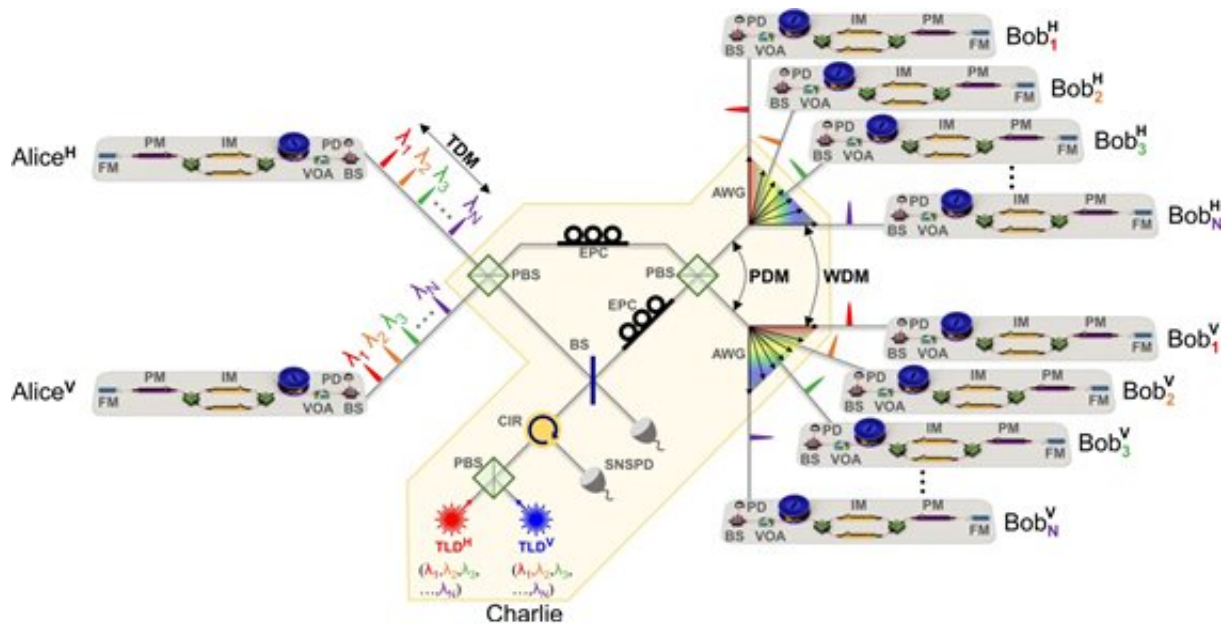


Researchers create key technology for quantum cryptography commercialization

July 22 2022



2:N TF QKD network structure. Credit: Korea Institute of Science and Technology

In modern cryptosystems, users generate public and private keys that guarantee security based on computational complexity and use them to encrypt and decrypt information. Recently however, modern public-key cryptosystems have faced potential security loopholes against quantum computers with great computational power. As a solution, quantum cryptosystems have been highly noticed. They use quantum keys that

guarantee security based on quantum physics rather than computational complexity; thus, they are secure even against quantum computers. Therefore, quantum cryptosystems are expected to replace modern cryptosystems.

