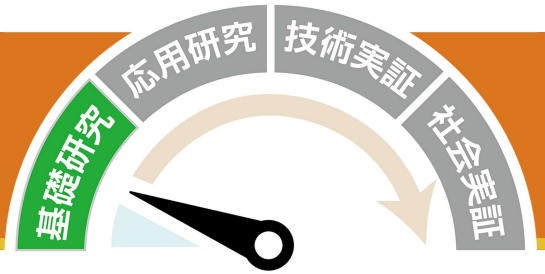
C 03

サイバーセキュリティ

耐量子計算機暗号の安全性評価

～ 量子コンピュータ時代に必要となる暗号技術とその標準化活動 ～

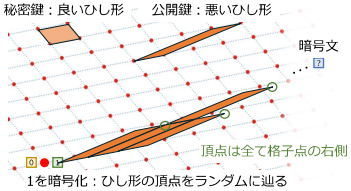


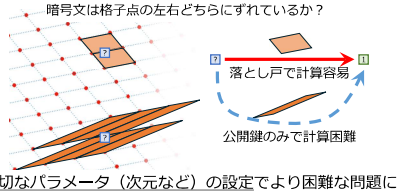
概要

量子コンピュータの実用化を見据え、耐量子計算機暗号（PQC）の研究開発や標準化が国内外で活発に進められています。PQCの信頼性確保に向けた安全性評価の取り組みと、それに連動する国内外の標準化動向について紹介します。

格子暗号（格子問題の求解困難性に基づく暗号技術）

格子	格子暗号	格子暗号の安全性
規則的に並んだ点の集合	基準格子点からのずれ方を利用	暗号文の座標から最も近い格子点の探索が計算量的に困難

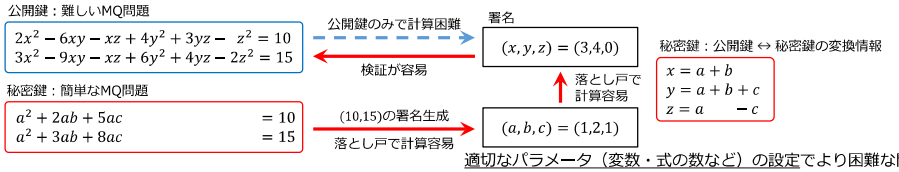




適切なパラメータ（次元など）の設定でより困難な問題に

多変数公開鍵暗号（MQ問題の求解困難性に基づく暗号技術）

MQ問題	多変数公開鍵暗号	多変数公開鍵暗号の安全性
二次の項を含む連立方程式	特殊な構造を持つMQ問題を利用	公開鍵のMQ問題の求解が計算量的に困難



適切なパラメータ（変数・式の数など）の設定でより困難な問題に

世界記録達成

- 格子問題の求解チャレンジ

例：いくつかの問題で**世界記録**

- MQ問題の求解チャレンジ

例：37変数74式の問題で**世界記録**

標準化活動への貢献

CRYPTREC Cryptography Research and Evaluation Committees

- PQCガイドラインの策定
  PQCの国内標準化（予定）

NIST

- PQC標準化プロジェクト
  例：FIPS 203-205の標準化

特徴

- 格子暗号、多変数公開鍵暗号の安全性評価
- 求解問題での世界記録を達成
- PQCガイドラインの策定・改定

格子問題　MQ問題　CRYPTREC

ユースケース

- 量子コンピュータ時代でも安全な暗号技術の設計
- PQC移行に向けたセキュリティ基盤の整備
- PQCに関する国内外の標準化活動に貢献

今後の展開

- 新しい安全性評価手法の提案、世界記録への挑戦
- より適切な暗号パラメータの選定に貢献
- PQC国内標準・PQC移行の検討

【お問合せ先】
サイバーセキュリティ研究所 セキュリティ基盤研究室
Mail：security@ml.nict.go.jp

NICT オープンハウス 2025