文章编号：1671-1742(2011)02-0149-06

一个基于身份和双线性对的多签名方案

陈泗盛[1]， 许 力[2]
(1.福建师范大学福清分校数学与计算机科学系，福建 福清 350300；2.福建师范大学网络安全与密码技术实验室，福建 福州 350007)

摘要：针对已提出的多签名方案不适用于基于双线性对的身份密码系统的情况，分析了一些特定应用环境对多签名思想和身份密钥系统的有着共同的需求，在Hess等人提出的数字签名方案的基础上，运用Harn等人构造多签名的方法构造出了一个适用于身份密码系统的基于身份和双线性对的多签名方案。并通过相关定理给出方案的正确性和安全性分析。

关 键 词：信息安全；数字签名；多签名方案；身份；双线性对
中图分类号：TP393 文献标识码：A

1 引言

数字多签名方案是允许多个签名者对同一消息共同签名，生成单一固定大小的签名数据，使验证者可以像一般的数字签名方案一样确认签名有效性的一类签名方案。1994年Harn等提出了一个基于离散对数问题的多签名方案[1]，正式的定义是在文献[2]中给出的。近年来，多签名方案的研究越来越受关注[1-5]，但现有的研究大多关注于基于身份的多签名方案。论文将从两个方面考虑提出一个基于身份和双线性对的多签名方案。

一方面，数字多签名的思想类似于门限签名方案，在门限签名方案中，一个签名结果是由一组签名者共同参与产生的，参与者的个数要大于或者等于预先设定的门限。但是二者存在着区别，多签名方案和门限或者组签名的最大区别就是，后者的签名者是预先选定好的，在应用过程中签名者群组是无法更改的；而在多签名方案应用中，签名者组可以由任意的签名者动态组成。另一方面，由于多签名方案可以将多个签名者对同一消息生成的多个签名变为一个固定长度的签名数据进行保存，而无须将每个签名者生成的签名单独保存；在验证的时候，只需验证一次便可确认多个签名者对同一消息进行了签名。因此，多签名方案节约节点的存储空间和减少节点验证签名的时间。多签名的这种动态性及节约资源的性质在资源有限的动态Ad Hoc网络中将有着广泛的应用，如在设计安全路由和安全数据发送协议，密钥管理，动态组通信等方面。

近年来双线性对在构造密码算法中获得到了广泛的应用。特别是在基于双线对的密码系统中，两个节点用户之间可以在不交换信息的情况下通过双方的身份ID(Identity)计算出双方之间的一个秘密共享密钥。另一方面，双线性对大多是在椭圆曲线上构造的，而在同等安全级别的情况下椭圆曲线上的密钥长度要小的多，这又可以降低密码算法的计算复杂度。因此，基于双线性对的密码系统在资源有限的网络中有着广泛的应用，如近年非常热门的自自组织网络，传感器网络和mesh网络等。

因此，为了集成多签名的特性和双线性对的应用优势，将在Hess签名方案[6]的基础上应用Harn等提出的基于RSA的多签名方案[5]构造思想设计一个有效的基于身份和双线对的多签名方案，该多签名方案能和身份密码系统及基于双线性对的密码系统兼容，使得多签名方案能有着更广泛的应用。

2 相关知识回顾

2.1 双线性映射及困难问题假设

双线性映射(Bilinear pairings)是构造基于身份的加密方案和签名方案的重要工具，通常是利用椭圆曲线和超椭圆曲线上的Weil对(Weil pairing)和Tate对(Tate pairing)[7]进行构造，其基本思想如下：

收稿日期：2011-04-13
基金项目：国家自然科学基金资助项目(61072080)

假设 G_1 是一个由 P 生成的循环加法群,它的阶是 q,G_2 是一个阶为 q 的循环乘法群,则双线性对是映射 $e:G_1\times G_1\rightarrow G_2$,满足以下性质:

(1)双线性:$\forall P,Q\in G_1,\forall a,b\in Z_q^*$,都有 $e(aP,bQ)=e(P,Q)^{ab}$,即 $\forall P,Q,R,S\in G_1$,都有 $e(P+Q,R+S)=e(P,R)\cdot e(P,S)\cdot e(Q,R)\cdot e(Q,S)$;

(2)非退化性:$\exists P,Q\in G_1$,使得 $e(P,Q)\neq 1$;

(3)可计算性:对于任意 $P,Q\in G_1$,存在着一个有效的算法计算 $e(P,Q)$。

下面,介绍在群 G_1 上的4个困难问题假设:

(1)椭圆曲线离散对数问题(Elliptic Cure Discrete Logarithm Problem, ECDLP):G_1 上的椭圆曲线上的两个离散点 P,Q,计算 a,使得满足 $aP=Q$;

(2)计算 Diffie-Hellman 问题(Compute Diffie-Hellman Problem, CDHP):随机给定一个三元组 $<P,aP,bP>\in G_1$,其中 $a,b\in Z_q^*$,计算 abP。

(3)双线性 Diffie-Hellman 问题(Bilinear Diffie-Hellman Problem, BDHP):随机给定一个四元组 $<P,aP,bP,cP>\in G_1$,其中 $a,b,c\in Z_q^*$,计算 $e(P,P)^{abc}$。

(4)反向双线性映射问题(Paring Inversion Problem, PIP):给定 $P\in G_1$ 和 $s\in G_2$,找到 $Q\in G_1$,满足 $e(P,Q)=s$。

2.2 Hess基于身份签名方案

Hess基于身份签名方案[6]由系统初始化、密钥生成、签名和验证4部分组成。系统中包括3方:可信中心(private key generator, PKG),签名者和验证者。下面给出 Hess 身份签名方案具体算法:

(1)系统初始化:PKG 选取生成元为 P,阶为 q 的循环加法群 G_1 和一个阶为 q 的循环乘法群 G_2,以及双线性对映射 $e:G_1\times G_1\rightarrow G_2$。选取主密钥 $s\in Z_q^*$,计算系统公钥 $Q_0=sP$。公开系统参数 $<G_1,G_2,e,P,q,Q_0,H_1,H_2>$,其中 $H_1:\{0,1\}^*\rightarrow G_1^*$,$H_2:\{0,1\}^n\times G_2\rightarrow Z_q^*$。

(2)密钥生成:假设节点 A 的身份是 ID_A,那么 PKG 计算 $S_{ID_A}=sH_1(ID_A)$,则 A 的公钥为 ID_A,对应的私钥为 S_{ID_A};

(3)签名:假设 A 要对消息 m 进行签名,则签名过程如下:

①随机选取 $P_1\in G_1^*$,$k\in Z_q^*$;

②计算 $r=e(P_1,P)^k$;

③$v=H_2(m,r)$;

④$u=vS_{ID_A}+kP_1$,$<u,v>$即为 A 对消息 m 的签名结果。

(4)验证:假设验证者收到来自 A 的签名消息 $<m,u,v>$,则验证过程如下:

①计算 $r'=e(u,p)\cdot e(H_1(ID_A),-Q_0)^v$;

②验证等式 $v=H_2(m,r')$是否成立。如果成立,则签名验证成功,否则验证失败。

2.3 基于身份(Identity)的RSA的多签名方案

文献[2]第一次给出了多签名的正式定义。其一般模型可以描述为:给定一个可能的签名者群 $G=\{P_1,P_2,\cdots,P_L\}$,它们拥有共同的密码系统参数 $<P>$,即它们在相同的密码参数下获取了公钥密钥对 (PK_i,SK_i),$i=1,2,\cdots,L$,则多签名方案是指允许 G 的任何子群 S(即 $S\subseteq G$)的签名者使用私钥 SK_i 对一个消息 m 进行共同签名,签名结果记为 $<m,Sign_S(m)>$,验证者根据 S 的所有公钥对 $<m,Sign_S(m)>$ 进行验证。整个多签名方案一般分为4个步骤:(1)系统参数的生成;(2)多签名密钥的计算,即计算 (PK_i,SK_i),$i=1,2,\cdots,L$;(3)多签名算法;(4)多签名验证算法。多签名与群签名的最大区别在于,前者可以随时调整签名者的子群 S,不需要预先设定好。

一个高效的多签名方案应该满足下面两个特性[5]:

(1)固定的长度:是指多签名的签名结果的长度跟一般的单签名的结果应该是一样,不会因为签名者数的增加而增加。

(2)不变的验证时间:是指多签名的验证过程中涉及的运算复杂度要和单个签名者签名结果验证时的复杂度一样,不会随着签名者数目的增加而增加。

2008 年,Harn 等在 Shamir 的基于身份的签名方案和 RSA 签名方案的基础上的提出一个满足上面两个特性的多签名方案[5]。接下来将介绍该多签名方案的构造方法。

2.3.1　PKG 密钥生成

私钥生成中心(Private Key Generator, PKG)按照以下步骤生成公钥和私钥对

(1)选取两个大素数 p 和 q,计算 $n=pq$;

