第 41 卷 第 2 期
2018 年 2 月
计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS
Vol. 41 No. 2
Feb. 2018

广义 Independent Biclique 攻击框架及其应用

崔竞一[1)] 郭建胜[1),2)] 刘翼鹏[1)]

[1)](信息工程大学 郑州 450001)

[2)](信息保障技术重点实验室 北京 100072)

摘 要 该文对 Biclique 攻击框架及其实现方法进行了研究. Biclique 攻击是一种结合 Biclique 初始结构与中间相遇攻击的一种攻击方法,有平衡 Biclique 攻击、非平衡 Biclique 攻击、Star 攻击等多种攻击形式. 该文提出了广义 Biclique 结构的概念,对 Biclique 结构重新进行了定义,涵盖了现有 Biclique 结构. 同时提出了一种广义 Biclique 结构分类方式,按照维数分为高维 Biclique 结构与低维 Biclique 结构. 通过进一步研究发现,高维 Biclique 结构可由低维 Biclique 结构直接构造得到,从而提出了一种高维 Biclique 结构构造方法,降低了结构构造过程的复杂度,同时利用该方法所得到的 Biclique 结构,结合计算与预计算技术,可以给出时间复杂度更优的 Biclique 攻击结果. 在此基础上,设计并提出了一个广义 Independent Biclique 攻击框架,借助自动化实现技术能够面向比特构造出算法包括平衡 Biclique 结构、Star 结构、非平衡 Biclique 结构在内的多种结构,同时能够给出算法在广义 Biclique 攻击下的安全性分析结果. 最后,以 LBlock 算法为例,利用框架综合分析了其在 Biclique 攻击下的安全性,同时改进了 AES-128 算法基于 Star 结构的相关分析结果. 获得分析结果如下:(1)针对 LBlock 算法,分别给出了两个低维 Biclique 攻击结果与两个高维 Biclique 攻击结果. 构造了明文方向 6 轮 4 维的平衡 Biclique 结构,给出了数据复杂度更优的平衡 Biclique 攻击结果,其时间复杂度为 $2^{78.425}$ 次全轮 LBlock 算法加密,数据复杂度为 2^{40} 选择明文;构造了明文方向 6 轮 4 维 Star 结构,给出了首个最低数据复杂度下全轮 LBlock 算法攻击结果,时间复杂度为 $2^{78.66}$ 次全轮 LBlock 算法加密,数据复杂度为 2 个已知明文;构造了明文方向 6 轮 8 维平衡 Biclique 结构,给出了目前最优的全轮 LBlock 算法分析结果,其时间复杂度为 $2^{78.14}$ 次全轮 LBlock 算法加密,数据复杂度为 2^{60} 个选择明文;构造了明文方向 6 轮规模 $2^4\times2^8$ 的非平衡 Biclique 结构,在 2^{40} 个选择明文条件下,给出了时间复杂度为 $2^{78.24}$ 的全轮 LBlock 算法分析结果;(2)针对 AES-128 算法,改进了算法在 Star 攻击下的安全性. 通过构造密文方向 2.5 轮 Star 结构代替明文方向的 2 轮 Star 结构,改进了最低数据复杂度下全轮 AES-128 的分析结果,其时间复杂度为 $2^{126.66}$ 次全轮 AES 加密,数据复杂度为 2 个已知明文.

关键词 Biclique 攻击;Independent Biclique 结构;广义 Biclique 结构;攻击框架;AES 算法;LBlock 算法

中图法分类号 TN918 **DOI 号** 10.11897/SP.J.1016.2018.00349

Generalized Independent Biclique Automated Attack Framework and Its Applications

CUI Jing-Yi[1)] GUO Jian-Sheng[1),2)] LIU Yi-Peng[1)]

[1)](*Information Engineering University*, *Zhengzhou* 450001)

[2)](*Science and Technology on Information Assurance Laboratory*, *Beijing* 100072)

Abstract This paper researches on the automated attack framework of Biclique cryptanalysis and its implementation method. Biclique cryptanalysis is a kind of meet-in-the-middle attack with the initial contractures such as balanced Biclique, unbalanced Biclique and Star. In this paper, a new concept was proposed to define all kinds of Bicliques, named generalized Biclique. The generalized Biclique contained the Bicliques known before such as balanced Biclique, unbalanced Biclique and Star. And a classification of generalized Bicliques was proposed. The Bicliques were divided into

收稿日期:2016-08-22;在线出版日期:2017-05-29. 本课题得到博士后科学基金(2014M562582)资助. **崔竞一**,男,1992 年生,硕士研究生,主要研究方向为对称密码设计与分析. E-mail: xd_cjy@126.com. **郭建胜**(通信作者),男,1972 年生,博士,教授,主要研究领域为信息安全与密码理论. E-mail: tsg_31@126.com. **刘翼鹏**,男,1992 年生,硕士研究生,主要研究方向为信息安全与量子密码.

two broad categories: high-dimension Bicliques and low-dimension Bicliques which are decided by the number of differential characteristics used in the structures while constructing the Bicliques. Furthermore, the further study showed that high-dimension Bicliques could be constructed by two or more low-dimension Bicliques, but not to exhaustively search the differential characteristics repeatedly. Based on this, a new method used to construct high-dimension Biclique was proposed to reduce the complexity in constructing Bicliques. At the same time, with the usage of the Bicliques constructed by this method, the Biclique attack could reach a better time complexity combined with precomputation and recomputation technique. Based on this method, a generalized Independent Biclique framework was designed. By programming, the bit-oriented Bicliques including balanced Biclique, unbalanced Biclique and Star could be constructed. And the attacks based on these Bicliques could be given at the same time. In the end, take LBlock for an example. By using the framework proposed in this paper, the security of LBlock under various Biclique attacks was analyzed automatically and the best attack on full-round LBlock was given. And the security of AES-128 under Biclique attack based on Star was improved. The details are as follows: As for LBlock, the framework firstly proposed two attacks on LBlock based on 4-dimension Bicliques and gave two attacks based on 8-dimension Bicliques then. A new 6-round 4-dimension balanced Biclique was constructed to improve the attack on full-round LBlock with a lower data complexity. The time complexity is $2^{78.425}$ full-round LBlock encryptions and the data complexity is 2^{40} chosen plaintexts. Based on 6-round 4-dimension Star, with the knowledge of 2 known plaintexts, the first Biclique attack of the full-round LBlock with minimum data complexity was given with the time complexity of $2^{78.66}$ full-round LBlock encryptions. The 6-round 8-dimension balanced Biclique was constructed and the framework gave the best attack on full-round LBlock known before. The time complexity and data complexity were $2^{78.14}$ full-round LBlock encryptions, 2^{60} chosen plaintexts respectively. Finally, based on 6-round unbalanced Biclique with the size of $2^4 \times 2^8$, the attack on full-round LBlock was presented with a time complexity of $2^{78.24}$ full-round LBlock encryptions and a data complexity of 2^{40} chosen plaintexts respectively. As for AES-128, the security of AES-128 under Star attack was imporved. There was a 2.5-round 8-dimension Star at the backward direction which was used to replace the 2-round 8-dimension Star at the forward direction. Based on this initial structure, the Star attack on AES-128 was improved with a time complexity of $2^{126.66}$ full-round AES-128 encryptions and a data complexity of 2 known plaintexts respectively.

Keywords Biclique attack; Independent Biclique; generalized Biclique; attack framework; AES; LBlock

1 引 言

Biclique 攻击由 Khovratovich 等人[1]在对哈希函数的安全性进行分析时提出. Biclique 攻击结合了 Biclique 结构与中间相遇攻击,Biclique 结构是由两个集合中元素所构成的完全二分图,主要思想源于对哈希函数分析过程中所使用的 splice-and-cut 技术[2-4]. Biclique 攻击在对 SHA 系列哈希算法家族的分析中取得了较好的效果[1].

在 Asiacrypt 2011 上,Bogdanov 等人[5]首次将 Biclique 攻击应用于对分组密码算法的分析中,提出了两种构造 Biclique 结构的方法及对应的密钥恢复算法,同时给出了首个低于穷举复杂度的全轮 AES 算法分析结果. 在 CRYPTO 2013 上,Canteaut 等人[6]提出了 sieve-in-the-middle 技术,进一步降低了 Biclique 攻击的复杂度. 在 ICISC 2014 上,Bogdanov 等人[7]提出了一种新的 Biclique 结构——Star 结构,利用该结构能够给出最低数据复杂度下的全轮 AES 算法优于穷举攻击的分析结果. 同时,文中改变了初

始结构的位置，对全轮 AES 算法 Biclique 攻击的时间复杂度与数据复杂度进行了优化. 在 ACISP 2015 上，Tao 等人[8]提出了非平衡 Biclique 结构的概念，基于非平衡 Biclique 结构给出了目前最优的全轮 AES 算法攻击结果. 同时，Biclique 攻击也在许多分组密码算法：HIGHT[9]、Piccolo[10]、TWINE[11]、LED[12]、mCrypton[12]、PRESENT[13]、KLEIN[14]的分析中得到了推广应用.

文献[5]中提出了两种初始结构的构造方法：Independent Biclique 与 Long Biclique. Independent Biclique 利用相互独立的相关密钥差分路径构造初始结构，对应地，称使用 Independent Biclique 结构的攻击为 Independent Biclique 攻击. 由于攻击轮数较多，Independent Biclique 攻击使用更为广泛. 本文仅针对 Independent Biclique 攻击展开研究.

下面介绍 Biclique 自动攻击框架相关研究的现状. 目前，针对 Biclique 自动攻击技术的研究主要集中在平衡 Independent Biclique 结构上. 在 FSE 2014 上，Abed 等人[15]提出了一个平衡 Independent Biclique 自动攻击框架. 文中所提出的 Independent Biclique 自动攻击框架能够自动搜索出一个特定算法的最优平衡 Biclique 攻击结果，包括 Biclique 结构构造与匹配过程，但是上述自动攻击框架没有对算法在 Star 结构、非平衡 Biclique 攻击下的安全性进行分析，如表 1 所示. 2016 年，Gong 等人[16]将 Biclique 结构的搜索问题归结于一个数学问题，主要对 Biclique 结构自动化搜索算法进行了研究，但对密码算法在 Biclique 攻击下的安全性进行分析时，需要结合理论分析才能给出完整的攻击过程. 2016 年，李云强等人[17]对 AES-128 算法在平衡 Biclique 攻击下安全性进行了分析，结合自动化技术得到了 AES-128 算法所有的平衡 Biclique 攻击结果，但文中没有对非平衡 Biclique 攻击与 Star 攻击的自动化搜索方法进行研究.

表 1　Biclique 自动攻击框架对比

平衡 Biclique 攻击	非平衡 Biclique 攻击	Star 攻击	出处
√	×	×	[15]
√	√	√	本文

结合前人工作，本文对 Biclique 攻击框架进行了研究，提出了一个能够对平衡 Independent Biclique 结构、Star 结构、非平衡 Independent Biclique 结构自动化搜索且能够给出完整攻击过程的框架，本文所提出的框架涵盖了平衡 Biclique 攻击、Star 攻击、非平衡 Biclique 攻击三种攻击，能够更全面地对算法安全性进行自动化分析. 首先，引入了广义 Biclique 结构的概念，涵盖了现有的平衡 Biclique 结构、非平衡 Biclique 结构、Star 结构，用来描述广义 Biclique 攻击中所使用的初始结构；其次，提出了一个高维 Biclique 结构的构造方法，降低了攻击过程中搜索构造 Biclique 结构的复杂度；然后，给出了广义 Biclique 攻击框架；最后，我们将框架应用于 LBlock 算法[18]，对 LBlock 算法在广义 Biclique 攻击下的安全性进行了全面分析，同时，对文献[7]中 AES-128 算法的 Star 攻击结果进行了改进，利用密文方向 2.5 轮 Star 结构，降低了全轮 AES-128 的 Star 攻击的时间复杂度.

本文第 2 节介绍广义 Biclique 结构及对应的攻击流程；第 3 节介绍新的 Biclique 结构构造方法及广义 Biclique 攻击框架；第 4 节应用框架对 LBlock 算法的安全性进行分析；第 5 节给出改进的全轮 AES-128 算法 Star 攻击结果；第 6 节总结全文工作.

2　广义 Biclique 攻击

首先对本文所使用的符号进行说明，其次引入广义 Biclique 结构的概念及构造方法，并对广义 Biclique 攻击流程进行简单说明.

2.1　符号说明

CP(Chosen Plaintext)：选择明文；

KP(Known Plaintext)：已知明文；

UB(Unbalanced Biclique)：非平衡Biclique 结构；

BB(Balanced Biclique)：平衡 Biclique 结构；

(l,d)-BB：l 轮 d 维平衡 Biclique 结构；

(l,d)-Star：l 轮 d 维 Star 结构；

(l,d_1,d_2)-UB：l 轮规模为 $2^{d_1}\times 2^{d_2}$ 的非平衡 Biclique 结构.

