Towards Side-channel Secure AE

Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Thomas Unterluggauer

FSE 2017
Introduction

Problem: side-channel attacks

Countermeasures: hiding, masking, TI . . .
Introduction

Problem: side-channel attacks

Countermeasures: hiding, masking, TI . . .

Reduce overhead of countermeasures

- ASCON, KETJE/KEYAK, PRIMATES, SCREAM, . . .
Introduction

Problem: side-channel attacks

Countermeasures: hiding, masking, TI . . .

Reduce overhead of countermeasures

- ASCON, KETJE/KEYAK, PRIMATES, Scream, . . .

Can we do more?

- LR and MR AE [Ber+16]
- ISAP
ISAP

Authenticated encryption scheme
- Following requirements of CAESAR call
- No assumptions on choice of the nonce

Provides protection against DPA for:
- Encryption
- Decryption

Solely based on sponges
- Limits the attack surface against SPA
SPA and DPA

Simple Power Analysis (SPA)
- Observe device processing the same or a few inputs
- Techniques directly interpreting measurements

Differential Power Analysis (DPA)
- Observe device processing many different inputs
- Allows for the use of statistical techniques
Is DPA Still a Threat?

- A. Moradi and T. Schneider Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series COSADE 2016

Fresh Re-keying [Med+10]
Fresh Re-keying [Med+11]

\[ \begin{align*}
& P \\
& E \\
& K \rightarrow g \\
& K^* \\
& N_a \\
& K \\
& g \\
& K^* \\
& N_b \\
& C \\
& E^{-1} \\
& P
\end{align*} \]
What About Storage?

- Encryption still fine
- Decryption causes problems
Multiple Decryption

Retain principles of fresh re-keying allowing multiple decryption
Multiple Decryption

Retain principles of fresh re-keying allowing multiple decryption

DPA protection in storage settings

- A. Moradi and T. Schneider *Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series* COSADE 2016

DPA protection in unidirectional/broadcast settings

Priciple of ISAP’s Decryption

“Bind” the session key to the data that is decrypted
Principle of ISAP’s Decryption

“Bind” the session key to the data that is decrypted
Priciple of ISAP’s Decryption

“Bind” the session key to the data that is decrypted

\[ N\|C \rightarrow MAC \rightarrow T \]

\[ C \rightarrow Dec \rightarrow P \]
ISAP’s Authentication/Verification

\[ IV \rightarrow p \rightarrow p \rightarrow \ldots \rightarrow p \rightarrow K_A \rightarrow y \rightarrow g \rightarrow K_A^* \rightarrow T \]
ISAP’s Authentication/Verification
ISAP’s Authentication/Verification

Use suffix MAC instead of hash-then-MAC
Possible $g$ to Absorb Key

- Modular multiplication [Med+10]
- LPL and LWE [Dzi+16]
- Sponges [TS14]
Absorbing the Key

Idea: Reduce rate to a minimum [TS14]
Related to the classical GGM construction [GGM86]
ISAP’s En-/Decryption
Sponges and Side-channel Leakage
Sponges and Side-channel Leakage

\[ c' = c - (\ell_i + \ell_{i+1}) \]
Instances

**KECCAK-\(p[400, n_r] \) as permutation [Ber+14]**

<table>
<thead>
<tr>
<th>Name</th>
<th>Security level</th>
<th>Bit size of</th>
<th>Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( k )</td>
<td>( r_1 )</td>
<td>( r_2 )</td>
</tr>
<tr>
<td>ISAP-128</td>
<td>128</td>
<td>144</td>
<td>1</td>
</tr>
<tr>
<td>ISAP-128a</td>
<td>128</td>
<td>144</td>
<td>1</td>
</tr>
</tbody>
</table>
## Implementation

One round per cycle

<table>
<thead>
<tr>
<th>Function</th>
<th>Area [kGE]</th>
<th>Initialization [cycles]</th>
<th>Initialization [µs]</th>
<th>Runtime per Block [cycles]</th>
<th>Runtime per Block [µs]</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAP-128</td>
<td>14.0</td>
<td>3401</td>
<td>20.1</td>
<td>36</td>
<td>0.20</td>
</tr>
<tr>
<td>ISAP-128a</td>
<td>14.0</td>
<td>564</td>
<td>3.3</td>
<td>28</td>
<td>0.16</td>
</tr>
</tbody>
</table>
Conclusion

- AE scheme following requirements of CAESAR call

- Provides protection against DPA
  - Encryption
  - Decryption

- Enables several use-cases
  - Multiple decryption of stored data
  - Unidirectional/Broadcast communication
Thank you
References I


Ketje
Submission to the CAESAR competition:
http://competitions.cr.yp.to, 2014

[Ber+16] F. Berti, F. Koeune, O. Pereira, T. Peters, and F.-X. Standaert

Leakage-Resilient and Misuse-Resistant Authenticated Encryption


Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems
CRYPTO 2016
<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal/Conference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[MS16]</td>
<td>A. Moradi and T. Schneider</td>
<td>Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series</td>
<td>COSADE 2016</td>
</tr>
</tbody>
</table>
References III

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

[TS14] M. M. I. Taha and P. Schaumont
Side-channel countermeasure for SHA-3 at almost-zero area overhead
HOST 2014