Il Colle di Galileo

Ilaria Vagniluca[1,2], Nicola Biagi[2], Davide Bacco[3], Alessandro Zavatta[2]

Un sistema di crittografia quantistica per cifrare la videochiamata del Premier a ESOF2020

A quantum cryptography system used to encrypt the Italian Prime Minister's videocall at ESOF2020

[1] Dipartimento di Fisica "Ettore Pancini" dell' Università degli Studi di Napoli "Federico II", Via Cinthia 21, 80126 Napoli (Italia)
[2] Consiglio Nazionale delle Ricerche - Istituto Nazionale di Ottica (CNR-INO), Largo E. Fermi 6, 50125 Firenze (Italia)
[3] CoE SPOC, DTU Fotonik, Technical University of Denmark, 2800 Kgs. Lyngby (Denmark)

Riassunto. Durante la cerimonia di chiusura dell'EuroScience Open Forum (ESOF2020), svoltasi lo scorso 6 settembre a Trieste, il Presidente del Consiglio Giuseppe Conte ha preso parte a una dimostrazione pubblica di un protocollo di crittografia quantistica, realizzata dal gruppo di Comunicazioni Quantistiche dell'Istituto Nazionale di Ottica di Firenze. La dimostrazione ha sfruttato la trasmissione di stati quantistici attraverso la rete in fibra ottica LightNet.

Parole chiave. Crittografia quantistica, tecnologie quantistiche, EuroScience Open Forum, fibra ottica, Trieste.

Abstract. During the closing ceremony of the EuroScience Open Forum (ESOF2020), held on 6 September in Trieste, Prime Minister Giuseppe Conte took part in a public demonstration of a quantum cryptography protocol, carried out by the Quantum Communications group of the National Institute of Optics of Florence. The demonstration exploited the transmission of quantum states through the LightNet fiber optic network.

Keywords. Quantum cryptography, quantum technologies, EuroScience Open Forum, optical fibers, Trieste

With the digital revolution and the advent of the Internet, information security is a fundamental requirement for today's society. This implies the ability to protect our communications from the multiple threats aimed at undermining the authenticity and integrity of information exchanged via the network. For this reason, it is necessary to safeguard sensitive data using

ISSN 2281-7727 (print)
ISSN 2281-9711 (online)
Vol. 10, 1, 2021, pp. 43-47
DOI: 10.36253/cdg-12718
www.fupress.com/cdg

Con la rivoluzione digitale e l'avvento di Internet, un requisito fondamentale per la società odierna è quello della sicurezza informatica, ovvero la capacità di proteggersi dalle molteplici minacce volte a minare l'autenticità e l'integrità delle informazioni scambiate via rete. Per questo motivo, si rende necessario salvaguardare i dati sensibili mediante opportune chiavi di crittografia, capaci di garantire il riconoscimento degli utenti che hanno il permesso di accedere all'informazione protetta. Punto centrale degli attuali sistemi di sicurezza è la distribuzione di queste chiavi di autenticazione, che devono essere recapitate ai soli utenti autorizzati, con il costante rischio di essere intercettate e duplicate durante la loro trasmissione, finendo così nelle mani di utenti indesiderati. La distribuzione quantistica delle chiavi (QKD) propone una soluzione originale al problema della distribuzione delle chiavi di crittografia, con un approccio sostanzialmente diverso da quello correntemente diffuso negli attuali sistemi crittografici. Tale approccio consiste nel codificare ciascun bit della chiave nello stato quantistico di un singolo fotone (o qubit), che viene poi trasmesso all'utente destinatario attraverso un collegamento in fibra ottica standard. In questo modo, grazie alla non-ortogonalità degli stati quantistici e al principio di indeterminazione di Heisenberg, un qualunque tentativo non autorizzato di estrarre, o copiare, l'informazione trasportata dal fotone può essere scoperto dal destinatario, che diventa così in grado di valutare l'effettiva sicurezza della chiave appena ricevuta.

Un sistema di QKD è stato presentato pubblicamente durante la cerimonia di chiusura di ESOF2020 (EuroScience Open Forum), svoltasi a Trieste lo scorso 6 settembre 2020. La dimostrazione è stata condotta dal gruppo di Comunicazioni

appropriate encryption keys, capable of guaranteeing the recognition of users who have permission to access the protected information. The central point of the current security systems is the distribution of authentication keys that must be delivered to authorized users only, avoiding the risk of being intercepted and duplicated during transmission and thus preventing them from falling into the hands of unwanted users.

Quantum key distribution (QKD) proposes an original solution to the key distribution problem, with a substantially new approach that differs from the one used in current cryptographic systems. This approach consists in encoding each bit of the key in the quantum state of a single photon (or qubit), which is then transmitted to the recipient user through a standard optical fiber link. In this way, thanks to the non-orthogonality of quantum states and Heisenberg's uncertainty principle, any unauthorized attempt to extract or copy the information carried by the photon can be discovered by the recipient, who thus becomes able to evaluate the actual security of the received key.

A QKD system was presented in a public demonstration during the closing ceremony of ESOF2020 (EuroScience Open Forum), held in Trieste on 6 September 2020. The demonstration was conducted by the Quantum Communications group of the National Institute of Optics (INO-CNR) of Florence, which realized the two stations for transmitting and receiving the quantum states of light, in collaboration with the Technical University of Denmark (DTU). The appropriately prepared qubits were transmitted through an optical fiber connection of about 10 km, which is part of the network LightNet. The optical fiber used for the QKD protocol al-

Quantistiche dell'Istituto Nazionale di Ottica (INO-CNR) di Firenze, in collaborazione con l'Univesità Tecnica della Danimarca (DTU), che si sono occupati della realizzazione delle due stazioni di trasmissione e di ricezione degli stati quantistici della luce. I qubit, opportunamente codificati, sono stati così trasmessi attraverso un collegamento in fibra ottica di circa 10 km, facente parte della rete LightNet. La fibra ottica utilizzata per il protocollo QKD, ha permesso di distribuire una chiave sicura tra il Dipartimento dei Sistemi Informativi dell'Università di Trieste e la sede di ESOF2020, situata nel Porto Vecchio di Trieste. La chiave di crittografia è stata quindi adoperata per l'autenticazione sicura di una videochiamata via web, alla quale hanno preso parte il Rettore dell'Università di Trieste Roberto di Lenarda, situato nel Dipartimento dei Sistemi Informativi e il Presidente del Consiglio Giuseppe Conte, che ha partecipato alla cerimonia dal palco dell'Auditorium di ESOF2020 (vedi foto). La dimostrazione pubblica è stata introdotta da un intervento del Presidente del CNR, il Prof. Massimo Inguscio.

lowed a secure key to be sent between the Department of Information Systems of the University of Trieste and the ESOF2020 headquarters, located in the Old Port of Trieste. The quantum encryption key was then used for the secure authentication of a web videocall between the Rector of the University of Trieste Roberto di Lenarda, who spoke from the Department of Information Systems, and the Italian Prime Minister Giuseppe Conte, who was attending the ceremony from the stage of the ESOF2020 Auditorium (see photo). The public demonstration was introduced by a speech given by the President of CNR, Prof. Massimo Inguscio.

A quantum cryptography system used to encrypt the Italian Prime Minister's videocall at ESOF2020

A quantum cryptography system used to encrypt the Italian Prime Minister's videocall at ESOF2020