Lightweight Leakage Resiliency for Symmetric Cryptography

Mostafa Taha
Sept 18, 2014

This research was partially supported by the VT-MENA program of Egypt, and by NSF grants.
Symmetric Cryptography

- Block-Ciphers
  Using AES

- Message Authentication Code
  Using SHA-3

\[
\text{Key} \quad \Downarrow \\
\text{E} \\
\downarrow \\
\text{MAC} = 100110101001
\]
Side-Channel Analysis
Side-Channel Analysis

- One Trace ➔ Simple Power Analysis (SPA)
- Many Traces ➔ Differential Power Analysis (DPA)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0x0F</td>
<td>4</td>
<td>0x82</td>
<td>2</td>
<td>0xF1</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0xAA</td>
<td>4</td>
<td>0x51</td>
<td>3</td>
<td>0x4E</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0xD3</td>
<td>5</td>
<td>0xA3</td>
<td>4</td>
<td>0x0B</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0x31</td>
<td>3</td>
<td>0xC7</td>
<td>5</td>
<td>0x92</td>
<td>3</td>
</tr>
</tbody>
</table>

Hypothesis Table
Side-Channel Countermeasures

- Variability Affects Power
- Hiding
- Predict Sensitive
- Masking
- Aggregate Info.
- Leakage Resiliency

Differential Analysis

\[ k_1 \rightarrow f \rightarrow k_2 \rightarrow f \rightarrow k_3 \]

\[ \text{0xAA} \]

\[ \text{0x32} \oplus \text{0x98} \]

\[ \text{0x25} \oplus \text{0x1F} \]

\[ \text{0x3A} \]
Outline

• Introduction
• Framework for Efficient Leakage Resiliency
  • Two Solutions for AES
  • Solution for SHA-3
• Conclusion
Background

Stateless Updating

Master Key → Stateless key-update → Pseudorandom Secret State → Stateful key-update

Nonce

Sufficient for Challenge-Response

Sufficient for Synchronized Application

Stateful Updating

Generic Applications

Sufficient for Synchronized Application
Part I: Stateless Key-Updating

- Previous Work:
  - GGM Construction
  - Goal: Black-box security and side-channel security
  - 128 full featured encryptions with fresh random variables
  - Very high performance overhead

[SPY+10]
Part I: Stateless Key-Updating

• Our Solution:
  – Goal: Side-channel security
  – Lightweight whitening functions
  – Requires only the nonce

• Requirements:
  – SPA-resistant
  – DPA-resistant against two traces
  – Non-linear
  – Balanced full diffusion
    (prevent aggregating info.)
  – At small area and performance overheads
Part II: Stateful Key-Updating

- Previous Work:
  - Goal: Black-box security and side-channel security
  - Goal: Side-channel security

\[
\begin{align*}
\text{Secret State} & \xrightarrow{R_0} E \xrightarrow{k_1} E \xrightarrow{k_2} E \xrightarrow{k_3} \text{Keystream} \quad \text{Encryption} \\
\text{Secret State} & \xrightarrow{H} k_1 \xrightarrow{k_2} k_3 \quad \text{Hashing}
\end{align*}
\]
Part II: Stateful Key-Updating

• Our Solution:
  – Goal: Side-channel security
  – Nothing required for SHA-3
  – Lightweight whitening functions for AES

• Requirements:
  – SPA-resistant
  – Non-linear
  – Balanced full diffusion
    (prevent aggregating info.)
  – At small area and performance overheads
  – (No required: DPA-resistant against two traces)
Outline

• Introduction
• Framework for Efficient Leakage Resiliency
• Two Solutions for AES
• Solution for SHA-3
• Conclusion
Background

• AES is a block-cipher.

