HOSTED BY unisel UNIVERSITI SELANGOR

Selangor Science &Technology Review
Special Issue: Science and Technology for Society
Vol 5 No 5 (2021)

A Systematic Literature Review on Lightweight Secured S-Box Design for mHealth Applications

Tasnuva Ali [1], A. H Azni [2], Nur Hafiza Zakaria [3]

[1] Daffodil International University
tasnuva@daffodilvarsity.edu.bd
[2] Faculty of Science and Technology, USIM
ahazni@usim.edu.my
[3] Faculty of Science and Technology, USIM
mzhafiza@usim.edu.my

Abstract: The process of designing powerful and secured S-Boxes is becoming an essential constituent in the field of modern cryptography. Different S-Box designs have been proposed to make it more suitable for IoT, mHealth and WBAN applications but proper implementation is still a deficient for their design complexity. In this paper, major criterions of S-Boxes for mHealth systems were conducted following a systematical literature review process and required findings were outlined. The paper also demonstrates the current designs in different areas like security, low power and less memory to find out the challenges and opportunities for designing a new S-Box in modern mHealth applications. Finally, the SLR also gives a research direction to choose major design properties of new S-Boxes for mHealth as well as IoT applications. After evaluating the result, this paper also suggested a composite S-Box with 3D design based on rotation, shifting and Galois Field 24 to (22)2 pipelining structure for less memory, power and secured applications. Thus, the intimation of Systematic Literature Review (SLR) is to give a clear concept to the future researchers in the area of composite 3D S- Box design in terms of security in mHealth applications.

Keywords: Systematic Review, mHealth, S-Box, Security.

1. Introduction

The mHealth has an enormous potential for promotion and easy communication on healthcare industry that supports private and public health service associated with wireless communication devices like cell phone, tablets and PDA's [1]. This mHealth system requires strong security to protect patient's privacy in wireless perception layer. As a result, cryptography is one of the most essential parts to ensure security of patients' sensitive data before sending in transmission medium. Moreover, the security of data relies on the encryption algorithm where the data is encrypting with a secret key [2]. Accordingly, the strength of the algorithm depends on the S-Box design to perform confusion of bits which is based on a nonlinear operation [3].

The massive quantity of researches and investigations has been conducted in the past decades to design a Look Up Table (LUT) based approach S-Boxes which have so many limitations in their own hardwires [4]. Besides, the mHealth system has a unique architectures, characteristics and applications which are not similar to traditional IoT or WBAN applications [5]. Thus, the recent studies have focused on different S-Box designs to meet various necessities like security, low power consumption and gate area diminution. However, the design of S-Box for mHealth system is more complex as it requires lightweight with minor number of gates, adequate security properties and low power utilization [6]. Moreover, 4X4 S-boxes are mainly suitable for lightweight algorithms as well as mHealth system for its compact hardware architecture and less memory constraint which security is not as much of 8X8 S-Boxes [7]. Therefore, this Systematic Literature Review aims to present upcoming challenges to design the secured S-box for mHealth applications in future. Consequently, the paper was evaluated systematically and the results were demonstrated considering the need of new strong S-Box design for IoT. This paper has also recommended a

new composite S-Box design with 3D rotation after appraising all the SLR reviews which is based on Galois Field theory to overcome all the demerits of current S-Boxes for IoT or mobile health applications.

Considering all the above belongings, the objectives of the SLR paper are considered; 1) to review different designs of S-Boxes systematically in IoT networks, 2) to analyze the methods and security parameters of different proposed models and 3) to focus open issues in S-Box security for future researchers.

The SLR are organized as follows: section 2 highlights the review methods. The analysis and results of the SLR were discussed in section 3 , section 4 finds research limitations and section 5 represents the conclusion of this SLR.

2. Review Method

The guidelines of a systematical literature review (SLR) are mainly focused on three segments that are: Planning, Conducting and Reporting of the review [8]. The first segment formulates research questions, selects sources and searches key words. The second segment is the inclusion-exclusion criterion which is measured as quality criterion in primary articles. And the last approach is used to select the primary studies for quality assessments of data extraction, monitoring progress and synthesis. In section 3, the selected studies in the previous parts are discussed in detail.

Fig 1. The steps in SLR.

