IoT Light Weight (LWT) Crypto Functions

https://doi.org/10.3991/ijim.v13i04.10524

Nubila Nabeel (✉), Mohamed Hadi Habaebi,
Nurul Arfah Che Mustapha, Md Rafiqul Islam
International Islamic University, Selangor, Malaysia
13ganesh@mail.com

Abstract—We are in the era of IoT and 5G technologies. IoT has wide range of applications in Smart Home, Smart cities, Agriculture, Health etc. Due to that, the number of connected sensor devices become increased. Along with that security of these devices become a challenging issue. By the next year there would be a great increase in the number of connected sensor devices. For the power constrained devices like sensors and actuators, they requires lightweight security mechanism. There are several Lightweight (LW) energy efficient Hashing techniques are available. They are photon, quark, spongent, Lesamnta-LW etc. These all are fixed length block sized and key sized LW hashing techniques. All transformation methods used today in LW hash function only support fixed block size and key size and requires high hardware requirements too. In this paper, we compare different types of LW hash families in terms of their design and introduce the possibility of variable length hash function using Mersenne number based transform.

Keywords—Diffusion, lightweight hashing techniques, Mersenne number, energy efficiency.

1 Introduction

Internet of Things connects everyday physical objects to the Internet. That means it allows to connect the objects around us to the Internet. The worst thing about object is its security. The IoT devices are resource constrained devices. So that the traditional cryptographic techniques cannot apply directly to the IoT devices [1]. The Lightweight (LW) crypto functions are designed for resource constrained devices ie, for less memory, less computing resource and less power applications [2]. The LW cryptography is lighter as well as faster compare to cryptographic techniques such as public key cryptography, SHA etc. There are lot of LW hashing techniques are available today such as PHOTON(PH) [3], QUARK(QK) [4], SPONGENT(SPT) [5], GLUON(GL) [2] and SPN-HASH(SPH) [6] etc. This paper compares these LW hash functions in terms of their design. Hash of a message is constructed by first dividing it into several blocks and then iteratively and systematically processing these blocks, this sequential method is the most widely used up to now. There are several hash construction methods are available such as Merkle-Damgard Construction, Wide Pipe Construction, HAIFA Construction, and Sponge Construction. Most of the LW hash functions are designed and implemented by Sponge construction method (SPGM). SPGM is a class of algorithms with finite internal state which produces an arbitrary length output bit stream from an input bit stream. The two main properties for designing cryptographic techniques includes Confusion and diffusion. These properties evaluate the security of hash function. If we want to design new hash function then we must ensure the confusion and diffusion property. Confusion property makes a relationship between cipher text and the key used in the algorithm. Confusion property makes relationship in such a way that cipher text depends on many parts of the key. Diffusion property on the other hand makes connection between plain text and cipher text. Hence if we try to change one bit of the cipher text, then there should have approximately one half of the plaintext bits change. These properties are implemented by substitutions and permutations operations. Substitution operation makes changes in certain bits using other bits, Permutation operation changes the order of symbols according to some algorithm. This paper compares different permutations and transformation functions used in different LW hash families and introduce new Mersenne number transformation functions for good diffusion property. We can say that the successful attack happens when there is a break in one of the security properties of hash functions such as collision, preimage or second preimage. Different attacks in hash function can be categorized into two: Brute force attacks and Cryptanalytical attacks. The New Mersenne number transform is very sensitive to any change in the input stream. So it is expected to be against different attacks.

2 Literature Review

2.1 Photon (PH)

Main challenge in designing security mechanisms in RFID and Sensor devices is its resource constrained problem. RFID security is the main challenge in today's cryptography. There are many LW hashing techniques available today. The PH LW hash function family known to be the most light weight hash function and very close to the IoT applications [3]. The basic RID applications need about 10000 logical gates, with only between 200 and 2000 gates possible for security. The main difficulty with PH LW hash family is the dependence of the memory registers required for the computation.

In the PH LW hash family, each type defined by its hash value between 64 and 256 bits. Five different types of PH are PH-80-20-16, PH-128-16-16, PH-160-36-36, PH-224-32-32 and PH-256-32-32, which uses internal permutations PRM100, PRM144, PRM196, PRM256 and PRM288 respectively.

