JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

Lightweight secure Approach for IOT Devices

Rana Fadhel Atiyah[1], Intisar Al-Mejibli[2]

[1] Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers & Informatics, Iraq, Baghdad, email: ms202010602@iips.icci.edu.iq

[2] Biomedical informatics college,University of Information Technology and Communications, Iraq, Baghdad, email: dr.intisar.almejibli@gmail.com

Received: 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10

Abstract

IoT devices are applied extensively in wide range of applications in various fields such as healthcare, military and agriculture. The data are collected by these devices from real environment and transfer it over the networks to the proper destination. Deploying IoT devices in a real-environmentfaces many challenges. Security is one of the seriousissuesin transmitted information. Due to reasons such as increasing component utilization, longer computation times, higher power consumption, and a greater need for memory, lightweight cryptography is necessary for IoT devices. In this paper presents lightweight secure approach for IoT devices. we describe Speck-U, a novel extremely lightweight cryptographic algorithm based on Speck and ECC to increase its security and then uses hash approach to increase its privacy and authentication. The results of testing the proposal demonstrate that it passes all of the NIST(15) tests.

Keywords : IOT, lightweight, cryptography, Speck , ECC , Hash function

1. Introduction

The Internet of Things has become a prominent topic of conversation across numerous industries (including medical, academia, and industry) and is frequently described in a variety of ways. In general, it refers to an infrastructure comprised of various computing devices that are nonetheless able to communicate with one another despite their vast differences. Internet users are able to communicate with one another, with people in general, and with other services without human assistance [1,2]. The European Technology Platform on Smart Systems Integration (EPoSS) defines the Internet of Things (IoT) as a global network of uniquely accessible networked objects utilizing standard communication protocols[3]. Online, "things" are referred to as "things" when they function as devices that link physical and digital language [4].

Typically, these things feature embedded devices positioned in numerous areas for varied reasons. It is possible to install them in hospitals, institutions, enterprises, and even homes. The devices comprising the Internet of Things include RFID tags, wireless sensors, actuators, etc. However, the majority of the aforementioned IoT devices have a variety of constraints. Low-resource devices have restricted processing speed, memory, battery life, and computer power. Therefore, it is essential to pay strict attention to such equipment, particularly for data processing. The exchange of vast quantities of data between all nodes of wireless networks will pose new threats and impediments. A limited quantity of resources (such as energy) is one of the situations that ultimately lead to financial constraints. However, the amount of resources committed to security is insignificant; it constitutes only a small portion of the overall available resources. Due to the low cost of these devices, security

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

The implemented comparisons between the proposal and other ciphers reveal that Speck functions effectively on hardware systems with limited resources on both 8-bit and 16-bit platforms. The results of implementation show that proposal is one of the most efficient ciphers in terms of energy usage and throughput. This encryption is also one of the most effective software-based ciphers among more than 50 tested methods.

3. Main Contribution

This research proposes Speck-U, a new ultra-lightweight reduction cipher based on Speckencryption algorithm. Speck is a well-known lightweight ARX (Addition/Rotation/XOR) encryption created in 2013 by the United States National Security Agency (NSA). It tries to provide security for low-resource devices. Additionally, it is recognized for its speed of execution, its security, and its ease of use. Speck-U is a hybrid cipher with roughly the same characteristics as Speck, but with the addition of "Dynamicity", which helps to defend against differential and linear attacks that previously succeeded against lower versions of Speck. A dynamic key-substitution layer was added to the structure of the original Speck in Speck-U. Consequently, Speck-U has fewer rounds than Speck. The key objective here is to reduce the execution time of Speck in the new version Speck-U while keeping a high level of security. The newly proposed encryption ensures (a) the robust secrecy of transmitted data content to protect it from attacks, and (b) a quick execution speed to suit the complicated requirements of modern devices. Extensive security testing has proven that Speck-U meets all requirements for a good lightweight cipher candidate.

