doi:10.11959/j.issn.1000-436x.2017101

LBlock 算法的相关密钥不可能飞来去器分析

谢敏，牟彦利
（西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071）

摘 要：研究了相关密钥不可能飞来去器分析方法及轻量级分组密码算法 LBlock 在该分析方法下的安全性。将不可能飞来去器分析方法和相关密钥分析方法相结合，针对 22 轮 LBlock 给出了新的攻击。构造了 15 轮的相关密钥不可能飞来去器区分器，通过向前扩展 3 轮，向后扩展 4 轮，成功攻击了 22 轮 LBlock。该攻击的数据复杂度仅为 $2^{51.3}$ 个明文，计算复杂度为 $2^{71.54}$ 次 22 轮加密。与已有结果相比，攻击的数据复杂度和计算复杂度均有明显下降。

关键词：LBlock 算法；轻量级分组密码；相关密钥；不可能飞来去器
中图分类号：TN918.1 **文献标识码**：A

Related-key impossible boomerang cryptanalysis on LBlock

XIE Min, MU Yan-li
（State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China）

Abstract: The related-key impossible boomerang cryptanalysis and the strength of the lightweight block cipher LBlock against this method were investigated. A new attack on 22-round LBlock was presented combining impossible boomerang attacks with related-key attacks. A 15-round related-key impossible boomerang distinguisher was constructed. Based on the new distinguisher, an attack on 22-round LBlock was mounted successfully by concatenating 3-round to the beginning and 4-round to the end. The attack on 22-round LBlock required data complexity of only $2^{51.3}$ plaintexts and computational complexity of about $2^{71.54}$ 22-round encryptions. Compared with published cryptanalysis results on 22-round LBlock, proposed attack has great advantages on data and computational complexities.

Key words: LBlock algorithm, lightweight block cipher, related-key, impossible boomerang

1 引言

为了适应资源受限的环境，轻量级分组密码的设计与分析越来越受到大家的关注，一系列的轻量级分组密码应运而生，如 MIBS[1]、LBlock[2]、TWIS[3]和 DBlock[4]等。

LBlock 密码算法是 2011 年在应用密码学与网络安全国际会议上提出的轻量级分组密码算法，它采用类 Feistel 结构，共 32 轮迭代，分组长度和主密钥长度分别为 64 bit 和 80 bit。算法设计者对该算法进行了安全性分析，给出了 14 轮的不可能差分路径，进行了 20 轮不可能差分攻击；给出了 15 轮的截断差分路径，其概率小于等于 2^{-64}，说明了没有可用的 15 轮差分区分器；设计者也对其进行了 20 轮的积分攻击[2]。近些年，研究者们对 LBlock 进行了多种安全性分析[5~11]。吴寿昌等[10]找到一条 13 轮的线性特征，利用该线性特征对应的线性逼近表达式对 LBlock 进行了 17 轮的线性攻击。Chen 和 Miyaji[11]用飞来去器的分析方法对 LBlock 进行了 18 轮的飞来去器攻击。Liu 等[5]通过算法设计者给出的不可能差分路径的构造方式给出一条 14 轮的不可能差分路径对 LBlock 进行了 21 轮的攻击。

收稿日期：2016-06-30；**修回日期**：2017-03-16
基金项目：国家自然科学基金资助项目（No.61373170, No.U0835004, No.U1536202）；国家 111 创新引智基金资助项目（No.B08038）
Foundation Items: The National Natural Science Foundation of China (No.61373170, No.U0835004, No.U1536202), The 111 Project of China (No.B08038)

Sasaki 等[6,7]用积分攻击方法分别对 LBlock 进行了 20 轮和 22 轮的积分攻击。Wen 等[9]找到一条 16 轮的相关密钥不可能差分路径对 23 轮 LBlock 进行了攻击。Liu 等[8]找到一条 16 轮相关密钥截断差分路径对 LBlock 进行了 22 轮的攻击，并给出了 16 轮的相关密钥飞来去器区分器，但并未在此区分器的基础上对其进行详细分析，而且所给出 22 轮截断差分攻击的数据复杂度远高于本文的攻击结果。

