国立研究開発法人
情報通信研究機構

プレスリリース
2018年1月11日
国立研究開発法人情報通信研究機構

量子コンピュータ時代に向けた新暗号技術を開発
～格子理論に基づき、かつ汎用性に優れた公開鍵暗号を国際標準化に提案～

【ポイント】

- 量子コンピュータでも安全な格子理論に基づく公開鍵暗号を開発
- 暗号技術の安全性評価手法を開発、統一的な基準で様々な格子暗号を比較可能に
- 米国 NIST 主催の量子コンピュータ時代に向けた暗号技術の標準化プロジェクトの候補暗号に

国立研究開発法人情報通信研究機構（NICT、理事長：徳田 英幸）サイバーセキュリティ研究所セキュリティ基盤研究室は、量子コンピュータでも解読が困難な格子理論に基づく新暗号方式 LOTUS（ロータス）を開発しました。LOTUS は、暗号文の復号の際にその構造をチェックする機能を持っており、現在の公開鍵暗号と置き換え可能な汎用性も有しています。さらに、格子理論に基づく暗号技術の安全性評価手法を同時に開発し、複数の格子暗号同士を統一的な基準で比較することが可能になりました。

LOTUS の特徴としては、量子コンピュータでも解読が難しい耐量子性を持ち、また、ブラウザ、データベースなどに組み込み可能な汎用性を持つことなどが挙げられます。そのため、暗号の専門家でなくても安全に使うことが可能です。

近年の量子コンピュータの発展に伴い、これら新しいタイプのコンピュータでも解読が困難な耐量子計算機暗号[*1] の標準化が急務となっています。米国国立標準技術研究所（National Institute of Standards and Technology: NIST）が現在の暗号方式を置き換える耐量子計算機暗号を世界中から公募[*2] していましたが、このたび、書類選考を通過した 69 件の候補が公開されました。NICT で開発した暗号方式もこの候補の一つです。今後数年かけて、これらの候補の評価・選定が行われます。

【背景】

インターネットを利用するときに使うウェブ・ブラウザ等には、パスワードやクレジットカード番号等の重要な情報を暗号化する機能が組み込まれています。この中で、RSA 暗号や楕円曲線暗号などの公開鍵暗号が使われています。

しかしながら、現在広く使われている RSA 暗号や楕円曲線暗号は、ある程度性能の高い量子コンピュータを使うと簡単に解読されてしまうことが数学的に証明されています。近年、量子コンピュータの商用販売や無償クラウド利用が提供されるなど、量子コンピュータの高性能化・普及が進んでおり[*3]、現行の公開鍵暗号では安全な通信ができなくなる可能性があります（図 1 参照）。

このような社会的背景の下、現在の公開鍵暗号を置き換えるための新たな暗号方式を標準化する議論が米国 NIST を中心に進んでいます。

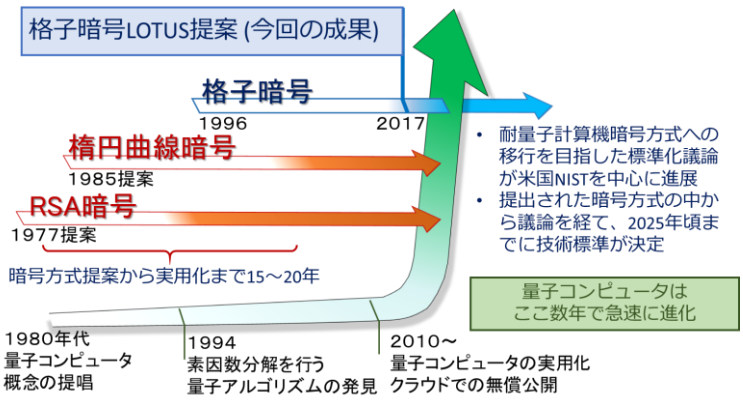


図 1 公開鍵暗号の変遷

【今回の成果】

量子コンピュータが普及した時代でも情報の安全性が守れるよう、NICT では以下の条件を満たす新暗号方式 LOTUS を開発しました。

① 耐量子性：通常のコンピュータのみならず、量子コンピュータでも解読が難しいこと。これにより、量子コンピュータ普及後も情報の安全性が守られます。

② 汎用性：ベースとなる暗号方式に対して、復号の際に暗号文が破損していないことをチェックする機構を追加することで、ブラウザ、データベースをはじめ、多くの通信・交通・産業システムに組み込むことが可能となりました。

