一种多安全策略的群签名方案

祝建华 崔国华 周时阳

(华中科技大学计算机学院信息安全系 武汉 430074)

摘要 提出了一种多安全策略的群签名体制。方案不仅具有前向安全性,能减小因为群成员的密钥暴露后所带来的不安全性,使群成员在密钥暴露前的签名仍然有效;同时还能有效地防止群成员的超前签名行为,任何群成员不能合法地提供出加入群之前的时间段的签名。方案有效地支持了群成员的撤销功能,一旦某个成员被撤销,这个成员就无法再代表群进行签名,而在撤销之前时间段的签名仍保持有效。签名具有可追踪性,一旦有签名发生争执,群管理员可以打开签名,确定签名者的身份,而除群管理员外的任何其他成员都无法打开签名。并且没有常用前向安全群签名方案中时间段的限制,避免了时间段到期后的系统重置。

关键词 群签名,前向安全,成员撤销,超前签名

中图分类号 TP309 **文献标识码** A

Group Signature Scheme with Multiple Security Strategy

ZHU Jian-hua CUI Guo-hua ZHOU Shi-yang

(College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074, China)

Abstract A group signature scheme equipped with multiple security strategy was proposed. This scheme has forward security which can minimize the damage caused by the exposure of any group member's signing key, and does not affect to the past signatures generated by this member; meanwhile, ahead signature generated by a group member before the joining date can be prevented via this strategy. Moreover, this scheme supports the group member revocable function efficiently, if a certain group member is cancelled from the group, he can sign a message on the behalf of the group no longer. There is traceability for signature, in the case of a dispute about a signature, GM can open the signature to determine the identity of a signature, anyone besides GM can not open any signature. Furthermore, there is no requirement for time period limits like previous schemes in which it is necessary to setup system while all time periods are used out.

Keywords Group signature, Forward security, Member revocation, Ahead signature

1 引言

Chaum 和 van Heyst 在 1991 年提出了群签名体制^[1]。与普通的签名体制不同,他提出了签名者的匿名性,群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名,验证者只能判断出签名者是否为群中的成员而不能确定是哪个成员。与其它数字签名一样,群签名是可以公开验证的,而且可以只用单个群公钥来验证。在出现争端时,任何一个群签名可以被一个指定的群管理员打开,揭露原始签名者的身份。同时,包括群管理员的任何人都不能产生假冒的有效签名。随后 J. Camenish 和 M. Stadler^[2], J. Camenish 和 M. Michels^[3], G. Ateniese 和 G. Tsudik^[4,5] 等对其进行了修改和完善。其中 J. Camenish 和 M. Stadler 在文献^[2]中首次提出了群公钥和签名长度都不依赖于群成员的个数的两个群签名方案。该方案为群签名走向实用排除了最大的障碍,因此在群签名发展史上具有非常重要的意义。

目前,在群签名方案的实用性研究中,以下方面的研究一

直被国内外学者们普遍关注。

(1) 成员的有效撤销性研究。成员一旦撤销,其签名被视为无效。作为一个实用的群签名方案,应允许成员动态地加入和撤销,现有的方案中,对成员的有效加入技术已相当完善,而在成员的有效撤销方面,尽管做出了大量的研究,但效果不太理想,甚至有些方案在提出后,被指出存在某些错误,有些方案理论上目前没有发现错误,但计算量太大,离实用有较大的距离。

(2) 前向安全性研究。若签名者的密钥被泄漏,那么这个签名者的所有签名(过去的和将来的)都有可能泄漏,目前各种吊销技术可以阻止用户接受泄漏密钥的签名,然而,即使有了吊销技术,在密钥泄漏前接受签名的用户也不能保证签名者是否足够诚实。为了突破这个局限性,人们提出了很多不同的方法,通常使用秘密共享技术。但是,这种方法耗费巨大,尤其对于单个用户来说实施起来极其昂贵,而且每个系统都可能受到相似的攻击,实际上并没有减少多少危险性。一个较好的方法是当密钥泄露的时候,能最大化地减少对系统

到稿日期:2008-10-28 返修日期:2009-01-22 本文受国家自然科学基金(60703048),湖北省自然科学基金(2007ABA313)资助。

祝建华(1962-),男,博士生,副教授,主要研究方向为信息安全,E-mail:zhu-jian-hua@tom.com;崔国华(1946-),男,教授,博士生导师,主要研究方向为密码学;周时阳(1960-),男,副教授,主要研究方向为信息安全。

