Crittografia quantistica: fantascienza o realtà?

di Enrico Zimuel (enrico@zimuel.it)

21 Agosto 2004

Metro Olografix Camp 2004 - Pescara

Note sul copyright (copyfree):

Questa presentazione è stata realizzata con OpenOffice 1.1, il software open source per l'automazione d'ufficio disponibile sui sistemi Gnu/Linux e Ms Windows.
www.openoffice.org

Ringrazio il **Dott. Leonida Gianfagna** per i numerosi consigli sulla meccanica quantistica che mi ha fornito nella realizzazione di questa presentazione.

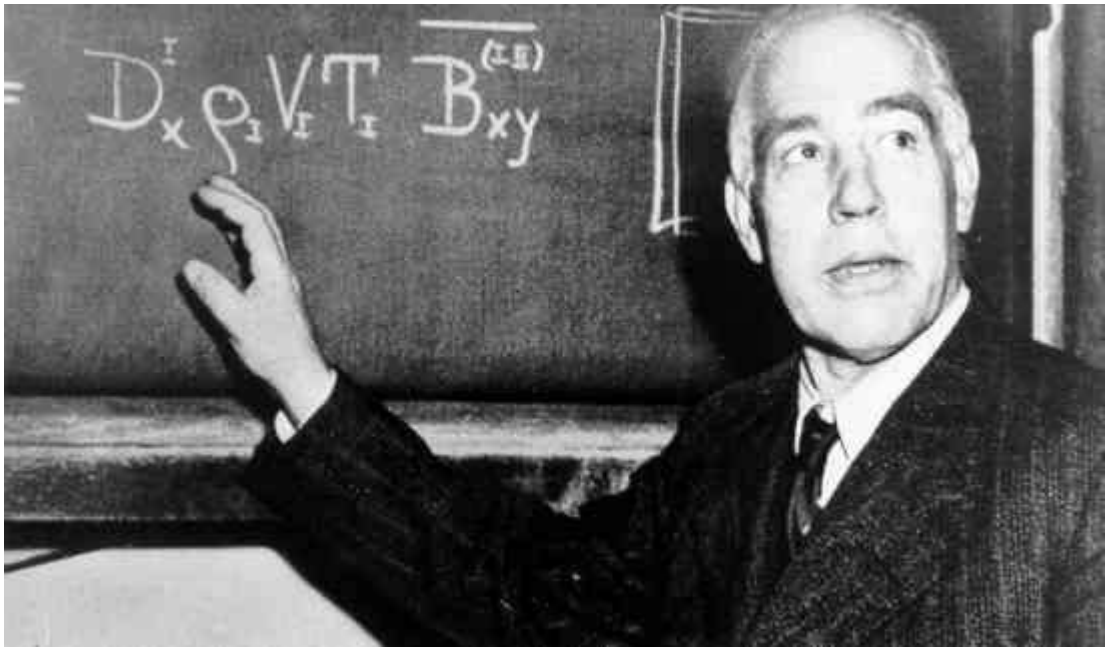
L'immagine riportata in prima pagina è un'elaborazione dell'opera ***Universe*** di **Kathy Ferdon** © 2003.

Sommario:

- Introduzione alla meccanica quantistica
- L'esperimento di Stern e Gerlach
- Il Quantum Key Distribution (QKD)
- Il protocollo BB84
- I limiti del protocollo BB84
- Attacco *man-in-the-middle* al protocollo BB84
- Esempi di implementazioni reali di QKD
- Bibliografia e siti Internet d'interesse

"Chiunque non rimanga scioccato dalla teoria quantistica vuol dire che non l'ha capita."

(Niels Bohr)



Introduzione alla meccanica quantistica

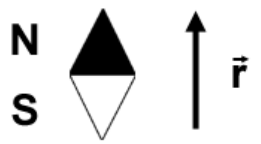
- La meccanica quantistica è una teoria che ha rivoluzionato il mondo della fisica ed il modo di concepire la realtà.
- Tale teoria, come la conosciamo oggi, è stata formulata nel biennio 1925-1927 grazie soprattutto a *W.Heisenberg* (Meccanica delle matrici), *E.Schroedinger* (Meccanica ondulatoria), *M.Born* (Interpretazione probabilistica), *P.A.M. Dirac* (formalismo generale che mostra l'equivalenza della teoria di Heisenberg e quella di Schroedinger).
- Con la meccanica quantistica si abbandona la visione deterministica del mondo fisico ossia l'idea della possibilità di conoscere l'andamento futuro di un sistema a partire dalla conoscenza di alcune grandezze fisiche in un certo istante.

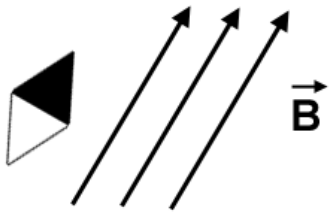
Introduzione alla meccanica quantistica

- Nella meccanica quantistica la realtà viene modellata attraverso l'introduzione di funzioni di probabilità, il “caso” gioca un ruolo essenziale, intrinseco del fenomeno (*Dio gioca a dadi?*).
- Ad esempio nella meccanica quantistica non è possibile conoscere contemporaneamente la posizione e la velocità di un elettrone (*principio di indeterminazione di Heisenberg*).
- Nella *fisica classica* il caso può essere dovuto solamente ad una conoscenza imperfetta dello stato iniziale, come avviene ad esempio nel lancio di un dado, nella meccanica quantistica il caso, la probabilità, è una proprietà intrinseca del sistema.
- Il processo che ha portato all'abbandono della fisica classica in favore di quella quantistica è essenzialmente concentrato nel periodo 1900-1925 quando si iniziano i primi esperimenti su scala atomica (dell'ordine di 10^{-10} metri).

