立方攻击研究综述*

马云飞, 王 韬, 陈 浩, 黄长阳
(军械工程学院 信息工程系, 石家庄 050003)

摘 要: 立方攻击是一种基于高阶差分理论的新型代数攻击方法,只要输出比特能够表示成关于明文变量和密钥变量的低次多元方程,立方攻击就有可能攻破此类密码。近年来立方攻击研究迅速开展,取得了一系列重要的成果。首先介绍了立方攻击原理及其变种:非线性立方攻击、立方测试和动态立方攻击;总结了基于中间状态泄露和基于故障信息泄露的两种旁路立方攻击模型及容错机制,给出了立方攻击扩展研究内容;最后分析了已有研究的不足并预测了下一步可能的研究方向。

关键词: 高阶差分; 代数攻击; 立方攻击; 旁路立方攻击
中图分类号: TP309.2 **文献标志码**: A **文章编号**: 1001-3695(2018)08-2245-06
doi:10.3969/j.issn.1001-3695.2018.08.002

Survey of cube attack

Ma Yunfei, Wang Tao, Chen Hao, Huang Changyang
(*Dept. of Information Engineering, Ordnance Engineering College, Shijiazhuang* 050003, *China*)

Abstract: The cube attack is a new type of algebraic attack based on higher-order difference theory. Cube attack could break any cipher if the output-bits could be represented as low-degree multivariate polynomials of public and secret variables. The research on cube attack was carried out rapidly and achieved a series of outcomes in recent years. This paper introduced the cube attack and its varieties: non-linear cube attack, cube tester, dynamic cube attack at first. Then it summarized two side-channel cube attack models which were based on internal states leakage and fault information leakage and analyzed fault-tolerant mechanisms after that. It gave some extended study on cube attack as well. Finally, it pointed out the shortcomings in existed researches and predicted the possible directions for further study.

Key words: higher-order difference; algebraic attack; cube attack; side-channel cube attack

近年来,针对现代密码体制的攻击方法可分为两类,一类是基于数学分析的攻击方法,另一类是基于密码实现旁路泄露的攻击方法。基于数学分析的攻击方法有差分攻击[1]、不可能差分攻击[2]、线性攻击[3]、代数攻击[4]等。尤其是 Courtois 等人[4]提出的代数攻击思想,将加密过程看做一系列复杂的代数运算,将密钥恢复转换为超定多变元高次方程组求解,为密码分析学提供了新思路,受到学者的广泛关注。

2008 年,Shamir 等人在高阶差分攻击(HODA)[5]和高阶 IV 差分攻击(AIDA)[6]基础上,提出了一种新型代数攻击——立方攻击(cube attack)[7]。只要算法的运算结果能表示成由密钥变量和明文变量组成的多项式,就可以通过该方法求得若干位密钥变量,甚至攻破整个密钥。立方攻击的优点在于可以在未知密码算法内部结构的前提下获得成功,因此该方法实用性很强。目前,立方分析已经对流密码 Trivium[7]、Hitag2[8]、Grain-128[9]和哈希函数 MD6[10]进行了成功分析。但对于分组密码,由于代数表达式次数和项数随着轮数增加急剧变大,使得多项式次数估算及立方体表示十分困难。

2009 年,Dinur 等人[11]将立方攻击和旁路攻击结合,提出旁路立方攻击(side channel cube analysis,SCCA)的思想。传统立方攻击由于全轮加密后多项式次数比较高,所以很难搜索到低次多项式。旁路立方攻击利用旁路攻击方法恢复中间密码状态比特,使得多项式的次数大大降低,提高了攻击的效率。旁路立方攻击已成功对 PRESENT[12,13]、Hummingbird-2[14]、KATAN[15]、AES[11]等分组密码进行了分析。此外,代数—立方攻击、迭代立方攻击、中间相遇立方攻击、容错旁路立方攻击等理论也纷纷涌现出来,丰富了立方攻击研究。立方攻击研究路线如图 1 所示,本文将从立方攻击原理及其变种、旁路立方攻击、立方攻击扩展研究几个角度进行介绍,重点分析旁路立方攻击两种泄露模型、物理实验及容错机制研究现状,并指明了立方攻击研究存在的不足及下一步可能的研究方向。

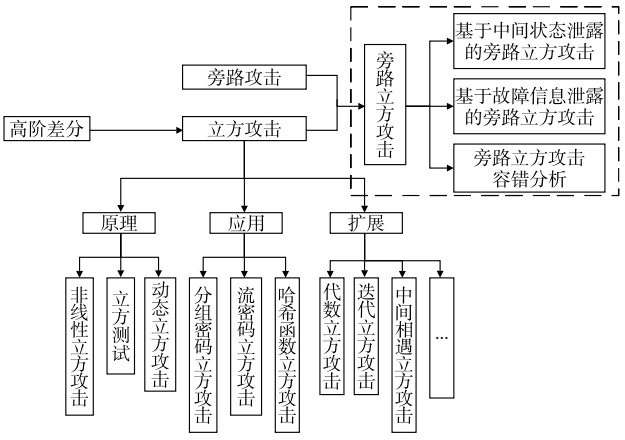

图1 立方攻击研究框架

1 基本原理

从代数角度考虑,算法输出的每一比特都可以表示为关于明文变量 $v_1, v_2, \cdots, v_n$ 以及密钥变量 $k_1, k_2, \cdots, k_l$ 的多项式 $p(v,k)$。假设 I 是明文集合 $\{v_1, v_2, \cdots, v_n\}$ 的子集,I 中变量下标的集合为 $\{i_1, i_2, \cdots, i_m\}$,$t_I = \prod_{i \in \{i_1, i_2, \cdots, i_m\}} v_i$,则在离线阶段随机选取立方体集合 I 可将多项式 $p(v,k)$ 拆分为两部分:

$$p(v,k) = t_I \times p_{S(I)} + q(v,k) \tag{1}$$

如果 $p_{S(I)}$ 最高次为 1,则称 t_I 为极大项,$p_{S(I)}$ 为超级多项式。立方攻击实现的关键在于下列定理的成立:

收稿日期: 2017-07-03; **修回日期**: 2017-08-31 **基金项目**: 国家自然科学基金资助项目(61272491,61309021)

作者简介: 马云飞(1992-),男,吉林德惠人,硕士研究生,主要研究方向为密码学立方攻击(fcz1992@sina.com);王韬(1964-),男,河北石家庄人,教授,博导,博士,主要研究方向为信息安全、密码学;陈浩(1987-),男,湖北武汉人,博士研究生,主要研究方向为对称密码代数故障攻击;黄长阳(1994-),男,黑龙江望奎人,硕士研究生,主要研究方向为密码学代数攻击.

