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

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.