Design and Implementation of Power-Efficient Cryptography Scheme Using a Novel Multiplication Technique

B. Srikanth (bsrikanthsri23@gmail.com)
Vardhaman College of Engineering https://orcid.org/0000-0002-8413-4764
JVR. Ravindra
Vardhaman College of Engineering
P. Ramakrishna
Anurag University
D. Ajitha
VIT University School of Computer Science and Engineering

Research Article

Keywords: Encryption and Decryption , Cryptanalysis , Power Consumption , Brute Force Attack , Transmission Delay

Posted Date: June 2nd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1699401/v1

Version of Record: A version of this preprint was published at Wireless Personal Communications on April 28th, 2023. See the published version at https://doi.org/10.1007/s11277-023-10427-y.

Abstract

The threat application has been increased a lot in the digital application; hence, protecting the data and the digital application is very important. Several crypto algorithms were already implemented with different sub-module to secure the data from the malicious event. However, the harmfulness of the malicious events has broken the security in many cases. This has resulted in high data theft, less confidential range and data loss So, the present article has designed a novel Bernoulli Data-encryption-standard (B-DES) for securing the digital communication in the wireless environment. Here, the Bernoulli function has been performed after the XOR process, and then during the decryption process, the function of the novel B-DES has been reversed. Moreover, the designed encryption approach is checked with the brute force attack**.** Here, the gained power usage by the designed scheme is 193 mW, compared to other models; it has diminished the power usage by 7%. Moreover, the earned memory utilization is 0.6 kB, compared to other compared models, it has reduced the memory utilization is 3%. The delay rated recorded by the designed model is 3.43 ns, compared to other models it has minimized the delay score by 3%.

1 Introduction

Secure communication has become the important topic in today's digital area for secure banking and other privacy based applications [1]. For secure communication, a series of steps must be taken to ensure that data sent through an insecure channel cannot be viewed by anybody other than the intended recipient [2]. Thus, the use of cryptography is essential to develop such a system [3]. Both encryption-decryption are the key components of cryptography, a security measure used to keep sensitive information out of the hands of unauthorised individuals or groups [4]. Once the data has been transmitted, it is decrypted and returned to the original form at the receiver's end using cryptography key [5]. Algorithms comprised different key types that are effectively employed to implement for encryption-decryption process [6]. Single key is worn for the encryption and decryption function in symmetric crypto procedure [7]. Moreover, in the asymmetric crypto model, double keys were employed to process the crypto functions [8]. Both key types encrypt data using a public and a secret key. The proliferation of content on the web led to the development of cryptography that led to the VLSI execution for the encryption and decryption of data that used a variety of different approaches [9]. Encrypted data delivered to a distant host that is encoded at the source host through the use of an encryption key [10], and then encrypted data had been sent to its recipient, where it is decoded to retrieve the original data [11].So that an attacker would not have the encrypted key to decrypt the message or info [12]. The concept with keys were effectively noticed through the examination of numerous encryption techniques [13]. As a result of the investigation, it has determined that a more secure framework can be established by lengthening the key [14]. Also, the wider key size require more electricity to operate and generate more heat [15].

Essentially, the crypto concept is trade-off among the security and operating expenses. Significant efforts are needed to construct a more robust encryption [16]. A highly effective block cipher should be

characterised by two chef parameters that are rapid response and complexity reduction [17]. Security is becoming increasingly crucial in network-connected technologies. There is a greater incentive to compromise network-connected ingredients than closed systems owing to circumstances such as a larger threat landscape via local and remote access and the possibility for major attacks to utilise compromised nodes that contains the large datasets [18]. Cryptography is one of the critical component against adversaries. Moreover, it is employed to ensure the confidentiality and integrity score of the data and give entities participating in communication with both anonymity and authentication [19]. Moreover, in this modern smart facilities, the crypto operations were enriched by the mathematical operations. Such as, addition, multiplication integration and so on [20]. In many cases, applying the mathematical constraints in the crypto concepts has been tended for irreversible process. So in advance, the binary arithmetic model has been proceed with the principle of mathematical equations. Hence, this process can help to mitigate the computation time and resource utilization.

Several powerful crypto techniques has been executed in past to enrich the digital application by improving security function. But some harmful attack like mirai botnet, DoS, etc., have been destroyed the confidential range of the digital application. So, the present research article has aimed to design a novel efficient Data Encryption-Standard (DES) based on the incorporation of the multiplication concepts. Here, after the XOR operation, the Bernoulli functions were performed, then the usage of the Bernoulli concept in the DES has been verified by validating the execution parameters. In addition, the brute force attack is launched in the final process to verify the robustness of the encryption functions.

The planned research work is described as follows, 2nd section detailed the recent associated work about the crypto models in the FPGA environment, 3rd section explained the normal DES system and issues, section.4 offered the novel solution for the mentioned issues, the outcome of the novel technique is revealed in 5th section and the research arguments were ended in 6th section.

2 Related Work

Some of the recent works related to FPGA are described below:

In the network, Internet-of-Things (IoT) has been incorporated several resource-strained devices. To avoid resource constraints reliable cryptography-based algorithms have been employed. Arthur Teodoro et al. [21] have presented Artificial Neuralarchitecture as Tree Parity scheme (TPS) for performing keys exchange through the networks mutual learning. In embedded systems area, FPGA have attained more space; therefore, TPS implementation in FPGA were analysed and tested to optimize the parameters of performance. Moreover, the presented TPS implementation takes less time for synchronization performance. However, increasing the parameter N value affects the performance of synchronization.

Chen et al. [22] have presented a polynomial ring-based processor with high-performance for algorithm named CRYSTALS-Kyber. Control logic was reused by inverse and forward Theoretic-based-Transform using effective configurable butterfly-based unit to mitigate the finite state-machine area. The

performance of presented method is validated by implementation of low-cost FPGA-based platform. The presented CRYSTALS-Kyber has higher memory throughput and efficiency. Moreover, this model can affect by channel attacks.

A scalable and efficient structure for bit-flipping functions implementation targeting high light-weight codes was presented by Zoni et al. [23] for post-quantum-based cryptography. Moreover, the light-weight cryptosystem has nine configurations were employed for implementation process. The result indicated that the optimized structure allows large encoded implementation on small FPGAs. However, the certain implementations reduce the average speed performance.

The varied composite field-based arithmetic unit implementation utilized in McEliece cryptosystem was presented by Canto et al. [24] for counter measures. It utilizes tailored and overhead-aware signatures. To indicate the proposed schemes feasibility, the FPGA implementations with Graphical processing model was performed. The result indicated that the presented approach covers high errors at viable overheads and low costs. However, this method takes more time for process.

Takougang et al. [25] have presented an analysis of autonomous 5G system stability, which includes quasi-periodic and periodic attractors, coexisting attractors, stability phenomenon, hop bifurcation, one-scroll and double-scroll chaotic attractor, reverse-period doubling, and offset boosting. Using FPGA, the presented 5G system model is implemented. The result indicated that attractors coexistence generated by FPGA implementation had attained better qualitative agreement. However, the execution time is high. The key contribution of this current work is described as follows

- Initially, DES has been modelled mathematically in the MATLAB environment with key exchanging parameter
- Consequently, the Bernoulli multiplication theorem is frame for the polynomials
- Moreover, the designed multiplication model is given to one of the S-box function of the DES
- Then the confidentiality and time complexity has been noted in both cases that are before and after applying the multiplication function, which is tested in matlab FPGA function
- The designed Bernoulli-DES is verified with other models in terms of security range, encryption time, execution duration, delay, power and energy.

3 System Model With Problem

The DES crypto system is utilized in many digital application real world. But, the growth of hacking and malicious vulnerability technologies have maximized the trouble in encrypting the data with the use of DES model. So, it has lacked in security function against the harmful malicious events. Hence, many arithmetic models are implemented together with DES to maximize the strength of the secret data. However, those system has raised the complexity range and time consumption.

The usual, DES system is represented in fig.1. Besides, several multiplication model also implemented in DES round but the outcome of those models were not appropriate. So, the present work has planned to implement a polynomial multiplication model in the DES round to enhance, the DES security. In normal DES model, the cipher text was gained by doing the XOR operations. But it is not secure in all cases, the probabilistic based malicious events can break the XOR and get the cipher text. Then the corrupted data was sent to the receiver side. These issues have motivated for implementing the multiplication model in the DES environment.

4 Proposed B-des Methodology For Improving Security Range

The key aim of this current work is to enrich the security of DES against the harmful malicious events. Here, the function of the DES [28] has been improved by applying the Bernoulli multiplication [27] constraints in the DES procedure. Hence, the planned modified DES is known as Bernoulli-DES (B-DES). Finally, the effectiveness of the designed multiplication based DES is tested against DoS attack. Subsequently, the key parameters were analysed and compared with other conventional model. Moreover, the proposed architecture is described in fig.2.

Finally, the designed model is checked against brute force attack. Hence, while applying the brute force attack in the encrypted data, the original data hasn't attained. It has verified the robustness of the designed crypto system. Also, the after incorporating the multiplication process, it has reduced the encryption time than the normal DES.

Here, the 64 bit size data has been given as the input of the Bernoulli DES, in that the key size bit counts are 56 and error parity check bits are 8. To make the plain text to the cipher text 16 rounds of operations have been done. After the IP the 64 bits are separated as 32+32, here, the 32 bits are processed in LS and other 32 bits were processed in RS. Moreover, the S-box in the B-DES has taken 6 bits as input and produced 4 bits block as output.

