

# QKD

---

quantum key  
distribution

9/12/2021

or 16:15

---

---

---

---



GRUPPO 0: ore 11  
11 1: ore 8:30  
11 2: ore 15

# MECCANICA QUANTISTICA

## SOVRAPPOSIZIONE

proprietà di un sistema quantistico di trovarsi in diversi stati contemporaneamente

## DECOERENZA

la misurazione di un sistema quantistico disturba il sistema:  
il sistema disturbato perde la sovrapposizione degli stati e  
collapsa in uno stato singolo

## NO-CLONING

Impossibilità di duplicare un sistema contenendo nella copia  
lo stato quantistico dell'originale (senza misurarlo)  
è impossibile copiare uno stato quantistico non noto

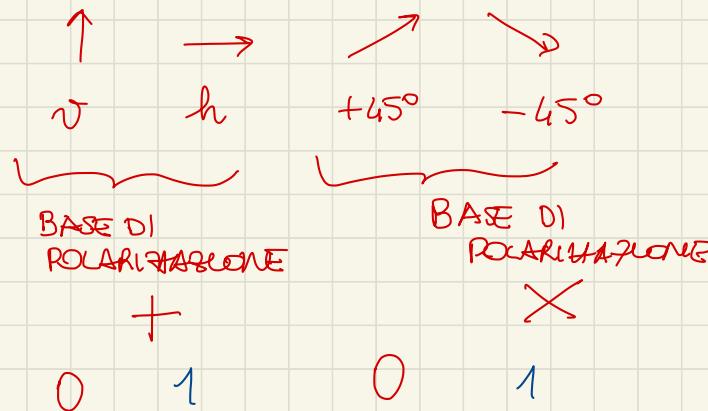
## ENTANGLEMENT

possibilità che due o più elementi si trovino in stati quantici  
correlati tra loro in modo che, pur se portati a grande distanza,  
mantengono la correlazione

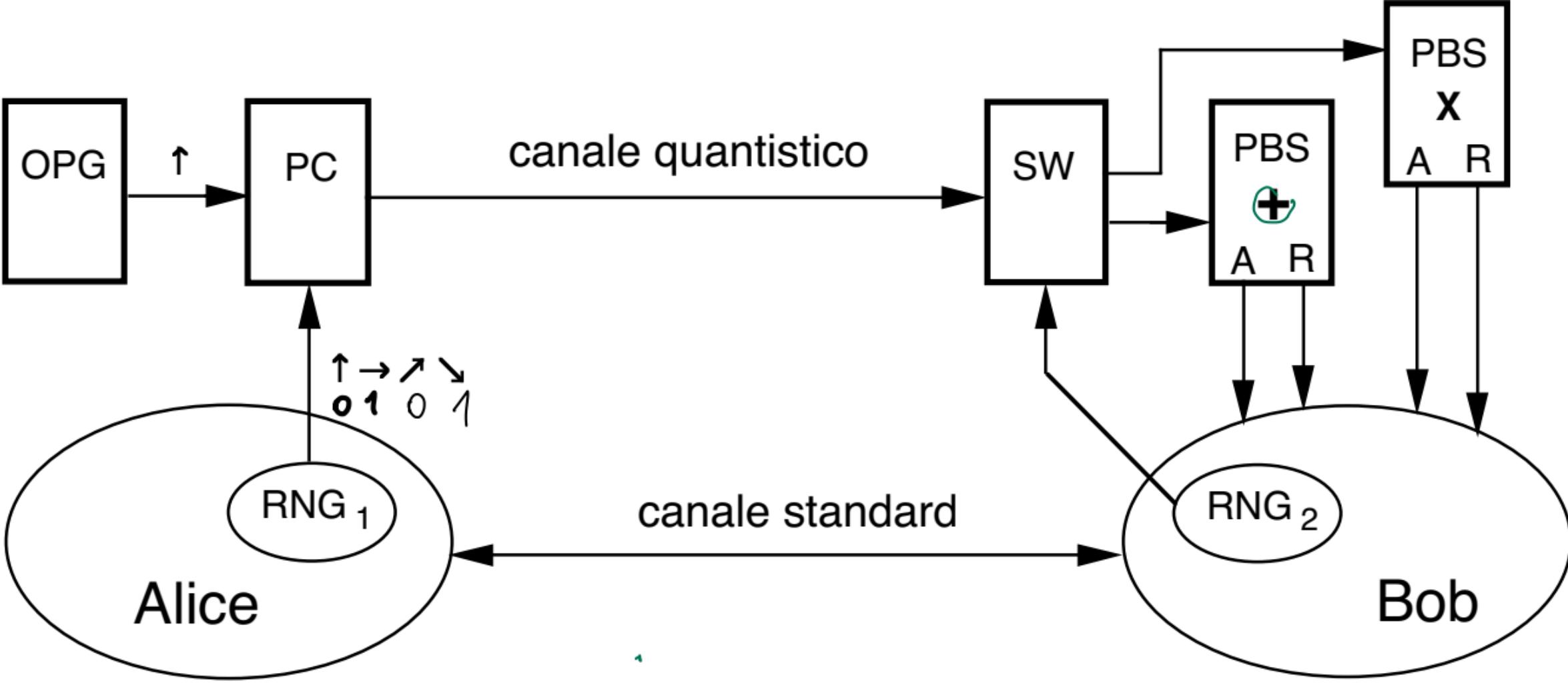
**PROTO CALLO BB84** (Bennet, Brassard)  
USA CA

