一类特殊布尔函数的代数免疫度研究

欧海文[1]，张玉娟[1,2]
（1. 北京电子科技学院，北京 100070；2. 西安电子科技大学 通信工程学院，西安 710071）

摘　要：构造具有好的代数免疫度的布尔函数是布尔函数研究的重要问题之一。基于布尔函数的级联构造方法，给出了一类具有好的代数免疫度的布尔函数；分析了所构造函数的性质，证明了构造布尔函数 h_{n+1} 与其子函数代数免疫度之间的关系，并确定了已构造一阶级联函数的代数次数、平衡性以及非线性度。研究结果表明，在级联构造方法下，i 次级联构造函数比一阶构造 H^0 的代数免疫度有显著提高。

关键词：布尔函数；代数免疫度；级联；子函数；非线性度
中图分类号：TN918　　**文献标志码**：A　　**文章编号**：1001-3695(2012)02-0637-03
doi:10.3969/j.issn.1001-3695.2012.02.062

On algebraic immunity of a class of special Boolean functions

OU Hai-wen[1], ZHANG Yu-juan[1,2]
(1. *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*; 2. *Institute of Telecommunication Engineering*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Constructing Boolean functions with good cryptographic characteristics is an interesting and significant problem in study of Boolean functions. Based on the properties of concatenation, this paper presented a class of Boolean functions with optimal algebraic immunity. It also showed the relation of algebraic immunity between the constructed function h_{n+1} and its element functions. Moreover, ascertained some other cryptographic properties, such as algebraic degree, balance, and nonlinearity of the constructed function. Finally, under the concatenation, this paper concludes that the algebraic immunity of *i*th-constructed function has improved significantly compared that of first order construction function H^0.

Key words: Boolean function; algebraic immunity; concatenation; element functions; nonlinearity

密码技术的关键问题之一是布尔函数的研究。布尔函数是构造密码算法的重要组件。代数攻击的提出和发展被认为是近年来密码分析技术最重要的突破之一。为了使密码体制能够有效地抵抗代数攻击，一个必要条件就是要求密码体制中所使用的布尔函数的代数免疫阶比较大，最好能达到最大。代数免疫度是评判布尔函数安全性的一个重要指标，它被用于衡量布尔函数抵抗代数攻击的能力，n 元布尔函数的最大代数免疫阶为$\lceil n/2 \rceil$[1]。因而，构造具有最大代数免疫度的布尔函数是布尔函数研究的一个重要问题。进一步研究代数免疫度与其他密码函数性质之间的关系，对于提高布尔函数抵抗各种已知攻击的能力具有重要的意义。

本文首先分析了级联构造函数的性质，并给出了其代数免疫度的性质；然后基于级联构造方法，给出了一类具有较好代数免疫度的布尔函数，并分析了所构造函数的代数次数、平衡性及非线性度等性质；最后分析了 i 阶级联函数的情形，研究了其代数次数及代数免疫度等性质，研究结果表明，通过多次级联构造的函数其代数免疫度能有较大的提高。

1　预备知识

定义 1[2]　n 元布尔函数 $f(x)$ 定义为一个从 F_2^n 到 F_2 的映射，其中，$x=(x_1,x_2,\cdots,x_n)\in F_2$，$f\in F_2$。用 B_n 表示所有 n 元布尔函数的集合。常数项为 0 的一次函数称为线性函数，用 L_n 表示线性函数的集合。

布尔函数常通过其真值表来表示。真值表完全由输入矢量的全部序列决定，左列列出 x 的值，右列为相应的函数值。故可将真值表唯一地表示为长度为 2^n 的二进制字符串：

$$\tau_f=f(a_0)f(a_1)\cdots f(a_{2^n-1})$$

称为布尔函数 f 的函数值向量。其中，a_i，$1\leqslant i\leqslant 2^n-1$ 是按字典序大小排列的 F_2^n 中的向量。

定义 2[2]　一个布尔函数 f 的非线性度定义为

$$N_f=\min_{l(x)\in L_n}|\{x\in F_2^n|f(x)\neq l(x)\}|$$

定义 3[1]　设 $f,g\in B_n$，若 $f\cdot g=0$，那么称 g 为 f 的零化子。记 f 的零化子集合为 $AN_n(f)$。

定义 4[1]　若 $f\in B_n$，g 为 f 或 $f+1$ 的非零零化子中次数最小的，则称 g 的次数为 f 的代数免疫度，记为 $AI_n(f)$。

由于对 $\forall f\in B_n$，$AI_n(f)\leqslant\lceil n/2\rceil$[1]，因此一个 n 元布尔函数的代数免疫不大于$\lceil n/2\rceil$，称达到这一上界的布尔函数为具有最优代数免疫度的布尔函数，记为 MAI 函数。

