doi:10.3969/j.issn.1000-436X.2012.10.019

立方攻击成功率分析

宋海欣[1,2]，范修斌[1]，武传坤[1]，冯登国[1]
（1．中国科学院 软件研究所信息安全国家重点实验室，北京 100190；2．中国科学院 研究生院，北京 100049）

摘 要：在一般随机布尔函数及布尔函数的代数次数或代数标准型项数受限情况下，从理论上分析了立方攻击的成功概率，对立方攻击密码分析方法提供了理论支持。理论结果与对流密码算法 Trivium 及 Grain v1 的实验结果是相吻合的。

关键词：立方攻击；成功概率；密钥恢复；Grain v1；布尔函数
中图分类号：TP309 **文献标识码**：B **文章编号**：1000-436X(2012)10-0143-06

Analysis of the success probability of cube attack

SONG Hai-xin[1,2], FAN Xiu-bin[1], WU Chuan-kun[1], FENG Deng-guo[1]
（1. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;
2. Graduate University of Chinese Academy of Sciences, Beijing 100049, China）

Abstract: The success probability of cube attack was theoretically discussed when a boolean function was chosen at random and the algebraic degree or the number of terms in its algebraic normal form representation was restricted. The results provided theoretic support to cube attack. The theoretical results meet with the experimental results of the analysis of the stream ciphers Trivium and Grain v1 very closely.

Key words: cube attack; success probability; key recovery; Grain v1; boolean function

1 引言

在 2009 年欧洲密码年会上，Dinur 和 Shamir 提出了立方攻击（cube attack）[1]的密码分析方法并对流密码算法 Trivium[2]进行了分析，立方攻击是一种新型的代数攻击方法，旨在寻找密码算法固有的低次方程以恢复密钥[3~7]或进行区分攻击[8~10]。

一般来讲，密码算法模型如图 1 所示。对分组密码来讲，密码算法可看作 *m*bit 明文与 *n*bit 密钥的函数，经过轮函数的迭代过程，产生密文。对流密码来讲，密码算法可看作 *m*bit 初始向量 *IV* 与 *n*bit 密钥的函数，流密码算法设计一般分为初始化过程和密钥流产生过程，很多流密码算法，如 Trivium[2]、Grain v1[11]、Mickey[12]、F-FCSR-H[13]等，其初始化过程均采用低次函数迭代一定拍数，使密钥和初始向量达到一定程度的混乱与扩散。无论是流密码算法还是分组密码算法，一般开始随着迭代拍数的增加，密码算法的代数次数和代数标准型(ANF)项数会戏剧性地增加，迭代一定拍数后，密码算法的代数次数和代数标准型项数会达到一个相对稳定且不可预测的状态。

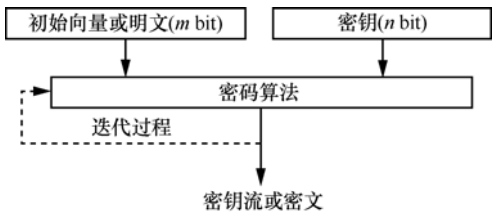


图 1 密码算法模型

收稿日期：2011-11-24；**修回日期**：2012-05-31
基金项目：国家自然科学基金资助项目（60833008，60902024）
Foundation Item: The National Natural Science Foundation of China (60833008, 60902024)

本文就一般随机布尔函数及布尔函数的代数次数或代数标准型项数受限情况下，从理论上分析了立方攻击的成功概率，设 $f(v_1,v_2,\cdots,v_m,k_1,k_2,\cdots,k_n)$ 为 m 个公开变量 $(v_1,v_2,\cdots,v_m)$ 及 n 个密钥变量 $(k_1,k_2,\cdots,k_n)$ 的布尔函数，证明了以下结论：1）针对一般随机布尔函数进行讨论，立方攻击的成功概率为 $2^{-\left(2^n-n-1\right)}$；2）针对布尔函数的代数次数进行讨论，设随机布尔函数的代数次数至多为 s，若代数次数 s 与极大项 (maxterm) [1]的代数次数 l 满足关系 $s-l=1$ 时，立方攻击的成功概率为 1；当 $s-l>1$ 时，成功概率为 $2^{-\left(\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{s-l}\right)}$；3）针对布尔函数的代数标准型项数进行讨论，若随机布尔函数可被极大项整除的代数标准型中，代数次数大于等于 $(l+2)$ 的代数标准型至多为 N 项，那么立方攻击的成功概率为 2^{-N}。