また、本暗号を組み込んだシステム全体も量子コンピュータに対して安全となることが数学的に証明されているため、暗号の専門家以外でも安心して使うことができます。

これまで、NICT セキュリティ基盤研究室では、耐量子計算機暗号の有力候補とされる格子暗号[*4] の開発と安全性評価に取り組んできました。その知見を活かし、今回、耐量子性だけではなく、汎用性[*5] を持った格子暗号方式の開発に取り組みました。格子暗号にはいくつかの方式がありますが、それらの中でも最も安全性に関する理論の研究が進んでいる LWE 問題[*6] に基づく方式を選択しました。この方式はそのままでは汎用性を持ちませんが、暗号文の復号の際にその構造をチェックする機能（補足資料参照）を追加することで、汎用的な暗号方式となります。これにより、米国 NIST が標準化を進めている、現在の公開鍵暗号方式と置き換え可能な方式を開発し、米国 NIST の耐量子計算機暗号の候補の一つとなりました。

さらに、格子理論に基づく暗号技術の安全性評価手法を同時に開発し、暗号の長期利用に適したパラメータの設定が可能になりました。この安全性評価手法は、他の格子暗号方式を評価することも可能であるため、多数提案されている格子暗号同士を統一的な基準で評価することにより、公平な議論に役立つと期待されます。

【今後の展望】

本暗号技術は、量子コンピュータ普及後も、引き続き、情報インフラの安全な利用を支えることができます。今回開発した方式の概要は、2018 年 4 月 12 日（木）～13 日（金）に米国フロリダ州で開催される会議 First PQC Standardization Conference において発表される予定です。

また、このたび米国 NIST が発表した候補暗号方式は、今後 3 年以上かけて専門家による詳細な解析が行われます。NICT は、本暗号技術の普及に向けた活動を続けるとともに、耐量子計算機暗号の安全性評価にも貢献していきます。

＜ 本件に関する問い合わせ先 ＞
国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
青野 良範、レ チュウ フォン
Tel: 042-327-6594
E-mail: lotus-inquiry@ml.nict.go.jp

＜ 広報 ＞
広報部 報道室
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp

＜用語解説＞

*1 耐量子計算機暗号

現在使われているコンピュータと、量子コンピュータのどちらを用いても解読に非常に時間がかかると期待されている暗号方式の総称。

現在、社会で使われている RSA 暗号や楕円曲線暗号は、ある程度高い性能を持つ量子コンピュータにより、高速に解読されてしまうことが 1994 年にピーター・ショアによって数学的に証明されている。そのため、このような問題が生じない耐量子計算機暗号への移行を目指した議論が進んでいる。

*2 米国 NIST における暗号標準化プロジェクト

米国 NIST は、現代暗号の黎明期から暗号技術の標準化活動を行っている。過去には、ブロック暗号 AES、ハッシュ関数 SHA-3 等の標準化に関して、世界中から集められた候補の中から 1 件を選ぶコンペティションを行っている。

2016 年から、耐量子計算機暗号の標準を決めるための標準化プロセスが開始された。世界中から 82 件の応募があり、内 69 件が候補として今後の議論の対象となる。今後 3 年以上かけ、安全性、実行速度、拡張性などの観点から複数の暗号方式が選ばれる予定である。

参考: 米国 NIST の耐量子計算機暗号標準化 ラウンド 1 候補暗号一覧
https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

*3 量子コンピュータの高性能化・普及

量子コンピュータは、量子回路を用いて一般的な計算を行う量子デジタルコンピュータと、特定の組み合わせ問題を量子的性質を用いて解くことに特化した量子アナログコンピュータとに分類される。前者は 20qubit のものが IBM 社によって公開され、後者も 2000 パラメータの問題を解くことが可能な量子ニューラルネットワーク計算機が 2017 年 11 月に NTT、NII、東大、JST、内閣府によって発表されている。

