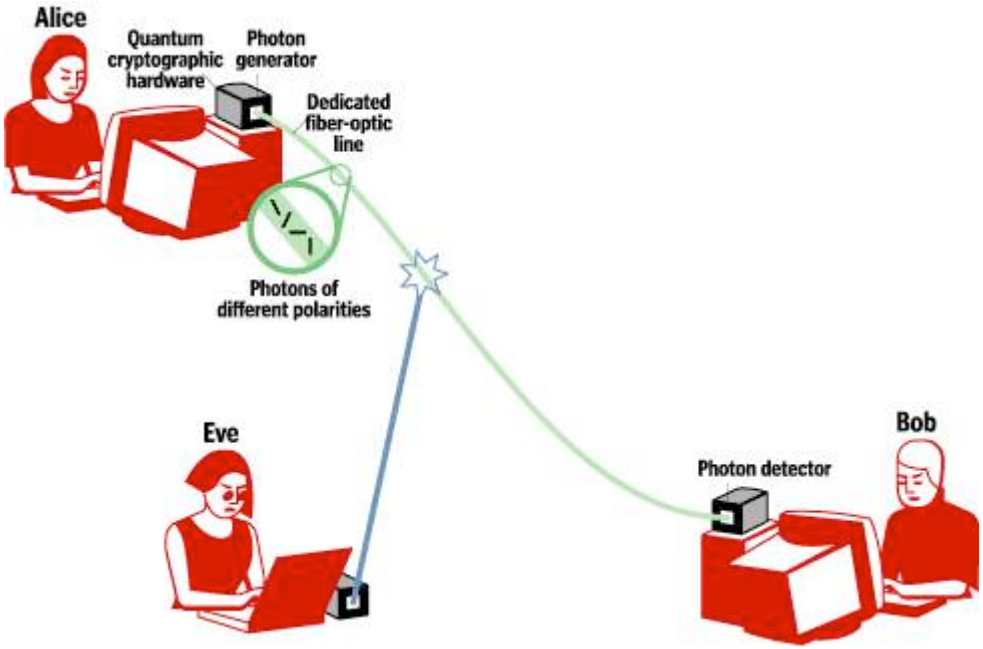
CRITTOGRAFIA QUANTISTICA

Oliver Morsch

CNR-INFM, Dipartimento di Fisica, Pisa

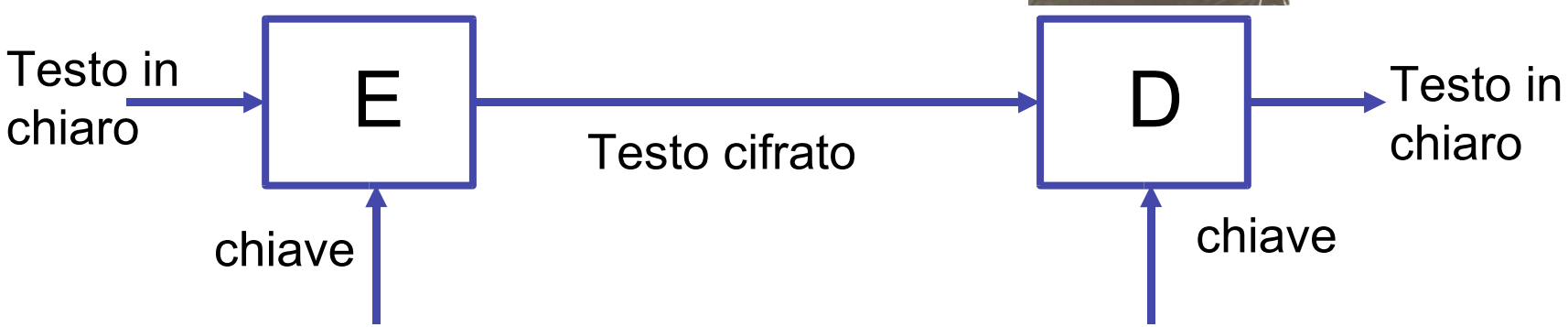
(basato su lucidi di Massimo Palma e Enrico Zimuel)



sommario

- Sistemi crittografici a chiave pubblica vs. sistemi a chiave privata
- La polarizzazione del fotone e le regole della meccanica quantistica
- Il protocollo BB84
- Quantum eavesdropping
- Sistemi crittogafici ed entanglement quantistico
- Implementazioni di crittografia quantistica

crittografia



•Alice trasforma il testo in chiaro in testo cifrato mediante un algoritmo di codifica E

•Bob estrae il testo in chiaro dal testo cifrato mediante un algoritmo di decodifica D

•Gli algoritmi E e D fanno uso di un'informazione segreta nota come "chiave"

sistemi a chiave pubblica (asimmetrica)

- Nei sistemi a chiave asimmetrica le chiave per la codifica e per la decodifica sono differenti
- Bob distribuisce chiavi publiche che consentono la codifica del messaggio C_{pub}
- Alice codifica il messaggio tramite C_{pub}
- Il testo cifrato può essere decrittato solamente da Bob mediante una chiave privata C_{priv} nota solamente a lui

Analogia: Bob mette a disposizione di Alice una casella di posta. Chiunque può imbucare un messaggio criptato ma solamente Bob può aprire la caselle i.e. decrittare il messaggio.

limiti dei sistemi a chiave asimmetrica

•I sistemi crittograficia chiave asimmetrica, e.g. l'RSA, si basano sull'esistenza di problemi computazionalmente difficili, quale la fattorizzazione di grandi numeri interi.

•Non essendo incondizionatamente sicuri tali sistemi sono affidabili solamente se le risorse necessarie ad Eve per decrittare il messaggio sono maggiori del valore dell'informazione contenuta nel testo cifrato

•La difficoltà computazionale di molti problemi non è provata e.g. non si sa se esiste un algoritmo polinomiale per la fattorizzazione (e non è detto che se tale algoritmo fosse scoperto sarebbe poi reso pubblico....)

