

Society5.0に向けた セキュアなIoT・AIの活用

岡山大学
大学院自然科学研究科
セキュリティ研究グループ
おかやまIoT・AI・セキュリティ講座

教授 野上 保之



岡山大学
OKAYAMA UNIV.

自己紹介：野上保之（48歳） 群馬県草津温泉の出身
信州大学で博士（工学）を取得 ← 師匠は杉村先生

有限体を中心とした研究を進めてきて、1994～

それがセキュリティ・とくに楕円曲線暗号になり、2000～

それが擬似乱数やサイドチャネル攻撃の研究も加わり、2008～

もはやIoTもAIも駆使して、色んなことを進めています。2017～

1. コロナ禍の中で作ったものとIoTセキュリティ **雑感**

話題 1：具体的に必要なセキュリティ要素とその実現方法

話題 2：IoT周辺の認証技術

2. 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）

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



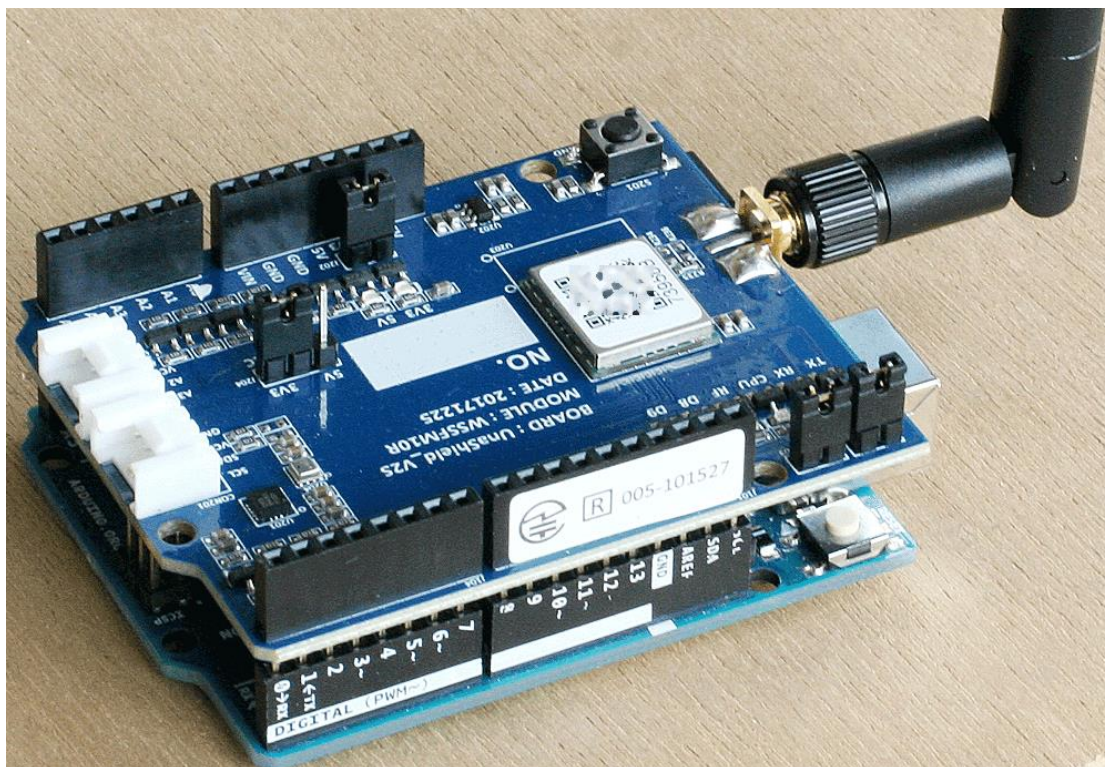
岡山大学
OKAYAMA UNIV.

