physical Review Letters 84, 4437 (2000)

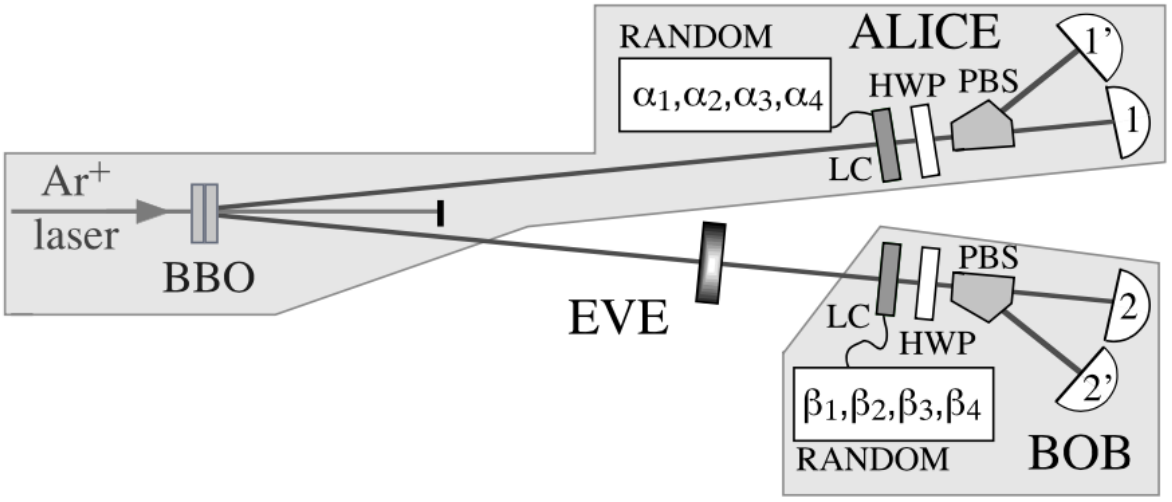

FIG. 1. Schematic of quantum cryptography system. 351.1 nm light from an Argon ion laser is used to pump two perpendicularly oriented nonlinear optical crystals (BBO). The resultant entangled photons are sent to Alice and Bob, who each analyze them in one of four randomly chosen bases. The eavesdropper, if present, was incorporated using either a polarizer or a decohering birefringent plate [both orientable, and in some cases with additional wave plates to allow analysis in arbitrary elliptical polarization bases (Fig. 2a and 2b)].

Coppia di fotoni emessi in PDC da laser “pompa” a 351 nm, nello stato di Bell

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle\,|H\rangle + |V\rangle\,|V\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle\right)$$

che non è lo stesso della proposta originale di Ekert. La sorgente è sempre la parametric down-conversion, in questo esperimento produce circa 5e9 coppie/s, di cui solo 1 su 10^6 viene rivelata come coincidenza. Le coincidenze vengono misurate da rivelatori con un efficienza quantistica di 0.6, a valle dei polarizzatori di analisi, con una temporale di 5 ns. Per ogni scelta della base di analisi, le coincidenze sono misurate su un periodo di 1 ms, in cui la probabilità di avere una coincidenza è prossima a 1, dato che il numero medio in questo intervallo è 5. Se occorrono più coincidenze, solo la prima viene conservata.

Anche l’analisi avviene con proiettori su una base diversa dalla proposta di Ekert. Alice usa i seguenti proiettori:

$$\{|\alpha\rangle\langle\alpha|, \mathbb{I} - |\alpha\rangle\langle\alpha|\}$$
$$|\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle)$$

scegliendo per l’angolo α i valori $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\pi/4,\, \pi/2,\, 3\pi/4,\, \pi)$. Si noti che nei primi 3 casi i casi, la base non corrisponde a due polarizzazioni lineari perpendicolari, come negli esperimenti di Clauser e Aspect. La proiezione lungo una base di polarizzazione non-lineare richiede l’uso di dispositivi ottici birifrangenti, ovvero una lamina a ritardo di fase (half-wave plate, HWP) e un dispositivo a cristalli liquidi (LCD)....

