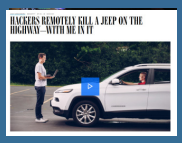
A Side-Channel Attack Method against Truncated MAC CAN Message based on AUTOSAR Specification

Takaya Kubota, Mitsuru Shiozaki, and Takeshi Fujino
Network LSI Laboratory, Ritsumeikan University

Introduction

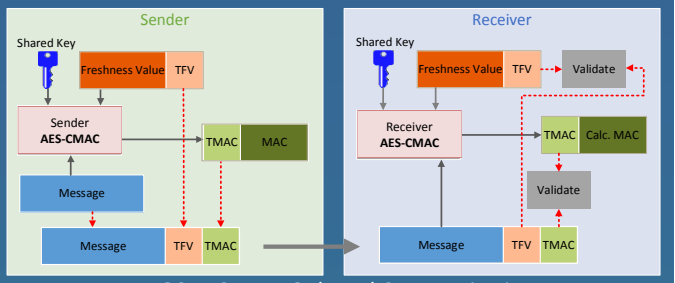
Threats: Connected cars are becoming a new attacking target by increasing the attack surface and several attack demonstrations have been done by researchers.



Proposed Solutions:
- The secure boot process for ECUs
- Introducing **a cryptographic technique MAC** into CAN communication
- CHE/SHE to accelerate theses crypto processes

Arising new threat:
- Side-channel attack is as known as a realistic method to break cryptographic modules

We illustrate combining two CPAs can reveal the secret of MAC for CAN using open source



AUTOSAR Secure Onboard Communication

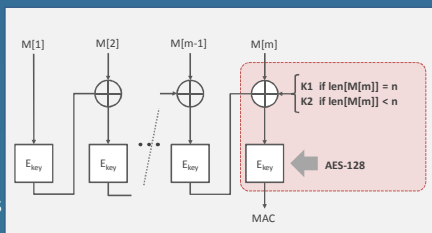
Method

The last round of AES-CMAC algorithm which is applied to MAC is divided into main two parts:

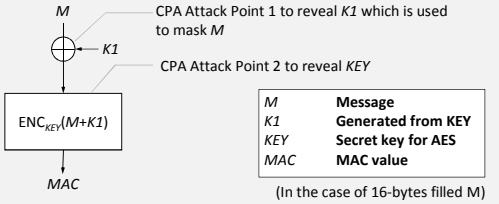
XOR Masking:
To mask the message with K1 generated from KEY

AES encryption:
To encrypt the masked message with KEY

An attacker needs to unveil K1 since he must obtain plaintexts supplied to AES

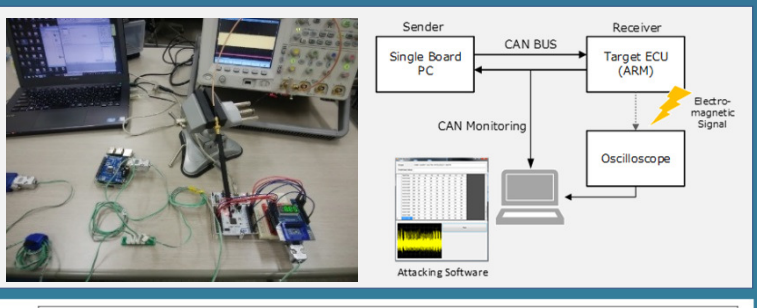


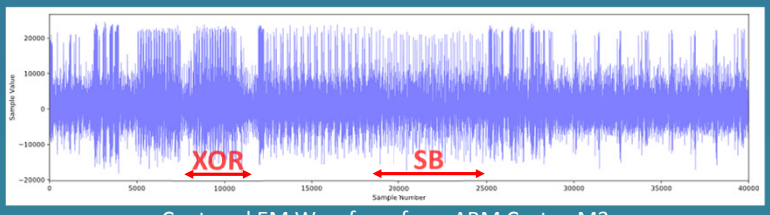
AES-CMAC algorithm



Attack points in AES-CAMC

Experiment

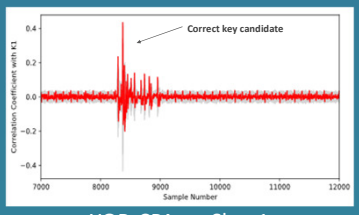




Captured EM Waveform from ARM Cortex-M3

CPA on XOR

- First Correlation Power Attack (CPA) is performed on the hamming weight model which can observe XOR of input data and guessed keys
- The correct subkey of K1 indicates a distinguishable high coefficient

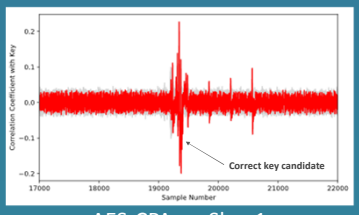


XOR-CPA on Sbox1

CPA on AES

- The obtained K1 is used to rebuild the plaintexts supplied to AES
- The second HW-CPA attack is performed at AES first round

By combining both these two attacks, the attacker can reveal all the 16 bytes subkeys

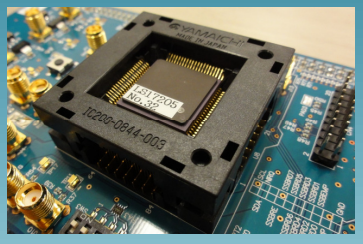


AES-CPA on Sbox1

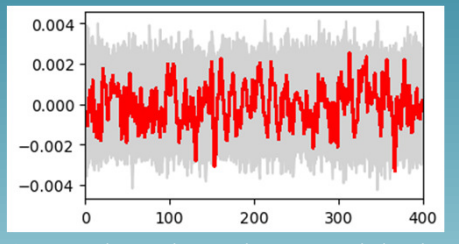
Conclusions & Discussions

The MAC authentication on in-vehicle CAN communication was implemented using an open source AES software on ARM processor. The side-channel attack method composed of 'CPA on XOR' and 'CPA on AES' successfully revealed the secret key for MAC authentication. Tamper resistant AES cryptographic hardware will be a good solution for the vulnerability against side-channel attack. We have already developed a tamper-resistant AES circuit using Masked Dual Rail-ROM (MDR) as an S-Box, and the same MAC authentication was implemented using this module. MDR-ROM can also acts as an physically unclonable function (PUF), so the secret key can be stored without secure memory.

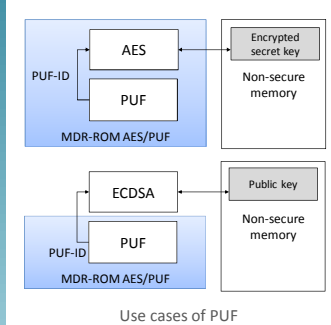
Our cryptographic LSI features



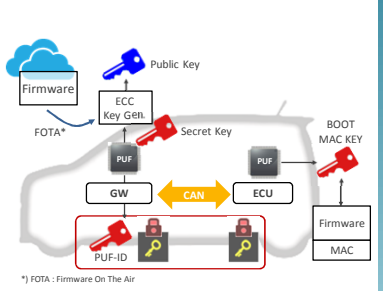
- 180nm technology
- tamper resistant AES-128
- PUF functionality based on transistor variations



- CPA evaluation has not been succeeded with 1M traces



Use cases of PUF



Proposed automotive security solutions using PUF

- Combination of PUF and AES offer a low cost and efficient key storage
- We also aim to generate public key pair for ECDSA from PUF

<Acknowledgments>
This work is based on results obtained from a project commissioned by the New Energy and Industrial Technology Development Organization (NEDO).