研究成果展開事業　研究成果最適展開支援プログラム
シーズ育成タイプ　事後評価報告書

研究開発課題名	：	耐タンパセキュリティハードウエアの車載システムへの応用
プロジェクトリーダー 所　属　機　関	：	パナソニックセミコンダクターソリューションズ株式会社
研　究　責　任　者	：	藤野毅（立命館大学）

1. 研究開発の目的

LSI 動作時に発生する電力や電磁波から秘密情報を解析するサイドチャネル攻撃が脅威となっている。一方、最近の自動車では、ECU(Electronic Control Unit)を用いた、ブレーキやアクセルなどの運転支援システムが実用化されており、上記攻撃に対しては、ハードウェア面でのセキュリティ対策が重要課題として取り上げられている。本開発では、サイドチャネル対策を施した暗号回路に物理複製不可能デバイス PUF(Physical Unclonable Function)を付加する高セキュアな車載向け耐タンパ LSI の試作/評価を行うと共に、試作した LSI をセキュア車載システムに搭載し、実用性検証を行うことで、車載 ECU としての LSI 設計技術を確立する。

2. 研究開発の概要

耐タンパ AES 暗号と PUF を統合したセキュリティ実証 LSI を設計、試作及び、評価を行い、サイドチャネル攻撃に対する耐タンパ性評価と固有デバイスの認証鍵の要件を満たす PUF 性能を確認した。最終的には、試作した LSI を組み込んだセキュア車載デモシステムを構築し、実用面での動作を実証した。

①成果

研究開発目標	達成度
① MDR-ROM を用いた耐タンパ AES 暗号回路と PUF を統合したセキュリティ実証 LSI の試作と評価を行い、耐タンパ性(100 万波形を用いても攻撃可能な鍵は 1 バイト以下)と、PUF のデバイス固有の認証鍵応用として実現可能な性能を確認する。	① 試作した LSI を用いて MDR-ROM 搭載の AES 暗号回路に対し、サイドチャネル攻撃(電力解析攻撃と電磁界解析攻撃)を実施し、100 万波形を用いても1バイトの鍵も窃取出来ないことを確認した。 また、2 種類の PUF(MDR-ROM、ReRAM)の性能評価では、ユニーク性(ハミング距：0.48-0.52)と再現性(電源変動：±10%、動作温度：-40～105℃)を達成し、車載環境でデバイス固有の認証鍵が安定的に生成できることを実証した。(達成度 100%)
② 車載セキュリティアプリケーションを実行するためのプロセッサおよび、車載通信(CAN)モジュールを搭載した FPGA ボードを試作し、車載アプリケーションを実行するためのハードウェアを完成させる。	② 業界標準である AUTOSAR 仕様に基づく Truncated MAC 付きのセキュア CAN 通信の実現と、セキュアな ECU リプログラミングを実現するためのハードウェア環境を構築した。(達成度 100%)

③ オペレーティングシステムを搭載し、CAN 通信の暗号化や ECU リプログラミングなどの車載セキュリティデモンストレーションを行う。	③ 業界標準である AUTOSAR 仕様に基づく Truncated MAC 付きのセキュア CAN 通信の実装と、PUF 技術を用いたファームウェア改竄防止を実現した ECU リプログラミングの実装を行い、車載セキュリティのデモを実施した。(達成度 100%)
④ ECU のサイドチャネル攻撃耐性を、CAN バスの通信プロトコルを用いて評価するシステムで、暗号化タイミングを ECU から出力しなくてもサイドチャネル攻撃可能な環境を構築する。	④ AUTOSAR 仕様に基づいた Truncated MAC 付き CAN 通信上に流れるメッセージの解析と、LSI の漏洩電磁波の観測により、MAC 認証に用いる認証鍵をサイドチャネル攻撃で窃取できる環境を構築し、組込総合技術展でデモ展示を行った。

②今後の展開

本研究で開発したデモシステムによって車載ネットワークへの攻撃で秘密情報が盗窃できることを示し、業界に対して耐タンパハードウェアの重要性を訴求することができた。そして PUF 技術についても車載環境にも適用できる性能を示した。今後、事業化に向けてサプライチェーンを含めた既存システムとの親和性を鑑みて業界標準化を睨みつつ検討を継続するとともに、車載製品だけにとらわれず IoT 全体をみた幅広い応用製品を模索する。

3. 総合所見

目標を達成し、次の研究開発フェーズに進むための成果が得られた。イノベーション創出が期待できる。大学における CREST などの技術成果である PUF とサイドチャネル攻撃対策の評価技術、企業における LSI の信頼性評価技術の連携により、ReRAM の PUF について企業化が期待できる。車載ビジネスへの適用は、国際標準化がキーとなるので、この先も大学と連携して標準化への技術誘導などを期待する。