https://doi.org/10.29042/2020-10-3-12-18

Helix (2020) 10 (3): 12-18

S-Box Implementation for Security Algorithms in IOT

*[1]Ashok Kumar K, [2]V. Karunakar Reddy, [3]K. Shravan Kumar

[1,2,3] Department of ECE, Matrusri Engineering College, Saidabad, Hyderabad, India

Email: kashok483@gmail.com, karuna0203@gmail.com, shravank1412@gmail.com

Received: 06th April 2020, Accepted: 05th May 2020, Published: 30th June 2020

Abstract

Internet of Things (IoT) is dominant technology for real time applications because it is integrated with various sensors, software and hardware. Security is the primary concern for IoT because of many ways of threats from different components. Typical encryption algorithms have less complexity and easy to decrypt thereby requiring high complexity security algorithm. The improved security algorithm must be less in size and power hence compatible to IoT based applications. This paper is used an Elliptic Curve Cryptography (ECC) to generate Substitution box (S-box) hence proposing 128-bit block cipher based on feistel network.

Keywords

IoT, Security, S-box, ECC, Cloud Computing.

Introduction

IoT is one of popular technology in recent years because of internetworking of various infrastructures that are physical devices and software. IoT is compulsory to society at present because of utensils converting into smart systems like smart farming, healthcare and so on. Typically, IoT based systems are collected and exchanged the data directly or indirectly by the server to target device. The purpose of achieving particular goals to provide rapid evolution of communication thereby proposing IoT based applications like smart factories, smart farming and intelligent transport system. As per mobility report-2017 given by Ericsson Company that approximately 18 billion devices are used IoT technology by 2022 hence analyzing importance of IoT technology [1]. The general wireless communication protocols like Bluetooth, Zigbee, Ethernet, Wi-Fi and 4-G are majorly used for transferring data in IoT devices. However, power consumption, reliability, long communication and security are primary aspects for IoT to obtain reliable communication between transmitter and receiver. Narrow band IoT (NB-IoT) of LTE is presented to obtain high throughput, low power consumption and high battery life because it is provided services form access to network through physical layer [2]. To address the requirements of IoT, NB-IoT architecture is simplified from evolved packet core structure. The NB-IoT is introduced many changes for medium access control to reduce power consumption thereby making the scheduling simple and flexible. HARQ is used for removing scheduling assignments hence reducing number of control bits to enhance robustness and efficiency. A light weight encryption system is popular used for IoT implementation because of bit permutation group operation [3].

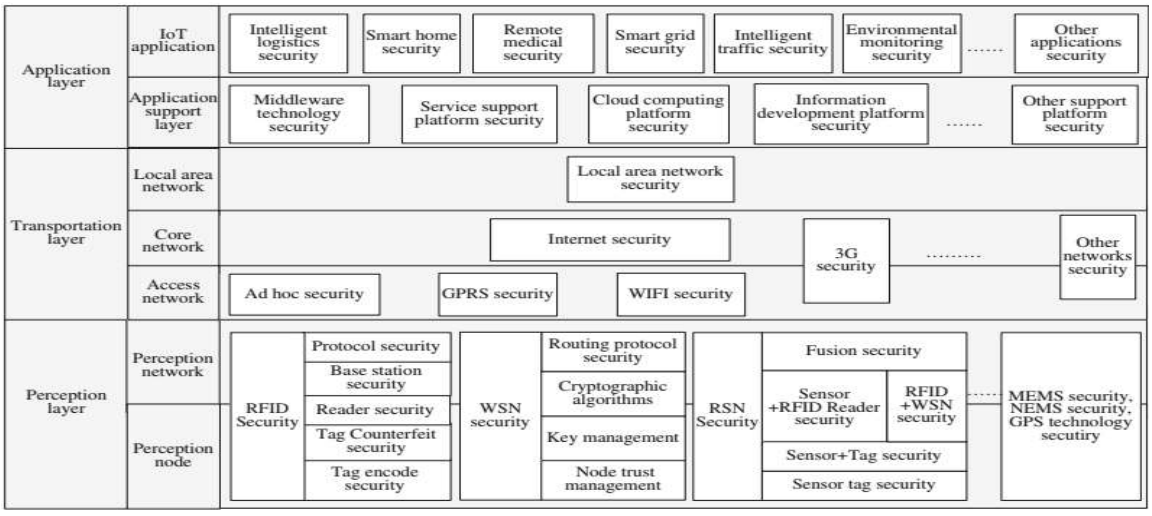

Fig. 1: Security in Various Aspects

Based on ciphers, cryptography system is classified into two categories that are stream ciphers and block ciphers. Stream ciphers are applied key to each bit of data stream based on algorithm and each bit is used at one time. The

 Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

stream ciphers are not used recently because of less authentication and protection. Block cipher is popularly used because of high protection and authentication. Data encryption Standard (DES) and Advanced Encryption Standard (AES) are the powerful encryption block cipher methods because key is applied to block of data. The size of block is changing from 56 to 128 and also both DES, AES are implemented on feistel network that is used two important techniques called substitution and permutation. The physical security of IoT is emphasized resource constraints hence addressing the level of security by lightweight cryptographic algorithms and its primitives. There are two powerful encryption methods for cryptography that are Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Based on the key size of cryptography, security algorithms are efficiently used in IoT. To implement these security services, block ciphers, hash functions and also signature algorithms. To meet high speed and high performance, an efficient security algorithm is deployed in Field Programmable Gate Array (FPGA) target device. FPGA is popular end device to develop a digital electronic model because of parallel processing. Fig.1 shows three layers of security that are Perception, Transportation and application layer. The security of IoT is analyzed in different phases of above layers. In present days, light weight security algorithms are majorly popularized research field because of perfect balance among power consumption, compactness and throughput. Clefia, PRESENT, DESXL and GRP are frequently used cryptographic algorithms for Substitution-box (S-box) implementation. IoT is intrinsically vulnerable to different types of attacks hence challenging security and privacy to users. The security is necessary in IoT based system to build data integrity, authority, availability, non-repudiation and confidentiality among users and also for avoiding serious threats. If cryptographic process is not taken which leads to data leakage and economy loss thereby damaging privacy of individuals. The components of IoT are open to physical attack because of unsupervised at high periods and also eavesdropping is extremely simple when IoT has wire-less communication. Another important challenge of IoT security is computational capability because of implementation of security algorithms are expansive thereby hindrance the performance in terms of energy [4]. Various modifications are introduced to obtain efficient hardware implementation in terms of security against side channel attacks [5]. A converter-gating technique is introduced based on work load aware thereby interleaving switched capacitance voltage is switched on and off with respect to load current.

This paper proposes an efficient security algorithm using S-box in encryption for IoT. A review is studied for secure IoT implementation with recent techniques thereby proposing high speed secure algorithm. An ECC is one of the encryption techniques for avoiding physical attacks. It is also implemented on Xilinx 14.7 software and implemented on Vertex-6 device for 128-bit feistel network. The remaining paper is as follows: section-II is presented literature of secure algorithms in IoT. Section-III is propounded an advanced S-box based ECC encryption algorithms for 128-bit feistel network and section-IV described implementation of results thereby discussion in IoT. Finally, section-V is concludes the paper.

Literature

IoT is one of dominant technologies from last decade because connecting millions of devices. The increase in communication among number of devices and data leads to increase in loss of data because of threats. The constraints and security challenges are examined in white paper which is posed by IoT devices, Wind River approach [6]. The evaluation of network security is also discussed and then identified new threats. Several security challenges are discussed with new threats thereby showing security in different modules of IoT system. Jing et. al. [7] discussed various security challenges with inclusion of internet issues. IoT has three layers of security that are perception layer, transportation layer and application layer. The individual problems of each layer are identified thereby proposing solutions separately. The comparison of IoT security with traditional network is presented with unified solution for IoT issues. Tay et.al. [8] proposed an 8-bit data path design to improve size of hardware in terms of Look-up Tables (LUT). The PRESENT based design is implemented in FPGA platform using Boolean S-Box through Karnaugh Map. To reduce complexity of system architecture, the common factor is divided into four expressions. The results are obtained in Vertex-5 FPGA device thereby presented 51.32 Mbps of throughput and 236.574 MHz of maximum frequency. The comparison is shown less area requirement but there is no improvement in throughput because of factorization. Usman etal. [9] presented a light weight cryptography algorithm called Secure IoT (SIT) to reduce complexity of encryption algorithm and also desired data integrity. It is designed with 64-bit block cipher and 64-bit key thereby utilizing mixture of feistel network and also uniform substitution-permutation network. The simulation results are shown the cryptography algorithm presented high security with five rounds of encryption thereby presenting high correlation and entropy. However, SIT based encryption is not simulated for different attacks. Zhang et.al. [10] propounded a Recryptor which consists of reconfigurable processor and also general purpose processor to compute encryption capabilities. It is also compatible in-memory processing capabilities using 10-T transistor bit cell thereby it supporting upto 512-bits. To get high throughput and speed, the customized system is composed with S-box, shifter and rotator. Still, the performance is lesser than AES because of long width computations involved in Recryptor. Khan

