January 2024

Independent Security Evaluation of Toshiba Quantum Key Distribution Technology

Building trust for practical secure deployments

Summary

The UK National Physical Laboratory (NPL) performed independent assessment of various critical parameters of Toshiba's Quantum Key Distribution (QKD) technology. These measured quantities are integral to the product's security and have been validated to match expected values.

Introduction

Quantum Key Distribution (QKD) has emerged as a powerful solution for securing digital communications in the era of quantum computing. QKD takes advantage of the laws of quantum mechanics to ensure that an eavesdropper cannot infer any bits of information during the generation of encryption keys that are used to secure private communications. This ensures 'provable security', known technically as 'information-theoretic security', stemming from the ability to quantify potential information leakage from the laws of quantum physics. QKD is thus resistant to attacks from future supercomputers and even quantum computers, unlike today's cryptography, which is known to already be vulnerable in the face of more advanced computing power. With these known weaknesses in conventional cryptography, it is important that organisations start moving towards quantum-safe communication technologies now, since even today's classically encrypted data could be harvested and stored for decryption in the future with more advanced computational resources.

QKD is a quantum-photonic technology, involving the generation, transmission and measurement of single particles of light ('photons') that encode single bits of information. While the theoretical QKD protocol is provably secure, the overall security of a QKD system relies on the hardware correctly implementing the protocol.

Any deviations from this, such as due to manufacturer error or low-performance components, could compromise security, since the system parameters are no longer matched to the theoretical security proofs.

This concern has led to the growing importance of the field of QKD 'Implementation Security,' which aims to assess the quality of the QKD system implementation compared to the requirements of the protocol. Toshiba and NPL have contributed to this area over many years through original research as well as providing input to worldwide standardisation activities.

One aspect of this work is the development of a security assurance framework for QKD technology. That is, a standardised methodology that can be used to evaluate QKD hardware and confirm it performs reliably and, therefore, securely. As with existing assurance programs for many information security technologies, the hardware assessment should be performed by an expert body, independent of the vendor.

Security Evaluation Measurements

Because independent security assessment is so valuable for building trust in QKD hardware, Toshiba and NPL have recently collaborated on this topic, funded by the European OpenQKD and MeTISQ projects[1,2]. As the UK's national measurement laboratory, NPL has unique expertise in precision measurement. It is well-placed to evaluate emerging quantum technologies where photon-level and picosecond-timescale accuracy is required.

For the security evaluation, NPL developed a set of tests to measure the primary hardware parameters that are critical to QKD security. These were applied to both QKD Transmitter and Receiver modules - thus considering both nodes of a typical QKD communication link. The tests considered many parameters. Of particular importance, this included a quantity called the 'photon flux', which is the effective light intensity - this has to be precisely set to the single-photon level in order to achieve the quantum mechanical phenomena upon which QKD's security is built (see Box 1). At the transmitter, the optical frequency of the photons was also characterised. Separate measurements at the receiver evaluated single-photon

detector parameters, such as dark count and after-pulsing probabilities and detection efficiency linearity. Short-term values and their long-term stabilities were measured.

The rate at which secure bits are generated is a key performance metric when comparing QKD hardware. NPL measured the variation of secure bit rate for the overall system as the link loss was adjusted through a range of accurately calibrated values.

