CRITTOGRAFIA QUANTISTICA

di Davide D'Arenzo e Riccardo Minciarelli

INTRODUZIONE

- Le leggi delle particelle elementari sconvolgono la fisica classica. L'osservazione altera lo stato delle particelle elementari.
- Sulla base della nuova fisica è stato possibile costruire sistemi di crittografia in linea di principio completamente sicuri.
- La necessità di una comunicazione sicura è sempre più rilevante.
- Con l'avvento dei "*Super Computer*" anche la crittografia asimmetrica è violabile.
- Primo prototipo quantistico sperimentato in Italia: Università degli Studi di Milano

INTRODUZIONE

- Attualmente esistono sistemi quantistici che trasmettono su fibra ottica per un massimo di 100 Km.
- Sono in fase di studio altri sistemi che utilizzano l'aria come canale di comunicazione (per ora in buio quasi assoluto), per comunicazioni satellitari.
- Ulteriori studi sono stati fatti su fotoni di tipo *entangled*, in grado di contenere informazioni compresse.
- Si tratta comunque di tecnologie troppo complesse e costose non adatti alla "User Network"

OBIETTIVI

- Costruire un sistema di Quantum Key Distribution [QKD] a basso costo, per l'utente finale.
- Permettere la trasmissione sicura dei dati indipendentemente da algoritmi e strutture di calcolo in possesso di possibili intrusori, creando un sistema adatto a transazioni ATM e internet.
- Capire se la comunicazione P2P è stata violata o meno.

IL PROTOCOLLO BB84

[BENNET BRASSARD 1984]

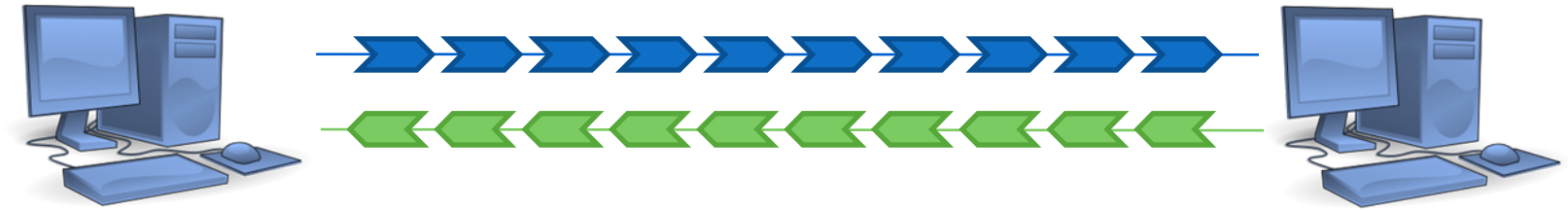
- Basato sulle leggi della fisica dei quanti come:
  - Il principio di indeterminazione di Heisenberg.
  - L'impossibilità di "fotocopiare" uno stato quantico sconosciuto senza introdurre errori sul canale.

- Permette lo scambio in linea di principio completamente sicuro di una chiave segreta.

IL PROTOCOLLO BB84

[BENNET BRASSARD 1984]

Trasmissione [TX] Ricezione [RX]



TX:

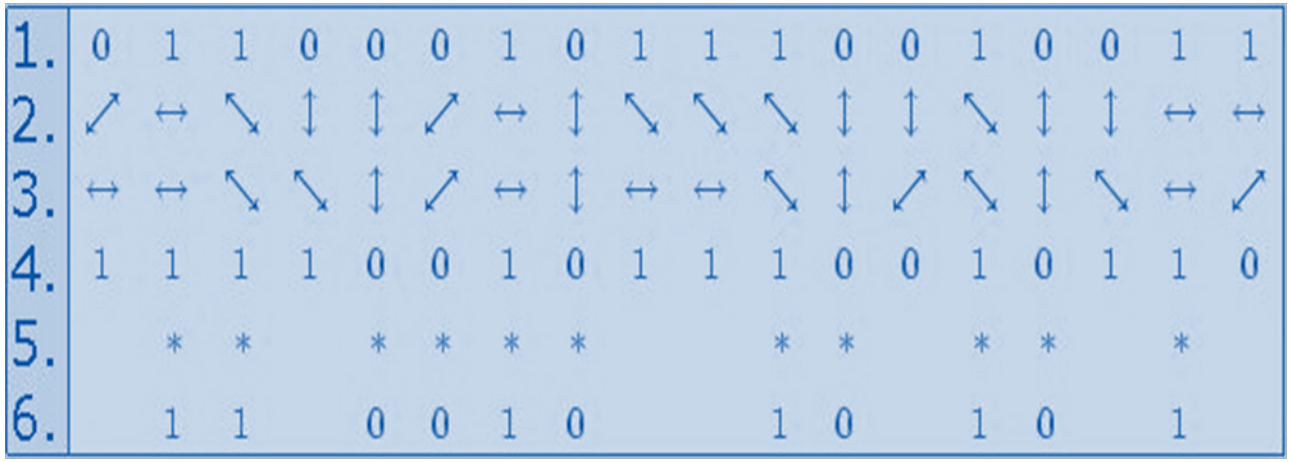
- Sceglie una sequenza casuale di 0 e 1 sottoforma di bit, i quali saranno trasformati in fotoni polarizzati e invia tutto a RX.
- Registra i risultati di RX e li confronta con i propri. Per ogni misurazione corretta, dunque, TX informerà RX che la posizione di quel dato è valida e il bit relativo ad essa sarà parte della chiave.

