Advances and Applications in Mathematical Sciences
Volume 22, Issue 1, November 2022, Pages 127-137
© 2022 Mili Publications, India

LIGHT WEIGHT CRYPTOGRAPHY (LWC) ALGORITHMS IN TERMS OF SOFTWARE METRICS FOR INDUSTRIAL INTERNET OF THINGS (IIOT)

S. SIVAGURUNATHAN and V. MUTHU GANESHAN

[1]Assistant Professor
[2]Research Scholar
The Gandhigram Rural Institute
(Deemed to be University), India
E-mail: svgrnth@gmail.com
muthuct8@gmail.com

Abstract

Electrical and electronic things functioning in a cooperated way with the help of internet is called Internet of Things (IoT). These things are ranging from tiny sensors to large electro mechanical devices, robotic arms and Cyber Physical Systems (CPS). IoT applications have emerged in the form of smart home, smart health-care, smart grid and smart industry. Smart industry is called Industrial IoT (IIoT) or industry 5.0. In IIoT, mass production of things are achieved by IIoT machines and devices with minimum labour support. These sensors and machines are specially designed for low power constrained devices with less processing and memory capacity. Hence the review was done for devices with only limited memory, energy, processing power and physical space. From data sensing to storing the data into cloud are the highly challenging process in various dimensions in achieving security objectives like authentication, confidentiality and integrity. Data security is the major challenge especially in these applications. To overcome this, Light Weight Cryptography (LWC) algorithms for IoT applications are explored. These algorithms receive input and process and communicate the data, which can be done only in a secured way with minimum time complexity and with less latency. Cryptographic algorithms are designed and developed with the standards called metrics. Those are Substitution Permutation Network (SPN), Feistel Network (FN), General Feistel Network (GFN), Add-Rotate-XOR (ARX), Non Linear Feedback Shift Register (NLFSR) and Hybrid. These LWC algorithms are to be standardized based on these metrics. In this article we have reviewed the metrics for the LWC algorithms used in IIoT systems.

2020 Mathematics Subject Classification: 11T71.

Keywords: IIoT, Security, Light Weight Cryptography (LWC), Standards and Metrics.

Received June 29, 2022; Accepted August 28, 2022

1. Introduction

Traditional manufacturing is very challenging to manufacture the mass production of things with reliability. It may consume more time to manufacturing the things. Nowadays, IIoT connected with electromechanical devices and internet to produce products of smart manufacturing. It transforms the traditional methods to digitalized typical consumer devices, people to people and people to machine communications for collecting, processing and storing data. It also enhances the technologies like distributed communication networks, Machine to Machine (M2M) communication, ultra efficient sensors and actuators, embedded systems, combinations of light and heavy machines to high performance gateways, and data analytics. Hence the applications of IIoT can take part in business and governments projects like smart home, smart cities, automation with intelligence. These applications are based on IIoT architecture. It comprises of four layers namely Device layer, Transport and network layer, processing layer and Application layer as shown in Figure 1.

Application Layer
Processing Layer
Transport and Network Layer
Device layer

Figure 1. IIoT Architecture.

Device Layer. This layer consists of devices and machines like sensors, Light Emitting Diodes (LED) and robotic arms. Each device has ID's namely Internet Protocol (IP), Electronic Product Code (EPC), Ubiquitous Code (UCode). These are identifying the particular machine for further process to manufacturing the things. This ID can also satisfy the security requirements like Authentication, Confidentiality and Integrity.

Transport and Network Layer. This layer transmits the data whatever data generated by the device layer. It communicates with heterogeneous devices and machines via networking protocols like ZigBee, WirelessHART. These protocols must satisfy the standards of IEEE 802.11 wireless standards.

Processing Layer. Data processing layer can evaluate the data transmitted by the network layer. Evaluation means arrange the data order of valuable information for further processing. Data processing may have three types like data-in-transit, data-in-rest and data-in-transform. Data in transit refers the data transfer in a secure manner from network layer to application layer using Secure Socket Layer (SSL) and Public Key Infrastructure (PKI). Data in rest refers the data stored in database using cloud or server with proper encryption. Data in transform refers to the data being manipulated by sorting or analysis by tools like queries.

Application Layer. This layer can execute the data based on the applications activated by software programs. It may work based on request and response manner. MQTT and XMPP protocols are working in this layer for executing the operations. This may be attacked by SQL injection, invalidated object indirect reference, Denial of Service (DoS) attack, password based attack, brute force attack and dictionary attacks. Protecting the data from above mentioned attacks through cryptographic algorithms is invariant. Light Weight Cryptography (LWC) algorithms are designed for these IoT applications [1].