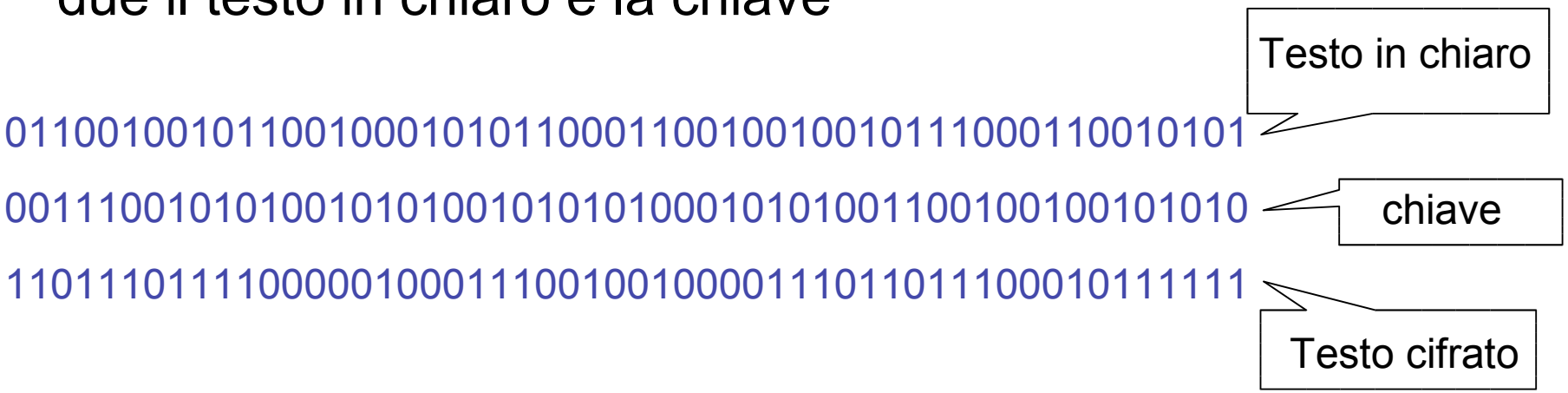
•Esiste un algoritmo *quantistico* efficiente (polinomiale) per la fattorizzazione di interi – l'algoritmo di Shor. Anche se non è ancora stato costruito un computer quantistico e meglio essere prudenti!

sistemi a chiave privata (simmetrica)

La stessa chiave viene utilizzata per la encrittazzione e per la decrittazzione

Es: il cifrario di Vernam o “ONE-TIME-PAD”.

Il testo cifrato si ottiene sommando modulo due il testo in chiaro e la chiave



Il testo in chiaro si ottiene sommando modulo due il testo cifrato e la chiave

distribuzione di chiavi crittografiche

Il cifrario di Vernam è incondizionatamente sicuro a patto che la chiave:

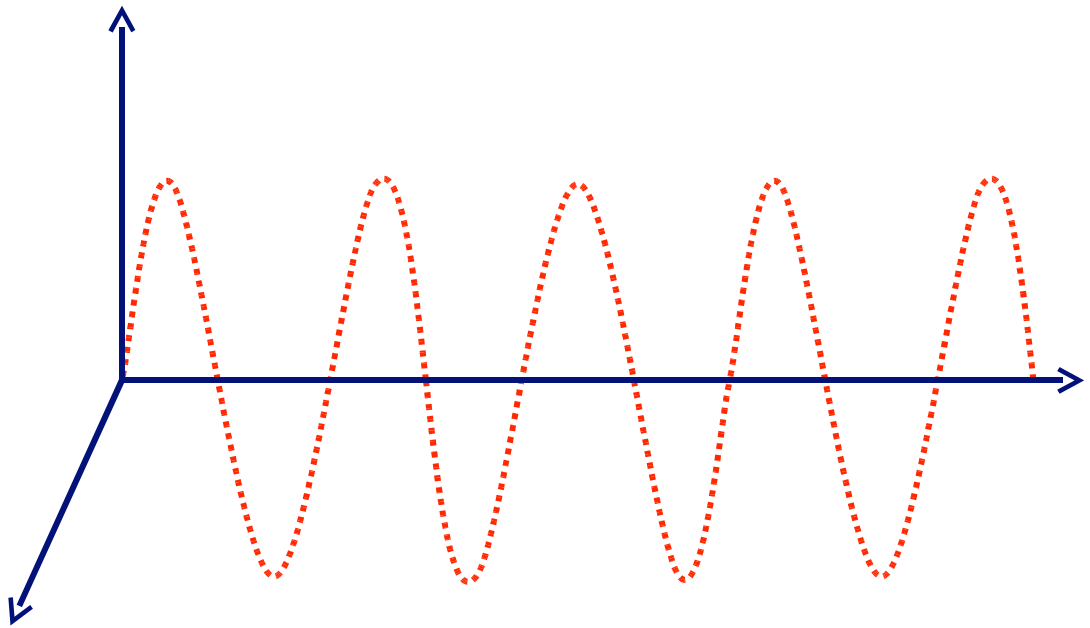
•Sia totalmente “random” e di lunghezza pari al testo in chiaro

•Sia usata solo una volta

•Sia segreta !

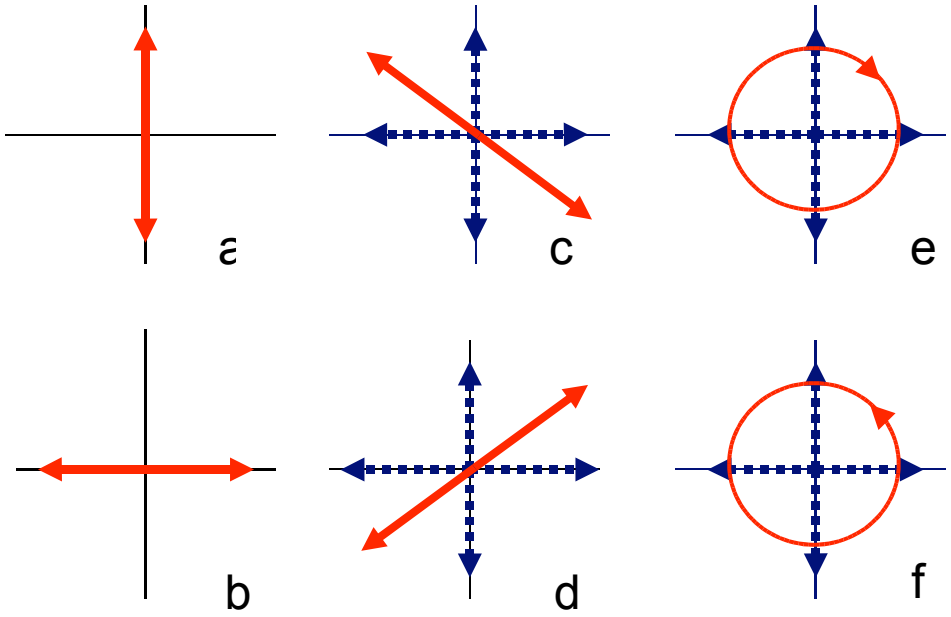
Il problema principale dei sistemi a chiave simmetrica è la distribuzione delle chiavi
La **distribuzione quantistica di chiavi** è una famiglia di protocolli che consentono a due utenti di stabilire una chiave comune anche se in presenza di parti ostili

la polarizzazione di un’onda e.m.



