Importance of Generic Construction of Block-Cipher Based Compression Function

[1] Rashed Mazumder, [2] Mohammad Shahriar Rahman, [1] Muhammad Shahin Uddin, [1] Mohammad Badrul Alam Miah
[1] Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Santosh, Tangail, 1902
Email: rakhu345@yahoo.com, shahin.mbstu@gmail.com, badrul_ict05@yahoo.com
[2] Department of Computer Science & Engineering, University of Liberal Arts Bangladesh, Dhaka-1209
Email: md.shahriarr@gmail.com

Abstract

A cryptographic hash function is an algorithm that receives input data in an arbitrary size and produces data in fixed size. In addition, this algorithm is infeasible to invert. There are many applications in the field of cryptographic hashing, including digital signatures, message authentication-code, password verification, and file identifier. In general, using a blockcipher-based compression function to build a cryptographic hash function is preferable than that of the scratch, because a blockcipher function is easier to implement than an encryption function. Typically, three variants of blockcipher are available under the double block-length (DBL), namely (n, n), (n, $2n$) and lightweight-cipher. Interestingly, many schemes have been proposed independently based on these blockcipher types. However, there is a lack of suitable scheme that can support all blockcipher types under a unique platform. Therefore, we addrees that a generalized blockcipher based compression function is important under the different kinds of communication platform.

Keywords— Blockcipher, Lightweight-cipher, Ideal Cipher Model, Collision resistance

Manuscript received on (date will be inserted) and accepted for publication on (date will be inserted).

1 INTRODUCTION

A cryptographic hash (CH) function is defined as a one-way function, i.e. it is infeasible to invert [1], [2]. The CH is one of the prominent tools in modern cryptography [1], [2]. Usually, a message and a chaining value are defined as the input of a CH [1]–[3]. In addition, the output of a CH is called a message-digest [2], [3]–[5]. A CH has many applications in the field of information security, including digital signatures, message authentication codes, password verification, and file/data identifier [1]–[2], [3]-[5], [6]-[7]. It is also used as ordinary hash functions for indexing data in hash tables [1], [3]–[5]. In certain cases, a CH is used for storing the encryption value of fingerprints, identifying duplicate data, and detecting accidental data corruption [1] – [3], [6], [7].

Ingeneral, a CH is built by a compression function [6], [8], [9]. Furthermore, the compression function has two prototypes, namely scratch and blockcipher (Fig. 1) [2]–[6]. Using a blockcipher-based compression function to build a cryptographic hash function is preferable to building one from scratch, because the blockcipher function can be directly implement as the encryption function [3], [6], [9]. According to internal construction, the blockcipher-based compression function has two types such as single block-length (SBL) and doubleblock-length (DBL) [8]–[10], [11], [12], [13]. However, because of birthday attacks, SBL is no longer secure [13]-[14]. According to Stam's conjecture [8], the DBL compression function comes under various pretexts. In principle, the DBL has three variants: (n, n), (n, 2n) and lightweight-cipher [14]-[15]. In the (n, n) blockcipher, the block-length and key-length are equal. Under the (n, 2n) blockcipher, the key-length is twice the block-length. Generally, AES and DES are used under the (n, n) and (n, 2n) blockciphers. Moreover, the latter is a lightweight-cipher based compression function. In addition, the lightweight-cipher based compression function depends on size and characteristics of lightweight ciphers such as Present, KATAN, TWINE, and Lblock [16]-[18].

