AN ADVANCED ACFA ARCHITECTURE FOR SECURED LIGHTWEIGHT ENCRYPTION AND DECRYPTION WITH LFSR

[1]JAYASHREE CHAVAN, [2]Dr.AMIT JAIN
[1]Research Scholar, Department of ECE, Sunrise University, Alwar, Rajasthan, India.
[2]Research Guide, Department of ECE, Sunrise University, Alwar, Rajasthan, India.

ABSTRACT: The advanced safety and security mechanisms can be very important in all of the smart applications for 5G communication. Lightweight encryption and decryption enables secure and efficient communication between networked smart objects. The adaptive composite field architecture (ACFA) is 128-bit cipher known to be highly efficient in hardware implementations. Therefore a modified ACFA is required for increasing the safety and security mechanisms in order to overcome the security weakness of the ACFA against attacks. In this proposal, an advanced ACFA architecture for secured Lightweight encryption and decryption with LFSR is presented. This advanced ACFA developed in this uses the Linear Feedback Shift Register (LFSR) designed with semiconductor device technology to overcome the security weakness against attacks. The LFSR is easy to implement in hardware and can be used to create pseudo random number generator that can generate a secure cryptographic key. Then low-cost top-level lightweight encryption/decryption is implemented for 5G communication by integrating the novel s-box approach using the developed advanced ACFA and its performance is analyzed. The proposed architecture can achieve a low area and a high throughput.

KEYWORDS: Lightweight encryption and decryption, adaptive composite field architecture (ACFA), Linear Feedback Shift Register (LFSR)

I. INTRODUCTION

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key [1]. The result of the process is encrypted information (referred to as ciphertext). Encryption has long been used by militaries and governments to facilitate secret communication. Decryption is the reverse process of encryption.

In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. ―software for encryption‖ can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).In decryption, the ciphertext is converted into its original format using the key. It is the process of decoding data that has been encrypted into a secret format. Decryption requires a secret key or password. However, the well known cryptographic primitives used on traditional systems, are not necessarily well suited for such constrained devices [2]. They require too much memory space and processing power (to have a fast execution), which leads to a high energy consumption [3].

Cryptographic algorithms can potentially be extremely heavy, and require a lot of computational power, memory and energy [4]. With the growth of 5G communication apllications and the use of constrained devices, which that demand for security, the design of new cryptographic algorithms that require fewer resources was necessary. This motivated a new paradigm on the cryptography community, the Lightweight Cryptography [5]. As a consequence, a new field of research has been created in the Cryptographic World: Lightweight Cryptography, which

comprehends the research and development of new cryptographic primitives and algorithms that can be executed quite fast, show diminished memory footprints and consume very little energy, aiming at achieving a good trade-off between security, cost (in terms of memory footprint and energy consumption), and performance. In the last years, several articles were published addressing Lightweight Cryptography issues such as the proposal of new lightweight ciphers. Nevertheless, most of such works are focused on hardware implementations [6]. However, with the growing of IoT and its open source projects, the investigation of software oriented lightweight ciphers suitable for implementations on constrained devices has been gaining more and more importance in the recent years [7]. In order to ensure better encryption of images, we implement a two-level encryption process wherein the pixels in each row will be shuffled first and then the columns. This is obtained with help of the LFSR. The decryption process is also implanted in the same way. It must be noted that the LFSR implemented for the encryption & decryption process is a cryptographically secure one and hence yields a significantly secure system [8]. Therefore first propose the process of implementing a secure LFSR and then subsequently propose the process of encryption.

II. LITERATURE SURVEY

However, traditional cryptography focus on the solutions in providing high levels of security, ignoring the requirements of constrained devices. The authors in their paper [9] have specifically proposed a completely new Key Management Protocol which has the integration of implicit certificates with the standardized Elliptic Curve Diffie-Hellman exchange. The integration is used to perform authentication and key derivation. By experimental result and proof of concept implementation they assured a maximum airtime savings of more than 86%. They have also provided comparisons of conventional approaches, robust key negotiation, fast re-keying, and efficient protection against replay attacks. Xuan Xia Yao et al. in [10], "A lightweight attribute-based encryption scheme for the Internet of things" proposed a lightweight no-pairing ABE technique based on elliptic curve cryptography. The security of this technique is based on ECDDH posit rather than bilinear Diffie-Hellman posit, which can curtail the data processing overhead and communication overhead.ABE technique layout just for one authority applications, it is not pertinent to Ubiquitous IoT applications.

