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　五百旗頭 健吾　亀川 哲志

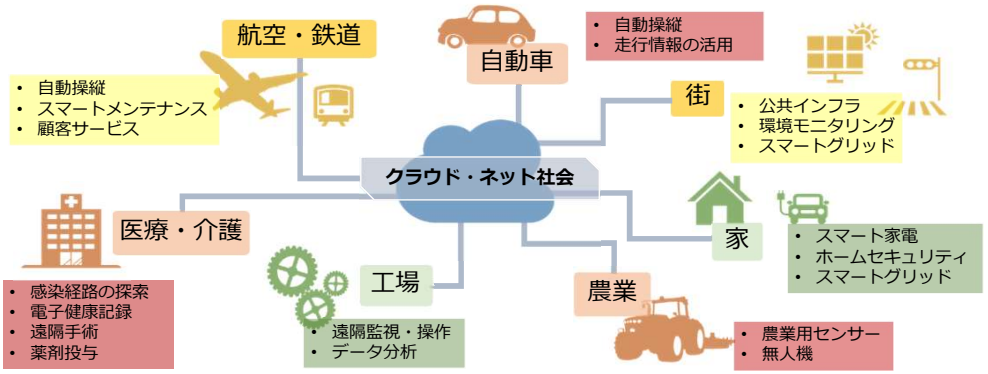
株式会社ゴフェルテック 川西 紀昭

九州工業大学 荒木 俊輔

The University of Rennes Prof. Sylvain Duquesne

Pusan National University Taehwan Park

IoT時代の到来



セキュリティ脅威

IoTデバイスの乗っ取り

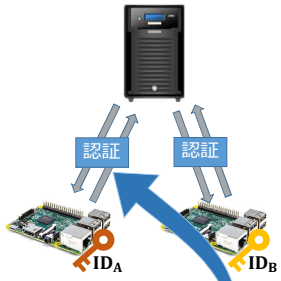
問題点

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ベース認証

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

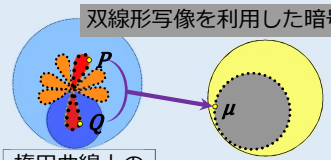
鍵の管理が容易なためIoTデバイスに適している

問題点

サイドチャネル攻撃によって鍵を盗まれる可能性がある

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：μ

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

メッセージ認証

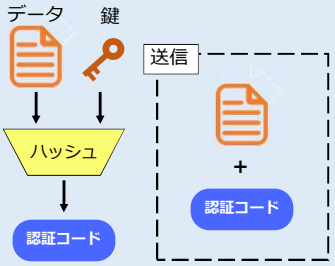
Arduinoを用いた車載ネットワーク用プロトコルへのメッセージ認証の実装

自動車の電子化が進み，外部と接続する機会増加

車載ネットワークへの侵入経路が増え，外部からのアクセスによる脅威増大

データと認証コードを合わせて送信することにより乗っ取りを防ぐ

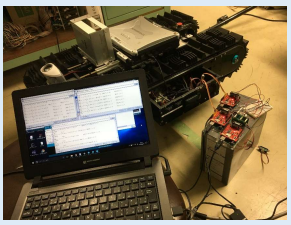
九州工業大学 荒木助教と共同研究



認証コード計算時間による遅延の通信への影響を検証

インタフェースシステム学研究室 亀川講師と共同研究

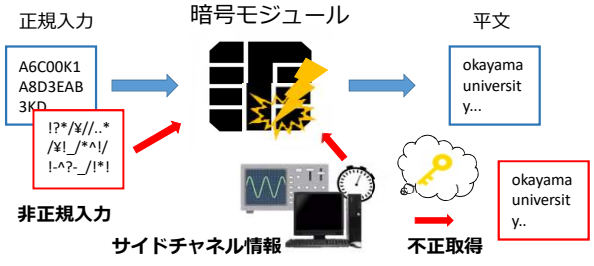
Arduinoで車載ネットワークを再現



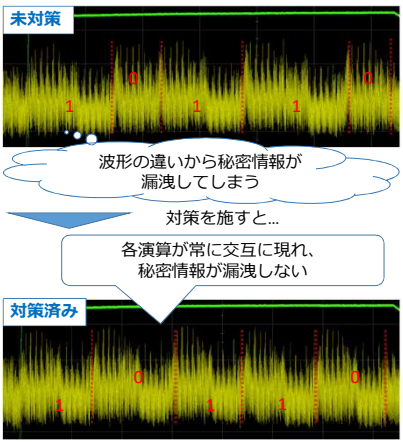
サイドチャネル攻撃の対策

サイドチャネル攻撃（SCA）とは

暗号化や復号を行うときの処理時間や消費電力、電磁波、熱、音など（サイドチャネル情報）の推移を物理的手段を用いて測定し、秘密情報を推定する攻撃手法



電力解析攻撃による波形図

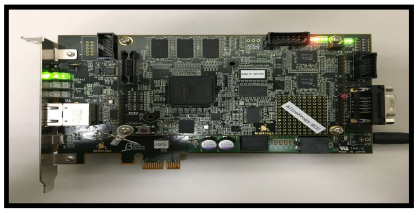


今後の展望

実製品に近いIoTデバイス

短い鍵長を実現する次世代暗号

FPGAボード ✚ 楕円曲線暗号



HW実装・SCA対策
（株）ゴフェルテックと共同研究中