Sicurezza Quantistica: L'uso delle Quantum Key Distribution su scala nazionale

Quantum Security: The use of Quantum Key Distributions on a national scale.

Francesco Matera ♦

♦ *Fondazione Ugo Bordoni*

Sommario

Questo articolo descrive uno studio sull'introduzione di sistemi di trasmissione che possiedono una gestione della sicurezza basata sulla meccanica quantistica, mediante le *Quantum Key Distribution (QKD),* nelle infrastrutture di telecomunicazione in fibra ottica già esistenti. In particolare, sono analizzate le soluzioni e le prestazioni in ciascun segmento di rete per definire percorsi fisici end-to-end QKD, da sorgente a destinazione, e compatibili con il concetto di partizione della rete, detto *slicing,* definito nelle architetture delle nuove reti 5G. E' riportata una analisi dei costi per l'introduzione delle QKD in ogni segmento di rete con particolari dettagli per i costi necessari per una rete di telecomunicazione italiana, sicura dal punto di vista quantistico.

Abstract

This article describes a study on the introduction of transmission links that have a security management based on quantum mechanics, through Quantum Key Distribution (QKD), in existing fibre optic telecommunication infrastructures. In particular, the solutions and performances in each network segment are analysed to define end-to-end QKD physical paths from source to destination, and compatible with the concept of network partition, called slicing, defined in the architectures of the new 5G networks. An analysis of the costs for the introduction of QKDs in each network segment is reported with particular details for an Italian telecommunications network, secure from a quantum point of view.

Keywords: QKD, WDM, Access, FSO, 5G, slicing

1. Introduzione

Le tecniche quantistiche stanno uscendo dai laboratori per essere utilizzate in diversi contesti, e in termini di sicurezza il quantum computing potrebbe rendere obsoleti gli attuali algoritmi crittografici, mettendo a rischio la protezione dei dati e delle comunicazioni. Questo aspetto sta portando ad un'accelerazione per l'adozione di contromisure, soprattutto per proteggere dati e infrastrutture critiche. Oggi, è ampiamente riconosciuto che è fondamentale iniziare a pensare ad infrastrutture di sicurezza a prova di futuro e sviluppare un piano di gestione del rischio basato su un approccio quantistico il prima possibile.

Va sottolineato che nel campo degli studi sull'uso degli effetti quantistici nei dispositivi per la commutazione l'Istituto Superiore delle Tecnologie delle Comunicazioni e dell'Informazione, ora Direzione Generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (DGTCSI - ISCTI), è stato uno dei primi centri di ricerca che già più di trenta anni fa, in collaborazione con la Fondazione Ugo Bordoni, aveva sperimentato specifiche tecniche come mostrato nel lavoro [1] che riguardava il trasferimento del momento angolare.

Attualmente, le Quantum Key Distribution (QKD) sono riconosciute come una delle più importanti metodologie di comunicazione quantistica sicura [2-5] e adottano un canale fotonico per crittografare le informazioni attraverso i principi della meccanica quantistica. I sistemi QKD sono già operativi in diversi contesti, permettendo anche collegamenti su lunghe distanze in configurazioni Point to Point (P2P) [6-10].

Inoltre, è stata ampiamente dimostrata la possibilità di far coesistere nella stessa fibra ottica canali quantistici e canali classici, mostrando così la possibilità di realizzare reti ibride senza la necessità di installare nuove fibre [11-14]. Tuttavia, rispetto ai sistemi classici devono essere prese alcune precauzioni, a cominciare dalla necessità di sostituire gli amplificatori ottici per la compensazione delle perdite nelle fibre ottiche, in quanto nel caso dei canali quantistici il rumore ASE, emesso da tali amplificatori, avrebbe un effetto devastante, e, al momento, deve ancora essere dimostrata la possibilità di adottare ripetitori quantistici in reti QKD [4]. Fortunatamente, la trasmissione di informazioni quantistiche sicure su lunga distanza può essere ottenuta suddividendo la tratta complessiva in segmenti, ognuno gestito con un apparato QKD, realizzando così dei nodi intermedi denominati Trusted Repeater Nodes (TRN) [3-4]. I TRN possono essere situati negli stessi luoghi degli amplificatori ottici, ed è infatti questa la soluzione adottata ad esempio nel collegamento tra Pechino e Shanghai [3].

