Crittografia Quantistica

Sandro Tosi

17 settembre 2003

Sommario

In questo documento cercheremo di mostrare come l'introduzione di un futuro computer quantistico annulli le attuali tecniche crittografiche e come, sempre grazie alla meccanica quantistica, sia possibile lo scambio di una chiave in modo assolutamente sicuro, per poi essere utilizzata in un cifrario a chiave condivisa.

1 La crittografia moderna

La necessità di mantenere delle informazioni segrete è da sempre di fondamentale importanza per l'uomo e la crittografia, l'arte di creare codici, ha radici lontane nel tempo che affondano addirittura al tempo dei babilonesi; anche Cesare, in epoca romana, utilizzava un particolare codice per spedire i suoi messaggi in una forma che li rendesse illeggibili nel caso fossero caduti in mano nemica.

Ai giorni nostri, dove l'utilizzo di Internet ormai permea quasi ogni aspetto della vita quotidiana e dove molte informazioni non devono essere rivelate (siano esse numeri di carte di credito o progetti industriali), la crittografia ricopre un ruolo molto importante.

Un tempo, la segretezza dei sistemi di cifratura dipendeva in massima parte dalla segretezza delle procedure di cifratura e decifratura: Enigma, la macchina utilizzata dai tedeschi per codificare i messaggi e la cui rottura è stata di forte impatto per l'esito della Seconda Guerra Mondiale, ha chiarito che la sicurezza delle informazioni cifrate deve basarsi unicamente sulla segretezza della chiave; per questo, attualmente, le tecniche crittografiche si possono dividere in due categorie: quelle a *chiave condivisa* e quelle a *chiave pubblica*.

Nella crittografia a chiave condivisa mittente e destinatario, che chiameremo rispettivamente Alice e Bob[1], devono condividere una chiave tramite la quale possono cifrare e decifrare le informazioni. La chiave, però, deve essere

[1]Questi sono i nomi classici che compaiono in letteratura e che verranno usati anche in questo documento. Useremo anche la convenzione di chiamare l'attaccante col nome di Eva.

condivisa *prima* di spedire il messaggio vero e proprio, e questo a volte può non essere gradito.

Il problema maggiore che si incontra con questa tecnica crittografica è proprio la condivisione della chiave. Per risolvere questo inconveniente, sono stati pensati alcuni protocolli che consentono lo scambio della chiave in *relativa* sicurezza, ma la soluzione migliore è venuta con un nuovo tipo di cifrario, quello a chiave pubblica. Ogni utente possiede due chiavi, una pubblica ed una privata; la prima viene usata dagli altri utenti che vogliono comunicare con lui in segreto, mentre la seconda viene usata dall'utente per decodificare i messaggi cifrati.

Questo tipo di cifratura si basa su alcune assunzioni della teoria dei numeri sulla difficoltà di eseguire certe operazioni: RSA, per esempio, si basa sulla difficoltà di fattorizzare un numero intero molto grande per garantire che, pur conoscendo la chiave pubblica, non esista alcun modo computazionalmente efficiente per ottenere la chiave privata; la scoperta di un algoritmo efficiente o di un teorema matematico che risolva questo problema, porterebbe alla sua inutilità.

2 Cenni di meccanica quantistica e quantum computer

> *Anyone who is not shocked by quantum theory has not understood it.* Niels Bohr

In questa sezione cercheremo di fornire alcune informazioni riguardo la meccanica quantistica in modo da poter poi introdurre il concetto di *computer quantistico* e poter sviluppare un metodo di cifratura quantistica assolutamente sicuro.

All'inizio del secolo scorso si è iniziato a notare che il mondo dell'infinitamente piccolo (dell'ordine di molecole ed atomi) non si comporta come il mondo macroscopico, ma anzi, in una maniera alquanto bizzarra: per esempio, la luce può essere descritta sia come un'onda elettromagnetica sia come un fascio di corpuscoli, detti *fotoni*; come vedremo, questa dualità sarà utile in seguito, in quanto possiamo concepire un raggio di luce come un gran numero di fotoni che possiedono anche le caratteristiche tipiche delle onde.

