ACSIJ Advances in Computer Science: an International Journal, Vol. 5, Issue 4, No.22 , July 2016
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

A Comprehensive Survey on Evaluation of Lightweight Symmetric Ciphers: Hardware and Software Implementation

Jaber Hosseinzadeh[1], Maghsoud hosseinzadeh[2]

[1] **Data communication and Security Lab, Faculty Of Engineering, Ferdowsi University Of Mashhad, Mashhad, Iran**
Jaber_hosseinzadeh@stu-mail.um.ac.ir

[2] **Faculty Of Engineering, Islamic Azad University Of Urmia, Urmia, Iran**
Maghsom10@yahoo.com

Abstract

Low-resource devices like wireless sensor networks have some limitations on memory, power and energy. Using common encryption algorithms are not appropriate for these devices due to their hard limitations and leads to a waste of energy and power. Here, lightweight symmetric ciphers have been evaluated in hardware and software implementations. Comprehensive Evaluation of lightweight ciphers in this work is performed based on cost, speed, efficiency and balance criterion. In each of the criteria, evaluation is done based on a specific measure and the best ciphers have been introduced in each. Evaluation in terms of hardware and software implementation indicates the superiority of SPECK and SIMON ciphers. Evaluation in terms of speed in hardware implementation indicates the superiority of Trivium and Grain, and it shows the superiority of MASHA and SPECK in software implementation. Results of the Evaluation in terms of efficiency express the superiority of SIMON and SPECK. The results of these evaluations helps finding ciphers appropriate to the user based on requirements and restrictions. The user sets his desired system and then obtains the system needs; at the final step, based on the type of requirements, the results of our work help the system to select the appropriate cipher.

Keywords: *Cost criterion; efficiency criterion; speed criterion; hardware implementation; software implementation*

1. Introduction

Lightweight cryptography has been developed specifically for low-cost resource-constrained devices, as its design allows it work with limited hardware[6,7,36,38,39]. Devices used in wireless sensor networks, RFID tags, and Internet of things (IoT) are mostly characterized by low computing power, limited batteries, low memory, low power consumption and low operating frequency range [1, 13, 17, 30, 31]. These devices are often employed in poorly accessible and sometimes critical environments (e.g. in military applications) and work with limited batteries and an insecure communication channel, and all these factors highlight their need to robust cryptographic solutions [12,17,30,31,50,55,56]. On the other hand, the high computation and energy requirements of common cryptography methods such as AES, RSA emphasize the focus on lightweight solutions. So the growing use and development of resource-constrained devices such as smart phones, smart cards, etc. and the rising importance of security as their core principle has led to increased interest to lightweight cryptography [1,3,9,13,31,47]. The lightweight symmetric ciphers can be categorized into two classes: Block-based and stream-based[8,10,11,59]. The following is a brief introduction to some of the lightweight ciphers available in the literature.

SEA: This cipher was designed in 2006 by Standaert et al. The design of this cipher is based on low memory requirements, minimal code size, and limited instruction set, plus flexibility, which is an unusual design criterion for ciphers. This cipher is based on Feistel structure and it can work with different text, key, and word sizes. This cipher is denoted by $SEA_{n,b}$, where n is the plaintext size and key size, and b is the processor (or word) size. Due to its simplicity constraints, this cipher employs a limited number of basic operations, such as bitwise XOR, substitution box S, word (left) rotation, inverse word rotation, bit rotation, and modular addition [44].

HIGHT: This cipher was developed by Deukjo Hong et al. in 2006. It uses a 64-bit block size and a 128-bit key size. Its basic structure is 32-round type-2 generalized Feistel Network (GFN-2). The encryption processing of this cipher starts with initial conversion of the block, continues with a 32-round iterative function, and ends with final transform of the output of round function. The mentioned round function employs two functions F_0 and F_1 plus XOR and addition operations. Functions F_0 and F_1 are based on simple XOR and shift operations [33].

Hummingbird: This cipher was introduced in 2010 by Daniel Engels et al. It has a hybrid structure composed of block- and stream-based designs. It employs a 16-bit block size, a 256-bit key size and an 80-bit internal state. The size of the key and the internal state of Hummingbird provides an adequate level of security for many embedded applications. The overall structure of the Hummingbird encryption algorithm uses four 16-bit block ciphers E_{k1},E_{k2},E_{k3},E_{k4}, plus 16-bit internal state registers, and a 16-stage LFSR. Each block cipher has a 16-bit substitution-permutation structure and a 64-bit key size. In the SPN structure, the block-based part of the cipher uses the XOR operation for Key Addition, four 4-bit different S-boxes for substitution layer, and a XOR-included linear transform [14].

PRESENT: This cipher, which was developed in 2007 by A. Bogdanov et al, is based on a substitution-permutation structure, 64-bit blocks, and 80-bit keys. Addition part of round key consists of simple XOR operation. The substitution layer is composed of sixteen 4-bit S-boxes and the permutation layer consists of bitwise permutation. This algorithm runs a 31-round iteration to return a ciphertext. In 2012, this cipher was approved by International Organization for Standardization (ISO / IEC 29192-2) as a standard lightweight block cipher [24].

PRINTcipher: In 2010, Lars Knudsen et al. designed this cipher specifically for IC-printing. The aim of their design was to ensure memory persistence. This design has two versions, 48-bit and 96-bit. The 48-bit version uses a 48-bit secret key. This cipher uses b-bit blocks ($b \in \{48, 96\}$) and an effective key length of (5/3*b)-bits, and its structure is based on b-round substitution-permutation network. For instance, the 48-bit version of this cipher uses 48-bit blocks and 80-bit key and enjoys a 48-round structure. The encryption process of this cipher starts with a 48-bit mapping on the input; cipher then applies one round of XOR on the 6 least significant bits, and subjects the output to key-dependent permutation and then to substitution layer. Substitution layer of this cipher consists of sixteen 3-bit S-boxes. The output of this layer is the output of one round. As mentioned earlier, the PRINTcipher-48 employs 48 rounds, which means 48 iteration of the described process [16].