This paper includes 2.LWC algorithms for IIoT 3. Metrics of LWC algorithms 4. Research Challenges and directions and Conclusion.

2. LWC Algorithms for IIoT

LWC algorithms are specially designed for low powered devices and suitable for IoT applications. It is categorized under stream cipher and block cipher. More than fifty LWC algorithms are available in market. An additional 57 LWC algorithms are submitted by researchers for National Institute of Security and Technology (NIST). This competition is resolved based on implementation cost, hardware and software performances. These metrics are analyzed based on their structure [2].

Structure of LWC Algorithms. Structures of LWC are namely Substitution Permutation Network (SPN), Fiestel Network (FN), General Fiestel Network (GFN), Add-Rotate-XOR (ARX), Non Linear Feedback Shift Register (NLSFR) and Hybrid methods. SPN is using most LWC algorithms by substituting alternative bits from mathematical operations and permutation table is defined for re arranging bits. FN functions split the block cipher into equal two halves. Diffusion function is applied on the one half and swapping the values in another half. In GFN blocks are divided into sub blocks and every sub block operation is done by FN. ARX comprises of Addition, rotation and XOR operations on bits. NLFSR consists of right shift and left shift operations based on rounds. ARX and NLFSR can be applied for both stream and block ciphers. Hybrid method is a combination of above mentioned structures like block arranging, optimal bits and improve the efficiency in anyone of the metrics like throughput or Gate Equivalence (GA) GA is the count of the number of gates used in the algorithm. Based on these metrics we can design LWC and apply them for different IoT applications [2].

LWC Algorithms Four LWC algorithms are used in IIoT applications namely

1. PRESENT
2. PRINCE
3. SIMON
4. MIDORI

PRESENT, PRINCE and MIDORI algorithms are designed using SPN structure. SIMON algorithm is designed using FN structure. The above mentioned algorithms are designed by hybrid method using various operations [2].

2.1 Present

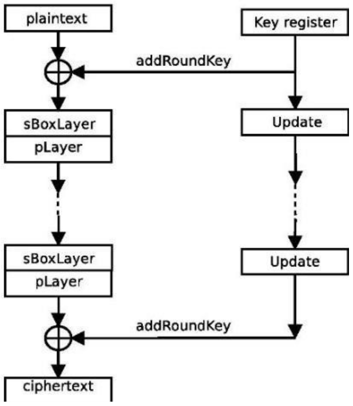
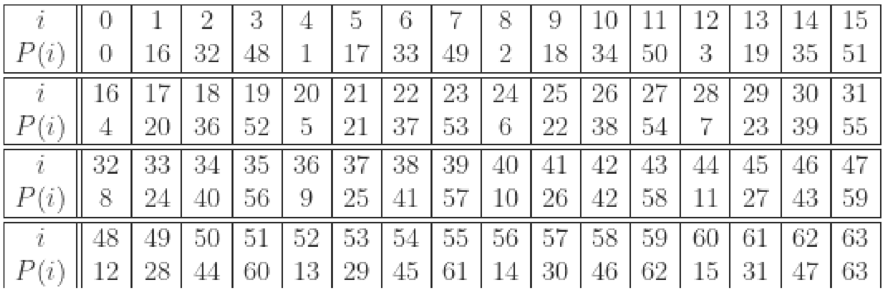


Figure 2.1. Present LWC Algorithm.

Present Algorithm Steps:

```
1. Generate → Round Key (RK) ()

2. for $n$ = 1, 2, …, 31

        add (RK) → (STATE, Kn)

        sbox(STATE)

        pbox(STATE)

        end for

3. add (RK) → (STATE, K32)
```

Present algorithm shown in figure 2.1 is 64 bit block cipher and 80,128 bit keys are used as 32 rounds of encryption comprises of XOR operations and bitwise permutation and substitution. RK executes 31 rounds with substitution and permutation operations. Afterwards the final state is done EXOR operation with key32. In S box 4 bits are added with every block in parallels of 16 times of each rounds. P box is designed by 4 layers namely $P(0)$, $P(1)$. $P(1)$ and $P(3)$, each layer has 16 bits and values are assigned. Every value is vertically increased 4 values in all layers serially as Show in Figure 2.2



i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Figure 2. 2 P-BOX of PRESENT Algorithm.

Key schedule. 80/128 bit Key is saved in key register called K. K is in order of K_{79}, K_{78}, K_0. From left most bit, every 64 bits are selected for subsequent rounds until the final round.

