对分组密码的形式化函数分析及其应用

彭昌勇[1,2],朱创营[3],黄 莉[4],祝跃飞[1],王靳辉[2]
(1.解放军信息工程大学网络空间安全学院,河南郑州 450002;2.解放军信息工程大学理学院,河南郑州 450002;
3.桂林电子科技大学,广西桂林 510540;4.解放军信息工程大学科研部,河南郑州 450002)

摘 要: 本文给出了分组密码的新的分析方法:形式化函数分析,即通过符号计算将密文形式地表示为明文和密钥的函数.作为应用本文给出了 13 轮 LBlock 轻量级分组密码的一个中间相遇攻击.对 13 轮 LBlock 的中间相遇攻击的时间复杂度为 $2^{76.2}$次 13 轮 LBlock 加密,数据复杂度为 1 个已知明文.优于 Nicolas Courtois 等人在 FSE 2012 上给出的 8 轮代数攻击,其数据复杂度为 6 个已知明文.

关键词: 形式化函数分析; 形式化编码方法; 鲁班锁分组密码; 符号计算; 中间相遇攻击; 分组密码
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2013) 11-2314-03
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.11.032

Formal Function Cryptanalysis of Block Cipher and Its Application

PENG Chang-yong[1,2], ZHU Chuang-ying[3], HUANG Li[4], ZHU Yue-fei[1], WANG Jin-hui[2]
(1. *Cyberspace security college, PLA Information Engineering University, Zhengzhou, Henan* 450002, *China*; 2. *College of Science, PLA Information Engineering University, Zhengzhou, Henan* 450002, *China*; 3. *School of Computer and Control, Guillin University of Electronic Technology, Guilin, Guangxi* 510540, *China*; 4. *Scientific Research Department, PLA Information Engineering University, Zhengzhou, Henan* 450002, *China*)

Abstract: This paper introduces FFC(formal function cryptanalysis)of block cipher that expresses each bit in the ciphertext as pure formal functions in terms of the bits of the plaintext and master key by symbolic computation. As an application, we give a meet in the middle attack on 13-round LBlock lightweight block cipher. The meet in the middle attack has a complexity of $2^{76.2}$ 13-round LBlock encryption using only 1 known plaintext, which is better than the algebraic attack given by Nicolas Courtois etc. at FSE 2012 on 8-round LBlock, with data complexity 6 known plaintexs.

Key words: formal function cryptanalysis; method of formal coding; LBlock; symbolic computation; meet in the middle attack; block cipher

1 引言

文献[1]给出了分组密码的形式化编码(Method of Formal Coding)的分析方法,即将密文表示为明文和密钥的异或和.Schaumuller-Bichl[2,3]研究了该方法并指出其需要巨大的内存而无法实现.

受形式化编码思想的启发,本文提出了分组密码的新的分析方法——形式化函数分析.其思想是将密文表示为明文和密钥的形式上的函数,而并不给出函数的具体表达式.如密文的最低比特其可能的表达式为 $f(p1, p2, k1, k2, k3)$,其中 $p1, p2$ 是两个明文比特,$k1, k2, k3$ 是三个密文比特.而密文的形式化函数表示是可以通过符号计算的方法获得的.

作为一个应用,我们给出了当前密码学研究中比较热门的轻量级密码[4~9]算法中的一个——LBlock[4]的 13 轮简化版的一个中间相遇攻击.其时间复杂度为 $2^{76.2}$次 13 轮 LBlock 加密,数据复杂度为 1 个已知明文.

表 1 LBlock 算法的已有攻击结果总结

轮数	攻击类型	数据复杂度	时间复杂度	文献
8	代数攻击	6 个已知明文对	2^{30}小时	[10]
13	中间相遇攻击	1 个已知明文对	$2^{76.2}$次 13 轮 LBlock 加密	本文
18	积分攻击	$2^{62.3}$选择明文对	$2^{62.3}$次 18 轮 LBlock 加密	[4]
20	积分攻击	$2^{63.7}$选择明文对	$2^{63.7}$次 20 轮 LBlock 加密	[4]
20	不可能差分攻击	2^{63}选择明文对	$2^{72.7}$次 20 轮 LBlock 加密	[4]
21	不可能差分攻击	$2^{62.5}$选择明文对	$2^{73.7}$次 21 轮 LBlock 加密	[11]
22	相关密钥不可能差分攻击	2^{47}选择明文对	2^{70}次 22 轮 LBlock 加密	[12]

