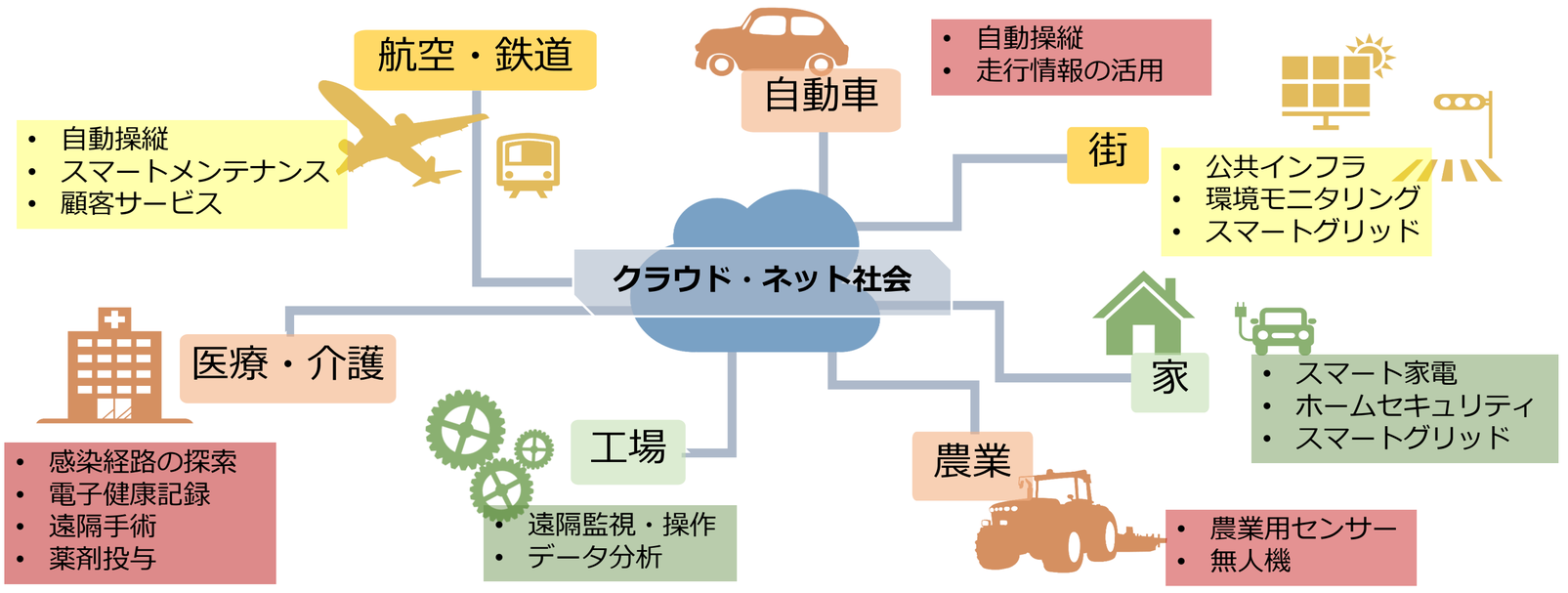
IoT時代における機器認証を安全に実現するセキュリティ計算チップの開発

岡山大学　野上 保之　五百旗頭 健吾
株式会社ゴフェルテック　川西 紀昭

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

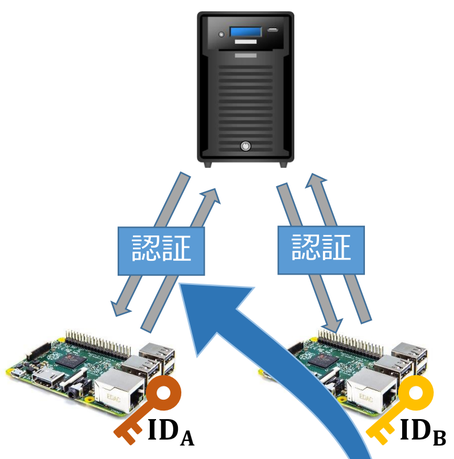
信号機の乗っ取り
交通網の混乱

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



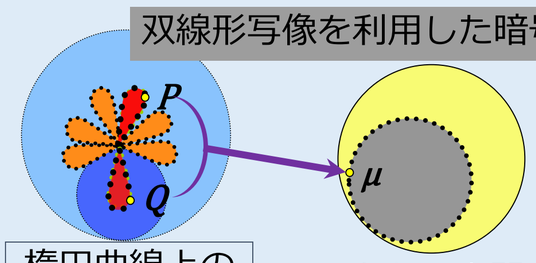
アドレスなどの任意の文字列を鍵として利用できる

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

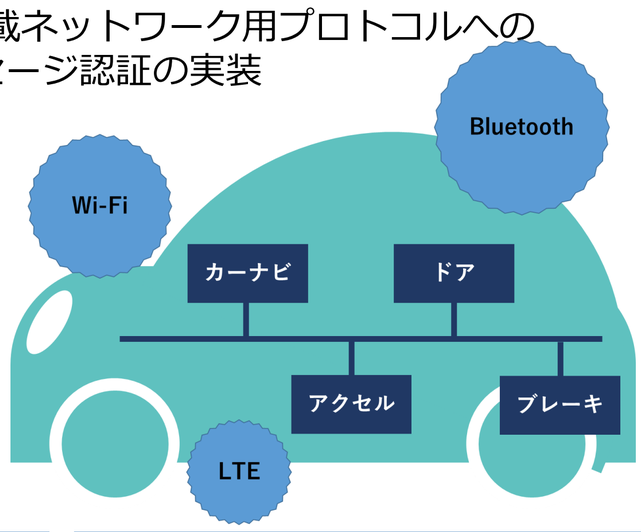
Rennes大学 Sylvain先生と効率化について共同研究中

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

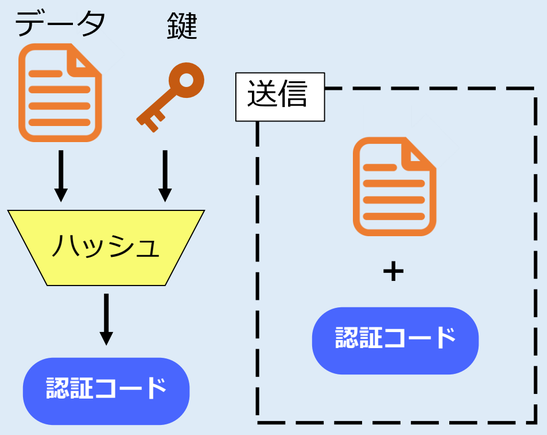
