# Biclique cryptanalysis of MIBS-80 and PRESENT-80

Mohammad Hossein Faghihi Sereshgi, Mohammad Dakhilalian, and Mohsen Shakiba

**Abstract** In this paper we present the first biclique cryptanalysis of MIBS block cipher and a new biclique cryptanalysis of PRESENT block cipher. These attacks are performed on full-round MIBS-80 and full-round PRESENT-80. Attack on MIBS-80 uses matching without matrix method and has a data complexity upper bounded by $2^{52}$ chosen plaintext where it reduced security of this cipher about 1 bit. Attack on PRESENT-80 has a data complexity of at most $2^{22}$ chosen plaintexts and computational complexity of $2^{79.37}$ encryptions that both complexities are lower than other cryptanalyses of PRESENT-80 so far.

## 1 INTRODUCTION

Along advances in low resource applications such as RFID tags and Internet of Things, lightweight cryptography became a popular field of study to find appropriate solutions to different purposes of security in low resource devices. So far, many block ciphers like MIBS [1], Lblock [2] and PRESENT [3] are introduced to satisfy conditions of constrained applications. Biclique cryptanalysis of block ciphers introduced by Andrey Bogdanov et al. [4]. After that, many studies have been done on security of different lightweight ciphers against biclique attack ([5], [6],[7],[8],).

The best known attack on PRESENT-80 is also a biclique cryptanalysis which covers all rounds of PRESENT-80 and has data complexity equals to $2^{25}$ chosen plaintext and computational complexity equals to $2^{79.49}$ with success probability equal to 100% [7]. Also there are other biclique cryptanalysis of PRESENT ([9],[7],[10]). The best known attack on MIBS-80 is a Multidimensional Linear

M.H. Faghihi Sereshgi and M.Dakhilalian
Isfahan University of Technology, Isfahan, Iran, e-mail: mh.faghihi@ec.iut.ac.ir ; mdalian@cc.iut.ac.ir

Mohsen Shakiba
Jundi-Shapur University of Technology, Dezful , Iran e-mail: m.shakiba@jsu.ac.ir

Cryptanalysis which covers 19 rounds of MIBS with data complexity equals to $2^{57.87}$ chosen plaintext and computational complexity equal to $2^{74.23}$ encryption of 19 rounds of MIBS with success probability equal to 90% [11]. There are also other cryptanalysis of MIBS([12],[11],[13]) . In this paper we will present the biclique cryptanalysis of MIBS-80 and PRESENT-80. These attacks are in single key mode.

This paper is organized as follow. Section 2. provides description of MIBS-80 cipher. Section 3 shows the key recovery attack on full-round MIBS-80. A brief description of PRESENT-80 cipher is provided in section 4. Biclique Cryptanalysis of PRESENT-80 is presented in section 5. A conclusion of this paper is given in section 6.

## 2 DESCRIPTION OF MIBS

Block cipher MIBS uses a standard Feistel structure with 64-bit block length and supports user key of lengths 64-bit and 80-bit. Each round function of MIBS consists of a key addition layer, a nibble-wise S-box layer , and a mixing layer can be represented by a simple matrix production $M : (GF(2^4)^8) \longmapsto (GF(2^4)^8)$. In this paper we consider 80 bit key length version of MIBS (MIBS-80). So, if $state^0$ is initialized by the 80-bit user key as $state^0 = k_{79}, k_{78}, ..., k_0$ , then 32 round keys ,$0 \leq i \leq 31$ , are generated as follows:

$$state^i = state^i >>> 19$$

$$state^i = Sbox(state^i_{[79:76]}) \,||\, Sbox(state^i_{[75:72]}) \,||\, state^i_{[71:0]}$$

$$state^i = state^i_{[79:19]} \,||\, \left(state^i_{[18:14]} \oplus Round - Counter\right) || \, state^i_{[13:0]}$$

$$K^i = state^i_{[79:48]}; state^{i+1} = state^i$$

## 3 KEY RECOVERY FOR MIBS-80

According to the key schedule of MIBS-80, the ’user key’ can be computed from each $state^i$ ,$0 \leq i \leq 31$ . For mounting the biclique attack on MIBS-80, vector space of $state^{28}$ is divided into $2^{72}$ subsets each of them includes $2^8$ values of $state^{28}$. For this purpose, in each subset only bits in positions $[44, 43, 42, 41, 11, 10, 9, 8]$ are varied and the rest remain unchanged.

