IoT デバイスにおける共通鍵暗号と完全準同型暗号を組み合わせた暗号化の高速化へ向けた検討

松本 茉倫† 小口 正人†

† お茶の水女子大学 〒 112–8610 東京都文京区大塚 2-1-1
E-mail: †marin@ogl.is.ocha.ac.jp, oguchi@is.ocha.ac.jp

あらまし スマートフォンを始めとする，IoT デバイスで取得したセンサデータを活用するためにクラウドサービスを利用した統計分析が普及している．IoT デバイスで取得したセンサデータの中には，位置情報などの秘匿性が高いデータが存在しており，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・乗算が可能な完全準同型暗号が注目されている．しかし，一般的に共通鍵暗号方式よりも公開鍵暗号方式は低速であり，公開鍵暗号方式である完全準同型暗号は処理時間がかかるため，計算能力の低い IoT デバイス上での実装が課題である．この問題に関し，例えばインターネット上でデータを暗号化して送受信するプロトコルである SSL では，低速な公開鍵暗号を高速に利用することを目的として，高速な共通鍵暗号方式と鍵共有が容易な公開鍵暗号方式を組み合わせたハイブリッド暗号方式という暗号方式が用いられている．本研究では，計算資源が限られたデバイスでも暗号化を高速に行ってクラウドサービス上で統計分析するため，共通鍵暗号方式と公開鍵暗号方式である完全準同型暗号を組み合わせた暗号化を提案する．

キーワード IoT デバイス，完全準同型暗号，共通鍵暗号

Speeding Up Sensor Data Encryption with a Common Key Cryptosystem combined with Fully Homomorphic Encryption on IoT Devices

Marin MATSUMOTO† and Masato OGUCHI†

† Ochanomizu University,
2–1–1 Otsuka, Bunkyou-ku, Tokyo 112–8610 Japan
E-mail: †marin@ogl.is.ocha.ac.jp, oguchi@is.ocha.ac.jp

1. はじめに

スマートフォン・スマートウォッチといった IoT デバイスの普及によって，位置情報・心拍数など様々なセンサデータを取得可能になった．取得したデータはクラウドサービス上で統計分析を行い，分析結果を活用することが期待されている．センサデータの中には，秘匿性が高いデータが存在しており，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．しかし通常の暗号化を行うとクラウド上で分析処理を行う事が出来なくなる．そこで，暗号文同士の加算・乗算が可能な完全準同型暗号 (以下 FHE: Fully Homomorphic Encryption) が注目されている．

しかし，一般的に共通鍵暗号方式に比べて公開鍵暗号方式は低速であり，公開鍵暗号方式である FHE による暗号化は共通鍵暗号方式に比べて処理に時間がかかる．また，FHE の暗号文サイズが大きいため通信量が大きくなってしまう．これらの欠点によって，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．低速な公開鍵暗号を高速に利用するために，インターネット上でデータを暗号化して送受信するプロトコルである SSL では高速な共通鍵暗号方式と鍵共有が容易な公開鍵暗号方式を組み合わせたハイブリッド暗号方式という暗号方式を用いている．

先行研究 [1] では，現在主流な共通鍵暗号方式である AES と FHE を組み合わせることで，暗号化の高速化と通信量削減を提案している．先行研究 [2] では，実際に Laptop を用いて AES と FHE を組み合わせた暗号の実装・評価を行った [3]．本研究では，スマートフォンのような IoT デバイスにおいて，共通鍵暗号と FHE を組み合わせることで FHE による暗号化の高速化と通信量削減を提案する．共通鍵暗号には AES と TRIVIUM を使用し，それぞれと FHE を組み合わせ，クライアントへの

負荷・通信量・サーバへの負荷を比較する．また，AES + FHE の暗号化モードは ECB モードと CTR モードを実装し，暗号モードによる比較も行った．

2. 完全準同型暗号 (FHE)

2.1 特　　徴

FHE とは式 (1)，(2) のように暗号文同士の加法・乗法の演算が成立する性質をもつ暗号である．

完全準同型暗号

$$Encrypt(m) \oplus Encrypt(n) = Encrypt(m+n) \quad (1)$$
$$Encrypt(m) \otimes Encrypt(n) = Encrypt(m \times n) \quad (2)$$

