別添１

＜基本計画書＞

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

１．目的

４Ｇや５Ｇといった無線通信において広く利用されている暗号技術については、近い将来実用化が想定される大規模量子コンピュータに、できるだけ早く対応していく必要がある。

公開鍵暗号方式については、実用的な大規模量子コンピュータが登場した場合、Shor のアルゴリズムにより多項式時間で効率的に解けるようになり、指数的な解読速度向上をもたらすことから、暗号として利用することができなくなる。このため、耐量子計算機暗号（Post-Quantum Cryptgraphy:PQC）と呼ばれる、大規模量子コンピュータにおいても計算困難性を有する新しい種類の暗号技術への移行が必要である。現在、PQC として様々な暗号技術が開発・提案されているが、現在公開鍵暗号方式として利用されている RSA 暗号の仕組みを利用した Post-quantum RSA 暗号を利用する場合、暗号文サイズは１ギガバイト（＝2^30 バイト）以上が必要であり、これは従来の RSA 暗号で必要とされる 2048 ビット（＝2^8 バイト）に比べて段違いに大きいサイズとなる。この場合、通信路を流れる膨大な暗号文データのため帯域がひっ迫することになる。その他、多数の PQC の方式が提案されており、例えば鍵長が長いが暗号文サイズが小さいものといったように、鍵長や暗号文サイズ、鍵生成や暗号化処理の時間といった多くの要素においてトレードオフの関係になっている（例えば、米国 NIST（国立標準技術研究所）に提案されている PQC の鍵長を見ても、数百バイト程度のものから数百キロバイト程度のものまで多様である。）。

また、共通鍵暗号方式については、大規模量子コンピュータを用いても Shor のアルゴリズムのような効率的な解法は知られていないものの、Grover のアルゴリズムにより従来の古典コンピュータに比べて鍵探索の速度向上が可能となるため、鍵長をおよそ２倍程度の 256 ビットに増やすことが必要とされている。鍵長が増えると、暗号化に要する計算量や処理に要する時間も増えることとなり、処理能力が同じであると仮定すると、単位時間当たりに処理可能なデータ量は減少することとなる。このため、数十 Gbps といった超高速通信においては、暗号化処理がボトルネックとなることが想定され、無線リソースを有効活用できない状態となる。

本研究開発は、大規模量子コンピュータの利用を想定し、５Ｇ及びより高度な無線通信が求める超高速・大容量・多用途に対応した新世代暗号技術に関する研究開発を実施する。具体的には、鍵長を 256bit にしても暗号化処理に要する計算量や処理時間を約 50%低減させ、超高速な暗号処理を可能とする高速共通鍵暗号方式を設計するとともに、５Ｇ等が利用される様々なユースケースに応じて、オーバーヘッドがより少なくなるように公開鍵暗号に基づく耐量子計算機暗号(PQC)の機能付

加技術等を研究開発することで、暗号文サイズ等のオーバーヘッドを最大８％以内に抑えつつ大規模量子コンピュータへの安全性を担保しながら、限られた通信容量（無線資源）においてより多くのデータ送受信を可能とし、周波数のひっ迫状況の解消を図るものである。

２．政策的位置付け

〇統合イノベーション戦略 2020（令和２年７月 17 日閣議決定）

第Ⅲ部

第１章　知の源泉

（２）信頼性のある自由なデータ流通の実現及びデータ駆動型社会の社会実装

②目標に向けた施策・対応策

＜サイバーセキュリティ統合知的基盤の構築＞

〇５Ｇに対応したセキュリティ検証技術、ＩｏＴ機器や通信機器等のコネクテッドデバイスのセキュリティ検証技術のほか、データのセキュリティやプライバシーを確保し、安全なデータ流通と利活用を促進する技術の創出を行うとともに、暗号技術の安全性評価や耐量子計算機暗号などの新たな暗号技術の開発により、量子計算機時代に安全に利用できる暗号基盤技術を確立する。