Oggi i sistemi QKD operano anche nel segmento delle reti di acceso, in collegamenti Point-to-Point (P2P), ma anche in architetture Gigabit Passive Optical Networks (GPON) [15], in collegamenti ottici nello spazio libero (Free Space Optical communication, FSO) [16] e recentemente anche in fibre multimode e multicore [17].

Tuttavia, per la loro completa introduzione, in tutta la rete di telecomunicazioni, dall'area di accesso a quella core, sono ancora necessari diversi passaggi tecnologici. Nonostante queste difficoltà, ci sono già molte proposte per includere le tecniche QKD in vaste aree geografiche

arrivando a gestire le risorse di tipo quantistiche [18], adottando approcci di Software Defining Network (SDN) [19-20] e operando con partizioni di tipo slice definite nel contesto delle reti 5G [21-22].

In questo articolo, per ogni segmento di rete, sono descritte le problematiche tecniche associate con l'adozione di una sicurezza quantistica basata su QKD al fine di poter definire percorsi QKD end-to-end che, compatibilmente con le nuove architetture sviluppate per le infrastrutture 5G, possano essere etichettati come una sorta di Quantum Slice. Il principale obiettivo di questo lavoro è l'analisi dei costi che sarebbe necessario sostenere per introdurre, in una rete che copra le principali città di un Paese come l'Italia sfruttando le infrastrutture già esistenti, un set minimo di dispositivi QKD per attuare un approccio di sicurezza quantistica.

2. Breve panoramica sulle QKD operanti nelle reti esistenti.

Sperimentazioni in tutto il mondo confermano l'efficacia della crittografia quantistica; tra questi possono essere citati gli esempi di Vienna [6], Tokyo [7], Firenze [8], Cambridge [9], nonché di particolare rilevanza il caso cinese tra Pechino e Shanghai [3]. Inoltre, la regolamentazione su QKD è studiata negli organismi ITU ed ETSI (ETSI ISG-QKD) ed un grande interesse per questa tecnologia è anche mostrato dalle Telco con le iniziative nel 3GPP per le reti 5G [22]. Le QKD sfruttano un canale quantistico solo per produrre e distribuire chiavi per crittografare (e de-crittografare) un messaggio scambiato su un canale classico di comunicazione [2].

Le basi ed i protocolli di questa procedura di sicurezza si possono trovare in letteratura [4] e come riferimento il protocollo più noto è quello BB84. Nonostante il notevole interesse su questo tema, è ancora presente un certo scetticismo principalmente perché questi sistemi funzionano con potenze molto basse, e quindi qualsiasi fonte di perdite e/o di rumore (classico e quantistico) degrada fortemente le loro prestazioni: come conseguenza il bit rate consentito dalle QKD per la trasmissione della chiave (key rate) è estremamente inferiore ai tradizionali sistemi di trasmissione ottica. In pratica, partendo dalla generazione di una sequenza di impulsi, solo un numero estremamente limitato di essi può essere effettivamente utilizzato per la trasmissione QKD, con una key rate che risulta essere molto inferiore alla frequenza degli impulsi generati e che si abbassa sempre di più all'aumentare delle perdite subite durante il percorso del segnale [3-5]. Inoltre, sono necessari diversi minuti prima che la sincronizzazione possa consentire al sistema QKD di funzionare nelle migliori condizioni [16]. Molti sforzi sono ancora necessari per aumentare la key rate, ma anche la massima distanza di propagazione, e quindi rendere i sistemi QKD economici, compatti e robusti.

