新技術説明会
New Technology Presentation Meetings!

次世代の高度なセキュリティ技術を実現する高速かつスケーラブルな暗号計算ライブラリ

岡山大学　大学院自然科学研究科
電気通信系学科
教授　野上　保之

令和2年12月15日

岡山大学
OKAYAMA UNIV.

目次

新技術説明会
New Technology Presentation Meetings!

岡山大学
OKAYAMA UNIV.

1. コロナ禍の中で作ったものとIoTセキュリティ雑感
2. 具体的に必要なセキュリティ要素とその実現方法
3. まとめ

最近の動きで気になっていること

- もとより大切なこととは
  - Society5.0/Industry4.0
  - 第4次産業革命
  - ゴールドラッシュ（DX：デジタルトランスフォーメーション）
  - MBAの考え方・シリコンバレー・深圳
    - リープフロッグという脅威
    - アイデア百出からの**プロトタイプ設計**
    - 【アジャイル】という考え方 vs 【日本的な匠】の取り組み
      - 現在主流になっているシステムやソフトウェアの開発手法の1つ
      - **「要件定義→設計→開発→実装→テスト→運用」**
        といった開発工程を機能単位の小さいサイクルで繰り返す
      - 仕様変更に強く，プロダクトの価値を最大化することに重点，少人数
      - リリースまでの時間を短縮（必ずしも完成品で無い）
    - こっそりデータ収集，BigDataへ（新たなコア）

気になるキーワード

1. ターゲット分野 **Xtech**
   交通/医療・介護/観光/農業/食品/防災・減災/インフラ維持管理/
   製造業/教育/エネルギー/働き方改革/金融/エドテック/その他
2. Society5.0を支える**ツール**
   - IoT（Internet of Things）デバイス：（FPGA，マイコン（RaspberryPi，Arduino），GPGPU，WEBカメラ）
   - AI（Artificial Intelligence），Tensorflow，YoLo
   - 各種センサ（GPS，LiDAR，人体，工場・ロボット，トラフィック）
   - 無線通信（Wifi，Bluetooth，LPWA（Sigfox，LoRa，…），5G）
   - クラウド（Connected to Connected）・エッジ（クレンジング）
   - ロボット（サーボモーター，マイコン制御）
   - OS（UNIX）・プログラミング（Python）
   - 信号処理・画像処理（OpenCV）
   - 3Dプリンタ，ドローン，タブレット，スマホ，WEB，etc

