



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

Investigation of Lightweight Cryptography Algorithms

Dr. J.S. Prasath

Professor, Department of Computer Science and Engineering, Sapthagiri NPS University, Bengaluru, India

jsprasath@gmail.com

DOI: <https://doi.org/10.47760/ijcsmc.2026.v15i09.004>

Abstract: Lightweight cryptographic algorithms are essential for end nodes in order to achieve end-to-end security. The amount of energy consumption for executing lightweight algorithms should be low for battery operated devices. The footprint of the lightweight cryptographic algorithms is smaller than the conventional cryptographic algorithms. The lightweight cryptographic primitives would open possibilities of more network connections with lower resource devices. The objectives of Lightweight cryptography are less complexity in computation, high speed of execution, low power consumption, and tiny memory footprint. This proposed work gives a detailed analysis of various standards and classification of cryptographic algorithms, features of lightweight cryptography, and variety of lightweight cryptography algorithms. Lightweight cryptography needs less computation, and it is widely used in constrained devices. The requirements of lightweight cryptography are memory and circuit size, power, energy consumption, throughput, and latency. Block ciphers accomplish both encryption and message authentication. When the identical block cipher is used, the efficiency and the security differ significantly based on the implementation structure of authenticated encryption. The energy required per bit is a suitable metric for energy-constrained low-resource device applications. The software latency is not based on technology whereas power and area consumption depends on technology. Throughput varies based on technology when the maximum throughput is required, as the extreme frequency depends on the technology being used. It is essential for a lightweight algorithm occupy tiny chip area for its implementation.

Keywords: Cryptography, Encryption, Decryption, Stream cipher, Block cipher



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

1. Introduction

Lightweight Cryptography (LWC) is a technique to guarantee security for resource limited Internet of Things (IoT) devices. It is suitable for implementing the security in IoT devices having tiny memory, least processing power, low battery power, and tiny physical surface. The characteristics of LWC are less computing complexity and tiny footprint. Lightweight algorithms need smaller block sizes of 64-bit or less and key sizes of about 80-bit or less as compared to standard algorithms like Advanced Encryption Standard (AES). Lightweight algorithms are designed to reduce the process involved in encryption and its complexity. This leads to low power consumption and high speed of computation. LWC offers security and efficiency, and allows usage of cryptographic algorithms in a huge range of resource-constrained devices and applications. The coding and size of RAM is preferred for lightweight applications. The implementation of LWC for hardware needs to consider the chip size and the power consumption.

The various standards in the field of cryptography to improve the lightweight standards for the resource-constrained devices are National Institute of Standards and Technology (NIST), USA, International Organization of Standardization and the International Electro-technical Commission (ISO/IEC), Cryptography Research and Evaluation Committees (Cryptrec), Japanese Government Standard, European Network of Excellence in Cryptology (Ecrypt), National Security Agency (NSA), USA, and CryptoLUX, University of Luxembourg, Luxembourg. The international standard ISO/IEC 29192 LWC was established at ISO/IEC JTC 1/SC 27. The U.S. National Institute of Standards and Technology (NIST) that issues guidelines on cryptographic technologies initiated the LWC Project in 2013 and announced a public call for applications of lightweight cryptographies in 2017.

Authenticated encryption that achieves both confidentiality and integrity has been attracting special attention and a technology competition called CAESAR has been held. NEC has developed TWINE, which is a lightweight block cipher, and OTR, which is an authenticated encryption method that has passed the CAESAR second-round selection. PRESENT is a block cipher regarded as being the precursor of lightweight cryptography. It was published in 2007 and has been registered in ISO/IEC 29192. It has a small circuit size that enables implementation in the RFID tag, which is not possible using the standard AES encryption. The U.S. National Security Agency (NSA) published lightweight block cipher SIMON/SPECK that features a very small ROM size suitable to a constrained microprocessor and proposed its addition to ISO/IEC 29192 with the aim of achieving international standardization. A block cipher mode of operation that can achieve both encryption and message authentication is called “authenticated encryption.” Considering the importance of false data detection in IoT, it is expected that encryption will mean authenticated encryption in the future. Even when the same block cipher is used, the efficiency and the security vary considerably depending on how it is implemented as an authenticated encryption. There exist NIST-recommended authenticated encryptions called the AES-CCM/GCM, but considering the importance of authenticated encryption and the progress in research, next-generation authenticated encryptions of lighter weight and higher security are desirable.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

