多维零相关线性分析模型的改进及在 23 轮 LBlock-s 算法中的应用

李灵琛[1),2)] 吴文玲[1)] 汪艳凤[1)]

[1)](中国科学院软件研究所可信计算与信息保障实验室 北京 100190)

[2)](中国科学院大学 北京 100190)

摘 要 基于相关性为零的线性逼近的多维零相关线性密码分析是目前最重要的分组密码分析手段之一.该文主要对多维零相关线性分析模型的密钥恢复阶段进行了深入的研究,通过定义等价密钥的距离来刻画等价密钥在压缩表达式中的位置关系,进一步约简区分器候选集合同时优化密钥猜测顺序,从而改进了原有的多维零相关线性分析的攻击模型.改进的模型首先找到所有最长的多维零相关线性区分器,然后利用密钥编排算法求得密钥恢复阶段所涉及的独立猜测密钥量,以此筛选区分器候选集合.最后,根据等价密钥的距离对候选区分器进行再次筛选,同时得到相应的密钥猜测顺序.LBlock-s 算法是 CAESAR 竞赛中所提交的认证加密算法 LAC 的核心分组算法.与 Lblock 算法不同,LBlock-s 采用具有更快混淆速度的密钥编排算法.基于改进的优化模型,该文分析了该算法抵抗多维零相关线性攻击的能力.研究表明,攻击 23 轮 LBlock-s 算法所需的数据复杂度为 $2^{62.3}$ 个选择明文,时间复杂度为 $2^{73.75}$ 次 23 轮 LBlock-s 加密,存储复杂度为 2^{56} 字节.这是目前针对 LBlock-s 算法的最优攻击结果.

关键词 分组密码;LBlock-s;多维零相关线性分析;逐步压缩技术;等价密钥

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2017.01192

Improved Multidimensional Zero-Correlation Linear Cryptanalysis and Applications to 23-Round LBlock-s

LI Ling-Chen[1),2)] WU Wen-Ling[1)] WANG Yan-Feng[1)]

[1)](*Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

[2)](*University of Chinese Academy of Sciences, Beijing* 100190)

Abstract Multidimensional zero-correlation linear cryptanalysis is a novel promising technique for block cipher. The distinguishing property used in the multidimensional zero-correlation linear cryptanalysis is the existence of zero-correlation linear hulls over a part of the cipher. In general, we take advantage of the partial-compression technique and the equivalent relations of guessed keys to reduce the complexity in the key recovery attack. In this paper, we mainly deeply research techniques in the key recovery attack and give an improved model of multidimensional zero-correlation linear cryptanalysis. For most ciphers, there are a large number of the longest zero-correlation linear hulls with the same dimension. The active position of the zero-correlation linear hull and key schedule algorithm decide the number of guessed keys and influence the result

收稿日期:2016-05-30;在线出版日期:2017-02-24.本课题得到国家"九七三"重点基础研究发展规划项目(2013CB338002)和国家自然科学基金(61272476,61232009,61202420)资助.**李灵琛**,女,1988 年生,博士研究生,主要研究方向为对称密码分析.E-mail:lilingchen@tca.iscas.ac.cn.**吴文玲**,女,1966 年生,博士,研究员,博士生导师,中国计算机学会(CCF)会员,主要研究领域为分组密码的设计与分析、分组密码工作模式和可证明安全理论的研究.**汪艳凤**,女,1989 年生,博士,主要研究方向为分组密码的分析与设计.

of security evaluation. The existing model regards the distinguishers with the least independent guessed keys as the optimal distinguishers. However, we found that the location of the equivalent keys in the compress expression and the order of guessed keys in partial-compression have an important influence on complexity. We introduced a new definition of the distance of equivalent keys. The distance of equivalent keys and is the number of extra guessed keys to obtain the compression of and after guessing one of them. Obviously, the distance of equivalent keys is proportional to the number of extra guessed keys. According to all the distance of equivalent keys, we can sieve to optimal distinguishers and obtain the order of guessed keys. In improved attack model, the following steps are processed to obtain the multidimensional zero-correlation linear attack on r-round cipher: Step1, find out all the longest multidimensional zero-correlation linear distinguishers for cipher by using the matrix method or other properties of encryption algorithm. Step2, expand the distinguisher to r-round and compute the number of related round keys. Save distinguishers with the least number of keys and the round number of partial encryption/decryption in set S. Step3, obtain the distinguishers with the least independent guessed keys from S by taking the key schedule algorithm and save the result in set O. Step4, minimize the set O to an optimal set L by using the distance of the equivalent keys. We need to compute all the distance of the equivalent keys. The distinguishers with the shortest distance will be saved. Step5, choose an element in set L to implement the key recovery attack. According to distances, we get the order of guessed keys. Obviously, the equivalent keys with the short distance should be guessed firstly. To demonstrate the practical impact of our attack's model, we applied the improved multidimensional zero-correlation linear cryptanalysis model to 23-round LBlock-s. LBlock-s is the kernel block cipher of the authentication encryption algorithm LAC. LBlock-s is an improved version of LBlock with 64-bit block size and 80-bit key size. The general structure of LBlock-s is a variant of Feistel Network. The number of iterative rounds is 32. Different from the LBlock, LBlock-s adopts an improved key schedule algorithm with a faster diffusion speed. We obtained a key recovery attack on 23-round LBlock-s by adding 5-round before and appending 4-round after the 14-round distinguisher ($0a000000$, 00000000)$\rightarrow$(00000000, $0000000b$). The result shows that the multidimensional zero-correlation linear attack on 23-round LBlock-s requires $2^{62.3}$ known plaintexts, $2^{73.75}$ 23-round LBlock-s encryption and 2^{56} bytes memory. As far as we know, this is the currently best result on LBlock-s.

Keywords　block cipher; LBlock-s; multidimensional zero-correlation linear cryptanalysis; partial-compression technique; equivalent keys

1　引　言

零相关线性分析最早由 Bogdanov 和 Rijmen 提出[1],此分析方法寻找密码算法概率为 1/2 即相关性为 0 的线性逼近作为零相关线性分析的区分器.该方法已被用于多个分组密码算法的安全性分析,例如 AES(Advanced Encryption Standard)、TEA(Tiny Encryption Algorithm)、CAST-256 等.但是,此区分器下的数据复杂度为全密码本或者一半密码本的选择明文量.为了降低零相关线性分析的数据复杂度,Bogdanov 等人[2]提出多重零相关线性分析,通过联合多条零相关线性逼近来降低攻击所需的数据复杂度,但是不同的零相关线性逼近需满足独立性假设.随后,又去掉了在多重零相关线性分析中线性逼近的独立性假设的要求,并给出了更完备的零相关线性分析理论——多维零相关线性分析[3].多维零相关线性分析已然成为当今最重要的分组密码分析方法之一.

2014 年,Wang 等人[4]探究了分组密码密钥编

排对多维零相关线性分析的影响,选择涉及独立猜测密钥量最少的区分器作为最优区分器,从而完善了多维零相关线性分析的攻击模型,并利用该模型得到了 23 轮 LBlock 算法,23 轮 TWINE-80 算法和 25 轮 TWINE-128 算法的多维零相关线性分析结果.但是,经过本文研究发现该模型仍然存在着一些不足的地方:

首先,原有模型中最后筛选得到的独立密钥量最少的候选区分器并不都是最优区分器.区分器的输入输出活跃位置决定了密钥恢复阶段中部分加解密需要猜测的密钥具体值.显然,是否能选择到真正最优的区分器将会直接影响密钥恢复阶段的分析.从而,本文的改进模型首先要对原有模型所得到的最优候选区分器进行二次筛选;

其次,密钥恢复阶段没有明确说明如何选择轮密钥的猜测顺序.研究表明轮密钥猜测顺序影响着部分压缩阶段的时间和存储复杂度,而这些阶段的复杂度对攻击的整体复杂度是有决定性影响的.如果密钥猜测顺序选择不当,就算是基于独立猜测密钥量最优的区分器也无法得到算法的最优攻击结果.于是,给定密钥恢复攻击的密钥猜测策略是十分必要的.