本文使用的相关密钥不可能飞来去器攻击方法[12]将 3 种不同的攻击方法相结合，这种多种攻击方法结合的方式利用了多种分析方法的优势，是当今密码分析的主流方式。当密码算法能够抵抗 3 种方法中单一的一种攻击方法时不一定能够抵抗相关密钥不可能飞来去器攻击，而且该方法近几年才被提出，对其研究也较少，因此，对相关密钥不可能飞来去器攻击方法的研究很有意义。在研究了密码算法 LBlock 结构性质的基础上，本文首次使用相关密钥不可能飞来去器攻击方法对 22 轮 LBlock 进行了攻击，通过构造密钥差分分别满足 $\Delta K^5=4$ （ΔK^5 表示初始密钥差分的第 5 个半字节)和 $\Delta K^5=8$ 的条件下的 15 轮相关密钥不可能飞来去器区分器，然后向前扩展 3 轮，向后扩展 4 轮，成功对 22 轮 LBlock 进行了攻击。

2　LBlock 分组密码介绍

2.1　LBlock 加密算法

LBlock 密码算法基于类 Feistel 结构，迭代轮数为 32 轮，分组长度为 64 bit，密钥长度为 80 bit，用 $P=X_1\|X_0$ 表示 64 bit 明文，其加密结构如图 1 所示。LBlock 算法每一轮的轮函数 F 包括密钥加、S 盒变换和 P 置换，轮函数结构如图 2 所示。

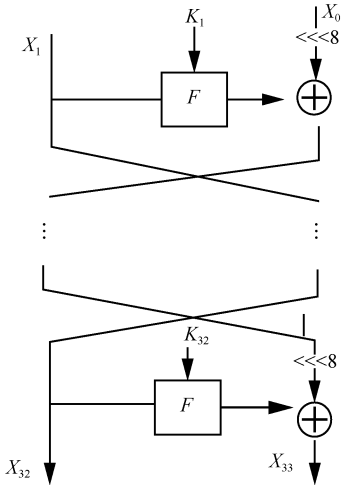


图 1　LBlock 的加密过程

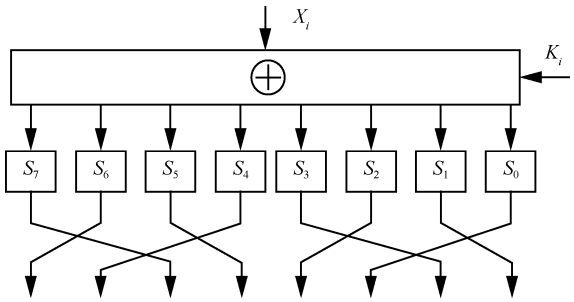


图 2　轮函数 F 的结构

2.2　LBlock 解密算法

LBlock 的解密算法就是其加密算法的逆过程，具体过程如下。

1) 对 $i=31,30,\cdots,1,0$，计算 $X_i=(F(X_{i+1},K_{i+1})\oplus X_{i+2}>>>8)$；

2) 输出 $P=X_1\|X_0$ 为 64 bit 明文。

2.3　LBlock 的密钥扩展算法

将 80 bit 主密钥 K 存入寄存器中，且密钥 K 标记为 $K=k_{79}k_{78}\cdots k_1k_0$，取当前主密钥的最左边 32 bit 作为轮密钥 K_1，对 $i=1,2,\cdots,31$, 重复下列操作。

1) $K<<<29$；

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) $[k_{50},k_{49},k_{48},k_{47},k_{46}]=[k_{50},k_{49},k_{48},k_{47},k_{46}]\oplus[i]_2$。

取寄存器的最左端 32 bit 密钥作为子密钥 K_{i+1}。

3　相关密钥不可能飞来去器攻击原理

相关密钥不可能飞来去器攻击将相关密钥[13,14]、不可能差分[15]和飞来去器[16]3 种攻击方法结合起来。其中，相关密钥攻击分别由 Biham 和 Knudsen 独立提出，主要根据密钥扩展算法的弱点，找到不同轮子密钥间存在的关系对加解密产生的影响来恢复出密钥，该方法对分组密码有着较好的分析效果[17,18]，因此被广泛用于密码分析中。不可能差分攻击方法和飞来去器攻击方法均是以差分分析作为基础的攻击方法，分别由 Bahim 和 Wagner 提出，自发展以来也广泛用于分组密码的分析中[17~21]。如第 1 节中所述相关密钥不可能飞来去器攻击方法充分利用了 3 种分析方法的优点，该分析方法结构与相关密钥飞来去器攻击结构有点相似，但又融入了不可能差分分析。而且相比相关密钥不可能差分而言，该方法更容易找到可分析的路径，在寻找相关密钥不可能差分路径时，确定了相关密钥差分路径，也

