NEW Ultra LIGHT-WEIGHT CRYPTOGRAPHY ENCRYPTION AND DECRYPTIONS FOR THE INTERNET OF THINGS

[1]Deepsikha Sharma

Assistant professor, Deepshikasharma06@gmail.com

[2] Jain Singh.

Assistant professor, jainsingh@gmail.com

[3] Niharika Namdev

Assistant professor, niharikanamdev5@gmail.com

[4] Suman Kumar Jha,

Assistant professor,Sumanjha1971@gmail.com

[1,2,3,4,]Department of Computer Science & Engineering IIMT College of Engineering G reater Noida, India

Abstract: Lightweight cryptographic model was an algorithm tailored for implementation in limited environments devices. However, the aim of applied lightweight cryptography is to use it in equipment with limited requirements (memory, power, size). The goal of NVLC has been a lightweight cipher that applied with a high level of security in the low-resource device. The proposed is described the new block cipher called NVLC, uses round function can be repeated as many times as necessary for more security. The algorithm worked with block symmetric cipher 64-bit and 80-bit/128-bit of the key used SPN structure.

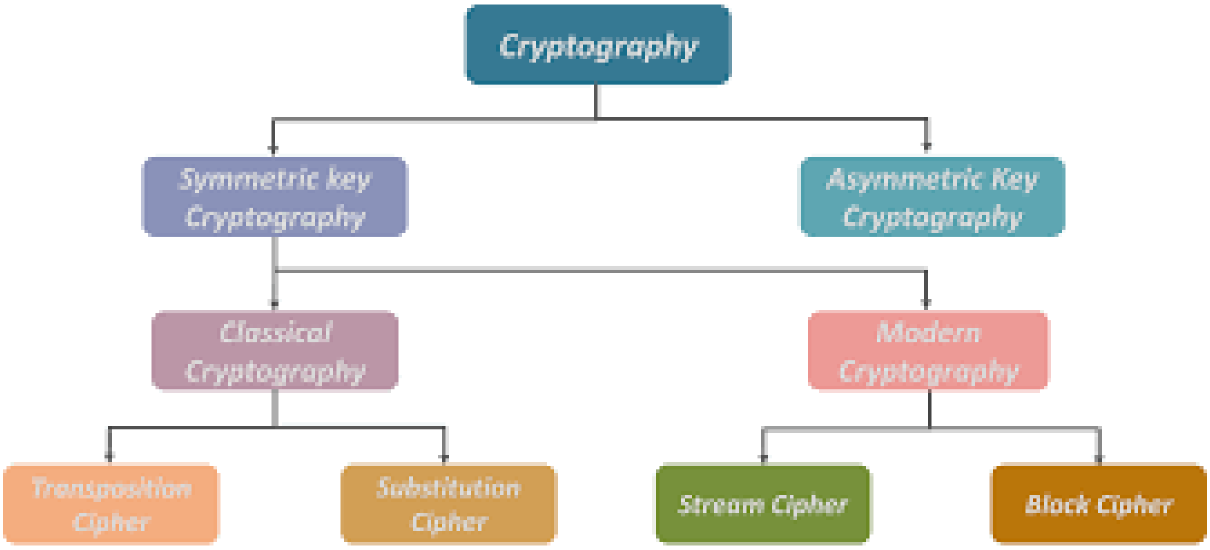
Keywords – Symmetric Key cryptography, Asymmetric Key cryptography, Light Weight cryptography, Light Weight cryptography, Ultra Light Weight cryptography.

