RECTIFIED DIFFERENTIAL CRYPTANALYSIS OF 16 ROUND PRESENT

Manoj Kumar[1], Pratibha Yadav, Meena Kumari

SAG, DRDO, Metcalfe House, Delhi-110054, India
mktalyan@yahoo.com[1]

ABSTRACT

In this paper, we have suggested rectifications in differential cryptanalysis of ultra-lightweight block cipher PRESENT reduced to 16 rounds. We have shown that proposed differential attack by Wang [3] on 16 round PRESENT can recover at the most 30 subkey bits, although the author has claimed to recover 32 bits of subkey for last two rounds. We have also computed data complexity and success probability for recovering 30 subkey bits accordingly by the differential attack on 16 round PRESENT.

KEYWORDS

Lightweight block cipher, differential cryptanalysis, PRESENT

1. INTRODUCTION

PRESENT [1] is an ultra-lightweight block cipher, proposed by A.Bogdanov et al. in CHES 2007 for extremely constrained environments such as RFID tags and sensor networks. Differential attack [2] against 16 round PRESENT was given by Wang [3] using 2^{64} chosen plaintexts, 2^{32} 6-bit counters and 2^{64} memory accesses and it was claimed to recover 32 subkey bits by differential attack on 16 round PRESENT. In this paper, we have shown that 32 subkey bits of reduced round PRESENT cannot be recovered by this attack [4]. We have also shown that we can recover at the most 30 subkey bits by the differential attack on PRESENT reduced to 16 rounds.

The rest of the paper is organized as follows: Section 2 gives a brief description of PRESENT. In section 3, differential attack on 16-round PRESENT given by Wang is discussed. In section 4, flaws in differential attack on PRESENT are analyzed and rectification for these flaws [4] is suggested. Section 5 concludes the paper.

2. DESCRIPTION OF PRESENT

PRESENT [1] is a symmetric key ultra-lightweight block cipher. It takes plaintext block of length 64 bits and produces ciphertext block of 64 bits. It consists of total 31 rounds. Based on the length of the key there are two variants of PRESENT, denoted by PRESEST-80 and PRESENT-128 with key of length 80 bits and 128 bits respectively. Brief description of the encryption process and the key schedule for PRESENT-80 is given below.

2.1 The Encryption Process

Each round of the PRESENT [1] has three layers of operations. The first layer of operations is *addRoundKey* described as follows: $b_j \rightarrow b_j \oplus k_{i,j}$

where b_j, $0 \le j \le 63$ is the current state and $k_{i,j}$ $1 \le i \le 32$, $0 \le j \le 63$ is the j^{th} subkey bit of round key K^i.

DOI:10.5121/ijcis.2012.2404

The second layer of operations is *sBoxLayer*. PRESENT uses only one S-box S (Table 1) of length 4-bit which is applied 16 times in parallel in each round.

Table 1: S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

The third layer of operations is *player*, the pLayer is a bit permutation layer, in which bit i of a stage is moved to bit position P(i) according to the following rule:

$$P(i) = i*16 \pmod{63}, \ 1 \le i \le 62 \quad \text{and} \quad P(i) = i, \text{ for } i = 0 \ \& \ i = 63$$

We omit the key schedule algorithm of PRESENT as it is not used in our analysis. Interested readers can refer to [1] for details.

3. Differential Cryptanalysis of Reduced Round PRESENT [3]

Differential cryptanalysis for recovering 32 subkey bits of 16 round PRESENT-80 by using 24 14-round differential characteristics of probability 2^{-62} is given by Wang.

3.1 Difference pairs for S-box

The difference distribution table (Table 2) for the S-box of PRESENT is given below, in which rows and columns represent ΔX and ΔY value (in hexadecimal) respectively. Each element of the table represents the number of occurrences of the corresponding output difference ΔY given the input difference ΔX, besides the special case of both input and output values being 0, the largest value in the table is 4. The smallest value in the table is 0 and occurs for many difference pairs. From table 2, we see that the maximum differential probability is 2^{-2}.