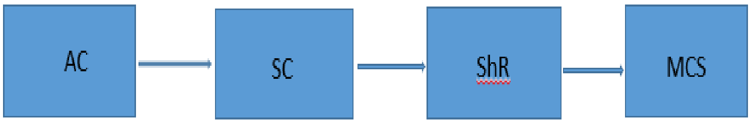

Fig. 1. Single round of a LW HASH permutation

Figure 1 shows the single round of permutation operation of PH. It contains four layers, Ad Constant (AC), Sub Cell (SC), Shift Rows (ShR) and Mix Columns Serial (MCS). The high power is needed for the serialized as well as parallelized implementation of Photon. If we consider the performance of various classes of PH we can see that for the PH hash function of small message has slight reduction in the throughput as compared to larger messages.

2.2 Quark (QK)

QK uses sponge construction method (SPGM). SPGM processes a text in three steps: First step is Initialization Step. Here the text is padded by appending one '1' bit followed by number of '0's. The second step is Absorbtion Step. In this step, the Xor operation is performed between *r*-bit message blocks and the last *r* bits of the state which is interleaved with the permutation *PER*. Third one is Squeezing Step. Here the hashed output is obtained by the last *r* bits of the state and interleaved with applications of the permutation *PER*, until desired output size returned.

The permutation *PER* implemented by non-linear Boolean functions and a linear Boolean function *PER*. The three classification of QK hash family are uQuark(U-QK), dQuark(D-QK), and tQuark(T-QK). Permutation of QK is showed in Figure 2. This uses two NFSRegisters (nonlinear feedback shift register), one LFSRegisters (linear feedback shift register) and three Boolean functions *f, g, h*. In addition to feedback registers there is a dedicated controller module.

U-Q provides 128 bit preimage resistance and 64 bit collision resistance. D-Q provides 160 bit preimage resistance and 80 bit collision resistance. And T-Q provides 224 bit preimage resistance and 112 bit collision resistance [4].

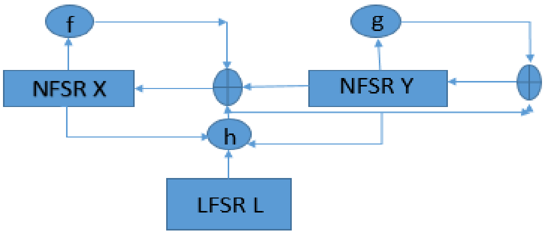

Fig. 2. Permutation of QK

The power required for U-Q, D-Q, and T-Q, are 2.96, 3.95 and 5.53μW respectively.

2.3 Present (PRT)

AES is most preferred by every block cipher cryptosystems. But AES could not work well for resource constrained devices in IoT. In these types of devices both security as well as hardware efficiency is important. So LW security mechanism is more essential for these kinds of devices. The main objective when designing Present was simplicity. PRT is implemented by SP-network, in Figure 3. It consists of 31 rounds. The block length is 64 bit and it support two key length 80 and 128. For more constrained devices 80 bits key length is preferred. In each 31 rounds consists of an XOR operation. The K_{32} is used to improve the security. The nonlinear layer uses a 4-bit Substitution box(S-Box) *S* and it is applied 16 times in each round in parallel.

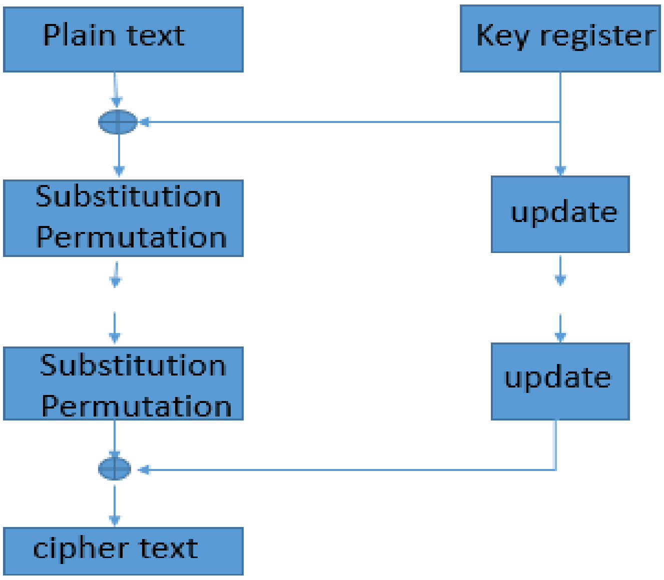

Fig. 3. Description of present

Present LW block cipher is applicable to resource-constrained devices. AES is considered to be require 1032 cycles per block and 3400 GE. Whereas Present require only 32 cycles per block and 1570 GE [7].

