一种基于标准模型的盲代理重签名方案

邓宇乔　杜明辉　尤再来　王晓华
(华南理工大学电子与信息学院　广州　510640)

摘　要：已提出的代理重签名方案都不具备消息致盲性，因此在保护原始签名者隐私方面存在缺陷。该文把一般的代理重签名方案进行扩展，借鉴盲签名的设计思想，首先给出盲代理重签名方案的定义；根据该定义，运用双线性映射的技术以及 Waters 提出的标准模型签名的框架，提出了一种基于标准模型的盲代理重签名方案，并证明了该方案的安全性。该方案实现了签名从原始签名者到代理重签名者之间的透明转换，保护了原始签名者的隐私；同时，由于方案设计过程中采用了标准模型的框架，具有一定的实用性。

关键词：盲签名；代理重签名；自适应选择消息攻击；双线性映射；标准模型
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2010)05-1219-05
DOI: 10.3724/SP.J.1146.2009.00754

A Blind Proxy Re-signatures Scheme Based on Standard Model

Deng Yu-qiao　Du Ming-hui　You Zai-lai　Wang Xiao-hua
(*School of Electronic and Information Engineering*, *South China University of Technology*, *Guangzhou* 510640, *China*)

Abstract: The proposed proxy re-signature schemes had no message blinded properties as yet, so there is a problem that they can not protect the original signer's privacy. The general proxy re-signature scheme is extended using the idea of blind signature. The definition of blind proxy re-signature scheme been given firstly; then according to the definition, the blind proxy re-signatures scheme Based on Standard Model is proposed using of bilinear mapping technology and standard model framework proposed by Waters, finally, the security of the scheme is proven. The transparent signature conversion from original signer to proxy re-signer is achieved in this paper which can protect the original signer's privacy, at the same time, the scheme is practicality as it is designed using the framework of standard model.

Key words: Blind signature; Proxy re-signatures; Chosen adaptively message attack; Bilinear map; Standard model

1　引言

代理重签名方案最初是由 Blaze 等在文献[1]中提出，但该方案一直没被学者深入研究。　文献[2]指出，这是由于该方案效率比较低并且具有缺陷，文献[2]在其基础上重新给出了代理重签名方案的定义，并提出了 3 个具有不同特点的代理重签名方案，同时给出了其安全性定义。文献[3]提出了一种在标准模型下的代理重签名方案，文献[4]提出了一种基于标准模型的代理重签名方案，文献[5]指出文献[4]中的方案存在安全漏洞，并提出了一个改进的方案。文献[6]提出了一种可复用的单向代理重签名方案。

盲签名是由 Chaum[7]首先提出的一种带附加性质的数字签名，目前已提出各种基于不同困难性盲签名方案[8−10]。但是，以上的代理重签名都不具备消息致盲性。即，当重签名代理在转换签名时，可以同时得知其转换的消息，这不利于某些需要隐藏消息的场合。

本文提出了一个盲代理重签名方案。该签名方案将盲签名的特性与代理重签名的特性进行有效融合，使重签名代理在转换签名时，消息对其而言是透明的。同时，考虑到随机预言机模型的签名方案在实际应用中存在不安全因素[11,12]，因此，本文的方案将基于标准模型提出，并在提出了整个方案后，给出完整的安全性证明。

2　盲代理重签名定义的提出

2.1 盲代理重签名的应用背景

在文献[2]中提到以下代理重签名的一个典型应用：一个企业 A 里的一些部门可能需要具有单独对文件签名的权限，但是相对外部企业 B 而言，在验证公钥数据库里包含对企业 A 里的每个部门的验证公钥显然是一种相当耗资源的行为。而且，当企业 A 里的新部门又产生新的验证公钥或旧部门需要更改验证公钥时，在 B 的公钥数据库里作出相应修改是件很繁琐的事。

因此，文献[2]中提出可以把代理重签名算法运用到密钥管理过程中。假设企业 A 对文件签名的公钥为 pk_A，如果其某部门 E 也需要具有单独签署文件的权限，企业为其创建公钥 pk_E，使其能对文件

2009-05-18 收到，2009-11-24 改回
广东省自然科学基金(05006593)资助课题
通信作者：邓宇乔　dengyugiao80@yahoo.cn