就固定了密钥差分路径下半部分的密钥差分，从而决定了解密过程中密文差分的输入；而在寻找相关密钥不可能飞来去器路径时，利用密钥扩展算法的弱点找到一条尽可能长的密钥差分路径，进而确定区分器的上半部分，而对于区分器下半部分的密钥差分仍可以灵活选择，寻找另外尽可能长的密钥差分路径来确定区分器的下半部分，这样不仅更容易找到理想的可分析路径，还可能使可分析的路径更长。

在该攻击方法中，将加密算法 E 表示成 2 个子算法的组合 $E_0 \circ E_1$。设 $\Delta\alpha \to \Delta\beta$ 和 $\Delta\alpha' \to \Delta\beta'$ 为 E_0 中 2 条概率为 1 的相关密钥差分路径，$\Delta\delta \to \Delta\gamma$ 和 $\Delta\delta' \to \Delta\gamma'$ 为 E_1^{-1} 中的 2 条概率为 1 的相关密钥差分路径，其中，α、α'、β、β'、δ、δ'、γ、γ' 均为 $n$bit 的数据块，并且 β、β'、γ、γ' 在中间相遇时满足 $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$，在该攻击方法中涉及的 4 个密钥分别为 K_A、K_B、K_C、K_D，它们的关系需要满足 $K_A \oplus K_B = K_C \oplus K_D = \Delta k_\alpha$，$K_A \oplus K_C = K_B \oplus K_D = \Delta k_\beta$，其相关密钥不可能飞来去器攻击示意如图 3 所示。

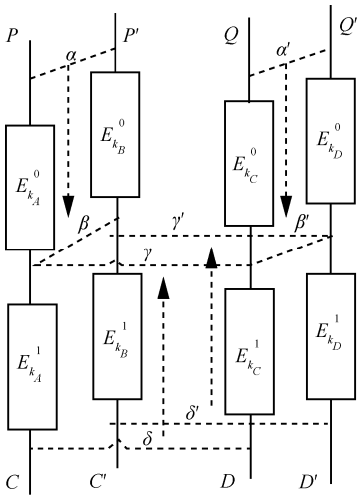


图 3 相关密钥不可能飞来去器攻击示意

4 LBlock 算法的相关密钥不可能飞来去器攻击

通过构造 15 轮的相关密钥不可能飞来去器区分器，然后向前扩展 3 轮，向后扩展 4 轮，对 22 轮 LBlock 算法进行了相关密钥不可能飞来去器攻击。在进行 22 轮相关密钥不可能飞来去器攻击时，所用到的前 12 轮的相关密钥差分由主密钥差分 ΔK 生成，每种主密钥差分会对应 2 条概率较大的差分路径，如表 1 所示。

表 1 相关密钥差分

密钥	主密钥差分路径			
	ΔK =0000000000000040000		ΔK =0000000000000080000	
ΔK_1	0000 0000	0000 0000	0000 0000	0000 0000
ΔK_2	0000 0008	0000 0008	0000 0010	0000 0010
ΔK_3	0000 0000	0000 0000	0000 0000	0000 0000
ΔK_4	0000 0000	0000 0000	0000 0000	0000 0000
ΔK_5	0000 0400	0000 0400	0000 0800	0000 0800
ΔK_6	0000 0000	0000 0000	0000 0000	0000 0000
ΔK_7	0000 0000	0000 0000	0000 0000	0000 0000
ΔK_8	0002 0000	0002 0000	0000 0400	0000 0400
ΔK_9	0000 0000	0000 0000	0000 0000	0000 0000
ΔK_{10}	0000 0000	0000 0000	0000 0000	0000 0000
ΔK_{11}	0600 0000	0200 0000	0200 0000	0600 0000
ΔK_{12}	0000 0000	0000 0000	0000 0000	0000 0000