Table 2: Difference distribution table of S-box

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

3.2 Differential Characteristics [3]

24 differential characteristics for PRESENT are given by Wang [3] with the probability of each characteristic as 2^{-62}. Out of the 24 differential characteristics, 20 differential characteristics have different input differences but the same output difference and 4 pairs of differential characteristics have same input difference but different difference from the output of round 2 to the input of round 8. All the characteristics have the same difference after 8^{th} round. All of the 24 differential characteristics have 2 active S-boxes located in the position 0,1,2,12,13 and 14, so the S-boxes in position from 3 to 11 and 15 are all non-active. According to the output difference of differential characteristics for 14-round, there are two active S-boxes in round 15 which are x_0 and x_8, whose input difference is 9 and output differences will be 2, 4, 6, 8, 12 or 14. The least significant bit of all the possible output differences is zero; therefore at most 6 bits are non zero for the output difference of S-boxes in round 15. After pLayer of round 15, the maximum number of active S-boxes for round 16 is 6 and minimum number of active S-boxes is 2 (E-mail communication: Wang, 2009).

Considering 6 S-boxes in round 16 namely x_4, x_6, x_8, x_{10}, x_{12} and x_{14}, Wang claimed to recover 24 bits of round subkey K^{17} namely $k_{17,4}$, $k_{17,20}$, $k_{17,36}$, $k_{17,52}$, $k_{17,6}$, $k_{17,22}$, $k_{17,38}$, $k_{17,54}$, $k_{17,8}$, $k_{17,24}$, $k_{17,40}$, $k_{17,56}$, $k_{17,10}$, $k_{17,26}$, $k_{17,42}$, $k_{17,58}$, $k_{17,12}$, $k_{17,28}$, $k_{17,44}$, $k_{17,60}$, $k_{17,14}$, $k_{17,30}$, $k_{17,46}$, $k_{17,62}$ and 8 bits of round subkey K^{16} namely $k_{16,0}$, $k_{16,8}$, $k_{16,16}$, $k_{16,24}$, $k_{16,32}$, $k_{16,40}$, $k_{16,48}$, $k_{16,56}$. The author has claimed to recover total 32 subkey bits.

For getting right pairs for differential cryptanalysis, we xor bits of ciphertext pairs corresponding to non-active S-boxes namely x_0, x_1, x_2, x_3, x_5, x_7, x_9, x_{11}, x_{13}, x_{15} and this sum should be zero for right pairs. After getting right pairs, bits of right pairs corresponding to active S-boxes in the last two rounds will be decrypted from 16^{th} round to 14^{th} round. 24 bits of round subkey K^{17} and 8 bits of round subkey K^{16} will be involved during decryption from round 16 to round 14.