FHE は公開鍵暗号方式の一つであり，秘密鍵で復号することなく暗号文同士の演算から平文同士の演算を暗号化した値を導くことができる．データ分析者が FHE の公開鍵と秘密鍵を生成し，スマートフォンを始めとする大量の IoT デバイスユーザとクラウドサービス側に公開鍵を送信し共有することで，デバイスユーザから集めた暗号化された大量のデータの統計分析をクラウドサービスで行うことが可能である．そして，データ分析者は暗号化された分析結果を秘密鍵で復号することで，個々のデバイスユーザのデータを得ずに分析結果のみを得ることができるようになることが期待される．

FHE の概念自体は，1970 年代後半に公開鍵暗号方式が考案された当初より Rivest らによって提唱されていたが [4]，2009 年に Gentry [5] が実現する手法を提案した．この実装は多項式環やイデアル格子を応用した暗号方式で，読解困難性を保つために，暗号文は平文を暗号化したものにランダムなノイズを加えた形式で表現される．しかしこの手法を用いた場合，1bit の平文を暗号化するとその暗号文は 1GB 程にもなってしまうなど，提案された当時は計算量の大きさから実用性がないとされていた．近年では効率の良い実装について多くの研究がなされて高速化や改良が進められており，実用化への期待が高まっている．

しかしながら，FHE には問題点もある．FHE の暗号文中の解読不可能性を高めるために加えられたランダムなノイズは，暗号文同士で計算を行うたびに増加する．特に乗算を行うことで大きく増加し，ノイズが閾値を超えると復号が不可能となる．bootstrapping と呼ばれるノイズをリセットする手法の導入することで演算回数の限定は解決することが出来るが，計算量が非常に大きくなる．

2.2 ライブラリ

FHE を実装しているライブラリには HElib [6]，SEAL [7]，PALISADE [8] などが挙げられる．HElib は IBM の研究者らによって初期に公開された，広く知られているライブラリの一つである．ノイズをリセットする手法の bootstrap をサポートしており，C++で実装されている．SEAL は Microsoft Research によって開発された C++で実装されたライブラリで，現時点では bootstrap はサポートされていない．PALISADE はニュージャージー工科大学によって開発されたライブラリで C++で実装されている．PALISADE もまた現在 bootstrap をサポートしていない．また，SEAL と PALISADE は外部ライブラリに依存していないが，HElib は GMP [9]，NTL [10] といった外部ライブラリに依存しているという特徴もある．本研究では 2019 年 5 月 21 日にコミットされたバージョンの HElib を実装に用いる．

3. AES

3.1 概　　要

AES(Advanced Encryption Standard) とは，アメリカ連邦政府標準の暗号方式として 2000 年に採用された共通鍵暗号方式の一つで，無線 LAN の暗号化になどに用いられる．また AES は高度な暗号化方式であり，現時点での解読方法は存在していないとされている．

AES は共通鍵暗号方式の一種であるブロック暗号で，鍵長は 128bit・192bit・256bit の 3 つが利用でき，128bit ずつ平文を区切って暗号化・復号を行う．

3.2 アルゴリズム

本研究では，128bit の鍵を使用しているため，鍵長が 128bit の場合の暗号化・復号アルゴリズムを示す．鍵長が 128bit の場合，変換のラウンド数は 10 回である．AES ではまず 128bit の鍵から (10 ラウンド+1) × 128bit の RoundKey を生成しておく．処理中の状態を state とし，以下のような 4 × 4 行列で表現する．初期値として，s_{ij} には平文を 8bit ずつ代入する．

$$\text{state} = \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$

暗号化する際にはラウンド数回，以下の処理を繰り返す．

(1) SubBytes
- state をガロア体 $GF(2^8)$ の逆数に変換．
- 行列変換を適用．

(2) ShiftRows
- 行ごとにを一定の規則で左シフト．

(3) MixColumns
- 列ごとに定数と state の AND 演算・XOR 演算．

(4) AddRoundKey
- RoundKey と state の XOR 演算．

復号する際にはラウンド数回，以下の処理を繰り返す．

(1) AddRoundKey
- RoundKey と state の XOR 演算．

(2) InvMixColumns
- 列ごとに定数と state の AND 演算・XOR 演算．

(3) InvShiftRows

- 行ごとにを一定の規則で右シフト.

(4) InvSubBytes

- state に行列変換を適用.
- ガロア体 $GF(2^8)$ の逆数に変換.

3.3 暗号化モード

ブロック暗号である AES にはブロック長 (128bit) よりも長い平文に対応するために暗号化モードを利用する．最も単純な仕組みの暗号化モードである ECB モードと CRYPTREC [11] で推奨され一般的に使用されている CTR モードについて示す.