的危害,即所谓的前向安全。确保密钥在短期使用时间内是安全的,其主要思想是当前密钥的泄露并不影响以前时间段签名的安全性,不需要对以前的签名进行重签名。通常,设计这样一个系统的困难之一是在公钥保持不变的情况下能够改变群成员的密钥^[10]。

(3)超前签名。当一个成员加入群后,应只能对加入群以后的时间段的消息进行签名,不能产生加入群以前的时间段的消息的合法签名,即要杜绝所谓的超前签名。

Anderson于1997年在文献[6]中首次提出了前向安全的概念。签名方案中的前向安全性,就是一旦发生密钥的泄漏,能尽可能地减少对系统安全的影响。常用的手段就是将时间分成若干个时间段 $1 \sim T$,群成员在时间段 i 的签名密钥对应为 $SK_i (i=1,2,\dots,T)$,通过单向函数由 SK_i 可计算出 SK_{i+1} ,而由 SK_i 计算 SK_{i-1} 在计算上是不可行的。这样一旦发生了 SK_i 泄漏,群成员用 $SK_1 \sim SK_{i-1}$ 对信息进行的签名的有效性不会产生影响。最开始 Anderson只是将前向安全的概念用于传统的个体签名,后来逐步被应用到了群签名方案中^[7-9]。同时在其它各类签名中也得到了广泛应用^[11]。

目前为止,一些学者在前向安全的群签名方案上做出了相关的研究。在文献[8]中,Cheng提出了一个有效取消的前向安全群签名体制,该方案中,验证取消展示所依赖的随机数不同于签名所用的随机数,这样会导致不诚实的签名者提供假的验证取消展示,使方案失去成员的可撤销性。同时,打开算法的模幂线性依赖于成员个数。在目前的基于大数分解和离散对数求解难题的前向安全群签名方案中^[8-11],都没有提出解决超前签名问题的方法,同时密钥的演化方法都是沿用文献[6]的思想,将系统时间固定分成 T 个时间段,一段到了时间段 T 之后,必须重新初始化系统中各群成员的资格证书。

2001年,在亚洲密码年会上,Boneh等人提出了一个短签名方案^[12]。在(超)椭圆曲线上利用双线性映射算法,把对消息的签名降到170比特左右,安全性建立在Gap Diffie-Hellman上^[12-14],相对于RSA算法的1024比特,DSA算法的320比特。短签名方案在网络传输中有着明显的优势,备受众多学者关注。在此基础上,Duc-Liem Vo等设计了一个基于双线性映射的前向安全的签名方案^[15],解决了固定时间段的限制问题,但该方案的设计思想不适应于群签名。目前基于双线性映射的群签名方案中都不能在同一方案中,同时具备前向安全性、成员的有效撤销以及签名的可追踪性等。另外,目前基于双线性映射的群签名方案都需要一个在线的可信第三方^[16,17]。如何设计一个不需要可信第三方的基于双线性映射的前向安全的签名方案,有待进一步的研究。

本文提出了一个基于大数分解和离散对数求解难题的多安全策略的群签名方案,方案既具备前向安全性,又首次提出了防止群成员超前签名的解决方法,从而有效地解决了成员撤销的验证问题。同时不需要将系统时间分成若干个固定时间段,避免了重新初始化系统的不足。

2 前向安全群签名模型

一个前向安全的群签名方案包含以下过程:

(1)创建。一个多项式时间概率算法,当输入安全参数后,产生系统参数、群公钥和私钥。

(2)加入。一个用户和群管理人之间的交互式协议,使用户成为群成员。该协议可产生群成员的私钥和成员证书。

(3)演化。从一个时间段到下一个时间段转化时,群密钥发生改变。

(4)签名。一个概率算法,当输入一个消息和一个群成员的私钥后,输出对消息的签名。

(5)验证。一个在输入对消息的签名及群公钥后确定签名是否有效的算法。

(6)打开。一个在给定一个签名及群私钥、群秘密信息的条件下确定签名人身份的算法。

一个好的群签名方案应满足以下的安全性要求:

(1)匿名性。给定一个群签名,对除了唯一的群管理人之外的任何人,确定签名人的身份在计算上是不可行的。

(2)不可关联性。在不打开签名的情况下,确定两个不同的签名是否为同一个群成员所做,在计算上是困难的。

(3)防伪造性。只有群成员才能产生有效的群签名。

(4)可跟踪性。群管理人在必要时可以打开一个签名以确定出签名人的身份,而且签名人不能阻止一个合法签名的打开。

(5)防陷害攻击。包括群管理人在内的任何人都不能以其他群成员的名义产生合法的群签名。

(6)抗联合攻击。即使一些群成员串通在一起也不能产生一个合法的不能被跟踪的群签名。

3 前向安全数字签名方案

3.1 预备知识

本文设计的群签名体制依赖于Diffie-Hellman假定和强RSA假定,并使用已有的零知识证明协议作为构件。这些零知识协议可以用理想的Hash函数非交互地实现。该体制还涉及到知识签名的一些已有的结论性的结构,包括离散对数知识签名等。

设 $N=pq$ 为RSA类的模, G 为 Z_N^* 的循环子群, g 是该循环子群的生成元, k 为安全参数,Hash函数 $H: \{0,1\}^* \rightarrow \{0,1\}^k$ 。

假设1(强RSA假设)不存在这样的概率多项式时间算法,已知 $z \in G$,找到 $u \in G$ 和 $e \in Z_N$,满足 $z \equiv u^e \pmod{N}$ 。

假设2(Diffie-Hellman假设)不存在这样的概率多项式时间算法,该算法以不可忽略的概率区分出分布的 D 和 R ,这里 $D = (g, g^x, g^y, g^z)$, $R = (g, g^x, g^y, g^{xy})$, $x, y, z \in_R Z_{\#G}$ 。

知识签名。离散对数的知识签名:给定 $y \in G$,称 $(c, s) \in \{0,1\}^k \times Z_N^*$ 为 y 对 g 关于消息 m 的知识签名,如果它满足 $c = H(m || y || g || g^y \cdot c)$ 。

3.2 方案设计

系统初始化:群签名方案中,有群管理员GM和群成员 U 类实体。首先GM选取两个不同大素数 $p=2p'+1$ 及 $q=2q'+1$,这里, p' 和 q' 也是大素数; $N=pq$, $R=p'q'$; g 为 Z_N 的 R 阶循环子群 G 的生成元,GM选择一对整数 (e, d) 满足 $\gcd(e, R)=1, ed=1 \pmod{R}$, e 为GM的加密公钥, d 为私钥;GM选择: $x \in_U Z_N^*$ 作为群私钥,计算 $y=g^x \pmod{N}$ 作为群的公钥。确定一个公开的无碰撞单向HASH函数 $H(\cdot)$ 。系统初始时,设置时间段参数 $t_i=1$,公开 $\{N, g, y, t\}$ 。

成员加入:假定用户 u 要在时间段 i 加入到群中,用户 u 选择 $x_u \in \mathbb{Z}_N^*$ 作为 u 的私钥,计算: $y_u = g^{x_u} \bmod N$,将 y_u 作为其公开密钥,并提供 $V_1 = \text{SKREP}[a: y = g^a]$ ("),这里 $\text{SKREP}[a: y = g^a]$ (")表示 y 对 g 的知识签名。

u 将 (y_u, V_1) 提交给 GM,GM 验证 V_1 后,为其选择一个随机素数: $e_u \in \mathbb{Z}_N^*$,计算: $c_{u,i} = (y_u g^{e_u x_u})^{-2^i d}$,GM 将 $(c_{u,i}, e_u, i)$ 秘密送给用户 u 作为 u 的资格证书,使用户 u 成为群成员。群成员 u 通过等式 $c_{u,i} \cdot (g^{e_u} y_u y)^{2^i} = 1$ 验证 $c_{u,i}$ 的正确性。通过验证后,群成员 u 将 $(c_{u,i}, e_u, x_u, i)$ 作为自己的群签名密钥秘密保存。

成员撤销:系统中,需要一个群成员撤销表 CRL,记录项为 $(c_{u,\tau}, \tau)$,这里, τ 为资格证书失效的时间段。 $c_{u,\tau}$ 表示群成员在时间段 τ 被删除时的资格证书,即表示当需要在时间段 τ 从群中删除某群成员 u 时,在撤销表 CRL 中加入记录 $(c_{u,\tau}, \tau)$ 。

演化:当时间段发生变化,由时间段 i 过渡到时间段 $i+1$ 时,需要完成资格证书的演化,计算 $c_{u,i+1} := c_{u,i}^2$,同时销毁 $c_{u,i}$ 。也可以在以后签名时再演变。

