La distribuzione quantistica di chiavi

"La scienza non è nient'altro che una perversione se non ha come suo fine ultimo il miglioramento delle condizioni dell'umanità."

Nikola Tesla

Samuele Altilia *Dipartimento di Fisica "Aldo Pontremoli", Università degli Studi di Milano*

Michele N. Notarnicola *Dipartimento di Fisica "Aldo Pontremoli", Università degli Studi di Milano*

Stefano Olivares *Dipartimento di Fisica "Aldo Pontremoli", Università degli Studi di Milano*

Tra le tecnologie che hanno beneficiato delle proprietà quantistiche della natura, particolare spazio è riservato alla comunicazione quantistica e alla cosiddetta "distribuzione quantistica di chiavi", che sta tuttora avendo un notevole sviluppo anche a livello commerciale. In queste pagine illustreremo gli aspetti fisici che stanno alla base della distribuzione quantistica di chiavi (*Quantum Key Distribution*, QKD) e illustreremo le principali applicazioni a variabili discrete e a variabili continue che utilizzano i fotoni per codificare e condividere in modo sicuro l'informazione.

La teoria che chiamiamo comunemente "Meccanica Quantistica" permette di descrivere con grande accuratezza il mondo che ci circonda. Questa teoria ha altresì alcuni aspetti peculiari che non solo la rendono affascinante e, per così dire, strana rispetto al senso comune, ma che spianano la strada ad applicazioni tecnologiche che vanno ben oltre quelle permesse dalla fisica classica, ovvero dalla meccanica, dalla termodinamica e dall'elettromagnetismo.

Nel seguito introdurremo i concetti di sovrapposizione ed *entanglement* quantistici su cui si fondano la comunicazione e la computazione quantistica. Ma non solo, in quanto il loro studio ha condotto allo sviluppo di tecnologie quantistiche, che sono l'oggetto della seconda rivoluzione quantistica di cui siamo spettatori in questi anni.

Nelle prossime pagine illustreremo come queste proprietà dei sistemi fisici possano permettere di condividere informazioni in modo più sicuro rispetto a quanto sia possibile fare con mezzi classici.

Tra teoria e realtà fenomenologica

La fisica è la scienza che studia i fenomeni naturali e le leggi che li governano.

Partendo dall'osservazione del mondo che ci circonda, vengono identificate alcune leggi (o paradigmi) fondamentali grazie alle quali è possibile dare una descrizione scientifica di quanto

accade nel mondo intorno a noi. Grazie a quelle leggi è anche possibile prevedere nuovi fenomeni che devono essere verificati progettando ed eseguendo esperimenti più o meno sofisticati per validare o meno la teoria stessa. Questo permette il progresso della scienza [1].

Da una parte troviamo teorie ormai assodate che vengono ulteriormente perfezionate e completate (si pensi, ad esempio, alla meccanica classica di Newton e Galileo e quella relativistica di Einstein). Dall'altra possono emergere indizi che mostrano l'inadeguatezza delle teorie note, conducendo alla nascita di nuove teorie, come nel caso del lavoro di Max Planck che ha portato al quanto d'azione e, infine, alla fisica quantistica [2, 3, 4].

Così come la meccanica classica si fonda sulle leggi di Newton, la termodinamica sui suoi tre principi (ma è possibile anche riformularla in modo prettamente assiomatico [5, 6]) e l'elettromagnetismo sulle equazioni di Maxwell, anche la meccanica quantistica ha i suoi postulati. C'è però una differenza sostanziale tra quella che chiamiamo comunemente fisica classica e quella quantistica, che anche i non esperti osservano quotidianamente senza a volte esserne consapevoli.

Le leggi della fisica classica descrivono i fenomeni con cui abbiamo a che fare ogni giorno: il cadere di una foglia, il raffreddarsi di una tazza di caffè o il ronzare di un motore elettrico. La descrizione quantitativa dei fenomeni che abbiamo menzionato può richiedere modelli matematici molto complicati, ma il risultato finale non ci stupirebbe in quanto la nostra esperienza li rende comunque intuitivi.

Non è così per le previsioni della meccanica quantistica che spesso si riferiscono al comportamento di sistemi microscopici (ma non solo!) che non sono direttamente accessibili alla nostra esperienza sensoriale. Ed ecco che spesso si parla di stranezze e misteri: niente di più fuorviante! Tutto nasce dal voler inquadrare ostinatamente nella nostra esperienza quotidiana fenomeni naturali che non abbiamo mai sperimentato. Si pensi all'esibizione di un bravissimo prestidigitatore che ci lascia a bocca aperta davanti ad una sua magia spettacolare: spesso il risultato va contro il nostro senso comune, ed ecco che ci appare magico. Tuttavia, una volta svelato il meccanismo a volte ingegnoso che sta dietro a quanto abbiamo visto (e quindi percepito con i nostri sensi), la nostra mente inquadra l'esibizione in una serie di passaggi logici che rendono tutto nuovamente intuitivo e, per così dire, naturale.

Possiamo affermare che qualcosa di simile valga anche per la Meccanica Quantistica. Certamente i suoi postulati ci permettono di descrive in modo accurato il mondo microscopico, quello a cui appartengono atomi, molecole e fotoni, i quanti di luce; ma grazie a questi possiamo anche dare una descrizione accurata e quantitativa, ad esempio, del perché il nostro cielo sia così azzurro oppure utilizzare tecnologie altrimenti inesistenti, come la risonanza magnetica nucleare o il GPS, che si basa sulla estrema precisione degli orologi atomici.

È possibile introdurre gli assiomi della Meccanica Quantistica partendo da alcune chiare situazioni sperimentali e qui ne consideriamo una specifica e, passateci il termine, paradigmatica: l'interferenza. Per un approfondimento divulgativo ma comunque sufficientemente rigoroso sui postulati fondamentali della meccanica quantistica con questo tipo di approccio si veda, ad esempio, la Ref. [7].

Sovrapposizione e interferenza

Vi sarà capitato di osservare quello che accade quando le onde su uno specchio d'acqua si sovrappongono: quando due creste passano contemporaneamente nello stesso punto si ha un aumento dell'altezza complessiva, quando una cresta incontra un ventre di un'altra onda, si ha una diminuzione dell'altezza. Si parla di "interferenza costruttiva e distruttiva", rispettivamente. Lo stesso fenomeno si ha quando si illuminano con una sorgente LASER due fenditure praticate su uno schermo: al di là dello schermo di osserva una figura di interferenza. In questo caso l'elettromagnetismo ci spiega che ogni fenditura genera dei fronti d'onda analoghi a quelli generati da un sasso gettato in uno stagno. Quando le onde provenienti dalle due fenditure (o sorgenti) si sovrappongono si ha, appunto, interferenza.

