International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Dynamic and Secure Substitution Box for Efficient Speech Encryption Engine

S. Bhakthavathsalam1, Dr. S. Leela Lakshmi2
[1]PG Scholar, [2]Professor
Department of ECE, VEMU Institute of Technology, P.Kothakota, Andhra Pradesh, India

ARTICLEINFO

Article History:
Accepted: 25 April 2023
Published: 10 May 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
116-125

ABSTRACT

The Dynamic and Secure Substitution Box (DS2B) design suitable for IoT and resource-constrained platforms for efficient encryption. The DS2B has the advantages of simple structure and good encryption performance. A different number of strong S-boxes could be generated with minor variations in the DS2B parameters. Performance analyses of the DS2B, including differential/linear cryptanalysis, bijective, nonlinearity, strict avalanche criterion (SAC), and bit independence criterion (BIC) have been presented where high nonlinearity, and low differential uniformity are achieved. Besides, a comparison with recent S-boxes is introduced which shows the robustness of the DS2B. To maximize the throughput rate LUT based S box is replaced with dynamic composite S box with associated pipelining technique. Here flip flop-based masking is carried out inside S box module to achieve maximum level of transformation for securing the cipher key and adding resistance to any scan-based attacks. In this paper, security enhancement and high-speed solutions are provided without affecting the quality of the proposed core. Performance of proposed method is tested with key generation module and the simulation results proves the performance efficiency and hardware synthesis will prove the other metrics like high throughput rate and complexity overhead using Xilinx VIVADO tool.

Keywords: FPGA, S-box, speech encryption, cryptanalysis, dynamic. etc.

I. INTRODUCTION

Recently, privacy and security of audio communication networks take many of researchers concerns. They try to achieve this goal using different fundamental ways of hiding information. Scrambling of audio samples is a widely-used way of hiding data in both analog and digital speech. In [1] Matsunaga e t al. showed how EFT can be used in analog audio scrambling while application on digital audio is presented. Another technique has introduced by depending on using substitution box to increase the immunity of higher-order systems against attacks. Cosine number transform (CNT) is used also a finite audio encryption scheme.

The security of IoTs continues to attract the attention of researchers due to their pervasive nature. Implementing security algorithms on edge devices is a highly challenging task as they tend to have limited computation capability, small memory, and small power budget. The projection of fifty Billion Internet-of-Things (IoT) devices by 2020 has pushed the energy harvesting research to study new solutions for improving the lifetime of batteries. Therefore, the optimization of hardware implementation of IoT cryptographic engines is of paramount importance to address the issues of cost, throughput, and power budget. Most existing encryption designs for low-cost and low-power systems focus on optimizing the S-box, which has a significant effect on the area and energy cost. S-boxes may occupy up to 60% of the total crypto area, and consume up to 30% of the total power budget. An S-box is the nonlinear element of block encryption algorithms, which provides confusion property by hiding the relationship between the cipher text and the key. It is used as a non-linear component in several block ciphers such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Without achieving confusion in the encryption algorithm, it becomes vulnerable to various attacks. The security of the encryption algorithm is increased by producing more confusion in the S-box output. Therefore, an S-box is the target for the attack in the encryption algorithms. Hence, more confusion is needed in the S-box to secure the block encryption design. Traditional S-box is realized based on a Look-Up-Table LUT and is used to replace one secret element with another element from the S-box. Static and dynamic S-box are the common methods for block encryption algorithms. A static S-box uses fixed data for all inputs and is used frequently in the encryption algorithm. To overcome the weakness of the static S-boxes, various studies have investigated new methods to implement dynamic S-boxes. Dynamic S-box techniques used in the literature are complex and require substantial hardware resources to implement. Consequently, there is a demand for an algorithm that is simple, and able to generate dynamic S-boxes.

