SCIENCE CHINA
Information Sciences

• LETTER •

April 2016, Vol. 59 049101:1–049101:3
doi: 10.1007/s11432-016-5540-x

Biclique cryptanalysis using balanced complete bipartite subgraphs

Zheng GONG[1,2*], Shusheng LIU[1], Yamin WEN[3], Yiyuan LUO[4] & Weidong QIU[5]

[1]*School of Computer Science, South China Normal University, Guangzhou* 510631*, China;*
[2]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[3]*School of Mathematics and Statistics, Guangdong University of Finance and Economics, Guangzhou* 510320*, China;*
[4]*School of Electronics and Information, Shanghai Dian Ji University, Shanghai* 200240*, China;*
[5]*School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China*

Received August 6, 2015; accepted December 29, 2015; published online February 29, 2016

Citation Gong Z, Liu S S, Wen Y M, et al. Biclique cryptanalysis using balanced complete bipartite subgraphs. Sci China Inf Sci, 2016, 59(4): 049101, doi: 10.1007/s11432-016-5540-x

Dear editor,

At Asiacrypt 2011, Bogdanov et al. [1] formally defined the biclique cryptanalysis method and proposed the first key recovery attack on full-round AES faster than exhaustible search in single-key model. The basic idea underlying the biclique cryptanalysis is to determine two independent (or interleaving) differential paths in the forward and the backward direction to construct a biclique for a meet-in-the-middle (MITM) attack to recover the certain bits in subkeys. Many biclique cryptanalysis results have been presented in recent years using independent related-key differentials. In [2], Wang et al. proposed a biclique cryptanalysis on the reduced-round Piccolo [3] without postwhitening keys. In [4], the results were extended to the full-round Piccolo-80 and Piccolo-128 with postwhitening keys. At FSE 2013, Abed et al. [5] proposed a framework for automated independent-biclique cryptanalysis of AES-like ciphers. In [6], non-isomorphic biclique was proposed for the key recovery attack on the full-round mCrypton [7]. In [8], Ahmadi et al. proposed a low-data complexity biclique cryptanalysis for Piccolo. Using a strategy similar to the biclique cryptanalysis, Huang and Lai [9] proposed an optimized key recovery method based on the MITM attack, which could be exploited on most block ciphers in practice. Although all these biclique cryptanalyses only slightly reduce the computational complexities, which is comparable with exhaustive key searching attacks, they are still useful as new criteria for checking whether the underlying algorithms achieve strong differential propagation property in both of the key schedule and round function [1].

In this paper, we propose a new search technique to construct independent related-key differentials based on the balanced complete bipartite subgraph (BCBS) problem [10]. After defining our algorithm for independent related-key differentials, we apply the algorithm to determine independent related-key differentials of mCrypton and Piccolo, and then describe new biclique cryptanalysis results on full-round mCrypton and Piccolo-80. Compared to the related work, our results on Piccolo-80 have the best time complexity ($2^{78.9}$, see Appendix A). Particularly, our attack on Piccolo-80 supports the proposal that it is possible to construct the maximum dimensional bicliques if the ciphers satisfy BCBS. We note that

* Corresponding author (email: cis.gong@gmail.com)

The authors declare that they have no conflict of interest.

the algorithms can be used to analyze other ciphers that fit the definitions of our search technique.

The balanced complete bipartite subgraph problem. Let $G = (V, U, E)$ denote a bipartite graph G where its vertices can be divided into two disjoint sets V and U with edges in E (see Appendix B for detail). In graph theory, a balanced complete bipartite graph is a special kind of balanced bipartite graph in which every vertex of V is connected to every vertex of U. Furthermore, the purpose of the maximum BCBS problem is to find a BCBS in a bipartite graph with maximum d. A formalized definition of the BCBS problem [10] is provided in Definition 1.

Definition 1 (The BCBS Problem [10])**.** Let $G = (V, U, E)$ be a bipartite graph and d is a positive integer. The balanced complete bipartite subgraph (BCBS) problem of G is to find a subgraph $G' = (V', U', E') \subseteq G$ such that $V' \subseteq V$, $U' \subseteq U$, $V' \cap U' = \emptyset$, $|V'| = |U'| = d$ and for all $v \in V'$, $u \in U'$, $(v, u) \in E'$. For simplicity, G' can also be called as a $2d$-vertex BCBS of G.

Constructing bicliques using BCBS. Khovratovich et al. [1] constructed bicliques from two independent related-key differentials (see Appendix C). We describe how to construct a bipartite graph G from a cipher $\mathcal{E} = f \circ g \circ h$, and then reduce the problem of constructing bicliques of $\mathcal{E}$ to the BCBS problem in G.