Se consideriamo un dato punto x al di là delle fenditure e indichiamo con $E_1(x)$ ed $E_2(x)$ i campi elettrici in tale punto delle onde provenienti dalle fenditure 1 e 2, l'intensità totale della

luce in x è data da (per semplicità assumiamo che i campi abbiano la stessa polarizzazione e frequenza):

$$I_{\text{tot}}(x) = \left|E_1(x) + E_2(x)\right|^2, \tag{1}$$

in quanto il campo in quel punto è fornito dalla combinazione lineare $E_{\text{tot}} = E_1 + E_2$. Ricordiamo che, in generale, il campo elettrico è rappresentato da un numero complesso, quindi se poniamo $E_1(x) = A_1\, e^{i\phi_1(x)}$ e $E_2 = A_2\, e^{i\phi_2(x)}$, otteniamo:

$$\begin{aligned} I_{\text{tot}}(x) = {} & A_1^2 + A_2^2 \\ & + 2A_1A_2 \cos\left[\phi_1(x) - \phi_2(x)\right], \end{aligned} \tag{2}$$

e l'ultimo termine è responsabile dell'interferenza osservata.

Così come accade per un fascio di luce, anche quando si inviano fasci di particelle materiali (elettroni, atomi, fullereni,...) opportunamente preparati si ottiene un risultato simile: interferenza! I postulati della meccanica quantistica ci dicono che per descrivere quanto accade dobbiamo associare una **funzione d'onda** complessa ψ ad ogni particella che passa dallo schermo in cui sono praticate le fenditure. Dal momento che ci sono due fenditure, la funzione d'onda in un dato punto x al di là dello schermo sarà (si veda la referenza [7] per i dettagli):

$$\psi(x) \propto \psi_1(x) + \psi_2(x), \tag{3}$$

dove i pedici 1 e 2 si riferiscono alle due fenditure come sopra.

Si nota l'analogia con quanto fatto per le onde elettromagnetiche (la luce), analogia che svanisce nel momento in cui consideriamo il modulo quadro di $\psi(x)$. I postulati della Meccanica Quantistica, infatti, affermano che la quantità:

$$p(x) \propto \left|\psi(x)\right|^2 \tag{4}$$

corrisponde alla densità di probabilità di trovare nel punto x la particella che proviene dallo schermo con le due fenditure [7]. Anche in questo caso possiamo scrivere $\psi_1(x) = \mathcal{A}_1\, e^{i\varphi_1(x)}$ e $\psi_2(x) = \mathcal{A}_2\, e^{i\varphi_2(x)}$ e ricaviamo:

$$\begin{aligned} p(x) \propto {} & \mathcal{A}_1^2 + \mathcal{A}_2^2 \\ & + 2\mathcal{A}_1\mathcal{A}_2 \cos\left[\varphi_1(x) - \varphi_2(x)\right], \end{aligned} \tag{5}$$

Il qubit

Un **qubit**, o bit quantistico, è un sistema fisico che può esistere in due soli stati ben distinti (ortogonali), che possiamo indicare con $|0\rangle$ e $|1\rangle$, mimando il bit classico che è associato ai simboli "0" e "1". Lo stato generico di un qubit può essere scritto come la sovrapposizione:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle.$$

ed ecco ancora il termine di interferenza!

Quello che abbiamo visto all'opera, responsabile dell'interferenza quantistica, è il cosiddetto "principio di sovrapposizione", conseguenza della linearità della teoria quantistica: una combinazione lineare di funzioni d'onda (opportunamente normalizzata) è ancora una legittima funzione d'onda del sistema in questione [7].

Il qubit

Supponiamo di avere un sistema fisico che possa avere solo due configurazioni particolari, o stati. Abbiamo diversi esempi in natura di un tale sistema: una lampadina accesa o spenta, un condensatore carico o scarico, oppure, passando al mondo microscopico, un atomo in un livello fondamentale o eccitato, un fotone polarizzato orizzontalmente o verticalmente ...

Per essere più generali possibili, indichiamo i due stati utilizzando la ben nota codifica binaria che si serve dei simboli "0" e "1" associati ad un *bit* di informazione. Per passare alla descrizione quantistica, possiamo dire che al sistema che si trovi nello stato "0" associamo la funzione d'onda ψ_0 e, analogamente, associamo la funzione d'onda ψ_1 a quello che si trova nello stato "1". Dal momento che abbiamo a che fare con un sistema binario, è utile associare a ψ_0 e ψ_1 due vettori colonna bidimensionali ortogonali che indicheremo con i simboli introdotti da Paul M. Dirac:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{6}$$

detti **ket**, e i corrispondenti vettori riga:

$$\langle 0| = (1,0) \quad \text{e} \quad \langle 1| = (0,1)\,, \tag{7}$$

chiamati **bra**. In questo modo diventa possibile rappresentare il **prodotto interno** riga per colonna tra i vettori come segue:

$$\begin{aligned}
\langle 0|0\rangle &= (1,0)\cdot\begin{pmatrix}1\\0\end{pmatrix} = 1,\\
\langle 1|1\rangle &= (0,1)\cdot\begin{pmatrix}0\\1\end{pmatrix} = 1,\\
\langle 0|1\rangle &= (1,0)\cdot\begin{pmatrix}0\\1\end{pmatrix} = 0,\\
\langle 1|0\rangle &= (0,1)\cdot\begin{pmatrix}1\\0\end{pmatrix} = 0,
\end{aligned} \tag{8}$$

Dati gli stati $|0\rangle$ e $|1\rangle$, la sovrapposizione:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{9}$$

rappresenta il generico stato di quello che comunemente si chiama bit quantistico o **qubit** (*quantum bit*). Osserviamo che lo stato $|\psi\rangle$ è normalizzato:

$$\left|\langle\psi|\psi\rangle\right|^2 = 1, \tag{10}$$

mentre le quantità

$$P_0 = \left|\langle 0|\psi\rangle\right|^2 = \cos^2\left(\frac{\theta}{2}\right), \tag{11}$$

e

$$P_1 = \left|\langle 1|\psi\rangle\right|^2 = \sin^2\left(\frac{\theta}{2}\right), \tag{12}$$

che seguono della linearità del prodotto interno e dalle (8), corrispondono alla probabilità che misurando il qubit utilizzando la base $\{|0\rangle, |1\rangle\}$ si ottenga come risultato "0", ovvero qubit nello stato $|0\rangle$, oppure "1", qubit nello stato $|1\rangle$.

Una sovrapposizione particolare è quella che si ha quando i due simboli, $|0\rangle$ e $|1\rangle$, hanno la stessa probabilità. In particolare, nel seguito ci focalizzeremo sui due stati:

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}. \tag{13}$$

Analogamente a quanto accade per i bit classici, i qubit permettono di codificare, trasmettere ed elaborare informazione. Tuttavia, mentre con n bit si può codificare una sola delle 2^n successioni di bit possibili, con lo stesso numero di qubit diventa possibile creare una sovrapposizione di tutte le 2^n possibilità. Ad esempio, nel caso di 2 bit, possiamo codificare volta per volta una sola delle coppie "00", "01", "10" e "11", mentre con 2 qubit è possibile creare la sovrapposizione:

$$\begin{aligned}
|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle\\
+ \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle
\end{aligned} \tag{14}$$

dove $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$ e la scrittura "$|x\rangle|y\rangle$" indica che il primo qubit si trova nello stato $|x\rangle$ e il secondo in $|y\rangle$.