Security of speech information is essential for many applications including smart devices, e-learning, and video conferencing. Speech includes a lot of confidential data, it is important to encrypt the speech data before uploading it to the cloud. A number of schemes have been proposed in the literature for encrypting speech files. Different works have been introduced to produce cryptographically strong S-boxes. The strength can be estimated using differential and linear cryptanalysis. Nonlinearity is an important measure to estimate the security of the S-box. In general, any S-box showing a higher nonlinearity is secure toward the linear cryptanalytic attacks. Feistel structure is used to create dynamic S-boxes. A block encryption technique based on S-boxes for wireless sensor network was introduced. The S-box was created using a compound chaotic map, sinusoidal chaotic map, Baker map and the linear congruence generator. Moreover, other researchers have proposed S-boxes using chaotic systems and showed that the S-box based chaotic system is decently resilient to various attacks. A random bit sequence generated based on chaotic Boolean function is used to construct an S-box and use it for image encryption. An 8×8 S-box was presented, which needed 2048-bits LUT. In [26], 4-bit S-box was used to build a speech encryption engine. The data inside the S-box is changed every clock cycle based on chaotic system output. Moreover, the S-box can be optimized by using Boolean logic instead of LUT for a small area.

The hardware realization of block encryption algorithms heavily relies on the S-box design. As the IoT devices are highly constrained with limited memory and low power/energy consumption. A straightforward hardware realization of the S-box can be built using a look-up table (LUT) which needs a huge area. For efficient hardware implementation, smaller S-boxes are required rather than large S-boxes

as in the conventional methods, however smaller S-boxes will reduce the security. This paper introduces:

- A Dynamic and Secure Substitution Box (DS2B) for efficient speech encryption engine.
- A large number of strong S-boxes can be produced with little changes in the DS2B parameters, where the DS2B address changes every clock cycle to select different data and generate a new S-box.
- Speech encryption engine is proposed to verify the DS2B method, where different security evaluations are presented including NIST, MSE, correlation, histogram, and spectrogram.
- A performance comparison analysis with recent S-boxes is introduced which shows the robustness of the DS2B.
- An FPGA experiment has been added to verify the proposed speech encryption design.

Chaos-based cryptography is one of the effective strategies that attract researchers at the start of last decade. Characteristics of chaotic systems are the main reason for using them in encryption schemes, Properties like sensitivity to initial conditions and unpredictability of chaotic systems behavior make them suitable to be used in encryption. Usually, chaotic systems are combined with one of the original encryption techniques. A corporation between data compression and chaotic map in speech encryption. Modified tent map is used with bit permutation strategy in speech encryption application.

In modern-day block ciphers, the role of substitution-boxes is to transform the plaintext data nonlinearly to generate cipher-text data with sufficient confusion. It has been well-confirmed that the robustness and security of such block ciphers heavily based on the cryptographic strength of the underlying substitution-boxes. Reason being, they are the only components that are held responsible to bring required nonlinearity and complexity into the security system which can frustrate the attackers. Accordingly, a number of different concepts have been explored to construct strong S-boxes. To move forward with the same aim, a novel simple modular approach, the very first time, is investigated to construct nonlinear S-box in this paper. The proposed new modular approach consists of three operations such as new transformation, modular inverses, and permutation. A number of highly nonlinear S-boxes can be easily constructed with slight changes in the novel transformation parameters. An example S-box is presented whose critical performance assessment against some benchmarking criterions such as high nonlinearity, absence of fixed points, fulfillment of SAC and BIC properties, low differential uniformity and linear approximation probability and comparison with recent S-boxes demonstrate its upright cryptographic potentiality. In addition, an image encryption algorithm is also proposed wherein the generated S-box is applied to perform the pixels shuffling and substitution for strong statistical and differential encryption performance.

Data and information communication has become very important ingredient of today's technological life and considered as significant assets of an individual or organization. If the confidentiality of information is compromised, then the information can be used for harmful purposes. Current innovations in information technology and their prolific applications in our life have caused in a gigantic growth in the size of the data being transmitted online. The private information being very sensitive assets require protection from attackers. Therefore, prior to its transmission, data demand its protection and needs methods for its transformation into a meaningless form for the invaders. Cryptographic algorithms are the mathematical methods and techniques that assist in the protection of data. Stream ciphers transform the data in a bit-by-bit or byte-by-byte manner. Whereas, the block ciphers transform data in chunks which comprise large number ofbits or bytes at a time. In modern symmetric encryption, block ciphers are considered as one of the most effective tools for data protection. Data Encryption Standard (DES), Blowfish, Advanced Encryption Standard (AES), RC5, etc. are

examples of contemporary block ciphers. Precise implementations of block ciphers are easy and are more general in nature than the stream ciphers. One category of prevalent block ciphers is known as the SP network-based block ciphers. These block ciphers use two major operations of substitution and permutation for the transformation of data into a perplexing form.

