PRESS RELEASE

2025 年 1 月 20 日
東京大学
日本電信電話株式会社
九州大学
長崎県立大学

米国標準化コンペ第 2 ラウンド 日本発のデジタル署名方式公開

――「QR-UOV」方式の仕様を公開、量子コンピュータ時代にも安全に利用可能――

発表のポイント

◆共同研究開発を進めているデジタル署名方式「QR-UOV」について、安全性証明および処理性能を向上させる実装技術を含む新たな技術仕様書を公開します。
◆今回、提案初期と比較して処理性能が向上したことにより、効率性とコンパクトさを両立することができ、提案方式の標準化採用や社会実装に大きく前進しました。
◆QR-UOV は米国標準化コンペに提出している方式で、2024 年 10 月に第 2 ラウンドへの進出が決まり、2025 年 9 月に開催される第 6 回 NIST PQC 標準化会議で発表する予定です。

QR-UOV 方式は UOV 方式に比べ、データサイズは半分以下に収まり、
署名の効率性は同程度である。

概要

東京大学大学院情報理工学系研究科、日本電信電話株式会社、九州大学マス・フォア・インダストリ研究所、長崎県立大学からなる共同研究チームは、デジタル署名（注１）方式「QR-UOV」を改良し、コンパクトさと効率性を両立する新たな仕様を公開します。現在、米国の国立標準技術研究所（以下「NIST」）では、量子計算機（注２）でも解読できない新たなデジタル署名方式の標準化コンペを実施しており、今回の仕様公開は、QR-UOV の標準化コンペ第 2 ラウンド進

出に合わせて行ったものです。QR-UOV は、多変数多項式問題（注３）の難しさを安全性の根拠としており、公開鍵および署名のデータサイズが小さいことが特徴です。量子計算機の時代においても安全かつ効率的なデジタル署名方式として、個人認証やデータ保護などに活用が可能となります。本署名方式が標準規格として採用された場合、世界中で広く利用されることが見込まれます。

なお、この新たな仕様に基づく QR-UOV については、2025 年 1 月 28～31 日に開催される 2025 年暗号と情報セキュリティシンポジウム SCIS2025、更には 2025 年 9 月 24～26 日に開催予定の第 6 回 NIST PQC 標準化会議で発表予定です。

図 1:　QR-UOV の特徴

発表内容

暗号技術は我々の生活の様々な場面で利用され、情報社会の安全性を支えるコア技術として重要性を増しています。一方で、将来大規模な量子計算機が実現すると、暗号技術のうち公開鍵暗号・鍵共有やデジタル署名において、現在普及している方式が簡単に解読されてしまうとも言われています。大規模な量子計算機の実用化を見据え量子計算機を用いても解読できないような暗号技術(耐量子計算機暗号, Post-Quantum Cryptography, PQC)の研究・開発が進んでおり、世界の暗号標準に強い影響力を持つ米国の NIST は、2016 年から耐量子計算機安全性を持つ公開鍵暗号・鍵共有方式ならびにデジタル署名方式の標準化を進めています。NIST 標準化のプロセスはラウンド制で進められ、段階的な絞り込みにより採用方式を決定しています。2017 年 12 月に 69 方式が受理されましたが、現在は 4 方式のみが標準化方式として採択されています。デジタル署名方式に関しては、2022 年 9 月に追加公募のアナウンスがなされ、2023 年 7 月に 40 方式が受理されました。そして、2024

年 10 月に 40 方式中 14 方式が第 2 ラウンドの選考候補として選定され、新しい仕様書が 2025 年 2 月に NIST のホームページで公開される予定です。

将来的に量子計算機が大規模化した時代でも安全に利用できるデジタル署名方式として、多変数多項式問題の難しさを根拠とした署名方式「UOV」が注目を集めています。UOV は 1999 年に提案されたデジタル署名であり、20 年以上にわたり本質的な解読法が報告されていない安全な方式とされています。また、NIST が追加公募の際に出した要件として『短い署名と高速な検証を行う方式』であることを挙げており、UOV は双方を満たす方式としても注目されています。その一方で検証の際に使用する公開鍵のデータサイズが大きくなることが UOV の課題となっていました。