定理 1[7] 如果有集合 $C_I=\{(v_1,v_2,\cdots,v_n)\mid i=i_1,i_2,\cdots,i_m$ 时,$v_i=0,1;i\neq i_1,i_2,\cdots,i_m$ 时,v_i 取值固定$\}$,那么存在 $\sum_{v_1,v_2,\cdots,v_n\in C_I}p(v,k)\equiv p_{S(I)} \bmod 2$。

证明 分两部分考虑多项式 $p(v,k)=t_I\times p_{S(I)}+q(v,k)$。

a)$q(v,k)$。根据多项式定义,$q(v,k)$每一个子项 q_J 中的明文变量乘积 t_J,至少不包含立方体集合 I 中的一项。假设 t_J 中的明文变量比集合 I 少了 r 个,则在 $p(v,k)$ 累加 2^m 次的过程中,有

$$\sum_{2^m}q_J=\sum_{2^r}\left(\sum_{2^{m-r}}q_J\right) \tag{2}$$

其中:$\sum_{2^{m-r}}q_J$ 表示 q_J 中包含的 $m-r$ 个明文变量取遍$\{0,1\}$的累加和,而剩余 r 个明文变量取遍$\{0,1\}$时,由于不影响 q_J 的值,所以 $\sum_{2^{m-r}}q_J$ 可以看做定值,2^r 个相同的值模 2 累加和为 0,所以有 $\sum_{2^m}q_J\equiv 0 \bmod 2$,即 $\sum_{v_1,v_2,\cdots,v_n\in C_I}p(v,k)$ 中 $q(v,k)$ 部分模 2 累加和为 0。

b)$t_I\times p_{S(I)}$。由 $t_I=\prod_{i\in\{i_1,i_2,\cdots,i_m\}}v_i$ 可知,仅当 $v_{i1}=v_{i2}=\cdots=v_{im}=1$ 时,$t_I=1$,否则 $t_I=0$。因此 $\sum_{v_1,v_2,\cdots,v_n\in C_I}p(v,k)$ 中 $t_I\times p_{S(I)}$ 部分为 $p_{S(I)}$。

综合 a)b)可得,$\sum_{v_1,v_2,\cdots,v_n\in C_I}p(v,k)\equiv p_{S(I)} \bmod 2$。

立方攻击具体实施可分为两阶段:

a)预处理。假设攻击者可以完全控制密码设备,能够根据需要设置公开变量和秘密变量。攻击者随机选取立方体,并验证其对应 $p_{S(I)}$ 是否为低次多项式。通过搜索获得大量立方体及其对应多项式,为线上阶段做准备。

b)线上阶段。与线下阶段不同,此时密码设备的秘密变量是固定的且是未知的。利用预处理获得的立方体,攻击者对其进行 0/1 赋值,观察输出目标比特,并进行累加以获取对应的多项式的值,最后求解得到的代数方程组系统获取密钥。

从本质上讲,立方攻击与 AIDA 攻击都是基于高阶差分的,但立方攻击与 AIDA 攻击又有不同[16]。Lai[5] 给出了高阶差分的定义,并推导了一条重要的性质,其被广泛应用于密码分析中。2007 年,Vielhaber[6] 提出 AIDA 攻击(algebraic IV differential attack),对 576 轮的 Trivium 算法,利用 26 个选择明文可恢复 47 bit 密钥。AIDA 与立方攻击异同点总结如表 1 所示。

表 1 AIDA 攻击与立方攻击比较

方法	相同点	不同点
AIDA 攻击	都是基于高阶差分原理,无论是 AIDA 和还是立方攻击累加和,都是目标多项式在一组点上的高阶差分	AIDA 和对应的是某比特密钥变量,而立方累加和对应的是关于密钥变量的多项式
立方攻击	都要求选择明文之外的明文变量取值固定	AIDA 要求除选择明文外的明文变量置 0,而立方攻击仅要求除选择明文外的明文变量取固定值

2 立方攻击变种

2.1 非线性立方攻击

线性立方攻击主要是提取令 $p_{S(I)}$ 最高次数为 1 的极大项 t_I 及其超级多项式,而非线性立方攻击就是对 $P_{S(I)}$ 次数大于 1 的 t_I 进行提取。目前非线性立方攻击主要关注 $P_{S(I)}$ 为 2 次时的 t_I,具体的方法与提取极大项类似。线性测试公式与非线性测试公式如式(3)(4)所示,其中 $a,b,c\in\{0,1\}^l$,l 为密钥比特位数。

$$p_{S(I)}(0)+p_{S(I)}(a)+p_{S(I)}(b)=p_{S(I)}(a+b) \tag{3}$$

$$p_{S(I)}(0)+p_{S(I)}(a)+p_{S(I)}(b)+p_{S(I)}(c)+p_{S(I)}(a+b)+p_{S(I)}(a+c)+p_{S(I)}(b+c)=p_{S(I)}(a+b+c) \tag{4}$$

此外,在非线性攻击中为了确定具体的项以及它们的系数,需要引入一种扩展的立方理论[17]。首先给出扩展立方体的定义,注意下文中将不再区分公开变量及秘密变量,统一用变量$\{x_1,x_2,\cdots,x_u\}$。

定义 1 扩展立方体定义。在立方攻击中,对于任意布尔立方体 $C_I(I\subseteq\{x_1,x_2,\cdots,x_u\})$,如果存在另一个立方体 $C_G(G\subseteq\{x_1,x_2,\cdots,x_u\})$并且 $I\cap G=\varnothing$,则 C_I 与 C_G 可以组成一个扩展的立方体 $C_{I\cup G}$。

例如,$I=\{x_1\}$,$G=\{x_2\}$,则 $C_{I\cup G}=\{(0,0,x_3,\cdots,x_n),(0,1,x_3,\cdots,x_n),(1,0,x_3,\cdots,x_n),(1,1,x_3,\cdots,x_n)\}$。有了扩展立方体的定义后可以将式(1)扩展为式(5)。

$$p(x_1,\cdots,x_u)=t_I\times t_G\times p_{S(I\cup G)}+q(x_1,\cdots,x_u) \tag{5}$$

类似地可证明

$$p_{S(I\cup G)}=\sum_{x_1,x_2,\cdots,x_u\in C_{I\cup G}}p(x_1,x_2,\cdots,x_u) \tag{6}$$