In addition, the F-function has represented the feistel process, the purpose of using the F-function is to decrypt the cipher text without any additional resources. Hence, it has minimized the computational cost of the encryption standard. Usually, to gain the chipper text XOR functions were used, but it is vulnerable to the malicious events. Hence, in this proposed DES, the Bernoulli equation was taken into the consideration. Hence, Bernoulli equation using eqn. (1),

$$B(DES) = n^{m-1} \sum_{i=0}^{n-1} B_m \left(a + \frac{i}{n} \right) \tag{1}$$

Here, represents the count of the plain text bits and the i/h has determined the XOR-ed output and α is the Bernoulli digits. Here, the Bernoulli digits were taken as same as the XOR-ed output. Moreover, the B_m is

the Bernoulli variable, its value is 1 and the constant variable is denoted as n. Then the binary addition has been performed, then to decrypt the data the concatenated digits of the Bernoulli is again XOR-ed from the XOR-ed cipher data. Because, the reverse process of XOR is XOR functions. Finally, the process has been reversed to attain the original text. The B-DES Simulink model is illustrated in fig.4.

The Simulink designed of the novel B-DES approach is described in fig.4. Here, the Double-Data-Rate (DDR) is the memory module of the novel B-DES. In addition to check the successful score of the developed crypto system an efficient malicious event was launched in the final layer of the B-DES. Then, the performance of the B-DES has been noted by transferring data. Moreover, the parameters of the novel B-DES is validated in the dual phases that is before and after applying the malicious features. Hence, the malicious features that has been considered to validate the designed crypto system is brute force model.

Algorithm 1: B-DES

```
start
{
    int p,k*                                  // data initialization
    Here, p is plain text and key is determined as K*
        Initial permutation ()
        {
            Bits64 → 32 + 32
            //LS 32 bits and RS 32 bits
            }
        F-function ()
        {
            operation → XOR
            RS_bit ⊕ LS_bit
            Results-XOR_ed bits                // XOR-ed results were obtained
        }
        Bernoulli model()
        {
            XOR_ed bits ⊕ Bernoulli_bits
            // here, the same XOR_ed bits are taken as the Bernoulli digits

            Bernoulli=cipher text
        }
        Final_permutation()
        {
            Launching brute force → Cipher_text
            performanœ → B – DES
            //Cryptanalysis has been processed
        }
        Decryption ()
        {
        Reversing Bernoulli DES
        }plain text
}
stop
```

Finally, the energy constrains and power usage has been measured by validating the particular formula, which is gained from the device utilization. Hence, the process of the B-DES is described in algorithm1.

5 Results And Discussion

The planned model is checked in the MATLAB environment and the robustness verification has been performed in the FPGA platform. The most advanced of the novel B-DES than the conventional DES is

computational cost. While using the multiplication model in the DES environment, it has reduced the computation duration up to 0.4%. Moreover, the specification of the execution parameter is tabulated in table1.

Table 1

Execution parameter specification

Execution parameter	Specifications
Register clock frequency	50 MHz
Internet_protocol clock frequency	100 MHz
CPU clock	1000 MHz
Clock frequency (controller)	200 MHz
data	64 bits
Bandwidth	2.3%
Read latency	15 clocks
Write latency	5 Clocks
Launguage	C
Tool chain	LInaro AArch32 Linuxv6.3.1

The FPGA wave form has been visualized in fig.5. Also, the processor that was used to value the designed crypto system is SOC_rfcapture. In addition, the utilized CPU clock rate to perform the crypto function is 1000 MHz. The recorded latency score for the process read and write is 5 clocks.

The signal wave form of the input and output data is described in fig.6. Here, the input and output data wave has verified the similar amplitude. Hence, it was proved that there is no attack threats happened in the communication medium. Moreover, the designed scheme is verified with the FPGA module in the MATLAB environment. Here, the blue line indicates the input data and rose colour line determined the output data.

Here, three wave form has been described in fig. here the signal frequency of plain text, cipher text and de-cipher text are compared. Considering the plain text signal, there is the major signal variation in cipher text signal, this verified that the proper encryption process was performed by the designed novel B-DES model. Finally, the signal of the de-cipher is same as plain text, it denotes the robustness of the designed B-DES scheme. Here, the signals have to gain in the basis of time versus amplitude. The signal variation of the input and crypto function has detailed in fig.7.

5.1 Case study

To check the function of the developed novel B-DES encryption model this case study has been elaborated. Moreover, the image data is taken as the input of the designed novel B-DES model. Hence, the taken input image, encrypted image and the decrypted image is determined in fig. 8.

After importing the image data, the histogram of the images were calculated, which is described in fig.9. The histogram has been measured for the original and the encrypted image. Moreover, the histogram values have been differed based on the image present features. For an example, if the '0' is set as the feature then for the zero's bits the histogram values are differed. In the initial phase, after the image training, the binary bits were extracted then for the encryption that extracted binary bits have been taken into an account.

The correlation of the images were determined based on the present features, in the B-DES the value 1 is taken as the Bernoulli polynomial value then for the concatenation process the same XOR-ed output is again added. The results of this process are considered as cipher text. Then for the decryption process, the concatenated Bernoulli data is subtracted from the cipher text then the XOR process has been reversed to gain the plain bits.

The recorded encryption duration of the image is 84.7 ms. Moreover, the designed B-DES model is suitable for the normal and visual graphics data. The correlation of the input image is described in fig.10.

A high UACI/NPCR value is commonly interpreted as great resistance based on the malicious events variations. Moreover, it is unclear how the high UACI/NPCR must be in order for the image cypher to have a high range of security. Moreover, to gain the highest UACI/NPCR, here Bernoulli concepts have been introduced in the DES model. In addition, the gained NPCR of the designed B-DES is 99.67% and UACI 18.1%.

5.2 Comparison assessment

To measure the improvement score of the designed model, the comparative analysis has been performed. The parameters that have considered for this comparative analysis is delay, energy usage, power and energy consumption. In addition, few existing approaches were considered for this comparative assessment that are, AES, PRESENT, DES, SIT, KATAN, and ELCM [26].

5.2.1 Delay Assessment

Delay is the important parameter for the digital application especially for the FPGA models. Hence, the metrics delay has been measured. This delay is the amount required time to send the data from the source to destination.

The scheme AES has observed the delay score as 11.98ns, the model PRESENT has recorded as 10.34ns delay, the conventional DES has recorded the delay range as 21.1ns, the SIT approach has earned the delay score as 7.6ns delay, the KATAN scheme has gained the delay measure as 8.5ns, and the method

ELCM has obtained the delay score as 5.4 ns. Considering all these methods the proposed B-DES has recorded the mitigated delay score as 3.43ns, this statistics are detailed in fig.11.

5.2.2 Memory usage

Estimation of the required resources and space is the chief parameter for the FPGA applications. Based on the CPU requirements the execution process has been differed. If the required memory spaces are too low then it has resulted in less execution time with less computation cost like energy and resource usage. If the model that has needed more memory to execute the process then it has resulted in high execution time.

To measure the memory usage, the RAM size has been calculated after performing the crypto process. The model ELCM has recorded the RAM usage as 0.9kB, KATAN scheme has recorded 1.3kB, the approach SIT has used 1.1 kB, the DES crypto scheme has utilized 4.6kB memory RAM, PRESENT model has utilized 1.3kB RAM, and AES scheme has employed 2kB RAM. The comparison of the memory usage is detailed in fig.12.

Table 2

Comparison Assessment

Overall comparison statistics

Methods	Delay (ns)	RAM (kB)	power (mW)
AES	11.98	2	290
PRESENT	10.34	1.3	240
DES	21.1	4.6	267
SIT	7.6	1.1	221
KATAN	8.5	1.3	234
ELCM	5.4	0.9	202
Proposed	3.43	0.6	193

5.2.3 Power consumption

Evaluating the energy usage is the crucial metrics to estimate the robustness of the designed crypto model. If the model that has taken more resources then it has taken more energy to execute the process. Also, if the data is too complex then the time taken for the encryption process became high that resulted in gaining wide range of energy consumption. Here, the consumed energy has been validated in terms of pica seconds/bit. Hence, the recorded energy consumption is 10 pica s/bits. The assessment of comparison is tabulated in table.2.

Estimating the power utilization is the chief parameter for the hardware based applications. Here, the metrics power has been validated in terms of mW. The comparison of the power utilization is graphically detailed in fig.13.

The obtained power consumption by the AES is 290mW, PRESENT model has recorded the power utilization score as 240mW, the approach DES has recorded the power utilization score as 267 mW, the power utilization recorded by the model Sit is 221mW, the method KATAN has measured the power usage as 234mW and the model ELCM has measure the power consumption score as 202 mW. Considering these all validation the proposed B-DES has recorded the power usage score as 193 mW.

5.3 Discussion

From the comparison assessment, the proposed B-DES has determined the finest results; also the recorded total execution period is 0.213 s. The conventional DES has recorded 0.6565 s for the execution functions. While considering the other conventional DES, this encryption period is very less, this has proved the proficiency of the designed novel B-DES model. In addition, the designed B-DES model is supported for privacy digital application in all fields to secure the people data in cloud. In future, incorporating the optimization module will be helped to reduce energy utilization of the FPGA module. The overall performance of the B-DES is described in table.3.

Table 3

Overall performance of B-DES

B-DES performance	
parameter	Performance
execution period (s)	0.213
Power usage (mW)	193
RAM (kB)	0.6
Delay (ns)	3.43
Energy utilization (pica s/bits)	10
Encryption duration (ms)	84.7

From all metrics the desired output has been attained, this shows the stability of the designed B-DES crypto model in securing the digital transformation. In future, designing the optimization model with B-DES will proved the better energy optimized results further.