デジタル署名方式 QR-UOV は、数値の行列で表現されていた UOV の公開鍵を剰余環（QR）（注４）と言われる代数系の多項式として表現することにより、安全性を低下させることなく公開鍵のデータサイズ削減を実現しています（図 2）。QR-UOV は UOV と同様に短い署名と高速な検証を実現する方式でかつ、UOV の課題となっている公開鍵サイズを大幅に削減する方式として優位性を持っています。NIST 標準化第 1 ラウンドの結論が 2024 年 10 月に発表され、欧米を中心とした研究機関などから候補方式 14 件が進出し、日本発の方式として QR-UOV が唯一選ばれました。

NIST は今後数年で標準化方式を選定するとしています。本研究チームは引き続き、QR-UOV の標準化採択に向けて、量子計算機の時代にも安心・安全なセキュリティを維持する技術の研究開発を進めていきます。

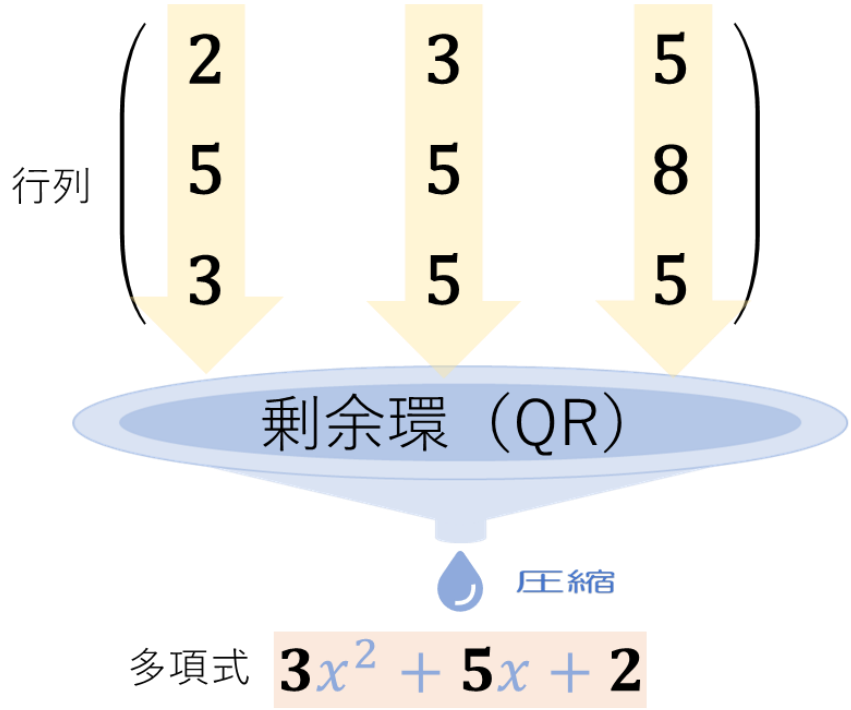

図 2：　数値の行列を剰余環（QR）により圧縮した多項式を公開鍵とする

〇関連情報：

「プレスリリース①量子コンピュータでも解読できない安全な暗号技術を開発 ～ データサイズが小さく効率的なデジタル署名 -QR-UOV- ～」(2021/11/24)
https://www.i.u-tokyo.ac.jp/news/press/2021/202111241931.shtml