3.3.1 ECB モード

図 1 は ECB モードの暗号化処理，図 2 は復号処理の概要である．図 1，2 の様に同じ平文ブロックを暗号化すると全て同じ暗号文になり，解読されやすくなってしまうという弱点がある.

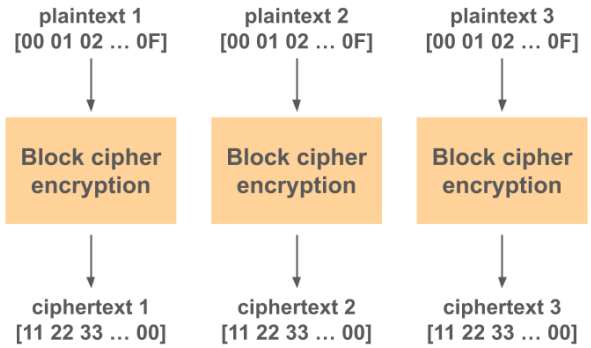

図 1 ECB モードによる暗号化

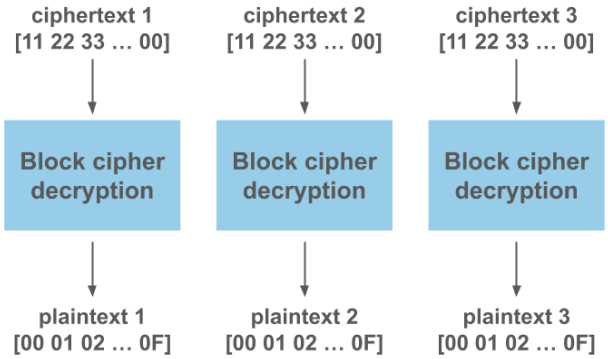

図 2 ECB モードによる復号

3.3.2 CTR モード

図 3 には CTR モードの暗号化処理を示す．ECB モードと異なるのはブロック暗号のアルゴリズムで暗号化するのはランダムに決められた Nonce と何番目のブロックかを示す Counter を組み合わせた値で，暗号化された Nonce，Counter と平文の XOR 演算を行うことで暗号文を生成する．ECB モードの様に同じ平文ブロックが存在しても同じ暗号文になることはない.

また，図 4 にあるように CTR モードの特徴として，復号する場合もブロック暗号の暗号化アルゴリズムを利用することが挙げられる.

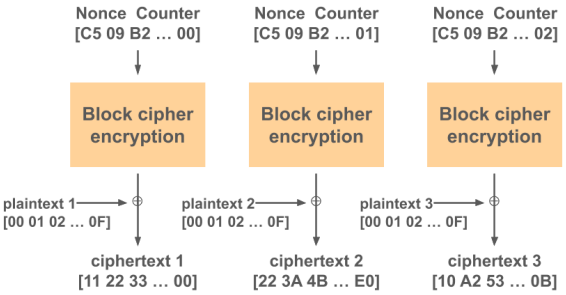

図 3 CTR モードによる暗号化

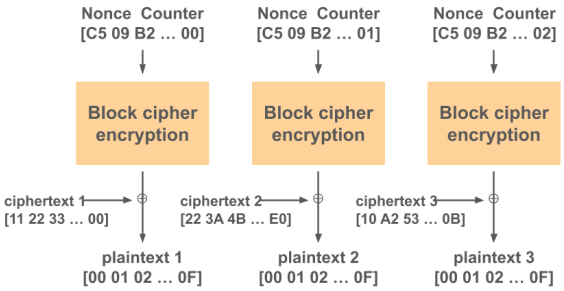

図 4 CTR モードによる復号

4. TRIVIUM

4.1 概　　要

TRIVIUM [12] とは，2008 年に eSTREAM という欧州における共通鍵暗号方式の一種，ストリーム暗号の評価プロジェクトで選定された暗号の一つである．TRIVIUM は構造が単純かつ高速であるため，eSTREAM に選定された 7 つの暗号の中でも特に高い評価を与えられた [13]．また，現時点では解読方法は存在していないとされている.

4.2 アルゴリズム

TRIVIUM では，80bit の鍵 (K)・80bit の初期化ベクトル (IV)・288bit の初期状態 (s) をパラメータとして使用し，以下のように K と IV で s の初期化を行う.

