A Security And Performance Review of IoT Encryption Algorithms

Hesham Hasan, Ghassan Ali, Wael Elmedany, Chitra Balakrishna
College of IT
University of Bahrain
Sakhair, Kingdom of Bahrain
syedhisham242@gmail.com
ghassan.juma@live.com
welmedany@uob.edu.bh
balakris@edgehill.ac.uk

ABSTRACT: *Internet of Things (IoT) is a trending new technology based on networking and microcomputing. It transfers normal devices into smart devices capable of communicating with other devices and the Internet. IoT-enabled devices are often resource-constrained devices. They have weak processors, small memory and low power supply. This hindered the implementation of the same security protocols and standards used in normal computing devices for IoT. A solution on the horizon is within the field of lightweight cryptography (LWC). The new field aims to provide algorithms optimized for IoT while assuring proper levels of security. This paper aims to review four LWC algorithms which were proposed in ISO/IEC 29192 standard: SIMON, SPECK, PRESENT, and CLEFIA. The review is made based on levels of security and performance of the algorithms on IoT-enabled devices. Several recommendations are then deduced from the review.*

Keywords: Internet of things, Lightweight Cryptography, SIMON, SPECK, PRESENT, CLEFIA, Security, Performance

Received: 28 January 2022, Revised 4 March 2023, Accepted 22 March 2022

DOI: 10.6025/dspaial/2022/1/2/84-92

1. Introduction

Internet of things is a trending buzzword nowadays. Imagine a world where electronic dumb devices like microwave ovens and transform into smart devices that can communicate and share data about themselves and their surroundings. The future is now possible with this emerging technological advancement.

Internet of Things (IoT) is defined as the network of physical items that allows the items to communicate data with each other. It enables items, dubbed “Things”, to have a brain of their own and sense their surroundings. IoT devices range from smart home appliances and wearable monitors to connected cars and smart traffic systems.

The motivation for developing IoT came from the need of individuals, business and governments to run efficiently and to make an optimized usage of their resources. To enable that, data must collected at multiple stages of business and everyday processes, and then analyzed. The resulting information allows better decision making.

Many entities can use and benefit from IoT. It can bring cost-savings to businesses, better governance to governments, and easier living to individuals. However, IoT implementations are riddled with some challenges that need to be overcome in order to minimize the risks. One of the main challenges is that resources are limited.

IoT-enabled devices are resource-constrained devices, meaning that they often have low processing power, smaller memory capacity and higher energy usage limitations. Usually, the devices should communicate with other devices that have a higher security standard. IoT devices may not be able to comply with certain security standards due to the aforementioned issues.

It is essential to secure IoT-enabled devices because of the sensitivity of data they collect. Data leakages can harm individuals, businesses and governments. A major concern comes from vulnerabilities in IoT which hackers may exploit to gain access to private user data. Another concern is that due to the infancy of the technology, there is a lack of standards and proper regulations to provide guidance in basic security issues such as access control, patching, and so on.

Not just that IoT-enabled devices collect and share data, but they also do so over the internet. That means that they are connected to a public network with thousands of potential adversaries while they are using security protocols weaker than everyday computers. This way, the devices are exposed to a wide variety of attacks that need to be mitigated or prevented. An important factor to help in achieving that purpose is to provide confidentiality of data, that is to make sure adversaries cannot read the communicated data without authorization.

To achieve confidentiality, encryption is used in communications between any two parties. Advanced encryption Standard (AES) is a common encryption algorithm used by most computers and servers. For key transport, RSA and DH algorithms are usually used, and for integrity there are SHA hashing algorithms. However, the computational load needed to run those algorithms is beyond the processing capability of most IoT devices.

High computational and other resource overheads in IoT have led to the development of a new branch of cryptography: Lightweight cryptography (LWC). The branch is mostly concerned with developing new cryptographic algorithms and techniques specifically for resource-constrained devices to enable them to achieve an acceptable level of security. LWC schemes aim to match standards used in normal computers with minimal compromises in security while pushing for high performance. This paper will attempt to analyze four cryptographic algorithms which are underway to becoming the standard of LWC. They were proposed to be adopted into ISO/IEC 29192 standard of LWC. The algorithms are: SIMON, SPECK , PRESENT, and CLEFIA.