定义 5　若 h_{n+1} 的函数值向量可以表示成 f 和 g 函数值向量的有序连接，记 $h=g\|f$，其中 $f\in B_n$，$g\in B_n$，且 g 和 f 称做 h_{n+1} 的子函数，将 h_{n+1} 称为 f 和 g 的级联。

由级联的定义可知，可以通过两个偶数元布尔函数构造一个奇数元布尔函数，同样可以用两个奇数元布尔函数构造一个偶数元布尔函数，即一对 n 元布尔函数 $f_1,f_2\in B_n$ 可以构造一

收稿日期：2011-06-21；**修回日期**：2011-08-11

作者简介：欧海文(1963-)，男，北京人，教授，硕导，博士，主要研究方向为密码编码与密码应用技术等；张玉娟(1987-)，女，硕士研究生，主要研究方向为密码算法及布尔函数、信息安全等(zhangyujuan1216@163.com)。

个 $n+1$ 元布尔函数，$f_1 \| f_2 = f \in B_{n+1}$；同样，一个 $n+1$ 元布尔函数可以分解成两个 n 元布尔函数 $f = f_1 \| f_2$，其中 $f_1, f_2 \in B_n$。

2 两类 MAI 函数的构造

以下基于级联构造方法构造两种 MAI 函数。级联构造方法是一种获得好的密码函数性质的重要方法。构造函数为 MAI 函数的关键问题是分析其子函数所具有的性质。以下的命题为本文提供了构造的基础。

命题 1 给定 $g, f \in B_n$，若 $h = g \| f$，则以下命题成立：

a) $h \in B_{n+1}$ 且 $h = (x_{n+1}+1)g + x_{n+1}f = g + x_{n+1}(g+f)$。

b) $\deg(h) \geqslant \deg(f)$。

证明 对 a)，由连接的有序性可得，令 $x_{n+1}=0$ 时，$h(x_1, \cdots, x_n, 0) = g(x_1, \cdots, x_n)$；$x_{n+1}=1$ 时，$h(x_1, \cdots, x_n, 1) = f(x_1, \cdots, x_n)$，故 $h = (x_{n+1}+1)g + x_{n+1}f$。

由 a) 的结果易得 b)，证毕。

命题 1 给出了级联构造的具体形式，为本文工作的基础。

命题 2 给定 $g, f \in B_n$，若 $h = g \| f$，则以下命题成立：

a) 若 g 和 f 都是平衡的，则 h 是平衡的；反之不然。

b) $h = g \| f \Leftrightarrow h+1 = (g+1) \| (f+1)$。

c) $\deg(h) = \deg(g+f)+1\}$。

事实上，由于 $h = g + x_{n+1}(g+f)$，且 g 中不存在含有 x_{n+1} 的项，则有 $\deg(h) \geqslant \deg(g)$ 且 $\deg(h) \geqslant \deg(g+f)+1$，所以对于 $h = g \| f$，下式成立：

$$\deg(h) = \begin{cases} \deg(g)+1 & \deg(h) > \deg(g) \\ \deg(f)+1 & \deg(h) < \deg(g) \\ \deg(g)+1 & \deg(g) = \deg(f) = \deg(g+f) \\ \deg(g) & \deg(g) = \deg(f) > \deg(g+f) \end{cases} \tag{1}$$

定理 1 给定 $g, g', f, f' \in B_n$，设 $h = g \| f, h' = g' \| f'$，则 $h' \in AN(h)$，当且仅当 $g' \in AN(g)$ 且 $f' \in AN(f)$。

事实上，定理 1 给出了通过子函数的零化子构造级联函数零化子的具体方法，为分析级联函数与其子函数代数免疫度的关系做好了准备。

以下为方便讨论，用 LDAN(f) 表示使得 $f \cdot f_1 = 0$ 或者 $(f+1) \cdot f_1 = 0$ 成立的代数次数最低的 f_1 所组成的集合。