Un risultato fondamentale di questa teoria, e che potremmo considerare un concentrato di tutta la fisica moderna, è il *Principio di Indeterminazione* di Heisenberg, il quale stabilisce che interagendo con un oggetto lo si modifica: più precisamente, "*ogni misura fatta su un sistema quantistico che estragga qualche informazione a riguardo di questo sistema, necessariamente disturba il sistema, anche se in misura molto piccola*". L'esempio classico è quello in cui si cerca di conoscere la velocità di una particella, e mentre si ottiene questa informazione, si perde completamente quella relativa alla sua posizione. Quantità di questo tipo, quelle cioè per cui più se ne conosce una e meno si ha certezza per l'altra, sono dette *coniugate*, *complementari* o *non ortogonali*.

La luce, si è detto, può essere analizzata anche come un'onda elettromagnetica, ed è quindi possibile descrivere come "vibra", la direzione dell'oscillazione dell'onda: è ciò che si chiama *polarizzazione* della luce. Per esempio, se l'onda oscilla lungo la direzione verticale, avremo una polarizzazione a 0 gradi, mentre se oscilla lungo la direzione orizzontale, la polarizzazione sarebbe a 90 gradi, e così via per le inclinazioni intermedie.

Normalmente, la luce che vediamo non ha una particolare polarizzazione, ed è in effetti emessa in tutte le angolazioni. Esistono particolari filtri, detti *filtri polarizzatori*, che consentono di selezionare una determinata polarizzazione della luce; un esempio di questi filtri sono le lenti Polaroid montate su alcuni occhiali da sole.

Un'idea molto particolare della meccanica quantistica è la seguente: finchè il comportamento di una particella è ignoto, tutto quello che essa può fare è autorizzata a farlo simultaneamente. Ogni possibilità è chiamata *stato* e poichè una particella può realizzare più stati si dice che essa si trova in una *sovrapposizione di stati*.

Per meglio chiarire questo concetto, il grande fisico Erwin Schrödinger ha escogitato il seguente esempio, detto del *gatto di Schrödinger*. Immaginiamo di collocare un gatto in una scatola. Due stati sono possibili: il gatto è vivo o morto. Quando mettiamo il gatto nella scatola vediamo che è vivo, quindi non ci troviamo in una sovrapposizione di stati. Mettiamo assieme al gatto anche una fiala di cianuro nella scatola e chiudiamola. Ci troviamo così in uno stato di ignoranza poichè non sappiamo se il gatto ha urtato la fiala, rompendola, e quindi sia morto oppure se sia ancora in vita: dal punto di vista classico ci sentiremmo di dire che il gatto si trova in uno stato ben preciso, o vivo o morto, anche se non sappiamo quale, mentre dal punto di vista quantistico il gatto si trova in una sovrapposizione di stati, sia vivo che morto.

L'incertezza permane solo nel periodo in cui l'oggetto è perso di vista; aprendo la scatola possiamo controllare lo stato del gatto: l'osservazione costringe l'oggetto in un unico stato.

2.1 Il computer quantistico

In un calcolatore classico il bit è l'unità fondamentale di elaborazione e può assumere i valori 0 oppure 1.

Un ipotetico computer quantistico, in quanto ubbidisce alle leggi della meccanica quantistica, opera su bit in stato di sovrapposizione tra 0 ed 1, i cosiddetti *qubit*. Un qubit, proprio come il gatto di Schrödinger, si trova in una sovrapposizione di stati finchè non ne viene chiesto il valore: a quel punto restituisce un valore.

Prendendo N qubit, possiamo immaginare che rappresentino tutti i numeri compresi tra 0 e $2^N - 1$: è proprio questa la potenza di un computer quantistico, in quanto è in grado di accettare come input non un solo valore, ma una sovrapposizione di molti valori differenti ed in seguito eseguire una computazione su tutti i numeri simultaneamente. In effetti potremmo guardare ad un quantum computer come ad un calcolatore massivamente parallelo.

3 Criptanalisi quantistica

Vogliamo qui evidenziare cosa potrebbe significare la futura introduzione di un computer quantistico per la crittografia attuale.

Un risultato eccezionale ottenuto da Peter Shor nel 1994 [Shor94] è stato quello di trovare un algoritmo efficiente per la fattorizzazione di numeri interi e per il calcolo del logaritmo discreto tramite l'uso di un calcolatore quantistico.

