資料8－2
※一部非公開資料※

ICTサイバーセキュリティ政策分科会第８回会合

「安全な無線通信サービスのための新世代暗号技術に関する研究開発」について

株式会社KDDI総合研究所、国立大学法人横浜国立大学

2024年５月27日

背景と目的

【背景】

- 大規模な量子コンピューターにより、現行の公開鍵暗号はすべて現実的な時間で解読できるようになる。共通鍵暗号に関しても、量子コンピューターにより鍵の探索処理が効率化される。
- 共通鍵暗号に関しては、鍵長を256ビット（現行の2倍）に伸ばすとともに、B5G/6Gでさらに高速・大容量化する通信に対しボトルネックを生じさせないよう、100Gbpsを超える処理速度を実現する必要がある。
- 公開鍵暗号に関しては、量子コンピューターに耐性を持つ耐量子計算機暗号への置き換えが必要となる。これに伴い、鍵長やデータ長が増大するため、通信のオーバヘッドを削減する技術も必要となる。

【目的】

- 鍵長を256ビットにしつつ、 処理速度200Gbps超を達成でき、処理時間を従来方式と比較し、最大50%削減できる高速共通鍵暗号を設計する。
- 様々なユースケースに合わせた耐量子公開鍵暗号の最適化技術等を確立し、通信の最重要項目におけるオーバヘッドを8%以内に抑えることで、電波の有効利用を図る。

技術課題と計画

技術課題ア 高速共通鍵暗号
５Ｇ等のための超高速・大容量に対応した共通鍵暗号方式技術

R3: 安全性・機能性評価指針の検討 → R4:アルゴリズムの設計、安全性評価・実装評価(一部前倒し) → R5:アルゴリズムの安全性評価・実装評価 → R6：無線通信環境での実証評価

技術課題イ耐量子コンピュータセキュリティ技術
５Ｇ等のための耐量子計算機暗号(公開鍵暗号)の機能付加技術等

R3:耐量子計算機暗号の機能評価 → R4: 機能拡張技術・最適化技術・管理運用技術の構築 → R5:技術の改良・特定ユースケースでの評価 → R6：無線通信環境での実証評価

研究開発の全体像

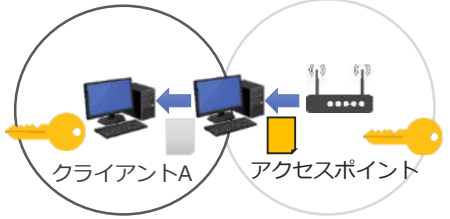
技術課題ア：５Ｇ等のための超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号）

