QUANTUM COMPUTER
E
CRITTOGRAFIA QUANTISTICA

IL FUTURO DELL'INFORMATICA E DELLA SICUREZZA NELLE COMUNICAZIONI

di Lorenzo Cesaretti

INTRODUZIONE

Un gruppo sempre più folto di scienziati sostiene che il futuro dell' informatica non avrà nulla a che vedere con i vecchi microchip fatti di miliardi e miliardi di "semplici" transistor di silicio ma piuttosto sarà popolato da nuove macchine raffinatissime costituite da molecole, raggi laser e superconduttori, funzionanti non secondo le leggi "classiche" dell'elettronica, ma secondo quelle della meccanica quantistica. Per comprendere come sono fatti questi nuovi computer introdurremo nel prossimo capitolo questa branca della fisica.

CAPITOLO PRIMO

LA MECCANICA QUANTISTICA

La meccanica quantistica è un complesso di teorie fisiche formulate nella prima metà del XX secolo che descrivono il comportamento della materia a livello microscopico, a scale di lunghezza inferiori o uguali a quelle dell'atomo o alle energie tipiche delle interazioni nucleari, dove cadono le ipotesi alla base della meccanica classica.

Questa nuova teoria fu elaborata per spiegare alcune contraddizioni tra modelli teorici e dati sperimentali emerse alla fine del 1800: gli spettri di emissione degli atomi, caratterizzati da una struttura discontinua, formata cioè da righe distinte, non spiegabili mediante le leggi dell'elettromagnetismo classico (ad esempio in figura 1 gli spettri del sodio); il problema del "corpo nero", cioè lo spettro della radiazione

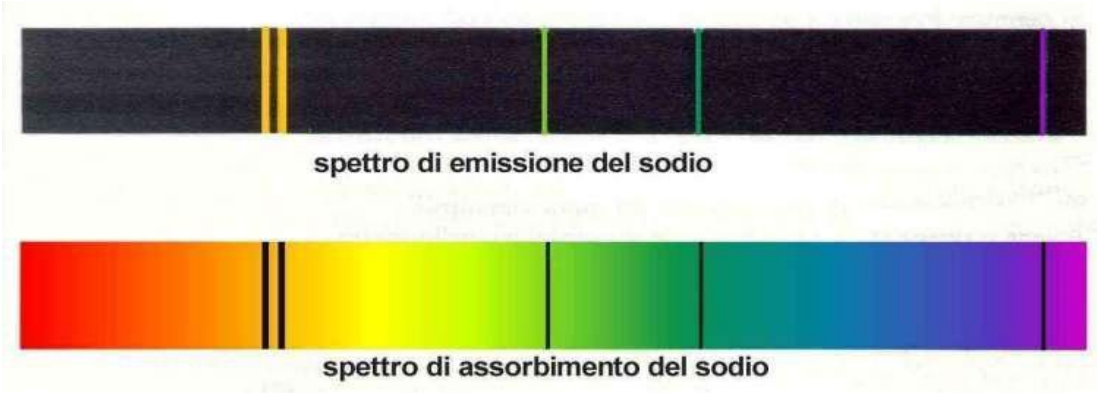


Fig. 1

emessa da un corpo caldo in funzione della frequenza , non spiegabile attraverso le teorie classiche. Più precisamente un corpo nero è un corpo ideale che assorbe tutte le onde elettromagnetiche che lo investono ed emette energia sotto forma di radiazione continua di intensità crescente all'aumentare della temperatura. Praticamente un corpo nero si ottiene con un involucro di pareti buone conduttrici di calore internamente annerito con nerofumo; nell'involucro si pratica un piccolissimo foro in libera comunicazione con l'esterno. A seguito delle riflessioni multiple sulle pareti interne della cavità ogni radiazione che penetra attraverso questo foro è praticamente tutta assorbita. L'elettromagnetismo classico non riusciva però a spiegare l'emissione di energia di questo corpo, soprattutto a frequenze basse. Nel 1900 Planck riuscì a risolvere la questione, ipotizzando che l'energia (E) emessa da corpi fossi quantizzata, cioè fosse costituita da multipli discreti di una quantità fondamentale ($h\nu$), detta quanto d'energia: $E = h\nu$ (dove ν è la frequenza della radiazione, h è una costante universale pari a $6{,}6 \times 10^{-34}$ Js). Planck stesso fu quasi spaventato dal suo

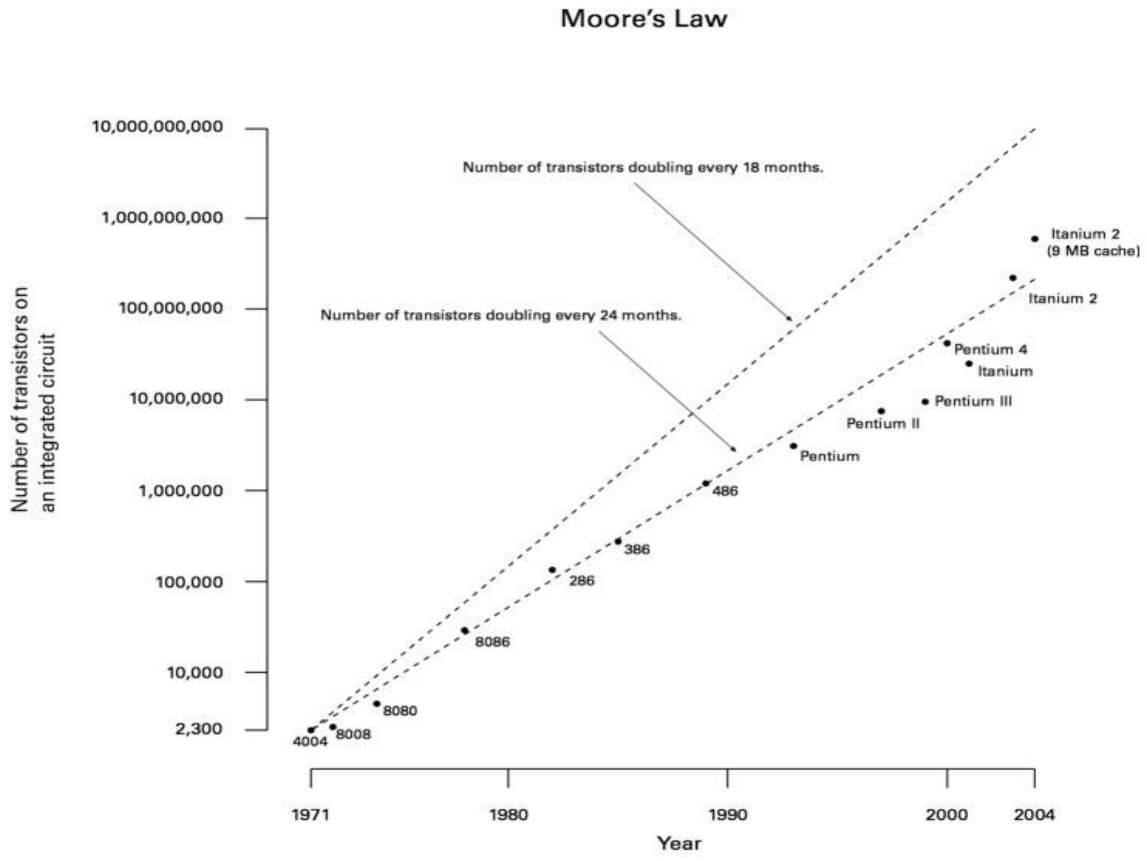
concetto innovativo di quanto, tanto che lo definì una "fortunata violenza puramente matematica contro le leggi della fisica classica"; la sua ipotesi infatti costituiva una vera e propria rivoluzione concettuale: si stava passando da una logica di continuità energetica dei fenomeni naturali (il continuo classico di Galileo, Leibniz, Newton, Maxwell), ad una concezione di discontinuità, in cui l'energia emessa dai corpi poteva essere scambiata sotto forma di tanti pacchetti proporzionali alla frequenza mediante la costante di Planck.

