IoT通信における属性ベース暗号の活用に向けた検討

佐々木 怜名[1,a)]　石川 裕[2]　竹房 あつ子[2]　中田 秀基[3]　小口 正人[1]

概要：IoT デバイスの普及により大量のデータの収集が可能となる一方で，IoT デバイスやサーバ間での秘匿性の高いデータの保護が必要とされる．インターネット上での IoT 通信では，Broker を介した Publisher/Subscriber モデルが多く利用されており，データの保護のために TLS 通信を用いる．TLS 通信では，クライアントとサーバ間で相互認証および鍵共有を行い，データを通信路で暗号化する．しかし，多数の IoT デバイスで構成されるシステムは，悪意のある攻撃に対して脆弱であり，通信路における暗号化のみならず，データが Broker などの一時保存領域に格納される際にも暗号化が必要であり，Subscriber や Broker へのアクセス制御も考慮しなければならない．本研究では，特定の属性を持つ者が暗号化・復号できるアクセス制御機能を備えた属性ベース暗号を用いて， Subscriber や Broker に送信されるデータの暗号化とデータに対するアクセス制御を行う IoT アプリケーション向けの通信プロトコルを検討する．提案モデルの妥当性を検討するため，属性ベース暗号ライブラリ OpenABE の性能評価を行う．また，属性ベース暗号と TLS を用いたクライアント・サーバ間の通信性能の評価を行い，TLS ハンドシェイクオーバヘッドに加え，TLS と属性ベース暗号による二重の暗号化処理が通信性能に与える影響について調査を行う．

Consideration of Attribute-Based Encryption Utilization in IoT Communication

Reina Sasaki[1,a)]　Yutaka Ishikawa[2]　Atsuko Takefusa[2]　Hidemoto Nakada[3]　Masato Oguchi[1]

Abstract: While IoT devices enable the collection of large amounts of data, there is a need to protect highly confidential data between IoT devices and servers. In IoT communication on the Internet, the Publisher/Subscriber model via Broker is widely used, and TLS is employed to protect data during communication. However, systems containing many IoT devices are vulnerable to malicious attacks. Therefore, encryption is required not only in the communication channel but also when data is stored in temporary storage areas such as Brokers, and access control to Subscribers and Brokers must also be considered. This study investigates a communication protocol for IoT applications that provides access control for data sent to Subscribers and Brokers using Attribute-based encryption (ABE). This system includes an access control function that allows a person with a specific attribute to encrypt and decrypt data. To validate the proposed model, we evaluate the performance of the attribute-based cryptography library OpenABE. Additionally, we assess the performance of client-server communication using Attribute-based encryption and TLS, and investigate the overheads of the double encryption process using TLS and Attribute-based encryption on the communication performance and the TLS handshake.

1. はじめに

スマートフォンやIoT（Internet of Things）の普及と性能向上に伴い，大量のセンサデータの収集が可能となり，収集したセンサデータを利活用することが求められている．

[1] お茶の水女子大学
Ochanomizu University
[2] 国立情報学研究所
National Institute of Informatics
[3] 順天堂大学
Juntendo University
[a)] g1820516@is.ocha.ac.jp

IoT デバイスを活用したシステムは，多岐にわたる分野で利用されており，多数の IoT デバイスを含むシステムも登場している [1]．一般的な IoT アプリケーションでは，生成した膨大な量のデータを，インターネットに公開されているエッジサーバやクラウドに保存することが多い．プライバシに関わる情報やビジネス上重要な情報を扱う場合，通信路上や，一時保存領域にデータが格納される際にも，秘匿性の高いデータの保護が必要となる [2]．

インターネット上の IoT 通信では，データの一時保存領域である Broker を介した Publisher/Subscriber 通信モデル [3] が多く利用されており，TLS (Transport Layer Security) を用いて通信路におけるデータ保護を実現している．TLS では，TLS Handshake プロトコルによりクライアントとサーバ間で相互認証，鍵共有，使用するアルゴリズムやパラメタの合意を行う．さらに，TLS Record プロトコルにより，通信路におけるデータの暗号化と，データの完全性の確認を行うことで，インターネット上での安全なデータ送受信を実現している．しかし，デバイス数が多いシステムでは，TLS の認証による処理・通信量の増大や，証明書の管理の複雑性も課題となる．

また，Broker は Publisher と Subscriber の中継をしており，リプレイアタックなど悪意のある攻撃を受けるリスクが上昇するため，通信路でのデータの暗号化や，Broker などの一時保存領域に格納されるデータの暗号化だけでなく，Subscriber や Broker へのアクセス制御も必要である．

通信路上や Broker 上で保存されるデータの暗号化と，Subscriber や Broker へのアクセス制御を行うために，特定の属性を持つ者が暗号化・復号できるアクセス制御機能を備えた属性ベース暗号（ABE: Attribute-Based Encryption）[4] の IoT システムにおける活用が注目されている [5]．

