基于双线性映射的 ID -代理签名与指定验证者代理签名

彭双和[1,3]　韩　臻[1]　盛可军[2]

（1　北京交通大学 计算机与信息技术学院，中国北京，100044）

（2　海军工程大学，中国武汉，430033）

（3　北京机械工业学院计算中心，中国北京，100085）

摘　要　该文从双线性映射的性质出发提出了一个新的基于身份的带委任状的部分代理签名方案以及指定验证者的代理签名方案，并对其安全性与效率进行了分析。新提出的代理签名方案能有效地避免代理签名权的滥用。

关键词　代理签名　指定验证者的代理签名　双线性映射

一、引　　言

代理签名是指当某个原始签名人由于某种原因不能签名时，将签名权委派给他人（代理人）替自己行使签名权。指定验证者代理签名是指原始签名者将签名权委派给代理人替自己行使签名权时，代理人签名的有效性只能由指定的验证者验证。日常生活中，当一个管理者因出差在外不能行使签名权时，通常委派一个可靠的代理人替自己行使签名权，被委派的代理人只能对指定的文件进行签名。数字签名也有同样的情况。为防止代理签名者滥用授予的签名权，原始签名者通常希望指定一个签名验证者，使得代理签名者替自己行使签名权时只能生成由指定验证者验证的签名。

代理签名作为一种特殊的签名机制，自 1996 年 M. Mambo 在文献[1]提出后，由于其在众多领域都有重要的应用，而受到人们的广泛研究。代理签名分为四类[2]：完全代理签名、带委任状的代理签名、部分代理签名和带委任状的部分代理签名。带委任状的部分代理签名与其他三种形式的代理签名相比，安全性要高。在本文中，为简单起见，我们将带委任状的部分代理签名简称为代理签名。

一个代理签名方案必须满足如下四个安全属性[1]：

1）不可伪造性：只有代理签名者可以产生代表原始签名者的合法代理签名；原始签名者和其他人都不能产生一个合法的代理签名。

2）可验证性：验证者可以验证代理签名，一旦验证通过，则相信此签名确实是经授权的合法代理签名。

3）不可抵赖性：一旦代理签名者代替原始签名者产生了一个合法的代理签名，代理签名者不能抵赖此次签名行为。

4）可辨认性：任何人可从代理签名中辨认代理签名者的身份。指定验证者的代理签名方案在上述四个安全属性的基础上还应满足如下的安全性要求[3]。

5）可区别性：指定验证者可以区别代理签名者产生的代理签名和原始签名者产生的

正常签名。

6）只有由原始签名者指定的验证者才能验证代理签名的有效性。

7）原始签名者不能否认指定了签名验证者。

目前，实现代理签名机制主要是用公钥密码体制。1984 年 Shamir 在文献[4]中提出了基于身份的公钥密码体制 ID-PKC(identity-based public key cryptography)，与基于 PKI 的公钥系统相比，它能简化密钥管理。用户的公钥是由用户的身份信息(E-mail 地址、IP 地址、电话号码等)决定的。因此，用户的公钥不需要保存，可以由任何人根据其身份计算出来。用户的私钥由私钥生成中心 PKG(private key generators)根据用户的身份和主密钥统一生成，发放给用户。文献[5]比较了传统的 PKI 和 ID-PKC。人们对于基于传统 PKI 体制的数字签名方案研究较多，相应地，基于这种签名方案的代理签名方案研究得也比较多，如文献[2,3,6～10]等。然而，人们对基于 ID-PKC 的代理签名方案研究较少。

双线性映射是构建 ID-PKC 的基本工具[11~13]，比如，文献[11]中 Boneh-Franklin 提出的基于身份加密方案。最近，利用椭圆曲线上的 Weil/Tate 配对的双线性性质构造出了几个基于身份的数字签名方案，但到了 2003 年才出现第一个使用 GDH (gap Diffie-Hellman)群构建的可证明安全的基于双线性映射的身份数字签名方案[13]，其安全性是建立在 CDHP(computational Diffie-Hellman problem)困难的基础上。但文献[13]没有构建数字代理签名方案。本文在文献[13]的基础上提出了一个基于身份的代理签名方案和指定验证者的代理签名方案。与通常的代理签名方案一样，ID－代理签名方案和指定验证者 ID－代理签名方案也应分别满足上述的四个和七个安全性需求。

