关于涂-邓猜想的一点注记

黄 昆[1] 李 超[1] 傅绍静[2,3]
(国防科技大学数学与系统科学系 长沙 410073)[1](国防科技大学计算机学院 长沙 410073)[2]
(上海市信息安全综合管理技术研究重点实验室 上海 200240)[3]

摘 要 为多种密码学构造性质良好的布尔函数一直是对称密码学研究中的一个难点问题。最近,涂自然和邓映蒲基于一个二元组合猜想的正确性,构造了两类具有最优代数免疫度的布尔函数,其中第一类函数是具有最优代数免疫度的 Bent 函数,另一类是平衡且具有最优代数免疫度的高非线性度函数。涂-邓猜想引起了国内外密码学者的高度关注。现通过分析涂-邓猜想中参数 t 满足 $wt(t)=3$ 情形时的二元 Hamming 重量的特性,给出涂-邓猜想在 $wt(t)=3$ 情形下的证明,并以推论的形式推出 $wt(t)=k-3$ 的证明。

关键词 对称密码,布尔函数,涂-邓猜想,Hamming 重量

Note on the Tu-Deng Conjecture

HUANG Kun[1] LI Chao[1] FU Shao-jing[2,3]
(Depart. of Mathematic and System Science, National University of Defense Technology, Changsha 410073, China)[1]
(College of Computer, National University of Defense Technology, Changsha 410073, China)[2]
(Shanghai Key Lab of Integrate Administration Technologies for Information Security, Shanghai 200240, China)[3]

Abstract It is a difficult challenge to find Boolean functions used in symmetric ciphers achieving many good cryptographic properties. Recently, two classes of Boolean functions with maximum algebraic immunity have been proposed by Tu and Deng based on correctness of the assumption of a combinatorial conjecture about binary. One class of the functions are bent functions with maximum algebraic immunity, and another class of the functions are balanced and have maximum algebraic immunity, optimal algebraic degree and good nonlinearity. Tu-Deng conjecture has received a lot of attentions from cryptographers. The conjecture in the case of $wt(t)=3$ was proved. As a corollary, the case of $wt(t)=k-3$ was also proved.

Keywords Symmetric ciphers, Boolean functions, Tu-Deng conjecture, Hamming weight

1 引言

为了抵抗代数攻击,对称密码算法中所使用的布尔函数必须具有较高的代数免疫度,构造具有最优代数免疫度的布尔函数成为近年来密码学研究中的重要问题[1-5]。但是,这些构造的布尔函数仅仅满足代数免疫达到最优,而非线性度等其他密码学性质不是很好。

2009 年,基于如下二元组合猜想:

猜想 设 $S_t=\{(a,b)\mid a,b\in Z_{2^k-1},a+b\equiv t(\mathrm{mod}\ 2^k-1),\omega(a)+\omega(b)\leqslant k-1\}$,其中 $1\leqslant t\leqslant 2^k-2,k\geqslant 2,\omega(x)$ 是 x 的 2-重量,那么 $\#S_t\leqslant 2^{k-1}$。

涂自然和邓映蒲首次构造了一类具有最优代数免疫度的 Bent 函数[6],进一步,他们通过调整所构造函数的部分点的取值,得到了具有最优代数免疫度和高非线性度的平衡布尔函数;2010 年,唐小虎等人基于涂-邓猜想,进一步提高了具有最优代数免疫度的平衡布尔函数的非线性度,同时也给出了一类代数次数最优、代数免疫度次优和非线性度良好的偶数元一阶弹性函数[8]。此后,基于涂-邓猜想,杜育松和张方国给出了一类代数次数最优、代数免疫度次优和非线性度良好的奇数元一阶弹性函数[10]。

在学者们基于涂-邓猜想为多种密码学构造性质良好的布尔函数的同时,关于涂-邓猜想的证明也受到了广泛的关注。在文献[6]中,涂自然和邓映蒲验证了猜想在 $k\leqslant 29$ 的情形下是正确的。2010 年,CUSICK 和 YUAN LI 等人给出了 $\omega(t)=1,2;t'=2^k-t,\omega(t')\leqslant 2;t'=2^k-t,3\leqslant\omega(t')\leqslant 4,t'$ 是奇数情形下猜想正确性的证明[7]。在文献[11]中,Gerard Cohen 给出了涂-邓猜想的一个变种的证明,但是仍然未能证明涂-邓猜想。本文通过分析涂-邓猜想中参数 t 满足 $wt(t)=3$ 情形时的二元 Hamming 重量的特性,给出了涂-邓猜想在 $wt(t)=3$ 情形下的证明,并以推论的形式推出 $wt(t)=k-3$ 的证明。

