SHA-1 Core Description

Contents

Version history

Version	Date	Description
v1	2014-04-28	Initial version. The description matches the core as of 2014-04-28.

Table 1: Document version history.

1 Introduction

The SHA-1 core is an implementation of the cryptographic hash function as specified by NIST in FIPS 180-4 [1].

The core is implemented in Verilog 2001 and is designed to be easty to implement in FPGA as well as ASIC technologies.

2 Architecture

Description of the architecture with core, submodules and wrapper.

3 API and Programming Model

Table with the API as specified by the top level wrapper. Table 2 lists all registers supported by the top level wrapper.

Address	Type	Name	Description
0x00	r	name0	
0x01		name1	
0x02		version	
0x10	r/w	ctrl	
0x11	r	status	
0x20	r/w	block0	
0x21	r/w	block1	
0x40	r	digest0	
0x41	r	digest1	

Table 2: The address map for the core.

4 Implementation Notes

The core uses a sliding window with 16 32-bit words for the round word schedule implementation. The block is stored in the window words at start of processing. For round words 16 to 79 the word needed for round processing is calculated on the fly as well as being stored as word 15 in the sliding window. The previous contents in words 1..15 is copied to words 0..14.

4.2 FPGA implementation Results

The core has been implemented in real FPGA platforms using two different Altera FPGA devices. Table 3 shows the implementation details for the FPGA implementations.

Altera Cyclone IV GX	
Number of registers	
Number of LEs	
Max clock frequency	
Altera Cyclone V	
Number of registers	
Number of ALMs	
Max clock frequency	

Table 3: Implementation results in FPGA devices

5 Verification Status

The core contain testbenches for:

- The core
- The core with the top level wrapper
- The W memory scheduler

The testsbenches use test vectors specified by NIST [2].

Testing has been done with the Icarus Verilog simulator [3] as well as ModelSim vy Mentor Graphics [4].

The core has also been tested using the coretest framework [5] in real FPGAs.

A References

[1] National Institute of Standards Technology (NIST). *Secure Hash Standard*. FIPS 180-4. March 4, 2012. http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[2] BLA BLA BLA

[3] BLA BLA BLA

[4] BLA BLA BLA

[5] J. Strombergson. *Coretest*. Part of the Cryptech Project. SUNET, 2014.