DOI:10.48047/ecb/2023.12.si12.019

1. INTRODUCTION

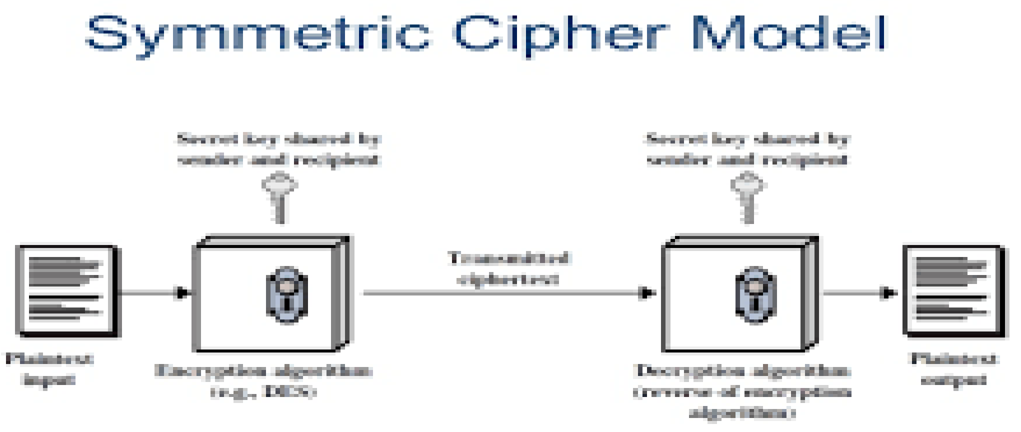
Light weight cryptography is the requirement of cryptography .becouse normal cryptography algorithms can be too slow ,too big or too energy consuming .this problem eliminate by light weight cryptography[1] .Light weight cryptography reduce key size ,cycle rate ,throughput rate, power consumption and area which are measure in gate equivalence(GE). It is generally defined for resource constrained device. It is a key tool for building robust security solution[2] for pervasive device. Light weight cryptography does not apply difficult algorithm . It is use simle algorithm .Light weight algorithm are very low requirement to main resource for target devices .genrally two types of light weight cryptography symmetric and asymmetric cipher.