2 立方攻击简介

立方攻击是一种新型的代数攻击方法，在选择 IV 或选择明文条件下，寻找关于密钥的仿射函数以恢复密钥或进行区分攻击，它吸收了饱和攻击[14]及高阶差分分析[15]的思想，该攻击方法主要基于下述定理。

定理 1[1] 设 $f(x_1,x_2,\cdots,x_n)$ 为含有 n 个变量的布尔函数，$S=\{x_1,x_2,\cdots,x_n\}$，$f(\cdot)$ 函数可表示为 $f(x_1,x_2,\cdots,x_n)=T(I)P\left(x_j\middle|x_j\in S\setminus I\right)\oplus R\left(x_j\middle|x_j\in S\right)$，其中，$I$ 为集合 S 的非空真子集，设 $I=\{x_{i_1},x_{i_2},\cdots,x_{i_d}\}$，$\left(1\leqslant i_1,i_2,\cdots,i_d\leqslant n,1\leqslant d\leqslant n-1\right)$，$T(I)=\left(\prod_{x_i\in I}x_i\right)$，$P(\cdot)$ 和 $R(\cdot)$ 均为代数标准型表示的布尔函数，$P(\cdot)$ 函数中的变量均取自集合 I 对 S 的余集 $S\setminus I$，$R(\cdot)$ 函数代数标准型中的每一项均不含 I 中的全部变量，那么，当对集合 I 中的变量跑遍所有可能取值并对 $f(\cdot)$ 函数求和，可得：$\sum_{\left(x_{i_1},x_{i_2},\cdots,x_{i_d}\right)\in F_2^d}f\left(x_1,x_2,\cdots,x_n\right)=P(\cdot)$。

为了进一步说明该定理，举例如下：

设 $f\left(v_1,v_2,v_3,k_1,k_2,k_3\right)=v_1v_2k_2\oplus v_1v_2k_3\oplus v_1v_2v_3\oplus k_1k_2k_3\oplus v_1v_2\oplus v_2k_2\oplus k_3\oplus 1$，

其可以表示为

$f\left(v_1,v_2,v_3,k_1,k_2,k_3\right)=v_1v_2\left(k_2\oplus k_3\oplus v_3\oplus 1\right)\oplus\left(k_1k_2k_3\oplus v_2k_2\oplus k_3\oplus 1\right)$

这里，$S=\{v_1,v_2,v_3,k_1,k_2,k_3\}$，$I=\{v_1,v_2\}$，$T(I)=v_1v_2$，$P(\cdot)=k_2\oplus k_3\oplus v_3\oplus 1$，$R(\cdot)=k_1k_2k_3\oplus v_2k_2\oplus k_3\oplus 1$。

$$\begin{aligned}&\sum_{(v_1,v_2)\in F_2^2}f\left(v_1,v_2,v_3,k_1,k_2,k_3\right)\\&=f\left(0,0,v_3,k_1,k_2,k_3\right)\oplus f\left(0,1,v_3,k_1,k_2,k_3\right)\oplus\\&\quad f\left(1,0,v_3,k_1,k_2,k_3\right)\oplus f\left(1,1,v_3,k_1,k_2,k_3\right)\\&=k_2\oplus k_3\oplus v_3\oplus 1\\&=P(\cdot)\end{aligned}$$

流密码算法中，在选择 IV 攻击条件下，初始向量 IV 为公开变量，密钥为未知变量。分组密码算法中，在选择明文攻击条件下，明文为公开变量，密钥为未知变量。

定义 1[1] 定理 1 中，若集合 I 中的变量均为公开变量，并且 $P(\cdot)$ 的代数次数为 1，就得到了关于未知变量的一个仿射方程 $P(\cdot)=\sum_{(x_{i_1},x_{i_2},\cdots,x_{i_d})\in F_2^d}f(x_1,x_2,\cdots,x_n)$，并称 $T(I)$ 为极大项 (maxterm)，称 $P(\cdot)$ 为超级多项式 (superpoly)。