In [11] proposed method of Design and Implementation of Block Cipher in Hummingbird Algorithm over Spartan -2 FPGA. In this work, Block cipher encrypts 16-bit data blocks using 64-bit subkey. The main idea of Hummingbird solution is used with a new Boolean function is derived for the S-box and Inverse S-boxes. However, in this architecture 64-bit sub-key is used which is too short. In [12] the authors have proposed A Lightweight Hybrid Security Framework for WSN (LHSFW). In this framework the advantages of Intrusion Detection System (IDS) and Cryptography techniques are combined. Symmetric key cryptography is used in this framework. IDS detects internal and external attacks accurately, while cryptography techniques provide data confidentiality. The hybrid security framework provides privacy of communication and detects various attacks such as spoofed, altered or replayed routing information, man- in-the-middle and denial of service attacks.

In [13] the authors have proposed a Light-Weight One-way Cryptographic Hash Algorithm (LOCHA). Authenticity of information is protected by cryptographic hash functions. Keeping this in mind, a one way light weight hash algorithm with fixed and relatively small hash digest is

developed for WSN. Low overhead operations such as MOD, SWAP are used to make the algorithm lightweight. Basic cryptographic properties of a one way hash function such as preimage resistance, collision resistance, and second preimage resistance are fulfilled by the algorithm. A Lightweight Secure Data Aggregation Technique (LSDAT) for WSN is proposed in [14]. In clustered WSN all nodes do not transmit data individually to the base station, but nodes within cluster send data to the CH/aggregator and then aggregator transmits data to the BS/sink. Thus the lifetime of the individual sensor is increased. But the problem is the aggregator exposes data in clear text and the data is vulnerable to various attacks by intruders. A Lightweight Authentication Scheme (LAS) for WSN is proposed in [15]. This scheme composed of a key management and an authentication protocol. It uses symmetric key cryptography, unkeyed and keyed-hash functions. The main goal of the scheme is to provide confidentiality and authenticity. The protocol keeps minimum size and minimum number of interchanged messages. It is also capable to transport session keys. The main objective of the scheme is to provide energy efficiency. The scheme protects from resource consumption attack, and node capture attack and most danger denial of service attack. The memory requirement is small.

III. LIGHTWEIGHT ENCRYPTION AND DECRYPTION WITH LFSR USING ADVANCED ACFA

3.1 ACFA S-box and Inverse S-box design

The first transformation, SubBytes, is used for encryption and inverse SubBytes used for decryption. The SubBytes substitution is a nonlinear byte substitution that operates independently on each byte of the State using a substitution table (S-box). Take the multiplicative inverse in the finite field GF (2^8) and affine transform to do the SubBytes transformation. Inverse affine transform have to find for inverse SubBytes transformation then multiplicative inverse of that byte. Inverse SubBytes transformation is inverse of SubBytes transformation. It can find in the similar way only table which is used for mapping the byte is different. The SubBytes transformation is done through S-box.

