基于无证书的两方跨域认证密钥协商协议

刘小琼, 潘 进, 李国朋
(西安通信学院, 西安 710106)

摘 要: 利用椭圆曲线上双线性对映射和离散对数问题,提出一种基于无证书的两方跨域认证密钥协商协议。该协议解决了传统的基于身份的跨域两方密钥协商协议中固有的密钥托管问题,实现了跨域通信双方的身份验证,防止了主动攻击。在保证协议正确性的基础上,采用应用 Pi 演算对协议进行形式化分析,并验证了协议的认证性和安全性。与其他跨域两方认证密钥协商协议性能相比,该协议的安全性和效率都更优。

关键词: 密钥协商; 双线性对; 无证书密码体制; 形式化分析; 多 PKG 环境
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)02-0646-04
doi:10.3969/j.issn.1001-3695.2012.02.065

Certificateless-based two-party authenticated key agreement protocol for multiple PKG environment

LIU Xiao-qiong, PAN Jin, LI Guo-peng
(*Xi'an Communications Institute*, *Xi'an* 710106, *China*)

Abstract: This paper proposed a certificateless-based two-party authenticated key agreement protocol for a multiple PKG environment based on bilinear pairings in elliptic curves and elliptic curve discrete logarithm, which solved the key escrow issues inherited in the identity-based schemes effectively and preventing active attack by identity authentication. After confirming the correctness, the formal analysis based on applied Pi calculus shows fulfilled authentication and security. Compared with other two-party authenticated key agreement protocols for a multiple PKG environment, the newly proposed key agreement protocol has better security and efficiency.

Key words: key agreement; bilinear pairings; certificateless-based; formal analysis; multiple PKG environment

0 引言

随着无线网络中终端漫游现象的日益增多,跨域通信成为研究的焦点。设计适合跨域通信的认证密钥协商协议是确保跨域通信安全的有效手段。传统的利用公钥密码体制设计的认证密钥协商协议主要是基于传统公钥密码体制(PKC-based)和基于身份的密码体制(ID-based)。基于传统公钥证书的认证密钥协商方案的主要问题是存在身份管理的复杂性,基于身份的认证密钥协商方案存在的主要问题是密钥托管问题。随着无证书密码体制(certificateless-based)[1]的出现,基于无证书密码体制成为设计认证密钥协商协议的新思路。该体制需要一个可信私钥生产中心(private key generator, PKG)的支持,由于用户的私钥包含两部分,一部分来自于 PKG 的生成,另一部分来自于自身的生成,因此该类方案一方面保持了基于身份的公钥密码体制的身份易管理性,同时也解决了基于身份的公钥密码体制中固有的密钥托管问题,使得构建的认证密钥协商协议具有更多的优势。当前,针对同一个 PKG 域设计的无证书认证密钥协商协议较多[1~8],但针对不同 PKG 域的研究[9~11]多是基于身份的,基于无证书的研究[12]相对较少。因此研究和设计基于无证书的两方跨域认证密钥协商协议有一定的理论和实用价值。

本文构建一个安全有效的两方无证书跨域认证密钥协商协议,并采用应用 Pi 演算对协议安全性进行了证明。与其他同类方案的比较表明,新方案满足目前已知的安全属性,同时保持了良好的性能。

1 预备知识

1.1 椭圆曲线上的双线性映射

双线性对是指两个循环群之间相对应的线性映射关系。设 G_1、G_2 分别是阶为 q 的加法循环群和乘法循环群,q 是大素数,且在 G_1、G_2 中离散对数问题都是难解的。$\hat{e}$ 是 $G_1 \times G_1 \to G_2$ 的双线性映射,满足如下性质:

a)双线性。对任意 $P, Q \in G_1$,所有 $a, b \in Z_q^*$,满足 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$;同时,对任意 $p_1, p_2, Q \in G_1$,有 $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q) \times \hat{e}(P_2, Q)$。

b)非退化性。若 P 是 G_1 的生成元,则 $\hat{e}(P, P) \in G_2$ 是 G_2 的生成元,即 $\hat{e}(P, P) \neq 1$。

c)可计算性。存在一个高效算法计算 $\hat{e}(P, Q)$, $P, Q \in G_1$。

1.2 椭圆曲线上离散对数问题

$E(F)$ 是定义在有限域 F_q 上的椭圆曲线,设任意两点 P, $Q \in E(F)$,若已知对某个整数 m 有 $Q = mP$ 成立,由 P、Q 及 E 求出 m 的问题称为 E 上的椭圆曲线离散对数问题。

