課題096

移動体通信システムに実装する耐量子計算機暗号技術等に関する研究開発

次期移動体通信システム等への実装が想定される耐量子計算機暗号（PQC）等の次世代暗号について、高水準の安全性を確保しつつモバイル環境での実用に適した暗号設計や、より確実な暗号移行を支援する技術の研究開発を実施し、将来における円滑な暗号移行と電波の有効利用を図る。

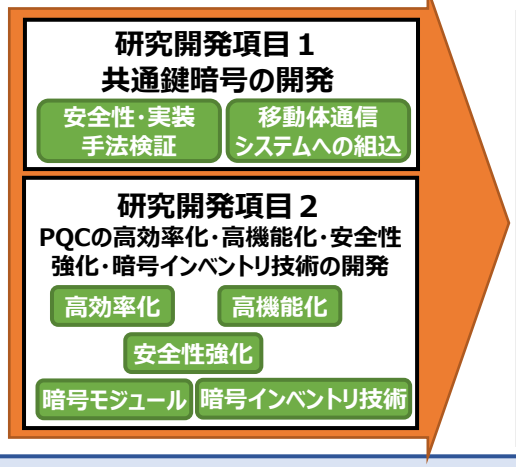
背景

現在の移動体通信システム等に実装されている従来型公開鍵暗号は、大規模量子コンピュータの開発･実用化の進展等に伴って、容易に解読されるリスクが高まるため、適切な時期に耐量子計算機暗号（PQC）に移行する必要がある。一方で、現行のPQCは、現代暗号に比べデータサイズの増大と暗号化･復号にかかる計算量の増加により、不適切な設定では無線リソースを圧迫する懸念がある。この課題を解決するためには、PQC及びこれとともに使用される共通鍵暗号について、 次世代移動体通信システム等の特徴を加味した上で、システムや利用者への影響を極力抑えて利用できるようになることが求められる。

概要

次世代移動体通信システム等への実装を念頭に、次世代暗号技術の安全性を確保しつつ高効率かつ安全な暗号の研究開発を実施する。また、既存の移動体通信システム等において移行が必要な暗号をリストアップし、円滑かつ迅速な移行を促進する、暗号インベントリ技術等の研究開発を行う。

- **研究開発項目１　量子コンピュータに対する安全性を確保した共通鍵暗号の移動体通信プロトコル等への導入に関する研究開発**
  - a) **新たな共通鍵暗号の安全性評価及び効率的な実装手法の検証**：次世代移動体通信システムにおいて導入すべき暗号方式を明らかにし、各種機能要件を満たす適切な利用モードを設計する。また、従来の攻撃手法に対する安全性評価に加え、量子アルゴリズムを含む最新の攻撃手法の適用の可否を検証する。
  - b) **移動体通信規格への組み込み手法の検証**：次世代の移動体通信システム等標準規格のプロトコルにa)で得られた最適な暗号方式及び利用モードを組み込み、Beyond5Gの移動体通信システムにおける暗号関連プロトコルを模擬した評価環境にて100Gbps以上の暗号処理を達成するとともに、従来の5G等の移動体通信システム等との後方互換性を検証・評価する。
- **研究開発項目２　PQCの高効率化・高機能化・安全性強化及び移行支援技術の研究開発**
  - a) **PQCの高効率化・高機能化・安全性強化及び次世代暗号モジュールの開発**：PQCの方式及び実装の改良による高効率化、高機能化及び安全性強化に関する研究開発を実施するとともに、国産暗号実装技術に基づく次世代暗号モジュールの開発等を実施する。
  - b) **暗号インベントリ技術の開発**：危殆化のおそれのある暗号をシステム内から検出する暗号インベントリ技術を開発する。



研究開発期間：契約締結日から2028年度（2026年度のステージゲート評価を踏まえ、継続の必要性等が認められた場合には、最長で2028年度まで継続予定。）

研究開発予算：総額2,000百万円（税込）を上限とし、最初の2年間での累計額上限を１,000百万円（税込）とする。　採択件数：１件