扩展的代数侧信道攻击及其应用

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 541004;4.解放军信息工程大学科研部,河南郑州 450002)

摘 要: Renauld 等人提出的代数侧信道攻击是将代数攻击和侧信道攻击结合起来的一种对分组密码的攻击方法.目前的研究主要针对算法的 8-bit 实现平台,对于更大的如 64-bit 实现平台,未见文献讨论.为此,本文提出一种扩展的代数侧信道攻击,直接将侧信道信息表示为密钥的显式函数.相比于通常的代数侧信道攻击,所需泄露信息更少.作为应用,给出了对 LBlock 轻量级分组密码的扩展的代数侧信道攻击,结果如下:对于 64-bit 平台实现的 LBlock,假设其 1-3 轮输出的 Hamming 重量可以准确获得,则利用 35 个已知明文,便可建立关于 LBlock 80-bit 主密钥的非线性方程组;在普通的 PC 机上,利用 Magma 数学软件 v2.12-16 求 Groebner 基,1 分钟内可以求得 80-bit 主密钥.这是对 LBlock 的首个代数侧信道攻击,同时说明 Renauld 等人给出的对代数侧信道攻击的其中一个防范方法:"将实现方法从 8-bit 平台转移到更大的设备"是不够的.

关键词: 轻量级分组密码; 鲁班锁分组密码; 代数侧信道攻击; Magma 数学软件; Groebner 基
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2013)05-0859-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.05.005

Extended Algebraic-Side Channel Attack 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* 541004, *China*;
4. *Scientific Research Department, PLA Information Engineering University, Zhengzhou, Henan* 450002, *China*)

Abstract: Algebraic-side channel attack(ASCA) was proposed by Renauld et al. which combines algebraic attack and side channel attack. The current research of ASCA mainly focuses on the 8-bit implementation of a block cipher. For 64-bit platform, there is no such research. This paper gives an extended algebraic side channel attack which represents the leaked information as explicit function of the key bits. Compared with the original ASCA, the extended ASCA needs less leaked information. As an application, we give an extended ASCA on LBlock light weight block cipher: For LBlock implemented on 64-bit platform, if the Hamming weight of the output of 1-3 round of LBlock can be obtained without error, then with 35 known plaintexts, an equation system concerning the 80 bit maser key can be set up; on a general PC, the 80 bit master key can be obtained in a minute by using Magma mathematical software v2.12-16 to find the Groebner basis. This is the first ASCA attack on LBlock, which shows that the method of moving form 8-bit platform to larger devices suggested by Renauld et al. to prevent ASCA is not enough.

Key words: lightweight block cipher; LBlock; algebraic side channel attack; Magma mathematical software; Groebner basis

1 引言

轻量级分组密码在 RFID、传感网等受限环境下有重要应用,是目前密码学的一个热点研究领域[1~9].对轻量级分组密码的安全性分析和传统分组密码的分析方法类似:主要有线性、差分及代数攻击等.这些攻击都是传统的基于数学的攻击.最近的一个趋势是将其与侧信道攻击结合起来,如 Renauld 等人提出的代数侧信道攻击[10~12]就是将代数攻击和侧信道攻击进行结合.目前对代数侧信道攻击的研究主要是针对算法的 8-bit 实现平台,对于更大的,如 64-bit 实现平台,未见文献讨论.Renauld 等人[10,11]认为代数侧信道攻击对 64-bit 平台可能失效.为了研究代数侧信道攻击在 64-bit 平台下的有效性,本文提出一种扩展的代数侧信道攻击,其思

收稿日期:2012-09-28;修回日期:2013-03-04
基金项目:郑州市科技创新团队项目(No.10CXTD150)

想是直接将侧信道信息表示为密钥和明文显式函数.