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。
オプションであったりする。

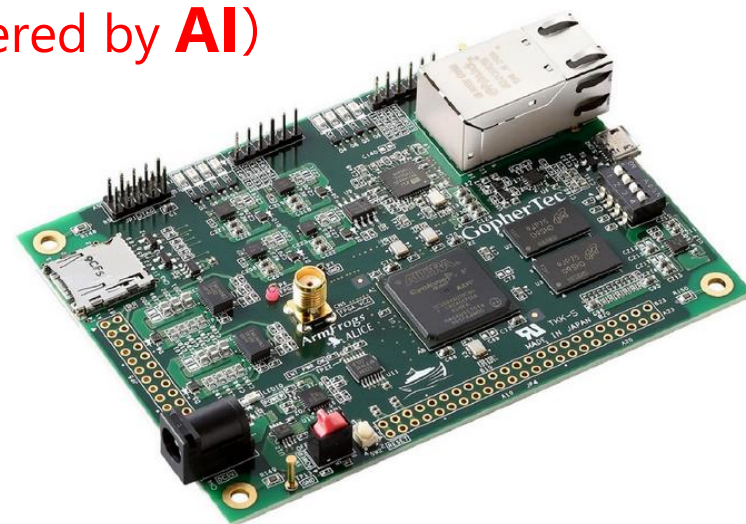
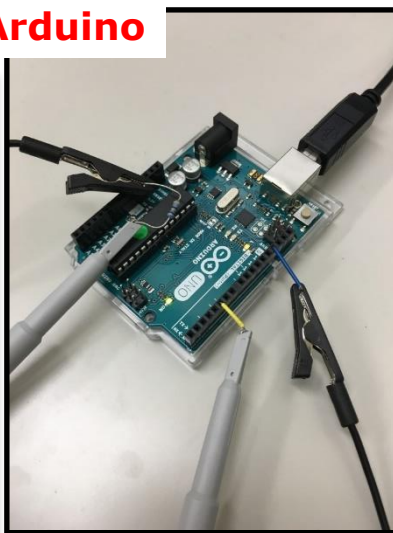
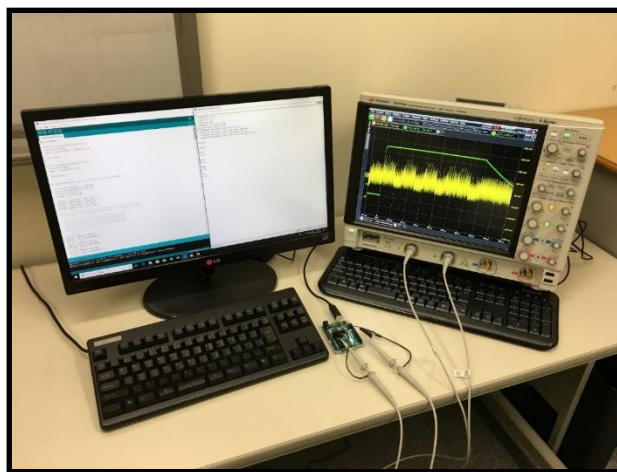
実際どこに注意が必要か

- 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・**アプリ連携**
 - 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

