



NTT社会情報研究所
特別研究員

ティブシ・メディ Mehdi Tibouchi

量子脅威から社会を守る，耐量子署名とIOWNが築く次世代セキュリティ

量子コンピュータの驚異的な計算能力が，現在の暗号技術を無効化する未来。その脅威に立ち向かう次世代セキュリティ技術の1つが「耐量子しきい値署名」です。この技術をIOWN (Innovative Optical and Wireless Network) へ実装することで，いかにして揺るぎない通信インフラが実現されるのでしょうか。最新プロトコル「Ringtail」が拓く次世代のセキュリティと技術の到達点について，今回はこの「耐量子暗号」のトップランナー，ティブシ・メディ特別研究員に伺いました。

◆PROFILE:2006年パリ第6大学数学研究科修士課程修了。2007年パリ高等師範学校(ENS)卒業。2011年パリ第7大学・ルクセンブルク大学博士号(情報科学)取得。同年10月日本電信電話株式会社ポスドクとして勤務。2012年10月同社に正社員として入社。暗号学の研究に従事し，現在に至る。2018年京都大学大学院情報学研究科客員准教授。2016年電子情報通信学会 情報セキュリティ研究専門委員会「イノベーション論文賞」。2022年国際暗号学会IACR「ASIACRYPT 2022最優秀論文賞」。2023年国際暗号学会IACR「ASIACRYPT 2023基調講演者」。



次世代の情報セキュリティ「耐量子署名」の重要性と実装

■最初に「耐量子署名」について教えてください。

「耐量子署名」とは，デジタル社会における情報の信頼性と安全性を担保するための次世代セキュリティ技術です。現在，電子署名は自筆サインや印鑑に代わる「本人確認」や「改ざん検知」の要として広く利用されており，例えばネット通販のサイトが本物であることやスマートデバイスの無線アップデートがマルウェアではないことを保証します。しかし，量子コンピュータが実用化されると，現在広く使われている署名方式のほとんどが容易に突破されるおそれがあります。結果的に，既存デバイスやサービスがサイバー攻撃のリスクにさらされます。これに備え，量子コンピュータでも解読されない新たな署名方式，すなわち耐量子署名への移行は，現在世界的に極めて重要な課題となっています。

耐量子署名の実現に向けて，ここ10年ほど研究を行って

おり，主に3つのテーマに挑んできました(図1)。第1に，安全性根拠のしっかりとした「耐量子暗号プリミティブ」の理論研究です。電子署名をはじめとする「暗号プリミティブ」は，暗号技術を構築するための基本部品です。新たにプリミティブを設計したり，そのアルゴリズムの改良を考案したりすることによって，暗号技術の効率向上と安全性のさらなる強化ができます。第2に「実装安全性とサイドチャネル対策」です。アルゴリズムの理論強度だけでなく，機器の電力消費や物理的信号から機密を盗むサイドチャネル攻撃を防ぐ物理的堅牢性を追求します。そして第3に「耐量子暗号プロトコル」の設計です。プリミティブが暗号技術の基本部品であるのに対し，暗号プロトコルは複数の利用者や機器がそれらの部品を組み合わせ，情報をやり取りしながら，認証や署名などの目的を安全に実現するための手順です。