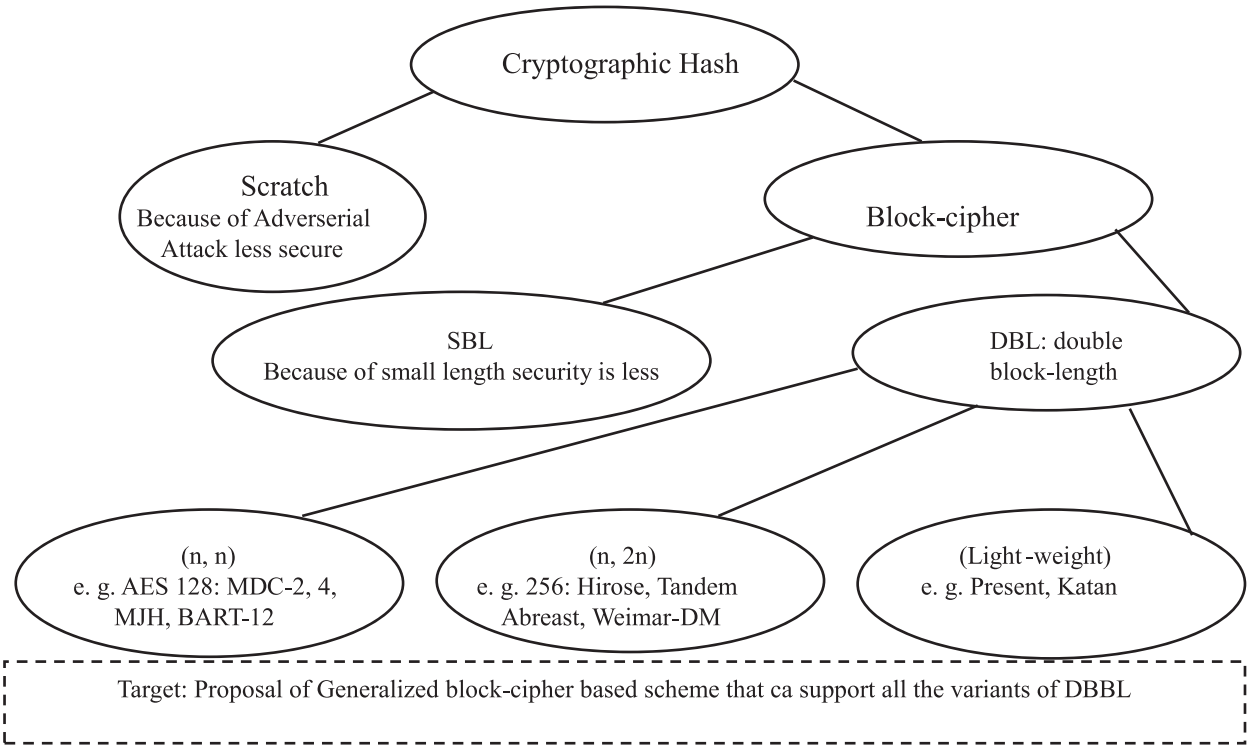

Figure 1: Basic of Cryptographic hash and Motivation [6], [8], [10], [11]-[12]

Motivations. Currently, many DBL-based schemes are available. The schemes of Weimar, MR, Hirose, Tandem, Abreast, Nandi, ISA-09, and CA are related to the (n, 2n) blockcipher [6]-[12]. The MDC-2, MDC-4, MJH, BART, MSR, and CIDM schemes are associated with the (n, n) blockcipher [19]-[21]. Furthermore, SH-L1 [16] and SH-L2 [17] schemes satisfy the lightweight-cipher based compression function. Interestingly, there is a lack of a construction that can support all the variants of DBL through a single platform.

TABLE 1
CURRENT STATUS OF DBL BLOCKCIPHER BASED COMPRESSION FUNCTION AND OUR CONCEPT

	Scheme Name	Security in CR	Efficiency	#E
(n, 2n) block-cipher based compression function	MR	$O(2^n)$	½	2
	Weimar	$O(2^n)$	½	2
	Hirose	$O(2^n)$	½	2
	Tandem	$O(2^n)$	½	2
	Abreast	$O(2^n)$	½	2
	ISA-09	$O(2^n)$	2/3	3
	Nandi	$O(2^n)$	$2/3$	3
(n, n) block-cipher based compression function	MDC-2	$O(2^{n/2})$	½	2
	MDC-4	$O(2^{5n/8})$	¼	4
	MJH	$O(2^{n/2})$	1	1
	BART	$O(2^{2n})$	$1/3$	3
	MSR	$O(2^{tn})$	t	2
	SKS	$O(2^{tn})$, $O(2^{tn/2})$	t, t/3	2, 3
Light-weight cipher based compression function	SH-L1	$O(2^n)$	½	2
	SH-L2	$O(2^n)$	½	2

