SecHack365

IoTのための秘密計算プラットフォームの開発

開発駆動コース　仲山ゼミ　橋本優太

構想

～ IoTによって収集されるユーザデータを暗号で保護して安全に活用 ～

IoT機器により様々な情報がインターネットを通じて収集

サイバー攻撃によるデータ流出や管理者による不正利用などプライバシー侵害のリスク

データを暗号化して保存しておくことによりリスクを回避

データを暗号化した状態で計算可能な秘密計算によって安全な統計処理を実現

利用例

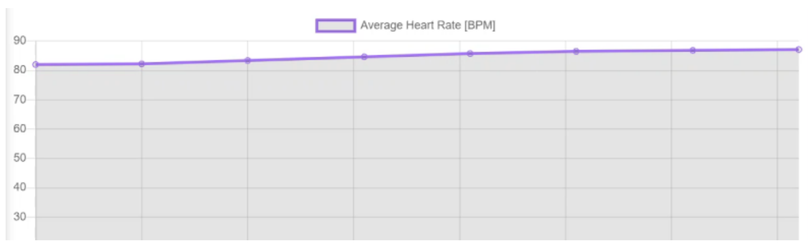
1. スマートウォッチで心拍数を計測し，Raspberry Pi上で暗号化し送信

```
Realtime heart BPM:89
{
  "mrQ_y": "HIJEv0/2Nd8sfgYbJHIlcHwQui58cJuQhNL2pc9vUyCwNkaRhS59pMc5m4+tbNRxTueADVNsAk0vkw==",
  "kind": 1,
  "mrQ_x": "Db0ov/Wir88NiXShxRiAYfO0Ol7QexFMtWkrQ+c4ZISZhOFmGhO1lQKI36Ss8feHroUAOTmLefc2nQ==",
  "rP_x": "AqQvkizYDWlSKlrkiSjW8NhXH6U7PmfNQXWWjzaNHO27uA4Ren1mDbNCfj790k3jyUNfO6tvZ6JPaw==",
  "rP_y": "IgeHLbZhCFR+iPIjf/5qwSd0/vQLcl+1whtudAPA9saQ14Dvr5YTrAzdNscrYq525EJB2QHVTIX3/Q==",
  "user": 1,
  "timestamp": 1580217083
}
```

2. プラットフォーム上で，暗号化した心拍数の加算

```
% python3 hadd_api.py
POST /func/add
POST /func/add
POST /func/add
POST /func/add
POST /func/add
POST /func/add
POST /func/add
```

3. 加算後の心拍数をブラウザ上で復号し，総数で割った平均心拍数を可視化



開発物

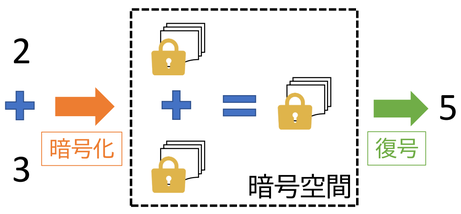
1. 準同型暗号ライブラリ

- **暗号化したデータの計算**を可能とする準同型暗号ライブラリ
- 外部ライブラリを利用しない**フルスクラッチ開発**
- 用途のための**複数言語に対応**
  - **Python**(Cython): **Raspberry Pi** 上でセンサデータの暗号化
  - **JavaScript**: **ブラウザ**上での暗号化/復号 & **AWS**上での準同型計算
- **Lifted EC-ElGamal暗号**の利用
  - 楕円曲線暗号を用いた**加法準同型暗号**

$Enc(m) = [P^r, P^{m+rs}] = C$　　(s: 秘密鍵，P: 初期点，r: 乱数)