1.3 密钥协商协议的安全属性

a)已知会话密钥安全。已知旧的会话密钥不会影响到其

收稿日期: 2011-07-08; **修回日期**: 2011-08-09

作者简介:刘小琼(1985-),女(羌族),四川绵阳人,硕士研究生,主要研究方向为网络安全(xtyliuxiaoqiong@163.com);潘进(1959-),男,教授,博士,主要研究方向为网络安全与对抗;李国朋(1982-),男,讲师,硕士,主要研究方向为网络安全与对抗.

他会话密钥的安全性。

b)前向安全性。如果一个或多个实体的长期私钥被攻破,以前建立的会话密钥的安全性不受影响。

c)密钥泄露伪装安全。如果 I 的长期私钥被攻破了,攻击者可以伪装成 I,但是不能对 I 伪装成其他实体。

d)未知密钥共享安全。实体 I 不能被迫与实体 C 共享一个会话密钥,而实际上 I 以为他正与实体 R 共享一个会话密钥。

e)已知临时会话信息安全性。临时私钥的泄露不能导致攻击者计算出会话密钥。

2　新的基于无证书的两方跨域认证密钥协商方案

2.1　系统初始化

设 G_1、G_2 分别是 q 阶的椭圆曲线加法循环群和乘法循环群,其中 q 是大素数,且在 G_1、G_2 中离散对数问题都是难解的。$\hat{e}$ 是 $G_1 \times G_1 \to G_2$ 的双线性映射。PKG_A、PKG_B 分别作为发起方 A 和响应方 B 的可信第三方,负责系统参数初始化、认证用户身份、生成和分发用户私钥等。

2.1.1　建立系统参数

PKG_A、PKG_B 作为发起方 A 和响应方 B 的私钥生成中心,它们分别随机选择 $s_a, s_b \in Z_q^*$ 作为本域系统主密钥秘密保存,同时计算各系统相应的公钥 $pk_{PKG_A} = s_a \cdot P$ 和 $pk_{PKG_B} = s_b \cdot P$,P 为 G_1 的生成元;定义两个 hash 函数 $H: G_2 \to \{0,1\}^k$ 和 $H_1: \{0,1\}^* \to G_1$。PKG_A 和 PKG_B 在各自域服务范围内公开系统参数 $params_A = \langle G_1, G_2, \hat{e}, P, pk_{PKG_A}, H_1, H_2 \rangle$ 和 $params_B = \langle G_1, G_2, \hat{e}, P, pk_{PKG_B}, H_1, H_2 \rangle$。

2.1.2　生成用户密钥

假定发起方 A 和响应方 B 分别隶属于 PKG_A、PKG_B,它们的身份信息分别为 ID_a,ID_b。PKG_A 计算 $Q_A = H_1(ID_a)$ 后,为发起方 A 计算并安全分发部分私钥 $D_A = s_a \cdot Q_A$,A 再随机选择一个秘密参数 $x_A \in Z_q^*$ 作为长期私钥,并计算 $P_A = x_A \cdot P$。则实体 A 完整的私钥为 $S_A = \langle D_A, x_A \rangle$,公钥为 $X_A = \langle P_A, P_{PKG_A} \rangle$,实体 B 也类似。

