La crittografia quantistica

Autori: Maria Welleda Baldoni, Ciro Ciliberto, Giulia Maria Piacentini Cattaneo

Sottotitolo:

Nel numero 49 della "Lettera" è apparso un articolo di Renato Betti, dal titolo "Invito alla Crittografia". È stato seguito, nel numero 52, dall'articolo "Primi e Segreti" di Stefano Leonesi, Sonia L'Innocente, Marika Marconi e Carlo Toffalori. Sono contributi che forniscono ai lettori un'introduzione ai metodi e modelli matematici che intervengono nella crittografia classica e in quella a chiave pubblica. Il presente articolo è invece dedicato a una nuova frontiera: la crittografia quantistica.

Crittografia e Fisica quantistica

La crittografia quantistica si basa su idee che hanno origine dalla *Fisica quantistica*. Il contributo di questa disciplina alla crittografia è duplice e di segno contrastante: distruttivo, in un certo senso; costruttivo in un altro.
Gli sviluppi della Fisica quantistica rendono, infatti, teoricamente possibile la creazione di un computer di tipo completamente diverso e innovativo rispetto a quelli classici, il cosiddetto *computer quantistico*. Se realizzato in pratica, sarebbe in grado di effettuare in tempo *polinomiale* calcoli svolti da un computer classico in tempo *esponenziale*. Questo renderebbe vulnerabile ogni attuale sistema crittografico, mettendo in serio pericolo sistemi di sicurezza civili, militari, bancari ecc. Il risultato potrebbe essere il collasso della nostra stessa civiltà, in gran parte basata su tali sistemi di sicurezza.
D'altro canto, le stesse idee su cui poggia il concetto di computer quantistico portano a concepire e realizzare *sistemi crittografici quantistici* assolutamente inattaccabili, anche da un eventuale computer quantistico, con la sorprendente capacità di scoprire se eventuali malintenzionati hanno solo tentato – anche senza riuscirvi del tutto – di intromettersi abusivamente in una comunicazione riservata.
La Fisica quantistica, sviluppatasi nel secolo scorso, è la branca più recente della Fisica. Parte dall'osservazione che le leggi della Fisica prevalentemente *deterministiche*, valide per la spiegazione dei fenomeni *macroscopici*, non sembrano potersi applicare con successo ai fenomeni *microscopici*. Si è trattato, da parte dei fisici, di concepire modi completamente nuovi – talvolta apparentemente bizzarri – contrari alla naturale intuizione e spesso controversi, di guardare ai fenomeni che riguardano il *molto piccolo*. In aggiunta, per la trattazione dei fenomeni in questione, si sono costruiti dei modelli matematici assai raffinati che giocano un ruolo basilare nella crittografia quantistica. Il futuro è ormai cominciato. La teoria, se non la pratica, dei computer quantistici è già sviluppata. Inoltre sono già disponibili, sebbene per ora solo su piccola scala, efficaci sistemi crittografici quantistici.

Per ulteriori letture di carattere divulgativo su questi argomenti, consigliamo [6], [7], [11], [14], cap. 8.

Una prima incursione nel mondo quantistico: l'esperimento di Young

Nella Meccanica classica, la posizione di un punto o di una particella è descritta dal vettore x delle sue coordinate in dato un sistema di riferimento dello spazio. Il vettore $x = x(t)$ è funzione del tempo t e soddisfa un sistema di equazioni differenziali, le *equazioni del moto*. Il problema fisico

classico è quello di determinare il moto del punto, ossia la funzione $x(t)$, una volta noto il suo valore e quello di alcune sue derivate nell'*istante iniziale* $t = t_0$. Come è noto dall'Analisi (sotto opportune condizioni), di solito verificate per sistemi fisici ragionevoli, le equazioni del moto hanno una e una sola soluzione che verifichi date condizioni iniziali. Ciò significa che il moto della particella, e dunque in particolare la sua posizione e la sua velocità in ogni istante, sono determinati dalle informazioni che abbiamo sulla particella in un dato istante. Per questo motivo si dice che la Meccanica classica è *deterministica*: tutto, nel suo ambito, viene *univocamente determinato* dalle condizioni iniziali.
Questo modello, valido per sistemi macroscopici, cade in difetto per i sistemi molto piccoli, ad esempio per le particelle elementari le quali sono governate da leggi di natura probabilistica, piuttosto che deterministica. Questo è l'oggetto della Fisica quantistica.

Cominciamo il nostro viaggio nel mondo della Fisica quantistica da molto lontano e cioè da un esperimento effettuato da uno scienziato inglese della fine del XVIII secolo, Thomas Young di Cambridge. All'epoca era in corso, tra i fisici, un serrato dibattito: la luce è un fenomeno *particellare* o *ondulatorio*? Quelli che propendevano per la prima possibilità sostenevano che la luce era composta da particelle, dette *fotoni* che, viaggiando nello spazio, colpiscono gli oggetti e, per dirla rozzamente, li illuminano. I sostenitori della teoria ondulatoria ritenevano invece che la luce fosse, in modo analogo al suono, trasportata da onde che si propagano nello spazio. La moderna Fisica quantistica, tagliando la testa al toro, ha dato ragione ad entrambe le teorie: è vero che la luce si compone di singole particelle, i fotoni, i quali però hanno anche un comportamento ondulatorio. La nostra percezione della luce come fenomeno ondulatorio o particellare, dipende dalle circostanze.
Questo apparente paradosso fa parte di un'inevitabile ambiguità, detta *dualità onda-particella* che è un caso particolare del cosiddetto *Principio di indeterminazione di Heisenberg*. Formulato negli anni '20 del secolo scorso, è la pietra angolare della Fisica quantistica, in quanto ne marca la profonda differenza rispetto al determinismo della Meccanica classica. Afferma, in forma qualitativa, che *vi sono coppie di proprietà osservabili di un sistema fisico microscopico, dette coniugate, come la posizione e la velocità, o l'energia e il tempo, che non si possono entrambe determinare o misurare in modo esatto allo stesso tempo*. In altri termini, la misurazione di una delle due proprietà coniugate altera irrimediabilmente l'altra. Tale alterazione, con conseguente impossibilità di contemporanea misurazione accurata di proprietà coniugate, non dipende dalle scarse capacità dei nostri sistemi di misurazione, ma è un'obiettiva impossibilità (che ha una dimostrazione matematica).
Per ora torniamo a Young, che era ben lontano dal pensare al *Principio di indeterminazione*. Con il suo esperimento, invece, riuscì a dare una convincente evidenza al carattere ondulatorio della luce. Come pare che capiti talvolta ai fisici inglesi – si pensi alla mela di Newton – l'idea, gli venne mentre era in un momento di *relax* a godersi la natura. Al contrario di Newton, Young non era però sotto un melo, ma in riva a un laghetto. Vide allora partire dalla riva due cigni che procedevano nuotando parallelamente l'uno all'altro. Young osservò che ciascuno dei due cigni lasciava dietro di sé due semicerchi di onde, le quali interferivano e formavano sulle calme acque del laghetto un disegno molto particolare. Esso era dovuto al fatto che, laddove due creste d'onda si incontravano, si formava una cresta più alta (di ciascuna delle due), laddove due avvallamenti si incontravano, si formava un avvallamento più basso di ciascuno dei due di partenza; se infine si incontravano una cresta e un avvallamento, essi si cancellavano a vicenda. Tutto ciò non ha niente di particolare. Si tratta di una scena alla quale, con ogni probabilità, ognuno di noi ha avuto modo di assistere. Quello che la rese molto interessante per Young fu che si ricordò, in quel momento, di aver già visto *esattamente lo stesso disegno* quale risultato di un esperimento ottico. L'esperimento funzionava nel modo seguente (cfr. Figura 1).

