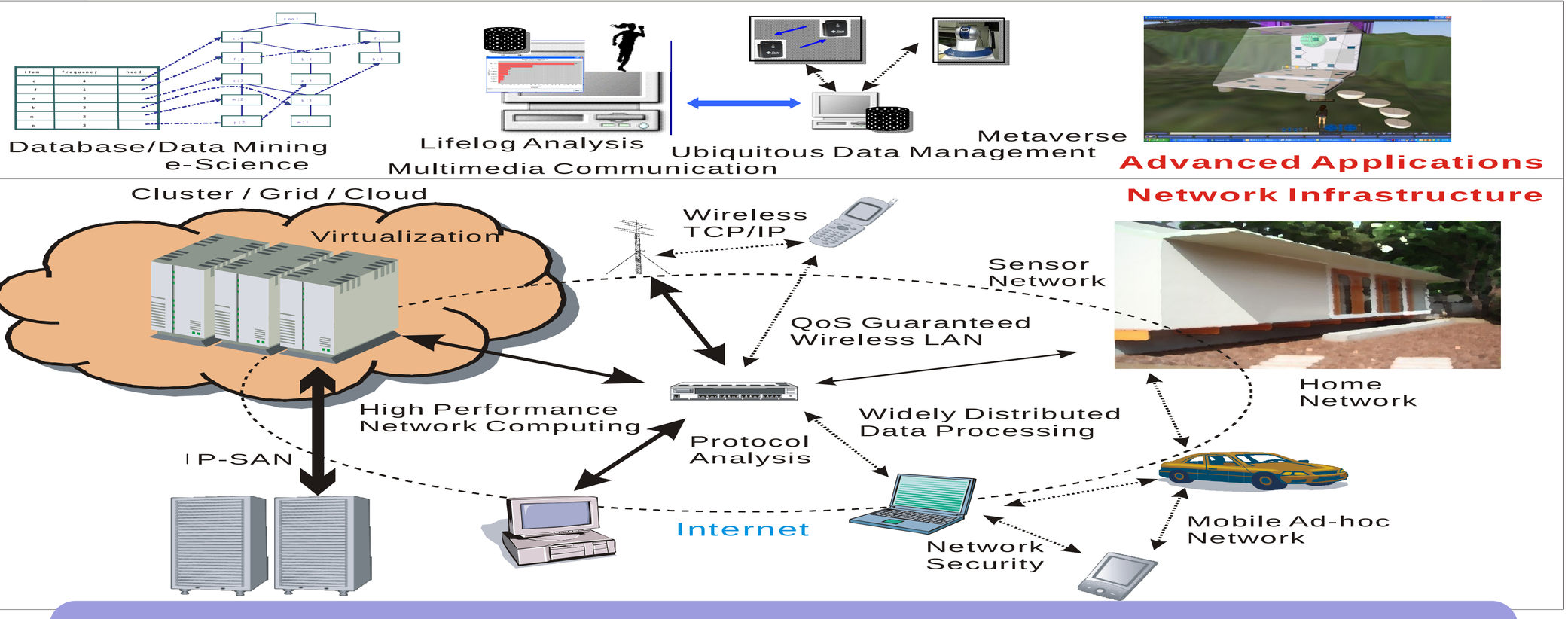
小口研究室　研究紹介　(2024年度)
(お茶の水女子大学理学部情報科学科)

次世代ネットワークコンピューティング基盤と先進的アプリケーション



◆研究テーマ：ネットワークコンピューティング・ミドルウェア
- ●多種多様な通信・計算機器が複雑に結びついて情報化社会のシステムを形成
- ●次世代ネットワークコンピューティング基盤に焦点を当て、先進的アプリケーションそれを支えるミドルウェアを研究

