Survey on Lightweight Block Cipher

Swarnendu Jana, Jaydeb Bhaumik, Manas Kumar Maiti

Abstract— With the rapid advances in wireless networks low-end devices, such as RFID tags, wireless sensor nodes are deployed in increasing numbers each and every day. Such devices are used in many applications and environments, leading to an ever increasing need to provide security. When choosing security algorithms for resource-limited devices the implementation cost should be taken into account, In order to satisfy these need, secure and efficient encryption and authentication schemes have to be developed. Symmetric-key algorithms, especially lightweight block ciphers, still play an important role to provide confidentiality in the said applications. In this paper, a survey of several existing light weight block ciphers has been provided.

Index Terms—Symmetric Key Cryptography, Lightweight Block Cipher.

I. INTRODUCTION

Advanced Encryption Standard (AES) is a popular block cipher which has already been analyzed widely for its Security. Till date, it is secure against various existing attacks except some attacks on physical implementation of AES in FPGA and smartcard. So ideally, the device vendors should have deployed AES in their devices. But the problem with AES is that it requires a significant amount of resource and power. Devices, such as RFIDs and sensor nodes contain sensitive and confidential information. But these miniature devices are resource constrained so it is not possible for them to run traditional cryptographic algorithms which require large memory and greater processing power than these miniaturized devices posses. Also AES provides more security than what is needed to such resource constraint applications. Therefore, AES is often inappropriate for such devices due to their size/power/memory constraints, even though there are constant efforts for designing small-footprint of AES. Hence the need was felt to design primitives to suit the resource constraints of small devices and at the same time these primitives should provide adequate security to the user. These are the scaled down version of traditional cryptographic primitives.

To fill the gap, a number of lightweight block ciphers have been proposed; for instance, TEA [15], XTEA [11], DESL [1], HIGHT [2], mCrypton [7], PRESENT [8], KATAN/KTANTAN [3], PRINCE [9] , TWINE [10], and many more. Lightweight block cipher TEA introduced by Needham and Wheeler in 1994, which is easy to implement. By exploiting its too simple key schedule, Kelsey et al. proposed a related-key attack on full round TEA [12]. In order to resist the attack, the authors enhanced the cipher with an improved key schedule and a different round function by rearranging the operations; the new version is called XTEA.

It uses modular addition (modulo 2^{32}), shift (left and right) and XOR in their round functions. Recently two attacks on XTEA namely impossible differential cryptanalysis and related key differential attacks have been mentioned in [13] [14]. Another lightweight block cipher HIGHT [2] is proposed by D. Hong et al. in 2006 for ultra-light weight implementation. For resource-constrained tiny devices, cipher mCrypton is introduced in [7]. Its designed architecture like as Crypton but some simplification on component functions has been introduced to enable much compact implementation in both hardware and software under restricted environments. Lightweight variants of the DES cipher called DESL and DESXL [1] which is strong, compact and efficient for implementation. Due to its low area overhead, DESL is especially suited for tiny devices; it uses a single S-box repeated for eight times. Andrey Bogdanov et al. proposed a new family of ultra- lightweight block ciphers called PRESENT. It offers a level of security and the hardware requirements which is comparable with today's leading compact stream ciphers. KTANTAN & KATAN are a family of block cipher composed of two sets having block sizes 32, 48, or 64-bit and key size 80-bit. KLEIN [4] is another lightweight block cipher which mainly focuses on software implementation; it also enjoys hardware efficiency resulting from its simple structure with an involutive S-box. The various key lengths of KLEIN offer flexibility and a moderate security level for ubiquitous applications. LED [5] mainly focuses on key schedule algorithm and protection against related-key attacks. The LED block cipher is simple to analyze and this allows us to precisely evaluate the necessary number of rounds to ensure proper security. LBlock [6] achieves good hardware performance and software efficiency on 8-bit microcontroller. It employs a variant of Feistel structure and the encryption algorithm is 4-bit oriented which can be implemented efficiently in both hardware and software. LBlock can achieve enough security margins against known attacks, such as differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis and related-key attacks etc. Cipher PRINCE [9] uses the same optimal S-box for 16 times to get the lowest possible gate count without compromising security.

In this paper, a survey on existing light weight block ciphers has been provided. Also a comparison between existing light weight block ciphers has been given. The remainder of this paper is organized as follows. Section 2 describes the design principle, security and application of popular light weight block ciphers. A comparison is provided in Section 3 and finally the paper is concluded in Section 4.