本研究では，属性ベース暗号を用いて，Subscriber や Broker に送信されるデータにを暗号化するとともに，アクセス制御を行う IoT アプリケーション向けの通信プロトコルを検討する．TLS による相互認証と，属性ベース暗号によるきめ細やかなアクセス制御および通信路におけるデータの暗号化を行う，提案モデルの妥当性を検討するため，属性ベース暗号の処理にかかる時間について調査を行う．また，Publisher と Broker や，Broker と Subscriber 同士が互いに信頼できるか検証するために，TLS Handshake プロトコルによる相互認証を行うが，TLS Record プロトコルによりデータを送信すると，属性ベース暗号で暗号化されたデータを TLS により暗号化することとなる．そこで，IoT デバイスとサーバ間において，TLS ハンドシェイク後に，TLS による暗号化データではなく属性ベース暗号で暗号化したデータを送信する方式で，クライアント・サーバ間通信にかかる時間を測定し，TLS Handshake プロトコルによるオーバヘッドや，TLS と属性ベース暗号による二重の暗号化処理が通信性能に与える影響について調査する．

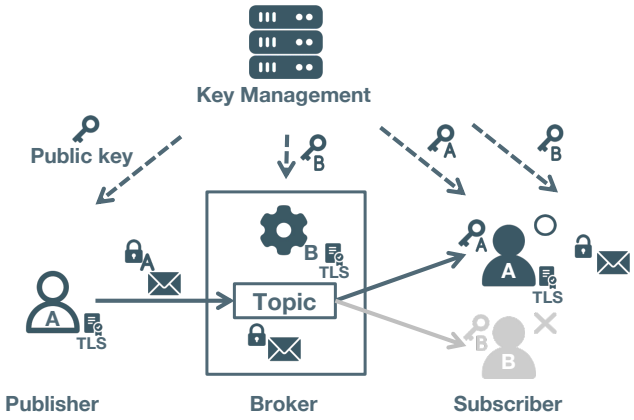


図 1: 提案する IoT 通信モデル

2. 属性ベース暗号を用いた IoT 通信プロトコルの提案

本研究では，TLS による相互認証と，属性ベース暗号によるきめ細やかなアクセス制御および通信路におけるデータの暗号化を行う，IoT のための通信プロトコルを提案する．**図 1** に提案する IoT 通信モデルを示す．Publisher, Broker, Subscriber は，事前に鍵生成サーバから属性ベース暗号の公開鍵や，各自が持つ属性やポリシに基づいた秘密鍵を受け取る．Publisher と Broker 間，Broker と Subscriber 間は TLS による相互認証を行い，互いに信頼できる相手にのみデータを送受信できるようにする．データ所有者である Publisher は，指定した属性やポリシを持つユーザのみが復号できるように属性ベース暗号で暗号化したデータを出版することで，復号できる属性やポリシを持たない Broker や Subscriber に対してデータを秘匿できる．

属性ベース暗号とは，ID ベース暗号 [6] を拡張した高機能暗号の一つであり，特定の属性や，属性の条件式 (ポリシ) を持つ者が暗号化・復号することが可能で，アクセス制御機能を備えている．ポリシとは，AND や OR などの論理演算を用いた属性の論理式であり，ポリシを木構造で表すことが多い．属性ベース暗号では，鍵生成サーバが，公開鍵と各ユーザが持つ属性やポリシに基づいた秘密鍵を配布する．データ所有者は配布された公開鍵に基づいてデータを暗号化し，ユーザは公開鍵と各自に配布された秘密鍵に基づいてデータを復号する．属性ベース暗号には，Ciphertext-Policy ABE (CP-ABE)[7] と Key-Policy ABE (KP-ABE)[8] の 2 つの方式があり，データの暗号化・復号の時に必要な属性情報がそれぞれ異なる．CP-ABE では，ユーザは各自の属性の集合に基づいた秘密鍵を鍵生成サーバから配布される．データ所有者は，ユーザが適切なポリシを保持していれば復号できるように，データを暗号化することができる．KP-ABE では，ユーザは各自が持つポリシに基づいた秘密鍵を鍵生成サーバに配布される．データ

表 1: 評価に使用した機器の構成

IoT デバイス	
CPU	ARM Cortex-A72 (4 cores, 1.8 GHz)
OS	Ubuntu 22.04.02 LTS
メモリ	4GiB
ライブラリ	OpenABE-1.0 relic-toolkit-0.5.0 gmp-6.3.0 openssl-1.1.1
サーバ 1	
CPU	Intel Core i9-9820X (20 cores, GHz)
OS	Ubuntu 22.04.4 LTS
メモリ	15.6GiB
ライブラリ	OpenABE-1.0 relic-toolkit-0.5.0 gmp-6.2.1 openssl-1.1.1
サーバ 2	
物理 CPU	Intel Xeon Platinum 8368 (38 cores, 2.4 GHz)
仮想 CPU コア数	16
OS	Ubuntu 20.04.5 LTS
メモリ	24.19GB
ライブラリ	OpenABE-1.0 relic-toolkit-0.4.0 gmp-6.2.0 openssl-1.1.1

