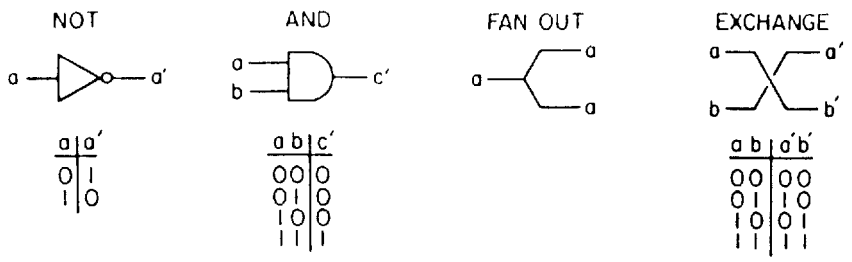
I gate quantistici

La Quantum Turing Machine introdotta da D. Deutsch svolge, nello studio dei calcolatori quantistici, un ruolo analogo a quello della macchina di Turing nella teoria classica della computazione. Essa costituisce infatti un modello di calcolo quantistico utile nell'analisi della complessità degli algoritmi ma poco maneggevole ai fini della realizzazione pratica di un calcolatore. Lo studio delle implementazioni si è di fatto sviluppato nel senso della scomposizione del calcolo in operazioni elementari che possano essere svolte coinvogendo un numero elementare di bit quantistici sottoposti a una classe ben determinata di trasformazioni unitarie. Si è in tal modo venuta a precisare l'idea di gate quantistico, concepito come l'analogo delle tradizionali porte logiche nei sistemi classici.

E' importante qui sottolineare le istanze pratiche e teoriche che motivano e giustificano la realizzazione di calcolatori fondati su reti di gate. L'esigenza pratica è quella di ridurre i supporti fisici del calcolo ad un insieme finito, standardizzato ed universale di dispositivi di bassa complessità realizzativa. Nel caso classico questo processo è stato portato a termine da alcuni decenni con la nascita delle famiglie di circuiti logici [Horowitz], che hanno stabilito uno standard *de facto* nella progettazione dei circuiti incoraggiandone il disegno "a blocchi" e permettendo l'abbattimento dei costi mediante la produzione su vasta scala. Perché questa tipizzazione sia possibile è daltronde necessario che si identifichino degli insiemi minimali di connettivi logici o, nel caso quantistico, operatori unitari che permettano di implementare efficientemente in un circuito qualunque funzione computabile nel modello di calcolo dato. Si tratta, in altri termini, di dimostrare che ogni macchina di Turing classica o quantistica è simulabile da un'appropriata rete di gate. Questo problema è stato affrontato,

Figura 6: Gate logici per il calcolo irreversibile e relative tavole di verità



come vedremo, con un certo successo anche per quanto riguarda il calcolo quantistico.

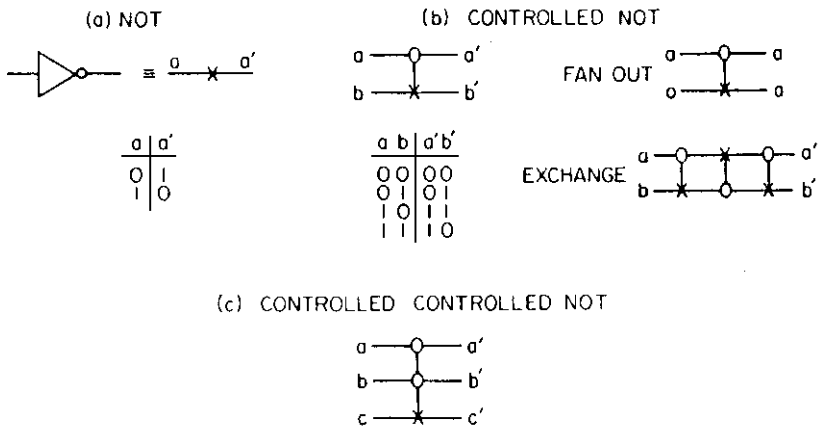
I gate classici reversibili

I computer che attualmente utilizziamo sono calcolatori universali costituiti da reti sufficientemente complesse di elementi primitivi, le porte logiche o gate, tra loro interconnessi. Seguendo l'usuale trattazione classica definiamo le interconnessioni come fili ideali che trasportano due valori standard di tensione che rappresentano i valori di verità 0 ed 1. Le sole porte logiche necessarie risultano essere il NOT e l'AND (Figura 6) che possono essere combinate nell'unico gate NAND[I], a due ingressi ed una uscita [Feynman]. In generale, quando i bit non sono rappresentati da valori di tensione, le interconnessioni rappresentano un problema non banale e devono logicamente essere considerate come un ulteriore gate, che chiameremo UNIT WIRE. Le funzioni di copia di un bit e di scambio tra due bit sono infine svolte dalle primitive logiche FAN OUT ed EXCHANGE.

Il gate NOT sopra introdotto è manifestamente reversibile, costituendo in effetti il proprio inverso. Il gate NAND, al contrario, è banalmente irreversibile in

[I] Un gate NAND (= NOT AND) è costituito da un AND seguito da un NOT. Quando uno degli ingresi è posto ad 1 l'uscita rappresenta la negazione dell'altro ingresso.

Figura 7: Gate logici reversibili e relative tavole di verità



quanto presenta un numero di linee di output inferiore al numero di linee di input, e non si presta quindi ad essere incluso in modelli di calcolo reversibile.

Una seconda primitiva reversibile di grande utilità è il CONTROLLED NOT, che presenta due ingressi, che chiameremo a e b, e due uscite, a' e b' (Figura 7). Il valore della linea a, o linea di controllo, viene sempre riportato inalterato su a'. Se il controllo è attivato (a=1) allora l'uscita b' (linea bersaglio) è la negazione di b (b'= NOT b); in caso contrario, b' contiene una copia di b. In altri termini, come si evince dalla tavola di verità, il valore di b' è a XOR b, ovvero la somma di modulo due di a e b, che vale 1 se e soltanto se a≠b. Notiamo tra l'altro che la funzione XOR non è di per sé reversibile, in quanto ad esempio la controimmagine dello zero contiene le due coppie (a,b)=(0,0) ed (a,b)=(1,1); la copia dell'ingresso a su a' risolve questa ambiguità. Indicheremo il CONTROLLED NOT, seguendo la notazione standard, con uno 0 sulla linea di controllo connesso mediante un tratto verticale ad una X sulla linea bersaglio. Questo gate svolge la funzione di FAN OUT, in quanto se l'ingresso b è posto a zero b' contiene una copia di a. Inoltre disponendo una sequenza di tre CONTROLLED NOT su un paio di linee in modo da alternare la linea di controllo si ottiene la funzione EXCHANGE, ovvero lo scambio del contenuto delle due linee.

Tabella 1: Tavola di verità del gate di Toffoli

a	*b*	*c*	*a'*	*b'*	*c'*
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

I gate NOT e CONTROLLED NOT non sono in realtà sufficienti ad implementare qualunque funzione logica reversibile: è necessario almeno un gate che operi su un numero superiore di linee. Il più comune è il gate di Toffoli, che presenta tre ingressi e tre uscite, ed è altrimenti denominato CONTROLLED CONTROLLED NOT (Figura 7 e Tabella 1). Esso presenta due linee di controllo a e b che compaiono inalterate nell'output e che cambiano il contenuto della terza linea da c a NOT c se e soltanto se sono enrambe attivate (a=b=1). Se l'ingresso della linea bersaglio è messo a zero (c=0), evidentemente avremo c'=1 se e soltanto se a e b sono entrambi 1. In tal modo, il gate di Toffoli realizza la funzione AND. Notiamo infine che ponendo l'ingresso a ad 1 e trascurando a' il gate si riduce ad un CONTROLLED NOT su b e c; ponendo poi anche b=1 e trascurando b' si ottiene un NOT sulla linea c. In ultima analisi l'insieme costituito dal solo gate di Toffoli, sorgenti di 0 ed 1 e fili unità permette di realizzare un circuito che calcoli qualunque funzione logica in modo reversibile. Il gate di Toffoli svolge perciò il ruolo di gate universale per il calcolo reversibile classico (il fatto che tale gate richieda molte più linee del NAND, la principale porta irreversibile, è probabilmente una delle principali ragioni per cui i gate irreversibili hanno avuto maggiore fortuna di quelli reversibili).

I gate quantistici

Passando ora ad una descrizione che più si attagli ad un sistema quantistico possiamo definire un gate [Deutsch2] come un dispositivo caratterizzato da una osservabile d'ingresso **I** e da una osservabile d'uscita **O**. I possibili ingressi corrispondono agli autostati di **I**; analogamente gli autostati di **O** generano lo spazio dei risultati. Sia C un sistema completo di osservabili per il gate, con $\mathbf{I} \in C$

(normalmente sarà anche $\mathbf{O} \in \mathcal{C}$, ma questo non è strettamente necessario). Il gate viene inizialmente preparato in uno degli autostati di I, o più in generale in una loro sovrapposizione, ed in un autostato standard di tutte le altre osservabili in $\mathcal{C}$. In seguito ad un'evoluzione che si assume richiedere un tempo costante il gate si arresta in uno stato complessivo determinato univocamente dall'ingresso. A questo punto, una misura dell'osservabile **O** fornisce informazioni sul risultato della computazione. In generale, comunque, anche l'evoluzione a partire da un autostato di **I** conduce ad una sovrapposizione degli autostati di **O**.

Supponiamo ora che gli autostati di **I** e di **O** corrispondano rispettivamente agli stati di base di un sistema di n bit quantistici in ingresso ed m bit in uscita. Se n=m, i bit in ingresso ed in uscita possono essere gli stessi oggetti fisici a tempi diversi, e le osservabili **I** ed **O** possono coincidere. In questo caso, le basi d'ingresso e d'uscita coincidono e prendono il nome di base computazionale. Possiamo pensare ai bit che passano attraverso il gate, ma il moto riguarda in realtà i loro portatori. In una rete complessa di gate, ad esempio, un bit potrebbe essere codificato nello stato di uno degli elettroni esterni di un atomo. Gli atomi portatori dei bit di ingresso verrebbero poi instradati verso il gate, dove gli elettroni subirebbero un'evoluzione congiunta; in seguito, gli atomi proseguirebbero verso altri gate. In questo processo i gradi di libertà computazionali sarebbero attivi solo all'interno dei gate, mentre gli spostamenti interesserebbero solo i gradi di libertà traslazionali dei portatori.

L'effetto di un gate logico reversibile su n bit, in questa descrizione, è di effettuare una permutazione dei 2^n stati della base computazionale dei bit che lo attraversano. Indichiamo ad esempio con $\{|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle\}$ i quattro stati della base computazionale dei due bit di ingresso del gate CONTROLLED NOT, rispettivamente bit di controllo e bit bersaglio. L'azione del gate può essere descritta come

$$\begin{cases} |0,0\rangle \rightarrow |0,0\rangle \\ |0,1\rangle \rightarrow |0,1\rangle \\ |1,0\rangle \rightarrow |1,1\rangle \\ |1,1\rangle \rightarrow |1,0\rangle \end{cases}$$

dove con $\rightarrow$ indichiamo "evolve in".

Una notazione alternativa consiste nell'indicare la trasformazione mediante la matrice

$$\mathbf{S} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

riferita alla base computazionale $\{|a,b\rangle\}$dei due bit, ovvero, anche con riferimento alle linee a-a' e b-b' della figura, $\mathbf{S}^{ab}_{a'b'} = \delta^{a}_{a'}\delta^{a\ \mathrm{XOR}\ b}_{b'}$.

La notazione matriciale può sembrare stravagante per un gate logico: le sole matrici ammissibili sono quelle che presentano uno ed un solo "1" su ogni riga e su ogni colonna. D'altra parte, il più generale gate quantistico è descrivibile con una matrice sulla base computazionale dei bit sui quali opera, col solo requisito che tale matrice sia unitaria. L'utilizzo della stessa notazione per i due tipi di gate costituisce però un procedimento euristico per la ricerca di gate universali quantistici. Il gate di Toffoli, ad esempio, è descritto dalla matrice

$$\mathbf{T}^{abc}_{a'b'c'} = \delta^{a}_{a'}\delta^{b}_{b'}\delta^{c\oplus ab}_{c'},$$

dove con c⊕ab indichiamo c XOR (a AND b). E' opportuno esprimere **T** nella forma

$$\mathbf{T}^{abc}_{a'b'c'} = \delta^{a}_{a'}\delta^{b}_{b'}\left[(1-ab)\delta^{c}_{c'} + ab\mathbf{N}^{c}_{c'}\right],$$

dove **N** è la matrice rappresentativa del gate NOT sulla base computazionale $\{|0\rangle,|1\rangle\}$dell'unico bit su cui esso agisce, ovvero

$$\mathbf{N} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Quest'ultima scrittura di **T** evidenzia come il gate di Toffoli agisca sulla linea c-c' come l'identità o come un gate NOT a seconda che a AND b valga zero od uno. Da questa espressione si costruisce, per analogia formale, il gate quantistico **Q** definito da

$$\mathbf{Q}^{abc}_{a'b'c'} = \delta^a_{a'}\delta^b_{b'}\left[(1-ab)\delta^c_{c'} + iab\,\mathrm{e}^{-\frac{1}{2}i\pi\alpha}\left(\mathbf{N}^\alpha\right)^c_{c'}\right]$$

dove α è un numero irrazionale fissato e

$$\mathbf{N}^\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^\alpha = \frac{1}{2}\begin{pmatrix} 1+\mathrm{e}^{i\pi\alpha} & 1-\mathrm{e}^{i\pi\alpha} \\ 1-\mathrm{e}^{i\pi\alpha} & 1+\mathrm{e}^{i\pi\alpha} \end{pmatrix}$$

rappresenta il gate NOT "elevato a potenza α". **Q** opera la trasformazione unitaria $\mathbf{N}^\alpha$ sul bit *c* se e soltanto se i due bit di controllo *a* e *b* valgono uno.

Il gate **Q** è stato ideato nel 1989 da D. Deutsch [Deutsch2], che ne ha dimostrato l'*universalità*: data qualunque trasformazione unitaria **U** esistono una successione $\{\mathbf{G}_n\}$ di reti composte da copie di **Q**, sorgenti di uni e di zeri e fili unità e una successione $\{\phi_n\}$ di angoli di fase tali che

$$\lim_{n\to\infty} \mathrm{e}^{i\phi_n}\,\mathbf{G}_n = \mathbf{U},$$

con l'ulteriore proprietà che ciascuna delle $\mathbf{G}_n$ sia un gate[I].

