Abstract

The NTRU cryptography is a lattice-based public key cryptography. Encryption and decryption process in NTRU are based on polynomial multiplication. This property makes NTRU to be very fast compared to other public key cryptography algorithm such as elliptic curve cryptography and RSA. In order to fast implementation of NTRU, hardware implementation of NTRU by employing residue number system is presented. To achieve high speed implementation, balanced three moduli set \{2^n, 2^{n+1}-1, 2^{n-1}\} is considered and the encryption and part of decryption process are implemented by considered RNS bases. The result shows the noticeable improvement compared to original NTRU cryptography.

References


6. Efficient NTRU Implementations: A Thesis Submitted to the Faculty of the Worcester Polytechnic Institute In partial fulfillment of the requirements for the Degree of Master of Science in Electrical & Computer Engineering by Colleen Marie O'Rourke - April 2002


Index Terms

Computer Science  Security

Keywords

NTRU cryptography, Residue number system, Reverse converter, Forward converter