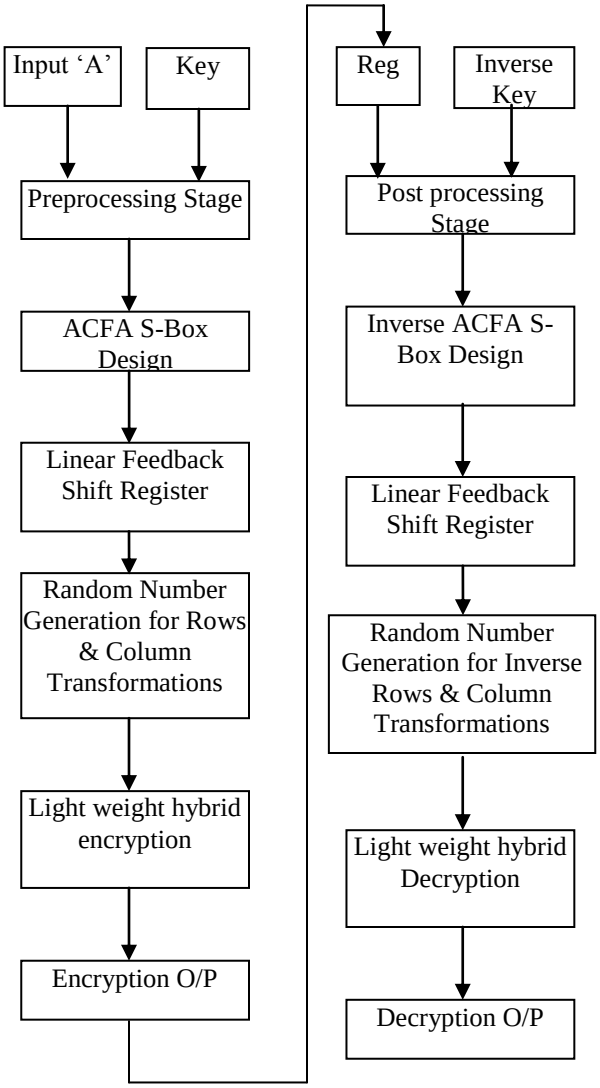

Fig. 1: Framework of Advanced ACFA Based Lightweight Encryption and Decryption Using LFSR

More feasible solution is to implement an S - box is by using Adaptive composite field arithmetic (ACFA) which uses only logic elements in the implementation. The S-BOX substitution starts by finding the multiplicative inverse of the data in GF (2^8), and then applying the affine transformation.

S-BOX substitution starts by finding the multiplicative inverse of the number in GF (2^8), and then applying the affine transformation. Implementing a circuit to find the multiplicative inverse in the finite field GF (2^8) is very complex and costly, therefore, the finite field GF (2^4) is suggested to use to find the multiplicative inverse of elements in the finite field GF (2^8). The substitute way is to design the S-Box circuit using combinational logic directly from its arithmetic operation. The S-Box transformation is essentially a combination of inversion and affine operations over the finite field GF(2^8). The inversion operation involved much more computational complexity than other arithmetic operations, and hence S-Box is the performance and area bottleneck. Although the inversion and affine mathematical complexity is hidden by

implementing high speed pipelined designs. Non-LUT based approaches, which employ combinational logic only, are attractive for their breakable delay of S-Box processing.

3.2 Linear Feedback Shift Register (LFSR)

Linear Feedback Shift Register (LFSR) is a shift register whose input bit is a linear function of its previous state. LFSR is used to generate Pseudo Random Numbers (PRN). The LFSR has two main parts which are a shift register and a feedback function. A shift register identifying function is shifting its contents into the adjacent positions within the register or, out of the register in the case of the position at the end. The position on the other end is left empty unless some new content is shifted into the register. The contents of a shift register are usually thought of as being binary, that is, ones and zeroes. For the shift register, there are three main parts. These are shift direction, output and input. Shift direction is the direction that the shift register will shift its contents. A shift register can shift its contents in either direction. The output refers to the bits that are shifted out of the register. The input refers to the bits that enter the register after the bit on the left end of the shift register and it is left empty. In the LFSR, the bits contained in selected positions in the shift register are combined in some sort of a function and the result is fed back into the register's input bit.

