岡山大学
OKAYAMA UNIVERSITY

IoT時代における機器認証を安全に実施するセキュリティ計算チップの開発

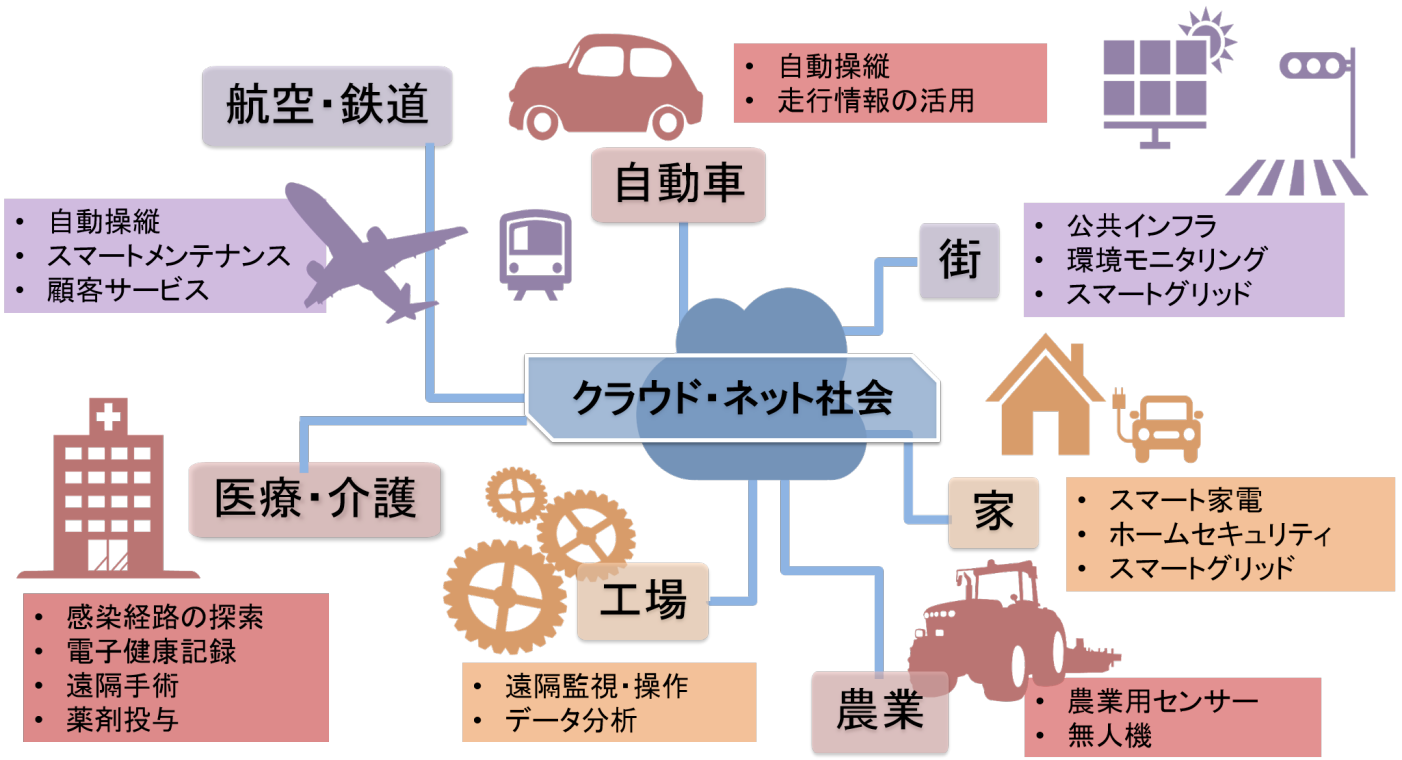
岡山大学　大学院自然科学研究科
野上 保之　籠谷 裕人　五百旗頭 健吾

株式会社ゴフェルテック　開発部
川西 紀昭

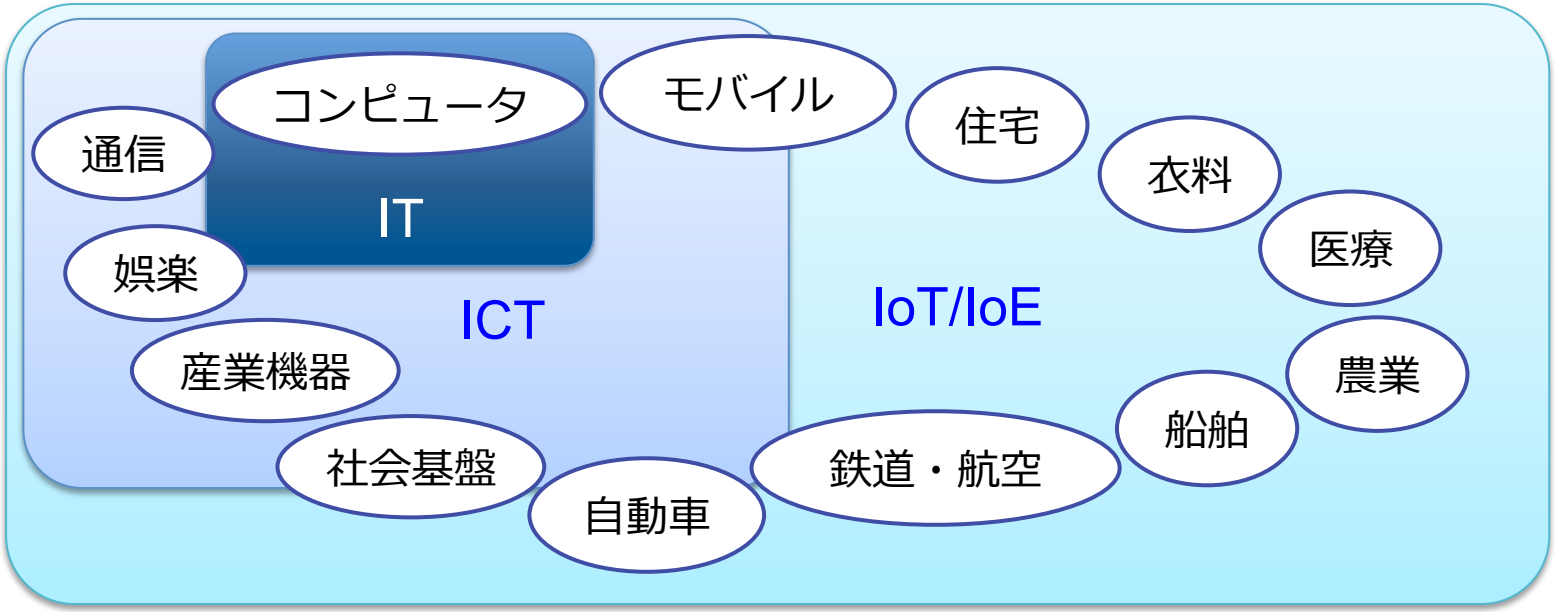
地域ICTイノベーションセミナー
2017年11月1日（水）

IoT時代

- 身の回りのあらゆるモノがインターネットにつながる時代
- あらゆる情報がインターネットを行き交う
- 情報をいかに使うかが価値を生む時代



プロジェクトの目的



- IoT時代を勝ち抜くために
  - 新しいサービスの開発
  - 情報セキュリティ技術を利用した差別化

暗号技術の基盤となるセキュリティ計算チップの開発

セキュリティ脅威

セキュリティ対策が充分ではなく
IoTデバイスが乗っ取られてしまった場合・・・

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

安全に信号を送受信・処理する方法の確立

攻撃事例

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer

Roel Verdult **Baris Ege** **Flavio D. Garcia**

Radboud University Nijmegen, The Netherlands

School of Computer Science, University of Birmingham, UK.

Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands
rverdult@cs.ru.nl *www.cs.ru.nl/~rverdult*

Roel Verdult — Radboud University Nijmegen

Practicality of Hitag2 Attacks

1. Communicate with the genuine car-key
   - With maximum wireless distance of **two inches**
2. Bypass other security measures of the car
   - Force the door locks of the car
   - Disable the alarm (separate protection)
   - Force the ignition lock (hot-wire the car)
3. Eavesdrop immobilizer messages from the car
4. Communicate **again** with the car-key
5. Perform a complex mathematical computation to recover the secret cryptographic key
6. Emulate the car key and start the car

Published in USENIX 2013

Hello, tell me your number →

Key number (identifier) ← Proceed **only** when identifier is **known**

Random number + Proof^{car} → Load random number, **only** respond to **valid** Proof^{car}