The CRYPTREC (Cryptography Research and Evaluation Committee) assesses electronic government-recommended ciphers and monitors the trends of cryptographic technologies in Japan. NEC's lightweight block cipher called TWINE1) is designed to solve issues with the previous lightweight cryptography PRESENT by its ease of implementation in software. At the same time its implementation will be enabled in small-size circuitry. It employs the same setting as for PRESENT, namely a block length of 64 bits and two kinds of secret key lengths of 80 and 128 bits. TWINE was selected as one of the ciphers to be evaluated by the Lightweight Cryptography and manifested top-class performances in both hardware and software. The block cipher is composed of algorithms that repeat the same processing procedures known as the round functions. With regard to hardware implementation, the circuit size per round of AES is 15K gates but that of TWINE is about 2K gates, which is about 1/7th that of AES (of a similar scale to PRESENT). When the circuit size per throughput is compared, the efficiency of TWINE is more than twice that of AES. For the high-speed communication compatibility, encryption increases the circuit scale due to parallel processing, but the small-scale circuitry of TWINE is also effective in such a case. On the other hand, AES is superior in terms of software implementation. In the case of the microprocessor (Renesas RL78) implementation, it is faster than the lightweight cryptographies including TWINE when the ROM is 1K bytes or more. Compared to PRESENT, the processing speed achieved by TWINE is higher at 250%. The amount of computation required for message authentication is equivalent to that for encryption (secrecy), and the computation amount of AES-CCM/GCM, NIST-recommended authenticated encryptions, is twice the amount required for merely encryption. Since the computation amount of authenticated encryption is more than that for encryption alone, the computation amount equivalent to that for encryption alone becomes the theoretical limit for authenticated encryptions. OCB is an authenticated encryption that can clear the theoretical limit, but it necessitates a block cipher decryption function to perform decryption. On the other hand, as is evident in the fact that AES-CCM configures the decryption processing via the block cipher encryption function, the size can be reduced by reducing the number of its composite elements. OTR2 developed by NEC is the world's first authenticated encryption that achieves the theoretical limit of computation amount using only block cipher encryption functions exclusively.

2. Related Work

The lightweight and hybrid cryptographic techniques are reviewed in order to secure IoT systems without overwhelming several resources [1]. The latest technologies including elliptic curve cryptography (ECC), attribute-based encryption (ABE) and quantum key distribution (QKD) is analysed in terms of low resource consumption. The novel cryptography algorithm is proposed for encryption of text messages [2]. This cryptography algorithm can perform encryption and decryption of combination of alphabets, numbers, and special characters. The hybrid security algorithm is proposed along with the exclusive hardware key using embedded system [3]. This hybrid security algorithm is an integration of asymmetric, symmetric and hash function algorithms which guarantees strong security. An innovative and lightweight authentication structure is proposed for IoT devices that integrate the delegation of blockchain



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

with the efficiency of lattice-based cryptography to address these security issues [4]. It utilizes a distributed identity management approach built on blockchain, removing susceptible central points and improving system flexibility. An Autonomous Bidirectional Authentication and Lightweight Encryption Protocol (ABA-LEP) is designed and analysed for drones under ARM architecture [5]. It works on simple operations like one-time pad limited XOR for lightweight secure communication encryption. Information security transmission scheme is designed for a data interchange framework based on lightweight AES encryption algorithm [6]. An AES data interchange platform data encryption communication technique is created, using attribute encoded data as input to guarantee information security. The performance evaluation of lightweight block ciphers, including PRESENT, Piccolo, RECTANGLE, SPARX, and LED, on various sensor motes is done [7]. This investigation begins with a careful selection of sensor motes and platforms, enabling realistic simulations and practical evaluations. A lightweight RFID protocol is proposed based on the Ring Learning With Errors (RLWE) problem, confirming post-quantum security while retaining efficiency for resource-constrained environments [8]. It gives a resilient foundation for creating quantum-resistant cryptographic structures. Ascon cryptography is implemented as a peripheral of a RISC-V System-on-a-Chip (SoC) [9]. The ASCON crypto core occupies 1,424 LUTs in FPGA and 17.4 kGE in 180nm CMOS technology while achieving 417 Gbits/J energy efficiency at a supply voltage of 1.0V and frequency of 2 MHz. A security protocol is proposed that is robust to the computational competencies of quantum computers [10]. This protocol is compared and analysed in terms of performance and security in contrast to existing protocols. The dual byte-based differential fault attack models is proposed for the diffusion characteristics of round function of the GIFT algorithm [11]. This model has substantial breakthroughs with respect to both the attack range and the number of required faults. An innovative lightweight multi-user public-key authenticated encryption scheme with keyword search (LM-PAEKS) is proposed for privacy preservation [12]. This design efficiently counters the inside keyword guessing attack (IKGA) while sustaining the sizes of ciphertext and trapdoor constant in multi-user scenarios. A lightweight hybrid cellular automata-based algorithm is proposed for IoT applications [13]. It utilizes several layers of hybrid cellular automata and a secondary secret key. IoT technology, architecture, and applications is reviewed [14]. The lightweight block ciphers, stream ciphers, and hybrid ciphers are discussed. A lightweight block cipher CARX for drones is proposed to rectify the security problem in drone communication [15]. The lightweight white-box encryption communication system for drones (LWED) is designed and simulated, which can complete the encryption and decryption operations and achieve secure transmission of data and images. An integrated analytical structure for lightweight ciphers is implemented within heterogeneous computing environments [16]. This technique is based on identified set of metrics that can sufficiently allow the capturing, ranking, and classifying the achieved performance. The encryption algorithm is proposed for secure transmission of underwater images over the Underwater Acoustic Networks [17]. It is based on a confusion-diffusion architecture employing the 2D Exponential-Cosine transform and DNA Encoding operations. An Enhanced Energy Efficient Lightweight Cryptography Method is proposed which employs the concept of 8-bit manipulation [18]. The hardware complication has been authorized



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

using Spartan3E XC3S500E FPGA devices. The efficient asymmetric multi-recipient cryptographic method is proposed to rectify the problem of computational overhead in performing both encryption and decryption. [19]. The sender communicates a ciphertext including dissimilar information to several receivers, where each receiver is only permitted to recover its specific selected information. The issues in the addition of security to the IoT network layer by comparing the performance of LWC algorithms with standard algorithms is addressed [20]. This study will guide the researchers in selecting an appropriate model and optimal LWC algorithm for IoT applications. The FPGA-based acceleration engine of Elliptic Curve Cryptography using binary Edward curves is presented [21]. This proposed design is lightweight of less than 1400 slices of Virtex-5 FPGA and it offers security level equivalent to 128-bits. The LWC algorithm is proposed for improving data security on cloud computing [22]. This algorithm achieves strong security level and a specious improvement in measures of cipher run time.