Nonostante la sua universalità il gate **Q** richiede però sul piano pratico il controllo dell'evoluzione congiunta di un sistema di tre bit, che appare di difficile attuazione. D. Di Vincenzo ha in seguito dimostrato, utilizzando gli strumenti forniti dalla teoria dei gruppi di Lie, che le reti di gate a due bit sono sufficienti,

[I] Una rete di gate non è, in generale, essa stessa un gate. Possono infatti esistere dei circuiti di feedback interni alla rete che la rendono instabile per qualche ingresso o che fanno in modo che l'uscita ad un dato istante dipenda non solo dall'ingresso a quell'istante, ma anche dalla storia dei valori d'ingresso precedenti.

congiuntamente al gate NOT, ad approssimare qualunque elemento del gruppo $U(2^3)$ e quindi, in virtù del risultato di Deutsch, la più generica trasformazione unitaria [DiVincenzo]. Questo risultato prescinde comunque da considerazioni di complessità riguardo il numero di gate effettivamente necessarî ed è fondato sull'ipotesi che si possa effettuare qualunque trasformazione unitaria su due bit, cosa che sembra difficile da realizzare praticamente.

Il tema della complessità è stato affrontato in un successivo articolo [DiVincenzo2] dallo stesso Di Vincenzo e da J. Smolin, che con tecniche di simulazione numerica hanno ricavato indicazioni sul fatto che il più generico gate a 3 bit possa essere approssimato da sei gate a 2 bit, anche questi però scelti arbitrariamente; D. Deutsch, A. Barenco e A. Ekert hanno in seguito stabilito che quasi tutti i gate a due bit sono universali [Deutsch3]. Un importante progresso sul problema dell'universalità è stato ottenuto da Bennett ed altri [Barenco] nel corso del Workshop on Quantum Computation tenutosi a Villa Gualino (Torino) nell'ottobre 1994. Essi hanno infatti dimostrato che la più generica trasformazione unitaria è implementabile con l'utilizzo del solo gate classico a due bit CONTROLLED NOT e di tutti i gate quantistici ad un bit[I]. Questo risultato è di grande importanza pratica in quanto esistono tecniche relativamente semplici, principalmente di ottica quantistica, per la realizzazione di qualunque trasformazione unitaria sul singolo bit e l'implementazione del gate CONTROLLED NOT.

Aspetti implementativi

La realizzazione di un calcolatore quantistico richiede, in ultima analisi, la capacità di effettuare trasformazioni unitarie su un singolo bit quantistico e di

[I] Notiamo che la presenza di almeno un gate a due bit è necessaria, in quanto una combinazione di gate ad un bit non potrà mai creare uno stato correlato di due o più bit.

attuare una *dinamica condizionata* di un insieme di due bit. Il gate CONTROLLED NOT, in effetti, altro non è che un dispositivo che applica ad un bit una trasformazione unitaria dipendente dallo stato dell'altro bit:

$$\mathbf{C-NOT} = |0\rangle\langle 0| \otimes \mathbf{Id} + |1\rangle\langle 1| \otimes \mathbf{NOT}.$$

Questa richiesta apparentemente semplice, tuttavia, maschera il complesso problema di selezionare esattamente di volta in volta i bit che devono subire l'interazione, per poi avviarli via via ad un nuovo gate come richiesto dall'algoritmo in esecuzione [DiVincenzo3]. In altri termini, i componenti classici più difficili da implementare in un circuito quantistico sono le piste conduttrici che connettono i piedini degli integrati sulle basette. Il motivo di questa difficoltà è evidente: i due bit che devono subire un'evoluzione congiunta devono essere sottoposti per un certo periodo di tempo, che in genere dovrà essere stabilito con precisione, ad una hamiltoniana di interazione che non interessi i bit adiacenti. D'altra parte, al passo successivo della computazione questa hamiltoniana microscopica dovrà interessare altri due bit, o ancora uno dei bit precedenti in congiunzione con una terza particella. Questo controllo finissimo dell'interazione costituisce una delle maggiori difficoltà sperimentali che in prospettiva si presentano, anche se già al momento esistono, come vedremo, alcune proposte per la sua soluzione.

L'altro problema fondamentale che il calcolo quantistico si trova ad affrontare è quello della decoerenza. L'inevitabile interazione del calcolatore quantistico, per quanto isolato, con l'ambiente circostante fa sì che la sua evoluzione non sia unitaria. Ciò comporta, in un tempo limitato, la perdita della coerenza nella sovrapposizione di stati in cui il calcolatore si viene a trovare. Questo fatto rappresenta un grosso impedimento al calcolo quantistico, in quanto possibili percorsi computazionali che si diramano all'inizio di una computazione possono interferire soltanto al termine della stessa, e fino a quel momento devono conservare inalterata la loro relazione di fase. Un parametro che risulta perciò

importante nella valutazione di quanto un sistema quantistico sia adatto ad essere utilizzato come calcolatore è rapporto tra il suo tempo di decoerenza t_Φ ed il "tempo di switching", ovvero il minimo intervallo di tempo richiesto da un gate per funzionare. Quest'ultimo può essere stimato basandosi direttamente sul limite fondamentale costituito dal principio di indeterminazione, che impone che esso sia maggiore di $\hbar/\Delta E$, dove ΔE è la separazione energetica tipica tra i due livelli del bit quantistico. Riportiamo di seguito una stima dell'ordine di grandezza di questi parametri per alcuni dei sistemi fisici che potrebbero, almeno in linea di principio, essere utilizzati [DiVincenzo3]:

Sistema quantistico	t_{switch} (s)	t_Φ (s)	Rapporto t_Φ/t_{switch}
Nucleo Mössbauer	10^{-19}	10^{-10}	10^{9}
Elettroni: GaAs	10^{-13}	10^{-10}	10^{3}
Elettroni: Au	10^{-14}	10^{-8}	10^{6}
Ioni intrappolati: In	10^{-14}	10^{-1}	10^{13}
Micro-cavità ottiche	10^{-14}	10^{-5}	10^{9}
Spin elettronico	10^{-7}	10^{-3}	10^{4}
Quantum dot elettronico	10^{-6}	10^{-3}	10^{3}
Spin nucleare	10^{-3}	10^{4}	10^{7}

A causa delle grandi differenze nella scala delle energie coinvolte, i tempi richiesti per un calcolo elementare variano su sedici ordini di grandezza. D'altra parte, non tutti questi sistemi risultano al momento utilizzabili: se ad esempio la tecnologia necessaria ad orientare gli spin nucleari in un campo magnetico mediante campi a radiofrequenza è già stata ampiamente sviluppata nell'ambito degli studi sulla NMR, la spettroscopia a raggi gamma che sarebbe necessaria per controllare le transizioni di nuclei Mössbauer è al momento inesistente. Inoltre, il particolare meccanismo utilizzato per realizzare ad esempio l'accoppiamento fra i vari bit può limitare la velocità di esercizio del calcolatore. Nel caso degli ioni intrappolati, l'utilizzo dei gradi di libertà fononici per realizzare una sorta di

"bus" interno al calcolatore limiterebbe il tempo di switching a 10^{-5} s anziché 10^{-14} s.

Analizziamo nel seguito in qualche dettaglio due delle tecnologie che appaiono, in prospettiva, più adatte per l'implementazione del calcolo quantistico.

Calcolo "in dimensione zero"

Una delle tecnologie attualmente più promettenti per la realizzazione di un calcolatore quantistico è quella dei *quantum dot* elettronici che costituiscono, almeno idealmente, un ponte gettato tra la regolarità dei fenomeni su scala atomica e la versatilità della tecnologia dei semiconduttori.

A temperatura ambiente, ovvero ad energie dell'ordine del quarantesimo di elettronvolt, la lunghezza d'onda tipica di un elettrone nel vuoto è circa 20 angstrom. Confinare l'elettrone ad un punto, perciò, significa restringerlo a muoversi in un cubo di 10 angstrom di lato (due volte il raggio di Bohr). All'interno di un semiconduttore, per effetto del potenziale degli atomi del reticolo, le onde elettroniche si propagano con una massa efficace che è circa un decimo della massa dell'elettrone (7% nell'arseniuro di gallio, 14% nel silicio); di conseguenza, un elettrone di conduzione costretto in una regione di semiconduttore di 100 angstrom di lato è sostanzialmente confinato ad un punto. Tale regione prende quindi il nome di *quantum dot*. Sotto molti aspetti, questo non è altro che un "atomo artificiale" del quale è possibile progettare ed eventualmente variare nel tempo la struttura (discreta) dei livelli energetici e la forma delle funzioni d'onda [Reed].

Sovrapponendo una griglia di elettrodi ad un *quantum well*, nel quale gli elettroni sono confinati in un piano, è possibile realizzare un reticolo di *quantum dot* che rappresenti l'analogo di un cristallo. Strutture di questo tipo, contenenti fino a 10^6 "atomi", sono state realizzate allo Stuttgart Max Planck Institute, alla

IBM ed alla AT&T. Esse si prestano, in prospettiva, alla realizzazione di un calcolatore quantistico, essendo possibile realizzare una dinamica condizionata di coppie di elettroni localizzati in siti adiacenti[I] [Ekert3].

Un *quantum dot* che sia più lungo in una direzione, che diremo *x*, rispetto alle direzioni perpendicolari può essere approssimato, a basse energie, come una buca di potenziale unidimensionale. Ai fini della computazione è sufficiente limitarsi a considerare i primi due livelli energetici, che indicheremo con $|0\rangle$ ed $|1\rangle$. In questi due stati la distribuzione di carica è simmetrica rispetto al centro della buca (Figura 8, riquadro A); tuttavia, in presenza di un campo elettrostatico esterno nella direzione *x*, la distribuzione di carica dello stato fondamentale e del primo livello eccitato risultano spostate rispettivamente nella direzione del campo e nella direzione opposta (*quantum confined Stark effect;* Figura 8, riquadro B). Diremo *attivato* un *quantum dot* così polarizzato ed indicheremo con $\pm d$ il suo momento di dipolo nello stato $|0\rangle$ od $|1\rangle$; realisticamente, *d* potrà variare da un *dot* all'altro.

In una coppia di *quantum dot* attivati ciascun elettrone risente del campo di dipolo del *dot* vicino, che ne modifica i livelli energetici ([Cohen], [Barenco2]). L'hamiltoniana complessiva

$$\mathcal{H}=\mathcal{H}_1+\mathcal{H}_2+\mathcal{V}_{12}$$

è la somma dell'hamiltoniana libera $\mathcal{H}_1+\mathcal{H}_2$ dei due *dot* e del termine $\mathcal{V}_{12}$ di interazione dipolo-dipolo. L'azione della prima sui propri autostati non degeneri $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$ è data da

$$\left(\mathcal{H}_1+\mathcal{H}_2\right)\left|\varepsilon_1\right\rangle\left|\varepsilon_2\right\rangle=\hbar\left(\varepsilon_1\omega_1+\varepsilon_2\omega_2\right)\left|\varepsilon_1\right\rangle\left|\varepsilon_2\right\rangle$$

[I] Per questi reticoli di *quantum dot* Norman Margolus del M.I.T. ha coniato il nome di *"crayonium"*.

con $\varepsilon_1, \varepsilon_2 \in \{0,1\}$; ω_1 ed ω_2 sono qui le frequenze risonanti per la transizione dei singoli elettroni dallo stato $|0\rangle$ allo stato $|1\rangle$ quando i *dot* vicini non sono attivati.

L'effetto del termine di interazione $\mathcal{V}_{12}$ può al primo ordine essere valutato calcolandone gli elementi diagonali sulla base degli autostati dell'hamiltoniana libera:

$$\langle \varepsilon_1, \varepsilon_2 | \mathcal{V}_{12} | \varepsilon_1, \varepsilon_2 \rangle = (-1)^{\varepsilon_1 + \varepsilon_2} \hbar \varpi$$

con

$$\varpi = -\frac{d_1 d_2}{4\pi\varepsilon_0 R^3},$$

dove d_1 e d_2 rappresentano il momento di dipolo rispettivamente del primo e del secondo *dot* ed R è la distanza fra questi nel reticolo. La frequenza corrispondente alla transizione di uno degli elettroni in una coppia di *dot* attivati dipende perciò, grazie all'interazione dipolo-dipolo, anche dallo stato dell'altro elettrone, e per il primo *dot* diviene $\omega_1 - \varpi$ o $\omega_1 + \varpi$ a seconda che l'altro si trovi nello stato $|0\rangle$ od $|1\rangle$ rispettivamente. Analogamente, la frequenza risonante del secondo *dot* diviene $\omega_2 \pm \varpi$ in funzione dello stato del primo (Figura 9).

L'effetto descritto può essere sfruttato per effettuare del calcolo quantistico coerente, illuminando i *dot* con opportuni impulsi di luce infrarossa sintonizzati su una delle quattro frequenze $\omega_1 \pm \varpi$ o $\omega_2 \pm \varpi$. Un impulso di durata ed intensità adeguate a fare transire l'elettrone di un *dot* da $|0\rangle$ ad $|1\rangle$ è detto impulso π per quel *dot*, e corrisponde all'azione di un gate NOT. Se sintonizzato sulla frequenza $\omega_2 + \varpi$, esso è sufficiente ad effettuare una operazione di CONTROLLED-NOT tra due *dot* adiacenti attivati, dei quali il primo rappresenta il bit di controllo mentre il secondo il bit bersaglio. La frequenza di transizione di quest'ultimo è, come abbiamo visto, $\omega_2 + \varpi$ soltanto se il primo *dot* si trova nello stato $|1\rangle$. L'effetto dell'impulso π sul bit bersaglio è pertanto, in questo caso,

quello di un gate NOT, mentre se il bit di controllo si trova nello stato $|0\rangle$ il secondo *dot* non viene influenzato.

La dinamica condizionata di coppie di *dot* può essere sfruttata per trasferire un bit quantistico di informazione lungo una catena di siti adiacenti, realizzando in tal modo un analogo dei fili di interconnessione classici. Il circuito così ottenuto avrebbe un aspetto "plastico", essendo definito istante per istante dalle tensioni applicate alla griglia di controllo e dagli impulsi laser, che potrebbero essere pilotati da un calcolatore classico. Notiamo inoltre che questo schema, oltre a rendere possibile il parallelismo quantistico, si presta anche all'implementazione di un parallelismo abbastanza spinto di tipo tradizionale, essendo in generale possibile attivare simultaneamente più *dot* o coppie di *dot* per eseguire su di essi operazioni indipendenti.

