Improved Lightweight Implementations of CAESAR Authenticated Ciphers

Farnoud Farahmand, William Diehl, Abubakr Abdulgadir, Jens-Peter Kaps and Kris Gaj
George Mason University, USA
CERG @ GMU
http://cryptography.gmu.edu/

10 PhD students
5 MS students
Cryptographic Standard Contests

- AES (IX.1997, X.2000) - 15 block ciphers → 1 winner
- NESSIE (XI.2000, XII.2002)
- CRYPTREC (XII.2002, XI.2004)
- eSTREAM (IV.2008, X.2007)
- SHA-3 (X.2007)
- CAESAR (I.2013, XII.2018)
- PQC (I.2013, XII.2018)

- 51 hash functions → 1 winner
- 57 authenticated ciphers → multiple winners

- 61 PQC candidates submitted
Evaluation Criteria

Security

Software Efficiency
- \( \mu \)Processors
- \( \mu \)Controllers

Hardware Efficiency
- FPGAs
- ASICs

Flexibility

Simplicity

Licensing
Authenticated Ciphers

Combine the functionality of **confidentiality**, **integrity**, and **authentication**

Notation: Npub = Public Message Number; (Enc) Nsec = (Encrypted) Secret Message Number; AD = Associated Data
# Round 3/Finalists CAESAR Candidates

1. ACORN  
2. AEGIS  
3. AES-OTR  
4. AEZ  
5. Ascon  
6. CLOC and SILC  
7. COLM  
8. Deoxys-II  
9. JAMBU  
10. Ketje  
11. Keyak  
12. MORUS  
13. NORX  
14. OCB  
15. Tiaoxin
CAESAR Finalists selected for each use cases

- **Use case 1 (Lightweight applications):**
  - ACORN
  - Ascon

- **Use case 2 (High-speed applications):**
  - AEGIS
  - MORUS
  - OCB

- **Use case 3 (Defense in depth):**
  - COLM
  - Deoxys-II
Suboptimal Implementations

- Majority of submitted implementations were optimized for high speed applications
  - Full-width datapaths (= more register writes/cycle, higher power)
  - Basic iterative architectures (= longer critical paths; glitch chains)
- CAESAR HW Development Package optimized for High Speed
  - External I/O bus widths $\geq$ 32 bits
  - Includes extra functionality e.g. padding unit
- It is difficult to protect High Speed implementations against side-channel attacks
Areas for Improvement in CAESAR Evaluation

- Improved lightweight implementations
- Adopt lightweight CAESAR development package
- Develop side channel protected design

High-speed footprint

Lightweight footprint
Support CAESAR Evaluations in This Research

- True LW implementations of selected CAESAR Round 3 ciphers:
  - ACORN, NORX, CLOC-AES, SILC-AES, and SILC-LED.

- Compliant with new version of the CAESAR Development Package supporting LW implementations

- Benchmark each HS and LW implementation pair in the Spartan-6 FPGA, and compare them in terms of area, TP, and TP/A ratio

- Compute power and energy per bit based on measured mean power consumption for each implementation pair
## Design Specifications

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>High-Speed</th>
<th></th>
<th>Lightweight</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Datapath Width [bits]</td>
<td>#Cycles per block</td>
<td>Datapath Width [bits]</td>
<td>#Cycles per block</td>
</tr>
<tr>
<td>ACORN</td>
<td>325</td>
<td>1</td>
<td>301</td>
<td>1</td>
</tr>
<tr>
<td>NORX</td>
<td>512</td>
<td>4</td>
<td>32</td>
<td>12</td>
</tr>
<tr>
<td>CLOC-AES</td>
<td>128</td>
<td>23</td>
<td>16</td>
<td>190</td>
</tr>
<tr>
<td>SILC-AES</td>
<td>128</td>
<td>23</td>
<td>16</td>
<td>182</td>
</tr>
<tr>
<td>SILC-LED</td>
<td>64</td>
<td>98</td>
<td>16</td>
<td>490</td>
</tr>
</tbody>
</table>
Top-level Block Diagrams
Lightweight CAESAR hardware API
ATHENa: Automated Tool for Hardware Evaluation (1)

- synthesis, implementation, and timing analysis in batch mode
- support for devices and tools of multiple FPGA vendors:
  - Xilinx (ISE)
  - Intel FPGA (Quartus)
- generation of results for multiple families of FPGAs of a given vendor
- automated choice of a best-matching device within a given family
ATHENa: Automated Tool for Hardware EvaluatioN (2)

- **automated verification** of designs through simulation in batch mode
- support for **multi-core processing**
- automated **extraction and tabulation of results**
- several **optimization strategies** aimed at finding
  - optimum options of tools
  - best target clock frequency
  - best starting point of placement
Improved Lightweight Implementations

But…

75% reduction in throughput

40% area reduction

Spartan-6 FPGA
Area Comparison of Selected CAESAR Round3 Candidates

Spartan-6 FPGA

Use case 1 (Lightweight) finalists

Power Measurement Equipment

FOBOS workbench:
Flexible Open-source workBench fOr Side-channel analysis
Power Measurement

- **20** FOBOS traces (using various test vectors of up to 2000 bytes each)
- **18,000** samples per trace
- **10 MHz** frequency
Mean Power Comparison

Spartan-6 @10MHz

55% power reduction
Energy per bit Comparison

Spartan-6 @10MHz

But, 3.6x increase in E/bit
Mean Power (Experimental vs. Simulation)

Simulated results generated using Xilinx XPA in vector-less mode

The maximum relative difference between the simulated and experimental power is 21%
Conclusions

• We presented the first medium-scale study of LW implementations of CAESAR Round 3 candidates targeting Use Case 1.

• Our LW implementations achieve an area on average 55% lower than their corresponding HS implementations, while TP decreases by 75%.

• The area results for candidates implemented in our works support the CAESAR finalist selection for lightweight use case.

• Our LW cipher implementations use on average 40% less power and 3.6 times more energy per bit than their corresponding HS implementations.

• Our open-source implementations provide useful starting points for more efficient side-channel resistant implementations.
Future works

- Side channel protected implementation of CAESAR finalists
- Analysis on advanced FPGAs
- Optimization using the Minerva hardware optimization tool
  - New version of ATHENa
  - Supports Vivado Design Suit
  - Supports 7- series Xilinx FPGA and beyond
  - 25 optimization strategies
Thank you!

Comments?

Questions?

Suggestions?