Review Article
Open Access
CrossMark

Biclique cryptanalysis of full round PRESENT with reduced data complexity

Abstract

Biclique cryptanalysis is a generic attack on block cipher to recovering the secret key faster than brute force. In this paper we use asymmetric independent biclique attack on full round PRESENT. The data complexities of our attacks are less than before, which for a full round attack on PRESENT-80 and PRESENT-128 are 2^{17} plain text-ciphertext pairs. The computational complexity is slightly improved.

Keywords: PRESENT, Lightweight block cipher, asymmetric independent biclique, key recovery

Volume 2 Issue 2 - 2018

M Hadian Dehkordi, Roghayeh Taghizadeh
Iran University of Science and Technology (IUST), Iran

Correspondence: M Hadian Dehkordi, Iran University of Science and Technology (IUST), Iran, Email mhadian@iust.ac.ir

Received: February 25, 2018 | **Published:** September 26, 2018

Introduction

Biclique cryptanalysis, introduced first in 2011[1] for hash cryptanalysis. After that, Bogdanove in[2] used this technique and introduced the first biclique attack on full round AES. We can see lots of cryptanalysis results on the other block cipher, such as IDEA, Piccolo, LBlock, SQUARE, KLINE, ARIA, TWINE and HIGHT where proposed.[3–10]

Biclique attack is a kind of meet in the middle (MITM) attack that is improved for cryptanalysis block cipher to find the unknown secret key.In a biclique attack; first, all possible secret keys are partitioned into a set of groups of keys. For each group of keys, a bipartite graph is constructed. After that, a partial matching is used to filter the wrong key and get the candidate key for the correct keys .Finally, the valid pair (p,c) is used to get the correct key.

PRESENT has a simple structure and belong to a family of light weight 64-bit block cipher proposed in 2007.[11] It supports two key sizes of 80 and 128 bits and denoted by PRESENT-80 and PRESENT-128. A number of biclique attacks on full round PRESENT have been published in.[12–14] In this paper, we use an asymmetric independent biclique attack on full round PRESENT to reduce the data complexity. The data complexity for a full round attack on PRESENT-80 and PRESENT-128 are 2^{17} plaintext-ciphertext pairs. By minimizing the number of active sboxes, the computational complexity is slightly improved. A summary of previous works and our result is given in Table 1.

Table 1 Summary of biclique cryptanalytic results on PRESENT

Version	Round	Computation	Data	Reference
PRESENT-80	full	279.76	223	15
	full	279.49	225	16
	full	279.86	223	17
	full	279.64	217	This attack
PRESENT-128	full	2127.81	219	15
	full	2127.32	223	16
	full	2127.91	219	17
	full	2127.5	217	This attack

Outline: First in section 2, the structure of PRESENT is described.We overview biclique cryptanalysis in section3.

Section 4 contains a detailed description of our attack and compute complexity.

Finally, we conclude our work in section 5.

Description of PRESENT

PRESENT is a 64-bit lightweight cipher that consists of 31 rounds with 80 or 128 bits secret key. After the final round, the state is added to XORed with round key to generate the ciphertext. Both versions of PRESENT, have the same structure as shown in Figure 1. But the key schedule is slightly different. See[11]for detail description of round function. The key schedule expands a secret key 80 or 128 bits to 32 round keys RK^r, $r = 0,...,31$ with 64 bits each. In PRESENT-80, the 80 bits secret key $K=(k_{79},...,k_0)$, is stored in 80 bits register $SK=(sk_{79},...,sk_0)$ with $sk_i = k_i$. After that, SK is updated as follow:

$$(sk_{79},...,sk_0) = (sk_{18}, ...,sk_0,sk_{79},...,sk_{19})$$

$$(sk_{79},sk_{78},sk_{77},sk_{76}) = sbox(sk_{79},sk_{78},sk_{77},sk_{76})$$

$$(sk_{19},sk_{18},sk_{17},sk_{16},sk_{15}) = (sk_{19},sk_{18},sk_{17},sk_{16},sk_{15}) \oplus (r+1).$$

