Performance Analysis of Contemporary Lightweight Block Ciphers on 8-bit Microcontrollers

Sören Rinne, Thomas Eisenbarth, and Christof Paar
Horst Görtz Institute for IT Security
Ruhr-Universität Bochum, Germany
Overview

1. Motivation
   - Embedded Systems
   - Our Platform

2. Implemented Ciphers
   - Overview of Ciphers
   - Implementation Criteria

3. Results and Comparison
   - Code Size
   - Throughput
What are Embedded Systems?

+ = Embedded System

• „Processor hidden in a product“, or
• „A computer that doesn't look like a computer“
• Single purpose device
• Interacts with the world
Is this really important?

Current CPU market by the numbers

- PC and Workstation CPUs (32 .. 64 bit) 2%
- all Embedded CPUs (4 ..32 bit) 98%
Lightweight Ciphers

Motivation:
- Ubiquitous computing evolves
- New lightweight ciphers are being proposed

Main Question:
Are lightweight ciphers able to outperform the AES on constrained devices?
8-bit Atmel AVR processor:
- e.g. ATmega family:
- ~130 instructions, most of them single cycle (RISC architecture)
- 32 general purpose registers of 8 bit size
- 8 - 128 kBytes of program memory (FLASH)
- 1 - 4 kBytes of volatile memory (SRAM)
- several Power Savings modes
Overview

1. Motivation
   • Embedded Systems
   • Our Platform

2. Implemented Ciphers
   • Overview of Ciphers
   • Implementation Criteria

3. Results and Comparison
   • Code Size
   • Throughput
# Discussed Ciphers

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Cipher remark</th>
<th>Presented at</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES(X)</td>
<td>DESX: key whitening</td>
<td>FIPS 46 1976</td>
</tr>
<tr>
<td>(X)TEA</td>
<td>Arithmetic operations only</td>
<td>FSE 1994</td>
</tr>
<tr>
<td>AES</td>
<td>DES successor</td>
<td>FIPS 197 1997</td>
</tr>
<tr>
<td>SEA</td>
<td>Parametric in text, key and processor size</td>
<td>ECRYPT Workshop 2005</td>
</tr>
<tr>
<td>HIGHT</td>
<td>8-bit oriented, high throughput</td>
<td>CHES 2006</td>
</tr>
<tr>
<td>DES-L</td>
<td>Single S-Box design</td>
<td>FSE 2007</td>
</tr>
<tr>
<td>PRESENT</td>
<td>Small outline SPN</td>
<td>CHES 2007</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cipher</th>
<th>DES</th>
<th>DESX</th>
<th>TEA</th>
<th>XTEA</th>
<th>AES</th>
<th>SEA</th>
<th>HIGHT</th>
<th>DES-L</th>
<th>PRESENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block length</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>128</td>
<td>96</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Key length</td>
<td>56</td>
<td>184</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>96</td>
<td>128</td>
<td>56</td>
<td>80</td>
</tr>
<tr>
<td>Rounds</td>
<td>16</td>
<td>16</td>
<td>32</td>
<td>32</td>
<td>10</td>
<td>141</td>
<td>32</td>
<td>16</td>
<td>32</td>
</tr>
</tbody>
</table>
PRESENT

Hard facts:
• 64 Bit block length
• 80 Bit key length
• 32 rounds

Performed operations:
• XOR with key
• 4x4 bit S-Box
• Bit permutation

Designed for hardware implementation
Design Criteria

Major design goal of embedded devices: **Low Costs**

**Security:**
- Lightweight Crypto

**Performance:**
- Small Payloads
- Response Time

**Cost:**
- Device Cost
- Overall System Cost
Implementation Step

Performance:
Response time and availability

Device cost:
small code size \(\rightarrow\) cheaper device

System cost:
wireless devices \(\rightarrow\) power consumption

Execution time is cost in energy storage!!!

We focus on cost: **code size-performance trade off**
Overview

1. Motivation
   • Embedded Systems
   • Our Platform

2. Implemented Ciphers
   • Overview of Ciphers
   • Implementation Criteria

3. Results and Comparison
   • Code Size
   • Throughput
Results - Our Implementations

Ciphers implemented in Assembly language
  • reduces code size
  • yields higher performance

Keep code size small wherever performance is not reduced too much.
  • Keep all states in registers
  • on the fly key scheduling (no SRAM usage)
  • only small LUTs (8-bit S-boxes) that give a good performance – code-size tradeoff
  • no macros (no loop unrolling)
Results – Code Size

- PRESENT
- TEA
- XTEA
- SEA
- DESL
- AES
- DES
- DESX
- HIGHT

Code size [byte]
Results – Throughput

Throughput of Encryption [bit/sec]
Throughput of Decryption [bit/sec]

AES HIGHT TEA SEA XTEA DESL DES DESX PRESENT
Results – Throughput- Code Size Ratio

Throughput-Code size ratio of Encryption
Throughput-Code size ratio of Decryption
Concluding Remarks

Generally AES seems to be the best allround choice.

For small code size (X)TEA and even PRESENT seem to be a decent choice.

Results will be put on the web, together with other implementations for the focused platform:

www.lightweightcrypto.org
Thanks for your attention!

eisenbarth@crypto.rub.de