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

et.al. [11] investigated the performances of various security algorithms thereby presenting results in terms of processing cycles and execution time. The two different cryptographic libraries are experimented and measured in Raspberry Pi environment. The black box is used in Raspberry Pi and then implemented in security algorithm. The overall performance of ECC is improved when compared with AES because of efficient use of libraries. Though, it is less stable and throughput because of processing steps is costlier. Prathiba and Bhaaskaran [12] proposed a light weight solution for guarantee security of IoT. The design is used a non-linear 4X4 substitution box (S-Box) which is realized by multiplicative inversion and also affine transformation. The multiplicative architecture is used Euclidian inversion algorithm in the composite field and also affine transformation employed in the field. The results are validated at both linear and differential cryptanalysis thereby observing 86.5% lesser gate count for realization of composite field and also 5% lesser than PRESENT based algorithm. However, the analysis is observed only in upper bound of S-box. Ara et.al. [13] proposed an ECC to produce dynamic S-boxes for obtaining of less compute time. The dynamic S-box is tested different criteria that are strict avalanche effect, Bijection, Bit-Independence and Non-Linearity. It is implemented with C++ using cryptography arithmetic library thereby utilizing resources in efficient manner. Though, the level of security is same as AES and PRESENT works. Tsai et. al. [14] propound a high security and low power data encryption of AES which is suitable for Long Range Wide Area Network (LoRaWAN). The AES is proposed with powerful algebra and also multiple encryption cycles thereby ensuring communication security. To simplify AES encryption algorithm, Secure Low Power Communication (SLPC) is proposed by reducing encryption power of end device. The SLPC is simulated for three attacks hereby minimizing 26.2% encryption power when compared with LoRaWAN.

However, SLPC is employed for application layer. Niu et.al. [15] proposed a new type of encryption algorithm for collision attack. It employs a typical three AES with edge computing which is able to masking methods from linear layers. In addition, a new method is proposed which is capable of collision attack and high efficiency thereby masking linear layers and S-box. The performance is compared in terms of power analysis for second order linear layers and collision attacks. Though, shuffling methods are increasing noise.

By reviewing literature, security of IoT is one of the essential research domains for different applications such as smart irrigation, smart health system and military etc. High security of IoT system leads to worse energy dissipation, throughput, area and speed hence there is a need to present an efficient encryption algorithm to obtain compatible the performance for different applications. This paper presents an improved S-box of block cipher in feistel network thereby employing to IoT system.

Elliptic Curve Cryptography

IoT is extending services in terms of internet technology sophisticated to the society. Though, it accompanies new challenges and threats to provide privacy security. An ECC is majorly dominant in security aspects of system because of the complex encryption algorithm and also easy to design.

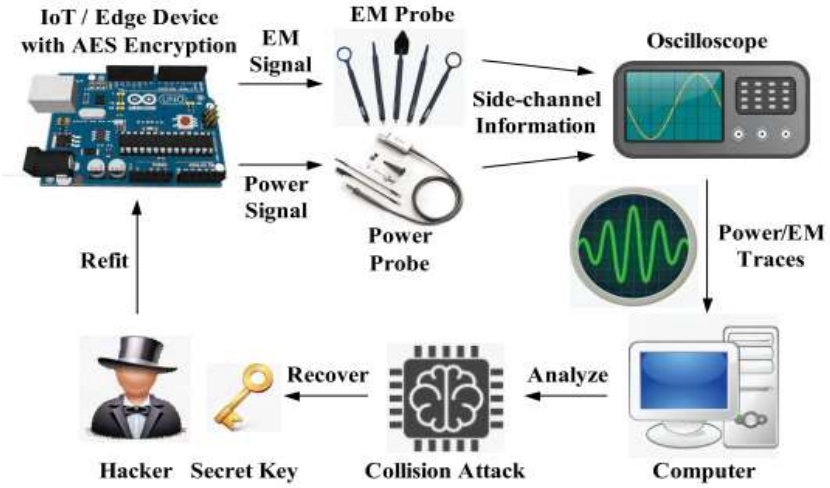

Fig. 2: AES Encryption Algorithm in Edge Computing and Collision Attack

However, design of secure IoT is highly complicated in terms of energy consumption because of implementing of data communication and data processing modules. Fig.2 presents the procedure of AES encryption algorithm for collision attack. The conventional AES is implemented for 128, 192, and 256 of block ciphers to prevent collision attack. An AT89S52 based IoT device equipped with AES algorithm to transmit encrypted data among different

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

servers thereby decrypting transmitted data between IoT device and other servers. The ECC is an asymmetric group of encryption algorithm which is utilized both public and private keys. The algorithm is composed an elliptic curve which is mathematically implemented.

