PRESS　RELEASE

2021 年 11 月 15 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　東証第 1 部）

アクセル、完全準同型暗号 TFHE に関する論文を共同発表

～ 国際会議 ACM CCS 主催の WAHC 2021 に採録 ～

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：松浦 一教）は、完全準同型暗号（TFHE: Torus Fully Homomorphic Encryption）に関する論文を京都大学と共同発表しました。論文は、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 WAHC 2021（9th Workshop on Encrypted Computing and Applied Homomorphic Cryptography）に採録されました。

■論文情報

Title：　Towards Better Standard Cell Library: Optimizing Compound Logic Gates for TFHE

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

論文 URL：https://dl.acm.org/doi/10.1145/3474366.3486927

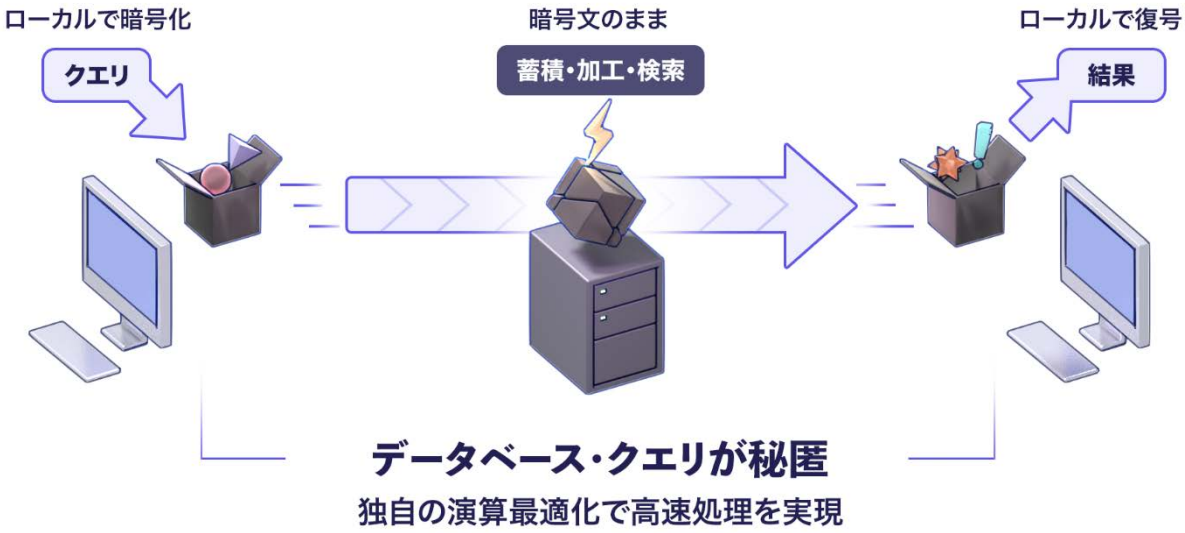
TFHE は秘密計算の一種で、「完全準同型暗号」とは加算と乗算を含む任意の演算が可能な秘匿演算技術です。暗号化したデータをサーバ/クラウドに置き、ユーザは暗号化した検索キーワードをサーバ/クラウドに送り、暗号化したデータ同士で演算処理を行います。サーバ/クラウド側は、演算処理の内容を知ることなく、ユーザに演算処理結果を返します。

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。

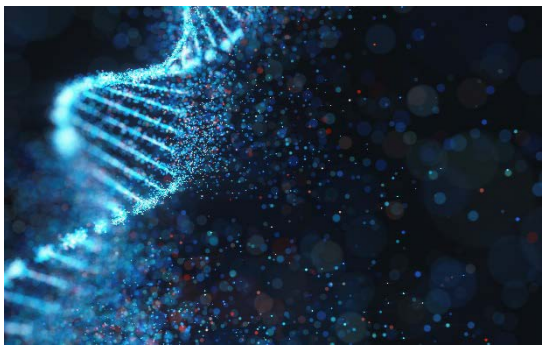
TFHE の原論文「TFHE: Fast Fully Homomorphic Encryption over the Torus」では、2 入力の論理演算を繰り返し行うための技術を提案しており、これを用いることで任意の演算が行えることをまとめています。しかしながら、実用化するには一つ一つの演算処理が重く、さらなる高速化がハードルの一つになっています。

アクセルが今回共同発表した論文は、演算処理の高速化についてまとめたものです。演算単位一つに対し、より複雑な計算を行うモジュールを作成し、同モジュールを使用することで、少な

い演算処理で複雑な計算を可能にしました。具体的には、原論文で提案された論理演算に加えて、Full Adder（全加算器）、AOI 演算（複合論理演算）等の 3 入力演算を最適化した構成を加えることで、システム全体として高速化することを発表しています。



<今回発表したシステム概要図>



<TFHE の応用が期待される分野：自治体、医療、インターネットバンキングなど>

アクセルでは、今回共同発表した論文の実証実験を行うことができる OSS（オープンソースソフトウェア）を GitHub に公開しています。また、専用サイトを開設し、GitHub で公開しているコードを使用したソリューションも展開していきます。
GitHub リンク：https://github.com/axell-corp/oveus-tfhe
専用サイトリンク：https://oveus.jp/

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 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。

アクセルホームページ：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

株式会社アクセル　Email：kouhou@axell.co.jp

以上
