Anitec-Assinform

White Paper

Tecnologie Quantistiche per la Sicurezza delle Comunicazioni Digitali

A cura del
Comitato Ricerca, Sviluppo e Innovazione
con la collaborazione del CNR

Maggio 2023

Associazione Italiana per l'Information and Communication Technology (ICT)
Milano, Via San Maurilio 21, 20123
Telefono 02 0063281
segreteria@anitec-assinform.it – anitec-assinform@pec.it – www.anitec-assinform.it
P.IVA: 10053550967 C.F.: 10053550967

Anitec-Assinform

Contributi di:

IBM S.p.A., ITALTEL S.p.A., LEONARDO S.p.A., SOGEI S.p.A., TIM S.p.A.

Anitec-Assinform

Sommario

EXECUTIVE SUMMARY

Il white paper "Tecnologie Quantistiche per la Sicurezza delle Comunicazioni Digitali" analizza lo scenario dell'evoluzione della sicurezza delle comunicazioni al cambiare delle tecnologie disponibili.

L'avanzamento della capacità di calcolo dei quantum computer, infatti, renderà "violabile" la crittografia comunemente utilizzata per proteggere le comunicazioni; la tecnologia quantistica, al contempo, mette a disposizione anche gli strumenti per fronteggiare questa potenziale minaccia.

La QKD (Quantum Key Distribution), che consente di trasferire una chiave crittografica con la garanzia di confidenzialità, e la QRNG (Quantum Random Number Generation), che contribuisce a generare chiavi crittografiche robuste attraverso la generazione di numeri casuali, sono due tecnologie quantistiche con un elevato livello di maturità con le quali poter realizzare soluzioni di altissimo livello di sicurezza, superiore anche alle capacità del quantum computer.

Molti Operatori in Europa (ad es. BT, DT, TID, TIM), negli USA (ad es. Verizon, AT&T) e in ASIA (ad es. SKT, NTT) stanno conducendo delle sperimentazioni in campo sui sistemi di sicurezza quantistica basate su QKD e QRNG.

A esempio, nel contesto dei progetti europei, si segnalano l'iniziativa Quantum Flagship e Euro-Quantum Communications Infrastructure (Euro-QCI) della Unione europea (H2020). L'iniziativa Quantum Flagship è stata lanciata nel 2018 con un budget di un miliardo di euro con una durata di dieci anni. La Flagship riunisce istituti di ricerca, università, industria, enti pubblici e privati in un'iniziativa congiunta e collaborativa sullo sviluppo delle tecnologie e dei servizi quantistici in Europa. L'obiettivo principale della Euro-QCI è consentire lo sviluppo di una rete pan-europea sicura basata sulla distribuzione di chiavi quantistiche, con collegamenti terrestri e satellitari.

Le aree su cui si sta operando sono:

1. *La standardizzazione*: tutti i principali enti di Normativa Internazionale, ITU-T, ETSI, IETF, CEN-CENELEC, GSMA, etc stanno producendo sforzi significativi per definire aree di applicazione, roadmap e snodi su cui preparare degli Standard.
2. *Lo sviluppo delle competenze:* nel campo della sicurezza quantistica delle comunicazioni, vi è un fabbisogno crescente di specialisti in

crittografia e, in generale, una rimodulazione delle competenze in ambito cybersecurity, a conferma del rapporto diretto competenza nello sviluppo delle tecnologie quantistiche *vs.* grado di sicurezza nelle comunicazioni.

È necessario, quindi, un programma di formazione con particolare focus sulle nuove tecnologie come, peraltro, ben indicato tra i fattori abilitanti della Strategia nazionale di cybersicurezza 2022-2026.

La sicurezza delle comunicazioni digitali spinge l'attuale rete di comunicazione italiana a conseguire un livello di sicurezza superiore all'attuale; per questo, è fondamentale procedere con una graduale introduzione dei sistemi quantistici nelle attuali reti, a fronte di un processo di standardizzazione, a partire da quelle aree di applicazione dove il vantaggio strategico di mercato è massimo, come ad esempio nella sicurezza.

In maniera più puntuale, si propone di dare seguito alle seguenti iniziative in previsione dei servizi offerti dalle future architetture di rete orientate alla quantum internet:

1) realizzare un'infrastruttura di rete fissa per la QKD e consolidare le relative attività di testing.
2) Supportare le aziende tecnologiche italiane per la realizzazione di una filiera quantistica nazionale.
3) Creare una rete geografica di distribuzione delle chiavi crittografiche come servizio di sicurezza.
4) Integrare i piani di formazione universitari per creare competenze specifiche
5) Garantire l'applicazione puntuale delle indicazioni previste dalla Misura #22 del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026.

1. PREMESSA

Lo sviluppo di un'industria quantistica nazionale sostenibile presuppone l'esistenza di un ecosistema quantistico ben definito e operativo che si ispiri a principi: competenza e cooperazione tra le parti, in particolare tra pubblico e privato.

Il quantum computing e le quantum secure communications costituiscono certamente due tra le aree di maggior potenziale per lo sviluppo di attività di ricerca e sviluppo e delle competenze correlate.

È da notare, inoltre, che, a differenza delle criticità affrontate oltre venti anni fa in preparazione dell'anno 2000 (*millenium bug*), l'impatto della corrispondente transizione al quantum – indicata come "Y2Q" – è oggi ben noto: rimangono soltanto da definirne le tempistiche e investire in tale direzione.

Anitec-Assinform – l'Associazione che rappresenta le aziende del settore ICT e dell'innovazione digitale – vuole offrire una fotografia dello stato dell'arte delle attività, dei progetti in questo settore e dello stato delle competenze nonché un'indicazione delle azioni necessarie nel prossimo futuro per garantire la piena competitività del Paese in questo campo.

Il Comitato Ricerca, Sviluppo e Innovazione, in collaborazione con il CNR, ha sviluppato due studi: "Il Quantum Computing a supporto della trasformazione digitale italiana" e "Tecnologie Quantistiche per sicurezza delle Comunicazioni Digitali".

Partendo da uno scenario comune, i due white paper affrontano distintamente: le peculiarità e le diverse applicazioni rese disponibili dalla tecnologia quantum applicata all'IT e le prospettive future della sicurezza nelle comunicazioni digitali.

2. Introduzione alle Tecnologie Quantistiche

La prima rivoluzione quantistica, sviluppatasi alcuni decenni or sono con l'introduzione dei transistor, ha permesso lo sviluppo della micro-elettronica attualmente di uso comune e, quindi, di tutti quei dispositivi e terminali di uso quotidiano, come ad esempio PC, smartphone, LED, Laser ma anche PET (Tomografia a Emissione di Positroni) e RMN (Risonanza Magnetica Nucleare) che sono ampiamente utilizzate in ambito clinico-diagnostico.

Oggi i trend osservati indicano che è in atto una seconda rivoluzione quantistica: si assiste a una nuova impressionante crescita di interesse per le applicazioni delle nuove tecnologie quantistiche, con investimenti da parte di organizzazioni pubbliche e private in tutto il mondo. Il nuovo sviluppo delle tecnologie quantistiche si basa su tre fenomeni quantistici, ben noti e ben sperimentati in fisica: sovrapposizione, entanglement e no-cloning. La sovrapposizione riguarda la proprietà degli oggetti quantistici di rimanere in una combinazione lineare di stati multipli finché non vengono osservati. L'entanglement è definito come la possibilità che due o più oggetti quantistici rimangano intrinsecamente collegati, in uno stato intrecciato, indipendentemente dalla distanza tra gli oggetti. Infine, il no-cloning riguarda il fatto che l'informazione quantistica non può essere duplicata.