定理 2 设 g, f 为关于变元 $x_1, x_2, \cdots, x_n$ 的 n 元布尔函数，$AI_n(f) = d_1$ 且 $AI_n(g) = d_2$。令 $h = f \| g$，则

a) 若 $d_1 \neq d_2$，则 $AI_{n+1}(h) = \min\{d_1, d_2\} + 1$。

b) 给定 $d_1 = d_2 = d$，有 $d \leqslant AI_{n+1}(h) \leqslant d+1$，

进一步，$AI_{n+1}(h) = d$，当且仅当存在次数为 d 的 $g_1, f_1 \in B_n$，使得 $\{f \cdot f_1 = 0, g \cdot g_1 = 0\}$ 或者 $\{(1+f) \cdot f_1 = 0, (1+g) \cdot g_1 = 0\}$ 且 $\deg(f_1 + g_1) \leqslant d-1$。

证明 令 $f_1 \in \text{LDAN}(f)$ 且 $g_1 \in \text{LDAN}(g)$，则不论是 $f \cdot f_1 = 0$ 使得 $(1+x_{n+1}) \cdot f_1 \cdot h = 0$ 或是 $(1+f) \cdot f_1 = 0$ 使得 $(1+x_{n+1}) \cdot (1+f_1) \cdot h = 0$；不论是 $g \cdot g_1 = 0$ 使得 $(1+x_{n+1}) \cdot g_1 \cdot h = 0$，还是 $(1+g) \cdot g_1 = 0$ 使得 $(1+x_{n+1}) \cdot (1+g_1) \cdot h = 0$。由此可以得出

$$AI_{n+1}(h) \leqslant \min\{AI_n(f), AI_n(g)\} + 1 \tag{2}$$

令 $p = p_1 \| p_2 \in \text{LDAN}(h)$，先考虑 $h \cdot p = 0$ 的情形，由 $h = (1+x_{n+1})f + x_{n+1}g$，$p = (1+x_{n+1})p_1 + x_{n+1}p_2$ 且 $h \cdot p = 0$，展开可得 $(1+x_{n+1})f \cdot p_1 + x_{n+1}g \cdot p_2 = 0$，所以有 $f \cdot p_1$ 且 $g \cdot p_2 = 0$。类似地，对于 $(1+h) \cdot p = 0$ 的情形，由 $(1+h) \cdot p = 0$ 可得 $(1+x_{n+1})(1+f) \cdot p_1 + x_{n+1}(1+g) \cdot p_2 = 0$，所以有 $(1+f) \cdot p_1 = 0$ 且 $(1+g) \cdot p_2 = 0$。

通过分析，上述两种情况均可以归结为以下三种情形：

a) $p_1 = 0$，但 $p_2 \neq 0$，则由 $AI_n(g) = d_2$ 得 $\deg(p_2) \geqslant d_2$，所以由式(1)：$\deg(p) \geqslant d_2 + 1$。

b) $p_2 = 0$ 但 $p_1 \neq 0$，则由 $AI_n(f) = d_1$ 得 $\deg(p_1) \geqslant d_1$，所以由式(1)：$\deg(p) \geqslant d_1 + 1$。

c) $p_1 \neq 0$ 且 $p_2 \neq 0$，则 $\deg(p_1) \geqslant d_1$ 且 $\deg(p_2) \geqslant d_2$，所以当 $d_1 \neq d_2$ 时，$\deg(p) \geqslant \max\{d_1, d_2\} + 1$。所以对 $d_1 \neq d_2$，有

$$AI_{n+1}(h) \geqslant \min\{AI_n(f), AI_n(g)\} + 1 \tag{3}$$

由式(2)(3)得定理 2a) 成立，即 $AI_{n+1}(h) = \min\{d_1, d_2\} + 1$。

对于定理 2 的 b)，令 $p = f_1 \| g_1 \in \text{LDAN}(h)$，由于 $d_1 = d_2 = d$ 且 $p = (1+x_{n+1})f_1 + x_{n+1}g_1$，则在 p 中的 $x_{n+1}f_1 + x_{n+1}g_1$ 的最高项可以抵消，所以 p 的次数减小 1。所以 $d \leqslant AI_{n+1}(h) \leqslant d+1$。令 $AI_{n+1}(h) = d$，则 f_1 和 g_1 的最高次项相同，使得 $\deg(f_1 + g_1) \leqslant d-1$。反过来，假设存在次数为 d 的 $g_1, f_1 \in B_n$，使得 $\deg(f_1 + g_1) \leqslant d-1$，且下式之一成立：

