A High-Performance Area-Efficient AES Cipher on a Many-Core Platform

Bin Liu and Bevan M. Baas

VLSI Computation Lab
ECE Department
University of California, Davis

November 9th, 2011
Asilomar Conference on Signals, Systems and Computers
Outline

- Advanced Encryption Standard
- Targeted Fine-Grained Many-Core Platform
- Implementations of AES Cipher
- Comparison with Related Work
Advanced Encryption Standard

- AES is a symmetric block encryption algorithm
- Plaintext: 128 bits, a 4-by-4 byte array
- Four basic operations in the main loop
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey

### Length of round key (bits) vs. Number of Rounds ($N_r$)

<table>
<thead>
<tr>
<th>Length of round key (bits)</th>
<th>Number of Rounds ($N_r$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>10</td>
</tr>
<tr>
<td>192</td>
<td>12</td>
</tr>
<tr>
<td>256</td>
<td>14</td>
</tr>
</tbody>
</table>
AES Basic Operations

**SubBytes**: byte substitution from a look up table

![S-box diagram]

**MixColumns**: each column multiplies a fixed polynomial over GF(2^8)

\[
\begin{bmatrix}
S'_0 & S'_4 & S'_8 & S'_12 \\
S'_1 & S'_5 & S'_9 & S'_13 \\
S'_2 & S'_6 & S'_10 & S'_14 \\
S'_3 & S'_7 & S'_11 & S'_15
\end{bmatrix}
= \begin{bmatrix}
02 & 03 & 01 & 01 \\
01 & 02 & 03 & 01 \\
01 & 01 & 02 & 03 \\
03 & 01 & 01 & 02
\end{bmatrix}
\times
\begin{bmatrix}
S_0 & S_4 & S_8 & S_{12} \\
S_1 & S_5 & S_9 & S_{13} \\
S_2 & S_6 & S_{10} & S_{14} \\
S_3 & S_7 & S_{11} & S_{15}
\end{bmatrix}
\]

**ShiftRows**: cyclically shift by one, two and three bytes in the 2nd, 3rd and 4th row

![ShiftRows diagram]

**AddRoundKey**: round key is added to input using a bitwise XOR operation

\[
\begin{bmatrix}
S'_0 & S'_4 & S'_8 & S'_12 \\
S'_1 & S'_5 & S'_9 & S'_13 \\
S'_2 & S'_6 & S'_10 & S'_14 \\
S'_3 & S'_7 & S'_11 & S'_15
\end{bmatrix}
= \begin{bmatrix}
K_0 & K_4 & K_8 & K_{12} \\
K_1 & K_5 & K_9 & K_{13} \\
K_2 & K_6 & K_{10} & K_{14} \\
K_3 & K_7 & K_{11} & K_{15}
\end{bmatrix}
\times
\begin{bmatrix}
S_0 & S_4 & S_8 & S_{12} \\
S_1 & S_5 & S_9 & S_{13} \\
S_2 & S_6 & S_{10} & S_{14} \\
S_3 & S_7 & S_{11} & S_{15}
\end{bmatrix}
\]
AES Key Expansion

**KeySubWord**: byte substitution from a look up table for a four-byte word

\[
\begin{bmatrix}
K_0 & K_1 & K_2 & K_3
\end{bmatrix} \xrightarrow{\text{S-box}} \begin{bmatrix}
K'_0 & K'_1 & K'_2 & K'_3
\end{bmatrix}
\]

**KeyRotWord**: left cyclic shift one byte

\[
\begin{bmatrix}
K_0 & K_1 & K_2 & K_3
\end{bmatrix} \xrightarrow{\text{left cyclic shift}} \begin{bmatrix}
K_1 & K_2 & K_3 & K_0
\end{bmatrix}
\]

**KeyXOR**: every word \(w[i]\) is equal to the bitwise XOR of the previous word, \(w[i-1]\), and the word \(Nk\) position earlier, \(w[i-Nk]\).

Note: \(Nk\) equals 4, 6 or 8 for the key length of 128, 192 or 256 bits
Outline

- Advanced Encryption Standard
- *Targeted Fine-Grained Many-Core Platform*
- Implementations of AES Cipher
- Comparison with Related Work
Targeted Fine-Grained Many-Core Platform

- 164 homogeneous fine-grained cores
  - In-order 6-stage pipeline
  - no specialized instructions
  - 128 x 32-bit instruction memory
  - 128 x16-bit data memory
  - Max. frequency 1.2GHz @ 1.3V
  - 0.17 mm² in 65nm CMOS
- On-chip reconfigurable 2D-mesh network
  - Nearby & long-distance communication

D. Truong et.al, JSSC, 2009
Outline

- Advanced Encryption Standard
- Targeted Fine-Grained Many-Core Platform
- Implementations of AES Cipher
- Comparison with Related Work
Preliminary Design of AES Cipher

- \((N_r - 1)\) times loop-unrolling is applied to both the main AES algorithm and the key expansion process
  - Key length = 128 bits, \(N_r = 10\)
- Throughput is 266 clock cycles per block, equaling 16.625 clock cycles per byte
  - Determined by the MixColumns cores.
- 70 cores are used for this implementation
Optimization I: Increasing Throughput

