An Improved Scenario for IoT Position Based Public-Key Lattice Cryptography

Mohammad A. Alia[1],

[1] *Faculty of Science and Information Technology, Al Zaytoonah University of Jordan*

Amman- Jordan P.O.Box: 130 Amman (11733) Jordan

dr.m.alia@zuj.edu.jo

Abstract: With the rapid evolution of the internet applications, internet of Things becomes one of today's hottest research areas due to its ability to interconnected things together which reduce costs associated with computing. Many IoT advantages are incorporated with our lives, which can help businesses, individuals, and society on a daily basis. IoT is Internet based computing due to shared resources and information which are dynamically delivered to consumers. However, IoT communications are vulnerable to attack during the party credentials possesses to verify him/her self. Therefore, this paper will explore verification technique for IoT by implementing Lattice Cryptography based cerographical position verification. The proposed scenario develops a problem transformation technique that enables prover to secretly transform information with verifiers. This work proposes the Lattice key exchange cryptographic protocols to enhance the security of the IoT accessibility. However, the proposed scenario is secure, easy and straightforward process. The position based Lattice key exchange protocol ensure the security of the proposed scenario. Though, the Lattice of the key size becomes crucial to prevent a brute force attack. Lattice problems offer the possibility of faster cryptographic protocols.

Keywords: Lattice, IoT, Security, and Cryptography.

References

[1] D. Evans (2011). The Internet of Things, How the Next Evolution of the Internet, Is Changing Everything. Cisco Internet Business Solutions Group (IBSG).

[2] R. James (2016). IoT Security Risks: How People Can Protect Their Network Of Devices. Available online: https://www.informationsecuritybuzz.com/articles/iot-security-risks-people-can-protect-network-devices/

[3] M. Elkhodr, S. Shahrestani, H. Cheung (2016). The Internet of Things: New Interoperability, Management And Security Challenges. International Journal of Network Security

[4] D. Chen, G. Chang, L. Jin, X. Ren, J. Li, F. Li (2011).A Novel Secure Architecture for the Internet of Thing. 2011 Fifth International Conference on Genetic and Evolutionary Computing.

[5] A. Luigi, I. Antonio, M. Giacomo (2010). The Internet of Things: A survey, Computer Networks, vol. 54, No. 15, pp. 2787-2805.
[6] N. Chandran, V. Goyal, R. Moriarty, R. Ostrovsky (2009). Position Based Cryptography In: Halevi S. (eds) Advances in Cryptology - CRYPTO 2009. CRYPTO 2009. Lecture Notes in Computer Science, vol 5677. Springer, Berlin, Heidelberg
[7] J. Bos, C. Costello, M. Naehrig, D. Stebila, Post-quantum key exchange for the TLS protocol from the ring learning with errors problem, in Proceedings of the IEEE Symposium on Security and Privacy, 2015.
[8] E. Alkim, L. Ducas, T. PÃppelmann and P. Schwabe, Post-quantum key exchange " a new hope, IACR Cryptology ePrint Archive, Report 2015/1092, 2015.
[9] Luca De Feo 2017, Mathematics of Isogeny Based Cryptography. CoRR, abs/1711.04062
[10] R. A. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystemsâ€, Communications of the ACM, 21(2), pp.120-126, 1978.
[11] W. Diffie, and M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, IT-22, pp. 644-654, 1976.
[12] E. L. Antonsen (2017). Lattice-based cryptography, A comparative description and analysis of proposed schemesâ€. Reprosentralen, University of Oslo.
[13] B. Elaine, W. Barker, W. Burr, W. Polk, and M. Smid, Recommendation for Key Management, Part 1: Generalâ€, NIST Special Publication 800-57, 2006.