签名:群成员 u 要在时间段 j 对消息 m 进行签名,此时 u 的群签名密钥为 $(c_{u,i}, e_u, x_u, i)$,如果 $j > i$,必须首先完成资格证书的演化, $c_{u,j} := c_{u,i}^{2^{j-i}}$,群签名密钥演变为 $(c_{u,j}, e_u, x_u, j)$ 。确认资格证书的新鲜性后,首先随机选择 $k \in \mathbb{Z}_N^*$,计算 $u_1 = g^k \bmod N$, $u_2 = H(u_1, m)$, $r_1 = c_{u,j}^{u_2} \bmod N$, $r_2 = e_u u_2 r_1^{2^j}$, $r_3 = k + x_u u_2 r_1^{2^j}$,将 $(u_1, u_2, r_1, r_2, r_3, j)$ 作为在时间段 j 对消息 m 进行签名。

验证:对 $(u_1, u_2, r_1, r_2, r_3, j)$ 的验证,可通过式(1)和式(2)进行。

$$u_1' = g^{r_2 + r_3 r_1^{e_u} y^{u_2 r_1^{2^j}}} \bmod N \quad (1)$$

$$u_2 = H(u_1', u_2, m) \quad (2)$$

式(1)和式(2)的验证通过后,在 CRL 中加入记录 $(c_{k,\tau}, \tau)$,当 $j \geq \tau$ 时,判断式(3)是否成立。

$$r_1 = c_{u,\tau}^{2^{j-\tau} u_2} \bmod N \quad (3)$$

如果成立,表示该成员已被删除,签名无效,否则接收签名。

打开:当发生争执时,GM 可以打开签名,通过式(4)确定签名者公钥 y_u 。

$$\zeta = (u_1^{-1} g^{r_3})^{2^{-j} u_2^{-1} r_1^{-1}} \bmod N \quad (4)$$

4 安全性及效率分析

4.1 方案的正确性证明

定理 1 如果 $(u_1, u_2, r_1, r_2, r_3, j)$ 是一个合法的群成员按照签名算法生成的群签名,则一定能通过式(1)和式(2)的验证。

证明:验证者首先按式(1)计算 u_1' ,因为:

$$\begin{aligned} u_1' &= g^{r_2 + r_3 r_1^{e_u} y^{u_2 r_1^{2^j}}} \\ &= g^{k + (e_u + x_u) u_2 r_1^{2^j} c_{u,j}^{u_2} y^{u_2 r_1^{2^j}}} \\ &= g^k g^{e_u u_2 r_1^{2^j}} g^{x_u u_2 r_1^{2^j}} (g^{e_u} y_u y)^{-e_u u_2 r_1^{2^j}} y^{u_2 r_1^{2^j}} \\ &= g^k = u_1 \end{aligned}$$

所以: $u_2 = h(u_1, m) = h(u_1', m)$

签名通过验证。

4.2 方案的安全性

方案满足前向安全群签名的所有安全性要求。

1) 群签名具有匿名性

给定一个群签名 $(u_1, u_2, r_1, r_2, r_3, j)$,因为其产生依赖于随机数,具有随机性,所以除签名者本身外的任何人都不能从签名中获得关于签名者的秘密信息。

2) 群签名具有不可连接性

给定两个不同的群签名 $(u_1, u_2, r_1, r_2, r_3, j)$ 和 $(u_1', u_2', r_1', r_2', r_3', j')$,因为 u_1, u_2 和 u_1', u_2' 依赖于不同的随机数,由签名过程中 r_1, r_2, r_3 和 r_1', r_2', r_3' 的产生方法可知 r_1, r_2, r_3 和 r_1', r_2', r_3' 间无任何关联,因而攻击者无法获得上述两个签名之间的关系。

3) 群签名具有不可伪造性

如果群管理员想伪造时间段 i 的签名,他可以选择 k 和 i ,由于知道群成员资格证书,能够计算出 u_1, u_2, r_1 和 r_2 ,但由于不知道成员的私钥,无法直接计算出 r_3 ,只有试图由式(1)获得 r_3 ,但这是一个离散对数的求解难题,所以群管理员无法进行伪造。而对于一般的攻击者,连合法的群成员资格证书都不知道,因此,更不可能伪造满足验证等式的群签名。由此可以得到结论,即方案也可以抵抗各种联合攻击和陷害攻击。