Nel 1905 Einstein applicò l'ipotesi quantistica per interpretare l'effetto fotoelettrico (l'emissione di elettroni da parte di una superficie metallica illuminata da una radiazione elettromagnetica), affermando che la radiazione luminosa è composta da pacchetti discreti di energia che interagiscono singolarmente con gli elettroni del metallo; Einstein ipotizzò cioè un modello corpuscolare della luce, composta da un insieme di quanti di energia, detti fotoni.

Nel 1913 Bohr propose un modello atomico planetario in cui gli elettroni negativi ruotano intorno al nucleo positivo su differenti orbite discrete stazionarie corrispondenti a diversi livelli energetici quantizzati. Questo modello permetteva la spiegazione della struttura discreta degli spettri di emissione: gli atomi possono scambiare energia solo mediante salti degli elettroni tra le diverse orbite, quindi sono emesse solo righe spettrali aventi frequenze $\nu_{nm} = (E_n - E_m)/h$ corrispondenti alle transizioni permesse tra i livelli energetici E_n ed E_m tipici dell'atomo.

L' INFLUENZA DELLA MECCANICA QUANTISTICA SULL' INFORMATICA

Perché la meccanica quantistica influenza anche l'informatica? Per rispondere a questa domanda dobbiamo fare riferimento alla legge di Moore, formulata da Gordon Moore negli anni '60: ogni diciotto mesi la potenza di calcolo dei processori in media raddoppia. Ciò è possibile grazie all'ingegno umano: i computer sono diventati sempre più veloci perché gli ingegneri sono riusciti a miniaturizzare sempre più i circuiti e le porte logiche che ne costituiscono il nucleo. Se dimezziamo l'ingombro di un componente di base, ne possiamo inserire il doppio nello stesso spazio, e quindi raddoppiare la velocità di calcolo. In base alla legge di Moore, tra breve l'ordine di grandezza di componenti informatici dovrebbe scendere fino a diventare quello di un atomo, raggiungendo quindi la scala di lunghezza governata dalle leggi della meccanica quantistica.



Il grafico precedente mostra l'aumento del numero dei transistor nei circuiti integrati dei computer dal 1971 al 2004: la legge ipotizzata da Moore è stata confermata in linea di principio, anche se il ritmo di crescita è stato un po' più lento in quanto i processori anziché ogni 18 mesi sono raddoppiati di velocità ogni 24 mesi.

Due sono i principi della meccanica quantistica che risultano determinanti per un computer quantistico: il principio di indeterminazione e il principio di sovrapposizione.

PRINCIPIO DI INDETERMINAZIONE

Questo principio fu formulato nel 1927 da Werner Heisenberg, ed esprime l'impossibilità di conoscere nello stesso tempo con precisione assoluta la posizione e la quantità di moto di una particella quantistica. Il principio di indeterminazione esprime il modo in cui sono legati i livelli di precisione con cui si possono determinare queste due grandezze complementari: una qualsiasi misura che renda più esatto il valore di una certa grandezza, automaticamente fa diminuire la precisione con cui si può conoscere la complementare. La misura è nei fatti un'azione che disturba il sistema, introducendo un'inevitabile livello di indeterminazione sul valore

rilevato. Ha scritto Heisenberg: “Nella discussione di alcune esperienze occorre prendere in esame quella interazione tra oggetto e osservatore che è necessariamente congiunta ad ogni osservazione. Nelle teorie classiche questa interazione veniva considerata o come trascurabilmente piccola o come controllabile in modo da poterne eliminare l’influenza per mezzo di calcoli. Nella fisica atomica tale ammissione non si può fare perché, a causa della discontinuità degli eventi atomici, ogni interazione può produrre variazioni parzialmente incontrollabili o relativamente gravi” (I principi fisici della teoria dei quanti).

PRINCIPIO DI SOVRAPPOSIZIONE

Questo principio afferma che i sistemi microscopici si trovano in uno stato quantistico costituito dalla sovrapposizione, cioè dalla combinazione lineare in termini matematici, di tutti i possibili stati in cui esso può esistere; è uno stato non definibile secondo le regole della logica classica che rappresenta tutte le proprietà potenziali di un sistema quantistico che viene poi determinato in seguito ad un processo di misura. A priori si può conoscere solo la probabilità che una misura riveli uno degli stati possibili del sistema. A chi non è mai capitato, guardando attraverso il vetro di una finestra, di vedere non solo il paesaggio esterno ma spesso anche la propria immagine, più o meno nitidamente? Questo fenomeno, troppo spesso osservato con indifferenza, è in realtà uno straordinario esempio per entrare direttamente in contatto con il mondo quantistico. La luce, come detto in precedenza, è costituita da fotoni. Questi ultimi attraversano il vetro per mostrare il paesaggio; ma non è detto. Il mondo quantistico delle particelle non è un mondo di certezze ma di possibilità. Il fotone che colpisce il vetro può attraversarlo, ma può anche esserne riflesso: il fotone ha una certa probabilità di passare o meno attraverso il vetro. È proprio questo il principio di sovrapposizione: se un’ entità quantistica può assumere due valori o essere in due stati sarà in una sovrapposizione dei due, con una probabilità non nulla di essere nell’uno o nell’altro. In una sovrapposizione, a differenza di un miscuglio, non si può dire che un corpo si trovi realmente in uno stato o nell’altro; la sovrapposizione contiene tutti i casi possibili, ma non equivale ad alcuno di essi. Possiamo concludere che lo stato di una particella è dato dalla sovrapposizione di tutti i suoi possibili stati futuri, ciascuno “pesato” con una probabilità.

CAPITOLO SECONDO

TEORIA QUANTISTICA DELL' INFORMAZIONE

La teoria dell' informazione è la teoria matematica che si occupa della trasmissione, dello stoccaggio, e dell'elaborazione dei dati, aspetti che riguardano molto da vicino il computer, sia classico che quantistico.

L'informazione è fondamentalmente di natura fisica, in quanto ogni elaborazione di dati richiede un supporto fisico. Questa affermazione, per quanto possa sembrare ovvia, risulta molto interessante se si considera la possibilità di utilizzare supporti che non ubbidiscono alle leggi classiche della meccanica.

L'unità minima di informazione è il bit (dall' inglese "binary unit") definito come la quantità di informazione equivalente alla scelta tra due alternative possibili. Il termine bit viene utilizzato anche per indicare il congegno in cui l'informazione stessa viene immagazzinata, ma in questo caso bit sta per "binary digit", poiché il ricorso al sistema binario è il più conveniente per gli elaboratori elettronici.

La teoria dell'informazione è piuttosto intuitiva: il massimo numero di messaggi diversi che si possono trasmettere utilizzando un oggetto che può trovarsi in uno di un insieme di N stati distinguibili risulta proprio uguale a N. Attraverso un sistema che può trovarsi solo in 2 stati che possono essere rappresentati dalle due cifre 0 e 1, non è possibile, a livello classico inviare più di due messaggi diversi: ad esempio Alice trasmetterà un bit di informazione corrispondente allo stato (0) per comunicare a Bob che l'indomani potranno incontrarsi, uno corrispondente allo stato (1) per fargli sapere che ciò non è possibile. Bob esegue una misura e, a seconda dell' informazione, riconosce in modo chiaro il messaggio di Alice. Se si considera un sistema quantomeccanico oltre allo stato $|0\rangle$ e $|1\rangle$ (0 e 1 sono in notazione bra-ket, usata in meccanica quantistica per descrivere uno stato quantistico), a causa del principio di sovrapposizione esso può trovarsi in qualsiasi loro combinazione lineare ($a|0\rangle + b|1\rangle$, con a e b che indicano rispettivamente la probabilità di trovarlo in uno stato o nell'altro).