在上述内容的基础上,文献[17]给出两条引理判断哪些密钥变量存在于 $p_{S(I)}$ 中以及这些密钥变量以怎样的组合形式存在于 $p_{S(I)}$ 中。

引理 1 设 $p(x_1,x_2,\cdots,x_u)$是关于 $x_1,x_2,\cdots,x_u$ 的布尔表达式,存在集合 $I\subseteq\{x_1,x_2,\cdots,x_u\}$,$s=|I|$ 为集合 I 中元素个数,t_I 为 I 中元素乘积。令 $p_{S(I)}=\sum_{x_1,x_2,\cdots,x_u\in C_I}p$,则 t_I 以子项或子式的一部分形式存在于 p 中当且仅当至少存在一个向量 $X\in\{0,1\}^{u-s}$使得 $p_{S(I)}(X)=\sum_{x_1,x_2,\cdots,x_u\in C_I}p(X)=1$。

引理 2 多项式 t_K 是 $P_{S(I)}$ 中的一个子项当且仅当令所有的 $x_i=0(x_i\notin I\cup K)$时,有 $p_{S(I\cup K)}=\sum_{x_1,x_2,\cdots,x_u\in C_{I\cup K}}p=1$。

利用引理 1、2 可以判断哪些密钥变量存在于 $p_{S(I)}$ 中以及这些密钥变量以怎样的组合形式存在于 $p_{S(I)}$ 中。

此外,王永娟等人[18] 对非线性立方攻击进行改进,降低了时间复杂度。改进思想如下:依次计算表达式 $p(v,k)$ 中的常数项 d_0,一次项系数 d_i、d_j,并将其存储起来;计算二次项系数 d_{ij}时,利用式(7)可将二次项系数的计算量减少为原来的 1/4。实验结果表明利用该方法,Trivium 和 PRESENT-80 密码立方攻击的时间复杂度均有下降。

$$d_{ij}=d_0\oplus d_i\oplus d_j\oplus\sum_{C_I,k_i=1,k_j=1}p(v,k) \tag{7}$$

2.2 立方测试与动态立方攻击

立方测试(cube testers)[10] 与立方攻击有相似性但又不完全相同。立方测试的目的是区别密码系统的输出与随机函数的输出,而立方攻击的目的是找到尽可能多的线性、非线性表达式以恢复密钥。两者相同点在于:都是通过控制输入向量让立方体取遍 0/1 实现的。以多项式 $f(x_1,\cdots,x_n)=x_1x_2\times p(x_3,\cdots,x_n)+q(x_1,\cdots,x_n)$ 为例,选取随机向量 $(x_3,\cdots,x_n)\in\{0,1\}^{n-3}$,在立方体 x_1x_2 上累加 f,得到

$$\sum_{(x_1,x_2)\in|0,1|^2}f(x_1,\cdots,x_n)=p(x_3,\cdots,x_n) \tag{8}$$

将上述过程重复 N 次,并记录 $p(x_3,\cdots,x_n)$的值。如果 f 是一个随机函数,当 N 取较大值时,至少有一个 $p(x_3,\cdots,x_n)\neq 0$。立方测试研究的多项式性质包括:

a)平衡性。一个随机函数在真值表中 0 和 1 的数量是相等的,计算超级多项式取 0 或取 1 的次数可以作为判断其随机性的依据。

b)常量性。多项式的常量特征分以下几种情况:多项式等于常量 0,多项式等于常量 1,多项式无常量但次数大于 1,多项式有常量且次数大于 1。

c)低次性。如果加密函数的次数较低,相应的 $p_{S(I)}$ 次数也会比较低。低次性是密码系统分析的一个重要性质,除了立方测试,研究者还利用其他方法进行了大量研究[19,20]。

动态立方攻击(dynamic cube attack)[9] 是在立方测试基础上提出的一种优化方法。密码算法输出中的高次项绝大部分是由非线性函数产生的,如果可以简化参与运算的某些中间比特位,则多项式的次数会大大降低,这些中间比特位称为关键比特位。研究者对密码算法进行深入分析后确定这些关键比特位并将其赋值为 0,所用到的特定输入比特称为动态变量。本文对立方攻击、立方测试与动态立方攻击总结如表 2 所示。

表2　立方攻击、立方测试与动态立方攻击比较

方法	目的	理论基础	原理	优点	局限性	相关研究
立方攻击	恢复密钥	高阶差分	通过选择明文赋值,将密码函数转换为低阶函数	将密码算法看做黑盒,无须知道其具体操作	当密码算法次数较高时,给立方体的表示和搜索造成很大困难	Trivium[7]、Hitag2[8]
立方测试	区分密码系统输出与随机函数输出	区分攻击	通过选择明文赋值,探测多项式性质,从而区分加密序列与随机序列	操作简单,无须掌握密码算法细节	为探测多项式性质,需要重复多次对选择明文赋值,数据复杂度较高	MD6[10]
动态立方攻击	恢复密钥	高阶差分	通过简化非线性运算中的某些关键比特,达到降次目的	适用于运算次数较高的密码算法	相比于立方测试,搜索成功率更低	SIMON[21,22]、Grain[9,23,24]

3　旁路立方攻击

旁路立方攻击利用旁路技术恢复密码中间状态比特或获得其他信息,等效于约简轮立方攻击,从而提高了攻击效率。旁路攻击[25]思想最初由 Kocher 提出,并成功利用计时信息破解了 RSA 智能卡密钥。由图 2 可知,攻击者从密码设备能够直接获得的泄露信息包括功耗、单比特值、电磁、故障、时间等,基于此,密码学家提出了功耗攻击[26]、探针攻击[27]、电磁攻击[28]、故障攻击[29]、声音攻击[30]、计时攻击[25]等。而目前与立方攻击结合的旁路泄露模型可分为中间状态泄露和故障信息泄露两种。

