NTRU暗号評価の現状報告 (スクリーニング評価)

平成14年1月28日

公開鍵暗号評価小委員会
委員　小暮　淳

NTRU暗号(応募者の主張)

- 応募暗号種別：守秘
- 安全性の根拠：CML(Convolution Modular Lattice)のSVP(Shortest Vector Problem)
- 証明可能安全性：①プリミティブをrandom paddingによりIND-CPA化②Fujisaki-Okamoto変換(random oracleモデルを仮定)によりIND-CCA2化
- 特長： 暗号化/復号速度が速い
- SW実装情報： Pentium III 800MHz, Palm Vx 20MHz , RIM 20MHz , ARM7 37MHz

スクリーニング評価状況
(仕様に関して)

以下の点の明確化が必要

- パラメータ設計基準
- 基本関数、補助関数への要求仕様
- 秘密鍵生成成功確率に関する評価
- 暗号文が大きくなることに関する評価

スクリーニング評価状況
(安全性に関して)

以下の点の詳細確認が必要

- パラメータ設計方針の妥当性
- random paddingされたプリミティブがIND-CPAとなること
- ショートカット解法の可能性