In addition, current communication networks are very complex [1], [26]–[29]. In communication channels, one of the most prominent areas is the Internet of Things (IoT) [26]–[29]. IoT networks are undergoing a rapid rate of growth. There are various types of devices connected to IoT networks, grid networks, and cloud networks [1]–[3], [26]–[30]. These devices have different properties to consider, such as resource-limitations, keyfactors, power-factors, memory-factors, and operational cost factors [18]-[19], [20]-[27]. Under these circumstances, these devices should satisfy better security and efficiency. As a security tool, cryptographic hashing blockcipher compression function plays an important role. However, there is no common platform based solution for implementing a blockcipher-based compression function (Fig. 1, Table 1). More specifically, there is a lack of a generalized construction for blockcipher (DBL) based compression function.

Related Work. Actually, the MR, Weimar, Hirose, Tandem, Abreast, Nandi, ISA-09, and CA-16 schemes are related to the (n, 2n) blockcipher-based compression function (Fig. 2) [6], [14]–[19], [22]. Furthermore, MR, Weimar, Hirose, Tandem, and Abreast provide an upper security bound [6], [14]-[19]. In addition, the Nandi and ISA-09 satisfy better e ciency [6], [14]-[19]. Interestingly, the CA scheme [7] is suitable for both higher e ciency and satisfactory security bounds. However, owing to their designs, the above constructions are not suitable for (n, n) and lightweight-cipher blockcipher based compression function. On the contrary, the MDC-2, MDC-4, MJH, MSR, BART, CIDM, and SKS constructions support (n, n) blockcipher based compression functions [19]-[23]. Although, these schemes have satisfactory security margin and upper e ciency, these schemes are not appropriate for (n, 2n) blockcipher based compression function. Moreover, these schemes cannot support lightweight-cipher because of their internal construction. Most recently, two more schemes have been proposed by Hirose and Kuwakado such as SH-L1 [16] and SH-L2 [17]. These two constructions are suitable for lightweight-cipher based compression functions.

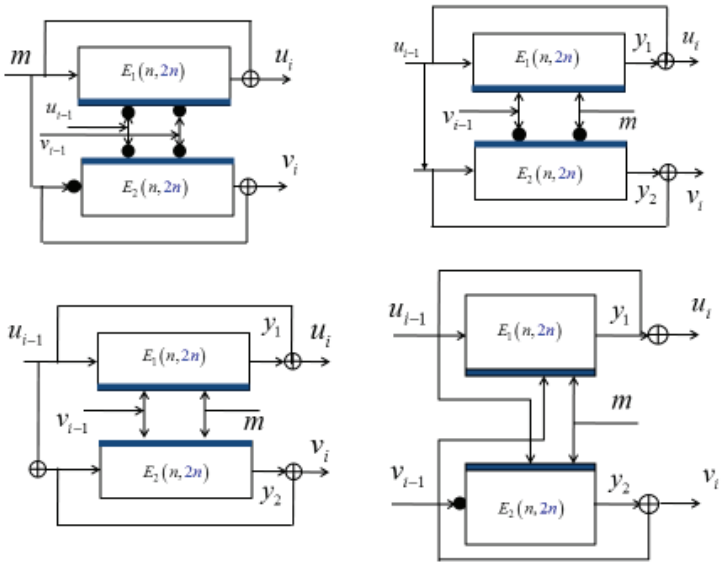

Figure 2: Certain well-known schemes of blockcipher compession function under (n, 2n) [11], [12], [13], [14], [20]

Our Contributions. In this paper, we address the issue of generalization of the DBL-based blockcipher compression function. Usually, a blockcipher-based compression function is an important tool for creating cryptographic hashes. However, there are several blockcipher variants such as (n, n), (n, 2n) and lightweight-cipher under the DBL. Hence, the compression function also varies based on the properties of the blockcipher. Interestingly, there is a lack of a common scheme of compression function that can support all blockcipher variants of the DBL. Therefore, we address that there is a need of generalized constructions of blockcipher based compression function. In addition, we propose a concept or idea of constructing a generic blockcipher based compression function.