Figure. 1

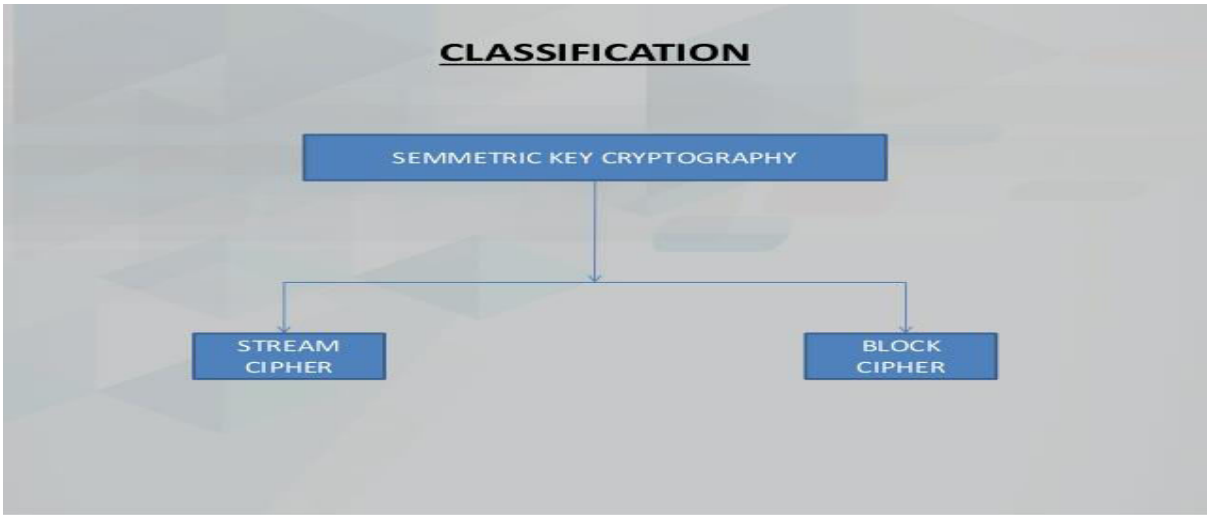


II. Symmetric ciphers

Symmetric ciphers can be classified as (streamand block cipher). Each one of them has a lot of known algorithms that are used in a security of data and information, A lot of works on symmetric ciphers are published during the past twenty years. As a result of most main applications of symmetric ciphers use the software system, it's no surprise that around all algorithms for example, the (AES) have been developed with good software performance in mind. The paradigm shift that we tend to foresee can probably cause an increasing demand for light-weight ciphers that perform well in H/W Therefore, we tend to focus here in recently published works on ciphers that were developed for minimal H/W requirements namely, Present Lightweight cryptography standards developed in (ISO/IEC JTC SC27) cover the necessary symmetric key based primitives Block cipher, stream cipher, hash function, and MAC[3]. The standards cover a relatively large range w.r.t. the hash value, key size, block size, etc. Public key based algorithms are mainly for authentication purpose designed for specific applications (radio frequency identification (RFID)), contactless transaction, and sensor networks). As the standard symmetric algorithms like advanced encryption standard (AES) cannot fit in these low cost small devices[3]. The cryptographic community has recently responded by designing a number of lightweight symmetric primitives appropriate for constrained environments Encrypted and decrypted using same key. it transform plaintext into cipher text using a secret
key .


Symmetric Cipher Model
Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Types of symmetric cipher



CLASSIFICATION

SEMMETRIC KEY CRYPTOGRAPHY

STREAM CIPHER

BLOCK CIPHER

(a) Stream cipher

A stream cipher is a type of symmetric encryption in which data is encrypted one bit or some time one byte at a time[18]. example of stream ciphers include SEAL, TWOPRIME
TYPES OF STREAM CIPHER.
(1).Synchronous stream
(2). Asynchronous stream
In synchronous stream ciphers where the key stream depends only on the key
A synchronous stream cipher where the key steam also depend only ciphertext.

(b) Block cipher

A block cipher is a method of encrypting text to produce ciphertext in which a cryptographic key and algorithm are applied to a block of data at once as a group rather than to one bit at a time .example 64 contiguois bit.

Types of block cipher.

