Performance Comparison of the Improved Power-Throughput AES and Blowfish Algorithms on FPGA

R. Ahmad and W. Ismail

Abstract The demand for wireless broadband access through mobile devices has increased impressively causing wireless security to be a very serious concern. Most of wireless communication standards implement an advanced encryption standard (AES) algorithm for protection against various classes of wireless attack such as interception, fabrication, modification and reply attacks. However, the AES is a complex algorithm that consumes more memory, time, and battery power. In this paper, the performance of the proposed AES and Blowfish algorithms with improved power-throughput are analysed and compared using Virtex6 field programmable gate array (FPGA) in terms of their architecture, throughput and power consumption. The results show that the proposed Blowfish has reduced slices usage and power consumption by 1 and 6 % respectively, and increased the throughput by 36 %.

Keywords Security • Advanced encryption standard • Blowfish • Field programmable gate array • Throughput • Power consumption

1 Introduction

Nowadays, there are a lot of security algorithms available and used in the information security across insecure networks like the internet. It is known that the IEEE standard has incorporated the advanced encryption standard (AES) algorithm to provide strong data encryption for various types of wireless communication

R. Ahmad (✉)
Collaborative MicroElectronic Design Excellence Centre (CEDEC), Sains@USM,
Level 1, Block C, No. 10 Persiaran Bukit Jambul, 11900 Penang, Malaysia
e-mail: rafidah.ahmad@usm.my

W. Ismail (✉)
Auto-ID Laboratory, School of Electrical and Electronic Engineering,
Engineering Campus, 14300 Nibong Tebal, Penang, Malaysia
e-mail: eewidad@usm.my

© Springer Science+Business Media Singapore 2017

H. Ibrahim et al. (eds.), *9th International Conference on Robotic, Vision, Signal Processing and Power Applications*, Lecture Notes in Electrical Engineering 398,
DOI 10.1007/978-981-10-1721-6_3

standard such as WiFi, Zigbee, WiMAX and Bluetooth. The AES algorithm which was developed by Daemen and Rijmen [1], is a symmetric block cipher that can encrypt and decrypt information.

Research trends are more concerned with small high-speed security architectures and systems with low power consumption for mobile wireless communication because they are very compact and have limited battery power. By referring to a study investigated by [2–8] on the performance comparison between AES and Blowfish, the result shows that the AES actually consumes more power and time than the Blowfish. This is shown in Table 1. Blowfish was designed in 1993 by Bruce Schneier, as a free and simple alternative to existing security algorithms. Therefore, this paper proposes a performance comparison of AES and Blowfish algorithms on Virtex6 XC6VLX240T-3-FF1156 field programmable gate array (FPGA) platform. FPGA is used for the implementation process because it can be reconfigured for multiple tasks with only a single chip. These algorithms were designed by using Verilog hardware description language (HDL).

The proposed AES and Blowfish algorithms are deeply evaluated based on three areas. The first area is the architectural parameter, which is done to obtain a minimum hardware requirement that can lead to smaller design size. The second area is high throughput design to carry out an encryption as fast as possible. Lastly, the third area is the low power design. It seeks to minimize power consumption at all costs. This comparison can help the researchers to decide the possibility of implementing Blowfish for any wireless communication standard instead of AES.

This paper is organized as follows. Section 2 introduces the proposed AES and Blowfish designs with improved power-throughput. The performance of the proposed AES and Blowfish designs in terms of architecture, throughput and power consumption are compared in Sect. 3. This is followed by the conclusion that is presented in Sect. 4.

Table 1 Performance comparison between AES and Blowfish based on previous research works

References	Algorithm	Throughput (Mbps)	Power consumption (mW)
[2]	AES	4.00	–
	Blowfish	25.00	–
[3]	AES	84.44	–
	Blowfish	108.57	–
[4]	AES	61.01	2000
	Blowfish	64.39	29.86
[5]	AES	15.56	–
	Blowfish	18.38	–
[6]	AES	11.48	470
	Blowfish	46.85	280
[7]	AES	10.26	–
	Blowfish	12.34	–
[8]	AES	5.31	–
	Blowfish	22.31	–

2 Proposed Design Architectures

2.1 AES

An improved power-throughput of AES with 128-bit block size and parallel input output (IO) data is proposed in this work. This architecture was designed with Verilog and each sub-blocks was executed sequentially. The AES design was then verified using Virtex6 FPGA. The schematic diagram of the proposed AES is illustrated in Fig. 1.