6 Conclusion

The present research work has designed a novel B-DES for the digital application to secure the data against the brute force attack. Finally, the designed model performance is validated in the MATLAB felid Programmable gate array (FPGA). Furthermore, the comparison analysis of the designed B-DES with other associated models have verified the improvement score of the designed model by earning the less power and memory usage. Hence, the proposed model is suitable for the digital applications to secure the data from the unauthorized users. In addition, compared to the Conventional DES model, the B-DES has recorded the 0.4% less execution time. So, the designed multiplication model is required module in the DES system to maintain the high confidential rate between the users. Also, the designed crypto system is suitable for all digital privacy applications, by incorporating the specific application process parameters.

Declarations

Acknowledgement

None

Compliance with Ethical Standards

1. Disclosure of Potential Conflict of Interest:

The authors declare that they have no potential conflict of interest.

2. Statement of Human and Animal Rights

i. Ethical Approval

All applicable institutional and/or national guidelines for the care and use of animals were followed.

ii. Informed Consent

For this type of study formal consent is not required.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. Fritzmann, T., Sepúlveda, J. (2019, May). Efficient and flexible low-power NTT for lattice-based cryptography. In *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* pp. 141-150. IEEE. doi: 10.1109/HST.2019.8741027.

2. Dutta, I. K., Ghosh, B., Bayoumi, M. (2019, January). Lightweight cryptography for internet of insecure things: A survey. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* pp. 0475-0481. IEEE. doi: 10.1109/CCWC.2019.8666557.
3. Yeh, L. Y., Chen, P. J., Pai, C. C., Liu, T. T. (2020). An energy-efficient dual-field elliptic curve cryptography processor for Internet of Things applications. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *67*(9), 1614-1618.doi: 10.1109/TCSII.2020.3012448.
4. Islam, M. M., Hossain, M. S., Shahjalal, M. D., Hasan, M. K., Jang, Y. M. (2020). Area-time efficient hardware implementation of modular multiplication for elliptic curve cryptography. *IEEE Access*, *8*, 73898-73906. doi: 10.1109/ACCESS.2020.2988379.
5. Karl, P., Gruber, M. (2021, April). A Survey on the Application of Fault Analysis on Lightweight Cryptography. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* pp. 1-3. IEEE. doi: 10.1109/NTMS49979.2021.9432667
6. James, A. P. (2019). An overview of memristive cryptography. *The European Physical Journal Special Topics*, *228*(10), 2301-2312. https://doi.org/10.1140/epjst/e2019-900044-x
7. Karthikeyan, S., Jagadeeswari, M. (2021). Performance improvement of elliptic curve cryptography system using low power, high speed 16× 16 Vedic multiplier based on reversible logic. *Journal of Ambient Intelligence and Humanized Computing*, *12*(3), 4161-4170. https://doi.org/10.1007/s12652-020-01795-5
8. Qazi, R., Qureshi, K. N., Bashir, F., Islam, N. U., Iqbal, S., Arshad, A. (2021). Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 547-566.https://doi.org/10.1007/s12652-020-02020-z
9. Goyal, T. K., Sahula, V., Kumawat, D. (2019). Energy efficient lightweight cryptography algorithms for IoT devices. *IETE Journal of Research*, 1-14. https://doi.org/10.1080/03772063.2019.1670103
10. Gao, L., Zheng, F., Emmart, N., Dong, J., Lin, J., Weems, C. (2020, May). DPF-ECC: accelerating elliptic curve cryptography with floating-point computing power of gpus. In *2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS)* pp. 494-504. IEEE. doi: 10.1109/IPDPS47924.2020.00058.
11. Almajed, H. N., Almogren, A. S. (2019). SE-ENC: A secure and efficient encoding scheme using elliptic curve cryptography. *IEEE Access*, *7*, 175865-175878.doi: 10.1109/ACCESS.2019.2957943.
12. Sadhukhan, D., Ray, S., Obaidat, M. S., Dasgupta, M. (2021). A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography. *Journal of Systems Architecture*, *114*, 101938.https://doi.org/10.1016/j.sysarc.2020.101938
13. Yassin, H. M., Mohamed, A. T., Abdel-Gawad, A. H., Tolba, M. F., Saleh, H. I., Madian, A. H., Radwan, A. G. (2019, July). Speech encryption on FPGA using a chaotic generator and S-Box table. In *2019 Fourth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)* pp. 1-4. IEEE.doi: 10.1109/ACTEA.2019.8851086.
14. Abdul Basith, K., Shankar, T. N. (2021). Energy and efficient privacy cryptography-based Fuzzy K-Means clustering a WSN using genetic algorithm. In *International Conference on Intelligent and*

Smart Computing in Data Analytics pp. 291-304. Springer, Singapore. https://doi.org/10.1007/978-981-33-6176-8_32

15. Khan, A. A., Kumar, V., Ahmad, M. (2019). An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. *Journal of King Saud University-Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2019.04.013
16. Sharafi, M., Fotouhi-Ghazvini, F., Shirali, M., Ghassemian, M. (2019). A low power cryptography solution based on chaos theory in wireless sensor nodes. *IEEE Access*, *7*, 8737-8753.doi: 10.1109/ACCESS.2018.2886384.
17. Benssalah, M., Sarah, I., Drouiche, K. (2021). An efficient RFID authentication scheme based on elliptic curve cryptography for Internet of Things. *Wireless Personal Communications*, *117*(3), 2513-2539. https://doi.org/10.1007/s11277-020-07992-x
18. Liu, W., Fan, S., Khalid, A., Rafferty, C., O'Neill, M. (2019). Optimized schoolbook polynomial multiplication for compact lattice-based cryptography on FPGA. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *27*(10), 2459-2463. doi: 10.1109/TVLSI.2019.2922999.
19. Zoni, D., Galimberti, A., Fornaciari, W. (2020). Efficient and scalable FPGA-oriented design of QC-LDPC bit-flipping decoders for post-quantum cryptography. *IEEE Access*, *8*, 163419-163433.doi: 10.1109/ACCESS.2020.3020262.
20. Andrzejczak, M. (2019, September). The low-area FPGA design for the post-quantum cryptography proposal Round5. In *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)* pp. 213-219. IEEE. doi: 10.15439/2019F230.
21. Teodoro, A. A., Gomes, O. S., Saadi, M., Silva, B. A., Rosa, R. L., Rodríguez, D. Z. (2021). An FPGA-based performance evaluation of artificial neural network architecture algorithm for IoT. *Wireless Personal Communications*, 1-32. https://doi.org/10.1007/s11277-021-08566-1
22. Chen, Z., Ma, Y., Chen, T., Lin, J., Jing, J. (2021). High-performance area-efficient polynomial ring processor for CRYSTALS-kyber on FPGAs. *Integration*, *78*, 25-35. https://doi.org/10.1016/j.vlsi.2020.12.005
23. Zoni, D., Galimberti, A., Fornaciari, W. (2020). Efficient and scalable FPGA-oriented design of QC-LDPC bit-flipping decoders for post-quantum cryptography. *IEEE Access*, *8*, 163419-163433. doi: 10.1109/ACCESS.2020.3020262.
24. Canto, A. C., Kermani, M. M., Azarderakhsh, R. (2020). Reliable architectures for composite-field-oriented constructions of Mceliece post-quantum cryptography on FPGA. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *40*(5), 999-1003. doi: 10.1109/TCAD.2020.3019987.
25. Takougang Kingni, S., Rajagopal, K., Çiçek, S., Srinivasan, A., Karthikeyan, A. (2020). Dynamic analysis, FPGA implementation, and cryptographic application of an autonomous 5D chaotic system with offset boosting. *Frontiers of Information Technology & Electronic Engineering*, *21*(6), 950-961. https://doi.org/10.1631/FITEE.1900167

26. Prakasam, P., Madheswaran, M., Sujith, K. P., Sayeed, M. S. (2022). Low Latency, Area and Optimal Power Hybrid Lightweight Cryptography Authentication Scheme for Internet of Things Applications. *Wireless Personal Communications*, 1-15. https://doi.org/10.1016/j.icte.2021.03.007
27. Defez, E., Ibánez, J., Alonso-Jordá, P., Alonso, J. M., Peinado, J. (2022). On Bernoulli matrix polynomials and matrix exponential approximation. *Journal of Computational and Applied Mathematics*, *404*, 113207. https://doi.org/10.1016/j.cam.2020.113207
28. Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., Shankar, K. (2020). Data encryption for Internet of Things applications based on catalan objects and two combinatorial structures. *IEEE Transactions on Reliability*, *70*(2), 819-830. doi: 10.1109/TR.2020.3010973.

