量子コンピュータ時代に向けた暗号技術の研究開発及び社会実装

①　計画の概要

大規模な量子コンピュータが実現すると、現在の情報インフラのセキュリティを支える多くの暗号技術の安全性が低下し、2030年には現在広く使われている公開鍵暗号RSA-2048 を解読できる量子コンピュータが出現するという予測がある。これを見すえて、世界的に、大規模量子コンピュータが実現しても安全性が保たれる「耐量子計算機暗号」(Post-Quantum Cryptography, PQC)の標準化が進められている。我が国としても長期的視野で本暗号技術の設計・安全性評価・実装方法に関する研究開発を強化する必要があるとともに、新たな暗号方式にどのように移行していくかが大きな課題となっている。

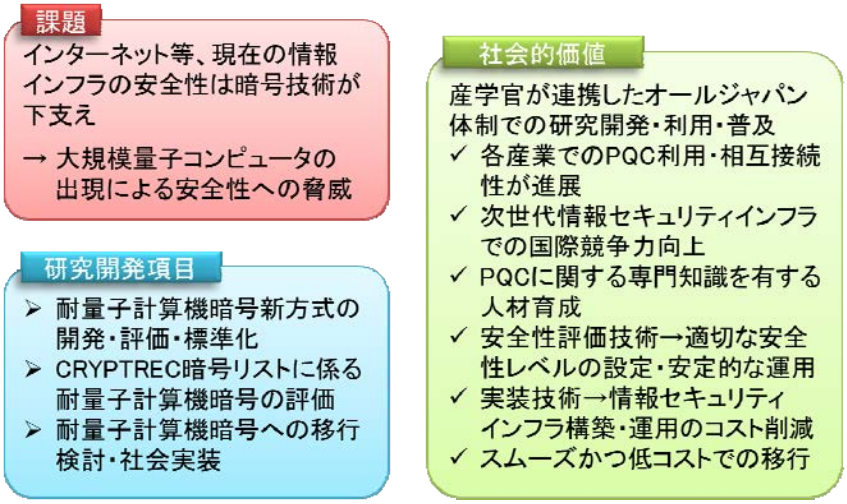

図１ 本研究開発課題のねらい

国内におけるこれまでの PQC への取り組みとして、いくつかの大学、企業、国立研究開発法人で新たな暗号方式が開発され、米国 NIST が進めている PQC 標準化に対して提案されたほか、JST CREST「数理モデリング」において次世代暗号に向けた暗号数理に関する研究プロジェクトが進められてきた。また、総務省・経産省が連携して運営する電子政府推奨暗号の安全性を評価・監視する CRYPTREC において、本技術の調査や技術報告書の発行が行われてきた。特に、CRYPTREC で 2023 年に予定されている政府調達暗号リストの改定において、本技術の導入を検討する上で安全性評価及び実装評価が必須となっている。また、現在の暗号技術から PQC への移行に関しては、内閣サイバーセキュリティセンターの主導のもと、移行計画を策定する必要があり、産学官および国際連携も活用して取り組むべき大きな研究開発及び社会課題となっている。

本研究開発プロジェクトでは、PQC の設計・安全性評価・実装方法に関する研究開発及び国際標準化、実システムでの実装評価、現在の暗号方式から新たな方式へのスムーズな移行方法など社会実装に係る検討を行う。

②　学術的な意義

大規模量子コンピュータが実現すると、現在使われている公開鍵暗号の安全性が急低下するというのは、このような公開鍵暗号の安全性の根拠となっている数学上の問題を多項式時間で解く量子アルゴリズムが見つかっているからである。具体的には、公開鍵暗号 RSA の安全性の根拠となっている「素因数分解問題」や電子署名 DSA の安全性の根拠となっている「離散対数問題」は量子ゲート方式の量子コンピュータ上で Shor のアルゴリズムにより効率的に解けることが示されている。ただ、現時点で実現している量子コンピュータは、15（＝３×５）や21(＝３×７)といった小さな合成数を素因数分解できるレベルで、現在主流の RSA-2048 で使われる 4092 ビットの合成数を解けるレベルの量子コンピュータの実現までは相当な技術的なギャップがあり、実現時期は予測不可能だという指摘もある。しかしながら、現在の暗号技術が危殆化する（安全性が低下し危険な状態になる）までに早期に対策を行う必要があるというのが世界的なコンセンサスとなっている。

これに対し、耐量子計算機暗号は、安全性の根拠となる数学上の問題を効率よく解く量子アルゴリズムが見つかっていない暗号技術で、大規模量子コンピュータが実現しても安全性が保たれると期待されている。耐量子計算機暗号として期待されている方式にはいくつかあり、格子に基づく暗号技術、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術等がある。耐量子計算機暗号の安全性評価は、これらの数学上の問題を解く計算量をより厳密に見積もることであり、これにより各方式の安全性レベルを決める適切なパラメータを設定することができる。耐量子計算機暗号の標準化が進められている一方、この安全性評価手法（計算量評価）は未確立であり、これを耐量子計算機暗号の普及期までに確立することは学術的・社会的意義が高い。

③　国内外の動向と当該研究計画の位置づけ

大規模量子コンピュータの実現に備えた暗号技術の開発及び標準化の動きが世界的に活発になってきたのが2015年前後である。米国ではNSA がPQC への移行を発表し、2016 年にNIST がPQC 標準化計画を発表、公募を開始した。EU でも 2015 年からH2020 の中でPQCRYPTO やSAFECrypto といった研究プロジェクトが開始された。国内でも 2014 年度から JST CREST において次世代暗号に向けた暗号数理に関する研究プロジェクトや、CRYPTREC においてPQC の調査が開始されている。米国NIST PQC 標準化への公募へは世界中から応募された 82 方式のうち 69 方式が発表された。ここには日本からの提案４方式が含まれていた。これらの方式は、2019 年１月に安全性や実装性能の観点から 26 件に絞り込まれたが、日本提案は１方式も残れなかった。この結果は