2 预备知识

引理 1[7] 用 $\omega(x)$ 表示整数 x 的二元 Hamming 重量,则下面断言是正确的:

(1)$\omega(2^k-1-x)=k-\omega(x),0\leqslant x\leqslant 2^k-1$;

本文受国家自然科学基金(61070215,61103191)和上海市信息安全综合管理技术研究重点实验室开放课题(AGK2012001)资助。

黄 昆(1989-),男,研究生,主要研究方向为编码密码理论及其应用;李 超(1966-),男,博士生导师,主要研究方向为编码密码理论及其应用;傅绍静(1984-),男,讲师,主要研究方向为编码密码理论及其应用。

(2)$\omega(x+2^i)\leqslant\omega(x)$，如果 $x_i=1$；

(3)$\omega(x+y)\leqslant\omega(x)+\omega(y)$，等号成立当且仅当对任意 i，$x_i+y_i\leqslant 1$；

(4)$\omega(x)=\omega(x-1)-i+1, x\equiv 2^i \pmod{2^{i+1}}$。

引理 2[7] 设一正整数 m，设

$N_r^{(i,j)}=\#\{x\mid 0\leqslant x\leqslant 2^m-1,\omega(2^i+2^j+x)=r+\omega(x)\}$，$0\leqslant i<j\leqslant m-1$，那么 $N_2^{(i,j)}=2^{m-2}$，$N_r^{(i,j)}=0$，$r\geqslant 3$，

$$N_1^{(i,j)}=\begin{cases}2^{m-2}+2^{m-3}, i+1<j=m-1\\ 2^{m-2}, i+1=j=m-1\\ 2^{m-2}, i+1<j\leqslant m-2\\ 2^{m-3}, i+1=j\leqslant m-2\end{cases}$$

$$N_0^{(i,j)}=\begin{cases}2^{m-3}+2^{m-4}, i+2<j=m-1\\ 2^{m-3}, i+2=j=m-1\\ 2^{m-2}, i+1=j=m-1\\ 2^{m-2}, i+2<j=m-2\\ 2^{m-3}+2^{m-4}, i+2=j=m-2\\ 2^{m-2}, i+1=j=m-2\\ 2^{m-3}+2^{m-4}, i+2<j\leqslant m-3\\ 2^{m-3}, i+2=j\leqslant m-3\\ 2^{m-3}+2^{m-4}, i+1=j\leqslant m-3\end{cases}$$

引理 3[7] 设

$N_r^{(i,j,l)}=\#\{x\mid 0\leqslant x\leqslant 2^m-1,\omega(2^i+2^j+2^j+x)=r+\omega(x)\}$

其中 $0\leqslant i<j<l\leqslant m-1$，则有：

(1) $N_3^{(i,j,l)}=2^{m-3}$，

(2)

$$N_2^{(i,j,l)}=\begin{cases}2^{m-2}, i+2<j+1<l=m-1\\ 2^{m-3}+2^{m-4}, i+2=j+1<l=m-1\\ 2^{m-3}+2^{m-4}, i+2<j+1=l=m-1\\ 2^{m-3}, i+2=j+1=l=m-1\\ 2^{m-3}+2^{m-4}, i+2<j+1<l\leqslant m-2\\ 2^{m-3}, i+2=j+1<l\leqslant m-2\\ 2^{m-3}, i+2<j+1=l\leqslant m-2\\ 2^{m-4}, i+2=j+1=l\leqslant m-2\end{cases}$$

