密码学中布尔函数的零化子

张文英[1], 武传坤[1], 于静之[2]
(1. 中国科学院软件研究所-中国科学院研究生院, 信息安全国家重点实验室, 北京 100080;
2. 山东医学高等专科学校, 山东济南 250002)

摘 要: 布尔函数的零化子与代数攻击息息相关, 但是如何构造一个给定函数的低次零化子仍然是一个悬而未决的问题. 本文对此问题进行了研究, 研究结果表明, 如果布尔函数的零点集有一个 k维子空间, 那么, 函数就会有代数次数为 $n-k$的零化子. 然而如何找到函数的具有最低代数次数的零化子仍然是一个亟待解决的难题.

关键词: 密码学; 代数攻击; 布尔函数的零化子
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2006) 01-0051-04

On the Annihilators of Cryptographic Boolean Functions

ZHANG Wen-ying[1], WU Chuan-kun[1], YU Jing-zhi[2]
(1. *State Key Lab of Information Security, Institute of Software – Graduate School of Chinese Academy of Sciences, Beijing 100080, China*; 2. *Shandong Medical College, Jinan, Shandong 250002, China*)

Abstract Annihilators of cryptographic Boolean functions have been shown to be closely related to algebraic attacks to stream ciphers. However how to construct annihilators of a given Boolean function remains a hard problem. As an approach to this problem, it gives an important characterization of annihilators with low degrees of a given Boolean function in terms of the set of x values on which $f(x)=0$. This gives a way to find annihilators of a given Boolean function, however how to find an annihilator of the lowest algebraic degree still remains unsolved.

Key words cryptography; algebraic attack; annihilator of Boolean functions

1 引言

基于线性反馈移位寄存器的代数攻击是由法国密码学家 Nicolas T. Courtois和 Willi Meier提出的[1], 此方法一经提出就对现有流密码体制形成了巨大威胁. 运用代数攻击的方法人们成功的破译了运用具有良好性质的布尔函数所设计的、能够抵抗所有已知攻击的 Toycrypt和 LILI-128[1-3]. Adi Shamir在 2004年的亚密会上作了题为 Stream Ciphers: Dead or Alive?[4] (流密码是死还是活)的报告, 使人们对流密码的前程倍感担忧. 由于代数攻击的提出, 使得一些新设计的流密码体制尽量避开使用基于线性移位寄存器的非线性组合函数, 而去仿效分组密码的块状结构模式, 例如最新提出的 Single-cycle T-function[5]和 Rabbit[6]流密码等. 在本文中我们假设读者已了解关于布尔函数的一些基本知识.

2 代数攻击的原理

定义 1 把 $f(x_1, \cdots, x_n)$中每个单项式都看作一个新的变量后所得到的线性方程叫做多变量方程 (multivariate algebraic equations).

例如 5元布尔函数

$$f(x)=x_1+x_3+x_5+x_1x_2+x_1x_5+x_2x_4+x_2x_5+x_3x_4+x_4x_5+x_3x_4x_5+x_1x_4x_5+x_2x_3x_5.$$

是 12个单项式的和, 从而 $f=0$是有 12个“变元”的多变量方程. 下文所说“变元”的个数均指方程中单项式的个数.

密码学中在设计同步流密码生成器时, 人们常将之分成两个部分——驱动部分和非线性组合部分. 它们的任务分别是: 驱动部分控制存储器的状态转移, 负责提供若干周期大、统计特性好的序列供组合部分使用, 而非线性部分则将由驱动部分提供的序列组合成满足要求的、性质好的密钥流序列. 驱动器部分采用 LFSR序列, 非线性组合部分对线性部分产生的序列进行混淆和扩散. 这种流密码的工作流程方式可以用方程组如下表示:

$$\begin{cases} b_0=f(s_0, s_1, \cdots, s_{n-1}) \\ b_1=f(L(s_0, s_1, \cdots, s_{n-1})) \\ b_2=f(L^2(s_0, s_1, \cdots, s_{n-1})) \\ \cdots \\ b_{m-1}=f(L^{m-1}(s_0, s_1, \cdots, s_{n-1})) \end{cases} \quad (1)$$

收稿日期: 2005-01-20; 修回日期: 2005-09-06
基金项目: 国家自然科学基金 (No. 90304007); 国家 973重点研究发展规划 (No. 2004CB318004); 中国博士后科学基金

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

其中 $(s_0, s_1, \cdots, s_{n-1})$是初态. 假设状态转移函数 L 及非线性组合函数 f都是事先给定的, 只有初态及初态的平移等价类未知. 攻击者的目的是通过分析观察到的输出密钥流序列 $(b_0, b_1, \cdots)$来恢复初态.

