La seconda rivoluzione quantistica: il computer quantistico e la crittografia.

Taira Giordani, Alessia Suprano, Fabio Sciarrino

Dipartimento di Fisica, Sapienza Università, Roma

Introduzione

La meccanica quantistica, ovvero quell'insieme di straordinarie intuizioni che furono e sono considerate come una vera e propria rivoluzione, è ormai una teoria affermatasi quasi un secolo fa. Eppure, se ci si sofferma su questo ultimo dettaglio, risulta ancora più sorprendente constatare quanto, rispetto ad altre teorie del passato, essa sia percepita anche a distanza di tanti anni come un qualcosa di nuovo, o di non completamente assimilato, e quindi di difficile comunicazione ad un pubblico non tecnico.

Ancora più sorprendente potrà sembrare il dover parlare di quella che viene definita come la seconda rivoluzione quantistica, ovvero la storia più recente delle applicazioni della teoria che riguardano più da vicino le tecnologie dell'informazione. Ogni rivoluzione, infatti, è figlia dei suoi tempi e non è un caso che questa seconda tappa sia nata non troppo successivamente, se non contemporaneamente, all'affermazione dei primi calcolatori, ai quali da qui in avanti ci riferiremo come computer classici. Infatti, perché non utilizzare proprio un sistema controllato da effetti genuinamente quantistici, ovvero su scale e condizioni fisiche tali da rendere questi effetti evidenti e misurabili, per poter investigare la natura, o tradotto, per poter ampliare la capacità di elaborazione di un computer? Questo fu il primo quesito, attribuito a Richard Feynman, da cui si partì per formalizzare una teoria dell'informazione che tenesse conto dei principi della meccanica quantistica.

In analogia con l'informatica, si definisce un'unità fondamentale, il **qubit**, un sistema costituito da due stati logici 0,1, mutualmente esclusivi. Il qubit descrive però un sistema quantistico per il quale saranno validi sia il principio di sovrapposizione, per cui saranno possibili stati in sovrapposizione dei due livelli logici come stati in sovrapposizione di più qubit, quanto il principio del collasso dello stato durante il processo di misura, ovvero, di estrazione dell'informazione in esso codificata. L'impalcatura teorica dell'informazione quantistica che si sviluppò a partire

dagli anni '80 aveva lo scopo di individuare per quali problemi un paradigma di computazione basato sulla meccanica quantistica potesse effettivamente offrire dei vantaggi, da cui sviluppare appunto protocolli di informazione e algoritmi puramente quantistici [1]. Quanta informazione si può processare e quanta se ne può estrarre da un qubit? Uno stato quantistico può essere copiato senza conoscerne in precedenza l'espressione negli stati logici? Questi sono solo due esempi di domande un po' più tecniche ma molto istruttive inerenti ai fondamenti della teoria dell'informazione quantistica. Esse, infatti, mostrano implicitamente vantaggi e potenziali limiti del paradigma quantistico. L'impossibilità di copiare uno stato quantistico è il principio alla base della sicurezza intrinseca dei protocolli di crittografia quantistica. Come vedremo in seguito più nel dettaglio, essi hanno lo scopo di ottenere uno scambio di una chiave di cifratura sicura tra due interlocutori attraverso comunicazione dell'informazione codificata nei qubit. Il principio di indeterminazione e il processo di misura in meccanica quantistica, si traducono infatti nel `no-cloning theorem`, la cui conseguenza in un protocollo crittografico è quella di proibire ad un terzo interlocutore di poter accedere all'informazione sui qubit scambiati senza alterarne lo stato [1]. Questo permette ai due comunicanti di individuare in linea di principio la presenza di un terzo nella comunicazione. Per quanto riguarda la computazione quantistica, la possibilità di avere stati o qubit in sovrapposizione fa intuire la possibilità di poter processare l'informazione in parallelo. Questo è indubbiamente uno dei fondamentali vantaggi che hanno motivato negli anni la ricerca nel campo. Ma i teoremi sopra citati e il processo stesso di misura che di fatto limita la quantità di informazione che può essere estratta da un sistema quantistico, spesso pongono dei paletti alle dimensioni del ventaglio dei problemi computazionali per cui si può ottenere un vantaggio. Per vantaggio è utile chiarificare che si indica un miglioramento di come le risorse computazionali quali il tempo di calcolo o il numero di operazioni e qubit, scalino rispetto alla taglia del problema da risolvere. Si ha un vantaggio quantistico se l'algoritmo richiede risorse che aumentano più favorevolmente rispetto all'equivalente classico con la dimensione del dato in ingresso al processo. Tra gli algoritmi quantistici più famosi che appartengono a questa classe figurano sicuramente quello di scomposizione degli interi in fattori primi, algoritmi di ricerca, algoritmi di ottimizzazione e più recentemente algoritmi quantistici di apprendimento. In questo articolo si vuole riassumere lo sviluppo e l'impatto della seconda rivoluzione quantistica nella teoria e nelle tecnologie dell'informazione. Pertanto, nel seguito, si illustreranno più nel dettaglio i possibili paradigmi di computazione e crittografia quantistica proposte fino ad oggi, insieme alla presentazione delle possibili realizzazioni di tali tecnologie quantistiche. Stato dell'arte, limiti e prospettive saranno infine discusse per capire in quale stagione di questa seconda rivoluzione siamo ormai giunti.

