Security Algorithm Analysis and Implementation in an IoT Environment

B.Kameswara Rao[1], Dr.A.Saranya[2], Mr Velidi Saibaba[3], P G Mamatha[4], Dillip Narayan Sahu[5], Venkata Naga Rani Bandaru[6]

[1]Associate Professor, Department of Computer Science and Engineering, Gandhi Institute of Technology and Management, GST, Gitam (Deemed to be university) Visakhapatnam Campus, Visakapatnam, India.

[2]Guest Lecturer, Department of Master of Computer Applications, Madurai Kamaraj University , Madurai, Tamilnadu, India.

[3]Assistant Professor, Department of Information Technology, Sagi Ramakrishnam raju Engineering College, Bhimavaram, Andhra Pradesh, India.

[4]Assistant professor, Dept of Electronics and Communication Engineering, Sree Vidyanikethan Engineering College,A. Rangampet. Andhra Pradesh, India.

[5]Lecturer, Department of MCA, School of Computer Science, Gangadhar Meher University (GMU), Sambalpur, Odisha, India.

[6]Department of Information Technology, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India.

Abstract

The Internet of Things (IoT) is becoming more and more popular, and both practitioners and scholars are becoming interested in it. In order to offer information and control over the condition of the items around us, the major goal of IoT is to bring everything in the world together under a single infrastructure, including things, people, places, and processes. A virtual perspective of real-world objects, both living and non-living, is made possible via the "Internet of Things." The Internet of Items (IoT) has significantly altered people's lives, and in the near future, it will have a greater influence on society and link far more things than just humans. IoT is assisting in several smart environment and application domains to address the difficulties that people and companies confront on a daily basis. No matter whether it's at home or at the business, our lives are altering drastically. This piece is focused on The design aspects that were helpful in creating the newly suggested family of lightweight block cyphers are then categorised. The lightweight block cypher family BRIGHT, as well as the super-lightweight UBRIGHT and Expanded BRIGHT for the Internet of Things, are discussed in this work. For environments with constraints, the suggested security algorithms offer a variety of block and key sizes. By supporting a variety of cryptographic systems, this allows customers to match their security demands with application requirements.

Keywords: *Algorithms, Cryptographic, IoT, Ciphers, Security and Environment.*

Number: 10.14704/nq.2022.20.9.NQ44320 **Neuro Quantology 2022; 20(9):2731-2742**

1. Introduction

We are fortunate to be alive during these dynamic, intriguing times. As technology advances, reality seems to be the norm and thinking becomes artificial. Technology is drastically altering our life, from the "Internet of Things" to neuromorphic devices [1]. Although there are many continuing new and inventive technologies, some of them are still more promising and rooted in reality than others. According to scientifically sound Gartner, only a small number of these many technologies have the potential to provide a slight advantage in the next years. The Gartner Hype Cycle for 2019 is shown in Figure.1, and it is obvious that IoT business solutions are further along the cycle and have revolutionary value. IoT is not about a single technology but rather a collection of related technical advancements that provide solutions to connect the physical and digital worlds.

