Quantum Key Distribution per la sicurezza delle tecnologie quantistiche: la sperimentazione PD-QTech

GARR e l'Università di Padova stanno studiando le applicazioni pratiche della Quantum Key Distribution sulle reti della ricerca. L'obiettivo è¨ definire tecniche, strumenti e buone pratiche per utilizzare l'infrastruttura ottica GARR nella distribuzione agli utenti di chiavi crittografiche quantistiche

Pubblicato il 17 lug 2023

Paolo Bolletta
Chief Optical Engineer GARR
Matteo Colantonio
Optical Innovation Engineer GARR

Già da diversi anni, la sicurezza è¨ considerata una delle killer application delle tecnologie quantistiche e, per alcuni aspetti è¨ senz'altro una delle più¹ mature. Questo non vuol dire però² che tutte le soluzioni siano già oggi chiavi in mano: al contrario, si tratta di un campo in cui c'è¨ ancora molta ricerca e sviluppo da fare e le sperimentazioni di questa tecnologia sono numerose sia nell'ambito della comunità della ricerca che altrove.

Quantum computing, una svolta per la ricerca: lo scenario europeo e i progetti in corso

Tra le attività in corso, c'è¨ anche una sperimentazione congiunta tra GARR e gli esperti di tecnologie quantistiche dell'Università di Padova (il team di ricerca PD-QTech di Paolo Villoresi) che sta studiando le applicazioni pratiche della QKD sulle reti della ricerca con dei primi risultati molto interessanti.

Indice degli argomenti

Cos'è¨ la Quantum Key DistributionObiettivi della sperimentazione PD-QTechControllo e la gestione di un sistema di QKD

Cos'è¨ la Quantum Key Distribution

QKD, acronimo di Quantum Key Distribution, è¨ una tecnica di crittografia che utilizza le proprietà della fisica quantistica per distribuire segreti (in particolare chiavi crittografiche simmetriche) in maniera intrinsecamente sicura. Il problema degli algoritmi tradizionali utilizzati per lo scambio di chiavi crittografiche è¨ infatti che non esiste una garanzia formale della loro sicurezza: in pratica, cioè¨, non sono intrinsecamente sicuri ma semplicemente confidano nel fatto di essere così¬ complicati da rendere troppo lunghi e costosi gli sforzi di un malintenzionato che voglia decifrare il codice. Questo significa che anche se oggi sono a tutti i fini pratici impenetrabili, con l'avvento dei computer quantistici, una maggiore disponibilità di risorse di calcolo e di nuovi algoritmi, diventeranno vulnerabili in futuro, esponendo anche vecchi dati che fino a quel momento erano in sicurezza. In pratica, la storia della crittografia tradizionale può² essere vista come una continua rincorsa tra la realizzazione di algoritmi di cifratura e di decifrazione sempre più¹ raffinati.

In questo scenario, la crittografia quantistica non è¨ un miglioramento ma una rivoluzione completa perché© offre una sicurezza incondizionata: sono le stesse leggi della fisica a garantire l'impenetrabilità del sistema anche rispetto ai possibili sviluppi futuri in termini di nuovi algoritmi e tecnologie. Come si può² immaginare, questa caratteristica di intrinseca sicurezza – un esempio da manuale di quello che si intende con "game changer" - ha spinto moltissimo la ricerca in questo settore, permettendo lo sviluppo di nuovi schemi e tecnologie e oggi i primi prototipi sono già disponibili sul mercato.

Tuttavia, anche se le prime applicazioni già esistono e promettono di essere invulnerabili agli attacchi presenti e futuri, ci sono una serie di sfide tecnologiche ancora tutte da affrontare, in particolare in relazione a come integrare questa tecnologia con le infrastrutture di telecomunicazione esistenti. Inoltre pur essendo estremamente promettente, la QKD è¨ una tecnologia nuova e ancora in fase di sviluppo, quindi ne vanno ancora approfonditi i casi d'uso, per la comunità della ricerca e dell'istruzione ma non solo.