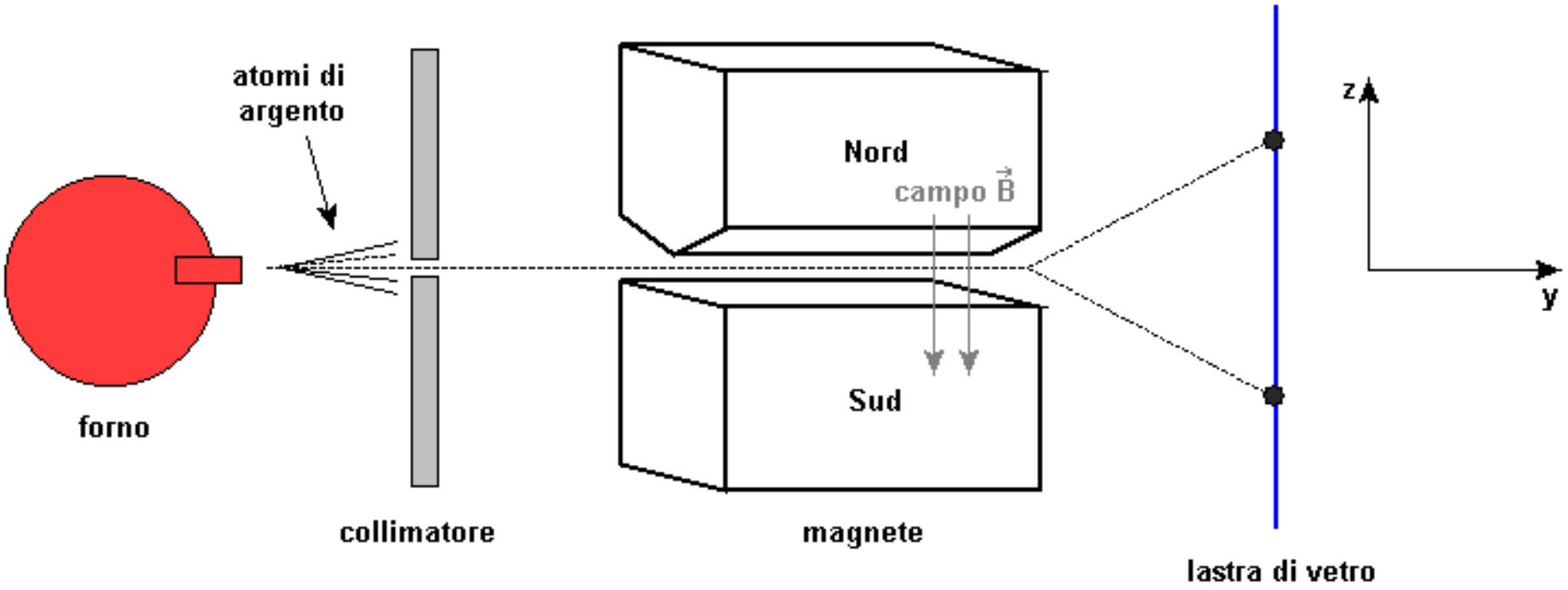
L'esperimento di Stern e Gerlach

- Questo esperimento fu ideato da Stern nel 1921 per misurare il momento magnetico dei sistemi atomici e fu realizzato nel 1922 da Stern e Gerlach con degli atomi di argento.
- In questo esperimento semplifichiamo molto il comportamento di un atomo di argento paragonandolo ad un piccolo ago magnetico.
- Il comportamento di un piccolo ago magnetico nelle vicinanze di un magnete (o più in generale di un campo magnetico **B**) è determinato da un vettore **r** detto momento magnetico che ha la direzione dell'ago, dal polo sud al polo nord, e modulo proporzionale al momento delle forze indotto da **B** sull'ago.

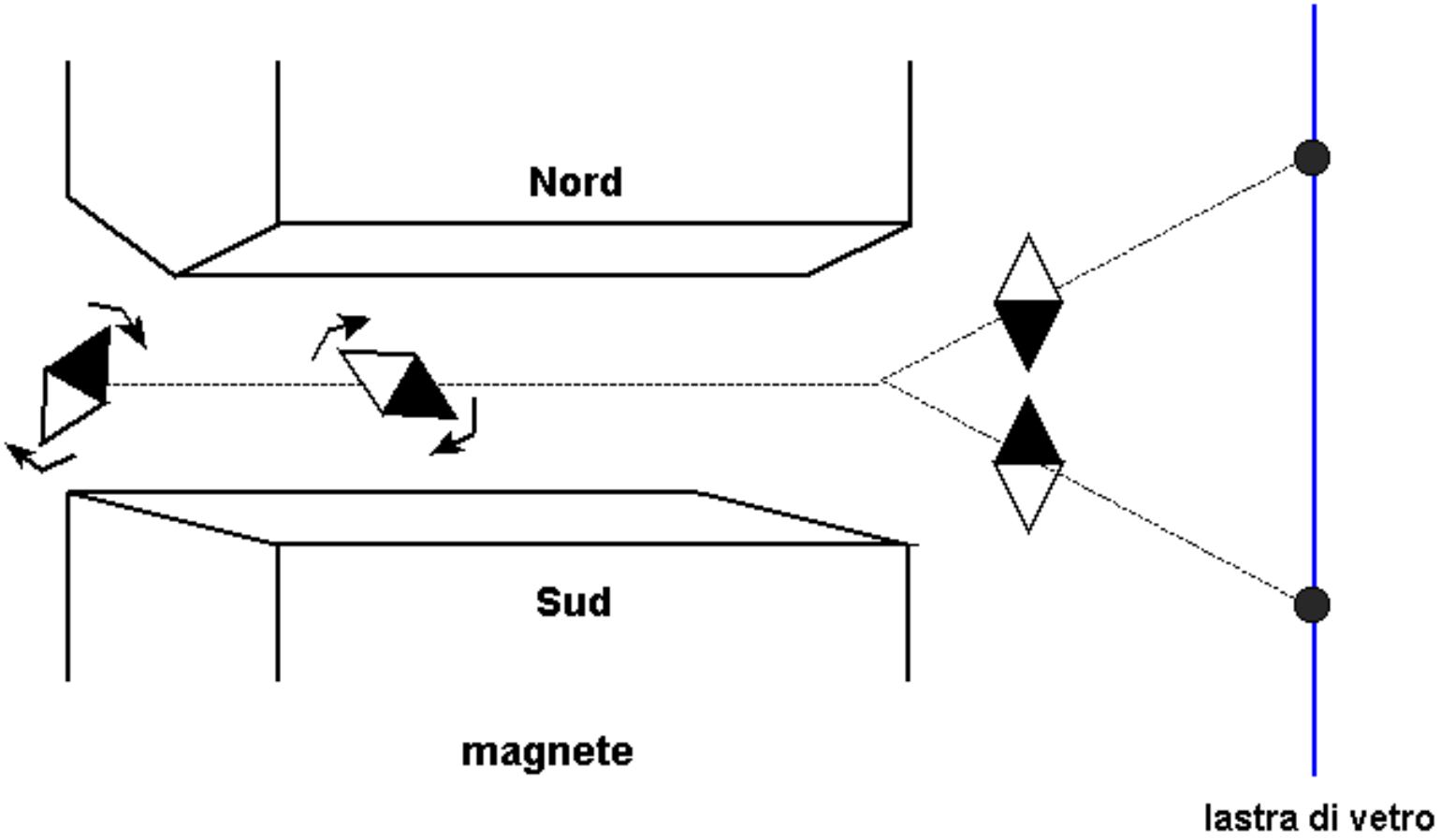




L'esperimento di Stern e Gerlach



L'esperimento di Stern e Gerlach



L'esperimento di Stern e Gerlach

- Gli atomi di argento escono dal forno con un momento angolare casuale, come mai sulla lastra di vetro si osservano soltanto due valori?