(2)选取一个随机数 e,满足 $\gcd(e,\varphi(n))=1$,e 作为 PKG 的公钥;

(3)计算 $d=e^{-1}\bmod\varphi(n)$,d 作为 PKG 的私钥。

2.3.2　多签名的生成

(1)签名密钥的生成

过程中,一个签名者 j 可以通过两个步骤从 PKG 中获取与之身份相对应的私钥:

①签名者 j 把自己的身份信息摘要,这里用 i_j 表示,发送给 PKG

②PKG 使用自己的私钥 d,做如下运算:

$$g_j=i_j^d \bmod n$$

并通过安全信道发送给签名者 j,签名者把 i_j 作为自己的公钥,g_j 是与之对应的私钥,即公开 i_j,保密 g_j。

(2)签名算法

每个签名参与者根据以下算法共同产生对消息 m 的基于身份的多签名结果:

①签名者 j 选取一个随机数 r_j,然后计算

$$t_j=r_j^e \bmod n;$$

②每个签名参与者把自己计算的 t_j 广播给其他签名参与者;

③每个签名者 j 收到所有的 t_j,$j=1,2,\cdots,l$(假设最终共有 l 个签名者参与签名),然后进行两个计算:

$$t=\prod_{j=1}^{l} t_j \bmod n \text{ 和 } s_j=g_j\cdot r_j^{H(t,m)} \bmod n;$$

④每个签名参与者 j 广播 s_j 给其它签名参与者;

⑤当收到所有的 s_j,$j=1,2,\cdots,l$,计算

$$s=\prod_{j=1}^{l} s_j \bmod n$$

最终,输出消息 m 的多签名结果 $\sigma=(t,s)$。方案的安全性分析见文献[6]。

2.3.3　验证算法

当验证者获得消息 m 的签名结果 $\sigma=(t,s)$,并知道这个多签名的签名者的身份是 $i_1,i_2,\cdots,i_l$,同时也获得了 PKG 的公钥 e,则其可以通过验证等式

$$s^e=(i_1\cdot i_2\cdot\cdots\cdot i_l)\cdot t^{H(t,m)} \bmod n$$

是否成立来验证签名的有效性。如果等式成立,则签名有效,否则签名无效。方案的安全性分析详见文献[5]。

3　基于双线性对的多签名方案 IBPMS

在 Hess 签名方案的基础上,借鉴基于 RSA 的多签名方案构造的思想设计一个基于身份和双线性对的多签名方案 IBPMS(Identity and Bilinear Paring based Multi-signature Scheme),从而集成双线对和多签名的优点。下面按照 RSA 的多签名方案的描述步骤来介绍一下多签名方案。

3.1　PKG 密钥的生成

PKG 选取生成元为 P 阶为 q 的循环加法群 G_1 和一个阶为 q 的循环乘法群 G_2,以及双线性对映射 $e:G_1\times G_1\to G_2$。选取主密钥 $s\in Z_q^*$,计算系统公钥 $Q=sP$,并选定哈希函数,$H_1:\{0,1\}^n\to G_1$,$H_2:\{0,1\}^n\times G_2\to Z_q^*$。

公开系统参数$<G_1,G_2,e,P,q,n,Q,H_1,H_2>$。

3.2 用户私钥的生成

假设节点用户 i 的身份信息为 ID_i,并将此身份信息作公钥,用户 i 从 PKG 获得相对应的私钥的步骤为:

(1)用户 i:发送自己的身份消息 ID_i 给 PKG;

(2)PKG:计算 $S_i=sH_1(ID_i)$,并将其通过安全信道发送给节点用户 i;

(3)用户 i 将 S_i 作为私钥,ID_i 作为公钥公开。

3.3 多签名结果的生成

假设共有 l 个节点用户$\{ID_1,ID_2,\cdots,ID_l\}$要对消息 m 进行共同签名,每个节点都进行如下操作共同产生签名结果。

(1)每个签名节点随机选取一个数 $r_i\in Z_q^*$;

(2)每个签名节点计算 $t_i=e(P,Q)^{r_i}$,并将 t_i 广播给其它签名节点;

(3)当每个签名节点收到所有的 t_i,$1\leqslant i\leqslant l$,计算 $t=\prod_{i=1}^{l}t_i$;

(4)计算 $v=H_2(m,t)$,$u_i=vS_i+r_iQ$,并将 u_i 发送给其它签名节点;

