1X-06

センサデータ活用のためのIoTデバイスにおける準同型暗号を用いた暗号化の高速化

松本 茉倫† 小口 正人†
†お茶の水女子大学

1 はじめに

IoTデバイスの普及に伴い，クラウドサービス上で取得したデータを統計分析した結果を活用することが期待されている．しかし，必ずしも安全とは言えないクラウドサービス上では情報漏洩に備えて，個人情報を保護する必要がある．そこで，暗号文同士の加算・乗算が任意回数可能な性質を持つ完全準同型暗号 (以下 FHE: Fully Homomorphic Encryption) やあらかじめ設定した回数の範囲内で加算と乗算が可能な Leveled 準同型暗号 (以下 LHE: Leveled Homomorphic Encryption) が注目されている．しかしながら，FHE と LHE は処理が重く，暗号文のサイズが大きいため通信量が多くなってしまうことが計算能力の低い IoT デバイス上での実装の課題となっている．先行研究で Lauter ら [1] は現在主流な共通鍵暗号である AES と FHE を組み合わせた暗号化の高速化と通信量削減を提案している．Gentry ら [2][3] は実際に Laptop を実験に用いて実装した結果を示した．著者ら [4][5] は AES に加えてストリーム暗号の TRIVIUM，軽量ブロック暗号の KATAN を LHE に組み合わせ，スマートフォンをクライアントとして実装し，クライアントへの負荷・通信量・サーバへの負荷を比較した．この手法では処理の重い FHE や LHE をクライアントで使うことに変わりはない．

本研究では，IoT デバイスでの暗号化の高速化・通信量削減を目指し，FHE や LHE より軽量な Somewhat 準同型暗号 (以下 SHE: Somewhat Homomorphic Encryption) を LHE に組み合わせる手法を提案する．実験の結果，提案した手法では LHE で暗号化した場合に比べてクライアントへの負荷を減せることが確認できた．

2 システムデザイン

2.1 LHE only

図 1 に示す LHE only はシンプルで実装が容易であるが，問題点として，クライアントにおける LHE を使った暗号化に時間がかかること，暗号文サイズが大きくなることが挙げられる．

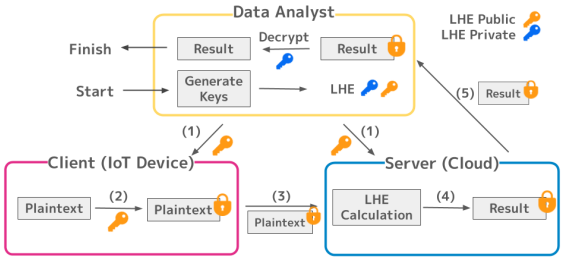

図 1: LHE only

2.2 SHE+LHE

クライアントには LHE よりも軽量な暗号を使わせ，サーバ側で LHE の暗号文に変換すればよいという発想から設計されたのが SHE+LHE である．

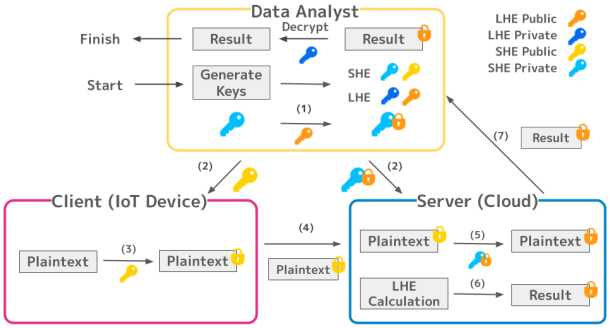

図 2: SHE+LHE

図 2 の SHE+LHE を利用する利点はクライアントが LHE を使わなくてよいことである．一方でサーバへの負荷は大きいという欠点があるが，クライアントの性能よりもサーバの性能が一般に高いことを活かすことができる．

3 実験

3.1 実験環境

実験に使用したマシンの性能を表 1 に示す．本研究ではクライアントとしてスマートフォンの Google Pixel 3，サーバとしてラップトップの MacBook Pro を実験に用いた．

Speeding Up Encryption on IoT Devices Using Homomorphic Encryption for Sensor Data Utilization
†Marin Matsumoto †Masato Oguchi
†Ochanomizu University

表 1: マシン性能

Device	OS	CPU	Number of Cores	Processor Speed	RAM
Google Pixel 3	Android 9.0	ARM Cortex-A75 ARM Cortex-A55	8	2.5 GHz 1.6 GHz	4GB
MacBook Pro	OS X 10.15	Intel Core i5	4	1.4GHz	8GB

