International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 6, December 2022, pp. 6114~6122
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i6.pp6114-6122

Implementation of the advanced encryption standard algorithm on an FPGA for image processing through the universal asynchronous receiver-transmitter protocol

Talapala Lakshmi Prasanna[1], Nalluri Siddaiah[1], Boppana Murali Krishna[1], Maheswara Rao Valluri[2]
[1]Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[2]School of Mathematical and Computing Sciences, Fiji National University, Suva, Fiji

Article Info

Article history:

Received Jul 5, 2021
Revised Jun 7, 2022
Accepted Jul 3, 2022

Keywords:

Advanced encryption standard
Field programmable gate array
Universal asynchronous receiver transmitter
Wireless image transmission
Zigbee

ABSTRACT

Communication among end users can be based either on wired or wireless technology. Cryptography plays a vital role in ensuring data exchange is secure among end users. Data can be encrypted and decrypted using symmetric or asymmetric key cryptographic techniques to provide confidentiality. In wireless technology, images are exchanged through low-cost wireless peripheral devices, such as radio frequency identification device (RFID), nRF, and ZigBee, that can interface with field programmable gate array (FPGA) among the end users. One of the issues is that data exchange through wireless devices does not offer confidentiality, and subsequently, data can be lost. In this paper, we propose a design and implementation of AES-128 cipher algorithm on an FPGA board for image processing through the universal asynchronous receiver transmitter (UART) protocol. In this process, the advanced encryption standard (AES) algorithm is used to encrypt and decrypt the image, while the transmitter and receiver designs are implemented on two Xilinx BASYS-3 circuits connected with a ZigBee RF module. The encrypted image uses less memory, such as LUTs (141), and also consumes less chip power (0.0291 w), I/O (0.003), block RAM (0.001 w), data, and logic to provide much higher efficiency than wired communication technology. We also observe that images can be exchanged through the UART protocol with different baud rates in run time.

Corresponding Author:

Maheswara Rao Valluri
School of Mathematical and Computing Sciences, Fiji National University
Samabula Fiji Lakeba Street Samabula, Suva, Fiji
Email: maheswara.valluri@fnu.ac.fj

1. INTRODUCTION

In the 18th century, the first wireless transmitting and receiving technology was introduced. The photo phone, a telephone that conducted audio conversations wirelessly over modulated light beams, was invented, and patented by Alexander Graham Bell and Charles Sumner Tainter in 1880 [1], and it was the world's first wireless telephone conversation. The term "wireless" became the primary usage in the 20th century [2], due to the advent of technology such as mobile broadband, Wi-Fi, and Bluetooth. Wireless communication is the process of data transmission from one device to many without using any external connections such as wires, cables, or any physical medium. Wireless communication devices such as mobile phones, wireless telephones, global positioning system (GPS), ZigBee wireless technologies, satellite TV, 3G and 4G networks, Bluetooth, and Wi-Fi technologies, are used to allow consumers to speak from remote areas. By using such technologies, an image is transmitted through wireless protocols among various devices.

To encode and decode the image to digital data, software tools such as MATLAB, Vivado, and reconfigurable hardware (RH) in the form of field programmable gate array (FPGAs) are used for wireless communication applications [3]–[6]. When we transmit images among devices, the images are read and converted into data. When the data in plaintext is transmitted through wireless communication, such data can be read by anybody over a public network. This may lead to several security issues for individuals and organizations. Around 1790 [7], Thomas Jeffers invented a secure method to encode and decode messages. In recent years [8], there has been a lot of research into developing new chaotic or hyperchaotic systems and their potential applications in real-time encryption and decryption in communications. For real-time secure multimedia data encryption systems ciphers such as DES [9], triple-DES [10], and IDEA [11] were used. Consequently, these encryption schemes are not suitable for many applications due to their security issues in real-time processing. One of the promising cipher algorithms is the advanced encryption standard (AES) algorithm [12], [13], which can be used for encrypting and decrypting images. The plaintext size in the AES is 128 bits, while the secret key size is one of 128, 192 or 256 bits [14], [15]. The FPGA [16] uses a state machine design to configure universal asynchronous receiver transmitter (UART). FPGAs have been widely used to generate numerically chaotic dynamics or cryptographic keys [17]. Furthermore, they allow for a considerable amount of chaotic system integration with the most recent digital communication technologies, such as the ZigBee protocol [18]. Wireless modules like ZigBee modules make it simple to link with the FPGA. In 2006 [19], ZigBee specifications were announced, and they replaced the message and key–value pair structure used in the 2004 stack with a cluster library [20]. In January 2017 [21], the ZigBee alliance renamed the library to dotdot and announced it as a new protocol. The dotdot has functioned as the default application layer for almost all ZigBee devices. Many real-time transmission tests were seen between two distanced Xilinx FPGA platforms [22], [23].