After the data is preprocessed and sate values determined, the initial seed is provided to the LFSR. Hence the random number sequence is generated. In an LFSR, certain bit positions are selected and some kind of function is performed to combine the bits in those positions and the result is fed into the input bit of the register. The positions of bits that are selected are called "taps". An initial value is required to generate a sequence of pseudorandom numbers. Changing the value of the initial seed will yield us a different sequence of such numbers. In order to obtain a cryptographically secure LFSR, we keep on changing the tap sequence of the LFSR. This is obtained with the help of a smaller LFSR which acts as a selector to a MUX. Eventually, quite a complex code can be generated. In the case, to implement a cryptographically secure LFSR, a PRNG and a MUX are needed. Each value of the PRNG is associated with a tap sequence. These sequences will be selected by the MUX. First, the initial seed is fed to the main LFSR. Then for each output sequence of the PRNG, a tap sequence is selected. The bits contained in these tap positions are XOR'ed and the output obtained is fed into the input bit of the LFSR. The LFSR then shifts one position to the right. This process continues till the desired sequence of output is obtained. Hence, we observe that the proposed method of implementing a cryptographically secure LFSR yields a more dynamic and complex code of pseudo-random numbers. The output sequence seems even less predictable in this scenario which will help a great deal in obtaining a better encryption and decryption of data.

3.3 Random Number Generation

Now the data is shuffled row-wise and a row-wise encrypted data is obtained. Again with the help of the random number generated, further obtain the column-wise encrypted data. First, the input bit values of each row of the data are shuffled and then the pixels of each column are shuffled. This shuffling is done with the help of the pseudo-random numbers generated by the LFSR. It is to be noted that the numbers in the sequence are restricted to the length of data during row shuffling and column shuffling.

3.4 Lightweight hybrid Encryption and Decryption

Encryption: The transformation is called ShiftRows performs in encryption, in which rows are cyclic shifting to the left. The number of shifting depends upon the row number of the state

matrix. First row no shifting, second row one byte, third row two bytes and fourth row three byte shifting left. The MixColumns transformation functions after the ShiftRows on the State column-bycolumn, considering each column as a four-term polynomial. The algorithm for MixColumns and Inverse MixColumns involves multiplication and addition in GF (2^8). The MixColumns multiplies the rows of the constant matrix by a column in the state

Decryption: The decryption process involves of the inverse steps, decryption round contains of: Inverse ACFA S-BOX used for Byte Substitution, Inverse Shift Rows and Inverse Mix Columns through LFS based pseudo random number generator. The round keys will be generated using a unit called the key generation unit. Decryption follows the same mechanism only in the reverse direction. The same initial seed is used to generate the sequence of pseudo-random numbers. Then the data is decrypted step by step by first decrypting it column-wise and then row-wise to eventually obtain the original input data bits. A good decryption scheme yields a decrypted data which is same as the original data. sIn the decryption, InvShiftRows transformation performs the right cyclic shifting operation inverse of ShiftRows; number of shifting depends on number of row number. Inverse MixColumns are the inverse process of MixColumns which is used in the decryption of cipher text. Finally, both the row-wise and the column-wise encrypted data are XORed to give the final encrypted data.

IV. RESULTS

The AFSA based S-box encryption and decryption algorithm using LFSR is implemented for AFSA128 bit using VHDL (Vey high speed Hardware Description Language). All findings are based on Xilinx ISE tools simulations. The architecture of ACFA based S-box 128-bit encryption and decryption is implemented as shown in Fig. 2 and 3.