これまで国内の企業・研究機関が自助努力で進めてきた本研究開発への投資意欲を冷やしかねず、我が国として大型研究計画を立て産学官連携体制のもと進めていかなくてはならない時期に来ている。

④ 実施機関と実施体制

本研究開発を集中して推進するために、首都圏のいずれかに研究開発拠点を構築して開発環境を整え、大学、企業、国立研究開発法人等から人材を出向等で集結させて実施する。 産学官が連携した国産暗号開発構想については、1990 年代に NICT の前身である旧通信・放送機構の暗号研究開発プロジェクトにおいて、辻井重男リーダ（当時中央大）が各企業に呼びかけたことがあった。当時は各社それぞれが独自暗号を開発できる体力があり、それが差別化技術になるという打算もあり、合意に至らなかった。しかしながら、 現在は１社のみで開発・実装・普及を担える体力のある会社はないと思われる。これから国産 PQC 方式を開発すると、NIST PQC 標準候補を見ながら優位性をもつ方式を開発することができる。共同開発した暗号は、十分な安全性評価を行い、ISO/IEC 等で行われる PQC 標準化にも日本標準として提案を行う。日本の産学官が連携して利用・普及に努めることで、PQC への移行、各産業での活用、相互接続性が進み、国際競争力をもつことが期待される。以前は、複数の国産暗号が乱立し、国際標準提案時の国内絞り込みや技術普及の障害となった経緯があるが、本構想では全ての参加組織が、PQC に関する専門知識をもった人材の育成、PQC 国内標準開発への貢献、各社におけるスムーズな移行や連携体制等の成長と実利を得られる Win-win 体制が期待でき、本プロジェクトへの人材を集められると期待できる。実施体制は、プロジェクトリーダーのもと、各企業等からの暗号開発の経験者（シニア～中堅層）と次世代を担う若手の人材構成バランスが重要である。また、暗号の実装や国際標準化動向に明るい人材も不可欠である。

⑤ 所要経費

○設備費 合計 8.2 億円
・研究開発拠点整備費 ２億円
・PQC 安全性評価サーバ構築費 ３億円
・PQC 実装評価サーバ構築費 ２億円
・資材消耗品・雑費 1.2 億円
○人件費 合計 35.7 億円
・プロジェクトリーダー
・耐量子計算機暗号の新方式の開発 研究者
・耐量子計算機暗号の普及・標準化 専門家
・耐量子計算機暗号の社会実装 技術者
・耐量子計算機暗号の移行検討
・耐量子計算機暗号の外部評価 研究者
・契約・発注業務、支援業務等
・サーバ・ネットワークの整備・運用技術者
○旅費 合計 1.2 億円
○外部評価費用 合計１億円
・安全性評価 0.5 億円
・実装評価（SW. HW） 0.5 億円
○その他調査費用 合計１億円
・海外動向調査、特許調査等

⑥ 年次計画

図２参照

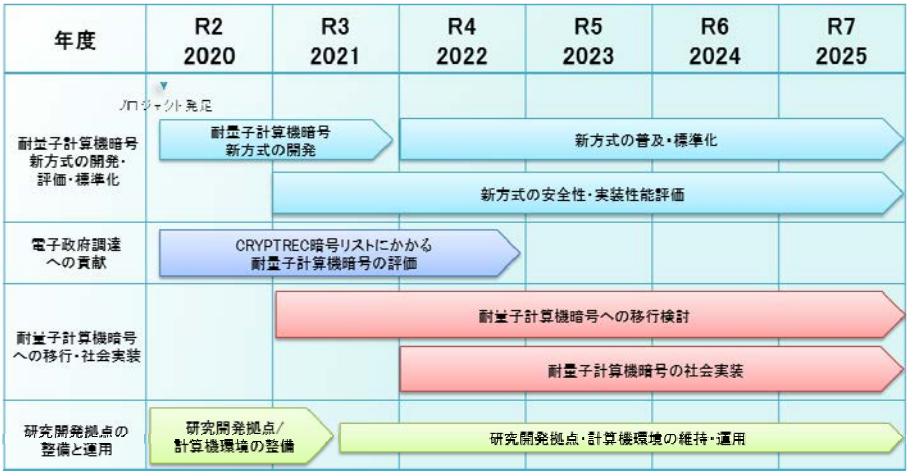

図2 年次計画

⑦ 社会的価値

現在のインターネットを含む情報インフラのセキュリティは暗号技術が下支えをしており、大規模量子コンピュータの出現によりその安全性への脅威が高まっている中、PQC の研究開発及び社会実装をオールジャパンで進めることは我が国として経済的・産業的価値が高い。

PQC の安全性評価に関する研究は、これにより各暗号方式の安全性レベルを決める適切なパラメータを設定することができ、長期間の安定的な運用が期待できる。

PQC の実装方法に関する研究については、PQC は必要メモリや速度等の観点で従来より高いコストが予想されることから、効率的な実装方法の確立は、将来の情報インフラの消費エネルギーの削減といった観点で意義がある。

また、国際的に競争力のある PQC 方式を開発し、デファクト標準を取ることができれば、開発に関わった国内企業等が量子コンピュータ時代の情報インフラ産業において強みをもつことが期待できる。

さらに、PQC への移行については、早期の移行方法の確立と余裕をもった移行作業の開始で SIer への負荷集中を避け、より低コストで進めることが可能となり、我が国の財政面への効果が見込まれる。

⑧ 本計画に関する連絡先

盛合 志帆（国立研究開発法人情報通信研究機構）