Secure Hash Algorithm IP Core

Author: marsgod
marsgod@opencores.org

Rev 1.0
May 16, 2004

Revision History

Rev.	Date	Author	Description
1.0	05/16/2004	marsgod	Initial Release

(This page intentionally left blank)

1

Introduction

This is a collection of SHA(Secure Hash Algorithm) cores. These include SHA-1, SHA-2 algorithms. In another word, these cores can perform following operations:

Core	Type	Message	Digest	Cycles	Note
sha1.v	SHA-1	512	160	81	With NSA fix
sha256.v	SHA-256	512	256	65	
sha512.v	SHA-384	1024	384	97	
sha512.v	SHA-512	1024	512	97	

These cores are non-pipelined version of SHA, and have simple interfaces with the host side. Some features of the cores:

- Support SHA-1(160), SHA-2(256/384/512)
- Use a simple 32-bit I/O bus interface
- High performance
- Share hardware between different SHA processing
- Can operate up to 200MHz at 0.18um Standard cell design

These cores have been verified with Shamus Software Ltd's MIRACL. You can get this software library from http://indigo.ie/~mscott/.

NOTE: The padding are not implemented in these cores, it is the host's job to do the message padding.