同时，在本文我们将使用 l 轮 d 维平衡 Biclique 结构的攻击称之为 l 轮 d 维平衡 Biclique 攻击.

2.2　广义 Biclique 结构

常见的 Biclique 结构有平衡 Biclique 结构、Star 结构、非平衡 Biclique 结构，参考文献[8]中非平衡 Biclique 结构的定义，给出广义 Biclique 结构的概念，用来统一表示这些结构.

定义 1.　考虑一个 l 轮算法 f 在密钥 K 的作用下，将中间状态集 S 中的元素映射到中间状态集

《计算机学报》

T 中的元素上，则有如下映射关系：

$$S \xrightarrow[f]{K} T.$$

令常数 $d_1, d_2 \geq 0$，若集合 $S=\{S_i: i=0,1,\cdots,2^{d_1}-1\}$，与状态集合 $T=\{T_j: j=0,1,\cdots,2^{d_2}-1\}$ 和对应的密钥集合 $\{K[i,j]: i=0,1,\cdots,2^{d_1}-1, j=0,1,\cdots,2^{d_2}-1\}$，能够满足对于所有的 $i\in\{0,\cdots,2^{d_1}-1\}$，$j\in\{0,\cdots,2^{d_2}-1\}$，均有 $T_j=f_{K[i,j]}(S_i)$，则称三元组 $(\{S_i\},\{T_j\},\{K[i,j]\})$ 为算法 f 上的一个广义 Biclique 结构.

由上述定义可以看出，广义 Biclique 结构可以涵盖现有 Biclique 结构. 一个 (l,d_1,d_2)-广义 Biclique 结构，在 d_1,d_2 取值不同时，可以具体表示为不同的 Biclique 结构. 当 $d_1=d_2=d\neq 0$ 时，则该广义 Biclique 结构是 (l,d)-BB；当 $d_1=0, d_2=2d\neq 0$ 时，可以表示 (l,d)-Star；当 $d_1\neq d_2, d_1\neq 0, d_2\neq 0$ 时，可以表示 (l,d_1,d_2)-UB，具体结构如图 1 所示.

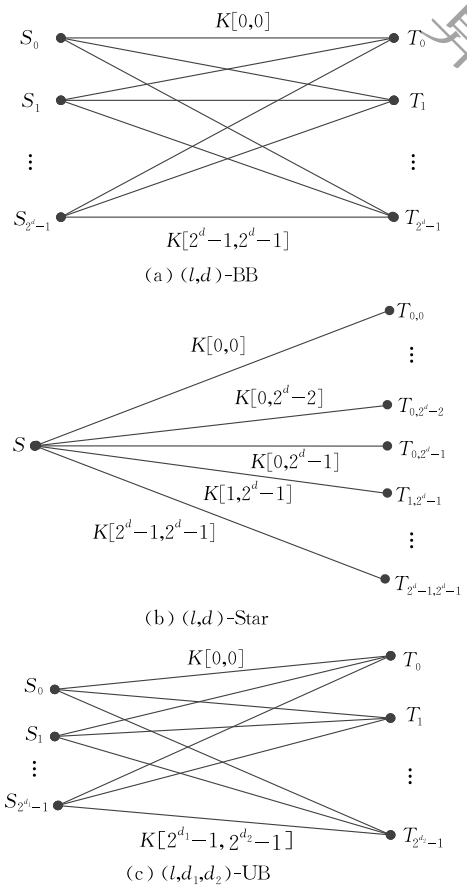


图 1 三类 Biclique 结构示意图

2.3 广义 Biclique 结构的构造

利用 Independent Biclique 构造方法[5]，固定一个三元组 $(S_0,T_0,K[0,0])$，满足子算法 f 通过密钥 $K[0,0]$ 将中间状态 S_0 映射至中间状态 T_0. 以此为基础，利用两条相互独立的相关密钥差分路径 Δ_j 与 ∇_i 构造一个映射关系，将 2^{d_1} 个中间状态 S_i 经过 $2^{d_1+d_2}$ 个密钥 $K[i,j]$ 向 2^{d_2} 个中间状态 T_j $(i=0,1,\cdots,2^{d_1}-1, j=0,1,\cdots,2^{d_2}-1)$ 映射：

$$S_0\oplus\nabla_i \xrightarrow[f]{K[0,0]\oplus\nabla_i^K\oplus\Delta_j^K} T_0\oplus\Delta_j,$$

其中 $i\in\{0,\cdots,2^{d_1}-1\}, j\in\{0,\cdots,2^{d_2}-1\}$.

那么我们令状态 $S_i=S_0\oplus\nabla_i, T_j=T_0\oplus\Delta_j$，密钥 $K[i,j]=K[0,0]\oplus\nabla_i^K\oplus\Delta_j^K$，就得到一个广义 Biclique 结构.

2.4 广义 Biclique 攻击流程

一个分组密码算法 e 将明文 P 映射到密文 C，假设该密码算法可以表示为 $e=g_2\circ f\circ g_1$，即如下形式：

$$e: P \xrightarrow[g_1]{} S \xrightarrow[f]{} T \xrightarrow[g_2]{} C.$$

通过在子算法 f 上构造广义 Biclique 结构，可以给出算法 e 的广义 Biclique 攻击过程如下：

(1) 划分密钥空间. 将算法 e 规模为 2^n 的主密钥空间划分为 $2^{n-(d_1+d_2)}$ 个规模为 $2^{d_1+d_2}$ 的密钥子空间 $K[i,j], i\in\{0,1,\cdots,2^{d_1}-1\}, j\in\{0,1,\cdots,2^{d_2}-1\}$；

(2) 构造广义 Biclique 结构. 对每一个密钥子空间 $K[i,j]$，在子算法 f 上，构造一个广义 Biclique 结构 $(\{S_i\},\{T_j\},K[i,j])$；

(3) 匹配过程. 对每一个密钥子空间 $K[i,j]$，当进行选择明文攻击时，如果存在一组 (T_j,C_i) 满足 $T_j \xrightarrow[g_2]{K[i,j]} C_i$，则将 $K[i,j]$ 选为候选密钥，否则剔除；当进行选择密文攻击时，如果密钥 $K[i,j]$ 满足 $P_i \xrightarrow[g_1]{K[i,j]} S_j$，则选为候选密钥，否则剔除；

(4) 搜索候选密钥. 对候选密钥集进行搜索，筛选出初始主密钥.

在上述攻击流程中，当子算法 g_1 是恒等映射时，分组密码简化为 $e=g_2\circ f$，这种攻击形式被称为明文方向的广义 Biclique 攻击. 文献[7]给出了全轮 AES 明文方向的 Star 攻击结果. 同样，若子算法 g_2 是恒等映射，文献[7]中利用密文方向的 Biclique 攻击给出了全轮 AES 算法的分析结果.

3 广义 Biclique 攻击框架

本节提出了一个新的高维 Biclique 结构构造方

《计算机学报》

法，降低了搜索构造广义 Biclique 结构的复杂度. 同时，给出了广义 Biclique 攻击框架，能够实现对算法在 Biclique 攻击下安全性的自动化评估.

3.1　高维 Biclique 结构构造方法

根据第 2 节中的介绍，可以使用(∇_i,Δ_j)表示一个广义 Biclique 结构. 本节提出了一种新的分类方式，将广义 Biclique 结构划分为低维 Biclique 结构与高维 Biclique 结构，下面分别给出其定义.

定义 2.　仅由两条相互独立的相关密钥差分路径(∇_i,Δ_j)构造得到的广义 Biclique 结构称为低维 Biclique 结构.

定义 3.　包含三条以上相互独立的相关密钥差分路径的广义 Biclique 结构称为高维 Biclique 结构.

低维 Biclique 结构包括低维平衡 Biclique 结构与 Star 结构，而高维 Biclique 结构包括高维平衡 Biclique 结构与高维非平衡 Biclique 结构. 此处的维度均是相对于算法的基本运算单元来说的. 例如 LBlock 算法中最小单元是半字节，因此 4 维称为低维，8 维及以上称为高维；AES 算法中最小单元是字节，因此 8 维称为低维，16 维及以上称为高维.

利用广义 Biclique 结构，可以给出算法在广义 Biclique 攻击下安全性分析结果，其中广义 Biclique 攻击包含平衡 Biclique 攻击、非平衡 Biclique 攻击与 Star 攻击三种. 对算法在广义 Biclique 攻击下安全性进行评估时，首先考虑算法在低维 Biclique 攻击下的安全性，其次考虑算法在高维 Biclique 攻击下的安全性. 高维 Biclique 结构可以由已知的低维平衡 Biclique 结构构造得到. 这种构造方法具有两个优势：一方面具有较高的搜索效率；另一方面利用这种方法得到的初始结构可以结合文献[8]中的预计算与重复计算技术，进一步降低 Biclique 攻击的时间复杂度. 这种构造方法具体可分为：

(1) 利用独立的低维平衡 Biclique 结构构造高维平衡 Biclique 结构

假设已知两个 l 轮 d 维的平衡 Biclique 结构(∇_i^1,Δ_j^1)与(∇_i^2,Δ_j^2)，如下所示：

$$\nabla_i^1 \xrightarrow[f]{\nabla_i^{K_1}\oplus\Delta_j^{K_1}} \Delta_j^1,\ i,j\in\{0,1,\cdots,2^d-1\},$$

$$\nabla_i^2 \xrightarrow[f]{\nabla_i^{K_2}\oplus\Delta_j^{K_2}} \Delta_j^2,\ i,j\in\{0,1,\cdots,2^d-1\}.$$

如果两条相关密钥差分路径$\nabla_i^1 \xrightarrow{\nabla_i^{K_1}} 0$ 与 $0 \xrightarrow{\Delta_j^{K_2}} \Delta_j^2$中差分活动的非线性变换不重合，同时$\nabla_i^2 \xrightarrow{\nabla_i^{K_2}} 0$ 与 $0 \xrightarrow{\Delta_j^{K_1}} \Delta_j^1$中差分活动的非线性环节不重合，则一定有$\nabla_i^1 \mid \nabla_i^2 \xrightarrow[f]{(\nabla_i^{K_1}\mid\nabla_i^{K_2})} 0$ 与 $0 \xrightarrow[f]{(\Delta_j^{K_1}\mid\Delta_j^{K_2})} \Delta_j^1\mid\Delta_j^2$中的差分活动的非线性环节不重合，同时满足密钥 $K[i_1,0]$与 $K[i_2,0]$的活动比特不重合且密钥 $K[0,j_1]$与 $K[0,j_2]$的活动比特不重合，可以构造出一个 l 轮 $2d$ 维的平衡 Biclique 结构$(\nabla_i^1\mid\nabla_i^2,\Delta_j^1\mid\Delta_j^2)$，如下所示：

$$\nabla_i^1\mid\nabla_i^2 \xrightarrow[f]{(\nabla_i^{K_1}\mid\nabla_i^{K_2})\oplus(\Delta_j^{K_1}\mid\Delta_j^{K_2})} \Delta_j^1\mid\Delta_j^2.$$

文献[8]中对全轮 AES-128 算法的 Biclique 攻击中所使用的 3 轮 16 维平衡 Biclique 结构就可以由两个 3 轮 8 维平衡 Biclique 结构来生成.

(2) 利用独立的低维平衡 Biclique 结构构造高维非平衡 Biclique 结构

已知两个 l 轮 d 维的平衡 Biclique 结构(∇_i^1,Δ_j^1)与(∇_i^1,Δ_j^2)，如下所示：

$$\nabla_i^1 \xrightarrow[f]{\nabla_i^{K_1}\oplus\Delta_j^{K_1}} \Delta_j^1,\ i,j\in\{0,1,\cdots,2^d-1\},$$

$$\nabla_i^1 \xrightarrow[f]{\nabla_i^{K_1}\oplus\Delta_j^{K_2}} \Delta_j^2,\ i,j\in\{0,1,\cdots,2^d-1\}.$$

已知差分路径 Δ_j^1与∇_i^1中差分活动的非线性变换不重合，若满足 Δ_j^2与∇_i^1中差分活动的非线性变换不重合，则可以得到∇_i^1与 $\Delta_j^1\mid\Delta_j^2$差分活动的非线性环节不重合，若密钥 $K[0,j_1]$与 $K[0,j_2]$的活动比特不重合，则可以构造出 l 轮规模为 $2^d\times2^{2d}$的非平衡 Biclique 结构$(\nabla_i^1,\Delta_j^1\mid\Delta_j^2)$，如下所示：

$$\nabla_i^1 \xrightarrow[f]{\nabla_i^{K_1}\oplus(\Delta_j^{K_1}\mid\Delta_j^{K_2})} \Delta_j^1\mid\Delta_j^2.$$

同理，可以利用(∇_i^1,Δ_j^1)和(∇_i^2,Δ_j^1)构造出 l 轮规模为 $2^{2d}\times2^d$的非平衡 Biclique 结构$(\nabla_i^1\mid\nabla_i^2,\Delta_j^1)$. 文献[8]中对全轮 AES 算法的攻击中所使用的 $2^8\times2^{16}$规模的非平衡 Biclique 结构可以由两个 3 轮 8 维平衡 Biclique 结构按照上述方法构造得到.