4) 方案具有向前安全性

由于演化函数具有单向性,即使攻击者得到某群成员在时间段 i 的群成员资格证书,也不可能计算出这个群成员在时间段 i 以前的资格证书。这样群管理员只需取消时间段 i 的群成员资格证书,那么在时间段 i 之前的群成员的签名仍然有效。

5) 群成员的有效取消

假定在时间段 i 群成员被取消,取消记号被群管理员公布在 CRL 中。验证签名时,通过式(3)可有效地验证群成员是否被取消,判定签名的有效性。

6) 群签名具有可追踪性

定理 2 如果 $(u_1, u_2, r_1, r_2, r_3, j)$ 是一个合法的群成员按照签名算法生成的群签名,则能够且只能由 GM 打开。

证明:打开算法的正确性证明如下。

$$\begin{aligned} \zeta &= (u_1^{-1} g^{r_3})^{2^{-j} u_2^{-1} r_1^{-1}} = (g^{-k} g^{k + x_u u_2 r_1^{2^j}})^{2^{-j} u_2^{-1} r_1^{-1}} \\ &= g^{x_u} = y_u \bmod N \end{aligned}$$

由于只有 GM 知道 R 和 $\phi(N)$,因此除管理员外,任何人不可能计算 $u_1^{-1}, u_2^{-1}, r_1^{-1}$,也就无法计算出 ζ ,既保证了方案的匿名性,又使方案具有可追踪性。在本方案的打开算法中,计算出 y_u 的模幂和求逆运算与成员个数无关。

7) 群成员不可超前签名

方案中,群成员 u 在时间段 i 加入到群中,群管理者提供的是时间段 i 的资格证书 $(c_{u,i}, e_u, x_u, i)$,由于 d 是管理员的秘密,群成员无法求出 $(c_{u,i-1}, e_u, x_u, i-1)$,这是一个强 RSA 假定的问题,这样就不可能产生一个满足 $j < i$ 的合法群签名 $(u_1, u_2, r_1, r_2, r_3, j)$,因此方案能有效防止群成员进行超前签名。

4.3 方案的效率分析

本文的方案中,为提高效率,对于计算 2^j ,可以在每个时间段的开始就进行。

(下转第 58 页)

息量的复杂度由 $O(n^2)$ 转变为 $O(n)$, 有效降低了入侵防御系统的网络负载。

结束语 本文提出了一种分布式 IPS 模型。模型从分布式 IPS 系统应用特点出发, 提取出影响节点间协作关系的邻近距离因子, 并通过邻近距离的计算优化节点通信范围, 裁减冗余消息, 以减少系统网络负载。模型中消息机制的引入, 缓解了节点间协作的耦合性, 扩展了系统部署的灵活性。网络负载小和系统部署灵活这两个特点使模型为中大规模网络环境中安全防御系统的部署提供了一套很好的解决方案。在下一步的工作中, 还需要对网络环境与邻近计算公式权值之间的关系做进一步的分析和探索, 以提高模型在实际应用中的性能。

参考文献

[1] 连一峰, 戴英侠, 胡艳, 等. 分布式入侵检测模型研究[J]. 计算机研究与发展, 2003, 40(8): 1196-1202
 [2] Abraham A, Jain R, Thomas J. Distributed soft computing intrusion detection systems[J]. Journal of Network and Computer

Applications, 2007, 30(1): 81-98
 [3] 马恒太. 基于 Agent 的分布式入侵检测系统模型[J]. 软件学报, 2000, 11(10): 1312-1319
 [4] 李旺. 分布式网络入侵检测系统 NetNumen 的设计与实现[J]. 软件学报, 2002, 13(8): 1723-1728
 [5] Patrick D, Allen D. Increasing Flexibility in Network Visibility and Intrusion Response [J]. Military Communications Conference, 2006, 8 (23-25): 1-6
 [6] 吴骏, 王崇骏, 陈世福. 基于多 Agent 的动态层次化分布式入侵检测系统[J]. 计算机科学, 2007, 34(2): 71-75
 [7] Feinstein B. The Intrusion Detection Exchange Protocol (IDXP) [S]. RFC4767. 2007
 [8] Kannadiga Z P. A distributed intrusion detection system using mobile agents[J]. Software Engineering, 2005, 25(23): 238-245
 [9] 孙即祥. 现代模式识别[M]. 长沙: 国防科技大学出版社, 2002: 15-17
 [10] Lupu E, Sloman M. Conflicts in Policy-based Distributed Systems Management[J]. IEEE Transaction on Software Engineering, 1999, 25 (6): 335-349

