

QKD

Quantum Distribution key

lezione di lunedì 7/12

Ore 11:15



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

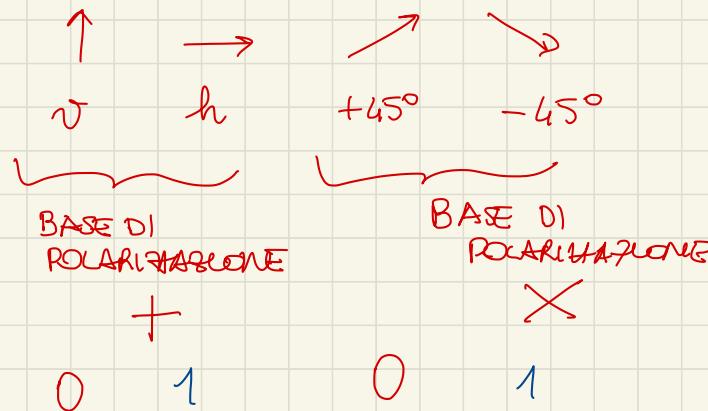
ENTANGLEMENT

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

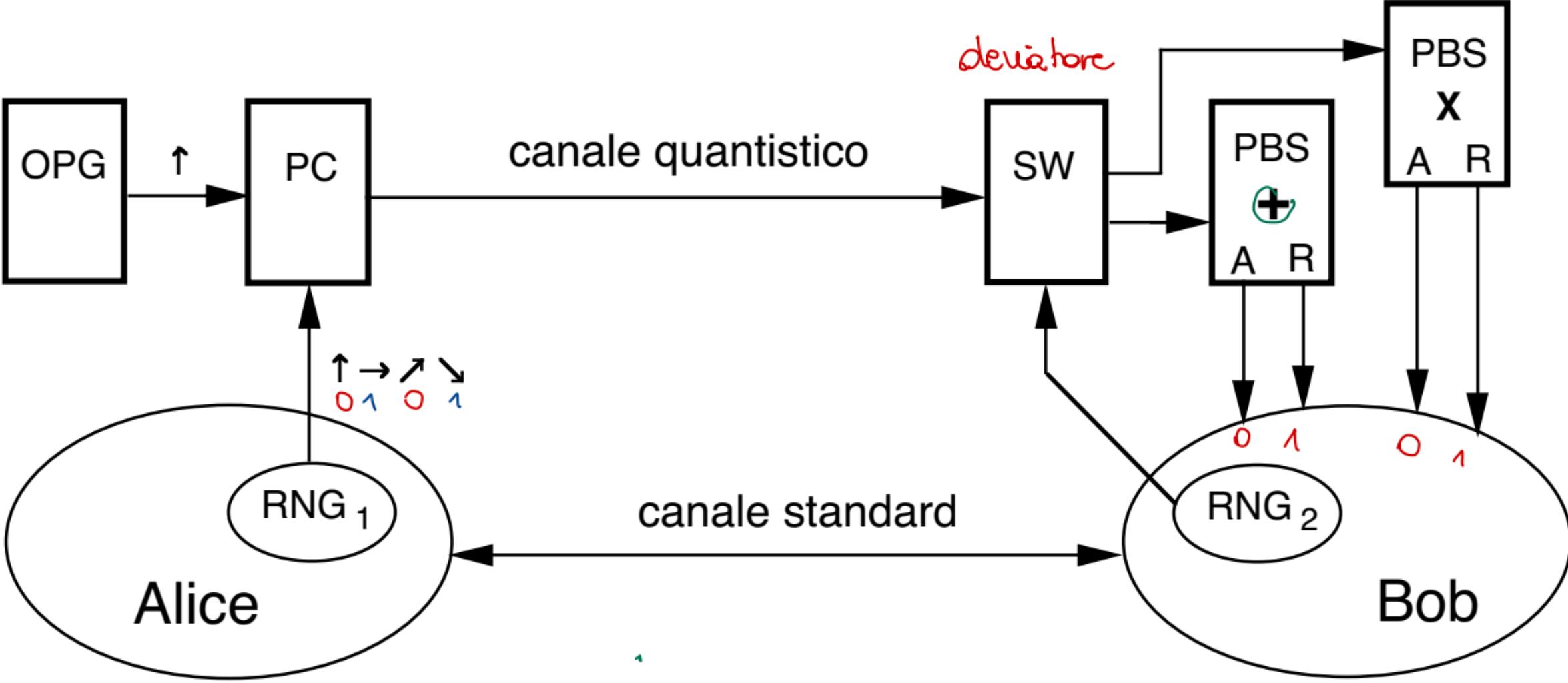
PROTO CALLO BB84 (Bennet, Brassard)
USA CA

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

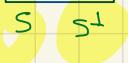


PBS: beam splitter polarizzante. Denzi il fascio verso uno tra le due uscite A e R.