(3) 利用非独立的低维平衡 Biclique 结构构造高维平衡 Biclique 结构

假设已知两个 l 轮 d 维的平衡 Biclique 结构(∇_i^1,Δ_j^1)与(∇_i^2,Δ_j^2)，如下所示：

$$\nabla_i^1 \xrightarrow[f]{\nabla_i^{K_1}\oplus\Delta_j^{K_1}} \Delta_j^1,\ i,j\in\{0,1,\cdots,2^d-1\},$$

《计算机学报》

$$\nabla_i^2 \xrightarrow[f]{\nabla_i^{K_2} \oplus \Delta_j^{K_2}} \Delta_j^2,\ i,j \in \{0,1,\cdots,2^d-1\}.$$

如果两条相关密钥差分路径 ∇_i^1 与 Δ_j^2 中差分活动的非线性变换不重合，同时 ∇_i^2 与 Δ_j^1 中差分活动的非线性环节不重合，则一定有 $\nabla_i^1 \mid \nabla_i^2$ 与 $\Delta_j^1 \mid \Delta_j^2$ 中的差分活动的非线性环节不重合. 如果密钥 $K[i_1,0]$ 与 $K[i_2,0]$ 的活动比特重合且活动比特数为 d_1，密钥 $K[0,j_1]$ 与 $K[0,j_2]$ 的活动比特重合且活动比特数为 d_2，则可以构造出一个 l 轮规模为 $2^{d_1} \times 2^{d_2}$ 的非平衡 Biclique 结构 $(\nabla_i^1 \mid \nabla_i^2, \Delta_j^1 \mid \Delta_j^2)$，如下所示：

$$\nabla_i^1 \mid \nabla_i^2 \xrightarrow[f]{(\nabla_i^{K_1} \mid \nabla_i^{K_2}) \oplus (\Delta_j^{K_1} \mid \Delta_j^{K_2})} \Delta_j^1 \mid \Delta_j^2.$$

利用上述构造方法，由低维向高维构造 Biclique 结构时，不需要单独搜索高维相关密钥差分路径，简化了广义 Biclique 结构搜索构造过程. 以 LBlock 算法为例，构造 4 维 6 轮平衡 Biclique 结构时，利用半字节来划分主密钥空间，共存在 77 种可能，需要遍历 $C_{77}^2 = 2926$ 条差分路径得到 188 个 4 维 6 轮平衡 Biclique 结构；构造 8 维 6 轮平衡 Biclique 结构时，不需要遍历 $C_{77}^4 = 1\,353\,275$ 条差分路径，仅需要遍历 $C_{188}^2 = 17\,578$ 种可能就可以完成搜索. 随着密钥长度增加及初始结构维数增大，该方法的优势会更加明显.

3.2 广义 Biclique 攻击框架

在广义 Biclique 攻击框架中，主要包括广义 Biclique 结构搜索和匹配筛选两个过程. 在广义 Biclique 结构搜索过程中，Biclique 结构的维数 d 与轮数 l 是可控变量；在匹配过程中，中间匹配向量 $\boldsymbol{v}$ 与中间匹配的位置 m 是可控变量. 因此，对算法在广义 Biclique 攻击下安全性进行分析时，需要综合权衡 Biclique 结构的维数与轮数、匹配向量的重量与位置等因素与攻击复杂度之间的制约关系.

3.2.1 广义 Biclique 结构搜索过程

根据 3.1 节中所介绍的广义 Biclique 结构的构造方法，对广义 Biclique 结构的搜索实质上是对子算法 f 的低维平衡 Biclique 结构进行搜索，换句话说就是对其低维独立相关密钥差分路径 (∇_i, Δ_j) 的搜索. 在构造过程中，首先需要确定主密钥空间的划分方式，计算其圈子密钥；其次，构造出相关密钥差分路径；最后，利用相关密钥差分路径构造出低维平衡 Biclique 结构和 Star 结构，进而构造出广义 Biclique 结构. 详细构造过程如下：

(1) 划分密钥空间. 令 k 为主密钥比特数，N_d 为主密钥的个数. 当密钥扩展算法是面向比特进行操作时，任意选取主密钥的 d_1 比特为活动比特位，其余比特为非活动位，记为 $K[i,0]$；任意选取主密钥的 d_2 比特为活动比特位，其余比特为非活动位，记为 $K[0,j]$. 其中 d_1 比特与 d_2 比特不相交，则称为对主密钥空间的一个划分. 对所有可能的划分关系进行遍历，得到存在的划分的总数分别为

$$N_{d_i} = \binom{k}{d_1},\ N_{d_j} = \binom{k-d_1}{d_2}.$$

当密钥扩展算法的非线性变换是面向 d 比特字时，广义 Biclique 结构的维数一般取 d 的倍数，以 $d_1 = d_2 = d$ 比特字划分主密钥空间. 主密钥包含 k/d 个 d 比特字，$K[i,0]$ 与 $K[0,j]$ 的划分数量为

$$N_{d_i} = k/d,\ N_{d_j} = k/d - 1.$$

对于 AES-128 算法，主密钥 $k=128$ 比特，密钥扩展算法采用面向字节的非线性变换，通常构造 $d=8$ 维的 Biclique 结构，密钥的活动字节可以选取 16 个字节中任意一个位置，因此 $K[i,0]$ 存在 16 种可能，$K[0,j]$ 存在 15 种可能. LBlock 算法的密钥扩展算法是面向比特进行变换的，因此选择以连续的 d_1、d_2 比特为活动比特，遍历 d_1，d_2 的取值完成对主密钥空间的划分.

(2) 计算圈子密钥. 令 $K[i,0]$ 与 $K[0,j]$ 中活动比特位为 1，非活动比特位为 0，得到了一组密钥的截断差分 (∇_i^K, Δ_j^K). 利用密钥扩展算法得到分组算法 e 对应的圈子密钥截断差分状态.

(3) 相关密钥差分路径构造. 对于特定轮数的子算法 f，选定中间状态 S_0 与主密钥 $K[0,0]$ 均为 0，则 $S_0 \xrightarrow[f]{K[0,0]} T_0$ 与 $S_0 \xrightarrow[f]{K[0,j]} T_j$ 中的差分活动字节是由密钥 $K[0,j]$ 的活动比特引入的，因此只需要利用密钥的截断差分 Δ_j^K，加密得到 $0 \xrightarrow[f]{\Delta_j^K} \Delta_j$，同理可以计算得到 ∇_i 差分.

(4) 构造广义 Biclique 结构. 通过遍历搜索所有的 Δ_j 差分，若两条 Δ_j 差分对应位置的非线性变换不同时差分活动，则将两条相关密钥差分路径进行或操作，可以得到明文方向的 Star 结构. 同理，通过遍历 ∇_i 差分可以构造出密文方向的 Star 结构.

对 Δ_j 差分空间与 ∇_i 差分空间同时进行遍历搜索，若 Δ_j 差分与 ∇_i 差分对应位置的非线性变换不同时差分活动，则将两条差分路径进行或操作，可以得到一个 l 轮 d 维的平衡 Biclique 结构.

对 l 轮 d 维的平衡 Biclique 结构所构成的空间进行遍历搜索，利用 3.1 节中所提出的构造方法能够构造出 l 轮 $2d$ 维的平衡 Biclique 结构与 l 轮规模

计算机学报

为 $2^d \times 2^{2d}$ 的非平衡 Biclique 结构. 通过迭代，可以搜索得到所有 Biclique 结构.

3.2.2　匹配过程

下面以明文方向的 Biclique 攻击为例对匹配过程的自动化搜索方法进行说明. 选择第 m 轮为中间匹配位置，中间匹配向量的截断差分为 $\Delta \boldsymbol{v}$，在给定一个广义 Biclique 结构后，确定其主密钥空间划分方式，从而可以使用已知的密钥 $K[i,0]$ 对 T_j 加密至第 m 轮，$K[0,j]$ 对 C_i 解密至第 m 轮，检测两者的截断差分是否为 $\Delta \boldsymbol{v}$，若满足则将 $K[i,j]$ 列为候选密钥，最后对候选密钥集进行筛选恢复正确密钥. 我们称对 T_j 加密的过程为前向匹配过程，对 C_i 解密的过程为后向匹配过程.

(1) 首先，将前向匹配过程 E 按照轮数划分为两个子算法 $E=E_1 \circ E_2$，满足 $0 \xrightarrow[E]{\Delta_j^K} \Delta \boldsymbol{v}$. 按照中间相遇的思想，只需要计算与中间匹配向量 $\Delta \boldsymbol{v}$ 活动比特有关的非线性变换. 令 a_1 与 a_2 为两个截断差分，分别计算截断差分路径 $0 \xrightarrow[E_1]{\Delta_j^K} a_1$ 与 $a_2 \xleftarrow[E_2]{} \Delta \boldsymbol{v}$，通过控制 E_1 与 E_2 的轮数使得 a_1 与 a_2 满足 $a_1=a_1 | a_2$，从而可以得到一个前向匹配过程；

(2) 对于后向匹配过程，利用同样的思想，将后向匹配过程按照特定轮数划分为两个子算法 $G=G_1 \circ G_2$，满足 $\Delta \boldsymbol{v} \xrightarrow[G]{\nabla_i^K} 0$. 分别计算 $\Delta \boldsymbol{v} \xrightarrow[G_1]{} b_1$ 与 $b_2 \xleftarrow[G_2]{\nabla_i^K} 0$，通过控制 G_1 与 G_2 的轮数使得 b_2 与 b_1 满足 $b_2=b_2 | b_1$，从而可以得到一个后向匹配过程；

(3) 改变匹配向量重量与匹配位置，综合考虑匹配过程预计算与重复计算的非线性变换的数量，以及筛选候选密钥进行全轮加密的时间复杂度，选取较优的匹配向量与匹配位置.

4　攻击框架在 LBlock 算法上的应用

LBlock 算法是 Wu 等人[18] 在 ACNS 2011 上提出的一个轻量级分组密码算法. 算法主体是一个 32 轮的变形 Feistel 结构，分组规模是 64 bit，密钥规模是 80 bit，算法适用于低功耗设备. 2012 年，Karakoc 等人[11] 利用一个 9 轮 3 维的平衡 Biclique 结构，给出了全轮 LBlock 算法的 Biclique 攻击结果. 同年，Wang 等人[19] 利用一个 8 轮 4 维的平衡 Biclique 结构给出了全轮 LBlock 算法 Biclique 攻击结果. 在 LightSec 2014 上，AlTawy 等人[20] 基于 Biclique 攻击提出了差分筛选技术，对 18 轮 LBlock 算法进行了攻击. 在 C2SI 2015 上，AlTawy 等人[21] 在 Biclique 攻击的基础上提出了高阶密钥区分攻击，对全轮 LBlock 算法进行了攻击.

本节利用第 3 节所给出的攻击框架对 LBlock 算法的安全性进行分析，分别给出了 LBlock 算法的低维 Biclique 攻击与高维 Biclique 攻击. 得到了目前最优的全轮 LBlock 算法攻击结果；同时，首次给出了 LBlock 算法在 Star 攻击下与非平衡 Biclique 攻击下的安全性分析结果.

4.1　LBlock 算法

加密算法. LBlock 算法的分组规模为 64 bit，密钥规模为 80 bit，迭代轮数为 32 轮，整体结构是变形 Feistel 结构迭代而成. 轮函数包括 3 个基本运算：圈密钥模加、混乱层 S 和扩散层 P. S 层是由 8 个并置的 4 比特 S 盒构成，P 层是一个 8 维面向 4 比特字的置换. 具体变换过程是左半分组与圈密钥模加后经过一个 SP 变换与右半分组循环移 8 位后模加值作为下一轮的左半分组；上一轮的左半分组直接作为下一轮的右半分组，具体形式如图 2 所示.

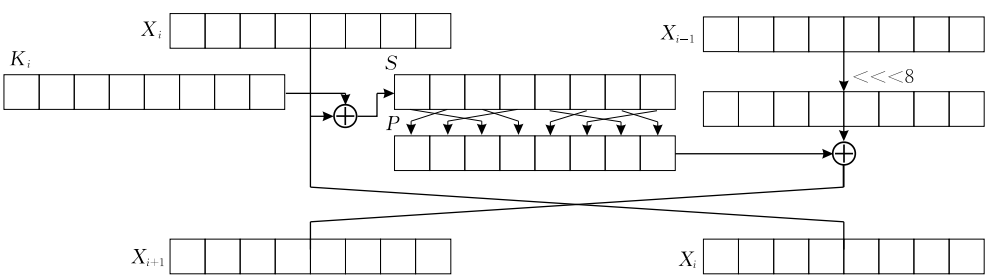


图 2　LBlock 算法轮函数

脱密算法. 由于 Feistel 结构的加脱密相似性，LBlock 算法的脱密算法与加密算法类似，只需要将输入右半分组的循环左移 8 位操作改为对输出左半分组的循环右移 8 位操作，同时倒序使用圈子密钥.

