An Analysis of Light Weight Block Ciphers in Wireless Body Area Networks

Radhika Rani Chintala, Sadineni Srujana, Nalluri Ajith Kumar

***Abstract:**The increasing use of wireless communications in electronic environment has raised the use of Wireless Body Area Networks (WBAN). In these networks, sensors can be placed on clothes, skin and even under the skin to measure the health parameters like sugar, blood pressure, etc. either internally or externally. These devices can help the users and medical personal in providing continuous health monitoring and can give the feedback. Hence, these sensors can improve the quality of life and even improves health care. As the users medical data is communicated among users and medical personnel through network then the question of security is raised which can be solved through cryptography. Memory, size, power and resources are mainly considered in the aspect of cryptography. As these resources are limited in sensor devices, security can be achieved using light weight cryptography. The term light weight never refers to low security. With the available resources it can provide the security in the maximum extent possible. This paper provides a review on the various light weight block ciphers which discusses about speed, performance, cost and balanced efficiency in hardware implementations.*

***Keywords:** Wireless Body Area Networks, Cryptography, Lightweight block cipher, Security*

I. INTRODUCTION

WBAN is defined as Wireless Body Area Networks which is a specialized sensor network that is designed specifically for connecting different medical sensors and various appliances, and the sensors may be located within or outside the body of human being. These can provide cost saving options and flexibilities for both patients and healthcare professionals. As we are dealing with these type of sensors we have only a limited number of resources. Light weight cryptography is also developed with limited hardware and low cost resource constrained devices. The sensors which are placed, can get access in critical environments and can also work with limited batteries. With the available resources in WBAN, security is provided through Light Weight Block ciphers. In this paper we deliberate about various lightweight block ciphers and their operations. In most of these ciphers, each round will makes use of the operations like Bit-Wise XOR, Bit-Wise AND, P-Boxes, and S-Boxes.

Substitution & Permutation Network (SPN) and Feistel structure are the commonly used structures in these ciphers. Feistel Structure is used for constructing the block ciphers and is symmetric in nature. Hardware implementation in cryptosystem is made easier as it is iterative in nature. In this structure both the encryption and decryption are done in similar fashion and almost equal in few cases, where it just requires only reversing the key schedule. As both the processes are similar, the size of the code may be reduced to half. In SPN structure, a sequence of interrelated mathematical computations is used. In this network a block of plaintext and a key is taken as inputs and performs alternating rounds(or layers) of S-boxes and P-boxes and can also perform bitwise rotation and Exclusive or (XOR) to produce cipher text.

In section 2, we discuss about various lightweight block ciphers such as TEA, HIGHT, Humming Bird, Present, Print, etc., and their parameters and operations used. In section 3, we speak about the efficient block ciphers SIMON and SPECK and their comparative analysis.

II. LIGHTWEIGHT BLOCK CIPHERS

In this part of section, we will have a discussion about various lightweight block ciphers.

2.1 SEA: Scalable Encryption Algorithm

Standaert et al designed this algorithm in the year 2006. This algorithm follows Feistel structure with different word and text sizes. This design consists of minimal code size, low memory requirements, flexibility, limited instruction set which is actually not an usual design criterion for ciphers. This algorithm is parametric in nature based on text, key, and processor size. There is well known fact that the algorithms will work differently on different platforms and is protected based on the key size. This algorithm provides encryption and authentication. As it is previously said that the algorithm uses the limited resources and less number of requirements, the cipher employees with a limited basic operations, such as modular addition, substitution box(S-box), bit rotation, left rotation, XOR, and inverse word rotation [27]. SEA is denoted as $SEA_{n,b}$. where n is plaintext and key size and b represents the processor size.

2.2 HIGHT

Deukjo Hong et al developed HIGHT cipher in the year 2006. It is suitable for low resource device. This cipher contains block size and key size as the parameters with the sizes 64-bit and 128-bit. This cipher includes encryption technique which starts with the conversion of the block, continues with 32-round iterative function, and ends with a transformed output for the round function. F_0 and F_1 are the two functions which will come in the round function mentioned above plus XOR and addition operations. The functions F_0 and F_1 are based mainly on shift and simple XOR operations. HIGHT is the fastest cipher compared to

Revised Manuscript Received on May 29, 2019.

