Tighter Security Bound of MIBS Block Cipher against Differential Attack

Xiaoshuang Ma[1,2], Lei Hu[1,2], Siwei Sun[1,2], Kexin Qiao[1,2], and Jinyong Shan[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] Data Assurance and Communication Security Research Center, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
{xshma13,hu,swsun,kxqiao13,jyshan12}@is.ac.cn

Abstract. Automatically calculating a lower bound of the number of differentially active S-boxes by mixed-integer linear programming (MILP) is a technique proposed by Mouha *et al.* in 2011 and it can significantly reduce the time spent on security evaluation of a cipher and decrease the possibility of human errors in cryptanalysis. In this paper, we apply the MILP method to analyze the security of MIBS, a lightweight block cipher proposed by Izadi *et al.* in 2009. By adding more constraints in the MILP problem, we get tighter lower bounds on the numbers of differentially active S-boxes in MIBS. We show that for MIBS, 18 rounds of iterations are sufficient to resist against single-key differential attack, and 39 rounds are secure against related-key differential cryptanalysis.

Keywords: MIBS block cipher, Differential attack, Active S-box, Mixed-Integer Linear Programming.

1 Introduction

Differential cryptanalysis was first proposed by Biham and Shamir in [3] and is one of the most powerful attacks on block ciphers. Differential cryptanalysis analyzes differential propagation patterns of a cipher to discover its non-random behaviors, and uses these behaviors to build a distinguisher or recover the key. Since the effectivity of differential attack heavily depends on an upper bound of the probabilities of differential propagation patterns which can be found by an attacker and the probability of a differential propagation pattern is characterized in terms of the number of active S-boxes involved, a practical approach to evaluate the security of a block cipher against differential attack is to determine the minimum number of active S-boxes under the differential propagation model.

In [11], Mouha *et al.* proposed an automatic method based on Mixed-Integer Linear Programming (MILP) for counting the minimum number of active S-boxes for some word-oriented symmetric-key ciphers, and used it to analyze the stream cipher Enocoro-128v2 [16].One significant advantage of the MILP based technique is that it can be applied to a wide variety of symmetric-key cipher

M.H. Au et al. (Eds.): NSS 2014, LNCS 8792, pp. 518–525, 2014.

constructions, which is composed of a combination of S-box operation, linear permutation layers and/or exclusive-or (XOR) operations, and less programming effort is needed with this technique compared with previous works which focus on automatically calculating a lower bound of the number of active S-boxes [6,4,5,9,13].

However, Mouha *et al.* 's method can not be applied directly to bit-oriented block ciphers. Sun *et al.* [14] extended this method applicable to symmetric-key ciphers involving bit-oriented operations by introducing new representations for XOR differences to describe bit/word level differences simultaneously and by taking the collaborative diffusion effect of S-boxes and bitwise permutations into account. In [15], Sun *et al.* gave a bound on the probability of the best related-key differential characteristic of the full-round LBlock block cipher by adding constraints of conditional differential propagation and constraints selected from the H-Representation of the convex hull of all differential patterns of the S-boxes. Very recently, Qiao *et al.* [10] refined the constraints about the XOR operation to avoid invalid characteristics due to a wider feasible region caused by inaccurate constraints of XOR operation, and achieved a tighter security bound of FOX.

In this paper, we apply the MILP based methods presented in [11,14,15] to MIBS [8], which is a lightweight 32-round lightweight block cipher. We get tighter lower bounds on the numbers of differentially active S-boxes for 2- to 7-round MIBS against both single-key and related-key differential attack. We prove that the 18-round MIBS is sufficiently secure against single-key differential attack, and for related-key differential attack we give an estimation of the security of the cipher against related-key differential attack and show the 39-round MIBS can resist against related-key differential cryptanalysis.

Organization of the Paper. In Section 2, we introduce the MIBS block cipher. In Section 3 we briefly describe the existing MILP techniques, and then we apply these methods to MIBS and present the results in Section 4. Finally we conclude the paper in Section 5.

2 The MIBS Block Cipher

2.1 Description of MIBS

In this section, we recall the design of MIBS and we refer the reader to [8] for more detailed description.