〇サイバーセキュリティ研究・技術開発取組方針（令和元年５月 17 日　サイバーセキュリティ戦略本部　研究開発戦略専門調査会）

４．今後の取組強化の方向性

④ 暗号等の基礎研究の促進

＜具体的取組＞

既存の暗号システムの危殆化につながる量子コンピュータ等の国際動向を把握しつつ、耐量子計算機暗号や量子暗号等の安全なセキュリティ技術の研究・技術開発に取り組む。

３．目標

本研究開発では、５Ｇ、及びより高度な無線通信において、近い将来実用化が想定される大規模量子コンピュータに対応できるよう、①現状と同等の安全性を確保するために鍵長を倍にしつつ、超高速・大容量に対応した共通鍵暗号方式、②５Ｇ等の様々なユースケースに合わせた耐量子計算機暗号（PQC）への機能付加技術等を確立し、256 ビット鍵を用いた共通鍵暗号処理に係る時間を最大 50%削減すること、および PQC における暗号文サイズ等のオーバーヘッドを最大８％以内に抑えることで、無線通信リソースの効率的な利用環境を提供することにより、無線リソースのひっ迫を抑止し電波の有効利用を図る。

４．研究開発内容

(1) 概要

５Ｇ等無線通信の高度化においては、将来的に実用化が想定される大規模量子コンピュータに対応する必要があり、共通鍵暗号方式においては、鍵長の増加、公開鍵暗号方式においては、PQC への移行という課題がある。一方、それらの技術を適用する際には、５Ｇ等が求める超高速・大容量等の通信特性を損なわず、計算資源や通信リソースにも影響を与えないよう配慮する必要がある。

本研究開発では、５Ｇ等の特性を損なわない形で、①現状と同等の安全性を確保するために鍵長を 256 ビットにしつつ、超高速・大容量に対応した共通鍵暗号方式、②５Ｇ等の様々なユースケースに合わせた PQC への機能付加技術等を確立し、無線リソースのひっ迫を抑止することで電波の有効利用を図る。また、実用化に向けて暗号アルゴリズムや PQC 活用ガイドラインの国際標準化に取り組む。

(2) 技術課題および到達目標

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）

５Ｇ、及びより高度な無線通信(端末と基地局の間の通信)においては、さらなる高速大容量化が図られると考えられ、既存の暗号方式よりも高速な共通鍵暗号方式が求められる。また、大規模量子コンピュータが実用化されると鍵の解読にかかる計算時間が削減されるため、現在利用されている鍵長（128 ビット）を 2 倍に伸ばし、256 ビット鍵を利用可能とする必要がある。一般に、速度と鍵長はトレードオフの関係にあり、既存の暗号方式で 256 ビット鍵を使用した場合には、速度低下を引き起こすため、５Ｇ等の無線通信に求められるようなさらなる高速化は実現できない。そのため、計算機リソースが限られた携帯端末にも実装が可能であり、大規模量子コンピュータへの安全性を確保しながら、５Ｇ等に適した高速な共通鍵暗号方式の確立が必要となる。

また暗号方式は、最新の解読手法、及び耐用年数を考慮しても十分な安全性を保持することが求められるため、最新の攻撃手法を調査するとともに、将来想定される攻撃手法の改良に対しても検討を行う必要がある。併せて、暗号方式の実用性を評価するためには、実利用に近い環境において、その性能等を実証評価する必要がある。

本課題においては、大規模量子コンピュータに対する安全性を確保しつつ、暗号化処理に要する計算量や処理時間を低減させた高速共通鍵暗号方式の確立を目的として、以下の研究開発を行う。

①高速共通鍵暗号方式の設計

大規模量子コンピュータにおいても、現実的な計算時間で解読できず、かつ計算機リソースが限られた携帯端末にも実装が可能な、５Ｇ等が求める超高速・大容量に対応した共通鍵暗号方式の設計を行う。

②高速共通鍵暗号方式の評価

最新の攻撃手法を調査し、将来想定される攻撃手法の改良も考慮に入れた安全性評価指標を検討し、第三者評価も含め、高速共通鍵暗号方式の安全性評価を行う。加えて、セキュリティ機能のパッケージとして、耐量子性を持つ認証・鍵共有方式と組み合わせた無線通信プロトコルを実装し、無線通信環境において実証評価を行う。また、５Ｇ等の無線通信において、鍵の管理方法や鍵のライフサイクルが拡張される可能性も考慮して、課題イにおいて検討する耐量子計算機暗号である公開鍵暗号を用いた鍵共有と共通鍵暗号による暗号化を組み合わせた評価も行う。

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）

５Ｇ環境では、すでに規格化された暗号化、認証、鍵管理技術が活用されているが、５Ｇの高度化の一環として、将来の大規模量子コンピュータの実用化を見据え、５Ｇの特性を損なわずに、PQC 技術を実装する必要がある。

