https://sites.google.com/view/yuntaowang/lab-jp

耐量子計算機暗号に向けた暗号方式の提案と安全性評価

王 研究室

王 賛弢
Yuntao WANG

現行のコンピューターである古典計算機の計算能力をはるかにしのぐ量子コンピューター（量子計算機）が、さまざまな領域で活用される未来が現実味を帯びつつあります。その一方で、安全なデータ通信や電子決済、デジタル署名、仮想通貨などに広く使われているＲＳＡ暗号や楕円曲線暗号といった従来の公開鍵暗号方式が、量子計算機の登場によって脆弱になる危険性が指摘されています。

量子計算機でＲＳＡ暗号は解読可能に

例えば、ＲＳＡ暗号の安全性の根拠となる「素因数分解問題」は量子アルゴリズムで効率的に解けることが数学的に証明されており、そのため量子計算機を使うことで、ＲＳＡ暗号を短時間で解読できると言われています。現在、安全とされる鍵長２０４８ビット（６１７ケタ）のＲＳＡ暗号は、２０３０年代の実用化が見込まれる１００万量子ビットの量子計算機を使えば、１週間以内に解読可能なことが分かっています。そのため、米国国立標準技術研究所（ＮＩＳＴ）は、このＲＳＡ-２０４８を２０３０年から「非推奨」とし、２０３５年には完全廃止とするガイドラインを定めています。

量子計算に耐性を持つ次世代暗号ＰＱＣ

こうした背景から、２０１５年、米国家安全保障局とＮＩＳＴは、量子計算に耐性を持つ「耐量子計算機暗号（ポスト量子暗号、ＰＱＣ）」への移行を宣言しました。ＰＱＣをテーマとする王賛弢准教授は、新しい暗号方式や署名方式の提案から、暗号の解読や安全性評価、さらには機械学習セキュリティや自動運転システム、サイバーセキュリティといった分野へのＰＱＣ技術の応用に至るまで幅広い研究を手がけています。

次世代暗号であるＰＱＣは古典計算にはもちろん、量子計算にも

公開鍵暗号の現状と今後の課題

量子計算機「叡（えい）」@富士通研究所

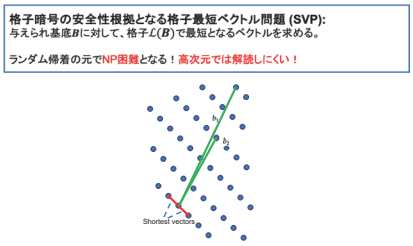
キーワード

公開鍵暗号、耐量子計算機暗号、デジタル署名、高機能暗号、情報セキュリティ、プライバシー保護、安全性評価、暗号応用、暗号解読、暗号標準化

所　属	大学院情報理工学研究科 情報学専攻
メンバー	王 賛弢 准教授
所属学会	情報処理学会、電子情報通信学会、国際暗号学会、米国電気電子学会、計算機協会、日本応用数理学会、日本人工知能学会
E-mail	y-wang@uec.ac.jp

耐性を持つ暗号です。PQCの中にも格子暗号や多変数多項式暗号、コードベース暗号、ハッシュベース暗号、同種写像暗号などさまざまな手法があり、各手法で安全性の根拠となる数学問題が異なります。王准教授はその中で最も注目され、「格子最短ベクトル問題（SVP）」を根拠とし、「NP困難」で高次元では解読しにくい格子暗号について研究しています。

格子暗号の安全性

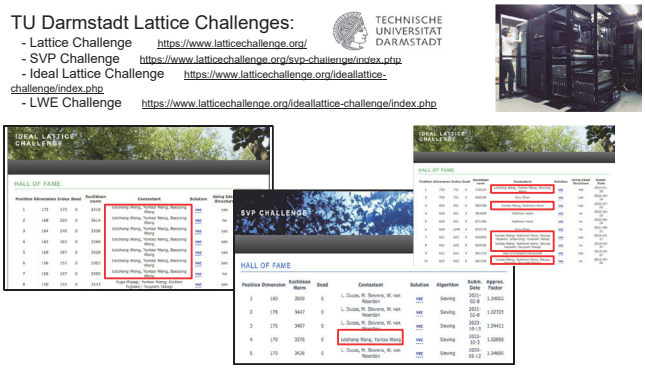


格子暗号の解読で世界記録を達成

特筆すべきは、王准教授はこのSVPに関する暗号解読の世界記録を保持しており、解読アルゴリズムの改良などにより、現在までに「SVP Challenge 170次元」と「Ideal Lattice Challenge 176次元（近似版750次元）」の記録を更新しています。また、格子暗号の安全性評価のための新しい解析手法も提案しています。格子暗号の安全性には「LWE問題」と呼ばれる計算困難性がよく使われますが、王准教授は既存の解読アルゴリズムを組み合わせることにより、提案手法がLWE問題の幅広いパラメータ領域に対して効果的であることを理論と数値実験の両方で実証しました。

さらに、PQCの新たな暗号方式として、王准教授は効率的な格子ベース鍵共有方式を開発し、NISTの次世代暗号標準プロジェクトに提案しました。これはRoundingと言われる鍵共有メカニズムを導入して変形した「RLWE問題」の困難性に基づく新しいDH型の鍵共有プロトコルです。シミュレーションと実装によって通信コストを減らした上で、暗号解読による安全性評価も行っており、「次世代暗号の標準化に貢献できる」と王准教授は考えています。

格子最短ベクトル問題(SVP)の世界解読記録を達成



機械学習セキュリティなどへ応用

そのほか、トレードオフの関係にある暗号の安全性評価と効率性評価を行いながら、暗号技術の応用にも取り組んでいます。例えば、機械学習セキュリティとして、準同型暗号を使ったプライバシー保護可能な連合学習のフレームワークを考案しました。分散しているデータを1カ所に集めずに学習できる「連合学習」を行う際に、準同型暗号による秘密計算を行うことで、個人情報などを暗号化したままサーバに送ることができるようになります。

王准教授は「最終的な目標は、こうした最新の暗号技術を社会展開することであり、そのために国内の大学や企業に加え、出身の中国や韓国、また米国、ドイツ、オランダなど海外の大学とも交流しながら、機械学習やブロックチェーンなどのサイバーセキュリティ、自動運転といった、さまざまな領域での応用を進めたい」と話しています。

【取材・文＝藤木信穂】

研究テーマ

A1. 研究内容Ⅰ：耐量子計算機(格子)暗号方式・デジタル署名の提案
- 鍵共有方式の構築、デジタル署名の構築、ハイブリッド暗号方式の設計

A2. 研究内容Ⅱ：暗号解読・安全性評価
- 暗号の困難問題に対する解読アルゴリズムの提案・改良・高速実装・世界記録達成

A3. 研究内容Ⅲ：暗号技術の応用
- 機械学習セキュリティ、自動運転システムへの応用、サイバーセキュリティなど