Figures

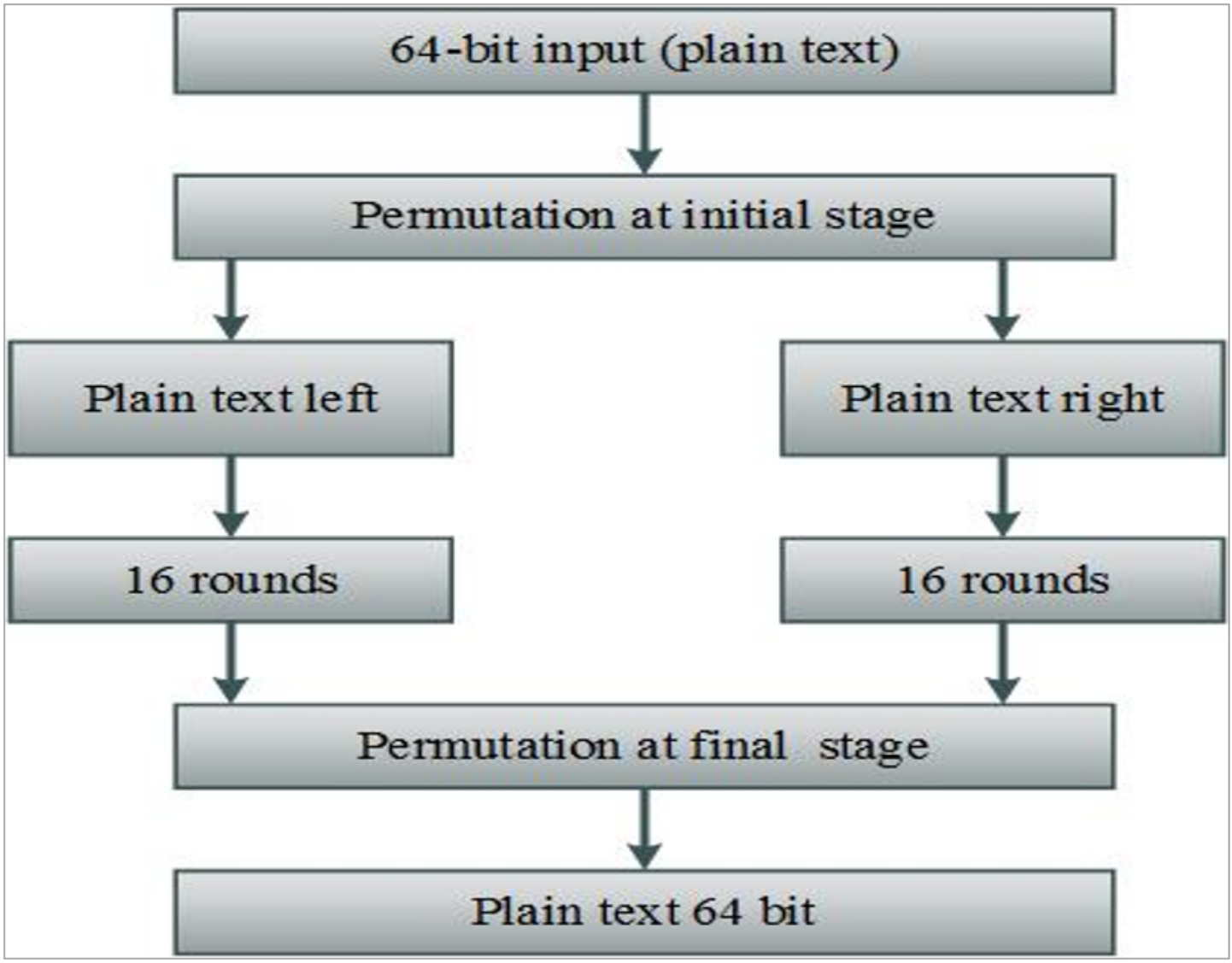

Figure 1

DES Function block

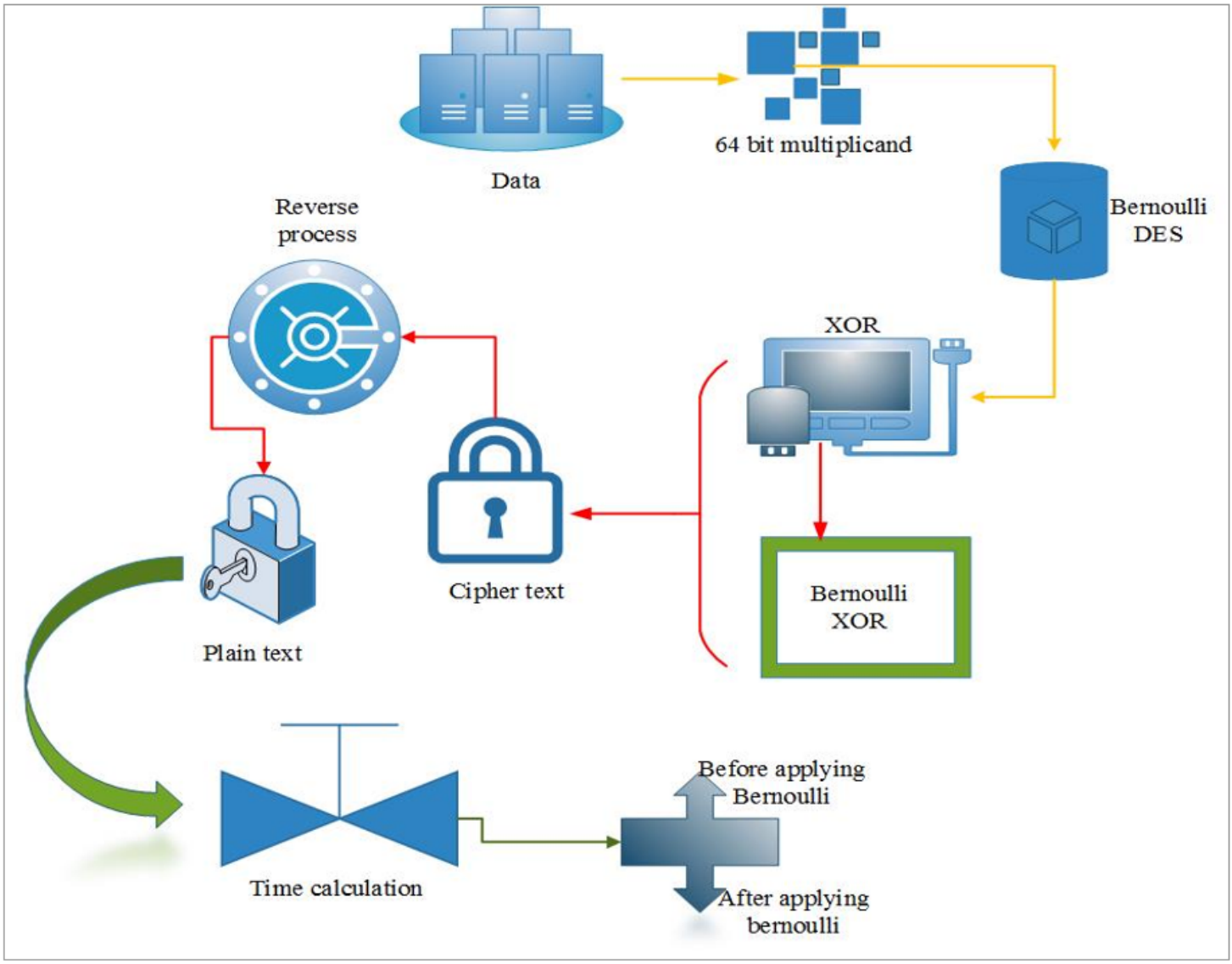

Figure 2

proposed methodology

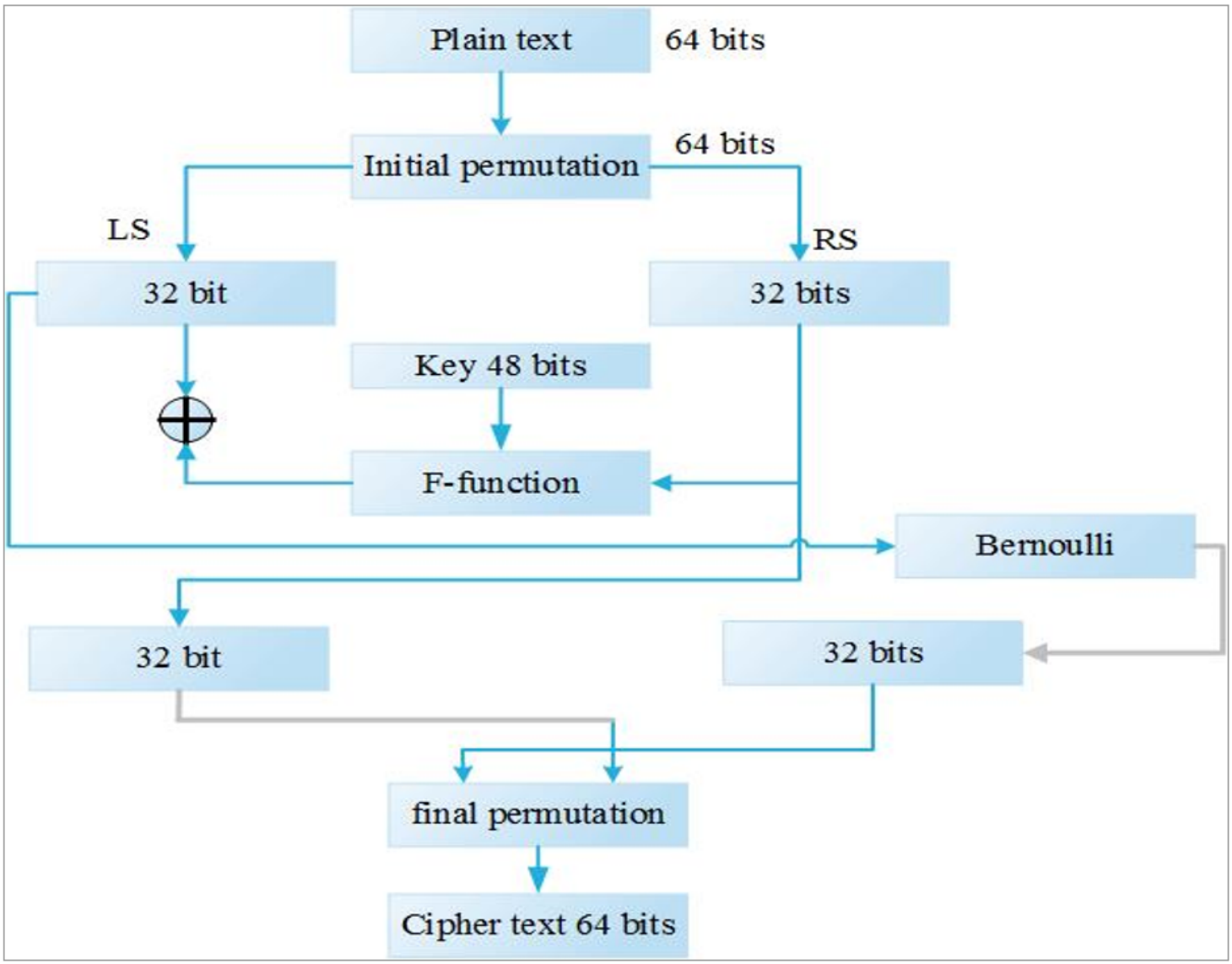

Figure 3

