International Journal of Future Generation Communication and Networking
Vol. 11, No. 5 (2018), pp.63-72
http://dx.doi.org/10.14257/ijfgcn.2018.11.5.06

FPGA Implementation of Secure Internet of Things (SIT) Algorithm for High Throughput Area Ratio

Um e Rabab[1,*], Irfan Ahmed[2], Muhammad Imran Aslam[3] and Muhammad Usman[4]

[1,2,3]*Department of Electronic Engineering, NED University of Engineering and Technology, University Road, Karachi 75270, Pakistan*
[4]*Faculty of Engineering Science and Technology, Iqra University, Defence View, Shaheed-e-Millat Road (Ext.), Karachi 75500, Pakistan*
[1,*]*rabijaffri@gmail.com,* [2]*irfans@neduet.edu.pk,* [3]*iaslam@neduet.edu.pk,* [4]*musman@iqra.edu.pk*

Abstract

In this paper, we present the results of hardware implementation of our previously proposed lightweight encryption algorithm named as Secure Internet of Things (SIT). By virtue of its low cost and computational simplicity, SIT can be a good candidate to meet the needs of resource constraint applications related to the futuristic demands of Internet of Things. In this work, we have implemented our proposed SIT algorithm on Field Programmable Gate Array (FPGA) and compared the results with the similar implementations reported in the literature. During the hardware implementation, we focused on obtaining high throughput area ratio which is essential parameter for the applications focusing on internet of things. Our implementation of the SIT algorithm on FPGA achieved a throughput of 4899 Mbps with encryption while using only 711 logic elements resulting in throughput area ratio of 6.89.

Keywords: *Cryptosystem; FPGA; Internet of Things; Secure Internet of Things (SIT)*

1. Introduction

Recently due to the easy access of the broadband internet, the amount of data generated and communicated has increased manifolds and with the advent of (IoT) the devices connected to the internet will be in billions [1], but these devices may or may not be composed of sophisticated controllers. The devices may be used to establish machine-to-human or machine-to-machine communication and data sharing resulting in so-called internet of things (IoT). The IoT will be composed of everyday devices with the sense of communication and connectivity to the peer devices [2] that will introduce greater complexities as the devices that make up the network could be approached from any place globally [3]. With all these developments the matter of security and integrity of the data will be of great concern [4]. To cater this issue, various encryption algorithms have been proposed in the literature. The classical encryption algorithms were designed to be used upon the conventional high computing machine with high processing capacity. However, IoT devices are resource constrained and must operate on scarce power supply. This makes the conventional encryption algorithm unsuitable for the IoT environment. To cater this drawback many lightweight algorithms have been proposed [5-9]. The hardware design significantly performs better than a relevant embedded software design [10, 11].

Recently we have proposed an efficient encryption algorithm named SIT (to abbreviate Secure Internet of Things) [12] specifically focusing on the security issues of resource-limited applications. Our proposed algorithm is lightweight block cipher that works on 64-bit data block and 64-bit key to encrypt the data. The proposed SIT algorithm can be

Received (May 19, 2018), Review Result (July 25, 2018), Accepted (August 20, 2018)

ISSN: 2233-7857 IJFGCN

implemented using uniform substitution-permutation network. In our preceding work, we have presented and analyzed the encryption capabilities and the performance of the proposed SIT algorithm through computer simulations and microcontroller-based implementation [12].

In this work, we have implemented our SIT algorithm on FPGA. FPGA due to their parallel architecture and flexibility are preferred by many researchers to test their design and measure the performance with the conventional sequential hardware modules. Exploiting the parallel processing capability of FPGA for data handling, the cryptosystem with high throughput area ratio can be implemented using techniques like pipelining, full and partial loop unrolling. In this work, we focused on designing a FPGA based cryptosystem using full loop unrolling technique based on SIT algorithm. Through FPGA-based implementation, we were able to achieve reasonably high throughput area ratio as compared to the reported literature values.

Rest of the paper is organized as follows. Section 2 provides a review of the closely related work on the hardware implementation of the cryptosystems. Section 3 presents the SIT algorithm followed by description of FPGA implementation in Section 4. The experimental setup, results and relevant discussion is presented in Section 5. Section 6 concludes of the paper.

