計算環境の変化に対応する暗号理論研究の最前線

キャッシュカードの偽造事件を契機としてNTTに暗号研究グループが発足してから35年になろうとしています．その流れをくむNTTセキュアプラットフォーム研究所（SC研）では普遍的価値を持つ暗号基礎理論の構築に貢献するとともに，進歩し続ける通信・計算環境の変化に対応した新しい暗号技術の創出に取り組んできました．本稿では発展の著しい量子計算機の出現に備えた暗号技術や情報処理技術に関するSC研の研究活動を紹介します．

阿部 正幸（あべ まさゆき） /徳永 裕己（とくなが ゆうき）
Mehdi Tibouchi /西巻 陵（にしまき りょう）
草川 恵太（くさがわ けいた）
NTTセキュアプラットフォーム研究所

背　景

暗号の安全性は攻撃者がどれくらいの計算資源，すなわちメモリ量や計算速度を持ち得るかによって相対的に評価されます．インターネットが普及し始めた1990年代には RSA暗号の公開鍵は512ビット程度で安全と考えられていました．電子署名法が成立した2001年には1024ビット，2008年から検討されている改定では少なくとも2048ビットが必要とされています．

現在では多くの暗号システムにおいて，より効率的な楕円曲線暗号へ移行しています．さらには，楕円曲線上のペアリング群によってIDベース暗号をはじめとする高機能な公開鍵暗号や，効率的なデジタル署名，非対話ゼロ知識証明が発展しました．暗号は鍵の管理方法によって情報へのアクセスをコントロールする機能を自然に持っています．従来の暗号通信では情報の送り手と受け手が１対１でしたが，クラウドへ暗号化データを保存しておき，送り手が定めた条件を満たす複数の受け手に向けて情報を発信するといった用途に向く高機能な暗号方式が開発されています．

一方，1994年に発表された Shorのアルゴリズムによって，十分な数の量子ビットを十分な精度で扱える汎用のゲート型量子計算機によって現在普及しているRSA暗号やDiffie-Hellman鍵共有などの効率的な公開鍵暗号が破られることが示されました．たとえそのような高度な量子計算機の実現が数十年後になるとしても，その脅威に対して安全な暗号，いわゆる耐量子計算機暗号の開発には量子計算機の実現を待たずに取り組む必要があり，実際に多くの研究開発と標準化が進んでいます．それは暗号システムを提供する者の責任感といった動機だけではなく，次の２つの現実的な理由によります．

まず，新しい暗号方式は開発から普及まで非常に長い時間を要することです．現状動いているようにみえるシステムを互換性のない新たなシステムにアップデートするのは，すべてのユーザが短期間でできることではありません．もう１つの理由は，現在のプライバシが将来の攻撃技術の進展によって毀損されることへの懸念，すなわち長期的な安全性の危殆化です．暗号化された通信であっても，それ自体が傍受・長期保存されて，将来の量子計算機の実現によって内容が暴露される懸念があります．つまり，数十年後に漏洩して困るようなコンテンツにとっては，量子計算機による攻撃は現時点で対応しておかねばならない脅威なのです．また，耐量子計算機暗号は量子計算機上で実行されるのではなく，現在の計算機上で実行されるものです．そのため，現在の計算機環境における実装も含めた安全性が検討される必要があります．

本稿では，まず，量子情報処理技術に関する本研究所での取り組みについて説明します．次に，耐量子計算機暗号に関する最新のトピックを紹介します．最後に，従来の公開鍵暗号の機能拡張の１つである属性ベース暗号について，最新の研究結果を紹介します．

量子情報処理

■SC研における量子情報処理技術

2019年10月，量子コンピュータがついに従来のコンピュータの能力を超える量子超越性を達成したとのニュースが駆けめぐりました．NTTセキュアプラットフォーム研究所（SC研）においても，量子力学の原理で情報処理をする量子コンピュータの研究開発を以前から進めています．

