（報道発表資料）

2025.5.12
日本電信電話株式会社

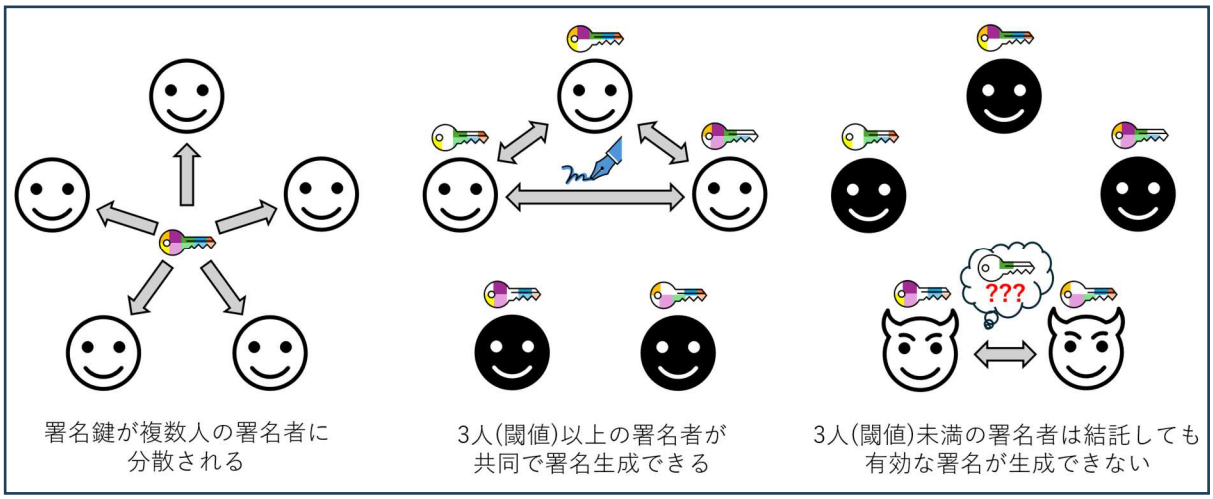
世界初、量子時代にも対応できる安全かつ高速な高機能電子署名技術を開発
～5 大陸間で 2.5 秒での署名生成を実証、行政や金融のインフラ基盤を支える仕組みを実現～

発表のポイント：

- **量子計算機に対する安全性に対応し、高速かつ安全な分散型の電子署名を世界で初めて開発しました。**
- **世界 5 大陸にあるサーバ間で署名生成を平均 2.5 秒で生成できることを実証し、現実のネットワーク上でも安定して使える性能を確認しました。**
- **電子投票や行政サービス、金融のシステムなどで、安全な多人数承認の仕組みとしての活用が期待されます。**

日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：島田 明、以下「NTT」）は、スイスの ETH Zurich、アメリカの UC Berkeley、フィンランドの Aalto University、イタリアの Bocconi University、アメリカの JPMorgan 社との共著の論文により、世界初の標準的安全性仮定に基づく 2 ラウンドの耐量子閾値署名（しきい値署名、threshold signature）方式「Ringtail」を開発しました。閾値署名は、単一の署名鍵を複数の関係者に安全に分散保管し、予め定められた数（しきい値）以上の関係者が協力することで初めて有効な電子署名が生成できる高度な暗号機能です（図 1）。これにより、一人の管理者による不正行為や、鍵の紛失・盗難といった単一障害点のリスクを大幅に低減できるため、暗号資産管理や重要インフラ・企業システム管理、分散型金融（DeFi）、Web3.0、電子投票システムなどで活用されます。「Ringtail」は、これらの応用において求められる高い効率性（通信回数が少なく高速）・信頼性（確かな安全性の保証）・将来性（量子計算機への耐久性）を兼ね備えた初めての方式であり、次世代の安心安全な分散型システムの基盤技術となることが期待できます。

本成果は 2025 年 5 月 12 日から 15 日まで、アメリカ・サンフランシスコで開催されるトップカンファレンス IEEE S&P 2025 にて採択論文※1 が発表されます。



