Scientific Research Publishing

Advances in Internet of Things, 2022, 12, 9-17
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

A Review of Lightweight Cryptographic Schemes and Fundamental Cryptographic Characteristics of Boolean Functions

Nahla Fatahelrahman Ibrahim[1], Johnson Ihyeh Agbinya[2]

[1]Faculty of Computer Science and Information Technology, Sudan University of Science and Technology (SUST), Khartoum, Sudan
[2]School of Information Technology and Engineering, Melbourne Institute of Technology, Melbourne Victoria, Australia
Email: nahla480@outlook.com, jagbinya@mit.edu.au

How to cite this paper: Ibrahim, N.F. and Agbinya, J.I. (2022) A Review of Lightweight Cryptographic Schemes and Fundamental Cryptographic Characteristics of Boolean Functions. *Advances in Internet of Things*, **12**, 9-17.
https://doi.org/10.4236/ait.2022.121002

Received: November 29, 2021
Accepted: January 16, 2022
Published: January 19, 2022

Abstract

In this paper, we survey a number of studies in the literature on improving lightweight systems in the Internet of Things (IoT). The paper illustrates recent development of Boolean cryptographic function Application and how it assists in using hardware such as the internet of things. For a long time there seems to be little progress in applying pure mathematics in providing security since the wide progress made by George Boole and Shannon. We discuss cryptanalysis of Boolean functions to avoid trapdoors and vulnerabilities in the development of block ciphers. It appears that there is significant progress. A comparative analysis of lightweight cryptographic schemes is reported in terms of execution time, code size and throughput. Depending on the schemes and the structure of the algorithms, these parameters change but remain within reasonable values making them suited for Internet of things applications. The driving force of lightweight cryptography (LWC) stems mainly from its direct applications in the real world since it provides solutions to actual problems faced by designers of IoT systems. Broadly speaking, lightweight cryptographic algorithms are designed to achieve two main goals. The first goal of a cryptographic algorithm is to withstand all known cryptanalytic attacks and thus to be secure in the black-box model. The second goal is to build the cryptographic primitive in such a way that its implementations satisfy a clearly specified set of constraints that depend on a case-by-case basis.

Keywords

Internet of Things, Lightweight Cryptographic Scheme, Vectorial Boolean Functions, IoT Differential Cryptanalysis

1. Introduction

Data security is an important issue in any wireless cryptographic protocol; a cryptographic algorithm is an essential part of network security. One of the breakthrough techniques is "Lightweight Cryptography (LWC)". A lightweight cryptographic scheme is suitable for implementation in resource-constrained environments such as RFID, sensor networks, healthcare, IoT, cyber-physical systems, distributed control systems, indicators, meters, custom controls, smart energy systems, etc. [1]. However, most of the above IoT devices suffer from many limitations. They are resource-poor devices with limited computing power, battery (lifetime), memory, and computational speed. Therefore, a lot of attention needs to be paid to these devices, especially when it comes to data processing. The huge amount of data exchanged between all nodes in wireless networks brings new risks and more challenges. One of them is the limitation of resources (e.g., energy), and many other combinations of factors suffer from financial constraints. However, the share of resources devoted to security is very small and represents only a fraction of the total resources available.

The structure of the paper is as follows: Section 2 discusses different types of cryptographic techniques. Section 3 briefly surveys various examples in the text that illustrate lightweight cryptographic algorithms for IoT. This paper should not consider as a comprehensive history of cryptology or the algorithms themselves, but rather a focused review on lightweight cryptography for IoT. Section 4 begins with a history of the notion of Boolean functions history, which attempts to illustrate their importance in the particular building blocks of symmetric cryptographic systems modern block ciphers, and also provides review includes cryptanalysis of Boolean functions. Finally Section 5 concludes the work.

2. Kind of Cryptographic Schemes

2.1. Lightweight Cryptographic Schemes

We define lightweight cryptography to have the following attributes, occupies less memory, small computational resources, and low energy consumption (when compared with state or the art standard cryptographic schemes such as AES, DES, RSA) to provide a security solution that can operate on resource-constrained devices. Lightweight cryptography is expected to be simpler and faster compared to traditional cryptography.

2.2. Heavy Cryptographic Schemes

Heavyweight cryptography systems such as DES and AES are not suitable for IoT scenarios as their resources such as energy and real-time execution are limited. Therefore, lightweight cryptography solutions are well desirable for IoT.