4. RECTIFIED DIFFERENTIAL CRYPTANALYSIS

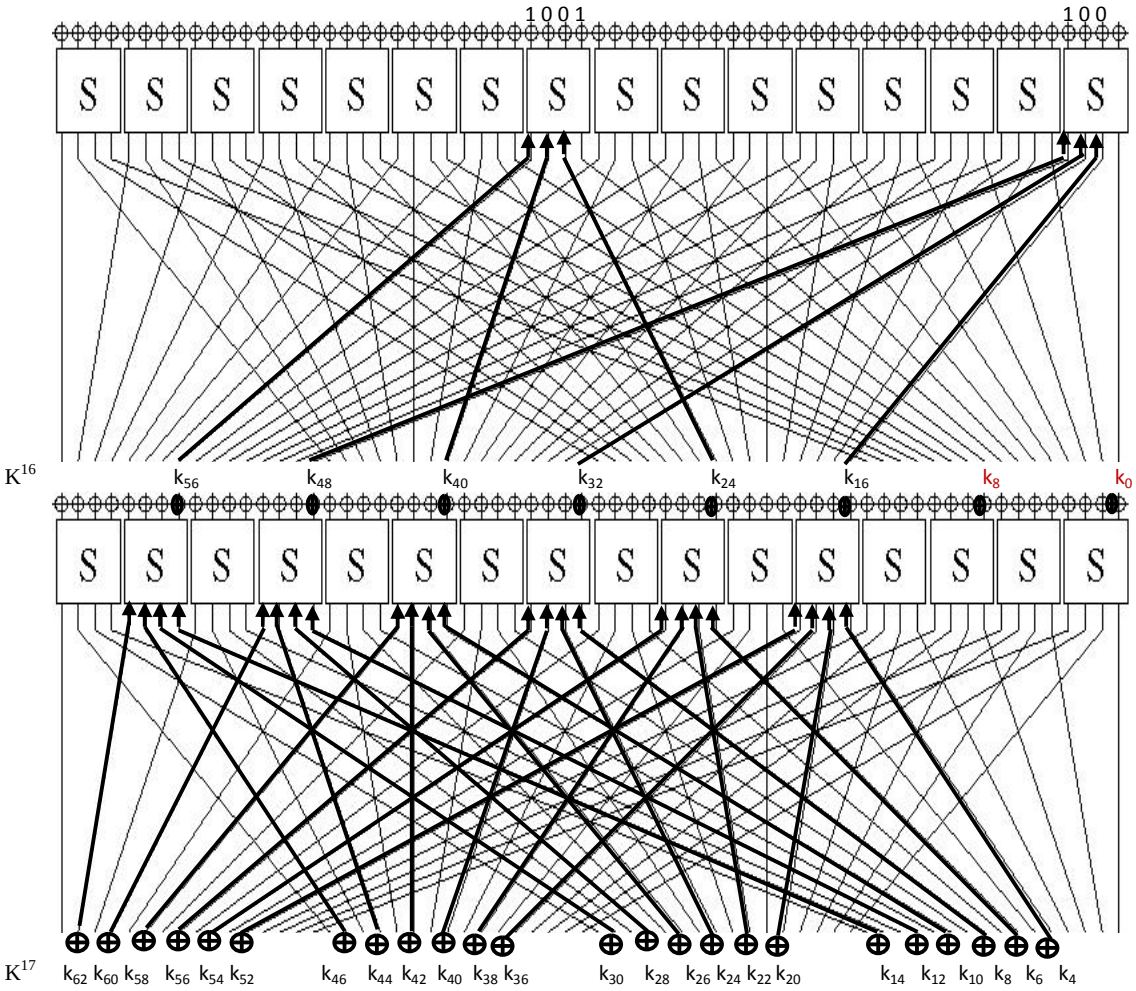
We found that 32 subkey bits as claimed by Wang cannot be recovered by this attack. One can recover 24 bits of round subkey K^{17} and 6 bits of round subkey K^{16}. Therefore at the most 30 subkey bits can be recovered by the proposed differential attack on 16 round PRESENT. This is shown graphically below in figure 1.

4.1 Flaws identified in Differential Cryptanalysis [4]

In round 16, 24 ciphertext bits corresponding to 24 bits of round subkey K^{17} are extracted for right pairs and x-ored with all possible values of 24 bits of round subkey K^{17}. After applying inverse pLayer, the intermediate 24 bits namely C_{16}, C_{17}, C_{18}, C_{19}, C_{24}, C_{25}, C_{26}, C_{27}, C_{32}, C_{33}, C_{34}, C_{35}, C_{40}, C_{41}, C_{42}, C_{43}, C_{48}, C_{49}, C_{50}, C_{51}, C_{56}, C_{57}, C_{58}, C_{59}, will be passed through inverse S-box.

In round 15, we are able to extract only 6 bits corresponding to 6 bits of round subkey K^{16} from 24 bits of previous round. Extract these 6 ciphertext bits and xor these bits with all possible values of 6 bits of round subkey K^{16}. After applying inverse pLayer, only 6 intermediate ciphertext bits namely C'_1, C'_2, C'_3, C'_{33}, C'_{34}, C'_{35} are left to pass through inverse S-box. But in practice, we need 4 bits to pass through one S-box, as PRESENT uses one 4x4 S-box, which take 4 bits as input and produces 4 bits as output. These 6 bits cannot be grouped together to pass through inverse S-box.

