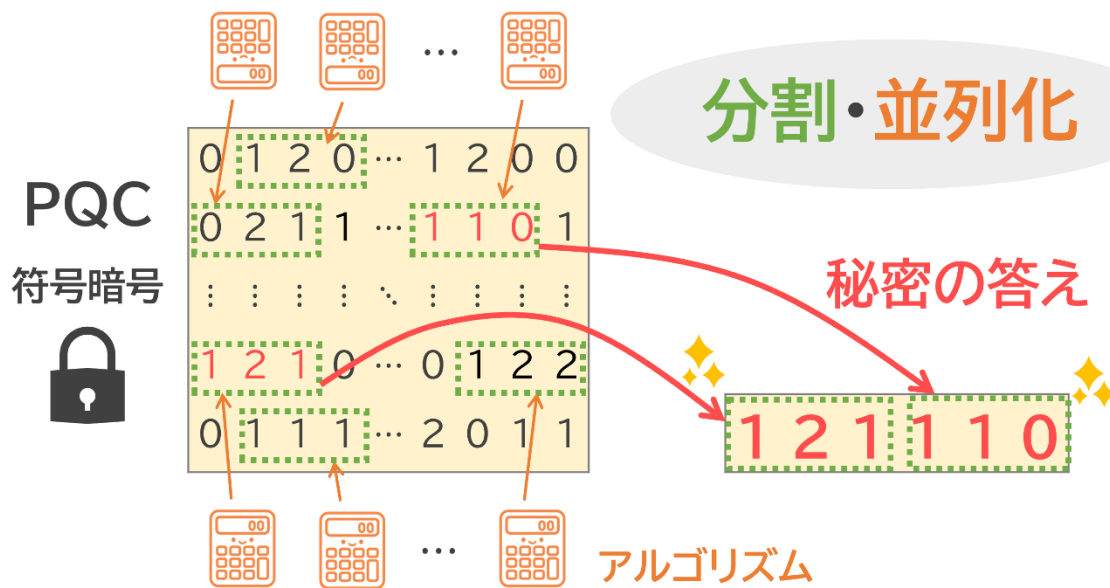


PQC に関する暗号解読コンテストで世界記録を達成 ～効率的な次世代暗号の実現に向けた安全性評価の理論を実証～

株式会社 KDDI 総合研究所（本社：埼玉県ふじみ野市、代表取締役所長：小西 聡、以下 KDDI 総合研究所）と東京大学大学院情報理工学系研究科の修士2年 若尾 武史 大学院生、相川 勇輔 助教、高木 剛 教授（以下 東京大学）は、次世代暗号として米国で標準化が進められている耐量子計算機暗号（以下 PQC：Post-Quantum Cryptography）の暗号解読コンテスト「Challenges for code-based problems（注1）」において、3元体（注2）にもとづく210次元、220次元、230次元、240次元の符号暗号の解読に成功（以下 本成果）しました。また、2025年12月15日、本成果により3元体にもとづく符号暗号は米国標準 PQC の符号暗号と比べ、1/10以下の次元数（データサイズ）で同等の安全性を満たすことを確認しました。

今回 KDDI 総合研究所と東京大学は、3元体上の符号暗号に対し分割・並列処理による効率的なアルゴリズムを開発・実装することで、これまで誰も解けなかった暗号を解読しました。本成果により、2元体や3元体などにもとづく暗号の安全性を詳細に評価するための理論的枠組みの有効性を実証し、新たな数学的構造を用いた暗号方式を実現する道筋を開きました。3元体にもとづく符号暗号を電子署名に利用した場合、2元体に比べ署名長を短くできるという特徴があり、スマートカードやIoTセンサーといった、データサイズに制約のある機器での活用が期待されます。