SPN –Network

AES

PRESENT

HAMMING BIRD

LED

PRINCE

PRINT CIPHER

KLEIN

FISTEL NETWORK

DESL/DESX

KATAN

KTANTAN

CLEFIA

HIGHT

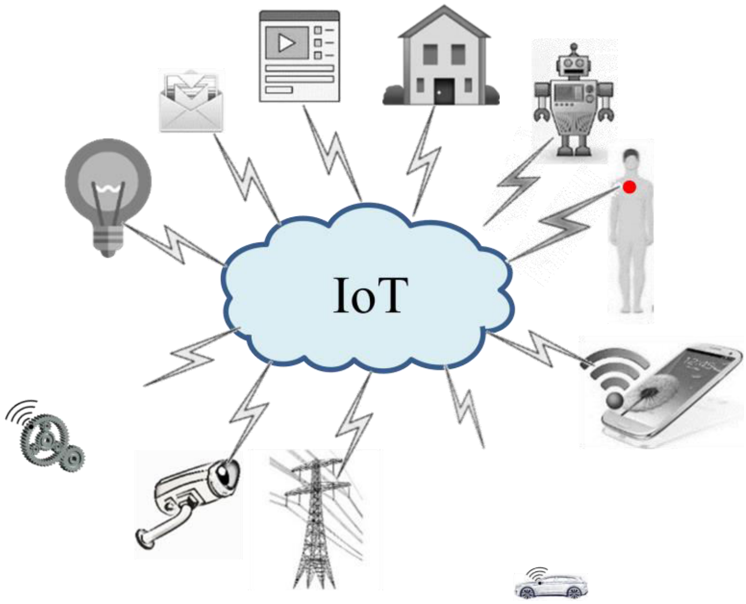
LBLOCK

SIMON/SPECK

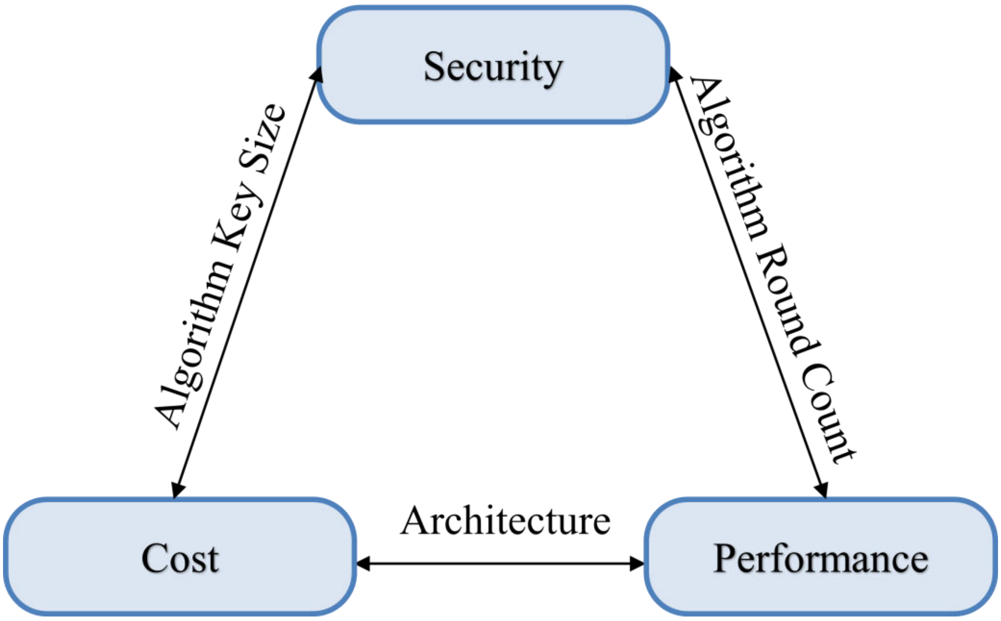
TWINE

II. ASYMMETRIC CIPHER

Among public key algorithms, established families of factual relevance: Rivest Shamir Adleman Elliptic curves, and discrete logarithms. Elliptic curves are tack into account the most attractive family for embedded environments attributable to its relatively lower computational requirements and smaller operand lengths. Elliptic curves have been accepted commercially and has adopted by standardizing bodies like the American National Standards Institute ANSI, the Institute of Electrical and Electronics Engineers, the International Organization for Standardization ISO, the Standards for Efficient Cryptography Group SECG,and the National Institute of Standard and technology. Cryptography is that the practice and study of hiding information. It is the science of reworking message to form them secure and resistant to attack. In cryptography, the original message is converted into other message at encryption side and converted into an original message at the receiver side. For constrained devices, normal cryptography algorithms can be too slow, too big or too energy-consuming. The term light-weight cryptography studies New algorithms to outdo this problem. Light-weight cryptography is generally defined as cryptography for resource-constrained devices,for which RFID tags and WSN are typically mentioned as examples.Light-weight encryption is a junction of two terms "Light and weight”, and it is a sector of a classical cryptographic algorithm.Light-weight encryption and decryption are implemented on platforms as well as hardware and software. In this paper, present analyzing study on the common use of recent hardware H/W and software S/W implementations of symmetric as well as asymmetric ciphers. The design of Internet of Things (IoT) is a copy of the computer everywhere possible. The spread of RFID, sensors and embedded systems is increasing in cars, smartphones, and others. It has become an inevitable fact that IoT is widely applied to social life applications such as smart grid, intelligent transportation, smart security, and smart home “as shown in fig. below”. In addition to these applications, Access cards, bus cards, and some other small applications are applied.