二、一个可证明安全的 ID -数字签名方案

一般来说，一个基于身份的数字签名方案由四个阶段组成：设置阶段、用户密钥产生阶段、签名阶段和签名验证阶段。前两个阶段由 PKG 运行。设置阶段，输入为一个安全参数，输出为 PKG 的公/私钥对(P_{pub},s)，其中 P_{pub}为 PKG 的公钥，s 为 PKG 的秘密主密钥；用户密钥产生阶段，输入 PKG 的主密钥和用户的身份 ID，输出用户的私钥 d_{ID}；签名阶段由签名的用户对给定的消息 m，根据 PKG 的公钥 P_{pub}以及用户的私钥 d_{ID}进行签名。签名验证阶段可由任何人对签名进行验证，输入 PKG 的公钥 P_{pub}和签名者的 ID，若验证正确，则返回 1，若验证不正确，则返回 0。

文献[13]提出了一个可证明安全的数字签名方案。若群 G_1 是一个 GDH 群，则该方案产生的数字签名能有效防止自适应选择明文攻击。该方案的步骤如下：

(1) 设置阶段

给定安全参数 k，PKG 选择群 G_1 和 G_2，这两个群的阶都为素数 q，其中 G_1 为加法群，G_2 为乘法群，$q>2^k$。P 为群 G_1 的生成元。

PKG 选择 $s\in_R Z_q^*$ 作为主密钥，$P_{pub}=sP$ 为 PKG 的公钥。明文空间 $M=\{0,1\}^n$，密文空间 $C=G_1^*\times\{0,1\}^n$，选择函数 $H_1:\{0,1\}^*\times G_1\rightarrow Z_q$，$H_2:\{0,1\}^*\rightarrow G_1$，双线性映射 $\hat{e}:G_1\times G_1\rightarrow G_2$，系统的公钥参数为

$$\text{params}=(G_1,G_2,\hat{e},n,P,P_{pub},H_1,H_2)$$

(2) 用户密钥生成阶段

给定用户 $ID\in\{0,1\}^*$,PKG 计算 $Q_{ID}=H_2(ID)\in G_1$,$d_{ID}=sQ_{ID}\in G_1$,d_{ID}为用户 ID 的私钥。

(3) 消息签名阶段

消息的签名者生成签名。用户 ID 使用私钥 d_{ID}对消息 $m\in M$ 进行签名,执行如下的步骤:

1) 选择随机数 $r\in Z_q^*$。

2) 计算 $U=rQ_{ID}$,$h=H_1(m,U)$,$V=(r+h)d_{ID}$。对消息 m 的签名为 $\sigma=(U,V)$。

(4) 签名的验证阶段

验证者执行如下的步骤对消息签名进行验证:

1) 计算 $h=H_1(m,U)$。

2) 判断 $\hat{e}(P,V)=\hat{e}(P_{pub},U+hQ_{ID})$是否成立,若成立,则验证通过,$\sigma$ 为消息 m 的有效签名;否则验证失败,σ 为消息 m 的无效签名。

签名验证过程的正确性证明如下:

$$\begin{aligned}\hat{e}(P_{pub},U+hQ_{ID})&=\hat{e}(sP,rQ_{ID}+hQ_{ID})=\hat{e}(sP,(r+h)Q_{ID})\\&=\hat{e}(P,(r+h)d_{ID})=\hat{e}(P,V)\end{aligned}$$

□

三、基于身份的代理签名方案

1. 基于身份的代理签名方案

我们基于上述数字签名方案构造了一个代理数字签名方案。设 Alice 为原始签名者,身份标识为 ID_A,Cindy 为代理签名者,身份标识为 ID_C,Alice 授权 Cindy 代理签名。m_w 为委任状,用于保证 Alice 确实授予了 Cindy 代理签名权。

首先 Alice 对 m_w 按照第 2 节的签名算法进行签名。Alice 对 m_w 的签名计算如下:

1) 选择随机数 $r\in Z_q^*$。

2) 计算

$$U=rQ_{ID_A},h_w=H_1(m_w,U),V=(r+h_w)d_{ID_A}$$

于是对消息 m_w 的签名为 $\sigma=(U,V)$。Alice 将(m_w,σ)发送给 Cindy。

Cindy 接收到(m_w,σ)后,对签名的验证如下:

1) 计算 $h_w=H_1(m_w,U)$。

2) 判断 $\hat{e}(P,V)\stackrel{?}{=}\hat{e}(P_{pub},U+h_wQ_{ID_A})$是否成立,若成立,则验证通过,则接受 Alice 的授权签名,否则拒绝 Alice 的授权。

若 Cindy 想在上述授权签名的基础上,代理 Alice 对消息 m 进行签名,Cindy 利用上述的验证方法验证签名后,计算自己对 m 的签名如下:

1) 计算

$$h_w=H_1(m_w,U),h=H_1(m,U)$$

2) 计算

$$V_C = V + (h + h_w)d_{ID_C}$$

Cindy 对 m 的签名为 $\sigma_C=(U,V_C)$。Cindy 将(m,m_w,σ_C)发送给签名验证者 Bob。

Bob 收到签名 σ_C后，对 σ_C验证如下：

1) 计算

$$h_w = H_1(m_w,U)$$

2) 判断 $\hat{e}(P,V_C)=\hat{e}(P_{pub},U+h_w(Q_{ID_A}+Q_{ID_C})+hQ_{ID_C})$是否成立，若成立，则代理签名验证通过，否则验证失败。

2. 安全性分析

1) 签名验证的正确性：签名验证的合理性计算如下：

$$\begin{aligned}\hat{e}(P,V_C) &= \hat{e}(P,V+(h+h_w)d_{ID_C}) = \hat{e}(P,V)\hat{e}(P,hd_{IDC})\hat{e}(P,h_wd_{ID_C})\\ &=\hat{e}(P,V)\hat{e}(P,shQ_{ID_C})\hat{e}(P,sh_wQID_C)\\ &=\hat{e}(P,V)\hat{e}(sP,hQ_{ID_C})\hat{e}(sP,h_wQ_{ID_C})\\ &=\hat{e}(P,V)\hat{e}(P_{pub},hQ_{ID_c})\hat{e}(P_{pub},h_wQ_{ID_C})\\ &=\hat{e}(P_{pub},U+h_wQ_{ID_A})\hat{e}(P_{pub},hQ_{ID_C})\hat{e}(P_{pub},h_wQ_{ID_C})\\ &=\hat{e}(P_{pub},U+h_w(Q_{ID_A}+Q_{ID_C})+hQ_{ID_c})\end{aligned}$$

□

2) 可区别性：由于有效的代理签名中包含了 m_w 信息，同时在代理签名验证方程中需要使用代理签名者和原始签名者的公钥信息，因此代理签名能有效地与原始签名区别开来。

3) 可验证性：消息 m 的有效代理签名为(m,m_w,U,V_C)。一般来说，m_w 包含代理签名者的身份标识以及对代理签名权的限制信息。因此，从 U、V_C 的计算以及代理签名的验证可知，验证者可以验证代理签名的有效性，一旦验证通过，则相信此签名确实是经授权的合法代理签名。

4) 不可伪造性：第三方若想要伪造有效的代理签名必须得有原始签名者对 m_w 的签名，而对 m_w 的签名是由证明安全的签名机制构造的，该签名体制是一可证明安全的 ID－数字签名方案[3]，能抵抗自适应选择明文攻击。因此，第三方不能伪造这一信息。另一方面，代理签名是代理签名者使用可证明安全的签名机制构造的，签名密钥为 $V_C=V+(h+h_w)d_{ID_C}$，其中包含了 d_{ID_C}，因此原始签名者不能伪造代理签名。