2. Hardware Implantation of Cryptosystems

Advent of Internet of Things (IoT) where almost everything, regardless of their size and characteristics is put on a network, implementation of cryptography has become more crucial for data security. Conventional cryptographic algorithms like AES-512 are very bulky and need a lot of processing are not the forego able choices in an IoT network given the limited availability of power and processing in many devices. Therefore, lightweight algorithms that can ensure data security while running on minimal power and processing are needed.

Many researchers have implemented cryptosystems on various hardware platforms to analyze their performance. In the case of IoT-based applications, the microcontrollers have been greatly targeted because of its cost and size. The evaluation of the cost, performance, speed, and balanced efficiency of lightweight block ciphers is done with the help of hardware implementation [13]. Acting as the metric determined SPECK and SIMON as the best ciphers in this respect according to the evaluation conducted in terms of cost and with Gate Equivalent. The conducted evaluation showed the better speed of mCrypton and KLEIN-80 as the evaluation criteria was based on clock-cycle-per-block, and SIMON and SPECK had the better results in the performance evaluation of lightweight block ciphers, which was based on throughput metric. Piccolo, SIMON, and SPECK are the best ciphers in the respect of evaluation conducted to measure the balanced efficiency of ciphers by figure of merit (FOM) metric. According to these results, in all individual metrics the ciphers SIMON and SPECK exhibited the best performance, and also scored a decent FOM along with Piccolo as expected [13].

Several FPGA based cryptosystems have been proposed with the aim to achieve high throughput values [14-18]. A usual practice is to use loop unroll technique so that the iterative rounds in an encryption algorithm are executed in parallel, resulting in better throughput. These FPGA based cryptosystem using Advanced Encryption Standard (AES) focus on achieving maximum security using the minimum resources to gain better throughput area ratio. A high performance AES implementation using pipelining technique has resulted in a throughput of 4121 Mbps using 5677 slices [16]. A similar implementation using 5177 slices achieved a throughput of 21.5 Gbps [17]. A combination of AES encryption and decryption used only 163 slices to achieve throughput of 208Mbps [18].

3. SIT (Secure Internet of Things)

Our proposed SIT algorithm falls into the category of symmetric key algorithms [19]. The algorithm works on the 64-bit data block and 64-bit encryption key. Detailed working principle and basic architecture of SIT has been presented in our previously published work [12]. The use of feistel and substitution-permutation network in SIT allows similar steps for encryption and decryption, decreasing overall complexity of the system by reducing number of required computational steps. Symmetric key algorithms require a key that encrypts the data on every round of the encryption. The SIT algorithm is based on five encryption rounds requiring five distinct keys. The algorithm takes a single 64-bit key from the user and expands it to generate keys for each round. The data is encrypted using the expanded keys. The details of expansion of key and procedure of encryption have been discussed in Section 3.1 and 3.2 respectively.

3.1. Expansion of Key

The key expansion process plays a vital role in the process of encryption and decryption. The key expansion block in SIT is responsible to generate five unique keys. The user will be required to input an initial 64-bit which is broken down into 4-bit chunks and after substitution and diffusion they are fed into the *f*-function block. The key expansion block works on the following steps.

1. The cipher key of size 64-bit is broken down in 16 smaller segments of 4-bits each.
2. Four *f* function blocks work on the data of 16-bit and the initial substitution is performed using

$$Kb_jf = P_{i=1}^{4} Kc_{(i-1)+j} \quad (1)$$

where Kc shows the cipher key input by the user. For first four rounds i = 1-4, the expanded keys Kb_jf are calculated using the permutations of the bits of the initially provided cipher key.

3. In the next round the 16-bits of Kb_jf are passed to the *f*-function to further expand the key using:

$$Ka_jf = f(Kb_jf) \quad (2)$$

The transformation using the *f*-function is based on the P and Q tables presented in Table 1. The P and Q tables perform linear and non-linear transformations resulting in confusion and diffusion.