3. A Lightweight Cryptographic Scheme for IoT

In [2], the authors proposed a family of new lightweight variants of DES (Data Encryption Standard), which are called DESL/DESX/DESXL (lightweight mod-

ified versions of the well-known DES). The main idea of the new variants of DES is to use just one S-box recursively, instead of eight different S-boxes in order to minimize the hardware implementation.

A study in [3] presented PRINCE in 2012, which provides a new dimension to lightweight cryptography by achieving low latency. It also focuses on hardware implementation. It utilized 128 bits key and comprised of 64 bits block with 12 rounds. The S-box of this cipher was non-linear *i.e.* it used Feistel structure. The main advantage of the Feistel structure is that the same program code can be used for the encryption and decryption process. It also helps in reducing the usage of memory. Unfortunately the cipher can be susceptible to related-key attacks if the Feistel structure utilizes alternating keys. Some other lightweight cryptographic schemes noteworthy to mention from this generation are Humming-Bird, KASUMI, and Piccolo.

A study in [4] have shown a simple, lightweight block cipher, SIMON, and SPECK in 2015 that performs on heterogeneous platforms with ease due to its inherent simplicity.

In [5] was presented in 2015. Notably is appropriate for RFID tags and WSN etc. The main idea in the design of Simeck is use of a slightly simplified version of the round function of Simon by changing shift numbers in order to realize an acceptable trade-off between hardware performance and security.

In [6], the authors proposed lightweight design choices for LED-like block ciphers. In this work, 4×4 Serial matrices are preferred choice for building diffusion layers of lightweight block ciphers in order to satisfy the optimization of a reduced area in hardware designs.

In a study [7], authors elaborated on various aspects of lightweight cryptography (LWC). The authors purposed a lightweight hybrid algorithm for IoT devices. It tells which LWC algorithm should be used on a specific device. This decision is made on the basis of memory storage, and power of the device alongside the computational power required for the LWC algorithm. This article covered the timeline until 2016.

In [8], authors proposed a simplified new version of the round function of the original Simon by reducing its impact by changing the shift numbers, so the first rotation is removed in order to enhance the speed of SIMON and execution time.

In [9], authors proposed a new and robust version of the original XXTEA by employing an improved S-box in order to enhance security to overcome such key-related and chosen-plaintext attacks.

Based on the literature survey conducted, some lightweight symmetric algorithms are mentioned on the basis of block size, key size, structure, and the number of rounds.

Generally, a significant amount of focus in LWC has been on design of the S-box to match execution speed, code size, low energy consumption and resistance to attack.

Table 1 and Table 2 provide a comparative overview of some lightweight cryptography schemes. The first table provides evidence on their structures which determine the outcomes in Table 2. Interestingly the execution times are very small typically less than 2.65 milliseconds for all of them. Simon and PRESEN have the highest code sizes of 1510 bytes and 936 bytes respectively which can fit fairly well in current IoT devices. They also require very little power to process them. Twine has the highest throughput of 1304 kilo bytes per second.

Table 1. Summary of the list of some lightweight cryptographic algorithms.

Algorithm	Block size	Key size	Structure	No. of rounds
AES [10]	128/192/256	128	SPN	10/12/14
DESL [2]	64	184	Feistel	16
Twine [11]	64	80/128	Feistel	32
PRESEN [12]	64	80/128	SPN	31
HIGHT [13]	64	128	GFS	32
Simon [8]	32	64	Feistel	32

Table 2. Comparison of lightweight cryptographic algorithms.

Algorithm	Execution time (μs)	Code size (bytes)	Power consumption (μm)	Throughput (kbs@100kHz)
AES-128 [10]	2.606	12.40	-	-
DESL [2]	-	3.192	0.18	44.40
Twine [11]	592.87	-	-	1304
PRESEN [12]	2648.65	936	0.18	200.00
HIGHT [13]	-	5.672	0.25	188.20
Simon [4]	105.67	1510	0.13	35.6
SPECK [4]	49.02		0.13	4.2
Simeck [5]	-	-	0.065	5.6
PRINCE [3]	-	-	0.13	529.9

4. Boolean Functions Fit Lightweight Cryptographic Schemes

4.1. Bit of History

Boolean function was introduced about 150 years ago by the English mathematician George Boole (1815-1864) in the context of the foundations of mathematics and mathematical logic as one of the most fundamental objects of study in pure and applied mathematics and computer science. Boole's treatment of the algebra of logic (now known as Boolean algebra) in his work "The Laws of Thought"

[14] laid the foundation for the development of modern digital computer circuits. Claude Shannon (1916-2001) was a gifted electrical engineer and mathematician. Claude worked on his mathematical theory of communications at the Advanced Study Institute in Princeton in 1940-41. During the world war years he worked at Bell Labs on fire control; he continued his work on communications and also on cryptography. Based on his nascent communication theory, he created a mathematical foundation for cryptography in 1945.