The efficient implementation is done by PRESENT cipher with 80 and 128 bit key on Field Programmable Gate Array (FPGA) based hardware architecture. It evaluates the data load and key load with [3]. It also evaluates from targeted IoT devices to nearest area, frequency and path delay [4]. Energy consumption analysis is also reviewed on energy in active mode, power and battery life [5]. Enhanced version of this cipher can resist side channel attack. It compares the probability of leakage data in percentage [6]. In mean time every cryptographic algorithm is enhanced in all dimensions like hybrid methods for block cipher and hybrid key generation [7].

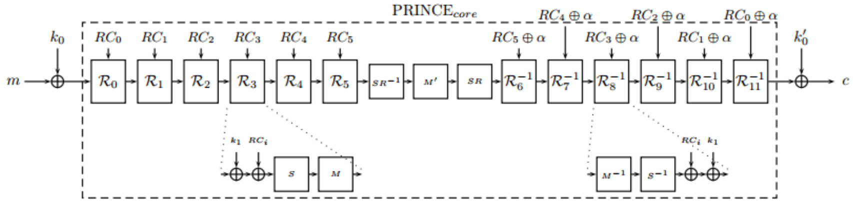


Figure 2. 3 PRINCE Algorithm.

PRINCE cipher is a 64 bit data block and 128 bit key size with 11 rounds of encryption method. Key bock 128 bits are divided into 2 halves as K0 and K1. K0 is encrypted with initial data block and moving to round functions namely forward, middle and backward functions. Forward function operates five rounds with Round Constants (RC) functions give hexadecimal output. non linear Non linear S consists of single 4 bit S boxes. This S layer is a middle layer. Backward function operates in five rounds of encryption exactly inverse of M'. Afterwards K0' is EXOR ed with final round of output and it gives Cipher text for single block. Until the final block this process repeated. Enhanced PRINCE cipher is tested with secure way in using dual mode of configurable security aware pipelining for high throughput applications [8]. Improved version of this cipher in Matrix Integer Linear Programming (MILP) is applied on matrix multiplications [9]. To protect from differential attack authors introduced unrolled PRINCE [10], designed in an efficient lightweight cryptographic instruction set using PRINCE and PRESENT combination [11]. Enhanced PRINCE cipher is designed with Block Balanced Mixing (BBM) algorithm. BBM is a necessary mix of the data with origin block like Initial Vector (IV). It compares cipher block generation time in milliseconds (ms) [12].

2.3 SIMON. SIMON block cipher comes in various sizes like 32,48,64,96 and 128 bits for data. Key size may include 64, 72, 96, 128,144, 192 or 256 bits. This cipher is a Fiestel Block Cipher designed by National Security Agency(NSA). It includes the operations like AND, OR and left circular shift. It improves the performance of hardware with good computation. In round function SIMON consists of two rounds in the form of these equations.

$$RK(x,\ y) = (y \oplus f(x) \oplus,\ X) \qquad (1).$$

Round key

$$f(x) = (Sx \ \&\ S^8 x) \oplus S^2 x \qquad (2)$$

Operations:

Bitwise AND denotes Bitwise AND operation between two random bits of n bits

Bitwise OR represents XOR operations on x and y bits.

Based on these operations, combination of SPECK and SIMON are enhanced to compare the execution times in various rounds with various data block sizes and its compared with Advanced Encryption Standard algorithm (AES) [13]. Enhanced with the optimization both SPECK and SIMON algorithms with various block sizes like 32,48,64,96 and 128 bits data blocks and three various key sizes like 128,192,256 [14]. This algorithm also checks the FPGA device to measure the energy level [15]. The robustness of this algorithm is evaluated in various stages in between rounds and minimum number of rounds [16]. It is also checks the various single data block size and double block size of keys [17].

2.4 MIDORI.

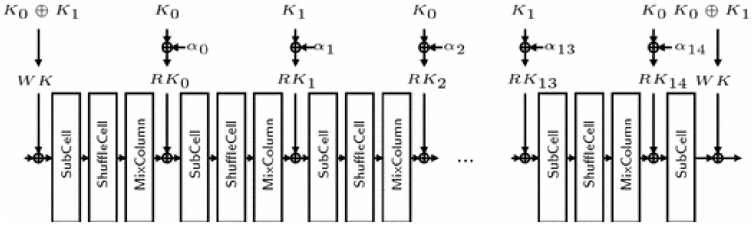


Figure 2. 4 Midori Algorithm.

