Abstract

This work proposes a lattice-based cryptosystem using embedded technique of the closest vector problem (CVP). It adopts the key-gen algorithms of [1], and improves on vector reduction method for encryption/decryption. With this we achieved great implementation speed and time for an acceptable security parameter.

References

Development of a Lattice-based Cryptosystem

University of Technology, Akure, Nigeria.


Index Terms

Computer Science
Security

Keywords

Lattice-based Cryptography
Quantum
Cryptography
Closest Vector Problem
Lattices
Quantum.