Implementation of a Boolean Masking Scheme for the SCREAM Cipher

William Diehl and Kris Gaj

Department of Electrical and Computer Engineering, George Mason University, Fairfax, Virginia, USA, http://cryptography.gmu.edu

Introduction

- Physical cryptographic implementations subject to side-channel attack (SCA)
- Boolean masking is one countermeasure applied against power-analysis SCA
- CAESAR, the Competition for Authenticated Encryption: Security, Applicability, and Robustness, evaluates cipher candidates to select a final portfolio
- SCREAM is a Round Two CAESAR candidate with bitwise S-Boxes designed to be easily masked using Boolean masking scheme
- This research implements 1st order Boolean masking scheme in the full SCREAM cipher, and compares masking cost with equivalent-masked version of AES

Previous Work

- Studies of Simple Power Analysis (SPA) and Differential Power Analysis (DPA) side-channel attacks (SCA) [Kocher et al., 1999]
- Duplication method; early Boolean masking [Goubin & Patarin, 1999]
- Security against probing attacks along d wires [Shai, Sahai, Wagner, 2003]
- Masking schemes for DES, AES, SHA-3 candidates [Bos et al., 2004; Oswald et al., 2004; Standaert et al., 2006; Francq et al., 2012]
- Boolean masking applied to GF(2^2) inversion of AES [Prouf & Rivain, 2010]
- Securing bitslice ciphers against power analysis attacks and “easy-to-mask” bitslices [Daemen et al., 2001; Grosso et al., 2014]
- AES implementations using subfields of GF(2^8) [Satoh et al., 2001; Canright, 2005]
- Masked AES Implementations using AES S-Box using subfields of GF(2^8) [Dowsell et al., 2005; Zakeri et al., 2007; Canright & Batina, 2008; Kim et al., 2007]
- Masking of AES in FPGA [Yuan et al., 2011; Regazzoni & Standaert, 2011]

Application of Boolean Masking to Sensitive Variable

- Apply Boolean masking to sensitive variable as follows:

ALGORITHM 1 – EXPANSION TO BOOLEAN MASKING
1. Variables a, b, c are separated as a = a' @ b @ c, where a', b', and c' are random variables
2. Expand expressions of type x = a @ b to x' = a' @ b @ c
3. Expand expressions of type x = a @ b @ c to x' = a' @ b @ c @ d @ e
4. Expand expressions of type x = a @ b @ c @ d @ e to x' = a' @ b @ c @ d @ e @ f

Estimated Overhead resulting from Boolean Masking

- In n-th order masking, sensitive variable separated into d + 1 shares
- The gate count increases as (d+1)-order for non-linear operations

Table 1 - masking cost in gate count for 3rd order Boolean masking

<table>
<thead>
<tr>
<th>Operation</th>
<th>Required XOR gates</th>
<th>Required AND/OR gates</th>
</tr>
</thead>
<tbody>
<tr>
<td>a @ b</td>
<td>(d+1) x #(XOR gates)</td>
<td>0</td>
</tr>
<tr>
<td>a @ b @ c</td>
<td>(d+1) x #(XOR gates)</td>
<td>(d+1) x #(AND gates)</td>
</tr>
<tr>
<td>a @ b @ c @ d</td>
<td>(d+1) x #(XOR gates)</td>
<td>(d+1) x #(AND gates)</td>
</tr>
</tbody>
</table>

Boolean Masking applied to SCREAM Block Cipher

- Boolean masking scheme applied on SCREAM step function using “Unrolled x2” (i.e., all rounds per clock cycle) architecture
- Masked step function (Fig. 3) shares invertible S-Boxes to save resources

Table 2 - Comparison of non-masked to masked version of Full SCREAM Cipher in terms of Area (LUTs), Performance (MHz), Throughput (Mbps) and Throughput-to-area (TP/A) ratio (Mbps/LUT)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>LUTs</th>
<th>Slices</th>
<th>Frequency (MHz)</th>
<th>Throughput (Mbps)</th>
<th>Throughput/Area (Mbps/LUT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCREAM Tweakable Block Cipher without shared S-Boxes</td>
<td>Non-masked 3533</td>
<td>1094</td>
<td>87.3</td>
<td>1117</td>
<td>0.246</td>
</tr>
<tr>
<td>Masked 4932</td>
<td></td>
<td>1474</td>
<td>77.0</td>
<td>986</td>
<td>0.278</td>
</tr>
<tr>
<td>Ratio 2.26</td>
<td>2.23</td>
<td>0.783</td>
<td>0.783</td>
<td>0.345</td>
<td></td>
</tr>
</tbody>
</table>

Table 3 - Comparison of non-masked to masked version of Full SCREAM Cipher in terms of Area (LUTs), Performance (MHz), Throughput (Mbps) and Throughput-to-area (TP/A) ratio (Mbps/LUT)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>LUTs</th>
<th>Slices</th>
<th>Frequency (MHz)</th>
<th>Throughput (Mbps)</th>
<th>Throughput/Area (Mbps/LUT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCREAM Tweakable Block Cipher with shared S-Boxes</td>
<td>Non-masked 3533</td>
<td>1094</td>
<td>87.3</td>
<td>1117</td>
<td>0.246</td>
</tr>
<tr>
<td>Masked 4932</td>
<td></td>
<td>1474</td>
<td>77.0</td>
<td>986</td>
<td>0.278</td>
</tr>
<tr>
<td>Ratio 2.26</td>
<td>2.23</td>
<td>0.783</td>
<td>0.783</td>
<td>0.345</td>
<td></td>
</tr>
</tbody>
</table>

Conclusion

- SCREAM cipher easily masked using Boolean masking scheme, but costly in terms of area and performance; lowers TP/A ratio by 50% in best case
- SCREAM block cipher has roughly equal masking cost with equivalently masked AES; TP/A decreases by 62% in masked version compared to non-masked version
- Introduces method of comparison to determine practical masking cost of CAESAR authenticated cipher candidates versus known standard (i.e., AES) and versus each other; supports Round Three and Final Round of CAESAR competition.