密钥扩展算法. LBlock 算法采用了一个面向比特的密钥扩展算法. 将 80 bit 的主密钥 $K=k_{79}k_{78}\cdots$

k_0存储在一个密钥寄存器中，生成第 i 轮圈子密钥时，取出当前寄存器中最左边 32 bit 作为圈子密钥 $K_i=k_{79}k_{78}\cdots k_{48}$. 每生成一个圈子密钥，对主密钥寄存器进行如下更新：

(1) $[k_{79}k_{78}\cdots k_1k_0]=$
$[k_{50}k_{49}k_{48}\cdots k_1k_0k_{79}k_{78}k_{77}\cdots k_{52}k_{51}]$

(2) $[k_{79}k_{78}k_{77}k_{76}]=s_9[k_{79}k_{78}k_{77}k_{76}]$
$[k_{75}k_{74}k_{73}k_{72}]=s_8[k_{75}k_{74}k_{73}k_{72}]$

(3) $[k_{50}k_{49}k_{48}k_{47}k_{46}]=[k_{50}k_{49}k_{48}k_{47}k_{46}]\oplus[i]_2$.

4.2 低维 Biclique 攻击

在广义 Biclique 攻击框架下，低维 Biclique 攻击包括低维平衡 Biclique 攻击与 Star 攻击. 本节首先给出低维 Biclique 攻击搜索算法；然后分别给出 LBlock 算法的低维平衡 Biclique 攻击和 Star 攻击.

4.2.1 低维 Biclique 攻击搜索算法

依据 3.2 节中所介绍的攻击框架，取 80 bit 密钥中任意连续的 d 比特作为活动比特位，记为 1，剩余 80-d 比特记为 0，从而针对每个 d 均可以构造出一个密钥的截断差分集 X. 任意选取其中两个元素，利用密钥扩展算法求出对应圈子密钥的截断差分并构造出两条 l 轮相关密钥差分路径 Δ 与 ∇，若两条差分路径中活动 S 盒没有重合，则可记作一个低维 Biclique 结构. 选取在第 m 轮进行匹配，且中间匹配向量为 $\boldsymbol{v}$，分别搜索前向匹配过程与后向匹配过程构成完整的匹配过程. 计算攻击过程中预计算与重复计算的 S 盒的个数，通过遍历 $d,l,m,\boldsymbol{v}$ 的取值搜索得到 LBlock 算法较优的低维 Biclique 攻击结果，详细过程可参见算法 1.

算法 1. LBlock 算法低维 Biclique 攻击搜索算法.

```
输入：维数集合 D；轮数集合 L；匹配位置集合 M；匹配
      向量集合 V
输出：LBlock 算法低维 Biclique 攻击结果
BEGIN
  FOR d in D
    令连续 d 比特为 1，80-d 比特为 0，构造一个密钥
    集 X
  END FOR
  FOR k1 in X, k2 in X, l in L
    构造两条相关密钥差分路径 Δ 与 ▽
    IF 差分路径中活动 S 盒不重合
      将低维 Biclique 结构存储在 B 中
    END IF
  END FOR
  FOR b in B, m in M, v in V
  针对不同低维 Biclique 结构，搜索不同匹配条件下的
  攻击，给出低时间复杂度的攻击结果
  END FOR
END
```

4.2.2 低维平衡 Biclique 攻击

利用 4.2.1 节中的算法 1 对低维平衡 Biclique 结构进行搜索可以得到结论 1.

结论 1. LBlock 算法不存在 9 轮及以上任意维数的明文方向平衡 Biclique 结构.

通过进一步搜索，可以给出一个数据复杂度较低的 6 轮 4 维平衡 Biclique 攻击，详细过程如下：

(1) 密钥空间划分. 选择 80 bit 主密钥中第 $\{18,19,20,21,24,25,26,27\}$ bit 为活动比特位. 令 $K[0,0]$表示第$\{18,19,20,21,24,25,26,27\}$ bit 取 0，其余 72 bit 任意取值的主密钥，将规模为 2^{80} 的主密钥空间划分形成了 2^{72} 个规模为 2^8 密钥子空间 $\{K[i,j],i\in\{0,1\}^4,j\in\{0,1\}^4\}$. 令$\{K[i,j],j\in\{0,1\}^4\}$表示第$\{18,19,20,21\}$ bit 遍历，其余比特固定的密钥集合；$\{K[i,j],i\in\{0,1\}^4\}$为第$\{24,25,26,27\}$ bit 遍历，其余比特固定的密钥集合.

(2) 平衡 Biclique 结构构造. 根据圈子密钥比特与主密钥比特对应关系，可以直接查表得到圈子密钥的活动比特位. 分别利用对应圈子密钥构造相关密钥差分路径 Δ_j 与 ∇_i，如图 3 所示 Δ_j 与 ∇_i 中没有重合的活动 S 盒，因此可以构造得到一个 6 轮 4 维平衡 Biclique 结构，图中黑色标识表示活动 S 盒，白色标识表示非活动 S 盒.

(3) 匹配过程. 对每个密钥子空间中 2^8 个密钥进行中间相遇匹配筛选. 选取第 19 轮为中间匹配位置，匹配向量 $\boldsymbol{X}_{18}=0$x21，分别向上解密 6 轮，向下加密 5 轮，构造中间相遇区分器，得到如图 4 所示的匹配过程. 结合预计算与重复计算技术，仅需要对图中灰色的 S 盒进行 1 次预计算存储，对黑色标识的 S 盒进行重复计算，即可完成匹配. 黑色标识表示活动 S 盒，白色标识表示非活动 S 盒，灰色标识表示在匹配过程中不需要计算的 S 盒.

(4) 搜索候选密钥. 由于中间匹配向量的重量为 8，因此平均一个错误密钥通过匹配检测的概率为 2^{-8}，而每个密钥子空间中包含 2^8 个密钥，因此每个密钥子空间平均有 $2^8\times2^{-8}=1$ 个密钥通过匹配检测. 最终，每次攻击都需要对剩余的 1 个候选密钥进行全轮加密，检测是否为初始正确密钥.

上述低维平衡 Biclique 攻击的数据复杂度、存储复杂度与时间复杂度结论由定理 1 给出. 由于在攻击中需要进行加解密操作，而其中 S 盒变换的耗时起决定性因素，因此以需要计算的 S 盒数量为时

《计算机学报》

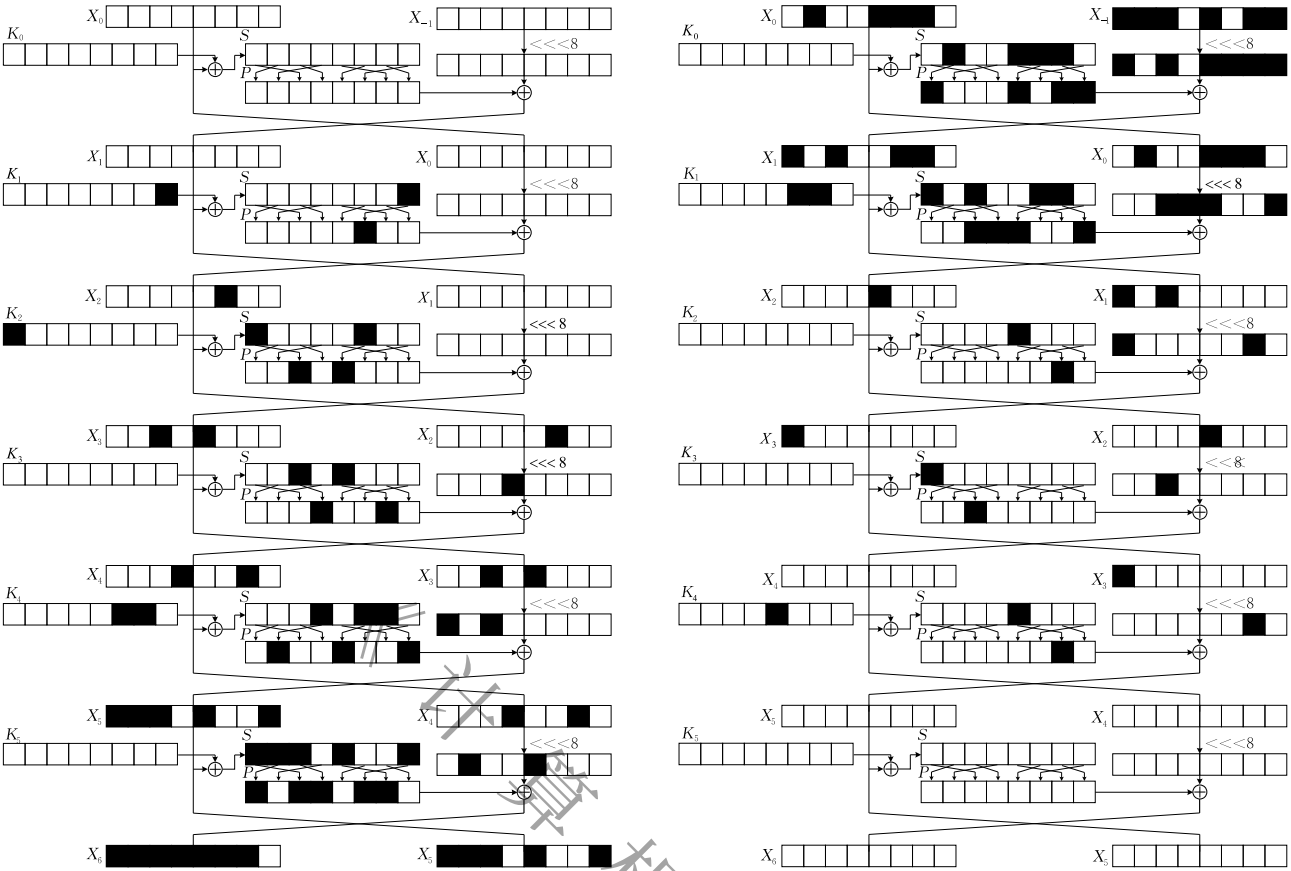


图 3　6 轮 4 维平衡 Biclique 结构

间复杂度的衡量指标[19]，一次全轮 LBlock 算法加密需要计算 318 个 S 盒(加密算法 256 个，密钥扩展算法 62 个)，利用上述关系可以将预计算与重计算的 S 盒个数转换为全轮 LBlock 算法的加密次数.

定理 1.　基于 6 轮 4 维平衡 Biclique 结构，低维平衡 Biclique 攻击可以恢复全轮 LBlock 算法的主密钥，其数据复杂度为 2^{40}，存储复杂度为 $2^{9.48}$，时间复杂度为 $2^{78.425}$.

证明.　数据复杂度. 攻击中使用了明文方向的 Biclique 结构，因此通过观察 Biclique 结构的输入形式，可以得知对每一个 Biclique 结构需要固定明文第 0，2，3，7，11，13 半字节为非差分活动的，因此攻击所需要的选择明文满足上述字节固定不变，其余半字节遍历所有可能的取值，数据复杂度为 2^{40} 个选择明文.

存储复杂度. 主要包括 Biclique 结构存储的复杂度与使用预计算与重计算技术，存储预计算的 S 盒的复杂度. 首先，需要对预计算得到的 Biclique 结构进行存储，其实质是明文状态与中间状态的一一对应关系，需要顺序存储 2^4 个明文与 2^4 个中间状态的对应关系，每个状态为 8 字节，因此共需要存储 $(2^4+2^4)\times 8$ 字节；其次，在攻击中使用预计算与重复计算技术，对不受活动比特影响的 S 盒进行计算并存储. 在生成圈子密钥的过程中，需要预计算存储 49 个非活动 S 盒；在匹配过程中，需要预计算存储 54 个非活动 S 盒，共存储 $49+2^4\times 54=913$ 个 S 盒，由于每个 S 盒均为 4 bit，因此共需要存储 $2^{8.83}$ 字节. 综上，上述 6 轮 4 维平衡 Biclique 攻击的存储复杂度为 $2^{9.48}$ 字节.

时间复杂度. 6 轮 4 维 Biclique 攻击实质上是对 2^{72} 个规模为 2^8 的密钥子空间分别进行攻击，构造候选密钥集，最后从候选密钥集中筛选出正确密钥的过程. 攻击的时间复杂度主要由 4 个过程的时间复杂度所构成.

(1) Biclique 结构构造过程中，需要进行 1 次 6 轮 LBlock 算法加密运算，得到一个三元组(S_0，T_0，$K[0,0]$)，其中共计算 48 个 S 盒. 利用 Δ_j 差分计算 T_j 时，需要重计算 13 个 S 盒；利用 ∇_i 差分计算 S_i 时，需要重计算 11 个 S 盒. 因此，Biclique 结构构造过程共计算 $2^4\times 13+2^4\times 11+48=432$ 个 S 盒.

