Abstract

Tripathi and Thakur proposed a new variant of NTRU cryptosystem [8] by using the Exclusive-OR operation. They proposed this system under the same general principles as that of the NTRU cryptosystem except the logical operators “Exclusive-OR” with the different bit size for encryption and decryption are used in place of truncated polynomial in NTRU cryptosystem. In this article we discuss some shortcomings of the scheme [8] and argue that the proposed scheme is not practical and secure.

References

   Key Authentication. In Proceeding of CryptTCS’99, City University of Hong-Kong Press, 7-19.
   Generation Based on Truncated Polynomials. International Journal of Computer Science and
   Network Security, 6.(8B, 156-161.
8. Tripathi, B.P. and Thakur, K. 2015. A logical XOR operation for NTRU Cryptosystem,

Index Terms

Computer Science Security

Keywords

NTRU Cryptosystem, Logical XOR operation, Boolean Algebra.