表 2: A: IoT デバイスとサーバ 1 間，B:IoT デバイスとサーバ 2 間の Ping 結果

	RTT [ms]				packet loss
	min	avg	max	mdev	
A	1.087	5.037	16.630	2.160	0%
B	4.274	9.065	52.726	5.606	0%

所有者は，ユーザが適切な属性の集合を保持していれば復号できるように，データを暗号化することができる．これらにより，属性ベース暗号では，データ所有者が，各ユーザからのアクセス権を管理し，一つ一つのアクセス要求に対処することなく，ユーザのアクセス制御を実現できる．属性ベース暗号を用いた IoT システムに関する研究は数多く存在しており [5], [9], [10]，属性ベース暗号できめ細かいアクセス制御をすることで，第三者のクラウドや，Broker，物理的にアクセス可能なセンサなど，信頼できないストレージにデータを安全に保存できるため，多くの IoT アプリケーションに適している．

3. 評価

IoT システム内で，任意の暗号化方式により暗号化したデータを TLS 通信で送信する場合，任意の暗号化方式によるデータの暗号化と，TLS Record プロトコルによる通信路でのデータの暗号化の二重の暗号化処理をすることになる．本研究では，TLS と属性ベース暗号による二重の暗号化処理が通信性能に与える影響を調査し，提案する IoT 通信モデルの妥当性を検討する．3.2 節で，属性ベース暗号における暗号文のサイズや，鍵生成・暗号化・復号処理にかかる時間を測定し，属性ベース暗号ライブラリである OpenABE[11] の性能評価を行う．3.3 節で，TLS と属性ベース暗号を用いた通信をクライアント，サーバ間で行う．TCP 通信または TLS 通信で，平文データまたは属性ベース暗号で暗号化したデータをサーバに送信し，TLS Handshake プロトコルによる相互認証のオーバヘッドや，TLS Record プロトコルによる通信路でのデータ暗号化にかかる時間を測定する．

異なるホスト間で一方向のメッセージ通信の性能を測定するには，ホスト間で厳密に時刻を同期させる必要があるが，1msec 以下の精度で NTP で時刻同期をさせるのは非常に難しい．よって，受信ホストがメッセージを受け取ったあと，送信ホストに対してソケット通信で 1 byte データ (ack data) を送信するようにし，送信ホストでメッセージの送信から ack data を受け取るまでの時間を通信時間として計測する．

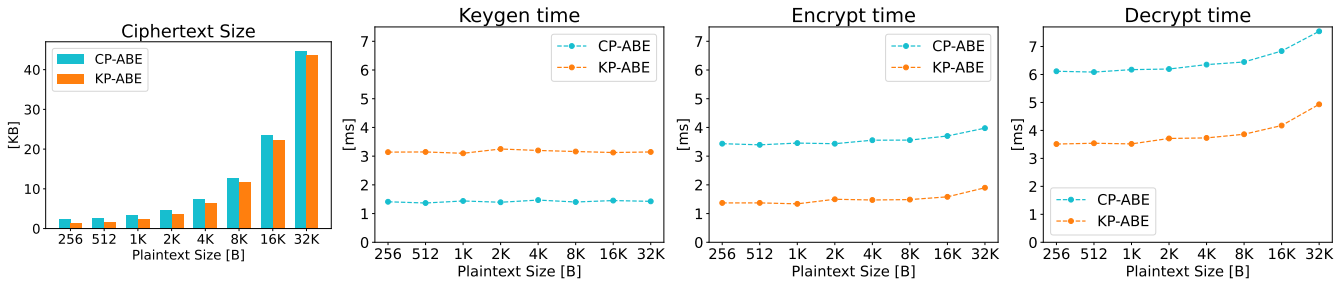
3.1 実験環境

実験で使用する IoT デバイス，サーバの詳細を**表 1** に示す．IoT デバイスとサーバ 1 は同一 LAN 上に存在している．サーバ 2 は，仮想マシンのデータ活用社会創成プラットフォーム mdx[12] を用いており，IoT デバイスとサーバ 2 はグローバルネットワークを介して通信する．IoT デバイスとサーバ 1 間，IoT デバイスとサーバ 2 間で，ping を用いて RTT を測定した．100 回測定した結果を**表 2** に示す．同一 LAN 上で計測した IoT デバイスとサーバ 1 間よりも，グローバルネットワークを介した IoT デバイスとサーバ 2 間の方が，RTT のばらつきが大きく，平均の値について，IoT デバイスとサーバ 1 間では 5.037 ms，IoT デバイスとサーバ 2 間では 9.065 ms であった．