La polarizzazione di un’onda elettromagnetica monocromatica è il piano di oscillazione del campo elettrico.

stati di polarizzazione

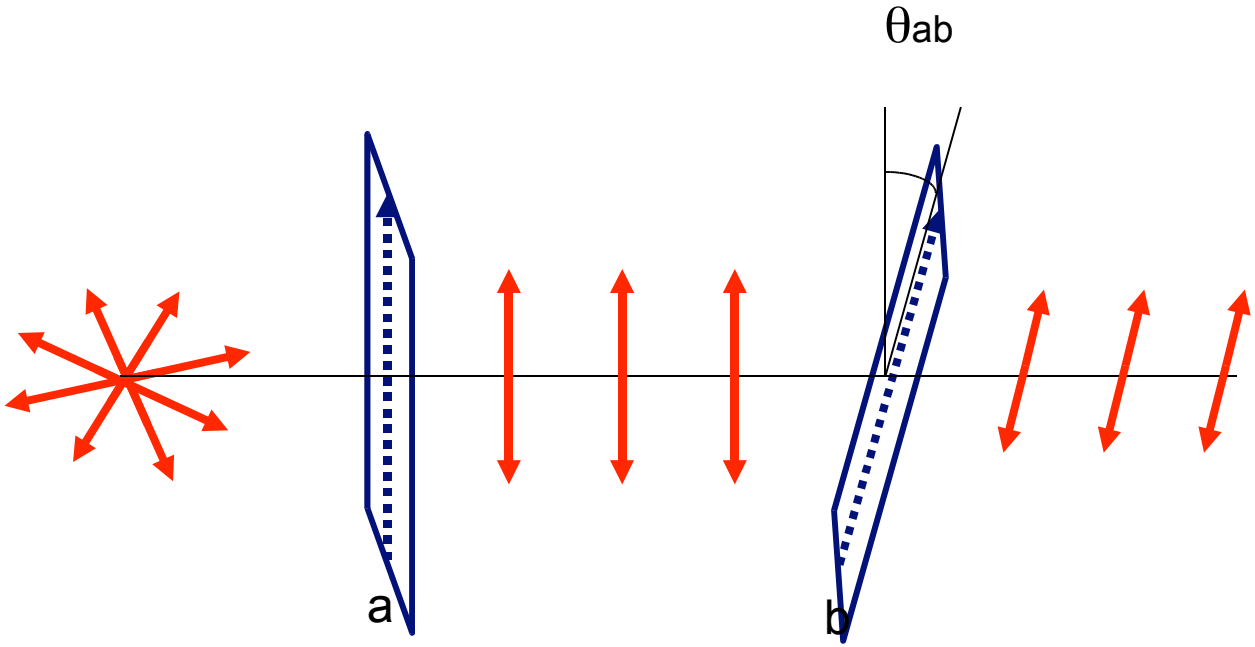


Per il principio di sovrapposizione è possibile ottenere vari stati di polarizzazione sovrapponendo un'onda verticalmente (a) e orizzontalmente (b) polarizzata:

(c), (d) Polarizzazione a -45° e 45°.

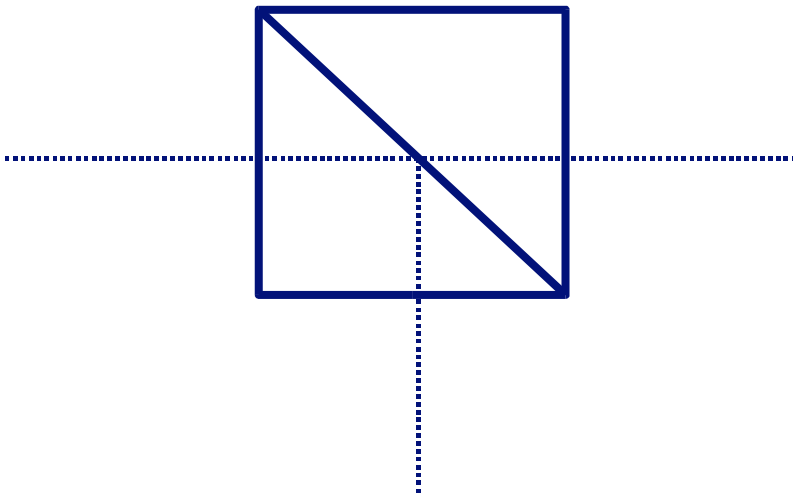
(e), (f) polarizzazione circolare destrorsa e sinistrorsa

il polarizzatore



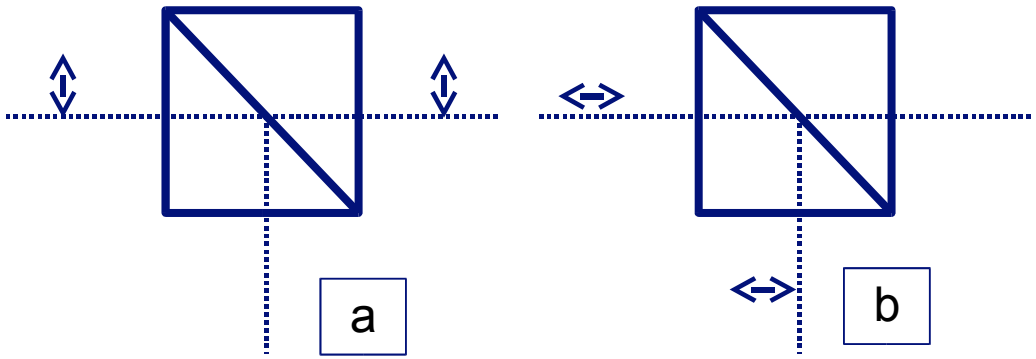
Un fascio luminoso non polarizzato attraversa un polarizzatore *a*. La luce che attraversa il polarizzatore è polarizzata lungo l'asse del polarizatore. Se viene inserito un secondo polarizzatore la luce trasmessa da *b* è meno intensa della luce trasmessa da *a* per un fattore $\cos^2\theta_{ab}$

50% beam splitters



un fascio luminoso incidente su un 50% beam splitter viene diviso in un fascio riflesso ed in un fascio trasmesso di uguale intensità

polarizing beam splitters



Polarizing Beam Splitter (PBS) con un asse verticale.