2.2　密钥协商与认证

系统初始化阶段完成后,双方的会话密钥协商过程如图 1 所示。

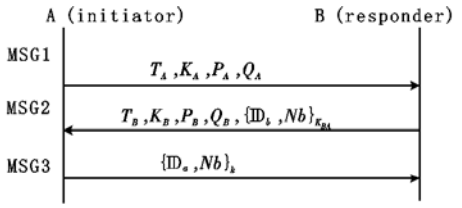

图1　基于无证书的跨域两方认证密钥协商过程

a)发起方首先秘密地随机选取参数 $a(a \in Z_q^*)$,并分别计算 $T_A = a \cdot P$ 和 $K_A = a \cdot pk_{PKG_A}$,$P_A = x_A \cdot P$ 然后向响应方发送消息 MSG1:T_A, K_A, P_A, Q_A。

b)响应方收到消息 MSG1 后,首先秘密地选取参数 $b(b \in Z_q^*)$ 和随机值 Nb,并分别计算 $T_B = b \cdot P$ 和 $K_B = b \cdot pk_{PKG_B}$,$P_B = x_B \cdot P$,接着再分别用对方发来的 Q_A 和自己的部分私钥 D_B 计算 $K_{BA1} = \hat{e}(b \cdot Q_A, K_A)$ 与 $K_{BA2} = \hat{e}(b \cdot D_B, T_A)$,然后用单项散列函数 H 计算密钥 $K_{BA} = H(K_{BA1}, K_{BA2})$,同时以 K_{BA} 为密钥采用对称密码算法加密自己的身份 ID_b 和随机值 Nb,得到 $e_B = \{ID_b, Nb\}_{KBA}$,最后向发起方发送消息 MSG2:T_B, K_B, P_B, Q_B, e_B。

c)发起方收到消息 MSG2 后,先用自己的部分私钥 D_A 和响应方的 Q_B 计算 $K_{AB1} = \hat{e}(a \cdot D_A, T_B)$,$K_{AB2} = \hat{e}(a \cdot Q_B, K_B)$,$K_{AB} = H(K_{AB1}, K_{AB2})$,再用密钥 K_{AB} 对称解密 e_B,然后再计算密钥 $P_{AB} = a \cdot P_B$,得到 ID_b 和 Nb。确认 B 的身份后,计算会话密钥 $k = H(K_{AB}, P_{AB})$。用 k 对称加密自己的身份 ID_a 和和响应方发来的 Nb,即 $eA = \{ID_a, Nb\}_k$,最后向响应方发送消息 MSG3:eA。

d)响应方收到消息 eA 后,计算 $P_{BA} = b \cdot P_A$ 以及会话密钥 $k = H(K_{BA}, P_{BA})$,并用会话密钥 k 对称解密 eA 得到 ID_a 和 Nb',确认 A 的身份后,验证 Nb 与 Nb' 是否相等,若相等,则确认双方可以用会话密钥 k 安全通信,协商过程结束。

2.3　正确性分析

首先,分析发起方计算的 K_{AB1}、K_{AB2} 值:

$$K_{AB1} = \hat{e}(a \cdot D_A, T_B) = \hat{e}(a \cdot s_a \cdot Q_A, bP) = \hat{e}(Q_A, P)^{abs_a}$$

$$K_{AB2} = \hat{e}(a \cdot Q_B, K_B) = \hat{e}(a \cdot Q_B, b \cdot pk_{PKG_B}) = \hat{e}(Q_B, p)^{abs_b}$$

其次,分析发起方计算的 K_{BA1}、K_{BA2} 值:

$$K_{BA1} = \hat{e}(b \cdot Q_A, K_A) = \hat{e}(b \cdot Q_A, a \cdot pk_{PKG_A}) = \hat{e}(Q_A, P)^{abs_a}$$

$$K_{BA2} = \hat{e}(b \cdot D_B, T_A) = \hat{e}(b \cdot s_a \cdot Q_B, aP) = \hat{e}(Q_B, P)^{abs_b}$$

可知:

$$K_{AB1} = K_{BA1} = \hat{e}(Q_A, P)^{abs_a}$$

$$K_{AB2} = K_{BA2} = \hat{e}(Q_B, P)^{abs_b}$$

$$K_{AB} = H(H_2(K_{AB1}) \mid H_2(K_{AB2})) =$$

$$K_{BA} = H(H_2(K_{BA1}) \mid H_2(K_{BA2}))$$

接着,再分析发起方的 P_{AB} 值和响应方的 P_{BA} 值:

$$P_{AB} = a \cdot P_B = a \cdot b \cdot P; P_{BA} = b \cdot P_A = b \cdot a \cdot P$$