本文对原有多维零相关模型存在的不足之处进行改进,其想法主要来源于等价密钥对逐步压缩阶段复杂度的影响.分组密码算法特别是轻量级的分组密码算法,其密钥编排算法过于简单,使得密钥恢复阶段包含的猜测密钥中存在等价关系,而等价密钥的存在降低了猜测密钥总数,也使得逐步压缩阶段的压缩效果更好,即所需要的时间更短,存储复杂度更低.但是,逐步压缩阶段的复杂度除了受等价密钥的数量影响之外,还与等价密钥在压缩表达式中的具体位置有关.

改进的多维零相关线性分析的攻击模型是建立在原有的攻击模型基础之上的,不仅继承了原有模型的优点,也改进了其不足之处.新的攻击模型的优化之处主要体现在:

一方面,对独立密钥量最少的候选区分器进行二次筛选.本文通过定义等价密钥间的距离来刻画其在压缩状态表达式中的位置关系,以此筛选出最优的区分器;

另一方面,提出逐步压缩技术中的轮密钥猜测策略.研究表明等价密钥的距离也决定着在逐步压缩过程中的密钥猜测策略,遵循该策略才能够得到最优的攻击复杂度.

为了证明该优化模型的实用性,本文对 23 轮 LBlock-s 算法抵抗多维零相关线性分析的安全性进行了重新评估.LBlock-s 算法①是认证加密算法 LAC 中所使用的核心分组密码算法,采用了与 LBlock 算法[5]相同的加解密结构,不同之处是 LBlock-s 算法采用了基于半字节的密钥编排算法,具有较 LBlock 密钥编排算法更快的混淆速度.密钥编排算法改进的主要目的是能够更好地抵抗双系分析[6].但是基于半字节的密钥编排算法使得所呈现出的轮密钥等价关系变得更加明确,这将更有利于攻击者分析多维零相关线性分析中涉及的猜测密钥间的等价关系.ICICS'15,Xu 等人[7]基于 Wang 等人[4]的多维零相关线性分析的攻击模型给出了 23 轮 LBlock-s 算法的多维零相关线性分析结果.本文的研究表明其最终得到的 4 种候选区分器并不都是最优的,并且在逐步压缩阶段的密钥猜测顺序没有使得攻击复杂度达到最优[7].基于新的攻击模型,本文给出了 23 轮 LBlock-s 算法的多维零相关线性分析的最新结果,缩短了时间并降低了存储复杂度,这也是目前针对 LBlock-s 算法的最优攻击结果.表 1 给出了本文与已有攻击结果的对比.

表 1 23 轮 LBlock-s 算法分析结果对比

攻击方法	轮数	数据复杂度	时间复杂度	存储复杂度	参考文献
双系分析	32	$2^{12}CP$	$2^{78.74}$	\	[8]
不可能差分分析	21	$2^{63}CP$	$2^{67.61}$	\	[9]
多维零相关线性分析	23	$2^{62.3}KP$	$2^{75.4}$	2^{60} bytes	[7]
多维零相关线性分析	23	$2^{62.3}KP$	$2^{73.75}$	2^{56} bytes	本文

注:CP 表示选择明文,KP 表示已知明文.

本文第 2 节简单介绍零相关线性分析的相关定义和原理;第 3 节给出等价密钥距离的定义和优化的多维零相关线性分析的攻击模型;第 4 节首先对 LBlock-s 算法进行简单介绍,随后给出基于改进模型的 23 轮 LBlock-s 算法的多维零相关线性攻击的详细过程;第 5 节,全文总结,并给出有待下一步研究的问题.

2 零相关线性密码分析

本节首先介绍与零相关线性区分器相关的基本

① Zhang L, Wu W, Wang Y, et al. LAC: A lightweight authenticated encryption cipher. http://competitions.cr.yp.to/round1/lacv1.pdf

概念和引理，随后给出多维零相关线性密码分析模型的基本原理.

2.1　零相关线性区分器

考虑一个 n 比特的分组密码 f，函数的输入为 $x\in F_2^n$，线性逼近 (u,v) 成立的概率为

$$p(u\cdot x,v\cdot f(x))=Pr_{x\in F_2^n}\{u\cdot x\oplus v\cdot f(x)=0\},$$

其中：u 为线性逼近的输入掩码；v 为线性逼近的输出掩码. 则线性逼近 (u,v) 的相关性为

$$c(u\cdot x,v\cdot f(x))=2p(u\cdot x,v\cdot f(x))-1.$$

分组密码的轮函数通常涉及 3 个基本的操作：异或操作、分支操作和可逆函数. 线性掩码在 3 个操作下的传播规则如下[1].

引理 1.　异或操作. 如果 $h(x_1,x_2)=x_1\oplus x_2$，那么当且仅当 $u_1=u_2=v$，$c(u_1\cdot x_1\oplus u_2\cdot x_2,v\cdot h(x_1,x_2))\neq 0$. 其中，$h$ 函数表示的是两个输入值的异或.

引理 2.　分支操作. 如果 $h(x)=(x,x)$，那么当且仅当 $u\oplus v_1\oplus v_2=0$，$c(u\cdot x,(v_1,v_2)\cdot h(x))\neq 0$.

引理 3.　可逆函数. 如果 $S(x)$ 为可逆函数，仅当输入掩码 u 和输出掩码 v 均为零或者均为非零时，$c(u\cdot x,v\cdot S(x))\neq 0$.

对于传统线性密码分析而言，通常选择相关度大的线性逼近作为区分器来区分分组密码算法与随机函数. 然而，零相关线性分析法则反其道而行之，利用相关性为零的线性逼近作为恢复密钥的区分器.

注意到，当且仅当 $c(u\cdot x,v\cdot f(x))=0$，线性逼近 (u,v) 成立的概率 $p(u\cdot x,v\cdot f(x))=\dfrac{1}{2}$. Soleimany 等人[10]提出在以上 3 条线性掩码的传播规则的基础上，能够利用矩阵方法和 miss-in-the-middle 技术来寻找最长轮的零相关线性逼近.

2.2　多维零相关线性分析

在多维零相关线性分析模型中，$l=2^m-1$ 条零相关线性逼近可以看作是由 m 条独立的零相关线性逼近扩展得到的，从而消除了多条零相关线性逼近相互独立的强假设条件.