立方攻击中，攻击者把密码算法看作一个黑盒子，它是关于公开变量和未知变量的未知多项式，只考虑输出的一个比特。对密码算法的立方攻击分为 2 个阶段：预处理阶段和密钥恢复阶段。在预处理阶段，攻击者可以改变公开变量及未知变量的值并可模拟算法的执行，目的是通过 BLR 线性测试的方法[16]找到尽量多的关于未知变量的超级多项式，预处理过程只进行一次。在密钥恢复阶段，攻击者只改变公开变量的值，通过在预处理阶段找到的超级多项式建立仿射方程组来恢复某些密钥比特或进行区分攻击。

在预处理阶段，若找到的多项式 P 为常量，为方便起见，下面讨论中仍视其为攻击成功。

下面就一般布尔函数及布尔函数的代数次数或代数标准型项数受限情况下对立方攻击的成功概率进行分析。

3 一般布尔函数立方攻击成功概率分析

在一般情况下，分析对随机布尔函数立方攻击的成功概率。

设 $V=\{v_1,v_2,\cdots,v_m\}$ 为 m 个公开变量，$K=\{k_1,k_2,\cdots,k_n\}$ 为 n 个密钥变量，$f(v_1,v_2,\cdots,v_m,k_1,k_2,\cdots,k_n)$ 为含 $(m+n)$ 个变量的布尔函数，立方攻击

在寻找超级多项式时，先选定集合V的一个非空子集I，不妨设$I=\{v_1,v_2,\cdots,v_l\}$，$1\leqslant l\leqslant m$，并将其他公开变量设置为常数 0 或 1，此时，$f(v_1,v_2,\cdots,v_m,k_1,k_2,\cdots,k_n)$函数就退化为含$(l+n)$个变量的布尔函数$g(v_1,\cdots,v_l,k_1,\cdots,k_n)=f(v_1,\cdots,v_l,c_1,\cdots,c_{m-l},k_1,\cdots,k_n)$，其中，$c_i\in\{0,1\},1\leqslant i\leqslant m-l$。

定理 2　设$I=\{v_1,v_2,\cdots,v_l\}$，$K=\{k_1,k_2,\cdots,k_n\}$，$g(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n)$为含$(l+n)$个变量的随机布尔函数，$g(\cdot)=T(I)P\left(x_j\middle|x_j\in K\right)\oplus R\left(x_j\middle|x_j\in K\cup I\right)$，其中，$T(I)=\prod_{1\leqslant i\leqslant l}v_i$，$P(\cdot)$和$R(\cdot)$均为代数标准型表示的布尔函数，$T(I)\nmid R(\cdot)$代数标准型中的任意一项，那么，$P(\cdot)$为仿射函数或常量的概率为$\dfrac{1}{2^{2^n-n-1}}$。

证明　根据以代数标准型表示的$g(\cdot)$函数中各项所含集合I中变量的个数，可将$g(\cdot)$函数表示如下

$$g(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n)=f_0+\sum_{i=1}^{l}v_i f_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_t\leqslant l}v_{i_1}v_{i_2}\cdots v_{i_t}f_{i_1i_2\cdots i_t}+\cdots+v_1v_2\cdots v_l f_{1,2,\cdots,l}\quad(1)$$

其中，f_0及$f_{i_1i_2\cdots i_t}\left(1\leqslant i_1<i_2<\cdots<i_t\leqslant l,1\leqslant t\leqslant l\right)$均为关于变量$(k_1,k_2,\cdots,k_n)$的以代数标准型表示的布尔函数。不妨以$f_{1,2,\cdots,l}$为例，其可表示如下

$$f_{1,2,\cdots,l}=a_0+\sum_{i=1}^{n}a_ik_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_t\leqslant n}a_{i_1i_2\cdots i_t}k_{i_1}k_{i_2}\cdots k_{i_t}+\cdots+a_{1,2,\cdots,n}k_1k_2\cdots k_n$$

其中，参数$a_0,a_{i_1i_2\cdots i_t}\left(1\leqslant i_1<i_2<\cdots<i_t\leqslant n,1\leqslant t\leqslant n\right)\in\{0,1\}$，且各参数取值 0 或 1 的概率均为1/2。

