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

  Message Authentication Code
  – SHA-3
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

Key

Sensitive

Power

Correlation
Side-Channel Countermeasures

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

Differential Analysis

0xAA

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

0xAA

0x3A

0x32 ⊕ 0x98

0x25 ⊕ 0x1F

0x3A
# 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</td>
</tr>
<tr>
<td>Profiled Attack at High Parallelism</td>
<td>on the Analysis of SHA-3</td>
</tr>
<tr>
<td>[ICCD-12]</td>
<td>[HOST-13]</td>
</tr>
<tr>
<td>Fault Attacks:</td>
<td>Systematic Attack &amp; Case Examples</td>
</tr>
<tr>
<td>Differential Fault Intensity Analysis</td>
<td>[IWSEC-13]</td>
</tr>
<tr>
<td>[FDTC-14]</td>
<td></td>
</tr>
</tbody>
</table>

## Attacks

- Power Attacks: Profiled Attack at High Parallelism [ICCD-12]
- Fault Attacks: Differential Fault Intensity Analysis [FDTC-14]

## Countermeasures

### Leakage Resiliency

- AES Custom Instructions [FPL-12]
- Quantitative Masking Strength [DAC-14]

## Framework for Efficient Leakage Resiliency

- Solution for AES Using Round-Reduced AES [Under Review @ IEEE-TIFS]
- Using Dedicated Circuit [DIAC-13] [Under Review @ Springer-JCEN]
- Solution for SHA-3 [HOST-14] [Patent Application]
Outline

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

Stateless updating

Master Key

Nonce

Stateless key-update

Pseudorandom Secret State

Stateful key-update

Stateful updating

$\begin{align*}
\text{Sufficient for Challenge-Response} & \quad \text{Sufficient for Synchronized Application} \\
\text{Generic Applications} & \quad \text{Generic Applications}
\end{align*}$
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

\[ \begin{align*}
K0 & \quad K1 \\
R_0^1 & \quad R_1^1 \\
R_0^2 & \quad R_1^2 \\
K00 & \quad K01 & \quad K10 & \quad K11
\end{align*} \]

[SPY+10]
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

Secret State $\rightarrow \mathcal{E} \rightarrow k_1 \rightarrow \mathcal{E} \rightarrow k_2 \rightarrow \mathcal{E} \rightarrow k_3 \rightarrow$ Keystream

$R_0 \rightarrow \mathcal{E} \rightarrow k_1 \rightarrow \mathcal{E} \rightarrow k_2 \rightarrow \mathcal{E} \rightarrow k_3 \rightarrow$ Encryption

$R_1 \rightarrow \mathcal{E} \rightarrow k_1 \rightarrow \mathcal{E} \rightarrow k_2 \rightarrow \mathcal{E} \rightarrow k_3 \rightarrow$ Encryption

$R_2 \rightarrow \mathcal{E} \rightarrow k_1 \rightarrow \mathcal{E} \rightarrow k_2 \rightarrow \mathcal{E} \rightarrow k_3 \rightarrow$ Encryption

[FPS12]

Secret State $\rightarrow \mathcal{H} \rightarrow k_1 \rightarrow \mathcal{H} \rightarrow k_2 \rightarrow \mathcal{H} \rightarrow k_3 \rightarrow$ Hashing

$\mathcal{H} \rightarrow k_1 \rightarrow \mathcal{H} \rightarrow k_2 \rightarrow \mathcal{H} \rightarrow k_3 \rightarrow$ Hashing

[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 of RR-AES process]

- One bit of the Nonce
- Master Key
- Round-Reduced AES
- Secret State
- Stateless Updating
- Stateful Updating
Results

AMS

Result

NLFSR

D=1

D=2

D=3

D=4

RR-AES

GGM-AES

[MSA12]

Minimum SP

[BSH+13]

Modular Mul

[MSG+10]

Previous Work

Our, NLFSR

Our, RR-AES

Stateless Key-Update

Smaller

Better

Faster

0

AES

01

AES

Clock Cycles

Area in KGE
Results

SHA-256
[Kocher11]

NLFSR
D=1

NLFSR
D=3

RR-AES
[YS13]

AES

Our, NLFSR

Previous Work

Masking
[MPL11]

Smaller

Better

Faster

Our, RR-AES

No performance overhead at small area overhead

RR-AES
only 6 cycles
at no area overhead

Clock Cycles

Area in KGE

1 2 3 4 5 6 7 8 9 10

300

250

200

150

100

50

0
Outline

• Introduction
• Our Contribution
• Framework for Efficient Leakage Resiliency
• Two Solutions for AES
  • Solution for SHA-3
• Conclusion
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.
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
- Relative Area
- (1.0001)
- Four-Shares
- (5.15)  Four-Shares
- Three-Shares
- (4.42)  Three-Shares
- No area Overhead

Compared to [BDN+13]
Results

Compared to [BDN+13]

Relative Throughput

Number of Input Blocks (m)

Higher Throughput

Unprotected

N₀, N₁

N₀

fᵣ

fᵣ

Our, s=4

Our, s=2

Our, s=1

(0.8596) Four-shares

(0.8376) Three-shares

m=25

m=49

m=98

m=21

m=41

m=82

N₀N₁

m=49

m=41

m=21

m=25

m=98

(0.8376) Three-shares

(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