已知 m 条独立的线性逼近：

$$(u_i,x)\oplus(v_i,y)=0,\ i=1,\cdots,m,$$

其中 x,y 分别表示加密过程子函数的输入和输出. 给定一对 (x,y)，可以同时计算 m 条线性逼近的值，得到 m 比特 z：

$$z=(z_1,\cdots,z_m),\ z_i=(u_i,x)\oplus(v_i,y).$$

对每个 $z\in F_2^m$，攻击者设置计数器 $V[z]$ 并初始化为全零. 对 N 个不同的状态对，计算 z 值并更新相应的计数器. 最后，计算统计值 T

$$T=\sum_{z=0}^{2^m-1}\frac{(V[z]-N\cdot 2^{-m})^2}{N\cdot 2^{-m}(1-2^{-m})}$$

$$=\frac{N\cdot 2^m}{1-2^{-m}}\sum_{z=0}^{2^m-1}\left(\frac{V[z]}{N}-\frac{1}{2^m}\right)^2.$$

统计值 T 服从 χ^2 分布. 在正确密钥下，其均值为 $\mu_0=l\dfrac{2^n-N}{2^n-1}$，方差为 $\sigma_0^2=2l\left(\dfrac{2^n-N}{2^n-1}\right)$. 在错误密钥下，其均值为 $\mu_1=l$，方差为 $\sigma_1^2=2l$. 令 α 为 type-1 型错误（正确密钥被删除），β 为 type-2 型错误（错误密钥被接受）. 那么，区分阈值为 $\tau=\mu_0+\sigma_0 z_{1-\alpha}=\mu_1+\sigma_1 z_{1-\beta}$. 并且，攻击所需的数据复杂度为

$$N'=\frac{2^n(z_{1-\alpha}+z_{1-\beta})}{\sqrt{l/2}+z_{1-\alpha}},$$

其中，$z_p=\Phi^{-1}(p)$，$0<p<1$，Φ 为标准正态分布的累积分布函数[2].

3　改进多维零相关线性密码分析的攻击模型

本节将对 Wang 等人[4]的多维零相关线性分析模型中的不足之处进行改进. 首先对等价密钥和逐步压缩技术进行更仔细的分析，给出等价密钥的距离定义，然后给出本文优化的 r 轮多维零相关线性分析的攻击模型.

3.1　改进动机

利用密钥编排的弱点，例如等价密钥、弱密钥[11]等，来改进攻击的复杂度的方式已在密码分析中得到了广泛的应用. 通常，在多维零相关线性分析中，分组算法存在多个同维数同轮数的零相关线性区分器. 由于算法特别是轻量级分组算法的密钥编排算法设计过于简单，部分加解密的轮密钥间存在明显的线性关系，即两个密钥可以看做是等价的关系，所以不同的活跃位置的零相关线性区分器在密钥恢复阶段所涉及的独立密钥猜测总量是不同的. 考虑独立密钥总量的多少来筛选最优区分器是原攻击模型的最大贡献. 但是仅仅考虑独立密钥猜测总量是不够的. 本文研究发现在密钥恢复阶段，独立密钥猜测总量相同的区分器在应用逐步压缩技术后得到的攻击复杂度仍然可能存在差异.

在密钥恢复阶段，将区分器的输入输出掩码位置的状态表示为明密文与密钥的表达式，通过逐字

节甚至逐比特猜测密钥,逐步压缩中间状态的规模,以降低攻击所需的时间复杂度.我们称该技巧为逐步压缩技术或部分和技术[12].通常,在逐步压缩过程中,一般的情况是猜测 n 比特密钥得到 n 比特压缩量.在存在等价密钥的情况下,在已知其中一个密钥后,可以不需要猜测另一个密钥也能获得状态压缩.但是,何时能免费获得这 n 比特的状态压缩还要看等价密钥在需要压缩的状态表达式中的具体位置.我们通过定义等价密钥的距离来衡量等价密钥在状态表达式中的位置关系.

定义 1. 等价密钥的距离.已知在逐步压缩过程中密钥 k_1 和 k_2 存在等价关系,称猜测 k_1(或者 k_2)后得到密钥 k_1 与 k_2 的状态压缩量所需要额外猜测的密钥最小量(以比特为单位)为等价密钥的距离,记为 $d(k_1,k_2)$.

逐步压缩技术实质上是一种时空折中的方法.我们总希望通过猜测越少的密钥量得到越多的压缩量.在逐步压缩过程中,前一步能够得到的压缩量对以后步骤的复杂度产生直接的影响.特别地,第一步的压缩量对该攻击能否执行起着决定性的作用.所以在具有等价密钥的情况下要尽可能早地利用等价密钥对状态进行压缩,最大化地减少进入下个步骤的状态量.对于不同距离的等价密钥,在选择密钥猜测顺序时要先猜测距离短的再猜测距离长的等价密钥.当然,等价密钥间需要借助额外的 d 比特密钥的猜测.观察 1 中的独立密钥是除服务于等价密钥之外的其余猜测密钥.

观察 1. 在逐步压缩过程中,前一步压缩后的状态规模与当前步骤的复杂度正相关.所以等价密钥优先于独立密钥的猜测,距离短的等价密钥优先于距离长的等价密钥.

通过下面的例子进一步说明在逐步压缩过程中,等价密钥的距离与表达式计算复杂度之间的关系.

例 1. 已知下面两个表达式中 k_1 和 k_2 存在等价关系:

$$x_4\oplus S(x_3\oplus S(x_2\oplus S(x_1\oplus k_1)\oplus k_2)\oplus k') \quad (1)$$

$$x_4\oplus S(x_3\oplus S(x_2\oplus S(x_1\oplus k_1)\oplus k')\oplus k_2) \quad (2)$$

其中:$x_1\sim x_4$,k_1,k_2 和 k' 都为 n 比特值.直接计算的两个表达式的时间复杂度为 $2^{4n+2n}\times 3$,存储复杂度为 2^n.采用逐步分压缩技术,表达式(1)的计算分两步:

1. 猜测 k_1 或 k_2,$3n$ 比特状态 $x_1|x_2|x_3$ 被压缩为 n 比特中间状态 y,$y=x_3\oplus S(x_2\oplus S(x_1\oplus k_1)\oplus k_2)$;

2. 猜测 k',得到最终状态 $z=x_4\oplus S(y\oplus k')$.

总的时间复杂度为 $2^{4n+n}\times 2+2^{2n+2n}$,存储复杂度为 $2^{2n}+2^n$.

类似地,表达式(2)的计算分两步:

1. 猜测 k_1,$2n$ 比特状态 $x_1|x_2$ 被压缩为 n 比特中间状态 y',$y'=x_2\oplus S(x_1\oplus k_1)$;

2. 猜测 k',由步骤 1 可以等价于已知 k_2,得到最终状态 $z'=x_4\oplus S(x_3\oplus S(y'\oplus k')\oplus k_2)$.

总的时间复杂度为 $2^{4n+n}+2^{3n+2n}\times 2$,存储复杂度为 $2^{3n}+2^n$.

易知,在表达式(1)中,$d(k_1,k_2)=0$,在表达式(2)中,$d(k_1,k_2)=n$.可见,表达式中等价密钥的距离越短,越有利于状态的压缩,所得到的复杂度也越低.表 2 给出了计算两个等式的复杂度比较结果.

表 2 表达式(1)与表达式(2)的复杂度比较

表达式	时间复杂度	存储复杂度
式(1)	$2^{4n+n}\times 2+2^{2n+2n}$	$2^{2n}+2^n$
式(2)	$2^{4n+n}+2^{3n+2n}\times 2$	$2^{3n}+2^n$

3.2 改进的攻击模型

根据 3.1 节对逐步压缩技术和等价密钥的分析,得到改进的 r 轮多维零相关线性密码分析的攻击模型.具体如下所示:

1. 基于算法部件的线性掩码传播规则,利用矩阵的方法找到所有可能的轮数最大的多维零相关线性区分器,总数记为 n,轮数记为 r_d,令 $site_{\text{in}}$ 与 $site_{\text{out}}$ 分别表示区分器的输入输出掩码的非零半字节位置.

