一类新的基于证书的代理盲签名

农　强[1,2], 吴顺祥[2]
NONG Qiang[1,2], WU Shun-xiang[2]

1.漳州师范学院 计算机科学与工程系, 福建 漳州 363000
2.厦门大学 自动化系 系统与控制研究中心, 福建 厦门 361005
1.Department of Computer Science and Engineering, Zhangzhou Normal University, Zhangzhou, Fujian 363000, China
2.Department of Automation, Center for Systems and Control, Xiamen University, Xiamen, Fujian 361005, China
E-mail: nong_qiang@163.com

NONG Qiang, WU Shun-xiang.Novel certificate-based proxy blind signature.Computer Engineering and Applications, 2008, 44(12):124-126.

Abstract: Based on the Certificate-Based Encryption(CBE) given by Gentry, a generic method to consturct Certificate-Based Signature(CBS) scheme is presented.Combining proxy signature with blind signature, a new certificate-based proxy blind signature scheme is proposed based on Gap Diffie-Hellman(GDH) group.Analysis shows that the new scheme overcomes the security leaks of forgery attacks and linkability in the existing identity-based proxy blind signatures.Furthermore, it also has distinct advantages in efficiency.
Key words: Certificate-Based Signature(CBS); GDH group; identity-based; proxy blind signature

摘　要: 在Gentry提出的基于证书加密(CBE)概念的基础上, 提出了构造基于证书签名(CBS)方案的一般性方法, 并在此基础上, 结合代理签名与盲签名, 利用间隙Diffie-Hellman(GDH)群的特点, 提出了一种基于证书的代理盲签名的新方案, 分析表明该方案不仅克服了基于身份的代理盲签名方案不能有效抵抗伪造攻击并缺少不可链接性等缺陷, 而且签名算法的效率也有明显提高。
关键词: 基于证书的签名; 间隙Diffie-Hellman群; 基于身份; 代理盲签名
文章编号: 1002-8331(2008)12-0124-03　　**文献标识码**: A　　**中图分类号**: TP309

1　引言

在传统数字签名机制(PKS)中, 用户的公钥需要由可信第三方(TTP)签名的证书来保证其可靠性, 而Shamir的基于身份的签名机制[1]尽管不再需要证书, 但用户的私钥无可避免地被TTP所托管。2003年欧密会上Gentry提出了基于证书加密(CBE)的概念[2], CBE把公钥加密体制(PKE)和基于身份加密体制(IBE)相结合并保持了两者的大部分优点。和PKE一样, CBE的用户生成自己的公私钥对并向CA请求一个证书。不同在于, CA使用IBE的算法在每个有效的周期里产生一个最新的(up-to-date)证书。该证书除了具有在传统PKI下所具有的所有功能外, 还可以作为解密密钥并且没有对证书状态的第三方查询问题(the third-party query)[2], 证书的传送也不需要安全信道。此外, CBE还消除了IBE具有的密钥托管问题, 因为CA并不知道用户的私钥。文中基于证书签名的概念类似于无证书签名[3]、自证实公钥签名[4]以及无可信中心的基于身份的签名[5]。

无证书的密码系统(certificateless cryptography)是Al-Riyami和Paterson在2003年的亚密会上提出的一种新的密码系统[3]。与基于身份的密码系统类似, 它不需要使用证书来保证公钥的可靠性, 而是依赖于一个拥有主密钥(master key)的可信机构。区别在于, 在采用无证书密码系统的签名体制中, 可信机构不直接生成用户的私钥, 它只产生与用户身份对应的部分私钥, 然后由用户自己把部分私钥和一些秘密信息结合从而获得实际的签名密钥。无证书签名有效地解决了基于身份密码系统中的密钥托管问题, 但是将部分私钥传送给用户时需要安全信道。