2.4 Spongent (SPT)

SPT is LW hash family which uses PRESENT (PRT) permutation. 13 types of SPT are available with different collision resistance, and preimage resistance with various implementation constraints. In some of the variants of SPT has reduced the second preimage resistance, while maintaining the collision resistance.

SPT uses PRT-permutation based SPGM. Figure 4 shows SPGM based on a b-bit PRT permutation π_b with capacity and rate bits c and r bits. m_i are r-bit input blocks. h_i are ith parts of the output.

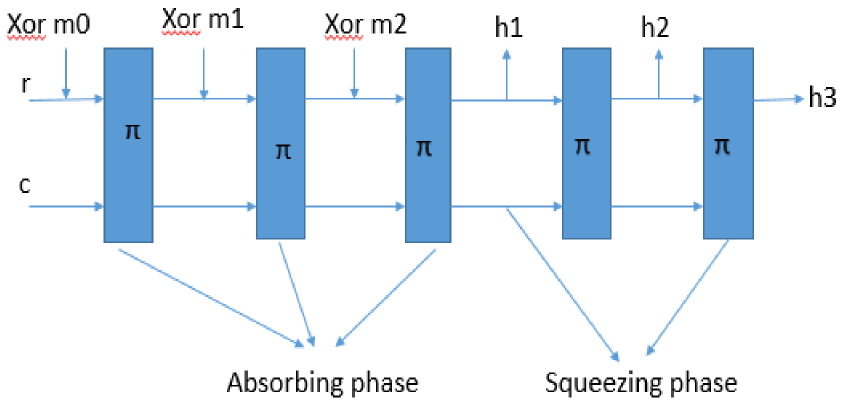

Fig. 4. Permutation Based SPM

The SPGM construction performed in three steps: First step is Initialization step. In this step padding the message using one bit ‘1’ and then a required number of 0 bits which must be multiple of r bits. Then padded input cut into blocks of r bits. Second one is Absorbing step. Here the xor operation is performed between r-bit input message and r bits of the state, and permutation operation π_b is interleaved. Next one is Squeezing step. In this step the r bits of the state are obtained as output, and perform interleaving with permutation PER π_b, until desired output length level returned.

The PER π_b: $F_2^b \longrightarrow F_2^b$ is the round transform of the b bits of state (st).

```
while i = 1 to R do
        st ← RlCounterb(i) $\oplus$ st $\oplus$ lCounterb(i)
        st ← SBoxLayerb (st)
        st ← PLayerb (st)
end while
```

Here SBoxLayerb and PLayerb describe about state(st) formation. Xor operation is performed between RlCounterb(i), st and lCounterb(i) in I th roiund. This state st is used in the Substitution box and obtained new state value. After that this state st is used in the permutation layer and generate new state value. The details of PRESENT is explained in [5].

2.5 Gluon (GL)

Gluon (GL) is a family of LW hash function which is implemented by SPGM. This family of Hash function uses Feedback with Carry Shift Register (FeCS). The hardware implementation is comparatively heavier than that of basic methods used in Quark and PH. FeCS registers are the alternative to Linear Feedback Shift Registers (LFS). The FeCS register has binary register and carry register but different from LFSRegister. LFSRegister perform XOR but in the case of FeCS register which perform addition with carry operation. FeCS register can help to solve the problems with LFS register. In LFS register based system requires filtering operation or Boolean function in order to break the linearity of LFSRegister. FeCS register based stream ciphers, this linearity problems solved by using the non-linearity property of the FeCS register. The transition function of an LFSRegister is linear at the same time quadratic that means nonlinear for an FeCS register. These are the main problems of LFSRegister based systems. However the implementation cost of an FeCS register is more than that of an LFSRegister. Like LFSRegister, FeCS register also not suitable to use directly for cryptography. It requires some filters to modify.