A: assorbimento

R: riflessione



F: polarizzazione del fascio



S: asse di polarizzazione dell'PBS

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

R: il fascio viene inviato a R con probabilità $\sin^2\theta$, e esce con polarizzazione \perp a S

$\theta = 0^\circ$ ($F = S$)

il fascio esce da A, con polarizzazione S (= F)
(la consente)

$\theta = 90^\circ$ ($F \perp S$)

il fascio esce da R, con polarizzazione S^\perp (= F)

$\theta = \pm 45^\circ$

$$\cos^2\theta = \sin^2\theta = \frac{1}{2}$$

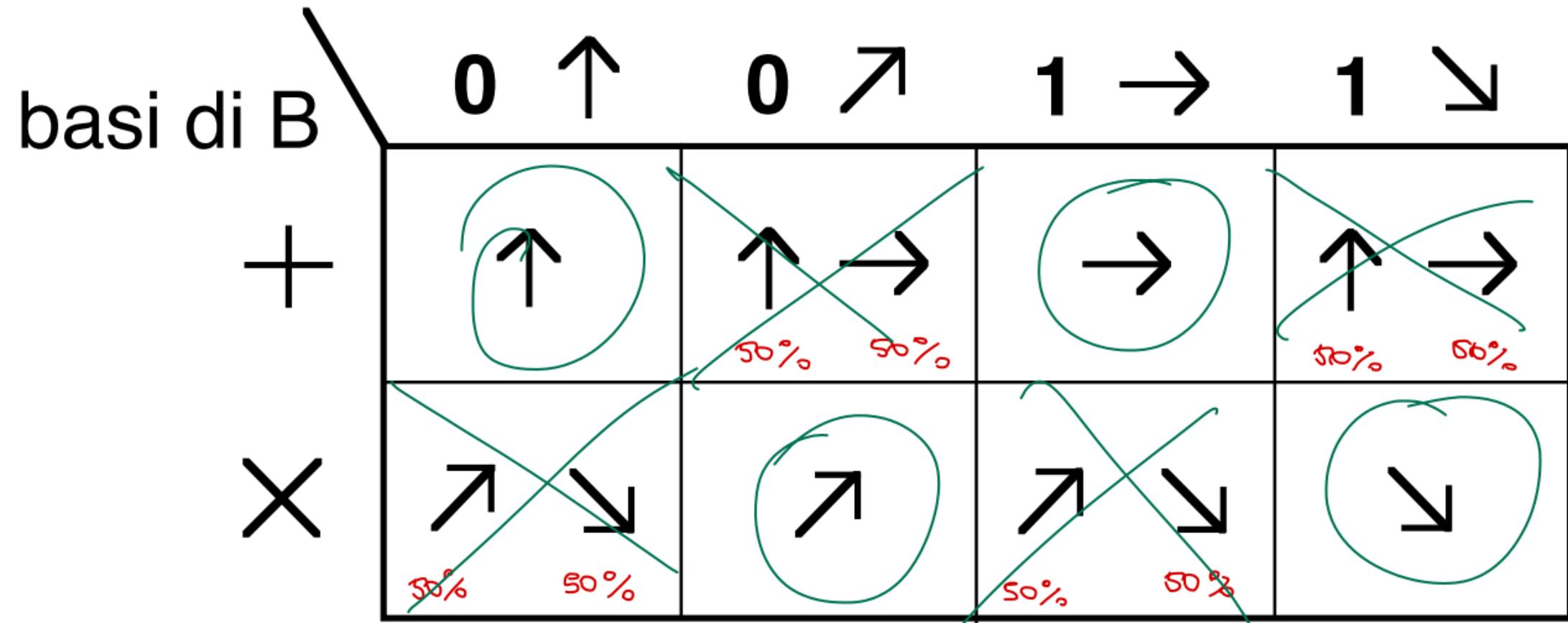
\Rightarrow il fascio esce con pari probabilità da A o R, e la sua polarizzazione combina (S, S^\perp)