4.2. Cryptographic of (Vectorial) Boolean Functions

Boolean functions are the building blocks of symmetric cryptographic systems. Boolean functions are found almost everywhere. In symmetric cryptography, we find Boolean functions in stream ciphers, in S-boxes in block ciphers. Little is known about similar trapdoor avoidance properties in block ciphers. In cryptography, confusion and diffusion are two properties of the operation of a secure cipher identified by Claude Shannon in his 1945 secret report a "Mathematical Theory of Cryptography" [15]. Some of the properties belonging to Boolean functions actually affect the properties of the cipher. This is of course true for the resistance to some attacks such as linear cryptanalysis, which was actually intended for the block cipher. The properties of the S-boxes affect the resistance of the cipher. But there is also some implementation properties that arise from the Boolean functions used in the cipher. Let $n, m \in \mathbb{N}$. A function $\mathbb{F}_2^n \to \mathbb{F}_2$ with

$$\left(x_1, \cdots, x_n\right) \to f\left(x_1, \cdots, x_n\right) \tag{1}$$

be called a Boolean function. Similarly, a Vectorial Boolean function or (vector-valued Boolean function) is a function $\mathbb{F}_2^n \to \mathbb{F}_2^m$ with

$$\left(x_1, \cdots, x_n\right) \to \left(f_1\left(x_1, \cdots, x_n\right), \cdots, f_m\left(x_1, \cdots, x_n\right)\right) \tag{2}$$

The functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ are also called the coordinate functions of *f*.

4.3. Cryptanalysis of Boolean Functions

A study in [16], one of the most important cryptographic criteria for Boolean functions used in block ciphers is called the generalization of the Strict Avalanche Criterion (SAC). The concepts of completeness and avalanche can be combined to define a new property, which we will call the strict avalanche criterion. A cryptographic function is said to satisfy the SAC if each output bit changes with probability one-half when a single input bit is added. The ideas of completeness and avalanche effect were first introduced by [17] and [18], respectively.

In [19], authors presented a new criterion called Global Avalanche Characteristics (GAC) to measure the global avalanche properties of cryptographic functions. In this work, two indicators for the new criterion were introduced. One predicts the cross sum and the other predicts the absolute avalanche characteristics of a function. However, in order to achieve good diffusion, cryptographic

functions should achieve low scores on both indicators.

In [20], authors presented in this work the first powerful cryptanalysis technique applied to symmetric key block ciphers: differential cryptanalysis. In the subsequent work [21], they cracked the FEAL cipher and recently they succeeded in cracking the full 16-round DES cipher by attacking with selected plaintexts [22].

Linear cryptanalysis was presented by [23] as a theoretical attack on the Data Encryption Standard (DES) and later successfully used in practical cryptanalysis of DES [24].

A study in [25] introduced a new type of attack, the algebraic attack, which was also presented in [26] [27]. Algebraic attacks involve recovering a secret key by solving over-defined systems of algebraic multivariate equations over GF (2). To defend against such attacks, many authors have focused on proposing Boolean functions that do not have a good linear approximation and are correlation-immune with respect to a subset of several input bits, see for example [28].

In a study [29], authors A elaborated on aspects of cryptographic properties of 4-bit S-boxes with Generation and Analysis of crypto secure S-boxes such as Output Bit Independence Criterion (BIC), SAC, Higher order SAC, Extended SAC, Linear Cryptanalysis, Differential Cryptanalysis, and Differential Cryptanalysis as well as Linear Approximation Analysis. It tells 4-bit S-boxes are better S-boxes than the 32 4-bit DES S-boxes. Boolean functions are in general lead to fast small times due to operating speeds on binary values rather than integers.