監視カメラ

学生・教員ともに大学に入れなくなった
盗難などの恐れ → **監視カメラを作ろう**

人感センサ・ラズパイ・
Wifi・Teams・画像処理

Op. 顔認証・暗号化・セキュア検索機能

サーモグラフィ

3密を避けて大学に入れるようになった
「体温を記録してください」 → **作ろう**

サーモグラフィ・WEBカメラ・
LCD・液晶モニタ（デモ用）・画像処理

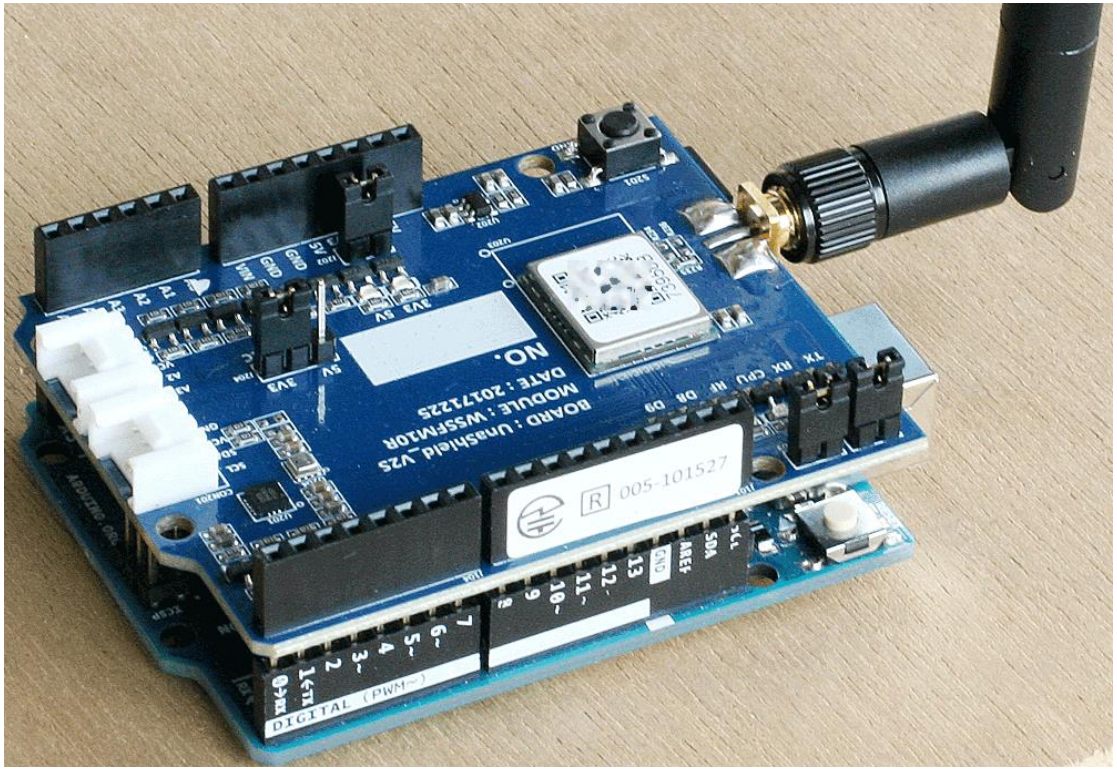
Op. 蓄積・暗号化・**学内で転用**

Sigfox＋Arduino UNO

Arduino
Sigfox（LPWA）
センサデータを加工して送信
蓄積して解析
予測してアラート

通信量が安価
広範囲に届く
電力消費が少ない

計算リソースも少ない
送信・受信データ量が少ない、
送信・受信回数にも制限がある
セキュリティは…



まずは室内温度・湿度監視という名目で…

少なくとも通信端末は頑張ろうと

- https://www.gsma.com/iot/news/new-report-outlines-security-considerations-lpwa-technology/
- https://fhcouk.files.wordpress.com/2017/05/lpwa-security-white-paper-1_0_1.pdf

	LTE-M	NB-IoT	EC-GSM-IoT	LoRaWAN	Sigfox
Forward Secrecy	No	No	No	No	No
Data Integrity	Limited [6]	Optional (with DoNAS)	Limited [6]	Limited [6]	Variable [7]
Control Integrity	Yes (EIAx)	Yes (EIAx)	Optional (GIA4/5)	Yes	unknown [8]
Replay Protection	Yes	Optional (with DoNAS)	Limited [9]	Yes	Yes
Reliable Delivery	Yes	Yes	Yes	No	No
Critical Infrastr. Class	Access Classes 11-15	Access Classes 11-15	Access Classes 11-15	No	No
Updatability (Device)	Possible	Possible	Possible	Limited [10]	No
Updatability (Keys / Algs.)	Optional (SIM OTA)	Optional (SIM OTA)	Optional (SIM OTA)	Limited	No
Nwk. Monitoring and Filtering	Yes	Yes	Yes	Limited	Monitoring only
Key Provisioning	pre-provisioned or RSP	pre-provisioned or RSP	pre-provisioned or RSP	pre-provisioned (ABP) or OTAA	pre-provisioned
Algorithm Negotiation	Yes	Yes	Yes	No	No
Class Break Resistance	Yes [11]	Yes [11]	Yes [11]	Optional [12]	Yes [11]
Certified Equipment	Required	Required			
IP Network	Optional	Optional			

情報公開されているようなされていないような。
公開しない方が良いような悪いような。

実際どこに注意が必要か

- 守るものも色々あり（命，財産，信用）
- コストとのバランスも必要（いたちごっこ）
- 白物家電や自動車のようにライフサイクルにも注意（危殆化）

- 守りの要所として（リソースの限界を意識すれば）
  - 入出力（正当性チェック）
  - データ暗号化
  - プログラムサイズ・正当性
  - 機器認証・データ認証
  - 更新可否（プログラム，秘密鍵）
  - 物理的な耐性（ハードウェアセキュリティ）
  - セキュアプログラミング
  - 前述の組み合わせ，階層的なセキュリティ対策も
  - 実行コマンドのホワイトリスト（ブラックリストでは限界も）