若将$g(\cdot)$函数表示如下

$$g(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n)=T(I)P\left(x_j\middle|x_j\in K\right)\oplus R\left(x_j\middle|x_j\in K\cup I\right)\quad(2)$$

其中，$T(I)=\prod_{1\leqslant i\leqslant l}v_i=v_1v_2\cdots v_l$，且$T(I)\nmid R(\cdot)$代数标准型中的任意一项，比较式(1)和式(2)可得：$P\left(x_j\middle|x_j\in K\right)=f_{1,2,\cdots,l}$。因此有

$$P(\cdot)=a_0+\sum_{i=1}^{n}a_ik_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_t\leqslant n}a_{i_1i_2\cdots i_t}k_{i_1}k_{i_2}\cdots k_{i_t}+\cdots+a_{12\cdots n}k_1k_2\cdots k_n\quad(3)$$

式(3)中，所有参数a_0及$a_{i_1i_2\cdots i_t}(1\leqslant i_1<i_2<\cdots<i_t\leqslant n,1\leqslant t\leqslant n)$的可能取值共有$S_a=2^{2^n}$。

若使$P(\cdot)$为仿射函数或常量，参数$a_i\left(0\leqslant i\leqslant n\right)$可任意取值为 0 或 1，参数$a_{i_1i_2\cdots i_t}\left(1\leqslant i_1<i_2<\cdots<i_t\leqslant n,2\leqslant t\leqslant n\right)$必须全部取值为 0，因此所有参数的可能取值共有$S_1=2^{n+1}$。

式(1)中，设函数f_0及$f_{i_1i_2\cdots i_t}(1\leqslant i_1<i_2<\cdots<i_t\leqslant l,1\leqslant t\leqslant l-1)$中各参数的可能取值共有$\Delta_1$，那么$P(\cdot)$为仿射函数或常量的概率为

$$Pr_1=\frac{S_1\Delta_1}{S_a\Delta_1}=\frac{2^{n+1}}{2^{2^n}}=\frac{1}{2^{2^n-n-1}}$$

从定理 2 可以推出如下结论。

推论 1　立方攻击中，针对随机布尔函数，$P(\cdot)$为仿射函数或常量的概率与选择的公开变量的子集I的大小l无关，只与密钥长度n有关。

密码算法设计的目的是使密钥和初始向量（或明文）达到充分的混乱与扩散，在密码算法接近于随机的情况下，又一般密钥长度$n\geqslant 80$，则由定理 2 可知：$Pr_1=2^{-\left(2^n-n-1\right)}\approx 0$。

4　布尔函数的代数次数受限情况下立方攻击成功概率分析

本节针对布尔函数的代数次数对立方攻击的成功概率进行分析。

定理 3　设$g(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n)$为含$(l+n)$个变量的随机布尔函数，该布尔函数的代数次数不大于$s(2\leqslant s\leqslant l+n)$，设$I=\{v_1,v_2,\cdots,v_l\}$，$1\leqslant l\leqslant s-1$，$K=\{k_1,k_2,\cdots,k_n\}$，将$g(\cdot)$函数表示如下：$g(\cdot)=T(I)P\left(x_j\middle|x_j\in K\right)\oplus R\left(x_j\middle|x_j\in K\cup I\right)$，其中，$T(I)=\prod_{1\leqslant i\leqslant l}v_i$，$P(\cdot)$和$R(\cdot)$均为代数标准型表示的布尔函数，$T(I)\nmid R(\cdot)$代数标准型中的任意一项，那么，$P(\cdot)$为仿射函数或常量的概率为

$$Pr_2=\begin{cases}1, & s-l=1\\ \dfrac{1}{2^{\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{s-l}}}, & s-l>1\end{cases}$$

证明 根据以代数标准型表示的 $g(\cdot)$ 函数中各项所含集合 I 中变量的个数，可将 $g(\cdot)$ 函数表示如下

$$g(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n)=f_0+\sum_{i=1}^{l}v_i f_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_t\leqslant l}v_{i_1}v_{i_2}\cdots v_{i_t}f_{i_1i_2\cdots i_t}+\cdots+v_1v_2\cdots v_l f_{1,2,\cdots,l} \quad (4)$$