シングルボードコンピュータを用いたトーラス上の完全準同型暗号におけるクライアント側演算の効率化
（研究担当:松本　茉倫）

背景: FHEによるSBCのデータ活用
- 完全準同型暗号 (以下 FHE) はシングルボードコンピュータ（以下 SBC）で収集した機微な情報を含むデータをクラウドサーバ上で保護しながら統計処理や機械学習を実行可能な技術.
- TFHE スキームは準同型NAND 演算が可能で，最小値・最大値・比較演算等のどんな演算も可能.→ 暗号化DBクエリ実行・機械学習に適している.
- TFHEでは LWE 暗号化が必要なので，RLWE 暗号化よりも暗号化の効率は悪く暗号文サイズが大きい.→ SBCの計算負荷・通信コスト大

FHEで扱う(Ring) Learning With Error暗号文
- **LWE: 1bitずつ暗号化.** 秘密鍵をベクトル$\vec{s} = (s_0, \dots, s_{n-1}) \in \{0,1\}^n$，$a_i \in \mathbb{Z}_q$は一様分布，$e \in \mathbb{Z}_q$は正規分布に従う乱数として，

$$(a_0, \dots, a_{n-1}, b) \in LWE_{\vec{s},\sigma}(\Delta m) \subseteq \mathbb{Z}_q^{n+1}, \text{where } \boldsymbol{b} = \sum_{i=0}^{n-1} \boldsymbol{a_i \cdot s_i} + \boldsymbol{\Delta m} + \boldsymbol{e}$$

- **RLWE: Nbitまとめて暗号化.** 秘密鍵を係数が{0, 1}の多項式 $S \in \mathcal{R}$,は$A \in \mathcal{R}_q$一様分布に従う乱数，$E \in \mathbb{Z}_q$ は正規分布に従う乱数として，

$$(A, B) \in RLWE_{S,\sigma}(\Delta M) \subseteq \mathcal{R}_q^2, \text{where } B = A \cdot S + \Delta M + E \in \mathcal{R}_q$$

提案: TFHE-SBCライブラリ
- 計算資源の限られたSBC 向けのTFHEライブラリ **TFHE-SBC を提案**.
- Raspberry Piの中で小型・低省電力・低価格なRaspberry Pi Zero 2Wを対象.
- 代表的なTFHEのライブラリのTFHEppをベースとして高速化.
- SBCに適した乱数生成や多項式乗算を検討.

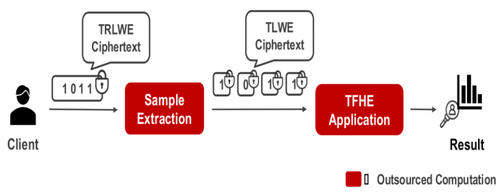
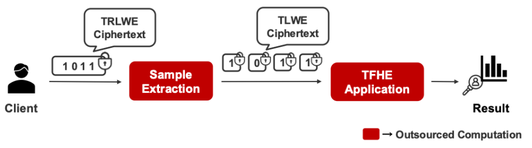


図1: TFHE-SBCによるTFHE暗号文の収集

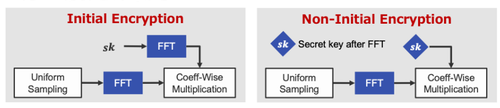
TFHE-SBCにおける最適化
最適化１：クライアントでのRLWE暗号化の利用
- クライアントがRLWE暗号化し，サーバサイドでRLWE→LWEへスイッチすることで高速化・暗号文を小さくする



最適化２：ハードウェア依存でない擬似乱数生成
- AESアクセラレータなどを必要としない擬似乱数生成のソフトウェア実装

最適化３：正規乱数生成アルゴリズムの改善
- TFHEppライブラリではPolar法による正規乱数生成を採用→ Polar法は内部の一様乱数生成が平均1.27回必要
- TFHE-SBCではZiggurat法を採用 →一様乱数生成が平均1.01回で効率的

最適化４：多項式乗算中のメモリ再利用
- 複数回の暗号化実行時には再サンプルが必要な一様乱数のみFFTを実行し，秘密鍵のFFT実行は１度だけ行う



評価
実験設定
- LWE・RLWE暗号文のベクトル・多項式の長さは1024．Raspberry Pi Zero 2Wで評価.
- TFHE-SBCはSBC向けに最適化したRLWE暗号化，TFHEppはLWE暗号化の値.