L'industria, tuttavia, non è ancora in grado di sfruttare appieno le potenzialità di questi fenomeni quantistici a causa principalmente dei costi elevati della tecnologia, ancora in una fase di sviluppo, e della mancanza di competenze di alto livello, presenti, in parte, a livello universitario ma non ancora diffuse nelle imprese. Anche per questo, la collaborazione pubblico-privato giocherà certamente un ruolo decisivo per la diffusione e l'utilizzo delle tecnologie quantistiche.

Le quattro principali aree di applicazione della seconda rivoluzione quantistica riguarderanno computer quantistici, sistemi avanzati di crittografia per la trasmissione sicura di dati, sensori e sistemi metrologici molto sensibili, oltre che metodi quantistici di simulazione per ambiti di progettazione complessa (fig. 1).

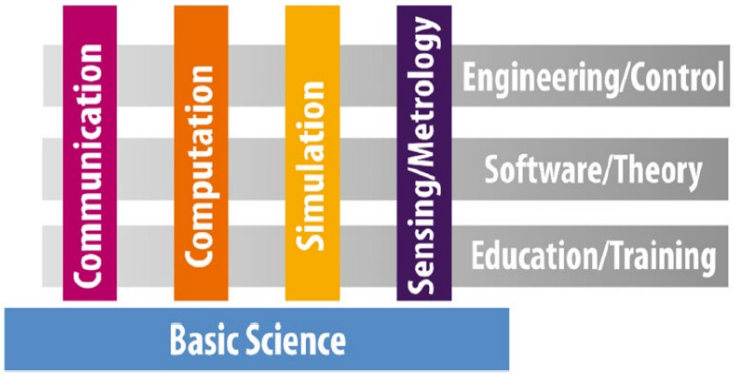

Figura 1: aree di applicazione delle tecnologie quantistiche [1]

Per quanto riguarda il tema della sicurezza delle comunicazioni digitali, oggetto di questo documento, si ritiene che l'avanzamento della capacità di calcolo dei quantum computer renderà "violabile" la crittografia comunemente utilizzata per proteggere le comunicazioni. La tecnologia quantistica, però, mette a disposizione anche gli strumenti per fronteggiare questa minaccia. La QKD e la QRNG (Quantum Random Number Generation) sono le due tecnologie quantistiche con un elevato livello di maturità con le quali poter realizzare soluzioni di altissimo livello di sicurezza, superiore anche alle capacità del quantum computer.

La QKD (Quantum Key Distribution) consente di trasferire una chiave crittografica con la garanzia di confidenzialità. La QRNG (Quantum Random Number Generation) contribuisce a generare chiavi crittografiche robuste attraverso la generazione di numeri casuali.

[1] Fonte: https://digital-strategy.ec.europa.eu/en/library/intermediate-report-quantum-flagship-high-level-expert-group

3. QUADRO DI RIFERIMENTO

Il processo di digitalizzazione abilita la comunicazione audio e video a lunga distanza e permette la dematerializzazione dei documenti.

Procedure che in passato richiedevano la presenza fisica possono oggi realizzarsi grazie alla rete internet che interconnette ogni angolo del globo. I dati trasportati su internet attraversano innumerevoli apparati di trasmissione e istradamento, i router, e possono quindi essere facilmente intercettati. Per questo motivo, per realizzare comunicazioni sicure su internet, è necessario utilizzare metodi per la protezione come quelli forniti dalla crittografia.

3.1. Crittografia in breve

Un algoritmo crittografico è come una cassaforte che può essere aperta solo da chi possiede la chiave giusta. Un dato o un messaggio vengono prima codificati utilizzando una chiave crittografica (encryption key) e poi possono essere tranquillamente spediti sulla rete internet. Se anche venissero intercettati, per essere letti devono essere prima decodificati, utilizzando la stessa chiave crittografica utilizzata per la codifica. Quindi, la sfida della crittografia consiste nella capacità di distribuire la chiave crittografica al legale destinatario di un messaggio.

Alcuni esempi di utilizzo della crittografia si sperimentano nella vita moderna tutte le volte che effettuiamo un'operazione con una banca online. Prima di tutto il protocollo "*https*" consente al browser di collegarsi al sito internet della banca mantenendo riservata la comunicazione. Inoltre, quando deve essere autorizzata un'operazione, viene normalmente richiesto di inserire un codice tramite un'applicazione sul nostro smartphone per ottenere un ulteriore livello di sicurezza.

Tutti i meccanismi di sicurezza appena descritti e utilizzati normalmente si basano sulla complessità computazionale, ossia su procedimenti matematici complessi che un normale computer potrebbe decodificare in centinaia o migliaia di anni. Tutto questo dovrebbe instillare un senso di sicurezza. E invece la minaccia alla riservatezza dei dati e delle comunicazioni ora è a rischio a causa delle enormi potenzialità del computer quantistico.

3.2. Il computer quantistico come opportunità e minaccia[2]

I computer quantistici promettono di portare grandi benefici in quasi tutti i settori industriali grazie alla loro capacità di risolvere problemi che non possono essere affrontati dai computer tradizionali in tempi ragionevoli per l'utilizzo nel business. Questo è dovuto al fatto che alcuni algoritmi che oggi usiamo sui nostri computer raddoppiano il tempo necessario alla loro esecuzione ogni volta che aggiungiamo complessità al problema trattato. Tale meccanismo si rileva in molti problemi di ottimizzazione: nella simulazione dei sistemi naturali, nell'intelligenza artificiale e in alcuni problemi algebrici.

Il computer quantistico è caratterizzato da un'architettura che permetterà di risolvere questi problemi, anche con livelli di complessità molto elevata in tempi ragionevoli. Il computer quantistico, per quanto possibile conoscere ora, sarà dunque uno strumento complementare ai computer attuali che permetterà di estendere il numero di problemi risolvibili con l'informatica. I primi computer quantistici reali sono stati messi a disposizione di tutti, in rete, da IBM nel 2016. Da quel momento, la potenza e la qualità di questi primi prototipi stanno migliorando anno dopo anno e a breve saranno pronti per essere usati in processi produttivi portando risultati più accurati e più rapidi dei computer tradizionali.

Tra i problemi che i computer quantistici saranno in grado di risolvere più rapidamente, ce ne sono anche alcuni che oggi vengono utilizzati per proteggere le chiavi crittografiche dei dati. In particolare, è già noto dal 1994 l'algoritmo di Shor[3] che permette di fattorizzare numeri, anche con moltissime cifre, in pochi giorni o settimane. L'incapacità dei computer attuali di effettuare la fattorizzazione in tempi inferiori alle centinaia di anni è alla base di molti schemi crittografici in particolare quelli a chiave asimmetrica. I computer quantistici attuali hanno ancora una potenza molto ridotta per eseguire questi calcoli, ma la stima della potenza necessaria per rompere la crittografia RSA 2048 è incrementata da 1 miliardo di qubit nel 2012 a 13.000 qubit nel

[2] Per approfondimenti, si veda il White Paper dedicato a "Il Quantum Computing a supporto della Trasformazione Digitale Italiana".

[3] L'algoritmo di fattorizzazione di Shor è un algoritmo ideato da Peter Shor nel 1994 per risolvere il problema della fattorizzazione dei numeri interi in numeri primi.

2021[4]. Oggi i computer con il maggior numero di qubit per processore ne hanno 400 e stanno progredendo speditamente.

Di fianco agli approcci matematici tradizionali è emersa l'esigenza di dotarsi di algoritmi resistenti agli attacchi quantistici, noti come Post Quantum Cryptography (PQC), che siano basati su problemi non risolvibili neanche da computer quantistici molto potenti. Per questo motivo il NIST (National Institute of Standards and Technology, USA) ha selezionato nel luglio del 2022, dopo un percorso di quasi sei anni, i primi quattro algoritmi PQC[5]. IBM è stata una delle principali contributrici nel processo di selezione con la realizzazione di tre dei quattro schemi selezionati che hanno evidenziato le debolezze di alcuni di quelli scartati.