设 f的代数次数为 k. 由于线性变换不改变函数的代数次数, 所以对任意的 t, $f(s_0, s_1, \cdots, s_{n-1})$和 $f(L^t(s_0, s_1, \cdots, s_{n-1}))$的代数次数都相同, 因此方程组 (1)中"变元"的个数至多为 $C_n^1 + C_n^2 + \cdots + C_n^k$个. 若式 (1)中方程的个数 m 大于"变元"的个数, 则称方程组 (1)为超定系统 (over defined system).

设 $f(x)$是 n元布尔函数, 满足 $f(x)g(x) = 0$的非 0函数 $g(x)$称为 $f(x)$的零化子[7]. 利用布尔函数的零化子, 攻击者可以得到一个关于初态和输出密钥流序列的代数次数较低的方程, 从而减少多变量方程中变元的个数, 此方法被称为代数攻击. 代数攻击的数学描述为: 若存在函数 g, 使得 g的代数次数 d远远低于 f的代数次数 k, 那么在满足 $f(x) = 1$的点 $L^i(s_0, s_1, \cdots, s_{n-1})$, $j = 1, 2, \cdots$, 有

$$\begin{cases} g(L^{i_1}(s_0, s_1, \cdots, s_{n-1})) = 0 \\ g(L^{i_2}(L(s_0, s_1, \cdots, s_{n-1}))) = 0 \\ \cdots \\ g(L^{i_l}(s_0, s_1, \cdots, s_{n-1})) = 0 \end{cases} \tag{2}$$

且方程组 (2)中变元个数至多为 $C_n^1 + C_n^2 + \cdots + C_n^d$这个数目也远远小于方程组 (1)中变元个数. 于是只要 (2)中线性无关的方程的个数大于变元的个数 $C_n^1 + C_n^2 + \cdots + C_n^d$就可以唯一的恢复密钥, 这比直接解方程组 (1)要快得多. 由于在实际应用中, 都要求非线性组合函数 f是平衡函数, 若观察到密钥流序列的长度是 m, 则 (1)中将有 $m/2$个 $b_t = 1 (0 \leqslant t \leqslant m)$, 从而方程组 (2)中方程个数的期望值为 $m/2$

3 布尔函数零化子的代数次数

由前面的介绍可知, 对基于线性移位寄存器的流密码体制代数攻击的成效取决于该体制中所使用的非线性组合函数的零化子的代数次数, 零化子的代数次数越低, 方程组 (2)所含变元的个数越少, 代数攻击的复杂度越低. 于是根据函数的结构形式寻找函数的具有较低代数次数 (尤其是最低次数)的零化子将对代数攻击具有重要的指导意义. 本节的主要工作是给出了函数有代数次数为 $n-k$次零化子的一个判定定理, 另外还研究了布尔函数的代数次数最低的零化子集合的结构特征, 给出了关于布尔函数代数免疫阶的一个紧的上界.

首先介绍一下 Meier等的工作. 若以 R_n 记所有 n元布尔函数所做成的代数系统, Meier等在文献[7]中给出了关于布尔函数的零化子集合的一个简洁、完美的刻画:

定理 1[7] 设 f是 n元布尔函数. 则 f的所有零化子的集合 $An(f)$是 R_n 中由 $1+f$生成的主理想, 即: $An(f) = \{(1+f)r \mid r \in R_n\} = \langle 1+f \rangle$.

受定理 1的启发, 我们得到了关于布尔函数的代数次数最低的零化子集合的结构特征:

定理 2 设 f是 n元布尔函数, 且其零化子的代数次数最低为 d. 则其所有 d次零化子做成 R_n 的一个子空间.

证明 设 d是所有零化子代数次数的最小值, N 是 f的所有代数次数为 d的零化子所做成的集合. 若 $g_1, g_2 \in N$, 则 $g_1 + g_2 \in N$且 $\deg(g_1 + g_2) \leqslant d$, 因 d是所有零化子代数次数的最小值, 故一定有 $\deg(g_1 + g_2) = d$, 所以 N 对加法运算封闭, 因此 N 是 R_n 的一个子空间.