なお、本成果の一部は、科学技術振興機構（JST）経済安全保障重要技術育成プログラム（JPMJKP24U2）の支援を受けて行いました。



<図1：分割・並列処理による解読のイメージ>

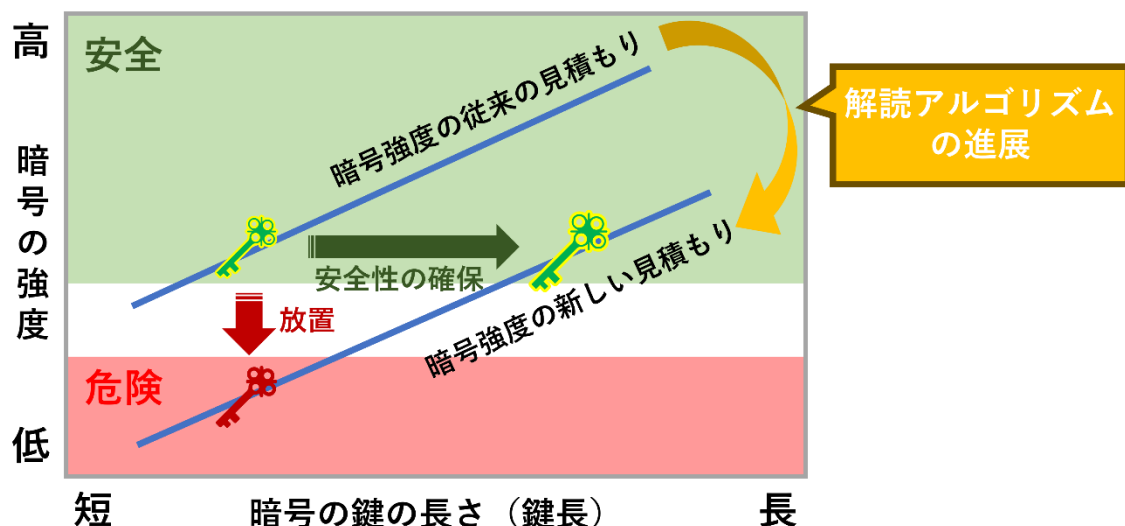
■背景

ネットショッピングやネットバンキングをはじめとする現代の情報サービスでは、個人情報をオンラ

イン上でやりとりする機会が増えています。これらのサービスを安心・安全に利用できるようにするためには、暗号技術による情報セキュリティの確保が不可欠です。

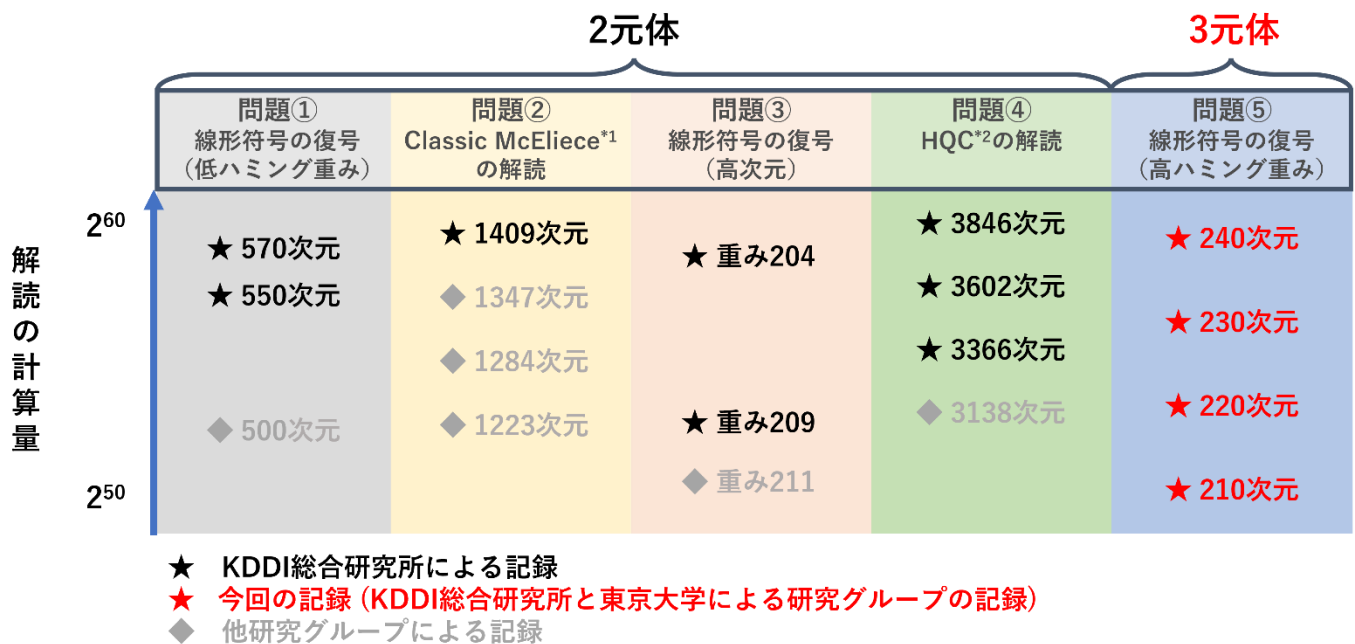
近年、量子コンピューターが登場し、2030年代には実用化が見込まれる中、将来的に従来の暗号の強度が不足する可能性が指摘されています。アメリカ国立標準技術研究所（以下 NIST）は、量子コンピューターの処理能力にも耐えうる PQC の検討を進めています。NIST は 2024 年 8 月に米国標準 PQC として 3 方式の正式な技術規格を公開（注 3）しており、2035 年までに現行の公開鍵暗号から PQC への移行を完了する予定です。また、2025 年 3 月には符号暗号である HQC を追加の米国標準 PQC に選定しています。さらに、現在 NIST は署名長の短い方式を米国標準に追加するための評価・選定を行っています。