秘密鍵
乱数
ハッシュ関数
AES暗号＋使用mode

公開鍵暗号は重たい

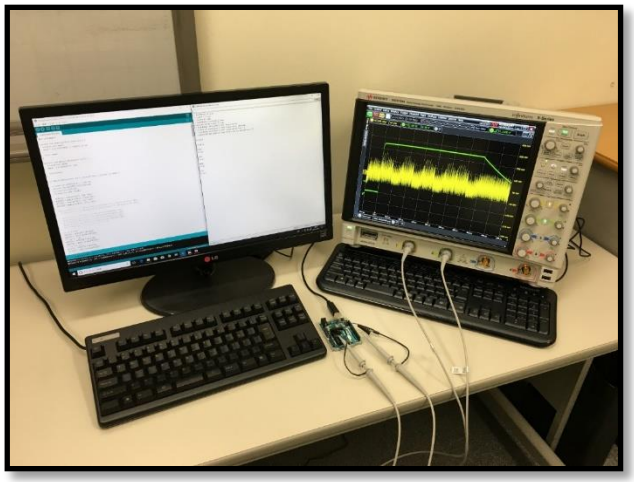
私が研究していること

新技術説明会
New Technology Presentation Meetings!

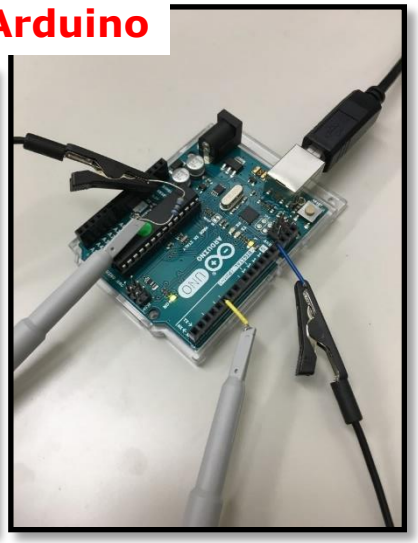
岡山大学
OKAYAMA UNIV.

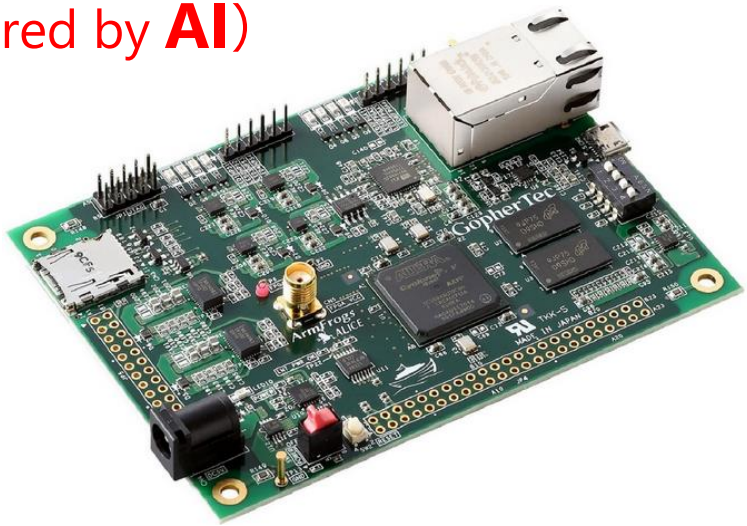
- IoT＋AI＋Securityの組み合わせが楽しく，様々なシステムを考案中
- とくにセキュリティ対策では，
  - 物理・擬似乱数生成
  - 機器認証・データ認証暗号
  - 鍵更新プロトコル，など **（リソースが限られているのでたいへん）**