一般的来讲, 函数 f自身不一定有低次零化子, 但是 $f+1$可能有低次零化子. 例如函数 $f = 1 + x_1x_2\cdots x_n$ 仅在 $(1, 1, \cdots, 1)$处函数值为 0, 其余点处函数值都是 1, 它只有一个非平凡零化子, 是 n次布尔函数 $x_1x_2\cdots x_n$. 容易验证任意线性函数 $w \cdot x, w \in GF^n$ (2)都是 $f+1$的零化子. 如果 f没有低次零化子, 但 $f+1$有低次零化子 g, 则在 $f+1 = 0$(即 $f+1 = 1$)的点有 $g(x) = 0$, 攻击者便可以在所观察到的满足 $f = 0$的点建立方程组 (2). 因此函数 f抗代数攻击的能力取决于 f和 $f+1$的代数次数的最小值, 称这个最小值为布尔函数的代数免疫阶, 记作 $AI(f)$ (Algebraic Attack Immune). 代数免疫阶愈大, 函数抗代数攻击的能力愈强, 反之就弱. 下面我们给出关于布尔函数的代数免疫阶上限的一个定理.

引理 1[7] 设 f是 n元布尔函数. 那么存在代数次数至高为 $\lceil n/2 \rceil$的非 0布尔函数 g, 使得 fg 的代数次数不超过 $\lceil n/2 \rceil$

定理 3 设 f是 n元布尔函数. 则 $AI(f) \leqslant \lceil n/2 \rceil$.

证明 由引理 1, 存在代数次数至多为 $\lceil n/2 \rceil$的非 0布尔函数 $g \neq 0$, 使得 $fg = h$的代数次数至多为 $\lceil n/2 \rceil$. 因 $fg = fh$, 若 $g \neq h$, 则 $f(g+h) = 0$, 从而 $g+h$ 是 f的代数次数不大于 $\lceil n/2 \rceil$的零化子. 若 $g = h$, 则有 $fh = h$, $(f+1)h = 0$, 则 h 是 $f+1$的代数次数不大于 $\lceil n/2 \rceil$的零化子.

令 $offset(f) = \{x: f(x) = 0\}$, $supp(f) = \{x: f(x) = 1\}$, 并分别称它们为 $f(x)$的零点集和支撑. 易知 g 是 f的零化子的充要条件是 g的支撑是 f的零点集的子集. 即 $g = 1$时 f一定等于 0. 于是以 f的零点集的子集为支撑的所有函数作成 f的零化子的全体. 于是欲构造 f的零化子, 只须从 $offset(f)$中取一子集, 以此集合为支撑的函数便是 f的一个零化子, 零化子的代数次数完全取决于所取集合的结构特点. 基于此我们给出了布尔函数有 $n-k$次零化子的一个充分条件, 首先来看一个引理:

引理 2 设 S是 GF^n (2)的一个 k维子空间, $\boldsymbol{M}$ 是以 S中所有元素为行作成的矩阵. 若 $\boldsymbol{M}$ 的第 j列非零, 那么该列中 0、1个数各半.

证明 设 $\alpha_1, \cdots, \alpha_k$是 S的一组基. 当 $\lambda = (\lambda_1, \cdots, \lambda_k)$ 取遍 GF^k (2)时, $\lambda(\alpha_1, \cdots, \alpha_k)^T$ 取遍 $\boldsymbol{M}$ 的所有行向量, 此处"T"表示矩阵或向量的转置. 以 $a_{1j}, \cdots, a_{kj}$记 $\alpha_1, \cdots, \alpha_k$ 的

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

第 j个分量. 当 $\lambda=(\lambda_1,\cdots,\lambda_k)$取遍 $GF^k(2)$时 $\lambda(a_{1j},\cdots,a_{kj})$,取遍矩阵$\boldsymbol{M}$的第 j列中所有元素, $(\lambda_1,\cdots,\lambda_k)(a_{1j},\cdots,a_{kj})$表示通常意义下的内积. 注意到若$\boldsymbol{M}$的第 j列非零, 由 $\alpha_1,\cdots,\alpha_k$是 S的一组基可以推得 $(a_{1j},\cdots,a_{kj})\neq 0$对于取定的 $(a_{1j},\cdots,a_{kj})\neq 0$,线性方程 $\lambda_1 a_{1j}+\cdots+\lambda_k a_{kj}=0$在$GF^k(2)$中有 2^{k-1}个解, 故 $a_{1j},\cdots,a_{kj}$有 2^{k-1}个组合为 0

定义 2　设 V是 $GF^n(2)$的 k维子空间, s是 $GF^n(2)$中非零向量, 称集合 $\{s+v, v\in V\}$为 $GF^n(2)$的 k维仿射子空间.