Key and IV setup

$(s_1, s_2, ..., s_{93}) \leftarrow (K_1, ..., K_{80}, 0, ..., 0)$
$(s_{94}, s_{95}, ..., s_{177}) \leftarrow (IV_1, ..., IV_{80}, 0, ..., 0)$
$(s_{178}, s_{279}, ..., s_{288}) \leftarrow (0, ..., 0, 1, 1, 1)$
$for\, i = 1\, to\, 4 \cdot 288\, do$
$t_1 \leftarrow s_{66} + s_{91} \cdot s_{92} + s_{93} + s_{171}$
$t_2 \leftarrow s_{162} + s_{175} \cdot s_{176} + s_{177} + s_{264}$
$t_3 \leftarrow s_{243} + s_{286} \cdot s_{287} + s_{288} + s_{69}$
$(s_1, s_2, ..., s_{93}) \leftarrow (t_3, s_1, ..., s_{92})$
$(s_{94}, s_{95}, ..., s_{177}) \leftarrow (t_1, s_{94}, ..., s_{176})$
$(s_{178}, s_{279}, ..., s_{288}) \leftarrow (t_2, s_{178}, ..., s_{287})$
$end\, for$

暗号化・復号の際は，初期化した s を利用して以下のように

生成した Key stream(z) と平文の XOR 演算を行う．

Key stream generation

$for\ i = 1\ to\ N\ do$

$t_1 \leftarrow s_{66} + s_{93}$

$t_2 \leftarrow s_{162} + s_{177}$

$t_3 \leftarrow s_{243} + s_{288}$

$z_i \leftarrow t_1 + t_2 + t_3$

$t_1 \leftarrow t_1 + s_{91} \cdot s_{92} + s_{171}$

$t_2 \leftarrow t_2 + s_{175} \cdot s_{176} + s_{264}$

$t_3 \leftarrow t_3 + s_{286} \cdot s_{287} + s_{69}$

$(s_1, s_2, ..., s_{93}) \leftarrow (t_3, s_1, ..., s_{92})$

$(s_{94}, s_{95}, ..., s_{177}) \leftarrow (t_1, s_{94}, ..., s_{176})$

$(s_{178}, s_{279}, ..., s_{288}) \leftarrow (t_2, s_{178}, ..., s_{287})$

$end\ for$

5. ハイブリッド暗号方式

ハイブリッド暗号方式とは共通鍵暗号方式と公開鍵暗号方式を組み合わせることで，それぞれの暗号方式の欠点を補い，長所を組み合わせた暗号方式である．図 5 にハイブリッド暗号方式の概要を示す．

まずクライアントは共通鍵，サーバは公開鍵と秘密鍵を生成し，公開鍵をサーバからクライアントに送信して共有する．次にクライアントは公開鍵で共通鍵を暗号化し，サーバに送信して共有する．そうすることで，サーバでは秘密鍵でこの鍵を復号し，共通鍵を安全に手に入れることができる．このように共通鍵を共有することによって，これ以降，高速にクライアントで暗号化，サーバで復号することができる．

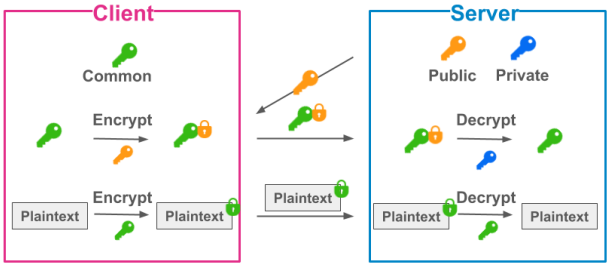

図 5　ハイブリッド暗号方式

6. 先行研究

Gentry ら (2015) は 8.1 節で述べる提案システムの (6) の処理にあたる，FHE による AES の復号処理の実装と評価を行った [2]．AES を評価に使用した理由としては，広く使われている暗号であり，並列処理や最適化しやすい構造であるためとしている．FHE のライブラリである HElib を用いて，2880B の平文を AES で暗号化し，FHE で暗号化された (10 ラウンド+1) × 128bit の AES の鍵を使い復号する設計になっている．実験に使用した Laptop の性能を表 1 に示す．　実装はシングルスレッドであるため，1 つのコアのみ使用している．2880B の AES 暗号文の復号に 18 分，16B あたり 6 秒を要した．

