Indonesian Journal of Electrical Engineering and Computer Science
Vol. 41, No. 3, March 2026, pp. 1134~1140
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v41.i3.pp1134-1140

Design and implementation of novel encryption architecture using mix column with novel adder

Radha Appisetty, Munuswamy Siva Kumar
Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India

Article Info

Article history:

Received Apr 5, 2024
Revised Sep 22, 2025
Accepted Dec 13, 2025

Keywords:

Advanced encryption standard
Arithmetic operations
Cryptography
Data security
Encryption architecture

ABSTRACT

Digital information is extremely simple to process these days, but it can be accessed by unauthorized people. Cryptography is one of the most effective and widely used methods for data security, to protect this information. The cryptography techniques are becoming popular and widely adopted due to the security threats during data transmission. An essential part of a cryptographic system, cryptography algorithms are developed and implemented to increase data security. The developers of these cryptographic algorithms took into consideration additional parameters, including speed, resource consumption, reliability, usage type, and flexibility, even if their primary goals are confidentiality, integrity, and authenticity. It's important to understand that each component affects the way that a cryptographic technique is designed. Hence, this analysis presents the design and implementation of a novel encryption architecture using mix column with a novel adder. The novel encryption algorithm is designed for an encryption architecture (EA) with mix column using novel adder. This novel encryption algorithm will attain better security and performance.

Corresponding Author:

Radha Appisetty
Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation
Andhra Pradesh, India
Email: reethu.a@gmail.com

1. INTRODUCTION

Data security in networks is becoming an important issue these days. Given the speed at which technology is developing, the importance of data integrity and confidentiality, data exchanged over networks is becoming more and more important. Enhancing the current methods and approaches to understand communication features in the presence of introducer hacking technologies are necessary due to security risks on data transfer. In simple terms, cryptography is the science of protecting communications data from external threats. It is also an effective method for protecting authentication, data integrity, and confidentiality. Consequently, information is secured using cryptographic techniques so that only those with the proper authorization can decode it [1].

Numerous modern technology applications, like computer passwords, Automated teller machine (ATM) cards, and e-commerce, require cryptography. Using a cryptographic approach, regular text can be transformed into ciphertext to enable secret writing. Data sent and received over networks is protected; this is the primary objective of security. An efficient encryption method is required to enhance data security and maintain confidentiality [2]. The most important part of an information security system is cryptography. It provides data integrity, accuracy, and security [3]. There are various cryptographic techniques that provide the possibility of verifying passwords and trade and installment to private exchanges. Cryptography is vital for secure interchanges; it is not enough without someone's help. The safe equivalent technique analysis

allows the message's sender and designated receiver to view its content. Encoding and decoding plaintext messages, such as emails, is one of the primary uses of cryptography in electronic communication [4]. Two categories of cryptography exist: i) Symmetric key cryptography: in this method, the encryption and decryption processes utilize the same key; ii) Asymmetric key cryptography: in this method, the public key and private key are used for the encryption and decryption processes, respectively [5].

Encryption and decryption techniques can be used to secure text files on a computer. One of the main tools for ensuring the security of information is cryptography. It offers digital signature, authentication, secret sub-storage, system security, and other features in addition to guaranteeing the confidentiality of the information. In order to guard against information manipulation, forgery, and counterfeiting, the encryption and decryption solution can guarantee information confidentiality, integrity, and certainty. Cryptographic techniques can avoid data loss or cyber theft in a number of applications, including social networking, online transactions, social security, and managing smart applications through the internet of things (IoT) [6].

The study of protecting communications and messages content is known as cryptography. The goal of cryptanalysis, the other subdiscipline, is to defeat or compromise the security that cryptography has provided. The basis of both cryptanalysis and cryptography is mathematics. Encryption, or the process of transforming data and information into a form that cannot be used by someone who is not authorized to access it, is frequently connected with cryptography [7]. Historically, important messages for diplomatic and military communications were encrypted to ensure their protection [8].