• AES Modes of Operation:
  – Encryption:
    • CBC, CFB, OFB, CTR.
  – Authenticated Encryption:
    • CCM, GCM, OCB.
## Previous Work

<table>
<thead>
<tr>
<th>Contribution</th>
<th>Stateless</th>
<th>Stateful</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Kocher03]</td>
<td>DES</td>
<td>DES</td>
</tr>
<tr>
<td>[MSG+10]</td>
<td>Modular MUL</td>
<td>—</td>
</tr>
<tr>
<td>[GFM10]</td>
<td>Modular MUL + AES</td>
<td>AES</td>
</tr>
<tr>
<td>[Kocher11]</td>
<td>GGM (hashing)</td>
<td>Hashing</td>
</tr>
<tr>
<td>[MSJ12]</td>
<td>GGM (AES)</td>
<td>—</td>
</tr>
<tr>
<td>[BSH+13]</td>
<td>GGM (Minimum SP Net)</td>
<td>—</td>
</tr>
<tr>
<td>[YS13]</td>
<td>—</td>
<td>AES</td>
</tr>
<tr>
<td>Our work (NLFSR)</td>
<td>Lightweight-Tree (NLFSR)</td>
<td>NLFSR</td>
</tr>
<tr>
<td>Our work (RR-AES)</td>
<td>Lightweight-Tree (RR-AES)</td>
<td>RR-AES</td>
</tr>
</tbody>
</table>
Our Solution Using NLFSRs

- Why NLFSR
- The NLFSRs from the Achterbahn stream-cipher
- High non-linearity
- High diffusion
- SPA and DPA protected
- Small implementation cost
Our Solution Using RR-AES

– Only 2 rounds with all 0’s or all 1’s
– High non-linearity
– High diffusion
– SPA and DPA protected
– Small implementation cost
Results

- Modular Mul
- NLFSR \( D=1 \)
- Minimum SP \[ \text{[BSH+13]} \]
- RR-AES

Previous Work

Our, NLFSR

Our, RR-AES

Stateless Key-Update

- Smaller
- Better
- Faster

Clock Cycles

Area in KGE

0

01

AES_r

AES_r
Results

SHA-256
[Kocher11]

NLFSR
\(D = 1\)

NLFSR
\(D = 3\)

RR-AES

AES
[YS13]

NLFSR
\(D = 4\)

Our, NLFSR

Previous Work

Our, RR-AES

Smaller

Better

Faster

Masking
[MPL11]

No performance overhead at small area overhead

RR-AES
only 6 cycles
at no area overhead

Clock Cycles

Area in KGE

Stateful Key-Update

18
Outline

- Introduction
- Framework for Efficient Leakage Resiliency
- Two Solutions for AES
- Solution for SHA-3
- Conclusion
Background

- Applications of SHA-3:
  - Regular Hashing, Salted Hashing, Random Number Generation
  - MAC-generation, Stream Encryption, Authenticated Encryption
Our Goal:
Single core for SHA-3.

We need a lightweight SCA-countermeasure that can be turned-off!
Previous Work

• The inventors of SHA-3 proposed a countermeasure using Masking [BDN+13] at:

  – Four times the required area
  – Low throughput
  – Always-on
Our Solution

1. The Key goes to a separate input.
2. While processing the Nonce, squeeze the rate to “one bit”, and number of Keccak rounds to only three, except for the last bit.
3. Process the last bit with full rounds of Keccak.
4. Then, proceed normally.

![Diagram of Our Solution]
1. The Key goes to a separate input.
2. While processing the Nonce, squeeze the rate to “one bit”, and number of Keccak rounds to only three, except for the last bit.
3. Process the last bit with full rounds of Keccak.
4. Then, proceed normally.
Results

Compared to [BDN+13]

- Unprotected reference
- (4.42) Three-Shares
- (5.15) Four-Shares
- (1.0001) Our Work

No area Overhead
Results

Compared to [BDN+13]

![Graph showing relative throughput vs. number of input blocks for different numbers of shares and input blocks. The graph illustrates higher throughput compared to [BDN+13] with annotations for specific points such as (0.8376) Three-shares and (0.8596) Four-shares.]
Outline

• Introduction
• Framework for Efficient Leakage Resiliency
• Two Solutions for AES
• Solution for SHA-3
• Conclusion
Conclusion of Leakage Resiliency

Practical Leakage Resiliency is very powerful and generic

But,

New Design to New Crypto
Protocol Level
Overhead of the Tree

Hiding
Masking
Masking
Thank You