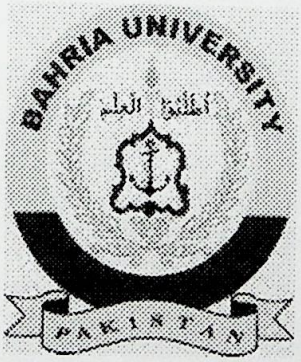
MCS Project Report

"Hashing in Hardware"

by

Shamaila Masood

Enrollment No: 141022-036



Supervised by

Mr. Jehanzaib Ahmad

Department of Computer Sciences
Bahria Institute of Management and Computer Sciences, Islamabad
Bahria University Islamabad

APPROVALS

We accept the work contained in this report as a confirmation to the required standard for the fulfillment of the MCS degree.

Mr. Fazal Wahab
Head of Department

Mr. Jehanzaib Ahmed
Supervisor

Mr. Shaftab Ahmed
Internal Examiner

Prof. Dr. Irfan Zafar
External Examiner

Acknowledgement

I would like to thank Mr. Jehanzaib Ahmad for his sincere support and advice for making it possible to complete the project and also for providing with all the required material . I would also like to express my sincere gratitude to Mr. Fazal-e-Wahab (Head of Department Computer sciences). I am obliged to Ms. Nazish Hayat for her support and encouragement.

Shamaila Masood

Table Of Contents

INTRODUCTION 6
LITERATURE SURVEY 9
PROPOSED SYSTEM & IMPLEMENTATION 20
EXPLANATION OF VERILOG CODE 31
CONCLUSIONS 34
BIBLIOGRAPHY 35

Table of figures

▼ Figure 1 : Block view of hashing circuitary 20
▼ Figure 2 : Flow of information in DES 21
▼ Figure 3 : Cipher function 22
▼ Figure 4 : Optimized Cipher function 23
▼ Figure 5 : random generator 24
▼ Figure 6 : random generator memory module 24
▼ Figure 7 : random generator controller 25
▼ Figure 8 : random generator overall design 26
▼ Figure 9 : hash key generator 27
▼ Figure10 : hash table bit distribution 28
▼ Figure 11 : linear probing state machine 30

Introduction

Hardware Description Languages

Digital systems are highly complex. At their most detailed level, they may consist of millions of elements, e.g., transistors or logic gates. For many decades, logic schematics served as the *lingua franca* of logic design, but not any more. Today, hardware complexity has grown to such a degree that a schematic with logic gates is almost useless, as it shows only a web of connectivity and not the functionality of design. Since the 1970s, computer engineers and electrical engineers have moved toward hardware description languages (HDLs). The most prominent HDLs in industry are Verilog and VHDL. Verilog is the top HDL used by over 10,000 designers at such hardware vendors as Sun Microsystems, Apple Computer and Motorola. Industrial designers prefer Verilog. The syntax of Verilog is based on the C language, while the syntax of VHDL is based on Ada. A free Verilog simulator is available from SynaptiCAD, Inc. For Windows 95/NT, Windows 3.1, Macintosh, SunOS and Linux platforms, they offer FREE versions of their VeriWell product, which is available from http://www.syncad.com/ver_down.htm. The free versions are the same as the industrial versions except they are restricted to a maximum of 1000 lines of HDL code.

Verilog HDL

Verilog HDL is a hardware description language used to design and document electronic systems. Verilog HDL allows designers to design at various levels of abstraction. It is the most widely used HDL with a user community of more than 50,000 active designers.
Verilog was invented as simulation language. Use of Verilog for synthesis was a complete afterthought.

The Verilog language provides the digital designer with a means of describing a digital system at a wide range of levels of abstraction, and, at the same time, provides access to computer-aided design tools to aid in the design process at these levels. Verilog allows hardware designers to express their design with behavioral constructs, deferring the details of implementation to a later stage of design in the design. An abstract representation helps the designer explore architectural alternatives through simulations and detect design bottlenecks before detailed design begins.