The rest of the paper is divided as follows: Section 2 presents an overview of the latest related work that has been done in the field of LWC, Section 3 state the current situation of LWC algorithms segregated by their different purposes, Section 4 discusses each of the four ISO/IEC 29192 algorithms in detail along with their security and performance aspects, and Section 5 concludes the research with a summary of the findings and recommendations for future work.

2. Literature Review

Lack of IoT security has been recognized as one of the most critical threats to consumers. That is due to the widespread use of those devices and adversary attacks including a recent attack which utilized a network of IoT-enabled devices to launch DDoS attacks with throughput up to 1TB/s, as per reports. A number of researchers proposed ways to enhance the security of IoT-enabled devices. [1] conducted a study of IoT threat models and developed a framework for embedded device security for IoT devices. The proposed framework is in its early stages. It lacks proper reviews by review and standardization.

Another solution was proposed by [2]. Their paper presents a survey of IoT challenges and opportunities focusing on the security issues and proposes a new public-key cryptographic scheme known as digital physical unclonable function (PUF). The technique serves as a fingerprint for uniquely identifying an IoT-enabled device. However, the digital PUF requires more study in order to determine its feasibility and in general, the use of public key cryptography consumes a lot of resources.

Over the years, many projects were initiated to address the weak points in IoT security. Most of the projects were described and compared in a publication by [3]. The research aimed to provide recommendations regarding which are the best holistic approaches that assure authentication, confidentiality, access control, privacy and other guarantees. The research concludes that a unified solution to provide all the assurances is still missing but suggests solutions which provide the most desirable

features. Our research will focus on addressing the confidentiality techniques rather than suggesting a holistic view. The techniques described in our research are compatible with the projects mentioned by the project review paper.

Most researches that were reviewed have stated the importance of using different encryption algorithms to achieve the security objectives in resource-constrained devices. We introduce a novel class of cryptography algorithms called lightweight cryptography. [4] provides a summary of the main security issues related to IoT devices including the current state of research on each problem. Among the issues highlighted in the paper is the selection of an appropriate security protocol for IoT communications. It is suggested that due to the lack of adequate resources in terms of computational power and energy usage, public-key cryptosystems remain hard to integrate within IoT. Such cryptosystems are said to take large overheads as compared to symmetric-key cryptosystems, which are easier to adopt but nevertheless still heavy on resource use. Since public-key cryptosystems are essential for proper source authentication and symmetric-key cryptosystems are preferred for normal communications, research is directing towards reducing the overheads and the overall complexity of all types of cryptographic algorithms. Lightweight alternatives exist for both public-key and private-key schemes.

A recent overall review of lightweight encryption algorithms for IoT was done by [5]. The paper classifies the most desirable features of a lightweight block cipher as: smaller block sizes, smaller key sizes, simpler rounds, and simpler key schedules. Having such features in a cipher will result in cost savings, lower energy consumption, lower number of needed computations, and lower memory requirements. A balance, however, needs to be made between the desirable features and the strength of a cipher against various attacks.

Reference [6] provides an overview of the state-of-art and standardization of lightweight cryptography (LWC) for IoT. It describes a new emerging standard of lightweight cryptography: ISO/IEC 29192. The standard sets the most important measures to evaluate lightweight properties as chip size and energy consumption for hardware implementations, and code size and RAM usage for software implementations.

Any LWC algorithms should also not exploit any securityefficiency trade-offs. The block ciphers adopted by ISO/IEC 29192 are PRESENT and CLEFIA. SIMON and SPECK were submitted to be included in the new version of the standard, in addition to the first two.

Both of the previous publications advocate the need for lighter algorithms while maintaining an appropriate level of security. Little information is given about the capabilities of IoT-enabled devices, the required security strength to be provided or whether the algorithms need to integrated within IoT security frameworks. Based on the recommendations from the papers, there is a consensus about which performance metrics should be used when evaluating an IoT lightweight cryptographic algorithm (memory usage, gate usage, etc.).

Reference [7] evaluates ten different LWC cryptography algorithms created for constrained devices, in the field of IoT-enabled health care systems. It compares them based on resource usage in terms of execution speed and memory occupation on a standard ATmega128 microcontroller. Out of the ten algorithms, the authors found that SPECK and SIMON are most efficient ones with the former outperforming the latter. The authors indicate that SPECK is fast, simple and reconfigurable, making it the algorithm of choice for any implementation of IoT for medical data. Some of the relevant LWC algorithms will be discussed in our paper.