Table 1. Summary of P and Q

Kc_j	P-Values P(Kc_j)	Q-Values Q(Kc_j)	Kc_j	P-Values P(Kc_j)	Q-Values Q(Kc_j)
0	3	0	8	D	F
1	F	E	9	A	0
2	E	5	A	9	4
3	0	6	B	6	D
4	5	A	C	7	7
5	4	2	D	8	B
6	B	3	E	2	1
7	C	C	F	1	8

4. The fifth key is obtained by performing an XOR operation between the four round keys as expressed in equation (3).

$$K_5 = K_1 \oplus K_2 \oplus K_3 \oplus K_4 \tag{3}$$

The overall flow of the Key expansion process is presented in Figure 1.

3.2. Encryption

The encryption processs is initiated after obtianing all keys. Data diffusion and confusion is attained by shift and logical operations as depicted in Figure 2. 16-bit segments are extracted from the 64-bit data which are represented by $P_{x_{0-15}}$, $P_{x_{16-31}}$, $P_{x_{32-47}}$ and $P_{x_{48-63}}$. To increase the cipher text confusion at each round text swapping is applied. Bitwise *XNOR* is applied between the cipher key K_1 & $P_{x_{0-15}}$ and K_4 & $P_{x_{48-63}}$ to obtain in RO_{11} and RO_{14} respectively in the first round. The result of *XNOR* is fed to the ***f***-function generating Ef_{l1} and Ef_{r1}. The ***f***-function used in encryption process is the same as that of the key expansion process. Bitwise *XOR* is then applied between Ef_{l1} & $P_{x_{32-47}}$ to attain RO_{12} and Ef_{r1} & $P_{x_{16-31}}$ to attain RO_{13}.

$$Ro_{j,i} = \begin{cases} Px_{j,i} \odot K_j \; ; & i = 1,4 \\ P_{x_{j,i+1}} \oplus Ef_{lj} \; ; & i = 2 \\ P_{x_{j,i-1}} \oplus Ef_{rj} \; ; & i = 3 \end{cases} \tag{4}$$

The transformation is made in a way that for the next round RO_{11} will become $P_{x_{16-31}}$, RO_{12} will become $P_{x_{0-15}}$, RO_{13} will become $P_{x_{48-63}}$ and RO_{14} will become $P_{x_{32-47}}$. The transformed data segements again encrypted using equation (4) with the second key generted from the key expension. The process is coninuted for all the five keys as shown in Figure 3. The final round results are joined together to extract the Cipher Text (Ct) given by

