BTRU, A Rational Polynomial Analogue of NTRU Cryptosystem

Abstract

NTRU is a public key cryptosystem based on polynomial ring over Z. Replacing Z with the ring of polynomial in one variable α over a rational field. In this paper the complexity of BTRU cryptosystem is faster than NTRU cryptosystem.

References

5. J. Hoffstein, J. Pipher, J. H. Silverman, An Introduction to Mathematical Cryptography,

Index Terms

Computer Science

Information Sciences

Keywords

NTRU, Rational Field, Encryption, Decryption