The MIBS block cipher, proposed by Izadi *et al.* [8] in 2009, is a lightweight 64-bit block cipher suitable for resource-constrained devices. MIBS is a Feistel cipher with 32 rounds of iterations and the block length is 64-bit, while two key lengths of 64-bit and 80-bit are supported.

The round function of MIBS is demonstrated in Fig. 1. It transforms the input block of the i-th round, $(L_{i-1}, R_{i-1}) \in \{0,1\}^{32} \times \{0,1\}^{32}$, to the output block $(R_{i-1} \oplus F(K_i, L_{i-1}), L_{i-1})$. The F-function of MIBS has an SPN structure which consists of four stages: an xor layer with a round subkey, a non-linear substitution layer of 4×4-bit S-boxes, a linear mixing layer with branch number 5, and a

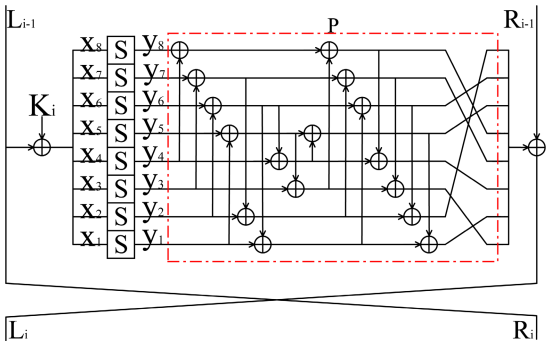

Fig. 1. The round function of MIBS

nibble-wise linear permutation. The operations in MIBS are all nibble-wise.The key schedule of MIBS is adapted from the key schedule of the PRESENT block cipher.

2.2 Known Cryptanalysis on MIBS

The designers of MIBS analyzed the security of MIBS against various attacks including linear cryptanalysis, differential cryptanalysis, algebraic attack and related key attack [8]. They showed MIBS is secure against differential and linear cryptanalysis.

In 2010, Bay *et al.* [1] presented multiple linear attack, linear attack, differential attack, and impossible-differential cryptanalysis on MIBS, which can attack the 17-round, 18-round, 14-round and 12-round MIBS, respectively.

3 MILP Based Methods

In [11], Mouha *et al.* presented a method based on MILP for counting the minimum number of active S-boxes for some word-oriented symmetric-key ciphers. Sun *et al.* extended Mouha *et al.* 's framework to be suitable for bit-level symmetric-key ciphers by imposing constraints describing S-box layers and adding constraints for conditional propagation and constraints selected from the H-Representation of the convex hull of all the differential pattern of the S-boxes [14,15].In the following description, the difference's value is denoted "1" if the difference is nonzero and "0" otherwise, for bit-level symmetric-key cipher.

Suppose a bit-oriented block cipher is composed of the following three operations:

1) XOR operation $\oplus$: $\mathbb{F}_2^\omega \times \mathbb{F}_2^\omega \to \mathbb{F}_2^\omega$;
2) S-box substitution $\mathcal{S}$: $\mathbb{F}_2^\omega \to \mathbb{F}_2^\omega$;and
3) Bit permutation P: $\mathbb{F}_{2^\omega}^m \to \mathbb{F}_{2^\omega}^m$

where m is the word size, ω is the input and output bit length of the S-box.

Constraints Induced by the XOR Operation. Let $x_{in_1}, x_{in_2}, \cdots, x_{in_l} \in \mathbb{F}_2$ be the input differences of the combination of $l-1$ XOR operations, and $x_{out} \in$

$\mathbb{F}_2^\omega$ be the corresponding output difference. Then the following inequalities give the bit-oriented constraints of the XOR operation:

$$\begin{cases} x_{in_1} + x_{in_2} + \cdots + x_{in_l} - x_{out} - 2d_\oplus = 0, \\ d_\oplus \geq 0, \\ d_\oplus \leq \lfloor l/2 \rfloor, \end{cases} \tag{1}$$

where $d_\oplus$ is a dummy variable taking values in integers.