Lightweight cryptographic model was an algorithm tailored for implementation in limited environments devices. However, the aim of applied lightweight cryptography is to use it in equipment with limited requirements (memory, power, size). Also, lightweight cipher must cope with the tradeoffs among security, cost, and performance as shown in fig below. Moreover, there is a real problem to provide security in such a low-end device. There are some design conditions, such as constrained environment must have a small footprint, low power, and energy consumption, and satisfactory speed

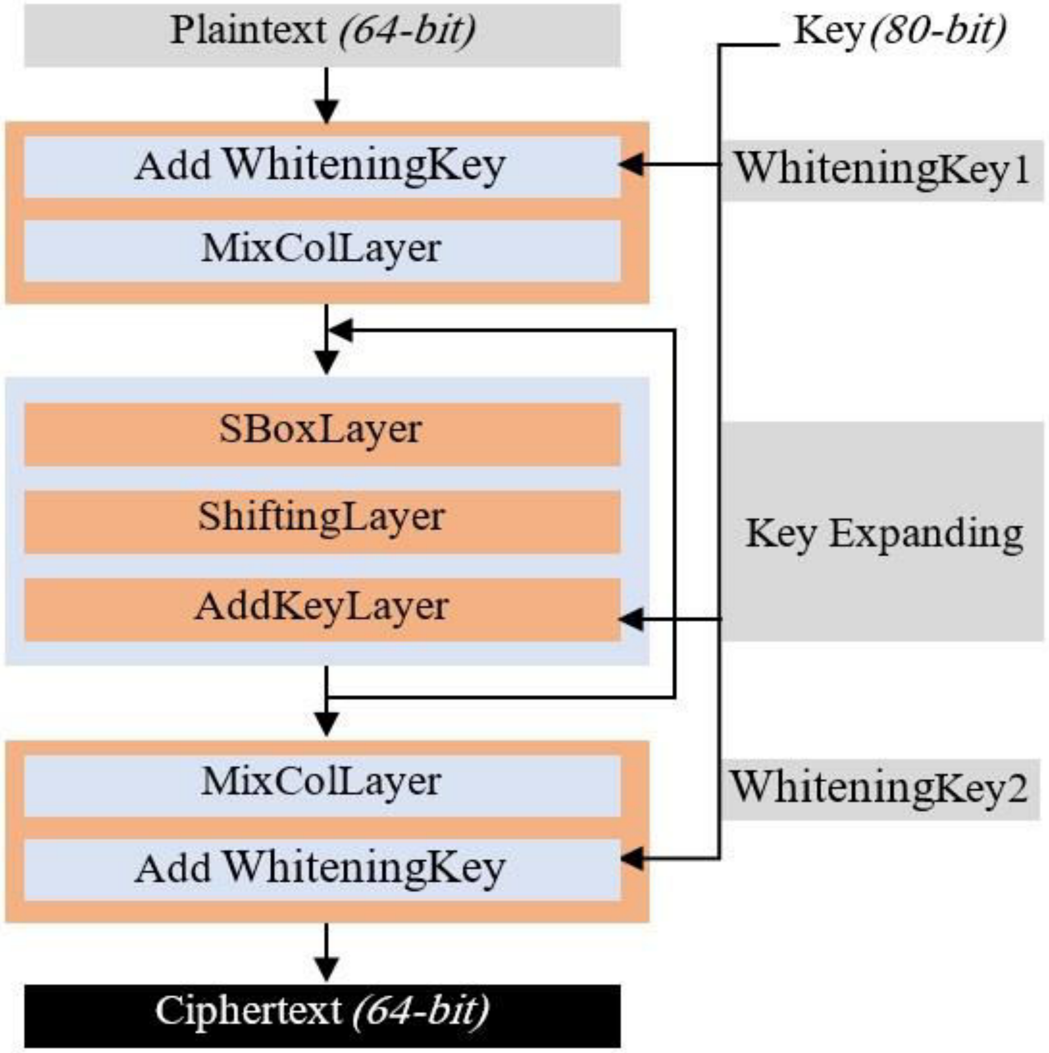


The proposed cipher inherited most of its main characteristics from the previous developed cipher likewise. These structures specify the general form of the work of the algorithm.

