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- ～

【発表概要】

東京大学大学院情報理工学系研究科と九州大学マス・フォア・インダストリ研究所は、日本電信電話株式会社と共同で、量子コンピュータでも解読できない新たなデジタル署名（注１）技術を開発し、既存の方式と比較して約３分の１まで公開鍵（注２）のデータサイズを削減することに成功しました。

今回開発したデジタル署名技術「QR-UOV 署名」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。量子コンピュータの時代においても安全かつ効率的な暗号技術として、個人認証やデータ保護などに利活用が可能となります。

この研究成果は、国際暗号学会主催の国際会議「International Conference on the Theory and Application of Cryptology and Information Security（Asiacrypt 2021）」（2021 年 12 月 6 日 - 10 日 オンライン開催）において発表します。

【発表のポイント】

◆成果：量子コンピュータでも解読できない新しい暗号技術を開発しました。
◆新規性：データサイズが小さい効率的なデジタル署名となります。
◆社会的意義、将来の展望：量子コンピュータの時代にも安全に利用できる効率的な暗号技術として、個人認証やデータ保護などに利活用が可能となります。

【発表内容】

＜研究の背景＞

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。現在普及している暗号方式として RSA 暗号（注４）および楕円曲線暗号（注５）がありますが、大規模な量子コンピュータが実現した場合に解読されることが知られています。そのため、将来的に量子コンピュータが大規模化した時代でも安全に利用できる暗号技術として、多変数多項式問題の難しさを安全性の根拠とした Rainbow 署名（注６）が注目を集めています。Rainbow 署名はデータの不正な書き換えを検出できるデジタル署名技術ですが、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問題となっていました。

＜研究内容＞

Rainbow 署名は 1999 年に提案された安全性の高い UOV 署名（注７）をマルチ階層構造として拡張することにより効率化していました。一方、今回の提案方式である QR-UOV 署名は、数値の行列で表現されていた UOV 署名の公開鍵を剰余環（注８）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ました

（図１）。実用的に安全性が十分に高いパラメータにおいてRainbow署名と比較したところ、公開鍵のデータサイズを約66%削減することが可能となりました（表１）。具体的には、Rainbow署名では252.3 KBであった公開鍵のデータサイズを、QR-UOV署名では約3分の1となる85.8 KBまで削減することに成功しました（KB：キロバイト）。

＜社会的意義・今後の予定＞

デジタル署名技術は、個人認証やデータの保護など情報セキュリティの向上を目的として広く利用されています。今回の提案方式は、量子計算コンピュータの時代にも安全となる効率的なデジタル署名であるため、その特徴を活かしたアプリケーションに貢献すると考えられます。特に、長期的な安全性が必要であり通信負荷の低減が求められるセキュリティシステムへの応用が期待できます。

米国標準技術研究所NISTは量子コンピュータに対して安全な暗号方式の標準化プロジェクトを進めていますが、デジタル署名技術に関しては2022年に再公募を行う計画を発表しています。研究グループは効率的なデジタル署名方式であるQR-UOV署名を、NISTの暗号標準化プロジェクトに応募し標準規格への採択を目指します。

【研究支援】

本研究成果は、以下の事業・研究課題の助成により得られました。
科学技術振興機構（JST）戦略的創造研究推進事業CREST「現代の数理科学と連携するモデリング手法の構築」研究領域（研究総括：坪井　俊）における研究課題 JPMJCR14D6「次世代暗号に向けたセキュリティ危殆化回避数理モデリング」

また、以下の事業・研究課題の助成により、実用システムで利用可能となる効率的なパラメータの導出に向けた研究を実施しています。
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」

【論文情報】

発表学会：「International Conference on the Theory and Application of Cryptology and Information Security（Asiacrypt 2021）」（2021年12月6日 - 10日 オンライン開催）
論文タイトル：A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV
著者：Hiroki Furue*, Yasuhiko Ikematsu, Yutaro Kiyomura, Tsuyoshi Takagi

【発表者】

高木　剛（東京大学大学院情報理工学系研究科数理情報学専攻　教授）
古江　弘樹（東京大学大学院情報理工学系研究科数理情報学専攻　博士課程（後期）1年）
池松　泰彦（九州大学マス・フォア・インダストリ研究所　助教）
清村　優太郎（NTT社会情報研究所　研究員）

