2023 年 1 月 30 日

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 の高速化に関する論文を共同発表

～ 「2023 年 暗号と情報セキュリティシンポジウム」において、
TFHE の算術演算の高速化に関する論文を発表 ～

高度なアルゴリズム開発力を強みに、先端 LSI の設計開発や機械学習/AI、暗号技術及びブロックチェーン技術を活用したソリューションを提供する株式会社アクセル（本社：東京都千代田区、代表者：斉藤昭宏）は、「2023 年 暗号と情報セキュリティシンポジウム（SCIS2023）」において、Integer-wise 型完全準同型暗号（TFHE: Torus Fully Homomorphic Encryption）の算術演算の高速化に関する論文を京都大学と共同発表しました。

本論文は、2021 年 11 月に開催された WAHC2021※にて共同発表した内容を発展させたもので、TFHE を実用化する際に課題となっている演算時間の高速化を行うものです。アクセルでは、今後、ユーザのプライバシー保護の重要性が高まると考えており、TFHE の高速化を行うことで、TFHE の実用化を加速させることを目指しています。

※WAHC 2021 は、コンピュータ及び通信のセキュリティに関する国際会議 ACM Conference on Computer and Communications Security（ACM CCS）が主催するオンラインワークショップです。

■TFHE について

完全準同型暗号「TFHE」とは、暗号化したデータを復号せずに暗号化したまま、加算と乗算を含む任意の演算が可能な秘匿演算技術です。サーバ/クラウド上に暗号化された状態で保管されているデータに対して、ユーザは暗号化した検索キーワードを送り、暗号化したデータ同士で演算処理を行うことが可能です。サーバ/クラウドに保管されているデータの秘匿性が確保されることに加え、サーバ/クラウド側に演算処理の内容を知られることなく処理結果を返すことから、ユーザのプライバシーも保護することが可能な技術です。情報を秘匿したままデータ解析ができるため、遺伝子（ゲノム）データ解析、患者の治療実績や薬剤服用履歴、類似症状の検索等、医療業界をはじめ、インターネットバンキングや住民情報を扱う自治体への応用も期待されています。

■2023 年 暗号と情報セキュリティシンポジウム（SCIS2023）

会期：2023 年 1 月 24 日（火曜日）～27 日（金曜日）
場所：リーガロイヤルホテル小倉
URL：https://www.iwsec.org/scis/2023/index.html

■発表の要旨 ※論文より引用

完全準同型暗号(FHE)の一種である TFHE を,平文に整数をとるように拡張した integer-wise TFHE において, 4-bit の符号付き・符号無し整数の乗算, 4-bit 整数の除算, Full Domain Functional Bootstrapping (FDFB)のより計算量の少ない構成法を提案する. これらの演算の構成において最も重い操作は Look Up Table (LUT)の暗号上での評価を行う, Blind Rotate (BR)と呼ばれる準同型演算である. 我々の提案法の

主なアイデアは，この LUT をそれぞれの演算に適した形で構成することで BR の数を削減することである. これにより提案法では、4-bit 符号無し乗算, 符号付き乗算, 除算, FDFB をそれぞれ 4BR, 6BR, 7BR, と 2BR で実現する.

■著者
Kotaro Matsuoka (Kyoto University, Kyoto, Japan)
Yusuke Hoshizuki (AXELL CORPORATION, Tokyo, Japan)
Takashi Sato (Kyoto University, Kyoto, Japan)
Song Bian (Kyoto University, Kyoto, Japan)

TFHE の応用が記載される分野：自治体、医療、インターネットバンキングなど

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、機械学習/AI や暗号・ブロックチェーン技術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
（報道関係）
IR・広報チーム 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。