2 Notations and Preliminaries

We define certain notations such as H, f_E. For example, H is defined as hash function. In addition, f_E is noted as compression function.

Ideal Cipher Model (ICM). A blockcipher obtains two paired algorithms, the first provides encryption (E) and the second handles decryption (D) [12]-[13]. Both algorithms can accept two inputs such as block size 'n', key size 'k' and return n-bit output. Typically, D is called as inverse of E (E=D^{-1}). Mathematically, the encryption and decryption algorithms are defined as $E(K, P) = C$; $D = E^{-1}(K, C) = P$ (Fig. 4), where P and C stands for plaintext and ciphertext. For example, a blockcipher encryption algorithm can receive 128 bits of plaintext as input and get back 128-bits of ciphertext. The transformation is controlled by the second input secret key. Decryption operates similarly do encryption but inreverse. For each key K, E^K is a permutation over the set of input blocks. Each key selects one permutation from the possible set of 2^n. In the ideal cipher model, the complexity of an attack is measured by adversary's total number of optimal queries to oracle E/E^{-1} [12], [13], [14]. The concept is depicted in Fig. 3.

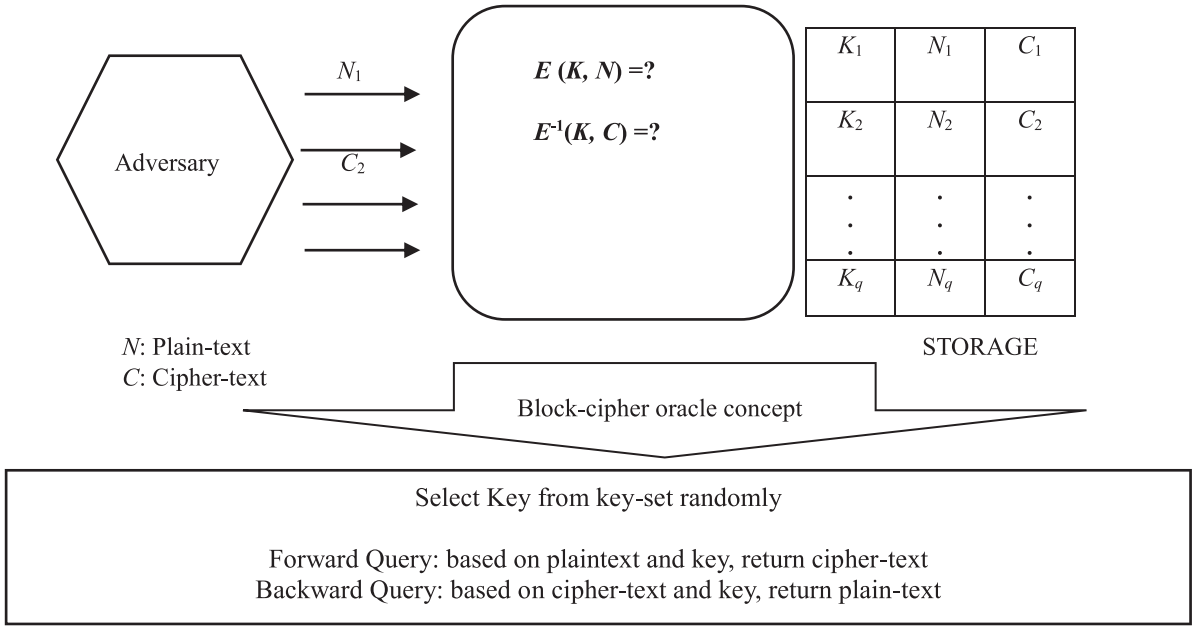

Figure 3: Concept of ICM and Query Method [6], [8]-[11]

Security Definition . An adversary, A is computationally unbounded -but always halts when a collision has occurred. Generally, A has access to an oracle E Block (K, N) for performing query through E and $D = E^{-1}$. This ensures that there is no chance of executing of duplicate query.

Collision resistance for hash function. Adversary A has access to blockcipher oracle. Let H is a hash function that is blockcipher-based. Adversary A has the advantage of finding a collision through Hash function (H), which is defined as Fig. 4.