本文我们假设侧信道信息已经准确地获得,对于侧信道信息如何获得不具体讨论.这里我们使用[10,11]中的 Hamming 重量泄露模型.作为应用,我们对 LBlock[1]轻量级分组密码在 64bit 平台上的实现进行模拟的扩展代数侧信道攻击(实际上对任何实现平台如 8bit、32bit 等,该方法同样适用),结果如下:对于 64bit 平台实现的 LBlock,假设其 1-3 轮输出状态的 Hamming 重量可以准确地获得,则利用 35 个已知明文可以建立关于 LBlock 80bit 主密钥的非线性方程组;在一个普通的 PC 机上(2GHZ CPU,2G RAM),利用 Magma 数学软件 v2.12-16 求 Groebner 基,1 秒内即可以求得 LBlock 的 80bit 主密钥.这是对 LBlock 的首个代数侧信道攻击.同时说明 Renauld 等人给出的对代数侧信道攻击的其中一个防范方法:"将实现方法从 8-bit 平台转移到更大的设备"是不够的.

本文提出的扩展的代数侧信道攻击也可以视为是形式化编码侧信道攻击,即将形式化编码的攻击[13]和侧信道攻击相结合.形式化编码的思想是将密码算法的输出,即密文表示为明文和密钥的完全展开的多项式表示——代数正规型(即单项式的异或和).由于该方法需要巨大的内存而无法实现,因此自 1982 年美密会上提出来后并未受到密码学界的重视.为了克服形式化编码方法的困难,本文对其进行了扩展,即将密文或算法的中间状态表示为明文和密钥的不完全展开的多项式(如 $y=(x+w)(a+b(c+d))$,其代数正规型为 $y=xa+xbc+xbd+wa+wbc+wbd$).并对 LBlock 轻量级分组密码用符号计算软件 Mathematica 进行了实现,得到了 LBlock 前 7 轮中间状态的以明文和主密钥为自变量的函数表达式.进而我们将扩展的形式化编码与侧信道攻击结合,得到形式化编码侧信道攻击(因此下面我们也称本文的扩展的代数侧信道攻击为形式化编码侧信道攻击).

LBlock 是我国学者吴文玲和张蕾在 ACNS2011 上提出的 32 轮类 Feistel 结构的轻量级分组密码,其密钥和分组长度分别为 80 和 64bit.本文对 LBlock 的形式化编码侧信道攻击具体实现思路如下:先用符号计算将 LBlock 的 1-3 轮的中间状态的每个比特表示为主密钥的显式多项式函数,进而可以将中间状态的 Hamming 重量 Mod2(即中间状态的 64 比特的 mod2 加)的结果表示为主密钥的显式多项式函数,在 Hamming 重量 Mod2 通过侧信道得到的前提下(设攻击者可以得到 35 个 1-3 轮的中间状态的 Hamming 重量),可以得到关于主密钥的方程组,利用 Magma 数学软件求解 Groebner 基,即可得到 80bit 主密钥.

2 LBlock 算法描述

LBlock 分组和主密钥长度分别为 64 和 80bit,加密轮数为 32 轮,是变体的 Feistel 结构.

设 $M=X_1\parallel X_0$ 为 64bit 明文,则加密过程如下:

(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 $C=X_{32}\parallel X_{33}$.

LBlock 的加密结构图如下:

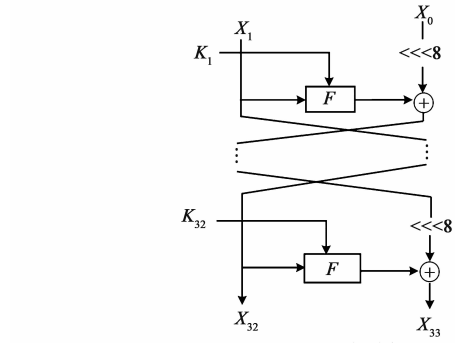


图1 LBlock 加密结构图

这里 $K_1,\cdots,K_{32}$都是 32bit 的轮子密钥,由主密钥通过密钥生成算法所生成.LBlock 的详细描述见文献[1].

3 形式化编码侧信道攻击在 LBlock 上应用

形式化编码侧信道攻击和代数侧信道攻击[10,11]类似,分为离线阶段和在线阶段两部分.代数侧信道攻击中是将泄漏的信息(如 Hamming 重量)用线性方程表示出来,插入到代数攻击的方程组中去.与代数侧信道攻击不同的是,这里我们直接将泄漏的信息(本文是 Hamming 重量 Mod2)表示为以明文和主密钥为自变量的显式函数.