Computazione quantistica

I principali schemi di computazione quantistica universali proposti nel corso di questi ultimi decenni sono essenzialmente tre, che possono essere riassunti nel `modello circuitale` [1], il `modello measurement-based` [2] e il modello di computazione di tipo `blind` [3, 4]. Uno schema invece totalmente alternativo rispetto ai precedenti è quello di tipo `analogico` [5]. Nel seguito tratteremo brevemente di ciascuno.

Il `modello circuitale` è quello storicamente introdotto per primo. Lo spirito di questo modello è di trasporre lo schema classico di computazione che prevede un set di bit e porte logiche elementari per costituire un computer universale. Alla stessa maniera, il modello circuitale quantistico prevede un registro di qubit e un insieme di porte logiche quantistiche con cui operare su di essi. Le porte quantistiche sono delle operazioni unitarie nello spazio di Hilbert che descrive il registro dei qubit. Il qubit, essendo uno stato quantistico, può essere considerato un oggetto matematico equivalente ad un vettore. Le porte logiche che operano sul singolo qubit saranno dunque delle rotazioni in tale spazio vettoriale. Il modello prevede anche delle porte logiche che operano su due qubit, le quali permettono le interazioni tra di essi e di creare stati di sovrapposizione tra più qubit. Esempi di questo tipo sono le porte controllate, come la negazione controllata (`controlled-not`) oppure la rotazione

controllata (`controlled-phase`), le quali operano sul secondo qubit in maniera condizionata allo stato del primo. La combinazione di rotazioni sul singolo qubit e porte controllate permette di avere uno schema universale per il computer quantistico.

Sebbene il modello circuitale sia il più naturale ed immediato per costruire un computer quantistico, esso può presentare alcune limitazioni nella sua realizzazione fisica. Allo stato attuale i qubit vengono generati e manipolati con un certo grado di rumore, il quale si propaga e si amplifica nelle varie operazioni logiche. In questo schema è quindi necessario introdurre tecniche di correzione degli errori, dette di `error-correction`, per mitigare la loro propagazione e tenere l'accuratezza di calcolo entro una data soglia di tolleranza [6]. In termini di risorse computazionali questo si traduce nell'impiego di qubit e porte ancillari che potrebbero limitare l'effettivo vantaggio dell'impiego di un algoritmo quantistico rispetto alla controparte classica.