Encryption is the process of scrambling data, including text, images, audio, video, and other types of content, to make it unreadable, invisible, or meaningless during transmission or storage. Maintaining data security from hackers is the primary goal of cryptography. Decryption restores the original data from encrypted data in the opposite direction [9].

Current cryptography aims to achieve the following four goals: i.) Confidentiality: the information cannot be analyzed by someone for whom it was not intended; ii.) Integrity: the information cannot be changed while being stored or transmitted between the sender and the intended recipient without the change being discovered; iii.) Non-repudiation: the information's creator or sender cannot later change their intentions; iv.) Authentication: the sender and recipient can verify each other's identities the information's origin, and destination.

Cryptography algorithms are used to achieve several objectives, including security or confidentiality, integrity, and authenticity. When developing these algorithms, several factors need to be taken into consideration, including speed, resource consumption, and usage type. Thus, satisfying each of these requirements at the same time when designing an algorithm is difficult and often impossible. Most algorithms can be cracked if different goals are taken into consideration when developing their design, and if the attacker has the necessary time, resources, and desire, they can reveal the information [10].

In data communication, cryptographic techniques are utilized to protect the data. The most widely used cryptographic approaches are the data encryption standard (DES), triple DES (3DES) [10], elliptic curve cryptography [10]. These days, a number of techniques have been developed to increase computing resource use and security at the same time [10]. This problem can be resolved using existing cryptographic techniques (such digital signatures or message authentication codes), but there might be additional challenges [11].

However, the advance encryption standard (AES) is regarded as the best option because of its advantages over the others. The advance encryption standard AES is a symmetric cryptography standard that was approved by the National Institute of Standards and Technology (NIST) for the encryption and decryption of data blocks. As a result of the AES's high level of security, quick hardware and software implementations, various essential applications that require dependable systems and architectures, it is widely used [12]. One of the key elements and the one in charge of diffusion in the AES is the MixColumns transformation. It is significant in relation to the cipher's wide trail approach. However, the encryption and decryption process of AES is resource-sensitive and can be slow at low-end devices.

A lightweight secure medical image encryption algorithm is designed to monitor the health data remotely. This model employs a weighted shift approximate adder (WSAA) based encryption logic. The data is encrypted using a 256-bit key, which increases the encryption's resistance to various attacks. This model performance is validated for its vertical, horizontal, entropy, key space, sensitivity, histogram and diagonal correlation. The obtained results indicated that this model had less computational complexity [13].

Using the AES and elliptic curve cryptography (ECC) algorithms, a two-level cryptographic technique is implemented to improve data security in cloud computing. With the use of two-level cryptography techniques, symmetric AES and asymmetric ECC, this study suggests an improved data security model. This method took into consideration the amount of time needed to complete cryptographic operations, improved data security against hackers by preventing them from obtaining the actual data, enabled data confidentiality and integrity, increased speed by using smaller ECC keys in the cryptographic process, and raise user trust levels for the cloud computing platform [14].

An implementation of an algorithm for cryptography using adders and subtractors is shown. The implementation of a cryptography algorithm using adders and subtractors is presented in this paper. The most difficult component of network applications, the internet, and data communication systems these days is data security. The better option is provided by cryptography, which uses various encryption and decryption techniques to transform plain text into a cipher form while protecting privacy, integrity, and authenticity. The results of the simulation indicate that the new approach has an excellent potential for success. The adder's structural changes allowed them to achieve a low-power and low-delay process [15].

A model was designed to improve the identity-based fully homomorphic encryption (IBFHE) which is designed while combining the identity-based encryption (IBE) and lattice-based cryptography. Utilizing the Micciancio's innovative trapdoor and Peikert's powerful Alperin-Sheriff and simple noise model evaluation enhanced the performance of IBFHE. Furthermore, a masking model was created in order to create an efficient multi-identity fully homomorphic encryption (MIFHE) technique. This was achieved by expanding the ciphertexts from a single identity key to an expanded under the combined key, allowing the ciphertext to be evaluated homomorphically under different identities [16].