The design of SIMON and SPECK lightweight cryptography algorithms was inspected in a paper by [8]. The research details the existing problems and the inspirations that led to the development of the two algorithms. One of the issues highlighted was that other lightweight ciphers, such as PRESENT, show good performance on ASIC implementations but fail to be upto the level on resource-constrained devices and FPGAs.

Another issue is that the existing lightweight ciphers have fixed block and key sizes, hence the lack of flexibility. SIMON and SPECK have block sizes of 32, 48, 64, 96, and 128 bits and up to three key sizes for each block. The research concludes that the two algorithms ended up with superior throughput on high-end systems as well due to the simplicity of their designs.

According the researches, SIMON and SPECK are demonstrably good performing algorithms. The two algorithms are recently gained popularity and are increasingly being seen in benchmark tests. Their structure was built to be reconfigurable, therefore its easier to modify and use them in a wide range of devices. In terms of flexibility, the two algorithms support many different key

and block sizes so they are fit for various applications. PRESENT and CLEFIA are ones of the best contenders in terms of performance and also provide resistance to more attacks than SIMON and SPECK.

A publication [9] demonstrates the applicability of SIMON and SPECK block ciphers to the domain of IoT. Several tests of the cipher algorithms were run on ASIC, FPGAs, microcontrollers, and high-end systems as to simulate different platforms for IoT implementations. The results show that in most platforms, either SIMON or SPECK appeared to be the best performing algorithm over all other algorithms including AES, ChaCha20, and others. The authors argue that the flexibility of SIMON and SPECK was one of the main factors leading to their superior test results. In addition, the authors also claim that implementing the two algorithms is easy and more error-free because of their simple designs, and that their simplicity can also lead to cheaper side-channel attack mitigation.

2.1. Inferences

It is evident from the literature review that a vast number of researchers have advocated the importance of providing an encryption algorithms that fit the requirements for IoT devices. Lower energy consumption and processing power use were cited as the most desired features of any IoT cryptographic algorithm. Despite the availability of innovative lightweight cryptographic algorithms, the schemes are still considered as in their early stages. They lack intensive performance and security testing to guarantee their ability to provide the promised level of security. Moreover, LWC algorithms require both expert evaluations and to be standardardized so they could be utilized effectively. The ISO has accepted four symmetric LWC algorithms to be studied prior to standardization. The algorithms are the following: SIMON, SPECK, PRESENT, and CLEFIA.

3. Overview of Cryptography In IoT

The aim of cryptography in IoT is to achieve two of the three main goals of information security: confidentiality and integrity of data. To ensure that the data passing through a communication channel is confidential, the data has to be encrypted. An IoT device can achieve this using am encryption algorithm. There are two classes of encryption algorithms: asymmetric and symmetric.

Asymmetric algorithms in IoT are very similar to those used in most computing devices. An IoT device can use RSA, Diffie-Hellman, ECC and most other asymmetric algorithms. However, due to the large computational overhead caused by asymmetric cryptography, most experts argue that ECC is the most appropriate algorithm. This is because ECC offers equivalent levels of security with less computing, lower memory usage and smaller keys (Goyal and Sahula, 2016). Furthermore, ECC was chosen as the asymmetric scheme of choice in ISO/IEC 29192 standard, utilizing it for authentication, exchange of session keys, and creation of digital signatures.

For data exchange, symmetric algorithms are used after their keys were exchanged through asymmetric means. IoT devices can use AES, DES, and other common algorithms but the resource boundaries persist. Most symmetric algorithms are very resource consuming, hence the advent of LWC. LWC ciphers are modeled specifically for resource-constrained devices. They aim to achieve the same level of security that the normal symmetric algorithms provide but with a lighter footprint. There are a number of emerging LWC algorithms. Some of which are Salsa20, Camelia, IDEA, LED, Rabbit, and many others that can be found in [7]. The latest ISO/IEC 29192 standard selected four LWC algorithms: SPECK, SIMON, PRESENT, and CLEDIA.

The integrity of data can be achieved by the use of digital signatures and message authentication codes (MACs). Hashing algorithms like MD5 and SHA1 are usually avoided in IoT due to their high processing requirements. Digital signatures can be accomplished using ECC which was discussed previously. The standardization efforts to select the best IoT hashing algorithm to use in HMACs are still underway. Three hashing algorithms were selected by the ISO/IEC 29192 standard. They include: PHOTON, SPONGENT, and Lesamnta-LW.