アー①　高速共通鍵暗号方式の設計

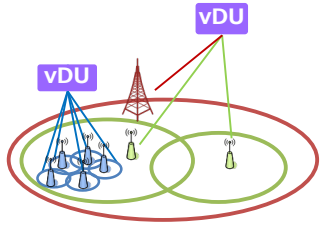
暗号方式の設計・安全性評価

アー② 高速共通鍵暗号方式の評価

評価指針の選定・実装評価



無線通信プロトコル・実装の安全性評価



無線通信環境での評価

技術課題イ：５Ｇ等のための耐量子計算機暗号の機能付加技術等（耐量子コンピュータセキュリティ技術）

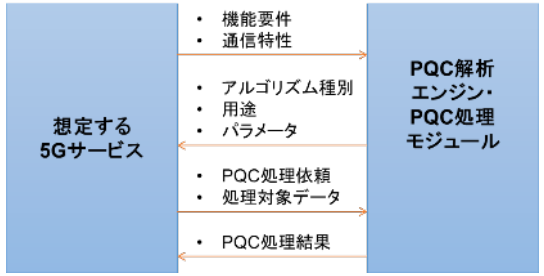
イー① 耐量子計算機暗号への機能付加技術

各種耐量子計算暗号の理論解析・安全性評価・機能付加等

イー④ 物理層セキュリティ技術

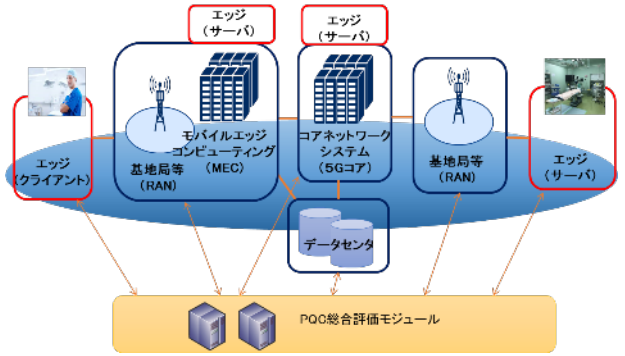
物理層セキュリティ技術、サイドチャネル対策技術等の確立

イー② ５Ｇのアプリケーションに特化した耐量子計算機暗号の管理運用技術



管理運用技術のためのセキュリティ用プロトコル設計

イー③ ５Ｇアプリケーション上の耐量子計算機暗号の最適化技術



耐量子計算機暗号の最適化技術と総合評価

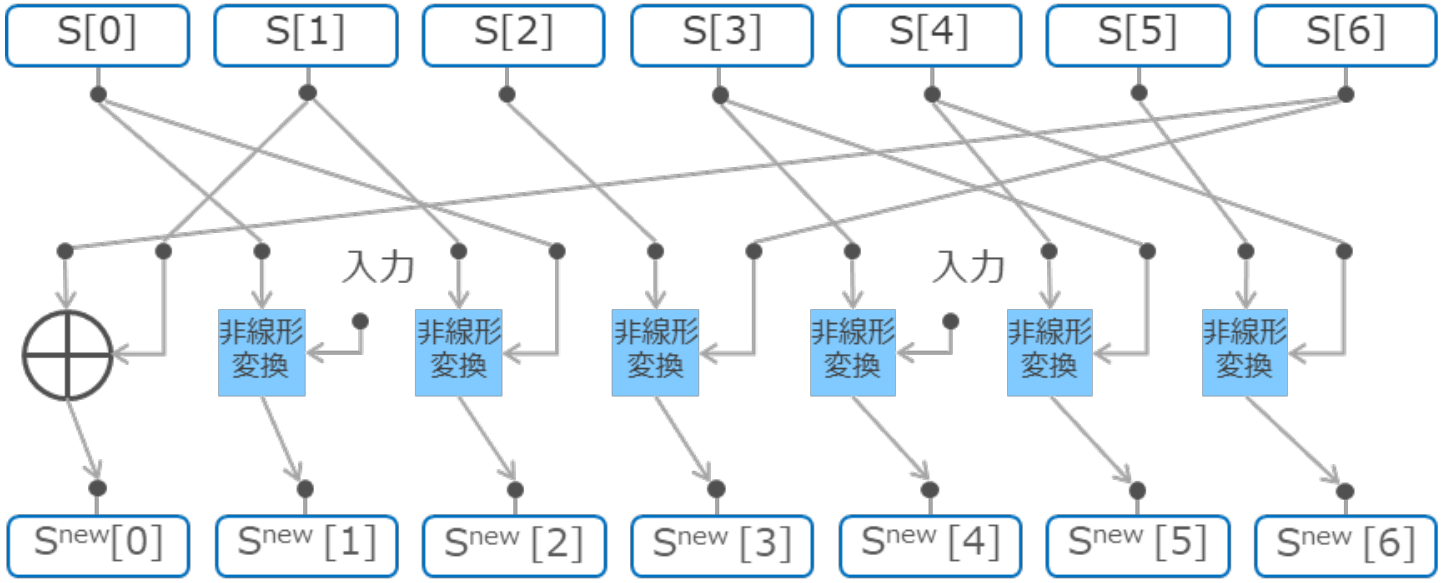
研究開発体制

- 研究開発課題：安全な無線通信サービスのための新世代暗号技術に関する研究開発
  - 安全な無線通信サービスのための新世代暗号技術に関する研究開発運営委員会
  - 技術課題ア：超高速・大容量に対応した共通鍵暗号方式技術（高速共通鍵暗号）（代表研究機関：KDDI総合研究所）
    - アー① 高速共通鍵暗号方式の設計（兵庫県立大学）
    - アー② 高速共通鍵暗号方式の評価
      - アー②－１　実装技術の確立（KDDI総合研究所）
      - アー②－２　無線通信プロトコル・実装の安全性評価（神戸大学）
      - アー②－３　無線通信プロトコルにおける評価（国際電気通信基礎技術研究所）
  - 技術課題イ：5G等のための耐量子計算機暗号機能付加技術等（耐量子コンピュータセキュリティ技術）（代表研究機関：横浜国立大学）
    - イー①耐量子計算機暗号への機能付加技術
      - イー①－１　PQCに対する機能拡張技術の開発（横浜国立大学）
      - イー①－２　PQCに対する構造を踏まえた安全性解析（情報通信研究機構）
      - イー①－３　同種写像問題、多変数多項式求解問題（MQ問題）に基づくPQCの解析・評価（東京大学）
      - イー①－４　格子問題、符号復号問題に基づくPQCの解析・評価（大阪大学）
      - イー①－５　不定方程式求解問題に基づくPQCの解析・評価（東芝）
    - イー② ５Gのアプリケーションに特化した耐量子計算機暗号の管理運用技術（国際電気通信基礎技術研究所）
    - イー③ ５Gアプリケーション上の耐量子計算機暗号の最適化技術（国際電気通信基礎研究所）
    - イー④ ５Gに適応する物理層セキュリティ技術開発
      - イー④－１　５Gにおける物理層セキュリティ技術開発（横浜国立大学）
