基于无证书签密的代理移动 IPv6 认证方案 *

张龙军[a], 莫天庆[a], 赵李懿[b]
(武警工程学院 a. 通信工程系; b. 电子技术系 网络与信息安全武警部队重点实验室, 西安 710086)

摘 要: 针对现有的代理移动 IPv6 认证方案存在的系统开销大和不能抵御暴力攻击的问题,提出了一种基于无证书签密的代理移动 IPv6 认证方案。该方案结合了无证书签密和代理移动 IPv6 的实际环境,在实现对移动节点认证的同时有效地解决了无线环境中密钥管理问题。对方案的安全性进行形式化分析证明,该方案在随机预言机模型下是可证明安全的。同时,效率分析表明,该方案不仅减少了节点之间的交互,而且保持了较小的计算量。

关键词: 代理移动 IPv6; 无证书签密; 认证; 随机预言机模型
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)02-0640-004
doi:10.3969/j.issn.1001-3695.2012.02.063

Authentication scheme based on certificateless signcryption in proxy mobile IPv6 network

ZHANG Long-jun[a], MO Tian-qing[a], ZHAO Li-yi[b]
(*a. Dept. of Communication Engineering, b. Key Laboratory of Network & Information Security of APF, Engineering College of APF, Xi'an 710086, China*)

Abstract: The proposed authentication scheme in proxy mobile IPv6 network has the flaw of system requirement and cannot resist the dictionary attack. To solve these problems, this paper proposed an authentication scheme based on certificateless signcryption in proxy mobile IPv6 network. The proposed scheme could not only realize mutual authentication between the end-points but also simplify the key management in wireless mobile environment. Performance analysis results show that the proposed mechanism is very efficient. Finally, it proved the new scheme's security in the random oracle model.

Key words: proxy mobile IPv6; certificateless signcryption; authentication; random oracle model

0 引言

针对移动 IPv6 协议[1]存在的对无线带宽和移动节点(mobile node,MN)要求高、切换时延以及数据包丢失等问题[2],IETF 工作组提出了代理移动 IPv6(proxy mobile IPv6,PMIPv6)协议[3]。但是,该协议没有规定 MAG(mobile access gateway)获取 MN 配置文件时与 AAA 的交互模式以及 MAG 代替 MN 发送代理绑定更新消息的授权方法。目前,针对这方面的研究还很少,文献[4]提出了一种基于 Diameter 协议的代理移动 IPv6 认证方法。该方法通过 AAA 与 MN、LMA(local mobility anchor)以及 MAG 之间预先共享密钥来实现认证,带来了额外的开销,且不能抵御暴力攻击。另外,该方法虽然考虑到了 AAA 认证框架与代理移动 IPv6 的结合,但忽略了认证框架下所采用的具体认证方法。Diameter 协议建议采用支持各种具体认证方法的 EAP(extensible authentication protocol)来实现认证功能[5,6]。因此,即使采用最简单的 EAP-MD5 来认证,至少都会增加一次 AAA 与 MAG 和 LMA 之间的交互,这就极大地降低了 MN 的接入效率。

基于上述分析,本文提出一种安全高效的无证书签密方案来解决 PMIPv6 协议引入认证后的效率和安全问题。该方案利用无证书签密的特性,将代理移动 IPv6 中的切换和认证过程有机地结合,提高了效率。在随机预言机模型下,该方案是可证明安全的。

1 基本知识

1.1 代理移动 IPv 6

基于网络移动性管理的 PMIPv6 协议通过移动代理实体代替 MN 来完成移动管理,降低了 MN 协议栈的复杂性,节省了无线带宽,提高了切换性能。对于 MN 而言,整个 PMIPv6 域就像一个家乡网络。因此,MN 可以在不改变 IP 地址的情况下完成域间切换。当 MN 接入 PMIPv6 域时,接入链路上的 MAG 识别该 MN,判断其是否有权限获得基于网络的移动性管理服务,如果有权限,则根据 MN 的策略文件完成绑定更新及地址配置等操作。具体过程参见 RFC5213。

1.2 无证书签密

文献[7]首次给出了无证书签密及其安全模型的定义。一个基于双线性对的无证书签密方案一般由初始化、部分密钥

收稿日期: 2011-07-06; **修回日期**: 2011-08-19 **基金项目**: 国家自然科学基金资助项目(60842006); 陕西省自然科学基金资助项目(2007F50); 武警部队科研基金资助项目(wjy201111); 武警工程学院基础基金资助项目(wxk2010-04); 武警工程学院研究生创新基金资助项目(2011S070)

作者简介: 张龙军(1964-),男,教授,博士(后),主要研究方向为信息安全和密码学; 莫天庆(1986-),女,硕士,主要研究方向为信息安全与密码学(motianqing11@163.com); 赵李懿(1986-),男,硕士,主要研究方向为信息安全.