Radhika Rani Chintala,Department of CSE, KLEF, Vaddeswaram, Guntur, Andhra Pradesh, India

SadineniSrujana,Department of CSE, KLEF, Vaddeswaram, Guntur, Andhra Pradesh, India

NalluriAjith Kumar,Department of CSE, KLEF, Vaddeswaram, Guntur, Andhra Pradesh, India

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

AES. This is used to preserve the original master key value, even after generating all the subkeys and the whitening keys. Due to this reason, during the encryption and decryption process itself these subkeys are generated. This cipher is proved to be secure for various cryptographic applications [20].

2.3 PRESENT

A. Bogdanov et al. developed this cipher in the year 2007. This cipher is mainly based on substitution-permutation structure. This contains block and bit keys as the parameters with sizes 64-bit and 80-bit. It is an ultra-lightweight block cipher. During the hardware implementation, even a minute variation may cause disastrous effect on the space which is necessary for implementation. Here, round key consists of XOR operation. Both Substitution and Permutation layers are included. Substitution layer contains sixteen of 4-bit S-boxes and Permutation layer contains bitwise permutation. 31 round iterations are run on this algorithm which returns cipher text. This is approved by ISO(International Standard Organisation) as a standard light weight block cipher. This algorithm is proved to be secure in Linear and Differential cryptanalysis, Structural, Algebraic and Key schedule attacks [15].

2.4 PRINT

Lars Knudsen designed this cipher for IC printing. Silicon links are used with which circuits can be printed on a wide-ranging materials using HD(High Definition) printing process. It has the ability to print on flexible and thin materials. IC printing allows the fabrication of RIFD tags that provides a security to the printed tag. The motive beside designing this cipher is to guarantee memory persistence. The parameters used in the cipher are 48-bit and 96-bit blocks and a key length of 80-bits and 160-bits. The structure is based on 48-bit and 96-bit round substitution and permutation network. The 48-bit version uses a 48-bit blocks and an 80-bit key and enjoys the 48 round structure. In this cipher encryption process is started by mapping the 48-bit on the input, then applies XOR of one round on the last 6 least significant bits and then provides the output to key0dependent permutation and then to substitution layer. 16 3-bit S-Boxes are there in the substitution layer of this cipher. The output acquired by this layer is the output of the one single round. This cipher which is 48-bit performs 48 rounds which indicated the 48 iterations [8].

2.5 Humming Bird

Daniel Engels et al. introduced this cipher in the year 2010. This cipher is mainly based on block and stream-based designs. This cipher contains a key size, block size and bit internal state as the parameters with the sizes 256-bit, 16-bit and 80-bit. High level of security for embedded applications can be provided by this cipher based on the size of the key and the internal state. The structure of the humming bird uses the 16-bit block ciphers such as EK1, EK2, EK3, and EK4, plus a 16-bit internal state registers, and a 16-stage LFSR. The substitution-permutation structure of this cipher is 16-bit and the key size is 64-bit. XOR operation is used by the block-based structure of the cipher in the SPN structure for key addition, four 4-bit s-boxes for substitution layer and the Linear transform containing XOR [3].

2.6 KATAN & KTANTAN

Christope De Canniere et al developed these ciphers in the year 2009. Both of these versions uses a block sizes of 32,48 and 64-bits, and share key of size 80-bits. These are efficient hardware oriented block ciphers. KATAN comes with three ciphers namely Katan32, Katan48 and Katan64. These accept keys with size of 80-bits and the block sizes for these three ciphers are different. These achieve minimal size and are highly compact in nature. KTANTAN32, KTANTAN48, and KTANTAN64 are the three ciphers which come under KTANTAN which are even small block ciphers. KTANTAN ciphers are more compact compared to KATAN and is only suitable for the devices which use only one key which will never be altered. In KTANTAN, the key is burnt into the device. The only difference among these two algorithms is the Key scheduling process. In these two ciphers the plaintext will be loaded in two registers, then performs Boolean functions and then sends the output to the LSB of shifted registers. For the efficient mixing this cipher needs 54 rounds. It is proved to be secure against Linear and differential cryptanalysis, and attacks such as combined, related-key and slide attacks, Cube Attacks and Algebraic Attacks [12].