离线部分:通过符号计算得到中间状态的 Hamming 重量 Mod2 的方程表示(以明文和主密钥为自变量的多项式).

在线部分:通过侧信道手段得到 Hamming 重量的具体数值,将其代入离线部分所得到的方程,用方程求解器(本文我们选用 Magma 软件求 Groebner 基的方法)得到主密钥的值.

这里我们假设攻击者已经获得了一些中间状态的 Hamming 重量,不考虑 Hamming 重量具体如何获得.

3.1 离线攻击部分:LBlock 中间状态 Hamming 重量 Mod2 的函数表示

我们利用数学软件 Mathematica 7.0 的符号计算功能,可以得到 LBlock 算法 1-7 轮输出的函数表示(视为明文和主密钥的函数).其具体实现这里不再给出,参见文献[14].

下面我们列出 LBlock 前几轮的代数次数与项数.记 $K=k_{79}k_{78}\cdots k_1k_0$ 为 LBlock 的 80bit 主密钥(最右边为最低比特位),$P=p_{63}p_{62}\cdots p_1p_0$ 为 64 比特明文.由于 LBlock 是类 Feistel 结构,这里只需要列出其低 32bit 的次数与项数即可.第 4 轮我们只能得到部分比特的次数与项数.第 5 轮到第 7 轮,尽管我们得到了其形如 $y=(x+w)(a+b(c+d))$的未完全展开的代数表达式,但要将其完全展开太复杂,因此无法给出其次数与项数.第一轮输出低 32bit 的次数与项数均为 1.

表 1　第二轮输出低 32bit 的次数与项数(31 为最高位,0 为最低位,下同)

位置	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
次数	3	3	2	2	2	3	3	2	3	3	2	2	3	2	3	2
项数	36	37	12	16	16	24	38	13	24	38	13	16	31	15	36	13
位置	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
次数	2	3	2	3	3	3	2	2	3	2	3	2	3	3	2	2
项数	15	31	13	36	24	38	16	13	37	16	36	12	31	36	13	15

表 2　第三轮输出低 32bit 的次数与项数

位置	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
次数	7	7	6	6	4	5	5	4	7	7	5	6	5	4	5	4
项数	1063	1700	293	415	164	438	820	124	1206	1744	334	432	540	223	809	161
位置	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
次数	4	5	4	5	5	5	4	4	5	4	5	4	5	5	4	4
项数	218	603	161	809	618	904	219	170	763	220	580	123	524	785	142	157

表 3　第四轮输出低 32bit 中部分比特的次数与项数

位置	29	28	27	4	1	0
次数	8	8	6	6	6	6
项数	3474	8038	3449	2219	2655	2614

由 1-3 轮输出的函数表示,可以得到 1-3 轮输出的 Hamming 重量 Mod2(分别记为 h_1、h_2、h_3)的函数表示,这里仅给出第 1 轮输出的 Hamming 重量 Mod2 的函数表示:

$$h_1=f_1(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_{49},k_{48})=$$
$$k_{48}+k_{49}+k_{54}+k_{58}+k_{60}+k_{62}+k_{63}+k_{64}+k_{65}+k_{70}+k_{72}+k_{74}+k_{75}+k_{76}+k_{77}+p_0+p_1+p_{10}+p_{11}+p_{12}+p_{13}+p_{14}+p_{15}+p_{16}+p_{17}+p_{18}+p_{19}+p_2+p_{20}+p_{21}+p_{22}+p_{23}+p_{24}+p_{25}+p_{26}+p_{27}+p_{28}+p_{29}+p_3+p_{30}+p_{31}+(k_{48}+p_{32})(k_{49}+p_{33})+p_{34}+(k_{48}+p_{32})(k_{50}+p_{34})+p_{35}+(k_{48}+p_{32})(k_{51}+p_{35})+(k_{49}+p_{33})(k_{51}+p_{35})+(k_{49}+p_{33})(k_{50}+p_{34})(k_{51}+p_{35})+p_{36}+p_{37}+(k_{52}+p_{36})(k_{53}+p_{37})+(k_{52}+p_{36})(k_{54}+p_{38})+p_{39}+(k_{52}+p_{36})(k_{55}+p_{39})+(k_{53}+p_{37})(k_{55}+p_{39})+(k_{54}+p_{38})(k_{55}+p_{39})+(k_{53}+p_{37})(k_{54}+p_{38})(k_{55}+p_{39})+p_4+p_{40}+p_{41}+(k_{56}+p_{40})(k_{57}+p_{41})+(k_{56}+p_{40})(k_{58}+p_{42})+p_{43}+(k_{56}+p_{40})(k_{59}+p_{43})+(k_{57}+p_{41})(k_{59}+p_{43})+(k_{58}+p_{42})(k_{59}+p_{43})+(k_{57}+p_{41})(k_{58}+p_{42})(k_{59}+p_{43})+p_{45}+(k_{60}+p_{44})(k_{61}+p_{45})+(k_{60}+p_{44})(k_{62}+p_{46})+(k_{60}+p_{44})(k_{63}+p_{47})+(k_{62}+p_{46})(k_{63}+p_{47})+(k_{61}+p_{45})(k_{62}+p_{46})(k_{63}+p_{47})+(k_{64}+p_{48})(k_{65}+p_{49})+p_5+p_{50}+(k_{64}+p_{48})(k_{66}+p_{50})+p_{51}+(k_{64}+p_{48})(k_{67}+p_{51})+(k_{65}+p_{49})(k_{67}+p_{51})+(k_{65}+p_{49})(k_{66}+p_{50})(k_{67}+p_{51})+p_{52}+p_{53}+(k_{68}+p_{52})(k_{69}+p_{53})+(k_{68}+p_{52})(k_{70}+p_{54})+p_{55}+(k_{68}+p_{52})(k_{71}+p_{55})+(k_{69}+p_{53})(k_{71}+p_{55})+(k_{70}+p_{54})(k_{71}+p_{55})+(k_{69}+p_{53})(k_{70}+p_{54})(k_{71}+p_{55})+p_{57}+(k_{72}+p_{56})(k_{73}+p_{57})+(k_{72}+p_{56})(k_{74}+p_{58})+(k_{72}+p_{56})(k_{75}+p_{59})+(k_{74}+p_{58})(k_{75}+p_{59})+(k_{73}+p_{57})(k_{74}+p_{58})(k_{75}+p_{59})+p_6+(k_{76}+p_{60})(k_{77}+p_{61})+p_{62}+(k_{76}+p_{60})(k_{78}+p_{62})+p_{63}+(k_{76}+p_{60})(k_{79}+p_{63})+(k_{77}+p_{61})(k_{79}+p_{63})+(k_{77}+p_{61})(k_{78}+p_{62})(k_{79}+p_{63})+p_7+p_8+p_9.$$

如果将上式完全展开,写成代数正规型,则有 268 项.

由上面的函数表示,第 1 轮输出的 Hamming 重量 Mod2,即 h_1,只与主密钥中的 32bit $k_{79},\cdots,k_{49},k_{48}$有关,即有 $h_1=f_1(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_{49},k_{48})$.对于第 2 轮和第 3 轮输出的 Hamming 重量 Mod2,即 h_2、h_3,其函数表示太复杂,这里不具体给出,h_2 的代数正规型所含的项数为 6332(将明文和主密钥都视为符号变量),对于 h_3,我们仅仅得到了其未展开的多项式表示.这里我们仅给出 h_2、h_3 的函数表示中所涉及的变量,将 h_1、h_2、h_3 的函数表示放在一起,我们得到了关于主密钥 $k_{79},k_{78},\cdots k_1,k_0$ 的方程组:

$$\begin{cases}h_1=f_1(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_{49},k_{48})\\h_2=f_2(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_{20},k_{19})\\h_3=f_3(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_1,k_0)\end{cases}\quad(1)$$

3.2 在线攻击部分:方程组的求解

方程组(1)如果直接求解很复杂,因为 h_2、h_3 的函数表示比较复杂.注意到方程组(1)中各个部分的复杂性不相同,我们采用分别征服的方法.即先求 h_1 中所涉及的变量 $k_{79}k_{78}\cdots k_{49}k_{48}$,将其代入到 $h_2=f_2(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_{20},k_{19})$,求得 $k_{47},\cdots,k_{20},k_{19}$,最后将前两次求得的 $k_{79},\cdots,k_{20},k_{19}$ 代入到 $h_3=f_3(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_1,k_0)$ 解得剩下的 19bit 密钥 $k_{18},\cdots,k_1,k_0$.