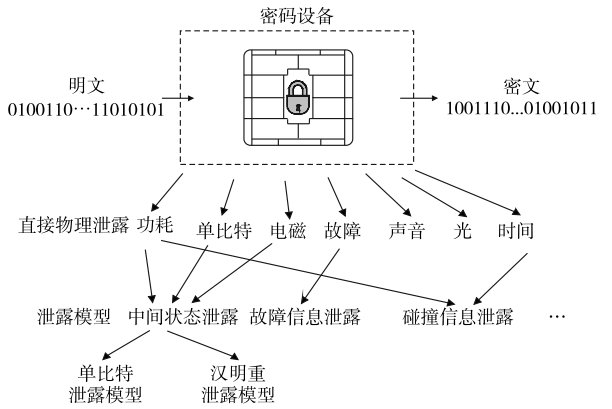

图2　旁路泄露框架

3.1　基于中间状态泄露的旁路立方攻击

利用探针技术、功耗分析、电磁分析获取密码算法中间状态泄露值。目前旁路立方攻击研究大多基于中间状态泄露模型,根据泄露值不同又可分为单比特泄露模型和汉明重泄露模型。

a)单比特泄露模型。通过激光设备和探针精确读取集成电路中的单比特泄露值。尽管这种方法在实践中较难完成且成本高,但该模型已成为旁路立方攻击研究的最典型的模型,文献[12~14]皆是基于单比特泄露模型。

b)汉明重泄露模型。利用模板分析比对密码算法泄露的功耗信息或电磁信息等,得到密码中间状态汉明重泄露值,该方法在实践中使用较多。假设以 Nibble(四位)为单位进行操作,一个 Nibble 值 $Y=(y_0,y_1,y_2,y_3)$,汉明重泄露值 $H=(h_0,h_1,h_2)$,$0\leqslant H\leqslant 4$,则 X 与 Y 的关系可用式(9)表示。

$$\begin{cases} h_0=\prod_{i=0}^{3}y_i \\ h_1=\sum_{t=0}^{5}\varepsilon_t y_i y_j\ (0\leqslant i<j\leqslant 3) \\ h_2=\sum_{i=0}^{3}y_i \end{cases} \tag{9}$$

观察方程组(9)发现 h_0 是三次的,h_1 是二次的,只有 h_2 是一次的。因此根据泄露比特选取的原则,一般选择 4 bit 的累加和(即方程组(9)中的 h_2)作为泄露位。

如图 3 所示,基于中间状态泄露的旁路立方攻击分为四步:

a)泄露位置选取。由于中间状态可选择的泄露位很多,不同泄露位对旁路立方攻击的效率有一定影响。目前对于泄露位选取主要考察如下指标[31]:泄露位覆盖的密钥位数;泄露位多项式项数;泄露位多项式次数。

b)离线搜索阶段。假设攻击者拥有一台相同的密码设备,能够根据需要设置明文与密钥值并观察输出。根据立方攻击原理,随机选取立方体并检验对应多项式是否为低次的。如果是,则将立方体和对应多项式记录下来为在线阶段做准备。

c)在线采集阶段。根据离线阶段得到的立方体,让被攻击设备按照立方体对应的选择明文依次运行,并使用探针、示波器获取单比特、电磁、功耗信息,根据探针分析或模板比对后得出单比特及汉明重泄露值。

d)结合处理阶段。根据离线阶段获得的低次多项式及在线阶段获得的低次多项式对应值列出代数方程组,利用高斯消元等方法进行求解以恢复密钥。

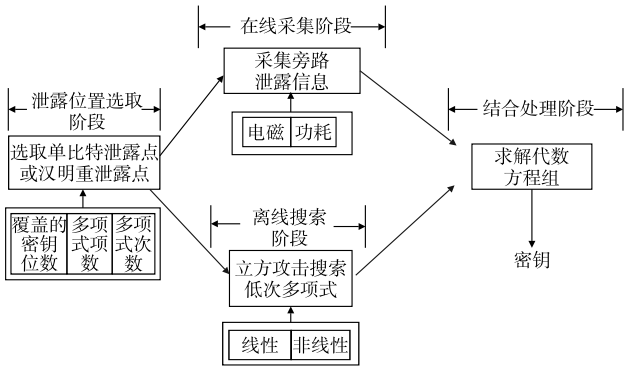

图3　基于中间状态泄露的旁路立方攻击框架

总结现有文献,发现旁路立方攻击对象基本上都是分组密码,而没有流密码或哈希函数密码,原因是现有旁路攻击主要针对分组密码体制。表 3 给出了近年来旁路立方攻击相关研究。

3.2　基于故障信息泄露的旁路立方攻击

故障攻击[29]是一种利用密码实现所依附的物理设备平台在外界强电流、高电压、强辐射等手段干扰下可能出现的寄存器故障或运算错误来恢复密钥的攻击方法。基于故障信息泄露的旁路立方攻击,通过故障将故障注入点到最末轮加密过程截取出来分析,有效降低了输出比特多项式的项数和次数,等效于约简轮立方攻击。

a)分组密码故障立方攻击[38]。结合立方与故障,以每一轮的中间状态比特作为 t_I,以输出比特作为目标多项式 p,统计每一轮线性及非线性多项式数量,作为选择泄露轮的依据;其次,以每一位输出比特 z_j 的差分 Δz_j 作为多项式累加和,考察每一位 Δz_j 对应的多项式类型(常量 0,1 或一个特定多项式)作为判定泄露位依据;最后利用立方攻击提取线性及非线性多项式,结合在线阶段获得的密文可恢复部分轮密钥值。

b)流密码 fault cube 攻击[39]。如果说分组密码故障立方攻击是利用立方对故障攻击进行改进,则流密码 fault-cube 攻击就是利用故障注入对立方攻击进行改进。以初始化第 u 拍为界将整个加密过程分为两部分(图 4[39]),在第 u 拍内部状态 $S_u=\{S_{1,u},S_{2,u},\cdots,S_{l,u}\}$ 中选择合适的故障注入点。Fault-cube 攻击分为两阶段,预处理阶段将输出比特 z 看做中间比特 $S_{1,u},S_{2,u},\cdots,S_{l,u}$ 的函数,寻找关于中间比特的 1 维 Cube;将 1 维 Cube 对应的超级多项式 $P_{S(I)}(S_{1,u},S_{2,u},\cdots,S_{l,u})$ 看做密钥和初始向量的函数,并寻找关于密钥 $k_1,k_2,\cdots,k_n$ 的线性多项式。最后联立两部分超级多项式,消去 $S_{1,u},S_{2,u},\cdots,S_{l,u}$。