The rationale of this paper is to make a wireless image transmission between two FPGA's (that is, Basys 3) with two ZigBee modules interface. One will be configured as a coordinator; the another as a router. The wireless image data will be communicated between them and will be displayed on the monitor through video graphics array (VGA). In this paper, we use the AES-128 cipher algorithm for encrypting and decrypting image data along with a key generator. The bit files of both transmitter and receiver are directly configured on Basys 3 (FPGA) along with configured ZigBee. This paper is organized: in section 2, the AES algorithm is implemented on an FPGA for image processing through the UART protocol. In section 3, the results of the AES algorithm implementation and the utilization of memory on board are presented. In section 4, hardware implementation results are shown. In section 5, different baud and power parameters are compared. Finally, concluding remarks are provided in section 6.

2. IMPLEMENTATION PROCESS OF THE AES

In this section, the AES algorithm is implemented on an FPGA for exchanging images securely in wireless communication technologies. The implementation of the AES algorithm will support one of the three different key lengths, like 128 bits, 192 bits and 256 bits. This can improve the interoperability of algorithm implementations. The encryption operation consists of four different operations, like substituting bytes, shifting rows, mixing columns, and adding a round key.

2.1. Flowchart of the implementation process for images

The Figure 1 is flowchart of the implementation process of the AES algorithm for images. In this flow, the UART control plays a major role in transmitting data either in series or in parallel. The UART protocol is used for baud generation and is interfaced with VGA to display the color images. In order to display the image, we need to provide an external memory back-up such as an SD card. The stored data from an SD card can be read by the ZigBee protocol. Then, we need to interface ZigBee and FPGA for wireless image transmission. The transmitted image can be converted into a text file using MATLAB.

2.1.1. UART control

The primary feature of the UART [24] is to send and receive serial data for transmission shown in Figure 2. It sends data in terms of bits, one by one, in a frame with start and stop bits, from the least significant bit to the most significant bit. This will help the communication channel manages precise timing between transmitter and receiver. Figure 2 [25] shows a driver circuit external to the UART manages electrical signaling speeds and displays the serial data. The VGA cable is interfaced with the UART to monitor the transmission of data.

2.1.2. VGA

The VGA cable is used to transmit video signals in digital data transmission. This is a connector between a machine and a monitor, or a computer and a television. The VGA color display screens have a

resolution of 640×480 pixels, a refresh rate of 60 Hz, and can display up to 16 colors at once. The IBM PS/2 and its VGA graphics system debuted the 15-pin connector in 1987, and it has since become common on PCs, as well as many other computers, projectors, and high-definition television sets. Other connectors, such as mini-VGA or Bayonet Neill Concelman (BNC), have been used to carry VGA-compatible signals, but the term "VGA connector" generally applies to this design [26].