3. Classification of Cryptography

Cryptography is classified into symmetric keys cryptography and asymmetric keys cryptography. Symmetric cryptography utilizes a single key to perform encryption and decryption of the data. Asymmetric cipher uses dual keys to encrypt and decrypt the data. Symmetric key cryptography is secure and relatively fast and the only drawback of symmetric key encryption is the key sharing among the communicating users. But this could be rectified by pre-sharing the key through a reliable third party. It ensures confidentiality, data integrity and authentication of the data. Asymmetric cryptography utilizes two keys which are public and private keys. It assures data confidentiality and integrity by using the public key of the receiver. It guarantees authentication by encrypting the data by using the sender's private key as a digital signature. The receiver decrypts it by using the sender's public key first and then using his/her private key. The limitation of asymmetric cryptography is its large key which raises the computational burden and slows down the process.

Figure 1 shows the classification of cryptography based on structure. Symmetric cryptography is suitable for IoT devices in the resource-constrained environment. Symmetric key cryptography could be further classified into three categories depending on how it works. These are block cipher, stream cipher, and hash functions. In block cipher, both encryption and decryption take place on a fixed size block of 64 bits or more at a time, whereas stream cipher constantly processes the input elements bit by bit or byte by byte. There are two basic properties of any cryptography, confusion and diffusion, introduced by Claude Shannon to strengthen the cipher. The stream cipher utilizes only the confusion property, whereas the block cipher uses both confusion and diffusion with a simple design compared to the stream one. The reverse encryption process used to extract the original text is the difficult task in a block cipher.

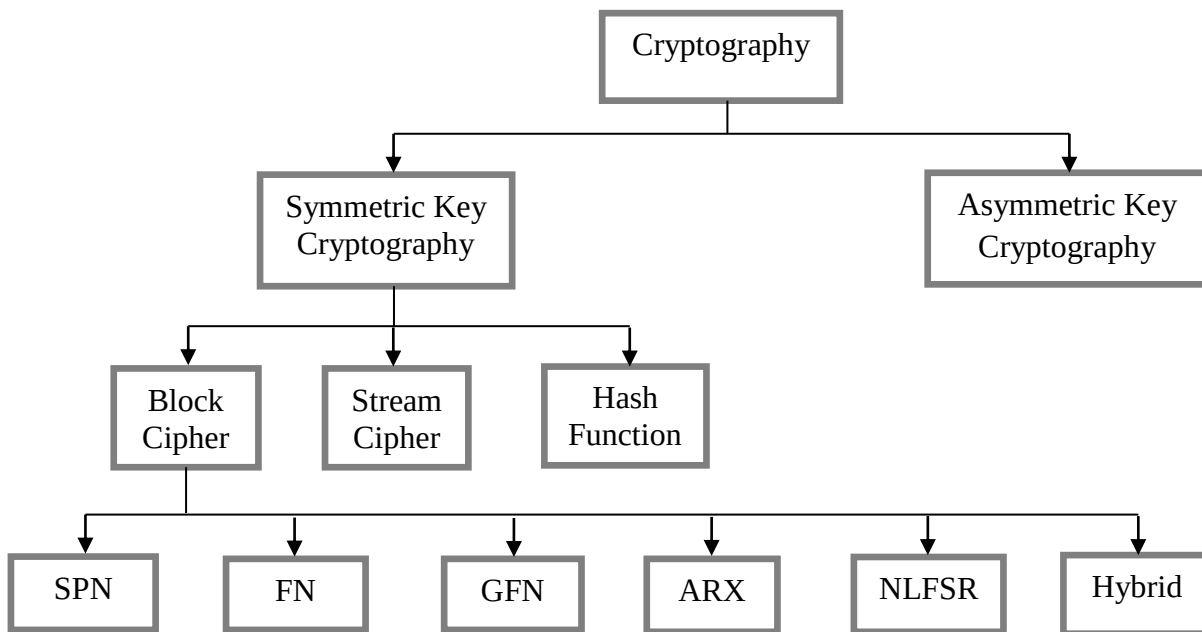


Figure 1 Classification of Cryptography based on Structure

A stream cipher performs XOR functions to encrypt the data, which could be easily reverted to its original form. The block cipher is classified into six following types depending on the functions used to create the cipher. These are Substitution-Permutation Network (SPN), Feistel Network (FN), General Feistel Network (GFN), Add-Rotate-XOR (ARX), Non-Linear Feedback Shift Register (NLFSR), and Hybrid encryption. SPN performs encryption of the data through a set of substitution boxes and permutation tables and formulates them for the following round. A Feistel network (FN) breaks the input block into equal halves and applies diffusion in each round to just one half. In addition, swapping of two halves happens at the beginning of each round. The generalized Feistel network (GFN) is an extrapolated version of the classic Feistel network. It splits the input block into many sub-blocks and applies the Feistel functions to every pair of sub-blocks, followed by a cyclic shift proportional to the number of sub-blocks. ARX performs encryption-decryption using addition, rotation and XOR functions without making use of S-box. Implementation of ARX is fast and compact but limited in security properties compared to SPN and Feistel ciphers. Nonlinear feedback shift register (NLFSR), applies to both stream and block ciphers, utilizes the building blocks of stream ciphers whose current state is derived from its last state,



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

which is a nonlinear feedback value. Hybrid cipher combines any three types (SPN, FN, GFN, ARX, NLFSR) or even mixes block and stream property to improve specific characteristics such as throughput, energy based on its application requirements.