其中，f_0 为关于变量 $(k_1,k_2,\cdots,k_n)$ 的以代数标准型表示的代数次数 $\leqslant s$ 的布尔函数，$f_{i_1i_2\cdots i_t}(1\leqslant i_1<i_2<\cdots<i_t\leqslant l,1\leqslant t\leqslant l)$ 均为关于变量 $(k_1,k_2,\cdots,k_n)$ 的以代数标准型表示的代数次数小于等于 $(s-t)$ 的布尔函数，$f_{i_1i_2\cdots i_t}$ 可表示如下

$$f_{i_1i_2\cdots i_t}=a_0+\sum_{i=1}^{n}a_i k_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_q\leqslant n,1\leqslant q\leqslant s-t}a_{i_1i_2\cdots i_q}k_{i_1}k_{i_2}\cdots k_{i_q}$$

其中，参数 $a_0,a_{i_1i_2\cdots i_q}(1\leqslant i_1<i_2<\cdots<i_q\leqslant n,\ 1\leqslant q\leqslant s-t)\in\{0,1\}$，且各参数取值 0 或 1 的概率均为 1/2。

若将 $g(\cdot)$ 函数表示如下

$$g(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n)=T(I)P\left(x_j\middle|x_j\in K\right)\oplus R\left(x_j\middle|x_j\in K\cup I\right) \quad (5)$$

其中，$T(I)=\prod_{1\leqslant i\leqslant l}v_i=v_1v_2\cdots v_l$，且 $T(I)\nmid R(\cdot)$ 代数标准型中的任意一项，比较式(4)和式(5)可得：$P\left(x_j\middle|x_j\in K\right)=f_{12\cdots l}$。因此有

$$P(\cdot)=a_0+\sum_{i=1}^{n}a_i k_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_q\leqslant n,1\leqslant q\leqslant s-l}a_{i_1i_2\cdots i_q}k_{i_1}k_{i_2}\cdots k_{i_q} \quad (6)$$

下面分 2 种情况进行讨论。

若 $s-l=1$，则有：$P(\cdot)=a_0+\sum_{i=1}^{n}a_i k_i$，因此 $P(\cdot)$ 为仿射函数或常量的概率为 1。

若 $s-l>1$，式(6)中，所有参数 a_0 及 $a_{i_1i_2\cdots i_q}(1\leqslant i_1<i_2<\cdots<i_q\leqslant n,1\leqslant q\leqslant s-l)$ 的可能取值共有 $S_b=2^{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{s-l}}$。

若使 $P(\cdot)$ 为仿射函数或常量，参数 $a_i(0\leqslant i\leqslant n)$ 可任意取值为 0 或 1，参数 $a_{i_1i_2\cdots i_q}(1\leqslant i_1<i_2<\cdots<i_q\leqslant n,2\leqslant q\leqslant s-l)$ 必须全部取值为 0，因此所有参数的可能取值共有 $S_2=2^{\binom{n}{0}+\binom{n}{1}}$。

式(4)中，设函数 f_0 及 $f_{i_1i_2\cdots i_t}(1\leqslant i_1<i_2<\cdots<i_t\leqslant l,1\leqslant t\leqslant l-1)$ 中各参数的可能取值共有 Δ_2，那么 $P(\cdot)$ 为仿射函数或常量的概率为

$$Pr_2=\frac{S_2\Delta_2}{S_b\Delta_2}=\frac{2^{\binom{n}{0}+\binom{n}{1}}}{2^{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{s-l}}}=\frac{1}{2^{\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{s-l}}}$$

从定理 3 可以看出，设随机布尔函数的代数次数至多为 s，若代数次数 s 与极大项的代数次数 l 满足关系 $s-l=1$，立方攻击的成功概率为 1。然而，若选择的公开变量的个数 l 过小，或算法的代数次数 $s>(m+1)$，则有 $s-l>1$，又一般情况下，密钥长度 $n\geqslant 80$，由定理 3 可知，$P(\cdot)$ 为仿射函数或常量的概率 $Pr_2\leqslant 2^{-\binom{n}{2}}=2^{-\frac{n(n-1)}{2}}$，即 Pr_2 几乎为 0。这可以解释为什么密码算法的代数次数较低时立方攻击的成功概率较高。

