CN43-1258/TP
ISSN 1007-130X
计算机工程与科学
COMPUTER ENGINEERING & SCIENCE
2009 年第 31 卷第 8 期
Vol 31, No 8, 2009

文章编号: 1007-130X(2009)08-0024-03

一种基于身份的群盲签名方案*

An Identity-Based Group Blind Signature Scheme

袁遇晴[1,2], 韩晓花[1], 李乔良[1]

YUAN Yu-qing[1,2], HAN Xiao-hua[1], LI Qiao-liang[1]

(1. 湖南大学计算机与通信学院, 湖南 长沙 410082; 2. 湖北汽车工业学院信息管理系, 湖北 十堰 442002)

(1. School of Computer and Communications, Hunan University, Changsha 410082;
2. Department of Information Management, Hubei University of Automotive Technology, Shiyan 442002, China)

摘 要: 基于身份和盲签名是当代密码学领域两个重要的概念, 基于身份用来简化基于证书的公钥环境中的密钥管理; 盲签名在实际应用中起着保护消息发送方隐私权的重要作用。本文将 Paterson 基于椭圆曲线的基于身份的签名方法与盲签名技术结合而提出一个新的基于身份的盲签名方案, 并利用已有的转换方法, 把我们提出的盲签名方案转换成一个群盲签名方案。分析表明, 新的方案满足不可伪造性、匿名性、可追踪性及不可陷害性等安全特性; 更重要的是, 该群签名以及群公开密钥的长度都与群成员的个数无关, 因此更适合群成员较多的大群。

Abstract: Identity-based signature and blind signature are two important concepts in the current cryptology. The identity-based scheme simplifies the key management in the certificate-based public key systems, and in practical applications. Blind signature plays an important role in the protection of the message sender's privacy. This paper presents a blind signature scheme based on the current identity-based signature, and then converts it to a group blind signature by the current convertsion method. Analysis shows that the new scheme meets the demands of unforgeability, anonymity, traceability and no-framing features, etc. Due to the independence between the group public key with the length of signature and the number of group members. This new scheme is suitable for large groups which contain a large number of members.

关键词: 基于身份; 群签名; 盲签名; 双线性对

Key words: identity-based; group signature; blind signature; bilinear pairing

中图分类号: TP309 文献标识码: A

1 引言

Chaum 于 1983 年提出了盲签名的概念[1], 之后对盲签名的研究不断深入, 强盲签名、部分盲签名的概念[2,3]陆续被提出。盲签名是一种特殊的数字签名, 要求签名者对所签署的消息是不可见的, 即消息持有者在不暴露消息内容的前提下获得签名者对真实消息的有效签名。基于盲签名的特点, 盲签名技术在电子货币、电子投票和电子支付等应用中的匿名性方面起着重要作用, 国内外学者就此进行了相关研究并取得了一定成果[4~7]。

1991 年, Chaum 和 Heyst 提出群签名[8]的概念。该技术允许群里任何成员以匿名的方式代表此群签署文件, 而任何验证者只需一把群公开密钥即可验证此数字签名的合法性。此外, 验证者无法从此签名中推出签署人的身份, 只有合法的群管理员可以追查出签署人的真实身份。群签名可被用来隐藏群的内部架构以及减少验证签名所需的密钥数量。群盲签名是由 Lysyanskaya A 等人提出的。群盲签名使得电子货币可以由多个银行发布, 从而使电子货币的应用更为广泛。

Shamir 于 1984 年提出基于身份的密码系统的概念后, 陆续有许多方法被提出[9~11], 然而这些方法都没有完全满足基于身份的密码系统的需求。例如, 部分方法要求使用者不能共谋, 有些方法在计算使用者私钥时需要大量的运算, 还有些系统需要防止篡改的硬件设备。2001 年 Boneh 和 Franklin 提出基于椭圆曲线上双线性对特性的基于身份的