表3 基于中间状态泄露的旁路立方攻击研究

文献	密码	研究内容	攻击轮数	选择明文数量	攻击后密钥搜索空间变化	研究成果提出时间
[12]	PRESENT	对第三轮的比特位进行归类,选取有代表性的泄露位进行旁路立方攻击;此外,对旁路立方攻击的泄露轮和泄露位选取方法均进行了说明	3	$2^{15.00}$	$2^{80}\rightarrow 2^{32}$	2009 年
[17]	PRESENT-80	提出非线性立方攻击方法,并在此基础上利用汉明重泄露模型对 1 轮后的 PRESENT-80 和 PRESENT-128 进行旁路立方攻击	1	$2^{13.00}$	$2^{80}\rightarrow 2^{16}$	2011 年
[17]	PRESENT-128		1	$2^{13.00}$	$2^{128}\rightarrow 2^{64}$	2011 年
[13]	PRESENT-80	在文献[12,18]基础上,应用线性、非线性、分而治之、迭代分析方法进一步降低了 PRESENT-80/128 的密钥搜索空间,是目前 PRESENT-80 和 PRESENT-128 旁路立方攻击最优结果	3	$2^{8.95}$	$2^{80}\rightarrow 2^{8}$	2013 年
[13]	PRESENT-128		4	$2^{9.78}$	$2^{128}\rightarrow 2^{7}$	2013 年
[32]	NOEKEON	对 NOEKEON 算法抗旁路立方攻击能力进行评估,从中间比特覆盖的密钥数量和中间比特次数两个方面确定最佳泄露轮,并给出了判定某个密钥是否被该比特位覆盖的方法。选取第 2 轮第 1 bit 作为泄露位,通过旁路立方攻击将恢复全部密钥时间复杂度下降为 $O(2^{68})$	2	$2^{10.27}$	$2^{128}\rightarrow 2^{68}$	2010 年
[33]	EPCBC(48,96)	提取立方大小最大为 5 的立方体,372 和 610 个选择明文可分别恢复 EPCBC(48,96)的 48 bit 密钥和 EPCBC(96,96)的 96 bit 主密钥,证明 EPCBC 易遭受黑盒旁路立方攻击	3	$2^{8.54}$	$2^{96}\rightarrow 2^{48}$	2012 年
[33]	EPCBC(96,96)		3	$2^{9.25}$	$2^{96}\rightarrow 2^{0}$	2012 年
[14]	Hummingbird-2	利用一种逐项二次检测方法,在 GPU 帮助下,以 Hummingbird-2 第 3 轮汉明重量最低位作为泄露位进行旁路立方攻击,最终将时间复杂度由 2^{128} 下降到 2^{80}	3	$2^{18.00}$	$2^{128}\rightarrow 2^{80}$	2012 年
[34]	MIBS	对 MIBS 安全性进行评估,基于单比特泄露模型进行旁路立方攻击,结果表明:选择第 1 轮第 5 bit 作为泄露位,利用 $2^{6.39}$ 个选择明文可将 MIBS 搜索空间下降为 2^{40}	1	$2^{6.39}$	$2^{64}\rightarrow 2^{40}$	2013 年
[35]	LBlock	对 LBlock 进行安全性评估,针对 LBlock 第 8 轮进行旁路立方攻击,共搜索得到 25 个立方体,结合密钥穷举总时间复杂度为 $O(2^{55.00})$	8	$2^{10.75}$	$2^{80}\rightarrow 2^{55}$	2013 年
[36]	LBlock	针对 LBlock 第 3 轮进行旁路立方攻击,发现该轮搜索得到的立方体数量更多,利用分而治之思想能够恢复 70 bit 密钥,优于文献[37]结果	3	$2^{11.10}$	$2^{80}\rightarrow 2^{10}$	2013 年

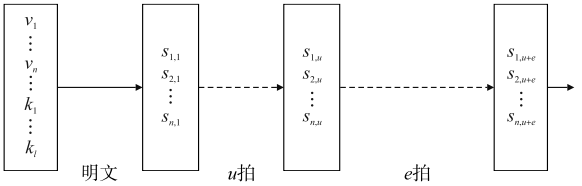

图4 fault cube攻击模型

3.3 旁路立方攻击容错分析

1)DS 模型与修正的 DS 模型 在立方攻击提出时,Dinur 等人[7]已经考虑到了实际攻击中可能存在错误的情况,并给出了一种基于 d-随机多项式的容错处理模型,在该多项式中包含 $d-1$ 个明文变量的子项很可能是极大项。假定泄露比特多项式是 d-随机多项式,文献[7]指出"为得到 n 个不同的极大项,需要大小为 $d+\log_d^n$ 的明文集合,因为$\binom{d+\log_d^n}{d}\approx d^{\log_d^n}=n$"。取大小为 k 的明文集合,其中 $k\geqslant d+\log_d^n$。设在实际攻击中,旁路泄露值的错误率为 ω,将出错的泄露值看成新变量。为了保证代数方程组有解可得

$$\binom{k}{d-1}\geqslant\omega\times 2^k+n \tag{10}$$

但在实际旁路立方攻击中,泄露位的代数方程并不一定满足 d-随机多项式要求,搜索到的立方体数量远小于$\binom{k}{d-1}$,且立方大小有很多种,并不是固定值 d。鉴于此,文献[36]给出了一种修正的 Dinur-Shamir 模型。假设在旁路立方攻击中,攻击者共搜索到 L 个立方体,其立方大小有 r 种,立方大小 η_i 的立方体数量为 δ_i,则攻击所需的所有泄露值个数为 $N^*=\sum_{i=1}^{r}\delta_i\times 2^{\eta_i}$。为保证代数方程组有解,需有下式成立:

$$L\times(1-\theta)\geqslant\omega\times N^*+n \tag{11}$$

2)线性分组码容错分析模型 2013 年,Li 等人[40]将包含错误信息的方程组求解问题转换为一组线性分组码解码(图5)问题,并对 PRESENT 第 1、2 轮的旁路立方攻击容错能力进行分析。容错旁路立方攻击问题即为根据超级多项式系数矩阵和泄露值序列求密钥的过程。如果将旁路立方攻击中系数矩阵作为生成矩阵,密钥看做消息序列,而泄露值序列看做接收到的码字,则求解密钥的过程可以看做数域 GF(2)上的线性分组码解码问题。文献[41]在此基础上,利用多项式近似和立方攻击变种方法降低了码率,进而提高了旁路立方攻击容错率。

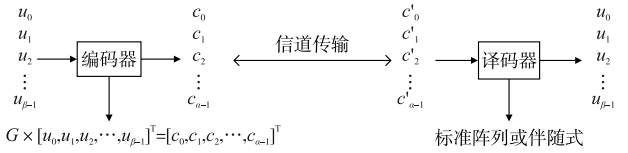

图5 线性分组码编码与解码过程

4 立方攻击扩展研究

4.1 立方攻击与代数攻击结合

Courtois 等人[42]给出了代数攻击的一般模型,并提出利用两个多项式相乘达到降次目的。文献[43]在此基础上提出一种快速代数攻击方法,并将其应用到 Toyocrypt、LILI-128 和 E0,改进了时间和空间复杂度。文献[44]将代数攻击方法与立方攻击结合,假设对于目标多项式 $z=f(x,v)$,可以找到 $g(x,v)$,使得 $h(x,v)=f(x,v)g(x,v)$ 的次数 $\deg(h)<\deg(f)$,则根据式(12)可将立方攻击转换为对 $h(x,v)$ 的攻击。

$$\sum_{v\in C}h(x,v)=\sum_{v\in C}f(x,v)g(x,v) \tag{12}$$

这种方法能够解决标准立方攻击搜索效率受多项式次数限制的问题,但其能搜索到的立方体数量会减少。文献[45]将代数立方攻击的方法应用到 LiLi-128 中,通过 3 维的 cube 集合恢复 LFSR 中的 88 位密钥,攻击复杂度下降为 2^{15}。