The 64 leftmost bits of SK selected as 64 bits round keys RK^r, for PRESENT-80. The above procedure is repeated until all round keys are constructed. The key schedule of PRESENT-128 is similar and is as follow

$$(sk_{127},...,sk_0) = (sk_{66},...,sk_0,sk_{127},...,sk_{67})$$

$$(sk_{123},sk_{122},sk_{121},sk_{120}) = sbox(sk_{123},sk_{122},sk_{121},sk_{120})$$

$$(sk_{127},sk_{126},sk_{125},sk_{124}) = sbox(sk_{127},sk_{126},sk_{125},sk_{124})$$

$$(sk_{66},sk_{65},sk_{64},sk_{63},sk_{62}) = (sk_{66},sk_{65},sk_{64},sk_{63},sk_{62}) \oplus (r+1)$$

The above procedure is repeated, and 64 bits round keys RK^r, for PRESENT-128 are constructed as 64 leftmost bits of S^K.

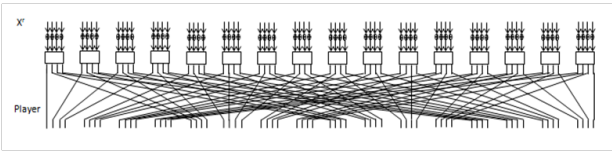

Figure 1 round function of Present.

Biclique cryptanalysis

In this section, we give a brief overview on biclique cryptanalysis. See[2] for complete detail of this. In a biclique attack, the biclique can be constructed in plaintext or ciphertext side. Here, we construct a biclique in ciphertext side so the attack is a chosen ciphertext attack, and we need the decryption oracle (for the biclique in plaintext side, the attack is a chosen plaintext attack, and we need the encryption oracle).[15–18]

(d_1, d2) -dimensional asymmetric biclique: let f be subciher of cipher E that maps an intermediate state S to the ciphertext $C, f_k(S) = C$. The 3 - tuple $\left\{\{c_i\},\{s_j\},\{K[i,j]\}\right\}$ is called a $(d1, d2)$ -dimensional asymmetric biclique if for all $i = 0,1,...,2^{d1}-1$ and $j = 0,1,...,2^{d2}-1$, $s_j = f^{-1}_{K[i,j]}(c_i)$. The structure (d_1, d2) -dimensional asymmetric biclique is shown in Figure 2.

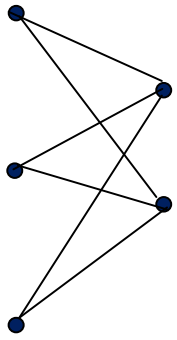

Figure 2 (d_1, d_2) dimensional asymmetric biclique in the ciphertext side.

The four main steps of the biclique attack are:

Key partitioning: An adversary chooses a partition of the key space into groups of key of cardinality $2^{(d1+d2)}$ each. A key in a group is indexed as an element of $2^{d1}\times 2^{d2}$ matrixes $K[i,j]$.

Constructing a biclique: Independent biclique is an efficient tool for making a biclique. The procedure of constructing the biclique is as follow:

1. Choose a random ciphertext c_0 and compute s_0 as $s_0 = f^{-1}_{k[0,0]}(c_0)$.
2. Compute s_i as $s_i = f^{-1}_{k[i,0]}(c_0)$ for $i = 1,...,2^{d2}-1$.
3. Compute c_j as $c_j = f_{k[0,j]}(s_0)$ for $j = 1,...,2^{d1}-1$.

Partial matching: Partial matching is an efficient way that all keys in a group are tested. By using this method the computational complexity is reduced significantly. Since the biclique is constructed in the ciphertext side, partial matching is performed at the plaintext side. The remaining parts of cipher E are split into the subcipher g_1 and g_2 , $E = g_1 0 g_2 0 f$. We choose the matching variable v after subcipher before g_1 subcipher g_2 The value of matching variable v is calculated in both directions to find the correct key. First, we called on the decryption oracle to obtain plaintext p_j , $j = 0,1,...,2^{d1}-1$. In forward direction, p_j is partially encrypted under key $k[0,j]$ to get $v(0,j)$, $j = 0,1,...,2^{d1}-1$ and stored 2^{d1} values. After that, in backward direction, s_i is partially decrypted under key $k[i,0]$ to get $v(0,j)$, $i = 0,1,...,2^{d2}-1$ and store 2^{d2} values. For checking the matching, $v(i,j) = v(i,j)$, we recomputed only those parts that differ from the stored values. Note that by using partial matching, we can reduce the computational complexity significantly.