Sebbene il momento in cui la minaccia di un attacco quantistico sia ancora relativamente lontano, è molto importante cominciare a proteggere i dati in anticipo per difendersi da attacchi di tipo *"harvest now, decrypt later",* ovvero entità che "copiano" i dati criptati oggi per poi decriptarli non appena saranno disponibili computer quantistici abbastanza potenti.

Per comprendere meglio l'innovazione portata dai computer quantistici, si deve partire dal modo nel quale vengono memorizzate le informazioni di base.

I computer che si usano quotidianamente rappresentano le informazioni con sequenze di bit che possono valere solo 0 o 1. L'unità di calcolo dei computer quantistici invece utilizza i qubit, i quali possono assumere un qualsiasi valore all'interno di una sfera di probabilità. Inoltre, i qubit possono essere messi in uno stato di sovrapposizione, una sorta di "forse digitale" che gli permette di rimanere indecisi tra sì e no fin quando non vengono letti. Poiché esistono infiniti gradi di indecisione, ad esempio 50% sì e 50% no, 30% sì e 70% no e così via, la sovrapposizione dei qubit permette di generare istantaneamente tutte le soluzioni possibili di un problema.

In sintesi, quello che con un computer tradizionale viene eseguito solo tramite una sequenza di operazioni, in un computer quantistico equivale a una singola operazione. Il vantaggio in termini di potenza computazionale è evidente. La sovrapposizione quantistica permette anche la realizzazione del *superdense*

[4] ("Factoring 2048-bit RSA Integers in 177 Days with 13436 Qubits and a Multimode Memory" Gouzien, Sangouard, 2021)
[5] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

coding, ovvero un protocollo di comunicazione impiegato nella trasmissione di una sequenza di bit di informazione con un minor numero di qubit, con la condizione che chi invia e chi riceve condividano delle risorse in entanglement.

Alcune delle applicazioni dei quantum computer riguardano problemi di ottimizzazione, simulazione dei sistemi naturali, algoritmi usati per l'intelligenza artificiale e alcuni problemi algebrici. Il computer quantistico disponibile oggi sarà dunque uno strumento complementare ai computer attuali che ci permetterà di estendere il numero di problemi risolvibili con l'informatica.

Nell'aprile 2016, la comunità internazionale della cybersecurity è stata scossa dall'annunciodel NIST: *"Regardless of whether we can estimate the exact time of the arrival the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing"* [6]. Questo vale in particolare per quelle tipologie di dati per cui è necessario garantire che restino segreti per lungo tempo.

Per tutte le altre tipologie di dati è comunque importante cominciare a fare l'inventario degli schemi crittografici in uso e definire dei processi per la loro rapida modifica. Questi ultimi processi passano sotto il nome di Crypto Agility. Lo stesso presidente degli Stati Uniti, Biden, nel maggio del 2022 ha inviato un memorandum alle agenzie governative statunitensi in cui definisce tempi molto chiari per la mappatura e sostituzione degli schemi crittografici vulnerabili[7].

Inoltre, è da valorizzare l'importanza di usare sistemi crittografici avanzati per garantire la sicurezza nell'uso di cloud computing ad alte prestazioni (HPC).

Nel seguito di questo documento si vedrà come la sicurezza informatica viene attualmente gestita e quali soluzioni vengono fornite dalle tecnologie quantistiche.

6 https://csrc.nist.gov/projects/post-quantum-cryptography

7 https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

3.3. Attività in corso in Europa (operatori e progetti di ricerca e innovazione)

Molti Operatori in Europa (ad es. BT, DT, TID, TIM), negli USA (ad es. Verizon, AT&T) e in ASIA (ad es. SKT, NTT) stanno conducendo delle sperimentazioni in campo sui sistemi di sicurezza quantistica, basati su QKD e QRNG. In queste sperimentazioni si stanno utilizzando sia apparati commerciali QKD, sia soluzioni prototipali ancora in via di sviluppo e integrazione.

A esempio, nel contesto dei progetti europei, si segnalano l'iniziativa Quantum Flagship e Euro-Quantum Communications Infrastructure (Euro-QCI) dell'Unione europea (H2020). L'iniziativa Quantum Flagship è stata lanciata nel 2018 con un budget di 1 miliardo di euro con una durata di dieci anni. La Flagship riunisce istituti di ricerca, università, industria, enti pubblici e privati in un'iniziativa congiunta e collaborativa sullo sviluppo delle tecnologie e i servizi quantistici in Europa.

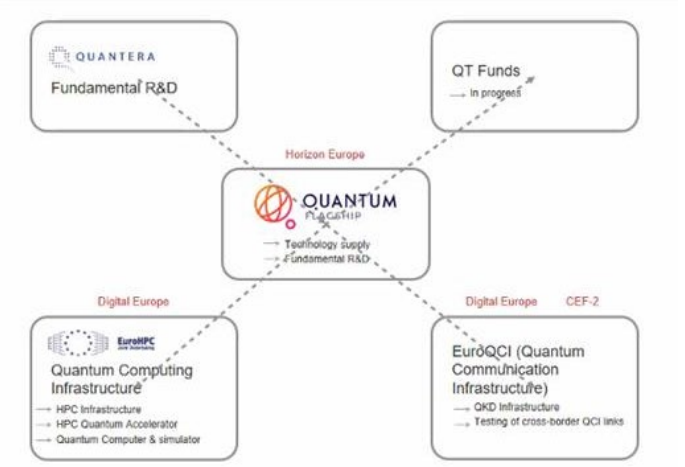

Fig. 2 Iniziative in corso in Europa finanziate dall'Unione europea[8]

L'obiettivo principale della Euro-QCI è consentire lo sviluppo di una rete pan-europea sicura basata sulla distribuzione di chiavi quantistiche, con collegamenti terrestri e satellitari. I primi utenti dell'infrastruttura Euro-QCI potrebbero essere istituzioni pubbliche e private, agenzie governative e autorità degli Stati membri e dell'Ue che richiedono un elevato livello di sicurezza per trasmettere informazioni riservate. Del consorzio, guidato da Airbus, fanno

[8] Fonte: Quantum Flagship https://qt.eu/

parte Leonardo, Orange, PwC France e Maghreb, Telespazio (Leonardo 67%, Thales 33%), il Consiglio Nazionale delle Ricerche (CNR) e l'Istituto Nazionale di Ricerca Metrologica (INRiM).

Euro-QCI integrerà le tecnologie e i sistemi quantistici nelle reti di comunicazione terrestre in fibra ottica e includerà un segmento spaziale che assicurerà una copertura completa in tutta l'Ue e in altri continenti. Infine, ciò consentirà di proteggere i sistemi di crittografia e le infrastrutture critiche europee, come le istituzioni governative, il controllo del traffico aereo, le strutture sanitarie, le banche e le reti elettriche, da minacce informatiche attuali e future.

In particolare, il segmento spaziale sarà sviluppato come parte di un altro progetto gestito dall'ESA (Agenzia spaziale europea) nell'ambito del progetto SAGA (Security And kryptoGrAphic mission).

Dal mese di giugno 2019, 26 stati membri hanno firmato la Dichiarazione EuroQCI per collaborare con la Commissione, sostenuta dall'Agenzia spaziale europea, allo sviluppo di un'infrastruttura di comunicazione quantistica che copra l'intera Unione europea. Il piano a lungo termine prevede che EuroQCI diventi la base di un'internet quantistica in Europa, collegando computer, simulatori e sensori quantistici, attraverso reti quantistiche per distribuire informazioni e risorse con una soluzione di sicurezza all'avanguardia.