暗号プロトコルの研究では，特に「耐量子しきい値署名」に力を入れてきました。しきい値署名は署名に必要な秘密情報と署名権限を複数の参加者に分散し，所定の人数が協

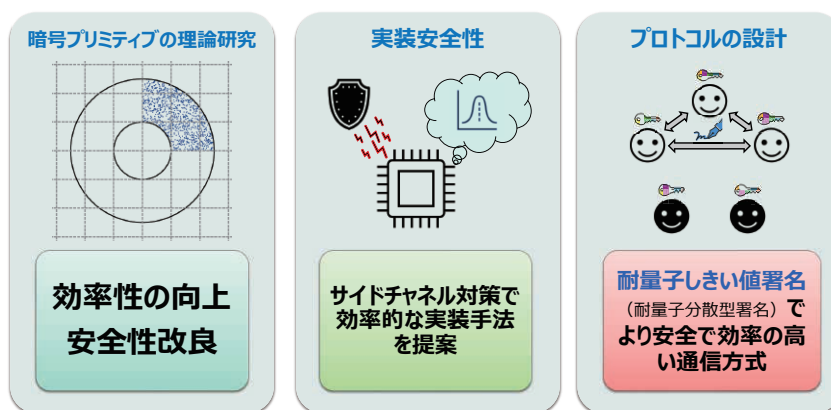


図1 耐量子署名の実現に向けて研究している3つのテーマ

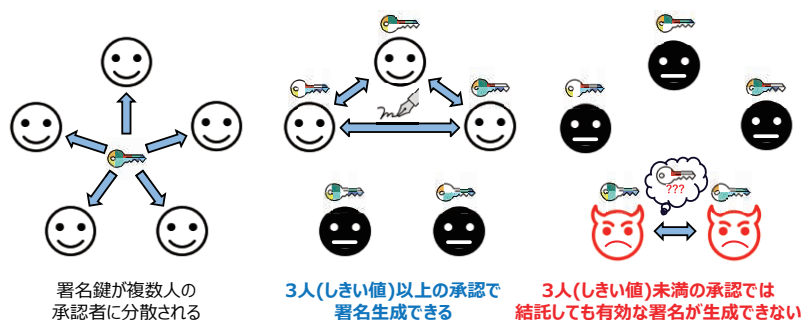


図2 しきい値署名の概念図

力したときにだけ署名を生成できるようにする技術です。暗号処理を分散させることで、秘密情報の漏洩や機器の故障、不正な操作といったリスクを抑え、システム全体の信頼性を高めるものです。現在は、理論的な設計に加えて実際のシステムで利用できる堅牢性や効率性も重視しながら耐量子しきい値署名の研究を進めており、量子コンピュータ時代の多様な情報サービスを支えるセキュリティ基盤を構築することをめざしています。

■「耐量子しきい値署名」に関する研究について詳しく教えてください。

通常の電子署名では、署名鍵を保有するユーザが単独で署名権限を行使しますが、この権限を複数人に分散することで安全性を大幅に高めることが可能であり、これがしきい値署名の根本的なアイデアです。これは企業における重要決済において、1人の承認で決済できる体制よりも複数名の承認を必須とすることで、安全性の面で有利になるというのと同じ理由です。2019年に、元教え子で立派な研究

者の高橋彰さんが当時留学していたデンマークのオーフス大学を訪れたことが耐量子しきい値署名の研究を始めたきっかけです。オーフス大学は世界有数の分散型暗号プロトコルの研究拠点であり、私は耐量子署名の研究を行っていたので、「分散型署名」と「耐量子署名」を組み合わせることは、互いの専門を活かせる自然な共同研究の対象となりました。その共同研究の結果として「MuSig-L（ミュージグエル）」という耐量子しきい値署名を開発しました。

しかし、この方式では安全性は確保できるものの、複数の承認者全員の承認がないと署名が生成できないという運用上の制約があり、改良が必要となりました。その結果開発されたのが、「Ringtail（リングテイル）」という署名方式です（図2）。

「Ringtail」の最大の特徴は、図2で示したように5名の署名者のうち任意の3名の承認が得られれば署名生成が可能となり、もし悪意のある署名者がいても3名未満の署名者の承認では署名生成が不可能になるというような方式を採用しています。この方式により、1台のサーバが攻撃さ



図3 5大陸間での分散署名実装実験

れても直ちに不正署名されることを防ぎ、故障や内部不正にも強い仕組みをつくることが可能になります。この署名者や承認者の人数（しきい値）は任意で調整することが可能で、人数を増やせばさらに安全性を向上させることができます。

加えて「Ringtail」には前述した「しきい値を任意にできる」という特徴以外にも、「2ラウンド構成」であるという決定的な強みがあります。ここでいうラウンド数とは通信の往復回数を指し、インターネット上での安全確認において過剰な通信回数は処理遅延やネットワーク負荷を増大させるため、可能な限り削減すべき指標です。「Ringtail」はこの2ラウンド構成を採用することで、通信全体にかかる負荷を効率的に軽減することに成功しました。これまでの耐量子しきい値署名は、効率面の追求か安全性への懸念のどちらかに問題を抱えていましたが、高度な安全性と通信効率の両立を高い次元で実現した耐量子しきい値署名としては、この「Ringtail」が世界初となりました。

■研究で苦勞された点や今後の研究に向けた課題点を教えてください。

これらの研究は日本をはじめ、欧州、北米、南米の研究者たちとの国際共同研究として進められていますが、各国の時差が常に実務的な課題となっています。日常的な打合せはオンライン会議が主体であり、各国の時間を調整するために、日本では早朝や深夜の対応を余儀なくされることも珍しくありません。特にコロナ禍においては、対面で集まれないことが研究遂行上の大きな障害となりました。

また技術面では、電子署名の生成にあたって通信回数（ラウンド数）、通信量、署名データサイズ、計算時間を同時に最小化する必要があります。しかし、通信量を減らそうとすると通信回数が増加するなど、1つの指標を改善すると別の性能が悪化するトレードオフが多く、これらのバランスを最適化することは非常に困難です。さらに、世界各地の通信環境の差異や、物理的距離に伴う遅延への対応も不可欠な課題でした。例えば、日本から見て地球の真裏にあたるブラジルとの間では、往復で0.4～0.6秒もの通信遅延が生じます。かつての通信速度からすればわずかな数値に思えるかもしれませんが、現代のデジタル環境においてこの遅延は決定的なボトルネックとなることがあります。