2. 将得到的多维零相关线性区分器向前扩展 r_{in} 轮,向后扩展 r_{out} 轮,$r_{\text{in}}+r_d+r_{\text{out}}=r$,根据算法的轮函数迭代性质,计算每个扩展方案涉及的密钥猜测总量.选择部分加解密所涉及的密钥总量最少的四元组($site_{\text{in}}$,$site_{\text{out}}$,r_{in},r_{out}),$0\le r_{\text{in}}\le r-r_d$,$0\le r_{\text{out}}\le r-r_d-r_{\text{in}}$,将其结果保留在集合 S 中.

3. 将集合 S 约简为集合 O.考虑密钥编排算法,找到部分加解密过程所需要的猜测密钥之间的所有等价关系,得到实际猜测密钥量最少的四元组($site_{\text{in}}$,$site_{\text{out}}$,r_{in},r_{out}),结果保留在集合 O 中.

4. 将集合 O 约简为最优集合 L.此时,我们需要对集合 O 中的每个元素计算其涉及的所有的等价密钥的距离.对每个方案得到的距离进行比较,筛选等价密钥的距离最短的四元组($site_{\text{in}}$,$site_{\text{out}}$,r_{in},r_{out}),将结果保留在集合 L 中.

(a) 对集合 O 中的所有元素逐一计算所有等价密钥的距离.根据轮函数的迭代性质计算其压缩状

态表达式. 对表达式所涉及的所有等价密钥进行逐一分析，计算其距离. 假设 $(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})$ 共有 m 对等价密钥，所有等价密钥的距离按照由小到大的顺序存放于向量 $\boldsymbol{d}^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})}$ 中：

$$\boldsymbol{d}^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})} = (\boldsymbol{d}_1^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})}, \boldsymbol{d}_2^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})}, \cdots, \boldsymbol{d}_m^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})}),$$

其中 $\boldsymbol{d}_1^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})} \leq \boldsymbol{d}_2^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})} \leq \cdots \leq \boldsymbol{d}_m^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})}$.

(b) 比较所有的 $\boldsymbol{d}^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})}$. 若存在

$$\boldsymbol{d}^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})} < \boldsymbol{d}^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})'},$$

则将 $(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})'$ 从集合 O 中删除. $\boldsymbol{d}^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})} < \boldsymbol{d}^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})'}$ 表示存在 $i \leq m$ 使得 $\boldsymbol{d}_i^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})'} > \boldsymbol{d}_i^{(site_{\text{in}}, site_{\text{out}}, r_{\text{in}}, r_{\text{out}})}$.

5. 选择最优集合 L 中的任一元素，恢复 r 轮算法的秘密密钥(假设区分器的维数为 m).

(a) 用 z 表示 m 条零相关线性逼近值的级联. 对所有的 m 比特 z 设置计数器 $V[z]$，初始化为 0.

(b) 利用逐步压缩技术，逐步猜测轮密钥，部分加解密已知的明密文至区分器边界位置，更新相应的计数器 $V[z]$. 轮密钥猜测策略如观察 1 所示，优先利用等价密钥对状态进行压缩，多个等价密钥中先利用距离短的等价密钥.

(c) 对每个猜测的密钥 k，计算统计值 $T_k = \frac{N \cdot 2^8}{(1-2^{-8})} \sum_{z=0}^{2^8-1} \left(\frac{V[z]}{N} - \frac{1}{2^8} \right)^2$.

(d) 如果 $T_k < \tau$，那么视该 k 为可能的正确候选密钥.

(e) 穷搜剩下的候选密钥，找到唯一的正确密钥.

经过以上步骤，在新的攻击模型下，能够得到算法复杂度最优的 r 轮多维零相关线性分析. 并且，新的攻击模型是建立在原有攻击模型的基础之上的，继承了原有模型的优点，修正了原有模型的不足之处. 与原有模型相比较，其优化之处主要体现以下两个方面：

1. 对候选区分器的二次筛选. 在步骤 4 中，基于集合 O 中的不同区分器和轮扩展方案下所得到的等价密钥距离的不同，对集合 O 中的元素进行进一步约简，得到最优集合 L. 最优集合 L 中保留下来的区分器、轮扩展方案及其对应的等价密钥的距离保障了在 r 轮密钥恢复阶段的逐步压缩过程达到最优复杂度.

2. 给出逐步压缩阶段的轮密钥猜测策略. 该策略保障了逐步压缩阶段的数据复杂度和存储复杂度都达到最优. 在步骤 5(b) 的逐步压缩阶段，我们强调先利用等价密钥进行状态压缩，在存在多个等价密钥的情况下，要先选择距离短的等价密钥对状态进行最大化的压缩，由此才得到最优的压缩复杂度. 并且密钥恢复阶段的复杂度主要由逐步压缩阶段产生，所以对逐步压缩阶段的复杂度的降低亦是对算法的 r 轮攻击复杂度的降低.

4　LBlock-s 算法的分析

本节将对 23 轮 LBlock-s 算法抵抗多维零相关线性攻击的能力进行分析. 首先给出 LBlock-s 算法的简单描述，然后对 14 轮 LBlock-s 算法多维零相关线性区分器的筛选进行详细说明，最后给出 23 轮 LBlock-s 算法密钥恢复攻击的具体过程.

4.1　LBlock-s 算法简介

LBlock-s 的加解密算法与 LBlock 算法完全一样，不同之处在于其采用了改进版的密钥编排算法. LBlock-s 算法是 CAESAR 竞赛[①]提交的认证加密算法 LAC 的核心分组算法.

4.1.1　LBlock-s 算法的加密流程

LBlock-s 算法的分组长度为 64 比特，密钥长度为 80 比特. LBlock-s 加密算法采用变体的 Feistel 结构，具体如图 1 所示.

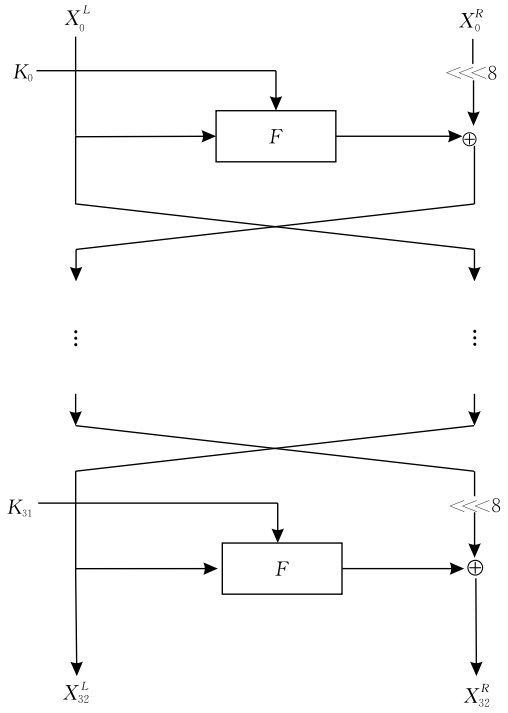

图 1　LBlock-s 的加密算法结构

① CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. http://competitions.cr.yp.to/caesar.html

LBlock-s 加密算法具体如下所示：

1. 输入明文 $P=(X_0^L,X_0^R)$

2. 对 $i=0\sim31$ 执行：

$$\begin{cases}X_{i+1}^L=F(X_i^L,K_i)\oplus(X_i^R\lll 8)\\X_{i+1}^R=X_i^L\end{cases}$$

3. 输出密文 $C=(X_{32}^L,X_{32}^R)$

LBlock-s 算法的轮函数主要包含 3 个基本变换：密钥加 AK，混淆层 S 和扩散层 P. 密钥加 AK 是简单的状态与密钥的异或运算；混淆层 S 包含 8 个不相同的 4 比特的 S 盒，$S_0\sim S_7$，具体内容见附录 1；扩散层 P 是对 8 个 4 比特的字进行置换操作. 轮函数的具体结构如图 2 所示.