2.1. Research Questions

The first step in a systematic review is to formulate the research questions (RQ) based on the primary studies in Table 1. In RQ1, the research question finds the answer of overall research trend in designing lightweight S-Boxes in IoT or mHealth applications. Based on RQ1, the published conferences and journal papers are identified dated since 2011 until 2020.The selected papers give the answer of RQ1 with identifying problems in the studies are also analyzed. With respect to RQ1, RQ2 evaluates the security approaches for S-Box with three different sub sections. Lastly, RQ3 provides the limitations of S-Box designing in security aspects, so that the recommendations give a clear overview in the area of IoT/mHealth security in future research.

Table 1. Research Questions

RQ#	Research Question Details
RQ1	What is the recent status of information on S-Box design in mHealth?
RQ2	How S-Box Security is analyzed in previous researches? RQ2.1 What are the S-Boxes design used for IoT applications? RQ2.2 What are the parameters/ used to evaluate S-Box security? RQ2.3 What are the recent improvements on designing lightweight S-Box security?
RQ3	What are the limitations of current studies in respect of security analysis in IoT/mHealth applications?

2.2. Objectives and Eligibility Criteria

The main objective of the Systematical Literature Review is to evaluate the existing S-Box architectures in terms of low gate area and faster speed by means of higher security necessities. This SLR also investigates the advantages and disadvantages of these existing architectures to find out the applicability of mHealth system in future. Thus, the eligibility criterias that will be addressed by SLR are:

- The recommended design for S-Box ensures better security compared to existing S-Box design.
- The proposed S-Box must be suitable for smart phones as well as IoT devices.

Accordingly, the evaluation process was structured as shown in fig. 2

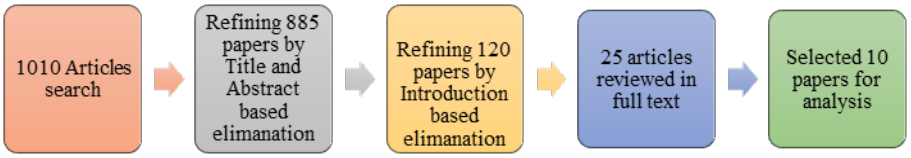

FIg 2. The Evaluation Process of SLR.

2.3. Search Strategy and Methodology

The unbiased search strategy is to find as many primary studies related to research questions with three eligibility criteria that are security, low gate area and low power for mHealth applications. Thus, the search strategies comprise to choose major researches from different electronic database such as

- IEEE
- SCOPUS
- ACM
- Springer

- Google Scholar

In this study, the primary search was based on three key words like mHealth, S-Box security and 3D algorithm design. Also, the review procedure was followed by Kithchenam's SLR that has the following steps:

- Set the research topic.
- Follow the exclusion and inclusion criteria to remove irrelevant and same research from database.
- Quality assessments of the research.

2.4. Inclusion-Exclision Criterion

The research articles are scanned following the inclusion and exclusion criteria to get the short list of primary articles. The Table 2 presents the inclusion and exclusion criteria.

Table 1. Research Questions

Number #	Inclusion criterion	Exclusion criterion
1.	LUP S-Box design, Composite S-Box, security analysis parameters of designing S-Box, 3D rotation policy are the main focal point to select the articles.	Articles were not focused on S-Box, 3D rotation and security analysis.
2.	Articles should cover the method used in strong S-Box design with NIST recommendations in IoT/mHealth applications.	Articles did not emphasis on S-Box design.
3.	Most recent articles were considered for improvement of S-Box design.	Articles did not support IoT applications.
4.	Peer- reviewed articles were considered.	Lecture Notes, duplicate articles, short articles were not considered for SLR analysis.

2.5. Quality and Qualitative Results

The principle of Quality Assessment in this review is to provide the limitations of each study related to S-Box design considering synthetic data analysis. Thus, the goal of the assessments is to eliminate articles that do not relate or involve the research and try to extract the relevant data from the selected researches based on Experiment or Design, Literature Review or Survey on Lightweight Algorithms and other categories. Moreover, the qualitative results were based on 35 articles; 16 of them provided secured S-Box design, 10 of them demonstrated small S-Box design, 7 of them presented less power S-Box design and the rest

of the reviews summarized the requirements to design the new lightweight S-Box design for future healthcare industry.