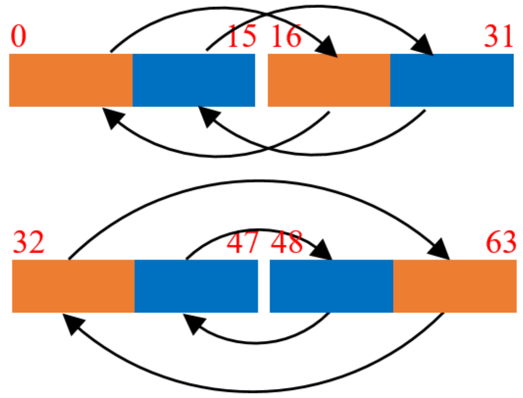
Type:	Symmetric block cipher
Structure:	Substitution Permutation Network
Data size:	64-bit
Key length:	80-bit or 128-bit

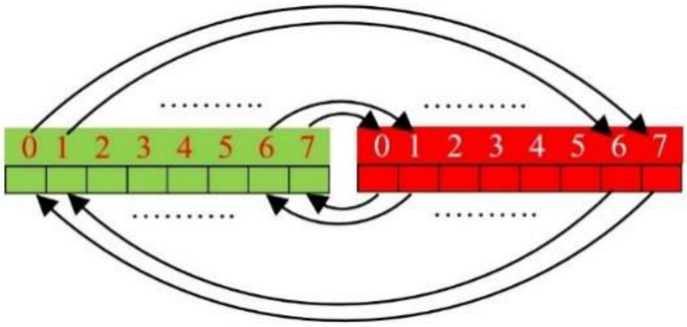
No. of rounds: 6 rounds is enough to maintain the security of data, and to increase the data security we can applying 20 rounds