Questo è un concetto poco intuitivo, per capirlo meglio possiamo fare un esempio: il bit classico è come una moneta che una volta lanciata, cadrà a terra mostrando inesorabilmente una delle due facce, mentre il qubit (abbreviazione di bit quantistico) può essere immaginato come una moneta che una volta lanciata cadrà a terra continuando a ruotare su sé stessa senza arrestarsi fino a che qualcuno non la schiacci

con una mano bloccandone la rotazione e obbligandola a mostrare una delle due facce.

La realizzazione di un bit quantistico

Isidor Isaac Rabi, premio Nobel per la fisica nel 1944, fu il primo a indicare il modo attraverso il quale scrivere l'informazione in un sistema quantistico, utilizzando atomi di idrogeno. Immaginiamo un atomo di idrogeno nello stato fondamentale, cui corrisponda una quantità di energia E_0. Per scrivere un bit 0 su questo atomo non si fa nulla; per scrivervi 1 si eccita l'atomo portandolo a un livello energetico superiore, E_1. Ciò si ottiene immergendolo in una luce laser costituita da fotoni aventi energia pari alla differenza tra E_1 e E_0. Se il fascio laser ha la giusta intensità ed è applicato per un tempo appropriato, l'atomo passa gradualmente dallo stato fondamentale allo stato eccitato perché il suo elettrone assorbe un fotone. Se l'atomo si trova già nello stato eccitato, lo stesso impulso gli fa emettere un fotone e lo fa passare nello stato fondamentale. In termini di registrazione di informazione, l'impulso ordina all' atomo di cambiare, o commutare il suo bit.

Se però la luce appropriata viene applicata per metà del tempo necessario a far passare l'atomo da 0 a 1, quest'ultimo si viene a trovare in uno stato simile alla sovrapposizione dello stato corrispondente allo 0 e dello stato corrispondente all'1. Questo bit quantistico viene commutato solo a metà, mentre il bit classico vale sempre 0 o 1. Un condensatore mezzo carico in un calcolatore tradizionale provoca errori, ma un qubit mezzo commutato apre la strada a calcoli di nuovo tipo.

I vantaggi di un bit quantistico

Per cogliere i vantaggi offerti dai qubit rispetto ai loro equivalenti classici cominciamo col considerare un problema estremamente semplice, cioè quello di immagazzinare in un'opportuna collezione di bit un numero in notazione binaria. Ad esempio consideriamo un caso semplice, il numero 57, che in notazione binaria si scrive 111001, utilizzando quindi 6 bit. Nel caso classico utilizzeremo tutti e 6 i nostri bit e li metteremo negli stati (1)(1)(1)(0)(0)(1), rispettivamente. In questo modo avremo immagazzinato l'informazione che ci interessa. Supponiamo ora di avere 6 bit quantistici, e di prepararli tutti nella loro combinazione lineare, cioè nello stato di

sovrapposizione tra 0 e 1. Otterremo ben 64 stati diversi $\left(D_6^2 = 2^6 = 64\right)$, in cui troveremo non solo il numero 57, ma tutti i numeri naturali da 0 a 63. Se volessimo memorizzare solo il 57 dovremmo sottoporre lo stato finale a opportune manipolazioni. E' però interessante segnalare come lo stesso numero di bit necessari per immagazzinare, a livello classico, un numero di 6 cifre, ci consente di disporre potenzialmente della registrazione di tutti i numeri con un massimo di 6 cifre in notazione binaria.

Con 6 qubit i 64 stati possono essere memorizzati e manipolati contemporaneamente: grazie al principio di sovrapposizione si realizza una "parallelizzazione" della elaborazione (cioè del calcolo) a livello dei primi componenti hardware le cui potenzialità crescono a livello esponenziale rispetto al numero di qubit coinvolti. I computer quantistici hanno quindi maggiori potenzialità rispetto ai computer classici perché consentono la possibilità di eseguire operazioni che finora richiedevano tempi di calcolo lunghissimi, e che erano quindi praticamente irrealizzabili.

CAPITOLO TERZO

COMPLESSITÀ COMPUTAZIONALE E CRITTOGRAFIA

Un tema di enorme rilevanza nella teoria dell'informazione è quello della complessità computazionale, cioè della classificazione di problemi in base alle risorse computazionali (memoria occupata e tempo di calcolo) richieste per la loro soluzione. Secondo la teoria della complessità computazionale un problema viene definito P se è possibile definire un algoritmo per la determinazione delle soluzioni del problema che sia computabile (cioè calcolabile) in tempo polinomiale (il computer deve eseguire solo addizioni e moltiplicazioni). Un problema si definisce NP se è possibile definire un algoritmo di verifica delle soluzioni del problema che sia computabile in tempo polinomiale, mentre il calcolo delle soluzioni attualmente richiederebbe tempi esponenziali.

Prendiamo ora in considerazione una famiglia di problemi che hanno una caratteristica peculiare. Date due operazioni che sono inverse, accade in certi casi che mentre l'operazione diretta è relativamente semplice da eseguire, l'operazione inversa può risultare estremamente ardua e costituire un problema con difficoltà computazionale NP. Il più noto problema di questo tipo è quello di decomporre nei suoi fattori il prodotto di due numeri primi. Il problema è interessante quando il numero delle cifre N del prodotto risulta notevolmente elevato. Si intuisce facilmente come risulti semplice moltiplicare tra loro due numeri primi anche nel caso che i due fattori abbiano un numero elevato di cifre e come qualsiasi calcolatore possa eseguire questa operazione in un tempo relativamente breve. Tuttavia l'operazione inversa di passare dal prodotto ai due fattori non risulta affatto semplice. Anche se non è stato ancora dimostrato che l'operazione inversa relativa alla decomposizione in fattori presenta effettivamente complessità non polinomiale nessuno è stato capace di elaborare un algoritmo che la renda velocemente eseguibile. Il procedimento da seguire risulta più o meno quello ovvio, vale a dire di provare a dividere il prodotto per tutti i numeri primi a partire da due in su, fino a che si ottenga una divisione senza resto.

Questa caratteristica singolare del problema ha fatto si che su di esso venisse basato il più commercializzato e diffuso sistema di crittografia, RSA. Prima però di descriverlo, analizziamo qualche interessante esempio di come in passato gli uomini hanno tentato di cifrare i messaggi. L' esigenza di nascondere ad occhi indiscreti per motivi di guerra, di spionaggio o di amore messaggi dal contenuto delicato si può

ritenere vecchia come il mondo. Tra i trucchi più semplici di cifratura c'è quello di tradurre le lettere dell' alfabeto in uso con altri simboli, oppure di permutarle tra di loro secondo una chiave prestabilita. Questi procedimenti erano usati sin dall' antichità anche da Giulio Cesare, che, nel corso delle sue numerose campagne di guerra dovendo corrispondere con i suoi luogotenenti e volendo evitare che i suoi ordini venissero intercettati e soprattutto capiti dai suoi nemici, talora li criptava traducendoli semplicemente in greco, talora provvedeva a permutare le lettere secondo uno schema fisso prestabilito. Ad esempio, il testo poteva essere cifrato spostando ogni lettera dell'alfabeto dei Romani di tre passi in avanti (A in D, B in E,…) e le ultime tre lettere nelle prime tre; il testo originale veniva poi decifrato col semplice procedimento inverso di tornare indietro di tre lettere; ovviamente la chiave 3 doveva essere concordata in anticipo e resa nota sia a chi cifrava sia a chi decifrava. In realtà Cesare e i suoi luogotenenti che non conoscevano le cifre 1,2,3,…, usavano al loro posto una sorta di anello con due circonferenze concentriche, che elencava nella fascia esterna tutte le lettere dell' alfabeto e le accompagnava internamente con tutte le loro sostituzioni. Nel Rinascimento Leon Battista Alberti e, poco dopo, il francese Vigenère avevano proposto l'idea di decifrare lettere di un dato messaggio non più con l'uso costante di un'unica permutazione, ma piuttosto utilizzando permutazioni diverse, dipendenti dal posto della lettera da cifrare. Ancora nella seconda guerra mondiale, l'esercito tedesco adoperava una macchina, denominata Enigma, che cifrava le informazioni segrete secondo un ripetuto uso dell'idea di Alberti e Vigenère, rinnovandone frequentissimamente la chiave. Questo sistema veniva usato, ad esempio, per trasmettere ai sottomarini tedeschi dell'Atlantico le coordinate dei convogli nemici in navigazione. I crittoanalisti inglesi che cercavano di violare questo codice e di carpire il significato dei messaggi si trovavano dunque di fronte alla difficoltà non solo di ricavarne la chiave (tecniche raffinate di analisi di frequenza già permettevano questo obbiettivo prima della guerra), ma anche e soprattutto di farlo in tempi rapidi, prima che la chiave stessa perdesse la sua validità e comunque in tempo per salvare il convoglio in navigazione. I loro sforzi coordinati, dal grande matematico del '900 Alan Turing, riuscirono alla fine nell'impresa, ed il loro successo contribuì all'esito del conflitto, almeno alla battaglia navale nell' Atlantico. Nel 1977 si arrivò grazie a Rivest, Shamir e Adleman, tre studiosi del Massachussetts Institute of Technology, alla creazione di RSA. Questo è un sistema a chiave pubblica, quindi differisce da tutti gli schemi ideati in precedenza, in quanto i