进行签署。但在外部企业 B 的老版本验证软件中，并没有储存这个新的验证公钥 pk_E，为了使签名能够照常验证，可以设置一个重签名代理，并产生重签名代理密钥 $rk_{E\to A}$，这样企业 A 里部门 E 的签名可以转化为企业 A 的签名，即可以通过企业 B 的签名验证软件的验证了。

但是，以上的代理重签名应用没有考虑到签名时消息的隐私特性。即，如果企业 A 里的部门 E 需要签名的文件具有部门隐私性，其阅读权限仅限部门内部，而非对整个企业公开时，以上所提出的代理重签名机制并不具有保护消息隐私的功能。例如，企业 A 里的部门 E 需要签署一份与企业 B 内某部门 F 之间的私密合同，该合同的阅读权限仅对于企业 A 内的部门 E 的主管和企业 A 的几个主要负责人公开，此时用传统的代理重签名进行签名转换明显不合时宜，因为重签名代理显然可以知道其签署的文件内容，这就造成了文件的泄密。因此，本文针对存在的这个问题，参照盲签名的概念，在下文中提出一个盲代理重签名方案。

2.2 盲签名定义

为了更好地阐述本文提出的盲代理重签名的定义，以下首先给出盲签名的一般性定义：

定义 1(盲签名定义) 盲签名有两个参与方:签名者和用户，签名者以盲方式对用户选择的消息 m 进行签名。一个盲签名方案由以下算法组成:

设置 这是一个概率多项式时间密钥生成算法，其输入一个安全参数 1^k，输出系统参数，并运行密钥生成算法 Gen 产生一个公钥/私钥对 (pk,sk)。下面用 $(pk,sk)\leftarrow \mathrm{Gen}(1^k)$ 表示密钥生成算法。

盲签名算法 这是一个由签名者和用户执行的概率多项式时间交互式协议，其以系统参数和公钥 pk 为公共输入，用户秘密输入其待签名的消息 m，签名者秘密输入其私钥 sk。协议在多项式时间内停止，并输出签名者对消息 m 的签名 $\sigma(m)$ 或 fail。

签名验证算法 这是一个确定性算法，其以系统参数、公钥 pk、消息 m 和签名 $\sigma(m)$ 为输入，并输出 true 或 false。

2.3 盲代理重签名定义

定义 2(盲代理重签名定义) 本文提出的盲代理重签名有 3 个参与方：原签名者(S)，重签名代理(P)，委托者(D)；由 7 个多项式时间算法组成(系统参数产生，重签名密钥产生，签名，消息盲化，盲重代理签名，脱盲，签名验证)。这些算法的定义如下：

系统参数产生: 产生标准的系统参数。

重签名密钥产生: 输入 S 和 D 的密钥 (sk_A, sk_B)，P 输出重签名密钥 $rk_{A\to B}$。

签名: 输入消息 m，S 产生对 m 的签名 σ_A。

消息盲化: 输入 m 及 S 对 m 的签名 $\sigma_A=(\sigma_{A1},\sigma_{A2})$，$D$ 输出盲化的签名 $\sigma'_A=(\sigma'_{A1},\sigma'_{A2})$。

盲重代理签名: 输入重签名密钥 $rk_{A\to B}$ 以及盲化后的 S 签名 $\sigma'_A=(\sigma'_{A1},\sigma'_{A2})$，首先验证盲化的签名是否正确，如果正确，$P$ 输出盲代理重签名 $\sigma'_B=(\sigma'_{B1},\sigma'_{B2})$，否则停止。

脱盲: 输入盲代理重签名 $\sigma'_B=(\sigma'_{B1},\sigma'_{B2})$，$D$ 首先验证该代理重签名的正确性，如果正确，输出脱盲后的签名 $\sigma_B=(\sigma_{B1},\sigma_{B2})$。

签名验证: 需要说明的是，代理重签名和代理签名的一个非常重要的不同之处在于，代理重签名方案所生成的重签名与原始签名者生成的签名在形式和结构上是相同的，即，在进行签名验证时，原签名和代理重签名是通过同样的方程进行验证的；而代理签名则不然，代理签名方案在生成代理签名后，代理签名的验证方程与原签名的验证方程是存在差异的。因此，本文提出的盲代理重签名的验证过程对于所有签名(无论是原签名者 S 的签名还是经过重签名代理转换过的 D 的签名)将采用统一的方程进行验证。