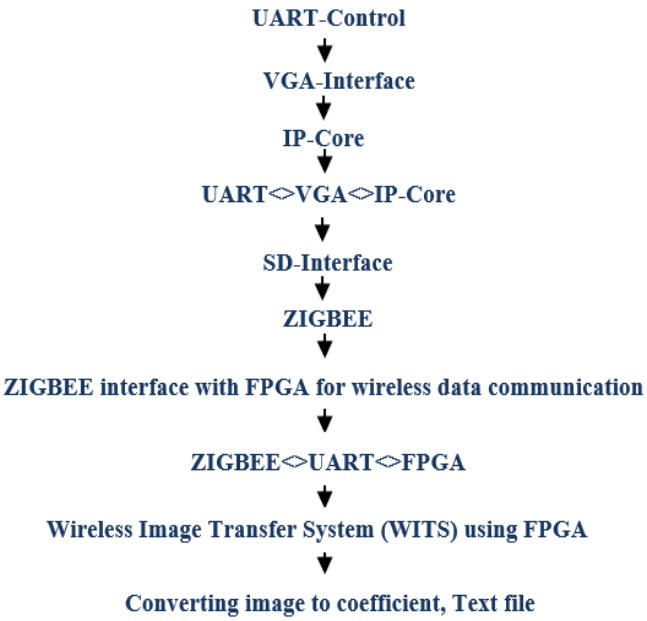

Figure 1. Flowchart of the implementation process for images

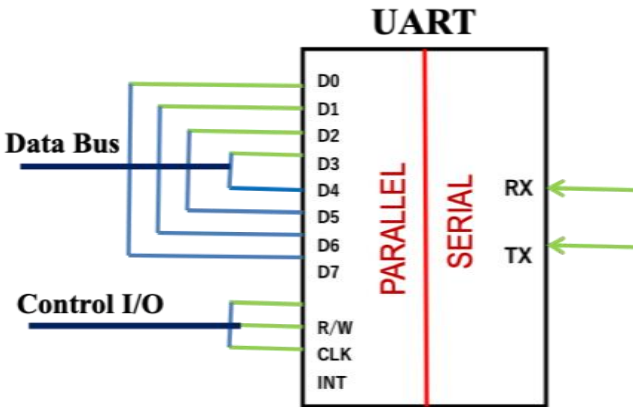

Figure 2. UART Pinout

2.1.3. IP core

An intellectual property core (IP core) is a block of data that is used in making FPGA or application-specific integrated circuit (ASIC) as a product. Ideally, the IP core should be entirely portable and easily inserted into any vendor technology or design methodology. IP cores include the UART, central processing units (CPUs), Ethernet controllers, and percutaneous coronary intervention (PCI) interfaces. Hard cores, firm cores, and soft cores are the three types of IP cores. The IP design is manifested physically in hard cores. These cores are best for plug-and-play applications, but they are less portable and adaptable than the other two categories. Firm (sometimes known as semi-hard) cores hold placement data like hard cores, but they can be customized for different applications. Soft cores are the most adaptable of the three, coming in the form of a netlist (a list of the logic gates and associated interconnections that make up an integrated circuit) or hardware description language (HDL) code.

2.1.4. SD-Card

A secure digital (SD) card is a small flash memory card used in automobile navigation systems, cellular phones, e-books, PDAs, smart phones, digital cameras, music players, digital video camcorders, and personal computers [27]. The SD card has a high data transfer rate and low power consumption, both of which are important features for portable devices. The SD card uses flash memory to provide non-volatile storage, which eliminates the need for a power source to keep data. Two different communication protocols are supported by the microSD memory card: SD and SPI Bus mode. Either of the modes can be selected by the host system. In both modes, the data on the microSD card can be read and written. These SD cards are directly inserted onto the FPGA board to read and write the stored data.

2.1.5. FPGA

FPGAs are digital integrated circuits that enable programming of customized digital logic as per user requirements [28]. FPGAs are solid-state semiconductor devices connected to configurable logic blocks (CLBs) through programmable interconnects. FPGAs are programmed for different applications after manufacturing. FPGAs can effectively implement a wide range of commutative and sequential logic functions. FPGAS are used in diverse applications like video gaming, automotive computing, aerospace applications, signal processing, and medical devices.

2.1.6. Basys 3 board

The Basys 3 board is a complete, ready-to-use digital circuit development platform based on Xilinx's new Artix-7TM FPGA [29]. With its large capacity FPGA (Xilinx product number XC7A35T-1CPG236C), low overall cost, and collection of USB, VGA, and other connectors, the Basys 3 can host designs ranging from simple combinational circuits to complicated sequential circuits. The Basys 3 can host designs such as embedded processors and controllers that range from introductory combinational circuits to complex sequential circuits. The Basys 3 kit includes enough switches, LEDs, and other I/O devices to facilitate the completion of a large number of designs without the need for any additional hardware, and enough uncommitted FPGA I/O pins to enable the use of digital pin modes or other custom boards and circuits to extend designs.