Proof^{key} ← Start the engine **only** when Proof^{key} is **valid**

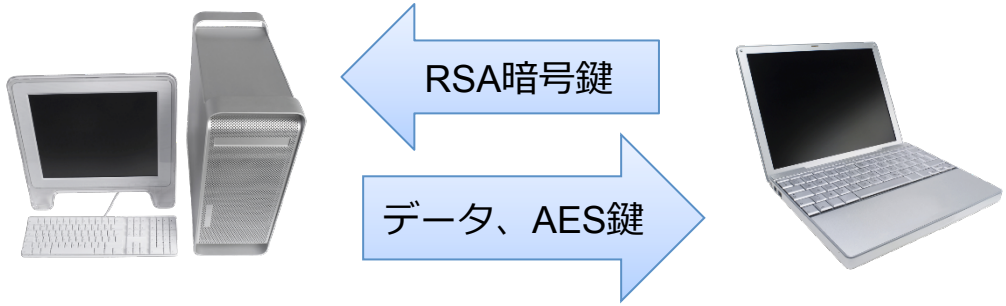
IoT時代の情報セキュリティ

- IoTの利点
  - 誰でも、いつでも、どこからでもあらゆる情報にアクセス可能
- IoTの問題点
  - 情報（個人情報や機密情報など）の保護
  - 正規ユーザかどうかの判定
- 解決法：暗号技術の適用
  - データの暗号化
  - ユーザ認証
- 技術的課題
  - IoT機器に適した暗号計算チップの開発

現代暗号

- 高度な数学に基づく高い安全性を実現
  - 数学・アルゴリム的な解読法
    - スパコンでも解読に数10年
- 暗号の種類
  - 秘密鍵暗号（DES, AES, MISTY1, KCipher-2, etc.）
    - 用途: データの暗号化
    - 特徴: 暗号化鍵と復号鍵が同じ
  - 公開鍵暗号（RSA, ElGamal, 楕円曲線暗号, etc.）
    - 用途: デジタル署名
    - 特徴: 暗号化鍵と復号鍵が異なる（暗号化鍵を公開）