$$f \cdot f_1 = 0, g \cdot g_1 = 0 \tag{4}$$

$$(1+f) \cdot f_1 = 0, (1+g) \cdot g_1 = 0 \tag{5}$$

构造 $p = (1+x_{n+1})f_1 + x_{n+1}g_1$，可得 $h \cdot p = 0$，则 $AI_{n+1}(h) = d$。证毕。

定理 2 给出了级联函数与其子函数代数免疫度之间的关系。由结果可知，一阶级联构造函数的代数免疫度并没有显著的提高，要使级联函数的代数免疫度较高，其子函数的代数免疫度不能太低。所以，进一步要考虑 i 阶级联构造下函数的代数免疫度。

由定理 2 的结论，当 n 分别取奇数和偶数时，可以得到具有 MAI 的级联构造函数的几种情况。

命题 3 若 n 为奇数，$f, g \in B_n$ 且 $h_{n+1} = f \| g$，则 $AI_{n+1}(h) = (n+1)/2$，当且仅当 f 和 g 满足以下条件之一：

a) $AI_n(g) = AI_n(f) = \lceil n/2 \rceil$。

b) $AI_n(g) = \lceil n/2 \rceil, AI_n(f) = \lceil n/2 \rceil - 1$。

c) $AI_n(g) = \lceil n/2 \rceil - 1, AI_n(f) = \lceil n/2 \rceil$。

d) $AI_n(g) = AI_n(f) = \lceil n/2 \rceil - 1$，且对任意的 $g' \in AN_n(g)$，$f' \in AN_n(f)$ 或者 $f' \in AN_n(1+f)$，$g' \in AN_n(1+g)$，$\deg(f') = \deg(g') = \lceil n/2 \rceil - 1$ 有 $\deg(f'+g') \leqslant \lceil n/2 \rceil - 1$。

证明 将定理 2 中的 d_1, d_2 分别取条件 a) ~ d) 中的值，即得证。

命题 4 若 n 为偶数，$f, g \in B_n$ 且 $h_{n+1} = f \| g$，则 $AI_{n+1}(h) = \lceil (n+1)/2 \rceil$ 当且仅当：

a) $AI_n(g) = AI_n(f) = \lceil n/2 \rceil$；

b) 对 $\forall g' \in AN_n(g)$，$f' \in AN_n(f)$ 或者 $f' \in AN_n(1+f)$，$g' \in AN_n(1+g)$，$\deg(f') = \deg(g') = \lceil n/2 \rceil$ 有 $\deg(f'+g') = \lceil n/2 \rceil$。

证明 n 为偶数，若 $AI_{n+1}(h) = \lceil (n+1)/2 \rceil = \lceil n/2 \rceil + 1$，则由定理 2 有 $\min\{AI_n(g), AI_n(f)\} = \lceil n/2 \rceil$，即 f 和 g 都有最优 AI，即 $\deg(f'+g') = \lceil n/2 \rceil$ 成立。证毕。

基于以上理论，可以得到两种构造 MAI 函数的方法。

构造 1 已知可通过分解一个 $n+1$ 元布尔函数 h_{n+1} 得到两个 n 元布尔函数 f_n 和 g_n，如 $h_{n+1} = f_n \| g_n$。故由命题 3 和 4 可知，为了获得偶数元具有 MAI 的函数，只需一个具有 MAI 的奇数元函数 h_{n+1}，则分解后的子函数 f 和 g 均为 MAI 布尔函数；同样为了获得具有 MAI 的奇数元函数，只需一个具有 MAI

的偶数元布尔函数 h_{n+1},则子函数 f 和 g 亦具有高的代数免疫度且不低于 $\lceil n/2\rceil-1$。

构造 2　已知可通过级联两个已选的 $n-1$ 元函数 f_{n-1} 和 g_{n-1},如 $f_{n-1}\parallel g_{n-1}=h_n$。故为了获得一个具有 MAI 的偶数元函数 h_n,仅需两个奇数元 f_{n-1} 和 g_{n-1},且满足定理 1 中的条件之一即可。类似地,为了获得一个具有 MAI 的奇数元函数 h_n,仅需两个偶数元 f_{n-1} 和 g_{n-1},且满足定理 2 的条件即可。