2.1.7. ZigBee

ZigBee is a low-power, low-data-rate wireless networking protocol based on IEEE 802.15.4 that is mainly used for two-way communication between sensors and control systems [30]. It is a short-range networking protocol similar to Bluetooth and Wi-Fi, with a range of 10 to 100 meters. The difference is that Bluetooth and Wi-Fi are high standard data rate communications that facilitate the transfer of complex structures such as media, and software. Simple data, such as that from sensors, can be transferred using ZigBee technology. The operational frequencies are 868 MHz, 902 to 928 MHz, and 2.4 GHz, and it can handle a modest data rate of roughly 250 kbps. The ZigBee technology shown in Figure 3 is typically utilized in applications that require low power, cheap cost, low data rate, and long battery life. Due to their low cost and compact size, mostly suitable for wireless applications, the ZigBee modules have to be configured as coordinator (Tx) and router (Tx) by using XCTU software.

For ZigBee coordinator: i) CH: C, ii) ID: 1001, iii) CE: coordinator, iv) baud rate: 9600 bps, and v) API: enable [1]. For ZigBee router: i) CH: C, ii) ID: 1001, iii) CE: router, iv) baud rate: 9600 bps, and v) API: enable [1]. The Figure 3 represents that the coordinator ZigBee and router ZigBee are communicating through wireless medium. The UART port will be responding by blinking continuously while the data is either being transmitted or received.

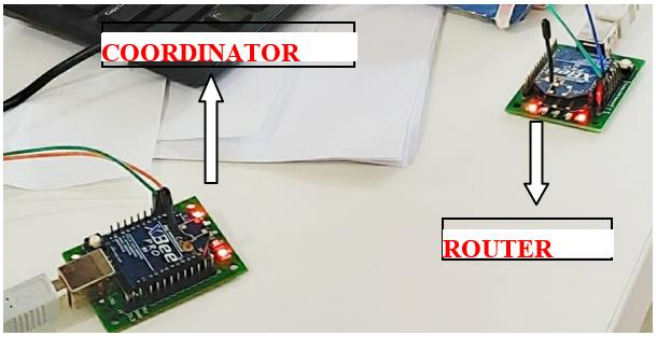

Figure 3. Configured ZigBee's

2.1.8. Serial communication using UART

Serial communication, on the other hand, uses a single wire or line to transfer data bit by bit [31]. For two-way communication between the transmitter and receiver, using serial data transmission. Fewer circuitry and wires are used in serial communication to reduce the implementation cost. As a result, serial communication requires more complex circuitry than parallel communication in real-time.

Figure 4 shows serial data transfers, on the other hand, have only one concern [31] speed. Since data transmission occurs over a single line, the serial communication transfer speed is lower than that of parallel communication [32]. The encryption and decryption algorithms were developed using a pipelined approach, and the AES-128 cipher algorithm was implemented on the Xilinx ZCU102 FPGA board and is used for 5G communications [33]. The encryption and decryption algorithms are widely developed and implemented on FPGA boards, which are frequently used in communication and parallel computing areas [34]–[36].

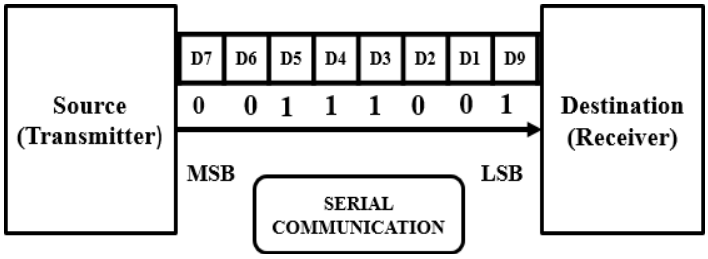

Figure 4. Serial communication

3. EXPERIMENTAL RESULTS

In this section, implementation results of AES algorithms and the utilization of memory on board are presented. The below are implementation results of the AES-128 algorithm. The encryption and decryption processes were done simultaneously on the images. For quick references, data and keys are represented in the terms of hexadecimals. Figure 5 shows the appropriate results for AES algorithm implementation by using message bits and following key bits for cipher.