4. Features of Lightweight Cryptography

The essential features of LWC are physical cost, physical area, keysize, block size, memory includes RAM, and ROM size, number of rounds, battery power consumption, key generation mechanism, computational capability, latency, throughput, strong internal structure, characteristics of cryptanalysis such as Linearity, Nonlinearity, Differential cryptanalysis, Avalanche Effect, Bit Independence criteria and Algebraic attacks.

Hardware and Software performance metrics

Hardware and Software requirements are based on physical and performance provided by LWC algorithms. It could be measured in terms of memory requirements, gate area, latency, throughput, and power and energy consumption.

Memory requirements

It is measured in KB and the RAM is required to store transitional values that can be used in computations, and ROM is required to store the program/algorithm, and static data, such as algorithm key, and S-box.

Gate Area

It is the physical area required to implement/run the algorithm on a board/circuit, measured in μm . This space can be defined using logical blocks for Field Programmable Gate Array (FPGA) or using Application Specific Integrated Circuits (ASIC).

Latency

It is the time taken to generate the cipher from the original text in terms of hardware performance whereas the amount of clock cycles per block (during encryption) defines the software latency.

5. Structure wise classification of LWC Algorithms

The block cipher is classified into six following types based on the internal structure used to create the cipher, These are Substitution-Permutation Network (SPN), Feistel Network (FN), General Feistel Network (GFN), Add-Rotate-XOR (ARX), Non-Linear Feedback Shift Register (NLFSR), and Hybrid structure. Table 1 shows the classification of LWC based on structure.

Substitution Permutation Network (SPN)

AES is a classic model of SPN based algorithm, regularized by NIST, performs on 128-bit block with 128, 192 and 256-bit key alternatives. The higher level of performance can be attained by utilizing extra resources. PRESENT algorithm is the most effective for implementing both hardware and software.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

It is Substitution-Permutation network-based which utilizes 64-bit block on two key alternates of 80-bit and 128-bit keys. GIFT is an enhanced version of PRESENT and it provides a lighter S-Box with tiny physical space. The number of rounds is fewer and provides large throughput along with a easier and faster key schedule. The two versions of GIFT are GIFT-64 involves 28-round with 64-bit block size and GIFT-128 involves 40-round with 128-bit block size. GIFT-64 and GIFT-128 operates on 128-bit key size and GIFT-64 is susceptible than GIFT128. SKINNY has two versions which are SKINNY-64 and SKINNY-128. SKINNY-64 utilizes 64-bit block with 64/128/192-bit key alternates to perform 32/36/40 rounds, and SKINNY-128 utilizes a 128-bit block with 128/256/384-bit key alternatives to perform 40/48/56 rounds. RECTANGLE is an ultra-lightweight block cipher used in variety of applications. TWINE is better than PRESENT and it rectifies the problems involved in implementation. It works on 64-bit input with two key alternatives of 80-bit and 128-bit respectively. MIDORI was designed with a emphasis on less energy budget and it has two different versions which are Midori64 and Midori128. Both of these versions utilize a 128-bit key on two dissimilar block sizes, 64-bit and 128-bit with 16 and 20 iterations respectively. NOEKEON operates on the identical block and key size, 128 bit, with 16 iterations. PUFFIN-2 utilizes 80-bit key length to perform 34 iterations on 64-bit data based on serialized SPN structure. PRINCE is both hardware and software efficient lightweight algorithm which performs on 64-bit input using a 128-bit key size.

Table 1 Classification of Lightweight Cryptography based on Structure

Structure Types	Lightweight Cryptography Algorithms
SPN	AES, Present, GIFT, SKINNY, Rectangle, Midori, mCrypton, Noekeon, Iceberg, Puffin-2, Prince, Pride, Print, Klein, Led, Picaro, Zorro, EPCBC, I-Present, ASCON, SHAMASH, PRIMATE, ICEPOLE
FN	DESL/DESXL, TEA/XTEA/XXTEA, Camellia, Simon, SEA, KASUMI, MIBS, LBlock, ITUbee, FeW, GOST, Robin, Fantomas
GFN	CLEFIA, Piccolo, Twis, Twine, HISEC
ARX	Speck, IDEA, HIGHT, BEST-1, LEA
NLFSR	KeeLoq, KATAN/KTANTAN, Halka
Hybrid	Hummingbird, Hummingbird 2, Present

Feistel Network (FN)

Feistel networks are classified into two types which are Classical Feistel Networks and Generalized Feistel networks (GFN). While classical Feistel ciphers divide a message into two sub-blocks, GFN divides a message into k sub-blocks for some $k > 2$ called the partition number. Feistel networks are a popular choice for implementing lightweight block ciphers. While classical Feistel



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

networks divide messages into two sub-blocks, the GFN divides them into k sub-blocks, where k is greater than 2. The GFN of Type-II, in particular, is a popular form where the Feistel transformation is applied to two consecutive sub-blocks, followed by a cyclic shift of sub-blocks.

