An Overview of Lightweight Cipher

Rupam Dixit, Lalbaboo Kumar, Sandhya Verma, Kapil Gupta and Sarika Jain

National Institute of Technology, Kurukshetra, Haryana, India.

Abstract

Lightweight cryptography is stylish because of its necessity for uprightness, privacy, and verification. With the intense advances in little gadgets, for example, Sensors, RFID labels, sensor hubs, clinical gadgets are being sent at a quick pace. These gadgets are being utilized in different applications which leads to the prerequisite of giving security. With the IoT frameworks that utilize information, in reality, the information assortment from gadgets can likewise be an objective of cyber-attacks. It is a direct result of this that countermeasures dependent on encryption are right now acquiring significance. Lightweight cryptography is an encryption technique that includes a little impression and additionally low computational complexity. It is pointed toward growing the uses of cryptography to compelled gadgets and its connected global normalization and rules aggregation are as of now underway. Symmetric-key calculations are as yet used to give secrecy in the previously mentioned applications. In this paper, the need for a lightweight cipher has been talked about and what all natives need to keep up a harmony between security, size, cost, and different elements are delineated. In this paper, investigations of security and shortcoming are examined.

Keywords 1

Lightweight Cipher, Security, IoT frameworks, Cyber-attacks.

1. Introduction

Cryptography is the approach to ensure and protect the data with secrecy, honesty, and validation. Cryptography has been related to superior processing. Nowadays the main aim and focus The IoT has made new qualities by associating different gadgets to the organization, yet has additionally prompted security danger turning out to be significant issues as found in the new reports of illicit observation camera control and auto hacking and so on. Encryption is a successful countermeasure, and the IoT is currently needed to apply encryption to sensor gadgets in conditions with different limitations that have not recently been dependent upon encryption. Lightweight cryptography is an innovation investigated and created to react to this issue. In this paper, the creator will depict the security dangers of IoT and talk about the countermeasures that depend on encryption. This paper compresses the most recent design prerequisites in lightweight cryptography. It additionally examines the most recent planned lightweight cryptography.

The paper shows different rules that are needed for the assessment of lightweight cryptography. It focuses on recently designed ciphers. We want to describe lightweight ciphers and comparisons of various lightweight ciphers. Because Embedded systems nowadays have issues of security. so, in this paper, we use various ciphers to eliminate those security issues.

ACI'21: Workshop on Advances in Computational Intelligence at ISIC 2021, February 25-27, 2021, Delhi, India
EMAIL: rupah_51910041@nitkkr.ac.in (R. Dixit);
lalbaboo_51910014@nitkkr.ac.in (L. Kumar);
sandhya_51910038@nitkkr.ac.in (S. Verma);
kapil@nitkkr.ac.in (K. Gupta);
jasarika@nitkkr.ac.in (S. Jain)

2. Related Work

Because of the significant role of lightweight cryptanalysis, Algorithms perform RFID tags (protected radio waves detection), digital wallets, a network of smart appliances, etc., in several durations of time implementations, which include security applications, the author reviews the latest evolutions of asymmetric and symmetric ciphers trying to target inbuilt hardware and software.

2.1. Literature Survey

The researcher had developed the lightweight block cipher i.e, PRESENT in the year 2007. its algorithms and designs were also introduced. The main lightweight research was conducted in that year. [1].

The Elliptic Curve crypto algorithms used by the researcher in 2014 resulted in the introduction of a more efficient symmetric key cryptographic scheme, the introduction of an encryption and decryption algorithm to meet efficiency including security needs, resulting in other scholars being able to distinguish the problems over known or lightweight secure crypto algorithms [2].

A safe and lightweight cryptographic technique using a chaotic map and genetic algorithms was proposed by the author in 2014. This device is secure, lightweight, and ideal for use in WSN networks of wireless sensors [3].