In particolare, gli stati di due qubit:

$$|\Psi^{(\pm)}\rangle = \frac{|0\rangle|1\rangle \pm |1\rangle|0\rangle}{\sqrt{2}}. \tag{15}$$

e

$$|\Phi^{(\pm)}\rangle = \frac{|0\rangle|0\rangle \pm |1\rangle|1\rangle}{\sqrt{2}}. \tag{16}$$

sono chiamati "stati di Bell", in onore di J. S. Bell scopritore delle celebrate "disuguaglianze", e sono stati *entangled*. In questo luogo non abbiamo modo di approfondire il concetto di *entanglement* e le sue implicazioni, vi rimandiamo perciò alla Ref. [7] per maggiori dettagli e per un'introduzione alle disuguaglianze di Bell, che hanno portato all'assegnazione dei premi Nobel per la Fisica del 2022 [8].

Abbiamo ora tutti gli elementi per comprendere il funzionamento del principale protocollo quantistico di distribuzione di chiavi, proposto da Charles H. Bennett e Gilles Brassard nel 1984 e noto come "BB84" [9].

Il problema della distribuzione quantistica di chiavi

L'importanza della *privacy* e della sicurezza delle comunicazioni è cruciale in molti contesti, sia privati, si pensi alla protezione dei dati sensibili personali o alle transazioni online, sia pubblici, come le comunicazioni governative e militari.

Per garantire che un messagio inviato tra due parti, che chiameremo Alice e Bob, sia al sicuro durante il suo trasferimento, si può ricorrere alla tecnica della cifratura: questa consiste nel manipolare in modo opportuno il messaggio stes-

so per mezzo di una sequenza o stringa di dati detta **chiave**. In questa maniera l'informazione diventa incomprensibile a chiunque non possegga la chiave e solo chi la possiede può, appunto, decifrare correttamente il messaggio. L'indecifrabilità del messaggio cifrato da parte di una spia, che chiameremo Eve, è garantita da un teorema matematico, noto come teorema di Vernam [10], a patto che la chiave sia completamente casuale, lunga quanto il messaggio stesso e utilizzata una sola volta (il cosiddetto *one-time pad*, OTP) [11].

Il problema della crittografia diventa quindi quello della distribuzione di chiave, ossia di far sì che Alice e Bob condividano una stessa chiave casuale sicura. Esistono vari protocolli classici di scambio di chiave, i quali tipicamente sfruttano la complessità computazionale di specifici problemi matematici. Un esempio rilevante tra questi è l'algoritmo RSA (dalle iniziali di Rivest, Shamir e Adleman, che lo hanno introdotto nel 1977 [12]), la cui sicurezza si fonda sulla notevole difficoltà nel fattorizzare in tempi brevi numeri interi molto, molto grandi; difficoltà che si traduce in tempi estrememante lunghi se paragonati a quelli di effettivo utilizzo della chiave stessa [12]. Tuttavia, pur non essendoci attualmente un algoritmo efficiente per la fattorizzazione, non esiste nemmeno una prova matematica definitiva che escluda la possibilità di scoprirne uno in futuro. Inoltre, il progresso della computazione quantistica costituisce una minaccia crescente per la sicurezza delle attuali tecnologie di crittografia. I computer quantistici, infatti, potrebbero in futuro comprometterne la robustezza grazie alla loro potenziale capacità di risolvere specifici problemi in tempi significativamente più brevi rispetto ai computer tradizionali sfruttando algoritmi quantistici, quale quello per la fattorizzazione proposto da Shor [13].

Se da una parte i principi della fisica quantistica rischiano di mettere in discussione i protocolli di crittografia attualmente in uso, dall'altra costituiscono anche una preziosa risorsa per risolvere in modo definitivo il problema dello scambio di chiave. Sistemi che implementano distribuzione quantistica di chiavi (*quantum key distribution*, QKD) sono già sufficientemente maturi dal punto di vista tecnologico da essere prodotti a livello commerciale e applicati in diversi contesti. Diversi protocolli di QKD sono stati disegnati sfruttando sia sistemi a variabili discrete, i.e. qubit, sia sistemi a variabili continue, come ad esempio impulsi LASER. Nel seguito presentiamo i principali risultati per ciascuna delle due piattaforme.

Sistemi a variabili discrete: il protocollo BB84

Il primo protocollo per la QKD ad essere stato introdotto, nonché ora il più diffuso a livello commerciale, è il BB84 [9]. Per realizzarlo sono necessari due canali di comunicazione: uno quantistico e uno classico. Attraverso il canale quantistico vengono inviati singoli fotoni e il grado di libertà fisico su cui viene tipicamente codificata l'informazione è la loro polarizzazione. Il canale classico, invece, deve essere autenticato per garantire la corretta provenienza dei messaggi scambiati, ma questi sono trasmessi in chiaro, quindi accessibili a chiunque possa intercettarli.

Utilizzando il formalismo introdotto nel paragrafo precedente, indicheremo con $|0\rangle$ e $|1\rangle$ gli stati con polarizzazione orizzontale e verticale, e con $|-\rangle$ e $|+\rangle$ le loro combinazioni lineari definite nella (13), che corrispondono fisicamente ai due stati di polarizzazione a $-45°$ e $+45°$. Chiameremo la base formata dai due stati $\{|0\rangle, |1\rangle\}$ "base $\bigoplus$" e quella degli stati $\{|-\rangle, |+\rangle\}$ "base $\bigotimes$". In questa codifica, possiamo ad esempio associare agli stati $|0\rangle$ e $|-\rangle$ il valore logico "0", e agli stati $|1\rangle$ e $|+\rangle$ il valore logico "1".

Elemento chiave del protocollo è che gli stati quantistici codificati in una base e misurati in un'altra non forniscono alcuna informazione deterministica. Infatti, se per esempio Alice invia a Bob lo stato $|+\rangle$ e Bob lo misura sulla base $\bigotimes$, il risultato ottenuto sarà sempre "1"; viceversa, se Bob lo misura sulla base $\bigoplus$ egli otterrà con uguale probabilità pari a $1/2$, i risultati "0" oppure "1", come si può ricavare facilmente ricordando le (11) e (12) e adattandole al nostro caso. In altre parole, se uno stato viene codificato in una base specifica e successivamente misurato in nell'altra base, il risultato della misura sarà totalmente casuale e non consentirà di ottenere alcuna informazione utile circa il segnale effettivamente inviato.

Il protocollo BB84

Nel protocollo BB84 Alice codifica su qubit una sequenza di bit casuali servendosi con il 50% di probabilità due basi differenti (non ortogonali tra loro). Gli stati vengono quindi inviati a Bob che li misura utilizzando di volta in volta una delle due basi scegliendole casualmente: solamente gli stati misurati con la medesima base della codifica porteranno ad ottenere con certezza il valore corretto del bit inviato da Alice. Per questo motivo, Alice e Bob comunicano pubblicamente (su un canale pubblico autenticato) le basi di codifica e di misura, rispettivamente, in modo da conservare solamente i bit in cui queste coincidono, scartando i rimanenti (*sifting*). In assenza di una spia le sequenze di bit ottenute dalle due parti, le cosiddette *sifted key*, coincidono. Nel momento in cui Eve interviene sul canale, intercettando gli stati inviati da Alice prima che arrivino a Bob, introduce inevitabilmente un rumore, come previsto delle leggi della Meccanica Quantistica. In particolare, tale rumore si manifesta introducendo degli errori nelle *sifted key*, che possono essere rivelati confrontando direttamente una frazione delle chiavi finali (si parla di fase di riconciliazione). Se la percentuale di errori, il QBER, è minore di una determinata soglia è possibile ritenere lo scambio di chiavi sicuro: diventa possibile distillare una chiave finale che Eve spia non sarebbe in alcun modo in grado di recuperare.

