Research Problems in Block Cipher Cryptanalysis: An Experimental Analysis

Amandeep, G. Geetha

Abstract*: Cryptography has always been a very concerning issue in research related to digital security. The dynamic need of applications and keeping online transactions secure have been giving pathways to the need of developing different cryptographic strategies. Though a number of cryptographic algorithms have been introduced till now, but each of these algorithms has its own disadvantages or weaknesses which are identified by the process of cryptanalysis. This paper presents a survey of different block ciphers and the results of attempts to identify their weakness. Depending upon the literature review, some open research problems are being presented which the cryptologists can depend on to work for bettering cyber security.

***Index Terms*: block ciphers, cryptanalysis, attacks, SPN, Feistel.**

I. INTRODUCTION

Cryptography is the science which deals with confidentiality, authenticity, and integrity of the data, which lead to ensure that the data stay secure during communication. Living in an age that has taken to digitalization in a big way, we have become dependent on online transactions in almost every aspect of life. So the security of communication becomes really important. Cryptographers are continuously putting in their best efforts to make the systems absolutely secure. They can make a system, and may prove that it is secure, but they cannot sit back and relax after making it. Here comes the role of a cryptanalyst. Whenever a security system is launched, cryptanalysts start finding weaknesses in the systems and report it so that the cryptographers can make necessary changes and ensure that the system is more and more secure. Before any adversary takes the advantage of the weaknesses of the system, it should be reported to the makers of the system.

Cryptography is basically categorized into two categories i.e. Symmetric and Asymmetric cryptography. The ciphers built under these categories follow some specific design patterns e.g. Fiestel structure, SPN, La Messy scheme etc. This paper has reviewed the block ciphers and their structures to check their strength, and reviewed the extent of cryptanalysis done on them.

Revised Manuscript Received on May 24, 2019.

Dr. Amandeep, Department of Computer Applications, Lovely Professional University, Phagwara, India.

Dr. G. Geetha, Department of Computer Applications, Lovely Professional University, Phagwara, India.

Organization of this paper is as follows. Section 2 lists the Block ciphers in a chronological order in a table having six columns stating name of the algorithm, year of publication, its
structure, block size, key size, and the cryptanalysis done on that particular cipher. This table becomes the basis of the analysis done in Section 3 and tabulates the information as to which structure has been cryptanalyzed more, thereby establishing a trend of structures analyzed Section 4 identifies the open research problems based on the analysis done in Section 3. Section 5 of the paper, presents the conclusion of this study.

II. RELATED WORK

This paper surveys 69 block ciphers and presents, in Table I, a summarized report as per the attacks concerned.

III. ANALYSIS

The following pie chart summarizes the design structure usage of a sample of 69 block ciphers that have been analyzed for this paper as represented in Fig. 1. The analysis says that to design block ciphers, the Feistel structure has been utilized most as compared to others. We have analyzed further and have shown how the design structures of ciphers have experienced the cryptanalysis attacks. The analysis has been shown design-wise and year-wise as depicted in Fig. 2.

IV. IDENTIFICATION OF RESEARCH PROBLEMS

Based upon the analysis shown in the previous section, some interesting open research problems have been identified, and these can be addressed in future research work in cryptology. Briefly put, these research problems are as follows:

- Lai-Massey structure has to be reconsidered in cryptology to design ciphers as this structure has not been sufficiently considered by cryptanalysts, and consequently subjected to far less attacks.

- Feistel structures must be redesigned with better strong module to thwart attacks as such modular design are yet to be adequately researched for their strength.

- SPN can be used more efficiently. This category of design though not fully exploited in block ciphers yet faces less attack and as such is suitable for light weight cryptography systems.