3.2 OpenABE の性能評価

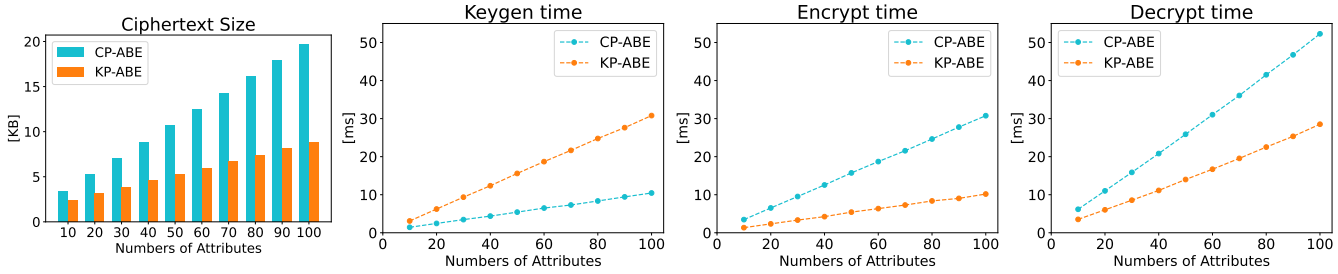
属性ベース暗号ライブラリ OpenABE を用いた時の各処理時間を計測する．OpenABE は，CP-ABE や KP-ABE などの属性ベース暗号化方式を用いることができ，認証済み共通鍵暗号化，公開鍵暗号化，デジタル署名，X.509 証明書の取り扱い，鍵導出関数，擬似ランダム生成器など，他の暗号機能も提供する C/C++ライブラリで，ペアリングライブラリには，relic-toolkit[13] を用いている．

まず，サーバ 1 において，CP-ABE と KP-ABE のそれぞれの方式において，平文サイズと，属性リストやポリシに含まれる属性数を変化させて，暗号文サイズ，ユーザの秘密鍵の生成時間，暗号化時間，復号時間を計測する．本実



(a) (b) (c) (d)

図 2: 平文サイズを変化させた時の暗号文サイズ，鍵生成時間，暗号化時間，復号時間 (属性数 10)



(a) (b) (c) (d)

図 3: 属性数を変化させた時の暗号文サイズ，鍵生成時間，暗号化時間，復号時間 （平文サイズ 1 KiB）

験でのポリシの設定は，例えば属性数が 3 の時，属性リストは”(Attr0, Attr1, Attr2)”，ポリシは”Attr0 AND Attr1 AND Attr2”と表すように，属性を全て AND で直列に連結することとする．属性数を 10 に固定し，平文サイズを 256 B から 32 KiB まで変化させ，各メッセージサイズにつき 100 セットの測定と，平文サイズを 1 KiB に固定し，属性数を 10 から 100 まで変化させ，各属性数につき 100 セットの測定を行う．次に，IoT デバイス上でもサーバ 1 と同様の測定を行い，CP-ABE を用いて，属性数を 10 に固定し平文サイズが 1 KiB，4 KiB，32 KiB のときと，平文サイズを 1 KiB に固定し属性数が 10，50，100 のときの，IoT デバイスとサーバ 1 それぞれにおける暗号化と復号の処理にかかる時間を比較する．

サーバ 1 で行う OpenABE の性能評価について，属性数を 10 に固定し，平文サイズを 256 B から 32 KiB まで変化した時の暗号文サイズと鍵生成，暗号化，復号にかかる時間の結果を**図 2** に示す．また，平文サイズを 1 KiB に固定し，属性数を 10 から 100 まで変化した時の暗号文サイズと鍵生成，暗号化，復号にかかる時間の結果を**図 3** に示す．

暗号文サイズについて，**図 2a** より，属性数を 10 に固定し平文サイズを変化させたときの CP-ABE と KP-ABE の差は小さいことがわかる．また，**図 3a** より，平文サイズを 1 KiB に固定し属性数を変化させた時，属性数が増えるほど，平文と暗号文のサイズの大きさの差が大きい．これは，暗号文生成時に，KP-ABE では属性リストを，CP-ABE では木構造で表されたポリシを組み込んでいるため，属性数が多いほど暗号文サイズが大きくなるためである [14]．

図 2b，**図 3b** より，鍵生成にかかる時間のみ KP-ABE の方が大きい．KP-ABE では，木構造で表されるポリシを組み込んだ秘密鍵を生成するためである [14]．図 2b, **図 2c**, **図 2d** より，属性数を 10 に固定し，平文サイズを変化させたとき，鍵生成時間，暗号化時間，復号時間は，大まかな傾向として横ばいである．また，図 3b, **図 3c**, **図 3d** より，平文サイズを 1 KiB に固定し，属性数を変化させた時，鍵生成時間，暗号化時間，復号時間は属性数に比例する．また，属性ベース暗号では，暗号化よりも復号に時間がかかり，その差は 2 倍近くになった．

次に，IoT デバイス上で，CP-ABE を用いてサーバ 1 と同様の測定を行い，IoT デバイスとサーバ 1 間で鍵生成，暗号化，復号の処理にかかる時間を比較した結果を，**図 4**，**図 5** に示す．サーバ 1 では Intel アーキテクチャ，IoT デバイスでは Arm アーキテクチャでコンパイルされた OpenABE ライブラリを使用しており，IoT デバイス上での各処理にかかる時間は，サーバ 1 よりもおよそ 10 倍大きい．また，**図 5a**，**図 5b**，**図 5c** より，属性数が 100 のとき，鍵生成に 93.109 ms，暗号化に 278.411 ms，復号に 490.644 ms の処理時間がかかる．IoT システム内のデバイス数が多い時や複雑なアクセス制御を行う時など，属性数が多いアクセスポリシを組み込んで暗号文を生成する場合，暗号化や復号には数百 ms の時間がかかることがわかった．