表 1　先行研究マシン性能

Device	OS	CPU	Number of Cores	Processor Speed	RAM
Lenovo X230	Ubuntu 14.04	Intel Core i5-3320M	2	2.6 GHz	4GB

7. 従来手法

提案手法の比較として，FHE のみを暗号化に使用する従来システムの概要を図 6 に示し，FHE only とする．

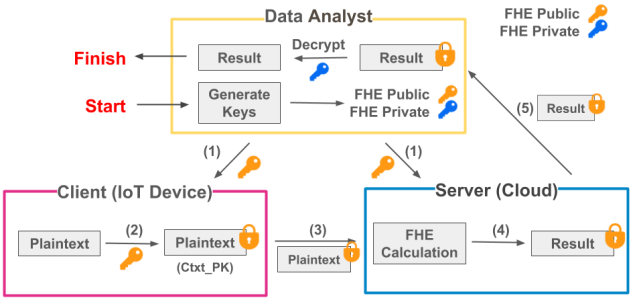

図 6　従来システム (FHE only)

(1) Data Analyst が FHE の公開鍵と秘密鍵を生成し，Client(IoT デバイスユーザ) と Server(クラウドサービス) に公開鍵を送信．

(2) Client は FHE の公開鍵で暗号化された暗号文 (Ctxt_PK) を生成．

(3) Ctxt_PK を Server に送信．

(4) Server は Ctxt_PK を使って分析．

(5) Server は分析結果を Data Analyst に送信．

従来システムの問題点として，Client における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．

8. 提案手法

8.1 概　　要

本研究では，図 7 の共有鍵暗号と公開鍵暗号方式の FHE を組み合わせた暗号化システムを提案する．図 7 中の Common Key は共通鍵暗号の AES・TRIVIUM の 2 通りで，それぞれの暗号を使った提案システムを AES+FHE，TRIVIUM+FHE とする．

(1) Data Analyst が FHE の公開鍵と秘密鍵を生成し，Client(IoT デバイスユーザ) と Server(クラウドサービス) に公開鍵を送信．

(2) Client は共通鍵 (CommonKey) を生成．

(3) Client は共通鍵で暗号化された暗号文 (Ctxt_Common) を生成．

(4) Client は FHE の公開鍵で暗号化された共通鍵 (CommonKey_PK) を生成．

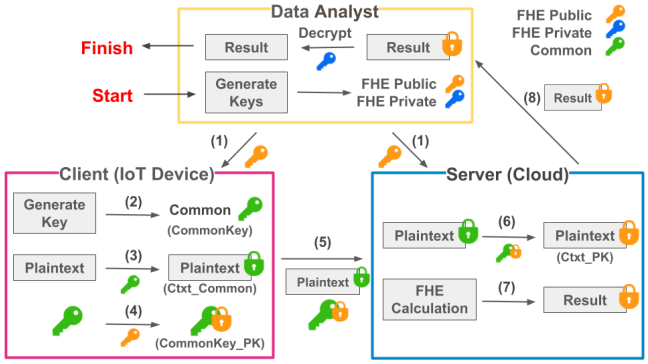

図 7　提案システム (AES+FHE，TRIVIUM+FHE)

(5)　Client は Ctxt_Common と CommonKey_PK を Server に送信.

(6)　Server は Ctxt_Common を CommonKey_PK で AES 暗号文の復号を行い，FHE の暗号文 (Ctxt_PK) を取得.

(7)　Server は Ctxt_PK を使って分析.

(8)　Server は分析結果を Data Analyst に送信.

平文が増加しても共通鍵で暗号化すれば良いため，従来手法よりも高速に暗号化できることが予想される.

提案手法では，5 節で説明したようなハイブリッド暗号方式と同様に共通鍵暗号方式と公開鍵暗号方式の FHE を組み合わせているが，ハイブリット暗号と異なるのは，サーバ (クラウド) は公開鍵と秘密鍵の作成も秘密鍵の所有もしないということである．サーバは FHE の性質を利用することで，FHE の公開鍵によって暗号化された共通鍵 (CommonKey_PK) を復号せずに共通鍵暗号によって暗号化された暗号文 (Ctxt_Common) を復号できる.

8.2　FHE による AES 暗号文の復号処理

AES では，16B ずつ区切った平文を 16B の鍵を使って暗号化し，16B ずつの暗号文を生成する．復号には，鍵と暗号文の XOR 演算や定数と暗号文の AND 演算を行う．FHE では暗号化したままで XOR 演算も AND 演算も行うことができるため，暗号化された AES の鍵と暗号文があれば，AES のみの復号を行い，FHE の暗号文にすることが可能である.