This paper will focus on the four symmetric lightweight schemes proposed by the ISO/IEC 29192 standard. Next, each of the four algorithms will be discussed in detail.

4. Lightweight Ciphers Proposed By ISO/IEC 29192

The purpose of standardization efforts within the field of IoT LWC is to propose symmetric algorithms that can be used by most IoT devices regardless of processing capabilities and energy constraints. ISO/IEC 29192 Part 2 is mainly concerned with

suggesting block ciphers with LWC features suitable for usage in IoT devices. In 2012, the initial standard proposed only PRESENT and CLEFIA. Later on in 2014, an amendment was made to add two new algorithms to the standard: SIMON and SPECK. The standard also set the minimum block size as 48 bits and the minimum key size as 96 bits (Katagi and Moriai, 2012). The following subsections will describe the way the four algorithms proposed in ISO/IEC 29192 work and highlight their main features.

4.1.. SIMON

Simon is one of the block cipher that been proposed by the National Security Agencys research directorate (NSA) in June 2013 for the use of the in constrained environments that have limited computational power and energy, utilizing their formidable experience in cryptography design to produce a new algorithm which they think is secure [7]. SIMON belongs to the Feistel network family which gives it an advantages in hardware because of the similarity of encryption and decryption operations which produce a require less hardware therefore the implementation requires a small circuit. Figure 1 depicts how one round operation of SIMON occurs.

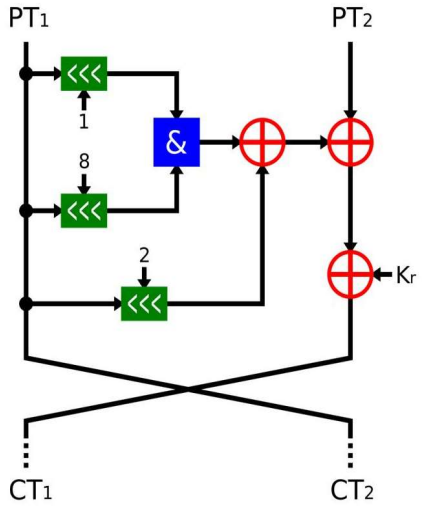

Figure 1. One round of SIMON

According to [9], the algorithm was aimed to support a wide range of devices and thus it needed to be flexible to be able to fit the security objectives multiple devices without requiring additional processing power. Simon use simple round functions are based on Feistel permutations iterated as many as required for security to avoid the additional complexity that S-boxes can add to the design. Table I summarize the different SIMON block size and the corresponding key size and no. of rounds.

Block Size	*Key size*	*No. of Rounds*
32	64	32
48	72	36
	96	36
64	96	42
	144	44
96	96	52
	144	54
128	128	68
	192	69
	256	72

Table 1. Simon Block Sizes, Key Sizes And Number of Rounds

As described in [10], SIMON utilizes a simple round function that uses basic operations such as XOR, AND and left circular shift. It has optimized performance in hardware but can still achieve a good performance in software. Implementation of SIMON encryption algorithm is optimized for low RAM usage and fast speed because of the simplicity of the operations used.

4.2. SPECK

As opposed to SIMON block cipher which was meant to achieve optimized performance on hardware implementations, SPECK is optimized for software-based implementations (especially on microcontroller processors). SPECK is both fast and low memory consuming as the algorithm applies only 32 operations on the input and does not require a lookup table [10]. Similar to SIMON, SPECK is also based on Feistel structure. In every Feistel round, the two branches are subjected to bitwise XOR, modular addition and circular shifts. Figure 2 shows how round functions work in SPECK along with the input keys from the key scheduler.

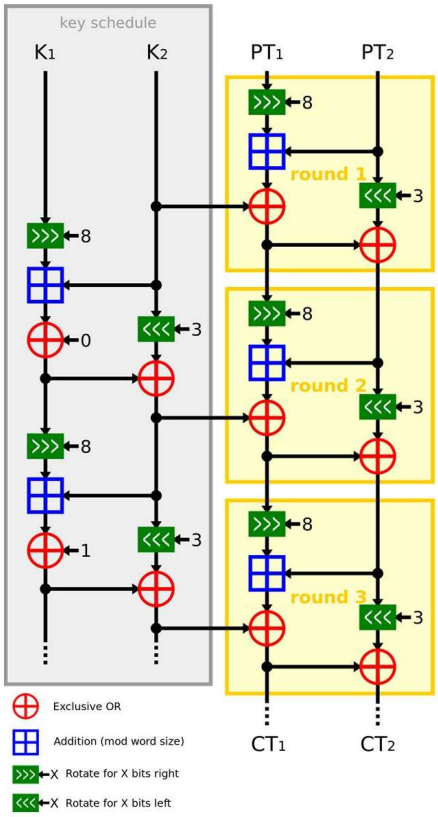

Figure 2. Three rounds of SPECK with key schedules

SPECK is a family of block ciphers with different input block and key sizes and different number of rounds. Table II highlights the main differences among members of the block cipher:

Table 2.Speck Block Sizes, Key Sizes And Number Of Rounds [10]

Those different members, like with the members of SIMON family, exist to suit various performance and security requirements which may differ from an application to another.

Those different members, like with the members of SIMON family, exist to suit various performance and security requirements which may differ from an application to another.

The round function works as follows: The left word is rotated to the left by number of times where = 8 is a 15 fixed constant. It

is then added to the right word modulos 2n = 128. The output of the modular addition is then XORed with the subkey generated for the round. The right word is later rotated right by a factor of = 3 bits. Finally, the left output is sent to next round. The right output is XORed with the left output then sent to the next round. According to [11], this round structure has enabled SPECK to avoid slide attacks and man-in-the-middle attacks which other algorithms are usually susceptible to. However, up to half the rounds were susceptible to differential and boomerang attacks. Those attacks do not a pose a real threat because they do not occur on the last round.

4.3. PRESENT

PRESENT is a hardware-oriented block cipher that is based on Substitution-Permutation networks (SPN). The cipher accepts a block size of 64 bits and two key sizes: 80 bits and 128 bits [10]. It is suitable for applications that do not require a high level of security. The data to be encrypted by this cipher is assumed to be of small to medium size, as the algorithm prioritizes performance and space. The second most important design consideration of PRESENT is to suit devices with average power consumption. Third most important metric is the execution time of the algorithm [12].

There are a range of attacks which PRESENT is susceptible to. Among the attacks are birthday attacks when encrypting a large amount of data. Side-channel attacks and invasive hardware attacks are also possible as with most other algorithms. The attacks exist, however they do not pose a significant risk as they solely depend on the implementation of the algorithm and not on the inherent nature of the algorithm itself.

The cipher uses a single 4-bit to 4-bit S-Box. This implementation is claimed to provide better hardware efficiency as it is more compact than a 8-bit S-Box. The algorithm is also said to be resistant to differential cryptanalysis, linear cryptanalysis and key schedule attacks [12].

An implementation of PRESENT was made on a UMC L180 0.18 1P6M Logic process in [12]. It required 32 clock cycles for an encryption of 64-bit block with a 80-bit key. It was found that the implementation utilized 1570 GE along with a power consumption of 5W. On software when implemented in C, however, the algorithm requires large sized lookup tables (up to 1 MB).

4.4. CLEFIA

CLEFIA is 128-bit block cipher that support a various key sizes including 128, 192, and 256-bits [13]. CLEFIA is structured on Feistel network with 4 data lines in which two 32-bit f function per one round. The algorithm use a novel approach with f-functions based on diffusion switching mechanism (DSM) which strengthen it against certain types of attacks, also its uses another novel approach that CLEFIA uses is the compact key scheduling and the doubleswap function which enable efficient round key generation. The proposed algorithm is efficient implementation in software and specifically in hardware. The algorithm supports multiple key size 128, 192 and 256 bits. CLEFIA utilizes 2 different 8 bit S-boxes.

CLEFIA demonstrates immunity against known attacks but [14] shows that differential attacks specifically at round 12 for 128 bit key and round 13 for 192 and 256 bit key can occur. To defend against such an attack in the future, proper formal definitions need to be laid out and inspected.