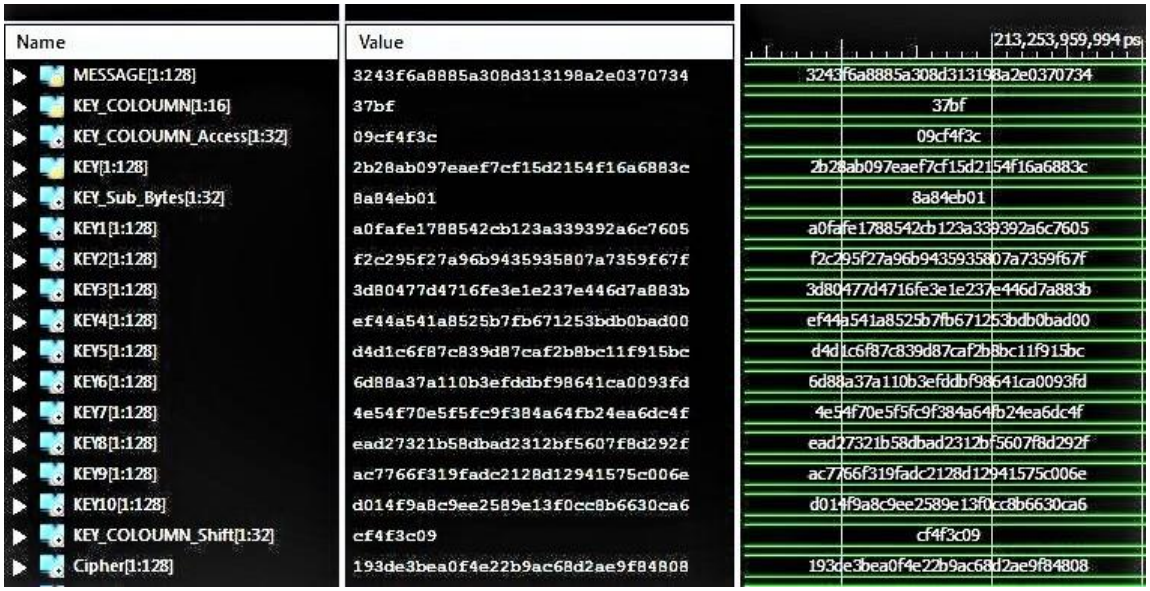

Figure 5. Implementation results of the AES

4. HARDWARE RESULTS

The Figure 6 ZigBee board is programmed by using Xilinx Vivado software to display the color bars on the monitor through an interfacing VGA cable. The Figure 7 illustrates the serially configured

ZigBee modules for communicating with each other through a wireless platform. In the XCTU tool window, the blue color frame indicates the transmitted message, and the red color frame indicates the received message. In order to maintain security and confidentiality in image processing applications, in our work images are encrypted and decrypted using the AES algorithm and transmitted between transmitter and receiver via Bluetooth RF module, also implemented on the Xilinx BASYS-3 FPGA board.

In Figure 8, it is illustrated that the programmed FPGAs were connected to two configured ZigBee's where the wireless image transmission between the two configured ZigBee's was communicated. The VGA cable is connected between FPGA and the display monitor to display both transmitted and received images. The rose images shown in Figure 8 were transmitted by the first system, while the third system image was received by the first system.

Figure 6. ZigBee board interface with VGA

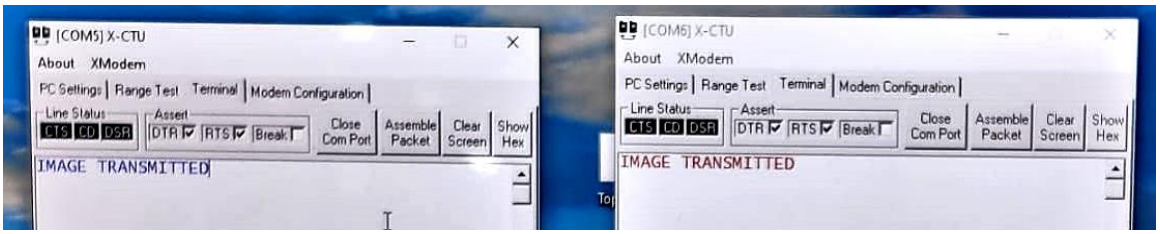

Figure 7. XCTU-Serial Communication over 2ZigBee's modules

Figure 8. Wireless image transmission between 2 FPGAs (Basys 3 boards)

5. POWER CONSUMPTION DETAILS FOR IMAGE PROCESSING ON VARIOUS FPGA MODULES

Power consumption for various parameters on different hardware boards is shown below. Basys3 employs maximum lookup tables (LUTs), whereas Artx-7 and ZedBoard employ minimum LUTs. The maximum chip power used by Artx-7 is 1.670w and the minimum chip power used by Basys3 is 0.291 w. Block RAM in Artx-7 and ZedBoard consumes the most power, whereas Basys3 block RAM consumes the least. Basys3 I/O devices are used at minimum power, but Artx-7 I/O devices are used at maximum power.