暗号が普及した後に安全性が低下した場合、多大な損害が発生する恐れがあります。こうしたリスクを防ぐためには、新しい暗号技術の実用化に先立ち、暗号の高い安全性（暗号の強度）を正確に検証することが求められます。暗号の強度は、暗号解読に必要な計算量が指標となり、この計算量を明らかにすることで、安全性と性能を両立する適切な鍵の長さ（鍵長）の導出につながります。例えば、図 2 のように解読アルゴリズムの進展によって暗号の強度が低下した場合には、鍵長を大きくして安全性を確保する必要があります。



< 図 2：解読技術の進展と適切な暗号の鍵の長さ >

PQC をはじめとする新しい暗号の安全性を十分に検証するために、国際的な暗号解読コンテストが開催されています。次世代暗号の研究を行う企業や団体は、より高速な暗号解読手法の開発を進め、難易度の高い暗号解読に挑戦しています。KDDI 総合研究所は継続的に暗号解読コンテストに参加し、これまでに世界記録を計 19 回更新しています。また、現在コンテストで出題されている 5 種類すべての問題で世界記録を保持しました。



*1 符号暗号の1方式であり、暗号文の長さが小さいことが特徴。

*2 正式名称はHamming Quasi-Cyclic。符号暗号の1方式であり、鍵の長さが小さいことが特徴。

<図3：符号暗号解読コンテストで達成した主な世界記録>

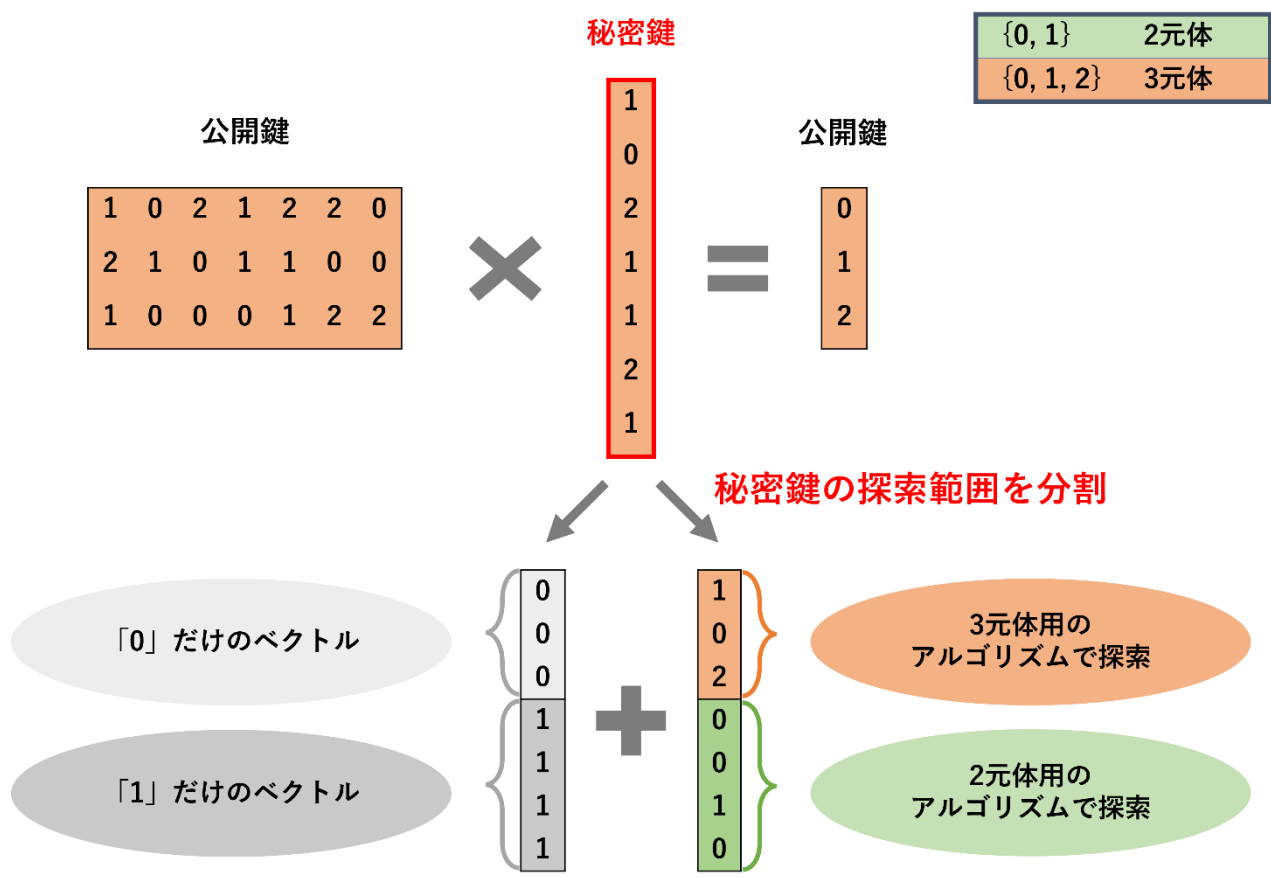
■本成果について

今回挑戦した問題は、3元体にもとづく符号暗号の安全性の根拠となる「シンドローム復号問題」と呼ばれるものです。これは、与えられた3元体にもとづく行列とベクトルに対して、条件を満たす秘密のベクトルを探索する問題であり、符号暗号の公開鍵から秘密鍵を求めることに相当します。

シンドローム復号問題を解く標準的な手法として、Information Set Decoding（注4）と呼ばれる解読アルゴリズムが知られています。通常、このアルゴリズムは2元体上の符号暗号を解読するために使用されるため、3元体上の符号暗号に対しては、より効率的な解読アルゴリズムとその実装を開発する必要がありました。そこで今回は、これまでの解読コンテストを通じて研究開発を行ってきた2元体用Information Set Decodingを3元体用に拡張しました。さらに、秘密鍵の探索時に2元体上の解読アルゴリズムと3元体用の解読アルゴリズムを組み合わせる分割統治法を適用することで、秘密鍵の探索効率を向上させました。開発した解読アルゴリズムを並列コンピューティング環境上に実装し、最大7台のデスクトップパソコンからなる計算環境を構築しました。これらの取り組みにより、解読処理を約1,000倍高速化（注5）しました。