Generalised Feistel Network (GFN)

GFN is introduced by SONY corporation and approved by NIST, CLEFIA offers 128-bit block with choice of 128, 192, 256 bit key through 18, 22, 26 round. It shows high performance and strong immunity against various attacks with comparative high cost as the most compact version requires 2488 GE (encryption only) for 128-bit key. GFN supports the creation of block ciphers from non-linear components with tiny domains, and has been implemented in various block ciphers. Piccolo is another ultra-lightweight cryptography algorithm suitable for extremely restricted environmental devices. It processes 64-bit input to perform two iterations, 25 and 31, using two key sets, 80-bit and 128-bit, respectively. The smallest hardware deployment (80-bit key) requires 432 GE and additional 60 GE to perform decryption. TWIS, derived from CLEFIA, takes equal size block and key (128-bit) to perform 10 iterations. It is a victim of differential distinguisher with probability one. TWINE, derived from LBlock, performs 36 iterations on a 64-bit state along with two key options, 80-bit and 128-bit. TWINE uses nibble permutation instead of bit permutation (for sub-key generation) of LBlock. Also, it uses a single S-box instead of ten S-Boxes of LBlock. HISEC performs 15 iterations on 64-bit input along with an 80-bit key, demanding 1695 GE. It shows good resistance against different attacks, and the characteristics are more like to PRESENT except bit-permutation.

6. Lightweight Cryptography Algorithms

The conventional cryptographic algorithms are not suitable for usage with IoT devices due to its resource constraints. IoT devices require security algorithms that should have lightweight, low energy consumption, and efficient computation. Lightweight cryptographic algorithms are utilized for resource-constrained devices, which provide secure communication with less computational complexity. The basic characteristics of lightweight cryptography are standard encryption algorithms, less computation time, robust design, high throughput, and occupies less memory space. The coding of lightweight cryptography should be implementing in tiny hardware, consuming low power, and it should be strong against differential attacks. Even-though the several lightweight encryption techniques are proposed, the various challenges still need to be addressed are high execution time, amount of power required to compile the program, internal state, chip size, overhead, and the attainment of security level.

The lightweight DES (Data Encryption Standard) operates on a similar block size (64-bit), key (56-bit) and a similar number of rounds as DES. The reduced number of S-box and multiplexer utilized in lightweight DES differentiates it from DES. Lightweight DES rejects the initial and final permutation of DES. DESXL is another lighter edition of DES with a key whitening feature to strengthen the cipher and with 2170 GE demands. It performs the same number of cycles and uses the same block size as DESL, but a larger key, 184-bit ($k=56$, $k_1=64$, $k_2=64$). Tiny Encryption Algorithm (TEA) is suitable for very



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

small, computationally weak and low-cost hardware. It works on 128-bit key on 64-bit input to accomplish 32 rounds. The key generation is simple but it is susceptible to brute force attack. Another drawback of the TEA method is its triple equivalent keys for decryption which makes it vulnerable to the intruders. The enhanced version of TEA is XTEA which utilizes the identical size of key and block but with increased iterations (64 rounds). It provides more difficult key scheduling with small change in Shift, XOR and addition functions. XTEA was additionally changed with XXTEA to protect against related-key rectangle attack.

NSA designed SIMON which is known for its small footprint in hardware. It offers various keys of size (64-bit, 72-bit, 96-bit, 128-bit, 144-bit, 192-bit, 256-bit) over the block of 32-bit, 48-bit, 64-bit, 96-bit, 128-bit through 32, 36, 42, 44, 52, 54, 68, 69, 72 rounds. The optimised software compilation needs 426 bytes with encryption cycle of 41604 on 8-bit micro-controllers. KASUMI takes 64-bit input to performs 8 iterations using a 128-bit key. It is mainly designed for GSM, UMTS and GPRS systems. LBlock is an ultra-lightweight cipher, performs 32 iterations on 64-bit input along with 80-bit keys. It is designed and developed by the government of the Soviet Union (1989), the lightweight version of GOST executes 32 times on 64-bit input with a 256-bit key. ITUbee is a software efficient cipher with a code size of 586 bytes and 2937 cycles (the most compact version of encryption. It takes the precise size of the key and block of 80-bit. The key scheduling is substituted by round-dependent constants to decrease software burden. FeW processes 64-bit input with dual varieties of the key, 80-bit and 128-bit for 32 times. It makes use of the S-box of Humminbird-2 and follows the key expansion process from PRESENT. There no cryptanalytic attack found on FeW.

Existing Lightweight Cryptography Algorithms

There are more than fifty symmetric LWC algorithms are proposed by various academia, proprietaries and government organizations with a focus on reducing cost, memory size, processing power, physical area, energy consumption and improved hardware and software performance such as latency, and throughput. Most of the symmetric block cipher cryptography algorithms are derived either from DES or AES, which are the milestones for cryptography algorithms. It could be said that PRESENT, inspired by AES, is the milestone of lightweight cryptography and is at the root of many newly proposed lightweight cryptography algorithms.