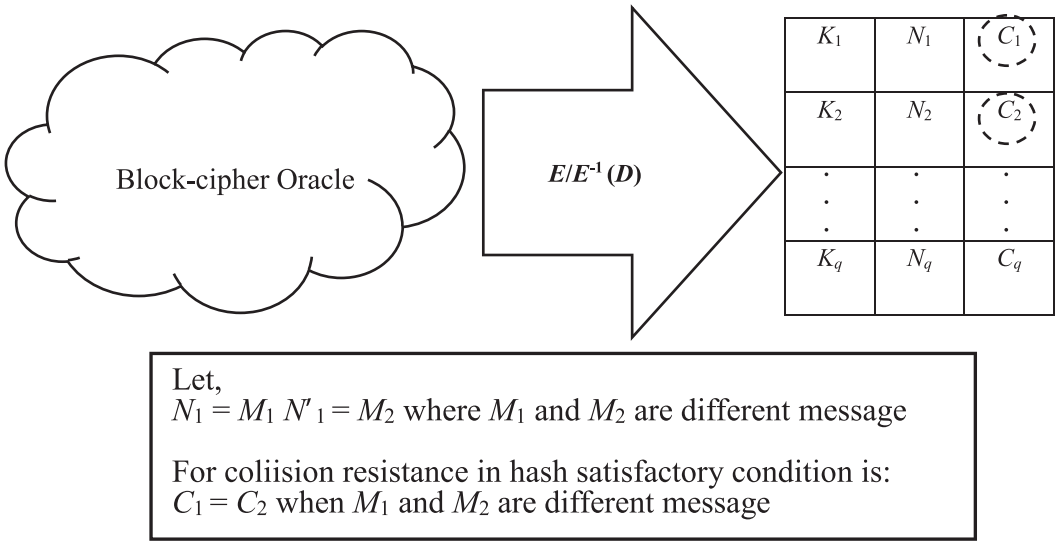

Figure 4: Concept of Collision Resistance [6], [8], [10]-[12]

3 Concepts of Design

Our concept of design is to satisfy the generic construction of blockcipher based compression function. The main principle is supporting of variable size of key. Generaly, the key size is fixed under the (n, n), (n, 2n), and lightweight-cipher based blockcipher ompression function. Hence, the construction principle is static. Under this circumstances, the construction principle should be dynamic. However, we mention an idea for creating this kind of construction by black-box model. Under this blac-box model, it can take two (02) input of message and key. Finally, in every iteration it produces two (02) chaining output values.

Our black-box is defined as ***B*** (Fig. 5), where we use input of x_1 and x_2. In addition, the output are o_1 and o_2. The condition is $x_1 + x_2 > o_1 + o_2$, where the size of key (k) is variable but less than message (m) size ($k < m$).

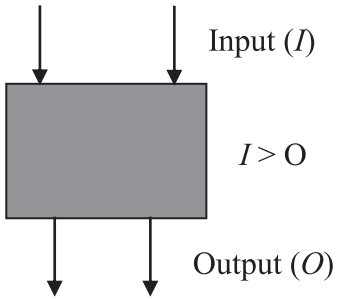

Figure 5: Concepts of design using black-box

4 Conclusion

In this paper, we describe using a blockcipher-based compression function as a cryptographic hash tool. The DBL blockcipher has three variants: (n, n), (n, 2n) and lightweight-cipher. There are certain schemes based on these three variants including, MR, Weimar, Tandem, Abreast, Nandi, ISA-09, MDC-2, MDC-4, MJH, Bart, MSR, SKS, SH-L1, and Sh-L2. However, there is a lack of a construction that can support the three variants listed above. In addition, generally, the communication networks are very complex and it depends on various types of devices. Furthermore, numerous devices are worked under IoT, cloud networks, and grid networks. These devices also have different properties such as resource-limitation, lightweightproperty, processing power and resource-adequate. Therefore, security solution schemes for these devices should be platform independent and generalized. Under these circumstances, we address the cracking issue of generalized construction of blockcipher based compession function. In future, we propose a specific design of blockcipher based compression function that will supports the characteristic of generalization.