【用語解説】

（注１）デジタル署名

作成されたデータが第三者によって不正に書き換えられないことを検証する技術であり、印鑑（押印）を電子的に実現した技術とも言えます。データに対応するデジタル署名を添付することにより、データの改竄（かいざん）と署名の偽造を検出することができます。

（注２）公開鍵

デジタル署名が正しいことを検証するときに用いる鍵のデータとなります。公開鍵のデータを用いて決められた手順で計算することにより、デジタル署名の正当性を検証します。

（注３）多変数多項式問題

n 個の変数を持つ m 個の 2 次多項式の共通解を計算する問題（図 2）であり、n と m を同程度の大きさで増加させた場合に計算が困難となることが知られています。

（注４）RSA 暗号

素因数分解の難しさを安全性の根拠とする暗号方式で、ウェブブラウザの暗号通信などで広く利用されています。

（注５）楕円曲線暗号

楕円曲線と言われる幾何的な構造を利用した暗号方式で、画像の著作権保護や暗号資産などで利用されています。

（注６）Rainbow 署名

多変数多項式問題の難しさを安全性の根拠とするデジタル署名方式であり、米国標準技術研究所 NIST の進める量子コンピュータに対して安全となる暗号方式の標準化プロジェクトで第 3 ラウンドの最終候補として選出されています。

（注７）UOV 署名

1999 年に提案された多変数多項式問題を基にし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。

（注８）剰余環

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となります。

【添付資料】

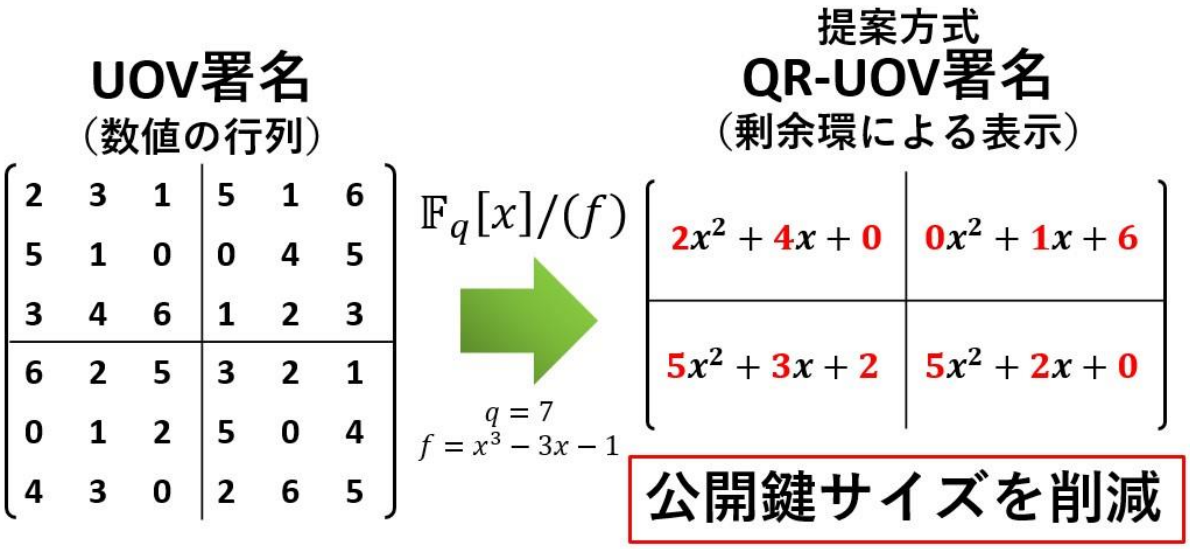

図１．提案方式の剰余環による公開鍵データサイズの削減

表 1. 提案方式と既存方式の公開鍵データサイズの比較（KB：キロバイト）

n: 変数の個数、m: 二次多項式の個数

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_{ij}^{(1)}x_i x_j + \sum_{i=1}^{n}\beta_i^{(1)}x_i + \gamma^{(1)} = 0$$

$$\vdots$$

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_{ij}^{(m)}x_i x_j + \sum_{i=1}^{n}\beta_i^{(m)}x_i + \gamma^{(m)} = 0$$

$\left(\alpha_{ij}^{(k)}, \beta_i^{(k)}, \gamma^{(k)} \in \mathbb{F}_q\right.$：有限体$\left.\right)$

図 2. 多変数多項式問題の説明図