定理 4　设 f是 n元布尔函数. 若 f的零点集有一 k维子空间(或仿射子空间) S, 则 f具有代数次数为 $n-k$的零化子.

证明　设 $S=\{(a_{i1}+c_1,\cdots,a_{in}+c_n), i=1,\cdots,2^k, c_r\in GF^k(2)$是常数, $r=1,\cdots,n\}$, g是以 S为支撑的布尔函数, 根据前面的讨论可知, g是 f的零化子, 并且 g的小项表示为

$$g(x_1,x_2,\cdots,x_n)=\sum_{(a_{i1}+c_1,\cdots,a_{in}+c_n)\in S}\prod_{l=1}^{n}(x_l+a_{il}+c_l+1),\quad c=(c_1,c_2,\cdots,c_n). \tag{3}$$

为书写方便, 用 y_l代替式(3)中的 x_l+c_l+1,有

$$\begin{aligned}h(y_1,y_2,\cdots,y_n)&=\sum_{(a_{i1}+c_1,\cdots,a_{in}+c_n)\in S}\prod_{l=1}^{n}(y_l+a_{il})\\&=\sum_{l=0}^{n}\Big(\sum_{i=1}^{2^k}a_{ij_{l+1}}a_{ij_{l+2}}\cdots a_{ij_n}\Big)y_{j1}y_{j2}\cdots y_{jl},\quad 1\leqslant l\leqslant n.\end{aligned} \tag{4}$$

此处 $j_1,j_2\cdots j_n$是 $1,2,\cdots,n$的一个排列, $\{j_{l+1},j_{l+2},\cdots,j_n\}=\{1,2,\cdots,n\}\setminus\{j_1,\cdots,j_l\}$. 易见 $\deg(h)=\deg(g)$. 因此只须再证明 h的代数次数为 $n-k$即可. 以 S中的所有元素为行作矩阵

$$M=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1k}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2k}&\cdots&a_{2n}\\a_{31}&a_{32}&\cdots&a_{3k}&\cdots&a_{3n}\\\cdots&\cdots&\cdots&\cdots&\cdots&\cdots\\a_{2^k1}&a_{2^k2}&\cdots&a_{2^kk}&\cdots&a_{2^kn}\end{pmatrix}$$

则 $y_{j1}y_{j2}\cdots y_{jl}$, $l\leqslant n$的系数等于 M的第 $j_{l+1},j_{l+2},\cdots,j_n$列中位于同一行的元素的乘积, 再对这些乘积作和. 下面分情况证明在 h的代数标准型中代数次数大于 $n-k$的单项式的系数都是 0

(i)因为矩阵 M有 2^k行, 所以 $y_1y_2\cdots y_n$的系数为 0

(ii)任一 $n-1$次项 $y_{j_1}y_{j_2}\cdots y_{j_{n-1}}$的系数是

$$\sum_{i=1}^{2^k}a_{ij_n}\pmod 2,$$

即矩阵 M的第 j_n列中所有元素之和. 若第 j_n列中元素全是 0,那么结论显然成立. 若不然, 则由引理 2知第 j_n列中 1的个数为 2^{n-1}, 于是当 $n>1$时, 也有

$$\sum_{i=1}^{2^k}a_{j_n}=0(\bmod 2).$$

(iii)任一 $n-2$次项 $y_{j1}y_{j2}\cdots y_{j_{n-2}}$的系数是 $\sum_{i=1}^{2^k}a_{ij_{n-1}}a_{ij_n}$ $(\bmod 2)$, 即矩阵 M的第 j_{n-1}列与第 j_n列的内积. 如果这两个列向量线性相关, 那么要么至少一个向量 0,此时结论显然成立; 要么两个向量都不为 0,但是相等, 类似于(ii)中的讨论可得此时

$$\sum_{i=1}^{2^k}a_{ij_{n-1}}a_{ij_n}=\sum_{i=1}^{2^k}a_{ij_{n-1}}=2^{k-1}\equiv 0(\bmod 2),\ k>1. \tag{5}$$

