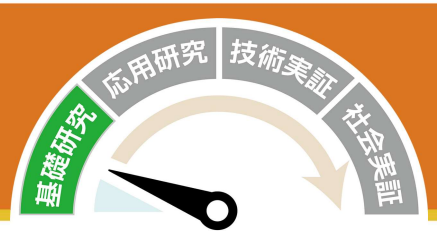
C 04 サイバーセキュリティ

次世代暗号: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向けた新しい暗号の必要性と標準化に向けて ～



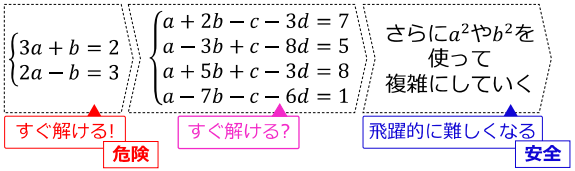
概要

量子コンピュータを用いても解読困難な暗号は耐量子計算機暗号(PQC)と呼ばれ、その標準化に向けて実用性と安全性の評価が求められています。安全性評価には理論的な部分だけでなく、実際にどこまでの問題を解けるのかの検証も重要です。

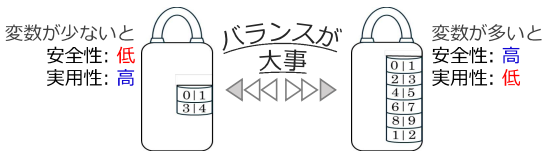
暗号の歴史: 情報通信技術の発展と共に、より複雑で安全な暗号が求められるように

現代の暗号の多くは「現実的な時間内では解けない」ことで安全性を担保している

例: 方程式を解くと暗号が解ける多変数暗号

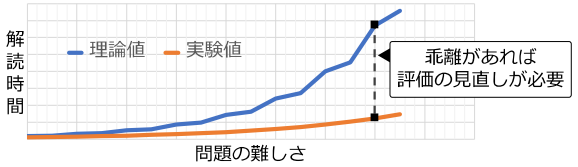


複雑にすれば安全性は向上するが、
処理速度などの実用性が下がるトレードオフも



理論上は安全でも、実環境で解読してみたら危ないとわかることも

例: 安全性評価の実験結果のイメージ



当研究室では解読手法の理論の研究とともに、実際に解読を行うことで暗号技術の安全性評価を行っている

多変数暗号の問題を解く
国際コンテストにて
世界記録を達成(2019)

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価の結果を
政府の暗号技術ガイドラインに
反映(2022)

特徴

- 新たな解読手法の提案、それを使用した安全性評価
- 暗号の安全性評価では理論値と実験値の両方が大切

ユースケース

- 量子コンピュータ時代でも安全な暗号の設計
- 近未来に向けたセキュリティ基盤の整備
- PQCガイドライン策定などの標準化活動に貢献

今後の展開

- 安全な暗号技術の利用促進
- 別の新たな解読手法の提案
- より適切な暗号パラメータの選定

【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2024