A impiegarla per primo sarà il servizio QKD, che trasmetterà le chiavi di crittografia attraverso canali di comunicazione quantistica sia su fibra ottica terrestre sia su collegamenti laser spaziali. L'utilizzo di stati fotonici quantistici rende la chiave di distribuzione immune alle vulnerabilità, a differenza delle soluzioni attualmente impiegate. Lo studio, della durata di 15 mesi, definisce i dettagli del sistema end-to-end e la progettazione del segmento terrestre a supporto del servizio QKD e prevede lo sviluppo di una roadmap dettagliata, che includa i costi e le tempistiche di ciascuna fase di implementazione.

Lo studio supporterà, inoltre, la Commissione europea nella realizzazione di un'infrastruttura avanzata di test e convalida QCI, che include gli standard, con l'obiettivo di avviare un progetto pilota EuroQCI entro il 2024 e un servizio operativo iniziale entro il 2027. Il consorzio beneficerà della complementarità dei suoi membri, che include grandi integratori di sistemi, operatori di telecomunicazioni e satcom, nonché fornitori di servizi insieme a istituti di ricerca. Lo studio farà leva, valorizzandoli, sui contributi esistenti incentrati su

vari progetti quantistici, realizzati da ciascun membro del consorzio, e beneficerà della vasta esperienza sul campo della dorsale quantistica italiana grazie al CNR e all'INRiM.

Nell'ambito del Digital European Programme (DEP), segnatamente nella Call DIGITAL-2021-QCI-01-DEPLOY-NATIONAL – Deploying advanced national QCI systems and networks, si è costituito un consorzio che ha proposto il progetto di prossima partenza Quantum Italy Deplyment – QUID. L'obiettivo primario del progetto è quello di dispiegare sul territorio nazionale sistemi e network per provare le tecnologie di comunicazione quantistica e in particolare per la distribuzione quantistica di chiavi crittografiche, con l'attenzione a integrarle con le comunicazioni esistenti. L'altro obiettivo parimenti importante è quello di usare questi sistemi e networks per sviluppare use cases a sostegno di iniziative QCI nazionali nel contesto del succitato EuroQCI.

Fanno parte del progetto QUID il coordinatore INRIM ed i partner CNR, Agenzia spaziale italiana, Leonardo S.p.A., Thales Alenia Spazio Italia, TIM, Telsy, Think Quantum, Cohaerentia, QTI e realtà accademiche quali Politecnico di Milano, Università de L'Aquila, Università di Padova, Università di Roma La Sapienza, Università di Trieste.

Contemporaneamente, attraverso la call DIGITAL-2021-QCI-01-INDUSTRIAL - Create a European Industrial Ecosystem for Secure QCI technologies and systems, sono state finanziate delle proposte miranti a creare l'ecosistema industriale in grado di realizzare, con filiera europea, i prodotti necessari per l'implementazione della EuroQCI. Fra i 7 progetti finanziati le aziende italiane sono presenti nel secondo per livello di finanziamento, European QUantum ecOsystems – EQUO che riunisce, sotto la guida di TIM le aziende italiane QTI, Telsy, MPD, Sparkle insieme a INRIM e a Eblana (IE), IMEC (BE), Alea (DK), Openlight (CZ), Merqury (MT).

4. PROTEZIONE DELLE COMUNICAZIONI NELL'ERA DELLE TECNOLOGIE QUANTISTICHE

Come si è visto nel capitolo 3 – Quadro di riferimento, la sicurezza dei dati e delle comunicazioni è a rischio per via della difficoltà di distribuire chiavi crittografiche in maniera confidenziale, ossia con la sicurezza assoluta che nessuno, se non il legale destinatario, possa essersi impossessato della chiave.

Utilizzare chiavi crittografiche simmetriche è fondamentale per garantire la sicurezza delle comunicazioni. Il fondamento matematico è dato dal teorema di Shannon[9] che introduce il concetto di sicurezza incondizionata (unconditional security). Un messaggio protetto da una chiave simmetrica della stessa lunghezza del messaggio non contiene nessuna informazione che consenta di decodificarlo. Invece, tutti i meccanismi che utilizzano algoritmi matematici e chiavi asimmetriche, sono violabili se si possiede sufficiente potenza computazionale.

Le tecnologie quantistiche QKD e QRNG offrono una soluzione sfruttando le leggi della meccanica quantistica.

Prima di approfondire queste tecnologie daremo una breve descrizione dei modelli di sicurezza in uso finora, mostrando i limiti che invece le tecnologie quantistiche possono adeguatamente superare.

4.1. Modelli di protezione attualmente in uso

Nella descrizione seguente, in accordo con la letteratura specialistica, si indicheranno[10] Alice e Bob i due utenti (A e B) che intendono realizzare una comunicazione sicura.

Il sistema maggiormente utilizzato per la protezione delle comunicazioni prende il nome di Public Key Infrastructure (PKI) e si basa su un meccanismo di scambio di chiavi asimmetriche e di certificati digitali. Ogni utente possiede una chiave privata con la quale, attraverso un algoritmo matematico, è in grado di generare tante chiavi pubbliche diverse tra loro che vengono inviate in rete. Utilizzando le proprie chiavi private e pubbliche, Alice a Bob generano un certo numero di chiavi intermedie fino ad accordarsi su una chiave simmetrica con la

[9] https://en.wikipedia.org/wiki/One-time_pad#Perfect_secrecy
[10] https://en.wikipedia.org/wiki/Alice_and_Bob

quale proteggere la propria comunicazione. La PKI prevede anche un sistema di certificati digitali, emessi da Certification Authorities (CA) che vengono considerate attendibili (trusted) e che garantiscono l'identità dei server di rete. Il modello PKI è utilizzato per le comunicazioni su internet con il protocollo HTTP. I punti deboli di PKI consistono nella complessità di configurazione e gestione dei certificati digitali e, soprattutto, nell'utilizzo di chiavi asimmetriche che sono facilmente attaccabili da un computer quantistico.

Attualmente per ottenere la sicurezza incondizionata esiste un sistema tanto semplice quanto difficilmente utilizzabile su larga scala. Il metodo Pre-Shared Key (PSK) consiste nel creare una lista di chiavi simmetriche e inviarla fisicamente a tutte le coppie di utenti (Alice e Bob) che devono comunicare in maniera sicura. Per scegliere quale chiave utilizzare, Alice e Bob devono semplicemente prendere la prima chiave della lista e poi cancellarla. Questo meccanismo può essere usato efficacemente quando il numero di utenti è molto piccolo. Infatti, a ogni utente deve essere recapitata una lista diversa per ogni altro utente con il quale intende parlare. Al crescere del numero di utenti il numero di liste PSK da distribuire cresce in maniera combinatoriale.

Un nuovo approccio è la Post-Quantum Cryptography (PSC) che consiste nella realizzazione di nuovi algoritmi matematici che non fanno uso di meccanismi quantistici, ma costruiscono problemi che risultano complessi anche per i quantum computer. Il vantaggio di questo meccanismo di protezione è che può essere utilizzato già oggi su computer di tipo tradizionale. La sperimentazione prosegue e, a settembre 2022, GSMA (Global System for Mobile Communication Association) ha annunciato una collaborazione con Vodafone, IBM e altre aziende per identificare i passaggi chiave necessari per l'implementazione di tecnologie a sicurezza quantistica in infrastrutture di telecomunicazione critiche[11].

4.2. Quantum Key Distribution

La Quantum Key Distribution (QKD) è una tecnologia quantistica che consente di effettuare una trasmissione confidenziale di una sequenza di bit tra i due estremi di un canale quantistico. La proprietà di "confidenzialità" è

[11] https://www.gsma.com/newsroom/press-release/gsma-ibm-and-vodafone-establish-post-quantum-telco-network-taskforce/

importantissima perché è quella che consente ad Alice e Bob di condividere la stessa informazione con la sicurezza che nessuno possa averla intercettata. Se l'informazione trasmessa è una chiave crittografica simmetrica, allora può essere usata per trasmettere messaggi incondizionatamente sicuri, ossia protetti anche dall'attacco di un computer quantistico. Tutto questo a patto che la chiave crittografica sia stata scelta a caso e non sia il risultato di una elaborazione matematica per quanto complessa possa essere.