又因为循环群 G_1 是阿贝尔群,因此 $P_{AB} = P_{BA} = abP$。

最后,分析发起方和响应方计算的会话密钥 k 值。因为跨域两方计算出的 $K_{AB} = K_{BA}$、$P_{AB} = P_{BA}$,所以它们最终计算出的会话密钥 k 值也是相等的,即

$$k = H(K_{AB}, P_{AB}) = H(K_{BA}, P_{BA})$$

由于跨域两方分别以自己的私钥和对方的公钥计算会话密钥,而只有正确地跨域两方才能计算出正确的会话密钥值,因此,该方法起到了相互认证的作用,从而可以抵御中间人攻击。

2.4　安全属性分析

a)已知会话密钥安全。由于在产生会话密钥时使用了临时值(a,b),一个会话密钥泄露了不影响以前的或者将来的会话。

b)前向安全性。如果实体 A 和 B 的长期私钥被泄露了,攻击者仍然不知道之前建立的会话密钥,因为计算 K_{AB} 需要知道 a,而计算 K_{BA} 需要知道 b,即使是 PKG 也不能恢复出会话密钥。

c)密钥泄露伪装安全。假设攻击者 E 知道 A 的私钥,并且拦截了 B 传递来的信息,但是 E 仍然无法得到会话密钥,因为计算 P_{AB} 需知道 a,计算 K_{BA} 需要知道 D_B。

d)未知密钥共享安全。如果 A 和 B 协商会话密钥,B 需使用 D_B 来计算会话密钥。因此,C 如果想算出同样的会话密钥,必须得到 D_B,而只有 PKG 和实体 B 知道 D_B,因此 C 无法计算出会话密钥。

e)已知临时会话信息安全性。假设攻击者得到会话的临时秘密值 a 和 b,它仍然无法计算 K_{BA} 和 K_{AB},但是如果攻击者是 PKG,那么它就能计算出来。此时,会话密钥的安全性则由 P_{AB} 和 P_{BA} 来保证,因为 PKG 不知道 x_A 和 x_B 的值。

3 协议的安全性证明

3.1 协议的应用 Pi 演算模型

协商过程用到的函数和代数相等关系主要包括：

fun $E/2$（对称密钥加密）

reduc $D(x,E(x,y)) = y$（对称密钥解密）

fun $H/1$（单向散列函数）

fun $H_1/1$（公钥生成散列算法）

fun $f/2$（椭圆曲线标量乘运算）

fun $F/2$（双线性映射函数）

equation $F(f(a,f(x_1,y_1)),f(b,p)) = F(f(b,y_1),f(a,f(x_1,p)))$

equation $F(f(a,y_2),f(b,f(x_2,p))) = F(f(b,f(x_2,y_2)),f(a,p))$

在以上定义的基础上，可以建立如下协议模型：

$A = \text{key}A(D_A).\ va.\ vx_A.$
  let $Q_A = H_1(\text{ID}_a)$ in
  let $T_A = f(a,P)$ in
  let $K_A = f(a,pk_{\text{PKG}_A})$ in
  let $P_A = f(x_A,P)$ in
  $\bar{c}\langle \text{cons1}(T_A,K_A,P_A,Q_A)\rangle.$
  $c(\text{cons2}(T_B,K_B,P_B,Q_B,eB)).$
  let $K_{AB1} = F(f(a,D_A),T_B)$ in
  let $K_{AB2} = F(f(a,Q_B),K_B)$ in
  let $K_{AB} = H((K_{AB1},K_{AB2}))$ in
  let $(=\text{ID}_b,Nb) = D\{K_{AB}\}(eB)$ in
  let $P_{AB} = f(a\cdot P_B)$ in
  let $k = H((K_{AB},P_{AB}))$ in
  let $eA = E\{k\}(\text{ID}_a,Nb)$ in
  $\overline{c\langle \text{cons3}(eA)\rangle}$
  $\overline{\text{connect}}(\text{ID}_a,\text{ID}_b,k).$