自证实公钥密码系统(self-certified public keys cryptography)的概念由Girault于1991年提出[4], 在自证明签名方案(SCS)中, 签名人用他的长期签名私钥和证书信息生成自证明签名公私钥对, 验证人只需验证签名人对消息的自证明签名, 从而省去了一次对证书的签名验证过程, 可是自证实公钥签名没有考虑到证书吊销(certificate revocation)问题。证书是用来绑定身份和其相应公钥的数据文件。通常, 这种绑定在证书的整个生命期里都是有效的。但是, 出于某些原因(如私钥泄露或用户职位变化时), 往往要求在证书有效期截止前, 提前解除这种绑定并撤销相应的公钥证书。

在代理签名方案中, 原始签名人能将其数字签名权力委托给代理签名人。在盲签名方案中, 消息和签名结果对签名人是

基金项目: 厦门大学985二期信息创新平台项目(2004-2007); 福建省教委科技项目(No.JA05290)。
作者简介: 农强(1978-), 男, 硕士研究生, 主要研究领域为密码学; 吴顺祥, 通讯作者, 男, 教授, 博士, 主要研究领域为信息安全, 数据挖掘, 智能信息系统, 人工智能与机器学习。

收稿日期: 2007-08-07　　修回日期: 2007-11-13

不可见的。在2000年, Lin和Jan第1个提出了代理盲签名方案[6]。之后, Tan等人在Schnorr盲签名的基础上提出了一个基于离散对数的代理盲签名[7]。但是后来, Wang等人证明Tan等人的方案是不安全的[8], 它既受到广泛伪造攻击, 又是可链接的。针对Tan等人方案的缺陷, Awasthi和Lal提出了一种新的代理盲签名方案[9]。Sun等人也指出Awasthi和Lal的方案不满足不可链接性[10]。最近, 利用双线性对构造的一些基于身份的代理盲签名方案[11-13]被提出, 具有一些较好的性质, 但容易发现在这些方案当中, PKG(私钥产生中心)可以计算系统内任何用户的私钥, 当然也可以伪造任何用户的代理盲签名, 而要求PKG绝对可信在实际中是不现实的, 并且也不满足不可链接性。

本文首次利用双线性对构造了一种有效的基于证书的代理盲签名方案, 并在安全性及性能方面和已提出的基于身份的代理盲签名方案进行了分析比较, 结果表明新方案具有安全性高、计算复杂性低等优点。

2 双线性映射

设G_1为循环加法群, G_2为循环乘法群, G_1、G_2的阶均为素数q。假定在G_1、G_2中计算离散对数问题是困难的。设$e: G_1\times G_1\to G_2$为一个双线性映射, 它满足以下三个性质:

(1) 双线性。$e(aP, bQ)=e(P, Q)^{ab}$, 对$\forall P, Q\in G_1$和$a, b\in Z_q^*$成立。

(2) 非退化性。$\exists P, Q\in G_1$, 使$e(P, Q)\neq 1$。

(3) 可计算性。如果$P, Q\in G_1$, 则$e(P, Q)$可以在多项式时间内有效计算出来。

定义1 计算离散对数问题CDHP(Computational Diffie-Hellman Problem): 对于$a, b\in_R Z_q^*$, P是G_1的生成元, 给定G_1中的元素P、aP、bP, 计算abP。

定义2 计算离散对数假设(Computational Diffie-Hellman (CDH) Assumption): 令IG是一个CDH参数生成器, 输入安全参数1^k, 说IG满足CDH假设, 如果对于充分大的k, 算法A解决关于G_1的CDH问题具有的优势$\mathrm{Adv}_{IG, A}(k)$定义为:

$$\mathrm{Adv}_{IG, A}(k)=\Pr\left(\begin{array}{l}A(q, G_1, aP, bP)=abP,\\ (q, G_1)\leftarrow IG(1^k), P\leftarrow G_1, a, b\leftarrow Z_q^*\end{array}\right)\geq \varepsilon(k)$$

参数生成器IG满足CDH假设, 如果对任何k的概率多项式时间算法A, 优势$\mathrm{Adv}_{IG, A}(k)$是可忽略量。在素数阶循环群G上, DDHP在多项式时间内能被解决, 但没有任何可能的算法可以解决CDHP, 称G为GDH(Gap Diffie-Hellman)群。GDH群能在有限域上的超奇异椭圆曲线或超椭圆曲线上找到, 双线性映射能通过Weil对或Tate对构造, 本文方案基于GDH群。