(2) 匹配过程中，分为前向匹配与后向匹配两个过程. 前向匹配由中间状态 T_j 经密钥 $K[i,0]$ 加

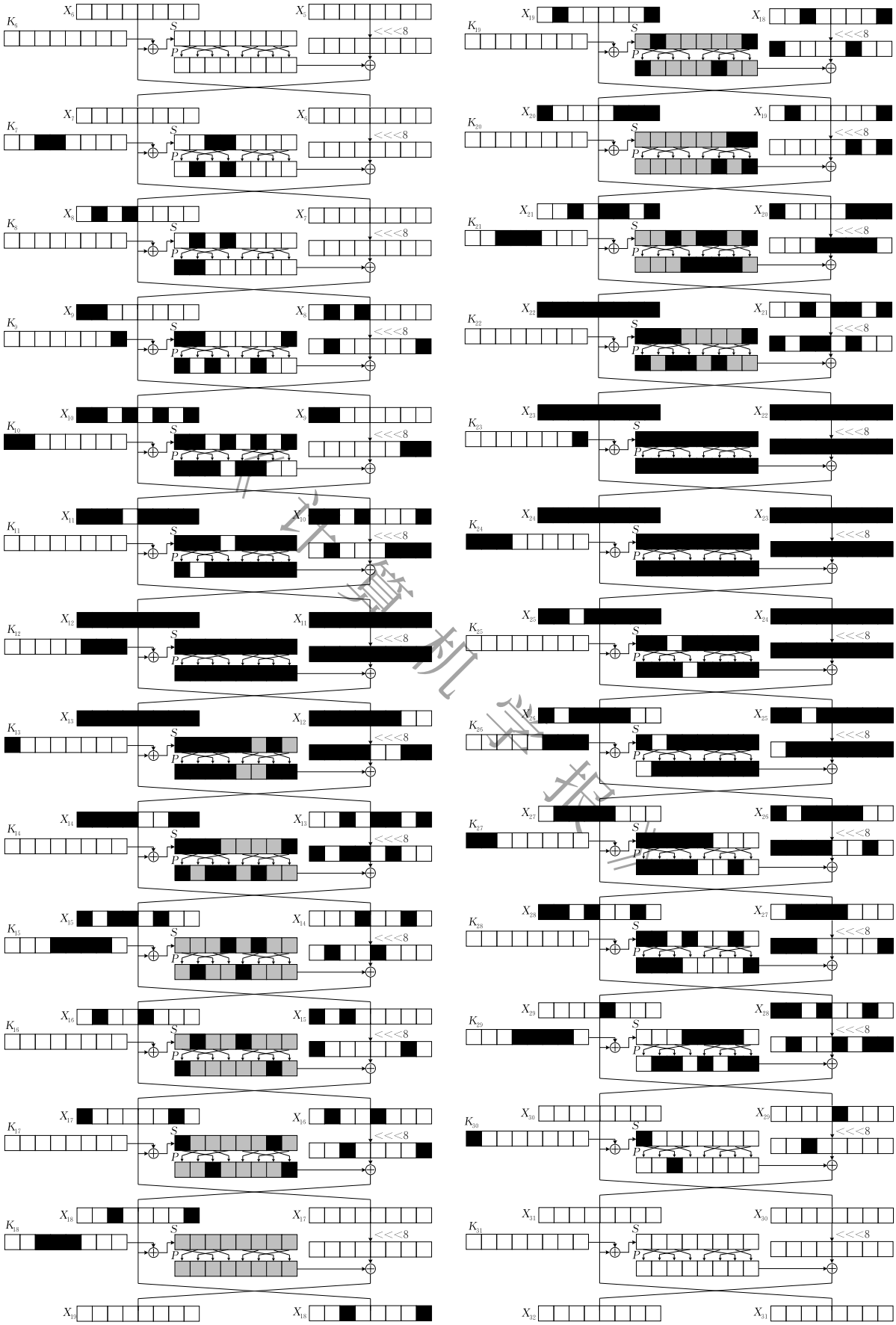


图 4 低维平衡 Biclique 攻击的匹配过程

密得到匹配向量 $\boldsymbol{v}$ 需重计算 43 个 S 盒，预计算 29 个 S 盒；后向匹配由密文 C_i 经密钥 $K[0,j]$ 解密得到匹配向量 $\boldsymbol{v}'$ 需重计算 56 个 S 盒，预计算 28 个 S 盒. 因此，共计算 $2^4\times(2^4\times(43+56)+28+29)=26\,256$ 个 S 盒.

(3) 计算圈子密钥的过程中，LBlock 算法的密钥扩展算法较为简单，根据主密钥与圈子密钥的比特对应关系，通过查表可知需要预计算 49 个 S 盒，重计算 17 个 S 盒，共计算 $2^4\times17+49=321$ 个 S 盒.

(4) 搜索候选密钥过程中，需要对每个密钥子空间通过中间相遇匹配检测后的候选密钥集进行全轮算法加密筛选，每个密钥子空间经过匹配检测后仅剩余 1 个候选密钥，因此需要进行 1 次全轮 LBlock 算法加密.

综上分析，6 轮 4 维平衡 Biclique 攻击的总时间复杂度为 $C=2^{72}\left(\frac{432+26\,256+321}{318}+1\right)\approx2^{78.425}$ 次全轮 LBlock 算法加密.　　证毕.

4.2.3　Star 攻击

Star 攻击是一种低数据复杂度下的 Biclique 攻击，使用 Star 结构进行攻击时，一般仅需要 2～3 个已知明文就可以恢复全轮算法的主密钥. 在现实生活中，由于使用安全协议等因素，攻击者通过截取、窃听等手段可获得的数据量严格受限，对算法抵抗攻击能力进行全面评估时，假设攻击者计算能力无限，已知数据量有限的情况具有一定的现实意义.

根据算法 1，使用连续比特对 LBlock 算法的主密钥空间进行划分，对 Δ_j 差分空间进行搜索构造 LBlock 算法明文方向 Star 攻击，得到如下结论 2.

结论 2.　LBlock 算法不存在 7 轮及以上任意维数的 Star 结构.

综合考虑复杂度，根据框架搜索得到的 Star 结构与匹配过程，下面给出 LBlock 算法的 6 轮 4 维 Star 攻击的思路：

(1) 密钥空间划分. 选择主密钥中第 $\{6,7,8,9,23,24,25,26\}$ bit 为活动位. 将规模为 2^{80} 的主密钥空间划分形成 2^{72} 个规模为 2^8 的密钥子空间 $\{K[j_1,j_2],j_1\in\{0,1\}^4,j_2\in\{0,1\}^4\}$.

(2) Star 结构构造. 根据圈子密钥比特与主密钥比特对应关系，分别利用对应密钥构造 Δ_{j_1} 差分与 Δ_{j_2} 差分，两条差分路径活动 S 盒没有重合，因此可以得到一个 6 轮 4 维的 Star 结构，具体结构如图 5 所示. 图中黑色标识表示活动 S 盒，白色标识表

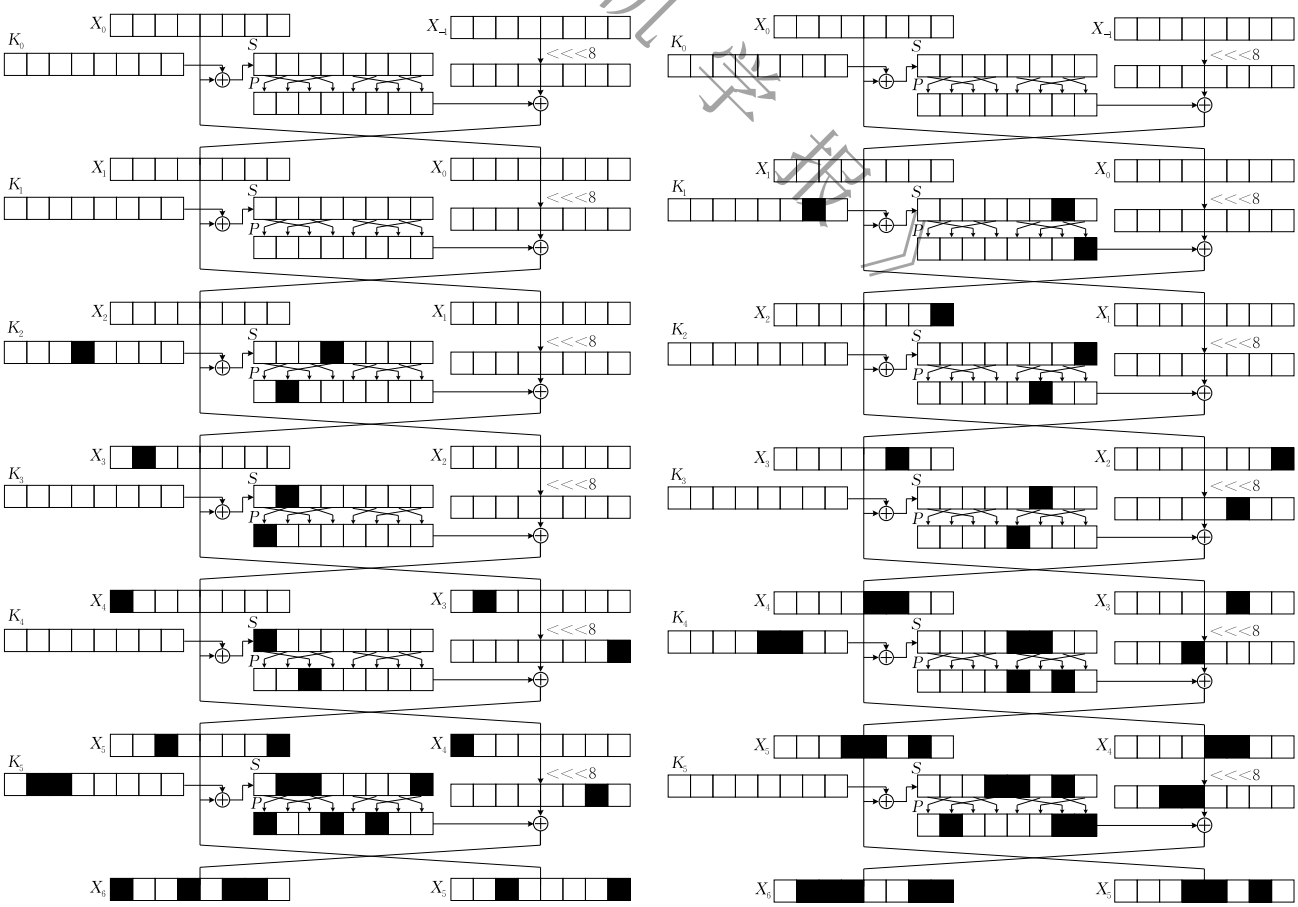


图 5　6 轮 8 维 Star 结构

计算机学报

示非活动 S 盒.

(3)匹配过程. 使用与 4.2.1 节攻击中类似的匹配过程,在第 19 轮进行部分匹配,匹配向量为 $\boldsymbol{X}_{18}=0\text{x}21$.

(4)搜索候选密钥. 每个密钥子空间的密钥量为 2^8,错误密钥通过检测的概率为 2^{-8},则平均剩余候选密钥量为 $2^8\times2^{-8}=1$. 对每一个密钥子空间,执行 1 次全轮 LBlock 算法加密可判断密钥的正确性.

利用定理 2 给出 6 轮 4 维 Star 攻击的复杂度分析结果,其证明过程类似定理 1.

定理 2. 基于 6 轮 4 维的 Star 结构,可以在最低数据复杂度下恢复全轮 LBlock 算法的主密钥,其数据复杂度为 2,存储复杂度为 $2^{11.31}$,时间复杂度为 $2^{78.66}$.

4.3 高维 Biclique 攻击

在广义 Biclique 框架下,高维 Biclique 攻击包含两种形式:高维平衡 Biclique 攻击与高维非平衡 Biclique 攻击.

4.3.1 高维 Biclique 攻击搜索算法

在搜索过程中,通过低维平衡 Biclique 结构分别构造出两种高维 Biclique 结构,并给出对应的高维非平衡 Biclique 攻击与高维平衡 Biclique 攻击,详细过程由算法 2 给出. 通过与算法 1 对比,可以看出利用 3.1 节中所提出的方法能够简化高维 Biclique 攻击搜索过程.