(3)

$$N_1^{(i,j,m-1)}=\begin{cases}2^{m-3}+2^{m-4}+2^{m-5}, i+4<j+2<l=m-1\\ 2^{m-3}+2^{m-4}, i+4=j+2<l=m-1\\ 2^{m-3}+2^{m-5}, i+3=j+2<l=m-1\\ 2^{m-3}+2^{m-4}, i+4<j+2=l=m-1\\ 2^{m-3}+2^{m-5}, i+4=j+2=l=m-1\\ 2^{m-3}, i+3=j+2=l=m-1\\ 2^{m-3}+2^{m-4}+2^{m-5}, i+3<j+1=l=m-1\\ 2^{m-3}+2^{m-4}, i+3=j+1=l=m-1\\ 2^{m-3}, i+2=j+1=l=m-1\\ 2^{m-3}+2^{m-4}+2^{m-5}, i+4<j+2<l=m-1\end{cases}$$

$$N_1^{(i,j,m-2)}=\begin{cases}2^{m-3}+2^{m-4}+2^{m-5}, i+4<j+2<l=m-2\\ 2^{m-3}+2^{m-4}, i+4=j+2<l=m-2\\ 2^{m-3}+2^{m-4}, i+3=j+2<l=m-2\\ 2^{m-3}+2^{m-4}, i+4<j+2=l=m-2\\ 2^{m-3}+2^{m-5}, i+4=j+2=l=m-2\\ 2^{m-3}+2^{m-5}, i+3=j+2=l=m-2\\ 2^{m-3}+2^{m-4}, i+3<j+1=l=m-2\\ 2^{m-3}+2^{m-5}, i+3=j+1=l=m-2\\ 2^{m-3}, i+2=j+1=l=m-2\end{cases}$$

$$N_1^{(i,j,l)}=\begin{cases}2^{m-3}+2^{m-4}, i+4<j+2<l\leqslant m-3\\ 2^{m-3}+2^{m-5}, i+4=j+2<l\leqslant m-3\\ 2^{m-3}+2^{m-5}, i+3=j+2<l\leqslant m-3\\ 2^{m-3}+2^{m-5}, i+4<j+2=l\leqslant m-3\\ 2^{m-3}, i+4=j+2=l\leqslant m-3\\ 2^{m-3}, i+3=j+2=l\leqslant m-3\\ 2^{m-3}+2^{m-5}, i+3<j+1=l\leqslant m-3\\ 2^{m-3}, i+3=j+1=l\leqslant m-3\\ 2^{m-4}+2^{m-5}, i+2=j+1=l\leqslant m-3\end{cases}$$

引理 4 设 $\forall t\in Z_{2^k-1}$，$\omega(t)=3$，$t=2^i+2^j+2^l$，$t_1=2^{i+k-1-l}+2^{j+k-1-l}+2^{k-1}$，则 $|S_t|=|S_{t_1}|$。

证明：实际上对任意的 $(a,b)\in S_t$，$2^{k-1-l}a+2^{k-1-l}b=t_1\equiv 2^{k-1-l}t \bmod 2^k-1$，$\omega(2^{k-1-l}a)+\omega(2^{k-1-l}b)=\omega(a)+\omega(b)\leqslant k-1$，因此有一对 $(a,b)\in S_t$，就有一对 $(2^{k-1-l}a,2^{k-1-l}b)\in S_{t_1}$。

引理 5 设

$\omega(2^i+2^j+v)=\omega(v)+2$，$1\leqslant v\leqslant 2^{k-1}-1-2^i-2^j-1$

则方程的解数为 $2^{k-3}-2$。

证明：$v=0$ 显然是方程的解，当 $2^{k-1}-1-2^i-2^j<v\leqslant 2^{k-1}-1$，必然有 $v_i=1$ 或者 $v_j=1$ 或者都为 1，它与方程所要求的 $v_i=0$，$v_j=0$ 矛盾，因此当 $2^{k-1}-1-2^i-2^j\leqslant v\leqslant 2^{k-1}-1$，只有 $v=2^{k-1}-1-2^i-2^j$ 是方程的解，显然 $v=0$ 是方程的解，所以方程的解数为 $2^{k-3}-2$；而当 $k=3$，$i=0$，$j=1$ 时，$v=2^{k-1}-1-2^i-2^j=0$，所以此时方程的解数为 $2^{k-3}-1$。

引理 6 $|S_t|+|S_{-t}|=2^k-|\{(a,b)\mid a,b\in Z_{2^k-1},a+b\equiv t \bmod 2^k-1,\omega(a)+\omega(b)=k\}|$。