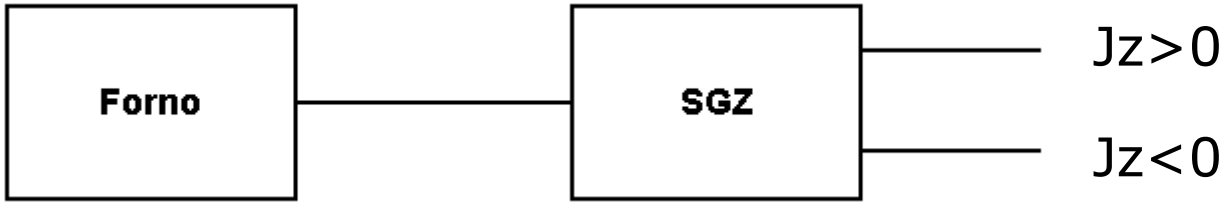
- Classicamente ci si aspetterebbe una distribuzione continua degli atomi di argento lungo la lastra di vetro (più precisamente una distribuzione gaussiana).

- Indicando con J il momento angolare dell'atomo di argento, alla fine dell'esperimento, risulta che tutti gli atomi vengono divisi in due gruppi, quelli che hanno $J_z>0$ e quelli che hanno $J_z<0$.

- Questo fenomeno prende il nome di *quantizzazione del momento angolare*.

L'esperimento di Stern e Gerlach

- Utilizziamo il seguente schema grafico dell'apparato sperimentale di Stern e Gerlach:

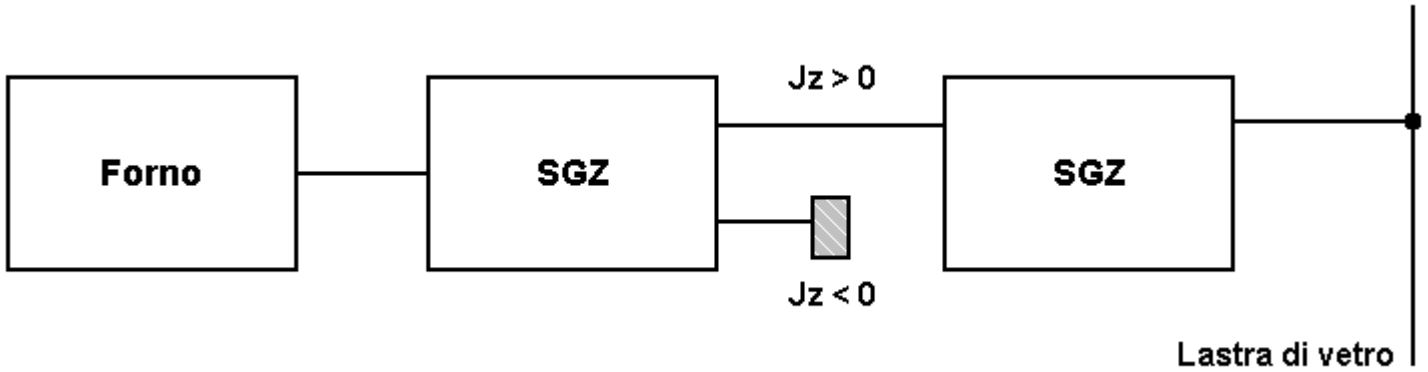


SG indica Stern e Gerlach mentre Z indica il fatto che la deflessione avviene nella direzione dell'asse Z (in pratica SGZ può essere considerato come un filtro che seleziona gli atomi di argento con Jz>0 e Jz<0).

- Ruotando l'apparato attorno all'asse Y di 90 gradi otteniamo una deflessione nella direzione X (uscente dal video). Indichiamo questo nuovo filtro con SGX.

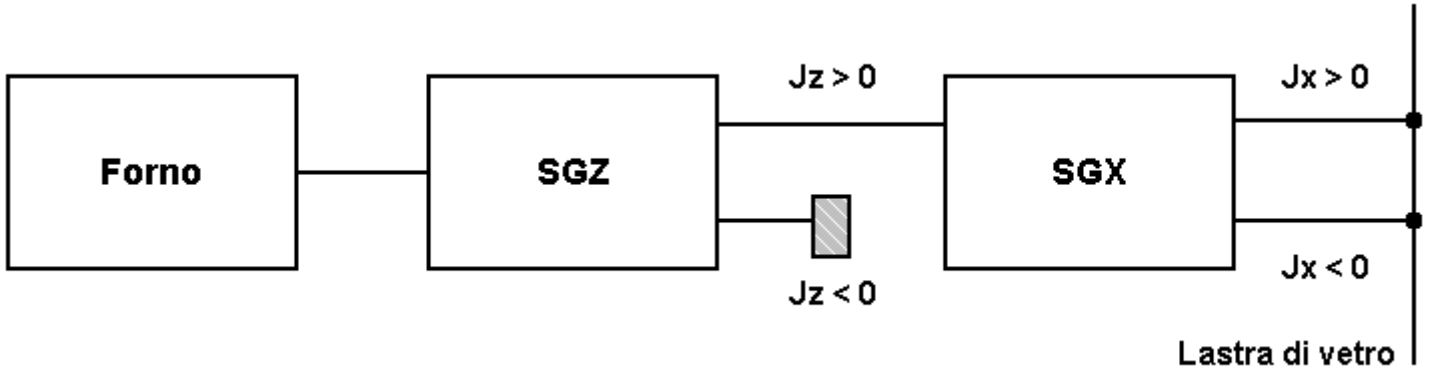
L'esperimento di Stern e Gerlach

- Inserendo in serie due dispositivi SGZ e bloccando all'uscita del primo gli atomi con Jz<0 otteniamo solo atomi con Jz>0.



- Il primo filtraggio SGZ sembra aver rimosso la casualità (50% Jz>0 e 50% Jz<0). Se inseriamo al posto del secondo SGZ un filtro SGX otteniamo nuovamente due macchie?

