Gwangju Institute of Science and Technology
Official Press Release — https://www.gist.ac.kr

Section of Public Relations	Dongsun Cho Section Chief 062-715-2061	Nayeong Lee Senior Administrator 062-715-2062
Contact Person for this Article	Professor Byoung S. Ham School of Electrical Engineering and Computer Science 062-715-3502	
Release Date	2021.02.22	

Professor Byoung S. Ham is the first to secure next generation secure communication with purely domestic technology

▫ GIST (Gwangju Institute of Science and Technology, President Kiseon Kim) School of Electrical Engineering and Computer Science Professor Byoung S. Ham (Center for Photon Information Processing director) conducted and verified the first basic test of a next-generation high-encryption communication* protocol that will guarantee unconditional security in telecommunication.

* Classic Cryptographic Key Distribution (USCKD): A method proposed by the domestic engineers in 2020 that guarantees unconditional security at the QKD level and is fully compatible with existing communication equipment and lines. It is free from the quantum trap of QKD because it does not require quantized keys or quantum lines. Above all, a next-generation cryptographic communication protocol that allows eavesdropping on classical track hacking by the principle of double-track quantum superposition, but it blocks cryptographic decryption at the source.

◦ As a result, unlike existing quantum key distribution* methods based on the principle of non-copyability, the next generation security communication technology, which is fully compatible with existing communication equipment and facilities, and guarantees unconditional security, is a purely domestic technology.

    * Quantum Key Distribution (QKD): Based on the principle of duplication of quantum mechanics, the security of the quantized key (cubit) is guaranteed only on quantum lines. It is not compatible with existing communication lines and equipment, and unconditional security is achieved conditionally due to quantum loophole.

- Professor Byoung S. Ham laid an important foundation for the practical use of unconditional secure communication using classical communication equipment and facilities by experimentally proving the unconditional security classical encryption key distribution protocol developed by himself in 2020 for the first time.

    - The USCKD classical encryption communication technology verified in this study is, above all, compatible with the current commercial system, achieves unconditional security with a classical light source, that is, a laser rather than a single photon, and doubles QKD quantum key distribution, the only absolute security method to date. It is related to the next-generation security communication secured by the line overlap, and its expected to be highly effective.

- In existing quantum cryptographic communication, the principle of absolute security was based on the principle of the inability to replicate a quantized signal; in this study, absolute security was secured not from the quantization of the signal but from the quantization of the channel (quantum superposition). It is considered an absolutely secure communication method that will realize the one-time pad (OTP), which is the aspiration of humanity, because the key distribution process is definite in the same way as the quantum memory principle, and the encryption key generation/exchange speed is in principle similar to the existing communication data transmission speed.

    - Above all, since the absolute security encryption communication technology proposed in this study is compatible with wireless communication devices and facilities as well as existing optical communication, it is possible to secure unconditional security at the QKD level by using the existing communication line as it is. Unlike QKD, it is free from copying/switching/routing, so it can be applied to the current Internet, which is mainly based on classical computers.

- Professor Byoung S. Ham said, "For the first time in the world, we pre-validate a new method of classical cryptographic key distribution technology that will guarantee classical absolute secure communications that are traditionally impossible in any way. In the future, it is expected that this will be applied to defense, administrative, and financial networks, as well as medical data transmission for remote medical services, education networks for remote lectures, and absolute security wired and wireless communication technologies essential for driving and flying."

  - The results were published online on February 18, 2021, in *Scientific Reports*, a sister journal of Nature.

GIST
Since 1993