An independent biclique of dimension 4, is placed in the five final rounds of cipher. For this purpose we consider two related-key differentials; the first one in the encryption path caused by 16 possible differences of four bits $[44, 43, 42, 41]$ of $state^{28}$ each of them represented by $\Delta K[i]$ , $0 \leq i \leq 15$ . The second related-key differential in the decryption path is also generated by 16 possible differences of four bits $[11, 10, 9, 8]$ of $state^{28}$ each of them represented by $\Delta K[j]$ , $0 \leq j \leq 15$ . As it can be seen in Fig. 1, these two related-key differentials share no active S-boxes, So they can be used to make an independent biclique, which covers $2^8$ possible differences $\Delta K[i,j] = \Delta K[i] \oplus \Delta K[j]$ , as it was expected.

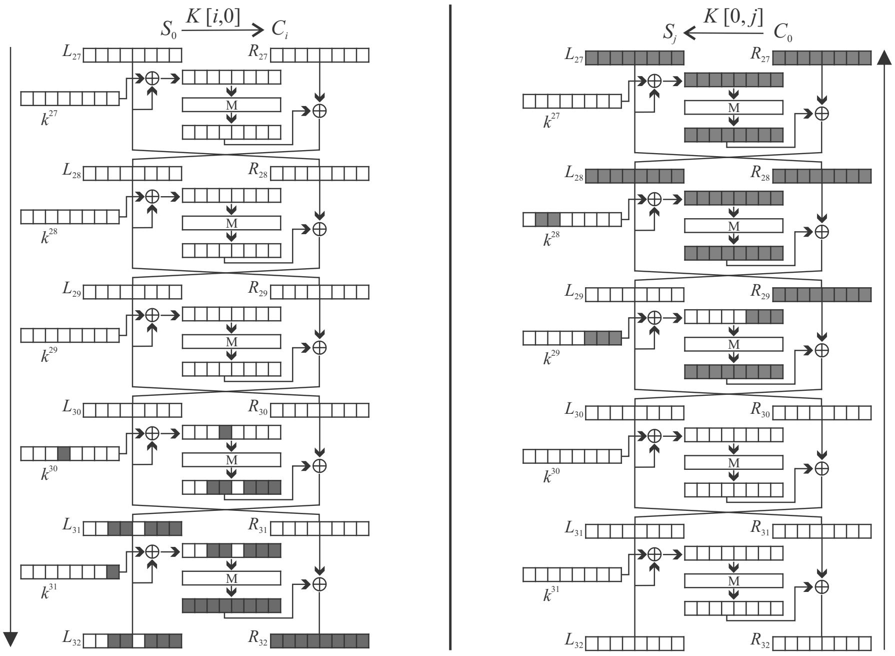

**Fig. 1** 4-dimension Biclique for MIBS over rounds 28-32

### 3.1 Matching without Matrix

The Matching without matrix method presented in [14] could reduce the computational complexity of the matching nibbles recomputation. According to the Feistel structure of MIBS cipher, we have

$$L_{i+1} = M(S(L_i \oplus K_i)) \oplus R_i$$

, which $M$ and $S$ represent the operation of mix and substitution layer . Also, it could be easily derived that

$$L_{i+1} = M(S(R_{i+3} \oplus K_{i+2})) \oplus L_{i+3}$$

. So we have the equality

$$M(S(L_i \oplus K_i)) \oplus R_i = M(S(R_{i+3} \oplus K_{i+2})) \oplus L_{i+3}$$

leads to the equality

$$S(L_i \oplus K_i) \oplus M^{-1}(R_i) = S(R_{i+3} \oplus K_{i+2}) \oplus M^{-1}(L_{i+3})$$

.

