文章编号:1001-9081(2005)09-2057-03

基于双线性对的门限部分盲签名方案

陆洪文[1,2],郑 卓[1]
(1. 同济大学 应用数学系,上海 200092;
2. 华东师范大学 网络信息安全研究所,上海 200062)
(zhuozzz@sohu.com)

摘 要:部分盲签名方案既有效保护消息发送方的隐私权,又通过加入签名方的信息控制发送方的权限。门限签名方案将密钥进行分享,限制了由单个签名者所组成的系统的不安全性。同时,基于双线性对的数字签名方案备受关注。文中基于双线性对提出一种新型的门限部分盲签名方案,并分析了该方案的安全性和效率,是第一次将双线性对引入到门限部分盲签名方案中。

关键词:门限签名;部分盲签名;双线性对;椭圆曲线
中图分类号:TP309.2 **文献标识码**:A

Threshold partially blind signature scheme from bilinear pairings

LU Hong-wen[1,2], ZHENG Zhuo[1]
(1. Department of Applied Mathematics, Tongji University, Shanghai 200092, China;
2. Institute of Network Information Security, East China Normal University, Shanghai 200062, China)

Abstract: Partially blind signature schemes in practice can not only protect the message sender's privacy efficiently but also limit the sender's ability by embedding the signer's information. A threshold signature scheme distributes the signing abilities to a group of signers, and avoids the system unsecurity. Recently the researches in these two signature schemes are popular. Meanwhile the signature schemes from bilinear pairings have attracted more attentions. In this paper a new threshold partially blind signature scheme from bilinear pairings was proposed. Furthermore the security and efficiency of the proposed scheme were analyzed.

Key words: threshold signatures; partially blind signatures; bilinear pairings; elliptic curve

部分盲签名技术已被广泛用于强调用户私有性的服务之中,如电子现金,无记名电子投票和智能网中的电话投票业务等[1],其在完全盲签名的基础上加入了签名方的信息,从而提高了方案的效率和功能,更引起人们的研究兴趣。另一方面,门限签名方案将密钥进行分享,限制了单个签名者所导致的系统不安全性,近年来的研究也很多。但目前存在的门限盲签名技术大都基于离散对数的困难性[2]或基于改进的RSA体制,而且涉及到门限部分盲签名技术的还不多。自MOV和 Frey-Rüch将双线性对引入数字签名后,基于双线性对的各种签名方案也出现了[3,4]。但在文献中利用双线性对构造门限部分盲签名方案的还没有涉及。正是针对这一点,本文在一种基于双线性对的部分盲签名方案基础上提出一种新型的门限部分盲签名方案,并分析了该方案的安全性和效率。本文是第一次提出基于双线性对构造门限部分盲签名方案。

1 预备知识

1.1 部分盲签名方案

部分盲签名是一种实用的密码技术,除满足一般数字签名的三个基本特征(签名者不能否认自己的签名;任何其他人都不能伪造签名;能够仲裁)外,还必须满足盲签名的两个条件:①签名者对其所签的消息是不可见的,即签名者不知道他所签的消息的内容;②签名信息是不可追踪的,即当签名信息被其所有者公布后,签名者无法知道这是他哪一次签名。同时所谓"部分"意味着待签名的信息是由发送方和签名方共同生成的,即签名方可以在待签名的盲签名候选中加入自己的信息,消息所有者在得到签名后不能对签名方加入的信息进行非法的篡改。通过部分盲签名方案的使用可以极大地提高电子现金的效率。部分盲签名的协议如下:

1) 发送方将致盲后的消息发送给签名方;

2) 签名方用它的私钥对消息进行签名,并在其中加入自己的信息,然后将签名结果发送给发送方;

3) 发送方检查签名是否满足验证函数,之后对签名进行脱盲从而得到最后的签名。

1.2 门限签名体制

自 Shamir首次提出门限方案[5]以来,门限签名在秘密的分享方面得到了广泛的应用。门限签名将签名权分散于一个签名团体,使得对消息的签名不能由事先决定的若干人产生,每次都需一定数量以上的人共同参与。这成功的将密钥权分享使得系统更加安全。在(t,n)门限方案中,秘密 s被分成 n份子秘密 $s_1, s_2, \cdots, s_n$分别分配给 n个人。该方案满足下列条件:

1) 知道任意 t个或者更多的子秘密 s_i,则容易计算出秘

收稿日期:2005-03-24;**修订日期**:2005-05-26
基金项目:国家自然科学基金资助项目(10471104);上海市科委基金资助项目(03JC14027)
作者简介:陆洪文(1939-),男,浙江东阳人,教授,博士生导师,主要研究方向:代数数论、密码学; 郑卓(1980-),女,吉林吉林人,硕士研究生,主要研究方向:密码学