提取、私钥提取、公钥提取、签密以及解签密构成。一个无证书系统面临两种不同能力的敌手:Type Ⅰ的敌手 $Adv_{Ⅰ}$ 和 Type Ⅱ的敌手 $Adv_{Ⅱ}$。$Adv_{Ⅰ}$ 代表第三方用户对无证书签密方案的攻击,即敌手 $Adv_{Ⅰ}$ 不能获得系统主密钥,但它可以自己选择一个值来替换任意用户的公钥。敌手 $Adv_{Ⅱ}$ 代表恶意的能产生部分私钥的 KGC,它拥有系统主密钥,但不能替换任何用户的公钥。同时,无证书签密需满足在适应性选择密文攻击下具有不可区分性和在适应性选择消息攻击下的不可伪造性[8]。本文方案的机密性和不可伪造性定义参见文献[9]。

2　一种新的 PMIPv 6 网络认证方案

2.1　无证书签密方案

a)初始化。给定安全参数 k,设 G_1 为由 P 生成的循环加法群,其阶为 q,G_2 为具有相同阶 q 的循环乘法群,且在 G_1、G_2 中离散对数问题都是难解的;E、D 为安全的对称密码算法;KGC 随机选择 $s \in Z_q^*$ 作为系统主密钥妥善保存,系统公钥 $p_{pub}=s\cdot P$;选择三个安全的 hash 函数,$H_1:\{0,1\}^{l_1}\times G_1 \to G_1$,$H_2:\{0,1\}^{l_2}\times\{0,1\}^n \to \{0,1\}^l$,$H_3:\{0,1\}^* \to Z_q^*$。其中 l_1 为身份标志的长度,l_2 为 G_1 中元素的长度,l 为一固定值,n 为明文的长度。系统公开的参数为 $\{G_1,G_2,q,\hat{e},p,p_{pub},H_1,H_2,H_3,E,D\}$。

b)部分密钥生成。用户向 KGC 提交身份标志 $Y_U=(ID_u, x\cdot P)$,其中随机数 $x \in Z_q^*$,KGC 先检查 Y_U 的合法性。若 Y_U 合法,则计算 $Q_u=H_1(Y_U)$,生成部分密钥 $W_u=s\cdot Q_u$。

c)私钥生成。给定用户身份 ID_u 和部分密钥 W_u,判断等式 $\hat{e}(W_u,P)=\hat{e}(Q_u,P_{pub})$ 是否成立,如果上述等式成立,用户随机选择 $z_u \in Z_q^*$ 作为秘密值,生成私钥 $s_u=z_u\cdot W_u$,并将其妥善保存。

d)公钥生成。给定用户身份 ID_u,用户计算 $P_u=z_u\cdot P_{pub}$ 作为自己的公钥并将其公开。

e)签密。当密钥为 (P_a,s_a) 的网络实体 A 要发送消息 $m \in \{0,1\}^*$ 给密钥为 (P_b,s_b) 的网络实体 B 时,对 m 进行如下操作:

(a)随机选择 $r \in Z_q^*$ 计算 $k_1=r\cdot P_b$;

(b)计算 $\omega=\hat{e}(P_b,s_a\cdot Q_a^{-1})$,$k_2=H_3(\omega)$;

(c)计算 $k_3=H_2(k_1,m)$,$t=r\cdot Q_a/s_a$,$\delta=E_{k_2}(t\|m\|k_3)$;

(d)发送消息 δ 给 B。

f)解密验证。当 B 收到 δ,进行如下操作:

(a)计算 $\omega=\hat{e}(P_a,s_b\cdot Q_b^{-1})$,$k_2=H_3(\omega)$;

(b)计算 $D_{k_2}(\delta)=t\|m\|k_3$;