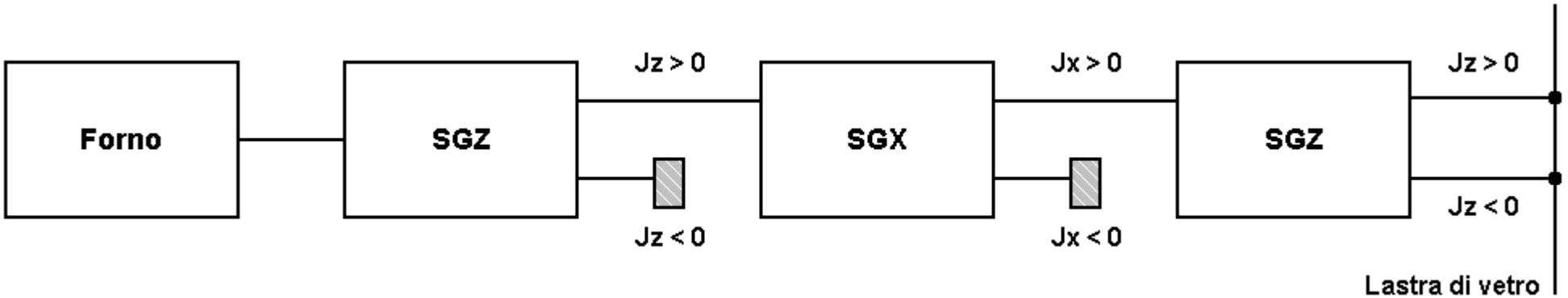
L'esperimento di Stern e Gerlach



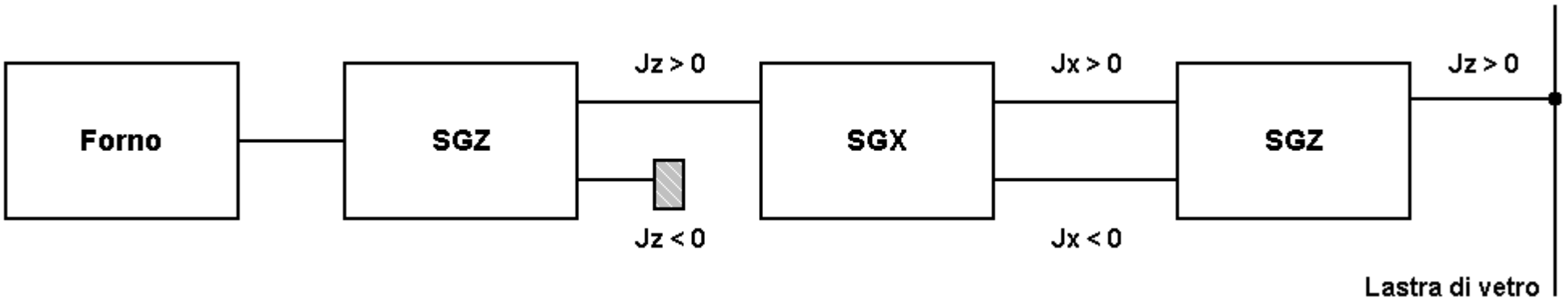
- Evidentemente l'aver selezionato Z non influenza il momento angolare lungo l'asse X. Questo risultato potrebbe essere interpretato considerando che all'uscita del forno gli atomi escono con momento angolare casuale. Dopo SGZ selezioniamo quelli con Jz>0 e blocchiamo quelli con Jz<0, dopo SGX otteniamo quindi atomi di argento con (Jx>0, Jz>0) e (Jx<0, Jz>0).

- Cosa succede se inseriamo un terzo filtro SGZ bloccando gli atomi con Jx<0 sul secondo filtro SGX? Secondo l'interpretazione precedente dovremmo ottenere (Jx>0, Jz>0)...

L'esperimento di Stern e Gerlach



- Otteniamo di nuovo Jz>0 e Jz<0? Com'è possibile dal momento che li avevamo eliminati con il primo filtro SGZ? E se proviamo a non bloccare Jx<0 sul fitro SGX, cosa accade?



L'esperimento di Stern e Gerlach

- In pratica se effettuiamo una misura (bloccando gli atomi di argento o osservando il risultato sulla lastra di vetro) eliminiamo in qualche modo l'informazione che avevamo acquisito lungo l'asse Z.

- Nell'ultimo schema il filtro SGX ha un comportamento neutro, può essere eliminato senza perturbare l'esito dell'esperimento.

- Il punto fondamentale è legato proprio al *processo di misurazione*. Non è possibile attribuire simultaneamente un valore alle due grandezze fisiche Jx e Jz. Se misuriamo Jx allora Jz ha valore positivo con probabilità ½ e valore negativo con probabilità ½ e viceversa.

- L'esperimento indica “l'incompatibilità” delle due grandezze Jx e Jz, questo fenomeno è tipico della meccanica quantistica e viene indicato con il *principio di indeterminazione di Heisenberg* già citato in precedenza.

L'esperimento di Stern e Gerlach

- A questo punto si potrebbe obiettare che in qualche modo il fascio di atomi di argento si comporta in questo modo “strano” perchè gli atomi si influenzano a vicenda. Proviamo ad inviare un atomo di argento alla volta, cosa succede?

- L'esito dell'esperimento rimane invariato! Ciò vuol dire che il modo “classico” di pensare le componenti del momento angolare di un atomo non è corretto. Gli atomi non hanno proprietà prestabilite sulle componenti del momento angolare, il fatto di dire che Jz>0 dopo averlo misurato non mi consente di affermare che l'atomo aveva questa proprietà (in effetti non so se Jz>0 prima di averlo misurato!).

- Questa visione del mondo si discosta enormemente dalla visione classica, si aprono così nuovi orizzonti per la fisica e non solo...

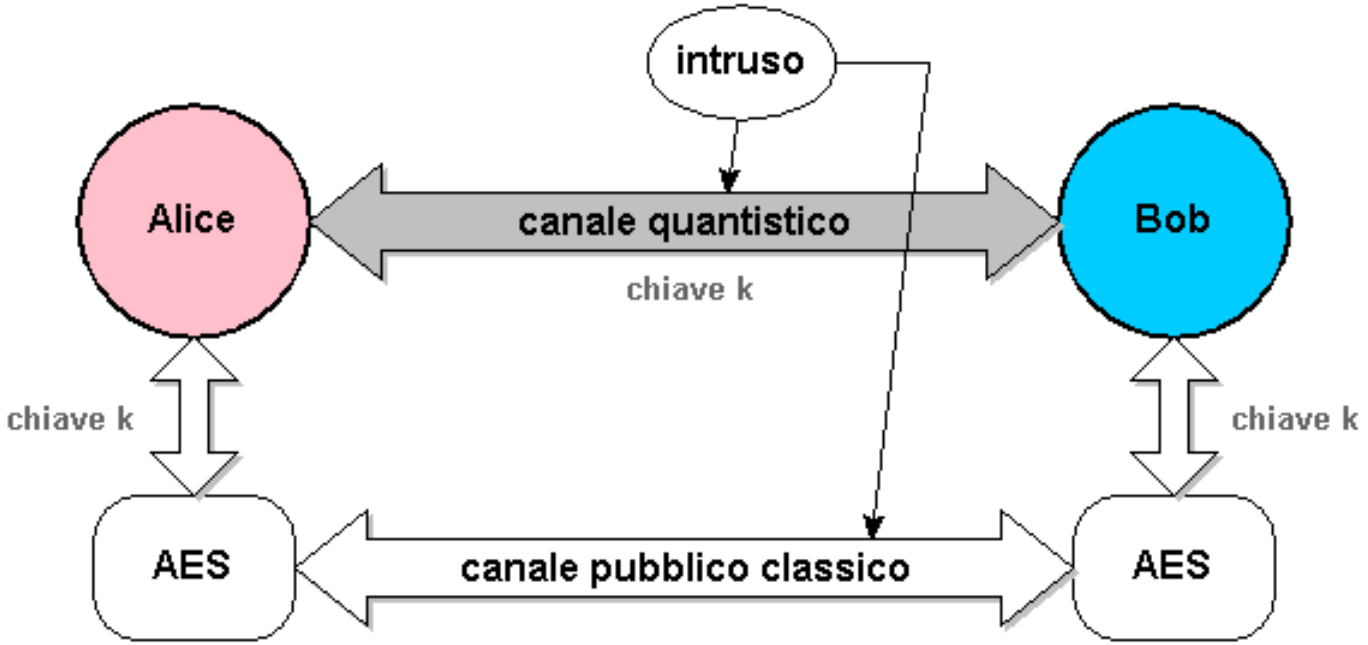
- Alcuni fisici, ad esempio David Deutsch, sostengono che ci sono molti universi che interferiscono tra loro (*teoria del multiverso*).