Bob usa i proiettori analoghi ad Alice, parametrizzati dall’angolo β, scegliendo i valori $\vec{\beta} = \vec{\alpha} - \pi/4$, di cui solo il primo corrisponde a polarizzazioni lineari.

Con queste basi, le probabilità congiunte sono:

$$\begin{aligned}
P_{TT} =& |\langle\alpha|\langle\beta|\Phi^+\rangle|^2 \\
=& \left|\frac{1}{2\sqrt{2}}[1 + e^{-i(\alpha+\beta)}]\right|^2 = \frac{1}{4}[1 + \cos(\alpha+\beta)] = P_{RR} \\
P_{TR} =& \frac{1}{4}[1 + \cos(\alpha+\pi+\beta)] = \frac{1}{4}[1 - \cos(\alpha+\beta)] = P_{RT}
\end{aligned}$$

Le scelte tra i 4 valori possibili vengono effettuate da Alice e Bob mediante due generatori di numeri casuali indipendenti, su computer distinti, che modificano i rispettivi LCD ogni 22 ms, in maniera sincrona. La velocità di commutazione dei LCD limita il rate di acquisizione a circa 40 Hz, una coincidenza acquisita ogni 25 ms.

Solo 1/4 delle coincidenze viene usata per la chiave, ovvero quando $\alpha + \beta = \pi$, per cui le rivelazioni di Alice e Bob sono completamente anti-correlate: $P_{TR} + P_{RT} = 1$. La metà delle coincidenze sono utilizzate per verificare le dis. di Bell su due distinti osservabili:

$$S = -E(\alpha_1, \beta_1) + E(\alpha_1, \beta_3) - E(\alpha_3, \beta_1) + E(\alpha_3, \beta_3)$$
$$S' = E(\alpha_2, \beta_2) + E(\alpha_2, \beta_4) - E(\alpha_4, \beta_2) - E(\alpha_4, \beta_4)$$

Per ogni teoria che obbedisce al realismo locale, $|S| < 2, |S'| < 2$.

TABLE I. Distribution of data dependent on Alice's and Bob's respective phase settings α_i and β_i (see text for details).

		Alice			
		α_1	α_2	α_3	α_4
Bob	β_1	S	$\cdots$	S	QKey
	β_2	$\cdots$	S'	QKey	S'
	β_3	S	QKey	S	$\cdots$
	β_4	QKey	S'	$\cdots$	S'

Nell'esperimento vengono verificate le dis. di Bell in 40 min, con $S = (-2.665 \pm 0.019)$ e S' $= (-2.644 \pm 0.019)$, deviazione pari a 34σ.

Viene anche osservato l'effetto di un disturbo sul canale di Bob, introducendo un polarizzatore prima dell'apparato di analisi

.