Due delle più importanti tecniche della crittografia attuale verrebbero a perdere della loro sicurezza una volta che questo algoritmo diventasse realizzabile: RSA sfrutta proprio la difficoltà di fattorizzare numeri interi molto grandi per garantire la sua sicurezza, ed il protocollo di scambio delle chiavi ideato da Diffie ed Hellman poggia le sue basi sulla difficoltà di calcolo del logaritmo discreto.

L'algoritmo di Shor consente di fattorizzare un numero in fattori primi in un numero di passi proporzionale al quadrato della lunghezza del numero (in simboli $\mathcal{O}((\log N)^2)$ dove N è il numero da fattorizzare), un notevole passo avanti rispetto agli algoritmi attuali; un esempio di algoritmo banale di fattorizzazione è il seguente: il nostro numero in esame è N con L cifre (quindi si ha $N \approx 10^L$) e lo dividiamo per $2, 3, \ldots, \sqrt{N}$ (possiamo naturalmente limitarci ai soli numeri primi tra 2 e $\sqrt{N}$) controllando il resto delle divisioni. Nel caso peggiore sono richieste $\sqrt{N} \approx 10^{\frac{L}{2}}$ divisioni, un numero che cresce esponenzialmente con la lunghezza di N.

Questo risultato è molto importante in quanto è da secoli che si cerca un modo efficiente per fattorizzare i numeri e, vista la difficoltà di questo compito, si ritiene che non sia possibile fare molto meglio dell'algoritmo banale su un computer classico.

Quello di Shor non è l'unico algoritmo quantistico esistente: nel 1996 Lov Grover ha trovato un modo [Grover97] per recuperare un elemento da una lista disordinata di N elementi in un tempo proporzionale a $\sqrt{N}$, contro un tempo proporzionale ad N per gli algoritmi classici; l'attacco a DES, il cifrario a chiave condivisa più utilizzato, richiede proprio la ricerca in una tabella di grandi dimensioni per essere portato a termine, e questo incremento prestazionale lo rende ancora più attuabile.

4 Crittografia quantistica

Sebbene l'avvento di un futuro computer quantistico renderà inutili le attuali tecniche crittografiche come DES ed RSA, one time pad rimane comunque un cifrario perfetto, anche dopo l'avvento di un dispositivo quantistico. Non abbiamo parlato ancora di questo cifrario, che sostanzialmente è un cifrario a chiave condivisa la cui peculiarità è l'utilizzo di una chiave lunga quanto il testo da cifrare e completamente casuale; il cifrario è provato essere *incondizionatamente sicuro*.

Come ben si può capire, il problema maggiore di questo cifrario è proprio la chiave, che deve essere nota a priori ad entrambi i comunicanti.

La crittografia quantistica, o come meglio si dovrebbe chiamare lo *scambio di chiavi quantistico*, mette a disposizione un metodo per risolvere il problema dello scambio delle chiavi tra Alice e Bob: tramite questo protocollo saranno in grado di scambiarsi su un canale non protetto una chiave casuale di lunghezza arbitraria in completa sicurezza con la certezza che ogni tentativo di intercettazione verrebbe rilevato inequivocabilmente.

La crittografia quantistica, a differenza di quella classica, basa la sua sicurezza sulle leggi della fisica piuttosto che su congetture sulla difficoltà di certe operazioni matematiche.

4.1 Il protocollo BB84

Descriveremo il protocollo ormai noto come BB84 (per una descrizione più dettagliata si veda [BB84], mentre per un articolo più introduttivo si veda [BBE92]) ideato da Bennett e Brassard nel 1984 e che consente lo scambio di una chiave in maniera sicura tra due utenti che *non* dispongono di alcuna informazione segreta in comune.

Supponiamo che Alice e Bob dispongano di due canali di comunicazione: uno quantistico (che consente la trasmissione di segnali basati su fenomeni quantistici e che solitamente è una fibra ottica) ed uno convenzionale, e che siano possibili intercettazioni passive su questi canali.

Le informazioni che Alice scambia con Bob sul canale quantistico sono singoli fotoni ad una determinata polarizzazione: possiamo scegliere, per semplicità, quelle orientate nelle direzioni $\updownarrow$, $\leftrightarrow$, $\nearrow$ e $\searrow$ che definiscono due basi $+$ e $\times$ non ortogonali tra loro: ciò significa che, per il Principio di Indeterminazione, non è possibile misurare contemporaneamente se la polarizzazione è diagonale o rettilinea.