Il Quantum Key Distribution (QKD)

- Come possiamo sfruttare i principi della meccanica quantistica in ambito crittografico?
- Il principio di indeterminazione di Heisenberg afferma sostanzialmente che non è possibile effettuare un processo di misurazione senza perturbare il fenomeno in questione.
- Tramite questo principio possiamo costruire un canale quantistico di comunicazione ed essere sicuri, almeno in teoria, che nessuno sia in grado di intercettare la comunicazione senza essere scoperto?
- Come possiamo costruire un canale quantistico? Come codifichiamo le informazioni su questo canale? Come possiamo rilevare la presenza di un eventuale intruso sulla linea di comunicazione?

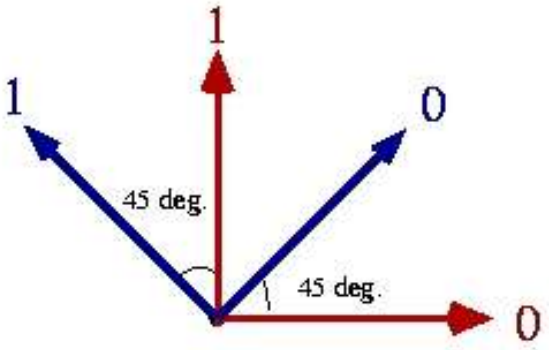
Il Quantum Key Distribution (QKD)

- Utilizziamo il canale quantistico per lo scambio di una chiave segreta k (di bit casuali). Questa chiave k, se non intercettata, verrà utilizzata come chiave di un sistema di cifratura con algoritmo simmetrico (ad esempio AES) per lo scambio dei dati cifrati su di un normale canale pubblico di comunicazione (ad esempio Internet).



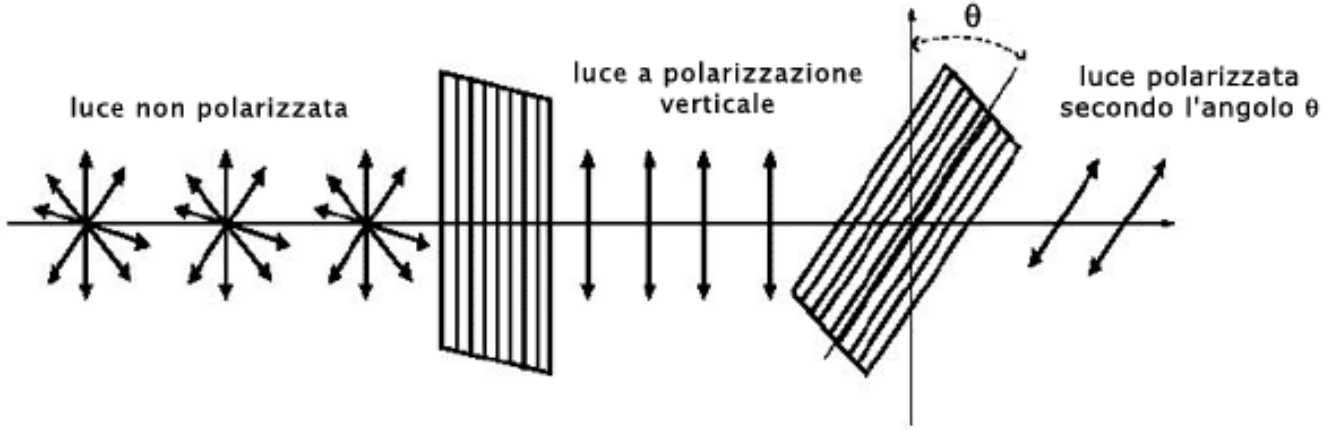
Il protocollo BB84

- Il protocollo BB84 è stato ideato da Bennet e Brassard nel 1984.
- E' un protocollo di tipo QKD che utilizza la fibra ottica e la polarizzazione dei fotoni per la tramissione e la codifica dei bit.
- Alice e Bob sono collegati tra loro tramite una fibra ottica. Alice ha a disposizione un dispositivo di emissione di fotoni polarizzati linearmente in 4 possibili modi. Le polarizzazioni vengono denominate *verticale*, *orizzontale*, *diagonale*, *anti-diagonale* ed indicate con i simboli |, -, /, \. Queste polarizzazioni (vettori) sono suddivise in due basi Gz={|,-} e Gx={/, \}.
- Ad ogni base è associata una coppia di valori binari 0 e 1 nel modo seguente: |=1, -=0 e /=0, \=1.
- Bob ha a disposizione un dispositivo per rilevare i fotoni emessi da Alice.



La polarizzazione dei fotoni

- La luce è di natura ondulatoria ossia è una funzione d'onda con un proprio angolo di polarizzazione θ (theta) compreso fra 0° e 180°.
- Utilizzando degli opportuni filtri di polarizzazione è possibile variare l'angolo θ (θ-filter).
- Un fotone a monte del filtro, polarizzato con un angolo φ (phi), oltrepassa un θ-filter con probabilità $p_{\varphi}(\theta)= \cos^2(\varphi-\theta)$ emergendo ovviamente con polarizzazione θ. La probabilità che lo stesso fotone sia invece respinto dal filtro è naturalmente $1-p_{\varphi}(\theta)= \mathrm{sen}^2(\varphi-\theta)$ (dal momento che $\mathrm{sen}^2(x)+\cos^2(x)=1$).



