A VHDL Implementation Of HMAC Using SHA-1 In FPGA

by

Roar Lien and Tapan Desai

Introduction

- HMAC using SHA-1 is a keyed authentication algorithm
- Inputs: 1) Key – up to 64 bytes
  2) Message – less than $2^{64}$ bits (approx 230000TB)
- Output: 160 bit digest
Design Objectives

- High speed execution 1 Gbit/s
- Efficient use of chip area
- Optimized for Xilinx FPGA
- FIPS 180 – 2 compliant

Methodology and Tools

1. Functional simulation
   - Aldec, Active-HDL
   - Xilinx, Foundation Series v. 3.1i

2. Synthesis and Implementation

3. Timing simulation
   - Aldec, Active-HDL

4. Experimental Testing
   - USC-ISI, SLAAC-IV FPGA board
SLAAC-1V

Xilinx FPGA devices

72-bit ring bus (64 bit data + 8 bit control)

User programmed part

Standard interface (PCI interface + control module)

Target FPGA Devices

Xilinx Virtex - XCV 1000

- 0.22 µm CMOS process
- 12 288 CLB slices
- 32 4-kbit block RAMs
- 1 mln equivalent logic gates
- Up to 200 MHz clock

Block RAMs

Configurable Logic Block slices (CLB slices)
Programmable Interconnects
SHA-1 Single Step

Derivation of $K_t$ and $W_t$

<table>
<thead>
<tr>
<th>Step Number</th>
<th>$K_t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[0 \cdot t \cdot 19]$</td>
<td>0x5A827999</td>
</tr>
<tr>
<td>$[20 \cdot t \cdot 39]$</td>
<td>0x6ED9EBA1</td>
</tr>
<tr>
<td>$[40 \cdot t \cdot 59]$</td>
<td>0x8F1BBCDC</td>
</tr>
<tr>
<td>$[60 \cdot t \cdot 79]$</td>
<td>0xCA62C1D6</td>
</tr>
</tbody>
</table>

Value of $K$ as function of $t$.

Derivation of $W_t$ for $t \cdot [0, 15]$

Derivation of $W_t$ for $t \cdot [16, 79]$
SHA-1 Architecture

312 bit data block

Control Unit

Counter

W_t Generator Architecture

data input

count

W_t

XOR

S
Results

♦ Each 512 bit block requires 81 clock cycles
♦ Up to 60 Mhz system clock
♦ Number of CLBs used is 3268 out of 12288~ 26%
♦ Data rate of 0.37 Gbit/s
Conclusion and further work

- Current throughput of the circuit does not meet the design goal of 1 Gbit/s
- May be achieved by loop unrolling and optimization of code
- More efficient use of chip area
- Implementation of HMAC

Acknowledgements

- Dr. Kris Gaj
- Pawel Chodowiec