Table I: List of Block Ciphers

Algorithm	Year	Structure	Block Size	Key Size	Cryptanalysis on the Cipher
Lucifer [3]	1971	Feistel	48, 32 or 128 bits	48, 64 or 128 bits	Differential Cryptanalysis [4], [5]
DES [6]	1975	Feistel	64 bits	56 bits (+ 8 parity bits)	Linear Cryptanalysis [7], Partial and higher order Differential Cryptanalysis [8]
DESX [9]	1984	Feistel	64 bits	184 bits	Related-key cryptanalysis [10]
FEAL [11]	1987	Feistel	64 bits	64 bits	Known Plaintext Attack [12], Statistical Attack [13]
RC2 [14]	1987	Feistel	64 bits	8–1024 bits, in steps of 8 bits; default 64 bits	Related-key cryptanalysis [10]
Khafre [15]	1989	Feistel	64 bits	512 bits	Differential Cryptanalysis [4]
Khufu [15]	1989	Feistel	64 bits	512 bits	Miss in the Middle Attacks [16]
FEALNX [17]	1990	Feistel	64 bits	128 bits	Statistical Attack [13], Known Plaintext Attack [18]
LOKI [19]	1990	Feistel	64 bits	64 bits	Differential Cryptanalysis [4] [20]
Redoc II [21]	1990	Fiestel Structure	80- bits	160 bits	Differential Cryptanalysis [4]
IDEA [22]	1991	Lai-Massey scheme	64 bits	128 bits	Narrow-Bicliques [23]
Blowfish [24]	1993	Feistel	64 bits	32-448 bits	Differential Attack , Reflection attack [25]
Safer K-64 [26]	1993	Iterated	64 bits	64 bits	Key-schedule cryptanalysis [27]
VINO [28]	1993	SPN	64 bits	128 bits	No cryptanalysis identified till date
GOST [29]	1994	Feistel	64 bits	256 bits	Key Recovery Attack [30]
MacGuffin [31]	1994		64 bits	128 bits	Differential Cryptanalysis [32]
RC5 [33]	1994	Feistel	32, 64 or 128 bits (64 suggested)	0 to 2040 bits (128 suggested)	Differential and Linear Cryptanalysis [34]
TEA [35]	1994	Feistel	64 bits	128 bits	Related-key cryptanalysis [10]
Misty1 [36]	1995	Feistel	64 bits	128 bits	Impossible differential and collision search [37]
Akelarre [38]	1996	Lai-Massey scheme	128 bits	128 bits	Chosen Plaintext attack, Ciphertext only attack [39]
BEAR [40]	1996	Feistel	On the order of 2^{13} to 2^{23} bits or more	160 or 128 bits	Meet in the middle attack [41]
CAST128 [42]	1996	Feistel	64 bits	40 to 128 bits	Differential Cryptanalysis [43], Higher Order Differential Attack [44]
LION [40]	1996	Feistel	On the order of 2^{13} to 2^{23} bits or more	160 or 128 bits	Analysis of Security features [41]
Shark [45]	1996	SPN	64 bits	128 bits	No cryptanalysis identified
ICE [46]	1997	Feistel	64 bits	64 bits	Differential cryptanalysis [47]
Square [48]	1997	SPN	128 bits	128 bits	Biclique cryptanalysis [49]
XMX [50]	1997	SPN	Variable	Variable, equal to block size	Multiplicative differentials [51]
AES [52]	1998	SPN	128 bits	128, 192 or 256 bits	Biclique Attack [53], Algebraic Cryptanalysis [54]
BKSQ [24]	1998	Square cipher structure with iterations	96 bits	96, 144, 192 bits	Independent – Biclique Attack on Full BKSQ-96, Independent – Biclique Attack on Full BKSQ-144, Independent – Biclique Attack on Full BKSQ-192 [55]
CAST256 [56]	1998	Feistel	128 bits	128, 160, 192, 224, 256 bits	Differential cryptanalysis [57]
CS Cipher [58]	1998	Feistel	64 bits	128 bits	Analysis on the basis of differential, linear and truncated differential cryptanalysis [59]
Crypton [60]	1998	SPN	128 bits	128, 192, 256 bits	Impossible differential cryptanalysis [61]
DEAL [62]	1998	Feistel	128 bits	128, 192, 256 bits	Key-Schedule Cryptanalysis [63]
DFC [64]	1998	Feistel	128 bits	128, 192, 256 bits	Differential Cryptanalysis [65]
E2 [66]	1998	Feistel	128 bits	128, 192, 256 bits	Impossible Differential Cryptanalysis [67]