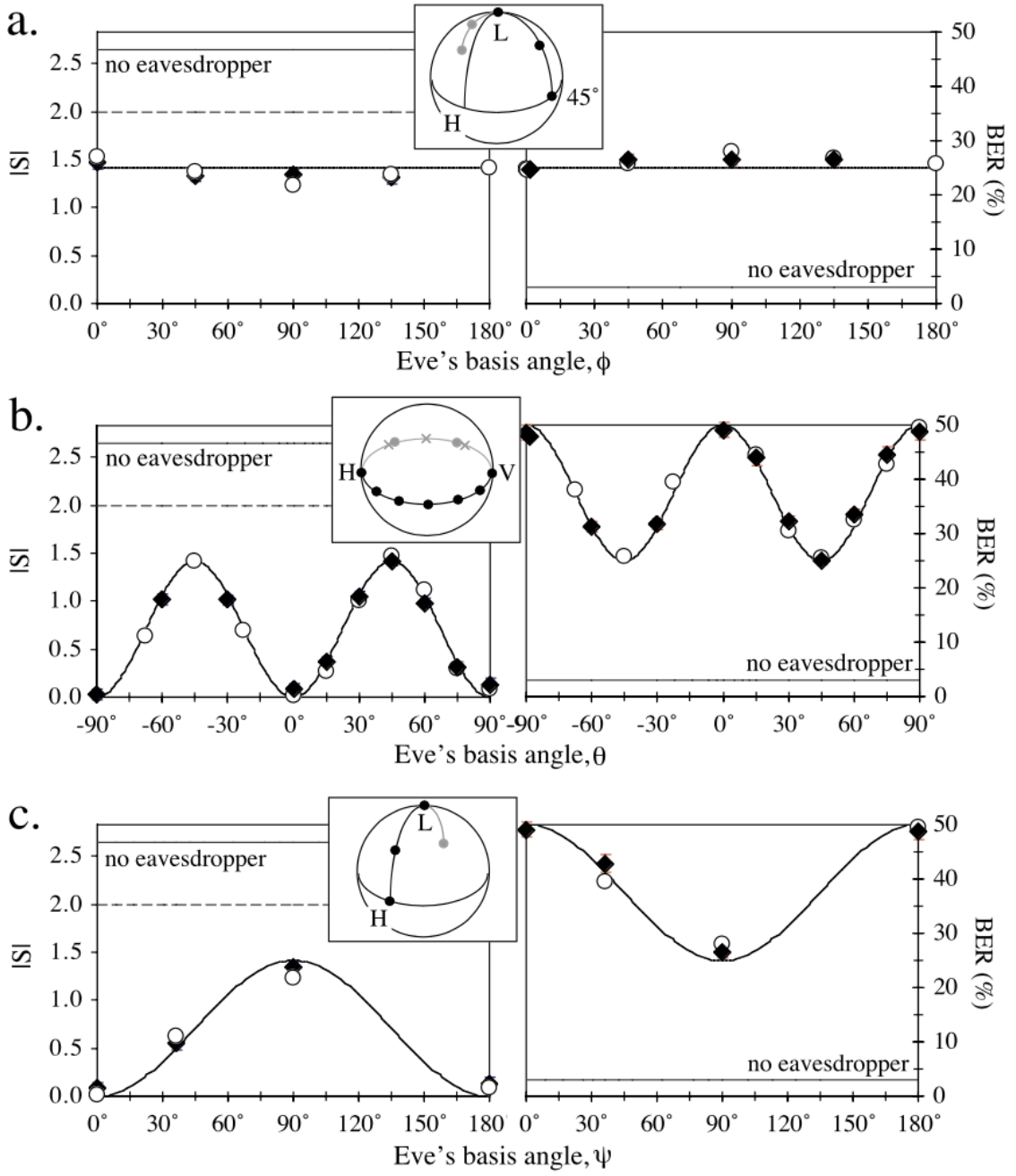

FIG. 2. Data and theory showing the effect of an eavesdropper on S and BER for various attack bases (as S' closely agrees with S, it is omitted for clarity). Diamonds represent strong measurements, made with a polarizer; circles represent QND attacks, simulated with a 3-mm-thick BBO crystal; error bars are within the points. The attack bases are (a) $|H\rangle + e^{i\phi}|V\rangle$; (b) $\cos\theta|H\rangle + \sin\theta|V\rangle$; and (c) $|45°\rangle + e^{i\psi}|-45°\rangle$; the actual measurement points in these bases are illustrated on the inset Poincaré spheres. The measured average values with no eavesdropper are indicated by unbroken grey lines, the broken lines represent the maximum classical value of $|S|$.

La presenza del disturbo, una delle possibili intercettazioni, viene rivelata sia dalle dis. CHSH, sia dall'aumento delle mancate coincidenze, bit error rate (BER).

Complessivamente in questo esperimento in 40 min è stata stabilita una chiave di 24252 bits, ad un rate di circa 10 bits/s.

