A Case Study of Quantum Key Distribution Operating in Private 5G Network System

Yu YU, Takahiro YAMAURA, Ririka TAKAHASHI, Yoshimichi TANIZAWA

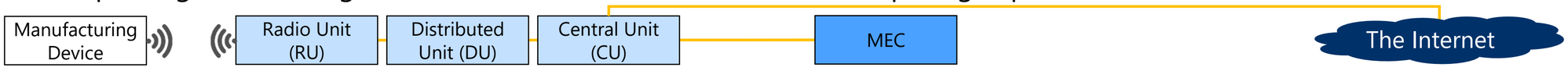
Corporate Research & Development Center, Toshiba Corporation
Email: yu2.yu@toshiba.co.jp

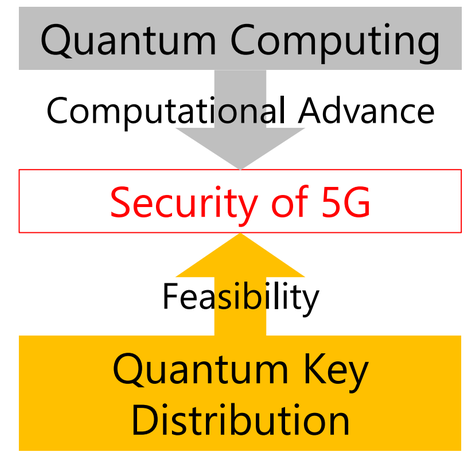
What?

An experimental scenario of remote control with equipment operating at the manufacturing site over private 5G network has been demonstrated. To further enhance the security level, quantum key distribution (QKD) has been applied to this private 5G network system. The results reveal that QKD could be applicable to provide secure communications in private 5G network system for practical use.

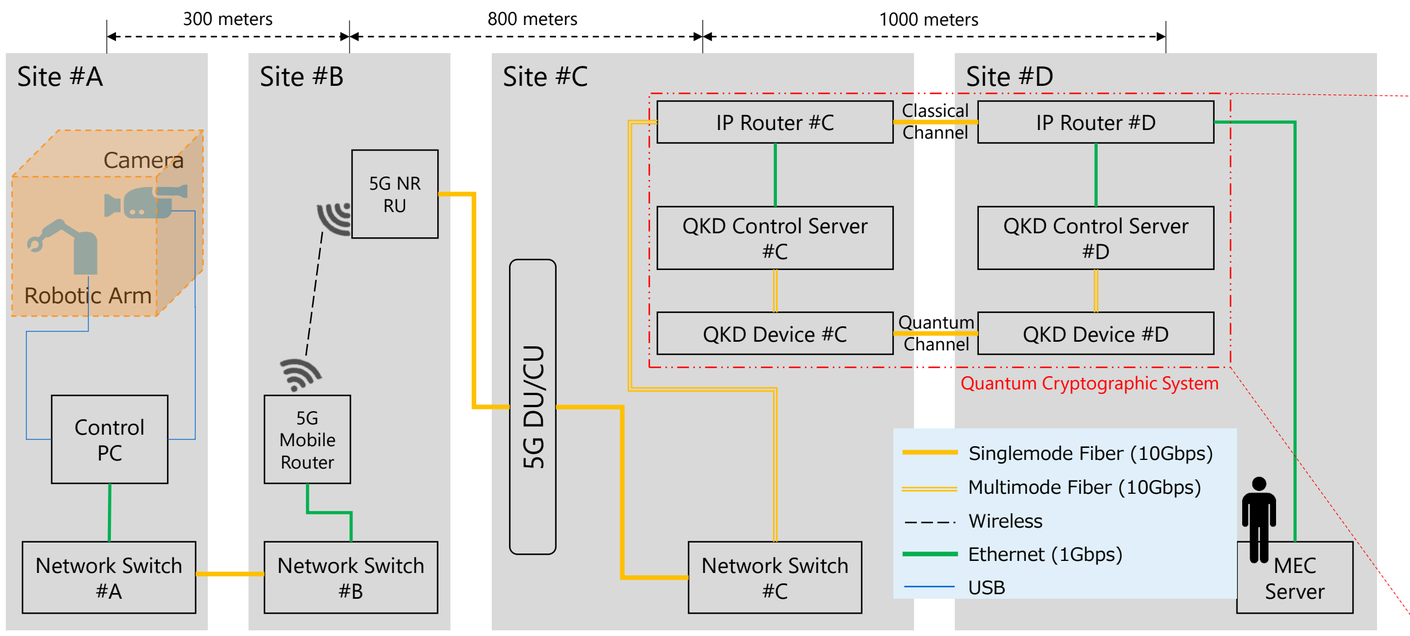
Why?

