

CRITTOGRAFIA CON FOTONI ENTANGLED

Quantum key distribution QKD

Protocollo BB84

Protocollo E91 , A. Ekert 1991

Alice e Bob ricevono fotoni entangled

$$\begin{aligned} |\Psi^-\rangle &= \frac{i}{\sqrt{2}} (|H\rangle_1 |V\rangle_2 - |V\rangle_1 |H\rangle_2) \\ &= \frac{i}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2) \end{aligned}$$

Alice rivela fotone 1 con polarizzatore ad angolo α

Bob " " 2 " " β

Probabilità di trasmissione da entrambi i polarizzatori

$$\begin{aligned} P_{TT}(\alpha, \beta) &= |\langle \alpha | \otimes \langle \beta | \Psi^- \rangle|^2 \\ &= \langle \Psi^+ | \Pi_\alpha \Pi_\beta | \Psi^- \rangle \end{aligned}$$

$$\Pi_\alpha = |\alpha\rangle \langle \alpha|$$

$$|\alpha\rangle = \cos \frac{\alpha}{2} |0\rangle + \sin \frac{\alpha}{2} |1\rangle$$

$$\begin{aligned} P_{TT}(\alpha, \beta) &= \frac{1}{2} \left| \cos\left(\frac{\alpha}{2}\right) \sin\left(\frac{\beta}{2}\right) - \sin\left(\frac{\alpha}{2}\right) \cos\left(\frac{\beta}{2}\right) \right|^2 \\ &= \frac{1}{2} \sin^2\left(\frac{\alpha}{2} - \frac{\beta}{2}\right) = P_{RR} \end{aligned}$$

$$P_{TR}(\alpha, \beta) = P_{RT}(\alpha_1, \beta) = \frac{1}{2} \cos^2\left(\frac{\alpha}{2} - \frac{\beta}{2}\right)$$

Alice scatta casuale di α su tre valori diversi

$$(\alpha_1, \alpha_2, \alpha_3) = \left(0, \frac{\pi}{4}, \frac{\pi}{2}\right)$$

Bob scatta casuale

$$(\beta_1, \beta_2, \beta_3) = \left(\frac{\pi}{4}, \frac{\pi}{2}, \frac{3}{4}\pi\right)$$

- Ricevono N coppie
- Alice / Bob scrive 1 per T, 0 per R
- Divulgano pubblicamente la direzione di analisi

Il sottoinsieme in cui $\alpha = \beta$ viene usato per generare la chiave

- Il sottoinsieme complementare viene usato per verificare la sicurezza

$$\begin{aligned} E(\alpha, \beta) &= (+1) [P_{TT}(\alpha, \beta) + P_{RR}(\alpha, \beta)] + \\ &\quad (-1) [P_{TR}(\alpha, \beta) + P_{RT}(\alpha, \beta)] \\ &= -\cos(\alpha - \beta) \end{aligned}$$

divulgano risultati delle misure e calcolano $E(\alpha, \beta)$

$$S = E(\alpha_1, \beta_1) - E(\alpha_1, \beta_3) + E(\alpha_3, \beta_1) + E(\alpha_3, \beta_3)$$

Distinguaglianza CHSH $|S| \leq 2$ teoria realistica locale

$$\text{QM} \quad S = -2\sqrt{2}$$

- Se non è violata dis. CHSH , Alice e Bob scambiano le chiavi

ESPERIMENTO DI NAIK et al. (2000)

Generazione di 2 fotoni entangled per parametric down-conversion da $\lambda = 351 \text{ nm}$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}} (|H\rangle|H\rangle + |V\rangle|V\rangle) =$$

$$= \frac{1}{\sqrt{2}} (|0\rangle|0\rangle + |1\rangle|1\rangle)$$

Differenza 1
da E91

Produzione 5e9 coppie/s
Coincidenze 5e3 /s

Differenza da E91 # 2:

- base analisi $\Pi_\alpha = |\alpha\rangle\langle\alpha|$

$|\alpha\rangle$ non è uno stato di polarizzazione lineare

$$= \frac{|0\rangle + e^{i\alpha}|1\rangle}{\sqrt{2}}$$

- Probabilità di trasmissione / riflessione

$$P_{TT} = |\langle\alpha| \otimes \langle\beta| \Psi^+ \rangle|^2 = \left| \frac{1}{2\sqrt{2}} (1 + e^{-i(\alpha+\beta)}) \right|^2$$

$$= \frac{1}{4} (1 + \cos(\alpha + \beta)) = P_{RR}$$

$$P_{TR} = P_{RT} = \frac{1}{4} (1 - \cos(\alpha + \beta))$$

Scelta casuale di Alice

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \left(\frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, \pi \right)$$

Scelta casuale di Bob

$$\vec{\beta} = \vec{\alpha} - \frac{T}{q}$$

Scelta casuale mediante dispositivi a cristalli liquidi
ogni 22 ms

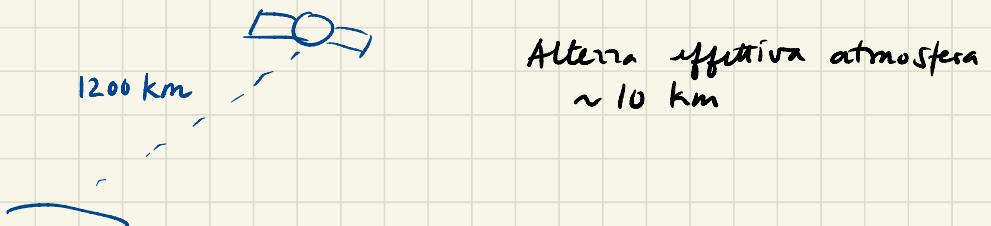
Misure di coincidenza rate di 40 Hz

QKD rate ~ 10 bits/s

Violate le dis. CHSH di 34 σ

QKD da Satellite (2017)

Nature 549, 43 (2017)



Protocollo BB84 da satellite a terra

Viene inviato fascio con divergenza $10 \mu\text{rad}$, dopo 1200 km
 $\text{dia} = 12 \text{ m}$

Raccolta telescopio $\text{dia} = 1 \text{ m}$, perdita $6 \cdot 10^{-3}$

Perdita turbolenza aria ~ 0.3

Efficienza ricezione, ~ 0.08

Emissione 100 MHz impulsi

Rate chiave filtrata $\sim 10 \text{ kbit/s}$

Chiavi MG (satellite Miiss - Graz)

MX (satellite " - China)

Satellite Miiss pubblica $P = MG \oplus MX$, XOR delle chiavi

Graz ottiene MX da $P \oplus MG = MX$ e viceversa.