For data processing applications, Bays3 boards use less power and Atrtx-7 boards use more power. In Table 1, it can be noted that the implementation of the AES algorithm offers efficiency for various boards. Unlike other devices, this module utilizes optimal I/O pins and consumes less power, LUTs, and memory.

Table 1. Utilization of power on board

Parameters	Artx-7	ZedBoard	Basys 3
LUTs	112	112	141of20800
Total on chip power	1.670 w	1.636 w	0.291 w
Block RAM	0.243 w	0.243 w	<0.001 w
I/O	0.253 w	0.243 w	0.003
DATA	0.546 w	0.512 w	<0.001 w
Clock enable	0.017 w	<0.001 w	0.003 w

6. CONCLUSION

In this paper, the AES-128cipher algorithm has been implemented on an FPGA module for image processing through the UART protocol. In this implementation, the transmitter and receiver configuration have been carried out on two Basys-3 FPGA boards along with intermediate communication ZigBee modules. When compared to wired communication technology, this provides a low number of LUT slices and a greater efficiency with a minimum utilization of on chip power consumption (<0.001 w), I/O ports (0.003), and Block RAM (<0.001 w). It has been observed that the image can be exchanged through the UART protocol with special baud rates 11200, 9600 in run time. For future research, one can implement real time video processing and communication applications.

REFERENCE

[1] D. L. Hutt, K. J. Snell, and P. A. Bélanger, "Alexander Graham Bell's photophone," *Optics and Photonics News*, vol. 4, no. 6, Jun. 1993, doi: 10.1364/OPN.4.6.000020.

[2] M. Rikitianskaia, G. Balbi, and K. Lobinger, "The mediatization of the air: wireless telegraphy and the origins of a transnational space of communication, 1900-1910s," *Journal of Communication*, vol. 68, no. 4, pp. 758–779, Aug. 2018, doi: 10.1093/joc/jqy030.

[3] J. Lorandel, J.-C. Prevotet, and M. Helard, "Fast power and performance evaluation of FPGA-based wireless communication systems," *IEEE Access*, vol. 4, pp. 2005–2018, 2016, doi: 10.1109/ACCESS.2016.2559781.

[4] B. M. Krishna, V. N. Nayak, K. Reddy, B. Rakesh, P. Kumar, and N. Sandhya, "Bluetooth based wireless home automation system using FPGA," *Journal of Theoretical and Applied Information Technology*, vol. 77, no. 3, 2015.

[5] Z. Khan and J. J. Lehtomaki, "FPGA-assisted real-time RF wireless data analytics system: design, implementation, and statistical analyses," *IEEE Access*, vol. 8, pp. 4383–4396, 2020, doi: 10.1109/ACCESS.2019.2962200.

[6] A. Hayek, Y. Suna, M. Schreiber, and J. Borcsok, "FPGA-based wireless sensor network for safety-related cognitive systems," in *2012 IX International Symposium on Telecommunications (BIHTEL)*, Oct. 2012, pp. 1–6, doi: 10.1109/BIHTEL.2012.6412071.

[7] P. K. Verma, M. El Rifai, and K. W. C. Chan, "Quantum key distribution," in *Multi-photon Quantum Secure Communication*, Springer Singapore, 2019, pp. 59–84, doi: 10.1007/978-981-10-8618-2_3.

[8] E. Agrawal and P. R. Pal, "A secure and fast approach for encryption and decryption of message communication," *International Journal of Engineering Science and Computing*, pp. 11481–11485, 2017

[9] J. E. John, A. S. Remya Ajai, and P. Poornachandran, "Effective implementation of DES algorithm for voice scrambling," in *Communications in Computer and Information Science*, Springer Berlin Heidelberg, 2012, pp. 75–84, doi: 10.1007/978-3-642-34135-9_8.