Manuscript Received November, 2013.

Swarnendu Jana, Department of Computer Science & Application, Vidyasagar University, Midnapore (Paschim Midnapore), India.

Jaydeb Bhaumik, Electronic and communication Engineering, Haldia Institute of technology, Haldia (Purba Midnapore), India.

Manas Kumar Maiti, Mahishadal Raj College, Mahishadal (East Midnapore) , India.

II. BASICS OF EXISTING LIGHTWEIGHT BLOCK CIPHERS

In this section, design principle, strength against existing attack and applications of DESL/DESXL, HIGHT, PRESENT, and ATAN/KTANTAN,KLEIN,LED,PRINCE, TWINE,TEX/XTEA have been discussed

A. DESL and DESXL

DESL & DESXL are new lightweight variants of DES using serial hardware architecture and replace the 8 original S-Boxes by a one S-Box for reducing the gate complexity. The S-box has been highly optimized in such a way that DESL resists common attacks, i.e. linear and differential cryptanalysis, and the Davies-Murphy-attack. Therefore DESL achieves a security level, which is appropriate for many applications. Additionally the initial permutation (IP) and its inverse (IP^{-1}) are omitted, because they do not provide additional cryptographic strength. The main goal of the developer was to reduce gate count in hardware implementations as compared to the original DES. DESL shows that differential cryptanalysis is not feasible anymore. It is more resistant against linear cryptanalysis than DES due to the improved non-linearity of the S-box. It is more secure, size-optimized, and power efficient than DES for this reason it is to be considered as an alternative for stream ciphers. For higher security, key whitening technique $DESX_{k.k1.k2}(x) = k2 \oplus DES_k(k1 \oplus x)$ is used. The 64 most significant bits and the 64 least significant bits are used for key whitening in order to prevent brute-force attack requires 2^{56} plaintexts. DESL is more resistant against linear cryptanalysis requires about 2^{43} chosen ciphertext. Ciphers are more resistant against linear cryptanalysis than DES due to the improved non-linearity of the S-box. DESL is secure, size-optimized, and power efficient for this reason DESL is to be considered as an alternative for stream ciphers.

B. HIGHT

HIGHT has a generalized Feistel-like structure which reduces the cost of implementation and the round function is light compared to substitution permutation-like structure. Every operation in HIGHT is 8-bit-processor-oriented. CPUs embedded into the sensors in USN (Ubiquitous Sensor Network) are based on 8-bit processor. So, HIGHT has efficient performance in such environment. In 8-bit-oriented software implementation HIGHT is faster than AES-128. It applies key-whitening technique in the first and the last rounds for avoiding direct retrieve from plaintexts and cipher texts. It is impossible to find differential characteristics of HIGHT for given 2^{64} possible input values. In differential attack on 13-round HIGHT without the final transformation recovers the subkeys of the 12th and 13th rounds required 2^{62} plaintexts. Truncated differential characteristic to recover 96 bits of the subkeys used from the 11th round to the 16th round in 16-round HIGHT with $2^{14:1}$plaintexts and $2^{108:69}$ encryptions. In linear attack on 13-round HIGHT without the final transformation recovers 36 bits of the subkeys of the 1st, 12th, and 13th rounds with 2^{57} plaintexts. In 14 rounds impossible differential characteristic to attack 18-round HIGHT requires $2^{46:8}$ chosen-plaintexts and $2^{109:2}$ encryptions .Also 16 round saturation attack requires 2^{42} plaintexts and 2^{51} encryptions of 16-round HIGHT. In 8-bit-oriented software implementation HIGHT is faster than AES-128. CPUs embedded into the sensors in USN (Ubiquitous Sensor Network) are based on 8-bit processor. So, HIGHT has efficient performance in such environment.

