Abstract

NTRU is an open-source public key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data. Unlike other popular public-key cryptosystems, it is resistant to attacks using Shor's Algorithm and its performance has been shown to be significantly greater. This paper talks about how Koblitz encoding from Elliptic Curve Cryptography (ECC) can be used to convert each character in a dataset to a point on an elliptic curve. A sum of squares analogy is pitted against the cantor pairing function to turn the point to a single number, which is converted to a sequence of coefficients in $\mathbb{Z}$. A polynomial is then generated for each of these characters. Then the polynomial is reduced, and then shown that choosing appropriate parameters for the cryptosystem can make it highly secure and that the decryption algorithm turns out taking linear time. Since each character is represented by its own polynomial, it increases obscurity thereby increasing the complexity for decryption and thus the security level. A form of data compression has also been implemented and it has been tested whether data compression and expansion during the encryption-decryption process results in original data with no or minimal loss.
References

1. Ajtai, M. (1996). Generating Hard Instances of Lattice Problems. ACM Symposium on Theory of Computing. Philadelphia, Pennsylvania: Association for Computing Machinery. doi:https://dl.acm.org/doi/10.1145/237814.237838

2. Brady, R., Davis, N., & Tracy, A. (2010, July). Encrypting with Elliptic Curve Cryptography. Retrieved from https://www.math.purdue.edu/~egoins/notes/Encrypting_Text_Messages_via_Elliptic_Curve_Cryptography.pdf.

3. Menon, U., & Bhowmik, A. (2020, March). NTRU Cryptography. Retrieved from https://github.com/7enTropy7/NTRU_cryptography.

4. Micciancio, D. (2005). Closest Vector Problem. SpringerLink. doi:https://doi.org/10.1007/0-387-23483-7_66.

5. Micciancio, D. (2005). Shortest Vector Problem. SpringerLink. doi:https://doi.org/10.1007/0-387-23483-7_392.

6. NTRU. (n.d.). Retrieved from LatticeHacks: https://latticehacks.cr.yp.to/ntru.html.

7. Silverman, J. H. (2015, January 12-16). NTRU and Lattice-Based Crypto: Past, Present, and Future. The Mathematics of Post-Quantum Cryptography. Retrieved May 19, 2020, from http://archive.dimacs.rutgers.edu/Workshops/Post-Quantum/Slides/Silverman.pdf.

8. Stallings, W. (2017). Finite Fields. In W. Stallings, The principles and Practice of Cryptography and Network Security 7th Edition (Vol. 20, pp. 123-152). Pearson Education.

9. Szudzik, M. (2006). An Elegant Pairing Function. Washington, DC. Retrieved from http://szudzik.com/ElegantPairing.pdf.

10. Union of Equivalence Classes is Whole Set. (n.d.). Retrieved from ProofWiki: https://proofwiki.org/wiki/Union_of_Equivalence_Classes_is_Whole_Set.

11. Zhang, Z. (2017, July 12). A short review of the NTRU cryptosystem. Retrieved from https://www.slideshare.net/OnBoardSecurity/a-short-review-of-the-ntru-cryptosystem.

Index Terms

Computer Science    Security

Keywords

Post quantum cryptography, lattice-based encryption, quantum cryptography, Koblitz encoding, post quantum cryptosystem, ntru cryptography, ntru cryptosystem.