UNIVERSITI PUTRA MALAYSIA

CRYPTOGRAPHIC PROTECTION OF BLOCK-ORIENTED STORAGE DEVICES USING AES-XTS IN FPGA

SHAKIL AHMED

CRYPTOGRAPHIC PROTECTION OF BLOCK-ORIENTED STORAGE DEVICES USING AES-XTS IN FPGA

By

SHAKIL AHMED

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Doctor of Philosophy

October 2013

COPYRIGHT

To my late mother Rashida Bashir,
To my father, my brothers, my sisters.
Finally, To All whom I love.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Doctor of Philosophy

CRYPTOGRAPHIC PROTECTION OF BLOCK-ORIENTED STORAGE DEVICES USING AES-XTS IN FPGA

By

SHAKIL AHMED

October 2013

Chairman: **Khairulmizam Bin Samsudin, PhD**
Faculty: **Engineering**

In recent years security has been a common concern for the data in-transit between communication networks as well as data at-rest in storage devices. Storage encryption (data at-rest) has now become an important aspect in today's computing environment. User data stored in computing devices that includes computers, personal digital assistant (PDA), flash drives and external hard drive are getting vulnerable to security attacks. Keeping this in view, IEEE P1619 Security in Storage Working Group (SISWG) proposed a standard for security of static data. One of the components of this standard is the cryptographic protection of data on block-storage devices. This standard uses AES-XTS as a building block for the protection of data. For an effective storage encryption implementation, two well known methods are software based encryption and hardware based encryption.

Software based encryption is relatively slow, consumes more power and also not secure but one of its advantage is that is economically feasible. Hardware based encryption are more secure since it is embedded into the drive and cannot be altered easily compared to software based encryption. At the same time, efforts have been made for the standardization of hardware-based encryption that could promote interoperability between products. Implementations based on hardware are further categorized into two; Application Specific Integrated Circuits (ASICs) and FPGAs (Field Programmable Gate Arrays). FPGAs offer several advantages in comparison to ASICS which are its time to market and overall cost. Although ASIC implementation of Hard disk drives (HDDs) could be more cost effective for high volume production and more enhanced performance but our work is targeting an initial level of implementation on FPGA whose initial cost of manufacturing is almost negligible.

In this thesis, different FPGA implementations of AES-XTS are proposed. First we present our sub-module optimizations with the comparison to other existing sub-modules. These designed sub-modules namely substitution box, TBOX and tweak value computation, were optimized in terms of area being utilized by FPGA. These different

sub-modules were then integrated into different AES-XTS designs. Four different kind of designs namely iterative, iterative based memory, parallel and pipelined designs were given. These different designs were being compared in terms of several performance parameters to few available AES-XTS designs to date.

In order to implement the designs Xilinx ISE webpack software was used, a well known FPGA simulator. Several parameters are being measured and compared to show the performance of implemented designs. In addition AES-XTS decryption modules were also designed. Also the parallel AES-XTS encryption and decryption design were used to develop integrated chip of AES-XTS on FPGA. The results show that pipelined implementation has outperformed all other implementations. In terms of throughput, the pipelined implementation has shown an improvement of 7.5% to that of unrolled parallel design and about 10 fold increase to iterative design. Further the proposed designs have provided comparative solution for currently available AES-XTS designs which showed significant improvements. The pipelined algorithm has provided an improvement of around 2.8 fold increase in efficiency (Mbps/Slice) to current AES-XTS available design. Also Integrated AES-XTS core has shown an improvement of around 2.4 fold increase in efficiency (Mbps/Slice) to existing AES integrated designs.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Doktor Falsafah

CRYPTOGRAPHIC PROTECTION OF BLOCK-ORIENTED STORAGE DEVICES USING AES-XTS IN FPGA

By

SHAKIL AHMED

Oktober 2013

Chairman: **Khairulmizam Bin Samsudin, PhD**
Faculty: **Kejuruteraan**

Dalam tahun-tahun baru-baru ini keselamatan telah menjadi kebimbangan biasa untuk data dalam transit antara rangkaian komunikasi serta data di-rehat dalam peranti storan. Penyulitan penyimpanan (data di-rehat) kini telah menjadi satu aspek penting dalam persekitaran pengkomputeran hari ini. Data pengguna yang disimpan di dalam peranti pengkomputeran yang merangkumi komputer, pembantu digital peribadi (PDA), flash drive dan cakera keras luaran semakin terdedah kepada serangan keselamatan. Menjaga pandangan ini, IEEE P1619 Keselamatan dalam Kumpulan Kerja Penyimpanan (SISWG) mencadangkan satu standard untuk keselamatan data statik. Salah satu komponen standard ini adalah perlindungan kriptografi data pada peranti blok-simpanan. Standard ini menggunakan AES-XTS sebagai blok bangunan untuk perlindungan data. Untuk pelaksanaan penyulitan storan berkesan, dua kaedah terkenal adalah penyulitan berasaskan perisian dan penyulitan berasaskan perkakasan.