PQC に関しては、現在、米国 NIST（国立標準技術研究所）が標準化のための評価(NIST PQC)を実施しており、格子問題、線形符号の復号問題、多変数連立方程式の求解問題等の計算困難性に基づいた複数方式の選定が見込まれる。将来の大規模量子コンピュータの実現を想定した５Ｇ等の無線環境においてこれら PQC を利活用するためには、鍵長や暗号文サイズ、鍵生成・暗号化・復号の処理時間などをユースケース毎に適切に検討することによる、無線リソースを逼迫させないための PQC の選定、および当該方式におけるパラメータの選択などが重要となる。一例として、医療サービスにおける「遠隔手術」のユースケースを想定した場合、扱われる手術関連データの完全性、手術システムの可用性や低遅延性などが重要な特性と考えられ、これらの特性を加味した形で PQC の適用方法、実装方法の検討を進める必要がある。また、その際には、計算機リソースが限られた端末でも５Ｇの特性（低遅延等）を実現するため、物理層セキュリティについても併せて検討を行うことが重要となる。

本課題においては、５Ｇの様々なユースケースに応じてオーバーヘッドがより少なくなるような、NIST PQC の選定候補を含めた複数の PQC への機能付加技術、管理運用技術、最適化技術（総称して耐量子暗号系セキュリティ技術）、及び耐量子暗号系セキュリティ技術において計算機リソースをより効率的に利用するための物理層セキュリティ技術（耐量子暗号系セキュリティ技術と総称して耐量子コンピュータセキュリティ技術）を確立することを目的として、以下の研究開発を行う。

①耐量子計算機暗号への機能付加技術

通信事業者が提供する５Ｇ基盤サービスを対象として、５Ｇの特性を維持した上で、既存の鍵配送方式、公開鍵暗号方式等を、耐量子計算機暗号と置き換えるための耐量子計算機暗号への機能付加技術の研究開発を実施する。具体的には、暗号文サイズを削減することで高速大容量通信の効果を上げ、暗号に動的アクセス制御機能等を付加することによりネットワーク内端末の多数接続状態を安全に管理し、復号時間を削減することで低遅延の効果を上げるための研究開発を行う。

②５Ｇ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

医療系、交通系等、５Ｇを活用する様々なセクタにおけるユースケースを整理し、ユースケース毎に異なるセキュリティの機能要件（機密性、完全性、可用性等）を明確にすることで、５Ｇに対応した耐量子暗号系セキュリティ技術の研究開発を行う。具体的には、抽出した機能要件に基づき、それらに適合する耐量子計算機暗号の要素技術（公開鍵暗号、鍵配送、デジタル署名等）の選択、様々なユースケースに応じてパラメータ設定を適切に調整・管理するための管理運用技術を確立する。管理運用技術により、伝送速度、遅延、信頼性、トラフィック密度、接続密度等の観点から、高速・大容量、低遅延、多数接続の特性を最大限に生かすためのセキュリティ用プロトコルの設計を行う。

③５Ｇアプリケーション上の耐量子計算機暗号の最適化技術

医療サービス、交通サービス、金融サービス、放送サービス、教育サービス等の幅広いサービスが最適な形で耐量子暗号系セキュリティ技術を活用するためには、①耐量子計算機暗号への機能付加技術および②５Ｇ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について、ユースケースに応じて適切に融合する必要がある。具体的には、５Ｇの特性を損なわないよう、様々なユースケースに応じた機能選択やパラメータ設定を行うための耐量子計算機暗号の最適化技術を構築する。さらに、最適化手法を導出する時間などの観点から、本研究開発による最適化技術を定量的に評価する。

④５Ｇに適応する物理層セキュリティ技術

①～③で開発した技術を、計算機リソースが限られた端末でも実現するため、物理層セキュリティを５Ｇ用に発展させたモデルおよびセキュリティ要件を構築する。５Ｇの特性それぞれを活かした鍵配送方式や暗号化方式の構築を行うことを目標とし、実装および実証を通して、開発技術の有効性を通信速度や遅延時間などの観点から定量的に評価する。

到達目標

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）

　共通鍵暗号として、大規模量子コンピュータにおいても、現実的な計算時間で解読できない方式、かつ計算機リソースが限られた携帯端末にも実装が可能な設計を行う。さらに、一般的に入手可能な既存の計算機環境における暗号処理のスループットとして 50Gbps を達成すること、および暗号処理に要する時間を従来方式と比較して最大 50%程度削減する。