- 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

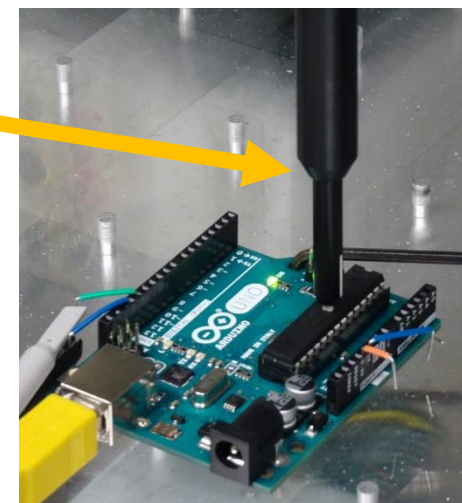
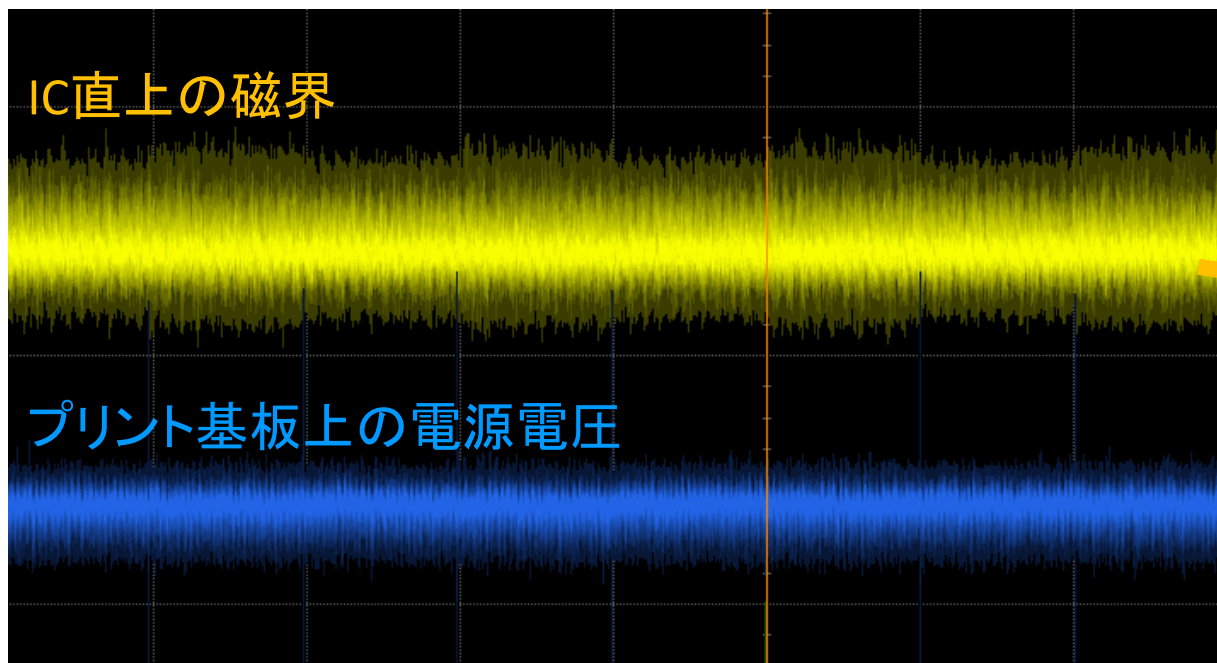
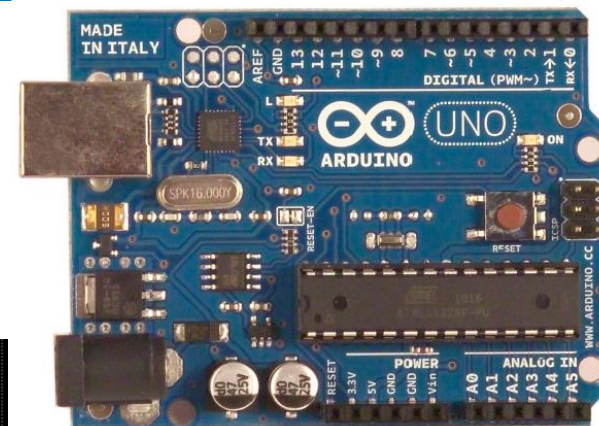
サイドチャネル攻撃の例



岡山大学
OKAYAMA UNIV.

