Advances in the Side-Channel Analysis of Symmetric Cryptography

Mostafa Taha
July 3, 2014

This research was supported in part by the VT-MENA program of Egypt, and by the NSF grant no. 1115839.
Symmetric Cryptography

- Block-Ciphers
  - AES

- Hashing Functions
  - SHA-3

\[ \text{Key} \rightarrow \text{E} \rightarrow \text{Digest} = 1011000101101 \]

\[ \text{Digest} \rightarrow \text{MAC} = 100110101001 \]

\[ \text{MAC} = 100110101001 \]
Side-Channel Analysis
Side-Channel Analysis

- One Trace $\Rightarrow$ Simple Power Analysis (SPA)
- Many Traces $\Rightarrow$ Differential Power Analysis (DPA)

Hypothesis Table

<table>
<thead>
<tr>
<th></th>
<th>$K_0$</th>
<th></th>
<th>$K_1$</th>
<th></th>
<th>$K_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0F</td>
<td>4</td>
<td>0x82</td>
<td>2</td>
<td>0xF1</td>
<td>5</td>
</tr>
<tr>
<td>0xAA</td>
<td>4</td>
<td>0x51</td>
<td>3</td>
<td>0x4E</td>
<td>4</td>
</tr>
<tr>
<td>0xD3</td>
<td>5</td>
<td>0xA3</td>
<td>4</td>
<td>0x0B</td>
<td>3</td>
</tr>
<tr>
<td>0x31</td>
<td>3</td>
<td>0xC7</td>
<td>5</td>
<td>0x92</td>
<td>3</td>
</tr>
<tr>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>
Side-Channel Countermeasures

- Variability Affects Power
- Hiding
- Predict Sensitive
- Masking
- Aggregate Information
- Leakage Resiliency

![Diagram](image1)

- Differential Analysis

![Diagram](image2)

- \(0xAA\)
- \(0x3A\)
- \(0x25 \oplus 0x1F\)
- \(0x32 \oplus 0x98\)
- \(k_1 \rightarrow f \rightarrow k_2 \rightarrow f \rightarrow k_3\)
## Our Contribution

<table>
<thead>
<tr>
<th>Block-Ciphers</th>
<th>Hashing Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Attacks:</td>
<td>Effect of Key-Length on the Analysis of SHA-3</td>
</tr>
<tr>
<td>Profiled Attack at High Parallelism</td>
<td>[HOST-13]</td>
</tr>
<tr>
<td>[ICCD-12]</td>
<td>Systematic Attack &amp; Case Examples</td>
</tr>
<tr>
<td>Fault Attacks:</td>
<td>[IWSEC-13]</td>
</tr>
<tr>
<td>Differential Fault Intensity Analysis</td>
<td></td>
</tr>
<tr>
<td>[FDTC-14]</td>
<td></td>
</tr>
</tbody>
</table>

### Countermeasures

<table>
<thead>
<tr>
<th>Leakage Resiliency</th>
<th>Countermeasures</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES Custom Instructions</td>
<td>[FPL-12]</td>
<td>Quantitative Masking Strength</td>
<td>[DAC-14]</td>
</tr>
<tr>
<td>Hiding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Masking</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Framework for Efficient Leakage Resiliency

<table>
<thead>
<tr>
<th>This Presentation</th>
<th>Solution for AES</th>
<th>Solution for SHA-3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Solution Using Round-Reduced AES</td>
<td>[HOST-14]</td>
</tr>
<tr>
<td></td>
<td>Using Dedicated Circuit</td>
<td>[Patent Application]</td>
</tr>
<tr>
<td></td>
<td>[DIAC-13]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Under Review @ Springer-JCEN]</td>
<td></td>
</tr>
</tbody>
</table>
Outline