该验证输入消息 m，签名者 S (或 D)的公钥 pk_A (或 pk_B)，上面提到，由于本验证过程与签名者身份无关，因此这里将需要验证的签名者公钥统一记为公钥 pk，S 的签名 $\sigma_A(m)$ (或 D 的签名 $\sigma_B(m)$)，同样，由于本验证过程与签名者身份无关，因此这里将需要验证的签名者的签名统一记为 σ。输出验证判断 $b\in\{0,1\}$，当 $b=0$，拒绝签名，否则，接受签名。

3 基于标准模型的盲代理重签名方案

3.1 基于标准模型的盲代理重签名方案

本文提出一个基于标准模型的盲代理重签名方案。该方案基于 Waters 在文献[13]中提出的签名方案，此方案需要一个双线性映射，并假设所有被签名的消息可以被表示成 n_m 长的比特字符串，长度 n_m 与双线性映射所在的双线性群的阶是无关的。为了达到这个目的，可以使用一个抗碰撞的密码哈希函数 $H:\{0,1\}^*\to\{0,1\}^{n_m}$。

系统参数产生: 输入安全参数 1^k，系统选择一个双线性映射：$e:G_1\times G_1\to G_2$，假设 G_1 和 G_2 的阶均为素数 q，g 是 G_1 的生成元，另外，还要从 Z_q^* 中任意选取一个数 a 和从 G_1 中任意选取 n_m+2 个随机数 $(g_2,u',u_1,\cdots,u_{n_m})$。最后输出公私钥对 $pk=g_1=g^a$ 和 $sk=a$，公开参数 $(G_1,G_2,e,pk,g_2,u',u_1,$

$\cdots, u_{n_m})$。

重签名密钥产生：输入签名者 S 和 D 的密钥 a,b，P 输出重签名密钥 $rk_{A\to B}=b/a$（$rk_{A\to B}$ 可以以某种秘密方式产生而使 P 不知道 sk_A, sk_B 的值[2]）。

签名：输入要签名的消息 m 以及 S 的私钥 a，S 输出对消息 m 的签名 $\sigma_A=(\sigma_{A1},\sigma_{A2})=(g_2^a w^r, g^r)$，这里 $r\in Z_q^*$ 是 S 随机选取的，$w=u'\prod_{i\in U}u_i$。$U\subset\{1,\cdots,n_m\}$ 是 $m[i]=1$ 的索引 i 的集合，$m[i]$ 是消息 m 的第 i 比特的值。

消息盲化：输入 S 的签名 $\sigma_A=(\sigma_{A1},\sigma_{A2})$ 及该签名消息对应的值 w，D 选取 $k\in_R Z_q^*$，计算 $w'=w\times g^k$，$\sigma'_{A1}=\sigma_{A1}\times\sigma_{A2}^k$，$\sigma'_{A2}=\sigma_{A2}$，并把签名 $\sigma'_A=(\sigma'_{A1},\sigma'_{A2})$ 发送给 P。

盲代理重签名：输入重签名密钥 $rk_{A\to B}$，w'，以及盲化后的 S 签名 $\sigma'_A=(\sigma'_{A1},\sigma'_{A2})$，$P$ 首先通过下式验证该签名的正确性：$e(\sigma'_{A1},g)=e(g_1,g_2)e(\sigma'_{A2},w)$。如果该签名正确，$P$ 通过下式得到盲代理重签名 $\sigma'_B=\sigma_A'^{rk_{A\to B}}=(\sigma_{A1}'^{rk_{A\to B}},\sigma_{A2}'^{rk_{A\to B}})=(g_2^b w'^{rb/a}, g^{rb/a})=(\sigma'_{B1},\sigma'_{B2})$。否则，$P$ 中止该过程。

脱盲：输入盲代理重签名 $\sigma'_B=(\sigma'_{B1},\sigma'_{B2})$，$D$ 首先通过下式验证该盲代理重签名的正确性：$e(\sigma'_{B1},g)=e(g'_1,g_2)e(\sigma'_{B2},w)$（其中 $g'_1=g^b$ 为 D 公钥）。如果正确，D 将其脱盲得到 $\sigma_B=(\sigma'_{B1}\cdot\sigma'^{-k}_{B2},\sigma'_{B2})=(g_2^b w^{rb/a}, g^{rb/a})=(\sigma_{B1},\sigma_{B2})$。