- Nationwide 5G networks are being widely commercialized, which would play more important role in human daily life
  - To provide increased bandwidth, enable lower-latency communication, as well as large-scale connections
- In addition, private 5G is a new network system that allows various entities including local companies and local governments to build and use 5G networks in their buildings and premises
- Manufacturing is one of the key sectors for private 5G, which requires wireless connectivity with ultra-reliable low latency
- To satisfy the latency-sensitive services demand of manufacturing, multi-access edge computing (MEC) has emerged as a novel paradigm at the edge of 5G networks due to its advanced computing capabilities

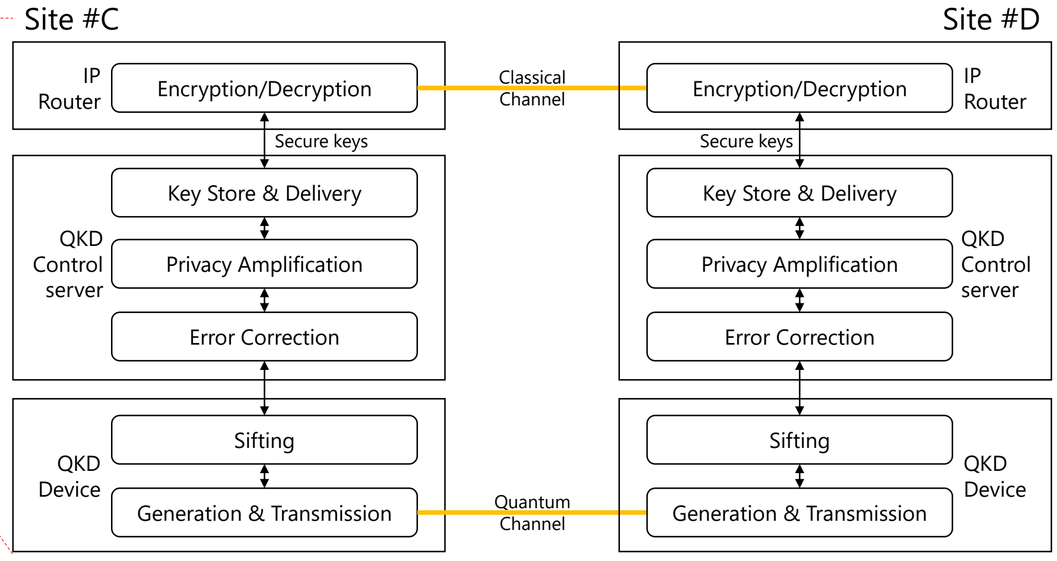




How?