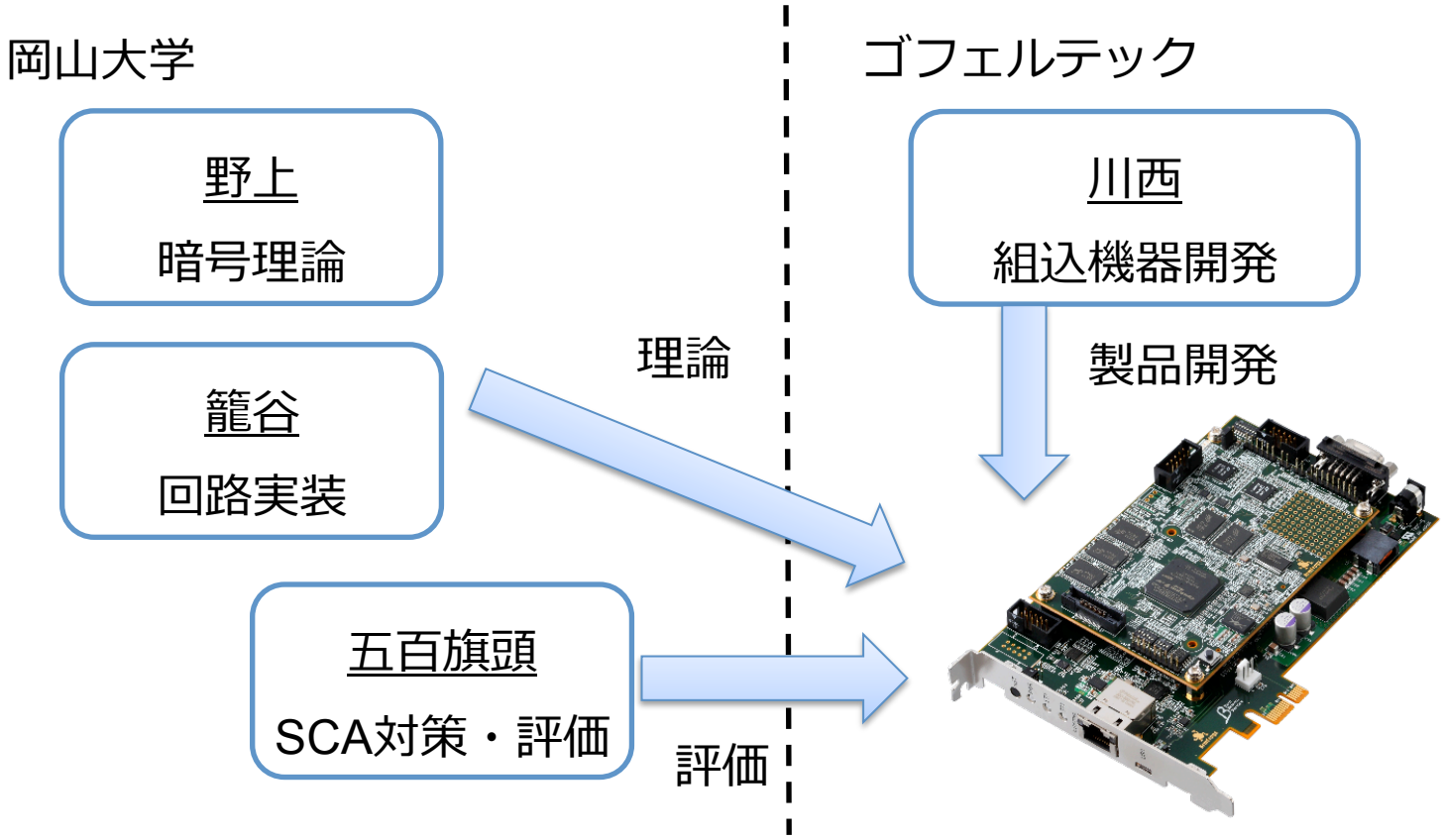
1. データをAESで暗号化
2. AES鍵をRSAで暗号化



1. AES暗号鍵を復号
2. AES暗号化されたデータを復号

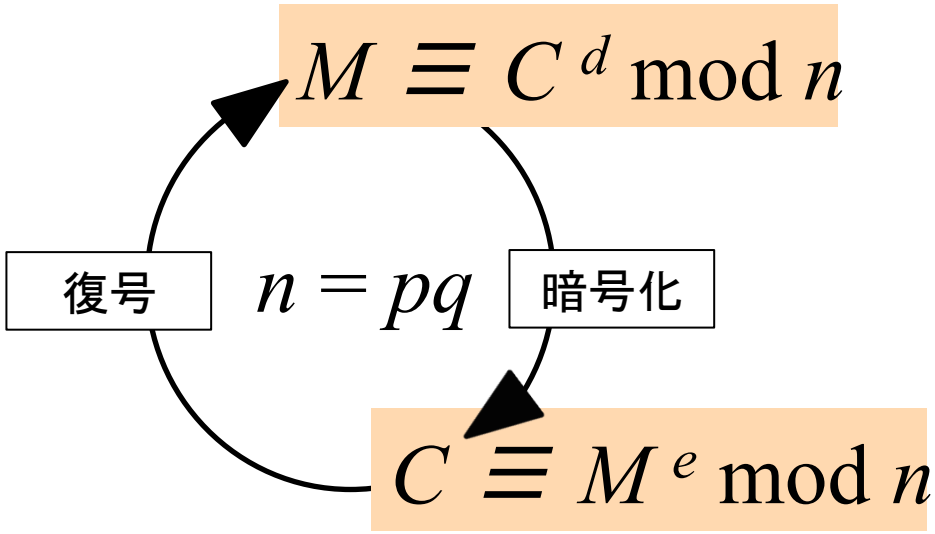
本プロジェクトの取組み

- 次世代暗号計算チップの開発
  - 楕円曲線暗号のFPGA実装
  - 新たな暗号解読攻撃への安全性保証



ユーザ／機器認証向け暗号

RSA暗号



M: 平文，C: 暗号文
p,q: 秘密鍵
n: 公開鍵

- 現在広く使われている公開鍵暗号
- 素因数分解の困難性を安全性の根拠としている

- 問題点
  - 計算機の性能向上に伴う鍵長の増大（**2000bit～**）の傾向

RSA暗号の限界

