一种高效的无证书多重签名方案 *

冯 蕾[a], 彭长根[b], 彭延国[a]
(贵州大学 a. 计算机科学与信息学院; b. 理学院, 贵阳 550025)

摘 要: 为了满足多个人对同一份文件签名的高效性,将无证书密码体制与多重签名方案相结合,提出一种高效的无证书多重签名方案。该方案有效地削弱了可信第三方的权力,并且被证明了在适应性选择消息攻击下是存在性不可伪造的,其安全性基于 CDH 问题的困难假设。与现有方案相比,该方案需要计算的双线性对计算次数少,降低了系统开销。

关键词: 无证书密码学; 多重签名; 不可伪造性; 双线性对
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2012)02-0644-02
doi:10.3969/j.issn.1001-3695.2012.02.064

Efficient certificateless multi-signature scheme

FENG Lei[a], PENG Chang-gen[b], PENG Yan-guo[a]
(*a. Dept. of Computer Science & Technology, b. Dept. of Mathematics, Guizhou University, Guiyang* 550025, *China*)

Abstract: In order to meet the high efficiency of the multi-signature, by combining certificateless cryptosystem with the multi-signature scheme, this paper proposed an efficient certificateless multi-signature scheme. The scheme was weaken the power of the trusted third party and proved existing unforgeability under the adaptive chosen message attack. The security of the scheme was based on the fact that computational Diffie-Hellman problem was hard. Compared with existing schemes, the scheme need calculate less bilinear pairing and reduce the system costs.

Key words: certificateless cryptography; multi-signatures; unforgeability; bilinear pairing

2003 年亚洲密码学会上,Al-Riyami 等人[1]首次提出无证书密码体制,该体制有效地解决了传统密码体制和基于身份密码体制中密钥托管和证书管理的问题。其效率高于传统的公钥密码体制,安全性强于基于身份的公钥密码体制,成为近几年来的研究重点。随着无证书密码体制的提出,出现了许多无证书签名方案。

多重签名的概念是由 Itakura 等人[2]提出的,是指多个签名者共同对同一个消息进行签名,任何人可以对签名的有效性进行验证,其优点是签名长度与签名人数无关。1994 年,Harn 等人基于 ELGamal 签名构造了一个只能应用于广播签名环境中的多重签名方案。2001 年,Micali 等人[3]给出了多重签名的正式定义和具体方案,该方案可以防止签名者作弊,但方案的效率不高。2003 年,Boldyreva 等人[4]基于 BLS 签名方案[5]首次提出了签名者间无须交互的多重签名方案。之后,Lu 等人于 2006 年首次提出了无随机预言机模型下可证明安全的多重签名方案,并进行了安全性证明。同年,Komano 等人给出了多重签名的安全定义和敌手模型,构造了一个多重签名方案,并对安全性进行了证明。以上方案都是基于传统的公钥密码体制。2008 年,梁红梅等人[6]首次将无证书公钥密码体制与多重签名相结合,提出了无证书多重签名的概念及安全模型,并基于双线性对构造了一个具体的无证书多重签名方案。在随机预言机模型下,证明了其方案在 CDH 困难假设下的安全性,但该方案需要计算的双线性对次数较多。2010 年,丁薇等人[7]给出了一个多重代理的多重签名方案。之后,张玉磊等人[8]设计了一个并行的多重签名方案,但需四次双线性对运算。基于此,本文提出了一种高效的无证书多重签名方案,在验证阶段只需两次双线性对运算,并证明了其在 CDH 问题困难性假设下满足存在性不可伪造。

1 预备知识

1.1 双线性对

G_1、G_2 分别是两个阶为 q 的乘法循环群和加法循环群,映射 $\hat{e}: G_1 \times G_1 \to G_2$ 称为双线性映射,满足以下条件:

a)双线性。若 $P, Q \in G_1$,对 $\forall a, b \in z_q$ 则满足 $\hat{e}(P^a, Q^b) = \hat{e}(P, Q)^{ab}$。

b)非退化性。存在着 $P \in G_1$,使得 $\hat{e}(P, P) \neq 1$。

c)可计算性。$P, Q \in G_1$,存在一个有效的方法计算 $\hat{e}(P, Q)$。

1.2 Diffie-Hellman(CDH)

已知(P, aP, bP),计算 abP,其中 $a, b \in Z_q^*$ 是未知的。

2 无证书多重签名方案(CLMS)

