

各位

東京都千代田区外神田四丁目 14 番 1 号
株式会社アクセル
(コード番号 6730 東証スタンダード)

完全準同型暗号（TFHE）高速化の論文が「CHES 2026」に採録決定

～暗号領域における著名な国際会議に論文が採録された特許出願中の新アルゴリズム～

株式会社アクセル（本社：東京都千代田区、代表取締役：松浦 一教、以下「アクセル」）は、松岡 航太郎 氏（京都大学大学院 情報学研究科）との共同研究により、暗号化したまま計算可能な次世代技術「TFHE（Fully Homomorphic Encryption over the Torus）」において、実用化に向けた最大の課題である処理速度を大幅に向上させる新アルゴリズムを開発いたしました。本研究成果をまとめた論文が、暗号ハードウェアおよび組み込みセキュリティ領域における国際学会「CHES 2026（International Conference on Cryptographic Hardware and Embedded Systems）」に採録されましたのでお知らせいたします。

（CHES 2026 について）

「CHES（International Conference on Cryptographic Hardware and Embedded Systems）」は、IACR（国際暗号学会）が主催する、暗号ハードウェアおよび組み込みセキュリティ領域における著名な国際会議です。本研究の論文は、同会議と連動する学術誌「TCHES（IACR Transactions on Cryptographic Hardware and Embedded Systems）」の査読を経て採録が決定したものであり、アクセルの高度なアルゴリズム開発力と技術の先進性が国際的に実証されたことを意味します。

（完全準同型暗号（TFHE）の将来性と課題）

「TFHE」は、クラウド上などに送信したデータを一切復号（暗号解除）することなく、暗号化した状態のままで検索や AI 推論などの各種演算を実行可能にする次世代の暗号技術です。現在主流のハードウェア方式（TEE 等）は、CPU や GPU の内部で一時的にデータを復号して計算する仕組みであるため、ハードウェア自体の脆弱性や物理的な攻撃によってデータが漏洩するリスクをゼロにすることはできません。一方で、TFHE は計算過程も含めデータを一度も復号しないため、ハードウェア依存のリスクを排除し、ソフトウェア（数学理論）のみで堅牢なセキュリティを実現できる点が評価されています。しかし、TFHE は暗号演算に伴う計算量が大きく、処理速度の向上が実用化に向けた研究課題となっています。当社ではこのボトルネックを解消するため、研究開発に取り組んでおります。

（本研究成果の要旨 ※論文より引用）

本研究では、TFHE の実用化に向けた最大の課題である処理速度の向上を目的として、暗号化した整数データに対する新たな除算および乗算アルゴリズムを構築いたしました。

従来の TFHE の整数除算は、条件分岐が困難なため処理コストの大きい筆算型アルゴリズムを用いざるを得ず、計算時間が極めて長くなる課題がありました。これに対し本研究では、除算を「逆数計算」と「乗算」に分解する手法に着目し、以下 2 つのアルゴリズムを考案いたしました。

LUTNR (LUT Newton-Raphson)

データの上位ビットからルックアップテーブル (LUT) を用いて「逆数の概算値」を高速に抽出し、整数ニュートン・ラプソン (NR) 法により高精度に補正する手法。既存の標準ライブラリ (TFHE-rs) と比較して約 1.8 倍の高速化を達成。

ReducedNR (Reduced Newton-Raphson)

極小の LUT から段階的に精度を倍々に引き上げて補正する手法。大型の LUT が配置しにくい環境においても安定した処理能力を発揮し、TFHE-rs と比較して約 1.3 倍の高速化を達成。

また、同一の割る数 (除数) を繰り返し使用する演算処理 (平均値計算や各種係数処理等) においては、算出済み逆数の再利用により最大約 3.6 倍の高速化を確認しております。

(今後の展望)

本成果は、ただちに製品や商用サービスへ適用されるものではなく、将来の社会インフラ構築を見据えた先駆的な基礎研究 (先行 R&D) の位置づけとなります。

今後、医療・ゲノムデータの安全なクラウド解析、金融・信販分野における機密データの高度照合や不正検知など、高度なプライバシー保護と計算処理の両立が要求される領域での実用化に向け、さらなる研究開発および技術アライアンスの構築を推進してまいります。

なお、本アルゴリズムに関しては特許を出願しており、特定のアプリケーションや TFHE に限定されず、他の暗号方式や高度な数値計算処理等への派生・応用も可能であることから、技術の広範な活用が期待されます。

(採録論文の概要)

論文題名

『Multiplicative Integer Division over Integer-wise TFHE』

著者

松岡 航太郎 (京都大学大学院 情報学研究科)

星月 優佑 (株式会社アクセル)

佐藤 高史 (京都大学大学院 情報学研究科 教授)

掲載誌

IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)

(関連プレスリリース)

2023 年 1 月 30 日 完全準同型暗号 TFHE の高速化に関する論文を共同発表

https://www.axell.co.jp/news/pdf/AXELL_PR20230130.pdf

2025 年 12 月 18 日 完全準同型暗号「TFHE」において特許登録件数 国内 No.1 を達成

<https://www.axell.co.jp/news/20251218.html>

(アクセルについて)

アクセルは、高度なアルゴリズム開発から製品化を担うソフトウェア・ハードウェア開発まで一貫した開発体制を保有する先端テクノロジー企業です。大規模な LSI の設計開発に加え、AI 等の先端技術を社会実装することで、デジタル技術によるビジネス改革に貢献します。

<https://www.axell.co.jp/>

■本リリースに関するお問い合わせ先

株式会社アクセル

E-mail : kouhou@axell.co.jp

以 上

- 記載されている会社名、製品名、サービス名、規格名等は、一般に弊社及び各社・団体の登録商標又は商標です。