5) 可辨认性：由于代理签名中包含了 m_w，因此，任何人能从 m_w 中辨认代理签名者的身份。

6) 不可抵赖性：与可辨认性的证明类似，由于有效的代理签名中包含了 m_w，验证阶段，代理签名者必须对 m_w 进行验证，而且不能对 m_w 进行修改。因此，一旦代理签名者代替原始签名者产生了有效的代理签名，代理签名者就不能抵赖此次签名行为。

7) 代理签名权的不可滥用性：由于使用了 m_w，因此，代理签名者不能对未授权的消息进行签名，防止了代理签名权的滥用。

四、指定验证者的代理签名方案

为更有效地防止代理签名者滥用授予的签名权，原始签名者通常希望指定一个签名验证者，使得代理签名者替自己行使签名权时只能生成由指定验证者验证的签名。为此，我们在第三节的基础上构造了一个指定验证者的代理签名方案。

1. 指定验证者的签名方案

假设对消息 m 签名，指定 B 才能验证该签名，则 A 对消息 m 的签名计算如下：

1）计算 $Q_B=H_2(ID_B)$。

2）选择随机数 $r\in_R Z_q^*$。

3）计算

$$U=rQ_B, h=H_1(m,U), Q_0=rP, V=hd_{ID_A}$$

对消息 m 的签名为：$\sigma=(U,Q_0,V)$。A 将(m,σ)发送给 B。

B 接收到(m,σ)后，验证式 $\hat{e}(P,V)\hat{e}(Q_0,d_{ID_B})\stackrel{?}{=}\hat{e}(P_{pub},hQ_A+U)$是否成立，若成立，则 σ 为有效的签名；否则，为无效的签名。

签名验证的正确性证明如下：

$$\hat{e}(P,V)\hat{e}(Q_0,d_{ID_B})=\hat{e}(P,hd_{ID_A})\hat{e}(rP,d_{ID_B})=\hat{e}(P,hsQ_A)\hat{e}(rP,sQ_B)$$

$$=\hat{e}(P_{pub},hQ_A)\hat{e}(P_{pub},rQ_B)=\hat{e}(P_{pub},hQ_A+rQ_B)=\hat{e}(P_{pub},hQ_A+U) \qquad \square$$

从签名的验证过程可以看出，只有 B 能验证签名，因为验证过程中用到了 B 的私钥 d_{ID_B}。

2. 指定验证者的代理签名方案

利用上述指定验证者签名方案，我们进一步设计指定验证者的代理签名方案。假定原始签名者为 A，指定验证者为 B，代理签名者为 C，该签名方案如下：

A 首先对委任状 m_w(其中包括代理签名者的身份标识，指定验证者的身份标识，授权信息，即授权 C 代理签名以及授权期限等)进行签名，其签名计算如下：

1）选择随机数 $r\in_R Z_q^*$。

2）计算

$$U_A=rQ_{ID_A}, h_w=H_1(m_w,U_A), V=h_wd_{ID_A}$$

A 对委任状 m_w 的签名为 $\sigma_A=(U_A,V)$，A 将(σ_A,m_w)发送给 C。

C 接收到(σ_A,m_w)，后，检查等式 $\hat{e}(P,V)\stackrel{?}{=}\hat{e}(P_{pub},h_wQ_{ID_A})$是否成立，若成立，则接受 A 的授权签名，否则，拒绝。

签名验证的正确性证明如下：

$$\hat{e}(P,V)=\hat{e}(P,h_wd_{ID_A})=\hat{e}(P,h_wsQ_{ID_A})=\hat{e}(sP,h_wQ_{ID_A})=\hat{e}(P_{pub},h_wQ_{ID_A}) \qquad \square$$

C 接受 A 的授权签名后，代理 A 对消息 m 进行签名，计算如下：

1）选择随机数 $r_C\in_R Z_q^*$。

2）计算

$$U_C = r_C Q_{ID_B}, h_C = H_1(m, U_C), V_C = V + h_C d_{ID_C}, Q_0 = r_C P$$

C 将签名 $\sigma_C = (U_A, U_C, Q_0, V_C)$以及 m_w 和 m 发送给 B。

B 接收到(σ_C, m_w, m)后，对该签名验证如下：

1）计算

$$h_C = H_1(m, U_C), h_w = H_1(m_w, U_A)$$

2）判断等式 $\hat{e}(P, V_C)\hat{e}(Q_0, d_{ID_B}) \stackrel{?}{=} \hat{e}(P_{pub}, h_w Q_{ID_A} + h_C Q_{ID_C} + U_C)$是否成立，若成立，则为有效的代理签名，否则，为无效的代理签名。