計算機性能の向上

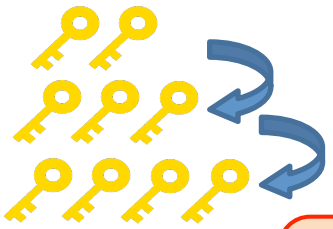
↓

解読リスク増加に伴う
鍵長の変更

IoTデバイスの普及

↓

計算機性能が制限された
環境への実装



伸びる鍵長

↓

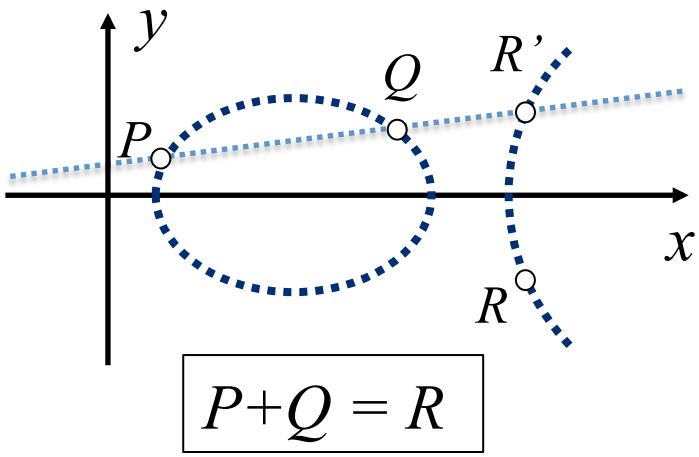
計算機性能が制限されている環境での
より長い鍵長の利用が今後厳しくなる

RSA暗号の限界

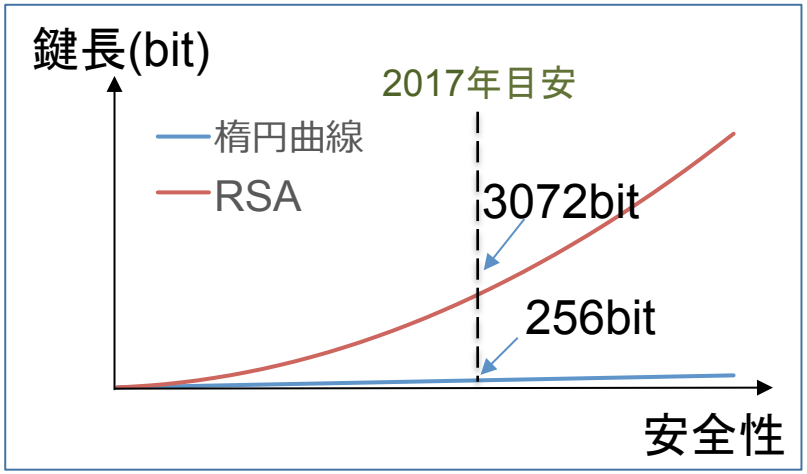
RSA暗号から 楕円曲線暗号 へ

楕円曲線暗号: ECC

- 楕円曲線上の点（有理点）を用いた暗号方式
- RSA暗号より短い鍵長で安全性を確保できる（160bit～）
  - RSA暗号に代わる次世代の公開鍵暗号として注目