Internally, the operations of the AES algorithm are performed on a two-dimensional array of bytes known as the *State*. In the *State* array denoted by the symbol s, each individual byte has two indices, with its row number r in the range of $0 \leq r < 4$ and its column number c in the range of $0 \leq c < N_b$. An individual byte of the *State* is referred to as either $s_{r,c}$ or $s[r, c]$. For the first round function of the AES algorithm, each byte of the *State* with a substitution table (*S-box*) is applied, which is known as *SubBytes* transformation. In this paper, the *S-box* values of a total of 128 bits were stored in read only memory (ROM)-based look-up tables (LUTs) in order to decrease the required gates and speed up the execution time. The same *S-box* memory is employed for *SubWord* in the key expansion unit as shown in Fig. 1. Meanwhile, *mode* is used to select either for encryption or decryption process.

In the *ShiftRows* transformation, the bytes in the last three rows of the *State* are cyclically shifted over different numbers of bytes. Then, the *MixColumns* processes the bytes of *State* column by column and independently mixes the data to produce new columns. Each column of the *State* is XOR-ed with a word from the key schedule at *AddRoundKey* block. The length of round key equals the size of the *State*. The expansion of the input key into the key schedule is processed through *SubWord*, *RotWord*, *Rcon*, and *w*[*i-Nk*] functions. All the sub-blocks in the key expansion and data units are processed for 10 rounds using a sequential technique.

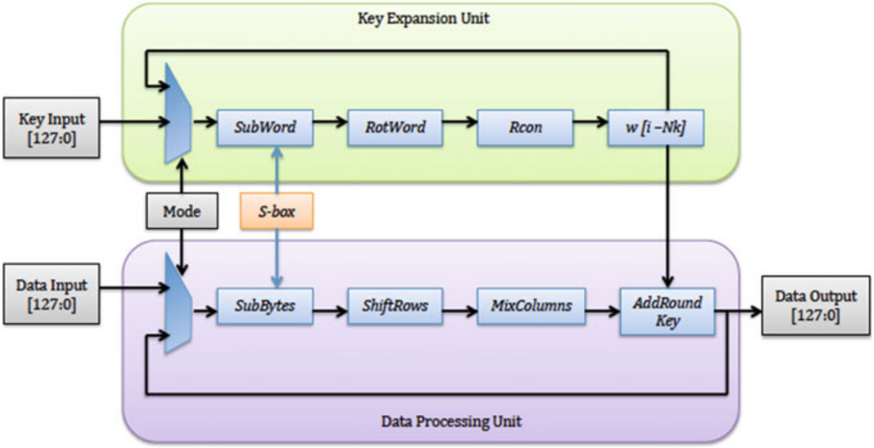


Fig. 1 Block diagram of the proposed AES core

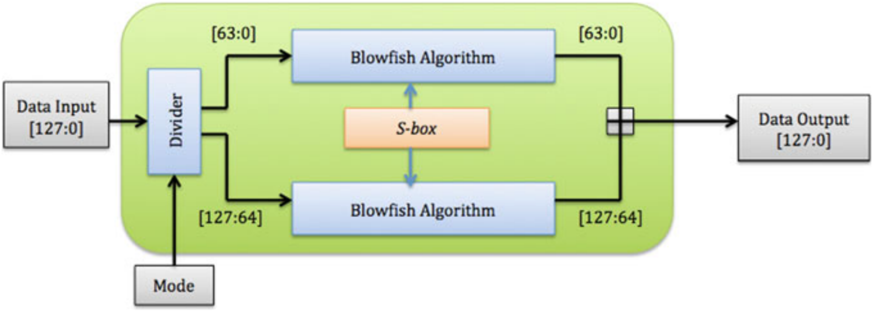


Fig. 2 Block diagram of the proposed Blowfish core

2.2 Blowfish

In order to have a fair comparison with the AES, an improved power-throughput Blowfish algorithm is proposed. This algorithm was designed with 128-bit block size, which is comprised of parallel blocks of 64-bit text input Blowfish algorithm that were simultaneously executed. This design technique enables the throughput of Blowfish algorithm to be maximized. As shown in Fig. 2, the parallel blocks share the same *S-box* that is used for Feistal (F) function. The *S-box* values of a total of 32 bits were stored in block random access memory (BRAM) where the performance can be improved by decreasing the delay into the clock-to-out value of the flip-flop (FF). BRAM is used for storage of larger amount of data. The *mode* is used to select for encryption or decryption process.