due interlocutori non hanno bisogno di accordarsi a priori su una chiave segreta. Ogni utente sceglie due chiavi: una la rende nota pubblicandola su una guida e qualunque altro utente la potrà usare per cifrare messaggi a lui destinati; l'altra chiave la tiene per sé e la userà per la decodifica dei messaggi a lui inviati. L'idea che sta alla base della crittografia a chiave pubblica è che uno dei due interlocutori sceglie una coppia di funzioni inverse, da usare una per la cifratura (per la cui computabilità si richiede un algoritmo di tipo P) e l' altra per la decifratura (per la cui computabilità si richiede un algoritmo di natura NP, per chi non conosce la chiave). Un altro utente può quindi usare l'algoritmo pubblico di cifratura per costruire un messaggio che solo chi ha fornito la chiave può decodificare. Perciò i due possono comunicare con riservatezza anche se inizialmente non condividono nulla di segreto.

Descritti brevemente alcuni metodi crittografici usati nella storia potremmo a questo punto chiederci se esistono criptosistemi perfetti. I sistemi fin qui considerati, a parte RSA, si basano su una permutazione rigida dei simboli dell'alfabeto o comunque di unità di messaggio. Questa rigidità è un punto di debolezza del sistema, quindi un involontario aiuto alla crittoanalisi di un qualsiasi pirata. Il Cifrario di Vigenère, ideato da Blaise de Vigenère nella seconda metà del '500, di cui già abbiamo parlato, cerca di ovviare a questi difetti e raffina e complica conseguentemente il procedimento di codifica e di decodifica. Propone infatti di cifrare mediante una permutazione delle lettere che non è costante ma varia in relazione alla loro posizione nel messaggio. In altre parole A e B concordano preventivamente una stringa di numeri naturali minori della cardinalità N dell'alfabeto (es. 14,7,8) e la fissano come chiave, dopo di che: A cifra i suoi messaggi addizionando 14 alla prima lettera, 7 alla seconda, 8 alla terza, 14 alla quarta e così via ciclicamente; B decifra conseguentemente sottraendo 14 dalla prima lettera, 7 dalla seconda…. Anche questo sistema, che è molto più raffinato di quello utilizzato da Cesare, ha i suoi punti deboli. Infatti la ripetitività della parola chiave può consentire a C, nel caso di messaggi molto lunghi, un qualche spiraglio per la crittoanalisi di frequenza. Si potrebbe operare un ricambio frequente della parola chiave, ma già sappiamo che la crittoanalisi può aggirare questa misura di prudenza, come la storia di Enigma e Turing. Maggiore sicurezza si può ottenere anche allungando la parola chiave. Operando in questo senso si arriva al caso limite in cui ogni messaggio è accompagnato da una sua propria parola chiave, della sua stessa lunghezza.

Il Cifrario di Vernam, proposto nel 1917 da Gilbert Vernam, prevedeva proprio questa strategia. All'epoca della sua scoperta questo suo cifrario non fece molto scalpore, forse perché la sua assoluta sicurezza fu dimostrata molto tempo dopo e perché la necessità di una chiave così ingombrante ostacolava l'uso generalizzato.

Nel 1949 Shannon affrontò con un approccio di tipo probabilistico il tema della sicurezza di un criptosistema: quando dichiararla assoluta, ed in ogni caso stabilirne il livello. Consideriamo sempre due interlocutori A e B e un pirata C che cerca di carpirne la corrispondenza. Immaginiamo che A e B utilizzino un criptosistema composto da: un insieme finito M di possibili messaggi; un insieme finito K di possibili chiavi; e che ogni $k \in K$ determini una coppia di funzioni da M a M, l'una inversa dell'altra, la prima $\mathbf{e_k}$ di codifica, la seconda $\mathbf{d_k}$ di decodifica. Quindi $\boldsymbol{d_k e_k(m)=m}$ per ogni messaggio m. Le lettere e,d sono suggerite dal compito richiesto a queste due funzioni, in inglese rispettivamente encrypt e decrypt. Possiamo introdurre quindi la definizione astratta di criptosistema: criptosistema è una struttura $\boldsymbol{(M, K, (e_k, d_k)_{k \in K})}$ dove M e K sono due insiemi finiti e, per ogni $k \in K$, e_k, d_k sono funzioni da M a M l'una inversa dell'altra.

Ammettiamo ora che mediante indagini statistiche sulla corrispondenza di A e B, C riesca ad assegnare a priori a ogni $m \in M$ una probabilità di essere inviato: dunque, se un dato messaggio m_o viene spedito da A a B, C può considerare la probabilità (Pr) al variare di $m \in M$ che m_o sia proprio m

$$\boldsymbol{Pr_{m \in M}(m_o = m)}$$

Ammettiamo poi che C intercetti la versione cifrata c_o di qualche messaggio. C non sa né il messaggio originario né la chiave che lo ha criptato, ma può considerare per ogni $m_o \in M$ la probabilità al variare di $k \in K$ che c_o sia proprio la codifica di m_o

$$\boldsymbol{Pr_{k \in K}(c_o = e_k(m_o))}$$

Possiamo ora definire un criptosistema perfetto: un criptosistema $(M, K,(e_k, d_k)_{k \in K})$ si dice perfetto se e solo se per ogni c_o in M, $\boldsymbol{Pr_{k \in K}(c_o = e_k(m_o))}$ è la stessa per tutti gli $m_o \in M$. In altre parole nessun vantaggio circa l' identificazione di m_o deriva a C dalla conoscenza di c_o. Shannon mostrò che l'unico cifrario perfetto è quello di Vernam, perché caratteristica fondamentale in un criptosistema perfetto è che in esso ci devono essere tante chiavi quanti sono i messaggi. Questa conclusione di Shannon è piuttosto scoraggiante, perché i cifrari di Vernam sono praticamente inutilizzabili, e quindi sembrerebbe di dover ammettere che non esistono criptosistemi perfetti che si possono adoperare nella vita comune.

CAPITOLO QUARTO

IL SISTEMA RSA

Ogni utente A del sistema dovrebbe utilizzare una sorgente che sia in grado di generare casualmente due numeri primi $p \neq q$ molto grandi e ne calcola il prodotto $N=pq$ (per la sicurezza del sistema è consigliabile un N dell' ordine di 10^{308}).

Conoscendo quindi N, p e q è molto semplice computare anche $\Phi(N) = (p-1)\,(q-1)$.

