（報道発表資料）

2023.11.27

Wi-Fi 接続の認証などの安全性を脅かすタイミング攻撃に対抗できる高速な暗号実装方法の実現

～平方剰余を判定する安全で高速なアルゴリズムを開発～

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、デンマークの Aarhus University との共同研究により、入力値に依存せず一定の時間で平方剰余※1を判定する高速で汎用性のあるアルゴリズムを開発しました。本技術は計算時間の変化を利用して情報を盗み取るタイミング攻撃を防止し、ブロックチェーンの分散電子署名・電子パスポートの認証・Wi-Fi ルータにおけるパスワード鍵交換などの暗号機能の安全かつ高速な実装に貢献します。今回「楕円曲線へのハッシュ関数」※2 の計算において本成果が高度な安全性と大幅な高速化を実証し、広く活用されている楕円曲線へのハッシュ関数の計算において、従来手法の 2.5～3.5 倍の高速化を実現しました（図 1）。また、より大きなパラメータの楕円曲線を用いる耐量子計算機暗号方式 CTIDH※3 の場合においては、楕円曲線へのハッシュ関数は最大 46 倍の高速化を実現しました。

なお、本成果は 2023 年 11 月 26 日から 30 日まで、デンマーク・コペンハーゲンで開催される ACM CCS 2023 にて採択論文※4 が発表されます。

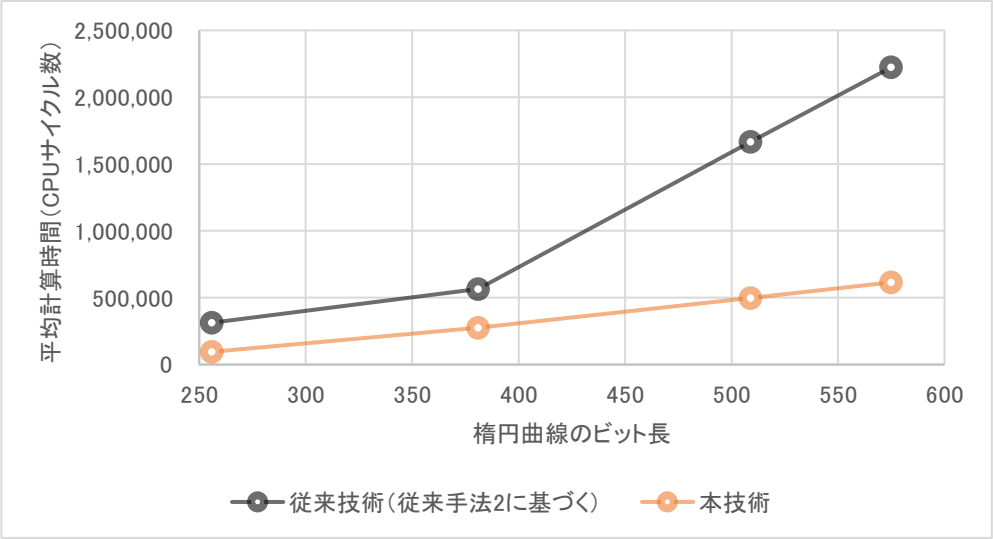

図 1　楕円曲線ハッシュ関数の計算速度比較

1. 研究の背景

現在もっとも普及している暗号技術のひとつである楕円曲線暗号は、秘密の値を楕円曲線上の点に変換する演算（楕円曲線へのハッシュ関数）が、ブロックチェーン技術で利用される BLS 電子署名、電子パスポートのパスワード認証鍵交換、Wi-Fi ルータの WPA3 標準などの演算に多用され

ています。さらに、量子コンピュータに対しても安全と考えられている同種写像を利用した次世代の耐量子計算機暗号方式 CTIDH などでも使われています。

楕円曲線へのハッシュ関数を計算するためには、与えられた整数値と楕円曲線のパラメータのひとつである素数に関する「平方剰余判定問題」を解く必要があります。これは、整数 a に素数 p の倍数を加えて完全平方数を作れるか否かを判定するもので、200 年以上の歴史をもつ基本的な数論の問題です。

また、楕円曲線へのハッシュ関数は秘密の入力値に依存しない一定の実行時間（コンスタント時間）となるよう実装することが必要です。入力値によって計算時間が変化してしまうと、攻撃者が計算時間を測定して秘密の入力値を推定する「タイミング攻撃」に対して脆弱となるためです。ウェブ・ネット通信暗号化プロトコル TLS を解読する Lucky Thirteen 攻撃や、Wi-Fi ルータの WPA3 標準プロトコルからパスワードを盗み出せる攻撃[※5] などがタイミング攻撃の実例として報告されており、暗号実装に対する現実的で深刻な脅威です。このため、楕円曲線へのハッシュ関数内部で使われる平方剰余判定のアルゴリズムも、コンスタント時間であることが求められます。