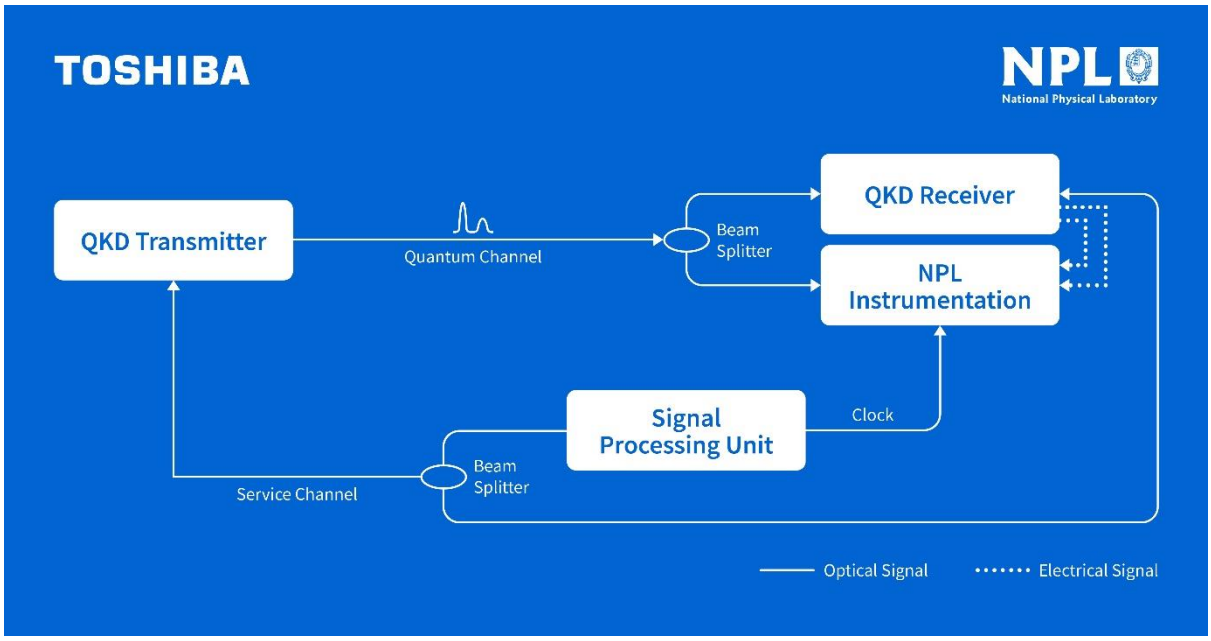

Figure 1 - Schematic of NPL's test setup, showing connections between the QKD system and NPL instrumentation.

Measurement Outcomes

Toshiba provided a standard QKD system upon which NPL could independently perform their measurements in their laboratory. All experimental measurements and system provisioning was performed directly at NPL.

In all cases, the data collected by NPL validated the technical specification of Toshiba's QKD hardware. This included all measured optical quantities matching the values used in the QKD security proofs for Toshiba's QKD systems[3,4]. For example, NPL measured the photon flux to be within experimental accuracy of the Toshiba-specified value[3]. Additionally, NPL confirmed that the system's reported secure bit

rate over their calibrated attenuation links matched or exceeded the rates quoted in Toshiba's product specification.

Conclusions

The independent evaluation of Toshiba QKD technology by NPL confirmed that all measured optical quantities were as specified, and thus, compatible with the requirements of the provably secure underlying theory. The work also identified new approaches for evaluating QKD hardware and paves the way for further activities to fully validate the security of a QKD system. This is an important step towards complete QKD product security assurance by independent verification to bolster trust in this emerging critical technology.

Box 1: Why are single photons needed?

Classical communication uses pulses of light to encode information – typically comprising millions of light photons per pulse. QKD, by contrast, encodes bits onto single photons. This is the basis for security since, according to quantum mechanics, light experiences very different properties at the single-photon level. Single photons can exist in a superposition state and a fundamental law of nature states that a photon cannot be cloned. Thus, by using a single (i.e. unclonable) photon for communication, any attempt to measure it by an attacker fundamentally destroys the information, thereby enabling the attack to be detected.

This, of course, requires the optical hardware to accurately generate single photons. Generating single photons at high speed is difficult, but can be effectively achieved using semiconductor laser sources, where the single-photon rate is quantified by a "photon flux" parameter. This parameter is used in the calculations that ensure QKD security and thus, physical QKD systems must precisely implement a specified photon flux value.

References:

1. H2020 Project OPENQKD under Grant 857156
2. EMPIR project MeTISQ; This project received funding from the EMPIR program co-financed by the Participating States and from the European Union Horizon 2020 research and innovation program.
3. M. Lucamarini et al., "Efficient decoy-state quantum key distribution with quantified security," Opt. Express **21**, 24550 (2013)
4. Z. Yuan et al., "10-Mb/s Quantum Key Distribution," J. Lightwave Technol. **36**, 3427 (2018)

National Physical Laboratory (NPL)

NPL is the UK's National Metrology Institute, providing the measurement capability that underpins the UK's prosperity and quality of life.

From new antibiotics to tackle resistance and more effective cancer treatments, to quantum-secured communications and superfast 5G, technological advances must be built on a foundation of reliable measurement to succeed. Building on over a century's worth of expertise, our science, engineering and technology provides this foundation. We save lives, protect the environment and enable citizens to feel safe and secure, as well as support international trade and commercial innovation. As a national laboratory, our advice is always impartial and independent, meaning consumers, investors, policymakers and entrepreneurs can always rely on the work we do.

Based in Teddington, south-west London, NPL employs over 800 scientists. NPL also has regional bases across the UK, including at the University of Surrey, the University of Strathclyde, the University of Cambridge and the University of Huddersfield's 3M Buckley Innovation Centre.

Toshiba

Toshiba Corporation leads a global group of companies that combines knowledge and capabilities from over 145 years of experience in a wide range of businesses – from energy and social infrastructure to electronic devices – with world-class

capabilities in information processing, digital and AI technologies. These distinctive strengths support Toshiba's continued evolution toward becoming an Infrastructure Services Company that promotes data utilization and digitization, and one of the world's leading cyber-physical-systems technology companies. Guided by the Basic Commitment of the Toshiba Group, "Committed to People, Committed to the Future," Toshiba contributes to society's positive development with services and solutions that lead to a better world. The Group and its 120,000 employees worldwide secured annual sales of 3.3 trillion yen (US$27.4 billion) in fiscal year 2021.