The author introduced the hybrid light-weight encryption device design in 2016 along with High efficiency, low voltage usage, and robustness. Each algorithm performs a 128-bits plain text operation with a 128-bits secret key and the same result code [4].

In 2017, the Internet of Things (IoT) lightweight cryptographic algorithm was renamed SIT's stable Internet of Things. The proposed techniques are applied for the Internet of Things to solve the challenges of protection and resource utilization. The proposed technique architecture has implemented a basic framework appropriate for the implementation of things on the internet. Substitution Permutation network is used by many famous block ciphers. Shannon's uncertainty plus diffusion properties are fulfilled by numerous alternate rounds of substitution and transposition that ensure the cipher text is altered in not a random manner. The Feistel architecture is used by another famous cipher, including SF, Blowfish, Camellia, and data encryption standards. Therefore, the use of features of both methods to enhance a lightweight algorithm which provides significant protection in the world of IoT during retaining the Complexity of computation at a moderate level [5].

3. Methodology

We aim “To check the robustness of different encryption of ciphers against ML or DL of attack”, which is currently being used in most real-world applications. The use of machine learning methods to derive decryption keys from cipher text blocks in cryptanalysis. Connecting machine learning with current cryptanalysis techniques in the search domain, to maximize their effectiveness in solving problems.

3.1. Cipher Scheme

A cipher is an encryption or decryption algorithm in cryptography, a sequence of well-defined steps that can be taken as a method. Block cipher and stream cipher are two types of the cipher. Lightweight block ciphers accept a set of encrypted text and produce encrypted text, normally like the same size, of cipher text bits. In a specified scheme, the input size is stabled. Cipher robustness is based on the length of the key. Digital Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), and so on are various schemes of the block cipher. One byte is encoded in the stream cipher at a time. In a stream cipher, a keystream and plaintext generate cipher text for encryption. The Plaintext will perform a keystream bits-by-bits XOR operation and generate the cipher text. A keystream and cipher text generate plaintext for decryption. The cipher text will perform a keystream bits-by-bits XOR operation and results from the original Plaintext. There are also some gaps in encryption techniques i.e., For a long period, most applications follow the encoding

technique, which allows the analyst can concentrate on this before he can identify the key.

Known secret altered every moment. Key alter leading to the intersection of key supervision and sample variables is a complex process. Mostly when the number of members increases then, for a long time, some departments continue to use the key, it will cause the scholars to research that. As time passes, all cryptographic systems grow to be vulnerable due to attacks. Because of these attacks, all cryptographic systems evolve to be insecure day by day time goes. And in later times, the group encryption techniques that have been evaluated as strong in a certain time would undoubtedly remain unreliable. In data encryption, for instance, the traditional approaches were also accurate [6].

3.1.1 Lightweight ciphers

Lightweight ciphers are the type of cryptography that includes cryptographic algorithms planned for use in low-resource, pervasive devices. Lightweight cryptography does not find difficult requirements for the description of an encryption system as lightweight, lightweight technique's presence is a quite lack of supply for primary tools for specific systems [7]. There are various forms of cryptographic solutions available to Protect our important records, but not all of them, sadly, are Suitable for resource-restricted environments such as IoT Appliances. To provide a region-efficient and power-efficient solution, lightweight cryptographic solutions are being extensively studied. Figure 1 shows the types and subtypes of lightweight cryptography.

Commercial, as well as industrial IoT-specific attacks, are vulnerable to devices. If we do, if we will continue to use the current flow of IoT system design, facing a security risk soon. It is possible to split the existing cryptographic techniques into two categories: Asymmetric key cryptography and Symmetric key cryptography [8].