References

[1] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin , "Hash Functions and RFID Tags: Mind the Gap," LNCS, CHES, vol. 5154, pp. 283-299, 2008.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, 5th edition, CRC Press, 2001.

[3] J. P. Kaps, B. Sunar, "Energy Comparison of AES and SHA-1 for Ubiquitous Computing," LNCS, Emerging Directions in Embedded and Ubiquitous Computing, vol. 4097, pp. 372-381, 2006.

[4] X. Wang, X. Lai, D. Feng, H. Chen, X. Yu, "Cryptanalysis of the Hash Functions MD4 and RIPEMD," LNCS, EUROCRYPT, vol. 3494, pp. 1-18, 2005.

[5] J. A. Black, P. Rogaway, T. Shrimpton, "Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV,"LNCS, CRYPTO, vol. 2442, pp. 320-335, 2002.

[6] E. Fleischmann, C. Forler, S. Lucks, J. Wenzel, "Weimar-DM: A Highly Secure Double-Length Compression Function," LNCS, ACISP, vol. 7372, pp. 152-165, 2012.

[7] O. Ozen, M. Stam, "Another Glance at Double-Length Hashing," LNCS, Cryptography and Coding, vol. 5291, pp. 176-201, 2009.

[8] F. Armknecht, E. Fleischmann, M. Krause, J. Lee, M. Stam, J. Steinberger, "The Preimage Security of Double-Block-Length Compression Functions," LNCS, ASIACRYPT, vol. 7073, pp. 233-251, 2011.

[9] M. Nandi, W. Lee, K. Sakurai, S. Lee, "Security Analysis of a 2/3 Rate Double Length Compression Function in the Black-Box Model," LNCS, FSE, vol. 3557, pp. 243-254, 2005.

[10] J. Lee, S. Hong, J. Sung, H. Park, "A New Double-Block-Length Hash Function Using Feistel Structure," LNCS, ISA, vol. 5576, pp. 11-20, 2009.

[11] J. Lee, D. Kwon, "The Security of Abreast-DM in the Ideal Cipher Model," IEICE Transactions, vol. 94-A (1), pp. 104-109, 2011.

[12] J. Lee, M. Stam, J. Steinberger, "The Collision Security of Tandem-DM in the Ideal Cipher Model," LNCS, CRYPTO, vol. 6841, pp. 561577, 2011.

[13] S. Hirose, "Some Plausible Constructions of Double-Block-Length Hash Functions," LNCS, FSE, vol. 4047, pp. 210-225, 2006.

[14] S. Hirose, H. Kuwakado., "Collision Resistance of Hash Functions in a Weak Ideal Cipher Model," IEICE Transactions, vol. 95 A (1), pp. 251-255, 2012.

[15] J. Lee, M. Stam, "MJH: A Faster Alternative to MDC-2," LNCS, CTRSA, vol. 6558, pp. 213-236, 2011.

[16] H. Kuwakado, S. Hirose, "Hashing Mode Using a Lightweight blockcipher," LNCS, Cryptography and Coding, vol. 8308, pages 213-231, 2012.