4.2 迭代立方攻击

迭代立方攻击[31]的基本思想是:利用已恢复的密钥化简目标多项式,从而达到降次目的。假设第一次立方攻击的目标多项式为 $f(P,K^1,K^2,\cdots,K^n)$,当第一轮 K^1 恢复出来之后,将明文 P 和 K^1 代入第一轮加密得到 S^1,再以 S^1 作为选择明文,$f(S^1,K^2,\cdots,K^n)$ 为目标多项式,利用立方攻击获取 K^2 的值,依此类推,直到获得所有扩展密钥值。经过迭代,目标多项式的规模将大大降低,可以在有限的时间内进行立方攻击。文献[46]利用迭代立方攻击思想,对 KATAN32 进行 4 次迭代立方攻击,恢复了 78 位密钥,剩下两位密钥通过暴力搜索获得,总计算复杂度为 $2^{16.38}$,优于传统的立方攻击[47]。文献[13]在文

献[17]的基础上,应用线性、非线性、分而治之、迭代分析方法,进一步将 PRESENT-80 和 PRESENT-128 的密钥搜索空间下降到 2^8 和 2^{29}。

4.3　中间相遇立方攻击

中间相遇立方攻击的思想是:通过猜测部分密钥,将观察到的密文输出逆推若干轮,与该轮立方攻击结合起来恢复密钥。Szmidt[48]对 4 轮 CTC 密码进行立方攻击,恢复全部 120 bit 密钥,之后利用中间相遇方法将攻击轮数扩展至 5 轮。李俊志等人[49]对 96 轮 KeeLoq 进行中间相遇立方攻击,先枚举部分密钥,得到 64 轮密码输出,再利用之前得到的 15 bit 密钥信息对其余密钥进行枚举,恢复全部密钥。

5　存在问题与研究展望

本文总结了自 2008 年以来的立方攻击研究进展,总体来说,2008—2013 年立方攻击发展速度最快。无论是单独的立方攻击还是立方攻击变种、立方攻击与旁路攻击的结合都取得了一定成果,但是对于立方攻击研究仍存在一些不足之处:

a)单独的立方攻击主要针对流密码,而在分组密码和哈希函数中的研究较少。立方攻击在分组密码中的实践较少,因为分组密码多项式次数和项数随轮数增加呈几何增长,对分组密码进行单独的立方攻击效果并不理想。通过比较流密码和分组密码立方攻击,发现流密码更易遭受立方攻击。由于密钥流的产生是通过一些线性或低次的函数来实现,这些线性和低次的部件使得流密码成为立方攻击的天然目标[50]。此外,立方攻击在哈希函数中的研究不足,与其复杂的结构和加密过程有关。关于分组密码和哈希函数的立方攻击研究仅有 KATAN[15]、CTC[37]、PHOTON[51]、SHA-3[52],而对于流密码的立方攻击研究总结如表 4 所示。

表 4　流密码立方攻击

流密码	攻击轮数	选择明文	密钥搜索空间	文献
Trivium	672	$2^{19.00}$	$2^{80}\rightarrow 2^{17}$	[7]
	735	$2^{30.00}$	$2^{80}\rightarrow 2^{27}$	[7]
	767	$2^{45.00}$	$2^{80}\rightarrow 2^{45}$	[7]
	784	$2^{39.00}$	$2^{80}\rightarrow 2^{38}$	[53]
	799	$2^{40.00}$	$2^{80}\rightarrow 2^{62}$	[53]
A5/1	576	$2^{12.63}$	$2^{80}\rightarrow 2^{11}$	[54]
	5	$2^{11.32}$	$2^{64}\rightarrow 2^{44}$	[54]
Grain v1	70	—	$2^{80}\rightarrow 2^{65}$	[55]

b)旁路立方攻击大多是基于中间状态泄露的,而基于故障信息泄露的研究较少,且已有旁路立方攻击大多建立在一种理想模型基础上,并未考虑实际中受噪声等因素影响可能出现的泄露值观测错误的情况。基于故障信息泄露的旁路立方攻击又可称为故障立方攻击或 fault-cube 攻击,目前研究文献仅有曾文[39]以初始化第 u 拍为界将整个加密过程分为两部分,该方法对 1 056 拍以下的 Trivium 算法有效,计算复杂度不超过 2^{53};Abdul-Latip 等人[38]结合立方原理,确定 KATAN 密码泄露轮以及故障注入比特,并根据线下阶段获得的多项式恢复部分密钥,通过 115 次故障注入,可将 KATAN32 密钥搜索空间降低为 2^{59}。并且在目前旁路立方攻击中,无论是单比特还是汉明重泄露模型,都假设攻击者能够获得完全正确的泄露值,代入离线阶段获得的低次多项式方程组中求得密钥,这在实际攻击中很难做到。关于旁路立方攻击容错仅有中国科学院的李振奇等人开展的研究,还有待于进一步探索。

c)旁路立方攻击物理实验研究亟待开展。关于物理实验的相关研究,仅有 Zhao 等人[56]利用一个 8 bit 的微处理器运行 PRESENT-80 密码算法,并使用示波器等设备收集功耗曲线;得到汉明重泄露值后,结合预处理阶段立方攻击提取的多项式恢复密钥。此外,该文献还对有时延防护及掩码防护的设备进行了实验。受实验设备等因素限制,目前旁路立方攻击研究主要停留在理论阶段,不足以证明该方法在实际攻击中的可行性。建议今后的研究多从实际出发,针对特定密码芯片验证旁路立方攻击有效性,且将密码芯片可能采取的防护措施考虑在内。