- その一方で，解読攻撃（S/W，H/W powered by **AI**）



Arduino



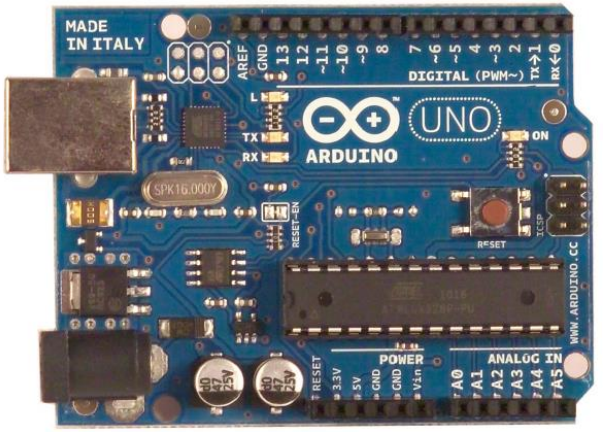


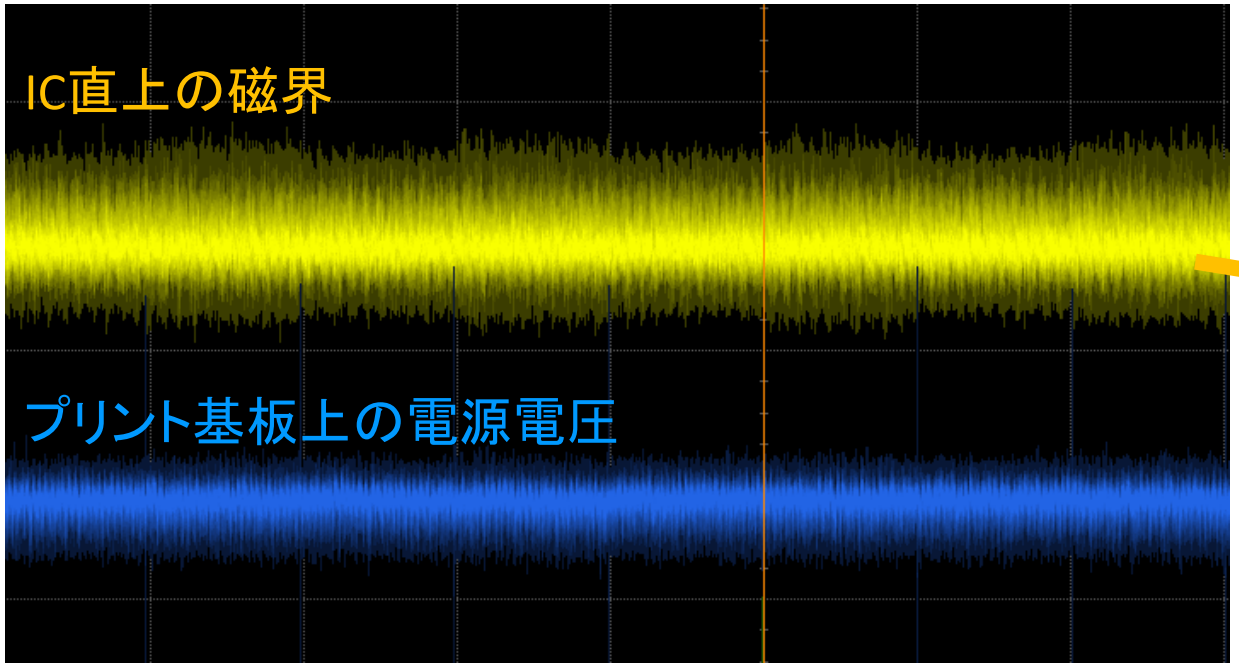
ArmFrogs-ALICE@ゴフェルテック

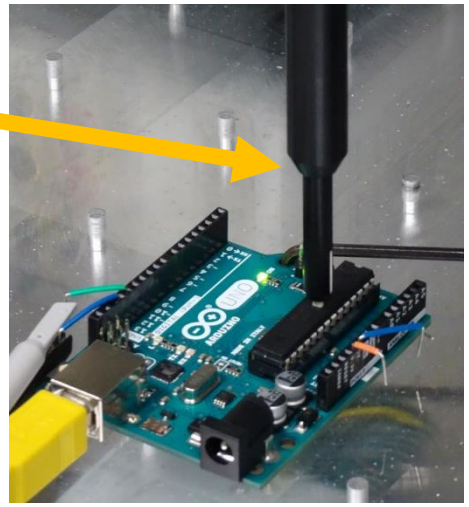
サイドチャネル攻撃の例

Arduino Uno

- ✓ 8-bit microcontroller
- ✓ 16 MHz clock

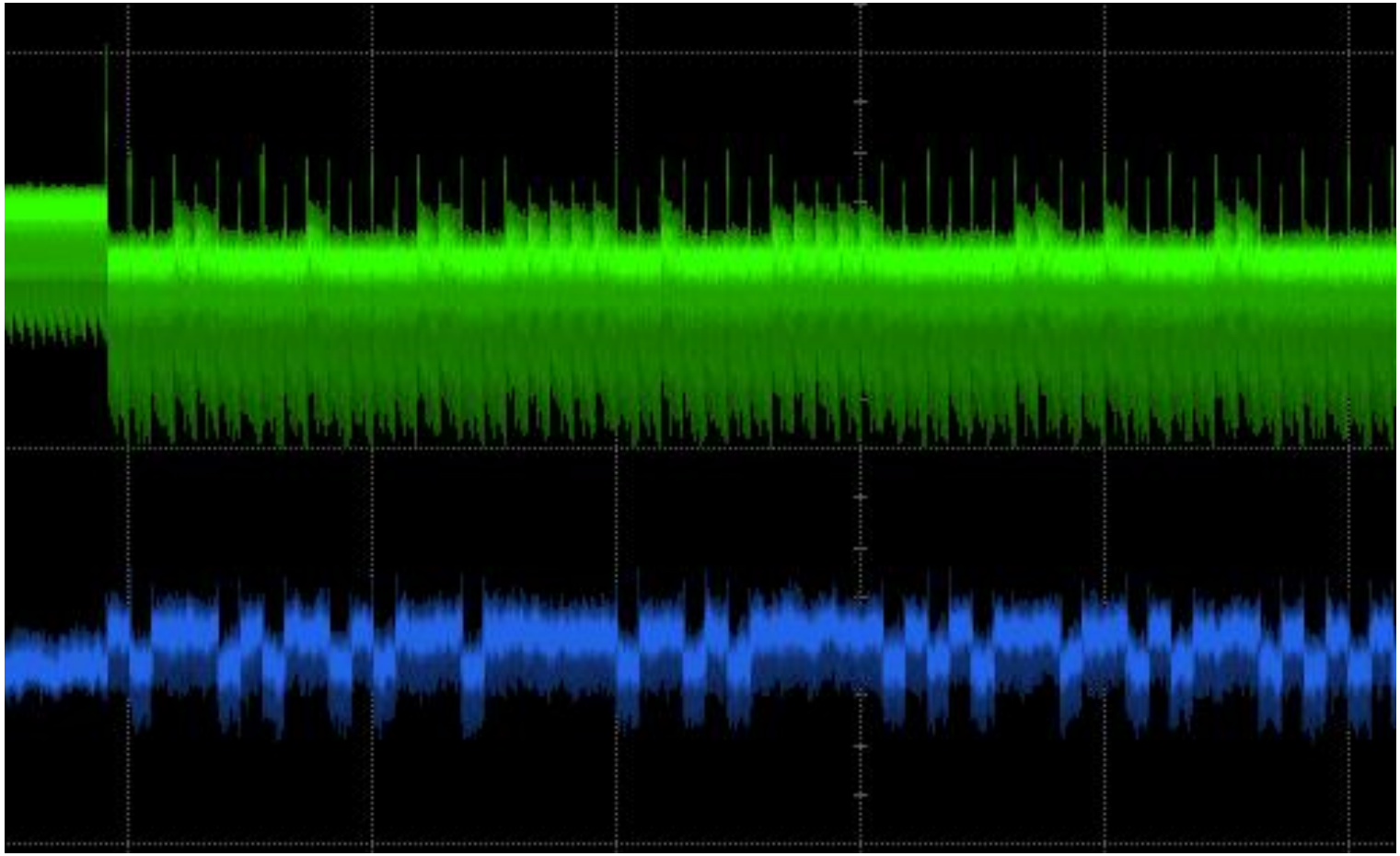




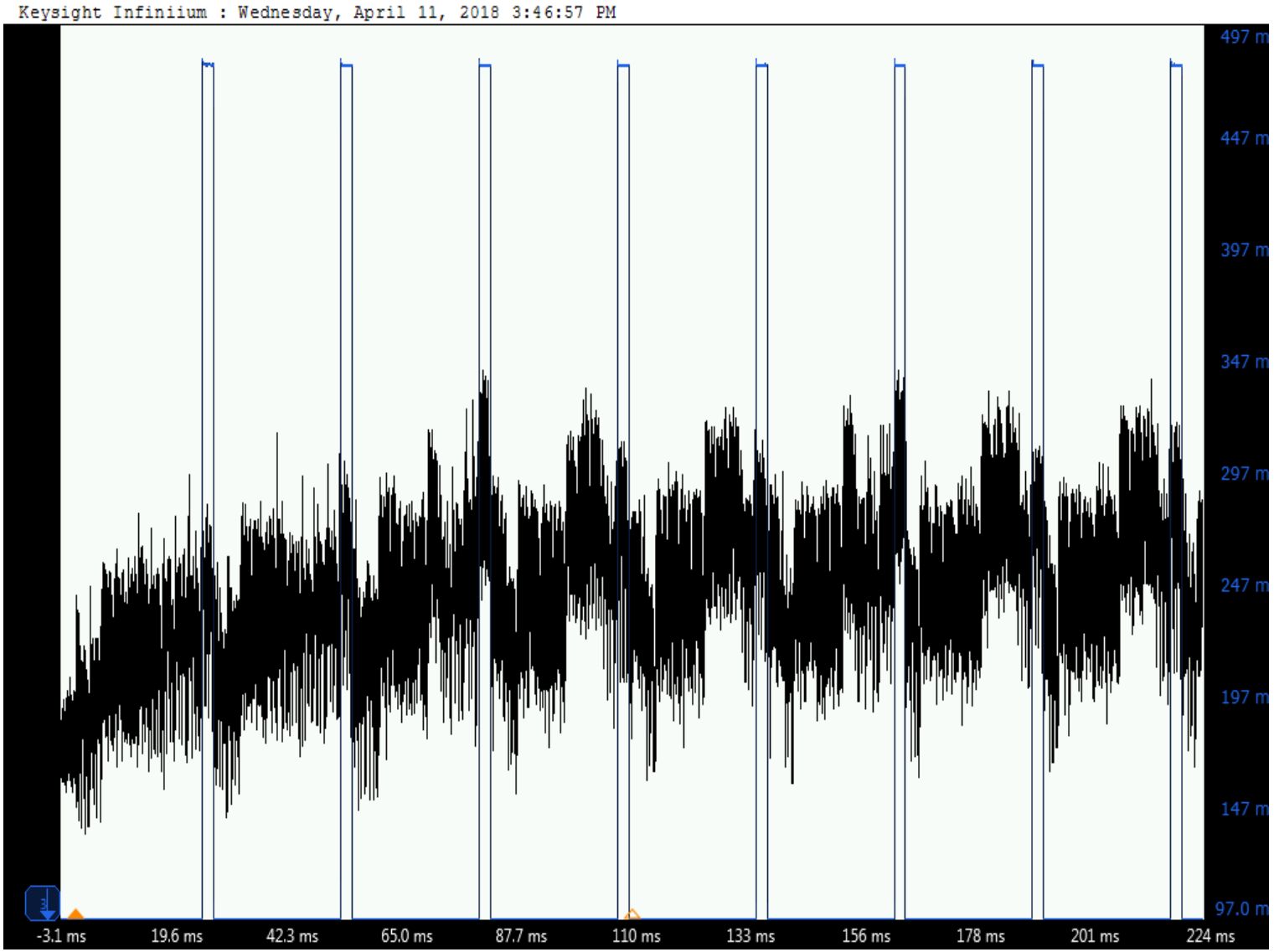


プリント基板への漏えいは小さいが、IC近傍磁界には漏洩

観測されるサイドチャネル波形（ダメな例）



計算処理の内容によって振幅に判別可能な差異が発生


Keysight Infiniium : Wednesday, April 11, 2018 3:46:57 PM
497 m
447 m
397 m