$L = \{P_1, P_2, \cdots, P_n\}$ 是 n 个签名者集合,params 是公共参数。无证书多重签名的算法由以下几部分组成:CLMS = (PMK, MK, MS, MV)。PMK 算法是输入公共参数 params,输出部分公私钥对;MK 算法是输入公共参数 params 和部分公私钥

收稿日期: 2011-07-16; **修回日期**: 2011-08-17 **基金项目**: 国家自然科学基金资助项目(60963023); 贵州省自然科学基金资助项目(2009-2113); 贵州省高层次人才特助经费项目(TZJF-2008-33); 贵州大学研究生创新基金资助项目(校研理工 2011037)

作者简介: 冯蕾(1987-),女(苗族),贵州道真人,硕士研究生,主要研究方向为密码学与可信计算; 彭长根(1963-),男,教授,硕导,博士,主要研究方向为密码学与信息安全(peng_stud@163.com); 彭延国(1986-),男,硕士研究生,主要研究方向为密码学与可信计算.

对,输出公私钥对(pk,sk),对每个签名者$P_i \in P$运行算法 MK 得到公私钥对(pk_i,sk_i);MS 算法是对于任意一个签名者集合 L、消息 M、公共参数 params 和签名者私钥 sk_i,输出三元组 $T=(M,L,\sigma)$,其中 σ 是对消息 M 的签名;验证算法 MV 是根据公钥和三元组 T 验证签名是否有效。无证书多重签名有以下几个步骤:

a)生成系统参数。G_1、G_2 分别是两个阶为 q 的乘法循环群和加法循环群,g 是 G_1 的一个生成元,$P=|G_1|$,hash 函数 $H_1:\{0,1\}^* \to Z_q^*$,$H_2:\{0,1\}^* \to G_1$。主密钥 $s \in Z_q^*$。公共参数$(G_1,G_2,q,g,P_{\text{pub}},H_1,H_2)$。

b)部分私钥生成算法(PMK)。根据用户的身份 $ID_i \in \{0,1\}^*$,按照以下步骤得到用户的部分私钥:

(a)计算 $Q_i=H_1(ID_i)$;

(b)输出部分私钥 $D_i=sQ_i$。

c)公私钥对生成算法(MK)。用户 ID_i随机选择一个秘密值 $x_i \in Z_q^*$,结合部分私钥 D_i,按如下步骤计算公私钥对:

(a)计算私钥 $sk_i=D_i+x_i$;

(b)计算公钥 $pk_i=g^{D_i+x_i}$。

d)签名算法(MS)。对任意的签名者 $P_i \in P$,利用私钥 $sk_i=D_i+x_i$ 对消息 M 进行签名 $\sigma_i=H_2(M)^{D_i+x_i}$。若有 n 个签名者对其进行多重签名,签名者集合 $L=\{P_1,\cdots,P_n\}$,计算多重签名 $\sigma=\prod_{i=1}^{n}\sigma_i$,最后输出三元组 $T=(M,L,\sigma)$。

e)验证算法(MV)。验证者收到三元组 $T=(M,L,\sigma)$,根据签名者集合 $L=\{P_1,\cdots,P_n\}$ 得出相应的公钥集合 $L=(pk_1,\cdots,pk_n)$,其中 $pk_i=g^{D_i+x_i}$,$i \in L$。验证者计算 $pk_L=\prod_{i=1}^{n}(pk_i)=\prod_{i=1}^{n}(g^{D_i+x_i})$,输出 VDDH$(g,pk_l,H_2(M),\sigma)$。验证通过,则说明签名有效;否则终止。