与其他构造方法不同,以上两种构造方法不需要详细的计算,复杂度较低。事实上,对于构造 1,从已知的 h_{n+1} 中可容易得到 f_n 和 g_n,即

$$g_n=g(x_1,x_2,\cdots,x_n)=h(x_1,x_2,\cdots,x_n,0)$$
$$f_n=h(x_1,x_2,\cdots,x_n,1)$$

对于构造 2,可以从 f_{n-1} 和 g_{n-1} 容易得出 $h_n=(1+x_{n+1})g+x_{n+1}f$。由此可知,通过构造 1 可从一个给定的布尔函数中得到两个函数,而构造 2 可以从两个给定的函数中得到一个布尔函数。

下面讨论通过以上两种构造方法所得函数的代数次数、平衡性和非线性性。

1)代数次数

对 $h=f\parallel g$,由式(1)得

$$\deg(h)=\begin{cases}\max & \deg(g)=\deg(f)>\deg(g+f)\\ \max+1 & \text{else}\end{cases}$$

其中:$\max=\max\{\deg(g),\deg(f)\}$。

上式说明通过选择高代数次数的 f 和 g 可以保证构造函数的代数次数较高。

2)平衡性

由命题 2 得,若奇数元函数 $h\in B_n$ 达到最大代数免疫度,则 h 为平衡的。通过构造 1 生成的偶数元函数 f 和 g,由于 h 为 MAI 函数,则 h 为平衡的,则若 f 和 g 其中之一平衡,另一个也平衡。通过构造 2 生成的奇数元函数 h,由命题 2,若 f 和 g 平衡,则 h 为平衡的,故选择两个平衡函数来生成 h 是较好的。事实上,若 f 和 g 为 MAI 函数,又为奇数元函数,则 f 和 g 必然平衡。

3)非线性性

若 $h\in B_n$,则 h 的非线性度上界为 $2^{n-1}-2^{\frac{n}{2}-1}$,即 $N_f\leqslant 2^{n-1}-2^{\frac{n}{2}-1}$ 成立。进一步,还有更好的结论:

推论 2[3]　设 $h\in B_{n+1}$ 且 $AI(h)=\lceil(n+1)/2\rceil$,则

a)当 n 为奇数时,$N_h\geqslant 2^n-\binom{n+1}{(n+1)/2}-\binom{n+1}{(n+1)/2-1}$。

b)当 n 为偶数时,$N_h\geqslant 2^n-\binom{n}{n/2}$。

由此可见,一个具有 MAI 的函数可以保证其非线性度很高。

3　i 阶级联函数

在定理 2 中,一阶级联函数相比其子函数代数免疫度并没有显著的提高,为使级联函数的代数免疫度较高,所选取的子函数代数免疫度不能太低。所以,为了得到更好的结果,考虑 i 阶级联构造函数。

假设 $f=f_1\parallel f_2$,令 $F=x_{n+2}+x_{n+1}+f$,$G=x_{n+2}+x_n+(1+x_{n+2}+x_{n+1})f_1+(x_{n+2}+x_{n+1})f$,设 $H=(1+x_{n+3})F+x_{n+3}G$,以下通过此方法构造 i 阶级联函数。

令 H^0 为 n 元初始函数,H^i 为经过上述 i 次变换之后的函数,记 $H^{i\prime}$ 为将 H^i 中变量 x_{n+3i} 用 $(x_{n+3i+2}+x_{n+3i+1})$ 代替所得。令 $F^{i+1}=x_{n+3i+2}+x_{n+3i+1}+H^i$,$G^{i+1}=x_{n+3i+2}+x_{n+3i}+H^{i\prime}$,则 $H^{i+1}=(1+x_{n+3i+3})F^{i+1}+x_{n+3i+3}G^{i+1}$。

命题 5[3]　对 $i>0$,$H^i=(1+Y_i)H^0+Y_iH^{0\prime}+Z_i$,其中:$\deg(Y_i)=i$ 且 $\deg(Z_i)=i+1$。