$y^2 = x^3 + ax + b$ where $4a^3 + 27b^2 \neq 0$ (1)

The different elliptical curves are framed by modifying a and b values thereby identifying a point P(x, y) which lies on the elliptical curve. An arbitrary number is considered for private hence obtaining the public key at point Q by multiplying with point P on the elliptical curve. If P and Q are lies on the elliptical curve and satisfies the equation Q=kP where k is the constant value.

Fig.3 represents the elliptical curve where P and Q points are infeasible for the constant k thereby performing single scalar multiplication operation for two points. It is also called as point addition with point doubling. This operation is performed for the two different points which lies on the same curve thereby resulting another point lies on the existing curve.

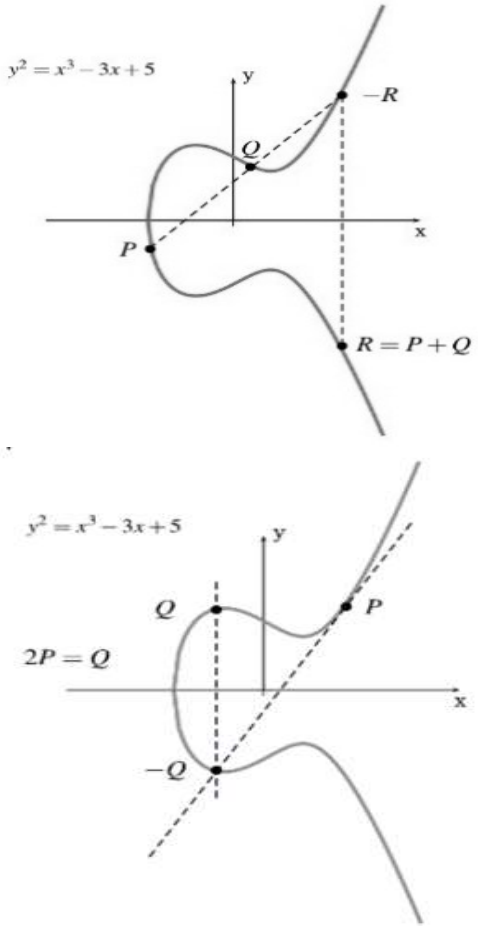

Fig. 3: Point Addition and Doubling on the Elliptical Curve

Assume points P and Q on the elliptical curve which is defined as $y^2 = x^3 - 3x + 5$