IV. The Encryption Algorithm

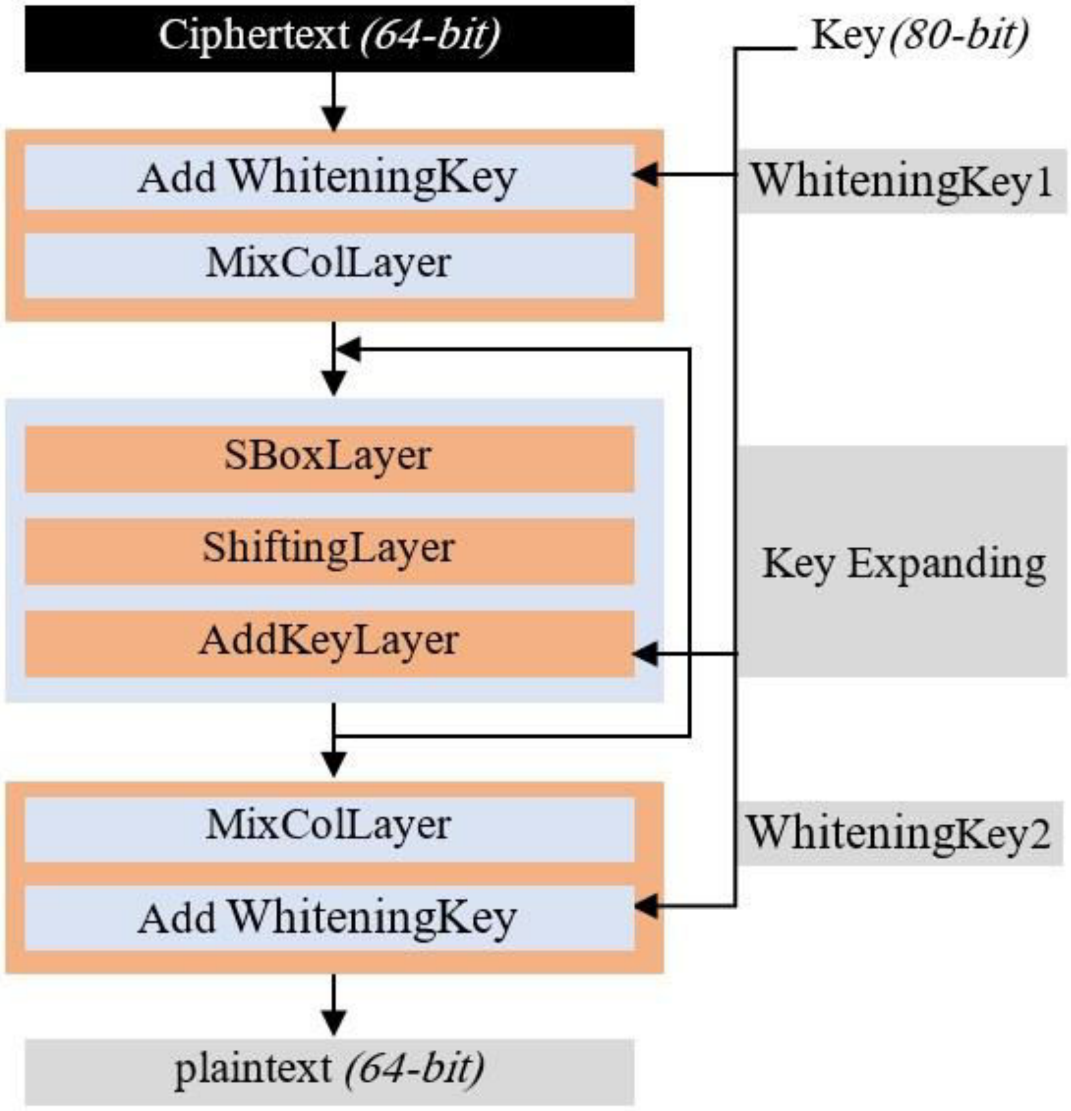


MixCol & Shifting Layers
MixCol & Shifting Layers
MixCol & Shifting Layers





V. The Decryption Algorithm



VI. Analysis Algorithm

While keeping the dimensions of the lightweight cryptography, proposed algorithm designs aim to offer a high level of security. The cipher is designed adopting the theory of provable security against differential and linear cryptanalysis. The suggested cipher presents a full diffusion feature to prevent shortcut attack accumulation. The power was consumed in NVLC algorithm is 1.83 µW with the frequency of 100 KHz

Algorithm	Key	Block size	S-Box	Area in GE	Power Consumption
AES-128	128	128	256	3600	0.35 µm
DESL	56	64	8×16	2310	0.18 µm
Hummingbird	128	16	4×16	2159	0.13 µm
PRESENT-80	80	64	16 (4 group)	1570	0.18 µm
SFN	64	64	16	1877	0.18 µm
NVLC	80	64	16	1134	1.13 µm

VI. Results & Conclusion

The goal of LWC has been a lightweight cipher that applied with a high level of security in the low-resource device. The proposed is described the new block cipher called NVLC, uses round function can be repeated as many times as necessary for more security. The algorithm worked with block symmetric cipher 64-bit and 80-bit/128-bit of the key used SPN structure. Pervasive computing permeates our lives, bringing us nearer to the vision of embedded devices This significant change in the usage and the form number of computing devices produce new challenges in terms of the security of their resources, as well as the connection data that are stored or transmitted. The scientific aspect of using light-weight cryptography that the LWC has become a branch of the modern cryptography and new brand in the analysis of moving towards modern security compared with other systems that do not have the term lightweight cryptography. Provide that the lightweight cryptography is an improvement to a classical or a traditional security when we get the same characteristic of the latter one but with high speed minimum time high performance and low cost. We reach in this survey to the scientific thinking aspect of using light weight cryptography presented a survey of light weight cryptography implementation and had drawn about the various ultra light weight block ciphers whose goal is to be software and hardware efficient.