* 收稿日期: 2009-01-03; 修订日期: 2009-04-09
基金项目: 国家自然科学基金资助项目(10571052); 湖南省教育厅优秀青年基金资助项目(04B047); 湖北省教育厅项目基金(2005q122)
作者简介: 袁遇晴 (1981-), 女, 湖北十堰人, 硕士生, 研究方向为电子商务和信息安全; 韩晓花, 硕士生, 研究方向为信息安全; 李乔良, 教授, 研究方向为信息安全和网络容错。
通讯地址: 442002 湖北省武汉市汽车工业学院信息管理系; Tel: 13477322226; E-mail: yyq115805@163.com
Address: Department of Information Management, Hubei University of Automotive Technology, Shiyan, Hubei 442002, P. R. China

密码系统，是第一个实用性较好的基于身份的加解密系统。之后提出的基于身份的数字签名方法[12~14]以及身份码密钥配置方法，也是基于椭圆曲线上的双线性对的。

2002 年 Paterson 利用椭圆曲线上双线性对特性提出一个新的基于身份签名方法。该系统有一个私钥产生中心(Private Key Generator，简称 PKG)，主要负责发放每个使用者的秘密密钥，而使用者的公开密钥皆由该使用者的公开身份码(Identity)经过哈希函数运算而得到。本文就是在此文的基础上构建群盲签名方案，即基于身份的群盲签名方案。

2 预备知识

椭圆曲线的 Weil Pairing 特性：设 G_1 为一椭圆曲线加法循环群(Additive Cyclic Group)，其序(Order)为 q，而 G_2 为具有相同序 q 的乘法循环群(Multiplicative Cyclic Group)，Weil Pairing 为一映射(Map) $e: G_1 \times G_1 \to G_2$，$e$ 具有下列特性：

(1)同一性(Identity)：$\forall P \in G_1$，$e(P, P) = 1$；

(2)交替性(Alternation)：$\forall P_1, P_2 \in G_1$，$e(P_1, P_2) \equiv e(P_2, P_1)^{-1}$；

(3)双线性(Bilinear)：$\forall P_1, P_2, P_3 \in G_1$，$e(P_1 + P_2, P_3) \equiv e(P_1, P_3) \cdot e(P_2, P_3)$

$\forall P_1, P_2, P_3 \in G_1$，$e(P_1, P_2 + P_3) \equiv e(P_1, P_2) \cdot e(P_1, P_3) \Rightarrow P, Q \in G_1$，$e(a \cdot P, b \cdot Q) \equiv e(P, Q)^{ab}$；

(4)非退化性(non-degeneracy)：$\forall P_2 \in G_1$，$e(P_1, P_2) = 1$ implies $P_1 \equiv O$

$\forall P_1 \in G_1$，$e(P_1, P_2) = 1$ implies $P_2 \equiv O$。

3 基于身份的群盲签名方案

3.1 Paterson 的基于身份的数字签名

用基于身份的加解密方法，Paterson 以可以利用的双线性对来实现其基于身份的数字签名[13]。G_1 为一椭圆曲线加法循环群，其序为一质数 q，G_2 为具有相同序 q 的乘法循环群，可以利用的双线性对为一映射 $\hat{e}: G_1 \times G_1 \to G_2$，使得离散对数问题在 G_1 及 G_2 下都很难在有效时间内被计算出来。

(1)系统初始阶段。ID 为一使用者的身份码，而 H_1、H_2 及 H_3 为满足下列特性的单向哈希函数：

$H_1: \{0, 1\}^* \to G_1$，$H_2: \{0, 1\}^* \to Zq^*$，$H_3: G_1 \to Zq^*$

系统首先选择生成元 $P \in G_1$，接着随机选择整数 $s \in Zq^*$ 为系统秘密值，系统的公钥 $P_{Pub} = s \cdot P$，$\{G_1, G_2, P, P_{Pub}, H_1, H_2, H_3\}$ 为系统公开参数；此外，身份为 ID 的使用者，其公钥为 $Q_{ID} = H_1(ID)$，由 PKG 产生的相对私钥 $D_{ID} = s \cdot Q_{ID}$。