scommesso di chiavare mediante invio di FOTONI POLARIZZATI

4 stati di POLARIZZAZIONE:



Non è possibile distinguere  
tra i 4 casi,  
l'unica misura possibile è  
che ha 2 stati ortogonali  
nella stessa base



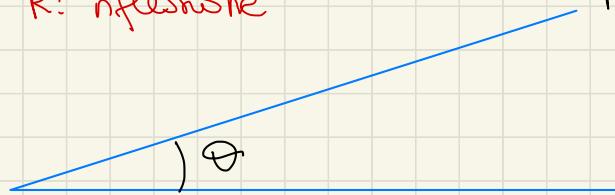
PBS: beam splitter polarizzante. Denzi il fotone verso uno  
tra le due uscite A e R.



A: assorbimento

R: riflessione

F: polarizzazione del fotone



S: asse di polarizzazione del PBS

A: il fotone viene inviato all'uscita A con probabilità  $\cos^2 \theta$   
e assume polarizzazione  $S$

R: il fotone viene inviato all'uscita R con probabilità  $\sin^2 \theta$   
e assume polarizzazione perpendicolare a  $S$  ( $S^+$ )

$$\theta = 0$$

$$(F = S)$$

il fotone esce da A, con probabilità 1,  
e con polarizzazione  $S (= F)$

$$\theta = 90^\circ$$

$$(F \perp S)$$

il fotone esce da R, con probabilità 1,  
e con polarizzazione  $S^+ (= F)$

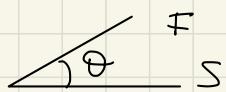
$$\theta = \pm 45^\circ$$

$$\cos^2 \theta = \sin^2 \theta = 1/2$$

$\Rightarrow$  il fotone esce con pari probabilità  $1/2$   
da A o da R, e la polarizzazione cambia  
(S o  $S^+$ )

Fenomeno quantistico

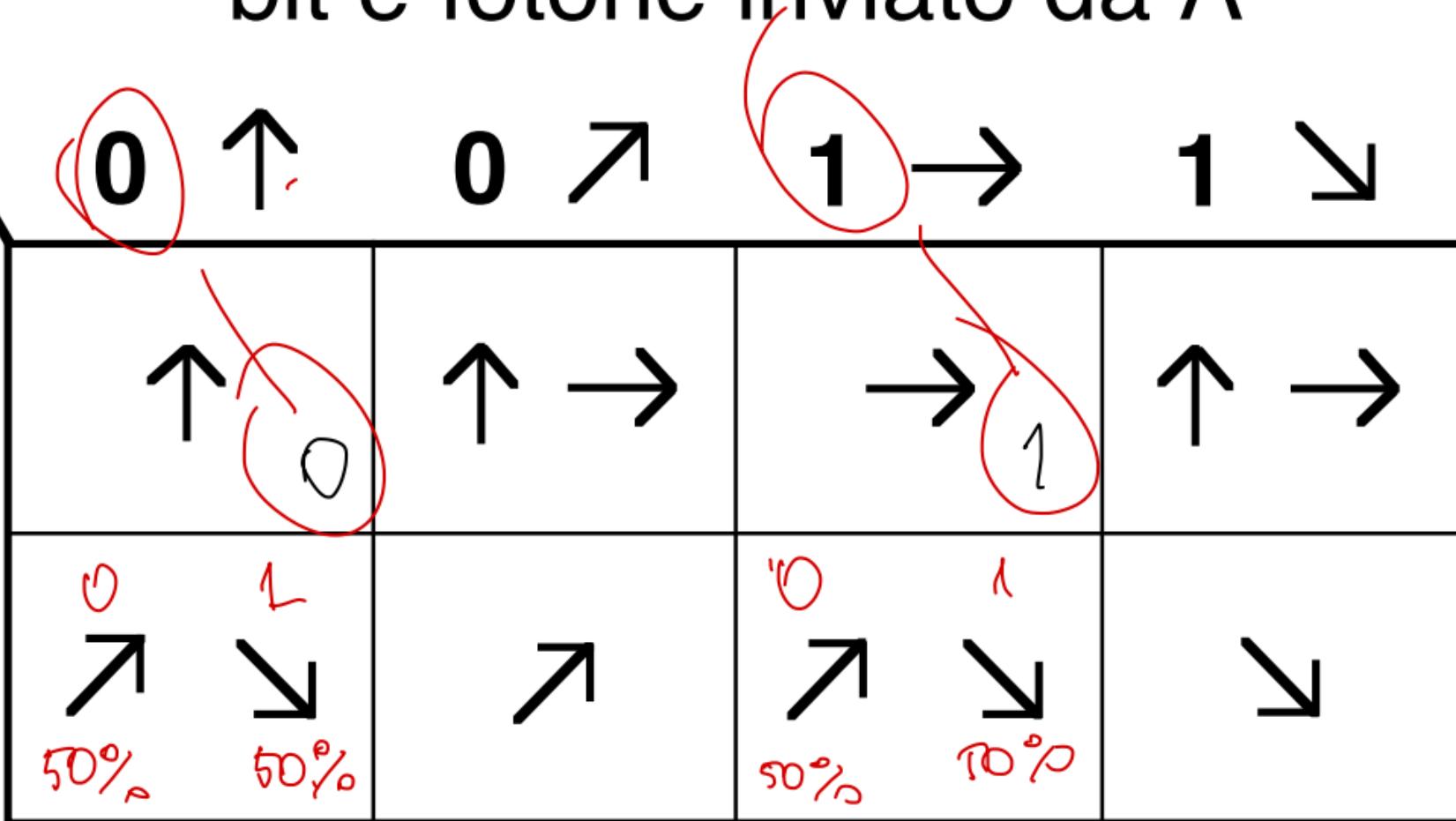
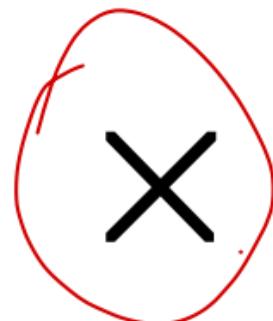
la lettura attraverso il PBS ha disruptto lo stato quantistico precedente