Proposed B-DES model

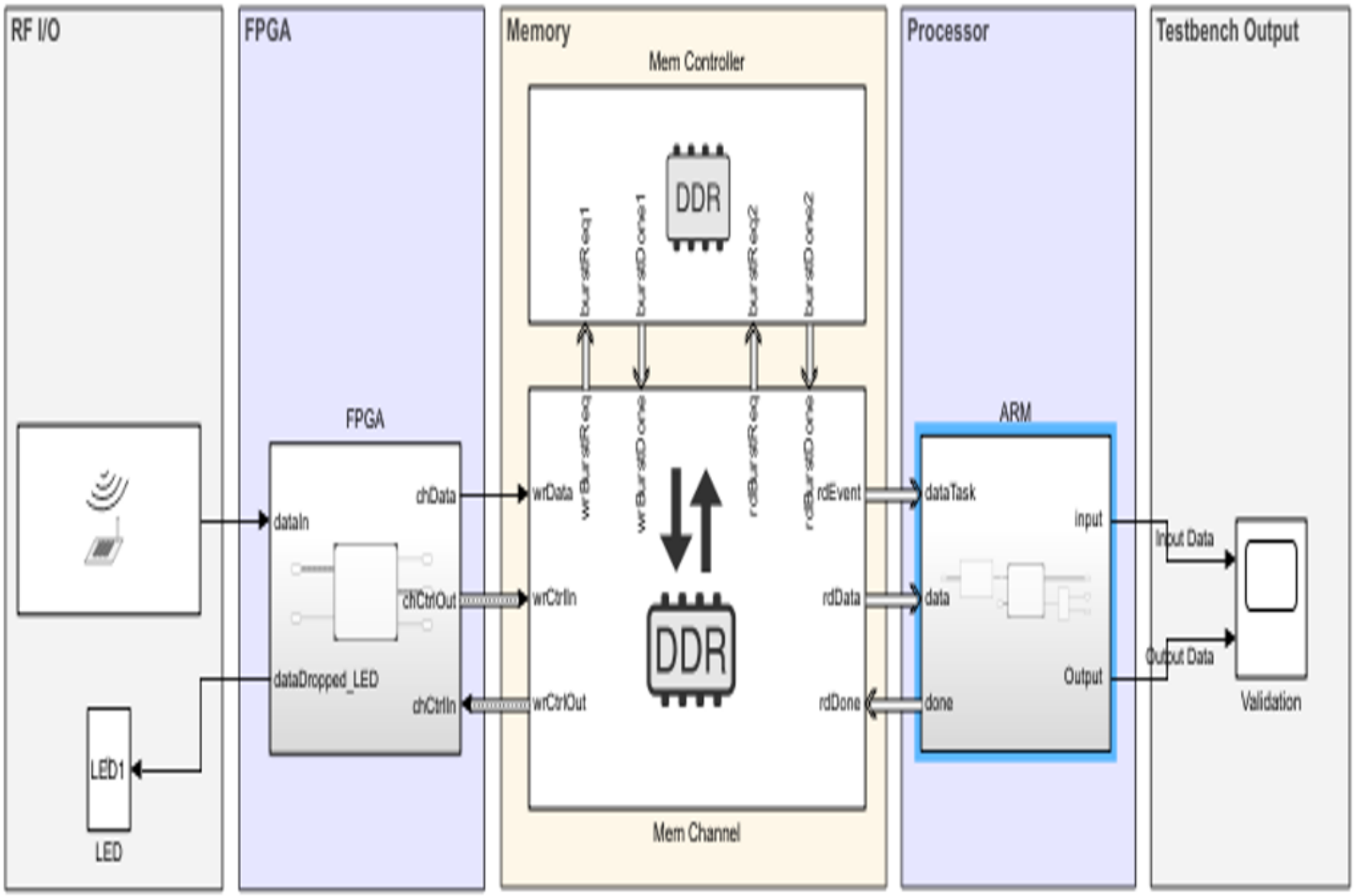

Figure 4

Simulink model of B-DES

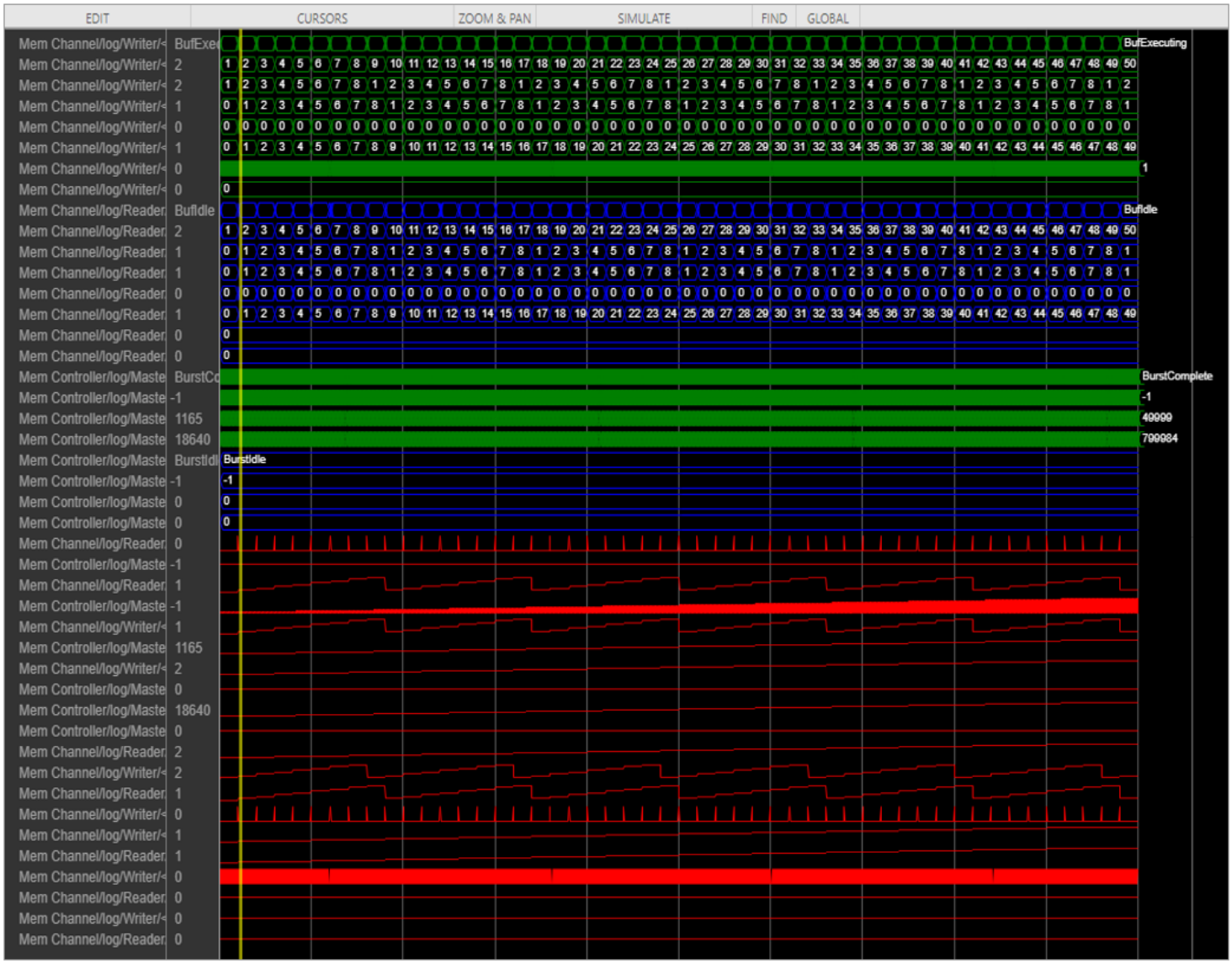

Figure 5

FPGA wave form of B-DES

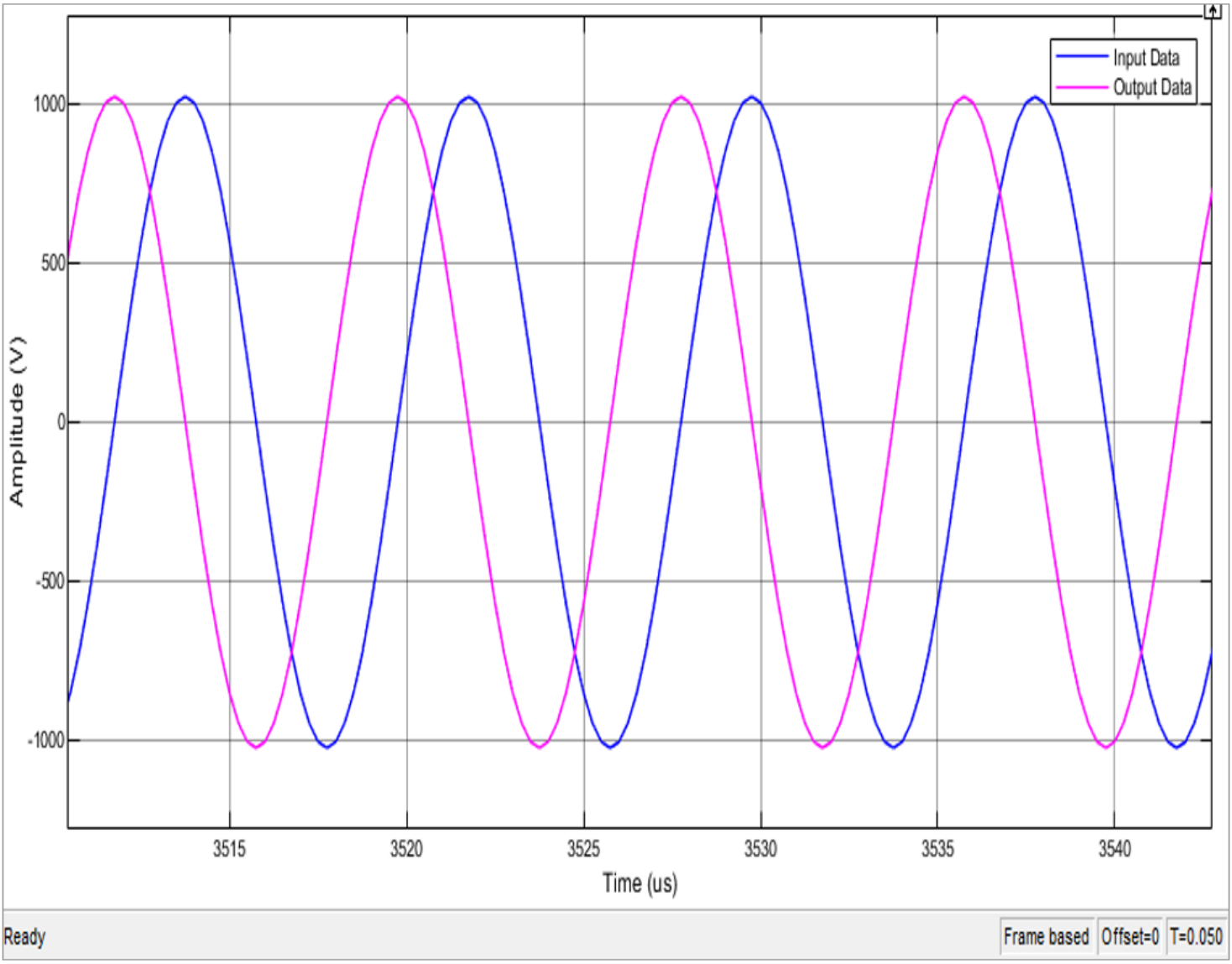