Three various form of GL hash function is available. GL-128-8, GL-160-16 and GL-224-32. In GL family transformation function is used instead of permutation in absorbing and squeezing parts of sponge construction. The transformation function f has good statistical property due to the 2-adic properties[2]

2.6 SPN Hash (SPNH)

SPNH is a new family of hash function which gives variable hash length of 128, 256 and 512 bits. It is constructed as resistance to collision as well as common attacks. The internal permutation is implemented as substitution- permutation network (SPN). SPNH uses Advanced encryption standard (AES) based permutations which only support fixed size key.

One single processing of an SPN structure consists of three layer parts. Key addition, substitution, and linear transformation (LT). The substitution part is made up of S boxes implemented in parallel. SPNH family has very effective confusion and diffusion properties. SPNH family uses JH mode operation which is the variant of SPNG. [6].

SPNH construction is based on fixed length unkeyed permutation PF. The internal state of *PF* is denoted by a matrix of order $x \times y$, where x is the number of bytes contained in a group, and y is the number of groups itself. Thus, *PF* works on a width of $b = 8xy$ bits, the rate and capacity are $4xy$-bit, and the output is a $4xy$-bit hash value. In the first step padding operation is performed on the input text m of length N bits and divided into blocks of $r = 4xy$ bits each. Then initialize the initialization variable (InV). For each padded message block, the JH mode of operation iteratively XORs the incoming $4xy$-bit input message block Mi into the left half of the state, applies the permutation $PF : GFe(2)8xy \rightarrow GFe(2)8xy$ to the internal state and XORs Mi into its right half.

SPNH-128: $y = 4, x = 8$

SPNH-256: $y = 8$, $x = 8$
SPNH-512: $y = 8$, $x = 16$

The 8xy-bit permutation PF iterates over 10 rounds. Its internal state is given by an x×y matrix. In Maximum distance separable (MDS) matrix, mix column is used for diffusion. The columns of the state are considered as a polynomial over GFe(2^8) and a mix columns operation is undertaken by multiplying the columns modulo a polynomial (x^4+2) with a fixed polynomial c(x). v is the output. The round function in SPNH is showed in Figure 6. After dividing padded input stream into blocks then substitution operation is performed then for the diffusion property Maximum distance separable transform is performed again this process continue.

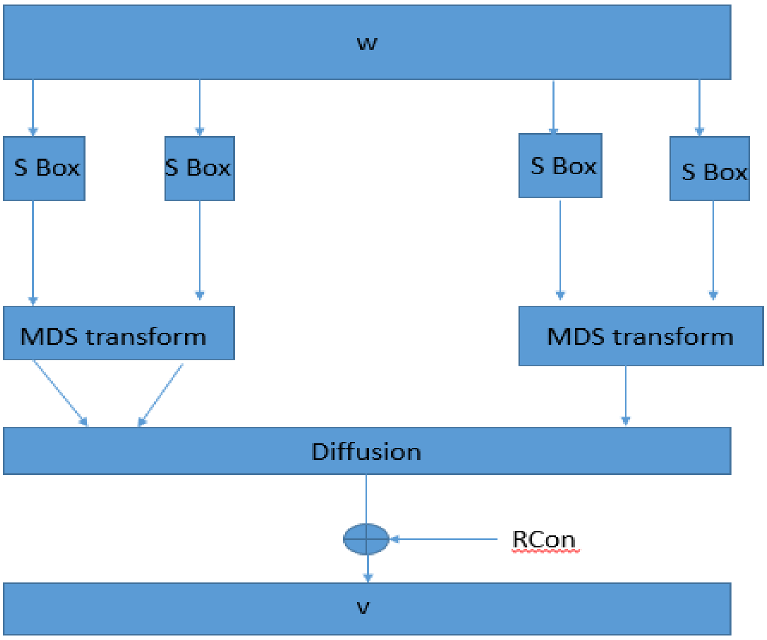

Fig. 5. The round function

These transformations are powerful in diffusing data. However, one drawback is that their length are fixed. So in order to meet the security requirements the key length and block size should become sufficient.