Supponiamo che il modo di rappresentare i bit 0 ed 1 sia noto a priori, e comunque sul quale è possibile accordarsi pubblicamente senza bisogno di segretezza: potremmo immaginare uno schema come quello proposto in tabella 1.

Alice si appresta a spedire i propri dati nel seguente modo: sceglie casualmente se spedire un bit 0 o 1, sceglie sempre casualmente che base utilizzare

base	0	1
$+$	$\updownarrow$	$\leftrightarrow$
$\times$	$\swarrow\!\!\!\nearrow$	$\nwarrow\!\!\!\searrow$

Tabella 1: Esempio di rappresentazione binaria.

per spedire il bit, se $+$ o $\times$, e quindi prepara il fotone con la polarizzazione risultante e lo spedisce a Bob.

Bob, non essendo a conoscenza della base scelta da Alice per spedire i fotoni, sceglie casualmente quale utilizzare per rilevarne la polarizzazione: se è la stessa utilizzata per crearli, l'identificazione avverrà correttamente, mentre se è sbagliata Bob otterrà comunque un valore nella base scelta (se è quella rettilinea, otterrà un fotone con polarizzazione o verticale od orizzontale) perdendo però le informazioni del fotone originario.

Cerchiamo di spiegare meglio quest'ultimo punto; prendiamo per esempio un rivelatore di polarizzazione; se Bob decide di controllare se i fotoni hanno polarizzazione verticale, l'utilizzo di un filtro $+$ consente di avere due possibilità: il fotone è rilevato con polarizzazione verticale, oppure il fotone è rilevato con polarizzazione orizzontale in modo certo. Se la particella che Bob sta analizzando era stata spedita utilizzando proprio la base $+$ la misura che ha effettuato è corretta e rispecchia le informazioni di Alice, ma se invece era stato spedito con base $\times$ il fotone supererà comunque il filtro $+$, ma avrà una polarizzazione casuale e che non ha nulla a che vedere con quella con cui era stato spedito.

Raggiunto un numero adeguato di questi scambi, Alice smette di spedire fotoni. Dal momento che, mediamente, Bob avrà scelto la base sbagliata nella metà delle misurazioni, i due devono trovare un modo per ottenere la stessa stringa di bit: Bob, allora, annuncia pubblicamente sul canale convenzionale la lista delle basi da lui utilizzate per misurare i fotoni, ma *non* cosa ha misurato. A questa lista, Alice risponde indicando quali basi Bob ha utilizzato correttamente, ma *non* cosa ha spedito.

In questo modo, vengono a conoscenza di quali misurazioni sono state effettuate correttamente cosicché le altre possono essere scartate per mantenere solo le polarizzazioni per le quali hanno utilizzato la stessa base ed ottenere una chiave identica da entrambe le parti e *sicuramente* segreta, e che quindi potrà essere utilizzata per cifrare messaggi.

4.2 Un esempio

Cerchiamo di chiarire, con un esempio, il funzionamento del metodo di scambio delle chiavi appena visto; in tabella 2 sono elencati i vari passaggi di cui diamo una breve spiegazione:

1.	0	1	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1
2.	×	+	×	+	+	×	+	+	×	×	×	+	+	×	+	+	+	+
3.	⤢	↔	⤡	↕	↕	⤢	↔	↕	⤡	⤡	⤡	↕	↕	⤡	↕	↕	↔	↔
4.	+	+	×	×	+	×	+	+	+	+	×	+	×	×	+	×	+	×
5.	↔	↔	⤡	⤡	↕	⤢	↔	↕	↔	↔	⤡	↕	⤢	⤡	↕	⤡	↔	⤢
6.	1	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1	0
7.		*	*		*	*	*	*			*	*		*	*		*	
8.		1	1		0	0	1	0			1	0		1	0		1	

Tabella 2: Esempio di trasmissione della chiave

1. Alice sceglie casualmente una serie di bit da inviare a Bob;
2. Alice sceglie ancora casualmente una serie di basi con cui spedire i bit scelti;
3. i fotoni corrispondenti vengono creati da Alice e spediti;
4. Bob sceglie casualmente quale base utilizzare per esaminare il fotone in arrivo;
5. Bob memorizza i risultati delle osservazioni;
6. Bob trasforma le informazioni sulle polarizzazioni in una sequenza di bit;
7. Bob, per sincerarsi di avere la stessa chiave di Alice, le manda le informazioni sulle basi utilizzate per misurare i fotoni a cui Alice risponde indicando quali sono corrette;
8. infine, la chiave che possono utilizzare è ricavata come una sottosequenza della stringa originaria, quella per cui hanno usato le stesse basi.