2.7 mCrypton

ChaeHoon Lim et al developed this cipher in the year 2005. The efficiency of the resource constrained applications should be optimised, which is considered as the main objective. It is designed using the Crypton structural design but with simplifying the component function to enable the information which is compact in both software and hardware. This mCrypton uses blocks of size 64-bits and keys of size 64, 96 or 128 bits. This processes 8-bit data blocks 4 expressed as 4 by 4 nibble array. Here four operations are done in each round i.e., nibble-wise substitution, column to row transposition, column-bit permutation and the key addition. Here the encryption procedure consists of 12 iterations [13].

2.8 KLEIN

Zheng Gong et al designed this cipher in the year 2011, specially for the devices that restricted to resource constraints. The hardware implementation is compact. It has an advantage of software performance which is on legacy sensor platforms. The security analysis on KLEIN says that it has a conservative security margin against cryptanalysis. This KLEIN structure is based on SPN and is designed with round counts 12,16, and 20 for 64,80, and 98 bit variations. One dimensional array of bytes is displayed to show the ciphers input and output. All the operations performed in this cipher are optimised using byte oriented algorithms. The Add-Round key is implemented via simple XOR operation. Here 16 similar involute s-boxes are used as it has an advantage of reducing the extra cost of inverse implementation which is leading to an efficient serialisation.

2.9 TWINE

T.Suzaki et al developed this cipher in the year 2013. It is a lightweight block cipher that contains multiple platforms. This cipher contains a block of size 64-bits and a key of sizes 80 bits or 128 bits. Considering the central processors, we suspect the hardware and software performance. The design of this cipher is based on GFN-2(type-2 Generalized Feistel Network) which contains 16 nibble blocks. TWINE cipher performs partitions on 64-bit block to 16Xi, and in line with GFN-2 structure, using the simple 8 F functions. The X's having even subscript is imported in F function and then XORs them with X's having odd subscript. The permutation employs 4-bit words and then forms a linear part of cipher. It is proved to be secure against Linear or Differential Cryptanalysis, and Key Schedule-based Attacks, Saturation Attacks and Impossible Differential Attacks. [18].

2.10 PRINCE

Julia Borghoff et al designed this cipher in the year 2012. The target o this cipher is having unrolled hardware implementations and low latency. This cipher uses a block size of 64-bit and key size of 128-bit. This is based on FX structure. To spread the effect of the key over the plaintext this cipher use Key whitening component and prevents the attacks occurred based on keys. 12-round PRINCE core is present between the key whitening parts. There are some operations which are undergone like simple XOR, addition of round constant, substitution and matrix. This cipher design uses similar 4-bit S-boxes and 12 64-bit round constants [16].

2.11 PRIDE

Matin R Albrecht et al developed this cipher in the year 2012. This cipher design is based on FX structure. Block size and key size are considered as the parameters in this cipher with 64-bit and 128-bit. First whitening key K is extracted from the first half and the second whitening key K1 is extracted from the second half by the cipher. At the starting and ending of the process cipher uses bit permutation to ensure the effectiveness of the bit-sliced implementation. The encryption firstly starts with initial bit permutation on the plaintext. The result is then subjected to the first whitening key K. Then 19 identical rounds of iteration are applied on the output. On the output which we get after 19th iteration is subjected to 20th round which is slightly different than the others. Then XOR operation is applied on the result with the second whitening key and then on the result secondary bit permutation is applied. The resultant will be a cipher text C. The round function R which is discussed earlier is the classical substitution-permutation network. 16 4-bit S-boxes are present in the substitution layer. [19].