【図１：閾値署名のイメージ。
白顔はプロトコルに参加しているユーザ、黒顔は参加していないユーザ。】

1. 研究の背景

通常の電子署名においては、署名鍵を持っている一人のユーザが単独で署名を行います。しかし、企業活動や社会システムにおいては、重要な権限が一人に集中することは望ましくない場面が多く存在しています。例えば、発注書を署名するのに、「管理職 3 名以上の承諾が必要」といった内部統制ルールがある場合や、暗号資産ウォレットで単一の鍵紛失や盗難による資産喪失リスクを避けたい場合などが挙げられます。こうした場面で有効とされている閾値署名は、「署名生成の権限を複数人に分散し、一定人数以上が協力した場合にのみ有効な署名を生成する」という仕組みを提供することで、これらのニーズに応える暗号技術です。

閾値署名は、特にブロックチェーン、Web3.0、分散型金融（DeFi）、分散型組織(DAO)など、中央管理者を置かない、あるいは権限を分散させたいシステムで広く採用されつつあります。これらのシステムでは、以下の 3 要素が重要とされています。

(1) 効率性：世界中に分散した参加者間で迅速に合意形成を行うため、通信コストや遅延が少ないこと

(2) 信頼性：巨額の資産管理や組織の重要な意思決定を扱うため、数学的に証明された高い安全性を持つこと

(3) 将来性：一度導入した基盤技術を後から変更するのは困難なため、将来の脅威（特に量子計算機）にも耐えうる長期的な安全性が確保されていること

近年、特に(3)の将来性の観点で、既存の閾値署名の多くが RSA 暗号や楕円曲線暗号といった、将来の汎用的量子計算機によって解読されるリスクのある暗号技術に基づいていることが大きな課題となっています。そのため、量子計算機に対しても安全な「耐量子」閾値署名方式の開発が急務とされています。

2. 従来方式における課題

これまでにも耐量子閾値署名方式は、格子暗号技術に基づく方式を中心としていくつか提案されてきましたが、従来方式には効率面または安全面に課題がありました。

理論的には任意の署名方式に対して「秘密計算」という技術による変換を施し閾値署名を設計できますが、既存の耐量子署名方式のほとんどは、秘密計算との相性が悪く、その変換により方式全体の計算コストが非常に増大してしまうことから実用的ではありません。格子ベース署名の場合は、安全性を確保するためにしばしば用いられる「棄却サンプリング」という処理がコスト増大の要因となります。

近年、この棄却サンプリングを用いない格子署名「Raccoon」が登場し、それを基にした閾値署名「Threshold Raccoon」※2が提案されました。Threshold Raccoon は署名サイズや計算コストが低いものの、署名生成に必要な通信の回数（ラウンド）が 3 回必要であり、より高速な通信が必要とされる分散システムには適していないという課題が残っていました。

この課題を解決するため、Espitau らが Threshold Raccoon を改良した 2 ラウンドの格子ベース閾値署名方式※3を開発しました。しかし、この方式の安全性証明は、「AOM-LWE」という、この方式のために新たに導入された特殊な安全性仮定に基づいていました。広く研究され、専門家コミュニティによって十分な安全性が吟味されている標準的な仮定（LWE など）とは異なり、この新しい仮定がどの程度信頼できるかが不透明であるため、金融システムなど極めて高い信頼性が要求される応用先での採用には懸念がありました。

3. 本技術のポイントと効果

本技術では、上述の課題を克服し、初めて 2 ラウンド構成、かつ、標準的な安全性仮定に基づく耐量子閾値署名方式「Ringtail」を開発しました。

技術的ポイント：過去の NTT の研究成果である格子ベース署名方式「MuSig-L」※4※5で用いられた安全性証明手法を発展させ、Espitau らの 2 ラウンドプロトコル構造に応用しました。プロトコル内部で使用する乱数の生成方法にガウス分布※6を利用することで、最も標準的で広く信頼されている格子暗号の安全性仮定である LWE の下で安全性を証明することに成功しました。