3.2 実験概要

平文サイズを 16B，32B，48B，64B，80B と変化させ，LHE only，SHE+LHE でクライアントへの負荷 (クライアントにおける実行時間)，通信量 (クライアントから送信するファイルサイズ)，サーバへの負荷 (サーバで LHE の暗号文へ変換する場合の実行時間) の 3 つの比較を行った．

3.3 実験結果

3.3.1 クライアントへの負荷

図 3 から，SHE+LHE では LHE only に比べて高速に暗号化できることが読み取れる．

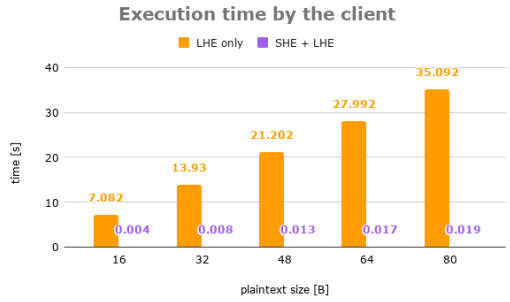

図 3: 実験結果：クライアントへの負荷

3.3.2 通信量

図 4 からは，平文がすべて LHE の暗号文になる LHE only では SHE+LHE と比較して大幅に通信量が多いことがわかる．

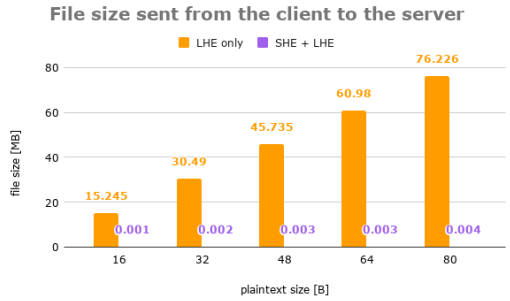

図 4: 実験結果：通信量

3.3.3 サーバへの負荷

図 5 にはサーバで LHE の暗号文へ変換する場合の実行時間を示す．この処理は LHE only では行わないため，0 秒である．

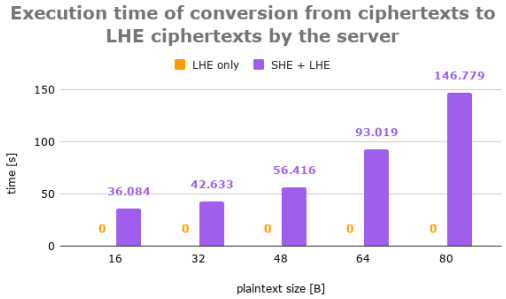

図 5: 実験結果：サーバへの負荷

4 まとめと今後の課題

IoT デバイスで取得したセンサデータを安全に統計分析などに有効活用する際には，暗号文同士の演算が可能な暗号の LHE が有用であるが，LHE による暗号化は時間がかかり，暗号文サイズが大きくなるという欠点がある．そこで本研究では IoT デバイス側では LHE よりも軽量な SHE によって平文を暗号化し，代わりにクラウドサービス側で SHE から LHE の暗号文へ変換する手法を提案した．

実験の結果，IoT デバイスにおいて平文を LHE で暗号化した場合に比べて，提案手法では IoT デバイスへの負荷が格段に減らせるため，提案手法の方が優れたシステムデザインであると考えられる．

今後はサーバ側での具体的なアプリケーションを想定した実験を検討している．

謝辞

本研究は一部，JST CREST JPMJCR1503 の支援を受けたものである．

参考文献

[1] Kristin Lauter, Michael Naehrig, and Vinod Vaikuntanathan. Can homomorphic encryption be practical? In *CCSW '11: Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, pp. 113–124, 2011.

[2] Craig Gentry, Shai Halevi, and Nigel P. Smart. Homomorphic evaluation of the aes circuit. In *Advances in Cryptology – CRYPTO 2012*, pp. 850–867, 2012.

[3] 佐藤宏樹, 馬屋原昂, 石巻優, 今林広樹, 山名早人. 完全準同型暗号のデータマイニングへの利用に関する研究動向. 情報科学技術フォーラム講演論文集 (FIT), pp. 165–172, 2016.

[4] 松本茉倫, 小口正人. 完全準同型暗号と共通鍵暗号を組み合わせた IoT デバイスにおけるセンサデータ暗号化の高速化. マルチメディア, 分散協調とモバイルシンポジウム 2020 論文集, pp. 712 – 719, 2020.

[5] Marin Matsumoto and Masato Oguchi. Speeding up sensor data encryption with a common key cryptosystem combined with fully homomorphic encryption on smartphones. In *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability (WS4 2020)*, pp. 500 – 505, 2020.