密 s。

2) 只知道 $t-1$个或者更少的子秘密 s_i,则无法计算出秘密 s。

这种门限方案的提出克服了只有一个主密钥的以下两个缺点:若主密钥偶然地或蓄意地被暴露,整个系统就容易受攻击;若在主密钥丢失或毁坏,系统中的所有信息就用不成了。目前门限方案有多种形式,本文中主要采用的是拉格朗日内插多项式法[6]。Shamir的方案中要求系统中存在一个完全可信任的密钥管理秘书负责密钥的分配和相关的计算,这增加了系统的不安全性。在本文中我们所采用的门限方案不设秘书,由全体成员共同生成群私钥,减少了系统的不安全性。

1.3 双线性对

令 G_1和 G_2分别为阶数为素数 q的加群和乘群,再令 P为加群 G_1的生成元。假设 G_1和 G_2这两个群中的离散对数问题都是困难问题。令 $\hat{\tau}: G_1 \times G_1 \to G_2$为满足下列性质的双线性对:

1) 双线性性:$\hat{\tau}(aP, bQ) = \hat{\tau}(P, Q)^{ab}$对所有 $P, Q \in G_1$和所有的 $a, b \in Z_q^*$;

2) 非退化性:$\hat{\tau}(P, Q) = 1, \forall Q \in G_1$则 $P = O$;

3) 可计算性:存在有效算法可以计算 $\hat{\tau}(P, Q)$,对所有 $P, Q \in G_1$。

鉴于目前对于椭圆曲线签名体制的讨论很多,在本文的方案中我们选择基于椭圆曲线的 Weil对或经改造的 Tate对来构造双线性对,由于各种文献[7]对双线性对的计算已有相当多的讨论,而且我们的目的在于构造基于双线性对的签名体制,所以在这里就不讨论双线性对的具体计算。

在这样的群 G_1上,定义以下几个密码学问题:

- 离散对数(DL)问题:给定 $P, Q \in G_1$,找出整数 n,使得 $P = nQ$,若这样的 n存在;
- 计算 Diffie-Hellman(CDH)问题:给定三元组 $(P, aP, bP) \in G_1^3$,对 $a, b \in Z_q^*$,找出 abP;
- 决策 Diffie-Hellman(DDH)问题:给定四元组 $(P, aP, bP, abP) \in G_1^4$,对于 $a, b, c \in Z_q^*$,判断 $c = ab \pmod q$是否成立;
- Gap Diffie-Hellman(GDH)问题:这是一类 GDH问题困难而 DDH问题容易的问题。

2 基于双线性对的部分盲签名方案

根据部分盲签名协议[8],方案由系统初始化,密钥生成,签名过程和验证过程四个部分组成。

2.1 系统初始化

设群 G_1和 G_2是阶数为素数 q,满足 1.3节中假设的群,这里我们取 G_1为有限域上的椭圆曲线上的点构成的加群,令 P为 G_1群的生成元。$\hat{\tau}: G_1 \times G_1 \to G_2$为一个安全的双线性对,选择两个 Hash函数 $H: \{0,1\}^* \to G_1 \setminus \{1\}$和 $H_1: \{0,1\}^* \times G_1 \to Z_q^*$。

2.2 密钥生成

从 Z_q^*中随机选取 s,并计算 $Y \leftarrow sP$,返回签名方的公钥为 $pk = (Y, P, G_1, G_2, H, H_1)$,签名方的私钥为 $sk = s$。

2.3 签名过程

假设用户想要得到公钥为 pk的签名者对消息 M的部分盲签名,且双方已经事先商定 c作为消息 M的附加信息。签名过程如下:

1) 签名方随机选取 $r \in Z_q^*$,计算 $Z = H(c)$, $U = rZ$,将 U发送给用户;

2) 用户进行加盲变换,随机选取 $\alpha, \beta \in Z_q^*$,计算 $U' = \alpha U + \alpha\beta H(c)$, $h = \alpha^{-1} H_1(M, U') + \beta$,将 h发给签名方;

3) 签名方计算 $S' = (r+h)sZ$并将 S'发给用户;

4) 用户在收到 S'后验证 $\hat{\tau}(S', P) = \hat{\tau}(U + hH(c), Y)$是否成立,如果成立后进行脱盲变换,计算 $S = \alpha S'$。

最后用户得到签名为 (U', S, M, c),可以交给验证方进行验证。

2.4 验证过程

任何验证者可以通过检查以下等式是否成立,作为对签名的验证:

$$\hat{\tau}(S, P) = \hat{\tau}(U' + H_1(M, U')H(c), Y)$$

签名验证过程的正确性可由如下的方程给出:

$$\begin{aligned}\hat{\tau}(S, P) &= \hat{\tau}(\alpha S', P)\\ &= \hat{\tau}(\alpha(r+h)sZ, P)\\ &= \hat{\tau}((\alpha r + \alpha h)Z, Y)\\ &= \hat{\tau}(\alpha U + \alpha\beta Z + H_1(M, U')H(c), Y)\\ &= \hat{\tau}(U' + H_1(M, U')H(c), Y)\end{aligned}$$