Figure 6

frequency of input and output signal

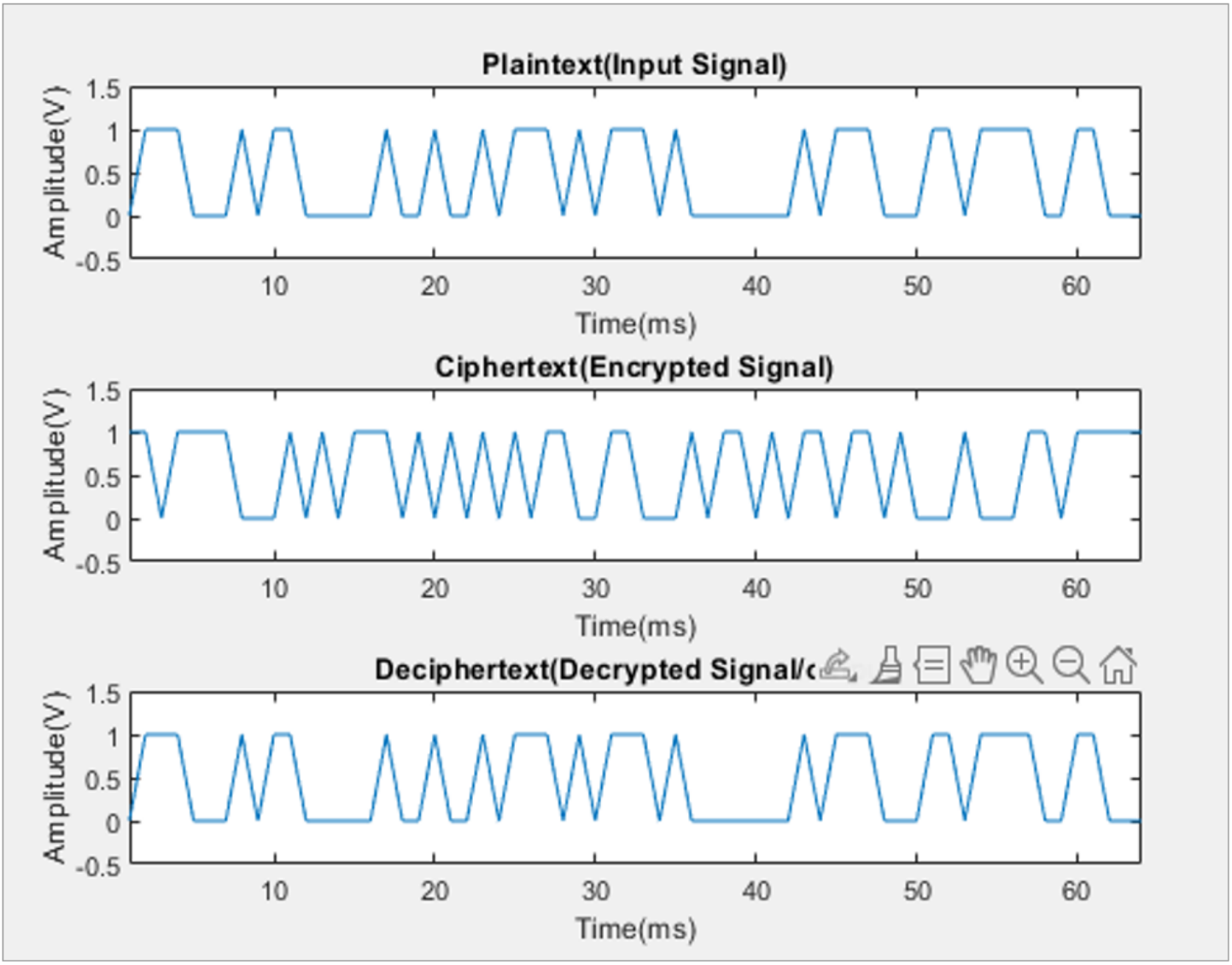

Figure 7

signal variation of the crypto process

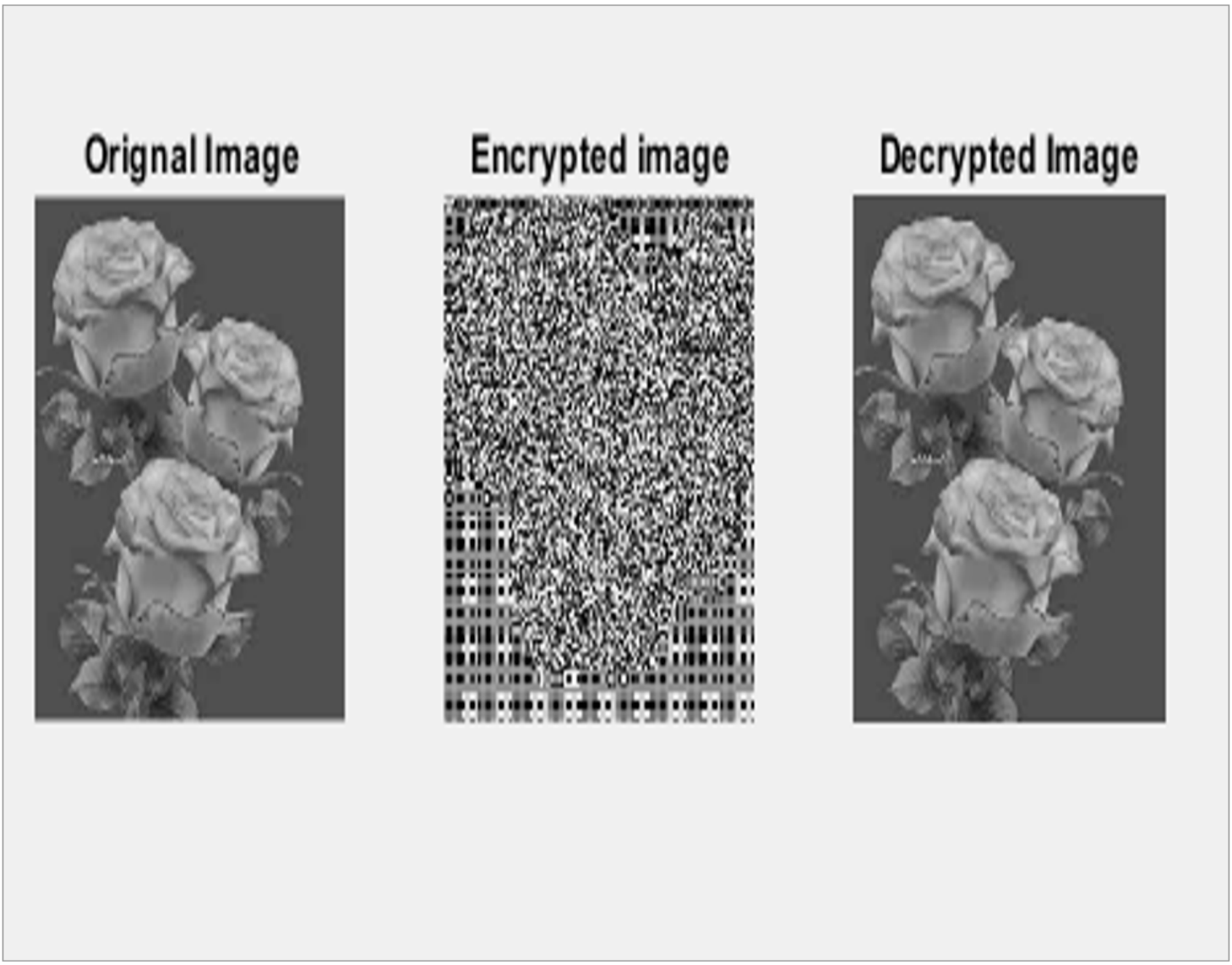

Figure 8