KATAN&KTANTAN: Christophe De Canniere et al. developed this family of ciphers in 2009. Both versions utilize 32, 48 and 64-bit block size, and share 80-bit key and security level. KTANTAN is the compact version of the cipher, where the key is burnt into the device and cannot be changed. In these ciphers, the plaintext is loaded into two registers. In each round, cipher selects several bits of registers, subjects them to Boolean functions and then loads the output into the least significant bits of the shifted registers. This cipher needs 254 rounds of iteration to ensure sufficient mixing [20].

mCrypton: This cipher, which was developed in 2005 by Chae Hoon Lim et al., uses 64-bit blocks and 64,96, or 128-bit key sizes. The main objective of this cipher is to optimize the efficiency for resource-constrained applications. mCrypton processes the 8-bit data blocks 4 expressed as 4 by 4 nibble array. Each round of transformation consists of 4 operations: nibble-wise substitution, column-wise bit permutation, column-to-row transposition, and key addition. The encryption process of this cipher consists of 12 iterations of round transformation [21].

KLEIN: This cipher was designed by Zheng Gong et al in 2011. The basic structure of this cipher is based on substitution-permutation network (SPN), and it has been designed with round counts of 12, 16, and 20 for 64, 80, and 98 bit variations. The cipher's input and output are in the form of one-dimensional array of bytes. In this cipher, operations are optimized with byte-oriented algorithms. Like many other SPN-based ciphers, the stage of Add-Round-key is implemented via simple XOR operation. The substitution stage uses 16 similar involutive S-boxes; this involution property means S(x)=y, S(y)=x and S(S(x))=x.

The advantage of using an involutive s-box is the reduction of extra cost of inverse implementation which leads to efficient serialization [15].

TWINE: This cipher was developed in 2013 by T. Suzaki et al. It uses 64-bit block size and 80 or 128 bit key size. The design of this cipher is geared toward desirable hardware and software performance on different types of central processors. This design is based on type-2 generalized Feistel Network (GFN-2) with sixteen nibble blocks. This cipher partitions the 64-bit block to sixteen X_i , and in line with GFN-2 structure, uses 8 simple F functions. The X's having an even subscript proceed to the next stage as they are, but they are inserted into the positions set by 4-bit-wise permutation. Cipher also imports the X's with even subscripts into F function and XORs them with the X's having an odd subscript. Here, permutation employs 4-bit words and forms the linear part of the cipher [27].

SIMON: In 2013, Ray Beaulieu et al. developed this family of ciphers with different block and key sizes. SIMON2n uses n-bit words (in this case block size is 2n), where n can be 16, 24, 32, 48, or 64- bit. This SIMON2n /

mn uses m-word (mn-bit) key. For instance SIMON64/128 will employ 64-bit blocks and 128-bit keys. All SIMON ciphers use the same Feistel rule. The algorithm of these ciphers is engineered to be easily serialized at different levels of extremely small hardware, but not at the expense of software performance [35].

SPECK: This cipher was specifically designed to provide optimized hardware and software performance on microcontrollers. Nomenclature of SPECK is similar to that explained for SIMON. For instance, SPECK96/144 will use 96-bit block and 144-bit key size. This cipher utilizes bitwise XOR, modular addition 2^n, left circular shift S^j by j bits, and right circular shift S^{-j} by j bits [35].

PRINCE: This cipher was designed in 2012 by Julia Borghoff et al. PRINCE uses 64-bit block size and 128-bit key size and is based on FX structure. The cipher employs a Key Whitening component to spread the effect of key throughout the plaintext and prevent key-based attacks. Between the key whitening parts is the 12-round PRINCE core. This core consists of simple XOR, addition of round constant, plus substitution and Matrix-M operations. This design uses similar 4-bit S-boxes, and twelve 64-bit round constants [25].

PRIDE: In 2012, Martin R. Albrecht et al. developed the PRIDE cipher, which like PPRINCE, is based on FX structure. This cipher uses 64-bit block size and 128-bit key size. This cipher extracts the first whitening key k from the first half the key k and uses the other half to obtain the second whitening key k_1 . To ensure effective bit-sliced implementation, it uses a bit permutation at the start and the end of process. The encryption process of this cipher starts with an initial bit permutation on plaintext. Cipher then subjects the results to an XOR with the first whitening key. It then applies 19 identical rounds of iteration on the output. The 20th round, which is applied on the output of round 19, is slightly different than the others. Cipher then XORs the results with the second whitening key and then applies the secondary bit permutation on the result. The output of this process will be the ciphertext c. The round function R, which is applied on the first 19 rounds, is a classical substitution-permutation network. In this function, the key Addition stage is implemented by a XOR. The substitution layer consists of sixteen 4-bit S-boxes. The linear parts of this function include the first bit permutation, the L function, and the second bit permutation. The 20th round includes only the substitution layer [28].

Hummingbird2: Daniel Engels et al. developed the HB2 in 2012. This cipher uses a 128-bit secret key and a 64-bit initialization vector. The main advantage of this cipher is its ability to produce authentication tags for each selectively processed message. This cipher has a 128-bit internal state which is initialized by a 64-bit array. HB2 is a hybrid construct composed of block and stream ciphers and, like HB, works with 16-bit block size. So its operations have been designed for 16-bit words. This cipher uses a nonlinear F function, which has been defined by a linear operation on 4 different nonlinear S-boxes. This means that the input of linear function is the output of non-linear function (S-box) [51].

LBLOCK: This cipher was introduced in 2011 by Wenling Wu et al. It works with 64-bit block size and 80-bit key size, and is based on 32-round Feistel structure. The security of Feistel structure is associated with the round function F. The round function of this cipher is composed of two parts, S and P, which establish the basic Shannon principles. The substitution layer S is responsible for clutter operation and the permutation layer P diffuses the Shannon principles. The substitution layer has eight parallel 4-bit S-boxes, and the permutation layer consists of eight 4-bit permutations, i.e. the basic element of this permutation works with 4 bits. It should be mentioned that this cipher uses 8 different S-boxes [17].