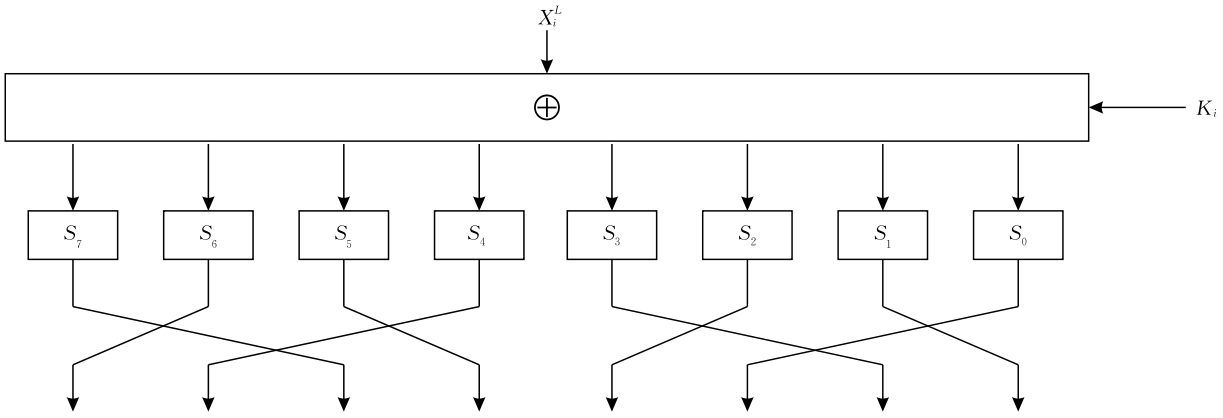

图 2 LBlock-s 算法的轮函数结构

4.1.2 LBlock-s 算法的密钥扩展方案

为了抵抗双系分析，LBlock-s 算法采用基于半字节的密钥编排算法，具有更快的混淆速度. 密钥编排算法将 80 比特的主密钥 MK 扩展为 32 个 32 比特的轮密钥.

LBlock-s 密钥编排算法具体如下所示：

1. $K_0=MK[0-31]$

2. 对 $i=1\sim31$ 执行：

(a) $MK=MK\lll 24$

(b)

$MK[24-27]=S_8(MK[0-3])\oplus MK[24-27]$

$MK[48-51]=S_9(MK[4-7])\oplus MK[48-51]$

$MK[12-15]=MK[8-11]\oplus MK[12-15]$

$MK[28-31]=MK[68-71]\oplus MK[28-31]$

(c) $MK[25-29]=MK[25-29]\oplus[i]_2$

(d) $K_i=MK[0-31]$

原有的密钥编排算法，见附录 2，即 LBlock 采用的密钥编排算法在步骤(a)采用的是循环左移 29 位，步骤(b)只用 2 个 S 盒对两个 4 比特的值进行更新，所以混淆太慢. 相比之下，改进后的密钥编排改变了循环移位量并增加了两个半字节间的异或操作，混淆速度更快. 但是，这样的密钥编排算法从基于比特的变换变为了基于半字节的变换，密钥间的等价关系更容易得到，也更有利于在密钥恢复攻击中实施逐步压缩技术.

4.2 23 轮 LBlock-s 多维零相关线性密码分析的改进

与大多数分组密码算法类似，LBlock-s 算法同样存在多条维数相同的最大长度的零相关线性区分器. 文献[7]基于原有的攻击模型，对 23 轮的 LBlock-s 算法进行了多维零相关线性分析.

基于文献[7]，在 23 轮 LBlock-s 的多维零相关线性分析中，原有的攻击模型只能得到集合 $O=\{(1,9,5,4),(1,11,5,4),(1,13,5,4),(1,15,5,4)\}$，其包含了 4 种可能的区分器及相应的轮扩展方案. 基于此结果，我们利用新的攻击模型，继续对集合 O 进行约简. 我们计算所有等价密钥的距离，分别为 $d^{(1,9,5,4)}=(4,4,8,12)$，$d^{(1,11,5,4)}=(4,8,12,12)$，$d^{(1,13,5,4)}=(4,8,12,12)$，$d^{(1,15,5,4)}=(4,4,8,12)$. 显然，通过比较所有的等价密钥的距离值，能够进一步将集合 O 约简得到最优集合 $L=\{(1,9,5,4),(1,15,5,4)\}$. 可见，最优集合 L 中只包含了两个元素，即只存在两种可能的区分器及相应的轮扩展方案能够使得 23 轮 LBlock-s 算法的多维零相关线性分析的攻击复杂度达到最优.

接下来，我们从最优集合 L 中随机选择一种方案来执行 23 轮 LBlock-s 算法的多维零相关线性攻击. 本文以(1,15,5,4)为例说明如何基于该区分器及轮扩展方案得到复杂度更低的密钥恢复攻击. 即密钥恢复攻击基于 14 轮 8 维零相关线性区分器

$(0a000000,00000000)\rightarrow(00000000,0000000b)$，其中，$a,b\in F_2^4$，$a\neq 0$ 且 $b\neq 0$. 将该区分器向前扩展 5 轮，向后扩展 4 轮，得到 23 轮的密钥恢复攻击. 具体如图 3 所示.