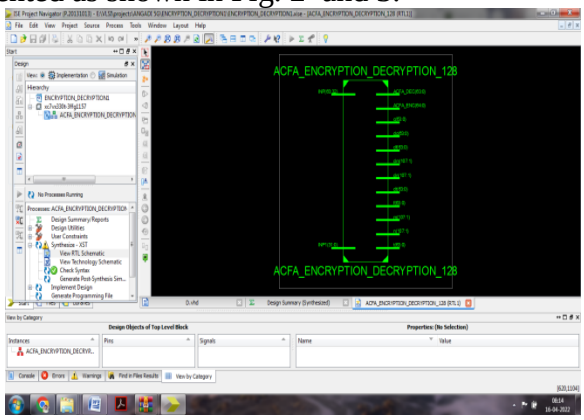

Fig. 2: RTL Schematic of 128-Bit Advanced ACFA based Encryption and Decryption

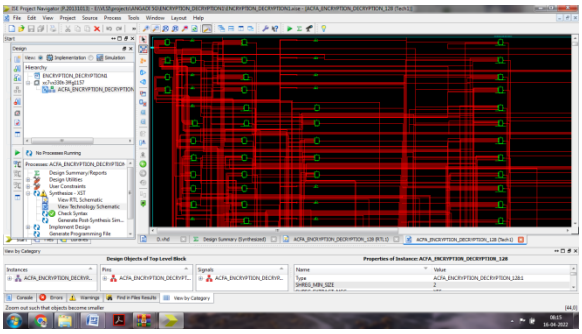

Fig. 3: Technology Schematic of 128-Bit Advanced ACFA based Encryption and Decryption

The Fig. 2 and Fig. 3 shows the RTL schematic and technology schematic of Advanced ACFA based S-box encryption and decryption with LFSR. RTL schematic is the combination of inputs and outputs. Register-transfer logic deliberation is utilized in equipment portrayal dialects (HDLs) i.e. VHDL to make elevated level portrayals of a circuit, from which lower-level portrayals and at last genuine wiring can be determined.

After running the VHDL code, checking for functionality, synthesizing and then implementing the code, we got the following results as shown in Fig. 4 which are summarized in the following.

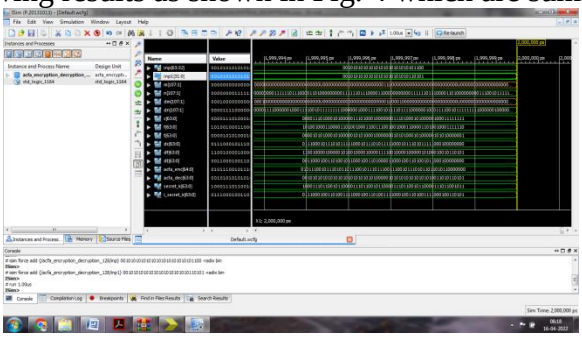

Fig. 4: Output Waveforms of 128-Bit Advanced ACFA based Encryption and Decryption

Technology schematic is the combination of Look up tables, Truth Tables, K-Map and equations. After the process of synthesis the following results regarding the LUTs, Total delay and memory utilization are shown in Fig. 5 and 6. It shows a representation of the design in terms of logic elements optimized to the target Xilinx device or example, in terms of LUTs, carry logic, I/O buffers, and other technology-specific components

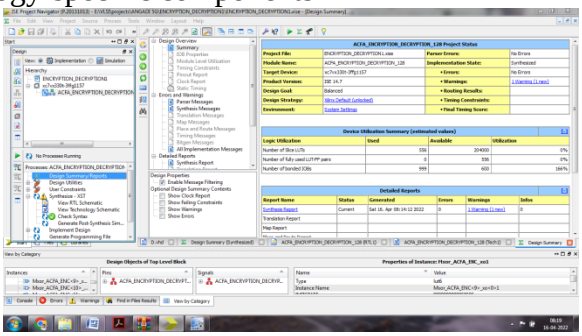

Fig. 5: Synthesis Report of 128-Bit Advanced ACFA based Encryption and Decryption

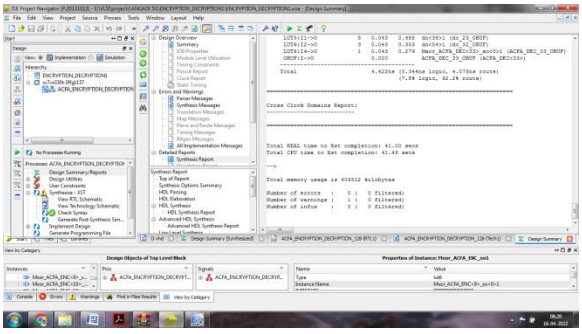

Fig. 6: Delay Report and Memory Utilization of 128-Bit Advanced ACFA based Encryption and Decryption

The following Graphs indicate the delay, memory and look Up Table (LUT) utilization for implementing the encryption. Here the Advanced ACFA based Encryption and Decryption is compared with the AES based encryption in terms of resources utilization like delay, memory and LUTs. It can be seen that Advanced ACFA based Encryption and Decryption has a better performance i.e. low delay as seen in Fig. 7, less memory as in Fig. 8 and LUTs utilization as in Fig. 9 compared to the AES encryption.

