修士学位論文要約（令和３年３月）

車載向けセキュア通信プロトコルに対するサイドチャネル解析に関する研究

永戸 謙成
指導教員：本間 尚文

A Study on Side Channel Analysis for In-Vehicle Secure Communication Protocols

Kensei NAGATO
Supervisor: Naofumi HOMMA

This paper presents a side-channel analysis (SCA) on a message authentication code (MAC) used in controller area network (CAN). SecOC (secure onboard communication) given by AUTOSAR (automotive open system architecture) employs CMAC with AES (AES-CMAC). The conventional SCA for the first-round of AES is not applicable to the AES-CMAC because an attacker cannot know the input to AES and the payload is only given by eight bytes. In addition, the conventional SCA is also difficult in the case that an output tag is truncated to two bytes. In contrast, the proposed SCA focuses on the second and third rounds in addition to the first round. The proposed SCA identifies intermediate values which depend on the payload, and estimates the payload-dependent values with a first-order SCA in a continuous manner. In this paper, we demonstrate the feasibility of the proposed SCA through an experiment with PASTA (Portable Automotive Security Testbed with Adaptability). The result shows that the proposed SCA can retrieve the entire secret key from all the versions of SecOC (SecOC_00192/00193/00194).

1. はじめに

近年、車を対象としたハッキング事例 [1)]が増加しており、その対策として自動車業界団体AUTOSAR(AUTomotive Open System ARchitecture)によって、暗号技術の導入が進められている。その一つである、安全な車載通信についての規格SecOC(Secure Onboard Communication)では通信へメッセージ認証符号(MAC)を導入することが規定されている。MAC を導入することで、偽装メッセージやメッセージの改ざんを防止可能であることが数学的に証明されている。一方で、暗号実装に対して、物理攻撃の脅威があることが知られている。特に、暗号演算中の副次的に発生する物理量を利用するサイドチャネル解析は現実な脅威となりうる。車載ネットワークへの暗号技術の導入に伴い、早急にそのサイドチャネル解析への安全性評価を行う必要がある。

本稿では、以上の背景から、車載認証暗号に対するサイドチャネル解析手法の提案と評価を行う。具体的には、SecOC 規格に準拠した国際標準暗号AES(Advenced Encrypt Standard)を使用したAES-CMAC(Cipher-based MAC)を対象としたサイドチャネル解析手法の提案を行う。また、自動車向けセキュリティ評価プラットフォーム PASTA(Portable Automotive Security Testbed with Adaptability) [2)]を用いた実験により提案手法の有効性を示す。

2. AES-CMAC へのサイドチャネル解析

本稿では、車載ネットワークプロトコル CAN (Control Area Network)で利用される AES-CMAC を解析の対象としている。CAN の特徴はバス型のネットワークを形成しており、ブロードキャスト通信をしていること、パケットのペイロードが 8 バイトであることがあげられる。AES-CMAC を含む認証暗号では、送信者が共有する鍵と呼ばれる秘密情報を用いて送受信者に改ざんがなかったものとして受け取らせることができる。すなわち、認証暗号の改ざん検知機構は鍵の秘密性に基づく。

AES-CMAC を対象とした解析の基礎となる、AES を対象とした解析 [3)]は、暗号演算への入力もしくは出力と暗号演算中の消費電力を計測することで。秘密情報である鍵を求める。同解析では、まず暗号モジュールに対して複数の既知情報を入力し、その時の消費電力を計測する、次に、測定した入力情報と鍵の予想値をもちいて SubBytes 処理時の中間値を求める。消費電力は演算結果の HW と相関があると仮定し求めた中間値の HW を取ることで消費電力モデルを作成する。最後に消費電力モデルと消費電力間の相関を取り、最も高い相関を示した鍵を正解鍵とすることで鍵を求める。上記の解析のように AES への入力もしくは出力が観測可能な場合は相関電力解析により鍵の取得が可能であることが知られている。