A substitution operation substitutes a byte/block with another byte/block using a substitution table known as a substitution box or S-box. On the other hand, a permutation process shuffles the input bits or bytes in some linear fashion. A substitution-box is a pivotal constituent of modern-day block ciphers that helps in the generation of a muddled cipher text for the specified plaintext. Through the incorporation of S-box, a nonlinear mapping among the input and output data is established to create confusion. The more confusion an S-box can create in the output data, the more secure a block cipher is. As a result, the provision of security by a block cipher employing one or more S-boxes directly depends on how much stronger S-boxes are. Block ciphers consist of many components in addition to one or more S-boxes. Contrary to other components, an S-box is the alone nonlinear component of block ciphers that supports the enhancement of data protection. Generally, a block cipher uses either a static S-box or one or more dynamic S-boxes. A static S-box is fixed for every incoming data and secret key which is used repeatedly in the block cipher. A block cipher based on a static S-box employs that S-box in all its rounds. A static S-box allows an attacker to inspect its characteristics, discover its fragilities, and eventually find the chance of getting plaintext from the respective cipher-text. As an example, static S-boxes employed in Data Encryption Standard (DES) were an easy target for the attackers. Consequently, to overcome the weaknesses due to static S-boxes, many cryptographers have explored innovative techniques to design dynamic S-boxes. Dynamic S-boxes are generated using cipher key and provide a way to augment the cryptographic power of a block cipher. Construction and usage of the key-dependent and dynamic S-boxes in a cipher enhance its cryptographic power. Blowfish cipher employs such dynamic S-boxes in its working.

The literature review is presented in section 2. Further, in section 3, Existing System was discussed. Moreover, in next section IV, briefly explain about Proposed System and finally the Simulation results discussed in section V. Conclusion and future work are presented by last sections VI.

II. LITERATURE SURVEY

A.H. Elsafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, "FPGA speech encryption realization based on variable S-box and memristor chaotic circuit," in Proc. 30th Int. Conf. Microelectron. (ICM), Dec. 2018, pp. 152–155.

This paper introduces a new encryption/decryption scheme based on a dynamic substitution box concept. Values of the proposed S-Box are different for each sample depending on the behavior of a memristor-based chaotic system. MATLAB simulations and FPGA implementation for the circuit are presented with throughput 4.266 Gbit/s. Also, FPGA realization for encryption/decryption scheme is proposed. Entropy, MSE, correlation coefficient tests are applied on two different input flies to examine the efficiency of this cryptosystem. Recently, privacy and security of audio communication networks take many of researchers concerns. They try to achieve this goal using different fundamental ways of hiding information. Scrambling of audio samples is a widely-used way of hiding data in both analog and digital speech. In [1] Matsunaga e t al. showed how EFT can be used in analog audio scrambling while application on digital audio is presented in [2], [3]. Another technique has introduced by [4] depending on using substitution box to increase the immunity of higherorder systems against attacks. Cosine number transform (CNT) is used also in [5] a finite audio encryption scheme. Characteristics of chaotic systems

are the main reason for using them in encryption schemes, Properties like sensitivity to initial conditions and unpredictability of chaotic systems behavior make them suitable to be used in encryption. Usually, chaotic systems are combined with one of the original encryption techniques. A corporation between data compression and chaotic map in speech encryption is proposed. In, modified tent map is used with bit permutation strategy in speech encryption application.

A.Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," Entropy, vol. 20, no. 7, p. 525, Jul. 2018.

In this paper, we present a novel method to construct cryptographically strong bijective substitution-boxes based on the complicated dynamics of a new hyperchaotic system. The new hyperchaotic system was found to have good characteristics when compared with other systems utilized for S-box construction. The performance assessment of the proposed S-box method was carried out based on criteria, such as high nonlinearity, a good avalanche effect, bit-independent criteria, and low differential uniformity. The proposed method was also analyzed for the batch-generation of 8 × 8 S-boxes. The analyses found that through a proposed purely chaos-based method, an 8 × 8 S-box with a maximum average high nonlinearity of 108.5, or S-boxes with differential uniformity as low as 8, can be retrieved. Moreover, small-sized S-boxes with high nonlinearity and low differential uniformity are also obtainable. A performance comparison of the anticipated method with recent S-box proposals proved its dominance and effectiveness for a strong bijective S-box construction.