Refrences

1. X. Yao, Z. Chen, and Y. Tian, “A lightweight attribute-based encryption scheme for the Internet of Things,” Futur. Gener. Comput. Syst., vol. 49, pp. 104–112, 2015.

2. M. favas, C. Fysarakis, K. Papanikolaou,“ a survey of EU research efforts. Security and Communication Networks,” A. Papaefstathiou Embedded systems security, Vol. 8, Iss 11, pp2016-2036, 2015.

3. S. N. Swamy, D. Jadhav, and N. Kulkarni, “Security threats in the application layer in IOT applications,” Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017, pp. 477–480, 2017.

4. O. Oualha, N .Nuha, K. Nguyen, "Light-weight Attribute-Based Encryption for the Internet of Things," In Computer Communication and Networks (ICCCN), 25th International Conference IEEE, USA, pp. 1-6, 2016.

5. Cryptrec, “CRYPTREC Cryptographic Technology Guideline (Lightweight Cryptography),” CRYPTREC Light. Cryptogr. Work. Gr., no. March, pp. 3–7, 2017.

6. Y. Bin Zikria, M. K. Afzal, F. Ishmanov, S. W. Kim, and H. Yu, “A survey on routing protocols supported by the Contiki Internet of things operating system,” Futur. Gener. Comput. Syst., vol. 82, pp. 200–219, 2018.

7. Dunkelman, O., Keller, N., Shamir, A. “A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. In: Rabin”, T. (ed.) International Association for Cryptologic Research 2013, Springer, Heidelberg, International conference on I-SMAC, p477, 2013.

8. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C., “PRESENT: an ultra-lightweight block cipher”. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, Springer, vol. 4727, pp450–466, 2007.

9. H. Cheng, H. M. Heys, and C. Wang, “PUFFIN: A novel compact block cipher targeted to embedded digital systems,” Proc. - 11th EUROMICRO Conf. Digit. Syst. Des. Archit. Methods Tools, DSD 2008, pp. 383–390, 2008.

10. G. Leander, C. Paar, A. Poschmann, and K. Schramm, “New Lightweight DES Variants,” Fast Softw. Encryption, FSE 2007, Springer, LNCS, vol. 4593, pp. 196–210, 2007.

11. C. De Cannière, O. Dunkelman, and M. Knežević, “KATAN and KTANTAN - A family of small and efficient hardware-oriented block ciphers,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5747 LNCS, pp. 272–288, 2009.

12. L. Li, B. Liu, Y. Zhou, and Y. Zou, “SFN: A new lightweight block cipher,” Microprocess. Microsyst., vol. 60, no. December 2017, pp. 138–150, 2018.

13. Omar A. Dawood, Abdul Monem S. Rahma and Abdul Mohsen J. Abdul Hossen: The Euphrates Cipher. IJCSI International Journal of Computer Science Issues, Volume 12, Issue 2, March 2015, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784.

14. Omar A. Dawood, Abdul Monem S. Rahma and Abdul Mohsen J. Abdul Hossen: The Euphrates Cipher. IJCSI International Journal of Computer Science Issues, Volume 12, Issue 2, March 2015, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784.

15. M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, “SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,” vol. 8, no. 1, pp. 1–10, 2017.

16. Omar A. Dawood, Abdul Monem S. Rahma, Abdul Mohssen J. Abdul Hossen: New Symmetric Cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher.

International Journal of Computer Network and Information Security (IJCNIS), Vol.9, No.4, pp. 29-36, 2017.DOI: 10.5815/ijcnis.2017.04.04.

17. Banik S., Bogdanov A., Isobe T., Shibutani K., Hiwatari H., Akishita T., and F., “Midori: A Block Cipher for Low Energy”, IACR-ASIACRYPT-2015, Nov 2015.

18. Z. Gong, S. Nikova, and Y. Law, "KLEIN: A New Family of Lightweight Block Ciphers RFID. Security and Privacy." Vol. 7055, Springer Berlin / Heidelberg, 2012, pp. 1-18.