Midori means “green” colour in Japanese. This algorithm is a family of two block ciphers of 32 and 64. Total encryption rounds are 16 as shown in Figure 2.4. Data blocks are split into 4×4 matrix called state. Each state can cross four various operational blocks namely sub cell, shuffle cell and mix column and key add. Sub cell is to do S-box operations. Shuffle cell shifts the cells based on mathematical operations. Mix column in mixing the column values between them. Finally key add is adding the round key. Midori 64 is split into two parts as K0 and K1. First and last rounds of K0 and K1 meet EXOR ed operation and is called whitening process. Each round is EXOR ed with round key for subsequent process until the 16 rounds of encryption. A linear analysis is done by using related key [18]. To optimize the minimum number of rounds of encryption Midori 64 checks the various attacks like differential attacks and dictionary attacks in various rounds [19]. To enhance the cryptanalysis for differential attacks in 10, 11 and 12 rounds of encryption with 287.7, 290.63 and 290.51 time complexity is done [20].

3. LWC Algorithms Software Metrics

LWC algorithms are standardized with various metrics levels. They are less complexity, secure architecture, rich encryption standard, high throughput, less execution time, less power, less memory and it must resist from various attacks like linear and differential attack [21]. Static operation of encryption algorithm is key and S box only. Random operations only calculate the computations and latency. LWC can measure it by (Gate Equivalence) GE. 1 GE = 2 NAND Gate). Within 2800 GE only comes under LWC metrics. Latency is defined by number of clock cycles per block. Throughput is calculated as bit per second at 100 Kilo Hertz (KHZ). Average of plaintext is processed by CPU clock cycle at 4 Mega Hertz (MHZ). Power consumption is measured by μW [2].

Energy Consumption

Energy $[\mu W]$ = (Latency [cycles/ block] * Power $[\mu W]$) / block size [bits] ...... (3)

Software Efficiency

Software Efficiency = Throughput [Kbps] / Code Size [KB] ...... (4)

4. Research Challenges and directions

A Strong LWC algorithm well balanced in cost, performance and security aspects are in need of hour. As more number of encryption rounds may affect the performance and cost, minimum number of encryption rounds may affect the security objectives like confidentiality, integrity and availability. In the mean time, fundamental structure of cryptographic algorithm is applied to maintain the standardization like S-box and P-box. Key scheduling is one of the challenges to ensure the optimal size. Key sizes may vary with 32, 64, 96, 128 and 256 keys. Wherever we need to modify the algorithms, we have to verify the all dimensions of LWC algorithms [2]. Various cryptanalysis are done on IIoT LWC algorithms as shown below in table 5.1.

Table 4.1. IIoT LWC Algorithms Cryptanalysis.

S.No	LWC Algorithm	Differential	Linear	Integral/ Square/ Saturation	Algebric / Cube	MITM/ Biclique	Related Key Attack	Side-Channel/ Differential fault attacks
1.	PRESENT	✓	-	-	-	✓	✓	✓
2.	PRINCE	✓	-	-	-	-	-	-
3.	SIMON	✓	-	-	✓	-	✓	-
4.	MIDORI	✓	✓	-	✓	✓	-	-

Conclusion

Industry 5.0 is now enhancing IIoT with robotics and artificial intelligence (AI). Therefore, heterogeneous IIoT devices and machines are capable of producing heterogeneous data. With the standardisation of measurements like throughput, latency, and software efficiency, LWC algorithms may be appropriate for these IIoT devices. Effective evaluation of these characteristics is required. As a result, a thorough analysis that was justified was done utilising mathematical analysis. It is a type of computational cryptanalysis that is carried out for numerous attacks on the PRESENT, PRINCE, SIMON, and MIDORI algorithms, including differential, linear, integral, algebraic, Man in the Middle, related key, and side channel attacks. These can be used in IIoT machinery and equipment.

References

[1] Soo Fun Tan and Azman Samsudin, Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (IIoT): A Survey, Sensors 21(19) (2021), 6647.

[2] Vishal A. Thakor, Mohammad Abdur Razzaque and Muhammad R. A. Khandaker, Lightweight Cryptography Algorithms for Resource- Constrained IoT Devices: A Review, Comparision and Research Opportunities, IEEE Access 2169-3536 (9) (2021), 28177-18193.

[3] Hangemah Delfan Azari and Dr. Prashant V. Joshi, An Efficient implementation of PRESENT cipher model with 80 bit and 128 bit key over FPGA based hardware architecture, International Journal of Pure and Applied Mathematics 119(14) (2018), 1825-1832.

[4] Anitha Kumari and Mahalinga V. Mandi, Implementation of PRESENT cipher on FPGA for IoT applications, International Journal of Engineering Research and Technology 8(08) (2019), 2278-0181.