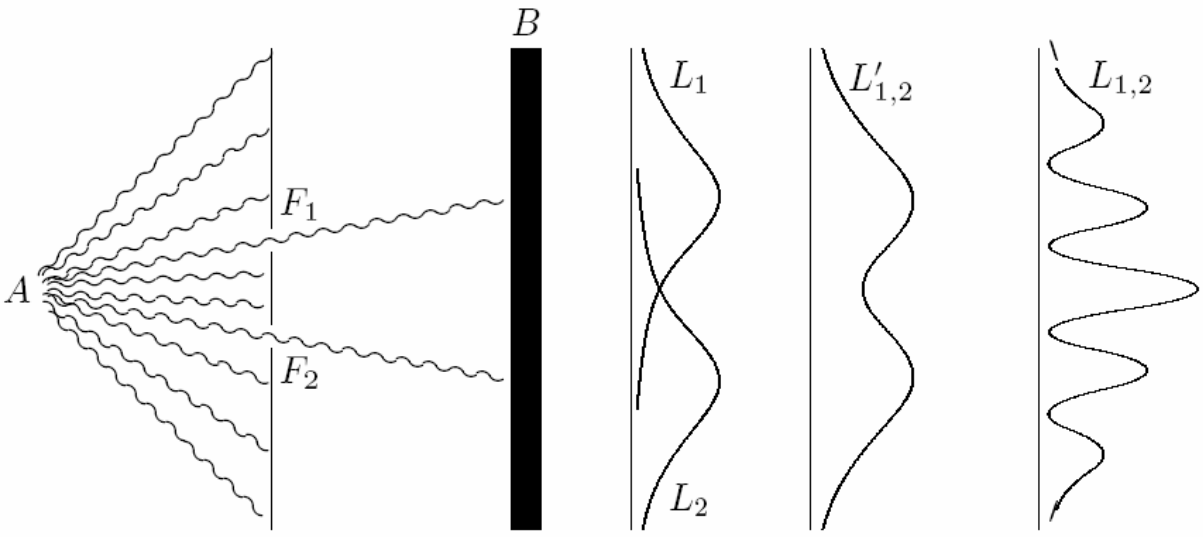

FIGURA 1. Esperimento di Young

Supponiamo di avere una sorgente di luce A posta davanti a una parete opaca con due piccole fenditure F_1 e F_2, al di là della quale c'è un'altra parete B che funge da schermo. La distribuzione della luce sullo schermo non è altro che la distribuzione dei fotoni assorbiti dalla parete B. Il grafico di tale distribuzione è una superficie, di cui in Figura 1 vediamo la sezione curvilinea data dalle curve L_1, L_2 e $L_{1,2}$. La curva L_1 descrive la distribuzione nel caso in cui la fenditura F_1 sia aperta e F_2 sia chiusa; la curva L_2 descrive la distribuzione nel caso in cui la fenditura F_2 sia aperta e F_1 sia chiusa. Stando alla Meccanica classica, e pensando alla luce come un fenomeno particellare (ossia pensando alla propagazione dei fotoni), Young si sarebbe aspettato che, nel caso in cui le due fenditure fossero entrambe aperte, la distribuzione degli elettroni segua l'andamento della curva $L'_{1,2}$ che è la *somma* di L_1 e L_2. Invece, l'esperimento mostrava che ciò non è vero: la distribuzione veniva descritta dalla curva $L_{1,2}$ e il relativo disegno sullo schermo era esattamente quello formato dalle onde lasciate dai cigni sul laghetto!

Questa, per Young, era la *prova definitiva* della natura ondulatoria della luce: i raggi luminosi che passano per le fenditure F_1 e F_2 si comportano esattamente come le onde lasciate sul laghetto dai due cigni e, per questo motivo, l'immagine sullo schermo è analoga al disegno formato dalle onde.

Fin qui, la Fisica quantistica sembra entrarci poco: in fin dei conti, con Young, siamo nel 1799 ben prima della nascita dei quanti e di Heisenberg. Tuttavia c'è un modo *moderno* di ripetere l'esperimento, che fa uso della più recente tecnologia, e che dà dei risultati davvero sorprendenti. Possiamo infatti emettere, a partire dalla sorgente luminosa A, *singoli fotoni* – diciamo uno al secondo – a una velocità assegnata ma con direzione variabile, in modo casuale, in un certo settore angolare D (come mostrato in Figura 1). Ogni fotone viaggia da solo verso la prima parete, qualcuno passa attraverso la fenditura F_1, qualche altro passa per la fenditura F_2, altri non passano per nessuna delle due e il tutto avviene in modo assolutamente casuale. Il nostro occhio non è in grado di *vedere* un singolo fotone, ma ci sono dei rivelatori di fotoni che possiamo mettere in azione sullo schermo B. Facciamo andare avanti l'esperimento per alcune ore, finché non siano passati tanti fotoni quanti ne erano passati con l'originario esperimento di Young fatto con una fonte luminosa sostanziosa, come una candela o una lampadina. Che immagine ci aspettiamo di vedere sullo schermo? L'immagine che vedevamo nell'esperimento originario di Young era causata dall'*interazione*, di natura ondulatoria, di più fotoni tra loro. Qui, poiché i fotoni viaggiano *indipendentemente* l'uno dall'altro, non c'è alcuna ragione per cui essi debbano interferire e dunque

non ci aspettiamo di vedere la stessa immagine. Se crediamo alla Meccanica classica, ci aspetteremmo piuttosto di vedere sullo schermo due zone luminose e cioè le proiezioni su *B*, a partire da *A*, delle fenditure F_1 e F_2. Invece - colpo di scena! - il risultato di questo secondo esperimento *è del tutto analogo* a quello dell'esperimento originario di Young. Questo è assolutamente inspiegabile nell'ambito della Meccanica classica.
La spiegazione del fenomeno presentata dalla Fisica quantistica è, invece, quella della cosiddetta *sovrapposizione di stati*. Interpretazioni alternative, basate ad esempio sull'esistenza di *universi paralleli* o *multiversi*, o di *variabili nascoste*, non hanno ricevuto alcuna verifica sperimentale. La spiegazione che daremo sarà per il momento intuitiva. Un cenno all'apparato matematico, che fornisca il relativo modello, verrà posposta successivamente.
Di una cosa possiamo essere certi: ogni fotone parte da *A* e, se passa da una delle due fenditure F_1 o F_2, allora arriva sullo schermo *B*. Tutto quello che accade nell'intervallo tra la partenza del fotone da *A* e il suo arrivo su *B* è per noi un mistero che non appare regolato da leggi deterministiche, ma da quelle della probabilità . In sostanza, il fotone ha uguale probabilità di passare per F_1 o F_2, e, per quanto appaia bizzarro, possiamo assumere il punto di vista che passi *sia* per F_1 *che* per F_2, interagendo, in tal modo, con se stesso e dunque determinando l'effetto ondulatorio che si manifesta nell'esperimento di Young. Ciascuna delle due possibilità – il passaggio da F_1 o F_2 – si chiama uno *stato* del fotone e, poiché stiamo supponendo che nella fase intermedia del passaggio da *A* a *B*, nella quale non interveniamo con osservazioni, si verifichino in qualche modo contemporaneamente i due stati, questo spiega la terminologia di *sovrapposizione di stati*. Per quanto strano sia questo punto di vista, esso può formalizzarsi matematicamente e porta ad una spiegazione del risultato dell'esperimento di Young. In definitiva, la sovrapposizione di stati è un modo di descrivere un oggetto durante un periodo di ambiguità, durante il quale non effettuiamo delle osservazioni o misure.
Va da sé che, nel momento in cui effettuiamo un'osservazione o una misura atta a chiarire quale sia l'effettivo stato del fotone, allora l'ambiguità cessa e di conseguenza cessa la sovrapposizione degli stati. Questo, in accordo con il *Principio di indeterminazione*, *modifica* irreversibilmente il sistema stesso. Ci aspettiamo pertanto che, se ripetiamo l'esperimento di Young in modo tale da misurare per quale delle due fenditure ciascun elettrone passa, questo stesso atto modifichi il risultato dell'esperimento. Per assurdo che possa sembrare, questo è in effetti ciò che accade. In questo secondo caso, infatti, la distribuzione dei fotoni assorbiti dallo schermo *B* non appare più regolata dalla curva $L_{1,2}$ bensì dalla curva $L'_{1,2}$: un po' come se, nell'osservare e misurare la traiettoria dei fotoni, li trattassimo come particelle con moto regolato dalla Meccanica classica, ottenendo per risultato appunto quello previsto dalla Meccanica classica!