Per la determinazione della chiave la tecnologia Quantum Random Number Generation (QRNG) svolge proprio il compito di generare numeri casuali, superando il limite della generazione di numeri cosiddetti pseudocasuali, ossia generati da un programma applicando una funzione matematica.

Dal punto di vista fisico, la QKD si basa sulla trasmissione di un singolo fotone su un canale quantistico che trasporta l'informazione di un qubit. Rispetto al bit un qubit può essere rappresentato come una distribuzione di probabilità in una sfera. Le leggi fisiche della meccanica quantistica assicurano che il qubit non può essere intercettato perché nel momento nel quale viene letto viene anche distrutta l'informazione che porta. Questo meccanismo sta alla basa della confidenzialità delle informazioni trasmesse sul canale quantistico.

Un ulteriore vantaggio della QKD consiste nel fatto che ogni tentativo di intercettazione viene rivelato dalla presenza di errori di trasmissione nello stato dei fotoni e il processo di generazione della chiave non avviene.

Il fotone utilizzato per la QKD non può essere amplificato lungo la tratta di trasmissione. Di conseguenza i collegamenti QKD hanno una lunghezza limitata, a esempio, nell'ordine del centinaio di chilometri su una fibra dedicata o su poche decine di chilometri su una fibra utilizzata anche per traffico dati. Questi limiti rappresentano importanti elementi da tener presenti nella costruzione della rete fisica dei collegamenti QKD.

Per ovviare a questo limite, vi sono diversi approcci. Il primo è basato sull'introduzione all'interno della rete di Trusted Node, ovvero di nodi nei quali la sicurezza è assicurata dalla mancanza di accesso fisico esterno. Un secondo metodo è basato sull'introduzione di un livello software di astrazione, il Key Management Layer.

4.3. Reti per la distribuzione della sicurezza

La QKD risolve molto bene il problema della trasmissione di una chiave crittografica su un singolo link realizzato da un canale quantistico (fibra ottica, free-space satellitare o terrestre) ma ha importanti limitazioni rispetto alla lunghezza e comunque alla distribuzione capillare. L'esigenza di sicurezza invece è quella di condividere la stessa chiave crittografica simmetrica tra ogni coppia di Alice e Bob, che devono comunicare tra loro all'interno di una rete molto vasta e indipendentemente dalle limitazioni della rete fisica.

Per risolvere questo problema è necessario introdurre un livello di astrazione, che si indicherà Key Management Layer, tra la rete fisica di generazione delle chiavi crittografiche e le applicazioni che le useranno. In questo livello il Key Manager consente di passare dal singolo link alla rete, ovvero di distribuire le chiavi per la sicurezza in una rete geografica estesa in maniera trasparente rispetto alla tecnologia fisica e le sue limitazioni. In ambito internazionale sono in corso attività di studio e standardizzazione per il Key Management Layer e per la QKD.

In Italia sono presenti diverse industrie importanti per quanto riguarda la costruzione dell'infrastruttura della rete fisica e per la realizzazione delle funzioni di controllo della stessa, tra le quali ricade il Key Management Layer. Questo tema rappresenta uno snodo fondamentale per la diffusione della tecnologia per la realizzazione di comunicazioni sicure nel mondo moderno. Coinvolge sicuramente anche aspetti legati alla sicurezza nazionale e dell'Unione europea. Gli standard non sono ancora arrivati a cogliere tutto il valore di questo concetto. Data la complessità e i costi di questa impresa è tuttavia chiaro che le aziende o anche le università da sole non sono in condizione di raggiungere il risultato descritto: è necessario, dunque, mettere a fattor comune competenze e risorse per consentire all'Italia di occupare una posizione di leader nel campo della sicurezza delle comunicazioni.

4.4. Aspetti di integrazione tra QKD e Post-Quantum Cryptography

Il termine Post Quantum Cryptography (PQC), a volte indicato anche come quantum-proof, quantum-safe o quantum-resistant, si riferisce ad algoritmi crittografici (solitamente algoritmi a chiave pubblica) che hanno l'ambizione di ritenersi sicuri anche a fronte di un attacco da parte di un computer quantistico.

Le tecniche PQC si basano su problemi matematici per cui non sono noti algoritmi risolutivi efficienti, indipendentemente dalla loro natura classica o quantistica.

Pur non essendo ancora dimostrata l'assoluta robustezza quantistica degli algoritmi PQC finora analizzati dal NIST, questa tecnologia ha l'ambizione di offrire un livello di protezione molto più elevato dei metodi tradizionali. Esiste pertanto un grande interesse nel combinare la PQC e la QKD per ottenere soluzioni con diversi livelli di flessibilità e di sicurezza che si dimostrano adeguati a diversi casi d'uso e contesti: aA esempio usare la QKD per la sicurezza a livello fisico e PQC ai livelli applicativi superiori e per l'autenticazione.

Va notato che l'autenticazione dei canali classici coinvolti in un processo QKD è estremamente rilevante:

- *Autenticazione del canale classico utilizzato per il protocollo QKD (accanto a quello quantistico) in qualsiasi connessione punto-punto tra nodi.* Se un utente malintenzionato si infiltra su questo canale, non può ottenere informazioni sulle chiavi segrete ma può forzare errori nella chiave condivisa finale
- *Autenticazione della comunicazione tra un nodo e i centri di controllo e gestione.* Se un utente malintenzionato interrompe questa autenticazione, può controllare liberamente il nodo e inviare informazioni errate per la gestione

L'autenticazione di un canale classico può avvenire in due modi: o utilizzando una chiave precondivisa, che identifica indubbiamente l'utente dall'altra parte del filo, oppure utilizzando schemi a chiave pubblica.

In una rete QKD una chiave precondivisa è necessaria per la prima autenticazione mentre per le sessioni successive possono essere utilizzate le chiavi generate nel processo QKD.

Poiché non si vuole che la sicurezza dell'infrastruttura sia compromessa dall'implementazione di schemi di autenticazione la cui sicurezza contro gli attacchi quantistici non sia stata sufficientemente studiata per lo scambio di tale chiave precondivisa, si possono utilizzare schemi di crittografia a chiave pubblica resistenti ad attacchi di computer quantistici (PQC) sfruttati nella forma Digital Signature Algorithms (DSA).

A questo scopo è naturale guardare ai 3 algoritmi finalisti DSA della standardizzazione post-quantistica del NIST: *Dilithium, Falcon, Rainbow* (vedi par. 3.2).

4.5. Stato della normativa internazionale

Attualmente, tutti i principali enti di normazione internazionale si stanno occupando della seconda rivoluzione quantistica. A esempio, ITU-T, ETSI, IETF, CEN-CENELEC, GSMA, etc stanno producendo sforzi significativi per definire aree di applicazione, roadmap e snodi su cui preparare degli standard. Di seguito si elencano i principali gruppi di lavoro nei diversi enti di standardizzazione.