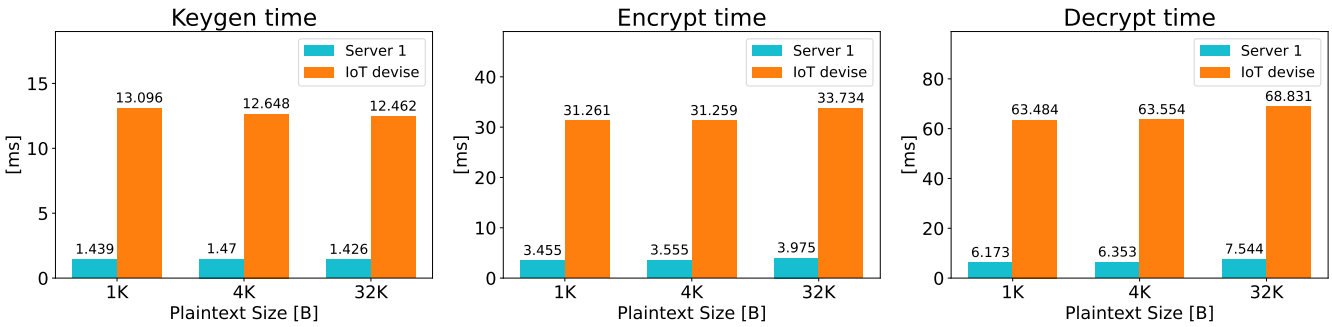


図 4: サーバ 1 と IoT デバイスの比較： 平文サイズを変化させた時の鍵生成時間，暗号化時間，復号時間 （属性数: 10）

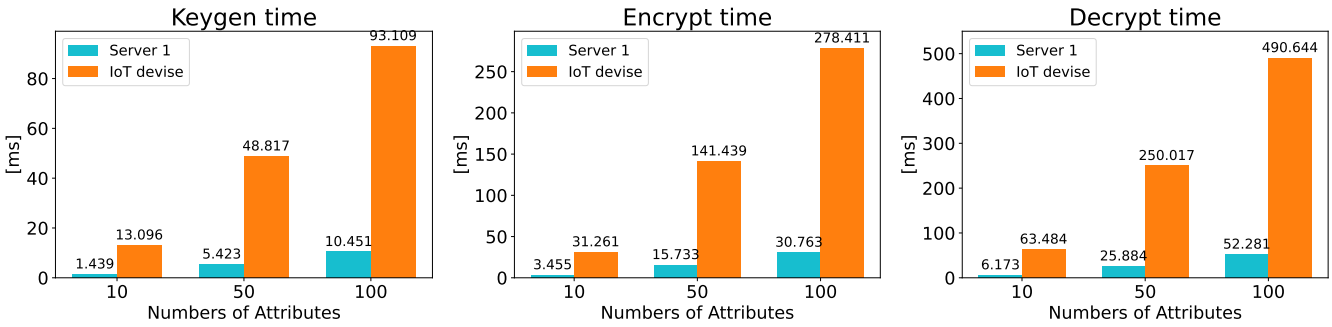


図 5: サーバ 1 と IoT デバイスの比較： 属性数を変化させた時の鍵生成時間，暗号化時間，復号時間 （平文サイズ 1 KiB）

3.3 TLS と ABE を用いたクライアント・サーバ間の通信性能評価

図 6 に以下に示す実験のシステム構成を示す．

(A) IoT デバイス内のプロセス間通信
(B) 同一 LAN 内での IoT デバイスとサーバ 1 間の通信
(C) グローバルネットワークを介した IoT デバイスとサーバ 2 間の通信
(D) グローバルネットワークを介したサーバ 1 とサーバ 2 間の通信

この 4 つの環境で，以下の (1) から (6) の処理を行う．全ての処理で，クライアントから 1 KiB のデータをサーバに送信し，認証，通信，暗号化にかかる時間をそれぞれ計測する．

(1) 平文を TCP 通信で送信
(2) 平文を TLS 通信で送信
(3) TLS の認証を行い，TLS 暗号化をせずに平文を TCP 通信で送信
(4) クライアントで ABE 暗号化を行い，暗号文を TCP 通信で送信
(5) クライアントで ABE 暗号化を行い，暗号文を TLS 通信で送信
(6) クライアントで ABE 暗号化と TLS の認証を行い，TLS 暗号化をせずに暗号文を TCP 通信で送信