3 基于证书的签名方案

基于证书的签名方案使用了与Gentry的基于证书的加密方案相同的系统参数和证书更新算法。签名人使用CA的证书与其秘密值产生签名密钥, 证书可以公开, 不需要安全信道, 因此没有密钥发布问题。签名方案由以下算法组成:

CA系统参数及密钥生成算法: 输入系统安全参数1^k和总的时间周期数T, 输出系统公开参数Params(其中包含了系统公钥PK_C)和系统主密钥SK_C。

用户秘密值设定算法: 输入系统安全参数1^k和总的时间周期数T, 输出用户的秘密值SK_U和用户公钥PK_U。

证书更新算法: 在第i($i=1, \cdots, T$)个时间周期, 输入系统主密钥SK_C, 系统参数Params, i和用户公钥PK_U, 输出证书$Cert_i$, 并将其发送给用户。

用户更新算法: 在第i($i=1, \cdots, T$)个时间周期, 输入系统参数Params, i, 证书$Cert_i$和$Cert_{i-1}$, 输出$Cert_i$。

签名算法: 在第i($i=1, \cdots, T$)个时间周期, 输入待签消息M, 系统参数Params, $Cert_i$和用户秘密值SK_U, 输出临时签名密钥$SK=f(SK_U, Cert_i)$和对消息M的签名σ, 其中f是一个公开的算法。

验证算法: 输入消息M, 签名σ, i, 系统公钥PK_C和用户公钥PK_U, 输出T(或者F)(其中T表示签名是有效的, F表示签名无效)。

4 基于证书的代理盲签名方案

这里在基于证书签名方案的基础上, 首次构造了一个基于证书的代理盲签名方案。在以下的签名算法中, 基于证书签名方案中的CA变成了原始签名人。这里假定签名涉及了三方参与者: 原始签名人Charlie、代理签名人Alice和盲签名消息持有人Bob。该方案由以下4个算法组成: 系统初始化及密钥产生算法, 代理私钥提取算法, 签名算法和验证算法。

4.1 系统初始化及密钥生成算法

输入安全参数1^K, 输出两个阶为q的循环群$(G_1, +)$和$(G_2, \times)$, q为大素数, P为G_1的生成元。定义G_1上的一个双线性映射$e: G_1\times G_1\to G_2$, 同时定义两个强无碰撞安全单向Hash函数$H_1: \{0, 1\}^*\to G_1$, $H_2: \{0, 1\}^*\to Z_q^*$。Charlie选择$SK_C=S_C\in_R Z_q^*$, 计算$PK_C=S_C P$将S_C秘密保存, 公开系统参数:

$$\mathrm{Params}=\{G_1, G_2, e, q, P, PK_C, H_1, H_2\}$$

Alice使用Charlie的公开参数Params计算其密钥/公钥对$(SK_A, PK_A)=(S_A, S_A P)$。

4.2 代理私钥提取算法

Charlie在开始代理授权之前先准备授权文件W, 其中包含代理人信息, 如代理签名人公钥以及代理签名的文件类型、时间等信息。Charlie首先计算一个短签名$Cert_A=S_C P_A$, 其中$P_A=H_1(i, PK_C, PK_A, W)$, 然后将$(Cert_A, W)$传送给Alice($Cert_A$及$W$传送给Alice时可以公开, 不需要秘密信道)。Alice验证以下等式是否成立:

$$e(Cert_A, P)=e(H_1(i, PK_C, PK_A, W), PK_C)$$

如果成立, Alice计算其代理签名密钥:

$$SKP_A=Cert_A+S_A P_A=(S_C+S_A)P_A$$

4.3 签名算法

(1) 代理签名人Alice随机选择$x\in_R Z_q^*$, 计算$K=xP_A$, 将K和P_A发送给Bob;