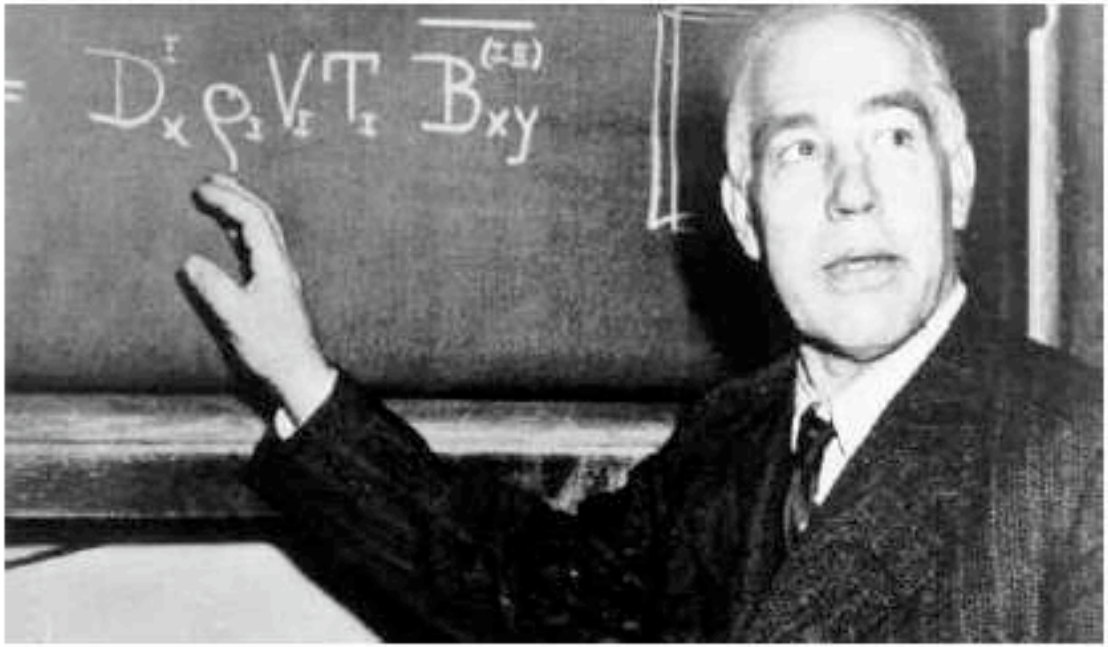
- La luce verticalmente polarizzata viene trasmessa (a)
- La luce orizzontalmente polarizzata viene riflessa (b)

Se un fascio luminoso di intensità *I* polarizzato ad un angolo θ rispetto alla direzione verticale incide su un PBS

- una frazione di intensità $I\cos^2\theta$ viene trasmessa mentre
- una frazione di intensità $I\sin^2\theta$ viene riflessa.

“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).

il fotone

- Quantisticamente la luce è descritta in termini di fotoni i.e. in termini di “particelle” indivisibili di massa nulla, ovvero in termini di “quanti di energia”, che si propagano a velocità *c*.
- L’intensità di un fascio luminoso è proporzionale al numero di fotoni nel fascio
- Ogni fotone ha una sua polarizzazione. In un fascio polarizzato tutti i fotoni hanno la stessa polarizzazione. In un fascio non polarizzato la polarizzazione dei fotoni è distribuita in modo random

ampiezze di probabilità

Lo stato di polarizzazione di un fotone viene definito in termini di “ampiezza di probabilità” rispetto ad una “base”

$|V\rangle$ fotone polarizzato verticalmente

$|H\rangle$ fotone polarizzato orizzontalmente

$|A\rangle = \alpha_V |V\rangle + \alpha_H |H\rangle$; con $(|\alpha_V|^2+|\alpha_H|^2=1)$

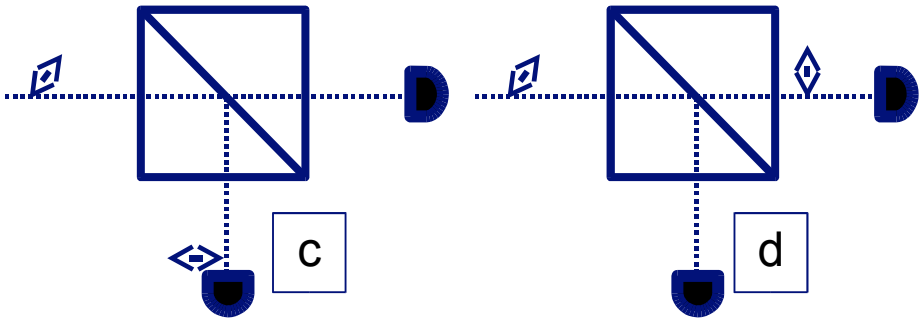
La scelta di base non è unica, esempio:

$|45°\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$; $|-45°\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$

e vice versa

$|H\rangle = (|45°\rangle + |-45°\rangle)/\sqrt{2}$; $|V\rangle = (|45°\rangle - |-45°\rangle)/\sqrt{2}$.

fotoni e polarizing beam splitters



Se un singolo fotone polarizzato ad un angolo θ incide su un PBS viene

- Trasmesso con probabilità $\cos^2\theta$
- Riflesso con probabilità $\sin^2\theta$

In entrambi i casi la polarizzazioe del fotone incidente cambia bruscamente. Questo è un esempio di misura quantistica proiettiva (o misura alla vonNeuman)

bennett & brassard 1984 (BB'84)

Alice sceglie una stringa random e codifica il bit di informazione in uno stato di polarizzazione

$$0 \rightarrow |V\rangle \; ; \; 1 \rightarrow |H\rangle$$

Il fotone viene inviato a Bob che lo misura nella base V/H

PROBLEMA: Eve può intercettare e misurare lo stato del fotone senza essere scoperta!

