A BIOMETRIC ENCRYPTION SYSTEM
ALGORITHM DEVELOPMENT AND SYSTEM LEVEL DESIGN

RABIA BAKHTERI

UNIVERSITI TEKNOLOGI MALAYSIA

A BIOMETRIC ENCRYPTION SYSTEM
ALGORITHM DEVELOPMENT AND SYSTEM LEVEL DESIGN

RABIA BAKHTERI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Electrical Engineering)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

AUGUST 2011

Dedicated to my beloved mother and father

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my mentor and PhD advisor, Prof. Dr. Mohamed Khalil Hani for giving me the opportunity to work with him and for all his advice and guidance on how to perform research and academic writing. The lessons of life that he taught me throughout my doctoral studies will stay with me always. I am also grateful for the TechnoFund grant provided by the Ministry of Science, Technology and Innovation that funded this research work.

I am indebted to the other lecturers in the VeCAD group especially Dr. Nadzir Marsono, Dr. Sheikh Nasir and Dr. Ooi Chia Yee for their guidance and support. I am most grateful to my senior, Dr. Hau Yuan Wen who acted as a guide and friend throughout the years.

I would also like to thank my research colleagues, Ilyasak, Syafeeza, Vishnu, Pei Chee, Andy, Annuar and Sathi for their help and assistance. They have been most pleasant company and my graduate life has been most enjoyable and unforgettable thanks to them.

Most of all, I would like to express my gratitude to both of my parents and my three siblings. Without their unwavering love and support, I would not have been able to even begin this journey.

ABSTRACT

Biometric encryption (BE) is a security scheme enhancement that overcomes the exploitable vulnerabilities of biometric authentication systems and the key storage issues of cryptographic schemes by combining both those systems. The practical application of security schemes often requires them to be stand-alone devices with tamper-resistant hardware implementation such as a System-on-Chip (SoC). Therefore, it is suitable to design a BE system architecture that is enhanced for speed and performance in a resource-constrained environment. This thesis proposes a novel algorithm for chaff generation (CG), which is a highly compute-intensive algorithm in the BE system. The proposed CG algorithm is suitable for hardware implementation in an SoC because it is proven to have lower algorithmic complexity of $O(n^2)$ compared to the existing Clancy's CG algorithm that has $O(n^3)$ complexity. Experimental results have shown that the proposed algorithm is about 150 times faster. Furthermore the proposed CG algorithm overcomes the security vulnerability detected in Clancy's CG algorithm. The design of such a complex system, which contains many compute-intensive algorithmic blocks, requires consideration of multiple options for system architecture, optimal hardware-software partitioning and early design verification. Hence, state-of-the-art system-level modeling using SystemC is applied in the design of the proposed BE system. In this thesis, the system-level design process has been enhanced by adding the Algorithmic Model level on top of the existing design abstraction levels. To verify the functionality of the BE design, appropriate testbenches must be generated and refined along with the system model throughout the different design abstraction levels. For this purpose, a new verification framework with a testbench generation methodology is also proposed, which generates testbench at the algorithmic level using MATLAB and incrementally refines it for use at lower levels of the design abstraction. This framework is applied in the early system-level verification of the proposed BE system. Experiments conducted have also shown that the proposed verification framework that integrates MATLAB testbenches with SystemC facilitates the verification process and reduces verification time through testbench refinement.

ABSTRAK

"*Biometric Encryption*" (BE) merupakan peningkatan sistem sekuriti yang mengatasi kerentanan yang boleh dieksploitasi dalam sistem pengesahan biometrik dan isu penyimpanan kunci dalam skim kriptografi dengan menggabungkan kedua-dua sistem tersebut. Aplikasi praktikal bagi sistem sekuriti memerlukan peranti mandiri dengan implementasi perkakas seperti "*System-on-Chip*" (SoC). Oleh itu, sistem BE sesuai dibina dengan senibina yang berprestasi dan kelajuan tinggi dalam persekitaran sumber-terhad. Tesis ini mencadangkan satu algoritma baru untuk kaedah "*Chaff Generation*" (CG), iaitu salah satu algoritma yang intensif dalam sistem BE. Algoritma CG tersebut sesuai untuk diimplementasi sebagai perkakas kerana telah dibuktikan mempunyai kompleksiti yang rendah iaitu $O(n^2)$ berbanding dengan algoritma CG Clancy yang mempunyai kompleksiti $O(n^3)$. Hasil eksperimen menunjukkan CG yang dicadang adalah 150 kali lebih pantas. Tambahan pula, algoritma cadangan juga mengatasi kerentanan sekuriti yang terdapat dalam CG cadangan Clancy. Proses merekabentuk sistem yang kompleks di mana ia mengandungi blok-blok algoritma yang intensif memerlukan pertimbangan daripada pelbagai pilihan merangkumi senibina sistem, pembahagian perkakasan-perisian yang optimum dan penentusahan awal. Oleh itu, pemodelan tahap sistem yang canggih menggunakan "*SystemC*" telah diaplikasikan di dalam rekabentuk sistem BE yang dicadang. Dalam tesis ini, proses rekabentuk tahap sistem telah dipertingkatkan dengan menambah tahap model algoritma di atas tahap-tahap peniskalan rekabentuk sedia ada. Aturcara penguji yang bersesuaian perlu dihasilkan dan diperhalusi mengikut model sistem untuk mengesahkan fungsi rekabentuk sepanjang tahap peniskalaan rekabentuk yang berbeza-beza. Bagi tujuan ini, satu rangka kerja baru untuk penentusahan bersama dengan satu kaedah penghasilan aturcara penguji telah dicadangkan yang menghasilkan aturcara penguji pada tahap algorithma menggunakan MATLAB dan lebih diperhalusi untuk penggunaan pada tahap peniskalaan rekabentuk yang lebih rendah. Rangka kerja ini diaplikasikan untuk penentusahan fungsi pada tahap sistem BE yang dicadangkan. Eksperimen telah menunjukkan bahawa rangka kerja penentusahan yang menggabungkan aturcara penguji dalam "*MATLAB*" dengan "*SystemC*" menyokong kerja pengesahan dan mengurangkan masa penentusahan melalui proses perhalusan aturcara penguji.