UNIVERSITI TEKNOLOGI MARA

AN ANALYSIS OF THE AA_B ASYMMETRIC ENCRYPTION SCHEME ON EMBEDDED DEVICES FOR IOT ENVIRONMENT

SYED FARID BIN SYED ADNAN

Thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Electrical Engineering)

Faculty of Electrical Engineering

December 2019

AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student : Syed Farid bin Syed Adnan

Student I.D. No. : 2014245398

Programme : Doctor of Philosophy in Electrical Engineering – EE950

Faculty : Electrical Engineering

Thesis Title : An Analysis of the AA*β* Asymmetric Encryption Scheme on Embedded Devices for IoT Environment

Signature of Student : ……………………………………………………..

Date : December 2019

ABSTRACT

Lightweight cryptography offers energy-efficient cryptographic capabilities on low powered devices such as those commonly found in the Internet of Things (IoT). One such lightweight scheme is the AA-Beta (AA_{β}) asymmetric cryptographic scheme whose algorithm consists of only basic arithmetic operations of addition and subtraction for both the encryption and decryption processes. These features resulted in faster runtime compared to the more established RSA asymmetric encryption scheme, making AA_{β} a potential alternative for IoT security. At the time of writing this thesis, AA_{β} algorithm still exists as a mathematical concept and proven in a mathematical based software. To date, this research found no known practical implementation of the AA_{β} algorithm to prove or to validate its efficiency on a real-world computing platform. There has been no analysis of the AA_{β} performance on any resource-constrained platform although previous mathematical simulations showed that it would perform well in resource-constrained platforms. It is also not known how the algorithm would perform against the widely used RSA on resource-constrained platforms. This thesis seeks to study the AA_{β} design philosophy and the specifications of the AA_{β} asymmetric encryption scheme, develop the AA_{β} encryption scheme and evaluate the computational speed, power consumption and feasibility of AA_{β} encryption scheme on an embedded system in the practical domain. The results from the study are being compared to the mathematical simulation, and experimentally, to the RSA. This investigation takes the form of an IoT environment, beginning with an in-depth examination of the AA_{β} encryption scheme design, and continuing into the development and real-world application of AA_{β} from its mathematical origin. The experimental analysis focused on the AA_{β} algorithm's performance on embedded platforms, namely, the Raspberry Pi microcomputer and microcontroller (ARM Cortex-M7) platforms. A feasibility assessment for an AA_{β} cryptosystem for sensor nodes including a client to server testbed with wireless communications was carried out in the final stage. In this research work, the performance analysis of the AA_{β} scheme produced remarkable timing improvements for the encryption and decryption of messages when compared to previous trials on a numeric computing environment. The research goes on to compare the energy consumptions for encryption and decryption using the AA_{β} scheme with similar processes using the Textbook RSA scheme on the aforesaid embedded platforms. The AA_{β} encryption process demonstrates a significantly lower energy consumption compared to RSA, where as much as three times less energy was used by AA_{β} when encrypting messages while considerable energy savings were also seen during AA_{β} message decryption on the Raspberry Pi 2 and ARM Cortex-M7 device. A conclusion can thus be made that the AA_{β} encryption scheme is a cryptographic scheme with a great potential for deployment on low-powered devices especially at the encryption side, offering fast and energy-efficient asymmetric cryptographic capabilities to all devices.

ACKNOWLEDGEMENT

Alhamdulillah, praise to Allah for His blessings and mercy, for me to complete this work.

First and foremost, I would like to thank Professor Ir. Dr. Habibah Hashim, my main supervisor for her endless help and motivation towards the journey of completing this thesis. I could not imagine of having a better advisor for my PhD study. Not to forget my co-supervisor, Ir. Dr. Yusnani Yusoff for her support on this PhD journey. Besides that, I would thank Dr Anuar Mat Isa for his kind help during this journey and to all InSTIL Lab members.

I would like to thank to my family for their never-ending support during this journey. I dedicated this thesis to my mom Salina and my father, Syed Adnan, my beloved wife Eryani and mostly to my kids Zhorif, Sarah and Sofiyyah.

TABLE OF CONTENTS