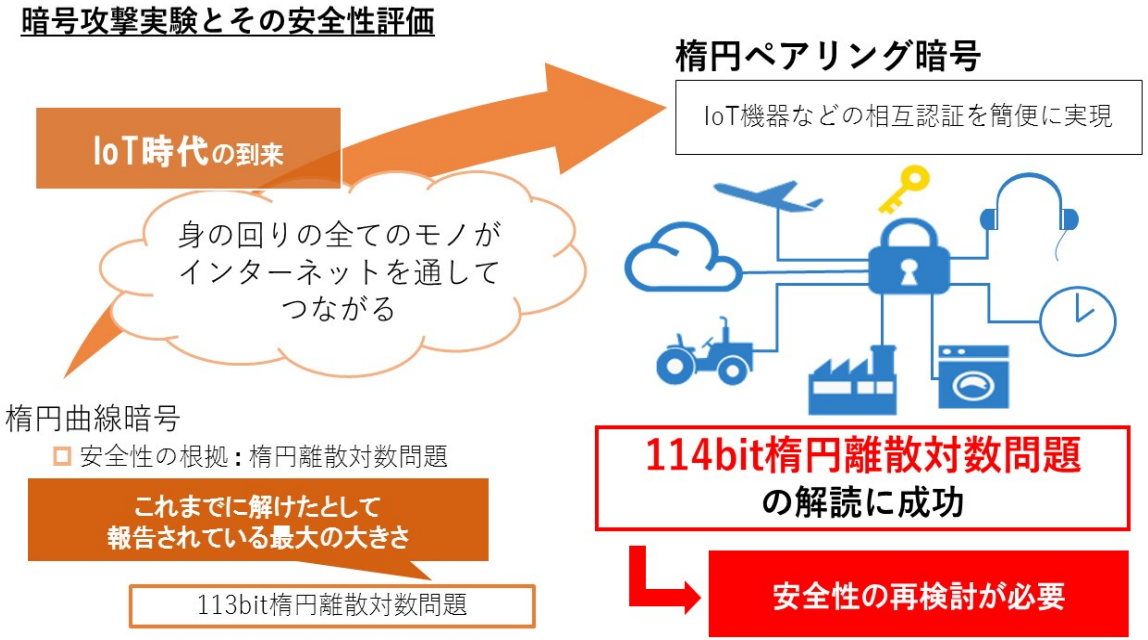


$$y^2 = x^3 + ax + b$$



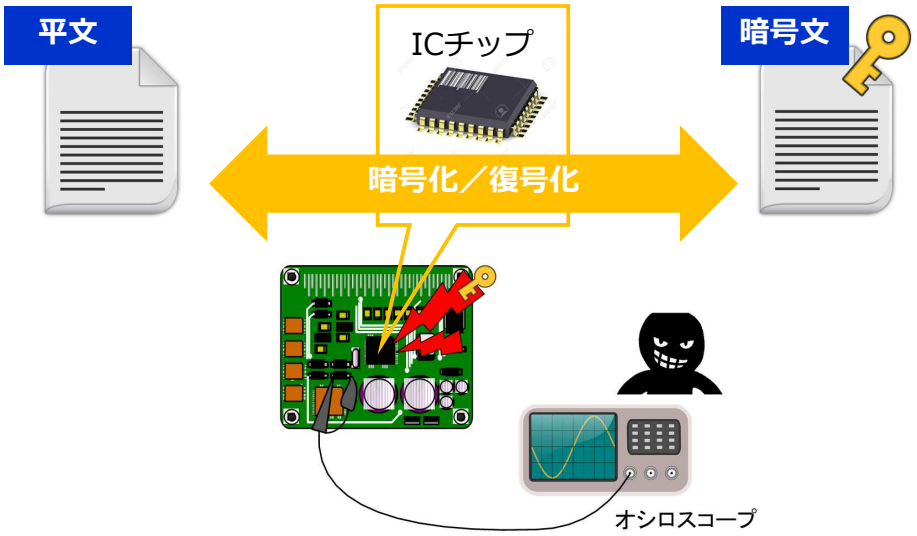
岡大SecGで推進している研究開発

- 暗号技術開発
  - AES, RSA, 楕円曲線暗号, セキュリティ用途の擬似乱数
- マイコンやFPGAなどでの実現
  - プログラムサイズ、回路規模、処理速度
- SW的な安全性評価・対策

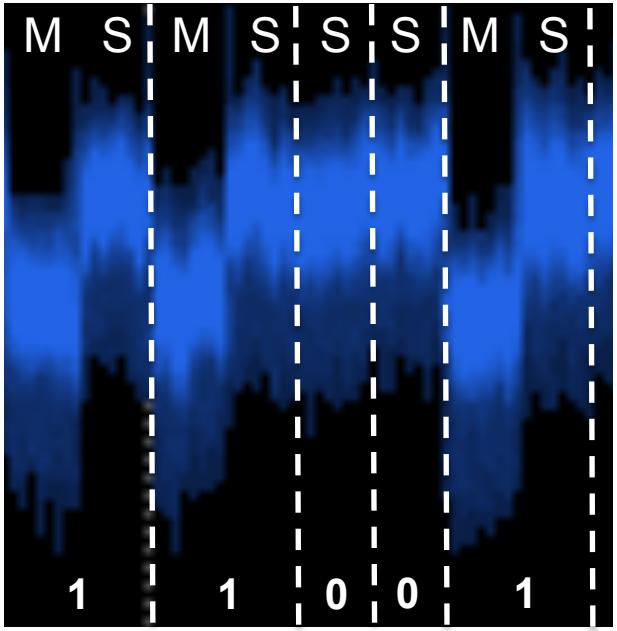


岡大SecGで推進している研究開発

- HW的な安全性の評価・対策技術の確立



サイドチャネル攻撃（新たな暗号解読攻撃法）



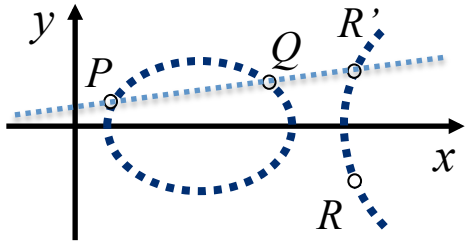
- サイドチャネル攻撃への対策法・安全性評価法
  - 等価回路モデルによる評価手法
  - 効率的なSCA対策手法