MIBS: Maryam Izadiet al. designed the MIBS cipher in 2009. This Feistel-based 32-round cipher uses 64-bit blocks and 46 and 80-bit keys. The round function of this cipher consists of 8 identical S-boxes with 24 XOR elements, and produces a good level of clutter. The method used in this round function is similar to methods of sorting networks. This means that the method by which cipher selects the XOR inputs is similar to methods sorting networks use to choose the (two) input elements. The key addition stage of this cipher utilizes a set of XOR elements, and its permutation layer is in the form of 4-bit element arrangements [18].

Puffin: This cipher was developed in 2011 by Huiju Cheng et al. It uses a 64-bit block size and a 128-bit key size, and is based on substitution-permutation network. The features of this cipher include its simple and involutive design. The SPN-based ciphers usually use several different data paths for encryption and decryption and depend on some elements to inverse the process, but the involutive nature of Puffin allows the use of encryption elements for inversion. Like many other SPN-based ciphers, the key addition stage of this cipher is implemented via an XOR

ACSIJ Advances in Computer Science: an International Journal, Vol. 5, Issue 4, No.22 , July 2016
ISSN : 2322-5157
www.ACSIJ.org

operation. Its substitution layer consists of sixteen parallel 4-bit S-boxes, and its permutation layer has a bit-wise design, which if implemented in wire crossings, does not cost any hardware gates. In each round of substitution operation, cipher runs the Add-Round-key and the permutation in that order, and repeats the process for 32 round of iteration [26].

ESF: Eight-sided fortress was developed by LIU Xuan et al. in 2014. Like many other block ciphers, it uses 64-bit block size and 80-bit key size and is based on Feistel structure. The main component of this structure is the round function, which in this cipher is based on substitution permutation network (SPN). The aim of this cipher is to optimize the computational requirements. The round function of this cipher first subjects the 32-bit round key k and a half-block to an XOR function. The cipher then processes the output of this XOR by eight 4-bit S-boxes. The permutation layer of this round function has been designed in the form of bit permutation [5].

Piccolo: developed in 2011 by Kyoji Shibutani et al., this cipher uses a 64-bit block size and an 80 or 128-bit key size, and is based on type-2 Generalized Feistel Network (GFN-2). Its round function F contains eight identical S-boxes. This round function first applies four parallel 4-bit S-boxes on the input and then uses the diffusion matrix M. To produce the final output, the round function again subjects the output to four parallel 4-bit S-boxes. The permutation part of this structure is based on bit-ward permutation [23].

Khudra: In 2014, S. Kolay et al. developed this cipher specifically for FPGAs. This GFN2-based cipher uses a 64-bit block size and an 80 -bit key size. It utilizes two F-functions with 16-bit inputs; each F-function is based on 4-bit GFN2 structure and is employed in 6-rounds of iteration. The cipher itself uses 18 rounds of iteration. The substitution boxes used in this cipher are similar to those used in the cipher PRESENT, and have maximum algebraic degree and minimum linear-differential probability [53].

2. LIGHTWEIGHT CIPHERS EVALUATION

Lightweight ciphers can be assessed in terms of cost, speed and efficiency. Implementation type affects the application of the desired measure for effective Evaluation. Lightweight ciphers will be evaluated based on these terms in the next sections.

2.1 Evaluation of lightweight ciphers in terms of cost

Lightweight ciphers Evaluation measure in terms of cost in hardware implementation is the gate equivalent, while in software implementation, we use the measures of RAM, ROM and code size. Lightweight ciphers Evaluation using these indicators is discussed in the following.

2.1.1 Hardware implementation

Cost in hardware implementation is the occupied space. It means the size of the space that is occupied by the designed hardware, and based on minimization of this criterion, the new cipher will be appropriate in terms of cost. Space needs are usually measured in μm^2, but the amount is dependent on the manufacturing technology and standard cell library. For independent comparison of space needs, the space is usually expressed as a Gate Equivalent (GE)[34,41,43,57,58]. One GE is equal to the space needed by dual-input NAND gate. Space in GE is achieved by dividing the occupied space in scale of μm^2 to dual-input NAND gate occupied space[48,49,52]. Fig. 1 shows the space occupied for lightweight ciphers in hardware implementation.

ACSIJ Advances in Computer Science: an International Journal, Vol. 5, Issue 4, No.22 , July 2016
ISSN : 2322-5157
www.ACSIJ.org

