自動車技術会　サイバーセキュリティ講座専門プログラム

1. 講座名	AES暗号実装と消費電力を用いたサイドチャネル攻撃
2. 講座概要	AES暗号は車載ネットワークにおけるMAC認証やECUマイコンのセキュアブートなどに使われており，暗号鍵が攻撃者に知られないようにするため，セキュアなメモリに格納したり隔離実行環境で暗号演算をおこなうことが必要です．しかしながら，これらの対策を行ったとしても，暗号演算時の消費電力波形を用いて暗号鍵を取得するというサイドチャネル攻撃により暗号鍵を取得することが可能です．本講義では，まず最初に，AES暗号の処理手順を説明するだけではなく，使われているガロア体の計算方法を暗号の数学的なバックグラウンドのない方にも理解できるように説明します．その後，LSIの内部動作に知識のない方にも理解できるよう消費電力をもちいたサイドチャネル攻撃の原理を説明し，最後に，取得済の消費電力波形を用いて，どのようにして暗号鍵を取得することができるのかを体験していただきます．
3. 想定する受講者	自動車業界の技術者を想定していますが特に制限はありません
4. 習得する技術	・AES暗号処理で行われている演算の理解 ・消費電力を用いたサイドチャネル攻撃攻撃技術
5. 受講の前提条件	・自動車サイバーセキュリティ講座の「サイバーフィジカルセキュリティ技術-基礎・暗号・計測セキュリティ-」を受講していることが望ましい． ・ガロア体の演算の理解演習とサイドチャネル攻撃の体験においてPythonを使用するのでプログラミングの経験があることが望ましい．
6. 日数（時間数）	1日(計6時間)
7. 最大受講人数	30名
8. セミナー講師	立命館大学　藤野　毅
9. 受講者の制限	特になし
10. 実習機材	Pythonを実行できる環境（Anacona上のJupyter Notebookが望ましい）をPC上にインストールしておいてください．ただし，演習や体験が必要でない場合は，環境を用意せずに受講していただいても差し替えありません．
11. 到達目標	代表的な対称鍵暗号であるAES暗号の基本的な演算処理内容を含めて理解する．さらに，消費電力を用いたサイドチャネル攻撃を用いることで暗号鍵を取得できるという脅威を体験し，対策の必要性を理解する．
12. 講座計画	(1)イントロダクション（AES暗号の車載応用） (2)多項式上の剰余演算を用いるガロア体の計算手法とAES暗号の基礎 (3)AES暗号回路のソフトウェア実装とサイドチャネル攻撃の原理 (4)消費電力を用いたサイドチャネル攻撃の体験（取得済の消費電力波形から暗号鍵を特定する） (5)関連話題提供（公開鍵暗号RSAにおけるサイドチャネル攻撃・深層学習を用いたサイドチャネル攻撃etc.）