我们对上述过程进行了模拟实验.实验环境:操作系统为 winxp sp3,CPU 2GHZ,2G 内存.实验软件为:Mathematica 7.0 和 Magma v2.12-16.

3.2.1 利用 $h_1=f_1(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_{49},k_{48})$ 获得密钥的高 32 比特 $k_{79}k_{78}\cdots k_{49}k_{48}$

设攻击者获得了 n_1 个已知明文 $P_i=p_{63,i},\cdots,p_{1,i},p_{0,i}(i=1,\cdots,n_1)$ 以及对应的 n_1 个第一轮输出的 Hamming 重量,从而得到了其 mod2 的值 h_1,记为 $h_{1,1},\cdots,h_{1,n_1}$.则得到关于密钥的高 32 比特 $k_{79}k_{78}\cdots k_{49}k_{48}$ 的方程组为:

$$\begin{cases} h_{1,1}=f_1(p_{63,1},\cdots,p_{1,1},p_{0,1},k_{79},\cdots,k_{49},k_{48}) \\ h_{1,2}=f_1(p_{63,2},\cdots,p_{1,2},p_{0,2},k_{79},\cdots,k_{49},k_{48}) \\ \cdots\cdots \\ h_{1,n_1}=f_1(p_{63,n_1},\cdots,p_{1,n_1},p_{0,n_1},k_{79},\cdots,k_{49},k_{48}) \end{cases} \tag{2}$$

我们对上述过程进行了如下的模拟实验:

(1)用 Mathematica 生成随机的一组密钥 $K=k_{79}k_{78}\cdots k_1k_0$.(这可以用 Mathematica 的内置命令 Table[RandomInteger[],{80}]来实现)

(2)用 Mathematica 随机生成 n_1 个已知明文 $P_i=p_{63,i},\cdots,p_{1,i},p_{0,i}(i=1,\cdots,n_1)$.用(1)中的密钥 K 加密这些明文,输出其 Hamming 重量 mod2 的值 $h_{1,1},\cdots,h_{1,n_1}$.将 $h_{1,1},\cdots,h_{1,n_1}$ 和 $P_i=p_{63,i},\cdots,p_{1,i},p_{0,i}(i=1,\cdots,n_1)$ 的值代入到方程组(2).

(3)用 Mathematica 将方程组(2)按照 Magma 求 Grobner 基要求的格式写成文本文件 mg.txt 输出.

(4)将(3)中的文本文件用 Magma 的命令"load mg.txt;"求 Grobner 基,得到方程组(2)的解.

我们分别对方程组(2)在 $n_1=35,40$ 进行了 50 次模拟(以下每种情况都是 50 次模拟),结果如下:

表 4 LBlock 第一轮 Hamming 重量泄露所得方程组(2)的求解情况

泄露的第一轮 Hamming 重量数	Magma 求解情况	平均求解时间
35	50 次中 4 次得到 2 个解,1 次得到 3 个解,45 次得到唯一的正确解	<1 秒
40	50 次中每次都得到唯一的正确解	<1 秒

3.2.2 利用 $h_2=f_2(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_{20},k_{19})$ 在 3.2.1 的基础上再获得密钥的中间 29 比特 $k_{47},\cdots,k_{20},k_{19}$

