UNIVERSITI MALAYSIA PERLIS
SCHOOL OF MICROELECTRONIC ENGINEERING

RANDOM NUMBER GENERATOR SIMULATION AND DIGITAL IC DESIGN FROM INVERSE CONGRUENTIAL ALGORITHM

by

AHMAD FIRDAUS BIN MOHAMAD RAZY

Thesis for the degree of Microelectronic Engineering

May 2011

UNIVERSITI MALAYSIA PERLIS
PUSAT PENGAJIAN KEJURUTERAAN MIKROELEKTRONIK

ABSTRAK

SIMULASI PENJANA NOMBOR RAMBANG DAN MEREKABENTUK DIGITAL IC DARI *INVERSE CONGRUENTIAL* ALGORITMA

oleh AHMAD FIRDAUS BIN MOHAMAD RAZY

Penjana nombor rambang adalah penghasilan rangkaian nombor rawak, di mana ia berdasarkan algoritma nombor rambang yang akan menghasilkan rangkaian nombor yang tidak boleh diramal. Penyelidikan ini menerangkan simulasi penjana nombor rambang dari beberapa algoritma nombor rambang, dan merekabentuk nombor rambang digital dari algoritma *Inverse Congruential* untuk tujuan penggunaan kriptografi. Dalam penyelidikan ini beberapa algoritma nombor rambang telah dipilih berdasarkan algoritma nombor rambang palsu, yang akan di simulasi oleh penganalisis simulasi teori. Penganalisis simulasi teori akan menghasilkan keputusan taburan data dan pola data nombor rawak. Keputusan itu mewakili penentuan rangkaian data serta pola data yang dihasilkan oleh nombor rawak. Selain itu algoritma *Inverse Congruential* akan diuji dengan penguji *NIST* untuk mengetahui tahap rawak rangkaian. Algoritma yang diuji dengan penguji *NIST* adalah algoritma yang terpilih dari penganalisis simulasi teori. Hasil ujian telah menunjukkan rangkaian nombor rawak secara linear adalah kompleks dan telah mencapai 13.75% tahap yang tidak dapat diramalkan. Tujuan merekabentuk penjana nombor rambang litar bersepadu digital adalah untuk mengurangkan saiz peralatan nombor rambang, dan pada masa yang sama mengurangkan penggunaan tenaga elektrik serta murah dalam penghasilan produk, berbanding penggunaan peralatan nombor rambang sekarang yang sedia maklum memerlukan kos yang tinggi bagi tujuan pembangunan kriptografi.

UNIVERSITI MALAYSIA PERLIS
SCHOOL OF MICROELECTRONIC ENGINEERING

ABSTRACT

RANDOM NUMBER GENERATOR SIMULATION AND DIGITAL IC DESIGN FROM INVERSE CONGRUENTIAL ALGORITHM

by AHMAD FIRDAUS BIN MOHAMAD RAZY

Random number generator is a generation of random number sequence based on random number algorithm, which will produce an unpredictable number of a sequence. This study describes the random number generator simulation for several random number algorithms and designing digital IC random number from Inverse Congruential algorithm for cryptography purpose. In this investigation, the several random number algorithms are selected based on pseudorandom number algorithm and are simulated by theoretical simulator analysis. The theoretical simulation analysis will show result of random number distribution data and random number pattern data. The results indicate of deterministic of sequences and pattern of generating random number. NIST tester is included in this project to evaluate the randomness of a sequence. The algorithm that was selected is Inverse Congruential algorithm based on the performance in theoretical simulation analysis. The test showed that the random number sequences for this algorithm achieved 13.75% of randomness. Meanwhile, result from NIST tester showed that, this algorithm has appeared high in linear complexity. The design of digital IC random number generator was purposely to reducing size of random number generator hardware, and at same time consumes low power and also cheaper in production cost compared to current random number generator hardware that need high cost for cryptographic development.