(2)签名产生阶段。若要对一信息 m 做数字签名，使用者首先随机产生整数 $k \in \mathbf{Z}q^*$，并计算信息 m 的数字签名(R, S)如下：$R = k \cdot P$，$S = k^{-1}(H_2(m) \cdot P + H_3(R) \cdot D_{ID})$，其中 k^{-1} 为随机值 k 在 Zq^* 下的乘法逆元素。

(3)签名验证阶段。若要验证信息 m 的数字签名(R, S)，验证者首先计算 $\hat{e}(R, S)$，并和 $\hat{e}(P, P)^{H_2(m)} \cdot \hat{e}(P_{Pub}, Q_{ID})^{H_3(R)}$ 做比较，若两者相同，则可确定(R, S)确实是身份为 ID 的使用者对信息 m 所产生的数字签名。

证明

$$\hat{e}(R, S) = \hat{e}(k \cdot P, k^{-1}(H_2(m) \cdot P + H_3(R) \cdot D_{ID})) =$$
$$\hat{e}(P, H_2(m) \cdot P + H_3(R) \cdot D_{ID}) =$$
$$\hat{e}(P, H_2(m) \cdot P) \cdot \hat{e}(P, H_3(R) \cdot D_{ID}) =$$
$$\hat{e}(P, P)^{H_2(m)} \cdot \hat{e}(P, D_{ID})^{H_3(R)} =$$
$$\hat{e}(P, P)^{H_2(m)} \cdot \hat{e}(P_{Pub}, Q_{ID})^{H_3(R)} \quad \square$$

(4)签名的效率。产生签名时只需两次哈希函数运算、椭圆曲线上的四次乘法运算、一次加法运算以及一个求乘法反元素运算即可，并不需计算双线性对 $\hat{e}$。而验证签名时需要三次双线性对 $\hat{e}$ 运算和二次指数运算。其中，$\hat{e}(P, P)$为 G_2 中的固定值，只要计算一次并将结果储存起来即可省去日后的重复计算；另外，$\hat{e}(P_{Pub}, Q_{ID})$和所签署的文件内容无关，因此对同一签署者来说皆为固定值，所以也可通过预先运算来减少验证所需要的时间。

下节接着介绍如何将 Paterson 的基于身份的签名方法加入盲签名的特性。

3.2 基于身份的盲签名

为了将 Paterson 基于身份的签名加入盲签名的特性，我们修改其签名产生阶段使其具有下列特性：

(1)在签名过程中签署人不会知道文件内容；

(2)在签名过程中签署人不会泄露其私钥；

(3)签署人无法得知或追踪其产生的盲签名；

(4)产生出来的签名无法延伸成为其它文件的签名。

(1)系统初始阶段。用 3.1 节的 Paterson 基于身份的签名方法，PKG 首先选择 $P \in G_1$，接着随机选择整数 $s \in Zq^*$ 当做其系统秘密值，并公开系统的公钥为 $P_{Pub} = s \cdot P$，$\{G_1, G_2, P, P_{Pub}, H_1, H_2, H_3\}$ 为系统公开参数，其中 H_1、H_2 及 H_3 为满足下列特性的单向哈希函数：$H_1: \{0, 1\}^* \to G_1$，$H_2: \{0, 1\}^* \to Zq^*$，$H_3: G_1 \to Zq^*$。而使用者的公钥为 $Q_{ID} = H_1(ID)$，其相对的私钥为 $D_{ID} = s \cdot Q_{ID}$。注意 D_{ID} 是由 PKG 所产生的。

(2)盲签名产生阶段。假设 Alice 有一文件 m 想取得 Bob 的盲签名，而 Bob 的公钥为 $Q_B = H_1(ID_B)$，私钥为 $D_B = s \cdot Q_B$。图 1 为所设计的基于身份的盲签名方法。