Il computer quantistico

Vediamo in che modo l'esperimento di Young e la sua strana spiegazione può portare a concepire un *computer quantistico*, capace di effettuare calcoli con rapidità tale da ridurre un tempo di calcolo esponenziale a uno polinomiale.
L'idea è dovuta ad un fisico inglese, David Deutsch, che introdusse il concetto nel 1984 (cfr. [8],[9]) partendo dall'osservazione che i computer classici operano usando le leggi della Fisica classica, mentre sarebbe stato desiderabile avere computer operanti mediante le leggi della Fisica quantistica in quanto queste possono giovare nell'effettuare più rapidamente delle operazioni. Vediamo come.
Se un computer classico deve esaminare un problema che richiede l'effettuazione di un certo numero di verifiche, esso procede in *modo seriale*. Si pensi ad esempio alla fattorizzazione di un numero intero positivo *n*. Il computer procede usando il crivello di Eratostene. Anzitutto divide *n* per 2, poi per 3, e così via fino a dividerlo, se necessario, per $[\sqrt{n}]$. È esattamente questa serialità la responsabile della crescita esponenziale del tempo di calcolo. Per contro, se si dispone di un computer quantistico, si può immaginare di usare il principio della sovrapposizione degli stati per evitare di specificare in modo seriale i numeri da 2 a $[\sqrt{n}]$. In sostanza, così come il fotone

dell'esperimento di Young, se non viene osservato, si trova in una situazione di sovrapposizione di stati nel passaggio da *A* a *B*, allo stesso modo possiamo immaginare un computer nel quale, mentre si effettua il calcolo e questo non è disturbato da fattori esterni, l'input sia suscettibile di assumere, allo stesso tempo, una serie di valori numerici, come fosse una variabile anziché un numero. In tal modo, il computer quantistico che dunque lavorerà, piuttosto che con i soli *bit* con dei *bit quantici* o *qubit*, potrebbe riuscire a fattorizzare il numero *n* procedendo non in modo seriale, ma effettuando *una sola operazione di divisione*. Questo evidentemente riduce il tempo di calcolo per il crivello di Eratostene, dall'esponenziale al polinomiale.

Questa, che sembra pura fantasia, almeno da un punto di vista teorico non lo è affatto. Basta infatti usare le proprietà delle particelle elementari e la loro Fisica quantistica per rappresentare i numeri e operare su di essi. L'idea è la seguente. Molte particelle elementari posseggono una proprietà osservabile – detto *spin* – che è, in senso lato, analogo al momento angolare di una pallina macroscopica che ruoti attorno ad un suo asse. È bene sottolineare le parole *in senso lato*, avvertendo che l'analogia tra le particellle elementari e le palline macroscopiche non va portata troppo in là . In ogni caso, alcune particelle dette *fermioni* hanno uno *spin* semintero e, tra queste, alcune – come gli elettroni – hanno *spin* di valore assoluto 1/2. Il valore dello *spin*, cioè di questo *momento angolare intrinseco*, se calcolato in relazione ad un determinato asse orientato, che chiameremo asse *z*, può assumere i valori S_z=1/2 e S_z= –1/2, corrispondenti, intuitivamente, a una *rotazione destrorsa* o *sinistrorsa*. Consideriamo dunque una particella p siffatta e decidiamo che essa rappresenti 0 se ha *spin* destrorso, mentre rappresenti 1 se ha *spin* sinistrorso. Se prendiamo *h* particelle di questo tipo p_1, ..., p_h e le poniamo in altrettante scatole distinte, numerate da 1 a *h*, e non comunicanti tra loro, in modo che non interferiscano l'una con l'altra, procedendo nel modo suddetto possiamo rappresentare tutti i numeri con *h* cifre binarie, cioè tutti i numeri da 0 a 2^h-1. Per rappresentare numeri diversi, dobbiamo dare alle particelle diverse componenti dello *spin* S_z lungo l'asse *z*. Ciò si può realizzare sottoponendo la particella ad un impulso di energia: se questo è sufficientemente elevato, la particella cambia il suo *spin*, altrimenti conserva lo *spin* che ha. Tuttavia noi vogliamo usare il principio della sovrapposizione di stati, affinché la particella abbia, in senso quantistico, la possibilità di avere contemporaneamente diverse componenti S_z dello *spin*. A tal fine, chiudiamo ciascuna particella nella sua scatola, e dunque non la osserviamo. Sottoponiamo poi ogni singola particella ad un impulso di energia non troppo forte né troppo debole, ma casuale. In tal modo ogni particella entra in una sovrapposizione di stati e rappresenta *contemporaneamente* 0 o 1. Questo è un *qubit*. Ora un numero formato da *h qubits* è un numero *quantico* che è, in sostanza, un qualunque numero tra 0 e 2^h-1. Se riusciamo ad operare con tali numeri, abbiamo risolto (almeno in via teorica) il problema della costruzione del computer quantistico.

Questo è, in sostanza, il contributo di Deutsch che lascia aperto un problema teorico importante e molti problemi pratici immensi. Il problema teorico è quello di immaginare degli algoritmi che effettivamente funzionino, almeno in linea di principio, su una macchina come un computer quantistico. Questo problema è stato risolto da Peter Shor nel 1994 (cfr. [13]), che ha trovato, tra l'altro, degli algoritmi per la fattorizzazione di grandi interi in tempo polinomiale su un computer quantistico.

La combinazione dei risultati di Deutsch e di Shor sembrerebbe devastante per la crittografia: tutti i sistemi crittografici, come ad esempio, il sistema a chiave pubblica *RSA*, basati sulla difficoltà di fattorizzare numeri grandi, sarebbero dunque inaffidabili e potrebbero essere facilmente elusi usando un computer quantistico? La risposta è sì ma, per ora, solo da un punto di vista *teorico*. I problemi pratici, connessi alla realizzazione dei computer quantistici, sembrano al momento difficili da sormontare. In particolare, un computer quantistico – per poter funzionare – deve essere rigorosamente isolato dall'esterno (isolamento in pratica impossibile da ottenere, allo stato delle nostre conoscenze). Questo problema, detto della *decoerenza quantistica*, come altri connessi al calcolo quantistico, è tra i più studiati dai fisici e non è escluso che venga prima o poi risolto. Tuttavia non è facile stimare quando. Certo, il giorno in cui verrà realizzato un computer

quantistico, tutti i sistemi crittografici che più o meno consapevolmente usiamo ogni giorno saranno eludibili e questo porrà in serio pericolo la nostra sicurezza.
Come vedremo tra breve, le idee stesse che portano ai computer quantistici conducono però anche ad una crittografia quantistica inattaccabile. Di questo discuteremo nei prossimi paragrafi.

Il cifrario di Vernam

Prima di discutere di crittografia quantistica, torniamo per un momento in ambito classico e diamo al lettore una buona notizia. Esistono cifrari assolutamente inattaccabili dal punto di vista teorico. Perché allora non si usano sempre? Ogni cosa a suo tempo: prima spieghiamo come sono fatti questi cifrari, poi risponderemo a questa naturale domanda. Infine, vedremo come la crittografia quantistica possa fornire un metodo per un uso ragionevole ed effettivo di tali cifrari.
Il cifrario di cui stiamo parlando è il cosiddetto *cifrario di Vernam*, cui si fa cenno anche nell'articolo di Betti che abbiamo citato all'inizio. Porta il nome di Gilbert S. Vernam, impiegato della Compagnia dei Telefoni degli Stati Uniti che, insieme al maggiore dell'esercito Joseph O. Mauborgne, lo propose durante la prima guerra mondiale. Nel suo fondamentale lavoro [12], C. E. Shannon ha dimostrato che i cifrari di Vernam sono inattaccabili alla crittoanalisi e che inoltre ogni cifrario inattaccabile alla crittoanalisi è un cifrario di Vernam. In altri termini, esiste un unico sistema crittografico perfettamente sicuro e questo è il cifrario di Vernam.
Vediamo di che si tratta. Questo cifrario viene anche detto *one time pad*. In inglese *pad* significa *blocco-notes*. Il motivo del nome risiede nel fatto che la chiave di cifratura veniva scritta agli interessati – ricevente e trasmittente – sui fogli di un blocco-notes, e non era riutilizzabile: era utilizzata una sola volta, cioè *one time*.
Il sistema è molto semplice. Il mittente e il ricevente hanno una stessa chiave, la quale deve soddisfare le seguenti proprietà:

(1) avere la stessa lunghezza del messaggio da trasmettere;
(2) essere una sequenza completamente casuale di caratteri;
(3) non essere mai riutilizzata.