これらの量子コンピュータは、計算問題の種類によっては通常のコンピュータよりもはるかに高速に解を求められることが実証されている。今後も回路規模や扱うことの可能なパラメータ数が大きくなることが予想される。

*4 格子暗号

空間内に規則的に並んだ点の集合を格子と呼び、この数学的な性質を使い安全性を確保する暗号を格子暗号と呼ぶ。規則的に並ぶという性質を行列で表現することで、暗号化及び復号処理を並列化することが可能であるため、効率的な実装が可能である。

NICT では、以前から格子暗号の安全性評価活動を継続しており、今回開発した安全性評価手法は、LOTUS のみではなく、他の格子暗号の評価にも使うことができると期待される。

参考: 2013 年 1 月 21 日付け NICT 報道発表「クラウド向け暗号技術の安全性評価で世界新記録を達成」
http://www.nict.go.jp/press/2013/01/21-1.html
2016 年 6 月 6 日付け NICT お知らせ「格子暗号の安全性評価アルゴリズムの実装コードを公開」
http://www.nict.go.jp/info/topics/2016/06/160606-1.html

*5 暗号技術の汎用性

開発された暗号技術が実社会で使用されるためには、暗号そのものが安全であるのはもちろんのこと、いくつかの暗号を組み合わせたシステム全体も安全である必要がある。この概念を数学的に説明したものが暗号技術の汎用性である。

この性質を持たない暗号方式を使う場合、組み合わせ方を間違えるとそこに脆弱性（攻撃者が付け入る余地）が生まれてしまい、システム全体が破たんする危険性があった。システム全体の安全性を保証するためには、暗号一つ一つの安全性を証明した後に、全体の安全性を証明するという二段階の手順を踏む。しかし、複雑なシステムでは専門家が何日もかけて検証しなければならず、また、その複雑さゆえに誤りが発生しやすい等の問題点があった。

暗号を設計する段階で、汎用性という性質を持たせることで、このような危険を避けることができる。汎用性を持った暗号方式同士を組み合わせたシステムは、安全であることが数学的に証明されているため、全体の安全性を証明するステップが省略可能となる。

開発した LOTUS では、ベースとなる格子暗号に対して、復号の際に暗号文の構造をチェックする機構を追加することで、データ破損への耐性を持たせた。このチェック機構により、他の暗号方式と組み合わせ可能な汎用性を持つことが数学的に証明されるため、開発した暗号から様々なシステムを作り、社会の様々な場面で活用することができる。

*6 LWE 問題

Learning **w**ith **E**rrors 問題の略称で、変数よりも式の数が多い連立一次方程式において、左辺と右辺の差が小さくなるような整数解を求める問題。パラメータによっては格子の最短ベクトル問題と同等の難しさとなることが証明されているため、量子コンピュータを用いてもその求解には非常に時間がかかると予想されている。

補足資料

LOTUS（ロータス）は、“**L**earning with err**O**rs based encryption with chosen ciphertex**T** sec**U**rity for po**S**t quantum era”の略称であり、格子暗号の技術を使っています。

格子暗号では、全てのデータは行列やベクトルで表現されます（図２参照）。暗号化処理は一度平文ベクトルをスクランブル（図中の薄緑から濃緑への矢印）した後、それを復元に必要な付加情報（図中の灰色の部分）とセットにして暗号文ベクトルとします。復号時には、秘密鍵と付加情報から、暗号文のスクランブルを解除するための情報を復元し、平文を計算します。この原理は、以前開発したセキュリティアップデータブル暗号（2015 年 1 月 19 日付け NICT 報道発表参照 http://www.nict.go.jp/press/2015/01/19-1.html）の基本部分と同じです。