4. SpeckEncryption Algorithm

SPECK is an ARX (Add, Rotate, Xor) architecture. The speck has been intended to deliver high performance in both hardware and software, but software performance has issues have begun to emerge. Researchers began to think differently, resulting in improvements to both the network and application layers [5]. The communicated data should be encrypted to provide security, confidentiality, and resistance to a variety of attacks. However, standard encryption technologies are inadequate and wasteful in such demanding conditions. Therefore, it was suggested that lightweight cryptography be utilized to meet the requirements of such constrained hardware. Numerous studies have concentrated on the creation of efficient, lightweight data-encryption techniques[6]. Nevertheless, lightweight cryptography must utilize fewer resources and eliminate any computational overhead generated by the encryption and decryption process. Numerous papers have been published in an effort to clarify and classify lightweight cryptography. The authors of [7] differentiate between (1) lightweight cryptography, (2) ultra-lightweight cryptography, and (3) Internet of Things (IoT) cryptography.

2. Methodology

Encryption techniques can be applied in two approaches symmetric and asymmetric. In practical implementations, the symmetric-key method is preferred since it involves less computational complexity in terms of memory usage and resources. symmetric ciphers have two types which are stream ciphers and block ciphers[8]. Devices with limited hardware capabilities are unable to applying these algorithms smoothly and may beimpact the entire system [9]. The main purpose of this research is to develop a new lightweight encryption method that can overcome these issues.The Speck encryption algorithm possesses all the necessary parameters for a lightweight cipher, thus it considered to enhancing its performance[10].

This research proposes Speck-U algorithm. It provideshigh level of security to the transmitted data between Internet of Things (IoT) deviceswith little computing overhead.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

key size. The use of these curves for encryption was independently proposed by IBM and first introduced by Neil Koblitz of the University of Washington and Victor Miller in 1985. Since 2005, they have been widely used, utilizing an algebraic structure of elliptic curveson essentially limited fields and an approach to encryption based on the public Key. ECC equations based on elliptic curves offer a beneficial property for cryptography: they are reasonably straightforward to solve[13].

Certicom has invented the ECC algorithm, and it is now licensed by Hifn, a producer of integrated circuits and network security solutions for integrated circuits. Certicom is a supplier of the security component of e-commerce on software loaded on mobile devices (ICs). Any communication is encrypted using ECC as coordinates on plane curves. These curves are based on cubic curve equations, and the following formula is used for elliptic curves:

$$y^2 = x^3 + ax + b\ (mod)\ p \text{.....(2.1) [13]}$$

Key exchange, encryption, and digital signature are all parts of the ECC algorithm. It is a public-key encryption method based on the theory of elliptic curves that can be used to make cryptographic keys faster, smaller, and better. ECC helps to set up the same level of security while using less computing power and battery resources. It is being used extensivelyin mobile apps[14].

The elliptic curve and the locations thattraverses contain some crucial information, such as the mathematical definition of an ellipse curve, an estimate of (a and b), Prime (y), and the shape of the elliptical curve that was derived from the curve's equation, which is as follows: $y^2 = x^3 + ax + b\ (mod)\ p$. Where (a) and (b) are the coefficients that produce the various elliptic curve points (x, y), and p is a huge prime integer [15]. as show in figure 2.

been optimized for more efficiency. SPECK has a notation similar to SIMON[11][12]. The SPECK 2n encryption maps utilize the subsequent operations on n-bit words:

- Bitwise XOR
- Modular Addition
- Left and right circular shift

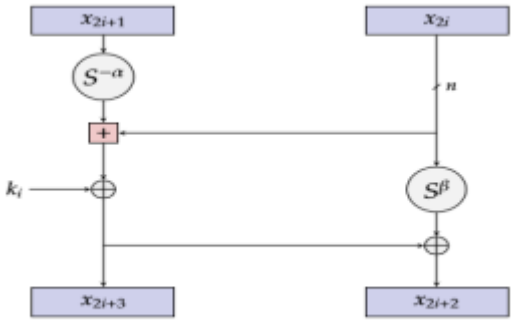

Fig1. Speck round function

The encryption round features of SPECK light-weight block cipher comprises of bitwise XOR operation, addition modulo 2 operations, left and right circular shift operation. In case of round key, it can be enlarged by key schedules. The round function will operate round number (T) time according to SPECK block cipher parameters. The key dependent SPECK 2n round function is map Rk:

$$Rk(x,y) = ((S^{-\alpha}\ x + y) \oplus k,\ S^{\beta}\ y \oplus (S^{-\alpha}\ x + y) \oplus k)$$

Where α=8 and β=3 and the reverse structure of the round function necessary for decryption.

5. Elliptic Curve Cryptography algorithm (ECC)

An asymmetric algorithm relies on trapdoor functionality, is regarded as one of the most secure algorithms, and does not require a large number of mathematical operations. Moreover, the key size is quite small in comparison to other algorithms, for example, a 112-bit key is equivalent to RSA's 512-bit

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

A hash function is one of the most essential algorithms for authenticating messages between sender and receiver. The SHA hash function was invented in 1995[16], theNational Institute of Standards and Technology(NIST) version is SHA-1 also known as SHA-160, the new versions are SHA-512, SHA-384, and SHA-256 also known as SHA-2, and they were released in 2002. In 2002, this corporation added SHA-224 as a new version. The table (1) provides a summary of hash functions. All prior hash algorithms utilized the same mathematical and logical procedures due to the identical structure of their versions [17], [18].

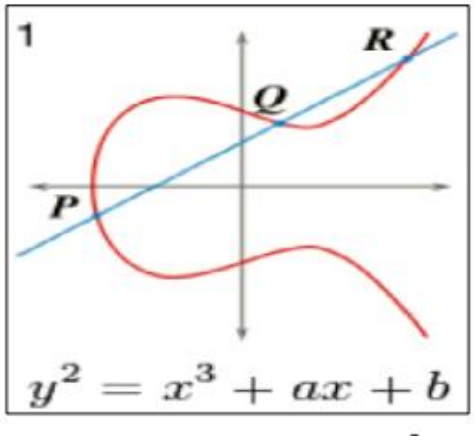

Fig.2: Elliptical curve with points defined as $y^2 = x^3 + ax + b$[15]

6. Secure Hash Algorithm (SHA)

Table (1): Standard Hash Functions [19]

Name	Block size (bits)	Word size (bits)	Output size (bits)	Round	Year of standard
SHA-0	512	32	160	80	1993
SHA-1	512	32	160	80	1995
SHA-224	512	32	224	64	2004
SHA-256	512	32	256	64	2002
SHA-384	1024	64	384	80	2002
SHA-512	1204	64	512	80	2002

Five algorithms, BLAKE, Grstl, JH, Keccak, and Skein, satisfied all of the NIST-specified SHA-3 requirements. High security, variety, analysis, and performance were the most notable of these requirements. In addition, NIST stipulated that the function chosen as the SHA-3 standard must be an open-source hash algorithm, available for public use globally, and compatible with a broad variety of software and hardware systems [19].

In addition, the winning SHA-3 algorithm had to support a message hash length of 224, 256, 384, and 512 bits, in addition to, a message length of at least (2^64 -1) bits. The NIST

6.1 SHA-3

One of its names is Keccak, which operates in a single direction with the purpose of generating digital outputs with a length of 32 bits (224, 256, 384 or 512 bits). Developed in 2008 by a team of writers lead by Yoan Dimen and accepted as the new FIPS standard in 2015. The method functions by combining the "coded sponge" with the pressure of the selected volume. The approach operates by combining 'cryptographic sponge' with volume compression [19].