令 E_0 表示第 4～12 轮，E_1 表示第 13～18 轮，构造的区分器的密钥关系为 $k_A = k_C$，$k_B = k_D$，E_0 的差分路径 $\Delta\alpha \to \Delta\beta$ 和 $\Delta\alpha' \to \Delta\beta'$ 均为(00000000, 00000004)→(???*???*,?*0?*??*)。如图 4 所示，使用的初始相关密钥差分为(0000000000000400000)或(0000000000000800000)，即 $k_A \oplus k_B = k_C \oplus k_D \circ E_1^{-1}$ 的其中一条差分路径 $\Delta\delta \to \Delta\gamma$ 为(0000*000, 00000000)→ (*0***0*0,**0**?**)，另一条差分路径 $\Delta\delta' \to \Delta\gamma'$ 为(0*000000,00000000)→ (0*0*0***, ****0**?)，其密钥差分均为 0，如图 5 所示。以上所述 4 条概率均为 1 的差分路径构成了 15 轮相关密钥不可能飞来去器区分器：((00000000，00000004), (00000000, 00000004))↛((0000*000, 00000000), (0*000000, 00000000))。这 4 条相关密钥差分路径中向下加密的 2 条路径和向上解密的 2 条差分路径在中间相遇时出现矛盾，即((??* ??*?,?*0? *??*)(??* ??*?,?*0? *??*))≠((*0** *0*0,**0* **?**)(0*0* 0***,*** 0**?))，该式中添加下划线的 4 个半字节处的异或肯定不为 0，由相关密钥不可能飞来去器攻击的原理可知此处存在矛盾。“*”表示非 0，“?”表示不确定值，(ΔX_i，ΔX_{i-1})表示第 i 轮差分输入。

在已构造区分器的基础上向上扩展 3 轮，向下扩展 4 轮，构成了 22 轮相关密钥不可能飞来去器路径。在 $\Delta K^5 = 4$ 的条件下，向上扩展和向下扩展的差分特征如图 6 所示。