A reversible data hiding in encrypted domain (RDH-ED) framework based on fully homomorphic encryption encapsulated-difference expansion (FHEE-DE). Bootstrapping and key switching methods were introduced for controlling the extension of ciphertext and homomorphic decryption failure. Key-switching-based least-significant-bit, or KS-LSB, was developed to enable direct data extraction from encrypted domains without requiring the use of a private key. Without utilizing the private key, the user, successful in deciphering the ciphertext that the server provided. The obtained results indicated that the presented model reversibility and embedding capacity were better than earlier encryption models [17].

The main objective was to design a trusted and proven model that can offer authenticated encryption (AE) for encoding as mapping the messaged to the curve. The model provided the analytical results, which are related to the security requirements of the presented model against various encryption models. In addition, a comparison is considered between presented model and previous model is to validate the performance. This model was outperformed other model in terms of number of encoding and decoding operations, being resistant to attacks [18].

Two hardware designs were optimized to accelerate the operation of brakerski/fan-vercauteren (BFV) homomorphic encryption and decryption model with better performance polynomial multipliers. The accelerator architecture was optimized to accelerate the simple encrypted arithmetic library (SEAL) which was developed by a cryptography research group. The hardware designs are implemented while targeting 102-degree polynomials with 8-bit coefficients for plaintext and 32-bit coefficients for ciphertext. These models achieved 7x and 12x latency speed-ups which includes input/output (I/O) operations for both offloaded encryption and decryption [19].

A ublock which is a lightweight cipher algorithm designed to improve the performance of encryption as well as decryption. Using sequential circuits in a simulation platform utilizing 90nm technology, the throughput of both encryption and decryption approached 1 Gb/s. With improved nanotechnology from hardware vendors, this model may see performance gains of more than two-fold improvement. With low power consumption, this device was able to attain the necessary degree of communication performance [20].

Two new dynamic searchable symmetric encryptions (DSSE) are designed for security and robustness (SR)- DSSEa and SR−DSSEb. Both of these methods maintained their robustness in the face of irrational queries while achieving Type I−-backward and forward security. SR−DSSEa has better round-trip and communication costs than SR−DSSEb. While the SR−DSSEb has better search performance compared to SR−DSSEa [21].

In order to transform the attribute-based encryption (ABE) model with external decryption into an ABE model with verifiable decryption, a model was created. This model was simple, optimal and general. With the help of a few non-dominant operations, this verifiable outsourced ABE is less expensive to utilize and has less users than a general outsourced ABE. It also doesn't increase the size of the ciphertext other than the addition of a hash value, which is less than 20 bytes for an 80-bit security level [22].

Many researchers have developed various encryption techniques for achieving secure and fast data transmission. However, most of the techniques were not effective for both speed and security and has more delay. To solve these issues, this work presents the design and implementation of novel encryption architecture (EA) using mix column with a novel adder. The remaining work is organized as follows: Section 2 demonstrates the design and implementation of novel encryption architecture using mix column with novel adder. Section 3 evaluates the result analysis of the presented approach. Finally, the conclusion is provided in section 4.

2. NOVEL ENCRYPTION ARCHITECTURE USING MIX COLUMN USING NOVEL ADDER

In this section, the design and implementation of a novel encryption architecture using a mix column with novel adder is presented. Figure 1 presents the architecture of the design and implementation of novel encryption architecture using mix column with novel adder. This novel encryption algorithm is designed with encryption technique with mix column using novel adder. The bottleneck of the entire ES cipher procedure is the substitution box, often known as S-Box. It is a non-linear transformation. Using a substitution table to replace data was the first modification made to the ES encryption cipher. The fixed table, known as the S-box, replaces the 16 input bytes and maintains every possible combination of eight-bit order. The new 16 bytes that are placed in a matrix with four rows and columns. An inverse S-box is used by inv-sub bytes to perform the inverse operation, or decryption.