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

(Addition/Rotation/XOR) is a collection of cryptographic methods employing three elementary arithmetic operations: modular addition, bitwise rotation, and exclusive-OR. Speck is derived from ARX. In recent years, the ARX cipher has attracted a great deal of attention and interest from both industry and academia. Utilizing a combination of linear (XOR, bit shift, bit rotation) and non-linear (modular addition) operations and repeatedly iterating them has rendered ARX algorithms increasingly resistant to differential and linear cryptanalysis. In this proposal, we intend to implement a dynamic substitution layer that enhances the cipher's security while preserving its ultra-lightweight characteristics. The proposed cipher avoids using a static diffusion operation, such as the MixColumn transformation of AES [21] or the key-dependent integer/binary diffusion operations of [22], [23], because these methods consume a considerable amount of execution time [23], [24]. Additionally, Speck-U is implemented in Electronic Code Book (ECB) mode, allowing it to be encrypted or decrypted in concurrently.

- **Flexibility:**It functions at the block level, which allows configurable number of bits, similar to the original Speck. This block size is customizable dependent on network capability and user preferences. The suggested method takes into account the block size utilized by lightweight ciphers and is adapted to the particularities of the devices.
- **Simple hardware and software implementations:** As stated previously, ARX ciphers are simple to use and are highly recommended for small, limited

defined additional qualities to be assessed for the new SHA-3 option, including simplicity, flexibility, computational efficiency, memory use, and licensing requirements. In October 2012, NIST declared the winner of the SHA-3 competition. Keccak was chosen as the new SHA-3 standard out of the five great algorithms that made it to Round 3.

6.2 Message authentication code based on hash (HMAC)

HMAC SHA3 is a safe encryption message based on hash functions and the shared key authentication protocol with a secure exchange mechanism; it prevents data from being intercepted and altered during the transmission process. It is a form of cryptographic hashing method utilized by the hash function of SHA-512 and as a Hash-based Message Authentication Code to protect the integrity, veracity, and security of data; it is also used as a Hash-based Message Authentication Code (HMAC). The HMAC technique combines the message data with a secret key and determines the result using the secret key. The hash value is then recombined and hashed a second time with 512-bit output [19].

7. The Proposed Approach of Speck-U

Before digging into previous versions of Speck, the goals of the enhanced version are described. This technique will be referred to as Speck-U, where "U" stands for "Ultra." Speck-two U's key contributions compared to Speck are increased efficiency and security. The desired system performance and security performance are described below.

7.1 System Performance:

- **Lightweight:**Modern lightweight cryptographic methods, such as the Hummingbird2 cipher, require a minimum of four repetitions [20]. Minimum rounds required for Speck are 22. ARX

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

features, is directly dependent on the underlying curve.

- **Dynamic key approach:**Speck has already proved that the dynamic key technique is a secure cipher with a secure key. The number of rounds experienced by the cipher influences the dynamic substitution layer that is applied to the encryption. The substitution layer is dynamic, therefore it is generated based on a previously chosen key. In contrast to previous cipher solutions, the suggested method utilizes a dynamic key that fluctuates in a pseudo-random fashion with each new session. The primary purpose of this suggestion is to make the session's repeat interval dependent on application or user requirements.

8. The Proposed Speck-U

In this study Speck-U is proposed which based on Speck method (128bit). It obtains its own private key from the ECC algorithm, which has a curve (curve secp192r1) rather than the previous method, and it uses only the first 128 bits of the ECC key. Figure 3 shows the block diagram of the proposal. The Speck-U algorithm was used for data encryption to achieve the primary goal of securing the sender's data. The HMAC-SHA3 hash function was utilized to authenticate the data also the SHA-3 uses the private key generated from ECC.

devices, particularly IoT devices. This makes the associated hardware and software easy to use and effective.