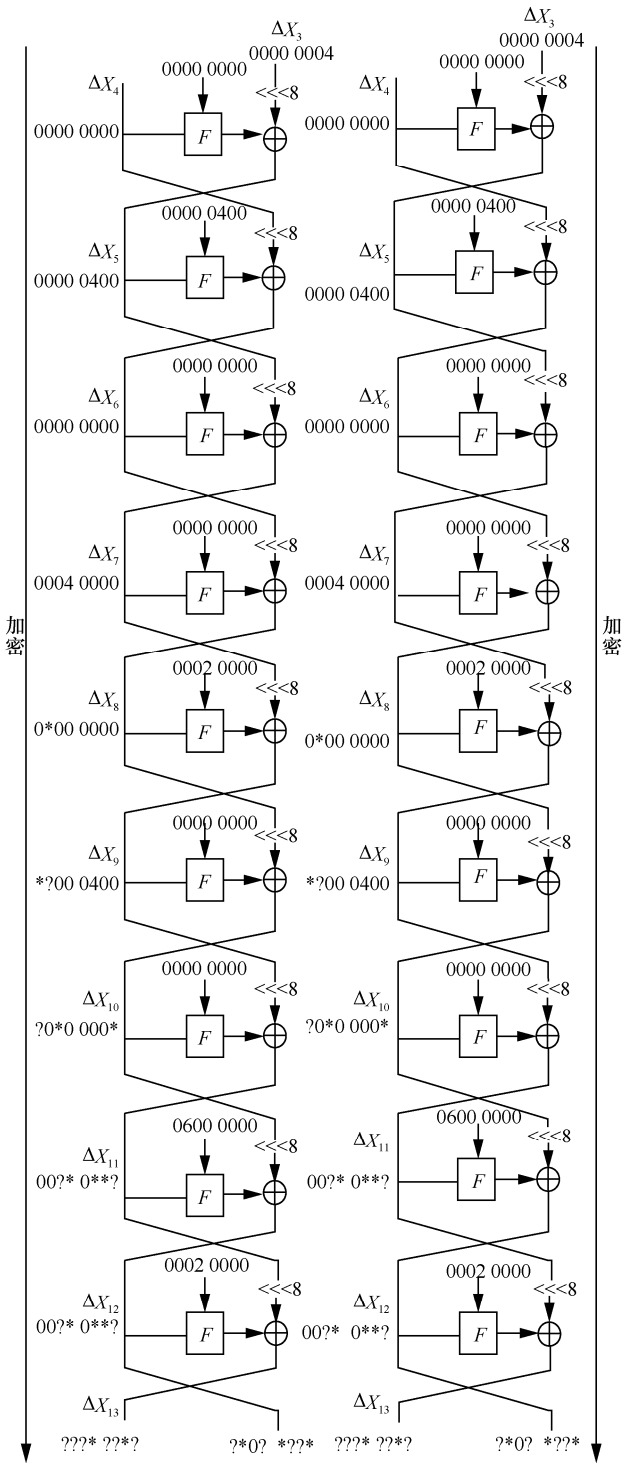


图 4　加密方向差分路径

这里用 $\Delta K=(0000000000000400000)$ 来描述具体的攻击过程，攻击过程如下。

1) 按照图 6(a)中明文差分的输入结构选取 2^n 个明文结构，每个结构包含 2^{20} 个明文，它们可构成 2^{n+39} 个明文对，记作(P,P')；继续选取 2^n 个这样的明文结构，仍可构成 2^{n+39} 个明文对，记作$(P^*,P^{*'})$。

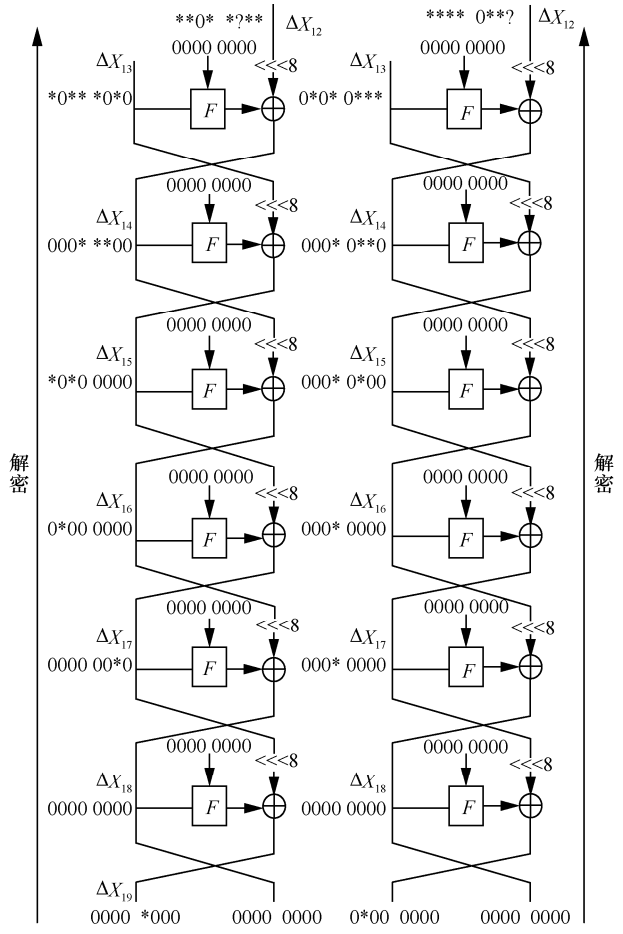
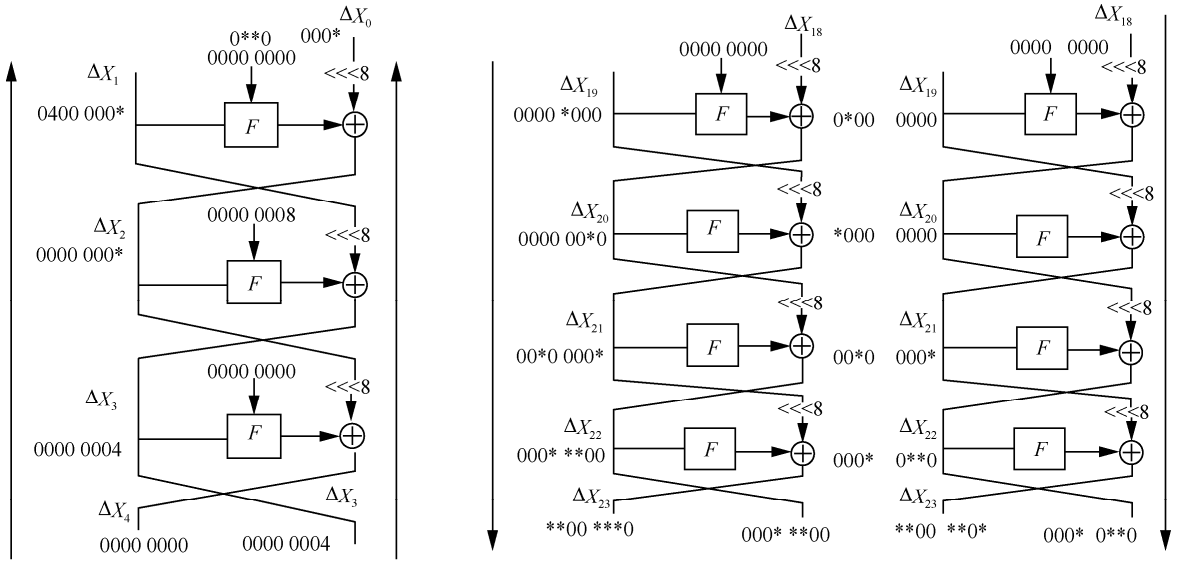