Input, encrypt and decrypt image

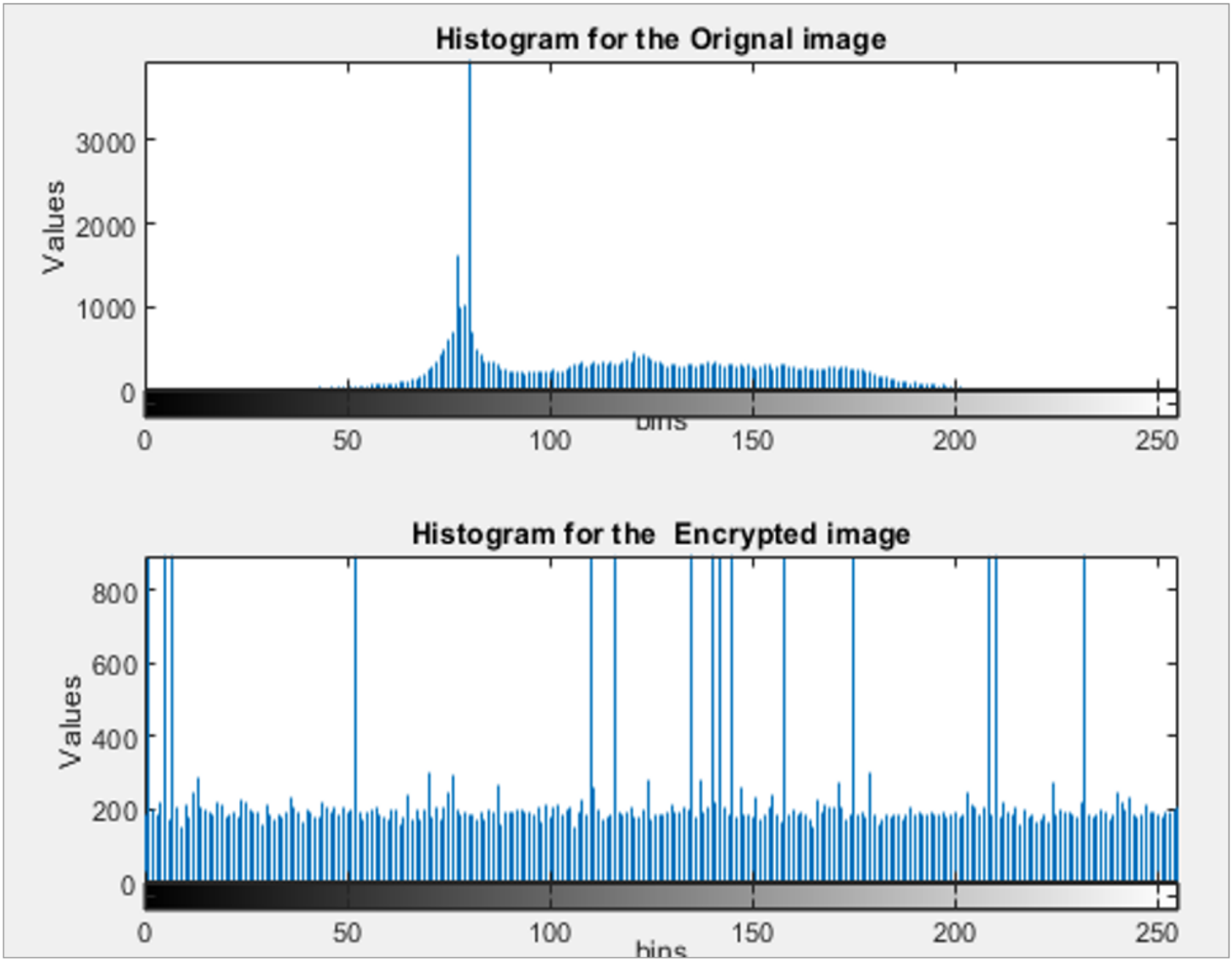

Figure 9

Image histogram data

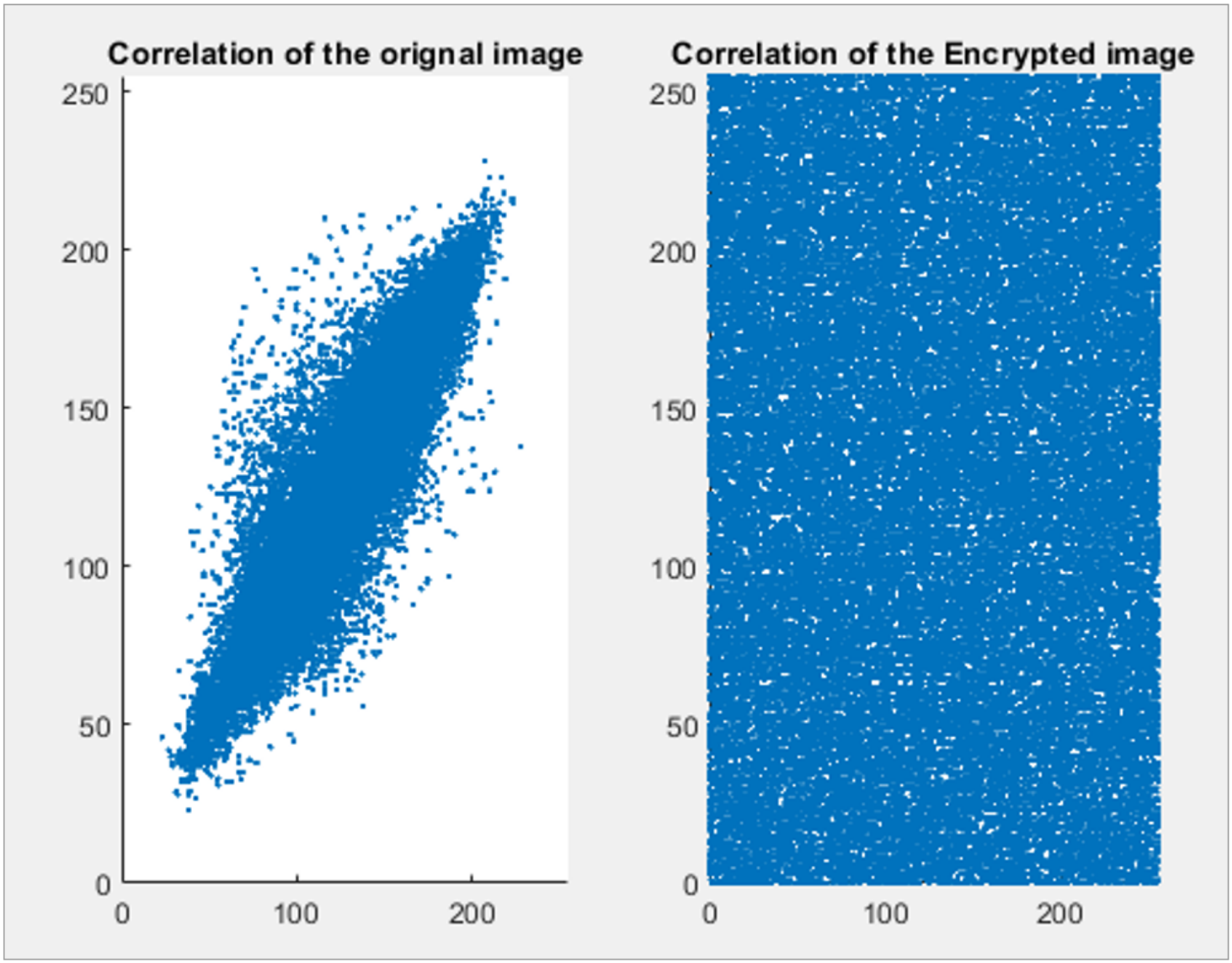

Figure 10

Correlation of the input data