3. 安全性分析

1）代理签名验证的正确性。代理签名验证的合理性计算如下

$$\begin{aligned}\hat{e}(P, V_C)\hat{e}(Q_0, d_{ID_B}) &= \hat{e}(P, V + h_C d_{ID_C})\hat{e}(Q_D, d_{ID_B}) = \hat{e}(P, V)\hat{e}(P, h_C d_{ID_C})\hat{e}(r_C P, s Q_{ID_B}) \\ &= \hat{e}(P_{pub}, h_w Q_{ID_A})\hat{e}(P, h_C s Q_{ID_C})\hat{e}(r_C P, s Q_{ID_B}) \\ &= \hat{e}(P_{pub}, h_w Q_{ID_A})\hat{e}(P_{pub}, h_C Q_{ID_C})\hat{e}(P_{pub}, U_C) \\ &= \hat{e}(P_{pub}, h_w Q_{ID_A} + h_C Q_{ID_C} + U_C)\end{aligned}$$

□

2）可区分性：由代理签名的产生知道，代理人 C 产生的一个合法代理签名是一个四元组 $\sigma_C = (U_A, U_C, Q_0, V_C)$，而原始签名人的正常数字签名是一个三元组 $\sigma = (U, Q_0, V)$。若攻击者把代理签名的四元组变为正常签名的三元组或反过来，均不能通过验证。因此，代理人 C 的代理签名和正常签名是可区分的。

3）可验证性：由验证方程 $\hat{e}(P, V_C)\hat{e}(Q_0, d_{ID_B}) = \hat{e}(P_{pub}, h_w Q_{ID_A} + h_C Q_{ID_C} + U_C)$可知，验证者可以验证代理签名的有效性。一旦验证通过，则相信此签名确实是经授权的合法代理签名。

4）不可伪造性：由验证方程 $\hat{e}(P, V_C)\hat{e}(Q_0, d_{ID_B}) = \hat{e}(P_{pub}, h_w Q_{ID_A} + h_C Q_{ID_C} + U_C)$可知，

$$V_C = V + h_C d_{ID_C}$$

其中包含了代理签名者的私钥信息 d_{ID_C}。因此只有代理签名者可以产生代表原始签名者的合法代理签名；原始签名者和其他人都不能产生一个合法的代理签名。

5）可辨认性：由代理签名信息(σ_C, m_w, m)以及代理签名验证方程

$$\hat{e}(P, V_C)\hat{e}(Q_0, d_{ID_B}) = \hat{e}(P_{pub}, h_w Q_{ID_A} + h_C Q_{ID_C} + U_C)$$

可知，代理签名者的身份包含在委任状 m_w 中，任何人可从代理签名中辨认出代理签名者的身份。

6）不可抵赖性：由不可伪造性知，代理签名信息 $\sigma_C = (U_A, U_C, Q_0, V_C)$中包含了代理签名者的私钥信息 d_{ID_C}，一旦代理签名者代替原始签名者产生了一个合法的代理签名，代理签名者不能抵赖此次签名行为。

7）只有由原始签名者指定的验证者才能验证代理签名的有效性：由代理签名的验证方程 $\hat{e}(P, V_C)\hat{e}(Q_0, d_{ID_B}) = \hat{e}(P_{pub}, h_w Q_{ID_A} + h_C Q_{ID_C} + U_C)$可知，签名验证过程需要用到指定验证者的私钥信息 d_{ID_B}，因此只有由原始签名者指定的验证者才能验证代理签名的有效性。

8）原始签名者不能否认指定了签名验证者：原始签名者以委任状 m_w 的形式指定了签名的验证者。若原始签名者对此否认，则代理签名者在验证原始签名者的授权时，由委

任签名 $\sigma_A=(U_A,V)$及其验证方程 $\hat{e}(P,V)=\hat{e}(P_{pub},h_\omega Q_{ID_A})$可知，若验证通过，原始签名人不能否认其指定了签名验证者。