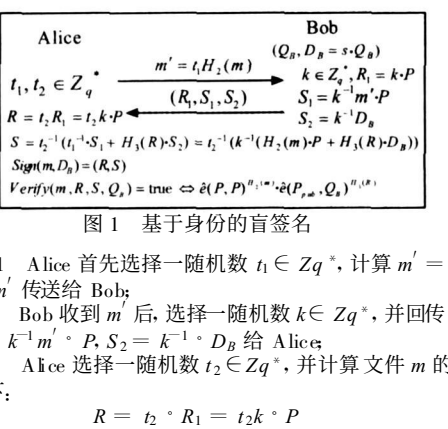

图 1 基于身份的盲签名

步骤 1 Alice 首先选择一随机数 $t_1 \in Zq^*$，计算 $m' = t_1 H_2(m)$，并将 m' 传送给 Bob；

步骤 2 Bob 收到 m' 后，选择一随机数 $k \in Zq^*$，并回传 $R_1 = k \cdot P$，$S_1 = k^{-1} m' \cdot P$，$S_2 = k^{-1} \cdot D_B$ 给 Alice；

步骤 3 Alice 选择一随机数 $t_2 \in Zq^*$，并计算文件 m 的签名(R, S)如下：

$$R = t_2 \cdot R_1 = t_2 k \cdot P$$
$$S = t_2^{-1}(t_1^{-1} \cdot S_1 + H_3(R) \cdot S_2) =$$

$$t_2^{-1}(t_1^{-1}k^{-1}m'\circ P+H_3(R)k^{-1}\circ D_B)=$$
$$t_2^{-1}(t_1^{-1}k^{-1}t_2H_2(m)\circ P+H_3(R)k^{-1}\circ D_B)=$$
$$t_2^{-1}(k^{-1}(H_2(m)\circ P+H_3(R)\circ D_B))$$

(3)盲签名验证阶段。若要用签署人的公钥 Q_B 验证信息 m 签名(R, S)，验证者首先计算 $\hat{e}(R, S)$并和 $\hat{e}(P, P)^{H_2(m)}\circ\hat{e}(P_{Pub}, Q_B)^{H_3(R)}$ 比较，若两者相同，则可确定(R, S)确实是 Bob 对信息所产生的数字签名。

定理 1 若(R, S)为Bob 对文件 m 产生的有效的基于身份的盲签名，则 $\hat{e}(R, S)=\hat{e}(P, P)^{H_2(m)}\circ\hat{e}(P_{Pub}, Q_B)^{H_3(R)}$。

证明

$$\hat{e}(R, S)=\hat{e}(t_2k\circ P, t_2^{-1}(k^{-1}(H_2(m)\circ P+$$
$$H_3(R)\circ D_B)))=\hat{e}(P, H_2(m)\circ P+H_3(R)\circ D_B)=$$
$$\hat{e}(P, P)^{H_2(m)}\circ\hat{e}(P, D_B)^{H_3(R)}=$$
$$\hat{e}(P, P)^{H_2(m)}\circ\hat{e}(P_{Pub}, Q_B)^{H_3(R)}$$ □

3.3 群盲签名

我们利用文献[15]的方法将 3.2 节所提出的基于身份的盲签名转换成一群盲签名，如此转换除了效率取决于原本基于身份的签名方法和保证安全性外，还具有群签名以及群公钥的长度与群成员的个数无关的特性，因此较其它现有的群签名更有效且更适合群成员较多的大群。

(1)系统初始阶段。系统首先选择生成元 $P\in G_1$ 以及下列三个单向哈希函数：$H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\rightarrow Zq^*$，$H_3: G_1\rightarrow Zq^*$，接着群管理员选择一随机整数 $s\in \mathbf{Z}q^*$ 当做其管理员秘密值，群的公钥为 $P_G=s\circ P$，而系统的公开参数为$\{G_1, G_2, P, P_G, H_1, H_2, H_3\}$。