Arduino Uno

- ✓ 8-bit microcontroller
- ✓ 16 MHz clock

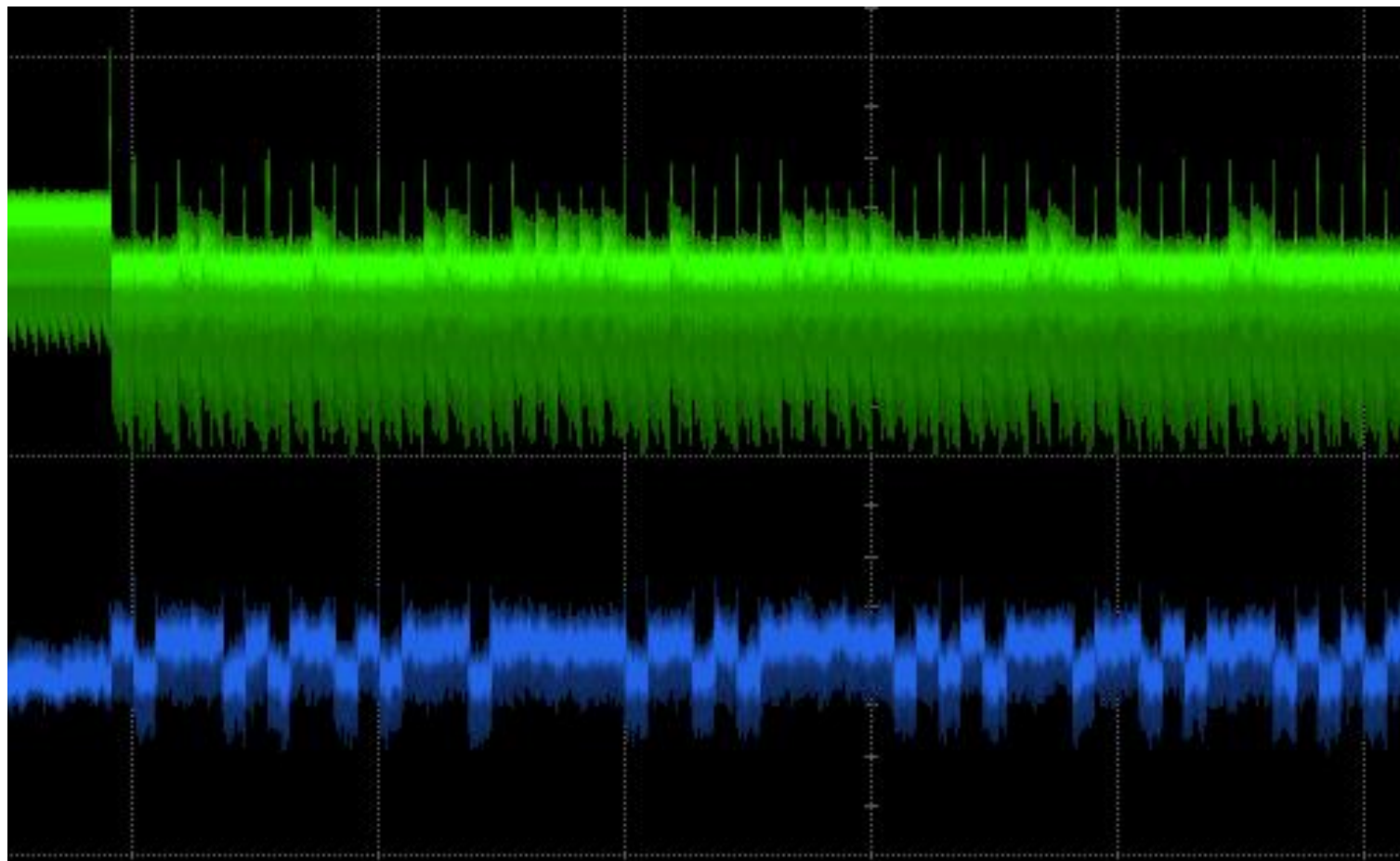


プリント基板への漏えいは小さいが、IC近傍磁界には漏洩

観測されるサイドチャネル波形 (ダメな例)