Un possibile approccio alternativo di più recente introduzione rispetto al modello circuitale è quello chiamato `measurement-based`. Questo modello prevede la generazione di uno stato di diversi qubit in sovrapposizione tra di loro. In altre parole, anziché preparare tutti i qubit separatamente e farli interagire attraverso un circuito di porte logiche, in questo schema la complessità della costruzione del dispositivo risiede nel generare uno stato di qubit altamente correlati, detto `stato cluster`. La computazione viene svolta da una sequenza di opportune misure su determinate basi di altrettanti determinati qubit del cluster. Il vantaggio dell'approccio measurement-based risiede proprio nell'essere per costruzione più robusto al rumore e agli errori. Inoltre, risulta una valida alternativa per tutte quelle piattaforme quantistiche nelle quali la realizzazione del modello circuitale risulta complessa, quali le architetture fotoniche [2] e gli ioni intrappolati [7].

Un terzo schema molto recente è quello noto come `blind quantum computing`. Rispetto ai precedenti, utilizza un paradigma totalmente diverso, che unisce elementi sia di comunicazione che di computazione. Nell'approccio blind, la computazione viene delegata dall'utente ad un server che svolge l'algoritmo. Un importante dettaglio è che non è richiesta da parte del server la conoscenza dello stato iniziale del cliente. Infatti, gli stati scambiati tra i server e gli utenti sono sempre codificati in maniera tale che né il server e né il cliente conosce lo stato quantistico dell'altro, rendendo il processo sicuro da eventuali intromissioni di un terzo interlocutore come in un protocollo crittografico. Pertanto, è richiesto che le operazioni computazionali del server vengano svolte a prescindere dallo stato che arriva dal cliente, al quale, di contro, viene solo richiesto di generare e prepare i qubit. Anche questo protocollo per la computazione quantistica offre dei vantaggi rispetto al numero di risorse quantistiche necessarie per la sua realizzazione. Chiaramente richiede che i qubit possano essere scambiati tra più parti attraverso canali di comunicazione quantistici. Questo elemento aggiuntivo restringe il campo delle piattaforme fisiche che si prestano alla realizzazione dello schema. Infatti, ad oggi, figurano solo primi esperimenti basati su qubit fotonici, i quali, non a caso, sono quelli che ben più si adattano a protocolli che prevedono comunicazione, come vedremo nella sezione dedicata alla crittografia.

L'`approccio analogico` alla computazione quantistica è fondato su principi completamente diversi. I parametri della computazione non sono le operazioni unitarie sui qubit, ma bensì l'energia di interazione tra di essi, descritti dall'hamiltoniana del sistema. La computazione quantistica analogica risulta vantaggiosa quando si vogliono realizzare, algoritmi di simulazione di una data hamiltoniana di cui è difficile individuare autovalori e autovettori, oppure, algoritmi di ottimizzazione in cui si fa coincidere la soluzione del problema con il livello fondamentale dell'hamiltoniana del processore quantistico [8]. Questo modello alternativo può favorire alcune piattaforme rispetto ad altre, come ad esempio quelle che sfruttano sistemi di atomi neutri.

Crittografia quantistica

Come introdotto nella precedente sezione, stabilire canali quantistici di comunicazione che siano sicuri rispetto ad eventuali intromissioni di un terzo interlocutore è un ingrediente fondamentale per lo sviluppo di `blind quantum computer`. Inoltre, nell'era digitale in cui viviamo, la sicurez-

za delle comunicazioni è diventata una preoccupazione sempre più rilevante che ha reso fondamentale trovare soluzioni avanzate per proteggere le informazioni sensibili. I sistemi tradizionali di crittografia, si basano su algoritmi matematici complessi la cui risoluzione richiede un numero di risorse computazionali troppo elevato per poter essere raggiunta con i computer classici. Conseguentemente, l'impiego di nuove tecnologie, come quelle quantistiche, per sviluppare calcolatori in grado di risolvere efficientemente tali algoritmi, potrebbe inficiare la sicurezza dei sistemi di crittografia classica. In questo contesto, la crittografia quantistica si è rivelata una tecnologia rivoluzionaria in grado di garantire una comunicazione intrinsecamente sicura.