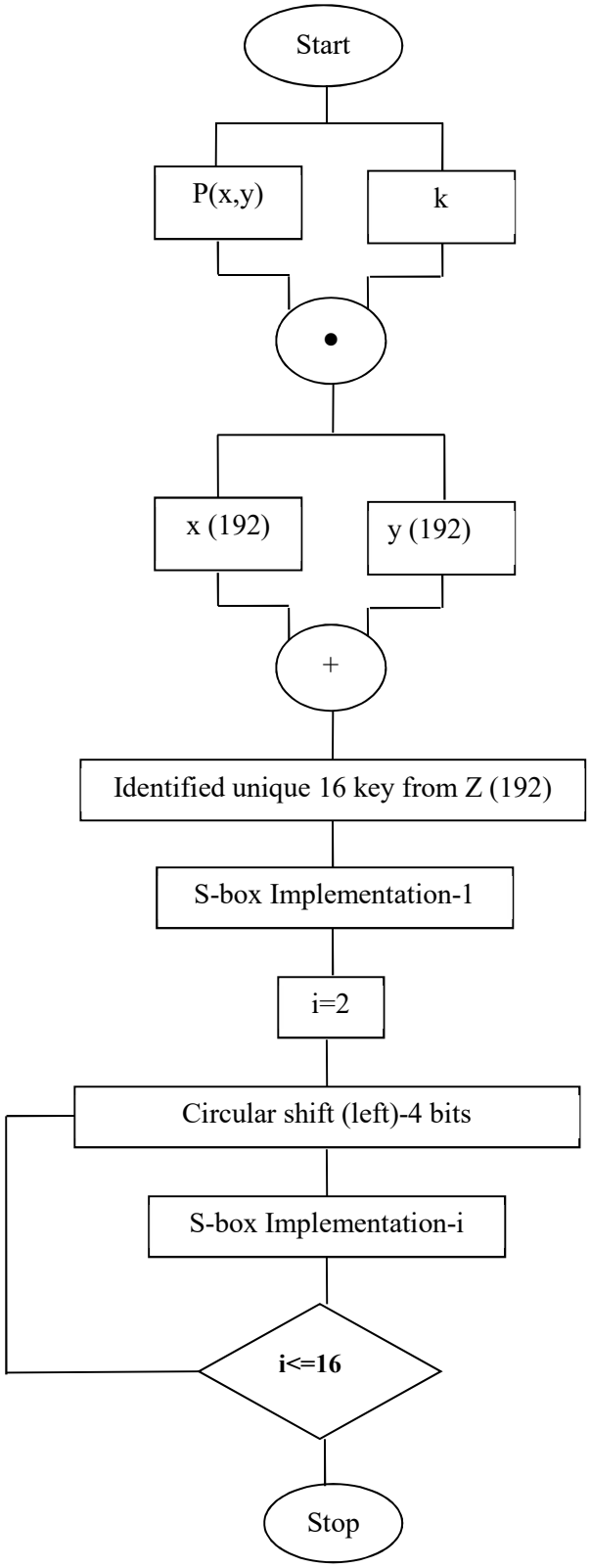

Fig. 4: Flowchart of Proposed S-box Algorithm

To get addition, the extended line is cut with –R which is passing through P and Q. the reflected point of R is lies on the same curve of X-axis thereby resulting P+Q=R. To perform double addition, consider a point P on the elliptical

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

curve, extend the line of elliptical curve which cuts at –Q. the same line lies on X-axis which creates a point R hence resulting 2P=Q. one of major advantage of ECC is high security with small key sixe.

(i). Proposed Algorithm

The performance of ECC scheme is based on the scalar multiplication of elliptical curves. The key size of algorithm presented the speed of ECC which is as same RSA cryptographic algorithm. The proposed algorithm is working based on the finite field theory and presented in fig.4. The proposed algorithm is executed in following stages which are initialization, scalar multiplication, extracting unique key point and exclusive-or operation. For particular 4-bit key, 16 hexadecimal is extracted from 192 bits of s-box. The algorithm is proposed with reference of NIST [16].

Implementation

The simulation and synthesis of proposed algorithm is implemented in Xilinx 14.3 and Spartan-5 FPGA device. The proposed S-box implantation is analyzed with various simulation parameters that are occupied slices, delay and power consumption. Table 1 shown S-box implementation for key 0010. For unique key (K), the point P on elliptical curve is identified initially thereafter the point Q is derived from the point P.

Table 1: S-box Implementation for Key 0010

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
SBox1(x)	7	9	5	6	B	1	4	F	D	0	E	3	2	C	8	A
SBox2(x)	9	5	6	B	1	4	F	D	0	E	3	2	C	8	A	7
SBox3(x)	5	6	B	1	4	F	D	0	E	3	2	C	8	A	7	9
SBox4(x)	6	B	1	4	F	D	0	E	3	2	C	8	A	7	9	5
SBox5(x)	B	1	4	F	D	0	E	3	2	C	8	A	7	9	5	6
SBox6(x)	1	4	F	D	0	E	3	2	C	8	A	7	9	5	6	B
SBox7(x)	4	F	D	0	E	3	2	C	8	A	7	9	5	6	B	1
SBox8(x)	F	D	0	E	3	2	C	8	A	7	9	5	6	B	1	4
SBox9(x)	D	0	E	3	2	C	8	A	7	9	5	6	B	1	4	F
SBox10(x)	0	E	3	2	C	8	A	7	9	5	6	B	1	4	F	D
SBox11(x)	E	3	2	C	8	A	7	9	5	6	B	1	4	F	D	0
SBox12(x)	3	2	C	8	A	7	9	5	6	B	1	4	F	D	0	E
SBox13(x)	2	C	8	A	7	9	5	6	B	1	4	F	D	0	E	3
SBox14(x)	C	8	A	7	9	5	6	B	1	4	F	D	0	E	3	2
SBox15(x)	8	A	7	9	5	6	B	1	4	F	D	0	E	3	2	C
SBox16(x)	A	7	9	5	6	B	1	4	F	D	0	E	3	2	C	8

Table 2 presents synthesis results of proposed s-box algorithm with basic ECC algorithms. The proposed algorithm is presented better performance than basic ECC algorithms in terms of various simulating parameters.