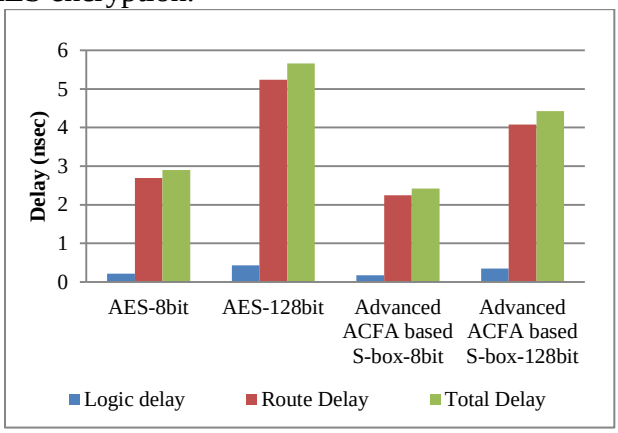

Fig. 7: Delay Comparison

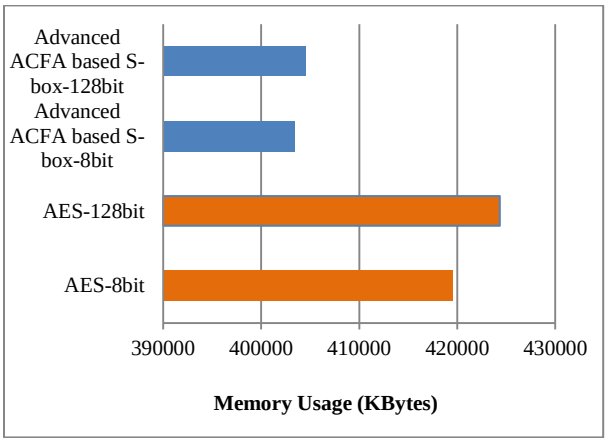

Fig. 8: Comparison of Memory Utilization

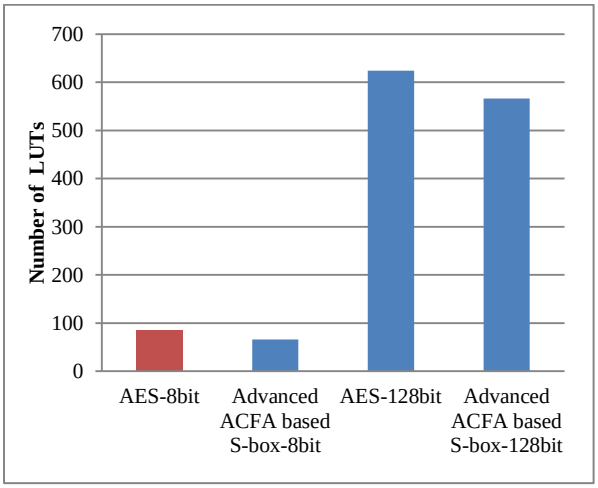

Fig. 9: Comparison of LUTs utilization

V. CONCLUSION

Keeping in mind the paramount importance of security, a highly efficient and robust encryption/ decryption technique was presented in this research. The primary objective of this work is to design a lightweight, secure ACFA based S-box that suits 5G communication applications. Modified light weight cryptography algorithm is proposed which uses the Linear Feedback Shift Register (LFSR) to provide high security against attacks. The combinational architecture in the finite field for the hardware implementation of the two states S-box is presented. The motive for the combinational two states ACFA S-box design is to pave the way for additional optimization mechanisms, namely sub pipelining in the S-box structure. The hardware structure for the realization of the S-box design has been carried out through extensive mathematical derivations and the finite field theory. The twolevel process of permutation and substitution of bit makes the final encrypted data unintelligible. The use of cryptographically secure LFSRs randomizes the process even more and subsequently increases the overall security of the system. Several tests were done in order to analyze the efficiency of the system and it was found that the proposed method is immune to a great extent.