Figure 1: Flaws in differential attack on 16 round PRESENT [4]



Therefore we need bits at position C'_0 and C'_{36} to complete the 4 bits set to pass through inverse S-box. For getting these two bits, either we need to decrypt additional 8 bits from 16th round or we should be able to extract 8 intermediate ciphertext bits form 15th round. But this is not possible due to output difference of difference distribution table for S-box in 15th round and the possible outputs of 15th round for input difference 1001 are all even with at the most 6 non zero bits, which leads to only 6 active S-boxes in 16th round though we require 8 active S-boxes here.

4.2 Rectification in Differential Cryptanalysis

For recovering 30 subkey bits, decrypt the ciphertext from round 16 to round 14. In round 16, extract 24 bits of ciphertext corresponding to 24 bits of round subkey K^{17} namely $k_{17,4}$, $k_{17,20}$, $k_{17,36}$, $k_{17,52}$, $k_{17,6}$, $k_{17,22}$, $k_{17,38}$, $k_{17,54}$, $k_{17,8}$, $k_{17,24}$, $k_{17,40}$, $k_{17,56}$, $k_{17,10}$, $k_{17,26}$, $k_{17,42}$, $k_{17,58}$, $k_{17,12}$, $k_{17,28}$, $k_{17,44}$, $k_{17,60}$, $k_{17,14}$, $k_{17,30}$, $k_{17,46}$, $k_{17,62}$ and x-or these with all possible values of 24 subkey bits, and then apply inverse permutation layer and inverse S-box. After that extract 6 intermediate ciphertext bits in 15th round corresponding to 6 bits of round subkey K^{16} namely $k_{16,16}$, $k_{16,24}$, $k_{16,32}$, $k_{16,40}$, $k_{16,48}$, $k_{16,56}$ and x-or these with all possible values of 6 subkey bits and then apply inverse permutation layer. Now for each intermediate ciphertext pair, assume all 4 possible values

of additional two bits to complete set of 4 bits to pass through inverse S-box. After that apply inverse S-box and find out x-or of the two decrypted pairs and check whether it is the same x-or as suggested by the characteristics. If it is the same x-or value then increase the counter of the corresponding key value by 1 and the key giving the desired x-or value maximum number of times will be our correct values for the 30 subkey bits.

4.3 Computational Complexity

As given by Wang [2], 2^{40} structures (of 2^{24} chosen plaintext each) are required in this attack. 2^{40} possible values can be taken as inputs to 10 non-active S-boxes in each structure and the inputs to any two active S-boxes in each structure characteristic among the six S-boxes have 2^{24} possible values. The number of pairs for each possible characteristic is $2^{40}*2^{16}*2^{7}=2^{63}$. The number of pairs satisfying 24 characteristics is $2^{63}*20 = 2^{67.32}$. Since each characteristic has the same probability 2^{-62}, so there are $2^{63}*2^{-62}*24 = 48$ right pairs satisfying any one characteristic. For each structure, there is $(2^{24})^2/2 = 2^{47}$ possible pairs, thus we have to consider total $2^{47}.2^{40}=2^{87}$ pairs of plaintext.

For each structure, each pair should have 10 non-active S-boxes in 16^{th} round satisfying each characteristic. After discarding wrong pairs, for each structure the number of candidates left for right pair is $2^{47}*2^{-40}=2^{7}$.

Among 16 S-boxes in round 16, 10 S-boxes must be non-active. Among the remaining 6 S-boxes in round 16, we will consider 36 cases according to the output of the S-box in round 15. As input to round 15 S-box is 9, therefore the possible outputs from the S-box difference distribution table will be

(2,2), (2,4), (2,6), (2,8), (2,C), (2,E), (4,2), (4,4), (4,6), (4,8), (4,C), (4,E), (6,2), (6,4), (6,6), (6,8), (6,C), (6,E), (8,2), (8,4), (8,6), (8,8), (8,C), (8,E), (C,2), (C,4), (C,6), (C,8), (C,C), (C,E), (E,2), (E,4), (E,6), (E,8), (E,C), (E,E).