現在までに実現された量子コンピュータはまだ数十量子ビット程度で

あり，規模の拡張性をどのように得ていくかについては，未解決の課題が山積みです．つまり，量子コンピュータをどのようにつくり，どのように拡張性を得ていくかの実装法の研究開発は，現在の暗号の安全性レベルを検証する試金石にもなっています．

また一方で，量子情報処理技術は新たなセキュリティ技術も生み出しています．量子状態は，むやみに観測すると状態を壊してしまう，コピーができないなどの通常のデータとは異なる性質を内在しています．これをうまく活用することにより新たなセキュリティ技術が生み出されます．

■量子コンピュータ開発への道筋

量子コンピュータ実現に向けての一番の障壁はエラーに弱いことです．量子ビットは，現代の主要な情報処理単位であるデジタルデータのようにエラーを小さくすることがそもそも難しいため，少し規模を大きくするとエラーに埋もれて正しい計算が困難になってきます．これを実際に解決する方法は，今までのところ，量子エラー訂正符号しか知られていません．量子エラー訂正符号を用いると，技術的に可能な範囲にある特定の誤り率を下回る制御を達成すれば，符号化された量子状態に載った量子情報の論理的な誤り率を小さくすることが可能となり，エラーに対する規模の拡張性を得られます．

もう１つの課題は量子ビット数自体の規模を拡大することです．個別の量子ビットを精度良く高速に制御しながら規模を大きくしていくことは相反するような技術開発であり，不安定な量子状態に対してこれまであまり行われてきませんでした．精度を保ちつつ，量子ビット数の桁数を上げていく量子物理工学的な技術開発におけるブレークスルーが期待されています．SC研は文部科学省Q-LEAPプロジェクトに参加し，超伝導量子コンピュータの開発に携わっています．量子エラー訂正が可能となるような高度な制御技術と規模の拡大をめざした研究開発に取り組んでいます．

量子セキュアネットワークに向けて

量子情報処理を活用した新たなセキュリティ技術の例が量子暗号（量子鍵配送）です．むやみに観測すると状態を壊すという性質を使うことで盗聴検出が可能となり，原理的に安全な鍵配送が可能になります．しかし，現状の技術の欠点は，損失に弱く通信距離に事実上の制限（100 km程度まで）があること，ネットワーク化する技術がないことです．これを解決する方法が量子中継です．これは高精度に光と物質の量子状態を制御し，損失に耐え得るような量子エラー訂正を行うことに対応します．そのため，実は小～中規模の量子コンピュータをつくるのにほぼ匹敵する技術です．量子中継をめざすためにも，やはり量子コンピュータを実装する研究開発とほぼ同等のことを行っていかなくてはなりません．SC研では，量子中継器に求められる，光と原子の量子状態を精度良く制御し，扱える量子状態の規模を大きくすることをめざした研究に取り組んでいます．

また，科学技術振興機構（JST）のCRESTプロジェクトに参加し，光と原子の相互作用を高精度に行える共振器電気力学を活用した研究開発に取り組んでいます．

耐量子計算機暗号

■安全な実装および標準化への貢献

RSA暗号や楕円曲線暗号といった従来暗号技術のほかに，量子暗号に対する耐久性を持つと思われる耐量子暗号技術は実は数十年も前から研究されています．もっとも基本的な機能である暗号方式と署名方式に関しては，量子計算機に破られにくい問題に基づく理論的な設計方法が昔から知られています．しかし，RSA暗号や楕円曲線暗号に比べて処理速度・通信量などの性能が著しく劣っており，実用性が低いと判断されていたため，耐量子暗号技術の実装はほとんどありませんで

した．

ここ数年，量子計算機の実現が目に見える脅威になってくるにつれ，この脅威がいよいよ真剣に検討され始めました．より高速・高性能の耐量子暗号技術の提案と実装が重要な研究課題となってきました．特に耐量子暗号の有力候補とみなされる「格子暗号」の分野では，強固な安全性根拠を持つ昔からの方式にさまざまな工夫を加え，RSA暗号などに並ぶ性能を達成した新方式が提案・実装されてきました．VPNソフトウェアなどへの実装実験も始まっています[1]．