C. PRESENT

In PRESENT [8] at the beginning of each round, 64-bit input of the round function is XORed with the sub key. Just after the subkey XOR, 16 identical 4×4-bit S-boxes are used in parallel as a non-linear substitution layer and finally a permutation is performed to provide diffusion. The key will be fixed at the time of device manufacture. Efficient use of space, the block cipher will be implemented as encryption-only. The 2x1 64-bit multiplexer selects either the initial Plaintext/Ciphertext or the output of the previous round. The round subkeys are generated on-the-fly. The value of the 80-bit key register is left rotated by 61-bitpositions. Then, the four most significant bits (79 to 76) are passed through an S-box and finally the bits k_{19} k_{18} k_{17} k_{16} k_{15} of K are XORed with the least significant bits of round counter. Linear cryptanalyst need only approximate 28 of the 31 rounds in PRESENT [41] to mount a key recovery attack with 2^{84} known plaintext/ciphertexts. It is suitable for extremely resource constrained environments, it is important to recognize that it is not building a block cipher that is necessarily suitable for wide-spread use. It is targeting some very specific applications for which the AES is unsuitable. It can be used within challenge-response authentication protocols and, with some careful state management, it could be used for both encryption and decryption of communications to and from the device by using the counter mode.

D. KTANTAN and KATAN

In KTANTAN & KATAN the plaintext is loaded into two registers L_1 & L_2 and each round its value are shifted to left I,e bit i is shifted to position i+1.Where the new computed bits are loaded in the least significant bits of L_1 & $L_{2.}$ After 254 rounds of the cipher, the contents of the registers are then exported as the ciphertext where bit 0 of L_2 is the least significant of the ciphertext. After the computation of the nonlinear functions, the registers L_1 & L_2 shifted left , where MSB bit falls off and the LSB bit are loaded with the output of second nonlinear function It implements the 8-bit LFSR counter in place of 8-bit counter for expected speed. The KTANTAN family is very similar to the KATAN family up to the key schedule i.e., the only difference between KATANn and KTANTANn is the key schedule part. In the KATAN family, the 80-bit key is loaded into a register which is then repeatedly clocked where KTANTAN family the key is fixed thus, the design problem in the KTANTAN ciphers is choosing a sequence of subkeys in a secure, yet an efficient manner. In KTANTAN & KATAN no differential characteristic with probability greater than 2^{-n} exists for 128 rounds. Also no linear approximations with bias greater than $2^{-n/2}$ exists for 128 rounds that ensure no differential-linear attack and boomerang attack exist for the entire cipher. Related-key attack or slide attack with time complexity smaller than 2^{80} exists on the entire cipher. For algebraic degree for the equation describing half the cipher is sufficient to thwart any algebraic attack.

E. KLEIN

KLEIN is a typical Substitution-Permutation Network (SPN) type block cipher. Several lightweight block ciphers use counter mode to avoid implementation cost of decryption but KLEIN avoids this cost without fixing on any cipher mode. KLEIN can accept different key sizes where round counters can be defined by a recursion rule or an LFSR sequence in $GF(2^8)$ to avoid the potential complementation. In KLEIN related-key weakness can be avoid by its key schedule technique. Linear and differential attacks can be resisting by using active S-boxes in a certain number of rounds. The design provides a practical and secure cipher for low-resource applications, especially for RFIDs and wireless sensor networks. Although KLEIN mainly focuses on software implementations, it also enjoys hardware efficiency resulting from its simple structure with an involutive S-box. The various key lengths of KLEIN offer flexibility and a moderate security level for ubiquitous applications. Therefore, the design increases the available options for lightweight block ciphers in low-resource applications. It can be used to construct block-cipher-based hash functions and message authentication codes.

F. LED

LED is a 64-bit SPN type lightweight block cipher that can handle key sizes from 64 bits up to 128 bits. The keyed permutation present in LED is inspired from the Advanced Encryption Cipher (AES) structure. LED is capable of providing strong security arguments against all state of the art attacks, even in the related-key model. In case of differential and linear cryptanalysis, it can be shown that any 4-round differential path for any of the LED versions contains at least 25 active S-boxes which are having a non-zero difference in the single-key model. Even in the more pessimistic related-key model, any 16-round differential path for any of the LED versions contains at least 50 active S-boxes. It is very compact in hardware and ultra-light key scheduling maintains a reasonable performance profile for software implementation.

G. PRINCE

Substitution permutation network is preferable over a Feistel-cipher, since a Feistel-cipher operates only on half the state resulting often in a higher number of rounds In order to minimize the number of rounds and still achieve security against linear and differential attacks, adopted a lightweight cipher PRINCE [9]. All round functions have to be identical for a cipher aiming for a fully unrolled implementation as PRINCE; it is very tempting to directly use the concept of code-concatenation to achieve a high number of active S-boxes over 4 rounds of the cipher. However, not only a serial implementation benefits from similar round functions. It is also very helpful for ensuring a minimum number of active S-boxes. The cipher can perform instantaneous encryption; a ciphertext is computed within a single clock cycle. There is no warm-up phase. If implemented in modern chip technology, low delays resulting in moderately high clock rates can be achieved. The α-reflection property of the core cipher does not introduce any generic attack with complexity significantly lower than the known generic attacks against the FX construction. Security of PRINCE against linear, differential, algebraic and Biclique attacks have been evaluated recently.