QKD da satellite (2017)

Nature 549, 43 (2017)

La QKD in fibra è limitata da assorbimento nelle fibre a distanze di ~ 100 km. Nelle trasmissione classica in fibra, si usano stadi di amplificazione, ma questo non è possibile con le coppie entangled. La trasmissione in atmosfera è un'alternativa e la trasmissione verso satellite è un'opzione praticabile dato che la densità dell'atmosfera diminuisce con la quota. In effetti l'atmosfera corrisponde a una altezza effettiva di 10 km.

La trasmissione avviene da satellite a terra, così la deviazione di fotoni dovuta alle turbolenze atmosferiche avviene in maniera predominante nella parte terminale del canale. Nell'esperimento cinese il "beam wandering" è dell'ordine della dimensione del fascio a terra, pari a circa 12 m: a causa della diffrazione è impossibile avere un fascio con divergenza identicamente nulla. Nell'esperimento cinese, il satellite produce un fascio con divergenza di $10\ \mu\mathrm{rad}$, che determina un diametro di 12 m a 1200 km di distanza. Il puntamento avviene con una precisione $1.2\mu\mathrm{rad}$ utilizzando laser ausiliari, che vengono utilizzati anche per la sincronizzazione necessaria per assegnare i fotoni in trasmissione e ricezione.

Temporalmente, le coincidenze vengono selezionate, conservando solo quelle che arrivano in una finestra di 2 ns, per ridurre il livello di rumore.

Perdite: diffrazione 22 dB (6e-3), turbolenza atmosferica 5dB (0.3), efficienza telescopio/fibre 0.16, rivelatori 0.5.

Il protocollo utilizzato è BB84, con "decoy state", strategia per utilizzare non singoli fotoni ma stati con molti fotoni attenuati, in cui il valor medio è ~ 1 fotone. Attualmente non ci sono sorgenti di singoli fotoni "on demand" con alto rate di emissione. Nell'esperimento cinese venivano emessi impulsi attenuati con rate 100 MHz, ma il rate della chiave filtrata è ~ 10 kbit/s.

Le perdite principalmente avvengono per diffrazione (x 6e-3), turbolenza atmosferica (x 0.3), efficienza di raccolta e rivelazione (x 0.08).

Al passaggio del satellite sopra la stazione ricevente, la trasmissione avviene per circa 300s con un rate variabile.