性能：Ringtail は、鍵生成や署名生成時の通信データ量が Threshold Raccoon や Espitau らの方式よりも少なく、効率面でも優れています。

実証実験：現実世界での性能を評価するため、日本、シンガポール、ドイツ、アイルランド、ブラジル、アメリカ東海岸と西海岸、およびオーストラリアの計 8 つのデータセンター拠点にサーバを設置し、プロトコル実装の動作実験を行いました。これらの拠点はアジア、ヨーロッパ、北米、南米、オセアニアの 5 大陸に分散しており、各拠点間の通信には大きなネットワーク遅延が発生します。このような地理的に広く分散した、実環境に近い厳しい条件下で実験を行うことで、グローバルな分散システムにおける実用性を検証しました。

実験結果：実験の結果、最も通信遅延が大きい拠点間（例：日本～ブラジル間など）を含む組み合わせにおいても、分散署名生成プロセス全体が平均約 2.5 秒で完了することを確認しました。（この時間には、署名生成のための準備段階（オフライン計算）と、実際の署名データ生成・検証（オンライン計算）が含まれます。）実際の署名操作に必要なオンライン処理時間は平均約 0.6 秒と非常に高速です。これは、日本と南米間のような物理的な距離によるネットワーク遅延と同程度の時間であり、プロトコル自体の効率が非常に高いことを示しています。企業の財務システムにおける高額送金の複数部署承認、暗号資産取引所での顧客資産

のコールドストレージからの移動、あるいは分散型ネットワークにおける重要なシステムパラメータ変更の共同決定など、高度なセキュリティと複数承認が求められる操作においては、十分に実用的な速度であると考えられます

プロトコル	閾値が任意	2 ラウンド構成	標準的安全性仮定
MuSig-L※4	× ※全閾値のみ対応※5	△ ※棄却のため、2+ε となる	○
Threshold Raccoon※2	○	× ※3 ラウンド方式	○
Espitau ら※3	○	○	× ※非標準仮定 AOM-LWE
Ringtail（本技術）※1	○	○	○

【表 1 ：MuSig-L、Threshold Raccoon、Espitau ら方式と Ringtail の特性比較】

4. 今後の展開

今後は、本技術のアプローチを、より複雑なアクセス制御を可能にする閾値グループ署名など、さらなる多機能暗号技術へと拡張する研究開発を進めます。これにより、量子計算機時代においても安心・安全な分散型システムの実現に貢献していきます。

NTT では、今後も高い安全性と優れた性能を両立し、社会で安心して利用できる安全な暗号技術の研究開発を推進していきます。

※1 “Ringtail: Practical Two-Round Threshold Signatures from Learning with Errors”. Cecilia Boschini, Darya Kaviani, Russell W. F. Lai, Giulio Malavolta, Akira Takahashi, Mehdi Tibouchi. In IEEE S&P 2025.

※ 2 “Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumption”. Rafael Del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, Markku-Juhani O. Saarinen. In EUROCRYPT 2024.

※3 “Two-Round Threshold Signature from Algebraic One-More Learning with Errors”. Thomas Espitau, Shuichi Katsumata, Kaoru Takemure. In CRYPTO 2024.

※4 “MuSig-L: Lattice-Based Multi-signature with Single-Round Online Phase”. Cecilia Boschini, Akira Takahashi, Mehdi Tibouchi. In CRYPTO 2022.

※5 MuSig-L は標準的安全性仮定に基づいて、ほぼ 2 ラウンド構成になっているのですが、一般的な閾値署名ではなく、ユーザ全員の承諾を必要とする「全閾値署名」となっているので、一般的な閾値署名に比べて応用例が限られています。

※6 ガウス分布は数値のばらつき方を表す最も基本的なパターンの一つで、平均値の周りに多くの値が集まり、平均値から離れるほど少なくなる「釣鐘（つりがね）」のような形が特徴

です。暗号技術においては、この分布が持っている数学的な特徴が方式の安全性を証明する上で重要な役割を果たす場合が多くあります。

■本件に関する報道機関からのお問い合わせ先
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
広報担当

問い合わせ先フォームへ