如果两个向量线性无关, 用 $P\{a_{ij}=1\}$表示 M的第 (i,j)个元素为 0的概率. 由引理 2 $P\{a_{ij_{n-1}}=1\}=P\{a_{ij_n}=1\}=1/2$且

$$\sum_{i=1}^{2^k}a_{ij_{n-1}}a_{ij_n}=P\{a_{ij_{n-1}}a_{ij_n}=1\}\times 2^k=2^{k-2}\equiv 0(\bmod 2),\ k>2 \tag{6}$$

(iv)下面我们分三种情况讨论(4)中 $y_{j_4}\cdots y_{j_n}$的系数:

- 第 j_1,j_2,j_3列线性无关;
- 有一列是其余两列之和;
- 有两列相等.

在第一种情形, 与式(6)类似有

$$\sum_{i=1}^{2^k}a_{ij_{n-2}}a_{ij_{n-1}}a_{ij_n}=P\{a_{ij_{n-2}}a_{ij_{n-1}}a_{ij_n}=1\}\times 2^k=2^{k-3}\equiv 0(\bmod 2),\ k>3.$$

在第二种情形,

$$\sum_{i=1}^{2^k}a_{ij_{n-2}}a_{ij_{n-1}}a_{ij_n}=\sum_{i=1}^{2^k}a_{ij_{n-2}}a_{ij_{n-1}}(a_{ij_{n-2}}+a_{ij_{n-1}})\equiv 0(\bmod 2). \tag{7}$$

而最后一种情形可以归结为等式(5)或(6).

(v)对一般的 $l(l>n-k)$次单项式 $y_{j_1}y_{j_2}\cdots y_{j_l}$的系数用数学归纳法. 当 M的其余 $n-l$列线性无关时, 类似于 $l=2$的情形, 我们有

$$\sum_{i=1}^{2^k}a_{ij_{l+1}}\cdots a_{ij_n}=2^{k-(n-l)}\equiv 0(\bmod 2),\ n-l<k.$$

如果这 $n-l$个列向量线性相关, 设 $\alpha_{j_1},\cdots,\alpha_{j_t}$, $t<n-l$是这些列向量的一组基, 则

$$\sum_{i=1}^{2^k}a_{ij_{l+1}}\cdots a_{ij_n}=\sum_{i=1}^{2^k}a_{ij'_1}\cdots a_{ij'_t}\lambda^{i_{t+1}}\cdot(a_{ij'_1},\cdots,a_{ij'_t})\cdots\lambda^{i_{n-l}}\cdot(a_{ij'_1},\cdots,a_{ij'_t}). \tag{8}$$

此处, $\lambda^{i_{t+1}},\cdots,\lambda^{i_{n-l}}\in F_2^k$, $\alpha_{j_1}=(a_{1,j'_1},\cdots,a_{2^k,j'_1})^{\mathrm{T}},\cdots,\alpha_{j_t}=(a_{1j'_t},\cdots,a_{2^kj'_t})^{\mathrm{T}}$. 在$\{\lambda^{i_{t+1}},\cdots,\lambda^{i_{n-l}}\}$中有一个 λ^{i_s}的汉明重量为偶数, 类似于(7), 对于 $1\leqslant i\leqslant 2^k$有

$$a_{ij'_1}\cdots a_{ij'_t}\lambda^{i_{t+1}}\cdot(a_{ij'_1},\cdots,a_{ij'_t})\cdots\lambda^{i_{n-l}}\cdot(a_{ij'_1},\cdots,a_{ij'_t})\equiv 0$$

若所有 $\lambda^{i_{t+1}},\cdots,\lambda^{i_{n-l}}$的汉明重量都为奇数, 则有

$$a_{ij'_1}\cdots a_{ij'_t}\lambda^{i_{t+1}}\cdot(a_{ij'_1},\cdots,a_{ij'_t})\cdots\lambda^{i_{n-l}}\cdot(a_{ij'_1},\cdots,a_{ij'_t})=a_{ij'_1}\cdots a_{ij'_t},$$

故

$$\sum_{i=1}^{2^k}a_{ij_{l+1}}\cdots a_{ij_n}=\sum_{i=1}^{2^k}a_{ij'_1}\cdots a_{ij'_t}=2^{k-t}\equiv 0(\bmod 2),\ t<k$$

