［DAS 招待講演］

耐タンパセキュリティハードウエアの開発と車載システムへの応用

藤野 毅
立命館大学

概要：
暗号回路を搭載した LSI は、クレジットカードや交通系非接触カードなどにおける利用者認証などの用途で広く使用されている。認証の安全性は、LSI の中に格納された秘密鍵が第３者に知られないことを前提にしている。一方、秘密鍵を窃取したい悪意ある攻撃者の手法は、暗号回路の動作を用いて鍵を窃取する方法と、鍵を格納しているメモリから窃取する方法の２種類に分類できる。前者に属する強力な攻撃としては、暗号回路が動作しているときの消費電力や電磁波等のサイドチャネル情報を利用する手法がある。本手法は、一般的な実験装置であるオシロスコープとＰＣを用いれば、暗号回路を数分動作させるだけで鍵を窃取できる強力な攻撃手法であり、サイドチャネル情報をリークさせない暗号回路の設計技術が必須となっている。後者では、秘密鍵の複製を防止する対策手法として、複製不可能デバイス（PUF: Physical Unclonable Function）を用いる手法がある。PUF を用いると、LSI 製造時のトランジスタなどの性能ばらつきを用いて、固体固有の ID を生成することが可能であり、かつこの ID は複製不可能であるという特徴を持つ。本 ID を用いて秘密鍵を暗号化した状態でメモリに保管することにより、攻撃者にメモリ内容を不正に読み出されたとしても、秘密鍵情報を取得できないようにすることができる。講演では、サイドチャネル攻撃を防止できる耐タンパ共通鍵暗号回路の設計技術と PUF を用いた暗号鍵の安全な格納技術に関して解説する。さらに、これらを用いた車載システムへの応用として、PUF を用いたキーレスエントリシステムについて紹介する。