      - イー④－２　PQCと物理層セキュリティ技術の連携・融合技術の開発（横浜国立大学）
      - イー④－３　PQCにおけるサイドチャネル攻撃への対策技術の開発（東京大学）

【技術課題ア 高速共通鍵暗号】これまでの主要な成果

■ 高速共通鍵暗号の設計を完了

- ソフトウェア実装で227Gbps、ハードウェア（ASIC）実装で2.02Tbps（ともに世界最速）の処理速度を達成。



■ 統合評価に向けた開発

- 評価基盤として選定したエミュレーション環境（Open Air Interface）に高速共通鍵暗号を実装し、動作検証を完了。
- ソフトウェア無線装置を用いた無線通信検証環境を構築。課題イとの評価環境を統合し、動作検証を完了。

投影限り

【技術課題イ 耐量子コンピュータセキュリティ技術】これまでの主要な成果

■ 画期的な耐量子計算機暗号（PQC）基礎技術を開発

- 同種写像問題に基づく新たな鍵共有方式を開発し、トップクラス国際会議EUROCRYPT 2023で発表（東京大学）
- 格子問題に基づくディジタル署名の高速化を開発し、トップクラス国際会議ASIACRYPT 2023で発表（大阪大学）

■ 実用的なPQCベース高機能暗号技術を開発

- 格子問題に基づく実用的なIDベース暗号の拡張方式（IDベースマッチング暗号）を開発（横浜国立大学）
  提案方式では、従来方式に比べて復号鍵サイズは約1/72のサイズ、暗号文サイズは約1/7のサイズ
- 同種写像問題に基づく実用的なIDベース署名を開発し、国際会議PQCrypto 2023で発表（横浜国立大学）
  提案方式では、従来方式に比べて鍵サイズは約1/20のサイズ、署名サイズは約1/250のサイズ
- 格子問題に基づく実用的な集約署名（アグリゲート署名）を開発（横浜国立大学）
  提案方式では、2^{10}個（約1000個）の署名を集約した場合の集約署名サイズは従来方式の約1/10のサイズ

■ CRYPTREC暗号技術ガイドラインへの貢献

- 本研究開発で得られた耐量子計算機暗号の高機能化・最適化技術や安全性評価手法に関する知見を活用し、 CRYPTREC暗号技術ガイドライン（高機能暗号・耐量子計算機暗号）を執筆することで、研究成果を社会に還元
  （横浜国立大学、東京大学、NICT）

投影限り

今後の取り組み

- PQCの更なる性能向上（暗号文・署名のサイズ、処理速度、安全性等）、パラメータ選定、運用指針、機能拡張など、PQCの導入に向けた課題を引き続きコンソーシアムで検討する。
- 高速共通鍵暗号方式や耐量子計算機暗号の機能付加技術について、国際標準化に向けた活動を引き続き推進する。国際標準に採用されることで、わが国発の次世代暗号技術が、世界的に普及することが期待される。
- 研究成果の一部オープンソース化も実施している。様々なサービスに導入されセキュリティ向上に資することが期待される。
- 世界トップレベルの研究成果を継続して創出できる人材の育成を継続し、研究成果の社会還元を促進しながら我が国の技術力の引き上げにも寄与する。