- **Low error propagation:** This proposal ensures low error propagation by treating each block independently. The block is divided into two semi-blocks. It will not affect complete image blocks, nor will the issue spread over the full data. Speck-U is designed to operate in ECB mode, preventing processes from chaining and propagating mistakes throughout the system. Consequently, there is minimal assurance of error propagation.
- **Large key space:**Since different versions of the original Speck employ different key sizes, the key might range from 64 to 256 bits. Speck-U is therefore impervious to brute-force attacks according to [25], as it adheres to the same constraints as Speck[25].

These changes to the cipher reduce the duration of the encryption and decryption processes and simplify their corresponding hardware implementations. Each primitive in this proposal has its own effect on the security and efficiency of the proposed cipher scheme.

7.2 Security Performance:

- **Key dependent approach:** Speck-U is based on a key-dependent method that, in addition to the requisite cryptographic

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

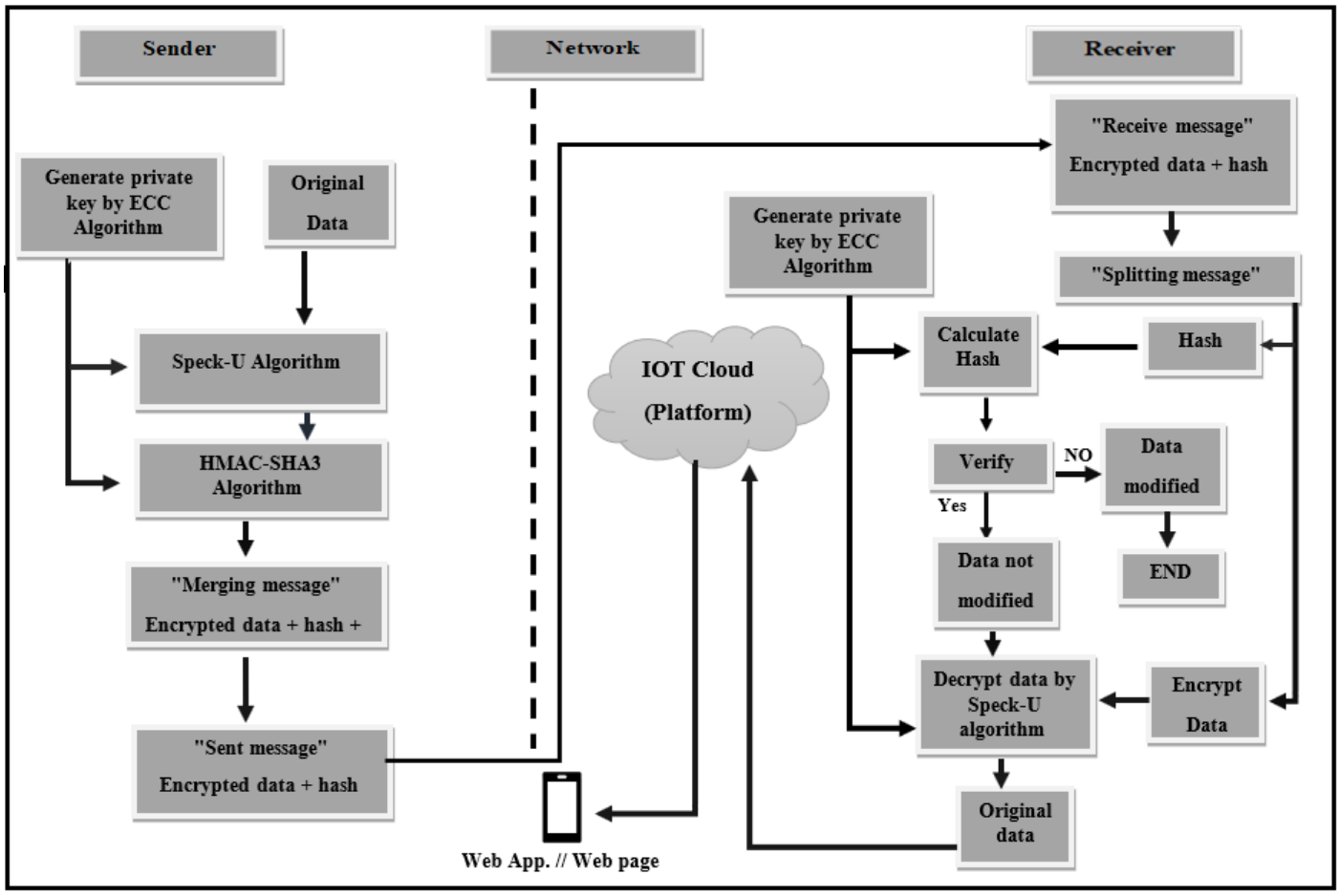

Figure 3: Block diagram of secure algorithm method to sent / receive data

However, some tools which are usually used to prove the randomness of pseudo-random generators are not used to prove the randomness of the output by the cipher.To determine the cipher's strength ofthe proposed system, the NIST test has been