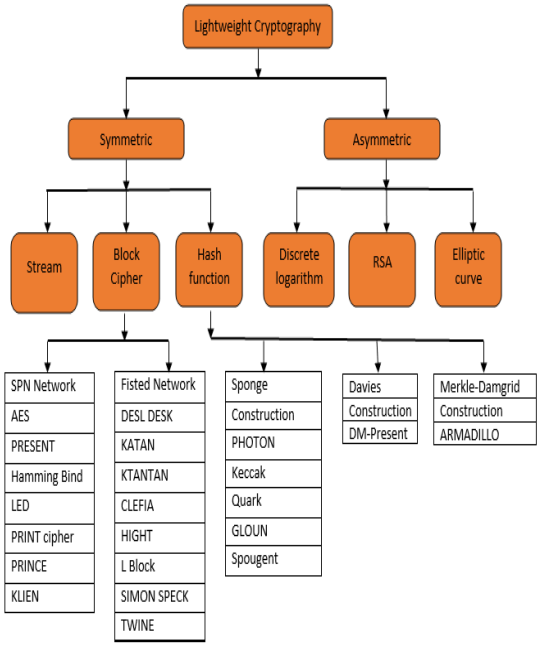

Figure1: Diagram for Lightweight Cryptography

A lightweight block cipher presented in [9, 10], works on two layers of a network including the substitution layer and permutation layer. It receives a 64-bits' size of input plaintext and works with 80,128-bits' keys. Its code run till 31 cycles of encryption and decryption because there is a limit of 32 round so the code will run 1 less than the round limit.64-bits' key produced in each cycle from the record of key execute XOR activity with unencrypted text then record of a key is refreshed. IoT technology is witnessing an ever-increasing need for tiny electronic devices with cryptographic necessities. Crypto researchers have been featuring lightweight ciphers to offer the right performance without a compromise with the security of facts. Advanced Encryption Standard (AES) as a block cipher has been studied and analyzed by the crypto network considering its standardization by using NIST in 1997. But, AES isn't always appropriate for resource-restricted devices including sensor networks and RFID tags. This encouraged researchers to layout light-weight ciphers. In our paintings, we will be analyzing the safety and strength of lightweight ciphers using system studying mainly deep learning. Lightweight cryptography answers security usage at the equipment level. These cryptographic strategies are exceptionally settled for installed frameworks. The utilization of IoT gadgets expanded everywhere in the world as a result of the lightweight strategy

utilized in IoT gadgets which likewise gives a start to finish correspondence security under calculation, memory cut-off points, and low force utilization. So lightweight equipment method with PRESENT code exceptionally relevant for extraordinary asset compelled applications and when AES calculation is unacceptable application. They are utilized with challenge-reaction verification convention, encryption, and decoding of correspondence in counter mode. These security issues can be handled by utilizing the PRESENT Cipher model which is a normalized one. The planned PRESENT code model is actualized by utilizing 80-bits and the 128-bits key, for 64-bits information input. Some deep learning technique is also described in the segments of the report.

3.1.1.1 Asymmetric Cipher

It is known as public-key encryption. Cryptography, since there is a public key pair in this technique and private key are required(figure2). The aim of lightweight ciphers has gradually changed to asymmetric cryptographic functions, but the results, such as symmetric cipher, are not yet accurate and beneficial. In terms of operation, an asymmetric cipher is complicated and does not waste time. Attack methods often make the scale of the operands and the constant growth of such algorithms dangerous. 3 developed families of factual importance among public key algorithms: RSA, ECC, and discrete logarithms seen in the preceding figure1.