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）

　通信事業者が提供する５Ｇ基盤サービスや各種ユースケースにおける５Ｇサービスにおいて、その特性を損なわない形の耐量子コンピュータセキュリティ技術を構築し、技術付与前と比較してそのオーバーヘッド（暗号文サイズ、処理時間等）を最大８％以内に抑える。また、PQC の活用の視点から、計算機リソースが限られた携帯端末等でも実装が可能な技術開発も行う。

　なお、上記の目標を達成するに当たっての年度毎の目標については、以下の例を想定している。

＜令和３年度＞

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）

　共通鍵暗号方式に関して、処理速度と安全性の観点から設計要件を抽出し、機能部品の選択等による設計指針の検討を行う。また、攻撃手法の調査等により、安全性及び機能性の観点から評価指針の検討を行う。

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）

　NIST PQC の選定候補を含めた複数の耐量子計算機暗号について、無線通信仮想環境における機能評価を行う。また、機能付加技術・最適化技術・管理運用技術に関する技術仕様設計および物理層セキュリティ技術のセキュリティ要件を検討する。

＜令和４年度＞

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）

　令和３年度に検討した設計指針に基づき、アルゴリズムの設計を行う。また、新たな攻撃手法の発見等、最新の情勢等に併せて評価指針の改良を行う。

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）

令和３年度に設計した技術仕様に基づき、機能拡張技術・最適化技術・管理運用技術の構築を行い、無線通信の仮想環境において評価を行う。また、物理層セキュリティ技術の構築及び評価を行う。

＜令和５年度＞

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）

令和４年に設計したアルゴリズムに対して、考えられる攻撃手法の計算量を見積もることで安全性の評価を実施する。また、アルゴリズムの実装を行い、処理速度等の機能性の評価を実施する。そして、抽出された課題に基づいて方式の改良を行う。

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）

令和４年度に構築した機能拡張技術・最適化技術・管理運用技術および物理層セキュリティ技術に対して、実用性の立場から課題を抽出し、技術改良を行う。また、特定ユースケースにおける評価を実施する。

＜令和６年度＞

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）

設計・改良したアルゴリズムについて、将来の無線通信環境を想定した環境で実証評価を行うとともに、課題イとの統合評価を行う。

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）

令和５年度までに開発した機能拡張技術・最適化技術・管理運用技術および物理層セキュリティ技術に対して、将来の無線通信環境を想定した環境で実証評価を行うとともに、課題アとの統合評価を行う。

５．実施期間

令和３年度から６年度までの４年間

６．その他

（１）成果の普及展開に向けた取組等

①国際標準化等への取組

国際競争力の強化を実現するためには、本研究開発の成果を研究期間中及び終了後、速やかに関連する国際標準化規格・機関・団体へ提案を実施することが重要である。このため、研究開発の進捗に合わせて、国際標準への提案活動を行うものとする。なお、提案を想定する国際標準規格・機関・団体及び具体的な標準化活動の計画を策定した上で、提案書に記載すること。

②実用化への取組

研究開発期間終了後も引き続き取り組む予定の「本研究開発で確立した技術の普及啓発活動」及び令和 11 年度までの実用化・製品展開等を実現するために必要な取組を図ることとし、その活動計画・実施方策については、提案書に必ず具体的に記載すること。

（２）提案および研究開発に当たっての留意点

提案に当たっては、基本計画書に記されている目標に対する達成度を評価することが可能な具体的な評価項目を設定し、各評価項目に対して可能な限り数値目標を定めること。また、従来の技術との差異を明確にした上で、技術課題及び目標達成に向けた研究方法、実施計画及び年度目標について具体的かつ実効性のある提案を行うこと。

研究開発の実施に当たっては、関連する要素技術間の調整、成果の取りまとめ方等、研究開発全体の方針について幅広い観点から助言を頂くと共に、実際の研究開発の進め方について適宜指導を頂くため、多方面から関連する分野の学識経験者、有識者等を含んだ研究開発運営委員会等を定期的に開催する等、外部の学識経験者、有識者等を参画させること。

なお、本研究開発において実用的な成果を導出するための共同研究体制又は研究協力体制について、研究計画書の中にできるだけ具体的に記載すること。特に、暗号技術を必要とする無線通信システムや先進的な暗号研究などの幅広い分野の研究機関が参加する等、研究開発を推進し、かつ技術開発状況や標準化動向に柔軟に対応出来る体制を構築すること。