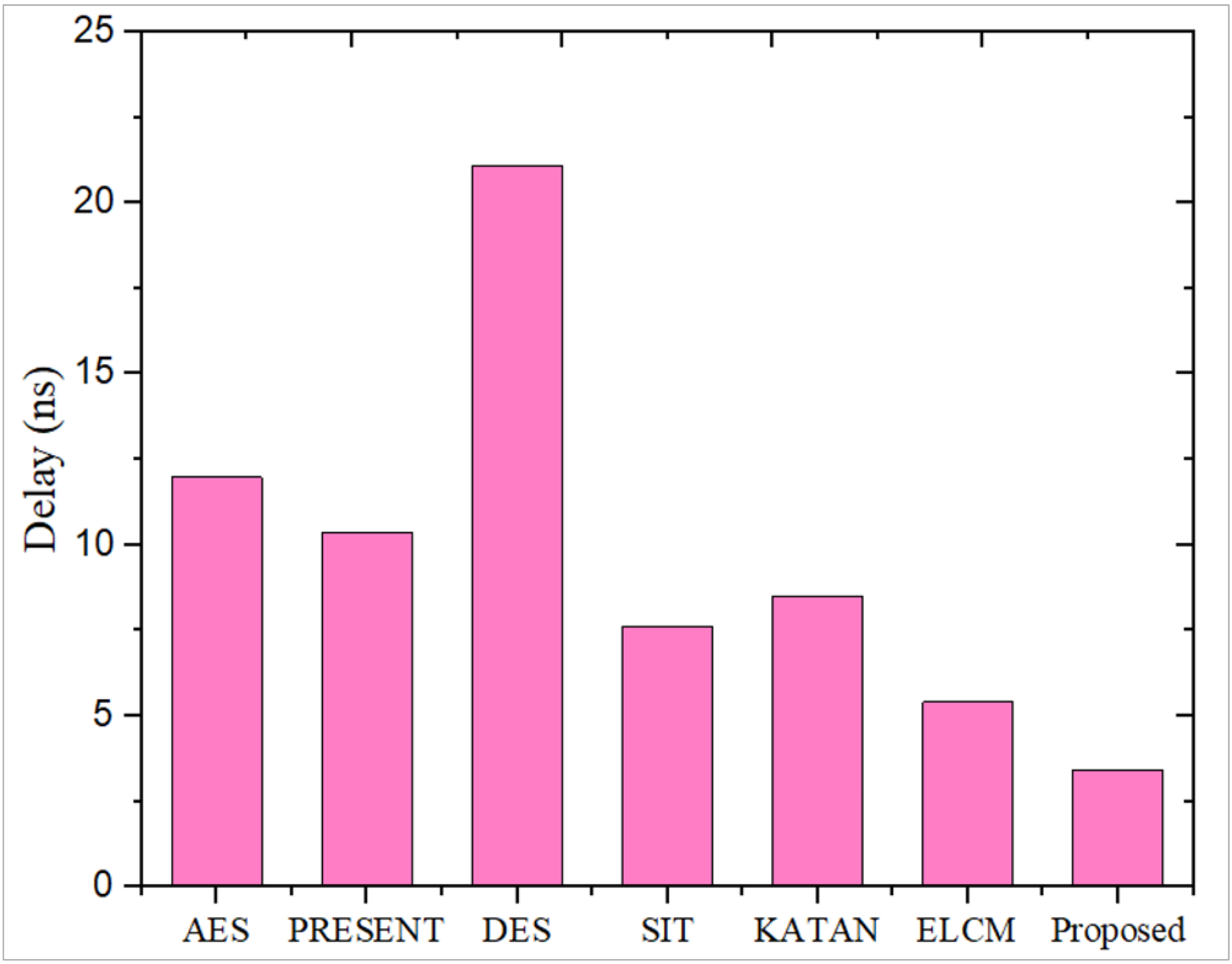

Figure 11

Transmission delay

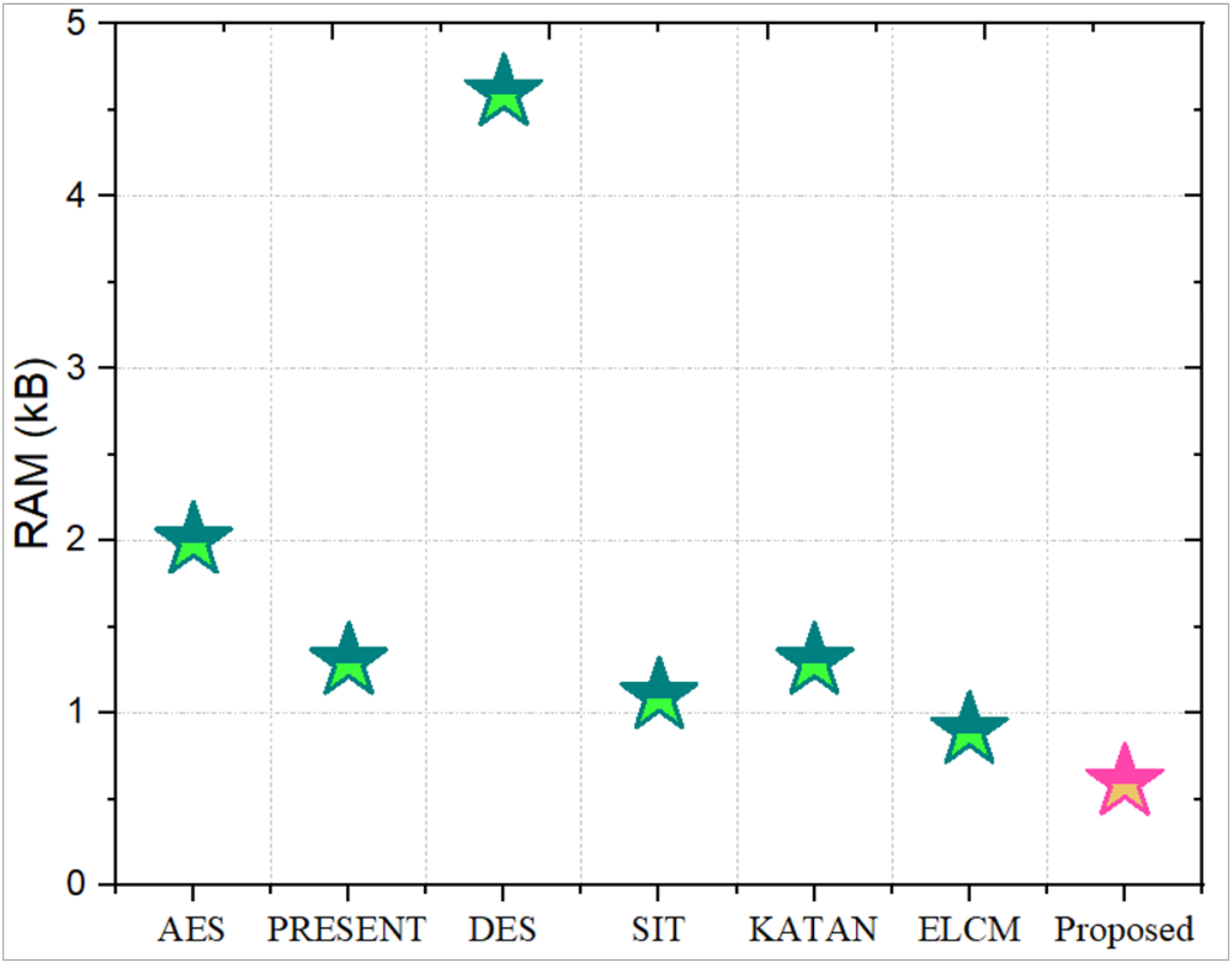

Figure 12

Comparison of memory usage

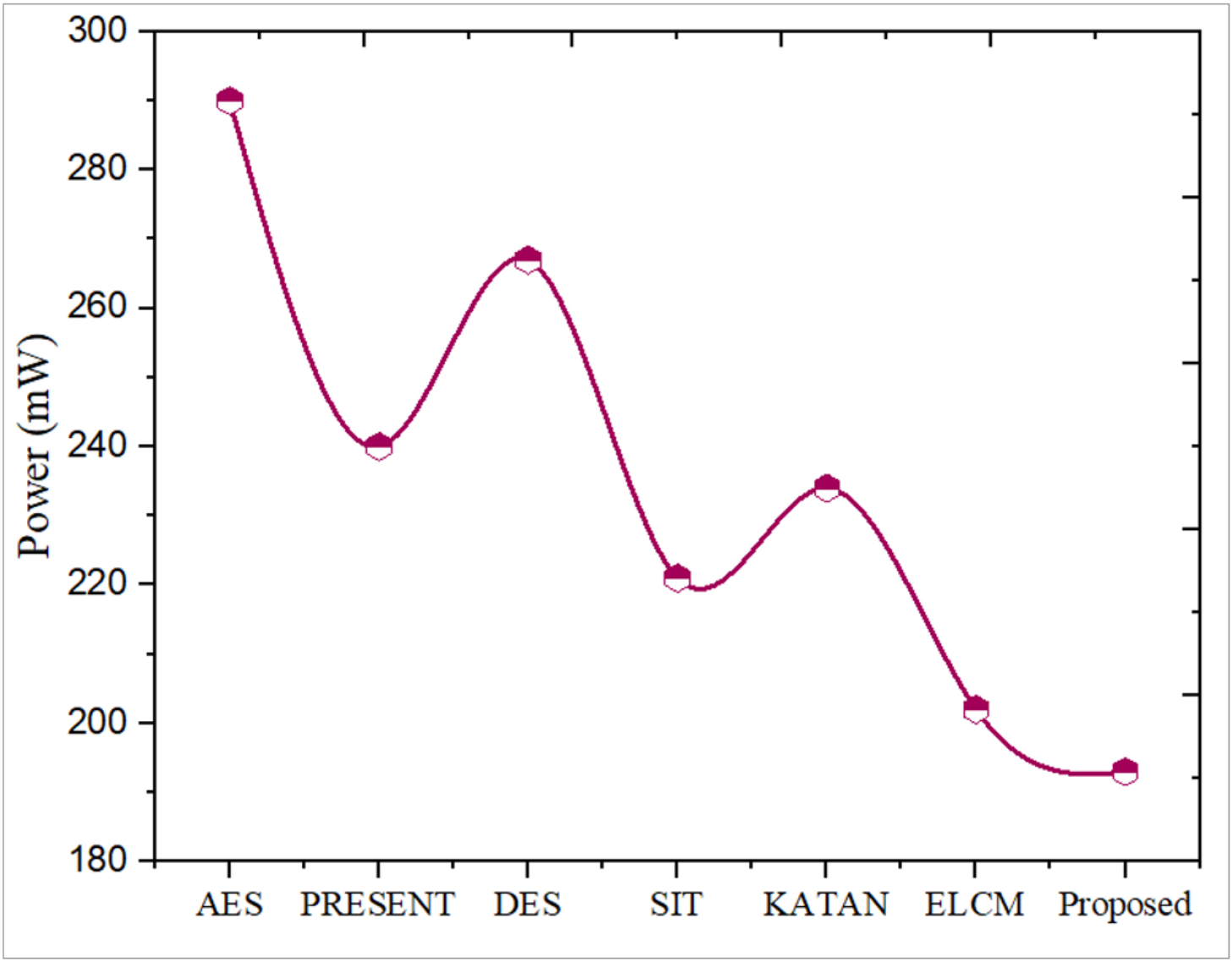

Figure 13

Power comparison