In questo modo, il protocollo BB84 si avvale della natura intrinsecamente probabilistica della meccanica quantistica per garantire la sicurezza della comunicazione tra Alice e Bob.

Più nel dettaglio, nel protocollo BB84 lo scambio di chiave è realizzato attraverso i seguenti passaggi principali:

1. Alice genera casualmente una sequenza di N bit. Per ogni bit, sceglie poi in maniera indipendente e casuale una delle due basi $\bigoplus$ o $\bigotimes$, e invia a Bob un fotone codificando bit grazie alla polarizzazione nella base scelta. Se, per esempio, il bit fosse "1" e la base scelta $\bigotimes$, il fotone inviato a Bob sarebbe nello stato $|+\rangle$. Essendo sia i bit che le basi scelte in modo completamente casuale, la probabilità di mandare ciascuno degli stati $|0\rangle$, $|1\rangle$, $|+\rangle$ e $|-\rangle$ è la stessa. Ognuno di questi viene quindi inviato approssimativamente $N/4$ volte.

2. Per ogni fotone (bit) inviato da Alice, Bob sceglie in modo casuale una delle due basi su cui effettuare la sua misura: un semplice conto mostra che, statisticamente, i due utilizzeranno la stessa base circa $N/2$ volte. Nel caso ideale di un canale di comunicazione non rumoroso, ossia tale per cui lo stato che giunge a Bob è esattamente lo stesso inviato da Alice, tutte le misure effettuate da Bob sulla stessa base utilizzata da Alice per codificare l'informazione daranno come risultato il valore del bit scelto originariamente da Alice. Al contrario, nelle misure in cui le basi scelte dai due sono diverse, i bit di Alice e di Bob saranno completamente scorrelati.

3. Il passo successivo consiste nell'eliminare i bit scorrelati. Al termine della trasmissione sul canale quantistico, Alice e Bob utilizzano il canale classico autenticato per dichiarare la base scelta per codificare e misurare ciascun fotone (ma non il valore codificato e misurato!). Quindi, conservano solamente i bit che sono stati codificati e misurati nella stessa base, scartando gli altri. Questo processo è chiamato *sifting* ("setacciamento") e bit rimanenti costituiscono la cosiddetta *sifted key*, che sarà quindi lunga circa $N/2$ bit.

4. Infine, una parte statisticamente significativa della sifted key viene rivelata pubblicamente sul canale classico — e quindi successivamente scartata — per valutare la percentuale di eventuali errori presenti nella sequenza finale di bit (*quantum bit error rate*, QBER). Come vedremo fra poco, dal QBER è possibile rilevare la presenza di una possibi-

	bit	1	0	0	1	1	0	1	0	0	1
ALICE	base codifica	⊕	⊗	⊕	⊗	⊗	⊕	⊗	⊗	⊕	⊕
	stato inviato	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$
BOB	base misura	⊕	⊗	⊗	⊕	⊕	⊕	⊗	⊕	⊕	⊗
	risultato misura	1	0	1	1	0	0	1	1	0	1
chiave finale (sifted key)		1	0				0	1		0	

Figura 1: Esempio di attuazione del protocollo BB84 nel caso ideale di un canale senza rumore. Quando la base di codifica e quella di misura coincidono, il bit ottenuto da Bob ha lo stesso valore di quello spedito da Alice (colonne evidenziate in giallo): condividono la stessa chiave. Si veda il testo per i dettagli.

	bit	1	0	0	1	1	0	1	0	0	1
ALICE	base codifica	⊕	⊗	⊕	⊗	⊗	⊕	⊗	⊗	⊕	⊕
	stato inviato	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$
EVE	base misura	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊕	⊕
	risultato misura	1	1	0	1	0	0	0	0	0	1
	stato inviato	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$
BOB	base misura	⊕	⊗	⊗	⊕	⊕	⊕	⊗	⊕	⊕	⊗
	risultato misura	1	1	0	0	0	0	0	0	0	0
chiave finale (sifted key)		1	1				0	0		0	

Figura 2: Esempio di attuazione del protocollo BB84 identica alla figura 1, ma con una spia nel canale che effettua un attacco di tipo intercept-resend. Ora può accadere che pur avendo la stessa base di codifica e di misura, il bit spedito da Alice non coincida con quello misurato da Bob, indice, questo, della presenza di una spia, Eve, che ha intercettato il segnale di Alice prima che giungesse a Bob misurandolo con la base sbagliata (celle della tabella evidenziate in rosso). Si veda il testo per i dettagli.

le spia nel canale e, di conseguenza, abortire la comunicazione se necessario.

Al termine del protocollo, se questo va a buon fine, Alice e Bob condividono una chiave casuale segreta di lunghezza approssimativamente $N/2$ bit, a cui vanno però tolti i bit resi noti sul canale classico per il calcolo del QBER. Questa chiave può essere utilizzata per crittografare un messaggio della stessa lunghezza utilizzando la tecnica del *one-time pad*, come precedentemente menzionato. Dopodiché, il messaggio può essere trasmesso attraverso un canale pubblico senza alcun rischio che l'informazione contenuta possa essere decifrata da terzi.

Nella Figura 1 è riportato un esempio di implementazione del BB84 su $N = 10$ bit, nel caso di un canale quantistico non rumoroso sul quale, cioè, non si sia introdotta nessuna spia. Nella figura abbiamo evidenziato in giallo le colonne in cui la base scelta da Alice per la codifica corrisponde a quella scelta da Bob per la sua misura. Si nota come i bit della chiave finale, la *sifted key*, siano perfettamente correlati a quelli inviati da Alice.

Passiamo ora a vedere come si comporta il protocollo BB84 in presenza di una spia. Questa situazione è rappresentata nella Figura 2, dove la spia, Eve, si è intromessa nel canale quantisrico, attuando una tecnica nota come *intercept-resend*: Eve intercetta il fotone mandato da Alice, lo misura e rispedisce un nuovo fotone a Bob codificando l'informazione che ha acquisito. Non conoscendo la base utilizzata da Alice per codificare ciascun bit (la dichiarazione delle basi avviene, infatti, solo alla fine del flusso di stati sul canale quantistico), Eve non può fare altro che scegliere la base di misura in modo casuale. In seguito invia a Bob lo stato corrispondente al risultato misurato codificandolo con la stessa base di cui si è servita per la sua misura.