2.7 Lesamnta-LW(LLW)

LLW-256 is a LW hash function. For the resource-constrained devices like RFID, Sensors requires security mechanisms under restricted resource condition. LLW uses advanced encryption standard based block cipher with 256-bit plaintext and a key size of 128-bit. In Padding step of LLW, the last block contain the length of the message input. It does not contain any part of the message. This property guarantees preimage resistance of LLW [8]

LLW uses a 64-round block cipher *E*. It takes 128-bit key and 256-bit plaintext as input. The block cipher consists of two phases. The first one key scheduling function and the second one mixing function, which takes plaintext as input and the round keys to produce a cipher text.

The mix function consists of XOR operations, a word wise permutation, and a nonlinear function *Gf*.

PQ = MixColumns(MXC) ◦ SubBytes(SB).

The sub byte is a nonlinear substitution. In this substitution, the input is taken as four bytes ($s0$, $s1$, $s2$ *and* $s3$) and then Advanced Encryption Standard substitution box applied. S'i=S-Box (Si). The MXC step is given by the AES maximum distance separable matrix multiplication defined over GFe (2^8) as follows.

$$\begin{bmatrix} s_0' \\ s_1' \\ s_2' \\ s_3' \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix}$$

The main problem with the maximum distance separable matrix is that it is fixed in length. Both h/w and s/w implementation of LLW is effective.

2.8 LHash(LH)

LH is a LW hash family. This LW hash family support 3-hash size output: 80, 96, and 128 bits. LH has good preimage and collision resistance.

The implementation of LH uses a Feistel-PG (FPG) structure as the permutation. Feistel-PG (FPG) has comparable diffusion property. The Sub-box and maximum distance separable layer are hardware-friendly. The transformation is similar to and more compact than that of PH [9],

The internal permutations $FP96$ and $FP128$ are constructed using an 18-round FPG. In the permutation operation, First divide the input text into two parts $X1//X0$. Then for $i = 2$, 3... 19, calculate $Xi = Gb\ (FP\ (Xi-1 \oplus Ci-1)) \oplus Xi-2$. At last, $X19//X18$ is the output of the permutation. *Gb* is the concatenation operation, *FP* is the permutation operation.

The comparison of different LW Hash function in terms of design can be seen in Table 1.

3 Comparison of Existing Hash Functions

Table 1. Comparison of different LW hash functions in Terms of Design

Light weight hash functions	**Properties of different light weight hash functions**	
	Techniques used and Contributions	***Drawbacks***
PH	It uses Sponge constuction. Both s/w and h/w implementation is possible. Available in 5 different Hash length.	Uses mix column transform for diffusion property. These transformations are powerful in diffusion but they support only fixed block length. So in order to hash large amount of data it takes long time.
QK	U-Quark provides 128 bit preimage resistance and 64 bit collision resistance. D-Quark provides 160 bit preimage reistance and 80 bit collision resistance. And T-Quark provides 224 bit preimage resistance and 112 bit collision resistance. Good preimage and collision resistance	In QK, permutation is constructed by using two NFS Register and one LFSRegister. The transformation function of LFSRegister is linear. So for breaking the linearity in LFSRegister, filters or Boolean functions are needed. This incurs extra cost and Quark is only optimized for hardware. It takes long time to hash the longer message
SPT	It uses PRESENT permutation. It requires less time as compared to Photon and Quark.	The PRESENT block cipher uses bit permutation for the linear diffusion layer. It also uses LFSRegister for the diffusion layer. However, the performance is somewhat similar to QK LW hash family and the same drawbacks persist
GL	The GL Hash family is based on FeCSRegister. Even if the software and hardware performances of GL are less than that of PH, they are comparable when considering parallel hardware versions of Quark.	The hardware size of such implementation is quite heavier than that of Quark and PH.
SPN	The internal permutation is implemented as substitution-permutation network (SPN). It uses AES- based internal permutations with fixed key size. SPN hash function uses MDS transform in its permutation layer	MDS transforms are powerful in diffusing data. But the main problem is that their lengths are fixed
LLW	This LW hash function uses AES-based block cipher with plaintext 256 and a 128 bit key size.	It uses mix column transformation. The main problem with the MDS matrix is that it is fixed.
LH	The design of LH uses a kind of Feistel-PG(FPG) structure in the internal permutation. F-PG has faster diffusion, comparatively shorter impossible differential paths and integral distinguishers.	It uses MDS transform. So only support fixed length block size.