图 5　解密方向差分路径

2 次选取的明文对将构成明文四元组 $(P,P',P^*,P^{*'})$，再将明文四元组中的 2 个明文对分别在密钥差分为 $\Delta K=(0000000000000400000)$ 的密钥对下进行加密，得到的密文四元组记作$(C,C',C^*,C^{*'})$。

2) 将密文四元组按照图 6(b)中的输出形式进行筛选，过滤掉密文差分不满足((**00 ***0，000* **00),(**00 **0*，000* 0**0))的四元组，剩余 2^{2n+14} 个密文四元组。然后猜测 K_{22}^2、K_{22}^4、K_{22}^3、K_{22}^1、其对应主密钥中的位置为 $k_{7\sim10}$、$k_{15\sim18}$、$k_{11\sim14}$、$k_{3\sim6}$，对剩余四元组部分解密一轮，检查输出的解密四元组中数据对右半部分差分的第 1、2、3、4、6、7 个半字节是否为 0，若不是则丢掉相应四元组，剩余 2^{2n-10} 个四元组。该步计算复杂度约为 $(2^{2n+14}\times2^4+2^{2n+6}\times 2^8+2^{2n-2}\times2^{12}+2^{2n-6}\times2^{16})\times\frac{1}{8}\times\frac{1}{22}=2^{2n+10.63}$。

3) 依次猜测 K_{21}^0、K_{22}^0、K_{21}^5、K_{22}^6，其对应主密钥中的位置为 $k_{28\sim31}$、$k_{0\sim2,79}$、$k_{48\sim51}$、$k_{23\sim26}$。对



(a) 向上扩展的差分路径 (b) 向下扩展的差分路径

图 6 向下扩展与向上扩展的差分特征

剩余四元组部分解密，检查输出的解密四元组中数据对右半部分差分的第 0、2 个半字节是否为 0，若不是则丢掉相应的四元组，剩余 2^{2n-26} 个四元组。该步计算复杂度约为 $2^{2n+8.54}$ 。

4) 猜测 K_1^6 、 K_1^0，其对应主密钥位置分别为 $k_{72\sim75}$ 、 $k_{48\sim51}$。对剩余四元组部分加密一轮，检查输出的四元组中数据对左半部分差分的第 2、7 个半字节差分是否为 0，若不是则丢掉相应的四元组，剩余 2^{2n-42} 个四元组。该步计算复杂度约为 $2^{2n+2.62}$ 。

5) 猜测 K_2^0 、 K_1^1，其对应主密钥中的位置为 $k_{19\sim22}$ 、 $k_{52\sim55}$。对剩余四元组部分加密 2 轮，检查输出的四元组中数据对左半部分差分的第 2 个半字节是否为 0，若不为 0 则丢掉相应的四元组，该步剩余 2^{2n-50} 个四元组。计算复杂度约为 $2^{2n-3.46}$ 。

6) 依次猜测 K_{20}^7、K_{21}^3、K_{22}^7、K_{20}^1、K_{21}^2、K_{22}^5，其对应主密钥中的位置为 $k_{5\sim8}$ 、 $k_{40\sim43}$ 、 $k_{27\sim30}$ 、 $k_{61\sim64}$ 、 $k_{36\sim39}$ 、 $k_{19\sim22}$，其中，$k_{5\sim8}$ 、 $k_{28\sim30}$ 、 $k_{19\sim22}$ 均已猜测，只需再猜测剩余的 13 位密钥。对剩余四元组解密，检查输出四元组中的 2 个数据对右半部分差分，其中一个的第 6 个半字节和另一个的第 3 个半字节是否均为 0，若不是则丢掉相应的四元组，将剩余 2^{2n-58} 个四元组。该步计算复杂度约为 $2^{2n+1.21}$ 。

