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

On Logical Operation for NTRU Cryptosystem


Index Terms
Computer Science  Security

Keywords
NTRU Cryptosystem, Logical XOR operation, Boolean Algebra.