$$Ct = \text{Concatinate}\,(R_{51}, R_{52}, R_{53}, R_{54}) \tag{5}$$

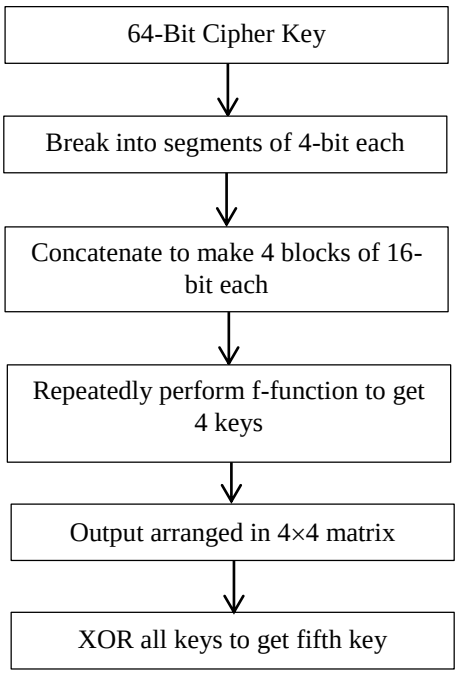

Figure 1. Key Expansion

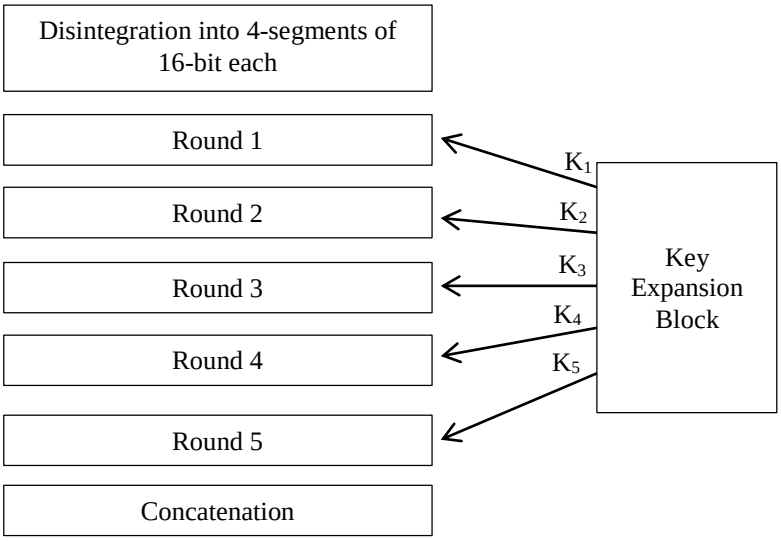

Figure 2. Encryption Process

4. FPGA Implementation

An FPGA can be configured by the user in various ways. It is composed of reconfigurable components that contains storage and logic elements. A compromise is made between combinational and sequential implementation for the improved efficiency of the system. The efficiency can be measured in one of the following three ways, by the ratio of throughput and area while calculating the area performances, by the ratio of total registers to the total number of look up tables are measured while calculating resource performance and by the ratio of power and the area in efficiency.

The implementation is based on the loop unrolling method. This leads to the exploitation of parallelism of the FPGA and ultimately increasing the throughput. For implementation purpose, Altera Cyclone II EP2C35F672C6N FPGA board is used. In the loop unrolling method, the iterations of the algorithm are unrolled and the output of each round is used as the input of the succeeding round as shown in Figure 3.

5. Experimental Setup

Based on their propagation delay, area utilization, power consumption and throughput [20, 21], the hardware implementation cryptographic algorithms are compared. The implementation is done on low cost EP2C35F672C6N Altera Cyclone II FPGA using Quartus II 12.1 sp1 edition software. For the hardware implementation, following evaluation parameters were used.

5.1. Area

The amount of circuits used by the algorithm or the number of logic units utilized refer to the area occupied on the FPGA. The minimum resource of the Altera FPGA is termed as logic element (LE) which is made up of a flip-flop and a four input look-up table.

5.2. Propagation Delay

Propagation delay is time taken by the slowest signal to move from the input to the output of the circuit. Complex operations and large area can lead to the greater propagation delays.

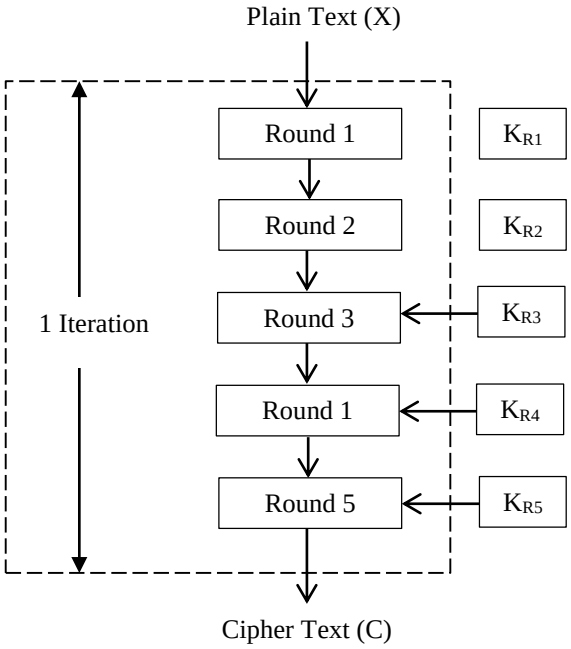

Figure 3. Full Loop Unrolled Encryption

5.3. Througput

The data (measured in terms of number of bits) processed per unit time is refered to as throughput. It a fundamental parameter for the evaluation of any hardware based system. The throughput must be high enough so as to match the speed of high speed data links present in the hardware.