Let $K = k_{\ell-1}k_{\ell-2}\cdots k_1k_0$, where k_i is the ith operating unit in key schedule. The set $\mathcal{I} = \{i \mid i \in [0, \ell)\}$ consists of all the indices of K. Let ΔK_I (or ∇K_J)-differentials denote a truncated differential that maps a zero (or non-zero) input difference to a non-zero (or zero) output difference under key difference ΔK_I (or ∇K_J) where subsets $I, J \subseteq \mathcal{I}$. To construct the biclique from independent related-key differentials, it is expected that for any $I, J \subseteq \mathcal{I}$, ΔK_I-differentials and ∇K_J-differentials are independent. We define the (strong) independent differential property between ΔK_I-differentials and ∇K_J-differentials. Thus $\forall i \in I$ and $\forall j \in J$, (ΔK_i-differentials, ∇K_j-differentials) are independent if the property holds.

Definition 2 (The (strong) independent differential property)**.** Let cipher $\mathcal{E} = f \circ g \circ h$.

• For any subset $I, J \subseteq \mathcal{I}$, if $\forall i \in I$ and $\forall j \in J$ (ΔK_i-differentials, ∇K_j-differentials) of h are independent, ΔK_I-differentials and ∇K_J-differentials are independent. We say h satisfies the independent differential property.

• For any subset $I, J \subseteq \mathcal{I}$, ΔK_I-differentials and ∇K_J-differentials are independent if and only if $\forall i \in I$ and $\forall j \in J$ (ΔK_i-differentials, ∇K_j-differentials) of h are independent. We say h satisfies the strong independent differential property.

If a subcipher h satisfies the (strong) independent differential property, related-key differentials (ΔK_I-differentials, ∇K_J-differentials) of h can be obtained by determining two subsets $I, J \in \mathcal{I}$ such that $\forall i \in I$ and $\forall j \in J$, (ΔK_i-differentials, ∇K_j-differentials) are independent. We prove that mCrypton and Piccolo satisfy the independent and the strong independent differential properties in Appendixes F.2 and G.2, respectively.

Based on Definition 2, we describe how to construct two subsets $I, J \in \mathcal{I}$ such that ΔK_I-differentials and ∇K_J-differentials of a subcipher h are independent. First, we define how two independent related-key differentials can be represented by a balanced bipartite graph $G = (V, U, E)$ from f in the following three steps. Let $K = k_{\ell-1}k_{\ell-2}\cdots k_1k_0$ denote the master key of $\mathcal{E}$.

Step 1. For each related-key difference ΔK_i ($0 \leqslant i < \ell$), it can be represented by the vertex $v_i \in V$. Thus, $V = \{v_i | 0 \leqslant i < \ell\}$ and $|V| = \ell$.

Step 2. For each related-key difference ∇K_j ($0 \leqslant j < \ell$), it can be represented by the vertex $u_j \in U$. Thus, $U = \{u_j | 0 \leqslant j < \ell\}$ and $|U| = \ell$.

Step 3. For each v_i and u_j, if (ΔK_i-differentials, ∇K_j-differentials) are independent, there exists an edge $(v_i, u_j) \in E$ which connects v_i and u_j,

If a graph G is constructed from a subcipher h, this implies that the balanced bipartite graph $G = (V, U, E)$ is derived from h according to the aforementioned three steps. Thus, the (strong) independent differential property can be reduced to the BCBS problem as follows (the proof is provided in Appendix D).

Theorem 1. Let a subcipher h of $\mathcal{E} = f \circ g \circ h$ satisfy the (strong) independent differential property, and the balanced bipartite graph $G = (V, U, E)$ is constructed from h. If (and only if) there exists a balanced complete bipartite subgraph $G' = (V', U', E') \subseteq G$, such that $I = \{i \mid v_i \in V', 0 \leqslant i < |V'|\}$, $J = \{j \mid u_j \in U', 0 \leqslant j < |U'|\}$ and $E' = \{(v_i, u_j) \mid v_i \in V', u_j \in U', i \in I, j \in J\}$, then ΔK_I-differential and ∇K_J-differential are independent.

Let a balanced bipartite graph $G = (V, U, E)$ be constructed from a block cipher $\mathcal{E} = f \circ g \circ h$, where there are at most $2\ell = |V| + |U|$ vertices in G. Considering the connected component of the bipartite graph $G = (V, U, E)$ and the degree of vertices, finding all BCBS of G is feasible. We propose Algorithm E1 to search the $2d$-vertices BCBS in G. Then Algorithm E1 is used by Algorithm E2 to determine the independent related-key truncated differentials in $\mathcal{E}$. The details of E1 and E2 can be found in Appendix E.