In queste ipotesi, non è necessario scegliere una funzione di cifratura complicata: si può utilizzare una funzione semplice come, ad esempio, l'addizione o la sottrazione. Ad esempio, se si sceglie l'alfabeto binario {0,1} costituito dalle due cifre 0 e 1, si può definire un cifrario di Vernam nel seguente modo.
Sia $m = m_1 m_2 \ldots m_r$ un messaggio binario da inviare. Sia $K = k_1 k_2 \ldots k_r$ la chiave, che è una stringa binaria della stessa lunghezza del messaggio, costituita da cifre casuali. La cifratura consiste nel sostituire il messaggio m col messaggio $c = c_1 c_2 \ldots c_r$ dove:

$$c_i = m_i + k_i \pmod 2,\ i = 1, \ldots r.$$

La chiave non deve essere più riutilizzata.
Ad esempio, supponiamo che il messaggio da inviare sia 01001 e che la chiave sia 11010. Il messaggio crittato sarà 10011.
Spieghiamo ora perché i cifrari di Vernam sono inattaccabili. Il motivo sta nella casualità dei caratteri che compongono la chiave. Infatti, chi non possiede la chiave e volesse decifrare il messaggio potrebbe, in linea di principio, tentare con ogni possibile chiave. Questa operazione ha una enorme complessità computazionale, in quanto il numero di chiavi cresce come un fattoriale al crescere della lunghezza r del messaggio. Tuttavia non è solo questo il motivo per cui il cifrario è inattaccabile. Abbiamo visto infatti che, con un possibile futuro avvento dei computer quantistici, problemi di calcolo di questo tipo potrebbero non essere più rilevanti. La vera ragione dell'inattacabilità del cifrario sta nel fatto che, a causa dell'arbitrarietà della chiave, si otterrebbero,

nel fare la suddetta analisi, tutti i possibili testi in chiaro di lunghezza *r*. Inoltre, per la casualità della chiave, tutti questi testi in chiaro sarebbero ugualmente probabili e dunque sarebbe impossibile optare per l'uno o l'altro di questi.
Ad esempio, tornando all'esempio precedente, una volta ottenuto il messaggio crittato 10011, la crittoanalisi che abbiamo proposto (che è l'unica possibile) dà come risultato che i messaggi in chiaro 00000, 00001, 00011, 00111, ecc., sono tutti ugualmente probabili!
È tuttavia fondamentale che la chiave non sia mai riutilizzata. Infatti, se chi spedisce facesse il fatale errore di usare di nuovo la stessa chiave, allora il cifrario presterebbe il fianco agli strali della crittoanalisi. Ad esempio, se nel caso già esaminato, il mittente utilizza ancora la chiave 11010 per crittare anche il messaggio 01101, il crittoanalista intercetta la prima volta il messaggio 10011, la seconda 10111 e da ciò deduce che i due messaggi in chiaro hanno lettere uguali in tutti i posti tranne che nel terzo. Supponiamo che il crittoanalista sappia che nessun messaggio in chiaro può iniziare e finire con la stessa cifra. Ne dedurrà che la chiave inizia e finisce con cifre diverse. Non è una grande informazione, ma è già qualcosa. Se il mittente va avanti a riutilizzare la chiave, il crittoanalista – usando idee simili – prima o poi finisce per scoprirla.
Come abbiamo già detto, questo cifrario, altrimenti inattaccabile, deve avere un tallone d'Achille. In caso contrario sarebbe universalmente usato con grande sicurezza e soddisfazione generale. I punti deboli ci sono e sono assai sostanziosi.
Il primo – non il principale – consiste nella generazione delle chiavi. Devono essere opportunamente lunghe per consentire lo scambio di messaggi sufficientemente articolati; debbono essere casuali e, visto che non possono essere riutilizzate, occorre produrne tante per aver modo di comunicare frequentemente. La generazione di numeri causali non è un problema banale dal punto di vista dell'Informatica e, a maggior ragione, non lo è la generazione di tante lunghe stringhe di numeri casuali.
Ma, come abbiamo detto, non è questo il problema principale del cifrario di Vernam. Il problema maggiore è il seguente: per comunicare in tutta sicurezza usando un cifrario di Vernam, occorre aver preventivamente inviato la chiave attraverso un canale che deve essere assolutamente sicuro. In altre parole, prima di potere comunicare in segreto occorre poter comunicare la chiave in segreto. Tuttavia, la chiave ha la stessa lunghezza del messaggio che dobbiamo inviare e dunque abbiamo il classico caso del serpente che si mangia la coda.
In definitiva, gli unici cifrari teoricamente sicuri – ossia i cifrari di Vernam – sono molto difficilmente utilizzabili in pratica. Infatti, sono stati usati ben poche volte: ad esempio, per le comunicazioni tra Casa Bianca e Cremlino laddove le chiavi sono state trasportate a mano e guardate a vista, in tutta sicurezza, dall'una all'altro. Si capisce che, nella gran parte dei casi, non si può ricorrere a questi sistemi e si utilizzano dei metodi, come l'*RSA* che, sebbene non teoricamente inattaccabili, offrono in pratica un ragionevole grado di sicurezza.
Resta tuttavia il fatto che, se si riuscisse a produrre chiavi casuali sufficientemente lunghe e se si riuscisse a spedirle in modo sicuro, in modo cioè da avere la certezza che nessun terzo incomodo si è intrufolato nella trasmissione per intercettare la chiave, si potrebbero tranquillamente e in tutta sicurezza, utilizzare i cifrari di Vernam. Questo è quanto è stato realizzato mediante la crittografia quantistica, della quale parleremo tra breve.

Un breve glossario di Fisica quantistica

In questo paragrafo, raccogliamo alcuni rudimenti dell'apparato matematico che occorre per la trattazione degli argomenti di Fisica quantistica che stiamo considerando.
L'ambiente matematico di lavoro è uno spazio vettoriale reale H, munito di un prodotto scalare $\langle , \rangle$ definito positivo. Talvolta, oltre che a H, si guarda anche al *complessificato* di H, che risulta munito di un prodotto scalare hermitiano definito positivo, che estende il prodotto scalare su H. Per i nostri scopi, basterà considerare qui solo il caso reale. Inoltre, per il seguito, basterà fissare l'attenzione sul caso in cui H abbia dimensione 2.

Lo spazio vettoriale H è detto *spazio degli stati* e ogni suo vettore non nullo è detto un *vettore di stato*. Di norma, un vettore di stato sarà assegnato a meno di una costante moltiplicativa. Quindi, possiamo rappresentare una classe di equivalenza di vettori di stato con un versore. Questo lascia una indeterminazione con la quale decidiamo di convivere: precisamente due versori u,v sono equivalenti se e solo se $u=tv$, con $|t|=1$.
Per sfogliare immediatamente il nostro glossario, illustriamo a quale situazione Fisica il precedente modello matematico si può applicare. Ricordiamo che la più piccola unità, o *quanto* di luce, è il *fotone*. Come abbiamo detto, in Fisica quantistica si può pensare come una particella ma ha anche un aspetto ondulatorio. In un modo molto semplificato, possiamo descrivere l'aspetto ondulatorio come segue: il fotone si può riguardare come un minuscolo campo elettromagnetico che si propaga descrivendo una sinusoide con asse di simmetria la retta d come indicato in Figura 2. Naturalmente, la sinusoide è contenuta in un piano π contenente la retta d. La direzione delle rette di π ortogonali a d è la direzione lungo cui il fotone oscilla, e prende il nome di *polarizzazione* del fotone.