Il protocollo BB84

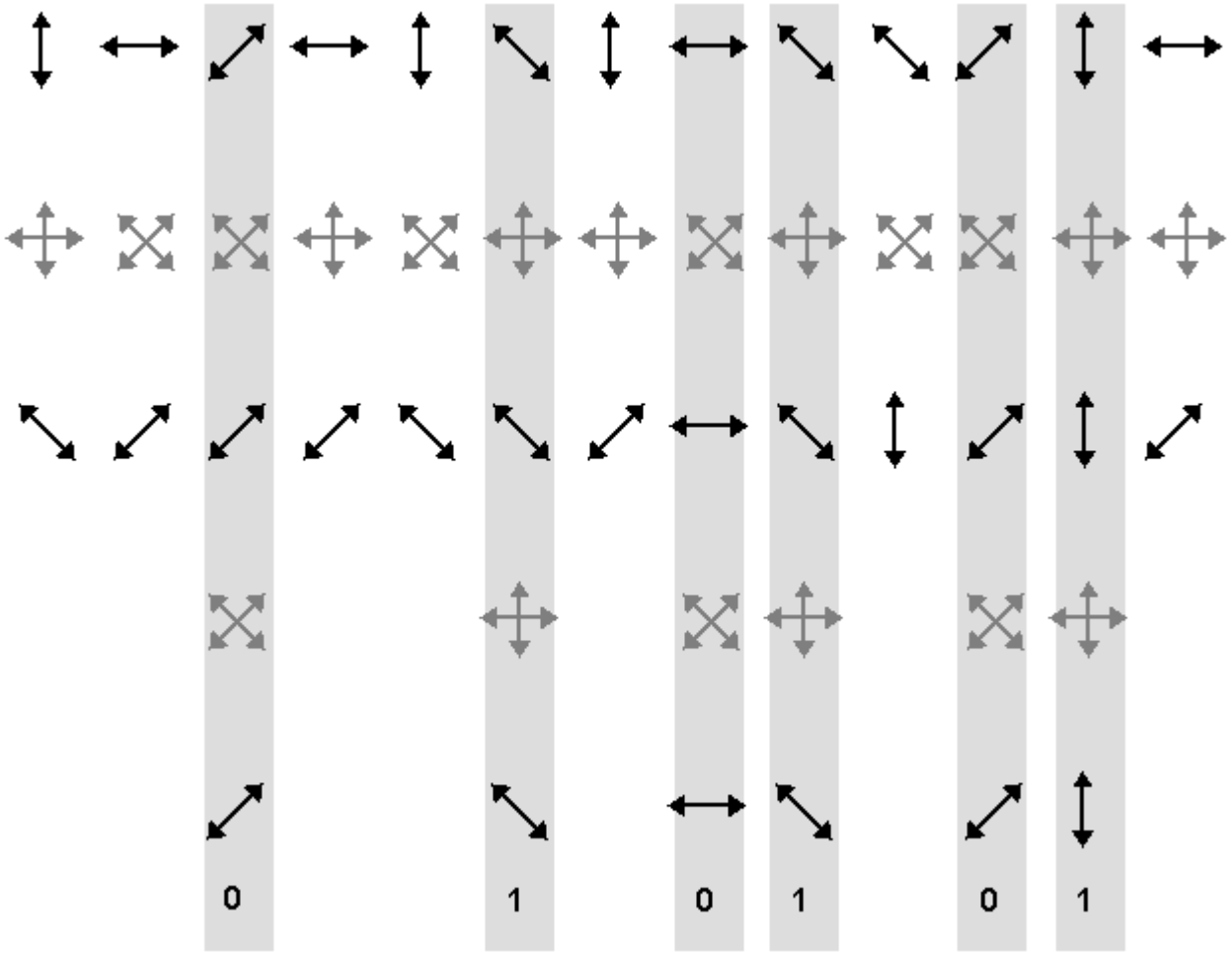
1) Alice sceglie casualmente, con una probabilità del 50%, n basi di polarizzazione Gz e Gx, e successivamente genera, sempre casualmente, n fotoni codificati in 0 o 1 nelle basi corrispondenti. Invia questi fotoni a Bob.

2) Per ogni fotone ricevuto Bob sceglie casualmente una delle due basi di polarizzazione Gz e Gx e misura la polarizzazione del fotone (in questo modo Bob ha una probabilità del 50% di indovinare la codifica binaria di Alice).

3) Alice e Bob utilizzano il canale pubblico di comunicazione per confrontare le basi di polarizzazione scelte da entrambi.

4) Con queste informazioni tutti e due possono determinare i bit che sono stati inviati correttamente, confrontando le basi identiche. Se, mediamente, si ottiene il 50% dei bit corrispondenti vorrà dire che nessun intruso ha intercettato il messsaggio e quindi questi bit possono essere utilizzati come chiave segreta (k). Se la percentuale d'errore è diversa, tipicamente con un incremento del 25% d'errore, la trasmissione della chiave dovrà essere rieseguita tornando al punto 1 (è stata rilevata la presenza di un intruso).

Il protocollo BB84 (esempio)



Alice invia a Bob n fotoni polarizzati casualmente.

Bob sceglie a caso la base di misurazione.

Bob registra il risultato della misurazione e lo tiene segreto.

Bob annuncia pubblicamente le basi scelte ed Alice le conferma quelle corrette.

Viene determinata la chiave decodificando le polarizzazioni.

Errore= 6/13=0,46 circa il **50%** ossia nessuna intercettazione. La chiave segreta risulta essere **010101**.

I limiti del protocollo BB84

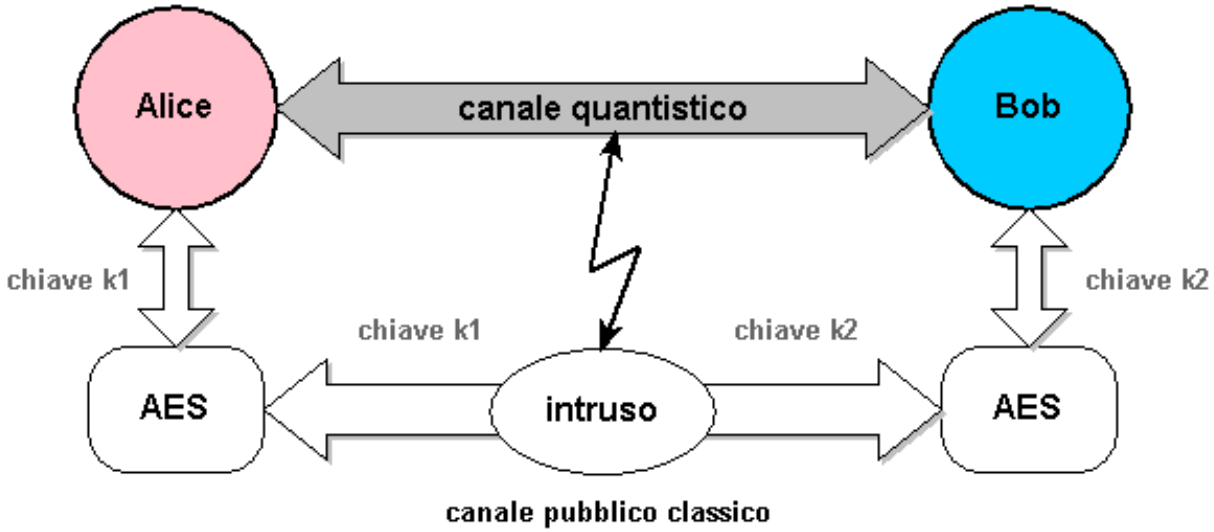
- In realtà il processo di rilevamento delle intrusioni è più complesso e si basa su tecniche di tipo statistico e di correzione degli errori. La sostanza del discorso è comunque la stessa.