下面通过讨论 H^0 的代数免疫度来研究 H^i 的代数免疫度。

定理 5　$AI_n(H^0)\leqslant AI_{n+3i}(H^i)\leqslant AI_n(H^0)+i+2$。

证明　为了证明 $AI_n(H^0)\leqslant AI_{n+3i}(H^i)$,只需证明 $AI_n(H^0)\leqslant AI_{n+3}(H^1)$,因为

$$H^1=(1+x_{n+3})F^1+x_{n+3}G^1$$

其中:$F^1=x_{n+2}+x_{n+1}+H^0$,$G^1=x_{n+2}+x_n+H^{0\prime}$。

令 $AI_n(H^0)=d$,所以 $AI_n(H^{0\prime})=d$。由命题 2、3 得 $AI_{n+2}(G^1)\geqslant d-1$,又由命题 1 得 $AI_{n+3}(H^1)\geqslant d$。

下面证明上界,由命题 3 得

$$H^i=(1+Y_i)H^0+Y_iH^{0\prime}+Z_i$$

其中:$\deg(Y_i)=i$ 且 $\deg(Z_i)=i+1$。令 $AI_n(H^0)=d$,则可假设存在一个多项式 g^0,$\deg(g^0)=d$,使得 $H^0\cdot g^0=0$ 或者 $(1+H^0)\cdot g^0=0$;令 $H^0=p+q\cdot x_n$,其中 p,q 均为与 x_n 无关的 $n-1$ 元布尔函数,则

$$(1+Y_i)H^0+Y_iH^{0\prime}=Y_i\cdot q\cdot(x_n+x_{n+1}+x_{n+2})+p+q\cdot x_n=Y_i\cdot q\cdot(x_n+x_{n+1}+x_{n+2})+H^0$$

构造函数 $U=g^0\cdot(1+Z_i)\cdot(1+x_n+x_{n+1}+x_{n+2})$,其次数至多为 $d+i+2$,则若 $H^0\cdot g^0=0$,有

$$H^i\cdot U=((1+Y_i)H^0+Y_iH^{0\prime}+Z_i)\cdot U=((1+Y_i)H^0+Y_iH^{0\prime}+Z_i)\cdot(g^0\cdot(1+Z_i)\cdot(1+x_n+x_{n+1}+x_{n+2}))=0$$

同样地,对于 $(1+H^0)\cdot g^0=0$,有 $(1+H^i)\cdot U=0$,那么 $AI_{n+3i}(H^i)\leqslant AI_n(H^0)+i+2$。证毕。

定理 5 说明,通过 i 阶级联构造所得的 $n+3i$ 元函数的代数次数和 AI 都明显提高,对于布尔函数中代数免疫度的研究很有意义。

4　结束语

本文通过对布尔函数的级联构造方法的研究,给出了一阶级联构造下两类 MAI 布尔函数的构造方法,并分析了所构造函数 h_{n+1} 的性质,给出了构造布尔函数 h_{n+1} 与其子函数代数免疫度之间的关系。由研究结果可知,一阶级联构造函数的代数免疫度相对其子函数有所提高,但并没有显著的提高。随后对已构造函数的代数次数、平衡性以及非线性度进行了分析,得出在适当选取子函数的情况下,级联构造函数的平衡性是比较好的,而且其代数次数和代数免疫度都相对较高。由于一阶级联函数的代数免疫度没有显著提高,所以进一步考虑了 i 阶级联构造下函数的代数免疫度,得出 i 阶级联函数的代数免疫度下界相对于一阶级联函数 H^0 显著提高,这一结果对密码分析具有一定的作用。

参考文献:

[1]　董新锋,张凤荣. 具有最优代数免疫阶的 i 阶弹性函数的构造[J]. 信息安全与通信保密, 2010(12):112-115.

[2]　万鑫. 布尔函数的代数免疫性研究[D]. 西安:西安电子科技大学,2009.