La funzione $\Phi(N)$, definita anche come funzione di Eulero, in onore del famoso matematico svizzero, permette di calcolare il numero degli interi ***a*** compresi tra 1 e N e primi con N. Se N è primo allora $\Phi(N) = N-1$**,** infatti ogni intero compreso tra 1 e N-1 è primo con N (ad esempio $\Phi(2) = 1$). Se N è una potenza p^k di un numero primo p, allora $\Phi(N) = p^{k-1}\,(p-1)$. Infatti siccome p è primo i numeri (tra 1 e N = p^k) che non sono primi con p sono p^{k-1}. Ecco la dimostrazione:

Tra p^{i-1} e p^i vi sono $\frac{\left(p^i - p^{i-1}\right)}{p}$ multipli di p cioè $\frac{p^{i-1}(p-1)}{p} = p^{i-2}(p-1)$(tra questi non è compreso p^{i-1}, per questo motivo nel prossimo conteggio aggiungeremo 1).

Suddividendo i numeri da 1 a p^k avremo: 1…p…p^2… p^{k-1}… p^k; tra 1 e p non vi sono multipli di p; i multipli di p sono:

$$\frac{(p^2-p)}{p}+\frac{(p^3-p^2)}{p}+\frac{(p^4-p^3)}{p}+.....+\frac{(p^k-p^{k-1})}{p}+1=$$

$$=\frac{p(p-1)}{p}+\frac{p^2(p-1)}{p}+\frac{p^3(p-1)}{p}+.....+\frac{p^{k-1}(p-1)}{p}+1=$$

$$=(p-1)+p(p-1)+p^2(p-1)+.....+p^{k-2}(p-1)+1=$$

$$=(p-1)(1+p+p^2+.....+p^{k-2})+1=(p-1)\frac{(1-p^{(k-2)+1})}{(1-p)}+1=$$

$$=-(1-p)\frac{(1-p^{k-1})}{(1-p)}+1=p^{k-1}-1+1=p^{k-1}$$

Di conseguenza i numeri primi con p sono $p^k - p^{k-1} = p^{k-1}\,(p-1)$. Ad esempio $\Phi(2^2) = 2^1 \cdot 1 = 2$. Se p e q sono due interi positivi primi tra loro allora $\Phi(p\,q) = \Phi(p) \cdot \Phi(q)$.

Abbiamo quindi dimostrato che $\Phi(N) = \Phi(p\,q) = \Phi(p)\;\Phi(q) = (p-1)\,(q-1)$.

Definiamo ora una congruenza: dati tre interi positivi a, b, n, con $n \neq 0$ diciamo che a e b sono congruenti modulo n se hanno lo stesso resto nella divisione per n ($a \equiv b \bmod(n)$).

Tutti i numeri naturali ***a*** chiamati a rappresentare le unità di messaggio sono molto minori di p e q, e conseguentemente, se diversi da zero, primi tanto con p quanto con q, e dunque anche con il prodotto N. Ogni **a** $\neq 0$ soddisfa il *teorema di Eulero*, che afferma: sia N un intero positivo, allora per ogni intero **a** primo con N

$$a^{\Phi(N)} \equiv 1 \pmod{N}$$

Ma **N** è primo anche con $\mathbf{a^t}$ per ogni intero positivo t, vale dunque:

$$(a^t)^{\Phi(N)} \equiv (a^{\Phi(N)})^t \equiv 1 \pmod{N}$$

Moltiplicando gli ultimi due membri di questa congruenza per **a** otteniamo:

$$(a^{\Phi(N)})^t \; a \equiv a \pmod{N}$$

A sceglie dunque 2 naturali $\mathbf{d_A}$ ed $\mathbf{e_A}$, l' uno inverso dell' altro modulo **Φ(N)**. Vale dunque:

$$d_A \, e_A \equiv 1 \pmod{\Phi(N)}$$

($\mathbf{d_A} \cdot \mathbf{e_A}$ ha resto 1 nella divisione per **Φ(N)** e dunque si può anche scrivere come: $d_A \, e_A = t \, \Phi(N) + 1$ per qualche opportuno naturale t). Allora per ogni naturale $\boldsymbol{a < p,q}$ (e quindi per ogni unità di messaggio) si ha

$$(a^{e_A})^{d_A} \equiv a^{e_A d_A} \equiv a^{t\phi(N)+1} \equiv (a^{\phi(N)})^t \, a \equiv a(\mathrm{mod}\, N)$$

A rende noti N e e_A come sua chiave pubblica, mantiene invece gelosamente segreto d_A ,la sua chiave privata. A questo punto, se un altro utente B vuole trasmettere ad A un messaggio **a**, lo eleva alla e_A modulo N

$$a \longrightarrow a^{e_A} (\mathrm{mod}\, N)$$

e lo invia così cifrato ad A. Questa è la procedura E_A di codifica per A.

A da parte sua recupera il testo originale elevando quanto ricevuto alla d_A modulo N

$$a^{e_A} \longrightarrow (a^{e_A})^{d_A} \equiv a(\mathrm{mod}\, N)$$

Così avviene la decodifica D_A.

Questo è il fondamento di RSA. Qual è il rischio che un pirata C riesca a violare un messaggio eventualmente intercettato? C conosce la chiave pubblica N, e_A e per decifrare deve recuperare a da a^{e_A}, in altre parole estrarre rapidamente le radici e_A-me modulo N.

La strada maestra per raggiungere questo obbiettivo sembra essere quella che si affida al recupero di d_A, infatti la radice e_A-me di un intero modulo N si ottiene elevando questo intero a d_A. D' altra parte d_A è identificato come l' inverso di e_A modulo Φ(N). Dunque il punto cruciale per infrangere RSA pare ridursi alla conoscenza di Φ(N) = (p - 1) · (q - 1), che a sua volta fa riferimento a p e q e, in conclusione alla

decomposizione di N in fattori primi. Siamo quindi nella situazione descritta in precedenza: poiché non esistono algoritmi rapidi per decomporre N, non c' è verso di infrangere RSA, almeno per questa via.

Sicuramente RSA è attualmente uno dei sistemi più sicuri per crittare messaggi. Con lo studio dei metodi di fattorizzazione la sicurezza di questo sistema è sempre minore. La matematica ha permesso la nascita di RSA, ma allo stesso tempo lo minaccia.

Un altro pericolo per questo sistema deriva dalla possibile costruzione di computer quantistici. Nel 1995 Peter Shor, un programmatore degli AT & Bell' s Laboratories del New Jersey ha presentato una serie di operazioni che possono essere eseguite su quantum computer e non su uno classico e ha mostrato come queste operazioni possono venir combinate in modo ingegnoso per risolvere in tempi brevissimi il problema della fattorizzazione . Nell' esempio di Shor il computer avrebbe richiesto 100.000 quantum bit che operassero coerentemente per un certo lasso di tempo, un sistema lontano da qualsiasi possibilità pratica. Ma Deutsch, Eckert e Barenco hanno trovato il modo per semplificare notevolmente il processo: un computer che potesse mantenere la coerenza fra 2000 quantum bit del tipo considerato sopra, risolverebbe il problema di fattorizzare RSA-129 in 8 secondi.

CAPITOLO QUINTO

CRITTOGRAFIA QUANTISTICA

Se da un lato la meccanica quantistica attraverso i quantum computer potrebbe distruggere l'attuale sistema più sicuro, dall'altro ha permesso di aprire nuovi orizzonti nel campo della crittografia. Abbiamo in precedenza dimostrato la sicurezza del cifrario di Vernam, resta però in sospeso un problema fondamentale: qualunque canale privato tradizionale può essere tenuto sotto controllo passivamente, senza che mittente e destinatario si accorgano di essere spiati. Per esempio, una chiave trasportata da un corriere fidato può essere letta di nascosto durante il trasferimento, senza che il corriere se ne accorga, con una scansione a raggi X ad alta risoluzione o con qualche altra tecnica molto avanzata per l'elaborazione di immagini. Più in generale la fisica classica consente di misurare tutte le proprietà fisiche di un oggetto senza perturbarle. Dato che tutte le informazioni, comprese le chiavi crittografiche, sono codificate tramite proprietà fisiche misurabili di qualche oggetto o segnale, la teoria classica offre la possibilità di atti di spionaggio passivi poiché consente alla spia di misurare le proprietà fisiche del sistema senza conseguenze su di esso.