由定理 3 易得，在立方攻击中，若布尔函数的代数次数 s 固定，随着选择的公开变量的子集 I 的大小 l 的逐渐增加，$P(\cdot)$ 为仿射函数或常量的概率也逐渐增加。因此，在对密码算法进行立方攻击时，若长时间找不到超级多项式，应适当增加选取的公开变量的个数 l，这也正是文献[1]中立方攻击所采用的手段。然而，立方攻击至少需要 2^l 次密码算法运算，因此随着 l 的增加，寻找超级多项式也变得越来越困难。

5 布尔函数的代数标准型项数受限情况下立方攻击成功概率分析

本节针对布尔函数的代数标准型项数对立方攻击的成功概率进行分析。

定理 4 设 $I=\{v_1,v_2,\cdots,v_l\}$，$K=\{k_1,k_2,\cdots,k_n\}$，$g(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n)$ 为含 $(l+n)$ 个变量的随机布尔函数，$g(\cdot)=T(I)P(x_j\,|\,x_j\in K)\oplus R(x_j\,|\,x_j\in K\cup I)$ v，其中，$T(I)=\prod_{1\leqslant i\leqslant l}v_i$，$P(\cdot)$ 和 $R(\cdot)$ 均为代数标准型 (ANF) 表示的布尔函数，$T(I)\nmid R(\cdot)$ 代数标准型中的任意一项。若 $g(\cdot)$ 函数可被 $T(I)$ 整除的代数标准型中，代数次数大于等于 $(l+2)$ 的代数标准型至多为 N 项且均匀出现，那么 $P(\cdot)$ 为仿射函数或常量的概率为 2^{-N}。

证明 根据以代数标准型表示的 $g(\cdot)$ 函数中各

项所含集合 I 中变量的个数，可将 $g(\cdot)$ 函数表示如下：

$$g(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n)=f_0+\sum_{i=1}^{l}v_i f_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_t\leqslant l}v_{i_1}v_{i_2}\cdots v_{i_t}f_{i_1i_2\cdots i_t}+\cdots+v_1v_2\cdots v_l f_{1,2,\cdots,l} \quad (7)$$

其中，f_0 及 $f_{i_1i_2\cdots i_t}\left(1\leqslant i_1<i_2<\cdots<i_t\leqslant l,1\leqslant t\leqslant l\right)$ 均为关于变量 $\left(k_1,k_2,\cdots,k_n\right)$ 的以代数标准型表示的布尔函数。不妨以 $f_{1,2,\cdots,l}$ 为例，其可表示如下：

$$f_{12\cdots l}=a_0+\sum_{i=1}^{n}a_i k_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_t\leqslant n}a_{i_1i_2\cdots i_t}k_{i_1}k_{i_2}\cdots k_{i_t}+\cdots+a_{12\cdots n}k_1k_2\cdots k_n$$

其中，参数 $a_0,a_{i_1i_2\cdots i_t}(1\leqslant i_1<i_2<\cdots<i_t\leqslant n,1\leqslant t\leqslant n)\in\{0,1\}$，且各参数取值 0 或 1 的概率均为 $1/2$。

若将 $g(\cdot)$ 函数表示如下

$$g\left(v_1,v_2,\cdots,v_l,k_1,k_2,\cdots,k_n\right)=T(I)P\left(x_j\left|x_j\in K\right.\right)\oplus R\left(x_j\left|x_j\in K\cup I\right.\right) \quad (8)$$

其中，$T(I)=\prod_{1\leqslant i\leqslant l}v_i=v_1v_2\cdots v_l$，且 $T(I)\nmid R(\cdot)$ 代数标准型中的任意一项，比较式(7)、式(8)可得：$P\left(x_j\left|x_j\in K\right.\right)=f_{1,2,\cdots,l}$。因此有

$$P(\cdot)=a_0+\sum_{i=1}^{n}a_i k_i+\cdots+\sum_{1\leqslant i_1<i_2<\cdots<i_t\leqslant n}a_{i_1i_2\cdots i_t}k_{i_1}k_{i_2}\cdots k_{i_t}+\cdots+a_{12\cdots n}k_1k_2\cdots k_n \quad (9)$$