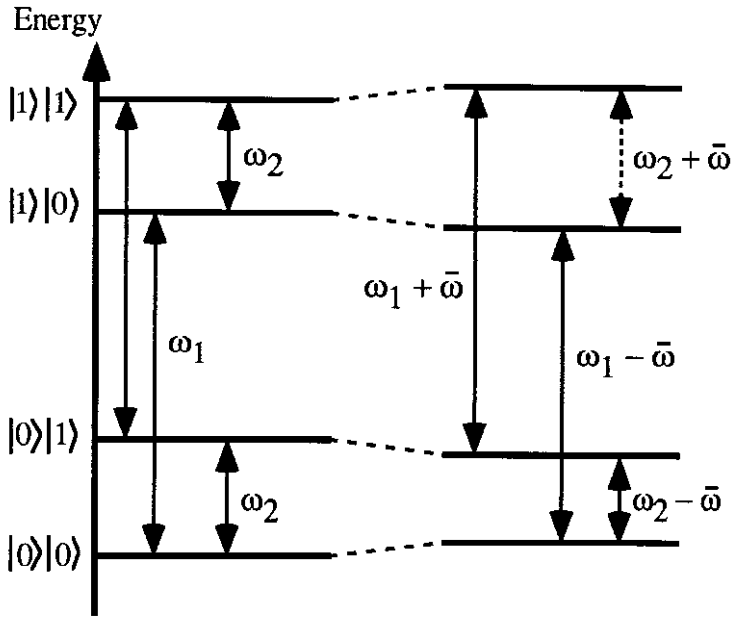


Figura 9: Effetto dell'interazione dipolo-dipolo sui livelli energetici di due dot adiacenti attivati.

Il calcolatore a ioni intrappolati

Una tecnologia attualmente abbastanza sviluppata, che potrebbe in futuro essere utilizzabile per il calcolo quantistico, è quella della manipolazione degli stati di ioni intrappolati ([Haroche], [Walther], [Castin]).

Gli esperimenti sono in genere compiuti utilizzando ioni di berillio o indio preparati mediante bombardamento elettronico di atomi neutri provenienti da un forno. Essi vengono intrappolati mediante un campo elettromagnetico a radiofrequenza (11 Mhz) e raffreddati mediante un fascio laser (raffreddamento Doppler) fino a temperature dell'ordine dl milliKelvin. La trappola, di dimensioni lineari inferiori ai 5 mm, è montata all'interno di una camera ad ultra-alto vuoto. Con una pressione del gas residuo dell'ordine di 10^{-10} mbar, il tempo di confinamento ottenibile è di alcune ore. E' possibile mantenere nella stessa trappola un certo numero di ioni, che sotto l'effetto combinato della repulsione coulombiana e del campo a radiofrequenza si organizzano a formare strutture ordinate (lineari, planari o anche tridimensionali, a seconda del numero degli ioni e del campo utilizzato per intrappolarli), la cui osservazione è direttamente possibile eccitando la fluorescenza degli ioni mediante luce laser [Walther]. Queste strutture possiedono dei gradi di libertà vibrazionali la cui energia può essere controllata con tecniche di raffreddamento laser.

Vediamo ora come una struttura lineare di ioni intrappolati possa, in linea di principio, essere utilizzata per implementare il calcolo quantistico [Costantini]. Il potenziale che confina il singolo ione può essere schematizzato come un potenziale armonico tridimensionale, in generale anisotropo. Tale anisotropia può essere sfruttata per fare in modo che lo ione, a bassa energia, si comporti come un oscillatore unidimensionale lungo una direzione privilegiata nella quale si suppone siano allineati tutti gli ioni costituenti il calcolatore. L'interazione

coulombiana tra gli ioni causa, come accennato, un accoppiamento fra i vari oscillatori, dando origine a modi vibrazionali della struttura nel suo insieme. Ad energie sufficientemente basse, gli unici livelli vibrazionali accessibili sono quelli del modo fondamentale, quello che comporta l'oscillazione del centro di massa.

Dal punto di vista della struttura elettronica degli ioni i livelli che qui ci interessano sono sostanzialmente tre: il livello fondamentale, che indicheremo con S, e due livelli eccitati P e D (Figura 10) tali che le transizioni S↔D abbiano una vita media molto superiore alle transizioni S↔P (per esempio rispettiva-mente 10 - 100s e 10^{-7} s). La presenza di due livelli con queste caratteristi-che è tipica degli elementi alcalini. Il livello D, a causa della sua maggiore stabilità, può essere utilizzato per rappresentare assieme al livello S uno degli stati del bit quantistico. Le transizioni al livello P si prestano invece ad essere sfruttate per leggere irreversibilmente lo stato del bit al termine della computazione, nonché per il raffreddamento degli ioni. Le transizioni S↔D ed S↔P sono eccitabili separatamente mediante l'uso di fasci laser di frequenza e polarizzazione opportune, fissate le quali ogni ione può essere considerato un sistema a due stati che indicheremo con $|g\rangle$ (lo stato S) ed $|e\rangle$ (di volta in volta lo stato P o lo stato D).

Gli stati del sistema complessivo degli *N* ioni nella trappola possono perciò

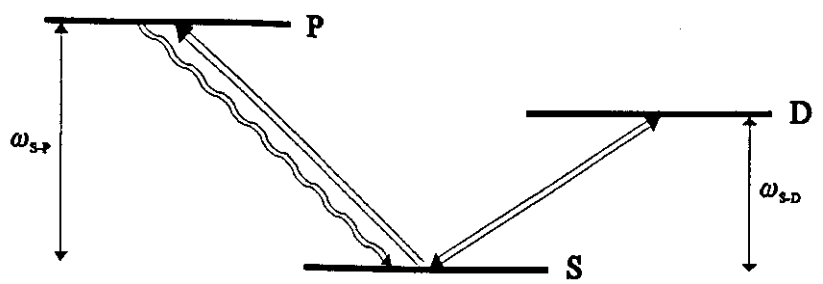


Figura 10: Struttura dei livelli elettronici di uno ione rilevanti ai fini della computazione.

essere sviluppati sulla base

$$\left\{|g\rangle_1, |e\rangle_1\right\} \otimes \left\{|g\rangle_1, |e\rangle_1\right\} \otimes \ldots \left\{|g\rangle_N, |e\rangle_N\right\} \otimes \left\{|0\rangle, |1\rangle, |2\rangle, \ldots, |n\rangle, \ldots\right\}$$

dove con $|0\rangle$, $|1\rangle$, $|2\rangle$, ..., $|n\rangle$, ... indichiamo i livelli vibrazionali di energia $E_n = \hbar\nu n$ del modo fondamentale, che supponiamo siano i soli energeticamente accessibili.

Puntando su ogni ione un laser differente è possibile fare in modo che ciascuno di essi interagisca separatamente col campo elettromagnetico (per le distanze tipiche tra gli ioni, dell'ordine dei 10 micron, questo è al presente fattibile). L'idea fondamentale è quella di regolare opportunamente la frequenza della radiazione in modo da eccitare transizioni nello spazio

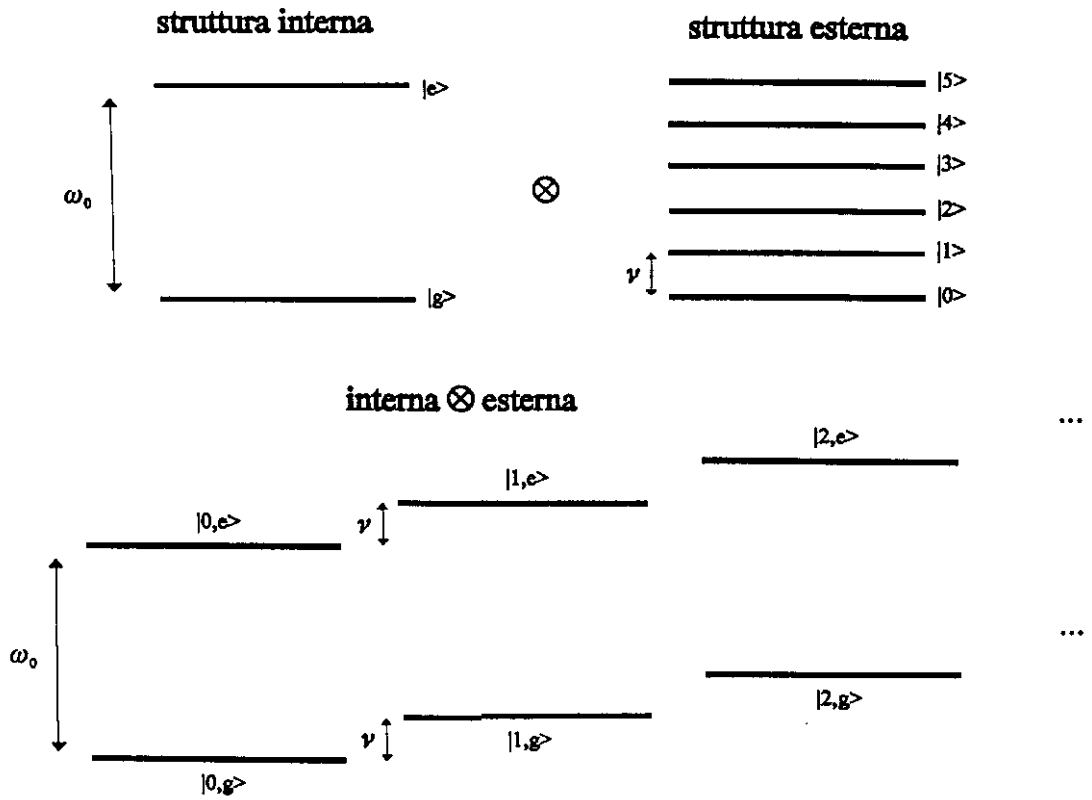
$$\left\{|g\rangle_i, |e\rangle_i\right\} \otimes \left\{|0\rangle, |1\rangle, |2\rangle, \ldots, |n\rangle, \ldots\right\}$$

prodotto degli stati interni dello ione *i*-esimo e dei livelli vibrazionali dell'intera struttura (Figura 11). Il moto collettivo di quest'ultima risulta perciò correlato con lo stato del bit *i*-esimo; questo fatto può essere sfruttato per ottenere una dinamica condizionata di tale bit e di uno qualunque dei rimanenti, e realizzare così dei gate quantistici. Il modo vibrazionale viene pertanto a svolgere un ruolo di interconnessione e trasporto dell'informazione analogo a quello svolto dal *"bus"* in un calcolatore classico.

Per chiarire come sia possibile, agendo sul singolo ione, modificare lo stato vibrazionale dell'intera struttura riportiamo qui le hamiltoniane che governano l'interazione col campo elettromagnetico nel caso in cui il fascio laser sia sintonizzato sulla frequenza di risonanza ω_0, sulla banda laterale inferiore $\omega_0 - \nu$ (*lower sideband, LSB*) o sulla banda laterale superiore $\omega_0 + \nu$ (*upper sideband, USB*):

$$\mathbf{H}_R = \frac{\Omega}{2}\left(\sigma^+ + \sigma^-\right)$$

Figura 11: Le transizioni avvengono nello spazio prodotto degli stati elettronici di un singolo ione e degli stati vibrazionali dell'intera struttura.



$$\mathbf{H}_{LSB} = -i\eta\frac{\Omega}{2}(\sigma^{+}\,a+\sigma^{-}\,a^{*})$$

$$\mathbf{H}_{USB} = -i\eta\frac{\Omega}{2}(\sigma^{+}\,a^{*}+\sigma^{-}\,a)$$

dove con a* ed a indichiamo gli operatori di costruzione e distruzione dei fononi del modo fondamentale, con $\sigma^{+} \equiv |e\rangle\langle g|$ e $\sigma^{-} \equiv |g\rangle\langle e|$ gli analoghi operatori per la struttura interna dello ione interessato, con Ω la frequenza di Rabi e con η una costante. Se il fascio laser ha durata ed intensità opportune (π-*pulse*) queste hamiltoniane producono transizioni tra gli stati illustrati in figura 11; impulsi di altro tipo permettono inoltre di realizzare sovrapposizioni coerenti degli stati interessati dalla transizione.

Ricordiamo infine che gli ioni intrappolati sono attualmente utilizzati per stabilire gli standard di frequenza, impiego che costituisce una delle principali motivazioni per un ulteriore sviluppo della tecnologia e che appare connesso con alcuni aspetti del calcolo quantistico, in particolare con gli algoritmi di correzione d'errore. Questi ultimi prospettano, infatti, la possibilità di preservare la coerenza di uno stato quantistico per un tempo virtualmente illimitato, cosa che costituirebbe un vantaggio decisivo nello stabilire standard di frequenza più precisi.

La crittografia quantistica

L'arte della crittografia risale ad almeno 2500 anni or sono, e fino dalla sua nascita ha avuto un ruolo importante nello svolgersi degli avvenimenti della storia. E' ben nota, ad esempio, l'importanza che ebbe nel secondo conflitto mondiale la capacità degli alleati di decodificare, ad insaputa di questi, i messaggi di Tedeschi e Giapponesi. Le complesse problematiche connesse con la codifica e la decodifica di messaggi hanno affascinato generazioni di matematici, mentre l'importanza strategica della criptoanalisi ha costituito una potente spinta per lo sviluppo dei moderni calcolatori.

La sempre crescente richiesta di tecniche crittografiche sicure ed efficienti che ha caratterizzato il nostro secolo è chiaramente da collegarsi alla nascita delle telecomunicazioni su larga scala. L'invenzione stessa della radio è emblematica di come il potenziamento delle comunicazioni abbia comportato l'adozione di canali fisicamente molto vulnerabili all'ascolto non autorizzato. Ultimamente, la diffusione delle reti di calcolatori ha esteso l'interesse per la crittografia dagli utenti tradizionali, i corpi diplomatici e le forze armate, al grande pubblico degli utilizzatori di risorse telematiche. In particolare la scelta delle compagnie commerciali di adottare o meno un uso massiccio delle reti, scelta dalla quale può dipendere il futuro delle telecomunicazioni e la realizzabilità del "villaggio globale", appare dipendere dalle garanzie di riservatezza che tali mezzi di comunicazione sono in grado di offrire.