7) 依次猜测 K_{19}^6、K_{20}^1、K_{21}^2、K_{22}^7、K_{19}^3、K_{20}^7、K_{21}^1、K_{22}^0，除去已猜测过的密钥只需猜测 5 个密钥位，该步将剩余 2^{2n-66} 个四元组，计算复杂度约为 $2^{2n+0.13}$ 。此时第 19 轮的解密输出为((0000 00*0,0000 *000),(*000 0000,0*00 0000))，满足 15 轮相关密钥不可能飞来去器路径的输出条件。

8) 利用 X_3 的第 0 个半字节位置确定密钥 K_3^0，总共有 2^8 种可能，进行第 3 轮加密，能够满足第 3 轮输出要求的概率为 $\frac{1}{6}$，故剩余四元组个数为 $2^{2n-66}\times2^8\times\frac{1}{6}$。若经过该步过滤后仍有四元组剩余，则说明所猜测的密钥是错误的，需要将其剔除。

若选取 $2^{30.3}$ 个明文结构，即取 $n=30.3$，则由步骤 8) 可知剩余四元组个数为 $2^{2\times30.3-66}\times2^8\times\frac{1}{6}\approx2^{0.2}$，恰好可以剔除所有错误的密钥，恢复出正确的密钥比特。

综上可知对 22 轮 LBlock 的相关密钥不可能飞来去器攻击可恢复出 66 个密钥比特。其中步骤 1) 2 次选取了 2^n 个结构，每个明文结构包括 2^{20} 个明文，取 $n=30.3$，所以该攻击共需要 $2^{n+1+20}=2^{51.3}$ 个明文。计算复杂度为 $2^{71.23}+2^{69.14}+2^{63.22}+2^{57.14}+2^{61.81}+2^{60.73}=2^{71.541\,47}$ 。所以攻击过程的数据复杂度为 $2^{51.3}$，计算复杂度大约为 $2^{71.54}$ 。

5 结束语

本文利用 LBlock 密钥扩展算法的弱点，结合不可能差分和飞来去器分析方法的优点，选取特定

的密钥差分，充分利用密钥差分对区分器中差分路径的影响，得到尽可能长的差分链。基于这些思想首次用相关密钥不可能飞来去器的方法构造了新的 15 轮区分器，对 22 轮 LBlock 进行了攻击,其数据复杂度仅为 $2^{51.3}$，计算复杂度为 $2^{71.54}$。相比 LBlock 的其他已有攻击结果，该数据复杂度大幅度减小，计算复杂度也相对较理想。表 2 给出了对 LBlock 算法部分攻击结果的比较。

表 2　　LBlock 算法的分析结果比较

攻击类型	攻击轮数	数据复杂度	计算复杂度	文献来源
不可能差分攻击	21	$2^{62.5}$	$2^{73.7}$	文献[5]
积分攻击	22	2^{61}	$2^{70.00}$	文献[7]
相关密钥飞来去器区分器	16	2^{60}	—	文献[8]
相关密钥截断差分分析	22	2^{67}	$2^{64.1}$	文献[8]
相关密钥不可能差分攻击	23	$2^{63.27}$	$2^{78.3}$	文献[9]
线性攻击	17	2^{62}	$2^{77.12}$	文献[10]
飞来去器攻击	18	$2^{63.26}$	$2^{70.84}$	文献[11]
相关密钥不可能飞来去器	22	$2^{51.3}$	$2^{71.54}$	本文

参考文献：

[1] IZADI M, SADEGHIYAN B, SADEGHIAN S S, et al. MIBS: a new lightweight block cipher[C]//8th International Conference on Cryptology and Network Security – CANS 2009. Kanazawa, Japan, 2009: 334-348.

[2] WU W L, ZHANG L. LBlock: a lightweight block cipher[C]//9th International Conference on Applied Cryptography and Network Security – ACNS 2011. Nerja, Spain, 2011: 327-344.

[3] OJHA S K, KUMAR N, JAIN K, et al. TWIS: a lightweight block cipher[C]//5th International Conference on Information Systems Security – ICISS 2009. Kolkata, India, 2009: 280-291.