In our attack, we choose the $L_{14}$ (left part of data register in round 15 that is the input of F-function in round 15) as matching point. So we can choose the data corresponding to the 4th and the 5th S-boxes in round 14 and their corresponding S-boxes in round 16 which mean the 4th and the 5th S-boxes in round 16 as matching variable

### 3.2 B. The attack procedure

Step 1: *Constructing biclique*. Set bits numbers $[44,43,42,41,11,10,9,8]$ of $state^{28}$ to zero and choose a new value for the other 72 bits, assume it as $K[0,0]$ and construct a biclique as follows:

- choose $C_0 = 0_{(64)}$ as ciphertext and decrypt it to round 28 using $K[0,0]$ to obtain $S_0$, the data register in round 28 (i.e. $L_{27}$ and $R_{27}$).

- Decrypt $C_0$ with keys $K[0,0] \oplus \Delta K[0,j]$ , $1 \leq j \leq 15$ , to obtain $S_j$ (in the input of round 28).

- Encrypt S0 with keys $K[0,0] \oplus \Delta K[i,0]$ , $1 \leq i \leq 15$ to obtain $C_i$. Also, get their corresponding plaintexts $P_i$ ,$0 \leq i \leq 15$ .

Step 2: *Matching*. Encrypt $P_i$ with $K[i,0]$ to round 14 to obtain the matching variable $\overrightarrow{v_{i,0}}$ and store the process $P_i \xrightarrow{K[i,0]} \overrightarrow{v_{i,0}}$ . Then encrypt $P_i$ with $\Delta K[i,j]$, $1 \leq j \leq 15$ to obtain $\overrightarrow{v_{i,j}}$ . Only compute those parts of these processes that differ from the process $P_i \xrightarrow{K[i,0]} \overrightarrow{v_{i,0}}$ . Decrypt $S_j$ with $\Delta K[0,j]$ to round 16 to obtain the matching variable $\overleftarrow{v_{0,j}}$ and store the process $\overleftarrow{v_{0,j}} \xrightarrow{K[i,0]} S_j$. Then decrypt $S_j$ with $\Delta K[i,j], 1 \leq i \leq 15$ to obtain $\overleftarrow{v_{i,j}}$ and only compute those parts that differ from $\overleftarrow{v_{0,j}} \xrightarrow{K[i,0]} S_j$. The procedure of matching is shown in Fig. 2 . A candidate key $\Delta K[i,j]$ leads to $\overrightarrow{v_{i,j}} = \overleftarrow{v_{i,j}}$ . While matching variables are 8 bits we anticipate $2^{8-8} = 1$ key candidate for each key set. Exhaustive search is needed to filter out wrong candidate keys.

*Data complexity*. According to Fig. 1, 3 nibbles of ciphertext is not effected by key differences. So the data complexity will not exceed $2^{64-12} = 2^{52}$ chosen plaintexts. *Computational complexit*y. In step 1, $24 \times (19+6) + 15 = 415$ S-boxes, in step 2, $24 \times (34 + 24 \times (71)) = 18720$ S-boxes plus $24 \times (9 + 24 \times (80)) = 20624$ S-boxes are computed. In key schedule $24 \times (3+9) + 52 = 244$ S-boxes are computed. Also there is 1 candidate key per each key set in average. The MIBS-80 uses 320 S-boxes in a full round encryption, so the computational complexity is as follow:

$$C_{full} = 2^{72}\left(\frac{39344 + 415 + 224}{320} + 1\right) = 2^{78.98}$$

Since we used all keys in this attack, its success probability is 100

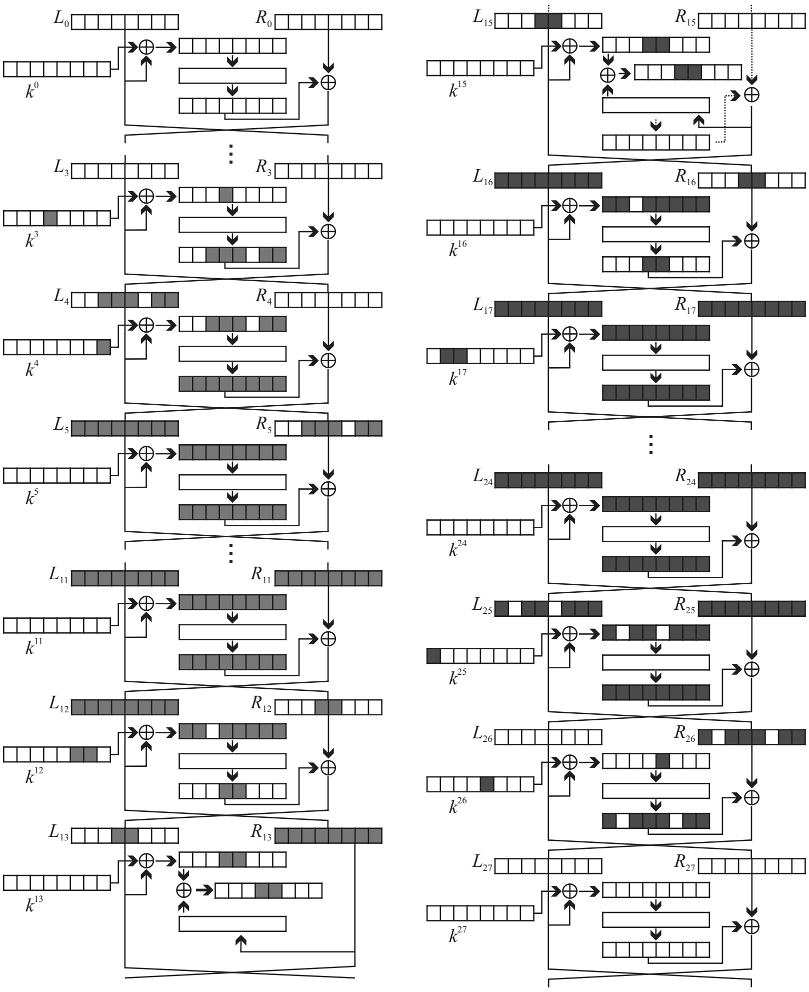

**Fig. 2** Matching over 27 rounds; left: Forward computation; right: Backward computation

## 4 DESCRIPTION OF PRESENT-80 CIPHER

PRESENT uses a SPN structure with 64-bit block length and supports user keys of lengths 80-bit and 128-bit. Each round function of PRESENT consists of a key addition layer, a nibble-wise S-box layer ($S : GF(2^4) \to GF(2^4)$ ) and a simple permutation layer. In this paper we consider 80 bit key length version of

PRESENT (PRESENT-80). So, if $state^0$ is initialized by the 80-bit user key as $state^0 = k_{79}k_{78}\dots k_0$ , then 31 round keys and the post whitening key $K^i$ , $0 \leq i \leq 31$ , are generated as follows:

$$K^i = state^i_{[79:16]}$$

$$state^i = state^i >>> 19$$

$$state^i = Sbox(state^i_{[79:76]}) \parallel state^i_{[75:0]}$$

$$state^i = state^i_{[79:20]} \parallel \left(state^i_{[19:15]} \oplus Round - Counter\right) \parallel state^i_{[14:0]};$$

$$state^{i+1} = state^i$$

## 5 KEY RECOVERY FOR PRESENT-80

In case of PRESENT, the vector space of $state^28$ is divided into $2^{72}$ subsets each of them includes $2^8$ values of $state^28$. To construct an independent biclique of dimension 4, we considered the four bits $[8,7,6,4]$ of $state^28$ to cause 16 differences $\Delta K[i]$ , $0 \leq i \leq 15$ , and four bits $[40,39,38,31]$ of $state^28$ to cause 16 differences $\Delta K[j]$ , $0 \leq j \leq 15$ , which according to Fig. 3 share no active S-boxes in differential trails in the last 3 rounds.