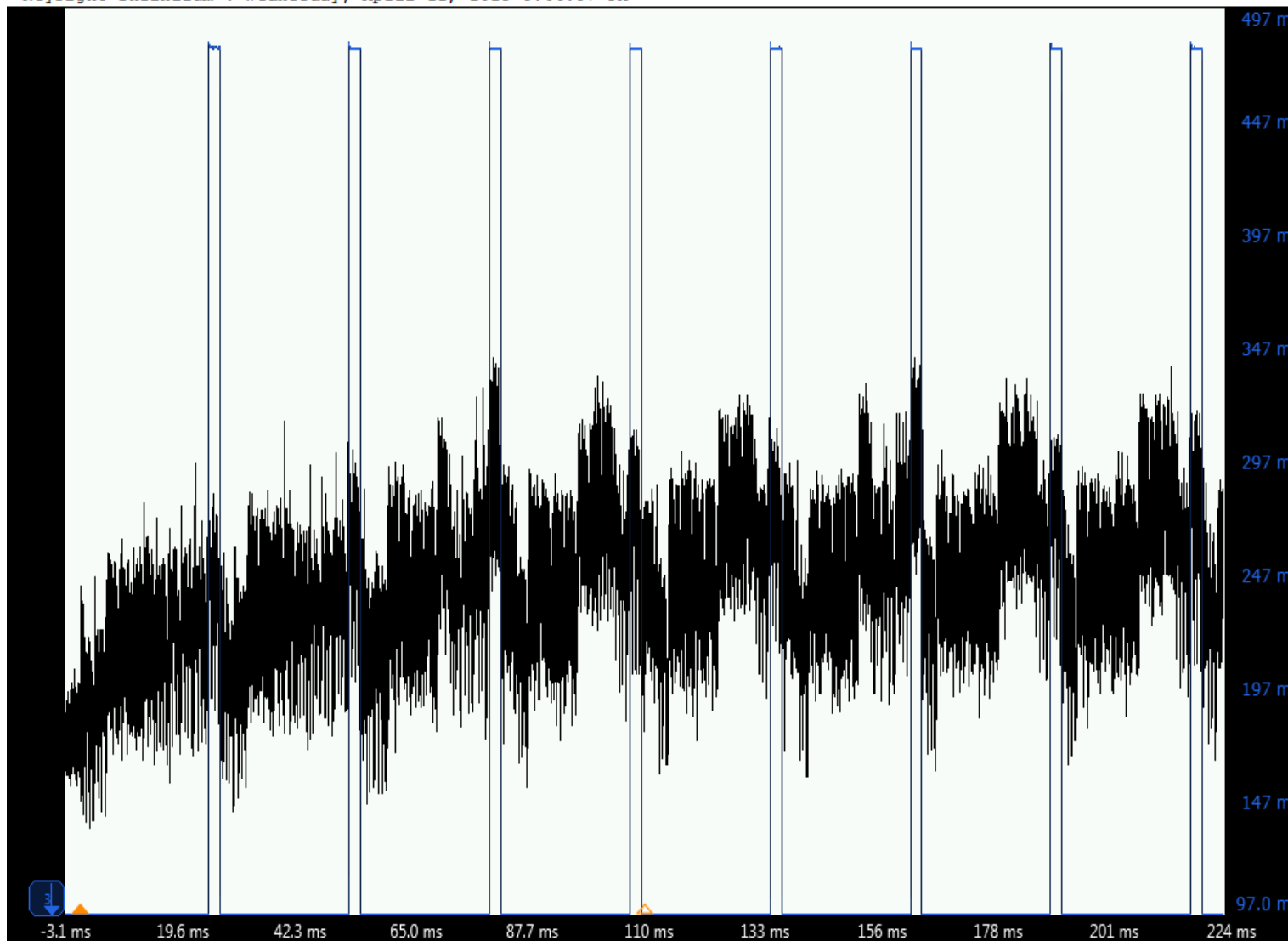
岡山大学
OKAYAMA UNIV.