Recent advancements in cloud computing, smart devices, social media, etc., for communication have substantially raised the amount of users' private data. Consequently, the issue of ensuring and maintaining end to end confidentiality of sensitive data has become more prominent than before. To provide data secrecy for storage and communication, block cryptosystems have been playing a crucial role in the past few decades.

S. N. George, N. Augustine, and D. P. Pattathil, "Audio security through compressive sampling and cellular automata," Multimedia Tools Appl., vol. 74, no. 23, pp. 10393–10417, Dec. 2015.

In this paper, a new approach for scrambling the compressive sensed (CS) audio data using two dimensional cellular automata is presented. In order to improve the security, linear feedback shift register (LFSR) based secure measurement matrix for compressive sensing is used. The basic idea is to select the different states of LFSR as the entries of a random matrix and orthonormalize these values to generate a Gaussian random measurement matrix. It is proposed to generate the initial state matrix of cellular automata using an LFSR based random bitstream generator. In order to improve the security and key space of the proposed cryptosystem, piecewise linear chaotic map (PWLCM) based initial seeds generation for LFSRs is used. In the proposed approach, the initial value, parameter value and the number of iterations of PWLCM are kept as secret to provide security. The proposed audio encryption method for CS audio data is validated with different compressive sensing reconstruction approaches. Experimental and analytical verification shows that the proposed encryption system gives good reconstruction performance, robustness to noise, high level of scrambling and good security against several forms of attack. Moreover, since the measurement matrix used for CS operation and the initial state matrix used for 2D cellular automata are generated using the secret key, the storage/transmission requirement of the same can be avoided.

A.Alghafis, N. Munir, and M. Khan, "An encryption scheme based on chaotic Rabinovich-Fabrikant system and S8 confusion component," Multimedia Tools Appl., vol. 80, no. 5, pp. 7967–7985, Feb. 2021.

In this research article, we have proposed a novel image encryption scheme for the confidentiality of digital information. The modern block ciphers based

on confusion and diffusion characteristic, as proposed by Claude Shannon in 1949. Firstly, we have designeda nonlinear confusion component of a block cipher and apply the action of symmetry groupS8to generate a pool of 40,320 substitution boxes with the same cryptographic strength. These nonlinear components are responsible for adding confusion in the encryptionalgorithm. Secondly, we have utilized a nonlinear chaotic dynamical system to add diffusion capability in our proposed encryption scheme. The suggested scheme is further examined under security performance evaluations, which shows the appropriateness of ouroffered scheme for digital contents.

Q. Zhang, Y. Li, Y. Hu, and X. Zhao, "An encrypted speech retrieval method based on deep perceptual hashing and CNN-BiLSTM," IEEE Access, vol. 8, pp. 148556–148569, 2020.

Since convolutional neural network (CNN) can only extract local features, and long shortterm memory (LSTM) neural network model has a large number of learning calculations, a long processing time and an obvious degree of information loss as the length of speech increases. Utilizing the characteristics of autonomous feature extraction in deep learning, CNN and bidirectional long short-term memory (BiLSTM) network are combined to present an encrypted speech retrieval method based on deep perceptual hashing and CNN-BiLSTM. Firstly, the proposed method extracts the Log-Mel Spectrogram/MFCC features of the original speech and enters the CNN and BiLSTM networks in turn for model training. Secondly, we use the trained fusion network model to learn the deep perceptual feature and generate deep perceptual hashing sequences. Finally, the normalized Hamming distance algorithm is used for matching retrieval. In order to protect the speech security in the cloud, a speech encryption algorithm based on a 4D hyperchaotic system is proposed. The experimental results show that the proposed method has good discrimination, robustness, recall and precision compared with the existing methods, and it has good retrieval efficiency and retrieval accuracy for longer speech. Meanwhile, the proposed speech encryption algorithm has a high key space to resist exhaustive attacks.

M. F. Tolba, W. S. Sayed, M. E. Fouda, H. Saleh, M. Al-Qutayri, B. Mohammad, and A. G. Radwan, "Digital emulation of a versatile memristor with speech encryption application," IEEE Access, vol. 7, pp. 174280–174297, 2019.