- I limiti del protocollo BB84 sono legati principalmente a fattori tecnologici (è molto difficile realizzare dispositivi che lavorino effettivamente con singoli fotoni con errori di trasmissione limitati) e a fattori di architettura del sistema (in pratica la sicurezza dell'intero sistema è affidata al sistema di crittografia a chiave simmetrica e non alla crittografia quantistica che viene utilizzata solo per l'interscambio della chiave; questo è un limite di tutti i sistemi QKD).

- Possibili attacchi al protocollo BB84 sono legati dunque alle limitazioni tecniche dei dispositivi di emissione e rilevamento dei fotoni ed a possibili attacchi di tipo *man-in-the-middle* sul canale pubblico e quantistico.

L'attacco man-in-the-middle al protocollo BB84

- Un eventuale intruso può posizionarsi tra Alice e Bob ed intercettare sia il segnale sul canale quantistico che sul canale pubblico.
- Sul canale pubblico l'intruso potrebbe rielaborare le basi di misurazione tra Alice e Bob in modo da far risultare un errore del 50%.
- A questo punto, l'intruso, può utilizzare due chiavi differenti per le comunicazioni tra Alice e l'intruso (**k1**) e tra l'intruso e Bob (**k2**).

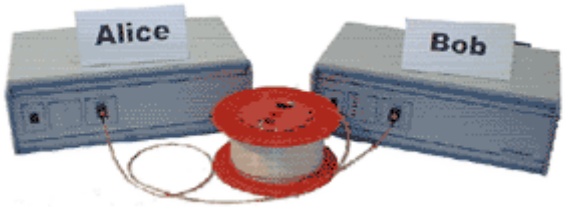


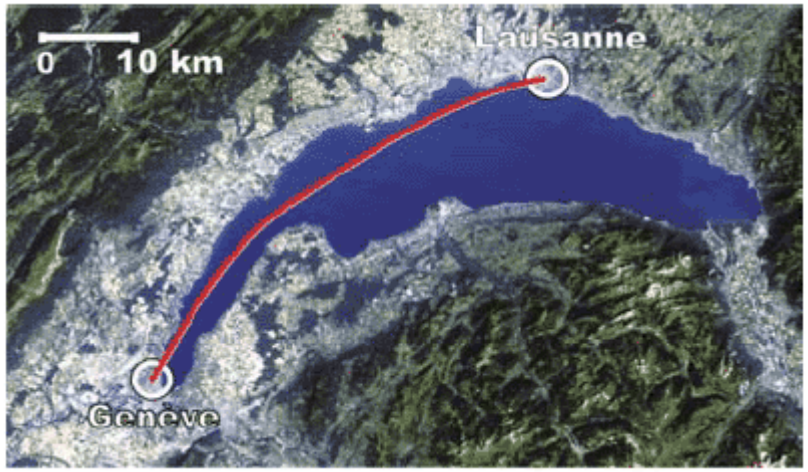
- Per ovviare a questo tipo di attacco è necessario utilizzare un **sistema di autenticazione** tra Alice e Bob nel canale pubblico di comunicazione.

Esempi di implementazioni reali di QKD

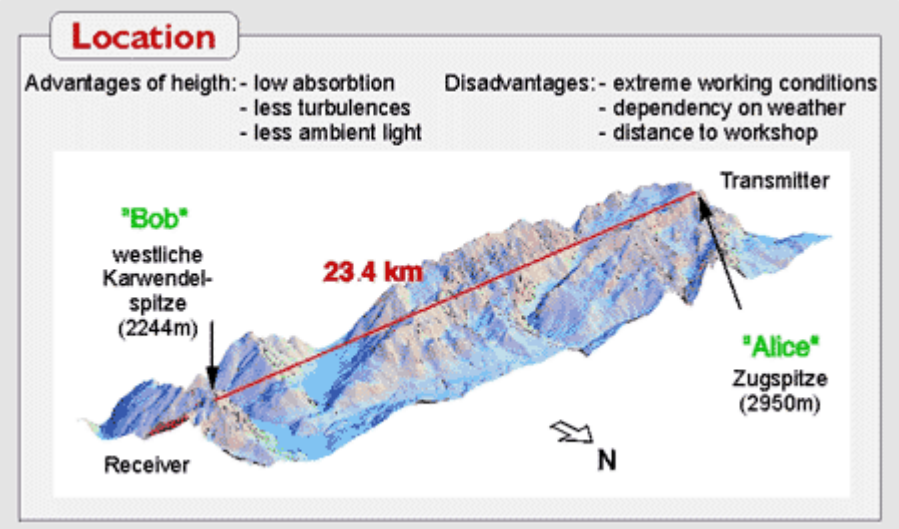
- Negli ultimi anni sono stati effettuati numerosi esperimenti di QKD. Ed ultimamente sono sorte anche delle aziende che producono dispositivi in grado di implementare un sistema QKD in fibra ottica interfacciandosi con una rete Ethernet per lo scambio delle informazioni sul canale pubblico.

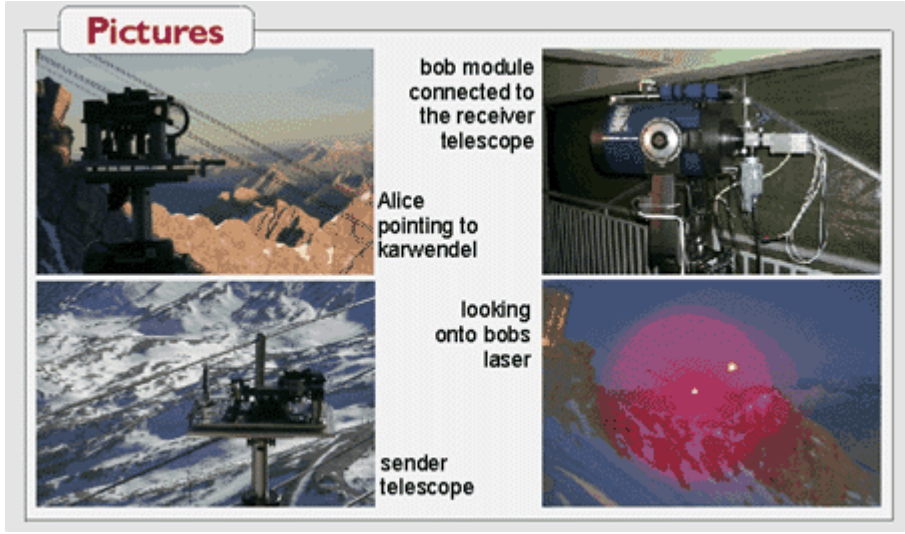
- Ad esempio nel 2001 presso il CERN di Ginevra è stato effettuato il primo esperimento di QKD tramite fibra ottica a lunga distanza (circa 67 Km lungo le linee standard della Swisscom).