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



機械学習で解析

あるオシロでは

RSA暗号の限界

計算機性能の向上

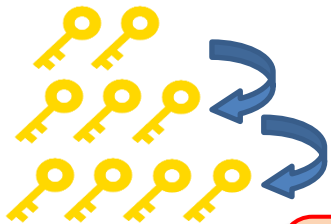


解読リスク増加に伴う
鍵長の変更

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



■IoTセキュリティはたいへんだ

12. IoTのセキュリティ対策の必要性

IoT 特有の性質とリスクを踏まえたセキュリティ対策を行うことが必要。

IoT特有の性質

- 1 脅威の影響範囲・影響度合いが大きいこと
- 2 IoT 機器のライフサイクルが長いこと
- 3 IoT 機器に対する監視が行き届きにくいこと
- 4 IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であること
- 5 IoT 機器の機能・性能が限られていること
- 6 開発者が想定していなかった接続が行われる可能性があること

出典：「IoTセキュリティガイドライン ver 1.0」総務省・経済産業省・IoT推進コンソーシアム

総務省：「IoT機器等の電波利用システムの適正利用のためのICT人材育成事業」より



岡山大学
OKAYAMA UNIV.

【第2章】IoTの技術・関連法制度 もっと知りたいIoT ～IoTの技術を知ろう～

13. IoTのセキュリティ対策

IoTセキュリティ対策の5つの指針

指針
1

IoT の性質を考慮した基本方針を定める

指針
2

IoTのリスクを認識する

指針
3

守るべきものを守る設計を考える

指針
4

ネットワーク上での対策を考える

指針
5

安全安心な状態を維持し、情報発信・共有を行う

出典：「IoTセキュリティガイドライン ver 1.0」総務省・経済産業省・IoT推進コンソーシアム

総務省：「IoT機器等の電波利用システムの適正利用のためのICT人材育成事業」より



岡山大学
OKAYAMA UNIV.

セキュリティ対策指針一覧

大項目	指針		要点	具体例
方針	指針 1	IoTの性質を考慮した基本方針を定める	要点 1. 経営者がIoTセキュリティにコミットする	経営者は、企業の存続にかかわる重要問題と捉え、IoTセキュリティの基本方針を決め、状況把握やその体制作りを主導します。
			要点 2. 内部不正やミスに備える	
分析	指針 2	IoTのリスクを認識する	要点 3. 守るべきものを特定する	対策レベルの低い機器があると、つながって連携している他の機器にも悪影響を及ぼし、全体に危険を招きうる事を想定します。
			要点 4. つながることによるリスクを想定する	
			要点 5. つながりで波及するリスクを想定する	
			要点 6. 物理的なリスクを認識する	
			要点 7. 過去の事例に学ぶ	
設計	指針 3	守るべきものを守る設計を考える	要点 8. 個々でも全体でも守れる設計をする	つながる機器やシステムは、単独での問題が無くとも、IoT機器との接続の組み合わせ等でリスクとなる可能性を含め、設計の検証・評価を実施します。
			要点 9. つながる相手に迷惑をかけない設計をする	
			要点 10. 安全安心を実現する設計の整合性をとる	
			要点 11. 不特定の相手とつながられて安全安心を確保できる設計をする	
構築・接続	指針 4	ネットワーク上での対策を考える	要点 12. 安全安心を実現する設計の検証・評価を行う	各IoT機器の性能、ネットワーク接続方法等から検討し、ネットワーク接続された全体のシステムとしてのセキュリティ確保をします。
			要点 13. 機器等がどのような状態かを把握し、記録する機能を設ける	
			要点 14. 機能及び用途に応じて適切にネットワーク接続する	
			要点 15. 初期設定に留意する	
運用・保守	指針 5	安全安心な状態を維持し、情報発信・共有を行う	要点 16. 認証機能を導入する	IoTは万一の事故の際には、機器メーカー、システム・サービス提供者からエンドユーザーと広範囲に影響を及ぼすため、予め各々の役割分担を協議し、決めておきます。
			要点 17. 出荷・リリース後も安全安心な状態を維持する	
			要点 18. 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える	
			要点 19. つながることによるリスクを一般利用者に知ってもらう	
			要点 20. IoTシステム・サービスにおける関係者の役割を認識する	
			要点 21. 脆弱な機器を把握し、適切に注意喚起を行う	

認証技術～需要面～



岡山大学
OKAYAMA UNIV.