Description of Algorithm E1. For any block

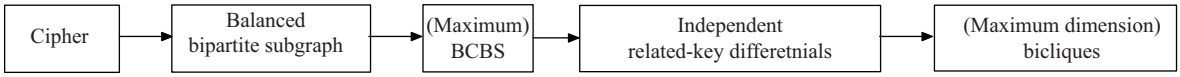

Figure 1 The process of calculating maximum dimensional bicliques of a subcipher.

cipher, the integer ℓ will not be greater than $|K|$. Moreover, because each edge in E cannot share the same vertices for independent related-key differentials, the number of edges $|E|$ will decrease when the diffusion of $\mathcal{E}$ increases by rounds. Therefore, the complexity of the (maximum) BCBS problem in G, which is constructed from $\mathcal{E}$, will be feasible. The base method of Algorithm E1 is first to construct a $2d$-vertex BCBS, and then construct a $2d+1$-vertex BCBS by adding an independent edge in E. By choosing a (maximum) range value D for the dimension of the biclique, Algorithm E1 will return a set of $2D$-vertex BCBS of G.

Description of Algorithm E2. After a set of $2d$-vertex BCBS of G is returned by Algorithm E1, we propose Algorithm E2 to transform those $2D$-vertex BCBS into independent related-key truncated differentials of subcipher h. For each BCBS constructed from Algorithm E1, all edges denote the independent relationship between the vertices set U and V. Thus each BCBS can be transformed into two independent related-key truncated differentials (ΔK_I-differentials, ∇K_J-differentials). By choosing BCBS with the largest cardinality of vertices, bicliques of h can be obtained from (ΔK_I-differentials, ∇K_J-differentials) with respect to Appendix C.

Based on the aforementioned algorithms, if a subcipher h of $\mathcal{E} = f \circ g \circ h$ satisfies the (strong) independent differential property, (a maximum dimensional) biclique of f can be obtained from the (maximum) BCBS by the process shown in Figure 1. The algorithms are used to construct new biclique attacks on mCrypton and Piccolo-80 (Appendixes F and G).

Conclusion. In this paper, we reduce the problem of finding independent related-key differentials of a subcipher to the BCBS problem, where a maximum BCBS can be used to construct maximum dimensional bicliques. In future work, we will attempt to apply our proposed algorithms to other biclique or cryptanalyses with respect to independent related-key differentials.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61572028, 61300204, 61402280), Natural Science Foundation of Guangdong (Grant Nos. 2015A030313630, 2014A030313439, 2013B010406008), Distinguished Young Teachers of Guangdong (Grant No. Yq2013051) and Project of Science and Technology of Guangzhou (Grant No. 2014J2200006). Weidong Qiu was also supported by the Ministry of Educations New Century Excellent Talents in University (Grant No. NCET-12-0358) and Technology Innovation Research Program of the Shanghai Municipal Education Commission (Grant No. 12ZZ019).

Supporting information Detailed algorithms and results on mCrypton and Piccolo (Appendixes A–G). The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Bogdanov A, Khovratovich D, Rechberger C. Biclique cryptanalysis of the full AES. In: Lee D, Wang X, eds. Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2011. 344–371
2 Wang Y, Wu W, Yu X. Biclique cryptanalysis of reduced-round Piccolo block cipher. In: Ryan M, Smyth B, Wang G, eds. Information Security Practice and Experience. Berlin: Springer, 2012. 337–352
3 Shibutani K, Isobe T, Hiwatari H, et al. Piccolo: an ultra-lightweight blockcipher. In: Preneel B, Takagi T, eds. Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2011. 342–357
4 Song J, Lee K, Lee H. Biclique cryptanalysis on lightweight block cipher: HIGHT and Piccolo. Int J Comput Math, 2013, 90: 2564–2580
5 Abed F, Forler C, List E, et al. A framework for automated independent-biclique cryptanalysis. In: Moriai S, ed. Fast Software Encryption. Berlin: Springer, 2014. 561–581
6 Shakiba M, Dakhilalian M, Mala H. Non-isomorphic biclique cryptanalysis and its application to full-round mCrypton. IACR Cryptology ePrint Archive, 2013, 2013: 141
7 Lim C H, Korkishko T. mCrypton-a lightweight block cipher for security of low-cost RFID tags and sensors. In: Song J, Kwon T, Yung M, eds. Information Security Applications. Berlin: Springer, 2005. 243–258
8 Ahmadi S, Ahmadian Z, Mohajeri J, et al. Low-data complexity biclique cryptanalysis of block ciphers with application to Piccolo and HIGHT. IEEE Trans Inf Foren Secur, 2014, 9: 1641–1652
9 Huang J L, Lai X J. What is the effective key length for a block cipher: an attack on every practical block cipher. Sci China Inf Sci, 2014, 57: 072110
10 Garey M R, Johnson D S. Computers and Intractability: A Guide to the Theory of NP-Completeness. San Francisco: W. H. Freeman, 1979