International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Report

Corrigendum 1

(04/2021)

XSTR-SEC-QKD

Security considerations for quantum key distribution networks

Corrigendum 1

Summary

This Corrigendum 1 of ITU-T TR.SEC-QKD "Security considerations for quantum key distribution network" changes relevant expressions relative to "IT-secure", changes "qubits" into "quantum states", changes "co-fibre" into "co-propagation" and modifies relevant content.

NOTE – This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Technical Report ITU-T TR.SEC-QKD

Security considerations for quantum key distribution networks

Corrigendum 1

5 Introduction to the QKDN

Revise the text of clause 5 as follows:

The concept of QKD network (QKDN) needs to be introduced by extending the point-to-point topology of QKD link to a multi-hop topology in order to share ~~information-theoretically secure (IT-secure)~~ keys between any user applications even when they are not directly connected via a QKD link.

…

– The quantum relay scheme is the ideal solution to distribute ~~relay qubits~~ quantum states ~~to~~over long distance but the required quantum memory and quantum repeater technology are currently under development and are not commercially available.

…

– A QKD link consists of a quantum channel and a classical channel. The quantum channel is a physical optical path that is only used to transmit quantum states~~qubits~~. The classical channel, which is used to exchange information ~~such as key synchronization and~~for key distillation, can be a conventional Internet~~ protocol (IP)~~ channel that is not necessarily optical.

6 Security considerations for QKDN

Revise the text of clause 6 as follows:

The key establishment process of ~~keys generated by~~ QKD protocol operated by two entities, for example, sender (Alice) and receiver (Bob), can be proven as information-theoretically secure based on the quantum information theory.

7 Standardization issues and suggestions for future work on QKDN

Revise the text of clause 7 as follows:

2) Issue 2: How to ensure security of trusted-relay-based QKDN?

Currently, QKD security study is being pursued in ETSI [b-ETSI White paper no. 27] and ISO~~ [b-ETSI White paper no. 27] and~~ [b-ISO/IEC QKD project 23837]~~[b-ISO/IEC QKD work items]~~.

3) Issue 3: How to reduce QKD deployment cost?

...The possible means include co-propagation ~~co-fibre transmission~~ of QKD signals ~~channels~~ and classical signals through a common fibre in existing optical transmission networks, integration of QKD modules into telecom network devices, etc.