Abstract

Ilaria Vagniluca

October 9, 2018

La distribuzione quantistica delle chiavi (QKD) è l'unica tecnica in grado di garantire, in linea di principio, la sicurezza incondizionata nella protezione di dati e informazioni private. Alla base della QKD vi è l'indeterminazione associata, inevitabilmente, alle misure eseguite su singoli oggetti quantistici (stati quantistici della luce), sui quali viene codificata la chiave crittografica. Ciò rende tale tecnica immune dall'avanzamento tecnologico, al contrario dei metodi di crittografia standard attualmente in uso.

Tra le varie tecnologie quantistiche, la QKD è oggi quella in stato più avanzato, sia dal punto di vista teorico che sperimentale. Negli ultimi anni sono stati sviluppati nuovi protocolli, capaci di resistere a sempre più svariate tipologie di attacco; sono state dimostrate trasmissioni di segnali quantistici su lunga distanza, anche grazie all'impiego di un satellite come nodo intermedio; nel frattempo dispositivi e soluzioni basati su QKD si stanno sempre più diffondendo in commercio. Una delle sfide di oggi è sicuramente quella di riuscire a integrare la sicurezza dei protocolli di QKD con le telecomunicazioni classiche su larga scala. In particolare si cercano nuove soluzioni e protocolli in grado di inserirsi nelle infrastrutture già esistenti, come le reti in fibra ottica attualmente impiegate nelle telecomunicazioni.

I protocolli con codifica a variabili continue (CV-QKD) sono certamente i più compatibili con le infrastrutture esistenti, poiché necessitano solamente di dispositivi già largamente impiegati nel campo delle telecomunicazioni ottiche. Nei protocolli di CV-QKD l'informazione è codificata nella quadratura del campo elettrico di impulsi laser molto attenuati (stati coerenti) e viene estratta per mezzo della rivelazione omodina.

Durante questo lavoro di tesi ho realizzato le stazioni di trasmissione e di ricezione costituenti un sistema di CV-QKD. L'apparato è totalmente integrato in fibra ottica a singolo modo, lavora a 1550 nm ed è composto da dispositivi commerciali già largamente impiegati nel campo delle telecomunicazioni. Una volta messo a punto il setup sperimentale, ne ho caratterizzato il funzionamento. Ho quindi testato la linearità di risposta del rivelatore omodina sfruttando impulsi laser di 100 ns di durata e un rate di ripetizione pari a 1 MHz. Ho inoltre studiato l'evoluzione temporale dell'offset di fase dell'apparato, determinando la finestra temporale di stabilità di fase che caratterizza le due stazioni. Infine ho testato un

possibile metodo per la compensazione attiva dell'offset di fase all'interno di questa finestra temporale, sfruttando la misura omodina di impulsi intensi e fase nota.

Nella seconda parte del mio lavoro di tesi ho studiato le caratteristiche di un canale metropolitano in fibra ottica, sul quale si prevede di testare in futuro il protocollo di CV-QKD. Si tratta di un collegamento in fibra nera tra Firenze e il Polo Scientifico di Sesto Fiorentino, lungo circa 20 km, facente parte di un'infrastruttura in fibra ottica gestita dall'Istituto Nazionale di Ricerca Metrologica di Torino. Ho testato la stabilità temporale del canale in termini di trasmissione, tempo di percorrenza ed effetto sulla polarizzazione della luce.