実際に私たちは「Ringtail」を用いて、5大陸・8地域間での同時展開実験を行いました（図3）。この実験では電子署名の生成に2.5秒を要しましたが、これは各地域のネットワーク環境や物理的な距離に起因する遅延によるものです。電子署名は本来、メッセージやデータのやり取りに先行して安全性を担保するための仕組みです。したがって、その処理にかかる時間は短ければ短いほど良く、この「先行する待ち時間」の短縮こそが、実用性を左右する極めて重要なポイントとなります。

■耐量子暗号の進化とIOWNが結実させるインフラの信頼性

■この研究の具体的な応用先や展望などを教えてください。

現在、私たちはこの「Ringtail」をさらに高速化・最適

化した「Tanuki (タヌキ)」という新しい耐量子署名を開発しています。また同時に、前述した技術的な課題へ個別にアプローチするための「Kettle (ケトル)」という耐量子署名プロトコルの研究も進行中です。これら「Tanuki」と「Kettle」は米国国立標準技術研究所 (NIST: National Institute of Standards and Technology) が開催するコンペへ投稿し、最終的には国際的な標準化をめざしています。

近い将来、NTTが推進するIOWN (Innovative Optical and Wireless Network) 構想のAPN (All-Photonics Network) によって大容量・低遅延な通信が実現すれば、医療画像のリアルタイム分析など、機密性の高いデータを遠隔地のクラウドで処理する局面も増加する見込みです。こうした重要な通信の内容を守るだけでなく、使用するソフトウェアや処理結果が改ざんされていない正しいものであることの確認が必須となります。耐量子署名は、そうした次世代通信サービスの信頼性を根底から支える技術です。一方、APNの低遅延性は、複数の署名者が相互に通信しながら署名を生成する分散型暗号の性能向上にも大きく貢献します。また、通信能力の向上によって署名者の人数を増やすことも可能となり、さらなる安全性向上が期待できます。このように、IOWNと耐量子しきい値署名は互いの技術を補完し合い、高め合う相互関係にあるといえます。

■所属されているNTT社会情報研究所について教えてください。

NTT社会情報研究所では情報技術を社会に役立てるための研究だけではなく、中には社会学や法律などの視点から情報と人との関係を考えるような人文的な研究をされている方もいます。ほかにもサイバーセキュリティやAIの安全性、デジタルウェルビーイング、個人データ保護の法制度などといった幅広いテーマに取り組んでいます。私が所属している暗号研究を専門分野とする阿部特別研究室については、企業の研究チームでありながら大学の研究室のような、アカデミックな環境に近い自由な雰囲気がある研究グループです。研究テーマも長期的な視点で選ぶことができ、海外の第一線の研究者が訪れる機会も多くあります。

私は1人で深く考える時間も大切にしていますが、複雑な問題に取り組む際には、異なる専門性やバックグラウンドを持つ方々との議論から生まれる化学反応が非常に重要だと感じています。多彩な研究者が1つの場所に集まっているこの研究所は、日本でも非常に恵まれた環境の1つだと思います。基礎研究と実社会への応用の両方を考えながら研究できることも大きな魅力です。

■最後に読者の方々へのメッセージをお願いします。

ビジネスの最前線にいる皆さんが現場で直面しているセキュリティの課題を、ぜひ研究者に聞かせていただきたいと思います。実社会の切実な困り事こそが、新しい技術の出発点であり、次の時代を創る研究テーマとなるからです。

研究者や学生の皆さんには、機会があれば、ぜひ海外の研究室を訪れたり、留学したりしてほしいと思います。費用の上昇や国際情勢などにより、以前より簡単ではない面もありますが、異なる研究文化や考え方に触れることで、新たな研究課題や問題の解き方を持ち帰ることができます。ただし、海外滞在は予定より長くなることもあります。私自身、最初は半年ほどのインターンとして日本に来ましたが、そのご縁が現在も続いています。

また、研究を続けるにあたっては、研究を通じて築いた友情や共同研究の絆を大切にすることと、皆で楽しく研究していくことが大事だと思います。私の好きな日本のことわざで、「笑う門には福来たる」があります。研究では、失敗したり長く行き詰まったりすることも珍しくないのですが、そのようなときでも、深刻になりすぎず、少しユーモアを持って皆で前向きに取り組むことをお勧めします。



(今回はリモートにてインタビューを実施しました)