VI. REFERENCES

[1] J. Breier, D. Jap, X. Hou and S. Bhasin, "On side channel vulnerabilities of bit permutations in cryptographic algorithms", *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1072-1085, 2020

[2] A Chakraborti, N. Datta, A. Jha, C. Mancillas-Lpez, M. Nandi and Y. Sasaki, "ESTATE: A lightweight and low energy authenticated encryption mode", *IACR Trans. Symmetric Cryptol. Greece*, vol. 2020, no. S1, pp. 350-389, June 2020

[3] B. Subhadeep, I. Takanori, M. Willi, T. Yosuke and B. Zhang, Triad v1-A Lightweight AEAD and Hash Function Based on Stream Cipher, 2019.

[4] S. Patranabis et al., "Lightweight design-for-security strategies for combined countermeasures against side-channel and fault analysis in IoT applications", *J. Hardware Syst. Secur.*, vol. 3, no. 2, pp. 103-131, 2019.

[5] y of lightweight and secure authenticated encryption ciphers", *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2018, no. 2, pp. 218-241, May 2018.

[6] C. A. Lara-Nino, A. Diaz-Perez and M. Morales-Sandoval, "Lightweight hardware architectures for the present cipher in fpga", *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 9, pp. 2544-2555, Sept 2017.

[7] F. Guo, Y. Mu, W. Susilo, H. Hsing, D. S. Wong and V. Varadharajan, "Optimized identity-based encryption from bilinear pairing for lightweight devices", *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 211-220, 2017.

[8] Z. Liu, J. Grosschadl, Z. Hu, K. Jarvinen, H. Wang and I. Verbauwhede, "Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the Internet of Things", *IEEE Trans. Comput.*, vol. 66, no. 5, pp. 773-785, 2017.

[9] G. Hatzivasilis, G. Floros, I. Papaefstathiou and C. Manifavas, "Lightweight authenticated encryption for embedded on-chip systems", *Inf. Secur. J. A Glob. Perspect.*, vol. 25, pp. 151-161, August 2016.

[10] S. Sciancalepore, G. Piro, G. Boggia, and G. Bianchi, "Public key authentication and key agreement in IoT devices with minimal airtime consumption," IEEE Embed. Syst. Lett., vol. 9, no. 1, pp. 1–4, 2016.

[11]. Shumit Saha, Md. Rashedul Islam, Habibur Rahman, Mehadi Hassan and A.B.M. Aowlad Hossain, "Design and Implementation of Block Cipher in Hummingbird Algorithm over FPGA", 5th ICCCNT, Hefei, China, IEEE – 33044, 2014, pp. 1-5.
[12] Sedjelmaci, Hichem, and Sidi Mohammed Senouci. "A lightweight hybrid security framework for wireless sensor networks." In Communications (ICC), 2014 IEEE International Conference on" pp. 3636-3641,IEEE, 2014.
[13] Chowdhury, Amrita Roy, Tanusree Chatterjee, and SipraDasBit. "LOCHA: A light- weight one-way cryptographic hash algorithm for wireless sensor network." Procedia Computer Science 32, pp. 497-504, 2014
[14] MdMizanur Rahman, Sk, Mohammad Anwar Hossain, Maqsood Mahmud, Muhammad Imran Chaudry, Ahmad Almogren, Mohammed Alnuem, and AtifAlamri. "A lightweight Secure Data Aggregation Technique for Wireless Sensor Network." In Multimedia (ISM), 2014 IEEE International Symposium on, pp. 387-392, IEEE, 2014.
[15] Delgado-Mohatar, Oscar, AmparoFuster-Sabater, and Jose M. Sierra. "A light-weight authentication scheme for wireless sensor networks." Ad Hoc Networks 9, pp.727-735, no. 5 , 2011