Frog [68]	1998	XOR and substitution based modular design	128 bits	128, 192, 256 bits	Differential Attack [69]
Hasty Pudding [70]	1998	Feistel	variable	Variable	Equivalent Keys [71]
LOKI97 [72]	1998	Feistel	128 bits	128, 192, 256 bits	Linear cryptanalysis for some keys [73]
Magenta [74]	1998	Feistel	128 bits	128, 192, 256 bits	Chosen Plaintext Attack [75]
Mars [76]	1998	Feistel	128 bits	128, 192, 256 bits	Preliminary Cryptanalysis of Reduced-Round MARS [77]
RC6 [78]	1998	Feistel	128 bits	128, 192, or 256 bits	Linear Cryptanalysis [79]
Rijndael [24]	1998	SPN	128 bits	128, 192, or 256 bits	Related-key attack [80]
Safer+ [81]	1998	substitution/linear-transformation cipher	128 bits	128, 192, or 256 bits	Linear Cryptanalysis [82]
Serpent [83]	1998	SPN	128 bits	128, 192, or 256 bits	The Rectangle Attack [84]
Skipjack [85]	1998	Feistel	64 bits	80 bits	Cryptanalysis using Impossible Differentials [86]
Twofish [87]	1998	Feistel	128 bits	128, 192 or 256 bits	Related-Key Attacks [88]
Triple-DES [89]	1998	Feistel	64 bits	168, 112 or 56 bits	A Differential Fault Attack [90]
UES [91]	1999	Feistel	128 bits	128, 192 or 256 bits	No cryptanalysis identified till date
Khazad [92]	2000	SPN	64 bits	128 bits	Extension of the Square attack [93]
Anubis [94]	2000	SPN	128 bits	128 to 320 bits in steps of 32 bits	Square Attack [95], Collision Attack [96]
Camellia [97]	2000	Feistel	128 BITS	128, 192, 256 bits	Impossible differential cryptanalysis [98]
DFCv2 [99]	2000	Feistel	128 bits	128, 192, 256 bits	No cryptanalysis identified till date
Grand Cru [100]	2000	SPN	128 bits	128 bits	No Cryptanalysis identified till date
Hierocrypt L1 [101]	2000	SPN	64 bits	128 bits	Differential and Impossible Differential Related-Key Attacks [102]
Hierocrypt3 [103]	2000	SPN	128 bits	128, 192, 256 bits	Impossible Differential Cryptanalysis [104]
Kasumi [105]	2000	Feistel	64 bits	128 bits	Related-Key Rectangle Attack [106]
Nimbus [107]	2000	Fiestel	64 bits	128 bits	Differential cryptanalysis [108]
Noekeon [109]	2000	wide-trail strategy.	128 bits	128 bits	Side Channel Cube Attacks [110]
NUSH [111]	2000	Non fiestel	64, 128, or 256 bits	128, 192, or 256 bits	Linear cryptanalysis [112]
Q [113]	2000	SPN	128 bits	128, 192 or 256 Bits	No cryptanalysis identified till date
Safer++ [114]	2000	substitution/linear-transformation cipher	128 bits	128 or 256 bits	Multiset and boomerang attacks [115]
SC2000 [116]	2000	SPN and Fiestel	128 bits	128, 192, or 256 bits	Differential cryptanalysis [117]
SHACAL [118]	2000	Fiestel	160 bits (SHACAL-1), 256 bits (SHACAL-2)	128 to 512 bits	Differential and Rectangle Attacks [119]
PRESENT [120]	2007	Fiestel	64 bits	80 or 128 bits	Related-key cryptanalysis [121]
KATAN and KTANTAN [122]	2009	Fiestel	32, 48, or 64-bit	80 Bits	3-subset meet-in-the-middle attack [123]
KLEIN [124]	2012	SPN	64 bits	64, 80 and 96-bits	Biclique Cryptanalysis [125]
LED [126]	2012		64 bits	64 bits, 128 bits	Differential analysis [127]
LEA [128]	2014	Non fiestel, based on ARX structure	128-bit	128, 192, or 256-bit	Power Analysis Attacks [129]
Simon and Speck [130]	2015	fiestel	32, 48, 64, 96 or 128 bits	64, 72, 96, 128, 144, 192 or 256 bits	Differential Analysis [131]