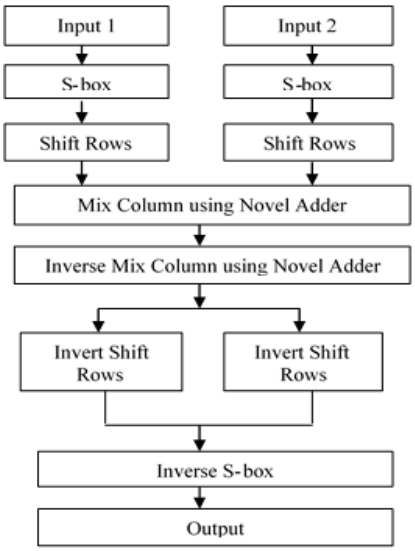

Figure 1. Novel encryption architecture using mix column with novel adder

Data rows are moved in the second transformation. In this procedure, the shift rows operation uses the subbytes' output as input. By moving bytes cyclically, the operation is carried out in this process. In this case, the encryption process shifts two bits in the third row, three bits in the fourth row, and one bit in the second row while leaving the first row of the matrix unchanged. In the process of decryption, the bits are shifted cyclically to the right in reverse order. The resulting matrix has the same 16 bytes, but they are arranged differently. The bytes in the final three rows of the State are cyclically shifted over varying numbers of bytes (offsets) in the shift rows (SR) transformation.

The third transformation now combines the columns together. This new adder that is being presented is used to operate the mix column. It appears to be a tree's structure used to carry out the mix column operation. For activities with greater performance, the innovative adder is used. This high-speed adder is implemented at the gate level logic using the smallest number of possible gates. As a result, it uses less memory and less time delay with this architecture. The mix column operation process uses the shift rows' result as input. Each column is treated as a four-term polynomial over galois field (GF) when performing the mix column operation, which is done through column-by-column matrix. Then, each of the four-byte columns is modified using a unique GF mathematical function. The function replaces the old column with four new bytes by outputting the four bytes that were input from the original column. The constant matrix is multiplied by each column on the leftmost matrix, and the resulting value is stated on the right side. For the following phases, the matrix on the right side is now regarded as the new state matrix. In this case, the additions are intended to be XOR operations. This multiplication causes a column's four bytes to be changed.

The mix column's reverse procedure is known as the inverse mix column. The transformation of shift rows is inversely represented by Inv shift rows. The final three rows of the State's bytes are cyclically shifted across a range of offsets, or bytes. There is no shift to the first row, r = 0. Nb shift (r, Nb) bytes are used to cyclically shift the bottom three rows; the shift value shift (r, Nb) is dependent on the row number. The byte substitution transformation, which applies the inverse S box to every byte in the State, is inversed by Inv sub bytes.

Firstly, the input data is applied to S-box. The S-box performs non-linear transformations of input data and provides security. The output of S-box is applied to Shift rows where it shifts each row cyclically to the left by a certain number of bytes. Here, the mix column operation is performed with the novel adder. This new adder that is being presented is used to operate the mix column. It appears to be a tree's structure used to carry out the mix column operation. Next mix column provides diffusion and non-linearity to the data and makes the data as resistant to various attacks. The mix column's reverse procedure is known as the inverse mix column. The transformation of shift rows is inversely represented by Inv shift rows. Through this all steps, the information is more secured compared to other approaches. To get the original information, first the InvMax column operation is performed. Next, the inverse operation shift row operation and inv s-box is performed. In this way, the data is secured.

3. RESULT ANALYSIS

In this section, design and implementation of a novel encryption architecture using mix column with novel adder is implemented. The implementation and simulation results are evaluated in this section. Figure 2 shows the register transfer level (RTL) schematic of novel encryption architecture using mix column with novel adder. Table 1 shows the performance comparison in terms of total delay, logic delay and route delay between ripple carry adder - advanced encryption standard (RCA-AES) and the presented novel EA.