SOLUZIONE: Alice codifica i bit scegliendo in modo random tra le basi V/H (base (+)) o 45°, -45° (base(X)):

base (X): $0 \rightarrow |45°\rangle; \; 1 \rightarrow |-45°\rangle$
base (+): $0 \rightarrow |V\rangle; \; 1 \rightarrow |H\rangle$

BB’84

PROBLEMA: Bob non sa in che base misurare I fotoni inviati da Alice

SOLUZIONE: Bob sceglie in modo random tra le basi V/H (base (+)) o 45°, -45° (base(X)):

•Se le basi di Alice e di Bob coincidono, in assenza di Eve il bit misurato da Bob coincide con il codificato da Alice

•Se le basi di Alice e di Bob non coincidono, qualunque sia il bit inviato da Alice, Bob misura con uguale probabilità 0,1

BB’84: il protocollo (1)

ALICE

•Sceglie una sequenza random di basi, (+) or (×)

•Sceglie in modo random una stringa binaria. Tali bit sono codificati come 0 → V / +45°, 1 → H / -45° a seconda della base scelta

•I fotoni sono inviati a Bob attraverso un canale quantistico.

BOB

•Sceglie una sequenza random di basi, (+) or (×)

•Misura lo stato dei fotoni ricevuti da Alice nella base scelta

Alla fine di questo stadio Alice e Bob sono in possesso di due stringhe random che sono correlate nel 50% dei casi

BB’84: il protocollo (2)

ALICE

•Annuncia pubblicamente la sequenza di basi utilizzata per la codifica ma non i bit codificati

BOB

•Annuncia pubblicamente per quali bit della stringa la sua base di misura coincide con la base di Alice ma non il risultato della misura

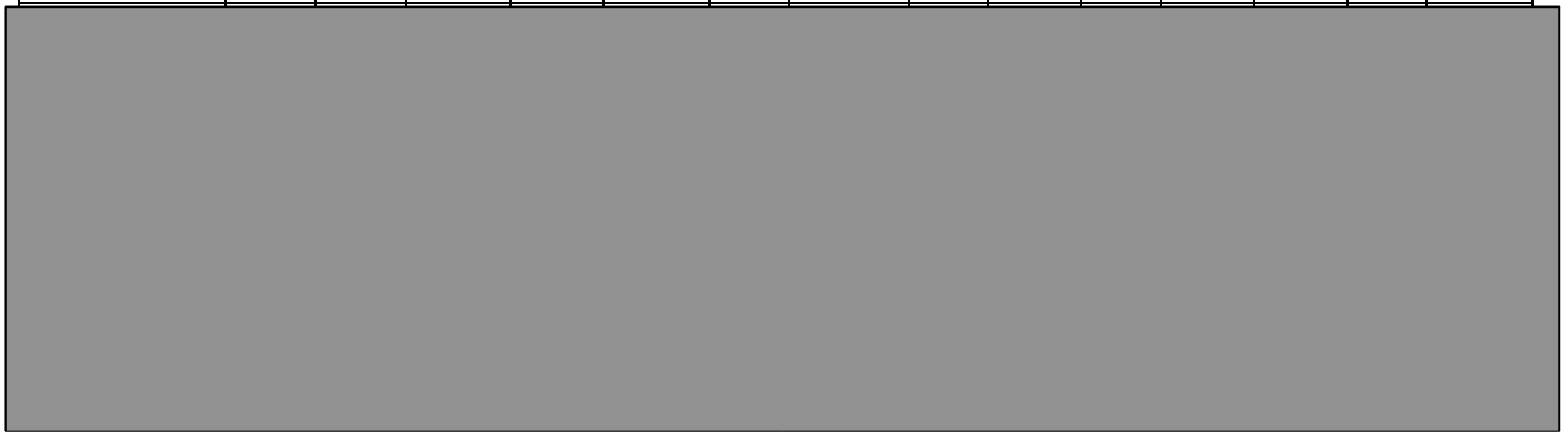
ALICE & BOB

•Scartano tutti i bit delle loro stringhe ogni qual volta le loro basi non coincidono

Alla fine di questo stadio Alice e Bob condividono una stringa, nota come chiave setacciata. In assenza di Eve le chiavi setacciate di Alice e di Bob coincidono

BB’84 – un esempio

Alice basis	+	+	×	+	×	+	×	+	+	+	×	+	×	×
Alice’s bits	1	0	0	1	1	0	0	0	1	0	0	1	0	1
Alice photons	H	V	45°	H	-45°	V	45°	V	H	V	45°	H	45°	-45°



BB’84 – un esempio

Alice basis	+	+	×	+	×	+	×	+	+	+	×	+	×	×
Alice’s bits	1	0	0	1	1	0	0	0	1	0	0	1	0	1
Alice photons	H	V	45°	H	-45°	V	45°	V	H	V	45°	H	45°	-45°
Bob’s basis	+	×	×	+	+	×	×	×	+	×	×	+	+	×

BB’84 – un esempio

Alice basis	+	+	×	+	×	+	×	+	+	+	×	+	×	×
Alice’s bits	1	0	0	1	1	0	0	0	1	0	0	1	0	1
Alice photons	H	V	45°	H	-45°	V	45°	V	H	V	45°	H	45°	-45°
Bob’s basis	+	×	×	+	+	×	×	×	+	×	×	+	+	×
Bob’s bits	1	0	0	1	0	1	0	1	1	1	0	1	0	1
Same basis?	Yes	No	Yes	Yes	No	No	Yes	No	Yes	No	Yes	Yes	No	Yes
Sifted key	1		0	1			0		1		0	1		1

BB’84: il protocollo (3)

ALICE & BOB

•Selezionano una sottostringa della chiave setacciata e confrontano pubblicamente il valore dei bit

•Effettuano una stima statistica della percentuale di errore (QBER = Quantum bit error rate)

•Confrontano il QBER con una soglia di sicurezza. Se il rumore è al di sotto del valore di soglia **correggono gli errori** ottenendo la “chiave riconciliata”

•Dalla chiave riconciliata **distillano** una chiave più corta segreta mediante un protocollo di **amplificazione di privacy**

•Se il QBER è al di sopra del valore di soglia rinunciano a stabilire una chiave segreta e ritentano in condizioni migliori