证明：令 $b=2^k-1-b_1$，$a=2^k-1-a_1$，则 $a+b\equiv t \bmod 2^k-1$ 等价于 $-a_1-b_1\equiv t(\bmod 2^k-1)$，并且 $\omega(a_1)+\omega(b_1)\geqslant k+1\Leftrightarrow a_1+b_1\equiv -t(\bmod 2^k-1)$，$\omega(a_1)+\omega(b_1)\geqslant k+1$，从而得出证明。

3 $\omega(t)=3$ 的情形下猜想的证明

定理 1 设 $S_t=\{(a,b)\mid a,b\in Z_{2^k-1},a+b\equiv t(\bmod 2^k-1),\omega(a)+\omega(b)\leqslant k-1\}$，这里 $1\leqslant t\leqslant 2^k-2$，$k\geqslant 2$，$\omega(x)$ 是 x 的 2-重量，那么当 $\omega(t)=3$ 时，$\#S_t\leqslant 2^{k-1}$。

证明：当 $\omega(t)=3$ 时，不妨设 $t=2^i+2^j+2^l$，$i<j<l$，由引理 4 知只需证明 $l=k-1$ 的情况：

对任意 $a\in Z_{2^k-1}$，如果 $a\leqslant t$，根据 $a+b\equiv t(\bmod 2^k-1)$，故 $b=t-a$；令 $\sigma=\omega(a)+\omega(2^i+2^j+2^{k-1}-a)$，

① 当 $1\leqslant a\leqslant 2^i$ 时

$\sigma=\omega(a)+\omega(2^{k-1}+2^j+2^i-1-(a-1))=\omega(a)+2+i-\omega(a-1)\leqslant 3+i\leqslant k-3+3=k$

并且 $\sigma=k\Leftrightarrow i=k-3$，$\omega(a)=\omega(a-1)+1$。$\sigma=k$ 的 $(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$ 共有 2^{k-4} 对。

② 当 $2^i+1\leqslant a\leqslant 2^i+2^j$ 时

$\sigma=\omega(a)+1+j-\omega(a-2^i-1)\leqslant 3+j\leqslant k+1$

经计算得到 $\sigma=k+1\Leftrightarrow j=k-2$，$\omega(a)-\omega(a-2^i-1)=2$，令 $x=a-2^i-1$，可得 $\omega(x+2^i+1)=\omega(x)+2$，$0\leqslant x\leqslant 2^j-1$，$j=k-2$，由引理 2 计算得出满足条件的 $(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$ 共有 2^{k-4} 对。

$\sigma=k\Leftrightarrow j=k-3$，$\omega(x+2^i+1)=\omega(x)+2$，$0\leqslant x\leqslant 2^j-1$ 或者 $j=k-2$，$\omega(x+2^i+1)=\omega(x)+1$，$0\leqslant x\leqslant 2^j-1$ 同样由引

理 2 得出满足 $j=k-3$ 条件的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$共有 2^{k-4} 对，而满足 $j=k-2$ 条件的，由引理 2 的 $N_1^{(i,j)}$ 的类似计算得出

$$\begin{cases}2^{k-4}+2^{k-5}, & 1<i=k-3\\ 2^{k-4}, & 1=i=k-3\\ 2^{k-4}, & 1<i\leqslant k-4\\ 2^{k-5}, & 1=i\leqslant k-4\end{cases}$$

③ 当 $2^j+2^i+1\leqslant a\leqslant 2^{k-1}+2^j+2^i$ 时

$\sigma=\omega(a)+\omega(2^{k-1}-1-(a-2^i-2^j-1))=k-1+\omega(a)-\omega(a-2^i-2^j-1)\leqslant k+2$

令 $x=a-2^i-2^j-1$，则满足条件 $\sigma=k+2$ 的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$对的个数相当于计算方程

$\omega(x+2^i+2^j+1)=\omega(x)+3, 0\leqslant x\leqslant 2^{k-1}-1$

的解数，由引理 3，该方程的解数为 2^{k-4}，从而满足条件 $\sigma=k+2$的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$对共有 2^{k-4}。同理满足条件 $\sigma=k+1$ 的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$对的个数和满足条件 $\sigma=k$ 的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$对的个数相当于分别计算方程