La protezione dell'informazione nel suo trasferimento da un mittente ad un destinatario o nella sua archiviazione è affrontabile lungo due direttrici, la crittografia e la protezione fisica dei canali, che sono, come vedremo, variamente correlate tra loro. La seconda alternativa sembra intuitivamente preferibile alla prima, in quanto si può a priori ritenere che un cifrario, per quanto raffinato,

possa venire forzato, mentre i limiti imposti dalle leggi fisiche alle modalità di osservazione di un segnale sembrano intrinsecamente invalicabili. Tuttavia questo tipo di garanzia è, nel caso classico, molto difficile ad ottenersi e non va confuso con l'assunzione, da parte di mittente e destinatario, che il terzo partito disponga di una tecnologia limitata. Un esempio tipico è quello delle trasmissioni radio. Esiste indubbiamente un limite nella potenza irradiata al di sotto del quale è praticamente impossibile la ricezione di una trasmissione. Tuttavia, trasmettere a bassa potenza non potrebbe essere considerata una valida protezione se non nell'ipotesi, difficile da giustificare, che nessun ascoltatore indesiderato disponga di un ricevitore di sensibilità equivalente a quello del legittimo destinatario del messaggio (come vedremo, una assunzione analoga è alla base della supposta sicurezza di uno degli algoritmi crittografici più in uso). In un caso particolare, però, si può ottenere una garanzia *fisica* della sicurezza del canale. Questo accade quando la frequenza di trasmissione scelta è in corrispondenza della risonanza di uno dei modi vibrazionali delle molecole d'acqua presenti nell'atmosfera (circa 60 GHz). In tal caso lo smorzamento della radiazione è esponenziale e si può assumere con sicurezza che nessuno, al di fuori di un raggio di alcuni chilometri, possa captare la trasmissione (questo accorgimento viene utilizzato per la comunicazione tra navi da guerra in navigazione).

Questo tipo di sicurezza intrinseca, come è evidente, può essere ottenuto solo in condizioni del tutto particolari. La crittografia quantistica si occupa appunto dello sviluppo di protocolli crittografici la cui sicurezza sia garantita direttamente dalle leggi della fisica, con particolare riferimento al principio di indeterminazione. L'utilizzo di sistemi quantistici, integrato con alcuni risultati della crittografia classica esposti nella seguente sezione, sembra in effetti garantire la possibilità di una comunicazione inviolabile.

Cenni di crittografia classica

Gli Spartani, attorno al 400 a.C., impiegavano un ingegnoso sistema di codifica per le comunicazioni militari. Il messaggio da trasmettere veniva scritto su una striscia di pelle avvolta a spirale attorno ad un bastone cilindrico (lo *scìtale*) seguendo la direzione dell'asse del bastone, in modo che ogni lettera cadesse su una spira differente. La striscia srotolata, che era inviata a destinazione, conteneva così una permutazione dei caratteri del testo in chiaro. Il ricevente, avuto il nastro, decrittava il messaggio riavvolgendolo su un bastone di eguale diametro. Giulio Cesare, dal canto suo, affidava la segretezza della sua corrispondenza alla sostituzione di ogni lettera con la successiva. Questi due algoritmi, trasposizione e sostituzione, compaiono variamente combinati alla base di molti cifrari odierni.

In principio, la sicurezza del sistema era in generale fondata sulla segretezza dell'intero procedimento di codifica e di decodifica. Tuttavia già nell'algoritmo usato dagli Spartani interviene un parametro, il diametro del bastone, ignorando il quale è per lo meno più complicato decrittare un messaggio, pur conoscendo il procedimento da utilizzare. Nei cifrari odierni, in effetti, l'algoritmo di codifica è pubblico e spesso standardizzato, per garantirne la sicurezza e assicurare la compatibilità reciproca dei software che lo implementano in pratica. Ogni utente "personalizza" però le trasformazioni che mappano il testo in chiaro nel crittogramma mediante la scelta di uno o più parametri, la cosiddetta *chiave*, che deve essere fornita all'algoritmo assieme al testo da cifrare o decifrare. Siccome tutti dispongono dello stesso algoritmo, la sicurezza del sistema dipende direttamente, anche se non unicamente, dalla segretezza della chiave, che deve essere nota esclusivamente al mittente ed al destinatario. Ogni utente è ovviamente libero di utilizzare chiavi diverse per comunicare con più interlocutori senza che nessuno di essi possa leggere messaggi a lui non indirizzati.

Come accennato, la segretezza della chiave non basta a garantire la riservatezza dell'informazione. Claude Shannon ha infatti dimostrato, attorno al 1940, che se la chiave è più breve del messaggio da codificare un avversario dotato di sufficiente potenza di calcolo può dedurre dal crittogramma alcune informazioni sul testo in chiaro, indipendentemente da quanto sia complesso il procedimento di codifica[I]. I cifrari commerciali più comunemente usati, quali ad esempio il Data Encryption Standard (DES), utilizzano una chiave di lunghezza fissata, nel caso specifico 56 bit, e sono perciò teoricamente violabili[II]. L'unico sistema crittografico a chiave provatamente sicuro rimane perciò il cifrario[III] Vernam, scoperto nel 1917 dal maggiore Joseph Mauborgne e da Gilbert Vernam dell'AT&T. Esso utilizza una chiave casuale della stessa lunghezza del messaggio, che non può venire riutilizzata per successive trasmissioni. La codifica è molto semplice, e si effettua come segue [Ekert3]. Supponiamo di utilizzare, per i messaggi, un alfabeto di trenta simboli comprendente le lettere, il carattere spazio "_" e alcuni segni di interpunzione. Assegniamo ad ogni simbolo il suo numero d'ordine:

A	**B**	**C**	**D**	**E**	**...**	**...**	**X**	**Y**	**Z**	**_**	**?**	**,**	**.**
00	01	02	03	04	...	...	23	24	25	26	27	28	29

[I] L'argomentazione di Shannon prescinde da considerazioni di complessità computazionale. La potenza di calcolo necessaria potrebbe in realtà richiedere maggiori risorse di quante l'Universo sia in grado di fornire; si veda al riguardo, nella sezione seguente, la discussione della sicurezza dei sistemi crittografici a chiave pubblica.

[II] Esiste in realtà un conflitto fra il diritto dei cittadini alla riservatezza dell'informazione e il desiderio dei servizi segreti governativi di limitare la disponibilità di sistemi crittografici sicuri. Ad esempio nel caso del Federal Data Encryption Standard, un cifrario convenzionale approvato negli Stati Uniti dal National Bureau of Standards, la National Security Agency ha convinto l'IBM, che ha progettato lo standard, a ridurre la lunghezza della chiave a 56 bit. La questione è controversa, ma è probabile che ciò sia stato fatto per indebolire lo standard, in modo da permettere alla National Security Agency di forzare il codice qualora venisse utilizzato da un'organizzazione straniera [Hellman].

[III] Tecnicamente, si indica con *cifrario* un algoritmo crittografico che, come la trasposizione e la sostituzione dei simboli, opera su un testo indipendentemente dalla sua struttura linguistica. I *codici* propriamente detti, che qui non discutiamo, operano su unità linguistiche quali parole o frasi.

Dato il testo in chiaro sostituiamo alle lettere i corrispondenti numeri d'ordine, ottenendo così una sequenza di numeri compresi tra 0 e 29. Supponiamo poi di disporre di un'altra sequenza di interi casuali compresi tra 0 e 29, che costituisce la chiave concordata con il destinatario. La chiave deve avere la stessa lunghezza del testo. Il crittogramma si ottiene semplicemente sommando modulo 30 i numeri corrispondenti nelle sue sequenze, come illustrato dal seguente esempio:

Testo in chiaro	**V**	**E**	**R**	**N**	**A**	**M**	**_**	**C**	**I**	**P**	**H**	**E**	**R**
Codifica numerica	21	04	17	13	00	12	26	02	08	15	07	04	17
Chiave	12	01	18	27	03	23	28	19	14	26	25	29	17
Crittogramma	**03**	**05**	**05**	**10**	**03**	**05**	**24**	**21**	**22**	**11**	**02**	**03**	**04**

Per decrittare il messaggio, il destinatario non deve fare altro che sottrarre modulo 30 ai numeri del crittogramma i corrispondenti numeri della chiave.

Nonostante questo cifrario sia provatamente sicuro, esso è chiaramente poco pratico. La trasmissione del crittogramma può essere effettuata attraverso qualunque canale pubblico, ad esempio stampandolo su un giornale, ma mittente e destinatario, che non condividono in partenza alcuna informazione segreta, devono ad un certo momento utilizzare un canale sicuro per stabilire la chiave. Questo è un problema di difficile soluzione pratica, in quanto i due utenti possono essere impossibilitati ad incontrarsi e d'altra parte l'uso di un qualunque canale, compreso l'invio di un messo fidato, li espone al rischio che la chiave venga spiata e quindi ogni successiva comunicazione che la utilizzi possa venire decifrata senza che essi ne siano a conoscenza.

Il problema della distribuzione della chiave è stato oggetto di molte ricerche da parte dei matematici. Un importante progresso in questo senso si è avuto negli anni 70 con l'invenzione della crittografia a chiave pubblica.

La crittografia a chiave pubblica

Descriviamo qui in qualche dettaglio la crittografia a chiave pubblica (PKC) in quanto essa rappresenta una brillante soluzione al problema della distribuzione della chiave basata sui risultati della teoria della complessità, soluzione che è stata recentemente messa in discussione dalle nuove possibilità di calcolo aperte dalla computazione quantistica.

Nei sistemi crittografici a chiave pubblica gli interlocutori, invece di accordarsi su una chiave comune, generano ciascuno due chiavi: una di codifica $\mathcal{C}$, che serve ad implementare l'algoritmo che cifra il messaggio, ed una di decodifica $\mathcal{D}$, utilizzata dall'algoritmo di decifrazione [Hellman]. Le due chiavi sono collegate tra loro in quanto servono a realizzare due operazioni opposte: l'applicazione successiva della trasformazione specificata da $\mathcal{C}$ e di quella specificata da $\mathcal{D}$ riproduce il testo in chiaro. Il fatto saliente è che la derivazione di $\mathcal{D}$ da $\mathcal{C}$ costituisce un problema computazionalmente intrattabile. E' in tal modo possibile realizzare un "elenco telefonico" pubblico delle chiavi di codifica dei singoli utenti senza che venga compromessa la segretezza delle chiavi di decodifica. Come nei sistemi crittografici convenzionali, gli algoritmi di codifica e di decodifica sono pubblici. Chiunque voglia comunicare ad una particolare persona delle informazioni riservate non deve perciò fare altro che consultare l'elenco e criptare il messaggio utilizzando la chiave di codifica di quella persona. Soltanto il destinatario designato, che possiede la chiave $\mathcal{D}$ di decodifica, sarà in grado di decifrare il crittogramma.

I sistemi a chiave pubblica sono basati sull'esistenza di una particolare classe di funzioni, denominate *trapdoor one-way functions.* Con *one-way function* si indica una funzione facilmente computabile la cui inversa non è computabile in pratica. Una *trapdoor one-way function* è una funzione facilmente computabile la cui inversa non è computabile in pratica a meno che non siano

note alcune informazioni aggiuntive impiegate nella "progettazione" della funzione stessa.

La ricerca di tali funzioni porta naturalmente alla classe dei problemi **NP**, ovvero a quei problemi a complessità esponenziale per i quali la verifica di soluzioni richiede però solo un tempo polinomiale. Essi si prestano infatti immediatamente alla costruzione di funzioni a senso unico; quelli utilizzabili a fini crittografici permettono anche l'implementazione del necessario meccanismo "a botola".

I due algoritmi PKC più noti si basano su una restrizione del problema **NP**-completo dello zaino (Hellman e Merkle) e sul problema **NP** della fattorizzazione (algoritmo RSA di Ronald Rivest, Adi Shamir e Leonard Adleman, 1979). Lo stesso Shamir ha dimostrato, nel 1982, che la restrizione del problema dello zaino utilizzata da Hellman e Merkle è computazionalmente trattabile, ragion per cui tale cifrario non è sicuro.

L'algoritmo RSA risulta invece al momento il cifrario più usato, ed ha scatenato una vera corsa alla determinazione di numeri primi sempre più grandi. La chiave pubblica consiste infatti nel prodotto di due numeri primi, mentre la chiave segreta viene ottenuta dai due fattori. E' importante notare che, siccome esistono algoritmi classici efficienti per la determinazione della primalità, riconoscere un numero primo è molto più facile che non fattorizzarne uno delle stesse dimensioni.

La scoperta dell'algoritmo di Shor pone dunque una seria ipoteca sull'affidabilità dell'algoritmo RSA. La sicurezza del cifrario rimane ormai legata solo all'attuale impossibilità tecnologica di implementare l'algoritmo di Shor. E' comunque opportuno ricordare che il problema della fattorizzazione non è **NP**-completo, e altri problemi **NP** possono perciò in linea di principio essere utilizzati per implementare algoritmi crittografici a chiave pubblica. Notiamo inoltre che qualunque problema di criptoanalisi è al più **NP**, in quanto data una chiave è

sempre facile controllare se è corretta. Perciò, la dimostrazione che forzare un certo cifrario costituisce un problema **NP**-completo equivale a garantire che quel cifrario offre il massimo grado di sicurezza possibile. Violarlo significherebbe infatti trovare un algoritmo polinomiale per un problema **NP**-completo, il che permetterebbe di risolvere tutti i problemi **NP** ed essere quindi in grado di decrittare i crittogrammi prodotti da qualunque algoritmo.

Distribuzione sicura della chiave

La crittografia quantistica consiste in protocolli di comunicazione che sfruttano la trasmissione su un canale quantistico per permettere a due interlocutori, che inizialmente non condividono alcun segreto comune, di stabilire una chiave provatamente segreta da utilizzare per la codifica di messaggi mediante il cifrario Vernam.

Ci sono sostanzialmente tre differenti algoritmi per la crittografia quantistica [Ekert3]:

- codifica basata su due osservabili che non commutano, proposta da S. Wiesner (1970) e da C. H. Bennett e G. Brassard (1984);
- codifica basata sugli stati correlati di tipo EPR proposta da A. Ekert (1990) e sue varianti proposte da E. Biham, B. Huttner e T. Mor (1996);
- codifica mediante l'utilizzo di due vettori di stato non ortogonali proposta da C. H. Bennett (1992).