図 7 に，各実験構成における，TLS と ABE を用いたクライアント・サーバ通信にかかる時間を示す．TCP 通信や TLS 通信にかかるセットアップの時間を setup とする．setup には，TCP 通信のコネクションにかかる時間や，TLS Handshake プロトコルによる認証にかかる時間が含まれている．transport には，クライアントが TCP 通信で send 関数でデータを送信し，サーバが recv 関数でデータを受信・ack data を送信し，クライアントが ack data を受信するまでの時間や，クライアントが TLS の write 関数でデータを送信し，サーバが read 関数でデータを受信・ack data を送信し，クラインとが ack data を受信するまでの時間が含まれている．(2)，(5) の TLS 通信の transport には，データの送受信にかかる時間の他に，TLS によるデータの暗号化と完全性の確認をする時間が含まれている．(4)，(5)，(6) の場合のみ，CP-ABE で平文 1 KiB を暗号化し，暗号化にかかる時間を encrypt とする．平文 1 KiB を属性ベース暗号で暗号化したとき，暗号文サイズは約 3.4 KB となる．(1)，(3) で送信するデータは 1 KiB の平文であり，(2) では，TLS Record プロトコルにより平文を暗号化してデータを送信する．(4)，(6) で送信するデータは約 3.4 KB の属性ベース暗号の暗号文であり，(5) では，TLS Record プロトコルにより属性ベース暗号の暗号文をさらに暗号化してデータを送信する．setup，transport，encrypt の積算時間は，クライアントがサーバにデータを送信するまでにかかる時間である．

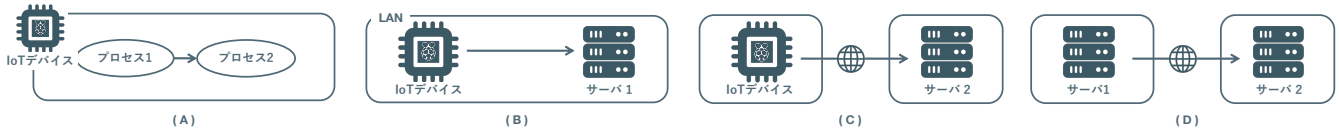
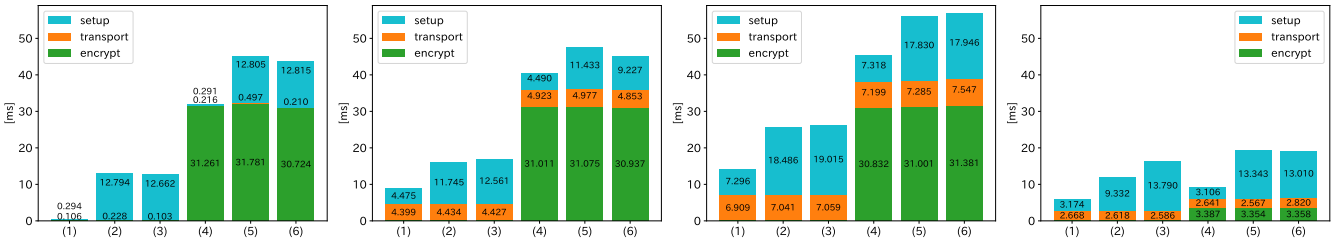


図 6: 3.2 節における実験機器の構成



(a) (A) IoT デバイス内のプロセス間通信 **(b)** (B) 同一 LAN 内での IoT デバイスとサーバ 1 間の通信 **(c)** (C) WAN を介した IoT デバイスとサーバ 2 間の通信 **(d)** (D) WAN を介したサーバ 1 とサーバ 2 間の通信

図 7: TLS と ABE を用いたクライアント・サーバ通信にかかる時間: (1) 平文を TCP 通信で送信，(2) 平文を TLS 通信で送信，(3)TLS の認証を行い平文を TCP 通信で送信，(4)ABE 暗号化を行い，暗号文を TCP 通信で送信，(5)ABE 暗号化を行い暗号文を TLS 通信で送信，(6)ABE 暗号化と TLS の認証を行い暗号文を TCP 通信で送信

(A)，(B)，(C)，(D) のいずれの場合も，図 7 より，(1) や (4) の setup の時間よりも (2)，(3)，(5)，(6) の setup の時間がかかるのは，TLS 認証をする時間が含むためである．この遅延は，ネットワーク遅延によって変化するものであり，表 2 の ping 結果から，本実験の遅延差は妥当であることがわかる．(2) と (5) の transport には，TLS の暗号化にかかる時間が含まれているが，**図 7b**，**図 7c**，**図 7d** より，リモートマシン間でクライアント・サーバ通信を行う (B)，(C)，(D) の場合，(2) と (3) 間や，(5) と (6) 間の transport の差は小さい．属性ベース暗号による暗号化処理により送信メッセージのサイズが平文より大きくなっても，TLS の暗号化時間がより大きくなることがないため，TLS と属性ベース暗号の二重の暗号化による通信性能への影響は小さいことがわかった．

図 7a，図 7b，図 7c より，ローカル環境で通信を行う (A)，同一 LAN 上でデータを送信する (B)，グローバルネットワークでデータを送信する (C) の順に，レイテンシの影響により，setup と transport を合わせた時間が大きくなる．広域通信では，ネットワーク遅延が大きくなるほど，setup と transport の値は大きくなり，encrypt に対する割合が大きくなることが予想できる．また，図 7d の (5)，(6) より，サーバ 1 では encrypt の時間よりも，TLS 通信にかかる setup と transport を合わせた時間の方が大きい．サーバ上では，データ送信にかかる時間に対して，属性ベース暗号による暗号化時間の影響が少ないことがわかった．