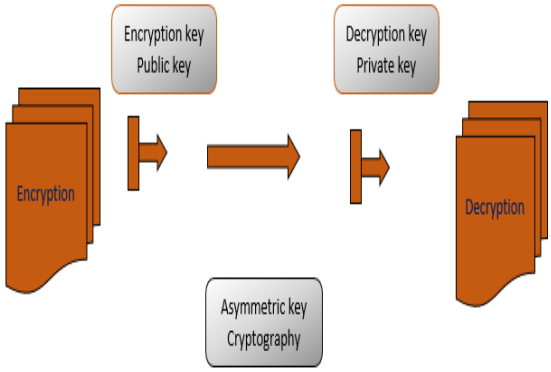

Figure2: Asymmetric key encryption

3.1.1.2 Symmetric Cipher

The symmetric cipher is often referred to as just a hidden key or Encryption with a common key (Figure3). The sender and receiver having a similar key for encoding and decoding by hidden communication. Due to its rapid practices, which are mainly XOR and variables, Symmetric cryptography is more fitting for IoT applications. It can have categorized as a hash function, stream cipher, block cipher. Every of these has several recognized techniques use for data protection and information protection as seen in figure1. Over the past twenty years, several studies on symmetric algorithms have been reported. Since the software framework is used by most major symmetric cipher applications, it is not surprising that with better software protection in the brain, all algorithms, such as The AES were designed.

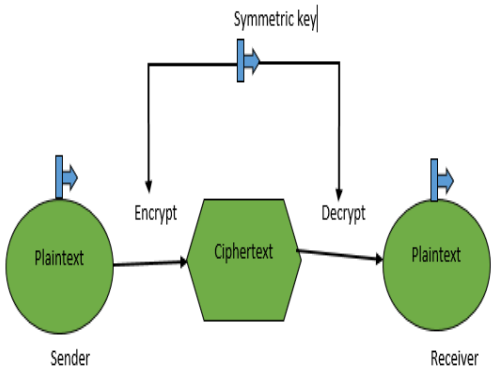

Figure3: Symmetric key encryption

Table1: Comparison of different block cipher

Cipher	Based on	Data block Size(bits)	Encryption key size(bits)	No. Of cycles	Cycles per block to Encrypt	Cycle per block to Decrypt
AES	Substitution Permutation network	128	128 192 256	10 12 14	6,637	7,429
DES	Feistel cipher structure	64	56	16	8,634	8,154
PRESENT	Substitution Permutation network	64	80 128	31	10,723	11,239
HIGHT	Generalize Feistel structure	64	128	32	2,964	2964
SEA	Feistel cipher structure	96	96	93	9,654	9,654
TEA	Feistel cipher structure	64	128	64	6,271	6,299

3.1.2 Data Encryption Standard (DES)

DES means Data Encryption standard. DES is a symmetric-key method of data encryption (figure-4). Asymmetric key means it uses a single key to encode and decode the input text, that single key should be recognized by the sender as well as the receiver. DES is a block cipher, it has a 64-bits block size to encrypt data, which means it takes an input of 64-bits plaintext and it gives an output of 64-bits ciphertext. DES using a single technique to encode and decode input text, along with some basic differences. The key length of 56-bits. We have mentioned that DES uses a 56-bits key.

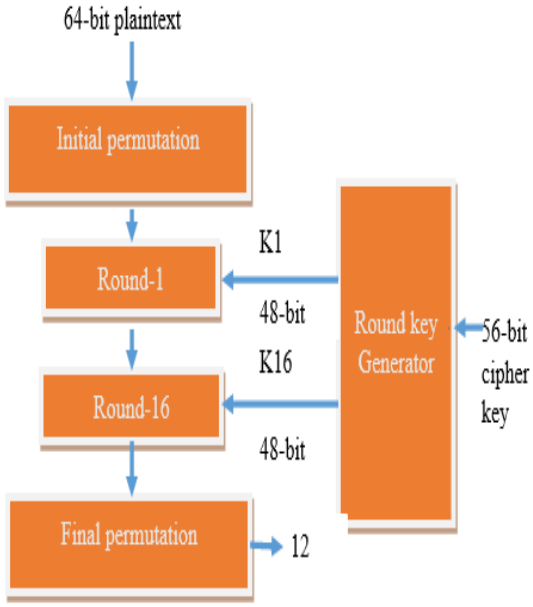

Figure4: General structure of DES

Initially, the key is taken 64-bits. but, every 8-bits of the key is rejected to generate a 56-bits key before the DES process even begins. That

is, there are discarded bit positions 8, 16, 24, 32, 40, 48, 56, and 64.