[17] H. Kuwakado, S. Hirose, "A Block-Cipher-Based Hash Function Using an MMO-Type Double-Block Compression Function, "LNCS, Provsec, vol. 8782, pages 71-86, 2014.
[18] A. Miyaji, M. Rashed, S. Tsuyoshi "A new (n, n) Blockcipher based Hash Function for Short Messages," IEEE, ASIAJCIS, 978-1-47995733, pp. 56-63, 2014.
[19] E. Fleischmann, C. Forler, and S. Lucks "The Collision Security of MDC-4, LNCS, Africacrypt, vol. 7374, pp. 252-269, 2012.
[20] J. Lee, M. Stam, "MJH: A Faster Alternative to MDC-2," CT-RSA, vol. 6558, 213-236, 2011.
[21] J. Coron, Y. Dodis, C. Malinaud, P. Puniya, "Merkle-Damgard Revisited: How to Construct a Hash Function," LNCS, CRYPTO, vol. 3621, pp. 430-448, 2005.
[22] A. Joux, "Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions," LNCS, CRYPTO, vol. 3152, pp. 306-316, 2004.
[23] P. Gauravaram, J. Kelsey, "Linear-XOR and Additive Checksums Protect Damgrd-Merkle Hashes from Generic Attacks," LNCS, CT-RSA, vol. 4964, pp. 36-51, 2008.
[24] X. Lai, X. Massey, L. J., "Hash function based on block ciphers," LNCS, EUROCRYPT, vol. 658, pp. 55-70, 1993.
[25] B. Mennink, "Optimal Collision Security in Double Block Length Hashing with Single Length Key," LNCS, ASIACRYPT, vol .7658, pp. 526-543, 2012.
[26] L. Barreto, A. Celesti, M. Villari, M. Fazio, A. Puliato, "An Authentication Model for IoT Clouds", IEEE, ASONAM, pp. 1032 -1035, 2015.
[27] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, A. Iera, "A systemic and cognitive approach for IoT security", IEEE explore, ICNC, pp. 183-188, 2014.
[28] J. Y. Lee, Y. H. Huang, "A lightweight authentication protocol for Internet of Things", IEEE explore, ISNE, pp. 1-2, 2014.
[29] H. Yoshida "On the standardization of cryptographic application techniques for IoT devices in ITU techniques for IoT devices in ITU-T and ISO/IEC JTC 1 T and ISO/IEC JTC1, https://www.ietf.org/proceedings/94/slides/slides-94-saag-2.pdf,2015
[30] G. S. Matharu, P. Upadhyay, "The Internet of Things: Challenges and security issues," IEEE ex., ICET, 978-1-4799-6088-0, pp. 54-59, 2014.

Rashed Mazumder He received his Bachelor's degree from University of Dhaka, Bangladesh in the field of Computer Science and Engineering. In 2010, he joined as a faculty of Mawlana Bhashani Science and Technology University (MBSTU), Bangladesh. He completed a Master's degree from the University of Japan Advanced Institute of Science and Technology (JAIST), Japan in 2014. After successful completion of master degree he finished his Ph.D degree under the school of Information Science of JAIST. Now he is serving as an Assistant Professor at the department of Information and Communication Technology (ICT) in MBSTU, Bangladesh.

Mohammad Shahriar Rahman He is currently an associate professor at the University of Liberl Arts Bangladesh. Earlier, he worked as associate professor at University of Asia Pacific, Bangladesh, and senior researcher at the Information Security group of KDDI Research, Japan. He received his Ph.D. and M.S. degrees in information science from Japan Advanced Institute of Science and Technology (JAIST), in 2012 and 2009 respectively, and B.Sc. in computer science and engineering from University of Dhaka, Bangladesh, in 2006. His research interests include secure protocol construction, privacy-preserving computation and security modeling. He is a member of International Association for Cryptologic Research (IACR).

Muhammad Shahin Uddin He received his B.Sc. Engineering degree in Electrical and Electronic Engineering from Rajshahi University of Engineering and Technology (RUET), Bangladesh and M.Sc. Engineering degrees in Electronics Engineering from Kookmin University, South Korea. He received the doctoral degree from the University of New South Wales, Australia. He worked for American International University Bangladesh (AIUB) and, Chittagong University of Engineering & Technology (CUET), Bangladesh. Since 2006, he has been with the department of Information and Communication Technology, Mawlana Bhashani Science and Technology University (MBSTU). He received the University Gold Medal from Rajshahi University of Engineering and Technology (RUET), Bangladesh. His research interests include, Visible Light Communication (VLC), LED-ID system, optical fiber, Bio-photonics and digital image processing.

Mohammad Badrul Alam Miah He received his BSc (Engg.) in Information and Communication Technology under the department of Information and Communication Technology (ICT) of Mawlana Bhashani Science and Technology University (MBSTU). He received the Masters degree from the University of MBSTU, Tangail, Bangladesh. He is now serving as an Associate Professor in the department of ICT. His research interests are Neural Network, Digital Image Processing, Data Mining, Network security, Computer Vision.