6. Results and Discussion

Implementation of the SIT algorithm was carried out on Altera DE2 with EP2C35F672C6N Cyclone II FPGA. Synthesis was perfomed using Quartus II 12.1 sp1. Summary of hardware utilization in FPGA implementation of the SIT algorithm is presented in Table 2. It can be observed that the entire encryption algorithm was implemented using very small resource utiliztion percentages of logic blocks. Important results obtained through FPGA implementation are listed in table 3 and a comparison with the related lterature values is presented in Figure 4. The implementation showed that the propagation delay of SIT is smaller than Secure Cipher [21] and HIGHT [22] both previously implemented on the Cyclone-II device and is also less than LEA [23] implemented on Cyclone-III. Whereas, DES [24] implemented on Vertix-II has much lower propagation delay, due to its better hardware capabilites, therfore its comparison is ignorable. The SIT also showed the highest throughput area ratio among all implemented algorithms as shown in Figure 4(b). Similarly the Figure 4(a) shows that throughput obtained through SIT is higher than Secure Cipher [21] and HIGHT [22] on Cyclone-II and LEA [23] on Cyclone-III and DES[24] on Vertix-II. In addition to having high throghput, our implementation show lesser propagation delay as observed from other Cyclone-II and Cyclone-III based implementations.

Table 2. Hardware Resource Utilization

Logic Blocks	Used	Utilization Percentage
Number of Slices	711	2.03 %
Number of Flip Flops	796	0.6%
Number of Look Up Tables	813	2.3%

Table 3. Comparison of Implementation Results

Design	Device	Propagation Delay (ns)	Throughput Area Ratio (Mbps/LE)
HIGHT [22]	Cyclone II	14.98	6.76
DES [24]	Vertix II	2.180	0.920
LEA [23]	Cyclone III	200	0.8
Secure Cipher [21]	Cyclone II	13.927	5.73
This work	Cyclone II	12.11	6.890

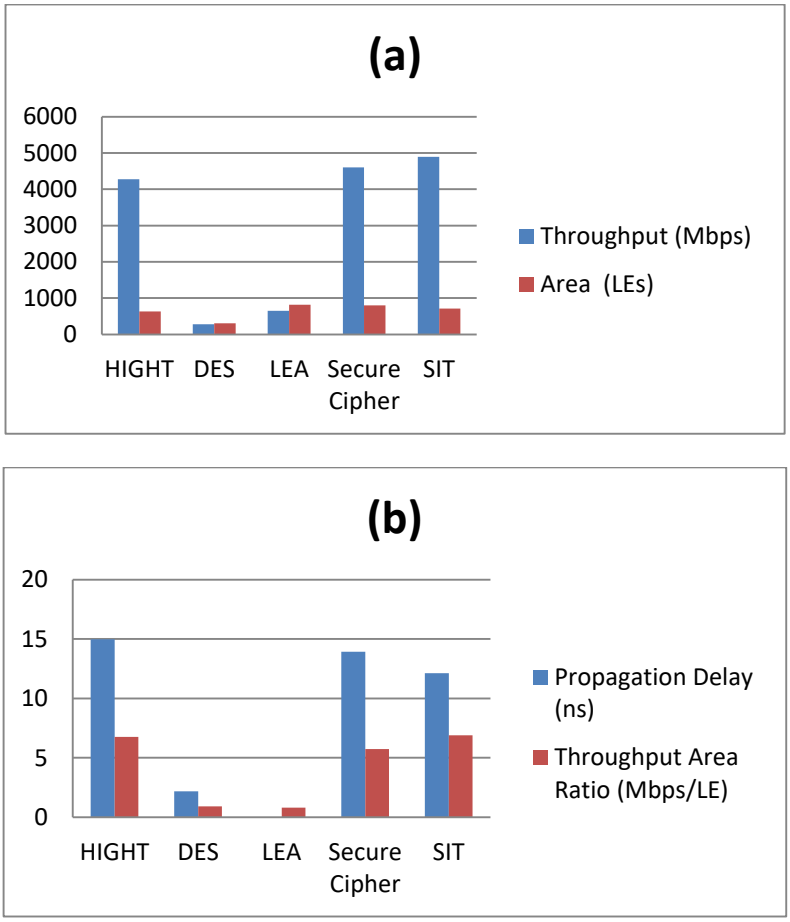

Figure 4. Comparison of our Work (SIT) with closely related literature values in terms of (a) Throughput and Area, (b) Propagation Delay and Throughput Area Ratio

6. Conclusion

The Internet of Things environment is composed of resource constrained devices. These devices must have a lightweight security mechanism to stand against the cyber attacks. We have presented the FPGA implementation results of our previously proposed encryption algorithm (SIT) and compare the results with other reported values. Using the full loop unroll technique the throughput as well as throughput to area ratio is increased. Our implementation was achieved using only 711 logic elements (LE). The throughput to area ratio of 6.890Mbps was achieved with the propagation delay of only 12.11ns. Therfore this paper concludes that SIT is truly a lightweight algortithm and thereby resource constrained devices can easily adapt the SIT alogorithm.