2. 従来手法の制限

従来、主にふたつの平方剰余判定方法が用いられてきました。ひとつは平方剰余の相互法則に基づく方法で、p を法とする a の平方剰余判定を p より小さい素数を法とする判定問題に帰着します（以下「従来手法 1」）。この方法はユークリッドの互除法に類似した手順で非常に高速ですが、より小さい法への帰着回数が入力 a に依存するためコンスタント時間とならず、タイミング攻撃に対して脆弱です。

もう一方は、フェルマーの小定理に基づいて平方剰余判定を法 p のべき乗演算に帰着する方法です（以下「従来手法 2」）。べき乗演算は入力値に依存しないコンスタント時間とすることが容易でありタイミング攻撃に対して安全ですが、演算自体が複雑となるため、従来手法 1 に比べて数十倍の時間がかかります。

このように、従来技術で楕円曲線へのハッシュ関数を実装する場合、安全性と高速性が同時に成り立たちませんでした。

3. 本技術のポイントと効果

上述のように、平方剰余判定の既存技術は概ね、高速であるがタイミング攻撃に対する脆弱な従来手法 1 に基づく技術と安全に実装できるが処理速度が遅い従来手法 2 に分けることができます。一方、本技術では安全性と効率性を両立した平方剰余判定を開発しました（図 2）。

- 本技術の基本的なアイデアは、従来手法 1 の高速な計算構造を定数の行列の乗算として書き換え、コンスタント時間の実装に変換することです。これは従来手法 1 と計算構造が類似しているユークリッドの互除法のコンスタント時間実装[※6] から着想を得ています。
- 平方剰余判定の計算に特有の状況として途中結果が負の値となる場合があるため、ユークリッドの互除法と同じアプローチでは直ちにコンスタント時間のアルゴリズムは得られません。本技術では負の値となる場合の符号判定方法を工夫して符号にかかわらない処理動作とすることによりこの問題を解決しました。

これによって、脆弱で高速な従来手法 1 と同程度の計算速度でありながら、低速で安全な従来手

法 2 と同等の安全性を実現しました(図 2)。BLS 電子署名で用いられる楕円曲線へのハッシュ関数の計算では、従来手法の 2.5～3.5 倍の高速化が確認できました(図 1)。より大きなパラメータの楕円曲線を用いる耐量子計算機暗号方式 CTIDH の場合の効果は顕著で、楕円曲線へのハッシュ関数は最大 46 倍の高速化となっています。

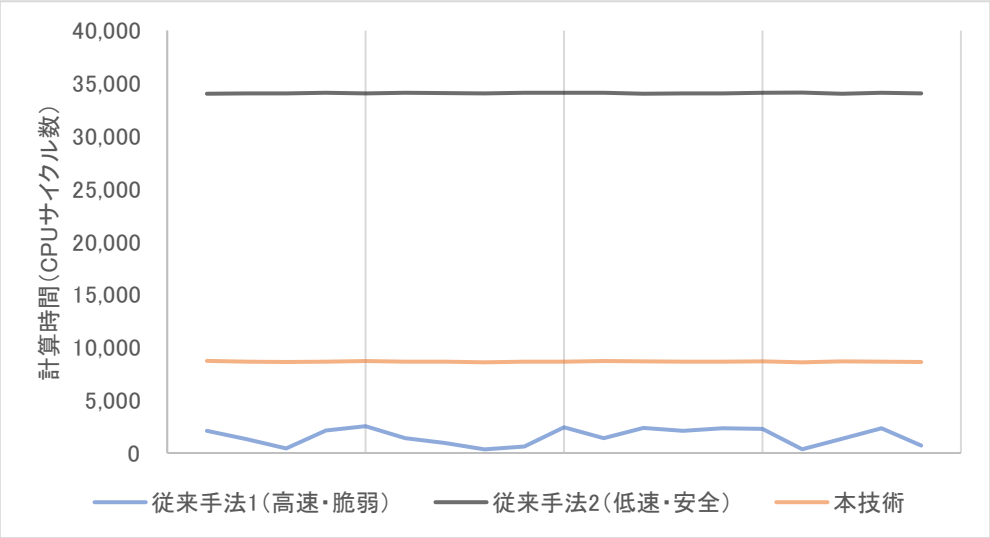

図 2 ランダムな低ハミング重み入力(横軸)に対する 254 ビット素数を法とした平方剰余判定の計算時間(縦軸)の比較。従来手法 1 は入力に依存して計算時間が異なる脆弱性が出現し、従来手法 2 は本技術の 3 倍以上の処理時間を要している。