Constraints Induced by the S-box Operation. Introduce a new binary variable A_t to represent the S-box, where the value of A_t is 0 iff all input bit differences are 0 and $A_t = 1$ as long as there is at least one non-zero input bit difference. Suppose $(x_{in_0}, x_{in_1}, \cdots, x_{in_{\omega-1}})$ and $(x_{out_0}, x_{out_1}, \cdots, x_{out_{\omega-1}})$ are the input and output bit-level differences of an S-box marked by A_t. Then the following equations give the constraints of the value of A_t:

$$\begin{cases} A_t - x_{in_i} \geq 0, i \in \{0, 1, \cdots, \omega - 1\}, \\ x_{in_0} + x_{in_1} + \cdots + x_{in_{\omega-1}} - A_t \geq 0. \end{cases} \tag{2}$$

H-Reptesentation of the Convex Hull. The convex hull of a set X of discrete points in the Euclidean space is the smallest convex set that contains X. Let the convex hull of a specific $\omega \times \omega$ S-box be the convex hull $\mathcal{V}_\mathcal{S} \subseteq \mathbb{R}^{2\omega}$ of all possible differential patterns of the S-box. Now we can describe the convex hull as the common solutions of a set of finitely many linear equations and inequalities as follows:

$$\begin{cases} \alpha_{0,0}x_{in_0} + \cdots + \alpha_{0,\omega-1}x_{in_{\omega-1}} + \alpha_{0,\omega}x_{out_0} + \cdots + \alpha_{0,2\omega-1}x_{out_{\omega-1}} + \alpha_{0,n} \geq 0, \\ \quad \cdots \\ \beta_{0,0}x_{in_0} + \cdots + \beta_{0,\omega-1}x_{in_{\omega-1}} + \beta_{0,\omega}x_{out_0} + \cdots + \beta_{0,2\omega-1}x_{out_{\omega-1}} + \beta_{0,n} = 0, \\ \quad \cdots \end{cases} \tag{3}$$

In computational geometry, a number of algorithms are known for computing the convex hull for a finite set of points. However, there are a considerable number of equations and inequalities in the H-Representation of a convex hull. It is impractical to add all of them to an MILP problem for counting the number of active S-boxes. Sun *et al.* [14,15] proposed a greedy algorithm to select constraints from the H-Representation of the convex hull of all the differential pattern computed for the S-box. Moreover, these equations give the constraints that nonzero input difference must result in nonzero output difference and vice versa.

Further details on the word-level and bit-level MILP method for calculating the number of active S-boxes can be found in [11] and [14,15] respectively.

4 Application to the MIBS Block Cipher

In this section, we apply the MILP based methods presented in previous section to the lightweight block cipher MIBS, in both single-key and related-key models respectively.

4.1 Results on MIBS in the Single-key Model

We develop a C++ program to generate the MILP instances for MIBS in the "lp" format [7]. For single-key differential attack on MIBS, the objective function of the MILP problem is the sum of all variables representing the S-boxes, with the constraint that there is at least one active S-box to avoid the trivial case that all variables are zero. Then we call the Gurobi 5. 6 optimizer [12] to solve the MILP instances. By default we run Gurobi 5. 6 on a PC using 4 threads with Intel(R) Core(TM) Quad CPU (3. 40GHz, 8. 00GB RAM, Windows 7).

Table 1. Results for MIBS in the single-key model

Rounds	Nibble-wise			Bit-oriented			
	# Var.	# Con.	# Active S-boxes	# Var.	# Con.	# Active S-boxes	Time(s)
2	96	201	1	432	1073	1	0.02
3	152	305	2	664	1609	2	0.24
4	208	409	6	896	2145	6	34.42
5	264	513	8	1128	2681	9	753.24
6	320	617	9	1360	3217	11	10776.15
7	376	721	11	1592	3753	-	-

The lower bounds of the number of active S-boxes for a round-reduced MIBS in the single-key model are presented in Table 1.

