ANALYSIS OF LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

I.S.Olimov,
Tashkent university of information technologies named after
Muhammad al- Khwarizmi
E-mail: iskandar.olimov@mail.ru

X.I. Ibrohimov
Tashkent university of information technologies named after
Muhammad al- Khwarizmi

Abstract: *This article explores the layers of the Internet of things, security issues, requirements, and methods for creating lightweight cryptographic algorithms. In addition, the classification of light cryptographic algorithms and their analysis is given.*

Keywords: *Internet of things (IoT), RFID, DDoS, Substitution-Permutation Network (SPN), Feistel Network (FN), General Feistel Network (GFN) , Add-Rotate-XOR (ARX), NonLinear-Feedback Shift Register (NLFSR), Hybrid (Hybrid))*

Introduction

In today's information society, the scope of the Internet of things is expanding and becoming more popular as a result of widening the fields of application. IoT devices collect data from the real environment and transmit it over networks. The Internet of things (IoT) has already become dominant and has already become a dominant research field due to its applications in various fields [4]. Because smart transportation, smart logistics, smart healthcare, smart environment, smart infrastructure (smart cities, smart homes, smart offices, smart shopping centers, industry), smart agriculture, etc. contribute to the development of society. It is a very

large number of small sensors to servers and the Internet of things has a number of challenges in connecting devices with the real world, because billions of smart devices (connected devices) running on different platforms, during the transition from servers to sensors for their owners or users a variety of unseen issues (such as security, privacy, interoperability, durability and supportability, etc.) arise with technology-related vulnerabilities [4].

In Internet of things applications, it is important to ensure data privacy in the process of communication between physical devices (such as energy, memory, processing power, and even physical space), but currently, ensuring privacy in the Internet of things is currently the most is an urgent issue [4,6]. This article explores the layers of the Internet of things, security issues, requirements, methods of creating lightweight cryptographic algorithms, and also provides an analysis of lightweight cryptographic algorithms.

The main components of the Internet of Things

Various definitions of Internet of things have been given by many researchers, industry experts, organizations depending on the applications and implementation field, but in simple words, Internet of things each has its own identity, the Internet of things. a set of connected technologies that can collect and share data with or without interaction [4].

Figure 1. Internet of things

Security issues in the Internet of things. When working with any digital data, the main requirement of the user is to incorporate information such as reliability and confidentiality. There are a number of security issues in the Internet of things today, including:

- cryptographic methods;
- management of keys;
- DDoS;
- compatibility;
- authentication and permission management.

Cryptographic methods. AES, which is a symmetric encryption algorithm, and asymmetric encryption algorithms (RSA, Diffie-Hellman, Elliptic curves) are among the most reliable algorithms currently used to ensure data privacy. Similarly, HESh algorithms used to ensure data integrity (SHA1, MD5) are safe and effective, but these algorithms require a high-power processor and a lot of time. Therefore, the use of these algorithms in secure information exchange in the Internet of things is not highly effective [1,4]. Based on the above considerations, developing new cryptographic algorithms that require less computing power and power, or improving existing cryptographic algorithms for battery-powered IoT devices, is one of the challenges of today's Internet of things.

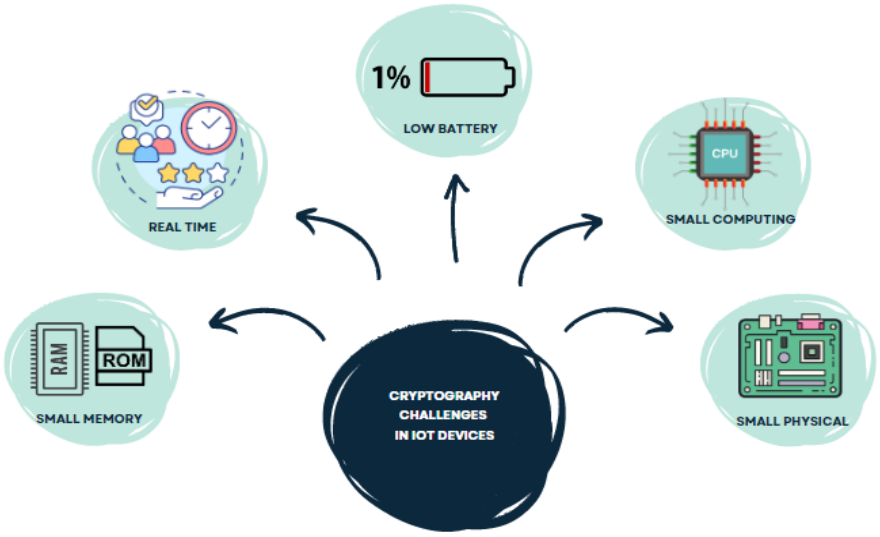

Figure 2. A cryptographic problem in the Internet of things

Lightweight cryptographic algorithms for Internet of things limited resources have the following characters. There are physical, performance, security [1,3]. Physical character consists of physical (GEs), memory (RAM, ROM), battery power. Performance includes computing power. Sucurity character consists of minimum security (bits), attack models. Requirements for lightweight cryptographic algorithms are tiny key and block, simple rounds, key generation, strong internal structure.