Therefore, the 56-bits key is from by rejecting every 8th bits of the key from the initial 64-bits key. It has 16 rounds to encrypt and decrypt the text.

3.1.3 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES). It can be detected about 6 times quicker than DES. As its main size was too small, a substitute for DES was needed. It was considered unsafe against thorough key search attacks with growing computing capacity.

The AES characteristics are as follows −

- Symmetric key cipher of symmetric block.
- 128-bits data, 128/192/256-bits keys[table].
- More efficient and quicker than DES.
- Provide complete specification and layout information.

It is based on 'network substitution-permutation'. All the calculations are performed by AES in bytes instead of bits. Therefore, 128-bits from a plaintext are treated as almost 16 bytes by AES. That 16 bytes (figure-5) are structured as a matrix for computation in four columns and four rows.

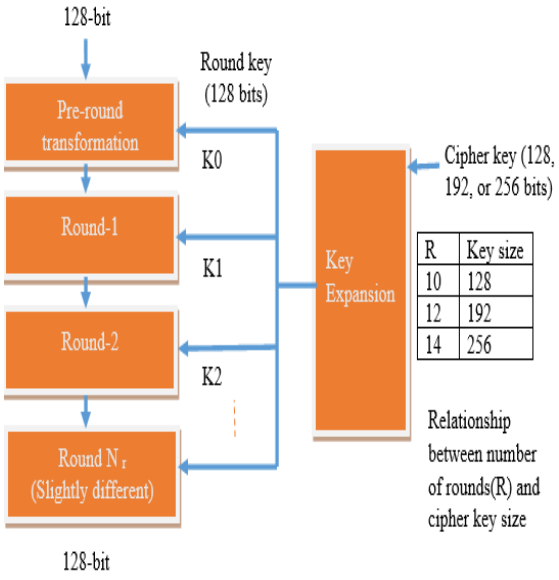

Figure5: Schematic of AES

AES encryption key cycle varies accordingly input size key, AES uses 10 rounds, 12 rounds for 192-bits keys, and 14 rounds for 256-bits keys. A separate 128-bits round key is used in each of these cycles, which is computed from the initial AES key [Table 1].

3.1.4 PRESENT Cipher

PRESENT is an underweighted symmetric block cipher. The purpose of PRESENT Cipher is broadly used in underweight cipher.

The Ultra-Lightweight Symmetric Block Cipher may be PRESENT. It was supervised in 2012 by The International. The Global Electro Specialized Commission (ISO/IEC) is mainly suitable for Lightweight Cryptography and is also developed for compulsory climate execution [1], [3], [4].

PRESENT Cipher's fundamental objective is its wide use in lightweight environments, such as RFID tags, sensor organizations, and IoT. Due to its lightweight nature, it has gained popularity by providing a significant level of protection in a limited climate with less area, less strength, fewer assets, and less memory. Present Cipher hardware execution is finished using FPGA because it is cheaper, simpler to use It uses less force and re-configurability.

- **PRESENT Algorithm**

PRESENT can be a block cipher based on a 31 round Substitution Permutation Network with a 64-bits input size and 80-bits or 128 key size cycle. The 64-bits keys are created by the Key Scheduling Algorithm handling the provided 80-bits input key within each round.

By using disarray and dispersion over information using three key tasks in each round, the input plain text is changed to accumulate the encoded Cipher text. They are RoundKey, Substitution Layer, Permutation Layer.