Compared to RCA-AES approach, the novel EA has very less total delay, logic delay and route delay. Figure 3 shows the total delay comparison. In Figure 3, x-axis indicates different encryption models where as y-axis indicates total delay in nanoseconds. Compared to RCA-AES, the novel EA has required very less total delay. Figure 4 demonstrates the logic delay comparative graph. Here, logic delay is measured in terms of nanoseconds. The logic delay performance of the presented novel EA is compared with RCA-AES. Presented ES model has very less logic delay than RCA-ES model.

Figure 5 shows the route delay comparison. The novel EA has consumed very less route delay than RCA-AES model. If the delay is less, then the speed will be more. The design and implementation of novel encryption architecture using a mix column with a novel adder has obtained better performance in terms of route delay, logic delay, and total delay than earlier encryption standard models.

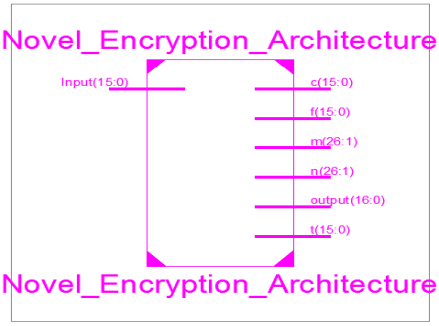

Figure 2. RTL schematic of novel encryption architecture using mix column with novel adder

Table 1. Delay performance comparison

Adders/delays	Total delay	Logic delay	Route delay
RCA-AES	12.325ns	7.947ns	4.3ns
Presented novel EA	3.125ns	0.311ns	2.9ns