applied. All of the statistical tests performed by the NIST team, which are displayed in Table 2, demonstrate the strength of the created cipher. It passed 15 of 15 examinations. Figure 4 displays the results of the random number test

The implemented method was created and constructed utilizing lightweight algorithms to ensure privacy, security, and integrity, in addition to flexibility and ease of use for authentication, authorization, and access control.

9. Discussion

Randomness is crucial for demonstrating the security of a cryptographic technique.

Table .2 The result of the NIST Test to prove strength cipher data

Test No.	Test	P-average	Result
Test1	Mono bit	0.49918759924281636	Pass
Test2	Frequencywithinblock	0.49864254251590695	Pass
Test3	Runs	0.497010077544853	Pass
Test4	longest_run_ones_in_a_block	0.49617366820330094	Pass

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

Test5	binary_matrix_rank	0.46101091994034715	Pass
Test6	DFT(Desecrate_Fourier_transform)	0.48107608360466547	Pass
Test7	non_overlapping_template_matching	0.446474028731358	Pass
Test8	overlapping_template_matching	0.01910370820175894	Pass
Test9	maurers_universal	0.9994445235628637	Pass
Test10	linear_complexity	0.3732492388570004	Pass
Test11	serial	0.49916029026647596	Pass
Test12	approximate_entropy	0.4975798225016702	Pass
Test13	cumulative_sums	0.5166452154212637	Pass
Test14	random_excursion	0.2546215026664759	Pass
Test15	random_excursion_varian	0.6685691650949235	Pass
The final result of the test		**15/15 pass**	