I sistemi QKD possono coesistere con un intenso traffico dati nella stessa fibra [9-13], tramite la tecnologia Wavelength Division Multiplexing (WDM), eliminando così la necessità di usare fibre dedicate, non solo costose ma spesso anche non disponibili. Pertanto, il backbone QKD-over-WDM è diventato una soluzione promettente e fattibile per le future reti quantistiche. Attualmente si suppone che una trasmissione WDM quantistica adotti tre diversi tipi di canali [17]: il *Measuring Base Channel* (MBCh), il *Traditional Data Channel* (TDCh) e il *Quantum*

Key Channel (QKCh). In particolare, l'MBCh è il canale pubblico che trasmette segnali classici ed ha il compito di trasportare la sequenza della base di misurazione selezionata e le informazioni per la correzione degli errori, il QKCh è il canale che trasmette i segnali quantistici ed i TDCh sono i classici canali che trasportano l'informazione ad alto bit rate.

Occorre comunque sottolineare che devono essere prese delle importanti precauzioni per la coesistenza tra canali quantistici e canali classici, anche per limitare le degradazioni dovute agli effetti non lineari della fibra; in particolare, lo scattering Raman [22] e gli effetti di missaggio a quattro onde (FWM) [4] indotti da MBCh e TDCh, che possono degradare le prestazioni nella trasmissione del QKCh.

I canali quantistici devono essere conformi ad un sistema DWDM commerciale, ad es. 40 lunghezze d'onda (con spaziatura dei canali a 100 GHz) o 80 lunghezze d'onda (con spaziatura dei canali a 50 GHz). Pertanto, il problema dell'allocazione della lunghezza d'onda per i tre tipi di canali deve essere considerato nelle reti ottiche abilitate al QKD. In alcuni lavori, per ottenere un isolamento appropriato dalla comunicazione dei dati, si alloca il QKCh nella banda O (1260–1360 nm) [17], mentre, nei sistemi DWDM commerciali, il TDCh si trova solitamente nella banda C (1530–1565 nm). Tuttavia, occorre osservare che nella banda O ci sono livelli di perdite più alti rispetto alla banda C, il che limita la velocità di trasmissione e la massima distanza raggiungibile. Di conseguenza, i tre canali possono essere allocati in banda C per garantire le migliori prestazioni di trasmissione. Inoltre, il posizionamento del QKCh in banda C può limitare gli effetti dovuti allo scattering Raman [22]. Pertanto, le lunghezze d'onda assegnabili per i QKCh possono iniziare da 1530 nm, e inoltre una spaziatura di 200 GHz può essere adottata come banda di guardia tra QKCh e gli altri canali classici per ridurre al minimo gli effetti di miscelazione a quattro onde (FWM). Il MBCh, che trasporta i segnali classici per la conferma della chiave segreta utilizzata, può condividere lunghezze d'onda nella banda C [16].

Per i collegamenti su lunga distanza con tecnologia QKD sarebbe necessario una sorta di ripetitore quantistico. Sfortunatamente i ripetitori quantistici non sono ancora fattibili con l'attuale tecnologia ed, al momento, una soluzione interessante per trasmettere segnali QKD su lunghe e lunghissime distanze si basa sull'introduzione di ripetitori che gestiscono i QKD come sistemi indipendenti [3], mentre MBch e TDCh sono otticamente amplificati da EDFA.

Diverse architetture di reti di accesso, basate sulla propagazione ottica, possono sfruttare le proprietà delle QKD ed in questo contesto le reti GPON appaiono molto attraenti, anche se le perdite dovute allo splitter riducono il numero di utenti QKD [14]. *QKD over FSO* [15] è un altro modo per sfruttare la propagazione ottica per la sicurezza quantistica evitando l'installazione della fibra; questo approccio risulta quindi essere molto interessante per l'introduzione del QKD sia nel segmento di accesso sia per il backhauling, e.g.: per connettere le terminazioni di apparati radio con le BaseBand Unit (BBU). Tornando al segmento core, sarà fondamentale la gestione delle varie lunghezze d'onda con l'ottimizzazione dello spettro WDM come mostrato ad esempio in [17-18]. Nonostante gli aspetti complessi sopra citati, l'importanza di queste tecnologie è testimoniata anche dall'interesse ad essere incluse nelle