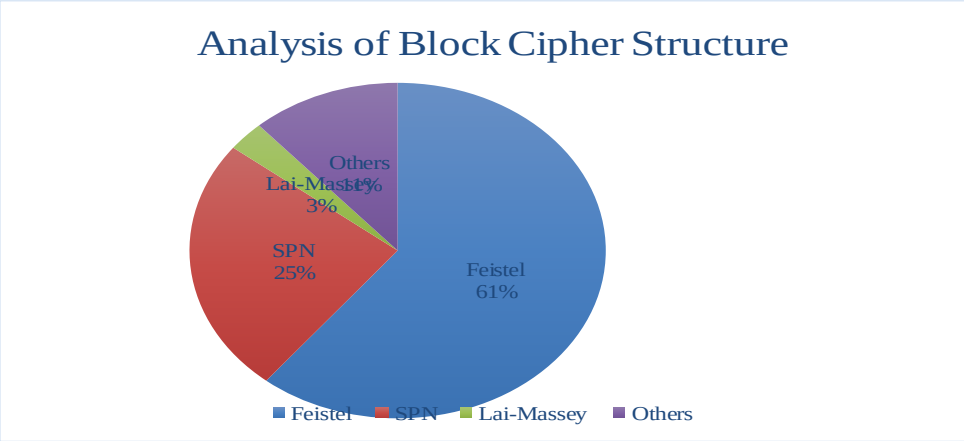

Fig. 1: Usage of Bock Cipher Structures

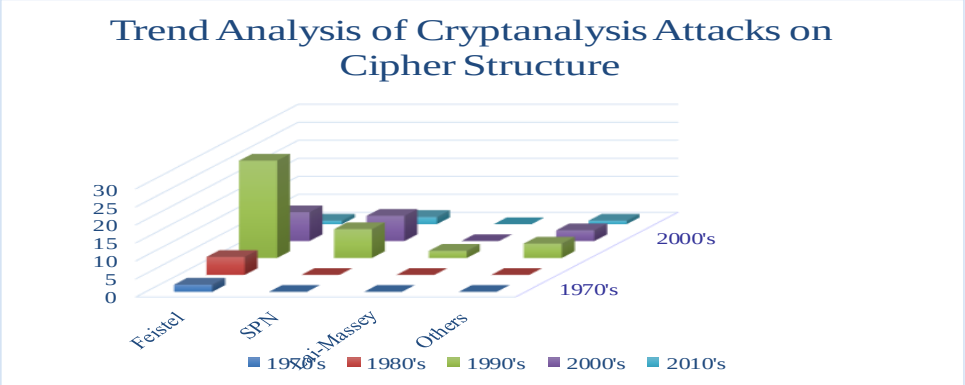

Fig. 2: Trend Analysis of Cryptanalysis Attacks on Cipher Structure

V.CONCLUSION

This paper has surveyed the attacks implemented on block ciphers, starting from linear cryptanalysis to differential cryptanalysis, and attempted to explain these attacks and their trends. The attacks were analyzed on the basis of the cipher design structure, and the time analysis of such attacks is also shown. By analyzing the cryptanalytic attacks on these block ciphers, some emerging research problems have been identified. Awareness of these research problems will help the upcoming research minds concentrate on strengthening the field of cryptology as well as the cryptanalysis domain for beefing up security of cyber data.