RX:

- Sceglie casualmente una misura di polarizzazione e la attribuisce al fotone in arrivo, lo converte in bit. Memorizza dunque le sue misure.
- Comunica a TX i risultati ottenuti ma indicando solo i dati relativi alle sue misure di polarizzazione. Il tutto tramite canale pubblico!

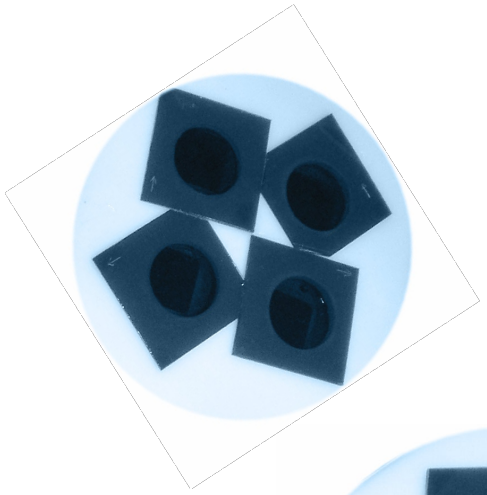
IL PROTOCOLLO BB84

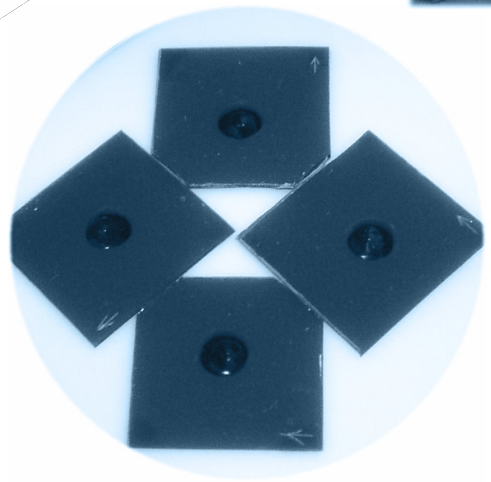
[BENNET BRASSARD 1984]

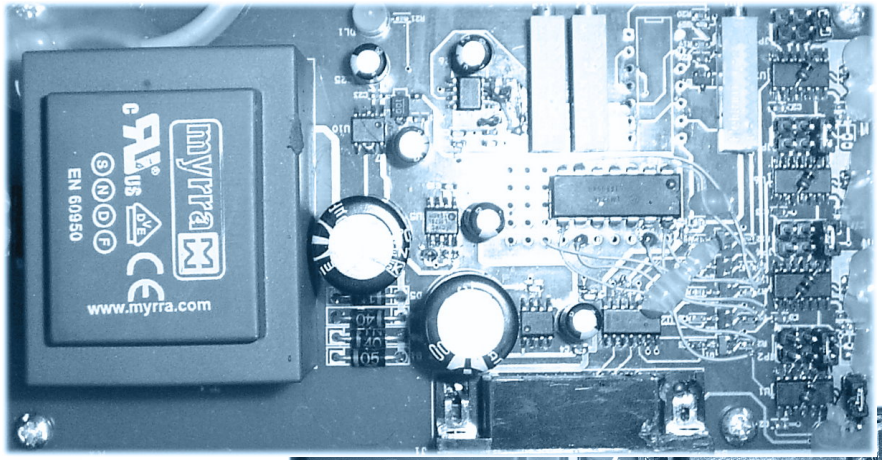


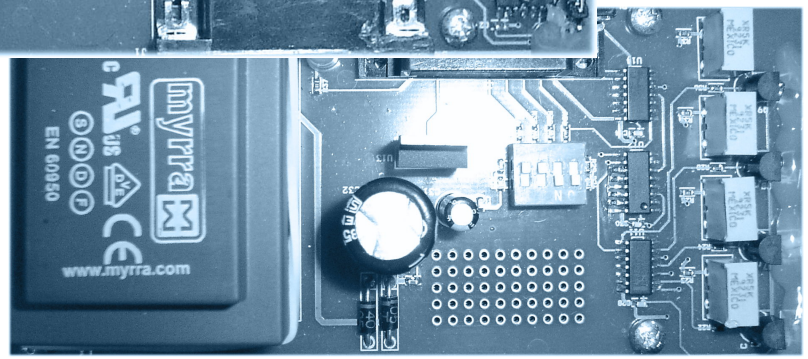
- Le due parti condividono quindi la stessa chiave sicuramente segreta.
- Un’eventuale intrusione è immediatamente rilevata poiché, introduce percentuale di errore a causa del principio quantistico dell’interferenza dell’osservatore.

IL SISTEMA









LE APPLICAZIONI

- Il sistema è usabile come *token* per terminali ATM, transazioni online etc.
- Può essere integrato nei normali PDA.
- E' un sistema compatto e assolutamente economico poiché utilizza un dispositivo innovativo: quattro LED polarizzati al posto di un unico laser e della sua costosissima tecnologia.

SVILUPPI FUTURI

- In futuro sarà possibile:
  - Integrare un TRNG [*IdQuantique*] al sistema.
  - Utilizzare fotodiodi a valanga.
  - Applicare algoritmi di gestione più compatti ed algoritmi per la correzione degli errori.

- Il sistema potrà essere accoppiato in fibra ottica tramite Relay quantistici ai sistemi di crittografia quantistica maggiori.
- Attualmente la città di Durban (Sud Africa) è stata completamente cablata con rete quantistica. Seguiranno a breve anche Madrid e Londra.
- Il presente della crittografia quantistica è cominciato.