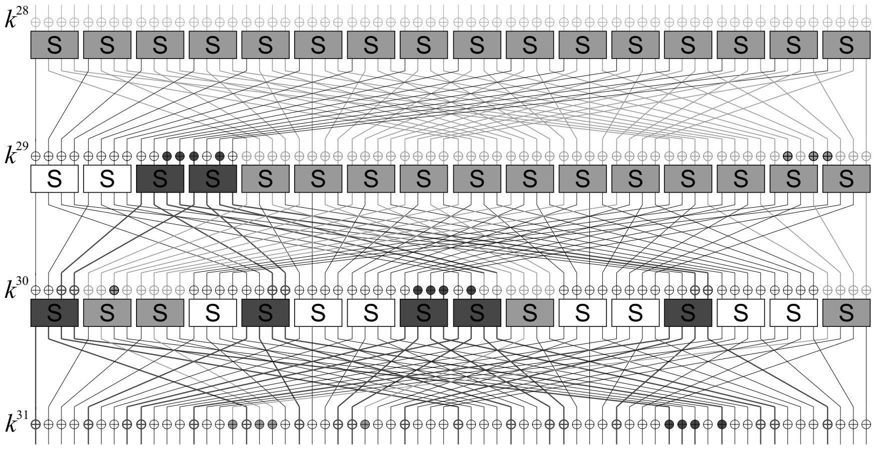

**Fig. 3** 4-dimension Biclique for PRESENT-80 over rounds 29-31

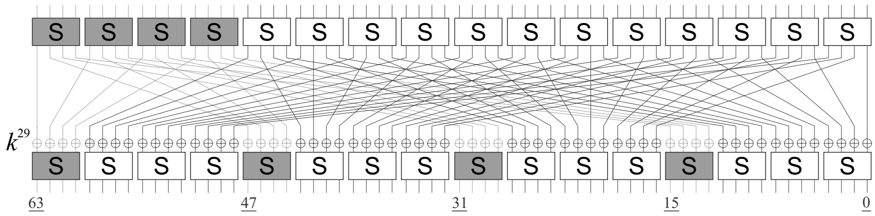

**Fig. 4** Sieve over the steps SLPLAKSL for PRESENT.

## 5.1 Sieve-In-The-Middle

To cryptanalysis the PRESENT block cipher we use the Sieve-In-The-Middle attack [12] and we use the sieve introduced in [11]. In this sieve we choose 16 left most bits of input of a subcipher Es=SLPLAKSL for input, and bits in positions (63,62,61,60,47,46,45,44,37,36,35,34,15,14,13,12) for the key and output, as is shown in Fig. 4. Prestored values of inputs and outputs of this superbox and their corresponding keys could be used as matching variables to filter out wrong keys.

## 5.2 The attack procedure

Step 1:*Constructing biclique*. Similar to step 1 of section 3.2 and by assuming $C_0 = 0_{(64)}$ and internal state S in round 28, we construct $S_j$,$0 \leq j \leq 15$ and $C_i$,$0 \leq i \leq 15$ and their corresponding $P_i$,$0 \leq i \leq 15$ .

Step 2: *matching*. We compute the value of $\overrightarrow{v_{i,j}}$s which are 12 bits in positions (63,62,61,59,58,57,55,54,53,51,50,49) of input of round 15 by encrypting $P_i$ with $\Delta K[i,j]$, $0 \leq j \leq 15$ and values of $\overleftarrow{v_{i,j}}$ which are 16 bits in positions (63,62,61,47,46,45,37, 36,35,15,14,13) of output of round 16 by decrypting each $S_j$s using $\Delta K[i,j], 0 \leq i \leq 15$.

So there are at most $2^4$ possible output values for $\overleftarrow{v_{i,j}}$. The possibility of a wrong key $K[i,j]$ matches in all 12 known bits of $\overleftarrow{v_{i,j}}$ is $24 \times 2^{-12} = 2^{-8}$. For a set of $2^8$ keys, we will have $2^{8-8} = 1$ candidate key in average. We have to test each candidate key by exhaustive search to filter out wrong keys.

*Data complexity*. According to Fig. 3, 42 bits of ciphertext are not important. So the data complexity will not exceed $2^{64-42} = 2^{22}$ chosen plaintexts. *Computational complexity*. In step 1, $24 \times (32+7) + 9 = 633$ S-boxes, in step 2, $24 \times (39 + 24(193)) = 50032$ S-boxes plus $24 \times (32 + 24(136)) = 35328$ S-boxes are computed. $24 \times (3+4) + 25 = 137$ S-boxes are computed in key schedule. Also there is 1 candidate key per each key set in average. The PRESENT-80 uses 527 S-boxes in a full round encryption, so the computational complexity is as follow:

$$C_{full} = 2^{72}\left(\frac{85360 + 633 + 137}{527} + 1\right) = 2^{79.365} \cong 2^{79.37}$$