[4] WU W L, ZHANG L, YU X L. The DBlock family of block ciphers[J]. Science China Information Sciences, 2015, 58(3): 1-14.

[5] LIU Y, GU D W, LIU Z Q, et al. Impossible differential attacks on reduced-round LBlock[C]//8th International Conference on Information Security Practice and Experience – ISPEC 2012. Hangzhou, China, 2012: 97-108.

[6] SASAKI Y, WANG L. Meet-in-the-middle technique for integral attacks against Feistel ciphers[C]//19th International Conference on Selected Areas in Cryptography – SAC 2012. Windsor, ON, Canada, 2013: 234-251.

[7] SASAKI Y, WANG L. Comprehensive study of integral analysis on 22-round LBlock[C]//15th International Conference on Information Security and Cryptology – ICISC 2012. Seoul, Korea, 2013: 156-169.

[8] LIU S S, GONG Z, WANG L B. Improved related-key differential attacks on reduced-round LBlock[C]//14th International Conference on Information and Communications Security – ICICS 2012. Hong Kong, China, 2012: 58-69.

[9] WEN L, WANG M Q, ZHAO J Y. Related-key impossible differential attack on reduced-round LBlock[J]. Computer Science and Technology, 2014, 29(11): 165-176.

[10] 吴寿昌. 对轻量级分组密码算法 LBlock 的线性分析[D].山东大学, 2014.
WU S C. Linear cryptanalysis of lightweight block cipher LBlock[D]. Shandong University, 2014.

[11] CHEN J G, MIYAJI A. Differential cryptanalysis and boomerang cryptanalysis of LBlock[C]//Security Engineering and Intelligence Information. Regensburg, Germany, 2013: 1-15.

[12] LU J Q. Cryptanalysis of block cipher[R]. University of London, 2016.

[13] BIHAM E. New types of cryptanalytic attacks using related key[J]. Journal of Cryptology, 1994, 7(4): 229-246.

[14] KNUDSEN L R. Cryptanalysis of LOKI91[C]//Advances in Cryptology–AUSCRYPT'92. Gold Coast. Queensland, Australia, 1992: 196-208.

[15] BIHAM E, BIRUUKOV A, SHAMIR A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C]//Advances in Cryptology – EUROCRYPT'99. Prague, Czech Republic, 1999: 12-23.

[16] WAGNER D. The boomerang attack[C]// 6th International Workshop on Fast Software Encryption – FSE'99. Rome, Italy, 1999: 156-170.

[17] 陈平, 廖福成, 卫宏儒. 对轻量级密码算法 MIBS 的相关密钥不可能差分攻击[J]. 通信学报, 2014, 35(2): 190-193.
CHEN P, LIAO F C, WEI H R. Related-key impossible differential attack on a lightweight block cipher[J]. Journal on Communications, 2014, 35(2): 190-193.

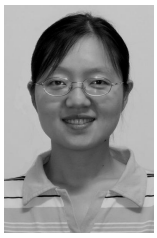
[18] MA X S, QIAO K X. Related-key rectangle attack on round-reduced Khudra block cipher[C]//The 9th International Conference on Network and System Security – NSS 2015. New York, NY, USA, 2015: 331-344.

[19] 付立仕, 金晨辉. MIBS-80 的 13 轮不可能差分分析[J]. 电子与信息学报, 2016, 38(4): 848-855.
FU L S, JIN C H. Impossible differential cryptanalysis on 13-round MIBS-80[J]. Journal of Electronics & Information Technology, 2016, 38(4): 848-855.

[20] 李曼曼, 陈少真. 对 ARIA 算法中间相遇攻击的改进[J]. 通信学报, 2015, 36(3): 277-282.
LI M M, CHEN S Z. Improved meet-in-the-middle attack on ARIA cipher[J]. Journal on Communications, 2015, 36(3): 277-282.

[21] KIRCANSKI A. Analysis of boomerang differential trails via a SAT-based constraint solver URSA[C]//13th International Conference on Applied Cryptography and Network Security – ACNS 2015. New York, NY, USA, 2015: 331-349.

作者简介：



谢敏（1976-），女，湖南桃源人，博士，西安电子科技大学副教授，主要研究方向为编码和密码。

牟彦利（1990-），女，河北沧州人，西安电子科技大学硕士生，主要研究方向为分组密码算法分析。