Rechecking the candidate keys: Since some candidate keys remain in each group of keys, to filter the wrong keys, the valid pair (p,c) is used to get the correct key. The structure of (d_1, d_2) -dimensional asymmetric biclique cryptanalysis is shown in Figure 3.

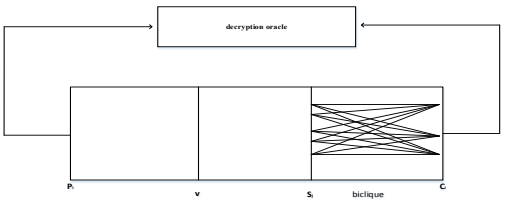

Figure 3 Representation of $(d1, d2)$ -dimensional asymmetric biclique cryptanalysis.

Independent asymmetric biclique attack on full round PRESENT-80

In this section, we first construct a $(1,3)$ -dimension asymmetric biclique on the ciphertext side for round 29-31 of PRESENT-80. The partial secret key used in RK^{28}, RK^{29}, RK^{30} and RK^{31} are as fallow

$$RK^{28} : (k_{51,...,} k_0, k_{79}, ..., k_{68})$$

$$RK^{29} : (k_{70,} k_{69,...,} k_7).$$

$$RK^{30} : (k_9, ..., k_0, k_{79}, ..., k_{26})$$

$$RK^{31} : (k_{28}, ..., k_0, k_{79}, ..., k_{45}).$$

The attack consist of four steps:

Key partitioning: The 80 bits key space is partitioned into 2^{76} groups of 2^4 keys each. The base keys $K[0,0]$ take all 80 bits of the secret key with 4 bits fixed to zero and the remaining 76 bits take all possible values. In our attack, the differences Δ_i^k are chosen by varying k_{52} in forward direction, and the key differences ∇_j^k are chosen by varying (k_{36}, k_{35}, k_{34}) in backward direction.

Constructing a biclique: We use these steps to construct a biclique for each group of keys in the ciphertext side. Let f be subcipher for round 29-31 of PRESENT-80.

Step1. Fix $c_0 = 0$ and compute $s_0 = f^{-1}_{k[0,0]}(c_0)$

Step2. Decrypt c_0 under different keys $K[i,0]$ to get corresponding states, s_i $i = 1,2,3$ .The active sboxes are visualized by the blue trail in backward direction in Figure 4. These sboxes should be calculated 2^3 times, while the other ones are computed only once; already done in step1.

Step3. Encrypt s_0 under key $K[0,1]$ to get the corresponding state c_1. The active sboxes are visualized by the red trail in forward direction in Figure 5. These sboxes should be calculated 2 times, while the other ones have already been computed.

Citation: Dehkordi MH, Taghizadeh R. Biclique cryptanalysis of full round PRESENT with reduced data complexity. *Electric Electron Tech Open Acc J.* 2018;2(2):251–255. DOI: 10.15406/eetoaj.2018.02.00021

Matching: We use partial matching by applying matching with precomputation and recomputation over the remaining round of the cipher to filter the wrong key. Let g_1 and g_2 be subciphers for rounds 1-15 and rounds 16-28 respectively. We take matching variable v in the bits $v_{63},...,v_{60}$ of the state $v(v_{63},...,v_0)$ after round 15. Then we detect the right key by computing v in both directions. The correct key is the one that meets in both directions.

Complexity

The cost of a biclique is dominated by the number of sboxes to be calculated, so we count the number of sbox operations in the round transformation and key schedule. Each round of PRESENT-80 together with one round of key schedule takes 17 sbox computations, so the complexity of single encryption equals calculation of $31\times17=527$ sboxes.

Biclique complexity: For each 2^{76} groups of keys, the following computations should be calculated.

Forward direction complexity: In forward direction, 5 sboxes should be calculated 2 times. The active sboxes are visualized by the red trail in forward direction in Figure 4.