} la polarizzazione
del fascio è
conservata

Fenomeno
quantistico

la lettura attraverso il PBS ha distrutto lo
stato quantistico precedente

bit e fotone inviato da A



PROTOCOLLO BB84

- 1) Alice: invia una sequenza S_A sul canale quantistico (S_A è sequenza di bit, codificati nelle polarizzazioni dei fotoni)
 - 2) Bob: interpreta S_A con le basi che ha scelto casualmente e ottiene S_B
(dove le basi coincidono, se ~~le~~ misure sono coincidenti)
 - 3) Bob: sul canale standard comunica ad Alice le basi scelte e Alice indica ~~che~~ quali sono convenuti alle tre
- in assenza di interferenze di Eve, Alice e Bob possono dare una stessa sequenza $S_A' = S_B'$ identica, ~~e~~ formata dai bit codificati e decodificati con basi comuni

$$|S_A'| = |S_B'| \simeq \frac{|S_A|}{2}$$

ESEMPIO

A 1 0 1 1 1 0 0 - - -

A + X + X X + X - - -

→ → → → ↑ ↑ - - -

+ + + X + X + - - -

→ → ↓ ↑ → - - -

1 1 1 1 0 0 1 - - -

S_A

basi di A

fonni di A

} A

basi di E

lettere di E

S_E

} E

B + X + + + X X - - -

→ → ↑ → → → - - -

1 0 1 0 1 1 0 - - -

→ → ↑ → → → - - -

1 1 1 0 0 0 1 - - -

→ → ↑ → → → - - -

1 1 1 0 0 0 1 - - -

→ → ↑ → → → - - -

1 1 1 0 0 0 1 - - -

basi di B

lettere di B

} B

S_B

senza Eve

con Eve

$$S_A^{-1} = S_B^{-1} = 1010$$

4) Alice e Bob

sacrificano una porzione S_A'' , S_B'' di S_A' e S_B' , in
possessi ni probabilità, concordando sul canale standard
(si passano al canali bit di S_A' e S_B')

Se $S_A'' \neq S_B'' \Rightarrow$ A e B indipendente
comunicazione (\rightarrow informazioni, molte fonti diversi)

Altri versi i usano

$$S_A' \setminus S_A'' = S_B' \setminus S_B'' \quad \text{come, chiede}$$

Alice e Bob \rightarrow

Quantum Bit Error Rate QBER
% probabile di bit errati (per errori dell'operatore sperimentale)

Nel confronto ha S_A'' e S_B'' , se lo $\%$ di errori è $>$ QBER \Rightarrow infusione di Eve chiede scatola

$r_E \leq QBER \Rightarrow$ sono un codice a ~~corretto~~
correzione di errori ~~er~~ per
ricostruire una chiede corretto

Protocollo BB84 (soggetto a interferenza)

CANALE QUANTISTICO

$S_A [1, n]$ → sequenza iniziale di bit da cui verrà estratto
la chiave (rappresentata con un codice a corrispondenze
di emoji)

for $i = 1$ to n

Alice: sceglie una base a caso, codifica $S_A (i)$,
invia il fotone a Bob

Eve (se presente): intercetta il fotone, lo misura con
una sua base, lo invia a Bob
e codice $S_E (i)$
(onde solo per qualche valore di 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 antidegradante

Bob: comunica ad Alice le sequenze di bit scritte

Alice: comunica a Bob le loro comuni

Alice e Bob:

- 1) estraggono S_A' e S_B' corrispondenti alle loro comuni e estraggono due sottosequenze di S_A' e S_B' , in posizioni corrette $\rightarrow S_A''$, S_B''
- 2) Si scambiano S_A'' e S_B'' . Se le % di bit \neq
 $\bar{e} > QBER \Rightarrow * STOP *$
- 3) ELSE:
Calcolano $S_A' \setminus S_A''$ e $S_B' \setminus S_B''$,
le decodificano con il codice a correzione di

erori \Rightarrow ottengono una sequenza come S_c

(Attenzione: Eve potrebbe conoscere due o più di S_c)

1) Alice e Bob col coloro

$$k = h(S_c)$$

e usano k come chiave.