Per valutare il QBER dovuto in questo caso alla presenza della spia, dobbiamo contare il numero di bit errati nella sifted key. Le basi scelte da Alice e Bob quindi sono da considerarsi sempre

uguali per tutti i bit, dal momento che le misure in cui questo non è vero sono comunque scartate. Nel 50% dei casi, la base scelta da Eve sarà la stessa utilizzata da Alice e Bob (si vedano le colonne gialle della Figura 2): gli stati inviati da Eve a Bob saranno quindi identici a quelli originariamente prodotti da Alice, senza che alcun errore venga introdotto (si vedano le colonne gialle della Figura 2). Nel restante 50% dei casi, in cui invece la base scelta da Eve non coincide con quella utilizzata da Alice e Bob (le celle rosse nella tabella della Figura 2), le misure di quest'ultimo risulteranno completamente casuali e, quindi, fedeli ai bit originari di Alice solamente la metà delle volte. Nella Figura 2 abbiamo evidenziato in arancione con un bordo rosso i bit della sifted key che differiscono da quelli inviati da Alice (per maggior chiarezza si paragonino anche le chiavi finali riportate nelle figure 1 e 2 in assenza e in presenza della spia, rispettivamente).

In un attacco di tipo *intercept-resend*, quindi, viene introdotto un QBER del 25%: ciò significa che, durante la procedura di riconciliazione, Alice e Bob scopriranno che circa il 25% dei bit della *sifted key* non coincide e, di conseguenza, interromperanno immediatamente la trasmissione, in quanto questa discrepanza manifesta chiaramente la presenza di una spia.

Se il rumore introdotto da un canale reale rimane al di sotto del 25%, allora è possibile considerare lo scambio di chiave come intrinsecamente sicuro rispetto a un attacco di tipo intercept-resend. La soglia sul QBER può essere innalzata al 27.6% [14] modificando opportunamente il protocollo iniziale e applicando metodi di *information reconciliation* e *privacy amplification* [15].

In linea di principio, Eve potrebbe lanciare anche attacchi più sofisticati, ottenendo un QBER inferiore. In tal modo, si dimostra che il protocollo BB84 è sicuro contro qualsiasi tipo di attacco fisicamente realizzabile a condizione che il rumore del canale sia inferiore all'11% [16]. Questo significa che, indipendentemente dalla particolare strategia adottata da Eve, la sicurezza del protocollo è garantita purché la qualità del canale (il livello di rumore) soddisfi quest'ultima condizione.

In vista di una realizzazione pratica, è bene sottolineare che il BB84 orginale qui descritto richiede che Alice generi un singolo fotone per ogni bit inviato. Tuttavia, la costruzione di sorgenti a singolo fotone è un problema non banale. Con le attuali tecnologie, infatti, una delle tecniche più efficienti utilizzate per generare singoli fotoni richiede processi di ottica non lineare e misure condizionate, capaci di generare i fotoni solamente in maniera probabilistica [17]. Per questa ragione, nelle realizzazioni sperimentali di BB84 vengono impiegati impulsi LASER attenuati, la cui energia media è dell'ordine di un fotone. Tale scelta non è priva di conseguenze. Infatti, come verrà discusso nelle sezioni successive, lo stato quantistico che descrive un impulso LASER, detto stato coerente, è una sovrapposizione quantistica di stati con diverso numero di fotoni. Dunque, con tale codifica, esiste sempre una probabilità non nulla di avere più di un fotone per impulso, con potenziali conseguenze sulla sicurezza del protocollo, in quanto la spia potrebbe sottrarne solo uno senza farsi scoprire [18, 19]. Per superare tali limitazioni e ripristinare la sicurezza intrinseca, diverse varianti di BB84 sono state proposte, tra cui la principale richiede l'utilizzo dei cosiddetti **stati decoy**, che significa "esca" [20, 21, 22].

La prima implementazione di decoy BB84, utilizzando un singolo stato decoy, è stata ottenuta nel 2006, modificando un sistema di QKD commerciale con una distanza di trasmissione di 15 km [23]. In seguito, nel 2007 tre gruppi sperimentali diversi hanno realizzato BB84 con due stati decoy, raggiungendo distanze di trasmissione pari a 102 km [24] e 107 km [25] in fibra ottica, e 144 km [26] in spazio aperto.

I sempre più avanzati progressi nel campo hanno portato nel 2018 a raggiungere la distanza di 421 km: un risultato ottenuto dal gruppo di H. Zbinden realizzando BB84 con un solo stato decoy attraverso una fibra ottica a perdite ultrabasse [27].

Introduzione ai sistemi a variabili continue

Storicamente i primi protocolli di QKD hanno riguardato sistemi a variabili discrete (discrete varibles, DV), in cui l'informazione viene codificata su un insieme discreto di simboli, ad esempio un qubit. D'altra parte, l'implementazione su larga

Il protocollo GG02

Nel protocollo GG02 Alice invia a Bob una serie di stati coerenti con i valori medi delle quadrature generati campionando una distribuzione Gaussiana. Bob effettua una misura di quadratura, scegliendo con uguale probabilità se misurare l'osservabile q oppure p. A seguito della misura, Alice e Bob condividono un'informazione mutua $\mathcal{I}(A:B)$.
Dopo lo scambio dei segnali, avviene la fase riconciliazione, che richiede che Alice e Bob si scambino una parte dei loro dati su un canale classico pubblico. Tipicamente si effettua la riconciliazione inversa, in cui è Bob a rivelare i suoi dati ad Alice. D'altro canto, anche Eve è in grado di estrarre un'informazione mutua non nulla a seguito di tale riconciliazione, pari a $\mathcal{I}(B:E)$.
Il KGR risulta, dunque, uguale alla differenza delle due informazioni mutue:

$$K = \mathcal{I}(A:B) - \mathcal{I}(B:E)\,,$$

espressa in numero di bit per impulso. In un protocollo realistico, tale quantità deve essere moltiplicata per la larghezza di banda, ovvero il numero di simboli al secondo generati da Alice, il cui valore tipico è dell'ordine del MHz.

scala di BB84 e di altri schemi più avanzati di DV-QKD risulta non banale per una duplice ragione. Come ricordato in precedenza, il principale ostacolo è rappresentato dalla generazione di singoli fotoni, sulla cui polarizzazione codificare i bit "0" e "1". In secondo luogo, le tecnologie richieste dalla DV-QKD non sono compatibili con i sistemi di comunicazione in fibra ottica impiegati attualmente nelle comunicazioni classiche, basati invece sullo scambio di impulsi LASER tra trasmettitore e ricevitore e su misure omodine o eterodine in grado di misurarne il campo elettrico [28]. Per queste ragioni, in tempi più recenti l'interesse è stato rivolto a sistemi a variabili continue (continuous variables, CV) che codificano l'informazione su un parametro continuo, come, per esempio, l'ampiezza o la fase di un segnale elettromagnetico. L'esempio paradigmatico di un sistema CV è rappresentato, per l'appunto, da un campo ottico, ossia un campo elettromagnetico monocromatico oscillante prodotto localmente da una sorgente (ad esempio un generatore di segnali) e in propagazione nello spazio libero. In questo scenario, gli impulsi LASER tipicamente impiegati nelle comunicazioni sono descritti dai cosiddetti stati "coerenti", indicati con $|\alpha\rangle$, caratterizzati da un'ampiezza complessa $\alpha \in \mathbb{C}$ proporzionale all'ampiezza media del campo elettrico. Osserviamo che anche in questo caso siamo in presenza di una sovrapposizione quantistica: lo stato coerente è, infatti, una sovrapposizione di infiniti stati $|n\rangle$, detti stati di Fock, contenenti ciascuno un numero $n \in \mathbb{N}$ di fotoni e con una ben determinata relazione di fase:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{17}$$

A proposito di campo elettrico, è bene ricordare un risultato fondamentale, valido anche nella teoria classica della radiazione. Per ricostruire il valore del campo elettrico $E(x)$ in un punto dello spazio x è necessario misurare due osservabili fisiche distinte, dette "quadrature", tradizionalmente identificate dai simboli q e p. Il campo elettrico di una qualunque sorgente risulta infatti essere proporzionale ad una combinazione lineare delle sue quadrature [29, 30]:

$$E(x) \propto q \cos\left(\frac{2\pi x}{\lambda}\right) + p \sin\left(\frac{2\pi x}{\lambda}\right) \tag{18}$$

dove λ è la lunghezza d'onda della radiazione.