Il concetto chiave della crittografia quantistica è la distribuzione di una chiave crittografica segreta tra due parti che desiderano comunicare in modo sicuro. Tale distribuzione avviene attraverso protocolli di `Quantum Key Distribution` (QKD), in cui la chiave viene codificata nello stato di particelle quantistiche e la sicurezza è garantita dal `no-cloning theorem`, che proibisce ad un terzo interlocutore di estrarre informazioni sulla chiave senza alterare lo stato delle particelle stesse. Sebbene, diverse particelle quantistiche potrebbero essere utilizzate per codificare informazioni, l'alta trasmissibilità e la bassa interazione dei singoli fotoni con l'ambiente, rendono questi ultimi particolarmente adatti alla trasmissione a distanza. Conseguentemente, nella maggior parte delle implementazioni sperimentali, la trasmissione delle chiavi crittografiche avviene inviando singoli fotoni e codificando l'informazione nei sui gradi di libertà, come la polarizzazione.

I diversi protocolli di QKD si possono dividere in due categorie principali: i protocolli di `preparazione e misura` e i protocolli basati sull'`entanglement` [9].

Per quanto riguarda la prima categoria, uno dei più conosciuti ed utilizzati è il protocollo BB84, sviluppato da Charles Bennett e Gilles Brassard nel 1984 [10] In quest'ultimo, i bit costituenti la chiave segreta sono codificati in fotoni polarizzati e il mittente (Alice) può scegliere tra due basi di codifica, di solito lineare o diagonale. Allo stesso modo, il destinatario (Bob) sceglierà casualmente la base di misura. Successivamente, confrontando le loro basi attraverso un canale pubblico, Alice e Bob sono in grado di individuare la presenza di un terzo interlocutore e selezionando solamente i bit non compromessi riescono a distribuire una chiave sicura.

D'altra parte, il protocollo E91, sviluppato da Artur Ekert nel 1991 [11], è il primo protocollo basato sull' entanglement. In questo caso, Alice e Bob, condividono una coppia di fotoni entangled. Entrambi i partecipanti misurano lo stato delle loro particelle in diverse basi e successivamente confrontano i risultati tramite un canale pubblico non sicuro. Sapendo che le correlazioni quantistiche tra la coppia di fotoni assicurano che chiunque intercetti uno dei due oggetti altera il sistema complessivo, Alice e Bob possono rilevare la presenza di terze parti e trasmettere una chiave crittografica sicura.

Oltre ai protocolli illustrati diverse varianti sono state sviluppate e implementate in piattaforme che sfruttano comunicazioni in fibre ottiche, nello spazio libero o tramite satelliti [12]. Un esempio degno di nota riguarda il lancio del satellite cinese Micius nel 2016. Quest'ultimo, generando fotoni entangled e trasmettendoli a stazioni terrestri distanti 1203 km, ha permesso di superare i limiti di distanza legati alla comunicazione terrestre [13].

Piattaforme computer quantistico

Sebbene teoricamente si è dimostrato che lo sfruttamento delle proprietà quantistiche in computazione permetterebbe di risolvere problemi complessi in modo molto più efficiente, la realizzazione sperimentale del computer quantistico è ancora in una fase di sviluppo in quanto presenta delle sfide significative. Per far fronte a tali sfide, sono state sviluppate diverse implementazioni basate su superconduttori, atomi, ioni o fotoni.

Il computer quantistico a superconduttori sfrutta circuiti superconduttori per manipolare e memorizzare informazioni quantistiche. In particolare, sono realizzati utilizzando dispositivi microelettronici a temperature vicine allo zero assoluto (-273,15 °C). I qubit sono implementati come giunzioni Josephson in grado di generare e controllare gli stati di sovrapposizione e l'interferenza quantistica [14]. Tale tecnologia, permette di manipolare velocemente lo stato dei qubit, ave-

re un elevato controllo su quest'ultimo e propone una piattaforma altamente scalabile. Tuttavia, i computer a superconduttore sono sensibili alle perturbazioni ambientali e necessitano un raffreddamento a basse temperature per sfruttare le proprietà superconduttive dei materiali [15].