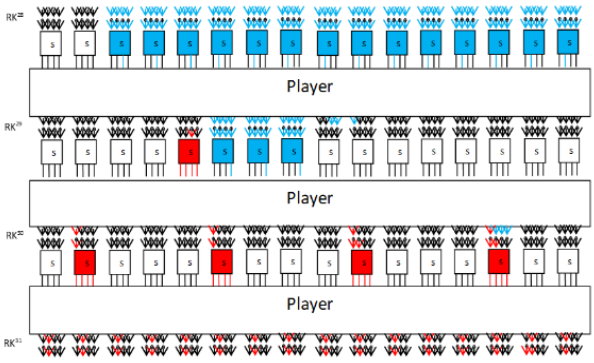

Figure 4 3-round (1,3)-asymmetric biclique for Present-80.

Backward direction complexity: In backward direction, 17 sboxes should be calculated2^3=8 times. The active sboxes are visualized by the blue trail in backward direction in Figure 4.The remaining 26 sboxes are calculated once. In total, $5\times2+17\times18+26=162$ sboxes should be calculated to construct a biclique.

Matching complexity: For each2^{76} groups of keys the following computations should be calculated.

Forward direction complexity: In forward direction, $2+5+12\times16+4=203$ sboxes in round transformation and 2 sboxes in key schedule should be calculated 2^3 times, and 25 sboxes are calculated only once. The active sboxes are visualized by the blue trail in forward direction in Figure 5. Note that 12 sboxes in round 15 need not to be computated. This procedure is repeated 2 times for all p_i 's, so in forward direction, $2\times\left(2^3\times205+25\right)=330$ sboxes should be calculated.

Backward direction complexity: In backward direction, 42 sboxes are calculated once, and $1+5+8\times16+4+1=139$ sboxes in round transformation and one sbox in key schedule should be calculated 2 times. The active sboxes are visualized by the red trail in backward direction in Figure 5. This procedure is repeated 2^3 for all s_j's, so in backward direction, $2^3\times\left(2\times140+42\right)=2576$ sboxes should be calculated.

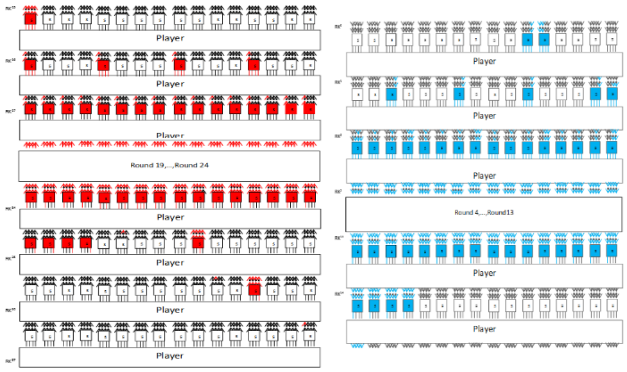

Figure 5 Recompilation in forward and backward direction for Present-80.

Rechecking the candidate keys complexity: Since in each group, 2^4 keys should be checked and the probability of matching is 2^{-4}, so $2^4\times2^{-4}=1$ remaining key candidate should be tested to get the correct key.

In total, the computational complexity of our attack is given by:

$$2^{76}\left(\frac{162+3330+2756}{527}+1\right)=2^{79.64}$$

Data complexity: We need at most 2^{17} chosen ciphertexts for performing a biclique attack.

Independent asymmetric biclique attack on full round PRESENT-128: In this section, we describe our attack on PRESENT-128. Since a biclique attack on full round PRESENT-128 is similar to PRESENT-80, we only state our results.

