Duy Nhan Cao

CS 415

Apr 6, 2018

Final Paper Proposal

Lattice-based cryptography

Lattice-based cryptography is the generic term for constructions of cryptographic primitives that, either in the construction itself or in the security proof, involve lattices. Under the threat of quantum computer, which renders widely used and known public-key schemes like RAS, Diffie-Hellman or even Elliptic-Curve vulnerable, lattice-based appear to be resistant to attack by both classical and quantum computers. It, however, is secure under the assumption that certain well-studied computational lattice problems cannot be solved efficiently.