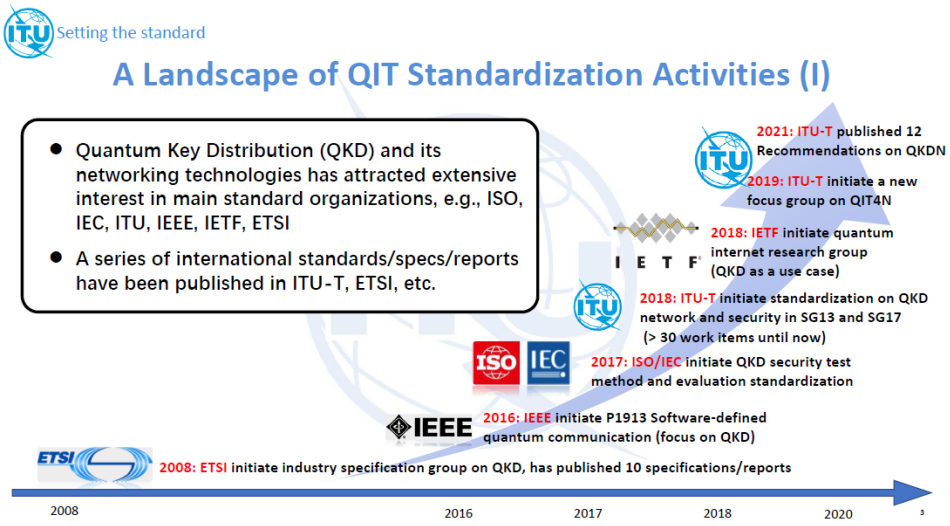

Fig. 3 Standardisation Activities – ITU

ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)

https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx

ETSI – Quantum Safe Cryptography

https://www.etsi.org/technologies/quantum-key-distribution

ETF – Quantum Internet Research Group (qirg)

https://datatracker.ietf.org/group/qirg/about/

CEN – CENELEC Focus Group on Quantum Technologies

https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/

GSMA IG Work-items on Quantum Technologies

https://www.gsma.com/newsroom/resources/ig-11-quantum-computing-networking-and-security/

https://www.gsma.com/newsroom/resources/quantum-networking-and-service/

Un aspetto centrale e di comune interesse dei vari Enti riguarda l'integrazione, dal livello fisico a quello di gestione e controllo, dei sistemi quantistici (ad esempio i sistemi QDK) nelle infrastrutture classiche (es. rete ottica e rete 5G). In tal senso, si prevedono attività di standardizzazione coordinata sullo sviluppo di architetture di rete e interfacce (API).

L'evoluzione degli attuali sistemi punto-punto QKD guarda a soluzioni di rete che prevedono, oltre all'aumento dei livelli di sicurezza nelle comunicazioni e nello scambio dati, anche un vero e proprio networking delle chiavi in topologie di rete articolate (*inter ed intra*). In tal senso, esistono alcuni punti di attenzione sui quali si stanno focalizzando le attività di standardizzazione, quali a esempio: la definizione delle architetture funzionali e di sistema delle reti quantistiche e delle interfacce dei sistemi e apparati quantistici, affinché questi ultimi possano essere facilmente integrabili – anche dal punto di vista della gestione e controllo – nelle attuali reti digitali. Il modello di riferimento che sta emergendo anche per la gestione e controllo di una rete quantistica QKD è basato sui concetti di piano di controllo, gestione e orchestrazione SDN (Software Defined Networks) che consentiranno l'integrazione multi-livello degli apparati, anche dal punto di vista della gestione e della programmabilità dei servizi di sicurezza quantistica.

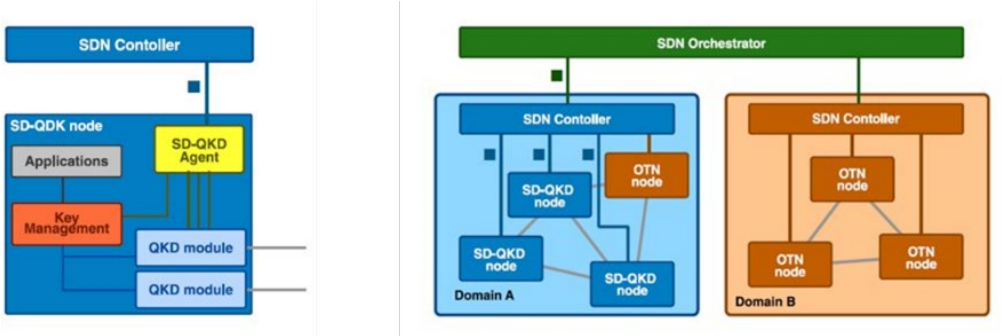

Fig. 4 Esempio di modello di riferimento SDN per il controllo ed orchestrazione di una rete ottica con sicurezza basata su sistemi QKD (fonte ETSI)

5. AMBITI DI APPLICAZIONE

La QKD, in linea teorica, fornirebbe servizi di elevati standard di sicurezza e la "Italian Quantum Backbone", che collega le principali città italiane da Milano a Matera, è uno di questi esempi. Nelle città di Milano e Napoli si stanno creando reti QKD tra aziende e centri di ricerca; Roma per ora, a parte il collegamento alla "Italian Quantum Backbone", sembra esclusa da questa attività. Eppure, uno use case interessante è proprio la comunicazione con QKD tra enti istituzionali, ministeri, aziende a partecipazione statale, dove lo scambio di informazioni confidenziali è cruciale. Esiste, inoltre, un grande interesse nel combinare la PQC e la QKD per ottenere soluzioni con diversi livelli di flessibilità e di sicurezza che si dimostrano adeguati a diversi casi d'uso e nei diversi contesti.

Di seguito, si riportano alcuni tra gli use case principali e i settori di applicazione.

5.1. Esempi di use cases e best practices

Use case possibili sono la definizione di nuovi standard e protocolli di sicurezza per il web, le applicazioni di chat, le VPN e blockchain quantum safe in generale per tutte le comunicazioni digitali.

Un'applicazione riguarda la cifratura per lo storage dei data base o più semplicemente di tutti quei file che si cifrano con una password e per i quali si riutilizza la stessa per decriptarlo in fase di lettura. Anche se è un argomento che non riguarda direttamente le comunicazioni digitali, è presente il rischio di data leak o attacchi hacker in cui dati sensibili vengono esposti in rete e successivamente decifrati da computer quantistici.

I metodi utilizzati per questo tipo di protezione sono algoritmi a chiave simmetrica**,** per esempio AES128, dove il livello di sicurezza è dato dalla lunghezza della chiave di protezione. Un computer classico per decifrare i dati senza conoscere la chiave di protezione deve procedere con "il metodo di forza bruta", ovvero provando tutte le chiavi possibili, rendendo praticamente impossibile la decifrazione. Al contrario, un computer quantistico può sfruttare l'algoritmo di Grover[12], che ha una potenza quadratica rispetto a una ricerca

[12] https://en.wikipedia.org/wiki/Grover%27s_algorithm

a forza bruta. Quindi, andrebbero aggiornati anche gli algoritmi a chiave simmetrica, o perlomeno aumentare opportunamente la lunghezza delle chiavi di cifratura per migliorarne la sicurezza.

Ancora, i sistemi QKD possono essere utilizzati per proteggere le comunicazioni e lo scambio dati in una rete di telecomunicazioni. Per esempio, la maggior parte dei collegamenti di backhaul (che connettono le centrali alle dorsali e le stazioni base al core della rete 5G) e di backbone di una rete di telecomunicazioni sono realizzati su fibra ottica: questo permette di trasportare canali classici e canali quantistici sulla stessa infrastruttura, per lo scambio dati crittografati e per distribuire le relative chiavi quantistiche crittografiche. Un altro esempio riguarda l'uso dei sistemi QKD per proteggere lo scambio dati tra Data Center.

L'impiego dei sistemi QKD può offrire servizi di sicurezza quantistica anche nel settore del collegamento a Edge e Cloud, p.es. in contesti Edge di Industry 4.0: la crittografia quantistica può essere applicabile per garantire alti livelli di sicurezza nello scambio dati nei sistemi di produzione, logistica e di processo, nel rispetto dei requisiti specifici di dominio in termini di criticità temporale e livelli di protezione. Un esempio di fattibilità di questo use case è stato recentemente dimostrato da TIM e il Competence Center CIM 4.0: in particolare è stata dimostrata la possibilità di trasmettere, in maniera sicura, i dati inviati da un braccio robotico del CIM 4.0 a un nodo Edge Cloud Computing che si trova in una centrale TIM posizionata a circa 10 km dalla sede CIM 4.0 [13].