nuove architetture e gestioni di rete basate sulle Software Defined Networking (SDN) come descritto ad esempio in [19-21]. Ad esempio, è dimostrato [16] che il monitoraggio in tempo reale dei parametri quantistici fornisce informazioni al controller SDN per proteggere i percorsi della luce nella rete ottica, con configurazioni dei percorsi ottici flessibili per garantire la distribuzione delle chiavi quantistiche anche in caso di attacchi. Inoltre, l'uso di QKD nel contesto delle Network Function Virtualization (NFV) è stato anche studiato con diverse dimostrazioni per verificare l'applicazione di approcci di crittografia utilizzando chiavi quantistiche per rendere sicure alcune funzioni NFV [18]. Sulla base dei progressi ottenuti sulle tecnologie QKD e sulla loro applicazione principalmente nei contesti relativi alle soluzioni SDN e NFV, l'uso di QKD sembrerebbe avere ora un ruolo molto importante anche per realizzare interconnessioni sicure all'interno del framework 5G [22].

3. Infrastrutture di reti basate su QKD

Seguendo le considerazioni descritte nella Sez. 2, e facendo riferimento al lavoro [23], la Fig. 1 illustra un esempio di rete completa che utilizza sistemi QKD sia nelle componenti di core sia in quelle di accesso (comprensive anche dei raccordi verso le antenne di accesso radio). Nell'area core (area gialla), ciascun nodo finale è costituito da un Quantum Backbone Node (QBN), equipaggiato con un ricevitore e trasmettitore QKD [4], che può funzionare sia come sorgente sia come destinazione; lungo il collegamento, che può essere anche di centinaia di km, un nodo di transito può operare come Trusted Repeater (TR) e ogni TR ha un trasmettitore e un ricevitore QKD. Per consentire ai canali QKCh, MBCh e TDCh di coesistere nella stessa fibra, nella fig. 1 è considerato uno schema di bypass EDFA che consente al QKCh di non passare attraverso gli EDFA, utilizzando speciali componenti come multiplexer e demultiplexer per separare il canale QKCh dai canali MBCh e TDCh, il che risulta necessario per evitare il rumore ASE degli EDFA.

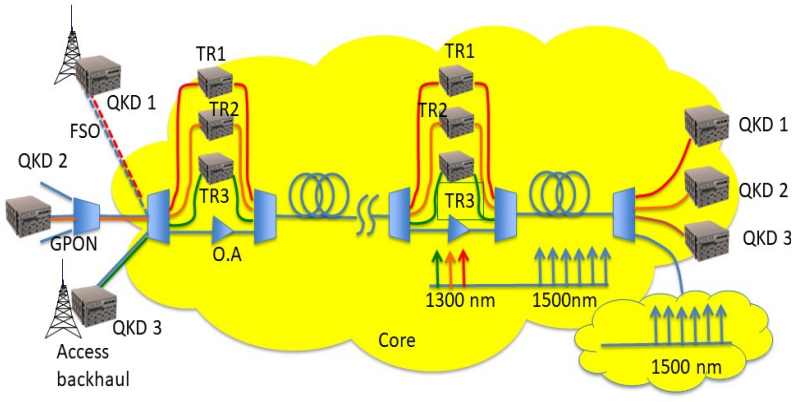

Figura 1 - *Esempio di una rete completa che utilizza le QKD. [23].*

Nell'area core si ipotizzano collegamenti costituiti da N tratte in fibra ottica lunghe 80 km che collegano i nodi di transito. Il core è collegato sia ai terminali QKD sia alle infrastrutture di

accesso/backhaul/ fronthaul, dove possono essere localizzati terminali QKD, sfruttando specifici canali ottici da adottare per la trasmissione quantistica, ed utilizzando sia fibre ottiche dedicate, sia canali WDM in infrastrutture in fibra condivisa come nel caso delle reti GPON o dei collegamenti FSO. I canali quantistici possono essere usati anche in fibre Multimodo e Multicore [17].