(2) 盲化: 消息持有人Bob随机选择两个盲因子$t_1, t_2\in_R Z_q^*$, 计算: $K'=t_1 K+t_1 t_2 P_A$和$h=t_1^{-1}H_2(M\| K')+t_2$, 并将$h$发送给代理签名人Alice;

(3) Alice收到h后, 计算$S=(x+h)SKP_A$, 将S发送给消息持有人Bob;

(4) 脱盲: 消息持有人Bob计算$S'=t_1 S$, 最后将$(m)=(K', S', M, W)$作为Alice对消息M的代理盲数字签名。

4.4 签名验证算法

已知基于身份的代理盲签名$(M)=(K', S', M, W)$, 验证

人验证下列等式是否成立:

$\hat{e}(S',P)=\hat{e}(K'+H_2(M\|K')P_A,PK_C+PK_A)$

如果等式成立,则签名 $\phi(M,\tilde{K}',S',M,W)$ 是 Alice 代表Charlie 的盲签名,Bob 接受;否则,为非法代理盲签名,丢弃。签名验证等式的成立可以通过下列等式证明:

$$\begin{aligned}\hat{e}(S',P)&=\hat{e}(t_1S,P)=\hat{e}(t_1x+t_1h)SKP_A,P)=\\&\hat{e}(t_1x+H_2(M\|K')+t_1t_2)P_A,PK_C+PK_A)=\\&\hat{e}(t_1x+t_1t_2)P_A+H_2(M\|K')P_A,PK_C+PK_A)=\\&\hat{e}(K'+H_2(M\|K')P_A,PK_C+PK_A)\end{aligned}$$

5 安全性分析

作为代理签名和盲签名的结合,代理盲签名应该满足可验证性、可区分性、强可识别性、强不可伪造性、强不可否认性、防止滥用性、盲性以及不可链接性等安全性要求[6-13]。由于完整有效的代理盲签名 $\phi(M,\tilde{K}',S',M,W)$ 中包含了授权证书 W,而且授权证书 W、原始签名人 Charlie 和代理签名人 Alice 的公钥 PK_C、PK_A 都要在代理盲签名的验证算法中出现,易证新的基于证书的代理盲签名方案满足可验证性、可区分性、强可识别性、强不可否认性、抗滥用性。下面分析所提出的新方案满足强不可伪造性、盲性以及不可链接性。

5.1 强不可伪造性

定理 1 基于证书的代理盲签名是强不可伪造的。

证明 因为主密钥 S_C 被 Charlie 秘密保存,通过 $PK_C=S_CP$ 得到 S_C 相当于破解 DLP。H_1 和 H_2 均为密码学上的强无碰撞安全单向 Hash 函数。因此,除代理签名人 Alice 以外的其他人(包括原始签名人和任何第三方)都不能通过原始签名人和代理签名人的公钥 PK_C 及 PK_A 来建立有效的代理密钥。即使攻击者和用户 Bob 合谋使伪造的对消息 M 的代理盲签名 (K',S',M,W) 通过验证,他们必须使 (K',S',M,W) 满足验证式:

$\hat{e}(S',P)=\hat{e}(K'+H_2(M\|K')P_A,PK_C+PK_A)$

然而 e 是一个安全的双线性对,找到一组数 (K',S',M,W) 满足上式在计算上是不可行的,所以满足强不可伪造性。

5.2 盲性

定理 2 基于证书的代理盲签名方案满足盲性。

证明 根据 Juels 等人[14]和 Abe 等人[15]对盲性所做的定义,下面证明代理签名人不能得到关于签名和被签消息的任何信息。根据签名算法,如果给定一个有效的代理盲签名 (K',S',M,W) 以及在签名发行过程中交换的数据 (K,h,S),下列等式成立:

$$S=t_1S \tag{1}$$

$$h=t_1^{-1}H_2(M\|K')+t_2 \bmod q \tag{2}$$

$$K=t_1K+t_1t_2P_A \tag{3}$$

很显然,对于任意合法的签名 (K',S',M,W),必存在一个唯一的盲因子 $t_1\in Z_q^*$ 满足等式(1),其中 $t_1=\log_S S'$;同理,也必存在另一个唯一的盲因子 $t_2\in Z_q^*$ 满足等式(2),其中 $t_2=h-t_1^{-1}H_2(M\|K')$。对于等式(3),根据双线性映射的非退化性,有:

$K=t_1K+t_1t_2P_A\Leftrightarrow$

$$\hat{e}(K',PK_C+PK_A)=\hat{e}(t_1K+t_1t_2P_A,PK_C+PK_A) \tag{4}$$

因此,只需证明存在两个盲因子 (t_1',t_2') 满足等式(4)。证明如下:

$$\begin{aligned}&\hat{e}(t_1K+t_1t_2P_A,PK_C+PK_A)=\\&\hat{e}(\log_SS'K+\log_SS'(h-(\log_SS')^{-1}H_2(M\|K'))P_A,PK_C+PK_A)=\\&\hat{e}(\log_SS'xP_A+\log_SS'hP_A,PK_C+PK_A)\hat{e}(H_2(M\|K'))P_A,PK_C+PK_A)^{-1}=\\&\hat{e}(\log_SS'(x+h)SKP_A,P)\hat{e}(S',P)^{-1}\hat{e}(K',PK_C+PK_A)=\\&\hat{e}((\log_SS')\cdot S,P)\hat{e}(S',P)^{-1}\hat{e}(K',PK_C+PK_A)=\hat{e}(K',PK_C+PK_A)\end{aligned}$$

从以上的推导过程可知盲因子 (t_1',t_2') 总是存在且能满足等式(4)的定义,因此本文提出的基于证书的代理盲签名具有盲性。

5.3 不可链接性

定理 3 基于证书的代理盲签名方案具有不可链接性。

证明 代理盲签名 $\phi(M,\tilde{K}',S',M,W)$ 是由消息持有人 Bob 进行脱盲变化后形成的,由于群 G_1 上的离散对数问题是难解的,因此代理签名人 Alice 不能通过 $S=t_1S$ 计算出盲因子 t_1 和 t_2。即使代理签名人 Alice 保存了 K、S,当代理盲签名 (K',S',M,W) 公布后,他也不能确定代理盲签名 (K',S',M,W) 是他的哪一次签名,所以新方案具有不可链接性。

6 效率分析

6.1 短签名

本文方案的代理盲签名长度很短:代理签名是群 G_1 中的两个元素,利用点压缩技术,每个元素的表示只需要 160 位,从而代理盲签名的长度为 320 位,相对以前基于 RSA 或者 Z_q^* 离散对数难题构造的代理盲签名长度都要短很多。

6.2 计算复杂性

在代理盲签名方案中,应尽可能地减少对运算以提高效率。表 1 将本文提出的代理盲签名方案和 Z-H-C 方案[11]、L-T-Y 方案[12]以及 Z-W 方案[13]从计算复杂性方面进行了比较。表 1 中有关符号的定义如下:P_a 表示双线性映射中的对操作,P_m 表示 G_1 上的标量乘,A_d 表示 G_1 上的点加操作,M_d 表示 Z_q 上的乘操作,I_m 表示 Z_q 上的求逆操作,M_dG_2 表示 G_2 上的乘操作,E_xG_2 表示 G_2 上的指数运算。这里忽略了所有的哈希运算,而且在考虑计算复杂性时已经对 Z-H-C 方案、L-T-Y 方案和 Z-W 方案中的相关双线性对进行了预计算。

表 1 本文方案与其他方案的计算复杂性比较

方案	代理密钥生成阶段	签名生成阶段	签名验证阶段
Z-H-C 方案	$2P_a+4P_m+1M_dG_2+1E_xG_2+4A_d$	$2P_a+6P_m+5A_d$	$3P_a+1P_m+1M_dG_2+1E_xG_2+1A_d$
L-T-Y 方案	$1P_a+2P_m+1E_xG_2+1A_d$	$1P_a+6P_m+5A_d$	$1P_a+1M_dG_2+1E_xG_2+1A_d$
Z-W 方案	$1P_a+2P_m+1E_xG_2+1A_d$	$5P_m+1M_dG_2+3E_xG_2+2A_d$	$1P_a+1M_dG_2+1E_xG_2+1A_d$
本文方案	$1P_a+2P_m+1A_d$	$5P_m+1A_d+1M_d+1I_m$	$2P_a+1P_m+1A_d$

