Comparison of Cost of Protection Against Differential Power Analysis of Selected Authenticated Ciphers

William Diehl, Abubakr Abdulgalid, Farnoud Farahmand, Jens-Peter Kaps and Kris Gaj

ECE Department, George Mason University, Fairfax, Virginia, USA, http://cryptography.gmu.edu

Introduction

- Authenticated ciphers combine confidentiality, integrity and authentication
- Can provide enhanced security in resource-constrained devices
- CAESAR, the Competition for Authenticated Encryption: Security, Applicability, and Robustness, evaluates cipher candidates to select a final portfolio
- Physical cryptographic implementations subject to side-channel attack (SCA)
- There are evaluations of SCA and countermeasures on individual ciphers, but no large-scale comparisons of costs of protection for CAESAR candidate ciphers
- We analyze 10 CAESAR Round 3 candidates (+AES-GCM) for costs of DPA protection

Authenticated Ciphers

- Provide confidentiality, integrity and authentication
- Multiple inputs, multiple outputs
- Complex protocol

Table: Notional Authenticated Cipher

<table>
<thead>
<tr>
<th>Authenticated Cipher</th>
<th>Implementation Authors</th>
<th>Key Size (bits)</th>
<th>Block Size (bits)</th>
<th>Tag Size (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-CCM</td>
<td>George Mason University</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>ACORN</td>
<td>Nanyang Technical University</td>
<td>128</td>
<td>8</td>
<td>128</td>
</tr>
<tr>
<td>Ascon</td>
<td>George Mason University</td>
<td>128</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>CLOC-CAES</td>
<td>George Mason University</td>
<td>128</td>
<td>128</td>
<td>64</td>
</tr>
<tr>
<td>CLOC-TWINE</td>
<td>CLOC-SILC Team</td>
<td>80</td>
<td>64</td>
<td>32</td>
</tr>
<tr>
<td>SILC-CAES</td>
<td>George Mason University</td>
<td>128</td>
<td>128</td>
<td>64</td>
</tr>
<tr>
<td>SILC-PRESENT</td>
<td>CLOC-SILC Team</td>
<td>80</td>
<td>64</td>
<td>32</td>
</tr>
<tr>
<td>JAMBU-AES</td>
<td>George Mason University</td>
<td>128</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>JAMBU-SIMON</td>
<td>Nanyang Technical University</td>
<td>96</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>Ketje Jr.</td>
<td>Ketje-Keyak Team</td>
<td>96</td>
<td>32</td>
<td>64</td>
</tr>
</tbody>
</table>

CAESAR Round 3 Authenticated Ciphers Evaluated in this Research

DPA Protection – Threshold Implementations

- Sensitive data separated into two or more shares for independent computation
- To share function of degree d, d+1 shares required
- Three properties
  1. Non-completeness. Every function is independent of at least one share of each of the input variables
  2. Correctness. The sum of the output shares gives the desired output
  3. Uniformity. Output distribution should preserve the input distribution

Test Vector Leakage Assessment (TVLA) with FOBOS

- Accelerated detection of DPA vulnerability without mounting attack (t-test)
- Easier than attack-based tests, but does not recover secret key nor show difficulty of attack (Cooper et al, 2013), [Goodwill et al, 2011], [Schneider et al, 2016]

TVLA of Unprotected & Protected Cipher Implementations

- Using FOBOS, t-tests with 2,000 “fixed-versus-random” traces conducted on unprotected implementations @ 780 kHz on Spartan-6 FPGA
- Leakage detected in all unprotected implementations
- Does not prove vulnerability to DPA; shows that countermeasures are needed
- Countermeasures against DPA using 3-share threshold protections (TI) Included
- TVLA (t-tests) using FOBOS are repeated on protected implementations
- Results show reduced leakage; improved resistance to DPA

Comparing Costs of Protection against DPA

- Unprotected and protected implementations benchmarked on Spartan-6 FPGA
- Comparisons of area (LUTs), throughput (TP)(Mpps), TP/A ratios (Mpps/LUT); Power (mW) and energy per bit (nJ/bit) @ 10 MHz

Summary of Results

<table>
<thead>
<tr>
<th>Rank</th>
<th>Area</th>
<th>Throughput</th>
<th>Throughput / Area</th>
<th>Power</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ACORN</td>
<td>Ketje Jr.</td>
<td>ACORN</td>
<td>ACORN</td>
<td>ACORN</td>
</tr>
<tr>
<td>2</td>
<td>JAMBU-AES</td>
<td>Ketje Jr.</td>
<td>JAMBU-AES</td>
<td>Ketje Jr.</td>
<td>JAMBU-AES</td>
</tr>
<tr>
<td>3</td>
<td>JAMBU-SIMON</td>
<td>JAMBU-SIMON</td>
<td>SILC-CAES</td>
<td>JAMBU-SIMON</td>
<td>SILC-CAES</td>
</tr>
</tbody>
</table>

Problem Areas

- Area: Minimize area footprint
- Throughput: Minimize area footprint
- Power: Minimize area footprint
- Energy: Minimize area footprint
- Randomness: Minimize area footprint

Acknowledgements

This poster is based upon work supported by the NSF under Grant No. 1314540.