签名验证：输入一个 n_m 比特长的消息 m，公钥 pk，以及对该消息的签名 $\sigma=(\sigma_1,\sigma_2)$，验证是否有：

$$e(\sigma_1,g)=e(g_1,g_2)e(\sigma_2,w) \tag{1}$$

如果式(1)成立，则输出 1，否则，输出 0。

3.2 方案安全性分析

3.2.1 消息盲性　本方案的消息具有盲性。由于本方案中 D 对与消息 m 有关的值 w 经过以下处理：$w'=w\times g^k$，其中 k 为 D 自己秘密选取的，P 要通过 w' 求得 w 并由此辨认出原来的消息明显是不可能的。所以，本文提的方案具有消息盲性。

3.2.2 安全性证明　本文所提方案的安全性是建立在 Computational Diffie-Hellman(CDH)问题成立的基础上的，以下给出计算CDH 问题的定义：

定义 3（计算 CDH 问题）　对于 $g\in G_1$,给定元组 (g,g^a,g^b)，要计算 g^{ab} 是困难的。

本文的安全性由以下的定理得到，该证明过程参考了文献[14]的证明方法。

定理　在标准模型中，本方案在 CDH 假设下其签名是不可伪造的。该假设是对于任何在 G_1 的元素 g，在 Z_q^* 中的元素 x 和 y，给定了 (g,g^x,g^y)，计算 g^{xy} 是困难的。

证明　如果存在一个攻击者 A 在要求系统提供不超过 q_K 个用户的公钥，最多查询了 q_S 次签名询问，q_R 次重签名询问后，可以以一个不可以忽略的概率 ε 攻破本方案，那么就有另外一个攻击者 B 可以以概率 $\dfrac{\varepsilon}{4q_K(q_S+q_R)(n_m+1)}$ 解决在群 G_1 的 CDH 问题。

输入 (g,g^a,g^b)，CDH 攻击者 B 根据下面的过程来模拟一个盲代理重签名过程。

为了准备这个模拟器，攻击者 B 首先设置 $l_m=2(q_S+q_R)$，并选择一个随机数 k_m，满足 $0\le k_m\le n_m$ 和 $l_m(n_m+1)<q$。接着，攻击者 B 选择 n_m+1 个任意的不大于 l_m 的正整数 $x', x_i(i=1,\cdots,n_m)$。最后，攻击者 B 从群 Z_q^* 中选择 n_m+1 个任意的 $y', y_i(i=1,\cdots,n_m)$。

为了描述方便，记：$F(m)=x'+\sum_{i\in U}x_i-l_m k_m$ 和 $J(m)=y'+\sum_{i\in U}y_i$。

攻击者 B 设置公开参数：$g_2=g^b$，$u'=g_2^{x'-l_m k_m}g^{y'}$，$u_i=g_2^{x_i}g^{y_i}(1\le i\le n_m)$。

由上面的表示可以看出，对于任意一个消息 m，存在下面的等式：$w=u'\prod_{i\in U}u_i=g_2^{F(m)}g^{J(m)}$。在 A 向 B 请求用户公钥时，B 猜测 A 需要仿造哪个公钥用户的签名。假设 B 猜测 A 想仿造公钥为 pk_t 的用户签名，B 设 $pk_t=g^a$。对于其他公钥询问，B 选取 $x_i\in Z_q$，并返回 $pk_i=g^{x_i}$。

签名询问：输入 (pk_i,m) 如果 A 询问签名的公钥 $pk_i\ne pk_t$，B 返回 $\sigma=(g_2^{x_i}w^r, g^r)$，这里 $w=u'\prod_{i\in U}u_i$；否则，B 做如下操作：

(1) 如果 $F(m)\ne 0 \bmod q$，B 随机选择一个数 $r\in Z_q$，并计算如下的签名

$$\sigma=\left(g_1^{-J(m)/F(m)}\left(u'\prod_{i\in U}u_i\right)^r, g_1^{-1/F(m)}g^r\right) \tag{2}$$

令 $\tilde{r}=r-a/F(m)$ 可得到

$$\begin{aligned}
&g_1^{-J(m)/F(m)}\left(u'\textstyle\prod_{i\in U}u_i\right)^r\\
&=g_1^{-J(m)/F(m)}(g^{J(m)}g_2^{F(m)})^r\\
&=g_2^a(g_2^{F(m)}g^{J(m)})^{-a/F(m)}(g_2^{F(m)}g^{J(m)})^r\\
&=g_2^a(g_2^{F(m)}g^{J(m)})^{r-a/F(m)}\\
&=g^{ab}\left(u'\textstyle\prod_{i\in U}u_i\right)^{\tilde{r}}
\end{aligned}$$