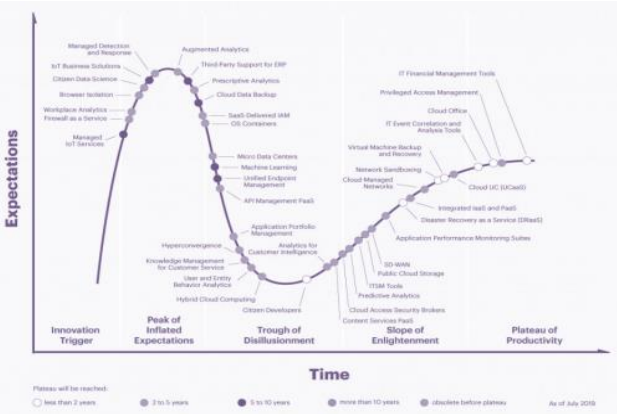


Figure.1. Gartner Hype Cycle

The wireless technologies of today are essential to our daily life. IoT uses a variety of wireless sensor technologies, including WiFi, ZigBee, RFID, actuators, and wireless sensor networks (WSNs). NFC, RFID, and 2D barcode are just a few of the tagging technologies that are used to identify real items online. The foundational elements of IoT are these wireless tagging technologies [2]. A layered architecture is the foundation of all IoT concepts. IoT architecture describes how each layer works in relation to the technology, services, and objects that surround it. Each tier has unique security concerns. IoT provides for the virtual representation and unique identification of items. IoT is assisting in several smart environment and application domains to address the difficulties that people and companies confront on a daily basis. No matter whether it's at home or at the business, our lives are altering drastically. In the not too distant future, the number of objects participating in IoT will be far bigger than the number of people participating [3]. IoT is favourably impacted by technological advancement and new business growth applications. In the Internet of Things (IoT), commonplace items are linked to a network, enabling vast applications in almost every sector, including smart cities, smart homes, smart agriculture, smart transportation, etc. Almost every element of life is being impacted by IoT, which has many uses in business, transportation, healthcare, government, and other fields. The Internet of Things (IoT) will soon be a multi-trillion dollar market thanks to the inclusion of people, things, locations, and processes [4]. IoT will have a broad range of applications in the near future for managing resources, energy, quality of service, interoperability, interfaces, security, and privacy. It is evident from a thorough literature review of IoT application domains that as websites transition from static to dynamic social networking websites, more on-demand data is created via queries. In this diverse context, data is transferred through short-range communication tools. Information security and privacy are side consequences of the development of this new technology, which increases societal efficiency. This is due to the fact that there is a lot of sensitive and private data on the network that has to be properly handled and enhanced by security measures. Among the crucial IoT topics are information security, data protection, and user privacy. Because IoT has such a broad range of applications, including smart governance, smart cities, intellectual property, and other social services, authors in [5] explore IoT security challenges at the national level. IoT security involves several duties, including setting up access control rules, safeguarding keys using hardware and software security features, integrating keying materials into device manufacture, and supplying additional features afterwards. IoT is a fairly broad word that describes the reality that most gadgets in the near future will be linked to one another rather than linking people together. IoT needs extreme data privacy and security in sensor networks where several sensor nodes are exchanging sensitive information [6]. Only a small percentage of them employ powerful CPUs and the same cryptographic techniques as standard desktop PCs. However, the majority of them use low-capability, low-power, and low-resource-utilization microcontrollers. In light of this, it is necessary to revisit and reinvent cryptographic solutions. In this respect, the study of lightweight cryptography, a relatively young area, was created to solve security concerns. Numerous resource-constrained devices, such as RFID (Radio Frequency Identification Devices) tags, sensor nodes, contactless smart cards, smart health devices, and others, utilise various communication protocols in lightweight cryptography. Because of their implementation-related constraints in terms of memory capacity, speed, power, security, and performance, it is not practical to use traditional cryptographic solutions. The creation of lightweight cyphers, particularly those that are software-oriented, is subject to several important restrictions and limitations [7]. Therefore, with devices with limited resources, certain compromises in the aforementioned parameters are necessary. Lightweight cryptography anticipates simple and quick security solutions in this age of ubiquitous computing. This section outlines tradeoffs for a lightweight encryption algorithm's design and some design considerations for lowering resource use. The research work done in this current study is carried out by taking into account the performance-improving concepts offered in this part. Simply said, this provides a foundation for creating effective lightweight cyphers for resource-constrained smart IoT environments [8]. The field of lightweight cryptography has already seen a tremendous amount of progress. Both software implementation and hardware implementation options are available for these. In comparison to hardware implementations, software-oriented encryption designs provide more flexibility at cheaper costs for manufacture and maintenance. Hardware-oriented block cyphers are vulnerable to side-channel attacks and may lose their keys even with excellent defences against mathematical assaults [9]. Low resource processors are taken into account in software implementations of lightweight cryptography, which is important since encryption in embedded systems may be performed in hardware while decryption is performed in software. Additionally, compared to hardware implementations, software-oriented encryption designs provide greater flexibility at reduced production and maintenance costs. So, in order to offer enough security guard against assaults, appropriate software design is necessary [10]. Lightweight cryptography often involves a compromise between performance and memory needs to increase an algorithm's efficiency. In this part, a novel family of ultra-lightweight block cyphers called UBRIGHT and a family of software-oriented lightweight block cyphers called BRIGHT are proposed. A variety of block and key sizes are supported by the proposed family of cyphers for IoT devices with resource limitations [11]. There are six different variations of the BRIGHT cypher, with the most common block sizes being 64 and 128 bits, respectively, and each supporting three key sizes. 96-bit and 48-bit block sizes are available in two versions of the expansion to BRIGHT called expanded BRIGHT. UBRIGHT is a 64-bit key, 32-bit block size ultra-lightweight encryption. Users may now match application requirements with their security demands thanks to this. Our goal in creating BRIGHT and UBRIGHT was to improve the encryption for Internet of Things applications.