其中，A 代表发起方进程。

$B = \text{key}_B(D_B).$
  $c(\text{cons1}(T_A,P_A,Q_A')).$
  $vb.\ vNb.\ vx_B.$
  let $T_B = f(b,P)$ in
  let $K_B = f(b,pk_{\text{PKG}_B})$ in
  let $P_B = f(x_B,P)$ in
  let $K_{BA1} = F(f(b,Q_A'),K_A)$ in
  let $K_{BA2} = F(f(b,D_B),T_A)$ in
  let $K_{BA} = H((K_{BA1},K_{BA2}))$ in
  let $eB = E\{K_{BA}\}(\text{ID}_b,Nb)$ in
  $\bar{c}\langle \text{cons2}(T_B,K_B,P_B,Q_B,eB)\rangle.$
  $c(\text{cons3}(eA)).$
  let $k = H((K_{BA},P_{BA}))$ in
  let $(\text{ID}_a,=Nb) = D\{k\}(eA)$ in
  if $QA' = H_1(\text{ID}_a)$ then
  $\overline{\text{accept}}(\text{ID}_a,\text{ID}_b,k).$

其中，B 代表响应方进程。

系统进程 S 由 A 和 B 进程并发组成，同时包括了 PKG 进程，PKG 进程负责生成用户名及公/私钥，并秘密分发私钥。

$S = v\text{ID}_a.\ v\text{ID}_b.\ vs_a.\ vs_b.$
  let $pk_{\text{PKG}_A} = f(s_a,P)$ in
  $\bar{c}\langle pk_{\text{PKG}_A}\rangle.$
  let $pk_{\text{PKG}_B} = f(s_b,P)$ in
  $\bar{c}\langle pk_{\text{PKG}_B}\rangle.$
  let $Q_A = H_1(\text{ID}_a)$ in
  let $D_A = f(s_a,Q_A)$ in
  $\overline{\text{key}_A\langle D_A\rangle}.$
  let $Q_B = H_1(\text{ID}_b)$ in
  let $D_B = f(s_b,Q_B)$ in
  $\overline{\text{key}_B\langle D_B\rangle}.$
  $(!\ A)\,|\,(!\ B)$

通道 init、connect、accept 代表交互的隐藏信道，环境无法与这些信道进行交互。通道 key_A、key_B 分别用来建模 PKG_A 与发起方 A、PKG_B 与响应方 B 传递信息的私有、安全信道，攻击者不能得到通道内的内容。一个安全的密钥协商协议应具有认证性与保密性[13]。本文采用形式化的方法证明协议的保密性、身份保护和认证性，部分形式化分析工作是在 ProVerif 的辅助下完成的。

3.2 协议的保密性

该协议用于跨域两方协商建立共享密钥，当环境无法区分双方传递的随机数 Nb 时，协议则实现了对内容的保护，即协议满足保密性。同时，发起方 A 和响应方 B 的身份是以密文的形式在信道中传递，因此身份保护是此协议保密性的拓展。对保密性和身份保护的验证可以被建模为安全属性查询：攻击者能否获得消息中的内容 Nb、ID_a 和 ID_b。该验证在自动化工具 ProVerif 下完成，查询（query）以下事实是否成立：

query attacker:Nb.

query attacker:ID_a.

query attacker:ID_b.

输出结果如图 2 所示。由图 2 可知，ProVerif 的输出结果为 true，表明即使在主动攻击模式下，攻击者也无法获得跨域两方密钥协商过程中传递消息的内容 Nb、ID_a 和 ID_b，即该协议能够满足保密性，同时实现了对发起方和响应方身份的保护。

3.3 协议的认证性

响应方 B 对发起方 A 的认证性：如果响应方接收了协商出的共享会话密钥，则发起方必定发起了该协商，并且所声称的身份是真实的。发起方 A 对响应方 B 的认证性：如果发起方基于协商出的安全参数建立了安全连接，则响应方已接收协商出的共享密钥，且所声称的身份是真实的。

该协议认证性的证明通过自动化工具 ProVerif 完成，查询语句如下：

query ev:BfinishedA(k)⇒ev:BverifA(ID_a).

query ev:AfinishedB(k)⇒ev:AverifB(ID_b)

&(ev:BfinishedA(k)⇒ev:BverifA(ID_a)).