References

[1] R. Want and S. Dustdar, "Activating the Internet of Things [Guest Editors 'Introduction]", Computer, vol. 48, no. 9, **(2015)**, pp. 16-20.
[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (Iot): A Vision, Architectural Elements, And Future Directions", Future Generation Computer Systems., vol. 29, no. 7, **(2013)**, pp. 1645-1660.
[3] M. Usman, S. Z.-U.-A. Abidi, M. H. S. Siddiqui and M. S. Ibrahim, "Implementation of Secure Force (64-Bit) On Low Cost 8-Bit Microcontroller", Proceeding of Open Source Systems & Technologies (ICOSST) 2016 International Conference, **(2016)** December, pp. 102-105.
[4] H. Suo, J. Wan, C. Zou and J. Liu, "Security in The Internet of Things: A Review", Proceeding in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference, IEEE, **(2012)**, pp. 648-651.
[5] C. H. Lim and T. Korkishko, "mcrypton–A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors", Proceeding of Information Security Applications, Springer, **(2005)**, pp. 243-258.
[6] D. Engels, M.-J. O. Saarinen, P. Schweitzer and E. M. Smith, "The Hummingbird-2 Lightweight Authenticated Encryption Algorithm", Proceeding of RFID, Security and Privacy, Springer, **(2011)**, pp. 19-31.
[7] M. Katagi and S. Moriai, "Lightweight Cryptography for The Internet of Things", Sony Corporation., **(2008)**, pp. 7-10.
[8] J. Lee, K. Kapitanova and S. H. Son, "The Price of Security in Wireless Sensor Networks", Computer Networks., vol. 54, no. 17, **(2010)**, pp. 2967-2978.
[9] G. Hatzivasilis, G. Floros, I. Papaefstathiou and C. Manifavas, "Lightweight Authenticated Encryption for Embedded On-Chip Systems", Information Security Journal: A Global Perspective., vol. 25, no. 4-6, **(2016)**, pp. 151-161.
[10] G. Ambika and P. Srivaramangai, "Review on Security in The Internet of Things", International Journal of Advanced Research in Computer Science, vol. 9, no. 1, **(2018)**, pp. 107-110.
[11] A. F. Mohammed, "Security Issues in IoT", International Journal of Scientific Research in Science, Engineering and Technology, vol. 3, no. 8, **(2017)**, pp. 933-940.
[12] M. Usman, I. Ahmed, M. I. Aslam, S. Khan and U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Thing", (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 8, no. 51, **(2017)**.
[13] J. Hosseinzadeh and A. G. Bafghi, "Evaluation of Lightweight Block Ciphers in Hardware Implementation: A Comprehensive Survey", Proceeding of International Conference on New Research Achievements in Electrical and Computer Engineering, **(2016)**.
[14] S. Khan, M. S. Ibrahim, H. Amjad, K. A. Khan and M. Ebrahim, "FPGA Implementation of 64-Bit Secure Force Algorithm Using Full Loop Unroll Architecture", Proceeding of 2015 IEEE International Conference on Control System, Computing and Engineering (ICCSCE), IEEE, **(2015)**, pp. 1-6.
[15] S. Khan, M. S. Ibrahim, M. Ebrahim and H. Amjad, "FPGA Implementation of Secure Force (64-Bit) Low Complexity Encryption Algorithm", International Journal of Computer Network and Information Security, vol. 7, no. 12, **(2015)**, pp. 60.
[16] F. Rodrıguez-Henrıquez, N. Saqib and A. Dıaz-Perez, "4.2 Gbit/S Single Chip FPGA Implementation of AES Algorithm", Electr. Lett., vol. 39, no. 15, **(2003)**, pp. 1115-1116.
[17] A. Hodjat and I. Verbauwhede, "A 21.54 Gbits/S Fully Pipelined AES Processor on Fpga", Proceeding 12th Annual IEEE Symposium, Field-Programmable Custom Computing Machines 2004 (FCCM), IEEE, **(2004)**, pp. 308-309.
[18] G. Rouvroy, F.-X. Standaert, J.-J. Quisquater and J.-D. Legat, "Compact and Efficient Encryption/Decryption Module for Fpga Implementation of the Aes Rijndael Very Well Suited For Small Embedded Applications", Proceeding Of Information Technology: Coding and Computing, 2004 International Conference, IEEE, vol. 2, **(2004)**, pp. 583-587.
[19] M. Ebrahim, S. Khan and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis", International Journal of Computer Applications (0975 – 8887), vol. 61, no. 20, **(2014)**.
[20] S. Khan, M. S. Ibrahim, K. A. Khan and M. Ebrahim, "Security Analysis of Secure Force Algorithm for Wireless Sensor Networks", Asian Journal of Engineering, Science and Technology, **(2015)**.
[21] M. S. Ibrahim, I. Ahmed, M. I. Aslam, M. Ghazaal, M. Usman, K. Raza and S. Khan, "A Low-Cost FPGA Based Cryptosystem Design for High Throughput Area Ratio", International Journal of Advanced Computer Science and Applications, vol. 8, no. 2, **(2017)**, pp. 385-393.
[22] B. J. Mohd, T. Hayajneh, Z. A. Khalaf, A. Yousef and K. Mustafa, "Modeling and Optimization of the Lightweight Hight Block Cipher Design with FPGA Implementation", Security and Communication Networks, **(2016)**.
[23] D. Lee, D.-C. Kim, D. Kwon and H. Kim, "Efficient Hardware Implementation of the Lightweight Block Encryption Algorithm LEA", Sensors, vol. 14, no. 1, **(2014)**, pp. 975-994.
[24] M. Abdel Wahab, "High Performance FPGA Implementation of Data Encryption Standard", Proceeding of 2015 International Conference Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), IEEE, **(2015)**, pp. 37-40.