REFERENCES

1. D. W. Davies, "Some Regular Properties of the DES," in Advances in Cryptology: A Report on CRYPTO 81, 1981.
2. S. Langford and M. Hellman, "Differential–linear cryptanalysis," in Advances in Cryptology - Crypto'94, Springer Verlag, 1994.
3. J. Smith, "The design of Lucifer: a cryptographic device for data communications," N.Y., USA, 1971.
4. E. B. a. A. Shamir, "Differential Cryptanalysis of Snefru, Khafre, REDOCII, LOKI and Lucifer," 1991.
5. E. Biham and I. Ben-Aroya, "Differential cryptanalysis of Lucifer," Journal of Cryptology, vol. 9, no. 1, pp. 21-34, 1996.
6. "Data Encryption Standard," 1999.
7. M. Matsui, " Linear Cryptanalysis Method for DES Cipher," in Advances in Cryptology -- EUROCRYPT '93, 1993.
8. L. Knudsen, "Partial and higher order differentials and its application to the DES," 1995.
9. P. Rogaway and J. Kilan, "How to protect DES against exhaustive key search," Journal of Cryptology, vol. 14, no. 1, pp. 17-35, 2001.
10. B. S. a. D. W. J. Kelsey, "Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA," in First International Conference on Information and Communication Security ICICS'97, London , 1997.
11. S. Shimizu and Miyaguchi, "Fast Data Encipherment Algorithm FEAL," in Advances in Cryptology - Eurocrypt '87, 1987.
12. A. Y. M. Matsui, "A New Method for Known Plaintext Attack of FEAL Cipher," in EUROCRYPT 1992, 1992. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar
13. G. C. H.Gilbert, "A Statistical Attack of the FEAL-8 Cryptosystem," in 10th Annual International Cryptology Conference on Advances in Cryptology, 1990.
14. R. Rivest, "A description of the RC2(r) encryption algorithm," 1998.
15. R. Merkle, "Fast software encryption functions," in Advances in Cryptology - Crypto'90, A. M. a. S. Vanstone, Ed., Santa Barbara, California, Springer-Verlag, 1990, pp. 476-501.
16. E. Biham, A. Biryukov and A. Shamir, "Miss in the Middle Attacks on IDEA and Khufu," in FSE 1999, L. R.Knudsen, Ed., Heidelberg, Springer, 1999, p. 124–138.
17. S. Miyaguchi, "The FEAL cipher family," in Advances in Cryptology - Crypto'90, A. M. a. S. Vanstone, Ed., California, Springer-Verlag, 1990, pp. 627-638.
18. H. Gilbert and A. Tardy-Corfdir, "A Known Plaintext Attack of FEAL-4 and FEAL-6," in 11th Annual International