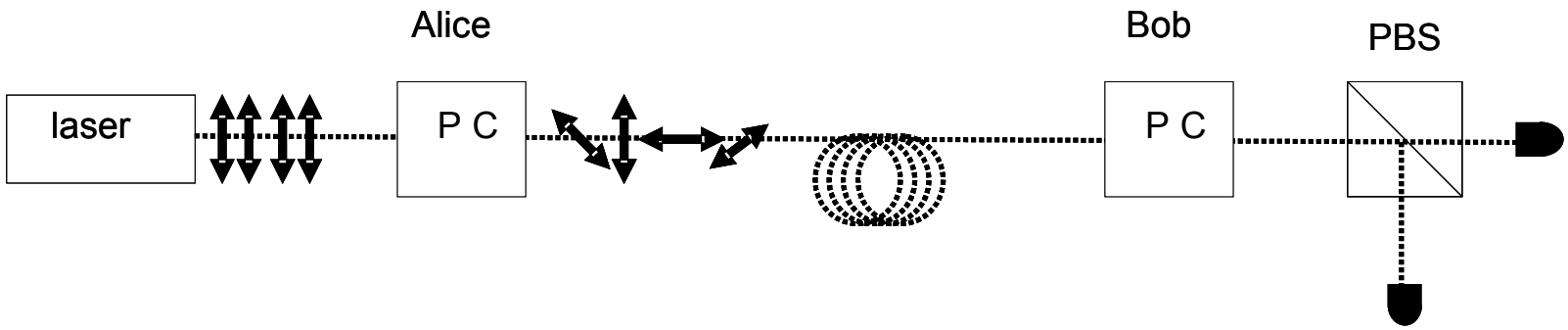
BB’84: commenti

•Il protocollo di quantum key distibution consente di distribuire chiavi crittografiche in modo sicuro, nel senso che consente di rivelare la presenza di Eve e di valutare se la stringa condivisa è segreta

•Il canale di comunicazione fra Alice e Bob deve essere autenticato in modo tale che Eve non finga di essere Bob con Alice e Alice con Bob

•Per l’autenticazione del canale è necessaria una breve chiave segreta. In questo senso abbiamo a che fare con un protocollo di accrescimento di chiave crittografica

BB’84 – schema sperimentale



Un laser emette una sequenza di impulsi a singolo fotone. Tramite una cella Pockels Alice ruota in modo random la polarizzazione del fotone. Bob sceglie in modo random la base di misura tramite una seconda cella Pockels ed un PBS

eavesdropping: intercept and resend

•La strategia più semplice per Eve è intercettare il fotone in transito, misurarlo e rispedirlo a Bob

•Eve non conosce la base di Alice, può solamente scegliere in modo random.

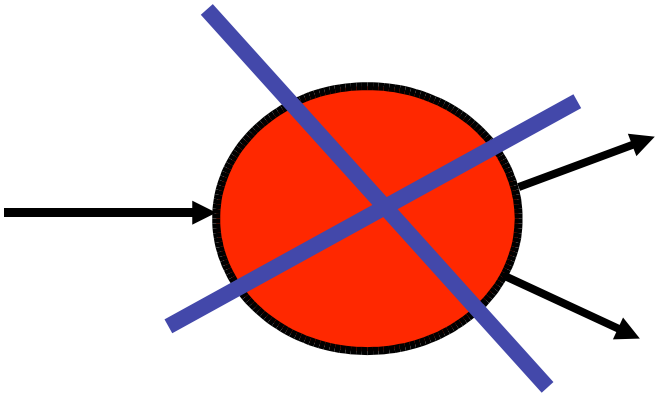
•**Eve misura nella base *corretta***, scopre il valore del bit in transito e invia a Bob un fotone nella corretta polarizzazione. Bob non può accorgersi della presenza di Eve. Il valore dei bit di Alice, Bob e Eve coincidono

•**Eve misura nella base *sbagliata***, non scopre il valore del bit in transito, manda a Bob un fotone nella base sbagliata. Il valore del bit di Eve e di Bob è scorrelato col valore del bit di Alice i.e. essi coincidono con probabilità del 50%.

•In generale confrontando il valore di un singolo bit Alice e Bob registrano un errore con una probabilità del 25%

no cloning

È impossibile fare una copia di un fotone in uno stato di polarizzazione sconosciuto



Questo è un caso particolare del teorema di NO CLONING

Eve non può fare una copia del fotone in transito, rispedire l'originale a Bob ed effettuare una misura sulla sua copia

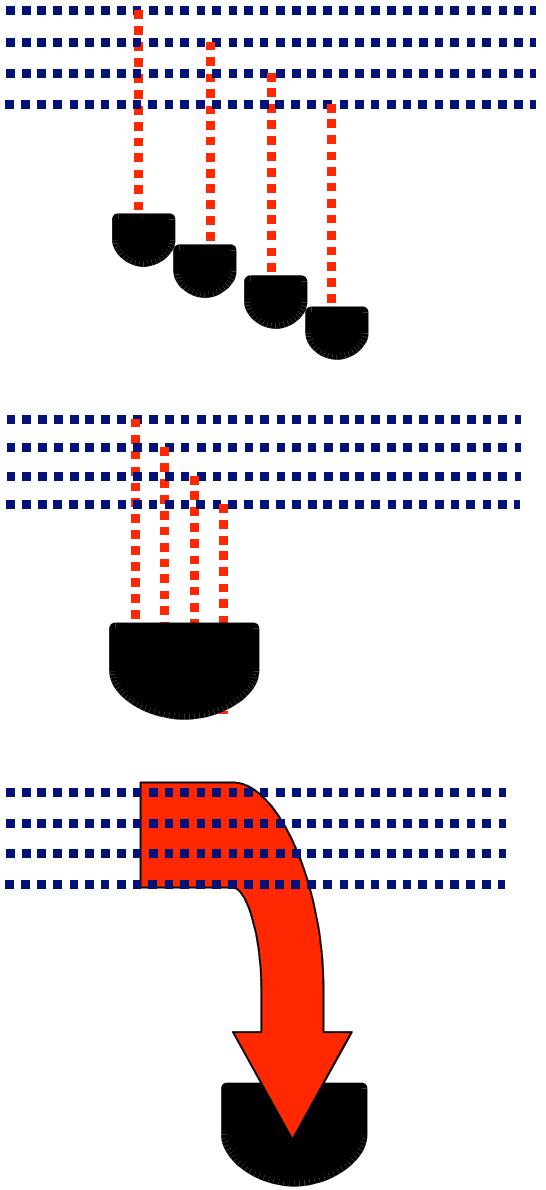
E' possibile fare delle copie approssimate, ma questo disturba lo stato originale

eavesdropping: strategie generali

ATTACCHI INDIVIDUALI: Eve fa interagire ognuno dei fotoni in transito con un suo probe che viene misurato individualmente