2. Literature Survey

Now-a-days An innovative paradigm change in the field of information technology is the Internet of Things. By integrating tangible items and living creatures into the cybersphere, it is playing a crucial part in everyone's life. The Internet of Things links living things like plants, humans, and animals in addition to inanimate objects. Things are actual items that may be distinguished in our physical or material universe [12]. In an Internet of Things (IoT) context, everything is virtual and has a networked counterpart that can be located and addressed. The virtual beings are aware of their physical states and act appropriately on their own. When physical items with embedded or connected sensors interact with one another through wireless communication, it is both easy and effective. Sensitive data is included in the latest smart environment technologies. Security is seen as a crucial component in limited end nodes in order to profit from this new environment. In the event that only one node is hacked, the network may suffer greatly. With confidentiality, integrity, and authentication services, the communication in the Internet of Things must be safeguarded. The essential component of security is cryptography, and a cypher transforms plain text into cypher text and back again [13]. The cryptographic technique is often categorised as a block cypher, a stream cypher, or a hash function. However, there are several limitations on embedded devices, such as low processing power, little memory, poor connection, low energy consumption, small register widths, various operating environments, etc. Ordinary cryptographic solutions concentrate on high levels of security, but owing to resource constraints, it is difficult to properly implement a wide range of cryptographic functions on IoT-based devices. "Lightweight cryptography," a relatively recent branch of encryption, is designed for situations with little resources [14]. The effectiveness of end-to-end communications and adoptability are the key drivers behind the adoption of lightweight cryptography for low power devices. Symmetric and asymmetric key cryptography algorithms are the two primary categories. The major purposes of symmetric key cyphers, which perform well, are authentication, confidentiality, and integrity checks. Additionally, symmetric-key security algorithms are important for IoT security. However, designing such algorithms efficiently is challenging due to the necessity to avoid depleting the limited resources of ordinary IoT devices. Secure and effective communication between linked smart networked things is made possible by lightweight cryptography [15]. To have a thorough understanding of various lightweight security solutions and to grasp their varied flavours, a thorough literature review has been conducted. This aids in putting out a potential dimension for creating a solid lightweight cypher. Different researchers in this field have provided a number of software and hardware implementations of lightweight cyphers. There is discussion of a few of the available light cyphers and comparison of them. By offering lightweight cyphers as a security solution, lightweight cryptography works in a smart IoT context. Threats in the IoT will, however, exceed its advantages in the absence of solid security underpinnings. Understanding security solutions, threats, and assaults against IoT security solutions is necessary to meet this problem. Cryptanalysis is the study of cryptographic methods with the goal of exposing secret information such as key, cipher's state, and cipher/plain text. An attacker does this by using various cypher assaults. Key retrieval is the primary goal of cryptographic assaults. A key can be found, and then the encryption can be cracked. The several assaults that may be used against a cypher must be carefully considered by the encryption's creators. A good cypher is one that offers adequate defences against plausible assaults [16]. Additionally, a cypher used in lightweight cryptography must be both resource-efficient and effective at deterring realistic assaults. In such a sophisticated setting, analysis of the consequences of different assaults is also provided, along with some preventative measures. This in turn gives the current scientific effort a strong basis.

2.1 IoT Security Algorithms

In the IoT paradigm, a large number of real-world things will be connected to the internet in some way, providing a diverse environment for IoT. In such a setting, information must be encrypted in order to protect chip identification from prying eyes. With confidentiality, integrity, and authentication services, the communication in the Internet of Things must be safeguarded. Sensor node data must be kept in an encrypted format [17]. Because sensors are open to the Internet and WSN, firewalls and IDC (Intrusion Detection Systems) are also necessary in addition to data encryption. The Internet of Things (IoT) is hampered by a variety of novel elements, including the involvement of a large number of nodes, limiting processing capacity, and unique operating environments. As a consequence, it is more challenging to implement a "one size fits all" security policy. Security is mostly comprised on cryptography. Confidentiality, privacy, authentication, and integrity are its primary roles. There are several security standards available today, including DES and AES. These cyphers dissipate a lot of power and have more gates. IoT-enabled devices cannot employ these sorts of cyphers in a practical sense. Since 4-bit/8-bit processors, which are used in small-scale embedded systems, have relatively limited memory capacities, they cannot even support programmes that consume a lot of power. Eight-bit microcontrollers are a major contribution to the worldwide CPU industry [18]. These are constrained in terms of their clock speed, register width, limited arithmetic capabilities, RAM capacity, and ROM/Flash size. Due to these restrictions on IoT-enabled devices, a new subject called lightweight cryptography has emerged. For Internet of Things (IoT) applications, a number of recent lightweight cypher implementations have been developed, including PRESENT, RECTANGLE, SIMON and SPECK, TWINE, HUMMINGBIRD-2, PICCOLO, PICO, HISEC, RoadRunneR, Extended-LILIPUT, SIT, SKINNY and MANTIS, CLEFIA, KLEIN, XTEA, LED, and many others. While some of these cyphers perform better when implemented in hardware, others are better suited for software implementation. Software solutions are less expensive and provide more flexibility in production and upkeep.

2.2 Block Cipher

By performing various operations on a collection of fixed length blocks, block cyphers operate on these blocks. The block and key sizes of these cyphers are fixed. Three important operations in cryptography are encryption, decryption, and key scheduling. A plaintext is turned into ciphertext via encryption, and back into plaintext by decryption. The specified secret master key is expanded into a number of distinct keys that the encryption and decryption algorithms may employ. Up until the requisite robustness is attained, the procedures are repeatedly iterated. Every round, which is what the iterations are called, changes the state. Finally, after using all rounds, ciphertext is acquired. Block cyphers employ the processes of confusion and diffusion to encrypt data [19]. A block cypher must produce enough confusion and diffusion throughout its operations to be considered secure. The link between the encryption key and the cypher text is complicated by confusion. Every key piece is expected to have an impact on every piece of cypher text. Diffusion spreads each bit's impact from a block of plain text across a number of bits in a block of cypher text, making the cypher text too vulnerable to statistical assaults.