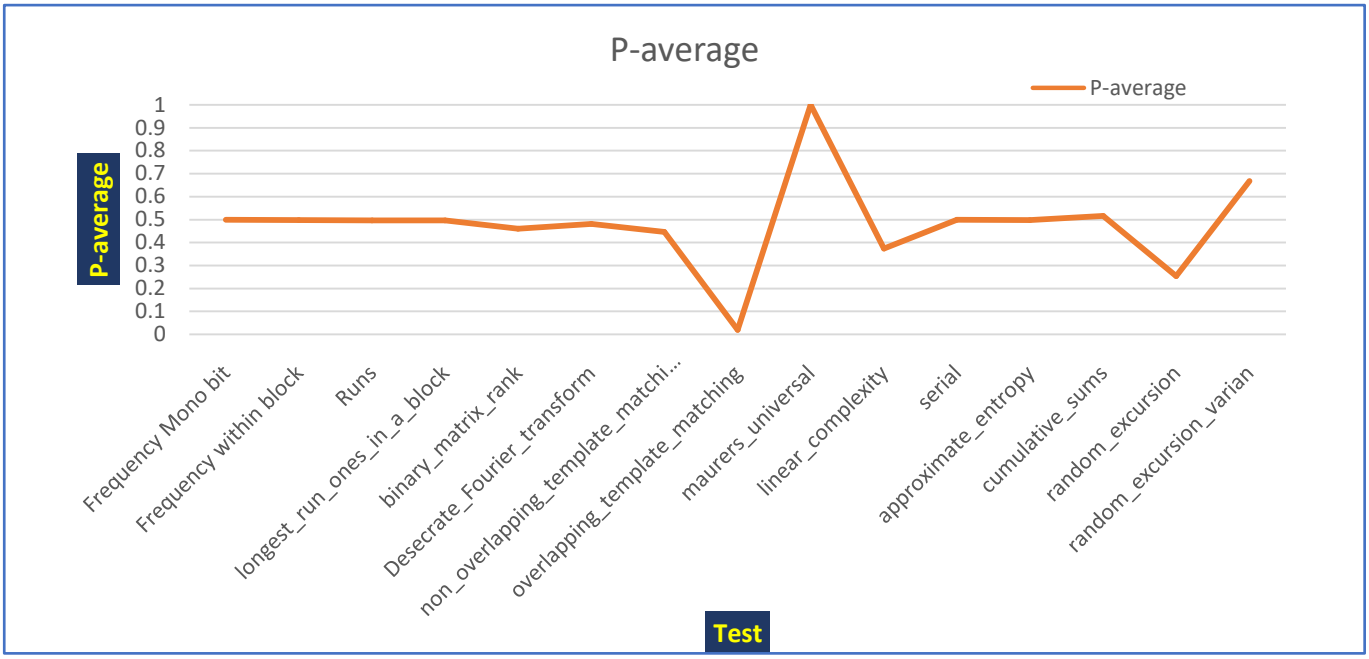

Figure 4 Random number test value of encryption data

10. Conclusion

This study proposed lightweight secure approach appropriate for IoT devices that featured with limited resource. The proposed approach based on implementing new version of Speck algorithm and applying SHA-3algorithm. Used Speck-U algorithm is depending on traditional Speck algorithm with ECC algorithm to obtain the key. The proposed Speck-U algorithm achieved security and SHA-3algorithm achieved integrity of the transmitted data.On the basis of test results and evaluations of the proposed system, the indicated objectives have been attained. The implementation of suggested system achieved the protection and integrity of sent and received data. In cryptography, it is believed that the proposed method of merging the ECC and Speck algorithms is superior, more efficient, and faster than existing methods such as DES and RSA. The success of randomization tests indicates the complexity of key generation. Using a 256-bit key with ECC gives excellent security and makes it difficult to break, even with modern CPUs. The execution time of

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

the ECC algorithm was successfully reduced by producing only its private Key and disabling its public Key. Using the (HMAC-SHA3) technique, the integrity of the data was ensured.