五、结 束 语

代理数字签名方案以及指定验证者的代理数字签名方案在电子商务中具有广泛的应用。然而，以往的方案都是基于传统的公钥加密体制。该文在可证明安全的基于身份的数字签名方案基础上，利用双线性映射构造了基于身份的代理数字签名方案以及指定验证者的代理数字签名方案。这些方案能满足代理签名和指定验证者的代理签名方案的安全性需求。

参 考 文 献

1 Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the Power to Sign Messages. IEICE Transactions Fundamentals, 1996, E79-A (9): 1338～1354

2 Hsu C L, Wu T S. Efficient Proxy Signature Schemes Using Self-Certified Public Keys. Applied Mathematics and Computation, 2004,152(3): 807～820

3 Dai J Z, Yang X H, Dong J X. Designated-receiver proxy signature scheme for electronic commerce. In: Proc. of IEEE International Conference on Systems. Man and Cybernetics, 2003,1:384～389

4 Shamir A. Identity Based Cryptosystems and Signature Schemes. In: Advances in Cryptology Crypto' 84, Lecture Notes in Computer Science 196. Springer-Verlag,1984, 47～53

5 Paterson K G, Price G. A Comparison between Traditional Public Key Infrastructures and Identity-based Cryptography. Information Security Technical Report, 2003,8(3):57～72

6 Kim S, Park S, Won D. Proxy Signatures, Revisited. In: ICICS'97, Lecture Notes in Computer Science1334. Springer-Verlag,1997, 223～232

7 Lee J Y, Cheon J H, Kim S. An Analysis of Proxy Signatures: Is a Secure Channel Necessary? In: CT-RSA'03, Lecture Notes in Computer Science 2612. Springer-Verlag, 2003, 68～79

8 Seo S H, Lee S H. New Nominative Proxy Signature Scheme for Mobile Communication. In: Proceedings of SPI (Security and Protection of Information). 2003, 149～154

9 Shum K, Wei V K. A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection. In: Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02). 2002, 55～56

10 Shao Z. Proxy Signature Schemes based on Factoring. Information Processing Letters 85, 2003, 137～143

11 Boneh D, Franklin M. Identity Based Encryption From the Weil Pairing. In: Advances in Cryptology-Crypto'01, Lecture Notes in Computer Science 2139. Springer-Verlag, 2001, 213～229

12 Chen L, Harrison K, Soldera D, Smart N. Applications of Multiple Trust Authorities in Pairing Based Cryptosystems. In: InfraSec'2002, Lecture Notes in Computer Science 2437. Springer-Verlag, 2002, 260～275

13 Cha J C, Cheon J H. An Identity-Based Signature from Gap Diffie-Hellman Groups. In: Proceedings of PKC'03, Lecture Notes in Computer Science 2567. Springer-Verlag, 2003, 18～30

ID-Based Proxy Signature and Designated-verifier Proxy Signature Scheme from Bilinear Maps

Shuanghe Peng[1,3] Zhen Han[1] Kejun Sheng[2]

(1 College of Computer and Information Technology, Beijing Jiaotong University, Beijing, PRC, 100044)

(2 Naval Engineering University, Wuhan, PRC, 430033)

(3 Computer Center, Beijing Institute of Mechanics, Beijing, PRC, 100085)

Abstract In this paper, we propose a new ID-based partial delegation signature scheme with warrant and designated-verifier proxy signature scheme based on the bilinear pairings. We also analyze their security and efficiency. The misuse of proxy signature is avoided in the proposed scheme.

Keywords Proxy signature Designated-verifier proxy signature Bilinear map

基于双线性映射的ID-代理签名与指定验证者代理签名

作者： 彭双和， 韩臻， 盛可军
作者单位： 彭双和(北京交通大学计算机与信息技术学院(中国北京);北京机械工业学院计算中心(中国北京))， 韩臻(北京交通大学计算机与信息技术学院(中国北京))， 盛可军(海军工程大学(中国武汉))