Come esempio tipico consideriamo il caso di fibre ottiche operanti a 1550 nm, in cui le perdite sono di circa 0,2 dB/ km; ricordando che i sistemi QKD possono funzionare con perdite massime fino a 30 dB [4] significa che il limite pratico per la massima distanza è di circa 150 km . Tuttavia, andare a questa distanza comporta anche un output con un key rate fortemente ridotto. Dai risultati riportati in [4-5] si può affermare che due sono i regimi di propagazione che si possono adottare per i QKCh, assumendo una lunghezza della fibra di 80 km; infatti oltre alla lunghezza d'onda a 1550 nm (banda C), in cui si può operare con un key rate di 0,5 Mb/s, si può utilizzare anche la banda a 1300 nm (banda O), che presenta però una attenuazione più alta, e come conseguenza un più basso key rate pari a 0,25 Mb/s. Per il segmento di accesso, nel caso di infrastrutture GPON la limitazione principale è data dalla "splitting loss" e quindi, nel caso di 32 ONU, la key rate può essere dell'ordine di 0,5 Mb/s [14]. Dettagli specifici per i canali quantistici nelle infrastrutture GPON, anche per limitare le perdite dovute allo splitter, possono essere trovati in [14]. Un key rate più elevato potrebbe essere ottenuto nei collegamenti P2P e nelle soluzioni FSO a causa delle minori distanze in gioco. Ipotizzando di operare con percorsi slice a partire dal segmento di accesso/backhaul, e attraversando l'intera rete core, la velocità massima deve essere fissata a 0,25 Mb/s e 0,5 Mb/s rispettivamente per le bande O e C.

4. Analisi dei costi per sistemi QKD nelle reti attuali

Scopo di questo paragrafo è fornire alcune informazioni sui costi per l'introduzione di un approccio sulla sicurezza basato sulle QKD nelle reti attuali, anche se i dati disponibili sui costi dei dispositivi sono molto pochi e l'unico riferimento completo è riportato nella tabella 1 di [4] e solo per reti dorsali. L'introduzione dei canali QKD nei collegamenti WDM richiede costi aggiuntivi piuttosto elevati a causa, oltre che di apparati QKD, anche per l'introduzione di ulteriori dispositivi come i filtri ottici [4]. Con riferimento alla fig. 1, per ogni collegamento QKD punto-punto il costo aggiuntivo è composto dai seguenti quattro principali contributi: C_Q è il costo relativo ai ricetrasmettitori QKD supposti uguali in tutti i nodi della rete (che operano come sorgente e destinazione), C_B è il costo legato alle apparecchiature ausiliarie per gli apparati sorgente e destinazione e C_T è il costo per le apparecchiature ausiliarie relative ad ogni TRN; inoltre è incluso anche un costo C_W per l'occupazione spettrale del canale QKD nel collegamento WDM.

Seguendo la tabella dei costi di [4] e assumendo valori medi, sono state considerate le seguenti assunzioni per i costi: C_Q = 25k €, C_B = 20k €, C_T = 12,5k € e C_W = 6,5 €/km. Il costo totale per un collegamento QKD nell'area core è quindi [4]:

$$C_T = C_Q N_a + C_B N_B + C_T N'_a + C_W L_a \quad (1)$$

dove N_a è il numero totale di ricetrasmettitori QKD, N_B è il numero totale di nodi endpoint, N'_a è il numero totale dei TR e L_a è la lunghezza totale del collegamento. Analizzando i costi relativi alle reti di accesso (anche per raggiungere apparati BBU), il contributo principale è dovuto al trasmettitore e al ricevitore nel caso di soluzioni P2P e FSO, mentre nel caso di soluzioni PON, dobbiamo distinguere se l'infrastruttura di riferimento è GPON o WDM-PON, poiché la soluzione WDM-PON ha già i filtri richiesti che devono essere invece aggiunti nella GPON. In moderni sistemi WDM-PON, la funzione di demultiplexing può essere realizzata da un reticolo a guida d'onda (WGR) [24] che, come riportato in [24], ha un costo di circa 20k € per un WGR 32x. Per quanto riguarda l'FSO, si può considerare un costo inferiore per l'infrastruttura senza fibra ottica, grazie a un apparato end-to-end più semplice.