Un'altra possibilità nell'implementare i computer quantistici si basa sullo sfruttamento di atomi neutri [16, 17] o ioni intrappolati [18] e raffreddati a temperature molto basse. Questi ultimi, conosciuti come computer quantistici ad atomi freddi, memorizzano l'informazione codificando i qubit negli stati quantistici degli atomi o degli ioni intrappolati. La manipolazione degli stati degli atomi o ioni avviene, rispettivamente, utilizzando laser o campi elettromagnetici.

Un'altra possibile codifica dei qubit risiede nello sfruttamento degli spin di singole particelle. In tali computer quantistici a qubit di spin, la manipolazione avviene attraverso campi magnetici, impulsi di microonde e altre tecniche di controllo per modificare gli stati di spin. Per la realizzazione di tali calcolatori, diverse piattaforme continuano ad essere esplorate, come i qubit di spin di ioni intrappolati [19], dei centri NV [20], molecolari [21] e basati su semiconduttori [22].

Infine, diverse piattaforme fotoniche sono state utilizzate per sviluppare computer quantistici che sfruttano la luce (fotoni) al fine di rappresentare e manipolare l'informazione quantistica. Sia le variabili discrete che continue possono essere sfruttate per codificare i qubit [23]. Nel primo caso, si utilizzano solitamente gli stati di polarizzazione dei fotoni o i loro stati di cammino (modalità spaziali), mentre nel secondo gli osservabili del campo elettromagnetico. Tramite l'ottica integrata è possibile proporre piattaforme scalabili, in cui la generazione, manipolazione e rivelazione dei singoli fotoni avviene attraverso elementi ottici integrati in una singola piattaforma oppure attraverso un approccio ibrido [24]. In questo caso, la sfida principale è di riuscire a scalare in maniera significativa il numero di elementi integrati e di minimizzare le diverse perdite del sistema.

Stato dell'arte e prospettive future

Nelle sezioni precedenti abbiamo introdotto i concetti chiave della computazione e della crittografia quantistica e discusso i possibili sistemi fisici che vengono oggigiorno investigati per poter sviluppare tecnologie nei suddetti campi. Attualmente l'informazione quantistica sta vivendo una stagione di transizione, ovvero da una situazione in cui la maggior parte della ricerca si svolge in ambito accademico ad uno scenario in cui grandi aziende e grandi investimenti incentivano lo sviluppo di tali tematiche, allo scopo di realizzare prototipi performanti da introdurre sul mercato.

Tra le piattaforme più mature per quanto riguarda la computazione quantistica figura quella che sfrutta qubit superconduttori e il modello circuitale. Google, Rigetti e IBM sono le più grandi aziende che hanno deciso di sviluppare un computer quantistico con questa tecnologia. In particolare, IBM mette a disposizione sul suo cloud [25] diversi dispositivi che contano fino a centinaia di qubit e prevede di aumentare la capacità di calcolo dei suoi processori raggiungendo i 100000 qubits nei prossimi 10 anni. Inoltre, recentemente, la start-up francese Alice & Bob sta proponendo una variante nel controllo dei qubit superconduttori allo scopo di mitigare il rumore e le procedure di error-correction nelle varie porte logiche.

Un approccio sempre di tipo circuitale è utilizzato dalla start-up IonQ che propone però processori basati su ioni intrappolati fino a 20 qubit. Il processore di IonQ è disponibile sul cloud di Amazon Braket [26], la piattaforma gestita da Amazon che permette l'utilizzo da remoto di diversi processori quantistici delle diverse aziende e start-up del settore.

Le piattaforme basate su atomi neutri intrappolati stanno raggiungendo livelli di complessità e performance siginficative. La start-up americana QuEra mette a disposizione sul cloud di Amazon Braket un computer ad atomi neutri che conta 250 qubit, mentre la start-up francese PASQAL commercializza processori con 100 qubit. Questi dispositivi sono basati sulla computazione analogica, in cui le operazioni logiche vengono realizzate cambiando l'hamiltoniana di

interazioni tra gli atomi.