4.3 BB84 in presenza di Eva

Finora abbiamo ignorato il caso in cui un attaccante sia in ascolto sul canale quantistico: vediamo dunque cosa questo comporta e come può essere *sempre* individuato dai comunicanti.

Eva cerca di ottenere informazioni sulla chiave che Alice e Bob si stanno scambiando: dal momento che le uniche informazioni che si scambieranno sul canale tradizionale sono le basi utilizzate, da queste informazioni Eva non può trarre niente di utile. È quindi costretta ad estratte qualche informazione dal canale quantistico, ma questa misurazione comporta una perturbazione del sistema.

Eva, infatti, non può far altro che comportarsi come Bob, cioè misurare i fotoni in transito sul canale quantistico scegliendo casualmente la base da utilizzare per misurarli. Ottenuti i valori Eva, per non essere scoperta subito, deve spedire a Bob dei fotoni, e lo fa secondo le informazioni ricevute.

Alla fine del protocollo descritto in precedenza, Alice e Bob hanno scartato le informazioni ottenute tramite basi che non corrispondono e credono di avere una chiave uguale. Dal momento che non si fidano del canale quantistico metto in pratica un metodo per verificare che effettivamente siano in possesso della medesima sequenza di bit: estraggono da questa un sottoinsieme di bit e li confrontano pubblicamente.

Durante il confronto controllano anche il tasso di errore: se questo è vicino al 25% allora possono essere sicuri della presenza di un estraneo sul canale; possono quindi ripetere lo scambio, pensando che l'intercettazione fosse solo momentanea, oppure possono abbandonare per il momento il protocollo.

Il motivo di questo è dato dal fatto che la presenza di Eva introduce un'ulteriore fonte di errore nel canale quantistico: immaginiamo che sia Alice che Bob abbiano utilizzato la base $+$, mentre Eva ha utilizzato la base $\times$; Eva, allora, avrà percepito sì un fotone con polarizzazione diagonale ma che avrà una valore casuale; rispedendo il fotone con questa polarizzazione, anche Bob otterrà un valore di polarizzazione verticale od orizzontale, ma il cui valore potrebbe non essere quello che Alice ha spedito.

Se, invece, la sequenza di bit estratta dalla stringa temporanea risulta uguale per entrambi, questa viene scartata e ciò che rimane è una chiave identica e sicura.

Il protocollo, però, risulta vulnerabile ad un attacco *man in the middle*, dove Eva agisce attivamente sul canale potendo poi intercettare e decodificare tutti i messaggi tra Alice e Bob.

Un altro attacco si basa sulle difficoltà tecniche di generare un singolo fotone: molto più facilmente viene generato un piccolo gruppo di fotoni; Eva, tramite l'uso di uno specchio semiriflettente, potrebbe catturare parte dei fotoni di ogni gruppo per ottenere informazioni sullo scambio della chiave, senza essere intercettata.

5 Conclusioni

I calcolatori quantistici sono ancora molto lontani dalla realtà; alcuni esperimenti hanno ottenuto dei risultati promettenti, come il gruppo di ricerca che è riuscito a fattorizzare il numero 15 facendo uso di 3 qubit: RSA è ancora al sicuro, ma questa è stata solo una dimostrazione di fattibilità dell'algoritmo e dimostra che non siano solo teorie.

Anche lo schema proposto da Bennett e Brassard è lungi dall'essere praticabile oggigiorno; già nel 1988, lo stesso Bennett (stanco di sentir parlare del suo metodo come funzionante solo in teoria), era riuscito a ottenere uno scambio completo di una chiave seguendo il suo protocollo, ma la distanza tra i due ricevitori era di appena 30 centimetri.

