



Contatti | Contacts

Alessandro Zavatta

Telefono | Phone

+39 055 907341

E-mail

info@qticompany.com

Sito | Website

www.qticompany.com

Sistemi di crittografia quantistica per la sicurezza delle comunicazioni

Quantum cryptography systems for secure communications

Sistemi per la distribuzione di chiavi crittografiche simmetriche (Quantum Key Distribution – QKD) che sfruttando le leggi della meccanica quantistica garantiscono la protezione incondizionata delle comunicazioni digitali da attacchi cyber classici e quantistici.

Quantum Key Distribution (QKD) systems that harnessing the laws of quantum mechanics provide unconditional protection of digital communications from classical and quantum cyber-attacks.

Value Proposition

La crittografia classica a chiave pubblica offre protezione in caso di intercettazioni effettuate da un potente computer convenzionale. La scoperta di algoritmi quantistici che accelerano la soluzione di problemi complessi ha sollecitato un recente lavoro di ridefinizione dei presupposti di sicurezza della crittografia a chiave pubblica. La Quantum Key Distribution (QKD) è un metodo di livello fisico che permette una crittografia future-proof (oggi e in futuro), potendo rilevare qualsiasi intercettazione nei canali di comunicazione tra due o più utenti grazie alle proprietà del sistema quantistico.

Present-day public-key cryptography offers security against an eavesdropper equipped with a powerful conventional computer. The discovery of quantum algorithms speeding up the solution of complex problems has prompted recent work to redefine the security assumptions of public-key cryptography. Quantum Key Distribution (QKD) is a physical layer method that enables future-proof encryption (today and in the future), being able to detect any eavesdropping in communication channels between two or more users thanks to the system's quantum properties.

Key Technologies

- **Quell-X:** sistema completo di Quantum Key Distribution (QKD) per la generazione di chiavi crittografiche. Implementabile su qualsiasi configurazione di rete e completamente integrabile nelle reti di telecomunicazione esistenti.
 - **Key Management Entity (QKME):** dispositivo di interfaccia tra il sistema QKD Quell-X e gli apparati di cifratura. Consente l'archiviazione e distribuzione sicura delle chiavi crittografiche e l'interoperabilità tra le tecnologie classica e quantistica.
 - **Quantum Software Defined Network (QSDN):** dispositivo di rete per la gestione di infrastrutture di comunicazione a più nodi, per un controllo dinamico e ottimizzato del network.
- Quell-X: a complete Quantum Key Distribution (QKD) system, able to generate symmetric cryptographic keys. The system can be implemented on any network configuration and be fully integrated into existing telecommunications networks.*
- Key Management Entity (QKME: an interface device between the QKD Quell-X system and encryption equipment. It enables secure storage and distribution of cryptographic keys and the interoperability between classical and quantum technology.*
- Quantum Software Defined Network (QSDN): the solution to manage multi-node communication infrastructures. It allows dynamic and optimised control of the network.*

Applications

La tecnologia QKD trova principale applicazione nei settori della ricerca, della grande industria, governativo, della difesa, finanziario e sanitario per la protezione di:

- infrastrutture e servizi nelle reti aziendali
- cloud data center
- sistemi di controllo, supervisione e acquisizione dati nelle infrastrutture critiche

QKD technology is mainly applied in the research, industry, government, defence, financial and healthcare sectors for the protection of:

- *infrastructure and services in corporate networks*
- *cloud data centres*
- *control, supervision and data acquisition systems in critical infrastructures*

Background

Publicazioni Publications

- D. Ribezzo et al., P.R. Applied 20, 044052 (2023)
- Ribezzo, D., et al., Adv. Quantum Technol. 6.2: 2200061 (2023)
- Bacco, D et al., Nature Photonics 17.5: 378-379 (2023)

Brevetti Patent

- Family patent: Rilevamento di impulsi deboli per ricevitore e metodo di distribuzione di chiavi quantistiche a variabile discreta - Weak pulse detection for discrete-variable quantum key distribution receiver and method. Pending in IT (IT202100013571), BR (BR112023024700) and CA (CA3221200)
- Family patent Trasmettitore di distribuzione a chiave quantistica Quantum key distribution transmitter. Pending in IT(IT202100005462), EP (EP4305801), CA(CA3212999) and BR (BR112023018383)

TRL

9

Collaborazioni Collaborations

Partnership con Telsy S.p.A, centro di competenza per la crittografia e la cybersicurezza del Gruppo TIM.
Partnership with Telsy S.p.A, the competence centre for cryptography and cybersecurity of the TIM Group.