There are several lightweight ciphers are proposed which includes ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, and Xoodoo. Besides these algorithms, the other algorithms are lightweight encryption algorithm (LEA), Few-Wave (FeW), Prince, Twine, Lblock, Piccolo, Lightweight Encryption Device (LED), Lightweight Stream Ciphers (LESCA), and LORMHE, SIMON and SPECK, PRESENT, CLEFIA, Hummingbird-2, Schwaemm, and Esch256.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

ASCON Cipher

ASCON is an efficient lightweight cryptographic algorithms designed for resource-constrained devices, including the Internet of Things (IoT) devices. It offers authenticated encryption with associated data (AEAD), hash functions, message authentication, and extendible output functions. ASCON was selected by the National Institute of Standards and Technology (NIST) as a standard for lightweight cryptography, demonstrating its efficiency and security for resource-constrained environments. ASCON is a duplex-based mode of operation to achieve authenticated encryption. ASCON Encryption involves initialization, associated data processing, plaintext processing, and finalization.

Elephant Cipher

Elephant is a family of lightweight authenticated encryption schemes designed for resource constrained IoT devices. It is based on a nonce-based encrypt-then-MAC construction. This ensures that the cipher text will vary when we are using the identical key and the identical plaintext. It offers Authenticated encryption with Associated Data (AEAD) and to provide excess data for the cipher. Unlike the nonce value, this additional data is not sent with the cipher text or used within the encryption method but can be used to authenticate the cipher text.

GIFT-COFB Cipher

GIFT-COFB is a light-weight crypto cipher works on combined feedback based Authenticated encryption with Associated Data mode. GIFT-128 cipher is an 128-bit Substitution-Permutation network (SPN) based block cipher with a key size of 128-bit. It is a 40-round iterative block cipher with same round function. Each round of GIFT-128 involves three operations that are SubCells, PermBits, and AddRoundKey.

Grain-128 AEAD Cipher

Grain-128 AEAD was designed to be an efficient and secure cipher in hardware. The performance of is better with respect to both hardware and software on constrained devices. Grain was first proposed as an 80-bit stream cipher in 2005, and the 128-bit variant cipher was presented in 2006. Grain-128 supporting Authenticated Encryption with Associated Data (AEAD) was proposed in 2019 to ensure data confidentiality and authentication. The cipher is logically divided into three phases for hardware implementation. The first phase involves loading of shift registers with the key and the nonce. The second phase is the initialization phase in which the registers and the authentication part are initialized. The third phase is the execution phase, in which pre-output is produced for both encryption and authentication. Hardware implementations also have a natural arrangement between gate complexity and speed. Grain-128 AEAD can be suitable for usage in case of Passive Keyless Entry and Start (PKES) system in automotive applications.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

ISAP Cipher

ISAP is a family of nonce-based authenticated ciphers with associated data (AEAD) designed to provide data security against passive side-channel attacks. ISAP involves small state, and simple permutation for constrained devices.

Romulus Cipher

Romulus is a family of lightweight, very efficient, and highly-secure algorithms. Romulus-M achieves n -bit security against nonce-respecting adversaries and $n/2$ -bit security against nonce-misusing adversaries. Romulus Cipher involves encryption of tiny message with associated data using a private key and a nonce, which generates cipher text and a tag for authentication. The benefits of Romulus ciphers are highly reliable security, misuse-resistant security, less complexity for tiny messages, tiny operating state size, and leakage resilience.

Sparkle Cipher

The Sparkle cipher is a lightweight cryptographic algorithm designed for use in authenticated encryption and hash functions. It works on different block sizes (256, 384, or 512 bits) and utilizes an ARX (Addition, Rotation, and XOR) approach. A universal implementation exists for all variants, taking block size and number of steps as inputs. The key is the Alzette transformation, which is a 64-bit transformation used in the round function of each Sparkle instance.

TinyJambu Cipher

TinyJAMBU mode is a small variant of the JAMBU mode which is a third-round candidate of the CAESAR competition. In the TinyJAMBU mode, a 128-bit keyed permutation is used, the state size is 128 bits, and the message block size is 32 bits. When nonce is reused, the TinyJAMBU mode provides better authentication security than the JAMBU mode. When nonce is reused, the TinyJAMBU mode provides better authentication security than the Duplex mode for the same permutation size and the same message block size. The reason is that the attacker can easily set part of the state to arbitrary value when nonce is reused in the Duplex mode, while it is difficult to do that in the TinyJAMBU mode.

Xoodyak Cipher

Xoodyak is a lightweight, versatile, cryptographic scheme suitable in constrained environments. It can be used for hashing, encryption, MAC computation and authenticated encryption. The Xoodyak encryption mode has a 128-bit key, a 128-bit nonce, and a 128-bit authentication tag. The Xoodyak hashing mode has a 256-bit fixed hash output and can also be used as an extensible output function. The Xoodyak specification describes a re-keying mechanism where the key for one packet is used to derive the key to use on the next packet. This provides some resistance against side channel attacks by making the session key a moving target.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

Lightweight Encryption Algorithm (LEA)

LEA is a symmetric block cipher designed for efficient hardware and software implementations. It involves a block size of 128 bits and supports key sizes of 128, 192, and 256 bits. The security level of the algorithm depends on simplicity, speed, and proven security, making it suitable for various applications, including mobile devices, embedded systems, and network communications.