[5] Bora Aslan, Fusun Yavuzer Aslan and M. Tolga Sakallai, Energy Consumption Analysis of Lightweight Cryptographic Algorithms That Can be Used in Security of Internet of Things Applications, Security and Communication networks, 1939-0114, Hindawi Willley, 2020.

[6] Nilupulle A. Gunathilake, Ahmed Al-Dubai, Wiliam J. Buchanan and Owen Lo, Electromagentic Side-Channel Attack Resilience against PRESENT Lightweight Block Cipher, Arixv, (2021), 2331-8422.

[7] Reece B. Disouza and Yash Priyadarshi, Improving Security of IoT Devices using Cryptographi Algorithms, International Research Journal of Engineering and Technology 08(11) (2021), 2395-0072.

[8] Nael Mizanur Rahman, Edward Lee, Venkata Chaitanya Krishna Chekuri, Arvind Singh and Saibal Mukhopadhyay, A Configurable Dual-Mode PRINCE Cipher with Security Aware Pipelining in 65 nm for High Throughput Applications, Custom Integrated Circuits Conference, IEEE, 2020.

[9] Murat Burhan Ilter and Ali Aydin Selcuk, A New MILP model for Matrix Multiplications with Applications to KLEIN and PRINCE, International Conference on Security and Cryptography (SECRYPT 2021), 2184-1152, pp 420-427, Science and Technology publications, 2021.

[10] Shu Takemoto, Yusuke Nozaki and Masaya Yoshikawa, Differential Power Analysis using Chosen-Plaintext for Unrolled PRINCE, International Conference on Robotics, Control and Automation Engineering, 978-1-4503-6102-6, ACM, 2018.

[11] Wajeh El Hadj Youssef, Ali Abdelli, Fethi Dridi, Rim Brahim and Mohsen Machhout, An Efficient Lightweight Cryptographic Instructions Set Extension for IoT Device Security, Security and Communication networks, 1939-0114, Hindawi, Willey 2022.

[12] Pallavi Jha, Haythem Yosef Zorkta, Dahham Allawi and Maher Riad Al-Nakkar, Improved Lightweight Encryption Algorithm, International Conference for Emerging Technology (INCET), 978-1-7281-6221, IEEE, 2020.

[13] Norah Alassaf, Adnan Gutub, Shabir A. Parah and Manal Al Ghamdi, Enhancing speed of SIMON: A light-weight cryptographic algorithm for IoT applications, Mutimedia Tools and Applications, 1380-7501, Springer (2019), 32633-32657.

[14] Anil G. Sawant, Sayali Kamthe, Yashasvini Shaha, Bapu Morajkar and Abhisek Sakpal, Implementation of SIMON and SPECK Algorithm, Journal of Emerging Technologies and Innovative Research, 2349-5162, 6(1) (2019), 292-296.

[15] Saed Abed, Reem Jaffal, Bassam Jamil Mohd and Mohammad Alshayeji FPGA Modeling and Optimization of a SIMON Lightweight Block Cipher, 913, sensors, 2019.

[16] B. H. Susanti, O. J. Permana and Amiruddin, Robustness Test of SIMON-32, SPECK-32 and SIMECK-32 Algorithms using fixed-point attacks, Journal of Physics Conference Series 1836 (2021) 012006.

[17] Tutu Wan and Emre Salman, Ultra Low Power SIMON Core for Lightweight Encryption, IEEE International Symposium on Circuits and Systems (ISACS), 978-1-5386-4881-0,IEEE, 2018.

[18] Hun Jun Ru, A new kind Linear Analysis of Invariant Bias of Midori-64 related keys, International Conference Artificial Intelligence and Security (ICAIS) 1865-0929, pp 376-384, Springer, 2020.

[19] Wenhao Liu and Yang Yang, The 7-Round subspace Trail-Based Impossible Differential Distinguisher of Midori-64, Security and Communication Networks, 1939-0114, Hindawi Willey, 2021.

[20] Aein Rezaei, Shahmirzadi, Seyyad Arash Azimi, Mahmoud Salmasizadeh, Javad Mohajeri and mohammad Reza Aref, Impossible Differential Cryptanalysis of Reduced Round Midori-64 Block Cipher, 2008-2045, ISecCure 10 (2018), 3-14.

[21] Deepti Sehrawat and Nasib Singh Gill Lightweight Block Ciphers for IoT based applications: A Review, International Journal of Applied Engineering Research, 0973-4562, Research India Publications 13(5) (2018), 2258-2270.