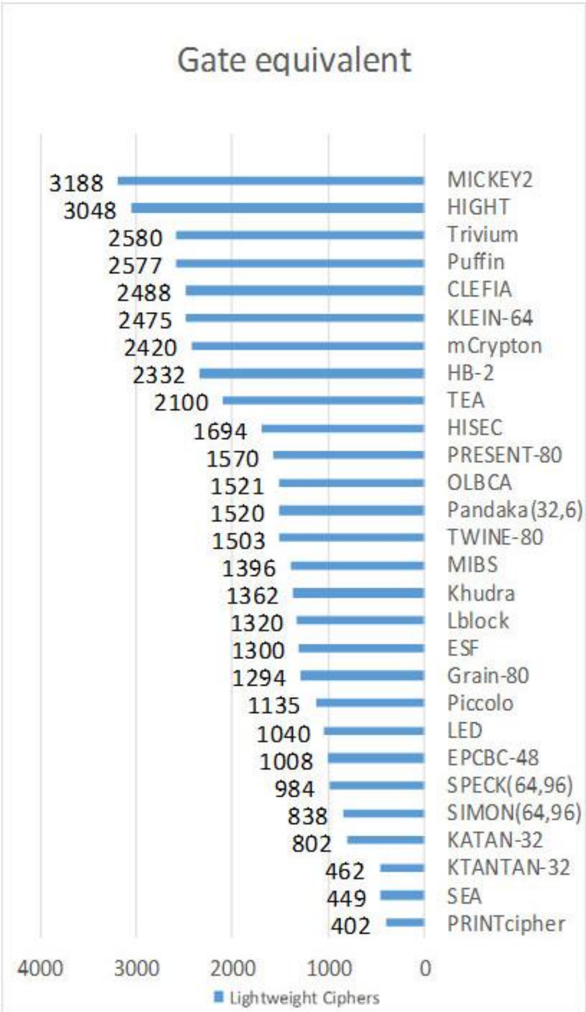

Fig.1. Evaluation of lightweight ciphers in terms of cost with GE measure

As it is obtained from Fig.1, it can be said that PRINTcipher [16] is the most appropriate cipher in terms of hardware cost with GE measure. But, unfortunately, this cipher is designed for a particular area with a specific purpose and is not suitable for general use because of poor security. SEA cipher is not suitable for general use due to security weaknesses and vulnerabilities against a lot of attacks. It seems that KTANTAN-32 [20] cipher is suitable for use. More of new ciphers select PRESENT cipher as their criteria for evaluation and optimal performance; this is because it is standard. The best ciphers are new ciphers of SIMEON and SPECK. Piccolo cipher is next in rank. If GE measure is our Evaluation criterion, PRINTcipher will be the most appropriate cipher, but one must bear in mind that the best cipher is the one that improves criteria of cost, efficiency and security in an equivalent state.

2.1.2 Software implementation

The cost of software implementation is the amount of RAM, ROM and code size. Evaluation of lightweight ciphers in terms of software implementation with RAM measure is shown in Fig. 2; and Fig. 2, Fig.3 and Fig. 4 show the implementation using ROM measure.

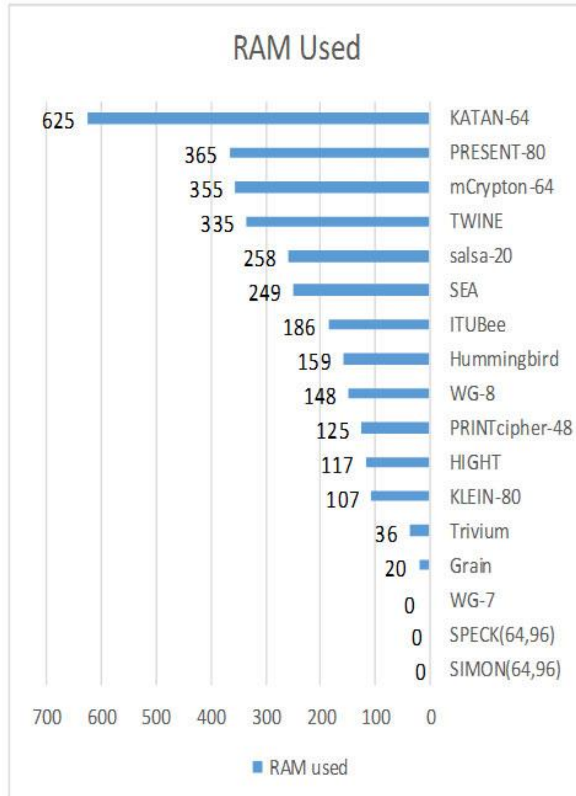

Fig.2. Evaluation of lightweight ciphers in terms of software implementation costs by the RAM used measure

As it is obtained from Fig.2, in the Evaluation of lightweight ciphers in terms of software implementation by the measure of RAM used in the implementation, lightweight ciphers of WG-7 [37], SIMON (64, 96), and SPECK (64, 96) with zero needed RAM, are the best lightweight ciphers in terms of RAM used. Ciphers of Grain, Trivium and KLEIN-80 are in the next ranks of the best lightweight ciphers in terms of the RAM used.

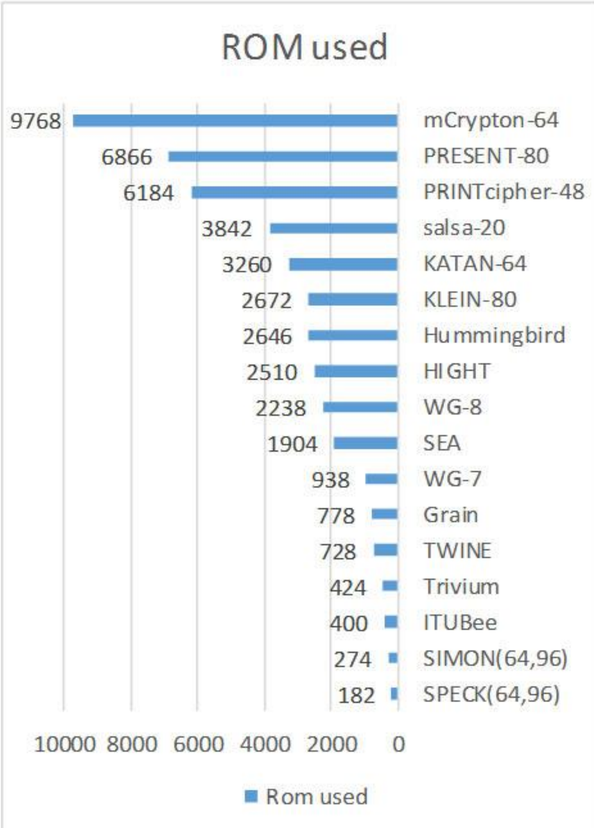

Fig.3. Evaluation of lightweight ciphers in terms of software implementation costs by the ROM used

As it is obtained from Fig. 3, in the Evaluation of lightweight ciphers in terms of software implementation by the measure of ROM used in the implementation, lightweight ciphers of SPECK (64, 96) and SIMON (64, 96) are of the best lightweight ciphers in terms of software implementation costs. ITUBee [19], Trivium[45], TWINE [27], Grain[46], WG-7 [2,37] are in the next ranks of the best lightweight ciphers in terms of the ROM used in the software implementation.

