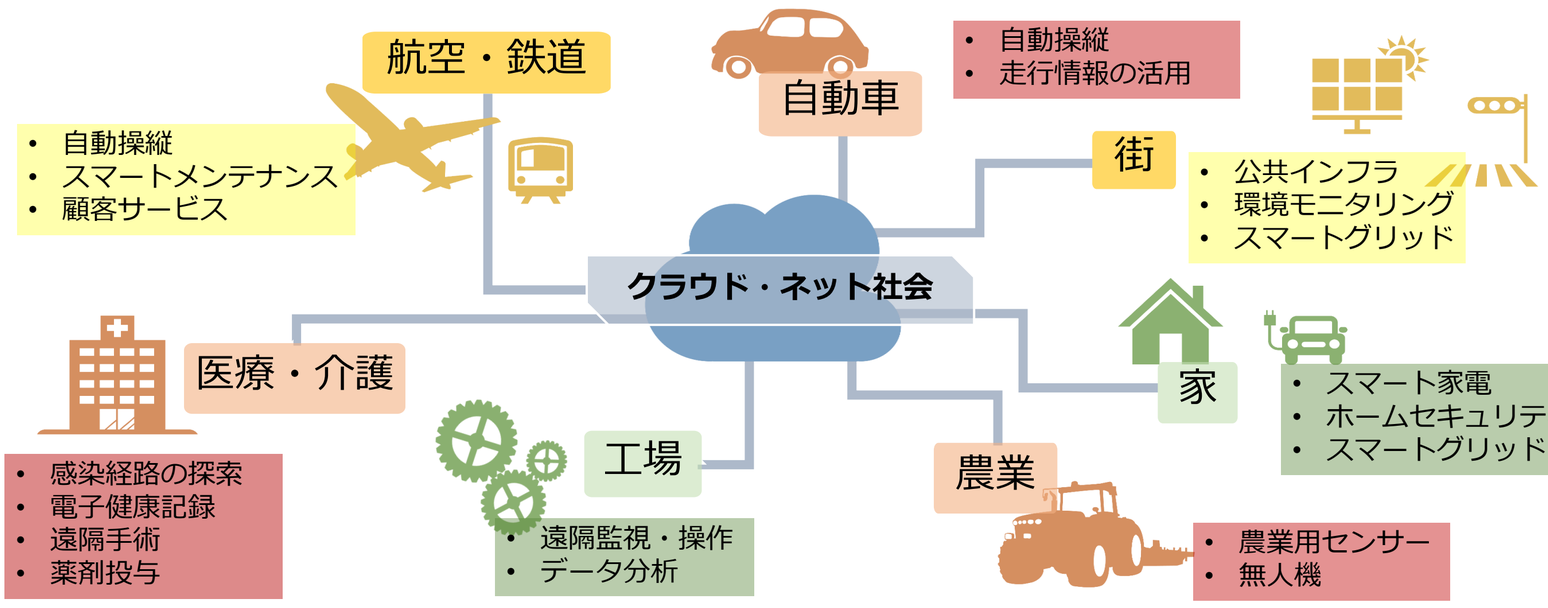
# IoTデバイス向けシステム開発とハードウェア実装

## System development and hardware implementation for IoT device

岡山大学　野上保之　日下卓也　小寺雄太　高橋裕人　多田羅友也　服部大地

## IoT時代の到来

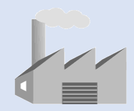



## セキュリティ脅威

IoTデバイスの乗っ取り

アクセル・ブレーキの乗っ取り

**交通事故**



産業用ロボットの乗っ取り

**生産ライン停止**

信号機の乗っ取り

**交通網の混乱**

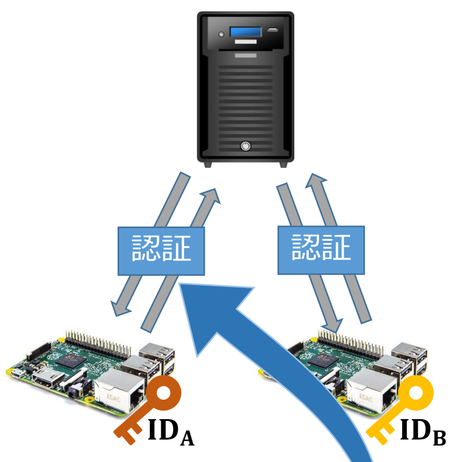
問題点

**IoTデバイスが乗っ取られると重大事故・事件につながる恐れ**

安全に情報を処理する技術が重要

## IDベース暗号

Raspberry Piを用いたIDベース認証の実装




アドレスなどの任意の文字列を鍵として利用できる

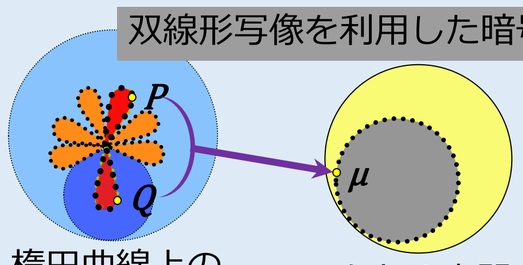
鍵の管理が容易なためIoTデバイスに適している

問題点

**計算時間が非常に長い**

## ペアリング暗号

双線形写像を利用した暗号




楕円曲線上の点 : $P, Q$

ベクトル空間上の点 : $\mu$

IoTデバイスは計算能力が乏しいため効率化技術が重要

Rennes大学 Sylvain教授と効率化について共同研究中