(2)群成员注册阶段。假设有一新的群成员 U_i 要加入此群，群管理员首先替其产生匿名身份码 AID_i，并计算该成员的公钥 Q_{AIDi} 以及私钥 D_{AIDi} 如下：

$$Q_{AID_i}=H_1(AID_i), D_{AID_i}=sQ_{AID_i}$$

(3)群盲签名产生阶段。与 3.2 节基于身份的盲签名的产生阶段相同，参考图 1，此时群成员的签署人 Bob 用群管理员所分发的匿名私钥 D_{AIDB} 来签署文件。

(4)群盲签名验证阶段。若要验证匿名成员 AID_B 对信息的群盲签名(R, S)，验证者首先计算 $\hat{e}(R, S)$并和 $\hat{e}(P, P)^{H_2(m)}.\hat{e}(P_G, Q_{AID_i})^{H_3(R)}$ 比较，若两者相同，则可确定(R, S)确实是某群成员对信息所产生的群盲签名。

(5)群盲签名开封阶段。给定任何合法的群签名(R, S)以及签署成员的匿名身份码 AID_i，群管理员可以追查出签署成员的真实身份，因为群管理员知道任何匿名身份码 AID_i 与群成员 U_i 的对应关系，此关联是在群成员注册阶段所建立的。

4 安全性分析和效率评估

我们提出的群盲签名除满足 3.2 节的四点安全性外，也满足下列安全性：

(1)不可伪造性(Unforgeability)。我们假设一拥有文件 m 的请求者以正常程序产生 $m'=t_1H_2(m)$，并将 m' 传送给一假冒群成员 U_i 的攻击者。攻击者在不知道管理员秘密值 s 及 U_i 的成员私钥 D_{AIDi} 的情况下，伪造成员私钥 $D_{AIDi}'=x\circ Q_{AIDi}$，其中 $x\in \mathbf{Z}q^*$ 为攻击者随意选取，并回传 R'_1、S'_1及 S'_2给请求者，$R1'=k\circ P, S_1'=k^{-1}m'\circ P$，$S_2'=k^{-1}\circ D_{AID_i}'$，其中 $k\in Zq^*$ 为攻击者随机选取。请求者接着以正常程序产生文件 m 的群签名(R, S)如下：

$$R=t_2\circ R_1=t_2k\circ P$$
$$S=t_2^{-1}(t_1^{-1}\circ S_1+H_3(R)\circ S_2')=$$
$$t_2^{-1}(t_1^{-1}k^{-1}m'\circ P+H_3(R)S_2')=$$
$$t_2^{-1}(t'^{-1}k^{-1}t_2H_2(m)\circ P+H_3(R)k^{-1}\circ D_{AID_i}')=$$
$$t_2^{-1}(k^{-1}(H_2(m)\circ P+H_3(R)\circ D_{AID_i}'))$$

然而，此伪造的群签名(R, S)将无法满足下列验证式 $\hat{e}(R, S)\equiv\hat{e}(P, P)^{H_2(m)}\circ\hat{e}(P_G, Q_{AID_i})^{H_3(R)}$，因为：

$$\hat{e}(R, S)=\hat{e}(t_2k\circ P, t_2^{-1}(k^{-1}(H_2(m)\circ P+$$
$$H_3(R)\circ D_{AID_i}')))=$$
$$\hat{e}(P, (H_2(m)\circ P+H_3(R)\circ D_{AID_i}'))=$$
$$\hat{e}(P, P)^{H_2(m)}\circ\hat{e}(P, D_{AID_i}')^{H_3(R)}\neq$$
$$\hat{e}(P, P)^{H_2(m)}\circ\hat{e}(P_G, Q_{AID_i})^{H_3(R)}$$

(2)匿名性(Anonymity)。由于群成员的匿名身份 AID_i 与该成员真实身份 U_i 的对应关系只有群管理员知道，而在群盲签名产生阶段，签署成员是利用匿名身份 AID_i 来对文件进行签署，因此除了群管理员外，任何人均无法从一群签名中推导出签署成员的真实身份。

