Quantum-safe Internet based on Service-oriented Quantum Key Distribution Network

Zhangchao Ma, Jianquan Wang

CAS Quantum Network Co,. Ltd.
E-mail: mazhangchao@casquantumnet.com

The fast development of quantum computer poses significant threat to today's cyber security. There are three routes to achieve quantum-safe internet. First, post-quantum cryptography which relies on new complexity-based asymmetric algorithms, is easy to deploy, but it cannot guarantee theoretical security against quantum computer and still requires time to mature and standardized. Second, quantum-key distribution (QKD) which relies on the quantum physics, is theoretically safe while its usage is limited to fiber-based scenarios currently and requires quantum-physics-based hardware support. Third, symmetric key-based systems, e.g., Kerberos, 3GPP mobile networks, are already resistant to attack by quantum computer [1]. However, Kerberos-like systems faces problems when applied to wide-scale public network, including how to safely deliver initial keys to terminals and how to refresh the keys.
Indeed, QKD provides a practical quantum-safe solution to deliver large number of keys from key distribution center (KDC) to terminals instead of using couriers, which can supplement the symmetric key management systems. The solution we would like to demonstrate is to construct a service-oriented QKD network which combine the advantages of QKD, KDC and PQC, in order to provide quantum-safe key management service. It is deemed to be able to achieve a real-world quantum-safe internet today and can greatly expand the usage of QKD.

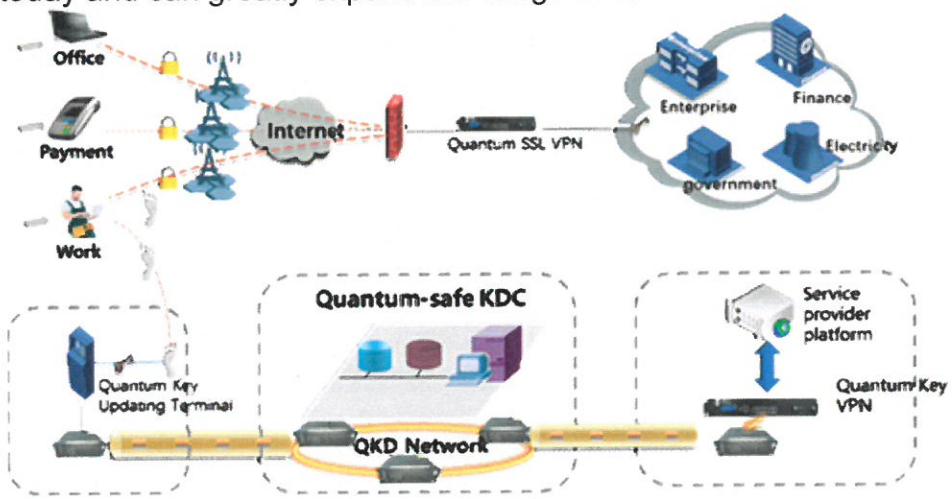

Fig. 1 QKD and KDC combined quantum-safe internet solution

References

[1] Campagna, Matt; Hardjono; Pintsov; Romansky; Yu (2013). "Kerberos Revisited Quantum-Safe Authentication" (PDF). ETSI.