Memristor characteristics such as nonlinear dynamics, state retention and accumulation are useful for many applications. FPGA implementation of memristor-based systems and algorithms provides fast development and verification platform. In this work, we first propose a versatile digital memristor emulator that exhibits either continuous or discrete behaviors, similar to valence change memories (VCM) or the electrochemical metallization memories. Secondly, the proposed memristor emulator is used to design a chaotic generator circuit utilizing the memristor's nonlinearity. Finally, the chaotic system is used to design a speech encryption engine to demonstrate its capabilities. The memristor emulator, chaotic generator, and the encryption system were implemented on Nexys 4 Artix-7 FPGA XC7A100T. The implementation results show an efficiency in throughput and hardware resources utilization compared to the previous works. In addition, the encryption system results show good performance against several perceptual, statistical attacks in addition to resistance to security attacks tests including differential attacks, NIST tests, key space analysis, mean square error (MSE), correlation, histogram and spectrogram.

III. EXISTING SYSTEM

In the existing method DES block ciphers are introduced. An S-box is the nonlinear element of block encryption algorithms, which provides confusion property by hiding the relationship between the cipher text and the key. It is used as a

non-linear component in several block ciphers such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Without achieving confusion in the encryption algorithm, it becomes vulnerable to various attacks. The security of the encryption algorithm is increased by producing more confusion in the S-box output. Therefore, an S-box is the target for the attack in the encryption algorithms.

An S-box is the nonlinear element of block encryption algorithms, which provides confusion property by hiding the relationship between the cipher text and the key. It is used as a non-linear component in several block ciphers such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Without achieving confusion in the encryption algorithm, it becomes vulnerable to various attacks. The security of the encryption algorithm is increased by producing more confusion in the S-box output. Therefore, an S-box is the target for the attack in the encryption algorithms. Hence, more confusion is needed in the S-box to secure the block encryption design. Traditional S-box is realized based on a Look-Up-Table LUT and is used to replace one secret element with another element from the S-box. Static and dynamic S-box are the common methods for block encryption algorithms. A static S-box uses fixeddata for all inputs and is used frequently in the encryption algorithm. To overcome the weakness of the static S-boxes, various studies have investigated new methods to implement dynamic S-boxes. Dynamic S-box techniques used in the literature are complex and require substantial hardware resources to implement. Consequently, there is a demand for an algorithm that is simple, and able to generate dynamic S-boxes.

Security of speech information is essential for many applications including smart devices, e-learning, and video conferencing. Speech includes a lot of confidential data, it is important to encrypt the speech data before uploading it to the cloud [12]. A number of schemes have been proposed in the literature for encrypting speech files. Different works have been introduced to produce cryptographically strong S-boxes.

IV. PROPOSED METHOD

S-Box is an essential component in the modern cryptographic algorithms that will add the confusion property to hide the relationship between the cipher text and the plaintext/key. The S-box block provides a nonlinearity between the input data and encrypted output data in which an attacker cannot deduce input information from the output encrypted data. The development of an S-box must be simple and efficient. This paper presents a method for obtaining dynamic and secure S-Box (DS2B) to be used in a speech encryption application. Figure 1 presents the DS2B look up table (LUT) design, where the 4-bits of the feedback signal Fb are used as an address (row and column addresses). The design process of creating the proposed S-box is performed as follows:

- Create a fixed 4-bit S-box LUT that achieved a good nonlinearity.
- Replace the address of the S-box with 4-bit Fb signal where Fb is a 4-bit taken from the previous encrypted output.
- The S-box LUT address is performed as follows: Fb[1] is inverted twice then repeated twice. Fb[0] is inverted for each row of the table. The same process is applied for Fb[3] and Fb[2].
- Based on the previous process of inverting Fb, all possible 4-bit Fb values will be covered and the proposed DS2B LUT is generated.

There are 24 possible S-boxes that could be generated for a specific inverting and non-inverting process in which 16 S-boxes can be generated from a 4-bit input. As shown in the example presented in Fig. 1, for each Fb value, an S-box is obtained.

- If Fb = 4'b1100, a new S-box address is created. In which, the input "0" will be replaced with "14".
- If Fb = 4'b0101, a new S-box address is created. In which, the input "0" will be replaced with "2".