Infine, un altro esempio è la sicurezza quantistica nello scambio dati tra Stati membri dell'Ue. Questo è l'obiettivo principale di Euro-QCI (Quantum Communications Infrastructure), cioè consentire la distribuzione di chiavi quantistiche per crittografia sicura nello scambio dati a livello paneuropeo. I primi utenti dell'infrastruttura Euro-QCI saranno agenzie governative e autorità degli Stati membri e dell'UE che richiedono un elevato livello di sicurezza per trasmettere informazioni riservate (prime dimostrazioni previste nel 2024). Tutti gli Stati membri hanno in corso di sviluppo i backbone QCI che verranno interconnessi tra loro creando la rete Euro-QCI.

[13] https://www.gruppotim.it/it/archivio-stampa/mercato/2023/CS-CIM4-0-TIM-16-03-23.html

6. Lo sviluppo delle competenze

Come abbiamo indicato nello studio "*Il Quantum Computing a supporto della Trasformazione Digitale Italiana*" (a cui si rimanda per una descrizione più dettagliata), all'alba di questa nuova fase tecnologica sta nascendo dal mondo industriale una richiesta di nuovi profili quali: *il Quantum Scientist, il Quantum Engineer, il Quantum Developer.*

A queste figure, nel campo della sicurezza quantistica delle comunicazioni, si aggiunge certamente la necessità di specialisti in crittografia e, in generale, una rimodulazione delle competenze in ambito cybersecurity a conferma del rapporto diretto tra competenza nello sviluppo delle tecnologie quantistiche e grado di sicurezza nelle comunicazioni.

È necessario, quindi, un programma di formazione con particolare focus sulle nuove tecnologie che è, peraltro, ben indicato tra i fattori abilitanti della Strategia nazionale di cybersicurezza 2022-2026.

La Promozione dell'uso della crittografia è infatti parte del manuale operativo del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 che alla Misura #22 prevede:

"Promuovere l'uso della crittografia in ambito non classificato, quale impostazione predefinita e comunque fin dalla fase di progettazione di reti, applicazioni e servizi, in conformità ai principi della sicurezza e della tutela della vita privata, nel rispetto dei principi stabiliti dalla normativa nazionale ed europea."

È un obiettivo, questo, la cui "misurazione" inizierà nell'anno 2023 per un raggiungimento previsto nell'anno 2026 come da cronoprogramma del piano; si prevede la partecipazione di tutti i soggetti coinvolti quali: Agenzia per la cybersicurezza nazionale e Dipartimento delle Informazioni per la Sicurezza, Ufficio Centrale per la Segretezza, Ministero della Giustizia, Ministero della Difesa, Ministero delle imprese e del made in Italy, Dipartimento per la trasformazione digitale, atenei e operatori privati.

Il riferimento agli operatori privati è peraltro parte dell'intera strategia nazionale che prevede (misura #5) di "*Supportare lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersicurezza e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane,*

favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato".

E ancora, in relazione alla richiamata Partnership Pubblico-Privato (PPP), *".... appare chiaro come il successo della strategia nazionale potrà essere assicurato soltanto tramite l'azione sinergica di istituzioni, industria, accademia e società civile, il cui rispettivo contributo, attraverso il conseguimento di singole azioni nei rispettivi ambiti, è essenziale per il raggiungimento degli obiettivi generali."*

7. LA COOPERAZIONE TRA PUBBLICO E PRIVATO

In Italia si sono state avviate diverse esperienze di collaborazione tra pubblico e privato che stanno dando luogo ad importanti iniziative di ricerca sulle tecnologie quantistiche. Di seguito si riportano alcuni esempi significativi:

Q-SecureNet. È un progetto di innovazione co-finanziato da EIT Digital. Il progetto, coordinato da Italtel, ha portato alla realizzazione di un trasmettitore e ricevitore per la QKD, utilizzando la tecnologia sviluppata dal Politecnico di Milano. Gli apparati sono stati sperimentati a Torino nella rete in esercizio dell'operatore Top-IX. I partner internazionali del progetto sono Telefonica e Universitad Politécnica de Madrid.

QUANCOM. Coordinata dal CNR è un'azione coordinata per lo sviluppo e la sperimentazione di protezione incondizionata della rete IP mediante criptografia quantistica (QKD). La sperimentazione avviene su di una rete ottica passiva metropolitana che verrà installata a Napoli, con uno dei nodi almeno all'interno della Università di Napoli *Federico II*. Il Progetto prevede anche l'esplorazione di altri due temi strategici come il completamento della rete in fibra mediante collegamento alla infrastruttura *quantum backbone* per la trasmissione del segnale di tempo sicuro in test QKD, e la sperimentazione di sistemi ibridi di comunicazione "optical fiber-free space" per lo sviluppo di applicazioni QKD in ambito spaziale.

PoliQI. Il progetto, attualmente in corso, coordinato dal Politecnico di Milano, ha lo scopo di realizzare una rete QKD nell'area di Milano per collegare almeno 5 siti con necessità di un altissimo livello di protezione delle comunicazioni.

QSAFE. Il progetto, coordinato da Deutsche Telekom e conclusosi a metà 2022, ha avuto come principale obiettivo la definizione dell'architettura di riferimento della Euro-QCI. L'Italia è presente con TIM che ha curato gli aspetti di evolutivi (sia di architettura di rete sia di controllo e gestione) verso il networking QKD (i.e., oltre il punto-punto).

EQUO. Il progetto, coordinato da TIM, è iniziato a gennaio 2023. L'obiettivo principale è portare a maturità tecnologica i sistemi QKD, anche dal punto di vista della gestione ed orchestrazione. La partecipazione italiana include Telsy, Sparkle e QTI.

QUID. Il progetto, coordinato da INRIM, inizia a gennaio 2023. L'obiettivo principale è sviluppare la QCI in Italia che si raccorderà con le QCI sviluppate

dagli altri Stati Membri in Europa a costituire la Euro-QCI. Il punto di partenza è l'Italian Quantum Backbone.

QIA. Il Framework Partnership Agreement (FPA) è un programma di ricerca e innovazione (2023-2029) con l'obiettivo di progettare e sviluppare l'Internet Quantistica in Europa (per l'Italia partecipa TIM).

QNSP. Questo FPA è un programma di ricerca ed innovazione (2023-2029) con l'obiettivo di sviluppare soluzioni evolute di sicurezza quantistica, a partire dagli attuali modelli QKD (per l'Italia partecipa TIM).

Quantum flagship. Avviata nel corso di Horizon2020 attraverso una serie di azioni di ricerca e innovazione strategicamente selezionate e orientate su quattro percorsi distinti (Computazione Quantistica, Simulazione Quantistica, Comunicazione Quantistica, Sensoristica e Metrologia Quantistica), si collega alle infrastrutture europee (European Quantum Communication Infrastructure-EuroQCI e European Quantum Computing/Simulation Infrastructure-EuroQCS) e si va strutturando sulla base di una prossima rete europea, attualmente in fase avanzata di definizione, di Istituti Nazionali per le Tecnologie Quantistiche. All'investimento per la Flagship, già programmato in Horizon2020 per un totale di 1 miliardo di euro ed una durata complessiva di 10 anni del Programma (2018-2028), si deve dunque aggiungere uno stanziamento ulteriore, che ad oggi è previsto essere di 1-2 miliardi di euro, per il cofinanziamento delle nuove infrastrutture europee ad esso legate.