8.3　FHE による TRIVIUM 暗号文の復号処理

TRIVIUM では，80bit の鍵と 80bit の初期化ベクトルから平文と同じ長さの Key stream を生成して平文と XOR 演算を行い，平文と同じ長さの暗号文を生成する．復号には Key stream と暗号文の XOR 演算を行う．FHE で暗号化された鍵から Key stream を生成して暗号文と XOR 演算を行えば，FHE で暗号化したまま TRIVIUM のみの復号を行い，FHE の暗号文にすることが可能である.

9.　実　　験

9.1　実験環境

実験に使用したマシンの性能を表 2 に示す.

表 2　マシン性能

Device	OS	CPU	Number of Cores	Processor Speed	RAM
Raspberry Pi 3 Model B+	Raspbian 10.0	ARM Cortex-A53	4	1.4GHz	1GB
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

9.2　予備実験 1

FHE による 1B の暗号化時間を MacBook Pro，Google Pixel 3，Raspberry Pi で比較した結果を図 8 に示す．IoT デバイス

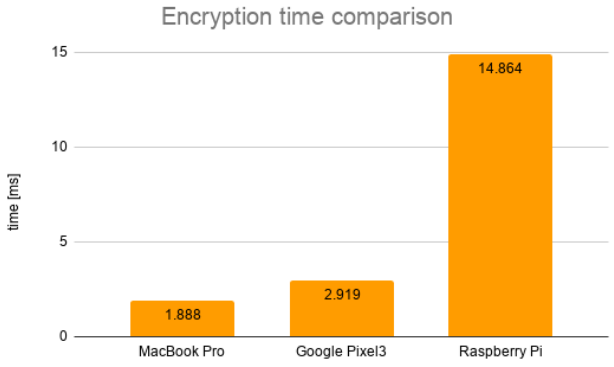

図 8　デバイスごとの FHE よる暗号化時間

である，Google Pixel 3 と Raspberry Pi に注目すると，処理速度は Google Pixel 3 が Raspberry Pi のおよそ 5 倍と格段に速いことがわかる.

また，IoT デバイスの中では高性能である Google Pixel 3 であっても，MacBook Pro に比べて約 1.5 倍低速である.

9.3　予備実験 2

提案手法で用いる共通鍵暗号の AES・TRIVIUM と公開鍵暗号方式の FHE で 1B の暗号化時間を比較した結果を図 9 に示す．実験には Google Pixel3 を使用した.

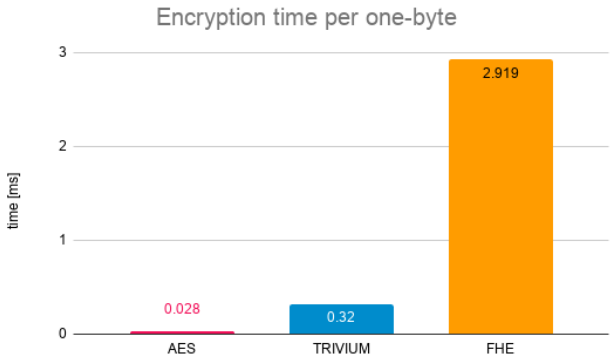

図 9　暗号方式ごとの暗号化時間

共通鍵暗号方式に比べ，公開鍵暗号方式の FHE が低速であ

ることは明らかである．

9.4 実験概要

Client は Google Pixel 3，Server は MacBook Pro を使用した．平文サイズを 16B，64B，128B，192B，256B，320B と変化させ，従来手法 (FHE only) と提案手法 (AES+FHE，TRIVIUM+FHE) で以下の 3 つの比較を行った．また，AES + FHE には 3.3 節で説明した ECB モードと CTR モードを実装した．

(1) Client における実行時間
(2) Client から Server に送信するファイルサイズ
(3) Server における共通鍵暗号の復号時間

9.5 実験結果

図 10 に (1)Client における実行時間 を示す．従来手法の実行時間には，FHE による平文の暗号化が含まれ，提案手法の実行時間には共通鍵の生成時間・鍵の暗号化・共通鍵暗号による平文の暗号化が含まれている．