算法 2. LBlock 算法高维 Biclique 攻击搜索算法.

```
输入:匹配位置集合 M;匹配向量集合 V
输出:LBlock 算法高维 Biclique 攻击结果
BEGIN
  FOR b1 in B, b2 in B
    IF 差分路径中活动 S 盒不重合
      将高维 Biclique 结构存储在 H 中
    END IF
  END FOR
  FOR h in H, m in M, v in V
    针对不同高维 Biclique 结构,搜索不同匹配条件下
    的攻击,给出低时间复杂度的攻击结果
  END FOR
END
```

4.3.2 高维非平衡 Biclique 攻击

通过对 LBlock 算法的 4 维平衡 Biclique 结构空间进行搜索,利用两个 6 轮 4 维平衡 Biclique 结构构造出一个(6,4,8)-非平衡 Biclique 结构,进而给出 LBlock 算法首个非平衡 Biclique 攻击结果. 详细过程如下:

(1)密钥空间划分. 选择 80 bit 主密钥中第{6,7,8,9,22,23,24,25,47,48,49,50}bit 为活动位. 令 $K[0,0,0]$表示第{6,7,8,9,22,23,24,25,47,48,49,50}bit 取 0,其余比特任意取值的主密钥,将主密钥空间划分为 2^{68} 个规模为 2^{12} 的密钥子空间$\{K[i_1,i_2,j],i_1,i_2,j\in\{0,1\}^4\}$. 令$\{K[i_1,i_2,j],i_1\in\{0,1\}^4\}$表示第{47,48,49,50}bit 遍历,其余比特取固定值形成的密钥子空间;$\{K[i_1,i_2,j],i_2\in\{0,1\}^4\}$表示第{22,23,24,25}bit 遍历,其余比特取固定值形成的密钥子空间,$\{K[i_1,i_2,j],j\in\{0,1\}^4\}$为第{6,7,8,9}bit 遍历,其余比特取固定值形成的密钥子空间.

(2)构造非平衡 Biclique 结构. 已知两个 6 轮 4 维平衡 Biclique 结构(∇_{i_1},Δ_j)与(∇_{i_2},Δ_j),那么根据 3.1 节中所介绍的构造方法,可以得到一个 6 轮非平衡 Biclique 结构,具体结构见图 6.

(3)匹配过程. 选择在第 19 轮进行部分匹配,匹配向量为 $\boldsymbol{X}_{18}=0\text{x}21$,分别构造前向匹配过程与后向区配过程,其中前向匹配过程是由两个前向匹配过程的截断差分路径合并得到[8],具体结构见附录 1.

(4)搜索候选密钥. 每个密钥子空间密钥量为 2^{12},平均每个密钥子空间剩余候选密钥量为 $2^{12}\times2^{-8}=2^4$. 对每一个密钥子空间,执行 16 次全轮 LBlock 算法加密即可检测密钥的正确性.

类似定理 1 的分析过程,用定理 3 给出了(6,4,8)-非平衡 Biclique 攻击的复杂度分析结果.

定理 3. 基于一个 6 轮规模为 $2^4\times2^8$ 的非平衡 Biclique 结构,可以恢复出全轮 LBlock 算法的主密钥,其数据复杂度为 2^{64},存储复杂度为 $2^{14.84}$,时间复杂度为 $2^{78.24}$.

4.3.3 高维平衡 Biclique 攻击

根据算法 2,对 LBlock 算法 4 维平衡 Biclique 结构空间进行搜索,利用两个 6 轮 4 维的平衡 Biclique 结构构造得到了一个 6 轮 8 维平衡 Biclique 结构,然后给出了目前最优的全轮 LBlock 算法分析结果.

(1)密钥空间划分. 选择 80 bit 主密钥中第{6,7,8, 9,18,19,20,21,24,25,26,27,47,48,49,50}bit 为活动位,令 $K[0,0,0,0]$表示第{6,7,8,9,18,19,20,21,24,25, 26,27,47,48,49,50}bit 取 0,其余比特取固定值的主密钥,将主密钥空间划分为 2^{64} 个规模为 2^{16} 的密钥子空间$\{K[i_1,i_2,j_1,j_2],i_1,i_2,j_1,j_2\in\{0,1\}^4\}$. $\{K[i_1,i_2,j_1,j_2],i_1\in\{0,1\}^4\}$表示第{47,48,49,50}bit 遍历,其余比特取固定值的密钥子空间;$\{K[i_1,i_2,j_1,j_2],i_2\in\{0,1\}^4\}$

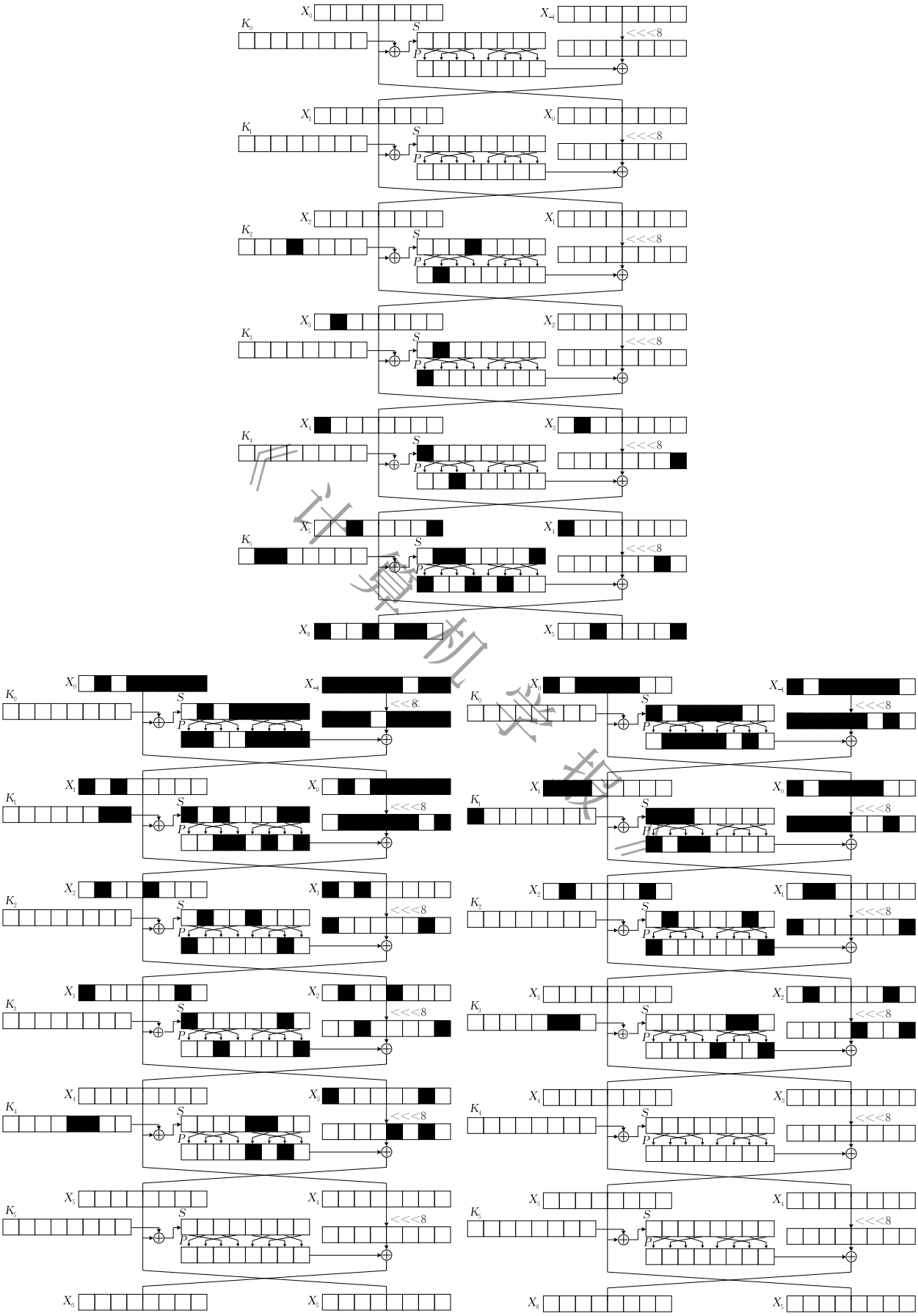


图 6　(6,4,8)-非平衡 Biclique 结构

表示第{24,25,26,27} bit 遍历,其余比特取固定值的密钥子空间;$\{K[i_1,i_2,j_1,j_2],j_1\in\{0,1\}^4\}$为第{6,7,8,9} bit 位遍历,其余比特取固定值的密钥子空间,$\{K[i_1,i_2,j_1,j_2],j_2\in\{0,1\}^4\}$表示第{18,19,20,21} bit 遍历,其余比特取固定值的密钥子空间.

(2) 构造高维平衡 Biclique 结构. 利用 3.1 节中的构造方法,由两个 6 轮 4 维平衡 Biclique 结构可以得到一个 6 轮 8 维平衡 Biclique 结构,如图 7 所示.

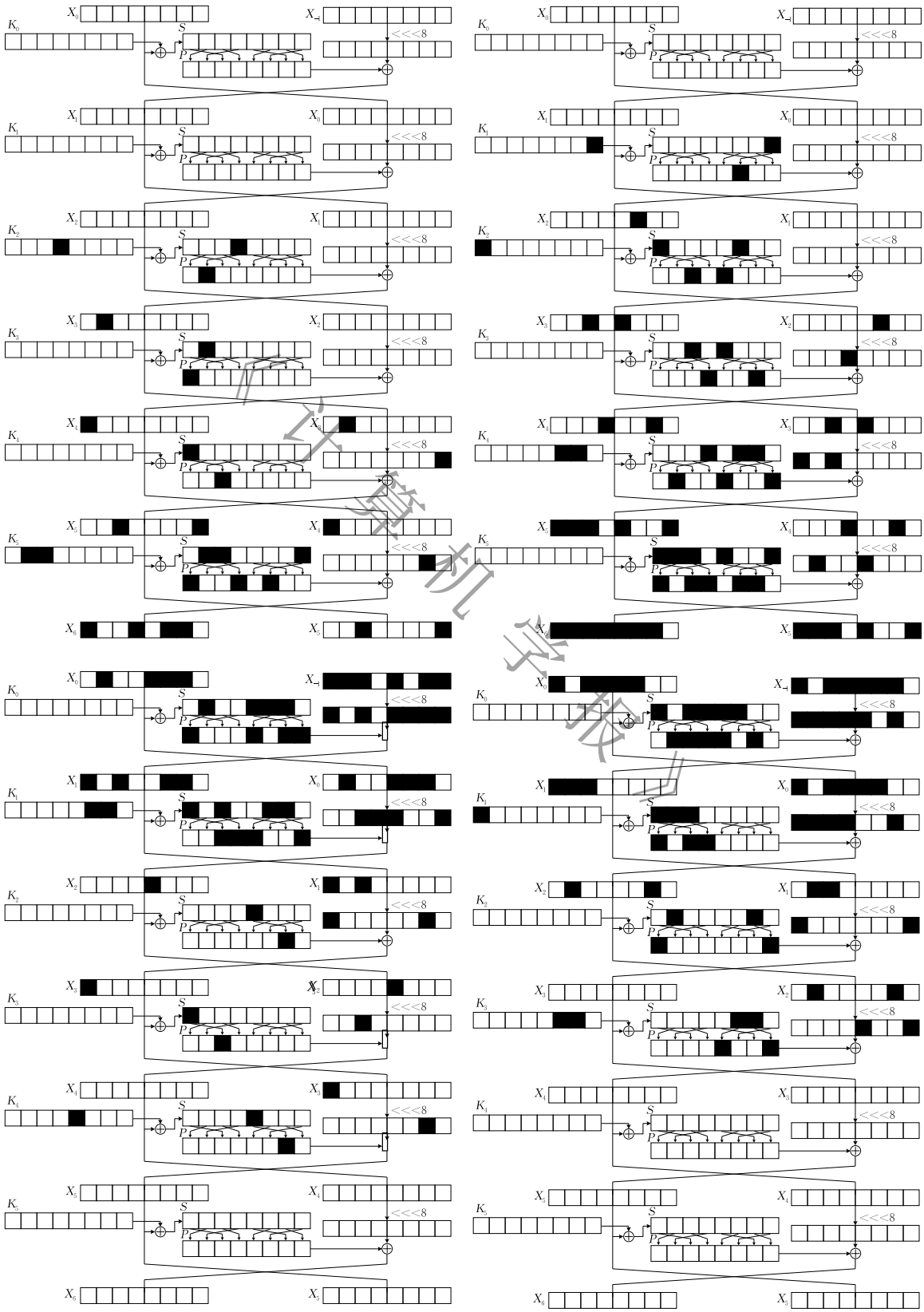


图 7 (6,8)-平衡 Biclique 结构

《计算机学报》

(3) 匹配过程. 选择在第 19 轮进行部分匹配，匹配向量为 $\boldsymbol{X}_{18}=0\text{x}21$，分别利用两个前向匹配与两个后向匹配的截断差分路径，构造得到与 4.3.2 节中相类似的匹配过程.

(4) 搜索候选密钥. 每个密钥子空间的规模为 2^{16}，平均每个密钥子空间剩余候选密钥量为 $2^{16}\times 2^{-8}=2^{8}$. 对每一个密钥子空间，执行 256 次完整 LBlock 加密即可检测候选密钥的正确性.