(3)可追踪性(Traceability)。只要群成员的秘密密钥是在群成员注册阶段由群管理员所分发的，群管理员必定可利用群盲签名开封阶段的方法追查出签署成员的真实身份，达到可追踪性。

(4)不可陷害性(No framing)。每一成员秘密密钥只有该成员及群管理员知道，因此其它成员无法伪造该成员的签名，即具有成员间的不可陷害性；然而，成员秘密密钥为群管理员所分发，因此群管理员可以假冒其它成员身份来进行签名，文献[15]讨论了到如何以另外的可信任机构(Trustee)来解决此问题。

(5)效率评估。群签名以及群公开密钥的长度与群成员的个数无关，在新成员加入时并不需更改，群公开密钥具有可扩充性，且适合群成员较多的大群，此外也可通过预先运算来减少验证的时间。

5 结束语

在本文中，我们扩展 Paterson 基于椭圆曲线 Wei pairing 特性的基于身份的签名方法，并与盲签技术结合而提出了一个新的基于身份的盲签名方法。利用文献[15]的转换方法，我们所提出的基于身份的盲签名可以转换成一群盲签名，这样的群签名以及群公开密钥的长度都与群成员的个数无关，因此更适合群成员较多的大群。

参考文献：

[1] Chaum D. Blind Signature for Untraceable Payments[C] // Proc of Crypto' 82, 1983: 199-203.

[2] Harn L. Cryptanalysis of the Blind Signature Based on the Discrete Logarithm Problem[J]. Electronics Letters, 1995, 31(14): 1136-1140.

[3] Masayukiabe, Fujisaki E. How to Date Blind Signatures[C]

(下转第 32 页)

Port、攻击时间等。

假定已经将预先输入的警报数据聚合成为 m 个类 C_1, C_2, …, C_m，对于给定一个新检测到的警报数据 A，需要将 A 与 C_1, C_2, …, C_m 中的每一个类进行比较，计算警报之间的加权相似度 $SIM(A, C_i)$。若 $SIM(A, C_i)$ 大于 H（H 是预先给定的概率阈值，可以由专家知识给出，也可以通过机器学习的方法自动从大量训练样本中获取），则把 A 加入类 C_i；否则创建新的分类 C_{m+1}，把 A 加入新类 C_{m+1}。

警报聚类关联算法中警报之间的加权相似度函数的计算公式为：

$$SIM(A, C_i) = \frac{\sum_{j=1}^{n} w_j SIM(A_j, C_{ij})}{\sum_{j=1}^{n} w_j}$$

其中，A 为待分类的警报向量；C_i 为某一分类；A_j、C_{ij} 为警报向量和分类的各关键属性，包括攻击类别、攻击源 IP 和源 Port、攻击目的 IP 和 Port、攻击时间等；w_j 为各关键属性的匹配权值，根据该关键属性在整体匹配中的影响程度而定；相应的 $SIM(A_j, C_{ij})$ 可根据实际情况规定。

新的警报数据不断加入到一个类或簇时，形成聚类以后，还可根据需要进一步对其中的警报进行合并表示。一个基于相同攻击类型、相同攻击源聚类和合并的示例如表 1 所示，其中 30 为在警报 10 和警报 20 基础上新生成的关联警报。

表 1　相同攻击类型、相同攻击源聚类和合并的示例

项目	项目内容		
警报标识	10	20	30
攻击类型	portscan	portscan	portscan
攻击开始时间	19:20:10	19:20:11	19:20:10
攻击源 IP 地址	xxx.xxx.130.21	xxx.xxx.130.21	xxx.xxx.130.21
攻击源端口	1064, 1065	1064, 1065	1064, 1065
攻击目的 IP 地址	xxx.xxx.150.229	xxx.xxx.150.231, xxx.xxx.150.232	xxx.xxx.150.229, xxx.xxx.150.231, xxx.xxx.150.232
攻击目的端口	11121	11121, 21300	11121, 21300
参考警报标识			10, 20