## LPWAを用いた多要素認証

Sigfox通信を用いたOne Time Password (OTP)の送受信によるIoTデバイス認証

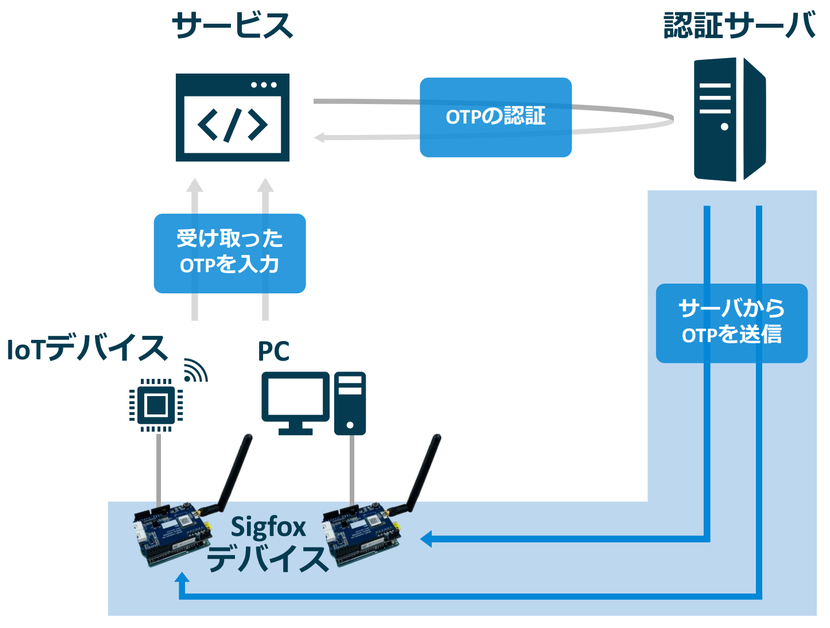
IoTデバイスの管理，認証を効率的に行う

通信路に**Sigfox**を活用，多数のIoTデバイスに対しても安価にセキュリティ対策

**Sigfox**

IoT向け通信規格

- 安価
- 低電力
- 低容量
- 低速



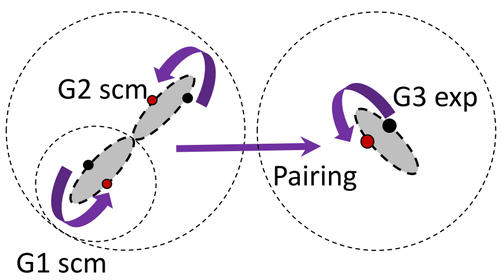

**セキュアで安価な独立した回線を提供**

## 世界最速のペアリング計算ライブラリELiPS

ELiPS(Efficient Library for Pairing Systems)とは…

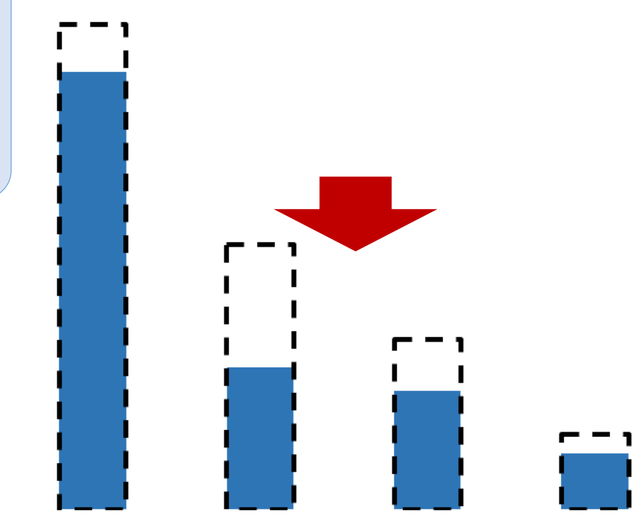
ペアリング計算には多くの計算リソースが必要となる．ELiPSは効率的アルゴリズムや高速計算ライブラリ（GMP）を用いてペアリング計算の高速化を図っている．

ペアリングライブラリの主要な計算項目




https://github.com/ISecOkayamaUniv/ELiPS

ELiPSと他ライブラリとの比較



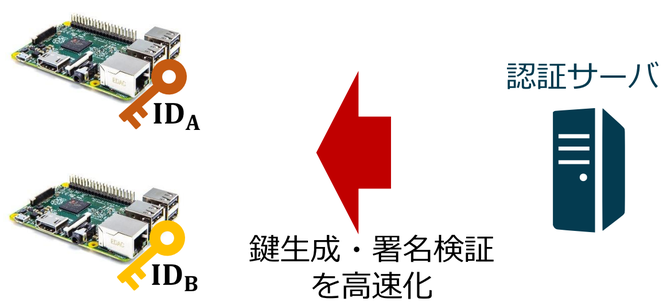

主要な各計算項目で演算時間が減少

## 今後の展望

高速なペアリングライブラリELiPS

LPWAを用いた多要素認証

認証サーバで効率的に鍵管理




**効率実装されたセキュアなプロトコルを提供**