2.12 Hummingbird2

Daniel Eagles et al developed this cipher in the year 2012. It is light weight authenticated encryption algorithm. This cipher contains a secret key and initialisation vector with 128-bit and 64-bit. As we are dealing with sensors which it could only handle a limited hardware, this algorithm deals with the same and also security is considered on the low-cost ubiquitous devices. This cipher doesn't come under either stream cipher or block cipher as it inherits properties from the both. For each message selected over here will have an authentication tag. The 128-bit internal state is initialized by a 64-bit array. As like humming bird 1, this can work with 16-bit block size. So, the operations are also designed with 16-bit words. Linear operation has designed a non-linear function F to apply on 4 different non-linear S-boxes. Thereby the input of the linear function is the output of the non-linear function [28].

2.13 LBLOCK

Wenling We et al introduced this cipher in the year 2011. Block size and key size of this cipher is 64-bit and 80-bit and based on feistel structure having 32-round. It is a light weight block cipher. The main properties of this cipher are, there is no need to encrypt large amounts of data, due to lack of computing ability these ciphers only need to achieve moderate security, this type of ciphers are implemented on the hardware and also on the software environment. Round function F provides the security to the cipher. S and P are the two parts considered in the round function, which establish the basic Shannon principles. Here S which refers to substitution layer is responsible for cluster operation and P which refers to Permutation is responsible for diffusing Shannon principles. S consists of 8 parallel 4-bit S-boxes and Permutation layer consists of 8 4-bit permutations [9].

2.14 MIBS

Maryam Izadiet al designed this cipher in the year 2009. This is a 32-round cipher which uses 64-bit block size and 80-bit keys. 8 identical S-boxes with 24 XOR elements are present in the round function and produce a cluster. Sorting networks is a type of method which is similar to round function. The method used to select the inputs in round function is similar to the method used to select the inputs in sensor networks. Set of XOR elements are used in key addition stage and the permutation layer in it is in the form of 4-bit element arrangements [10].

2.15 Puffin

Hujju Cheng et al developed this cipher in the year 2011. This cipher uses block size of 64-bit and key size of 128-bit. This cipher is based on SPN and is suitable for embedded applications. This structure is based on, encryption process which consists of permutation and substitution, same data path is needed for both encryption and decryption which is facilitated by involuntary operations, and a sub key generation which is composed of permutation and inversions. Key addition of this cipher is performed via XOR operation like many other SPN-based ciphers. The substitution layer contains 16 parallel 4-bit S-boxes, and permutation layer contains bit-wise design. In each round of substitution operation, cipher performs Add-Round-Key and the permutation repeats 32-round iteration [17].

2.16 ESF

ESF-Eight Sided Fortress was developed by LIU Xuanet at in the year 2014. The block size is of 64 bit and key size is of 20-bit, which is similar to many other block cipher and is based on Feistel Structure. Round function is the main component of this cipher, which is based on SPN. Computational requirements are considered as the main aim of this cipher. The round function used in this cipher is subjects to 32-bit round key k and XOR function is performed on the half block. The cipher process the output by eight 4-bit S-boxes. Permutation layer is designed in the form of bit permutation [6].

2.17 Piccolo

KyojiShibutani et al developed this cipher in the year 2011. This cipher uses block size of 64-bit and key size of 80 or 128-bit. This cipher is based on GFN-2(type-2 Generalized Feistel Network). 8 identical S-boxes are present in round function which first applies 4 parallel 4-bit S-boxes on the input and then uses diffusion matrix M. The output is then subjected to 4 parallel 4-bit S-boxes to form the final output and the permutation is based on bit-ward permutation [14].

2.18 Khudra

S.Kolay et al developed this cipher in the year 2014. This is specifically for FPGAs. Block size is of 64-bit and key size is based on 80-bit. This cipher utilises two F-functions with 16-bit inputs. Each F-function is based on 4-bit GFN2 structure and 6 rounds iteration is performed. 18 rounds of iteration is used by the cipher. The S-boxes used in this cipher is similar to the S-boxes used in PRESENT, and have algebraic degree in maximum and linear-differential probability in minimum.