The Blowfish algorithm consists of two units: key expansion and data encryption units. The Blowfish uses P-array (P1–P18) that consists of 18 32-bit subkeys for key expansion unit. This algorithm has 16 rounds with each round implements the F function. In the F function block, there are four 32-bit *S-boxes* with 256 entries each. After the sixteenth round, the two 32-bit halves data are recombined to get the cipher text.

3 Results Comparison

In this section, the performance of the proposed AES and Blowfish architectures are compared with the architectures from previous research works. This section is divided into three parts. The first part shows the architecture/hardware comparison. The second part presents the parameters of the performance comparison. The third part provides a comparison of the power consumption of the available architectures. The proposed architecture is verified and implemented on Xilinx Virtex6, which was operated at a maximum clock frequency of 137 MHz for the AES-128, and 174 MHz for the Blowfish.

3.1 Architectural Comparison

Table 2 shows that the proposed AES and Blowfish architectures only need a small part of Virtex6's slices. The proposed Blowfish requires only 2,348 slices, which is less 1 % than the slices used by the proposed AES. Less slices means less logic resources are used to perform logic, arithmetic and ROM functions by the proposed Blowfish. From Table 2, the proposed Blowfish also used 10 % less slice LUTs compared to the proposed AES. The slice LUTs are used for logic and memory functions where they store a predefined list of outputs for every combination of inputs, and provide a fast way to retrieve the output of a logic operation. The total of LUT FF pairs show different value since it is depends on the operation of the proposed AES and Blowfish. Even though the proposed Blowfish used 39 % of fully used LUT FF pairs, the total of LUT FF pairs is 81 % less than the proposed AES. The usage of IOBs also can be decreased about 92 % by the proposed Blowfish. In overall, the proposed Blowfish shows that it has the smallest design core with fewest hardware requirements.

3.2 Performance Comparison

Performance comparison is measured in terms of throughput. The throughput is calculated as Eq. (1).

$$\text{Throughput (Gbps)} = \frac{\text{128 bits}^{*}\ \text{Clock Frequency (MHz)}}{\text{Latency}} \tag{1}$$

Latency is the time consumed for encryption or decryption process, which is calculated in clock cycles. Latency should be as small as possible to achieve a power saving system.

Figure 3 shows that the throughput for both the proposed AES and Blowfish is still higher than the previous research works. The proposed Blowfish with the smallest latency of 24 clock cycles has the highest throughput of 0.928 Gbps, which is 36 % higher than the proposed AES. The highest throughput achieved by the

Table 2 Architectural characteristics of the proposed AES and Blowfish designs

Algorithm	Slices	Slice LUTs	LUT FF pairs	IOBs
AES	5200/301440 (1 %)	17498/150720 (11 %)	3667/19031 (19 %)	555/600 (92 %)
Blowfish	2348/301440 (0 %)	2582/150720 (1 %)	1393/3537 (39 %)	3/600 (0 %)