从表 1 可以看出,本文方案的效率比 Z-H-C 方案的效率要高得多,同时比 L-T-Y 方案的效率也高。本文方案和 Z-W 方案在生成签名阶段都不需要双线性对运算,而 Z-H-C 方案和 L-T-Y 方案则分别需要 2 个和 1 个双线性对运算。和 Z-W 方案相比,本文方案在代理密钥生成阶段和签名生成阶段的效率比较高,而在签名的验证阶段,本文方案需要 2 个双线性对运算。电子货币是代理盲签名在电子商务领域中的一个重要应用。在电子货币系统中,对代理盲签名的验证由商家来完成,不失一般性,可以假定商家有比用户更强的计算能力。

6.3 批量验证

当需要同时验证数量很大的签名时,本文方案的效率优势会更加明显。例如:银行指定其信赖的部门代表其发行了大量的电子货币,客户希望能够迅速地验证这些货币的合法性。这

(下转 165 页)

的问题。

6　结语

本文从数学规划的角度重新表述了单维布尔型频繁项挖掘问题,并利用新定义的加法和数乘及范数运算将其归结为一个非线性 0-1 规划问题,更加清晰和严格地描述了频繁项挖掘问题。通过对频繁项挖掘问题困难原因的讨论,确立了以数据库记录作为初始种群,直接以 0-1 变量作为是否包含项目的变量,利用遗传算法进行求解的方法。实际计算结果表明,该方法一般在几代内即可找到一批长频繁模式。

对初始种群选择的深入研究、对遗传算法中适应数据挖掘的新个体产生的方法的深入研究是将来的研究方向。

参考文献:

[1] 刘同明.数据挖掘技术及其应用[M].北京:国防工业出版社,2001.

[2] 张云涛,龚玲.数据挖掘原理与技术[M].北京:电子工业出版社,2004.

[3] Agrawal R,Imielinski T,Swami A.Mining association rules between sets of items in large database[C]//Proc of the ACM SIGMOD Intl Conf on Management of Data,Washington D C,1993:207-216.

[4] Park J S,Chen M S,Yu P S.An effective hash based algorithm for mining association rules[C]//ACM SIGMOD International Conference Management of Data,1995:175-186.

[5] Savasere A,Omiecinski E,Navathe S.An efficient algorithm for raining association rules in large database[C]//Proc of 2nd Intl Conf on Very Large Database,Zurich,Swaziland,1995:432-443.

[6] Pasquier N,Bastide Y,Taouil R,et a1.Discovering frequent closed item sets for association rules[C]//ICDT'99,Israel,1999:398-416.

[7] Han Jia-wei,Kamber M.Data mining:concepts and techniques[M].[S.l.]:Morgan Kaufmann Publishers,2001.

[8] Pasquoer N,Bastide Y,Taouil R.Efficient mining of association rules using closed itemset lattices[J].Information System,1999,24(1):25-46.

[9] Berzal F do,Cubero J C,Marin N.TBAR:an efficient method for association rule mining in relational databases[J].Data & Knowledge Engineering,2001,37:47-64.

[10] 皮德常,秦小麟,王宁生.基于动态剪枝的关联规则挖掘算法[J].小型微型计算机系统,2004(10):1850-1852.

[11] Borgelt C.Efficient implementations of Apriori and Eclat[C]//Proc of 1st IEEE ICDM Workshop on Frequent Item Set Mining Implementations(FIMI 2003,Melbourne,FL),CEUR Workshop Proceedings 90,Aachen,Germany,2003.

[12] 张禾瑞,赫炳新.高等代数[M].3 版.北京:高等教育出版社,1993.

[13] 史忠植.知识发现[M].北京:清华大学出版社,2002.

