Performance Evaluation of Fully Homomorphic Encryption for End-to-End Cryptographic Communication in Multihop Networks

Hye-Yeon Shim*, Tae-Rim Park**, Il-Gu Lee*

*Department of Future Convergence Technology Engineering, Sungshin University, South Korea

**Department of Future Convergence Technology Engineering, Sungshin University, South Korea

{20180922, 20180917, iglee} @sungshin.ac.kr

Abstract— **With the advent of a hyperconnected society, network services that connect the cloud and user terminals are emerging. Accordingly, the security technology that guarantees security and speed in end-to-end communication is becoming more important. Homomorphic encryption is useful in environments that require security in the end-to-end communication that can be operated without decryption. However, it is difficult to apply in an actual communication environment because the speed is slower than other encryption methods. In this study, we used fully homomorphic encryption and advanced encryption standards. And we built an end-to-end encryption communication network simulation environment that transmits data. Based on this, this study compares the transmission time according to the transmission environment. According to the experimental results of this study, a more effective encryption method can be selected and transmitted according to the length of the transmitted message, number of intermediate nodes, and encryption setting.**

Keyword— **Homomorphic encryption, network, communication, Advanced Encryption Standard, fully homomorphic encryption**

Hye-Yeon Shim received her BS degree from the Department of convergence security engineering at Sungshin University, Seoul, Korea. She is a student in an MS course in the Department of Convergence Security Engineering at Sungshin University, Seoul, Korea. Her current research interests are artificial intelligence, deep learning, malware detection, and programming.

Tae-Rim Park received her BS degree from the Department of convergence security engineering at Sungshin University, Seoul, Korea. She is a student in an MS course in the Department of Convergence Security Engineering at Sungshin University, Seoul, Korea. Her current research interests are artificial intelligence, communication, and convergence security.

Il-Gu Lee received his BS degree in electrical engineering from Sogang University, Seoul, Korea, in 2003 and his MS degree from the Department of Information and Communications Engineering at the Korea Advanced Institute of Science and Technology (KAIST) in Daejeon, Korea in 2005. He also received his MA degree in intellectual property from KAIST in 2012. He received his Ph.D. degree from the Graduate School of Information Security at the Computer Science and Engineering Department at KAIST in 2016. He is a professor at the Department of Convergence Security Engineering at Sungshin University (SU), Seoul, Korea. Before joining SU in March 2017, he was with the Electronics and Telecommunications Research Institute as a senior researcher from 2005 to 2017 and served as a principal architect and project leader for Newratek (KR) and Newracom (US) from 2014 to 2017. His current research interests are wireless/mobile networks with an emphasis on information security, networks, wireless circuits, and systems. He has authored/coauthored more than 55 technical papers in the areas of information security, wireless networks, and communications and holds about 160 patents. He is also an active participant of and contributor to the IEEE 802.11 WLAN standardization committee.