その結果、210次元から240次元の符号暗号を数十分から数日で解読することに成功しました。本成果を基に、3元体にもとづく符号暗号が600次元以上のパラメータに対して128ビット級の高い安全性（注6）を有することを実証しました。また、過去に解読した2元体にもとづく符号暗号と今回の暗号を含む符号暗号の安全性評価のための理論を構築し、多様な符号暗号の精緻な安全性を評価・実証しました。

なお、KDDI総合研究所と東京大学は、本成果を2026年1月26日から1月30日に函館市で開催される「2026年 暗号と情報セキュリティシンポジウム（SCIS 2026）」（注7）で発表する予定です。



<図4：3元体上のシンドローム復号問題と解読のアプローチ>

■今後の取り組み

KDDI 総合研究所と東京大学は、引き続き暗号解読コンテストに挑戦し、PQC の安全性の検証を行うとともに、これまで培ってきた暗号解読の知見を生かし、PQC 実装時に求められる暗号アルゴリズムの高速実装やスマートカードや IoT 機器向けの軽量実装の研究開発にも取り組んでいきます。今後も、量子コンピュータの実用化が予想される 2030 年代を見据え、世界中のお客さまに安心・安全な通信サービスを提供できるよう、研究・技術開発を通じて社会に貢献していきます。

- (注1) フランス国立情報学自動制御研究所 (INRIA) が主催する国際的な暗号解読コンテスト。2019年7月21日にウェブサイトが公開され、コンテストが開始された。符号暗号に関連する計5種類の問題が出題され、世界中の暗号研究者が参加している。今回挑戦した問題以外には、米国標準として選定された HQC の解読に関する問題などが出題されている。
<https://decodingchallenge.org>
- (注2) 「0」、「1」、「2」の3つの要素からなる集合で、加算・乗算を含む演算が定義されている数学的な構造。「0」、「1」の2つの要素からなる集合は2元体という。
- (注3) 米国標準 PQC として選定済みの ML-KEM、ML-DSA 及び SLH-DSA の連邦情報処理標準 (FIPS: Federal Information Processing Standards) を公開。
- (注4) 線形代数と組み合わせ論によって、シンドローム復号問題を求解する指数時間アルゴリズム
- (注5) GPU を搭載した PC において、一般的な符号暗号の解読アルゴリズムを動作させたときの処理速度に比べ 1,000 倍高速化。
- (注6) その暗号を破るためには約 2^{128} 回の計算が必要であるということ。現代暗号の安全性において一つの基準となっている。
- (注7) 2026年 暗号と情報セキュリティシンポジウム (SCIS2026)
<https://www.iwsec.org/scis/2026/>

以上