Protocollo BB84

Bennet e Brassard, protocollo quantistico per lo scambio di chiavi. La sequenza di bit viene inviata su un canale quantistico insicuro, sfruttando la proprietà di decoerenza per stabilire se la comunicazione è stata intercettata (ed eventualmente scartare la chiave).

Fisica

Proprietà di sistemi quantistici:

sovrapposizione possibilità di trovarsi in diversi stati contemporaneamente;

decoerenza la misurazione del sistema lo disturba, facendolo collassare in uno stato singolo;

no-cloning impossibilità di duplicare un sistema senza misurarlo (e perdere la sovrapposizione);

entanglement possibilità di avere stati quantici correlati tra due particelle, e questa correlazione è mantenuta a grandi distanze.

Polarizzazione di fotoni:

- base ortogonale: verticale o orizzontale;
- base diagonale: $\pm 45°$;
- non si può distinguere tra le 4 polarizzazioni con una misura;
- conoscendo la base si può determinare la polarizzazione tra le 2 possibili;
- codifichiamo 0 con $\uparrow$ e $\nearrow$, 1 con $\rightarrow$ e $\searrow$.

Misurazione della polarizzazione con PBS (polarizing beam splitter):

- F polarizzazione del fotone, S asse di plarizzazione del PBS, θ angolo tra F e S;
- due uscite, A e R;
- il fotone viene inviato all'uscita A con polarizzazione S (misurare disturba la polarizzazione) con probabilità $\cos^2\theta$;
- all'uscita R con polarizzazione $S^\perp$ con probabilità $\sin^2\theta$.

Quindi:

- se $F = S$ allora esce sempre da A, se $F \perp S$ esce da B, e in entrambi casi la nuova polarizzazione è uguale a quella originale;
- se $\theta = \pm 45°$ allora $\cos^2\theta = \sin^2\theta = \frac{1}{2}$, il fotone esce con pari probabilità da A o R e perde la sua polarizzazione (diventa S o $S^\perp$ – la lettura ha distrutto lo stato quantistico precedente).

	$\uparrow$	$\nearrow$	$\rightarrow$	$\searrow$
$+$	$\uparrow$	$\uparrow \rightarrow$	$\rightarrow$	$\uparrow \rightarrow$
$\times$	$\nearrow \searrow$	$\nearrow$	$\nearrow \searrow$	$\searrow$

Le colonne indicano la polarizzazione del fotone inviato, le righe la base di misura, le celle i possibili risultati della misurazione.

Protocollo

Alice genera una sequenza iniziale di bit S_A (rappresentata con un codice a correzione di errori) da cui sarà estratta la chiave.

Sul canale quantistico:

- Alice sceglie una base a caso, codifica $S_A[i]$ con quella base e invia il fotone a Bob;
- Bob sceglie una base a caso, interpreta il fotone ricevuto e lo inserisce in $S_B[i]$ (se le basi non coincidono è un bit casuale).

Sul canale standard (anche in chiaro, ma autenticata):

- Bob comunica ad Alice la sequenza di basi scelte;
- Alice comunica a Bob le basi comuni;
- determinano le sottosequenze S'_A e S'_B corrispondenti alle basi comuni (lunghe in media la metà di S_A), da cui estraggono secondo una regola concordata le sottosequenze S''_A e S''_B
- si scambiano S''_A e S''_B e determinano la percentuale di bit diversi: se sono più del QBER (quantum bit error rate, rumore introdotto dalle apparecchiature) prestabilito allora c'è stato un intervento di Eve e le sequenze vengono scartate;
- altrimenti eliminano S''_A e S''_B dalle sequenze, decodificano con il codice a correzione di errori e ottengono una sequenza comune S;
- calcolano la chiave $k = h(S_C)$.

Eve può:

- intercettare e rispedire il fotone, ma per il principio no-cloning deve misurare il fotone, e se misura nella base sbagliata (deve sceglierla a caso perché al momento della trasmissione solo A la conosce) altera la sua polarizzazione;
- intercettare pochi bit in modo da non lasciare tracce significative, ma visto che la chiave è il risultato del calcolo di una funzione hash questo non aiuta;
- intercettare S''_A e S''_B, che però non vengono usate per generare la chiave;
- intercettare le basi, ma non sa comunque la polarizzazione del fotone spedito.