(c)计算 $k_1=t\cdot P_a\cdot s_b\cdot Q_b^{-1}$,若 $k_3=H_2(k_1,m)$ 成立则接收该消息,否则将其拒绝。

正确性证明(本方案的正确性取决于以下两个等式的正确性)。

$$\hat{e}(P_a,s_b\cdot Q_b^{-1})=\hat{e}(P_b,s_a\cdot Q_a^{-1}) \tag{1}$$

证明　$\hat{e}(P_a,s_b\cdot Q_b^{-1})=\hat{e}(z_a\cdot P_{pub},z_b\cdot s\cdot Q_b\cdot Q_b^{-1})=\hat{e}(z_b\cdot P_{pub},z_a\cdot s)=\hat{e}(P_b,z_a\cdot s\cdot Q_a\cdot Q_a^{-1})=\hat{e}(P_b,s_a\cdot Q_a^{-1})$

$$t\cdot P_a\cdot s_b\cdot Q_b^{-1}=r\cdot P_b \tag{2}$$

证明　$[(r\cdot Q_a)/(z_a\cdot s\cdot Q_a)]\cdot z_a\cdot P_{pub}\cdot z_b\cdot s\cdot Q_b\cdot Q_b^{-1}=r\cdot z_b\cdot P_{pub}=r\cdot P_b$

2.2　认证方案的实现流程

设网络中的节点都支持无证书签密技术,每个实体的身份 ID 为其 NAI,且每个实体都已经通过密钥生成算法得到了相应的密钥对。当 MAG 检测到有新的 MN 节点接入时,分两个阶段进行消息交互:第一阶段,MN 发送携带 AS(服务者请求)的消息给 MAG,同时触发 MAG 与 AAA 进行一次交互来获得 MN 的签密参数,然后产生随机数 N_0,并将 N_0 和签密参数一起通过 AA(服务者通告)消息发送给 MN;第二阶段,当 MN 收到 AA 后,开始接入认证和绑定更新。具体过程如图 1 所示。

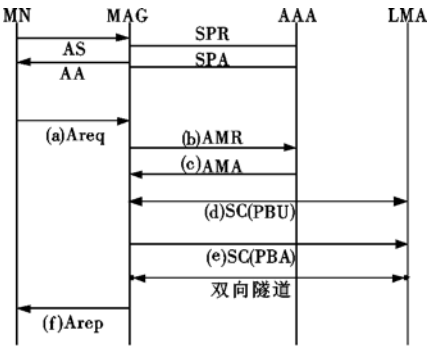

图1　接入认证流程

a)MN 从 AA 消息中取出 N_0 和签密参数,利用本文所提出的签密算法计算身份 ID_{MN} 和随机数 N_0 的签密密文 σ、N_0 的 hash 值 c,向 MAG 发送认证请求消息,即 MN→MAG:Areq,其中 $Areq=\langle signcrypt(P_{AAA},s_{MN},(ID_{MN},N_0)),H_3(N_0)\rangle$。

b)MAG 收到 Areq 消息后计算 $c'=H_3(N_0)$,并与接收到的 c 比较,若相等,则将 Areq 转换为 MAG 的认证请求消息(AMR)然后发送给 AAA,即 MAG→AAA:$AMR=\langle signcrypt(P_{AAA},s_{MN},(ID_{MN},N_0))\rangle$。

c)AAA 收到 AMR 消息后进行解签密运算,实现 AAA 对 MN 的认证,得到 MN 的身份 ID_{MN} 并查询数据库,取出包含 LMA 的地址信息、签密参数以及 MN 的地址配置方式等的策略文件 m,并将其进行签密处理后发送给 MAG,即 AAA→MAG:AMA,其中 $AMA=\langle signcrypt(P_{MAG},s_{AAA},(m,N_0))\rangle$。

d)MAG 收到 AMA 消息后,进行解签密处理,实现对 AAA 的认证,得到 MN 的策略文件,选择随机数 N_1,将代理绑定更新(PBU)报文和 N_1 进行签密处理后发送给 LMA,即 MAG→LMA:$\langle SC(PBU,N_1)\rangle$,其中 $\langle SC(PBU,N_1)\rangle=signcrypt(P_{LAM},S_{MAG},(PBU,N_1))$。