3　方案分析

3.1　正确性分析

因为 $\hat{e}(pk_L,H_2(M))=\hat{e}(\prod_{i=1}^{n}pk_i,H_2(M))=\hat{e}(\prod_{i=1}^{n}g^{D_i+x_i},H_2(M))=\hat{e}(g^{\sum_{i=1}^{n}D_i+x_i},H_2(M))=\hat{e}(g,H_2(M))^{\sum_{i=1}^{n}D_i+x_i}$,又 $\hat{e}(g,\sigma)=\hat{e}(g,\prod_{i=1}^{n}\sigma_i)=\hat{e}(g,\prod_{i=1}^{n}H_2(M)^{D_i+x_i})=\hat{e}(g,H_2(M)^{\sum_{i=1}^{n}D_i+x_i})=\hat{e}(g,H_2(M))^{\sum_{i=1}^{n}D_i+x_i}$,即 $\hat{e}(pk_L,H_2(M))=\hat{e}(g,\sigma)$。正确性得证。

3.2　安全性分析

根据无证书签名的特点,有以下两种敌手模型:

类型Ⅰ　敌手 $A_Ⅰ$ 不能获得系统主密钥,但可通过选择一个新的值替换用户的公钥,同时 $A_Ⅰ$ 可以进行多项式次适应性公钥询问、公钥替换、部分私钥询问。其中 ID^* 是给定的挑战者,P^* 是挑战者公钥。

类型Ⅱ　敌手 $A_Ⅱ$ 拥有系统主密钥,但不能替换用户的公钥,同时 $A_Ⅱ$ 可以进行多项式次适应性秘密值询问、公钥询问。一个无证书多重签名方案对适应性选择消息攻击是存在性不可伪造的,当且仅当在上述两种攻击下是安全的。

定理 1　在随机预言机模型下,若适应性选择消息攻击下敌手Ⅰ能够以 ε 的概率攻破方案,则存在另一个算法能够以 $\varepsilon' \geqslant (\mu_H-\mu_{pmk})\varepsilon/\mu_H$ 的概率解决 CDH 问题。其中,μ_H、μ_{pmk}分别是敌手作 H_1 询问和部分私钥询问的次数。

证明　设 F 是提出的签名方案的第一类型攻击者,它可以替换任何用户的公钥。F 从签名者成员集合 L 中任意选取 n 个人作为无证书多重签名的签名者,其中每个用户对应的公钥分别为 P_i。可以构造一个算法 B,它能够利用 F 的伪造签名来解决 CDH 问题。

B 通过维护 List 和 H-List 两个列表来回答 F 的预言机询问,其中,List 包括(ID_i,l_i,P_i),l_i 表示用户的秘密值,P_i 表示对应的公钥;H-List 包括(D_i,r_i,P_i,h_i),r_i 表示随机选取的数,h_i 代表对(ID_i,P_i)进行 H_1 询问后的 hash 值,D_i 表示部分私钥,模拟开始阶段两个列表初始化为空。

系统参数建立。首先 B 设 $P_{\text{pub}}=bg$,选择 $l \in Z_q^*$,计算挑战用户 ID^* 的公钥 $P^*=lP_{\text{pub}}=lbg$,然后将系统公开参数$(G_1,G_2,q,g,P_{\text{pub}},H_1,H_2)$及挑战公钥 P^* 发送给 F。

H_1 询问。当 F 对 ID_i 作 hash 值询问时,若 $ID_i \neq ID^*$,则 B 首先在 H-List 中查找,若 $ID_i \in H$-List,则返回相应的 h_i 给 F,若 ID_i 不属于 H-List,则随机选择 $r_i \in Z_q^*$ 计算 $h_i=r_iP=H_1(M)$,并返回 h_i;若 $ID_i=ID^*$,则令 $h_i=ag$,并将相应的值存储到列表 H-List 中,返回 h_i 作为 ID_i 的 hash 值询问回答。