The inverting and non-inverting process could be changed to obtain other 16 S-boxes. The proposed method for generating the 4-bit S-box can be generalized to produce an 8-bit S-box as shown in Fig. 2. As can be seen, the addresses are 4-bits (row) and 4-bits (column). Each selected data is composed of 8 bits.

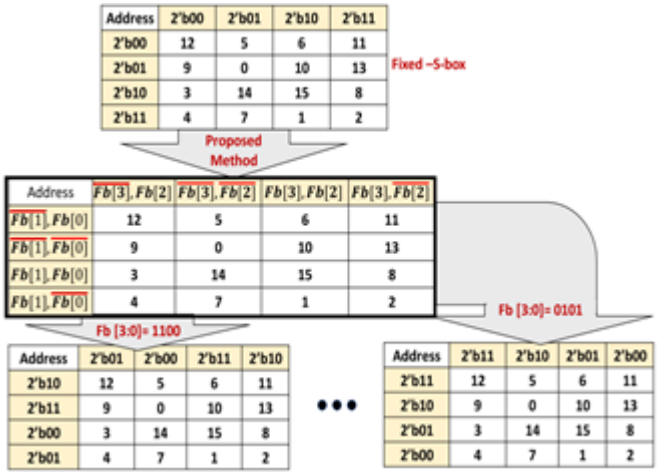

Figure 1: Proposed DS2B LUT design, where the address is created based on changing Fb bits. The addresses are 2-bits (row) and 2-bits (column). Each selected data is composed of 4 bits.

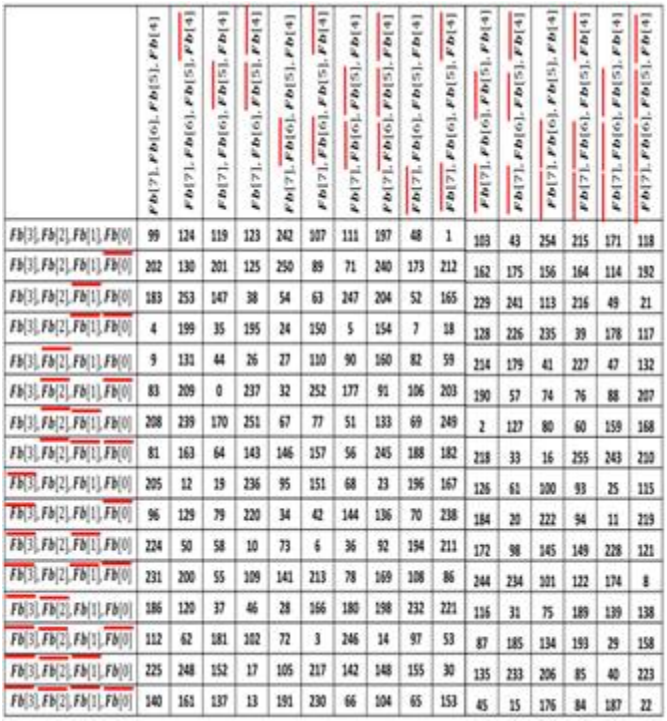

Figure 2: DS2B LUT design, where the address is created based on changing Fb bits. The addresses are 4-bits (row) and 4-bits (column). Each selected data is composed of 8 bits.

Speech Encryption Scheme:

This Section aims to introduce a speech encryption scheme based on the DS2B which was presented in the previous Section II. Figure 3 shows the hardware architecture of the proposed encryption/decryption scheme without the key generation procedure, where the input is a 16-bit fixed-point voice sample. The 16 bits input is divided into four parts (4-bits in each part) to drive the 4 DS2B blocks. The 4 DS2B blocks inputs are the Fb [15:0] and the 16 bits of the input speech signal. Each DS2B block is designed based on a 4-bit to 4-bit swap operation that was introduced. The outputs of the four DS2Bs are concatenated then "Xored" with the Fb signal to produce the encrypted signal.