Substitution Permutation Network (SPN) and Feistel-based Network are two types of block cyphers. Feistel networks may also be divided into two subcategories: classical and generalised. A series of connected mathematical procedures make up SPN. Shannon recommended using two conceptually distinct functions called substitution and permutation to produce confusion and diffusion in a product cipher [20]. A round of SPN is made up of a replacement layer, a permutation layer, and key mixing. A layer of replacement and confusion is provided by a substitution function or confusion function. It is sometimes referred to as an S-box, which causes confusion and may be represented by values being mapped into a table. This layer consists of bit-slice implementation or S-box-based (Look-up-Tables based) nonlinear operations. Diffusion is provided via the permutation function known as the P-box. In Feistel networks, the encryption and decryption functions are comparable as opposed to SPN cyphers, which use separate methods for each. Horst Feistel created the Lucifer family of block cyphers in the late 1960s, which include identical encryption and decryption processes. Feistel's suggestion was to divide the cipher's state into two equal parts before performing a source branch function on either one of the halves [21]. The second half, which is referred to as the target, is then constructed from the outcome of this source branch. Up until this point, the source branch has not changed, and now the two branches have been switched. Feistel networks are relatively similar to SPNs, except in SPNs the full state is updated in each round, but in Feistel networks just half the state is modified in each round. As a result, diffusion in Feistel networks proceeds slowly and typically takes more rounds than in SPNs.

The benefits of SPN and Feistel networks are integrated in the Lai-Messey architecture. The IDEA cypher is the first to use this technique, combining the two halves of the state before feeding it to the F-function. Then, both halves of the state are given the F-output function's as a result. This quickens the cipher's level of confusion and dissemination [22]. SPN and Feistel structure were combined in a single encryption in the SIT and SFN lightweight block cyphers.

By using the essential whitening idea, the Even-Mansour scheme is provided. The block size is the same as the size of the whitening keys. The EM technique encrypts the n-bit plaintext before XORing it with an n-bit key, sending the result through a permutation function, and then XORing it once again with another n-bit key. With this sort of encryption, it is assumed that the shortened version of the cypher will be simple to crack if any key whitening (Pre or Post) or permutation is left out. Typically, a difficult to create pseudorandom function is utilised as a permutation function.

Modular addition is used in ARX (Addition-Rotation-XOR) based cyphers to provide the encryption enough non-linearity. Word-wise rotation and the XOR operator are used for diffusion. The ARX cipher's structure is here what really matters [23]. Modular addition is expensive to implement in hardware, but it is inexpensive to do in software. Therefore, this kind of block cypher is a very appropriate option for a cypher that relies on software implementation. Figure.2. compares how strategies used by researchers in various lightweight block cyphers are used against the number of publications referenced.

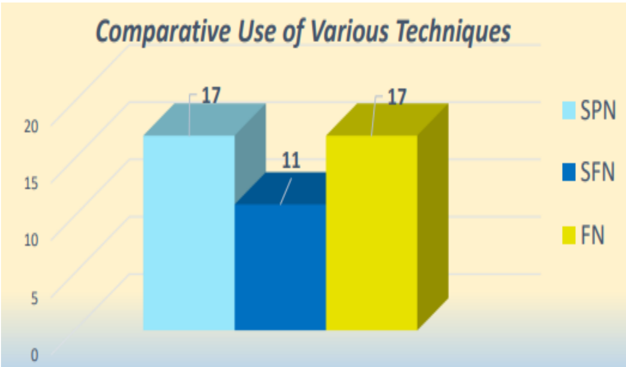
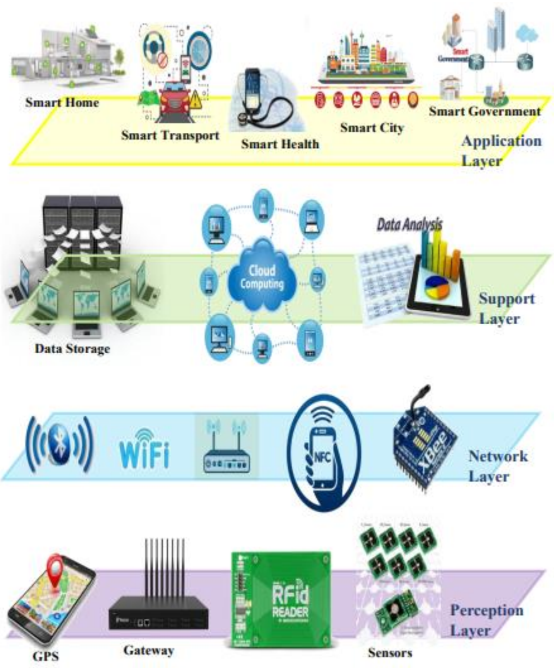