評価結果 (表1)
- 暗号化速度は**最大2490倍高速化**
- 通信コストは**1/512に低減**
- エネルギー消費量は**最大2004倍効率化**

表1: TFHE暗号化・暗号文サイズの評価

	TFHE-SBC	TFHEpp
Encryption Time [ms]	**3.1**	7705.6
	1 ×	**2486 ×**
Ciphertext Size [KiB]	**8**	4096
	1 ×	**512 ×**
Memory [KiB]	**336.2**	4297.7
	1 ×	**12.8 ×**
Energy [mJ]	**5.0**	10017.3
	1 ×	**2003.5 ×**

IoT通信における属性ベース暗号の活用に向けた検討
（研究担当:佐々木　怜名）

背景
- IoTシステムとセキュリティ
  - 多数のIoTデバイスを含むシステムの登場[1]
  - TopicベースのPublisher/Subscriber通信モデルが一般的
- Publisher/Subscriber通信セキュリティ
  - Broker上・通信路上における秘匿性の高いデータ保護が必要[2]
  - TLSを用いた通信路上のデータ保護
- Brokerは攻撃を受けるリスクが上昇[3,4]
  - SubscriberやBrokerへのアクセス制御が必要
- IoTデバイス上でABE処理の実用性の評価[5-7]
  - IoTデバイスの高性能化に伴う再評価の必要性

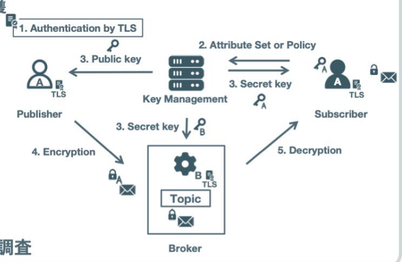
属性ベース暗号
- ABE: Attribute-Based Encryption
- 特定の属性集合や，ポリシを持つ者のみが復号可能で，アクセス制御機能を持つ
- 第三者鍵生成局が，マスタ公開鍵と属性/ポリシに基づいた 秘密鍵を発行
  - 属性リスト例: “Female”, “nurse”, “Birthdate: 10/14/1990”
  - Policy例: (“doctor” OR “nurse”) AND (Over the age of 30)

研究目的
TLSを考慮し，リッチなIoTデバイス上におけるABE暗号化処理の実用性を評価

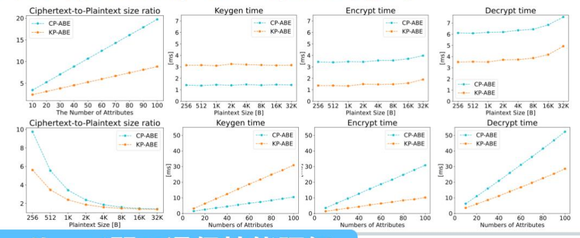
ABEを用いたIoT通信プロトコルの検討
- TLSによる相互認証とABEを用いて，データのアクセス制御と通信路上の保護
  - TLS認証のみ行い，TLS recordプロトコルを用いずにABE暗号文を送信

1. 鍵サーバが公開鍵と，各ユーザが持つ属性リスト・ポリシに基づいた秘密鍵を配布
2. Publisher - Broker間，Broker - Subscriber間でTLS相互認証を行う
3. PublisherはBrokerにABE暗号文を送信
4. SubscriberはBrokerからtopicデータを受信し，ABEで復号

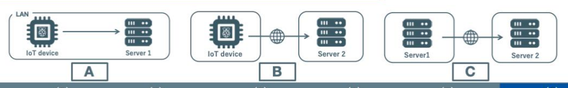
- 実験
  - ➢ ABEライブラリ（OpenABE）の性能評価
  - ➢ TLSによる相互認証のオーバヘッドの調査
  - ➢ TLS recordプロトコルとABEによる二重の暗号化処理が通信に与える影響の調査