(上接第 38 页)

如表 1 所列, 将本文方案与文献[8]中提出的方案作了比较, 签名和验证过程中模幂运算太多的一些方案没有在表中列出进行比较。表中 EXP 表示模幂运算, INV 表示求逆运算, n 表示群成员个数, m 表示撤销成员的个数。

表 1 方案的比较

方案	签名	验证	打开
本文方案	2EXP	(3+m)EXP	3EXP+3INV
CHEN 的方案	3EXP	(3+m)EXP	(n/2+3)EXP+3INV

结束语 本文在充分考虑到群签名过程中可能出现的各种问题的前提下, 提出了一种多安全策略的群签名方案, 方案不仅具有前向安全性, 同时首次在群签名方案中能有效地防止群成员的超前签名。方案支持成员的有效撤销。签名的打开算法, 将模幂运算和求逆运算量与成员个数线性相关优化成线性无关, 效率得到了较大程度的提高。本文所提出的方案, 没有时间段周期的限制, 解决了一旦时间周期结束, 就必须重新初始化系统的弊病。

参考文献

[1] Chaum D, van Heyst E. Group signatures[C]// Advances in Cryptology-EuroCrypt'91, Lecture Notes in Computer Science 547. Berlin: Springer, 1991: 257-265
 [2] Camenish J, Stadler M. Efficient group signatures for large groups[C]// Proceedings of CRYPTO'97, Lecture Notes in Computer Science. Springer-Verlag, 1997, 1296: 410-424
 [3] Camenish J, Michels M. A. group signature scheme with improved efficiency[C]// Proceedings of ASIACRYPT'98, Lecture Notes in Computer Science. Springer-Verlag, 1998, 1541: 160-174
 [4] Ateniese G, Tsudik G, Tsudik. A coalition-resistant group signature[EB/OL]. <http://www.isi.edu/~gts/pubs.html>
 [5] Ateniese G, Tsudik G. Some open issues and new directions in group signatures[EB/OL]. <http://www.isi.edu/~gts/pubs.html>

html
 [6] Anderson R. Invited lecture[C]// Proceedings of the 4th ACM Conference on Computer and Communications Security. Zurich, Switzerland, 1997: 1-7
 [7] Song D-X. Practical forward secure group signature schemes [C] // Proc. of the 8th ACM Conf on Computer and Communications Security (CCS 2001). New York: ACM Press, 2001: 225-234
 [8] 陈少真, 李大兴. 有效取消的向前安全群签名体制[J]. 计算机学报, 2006, 29 (6): 998-1003
 [9] 李如鹏, 于佳, 李国文, 等. 高效撤销成员的前向安全群签名方案[J]. 计算机研究与发展, 2007, 44 (7): 1219-1226
 [10] Michel A, Leonid R. A New Forward-Secure Digital Signature Scheme [C]// ASIACRYPT2000, LNCS 1976. Berlin Heidelberg: Springer-Verlag, 2000: 116-129
 [11] 王晓明, 符方伟, 张震. 前向安全的多重数字签名方案[J]. 计算机学报, 2004, 27 (9): 1177-1191
 [12] Chaum D, van Heyst E. Group signatures[C]// Advances in Cryptology-EuroCrypt'91, Lecture Notes in Computer Science 547. Berlin: Springer, 1991: 257-265
 [13] Boneh D, Boyen X. Short signatures without random oracles [A]// Christian Cachin, Jan Camenisch, eds. Eurocrypt'04 [C]. Interlaken, Switzerland: Springer-Verlag, 2004: 56-73
 [14] Mitsunari S, Sakai R, Kasahara M. A new traitor tracing[J]. IE-ICE Trans. Fundamentals, 2002, E85A (2): 481-484
 [15] Vo Duc-Liem, Kim Kwangjo. Yet Another Forward Secure Signature from Bilinear Pairings [C]// ICISC 2005, LNCS 3935. Berlin Heidelberg: Springer-Verlag, 2006: 441-455
 [16] Cheng X, Zhu H, Qiu Y, et al. Efficient Group signatures from Bilinear Pairing [C]// CISC'05 LNCS 3822. Springer-Verlag, 2005: 128-139
 [17] Park H, Kim H, Chun K, et al. Untraceability of Group Signature Scheme based on Bilinear Mapping and their Improvement [C]// International Conference on Information Technology (IT-ING'07). IEEE, 2007: 103-109