H. TWINE

TWINE is a 64-bit block cipher having 80-bit or 128-bit key. It employs the type-2 Generalized Feistel Structure (GFS) with 16 4-bit sub-blocks. A round function of TWINE consists of a nonlinear layer using 4 bit S-boxes and a diffusion layer, which permutes the 16 blocks. The drawback of such design is poor diffusion property, leading to a slow cipher with quite many rounds. To overcome the problem, it employs the idea of Suzaki and Minematsu at FSE '10 [21] which substantially improve diffusion by using a different block shuffle from the original. Unlike type-2 GFS, the diffusion layer is not a circular shift and is designed to provide a better diffusion that the circular shift, according the result of [21]. The key schedule of TWINE inserts distinct constants for each round that prevent slide attacks. For Meet-In-The-Middle (MITM) attack, the round keys for the first 3 (5) rounds contain all key bits for the 80-bit (128-bit) key case. So, it is difficult to mount the basic MITM attack against the full round TWINE. The recently-proposed MITM variant, called Biclique attack [27], may work even when all key bits are used in the relatively small number of rounds.

I. TEA and XTEA

Lightweight block cipher TEA was introduced by Needham and Wheeler in 1994, which is easy to implement. By exploiting its too simple key schedule, Kelsey et al. proposed a related-key attack on full round TEA [12]. In order to improve the security of TEA against related-key attack, an improved version of TEA called XTEA was introduced. Like TEA, XTEA is a 64-bit block Feistel network with a 128-bit key and a suggested 64 rounds. Several differences from TEA are apparent, including a somewhat more complex key-schedule and a rearrangement of the shifts, XORs, and additions. The use of dynamic plaintext dependant key scheduling means that there is no preset order for the use of the scheduled keys, and that they require no memory. This is quite a useful property as detecting which scheduled keys were used is most likely a difficult task. The key schedule is most likely more resistant to differential analysis since the bits in the key can effect any 1/32 possible other bits. The use of non-linear algebra (mixing addition with binary XOR) is considered effective against linear analysis. There are no known weaknesses in the use of mixed algebraic operations. XTEA has potentials in low power wireless security applications. It is helpful to create mutual authentication and trust between two entities. The efficient application in wireless sensor network will be an interesting area to investigate.

III. PERFORMANCE ANALYSIS AND COMPARISONS

The main differences between the conventional block ciphers and the lightweight block ciphers are centered on: the block size which is in general 32, 48 or 64 bits for a lightweight block cipher and equal to 64 or 128 bits for a conventional block cipher;

the same condition also holds for the different possible key sizes. Lightweight block ciphers also rely more on elementary operations such as binary XOR, binary AND, etc. which are leading in an increase of required number of rounds; Lightweight block ciphers generally extremely simplify the key schedule due to memory requirements. A comparison of existing lightweight block ciphers are given in Table1.

IV. CONCLUSION

A survey of different lightweight block ciphers is given in this paper. Light weight block ciphers have smaller block size to save gates on internal flip-flop registers and use very few different sub- functions(e.g. 6-to-4 bit S-boxes). It must be possible to implement the cipher in a serialized fashion. This study can be the starting point to improve the lightweight block ciphers in many directions like number of clock cycle, size of memory, number of chosen plaintext, GE, throughput and attacks.

ACKNOWLEDGMENT

I would like to place on record my deep sense of gratitude to Assistant Prof. Jaydeb Bhaumik of Electronics and Communication Engineering, HIT (Haldia) for his generous guidance, help and useful suggestions. His assistance is very much beneficial for me to carry out the process of research in this field. Key improvements in the proposed research work would not be possible without the valuable suggestion and the feedback of my guide. I would also like to thanks Assistant Prof. Manas Kumar Maiti, for his generous guidance, suggestions. His guidance is very much beneficial for me to carry out the process of research in this field.