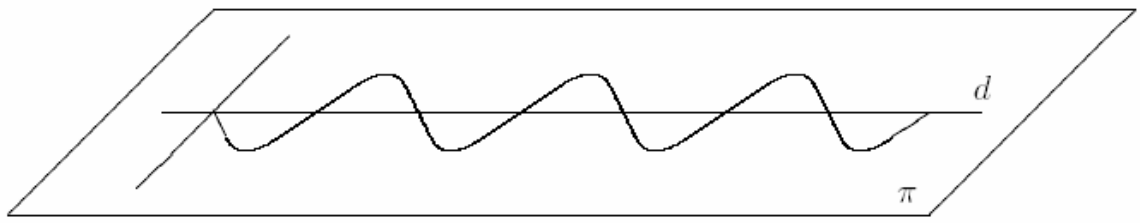

FIGURA 2. Polarizzazione del fotone

In definitiva, il modo di tenere traccia di questo aspetto ondulatorio del fotone, per rappresentarlo matematicamente, è di riguardarlo non come un punto bensì come un vettore la cui direzione è la polarizzazione del fotone. Questo spiega l'ambiente matematico nel quale ci siamo posti: possiamo pensare cioè al nostro spazio vettoriale H come all'insieme degli stati di polarizzazione dei fotoni. Il motivo per cui è lecito assumere H di dimensione 2 è chiaro: se i fotoni, partendo da una certa fonte luminosa, si propagano lungo la direzione d nello spazio a tre dimensioni, allora le polarizzazioni dei fotoni emessi dalla fonte luminosa sono vettori nel piano dello spazio ortogonale a d.
È ben noto che in H esistono *basi ortonormali* che consentono di identificare H con R^2. In questa identificazione, il prodotto scalare <,> si identifica con il prodotto scalare euclideo. Supponiamo di aver scelto una base – detta *base rettilinea* – che viene indicata con (↑,→): i suoi stati corrispondono a fotoni polarizzati *verticalmente* e *orizzontalmente*. Un'altra base ortonormale naturale è la *base diagonale* (↗,↘) dove ↗ e ↘ corrispondono rispettivamente agli stati dei fotoni polarizzati diagonalmente a 45 e -45 gradi rispetto alla base rettilinea. Il legame tra le due basi è dato dalle seguenti relazioni:

$$\begin{pmatrix} \nearrow \\ \searrow \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \uparrow \\ \longrightarrow \end{pmatrix}, \qquad \begin{pmatrix} \uparrow \\ \longrightarrow \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \nearrow \\ \searrow \end{pmatrix}.$$

Veniamo ora a formalizzare dal punto di vista matematico il concetto di osservazione o misura di un fotone. Nel contesto matematico costituito dallo spazio vettoriale H, chiameremo *quantità osservabile* ogni applicazione lineare: $A : \mathsf{H} \to \mathsf{H}$ *simmetrica* tale cioè che $<A(u),v>=<u,A(v)>$.

Data una base e dunque identificato H con R^2, ogni applicazione A come sopra si identifica con una matrice quadrata d'ordine 2 su R^2. Se la base è ortonormale, la matrice è simmetrica.
Un'applicazione lineare $A: \mathsf{H} \to \mathsf{H}$ che sia simmetrica è *ortogonalmente diagonalizzabile* ossia esiste una base ortonormale (v_1,v_2) formata da autovettori per A. Questo è il contenuto del cosiddetto *Teorema spettrale*. In una tale base, la matrice di A diviene diagonale:

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{pmatrix}$$

dove λ_1,λ_2 sono gli autovalori di A. Essi si dicono anche le *misure* dell'osservabile A. Dunque l'osservabile A ha misura λ_i solo se applicato all'autovettore v_i, i=1,2, o a un vettore ad esso proporzionale.
In generale, dato uno stato del sistema $v \in \mathsf{H}$, che possiamo supporre sia un versore, si ha:

$$v=<v, v_1> v_1+<v, v_2> v_2$$

e dunque:

$$A(v)=\lambda_1<v, v_1>v_1+\lambda_2<v, v_2>v_2.$$

Per la disuguaglianza di Cauchy-Schwartz, si ha $0<|<v, v_i>|\leq 1$ e $|<v,v_i>|= 1$ se e solo se v è proporzionale a v_i, i=1,2. Essendo:

$$1= ||v||= |<v,v_1>|^2+|<v,v_2>|^2$$

quanto più grande è $|<v,v_1>|$, tanto più piccolo è $|<v,v_2>|$, e dunque più vicino è v a v_1. Similmente scambiando v_1 con v_2.
È dunque naturale definire $|<v,v_i>|^2$ come la *probabilità* $P(A,v,\lambda_i)$ che A abbia misura λ_i nello stato v (i=1,2). In particolare, se tale valore è 1, allora la misura di A nello stato v sarà proprio l'autovalore λ_i. Inoltre, come ci si aspetta:

$$P(A,v,\lambda_1)+P(A,v,\lambda_2)=|<v,v_1>|^2+|<v,v_2>|^2=1.$$

È di nuovo tempo di sfogliare il nostro glossario e vedere come il linguaggio matematico che abbiamo introdotto si applichi a ben precise questioni fisiche.
Torniamo dunque alla luce e ai fotoni che, come abbiamo visto, si rappresentano come vettori stato che tengono traccia della loro polarizzazione. La luce che vediamo di solito consiste di un numero enorme di fotoni che hanno polarizzazioni molto diverse tra loro sicché, di norma, noi non percepiamo affatto il fenomeno della polarizzazione. A meno che – come sappiamo dall'esperienza – non indossiamo degli occhiali polarizzanti. Qual è il loro effetto? Cerchiamo di spiegarlo.
Vi sono dei vetri che hanno una struttura cristallina unidirezionale. Se si fa passare la luce attraverso di loro, i fotoni polarizzati nella stessa direzione dei cristalli che formano il vetro passano indisturbati; quelli aventi polarizzazione ortogonale vengono assorbiti, ossia ne viene impedito il passaggio; i rimanenti hanno una certa probabilità di passare ma, se passano, emergono sempre polarizzati nello stesso modo. In definitiva, se interponiamo tra la luce e il nostro occhio un tale filtro, percepiamo soltanto *luce polarizzata* nella direzione che il filtro lascia passare. È chiaro che, ruotando il filtro, possiamo lasciar passare luci con differenti polarizzazioni.
Vediamo qual è la formulazione matematica del fenomeno. Per fare ciò, puntiamo l'attenzione sull'osservabile A che, nel riferimento rettilineo, ha matrice:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Quale effetto otteniamo applicando A ad un qualunque stato dato da un versore v? È ovvio che, se $v=\uparrow$, allora $A(v)=v=\uparrow$; se invece $v=\rightarrow$, si ha $A(v)=0$. In generale, se:

$$v=(x,y)=x\cdot\uparrow+y\cdot\rightarrow,$$

dunque si ha:

$$A(v)=<v,\uparrow>\cdot\uparrow=x\cdot\uparrow .$$

L'effetto di A pertanto è quello di un filtro polarizzatore verticale, che chiameremo filtro di tipo ↑. I fotoni con polarizzazione verticale passano indisturbati; quelli con polarizzazione orizzontale non passano affatto; quelli con polarizzazione $v=(x,y)$ hanno, in accordo con la nostra descrizione matematica, probabilità x^2 di passare, sempre con polarizzazione verticale.
Ad esempio, il fotone $\nearrow = 1/\sqrt{2}\uparrow +1/\sqrt{2}\rightarrow$ ha probabilità 1/2 di passare, e lo stesso accade per il fotone ↘. In sostanza, per tornare ad un concetto introdotto nel §2, rispetto all'osservabile A, i fotoni ↗ e ↘ si trovano in una situazione di *sovrapposizione di stati*. Facendo passare il fotone ↗ attraverso un polarizzatore di tipo ↑, stiamo sottoponendo il fotone ad una osservazione: *osserviamo* se la luce esce polarizzata verticalmente o non esce. Seguendo le parole di P. A. M. Dirac, uno dei padri della Fisica quantistica, l'effetto di questa osservazione è di *costringere il fotone interamente nello stato di polarizzazione verticale o orizzontale. Esso dovrà fare un brusco salto per passare dalla condizione di parziale appartenenza a ciascuno di tali stati a quello di appartenenza totale ad uno solo di essi. In quale dei due stati salterà non è previsto: il fenomeno è regolato soltanto da leggi probabilistiche*. (cfr. anche [10]).
Ovviamente l'osservabile:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

agisce come un filtro polarizzatore orizzontale, ossia di tipo →, mentre gli osservabili:

$$\begin{pmatrix} \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} \\ -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} \end{pmatrix}$$

agiscono come filtri polarizzatori di tipo ↗ e ↘ rispettivamente.
I filtri di tipo ↑ o → vengono detti di *tipo rettilineo* o di tipo +. I fotoni con polarizzazione ↗ e ↘ hanno sempre probabilità (1/2) di passare con polarizzazione ↑ o →. I filtri di tipo ↗ e ↘ hanno analoghe proprietà e si dicono di *tipo diagonale* o di tipo ×.