收稿日期:2012-09-11;修回日期:2013-01-20;责任编辑:蓝红杰
基金项目:郑州市科技创新团队项目(No.10CXTD150)

2 形式化函数分析

形式化函数分析的思想非常简单:即将密文的每比特形式地表示为明文和密钥的函数,而并不给出具体的表达式.先给出分组密码的每个组件的形式化函数表示.以一个 4 * 4 的 S 盒为例.设 S 盒的输入为 $x_3x_2x_1x_0$,则 S 盒的输出可以形式地表示为 $y_3(x_3,x_2,x_1,x_0)$, $y_2(x_3,x_2,x_1,x_0)$, $y_1(x_3,x_2,x_1,x_0)$, $y_0(x_3,x_2,x_1,x_0)$.分组密码的其他组件如线性层也可以形式地给出其表达式.有了每个组件的形式上的函数表示就可以给出整个算法以及其中间状态的形式上的函数表示.这些都可以比较容易地用符号计算实现.本文我们选择数学软件 Mathematica 7.0 作为符号计算的实现平台.

我们以一个微型的 SPN 结构的分组密码 toyBlockCipher 为例来具体说明.设该分组密码的密钥和分组长度都是 6 比特.非线性层即 S 层是两个相同的 3 * 3 的 S 盒的并.线性层即 P 层是对 6 比特进行左循环移 1 位的操作.第 i 轮的子密钥就是主密钥左循环移 i 位.1 轮的具体操作为:密钥加,S 层,P 层.轮数也视为算法的参数.经过 r 轮操作后,内部状态与主密钥异或后即为算法的输出密文.下面是该微型分组密码的 Mathematica 代码.

```
toyBlockCipher[p_,k_,r_]:=
  Module[{i,c},c=p;
For[i=1,i<=r,i++,
c=c+RotateLeft[k,i];
c={s3[c[[{1,2,3}]]],s2[c[[{1,2,3}]]],s1[c[[{1,2,3}]]],
s3[c[[{4,5,6}]]],s2[c[[{4,5,6}]]],s1[c[[{4,5,6}]]]};
c=RotateLeft[c,1]];
c=c+k;Return[c]]
```

在 Mathematica 7.0 中输入 toyBlockCipher[{$p6,p5,p4,p3,p2,p1$},{$k6,k5,k4,k3,k2,k1$},1]后,可以得到 1 轮 toyBlockCipher 算法在明文 $p6,p5,p4,p3,p2,p1$ 和密钥 $k6,k5,k4,k3,k2,k1$ 下的输出为:

$$\begin{aligned}
&\{k6+s2[\{k5+p6,k4+p5,k3+p4\}],\\
&k5+s1[\{k5+p6,k4+p5,k3+p4\}],\\
&k4+s3[\{k2+p3,k1+p2,k6+p1\}],\\
&k3+s2[\{k2+p3,k1+p2,k6+p1\}],\\
&k2+s1[\{k2+p3,k1+p2,k6+p1\}],\\
&k1+s3[\{k5+p6,k4+p5,k3+p4\}]\}.
\end{aligned}$$

完全类似以上的例子,我们可以比较容易地用符号计算的方法得到一个实际的分组密码的密文比特的形如 $f(p_1,\cdots,p_n,k_1,\cdots,k_m)$的形式化函数表示,其中 $p_1,\cdots,p_n$ 是明文比特,$k_1,\cdots,k_m$ 是主密钥比特.

3 形式化函数分析的应用—13 轮 LBlock 的中间相遇攻击

3.1 LBlock 算法描述

LBlock[4]是我国学者吴文玲等在 ACNS2011 上提出的轻量级分组密码,其加密轮数为 32 轮,分组和主密钥长度分别为 64 和 80 比特,是变体的 Feistel 结构.

设 $M=X_1\|X_0$ 为 64 比特明文,则加密过程为:

(1)对 $i=2,3,\cdots,33$,循环执行 $X_i=F(X_{i-1},K_{i-1}\oplus(X_{i-1}<<<8)$.其中 $X_{i-1}<<<8$ 表示对 X_{i-1}左循环移 8 位,K_{i-1}表示第 $i-1$ 轮的轮子密钥.