Table.1 shows comparison between existing block cipher

Cipher Name	Year of design	Block Size (Bits)	Key Size (Bits)	Cycles per block	Network Type	Area (GE)	Best Known attack
PRINCE [9]	2012	64	128	12	SPN	3779	Multi-linear attacks
KLEIN [4]	2011	64	64/80/96	12/16/20	SPN	1220/1478/1528	Biclique Cryptanalysis
TWINE [10]	2011	64	80/128	36	Feistel	1500	Biclique Cryptanalysis
LED [5]	2011	64	64/128	48	SPN	3194/3309	Meet-in-the-middle attack
KTANTAN & KATAN [3]	2009	32/48/64	80	254	LFSR	462/588/688	Differential attack
DESL/DESXL [1]	2007	64	56/184	16	Feistel	1848/2168	No attack has been exhibited
PRESENT [8]	2007	64	80/128	31	SPN	3105/3707	Biclique Cryptanalysis
HIGHT [2]	2006	64	128	32	Feistel	3048	Impossible Differential attack
XTEA [11]	1997	64	128	32	Feistel	2521	Meet-in-the-middle attack/ Impossible Differential attack

REFERENCES

1. G. Leander et al., "New Lightweight DES Variants," Proc. of Fast Software Encryption , LNCS, vol. 4593, Mar. 2007, pp. 196-210.
2. D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee," HIGHT: A New Block Cipher Suitable for Low-Resource Device, " Proc of Cryptographic Hardware and Embedded Systems, LNCS, vol. 4249, Oct. 2006,pp. 46-59.
3. C. Canniere, O. Dunkelman, and M. Knezevic , "Katan and ktantan - a family of small and effcient hardware-oriented block ciphers," Proc. of Cryptographic Hardware and Embedded Systems, LNCS, vol. 459, Sept. 2009,pp. 272-288.
4. Z. Gong, S. Nikova, and Y. W. Law, "KLEIN: A New Family of Lightweight Block Ciphers," Proc. of RFID. Security and Privacy, LNCS, vol. 6, Jun. 2011, pp. 1–18.
5. J. Guo, T.Peyrin, A.Poschmann, and M. Robshaw, "The led block cipher Cryptographic Hardware and Embedded Systems, LNCS, vol. 6917, Sept. 2011, pp. 326-341.
6. Y. Wang, W. Wu, X. Yu, and L. Zhang," Security on lblock against biclique cryptanalysis," Proc. of Information Security Applications, LNCS , vol. 7690, Aug. 2012, pp.1-14.
7. Chae Hoon Lim and Tymur Korkishko," mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors," Proc. of Information Security Applications, LNCS, vol. 3786, Aug. 2005,pp. 243-258.
8. A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," Proc. of Cryptographic Hardware and Embedded Systems, LNCS, vol. 4727, Sept. 2007,pp. 450-266.
9. J . Borgho,A. Canteaut T. uneysu, S.S. Thomsen and T. Yalcin, "Prince - a low-latency block cipher for pervasive computing applications - extended abstract," Proc. of Advances in Cryptology, LNCS, vol.7658, Dec. 2012,pp. 208-225.
10. T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, "TWINE: Lightweight Block Cipher for Multiple Platforms," Proc. of Selected Areas in Cryptography, LNCS , vol. 7707, Aug. 2013,pp. 339-354.
11. R. Needham, D. Wheeler, " eXtended Tiny Encryption Algorithm," Technical Report, Cambridge University, England, Oct. 1997.
12. D. Wheeler and R. Needham, " TEA, a Tiny Encryption Algorithm," Proc. of the Second International Workshop on Fast Software Encryption, 1995, pp. 97-110.
13. A. Juels, "RFID Security and Privacy ," IEEE Journal on Selected Areas in Communications, vol. 24, 2006, pp.381-394.
14. K. Kim, K. Chung, J. Shin, H. Kang, S. Oh, C. Han, and K. Ahn, "A Lightweight RFID Authentication Protocol using Step by Step Symmetric Key Change," Proc. of 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009
15. S. Ojha,N. Kumar,K. Jain and S.Lal, "TWIS - A Lightweight Block Cipher," Information Systems Security, LNCS, vol. 5905, Dec. 2009, pp. 280-291.
16. A. Arora, and S. Pal," A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers," Proc. of International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 2, Apr. 2012.
17. T. Suzaki and K. Minematsu, "Improving the Generalized Feistel," Proc. of Fast Software Encryption, LNCS, vol. 6147, Feb. 2010, pp. 19-39.
18. A. Poschmann. "Lightweight Cryptography - Cryptographic Engineering for a Pervasive World," Cryptology ePrint Archive, Report 2009/516, 2009.
19. O. Ozen, K. Varici, C. Tezcan and C. Kocair, "Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT," Proc. Of Information Security and Privacy, LNCS, vol. 5594, July 2009, pp. 90-107.
20. K. Minematsu, T. Suzaki, and M. Shigeri, "On Maximum Differential Probability of Generalized Feistel," Proc. Of Information Security and Privacy, LNCS, vol. 6812, July. 2011, pp. 89-105.
21. M. Izadi, B. Sadeghiyan, S. S. Sadeghian, and H. A. Khanooki, "MIBS: A New Lightweight Block Cipher," Proc. of Cryptology and Network Security, LNCS, vol. 5888, Dec. 2009, pp. 334-348.
22. A. Bogdanov, D. Khovratovich and C. Rechberger, "Biclique Cryptanalysis of the Full AES," Advances in Cryptology – ASIACRYPT, LNCS, vol. 7073, Dec. 2011, pp. 344-371.
23. A. Biryukov, "DES-X (or DESX). In Encyclopedia of Cryptography and Security (2nd Ed.)," 2011, pp. 331.
24. H.Yue-chao and W.Yi-ming, "Secure RFID system based on lightweight block cipher algorithm of optimized S-box," Proc. of IEEE International Conference, June 2010,pp. 17-19.
25. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, " The 128-bit blockcipher clefia (extended abstract)," Proc. of Fast Software Encryption , LNCS, vol.4593, Feb.2007,pp. 181-195.