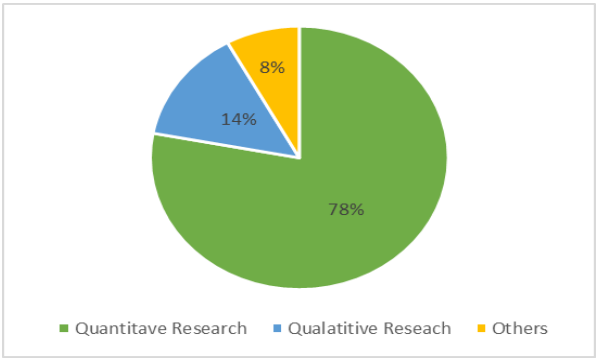

FIg 3. Data Analysis Graph.

3. Results and Discussions

3.1. Selected Articles

The total 120 articles are collected from peer reviewed journals, journals, conferences, proceedings, online book chapters, thesis, web page articles and technical reports. The articles that are matched with IoT security and secured S-Box designs are selected from 25 articles based on full article review process. Moreover, 10 more additional articles are chosen based on their abstract and title. Finally, 35 final selected articles are preferred as a primary study for this research.

3.2. IoT/ mHealth Research

- RQ1: What is the recent status of information on S-Box design in mHealth?

This study is based on number of articles with publication years which will be considered from 2011 to 2020 before the final assessment was done. From the graph, it can be seen that the number of papers on mHealth/ IoT topics were not the main concern in the early years of wireless researches because of its limited applications. When the IoT applications were increased, these studies are the most demanding research from year 2011 to 2020.

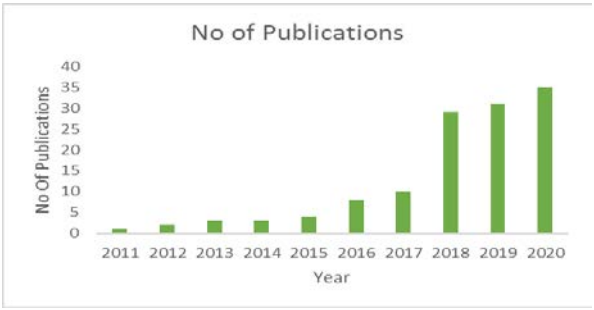

FIg 4. IoT/mHealth Research from year 2011 to year 2020

3.3. Lightweight Secured S-Box Research

- RQ2: How S-Box Security is analyzed in previous researches?

To answer RQ2 precisely, this study is divided into three sub sections to analyze the security in IoT/mHealth applications which depends on designing strong S-Box.

- RQ2.1: What is the S-Boxes design used for IoT/mHealth applications?

- Low Power S-Box for IoT/mHealth:

The traditional Look Up Table (LUP) based S-Box provides unbreakable delay, large size memory and gate area with more clock frequencies to operate. Some studies [6,9, 10, 29, 31,32, 33] among selected papers were focused on Galois Field based S-Box design to achieve the goal of low power requirements. In the study by D. K. Sushma and M. Devi [9] proposed a new S-Box that uses resource sharing multiplicative inverse module to accomplish the goal of less power consumption. The proposed architecture also showed 19.8 ns overall delay that consumes less power like 14 mW. Moreover, the proposed S-Box design is very well worked on cell phones or IoT devices for limited power consumption. This architecture is a mixture of LUT and SOP approach that gives faster speed but efficient in cost.

To achieve the low power design, the authors in [10] proposed a new design of S-Box that apply second orders reversible one-dimensional cellular automata (RCA^2) to overcome the limitations of LUT bases S-Boxes. The performance of S-Box was based on SAC, entropy, non-linearity and correlation immunity bias criteria. This new approach is also capable to consume low power and less energy for Wireless body network (WBAN) as well as mHealth applications.