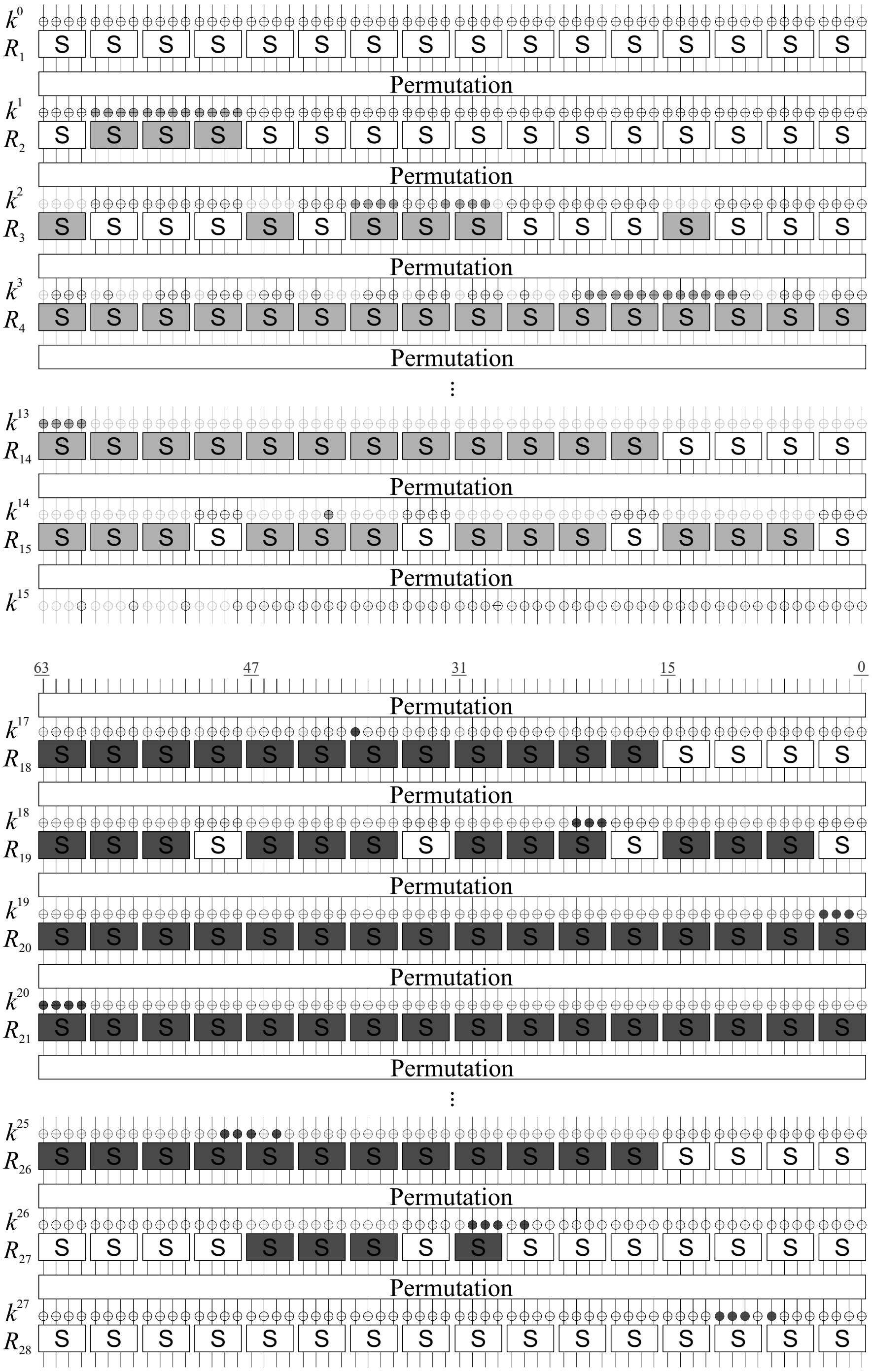

**Fig. 5** Matching over 28-rounds; up: Forward computation; down: Backward computation

The success probability of this attack is 100

## 6 CONCLUSION AND DISCUSSION

In this paper we presented the first independent biclique attack on full-round MIBS-80 and a new independent biclique attack on PRESENT-80. The attack on MIBS-80 uses matching without matrix method with biclique cryptanalysis for the first time, and results in reduction of the ciphers security about 1 bit. The attack on PRESENT-80 uses advantages of Sieve-In-The-Middle attack and results data and computational complexities better than other introduced attacks on full round PRESENT-80 so far.