e)LMA 收到 $SC(PBU,N_1)$ 消息后,通过解签密运算实现对 MAG 的认证,随机选择 N_2,并将其与代理绑定更新确认(PBA)一起经过签密处理后发送给 MAG。保存隧道标志 $a=(N_1|N_2)$,即 LAM→MAG:$SC(PBA,N_2)$,$SC(PBA,N_2)=signcrypt(P_{MAG},S_{LAM},(PBA,N_2))$。

f)MAG 收到绑定确认消息后进行解签密处理,实现对 LMA 的认证,计算隧道标志 $a=(N_1|N_2)$,建立与 LMA 之间的双向隧道并发送包含家乡网络地址前缀等选项的认证响应消息给 MN,即 MAG→MN:Arep。

在 PMIPv6 域中,完成了初始地址配置的 MN 切换到新链路时,新链路上的 MAG(NMAG)向 MN 的 LMA 发送 PBU 消息来更新 MN 当前的位置信息,操作流程与接入认证过程相同。而 MN 之前附着的 MAG(PMAG)向 LMA 发送解注册请求消息来通知 LMA 取消对 MN 的绑定和路由状态。当 LMA 收到该请求后,停止将 CN 发送给 MN 的数据发送给 PMAG,等待一段时间后删除相应的绑定缓存列表条目(BCE)。如果在这段时间内 LMA 收到了 NMAG 的 PBU 消息,则更新 BCE 中的代理转交地址等信息,然后建立与 NMAG 之间的隧道。同时删除与 PMAG 之间的隧道和对应信息,发送解注册确认给 PMAG,完成切换认证。

3 证明与分析

3.1 安全性证明

3.1.1 机密性

定理 1 类型Ⅰ攻击下的保密性。在随机预言机模型中，若存在一个 IND-CLSC-CCA2 敌手 Adv_I 能够在多项式有限时间 t 内，以 ε 的优势赢得文献[9]3.2.1 节中定义的游戏 Game IND-CCA2-Ⅰ（最多进行 q_i 次 H_i 询问，$i=1,2,3$），则存在一个区分者 D，能够在多项式有限时间 $t'<(q_{H_1}+q_{H_2})\cdot t_e+t$ 内，以 $\varepsilon'\geqslant[\varepsilon/(q_{H_1}\cdot q_{H_2}\cdot q_{H_3})]\cdot(1-q_u/2^k)$ 的优势解决 BDH 问题。其中 t_e 表示双线性对运算花费的时间。

证明 区分者 D 接收一个随机的 BDH 问题实例 (P,aP,bP,cP)，目标是计算 $\hat{e}(P,P)^{abc}$。在这里，$a,b,c\in Z_q^*$ 是未知整数。D 将 Adv_I 作为子程序并扮演 IND-CLSC-CCA2 游戏中的挑战者 C。在整个游戏过程中，假设任何包含身份 ID 的询问都在 H_1 询问之后。游戏一开始，D 随机选取 $\eta\in\{1,2,\cdots,q_1\}$，发送系统参数 $\{G_1,G_2,q,\hat{e},P,P_{pub},H_1,H_2,H_3,E,D\}$ 给 Adv_I。定义 L_1、L_2、L_3、L_{par}、L_{pri}、L_{pub}、L_s，和 L_u 分别用于跟踪 Adv_I 对随机预言机 H_1、H_2、H_3、部分密钥提取、私钥提取、公钥提取、签密和解签密询问。

H_1 询问。当 Adv_I 询问$\langle ID_u,(h_1)\rangle$时，若表 L_1 中存在相应的记录，则返回相应的值。否则，当 $u\neq\eta$ 时，D 随机选择 $h_1\in G_1$，将其返回作为回答，并将$\langle ID_u,(h_1)\rangle$加入表 L_1 中；当 $u=\eta$ 时，令 $h_1=e$，并将其返回作为回答，然后将$\langle ID_u,(h_1)\rangle$加入表 L_1 中。

H_2 询问。当 Adv_I 询问$\langle k_1,m,(h_2)\rangle$时，若表 L_2 中有相应的记录，则返回相应的值；否则，D 随机选择选择 $h_2\in Z_q^*$，将其返回作为回答，并将$\langle k_1,m,(h_2)\rangle$加入表 L_2 中。