- Composite S-Box for IoT/mHealth:

The design of S-Box also needs byte substitution and Inv byte substitution operation based on nonlinear transformation that transfers each byte to different value using S box and Inv S box table. This table needs much space to store all the possible values in memory. Therefore, the composite field arithmetic in finite fields (GF) method has been introduced which provides more advantages compared to conventional LUT method as the S box and Inv S box use same enable pin for both encryption and decryption. Thus, the identical hardware used for both operations which reduce number of gates as well as memory space (lightweight) which is one of basic requirements for mHealth system. To achieve the same goal, A. Prathiba and V. S. Kanchana proposed a new 4X4 non-linear S-Box that enables sub pipelining to reduce the gate equivalent area instead of LUT based S-Boxes [6]. This type of S-Box gives better result for differential and linear cryptanalysis compared to all lightweight ciphers. Moreover, a new approach has been used by M. Hanem and A. Omayma to construct small S-Boxes over 2^4 Galois Field. In the study, the S-Box was divided into small S-Boxes that has different equations [11]. Each Equation is extracted using three different irreducible

polynomials and requires 2048 bits storing capacity which occupies less memory than the existing architecture. Therefore, the speed of the recommended design is faster as well as suitable for small size applications.

- RQ2.2: What are the parameters/ used to evaluate S-Box security?

The first necessity of S-Box design is security issues that must be fulfilled by several cryptographic properties such as robustness (differential cryptanalysis), balancing, SAC (Strict Avalanche Criterion), nonlinearity (linear cryptanalysis), differential uniformity (differential cryptanalysis), linear approximation (linear cryptanalysis), algebraic complexity (interpolation attack), fixed and opposite fixed points (static cryptanalysis) and bit independent criterion [12]. However, the analysis of S-Box properties in block ciphers is still lacking because of specific guidelines and techniques to discover all attacks in a single S-Box collectively. Moreover, in their study, the authors also proposed a dynamic S-Box instead of static one because of use complex key arrangement which is difficult to break. This key has been changed in every round of the block cipher in dynamic design to ensure more security compared to static one. Finally, the authors suggested a new model or software that needs to be essential to analyze all the properties of S-Box properly to prove the security against all possible attacks.

In the study by S. Dey and R. Ghosh [13], the same approach they used but the goal is to apply a shifting property to construct a secured S-Box design based on SAC property for four bits Boolean Function (BF's). In this paper, the authors also summarized few new techniques to find the existing Linear Relations or Linear Approximations for a particular 4-bit S-Box that proves far better performance compared to 32, 4-bit S-Boxes.

- RQ2.3: What are the recent improvements on designing lightweight S-Box security?

Still in the area of security, N. H. Zakaria and R. Mahmod propose a new S-box algorithm, which seeks to enhance the security with adding one new function named as crossover and mutation process [14]. The authors also anticipate better security after passing the NIST test as the S-Box is capable to generate random outputs which give larger confusion and diffusion, signifying better performance compared to existing ones. One better solution to enhance the security of lightweight block cipher is 3D cipher design. The 3D design was first developed by J. Nakahara [15]. This 3D can improve the confusion and diffusion properties but increases the block and key size which may reduce the efficiency of the algorithm. Later on, P. R. Suri and S. S. Deora propose a new 3D rotation cipher design which gives satisfactory randomness property but great number of iterations with large key [16]. Lastly, [17] proposes a new 3D cipher which enhances security without increasing size of block and key.

4. Research Limitations

- RQ3: What are the limitations of current studies in respect of security analysis in IoT/mHealth applications?

Different cryptographic algorithms have been used to ensure security in different studies for IoT/mHealth applications but their implementation is still disputed for their hardware configuration [3-6, 12-23, 25, 26, 28]. Though the lightweight cipher provides better security, but at the same time experiences different attacks like impossible differential attack, related key attacks, key recovery attack, saturation attack etc. which can leakage information or hamper the security of the application. Hence a less power, low-cost and secured cryptographic algorithm must be selected to minimize all these attacks and requires consideration towards its confidentiality. In literature, A. Moradi et al. (2017) proposed 128 bits AES block cipher which gave high security for 256 large keys [18] but faced related key attacks. Moreover, P. Kumar Kushwaha presented a survey on lightweight TWIN which has small hardware and works good on embedded software [19] but faces saturation and meet in middle attacks. Also R. Beaulieu proposed SIMON and SPECK lightweight ciphers which give finest result both in hardware and software but facing Boomerang and Key Recovery attack [20]. W. Zhang proposed mHealth based smart home system which has good resistivity of Linear and Differential attack but facing related key and statistical saturation attack [21]. The most recent invention is lightweight ARX based SPARX algorithm for small memory devices and wide range applications for resource constrained devices but hardware implementation is not easy for high FOM [22]. Therefore, it is fundamental requirements to develop a secured S-Box which will meet the above requirements for recent IoT/mHealth applications.