レイテンシが大きいほど TLS 認証や通信に時間がかかるため，全体のデータ送信に占める属性ベース暗号の暗号化処理の時間は小さくなることが想定できる．よって，属性数が少ない場合や，広域通信を行う IoT システムにおいて，IoT デバイス上で属性ベース暗号による暗号化処理を行うことは現実的であることが確認できた．

4. 関連研究

IoT システムでは，IoT デバイスとサーバ間の双方向の暗号通信を行うため，互いに信用できるか検証するための相互認証や鍵共有が必要である．IoT システムでの相互認証や鍵共有には，TLS を用いることが一般的であるが，システム内のデバイス数が多くなるほど証明書の管理が複雑になり，処理や通信量の増大が課題となる．この課題に対して，属性ベース認証付鍵交換方式 [15] を用いたグループ鍵共有方式が提案されている [16]．属性ベース認証付鍵交換とは，ある特定のポリシに含まれる属性を持つユーザのグループ内で，アクセスポリシを満たす属性を持つユーザのみがセッションキーを計算できるようにすることで，グループ内で共通鍵の交換を可能にする手法である．これにより，デバイス数が多い IoT システムでも，TLS の証明書の検証や送受信を省略することができ，特定のポリシを満たす複数の機器間で鍵共有が可能となる．本研究では，TLS を用いて相互認証を行い，鍵共有せずにクライアントからサーバへ送信するデータを属性ベース暗号で暗号化する通信モデルを検討しており，TLS による相互認証の処理時間や IoT デバイス上での属性ベース暗号によるデータの暗号化・復号処理の負荷に関する調査を行う．

属性ベース暗号を用いた機密性の高いデータ保護を IoT に実装する研究の一つとして [10] が挙げられる．属性ベース暗号による暗号化処理を，IoT デバイスではなくフォグノードで行い，アクセス制御が可能となるデータをクラウドにアップロードするモデルを検討している．また，データ所有者がクラウドにアップロードされた暗号文を更新

する時に，クラウドがデータ所有者の認証をする必要がある．そこで，属性ベース署名 (Attribute-Based Signature: ABS)[17] を用いて，データ更新時にデータ所有者が署名をし，許可されたユーザであればクラウド上のデータの修正を可能にしている．暗号化・復号，署名の計算の大部分をフォグノードで行うことで，IoT デバイス上の処理負荷を抑えている．しかし，IoT デバイスの性能向上に伴い，これらのデバイスが従来は高負荷とされていた暗号化技術を自律的に処理できる可能性が高まっている．よって，属性ベース暗号のような計算リソースを多く必要とする処理を，フォグノードやエッジサーバなどにアウトソースせずに，IoT デバイスがその処理を担う可能性を踏まえ，本研究では，IoT デバイス上での属性ベース暗号の実装が現実的かつ有効であるか検討する．

Topic ベースの Publisher/Subscriber 通信モデルをとる IoT システムでは，Broker が Topic 名や Publisher から受信したメッセージを保持しており，暗号文置換攻撃などの攻撃対象になりやすい．Broker で保存データを暗号化するだけでなく，前方秘匿性をもち，悪意のある Subscriber を判別することが必要である．論文 [18] では，トピックベースの Publisher/Subciber 通信を行う IoT システムのセキュリティを向上させるため，属性ベース暗号と属性ベースアクセス制御を用いたフレームワークを検討している．ペイロードを暗号化する共通鍵を CP-ABE 方式で暗号化し，複数の Publisher と Subscriber において，データに対するアクセス制御を行う．また，Broker からトピックデータを秘匿するために，ユーザ失効を伴う属性ベースのキーワード検索手法 (Attribute-Based Keyword Search-User Revocation: ABKS-UR)[19] を改良し，Topic を暗号化する．さらに，ABS を用いて，Publisher が出版するデータに自身の属性に基づいた署名をして認証する．属性ベース暗号や ABKS-UR で用いるマスタ公開鍵やマスタ秘密鍵を更新し，正当なユーザは新たに各自の属性に基づいた秘密鍵を修正することで，リアルタイムに失効ユーザをシステムから排除することができる．IoT デバイス上の Publisher と，仮想マシン上の Subsriber や MQTT Broker により提案フレームワークを実装し，セットアップにかかる時間，出版にかかる時間，属性ベース暗号によって生成されたデータサイズを測定している．

