|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION  **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2022-2024 | | | TSAG-C065 |
| TSAG |
| Original: English |
| **Question(s):** | | N/A | Geneva, 22-26 January 2024 | |
| **CONTRIBUTION** | | | | |
| **Source:** | | Korea (Rep. of), KT | | |
| **Title:** | | Encouraging TSAG to consider recommending ITU-T SGs to work on quantum-resistant | | |
| **Contact:** | | Hyungsoo KIM KT corp. Korea (Rep. of) | | Tel: +82 10 6808 5199 E-mail: hans.kim@iotct.net |
| **Contact:** | | Heung Youl Youm Soonchunhyang University Korea (Republic of) | | Tel: +82-41-530-1328 Email: [hyyoum@sch.ac.kr](mailto:hyyoum@sch.ac.kr) |
| **Contact:** | | Sungchae Park Soonchunhyang University Korea (Republic of) | | Tel: +82-41-530-1328 Email: [zoesc.park@sch.ac.kr](mailto:zoesc.park@sch.ac.kr) |

|  |  |
| --- | --- |
| **Abstract:** | Standardization of quantum-resistant for ITU-T SGs is identified for future activity, including NSP aspect. |

**Introduction**

The ITU PP 2022 Resolution 71 mentions the potential of quantum computing, highlighting the positive aspects.

* Meanwhile, the Internet of Things, quantum computing and artificial intelligence are becoming more sophisticated and widespread. These technologies have the potential to improve operational efficiency, accelerate automation and unlock new capabilities.

However, it has not yet considered the concerns about attacks from large scale quantum computers that have already proven their capability to hack certain cryptographic algorithms.

Certainly, some SGs are conducting related studies, but they are limited to the QKD Network. And, the standardization of QKD network in ITU-T is being developed with a focus on cost-effective and stable networking technology for QKD services.

* Since 2018, ITU-T SG13 has been working on standardizing the QKD network, completing 20 Recommendations to date with over 15 more in progress.
* SG 17 has completed 5 Recommendations and is developing 5 more.
* SG 11 has completed 5 Recommendations and is developing 2 more.

Although QKD technology is one of the quantum-resistant technologies, it is only used to supply secrete keys for symmetric key cryptography in the modern cryptographic system. Therefore, a different approach is needed for other public key cryptographic functions, such as key encapsulation and digital signature methods. It is possible to defend against attacks by large scale quantum computers by enhancing modern cryptographic algorithms, referred to as PQC (Post Quantum Cryptography). For this purpose, the U.S. NIST is developing a PQC algorithm, while Korea (Republic of) is working on developing a KPQC algorithm.

However, further work is also needed to study PQC (Post-Quantum Cryptography) algorithms to overall security infrastructure and application. For instance, security protocols like TLS or IKE, which use standardized cryptographic algorithms in modern cryptographic systems, require additional technical standardizations, such as how to incorporate PQC algorithms. To this end, organizations like ETSI and GSMA are developing contents related to migration strategies for making existing cryptographic systems quantum-resistant.

* ETSI TR 103 949 V1.1.1 (2023-05), Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study
* ETSI TR 103 619 V1.1.1 (2020-07), CYBER; Migration strategies and recommendations to Quantum Safe schemes
* ETSI GR QSC 003 V1.1.1 (2017-02), Quantum Safe Cryptography; Case Studies and Deployment Scenarios
* GSMA Whitepaper (2023-02), Post Quantum Telco Network Impact Assessment
* GSMA Whitepaper (2023-09), Guidelines for Quantum Risk Management for Telco

Meanwhile, SG17, as a dedicated group for security, has been leading critical standardizations such as X.509 and X.800 over many Study Periods. However, it appears that they have not yet fully considered the security threats posed by Quantum computing. In light of this, there is an emerging need within SG17 for immediate study and standardization activities related to quantum-resistant security.

Not only SG17 but also other SGs should study the possibility and impact of attacks from quantum computer for their Recommendations and on-going draft documents. Thereafter progress towards quantum-resistant standardization could be considered as some examples below;

* SG 3: expected policy issues following the introduction and deployment of quantum resistance
* SG 11: testing methodology and evaluation process of quantum resistance
* SG 13: quantum resistance-oriented network architecture and functional requirements
* SG 20: quantum resistance-oriented IoT, smart cities and communities

However, considering the extensive study areas of SGs for the above, deciding which standards to focus on and in what order, along with the direction of study, is expected to demand significant effort and time. It might be worth considering the establishment of a specialized task force to undertake such critical tasks.

Note - It is noted that JCA-QKDN under the auspicious of TSAG coordinates standardization work on quantum key distribution networks (QKDNs) within ITU-T and acts as the point of contact within ITU-T and other standards development organizations, consortia and forums working on QKD-related standardization only.

**Proposal**

Republic of Korea suggest TSAG to consider recommending ITU-T SGs to consider the following potential actions, under the leadership on CG-QR (Corresponding Group towards Quantum Resistance) of TSAG:

* Example action 1: Revision of existing standards for quantum resistance (e.g., the x.509 series, Y.3800-series, etc.)
* Example action 2: establishing quantum-resistant standardization migration roadmap in ITU-T SGs
* Example action 3: developing guidelines for making existing technologies to be quantum-resistant.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_