Crittografia quantistica

I principi della Fisica quantistica possono venire utilizzati per la risoluzione del problema della creazione e trasmissione di chiavi casuali, rendendo possibile usare i cifrari di Vernam. La trasmissione verrà effettuata in totale sicurezza e trasmittente e ricevente sono posti in grado di

accorgersi di eventuali intrusioni di terzi. Vedremo in sostanza come l'*incertezza* del mondo quantistico fornisca delle certezze sulla sicurezza delle comunicazioni.
Le prime idee della Crittografia quantistica si possono rintracciare in un importante contributo di S. Wiesner (cfr. [15]), già noto in forma di manoscritto intorno al 1970, ma pubblicato solo nel 1983 in quanto rifiutato da più riviste che non ne avevano capito il grande valore innovativo. Queste idee furono poi riprese da C. H. Bennett e G. Brassard intorno al 1980. Essi elaborarono un protocollo per la *distribuzione quantistica delle chiavi*, oggi detto protocollo BB84 in quanto il relativo articolo [3] risale al 1984 (si veda anche l'articolo divulgativo [5]).
Vediamo su cosa si basa l'idea di Bennet e Brassard. Allo scopo di illustrarla, torniamo per un momento su quanto detto alla fine del §2. In quella situazione, possiamo supporre che A (la sorgente di fotoni) sia chi trasmette un messaggio, chiamiamola *Alice*, e lo schermo B sia chi riceve il messaggio, chiamiamolo *Bob*. Come abbiamo visto, il messaggio – in assenza di intrusioni – consiste in un'immagine che è descritta dalla curva $L_{1,2}$. Tuttavia se vi fosse un'intrusa, chiamiamola *Eva*, che cerca di misurare i fotoni nel loro passaggio attraverso le fenditure F_1 e F_2, questo altererebbe l'immagine, che sarebbe descritta dalla curva $L'_{1,2}$ invece che dalla curva $L_{1,2}$ sicché Bob dialogando, ad esempio per telefono, con Alice e descrivendo, se non tutta l'immagine, almeno qualche sua caratteristica, di certo si accorgerebbe dell'intrusione e potrebbe comunicarlo ad Alice.
L'idea della Crittografia quantistica non è molto differente. La trasmissione delle informazioni tra Alice e Bob avviene attraverso due canali: la prima parte attraverso un *canale quantistico*, ad esempio una fibra ottica che trasmette fotoni polarizzati; la seconda, costituita a sua volta da due momenti, attraverso un canale ordinario e non necessariamente sicuro.

PASSO 1: *comunicazione mediante trasmissione di fotoni attraverso un canale quantistico*.

A) Alice, che trasmette, ha a disposizione quattro filtri polarizzatori che le consentono di inviare, attraverso il canale di trasmissione, fotoni aventi le quattro polarizzazioni ↑, →, ↗ e ↘. Alice e Bob (che riceve) avranno preventivamente concordato di attribuire un valore numerico binario a un fotone polarizzato in uno dei suddetti modi, secondo il seguente schema:

Fotoni polarizzati	↑	→	↗	↘
Cifre binarie corrispondenti	1	0	1	0

Alice sceglie un numero r molto più grande della lunghezza della chiave che vuole spedire a Bob. Inoltre Alice sceglie in modo casuale una stringa, cioè una r-pla ordinata, di polarizzatori e invia a Bob, conservandone traccia, la corrispondente stringa di fotoni polarizzati. In tal modo, Alice ha in effetti inviato a Bob una successione di r cifre binarie, cioè un numero che in definitiva è il messaggio di Alice a Bob.
Pensiamo ad esempio alla seguente semplice situazione:

Polarizzazione dei fotoni inviati da Alice	↑	↑	↗	↘	↑	↘	↑	→
Messaggio inviato da Alice	1	1	1	0	1	0	1	0

Naturalmente, se Bob si limitasse a ricevere i fotoni così polarizzati, leggesse il numero inviato da Alice e usasse questo come chiave, non ci sarebbe alcuna garanzia di sicurezza in quanto Eva, il terzo incomodo intenzionato ad intromettersi, potrebbe – al pari di Bob – leggere lo stesso numero

inserendosi abusivamente nel canale di trasmissione. D'altra parte, nulla di quantistico si è realmente usato fin qui. Vediamo come invece deve operare Bob per conseguire la segretezza della chiave.

B) Bob ha a disposizione quattro filtri, due di tipo rettilineo +, ossia ↑ e →, e due di tipo diagonale ×, ossia ↗ e ↘ che funzionano come spiegato nel paragrafo §5. Bob non conosce quali siano le polarizzazioni dei fotoni inviatigli da Alice. Allora lascia passare i fotoni inviatigli attraverso i suoi filtri interposti in modo casuale e in tal modo ne *misura* la polarizzazione. Attribuisce poi a ciascun fotone polarizzato il suo equivalente numerico e determina un messaggio ricevuto.
Ad esempio potrebbe aversi la seguente situazione:

Messaggio inviato da Alice	1	1	1	0	1	0	1	0
Polarizzazione dei fotoni inviati da Alice	↑	↑	↗	↘	↑	↘	↑	→
Filtri usati da Bob	↑	↗	↘	→	↑	↘	↗	↗
Polarizzazione dei fotoni ricevuti da Bob	↑	↘	∅	↑	↑	↘	↗	↘
Messaggio ricevuto da Bob	1	0	1	1	1	0	1	0

Osserviamo che, al terzo passo della trasmissione, Bob ha interposto al fotone inviato da Alice un filtro che lo assorbe e non lo lascia passare. Abbiamo indicato questa circostanza col simbolo ∅. Da ciò, tuttavia, Bob deduce che il messaggio inviato da Alice è 1 poiché ad 1 corrisponde appunto l'unica polarizzazione incompatibile col filtro da lui usato.
Notiamo che, in questo procedimento, Bob può commettere un certo numero di *errori*. Infatti, se interpone il filtro + [risp. il filtro ×] a un fotone con polarizzazione rettilinea [risp. diagonale], non si verifica alcun errore. Invece, se interpone il filtro + [risp. il filtro ×] a un fotone con polarizzazione diagonale [risp. rettilinea], di certo questo altera la ricezione del relativo fotone. Poiché sia la polarizzazione dei fotoni trasmessi da Alice che la interposizione dei filtri di Bob è casuale, c'è da aspettarsi che vi siano errori con probabilità 1/2. Tuttavia, non è detto che ciascuno di questi errori produca di conseguenza un errore nel messaggio ricevuto. Infatti, per ogni errore fatto nell'interporre ai fotoni inviati da Alice un filtro sbagliato, c'è una probabilità su due che la cifra corrispondente sia quella giusta, pur essendo errata la polarizzazione del relativo fotone. Ad esempio, come si vede nella tabella precedente, se Alice invia un fotone con polarizzazione ↑, come accade nei passi 2 e 7 della trasmissione, e se erroneamente Bob interpone il filtro ×, può accadere, con uguale probabilità 1/2 o che Bob riceva un fotone con polarizzazione ↘, il che effettivamente accade al passo 2 della trasmissione, o che egli riceva un fotone con polarizzazione ↗, come accade al passo 7 della trasmissione. Nel primo caso, la cifra corrispondente sarà errata; nel secondo sarà quella giusta. In definitiva, la probabilità P che ha Bob di non commettere errori nella ricezione del messaggio è:

$$P=1/2\cdot 1+1/2\cdot 1/2=3/4=75\%$$

Il primo addendo corrisponde al caso, con probabilità 1/2, in cui Bob non sbagli nella scelta del filtro; il secondo addendo corrisponde al caso, ancora con probabilità 1/2, in cui la scelta del filtro non sia quella giusta. La percentuale di errore di Bob è quindi del 25%. Questa è anche la percentuale di errore di chiunque altro, come Eva, abusivamente si intrometta sul canale di trasmissione e legga il messaggio.