ATTACCHI COERENTI: Eve fa interagire ognuno dei fotoni in transito con un un suo probe e questi vengono misurati collettivamente

ATTACCHI CONGIUNTI: i fotoni in transito interagiscono collettivamente con un opportuno sistema ausiliario



eavesdropping: attacchi individuali

•Dopo aver effettuato le misure Alice, Bob ed Eve sono in possesso di tre stringhe di bit a,b,e descritte da una distribuzione congiunta di probabilità P(a,b,e)

•Alice e Bob possono stabilire una chiave crittografica segreta mediante amplificazione di privacy se la mutua informazione fra Alice e Bob è maggiore della informazione che Eve ha sulle stringhe di Alice o Bob

•Per il BB'84, nel caso di attacchi individuali, ciò è possibile per un QBER 15%

entanglement

Stato EPR (Einstein – Poldoski – Rosen)

$$|\psi\rangle = (|V\rangle_A|H\rangle_B - |H\rangle_A|V\rangle_B)\sqrt{1/2}$$

Una misura dello stato del fotone A modifica ISTANTANEAMENTE lo stato del fotone B !

Questo è vero IN QUALUNQUE BASE VENGA FATTA LA MISURA!!!

$$|\psi\rangle = (|N\rangle_A|N_\perp\rangle_B - |N_\perp\rangle_A|N\rangle_B)\sqrt{1/2}$$

ekert 91: il protocollo

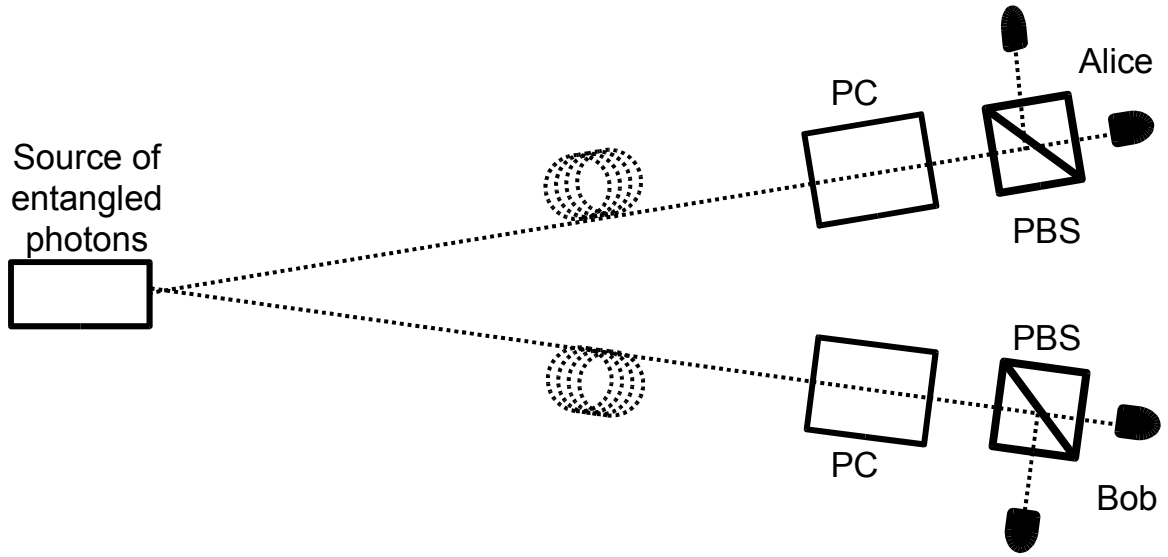
Versione “alla BB’84”

•Alice e Bob scelgono indipendentemente e in modo casuale di misurare ciascuno uno dei fotoni nello stato EPR nella base (+) o (x). Se le basi coincidono i risultati delle misure sono perfettamente (anti)correlati, se le basi sono differenti i risultati sono random e scorrelati. Il resto del protocollo è analogo al BB’84

Versione “alla Bell”

•Alice e Bob misurano la polarizzazione scegliendo in modo random *tre* basi non ortogonali differenti. I risultati delle misure fatte lungo basi non coincidenti non vengono scartati ma vengono utilizzati per fare un test della disuguaglianza di Bell i.e. per verificare che i due fotoni siano quantisticamente correlati (entangled)

ekert 91- schema sperimentale



Una sorgente emette coppie di fotoni entangled. Il primo fotone della coppia è spedito a Alice ed il secondo a Bob. Tramite celle Pockels e PBS essi eseguono misure di polarizzazione lungo direzioni random.

conclusioni

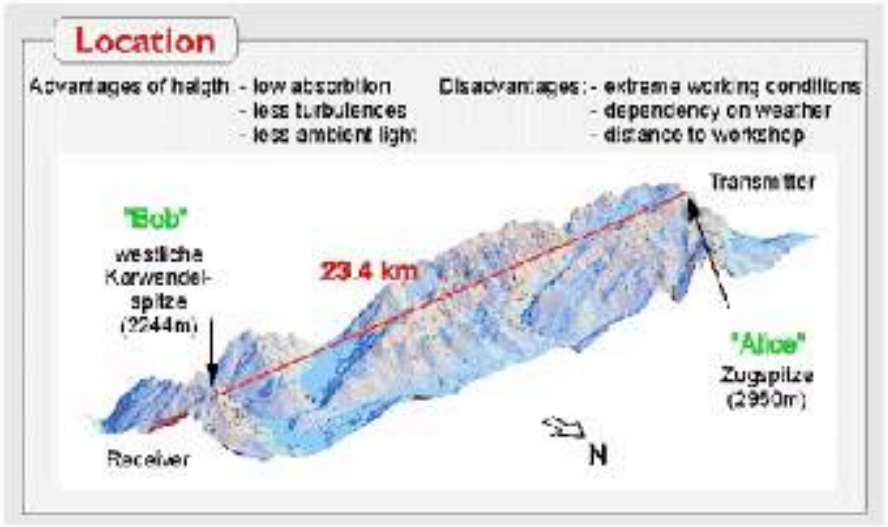
- L’uso congiunto di una codifica su sistemi quantistici e di protocolli classici consente la distribuzione di chiavi crittografiche anche se in presenza di eavesdroppers
- La crittografia quantistica non è fantascienza: esistono prototipi preindustriali operanti su fibra ottica su distanze dell’ordine di 60 – 100 Km