5. Conclusion

In this study, a systematical literature review on mHealth S-Box design was addressed and the final outcomes were provided. According to SLR analysis for three different parameters as mentioned above, the future design for new S-Box of IoT/mHealth is composite one which is based on 2^4 Galois Field Theory. The composite S-Box with pipelining design is suitable for mHealth applications because of its low gate area as well as low power consumption. Moreover, this type of S-Box gives more security compared to LUT based S-boxes which values are predefined and also needs much area to store in device. With the composite S-Box, the 3D algorithm design may be added to enhance the security. The Composite S-Box with 3D combination can meet the requirements of security, less power and less area which are the primary requirements in IoT/mHealth applications. Thus, the final conclusion of the SLR is to design a new S-Box especially for mHealth applications that must be a combination of security, low power and less gate area. Moreover, this study also provides future scopes for improving the existing architecture based on the above three basic criterions.

6. References

[1] Matias, N., Sousa, M. J. (2016). Mobile Health as a Tool for Behaviour Change Chronic Disease Prevention. *11th Iberian Conference on Information Systems and Technologies (CISTI).*

[2] Mushtaq, A. M.,Jamel, S., Disina, A.H., Shakir, N.S.A.,Deris, M. (2017). A Survey on the Cryptographic Encryption Algorithms. *International Journal of Advanced Computer Science and Applications.*

[3] Biryukov, A., Perrin, L. (2017). State of the Art in Lightweight Symmetric Cryptography. *International Association for Cryptographic Research. Esch-sur-Alzette, Luxembourg.*

[4] Wong, M.M.,Wong, M.L.D., Nandi, A.K., Hijazin, I. (2011). Composite field GF $(((2^2)^2)^2)$ Advanced Encryption Standard (AES) S-box with algebraic normal form representation in the subfield inversion. *IET Circuits Dev. Syst. 2011, 5, 471–476.*

[5] Li, X., Ibrahim, M. H., Kumari, S., Kumar, R. (2018). Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors. *Telecommunication Systems, Springer*.

[6] Prathiba, A. and Bhaaskaran, V. S. K. (2018). Lightweight S- Box Architecture for Secure Internet of Things. *MDPI Journals*.

[7] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y. & Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher.*CHES, 4727, 450–466*

[8] Kitchenham, B. (2004). Procedures for Performing Systematic Reviews.*Technical Report TRISE-040J, Keele University, NICTA.*

[9] Sushma, D. K. and Devi, M. (2018). Design of S- box and INV S-box using composite Field Arithmetic for AES Algorithm. *International journal on Engineering Research and Technology (IJERT).*

[10] Gangadari, B. R., Ahamed, S. R. Design of cryptographically secure AES like S-Box using second order reversible cellular automata for wireless body area network applications.*IEEE international conference on EESCO.*

[11] El-Sheikh, H. M., El-Mohsen, O. A. (2012). A New Approach for Designing Key-Dependent S-Box Defined over GF (2^4) in AES. *International Journal of Computer Theory and Engineering Vol. 4, No. 2.*

[12] Mohamed, K., Pauzi, M. N. M. Study of S –Box Properties in Block Cipher. *International Conference on Computer, Communications, and Control Technology (I4CT).*

[13] Dey, S. and Ghosh, R. A review of Cryptographic Properties of S- Boxes with generation and Analysis of Crypto Secure S- Boxes. *Peer J Preprints 6:e26452v1.*

[14] Zakaria, N. H., Mahmod, R., Udzir, N. I., Zukarnain, Z. A. Enhancing Advanced Encryption Standard (AES) S-Box Generation Using Affine Transformation. *Journal of Theoretical and Applied Information Technology 72(1):18-22*

[15] Nakahara, J. (2008). 3D: A three-dimensional block cipher. *Proc. Int. Conf. Cryptol. Netw. Secur. Berlin, Germany: Springer, pp. 252–267*