$\omega(x+2^i+2^j+1)=\omega(x)+2, 0\leqslant x\leqslant 2^{k-1}-1$

的解数以及方程

$\omega(x+2^i+2^j+1)=\omega(x)+1, 0\leqslant x\leqslant 2^{k-1}-1$

的解数，这些解数都可以由引理 3 给出。

$\sigma=k+1$ 的情况由引理 3 的 $N_2^{(i,j,l)}$ 的类似计算得出在 $2=i+1=j\leqslant k-3$ 的情形下最少的解数有 2^{k-5}对，其余情形的解数都$\geqslant 2^{k-4}$；

$\sigma=k$ 的情况由引理 3 的 $N_1^{(i,j,l)}$ 的类似计算得出最少解数在 $2=i+1=j=k-3$ 时有 2^{k-4}对，在 $2=i+1=j\leqslant k-4$ 时有 $2^{k-5}+2^{k-6}$对，其余情形的解数都$\geqslant 2^{k-4}$。

如果 $a>t$，根据 $a+b\equiv t(\mathrm{mod}\ 2^k-1)$，这时设：

$a=t+v, b=2^k-1-v, v=1,2,\cdots,2^k-t-2$

并令$\sum=\omega(2^i+2^j+2^{k-1}+v)+k-\omega(v)\leqslant k+3$。

同样可以分 4 种情况讨论：

① 当$\sum=k+3$ 时，$v_i=0, v_j=0, v_{k-1}=0$，等价于计算 $\omega(2^i+2^j+2^{k-1}+v)=\omega(v)+3\Leftrightarrow\omega(2^i+2^j+v)=\omega(v)+2, 1\leqslant v\leqslant 2^{k-1}-1-2^i-2^j-1$。由引理 6 可得满足条件 $\Sigma=k+3$ 的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$小于或等于 $2^{k-3}-2$ 对；

② 当$\sum=k+2$ 时，

$\omega(v+2^j+2^i+2^{k-1})=\omega(v)+2\Leftrightarrow\omega(2^j+2^i+v)=\omega(v)+1, 1\leqslant v\leqslant 2^{k-1}-2-2^i-2^j$

经分析并利用引理 3 得到满足条件 $\Sigma=k+2$ 的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$对的个数为：

$$\begin{cases}2^{k-3}, & i+2<j+1<k-1\\ 2^{k-4}, & i+2=j+1<k-1\\ 2^{k-4}, & i+2<j+1=k-1\\ 0, & i+2=j+1=k-1\end{cases}$$

③ 当$\sum=k+1$ 时，

$\omega(v+2^j+2^i+2^{k-1})=\omega(v)+1\Leftrightarrow\omega(v+2^j+2^i)=\omega(v), 1\leqslant v\leqslant 2^{k-1}-2-2^i-2^j$

经计算和分析得到满足条件 $\Sigma=k+1$ 的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$对的个数为：

$$\begin{cases}2^{k-3}, & i+4<j+2<k-1\\ 2^{k-4}, & i+4=j+2<k-1\\ 2^{k-4}+2^{k-5}, & i+3=j+2<k-1\\ 2^{k-4}, & i+4<j+2=k-1\\ 2^{k-5}, & i+4=j+2=k-1\\ 2^{k-4}, & i+3=j+2=k-1\\ 2^{k-5}, & i+3<j+1=k-1\\ 0, & i+3=j+1=k-1\\ 0, & i+2=j+1=k-1\end{cases}$$

④ 当$\sum=k$ 时，

$\omega(v+2^j+2^i+2^{k-1})=\omega(v)\Leftrightarrow\omega(v+2^j+2^i)=\omega(v)-1, 1\leqslant v\leqslant 2^{k-1}-2-2^i-2^j$

由引理 2 计算和分析得到满足条件 $\Sigma=k$ 的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$对的个数为：

$$\begin{cases}2^{k-6}-2^i, & i+3<j\leqslant k-2\\ 2^{k-6}, & i+3<j+3\leqslant k-2\\ 2^{k-6}, & i+3<j+1\leqslant k-2\\ 2^{k-6}, & i+3<j+2\leqslant k-2\end{cases}$$

于是当 $i+2=j+1=l=k-1$ 时，满足条件 $\Sigma=k$ 的$(a,b)\in Z_{2^k-1}\times Z_{2^k-1}$的个数为 0。