5. Conclusions

A number of studies related to the design of lightweight cryptographic schemes have been reviewed. A brief history of Boolean function has been expressed, for shedding light on this function's progress and applications. The role of Boolean function in lightweight cryptography has been recognized with accompanying application to IoT.

Future application opportunities for Boolean function in IoT are expected to increase as demonstrated recently and used in a wide area. **Table 1** compares the system parameters for the schemes reviewed. Apparently, the size of the key and cryptographic architectures are determinants for the processing times. The performance of lightweight cryptographic schemes is provided as a guide in the choice of application for chosen IoT devices and networks.

Acknowledgements

We thank Prof. Johnson Ihyeh Agbinya for his contributions for many useful comments and his encouraging this work.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Kiran Kumar, V.G., Mascarenhas, S.J., Kumar, S. and Viven Rakesh, J.P. (2015) Design and Implementation of Tiny Encryption Algorithm. *Journal of Engineering Research and Applications*, 94-97. http://academia.edu

[2] Leander, G., Paar, C., Poschmann, A. and Schramm, K. (2007) New Lightweight DES Variants. 14th *Annual Fast Software Encryption Workshop* (*FSE* 2007), Luxembourg, 26-28 March 2007, 196-210. https://doi.org/10.1007/978-3-540-74619-5_13

[3] Borghof, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S. and Yalçın, T. (2012) PRINCE—A Low-Latency Block Cipher for Pervasive Computing Applications. *International Conference on the Theory and Application of Cryptology and Information Security*, Beijing, 2-6 December, 208-225. https://doi.org/10.1007/978-3-642-34961-4_14

[4] Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J. and Wingers, L. (2013) The SIMON and SPECK Lightweight Block Ciphers. *Proceedings of the 52nd Annual Design Automation Conference*, San Francisco, 7-11 June 2015, Article No. 175. https://doi.org/10.1145/2744769.2747946

[5] Yang, G., Zhu, B., Suder, V., Aagaard, M.D. and Gong, G. (2015) The Simeck Family of Lightweight Block Ciphers. *International Workshop on Cryptographic Hardware and Embedded Systems*, Saint Malo, 13-16 September 2015, 307-329. https://doi.org/10.1007/978-3-662-48324-4_16

[6] Sarkar, S., Syed, H., Sadhukhan, R. and Mukhopadhyay, D. (2017) Lightweight Design Choices for LED-Like Block Ciphers. *International Conference on Cryptology in India*, Chennai, 10-13 December 2017, 267-281. https://ia.cr/2017/1031 https://doi.org/10.1007/978-3-319-71667-1_14

[7] Singh, S., Sharma, P.K., Moon, S.Y. and Park, J.H. (2017) Advanced Lightweight Encryption Algorithms for IoT Devices: Survey, Challenges and Solutions. *Journal of Ambient Intelligece & Human Computing*. https://doi.org/10.1007/s12652-017-0494-4

[8] Alassaf, N., Gutub, A., Parah, S.A. and Al Ghamdi, M. (2018) Enhancing Speed of SIMON: A Light-Weight-Cryptographic Algorithm for IoT Applications. *Multimedia Tools and Applications*, **78**, 32633-32657. https://doi.org/10.1007/s11042-018-6801-z

[9] Ragab, A.A.M., Madani, A., Wahdan, A.M. and Selim, G.M.I. (2021) Design, Analysis, and Implementation of a New Lightweight Block Cipher for Protecting IoT Smart Devices. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02782-6

[10] Anderson, R., Biham, E. and Knudsen, L.R. (1998) Serpent: A Proposal for the Advanced Encryption Standard. NIST AES Proposal. https://networkdls.com

[11] Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E. (2012) TWINE: A Lightweight Block Cipher for Multiple Platforms. *International Conference on Selected Areas in Cryptography*, Windsor, 15-16 August 2012, 339-354. https://doi.org/10.1007/978-3-642-35999-6_22

[12] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y. and Vikkelsoe, C. (2007) PRESENT: An Ultra-Lightweight Block Cipher. *International Conference on Cryptographic Hardware and Embedded Systems*, Vienna, 10-13 September 2007, 450-466. https://doi.org/10.1007/978-3-540-74735-2_31

[13] Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J. and Chee, S. (2006) HIGHT: A New Block Cipher Suitable for Low-Resource Device. *International Workshop on Cryptographic Hardware and Embedded Systems*, Yokohama, 10-13 October 2006, 46-59. https://doi.org/10.1007/11894063_4