H_3 询问。当 Adv_I 询问$\langle\omega,(h_2)\rangle$时，若表 L_3 中存在相应的记录，则返回相应的值；否则，D 随机选择 $h_3\in Z_q^*$，将其返回作为回答，并将$\langle\omega,(h_3)\rangle$加入表 L_3 中。

部分密钥询问。当 Adv_I 询问$\langle ID_u,(W_u)\rangle$时，若 $u=\eta$，则终止模拟；否则，若表 L_{par} 中存在相应的记录则返回相应的值，若不存在，则从表 L_1 中取出 h_1，随机选取 $s\in Z_q^*$，计算 $W_u=s\cdot h_1$，把$\langle ID_u,(W_u)\rangle$加入表 L_{par}，返回 W_u 作为回答。

私钥提取询问。当 Adv_I 询问$\langle ID_u,W_u,(s_u)\rangle$时，若 $u=\eta$，则终止模拟。否则，若表 L_{pri} 中存在相应的记录则返回其相应的值；若不存在，则查询表 L_{par}，如果 L_{par} 中存在相应的记录，则从表中取出相应的 W_u，随机选择 $s\in Z_q^*$ 计算 $s_u=z_u\cdot W_u$，将$\langle ID_u,W_u,(s_u)\rangle$加入表 L_{pri} 中并返回 s_u；如果 L_{par} 中不存在相应的值，则查询 L_1 取出相应的 h_1，随机选取 $S',z'_utZ_q^*$，计算 $S_u=Z'_u\cdot S'\cdot h_1$，返回 s_u，将$\langle ID_u,W_u,(s_u)\rangle$加入 L_{pri}。

公钥提取询问。当 Adv_I 询问$\langle ID_u,(P_u)\rangle$时，若表 L_{pub} 中存在相应的记录则返回相应的值；否则选择随机数 $z_u\in Z_q^*$，计算 $P_u=z_u\cdot P_{pub}$，返回 P_u 将$\langle ID_u,(P_u)\rangle$加入表 L_{pub} 中。

公钥替换询问。Adv_I 随机选择一个新的值代替 ID_u，并用新的公钥 P'_u 代替签名者原来的公钥 P_u。

签密询问。当 Adv_I 询问$\langle ID_a,ID_b,m,(\sigma)\rangle$时分为两种情况：(a)如果 $ID_a\neq\eta$，D 通过查询$\langle ID_b,(P_b)\rangle$获得相应的 P_b，并对 ID_a 执行部分密钥提取询问和私钥提取询问得到相应的私钥 s_a，依据签密算法可计算 $\sigma=\text{signcrypt}(P_b,s_a,m)$，将 σ 返回；(b)如果 $ID_a=\eta$，D 通过查询$\langle ID_a,(P_a)\rangle$，$\langle ID_b,(P_b)\rangle$获得相应的公钥 P_a、P_b，对 ID_b 执行分密钥提取询问和私钥提取询问得到相应的私钥 s_b，然后从 Z_q^* 中随机选择两个值 r'、t'，计算 $k'_1=r'\cdot P_b$，$\omega=\hat{e}(P_a,s_b\cdot Q_b^{-1})$，$k_2=H_3(\omega)$，检查 L_2 表中是否已经存在，若已经存在，则重新选取 r'，直到(k'_1,m)在表 L_2 中的项中的前两个元素都没有出现过为止。计算 $k'_3=H_2(k'_1,m)$，$\sigma=E_{k_2}(t'\|m\|k'_3)$，并将 σ 返回给 Adv_I。

解签密询问。当 Adv_I 询问$\langle ID_a,ID_\eta,\sigma\rangle$时，D 回答该密文无效；当 Adv_I 询问$\langle ID_a,ID_b,\sigma\rangle$，其中 $b\neq\eta$，查询表 L_{pub}，当 P_a 不存在时，随机选择 $z_a'\in Z_q^*$，计算 $P_a=z_a'\cdot P_{pub}$，$\omega=\hat{e}(P_a,s_b\cdot Q_b^{-1})$，$k_2=H_3(\omega)$，$(t'\|m\|k'_3)=D_{k_2}(\sigma)$，$k'_1=(t'\cdot P_a\cdot z_b)/W_b$，检查 L_2 中$\langle k'_1,m,k'_3\rangle$是否存在，若存在，则输出 m，否则输出 $\perp$。