2.19 SIMON

SIMON is a light weight block cipher which is released publicly by the National Security Agency in the year of 2013 june. It is a balanced feistel cipher which has been optimised for the performance in hardware implementations. The warning is received from the security researches for having the backdoor which would compromise the effectiveness of the algorithm. The detailed technical details are not given by the privacy concerns came after NSA to the researches thereby the standardisation of the algorithm has not taken place.

2.20 SPECK

SPECK is also released in the same year. It has been optimised for the performance in software implementations. It is an add-rotate-XOR(ARX) cipher. This cipher provides high level of security for each key size and block, against standard chosen-plaintext and chosen-ciphertext. No specific efforts are made to resist attacks nor the designers evaluate the use of hash functions. Differential cryptanalysis attacks are the best published attacks on speck which are marginally faster than the brute force. While designing speck, the team members came across differential attacks to be the limiting attacks i.e., the type of attacks facing during the rounds then they set the number of rounds to leave the security margin, which is too small for the speck.

Compared to the algorithms discussed so far, SIMON and SPECK are chosen as the best.

III. SIMON AND SPECK COMPARITIVE ANALYSIS:

SIMON and SPECK both are considered as the sisters. Ray Beaulieu et developed this cipher in the year 2013 with different block and key sizes. SIMON and Speck both can support different block sizes of 32, 48, 64, 96, and 128 bits and also up to three key sizes to support the block size. Following table describes the different block sizes and the related key sizes in bits.

On 64-bit processors SPECK has the highest throughput. For pipelined ASIC implementations, SIMON have highest throughput. Rather than SPN, these ciphers are based on Feistel Permutations which can provide good balance between non-linear confusion and linear diffusion operations. Diffusion takes care of bit permutations which we use for rotations. Composition of two rotations and bitwise AND is used in SIMON which requires limited hardware whereas modular addition is used for nonlinearity in SPECK which is cryptographically stronger than AND operation used in SIMON which is used for implementations in software.

Cryptanalysis of SIMON:

- No(public) cryptanalysis or security arguments from the designers.
- Many Contributors are from the cryptographic community.
- Attacks cover up to 74% of rounds.

3.1 FURTHER CONSIDERATIONS

Simplicity:

Simon and Speck ciphers perform very simple rounds and iterations as many times as necessary to provide security whereas, complex round functions are performed but fewer rounds are required.

Uniformity:

Coming to uniformity, same set of parameters are used in SIMON and SPECK so that it makes for the best description of the algorithms and also that in hardware and software, smaller joint implementations are done.

Moves:

Software implementations with less number of moves are intended. SIMON requires multiple operations whereas SPECK can do with in-place operations so the moves are unnecessary.

Encrypt and Decrypt symmetry:

It is best to use encryption look like decryption instead of using joint implementations. In SIMON decryption is done by swapping text words, reading the round keys in reverse order, then swapping the resultant whereas SPECK decryption requires modular subtraction and one of the rotations is required.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Constants:

One-up counter is used by the SPECK in its key schedule whereas in SIMON circuit size is reduced. All the constants in software are packed into words and stored but is less efficient as we just use a one-up counter.

Key schedules:

Reuse of round function for key scheduling is done in SPECK. It is possible to have key schedules more simpler than the ones used in SIMON and SPECK.

Security:

Security is on major issue raises in ciphers. So the main implementation is about security. Here is the way we provide security from the hexadecimal text.

We have used XOR over here and there are some advantages in using this:

- Mostly in hardware, XOR is computed fastly.
- There is no difference in making whether it is on left side or right side.
- Easily understandable and analyse
- Order of XOR values in not mattered.

The NSA cryptanalysis found that the algorithms doesn't have any weaknesses and low level of security and approved both the SIMON and SPECK for use in national security systems.