理論的な安全性根拠が徹底的に検討されている一方，サイドチャネル攻撃やフォールト攻撃などの実装上の脆弱性があまり考慮されていません．また，実装に値する効率的な新方式は「離散ガウス分布の生成」や「棄却サンプリング」など，従来暗号技術に存在しないテクニックに基づいており，実装上の新たな課題になっています．SC研では，これらの実装上の課題に取り組むべく，とりわけ格子署名方式を対象に実装攻撃に対する安全性評価を行い，数多くの脆弱性を発見しました[2]．例えば，格子ベース署名の最速方式として知られているBLISS方式の複数の実装を対象に，署名生成時の電力消費や処理時間を測定することにより，代数学や数論の結果を用いて秘密鍵を完全に復元できることを示しました．このような脆弱性を克服するための対策および新たな実装手法を提案し，その安全性の証明もしています．最高水準の性能を維持したまま，実装攻撃に対する強い安全性を持つ格子ベース署名方式も達成しました[3]．

この一連の研究は，米国標準技術局（NIST）が2016年に立ち上げた現在進行中の耐量子暗号標準化プロセス（NISTコンペ）に大きな影響を及ぼしました．とりわけ，BLISS方式の実装上の脆弱性に関する結果が，提案方式の１つDilithiumなどの設計方針で実装上の脅威として検討されています．その結果により，NISTコンペのほとんどの方式において「離散ガウス分布の生成」が避けられました．なお，NISTコンペ開始後にもDilithiumやFalconの安全な実装に関する成果を得たほか，安全性根拠が薄弱な方式を完全に破り敗退に追い込んだなど，貢献をし続けてきました[4]．

■量子計算機を用いた共通鍵暗号の安全性評価手法

共通鍵暗号に対する汎用的な量子アルゴリズムは今のところ知られていません．そのためGroverのアルゴリズムや量子ランダムウォークアルゴリズムを適用した攻撃が最良のものとして知られています．SC研では，共通鍵暗号の内部まで詳しく解析することで，新たな安全性評価手法を生み出してきました．例えば，NTTコミュニケーション科学基礎研究所と共同で取り組んだハッシュ関数の多重衝突発見問題の改良が挙げられます[5]．

また，将来的に量子計算機を入手できることを見越して，現時点から情報収集・窃取を行っている敵対者も考えられます．このような敵対者の影響を見積もるための安全性評価手法にも取り組んでいます[6]．

■量子計算機を考慮した安全性証明技法

これまでの多くの安全性証明では，敵対者が量子計算機を所持していることを想定していませんでした．そのため，安全性が証明された方式であっても，敵対者が量子計算機を用いて安全性を破ってしまう可能性が残っています．そこで2010年以降，量子計算機を考慮した安全性証明技法が数多く編み出されてきました．SC研でもそのような研究に取り組んでいます．耐量子公開鍵暗号の安全性強化手法[7]や，ハッシュ関数の耐量子安全性[8]，Feistel構造を持つ共通鍵暗号の耐量子安全性[9]，事前計算を許した場合のハッシュ関数への攻撃の一般的な下界評価[10]などがその例です．