Solo ora si sono ottenuti risultati di trasmissione di informazioni quantistiche a 100 chilometri di distanza usando una singola fibra, una misura ancora troppo corta per un utilizzo pratico, ed il cui limite risiede fondamentalmente nel dover utilizzare una fibra unica. La strada che si sta cercando di percorrere è quella satellitare, che potrebbe consentire un utilizzo su più larga scala, ma di cui siamo solo agli inizi. Nonostante il metodo di trasporto, il protocollo è comunque molto *lento*, in quanto le tecnologie attuali non consentono una generazione rapida di fotoni.

Se, poi, proprio il fatto di non poter ottenere informazioni dal canale quantistico ci pone al riparo da eventuali intercettazioni, rende anche impossibile replicare le informazioni: risulta quindi impossibile "rinfreschare" le informazioni (quello che avviene normalmente sui doppini telefonici: si legge l'informazione per riscriverla sul canale in modo da contrastare l'attenuazione del segnale) e la connessione di diversi canali quantistici.

Nonostante questo, la crittografia quantistica si basa su principi fondamentali della meccanica quantistica piuttosto che su assunzioni non provate ed, inoltre, la sua sicurezza è stata provata (si veda, per esempio, [Mayers98]).

Nessuno degli attuali sistemi a chiave pubblica sopravviverà al calcolatore quantistico e nuovi metodi dovranno essere utilizzati: da oltre ottant'anni la meccanica quantistica sta rivoluzionando il nostro modo di comprendere la realtà, ed ora sta anche entrando nel mondo dell'informatica: possiamo ancora chiamarla solo "teoria"?

Riferimenti bibliografici

[Shor94] Peter W. Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer.* FOCS 1994. Disponibile presso `quant-ph/9508027`.

[Grover97] Lov K. Grover. *Quantum computers can search arbitrarily large databases by a single query.* Gennaio 1997. Disponibile presso `quant-ph/9706005`.

[BB84] Charles H. Bennett, Gilles Brassard. *Quantum cryptography: Public-key distribution and coin tossing* Dicembre 1994. Disponibile su "Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India" pp. 175 - 179.

[BBE92] Charles H. Bennett, Gilles Brassard, Artur K. Ekert. *Quantum cryptography.* Ottobre 1992. Disponibile presso "Scientific American", pp. 50 - 57; in edizione tradotta in italiano su "Le Scienze", Dicembre 1992, pp. 84 - 93.

[Ekert95] Artur K. Ekert. *Quantum cryptoanalysis - Introduction.* Disponibile presso `http://www.qubit.org/library/intros/cryptana.html`.

[deWolf99] Ronald de Wolf. *Quantum Computation and Shor's Factoring Algorithm.* Gennaio 1999. Disponibile presso `http://www.cwi.nl/~rdewolf/publ/qc/survey.ps.gz`.

[Mayers98] Dominic Mayers. *Unconditional security in Quantum Cryptography.* Febbraio 1998. Disponibile presso `quant-ph/9802025`.

[Caboom00] Caboom. *Quantum Cryptography* Gennaio 2000. Disponibile presso `http://acksyn.infosecwriters.com/caboomquantum.htm`.

[Brassard93] Gilles Brassard. *A Bibliography of Quantum Cryptography.* Dicembre 1993. Disponibile presso `http://www.enricozimuel.net/documenti/QCbib.ps`

[BBBSS91] Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, John Smolin. *Experimental Quantum Cryptography.* Settembre 1991. Disponibile presso `http://www.enricozimuel.net/documenti/BBBSS92.ps`.

[CG96] Rosario Cretella, Gerardo Gioiella. *Crittografia quantistica* Maggio 1996. Disponibile presso `http://www.enricozimuel.net/documenti/quantum_cryptography.ps`.

[Vittorio02] Salvatore Vittorio. *Quantum Cryptography: Privacy Through Uncertainty.* Ottobre 2002. Disponibile presso `QuantumCryptography:PrivacyThroughUncertainty`.

[Gold96] Sharon Goldwater. *Quantum Cryptography and Privacy Amplification.* Ottobre 1996. Disponibile presso `http://www.ai.sri.com/~goldwate/quantum.html`.

[Singh99] Simon Singh. *Codici & segreti.* Aprile 2001. Disponibile presso la collana "BUR Saggi".

[Lomonaco] Samuel J. Lomonaco, Jr. *A talk on quantum cryptography or How Alice outwits Eve* Disponibile presso `http://www.csee.umbc.edu/~lomonaco/ams/lecturenotes/SamCrypto.pdf`.