Introduciamo qui la terminologia universalmente accettata in crittografia quantistica, indicando con Alice e Bob mittente e destinatario legittimi e con Eve (dall'inglese *to eavesdrop*=origliare) un ascoltatore non autorizzato. I tre protocolli elencati richiedono che Alice e Bob dispongano di un canale quantistico in grado di trasmettere una particella (tipicamente un fotone) senza

alterarne lo stato, nonché di un canale pubblico classico. Eve può naturalmente ascoltare le comunicazioni sul canale pubblico, ma si assume che non possa modificarle. Eve può inoltre tentare di osservare la comunicazione sul canale quantistico, che si ammette non sia protetto in maniera particolare. La peculiarità della crittografia quantistica consiste nel fatto che qualunque tentativo di osservazione di tale canale da parte di Eve comporta necessariamente delle alterazioni dello stato trasmesso tali da rivelare ad Alice e Bob che il canale è stato spiato. Questa garanzia riposa sulle leggi stesse della meccanica quantistica, ed è perciò indipendente dalla tecnologia utilizzata da Eve.

Lo schema di Bennett e Brassard

Questo protocollo si basa sulla trasmissione lungo il canale quantistico di fotoni polarizzati ([Bennett5], [Ekert3]).

Supponiamo che Alice e Bob possano preparare, trasmettere e misurare fotoni polarizzati orizzontalmente, verticalmente o lungo gli assi diagonali a 45 e 135 gradi rispetto all'orizzontale. Alice prepara una serie di fotoni con polarizzazione scelta a caso fra le quattro direzioni e li invia a Bob. Questi, a sua volta, sceglie casualmente per ogni fotone se misurare la polarizzazione lungo gli assi orizzontale e verticale o lungo gli assi diagonali.

In un secondo momento, Bob rivela ad Alice sul canale pubblico su quale base ha proiettato i singoli fotoni. Alice, a sua volta, segnala a Bob quali fotoni erano stati polarizzati diagonalmente e quali, invece, a 0 o 90 gradi. Chiaramente, quando gli assi di preparazione non coincidono con gli assi di misura il risultato ottenuto da Bob è completamente casuale. I fotoni preparati e misurati sulla stessa base, mediamente metà del totale, costituiscono però dei bit condivisi tra Alice e Bob: è sufficiente infatti che i due convengano di assegnare il valore "0", ad esempio, ai fotoni polarizzati a 0 o 45 gradi, e il valore "1" ai rimanenti.

Questa successione di bit casuali è candidata ad essere usata come chiave per il cifrario Vernam.

A questo punto, Alice e Bob devono assicurarsi che il canale quantistico non sia stato osservato. Questo è facilmente realizzabile confrontando sul canale pubblico un campione statistico dei bit condivisi. Supponiamo infatti che i due abbiano trasmesso e misurato un bit utilizzando gli assi orizzontale e verticale: essendo la scelta casuale, Eve avrà utilizzato la stessa base o la base diagonale con probabilità ½. Nel caso però che Eve abbia scelto gli assi diagonali, il risultato della misura di Bob è completamente casuale. Possiamo perciò attenderci che l'effetto netto sia di introdurre errori in un quarto dei bit che sono stati osservati da Eve.

In realtà, il semplice procedimento di paragonare un campione di bit risulta poco efficiente, in quanto troppi bit devono essere sacrificati per ottenere una ragionevole certezza che il canale non sia stato osservato. Un sistema migliore consiste nel paragonare la parità di un sottoinsieme comprendente circa la metà dei bit della chiave, scelto casualmente e concordato tra i due attraverso il canale pubblico. Si può dimostrare che questo procedimento è in grado di stabilire con probabilità ½ se le sequenze di Alice e Bob contengono delle differenze, indipendentemente dal numero e dalla posizione degli errori. Ripetendo questo test una ventina di volte, con venti insiemi diversi scelti a caso, si può così ridurre la probabilità che vi siano errori non individuati a meno di uno su un milione.

Codifica mediante stati non ortogonali

Una seconda alternativa, proposta da C.H. Bennett nel 1992, prevede che Alice e Bob assegnino a due stati non ortogonali $|u\rangle$ e $|v\rangle$ il significato di zero e di uno rispettivamente ([Ekert2], [Ekert3]). Alice trasmette a Bob una sequenza di bit preparati casualmente nello stato $|u\rangle$ o nello stato $|v\rangle$.

Poiché $\langle u|v\rangle \neq 0$, non esiste un procedimento di misura in grado di distinguere i due stati con certezza. Bob può tuttavia effettuare un test che non sempre ha successo, ma che non può in alcun caso fornire risposte errate. L'approccio più semplice (anche se non il più efficiente) consiste nel misurare con la stessa probabilità i due proiettori $P_{\neg u} = 1 - |u\rangle\langle u|$ o $P_{\neg v} = 1 - |v\rangle\langle v|$. Possiamo pensare a questi operatori come a due filtri che selezionano rispettivamente gli stati ortogonali ad $|u\rangle$ e a $|v\rangle$. Nel caso ad esempio che $|u\rangle$ e fossero gli stati di polarizzazione di un fotone lungo le direzioni non ortogonali *u* e *v*, $P_{\neg u}$ sarebbe implementabile mediante un polarizzatore con l'asse ottico ortogonale a *u*, in modo tale da trasmettere lo stato $|u\rangle$ con probabilità nulla; analogamente $P_{\neg v}$ sarebbe realizzato da un polarizzatore con l'asse ottico ortogonale a *v*.

Un risultato positivo per $P_{\neg u}$ indica con certezza che il bit trasmesso era nello stato $|v\rangle$, in quanto tale filtro sopprime lo stato $|u\rangle$; viceversa, un risultato positivo per $P_{\neg v}$ segnala un bit nello stato $|u\rangle$. Se Bob, misurando ad esempio $P_{\neg u}$, sopprime il segnale, ottiene una informazione ambigua non utilizzabile, in quanto non è in grado di stabilire se si tratti di uno stato $|u\rangle$ o di uno stato $|v\rangle$ che è stato proiettato lungo $|u\rangle$. I risultati nulli forniscono in effetti solo probabilità a posteriori per gli stati $|u\rangle$ e $|v\rangle$.

Al termine della trasmissione, Bob comunica ad Alice per quali bit è riuscito ad ottenere un risultato certo; tali bit costituiscono la chiave, mentre i rimanenti vengono scartati. La segretezza è garantita dal fatto che nemmeno Eve può distinguere con certezza uno stato $|u\rangle$ da uno stato $|v\rangle$. Un bit interpretato erroneamente da Eve e ritrasmesso a Bob nello stato errato ha però una certa probabilità di causare un errore nella chiave; un adeguato test statistico, come ad esempio quello descritto nel caso precedente, permette perciò ad Alice e Bob di rilevare l'intrusione.

Codifica mediante stati correlati

Il protocollo proposto nel 1990 da Artur Ekert utilizza per la trasmissione della chiave le proprietà non locali degli stati correlati di tipo EPR ([Ekert5], [Bennett5]).

Tale soluzione prevede che Alice e Bob abbiano a disposizione una sorgente di fotoni nello stato di singoletto

$$\Psi^{(-)} = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B\right) = \frac{1}{\sqrt{2}}\left(|\leftarrow\rangle_A|\rightarrow\rangle_B - |\rightarrow\rangle_A|\leftarrow\rangle_B\right)$$

dove $|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)$ e $|\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right)$.

Alice trattiene uno dei fotoni per sé e invia l'altro a Bob. I due convengono di proiettare ciascuno il proprio fotone scegliendo di volta in volta a caso fra una delle due basi $\{|\uparrow\rangle, |\downarrow\rangle\}$ e $\{|\rightarrow\rangle, |\leftarrow\rangle\}$. Gli unici casi rilevanti ai fini della trasmissione della chiave sono quelli in cui Alice e Bob utilizzano la stessa base: in tal caso, infatti, ad un risultato $|\uparrow\rangle$ (oppure $|\rightarrow\rangle$) ottenuto Alice corrisponde necessariamente un risultato $|\downarrow\rangle$ (o $|\leftarrow\rangle$) ottenuto da Bob. Questo permette ai due, assegnando un valore logico ai possibili esiti di ogni misura, di ottenere una sequenza binaria condivisa, da utilizzare appunto come chiave.

La scelta casuale delle basi ha anche in questo caso lo scopo di impedire ad Eve di conoscere a priori quale misura effettuare sui fotoni in transito. In tal modo, qualsiasi tentativo di intrusione porta necessariamente a degli errori rilevabili mediante il solito controllo statistico.

Una interessante modifica a questo protocollo è stata proposta nel 1996 da Eli Biham, Bruno Huttner e Tal Mor con la denominazione di ***"time-reversed EPR scheme"*** [Biham2]. In questo schema, Alice e Bob preparano ciascuno un fotone o un'altra particella di spin ½ scegliendo a caso uno fra gli stati $|\uparrow\rangle$, $|\rightarrow\rangle$,

$|\downarrow\rangle$ o $|\leftarrow\rangle$ e li inviano ad una terza persona, che chiameremo un *centro*. Il centro, ricevute le particelle, ne misura lo spin totale. Se il risultato della misura è zero, le due particelle sono proiettate sullo stato $\Psi^{(-)}$ di singoletto. La definizione di $\Psi^{(-)}$ garantisce in tal caso che, se Alice e Bob hanno utilizzato la stessa base per la preparazione, gli spin delle due particelle erano inizialmente opposti (due particelle preparate con lo stesso spin lungo lo stesso asse sono in uno stato ortogonale allo stato di singoletto). In tal modo Alice conosce il bit di Bob e viceversa. Il protocollo funziona dunque come segue:

- Il centro riceve le particelle di Alice e Bob e ne misura lo spin totale, utilizzando un canale pubblico per comunicare ai due il risultato della misura.
- Alice e Bob scartano i bit per i quali lo spin totale è diverso da zero.
- I due interlocutori rivelano sul canale pubblico la base utilizzata per preparare le particelle rimanenti. Grazie alle informazioni del centro, essi sanno che quando le due basi coincidono i bit sono anticorrelati. Tali bit costituiscono la chiave.

La scelta casuale fra due basi ha ancora lo scopo di impedire l'osservazione "silenziosa" del canale durante l'invio delle particelle di Alice e Bob al centro. Un centro onesto, che proietta le due particelle sullo stato di singoletto, non ottiene alcuna informazione sul valore dei due bit. Per conoscere tale valore il centro dovrebbe quindi proiettare le particelle su un altro stato. D'altra parte, lo stato di singoletto è l'unico a garantire che i bit siano anticorrelati indipendentemente da quale base Alice e Bob abbiano utilizzato. Un tentativo di osservazione da parte del centro introduce perciò necessariamente degli errori nella chiave, ed è quindi rilevabile da Alice e Bob mediante un test statistico.

Questo protocollo, apparentemente più complicato, si presta però alla realizzazione di una rete crittografica quantistica analoga alle reti classiche, basata su un centro crittografico.

In una rete classica il centro custodisce le chiavi depositate da un gruppo di utenti e le utilizza per permettere, su richiesta, ad ognuno di condividere una chiave segreta con un qualunque interlocutore che abbia anch'egli depositato una propria chiave presso il centro. In pratica, quando Alice richiede al centro una chiave segreta per comunicare con Bob questo utilizza la stinga di bit depositata da Alice per codificare col cifrario Vernam la chiave di Bob, e invia il crittogramma ad Alice. In tal modo Alice viene a conoscenza della chiave di Bob e può utilizzarla per cifrare un testo che lui, poi, può decrittare. Questo tipo di rete permette ad un gruppo di persone di comunicare fra loro senza per questo che ognuno debba stabilire in precedenza una chiave comune con ciascuno degli altri utenti. Lo scotto pagato per questa versatilità è l'utilizzo di un centro al quale sono affidate tutte le chiavi, che è quindi in grado di decrittare qualsiasi messaggio.

Il *time-reversed EPR scheme* si presta alla realizzazione di una rete crittografica che protegga gli utenti anche dai tentativi di intrusione da parte del centro. Tale rete richiede che il centro sia dotato di memorie quantistiche nelle quali poter conservare, senza misurarle, serie di particelle di spin ½ consegnate da ciascun utente e preparate, ad insaputa del centro, in uno dei quattro stati $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\downarrow\rangle$ o $|\leftarrow\rangle$. Quando Alice e Bob vogliono stabilire una chiave per comunicare fra loro richiedono al centro di prelevare dalle rispettive riserve personali coppie di particelle e di misurarne lo spin totale. Il centro comunica poi il risultato delle misure, e Alice e Bob proseguono come indicato dal *time-reversed EPR scheme*. In effetti non esistono differenze di principio tra la situazione descritta in precedenza, che vede Alice e Bob inviare dei bit al centro che li misura immediatamente, e la rete crittografica nella quale il centro "congela" i bit fino a

quando non sono richiesti. Le due procedure offrono perciò le stesse garanzie di segretezza della comunicazione, anche per quanto riguarda l'impossibilità di un'intrusione da parte del centro stesso.

La rete crittografica offre il vantaggio fondamentale di non richiedere l'esistenza di un canale quantistico per ogni coppia di interlocutori che vogliano stabilire una chiave condivisa. Al contrario, una volta che le particelle sono depositate presso il centro, *non è necessario alcun canale quantistico*. La consegna stessa delle particelle potrebbe avvenire a mezzo corriere, e non pone particolari problemi di sicurezza in quanto un tentativo di osservazione sarebbe comunque rilevabile dopo la creazione della chiave mediante un controllo statistico. Anche volendo utilizzare un canale quantistico per la consegna al centro delle particelle, il numero di linee richiesto sarebbe comunque pari al numero di utenti, anziché al numero di tutte le possibili coppie di utenti.

La rete crittografica sposta quindi la sfida tecnologica dallo studio di canali efficienti per la trasmissione a distanza di stati quantistici allo sviluppo di dispositivi che permettano la conservazione nel tempo di tali stati.