Cryptology Conference on Advances in Cryptology, Santa Barbara, California, 1991.
19. M. K. J. P. a. J. S. L. Brown, "Improving resistance to differential cryptanalysis and the redesign of LOKI," in Advances in Cryptology - ASIACRYPT'91, R. R. a. M. H. Imai, Ed., Fujiyoshida, Springer-Verlag, 1991, pp. 36-50.
20. L. Knudsen, "Cryptanalysis of LOKI," in Advances in Cryptology—ASIACRYPT' 91, 1993.
21. M. Wood and T. Cusick, "The RedocII cryptosystem," in Advances in Cryptology - Crypto'90, A. M. a. S. Vanstone, Ed., California, Springer-Verlag, 1990, pp. 545-563.
22. X. Lai, J. Massey and S. Murphy, "Markov ciphers and differential cryptanalysis," in Advances in Cryptology - Eurocrypt'91, D. Davies, Ed., Brighton, Springer-Verlag, 1991, pp. 17-38.
23. D. Khovratovich, G. Leurent and C. Rechberger, "Narrow-Bicliques: Cryptanalysis of Full IDEA," in Advances in Cryptology – EUROCRYPT 2012, D. P. a. T. Johansson, Ed., Heidelberg, Springer, 2012, pp. 392-410.
24. J. D. a. V. Rijmen, " The Block Cipher Rijndael," in Smart Card Research and Applications, B. S. Jean-Jacques Quisquater, Ed., Springer-Verlag , 2000, pp. 277-284.
25. T. Gonzalez, " A Reflection attack on blowfish," J Latex Files 6, 2007.
26. J. Massey, "SAFER-K: a byte-oriented block-ciphering algorithm," in Fast Software Encryption, R. Anderson, Ed., Cambridge, Springer-Verlag, 1994, pp. 1-17.
27. B. S. a. D. W. J. Kelsey, "Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and triple-DES," in Advances in Cryptology—CRYPTO '96, N. Koblitz, Ed., Springer-Verlag, 1996, pp. 237-251.
28. W. Wlfovics and A. Di Porto, "VINO: a block cipher including variable permutations," in Fast Software Encryption, R. Anderson, Ed., Cambridge, Springer-Verlag, 1994, pp. 205-210.
29. G. C. o. t. U. f. Standards, GOST - Gosudarstvennyi Standard 28147-89, 1989.
30. E. Fleischmann, M. Gorski, J. Huehne and S. Lucks, "Key Recovery Attack on full GOST Block Cipher with Negligible Time and Memory," in Western European Workshop on Research in Cryptology (WEWoRC), 2009.
31. M. B. a. B. Schneier, "The MacGuffin cipher algorithm," in ast Software Encryption: Second International Workshop, B. Preneel, Ed., Leuven, Springer-Verlag, 1995, pp. 97-110.
32. V. R. a. B. Preneel, "Cryptanalysis of MacGuffin," in FSE 1994, B. Preneel, Ed., Heidelberg, Springer, 1995, p. 353–358.
33. R. Rivest, "The RC5 encryption algorithm," in Fast Software Encryption: Second International Workshop, B. Preneel, Ed., Leuven, Springer-Verlag, 1995, pp. 86-96.
34. Y. Yin and B. Kaliski, "On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm," in Advances in Cryptology — CRYPTO'95, 1995.
35. D. W. a. R. Needham, "TEA, a Tiny Encryption Algorithm," in Proc. FSE, 1994.
36. M. Matsui, "New block encryption algorithm MISTY," in Fast Software Encryption: 4th International Workshop, FSE'97, E. Biham, Ed., Haifa, Springer-Verlag, 1997, pp. 53-67.
37. Ulrich Kühn, "Cryptanalysis of Reduced-Round MISTY," in Advances in Cryptology — EUROCRYPT 2001, 2001.
38. G. Alvarez, D. d. l. Guia, F. Montoya and A. Peinado, "Akelarre: a new block cipher algorithm," in SAC'96, Workshop Record, Queen's University, Kingston, Ontario, Canada, 1996.
39. B. Schneier and N. Ferguson, "Cryptanalysis of Akelarre," in SAC'97 Fourth Annual Workshop on Selected Areas in Cryptography, Carleton University, 1997.
40. E. Biham and R. Anderson, "Two practical and provably secure block ciphers: BEAR and LION," in Fast Software Encryption, D. Gollmann, Ed., Cambridge, Springer-Verlag, 1996, pp. 99-111.
41. L. R. Knudsen, "On the security of Bear & Lion & ladder - DES," in Fast Software Encryption Workshop, Haifa, Israel, 1997.
42. C. Adams, "Constructing symmetric ciphers using the CAST design procedure," Designs, Codes and Cryptography, vol. 12, no. 3, pp. 283-316, 1997.