Authors

Um-e-Rabab was born in Karachi, Pakistan, in 1994. She received her B.S degree in Telecommunication engineering from Sir Syed University of Engineering & Technology Karachi, Pakistan in 2015 and M.S. degree in Telecommunication engineering from NED University Karachi in 2017. From December 2016 to September 2017, she served as a visiting Lab Engineer at NED University in the Telecommunication department. She later joined Bahria University Karachi Campus in January 2018 as a visiting lecturer and is currently working there. Her research interests include, wireless communication, data security, cryptography and encryption and coding techniques.

Irfan Ahmed was born in Karachi, Pakistan, in 1970. He received the B.E., M.E., degrees in electrical engineering from NED University Karachi, Pakistan in 1994 and 2005 respectively, and the Ph.D. degree in Electrical engineering from the Michigan Technological University, Houghton MI, USA in 2011.

From 1994 to 1996, he worked as an electrical engineer in the renowned engineering consulting/construction firm Zelin (Pvt) Ltd, Karachi Pakistan. From 1996 to 2001 he serves as electrical engineer in Black & Veatch international, at their project in Karachi Pakistan. He joined NED University as Lecturer in 2001, and became Associate Professor in 2012 where he is still serving. His research interests include, wireless communication, antenna design, electromagnetics, green telecommunication, smart grid and alternative energy**.**

Muhammad Imran Aslam was born in Karachi, Pakistan. He received the B.E., M.Engg., degrees in electrical engineering from NED University Karachi, Pakistan in 2001 and 2005 respectively, and the Ph.D. degree in Electrical engineering from the Michigan Technological University, Houghton MI, USA in 2012. He is currently serving at NED University as Associate Professor. His research interests include, wireless communication, electromagnetics, Optical metamaterials, and green telecommunication.

Muhammad Usman is a telecommunication engineer, serving as a lecturer in the telecommunication department at Iqra University Karachi. He received his bachelors and masters degree in telecommunication from Iqra University and NED University respectively. His research interests include signal processing, information theory and cryptography.