因 $g(\cdot)$ 函数可被 $T(I)$ 整除的代数标准型中，代数次数不小于 $(l+2)$ 的代数标准型至多为 N 项，因此式(9)中所有参数 a_0 及 $a_{i_1i_2\cdots i_t}(1\leqslant i_1<i_2<\cdots<i_t\leqslant n,1\leqslant t\leqslant n)$ 的可能取值共有 $S_c=2^{\binom{n}{0}+\binom{n}{1}+N}$。

若使式(9)中 $P(\cdot)$ 为仿射函数或常量，参数 $a_i(0\leqslant i\leqslant n)$ 可任意取值为 0 或 1，参数 $a_{i_1i_2\cdots i_t}(1\leqslant i_1<i_2<\cdots<i_t\leqslant n,1\leqslant t\leqslant n)$ 必须全部取值为 0，因此所有参数的可能取值共有 $S_3=2^{\binom{n}{0}+\binom{n}{1}}$。

式(7)中，设函数 f_0 及 $f_{i_1i_2\cdots i_t}(1\leqslant i_1<i_2<\cdots<i_t\leqslant l,1\leqslant t\leqslant l-1)$ 中各参数的可能取值共有 Δ_3，那么 $P(\cdot)$ 为仿射函数或常量的概率为

$$Pr_3=\frac{S_3\Delta_3}{S_c\Delta_3}=\frac{2^{\binom{n}{0}+\binom{n}{1}}}{2^{\binom{n}{0}+\binom{n}{1}+N}}=\frac{1}{2^N}$$

由定理 4 可以看出，若布尔函数可被极大项整除的代数标准型中，代数次数不小于 $(l+2)$ 的项数至多为 N 项，那么随着 N 的逐渐减小，立方攻击的成功概率逐渐增大。

6　实验结果

上述理论分析结果与文献[1]中对 Trivium 算法的实验分析结果是相吻合的，如表 1 所示。为了节省硬件资源，Trivium 算法初始化过程采用二次函数迭代 1 152 拍，迭代 672 拍时，找到 63 个超级多项式，选取的公开变量的个数 l =12；迭代 735 拍时，找到 52 个超级多项式，l =23；迭代 770 拍时，找到 4 个超级多项式，l =29，30。再随着迭代拍数的增加，密码函数的代数次数增高，代数标准型项数增多，需要选择的公开变量的个数 l 也随之增加，理论上立方攻击的成功概率越来越低，实际上也超出了计算机的运算能力，因此并没有找到更多的超级多项式。

表 1　　对 Trivium 算法的立方攻击结果

迭代拍数	超级多项式个数	公开变量个数
672	63	12
735	52	23
770	4	29，30
大于 770	0	0

应用立方攻击方法，编程对 Grain v1 算法进行了分析[17]，如表 2 所示，实验结果与上述命题及结论也是吻合的。Grain v1 算法与 Trivium 算法相比，非线性次数较高，密钥扩散速度快，Grain v1 算法非线性反馈移存器的反馈多项式的非线性次数为 6，过滤函数的非线性次数为 3，而 Trivium 算法非线性反馈移存器的反馈多项式的非线性次数为 2，过滤函数是线性的。Grain v1 算法初始化过程共迭代 160 拍，迭代 70 拍时，找到 19 个超级多项式，迭代 75 拍时，找到 1 个超级多项式，再随着迭代拍数的增加，程序运行了数月仍未找到超级多项式。

表 2　　对 Grain v1 算法的立方攻击结果

迭代拍数	超级多项式个数	公开变量个数
70	19	7，8，9，10
75	1	8
大于 75	0	0

7 结束语

本文就一般布尔函数及布尔函数的代数次数或代数标准型项数受限情况下，从理论上分析了立方攻击的成功概率，为立方攻击密码分析方法提供了理论支持，理论结果与对流密码算法 Trivium 及 Grain v1 的实验结果是相吻合的。

在实际密码算法运行过程中，算法的迭代过程也是密钥的扩散过程，若算法迭代一定拍数后，代数次数已经比较高，且代数标准型项数也比较多，按照上述理论分析结果，这时找到超级多项式的概率几乎为 0，若在实际立方攻击过程中仍能找到超级多项式，则说明密码算法设计中密钥的扩散能力较差，因此立方攻击可作为密码算法设计中检验密钥扩散能力的一种手段。

致谢 在此，我们向对本文的工作给予支持和建议的同行，尤其是冯登国教授领导的讨论班上的同学和老师表示衷心的感谢。

参考文献：

[1] DINUR I, SHAMIR A. Cube attacks on tweakable black box Polynomials[A]. EUROCRYPT 2009[C]. Cologne, Germany, 2009. 278-299.