上述推导运用了双线性对的性质。

3 基于双线性对的门限部分盲签名方案

我们提出一种新型的门限部分盲签名方案,仍由系统初始化、密钥生成、签名过程和验证过程四个部分组成。

3.1 系统初始化

设群 G_1和 G_2是阶数为素数 q,满足 1.3节中假设的群,这里我们取 G_1为有限域上的椭圆曲线上的点构成的加群,令 P为 G_1群的生成元。$\hat{\tau}: G_1 \times G_1 \to G_2$为一个安全的双线性对,选择两个 Hash函数 $H: \{0,1\}^* \to G_1 \setminus \{1\}$和 $H_1: \{0,1\}^* \times G_1 \to Z_q^*$。

3.2 密钥生成

设 (t, n)门限方案满足 $n \geqslant 2t-1$,且满足 $q \geqslant t$,群体中的 n个成员为 $\{P_1, \cdots, P_n\}$,群公钥为 Y,群私钥为 s,每个成员 P_i的个人分享公钥为 Y_i,个人分享私钥为 s_i。

成员 P_i通过以下步骤产生一个分享的私有密钥 s_i:

1) 随机选取 $a_{i0} \in Z_q^*$,将其保密,并广播 $a_{i0}P$;

2) 随机选取系数在 Z_q中,次数为 $t-1$的多项式 $f_i(x)$,满足 $f_i(0) = a_{i0}$,令

$$f_i(x) = a_{i,t-1}x^{t-1} + a_{i,t-2}x^{t-2} + \cdots + a_{i1}x + a_{i0}$$

3) 计算并广播 $a_{ij}P$ $(j = 1, 2, \cdots, t-1)$,将 $f_i(j)$秘密地发送给其他签名成员 P_j, $j = 1, 2, \cdots, n$; $j \neq i$;

4) P_i在收到其他 P_j发送的 $f_j(i)$, $j = 1, 2, \cdots, n$; $j \neq i$后,用下面的等式是否成立来验证 $f_j(i)$的有效性:

$$f_j(i)P = \sum_{k=0}^{t-1} i^k a_{jk}P$$

如果未通过验证 P_i将给 P_j数据无效的意见,这里假设没有这种情况;

5) 计算分享私钥 $s_i = \sum_{k=1}^{n} f_k(i)$,设 $f(x) = \sum_{i=1}^{n} f_i(x)$,则

$s_i = f(i)$;分享公钥为 $Y_i = s_iP$。

在执行完密钥生成过程后,群公钥为 $Y = sP$,这里 $s = \sum_{i=1}^{n} a_0$ 由全体成员共同生成,不需要另外的密钥管理秘书,且每个群成员都无法获知群私钥。最后系统返回公钥为 $pk = (Y, Y_1, \cdots, Y_n, P, G_1, G_2, H, H_1)$,私钥为 $sk = (s_1, \cdots, s_n, s)$。

3.3 签名过程

假设用户想要获得公钥为 pk的签名群体对消息 M的部分盲签名,且已经与其中至少 t个成员事先商定 c作为消息 M的附加信息,不妨设 t个签名者为 $P_1, \cdots, P_t$,签名的过程如下:

1)每个签名成员 P_i随机选取 $r_i \in Z_q^*$,计算 $Z = H(c)$, $U_i = r_iZ$,将 U_i发送给用户;

2)用户计算 $U = \sum_{i=1}^{t} U_i$随机选取 $\alpha, \beta \in Z_q^*$,计算 $U' = \alpha U + \alpha\beta H(c)$, $h = \alpha^{-1}H_1(M, U') + \beta$,将 h和 U发给每个签名成员 P_i;

3)每个签名成员 P_i计算 $S'_i = w_is_iU + hs_iw_iZ$,其中 $w_i = \prod_{j=1, j\neq i}^{t} \frac{j}{j-i}$并将 S'_i发送给用户;

4)用户在收到 S'_i后验证 $\hat{e}(S'_i, P) = \hat{e}(w_iU + w_ihH(c), Y)$是否成立,判断成立后计算 $S' = \sum_{i=1}^{t} S'_i$,并进行脱盲变换 $S = \alpha S'$,最后得到签名为 (U', S, M, c)。