If an S-box is active, the input difference to this S-box should be 1 and output difference will be 3, 7, 9 or 13 and if S-box is non-active then input and output differences will be 0. Using this filter, discard any pair with a wrong output difference. So the expected number of remaining pairs for each structure is about:

$$2^{7}*\{9*(4/16)^{2}(1/16)^{4}+12*(4/16)^{3}(1/16)^{3}+10*(4/16)^{4}(1/16)^{2}+4*(4/16)^{5}(1/16)+(4/16)^{6}\}$$
$$= 2^{7}*2^{-10.49} = 2^{-3.49}$$

For each structure, it is checked that whether the remaining pairs satisfy one of the 24 possible plaintext differences corresponding to 24 characteristic. Number of remaining pairs is a fraction of about $2^{-24}*20 = 2^{-19.68}$ out of the 2^{24} possible plaintext differences. So the expected number of remaining pairs in all 2^{40} structures is

$$2^{40}*2^{-3.49}*2^{-19.68} = 2^{16.83}.$$

We guess the 24 bits of round subkey K^{17} and 6 bits of round subkey K^{16} and decrypt the remaining ciphertext pairs from round 16 to round 14. There are at the most 4 pairs of occurrences for the given input difference and output difference, according to the difference distribution table of S-box for PRESENT. We denote number of active S-boxes in round 16 by t ($2 \le t \le 6$). We consider 5 cases according to the value of t as given in the table 3 below:

Table 3: Cases according to the number of active S-boxes

t	NCP	TCS	TCSRP
2	$2^{16.83}*2^{-16}= 2^{0.83}$	4^4*16^4	$2^{0.83}*4^4*16^4= 2^{24.83}$
3	$2^{16.83}*(2^{-12}- 2^{-16})= 2^{4.74}$	4^5*16^3	$2^{4.74}*4^5*16^3= 2^{26.74}$
4	$2^{16.83}*(2^{-8}- 2^{-12})= 2^{8.74}$	4^6*16^2	$2^{8.74}*4^6*16^2= 2^{28.74}$
5	$2^{16.83}*(2^{-4}- 2^{-8})= 2^{12.74}$	4^7*16^1	$2^{12.74}*4^7*16^1= 2^{30.74}$
6	$2^{16.83}*(1-2^{-4})= 2^{16.74}$	4^8*16^0	$2^{16.74}*4^8*16^0= 2^{32.74}$

where NCP = number of ciphertext pairs satisfying the condition of t active S-boxes

TCS = the total counted subkey
TCSRP = the total counted times of subkey for the remaining pairs

The total counted times of subkey are about $2^{24.83} + 2^{26.74} + 2^{28.73} + 2^{30.75} + 2^{32.74} = 2^{33.15}$ .Therefore, on an average wrong subkey will hit about $2^{33.155}/2^{30}= 8.9$ times, but still the right key can be identified because it is counted for the right pairs about 48 times. Therefore we can retrieve 30 subkey bits using at the most $2^{33.15}$ times encryptions of 2-round PRESENT and 2^{30} 6-bit counters. We can find out 80 bit master key by exhaustively searching the remaining 50 bits of master key and the time complexity in this step will be 2^{50} 16 round PRESENT encryptions.
In modified attack, the signal to noise ratio [4] is

$$S/N = (p*2^k) / (\alpha*\beta) \quad = 2^{-62}*2^{30} / (2^{33.15-16.83}*2^{16.83-67.32}) = 4.5$$

where p is the probability of the differential characteristics, k is the number of subkey bits involved in decryption from 16^{th} to 14^{th} round, α is the average count of keys that are suggested per analyzed pair after excluding the wrong pairs discarded before counting and β is the fraction of analyzed pair among all pairs.