26. C. Rebeiro, R. Poddar, A. Datta, and D. Mukhopadhyay, "An Enhanced Differential Cache Attack on CLEFIA for Large Cache Lines," Proc. of Indocrypt, vol. 7107, 2011, pp. 55-75.
27. S. Khurana, S. Kolay, C. Rebeiro and D. Mukhopadhyay, ”Lightweight Cipher Implementations on Embedded Processors”’, Proc. of DTIS , Mar.2013.
28. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, “A Survey of Lightweight-Cryptography Implementations,” IEEE Design & Test, vol. 24, Dec. 2007,pp. 522–533.
29. T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi. TWINE: A Lightweight, Versatile Block Cipher. Available: www.nec.co.jp/rd/media/code/research/images/twine_LC11.pdf.
30. G. Gaubatz , "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proc. of 3rd IEEE Int'l Conf. Pervasive Computing and Communications (PERCOMW 05), pp. 146-150, 2005.
31. M. Wang, “Differential cryptanalysis of reduced-round PRESENT,” Proc. of Progress in Cryptology AFRICACRYPT, vol. 5023, Jun. 2008, pp. 40–49.
32. J.Y.Cho, “Linear cryptanalysis of reduced-round PRESENT,” Proc. of Topics in Cryptology, LNCS, vol. 5985 Mar. 2010,pp.302-317.
33. Rajashekarappa, K M Sunjiv Soyjaudah and Sumithra Devi K A, “Study on Cryptanalysis of the Tiny Encryption Algorithm,” International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, vol. 2, Feb. 2013

AUTHOR PROFILE

Swarnendu Jana is a M.Sc Pass out student in the Department of Computer Science and Application, Vidyasagar University, Midnapore, Paschim Medinipur, India. He received his B.Sc. degree in Computer Science from Midnapore College under Vidyasagar University in the year 2006. His research interests include Symmetric Key Cryptography.

Jaydeb Bhaumik is currently working as an Associate Professor in the Department of Electronics and Communication Engineering, Haldia Institute of Technology, Haldia, India. He obtained his PhD degree from G. S. Sanyal School of Telecommunications, Indian Institute of Technology Kharagpur, India in 2010. He received his B. Tech. and M.Tech. degrees in Radio Physics and Electronics from University of Calcutta in 1999 and 2001 respectively. His research interests include Cryptography, Cellular Automata, Error Correcting Codes, and Digital VLSI Design. He is a member of IEEE and Cryptology Research Society of India.

Manas Kumar Maiti is currently working as an Assistant Professor in the Department of Mathematics, Mahishadal Raj College, and Mahishadal India. He obtained his PhD degree from Vidyasagar University, India. His research interests include fuzzy logic, fuzzy set, crisp set and cryptography and network security. He is a member of some Research Society of India.