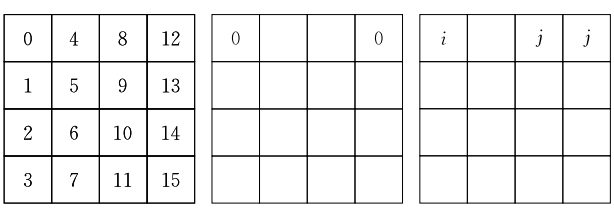
类似定理 1 的分析过程，利用定理 4 给出 6 轮 8 维平衡 Biclique 攻击的复杂度分析结果.

定理 4.　基于 6 轮 8 维的平衡 Biclique 结构可以恢复全轮 LBlock 算法主密钥，其数据复杂度为 2^{60}，存储复杂度为 $2^{16.07}$，时间复杂度为 $2^{78.14}$.

5　AES-128 算法的改进 Star 攻击

本节主要对 AES-128 算法的 Star 攻击结果进行了改进，通过扩展 Star 结构的轮数，使用密文方向 2.5 轮 Star 结构降低攻击的时间复杂度. 本节使用 \$0，\$1，\$2，…来表示圈子密钥.

(1) 密钥空间划分. 由于 AES-128 的密钥扩展算法是双射，将主密钥一一映射至第 10 轮圈子密钥 \$10，因此我们可以对第 10 轮圈子密钥 \$10 的空间进行划分，然后通过映射完成对主密钥空间的划分. $K[0,0]$表示第 0 字节 $\$10_0$、第 12 字节 $\$10_{12}$ 为 0，其余字节遍历的所有 2^{112} 个密钥. $\{K[i,0]\}$表示在 $K[0,0]$的基础上，$\$10_0$ 遍历所有可能值所形成的密钥子空间. $\{K[0,j]\}$表示在 $K[0,0]$的基础上，$\$10_8$ 与 $\$10_{12}$ 遍历所有可能值所形成的密钥子空间. 因此，将第 10 轮圈子密钥 \$10 空间划分为了 2^{112} 个规模为 2^{16} 的密钥子空间，如图 8 所示.



(a) AES状态　(b) 密钥划分关系　(c) 活动比特位置

图 8　AES-128 状态表示

(2) Star 结构的构造. 在 AES-128 算法的密文方向处构造 8 维 2.5 轮的 Star 结构，两条相关密钥差分路径如图 9 所示，可以看出两条相关密钥差分路径中的活动 S 盒不相交.

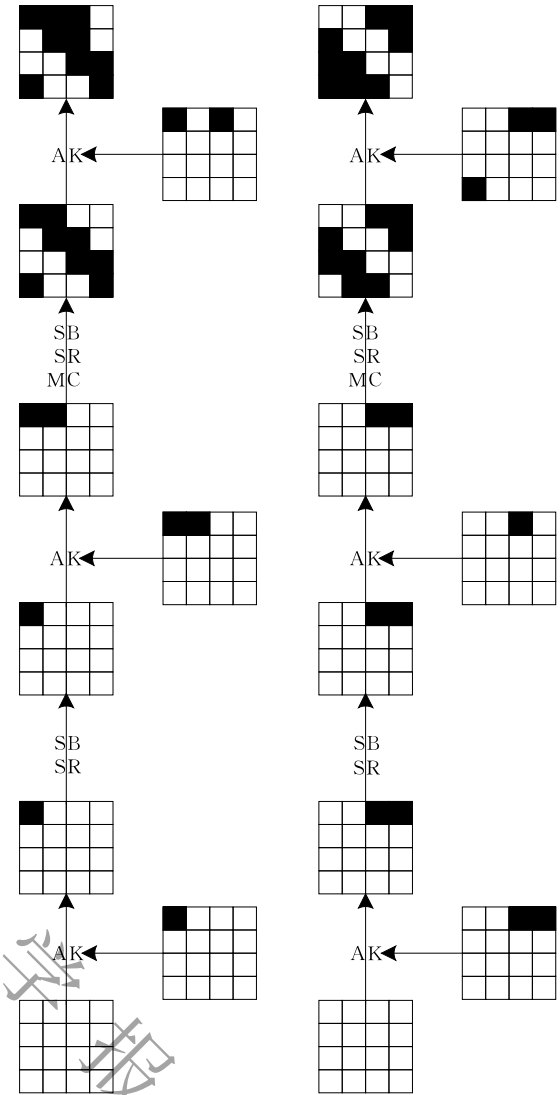


图 9　AES-128 算法的 Star 结构

(3) 计算圈子密钥. 对每一个第 10 轮圈子密钥 $K[i,j]$，计算出对应的 10 轮圈子密钥 \$0，\$1，…，\$9. 密钥扩展算法中，生成每个圈子密钥的第一列时需要使用非线性变换 S 盒，因此可以利用预计算与重计算技术降低这部分的时间复杂度，其余三列仅需要 xor 运算，因此这部分时间复杂度可以忽略[8].

在预计算阶段，预计算 $K[i,0]$与 $K[0,j]$为主密钥时的前 10 个圈子密钥，至多需要执行 2×2^{8} 次 10 圈子密钥扩展算法；

在重计算阶段，计算 $K[i,j]$为主密钥时前 10 个圈子密钥. 只需要简单的 xor 计算与查表操作. 白色表示在预计算阶段可以得到的，黑色表示在重复计算阶段重复计算的 S 盒. 对 * 标识的字节值进行存储，对◦标识字节的 S 盒输出值进行存储，进一步减少了计算的 S 盒数量，如图 10 所示.

《计算机学报》

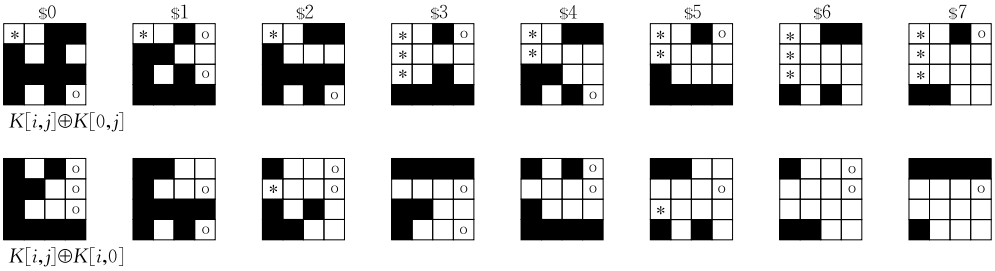


图 10 AES-128 算法的圈子密钥活动性

(4) 7.5 轮匹配过程. 检测加密所使用的密钥是否属于密钥子空间$\{K[i,j]\}$. 以 4 轮加密后的第 0 个字节为匹配位置,因此只需要重计算第 4 轮的 4 个字节,第 5 轮的 1 个字节,第 6 轮的 4 个字节. 同时,利用预计算与重复计算技术,在第 0 轮与第 7 轮处可以减少时间复杂度. 在第 0 轮仅需要重复计算 5 个字节,在第 7 轮仅需要重复计算 2 个字节. 具体如图 11 所示.

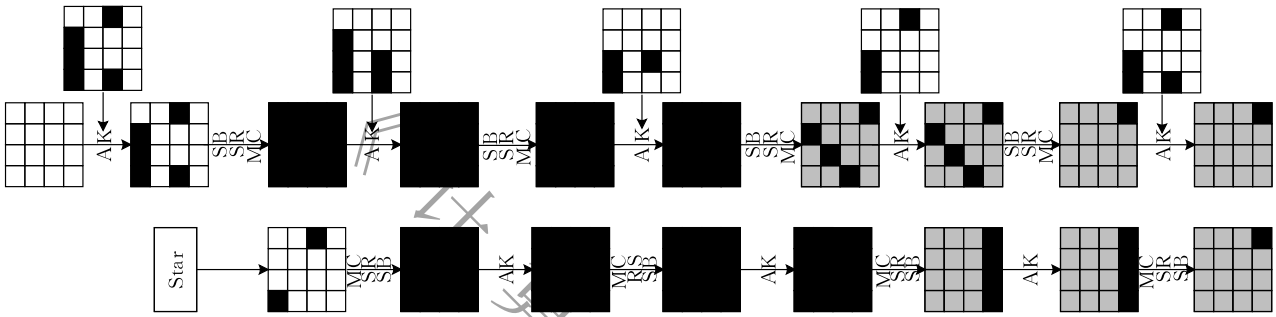


图 11 AES-128 算法 Star 攻击的 7.5 轮匹配过程

相比文献[7]中 AES-128 算法明文方向的 Star 攻击,上述攻击在匹配过程中减少了 2 个重复计算的 S 盒,从而降低了时间复杂度. 定理 5 给出了改进 AES-128 的 Star 攻击的复杂度分析结果.

定理 5. 基于密文方向的 2.5 轮 Star 结构,可以恢复全轮 AES-128 算法的主密钥,数据复杂度为 2,存储复杂度为 $2^{21.01}$,时间复杂度为 $2^{126.66}$.

证明. 存储复杂度. 需要存储 Star 结构和在线攻击阶段中所预计算的状态值. Star 结构包括 2^{16} 个中间状态,1 个密文状态,每一个都是 16 字节,共需$(2^{16}+1)\times 16$ 字节;在密钥扩展算法中需要存储 $2^8\times(24+17)$ 个字节;在匹配阶段,需要存储第 1 轮 11 个字节,第 8 轮需要存储 14 个字节,共 $2^8\times(11+14)$ 个字节. 因此,攻击的存储复杂度为 $(2^{16}+1)\times 16+2^8\times(24+17)+2^8\times(11+14)=2^{21.01}$ 个字节.

时间复杂度. AES-128 算法中共有 200 个 S 盒(加密算法 160 个,密钥扩展算法 40 个). 对每一个密钥子空间攻击中,时间复杂度含以下几部分:

(1) Star 结构构造. 构造一个 2.5 轮 Star 结构需要 2.5 轮基本运算,预计算 32 个 S 盒,重计算 19 个 S 盒,共计算 $2^8\times 19+32=4896$ 个 S 盒;

(2) 匹配过程. 前向匹配过程中重计算 41 个 S 盒,预计算 11 个 S 盒;后向匹配过程中重计算 37 个 S 盒,预计算 14 个 S 盒. 共计算了 $2^8\times((41+37)\times 2^8+11+14)=5\,118\,208$ 个 S 盒;

(3) 密钥扩展算法. 预计算阶段需要对每一个规模为 2^8 的 $K[i,0]$ 与 $K[0,j]$ 求出 10 轮的圈子密钥,而重复计算阶段仅由查表与 xor 操作构成因此不考虑重复计算的复杂度. 因此,整个密钥扩展算法需要预计算 $2\times 2^8\times 40$ 个 S 盒,重计算 0 个 S 盒. 共计 $2\times 2^8\times 40=20\,480$ 个 S 盒;

(4) 筛选候选密钥. 对候选密钥进一步筛选的时间复杂度. 每个密钥子空间的规模为 2^{16},错误密钥通过匹配检测的概率为 2^{-8},因此需要候选密钥集的规模为 $2^{16}\times 2^{-8}=2^8$,需要进行 2^8 次全轮 AES-128 加密运算.

综合上述 4 种时间复杂度,可以得到总的时间复杂度为

$$C=2^{112}\left(\frac{4896+5\,118\,208+20\,480}{200}+2^8\right)\approx 2^{126.66}.$$

证毕.

6 总结及未来研究方向

本文提出了一个新的高维 Biclique 结构构造方法,利用低维平衡 Biclique 结构构造高维 Biclique

结构，降低了搜索 Biclique 结构的复杂度；同时提出了一个完整的广义 Biclique 攻击框架，能够自动化完成对算法在广义 Biclique 攻击下的安全性综合评估，简化了算法在 Biclique 攻击下安全性分析工作；同时对 LBlock 算法在广义 Biclique 攻击下的安全性进行了综合评估，本文所得到的结果与现有结果对比如表 2 所示. 对 AES-128 算法在 Star 攻击下的安全性进行了改进，进一步降低了时间复杂度，如表 3 所示.

表 2　LBlock 算法的 Biclique 及其改进攻击结果

攻击方法	轮数	数据	时间	存储	出处
(8,4)-BB	32	2^{52}CP	$2^{78.40}$	2^{8}	[19]
(9,3)-BB	32	2^{64}CP	$2^{78.7}$	—	[11]
(6,4)-BB	32	2^{40}CP	$2^{78.425}$	$2^{9.47}$	Sect. 4. 2. 2
(6,8)-BB	32	2^{60}CP	$2^{78.14}$	$2^{16.07}$	Sect. 4. 3. 2
2-Step Matching	18	2^{17}CP	2^{78}	2^{17}	[20]
高阶密钥区分攻击	32	2KP	$2^{78.338}$	2^{7}FC	[21]
(6,4)-Star	32	2KP	$2^{78.66}$	$2^{11.31}$	Sect. 4. 2. 3
(6,4,8)-UB	32	2^{64}CP	$2^{78.24}$	$2^{14.81}$	Sect. 4. 3. 3

表 3　全轮 AES-128 算法的 Biclique 攻击结果

攻击方法	数据	时间	存储	出处
(3,8)-BB	2^{88}CP	$2^{126.21}$	$2^{14.32}$	[5]
(3,8)-BB	2^{72}CP	$2^{126.72}$	2^{8}	[15]
(3,8)-BB	2^{48}CP	$2^{126.37}$	—	[17]
(3,8)-BB	2^{58}CP	$2^{126.28}$	—	[17]
(3,8)-BB	2^{88}CP	$2^{126.18}$	—	[17]
(3,16)-BB	2^{72}CP	$2^{126.01}$	$2^{26.14}$	[8]
(3,8,16)-UB	2^{56}CP	$2^{126.13}$	$2^{22.07}$	[8]
(1,8)-Star	2 KP	$2^{126.67}$*	$2^{14.32}$	[7]
(2.5,8)-Star	2 KP	$2^{126.66}$	$2^{21.01}$	Sect. 5

注：* 按照本文的计算方法时间复杂度为 $2^{126.70}$.