Tuttavia, a differenza del caso classico, per un campo ottico in regime quantistico descritto dallo stato coerente $|\alpha\rangle$ non è possibile conoscere il valore delle due quadrature con precisione arbitraria. Si tratta di una conseguenza delle relazioni di indeterminazione di Heisenberg. Nel caso specifico, a causa delle proprietà quantistiche degli stati coerenti [29], misurando le osservabili q e p si registrano valori che fluttuano secondo una distribuzione Gaussiana. Le probabilità $P(q)$ e $P(p)$ di misurare i valori q e p, rispettivamente, risultano quindi pari a [29, 30]:

$$\begin{aligned} P(q) &= \mathcal{N}_{\sigma_0}\big(q; \Re\mathrm{e}(\alpha)\big)\,, \\ P(p) &= \mathcal{N}_{\sigma_0}\big(p; \Im\mathrm{m}(\alpha)\big)\,. \end{aligned} \tag{19}$$

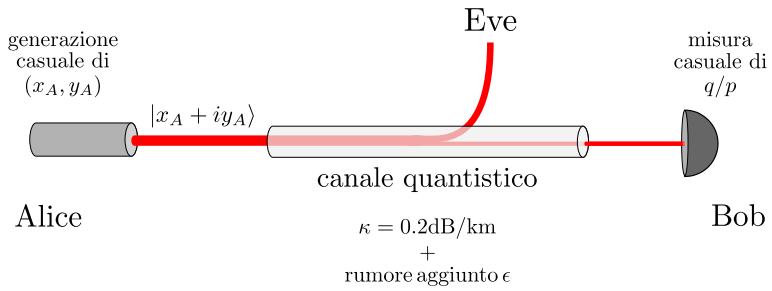

Figura 3: Schema del protocollo GG02. Alice invia a Bob una sequenza di stati coerenti generati secondo una distirbuzione normale. I segnali viaggiano lungo il canale quantistico dove vengono attenuati e acquistano un rumore aggiunto $\epsilon > 0$. Bob misura una delle due quadrature q o p del segnale ricevuto, estraendo l'informazione mutua $\mathcal{I}(A : B)$. Il protocollo è sicuro se tale informazione mutua è maggiore di quella potenzialmente estratta da una spia, Eve.

dove:

$$\mathcal{N}_{\sigma_0}(z;\mu) = \frac{\exp\left\{-\frac{(z-2\sigma_0\,\mu)^2}{2\sigma_0^2}\right\}}{\sqrt{2\pi\sigma_0^2}}. \qquad (20)$$

Si osserva innanzitutto che il valor medio delle quadrature per uno stato coerente risulta proporzionale alla sua ampiezza: $\langle q\rangle \propto \Re\mathrm{e}(\alpha)$ e $\langle p\rangle \propto \Im\mathrm{m}(\alpha)$. Inoltre le distribuzioni di probabilità (19) hanno una varianza non nulla $\sigma_0^2 > 0$, conseguenza diretta della quantizzazione del campo e che va sotto il nome di rumore di vuoto. Si noti, infatti, che anche il campo elettrico nello stato di vuoto, corrispondente al caso $\alpha = 0$, mostra delle fluttuazioni non nulle nelle due quadrature, che ora hanno entrambe valore medio pari a 0.

A differenza dei sistemi DV, una codifica di questo tipo basata sull'ampiezza (e la fase) del campo risulta compatibile con le tecniche comunemente usate per le comunicazioni classiche, rivelandosi di interesse per un'estensione degli attuali sistemi di comunicazione ottica in regime quantistico.

La presenza del rumore di vuoto rende due segnali coerenti distinti $|\alpha\rangle$ e $|\beta\rangle$ aventi ampiezze sufficientemente vicine, cioè $|\alpha - \beta| \sim \sigma_0$, indistingubili dalla sola misura di una quadratura. Questa proprietà torna estremamente utile per la crittografia. Infatti, codificando dei simboli su stati coerenti è possibile trasmettere dell'informazione sicura tra un ricevitore e un trasmettitore, in modo che un'eventuale terza parte non sia in grado di intromettersi e inferire il particolare simbolo generato dalla sorgente. È questo il principio base dei protocolli di distribuzione quantistica di chiave a variabili continue (CV-QKD), il cui esempio paradigmatico è costituito dal protocollo proposto da Fréderic Grosshans e Philippe Grangier nel 2002 e noto come GG02 [31].

Il protocollo GG02

Lo schema del protocollo GG02 è riportato in Figura 3. Il trasmettitore, Alice, estrae una coppia (x_A, y_A) di numeri casuali reali campionando una distribuzione Gaussiana $\mathcal{N}_\Sigma(z;0)$. Quindi genera un impulso LASER, i.e. uno stato coerente $|\alpha_A\rangle$, con ampiezza $\alpha_A = x_A + iy_A$ e lo invia al ricevitore, Bob, attraverso un canale quantistico [31].

Con il termine "canale" ci si riferisce al supporto fisico, tipicamente rumoroso, che connette Alice e Bob e nel quale propagano i segnali generati. In contesti pratici, il canale quantistico descrive sistemi fisici differenti a seconda della piattaforma utilizzata. Lo scenario tipico è rappresentato dalle comunicazioni in fibra, in cui il canale descrive la fibra ottica che connette Alice e Bob, caratterizzata da un tasso di perdita κ dovuto alla propagazione del segnale nel dielettrico di cui è composta la fibra e da un rumore aggiunto $\epsilon > 0$ causato dalle imperfezioni del generatore di segnali impiegato da Alice [32].

Possono comunque presentarsi situazioni più complesse. Ad esempio, nelle comunicazioni in spazio aperto o sottomarine, il canale descrive il mezzo stesso di propagazione, rispettivamente

aria o acqua, e, oltre alle perdite, modella anche i fenomeni di assorbimento e dispersione che possono verificarsi in questi ambienti.

Qualunque sia il supporto fisico modellizzato, il canale introduce delle distorsioni dello stato coerente in ingresso e, per questa ragione, viene considerato non fidato, assumendo che tali distorsioni siano opera di una spia, Eve, interessata ad estrarre in tutto o in parte la chiave sicura generata Alice e Bob (si veda la Figura 3). Nel caso di comunicazioni in fibra, ad esempio, si suppone che Eve intercetti la frazione di segnali persa durante la propagazione, e che sia lei stessa a generare il rumore aggiunto $\epsilon > 0$ osservato sugli impulsi coerenti in uscita [32].