IV. CONCLUSION:

Wireless Body network is mostly used in medical environment. Sensors are used here, which can be placed on the skin or under the skin and even on the clothes. With the help of this, patients can come to know about the status of their health. Not only the users but also the doctors or medical personnel can know the status of the user health condition. As the data is being communicated, Security is treated as the main issue as the health related data of any patient can be manipulated and it may even cause serious problems. So the need for security is needed for health data and hence the concept of cryptography arises. We have gone through many lightweight block ciphers which will utilize limited resources and provide required security. Among all the block ciphers discussed, SIMON and SPECK are treated as the best.

REFERENCES:

1. Kitsos, Paris, Nicolas Sklavos, Maria Parousi, and Athanassios N. Skodras. "A comparative study of hardware architectures for lightweight block ciphers."Computers& Electrical Engineering 38, no. 1 (2012): 148-160.
2. Ding, Lin, Chenhui Jin, Jie Guan, and Qiuyan Wang. "Cryptanalysis of lightweight WG-8 stream cipher." Information Forensics and Security, IEEE Transactions on 9, no. 4 (2014): 645-652.
3. Engels, Daniel, Xinxin Fan, Guang Gong, Honggang Hu, and Eric M. Smith. "Hummingbird: ultra-lightweight cryptography for resource-constrained devices." In Financial Cryptography and Data Security, pp. 3-18. Springer Berlin Heidelberg, 2010.
4. Jana, Swarnendu, JaydebBhaumik, and Manas Kumar Maiti. "Survey on Lightweight Block Cipher." International Journal of Soft Computing and Engineering 3 (2013): 183-187.
5. Poschmann, Axel York. "Lightweight cryptography: cryptographic engineering for a pervasive world." In Ph. D. Thesis. 2009.
6. Xuan, L. I. U., Wen-ying ZHANG, Xiang-zhong LIU, and L. I. U. Feng. "Eight-sided fortress: a lightweight block cipher." The Journal of China Universities of Posts and Telecommunications 21, no. 1 (2014): 104-128.
7. Gong, Zheng, SvetlaNikova, and Yee Wei Law. KLEIN: a new family of lightweight block ciphers. Springer Berlin Heidelberg, 2012.
8. Knudsen, Lars, Gregor Leander, Axel Poschmann, and Matthew JB Robshaw. "PRINTcipher: a block cipher for ICprinting." In Cryptographic Hardware and Embedded Systems, CHES 2010, pp. 16-32. Springer Berlin Heidelberg, 2010.
9. Wu, Wenling, and Lei Zhang. "LBlock: a lightweight block cipher." In Applied Cryptography and Network Security, pp. 327- 344. Springer Berlin Heidelberg, 2011.
10. Izadi, Maryam, BabakSadeghiyan, SeyedSaeedSadeghian, and HosseinArabnezhadKhanooki. "MIBS: a new lightweight block cipher." In Cryptology and Network Security, pp. 334-348. Springer Berlin Heidelberg, 2009.
11. Karakoç, Ferhat, HüseyinDemirci, and A. EmreHarmancı. "ITUbee: a software oriented lightweight block cipher." In Lightweight Cryptography for Security and Privacy, pp. 16-27. Springer Berlin Heidelberg, 2013.
12. De Canniere, Christophe, Orr Dunkelman, and MiroslavKnežević. "KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers." InCryptographic Hardware and Embedded Systems-CHES 2009, pp. 272-288. Springer Berlin Heidelberg, 2009.
13. Lim, ChaeHoon, and TymurKorkishko. "mCrypton–a lightweight block cipher for security of low-cost RFID tags and sensors." In Information Security Applications, pp. 243-258. Springer Berlin Heidelberg, 2006.
14. Shibutani, Kyoji, TakanoriIsobe, HarunagaHiwatari, Atsushi Mitsuda, Toru Akishita, and TaizoShirai. "Piccolo: an ultralightweightblockcipher." InCryptographic Hardware and Embedded Systems–CHES 2011, pp. 342-357. Springer Berlin Heidelberg, 2011.
15. Bogdanov, Andrey, Lars R. Knudsen, Gregor Leander, ChristofPaar, Axel Poschmann, Matthew JB Robshaw, YannickSeurin, and Charlotte Vikkelsoe.PRESENT: An ultra-lightweight block cipher. Springer Berlin Heidelberg, 2007.
16. Borghoff, Julia, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, MiroslavKnezevic, Lars R. Knudsen, Gregor Leander et al. "PRINCE–a low-latency block cipher for pervasive computing applications." In Advances in Cryptology–ASIACRYPT 2012, pp. 208-225. Springer Berlin Heidelberg, 2012.
17. Cheng, Huiju, Howard M. Heys, and Cheng Wang. "Puffin: A novel compact block cipher targeted to embedded digital systems." In Digital System Design Architectures, Methods and Tools, 2008. DSD'08. 11th EUROMICRO Conference on, pp. 383-390. IEEE, 2008.
18. Suzaki, Tomoyasu, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. "\ textnormal {\ textsc {TWINE}}: A Lightweight Block Cipher for Multiple Platforms." In Selected Areas in Cryptography, pp. 339-354. Springer Berlin Heidelberg, 2013.
19. Albrecht, Martin R., BenediktDriessen, Elif Bilge Kavun, Gregor Leander, ChristofPaar, and TolgaYalçın. "Block ciphers–focus on the linear layer (feat. PRIDE)." In Advances in Cryptology–CRYPTO 2014, pp. 57-76. Springer Berlin Heidelberg, 2014.