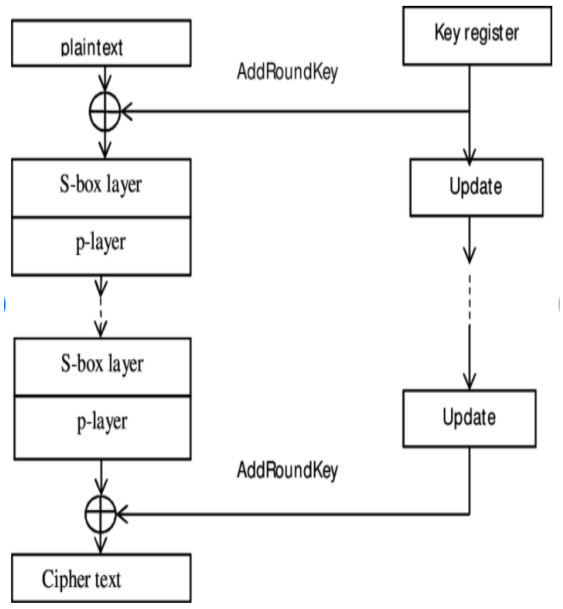

Figure6: Schematic drawing of PRESENT cipher

- **RoundKey**

The bitwise X-OR operation between the plaintext block and thus the round key operates.

- **Substitution Layer**:

The S-box replaces another block of bits for a contact block of bits (the contribution of the S-box) (the yield of the S-box). To ensure invariability, this substitution needs to be coordinated (henceforth unscrambling). Specifically, the length of the yield needs to be like the length of the knowledge (the picture on the privilege has S-boxes with 4 information and 4 yield bits), which isn't quite an equivalent as S-confines general that would likewise alter the length, as in DES (Data Encryption Standard Typically, an S-box is not just a stage for the bits. Or maybe an honest S-box would have the property that re-modelling one data spot will alter the portion of the yield bits (or a torrential slide impact). It will also have the property that every yield spot depends on each bits of knowledge.)

- **Permutation Layer**

A Permutation box can be an all-bits permutation: it takes the yields of all 1-round S-boxes, permits the bits, and feeds them into subsequent round S-boxes. An honest P-box has the property that any S-yield box's bits are suited to any number of S-box contributions as may be required under the circumstances.

These embedded devices record, store, and transmit massive quantities of data across the network. A large field of concern for IoT networks is the protection of data transmission. In recent years, various encryption techniques have been introduced regarding the safety of data transmitted through the IoT network. From the above comparison table 1, we conclude that.

AES is a symmetric block cipher that is implemented in software. In numerous applications, the AES cipher is used to provide secrecy and works on a substitution permutation network. AES takes data block size of 128-bits and key sizes of 128, 192, or 256-bits.128-bits' key takes 10 cycles,192-bits' key takes 12 cycles and 256-bits takes 14 cycles for their operation. The power of AES is strengthened by a large key because the more core recovery is an effective assault on AES. AES with a 256-bits' key is much harder to decipher than a 128-bits key for brute-force attack, it takes millions of years to guess the key. So AES with 256-bits' key size is more secure. Researchers have found AES is more secure as compared to another cipher.

DES is among the first LWC ciphers to be researched. It utilizes a 56-bits key via 16 rounds of 64-bits blocks. The downside of DES would be the small key size (i.e. 56-bits) comparison with AES, resulting in a low level of security. AES's logical design is closed down. The process of selection for this is confidential. 16 cycles of similar operations are involved in DES. The technique focuses on a Feistel network. It utilizes 56-bits' key size with 64-bits input data size.

PRESENT cipher works on a substitution permutation network like AES. Just one distinction is the sequence and its utilization of inverse decryption functions. It receives a 64-its' size of input plaintext and works with 80,128-bits' keys. Its code runs till 31 cycles of encryption and decryption. One of the drawbacks of this algorithm is the large capacity requirement PRESENT cipher with 80-bits' key size requires 284 calculations to maintain security, even though no specific linear cryptanalysis has been implemented on PRESENT cipher with 128-bits' key size, it can be presumed that a higher-order would be PRESENT with 128-bits' key size [8].