输出结果如图 3 所示。由图 3 可知，ProVerif 的输出结果为 true，表明跨域的通信双方互相确认了对方的身份，该协议满足认证性。

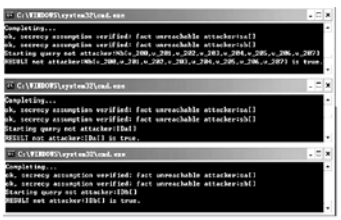

图2 协议的保密性与身份保护验证结果

图3 协议的认证性验证结果

4 性能分析与比较

协议的性能主要从信息交换的次数、执行运算的复杂度及安全属性等方面来考虑。

从表 1 可以看出,新方案与文献[11]中方案相比解决了密钥托管问题,与文献[12]中方案相比减少了二次双线性对乘法运算和二次标量乘运算,用较小的通信开销和计算开销实现了协议安全性。

表 1　各方案性能比较

性能	方案		
	文献[11]方案	文献[12]方案	本文方案
消息发送条数	2	4	3
双线性对运算	4	4	4
ECC 标量乘运算	2	4	2
双线性对乘法运算	0	2	0
密钥托管问题	×	√	√
身份主动保护	×	×	√

5　结束语

本文提出了一个基于无证书的两方跨域密钥协商协议,通过较小计算量,解决了传统的基于身份的两方跨域密钥协商协议的密钥托管问题,实现了显式身份认证和通信双方身份的保护。采用形式化分析证明了协议的安全性,下一步将研究其性能优化和实际应用。

参考文献

[1] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Lecture Notes in Computer Science, vol 2894. Berlin: Springer-Verlag, 2003: 452-473.

[2] WANG Sheng-bao, CAO Zhen-fu, WANG Li-cheng. Efficient certificateless authenticated key agreement protocol from pairings[J]. Wuhan University Journal of Natural Sciences, 2006, 11(5): 1278-1282.

[3] MANDT T K, TAN C H. Certificateless authenticated two-party key agreement protocols[C]//Lecture Notes in Computer Science, vol 4435. Berlin: Springer-Verlag, 2008: 37-44.

[4] SHI Yi-juan, LI Jian-hua. Two-party authenticated key agreement in certificateless public key cryptography[J]. Wuhan University Journal of Natural Sciences, 2007, 12(1): 71-74.

[5] WANG Sheng-bao, CAO Zhen-fu, BAO Hai-yong. Efficient certificateless authentication and key agreement (CL-AK) for grid computing [J]. International Journal of Network Security, 2008, 7(3): 342-347.

[6] 朱志馨,董晓蕾. 高效安全的无证书密钥协商方案[J]. 计算机应用研究,2009,26(12):4787-4789.

[7] 侯孟波,徐秋亮,蒋瀚. 构建无证书的两方认证密钥协商协议[J]. 计算机工程与应用, 2010,46(8):1-4.

[8] 舒剑. 一种实用的无证书两方认证协议[J] 小型微计算机系统, 2010,31(9):1889-1893.

[9] KUDLA C. Identity-based authenticated key agreement protocols from pairings, Report 2002/184[R]. 2003: 219-233.

[10] KIM S, LEE H, OH H. Enhanced ID-based authenticated key agreement protocols for a multiple independent PKG environment[C]//Lecture Notes in Computer Science, vol3783. 2005: 323-335.

[11] LEE H, KIM D, KIM S, *et al*. Identity-based key agreement protocols in a multiple PKG environment[C]//Lecture Notes in Computer Science, vol3483. 2005: 877-886.

[12] 陈家琪,冯俊,郝妍. 无证书密钥协商协议对跨域 Kerberos 的改进[J]. 计算机工程,2010,36(20):150-152.

[13] 赵华伟,李大兴. 密钥交换协议的安全性分析[J]. 山东大学学报:理学版,2006,41(4):101-106.