Existing lightweight cryptographic algorithms and their creation methods

Table 1. Classification of light cryptographic algorithms according to their structure

<table>
<tr><td rowspan="10">Lightweight cryptography</td><td>Asymmetric</td><td colspan="3">Elliptic Curve Cryptography, RSA Algorithm</td></tr>
<tr><td rowspan="9">Symmetric</td><td rowspan="8">Block cipher</td><td>SPN</td><td>Midori, mCryton, Noekeon, Iceberg, AES, Present, Led, Picaro, Zorro, 1-Present, EPCBC, GIFT, SKINNY, Rectangle, Puffin-2, Prince, Pride, Print, Klein.</td></tr>
<tr><td>FN</td><td>Camellia, Simon, SEA, KASUMI, DESL/DESXL, TEA/XTEA/XXTEA, MIBS, LBlock, ITUbee, FeW, GOST, Robin, Fantomas</td></tr>
<tr><td>GFN</td><td>Piccolo, Twine, CLEFIA, HISEC</td></tr>
<tr><td>ARX</td><td>Speck, IDEA, HIGHT, BEST-1, LEA</td></tr>
<tr><td>NLFSR</td><td>Halka, KeeLoq, KATAN/KTANTAN</td></tr>
<tr><td>Hybrid</td><td>Hummingbird, Hummingbird-2, Present-GRP</td></tr>
<tr><td colspan="2">Stream cipher</td><td>Trivium, Rabbit, HC-128</td></tr>
</table>

PRESENT. This algorithm is convenient in terms of hardware and software, and it is the most efficient algorithm approved by ISO/IEC (29192-2P:2012). It is based on a permutation network, with a block length of 64 bits and a key length of 80 bits and 128 bits, respectively. GE requirements for PRESENT are 1570 and 1886. PRESENT is convenient to represent in hardware form using 4-bit S-boxes, except (replaces eight S-boxes with one S-box). In software, it requires large cycles [1,3].

TEA (Tiny Encryption Algorithm). Although its algorithm is not based on the Feistel network, it is a simple and similar algorithm. In other words, encryption and decryption functions are different. The TEA algorithm uses 64-bit plaintext blocks and a 128-bit key. The algorithm is designed to perform operations with 32-bit words and therefore uses the operation $SSeedd232$. The number of rounds in this algorithm is variable, and from the point of view of risk, the number of rounds must be at least 32. Each round of the TEA algorithm is equivalent to two rounds of the Feistel network. When designing block ciphers, there must be a balance between the complexity of the round function and the number of rounds. For example, if the round function is simpler, the number of rounds will be less or vice versa. Since the TEA algorithm is a simple algorithm, a large selection of the number of rounds is necessary to be robust. The encryption function of the TEA algorithm is given below.

(LL, XX) = plaintext block (64 bits)

$ddeeeeSSaa = 0xx9ee3779aa9$

$ssssSS = 0$

$aaeeSS\ SS$ = 1 to 32

$ssssSS = ssssSS + ddeeeeSSaa$

$LL = LL + (((XX \ll 4) + KK[0]) \oplus (XX + ssssSS) \oplus ((XX \gg 5) + KK[1]))$

$XX = XX + (((LL \ll 4) + KK[2]) \oplus (LL + ssssSS) \oplus ((LL \gg 5) + KK[3]))$

then SS

ciphertext = (LL, XX)

Here, the operation "≪" is the operation to shift the number to the left, and the operation "≫" is the operation to shift it to ten. For example, if a one-byte number in

binary form is "10110101", then shifting this number to the left by 4 units will result in "01010000". The result of moving this number to 5 decimal places is "00000101". Although the TEA algorithm is not based on the Feistel network (encryption and decryption functions are the same in the Feistel network), the decryption does not use addition or division operations instead of the XOR operation.

IDEA. It was developed by Lai and Massey, block length is 64 bits, key length is 128 bits, it uses 16-bit unsigned, data operations such as integer and XOR, addition and modular multiplication are S- box or without using P-box. It will perform best on embedded systems with a throughput of 94.8 Kbps with a memory requirement of 596 bytes [1,4].