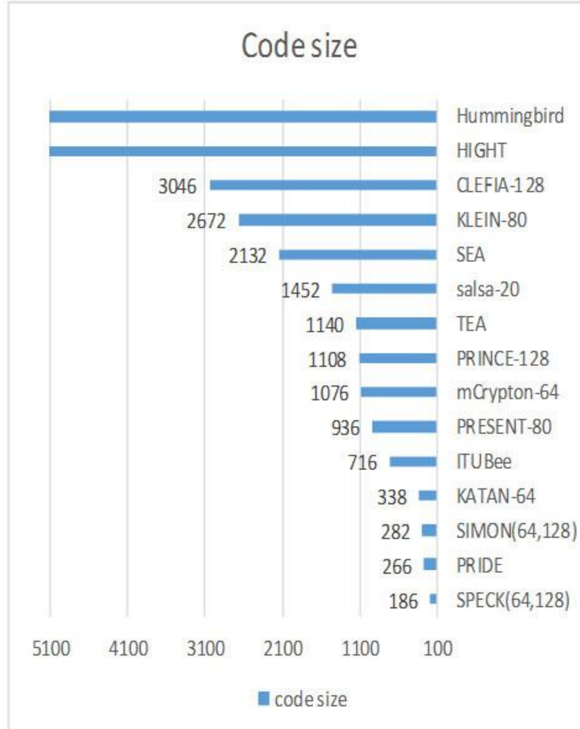

Fig.4. Evaluation of lightweight ciphers in terms of software implementation costs by code size measure

As it is obtained from Fig. 4, in the Evaluation of lightweight ciphers in terms of software implementation by the measure of code size, ciphers of SPECK (64, 128) and PRIDE [28] are suitable ciphers. SIMON (64,128), KATAN-64, ITUBee are in the next ranks of the best lightweight ciphers in terms of software implementation costs by the measure of code size. The size of Hummingbird and HIGH ciphers is higher than the scaled and maximum values of the figure.

2.2 Evaluation of lightweight ciphers in terms of speed

The measures of lightweight ciphers Evaluation in terms of speed are the number of clock cycles per block and the number of cycles to byte in the hardware and software implementation, respectively. Evaluation of lightweight ciphers using these measures is as follows.

2.2.1 Hardware implementation

In the Evaluation of lightweight ciphers in terms of speed in hardware implementations, the number of clock cycles per block and the time required are the most important measures. The required amount of time for a given task can be achieved by dividing the number of cycles to the operating frequency. Since the operating frequency should be the same to properly assess the lightweight ciphers by time measure, in fact, this measure can be considered dependent on the number of cycles. After Evaluation, one of these measures of time and cycle is sufficient. The Evaluation of lightweight ciphers in terms of speed by the measure of the number of clock cycles per block is shown in Fig. 5.

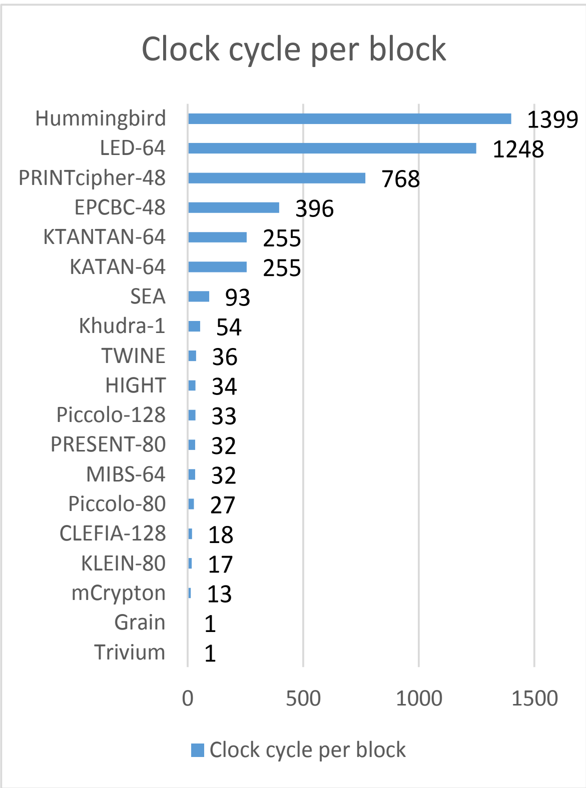

Fig.5. Evaluation of lightweight ciphers in hardware implementation in terms of speed by the measure of clock cycle per block

As can be seen in Fig. 5, the best lightweight ciphers in hardware implementation in terms of speed by the measure of clock cycle per block are the ciphers of Trivium[45] and Grain[46] with 1 clock cycle per block. Lightweight ciphers of mCrypton, KLEIN-80, CLEFIA-128[42], Piccolo-80, MIBS-64 are in the next ranks of the best lightweight ciphers in hardware implementation in terms of speed by the measure of clock cycle per block.

2.2.2 Software implementation

The measure of lightweight ciphers Evaluation in terms of speed in software implementation is the number of clock cycle per byte[4,22,32,35,54]. Evaluation of lightweight ciphers in terms of speed in software implementation by the measure of clock cycle per byte is shown in Fig. 6.

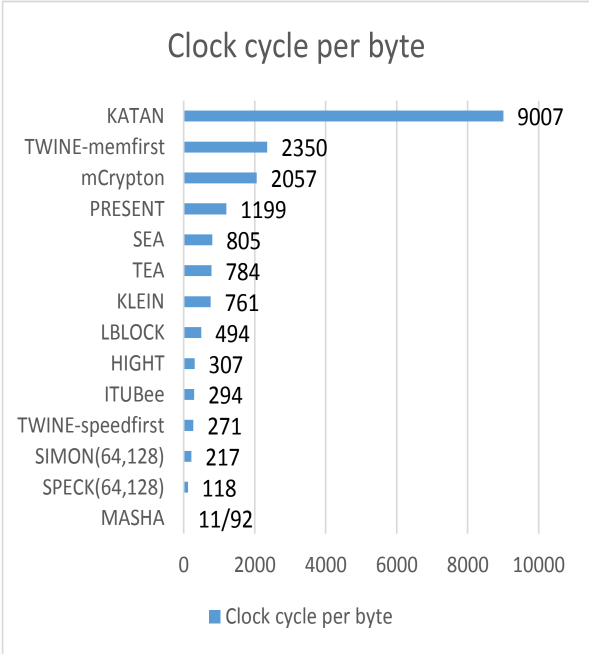

Fig.6. Evaluation of lightweight ciphers in terms of speed in software implementation by the measure of clock cycle per byte

As can be seen in Fig. 6, the best lightweight ciphers in hardware implementation in terms of speed by the measure of clock cycle per byte is the cipher MASHA [32]. SPECK (64,128), SIMON (64,128), TWINE-speedfirst [27] are in the next ranks of the best lightweight ciphers in software implementation in terms of speed by the measure of clock cycle per byte.