Italian Quantum Backbone. Realizzato da INRIM e CNR, è una dorsale in fibra lunga 1850 km che collega le città italiane di Torino, Milano, Bologna, Firenze, Roma, Napoli per raggiungere Matera. L'IQB arriva fino al confine franco-italiano presso il traforo del Fréjus e può essere collegato in principio con infrastrutture analoghe in Svizzera, Austria, Germania e Slovenia. L'IQB offre ai ricercatori accesso completo 24 ore su 24 e può ospitare attrezzature di ricerca in edifici protetti ad accesso riservato posti ogni 50-100 km. Esso può essere collegato a reti metropolitane, che sono già state attrezzate nei test-bed dell'area di Torino e di Firenze. È inoltre possibile lo sviluppo di siti intermodali (Matera, Firenze, Padova) per tecnologie quantistiche terra-spazio.

8. Proposte di policy per lo sviluppo della tecnologia QKD in Italia e la ricerca & sviluppo del settore ICT

Le tecnologie quantistiche rappresentano indubbiamente un ambito di sviluppo di soluzioni per il mercato, per la sicurezza nazionale e per il benessere, in primis, dei cittadini italiani; inoltre costituiscono una risorsa strategica per l'intera Unione europea.

L'Italia vanta una fortissima competenza scientifica sulle tecnologie quantistiche. CNR, Politecnici e Università hanno estese relazioni internazionali nel mondo della ricerca e hanno sviluppato tecnologie e competenze di altissimo livello in Italia. Grazie anche alla recente disponibilità di nuovi fondi dal PNRR sarà possibile incrementare il nostro livello di sviluppo.

Le industrie operanti in Italia hanno sviluppato consolidate relazioni di collaborazione con il mondo della ricerca e sono attive a livello internazionale, essendo coinvolte in progetti di ricerca e innovazione con i principali attori dell'evoluzione scientifica e tecnologica.

Tuttavia, si tratta di tecnologie ancora molto costose, che in parte possono essere già utilizzate ma che richiedono un investimento importante per la loro integrazione industriale e la loro diffusione.

Per permettere all'Italia di consolidare la propria presenza nel campo delle comunicazioni quantistiche e di proteggere la propria sovranità digitale e la sicurezza nazionale è, quindi, assolutamente indispensabile realizzare un sistema virtuoso di collaborazione tra pubblico e privato.

Nel vasto panorama delle tecnologie quantistiche, QKD e QRNG, presentate in questo documento, sono tra le soluzioni più mature e già pronte per essere acquisite dall'industria per la realizzazione di nuovi prodotti e soluzioni. L'ambito principale di applicazione principale di QKD e QRNG è la sicurezza delle comunicazioni digitali; il che porta all'opportunità di far evolvere l'attuale rete di comunicazione italiana verso un livello di sicurezza altissimo.

Per questo, è fondamentale procedere con una graduale introduzione dei sistemi quantistici nelle attuali reti, a fronte di un processo di standardizzazione, a partire da quelle aree di applicazione dove il vantaggio strategico di mercato è massimo, come ad esempio nella sicurezza.

Questo potrebbe significare, da un lato, il dispiegamento sul territorio nazionale di sistemi e reti quantistiche per validare la distribuzione quantistica di chiavi

crittografiche, con l'attenzione a integrarle con le comunicazioni esistenti; dall'altro, l'utilizzo di queste infrastrutture per sviluppare le soluzioni di rete a sostegno delle citate iniziative Quantum Communications Infrastructure (QCI) nazionali, nel contesto internazionale della EuroQCI.

In maniera più puntuale, si propone di dare seguito alle seguenti iniziative:

1) *Realizzare un'infrastruttura di rete fissa per la QKD e consolidare le relative attività di testing.* Si pensa reti QKD metropolitane (reti in fibra ottica, collegamenti ottici terresti e satellitari) che saranno il primo oggetto di test per cui è opportuno anche iniziare a immaginare connessioni fra distretti industriali e/o Innovation Hub (intesi sia come DIH sia come Centri di competenza o Case delle Tecnologie).

2) *Supportare le aziende tecnologiche italiane per la realizzazione di una filiera quantistica nazionale.*

   - In Italia è presente un elevato livello di competenza nelle università, CNR, centri di ricerca, industrie, PMI.
   - Esiste un importante gruppo di aziende e PMI italiane in grado di realizzare soluzioni QKD.
   - Esistono importanti realtà italiane nella gestione di infrastrutture adatte alla tecnologia: reti in fibra e optical free space.

3) *Creare una rete geografica di distribuzione delle chiavi crittografiche come servizio di sicurezza.*

   - Superamento delle attuali limitazioni: fisica sulla lunghezza del link e tecnologica della protezione del singolo link.
   - Integrazione degli apparati e delle tecnologie disponibili (sia italiane che internazionali).

4) *Integrare i piani di formazione universitari per creare competenze specifiche* per l'utilizzo di sistemi crittografici avanzati così da garantire la sicurezza nell'uso del cloud computing ad alte prestazioni (HPC). L'infrastruttura di comunicazione che collegherà i nodi HPC dovrà essere, infatti, "quantum compatible". Non solo perché all'interno dei nodi HPC

saranno presenti i primi Quantum Computer ma anche per rafforzare la sicurezza della computazione classica.

5) *Garantire l'applicazione puntuale delle indicazioni previste dalla Misura #22 del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026* in relazione all'uso della crittografia fin dalla fase di progettazione di reti, applicazioni e servizi.

Con l'obiettivo di disporre di un quadro informativo il più possibile completo e accessibile, appare opportuno che i *policy makers* siano sufficientemente informati e consapevoli di tutti profili relativi a questo tema e alle attività già in corso.

Andrebbe, valutata l'opportunità di svolgere un'indagine conoscitiva in sede parlamentare e in altra sede deputata più consona, che potrebbe servire ad approfondire la tematica grazie alle audizioni di esperti, tecnici e aziende e fare insieme il punto della situazione, del contesto tecnologico e industriale e delineare le prospettive del settore.

9. Conclusioni

Le tecnologie quantistiche stanno diventando disponibili e permetteranno di realizzare scenari ad oggi soltanto ipotizzabili.

Se da una parte le tecnologie quantistiche, come il *quantum computing*, oltre a rappresentare una potenzialità possono costituire una minaccia alla sicurezza dei dati e delle comunicazioni, altre tecnologie quali la QKD e la QRNG forniscono gli strumenti per realizzare sistemi incondizionatamente sicuri, per i quali il livello di sicurezza non dipende dalla capacità computazionale del potenziale "avversario".

La letteratura dei progetti internazionali di innovazione fornisce un'ampia gamma di esempi di casi d'uso che riguardano la fornitura di servizi di sicurezza quantistica per reti ottiche e 5G: servizi QKD per banche, ministeri, agenzie governative, enti sanitari che richiedono un elevato livello di sicurezza nello scambio di dati ed informazioni altamente riservate tra sedi, nonché l'industria manifatturiera e di processo (Industry 4.0), tenendo conto dei requisiti specifici del contesto industriale. Inoltre, il settore della logistica sta aumentando di importanza: connessioni sicure e certificate verso i porti e gli interporti diventano sempre più essenziali.

L'Italia ha già posto in essere una serie di progetti per la realizzazione di una vera e propria filiera nazionale per le tecnologie quantistiche. Lo sviluppo e la messa in campo delle tecnologie quantistiche richiedono importanti investimenti ed è necessario attuare un'opera diffusa di educazione e formazione alla sicurezza informatica.

Questi sono i principali motivi per i quali al momento non è semplice ipotizzare previsioni su valore e andamento del mercato connesso alle iniziative industriali in questo campo.

Tuttavia, attendere che le condizioni di mercato siano mature significherebbe non posizionarsi all'interno di questi mercati in favore di altri attori che nel frattempo avranno investito e sviluppato tecnologie e competenze.

Per questo, l'industria ICT e digitale operante in Italia e il mondo della ricerca (CNR, Università, Politecnici) ritengono fondamentale rafforzare la collaborazione pubblico-privata per potere intensificare i progetti di sviluppo tecnologico e arrivare così a disporre di un adeguato livello di autonomia strategica nel settore che consenta di garantire la sicurezza digitale del Paese.