自動車の電子化が進み，外部と接続する機会増加

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

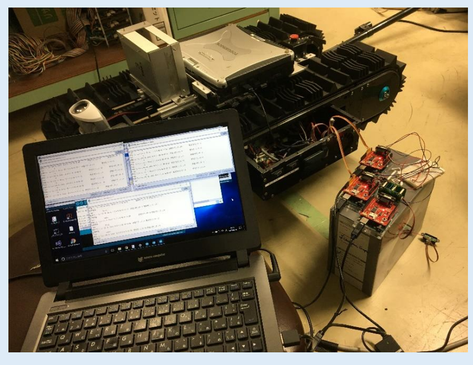
九州工業大学 荒木先生と共同研究中



認証コード計算時間による遅延の通信への影響を検証

岡山大学 亀川先生と共同研究中

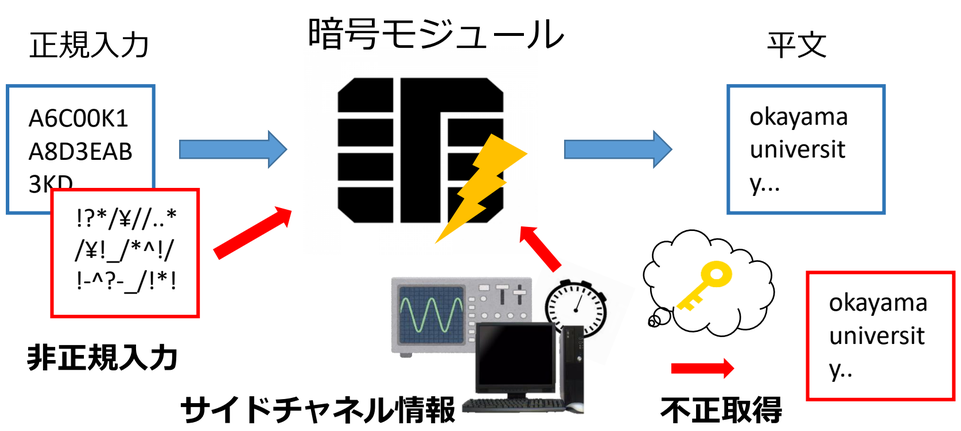
Arduinoで車載ネットワークを再現



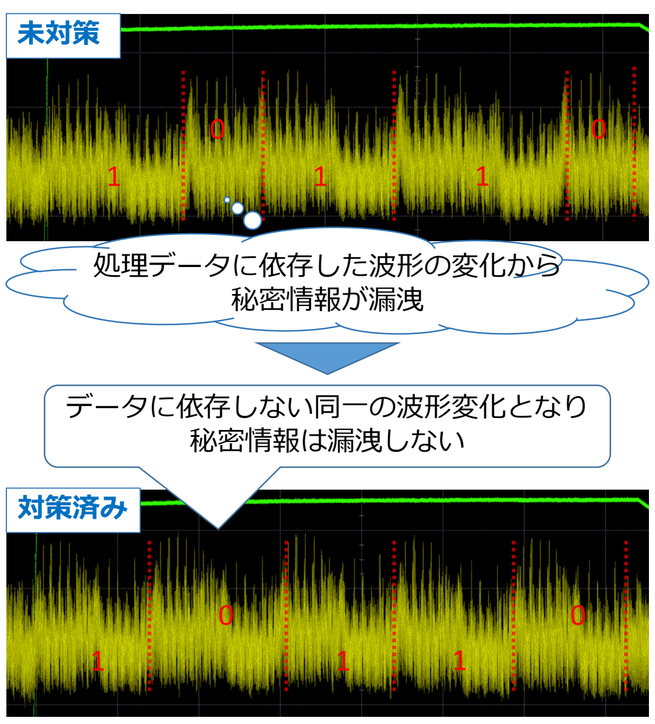
サイドチャネル攻撃の対策

サイドチャネル攻撃（SCA）とは

暗号化や復号処理の時間やその時に暗号回路で発生する消費電力、電磁波、熱、音などの物理状態の変化（サイドチャネル情報）を測定し、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

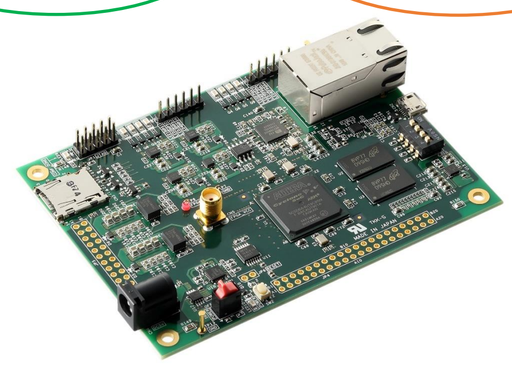


今後の展望

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