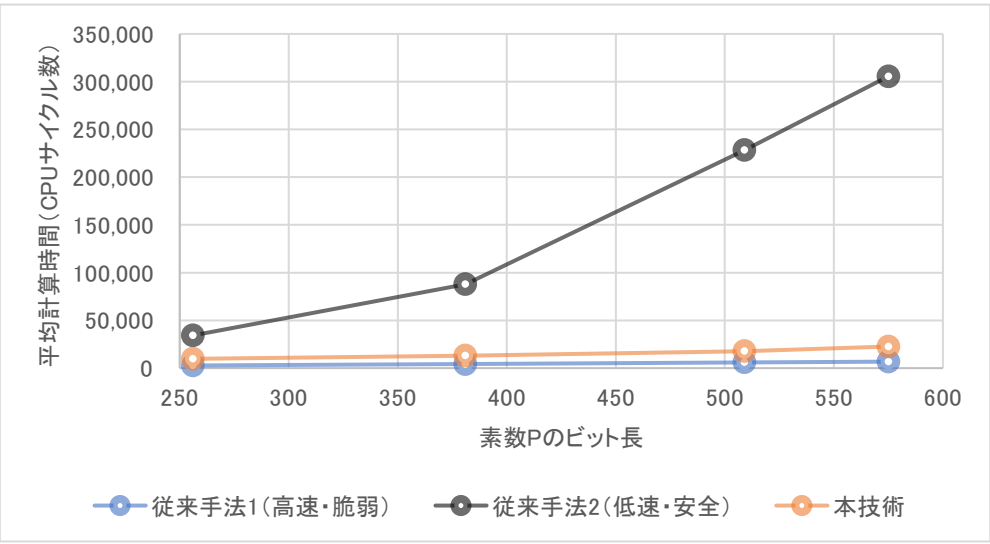

図 3 パラメータサイズに対する平方剰余判定の計算速度比較

今回の平方剰余判定アルゴリズムを国際会議 ASIACRYPT 2022 で先行発表し論文賞を獲得した楕円曲線へのハッシュ関数の改良技術[※7]と組み合わせることで一層の高速化が期待できます。

4. 今後の予定

今回開発した方式は暗号技術で用いられる楕円曲線の種類やパラメータによらず、プラグイン利用できる高い汎用性を持つ技術である。この成果により現在使用されている様々な暗号技術のタイミング攻撃に対する安全性向上に貢献するだけでなく、近い将来の耐量子計算機暗号を高速化し、その実用化に向けて貢献することが期待できます。

NTT では、今後も安全性と性能を高いレベルで両立し、理論的成果で実用に貢献する安全な暗号実装の研究開発を推進していきます。

※1 9＝3×3 や 49＝7×7 など、とある整数の 2 乗である整数は完全平方と言います。なお、完全平方を素数pで割ったときの余りとなる整数は「p を法とした平方剰余」と言います。たとえば、7 で割ったときに 9 の余りは 2 になるため、2 は 7 を法とした平方剰余です。一方、3 は 7 を法とした平方剰余ではないことを証明できます。p より小さい自然数 a が p を法とした平方剰余であるかどうかを判定するのは「平方剰余判定」です。現在標準的に使われている楕円曲線暗号をはじめ、次世代の耐量子計算機暗号でも必要とされる基本的な数学操作です。

※2 楕円曲線は、現在の暗号技術の大部分において「暗号計算の空間」となるような曲線です。楕円曲線へのハッシュ関数は、メッセージ（パスワード・鍵など）を楕円曲線の点として表す方法となります。新たなメッセージを表す点はランダムであることなどの安全性条件を満たすべきです。

※3 大規模な量子計算機が将来的に実現されたら、楕円曲線暗号を含め現在日常的に使用されているほとんどの公開鍵暗号技術が短時間で解読される手法（Shor アルゴリズム）が知られているため、量子計算機に対する耐久性を持つ「耐量子計算機暗号技術」の開発と普及が最近の暗号学研究の緊急課題です。鍵サイズや暗号文サイズが非常に短いとして耐量子計算機暗号の有力候補とされている CTIDH 方式においても、楕円曲線へのハッシュ関数が使われており、本技術で劇的に高速化できます。

※4 “Faster constant-time evaluation of the Kronecker symbol with application to elliptic curve hashing”. Diego F. Aranha, Benjamin Salling Hvass, Bas Spitters, Mehdi Tibouchi. In ACM CCS 2023.

※5 “Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd”. Mathy Vanhoef, Eyal Ronen. In IEEE Symposium on Security & Privacy 2020.

※6 “Fast constant-time GCD computation and modular inversion”. Daniel J. Bernstein, Bo-Yin Yang. IACR TCHES 2019(3):340-398, 2019.

※7 “SwiftEC: Shallue-van de Woestijne indifferentiable function to elliptic curves”. Jorge Chavez-Saab, Francisco Rodriguez-Henriquez, Mehdi Tibouchi. In ASIACRYPT 2022.

■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

nttrd-pr@ml.ntt.com