La precedente tabella spiega bene quanto abbiamo detto: gli errori di Bob nella interposizione dei filtri accadono ai passi 2, 4, 7 e 8 della trasmissione, cioè nella metà dei casi, mentre si ha un errore nel messaggio trasmesso solo nei passi 2 e 4 della trasmissione, cioè in un quarto dei casi.
A questo punto, un messaggio è stato trasmesso. Per farlo, Alice e Bob hanno usato in maniera determinante proprietà quantistiche. Tuttavia, a causa della presenza di errori, non possono fermarsi qui. Questi errori, come vedremo, possono essere eliminati e il fatto che abbiano luogo è anzi cruciale per scoprire, successivamente, eventuali intromissioni di Eva. Occorrono dunque ancora altri passi del protocollo.

PASSO 2 *Comunicazione su un canale non protetto per l'eliminazione degli errori e l'estrazione della* chiave grezza.

In questo passo del protocollo Alice e Bob, senza preoccuparsi ancora di eventuali intromissioni da parte di Eva, procedono alla individuazione ed eliminazione degli errori commessi da Bob nel ricevere il messaggio, ossia nella interposizione dei filtri. Nel caso non ci fosse stata intromissione da parte di Eva, il risultante messaggio, privo di errori, potrebbe essere adoperato come chiave per un cifrario di Vernam. Poiché tuttavia Alice e Bob non possono essere affatto sicuri che non vi siano stati interventi da parte di Eva, la chiave che essi otterrano, detta *chiave grezza*, oltre ad essere insicura, potrebbe ancora essere errata. Occorrerà dunque un ulteriore passo per verificare la presenza o meno di intromissioni.
L'eliminazione degli errori commessi da Bob è semplice. Infatti, a questo punto, Alice e Bob hanno ciascuno un pezzo di informazione: Alice conosce la stringa delle polarizzazioni dei fotoni inviati a Bob mentre Bob conosce quali filtri ha ad essi interposti. Allora, usando una canale eventualmente insicuro, come posta elettronica o telefono, Bob comunica ad Alice quali filtri ha usato e Alice gli comunica quali di questi erano quelli giusti. Dopo questo scambio di informazioni, Alice e Bob cancellano nei messaggi inviati e ricevuti tutte le cifre corrispondenti alle posizioni in cui il filtro interposto da Bob era errato. Nelle rimanenti posizioni, Bob non ha commesso alcun errore e dunque, *in assenza di intrusioni sul canale quantistico*, la relativa parte di messaggio, la chiave grezza, sarà la stessa sia per Alice che per Bob. Nell'esempio che stiamo trattando, e che corrisponde alle precedenti tabelle, Bob comunica ad Alice la stringa di filtri:

\+ × × + + × × ×

e Alice gli comunica che solo nei passi 1, 3, 5 e 6 della trasmissione Bob ha interposto il filtro giusto. I due, cancellando dai messaggi inviato e ricevuto le cifre dei posti 2, 4, 7 e 8, corrispondenti agli errori di interposizione di filtro commessi da Bob, ne deducono la chiave grezza:

1 1 1 0

che rimane segreta. Notiamo infatti che nello scambiarsi le informazioni sugli errori commessi da Bob, quest'ultimo e Alice non rivelano ad Eva, nel caso questa si inserisca abusivamente sul canale insicuro di comunicazione tra i due, alcuna informazione sulla chiave grezza. Infatti, se Eva non è intervenuta sul canale quantistico, il sapere da parte sua che nei passi 1, 3, 5 e 6 della trasmissione Bob ha interposto il filtro giusto al fotone inviato da Alice, non le dà alcuna informazione su quali siano i fotoni effettivamente trasmessi, e dunque le cifre ad essi corrispondenti, che formano la chiave grezza, rimangono segrete.

PASSO 3. *Comunicazione su un canale non protetto per verificare la presenza di Eva.*

A questo punto, Alice e Bob debbono appurare se vi sia stata o meno un'intrusione, sul canale quantistico, da parte di Eva. Ricordiamo infatti che un'eventuale intrusione di Eva *solo* sul canale non protetto sul quale hanno comunicato nel passo 2 non ha alcuna rilevanza. Se non vi è stata intrusione, i due possono utilizzare la chiave grezza, o parte di essa, come chiave per un cifrario di Vernam. Se invece vi è stata intrusione, Alice e Bob non hanno altra scelta che buttar via tutto quel che hanno fatto finora e ricominciare da capo, sperando che Eva si stanchi di spiare o usando un canale quantistico più sicuro.
Per capire come procedere in questo passo, è bene premettere una considerazione. Si osservi anzitutto che l'uso da parte di Alice e Bob di fotoni polarizzati in modo rettilineo e diagonale, è proprio motivato dalla necessità di rivelare se avviene o meno un'intrusione da parte di Eva. Se infatti i due si servissero solo di fotoni polarizzati in modo rettilineo, non avrebbero modo di accorgersi di un'intrusione da parte di Eva. In questo caso, Eva potrebbe intercettare la trasmissione di Alice con una precisione del 100%, interponendo ad esempio un filtro di tipo verticale, e poi imitare Alice ritrasmettendo gli stessi dati a Bob. Una tale strategia da parte di Eva prende il nome di *intrusione opaca*.
Per contro, l'uso, da parte di Alice e Bob, di fotoni con due tipi di polarizzazione rende un'eventuale intrusione di Eva evidente. Infatti, se Eva si intromette sul canale quantistico e vuole leggere il messaggio di Alice, deve misurare la polarizzazione dei fotoni trasmessi. Poiché a questo punto si trova nelle stesse condizioni di Bob, l'unica cosa che può fare è procedere come lui, il che la obbliga, come sappiamo, a commettere degli errori. Quindi, se successivamente si sostituisce ad Alice e trasmette a Bob il messaggio da lei letto, il messaggio da lei inviato sarà diverso da quello originario di Alice, ossia *conterrà degli errori*, e dunque Alice e Bob, confrontando le loro chiavi grezze, hanno buona probabilità di scoprire se c'è stata intrusione.
Per dare sostanza matematica a quanto stiamo dicendo, notiamo che un'eventuale intrusione da parte di Eva ha un immediato impatto sulla probabilità di errore nella ricezione del messaggio da parte di Bob, che abbiamo calcolato nel passo 1 essere P=1/4.
Supponiamo che Eva interferisca con probabilità s, con $0 \le s \le 1$. In altre parole, s misura la percentuale di fotoni che Eva manomette intromettendosi tra Alice e Bob. Se $s = 0$, vuol dire che Eva non interferisce mai; se $s = 1$, vuol dire che Eva misura ogni singolo fotone inviato da Alice a Bob. Per valori intermedi di s vuol dire che Eva a volte ci prova, a volte no. Dato che, a causa delle ipotesi di casualità che abbiamo fatto, le scelte dei filtri da parte di Bob e Eva sono indipendenti le une dalle altre e indipendenti dalla scelta delle polarizzazione dei fotoni inviati da Alice, si può avere un errore nel messaggio ricevuto da Bob solo se:

- Bob sbaglia, il che, come sappiamo, capita con probabilità 1/4, senza che sia intervenuta Eva, il che ha probabilità $1 - s$;
- Bob non sbaglia, il che capita con probabilità 3/4, ma Eva interviene, con probabilità s, e determina un errore nella interposizione del filtro, il quale a sua volta causa un errore nel messaggio ricevuto con probabilità 1/2.

In definitiva, la nuova probabilità di errore P' nella ricezione del messaggio da parte di Bob è data dalla seguente formula:

$$P' = \frac{1}{4}(1-s) + \frac{3}{4}\cdot\frac{1}{2}s = \frac{1}{4} + \frac{s}{8}.$$