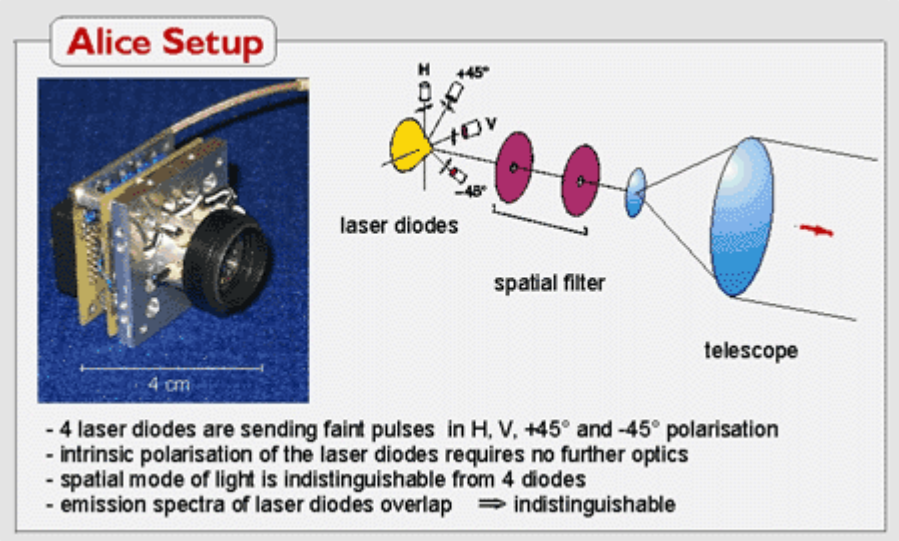


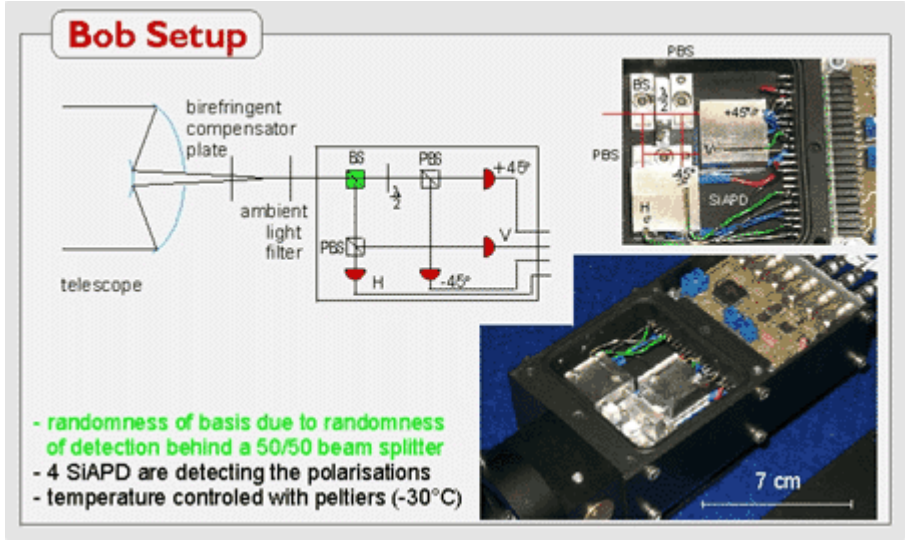


- Alcuni ricercatori tedeschi dell'istituto Max-Plank hanno effettuato esperimenti di QKD via etere tramite raggi laser.



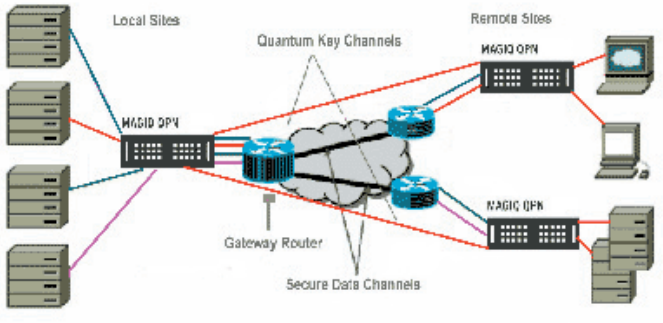






Esempi di implementazioni commerciali di QKD

- La società americana MagiQ Technologies nata nel 2002 che produce sistemi di QKD integrati con soluzioni VPN (QPN5505). Alcuni dati tecnici: refresh massimo delle chiavi 100 al secondo, VPN tramite IPSEC, standard AES, 3DES, BB-84, distanza massima fibra ottica 120 Km, generatore di numeri casuali.



- La società svizzera idQuantique nata nel 2001 da uno spin-off di alcuni ricercatori dell'Università di Ginevra. Oltre a produrre dispositivi di QKD si è dedicata allo sviluppo di sistemi di generazione di numeri casuali con dispositivi quantistici. Nei primi di Agosto del 2004 ha lanciato un nuovo prodotto: Quantis-PCI, un generatore di numeri casuali quantistico su scheda PCI.

Bibliografia (in italiano):

- J. Brown, “Menti, macchine e multiverso”, Einaudi, 2003
- R. Feynman, “Sei pezzi facili”, Adelphi, 2000
- R. Feynman, “La fisica di Feynman. Vol III, meccanica quantistica”, Zanichelli, 2001
- G.G. Ghirardi, “Un'occhiata alle carte di Dio”, Il Saggiatore, 1997
- D. Lindley, “La luna di Einstein”, TEA Edizioni, 2001
- J.J. Sakurai, “Meccanica quantistica moderna”, Zanichelli, 1996
- L.D. Landau, E.M. Lifsits “Meccanica quantistica (teoria non relativistica)”, Editori Riuniti, Edizioni Mir, 1991
- C.H. Bennet, G. Brassard, A.K. Ekert, “Crittografia quantistica”, Le Scienze quaderni, n. 112 – pagg. 88-95
- A.K. Ekert, R.Lupacchini, “Calcolatori quantistici”, Il Nuovo Saggiatore vol. 15 (2000) – pagg. 58-64

Siti Internet d'interesse (in inglese):

- http://www.qubit.org
- http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html
- http://www.cs.dartmouth.edu/~jford/crypto.html
- http://www.ecst.csuchico.edu/~atman/Crypto/quantum/quantum-index.html
- http://xqp.physik.uni-muenchen.de
- http://tph.tuwien.ac.at/~oemer/qcl.html
- http://www.ucci.it/it/qc/whitepapers/index.html (alcuni articoli in italiano)
- http://www.arxiv.org/ (ricerca quantum cryptography)
- http://www.magiqtech.com
- http://www.idquantique.com/