プロジェクトの進捗状況（初年度）

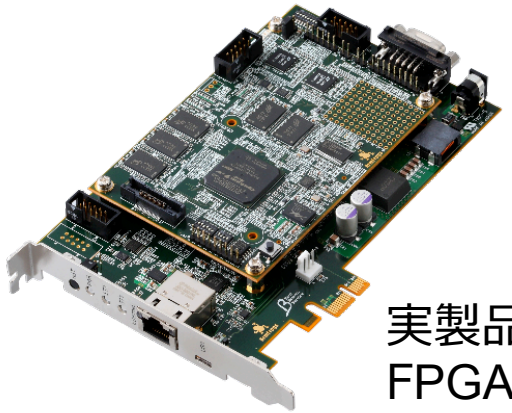
2016年度の成果

- 楕円曲線暗号のFPGA実装
  - プロトタイプを作成
- SCA耐性評価
  - 評価環境の構築
  - 実攻撃を想定したSCA波形取得ポイントの決定

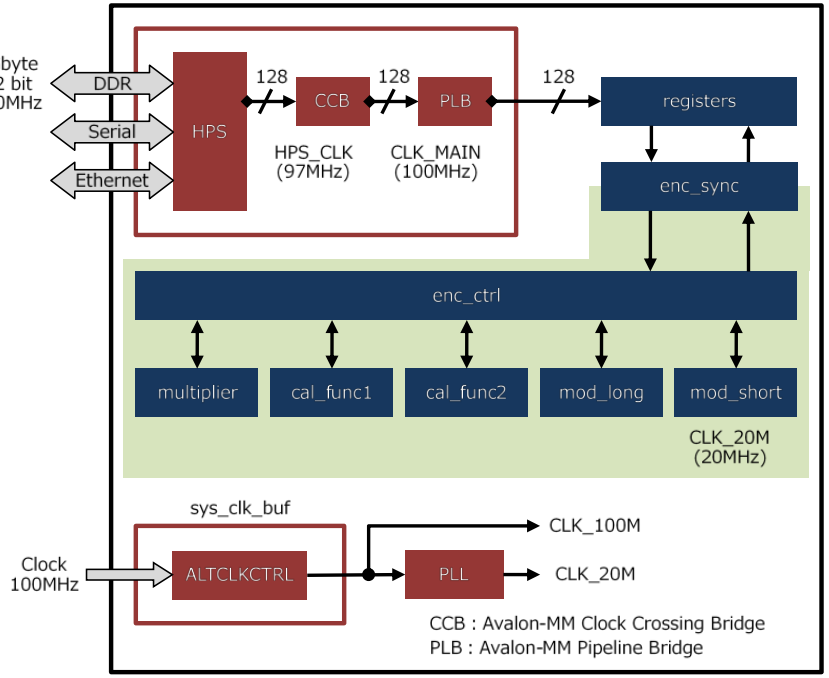
楕円曲線暗号のFPGA実装



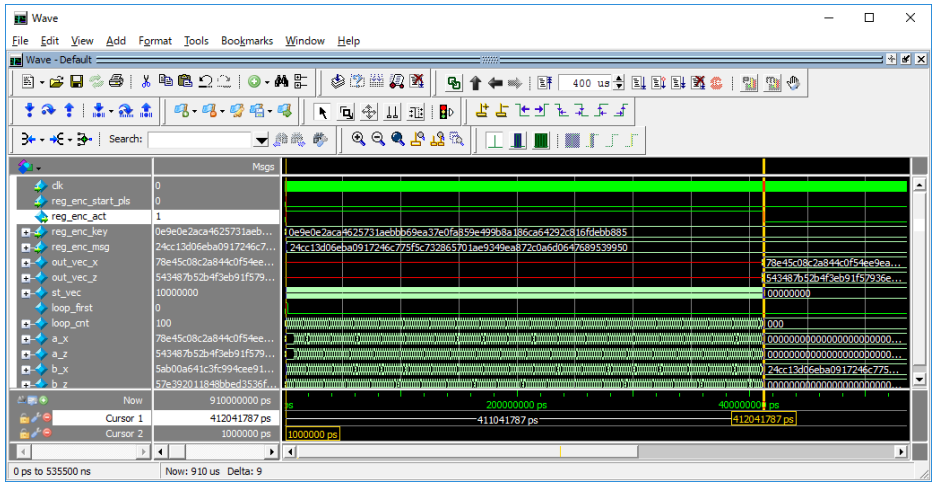
実装



実製品仕様の
FPGAボード



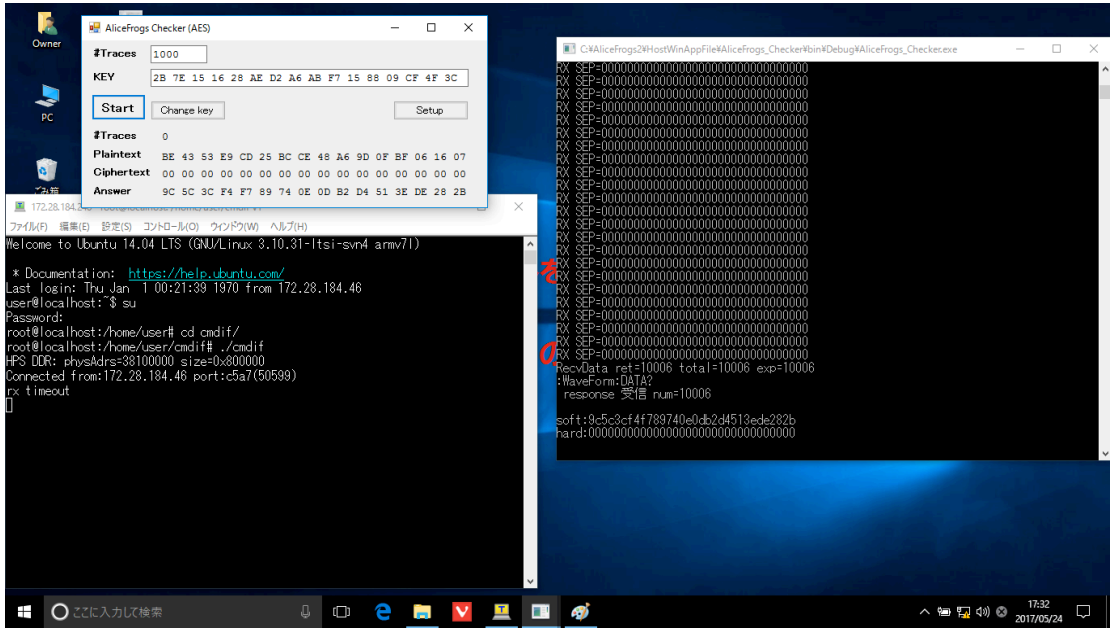
楕円曲線暗号回路の構成



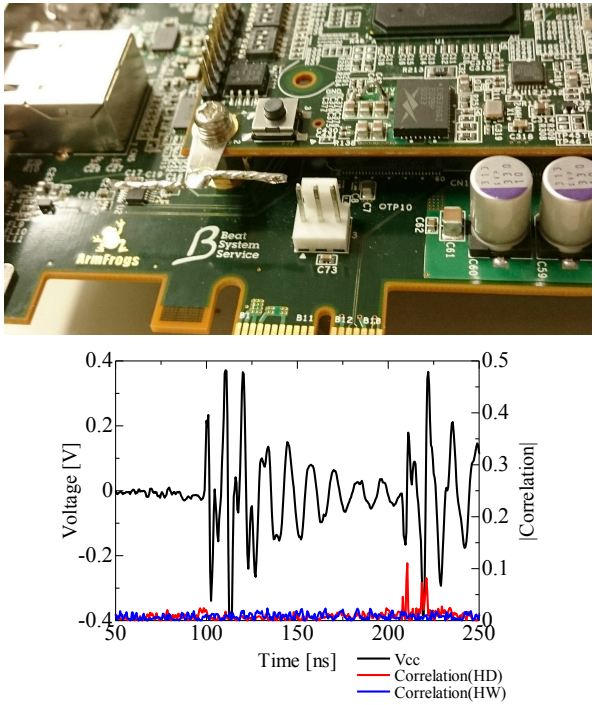
楕円曲線暗号回路の動作確認

SCA耐性評価環境の整備

- 評価用ソフトウェアの開発
  - 評価用データを自動取得
- サイドチャネル波形計測ポイントの検討
  - 実攻撃を想定した計測ポイントの選定



評価用ソフトウェアによるデータ自動取得の様子



実攻撃を想定した計測ポイント

プロジェクトの進捗状況

2016年度の成果

- 楕円曲線暗号のFPGA実装
  - プロトタイプを作成
- SCA耐性評価
  - 評価環境の構築
  - 実攻撃を想定したSCA波形取得ポイントの決定

2017年度

-
  - 改良により世界最速を伺う
-
  - SCA耐性有り（1stデータ）
  - 詳細評価の準備
  - 最悪攻撃シナリオを想定したSCA波形取得ポイントの検討