Obiettivi della sperimentazione PD-QTech

L'obiettivo della sperimentazione che GARR sta conducendo con l'Università di Padova è¨ definire delle opportune tecniche, strumenti e buone pratiche per utilizzare l'infrastruttura ottica GARR nella distribuzione agli utenti di chiavi crittografiche quantistiche: esse sarebbero trasportate insieme alle altre tipologie di dati, eventualmente crittografati con queste stesse chiavi. Il gruppo di ricerca dell'Università di Padova è¨ inoltre interessato a individuare e studiare casi d'utilizzo per la tecnologia che si sta sviluppando e che potrebbe presto trasformarsi in un servizio: proprio come spin-off di questa attività di ricerca e sviluppo è¨ infatti nata una startup.

Per GARR, l'obiettivo principale è¨ comprendere se sia possibile distribuire le chiavi quantistiche utilizzando le fibre già usate per il trasporto dati e quale potrebbe essere l'impatto di un servizio di questo genere sul traffico IP.

All'interno della collaborazione, PD-QTech si occupa di realizzare e gestire il sistema di scambio delle chiavi, dopo aver

Quantum Key Distribution per la sicurezza delle tecnologie quantistiche: la sperimentazione PD-QTech

validato in laboratorio l'hardware e le configurazioni necessarie. L'Università di Padova ha inoltre reso disponibili le fibre spente e le loro connessioni nei nodi della rete GARR presso l'Ateneo.
GARR ha poi realizzato l'ambiente di test, collegando due router nei due nodi di Padova con ottiche a 10 Gbps, di solito utilizzate per l'accesso da parte degli utenti alla rete. Su questa coppia di fibre sono stati poi collegati anche gli apparati QKD dell'Università attraverso la multiplazione in frequenza del segnale classico e di quello quantistico.
Dal punto di vista della rete, gli elementi che entrano in gioco nella sperimentazione sono interfacce e nodi IP/MPLS della dorsale GARR utilizzati per il trasporto dati IP.
? stato inoltre messo a disposizione anche il laboratorio ottico GARR (GOAL – GARR Optical Automation Lab), per testare setup specifici di interesse della collaborazione.
Questo setup permetterà di verificare l'applicabilità delle tecniche di QKD studiate a un contesto di rete di trasporto di produzione ("Brown-Field") attraverso la sperimentazione in laboratorio e in field trial circoscritti. In particolare, vengono studiati gli impatti in termini di performance e operativi che deriverebbero dalla coesistenza di un nuovo canale quantistico per la QKD con il canale classico di trasporto dei dati.
Controllo e la gestione di un sistema di QKD
Un altro aspetto molto importante per passare dalla sperimentazione a un servizio di produzione sarà la definizione e realizzazione di prototipi per il controllo e la gestione di un sistema di QKD. In futuro, su questa infrastruttura di test sarà anche possibile andare a definire protocolli per lo scambio di dati crittografati usando le chiavi quantistiche e sperimentarli sul campo.
Insomma, possiamo dire che oggi con questa sperimentazione abbiamo la possibilità di porre le basi per nuovi utilizzi dell'infrastruttura in fibra della rete GARR-T che vanno al di là del classico trasporto dati: come già con altri servizi sperimentali, come ad esempio il lavoro fatto in collaborazione con INRIM sull'utilizzo delle reti in fibra ottica per la distribuzione di segnali di tempo e frequenza, l'utilizzo innovativo della rete ottica promette di offrire un alto valore aggiunto alla comunità dell'università e della ricerca. Non è¨ un caso che questo lavoro stia suscitando interesse a livello internazionale: i risultati della sperimentazione sono stati presentati alla comunità internazionale delle reti della ricerca all'evento TNC23 che si è¨ svolto a giugno a Tirana.

Valuta la qualità di questo articolo