Compact Dual Block AES core on FPGA for CCM Protocol

João Carlos C. Resende    Ricardo Chaves
Outline

- Introduction & Motivation
  - Digital Security Today
  - The AES Block Cipher
  - The CCMP Encryption mode

- State of the Art in AES implementations on FPGA

- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improved Solution

- Result Analysis
  - Resource requirements and performance
  - Comparison with related State of the Art

- Conclusions
Digital Security Today

Encryption

Authentication

Integrity

Non-repudiation
Digital Security Today

- Ciphers
- Hash functions
- Higher Lvl Protocols

- Encryption
- Authentication
- Integrity
- Non-repudiation
Digital Security Today

- Ciphers
- Hash functions
- Higher Lvl Protocols
- Ciphers + Hash
  - 2 cores
Digital Security Today

- Ciphers
- Hash functions
- Higher Lvl Protocols

- Ciphers + Hash
  - 2 cores

- Ciphers + Cipher Modes
  - CCM
  - GCM

Encryption
Authentication
Integrity
Non-repudiation
Cipher Modes (more easily embeddable & efficient)

- It specifies the order in which blocks are encryption
- AES-CCM most common:
  - Advanced Encryption
  - Standard
  - Counter with
  - CBC-MAC
• **Cipher Modes** *(more easily embeddable & efficient)*
  - It specifies the order in which blocks are encryption
  - AES-CCM most common:
    - Advanced Encryption Standard
    - Counter with CBC-MAC
  - Used in:
    - IEEE 802.11 (WLAN)
    - IEEE 802.16 (Broadband Wi-Fi)
    - IPSec
    - TLS 1.2
The AES Block Cipher

- Official NIST standard since 2001
  - FIPS 197
- 128-bit block cipher
- Logic or Table implementation
- Shared structure for Enc/Dec
- Input keys of 128, 192 or 256 bits
  - 10, 12 or 14 iterative rounds
The Counter with CBC-MAC Protocol

- Original submission 2002
  - RFC 3610

- Encryption; Authentication; Integrity for any block cipher
  - Typically AES
The Counter with CBC-MAC Protocol

- Two stream chains
  - **Counter**: non-feedback mode
    Counter tags for each independent Plaintext block
  - **CBC-MAC**: feedback mode
    Chained and dependent Plaintext encryption

- Cipher’s decryption is not required
- Additional Shared Data for extra security
Outline

- Introduction & Motivation
  - Digital Security Today
  - The AES Block Cipher
  - The CCMP Encryption mode

- State of the Art in AES implementations on FPGA

- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improved Solution

- Result Analysis
  - Resource requirements and performance
  - Comparison with related State of the Art

- Conclusions
Chodowiec and Gaj [2003]
- ShiftRows performed by addressable Shift Register
- SubBytes performed by BRAM-based S-Boxes
- MixColumns performed by logic
State of the Art in AES implementations on FPGA

- Rouvroy et al. [2004]
  - ShiftRows performed by Shift Register
  - SubBytes & MixColumns performed by BRAM-based T-Boxes
  - Extra InvS-Box in BRAM for decryption
  - Embedded Key Scheduler
State of the Art in AES implementations on FPGA

- Drimer et al. [2010]
  - ShiftRows performed by Logic Shift Register
  - SubBytes & MixColumns by BRAM based T-Boxes
  - XOR operations performed by Cascade of 4 DSPs
  - 8-stage Pipeline for maximum clock frequency
Outline

- Introduction & Motivation
  - Digital Security Today
  - The AES Block Cipher
  - The CCMP Encryption mode
- State of the Art in AES implementations on FPGA
- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improved Solution
- Result Analysis
  - Resource requirements and performance
  - Comparison with related State of the Art
- Conclusions
Proposed Architecture: Description and Implementation

- Proposed Structure
  - Combine solutions from State of the Art
  - Improve efficiency through:
    - Removal of DSPs
    - Most use of LUT6 technology
    - Improved Scheduling/Pipelining
    - Minimize Critical Path
Proposed Architecture: Description and Implementation

- Step-by-step components
  - Initial Whitening Keys
Proposed Architecture: Description and Implementation

- **Step-by-step components**
  - Initial Whitening Keys
  - Shift Register for AES

![Diagram of Proposed Architecture](attachment:image.png)
Proposed Architecture: Description and Implementation