Le cose stanno diversamente nella fisica quantistica. È opinione generale che la meccanica quantistica governi il comportamento di tutti gli oggetti, ma le sue conseguenze sono più rilevanti per gli oggetti microscopici, come singoli atomi o particelle subatomiche. L' atto della misurazione è parte integrante della fisica dei quanti, quindi è possibile progettare un canale quantistico in maniera tale che ogni tentativo di spiare il canale disturbi necessariamente il canale con conseguenze osservabili. In particolare è stato sfruttato il principio di indeterminazione per progettare un canale completamente sicuro basato sulle proprietà quantistiche della luce.

Nel 1984 è stato sviluppato il primo protocollo di crittografia quantistica, il BB84, dai nomi di Bennet e Brassard che lo proposero. In questo protocollo un bit viene codificato in una particolare polarizzazione di un fotone (un fotone può essere concepito come un minuscolo campo elettrico oscillante, e la direzione dell' oscillazione è la polarizzazione del fotone) a scelta fra le quattro fissate (0,45,90,135 gradi). Due polarizzazioni vengono interpretate con il valore 0 (0,45 gradi), due con il valore 1 (90,135 gradi). Per creare una chiave segreta, A sceglie a caso una delle quattro polarizzazioni, crea un fotone così polarizzato e lo invia a B, e ripete questa operazione per ogni bit della sua chiave che vuole creare. B riceve il fotone, ma non

sa quale polarizzazione ha scelto A, e deve effettuare una misura sul fotone per scoprirlo. Ma la scelta delle quattro polarizzazioni lo obbliga a scegliere fra due diverse misure non compatibili, una misura rettilinea che gli permette di scoprire due polarizzazioni (0,90 gradi), e una diagonale gli permette di rilevare le altre due (45,135 gradi). Se B sceglie la misura sbagliata rispetto alla polarizzazione usata da A, il risultato della misura è casuale, ovvero 0 od 1 a caso. Il punto fondamentale per la sicurezza è che anche C si trova nella stessa situazione di B: se intercetta dei fotoni deve scegliere fra le due misure possibili e se sceglie quella sbagliata ottiene un risultato casuale. Alla fine dell'invio dei fotoni B annuncia pubblicamente il tipo di misurazione che ha fatto, e A gli dice quali erano corrette. A questo punto A e B scartano tutti i fotoni/bit per i quali B ha scelto la misurazione sbagliata. A e B cioè hanno creato e si sono scambiati una chiave casuale detta "sifted key". Come fanno però a essere sicuri che C non l' ha intercettata? Se C ha in qualche modo intercettato i fotoni nel tragitto tra A e B, a causa del principio di indeterminazione esposto in precedenza, li ha per forza modificati. Se C ha intercettato e modificato dei fotoni, le misure di B avranno degli errori rispetto alle polarizzazioni inviate da A. Quindi se la sifted key di B è diversa da quella di A, vuol dire che C ha intercettato i fotoni e che la chiave non è sicura, poiché C è a conoscenza di almeno una parte di essa. Purtroppo c'è anche un altro problema che si va ad aggiungere: gli strumenti non sono perfetti e vi sono sempre fotoni persi o che non sono rilevati correttamente, cioè i cosiddetti errori sperimentali. È molto difficile distinguere con sicurezza tra errori dovuti a C e errori sperimentali. La soluzione del problema però è molto semplice: prima di tutto si assume che gli errori siano dovuti sempre a C; poi A e B debbono applicare due ulteriori fasi del protocollo alla sifted key. La prima si chiama Reconciliation e permette ad A e B di eliminare tutti gli errori della chiave e al contempo di stimare la percentuale di errori trovati. Se questa percentuale è minore dell' 11% allora si passa alla fase seguente detta Privacy Amplification: la chiave segreta viene modificata secondo una procedura tale che l' informazione che nel caso C possiede sulla chiave viene ridotta praticamente a zero. Questo è possibile perché se C ha introdotto errori solo per al più l' 11%, vuol dire che la sua conoscenza sulla sifted key è sufficientemente ridotta, quindi modificando appropriatamente la chiave segreta A e B possono eliminare i bit a conoscenza di C. In questo modo è possibile realizzare un cifrario perfetto, con la certezza che la chiave, lunga quanto il messaggio, non sia stata intercettata.

La crittografia quantistica è un' alternativa all'uso dei protocolli a chiave pubblica, come RSA; la differenza principale è che essa non teme attacchi basati sulla potenza di calcolo degli elaboratori (come i quantum computer) o sugli sviluppi di tecniche matematiche che permettano di rompere sistemi a chiave pubblica.

CAPITOLO SESTO

QUANTUM COMPUTER E CRITTOGRAFIA QUANTISTICA: APPLICAZIONI ATTUALI E PROSPETTIVE FUTURE

Il 3 giugno 2004 , Chip Elliot, capo della sezione di ricerca quantistica alla BBN Technologies di Cambridge, ha inviato il primo pacchetto di dati su Quantum Net, la prima rete a crittografia quantistica mai realizzata.

In questo campo sono possibili molti miglioramenti: infatti con le tecniche che utilizzano i fotoni è necessario avere a disposizione un' unica fibra ottica, il che limita la distanza di applicazione (ad oggi il massimo raggiunto è 150 chilometri).

Si prevede però che fra qualche anno saranno disponibili altre implementazioni della crittografia quantistica, anche via satellite, con la possibilità di copertura dell' intero globo terrestre.

Per quanto riguarda i computer quantistici, nel 2001 l'IBM all'Almaden Research Center ha creato un elaboratore quantistico a 7 qubit in grado di implementare l'algoritmo di fattorizzazione di Shor su numeri piccoli (precisamente sul 15, fattorizzato in 5 per 3). Il 13 febbraio 2007 la D-wave Systems al Museo di Storia dei Computer nella Silicon Valley ha presentato un nuovo prototipo di computer quantistico. Orion, questo è il nome del calcolatore, possiede 16 qubit, ed è riuscito a risolvere problemi banali, come un caso semplice del problema del Commesso Viaggiatore ed un puzzle Sudoku. La D-Wave si propone di arrivare entro la fine dell'anno a 32 qubit, 512 all'inizio del 2008 e 1024 entro la fine del 2008.

Il problema che hanno dovuto affrontare sia l'IBM che la D-Wave è la decoerenza quantistica: le particelle utilizzate come qubit rischiano di interagire con le particelle del mondo circostante e trasformarsi in modo praticamente casuale. Questo ovviamente porterebbe a risultati casuali. Un altro dubbio è stato sollevato da molti scienziati che si occupano di Elaboratori Quantistici. D-Wave ha scelto di realizzare il proprio elaboratore usando dei sistemi a superconduttori a temperature vicine allo zero assoluto, non è chiaro quindi se se Orion sia veramente un elaboratore quantistico o solamente un elaboratore superconduttore. La differenza fra questi due tipi di elaboratori è sostanziale: il primo adotta la logica quantistica ed è in grado di fare operazioni in modo impossibile altrimenti, il secondo adotta l'usuale logica digitale, ma raggiunge velocità impossibili altrimenti grazie alla superconduttività. D-Wave afferma di essere certa che Orion si comporta come un elaboratore quantistico, e che presto renderà pubbliche queste prove.

CAPITOLO SETTIMO

MECCANICA QUANTISTICA E FILOSOFIA

La meccanica quantistica è stata considerata non solo una rivoluzione in campo scientifico, ma anche in quello filosofico.

Abbiamo già parlato del principio di indeterminazione di Heisenberg, grazie al quale sappiamo che si possono fare solo previsioni probabili in base a statistiche opportunamente stabilite, ma non previsioni sicure sul comportamento futuro di una particella atomica sottoposta ad una osservazione. Con ciò il determinismo è stato espulso dalla scienza, così come il principio di causalità ritenuto il fondamento della spiegazione scientifica da tutta la scienza e la filosofia dell' '800. Non c' è dubbio infatti che l'interpretazione rigorosa del principio di causalità includa il determinismo, nel senso della possibilità della previsione infallibile di eventi futuri.