2.3 Evaluation of lightweight ciphers in terms of efficiency

Evaluation of lightweight ciphers in terms of efficiency has been emerged in the scientific literature with measures of Throughput and low Latency. Throughput includes the rate at which the output is produced[22,29]. In fact, it is the number of output bits in time. It is expressed by the unit of bits per second (bps). Evaluation of lightweight ciphers in terms of efficiency with Throughput measure is expressed in Fig. 7.

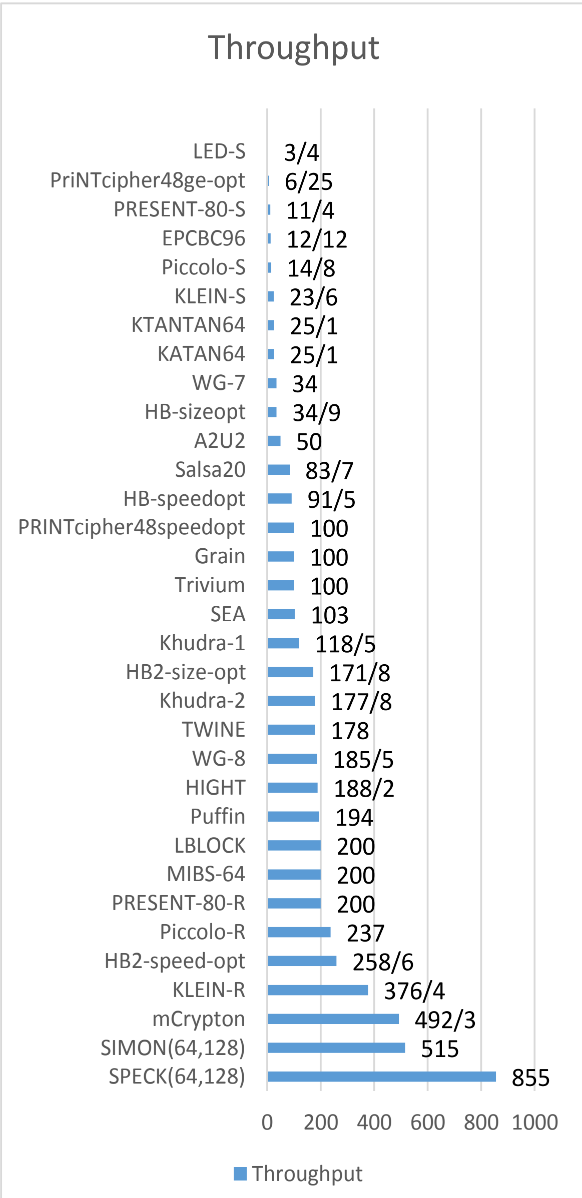

Fig.7. Evaluation of lightweight ciphers in terms of efficiency with Throughput measure

As can be seen in Fig. 7, SPECK (64,128) is the best lightweight cipher in terms of efficiency with Throughput measure. Ciphers of SIMON (64,128), mCrypton, KLEIN-R, HB2-size-optimize are in the next ranks of the best lightweight ciphers in terms of efficiency with Throughput measure.

Latency

It is the time that is required to encrypt a block of message. The Latency or delay can be obtained by multiplying the number of cycles on the critical path[40]. Throughput of and latency are different. The latency depends on the inherent qualities of cryptographic algorithms while Throughput can be simply increased by the use of common signal processing techniques such as parallel computing and pipeline[40]. The Latency has not been more examined in the lightweight ciphers, because the ciphers with low latency are not usually considered as lightweight ciphers. This is why few studies have been done in the literature for lightweight ciphers. Evaluation of lightweight ciphers in terms of efficiency with low latency measure is shown in Fig. 8.

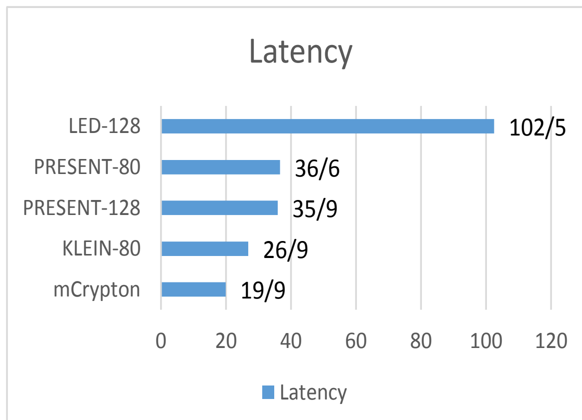

Fig.8. Evaluation of lightweight ciphers in terms of efficiency with low latency measure

As can be seen in Fig. 8, mCrypton96 is the best lightweight cipher in terms of efficiency with low latency measure. Ciphers of KLEIN 80, PRESENT 128, PRESENT 80 are in the next ranks of the best lightweight ciphers in terms of efficiency with latency measure.

3. Conclusions

Lightweight ciphers have not been comprehensively examined and evaluated in terms of speed, cost and efficiency. This led us to review and assess the lightweight ciphers in this work. Evaluation in terms of costs in the hardware and software implementation shows the superiority of SPECK and SIMON ciphers. Evaluation in terms of speed in the hardware implementation indicates the superiority of Trivium, Grain, and it shows the superiority of MASHA and SPECK ciphers in software implementation. The results of Evaluation in terms of efficiency indicate the superiority of SIMON and SPECK. Using the results of these Evaluations, we can express the best available cipher based on the needs and limitations. This helps finding the most appropriate cipher for the user's desired system based on requirements and restrictions.