$Dec(C) = \log_P(P^{m+rs}/(P^r)^s) = m$

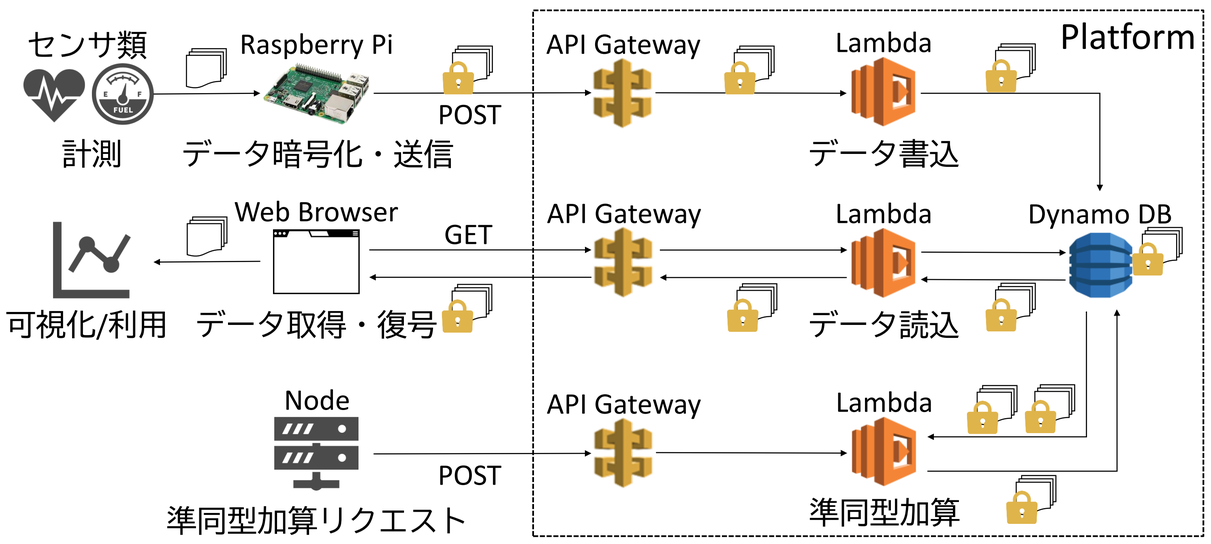
$Add(C, C') = \left[P^{r+r'}, P^{(m+m')+(r+r')s}\right] = C''$



- **乗法準同型性**にも発展可能

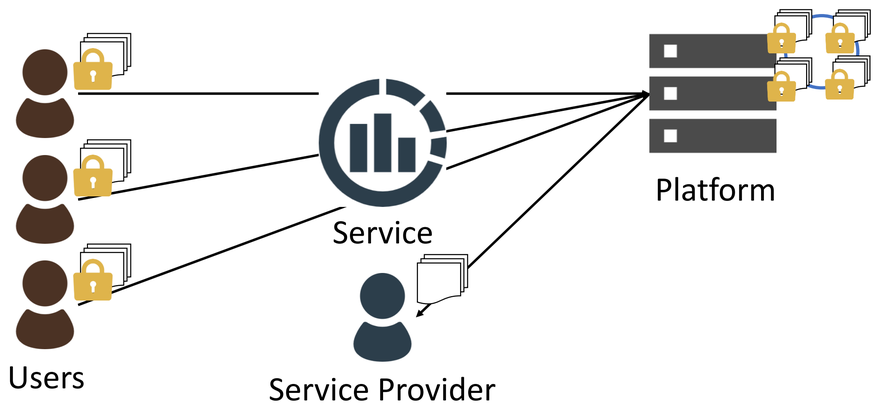
2. 秘密計算プラットフォーム

- AWSを利用した**サーバレスアーキテクチャ**を適用
- **JSON**形式による暗号化データの送受信
- シンプルな**RESTful API**によってプラットフォームを制御
  - **データ取得**　- GET /data/:user/:kind
  - **データ保存**　- POST /data/:user/:kind
  - **準同型計算**　- POST /function/:name
- **独自の秘密計算プロトコル**の設計



<u>**異なる秘密鍵を用いたユーザ間の統計**を暗号化されたデータから求める</u>

1. 各ユーザのデータを暗号化してプラットフォーム上に保存
2. サービス側は各ユーザに対して，データの統計利用について可否を確認
3. ユーザは自身の意思によって可否を返答
4. 承諾したユーザのデータを暗号化された状態で秘密計算
5. サービス側は統計結果のみを取得可能



特徴

- **ユーザサイドでデータの暗号化**を行い，**通信路とクラウド上の処理経路**でユーザデータを**保護**
- 個々のデータの復号に必要な**秘密鍵はユーザのみが所有**するため，**ユーザのみが自身のデータを閲覧可能**
- サービス側は**ユーザ間の統計データのみ**を，**ユーザの承認により**取得可能

性能

- 暗号化/復号処理時間の目安 (462-bit BN Curve)
  - Raspberry Pi 3 model B 上での暗号化: 53 [ms]
  - Chrome(Ver.79) 上での復号:
    10 [ms] (1-bit), 45 [ms] (8-bit), 150 [ms] (10-bit)

今後の課題

- 乗法準同型性などによる秘密計算機能の発展
- 独自プロトコルの実装と検討
- その他手法との比較と見直し

NICT 国立研究開発法人 情報通信研究機構