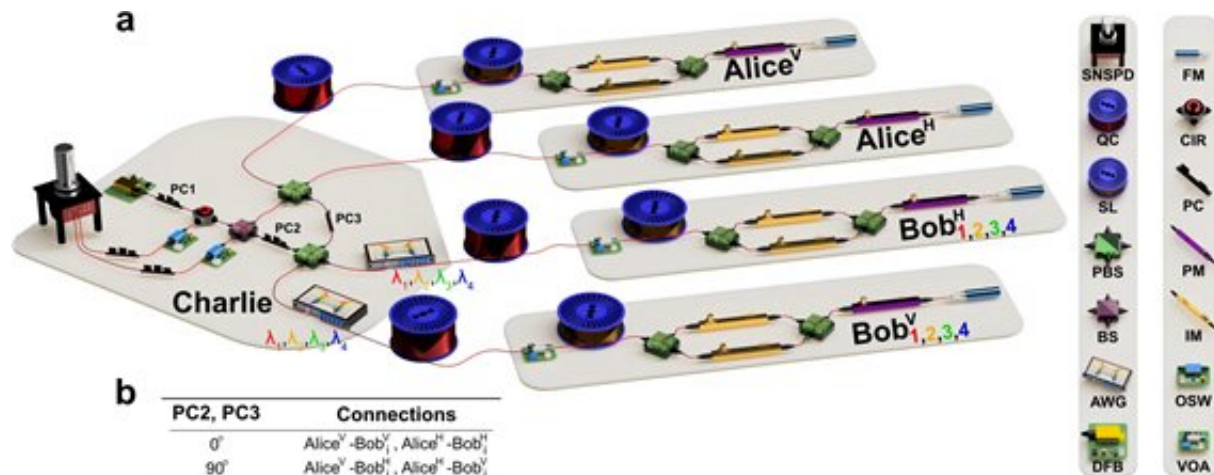
Quantum key distribution (QKD) is the most important technology for realizing quantum cryptosystems. Two main technical issues should be addressed to commercialize QKD. One is the communication distance, and the other is the expansion from one-to-one (1:1) communication to one-to-many (1:N) or many-to-many (N:N) [network](#) communication.

Twin-field (TF) QKD, announced in 2018, is a long-distance protocol, which can dramatically increase the communication distance of QKD systems. In TF QKD, two users can distribute a key by transmitting quantum signals to an intermediate third-party that is for measurement. Given the inevitable channel loss, this architecture allows the users to increase the communication distance. However, despite its innovativeness, it has been experimentally demonstrated by only a few global QKD leading groups owing to the significant difficulty of system implementation, and research on the TF QKD network is still insufficient.

The Korea Institute of Science and Technology (KIST, Director Seok-jin Yoon) announced that their research team, the Center for Quantum Information, led by director Sang-Wook Han, succeeded in an experimental demonstration of a practical TF QKD network. This is the second experimental demonstration of the TF QKD network in the world after the University of Toronto in Canada.

In their study published in *npj Quantum Information*, the research team proposed a new TF QKD network structure scalable to a two-to-many (2:N) network based on polarization-, time-, and wavelength-division multiplexing. Unlike the first demonstration of the University of

Toronto based on a ring network structure, the research team's architecture is based on a star network. The quantum signal in a [ring structure](#) must pass through every user connected to the ring, however, the star structure only has it go through the center, making it possible to implement a more practical QKD system.



Experiment diagram. Credit: Korea Institute of Science and Technology

Besides, to overcome the main implementation obstacles to developing the TF QKD system, the team applied a plug-and-play (PnP) structure. A conventional TF QKD system requires many [control systems](#), such as timing, wavelength, phase, and polarization controllers, to maintain the indistinguishability of two quantum signals emitted by two users' different light sources. Whereas in the PnP TF QKD architecture developed by the KIST research team, the middle third-party generates and transmits the initial signals to both users using a single light source, and the signals return to the third-party by making a round trip. Therefore, the polarization drift due to the birefringence effect of the channel is automatically compensated, and users have fundamentally the

same wavelength. In addition, due to the two signals passing through the same route in [opposite directions](#), the arrival times of the signals are naturally identical. As a result, only a phase controller is required for implementing the research team's architecture. Based on the architecture, the team successfully conducted an experimental demonstration of a TF QKD network.

"It is a significant research achievement showing the possibility of solving the two main obstacles to QKD commercialization, and we have gained a key technology leading the corresponding research," said Sang-Wook Han, the leader of the Center for Quantum Information.

More information: Chang Hoon Park et al, 2×N twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing, *npj Quantum Information* (2022). [DOI: 10.1038/s41534-022-00558-8](https://doi.org/10.1038/s41534-022-00558-8)

Provided by National Research Council of Science & Technology

Citation: Researchers create key technology for quantum cryptography commercialization (2022, July 22) retrieved 16 April 2024 from <https://techxplore.com/news/2022-07-key-technology-quantum-cryptography-commercialization.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.