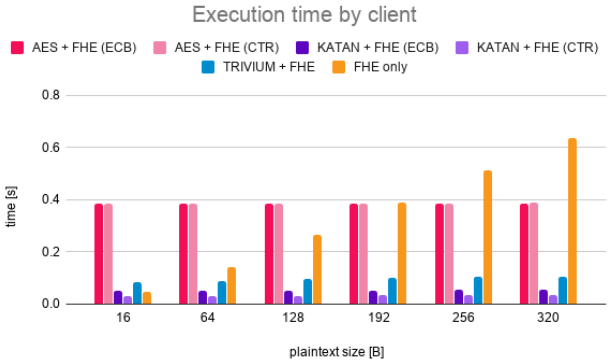

図 10 Client における実行時間

図 11 には (2)Client から Server に送信するファイルサイズを示す．従来手法のファイルサイズには FHE の暗号文のみが含まれ，提案手法のファイルサイズには，FHE で暗号化された共通鍵と共通鍵で暗号化された暗号文が含まれる．

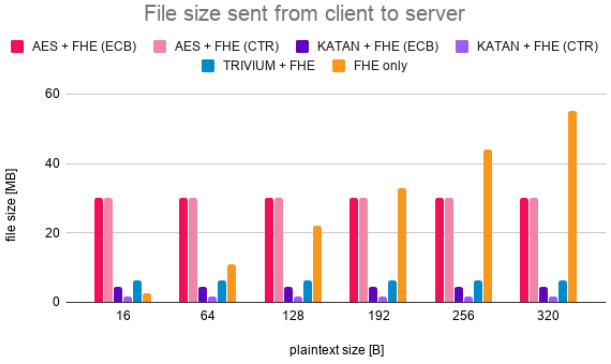

図 11 Client から Server に送信するファイルサイズ

図 12 に (3)Server における共通鍵暗号の復号時間を示す．FHE only では共通鍵暗号の復号処理は行わないため 0 秒である．

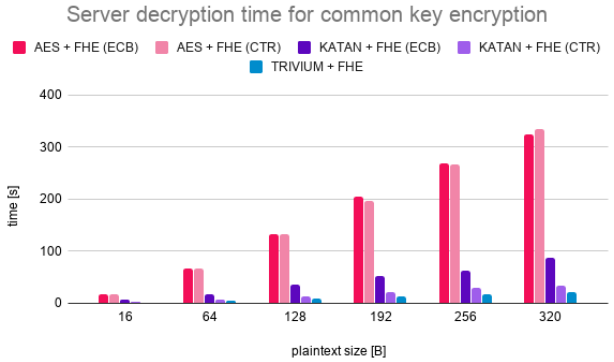

図 12 Server における共通鍵暗号の復号時間

9.6 実験結果まとめ

平文が長い場合 (plaintext size > 192) の従来手法と提案手法の比較を表 3 にまとめた．

表 3 平文が長い場合

	Client load	Traffic	Server load	Safety
FHE only	×	×	○	○
AES + FHE (ECB)	△	△	×	△
AES + FHE (CTR)	△	△	×	○
TRIVIUM + FHE	○	○	△	△

表 4 には平文が短い場合 (plaintext size < 64) の従来手法と提案手法の比較をまとめた．

表 4 平文が短い場合

	Client load	Traffic	Server load	Safety
FHE only	○	○	○	○
AES + FHE (ECB)	×	×	×	△
AES + FHE (CTR)	×	×	×	○
TRIVIUM + FHE	△	△	△	△

なお，表 3 と表 4 に示した Safety は，それぞれの手法で用いる暗号の鍵長から判断した簡易的なものである．AES + FHE については，3.3 節でもあったように ECB モードで暗号化した場合に同じ平文ブロックから同じ暗号文が生成されて強度が下がる．そのため，CTR モードの方が ECB モードよりも安全性が高いとした．

10. 考察

10.1 Client における実行時間 (Client への負荷)

図 10 より，平文サイズが増加するにつれて，従来手法 (FHE only) と提案手法 (AES+FHE，TRIVIUM+FHE) の差が顕著になっている．図 9 では 1B あたりの AES の暗号化時間より

TRIVIUM の暗号化時間の方が長いという結果にも関わらず，TRIVIUM+FHE が AES+FHE より高速な理由は，TRIVIUM+FHE で暗号化される共通鍵が AES+FHE で暗号化される共通鍵より短いためである．

一方で，平文サイズが小さい場合は，FHE only の方が高速であるという結果になった．提案手法で FHE によって暗号化される共通鍵の長さが，従来手法で FHE によって暗号化される平文より長い場合にそのような結果になる．