综合(i)-(v), 我们证明了代数次数大于 $n-k$的单项式系数都是 0下面我们证明若 M的第 $j_{n-k+1},j_{n-k+2},\cdots,j_n$列线性无关, 那么在 h的代数表达式中 $x_{j_1}x_{j_2}\cdots x_{j_{n-k}}$的系数为 1.事实上, 在仅以 M的 $j_{n-k+1},j_{n-k+2},\cdots,j_n$列为列向量作成的新矩阵中, 只有一个全 1行, 故

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$$\sum_{i=1}^{2^t} a_{j_{n-k+1}} a_{j_{n-k+2}} \cdots a_{j_n} = 1.$$

因此, h的代数次数为 $n-k$, 从而 g的代数次数也为 $n-k$.

例 令 $f(x) = x_1 + x_3 + x_5 + x_1x_2 + x_1x_4 + x_1x_5 + x_2x_4 + x_2x_5 + x_3x_4 + x_1x_2x_3 + x_2x_3x_4x_5$.

则 $f(x)$是 F_2^5上的平衡函数, 在 $f(x)$的零点集中有一个 3维子空间

$S = \{(00000), (11100), (11010), (00110), (01001), (10101), (10011), (01111)\}$.

若定义 $$g(x) = \begin{cases} 1 & x \in S \\ 0 & \text{其它} \end{cases}$$

则 g是 f的 5-3=2次零化子, g的 ANF是

$g(x) = 1 + x_1 + x_2 + x_3 + x_4 + x_5 + x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_5 + x_4x_5$.

4 结论

代数攻击是分析现有密码体制的一种新的强有力的分析方法. 如果 f的零点集包含一个维数较高的子空间或仿射子空间, 将导致 f存在低次零化子, 进而攻击者就可以建立一个关于密钥和输出序列 (明文)的低次方程, 于是得以快速恢复密钥. 因此, 为了抵抗代数攻击, 设计者应尽量避免使用零点集中包含一个维数较高的子空间或仿射子空间的密码函数.

参考文献:

[1] NicolasT Courtois, WilliMeier. Algebraic attacks on stream ciphers with linear feedback[A]. Advances in Cryptology-EUROCRYPT 2003[C]. LNCS 2656, Berlin: Springer-Verlag, 2003. 346-359.

[2] M Mihaljevic, H Imai. Cryptanalysis of Toyocrypt-HS1 stream cipher. IEICE Transactions on Fundamentals, vol. E85-A, 66-73[OL]. http://www.csl.esat.sony.co.jp/atl/papers/IEICE jan02.pdf

[3] Steve Babbage. Cryptanalysis of LILI-128, Nessie project internalreport[OL]. http://www.cosic.esat.kuleuven.ac.be/nessie/reports/, January 2001. 22.

[4] Adi Shamir. Stream ciphers: dead or alive[A]. Advances in Cryptology-ASIACRYPT 2004[C]. LNCS 3329. Berlin: Springer-Verlag, 2004. 78.

[5] Jin Hong, Dong Hoon Lee, Yongjin Yeom, Daewan Han. A new class of single cycle T-functions[A]. Fast Software Encryption 2005[C]. LNCS 3557, Berlin: Springer-Verlag, 2005.

[6] Martin Boesgaard, Mette Vesterager, Thomas Pedersen, Jesper Christiansen, Ove cavenius. Rabbit: A newHigh-performance stream cipher[A]. Fast Software Encryption 2003[C]: LNCS 2887, Berlin: Springer-Verlag, 2003. 307-329.

[7] WilliMeier, Enes Pasalic, Claude Carlet. Algebraic attacks and decomposition of Boolean functions[A]. In Advances in Cryptology-EUROCRYPT 2004[C]. LNCS3027, Berlin: Springer-Verlag, 2004. 474-491.

作者简介:

张文英 女, 1970年 6月出生于山东省鄄城县, 中科院软件所博士后, 副教授, 研究方向为密码学. E-mail: wenyingzh@is.iscas.ac.cn

武传坤 男, 1964年 7月出生于山东沂水县, 中科院软件所研究员, 博导, 中科院百人计划引进人才, 主要研究方向为密码学, 网络安全和电子商务等. E-mail: ckwu@is.iscas.ac.cn.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net