

UNIVERSITÀ DEGLI STUDI DI BOLOGNA
FACOLTÀ DI INGEGNERIA
Corso di Laurea Magistrale in Ingegneria Informatica



Progetto VHDL di Calcolatori Elettronici M

Implementazione della funzione hash crittografica SHA-1 su FPGA

Progetto di:

Francesco Ongaro

Professori:

Prof. Giovanni Neri

Prof. Stefano Mattoccia

Anno Accademico 2011 - 2012

Indice

Introduzione.....	1
Capitolo 1. Hash e meccanismi crittografici.....	2
Capitolo 2. Evoluzione delle funzioni hash.....	6
Capitolo 3. SHA-1.....	8
3.1 Caratteristiche.....	8
3.1.1 Osservazioni.....	10
3.2 Algoritmo.....	10
3.2.1 Metodo alternativo.....	15
Capitolo 4. Implementazione in VHDL.....	16
4.1 File di configurazione.....	18
4.2 Message Schedule component.....	19
4.2.1 Testbench.....	23
4.3 Round Processor component.....	25
4.3.1 Testbench.....	30
4.4 Sha component.....	32
4.4.1 Individuazione del tipo di padding.....	32
4.4.2 Calcolo del numero totale di blocchi.....	33
4.4.3 Gestione del blocco finale.....	34
4.4.4 Schematico.....	41
4.4.5 Testbench.....	43
4.5 Sintesi su FPGA.....	46
4.5.1 Throughput.....	47

Capitolo 5. Conclusioni e sviluppi futuri.....	49
Appendice A. Alcuni esempi testati.....	50
Esempio 1. FIPS.....	50
Esempio 2. FIPS.....	51
Esempio 3.	52
Esempio 4.	53
Esempio 5.	54
Riferimenti Bibliografici.....	55

Introduzione

Questo progetto ha come obiettivo quello di implementare in linguaggio VHDL la funzione hash crittografica SHA-1.

Nel primo capitolo si forniscono i principali aspetti legati alle funzioni hash e ai meccanismi crittografici in cui esse sono utilizzate. Inoltre si forniscono dettagli relativi all'utilizzo di tali funzioni con riferimento alla normativa italiana e alle specifiche tecniche europee di riferimento.

Il secondo capitolo invece fornisce un quadro sulle varie evoluzioni delle funzioni hash, specificando i dettagli principali di ognuna di esse.

Il terzo capitolo approfondisce la funzione hash crittografica SHA-1, oggetto di questo progetto, presentando, nel quarto capitolo, l'implementazione vera e propria nel linguaggio VHDL.