这里我们将 3.2.1 中所得到的解代入 $h_2=f_2(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_{20},k_{19})$ 中.设攻击者获得了 n_2 个已知明文 $P_i=p_{63,i},\cdots,p_{1,i},p_{0,i}(i=1,\cdots,n_2)$ 以及对应的 n_2 个第二轮输出的 Hamming 重量,从而得到了其 mod2 的值 h_2,记为 $h_{2,1},\cdots,h_{2,n_2}$.则得到关于密钥的中间 29bit $k_{47},\cdots,k_{20},k_{19}$ 的方程组

$$\begin{cases} h_{2,1}=f_2(p_{63,1},\cdots,p_{1,1},p_{0,1},k_{79},\cdots,k_{48},k_{47},\cdots,k_{19}) \\ h_{2,2}=f_2(p_{63,2},\cdots,p_{1,2},p_{0,2},k_{79},\cdots,k_{48},k_{47},\cdots,k_{19}) \\ \cdots\cdots \\ h_{2,n_2}=f_2(p_{63,n_2},\cdots,p_{1,n_2},p_{0,n_2},k_{79},\cdots,k_{48},k_{47},\cdots,k_{19}) \end{cases} \tag{3}$$

模拟实验的步骤和 3.2.1 完全类似,这里不再赘述.方程组(3)的模拟结果如下:

表 5 3.2.1 中所得高 32bit 为错误解时方程组(3)的求解情况

泄露的第二轮 Hamming 重量数	Magma 求解情况	平均求解时间
35	50 次都无解	<1 秒
40	50 次都无解	<1 秒

表 6 3.2.1 中所得高 32bit 为正确解时方程组(3)的求解情况

泄露的第二轮 Hamming 重量数	Magma 求解情况	平均求解时间
35	50 次中 49 次获得唯一解,1 次获得 2 个解	<1 秒
40	50 次中每次都获得 29 比特	<1 秒

3.2.3 利用 $h_3=f_3(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_1,k_0)$ 在 3.2.1 和 3.2.2 的基础上再获得密钥的低 19 比特 $k_{18},\cdots,k_1,k_0$

这里我们将 3.2.1 和 3.2.2 中所得到的解代入到 $h_3=f_3(p_{63},p_{62},\cdots,p_1,p_0,k_{79},\cdots,k_1,k_0)$ 中.设攻击者获得了 n_3 个已知明文 $P_i=p_{63,i},\cdots,p_{1,i},p_{0,i}(i=1,\cdots,n_3)$ 以及对应的 n_3 个第三轮输出的 Hamming 重量,从而得到了其 mod2 的值 h_3,记为 $h_{3,1},\cdots,h_{3,n_3}$.那么得到关于密钥的低 19 比特 $k_{18},\cdots,k_1,k_0$ 的方程组:

$$\begin{cases} h_{3,1}=f_3(p_{63,1},\cdots,p_{1,1},p_{0,1},k_{79},\cdots,k_{19},k_{18},k_{17},\cdots,k_0) \\ h_{3,2}=f_3(p_{63,2},\cdots,p_{1,2},p_{0,2},k_{79},\cdots,k_{19},k_{18},k_{17},\cdots,k_0) \\ \cdots\cdots \\ h_{3,n_3}=f_3(p_{63,n_3},\cdots,p_{1,n_3},p_{0,n_3},k_{79},\cdots,k_{19},k_{18},k_{17},\cdots,k_0) \end{cases} \tag{4}$$

模拟实验的步骤也和 3.2.1 完全类似,不再赘述.方程组(4)的模拟结果如下:

表 7　3.2.1 和 3.2.2 中所得高 61bit 为错误解时，方程组(4)的求解情况

泄露的第三轮 Hamming 重量数	Magma 求解情况	平均求解时间
22	50 次都无解	< 1 秒
30	50 次都无解	< 1 秒

表 8　3.2.1 和 3.2.2 中所得的密钥的高 61bit 为正确解时方程组(4)的求解情况

泄露的第三轮 Hamming 重量数	Magma 求解情况	平均求解时间
22	50 次中 44 次得到唯一的正确解，4 次得到 2 个解，1 次得到 3 个解	< 1 秒
30	50 次中每次都得到唯一的正确解	< 1 秒

3.2.4　最终的求解结果

根据 3.2.1 到 3.2.3 的模拟结果，我们可以得到对 LBlock 的扩展的代数侧信道攻击结果如下：

给定 35 个已知明文以及 92 个 1-3 轮输出的 Hamming 重量(其中 35 个 1 轮的，35 个 2 轮的，22 个 3 轮的)，则可以通过 Magma 求 Grobner 基 1 分钟内恢复 LBlock 的 80bit 主密钥(实际上所需要的 Hamming 重量数还可以进一步降低. 如得到密钥的高 61bit 后，低 19bit 可以穷举，这时候只需要 70 个 Hamming 重量泄露).