- Step-by-step components
  - Initial Whitening Keys
  - Shift Register for AES
  - BRAM based T-Boxes
Proposed Architecture: Description and Implementation

- **Step-by-step components**
  - Initial Whitening Keys
  - Shift Register for AES
  - BRAM based T-Boxes
  - AddRoundKey and Feedback
Proposed Architecture: Description and Implementation

- Step-by-step components
  - Initial Whitening Keys
  - Shift Register for AES
  - BRAM based T-Boxes
  - AddRoundKey and Feedback
  - Output Block Addition

// Immediate load of new Block (Counter)
Proposed Architecture:
Description and Implementation

• Scheduling
  – Each block takes 9 cycles to process & re-store.
  – There are 2 blocks = 8 Words (32 bits)
  – 1 dead cycle = 1 register too many
Proposed Architecture: Description and Implementation

- **Scheduling**
  - Each block takes 9 cycles to process & re-store.
  - There are 2 blocks = 8 Words (32 bits)
  - 1 dead cycle = 1 register too many

Two viable solutions
Proposed Architecture: Description and Implementation

- Scheduling
  - Each block takes 9 cycles to process & re-store.
  - There are 2 blocks = 8 Words (32 bits)
  - 1 dead cycle = 1 register too many

- Removal of the SRL output register
  - Shorter propagation signal

- Each block takes 8 cycles to process & re-store.
- There are 2 blocks = 8 Words (32 bits)
- 0 dead cycles
Proposed Architecture: Description and Implementation

- Compact Double Block AES FPGA core.
  - Double Input (Counter or CBC-MAC)
  - Shift Register for Shift Rows
  - BRAM-based TBoxes
  - Output Stage with Final block addition
  - **Overlapping Input/Output cycles**
  - Critical Path = 1 Logic level + routing
  - Total of 96 LUTs + 2 BRAMs (+32 isolated FFs)
Outline

- Introduction & Motivation
  - Digital Security Today
  - The AES Block Cipher
  - The CCMP Encryption mode

- State of the Art in AES implementations on FPGA

- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improved Solution

- Result Analysis
  - Resource requirements and performance
  - Comparison with related State of the Art

- Conclusions
## Result Analysis

- **State of the Art Comparison (double block)**

<table>
<thead>
<tr>
<th>Round Structure</th>
<th>Device</th>
<th>Resources</th>
<th>Throughput</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Slices</td>
<td>BRAMs</td>
<td>DSPs</td>
</tr>
<tr>
<td><strong>Rolled(128b)</strong></td>
<td>V5</td>
<td>303</td>
<td>8+2</td>
<td>0</td>
</tr>
<tr>
<td><strong>Rolled(128b)</strong></td>
<td>V5</td>
<td>407</td>
<td>8+2</td>
<td>0</td>
</tr>
<tr>
<td><strong>Rolled(128b)</strong></td>
<td>V5</td>
<td>400</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Rolled(32b)</strong></td>
<td>V5</td>
<td>107</td>
<td>2+1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Rolled(32b)</strong></td>
<td>V5</td>
<td>212</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td><strong>Rolled(32b)</strong></td>
<td>V6</td>
<td>70</td>
<td>2+1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Rolled(32b)</strong></td>
<td>S3</td>
<td>142</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td><strong>Rolled(32b)</strong></td>
<td>V5</td>
<td>123</td>
<td>2+1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Rolled(32b)</strong></td>
<td>V6</td>
<td>115</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td><strong>Unrolled</strong></td>
<td>V5</td>
<td>3579</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td><strong>Unrolled</strong></td>
<td>V6</td>
<td>3121</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td><strong>Unrolled</strong></td>
<td>A7</td>
<td>80</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td><strong>Unrolled</strong></td>
<td>S3</td>
<td>633</td>
<td>53</td>
<td>0</td>
</tr>
<tr>
<td><strong>Unrolled</strong></td>
<td>S3</td>
<td>731</td>
<td>1031</td>
<td></td>
</tr>
<tr>
<td><strong>2xUnrolled</strong></td>
<td></td>
<td>2154</td>
<td>106</td>
<td>0</td>
</tr>
<tr>
<td><strong>2xRolled(128b)</strong></td>
<td>S3</td>
<td>1041</td>
<td>18</td>
<td>0</td>
</tr>
</tbody>
</table>
Result Analysis

