A Review of Cryptography Algorithms for IoT

Zahra Dorostkar
Department of Computer Science and Engineering
Saint Petersburg Electrotechnical University
Saint Petersburg,Russia
zdorostkar@stud.etu.ru

Nikolay N.Vasiliev
Department of Algorithmic Mathematic
Saint Petersburg Electrotechnical University
Saint Petersburg,Russia
vasiliev@pdmi.ras.ru

Ghader Ahmadi Didehbani
APA Moshaver
Tabriz,Iran
ahmadi.di90@gmail.com

***Abstract*—The Internet of things has made demands on ensuring quality of communication between nodes and security. It is vital to provide a reliable encryption algorithm with reasonable complexity and computational expense in IoT. There are many different cryptography algorithms that the proper selection between them is an important issue. In this article we briefly review all types of cryptography algorithms for IoT.**

Keywords—Information Technology Security, IoT, Cryptography, Encryption, Hashing, Symmetric, Asymmetric, Quantum, Post-quantum

I. Introduction

There are many different algorithms which can ensure security in different aspects. These algorithms can be categorized in three main groups, including Physical cryptography, Mathematical cryptography and Quantum cryptography, and also an additional group is considered as Post-quantum cryptography. However, not all can be used in IoT, since in IoT we face many restrictions that must be considered. So In addition to all of the above, a new group of algorithms has appeared in recent years, so called Lightweight algorithms, which are particularly designed for IoT. In this article, we review the main types of algorithms briefly and have an overview of important terms of them such as speed, level of security, effectiveness, attacks, etc. Since in previous works just one or two categories in IoT have been considered in this work a more comprehensive view and also efficient and most common algorithms in IoT are considered.

II. Types of Cryptography

A. Physical Cryptography

The name physical has been used because in this type of cryptography, no special mathematical function or processing is done on the text. The most common method is to move or exchange alphabetic letters (characters) or words, or to hide information inside other information such as an image or audio (Steganography and Watermarking). These types of algorithms are not used for IoT purposes.

The most famous ones are followings:
Atbash, *ROT13*, *Caesar, Affine, Rail-fence, Baconian, Polybius Square, Simple Substitution, Codes and Nomenclators, Columnar Transposition, Autokey, Beaufort, Porta, Running Key*, *Vigenère and Gronsfeld, Homophonic Substitution*, *Four-Square, Hill, Playfair, ADFGVX, ADFGX*, *Bifid*, *Straddle Checkerboard*, *Trifid*, *Base64, Fractionated Morse***.**

B. Mathematical Cryptography

In this type, mathematical algorithms are used for changing information of text or any multimedia such as image or audio signal etc. There are three considerable categories here: *Hashing*, *Symmetric* and *Asymmetric*.

Hashing algorithms include MD2, MD4, MD5, SHA-1, RIPEMD-160, Whirlpool, SHA-2, SHA-3, BLAKE2 and BLAKE3. Symmetric algorithms are DES, Advanced Encryption Standard (AES, Rijndael), MARS, Triple DES (3DES), Educational Data Encryption Standard (E-DES), Blowfish Encryption, SEAL Algorithm, RC2, RC4, RC6, Twofish, Serpent, IDEA, CAST, HiSea and asymmetric algorithms include RSA, ECC, ElGamal Encryption System(DSA), Diffie-Hellman, XTR.

On the basis of the input data, encryption algorithms are classified as *block ciphers*, in which the size of the block is of fixed size for encryption and *stream ciphers* in which a continuous stream is passed for encryption and decryption. RC2, AES, DES, RC6 and BLOWFISH are some of the examples of block cipher. In a symmetric algorithm high security can't be achieved as it makes use of the same key for both encryption and decryption, hence asymmetric algorithms are used. It is also known as Public key encryption. [1],[2],[3],[4] A new approach is to use chaotic dynamics in cryptography in two ways: To generate pseudo-random sequences, which are used as keystreams to mask the plaintext and corresponds to stream ciphers. To use as initial state and the ciphertext follows from the orbit being generated, in block ciphers. Also they are being proposed for hashing, key-exchange protocols, authentication, etc.

- Symmetric algorithms

Symmetric keys encryption only uses one key to encrypt and decrypt data. The key should be distributed before transmission between entities.[5]

Below, a comparison between the different symmetric algorithms is presented [6],[7].