However, some of the feasible solutions of the MILP model got from the Gurobi optimizer turn out to be invalid differential paths. For instance, one of the differential path of 6-round MIBS satisfies the above constraints is shown in Fig. 2. According to the difference distribution table of the MIBS S-box shown in [1], the S-boxes marked by slash notation are invalid differential propagation pattern for MIBS S-boxes. To avoid this situation, we apply a method proposed by Sun *et al.* [15] in 2013. By adding constraints selected from the H-Representation of the convex hull of all the differential pattern of the MIBS S-boxes, we have tightened the feasible region of the MILP model.

According to the greedy algorithm described in [15], we pick 27 inequalities out of the whole 378 constraints of the convex hull of MIBS S-box, which are shown in Appendix A . The results obtained with the inequalities selected from the H-Representation of the convex hull are summarized in Table 2.

In [9] Kanda *et al.* showed the minimum number $D^{(4r)}$of active S-boxes in differential attack for a $(4r)$-round Feistel ciphers with SPN round function satisfies $D^{(4r)} \geq r \times B_d + \lfloor r/2 \rfloor$, where $B_d = 5$ is the differential branch number of the linear transformation for MIBS. Moreover, it is clearly shown in the difference distribution table of the MIBS S-box in [1] that the maximum differential probability for any differential propagation across this S-box is 2^{-2}. So, the designers claims that a lower bound of the number of active S-boxes with respect to differential cryptanalysis on the fully 32-round MIBS is $D^{(32)} \geq 8 \times 5 + \lfloor 8/2 \rfloor = 44$.

From Tables 1 and 2, we have learnt that the 5-round and 6-round MIBS in single-key model has at least 9, and 11 active S-boxes respectively. From the

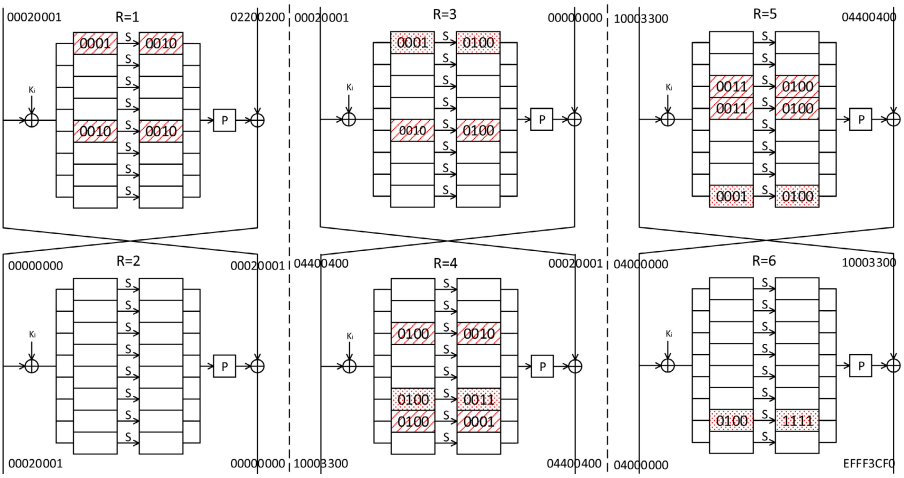

Fig. 2. The feasible solution of the 6-round MIBS MILP model got from the Gurobi optimizer. The blank boxes denote the zero differences, the boxes marked by dot notation denote the valid differences, and those with slash notation denote the invalid differences according to the difference distribution table in [1].

result the number of active S-boxes of fully 32-round MIBS is lower bounded by $4 \times 9 + 2 \times 11 = 58$, which is tighter than 44 given by the designers. Therefore, the upper bound of the maximum differential probability of the full-round MIBS is $(2^{-2})^{58} = 2^{-116}$, which is much lower than the probability of success of the brute force attack. We can conclude that the full-round MIBS is resistant to single-key differential attack. Since a lower bound of the active S-boxes of the 18-round MIBS is $3 \times 11 = 33 > 32$, it is clearly that for MIBS, 18 rounds of iterations are sufficient to resist against single-key differential attack.

4.2 Results on MIBS in the Related-key Model

Related-key attack [2] is a type of cryptanalysis which uses some weakness of the key schedule. In this section, we apply the MILP based methods to MIBS in related-key model.