Penyulitan berasaskan perisian adalah agak perlahan, menggunakan lebih banyak kuasa dan juga tidak selamat tetapi salah satu kelebihan adalah yang dilaksanakan dari segi ekonomi. Penyulitan berasaskan perkakasan adalah lebih selamat kerana ia tertanam ke dalam pemacu dan tidak boleh diubah dengan mudah berbanding dengan penyulitan berasaskan perisian. Pada masa yang sama, usaha-usaha telah dibuat bagi piawaian penyulitan perkakasan berasaskan yang boleh menggalakkan interoperability antara produk. Perlaksanaan berdasarkan perkakasan lagi dikategorikan kepada dua; Permohonan Litar Bersepadu Khusus (ASIC) dan FPGAs (Field Programmable Gate Perlengkapan). FPGAs menawarkan beberapa kelebihan berbanding dengan Asics yang masa ke pasaran dan keseluruhan kosnya. Walaupun pelaksanaan ASIC pemacu cakera keras (HDD) boleh menjadi lebih kos efektif untuk pengeluaran yang tinggi dan prestasi yang lebih dipertingkatkan tetapi kerja-kerja kami menyasarkan tahap awal pelaksanaan pada FPGA yang kos pengeluaran awal adalah hampir diabaikan.

Dalam tesis ini, pelaksanaan FPGA berbeza AES-XTS dicadangkan. Mula-mula kita membentangkan pengoptimuman sub-modul kami dengan perbandingan untuk sub-modul lain yang sedia ada. Ini direka sub-modul iaitu kotak penggantian, TBOX dan tweak pengiraan nilai, telah dioptimumkan dari segi kawasan yang digunakan oleh FPGA. Ini berbeza sub-modul kemudiannya disepadukan ke dalam yang berbeza AES-XTS reka bentuk. Empat pelbagai jenis reka bentuk iaitu lelaran, lelaran memori berasaskan, reka bentuk selari dan saluran maklumat yang diberikan. Ini reka bentuk yang berbeza telah dibandingkan dari segi beberapa parameter prestasi yang terdapat AES-XTS reka bentuk terkini.

Dalam usaha untuk melaksanakan reka bentuk Xilinx ISE perisian webpack telah digunakan, FPGA simulator terkenal. Beberapa parameter yang diukur dan dibandingkan dengan menunjukkan prestasi reka bentuk dilaksanakan. Di samping itu modul penyahsulitan AES-XTS juga direka. Juga AES-XTS penyulitan dan penyahsulitan reka bentuk selari telah digunakan untuk membangunkan cip bersepadu AES- XTS pada FPGA. Keputusan menunjukkan bahawa pelaksanaan saluran maklumat telah mengatasi semua pelaksanaan yang lain. Dari segi pemprosesan, pelaksanaan saluran maklumat telah menunjukkan peningkatan sebanyak 7.5% kepada reka bentuk yang dibentang selari dan kira-kira 10 kali ganda untuk lelaran reka bentuk. Lagi reka bentuk yang dicadangkan telah menyediakan penyelesaian perbandingan bagi sedia ada AES- XTS reka bentuk yang menunjukkan peningkatan yang ketara. Algoritma saluran maklumat telah menyediakan peningkatan kira-kira 2.8 kali ganda dalam kecekapan (Mbps/Slice) untuk semasa reka bentuk AES-XTS ada. Juga Bersepadu AES-XTS teras telah menunjukkan peningkatan kira-kira 2.4 kali ganda dalam kecekapan (Mbps / Slice) kepada yang sedia ada reka bentuk bersepadu AES.

ACKNOWLEDGEMENTS

I thank God for all things throughout my voyage of knowledge exploration.

I would like to express my sincere gratitude to my supervisor Senior Lecturer Dr. Khairulmizam Bin Samsudin and also my supervisory committee members Associate Professor Dr. Abdul Rahman b. Ramli and Senior Lecturer Dr. Fakhrul Zaman Rokhani for their guidance and advice throughout this work in making this a success.

My deepest appreciation to my family especially my father for their utmost support and encouragement without which all these would not be possible.

For the others who have directly or indirectly helped me in the completion of my work, I thank you all.

I certify that a Thesis Examination Committee has met on 22 October 2013 to conduct the final examination of Shakil Ahmed on his thesis entitled "Cryptographic Protection of Block-Oriented Storage Devices using AES-XTS in FPGA" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Ahmad Fauzi bin Abas @ Ismail, PhD
Associate Professor Ing.
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Roslina binti Mohd Sidek, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Mohd Nizar bin Hamidon, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Mohammad Liakot Ali, PhD
Professor
Bangladesh University of Engineering and Technology
Bangladesh
(External Examiner)

NORITAH OMAR, PhD
Associate Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 19 December 2013

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Khairulmizam bin Samsudin, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abdul Rahman bin Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Fakhrul Zaman bin Rokhani, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

_____
BUJANG BIN KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or other institution.

_____

SHAKIL AHMED

Date: 22nd October, 2013

TABLE OF CONTENTS