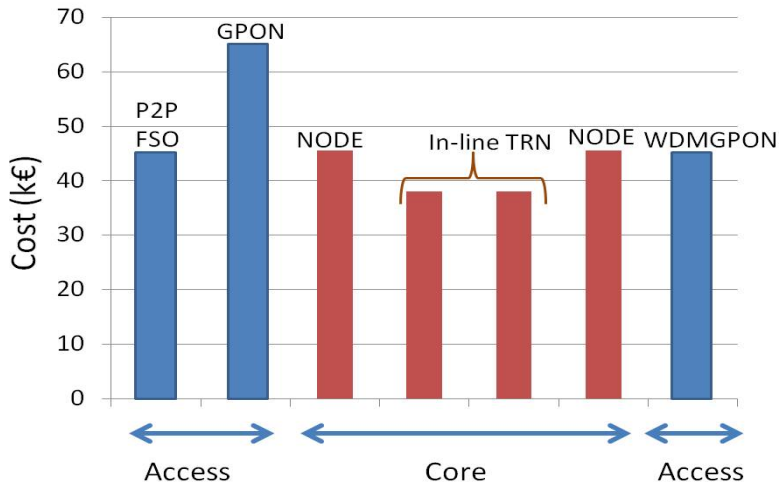

Figura 2 - *I costi in ciascun segmento della rete*

Nella fig. 2, per ogni segmento di rete, è illustrato il dettaglio dei costi tipici per l'introduzione delle QKD in un ambiente End-to-End (E2E). Da ciò deriva che un collegamento QKD E2E lungo 800 km, compresi gli accessi P2P, richiede un costo aggiuntivo di circa 561k €, che è piuttosto elevato, ma va confrontato con il costo di un apparato ottico classico (e.g.: lo switch ottico 128x128 con porte da 10 Gb/s ha un costo di circa 500k € con 41k € per l'interfaccia da 10 Gb/s) [25].

5. Un esempio per l'introduzione delle QKD in Italia.

Come esempio, per l'introduzione di un approccio di sicurezza QKD in una rete nazionale completa, si ipotizza il caso Italia supponendo di considerare un numero di nodi pari a 17, rappresentativi delle principali città, con i 16 link riportati nel riquadro di fig. 3 (parte sinistra). Nella figura 3 (parte destra), le barre blu riportano i costi totali di ogni collegamento. Il risultato

principale di tale analisi è che per realizzare una connessione sicura quantistica completa relativa all'Italia basata sulla topologia illustrata in fig. 3 è necessario un investimento di circa 3M€.