属性ベース暗号

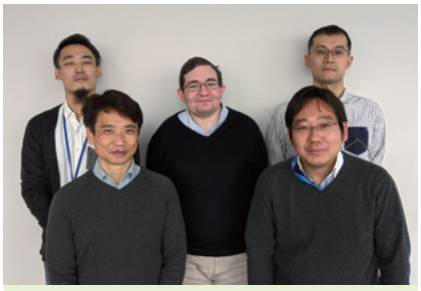
公開鍵暗号の中でも主たるテーマは

いくつかありますが，本稿ではその中の１つである「実用的な効率性を持つ属性ベース暗号の実現」に焦点を絞って紹介します．

公開鍵暗号では情報の送り手は受け手の公開鍵を使って暗号化し，その公開鍵に対応する秘密鍵を持つ受け手のみが情報を復元できる暗号文を生成できています．属性ベース暗号とは，情報の受け手を１人に限定せず，送り手が自由に受け手を指定可能な暗号です．より詳しくいうと，暗号文に受信ポリシーが，秘密鍵に受け手の属性が埋め込まれており，受け手の属性が暗号文の受信ポリシーに合致する場合にのみ受け手は情報を受け取ることができます．このように暗号文と秘密鍵にロジックを埋め込み，きめ細かい情報授受の制限を実現できます．これまでに数多くの属性ベース暗号方式が提案されていますが，実際のシステムに実装することを考えると不十分な点が多くありました．一例としてスケーラビリティが挙げられます．既存の多くの方式は，最初のシステム構築の際に，使用する属性をすべて決める必要があり，以降追加できませんでした．スケーラビリティを考えると，利用できる属性をいつでも追加できるほうが望ましいです．ほかにデータサイズの問題がありました．既存の方式では暗号文のサイズが，埋め込まれるポリシーのサイズや使用する属性の数に比例して大きくなるものがありました．これはストレージを圧迫するので望ましくありませんでした．このように実際に利用するうえでさまざまな性能基準が考えられましたが，そのすべてについて実用上望ましいレベルに達している方式は提案されていませんでした．当グループでは，実用上望ましい性質をすべて兼ね備えた属性ベース暗号を新たに開発しました．

■参考文献

(1) https://github.com/Microsoft/PQCrypto-VPN
(2) T. Espitau, P.-A. Fouque, B. Gerard, and M. Tibouchi：“Side-channel attacks on BLISS lattice-based signatures,” Proc. of ACM CCS 2017, pp.1857-1874, Dallas, U.S.A., May. 2017.
(3) G. Barthe, S. Belaid, T. Espitau, P.-A. Fouque, B. Gregoire, M. Rossi, and M. Tibouchi：“Masking the GLP lattice-based signature scheme at any order,” Proc. of EUROCRYPT 2018, Vol.10821, pp.354-384, 2018.
(4) J. Bootle, M. Tibouchi, and K. Xagawa：“Cryptanalysis of Compact-LWE,” Proc. of CT-RSA 2018, Vol.10808, pp.80-97, 2018.
(5) A. Hosoyamada, Y. Sasaki, S. Tani, and K. Xagawa：“Improved Quantum Multicollision-Finding Algorithm, ” Proc. of PQCrypto 2019, Vol.11505, pp.350-367, 2019.
(6) A. Hosoyamada and Y. Sasaki：“Cryptanalysis Against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations,” Proc. of CT-RSA 2018, Vol.10808, pp.198-218, 2018.
(7) T. Saito, K. Xagawa, and T. Yamakawa：“Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model,” Proc. of EUROCRYPT 2018, Vol.10822, pp.520-551, 2018.
(8) A. Hosoyamada and K. Yasuda：“Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions,” ASIACRYPT 2018 Part I, LNCS, Vol.11272, pp.275-304, 2018.
(9) A. Hosoyamada and T. Iwata：“4-Round Luby-Rackoff Construction is a qPRP,” Asiacrypt 2019, pp.145-174, Kobe, Japan, Dec. 2019.
(10) M. Hhan, K. Xagawa, and T. Yamakawa：“Quantum Random Oracle Model with Auxiliary Input,” Asiacrypt, pp.84-614, Kobe, Japan, Dec. 2014.



（後列左から）草川 恵太/
Mehdi Tibouchi/
西巻 陵
（前列左から）阿部 正幸/ 徳永 裕己

NTTセキュアプラットフォーム研究所では，暗号技術の研究開発を通じて，安心・安全なサービスの実現をめざします．

◆問い合わせ先

NTTセキュアプラットフォーム研究所
企画担当
E-mail scpflab@hco.ntt.co.jp