[14] Synthetic data generation code for associations and sequential patterns.Intelligent Information Systems,IBM Almaden Research Center.http://www.almaden.ibm.com/software/quest/Resources/index.shtml.

[15] Zaki M J.Scalable algorithms for association mining[J].IEEE Transactions on Knowledge and Data Engineering,2000,12(3):372-390.

[16] 刘淳安.解非线性规划的多目标遗传算法及其收敛性[J].计算机工程与应用,2006,42(25):27-29.

(上接 126 页)

里假设(K_1,S_1'),(K_2,S_2'),…,(K_n,S_n')是消息 M_i($i=1,\cdots,n$)的代理盲签名,M_i 对应同一个代理授权证书 W,进行批量验证时只需要验证以下等式是否成立:

$$(\sum_{i=1}^{n} S_i', P) = (\sum_{i=1}^{n} K_i + \sum_{i=1}^{n} H(M_i \| K_i')P_A, PK_C + PK_A)$$

如果对 n 个签名进行逐一验证,那么将需要消耗的计算代价为 $2nP_a+nP_m+nA_d$,而进行批量验证时,计算代价仅为 $2P_a+1P_m+(3n-1)A_d$。

7　结束语

本文针对基于身份的代理盲签名方案不能有效抵抗伪造攻击和不具有不可链接性等缺陷,利用双线性对构造了一种新型的基于证书的代理盲签名方案,通过比较分析,本方案具有更高的安全性和效率等优点。

参考文献:

[1] Shamir A.Identity-based cryptosystems and signature schemes[C]//LNCS 196 Crypto 1984,Berlin,1984:47-53.

[2] Gentry C.Certificate-based encryption and the certificate revocation problem[C]//LNCS 2656:Advances in Cryptology-EUROCRYPT 2003.[S.l.]:Springer-Verlag,2003:272-293.

[3] Al-Riyami S S,Paterson K G.Certificateless public key cryptography[C]//LNCS 2894:Advances in Cryptology-ASIACRYPT 2003.Berlin:Springer-Verlag,2003:452-473.

[4] Girault M.Self-certified public keys[C]//LNCS 434:Advances in Cryptology:Proc Eurocrypt 1991.[S.l.]:Springer,1991:490-497.

[5] Chen X,Zhang F,Kim K.A new ID-based group signature scheme from bilinear pairings[EB/OL].[2006].http://eprint.iacr.org/2003/116.pdf.

[6] Lin W D,Jan J K.A security personal learning tools using a proxy blind signature scheme[C]//Proceedings of International Conference on Chinese Language Computing,Illinois,USA,2000:273-277.

[7] 谭作文,刘卓军,唐春明.基于离散对数的代理盲签名[J].软件学报,2003,14(11):1931-1935.

[8] 王蜀洪,王贵林,鲍丰,等.对一个基于离散对数代理盲签名的密码分析[J].软件学报,2005,16(5):911-915.

[9] Awasth I AK,Lal S.Proxy blind signature scheme[J].JFCR Transaction on Cryptology,2005,2(1):5-11.

[10] Sun H M,Hsieh B T.On the security of some proxy blind signature schemes[J/OL].[2003].http://eprint.iacr.org/2003/68.

[11] Zheng D,Huang Z,Chen KF.ID-based proxy blind signature[C]//ANNA 2004,IEEE Computer Society,2004,2:380-383.

[12] Lang W M,Tan Y M,Yang Z K.A new efficient ID-based proxy blind signature scheme[C]//ISCC 2004,IEEE Computer Society,2004,1:407-411.

[13] 张学军,王育民.高效的基于身份的代理盲签名[J].计算机应用,2006,26(11):2586-2588.

[14] Juels A,Luby M,Ostrovsky R.Security of blind digital signatures[C]//LNCS 1294:Advances in Cryptology-Crypto 97.[S.l.]:Springer-Verlag,1997:150-164.

[15] Abe M,Okamoto T.Provably secure partially blind signatures[C]//LNCS 1880:Advances in Cryptology-Crypto 2000.[S.l.]:Springer-Verlag,2000:271-286.