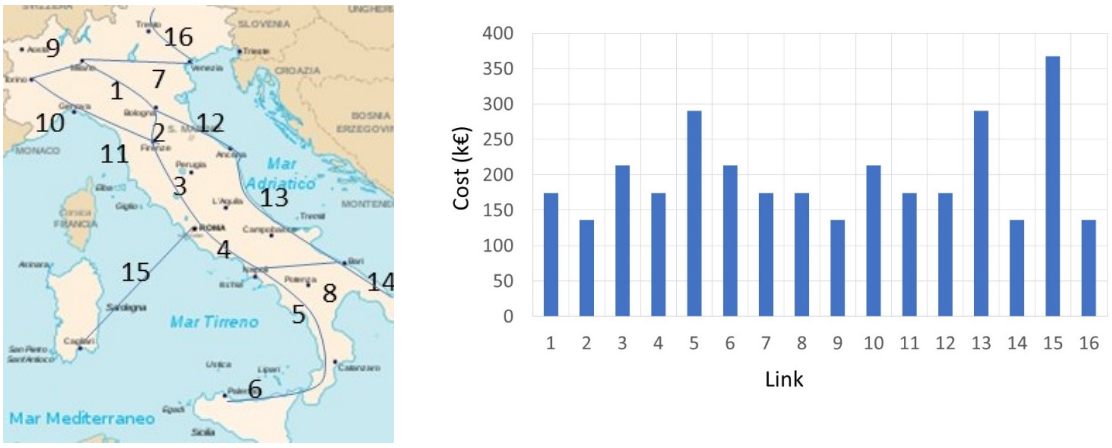

Figura 3 - *Collegamenti tra le principali città italiane in cui si suppone l'introduzione di sistemi QKD. A sinistra i collegamenti sono numerati da 1 a 16. A destra i relativi costi complessivi degli apparati QKD per ciascun link.*

Tuttavia, per avere una comunicazione QKD efficace tra tutti i nodi della rete italiana è necessaria un'architettura che tenga conto di tutte le possibili richieste QKD da qualsiasi sorgente a qualsiasi destinazione, e ciò significa avere molti più collegamenti QKD tra nodi che possono essere anche molto distanti l'uno dall'altro.

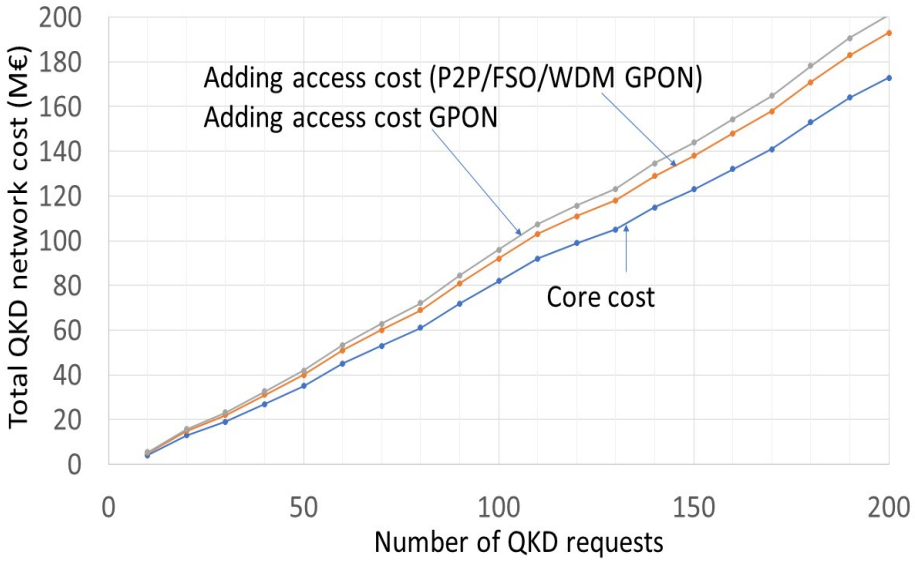

Figura 4 - *Costi totali per una rete QKD italiana in funzione delle richieste per connessioni QKD*

Per avere un'idea degli investimenti necessari per supportare tutte le diverse richieste QKD, che possono venire dai 17 nodi, è stata effettuata un'analisi dei costi calcolando il valore di ogni collegamento tra due nodi scelti casualmente tra quelli riportati in fig. 3, e ipotizzando richieste QKD che vanno da 10 a 200 come riportato in fig. 4. Tale intervallo è stato scelto poiché in questa rete con V = 17 nodi, tutte le connessioni possibili sono V * (V-1) / 2 = 136, inclusi alcuni collegamenti molto lunghi. Inoltre, alcune coppie di nodi, per origine e destinazione, potrebbero richiedere più connessioni QKD o key rate più elevati, che è anche equivalente a più lunghezze d'onda QKCh. I percorsi tra i nodi sono calcolati dall'algoritmo del percorso più breve di Dijkstra [4] e applicando la relazione 1 si valutano i costi complessivi come riportato in fig. 4 distinguendo i casi della sola rete core e quelli comprendenti i costi aggiuntivi per la parte di accesso supponendo sia l'accesso basato su P2P/FSO/WDM-GPON sia l'accesso su GPON. L'aumento dei costi è pressoché lineare con alcune piccole variazioni di pendenza dovute principalmente alla diversa lunghezza del collegamento preso in considerazione. Tali costi potrebbero anche essere ridotti introducendo alcune strategie nella scelta dei percorsi come descritto in [4] per condividere alcune risorse di rete.