Table 2: Simulation Results various Cryptographic Algorithms

ECC algorithms	**Add**	**Scalar Multiplication**	**Proposed**
Synthesis Result			
Min Period	5.204ns	6.740ns	4.276ns
Max Achieved Frequency	192.175MHz	148.377MHz	233.86MHz
Maximum combinational path delay	7.69ns	8.32ns	6.06ns
Device Utilization			
Occupied Slices	6694 (7%)	7272/89088 (8%)	321(1%)
4 input LUTs	12099 (6%)	13780/178176 (7%)	520 (1%)
Flip Flops	6141 (3%)	7451/178176 (4%)	394 (1%)
Estimated Power Consumption	1.376(W)	1.49(W)	1.349(W)
Timing Result			
Cycles	8	8	8
Time	2.7us	0.552ms (max)	0.234ms
Synthesis prerequisite			
Computer RAM	4GB	4GB	4GB
Time for synthesis	16.72s	19.59s	21.45s
FPGA type---xc4vlx200-11ff1513			

Conclusion

The proposed ECC algorithm based on S-box is simple and easy to implement than other ECC algorithms. It is majorly important to IoT because of many devices and sensors are connected. The proposed S-box algorithm generates 16 bit unique key to provide high security than other algorithms. The simulation and synthesis results are proven that the proposed algorithm is better than conventional security algorithms.

References

1. Cerwall, P., Jonsson, P., Möller, R., Bävertoft, S., Carson, S., & Godor, I. (2015). Ericsson mobility report. *On the Pulse of the Networked Society. Hg. v. Ericsson*.
2. Zayas, A. D., & Merino, P. (2017). The 3GPP NB-IoT system architecture for the Internet of Things. In 2017 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 277-282). IEEE.
3. Bansod, G., Raval, N., & Pisharoty, N. (2014). Implementation of a new lightweight encryption design for embedded security. IEEE Transactions on Information Forensics and Security, 10(1), 142-151.
4. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. Wireless Personal Communications, 61(3), 527-542.
5. Uzun, O. A., & Köse, S. (2014). Converter-gating: A power efficient and secure on-chip power delivery system. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 4(2), 169-179.
6. SECURITY IN THE INTERNET OF THINGS, White Paper, 2015 Wind River Systems, Inc.
7. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.
8. Tay, J. J., Wong, M. D., Wong, M. M., Zhang, C., & Hijazin, I. (2015, August). Compact FPGA implementation of PRESENT with Boolean S-Box. In 2015 6th Asia Symposium on Quality Electronic Design (ASQED) (pp. 144-148). IEEE.
9. Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: a lightweight encryption algorithm for secure internet of things. arXiv preprint arXiv:1704.08688.
10. Zhang, Y., Xu, L., Dong, Q., Wang, J., Blaauw, D., & Sylvester, D. (2018). Recryptor: A reconfigurable cryptographic cortex-M0 processor with in-memory and near-memory computing for IoT security. IEEE Journal of Solid-State Circuits, 53(4), 995-1005.
11. Khan, N., Sakib, N., Jerin, I., Quader, S., & Chakrabarty, A. (2017, December). Performance analysis of security algorithms for IoT devices. In 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) (pp. 130-133). IEEE.
12. Prathiba, A., & Bhaaskaran, V. S. (2018). Lightweight S-box Architecture for secure Internet of Things. Information, 9(1), 13.
13. Ara, T., Shah, P. G., & Prabhakar, M. (2018, February). Dynamic key Dependent S-Box for Symmetric Encryption for IoT Devices. In 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC) (pp. 1-5). IEEE.
14. Tsai, K. L., Huang, Y. L., Leu, F. Y., You, I., Huang, Y. L., & Tsai, C. H. (2018). AES-128 based secure low power communication for LoRaWAN IoT environments. IEEE Access, 6, 45325-45334.
15. Niu, Y., Zhang, J., Wang, A., & Chen, C. (2019). An Efficient Collision Power Attack on AES Encryption in Edge Computing. IEEE Access, 7, 18734-18748.
16. Brown, M., Hankerson, D., López, J., & Menezes, A. (2001, April). Software implementation of the NIST elliptic curves over prime fields. In Cryptographers' Track at the RSA Conference (pp. 250-265). Springer, Berlin, Heidelberg.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495