5. Conclusion

In this paper, we studied four lightweight cryptographic (LWC) algorithms. The main goal of the algorithms is to allow secure communications among power-constrained devices without consuming excessive amount of resources. The ISO standard established the first steps for industry adoption of LWC with the announcement of ISO/IEC 29192 standard. The following algorithms from the standard were detailed in this paper: SIMON, SPECK, PRESENT and CLEFIA. SIMON is block cipher that supports key sizes of 64 up to 256 bits and block sizes of 32 up to 128 bits. It belongs to Feistel network family of algorithms and is optimized for hardware-based implementations. On the other hand SPECK is optimized for software-based implementations. SPECK requires a small amount of memory space because of the number of operations used in its code. Similar to SIMON, it also belongs to the Feistel network structure and supports key sizes of 128 up to 256 bits with a block size of 128 bits. PRESENT is a hardware oriented block cipher the accepts two key sizes, 80 and 128 bits, with a block size of 64 bits. PRESENT is based on the substitution-permutation networks (SPN). It is suitable for applications which doesn't require a high level of security. PRESENT is susceptible to several attacks including birthday attacks, but when encrypting a large amount of data such attacks risk can be mitigated in proper implementations of the algorithm. CLEFIA is based on the Feistel network. It accepts a 128 bit plaintext block

and supports multiple key sizes of 128 up to 256 bits. Related works demonstrated that CLEFIA is vulnerable to differential attacks. However, an advantage is that CLEIFA is considered efficient in both hardware and software implementation. The choice of implementing lightweight encryption depend on the hardware of the IoT device and the desired level of security.

6. Recommendations

Many LWC algorithms were developed over the past 5 years. Most of them are never utilized in real hardware or are simply dismissed because they lack certain features. The ISO/IEC 29192 standard is currently the only effort to establish a baseline through which researchers can take as a starting point for new developments. Since the standard was merely a grouping of the best algorithms found in the literature, we that recommend a new LWC solution be built based on the best features from each of the four algorithms. The new cryptographic solution should be flexible in terms of block and key sizes, well-performing on both hardware and software implementation and resistant to the various cryptanalytic and bruteforce attacks. The new algorithm could be developed by merging elements from each of the four algorithms.

References

[1] Stango, S.A., Prasad, N., Sen, J. & Prasad, R. (2011) Babar. Proposed Embedded Security Framework for Internet of Things (iot). In: Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE) 2nd International Conference on, Vol. 2011. *IEEE Publications*, pp. 1–5.

[2] Xu, T., Wendt, J.B. & Potkonjak, M. (2014) Security of iot systems: Design challenges and opportunities. In: Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design. IEEE Publications, pp. 417–423.

[3] Sicari, S., Rizzardi, A., Grieco, L.A. & Coen-Porisini, A. (2015) Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76, 146–164.

[4] Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K. & Shieh, S. (2014) Iot security: Ongoing challenges and research opportunities. In: 7th International Conference on Service-Oriented Computing and Applications. *IEEE Publications*, pp. 230–234, Nov 2014.

[5] Singh, S., Sharma, P.K., Moon, S.Y. & Park, J.H. (2017) Advanced lightweight encryption algorithms for iot devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*.

[6] Katagi, M. & Moriai, S. (2012). *Lightweight Cryptography for the Internet of Things*, Vol. 05.

[7] Alassaf, N., Alkazemi, B. & Gutub, A. (2017). *Applicable Light-Weight Cryptography to Secure Medical Data in Iot Systems*, Vol. 2, pp. 50–58, 04.

[8] Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J. & Wingers, L. (2015) The simon and speck lightweight block ciphers. In: 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 1–6, June 2015.

[9] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. & Wingers, L. (2015). "Simon and speck: Block ciphers for the internet of things." Cryptology E-print Archive, Report 2015/585. https://eprint.iacr.org/2015/585.

[10] Dinu, D., Corre, Y.L., Khovratovich, D., Perrin, L., Großschädl, J. & Biryukov, A. (2015) "Triathlon of lightweight block ciphers for the internet of things," tech [Rep.]. IACR Eprint Archive.

[11] Abed, F., List, E., Lucks, S. & Wenzel, *J. Cryptanalysis of the Speck Family of Block Ciphers*.

[12] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y. & Vikkelsoe, C. (2007) Present: An ultralightweight block cipher. In: Cryptographic Hardware and Embedded Systems – CHES (edited by P. Paillier & I. Verbauwhede), (Berlin, Heidelberg). Springer: Berlin, Heidelberg, pp. 450–466.

[13] Shirai, T., Shibutani, K., Akishita, T., Moriai, S. & Iwata, T. (2007) The 128-bit blockcipher clefia. In: International Workshop

on Fast Software Encryption. Springer: Berlin, pp. 181–195.

[14] Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T. & Kubo, H. (2008) Impossible differential cryptanalysis of clefia. In: International Workshop on Fast Software Encryption. Springer: Berlin, pp. 398–411.