43. M. Wang, X. Wang, K. Chow and L. Hui, "New Differential Cryptanalytic Results for Reduced-Round CAST-128," IEICE TRANSACTIONS on Fundamentals of Electronics, Vols. E93-A, no. 12, pp. 2744-2754, 10 2010.
44. S. S. T. K. T. Moriai, "Higher order differential attack of a CAST cipher," FSE 1998, vol. 1372, p. 17–31, 1998.
45. V. Rijmen, J. Daemen, B. Preneel, A. Bossalaers and E. Win, "The cipher Shark," in Fast Software Encryption, D. Gollman, Ed., Cambridge, Springer-Verlag, 1996, pp. 99-111.
46. M. Kwan, "The design of the ICE encryption algorithm," in Fast Software Encryption: 4th International Workshop,FSE'97, E. Biham, Ed., Haifa, Springer-Verlag, 1997, pp. 69-82.
47. L. Knudsen, V. Rijmen and B. Rompay, "Differential cryptanalysis of the ICE encryption algorithm," in 6th International Workshop Fast Software Encryption - FSE'98, 1998.
48. J. Daemen, L. Knudsen and V. Rijman, "The block cipher Square," in Fast Software Encryption, E. Biham, Ed., Springer Berlin Heidelberg, 1997, pp. 149-165.
49. H. Mala, "Biclique-based cryptanalysis of the block cipher SQUARE," Information Security, IET, vol. 8, no. 3, pp. 207-212, May 2014.
50. D. M'Raihi, D. Naccache, J. Stern and S. Vaudenay, "XMX: A firmware-oriented block cipher based on modular multiplications," in Fast Software Encryption, E. Biham, Ed., Haifa, Springer-Verlag, 1997, pp. 166- 171.
51. M. C. R. J. a. D. W. N. Borisov, "Multiplicative differentials," in Fast Software Encryption 2002, Berlin, Springer, 2002, pp. 17 -33.
52. J. D. a. V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, 2002.
53. A. Bogdanov, D. Khovratovich and C. Rechberger, "Biclique cryptanalysis of the full AES," ASIACRYPT 2011, vol. 7073, no. Springer, Heidelberg (2011), pp. 344-371, 2011.
54. H. Nover, "Algebraic Cryptanalysis of AES: An Overview," 2005.
55. F. Abed, C. Foller, E. List, S. Lucks and J. Wenzel, "A Framework for Automated Independent-Biclique Cryptanalysis," in Fast Software Encryption - 20th International Workshop, FSE 2013, S. Moriai, Ed., Springer, 2013, pp. 561-581.
56. H. Heys, C. Adams, S. Tavares and M. Wiener, "CAST256: a submission for the Advanced Encryption Standard," in First AES Candidate Conference (AES1), Ventura, California, USA, 1998.
57. A. Pestunov, "Differential cryptanalysis of 24-round cast-256," in IEEE Region 8 International Conference on Computational Technologies in Electrical and Electronics Engineering, SIBIRCON 2008, Novosibirsk , 2008.
58. S. Vaudenay and J. Stern, "CS-Cipher," in Fast Software Encryption, S. Vaudenay, Ed., Paris, Springer-Verlag, 1998, pp. 189-205.
S. Vaudenay, "On the security of CS-cipher," in Fast Software Encryption, L. Knudsen, Ed., Springer Berlin Heidelberg, 1999, pp. 260-274.

AUTHORS PROFILE

Dr. **Amandeep Bagga** attained her Ph.D. Degree at Lovely Professional University in 2016. She is an Associate Professor and Deputy Dean, Computer Applications in Lovely Professional University Punjab, India. Her broad area of research is Network Security, including sub area of Cryptanalysis. She has 10 years of research experience and total of 13 years teaching experience. She has more than 15 publications in the field of networking & security and currently working on research in crypto currency.

Dr. G. Geetha is presently working as the Professor and Additional Dean in Division of Research and Development at Lovely Professional University, Punjab, India. Her research interests include Cryptography and Security and Software Engineering. She has published more than 70 papers in International Journals and Conferences. She is also performing her responsibilities as a member of the Editorial Board in various international journals.