<table>
<thead>
<tr>
<th></th>
<th>Slices</th>
</tr>
</thead>
<tbody>
<tr>
<td>El Maraghy</td>
<td>303</td>
</tr>
<tr>
<td>Chaves</td>
<td>407</td>
</tr>
<tr>
<td>Bulens</td>
<td>400</td>
</tr>
<tr>
<td>Drimer w/ DSPs</td>
<td>107</td>
</tr>
<tr>
<td>Drimer w/o DSPs</td>
<td>212</td>
</tr>
<tr>
<td>This Work V5</td>
<td>70</td>
</tr>
<tr>
<td>This Work V6</td>
<td>51</td>
</tr>
<tr>
<td>This Work S3</td>
<td>142</td>
</tr>
<tr>
<td>Resende V5</td>
<td>123</td>
</tr>
<tr>
<td>Resende V6</td>
<td>115</td>
</tr>
<tr>
<td>Liu V5</td>
<td>3579</td>
</tr>
<tr>
<td>Liu V6</td>
<td>3121</td>
</tr>
<tr>
<td>de la Piedra</td>
<td>80</td>
</tr>
<tr>
<td>Lopez-Trejo ECB</td>
<td>633</td>
</tr>
<tr>
<td>Lopez-Trejo w/..</td>
<td>731</td>
</tr>
<tr>
<td>Lopez-Trejo MAC</td>
<td>1031</td>
</tr>
<tr>
<td>Lopez-Trejo Total</td>
<td>2154</td>
</tr>
<tr>
<td>Algredo-Badillo</td>
<td>1041</td>
</tr>
</tbody>
</table>
Result Analysis

<table>
<thead>
<tr>
<th></th>
<th>Efficiency [Mbps/S]</th>
</tr>
</thead>
<tbody>
<tr>
<td>El Maraghy</td>
<td>8.75</td>
</tr>
<tr>
<td>Chaves</td>
<td>5.96</td>
</tr>
<tr>
<td>Bulens</td>
<td>5.46</td>
</tr>
<tr>
<td>Drimer w/ DSPs</td>
<td>16.45</td>
</tr>
<tr>
<td>Drimer w/o DSPs</td>
<td>8.3</td>
</tr>
<tr>
<td>This Work V5</td>
<td>24.22</td>
</tr>
<tr>
<td>This Work V6</td>
<td>30.49</td>
</tr>
<tr>
<td>This Work S3</td>
<td>4.05</td>
</tr>
<tr>
<td>Resende V5</td>
<td>8.23</td>
</tr>
<tr>
<td>Resende V6</td>
<td>8.3</td>
</tr>
<tr>
<td>Liu V5</td>
<td>1.22</td>
</tr>
<tr>
<td>Liu V6</td>
<td>1.95</td>
</tr>
<tr>
<td>de la Piedra</td>
<td>2.44</td>
</tr>
<tr>
<td>Lopez-Trejo ECB</td>
<td>1.68</td>
</tr>
<tr>
<td>Lopez-Trejo w/ CTR</td>
<td>1.45</td>
</tr>
<tr>
<td>Lopez-Trejo MAC</td>
<td>1.03</td>
</tr>
<tr>
<td>Lopez-Trejo Total</td>
<td>0.49</td>
</tr>
<tr>
<td>Algedro-Badillo</td>
<td>1.04</td>
</tr>
</tbody>
</table>
Conclusions

• **Compact** Double Block AES core on FPGA for CCMP
  – Processing of 2 data streams
  – **51 Slices+3 BRAMs** ; 486 MHz ;
  – 1,55 Gbps ; **30,49 Mbps/Slice**

• **Improvements** (Virtex 5)
  – Smallest 32-bit structure to date
  – Most efficient AES structure in the state of the art

<table>
<thead>
<tr>
<th></th>
<th>Resources</th>
<th>Throughput</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>de La Piedra “16xDSPs”</td>
<td>-12,5%</td>
<td>+770%</td>
</tr>
<tr>
<td></td>
<td>Drimer “4xDSPs”</td>
<td>-34%</td>
<td>-4%</td>
</tr>
<tr>
<td></td>
<td>Drimer “0xDSPs”</td>
<td>-67%</td>
<td>-4%</td>
</tr>
<tr>
<td>128-bit</td>
<td>El Maraghy</td>
<td>-76%</td>
<td>-36%</td>
</tr>
</tbody>
</table>
Thank you!

Questions?

Email:
joaocresende@tecnico.ulisboa.pt
ricardo.chaves@inesc-id.pt