尽管近年来立方攻击研究热度有所下降,但作为一种经典的代数分析方法,立方攻击仍可从以下方面进一步探索:

a)三次及以上多项式的提取与利用。目前对超级多项式(一次)、二次多项式提取的研究已较为成熟,但如果想要恢复更多密钥,可以考虑三次及以上多项式提取方法。同时,对于较高次多项式的密钥求解,可以考虑利用代数攻击中经常使用的基于 SAT[57]的方法(借助 MiniSat、CryptoMiniSat 等解析器)、基于线性化的方法(直接线性化 XL、扩展线性化 XSL)以及基于 Gröbner 基[58]的方法。

b)对哈希函数的立方攻击研究。随着物联网技术迅猛发展,许多用于轻量级设备的轻量级密码算法纷纷出现。一些新型哈希函数采用分组密码部件进行设计(如 Streebog),多项式次数较低,便于进行代数攻击。此外,针对约简轮哈希函数密码的立方攻击研究也有待加强。

c)旁路立方攻击研究仍有很大研究空间。已有旁路立方攻击主要是基于中间状态泄露和基于故障信息泄露。除了两种泄露模型,还可考虑碰撞泄露、光泄露等其他模型与立方攻击的结合;对于故障信息泄露的旁路立方攻击研究不足,相关理论不够成熟,应用也较少,有待于进一步探索;物理实验由于实现较为困难,仅有一篇文献进行了物理实验,且针对密码设备防护措施的相关研究少;容错分析研究不足,可以考虑其他容错模型,如文献[59]将包含错误的代数方程组求解转换为布尔最优化问题,利用最优化问题解析器进行破解。

6　结束语

自 2008 年立方攻击提出以来,由于该方法具有可在不知道密码算法细节情况下进行攻击等优点,受到了学者广泛关注。通过梳理 2008 年以来的文献,本文从立方攻击原理、立方攻击变种、旁路立方攻击、立方攻击拓展等角度介绍了目前国内外关于立方攻击的主要研究成果,并在此基础上分析了已有研究存在的不足,以及未来可以进行深入研究的方向,以期对立方攻击的进一步研究提供一定的借鉴。

参考文献:

[1] Biham E, Shamir A. Differential cryptanalysis of the data encryption standard [M]. New York:Springer-Verlag,1993: 2-21.

[2] Biham E, Biryukov A, Shamir A. Miss in the middle attacks on IDEA and Khufu [C]//Proc of International Conference on Fast Software Encryption. Berlin:Springer,1999: 124-138.

[3] Matsui M. Linear cryptanalysis method for DES cipher [C]//Advances in Cryptology: EUROCRYPT. Berlin: Springer, 1994: 386-397.

[4] Courtois N T, Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations [C]//Advances in Cryptology: ASIACRYPT. Berlin:Springer,2002:267-287.

[5] Lai Xuejia. Higher order derivatives and differential cryptanalysis [C]//Communications and Cryptography. Boston: Springer, 1994: 227-233.

[6] Vielhaber M. Breaking On: Fivium by AIDA an algebraic IV differential attack[EB/OL]. (2007-10-28)[2017-08-30]. http://eprint.iacr.org/2007/413.pdf.

[7] Dinur I, Shamir A. Cube attacks on Tweakable black box polynomials [EB/OL]. [2017-08-30]. http://eprint.iacr.org/2008/385.pdf.

[8] Sun Siwei, Hu Lei, Xie Yonghong, *et al*. Cube cryptanalysis of Hitag2 stream cipher[C]//Proc of the 10th International Conference on Cryptology and Network Security. Berlin:Springer-Verlag,2011:15-25.

[9] Dinur I, Shamir A. Breaking Grain-128 with dynamic cube attacks [C]//Proc of International Conference on Fast Software Encryption. Berlin:Springer,2011: 167-187.

[10] Aumasson J P,Dinur I, Meier W, *et al*. Cube testers and key recovery attacks on reduced-round MD6 and Trivium[C]//Proc of International Conference on Fast Software Encryption. Berlin: Springer, 2009:1-22.

[11] Dinur I, Shamir A. Side channel cube attacks on block ciphers[EB/OL]. (2009-03-18)[2017-08-30]. http://eprint.iacr.org/2009/127.pdf.