- スマートロック：自動車も、玄関も
- Hardware Wallet：お金も
- HTTPS、WSS（WebSocket）：サーバ・クライアント認証

- 機器・ユーザ・接続認証：
- Message認証：LPWAで紹介した
- サービス間・API間認証：認証トークン

認証技術～テクニカル面～



岡山大学
OKAYAMA UNIV.

- Basic認証 : ID、PW
- Hash、OTP、CounterMode
- 公開鍵認証 : RSA、ECC
- 二要素認証
- FIDO : バイオメトリクス
- 認証トークン : USBキー (物理) 、 Authenticator (ソフト) 、 SMS
- BlueToothなど近接認証
- AI認証 : 動作、パターン
- Oauth、OpenID : Webアプリ間のアクセストークン、JWT
- セッション・クッキー
- MAC : CMAC、HMAC
- VPN : トンネリング・暗号化

IoTに対して何が可能で現実的か : 必要性、GWなど構成、追加暗号化など

暗号技術について Cryptorec



岡山大学
OKAYAMA UNIV.

電子政府における調達のために参照すべき暗号のリスト (CRYPTREC暗号リスト)

平成25年3月1日
総務省
経済産業省

電子政府推奨暗号リスト

暗号技術検討会¹及び関連委員会(以下、「CRYPTREC」という。)により安全性及び実装性能が確認された暗号技術²について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS ^(注1)
		RSASSA-PKCS1~v1_5 ^(注1)
	守秘	RSA-OAEP ^(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64 ビットブロック暗号 ^(注2)	該当なし
	128 ビットブロック暗号	AES
	ストリーム暗号	Camellia
		KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用 モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード ^(注13)	CCM
		GCM ^(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS ^(注1)
		RSASSA-PKCS1-v1_5 ^(注1)
	守秘	RSA-OAEP ^(注1)
	鍵共有	DH
共通鍵暗号	64 ビットブロック暗号 ^(注2)	ECDH
		該当なし
	128 ビットブロック暗号	AES
	ストリーム暗号	Camellia
ハッシュ関数		KCipher-2
		SHA-256
		SHA-384
		SHA-512

<https://safecurves.cr.yyp.to/>

		Parameters:			ECDLP security:				ECC security:			
Curve	Safe?	field	equation	base	rho	transfer	disc	rigid	ladder	twist	complete	ind
Anomalous	False	True✓	True✓	True✓	True✓	False	False	True✓	False	False	False	False
M-221	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
E-222	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
NIST P-224	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False	False
Curve1174	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Curve25519	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
BN(2,254)	False	True✓	True✓	True✓	True✓	False	False	True✓	False	False	False	False
brainpoolP256t1	False	True✓	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False
ANSSI FRP256v1	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False	False
NIST P-256	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	True✓	False	False
secp256k1	False	True✓	True✓	True✓	True✓	True✓	False	True✓	False	True✓	False	False
E-382	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
M-383	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Curve383187	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
brainpoolP384t1	False	True✓	True✓	True✓	True✓	True✓	True✓	True✓	False	True✓	False	False
NIST P-384	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	True✓	False	False
Curve41417	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Ed448-Goldilocks	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
M-511	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
E-521	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓

ある曲線への攻撃では、
WRを達成した

私の研究室では IoT時代に必要な機能を実現する研究



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をgithubで公開中
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 (素数) , m (次元数) , h (可変パラメータ) 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
- $0 \sim p-1$ 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

- 以下の話題についてセキュリティ雑感を述べさせていただきました

話題 1 : 具体的に必要なセキュリティ要素とその実現方法

話題 2 : IoT周辺の認証技術

- ご清聴ありがとうございました