Abstract

The NTRU public key cryptosystem was first presented by J. Hoffstein, J. H. Silverman and J. Pipher in 1996. This system is based on shortest and closest vector problem in a lattice and operations based on objects in a truncated polynomial ring. In this paper we propose new variant of NTRU cryptosystem which is based on logical exclusive OR operator. This system works 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 which are used in place of truncated polynomial in NTRU cryptosystem. We also calculate the time complexity which shows that this system is faster than NTRU cryptosystem.

References

2. J. Hoffstein, D. Lieman, J. Silverman “Polynomial Rings and Efficient Public Key
Authentication", Proceeding of the International Workshop on Cryptographic Techniques and
Generation Based on Truncated Polynomials". IJCSNS International Journal of Computer

Index Terms
Computer Science Applied Mathematics

Keywords
NTRU, logical operator, Boolean function, Encryption, Decryption.