(2)输出密文 $C=X_{32}\|X_{33}$. LBlock 的加密结构图及 F 函数如图 1 所示.图 1 中每个 s_i 是 4 进 4 出的 S 盒.具体定义见文献[4].

3.2 13 轮 LBlock 的中间相遇攻击

中间相遇攻击首先是由 Diffie 和 Hellman 在文献[13]中所给出,其思想是将密码算法分别从明文端进行加密,从密文端解密,并使其在中间某轮相遇.中间相遇攻击 13 轮 LBlock 的中间相遇攻击基于用形式化函数分析的方法(其具体实现完全类似于第 2 节中的微型 SPN 分组密码)所得到的 13 轮 LBlock 的如下性质.

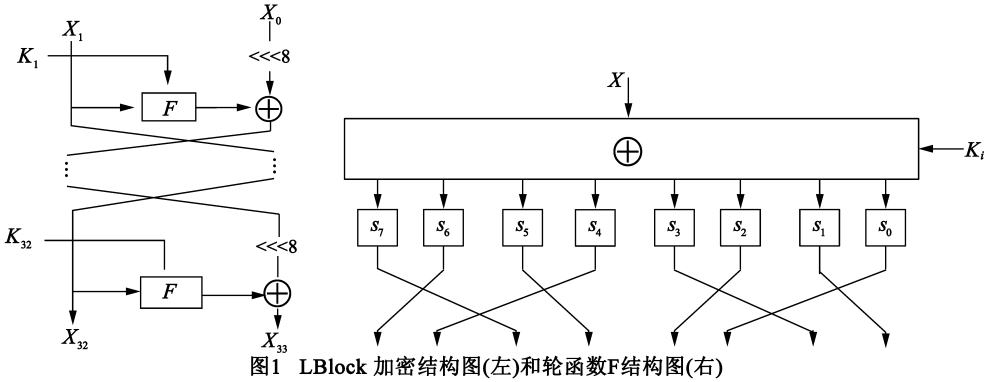


图1 LBlock 加密结构图(左)和轮函数F结构图(右)

定理 1 设 $E=E_2\cdot E_1$ 表示 13 轮 LBlock 的加密算法. E_1 是 1 到 6 轮的加密, E_2 是 7 到 13 轮的加密.设 $K=\{k_{79},k_{78},\cdots,k_0\}$是主密钥($k_0$ 是最低比特), $K'=K\setminus\{k_{69},k_9,k_8,k_7,k_6,k_5,k_4\}$,$(P,C)$是 13 轮 LBlock 的一

对明密对.设 $Y = y_{63}y_{62}\cdots y_0 = E_1(P,K)$,即 1 到 6 轮加密后的 64 比特输出,也等于 $E_2^{-1}(C,K)$,即第 13 轮到第 7 轮解密运算的输出.则 $y_i = f_i(P,K')$, $y_i = g_i(C,K')$ $i = 55,54,53,52$.

基于定理 1,我们给出 13 轮 LBlock 的中间相遇攻击,其数据复杂度为 1 个已知明文(记号同定理 1).

①任意选取 13 轮 LBlock 的一个明密对(P,C).

②对每个 $K' \in GF(2)^{73}$,计算 $y_{63}y_{62}\cdots y_0 = E_1(P,K')$和 $z_{63}z_{62}\cdots z_0 = E_2^{-1}(C,K')$.若对 $i = 55,54,53,52$ 都有 $y_i = z_i$,将该 K'保留.否则尝试下一个 K'.设最后保留下来的 K'的集合为κ.

③对每个 $K' \in \kappa$ 和每个$(k_{69},k_9,k_8,k_7,k_6,k_5,k_4) \in GF(2)^7$,若 $C = E(P,K)$,则 K 为密钥,否则继续③.

上述攻击的时间复杂度分析:经过步骤②后,κ 中平均所含的密钥数为 $2^{73}/2^4 = 2^{69}$,因此上述攻击的时间复杂度为:$2^{73} + 2^{69}2^7 = 2^{76.2}$次 13 轮 LBlock 加密.

4 结论

本文给出了分组密码的新的分析方法:形式化函数分析.作为应用给出了 13 轮 LBlock 的一个中间相遇攻击.文中对 LBlock 的形式化函数分析的方法具有一般性,也可以用来对其他分组密码进行分析,其攻击过程完全类似.形式化函数分析对一个具体的分组密码能够攻击到多少轮取决于算法的扩散性.扩散性越慢,形式化函数分析所能攻击的轮数越多,否则就越少.