Ad esempio, se $s = 1$, ossia se Eva interviene sempre, allora la percentuale di errore di Bob passa da 1/4 a 3/8, che è un aumento considerevole e constatabile.
Vediamo come questo si riflette sulla probabilità che vi siano discrepanze tra la chiave grezza di Alice e quella di Bob: si ricordi che, in presenza di intrusioni da parte di Eva, tali chiavi potrebbero essere diverse. Siamo dunque in presenza di una discrepanza solo se Eva interviene, il che accade

con probabilità s. In tal caso Eva commette un errore, con probabilità 1/2, nell'interposizione del filtro, e viene commesso un errore nel messaggio con ulteriore probabilità 1/2. In definitiva la probabilità P_K di discrepanza tra le due chiavi è :

$$P_K = \frac{1}{2} \cdot \frac{1}{2} s = \frac{s}{4}.$$

Questo ci fa capire come dovranno operare Alice e Bob per individuare l'eventuale presenza di Eva. Poiché ogni discrepanza tra la chiave grezza di Alice e quella di Bob è dovuta ad Eva, i primi due saranno sicuri della intromissione di quest'ultima se trovano anche *una sola* differenza tra due chiavi grezze. Allora individuano, comunicando sul canale insicuro, un sottoinsieme casuale di m cifre delle loro chiavi grezze, che potrebbero ora essere diverse, e le confrontano. Se è intervenuta Eva, troveranno all'incirca $m \cdot s/4$ differenze tra le due chiavi. Dunque, se m è molto grande è ragionevole pensare che Alice e Bob individuino prima o poi una discrepanza, avendo così la sicurezza dell'intervento di Eva.
Ad esempio, se essi stimano la probabilità di intervento di Eva in $s \leq 1/1000$, confrontando 20.000 cifre della chiave grezza possono sperare di trovare circa 5 discordanze.
Se, d'altra parte, per nessuna delle m cifre prescelte, Alice e Bob hanno riscontrato una discrepanza, allora la probabilità che Eva si sia intromessa, ma che la sua intromissione non sia stata avvertita, è:

$$(1 - \frac{s}{4})^m$$

Se m è molto grande, tale probabilità è molto bassa. Ad esempio, se $s = 1$ e $m = 30$ si ha:

$$(\frac{3}{4})^{150} < 2^{-50}$$

che è un numero molto piccolo, a proposito del quale ricordiamo la frase di E. Borel in *Les probabilités et la vie*: "*un fenomeno la cui probabilità è* 10^{-50} *non accadrà mai, o, quanto meno, non sarà mai osservato*".
In conclusione, se, dopo questo controllo, Alice e Bob raggiungono una ragionevole sicurezza, se non la certezza, che Eva non si sia intromessa, allora possono usare come chiave per un cifrario di Vernam quel che rimane dopo aver cancellato dalla chiave grezza le m cifre adoperate per il controllo. Se invece trovano una discrepanza tra le due chiavi grezze, e quindi sanno che Eva si è intromessa, debbono ricomiciare tutto daccapo. Certo non sarà piacevole, ma meglio che esporsi allo spionaggio di Eva.

Prima di concludere, è bene fare qualche osservazione sul protocollo *BB84*. Quello che abbiamo qui esposto non ne delinea che i tratti essenziali, lasciando fuori i problemi tecnici che si presentano nella sua effettiva messa in opera, i quali a loro volta pongono altrettanti interessanti problemi teorici. Senza entrare in dettagli, sarà comunque bene accennare ai più rilevanti tra questi, rinviando all' articolo [5] per ulteriori informazioni.
Il problema principale è forse che il modello di cui abbiamo parlato non tiene in nessun conto eventuali errori che potrebbero derivare dalla trasmissione dei fotoni attraverso il canale quantistico, ossia errori dovuti a *rumore* presente sul canale. Per ovviare a ciò, si può far uso delle tecniche di teoria dei codici correttori di errori, argomento in cui qui non ci addentriamo (cfr. [2]). Non è possibile tuttavia, se c'è rumore, escludere del tutto errori dovuti a quest'ultimo. La loro presenza

mette a serio rischio il passo 3 del protocollo, nel senso che potrebbe portare Alice e Bob a credere nell'intervento di Eva, anche se non c'è stato, e dunque potrebbe portare a un blocco della comunicazione tra i due. A questo problema, si può far fronte stimando quanto il rumore influisce sulla probabilità della presenza di errori nella chiave grezza, procedendo poi come nel passo 3 per determinare se vi sia stata o meno intromissione da parte di Eva. Più complicata è invece la determinazione di una chiave comune senza errori dovuti al rumore. Anche su questo non ci tratteniamo, rinviando a [4].
Un altro problema tecnico importante è il seguente. Nel protocollo che abbiamo illustrato è essenziale che la trasmissione avvenga *un fotone per volta*. Questa è un'operazione tecnicamente assai complicata se si trasmette nel vuoto o, peggio, nell'aria. Ci si riesce usando una fibra ottica, cosa che per il momento limita la realizzazione tecnica del sistema. Ad ogni modo, si pensi di inviare (invece di un singolo fotone per volta) fasci di luce polarizzati composti di più fotoni. Questo espone immediatamente Alice e Bob all'intrusione di Eva. Costei, infatti, potrebbe sottrarre da ciascun pacchetto di fotoni trasmesso da Alice, uno di questi ed effettuarne la misurazione, facendo proseguire gli altri verso Bob senza averli alterati. È chiaro che questo vanifica la ricerca dell'intrusione di Eva nel passo 3 del protocollo. Certo – si potrà dire – Bob, che si vede arrivare un fotone in meno, da questo fatto può accorgersi dell'intervento di Eva. È vero, ma, ciò ha senso solo se il numero dei fotoni inviati da Alice in ogni fascio di luce è basso. In caso contrario, sarà ben difficile da parte di Bob stimare l'assenza di un singolo fotone da ciascun pacchetto e, perfino se fosse in grado di farlo, potrebbe attribuire la cosa ad una naturale dispersione dei fotoni nel mezzo di trasmissione.
In ogni caso, la Crittografia quantistica, a differenza del computer quantistico che per il momento è solo teoria, è una realtà . C. Bennet e J. Smolin, nel 1988, hanno realizzato un primo sistema per l'invio di chiavi sfruttando il protocollo *BB84*. All'epoca, furono in grado di inviare messaggi ad una distanza di soli pochi centimetri. Attualmente, usando fibre ottiche, si è riusciti a inviare messaggi su scala abbastanza grande. Ad esempio, nel 1995, ricercatori dell'Università di Ginevra sono stati in grado di inviare chiavi numeriche con il protocollo *BB84* a una distanza di 23 chilometri. Attualmente, la ricerca è attiva sulla possibilità di invio di messaggio nell'aria o via satellite. Dunque, come spesso è capitato nella storia, anche qui i crittologi sono in vantaggio sui crittoanalisti. E questa volta pare che il vantaggio sia incolmabile!

Bibliografia

[1] M. W. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo, *Aritmetica, crittografia e codici*, Serie Unitexts, Springer-Verlag Italia, 2006.
[2] J. Baylis, *Error-correcting codes*, Chapman and Hall Math., 1998.
[3] C.H. Bennet, G. Brassard, *Quantum cryptography: public key distribution and coin tossing*, International Conference on Computers, Systems & Signal Processing, Bagalore, India, 1984, pp. 175-179.
[4] C.H. Bennet, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *Experimental quantum cryptography*, J. Cryptology, 5 (1992) pp. 3-28.
[5] C.H. Bennet, G. Brassard, A. Ekert, *Quantum cryptography*, Scientific American, October 1992, pp. 26-33..
[6] N. Crato, *Quantum cryptography*, Newsletter of the European Math. Soc., 52 (2004), pp. 15-16.
[7] N. Crato, *Codici indecifrabili, messaggi sicuri*, Bollettino U.M.I., Sezione A, La Matematica nella Società e nella Cultura, Serie VIII, Vol. VII-A, 275-289.
[8] D. Deutsch, *The fabric of Reality*, London, Allen Lane, 1977.
[9] D. Deutsch, A. Ekert, *Quantum Computation*, Physics World, 11 (3) (1998), pp. 33-56.
[10] P.A.M. Dirac, *The principles of quantum mechanics*, Oxford University Press, 1958.

[11] S. Lomonaco, Jr., *A talk on quantum cryptography or How Alice outwits Eve*, AMS PSAPM, 58, (2002), pp. 237 - 264. Pubblicato anche in "Coding Theory and Cryptography: From the Geheimschreiber and Enigma to Quantum Theory", (ed. D. Joyner), Lecture Notes in Computer Science and Engineering, Springer-Verlag, 1999, pp. 144-174.
[12] C. E. Shannon, *Communication theory of secrecy systems*, Bell Systems Technical Journal, 28 (1949), pp. 656-715.
[13] P.W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithm on a Quantum Computer*, SIAM J. Computing 26 (1997), pp. 14-84.
[14] S. Singh, *The code book*, Anchor Books, New York, 1999 (trad.it. *Codici e segreti*, BUR, Milano, 2001).
[15] S. Wiesner, *Conjugate Coding*, SIGACT News, 15:1 (1983), pp. 78-88 (Manoscritto intorno al 1970).