经过多项式有界次询问后，Adv_I 输出两个不同的身份 (ID_a^*,ID_b^*)和两个等长的消息$\{m_0,m_1\}$进行挑战，若 $ID_b^*\neq ID_\eta$ 则终止模拟，否则 D 随机地投掷一枚硬币 $\theta\in\{0,1\}$，对 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_θ,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 $k_2^*=H_2(k_1^*,m_\theta)$，计算签密密文 $\sigma^*=E_{k_2^*}(t^*\|m\|k_3^*)$，返回 σ 给 Adv_I 作为挑战密文，其中 D 知道被替换公钥的相关信息。

Adv_I 在不执行对 σ^* 解签密询问的前提下继续进行多项式有界次询问。在模拟结束时，Adv_I 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_I 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 D 拒绝了一个合法的密文，则 D 将失败。因此，D 至少以 $\varepsilon'\geqslant[\varepsilon/(q_{H_1}\cdot q_{H_2}\cdot q_{H_3})]\cdot(1-q_u/2^k)$ 的优势解决 BDH 问题。其中 $k\in\{1,2,\cdots,(q_{H_2}+q_s)\}$。

定理 2 类型Ⅱ攻击下的保密性。在随机预言机模型中，若存在一个 IND-CLSC-CCA2 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]3.2.1 节中定义的游戏 Game IND-CCA2-Ⅱ，则存在一个区分者 D，能够在多项式有限时间内，以 $\varepsilon'\geqslant[\varepsilon/(q_{H_1}\cdot q_{H_2}\cdot q_{H_3})]\cdot(1-q_u/2^k)$ 的优势解决 BDH 问题。

证明 区分者 D 接收一个随机的 BDH 问题实例，将 $Adv_{Ⅱ}$ 作为子程序并扮演 IND-CLSC-CCA2 游戏中的挑战者 C。其他的初始化过程参见定理 1。

攻击者 $Adv_{Ⅱ}$ 可以进行定理 1 中的 H_1、H_2、H_3、公钥提取、签密和解签密询问。

部分密钥询问。当 $Adv_{Ⅱ}$ 询问$\langle ID_u,(W_u)\rangle$时，如果 $u=\eta$，则终止模拟。否则当 L_{par} 表中存在相应的记录则返回相应的值；当 L_{par} 表中不存在相应的值时，从 L_1 表中取出相应的 h_1，计算 $W_u=s\cdot h_1$，将$\langle ID_u,(W_u)\rangle$加入表 L_{par} 中，返回 W_u。

私钥提取询问。当 $Adv_{Ⅱ}$ 询问$\langle ID_u,W_u,(S_u)\rangle$时，如果 $u=\eta$ 则终止模拟。当 L_{pri} 表中存在相应的记录则返回相应的值；否则查询表 L_{par}，从中取出相应的 W_u，随机选择 $z_u\in Z_q^*$，计算$s_u=z_u\cdot W_u$，将$\langle ID_u,(W_u)\rangle$加入表 L_{pri}，返回 s_u。若表 L_{par} 中不存在相应的值，则查询表 L_1，从中取出相应的 h_1，随机选择$z_u\in Z_q^*$计算 $s_u=z_u'\cdot s\cdot h_1$，返回 s_u 并将$\langle ID_u,(W_u)\rangle$加入 L_{pri}。

经过多项式有界次询问后，$Adv_{Ⅱ}$ 输出两个不同的身份 $(ID_a^{*'},ID_b^{*'})$和两个等长的消息$\{m_0,m_1\}$进行挑战，若 $ID_b^{*'}\neq ID_b^{*'}$ 则终止模拟，否则 D 随机地投掷一枚硬币 $\theta\in\{0,1\}$，对

$ID_b^{*'}$ 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 $\varepsilon'\geqslant[\varepsilon/(q_{H_1}\cdot q_{H_2}\cdot q_{H_3})]\cdot(1-q_u/2^k)$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 $\varepsilon'\geqslant[(\varepsilon/(q_{H_1}\cdot q_{H_3})]$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 $\varepsilon'\geqslant[\varepsilon/(q_{H_1}\cdot q_{H_3})]$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 $\varepsilon'\geqslant[(\varepsilon/(q_{H_1}^2\cdot q_{H_3})]$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 $\varepsilon'\geqslant[\varepsilon/(q_{H_1}^2\cdot q_{H_3})]$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.