HIGHT takes 64-bits block size of the input and 128-bits' key size. It works on generalized Fiestle Structure and performs 32 cycles in each iteration. It is an ultra-lightweight cipher that consumes less energy and is implemented at a low cost. HIGHT's popular feature is that it

comprises basic functions like XOR, mod 28 addition, and bit-wise rotation left. Thus, instead of software applications, it is hardware components. The 8-bits integrated CPU in the sensor network communication for sensor nodes is based. Even in terms of 8-bits based software configuration, HIGHT is much quicker than AES. After processing the whitening keys as well as all sub keys, HIGHT's key schedule algorithm is programmed to preserve the initial value of the master key.

SEA takes 96-bits' data block size with 96-bits' key size of encryption and runs till 93 cycles. The majority of recent block ciphers such as AES are built to identify just a reasonable difference among price, protection, and results. But on the other hand, SEA was developed as a low-cost encoding technique that runs on very limited resources for processing. An identical structure is followed by SEA and PRESENT cipher; however, SEA was executed in system software whereas PRESENT cipher was executed in machinery. SEA has already been applied in machinery however due to the bit-wise permutation used by PRESENT, it's tough to apply PRESENT in system software. In technology, AES is the fastest, which has the largest computation time and power consumption. Each cipher's speed will depend on the number of gate equivalents utilized within the application of machinery. SEA's primary benefit is that it is flexible and can therefore be customized to execute on several various systems.

TEA is easily implemented in hardware as well as software and consumes low memory. So it is more desirable between all ciphers. It uses a single key in all encryption cycles i.e, the main issue with this cipher resulting in lower protection. Also, it takes more time to encrypt and decrypt the text resulting in poorer performance in networks of IoT with portable systems. It works on the Fiesta network structure. It takes 64-bits data block size with 128-bits key size of encryption and runs till 64 cycles.

4. Conclusion

Our lives are permeated by ubiquitous computing, taking us closer to the sight of IoT systems. This major shift within the application and the type of computer systems generate novel difficulties regarding the protection of its materials, storing data distributing data too. In contrast with other frameworks which do not have lightweight cryptographic functions, the conceptual idea of utilizing lightweight cryptographic techniques has been a part of current cryptographic techniques and a new product in the research of advancing into current protection. Providing such lightweight cryptographic techniques is an enhancement to standard protection only when we receive the similar feature of last along with fast speeds, less period, good efficiency, and less price.

5. References

[1] T. Eisenbarth C., Paar, A. Poschmann, S Kumar., L. Uhsadel, "A survey of lightweight cryptography – implementations," IEEE Design and Test of Computers. 2007.

[2] S. Mohsen, Ghoreishi, S. Abd Razak, I. Fauzi Isnin, H. Chizari, "Security Evaluation Over Lightweight Cryptographic Protocols," International Symposium on Biometrics and Security Technologies (ISBAST). 2014.,

[3] K. Biswas," Light-weight Security Protocol for Wireless Sensor Networks," School of ICT, Griffith University. 2014.

[4] M.Sangeetha1,M.Jagadeeswari," Design and Implementation of New Lightweight Encryption Technique," International Journal of Innovative Research in Science, Engineering and Technolog (An ISO 3297: 2007 Certified Organization) Vol. 5, Issue 5, May 2016.

[5] M. Usman, I. Ahmed , M. Imran , S. Khan, U. Ali , "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1. 2017.

[6] M. Favas, C. Fysarakis, K. Papanikolaou," a survey of EU research efforts. Security and Communication Networks," A. Papaefstathiou Embedded systems security. 2015.

[7] J. Wurm, K. Hoang, O. Arias, A. R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," Proc. Asia South Pacific Des. Autom. Conf. ASP-DAC, IEEE, 2016.

[8] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann1, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An UltraLightweight Block Cipher,". 2007.
[9] C.G. Thorat, V.S. Inamdar," Implementation of new hybrid lightweight cryptosystem" Applied Computing and Informatics. 2018, doi.org/10.1016/j.aci.2018.
[10] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic Curve Lightweight Cryptography: a Survey," IEEE Access, vol. PP, no. c, pp. 1–1. 2018.