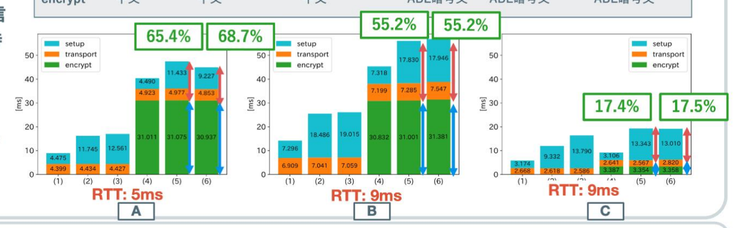
OpenABEの暗号文サイズ/鍵生成時間/暗号化時間/復号時間の計測
- OpenABE[6]：C/C++実装ライブラリ，ペアリングライブラリ(relic-toolkit)・GMP・OpenSSLを用いる
- 上段: 平文サイズ(256 B~32 KiB)，属性数 = 10
  - OpenABEの処理時間は平文サイズに依存しない
  - OpenABEでは鍵カプセル化による暗号化・復号処理をするため
- 下段: 平文サイズ = 1 KiB，属性数(10,20, …, 100)
  - 属性数とABEの処理時間は比例
  - 各属性ごとに指数演算やペアリング演算をするため



TLSとABEを用いたクライアント・サーバ間の通信性能評価
- 6通りの通信手法を比較
  - データ送信時間 = setup + transport + encrypt
- transport: TLS暗号化処理よりもレイテンシの影響が大きい
  - ➢ ABEとTLS record プロトコルの二重の暗号化処理の通信性能への影響が小さい
- レイテンシが大きい時，TLS認証/送信に時間がかかるため，ABEの暗号化時間は相対的に小さくなる
  - Raspberry Pi 4B (B): 55%, Server (C): 17%
  - ➢ 属性数小(~10)/広域通信/リッチデバイス上のABE暗号化処理は実用的



	(1)	(2)	(3)	(4)	(5)	(6)
setup	TCP socket connection	TLS Handshake認証	TLS Handshake認証	TCP socket connection	TLS Handshake認証	TLS Handshake認証
transport	TCP socket	TLS Record protocol	TCP socket	TCP socket	TLS Record protocol	TCP socket
encrypt	平文	平文	平文	ABE暗号文	ABE暗号文	ABE暗号文



今後の課題
ARM実装の最適化，Revocationに対処できるセキュアなシステムの検討

[1] Hu Xiong et,al. 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] C. Esposito and M. Ciampi, “On Security in Publish/Subscribe Services: A Survey,” in IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 966-997, Secondquarter 2015.
[3] Olivier Blazy et al., An IoT Attribute-Based Security Framework for Topic-Based Publish/Subscribe Systems. IEEE Access, Vol. 9, pp. 19066–19077, 2021.
[4] M. Rasori et al., “A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things,“ in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8269-8290, 1 June1, 2022.
[5] Moreno Ambrosin, Arman Anzanpour, Mauro Conti, Tooska Dargahi, Sanaz Rahimi Moosavi, Amir M. Rahmani, and Pasi Liljeberg. On the feasibility of attribute-based encryption on internet of things devices. *IEEE Micro*, Vol. 36, No. 6, pp. 25–35, 2016.
[6] MorenoAmbrosin,MauroConti,andTooskaDargahi.Onthefeasibility of attribute-based encryption on smartphone devices. In *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*, p. 49–54, 2015.
[7] Xinlei Wang, Jianqing Zhang, Eve M. Schooler, and Mihaela Ion. Per- formance evaluation of attribute-based encryption: Toward data privacy in the iot. In *2014 IEEE International Conference on Communications (ICC)*, pp. 725–730, 2014.

https://www.is.ocha.ac.jp/~oguchi_lab/　　oguchi@is.ocha.ac.jp