6. Conclusioni

Questo lavoro ha riportato uno studio sulla fattibilità di una rete operante con un approccio di sicurezza basato sulla tecnologia QKD, collegando le principali città d'Italia, e includendo anche il segmento di accesso fino all'antenna radio e consentendo di definire dei percorsi *slice* di tipo quantistico per essere gestiti in un framework 5G. I risultati mostrano la necessità di ampi investimenti che, però, rientrano in quelli necessari per la realizzazione di nuove reti. E'

anche vero che questo passo appare necessario visto ciò che stanno facendo altri Paesi nei prossimi anni sui temi della sicurezza quantistica.

Ringraziamenti.

Si ringrazia la Direzione Generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (DGTCSI - ISCTI) per il supporto a questa attività e la Dott.ssa Marina Settembre per il supporto teorico sulle tematiche quantistiche e sulla sicurezza nelle reti.

Riferimenti bibliografici

[1] A. Santamato, M. Settembre, M. Romagnoli, B. Daino, Y. Shen, "Self-Induced Stimulated Light Scattering" Physical Review Letters vol. 61, 113 (1988).
[2] E. Diamanti et al, Nature Partner Journal **2**, 16025 (2016)
[3] Q. Zhang, F.Xu, Y. Chen, C. Peng, J. Pan, Optics Express **26**, (2018).
[4] Y. Cao et al, J. Opt. Comm. Netw. 285-298 **11** (2019).
[5] P. Eraerds, et al, New J. Phys., **12** 063027 (2010)
[6] M. Peev et al.," New J. Physics, **11**, (2009)
[7] M. Sasaki et al., Opt. Express **19**, 10 387 (2011)
[8] D. Bacco et al., EPG Quantum Technology (2019)
[9] A. Wonfor et al, Int. Conf. Quantum Cryptography, 1–3 (2017).
[10] T. A. Eriksson et al., Commun. Physics **2**, (2019)
[11] R. Lin et al, in Proc. ECOC 2018
[12] L. J. Wang, et al, Appl. Phys. Lett., **106**, 081108 (2015)
[13] N. A. Peters, et al, New J. Phys., **11**, (2009)
[14] S. Aleksic , et al, 18th NOC-OC&I (2013).
[15] P. V. Trinh , et al IEEE Access **6,** 4159-4175 (2018)
[16] E. Hugues-Salas, et al, J. Opt. Commun. Netw. **11**, A209–A218 (2019)
[17] Y. Cao, et al, J. of Opt. Comm. and Networking **9**, 995-1004 (2017).
[18] Y. Zhao et al., IEEE Commun. Mag. **56**, 130–137 (2018)
[19] A. Aguado et al, J. Lightw. Technol., **35**, 1357–1362 (2017)
[20] R. Wang et al , J. Lightw. Technol. **38**, 139-140 (2020)
[21] Jin Cao , et al , IEEE Communication & Tutorials, **22**, 170-195 (2020),
[22] H. Kawahara, A. Medhipour, and K. Inoue, Opt. Commun., **284**, 691–696 (2011).
[23] F. Matera, "Quantum Key Distribution in Optical Networks" IEEE ICOP 2020.
[24] G. Maier et al J. of Lightwave Techn., **18**, 125-143 (2000)
[25] S. Sengupta et al IEEE Commun. Mag. **41**, 60-70 (2003).