10.2 Client から Server に送信するファイルサイズ (通信量)

図 11 より，平文サイズが増加するにつれて，従来手法 (FHE only) と提案手法 (AES+FHE， TRIVIUM+FHE) の差が顕著になっていることが分かる．これは，FHE の暗号文サイズが共通鍵暗号方式の暗号文サイズよりもはるかに大きいことが影響している．TRIVIUM+FHE より AES+FHE のファイルサイズが小さいのは，TRIVIUM の共通鍵が AES の共通鍵より短いためである．

一方で，平文サイズが小さい場合は，FHE only の方が通信量が少ないという結果になった．提案手法で FHE によって暗号化される共通鍵の長さが，従来手法で FHE によって暗号化される平文より長い場合にそのような結果になる．

10.3 Server における共通鍵暗号の復号時間 (Server への負荷)

図 12 より，AES+FHE に比べて TRIVIUM+FHE の方がサーバへの負荷が少ない．これは，AES の復号処理よりも TRIVIUM の復号処理の方が加算・乗算の回数が少なくシンプルなためである．

10.4 暗号化モード

AES の ECB モードと CTR モードとでは 3.3 節にあるように，サーバにおける AES 暗号文の復号処理は異なるが，図 12 の AES + FHE (ECB) と AES + FHE(CTR) に注目すると，暗号化モードによるサーバへの負荷はあまり変わらない．

11. まとめと今後の課題

スマートフォンを始めとする IoT デバイスで取得したセンサデータを活用するために有用な完全準同型暗号による暗号化を高速化することを目的として，共通鍵暗号方式の AES･TRIVIUM と FHE を組み合わせた暗号 (AES+FHE，TRIVIUM+FHE) を実装した．その結果，平文が長い場合は従来手法よりも提案手法の方が Client における暗号化が高速で，通信量を削減することが可能になった．また，1B あたりの AES の暗号化時間より TRIVIUM の暗号化時間の方が長いが，FHE で暗号化する共通鍵の鍵長が TRIVIUM の方が短いため，AES+FHE より TRIVIUM+FHE のほうが高速で通信量を減らせることができた．提案手法で行う，サーバにおける共通鍵暗号の復号処理は AES+FHE より TRIVIUM+FHE の方がサーバへの負荷が少ないことが分かった．また，AES + FHE における暗号化モードを ECB モードと CTR モードで実装し，比較を行ったが暗号化モードによるクライアントへの負荷・通信量・サーバの負荷はあまり変わらなかった．

今後は AES・TRIVIUM 以外の共通鍵暗号を使った暗号の実装を検討している．

謝　　辞

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

文　　献

[1] Kristin Lauter, Michael Naehrig, Vinod Vaikuntanathan: Can homomorphic encryption be practical?, Proc. of the 3rd ACM workshop on CCSW ’11, pp. 113–124, 2011
[2] Craig Gentry, Shai Halevi, Nigel P. Smart: Homomorphic Evaluation of the AES Circuit, January 3, 2015
[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，第 15 回情報科学技術フォーラム，2016
[4] R. L. Rivest, L. Adleman, M. L. Dertouzos, et al.: On data banks and privacy homomorphisms, Foundations of secure computation 4.11 (1978), pp. 169–180.
[5] Craig Gentry, et al: Fully homomorphic encryption using ideal lattices. In STOC, Vol. 9, pp. 169–178, 2009
[6] HElib, https://github.com/homenc/HElib (2019/08 閲覧)
[7] Microsoft SEAL, https://github.com/Microsoft/SEAL (2019/08 閲覧)
[8] PALISADE, https://palisade-crypto.org/software-library/ (2020/02 閲覧)
[9] GMP, https://gmplib.org/ (2019/08 閲覧)
[10] NTL, https://www.shoup.net/ntl/ (2019/08 閲覧)
[11] CRYPTREC 暗号リスト (電子政府水推奨暗号リスト), https://www.cryptrec.go.jp/list.html (2020/02 閲覧)
[12] Christophe De Canni‘ere, Bart Preneel: Trivium Specifications, eSTREAM, ECRYPT Stream Cipher Project, 2006
[13] 森井 昌克，寺村 亮一: ストリーム暗号の現状と課題，電子情報通信学会 基礎･境界ソサイエティ Fundamentals Review Vol.2 No.3，2009