L'ideale deterministico della scienza era stato espresso da Pierre Simon Laplace con queste celebri parole: "Noi dobbiamo considerare lo stato presente dell'universo come l'effetto del suo stato anteriore e la causa di quello che seguirà. Un'intelligenza che, per un dato istante, conoscesse tutte le forze da cui la natura è animata e la situazione rispettiva degli esseri che la compongono, se fosse abbastanza vasta per sottomettere questi dati al calcolo, abbraccerebbe nella stessa formula i movimenti dei più grandi corpi dell'universo e quelli del più leggero atomo: niente sarebbe incerto per essa e l'avvenire come il passato sarebbe presente ai suoi occhi " (Theorie analytique des probalites).

La fisica dei quanti ha smentito questo ideale, la previsione infallibile infatti non è possibile, non per un' imperfezione dei mezzi di osservazione o di calcolo in possesso dell' uomo, ma perché questi mezzi influiscono imprevedibilmente sui fatti osservati.

Per salvare il determinismo rigoroso Max Planck ricorreva all'ipotesi di uno spirito ideale il quale, a differenza dell'uomo, non faccia parte della natura e non ne subisca le leggi cosicché possa conoscerla senza influenzarla: per questo spirito il principio di indeterminazione ovviamente non varrebbe.

Nel 1932 Von Neuman scriveva: "Non v'è oggi alcuna ragione che permetta d' affermare l'esistenza della causalità in natura e nessuna esperienza che possa darcene la prova" (Les fondements mathématiques de la mécanique quantique). Ciò non significa che la libertà e l' arbitrio siano stati riconosciuti come dominanti in natura. La fine del determinismo rigoroso espresso dalla formula classica del principio di causalità non significa la vittoria dell'indeterminismo, piuttosto l'avvio all'

elaborazione di nuovi schemi esplicativi, nei quali alla connessione necessaria degli eventi si sostituiscono le connessioni possibili. Nel XVIII secolo Hume aveva anticipato una concezione simile, come possiamo leggere nel suo Trattato sulla natura umana: "Tutti i ragionamenti che riguardano la causa e l'effetto sono fondati sull'esperienza e tutti i ragionamenti che derivano dall'esperienza sono fondati sulla supposizione che il corso della natura continuerà ad essere uniformemente lo stesso. Noi concludiamo che cause simili, in circostanza simili,produrranno sempre effetti simili. […] Quando vedo una palla da biliardo che si muove verso l'altra, la mia mente è immediatamente spinta dall'abitudine verso il consueto effetto ed anticipa la mia vista concependo la seconda palla in movimento. Non c'è nulla in questi oggetti, astrattamente considerati, ed indipendentemente dall'esperienza, che mi porti a formulare una simile conclusione; ad anche dopo che io abbia avuto esperienza di molto effetti di questo genere che si siano ripetuti, non c'è argomento che mi determini a supporre che l'effetto sarà conforme all'esperienza passata".

Oltre a mettere in crisi il principio di casualità, la fisica quantistica minaccia un altro ideale scientifico: quello della descrizione della natura. Il concetto di descrizione è servito alla scienza positivista dell'800 da un lato a liberare la scienza dalle sue soprastrutture metafisiche, dall'altro ad accentuare il carattere sperimentale e d'osservazione. Ma la possibilità di una descrizione della natura (cioè del corso oggettivo dei fenomeni) viene messa in crisi dalla fisica dei quanti. È Einstein ad affermare: "La fisica quantistica prescinde da leggi individuali riferibili a particelle elementari e formula direttamente leggi statistiche governanti gli aggregati. Non è possibile basarsi sulla fisica quantistica per descrivere posizioni e velocità di una particella elementare o per predirne il percorso, come avviene nella fisica classica. La fisica dei quanti tratta unicamente gli aggregati e le sue leggi valgono per le moltitudini e non per gli individui"(The Evolution of Physics). E ancora"La teoria dei quanti non ci fornisce un modello di descrizione degli eventi reali dello spazio-tempo ma solo le distribuzioni di probabilità per le misure possibili in funzione del tempo" (Conceptions scientifiques morales et sociales).

Con la meccanica quantistica è lo stesso concetto di realtà fisica ad entrare in crisi, e possiamo distinguere due diverse interpretazioni di esso; la prima è quella di Niels Bohr, definita ortodossa, condivisa da Heisenberg e Jordan, secondo la quale il concetto di realtà fisica deve includere le condizioni che rendono possibile l' osservazione della realtà stessa; e da questo punto di vista l'influenza che l'

osservazione esercita sul comportamento futuro di un sistema fisico fa parte dello stesso sistema fisico; la meccanica quantistica non è quindi incompleta o provvisoria, ma destinata a svilupparsi nella direzione già presa.

L'altra interpretazione è quella di Einstein, sostenuta anche da De Broglie e Scrödinger, che si mantiene fedele al concetto tradizionale della realtà fisica come insieme di entità individuali, i cui caratteri sono indipendenti dall'osservazione. "Non posso non confessare", dice Einstein, "che attribuisco un'importanza solo transitoria all'interpretazione quantistica. Io credo ancora nella possibilità di un modello di realtà, credo in una teoria che rappresenti le cose stesse e non semplicemente la probabilità del loro manifestarsi" (On the Method of Theoretical Physics). È errata l' immagine comunemente diffusa di un Einstein arroccato su posizioni anacronistiche di rifiuto della meccanica quantistica (celebri le sue parole "Dio non gioca a dadi"): egli, da considerarsi uno dei fondatori della teoria stessa, ha riflettuto molto su questo nuovo formalismo mutando la sua posizione e mantenendo un atteggiamento critico su alcuni suoi aspetti, che sarà il punto di partenza per le riflessioni e le scoperte scientifiche future. "La funzione d'onda quantistica non fornisce una descrizione completa della realtà fisica. In futuro s'imporrà una teoria che farà a meno degli aspetti statistici, ma dovrà introdurre un notevole numero di variabili" (Il paradosso EPR, di Einstein, Podolsky e Rosen).

Analizzati i motivi per cui la meccanica quantistica viene considerata una rivoluzione, sia scientifica che filosofica, soffermiamoci ora sulle modalità attraverso le quali si realizza una rivoluzione scientifica. In particolare esaminiamo l'opera di Kuhn, pubblicata nel 1962, "La struttura delle rivoluzioni scientifiche", che segna l'avvio della crisi della epistemologia di orientamento positivistico e l'inizio di una epoca di dibattiti epistemologici. Carnap, Popper, e altri esponenti della tradizione neoempiristica, ispirati al filone illuministico settecentesco e positivistico ottocentesco, rivendicavano alla scienza il compito essenziale di dirci come è fatto il mondo, come funziona, quali leggi ci consentono di prevedere i fatti futuri.

L'opera di Kuhn è fuori da questa concezione logica: la scienza non ha il compito di spiegare o conoscere il mondo, di fornirci le leggi del suo funzionamento, ma è un' attività svolgentesi nell'ambito di tradizioni e comunità, diretta a risolvere "rompicapi". Le rivoluzioni scientifiche non vengono analizzate da Kuhn dal punto di vista della maggiore o minore conoscenza fornita dalle teorie scientifiche vincenti o

perdenti, ma dal punto di vista della maggiore o minore efficacia nella offerta di strumenti per risolvere rompicapi.

Al centro degli interessi filosofici ed epistemologici di Kuhn è il problema di come e perché avvengono i mutamenti radicali nelle scienze. Kuhn anticipa nel saggio del 1959 "La tensione essenziale" alcuni temi fondamentali della sua filosofia della scienza; egli rifiuta le interpretazioni prevalenti che considerano l'emergere di nuove scoperte e teorie scientifiche come il risultato di un processo cumulativo, per cui non sarebbero altro che "semplici aggiunte alla raccolta attuale delle conoscenze scientifiche". La sue tesi è invece che "la scoperta e l'invenzione nelle scienze sono in generale intrinsecamente rivoluzionarie", cioè che quando si verificano episodi di questo tipo "una comunità scientifica abbandona una modalità di guardare al mondo e di esercitare la scienza un tempo affermata, in favore di un qualche altro , usualmente incompatibile, approccio alla disciplina" (La tensione essenziale).