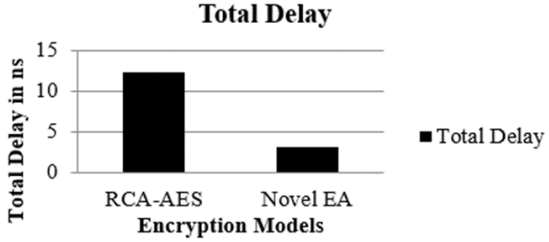

Figure 3. Total delay comparison

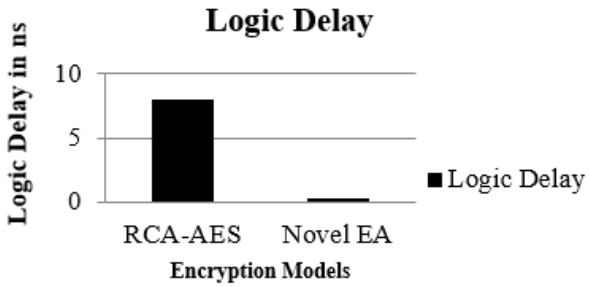

Figure 4. Logic delay comparison

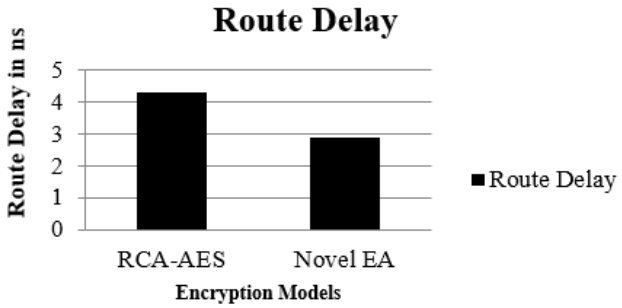

Figure 5. Route delay comparison

4. CONCLUSION

In this work, design and implementation of novel encryption architecture using mix column with novel adder is presented. The main steps included in this process are s-box, shift rows, mix column, inverse mix column, invert shift rows, inverse S-box. Using a substitution table (S-box), the sub bytes transformation is a non-linear byte replacement that works independently on every byte in the State. This new adder that is being presented is used to operate the mix column. It appears to be a tree's structure used to carry out the mix column operation. The mix column's reverse procedure is known as the inverse mix column. The transformation of shift rows is inversely represented by Inv shift rows. Through this all steps, the information is more secured compared to other approaches. The performance of presented approach is measured in terms of total delay, logic delay, and route delay. Compared to earlier approaches, presented novel EA has very less route delay, logic delay and total delay. As a result, speed is more. Hence, this approach has provided high speed and more security to the data. In future, hybrid encryption and decryption standard will be implemented with this novel encryption structure for providing more security within less time.

REFERENCES

[1] Y. N. A. Taher, K. A. Ameen, and A. M. Fakhrudeen, "An efficient hybrid technique for message encryption using caesar cipher and deoxyribonucleic acid steganography," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 28, no. 2, pp. 1096–1104, Nov. 2022, doi: 10.11591/ijeecs.v28.i2.pp1096-1104.

[2] A. A. Yassin, A. M. Rashid, A. J. Yassin, and H. Alasadi, "A novel image encryption scheme based on DCT transform and DNA sequence," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 21, no. 3, pp. 1455-1464, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1455-1464.

[3] R. Verma and J. Dhiman, "Implementation of improved cryptography algorithm," *International Journal of Information Technology and Computer Science*, vol. 14, no. 2, pp. 45-53, Apr. 2022, doi: 10.5815/ijitcs.2022.02.04.

[4] B. E. H. H. Hamouda, "Comparative study of different cryptographic algorithms," *Journal of Information Security*, vol. 11, no. 3, pp. 138-148, Jul. 2020, doi: 10.4236/jis.2020.113009.

[5] L. Yang, Y. Liu, X. S. Yang, T. Guo, and Z. Liang, "A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks," *Networking and Internet Architecture*, arXiv:2207.09936, 2022, doi: 10.48550/arXiv.2207.09936.

[6] K. Sudhakar, S. Gowsikaa, G. Karishma, and K. Ponragavi, "An efficient cryptography VLSI design for data security," in *Proceedings - International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2022*, IEEE, May 2022, pp. 1381-1386. doi: 10.1109/ICAAIC53929.2022.9793250.

[7] V. M. S. Gracia. R. F. Carapia, C. R. Marquez, B. L. Benoso, and C. A. J. Vazquez, "Images encryption using AES and variable permutations," *Cryptography and Security*, 2014, doi: 10.48550/arXiv.1409.5491.

[8] Y. T. Teng, W. L. Chin, D. K. Chang, P. Y. Chen, and P. W. Chen, "VLSI architecture of s-box with high area efficiency based on composite field arithmetic," *IEEE Access*, vol. 10, pp. 2721–2728, 2022, doi: 10.1109/ACCESS.2021.3139040.