Overview of experimental demonstration in Toshiba Fuchu Complex

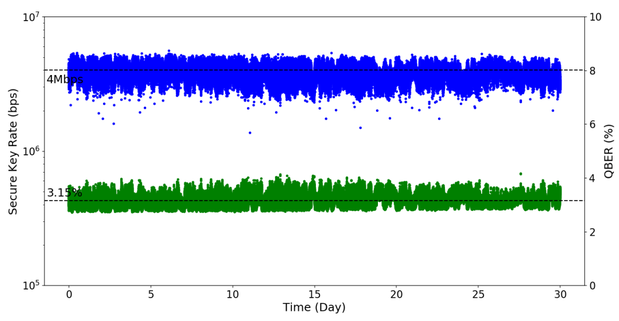


Schematic diagram of QKD system

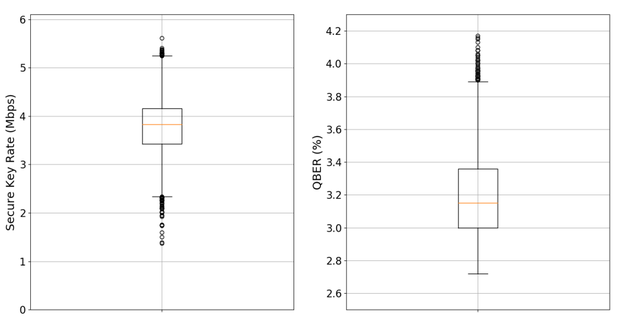
- An operator at site #D remotely controls a robotic arm while watching the real-time video streaming from a camera in site #A is assumed
- All video/control data are communicated through private 5G network system
- Quantum Cryptographic System (QKD System) is deployed between 5G distributed unit/central unit (DU/CU) and MEC server

- Efficient decoy BB84 protocol with phase encoding [1]
- Software based prototype one-time-pad cryptographic method [2]
- Sifting process based on FPGA
- Error correction and privacy amplification based on CPU

Results and Discussion



30 days continuous secure key rate and QBER



Box plot of the secure key rate and QBER

Throughput of OTP with QKD keys between site #C and #D

Direction	Downlink	Uplink
OTP throughput	83.02 Mbps	82.78 Mbps

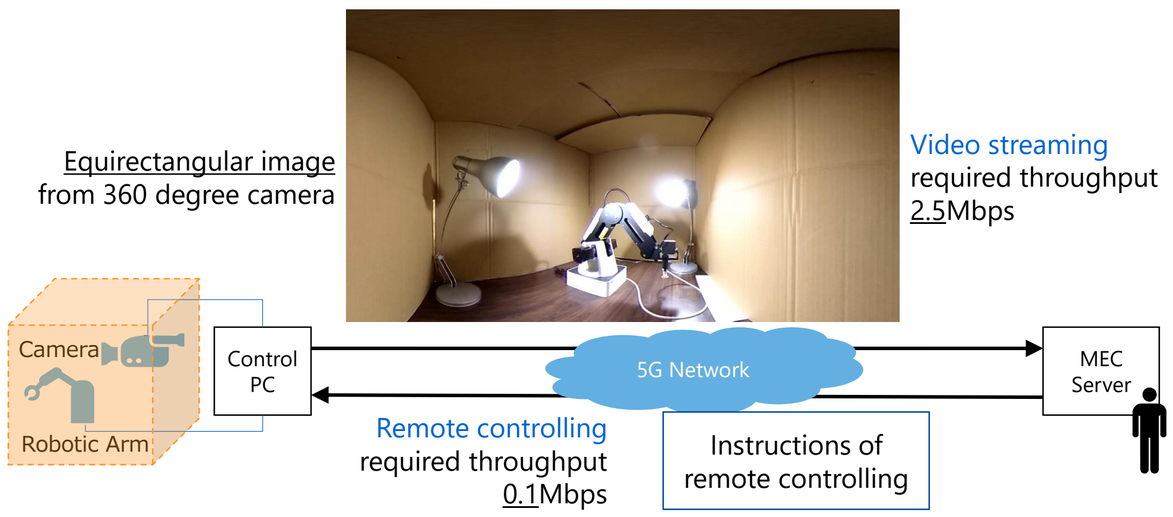


Image of video streaming and remote controlling

- The box plot figure showed that 3.83 Mbps of average secure key rate with 3.15% average quantum bit error rate (QBER) was achieved
- The results of table indicate that with pre-stored secure keys, the QKD system is sufficient for the practical use over private 5G network
- Further research work will be conducted to improve the performance of QKD system and apply QKD to the front-haul of private 5G network system

Reference:

[1] Z. Yuan et al., Journal of Lightwave Technology, doi: 10.1109/JLT.2018.2843136 (2018).
[2] R. Takahashi et al., doi: 10.1109/ICUFN.2019.8806052 (2019).

Acknowledgment:

This work is supported by the Ministry of Internal Affairs and Communications (MIC), “R&D of ICT Priority Technology Project (JP MI00316)”. The authors would like to thank to Toshiba Infrastructure Systems & Solutions Corporation and Toshiba Fuchu Complex for the private 5G network operation and management.