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

Stateless Updating

Master Key → Stateless key-update

Nonce

Pseudorandom Secret State

Stateful Updating

Stateful key-update

$k_1$ → $k_2$ → $k_3$

Sufficient for Challenge-Response

Sufficient for Synchronized Application

Generic Applications
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

\[ \begin{align*}
  &\text{Master Key} \\
  &\downarrow \text{Step} \\
  &\begin{array}{c}
    R_0^1 \\
    R_0^2 \\
    K00 \\
    K01 \\
  \end{array} \\
  &\downarrow \text{Encryption} \\
  &\begin{array}{c}
    K1 \\
    K10 \\
    K11 \\
  \end{array} \\
  &\downarrow \text{Keystream} \\
  &\begin{array}{c}
    K0 \\
    K0 \times 1 \\
  \end{array} \\
  &\begin{array}{c}
    R_1^1 \\
    R_1^2 \\
  \end{array} \\
  &\text{Encryption} \\
  &\begin{array}{c}
    n(0) \\
    n(1) \\
  \end{array}
\end{align*} \]
Part I: Stateless Key-Updating

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

• Requirements:
  – Non-linear with high diffusion (prevent aggregating info.)
  – SPA-resistant
  – DPA-resistant against two traces
  – 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

\[ k_1 \rightarrow E \rightarrow k_2 \rightarrow E \rightarrow k_3 \rightarrow \text{Encryption} \]

\[ R_0 \rightarrow E \rightarrow k_1 \rightarrow E \rightarrow k_2 \rightarrow E \rightarrow k_3 \rightarrow \text{Keystream} \]

\[ k_1 \rightarrow H \rightarrow k_2 \rightarrow H \rightarrow k_3 \rightarrow \text{Hashing} \]

[FPS12] [Kocher11]
Part II: Stateful Key-Updating

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

• Requirements:
  – Non-linear with high diffusion
    (prevent aggregating info.)
  – At small area and performance overheads

Protected against SPA and DPA by design
Outline

- Introduction
- Our Contribution
- 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

Diagram:

- Master Key
- One bit of the Nonce

Round-Reduced AES

Stateless Updating

Stateful Updating

Secret State

AES_{r} \rightarrow k_{1} \rightarrow AES_{r} \rightarrow k_{2} \rightarrow AES_{r} \rightarrow k_{3}
Results

<table>
<thead>
<tr>
<th></th>
<th>Clock Cycles</th>
<th>Area in KGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous Work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our, NLFSR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our, RR-AES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Diagram:
- **AES_{0}**
- **AES_{01}**
- **GGM-AES [MSA12]**
- **Minimum SP [BSH+13]**
- **Modular Mul [MSG+10]**
- **NLFSR D=1**
- **NLFSR D=2**
- **NLFSR D=3**
- **NLFSR D=4**

Stateless Key-Update
- Smaller
- Better
- Faster
Results

SHA-256 [Kocher11]

NLFSR $D=1$

Masking [MPL11]

Previous Work

Our, NLFSR

Our, RR-AES

Smaller

Better

Faster

Clock Cycles

Area in KGE

AES [YS13]

RR-AES

only 6 cycles
at no area overhead

RR-AES

No performance overhead
at small area overhead

AES

NLFSR $D=1$

NLFSR $D=2$

NLFSR $D=3$

NLFSR $D=4$
Outline

• Introduction
• Our Contribution
• 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
Background

• 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.
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.

Rate = \( r \)  
Rate = 1  
Rate = \( r \)

Key State

Tree Structure

24 Rounds  3 Rounds  24 Rounds

C₀  C₁
Results

Compared to [BDN+13]

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

No area Overhead
Results

Compared to [BDN+13]

- Relative Throughput vs. Number of Input Blocks (m)
  - Unprotected
  - Higher Throughput

Symbols:
- $N_0$, $N_0N_1$, $f_r$

Equations:
- $N_0$, $N_1$
- $f_r$

Graphs:
- Curves for different values of $m$ (m=25, m=49, m=98)
- Comparison between (0.8376) Three-shares and (0.8596) Four-shares

Outline

• Introduction
• Our Contribution
• 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