Contents

Abstrak ii

Abstract iii

List of tables vii

List of figures viii

Declaration of Authorship ix

Acknowledgement x

Chapter 1 Introduction 1

1.1 Project Background 1
1.2 Objectives 3
1.3 Scope of Project 3
1.4 Problem Statement 3
1.5 Chapter Outlines 4

Chapter 2 Literature Review 5

2.1 Random Number Generator 5
2.2 Pseudorandom Number Generator 6
2.3 Digital Random Number Generator 7
2.4 Pseudorandom Number Generator Algorithms 8
2.4.1 Linear Congruential Generator 8
2.4.2 Multiply with Carry Generator 9
2.4.3 Complimentary Multiply with Carry Generator 10
2.4.4 Additive Lagged Fibonacci Generator 11
2.4.5 Park Miller/Lehmar Random Number Generator 12
2.4.6 Blum Blum Shub Generator 13
2.4.7 Linear Feedback Shift Register Generator 14
2.4.8 Inverse Congruential Generator 15
2.5 Random Number Generator Criteria 17

Chapter 3 Methodology 18

3.1 Introduction 18
3.2 Random Number Algorithm Theoretical Simulator 20
3.2.1 Microsoft Office Excel 2007 20
3.2.2 Theoretical Simulator Process 21
3.3 Random Number Generator Program 23
3.4 NIST Test 26
3.5 Digital Random Number Generator Design 27
3.5.1 Quartus II 9.0sp2 Web Edition 27
3.5.2 Digital Random Number Generator Design 28

Chapter 4 Result and Discussion 30

4.1 Introduction 30
4.2 Theoretical Test 31
4.2.1 Linear Congruential Generator 31
4.2.2 Multiply with Carry Generator 32
4.2.3 Complimentary Multiply with Carry Generator 33
4.2.4 Additive Lagged Fibonacci Generator 34
4.2.5 Park Miller / Lehmar Generator 35
4.2.6 Blum Blum Shub Generator 36
4.2.7 Linear Feedback Shift Register Generator 37
4.2.8 Inverse Congruential Generator 38
4.3 Inverse Congruential Algorithm Program Design 40
4.4 NIST Tester 43
4.5 Digital Inverse Congruential Random Number Generator Design 49

Chapter 5 Conclusion 54

5.1 Summary 54
5.2 Recommendation for future project 55
5.3 Commercialization Potential 55

Appendix A Theoretical Simulation Analysis

A.1 Linear Congruential Generator
A.2 Multiply with Carry Generator
A.3 Complimentary Multiply with Carry Generator
A.4 Additive Lagged Fibonacci Generator
A.5 Park Miller / Lehmar Generator
A.6 Blum Blum Shub Generator

A.7 Linear Feedback Shift Register Generator
A.8 Inverse Congruential Generator
A.9 Euclid's Algorithm

Appendix B Inverse Congruential Generator Program

B.1 Inverse Congruential Generator Program (Seed=7)
B.2 Inverse Congruential Generator Program (Seed=17)
B.3 Inverse Congruential Generator Program (Seed=23)
B.4 Inverse Congruential Generator Program (Seed=37)
B.5 Inverse Congruential Generator Program (Seed=49)

Appendix C NIST Test Analysis

C.1 Parameterized Test
C.2 Non-Parameterized Test
C.3 Non-Overlapping Templates

Appendix D Digital Inverse Congruential Generator Design

D.1 Verilog HDL Design
D.2 RTL Netlist Viewer
D.3 Technology Map Viewer – Post Mapping

Appendix E Technical Review Paper

Appendix F Technical Paper

References 143

List of tables

Table 4.1 Inverse Congruential Generator Program Properties 43
Table 4.2 NIST Tester Properties 43
Table 4.3 NIST Parameterized Test Result 44
Table 4.4 NIST Non-Parameterized Test Result 46
Table 4.5 Digital Random Number Generator Simulation Configuration 50