[10] F. Ren, L. Chen, and T. Zhang, "3DES implementation based on FPGA," in *Communications in Computer and Information Science*, Springer Berlin Heidelberg, 2011, pp. 218–224, doi: 10.1007/978-3-642-24273-1_29.

[11] D. Pinchera, M. D. Migliore, and G. Panariello, "Synthesis of large sparse arrays using IDEA (inflating-deflating exploration algorithm)," *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 9, pp. 4658–4668, Sep. 2018, doi: 10.1109/TAP.2018.2846777.

[12] S. Aljawarneh, M. B. Yassein, and W. A. Talafha, "A resource-efficient encryption algorithm for multimedia big data," *Multimedia Tools and Applications*, vol. 76, no. 21, pp. 22703–22724, Nov. 2017, doi: 10.1007/s11042-016-4333-y.

[13] B. M. Krishna *et al.*, "FPGA implementation of DNA based aes algorithm for cryptography applications," *International Journal of Pure and Applied Mathematics*, vol. 115, no. 7, pp. 525–530, 2017

[14] F. T. Bin Muhaya, "Chaotic and AES cryptosystem for satellite imagery," *Telecommunication Systems*, Jun. 2011, doi: 10.1007/s11235-011-9462-z.

[15] P. N. Khose and V. G. Raut, "Implementation of AES algorithm on FPGA for low area consumption," in *2015 International Conference on Pervasive Computing (ICPC)*, Jan. 2015, pp. 1–4, doi: 10.1109/PERVASIVE.2015.7087102.

[16] M. Jasmin, T. Vigneshwaran, and S. B. Hemalatha, "Design of power aware on chip embedded memory based FSM encoding in FPGA," *Indian Journal of Science and Technology*, vol. 8, no. 32, Nov. 2015, doi: 10.17485/ijst/2015/v8i32/89043.

[17] B. Karakaya, A. Gülten, and M. Frasca, "A true random bit generator based on a memristive chaotic circuit: Analysis, design and FPGA implementation," *Chaos, Solitons and Fractals*, vol. 119, pp. 143–149, Feb. 2019, doi: 10.1016/j.chaos.2018.12.021.

[18] D. S. Pereira *et al.*, "Zigbee protocol-based communication network for multi-unmanned aerial vehicle networks," *IEEE Access*, vol. 8, pp. 57762–57771, 2020, doi: 10.1109/ACCESS.2020.2982402.

[19] T. Kim and D. Kim, "Opportunistic shortcut tree routing in ZigBee networks," *IEEE Sensors Journal*, vol. 16, no. 12, pp. 5107–5115, Jun. 2016, doi: 10.1109/JSEN.2016.2557344.