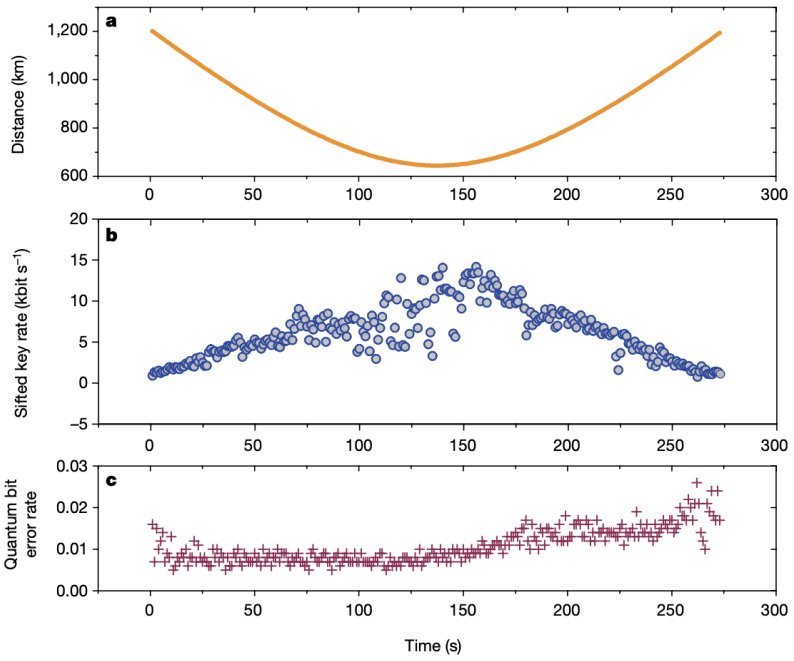

Figure 3 | Performance of satellite-to-ground QKD during one orbit. a, The trajectory of the Micius satellite measured from Xinglong ground station. **b**, The sifted key rate as a function of time and physical distance from the satellite to the station. **c**, Observed quantum bit error rate. See text for detailed discussion of the results, and Extended Data Table 2 and Extended Data Fig. 1 for additional data on different days.

Esteso a comunicazione intercontinentale

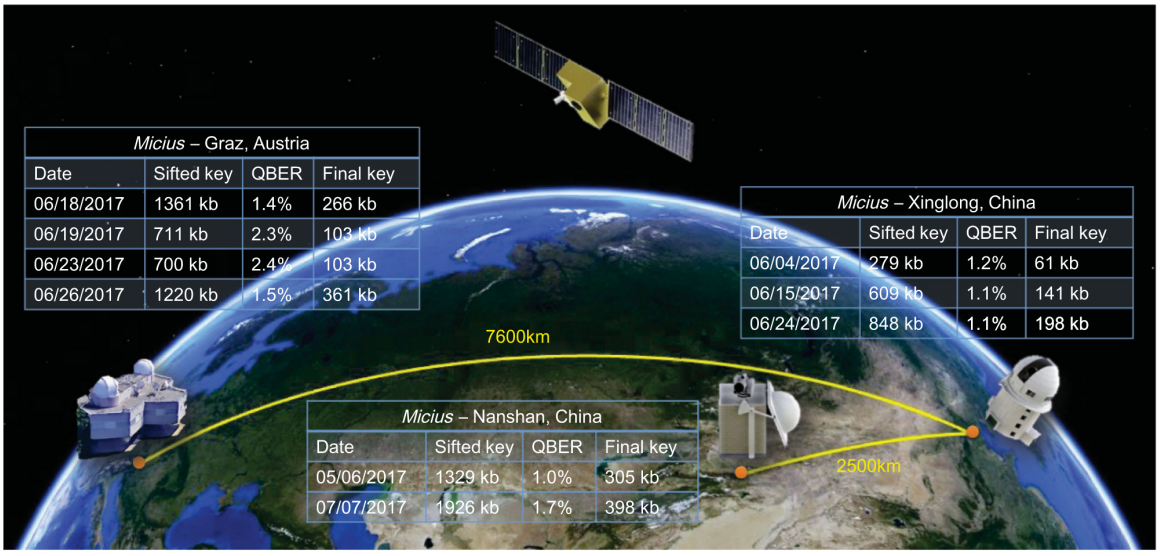

FIG. 1. Illustration of the three cooperating ground stations (Graz, Nanshan, and Xinglong). Listed are all paths used for key generation and the corresponding final key length.

Il satellite trasmette due chiavi, ad es. MX (Micius Xinglong) e MG (Micius-Graz), che non sono le stesse. A bordo del satellite ci sono entrambe le chiavi. Per permettere a G di ricostruire la chiave MX (e viceversa), il satellite calcola e trasmette PUB = MG $\oplus$ MX, ovvero l'XOR delle 2 chiavi. Se l'i-simo bit PUB(i) = 0, MG(i) = MX(i); al contrario se PUB(i)=1, i bit corrispondenti delle due chiavi sono opposti. Equivalentemente, MX = MG $\oplus$ PUB, quindi G ricostruisce MX calcolando XOR tra la propria chiave e la chiave PUB. Analogamente X ottiene MG.

Riferimenti

A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. 67, 661 (1991)

D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, *Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol,* Phys. Rev. Lett. 84, 4437 (2000)

S.-K. Liao et al., *Satellite-to-Ground Quantum Key Distribution*, Nature **549**, 43 (2017)