(下转第 643 页)

$ID_b^{*'}$ 进行公钥提取询问获得其公钥 $P_b^{*'}$,随机选取 $r^{*'}$、$t^{*'}$,计算 $k_1^{*'}=r^{*'}\cdot P_b^{*'}$,检查表 L_2 表中是否已经存在($k_1^{*'}$,$m\theta$,$k_3^{*'}$),若已经存在,则重新选取 $r^{*'}$,直到($k_1^{*'}$,m_θ)在表 L_2 中的项中的前两个元素都没有出现过为止。计算 $k_3^{*'}=H_2(k_1^{*'},m_\theta)$,随机选取 $\omega^{*'}=h^*$,计算 $k_2^{*'}=H_3(\omega^{*'})$,计算签密密文 $\sigma^{*'}=E_{k_2}^{*'}(t^{*'}\|m\|k_3^{*'})$,返回 $\sigma^{*'}$ 给 $Adv_{Ⅱ}$ 作为挑战密文。

$Adv_{Ⅱ}$ 继续进行经过多项式有界次询问,并在模拟结束时输出 θ' 作为 θ 的猜测,若 $\theta'=\theta$,D 输出一个值为 BDH 问题的答案;否则,D 没有解决 BDH 问题。若 $Adv_{Ⅱ}$ 没有选择 ID_η,对 k_1、ω 执行了 H_2、H_3 询问,或在解签密询问中拒绝了一个合法的密文则 D 失败。因此,D 至少以 $\varepsilon'\geq[\varepsilon/(q_{H_1}\cdot q_{H_2}\cdot q_{H_3})]\cdot(1-q_u/2^k)$ 的优势解决 BDH 问题。

3.1.2　不可伪造性

定理 3　类型Ⅰ攻击下的不可伪造性。在随机预言机模型中,若存在一个 EUF-CLSC-CMA 敌手 $Adv_Ⅰ$ 能够在多项式有限时间内,以 ε 的优势赢得文献[9]3.2.2 节中定义的游戏 Game EUF-CMA-Ⅰ,则存在一个区分者 D,能够在多项式有限时间内以 $\varepsilon'\geq[(\varepsilon/(q_{H_1}\cdot q_{H_3})]$ 的优势解决 CDH 问题。

证明　区分者 D 接收一个随机的 CDH 问题实例(P,aP,bP),目标是计算 abP。在这里,$a,b\in Z_q^*$ 是未知整数。D 将 $Adv_Ⅰ$ 作为子程序并扮演 EUF-CLSC-CMA 游戏中的挑战者 C。其他的初始化过程参见定理 1。

在多项式有界的时间范围内,攻击者 $Adv_Ⅰ$ 可以进行定理 1 中的询问。若 $ID_a\neq ID_\eta$ 则终止模拟;否则,$Adv_Ⅰ$ 随机选取 $z'_a,s'\in Z_q^*$ 计算 $s'_a=z'_a\cdot s'\cdot h_1$,最后 $Adv_Ⅰ$ 输出一个合法的从 ID_a 到 ID_b 的伪造签密密文 $\sigma'=\text{signcrypt}(s'_a,P_b,m)$。其中 D 知道被替换的公钥,若伪造成功,则 D 解决了 CDH 问题;否则 D 没有解决 CDH 问题。若 $Adv_Ⅰ$ 没有选择 ID_η 或对 ω 执行 H_3 询问则 D 失败。因此 D 至少以 $\varepsilon'\geq[\varepsilon/(q_{H_1}\cdot q_{H_3})]$ 的优势解决 CDH 问题。

定理 4　类型Ⅱ攻击下的不可伪造性。在随机预言机模型中,若存在一个 EUF-CLSC-CMA 敌手 $Adv_{Ⅱ}$ 能够在多项式有限时间内,以 ε 的优势赢得文献[9]3.2.2 节中定义的游戏 Game EUF-CMA-Ⅱ,则存在一个区分者 D,能够在多项式有限时间内以 $\varepsilon'\geq[(\varepsilon/(q_{H_1}^2\cdot q_{H_3})]$ 的优势解决 CDH 问题。

证明　区分者 D 接收一个随机的 CDH 问题实例将 $Adv_{Ⅱ}$ 作为子程序并扮演 EUF-CLSC-CMA 游戏中的挑战者 C。其他的初始化过程参见定理 1。