Figure .2. Comparative Use of Various Techniques in Lightweight Block Ciphers

3. IoT Concepts and its Architecture

The Internet of Things is seen as a dynamic technology revolution that represents future computers and communications in a number of fields. Internet of Things (IoT), a term that combines the terms "Internet" and "Things," is a buzzword in the modern digital sphere. The first device to be linked to the Internet by programmers was a Coke machine at Melon University in the early 1980s. The phrase "Internet of Things" was coined in 1999 by Kevin Auston, and it quickly rose to popularity. A virtual picture of real-world objects, both living and non-living, is offered through the "Internet of Things." It incorporates physical items into the cyberspace where physical objects are connected through a network to exchange data about those objects or their surroundings to which sensors are attached. By automating objects to interact in a network, IoT is significantly influencing everyone's life. IoT is not a single technology; rather, it is the confluence of a number of recent technologies that contribute to its success. IoT is enhancing our lives by putting up massive facilities all throughout. Non-living objects actively participate in the Internet of Entities (IoT), sharing information across the network in addition to communicating live things. IoT covers everything needed for global sensor network communication. The demand for storage and the stress on the network are exponentially increased by this all-inclusive approach. Among the key IoT technologies are RFID, Bluetooth, WiFi, ZigBee, Nanotechnology, sensor nodes, GPS-enabled devices, Actuators, Electronic Product Code (EPC), Internet Protocol, and Wireless Sensor Networks (WSN). RFID serves as the IoT's networking core and is the technology's foundation [24]. RFID is a wireless technology that transmits a serial number serving as an object's identify via radio waves. It is dependable, effective, secure, and reasonably priced. Every physical thing, everywhere in the world, will have a unique identification thanks to the EPC, which is intended to serve as a global identifier. On an RFID tag, a 64/98-bit code is electrically stored. IoT objects employ various technologies in various environments to create a smart environment. As a consequence, a platform-independent WSN infrastructure is needed to support the complex dynamic system that arises. This massive sensor network must be able to handle data, process information, and analyse data. A layered architecture is the foundation of all IoT concepts. Perception, Network, Session, and Application layers are the four levels that make up the IoT architecture. Each layer is outlining its own functionality with relation to other levels. Each layer is defined by the participating devices, various technologies, and services it offers [25]. The operation of each layer of the IoT architecture is directly impacted by threats to that layer. Despite the general optimism around the Internet of Things, authors in demonstrate that security vulnerabilities are ignored in crucial social services. Figure. 3 demonstrates the IoT architecture and how the four levels use the various IoT network devices for communication.



Figuer.3. IoT Architecture

The perception layer, sometimes referred to as the sensors layer, collects data from the surroundings via sensors. The perception layer uses sensors and RFID readers, which are less secure because of their low power, limited processing capability, and limited memory. Information from these participating devices is collected by sensors that are connected to them. This layer also makes use of GPS for network-based position tracing for spatial applications. The Perception layer combines IoT nodes for local and short-range communication. It keeps track of things, gathers data, analyses it, and sends it to the network layer. Threats in this layer mostly target operations involving sensor-based data collecting. The perception layer is associated with a number of security vulnerabilities. In the perception layer, RFIDs, sensors, and intelligent embedded technologies are susceptible to several assaults. Here are a few security weaknesses and potential risk reduction measures: Security concerns on authentication and secrecy of the sensor network include eavesdropping, replay attacks, spoofing, and packet alteration. Protection: Strong, dependable, efficient, and strong cryptographic systems may reduce these kinds of assaults.

Assaults known as Denial of Services (DoS) attacks aim to interfere with the sensor network's availability. Since sensor networks are separated into layers, this kind of DoS attack may affect any layer of a sensor network. Path-based DoS attack (PDoS), in which system availability is decreased and nodes' batteries are depleted, is described in a research of a similar kind by [7].

4. Proposed Model

The BRIGHT family of compact block cyphers is the proposed design. BRIGHT is a four-branch Generalized Feistel Network with very simple round functions since decryption may be carried out from encryption with little difficulty. It has a demonstrable security margin and little decryption overhead. When used in software, smaller block sizes have a low memory footprint, and keys with lengths of less than 80 bits have a limited security margin against brute-force search assaults. In light of this, the minimum key size and block size for the BRIGHT family of block cyphers, respectively, have been set at 64 bits and 80 bits, respectively. Here, the word "lightweight" refers to a security technique that should be platform-independent in addition to being adequate for a platform with certain limitations. The application-independent design choice of the proposed family of BRIGHT cyphers offers high performance across several systems. The suggested cypher offers a broad range of possibilities in the form of block sizes and key sizes due to the large variety of devices and applications. The most common block sizes are 64-bit and 128-bit, while key sizes depend on the required degree of security; for example, a relatively inexpensive device may be sufficiently secure with just 64-bits of a key, but more sensitive applications may need 256 bits of key. In order to accommodate many key sizes, including 64-bit and 128-bit blocks, we built BRIGHT. Each of the block sizes is 80, 96, 128, 192, or 256 bits, with a total of three key sizes. We first make an effort to determine the minimal number of rounds "R" necessary to execute full diffusion for each version of the BRIGHT family in order to give enough security buffer against current attacks. The suggested cypher satisfies SAC from the very first round, i.e., the BRIGHT family cyphers change around 50% of their bits in each round. The entire dispersion of all BRIGHT family cyphers takes a maximum of 8 cycles. The formula 4R is used to calculate the actual number of rounds for each version, and the next variants are added to the preceding variant by one round, such that BRIGHT 64/96 has 4R+1 rounds. As a result, the cyphers are protected against assaults. The BRIGHT family of cyphers offers a high degree of protection against related-key attacks when it comes to key scheduling. The numerous operations carried out on it, such as circular shift, XOR, and modular addition, define this map. At the conclusion of each round, a round permutation is performed, greatly enhancing confusion and dispersion. Because it is very simple to map the block cypher with visible weakness when non-linear operations of cyphers rely on the real key values, initial round key whitening is used, i.e. the key is XORed prior to its usage in round function. Figure 4 depicts the impact and operations on the single-round function Rki.