Al momento attuale, la tecnologia più promettente per la realizzazione di memorie quantistiche è quella degli ioni intrappolati. Nelle trappole i bit quantistici possono essere codificati nei gradi interni di libertà degli ioni, ad esempio lo spin, e operazioni su due bit possono essere compiute servendosi dei gradi di libertà fononici di due o più ioni intrappolati insieme. E' al momento possibile conservare gli stati di spin degli ioni per più di dieci minuti. Inoltre, le tecniche di correzione d'errore attualmente in fase di studio (vedi pag. 113 e sgg.) sembrano indicare la possibilità di ottenere un significativo aumento del tempo di conservazione dello stato a spese di una ulteriore elaborazione dell'informazione, senza porre richieste più stringenti sull'isolamento dei portatori fisici dei bit.

Notiamo infine che la scelta di misurare lo spin totale delle particelle di Alice e Bob non è particolarmente conveniente in quanto la probabilità di ottenere

lo stato di singoletto è solo 1/4, il che, tenuto conto del fatto che gli unici bit validi sono quelli preparati lungo gli assi di una stessa base, riduce ad 1/8 la frazione di bit utilizzabili. Una scelta più efficiente, per quanto più difficile da implementare, consiste nel misurare sulle due particelle l'operatore di Bell, i cui autostati sono lo stato di singoletto $\Psi^{(-)}$ e i seguenti tre stati:

$$\Phi^{(+)} = \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle\right) = \frac{1}{\sqrt{2}}\left(|\leftarrow\leftarrow\rangle + |\rightarrow\rightarrow\rangle\right),$$

$$\Psi^{(+)} = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle\right) = -\frac{1}{\sqrt{2}}\left(|\leftarrow\leftarrow\rangle - |\rightarrow\rightarrow\rangle\right),$$

$$\Phi^{(-)} = \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle\right) = \frac{1}{\sqrt{2}}\left(|\leftarrow\rightarrow\rangle + |\rightarrow\leftarrow\rangle\right),$$

dove la seconda espressione è ottenuta, per ogni stato, espandendolo sulla base $\{|\rightarrow\rangle, |\leftarrow\rangle\}$ analogamente a quanto fatto per il singoletto. Consideriamo il caso in cui Alice e Bob hanno preparato le loro particelle in stati della stessa base. La conoscenza di tale base e il risultato della misura determinano univocamente se i due bit sono correlati (per esempio, risultato della misura $\Phi^{(-)}$ e base $\{|\uparrow\rangle, |\downarrow\rangle\}$) o anticorrelati (per esempio, risultato della misura ancora $\Phi^{(-)}$ ma base $\{|\rightarrow\rangle, |\leftarrow\rangle\}$), senza che alcuna coppia di bit debba essere scartata. Tenuto conto della casualità nella scelta della base, non eliminabile in quanto garantisce la segretezza della trasmissione, il numero di particelle effettivamente utilizzabili per stabilire la chiave risulta essere la metà del totale, con una efficienza pari a quella ottenibile nella versione originale del protocollo proposta da A. Ekert.

Realizzazioni pratiche

La prima implementazione pratica di un apparato per la crittografia quantistica, basato sul protocollo di Bennett e Brassard, è stata realizzata nel 1991 presso i laboratori IBM [Bennett5] utilizzando la trasmissione di fotoni in

aria su una distanza di 30 cm (Figura 12). La sorgente di fotoni singoli era costituita da un led verde alimentato ad impulsi, che venivano attenuati fino ad un contenuto medio di 0,1 fotoni per flash. I quattro stati di polarizzazione $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\downarrow\rangle$ e $|\leftarrow\rangle$ utilizzati dal protocollo venivano preparati mediante un polarizzatore seguito da due dispositivi elettro-ottici per la rotazione della polarizzazione (celle di Pockels) controllati dal calcolatore che emulava Alice. Il calcolatore simulante Bob agiva invece su una ulteriore cella di Pockels per selezionare gli assi di misura; i fotoni polarizzati in direzioni ortogonali venivano poi instradati da un cristallo birifrangente a due fotomoltiplicatori.

Più recentemente A. Muller, H. Zbinden e N. Gisin dell'Università di Ginevra [Muller] hanno realizzato un canale crittografico a fotone singolo adoperando una fibra ottica commerciale della lunghezza di 23 km, una fra le quaranta fibre contenute in un cavo utilizzato dall'ente svizzero PTT per il trasferimento dati a 2,5 Gbit/s tra Nyon e Ginevra, posato sul fondo del lago. L'esperimento ha dimostrato la possibilità di trasmettere e rilevare impulsi polarizzati costituiti in media da 0,12 fotoni l'uno, ottenuti attenuando un laser ad impulsi della lunghezza d'onda di 1,3 μm. La larghezza degli impulsi utilizzati era 1 ns e la frequenza di ripetizione 1,1 Mhz. La percentuale di bit errati sul totale dei bit trasmessi, in gran parte dovuta a rumore nel rilevatore, è stata pari al 3,4%, un valore abbastanza ridotto da garantire comunque la privacy del canale.

Una possibile implementazione del protocollo basato su stati non ortogonali proposto da Bennett, alternativa all'uso degli stati di polarizzazione, è

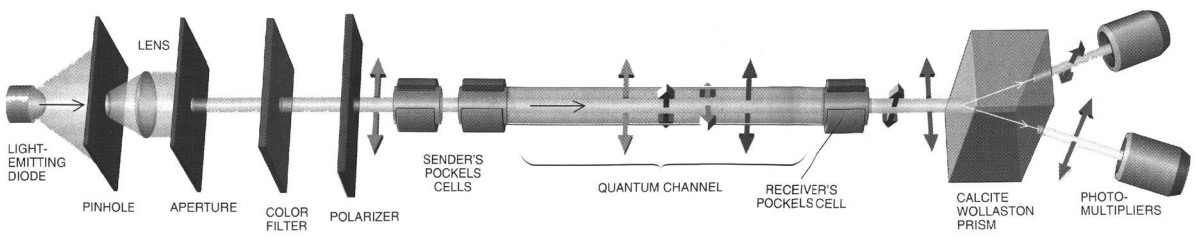


Figura 12: Crittografia quantistica con osservabili che non commutano.

fondata sull'uso di interferometri [Ekert3]. Una combinazione lineare di stati ortogonali può essere realizzata facendo "percorrere" ad un singolo fotone i due bracci di un interferometro. Ciascun percorso può essere considerato uno stato ortogonale all'altro e i coefficienti della sovrapposizione coerente sono determinati dagli specchi semiargentati impiegati come *beam-splitters*. Lo stato risultante del fotone nell'interferometro può essere scritto come

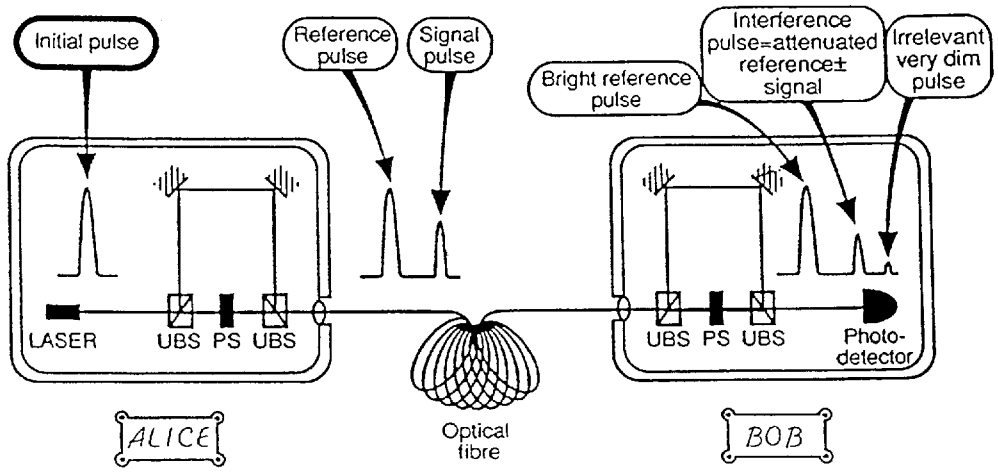
$$|u\rangle = \sqrt{t}|I\rangle + i\sqrt{r}|II\rangle$$

dove $|I\rangle$ e $|II\rangle$ denotano i due percorsi possibili, mentre *t* ed *r* rappresentano i coefficienti di trasmissione e di riflessione dello specchio semiargentato. Per generare un secondo stato non ortogonale al primo è sufficiente variare il cammino ottico del fotone lungo uno dei due bracci, ad esempio mediante l'introduzione di una lamina di spessore opportuno, in modo da ottenere

$$|v\rangle = e^{i\varphi}\sqrt{t}|I\rangle + i\sqrt{r}|II\rangle .$$

Modificando lo sfasamento fra 0 e π si ottengono rispettivamente due stati $|u\rangle$ e $|v\rangle$ tali che $|\langle u|v\rangle|^2 = (r-t)^2$.

Figura 13: Implementazione interferometrica della crittografia quantistica mediante stati non ortogonali.



I due stati $|u\rangle$ e $|v\rangle$ possono essere prodotti e rilevati da interferometri di Mach e Zehnder (Figura 13). Alice e Bob sono in possesso di due interferometri identici con *beam-splitters* asimmetrici (UBS in figura), in modo tale che l'intensità dell'impulso ritardato dal braccio più lungo sia sensibilmente maggiore di quella che percorre il braccio più corto. Su quest'ultimo percorso è presente uno *phase-shifter* (PS in figura) che può introdurre, a scelta, due diversi sfasamenti, in modo tale da permettere la codifica da parte di Alice ed il filtraggio da parte di Bob. Se Alice e Bob hanno selezionato lo stesso sfasamento, nell'interferometro di Bob si avrà interferenza costruttiva tra il segnale e l'impulso attenuato di riferimento, portando così ad un conteggio nel rilevatore di Bob. Nel caso contrario, l'interferenza distruttiva non può portare ad un conteggio nel rivelatore. L'impulso ritardato di maggiore intensità serve a confermare a Bob l'avvenuta trasmissione di un bit.

La realizzazione pratica di questo dispositivo richiede, anche in questo caso, una sorgente di fotoni, una fibra ottica per telecomunicazioni a bassa attenuazione e un buon rivelatore per fotoni singoli. Ecco alcune considerazioni sulle tecnologie disponibili:

- Una buona sorgente di fotoni singoli può essere ottenuta, come già accennato, attenuando gli impulsi di un laser a semiconduttore. Essendo la distribuzione dei fotoni poissoniana a bassa intensità, quando il numero medio di fotoni è ridotto a 0,1 per impulso la probabilità di trovare impulsi con due più fotoni vale circa 0,005. Con questo sistema, in media, 100 impulsi su 1000 conterranno esattamente un fotone, 895 saranno vuoti, e i rimanenti 5 conterranno due o più fotoni.

- Come l'esperimento di A. Muller, H. Zbinden e N. Gisin ha dimostrato, la qualità delle fibre ottiche commerciali è all'altezza della situazione. L'attenuazione nelle fibre ha due origini: lo scattering di Rayleigh e l'assorbimento. La composizione chimica della fibra varia da punto a punto

causando una fluttuazione dell'indice di rifrazione nel materiale. Se la scala di tali fluttuazioni è inferiore ad un decimo della lunghezza d'onda, ogni irregolarità diviene un centro di scattering puntiforme. Ne risulta un coefficiente efficace di assorbimento che varia come $1/\lambda^4$. Le perdite per assorbimento nella regione del visibile e dell'infrarosso vicino sono dovute alle impurezze, in particolare a tracce di ioni metallici e ioni ossidrile. La regione dell'infrarosso vicino è particolarmente interessante perché molti collegamenti a fibre ottiche ad alta capacità lavorano attualmente a 1,3 μm o 1,5 μm.

- In questa regione di lunghezze d'onda i rivelatori più adatti risultano essere i fotodiodi a valanga (APD). Si tratta di dispositivi a semiconduttori nei quali un elettrone ed una lacuna generati dall'assorbimento di un fotone vengono accelerati in opposte direzioni da un campo elettrico. L'elettrone può urtare altri elettroni, portandoli nella banda di conduzione. Il risultante effetto a valanga dà origine ad un segnale rilevabile al fondo del chip. L'efficienza di tali rivelatori è purtroppo piuttosto bassa, essendo attorno al 5%.

  La principale sorgente di errori, in assenza di tentativi di osservazione del canale, è data dai conteggi oscuri dei rivelatori, dovuti a valanghe originate da coppie elettrone-lacuna di origine termica. Raffreddando il rivelatore alla temperatura dell'azoto liquido si riduce il fenomeno, ma rimane pur sempre necessario conoscere il tempo di emissione dell'impulso laser per distinguere il segnale utile dai conteggi oscuri. I difetti presenti nel semiconduttore possono inoltre intrappolare elettroni e lacune per poi rilasciarli successivamente, dando luogo all'"*afterpulsing*", che deve ovviamente essere tenuto in considerazione nell'analisi dei dati.

Segnaliamo infine che British Telecom ha effettivamente realizzato un canale ad interferenza a fotone singolo in grado di trasmettere la chiave ad una velocità di 20 kbit/s su una distanza di 10 km.

Crittografia ed “intercettazione quantistica”

I protocolli crittografici descritti sono caratterizzati dall’utilizzo, in tempi successivi, di un canale quantistico ed un canale classico. E’ intuitivo che una osservazione diretta del canale quantistico non possa che introdurre degli errori nella trasmissione, e di conseguenza mettere Alice e Bob in grado di rilevare l’intercettazione. Tuttavia, la computazione quantistica mette in mano ad Eve uno strumento in apparenza più potente. Ella può infatti correlare il bit quantistico in transito con un proprio sistema *senza effettuare misure*, attendere che Alice e Bob abbiano ultimato lo scambio delle informazioni sul canale classico, e solo a quel punto cercare di ottenere informazioni sui bit validi proiettando il proprio sistema su una base opportuna. Questa tecnica di intercettazione richiede tra l’altro la capacità di conservare inalterato lo stato del sistema di Eve per periodo di tempo anche lungo, e appare quindi al momento difficilmente realizzabile. Ciononostante, è necessario stabilire se la crittografia quantistica presenti una robustezza intrinseca contro questa classe più generale di attacchi o se, al contrario, l’unica garanzia della riservatezza di un messaggio risieda ancora una volta nella difficoltà tecnologica di realizzare una intercettazione efficiente. In quest’ultima ipotesi la crittografia quantistica verrebbe infatti ad assumere uno *status* inferiore a possibili futuri cifrari classici a chiave pubblica basati su problemi **NP**-completi (cfr. al riguardo le pagine 85-86).