Stream Cipher

Rabbit is a lightweight stream cipher and was first presented by Martin Boesgaard, Mette Vesterager, Thomas Christensen and Erik Zenner at an encryption workshop in 2003 [8]. It creates a key stream from an 128 bit key and a 64 bit IV. The use of IV can prevent collision and pre-image related attacks. The encrypted value has equal bit-length to the message, thus no overhead storage. Rabbit is nearly twice as fast as RC4 (Rivest Cipher 4) and HC-128 is about 5 fold, and is about 3 times faster than AES. Therefore, if you have speed concerns about SSL, using more compacted version of SSL with lightweight stream ciphers should alleviate the performance burden [9]. Also, it can be used in Elliptic Curve Integrated Encryption Scheme (ECIES) as key stream derivation function for the shared session secret produced by the elliptic curve method [1,2].

Trivium is another low footprint hardware utilised lightweight stream cipher proposed by Christophe De Canniére and Bart Preneel. It has key stream and IV both of 80 bits and output of 264 bits.

Asymmetric cipher

Elliptic Curve Cryptography. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. While RSA is based on exponentiation on finite fields, ECC depends on

point multiplication on elliptic curves. An elliptic curve E over the finite field K (whose characteristic is not equal to 2 and 3) is defined as:

E(K) : y2 = x3 + ax + b with a, b ∈ K

Points P = (x, y) ∈ E(K) form an Abelian group, so point addition and scalar point multiplication can be performed. ECC provides higher security and a better performance than the first-generation public-key techniques, RSA and Diffie–Hellman. Moreover, ECC is the most interesting public-key cryptographic family for embedded environments because it can reach the same security level as RSA with much shorter keys, and with computationally lighter operations, like addition and multiplication, rather than exponentiation [1,5].

Table 2. Lightweight cryptographic algorithms

Encryption algorithm	*Tech*	*K_size*	*B_size*	*Num of round*	*Area (GEs)*
AES	SPN	128	128	10,12,14	2060
PRESENT	SPN	80	64	31	1570
GIFT-64/128	SPN	128	64,128	28,40	1345
SKINNY	SPN	n, 2n, 3n	64,128	32,56	1477
RECTANGLE	SPN	80	64	25	1467
MCrypton	SPN	128	64	13	2594
NOEKEON	SPN	128	128	16	2604
ICEBERG	SPN	128	64	16	5817
PUFFIN-2	SPN	80	64	34	1083
PRINCE	SPN	128	64	12	2953
Klein	SPN	64	64	12	1220
1-PRESENT	SPN	80	64	30	2467
EPCBC	SPN	96	48	32	1008
TEA	FN	128	64	32,64	2355
SIMON	FN	96	48	32-72	763
KASUMI	FN	128	64	8	3437
MIBS	FN	64	64		1396
LBlock	FN	80	64	32	1320
CLEFIA	GFN	128	128	128	2678

PICCOLO	GFN	80	64	25,31	1136
TWINE	GFN	80	64	36	1503
SPECK	ARX	96	48		884
HIGHT	ARX	128	64	32	2608
RC4(flexible)		128	80		11300
Rabbit		128	64		3800
Trivium		80	80		2599
RSA		1024 to 4096 modulus			50000
ELLI		256 private key		256 public key	6660

Conclusion

The current development of the Internet of things system leads to an increase in the demand for its security. This article explores the layers of the Internet of things, security issues, security requirements, and methods of creating lightweight cryptographic algorithms. At the same time, an analysis of light cryptographic algorithms and a number of their features is provided. The analysis of the cryptographic problem shows that it is necessary to develop a crypto-algorithm with high crypto resistance, which requires less time, energy and power in the transmission of information through the network, and in addition, it is possible to achieve high efficiency by improving the existing encryption algorithms.

LITERATURE

1. Thakor, Vishal A., Mohammad Abdur Razzaque, and Muhammad RA Khandaker. "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities." *IEEE Access* 9 (2021): 28177-28193.

2. Banani, Sam, et al. "A Dynamic Light-Weight Symmetric Encryption Algorithm for Secure Data Transmission via BLE Beacons." *Journal of Sensor and Actuator Networks* 11.1 (2021): 2.

3. Akmuratovich S. M. et al. A Creation Cryptographic Protocol for the Division of Mutual Authentication and Session Key //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – C. 1-6.

4. Salimbayevich O. I. et al. Internet of things architecture and security challenges //2020 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2020. – C. 1-4.

5. Meng, Thomas Xuan, and William Buchanan. "Lightweight cryptographic algorithms on resource-constrained devices." *Preprints* (2020).