经比较和归纳发现，在 $i+2=j+1=k-1$ 且$(i>2)$这个情形下Σ和 σ 的总个数最少，因而

$\#\{(a,b)\mid\Sigma\geqslant k,\sigma\geqslant k\}_{\min}\geqslant 2^{k-4}+2^{k-4}+2^{k-4}+2^{k-5}+2^{k-4}+2^{k-4}+2^{k-5}+2^{k-4}+2^{k-5}+2^{k-3}-2=2^{k-1}+2^{k-4}+2^{k-5}-1$

所以当 $k\geqslant 5$ 时，有 $|S_t|\leqslant 2^k-2^{k-1}-2^{k-4}-2^{k-5}+1\leqslant 2^{k-1}$。通过上述讨论，再加上 $k\leqslant 29$ 的情形已被验证，我们完成了对 $\omega(t)=3$ 时涂-邓猜想的证明。

推论 1 当 $\omega(t)=k-3$ 时，猜想也成立。

证明：由引理 6 知，在 $\omega(t)=k-3$ 时，$t=2^k-1-t_1, \omega(t_1)=3$，只需证明 $\#\{(a,b)\mid a+b\equiv t_1\ \mathrm{mod}\ 2^k-1, \Sigma\geqslant k+1, \sigma\geqslant k+1\}\leqslant 2^{k-1}$。从定理 1 的证明以及比较和归纳发现：

$$\begin{aligned}&\#\{(a,b)\mid\Sigma\geqslant k+1,\sigma\geqslant k+1\}_{\max}\\ &\leqslant 2^{k-3}-1+2^{k-4}+2^{k-4}+2^{k-4}+2^{k-4}+2^{k-3}\\ &\leqslant 2^{k-1}-1\end{aligned}$$

结束语 基于涂-邓猜想构造出的一系列布尔函数都具有很好的密码学性质，若能成功证明该猜想无疑是非常有意义的。本文基于文献[2]中的引理和方法，通过分析涂-邓猜想中参数 t 满足 $wt(t)=3$ 情形时的二元 Hamming 重量的特性，给出了涂-邓猜想在 $wt(t)=3$ 情形及 $wt(t)=k-3$ 情形下的证明。但是，本文的证明方法不能推广到 $wt(t)$取其他整数值的情形，因此，尝试给出 $wt(t)$取一般整数值的证明是我们下一步研究的重点。

参 考 文 献

[1] Carlet C. A method of construction of balanced functions with optimum algebraic immunity. http://eprint.iacr.org/2006/149

[2] Carlet C, Dalai D K, Gupta KC, et al. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction[J]. IEEE Transactions on Information Theory, 2006, 52: 3105-3121

(下转第 17 页)

量链表前先保存调用者的变量链表，被调用函数执行完成后要恢复调用者的变量链表。

3 基于 SDLSCA 的 AES 算法的描述

下面以 AES 算法为例，给出库函数、用户自定义函数在算法描述中的灵活性和简洁性。根据 AES 算法结构特点，在算法描述中首先用户自定义了字节代替、行移位和轮密钥加等函数，在描述上述用户自定义函数时，调用了 S 变换等库函数。在随后算法加解密主过程中，直接调用这些用户自定义函数和系统自带的库函数。下面仅以字节代替函数为例说明函数在算法描述中的地位和作用。

字节代替函数的定义：

```
/function SubstituteBytes(0)(&State(128))
  (s00(8) || s10(8) || s20(8) || s30(8) || s01(8) || s11(8) || s21(8) || s31(8) || s02(8) || s12(8) || s22(8) || s32(8) || s03(8) || s13(8) || s23(8) || s33(8))=State(128);
  s00(8)=substitute(8,8){S}(s00(8));//S 变换，S 为 AES 算法中的 S 盒，substitute 为库函数
  ……
  s33(8)=substitute(8,8){S}(s33(8));
  State(128)=(s00(8) || s10(8) || s20(8) || s30(8) || s01(8) || s11(8) || s21(8) || s31(8) || s02(8) || s12(8) || s22(8) || s32(8) || s03(8) || s13(8) || s23(8) || s33(8));
\function
```

在 AES 加密主过程中直接调用字节代替函数。

```
//AES 加密主过程循环部分
/loop(s=1;step=1)=9
  RoundKey=Rkey[s * 4] || Rkey[s * 4+1] || Rkey[s * 4+2] || Rkey[s * 4+3];
  function SubstituteBytes(&State);//字节代替
  function ShiftRow(&State);//行移位
  function MixColumn(&State);//列混淆，该函数为库函数
  function AddRoundKey(&State,RoundKey);//轮密钥加，该函数为用户自定义函数
\loop
```