347 m
297 m
247 m
197 m
147 m
97.0 m
-3.1 ms
19.6 ms
42.3 ms
65.0 ms
87.7 ms
110 ms
133 ms
156 ms
178 ms
201 ms
224 ms

RSA暗号の限界

計算機性能の向上

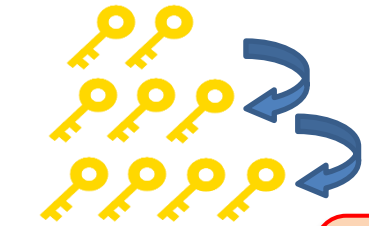
↓

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

Arduino上での楕円曲線暗号の実装

Arduino uno

Arduino uno 上で暗号化・デバイス認証処理を行い

実際のIoTデバイス環境でのセキュリティ評価

楕円スカラ倍算
　楕円曲線上の有理点に対する演算
　アフィン座標、射影座標、ヤコビアン座標に対応

モンゴメリラダー
　アルゴリズム対象化によるサイドチャネル攻撃(SCA)対策

セキュアで高速かつスケーラブルな楕円曲線暗号の実現

以上をまとめて

IoT時代にまさに必要な機能

新技術説明会
New Technology Presentation Meetings!

岡山大学
OKAYAMA UNIV.

① セキュリティ強度を自在に調整でき ← 他に類を見ない

② プロトコルにおけるデータ送受信量を削減でき ← 半減できます

③ 計算実装がコンパクトで ← 楕円曲線暗号・マイコン実装も可能

④ 処理速度が高速である ← 世界最高速ライブラリELiPS

⑤ データ暗号化＋機器認証できる ← 公開鍵暗号である

⑥ 多要素認証も実現できる ← 独自シナリオをもっています

⑦ サイドチャネル攻撃耐性をもつ ← 持っています・対策しています

開発ライブラリの特徴（１）

- 3つの整数パラメータ*p,m,h*を使う
  - 通常は、*p,m*のみ
  - *h*が追加されている
- 暗号強度が*m* log *p*で可変である
  - 通常、これを行うのはソフト・ハードの変更が必要
  - *h*の追加により問題解消（特許１）
  - 高速かつコンパクト、 無限にスケーラブル（類を見ない特長）

- 一部のパラメータでは世界最高速を実現
- *0*～*p-1*までの数字だけが表れる*m*次元ベクトル空間における
  - ベクトル乗算を行うアルゴリズム（CVMA）

開発ライブラリの特徴（２）

- CVMAを用いる暗号系すべてにその特長が波及
  - 楕円曲線暗号にも適用できる
    - 高速・コンパクト・スケーラブル
- 暗号データの圧縮を実現
  - サイズを約半分にする技術を開発（特許２）
  - データ格納効率の向上（例：ブロックチェーン技術）

- ターゲット（IoTセキュリティの高度化・高機能化）
  - 各種の通信デバイス＋マイコン：Sigfox＋Arduinoなど
  - 各種のストレージシステム：ブロックチェーン＋PCなど

まとめ

- Arduino UNOなど8ビットマイコンにも実装できる
  - HWにおける機器認証などへの応用も
  - ラズベリーパイなどと連携させた高機能システムへ
  - ブロックチェーン技術などとの相性も良い
- IoTのセキュリティ実装に関してぜひご相談ください

ご清聴ありがとうございました

お問い合わせ先

岡山大学　研究推進機構
産学連携・知的財産本部
知的財産プロデューサー　平野　芳彦

ＴＥＬ 086-251-8476
ＦＡＸ 086-251-8961
e-mail chizai@okayama-u.ac.jp