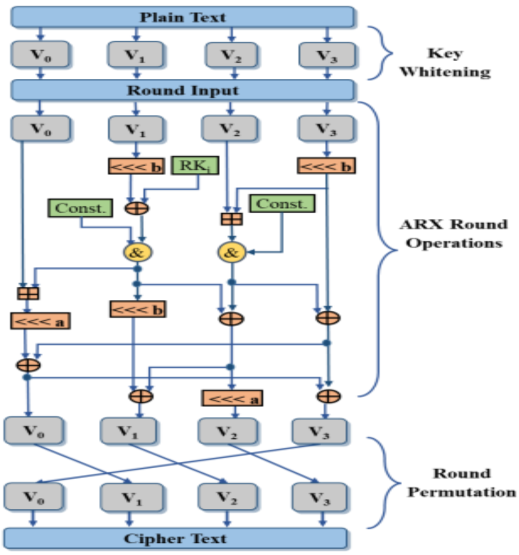


Figure.4. Structure of BRIGHT cipher

The identical round function is used for decryption, except here the round keys, operations, and constants are performed in the opposite sequence. Key whitening has been successfully used by several researchers to provide defence against different threats. Key whitening is a notion that prevents weak key assaults like SIT by XORing the real key before usage. Most analytical assaults, such as linear and differential cryptanalysis, are not prevented by key whitening. It enhances the difficulty of a brute force assault and offers defence against MITM attack. The BRIGHT family of cyphers uses a sub-key before the first round to perform key whitening. An attacker is said to be unable to anticipate input after whitening. Key whitening prevents most assaults from being extended by even one round since doing so would involve finding all of the n-keys (256-bit keys in 256-bit version). Therefore, key whitening is crucial in providing defence against certain assaults. Addition, Rotation, and XOR operations are referred to as ARX. The encryption, decryption, and key scheduling methods are effectively implemented in parallel using ARX designs, which also have highly efficient software implementations. The ARX structures used by the BRIGHT family have operations set up in a way that promotes rapid diffusion and robust resistance to intrusion. The operations the cypher does are used to characterise the cipher's above map. Four layers make up the encryption and decryption processes. These four levels are round permutation, pre key-whitening, ARX round operations, and post key-whitening. The input plain text is first divided into two words of equal length, known as branches. The first layer then receives these two words and applies pre-whitening to the keys. The output of the preceding layer is sent into the following layer as an input for further processing. For example, the two words are now sent to the second layer as a round input following the initial key whitening in the first layer, where ARX-based operations are carried out on these two words. The second and third layers' operations are carried out "R" times, where "R" is the number of rounds. Figure.5 shows the UBRIGHT suggested cipher's structural layout.

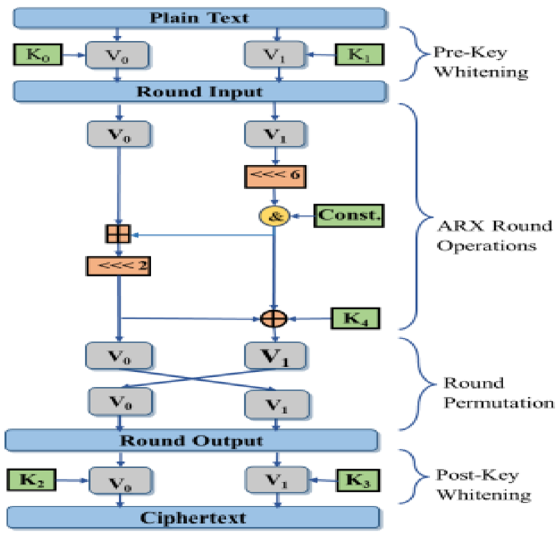


Figure.5. Layers in the UBRIGHT cipher

The proposed UBRIGHT cypher is designed with its operations in a way that shields it against the majority of attackers. Software implementation using ARX-based cyphers is more effective than using any other kind of parallel computation. The modular addition, XOR, and circular shift operations are organised in the proposed UBRIGHT cypher in an effective manner that enables the cypher to conduct quick diffusion. XOR is used in combination with addition modulo 2 n. Non-linear processes like addition modulo 2 n propagate differences indefinitely at the same rate as bitwise XOR when used in combination with other operations. So the suggested approach gains nonlinearity by addition modulo 2 n. The suggested encryption uses less rotations when rotation is taken into account. Strong diffusion layer is created in the cypher by using addition modulo 2 n and various shift amounts. Additionally, diffusion constants are also included to the suggested design to further boost the rate.

5. Results and Discussion

The majority of IoT devices communicate with other comparable devices and more sophisticated backend servers. These limitations need systems to carry out certain tasks, such as gathering data from sensors or inventories. Therefore, 64-bit CPUs should be able to handle lightweight block cyphers with good speed. Flexible safe block cyphers that work well on various systems are required. On an Intel (R) Core (TM) i5-2430M CPU running at 2.40 GHz, the proposed BRIGHT family of lightweight cyphers' implementation outcomes are shown. There are various limitations in IoT-based devices, such as low compute power, constrained memory, constrained battery usage, etc. The majority of IoT devices only have a little amount of memory accessible to them, which is a huge issue for IoT applications with restricted resources. Evaluation of the proposed BRIGHT cipher's memory use Figure.6 compares the memory use of BRIGHT family cyphers to other lightweight block cyphers based on ARX that are already in use on the same platform (64-bit processor).