Nel saggio di Kuhn è presente anche una tesi che farà discutere molto: la condizione normale della scienza non è affatto quella di fare scoperte, infatti spetta alle rivoluzioni scientifiche l'ambito della invenzione e del rinnovamento; ma "le rivoluzioni sono solo uno dei due aspetti complementari del progresso scientifico". L' aspetto rivoluzionario e quello normale (o convergente), nelle scienze danno luogo a quello che nel saggio viene definita "tensione essenziale ", implicita nella ricerca scientifica. Secondo l'autore statunitense la norma è la ricerca normale o convergente, mentre le rivoluzioni costituiscono l'eccezione; esse infatti introducono il dissenso, la divergenza, e portano alla crisi delle modalità d'approccio dominanti e alla loro sostituzione con nuove modalità di approccio.

Ne "La struttura delle rivoluzioni scientifiche" Kuhn riprende il concetto della "tensione" presente tra scienza normale e rivoluzione scientifica; inizialmente si sofferma sul rapporto tra scienza normale e paradigmi (l' insieme di regole, teorie procedure comunemente accettato e praticato da una comunità scientifica): la normalità è il raggiungimento della maturità da parte di una scienza, e ciò avviene quando la comunità di ricercatori pratica e difende un paradigma. Il significato preciso del termine paradigma viene precisato dall'autore: non è un modello o schema che consente la sola riproduzione, ma è uno strumento che consente di operare in maniera innovativa nel risolvere problemi e rompicapi che si presentano nell'attività quotidiana della scienza normale. Ogni comunità scientifica tende, secondo Kuhn, a rimanere nell'ambito dei problemi ordinari, il paradigma infatti offre "un criterio per

scegliere i problemi che, nel tempo in cui si accetta il paradigma, sono ritenuti solubili". Questo è chiaramente un atteggiamento difensivo e conservativo poiché in questo modo vengono scartati altri problemi "respinti come metafisici, come appartenenti ad un'altra disciplina, o a volte troppo problematici per meritare che si sciupi del tempo attorno ad essi". Kuhn sottolinea i pericoli di questo atteggiamento conservativo: "Un paradigma può finire addirittura, per questa via, con l'isolare la comunità da quei problemi socialmente importanti che non possono venire formulati nei termini degli strumenti tecnici e concettuali forniti dal paradigma" .

La storia della scienza è però fatta anche da scoperte e invenzioni, che danno poi origine a nuovi paradigmi che sostituiscono quelli vecchi, incapaci di spiegare quelle scoperte e invenzioni. "La scoperta comincia con la presa di coscienza di una anomalia, ossia col riconoscimento che la natura ha in un certo modo violato la aspettative suscitate dal paradigma che regola la scienza normale; continua poi con una esplorazione dell' area dell' anomalia, e termina solo quando la teoria paradigmatica è stata riadattata, in modo che ciò che appariva anomalo diventi ciò che ci si aspetta". Il riadattamento però non è una semplice aggiunta, ma è un riorientamento complessivo che porta a guardare in maniera differente i fatti nuovi, che altrimenti non potrebbero rientrare nella categoria di fatti scientifici. In tutte le rivoluzioni scientifiche l'abbandono del vecchio paradigma e l'accettazione di uno nuovo sono preceduti e accompagnati da una situazione di crisi; infatti il vecchio paradigma risulta incapace di spiegare le anomalie presentatesi; questo fallimento provoca una "proliferazione di teorie" che in maniera diversa tentano di dare una spiegazione soddisfacente; la teoria vincente pone termine alla crisi e viene accettata come un nuovo paradigma: a questo punto la rivoluzione scientifica è compiuta.

Kuhn si domanda poi perché un mutamento di paradigma dovrebbe essere chiamato rivoluzione, un termine che ha una sua più diffusa presenza in campo politico e sociale. Costruisce così un' analogia tra rivoluzioni scientifiche e politiche: "Le rivoluzioni politiche mirano a mutare le istituzioni politiche in forme che sono proibite da quelle stesse istituzioni. Il loro successo richiede perciò l'abbandono parziale di un insieme di istituzioni a favore di altre, e nel frattempo la società cessa completamente di essere governata da istituzioni". È la stessa situazione di crisi che si verifica in ambito scientifico: alla proliferazione delle teorie corrisponde la proliferazione di partiti e programmi politici; alla vittoria di un nuovo paradigma che

porta ad una nuova scienza normale corrisponde la vittoria di un partito e di un programma politici che portano ad un nuovo assetto istituzionale.

Esiste a questo punto un criterio di verità per le scienze e di giustizia sociale assoluta per i programmi politici? La risposta di Kuhn è negativa: sia le teorie rivali sia i partiti politici rivali non possono fare riferimento ad alcunché di esterno ad essi; la loro forza quindi sta soltanto nella capacità di argomentare e persuadere, per cui l' unico criterio del loro successo è individuabile nel consenso che riescono ad ottenere.

"Tanto nelle rivoluzioni politiche come nella scelta di paradigmi, non v' è nessun criterio superiore al consenso della popolazione interessata". Non le verità, né la ragione, ma la persuasività è la condizione indispensabile perché una nuova teoria vinca e diventi il nuovo paradigma di una scienza normale.

Tradizionalmente il processo scientifico fa riferimento ad uno scopo, una meta, verso cui le scienze e la conoscenza tenderebbero: la rappresentazione vera della realtà.

Kuhn è molto lontano da questa posizione teorica e, in un certo senso, la rovescia: il progresso di cui parlerà è infatti progresso a partire da un qualche paradigma, non progresso verso qualcosa. Egli intende discutere e sostituire la nozione tradizionale che connette il progresso scientifico al raggiungimento della verità: infatti molti problemi, connessi con la tematica del progresso, verranno accantonati, si dissolveranno, se sostituiamo "l'evoluzione verso ciò che vogliamo conoscere con l'evoluzione a partire da ciò che conosciamo".

Uno degli aspetti più innovativi dell'opera di Kuhn riguarda la mancanza di continuità di tipo cumulativo tra una scienza normale perdente e un nuovo paradigma vincente: "Paradigmi successivi ci dicono cose differenti sugli oggetti che popolano l'universo e sul comportamento di tali oggetti […] Ma i paradigmi differiscono anche in qualcos'altro che negli oggetti, giacché essi sono rivolti, non solo alla natura, ma anche alla scienza precedente che li ha prodotti". Essi producono un riorientamento complessivo, con un nuovo vocabolario, nuovi concetti, nuovi metodi e regole, per cui "l'accoglimento di un nuovo paradigma spesso richiede una nuova definizione di tutta la scienza corrispondente"; Kuhn arriva alla conclusione che la situazione prodotta da una rivoluzione scientifica è incompatibile con la situazione precedente di dominio di una scienza normale.

BIOBLIOGRAFIA

S. Leonesi, C. Toffalori, ”Numeri e Crittografia ”, Edizioni Springer

S. Lloyd, “Il programma dell’universo”, Einaudi Editore, 2006

G. C. Ghirardi, “Un’occhiata alle carte di Dio”, Edizioni Est, 2001

M. Ghiozzi, “Storia della Fisica”, Bollati Boringhieri, 2003 (edizione ampliata)

“Le Scienze” (Scientific American), numero 112 “Fenomeni Quantistici”, gennaio 2002 (ristampa); articoli: “Calcolatori quantistici” di S. Lloyd, “Crittografia quantistica” di Bennet, Brassard, Ekert.

SITOGRAFIA

www.dwavesys.com

www.tdf.it (“I computer quantistici” di Luisa Spairani)

www.ecplanet.com

www.wikipedia.org

INDICE