For related-key differential attack, we add an extra constraint to ensure that there is a difference between the related-keys. Let $(k_1, k_2, \cdots, k_n)$ be the bit difference of the related subkeys, we require a constraint that $k_1 + k_2 + \cdots + k_n \geq 1$.

We denote the 64-bit user key version of MIBS as MIBS-64. The results obtained for a round-reduced MIBS-64 in the related-key model are presented in Table 2. In particular, we have proved that there are at least 7 active S-boxes in the best related-key differential characteristic for any consecutive 8-rounds of MIBS-64. Therefore, the probability of the best related-key differential characteristic of the 32-round MIBS-64 is $((2^{-2})^7)^4 = 2^{-56}$. This is slightly larger than the probability of success for an exhaustive search attack. Since the probability of the best related-key differential characteristic for 7-round MIBS-64

Table 2. Results for MIBS-64 with convex hull

Rounds	single-key model				related-key model			
	# Var.	# Con.	# A-S	Time(s)	# Var.	# Con.	# A-S	Time(s)
2	432	1505	1	0. 05	570	1893	0	0.03
3	664	2257	2	0. 20	839	2839	0	0.03
4	896	3009	6	91. 07	1108	3785	0	0.08
5	1128	3761	9	7601. 49	1377	4731	1	12.58
6	1360	4513	11	262080.50	1646	5677	3	31.61
7	1592	5265	-	-	1915	6623	5	4843.43

is upper bounded by $(2^{-2})^5$, the probability of the best related-key differential characteristic for the $39(= 8 \times 4 + 7)$-round MIBS-64 is upper bounded by $((2^{-2})^7)^4 \times (2^{-2})^5 = 2^{-66}$. Thus, we prove that for MIBS-64, 39 rounds of iterations are sufficient to resist differential attack in related-key model.

5 Conclusion

In this paper, we have applied Mohua *et al.* 's and Sun *et al.* 's methods to the 32-round block cipher MIBS and obtained tighter upper bounds on the probability of best differential characteristics of MIBS in both the single-key and related-key differential attacks. We have shown that 18 rounds of iterations of MIBS are sufficient to resist against single-key differential attack and 39 rounds of iterations are sufficient to resist against related-key differential cryptanalysis for MIBS with 64-bit keys. Our work is expected to be applicable to other block ciphers with more complex diffusion layers.

Acknowledgements. The authors would like to thank anonymous reviewers for their helpful comments and suggestions. The work of this paper was supported by the National Key Basic Research Program of China (2013CB834203), the National Natural Science Foundation of China (Grant 61070172), the Strategic Priority Research Program of Chinese Academy of Sciences under Grant XDA06010702, and the State Key Laboratory of Information Security, Chinese Academy of Sciences.

References

1. Bay, A., Nakahara Jr., J., Vaudenay, S.: Cryptanalysis of reduced-round MIBS block cipher. In: Heng, S.-H., Wright, R.N., Goi, B.-M. (eds.) CANS 2010. LNCS, vol. 6467, pp. 1–19. Springer, Heidelberg (2010)
2. Biham, E.: New types of cryptanalytic attacks using related keys. Journal of Cryptology 7(4), 229–246 (1994)

3. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4(1), 3–72 (1991)
4. Bogdanov, A.: Analysis and Design of Block Cipher Constructions. Ruhr University Bochum (2010)
5. Bogdanov, A.: On unbalanced Feistel networks with contracting MDS diffusion. Designs, Codes and Cryptography 59(1-3), 35–58 (2011)
6. Daemen, J., Rijmen, V.: The wide trail design strategy. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001)
7. IBMsoftware-group: User-manual cplex 12 (2011), `http://www-01.ibm.com`
8. Izadi, M., Sadeghiyan, B., Sadeghian, S.S., Khanooki, H.A.: MIBS: A new lightweight block cipher. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS 2009. LNCS, vol. 5888, pp. 334–348. Springer, Heidelberg (2009)
9. Kanda, M.: Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 324–338. Springer, Heidelberg (2001)
10. Kexin, Q., Lei, H., Siwei, S., Xiaoshuang, M.: Improved MILP Modeling for Automatic Security Evaluation and Application to FOX (2014)
11. Mouha, N., Wang, Q., Gu, D., Preneel, B.: Differential and linear cryptanalysis using Mixed-Integer linear programming. In: Wu, C.-K., Yung, M., Lin, D. (eds.) Inscrypt 2011. LNCS, vol. 7537, pp. 57–76. Springer, Heidelberg (2012)
12. Optimization-Gurobi: Gurobi optimizer reference manual (2012), `http://www.gurobi.com`
13. Shibutani, K.: On the diffusion of generalized Feistel structures regarding differential and linear cryptanalysis. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, pp. 211–228. Springer, Heidelberg (2011)
14. Sun, S., Hu, L., Song, L., Xie, Y., Wang, P.: Automatic security evaluation of block ciphers with S-bP structures against related-key differential attacks. In: Inscrypt 2013 (2013)
15. Sun, S., Hu, L., Wang, P.: Automatic security evaluation for bit-oriented block ciphers in related-key model: Application to PRESENT-80, LBlock and others. Cryptology ePrint Archive (2013), `http://eprint.iacr.org/2013/676`
16. Watanabe, D., Okamoto, K., Kaneko, T.: A hardware-oriented light weight pseudorandom number generator enocoro-128v2. In: The Symposium on Cryptography and Information Security, pp. 3D1–3 (2010)

A The Convex Hull of the MIBS S-box

According to the greedy algorithm in [15], we pick 27 inequalities out of the whole 378 constraints of the convex hull of the MIBS S-box, which are given below. For instance, the vector $(-3,-3,1,-2,1,-2,1,2,7)$ denotes the inequality

$$-3x_{in_0} - 3x_{in_1} + x_{in_2} - 2x_{in_3} + x_{out_0} - 2x_{out_1} + x_{out_2} - 2x_{out_3} + 7 \geq 0,$$

where $(x_{in_0}, \cdots, x_{in_3})$ and $(x_{out_0}, \cdots, x_{out_3})$ are the input and output bit-level differences of the MIBS S-box. According to the greedy algorithm in [15], we pick 27 inequalities out of the whole 378 constraints, which are marked by $*$.

```
(-3,-3, 1,-2, 1,-2, 1, 2, 7)    (-2,-1,-2, 1, 2, 2,-1, 1, 4)    (-2, 1,-3,-1,-1,-3,-2,-2,11)  (-2, 1,-1, 2,-2, 1,-1,-1, 5)
(-2, 1, 1,-1,-1,-1,-1,-1, 2, 4)  (-2, 2, 4, 1, 3, 1,-3,-3, 4)    (-1,-4, 3, 2,-1,-3, 4, 2, 5)     (-1,-2,-4, 4,-4, 2, 1,-3,10)
(-1,-1,-1,-1, 3, 3, 3, 3, 0)    (-1,-1, 1,-1,-1, 0,-1,-1, 5)  (-1, 0, 0,-1,-1,-1, 1, 1, 3)     (-1, 2,-1,-1,-1, 1, 2,-2, 4)
(-1, 2,-1, 1, 2,-2, 1,-1, 3)    (-1, 2, 2,-2, 1, 0,-2, 1, 3)    ( 0,-1, 0,-1, 1,-1,-1, 1, 3)     ( 0,-1, 1,-1, 1,-1, 1,-1, 3)
( 1,-2,-2,-1, 1,-2,-2, 0, 7)    ( 1,-2,-2, 2, 1, 1,-1,-2, 5)    ( 1,-1,-2,-2,-1,-1,-1,-1, 7)  ( 1,-1, 2, 1,-1, 1,-2, 1, 2)
( 1, 1,-2,-1,-2,-1,-2, 1, 6)    ( 1, 2, 1, 2,-2, 1, 1, 1, 0)    ( 1, 3,-2,-3, 1, 3, 2,-1, 3)     ( 2,-3, 1, 1, 3, 2, 2, 1, 0)
( 2, 1,-2, 2, 3,-1, 1, 2, 0)    ( 3,-2, 1,-2,-3, 3,-1, 1, 5)    ( 5, 4, 4, 3,-1,-2, 1,-2, 0)
```