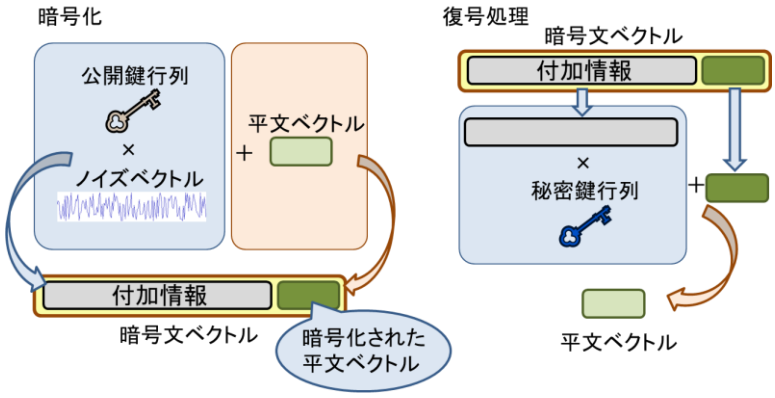


図２　格子暗号の概要（2015 年 1 月 19 日報道発表の図３から引用）

この図のような暗号方式を実社会でシステムに組み込むとき、データの破損が問題になります（図３参照）。例えば、保存してある暗号文ベクトルがメディアの損傷などで、元とは異なるものに変化してしまった場合、その暗号文を正しい鍵で復号しても元の平文を得られません。また、悪意のある攻撃者は、意図的にこのデータ破損を引き起こし、情報を復元不可能にしてしまうか、無理やり破損した暗号文を復号した結果を利用して、さらに、他の秘密情報を読み取る危険性があります。

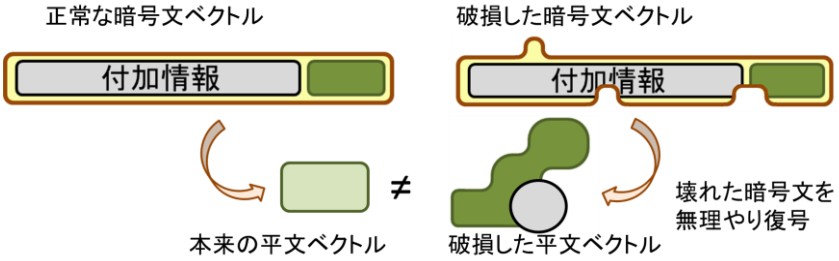
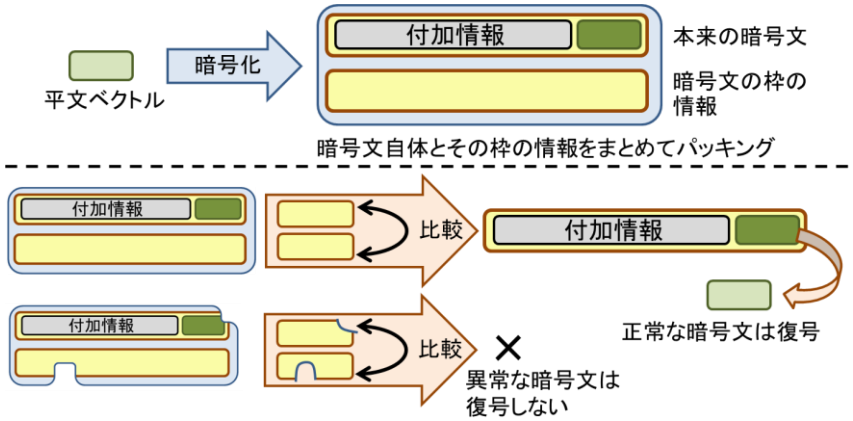


図３　破損した暗号文の復号結果は悪用される危険性がある

このような暗号文破損への対策として、LOTUS　では暗号化の際に暗号文とその枠の形を示す情報を一度にパッキングし（図 ４ 上参照）、復号の直前にそれらを比較し暗号文の破損が起きていないことをチェックする機構を付け加えました（図４下参照）。もしもデータが破損していた場合、上と下で枠の形が異なるため、データの異常を検知して復号を中断することで、攻撃者が余分な情報を得ることを防げます。このチェック機構の追加を専門的には、「藤崎・岡本変換」と呼びます。また、この機構を組み込むことで、暗号方式が汎用性を持ち、多くのシステムに組み込むことが可能となります。



復号前に、暗号文と枠の形が同じかどうかをチェックする機構を挿入

図４　藤崎・岡本変換によって汎用性を持たせた格子暗号