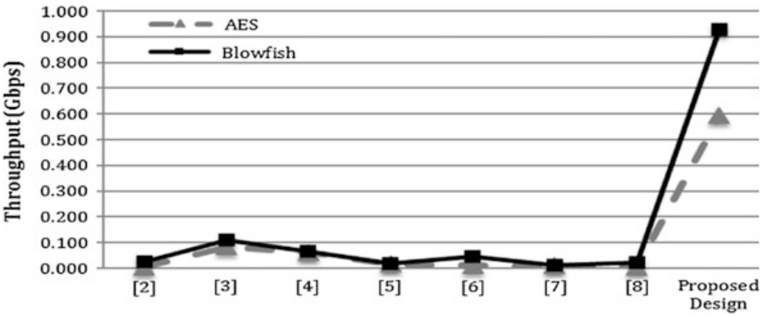
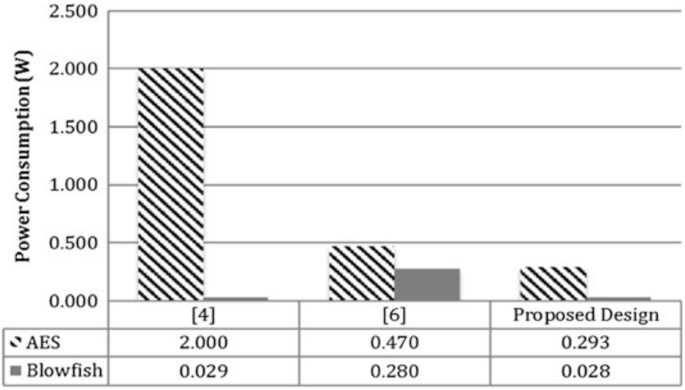


Fig. 3 Performance comparison of the proposed AES and Blowfish with previous research works

proposed architecture indicates that the said architecture has the highest encryption speed and the best performance.

3.3 Power Comparison

The power requirements for the proposed AES and Blowfish architectures are discussed in this section. The Xilinx XPower analysis tool was used to analyze the power consumption. Figure 4 shows the comparison of power consumption performed by the proposed AES and Blowfish algorithms with the previous research works. In overall, the lowest power consumed is 0.028 W by the proposed Blowfish, which is 90 % lower than the proposed AES. The power consumed by the



	[4]	[6]	Proposed Design
▨ AES	2.000	0.470	0.293
■ Blowfish	0.029	0.280	0.028

Fig. 4 Comparison of power consumption of the proposed AES and Blowfish with previous research works

S-box is 39 % of the total power consumption of this Blowfish. However, the proposed Blowfish has reduced about 6 % of power consumption if compared to the Blowfish design in [4].

4 Conclusion

The performance comparison between AES and Blowfish algorithms on FPGA is proposed in this paper. Seven papers from previous research works are compared with the proposed AES and Blowfish that have been improved in terms of power-throughput. The best performance was defined strictly as the fewest hardware requirements, highest throughput, and lowest power consumption. The output results presented in this paper show that the proposed AES and Blowfish have higher throughput and lower power consumption through Virtex6 if compared to the previous research works. However, the findings indicate that the proposed Blowfish has the smallest design core, the highest throughput, and the lowest power consumption among other architectures. These findings prove the superiority of the proposed Blowfish design.

These characteristics are important for current research trends given that wireless mobile devices are very compact and have limited battery power. With the improved power-throughput of the proposed Blowfish shown in this paper, the battery lifecycle can be expanded and this will lead to a lower cost maintenance of mobile devices.

Acknowledgments This research was financially supported by the MOSTI Science Fund Research Grant, Project No. 06-01-05-SF0640 and the USM RUI Grant, Project No. 1001/PELECT/814241.

References

1. Daemen J, Rijmen V (2002) The design of AES-The advance encryption standard. Springer
2. Abd Elminaam DS, Kader HMA, Hadhoud MM (2010) Evaluating the performance of symmetric encryption algorithms. Int J Network Secur 10(3):213–219
3. Thakur J, Kumar N (2011) DES, AES and Blowfish: symmetric key cryptography algorithms simulation based performance analysis. Int J Emerg Technol Adv Eng 1(2):6–12
4. Dakate DK, Dubey P (2012) Performance comparison of symmetric data encryption techniques. Int J Adv Res Comput Eng Technol 1(4):163–166
5. Kumar A, Karthikeyan S (2012) Investigating the efficiency of Blowfish and Rejindael (AES) algorithms. Int J Comput Network Inform Secur 2:22–28
6. Mandal PC (2012) Superiority of Blowfish algorithm. Int J Adv Res Comput Sci Softw Eng 2 (9):196–201
7. Pavithra S, Ramadevi E (2012) Study and performance analysis of cryptography algorithms. Int J Adv Res Comput Eng Technol 1(5):82–86
8. Mathur M, Kesarwani A (2013) Comparison between DES, 3DES, RC2, RC6, Blowfish and AES. In: National conference on new horizons in IT (NCNHIT2013). Mumbai, India, pp 143–148