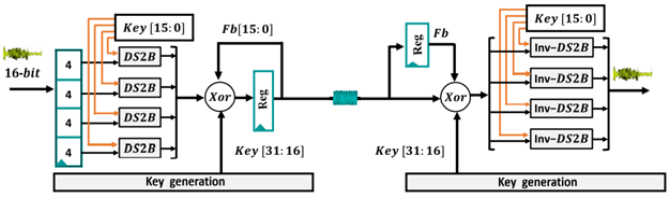

Figure 3: Proposed encryption hardware implementation with the key generation

The decryption process can be done by inverting the operation as shown in Fig. 3. The proposed speech encryption can be improved by adding the key generation block as presented in Fig. 4. The input encryption key is 128 bits. The encryption key drives the key generation block, where a multiplexer is used to load the input key when the "sel" signal is set to "1" or to select the previous encryption key when the "sel" signal is set to "0". The key registeris shifted left (33-bit) as shown in Fig. 5. The 16 most significant bits of the shifted key register drives four DS2B blocks. The outputs of the four DS2B blocks (16-bit) are concatenated with the 116 LSB of the shifted key register to create the new encryption key. In speech encryption with the key generation, the input signal derives the four DS2Bs. Key [15:0] bits are used to create the 4 DS2Bs. Finally, the DS2Bs outputs are XORed with the key [31:16] to generate the encrypted speech signal. The decryption process can be easily done by inverting the operation in Fig. 4.

The 4-bit DS2B size can be reduced further into a 2-bit DS2B, where 8 (2-bit) DS2Bs are required in the proposed encryption instead of 4 (4-bit) DS2Bs but this will reduce the security level substantially.

V. SIMULATION RESULTS

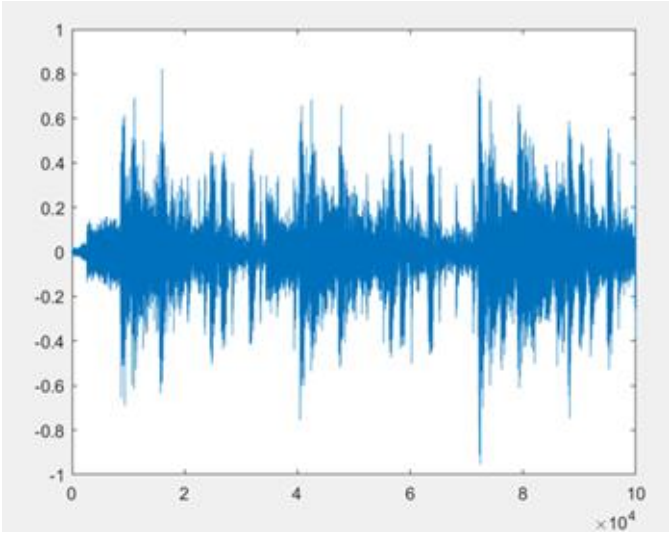

Figure 4: Input speech signal

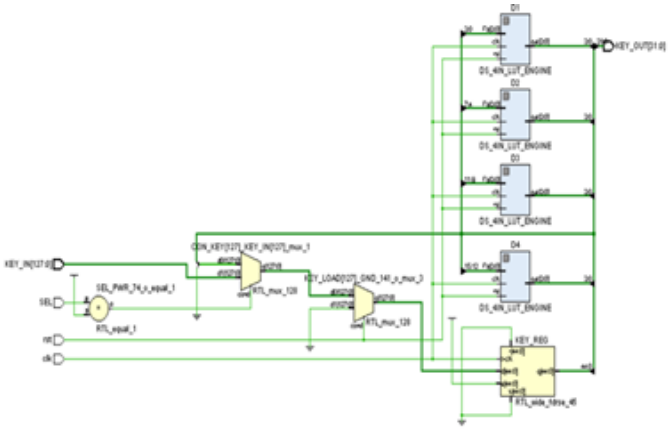

Figure 5: RTL Schematic

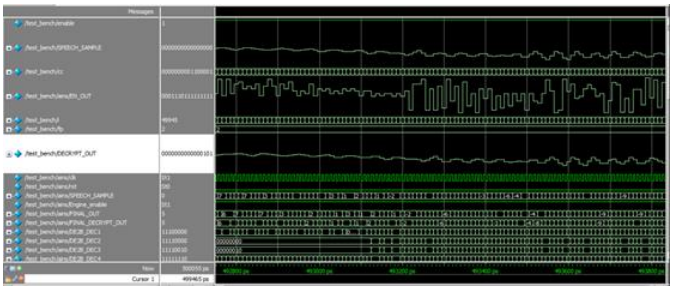

Figure 6: output Waveform

VI. CONCLUSION

A speech encryption scheme based on a DS2B was designed and realized on an FPGA using Verilog HDL. The DS2B passed through a number of existing tests to examine its cryptographic strength; achieved results proved the ability to build S-boxes that possess high resistance against linear attack and differential attack. Various comparisons based on different security evaluation techniques and hardware resource usage were presented. The encryption system hardware implementation requirements were more efficient than previous work. The encryption scheme achieved a throughput highcompared with the previous work. The proposed design with key generation encrypts silence periods and make them much harder to detect unlike previous works.