- Cores running *MixColumns* workloads are 2x slower than other cores, which are the bottlenecks of the design.
- Parallelize each *MixColumns* core into two *MixCol-8* cores
  - Each *MixCol-8* processes two columns (8 bytes) instead of four columns
- Throughput is increased by 43% (152 cycles per block)
  - 10 more cores are required

<table>
<thead>
<tr>
<th>Processor Name</th>
<th>Execution Time for Processing One 128-bit Data Block (Clock Cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubBytes</td>
<td>132</td>
</tr>
<tr>
<td>ShiftRows</td>
<td>38</td>
</tr>
<tr>
<td>MixColumns</td>
<td>266</td>
</tr>
<tr>
<td>AddRoundKey</td>
<td>22</td>
</tr>
<tr>
<td>KeySubWord</td>
<td>56</td>
</tr>
<tr>
<td>KeyRotWord</td>
<td>26</td>
</tr>
<tr>
<td>KeyXOR</td>
<td>56</td>
</tr>
</tbody>
</table>
Optimization II: Reducing Cores

- **Before optimization:**
  - ~22% average IMem usage
  - ~43% average DMem usage

- **Combine the neighboring SubBytes and ShiftRows core into one SubShift core**
  - $T_{\text{EXE}} = 148$ cycles per data block
  - 80% IMem usage and 100% DMem usage

- **Combine the neighboring KeyRotWord and KeyXOR cores into one KeyScheduling core**
  - $T_{\text{EXE}} = 60$ cycles per data block
  - 24% IMem usage and 28% DMem usage

- Further core merging would reduce the throughput of the design or exceed the memory limitations
Optimized Design of AES Cipher

- The optimized cipher achieves a 43% higher throughput (9.5 cycles per data block)
- The optimized design requires 16% fewer cores (59 cores)
- The execution activity of processors for the optimized cipher is more balanced compared with the preliminary design.
Outline

- Advanced Encryption Standard
- Targeted Fine-Grained Many-Core Platform
- Implementations of AES Cipher
- *Comparison with Related Work*
Comparison with Related Work

<table>
<thead>
<tr>
<th>Platform</th>
<th>Method</th>
<th>Tech. (nm)</th>
<th>Area (mm²)</th>
<th>Max Freq. (MHz)</th>
<th>Throughput (cycles/byte)</th>
<th>Scaled Throughput (Mbps)</th>
<th>Scaled Area (mm²)</th>
<th>Scaled Throughput/Area (Mbps/mm²)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pentium 4 561</td>
<td>Bitslice</td>
<td>90</td>
<td>112</td>
<td>3600</td>
<td>16</td>
<td>2492</td>
<td>58.42</td>
<td>42.66</td>
</tr>
<tr>
<td>Athlon 64 3500</td>
<td>Bitslice</td>
<td>90</td>
<td>193</td>
<td>2200</td>
<td>10.6</td>
<td>2299</td>
<td>101</td>
<td>22.76</td>
</tr>
<tr>
<td>Core 2 Duo E6400</td>
<td>Bitslice</td>
<td>65</td>
<td>111</td>
<td>2130</td>
<td>9.19</td>
<td>1854</td>
<td>111</td>
<td>16.70</td>
</tr>
<tr>
<td>Core 2 Quad Q6600 (one core)</td>
<td>Bitslice + SSSE3</td>
<td>65</td>
<td>286/2 = 143</td>
<td>2400</td>
<td>9.32</td>
<td>2060</td>
<td>143</td>
<td>14.41</td>
</tr>
<tr>
<td>Core 2 Quad Q9550 (one core)</td>
<td>Bitslice + SSSE3</td>
<td>45</td>
<td>214/4 = 53.5</td>
<td>2830</td>
<td>7.59</td>
<td>2065</td>
<td>112</td>
<td>18.44</td>
</tr>
<tr>
<td>Core i7 920 (one core)</td>
<td>Bitslice + SSSE3</td>
<td>45</td>
<td>263/4 = 65.75</td>
<td>2668</td>
<td>6.92</td>
<td>2135</td>
<td>133</td>
<td>16.05</td>
</tr>
<tr>
<td>TI C6201</td>
<td></td>
<td>180</td>
<td>NA</td>
<td>200</td>
<td>14.25</td>
<td>311</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>GeForce 8800 GTX</td>
<td>T-Box</td>
<td>90</td>
<td>484</td>
<td>575</td>
<td>NA</td>
<td>11500</td>
<td>252</td>
<td>45.63</td>
</tr>
<tr>
<td>This Work AsAP</td>
<td></td>
<td>65</td>
<td>6.63</td>
<td>1210</td>
<td>9.5</td>
<td>1019</td>
<td><strong>6.63</strong></td>
<td><strong>153.70</strong></td>
</tr>
</tbody>
</table>

- Compared to CPUs, our design achieves 3.6–10.7x higher throughput per chip area
- Compared to DSP, our design achieves 1.5x higher throughput
- Compared to GPU, our design achieves 3.4x higher throughput per chip area
Acknowledgments

- NSF Grant 0430090, 0903549; and CAREER Award 0546907
- SRC GRC Grant 1598, 1971; and CSR Grant 1659
- UC Micro
- ST Microelectronics
- Intel
- Intellasys
- C2S2 Focus Center, one of six research centers funded under the Focus Center Research Program (FCRP), a Semiconductor Research Corporation entity.