参考文献

[1] M E Hellman, R. Merkle, R. Schroppel, L Washington, W Diffe, S Pohlig, P Schweitzer. Results of an Initial Attempt to cryptanalyze the NBS Data Encryption Standard[R]. Stanford Univercity: Technical Report, SEL 76 – 042, 1976. 3 – 10.

[2] Ingrid Schaumuller-Bichl. Zur Analyse DES Data Encryption Standard UndSynthese Verwandter Chiffriersysteme[D]. Linz University, 1981. 17 – 27.

[3] I Schaumuller-Bichl. Cryptanalysis of the data encryption standard by the method of formal coding[A]. David Chaum. Advances in Cryptology, Proceedings of CRYPTO 1983[C]. USA: Springer-Verlag, LNCS 149, 1983. 235 – 255.

[4] Wenling Wu, Lei Zhang. LBlock: A lightweight block cipher [A]. 2011 9th International Conference on Applied Cryptography and Network Security[C]. Spain: Springer-Verlag, LNCS 6715, 2011. 327 – 344.

[5] 张文英,刘祥忠.对基于 NLFSR 分组密码 KTANTAN32 的相关密钥中间相遇代数攻击[J].电子学报,2012,40(10):2097 – 2100.
Zhang Wen-ying, Liu Xiang-zhong. An related-key meet-in-the-middle algebraic attack on the NLFSR based block cipher KTANTAN32[J]. Acta Electronica Sinica, 2012, 40(10): 2097 – 2100. (in Chinese)

[6] 李昕,林东岱.对 Bivium 流密码的变元猜测代数攻击[J].电子学报,2011,39(8):1727 – 1732.
Li Xin, Lin Dong-dai. Guessing specific variables in algebraic attacks on bivium[J]. Acta Electronica Sinica, 2011, 39(8): 1727 – 1732. (in Chinese)

[7] 唐学海,孙兵,李超.对 8 轮 CLEFIA 算法的一种现实攻击[J].电子学报,2011,20(7):1608 – 1612.
Tang Xue-hai, Sun Bing, Li Chao. A real-world attack of 8-round CLEFIA[J]. Acta Electronica Sinica, 2011, 20(7): 1608 – 1612. (in Chinese)

[8] Izadi, M Sadeghiyan, B Sadeghian, S Khanooki. MIBS: A new lightweight block cipher[A], Otsuka, Akira. 2009 8th International Conference on Cryptology and Network Security[C]. Japan: Springer-Verlag, LNCS 5888, 2009. 334 – 348.

[9] Guo J, Peyrin T, Poschmann A, Robshaw M. The LED block cipher[A]. 2011 Workshop on Cryptographic Hardware and Embedded Systems[C]. Japan: Springer-Verlag, LNCS 6917, 2011. 326 – 341.

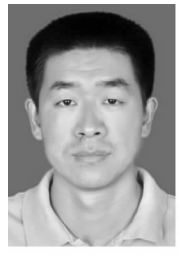
[10] Nicolas T Courtois, Pouyan Sepehrdad, Petr Susil, Serge Vaudenay. ElimLin algorithm revisited[A]. Fast Software Encryption 2012[C]. Washington, DC: Springer-Verlag, LNCS 7549, 2012. 306 – 325.

[11] Ya Liu, Dawu Gu, Zhiqiang Liu, Wei Li. Impossible differential attacks on reduced-round LBlock[A]. The 8th International Conference on Information Security Practice and Experience 2012 [C]. Hangzhou: Springer-Verlag, LNCS 7232, 2012. 97 – 108.

[12] Marine Minier , Maria Naya-Plasencia. A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock[J]. Information Processing Letters, 2012 (112): 624 – 629.

[13] Diffie, W, Hellman, M. Special feature exhaustive cryptanalysis of the NBS data encryption standard [J]. Computer, 10, 1977: 74 – 84.

作者简介



彭昌勇 男,1974 年生于湖南永州.解放军信息工程大学博士研究生.研究方向为分组密码.
E-mail: cy.peng@163.com

朱创营 男,1986 年生于河南尉氏.硕士生.研究方向为形式化验证和信息安全.
E-mail: 39463021@qq.com