Future works

In future the proposed work can be extended with the DS2B-based speech encryption scheme can be integrated with other systems, such as cloud-based speech recognition and natural language processing systems. This would enhance the security of these systems and ensure that sensitive information is protected.

VII. REFERENCES

[1]. W. Yu and S. Köse, "A lightweight masked AES implementation for securing Iot against CPA attacks," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 64, no. 11, pp. 2934–2944, Nov. 2017.

[2]. M. Alhawari, D. Kilani, B. Mohammad, H. Saleh, and M. Ismail, "An efficient thermal energy harvesting and power management for μwatt wearable biochips," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2016, pp. 2258–2261.

[3]. M. Alhawari, T. Tekeste, B. Mohammad, H. Saleh, and M. Ismail, "Power management unit for multi-source energy harvesting in wearable

electronics," in Proc. IEEE 59th Int. Midwest Symp. Circuits Syst. (MWSCAS), Oct. 2016, pp. 1–4.

[4]. S. Mathew, S. Satpathy, V. Suresh, M. Anders, H. Kaul, A. Agarwal, S. Hsu, G. Chen, and R. Krishnamurthy, "340 mV–1.1 V, 289 Gbps/W, 2090-gate nanoAES hardware accelerator with area-optimized encrypt/decrypt GF(2 4) 2 polynomials in 22 nm tri-gate CMOS," IEEE J. Solid-State Circuits, vol. 50, no. 4, pp. 1048–1058, Apr. 2015.

[5]. G. Bansod, N. Raval, and N. Pisharoty, "Implementation of a new lightweight encryption design for embedded security," IEEE Trans. Inf. Forensics Security, vol. 10, no. 1, pp. 142–151, Jan. 2015.

[6]. D.-H. Bui, "An innovative lightweight cryptography system for Internetof-Things ULP applications," Ph.D. dissertation, Dept. Micro Nanotechnol./Microelectron., Hanoi Nat. Univ., Hanoi, Vietnam, Univ. Grenoble Alpes, Grenoble, France, 2019. [Online]. Available: https://tel.archivesouvertes.fr/tel-02295267/

[7]. F. Özkaynak, V. Çelik, and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic Chen system," Signal, Image Video Process., vol. 11, no. 4, pp. 659–664, May 2017.

[8]. A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," IEEE Access, vol. 8, pp. 150326–150340, 2020.

[9]. E. A. Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," Entropy, vol. 20, no. 7, p. 525, Jul. 2018.

[10]. S. N. George, N. Augustine, and D. P. Pattathil, "Audio security through compressive sampling and cellular automata," Multimedia Tools Appl., vol. 74, no. 23, pp. 10393–10417, Dec. 2015.

[11]. A. Alghafis, N. Munir, and M. Khan, "An encryption scheme based on chaotic Rabinovich-Fabrikant system and S8 confusion component," Multimedia Tools Appl., vol. 80, no. 5, pp. 7967–7985, Feb. 2021.

[12]. Q. Zhang, Y. Li, Y. Hu, and X. Zhao, "An encrypted speech retrieval method based on deep perceptual hashing and CNN-BiLSTM," IEEE Access, vol. 8, pp. 148556–148569, 2020.

[13]. M. F. Tolba, W. S. Sayed, M. E. Fouda, H. Saleh, M. Al-Qutayri, B. Mohammad, and A. G. Radwan, "Digital emulation of a versatile memristor with speech encryption application," IEEE Access, vol. 7, pp. 174280–174297, 2019.

Cite this Article

S. Bhakthavathsalam, Dr. S. Leela Lakshmi, "Dynamic and Secure Substitution Box for Efficient Speech Encryption Engine", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 3, pp. 116-125, May-June 2023. Journal URL : https://ijsrst.com/IJSRST5231037