## References

[1] M. Izadi, B. Sadeghiyan, S. Sadeghian, and H. Khanooki. Mibs: A new lightweight block cipher. In J.A. Garay, A. Miyaji, and A. Otsuka, editors, *CANS 2009. LNCS*, volume 5888, pages 334–348. Springer, Heidelberg, 2009.

[2] W. Wu and L. Zhang. Lblock: A lightweight block cipher. In J. Lopez and G Tsudik, editors, *ACNS 2011. LNCS*, volume 6517, pages 327–344. Springer, Heidelberg, 2011.

[3] 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. In P. Paillier and I Verbauwhede, editors, *CHES 2007. LNCS*, volume 4727, pages 450–466. Springer, Heidelberg, 2007.

[4] A. Bogdanov, D. Khovratovich, and C. Rechberger. Biclique cryptanalysis of the full aes. In D.H. Lee, editor, *ASIACRYPT 2011. LNCS*, volume 7073, pages 344–371. Springer, Heidelberg, 2011. Full paper is availavle at Cryptology ePrint Archive, Report 2011/449, http://eprint.iacr.org/2011/449.

[5] Hong D., Koo B., and Kwon D. Biclique attack on the full hight. In H. Kim, editor, *ICISC 2011. LNCS*, volume 7259, pages 365–374. Springer, Berlin, (2012), 2011.

[6] M. Shakiba, M. Dakhilalian, and H. Mala. Cryptanalysis of mcrypton-64. *International Journal of Communication Systems*, 2014. Published Online, DOI: 10.1002/dac.2721. John Wiley & Sons, Ltd (2014).

[7] Abed F., Forler C., List E., Lucks S., and Wenzel J. Biclique cryptanalysis of present, led, and klein. *Cryptology ePrint Archive: Report 2012/591. Revised version 2013*, 2012.

[8] S. Ahmadi, Z. Ahmadian, J. Mohajeri, and M.R. Aref. Low-data complexity biclique cryptanalysis of block ciphers with application to piccolo and hight. *IEEE Transactions on Information Forensics and Security*, 9(10):1641–1652, october 2014.

[9] Lee Ch. Biclique cryptanalysis of present-80 and present-128. *The Journal of Supercomputing*, 2012. . Published online, DOI: 10.1007/s11227-014-1103-3,Springer US.

[10] A. Canteaut, M. Naya-Plasencia, and B. Vayssire. Sieve-in-the-middle: Improved mitm attacks (full version). *Cryptology ePrint Archive, Report 2013/324 (2013), http://eprint.iacr.org/2013/324,* 2013.

[11] A. Bay, J. Huang, and S. Vaudenay. Improved linear cryptanalysis of reduced-round mibs. In M. Yoshida and K. Mouri, editors, *IWSEC 2014, LNCS*, volume 8639, pages 204–220. Springer International Publishing Switzerland, 2014.

[12] A. Bay, J. Nakahara Jr., and S. Vaudenay. Cryptanalysis of reduced-round mibs block cipher. In S. H. Heng, R.N. Wright, and B. M. Goi, editors, *CANS 2010. LNCS*, volume 4727, pages 450–466. Springer, Heidelberg, 2010.

[13] X. Ma, L. Hu, S. Sun, K. Qiao, and J. Shan. Tighter security bound of mibs block cipher against differential attack. In M.H. et al Au, editor, *NSS 2014, LNCS*, volume 8792, pages 518–525. Springer, 2014.

[14] Isobe T. and Shibutani K. Generic key recovery attack on feistel scheme. In K. Sako and P. Sarkar, editors, *ASIACRYPT 2013 Part I, LNCS*, volume 8269, pages 464–485. International Association for Cryptologic Research, 2013.