第5回自動車サイバーセキュリティ講座　専門プログラム⑥

1. 講座名	AES暗号実装と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います．このAES暗号技術について，単に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．また，半導体の回路実装経験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，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． ・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くこと
11. 到達目標	代表的な対称鍵暗号であるAES暗号の処理内容をガロア体の理論を含めて理解し，発展的な内容として，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)ガロア体の計算とAES暗号の基礎 (3)AES暗号回路のハード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（取得済の波形から暗号鍵を特定する） (5)関連話題提供（深層学習を用いたサイドチャネル攻撃，PUFなど）