(5)当每个签名节点收到所有 u_i,$1\leqslant i\leqslant l$,计算 $u=\sum_{i=1}^{l}u_i$

(6)$<u,v>$即为签名者组$\{ID_1,ID_2,\cdots,ID_l\}$对消息 m 的共同签名结果。

3.4 多签名的验证

当节点用户 Bob 收到消息$<m,u,v>$,可以利用所有签名节点的身份信息即公钥$\{ID_1,ID_2,\cdots,ID_l\}$对签名结果进行验证,验证步骤如下:

(1) Bob 计算 $ID=\sum_{i=1}^{l}H_1(ID_i)$

(2) Bob 计算 $t'=e(u,P)\cdot e(ID,Q)^{-v}$

(3) 验证等式 $v=H_2(m,t')$是否成立。如果成立,则签名验证成功,即相信$<u,v>$为节点组$\{ID_1,ID_2,\cdots,ID_l\}$对消息 m 的签名结果,否则验证失败。

4 IBPMS 方案的正确性与安全性分析

对比 Hess 签名方案和 IBPMS 多签名方案的签名结果和验证等式,可以得出 IBPMS 满足 2.3 节提出的两个特性。因此在这一部分只需要证明方案的正确性和安全性。

4.1 多签名方案的正确性分析

这里将证明多签名方案的正确性,即在签名验证过程中验证者能正确恢复出参数 t。下面以定理的形式给出 t'的完全计算过程。

定理 1 在 IBPMS 方案中 $H_2(m,t')=v$。

证明:因为,

$$\begin{aligned}e(ID,Q)^{-v}&=e(\sum_{i=1}^{l}H_1(ID_i),Q)^{-v}\\&=e(\sum_{i=1}^{l}H_1(ID_i),sP)^{-v}\\&=e(\sum_{i=1}^{l}sH_1(ID_i),P)^{-v}\\&=e(\sum_{i=1}^{l}S_i,P)^{-v}\end{aligned}$$

$$= e\left(\sum_{i=1}^{l} S_i, P\right)^{-v}$$

$$= e\left(-v\sum_{i=1}^{l} S_i, P\right)$$

且, $e(u,P) = e\left(\sum_{i=1}^{l} u_i, P\right) = e\left(\sum_{i=1}^{l} vS_i + \sum_{i=1}^{l} r_i Q, P\right)$

所以, $t' = e(u,P)e(S,Q)^{-v} = e\left(\sum_{i=1}^{l} r_i Q, P\right) = \prod_{i=1}^{l} e(P,Q)^{r_i} = t$

从而, $H_2(m,t') = H_2(m,t) = v$。证毕。

由上面定理知,在验证过程中,可以正确恢复出参数 t,因此在验证过程中可以有效地验证签名结果的正确性,即签名方案是满足正确性的。

4.2 多签名方案的安全性分析

首先,方案采用 Harn 等的提出的 RSA 多签名方案的思想对 Hess 签名方案的进行扩展,因此方案的结构上的安全性可以由 Hess 签名方案的结构安全性来保证,Hess 签名方案安全性详见文献[6]。这里同 RSA 多签名方案一样,主要分析多签名特性的安全性。

定理 2　IBPMS 多签名方案能抗选择明文攻击。

证明:要证明 IPBMS 方案能抗选择明文攻击,即证明攻击者不能伪造出签名组$\{ID_1, ID_2, \cdots, ID_l\}$的对某个消息 m 签名结果$<u', v'>$通过验证算法。在验证过程中核心的一步是满足等式 $-v\sum_{i=1}^{l} S_i + u = \sum_{i=1}^{l} r_i Q$,即 $-\sum_{i=1}^{l} vS_i + \left(\sum_{i=1}^{l} vS_i + \sum_{i=1}^{l} r_i Q\right) = \sum_{i=1}^{l} r_i Q$。所以要进行选择明文攻击必须伪造出$<S', v'>$满足 $-\sum_{i=1}^{l} v'S_i + v'S' = 0$。

其中, $v = H(m,t)$,有进行 hash 函数运算,同时验证中有 $v = H_2(m,t')$,因此由 hash 的单向性的知参数 v 不能任意选取,从而没有办法伪造,即 $v' = v$。从而只能考虑伪造 S',满足 $-\sum_{i=1}^{l} S_i + S' = 0$。因为, $\sum_{i=1}^{l} S_i = sID$,所以,要伪造必须构造 $S' = -sID$。对于攻击者来说,只知道 v 和 ID。而在知道 v 和 ID 下想构造出 $S' = -sID$ 等价于能计算出 s。Hess 签名方案证明中,在知道 P, Q 下计算 s 是椭圆曲线上的离散对数问题,是一个困难问题。综上可以说明 IBPMS 多签名方案能抵抗选择明文攻击的。证毕。