4　结束语

入侵检测系统是利用警报数据向网络管理员或者安全管理员报告网络和系统的安全状况的，警报数据关联是分布式 IDS 检测的最重要组件，可直接影响入侵检测系统在实际应用中的效果。本文对分布式入侵检测系统的警报数据关联进行了研究，提出了一种分布式入侵检测警报数据关联模型，并给出了警报数据相似度聚类实现算法。使用该模型和关联方法能较为快速有效地实现对警报数据时间、空间以及过程的多层次、多角度的关联，达到去掉冗余、精确挖掘和识别入侵情况的目的，提高了系统的检测效率和精度。

参考文献：

[1] 曹大元. 入侵检测技术[M]. 北京：人民邮电出版社，2007.

[2] Snapp S R, Brentano J, Dias G V, et al. DIDS (Distributed Intrusion Detection System): Motivation, Architecture, and an Early Prototype[C] //Proc of the 14th National Computer Security Conf, 1991: 167-176.

[3] Spafford E H, Zamboni D. Intrusion Detection Using Autonomous Agents[J]. Computer Networks, 2000, 34(4): 547-570.

[4] Cuppens F. Managing Alerts in a Multi-Intrusion Detection Environment[C] //Proc of the 17th Annual Computer Security Applications Conf, 2001: 22-32.

[5] Valeur F, Vigna G, Kruegel C. A Comprehensive Approach to Intrusion Detection Alert Correlation[J]. IEEE Trans on Dependable and Secure Computing, 2004, 1(3): 146-169.

[6] 韩景灵，孙敏. 入侵检测报警信息融合系统的构建与实现[J]. 计算机技术与发展，2007: 17(6): 159-162.

[7] Ning P, Cui Y, Reeves D S. Constructing Attacking Scenarios Through Correlation of Intrusion Alerts[C] //Proc of the 9th ACM Conf on Computer and Communications Security, 2002: 245-254.

（上接第 26 页）

//Proc of the Int' l Conf on the Theory and Applications of Cryptology and Information Security, 1996: 244-251.

[4] Okamoto T S. Provable Secure and Practical Identification Schemes and Corresponding Signature Schemes[C] //Proc of the 12th Annual Int' l Cryptology Conf on Advances in Cryptology, 1992: 31-53.

[5] Camenisch J L, Pivetean J M, Stadler M A. Blind Signatures Based on the Discrete Logarithm Problem[C] //Proc of Eurocrypt' 94, 1995: 428-432.

[6] 张方国，王常杰，王育民. 基于椭圆曲线的数字签名与盲签名[J]. 通信学报，2001, 22(8): 22-28.

[7] 张龙军，邹涛，沈均毅. 一种基于椭圆曲线密码体制的盲数字签名方案[J]. 计算机应用，2001, 21(3): 17-19.

[8] Chaum D, Heyst E. Group Signatures[C] //Proc of Eurocrypt' 91, 1991: 257-265.

[9] Desmedt Y, Quisquater J. Public-key Systems Based on the Difficulty of Tampering[C] //Proc of Crypto' 86, 1986: 111-117.

[10] Maurer U, Yacobi Y. Non-Interactive Public-Key Cryptography[C] //Proc of Crypto' 91, 1991: 498-507.

[11] Tanaka H. A Realization Scheme for the Identity-Based Cryptosystem[C] //Proc of Crypto' 87, 1987: 341-349.

[12] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing[C] //Proc of Advances in Cryptology ASIACRYPT' 01, 2001: 514-532.

[13] Paterson K G. ID-Based Signatures from Pairings on Elliptic Curves[J]. Electronics Letters, 2002, 38(18): 1025-1026.

[14] Hess F. Exponent Group Signature Schemes and Efficient Identity Based Signature Schemes Based on Pairings[EB/OL]. [2002-07-10]. http://eprint.iacr.org.

[15] Castelluccia C. How to Convert any ID-Based Signature Scheme into a Group Signature Scheme[R]. Technical Report 2002/116, 2002.