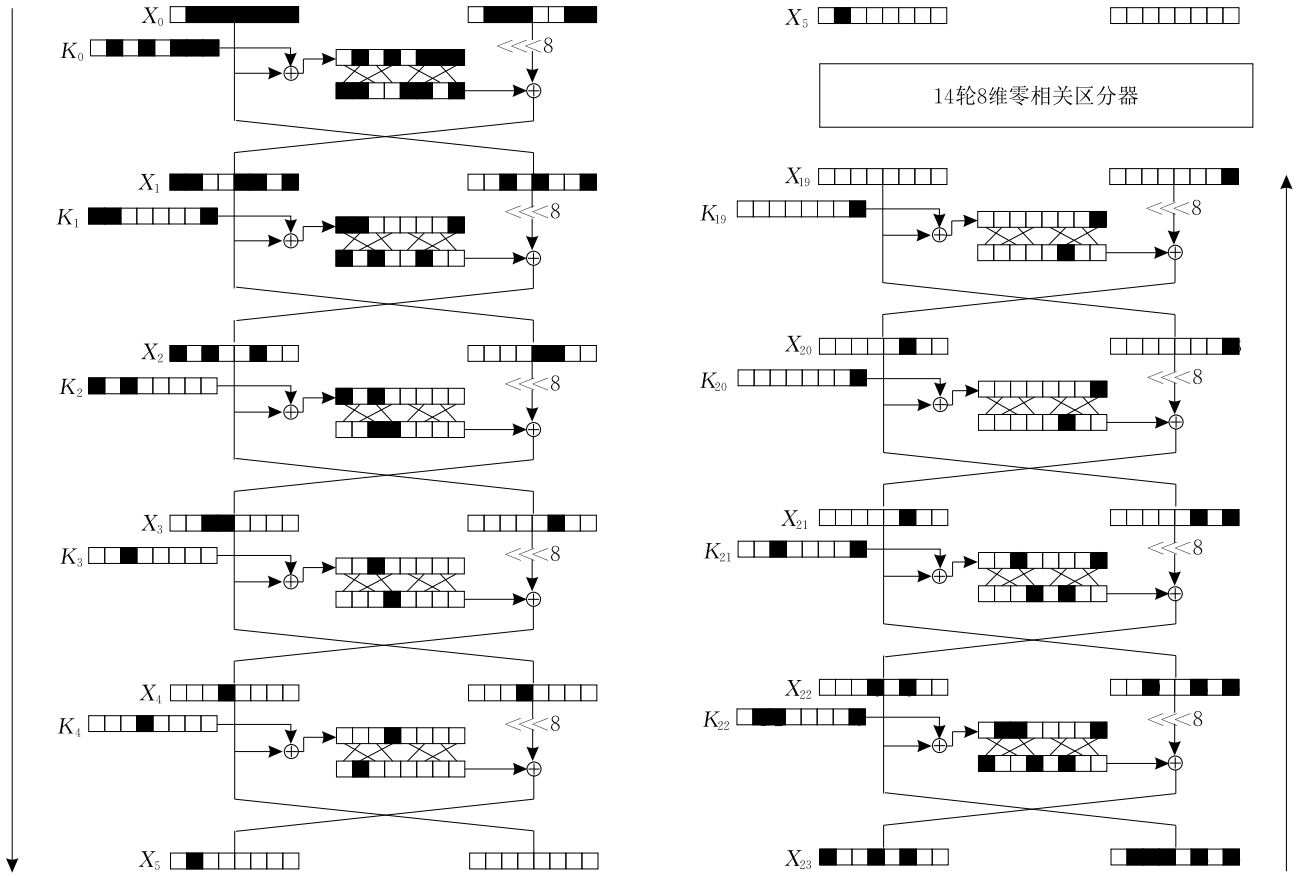

图 3　23 轮 LBlock-s 算法的多维零相关线性攻击

如图 3 所示，区分器的输入掩码位置 X_5^1 共涉及 48 比特的明文和 48 比特的轮密钥，其表达式的具体形式为

$$\begin{aligned}X_5^1 =& X_0^{15}\oplus S(X_0^7\oplus K_0^7)\oplus S(X_0^4\oplus S(X_0^{10}\oplus\\ & S(X_0^1\oplus K_0^1)\oplus K_1^0)\oplus K_2^2)\oplus\\ & S(X_0^7\oplus S(X_0^9\oplus S(X_0^6\oplus K_0^6)\oplus K_1^7)\oplus\\ & S(X_0^{14}\oplus S(X_0^5\oplus K_0^5)\oplus S(X_0^2\oplus\\ & S(X_0^{11}\oplus S(X_0^3\oplus K_0^3)\oplus K_1^1)\oplus K_2^0)\oplus\\ & K_3^2)\oplus K_4^3).\end{aligned}$$

类似地，区分器的输出掩码位置 X_{19}^{15} 共涉及 32 比特的密文和 28 比特的轮密钥，其表达式的具体形式为

$$\begin{aligned}X_{19}^{15} =& X_{23}^{11}\oplus S(X_{23}^0\oplus S(X_{23}^9\oplus K_{22}^1)\oplus K_{21}^2)\oplus\\ & S(X_{23}^3\oplus S(X_{23}^{10}\oplus K_{22}^2)\oplus S(X_{23}^{13}\oplus S(X_{23}^5\oplus\\ & S(X_{23}^{15}\oplus K_{22}^7)\oplus K_{21}^7)\oplus K_{20}^7)\oplus K_{19}^7).\end{aligned}$$

通过分析 LBlock-s 的密钥编排算法，可以知道密钥恢复阶段涉及的所有等价密钥有

$$K_0^6\Leftrightarrow K_1^0,\ K_0^7\Leftrightarrow K_1^1,\ K_0^6\mid K_0^7\Leftrightarrow K_4^3,\ K_{21}^7\Leftrightarrow K_{22}^1.$$

根据 X_5^1 和 X_{19}^{15} 的表达式，很容易计算出等价密钥的距离，它们分别为

$$d(K_0^6,K_1^0)=4,\ d(K_0^7,K_1^1)=8,$$

$$d(K_0^6\mid K_0^7,K_4^3)=12,\ d(K_{21}^7,K_{22}^1)=4.$$

假设攻击需要 N 个已知明文，基于逐步压缩技术的密钥猜测原则，密钥猜测顺序如表 3 的第 2 列所示. 表 3 的第 3 列表示每次压缩需要的时间复杂度并以 S 盒为单位进行衡量，第 4 列表示每次压缩后得到的中间状态. 对每个可能的 $x_i(1\leq i\leq 12)$，我们需要一个计数器 $N_i[x_i]$ 来统计有多少个明-密文对得到 x_i. 表 3 中的最后一列说明了计数器 $N_i[x_i]$ 的大小.

表 3 LBlock-s 算法的逐步压缩过程

步骤	猜测密钥	时间	中间状态	存储
1	$K_0^1 \mid K_1^0 \mid (K_0^6) \mid K_{22}^1 \mid K_{22}^7 \mid (K_{21}^7)$	$N_0 \times 2^{16} \times 6$	$x_1 = X_0^{15} \mid X_0^7 \mid X_2^2 \mid X_1^7 \mid X_0^{14} \mid X_0^5 \mid X_0^2 \mid X_0^{11} \mid X_0^3 \mid X_{23}^{11} \mid X_{22}^{10} \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{56}
2	K_0^3	$2^{56} \times 2^{16+4}$	$x_2 = X_0^{15} \mid X_0^7 \mid X_2^2 \mid X_1^7 \mid X_0^{14} \mid X_0^5 \mid X_0^2 \mid X_1^{11} \mid X_{23}^{11} \mid X_{22}^{10} \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{52}
3	K_1^1	$2^{52} \times 2^{20+4}$	$x_3 = X_0^{15} \mid X_0^7 \mid X_2^2 \mid X_1^7 \mid X_0^{14} \mid X_0^5 \mid X_2^0 \mid X_{23}^{11} \mid X_{22}^{10} \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{48}
4	$K_1^7 \mid (K_0^7)$	$2^{48} \times 2^{24+4} \times 2$	$x_4 = X_2^{13} \mid X_2^2 \mid X_2^5 \mid X_0^{14} \mid X_0^5 \mid X_2^0 \mid X_{23}^{11} \mid X_{22}^{10} \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{44}
5	K_0^5	$2^{44} \times 2^{28+4}$	$x_5 = X_2^{13} \mid X_2^2 \mid X_2^5 \mid X_1^4 \mid X_2^0 \mid X_{23}^{11} \mid X_{22}^{10} \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{40}
6	K_2^0	$2^{40} \times 2^{32+4}$	$x_6 = X_2^{13} \mid X_2^2 \mid X_2^5 \mid X_3^2 \mid X_{23}^{11} \mid X_{22}^{10} \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{36}
7	$K_3^2 \mid (K_4^3)$	$2^{36} \times 2^{36+4} \times 2$	$x_7 = X_2^2 \mid A_1 \mid X_{23}^{11} \mid X_{22}^{10} \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{28}
8	K_2^2	$2^{28} \times 2^{40+4}$	$x_8 = X_5^1 \mid X_{23}^{11} \mid X_{22}^{10} \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{24}
9	K_{21}^2	$2^{24} \times 2^{44+4}$	$x_9 = X_5^1 \mid X_{20}^5 \mid X_{23}^3 \mid X_{23}^{10} \mid X_{21}^{15}$	2^{20}
10	K_{22}^2	$2^{20} \times 2^{48+4}$	$x_{10} = X_5^1 \mid X_{20}^5 \mid X_{21}^5 \mid X_{21}^{15}$	2^{16}
11	K_{20}^7	$2^{16} \times 2^{52+4}$	$x_{11} = X_5^1 \mid X_{20}^5 \mid X_{20}^{15}$	2^{12}
12	K_{19}^7	$2^{12} \times 2^{56+4}$	$x_{12} = X_5^1 \mid X_{19}^{15}$	2^8

注：$A_1 = X_2^{13} \oplus S(X_2^5 \oplus S(X_2^3 \oplus K_3^2) \oplus K_4^3)$.