20. Hong, Deukjo, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee et al. "HIGHT: A new block cipher suitable for low-resource device." In Cryptographic Hardware and Embedded Systems-CHES 2006, pp. 46-59. Springer Berlin Heidelberg, 2006.
21. Guo, Jian, Thomas Peyrin, Axel Poschmann, and Matt Robshaw. "The LED block cipher." In Cryptographic Hardware and Embedded Systems–CHES 2011, pp. 326-341. Springer Berlin Heidelberg, 2011.
22. Beaulieu, Ray, Douglas Shors, Jason Smith, Stefan TreatmanClark, Bryan Weeks, and Louis Wingers. "The SIMON and SPECK Families of Lightweight Block Ciphers." IACR Cryptology ePrint Archive 2013: 404.
23. Manifavas, Charalampos, George Hatzivasilis, KonstantinosFysarakis, and KonstantinosRantos. "Lightweight cryptography for embedded systems–A comparative analysis." In Data Privacy Management and Autonomous Spontaneous Security, pp. 333- 349. Springer Berlin Heidelberg, 2014.
24. Kong, JiaHao, Li-MinnAng, and KahPhooiSeng. "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments." Journal of Network and Computer Applications 49 (2015): 15-50.
25. Mohd, Bassam J., ThaierHayajneh, and Athanasios V. Vasilakos. "A survey on lightweight block ciphers for lowresource devices: Comparative study and open issues." Journal of Network and Computer Applications (2015).
26. Wheeler, David J., and Roger M. Needham. "TEA, a tiny encryption algorithm." In Fast Software Encryption, pp. 363-366. Springer Berlin Heidelberg, 1995.
27. Standaert, François-Xavier, Gilles Piret, Neil Gershenfeld, and Jean-Jacques Quisquater. "SEA: A scalable encryption algorithm for small embedded applications." In Smart Card Research and Advanced Applications, pp. 222-236. Springer Berlin Heidelberg, 2006.
28. Engels, Daniel, Markku-Juhani O. Saarinen, Peter Schweitzer, and Eric M. Smith. "The Hummingbird-2 lightweightauthenticated encryption algorithm." InRFID. Security and Privacy, pp. 19-31. Springer Berlin Heidelberg, 2012.
29. Kolay, Souvik, and DebdeepMukhopadhyay. "Khudra: A New Lightweight Block Cipher for FPGAs." In Security, Privacy, and Applied Cryptography Engineering, pp. 126-145. Springer International Publishing, 2014.