ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Hardware design and modeling of lightweight block ciphers for secure communications

Bassam Jamil Mohd [a,*], Thaier Hayajneh [b], Khalil M. Ahmad Yousef [a], Zaid Abu Khalaf [c], Md Zakirul Alam Bhuiyan [b]

[a] Computer Engineering Department, Hashemite University, Zarqa 13133, Jordan

[b] Department of Computer and Information Sciences, Fordham University, New York, NY 10458, USA

[c] School of Engineering and Computing Sciences, New York Institute of Technology, NY, USA

HIGHLIGHTS

- Study the structure of lightweight ciphers and select a candidate representative cipher.
- Design and optimize the hardware implementation of the representative cipher.
- Test various design options like block sizes and number of implemented rounds.
- Derive models for speed, resources, and power/energy from the implemented designs.
- Apply the derived models on a different cipher for evaluation.

ARTICLE INFO

Article history:
Received 31 October 2016
Received in revised form
21 February 2017
Accepted 22 March 2017
Available online xxxx

Keywords:
Security
Information security
Cipher
Encryption
Cryptography
Block cipher
Lightweight block cipher
FPGA
Power
Energy
Low-resource devices
KATAN
KTANTAN

ABSTRACT

Lightweight ciphers are essential for secure communication in resource-constrained devices. The objective of this research is to implement lightweight ciphers in hardware; and optimize and model their design metrics. Design metrics are measured by advanced design flow which includes implementing ciphers in hardware and conducting simulations. To achieve the stated objective, the presented study selects one representative cipher – namely the KATAN/KTANTAN algorithms – to be modeled, implemented and optimized on specific hardware technology; the Field Programmable Gate Array (FPGA) platform. Various designs are implemented to exercise numerous options e.g. block sizes, number of implemented rounds and key scheduling. Then, design metrics are measured and modeled.

In general, results demonstrate that number of resources and measured power consumption exhibit similar, but not identical, profile against design options. Measured energy trends are more complex. Specifically, results show that employing variable key scheduling increases resources, power and energy by 30%, 42% and 58%, respectively. Further, increasing the block size by 50% increases resources and power by about 53% and 55% respectively, but reduces energy by an average of 10%. Doubling number of implemented rounds in hardware increases resources and power by an average of 43% and 38% respectively. Optimum energy per bit design is produced in the designs with small block size (*i.e.* 32-bit) in the cases when number of implemented rounds equals to 32 or 64 rounds. When the energy and area design requirements are to be balanced, the optimum design is the 16-round implementation. Furthermore, developed models are tested on HIGHT cipher and demonstrate good accuracy.

1. Introduction

Recently, there is growing demand to connect low-resource devices to interact with each other, *e.g.* Internet of Things (IoT) and Vehicular Ad-hoc Networks (VANETs) [1]. Information security is obviously essential requirement for connected devices. More challenging, attackers are randomly distributed (*i.e.* unknown number and locations) [2]. Hence, security solutions are desired to

* Corresponding author.
E-mail address: bassam@hu.edu.jo (B.J. Mohd).

http://dx.doi.org/10.1016/j.future.2017.03.025
0167-739X/

integrate at all levels; at the low-resource devices as well as at the cloud environment [3].

A lightweight cipher is a cryptographic algorithm targeted for low-resource device, optimized for minimal area and/or memory overhead, low-power design and adequate security level [4,5]. Compared with conventional ciphers, a lightweight cipher has smaller block size, smaller key size, and implements simpler operations and scheduling techniques [6]. Important applications for lightweight ciphers include wireless sensor network (WSN) [7], wireless body area network (WBAN) [8], Internet of Things (IoT) [9], smart card [7], radio-frequency identification (RFID) [7] and devices in cyber–physical systems [10].

Implementing a lightweight cipher in either software or hardware is a challenging task, as it requires carefully balancing security level and performance metrics. Software implementation of lightweight cipher minimizes memory footprint and number of execution cycles. Hardware implementation, however, must optimize power, energy, area and speed, which are the main focus of this research.

Hardware implementation provides faster and lower power and energy solution compared to software implementation. Numerous options exist to realize the hardware implementation including ASIC and Field Programmable Gate Array (FPGA). While ASIC designs are faster compared to FPGA ones, newer process technology has reduced the speed gap between them [5]. Additionally, FPGA provides low-cost development and flexibility. Also, FPGA was shown to be very advantageous to the implementation of ciphers, as it facilitates algorithm agility, upload and modification as well as architecture efficiency and resource efficiency [11].

