The Last SCARE-Frontier

Practical Reverse Engineering of Protected AES-Like Ciphers

Andrea Caforio[1] Fatih Balli[1,2] Subhadeep Banik[1]

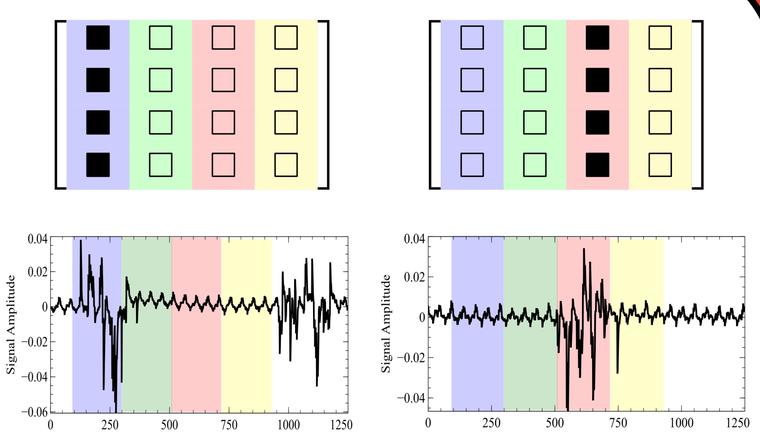
[1] LASEC, Ecole Polytechnique Fédérale de Lausanne, Switzerland
[2] CSEM, Switzerland

State of the Art

- Undisclosed AES-like ciphers are still being deployed in proprietary products.
- The first practical side-channel-assisted reverse engineering (SCARE) of an AES-like cipher has only recently been demonstrated [1].
- The attack bases itself on the novel side-channel-assisted differential plaintext attack (SCADPA) methodology that fuses differential power analysis with conventional differential cryptanalysis.

```
; Round key addition        ; Byte substitution
LD R1, [ADDR PT]            LD R1, [ADDR STATE]
LD R2, [ADDR KEY]           ADD R2, R1, [ADDR SBOX]
XOR R1, R2                  LD R3, R2
ST R1, [ADDR PT]            ST R3, [ADDR STATE]
```

- Straightforward unprotected byte-wise implementation of the AddRoundKey, SubBytes, ShiftRows, MixColumns functions on {8,32}-bit architectures.



- Use SCADPA to track differentials through the rounds and ultimately recover the description of the undisclosed cipher.

Can SCADPA be used to recover the description of side-channel protected implementations?

Shuffling

- Shuffling individual operations within the AES round function is a popular countermeasure aimed at complicating side-channel analysis. The randomness required for the individual shuffles is provided a priori.

$$\begin{bmatrix} 0 & 4 & 8 & C \\ 1 & 5 & 9 & D \\ 2 & 6 & A & E \\ 3 & 7 & B & F \end{bmatrix} \longrightarrow \begin{bmatrix} 4 & C & 5 & F \\ D & A & 9 & E \\ 3 & 0 & 2 & 7 \\ 6 & 1 & B & 8 \end{bmatrix}$$

- A common approach consists in permuting the execution order of the sixteen byte-substitutions during the S-box layer.

$$\begin{bmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{bmatrix} \longrightarrow \begin{bmatrix} c & a & d & b \\ b & d & c & a \\ d & c & b & d \\ c & b & a & c \end{bmatrix}$$

- Further shuffling can be achieved by choosing the order of the state columns to be multiplied during the MixColumns procedure.

⚡ **In order to obtain stable SCADPA measurements encryptions need to be repeated several times depending on the noise level of the underlying hardware. However, the shuffle is different for each encryption, hence differentials may not show up as easily in the differential power traces.**

Masking

- To boost the effectiveness of shuffling the intermediate cipher state is masked. A straightforward first-order masking scheme prevents conventional DPA, and thus complicates any SCADPA attempt.
- ANSSI [2] put forward a shuffled/masked 32-bit implementation of AES for the ARM Cortex processor family. It shuffles the SubBytes, ShiftRows and MixColumns according to some seed. Furthermore, the cipher state is protected through an affine masking scheme:

$$(\boldsymbol{a} \otimes \boldsymbol{x}) \oplus \boldsymbol{b}$$

- Here, **x** denotes the intermediate state, **a** the multiplicative mask and **m** the additive mask. The ANSSI proposal was subsequently dismantled in a statistical template attack by Bronchain and Standaert [3], which recovered the encryption key in approximately 2000 measurements. There are indications that a similarly protected scheme targeting 8-bit CPUs is vulnerable as well.

⚡ **There is ample scope to enrich SCADPA with statistical approaches as in the current state it solely relies on the ability to observe distinct drops/spikes in the differential power traces.**

Related Work

- The first SCARE attacks targeted the hidden S-boxes of A3/8 as part of GSM [4].
- Later, Clavier et al. presented a theoretical reverse enginnering procedure of AES-like ciphers; subsequently extended by Rivain and Roche to generic SPN constructions [5,6].
- The first pratical SCARE by Jap and Bhasin recovered 159 out of the 256 AES S-box entries [7].

References

[1] Complete Practical Side-Channel-Assisted Reverse Engineering of AES-Like Ciphers, Andrea Caforio and Fatih Balli and Subhadeep Banik, CARDIS 2021
[2] https://github.com/ANSSI-FR/SecAESSTM32
[3] Side-Channel Countermeasures' Dissection and the Limits of Closed Source Security Evaluations, Olivier Bronchain and François-Xavier Standaert , TCHES 2020(2)
[4] Side-Channel Attack on Substitution Blocks, Roman Novak, ACNS 2003
[5] An Improved SCARE Cryptanalysis Against a Secret A3/8 GSM Algorithm, Christophe Clavier, ICISS 2007
[6] Complete SCARE of AES-like Block Ciphers by Chosen Plaintext Collision Power Analysis, Christophe Clavier and Quentin Isorez and Antoine Wurcker, INDOCRYPT 2013
[7] Practical Reverse Engineering of Secret Sboxes by Side-Channel Analysis, Dirmanto Jap and Shivam Bhasin, ISCAS 2020