[2] CANNIÈRE C, PRENEEL B. TRIVIUM - a stream cipher construction inspired by block cipher design principles[EB/OL]. eStream- ECRYPT Stream Cipher Project, Report 2005/030, http:// www. ecrypt.eu. org/stream/trivium.html, 2005.

[3] AUMASSON J, DINUR I, MEIER W, *et al*. Cube testers and key recovery attacks on reduced-round MD6 and trivium[A]. FSE 2009[C]. Leuven, Belgium, 2009. 1-22.

[4] YANG L, WANG M, QIAO S. Side Channel Cube Attack on PRESENT[A]. CANS 2009[C]. Beijing, China, 2009. 379-391.

[5] FISCHER S, KHAZAEI S, MEIER W. Chosen IV statistical analysis for key recovery attacks on stream ciphers[A]. AFRICACRYPT 2008[C]. Casablanca, Morocco, 2008. 236-245.

[6] KHAZAEI S, MEIER W. New directions in cryptanalysis of self-synchronizing stream ciphers[A]. INDOCRYPT 2008[C]. Kharagpur, India, 2008. 15-26.

[7] VIELHABER M. Breaking ONE FIVIUM by AIDA an algebraic IV differential attack[EB/OL]. http://eprint.iacr.org/2007/413, 2007.

[8] ENGLUND H, JOHANSSON T, TURAN M S. A framework for chosen IV statistical analysis of stream ciphers[A]. INDOCRYPT 2007[C]. Chennai, India, 2007. 268-281.

[9] FILIOL E. A new statistical testing for symmetric ciphers and hash functions[A]. ICICS 2002[C]. Singapore, 2002. 342-353.

[10] SAARINEN M. Chosen-IV statistical attacks on eStream ciphers[A]. SECRYPT[C]. Setubal Portugal, 2006. 260-266.

[11] HELL M, JOHANSSON T, MAXIMOV A, *et al*. The Grain family of stream ciphers[A]. LNCS 4986[C]. Setubal, Portugal, 2008. 179-190.

[12] BABBAGE S, DODD M. The stream cipher MICKEY[EB/OL]. http://www.ecrypt.eu.org/stream, 2005.

[13] ARNAULT F, BERGER T, LAURADOUX C. Update on F-FCSR stream cipher[EB/OL]. http://www.ecrypt.eu.org/stream, 2006.

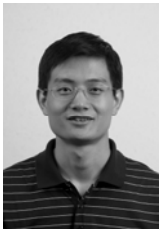
[14] LUCKS S. The saturation attack - a bait for Twofish[A]. FSE 2001[C]. Yokohama, 2001. 1-15.

[15] KNUDSEN L. Truncated and higher order differentials[A]. FSE 1994[C]. Leuven, Belgium, 1995. 196-211.

[16] BLUM M, LUBY M, RUBINFELD R. Self-testing/correcting with applications to numerical problems[A]. Proc 22nd Annual ACM Symp on Theory of Computing[C]. New York, USA, 1990. 73-83.

[17] 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.
SONG H X, FAN X B, WU C K, *et al*. Cube a ttack on Grain[J]. Journal of Software, 2012, 23(1): 171-176.

作者简介：



宋海欣（1976-），男，山东泗水人，中国科学院软件所博士生，主要研究方向为流密码。

范修斌（1966-），男，山东泰安人，中国科学院软件所教授、博士生导师，主要研究方向为密码学与信息安全。

武传坤（1964-），男，山东临沂人，中国科学院软件所研究员、博士生导师，主要研究方向为密码学与信息安全。

冯登国（1965-），男，陕西榆林人，中国科学院软件所研究员、博士生导师，主要研究方向为密码学与信息安全。