発表者・研究者等情報

東京大学大学院情報理工学系研究科
　数理情報学専攻　高木 剛　教授
日本電信電話株式会社 サービスイノベーション総合研究所
　古江 弘樹　研究員，小菅 悠久　主任研究員，山越 公洋　主任研究員，秋山 梨佳　研究員，中邑 聡史　研究員，折原 慎吾　主任研究員，金城 皓羽　研究主任
九州大学マス・フォア・インダストリ研究所
　先進暗号数理デザイン室　池松 泰彦　准教授
長崎県立大学 情報システム学部
　情報セキュリティ学科　星野 文学　教授

論文情報

タイトル：QR-UOV
著者：Hiroki Furue, Yasuhiko Ikematsu, Fumitaka Hoshino, Tsuyoshi Takagi, Haruhisa Kosuge, Kimihiro Yamakoshi, Rika Akiyama, Satoshi Nakamura, Shingo Orihara, Koha Kinjo
会議名： NIST Post-Quantum Cryptography: Round 2 Additional Signatures
https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures

※上記の仕様書の概要については以下のシンポジウムで発表予定
タイトル：NIST PQC Additional Signatures Second Round Candidate: QR-UOV
著者：上記の仕様書と同じ
会議名：暗号と情報セキュリティシンポジウム（SCIS2025）
https://www.iwsec.org/scis/2025/

研究助成

本研究は科学技術振興機構（JST）戦略的創造研究推進事業 CREST「数学・数理科学と情報科学の連携・融合による情報活用基盤の創出と社会課題解決に向けた展開」研究領域（研究総括：上田修功）における研究課題 JPMJCR2113「ポスト量子社会が求める高機能暗号の数理基盤創出と展開」の支援により実施されました。また、本研究は JSPS 科研費 JP22K17889, JP24K02939 の助成を受けたものです。

用語解説

（注 1）デジタル署名：電子データに対する署名機能を実現する暗号技術で、データの改ざんやなりすまし防止の用途で電子契約書などに用いられています。

（注２）量子計算機：量子力学の原理を計算に用いた計算機で、従来の計算機で解くには膨大な時間を要する問題を効率的に解くことができます。特に暗号分野では、現在普及している暗号技術が帰着する数学的問題を効率的に解く量子アルゴリズムが発見されていることから、耐量子計算機暗号への移行に向けた取り組みが活発になっています。

（注３）多変数多項式問題：多変数多項式からなる連立方程式を解く問題で、パラメータの選び方により求解が困難となることが知られています。

（注４）剰余環（QR）：足し算と掛け算が可能な代数系を特定の部分集合で割ることにより得られる、新しい足し算や掛け算が可能となる代数系を指します。今回の場合、多項式の割り算から得られる余りを計算することにより、新しい足し算や掛け算が可能となる代数系を得ることができます。

問合せ先

（研究内容については発表者にお問合せください）

東京大学大学院情報理工学系研究科
教授　高木　剛（たかぎ　つよし）
Tel：03-5841-6940　E-mail：takagi@mist.i.u-tokyo.ac.jp

九州大学マス・フォア・インダストリ研究所　先進暗号数理デザイン室
准教授　池松 泰彦（いけまつ　やすひこ）
Tel：092-802-4425　E-mail：ikematsu@imi.kyushu-u.ac.jp

長崎県立大学 情報システム学部　情報セキュリティ学科
教授　星野 文学（ほしの　ふみたか）
Tel: 095-813-5135　E-mail: hoshino@sun.ac.jp

東京大学大学院情報理工学系研究科 広報室
Tel：080-3440-9757　E-mail：ist-pr.t@gs.mail.u-tokyo.ac.jp

日本電信電話株式会社 サービスイノベーション総合研究所
企画部 広報担当
https://tools.group.ntt/jp/rd/contact/index.php?param01=R&param02=203

九州大学 広報課
Tel：092-802-2130　FAX：092-802-2139
E-mail：koho@jimu.kyushu-u.ac.jp

長崎県立大学 NAGASAKI セキュリティベース研究所
岩田 正嗣 産学連携推進マネージャー
Tel：095-813-5305　E-mail：n-s-base@sun.ac.jp