Algorithm	***DES***	***AES***	***3DES***	***MARS***	***TEA***
Key Size(bits)	56 + 8 parity	128, 192, 256	112 or 168	128, 192, 256	128
Block Size(bits)	64	128	64	128	64
Round	16	10, 12, 14	48	32	Varies
Encryption Speed	Slow	Fast	Very Slow	Fast	Slow
Level of Security*	A	E	A	H	H
Effectiveness**	Slow in	Ef in	Slow in	E in	Ef in H

	S&H	S&H	S	S&H	
Attacks***	B	S	B, KP, ChP	MM	ChP, RK
Algorithm	***Blowfish***	***SEAL***	***RC2***	***RC4***	***RC6***
Key Size	32-448	160	8,128,64	Varies	128-256
Block Size	64	32	64	40-2048	128
Round	16	2	16	256	20
Encryption Speed	Fast	Fast	Very slow	Fast	Fast
Level of Security	E	M	G	G	G
Effectiveness	E in S	E in S	Slow in S	E in S	Ef in S
Attacks	D	Not yet	Df, L	BEAST	C
Algorithm	***Twofish***	***Serpent***	***IDEA***	***CAST***	***HiSea***
Key Size	up to 256	128, 192, 256	128	40 to 128	1-4096 set of int
Block Size	128	128	64	64	64
Round	16	32	8.5	12 /16	4
Encryption Speed	Fast	Slow	Slow	Slow	Fast
Level of Security	H	A	H	E	M
Effectiveness	E in S&H	Slow in S&H	Ef in S&H	Slow in S&H	E in S
Attacks	TD	R, L	W	KP, ChP	Not yet

*M: Moderate, A: Adequate, G: Good, E: Excellent, H: High
**S: Software, H: Hardware, Ef: Effective, E: Efficient
***B: Brute force, S: Side channel, KP: Known plain text, ChP: Chosen plain text, MM: Meet in the middle, D: Dictionary, Df: Differential, L: Linear, C: Correlation, R: Rectangle algebraic, TD: Truncated differential, W: Weak key, RK: Related key

Main usages of symmetric key algorithms are:

- ➢ Confidentiality is achieved as encryption and decryption is performed using a single key.
- ➢ Integrity and source authentication is achieved by using Message Authentication Codes because the MAC is generated and validated by the same key.
- ➢ Generation of pseudo random numbers [8]

AES meets U.S. Government requirements for HIPAA data protection and FINRA standards for protecting financial records[9]. Regarding the power consumption, it is the best symmetric algorithm for Raspberry Pi 3. With regard to the energy cost, It is more efficient than DES , with a better security level than DES or 3DES[10]. 3DES is now considered obsolete, but is still used by some IoT products because of its compatibility and flexibility.What Triple DES does well is protect against brute force attacks. Twofish is efficient on computers with lower capacity processors and IoT device smart cards[9].

Blowfish is superior to AES in terms of the throughput, and encryption time in small messages.

- Asymmetric algorithms

Asymmetric cryptography, also known as public-key cryptography, uses a pair of keys, one public and one private, to encrypt and decrypt.

RSA:
Features: Excellent security, Slow.
Possible attacks: Guessing d, Cycle, Common Modulus, Faulty Encryption, Low Exponent, Factoring the Public Key

ECC:
Features: Excellent security, Fast.
Possible attacks: Side-channel, Backdoors, Invalid curve

ElGamal(DSA):
Features: Efficient security, Fast.

McEliece:
Features: Excellent security, Fast.
Possible attacks: Brute-force/Unstructured, Structural, Side-channel, Timing, Power consumption

Diffie-Hellman:
Features: Good security, Slow.
Possible attacks: Dictionary, Denial of service, Outsider, Insider, Man in the Middle, Attacks Based on Number Theory, Degenerate Message, Simple Exponents, Simple Substitution, Timing

XTR:
Features: Excellent security, Fast.
Possible attacks: Side-channel, Collision

Basic uses of asymmetric algorithms are:

- ➢ Creation of digital signatures
- ➢ To establish/distribute session keys such as in case of TLS protocol

In previous works ECC and RSA for secure sockets layer (SSL) have been evaluated. ECC was shown to be faster especially when considering higher encryption standards.[11]

- Hash algorithms

Let ℓ, *n* be positive integers. We call *f* a hash function with *n*-bit output and ℓ-bit key if *f* is a deterministic function that takes two inputs, the first of arbitrary length, the second of length ℓ-bits, and outputs a binary string of length *n*. Formally, $H:\{0,1\}^{*}\times\{0,1\}^{\ell}\rightarrow\{0,1\}^{n}$.[12]

Different types of hash functions include: Based on block cipher, Based on modular arithmetic, Based on cellular automation, Based on knapsack problem, Based on algebraic matrices.

MD2, *MD4, MD5, SHA, BLAKE, HAVAL*, *RIPEMD, Whirlpool.*

Primary purposes of hash functions are:

- ➢ Generation and verification of digital signatures
- ➢ Checksum/Message integrity checks

- ➢ Source integrity services via MAC
- ➢ Derivation of sub-keys in key-establishment protocols & algorithms
- ➢ Generation of pseudorandom numbers

Hash algorithms have approximately similar throughput as the symmetric group. Between hash functions MD5 and SHA-1 have better speed, however because of security flaws they are not recommended anymore[10].

