Efficient Hardware Implementations and Hardware Performance Evaluation of SHA-3 Finalists

By

Kashif Latif, Athar Mahboob, Arshad Aziz and M Muzaffar Rao

Information Security Research Laboratory
National University of Sciences and Technology, Islamabad, Pakistan
OUTLINE

• Objective
• Implementation Methodology
• LUT Primitives in Xilinx HDL Library
• Implementation Details SHA-3 Finalists
• Results
• Performance Comparison
• Conclusion
• Q/A
OBJECTIVE

• Resource efficient and high speed implementations
• Fully autonomous designs
• Utilization of specific internal resources of FPGAs instead of direct coding
• Fair comparison using uniform implementation environment
IMPLEMENTATION METHODOLOGY

- Common environment:
  - Level of expertise → common implementer
  - Coding language → Verilog®
  - Development platform → Xilinx ISE 13.1
  - Design methodology → on next slide
- Common Input/Output interface
- Overhead suppression
  - Padding → assume already padded message
  - Salt input
  - HMAC
  - Hash Tree functionality
DESIGN METHODOLOGY

• Same set of hardware resources
• Assured it by forcing our designs to map on LUT based logic and not to use dedicated resources like BRAMs, Multipliers and DSP Slices.
• Mapping to LUT is assured by using LUT primitives from Xilinx HDL library
• Memories are implemented using distributed RAMs/ROMs
LUT5 and LUT6_2 Primitives from Xilinx HDL Library

![Diagram of LUT5 and LUT6_2 primitives]

**LUT5**
- **Attributes**
- **INIT** = 00000000

**LUT6_2**
- 6-Input Look-Up Table

---

ISRL Information Security Research Laboratory
IMPLEMENTATION

• Input/output interface
IMPLEMENTATION

- Data path and Control path
IMPLEMENTATION

• Data path Architecture for BLAKE
IMPLEMENTATION

• Data path Architecture for Grøstl
IMPLEMENTATION

• Data path Architecture for JH

(a) Data path of JH
(b) 5-to-4 bit S-box
(c) Linear Transformation
IMPLEMENTATION

• Data path Architecture for Keccak

![Diagram of Keccak data path architecture]

- **LUT5**
  - Attributes: INIT = 96696996
  - 5-Input Look-Up Table
  - $O = i_0 \oplus i_1 \oplus i_2 \oplus i_3 \oplus i_4$
  - 5-bit XOR used in $\theta$ step

- **LUT3**
  - Attributes: INIT = 96
  - 3-Input Look-Up Table
  - $O = i_0 \oplus i_1 \oplus i_2$
  - 3-bit XOR used in $\theta$ step

- **LUT3**
  - Attributes: INIT = D2
  - 3-Input Look-Up Table
  - $O = i_0 \oplus (\sim i_1 \& i_2)$
  - 3-bit Logic used in $\chi$ step

- **LUT2**
  - Attributes: INIT = 6
  - 2-Input Look-Up Table
  - $O = i_0 \oplus i_1$
  - 2-bit XOR used in $i$ step

ISRL Information Security Research Laboratory
IMPLEMENTATION

- Data path Architecture for Skein

(a) Data path of Skein

(b) Key_Schedule Module

(c) Selection between two rotation constants in MIX operation
<table>
<thead>
<tr>
<th>SHA 3 Finalist</th>
<th>Device</th>
<th>256 bit</th>
<th>512 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLAKE</td>
<td>Virtex 5</td>
<td>512</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Virtex 6</td>
<td>512</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Virtex 7</td>
<td>512</td>
<td>28</td>
</tr>
<tr>
<td>Grøstl</td>
<td>Virtex 5</td>
<td>512</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Virtex 6</td>
<td>512</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Virtex 7</td>
<td>512</td>
<td>10</td>
</tr>
<tr>
<td>JH</td>
<td>Virtex 5</td>
<td>512</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Virtex 6</td>
<td>512</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Virtex 7</td>
<td>512</td>
<td>42</td>
</tr>
<tr>
<td>Keccak</td>
<td>Virtex 5</td>
<td>1088</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Virtex 7</td>
<td>1088</td>
<td>24</td>
</tr>
<tr>
<td>Skein</td>
<td>Virtex 5</td>
<td>512</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Virtex 6</td>
<td>512</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Virtex 7</td>
<td>512</td>
<td>19</td>
</tr>
</tbody>
</table>
PERFORMANCE COMPARISON OF 256-bit VARIANTS OF SHA-3 FINALISTS
PERFORMANCE COMPARISON OF 512-bit VARIANTS OF SHA-3 FINALISTS

<table>
<thead>
<tr>
<th></th>
<th>Virtex 7</th>
<th>Virtex 6</th>
<th>Virtex 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLAKE-512</td>
<td>Blue</td>
<td>Red</td>
<td>Pink</td>
</tr>
<tr>
<td>Grøstl-512</td>
<td>Red</td>
<td>Blue</td>
<td>Pink</td>
</tr>
<tr>
<td>JH-512</td>
<td>Green</td>
<td>Yellow</td>
<td>Pink</td>
</tr>
<tr>
<td>Keccak-512</td>
<td>Purple</td>
<td>Green</td>
<td>Yellow</td>
</tr>
<tr>
<td>Skein-512</td>
<td>Blue</td>
<td>Green</td>
<td>Yellow</td>
</tr>
</tbody>
</table>
## PERFORMANCE RANKING

<table>
<thead>
<tr>
<th>Rank</th>
<th>256-bit</th>
<th>512-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TPA</td>
<td>TP</td>
</tr>
<tr>
<td>1</td>
<td>Keccak</td>
<td>Keccak</td>
</tr>
<tr>
<td>2</td>
<td>JH</td>
<td>Grøstl</td>
</tr>
<tr>
<td>3</td>
<td>Grøstl</td>
<td>JH</td>
</tr>
<tr>
<td>4</td>
<td>Skein</td>
<td>Skein</td>
</tr>
<tr>
<td>5</td>
<td>BLAKE</td>
<td>BLAKE</td>
</tr>
</tbody>
</table>
CONCLUSION

• We have presented efficient and high throughput implementations of SHA-3 finalists
• Results shown for Xilinx Virtex 5, Virtex 6 and Virtex 7
• Performance figures reported in terms of Area consumption, throughput and throughput per area
• Performance comparison on latest Xilinx FPGAs is presented
• This work serves as performance investigation of SHA-3 finalists on most up-to-date FPGAs