Nonostante vi siano forti indicazioni riguardo alla sicurezza dei protocolli quanto-crittografici a questa forma di “attacco coerente”, il problema è al presente ancora aperto. Uno degli ostacoli maggiori è rappresentato dalla necessità di tenere conto dell’inevitabile livello di errore comunque presente sulla linea, che potrebbe mascherare gli effetti di un’intrusione o comunque indurre Alice e Bob a condividere una quantità maggiore di informazione sul canale

classico per poter applicare ai propri bit una procedura di correzione d'errore [Biham].

Illustriamo nel seguito un possibile attacco coerente ad una distribuzione della chiave basata sui principali protocolli descritti, ai quali di volta in volta rimandiamo il lettore.

Il dispositivo di intercettazione

Nei tre esempi che seguono faremo uso dello stesso dispositivo di intercettazione, descritto in figura 14. L'intercettazione dell'informazione quantistica è svolta attraverso un gate CONTROLLED-NOT nel quale il bit quantistico in transito tra Alice e Bob funge da bit di controllo, mentre una particella originata da una "sorgente di zeri" in possesso di Eve costituisce il bit bersaglio (vedi pagg. 64 - 65). L'effetto del gate è di "copiare" lo stato della particella inviata da Alice sul bit di Eve, come specificato dalle equazioni

$$|0\rangle_A|0\rangle_E \rightarrow |0\rangle_B|0\rangle_E$$

$$|1\rangle_A|0\rangle_E \rightarrow |1\rangle_B|1\rangle_E$$

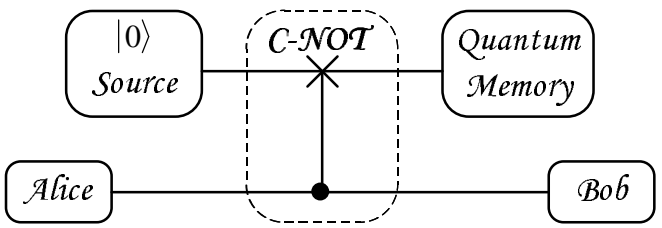
dove cambiando l'indice della prima particella da A a B intendiamo suggerire che essa prima dell'interazione col sistema di Eve è in possesso di Alice, mentre in seguito viene ricevuta da Bob. Essendo la seconda particella sempre inizialmente nello stato $|0\rangle_E$ queste due relazioni sono sufficienti a descrivere il comportamento del gate. Per la generica sovrapposizione $\alpha|0\rangle_A + \beta|1\rangle_A$ si avrà pertanto

$$\left(\alpha|0\rangle_A + \beta|1\rangle_A\right)|0\rangle_E \rightarrow \alpha|0\rangle_B|0\rangle_E + \beta|1\rangle_B|1\rangle_E,$$

per cui lo stato finale dei bit di Bob ed Eve è, ovviamente, uno stato *correlato*.

Supponiamo inoltre, con riferimento alla figura 14, che Eve disponga di una "memoria quantistica" nella quale conservare inalterato il proprio bit fino a

Figura 14: Dispositivo per l'intercettazione quantistica.



quando Alice e Bob non abbiano ultimato, relativamente a quel bit, la discussione sul canale pubblico, per poi misurarlo soltanto in seguito. In tal modo Eve non soltanto evita di perturbare anzitempo, con la propria misura, lo stato del sistema, ma usufruisce di un duplice vantaggio:

- per via della correlazione esistente tra le due particelle, l'osservazione effettuata da Bob sul proprio bit modifica, pur senza trasmettere informazione, istantaneamente lo stato della particella di Eve; successivamente,
- attraverso l'ascolto del canale pubblico Eve apprende che tipo di misura è stato effettuato da Bob. Conoscendo a priori i possibili effetti della misura di Bob sul proprio bit, ella può in tal modo proiettare quest'ultimo sulla base più appropriata per tentare di ricostruire il risultato ottenuto (e non divulgato) da Bob.

Protocollo di Bennett e Brassard

Questo protocollo, descritto a pagina 87, prevede che Alice trasmetta a Bob fotoni polarizzati scegliendo a caso tra 0, 45, 90 e 135 gradi rispetto ad una direzione fissata. Indicheremo questi stati con

$$|\uparrow\rangle, \qquad |\downarrow\rangle, \qquad |\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right), \qquad |\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right).$$

E' necessario stabilire una corrispondenza fra la base computazionale $\{|0\rangle, |1\rangle\}$ dei bit sui quali opera il CONTROLLED-NOT di Eve e questi stati. E' conveniente porre $|0\rangle \equiv |\downarrow\rangle$ e $|1\rangle \equiv |\uparrow\rangle$.

Supponiamo ora che Alice trasmetta uno stato $|\uparrow\rangle$. L'effetto del gate è il seguente:

$$|\uparrow\rangle_A|0\rangle_E \equiv |1\rangle_A|0\rangle_E \rightarrow |1\rangle_B|1\rangle_E \equiv |\uparrow\rangle_B|\uparrow\rangle_E$$

La trasmissione stabilisce un bit valido soltanto se Bob decide di proiettare il proprio fotone sulla base $\{|\uparrow\rangle,|\downarrow\rangle\}$ (ottenendo pertanto $|\uparrow\rangle_B$). La particella di Eve non è influenzata dalla misura, e rimane pertanto nello stato $|\uparrow\rangle_E$. Quando apprende dalla discussione pubblica che Alice e Bob hanno preparato e misurato il loro fotone lungo uno stato della base $\{|\uparrow\rangle,|\downarrow\rangle\}$, Eve proietta il proprio sulla stessa base ottenendo un risultato identico a quello di Bob. Eve è dunque in grado di riconoscere con probabilità uno un fotone trasmesso nello stato $|\uparrow\rangle$ senza peraltro introdurre errori nella trasmissione. Si noti che il ruolo svolto dalla memoria quantistica è fondamentale: per decidere quale osservabile misurare sul suo fotone, Eve deve conoscere la base utilizzata da Alice e Bob.

L'intercettazione di un fotone $|\downarrow\rangle$ avviene analogamente senza difficoltà; osserviamo invece cosa accade quando Alice trasmette una particella nello stato $|\rightarrow\rangle$. L'identificazione fra la base computazionale $\{|0\rangle,|1\rangle\}$ e gli stati $\{|\uparrow\rangle,|\downarrow\rangle\}$ non può logicamente essere alterata a questo punto, in quanto Eve non ha ovviamente modo di sapere a priori che la base utilizzata da Alice per la preparazione è questa volta $\{|\rightarrow\rangle,|\leftarrow\rangle\}$. Abbiamo pertanto:

$$|\rightarrow\rangle_A|0\rangle_E = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A + |\downarrow\rangle_A\right)|0\rangle_E \equiv \frac{1}{\sqrt{2}}\left(|1\rangle_A + |0\rangle_A\right)|0\rangle_E$$

che per effetto del CONTROLLED-NOT diviene:

$$\frac{1}{\sqrt{2}}\left(|1\rangle_B|1\rangle_E + |0\rangle_B|0\rangle_E\right) \equiv \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_B|\uparrow\rangle_E + |\downarrow\rangle_B|\downarrow\rangle_E\right) = |\phi_{BE}^{(+)}\rangle,$$

uno degli stati della base di Bell. Tali stati hanno statistica marginale casuale per misure effettuate separatamente su una delle particelle, per cui il contenuto di

informazione trasmesso da Alice è irrimediabilmente perduto per effetto dell'interazione del fotone col bit di Eve (indipendentemente da quale osservazione ella compia sulla sua particella). In ogni caso, per essere utile ai fini della trasmissione della chiave, il fotone trasmesso da Alice nello stato $|\rightarrow\rangle$ avrebbe dovuto deve essere proiettato da Bob sulla base $\{|\rightarrow\rangle,|\leftarrow\rangle\}$. Riscrivendo $|\phi_{BE}^{(+)}\rangle$ su tale base otteniamo

$$|\phi_{BE}^{(+)}\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle_B|\rightarrow\rangle_E + |\leftarrow\rangle_B|\leftarrow\rangle_E\right).$$

Concludiamo pertanto che se Alice e Bob dichiarano di avere entrambi utilizzato per la preparazione e la misura di un certo fotone la base $\{|\rightarrow\rangle,|\leftarrow\rangle\}$ (e quindi assumono che quel fotone trasporti un bit valido), si verificano i seguenti due fatti:

- il bit ottenuto da Bob è casuale, il che conduce ad un tasso di errore nella chiave pari al 25%;
- Eve può comunque proiettare il proprio fotone sulla stessa base, ottenendo con certezza una copia del bit (eventualmente errato) di Bob.

Eve e Bob si trovano in sintesi, al termine della trasmissione, in possesso di due chiavi identiche, che differiscono da quella di Alice in media per un quarto dei bit. Il fatto che Eve ottenga più informazione sulla sequenza di bit ricevuta da Bob che non su quella trasmessa da Alice sembra essere una caratteristica comune anche ad altre tecniche di attacco quantistico, dirette contro altri protocolli [Ekert2].

Codifica mediante stati correlati

Analizziamo ora, sempre con riferimento all'apparato schematicamente descritto in figura 14, l'efficacia della medesima tecnica di intercettazione

quantistica nel caso che la distribuzione della chiave faccia uso di coppie di fotoni in stati correlati di tipo EPR, secondo il protocollo descritto a pagina 90 e seguenti. Supponiamo pertanto che Alice prepari, per ogni trasmissione, una coppia di fotoni nello stato di singoletto

$$\left|\Psi_{AB}^{(-)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_A\left|\downarrow\right\rangle_B - \left|\downarrow\right\rangle_A\left|\uparrow\right\rangle_B\right) = \frac{1}{\sqrt{2}}\left(\left|\leftarrow\right\rangle_A\left|\rightarrow\right\rangle_B - \left|\rightarrow\right\rangle_A\left|\leftarrow\right\rangle_B\right),$$

con $|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)$ e $|\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right)$. Alice tratterrà per sé la particella contrassegnata dalla lettera A, ed invierà a Bob la particella B. Supponiamo che solo quest'ultima sia intercettabile da Eve e funga da bit di controllo per il gate CONTROLLED-NOT di figura 14. Per quanto riguarda la base computazionale di quest'ultimo, manteniamo le identificazioni $|0\rangle \equiv |\downarrow\rangle$ e $|1\rangle \equiv |\uparrow\rangle$.

L'azione del gate modifica lo stato complessivo delle particelle di Alice, Bob ed Eve nel modo seguente:

$$\left|\Psi_{AB}^{(-)}\right\rangle|0\rangle_E \equiv \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_A|0\rangle_B - \left|\downarrow\right\rangle_A|1\rangle_B\right)|0\rangle_E \rightarrow$$

$$\rightarrow \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_A|0\rangle_B|0\rangle_E - \left|\downarrow\right\rangle_A|1\rangle_B|1\rangle_E\right) \equiv \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_A\left|\downarrow\right\rangle_B\left|\downarrow\right\rangle_E - \left|\downarrow\right\rangle_A\left|\uparrow\right\rangle_B\left|\uparrow\right\rangle_E\right) = |\Xi\rangle.$$

Come indicato dal protocollo, Alice e Bob scelgono indipendentemente se proiettare il proprio fotone sulla base $\{|\uparrow\rangle, |\downarrow\rangle\}$ o sulla base $\{|\rightarrow\rangle, |\leftarrow\rangle\}$. Soltanto i casi i cui essi effettuano la stessa scelta sono significativi ai fini della trasmissione della chiave. E' evidente che nel caso in cui la base utilizzata sia la prima la correlazione fra il risultato di Alice e quello di Bob è preservata. Informata dalla discussione pubblica della scelta Eve può compiere la stessa misura sul proprio fotone ottenendo, un risultato identico a quello di Bob (e quindi opposto a quello di Alice) e venendo così a conoscenza del corrispondente bit della chiave.

L'esito dell'intercettazione è però differente, anche in questo caso, se la scelta di Alice e Bob cade sulla base $\{|\rightarrow\rangle, |\leftarrow\rangle\}$. Lo stato $|\Xi\rangle$ delle tre particelle si scrive infatti, in questa base, come

$$|\Xi\rangle = \frac{1}{2}\left[\left(|\rightarrow\rangle_B|\rightarrow\rangle_E + |\leftarrow\rangle_B|\leftarrow\rangle_E\right)|\leftarrow\rangle_A - \left(|\rightarrow\rangle_B|\leftarrow\rangle_E + |\leftarrow\rangle_B|\rightarrow\rangle_E\right)|\rightarrow\rangle_A\right]$$

ovvero più succintamente, in termini degli stati della base di Bell,

$$|\Xi\rangle = \frac{1}{\sqrt{2}}\left(\left|\phi_{BE}^{(+)}\right\rangle|\leftarrow\rangle_A - \left|\phi_{BE}^{(-)}\right\rangle|\rightarrow\rangle_A\right).$$

Se ne deduce che, nel caso che Alice sia la prima ad osservare il proprio fotone, l'effetto della misura è di lasciare le rimanenti particelle in uno degli stati $\left|\phi_{BE}^{(+)}\right\rangle$ o $\left|\phi_{BE}^{(-)}\right\rangle$. Poiché questi stati hanno statistica marginale casuale per misure effettuate separatamente su una delle due particelle, il risultato ottenuto da Bob con la proiezione sulla base $\{|\rightarrow\rangle, |\leftarrow\rangle\}$ è completamente casuale. Effettuando la stessa misura sul proprio fotone, infine, Eve otterrà lo stesso risultato di Bob o un risultato opposto a seconda che le particelle dei due fossero nello stato $\left|\phi_{BE}^{(+)}\right\rangle$ o nello stato $\left|\phi_{BE}^{(-)}\right\rangle$. Siccome discriminare tra queste due alternative richiede la conoscenza del risultato della misura di Alice, che non è accessibile ad Eve, questa non ottiene alcuna informazione né sul bit di Alice né sul bit (casuale) di Bob.

Per quanto il ruolo svolto da Alice e Bob nel protocollo crittografico sia identico, il tentativo di intercettazione introduce un'asimmetria, in quanto è solo il fotone di Bob ad interagire col sistema di Eve. Lo stato $|\Xi\rangle$ rimane tuttavia inalterato, a meno di un fattore di fase globale, per scambio della particella di Alice con quella di Bob. In virtù di questo fatto l'effetto dell'intercettazione è il medesimo anche se la prima misura è compiuta da Bob. Un simile attacco causerà quindi un tasso di errore del 25% nella trasmissione della chiave, rivelando ad Eve in media la metà dei bit.