应用函数的功能描述 AES 算法仅需 111 行代码，而在 AES 征集时提交的 C 语言代码则需要 300 多行。同时应用函数的功能描述其他密码算法，与其公开的 C 语言代码进行比较，代码的行数都大大减少。实践证明，运用函数的功能可大大减少算法描述的代码行数，提高算法描述的准确性。

结束语 本文在分析密码算法设计特点的基础上，运用模块化的思想，设计并实现了 SDLSCA 函数的功能。最后以 AES 为例，利用库函数和用户自定义函数进行算法描述，把加密结果和公开的测试向量进行对比，进而验证密码算法描述的正确性。同时与利用函数功能之前描述的算法进行了对比，结果表明，应用函数功能可以大大简化算法的描述，提高算法描述的效率和利用率，为 SDLSCA 推广应用打下了坚实的理论和实际基础。

参 考 文 献

[1] 李凤华，阎军智，谢绒娜，等. 面向分组密码算法的程序. 设计语言[J]. 电子学报，2009，37(12)：2705-2710

[2] Li Feng-hua, Yan Jun-zhi, Xie Rong-na, et al. Research on the Programming Language forSymmetric Cryptographic Algorithms[J]. Chinese Journal of Electronics, 2010, 19(2): 303-306

[3] 吴文玲，冯登国，张文涛. 分组密码的设计与分析[M]. 北京：清华大学出版社，2009：8-13

[4] Knudsen L R. Block Ciphers-a survey [J]. LNCS, 1998, 1582: 18-48

[5] Knudsen L R. Block ciphers-analysis, design and applications [D]. DAIMI PB 485, Aarhus University, Denmark, 1994

[6] Adams C, Tavares S. The structured design of cryptographically good s-boxes [J]. Journal of Cryptology, 1990, 3(1): 27-41

[7] 金晨辉，孙莹. AES 密码算法 S 盒的线性冗余研究[J]. 电子学报，2004，32(4)：639-641

[8] NIST. Advanced Encryption Standard (AES), FIPS-Pub 197 [S]. National Bureau of Standards, 2001

[9] Biryukov A. Block Ciphers and Stream Ciphers: The State of the Art [EB/OL]. http://eprint.iacr.org/2004/094.pdf, 2004

[10] Terence P. An introduction to ANTLR [EB/OL]. http://www.cs.usfca.edu/~parrt/course/652/lectures/ANTLR.html

[11] Rod C, Paul H. Create Domain Specific Languages with ANTLR [EB/OL]. http://www.devx.com /semantic/Articel/35973?trk=DXRSS_JAVA, 2007

(上接第 8 页)

[3] Carlet C, Feng K. An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity[C]// Advances in Cryptology-ASIACRYPT 2008, LNCS 5350. Springer, Heidelberg, 2008: 425-440

[4] Dalai D K, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity [J]. Des. Codes, Cryptography, 2006, 40(1): 41-58

[5] Li N, Qi W. Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity[C]// Advances in Cryptology-Asiacrypt 2006, LNCS 4284. Springer, Heidelberg, 2006: 84-98

[6] Tu Z R, Deng Y P. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity[J]. Des. Codes Cryptogr., 2011, 60: 1-14

[7] Cusick T W, Li Yuan, Stanica P. On a combinatoric conjecture. Cryptology ePrint Archive, Report 2009/554[EB/OL]. http://eprint.iacr.org/, 2009

[8] Tang X H, Tang D, Zeng X, et al. Balanced Boolean Functions with (Almost) Optimal Algebraic Immunity and Very High Nonlinearity, Cryptology ePrint Archive[R]. Report 2010/443, 2010. http://eprint.iacr.org/

[9] Dillon J F. Elementary Hadamard Difference Sets [D]. University of Maryland, 1974

[10] Du Yu-song, Zhang Fang-guo. A note on the Tu-Deng function [C]// Cchinacrypt2011. 2011: 59-63

[11] Cohen G, Flori J-P. On a generalized combinatorial conjecture involving addition mod 2^k-1[OL]. http://eprint.iacr.org/2011/400.pdf