(上接第 645 页)则 B 首先在 List 中查找,若 $ID_i \in List$,则找出对应的公钥 P_i,否则 B 随机选择一个 $l_i \in Z_q^*$ 计算 $P_i = l_i sg = l_i P_{pub}$,并将$(ID_i, l_i, P_i)$存储到列表 List 中,返回 P_i 作为对 ID_i 的公钥询问回答。

秘密值询问。当 F 询问用户 ID_i 的秘密值时,若 $ID_i \neq ID^*$,则 B 在 List 中查找,若 $ID_i \in List$,则 B 返回相应的 l_i;若 $ID_i \notin List$,则 B 向自身对 ID_i 作公钥询问,并返回 l_i。若 $ID_i = ID^*$,则 B 终止对 F 的询问回答。最终,F 输出一个签名者集合对任意选择的消息 M^* 的伪造签名 σ^*。由签名的验证式,B 可以得到 $\hat{e}(g,\sigma) = \hat{e}(pk_L, H_2(M)) = \hat{e}(\prod_{i=1}^{n}(pk_i), H_2(M)) = \hat{e}(sbg \prod_{i=2}^{n}(l_i ag), ag) = \hat{e}(sabg \prod_{i=2}^{n}(l_i bg), g)$,从而 $\sigma^* = sabg \prod_{i=2}^{n}(l_i bg)$,于是解得 $abg = \sigma / s\prod_{i=2}^{n} l_i bg$,即 B 成功地解决了 CDH 问题。秘密值询问不终止的概率为 $(u_{pk}-1)/u_{pk} \cdots (u_{pk}-u_x)/(u_{pk}-u_x+1) = (u_{pk}-u_x)/u_{pk}$,而 F 成功伪造签名的概率是 ε,于是 B 成功解决 CDH 问题的概率为 $\varepsilon' \geq (u_{pk}-u_x)\varepsilon/u_{pk}$。

3.3　效率分析

将本方案与其他方案进行比较。比较需要的符号说明如下:BP 为双线性对;PA 为 G_1 内的加法;E 为 G_1 内的乘法;H 为哈希函数;N 为签名者数目。

表 1 说明本文方案的效率高于文献[6,8]方案的效率,在密钥托管问题上优于文献[5]的方案。

表 1 效率比较

方案	签名算法	验证算法	密钥托管问题
文献[6]	N(1H+1E+1PA)	N(2H+2E)+(N+1)BP	否
文献[5]	N(1H+2E)	1H+NE+2BP	是
文献[8]	N(3H+3E)	N(4H+E)+4BP	否
本文	N(1H+2E+1PA)	1H+NE+2BP	否

4　结束语

本文结合多重签名的优点和无证书密码体制的优势的无证书多重签名方案在 CDH 困难假设下是存在性不可伪造的,效率更优。

参考文献:

[1] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Lecture Notes in Computer Science, vol 2894. Berlin: Springer, 2003: 452-473.

[2] ITAKURA K, NAKAMUPA K. A public key cryptosystem suitable for digital multisignatures [J]. NEC Research & Develepment, 1983, 71: 1-8.

[3] MICALI S, OHTA K, REYZIN L. Accountable sub group multisignatures[C]//Proc of the 8th ACM Conference on Computer and Communications Security. New York: ACM, 2001: 245-254.

[4] BOLDYREVA A. Threshold signature, multisig nature and blind signature schemes based on the gap Diffie-Hellman-group signature scheme[C]//Lecture Notes in Computer Science, vol 2567. Berlin: Springer, 2003: 31-46.

[5] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[J]. Journal of Cryptology, 2004, 17(4): 297-319.

[6] 梁红梅,黄慧,吴晨煌. 无证书多重签名[J]. 集美大学学报,2008, 13(2):127-131.

[7] 丁薇,张建中. 一种新的多重代理多重数字签名方案[J]. 计算机应用研究,2010,27(8):81-82.

[8] 张玉磊,王彩芬. 高效的无证书并行多重签名方案[J]. 计算机应用,2010,30(12):3337-3340.