Codifica mediante stati non ortogonali

Analizziamo infine l'efficacia del dispositivo schematizzato in figura 14 nell'intercettazione di una chiave distribuita mediante il protocollo a stati non ortogonali proposto nel 1992 da C.H. Bennett, descritto a pagina 88 e seguenti.

Il protocollo crittografico in esame si basa sulla trasmissione di una sequenza di particelle preparate casualmente in uno di due stati $|u\rangle$ e $|v\rangle$ scelti in modo tale che $\langle u|v\rangle \neq 0$. Fissiamo la base computazionale del gate CONTROLLED-NOT in modo che si abbia

$$|u\rangle = |0\rangle \qquad \text{e} \qquad |v\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Bob può scegliere di misurare su ciascuna particella che riceve l'uno o l'altro dei proiettori

$$\mathrm{P}_{\neg u} = 1 - |u\rangle\langle u| = |1\rangle\langle 1|$$

e

$$\mathrm{P}_{\neg v} = 1 - |v\rangle\langle v| = \left|v^{\perp}\right\rangle\left\langle v^{\perp}\right|$$

con $\left|v^{\perp}\right\rangle = \beta^{*}|0\rangle - \alpha^{*}|1\rangle$. Un risultato positivo nella misura di $\mathrm{P}_{\neg v}$ indica a Bob con certezza che la particella era stata trasmessa nello stato $|u\rangle$; viceversa, un risultato positivo per $\mathrm{P}_{\neg u}$ segnala uno stato $|v\rangle$. I casi in cui il proiettore utilizzato non ha successo non sono significativi, in quanto forniscono un'informazione ambigua.

Supponiamo dapprima che Alice trasmetta uno stato $|u\rangle$. In assenza di interferenze sulla linea, questo verrà rivelato dal proiettore $\mathrm{P}_{\neg v}$ con probabilità

$$\langle u|\mathrm{P}_{\neg v}|u\rangle = \left\langle u\middle|v^{\perp}\right\rangle\left\langle v^{\perp}\middle|u\right\rangle = |\beta|^{2}.$$

In presenza del dispositivo di intercettazione, la particella di Alice interagisce col bit quantistico di Eve nel gate CONTROLLED-NOT come indicato:

$$|u\rangle_A|0\rangle_E \equiv |0\rangle_A|0\rangle_E \xrightarrow[C\text{–}NOT]{} |0\rangle_B|0\rangle_E \equiv |u\rangle_B|0\rangle_E .$$

Tale interazione non altera, evidentemente, la probabilità di successo del proiettore $\mathrm{P}_{\neg v}$; dopo la misura di Bob, inoltre, i bit di Eve rimane nello stato $|0\rangle$.

Consideriamo ora quanto accade quando Alice trasmette una particella nello stato $|v\rangle$. Nell'ipotesi che il canale non venga osservato la probabilità che lo stato sia rilevato dal proiettore $\mathrm{P}_{\neg u}$ è, anche in questo caso,

$$\langle v|\mathrm{P}_{\neg u}|v\rangle = \langle v|1\rangle\langle 1|v\rangle = |\beta|^2 .$$

Introducendo ora il dispositivo di intercettazione, ricaviamo lo stato complessivo delle particelle di Eve e Bob dopo che queste hanno interagito nel gate:

$$|v\rangle_A|0\rangle_E \equiv \left(\alpha|0\rangle_A + \beta|1\rangle_A\right)|0\rangle_E \xrightarrow[C\text{–}NOT]{} \alpha|0\rangle_B|0\rangle_E + \beta|1\rangle_B|1\rangle_E \equiv |\Xi\rangle .$$

La probabilità che Bob, operando con $\mathrm{P}_{\neg u}$ sulla propria particella, ne confonda lo stato con $|v\rangle$ è data da

$$\langle \Xi|\mathrm{P}_{\neg u} \otimes \mathrm{Id}|\Xi\rangle = \langle \Xi|\left[|1\rangle\langle 1| \otimes \left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)\right]|\Xi\rangle = |\beta|^2 ,$$

pari alla probabilità di rivelare uno stato $|v\rangle$ in assenza di intercettazione. La misura di Bob ha inoltre l'effetto di proiettare le due particelle sullo stato $|1\rangle_B|1\rangle_E$.

Riepilogando, abbiamo i seguenti due casi:

- Alice trasmette uno stato $|u\rangle$ e Bob misura $\mathrm{P}_{\neg v}$: se la misura ha successo Bob ritiene di avere ricevuto uno stato $|u\rangle$ ed il bit di Eve è lasciato nello stato $|0\rangle$.

- Alice trasmette uno stato $|v\rangle$ e Bob misura $\mathrm{P}_{\neg u}$: se la misura ha successo Bob ritiene di avere ricevuto uno stato $|v\rangle$ ed il bit di Eve è lasciato nello stato $|1\rangle$.

Queste considerazioni sembrano suggerire che Eve non abbia altro da fare che proiettare la propria particella sulla base computazionale $\{|0\rangle,|1\rangle\}$ per ottenere un'informazione completa sulla chiave, senza che Alice e Bob possano accorgersi di nulla. In realtà, se il proiettore $\mathrm{P}_{\neg u}$ non permette di discriminare uno stato $|v\rangle$ trasmesso inalterato dallo stato $|\Xi\rangle$ conseguente alla sua intercettazione, $\mathrm{P}_{\neg v}$ assume invece sui due stati un valor medio differente. Per definizione abbiamo infatti, essendo $\mathrm{P}_{\neg v}$ il proiettore sull'ortogonale di $|v\rangle$,

$$\langle v|\mathrm{P}_{\neg v}|v\rangle = 0,$$

per cui si presume che un successo di $\mathrm{P}_{\neg v}$ indichi la trasmissione di uno stato $|u\rangle$. Al contrario, però, si ha

$$\langle \Xi|\,\mathrm{P}_{\neg v}\otimes \mathrm{Id}|\Xi\rangle = \langle \Xi|\left[\left|v^{\perp}\right\rangle\!\left\langle v^{\perp}\right|\otimes\left(|0\rangle\langle 0|+|1\rangle\langle 1|\right)\right]|\Xi\rangle =$$

$$= \left|\left(\alpha^{*}\langle 0|_{B}\langle 0|_{E}+\beta^{*}\langle 1|_{B}\langle 1|_{E}\right)\left[\left(\beta^{*}|0\rangle-\alpha^{*}|1\rangle\right)\left(|0\rangle+|1\rangle\right)\right]\right|^{2} = 2|\alpha|^{2}|\beta|^{2}\neq 0.$$

Una particella trasmessa da Alice nello stato $|v\rangle$ ha dunque, per effetto dell'intercettazione, una probabilità non nulla $2|\alpha|^2|\beta|^2$ di essere rivelata da $\mathrm{P}_{\neg v}$ e portare quindi ad un bit errato nella chiave condivisa da Alice e Bob. Come è facile verificare riscrivendo $|\Xi\rangle$ in termini di $|v\rangle$ e $\left|v^{\perp}\right\rangle$, quando ciò si verifica la particella di Eve viene lasciata nello stato $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$, che le fornisce un bit casuale senza permetterle di stabilire che un errore si è effettivamente verificato.

Notiamo per inciso che una particella trasmessa da Alice nello stato $|u\rangle$ dà origine, come abbiamo visto, allo stato complessivo $|0\rangle_B|0\rangle_E$ sul quale il proiettore $\mathrm{P}_{\neg u}$ ha valore medio nullo; non è quindi possibile che Bob interpreti lo stato della particella come $|v\rangle$. Questa asimmetria dipende dalla scelta, totalmente arbitraria,

di identificare lo stato $|u\rangle$ con lo $|0\rangle$ della base computazionale del gate. Gli errori introdotti dall'intercettazione influiscono in questo caso sul numero di stati $|u\rangle$ che Bob crede di riconoscere, aumentandolo; siccome il protocollo prevede che Alice trasmetta particelle preparate con eguale probabilità in ciascuno dei due stati, l'effetto dell'intercettazione è facilmente rilevabile semplicemente sulla base di un conteggio delle frequenze. L'asimmetria negli errori introdotti può tuttavia essere rimossa "ruotando" casualmente, ad ogni particella trasmessa, la base computazionale del gate CONTROLLED-NOT in modo da rendere equiprobabili le identificazioni $|0\rangle \equiv |u\rangle$ e $|0\rangle \equiv |v\rangle$; un'altra possibilità, che qui non analizzeremo, consiste nello scegliere una base computazionale simmetrica rispetto agli stati $|u\rangle$ e $|v\rangle$.

Eliminata con questi accorgimenti l'asimmetria, un ulteriore effetto dell'intercettazione si manifesta, per Bob, nell'aumento della percentuale di particelle il cui stato egli crede di potere identificare con sicurezza. Nel caso che il canale non venga osservato, infatti, la probabilità di riconoscere ad esempio uno stato $|u\rangle$ è data da

$$\frac{1}{2}\langle u|\mathrm{P}_{\neg v}|u\rangle = \frac{1}{2}|\beta|^2,$$

prodotto delle probabilità si scegliere il proiettore adatto e di ottenere un risultato positivo della misura. Essendo identica la probabilità di riconoscere uno stato $|v\rangle$, la percentuale χ di particelle utilizzabili risulta essere $\frac{1}{2}|\beta|^2$. Nel caso però che sulla linea sia operante il dispositivo di intercettazione, una particella trasmessa in *uno solo* dei due stati (nella nostra descrizione lo stato $|v\rangle$ che il gate trasforma in $|\Xi\rangle$) ha in aggiunta una probabilità (pesata sulla scelta dei proiettori)

$$\frac{1}{2}\langle \Xi|\mathrm{P}_{\neg v}|\Xi\rangle = |\alpha|^2|\beta|^2$$

di entrare a far parte della chiave come bit errato. Questo conduce ad un aumento della frazione di particelle ritenute utilizzabili che diviene $\chi' = \frac{1}{2}|\beta|^2\left(1+|\alpha|^2\right)$, risultando così praticamente raddoppiata quando $|\alpha|^2 = |\langle u|v\rangle|^2 \approx 1$, ovvero nella condizione normale di impiego del protocollo con stati $|u\rangle$ e $|v\rangle$ quasi paralleli. L'insolita "efficienza" della comunicazione rivela ovviamente ad Alice e Bob il tentativo di intercettazione.

Notiamo infine che nonostante la probabilità

$$P(E) = \frac{1}{2}|\alpha|^2|\beta|^2 = \frac{1}{2}|\alpha|^2\left(1-|\alpha|^2\right)$$

che il dispositivo di Eve causi una ricezione errata dello stato di una specifica particella tenda a zero all'aumentare di $|\alpha|^2$ la percentuale di bit errati sul totale di bit della chiave, calcolabile come rapporto tra P(E) e χ', è

$$\frac{\frac{1}{2}|\alpha|^2|\beta|^2}{\frac{1}{2}|\beta|^2\left(1+|\alpha|^2\right)} = \frac{|\alpha|^2}{1+|\alpha|^2}$$

che tende ad ½ al tendere ad uno di $|\alpha|^2$, coerentemente col fatto che in tali condizioni $\chi' \approx 2\chi$.

Un problema aperto

Nei precedenti paragrafi abbiamo analizzato in qualche dettaglio l'efficacia del dispositivo di intercettazione quantistica descritto in figura 14 mettendolo a confronto con i tre principali protocolli di crittografia quantistica. Come abbiamo potuto constatare, in ciascuno dei casi l'interazione della particella trasferita da Alice a Bob con il sistema di Eve introduce nella trasmissione degli errori facilmente rilevabili dai due interlocutori; la segretezza della comunicazione viene in tale modo salvaguardata. a nostra trattazione non ha chiaramente alcuna

pretesa di generalità, tanto più in quanto nessun tentativo è stato compiuto per ottimizzare il dispositivo rispetto ad un particolare protocollo. Discussioni di altre strategie di attacco e stime del tasso di errore da esse introdotto sono reperibili in letteratura.

Il problema generale della sicurezza dei protocolli crittografici reali è ulteriormente complicato dalla necessità di utilizzare un codice di correzione d'errore per eliminare gli errori di trasmissione dovuti alla rumorosità del canale: la ridondanza così introdotta, se eccessiva, potrebbe infatti permettere ad Eve di acquisire informazioni sulla chiave. Una soluzione completa del problema richiederebbe in ogni caso l'analisi della percentuale d'errore minima introdotta da *tutte* le possibili strategie di intercettazione.

Tralasciando i problemi connessi col rumore, ci si può legittimamente domandare se l'inefficacia del dispositivo di intercettazione da noi analizzato non dipenda sostanzialmente dalla sua estrema semplicità, ed in particolare dalla bassa dimensionalità dello spazio di Hilbert del sistema a disposizione di Eve. Tutti i protocolli crittografici generano, durante la trasmissione, grandi quantità di informazione inutile, sotto forma ad esempio di misure delle osservabili errate che portano ad un bit casuale. Questa cospicua inefficienza è essenziale al funzionamento dei protocolli, in quanto ne garantisce la sicurezza contro l'osservazione classica del canale. Fatto salvo il fatto che l'interazione della particella in transito fra Alice e Bob con un altro sistema ne modifica lo stato e quindi in generale altera i risultati delle misure di Bob, è lecito chiedersi se non sia possibile progettare lo stato del sistema complessivo in modo che tali alterazioni interessino soltanto quelle misure che sarebbero comunque giudicate inconcludenti dai due interlocutori. Un approccio al problema potrebbe consistere nel tradurre i requisiti di "onniscienza" ed "invisibilità" di Eve in un sistema di equazioni che vincolino lo stato cercato. Tali equazioni risulterebbero verosimilmente essere incompatibili, escludendo così una soluzione esatta. Ai fini

pratici, tuttavia, delle soluzioni approssimate che rappresentassero una intercettazione abbastanza efficiente e poco rumorosa proverebbero comunque la vulnerabilità del protocollo crittografico in esame. Essendo il numero dei vincoli costante si può supporre che tali soluzioni approssimate, se esistono, siano tanto migliori quanto maggiore è il numero dei gradi di libertà, ovvero la dimensione d dello spazio di Hilbert del sistema utilizzato da Eve; sarebbe pertanto interessante studiare, in funzione di d, l'andamento della minima percentuale di bit errati introdotta dalle tecniche di intercettazione implementabili in uno spazio d-dimensionale.