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] Jana, Swarnendu, Jaydeb Bhaumik, and Manas Kumar Maiti. "Survey on Lightweight Block Cipher." *International Journal of Soft Computing and Engineering* 3 (2013): 183-187.

[4] Cazorla, M., Gourgeon, S., Marquet, K., & Minier, M. (2015). Survey and benchmark of lightweight block ciphers for MSP430 16-bit microcontroller. *Security and Communication Networks*, *8*(18), 3564-3579.

[5] 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.

[6] Cazorla, Mickaël, Kevin Marquet, and Marine Minier. "Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks⋆." *IDEA* 64, no. 128 (2013): 34.

[7] Kong, Jia Hao, Li-Minn Ang, and Kah Phooi Seng. "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments." *Journal of Network and Computer Applications* 49 (2015): 15-50.

[8] Mohd, Bassam J., Thaier Hayajneh, and Athanasios V. Vasilakos. "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues." *Journal of Network and Computer Applications* (2015).

[9] Zhu, Xiaowei, Samar K. Mukhopadhyay, and Hisashi Kurata. "A review of RFID technology and its managerial applications in different industries." *Journal of Engineering and Technology Management* 29, no. 1 (2012): 152-167.

[10] Delgado-Mohatar, Oscar, Amparo Fúster-Sabater, and José M. Sierra. "A light-weight authentication scheme for wireless sensor networks." *Ad Hoc Networks*9, no. 5 (2011): 727-735.

[11] Movassaghi, Samaneh, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour. "Wireless body area networks: A survey." *Communications Surveys & Tutorials, IEEE* 16, no. 3 (2014): 1658-1686.

[12] Tian, Yun, Gongliang Chen, and Jianhua Li. "QUAVIUM-a new stream cipher inspired by TRIVIUM." *Journal of Computers* 7, no. 5 (2012): 1278-1283.

[13] Hoang, Viet Tung, and Phillip Rogaway. "On generalized Feistel networks." In*Advances in Cryptology–CRYPTO 2010*, pp. 613-630. Springer Berlin Heidelberg, 2010.

[14] 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.

[15] Gong, Zheng, Svetla Nikova, and Yee Wei Law. *KLEIN: a new family of lightweight block ciphers*. Springer Berlin Heidelberg, 2012.

[16] Knudsen, Lars, Gregor Leander, Axel Poschmann, and Matthew JB Robshaw. "PRINTcipher: a block cipher for IC-printing." In *Cryptographic Hardware and Embedded Systems, CHES 2010*, pp. 16-32. Springer Berlin Heidelberg, 2010.

[17] Wu, Wenling, and Lei Zhang. "LBlock: a lightweight block cipher." In *Applied Cryptography and Network Security*, pp. 327-344. Springer Berlin Heidelberg, 2011.

[18] Izadi, Maryam, Babak Sadeghiyan, Seyed Saeed Sadeghian, and Hossein Arabnezhad Khanooki. "MIBS: a new lightweight block cipher." In *Cryptology and Network Security*, pp. 334-348. Springer Berlin Heidelberg, 2009.

[19] Karakoç, Ferhat, Hüseyin Demirci, and A. Emre Harmancı. "ITUbee: a software oriented lightweight block cipher." In *Lightweight Cryptography for Security and Privacy*, pp. 16-27. Springer Berlin Heidelberg, 2013.

[20] De Canniere, Christophe, Orr Dunkelman, and Miroslav Knežević. "KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers." In*Cryptographic Hardware and Embedded Systems-CHES 2009*, pp. 272-288. Springer Berlin Heidelberg, 2009.

[21] Lim, Chae Hoon, and Tymur Korkishko. "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.

[22] Chen, Min, Shigang Chen, and Qingjun Xiao. "Pandaka: A lightweight cipher for RFID systems." In *INFOCOM, 2014 Proceedings IEEE*, pp. 172-180. IEEE, 2014.

[23] Shibutani, Kyoji, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. "Piccolo: an ultra-lightweight blockcipher." In*Cryptographic Hardware and Embedded Systems–CHES 2011*, pp. 342-357. Springer Berlin Heidelberg, 2011.

[24] Bogdanov, Andrey, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe.*PRESENT: An ultra-lightweight block cipher*. Springer Berlin Heidelberg, 2007.

[25] Borghoff, Julia, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, 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.

[26] 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.

[27] 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.

[28] Albrecht, Martin R., Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, and Tolga Yalçın. "Block ciphers–focus on the linear layer (feat. PRIDE)." In *Advances in Cryptology–CRYPTO 2014*, pp. 57-76. Springer Berlin Heidelberg, 2014.

[29] David, Mathieu, Damith C. Ranasinghe, and Torben Larsen. "A2U2: a stream cipher for printed electronics RFID tags." In *RFID (RFID), 2011 IEEE International Conference on*, pp. 176-183. IEEE, 2011.

[30] Chen, Tieming, Liang Ge, Xiaohao Wang, and Jiamei Cai. "TinyStream: A lightweight and novel stream cipher scheme for wireless sensor networks." In*Computational Intelligence and Security (CIS), 2010 International Conference on*, pp. 528-532. IEEE, 2010.

[31] Fan, Xinxin, Kalikinkar Mandal, and Guang Gong. "Wg-8: A lightweight stream cipher for resource-constrained smart devices." In *Quality, Reliability, Security and Robustness in Heterogeneous Networks*, pp. 617-632. Springer Berlin Heidelberg, 2013.

[32] Kiyomoto, Shinsaku, Matt Henricksen, Wun-She Yap, Yuto Nakano, and Kazuhide Fukushima. "MASHA–Low Cost Authentication with a New Stream Cipher." In *Information Security*, pp. 63-78. Springer Berlin Heidelberg, 2011.

[33] 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.

[34] 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.

[35] Beaulieu, Ray, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. "The SIMON and SPECK Families of Lightweight Block Ciphers." *IACR Cryptology ePrint Archive* 2013 (2013): 404.