しかし、本稿で対象とする CAN 上の AES-CMAC では、AES への入力や出力のすべてを知ることが困難であり、解析の脅威が明らかではなかった。

3. 提案するサイドチャネル解析手法

AES への入力は 16 バイトで固定されている。それに対して、CAN のペイロードは 8 バイトしかないため、攻撃者が観測可能な情報は 8 バイトしかない。また、CMAC のパディング処理や CMAC の鍵加算により攻撃者は AES への入力を知ることができない。したがって従来の手法を適応することは困難である。提案手法では。AES の第 1-3 ラウンドの SubBytes 処理を対象とした相関電磁波解析を逐次的に行い、中間値を推定し、最終的に第3ラウンドのラウンド鍵を取得する。ラウンド鍵は鍵の逆スケジューリングにより秘密鍵に戻すことが可能であることから結果、秘密鍵の推定が可能となる。基本的なアイデアは、AES 計算における中間値を観測のたびに固定された情報(定数)と観測のたびに変化する情報（変数)に分離し、相関解析を行うことで定数部分を推定する。既存手法では、固定された情報が鍵、変化する情報が平文となるため1ラウンドの SubBytes を対象とした解析により鍵の推定が可能となるが、CMAC を推定した解析の場合固定された情報は鍵そのものとはならない。相関解析により推定した中間値をもとに AES の ShiftRows と MixColmuns を行い次のラウンドの入力を求める。この操作を繰り返し行うことで第3ラウンドへの入力がすべてわかる状態になる。したがって、第 3 ラウンドを対象とした相関電磁波解析解析を行うことでラウンド鍵を取得することが可能となる。

また、SecOC では MAC への入力にカウンタを用いる規格がある。この場合、カウンタ値は攻撃者が知ることのできないうえに観測のたびに変化する。そのため、固定値と既知の変数に分けるという提案手法を利用することができない。そこで、Jaffe らが提案した AES カウンタモード(AES-CTR)に対する解析手法 [3] を組み合わせることで入力にカウンタを用いた場合の MAC についても解析可能となる。具体的には、1 ラウンド目の解析でカウンタ部の初期値と秘密鍵などが入った未知の固定値の組み合わせを推定する問題を追加で解くことで解析を行うことが可能となる。

4. 評価実験

CMAC 演算に対して提案手法を用いることにより、鍵(第3ラウンド鍵)が取得できることが可能となることを確認するため、実機を用いた検証を行た。実験には AES-CMAC 実装のされた ECU を用いて行った。実験では MCU の直上で電磁波の計測を行った(図 2)。図 2 は、縦軸を相関値、横軸を計測時間とする。

図 2 より、第 3 ラウンドの解析において正解の鍵値で高い相関を示すことがわかる。第 3 ラウンドを対象とした解析には第 1、2 ラウンドの解析結果を用いて

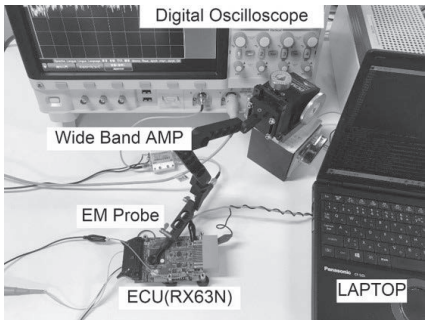

図 1　実験セットアップ

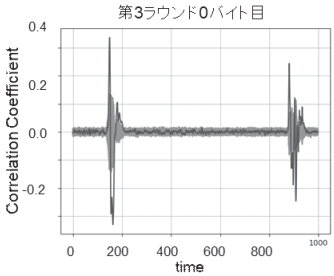

図 1　実験セットアップ

いる。したがって、第 1-3 ラウンドに渡った解析を行うことにより鍵の情報が取得可能であることがわかる。

5. まとめ

本稿では、SecOC で規定された AES-CMAC 実装に対するサイドチャネル解析手法に対するサイドチャネル解析手法を提案し、自動車向けセキュリティ評価プラットフォームを用いた実機検証とシミュレーションにより SecOC で規定されたすべての MAC について解析手法が有効であることを示した。今後の課題は、提案手法への対策手法の考察や解析シナリオに従った通信路上のサイドチャネル情報を利用した解析可能性の検討である。

文献

1) C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehi- cle,” Black Hat USA, vol.2015, p.91, 2015.
2) T.Toyama,T.Yoshida,H.Oguma,andT.Matsumoto,“ PASTA:PortableAuto-motiveSecurityTestbedwithAdaptability,” https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-Toyama-PASTA-Portable-Automotive-Security-Testbed-with-Adaptability-wp-2.pdf.
3) J. Jaffe, “A first-order DPA attack against AES in counter mode with unknown initial counter,” International Workshop on Cryptographic Hardware and Em-bedded SystemsSpringer, pp.1–13 2007.