The partial keys used in RK^{27}, RK^{28}, RK^{29}, RK^{30} and RK^{31} are as fallow:

$$RK^{27}: \left(k_{16},...,k_0,k_{127},...,k_{81}\right)$$
$$RK^{28}: \left(k_{83},...,k_{20}\right)$$
$$RK^{29}\left(k_{22},...,k_0,k_{127},...,k_{87}\right)$$
$$RK^{30}: \left(k_{89},...,k_{26}\right)$$
$$RK^{31}: \left(k_{28},...,k_0,k_{127},...k_{93}\right)$$

We construct (1, 3)-dimensional asymmetric biclique on the ciphertext side for round 27-31. The key differences

Δ_i^k are chosen by varying k_{19} in forward direction and the key differences ∇_j^k are chosen by varying $\left(k_{92},k_{91},k_{90}\right)$ in backward direction. The biclique construction is illustrated in Figure 6. Here, f, g_1 and g_2 are subciphers for rounds 28-31, rounds 1-14 and rounds 15-27 respectively. As we see, the Δ_i^k affects only 17 bits of ciphertext, and since we use the same value for c_0 in each biclique, the data complexity does not exceed 2^{17}. We take matching variable v; the least significant 4 bits of the output value after round 14 as shown in Figure 7.

Citation: Dehkordi MH, Taghizadeh R. Biclique cryptanalysis of full round PRESENT with reduced data complexity. *Electric Electron Tech Open Acc J.* 2018;2(2):251–255. DOI: 10.15406/eetoaj.2018.02.00021

Figure 6 4-round (1,3)-asymmetric biclique for Present-128.

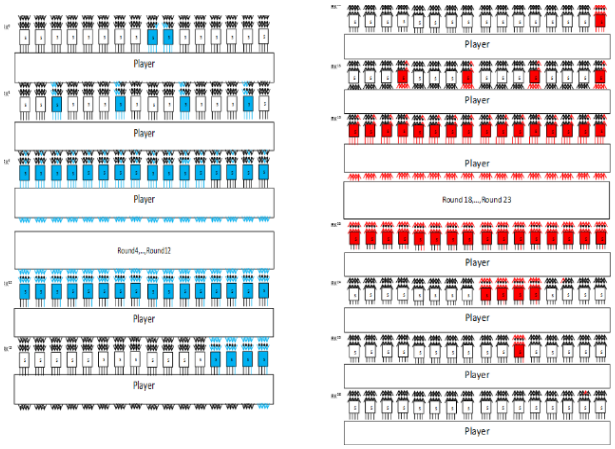

Figure 7 Recompilation in forward and backward direction for Present-128.

Complexity

Each round of PRESENT-128 together with one round of key schedule takes 18 sbox computations, so the complexity of single encryption equals calculation of $31 \times 18 = 558$ sboxes. The complexity of our attack is given by:

Biclique complexity: In forward direction, 5 sboxes in round transformation and one sbox in key schedule should be calculated 2 times. The active sboxes are visualized by the red trail in forward direction in Figure 6. In backward direction, 15 sboxes should be calculated 2^3=8 times. The active sboxes are visualized by the blue trail in backward direction in Figure 6. The remaining 44 sboxes are calculated once. In total $6 \times 2 + 15 \times 8 + 44 = 176$ sboxes should be calculated to construct a biclique.

Matching complexity: In forward direction, $2 + 4 + 11 \times 16 + 4 = 186$ sboxes in round transformation and one sbox in key schedule should be calculated 2^3 times and 26 sboxes are calculated once only. The active sboxes are visualized by the blue trail in forward direction in Figure 7. This procedure is repeated 2 times for all $p_i i$'s, so in forward direction $2 \times \left(2^3 \times 187 + 26\right) = 3044$, sboxes should be calculated. In backward direction, 43 sboxes are calculated once and $1 + 4 + 8 \times 16 + 4 + 1 = 138$ sboxes in round transformation should be calculated 2 times. The active sboxes are visualized by the red trail in backward direction in Figure 7. This procedure is repeated 2^3 times for all s_j 's, so in backward direction, $2^3 \times \left(2 \times 138 + 43\right) = 2552$ sboxes should be calculated.

Rechecking the candidate keys complexity: Since in each group, 2^4 keys should be checked and the probability of matching is 2^{-4}, so $2^4 \times 2^{-4} = 1$ remaining key candidate should be tested to reach the correct key.

In total, the computational complexity of our attack is given by:

$$2^{124} \times \left(\frac{176 + 3044 + 2552}{558} + 1 \right) = 2^{127.50}$$

Data complexity: We need at most 2^{17} chosen ciphertexts for performing a biclique attack.