In ambito fotonico le principali start-up, ovvero l'americana Psi Quantum e la canadese Xanadu, stanno procedendo verso un computer quantistico basato sull'approccio measurement-based. Più precisamente, Psi Quantum sta puntando su qubit processati attraverso fotonica integrata. La start-up Xanadu invece sta utilizzando il cosiddetto schema a variabili continue, nel quale l'informazione viene codificata nei valori attesi degli osservabili del campo elettromagnetico, che possono assumere, per l'appunto, valori continui. Xanadu ha a disposizione due dispositivi sul proprio cloud [27], compreso Borealis (disponibile fino allo scorso 2 giugno 2023), il processore quantistico non universale che ha dimostrato recentemente la possibilità di superare un computer classico nella risoluzione di uno specifico problema di campionamento [28]. In ambito europeo, segnaliamo le startup Quandela e QuiX, la prima impegnata principalmente nella produzione di sorgenti di singoli fotoni performanti e commercializzabili, mentre la seconda si occupa del design e dello sviluppo della parte circuitale dei dispositivi fotonici integrati. Come anticipato nelle precedenti sezioni, i qubit fotonici sono impiegati soprattutto nell'ambito delle comunicazioni e della crittografia. Le aziende Toshiba e ID Quantique sono impegnate nel produrre strumenti e dispositivi per la crittografia quantistica. Un prototipo di rete di comunicazione quantistica su grande scala è stato realizzato in Cina, il quale comprende canali di comunicazione in fibra ottica tra le città di Beijing, Hefei, Shanghai e Jinan e il canale satellitare tra gli osservatori di Nanshan e Xinglong [29]. Altre reti quantistiche basate su fibre sono in sviluppo nel Regno Unito [30] e in Europa [31], compresa l'Italia.

Dal quadro appena fornito risulta evidente quanto le tecnologie quantistiche siano ad oggi di centrale interesse. Gli investimenti fatti da diverse aziende e nazioni in queste tematiche hanno subito un vistoso incremento negli ultimi 5 anni. La sfida dei prossimi anni sarà quindi di riuscire a sviluppare quella svolta tecnologica necessaria per rendere tali dispositivi utilizzabili e performanti in problemi concreti. Ovvero, in altre parole, di poter considerare conclusa la stagione della seconda rivoluzione quantistica, per aprire la strada alla terza, quella dello sviluppo tecnologico vero e proprio.

Ringraziamenti

Questo lavoro è supportato dalla sovvenzione ERC Advanced QU-BOSS (Grant Accordo n. 884676) e dal progetto PNRR MUR PE0000023-NQSTI.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (UK) (2010).

[2] H. Briegel et al.: *Measurement-based quantum computation*, Nature Phys., 5 (2009) 19.

[3] A. Broadbent, J. Fitzsimons, E. Kashefi *Universal Blind Quantum Computation* 2009 50th Annual IEEE Symposium on Foundations of Computer Science, Atlanta, GA, USA, (2009) 517.

[4] V. Giovannetti, L. Maccone, T. Morimae, T. G. Rudolph: *Efficient Universal Blind Quantum Computation*, Phys. Rev. Lett., 111 (2013) 230501.

[5] E. Farhi, S. Gutmann: *Analog analogue of a digital quantum computation*, Phys. Rev. A, 57 (1998) 2403.

[6] S. J. Devitt, W. J. Munro, K. Nemoto: *Quantum error correction for beginners.*, Reports on Progress in Physics, 76 (2013) 076001.

[7] B. P. Lanyon et al.: *Measurement-Based Quantum Computation with Trapped Ions*, Phys. Rev. Lett., 111 (2013) 210501.

[8] A. Das, B. K. Chakrabarti: *Colloquium: Quantum annealing and analog quantum computation*, Rev. Mod. Phys., 80 (2008) 1061.

[9] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden : *Quantum cryptography*, Reviews of modern physics, 74 (2002) 145.

[10] A. K. Ekert: *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., 67 (1991) 661.

[11] C. H. Bennett, G. Brassard: *Quantum cryptography: Public key distribution and coin tossing*. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, New York, 175 (1984) 8.