在多项式有界的时间范围内,攻击者 $Adv_{Ⅱ}$ 可以进行定理 2 中的询问。若 $ID_a\neq ID_\eta$ 则终止模拟;否则,在经过多项式有界次的定理 2 中所述的询问后,$Adv_{Ⅱ}$ 随机选取 $z_a^*,r^*\in Z_q^*$ 计算 $k_1^*=r^*\cdot P_b$,$k_3^*=H_2(k_1^*,m)$,$s_a^*=z_a^*\cdot W_a$。计算对 m 的有效伪造签密密文 $\sigma^*=\text{signcrypt}(s_a^*,P_b,m)$。其中 D 知道系统主密钥,若伪造成功,则 D 成功解决 CDH 问题;否则 D 没能解决 CDH 问题。若 $Adv_{Ⅱ}$ 没有选择 ID_η、没有对 ID_η 执行过私钥询问或对 ω 执行了 H_3 询问则 D 失败。因此 D 至少以 $\varepsilon'\geq[\varepsilon/(q_{H_1}^2\cdot q_{H_3})]$ 的优势解决 CDH 问题。

3.2　认证方案的效率分析

与文献[4]相比,本文的方案在效率方面有所提高。具体的差别如表 1 所示。

表 1　认证方案的效率比较

认证方法	t_{ma}	t_{la}	t_{ml}	LMA 与 MAG 认证	共享密钥
文献[4]	2	2	0	否	是
本文	1	0	1	是	否

其中:t_{ma} 表示 MAG 与 LMA 之间的交互次数;t_{la} 表示 LMA 与 AAA 之间的交互次数;t_{ml} 表示 MAG 与 LMA 之间的交互次数。此外,本文的方案还保持了较低的计算量,在签密阶段只需花费 2 次点乘运算和 1 次双线性对预运算,在解签密阶段也只需花费 1 次点乘运算和 1 次双线性对预运算。

4　结束语

本文基于无证书签密的特点,结合代理移动 IPv6 的实际环境提出了一种基于无证书签密的 PMIPv6 认证方案,然后对该方案的安全性进行了形式化分析。结果表明该方案在随机预言机模型下是可证明安全的。最后对该方案的效率分析表明:该认证方案减少了节点之间的交互,不需要花费额外的开销来管理密钥,保持了较小的计算量。

参考文献:

[1] JOHNSON D, PERKINS C, ARKKO J. RFC 3775, mobility support in IPv6[S]. [S.l.]: IETF, 2004.

[2] KONG K S, LEE W J. Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6[J]. IEEE Wireless Communications, 2008, 15(2): 36-45.

[3] GUNDAVELLI S, LEUNG K, DEVARAPALLI V, *et al*. RFC 5213, proxy mobile IPv6[S]. [S.l.]: IETF. 2008.

[4] 周华春,张宏科,秦雅娟. 一种代理移动 IPv6 认证协议[J]. 电子学报, 2008, 36(10): 1873-1880.

[5] ERONEN P, HILLER T, ZORN G. RFC 4072, diameter extensible authentication protocol (EAP) application[S]. [S.l.]: IETF, 2005.

[6] ABOBA B, BLUNK L, VOLLBRECHT J, *et al*. RFC 3748, extensible authentication protocol (EAP)[S]. 2004.

[7] BARBOSA M, PARSHIM F. Certificateless signcryption [EB/OL]. (2008). http://eprint.iacr.org/2008/143.

[8] WU Chen-huang, CHEN Zhi-xiong. A new efficient certificateless signcryption scheme[J]. Information Science and Engineering, 2008, 12(30): 661-664.

[9] 谢文贤,张彰. 无证书签密的研究[D]. 南宁:广西民族大学, 2010.

(上接第 639 页)

[3] SONG Shou-chao, ZHANG Jie, DU Jiao, *et al*. On the construction of Boolean functions with optimal algebraic immunity and good other properties by concatenation[C]//Proc of IEEE International Conference on Progress in Informatics and Computing (PIC). [S.l.]: IEEE, 2010: 417-422.

[4] MEIER W, PASALIC E, CLAUDE C. Algebraic attacks and decomposition of Boolean functions[C]//LNCS, vol 3027. Berlin: Springer-Verlag, 2004: 474-491.

[5] DALAI O K, GUPTA K C, MAITRA S. Results on algebraic immunity for cryptographically significant Boolean functions[C]//LNCS, vol 3348. Berlin: Springer-Verlag, 2004: 92-106.

[6] CARLET C, DALAI D K, GUPTA K C. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction [J]. IEEE Trans on Information Theory, 2006, IT-52(7): 3105-3121.

[7] LOBANOV M. Tight bound between nonlinearity and algebraic immunity[EB/OL]. (2005). http://eprint.iacr.org/2005/441.