4 Mersenne Number Transform (NMNT)

The most popular and important Number Theoretic Transform NTTs are the Fermat number transform (FeNT) and the Mersenne numbers transform (MeNT). The arithmetic operations used in calculating the FeNTs and MeNTs are simple and need only additions and multiplication.[10] [11].

4.1 The properties of NMNT

In order to design the lightweight(LW) security mechanism suitable for IoT, mainly consider the advantages of Mersenne prime numbers. This includes 1) any arithmetic modulo Mersenne number is hamming weight preserving. 2) And also we can calculate any number modulo Mersenne number operation within less time. 3) New Mersenne number transform support variable length block size. NMNT is defined as the operation modulo of the Mersenne numbers (MpN). New Mersenne number transform (NMNT) is more flexible than that of FeNT and MeNT technique. The Mathematical Formula of [NMNT] is in Equation 1. This formula X(k), is defined for an integer sequence x(n), with a length equal to N is given by as follows

$$X(k) = \langle \sum n \;\; x(n)\, \beta(nk) \rangle MpN \tag{1}$$

n = 0 to N-1

k = 0 to N-1

Where MpN is the Mersenne prime in the form of MpN=2p-1 (where p is prime numbers).

$$\beta(nk) = \beta_1(nk)+\beta_2(nk) \tag{2}$$

$$\beta_1(nk) = \langle \mathrm{Re}(\alpha_1+ j\alpha_2)^{nk} \rangle_{MpN} \tag{3}$$

$$\beta_2(nk) = \langle \mathrm{Im}(\alpha_1+ j\alpha_2)^{nk} \rangle_{MpN} \tag{4}$$

The value of β(nk) is in Equation 2. $\beta_1(nk)$ and $\beta_2(nk)$ are showed in Equation 3 and 4 respectively. Here Re(•) and Im(•) indicates real and imaginary parts. The values of β1 and are for transform length. The values of α1 and α2 can be obtained using Equation 5 and 6.

$$\alpha_{1=}\pm\langle 2^q \rangle_{MpN} \tag{5}$$

$$\alpha2=\pm\langle -3q \rangle MpN \tag{6}$$

where, $q=2^{p-2}$

The NMNT has the following advantages in addition to advantages of number transforms.

- Variable transform length (powers of two)
- Variable block size
- Fast algorithm to compute the transform
- Good diffusion

5 Conclusion

The LW hash families that we have seen so far do not support variable length block size and key size that are necessary requirements for IoT applications. This property is considered to be the factor for improving security. Hence, building a novel LW hash function which uses a new transformation function based on Mersenne numbers in permutation layer in order to improve the diffusion such that this transformation also support variable length block and key size in order to improve the security. This paper compared different LW hash functions with respect to IoT and introduced Mersenne Number Transform to achieve the requirements of IoT.

6 Acknowledgement

This work is partially supported by International Islamic University Malaysia, Research Initiative Grant Scheme no. RIGS17-023-0598. It was conducted at IoT & Wireless Communication Protocols Lab, ECE/KoE/IIUM.

7 References

[1] G. Sánchez-Arias, C. González García, and B. C. Pelayo G-Bustelo, “Midgar: Study of communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things,” Futur. Gener. Comput. Syst., 2017.

[2] B. Tareq Hammad, N. Jamil, M. Ezanee Rusli, and M. Z. Reza, “A survey of Lightweight Cryptographic Hash Function,” Int. J. Sci. Eng. Res., vol. 8, no. 7, 2017.

[3] W. Li, L. Liao, D. Gu, C. Ge, and Z. Gao, “Security Analysis of the PHOTON Lightweight Cryptosystem in the Wireless Body Area Network,” vol. 12, no. 1, pp. 476–496, 2018.