5. まとめと今後の課題

特定の属性を持つ者が暗号化・復号できるアクセス制御機能を備えた属性ベース暗号を用いて， Subscriber や Broker に送信されるデータに対するアクセス制御を行う IoT アプリケーション向けの通信モデルの検討をした．属性ベース暗号ライブラリ OpenABE の性能評価と，TLS と属性ベース暗号を用いたクライアント・サーバ間の通信性能の評価を行った．TLS と属性ベース暗号の二重の暗号化による通信時間への影響は小さいことがわかった．同一 LAN 上で IoT デバイスとサーバ 1 間でデータを送る場合と比べて，グローバルネットワークを介した IoT デバイスとサーバ 2 間では，レイテンシの影響により，TLS の認証や TLS 通信にかかる．レイテンシが 9 ms の IoT デバイスとサーバ 2 間では，平文 1KiB を TLS 認証した時のデータ送信時間は約 30 ms であるのに対し，属性ベース暗号の暗号文を TLS 認証したときは約 60 ms で，約 2 倍になることが確認できた．また，IoT デバイスとサーバ間のレイテンシが大きいときや，IoT デバイスがサーバに近い性能のマシンであれば，データ送信における属性ベース暗号化の占める割合は小さくなるため，IoT デバイス上で属性ベース暗号による暗号化処理を行うことは現実的であることがわかった．本実験では，サーバ 1 と 2 に Intel アーキテクチャ，IoT デバイスに Arm アーキテクチャでコンパイルされた OpenABE ライブラリを使用しており，OpenABE の Arm 実装の最適化の余地が存在する．

今後の課題は，IoT デバイス上における属性ベース暗号にかかる処理時間の削減に向けて，OpenABE の Arm 実装の最適化に向けた検討が必要である．また，暗号化・復号処理の負荷や通信コスト，セキュリティ強化の観点から，属性ベース暗号により暗号化した共通鍵を用いる場合のシステム全体のオーバーヘッドや安全性と比較し，メッセージそのものを属性ベース暗号で暗号化した場合の有効性と必要性について調査する．さらに，Publisher/Subscriber 通信での属性ベースアクセス制御と属性ベース暗号を用いたシステムモデルの検討を行う．

謝辞 本研究の一部は，JST CREST JPMJCR22M2 の支援を受けたものである．

参考文献

[1] Hu Xiong, Zheng Qu, Xin Huang, and Kuo-Hui Yeh. Revocable and unbounded attribute-based encryption scheme with adaptive security for integrating digital twins in internet of things. *IEEE Journal on Selected Areas in Communications*, Vol. 41, No. 10, pp. 3306–3317, 2023.

[2] Atsuko Takefusa, Jingtao Sun, Ikki Fujiwara, Hiroshi Yoshida, Kento Aida, and Calton Pu. SINETStream: Enabling research iot applications with portability, security and performance requirements. In *Proc. COMPSAC 2021*, pp. 482–492, 2021.

[3] Patrick Th. Eugster, Pascal A. Felber, Rachid Guerraoui, and Anne-Marie Kermarrec. The many faces of publish/subscribe. *ACM Comput. Surv.*, Vol. 35, No. 2, p. 114–131, 2003.

[4] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24*, pp. 457–473, 2005.

[5] Marco Rasori, Michele La Manna, Pericle Perazzo, and Gianluca Dini. A survey on attribute-based encryption

schemes suitable for the internet of things. *IEEE Internet of Things Journal*, Vol. 9, No. 11, pp. 8269–8290, 2022.

[6] Adi Shamir. Identity-based cryptosystems and signature schemes. In George Robert Blakley and David Chaum, editors, *Advances in Cryptology*, pp. 47–53, Berlin, Heidelberg, 1985.

[7] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, 2007.

[8] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, p. 89–98, 2006.

[9] Dilxat Ghopur. Attribute-based searchable encryption with forward security for cloud-assisted iot. *IEEE Access*, Vol. 12, pp. 90840–90852, 2024.

[10] Qinlong Huang, Yixian Yang, and Licheng Wang. Secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things. *IEEE Access*, Vol. 5, pp. 12941–12950, 2017.

[11] OpenABE. `https://github.com/zeutro/openabe`.

[12] Toyotaro Suzumura, et al. mdx: A cloud platform for supporting data science and cross-disciplinary research collaborations. In *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pp. 1–7, 2022.

[13] D. F. Aranha and C. P. L. Gouvêa. RELIC is an Efficient LIbrary for Cryptography. `https://github.com/relic-toolkit/relic`.

[14] National Institute of Standards and Technology (NIST). Overview and Considerations of Access Control Based on Attribute Encryption. Technical Report NIST IR 8450, National Institute of Standards and Technology, September 2023. Withdrawn on December 20, 2023. Superseded by NIST IR 8450-upd1.

[15] M Choudary Gorantla, Colin Boyd, and Juan Manuel González Nieto. Attribute-based authenticated key exchange. In *Australasian Conference on Information Security and Privacy*, pp. 300–317, 2010.

[16] 椿雄介, 中西透. IoT 向け属性ベースグループ鍵共有プロトコルの実装. 研究報告コンピュータセキュリティ（CSEC）, No. 13, 2018.

[17] Jin Li, Man Ho Au, Willy Susilo, Dongqing Xie, and Kui Ren. Attribute-based signature and its applications. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '10, p. 60–69. Association for Computing Machinery, 2010.

[18] Olivier Blazy, Emmanuel Conchon, Mathieu Klingler, and Damien Sauveron. An IoT Attribute-Based Security Framework for Topic-Based Publish/Subscribe Systems. *IEEE Access*, Vol. 9, pp. 19066–19077, 2021.

[19] Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou, and Hui Li. Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 226–234, 2014.