List of figures

Figure 3.1 Flow chart of project 19
Figure 3.2 Algorithm Theoretical Simulator by using Microsoft Office Excel 2007 20
Figure 3.3 Flow chart of Theoretical Simulator process for each algorithm 21
Figure 3.4 Table of algorithm result at Microsoft Office Excel 2007 22
Figure 3.5 Flow chart of Random Number Generator program 23
Figure 3.6 Bloodshed Dev C++ software 24
Figure 3.7 Command Prompt platform 25
Figure 3.8 NIST Statistical Test Suite 26
Figure 3.9 Quartus II 9.0sp2 Web Edition software 27
Figure 3.10 Flow chart of Digital Random Number Generator design 29
Figure 3.11 Example of waveform output 29
Figure 4.1 Linear Congruential Generator data distribution 31
Figure 4.2 Linear Congruential Generator data pattern 31
Figure 4.3 Multiply with Carry Generator data distribution 32
Figure 4.4 Multiply with Carry Generator data pattern 32
Figure 4.5 Complimentary Multiply with Carry Generator data distribution 33
Figure 4.6 Complimentary Multiply with Carry Generator data pattern 33
Figure 4.7 Additive Lagged Fibonacci Generator data distribution 34
Figure 4.8 Additive Lagged Fibonacci Generator data pattern 34
Figure 4.9 Park Miller Generator data distribution 35
Figure 4.10 Park Miller Generator data pattern 35
Figure 4.11 Blum Blum Shub Generator data distribution 36
Figure 4.12 Blum Blum Shub Generator data pattern 36
Figure 4.13 Linear Feedback Shift Register Generator data distribution 37
Figure 4.14 Linear Feedback Shift Register Generator data pattern 37
Figure 4.15 Inverse Congruential Generator data distribution 38
Figure 4.16 Inverse Congruential Generator data pattern 38
Figure 4.17 Euclid's Algorithm data distribution 39
Figure 4.18 Euclid's Algorithm Generator data pattern 39
Figure 4.19 Inverse Congruential Generator Program design flowchart 40
Figure 4.20 Inverse Congruential Generator Program output in binary form 41
Figure 4.21 Inverse Congruential Generator Program output in decimal form 41
Figure 4.22 Inverse Congruential Generator Program output in hexadecimal form 42
Figure 4.23 Digital Inverse Congruential Generator Design waveform 1 51
Figure 4.24 Digital Inverse Congruential Generator Design waveform 2 52
Figure 4.25 Digital Inverse Congruential Generator Design waveform 3 53

Declaration of Authorship

I, Ahmad Firdaus Bin Mohamad Razy, declare that the thesis entitled Random Number Generator Simulation and Digital IC Design from Inverse Congruential Algorithm and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was done wholly or mainly while in candidature for a bachelor degree at Universiti Malaysia Perlis;
- where any part of this thesis has previously been submitted for a degree or any other qualification at Universiti Malaysia Perlis or any other institution, this has been clearly stated;
- where I have consulted the published work of others, this is always clearly attributed;
- where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;

Signed:.....
Date:.....

Acknowledgement

I would like to express my sincere appreciation to my supervisor, Mrs Siti Zarina Naziri and Mr Mohd Fairus Ahmad, who has the attitude and the substance of a intelligence; their continually and convincingly conveyed a spirit of adventure in regard to research and an excitement in regard to teaching. Without their guidance and persistent help this dissertation would not have been possible.

Special thanks to all Microelectronic Engineering staff that always gives helps for me with information and application of software. Not forgotten to our committee members of Final Year Project in Microelectronic Programme. They always give full commitment to make the student achieved wonderful experience in their final year project.

In addition, thank you to my friend, who always support me in deepen experience of a programmer design. Who also gives me the solution and idea every time when I face new problems in term of design.

Finally, I would like to thanks my family which always encourages me traverse the challenge in final year project with motivating me. Special thanks go to my parent, they always reminded me about the important of accomplishing Final Year Project and this is one of the turning points for my future profession as a Microelectronic Engineer.