[4] Andreeva E. et al. (2015) "APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography". In: Cid C., Rechberger C. (eds) Fast Software Encryption. FSE 2014. Lecture Notes in Computer Science, vol 8540. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-46706-0_9

[5] Zhang W., Bao Z., Rijmen V., Liu M. (2015) "A New Classification of 4-bit Optimal S-boxes and Its Application to PRESENT, RECTANGLE and SPONGENT". In: Leander G. (eds) Fast Software Encryption. FSE 2015. Lecture Notes in Computer Science, vol 9054. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48116-5_24

[6] Canteaut, Anne & Roué, Joëlle. (2015). Differential Attacks Against SPN: A Thorough Analysis. 9084. 45-62. 10.1007/978-3-319-18681-8_4. https://doi.org/10.1007/978-3-319-18681-8_4

[7] B. Collard and F. X. Standaert, "A statistical saturation attack against the block cipher present," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5473, pp. 195–210, 2009. https://doi.org/10.1007/978-3-642-00862-7_13

[8] A. Akhimullah and S. Hirose, "Lightweight hashing using lesamnta-lw compression function mode and MDP domain extension," Proc. - 2016 4th Int. Symp. Comput. Networking, CANDAR 2016, pp. 590–596, 2017.

[9] W. Wu, S. Wu, L. Zhang, J. Zou, and L. Dong, "LHash: A lightweight hash function," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8567, pp. 291–308, 2014.

[10] G. Li, L. Lei, and W. Zhou, "Radix-8 algorithm for the new Mersenne number transform," 2013 Int. Conf. Commun. Circuits Syst. ICCCAS 2013, vol. 2, no. 12, pp. 143–146, 2013.

[11] N. Rutter, S. Boussakta, and A. Bystrov, "Assessment of the one-dimensional generalized new mersenne number transform for security systems," IEEE Veh. Technol. Conf., 2013. https://doi.org/10.1109/VTCSpring.2013.6692461

8 Authors

Nubila Nabeel is pursuing her Ph.D. at the department o electrical and computer engineering, International Islamic University Malaysia. Her research interests are in Internet o Things, security, Artificial intelligence, and blockchain technology.

Mohamed Hadi Habaebi is with the department of electrical and Computer Engineering, International Islamic University Malaysia. His research interests are in the Internet of Things, Security, wireless communications and Networking, Block chin technology and application of deep learning algorithms to image processing.

Nurul Arfah Che Mustapha received the B. Eng. Electronics-Computer and Information Engineering and M. Sc. (Electronics Engineering) from the International Islamic University Malaysia (IIUM), Malaysia in 2008 and 2011, respectively. She obtained her Ph.D. degree in Electronics Engineering from IIUM in 2017. She was a graduate research assistant from 2009-2016 and received IIUM Fellowship from 2011-2015 for her Ph.D. degree. Currently, Nurul Arfah works as an Asst. Prof. at the Electrical and Computer Engineering Department, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM). Her research interest is in CMOS, VLSI circuit design, Energy Harvesting, and Wireless Sensor Networks, and signal processing of capacitive sensor. Nurul Arfah is also a graduate member of the Institution of Engineers Malaysia since March 2018 and Member of Institute of Electrical and Electronic Engineers (IEEE), M'18, since early 2018.

Md Rafiqul Islam (M'02) received his Bachelor of Science in Electrical and Electronic Engineering from Bangladesh University of Engineering & Technology (BUET), Dhaka in 1987. He received his MSc and Ph.D. both in Electrical Engineering from the University of Technology Malaysia in 1996 and 2000 respectively. He is currently working as a professor in the Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University

Malaysia. He has supervised more than 50 Ph.D. and MSc students and has published more than 200 research papers in international journals and conferences. His areas of research interest are wireless channel modeling, radio link design, RF propagation measurement and modeling in tropical and desert, RF design, smart antennas, and array antennas design, FSO propagation and modeling etc. He is a Life Fellow of Institute of Engineers Bangladesh and member of IEEE and IET.

Article submitted 2019-01-22. Resubmitted 2019-03-03. Final acceptance 2019-03-04. Final version published as submitted by the authors.