下面对表 3 的压缩过程给出详细的说明.

1. 设置 56 比特计数器 $N_1[x_1]$. 猜测轮密钥 $K_0^1 \mid K_1^0 \mid (K_0^6) \mid K_{22}^1 \mid K_{22}^7 \mid (K_{21}^7)$，可以最多利用 8 比特等价密钥，实际猜测密钥量为 16 比特. 利用猜测的密钥对 N 个已知明-密文进行加解密，将 x_0 压缩为 x_1. x_0 所涉及的明-密文可以表示为

$$\begin{aligned} x_0 = {} & X_0^{15} \mid X_0^7 \mid X_0^4 \mid X_0^{10} \mid X_0^1 \mid X_0^9 \mid X_0^6 \mid \\ & X_0^{14} \mid X_0^5 \mid X_0^2 \mid X_0^{11} \mid X_0^3 \mid X_{23}^{11} \mid X_{23}^0 \mid \\ & X_{23}^9 \mid X_{23}^3 \mid X_{23}^{10} \mid X_{23}^{13} \mid X_{23}^5 \mid X_{23}^{15}. \end{aligned}$$

由于

$$\begin{cases} X_2^2 = X_0^4 \oplus S(X_0^{10} \oplus S(X_0^1 \oplus K_0^1) \oplus K_1^0) \\ X_1^7 = X_0^9 \oplus S(X_0^6 \oplus K_0^6) \\ X_{22}^{10} = X_{23}^0 \oplus S(X_{23}^9 \oplus K_{22}^1) \\ X_{21}^{15} = X_{23}^5 \oplus S(X_{23}^{15} \oplus K_{22}^7) \oplus K_{21}^7 \end{cases}.$$

所以，猜测 16 比特轮密钥 $K_0^1 \mid K_1^0 \mid (K_0^6) \mid K_{22}^1 \mid K_{22}^7 \mid (K_{21}^7)$，能够将 80 比特的 x_0 压缩为 56 比特的 x_1. 更新 X_5^1 和 X_{19}^{15}：

$$\begin{aligned} X_5^1 = {} & X_0^{15} \oplus S(X_0^7 \oplus K_0^7) \oplus S(X_2^2 \oplus K_2^2) \oplus \\ & S(X_0^7 \oplus S(X_1^7 \oplus K_1^7) \oplus S(X_0^{14} \oplus \\ & S(X_0^5 \oplus K_0^5) \oplus S(X_0^2 \oplus S(X_0^{11} \oplus \\ & S(X_0^3 \oplus K_0^3) \oplus K_1^1) \oplus \\ & K_2^0) \oplus K_3^2) \oplus K_4^3), \\ X_{19}^{15} = {} & X_{23}^{11} \oplus S(X_{22}^{10} \oplus K_{21}^2) \oplus S(X_{23}^3 \oplus \\ & S(X_{23}^{10} \oplus K_{22}^2) \oplus S(X_{21}^{15} \oplus K_{20}^7) \oplus K_{19}^7). \end{aligned}$$

2. 设置 52 比特计数器 $N_2[x_2]$. 由于 $X_1^1 = X_0^{11} \oplus S(X_0^3 \oplus K_0^3)$，猜测 4 比特密钥 K_0^3，将 56 比特的状态 x_1 压缩为 52 比特状态 x_2. 注意，猜测是 K_0^3 的目的是能够尽早利用等价密钥 K_1^1 与 K_0^7 进行状态压缩.

以此类推，后面的压缩步骤类似，不再作说明. 仍然需要强调的是压缩过程中的轮密钥猜测顺序要与等价密钥的距离相对应，这样做的目的是达到最优的压缩复杂度.

为了进一步恢复秘密密钥，需要计算统计量来区分所猜测的密钥是否正确，继续执行以下步骤：

1. 为 8 比特的 z 设置计数器 $V[z]$.

2. 对 x_{12} 的所有 2^8 个值：

(a) 计算 z 值；

(b) 更新 $V[z]$，$V[z] = V[z] + N_{12}[x_{12}]$.

3. 对猜测的每个密钥 k，计算统计值 $T_k = \frac{N \cdot 2^8}{(1-2^{-8})} \sum_{z=0}^{2^8-1} \left(\frac{V[z]}{N} - \frac{1}{2^8} \right)^2$.

4. 如果 $T_k < \tau$，那么将该 k 视为可能的正确候选密钥.

5. 穷搜剩下的所有候选密钥，找到唯一的正确密钥.

复杂度评估.

与文献[7]类似，为了保证攻击的成功率为 85%，令 type-1 型错误的概率为 $\alpha = 2^{-2.7}$，type-2 型错误的概率为 $\beta = 2^{-9}$，得到 $z_{1-\alpha} \approx 1$，$z_{1-\beta} \approx 2.88$，

又由于 $n=64, l=2^8-1=255$. 所以攻击需要的数据复杂度为 $N=\frac{2^n(z_{1-\alpha}+z_{1-\beta})}{\sqrt{l/2}+z_{1-\alpha}}\approx 2^{62.3}KP$. 区分的阈值为 $\tau=\mu_0+\sigma_0 z_{1-\alpha}=\mu_1+\sigma_1 z_{1-\beta}\approx 320$. 将表 3 中步骤 1～12 的时间复杂度相加求和，得到逐步压缩阶段需要的时间复杂度为 $2^{81.25}\times\frac{1}{8\times 23}\approx 2^{73.75}$ 次 23 轮 LBlock-s 加密. 最后，需要对剩下的 $2^{80-9}=2^{71}$ 个候选密钥进行穷搜，穷搜的时间复杂度为 2^{71} 次 23 轮 LBlock-s 加密. 所以，攻击的总时间复杂度为 $2^{73.75}$ 次 23 轮 LBlock-s 加密，存储复杂度为 2^{56} 字节. 较已有的攻击结果，新攻击结果在时间和存储复杂度上都有较大的改进.

5　总　结

在本文中，通过定义等价密钥的距离进一步给出了多维零相关线性分析的改进模型. 研究发现等价密钥在所需压缩表达式中的不同位置会影响多维零相关线性分析中区分器的选择和逐步分压缩过程的时间和存储复杂度. 我们利用等价密钥距离的概念来刻画这种影响. 新模型不仅考虑了密钥恢复阶段独立密钥猜测总量，而且利用等价密钥的距离对区分器进行进一步筛选，还给出了基于等价密钥的距离的密钥猜测策略. 实验表明，猜测距离较短的等价密钥比猜测距离较长的等价密钥，整体压缩效果要好，即时间更短，存储复杂度更低. 为了证明新模型的实用性，我们将该优化模型应用到 23 轮 LBlock-s 算法中，更新了其抵抗多维零相关线性的安全性分析结果. 该结果是目前针对 LBlock-s 算法在单密钥模型下的最好的攻击结果.

