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

Section of Public Relations	Hyo Jung Kim Section Chief (+82) 62-715-2061	Nayeong Lee Senior Administrator (+82) 62-715-2062
Contact Person for this Article	Professor Byoung S. Ham School of Electrical Engineering and Computer Science +(82) 62-715-3502	
Release Date	2020.07.16	

Professor Byoung S. Ham devises a new absolutely secure cryptographic technology

☐ GIST (Gwangju Institute of Science and Technology, President Kiseon Kim) School of Electrical Engineering and Computer Science Professor Byoung S. Ham has proposed a new absolute secure cryptographic communication protocol that can completely replace the quantum cryptographic key distribution technology and is compatible with existing optical communication networks regardless of the transmission distance.

- Professor Byoung S. Ham secured unconditional information and communication security at a level compatible with traditional classical cryptographic communication methods, as well as completely excluding the three essential elements of quantum signals, quantum channels, and quantum detectors.

☐ Quantum Key Distribution (QKD) is a technology that distributes and manages secret keys for quantum communication. It is a quantum technology* for unconditionally secure cryptographic communication that has been studied for the past 36 years since it was first presented in 1984. However, due to incompleteness of quantum signals, quantum channels, and quantum detectors, it is impossible to secure unconditional security**. Above all, the quantum key cannot be reused for absolute security, so it is difficult to apply it to financial/administrative computer networks in a city.

* quantum technology: It is a next-generation information and communication technology that has taken a step forward from existing information and communication through security, ultra-fast computation, etc. by applying unbreakable quantum properties to the field of information and communication.

** unconditional security: In classical cryptographic communication, unconditional security is fundamentally impossible, so hacking is a frequent problem. For unconditional security, it must be secured only from randomness, such as flipping a coin, according to Shannon's positive theory. The problem is that quantum cryptographic key distribution is the only way to transmit/exchange such randomness.

□ This research is about a new cryptographic communication technology that guarantees unconditional security that replaces traditional classical cryptography, such as public key method as well as existing quantum cryptography based on quantum cryptographic key generation/exchange technology. The impact is expected to be enormous as it uses general channels as communication lines and classic signals as keys, but guarantees absolute security like quantum cryptography.

◦ In existing quantum cryptography communication, absolute security was based on the principle of non-reproducibility of quantized signals, but this study secured absolute security not in quantization of signals but in quantization of channels (quantum overlap)*, and the key distribution process is definitive as in the optical memory principle. In addition, since the encryption key generation/exchange rate is similar to the transmission speed of optical communication data, it can be applied to realize a One Time Pad, or direct absolute secure communication of information, which is a long-cherished project of humanity.

* quantum overlap: one of the coherence characteristics as interference of light in double slit experiments where, in principle, the unconditional security of data transmission is ensured by the principle of allowing eavesdropping of data on one or both tracks but not decrypting eavesdropped data

□ Professor Byoung S. Ham said, "This research achievement has the greatest significance in that it has devised the world's first encryption key distribution technology that guarantees absolute security, which is impossible by any other method. I hope that it can be applied to various security areas in the future, including defense, administrative and financial networks, as well as medical data transmission for telemedicine or education networks for remote lectures."

◦ The results were published on July 15, 2020, in *Scientific Reports*, a sister journal of *Nature*.

⌘