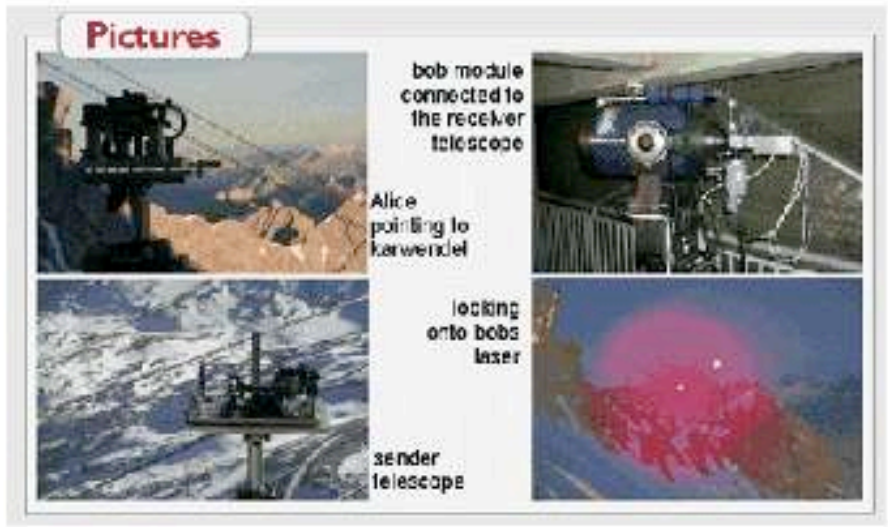
Esempi di implementazioni reali di QKD

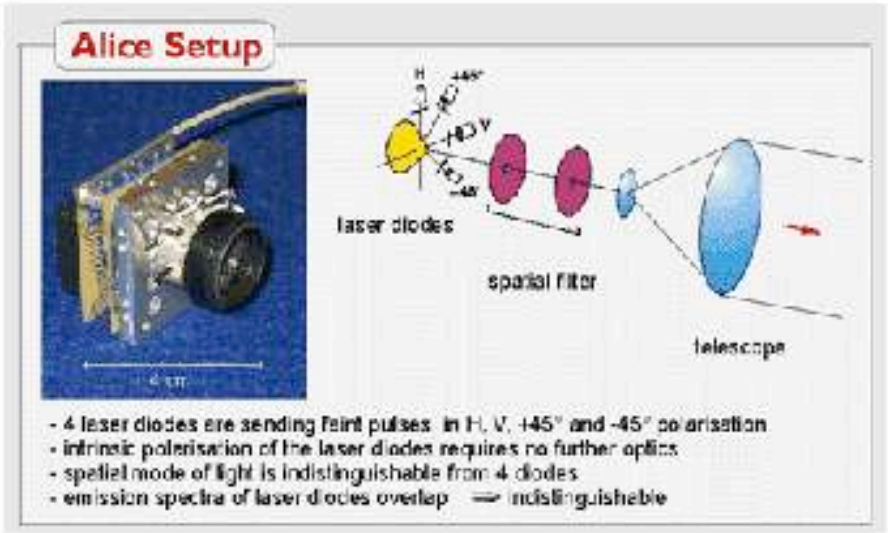
- Negli ultimi anni sono stati effettuati numerosi esperimenti di QKD. Ed ultimamente sono sorte anche delle aziende che producono dispositivi in grado di implementare un sistema QKD in fibra ottica interfacciandosi con una rete Ethernet per lo scambio delle informazioni sul canale pubblico.

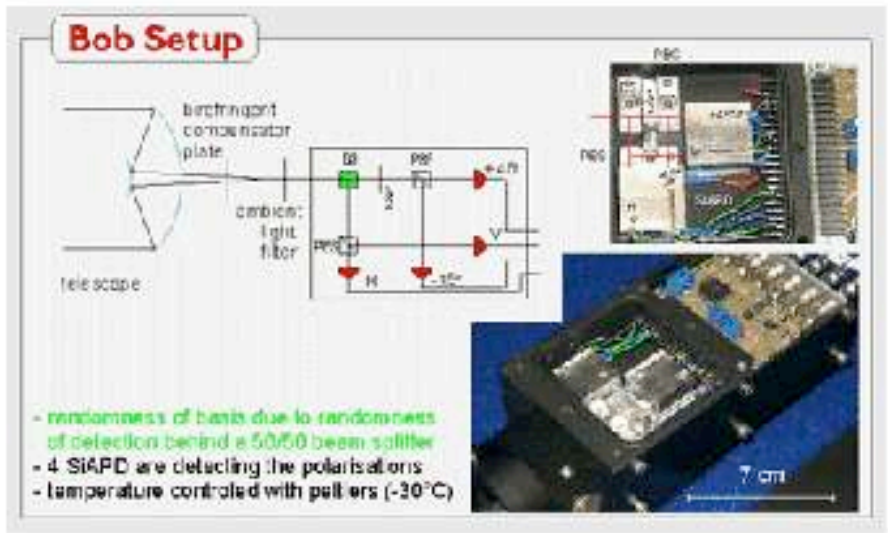
- Ad esempio nel 2001 presso il CERN di Ginevra è stato effettuato il primo esperimento di QKD tramite fibra ottica a lunga distanza (circa 67 Km lungo le linee standard della Swisscom).

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





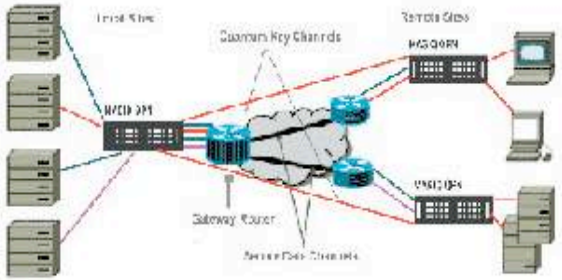




conclusioni

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.

sviluppi più recenti…

- **Quantum cryptography tackles video**
- 10 May 2005
- **Physicists at Toshiba have used quantum cryptography to transmit voice and video over a secure optical fibre link. The demonstration is significant because it shows that the single-photon encryption technology is compatible with real Internet Protocol (IP) traffic and also robust enough for deployment on commercial optical fibre networks. The system was shown to financial institutions and government representatives in London by Andrew Shields and colleagues from Toshiba Research Europe in Cambridge.**

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