公钥询问。当 F 询问用户 ID_i 的公钥时,则 B 首先在 List 中查找,若 $ID_i \in$ List,则得到相应的公钥 P_i,否则随机选择 $l_i \in Z_q^*$ 计算 $P_i=l_iP_{\text{pub}}=l_ibg$,并将$(ID_i,l_i,P_i)$存储到列表 List 中,返回 P_i 作为 F 对 B 的公钥询问回答。

公钥替换询问。当 F 自己产生一个 P'_i 来替换用户 ID_i 的公钥时,则 B 在 List 中查找,若 $ID_i \in$ List,则用$(ID_i,\perp,P'_i)$替换已有记录,否则,B 在 List 中增加记录$(ID_i,\perp,P'_i)$。

秘密值询问。当 F 询问用户 ID_i 的秘密值时,B 在 List 中查找,若 $ID_i \in$ List,且 $l_i \neq \perp$,则 B 返回相应的 l_i;若 $ID_i \in$ List,且 $l_i=\perp$,则 B 返回相应的 $\perp$,这种情况说明公钥被替换,若 $ID_i \notin$ List,则 B 向自身作公钥询问,并返回 l_i。

部分私钥询问。当 F 对 ID_i 作部分私钥询问时,若 $ID_i \neq ID^*$,则 B 先在 H-List 中查找,若 $ID_i \in$ List,则返回对应的值 D_i,否则,B 选择 $r_i \in Z_q^*$ 计算 $D_i=r_ibg=sH_1(ID_i)$,将相应的值存入到列表 H-List 中,并返回 D_i 给 F。若 $ID_i=ID^*$,则 B 终止对 F 的询问回答。

对预言机 H_2 的询问方法类似对随机预言机 H_1 的模拟。通过上面各种询问的模拟,相应的签名可以很容易模拟出来。最终,B 可以得到 F 关于消息 M^* 的一个伪造签名,记为(M^*,σ^*,L^*),其中 $ID^* \in L^*$。设 $ID^*=ID_1^*$,则 B 通过验证方程可以得到 $\hat{e}(g,\sigma^*)=\hat{e}(pk_L,H_2(M))=\hat{e}(\prod_{i=1}^{n}(pk_i),H_2(M))=\hat{e}(\prod_{i=1}^{n}l_ibg,ag)=\hat{e}(a\prod_{i=1}^{n}l_ibg,g)$,从而 $\sigma^*=a\prod_{i=1}^{n}l_ibg=ablg\prod_{i=2}^{n}l_ibg$,于是解得 $abg=\sigma/l\prod_{i=2}^{n}l_ibg$,即 B 成功地解决了 CDH 问题。部分私钥询问不终止的概率为$(\mu_H-1)/\mu_H\cdots(\mu_H-\mu_{pmk})/(\mu_H-\mu_{pmk}+1)=(\mu_H-\mu_{pmk})/\mu_H$,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 $\varepsilon' \geqslant (q-\mu_{pmk})\varepsilon/q$。

定理 2　在随机预言机模型下,若适应性选择消息攻击下敌手Ⅱ能够以 ε 的概率攻破方案,则存在另一个算法能够以 $\varepsilon' \geqslant (u_{pk}-u_x)\varepsilon/u_{pk}$的概率解决 CDH 问题。其中,$u_{pk}$、$u_x$ 分别是敌手作公钥询问和秘密值询问的次数。

证明　设 F 是无证书多重签名方案的第二型攻击者,它拥有系统主密钥,但不能替换用户的公钥。下面构造算法 B 来解决 CDH 问题。首先,B 随机选择 $s \in Z_q^*$,并计算挑战用户 ID^* 的公钥 $P^*=sbg$,然后将主私钥 s、系统参数$(G_1,G_2,q,g,P_{\text{pub}},H_1,H_2)$及挑战公钥 P^* 发送给 F,其中 $P_{pub}=sg$。

H1 询问。B 用定理 1 中的方法来对 F 的询问作出回答。

公钥询问。当 F 询问用户 ID_i 的公钥时,

(下转第 649 页)

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。

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。

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

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.