5. Conclusions

In this work, we proposed a new construction of an OPEnc scheme based on an OREnc scheme with the optimal client storage and round complexities. The security of the resulting OPEnc scheme is at least as strong as the underlying OREnc's security. We also gave comparison result our construction with the existing ideally-secure OPEnc schemes in terms of efficiency and security. Finally, from our construction, we showed that it's theoretically possible to construct a non-interactive ideally-secure OPEnc scheme with a constant client-side storage.

Acknowledgement

This work was supported by research grants from Daegu Catholic University in 2019.

References

[1] F. Kerschbaum, "Frequency-hiding order-preserving encryption," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, CO, 2015, pp. 656-667.

[2] D. S. Roche, D. Apon, S. G. Choi, and A. Yerukhimovich, "POPE: partial order preserving encoding," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 2016, pp. 1131-1142.

[3] N. Chenette, K. Lewi, S. A. Weis, and D. J. Wu, "Practical order-revealing encryption with limited leakage," in *Fast Software Encryption*. Heidelberg: Springer, 2016, pp. 474-493.

[4] K. Lewi and D. J. Wu, "Order-revealing encryption: New constructions, applications, and lower bounds," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 2016, pp. 1167-1178.

[5] D. Boneh, K. Lewi, M. Raykova, A. Sahai, M. Zhandry, and J. Zimmerman, "Semantically secure order-revealing encryption: multi-input functional encryption without obfuscation," in *Advances in Cryptology – EUROCRYPT 2015*. Heidelberg: Springer, 2015, pp. 563-594.

[6] E. Miles, A. Sahai, and M. Zhandry, "Annihilation attacks for multilinear maps: cryptanalysis of indistinguishability obfuscation over GGH13," in *Advances in Cryptology – CRYPT 2016*. Heidelberg: Springer, 2016, pp. 629-658.

[7] J. H. Cheon, K. Han, C. Lee, H. Ryu, and D. Stehle, "Cryptanalysis of the CLT13 multilinear map," *Journal of Cryptology*, vol. 32, no. 2, pp. 547-565, 2019.

Kee Sung Kim https://orcid.org/0000-0001-9160-8692

He received M.S. and Ph.D. degrees in Graduate School of Information Security from Korea University, Seoul, Korea, in 2011 and 2015, respectively. He is currently an assistant professor at School of Information Technology Engineering, Daegu Catholic University, Korea. His research interests focus on cryptography, database security, privacy enhancing technology, and secure protocols.