Una volta ricevuti i segnali uscenti dal canale, il ricevitore, Bob, effettua una misura di una delle due quadrature del corrispondente campo elettrico, scegliendo casualmente l'osservabile q o p con uguale probabilità. Il risultato della misura è un numero reale z_B distribuito secondo le Eq. (19) con $q = x_A$ e $p = y_A$ ma con una varianza σ_ϵ^2 maggiore del rumore del vuoto, $\sigma_\epsilon^2 > \sigma_0^2$. Il valore di z_B risulta, dunque, correlato alla coppia di simboli in ingresso (x_A, y_A). Attraverso un processo di *post-processing* detto "riconciliazione", Bob è in grado di estrarre una parte dell'informazione codificata da Alice nella fase di preparazione del protocollo. Questa quantità, vale a dire la quantità di informazione che Alice e Bob riescono a condividere dopo la misura, prende il nome di "informazione mutua" $\mathcal{I}(A:B)$.

Considerazioni analoghe valgono anche per l'azione di Eve, la quale attacca il canale, raccogliendone le perdite e nascondendosi dietro il rumore aggiunto, ed è, dunque, in grado di estrarre un'informazione mutua $\mathcal{I}(B:E)$ non nulla tramite una misura opportuna.

Pertanto, si conclude che il protocollo è sicuro fintanto che l'informazione mutua estratta da Eve sia inferiore all'informazione mutua scambiata tra Alice e Bob. In tal caso, a seguito del processo di riconciliazione, Alice e Bob possono applicare una serie di tecniche numeriche di *privacy amplification* volte ad estrarre una chiave casuale sicura a partire dalle rispettive liste di dati (x_A, y_A) e z_B.

La differenza tra le due informazioni mutue definisce il **tasso di generazione della chiave** (*key generation rate*, KGR), che rappresenta la lunghezza della chiave estratta, ossia il numero di bit sicuri generati per unità di tempo.

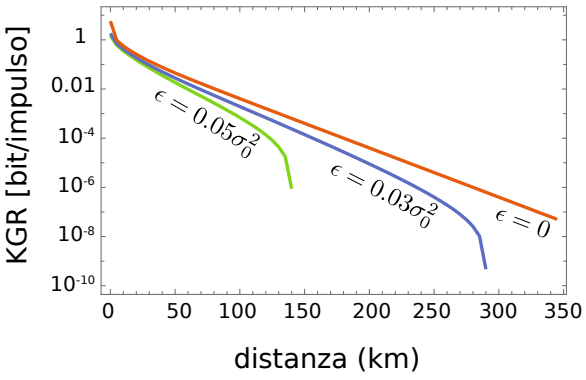

Figura 4: KGR in funzione della distanza di trasmissione in km per diversi valori del rumore aggiunto ϵ. La presenza del rumore aggiunto introduce una distanza massima di trasmissione oltre la quale non è più possibile distillare una chiave sicura.

Nella Figura 4 è riportato il valore del KGR (in presenza di *reverse reconciliation*) in funzione della distanza di trasmissione espressa in km per alcuni valori realistici dei parametri. Il tasso di perdita delle comuni fibre ottiche è pari a $\kappa = 0.2$ dB/km, mentre il rumore aggiunto è tipicamente compreso tra $0.01\sigma_0^2 < \epsilon < 0.05\sigma_0^2$. Come si osserva, solamente in assenza di rumore aggiunto ($\epsilon = 0$) è possibile effettuare comunicazione sicura a distanze arbitrariamente grandi, mentre per $\epsilon > 0$ esiste una distanza massima di trasmissione oltre la quale il KGR diventa nullo.

Le potenzialità mostrate dalla CV-QKD sono state anche verificate sperimentalmente. Sino ad oggi, diverse realizzazioni di GG02 sono state testate in laboratorio, analizzando il livello di sicurezza sotto diversi paradigmi. I primi esperimenti *proof-of-principle* risalgono al 2003, in cui è stata impiegata luce visibile a 780 nm e la presenza del canale è stata simultata attraverso un *beam splitter* di transmissività variabile [33]. Tuttavia, le tecniche impiegate in questo lavoro e nei suoi successivi sviluppi [34, 35, 36], pur costituendo una prima dimostrazione pratica, risultano inadatte per un'applicazione in fibra ottica a causa della radiazione utilizzata (incompatibile con le lunghezze d'onda infrarosse impiegate per la comunicazione in fibra, che comunemente sono in tre finestre attorno a 850 nm, a 1300 nm oppure a 1550 nm, lunghezze d'onda *telecom*) e la scarsa

efficienza dei componenti del *setup* e dei codici di riconciliazione.

La prima vera CV-QKD a lunghezze d'onda *telecom* è stata ottenuta solo nel 2007 dal gruppo di Jérôme Lodewyck [37], riuscendo a raggiungere distanze di trasmissione superiori a 25 km. A partire da quella data, nel 2013 e 2016 sono state raggiunte le distanze di 80 km [38] e 100 km [39], rispettivamente. Infine, attraverso l'utilizzo di fibre ottiche a perdite ultrabasse, nel 2020 è stato possibile distillare una chiave sicura a distanze superiori ai 200 km [40]. Parallelamente al tentativo di raggiungere distanze di trasmissione sempre maggiori, le più recenti innovazioni nel campo delle lunghezze *telecom* hanno fatto sì che si potesse anche incrementare il KGR a più basse distanze, riuscendo a estrarre un maggior numero di bit sicuri al secondo. Sui 25 km si è passati dai 2 kbps (kilobit al secondo) dello schema di Lodewyck [37] a 1 Mbps (megabit al secondo) [41], mentre sui 50 km sono stati ottenuti KGR pari a 7.57 kbps [42] e 52 kbps [43].

Conclusione

Da un lato, la descrizione della natura data dalla Meccanica Quantistica ha permesso di comprendere i suoi meccanismi in maniera più profonda, meccanismi altrimenti elusivi in quanto spesso molto lontani dalla nostra intuizione e dal senso comune. D'altro canto, lo studio approfondito di questa teoria ha aperto la strada a progressi tecnologici irraggiungibili e inimmaginabili nell'ambito della sola fisica classica. A tal riguardo ci piace ricordare la risonanza magnetica nucleare, potente tecnica diagnostica con molteplici sfaccettature, gli orologi atomici che scandiscono il nostro tempo ma, soprattutto, sono fondamentali per il funzionamento del sitema GPS, ma anche tutta la tecnologia basata sul silicio e sui semiconduttori.

In queste pagine vi abbiamo mostrato, seppure in modo semplificato, come la fisica quantistica permetta di dare un contributo rilevante anche alla trasmissione sicura di informazione, focalizzandoci sul problema della distribuzione di chiavi quantistica. Si tratta di un esempio in cui gli sforzi teorici e sperimentali hanno permesso di trasformare le previsioni quantistiche in sistemi funzionanti e ormai integrati in alcuni scenari della nostra società fino al livello commerciale.

Un esempio tra tanti della "seconda rivoluzione quantistica" che stiamo vedendo e vivendo in questi anni e che, si spera, possa concorrere a migliorare le condizioni dell'umanità come affermava Nikola Tesla.

