UNIVERSITI MALAYSIA PERLIS
SCHOOL OF MICROELECTRONIC ENGINEERING

THE DESIGN OF AN ENCRYPTION CHIP USING VIGENÈRE CIPHER

by

Tan Shih Peng

Thesis in partial fulfillment of
requirements for the Degree of
Bachelor of Electronic Engineering

April 2011

UNIVERSITI MALAYSIA PERLIS

SCHOOL OF MICROELECTRONIC ENGINEERING

ABSTRAK

REKAAN SEBUAH CIP ENKRIPSI MENGGUNAKAN VIGENERE CIPHER

oleh Tan Shih Peng

Projek ini mencadangkan pelaksanaan peranti keras pada sebuah algoritma Vigenère cipher yang diubahsuai. Pengubahsuaian algoritma Vigenère terdiri daripada plaintext tersebar disulitkan dengan pseudorawak sesi kunci secara simetris. Kunci utama kemudian disulitkan menggunakan teknik enkripsi asimetris. Kombinasi algoritma enkripsi simetri dan asimetri mencapai keselamatan mesej dan kunci semasa penghantaran kepada penerima. Perekaan ini ditulis dalam kod HDL Verilog disintesis, dan ciphertext disahkan melalui dekripsi kepada mesej asal. Peranti keras menggunakan 3,215 elemen lojikal pada cip FPGA Altera Cyclone II dan beoperasi pada 10.76 MHz.

April 2011

UNIVERSITI MALAYSIA PERLIS

SCHOOL OF MICROELECTRONIC ENGINEERING

ABSTRACT

THE DESIGN OF AN ENCRYPTION CHIP USING VIGENÈRE CIPHER

by Tan Shih Peng

This project proposes a hardware implementation of a modified Vigenère cipher algorithm. The modified Vigenère algorithm comprises of a diffused plaintext encrypted with a pseudorandom session key generator symmetrically. The master key then is encrypted using asymmetric encryption technique. The combination of symmetric and asymmetric encryption algorithm achieves security of the message and the key during transfer to the receiver. The design is written in synthesizable Verilog HDL code and the ciphertext is verified through decryption of itself to obtain the original message. The hardware resource consumes 3,215 LEs on an Altera CycloneII FPGA chip and operates at 10.76 MHz.

Contents

List of Tables

List of Figures

Declaration of Authorship

I, TAN SHIH PENG, declare that the thesis entitled THE DESIGN OF AN ENCRYPTION CHIP USING VIGENÈRE CIPHER 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 this University;

- where any part of this thesis has previously been submitted for a degree or any other qualification at this University 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: 20/4/11

Acknowledgement

I am heartily thankful to my supervisors, Siti Zarina Md Naziri and Mohd Fairus Bin Ahmad, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

The lessons and experience gained over this two semesters has been immeasurable.

Lastly, I offer my regards and blessings to all of those who supported me in any respect and patiently gave me their time in all of my case studies during the completion of the project.

Despite the geographical distance, my family was always nearby. My mother made sure I felt her confidence and encouragement, and his advice was consistently timely and useful.

Shih Peng Tan

Nomenclature

PT	Plaintext
CT	Ciphertext
K	Encryption/Decryption Key (for symmetric encryption)
N	Modulus of asymmetric encryption
E	Encryption key, public key (for asymmetric encryption)
D	Decryption key, secret key (for asymmetric encryption)
Mod	Mathematical representation of modulus
LE	Logical element