针对密码算法的 Biclique 攻击，一般是通过构造新的 Biclique 结构，结合预计算与重复计算技术降低其时间复杂度，而由于各密码算法的扩散性不同，所得到的改进效果也不同. LBlock 算法能够存在优于穷举攻击的 Biclique 攻击结果，主要原因是圈子密钥与主密钥之间存在比特对应关系，密钥扩展算法的扩散性较弱，可以构造得到多条不相交的差分路径，从而存在高维的 Biclique 结构；同时，主算法的扩散性较弱，存在较长轮数的区分器，两者结合能够有效地降低攻击的复杂度.

AES-128 算法在最后一轮只有字节代替、行移位、密钥模加操作，没有列混合操作，根据分枝数理论可以构造较长轮数的 Star 结构，而在同维数下增加 Star 结构的轮数能够降低攻击的时间复杂度.

普适性与自动化分析水平提高的同时，导致分析的精细度不够. 在构造低维 Biclique 结构时，划分密钥空间的维数没有明确的界定，因此构造低维 Biclique 结构与构造高维 Biclique 结构的过程中进行了重复搜索，框架的运行效率有待进一步提高.

致　谢　向各位辛勤工作的编辑老师和对本文提出宝贵修改意见的评审老师致以衷心的感谢！

参　考　文　献

[1] Khovratovich D, Rechberger C, Savelieva A. Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family//Proceedings of the Fast Software Encryption-FSE 2012. Washington, USA, 2012: 244-263

[2] Aoki K, Sasaki Y. Preimage attacks on one-block MD4, 63-step MD5 and more//Proceedings of the Selected Areas in Cryptography-SAC 2008. New Brunswick, Canada, 2008: 103-119

[3] Aoki K, Sasaki Y. Meet-in-the-middle preimage attacks against reduced SHA-0 and SHA-1//Proceedings of the CRYPTO 2009. Santa Barbara, USA, 2009: 70-89

[4] Guo J, San L, Rechbeger C, Wang H. Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2//Proceedings of the ASIACRYPT 2010. Singapore, 2010: 56-75

[5] Bogdanov A, Khovratovich D, Rechbeger C. Biclique cryptanalysis of the full AES//Proceedings of the ASIACRYPT 2011. Seoul, South Korea, 2011: 344-731

[6] Canteaut A, Naya-Plasencia M, Vayssiere B. Sieve-in-the-middle: Improved MITM attacks//Proceedings of the CRYPTO 2013. Santa Barbara, USA, 2013: 222-240

[7] Bogdanov A, Chang D, Ghosh M, Sanadhya S K. Biclique with minimal data and time complexity for AES//Proceedings of the Information Security and Cryptology-ICISC 2014. Seoul, Korea, 2014: 160-174

[8] Tao B, Wu H. Improving the Biclique cryptanalysis of AES//Proceedings of the ACISP 2015. Brisbane, Australia, 2015: 39-56

[9] Hong D, Koo B, Kwon D. Biclique attack on the full HIGHT//Proceedings of the Information Security and Cryptology-ICISC2011. Seoul, Korea, 2011: 365-374

[10] Ahmadi S, Ahmadian Z, Mohajeri J, et al. Low-data complexity Biclique cryptanalysis of block ciphers with application to Piccolo and HIGHT. IEEE Transactions on Information Forensics and Security, 2014, 9(10): 1641-1652

[11] Karakoc F, Demirci H, Harmanci A E. Biclique cryptanalysis of LBlock and TWINE. Information Processing Letters, 2013, 113(12): 423-429

[12] Jeong K, Kang H, Lee C, et al. Weakness of lightweight block ciphers mCrypton and LED against Biclique cryptanalysis. Peer-to-Peer Networking and Applications, 2015, 8(4): 716-732

[13] Lee C. Biclique cryptanalysis of PRESENT and LED lightweight ciphers. Journal of Supercomputing, 2014, 70(1): 95-103

计算机学报

[14] Ahmadian Z, Salmasizadeh M, Aref M S. Biclique cryptanalysis of the full-round KLEIN block cipher. IET Information Security, 2015, 9(5): 294-301

[15] Abed F, Forler C, List E, et al. A Framework for automated Independent-Biclique cryptanalysis//Proceedings of the Fast Software Encryption-FSE 2013. Singapore, 2013: 561-581

[16] Gong Zheng, Liu Shu-Sheng, Wen Ya-Min, et al. Biclique cryptanalysis using balanced complete bipartite subgraphs. Science China Information Sciences, 2016, 59(4): 1-3

[17] Li Yun-Qiang, Zhang Xiao-Yong, Wang Ai-Lan. Distribution characteristics of the AES-128 Biclique structure. Journal of Electronics & Information Technology, 2016, 38(1): 135-140(in Chinese)
(李云强，张小勇，王爱兰. AES-128 Biclique 结构的分布特征. 电子与信息学报，2016，38(1)：135-140)

[18] Wu Wen-Ling, Zhang Lei. LBlock: A lightweight block cipher //Proceedings of the Applied Cryptography and Network Security-ACNS 2011. Nerja, Spain, 2011: 327-344

[19] Wang Yan-Feng, Wu Wen-Ling, Yu Xiao-Li, et al. Security on LBlock against Biclique cryptanalysis//Proceedings of the Information Security Applications-WISA 2012. Jeju Island, Korea, 2012: 1-14

[20] AlTawy R, Youssef A M. Differential sieving for 2-step matching meet-in-the-middle attack with application to LBlock//Proceedings of the Lightweight Cryptography for Security and Privacy-LightSec 2014. Istanbul, Turkey, 2014: 126-139

[21] AlTawy R, Tolba M, Youseef A M. A higher order key partitioning attack with application to LBlock. Global Change Biology, 2015, 19(6): 1804-1815

CUI Jing-Yi, born in 1992, M. S. candidate. His research interests include design and cryptanalysis on symmetric cryptology.

GUO Jian-Sheng, born in 1972, Ph. D., professor. His research interests include information security and cryptology theory.

LIU Yi-Peng, born in 1992, M. S. candidate. His research interests include information security and quantum cryptology.

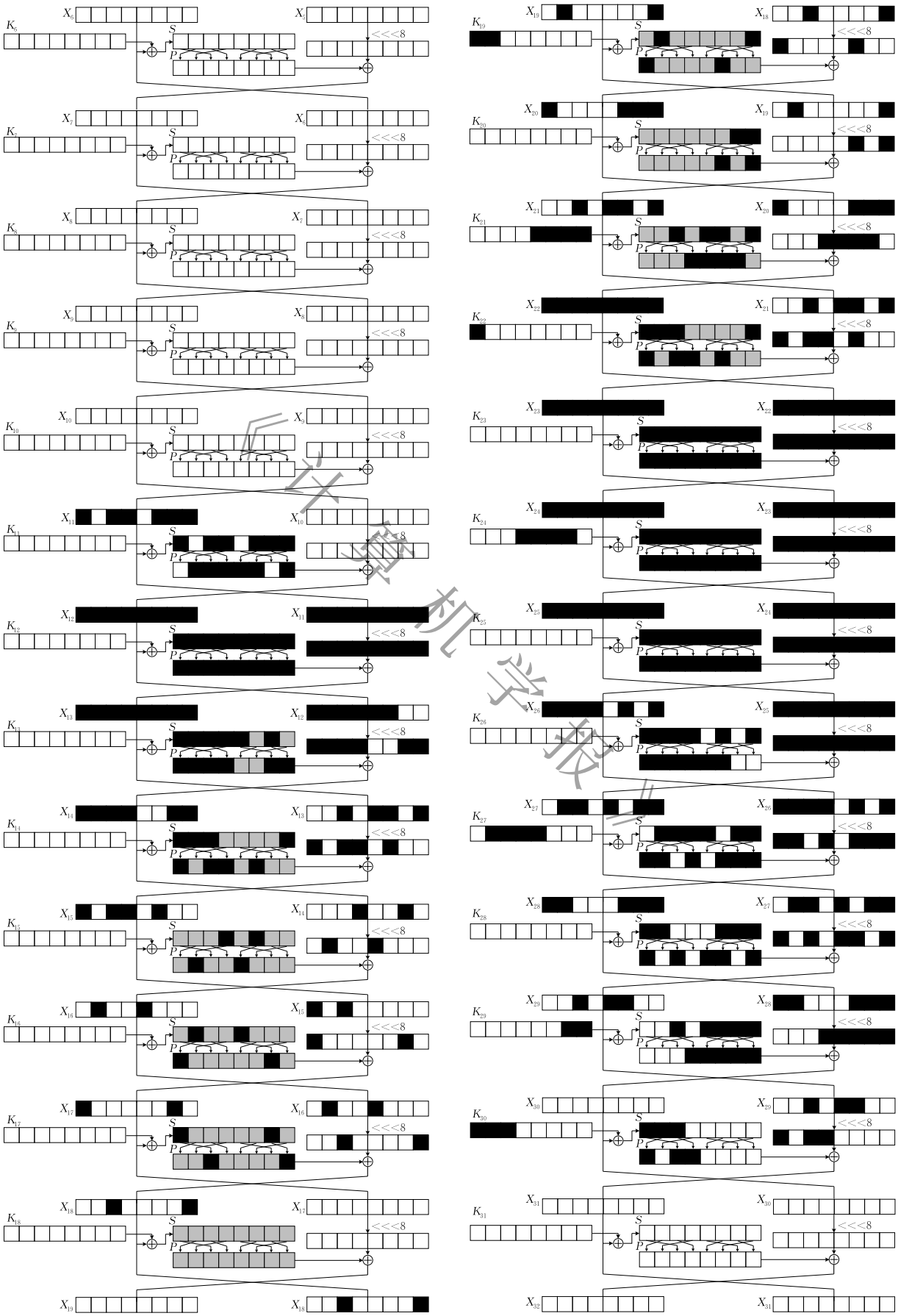
《计算机学报》

Background

Biclique cryptanalysis was first proposed to analyze hash function and it was introduced to attack block cipher in 2011. Biclique attack on AES demonstrated a great power on iterative block ciphers. Khovratovich et al. gave the first attack on full-round of three variants of AES in the single key setting which interested many cryptographers around the world. Biclique cryptanalysis was used to attack many block ciphers such as CLEFIA, ARIA, Camellia, KLEIN, HIGHT, Piccolo, TWINE, PRESENT and PRINCE.

Biclique cryptanalysis is based on the structure called Biclique, which is a complete bipartite graph. Combined with meet-in-the-middle attack, Biclique attack could attack full-round of block ciphers. In 2011, Khovratovich et al. introduced Biclique attack to give the first full-round attack on AES whose time complexity is lower than exhaustive search. In 2013, Canteaut et al. concentrated on meet-in-the-middle attack used in Biclique cryptanalysis and sieve-in-the-middle technique was proposed to improve the time complexity. Later, people found that the improvement of the contracture could also improve the complexity. In 2014, Bogdanov et al. introduced a new structure "Star" which could give the attack on AES with the minimal data complexity. In 2015, Tao et al. claimed that the unbalanced Biclique could greatly improve the time complexity.

People desired to attack the block cipher automatically. In 2014, F. Abed et al. proposed a framework to find the Biclique automatically by using the computer. And they found the balanced Biclique of AES and BKSQ. In 2016, Gong et al. proposed to use mathematic method to solve this problem. Li et al. found all balanced Bicliques of AES-128 by programming. In our work, we want to search balanced Biclique, Star and unbalanced Biclique together and give the meet-in-the-middle attack at the same. We proposed a definition of generalized Biclique to cover all kinds of Biclique. Based on the generalized Biclique, a framework was introduced that could search generalized Biclique and find a suitable match to complete the whole Biclique attack on the specific block cipher. In the end, we gave the full-round attacks on LBlock with the minimal data complexity and lower time complexity than those known before. And we also improved the attack on AES-128 with 2 known plaintexts.

This paper is funded by the China Postdoctoral Science Foundation (2014M562582).

附录 1.　(6,4,8)-非平衡 Biclique 攻击的 26 轮匹配过程.