C. Lightweight Cryptography(LWC)

In the IoT area the main challenges are *minimum resources* which are hard to be secured, *low-energy* devices or *battery life* issues, *speed* and *power drain*. Between previously discussed algorithms just some of them could have all the features of speed, security level and effectiveness altogether to be used in IoT. So a new category of algorithms has been presented as lightweight cryptography(LWC). In comparison, from the input point of view, block cipher is preferred in resource-constrained IoT devices over stream cipher [13]. More than fifty symmetric LWC algorithms are proposed with focus on reducing cost (energy consumption, processing power, memory and physical area) and enhanced software and hardware performance (throughput, latency).

In following a comparison between the most important LWC algorithms is presented[13].

	Key Size	***Block Size***	***Software Efficiency*** *(Kbps/KB)*	***Hardware Efficiency*** *(Kbps/KGE)*
AES	128	128	132.9	23.6
PRESENT	128	64	35.91	127.38
RECTANGLE	-	-	-	167.68
MIDORI	-	-	-	259.4
mCrypton	96	64	14.41	12.91
NOEKEON	128	128	59.62	1.32
ICEBERG	-	-	-	68.76
PUFFIN-2	-	-	-	4.8
PRINCE	128	64	63.9	180.59
PRIDE	128	64	635.34	-
PRINT	80	64	33.12	198.8
Klein	80	64	3.36	25.32
LED	-	-	-	5.27
I-PRESENT	-	-	-	-
EPCBC	-	-	-	12.02
DESL	56	64	9.88	24.02
TEA	-	-	-	42.46
XTEA	128	64	28.97	-
Camellia	128	128	6.34	44.55
SIMON	96	48	1900	20.7
SEA	96	96	21.6	0.89
KASUMI	128	64	16.93	33.5
MIBS	64	64	1.63	143.26
LBlock	80	64	13.81	151.51
ITUbee	80	80	171.37	-
GOST	256	64	5.27	200
Robin	128	128	53.42	-
Fantomas	128	128	73.14	-
CLEFIA	128	128	5.84	28.37
PICCOLO	80	64	12.35	208.66
TWINE	80	64	10.58	118.42
SPECK	96	48	3511.19	13.57
IDEA	128	64	159.06	-
HIGHT	128	64	7.02	72.08
LEA	128	128	165.76	19.91
KATAN	80	64	10.36	15.58
KTANTAN	80	32	0	27.05
Hummingbird	128	16	7.57	-
Hummingbird-2	128	16	54.68	37.05

D. Quantum Cryptography

In quantum cryptography, a series of photons are used to send a message. If the message in destination is understood by its algorithm, it can be decoded. Otherwise the sender changes the series of photons and resends the message. Quantum cryptography is very expensive and has limited applications. The unit of information in traditional computers is bit which can be 0 or 1 while a quantum state which is named qubit is an element of a finite-dimensional complex vector space (or Hilbert space) H [14],[15].

E. Post-Quantum Cryptography

The rise of Quantum computers in recent years have given a major setback to classical schemes. RSA and ECC depend on integer factorization and discrete logarithm, which can be easily solved by quantum computers of sufficiently large size running the infamous Shor's Algorithm. Therefore cryptography schemes which are difficult to solve in both traditional as well as quantum computers are needed to be evaluated.

Types of post-quantum cryptography are:

- Public-key encryption:

  - Lattice based Cryptography(NTRU, Ring LWE, BLISS)
  - Code based Cryptography(McEliece, Niederreiter)
- Public-key signatures:
  - Multivariate Cryptography(Rainbow)
  - Hash based Cryptography(Lamport Signature, Merkle Signature)

Algorithm	***Hash-Based***	***Code-Based***	***Multivariate-Based***	***Lattice-Based***
*Schemes**	S	S, E, H	S, E	S, E, H, O, I, HE
Practical Speeds	Extremely Fast	Good	Under Test	Under Test
Advantages	Extreme Fast and Modular	Mature and Secure	Fast and Small Key Sizes	Excellent Security Robust Flexible
Disadvantages	Large Footprint Only Signature	Extensive Memory Requirements Variants Proven Insecure	Low Security	Not Fully Tested

* S: Signature, E: Encryption, H: Hash, O: Oblivious Transfer, I: Identity-Based Encryption, HE: Homomorphic Encryption[16]

- *Performance restrictions* - In this case the cryptography algorithms should have minimal cycles. The key exchange protocols that take up to several tens of ms in total can be suitable. Lattice-based schemes are the most efficient.
- *Memory restrictions*- They are systems like microcontrollers with several KB, smart cards as secure elements etc. All parameters and keys used should have moderate sizes and take reasonable-portion of memory (RAM, EEPROM) in nodes. Isogeny-based schemes such as isogeny-based Supersingular Isogeny Diffie-Hellman (SIDH) that employ supersingular elliptic curves offer short lengths of parameters and keys. On other hand, Multivariates such as Rainbow use secret and public keys having several tens of kB. The long keys are also used in code-based cryptography (e.g. the McEliece scheme).[17]
- *Restricted communication protocols*- This restriction requires that messages must keep minimal sizes during the key establishment. Code-based schemes that send hundreds kB length messages are not suitable in this scenario[17].