The features of the LEA Algorithm are higher level of security, lightweight design, variety of key length, and effective hardware implementation.

- **ASCON:** A widely adopted algorithm.
- **Elephant:** Another finalist.
- **GIFT-COFB:** A cryptographic algorithm.
- **Grain128-AEAD:** A lightweight authenticated encryption algorithm.
- **ISAP:** A lightweight authenticated encryption algorithm.
- **Photon-Beetle:** A lightweight authenticated encryption algorithm.
- **Romulus:** A lightweight authenticated encryption algorithm.
- **Sparkle:** A lightweight authenticated encryption algorithm.
- **TinyJambu:** A lightweight authenticated encryption algorithm.
- **Xoodyak:** A lightweight authenticated encryption algorithm.

Other Notable Algorithms

- **LEA (Lightweight Encryption Algorithm):** Developed by South Korea, LEA is a 128-bit block cipher designed for high-speed environments like big data and cloud computing, as well as resource-constrained devices like IoT and mobile devices.
 - **FeW (Few-Wave):** A family of lightweight authenticated encryption algorithms.
 - **Prince:** A lightweight block cipher.
 - **TWINE:** A lightweight block cipher.
 - **Lblock:** A lightweight block cipher.
 - **Piccolo:** A lightweight block cipher.
 - **LED (Lightweight Encryption Device):** A lightweight block cipher.
 - **LESCA:** A lightweight stream cipher.
 - **LORMHE:** A lightweight stream cipher.
- **SIMON and SPECK:** Families of lightweight block ciphers designed for simplicity and performance in hardware and software.
 - **PRESENT:** A lightweight block cipher.
 - **CLEFIA:** A lightweight block cipher.
 - **Hummingbird-2:** A lightweight authenticated encryption algorithm.
 - **Schwaemm:** A family of lightweight authenticated encryption algorithms.
 - **Esch256:** A lightweight hash function.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

Key Considerations for Lightweight Cryptography

- **Resource Constraints**

These algorithms are designed to minimize memory, processing power, and energy consumption, making them suitable for resource-limited devices like IoT sensors and mobile devices.

- **Performance**

They prioritize speed and efficiency, particularly for real-time applications.

- **Security**

They provide a strong level of security against common attacks, while also being adaptable to evolving threats.

7. Conclusion

Lightweight cryptography has received with more considerations from both researchers and industries. The huge number of lightweight algorithms have been developed including PRESENT, CLEFIA, LED, KANTAN, especially for constrained devices. This paper discussed about popular lightweight cryptography algorithms and analysed its features and computational capability. This paper also gives an overview of classification of cryptography based on structure. The parameters of cryptography such as block sizes, key sizes, and key scheduling should be taken into account and it should as small as possible. Tiny blocks and short-key size can reduce the time to perform encryption and decryption process. The use of mathematical operations such as addition, AND, OR, XOR and shift are efficient because simple operations can be applied to all elementary platforms. When the number of iteration rounds is increased, the execution time also increases. The key size determines the strength of cryptographic algorithms, but faster and stronger ciphers usually come with higher costs. The energy consumption are critical for few applications whereas latency is an essential factor for most applications. None of the lightweight algorithms in general meets all the criteria for both hardware and software performance metrics. The standard hardware and software security mechanisms and performance metrics need to be developed to evaluate the security level of lightweight cryptography and its implementation.

References

- [1]. Zeeshan Ali Haider, Asim Zeb, A.K.M.Muzahidul Islam, Taj Rahman, Ali Arishi, Inam Ullah, "Enhancing IoT security with resource-efficient cryptography: A comprehensive review of lightweight and hybrid algorithms," Computer Science Review, Vol. 59, pp. 1-28, 2026.
- [2]. J.S.Prasath, "PrasathSrinivasan Cryptography Algorithm for Text Encryption and Decryption," International Journal of Scientific Research in Science, Engineering and Technology, Vol. 13, No. 3, pp. 427-445, 2026.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