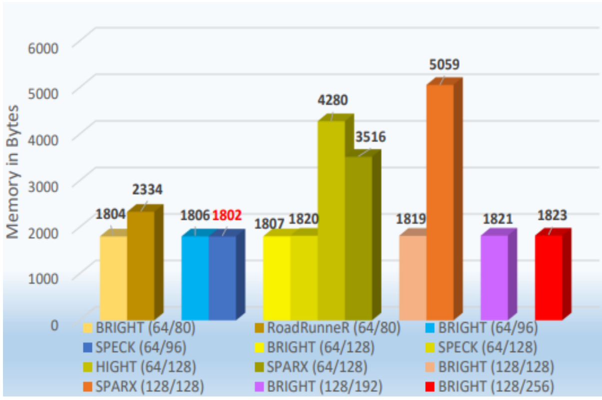


Figure.6. Memory analysis of standard ARX-block ciphers with BRIGHT family implemented on a 64-bit platform

The proposed BRIGHT family of cyphers uses less memory than existing cyphers, which is advantageous for its implementation in IoT. Additional code size reductions are feasible, but the performance is decreased. In contrast, loop unrolling may be used to increase register utilisation, speed up the operation, but at the expense of growing the memory footprint. Therefore, balanced performance may be achieved by using a loop unrolling intermediate idea. Everything relies on the requirements of a certain application. Except for the variation with block size 64 and key size 96, all variants of the BRIGHT family cyphers have the lowest memory usage in terms of flash memory. Memory use is lower for SPECK (64/96) than BRIGHT (64/96). The SPECK family has the smallest flash memory, yet SPECK lacks security proof, and several attacks are effectively used against SPECK due to its simplistic structure. Some of these assaults are differential and linear assaults.

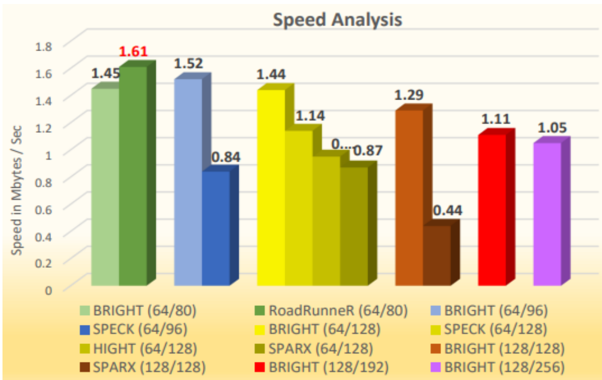


Figure.7. Speed analysis of standard ARX-block ciphers with BRIGHT family implemented on a 64-bit platform

Figure.7. to compare their parameters on the same platform are implemented in C on a 64-bit CPU. This was done to ensure that there aren't any platform-related artefacts in the BRIGHT cipher's findings or in comparisons with other cyphers. With the exception of the RoadRunneR (64/80), every variation of the BRIGHT family member exhibits faster execution times than other current lightweight ARX cyphers. The RoadRunneR cypher operates quickly thanks to on-the-fly key scheduling. Additionally, RoadRunneR's usage of basic key scheduling may result in weak key assaults. BRIGHT cipher's speed may be boosted even more, but only at the expense of more memory. In order to account for this, a speed-to-memory tradeoff was included in the architecture of the proposed BRIGHT cypher.

6. Conclusion

A lightweight cipher's simultaneous design and implementation have made certain important limitations and inherent conditions clear. The limitations provided by devices with limited resources must be taken into account when designing a security algorithm for IoT connected devices. For instance, certain lower limitations are set on the size of a block and key for various implementation contexts in order to achieve a given security level. Lightweight cryptographic techniques still have unresolved issues that need careful consideration. In this section, several design considerations and tradeoffs are discussed for reducing resource needs. The primary goal of this study is to propose concepts for achieving an effective and ideal software implementation of LBC for low-resource embedded IoT devices. In this study, alternative security models for IoT enabled devices are described based on these design concerns and countermeasures. UBRIGHT is an ultra-lightweight block cypher that supports 32-bit block size and an 80-bit key. BRIGHT is a family of lightweight block cyphers with six instances that enable block sizes of 64-bit and 128-bit. Expanded-BRIGHT cypher offers two more variations by significantly extending the BRIGHT cypher. By supporting a variety of cryptographic systems, this allows customers to match their security demands with application requirements. A solid trade-off will guarantee steady advancement toward realising and securing the IoT as intended. Various factors are used to assess how well the proposed family of lightweight cyphers performs. The proposed family cyphers outperform all currently benchmarked cyphers except for RoadRunneR (64/80) on 64-bit platforms, however on 32-bit platforms, the suggested cyphers outperform all comparable LBCs in terms of execution time and cost. With the exception of the variation with a 64-bit block size and 96-bit key size, all of the proposed family cypher variants have the lowest memory usage in terms of flash memory.