下面将讨论一个针对多签名方案的安全攻击,叫做自适应选择身份(ID)攻击。所谓的自适应选择身份 ID 攻击,是指一组合法签名者组成员通过调整自己的身份 ID 并向 PKG 获取相应的私钥,从而伪造另一签名者组的消息签名[5]。下面通过一个定理说明提出的方案是抗自适应选择身份 ID 攻击的。

定理 3　IBPMS 多签名方案能抗自适应选择身份 ID 攻击。

证明:假设一组攻击者想伪造签名者组$\{ID_1, ID_2, \cdots, ID_l\}$的对消息 m 的签名,只需调整自己的身份 ID 为$\{ID'_1, ID'_2, \cdots, ID'_l\}$,让其满足 $\sum_{i=1}^{l} H_1(ID_i) = \sum_{i=1}^{l} H_1(ID'_i)$,并通过 PKG 获得$\{ID'_1, ID'_2, \cdots, ID'_l\}$对应的私钥,这样就可以构造出$\{ID_1, ID_2, \cdots, ID_l\}$对消息 m 的签名。但是,在等式 $\sum_{i=1}^{l} H_1(ID_i) = \sum_{i=1}^{l} H_1(ID'_i)$ 中使用可单向 hash 函数,由 hash 函数的单向性可知,找一对 $x, y, x \neq y$ 使得 $H_1(x) = H_1(y)$在计算上是困难的。所以,攻击者注册得到满足条件的身份组$\{ID'_1, ID'_2, \cdots, ID'_l\}$在计算上是困难的。故,IBPMS 多签名方案能抗自适应选择身份 ID 攻击。证毕。

5　结束语

为满足特定的应用环境对基于身份和双线性对的多签名的需求,在 Hess 签名方案的基础上借鉴 RSA 多签名方案构造方法,提出一个基于身份和双线性对的多签名方案 IBPMS,方案能够应用在基于双线性对的身份密

码系统中,扩大多签名思想适用的系统环境。最后,分析了IBPMS方案的正确性和安全性。

参考文献:

[1] Harn L.. Group-oriented (t, n) threshold digital signature scheme and digital multisignature[C]. Proceeding of IEEE computers and digital techniques, 1994,141(5):307-313.

[2] Micalis, Ohtak, Reyzin L. Accountable subgroup multi-signatures:extended abstract[C]. Proceeding of ACM Conference on Computer and Communications Security, ACM Press,2001:245-254.

[3] Boldyreva A. Threshold signature, multisignatures, multisignatures and blind signatures based on gap-Difie-Hellman-group signature scheme[C]. Proceeding of Public Key Crypotgraphy, Springer, 2003:31-46.

[4] Lu S,Ostrovsky R,Sahai A,et al. Aggregate sequential signaturns and multi-signatures without random oracle [C]. Proceeding of EUROCRYPT, Springer,2006:465-485.

[5] Harn L. ,Ren J... efficient identity-based RSA multisignatures[J]. Computer and Security,2008,27:12-15.

[6] F. Hess. Efficient Identity Based Signature Schemes Based on Pairings [C]. In proceedings of SAC'02, London, UK, Springer-Verlag, 2003: 310-324.

[7] Han Jiawei, Kamber M. 数据挖掘:概念与技术 [M]. 北京:机械工业出版社,2001.

An Identity and Bilinear Paring Based Multi-signature Scheme

CHEN Si-sheng[1], XU Li[2]

(1. The Department of Maths and Computer Science, Fuqing breach of Fujian Normal University,Fuqing 350300,China;2. Key Laboratory of Network Security and Cryptology, Fujian Normal university,Fuzhou 350007,China)

Abstract: In view of that the proposed multi-signature schemes can't be employed in the identity based cryptography system, the thesis analyzed the necessity of integration of multi-signature and identity based cryptography. Then, based on the signature scheme proposed by Hess, with the method used by Harn et al to construct multi-signature scheme, the author proposed a multi-signature solution with identity and bilinear pairing techniques, which could be fit for application pairing-based cryptography system. At last, the correctness and security analysis of the proposed scheme were formally proved.

Key words: information security; digital signature; multi-signature; identity; bilinear Paring.