[12] Yang Lin, Wang Meiqin, Qiao Siyuan. Side channel cube attack on

PRESENT[C]//Proc of International Conference on Cryptology and Network Security. Berlin:Springer,2009:379-391.
[13] Zhao Xinjie, Guo Shize, Zhang Fan, *et al*. Enhanced side-channel cube attacks on PRESENT [J]. IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences,2013,96(1):332-339.
[14] Fan Xinxin, Gong Guang. On the security of Hummingbird-2 against side channel cube attacks [C]//Proc of Western European Workshop on Research in Cryptology. Berlin:Springer,2012:18-29.
[15] Bard G V, Courtois N T, Nakahara J, *et al*. Algebraic, AIDA//cube and side channel analysis of KATAN family of block ciphers[C]// Proc of the 11th International Conference on Cryptology in India. Berlin:Springer,2010:176-196.
[16] 孙宇,王永娟. Cube 攻击原理与改进[J]. 计算机科学,2012,39(Z6):77-80.
[17] Abdul-Latip S F, Reyhanitabar M R, Susilo W, *et al*. Extended cubes: enhancing the cube attack by extracting low-degree non-linear equations[C]//Proc of the 6th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2011:296-305.
[18] 王永娟,丁立人,任泉宇,等. 二次检测立方攻击改进与实现[J]. 国防科技大学学报,2015,37(2):106-111.
[19] Alon N, Kaufman T, Krivelevich M, *et al*. Testing low-degree polynomials over *GF*(2)[C]//Approxiumation, Randomization and Combinatorial Optimization, Algorithms and Techniques. Berlin:Springer, 2003:188-199.
[20] Samorodnitsky A. Low-degree tests at large distances[C]//Proc of the 39th Annual ACM Symposium on Theory of Computing. New York:ACM Press,2007:506-515.
[21] Rabbaninejad R, Ahmadian Z, Salmasizadeh M, *et al*. Cube and dynamic cube attacks on SIMON32/64[C]//Proc of the 11th International ISC Conference on Information Security and Cryptology. Piscataway,NJ: IEEE Press,2014:98-103.
[22] Ahmadian Z, Rasoolzadeh S, Salmasizadeh M, *et al*. Automated Dynamic cube attack on block ciphers: cryptanalysis of SIMON and KATAN[EB/OL]. (2015-01-16)[2017-08-30]. http://eprint. iacr. org/2015/040. pdf.
[23] Banik S. Dynamic cube attack on 105 round Grain v1 [EB/OL]. (2014-08-22)[2017-08-30]. http://eprint. iacr. org/2014/652. pdf.
[24] Rahimi M, Barmshory M, Mansouri M H, *et al*. Dynamic cube attack on Grain-v1[J]. IET Information Security,2016,10(4):165-172.
[25] Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]//Proc of Annual International Cryptology Conference. Berlin:Springer,1996:104-113.
[26] Kocher P, Jaffe J, Jun B. Differential power analysis[C]//Proc of Annual International Cryptology Conference. Berlin: Springer, 1999: 388-397.
[27] Handschuh H, Paillier P, Stern J. Probing attacks on tamper-resistant devices[C]//Proc of Internatioanl Conference on Cryptographic Hardware and Embedded Systems. Berlin:Springer,1999:303-315.
[28] Quisquater J J, Samyde D. A new tool for non-intrusive analysis of smart cards based on electro-magnetic emissions: the SEMA and DEMA methods[C]//Proc of Eurocrypt Rump Session. 2000.
[29] Boneh D , Demillo R A, Liprion R J. On the importance of checking cryptographic protocols for faults[C]//Advances in Cryptology: EUROCRYPT. Berlin:Spinger,1997:37-51.
[30] Shamir A, Tromer E. Acoustic cryptanalysis: on nosy people and noisy machines[EB/OL]. (2004-05-11)[2009-03-05]. http://www. wisdom. weizmann. ac. il/~tromer/acoustic/.
[31] 郭世泽,王韬,赵新杰. 密码旁路分析原理与方法[M]. 北京:科学出版社,2014.
[32] Abdul-Latip S F, Reyhanitabar M R, Susilo W, *et al*. On the security of NOEKEON against side channel cube attacks[C]//Proc of the 6th International Conference on Information Security, Practice and Experience. Berlin:Springer,2010:45-55.
[33] 赵新杰,郭世泽,王韬,等. EPCBC 密码旁路立方体攻击[J]. 成都信息工程学院学报,2012,27(6):525-530.
[34] 刘会英,王韬,郭世泽,等. MIBS 密码旁路立方体攻击[J]. 计算机仿真,2013,30(5):302-305.
[35] Islam S, Afzal M, Rashdi A. On the security of LBlock against the cube attack and side channel cube attack[C]//Proc of International Conference on Availability, Relin Bility and Security. Berlin:Springer, 2013:105-121.
[36] Li Zhenqi, Zhang Bin, Yao Yuan, *et al*. Cube cryptanalysis of LBlock with noisy leakage[C]//Proc of the 15th International Conference on Information Security and Cryptology. Berlin: Springer, 2012: 141-155.
[37] 穆道光,张文政. 分组密码算法 CTC 的立方分析[J]. 信息安全与通信保密,2012(7):132-135.
[38] Abdul-Latip S F, Reyhanitabar M R, Susilo W, *et al*. Fault analysis of the KATAN family of block ciphers[C]//Proc of the 8th International Conference on Information Security Practice and Experience. Berlin:Springer,2012:319-336.
[39] 曾文. Trivium 算法的 fault cube 攻击与可滑动对研究[D]. 郑州:信息工程大学,2011.
[40] Li Zhenqi, Zhang Bin, Fan Junfeng, *et al*. A new model for error-tole-rant side-channel cube attacks[C]//Proc of the 15th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin:Springer,2013:453-470.
[41] Li Zhenqi, Zhang Bin, Roy A, *et al*. Error-tolerant side-channel cube attack revisited[C]//Proc of Conference on Selected Areas in Cryptography. Cham:Springer,2014:261-277.
[42] Courtois N T, Meier W. Algebraic attacks on stream ciphers with linear feedback[C]//Proc of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin:Spinger,2003: 345-359.
[43] Courtois N T. Fast algebraic attacks on stream ciphers with linear feedback[C]//Proc of the 23rd Annual International Cryptology Conference. Berlin:Springer,2003:176-194.
[44] Zhang A, Lim C W, Khoo K, *et al*. Extensions of the cube attack based on low degree annihilators[C]//Proc of the 8th International Conference on Cryptology and Network Security. Berlin: Springer, 2009:87-102.
[45] 丁立人,王永娟. 对序列密码算法的改进 cube 攻击[J]. 计算机工程与应用,2015,51(21):111-115.
[46] 穆道光,张文政. 迭代立方攻击及其应用[J]. 计算机工程与应用,2014,50(19):99-102.
[47] Mroczkowski P, Szmidt J. The algebraic cryptanalysis of the block cipher KATAN32 using modified cube attack[D]. Warsaw: Military University of Technology,2011:345-354.
[48] Szmidt J. The cube attack on courtois toy cipher[C]//Proc of International Conference on Number-Theoretic Methods in Cryptology. Cham:Springer,2017:241-253.
[49] 李俊志,李文,李伟,等. 对简化版 KeeLoq 算法的中间相遇—立方攻击[J]. 上海交通大学学报,2015,49(10):1540-1544.
[50] Dinur I, Shamir A. Applying cube attacks to stream ciphers in realistic scenarios[J]. Cryptography and Communications,2012,4(3-4):217-232.
[51] Lu Chiayu, Lin Youwei, Jen Shangming, *et al*. Cryptanalysis on PHOTON hash function using cube attack[C]//Proc of International Conference on Information Security and Intelligent Control. Washington DC:IEEE Computer Society,2012:278-281.
[52] Dinur I, Morawiecki P, Pieprszyk J, *et al*. Cube attacks and cube-attack-like cryptanalysis on the round-reduced Keccak sponge function [C]//Proc of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin:Springer,2015:733-761.
[53] Fouque P A, Vannet T. Improving key recovery to 784 and 799 rounds of trivium using optimized cube attacks[C]//Proc of the 20th International Workshop on Fast Software Encryption. Berlin:Spirnger, 2013:502-517.
[54] Islam S, Haq I U. Cube attack on trivium and A5/1 stream ciphers [C]//Proc of the 13th International Conference on Applied Sciences and Technology. Piscataway,NJ:IEEE Press,2016:409-415.
[55] 宋海欣,范修斌,武传坤,等. 流密码算法 Grain 的立方攻击[J]. 软件学报,2012,23(1):171-176.
[56] Zhao Xinjie, Guo Shize, Zhang Fan, *et al*. Efficient hamming weight based side-channel cube attacks on PRESENT [J]. Journal of Systems & Software,2012,86(3):728-743.
[57] Soos M, Mohl K, Castelluccia C. Extending SAT solvers to cryptographic problems[C]//Proc of the 12th International Conference on Theory and Applications of Satisfiability Testing. Berlin: Springer, 2009:244-257.
[58] Faugere J C. Gröbner bases[EB/OL]. (2007)[2017-08-30]. http://fse2007. uni. lu/slides/faugere. pdf.
[59] Oren Y, Kirschbaum M, Popp T, *et al*. Algebraic side-channel analysis in the presence of errors [C]//Proc of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2010:428-442.