[14] Boole, G. (1958) An Investigation of the Laws of Thought on Which Are Founded the Mathematical Theories of Logic and Probabilities. Walton and Maberly, London, 1854; Reprinted with Corrections, Dover Publications, New York. https://doi.org/10.5962/bhl.title.29413

[15] Shannon, C.E. (1945) A Mathematical Theory of Cryptography. Bell System Technical Memo MM 45-110-02, September 1. https://evervault.com/papers/shannon.pdf

[16] Webster, A.F. and Tavares, S.E. (1986) On the Design of S-Boxes. *Conference on the Theory and Application of Cryptographic Techniques*, Santa Barbara, 18-22 August 1985, 523-534. https://doi.org/10.1007/3-540-39799-X_41

[17] Kam, J.B. and Davida, G. I. (1979) Structured Design of Substitution Permutation Encryption Networks. *IEEE Transactions on Computers*, **28**, 747-753. https://doi.org/10.1109/TC.1979.1675242

[18] Feistel, H. (1973) Cryptography and Computer Privacy. *Scientific American*, **228**, 15-23. https://doi.org/10.1038/scientificamerican0573-15

[19] Zhang, X.-M. and Zheng, Y. (1995) GAC—The Criterion for Global Avalanche Characteristics of Cryptographic Functions. In: Maurer, H., Calude, C. and Salomaa, A., Eds., *Journal of Universal Computer Science*, Vol. 1, Springer, Berlin, Heidelberg, 320-337. https://doi.org/10.1007/978-3-642-80350-5_30

[20] Biham, E. and Shamir, A. (1991) Differential Cryptanalysis of DES-Like Cryptosystems. *Journal of Cryptology*, **4**, 3-72. https://doi.org/10.1007/BF00630563

[21] Biham, E. and Shamir, A. (1991) Differential Cryptanalysis of FEAL and N-Hash. 1991 *Workshop on the Theory and Application of Cryptographic Techniques*, Brighton, 8-11 April 1991, 1-16. https://doi.org/10.1007/3-540-46416-6_1

[22] Biham, E. and Shamir, A. (1992) Differential Cryptanalysis of the Full 16-Round DES. *Annual International Cryptology Conference* 1992, Santa Barbara, 16-20 August 1992, 487-496. https://doi.org/10.1007/3-540-48071-4_34

[23] Matsui, M. (1994) Linear Cryptanalysis Method for DES Cipher. *Workshop on the Theory and Application of Cryptographic Techniques* 1993, Perugia, 9-12 May 1994, 386-397. https://doi.org/10.1007/3-540-48285-7_33

[24] Matsui, M. (1994) The First Experimental Cryptanalysis of the Data Encryption Standard. *Annual International Cryptology Conference* 1994, Santa Barbara, 21-25 August, 1-11. https://doi.org/10.1007/3-540-48658-5_1

[25] Courtois, N. (2003) Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. *Annual International Cryptology Conference* 2003, Santa Barbara, 17-21 August 2003, 177-194. https://doi.org/10.1007/978-3-540-45146-4_11

[26] Courtois, N. and Meier, W. (2003) Algebraic Attacks on Stream Ciphers with Linear Feedback. *International Conference on the Theory and Applications of Cryptographic Techniques* 2003, Warsaw, 4-8 May, 346-359. https://doi.org/10.1007/3-540-39200-9_21

[27] Faugére, J.-C. and Ars, G. (2003) An Algebraic Cryptanalysis of Nonlinear Filter Generators Using Grobner Bases. RR-4739, INRIA (National Institute for Research in Digital Science and Technology), Paris. https://hal.inria.fr/inria-00071848

[28] Camion, P., Carlet, C., Charpin, P. and Sendrier, N. (1991) On Correlation-Immune Functions. *Annual International Cryptology Conference* 1991, Santa Barbara, 16-20 August 1991, 86-100. https://doi.org/10.1007/3-540-46766-1_6

[29] Dey, S. and Ghosh, R. (2018) A Review of Cryptographic Properties of S-Boxes with Generation and Analysis of Crypto Secure S-Boxes. *PeerJ Preprints*, **6**, Article ID: e26452v1. https://doi.org/10.7287/peerj.preprints.26452v1