量子コンピュータと格子暗号

Quantum Computers and Lattice Cryptography

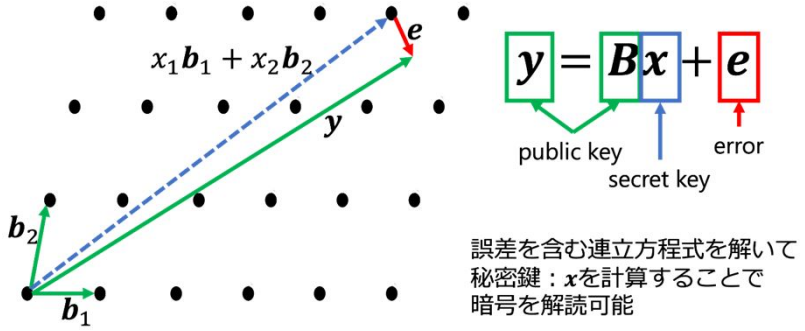
小倉朱門・暗号認証分科会・中央大学大学院

耐量子計算機暗号

量子コンピュータにより，現在の暗号が破られる→耐量子計算機暗号の必要

格子暗号

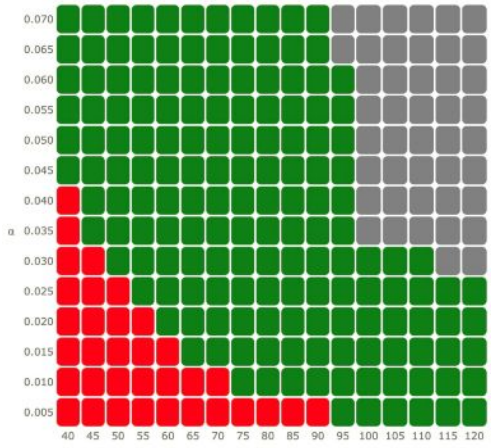
格子問題(LWE問題など)に基づく暗号



本年度は格子暗号の基礎を一般の人に理解できる説明を試みた

今後の研究内容

- 格子暗号解読(LWE Challenge, SVP Challenge etc.,)の状況の調査
- 格子暗号に対する攻撃方法の調査と一般の人に向けた説明方法の検討



LWEチャレンジの解読状況(2024/02/20)
https://www.latticechallenge.org/lwe_challenge/challenge.php