Conclusion

In this paper, we present a Biclique cryptanalysis of full round PRESENT with redduced data complexity. . In this paper we use asymmetric independent biclique attack on full round PRESENT. We construct a asymmetric biclique in ciphertext side for round 29-31 of PRESENT-80 and round 27-31 of PRESENT-128.

The data complexities of our attacks are less than before, which for a full round attack on PRESENT-80 and PRESENT-128 are 2^{17} plain text-ciphertext pairs. The computational complexity is slightly improved.

Acknowledgements

None.

Conflicts of interests

The author declares there are no conflicts of interests.

References

1. Dmitry Khovratovich, Christian Rechberger, Alexandra Savelieva. Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family. 2012;1:244–263.
2. Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger. Biclique Cryptanalysis of the Full AES. *Advances in Cryptology – asiacrypt*.2011;1:344–371.
3. Dmitry Khovratovich, Gaëtan Leurent, Christian Rechberger. Narrow-Bicliques: Cryptanalysis of Full IDEA. *Advances in Cryptology – eurocrypt*. 2012;392–410.
4. Yanfeng Wang, Wenling Wu, Xiaoli Yu. Biclique Cryptanalysis of Reduced-Round Piccolo Block Cipher. In Mark Dermot Ryan, Ben Smyth, Guilin Wang, editors. *Information Security Practice and Experience*. 2012;337–352.
5. Yanfeng Wang, Wenling Wu, Xiaoli Yu, et al. Security on L Block against Biclique Cryptanalysis. *Information Security Applications*. 2012;1–14.
6. Hamid Mala. Biclique Cryptanalysis of the Block Cipher square. 2014;8(3):207–212.
7. Zahra Ahmadian, Mahmoud Salmasizadeh, Mohammad Reza Aref. Biclique Cryptanalysis of the Full-RoundKLEIN Block Cipher. *Iet Information Security*.2015;9(5):294–301.
8. Shaozhen Chen, Tianmin Xu. Biclique Attack of the Full ARIA-256. 2012.
9. Mustafa Coban, Ferhat Karakoc, Özkan Boztacs. Biclique Cryptanalysis of TWINE. *Cryptology and Network Security*. 2012;1:43–55.
10. Deukjo Hong, Bonwook Koo, Daesung Kwon. Biclique Attack on the

Full HIGHT. Howon Kim, editor. *Information Security and Cryptology – ICISC*. 2011;365–374.

11. Andrey Bogdanov, Lars R Knudsen, Gregor Leander, et al. PRESENT: An Ultra-Lightweight Block Cipher. In: Pascal Paillier, Ingrid Verbauwhede, editors. IACR, India; 2007.
12. Kitae Jeong, Hyung Chul Kang, Changhoon Lee, et al. Biclique cryptanalysis of lightweight block ciphers PRESENT, piccolo and led. 2012.
13. Farzaneh Abed, Christian Foler, Eik List, et al. BicliqueCryptanalysis of PRESENTand LED Lightweight Ciphers. 2012.
14. Changhoon Lee. Biclique cryptanalysis of PRESENT-80 and PRESENT-128.*J Supercomput*. 2014;(70):95–103.
15. Bar On A, Dinur I, Dunkelman O, et al. Improved Analysis of Zorro-Like Ciphers. 2014.
16. Blondeau C, Bogdanov A, Wang M. On the (In) Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers. In: Boureanu I, Owesarski P, Vaudenay S, editors. *Applied Cryptography and Network Security*. 2014;271–288.
17. Bogdanov A, Geng H, Wang M, et al. Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In: Lange T, Lauter K, Lisonek P, editors. *Selected Areas in Cryptography – SAC*. 2013;306–323.
18. Donghoon Chang, Mohona Ghosh, Somitra Kumar Sanadhya. Biclique Cryptanalysis of full round AES-128 based hashing modes. In: Dongdai Lin, Moti Yung, Xiaofeng Wang, editors. *Inscrypt*. 2015;2:3–21.

Citation: Dehkordi MH, Taghizadeh R. Biclique cryptanalysis of full round PRESENT with reduced data complexity. *Electric Electron Tech Open Acc J.* 2018;2(2):251–255. DOI: 10.15406/eetoaj.2018.02.00021