References

1. Al-Dabbagh, S. S. M., Al Shaikhli, I. F. T., Al-Enezi, K. A., & Alyaqoup, M. J. (2015, December). Enhancing Lightweight Block Cipher Algorithm OLBCA through Decreasing Cost Factor. In 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT) (pp. 159-164).
2. Ankele, R., Banik, S., Chakraborti, A., List, E., Mendel, F., Sim, S. M., & Wang, G. (2017, July). Related-key impossible-differential attack on reduced-round S kinny. In International Conference on Applied Cryptography and Network Security (pp. 208-228).
3. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., & Tokita, T. (2000, August). Camellia: A 128-bit block cipher suitable for multiple platforms—design andanalysis. In International Workshop on Selected Areas in Cryptography (pp. 39-56).
4. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., & Regazzoni, F. (2015, November). Midori: A block cipher for low energy. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 411-436).
5. Basha, S. N., Jilani, S. A. K., & Arun, M. S. (2016). An intelligent door system using Raspberry Pi and Amazon web services I0T. International Journal of Engineering Trends and Technology (IJETT), 33(2), 84-89.
6. Bellare, M., & Kohno, T. (2003, May). A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In

International Conference on the Theory and Applications of Cryptographic Techniques (pp. 491-506). Springer, Berlin, Heidelberg.

7. Biham, E., Anderson, R., & Knudsen, L. (1998, March). Serpent: A new block cipher proposal. In International workshop on fast software encryption (pp. 222-238). Springer, Berlin, Heidelberg.
8. Biryukov, A., Velichkov, V., & Le Corre, Y. (2016a, March). Automatic search for the best trails in ARX: application to block cipher speck. In International Conference on Fast Software Encryption, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), 9783(2008), 289- 310.
9. Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., & Verbauwhede, I. (2012). Spongent: The design space of lightweight cryptographic hashing. IEEE Transactions on Computers, 62(10), 2041-2053.
10. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., Leander, G., Nikov, V., Paar, C., Rechberger, C. & Rombouts, P. (2012, December). PRINCE–a low-latency block cipher for pervasive computing applications. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 208-225).
11. Cazorla, M., Marquet, K., & Minier, M. (2013, July). Survey and benchmark of lightweight block ciphers for wireless sensor networks. In 2013 International Conference on Security and Cryptography (SECRYPT) (pp. 1-6). IEEE.
12. Diehl, W., Farahmand, F., Yalla, P., Kaps, J. P., & Gaj, K. (2017, September). Comparison of hardware and software implementations of selected lightweight block ciphers. In 2017 27th International Conference on Field Programmable Logic and Applications (FPL) (pp. 1-4). IEEE.
13. Dinur, I. (2014, August). Improved differential cryptanalysis of round-reduced speck. In International Conference on Selected Areas in Cryptography (pp. 147-164). Springer, Cham.
14. Dutta, I. K., Ghosh, B., & Bayoumi, M. (2019, January). Lightweight Cryptography for Internet of Insecure Things: A Survey. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0475-0481). IEEE.
15. Eun, H., Lee, H., & Oh, H. (2013). Conditional privacy preserving security protocol for NFC applications. IEEE Transactions on Consumer Electronics, 59(1), 153- 160.
16. Friansa, K., Haq, I. N., Santi, B. M., Kurniadi, D., Leksono, E., & Yuliarto, B. (2017). Development of battery monitoring system in smart microgrid based on internet of things (IoT). Procedia engineering, 170, 482-487.
17. Gong, Z., Nikova, S., & Law, Y. W. (2011, June). KLEIN: a new family of lightweight block ciphers. In International Workshop on Radio Frequency Identification: Security and Privacy Issues, Lecture Notes in Computer Science, 7055, 1-18.
18. Gupta, N., Saeed, H., Jha, S., Chahande, M., & Pandey, S. (2017, May). Study and implementation of IoT based smart healthcare system. In 2017 International Conference on Trends in Electronics and Informatics (ICEI) (pp. 541-546).
19. Hao, Y., Bai, D., & Li, L. (2015, November). A meet-in-the-middle attack on roundreduced mCrypton using the differential enumeration technique. In International Conference on Network and System Security (pp. 166-183). Springer, Cham.
20. Istepanian, R. S., Hu, S., Philip, N. Y., & Sungoor, A. (2011, August). The potential of Internet of m-health Things “m-IoT” for non-invasive glucose level sensing. In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (pp. 5264-5266). IEEE.
21. Jeong, K., Kang, H., Lee, C., Sung, J., Hong, S., & Lim, J. I. (2015). Weakness of lightweight block ciphers mCrypton and LED against biclique cryptanalysis. Peer-to-Peer Networking and Applications, 8(4), 716-732.
22. Joshitta, R. S. M., & Arockiam, L. (2018, November). A novel block cipher for enhancing data security in healthcare internet of things. In Journal of Physics: Conference Series (Vol. 1142, No. 1, p. 012002). IOP Publishing.
23. Lim, C. H., & Korkishko, T. (2005, August). mCrypton–a lightweight block cipher for security of low-cost RFID tags and sensors.

In International Workshop on Information Security Applications (pp. 243-258). Springer, Berlin, Heidelberg.

24. McDonald, C., Charnes, C., & Pieprzyk, J. (2008). An algebraic analysis of Trivium ciphers based on the boolean satisfiability problem. In Proceedings of the 4th International Workshop on Boolean Functions: Cryptography and Applications (pp. 173-184).

25. Ojha, S. K., Kumar, N., & Jain, K. (2009, December). TWIS–a lightweight block cipher. In International Conference on Information Systems Security (vol. 5905, pp. 280-291). Springer, Berlin, Heidelberg.