References

[1] Pouya Kamalinejad, Chinmaya Mahapatra, Zhengguo Sheng, Shahriar Mirabbasi, Victor CM Leung, and Yong Liang Guan. "Wireless energy harvesting for the internet of things. IEEE Communications Magazine", 53(6):102–108, 2015.
[2] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park."Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions". Journal of Ambient Intelligence and Humanized Computing, pages 1–18, 2017
[3] DG INFSO et al. "Internet of things in 2020: Roadmap for the future. INFSO D, 4, 2008.
[4] Alex S Weddell and Michele Magno. "Energy harvesting for smart city applications. In 2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM) ", pages 111–117. IEEE, 2018
[5] Zhaogang Shu, Jiafu Wan, Di Li, Jiaxiang Lin, Athanasios V Vasilakos, and Muhammad Imran. "Security in software defined networking: Threats and countermeasures. Mobile Networks and Applications", 21(5):764–776, 2016.
[6] NSA. Lightweight cryptography, 2019. [Online; 2019]
[7] Alex Biryukov and Léo Paul Perrin. State of the art in lightweight symmetriccryptography. 2017.
[8] Joan Daemen and Vincent Rijmen. The design of Rijndael, volume 2. Springer, 2002.
[9] Kerry McKay, Larry Bassham, Meltem Sönmez Turan, and Nicky Mouha. Report on lightweight cryptography (nistir8114). National Institute of Standards and Technology (NIST), 2017.2
[10] George Hatzivasilis, Konstantinos Fysarakis, Ioannis Papaefstathiou, and Charalampos Manifavas. "A review of lightweight block ciphers. Journal of Cryptographic Engineering", 8(2):141–184, 2018.
[11] Ray Beaulieu, Douglas Shors , Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers, "The Simon and Speck of lightweight block ciphers," National Security Agency 9800 Savage Road, Fort Meade, MD 20755, USA, JUNE 2013.
[12] C. D. Cannière, O. Dunkelman and M. Kneževi´c, "KATAN and KTANTAN - A Family of Small and Efficient HardwareOriented Block Ciphers,"Springer-Verlag, 2009 [In CHES 2009, the Lecture Notes in Computer Science No. 5747, pages 272–88.
[13] R. Sridevi, "10-2016 E-Health Security using ECC algorithm.pdf," vol. 2, no. 19, pp. 114–117, 2016.
[14] K. Bae, S. Moon, D. Choi, Y. Choi, H. D. Kim, and J. Ha, "A practical analysis of fault attack countermeasure on AES using data masking," Proc. - 2012 7th Int. Conf. Comput. Converg. Technol. (ICCIT, ICEI ICACT), ICCCT 2012, no. September 2016, pp. 508–513, 2012.
[15] A. Al-Mamun, S. S. M. Rahman, T. A. Shaon, and M. A. Hossain, "Security analysis of AES and enhancing its security by modifying sbox with an additional byte," Int. J. Comput. Networks Commun., vol. 9, no. 2, pp. 69–88, 2017, doi: 10.5121/ijcnc.2017.9206
[16] C. Paar and J. Pelzl, "SHA-3 and The Hash Function Keccak,"Underst. Cryptogr. — A Textb. Students Pract., 2010, [Online].Available: http://www.crypto-textbook.com/.S. P. Godse and P. N.Mahalle, "A Computational Analysis of ECC Based Novel.

Volume 13, No. 3, 2022, p. 4069-4078
https://publishoa.com
ISSN: 1309-3452

[17] S. Bressan *et al.*, *Cryptographic Hardware and Embedded Systems -CHES 2007*, vol. 3671. 2005
[18] [18] W. Stallings, *Cryptography*. *Computer Security Princuplew andPractices*.2004.
[19] A. K. Sharma and S. K. Mittal, "Comparative analysis ofcryptographic hash functions," vol. 4, no. September, pp. 2013–2016,2018, [Online]. Available:https://www.researchgate.net/publication/327664102_COMPARATIV E_ANALYSIS_OF_CRYPTOGRAPHIC_HASH_FUNCTIONS
[20] Daniel Engels, Markku-Juhani O Saarinen, Peter Schweitzer, and Eric M Smith. The hummingbird-2 lightweight authenticated encryption algorithm. In International Workshop on Radio Frequency Identification: Security and Privacy Issues, pages 19–31. Springer, 2011
[21] Joan Daemen and Vincent Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.
[22] Zeinab Fawaz, Hassan Noura, and Ahmed Mostefaoui. An efficient and secure cipher scheme for images confidentiality preservation. Signal Processing: Image Communication, 42:90–108, 2016.
[23] Hassan Noura, Lama Sleem, Mohamad Noura, Mohammad M Mansour, Ali Chehab, and Raphaël Couturier. A new efficient lightweight and secure image cipher scheme. Multimedia Tools and Applications, 77(12):15457–15484, 2018.
[24] Salim Muhsin Wadi and Nasharuddin Zainal. High definition image encryption algorithm based on aes modification. Wireless personal communications, 79(2):811–829, 2014.
[25] Xingyuan Wang, Lin Teng, and Xue Qin. A novel colour image encryption algorithm based on chaos. Signal Processing, 92(4):1101–1108, 2012.