la polarizzazione  
del fotone è  
CONSERVATA

bit e fotone inviato da A

## basi di B



# Protocollo BB84

## CANALE QUANTISTICO

$S_A [1, n]$  → sequenza iniziale di bit da dei segnali estratti  
da chiavi (rappresentata con un codice a correzione  
di errori)

for  $i = 1$  to  $n$

- Alice: sceglie una base a caso, codifica  $S_A [i]$  e invia il fotone a Bob

→ Eve (se presente): intercetta il fotone, lo misura con una  
sua base, lo invia a Bob,  
costruisce  $S_E [i]$  (non necessariamente  
per ogni  $i$ )

- Bob: sceglie una base a caso, interpreta il fotone  
ricevuto, costruisce  $S_B [i]$

## CANALE STANDARD

QBER: % di errori dovuti al rumore

$h$ : funzione hash crittografica

- Bob: comunica ad Alice la sequenza di basi scelte
- Alice: comunica a Bob le basi comuni
- Alice e Bob:
  - 1) estraggono  $S_A'$  e  $S_B'$  corrispondenti alle basi comuni; quindici estraggono due sottosequenze di  $S_A'$  e  $S_B'$  in posizioni concordate:  $S_A''$  e  $S_B''$
  - 2) si scombinano  $S_A''$  e  $S_B''$   
se le % di bit diversi è maggiore del QBER  $\Rightarrow \star STOP \star$
  - 3) altrimenti calcolano  $S_A' \setminus S_A''$  e  $S_B' \setminus S_B''$ , le decodificano con un codice a correzione di errori e ottengono una sequenza comune  $S_C$
  - 4) Calcolano  $k = h(S_C)$  e lo usano come chiave

S<sub>A</sub>: 1 0 1 1 1 0 0 ...

bit di Alice

basi : + X + X X + X ...

basi di Alice

→ ↗ → ↘ ↙ ↗ ..

fotoni di Alice

+ + + X + X + ...

basi di Eve

→ → → ↘ ↑ ↗ → - - .  
S<sub>E</sub> 1 1 1 1 0 1 1 - - .

lettura di Eve  
bit di Eve

+ X + + + X X - -  
→ ↗ → → ↑ ↘ ↑  
1 1 1 1 0 1 0 - -

basi di Bob  
lettura di Bob  
bit di Bob

} con Eve

basi : + X + + + X X - -

basi di Bob

→ ↗ → ↑ → ↗ ↘  
S<sub>B</sub> 1 0 1 0 1 1 0

fotoni di Bob  
bit di Bob

Algorithmus di Grover

für eine Sequenz (DB non shuffled)  
ansey non ordered)

$$\mathcal{O}(n)$$

Maze. Q:

$$\mathcal{O}(\sqrt{n})$$

$$\sqrt{2^n} = 2^{n/2}$$

$$\mathcal{O}(2^n)$$

$$\xrightarrow{\quad} \mathcal{O}(2^{n/2})$$