In general, encryption algorithms can either be asymmetric (public key) or symmetric (private key) algorithms. Asymmetric algorithms provide better security features compared to the symmetric algorithms; however, they are computationally more expensive [12,13]. Hence, lightweight ciphers are typically being implemented as symmetric ciphers.

Symmetric lightweight ciphers either process input data as stream of bits where they are called stream lightweight ciphers, or process input data as blocks of data, where in this case they are called block lightweight ciphers. In the literature, it is more common to use the block lightweight ciphers for constrained and low-resource devices as pointed out by Bogdanov et al. [14]. Block lightweight ciphers can further be classified into substitution permutation network (SPN), Feistel, stream and Lai–Massey ciphers [6].

Since it is essential in the implementation of any lightweight cipher to minimize its resources and energy, the main motivation of our research is to study and optimize the hardware implementation of a given lightweight cipher in terms of its utilized resources and measured power/energy, which are required for secure communication of resource-constrained devices. The presented research thus, for a given lightweight cipher, examines the relationship between the performance of its optimized hardware implementation and algorithmic/design options such as key scheduling, block size and number of implemented rounds in hardware. Subsequently, the main objective of this paper is to utilize minimum hardware resources, and reduce measured power and energy consumption in the hardware implementations of lightweight ciphers.

The main contributions of this paper are summarized as follows:

- Examine the general structure of lightweight ciphers and select a candidate cipher for the implementation phase, which we refer to as a representative cipher.
- Design and optimize FPGA implementation of the selected cipher with one implemented algorithm round.
- Study the optimized design of the selected cipher with different number of implemented rounds and different block size; with and without key scheduling.
- Derive models for speed, resources, measured power and energy from all of the implemented designs.
- Apply derived models on a different cipher for evaluation.

It is worth noting that the hardware implementation must execute the full number of the cipher rounds by iterating until completion. In other words, the various hardware implementations of the cipher do not alter the cipher algorithm.

The rest of the paper is organized as follows. Section 2 reviews published lightweight cipher studies in the literature. Section 3 discusses design and measurement methodology. Section 4 briefly describes what is a lightweight cipher in general terms and what virtues should be found in the selected lightweight cipher to serve as a representative cipher in the study presented in this paper. Section 5 describes selected representative ciphers, which are KATAN and KTANTAN family of ciphers. Section 6 presents FPGA implementations of the KATAN and KTANTAN ciphers. Section 7 summarizes the FPGA designs' results. Section 8 discusses the results and draw guidelines and trends. Section 9 applies derived models on different cipher. Section 10 presents concluding remarks and future directions.

2. Lightweight cipher studies in literature

Published articles in lightweight cipher implementation can be classified into the following categories: surveys, new cipher proposal, existing cipher optimization, and performance modeling. The rest of the section discusses each category in detail.

Survey studies focus on either software implementations, hardware implementations or both. Software surveys compare performance of machine-dependent cipher programs executed on low-end micro-controllers platform. The studied software performance metrics include number of cycles, throughput and memory footprint [5]. Some examples of software surveys are [12,15,16,6].

Another category of software surveys, though few in numbers, examines machine-independent software designs as demonstrated in [17,18].

Hardware surveys examine designs realized in application specific integrated circuit (ASIC) technology or FPGA platform. The studied hardware performance metrics include area, throughput, power and energy [5]. Enhancing a particular metric often results in degrading other metrics, and therefore **combined metrics** are employed to compare cipher performance across multiple metrics. Examples of combined metrics are efficiency [7], energy per bit [19] and *throughput/(area* $\times$ *energy per bit)* [19]. Cipher hardware surveys were examined in [19,20,16,21,22].

Comparative analysis presented in cipher surveys illustrates relative performance of cipher implementations. For example, Mohd et al. [5] examined the software and hardware implementations of forty six ciphers. Summary of top performing ciphers are shown in Figs. 1 and 2. Clearly, Figs. 1 and 2 show the top performing ciphers in the various performance categories for software and hardware implementations, which will help in selecting the representative cipher in this research work as shall be seen later in the paper.

E.g.

New cipher study compares implementation of newly proposed cipher with published reports of previously implemented ciphers. In most of the studies, compared designs are implemented in different technologies, resulting in inaccuracies and erroneous conclusions [5]. Examples of this category of research include [23–31].

Please cite this article in press as: B.J. Mohd, et al., Hardware design and modeling of lightweight block ciphers for secure communications, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.03.025