III. Discussion and Conclusion

In this article we reviewed all types of cryptography algorithms. In previous works, some main cryptography algorithms have been considered. From a security point of view physical algorithms are not secure so they are mostly used in watermarking and steganography and not in IoT particularly. In Mathematical group, block cipher type is preferable to stream cipher and the most efficient algorithm is AES. Although some others like IDEA, TEA, Twofish, Blowfish, DES and 3DES, RSA and ECC are used as well. In addition, a particular group of algorithms recently is presented for IoT devices as Lightweight algorithms which are more efficient for software and hardware. With the rise of quantum computers more secure algorithms have appeared and classic ones are at risk of being broken. So, the post-quantum group of algorithms has been presented. In this group, the lattice-based schemes seem to be promising for various scenarios in IoT due their efficiency and relatively reasonable lengths of keys and parameters.

References

[1] O.Abood, S.Guirguis, *A Survey on Cryptography Algorithms*. International Journal of Scientific and Research Publications. 8. 495-516. 10.29322/IJSRP.8.7.2018.p7978.

[2] M.Mushtaq et al. *A Survey on the Cryptographic Encryption Algorithms*. International Journal of Advanced Computer Science and Applications. 8. 333-343,2017

[3] S.V. Swathi, P.M. Lahari, B.A. Thomas. *Encryption Algorithms: A Survey*, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016), Vol. 4, Issue 2.

[4] C. Burwick and D. Coppersmith, *The Mars Encryption Algorithm*, NIST AES Propos., pp. 1–12, 1999, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.35.5887&rep=rep1&type=pdf.

[5] T. Nie and T. Zhang, *A study of DES and blowfish encryption algorithms*, IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, pp. 1–4, 2009, doi: 10.1109/TENCON.2009.5396115.

[6] S. Charbathia and S. Sharma, *A Comparative Study of Rivest Cipher Algorithms*, vol. 4, no. 17, pp. 1831–1838, 2014.

[7] M. Ubaidullah and Q. Makki, *A Review on Symmetric Key Encryption Techniques in Cryptography,* Int. J. Comput. Appl., vol. 147, no. 10, pp. 43–48, 2016, doi: 10.5120/ijca2016911203.

[8] A. M. Parker, *Differences between Hash functions, Symmetric & Asymmetric Algorithms*, October 27, 2017, Accessed on: March 25, 2021[online],Available:https://www.cryptomathic.com/news-events/blog/differences-between-hash-functions-symmetric-asymmetric-algorithms

[9] *Top 5 encryption algorithms for IoT,* May 16, 2019, Accessed on: April 2, 2021[online], Available: https://ubidots.com/blog/top-5-encryption-algorithms-for-iot/

[10] M. El-Haii, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of Cryptographic Algorithms on IoT Hardware platforms," 2018 2nd Cyber Secur. Netw. Conf. CSNet 2018, no. October, 2019, doi: 10.1109/CSNET.2018.8602942.

[11] F. Jonsson and M. Tornkvist, *RSA authentication in Internet of Things Technical limitations and industry expectations*, 2017.

[12] I. Mironov, *Hash functions : Theory, attacks, and applications Theory of hash functions*, Microsoft Res. Silicon Val. Campus, pp. 1–22, 2005, [Online]. Available: http://research.microsoft.com/pubs/64588/hash_survey.pdf.

[13] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, *Lightweight cryptography for IoT: A state-of-the-art,* arXiv, pp. 1–19, 2020.

[14] R. Kumar. *A Survey on Post-Quantum Cryptography for Constrained Devices*. International Journal of Applied Engineering Research. 14. 2608-2615. 2019.

[15] D. Bruss, G. Erdelyi, T. Meyer, T. Riege, and J. Rothe, 2007, ACM Computing Surveys, Vol. 39, No. 2, Article

[16] R. Asif, *IoT Post-Quantum Cryptosystems for Internet-of-Things : A Survey on Lattice-Based Algorithms*, pp. 71–91, 2021.

[17] L. Malina, L. Popelova, P. Dzurenda, J. Hajny, and Z. Martinasek, *On Feasibility of Post-Quantum Cryptography on Small Devices*, IFAC-PapersOnLine, vol. 51, no. 6, pp. 462–467, 2018, doi: 10.1016/j.ifacol.2018.07.104.