[20] V. Moravcevic, M. Tucic, R. Pavlovic, and A. Majdak, "An approach for uniform representation and control of ZigBee devices in home automation software," in *2015 IEEE 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin)*, Sep. 2015, pp. 237–239, doi: 10.1109/ICCE-Berlin.2015.7391244.
[21] C. Rehu and F. Al-Ali, "Internet of things: survey, observations and future trends," *CITRENZ*, pp. 1–9, 2017.
[22] J. Fjeldtvedt, M. Orlandic, and T. A. Johansen, "An efficient real-time FPGA implementation of the CCSDS-123 compression standard for hyperspectral images," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 11, no. 10, pp. 3841–3852, Oct. 2018, doi: 10.1109/JSTARS.2018.2869697.
[23] G. Piccinni, G. Avitabile, G. Coviello, and C. Talarico, "Real-time distance evaluation system for wireless localization," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 10, pp. 3320–3330, Oct. 2020, doi: 10.1109/TCSI.2020.2979347.
[24] E. Raghuveera K, H. Kishore, S. S. Vali, and G. S. Vennela, "Verilog implementation of UART with BIST technique for TPG," *International Journal of Pure and Applied Mathematics*, vol. 115, no. 7, pp. 531–536, 2017.
[25] Y. Wang and K. Song, "A new approach to realize UART," in *Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology*, Aug. 2011, pp. 2749–2752, doi: 10.1109/EMEIT.2011.6023602.
[26] B. M. Krishna, V. G. S. Swaroop, K. G. Deepika, and H. Khan, "PS2-VGA peripheral based character display using FPGA," *International Journal of Computer Applications*, vol. 48, no. 9, pp. 1–5, Jun. 2012, doi: 10.5120/7373-9843.
[27] S. Hawayek, C. Hargrove, and N. A. BouSaba, "Real-time bluetooth communication between an FPGA based embedded system and an Android phone," in *2013 Proceedings of IEEE Southeastcon*, Apr. 2013, pp. 1–4, doi: 10.1109/SECON.2013.6567418.
[28] I. Nanda and N. Adhikari, "Application and performance of FPGA using partial reconfiguration with Xilinx PlanAhead," in *2017 IEEE Transportation Electrification Conference (ITEC-India)*, Dec. 2017, pp. 1–4, doi: 10.1109/ITEC-India.2017.8333891.
[29] J. L. Bonniwell and S. C. Schneider, "Using the Basys-3 trainer to support VHDL in digital logic fundamentals course," in *2016 IEEE Frontiers in Education Conference (FIE)*, Oct. 2016, pp. 1–4, doi: 10.1109/FIE.2016.7757383.
[30] P. Gopi Krishna, K. S. Ravi, K. H. Kishore, K. KrishnaVeni, K. N. S. Rao, and R. D. Prasad, "Design and development of bi-directional IoT gateway using ZigBee and Wi-Fi technologies with MQTT protocol," *International Journal of Engineering and Technology*, vol. 7, no. 2.8, Mar. 2018, doi: 10.14419/ijet.v7i2.8.10344.
[31] Y. Fang and X. Chen, "Design and simulation of UART serial communication module based on VHDL," in *2011 3rd International Workshop on Intelligent Systems and Applications*, May 2011, pp. 1–4, doi: 10.1109/ISA.2011.5873448.
[32] D. V Gadre and S. Gupta, "Universal asynchronous receiver and transmitter (UART)," in *Getting Started with Tiva ARM Cortex M4 Microcontrollers*, New Delhi: Springer India, 2018, pp. 151–167, doi: 10.1007/978-81-322-3766-2_12.
[33] P. Visconti, R. Velazquez, S. Capoccia, and R. De Fazio, "High-performance AES-128 algorithm implementation by FPGA-based SoC for 5G communications," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4221–4232, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4221-4232.
[34] G. Renuka, V. U. Shree, and P. C. S. Reddy, "Comparison of AES and DES algorithms implemented on virtex-6 FPGA and microblaze soft core processor," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 5, pp. 3544–3549, Oct. 2018, doi: 10.11591/ijece.v8i5.pp3544-3549.
[35] A. T. Hashim, A. M. Hasan, and H. M. Abbas, "Design and implementation of proposed 320 bit RC6-cascaded encryption/decryption cores on altera FPGA," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6370–6379, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6370-6379.
[36] M. E. Hameed, M. Mat Ibrahim, N. Abd Manap, and M. L. Attiah, "Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 4850–4859, Dec. 2019, doi: 10.11591/ijece.v9i6.pp4850-4859.

BIOGRAPHIES OF AUTHORS

Talapala Lakshmi Prasanna received B. Tech from Padmavati Mahila University, Tirupati, India and she did M. Tech from K. L University, India. Her research interests are Low power VLSI design and modeling. She can be contacted at email: Prasanna1372040@gmail.com.

Nalluri Siddaiah received M.E from Satyabama University, Chennai, India and Ph.D from Andhra University, Andhara Pradesh, India. He is currently working as Associate professor in K. L University, India. He was published nearly 40 National and International journal and his research interests are VLSI deign, modeling and MEMS devices design. He can be contacted at email: nalluri.siddu@gmail.com.

Boppana Murali Krishna received M.Tech from GITAM University, Andhra Pradesh, India and Ph.D from K. L University, Andhra Pradesh, India. He was published 45 National and International journals. His research interests are low power VLSI design and VLSI signal processing. He can be contacted at email: boppana.muralikrishna@gmail.com.

Maheswara Rao Valluri received his Ph.D. from Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India. He is currently working as an Associate Professor at the School of Mathematical and Computing Sciences, Fiji National University, Fiji. His areas of interest include number theory, algebraic geometry, and applications to cryptography. He can be contacted at email: maheswara.valluri@fnu.ac.fj.