Success probability [4] for $\mu = p*N = 2^{-62}*2^{63}*24 = 48$ right pairs and k = 30 subkey bits involved in decryption from round 16 to round 14 is: $P_s= 0.999999904$

Thus we can obtain 30 subkey bits with the probability 0.999999904. Time complexity is almost same as in [3], except the time complexity of 2^{50} 16-round PRESENT encryptions in step 3 of the algorithm presented in [3].

5. CONCLUSION

In this paper, we have shown that proposed differential attack on 16 round PRESENT [2] cannot recover 32 subkey bits of 80 bit master key. We have also shown that one can recover at the most 30 subkey bits by the differential attack with the success probability of 0.999999904. Lots of work has been done and is being done in [6], [7], [8], [9] on the basis of this differential attack given by Wang [3] assuming to recover 32 subkey bits of 16 round PRESENT, therefore the rectifications made out to come to the conclusion that the number of subkey bits recoverable by this attack is exactly 30 and not 32 as claimed earlier is very important for further research.

ACKNOLEDGEMENTS

Authors are grateful to Dr. PK Saxena, Director SAG and Dr. SS Bedi, Associate Director SAG for their support and encouragement. We also thank Ms. Noopur Shrotriya for helping us in s/w implementation and Mr. Dhananjoy Dey for giving his valuable time in fruitful discussions. Authors are also thankful to anonymous reviewer for their fruitful comments and suggestions in improving the paper.

REFERENCES

[1] A Bogdanov, L Knudsen, G Leander, C Paar, A Poschmann, M Robshaw, Y Seurin and C Vikkelsoe; (2007) "PRESENT: An Ultra-Lightweight Block Cipher", in the proceedings of CHES 2007, LNCS, vol. 4727, pp 450-466.

[2] Eli Biham and Adi Shamir; (1991) "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, 1991, Vol. 4, No. 1, pp 3–72

[3] M Wang; (2008) "Differential Cryptanalysis of Reduced-Round PRESENT", in the proceedings of AFRICACRYPT 2008, LNCS, vol. 5023, pp 40-49.

[4] M Kumar, P Yadav and M Kumari; (2010) "Flaws in Differential Cryptanalysis of Reduced Round PRESENT", Cryptology e-Print Archive Report 2010/407. Available at http://eprint.iacr.org/2010/407.pdf

[5] AA Selcuk; (2008) "On Probability of Success in Linear and Differential Cryptanalysis", Journal of Cryptology, 2008, Vol. 21, No.1, 131–147.

[6] Albrecht, M. and Cid, C. Algebraic Techniques in Differential Cryptanalysis, in the proceedings of Workshop on FSE 2008, LNCS, Vol. 5665, pp 193-208

[7] C Blondeau and B Gerard; (2010) "Links between Theoretical and Effective Differential Probabilities: Experiments on PRESENT", in Workshop on Tools for Cryptanalysis 2010 at http://www.rocq.inria/fr/secret/Celine.Blondeau/PDF/tools10.pdf

[8] C Blondeau and B Gerard; (2011) "Multiple Differential Cryptanalysis: theory and practice", in the proceedings of Workshop on Fast Software Encryption 2011, Available at http://www.rocq.inria/fr/secret/Celine.Blondeau/PDF/FSE.pdf

[9] F Abazari and B Sadeghian; (2011) "Cryptanalysis with Ternary Difference: Applied to Block Cipher PRESENT, in Cryptology e-Print Archive Report 2011/22. Available at http://eprint.iacr.org/2011/022.pdf

Authors

Manoj Kumar received M.Sc. and M.Phil in Mathematics from CCS University, Meerut, India in year 2001 and 2004 respectively. He is currently pursuing Ph.D. in Cryptography from Department of Mathematics, University of Delhi, India. His main research areas are Design and Cryptanalysis of Block Ciphers.

Pratibha Yadav received M.Sc. in Mathematics from University of Delhi, India in the year 1985. Her main research interests are fuzzy logic and cryptology.

Meena Kumari received Ph.D. degree on "Some Studies in Periodic Sequences over GF(2)" from University of Delhi, India (1985). Her main research interests are design and analysis of crypto-algorithm.