[16] Suri, P. R. and Deora, S. S. (2011). 3D array block rotation cipher: An improvement using lateral shift. *Global J. Comput. Sci. Technol., vol. 11, no. 19, pp. 17–23.*

[17] Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., Daud, M. (2020).Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT. *IEEE.*

[18] Moradi, A., Poschmann, A. (2017). A very compact and a threshold implementation of AES. *Advances in Cryptology, Springer, vol. 6632, p. 69-88.*

[19] Kushwaha, P. K. (2014). A survey on lightweight block ciphers. *International Journal of Computer Applications, vol. 96, p. 1-7.*

[20] Beaulieu, R., Shors, D. (2015). The simon and speck lightweight block ciphers. *Proceedings of the 52nd Annual Design Automation Conference.*

[21] Zhang, W., Bao, Z. (2015). RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *China Information Sciences, vol. 58, pp 1-15.*

[22] Dinu, D., Perrin, L. (2017). SPARX: a family of arx-based lightweight block ciphers provably secure against linear and differential attacks. *proceedings of Asiacrypt16.*

[23] Kotz, D., Gunter, C. A., Kumar, S., Weiner, J. P. (2016). Privacy and security in mobile health: a research agenda. *Computer, vol. 49, issue: 6.*

[24] Akishita, T., Hiwatari, H. (2012).Very compact hardware implementations of the blockcipher CLEFIA. *Selected Areas In Cryptography Lecture Notes in Computer Science Springer, p. 278-292.*

[25] Patel, S. T., Mistry, N. H. (2015). A survey: lightweight cryptography in WSN. *International Conference on Communication Networks (ICCN). IEEE.*

[26] Usman, M., Ahmed, I. (2017). SIT: a lightweight encryption algorithm for secure internet of things. *International Journal of Advanced Computer Science and Applications, vol. 8, no. 1.*

[27] Liu, J., Bai, G. and Wu, X. (2016). Efficient hardware implementation of roadrunner for lightweight application. *Proc. IEEE Trustcom/BigDataSE/ISPA, pp. 224–227.*

[28] Guo, X., Hua, J., Zhang, Y. and Wang, D. (2019). A complexity-reduced block encryption algorithm suitable for Internet of things. *IEEE Access, vol. 7, pp. 54760–54769.*

[29] Biswas, A., Majumdar, A., Nath, S., Dutta, A. and Baishnab, K. L. (2020).LRBC: A lightweight block cipher design for resource constrained IoT devices. *J. Ambient Intell. Humanized Comput., pp. 1–15.*

[30] Singh, P., Acharya, B. and Chaurasiya, R. K. (2019). A comparative survey on lightweight block ciphers for resource constrained applications. *Int. J. High Perform. Syst. Archit., vol. 8, no. 4, pp. 250–270.*

[31] Yedav, R., Sharma, R. M. (2018). Efficient Energy Utilization in Internet of Things (Iot) Network. *International Journal of Management Systems and Management Science, vol.. 1, no 2.*

[32] Henkel, J., Pagani, S., Amrouch, H., Bauer. (2017). Ultra-Low Power and Dependability for IoT Devices. *Design, Automation and Test in Europe Conference, Switzerland.*

[33] Rekha, C., Krishnamurthy, G. N. (2020). Area and Power Optimized AES For Iot Applications Using Dual Port ROM Based S-Box and Security By Optimized Key Scheduling Algorithm.*International Journal of Scientific and Technology Research, vol.9.*

[34] Maitra, S., Yelamarthi, K. (2019). Rapidly Deployable IoT Architecture with Data Security. *Implementation and Experimental Evaluation. Sensors.*

[35] Shanthini, N., Rajasekar, P., Mangalam, H. (2014).Design of low power S-Box in Architecture Level using GF.*International Journal of Engineering Research and General Science, Vol. 2.*

[36] Rashidi, B. (2021). Compact and efficient structure of 8-bit S-box for lightweight cryptography. *ScienceDirect, Vol. 76.*

[37] Liu, Y., Wu, N., Zhang, X. , Zhou, F. (2017). A new compact hardware architecture of S-Box for block ciphers AES and SM4. *IEICE Electronics Express, Vol.14.*

atics and its applications. New York: Random House, Inc.