[12] S. Pirandola et al.: *Advances in quantum cryptography*, Advances in optics and photonics, 12 (2020) 1012.

[13] S. K. Liao et al.: *Satellite-to-ground quantum key distribution*, Nature, 549 (2017) 43.

[14] M. H. Devoret, A. Wallraff, J. M. Martinis *Superconducting Qubits: A Short Review* (2004) ArXiv. /abs/cond-mat/0411174

[15] M. Kjaergaard et al.: *Superconducting qubits: Current state of play*, Annual Review of Condensed Matter Physics, 11 (2020) 369.

[16] H. J. Briegel et al.: *Quantum computing with neutral atoms*, Journal of modern optics, 47 (2000) 415.

[17] L. Henriet et al.: *Quantum computing with neutral atoms*, Quantum, 4 (2020) 327.

[18] C. D. Bruzewicz, J. Chiaverini, R. McConnell, J. M. Sage: *Trapped-ion quantum computing: Progress and challenges*, Applied Physics Reviews, 6 (2019) 021314.

[19] You-Song Ding, Yi-Fei Deng, Yan-Zhen Zheng: *The rise of single-ion magnets as spin qubits*, Magnetochemistry, 2 (2016) 40.

[20] L. Childress, R. Hanson: *Diamond NV centers for quantum computing and quantum networks*, MRS bulletin, 38 (2013) 134.

[21] A. Gaita-Ariño, F. Luis, S. Hill, E. Coronado: *Molecular spins for quantum computation*, Nature chemistry, 11 (2019) 301.

[22] J. J. Pla et al.: *A single-atom electron spin qubit in silicon*, Nature, 489 (2012) 541.

[23] F. Flamini, N. Spagnolo, F. Sciarrino: *Photonic quantum information processing: a review*, Reports on Progress in Physics, 82 (2018) 016001.

[24] J. Wang, F. Sciarrino, A. Laing, A., M. G. Thompson: (2020). *Integrated photonic quantum technologies* Nature Photonics, 14 (2020) 273;
E. Pelucchi et al. *The potential and global outlook of integrated photonics for quantum technologies* Nature Reviews Physics, 4 (2022) 194.

[25] IBM Quantum https://quantum-computing.ibm.com/

[26] Amazon Web Service (AWS), Amazon Braket https://aws.amazon.com/it/braket/

[27] Xanadu, Xanadu cloud, https://www.xanadu.ai/

[28] L. S. Madsen et al.: *L*, ., S (.) ,. Laudenbach, F., Askarani, M.F. et al. Quantum computational advantage with a programmable photonic processor Nature 6062022 75

[29] Y.A. Chen et al.: *An integrated space-to-ground quantum communication network over 4,600 kilometres*, Nature, 589 (2021) 214.

[30] Quantum Communications Hubs, https://www.quantumcommshub.net/

[31] The European Quantum Communication Infrastructure (EuroQCI) Initiative, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

Taira Giordani: ha conseguito il dottorato di ricerca nel 2020 nel Dipartimento di Fisica della Sapienza Università di Roma dove è attualmente ricercatrice. Le sue attività di ricerca riguardano protocolli di computazione quantistica basati su piattaforme fotoniche. In particolare, si occupa di esperimenti su fotonica integrata e bulk, sfruttando diversi gradi di libertà di stati a singolo fotone.

Alessia Suprano: ha conseguito il dottorato di ricerca nel 2022 nel Dipartimento di Fisica della Sapienza Università di Roma dove attualmente è titolare di un assegno di ricerca. Le sue attività si focalizzano principalmente su protocolli di informazione quantistica che impiegano risorse fotoniche ad alta dimensione.

Fabio Sciarrino: è Professore Ordinario presso il Dipartimento di Fisica dell'Università di Roma La Sapienza e Senior Research Fellow presso la Scuola Internazionale Superiore di Studi Avanzati Sapienza, SSAS. È Principal Investigator del Quantum Information Lab, Dipartimento di Fisica. Le sue principali competenze sono l'ottica quantistica sperimentale, il calcolo e l'informazione quantistica e le basi della meccanica quantistica.