[36] Kumar, Naveen, Shrikant Ojha, Kritika Jain, and Sangeeta Lal. "BEAN: a lightweight stream cipher." In *Proceedings of the 2nd international conference on Security of information and networks*, pp. 168-171. ACM, 2009.

[37] Luo, Yiyuan, Qi Chai, Guang Gong, and Xuejia Lai. "A lightweight stream cipher WG-7 for RFID encryption and authentication." In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1-6. IEEE, 2010.

[38] Manifavas, Charalampos, George Hatzivasilis, Konstantinos Fysarakis, and Konstantinos Rantos. "Lightweight cryptography for embedded systems–A comparative analysis." In *Data Privacy Management and Autonomous Spontaneous Security*, pp. 333-349. Springer Berlin Heidelberg, 2014.

[39] Standaert, François-Xavier, Gilles Piret, Gaël Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat. "ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware." In *Fast Software Encryption*, pp. 279-298. Springer Berlin Heidelberg, 2004.

[40] Knežević, Miroslav, Ventzislav Nikov, and Peter Rombouts. "Low-Latency Encryption–Is “Lightweight= Light+ Wait”?." In *Cryptographic Hardware and Embedded Systems–CHES 2012*, pp. 426-446. Springer Berlin Heidelberg, 2012.

[41] Wheeler, David J., and Roger M. Needham. "TEA, a tiny encryption algorithm." In *Fast Software Encryption*, pp. 363-366. Springer Berlin Heidelberg, 1995.

[42] Shirai, Taizo, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. "The 128-bit blockcipher CLEFIA." In *Fast software encryption*, pp. 181-195. Springer Berlin Heidelberg, 2007.

[43] Babbage, Steve, and Matthew Dodd. "The MICKEY stream ciphers." In *New Stream Cipher Designs*, pp. 191-209. Springer Berlin Heidelberg, 2008.

[44] 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.

[45] De Cannière, Christophe. "Trivium: A stream cipher construction inspired by block cipher design principles." In *Information Security*, pp. 171-186. Springer Berlin Heidelberg, 2006.

[46] Hell, Martin, Thomas Johansson, and Willi Meier. "Grain: a stream cipher for constrained environments." *International Journal of Wireless and Mobile Computing* 2, no. 1 (2007): 86-93.

[47] Ojha, Shri Kant, Naveen Kumar, and Kritika Jain. "TWIS–A Lightweight Block Cipher." In *Information Systems Security*, pp. 280-291. Springer Berlin Heidelberg, 2009.

[48] AlDabbagh, Sufyan Salim Mahmood, Al Shaikhli, Imad Fakhri Taha, and Mohammad A. Alahmad. "HISEC: A New Lightweight Block Cipher Algorithm." In *Proceedings of the 7th International Conference on Security of Information and Networks*, p. 151. ACM, 2014.

[49] Yap, Huihui, Khoongming Khoo, Axel Poschmann, and Matt Henricksen. "EPCBC-a block cipher suitable for electronic product code encryption." In*Cryptology and Network Security*, pp. 76-97. Springer Berlin Heidelberg, 2011.

[50] Feng, Dengguo, Xiutao Feng, Wentao Zhang, Xiubin Fan, and Chuankun Wu. "Loiss: A byte-oriented stream cipher." In *Coding and Cryptology*, pp. 109-125. Springer Berlin Heidelberg, 2011.

[51] Engels, Daniel, Markku-Juhani O. Saarinen, Peter Schweitzer, and Eric M. Smith. "The Hummingbird-2 lightweight authenticated encryption algorithm." In*RFID. Security and Privacy*, pp. 19-31. Springer Berlin Heidelberg, 2012.

[52] Aldabbagh, Sufyan Salim Mahmood, and Imad Fakhri Taha Al Shaikhli. "OLBCA: A New Lightweight Block Cipher Algorithm." In *Advanced Computer Science Applications and Technologies (ACSAT), 2014 3rd International Conference on*, pp. 15-20. IEEE, 2014.

[53] Kolay, Souvik, and Debdeep Mukhopadhyay. "Khudra: A New Lightweight Block Cipher for FPGAs." In *Security, Privacy, and Applied Cryptography Engineering*, pp. 126-145. Springer International Publishing, 2014.

[54] Tahir, Ruhma, Muhammad Younas Javed, Attiq Ahmad, and Raja Iqbal. "SCUR: Secure Communications in Wireless Sensor Networks using Rabbit." In *Proceedings of the World Congress on Engineering*, vol. 1, pp. 2-4. 2008.

[55] Leander, Gregor, Christof Paar, Axel Poschmann, and Kai Schramm. "New lightweight DES variants." In *Fast Software Encryption*, pp. 196-210. Springer Berlin Heidelberg, 2007.

[56] Rolfes, Carsten, Axel Poschmann, Gregor Leander, and Christof Paar. "Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents." In *Smart Card*

Research and Advanced Applications, pp. 89-103. Springer Berlin Heidelberg, 2008.
[57] Kaps, Jens-Peter. "Chai-tea, cryptographic hardware implementations of xtea." In *Progress in Cryptology-INDOCRYPT 2008*, pp. 363-375. Springer Berlin Heidelberg, 2008.
[58] Poschmann, Axel York. "Lightweight cryptography: cryptographic engineering for a pervasive world." In *Ph. D. Thesis*. 2009.
[59] Ågren, Martin. "On some symmetric lightweight cryptographic designs." PhD diss., Lund University, 2012.

Jaber hosseinzadeh is completed the Bachelor of Science in software engineering from Urmia University in 2013. He is a student in Master of Science in software engineering at Ferdowsi University of Mashhad. He is a member Of Data Communication and Security Lab in Ferdowsi University of Mashhad. His area of interest spans Network Security and Cryptography and Wireless sensor Networks security.

Maghsoud Hosseinzadeh is completed the Bachelor of Science in software engineering from Islamic Azad University of Urmia in 2011. His area of interest spans Cryptography and Wireless sensor Networks security.