[1] T. S. Kuhn: *La struttura delle rivoluzioni scientifiche*, Einaudi, Torino (2009).

[2] L. Belloni e S. Olivares: *Planck – La rivoluzione quantistica*, Pelago, (2021).

[3] P. Ball: *Beyond Weird*, Vintage, Redding, CA (2018).

[4] L. Branchetti, A. Cattabriga and O. Levrini: *Interplay between mathematics and physics to catch the nature of a scientific breakthrough: The case of the blackbody*, Phys. Rev. Phys. Educ. Res., 15 (2019) 020130.

[5] H. B. Callen: *Thermodynamics and an Introduction to Thermostatistics*, John Wiley & Sons, Hoboken, NJ (1985).

[6] S. Olivares: *Appunti di Termodinamica*, Milano University Press, Milano (2023).

[7] M. L. Giliberti, L. Lovisetti, S. Olivares e M. G. A. Paris: *Meccanica quantistica, entanglement e nonlocalità*, Giornale di Fisica, LXIV (2023) 161.

[8] The Nobel Prize in Physics 2022: `https://www.nobelprize.org/prizes/physics/2022/`

[9] C. H. Bennett and G. Brassard: *Quantum cryptography: Public key distribution and coin tossing*, Theor. Comput. Sci., 560 (2014) 7.

[10] G. S. Vernam: *Cipher printing telegraph systems for secret wire and radio telegraphic communications*, Trans. AIEE, XLV (1926) 295.

[11] C. E. Shannon: *Communication theory of secrecy systems*, Bell Syst. Tech. J., 28 (1949) 656.

[12] R. L. Rivest, A. Shamir, and L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM, 21 (1978) 120.

[13] P. W. Shor: *Algorithms for quantum computation: Discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science, (1994) 124.

[14] H. F. Chau: *Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate*, Phys. Rev. A, 66 (2002) 60302.

[15] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin: *Experimental Quantum Cryptography*, J. Cryptol., 5 (1992) 3.

[16] D. Mayers: *Unconditional security in quantum cryptography*, J. ACM, 48 (2001) 351.

[17] G. S. Buller and R. J. Collins: *Single-photon generation and detection*, Meas. Sci. Technol., 21 (2010) 012002.

[18] D. Gottesman, H. K. Lo, Lütkenhaus and J. Preskill: *Security of quantum key distribution with imperfect devices*, Quant.Inf.Comput., 5 (2004) 325.

[19] V. Scarani, A. Acin, G. Ribordy and N. Gisin: *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak LASER Pulse Implementations*, Phys. Rev. Lett., 92 (2004) 057901.

[20] X.-B. Wang: *Beating the photon-number-splitting attack in practical quantum cryptography*, Phys. Rev. Lett., 94 (2005) 230503.

[21] H.-K. Lo, X. Ma and K. Chen: *Decoy State Quantum Key Distribution*, Phys. Rev. Lett., 94 (2005) 230504.

[22] X.-B. Wang: *Decoy-state protocol for quantum cryptography with four different intensities of coherent light*, Phys. Rev. A, 72 (2005) 012322.

[23] Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qia: *Experimental Quantum Key Distribution with Decoy States*, Phys. Rev. Lett., 96 (2006) 070502.

[24] C.-Z. Peng et al.: *Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding*, Phys. Rev. Lett., 98 (2007) 2.

[25] D. Rosenberg et al.: *Long-Distance DecoyState Quantum Key Distribution in Optical Fiber*, Phys. Rev. Lett., 98 (2007) 010503.

[26] T. Schmitt-Manderbach et al.: *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km*, Phys. Rev. Lett., 98 (2007) 010504.

[27] A. Boaron et al.: *Secure Quantum Key Distribution over 421 km of Optical Fiber*, Phys. Rev. Lett., 121 (2018) 190502.

[28] G. Cariolaro: *Quantum Communications*, Springer International Publishing, Berlino (2015).

[29] S. Olivares: *Introduction to generation, manipulation and characterization of optical quantum states*, Phys. Lett. A, 418 (2021) 127720.

[30] S. Olivares: *Quantum optics in the phase space: A tutorial on Gaussian states*, Eur. Phys. J. Special Topics, 203 (2012) 3.

[31] F. Grosshans and P. Grangier: *Continuous Variable Quantum Cryptography Using Coherent States*, Phys. Rev. Lett., 88 (2002) 057902.

[32] F. Laudenbach et al.: *Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations*, Adv. Quantum Technol., (2018) 1800011.

[33] F. Grosshans et al.: *Quantum key distribution using gaussian-modulated coherent states*, Nature, 421 (2003) 238.

[34] S. Lorenz, N. Korolkova and G. Leuchs: *Continuous variable quantum key distribution using polarization encoding and post selection*, App. Phys. B, 79 (2004) 273.

[35] A. Lance et al.: *No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light*, Phys. Rev. Lett., 95 (2005) 180503.

[36] J. Lodewyck et al.: *Controlling excess noise in fiber-optics continuous-variable quantum key distribution*, Phys. Rev. A, 72 (2005) 050303.

[37] J. Lodewyck et al.: *Quantum key distribution over 25 km with an all-fiber continuous-variable system*, Phys. Rev. A, 76 (2007) 042305.

[38] P. Jouguet et al.: *Experimental demonstration of long-distance continuous-variable quantum key distribution*, Nat. Photonics, 7 (2013) 378.

[39] D. Huang, P. Huang, D. Lin and G. Zeng: *Long-distance continuous-variable quantum key distribution by controlling excess noise*, Sci. Rep., 6 (2016) 19201.

[40] Y. Zhang et al.: *Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber*, Phys. Rev. Lett., 125 (2020) 010502.

[41] D. Huang et al.: *Continuous-variable quantum key distribution with 1 Mbps key rate*, Opt. Express, 23 (2015) 17511.

[42] Y. Zhang et al.: *Continuous-variable QKD over 50 km commercial fiber*, Quantum Sci. Technol., 4 (2019) 035006.

[43] C. Wang et al.: *25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel*, Sci. Rep., 5 (2015) 14607.

Samuele Altilia: è un fisico sperimentale, dottorando presso il Dipartimento di Fisica "Aldo Pontremoli" dell'Università degli Studi di Milano. Attualmente si occupa di sistemi ottici per la generazione e la rivelazione di stati quantistici per applicazioni nella comunicazione quantistica.

Michele N. Notarnicola: è un fisico teorico, dottorando presso il Dipartimento di Fisica "Aldo Pontremoli" dell'Università degli Studi di Milano. I suoi principali interessi sono la comunicazione quantistica e la distribuzione di chiave quantistica a variabili continue.

Stefano Olivares: è un fisico teorico e si occupa di ottica quantistica, informazione quantistica con interesse particolare per la comunicazione quantistica e le sue realizzazioni fotoniche. È Professore Associato presso il Dipartimento di Fisica "Aldo Pontremoli" dell'Università degli Studi di Milano e docente degli insegnamenti di Termodinamica e di Teoria Quantistica della Computazione. Collabora attivamente con diversi gruppi sperimentali ed è anche impegnato nella divulgazione scientifica.