[9] S. Harb, M. O. Ahmad, and M. N. S. Swamy, "A high-speed FPGA implementation of AES for large scale embedded systems and its applications," in *2022 13th International Conference on Information and Communication Systems, ICICS 2022*, IEEE, Jun. 2022, pp. 59-64. doi: 10.1109/ICICS55353.2022.9811140.
[10] K. Vivek, M. R. Kale, V. S. K. Thotakura, and K. Sushma, "An efficient triple-layered and double secured cryptography technique in wireless sensor networks," in *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics, DISCOVER 2021 - Proceedings*, IEEE, Nov. 2021, pp. 117-122. doi: 10.1109/DISCOVER52564.2021.9663674.
[11] C. Arul Murugan, P. Karthigaikumar, and S. Sathya Priya, "FPGA implementation of hardware architecture with AES encryptor using sub-pipelined S-box techniques for compact applications," *Automatika*, vol. 61, no. 4, pp. 682-693, Oct. 2020, doi: 10.1080/00051144.2020.1816388.
[12] D. Kodzo, M. Hodowu, D. R. Korda, and E. Danso Ansong, "An enhancement of data security in cloud computing with an implementation of a two-level cryptographic technique, using AES and ECC algorithm," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. March 2021, pp. 2278-0181, 2020, [Online]. Available: http://www.ijert.org
[13] N. Manikandan, R. Muthaiah, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "A novel random error approximate adder-based lightweight medical image encryption scheme for secure remote monitoring of health data," *Security and Communication Networks*, vol. 2021, pp. 1-14, Nov. 2021, doi: 10.1155/2021/3570904.
[14] B. Swathi, M. O. V. P. Kumar, D. G. M. Sheeba, M. Kiran, and Y. S. Reddy, "An Efficient VLSI Design of AES cryptography in memory implementation," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 4, pp. 1796-1801, Nov. 2019, doi: 10.35940/ijrte.c6188.118419.
[15] F. Noorbasha, K. Sundar Teja, B. Endreddy, N. Adidela, and C. Naga Pavan Kumar, "Implementation of cryptography algorithm with adders and subtractor," *Indian Journal of Science and Technology*, vol. 10, no. 4, Jan. 2017, doi: 10.17485/ijst/2017/v10i4/110667.
[16] T. Shen, F. Wang, K. Chen, K. Wang, and B. Li, "Efficient leveled (multi) identity-based fully homomorphic encryption schemes," *IEEE Access*, vol. 7, pp. 79299-79310, 2019, doi: 10.1109/ACCESS.2019.2922685.
[17] Y. Ke, M. Q. Zhang, J. Liu, T. T. Su, and X. Y. Yang, "Fully homomorphic encryption encapsulated difference expansion for reversible data hiding in encrypted domain," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 8, pp. 2353-2365, Aug. 2020, doi: 10.1109/TCSVT.2019.2963393.
[18] H. N. Almajed and A. S. Almogren, "SE-Enc: a secure and efficient encoding scheme using elliptic curve cryptography," *IEEE Access*, vol. 7, pp. 175865-175878, 2019, doi: 10.1109/ACCESS.2019.2957943.
[19] A. C. Mert, E. Ozturk, and E. Savas, "Design and implementation of encryption/decryption architectures for BFV homomorphic encryption scheme," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 2, pp. 353-362, Feb. 2020, doi: 10.1109/TVLSI.2019.2943127.
[20] C. Liu, Y. Zhang, J. Xu, J. Zhao, and S. Xiang, "Ensuring the security and performance of IoT communication by improving encryption and decryption with the lightweight cipher uBlock," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5489-5500, Dec. 2022, doi: 10.1109/JSYST.2022.3140850.
[21] H. Dou *et al.*, "Dynamic searchable symmetric encryption with strong security and robustness," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2370-2384, 2024, doi: 10.1109/TIFS.2024.3350330.
[22] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1384-1393, Jul. 2015, doi: 10.1109/TIFS.2015.2410137.

BIOGRAPHIES OF AUTHORS

Radha Appisetty working as an assistant professor in the Department of Electronics and Communication Engineering at University College of Engineering, Narasaraopet. She is pursuing her Ph.D. in the field of low power VLSI at Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. Her area of interest is VLSI design. She can be contacted at email: reethu.a@gmail.com.

Dr. Munuswamy Siva Kumar is working as an associate professor in Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation. He completed his Ph.D. in the field of low-power VLSI from Gulbarga University in 2016. Similarly, he has completed his master's in the field of VLSI from Bharath University at Chennai in 2005. He has published more than 60 papers, 2 Patents, his H-Index is 15, & Citations are more than 371+. He is a reviewer for several journals. In addition to the papers, he had completed one government-funded project. Interested research area: MEMS-modelling, fabrication and characterization, low power VLSI, antennas, and filters. He can be contacted at email: msivakumar@kluniversity.in.