新的多维零相关优化模型是一个通用的分析模型，适用于大多数分组密码. 基于新的模型，除 LBlock-s 算法以外的其他分组密码算法抵抗多维零相关线性分析的能力也许需要重新的评估. 新的优化模型对攻击复杂度的改进是有限的，主要对时间和存储复杂度进行了缩短和降低，而攻击的数据复杂度仍然要求很高. 如何进一步优化模型，降低攻击的数据复杂度和进一步提高攻击轮数是下一步研究的方向. 另外，针对多维零相关线性区分器的自动化搜索算法已经很成熟了，但是如何实现密钥恢复攻击阶段的自动化分析是下一步研究的内容.

致　谢　在此感谢中国科学院软件研究所和可信计算与信息保障实验室，感谢对本论文工作提出建议的老师、师兄师姐和同学们，感谢编辑及评审老师给出的宝贵意见！

参　考　文　献

[1] Bogdanov A, Rijmen V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Designs, Codes and Cryptography, 2014, 70(3): 369-383

[2] Bogdanov A, Wang M. Zero correlation linear cryptanalysis with reduced data complexity//Proceedings of the Fast Software Encryption. Washington, USA, 2012: 29-48

[3] Bogdanov A, Leander G, et al. Integral and multidimensional linear distinguishers with correlation zero//Proceedings of the Advances in Cryptology—ASIACRYPT 2012. Beijing, China, 2012: 244-261

[4] Wang Y, Wu W. Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE//Proceedings of the Information Security and Privacy. Wollongong, Australia, 2014: 1-16

[5] Wu W, Zhang L. LBlock: A lightweight block cipher//Proceedings of the Applied Cryptography and Network Security. Nerja, Spain, 2011: 327-344

[6] Wang Y, Wu W, Yu X, et al. Security on LBlock against biclique cryptanalysis//Proceedings of the Information Security Applications. Jeju Island, Korea, 2012: 1-14

[7] Xu Hong, Jia Ping, Huang G, et al. Multidimensional zero-correlation linear cryptanalysis on 23-round LBlock-s//Proceedings of the Information and Communications Security. Beijing, China, 2015: 97-108

[8] Ahmadi S, Ahmadian Z, Mohajeri J, et al. Biclique cryptanalysis of LBlock with modified key schedule//Proceedings of the 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology. Rasht, Iranian, 2015: 1-5

[9] Jia Ping, Xu Hong, Lai Xue-Jia. Impossible differential cryptanalysis of reduced-round LBlock-s//Proceedings of the Conference on Computer Network and Information Security. Hangzhou, China, 2015(in Chinese)
(贾平，徐洪，来学嘉. LBlock-s 算法的不可能差分分析//第八界中国计算机网络与信息安全学术会议. 杭州，中国，2015)

[10] Soleimany H, Nyberg K. Zero-correlation linear cryptanalysis of reduced-round LBlock. Designs, Codes and Cryptography, 2014, 73(2): 683-698

[11] Liu Z, Sun B, Wang Q, et al. Improved zero-correlation linear cryptanalysis of reduced-round Camellia under weak keys. IET Information Security, 2016, 10(2): 95-103

[12] Bogdanov A, Geng H, Wang M, et al. Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA//Proceedings of the International Conference on Selected Areas in Cryptography. Burnaby, Canada, 2013: 306-323

附录 1.

附表 1 LBlock-s 算法的 S 盒

S_0	14, 9, 15, 0, 13, 4, 10, 11, 1, 2, 8, 3, 7, 6, 12, 5
S_1	4, 11, 14, 9, 15, 13, 0, 10, 7, 12, 5, 6, 2, 8, 1, 3
S_2	1, 14, 7, 12, 15, 13, 0, 6, 11, 5, 9, 3, 2, 4, 8, 10
S_3	7, 6, 8, 11, 0, 15, 3, 14, 9, 10, 12, 13, 5, 2, 4, 1
S_4	14, 5, 15, 0, 7, 2, 12, 13, 1, 8, 4, 9, 11, 10, 6, 3
S_5	2, 13, 11, 12, 15, 14, 0, 9, 7, 10, 6, 3, 1, 8, 4, 5
S_6	11, 9, 4, 14, 0, 15, 10, 13, 6, 12, 5, 7, 3, 8, 1, 2
S_7	13, 10, 15, 0, 14, 4, 9, 11, 2, 1, 8, 3, 7, 5, 12, 6
S_8	14, 9, 15, 0, 13, 4, 10, 11, 1, 2, 8, 3, 7, 6, 12, 5
S_9	4, 11, 14, 9, 15, 13, 0, 10, 7, 12, 5, 6, 2, 8, 1, 3

附录 2.

LBlock 密钥编排算法如下所示：

1. $K_0 = MK[0-31]$

2. 对 $i=1\sim31$ 执行：

(a) $MK = MK <<< 29$

(b) $MK[0-3] = S_8(MK[0-3])$

$MK[4-7] = S_9(MK[4-7])$

(c) $MK[29-33] = MK[29-33] \oplus [i]_2$

(d) $K_i = MK[0-31]$.

LI Ling-Chen, born in 1988, Ph. D. candidate. Her research interest is cryptanalysis of symmetric ciphers.

WU Wen-Ling, born in 1966, Ph. D., professor, Ph. D. supervisor. Her research interests include design and cryptanalysis of block cipher, modes of operation for block ciphers and the theory of provable security.

WANG Yan-Feng, born in 1989, Ph. D. Her research interest is design and cryptanalysis of block cipher.

Background

Block cipher is one of the important symmetric cryptography, which has the characteristics of fast speed, easy standardization, and easy to implement. It has a wide application in the field of information security. In cryptanlysis, there are many methods for block cipher, for example, differential attack, linear attack, meet-in-the middle attack, integral attack etc. In 2010, Bogdanov et al. proposed the zero-correlation linear cryptanlysis, which uses the zero-correlation linear approximation to distinguish the block cipher and the random permutation. Then, the multiple and multidimensional zero correlation linear analysis has been proposed in succession, and the zero-correlation linear cryptanlysis already becomes a complete method and has been used in the cryptanlysis of many block ciphers, such as AES, CLEEFIA, TWINE, TEA, etc.

The multidimensional distinguisher is constructed for the zero-correlation property at ASIACRYPT'12, which removed the unnecessary independency assumptions in distinguishers. In the follow-up work at ACISP'14, an attack model of the multidimensional zero-correlation linear cryptanalysis was proposed by taking the equivalent relations of guessed keys and the partial-compression technique. An attack on 23-round LBlock, 23-round TWINE-80 and 25-round TWINE-128 were achieved. Based on the model, an attack on 23-round LBlock-s was achieved at ICICS'15.

In this paper, we improved the attack model of the multidimensional zero-correlation linear cryptanalysis by using the distance of equivalent keys which is a new definition in the paper. It's important that we consider the specific location of the guessed keys in the compression expression of the key recovery attack to further filter the distinguishers. Beside, we give an order of guessed keys based on the distances. Moreover, to demonstrate the practical impact of our model, we improve the multidimensional zero-correlation linear cryptanalysis on 23-round LBlock-s. As far as we know, this is the currently best result on LBlock-s.

This work is supported by the National Basic Research Program (973 Program) of China (No. 2013CB338002) and the National Natural Science Foundation of China (Nos. 61272476, 61232009 and 61202420).