- [3]. J.S.Prasath, "Proposed Hybrid RSA, AES and SHA Algorithms with Hardware Key Security Mechanisms for Embedded Systems with Internet of Things," *The Indonesian Journal of Computer Science*, Vol. 15, No. 3, pp. 4299-4313, 2026.
- [4]. Yingpan Kuang, Qiwen Wu, Riqing Chen, Xiaolong Liu, "Blockchain based lightweight authentication scheme for internet of things using lattice encryption algorithm," *Computer Standards and Interfaces*, Vol. 93, 103981, 2025.
- [5]. Qian Zhou, Jiayang Wu, Weizhi Meng, "ABA-LEP: Autonomous Bidirectional Authentication and Lightweight Encryption Protocol for drones under ARM architecture," *Journal of Information Security and Applications*, Vol. 95, 104268, 2025.
- [6]. Wenliang Wang, Jishun Ma, Bin Zhao, Peng Han, Peng Zeng, "Information security transmission method of data exchange platform based on lightweight AES encryption algorithm," *Egyptian Informatics Journal*, Vol. 32, 100831, 2025.
- [7]. Amal Hkiri, Mouna Karmani, Fawaz Hasan Alasmay, Omar BenBahri, Ahmed Mohammed Murayr, Mohsen Machhout, "In-depth study of lightweight block ciphers: Performance assessment and implementation on sensor motes," *Alexandria Engineering Journal*, Vol. 113, pp. 461-479, 2025.
- [8]. Haradhan Ghosh, Pramod Kumar Maurya, Satya Bagchi, Ashutosh Dhar Dwivedi, "Lightweight RFID-enabled authentication protocol in post-quantum environment," *Computers and Electrical Engineering*, Vol. 124, 110367, 2025.
- [9]. Khai-Duy Nguyen, Tuan-Kiet Dang, Binh Kieu-Do-Nguyen, Duc-Hung Le, Cong-Kha Pham, Trong-Thuc Hoang, "ASIC Implementation of ASCON Lightweight Cryptography for IoT Applications," *IEEE Transactions on Circuits and Systems*, Vol. 72, No.1, pp. 278-282, 2025.
- [10]. Salahdeen Duraibi, Abdullah Mujawib Alashjaee, "Lightweight Post-Quantum Secure Communication Protocol for IoT Devices using Code-based Cryptography," *IEEE Transactions on Consumer Electronics*, Vol. 71, No. 4, pp. 11228-11236, 2025.
- [11]. Yuan Gao, Zhongya Zhang, Zhiyong Zhang, "Differential Fault Attack of Lightweight Cipher GIFT Based on Byte Model," *IEEE Internet of Things Journal*, Vol. 12, No. 1, pp. 435-444, 2025.
- [12]. Yongliang Xu, Hang Cheng, Jiguo Li, Ximeng Liu, Xinpeng Zhang, Meiqing Wang, "Lightweight Multi-User Public-Key Authenticated Encryption With Keyword Search," *IEEE Transactions on Information Forensics and Security*, Vol. 20, pp. 3234 – 3246, 2025.
- [13]. Abrar Hasan, M. M. A. Hashem, "A Lightweight Cryptographic Framework Based on Hybrid Cellular Automata for IoT Applications," *IEEE Access*, Vol. 12, pp. 192672 – 192688, 2024.
- [14]. Fursan Thabit, Ozgu Can, Asia othman Aljahdali d, GhalebH. Al-Gaphari, Hoda A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security," *Internet of Things*, Vol. 22, 100759, 2023.
- [15]. Yatao Yang, Hui Dong, Zhaofu Li, Song Xiao, "LWED: Lightweight white-box encryption communication system for drones over CARX algorithm," *Journal of King Saud University - Computer and Information Sciences*, Vol. 35, No. 9, 101727, 2023.
- [16]. Issam W. Damaj, Hadi Al-Mubasher, Mahmoud Saadeh, "An extended analytical framework for heterogeneous implementations of light cryptographic algorithms," *Future Generation Computer Systems*, Vol. 141, pp. 154-172, 2023.
- [17]. S.B. Goyal, Renjith V. Ravi, Chaman Verma, Maria Simona Raboaca, Florentina Magda Enescu, "A Lightweight Cryptographic Algorithm for Underwater Acoustic Networks," *Procedia Computer Science*, Vol. 215, pp. 266-273, 2022.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Dr. J.S. Prasath, Volume 15, Issue 9, September 2026, pg. 41-56

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

- [18].Prakasam P, Madheswaran M, Sujith K.P, Md Shohel Sayeed, “An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices,” ICT Express, Vol. 7, pp. 487-492, 2021.
- [19].Ahmad Mansour, Khalid M. Malik, Niko Kaso, “AMOUN: Asymmetric lightweight cryptographic scheme for wireless group communication,” Computer Communications, Vol. 169, pp. 154-167, 2021.
- [20].Amir Fotovvat, Gazi M. E. Rahman, Seyed Shahim Vedaei, Khan A. Wahid, “Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes,” IEEE Internet of Things Journal, Vol. 8, No. 10, pp. 8279-8290, 2021.
- [21].Carlos Andres Lara-Nino, Arturo Diaz-Perez, Miguel Morales-Sandoval, “Lightweight elliptic curve cryptography accelerator for internet of things applications,” Ad Hoc Networks, Vol.103, 102159, 2020.
- [22].Fursan Thabit, Sharaf Alhomdy, Abdulrazzaq H.A. Al-Ahdal, Sudhir Jagtap, “A new lightweight cryptographic algorithm for enhancing data security in cloud computing,” Global Transitions Proceedings, Vol. 2, No. 1, pp. 91-99, 2021.

AUTHOR PROFILE



Dr. J.S.Prasath received Master of Engineering degree in Process Control and Instrumentation Engineering from Annamalai University, Chidambaram and Doctor of Philosophy degree in Wireless Sensor Networks for Industrial Security from Hindustan Institute of Technology and Science, Chennai, India. Currently he is working as a Professor in the Department of Computer Science and Engineering at Sapthagiri NPS University, Bengaluru, India. He is an interdisciplinary and guiding many Research projects at Under graduate and Post graduate level. Earlier he served in SRM University, Hindustan University, KCG College of Technology and Narayana Engineering College. His research interests are Embedded Systems,

Wireless Sensor Networks, Internet of Things, Process Control and Industrial Automation. He has published thirty one articles in International Journals, presented twenty papers in International Conference, published two patents, written two books and three book chapters. He received the best teacher award and the two innovation awards for his research work.