4　结论

本文我们结合形式化编码与侧信道攻击，提出了形式化编码侧信道攻击方法，该方法可以视为是一种扩展的代数侧信道攻击. 文中通过该方法对 LBlock 分组密码进行了有效的攻击，模拟实验表明，代数侧信道攻击对于 64bit 等大平台也是适用的. 该方法具有一般适用性，也可以用于对其他分组密码算法的攻击. 本文接下来的工作是用该方法对其他分组密码算法的形式化编码侧信道攻击.

参考文献

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

[2] Bogdanov A, Knudsen L R, Leander G, Parr C, Poschmann A, Robshaw M J B, Seurin Y, Vikkelsoe C. PRESENT: an ultra-lightweight block cipher [A]. Paillier, P, Verbauwhede, I. 2007 Workshop on Cryptographic Hardware and Embedded Systems [C]. Austria: Springer-Verlag, LNCS 4727, 2007. 450 – 466.

[3] De Canniere, C, Dunkelman, Orr, Knezevic, M. KATAN and KTANTAN-a family of small and effcient hardware-oriented block ciphers [A]. Clavier, C, Gaj, K. 2009 Workshop on Cryptographic Hardware and Embedded Systems [C]. Switzerland: Springer-Verlag, LNCS 5747, 2009. 272 – 288.

[4] Lim C, Korkishko T. mCrypton-a lightweight block cipher for security of low-cost RFID tags and sensors [A]. JooSeok Song, Taekyoung Kwon, Moti Yung. 2005 6th Workshop on Information Security Applications [C]. Korea: Springer-Verlag, LNCS 3786, 2006. 243 – 258.

[5] Leander G, Paar C, Poschmann A. New lightweight DES variants [A]. Alex Biryukov. 2007 14th Fast Software Encryption [C]. Luxembourg: Springer-Verlag, LNCS 4593, 2007. 196 – 210.

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

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

[8] 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)

[9] 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)

[10] Mathieu Renauld, Francois-Xavier Standaert. Algebraic side-channel attacks [A]. Feng Bao, Moti Yung, Dongdai Lin, and Jiwu Jing. 2009 5th China International Conference on Information Security and Cryptology [C]. China: Springer-Verlag, LNCS 6151, 2009. 393 – 410.

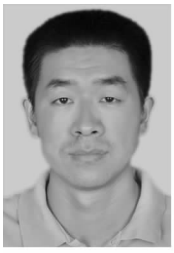
[11] Mathieu Renauld, Franois-Xavier Standaert, Nicolas Veyrat-Charvillon. Algebraic side-channel attacks on the AES: Why time also matters in DPA [A]. Christophe Clavier and Kris Gaj. 2009 Workshop on Cryptographic Hardware and Embedded Systems [C]. Switzerland: Springer-Verlag, LNCS 5747, 2009. 97 – 111.

[12] X J Zhao, S Z Guo, F. Zhang, et al. MDASCA: an enhanced algebraic side-channel attack for error tolerance and new leakage model exploitation [A]. Schindler, Werner; Huss, Sorin. 2012 3rd International Workshop on Constructive Side-Channel Analysis and Secure Design [C]. Germany: Springer-Verlag, LNCS 7275, 2012. 231 – 248.

[13] 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.

[14] 彭昌勇,祝跃飞,顾纯祥,米顺强. 1 ~ 5 轮 LBlock 的多项式表示及完全性分析[J]. 计算机工程,2012,38(9):155 – 157.
Peng Chang-yong, Zhu Yue-fei, Gu Cun-xiang et al. Polynomial expression and completeness analysis of 1 ~ 5 round LBlock [J]. Computer Engineering, 2012, 38(9): 155 – 157. (in Chinese)

作者简介



彭昌勇(通讯作者) 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