3.4 验证过程

任何验证者可以通过检查以下的等式是否成立,来验证签名的合法性:

$$\hat{e}(S, P) = \hat{e}(U' + H_1(M, U')H(c), Y)$$

签名验证过程的正确性可由如下的方程给出:

$$\begin{aligned}\hat{e}(S, P) &= \hat{e}(\alpha S', P)\\ &= \hat{e}(\alpha \sum (w_is_iU + hs_iw_iZ), P)\\ &= \hat{e}(\alpha U + \alpha\beta Z + H_1(M, U')H(c), Y) \quad (1)\\ &= \hat{e}(U' + H_1(M, U')H(c), Y) \quad (2)\end{aligned}$$

上述过程中从(1)式到(2)式可由拉格朗日插值多项式推出:

$$\sum_{i=1}^{t} w_is_i = s = \sum_{i=1}^{n} f_i(0) = f(0)$$

4 门限部分盲签名方案的分析

4.1 方案的安全性

对于门限部分盲签名方案的安全性分析从以下几方面考虑:

1)部分盲签名性:在签名的过程中,签名方和用户将事先协商好的附加信息加入到签名中去,这首先保证了签名的部分性,在用户的加盲变换中是随机选取的 α, β这使 h在 Z_q^*上也是随机的,签名方想要通过 h来获得消息 M是基于椭圆曲线上离散对数困难问题的(ECDLP),所以每位参与签名者都没有办法获知消息的内容,这就保证了消息的盲签名性。

2)门限的安全性:在签名方案中,任意少于 t个成员组成的团体都无法获得群私钥,也就是说即使攻击方收买了 t-1个成员要获得群私钥也是困难的,这在文献[9]中已经予以证明,任意 t-1个成员要想在缺少一个成员的情况下伪造消息也是困难的,见文献[8]。

3)抗更改协定信息的攻击性:更改协定信息的攻击是指用户想在获得签名方的签名后试图将事先协定的附加信息 c更改成 c',同时保证签名的有效性。在我们的方案中,由于签名成员对于用户是未知的,要将 $H(c)$改为 $H(c')$需要解决CDH问题,这在计算上也是不可行的。

从这些角度,我们的方案在满足部分盲签名和门限签名的要求下,对于消息的签名是安全的。

4.2 方案的效率

方案所用的运算主要包括 G_1中的点的加法,点数乘, Z_q中的乘法和除法,哈希函数的运算,双线性对的运算等。与现有的各种基于 RSA和离散对数的门限签名和盲签名相比,我们所用的双线性对方案计算的效率更高,更具有实际应用价值。

5 结语

本文利用双线性对构造了一个新型门限部分盲签名方案。第一次将双线性对用于门限部分盲签名方案中。利用了双线性对在密码学应用中的各种好处和椭圆曲线密码体制密钥量小,安全性高和灵活性强的特点,将部分盲签名与门限签名结合起来,既有效保护消息发送方的隐私权又能够通过加入签名方的信息来控制发送方的权限,对于签名方也由密钥独享变换为门限共享,提高了整个系统的安全性能。该方案具有安全性能强和计算效率高的优点。

参考文献:

[1] JUANG W S, LEI C L. A Secure and Practical Electronic Voting Scheme for Real World Environments[J]. IEICE Transactions on Fundamentals, 1997, E80-A(1): 64-71.

[2] JUANG W S, LEI C L. Blind threshold signature based on discrete logarithm[A]. Proceedings of the 2nd Asian Computing Science Conference[C]. Lecture Notes in Computer Science, Springer-Verlag, 1996. 1179. 172-181.

[3] ZHANG F, KIM K. Efficient ID-Based blind signature and proxy signature from bilinear parings[A]. Proc of ACISP'03[C]. Wollongong, Australia, LNCS 2727, Berlin: Springer-Verlag, 2003. 312-323.

[4] 钱海峰,曹珍富,薛庆水. 基于双线性对的新型门限代理签名方案[J]. 中国科学 E辑·信息科学, 2004, 34(6): 711-720.

[5] Shamir A. How to Share a Secret[J]. Communication of ACM, 1979, 22(11): 612-613.

[6] 王育民,肖国镇. 密码学与数据安全[M]. 北京:国防工业出版社, 1991. 211-215.

[7] BARRETO P, KIM H, LYNN B, et al. Efficient Algorithems for Pairing-Based Cryptosystems[A]. CRYPTO 2002[C]. Springer-Verlag, 2002, LNCS 2442. 354-368.

[8] CHOW S S M, HUI L C K, YIU S M, et al. Two Improved Partially Blind Signature Schemes From Bilinear Pairings[J/OL]. Cryptology ePrint Archive: Report 2004. 108.

[9] VO D L, ZHANG F G, KIM K. A New Threshold Blind Signature Scheme From Pairings[A]. SCIS2003[C]. Itaya, Japan, 2003, vol 1/2. 233-238.