A Low-Cost Cryptographic Processor for Security Embedded System

Speaker: Ronghua Lu

Xiaoyang Zeng, Jun Han, Qing Li, Lang Mai, Jia Zhao
Outline

- **Background**
- Hardware Architecture
- Implementation Results
- Conclusions


**Background**

- Cryptographic algorithms are widely used in security embedded systems.

- Several algorithms are need to be implemented together in a single system.

- Cost & flexibility are as crucial as performance in these systems.
Background (Cont’d)

- Two most popular solutions for these systems:
  1) **Software**-based solutions
     - Flexibility (✓) Speed & Throughput (✗)
  2) **SoC**-based solutions
     - Flexibility (✗) Speed & Throughput (✓) cost (✗)

- Cryptographic processors:
  1) Software-like flexibility
  2) Hardware-like performance
  3) Low cost
Outline

- Background
- *Hardware Architecture*
- Implementation Results
- Conclusions
The processor has a common 5-stage pipeline structure.

Special function units (FU) are added to speed up the execution.
Main Data Path of the Processor

- Special purpose registers are added to help the software calculate the parameters.
- Data path is slightly modified to fit the data flow of those algorithms.
- Breaking down the algorithms & using minimum hardware to execute most complicated parts of the algorithm.
Outline

- Background
- Hardware Architecture
- Implementation Results
- Conclusions
## Implementation Results

<table>
<thead>
<tr>
<th>Technology (um)</th>
<th>0.18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency (MHz)</td>
<td>200</td>
</tr>
<tr>
<td>Area (k-gates)</td>
<td>32</td>
</tr>
</tbody>
</table>

![Diagram of a system architecture](image)
Comparison Results

RSA Performance

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>1024-bit RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARM</td>
<td>Secure Core SC200</td>
<td>594ms</td>
</tr>
<tr>
<td>MIPS</td>
<td>SmartMIPS 4KSc</td>
<td>320ms</td>
</tr>
<tr>
<td>NEC</td>
<td>V-WAY32 uPD7921500</td>
<td>436ms</td>
</tr>
<tr>
<td>Ours</td>
<td>Aegis</td>
<td>150ms</td>
</tr>
</tbody>
</table>

AES Performance

Power & Cost
Conclusions

- A low-cost cryptographic processor is proposed.
- The architecture of the processor is RISC-like.
- A SoC testing platform is proposed.
- This low-cost design is very suitable for applications in security embedded systems.
Thank You!

leonrhlu@gmail.com