和

$$g_1^{-1/F(m)}g^r=g^{r-a/F(m)}=g^{\tilde{r}}$$

上面的推导式说明了所产生的 σ 和实际方案运行产生的签名是一致的。

(2)如果 $F(m)\equiv 0(\bmod q)$，攻击者 B 就不能计算出签名 σ，模拟器宣告失败。

重签名密钥询问：假设 A 要求返回公钥为 pk_i, pk_j 的用户的重签名密钥 $rk_{i\to j}$，如果 $i\neq t, j\neq t$，则 B 返回 x_j / x_i；否则中止过程。

盲代理重签名询问：假设 A 要求返回一个以下的盲代理重签名：$\sigma_{i\to j}$(即把公钥为 pk_i 的用户的签名转化为公钥为 pk_j 的用户的签名)。在这一步，要说明的是，A 询问的盲代理重签名中不能出现 $j=t$ 的情况。这是因为 A 可以通过这步直接通过重签名代理得到 B 所不知道的消息的签名。因此，该步骤的询问及回答过程如下：

首先通过式(1)检查输入的盲化签名 $\sigma_i^{'}(m)$ 是否正确，如果否，中止该过程；如果正确，检查是否 $pk_j=pk_t$，如果是，中止询问过程；否则返回 $\sigma=(g_2^{x_j}w^{rr}, g^r)$。

以上过程中，算法 B 模拟了整个签名过程，由假设，算法 A 在某时刻能够对某个消息 $m*$ 返回一个伪造的签名 $\sigma^*=(\sigma_1{}^*,\sigma_2{}^*)$，且该签名的验证公钥为 pk_t。如果 $F(m^*)\neq 0(\bmod q)$，那么 B 退出，模拟失败。否则，该伪造必然满足：

$$\begin{aligned}\sigma^* &= \left(g^{ab}\left(u'\prod\nolimits_{i\in U}u_i\right)^{r^*}, g^{r^*}\right)\\ &= (g^{ab}(g_2^{F(m^*)}g^{J(m^*)})^{r^*}, g^{r^*})\\ &= (g^{ab+J(m^*)r^*}, g^{r^*}) = (\sigma_1{}^*,\sigma_2{}^*)\end{aligned}$$

由此，攻击者 B 能够得到 $(\sigma_1{}^*)\cdot(\sigma_2{}^*)^{-J(m^*)}=g^{ab}$

以下将计算攻击者 B 能够完成整个模拟过程的概率。要完成模拟，需要所有的输入消息 m 必须满足 $F(m)\equiv 0(\bmod q)$ 和 $F(m^*)\neq 0(\bmod q)$，并且攻击者 A 的确是伪造公钥为 pk_t 的用户的签名。

首先，定义事件 E_K 为 B 成功猜出 A 试图伪造的用户的公钥。容易得到：$\Pr[E_K]=1/q_K$。下面计算满足条件 $F(m)\equiv 0(\bmod q)$ 和 $F(m^*)\neq 0(\bmod q)$ 的概率。

设 $m_1, m_2, \cdots, m_{q_Q}$ 是查询中出现的消息，但是不包括消息 $m*$。显然，有 $q_Q\le q_S+q_R$。定义事件 E_i，$E_i^{'}$ 和 $E*$ 如下：

$$E_i: F(m_i)\neq 0\bmod q,\ E_i^{'}: F(m_i)\neq 0\bmod l_m,$$
$$E^*: F(m^*)\equiv 0\bmod q$$

首先可以看出，事件 $\wedge_{i=1}^{q_Q}E_i\wedge E*$ 和事件 E_K 是独立的，因此，攻击者 B 不退出的概率 $\Pr[\neg\text{abort}]\ge\Pr[\wedge_{i=1}^{q_Q}E_i\wedge E^*]\Pr[E_K]$。

很容易看出事件 $(\wedge_{i=1}^{q_Q}E_i)$，$E*$ 是不相关的。因为 $l_m(n_m+1)<q$、$x', x_i(i=1,\cdots,n_m)$ 都是比 l_m 小的正整数，所以有 $0\le l_m, k_m<q$ 和 $0\le x'+\sum_{i\in U}x_i<q$。另一方面，很容易从 $F(m)\neq 0\bmod q$ 得出 $F(m)\equiv 0\bmod l_m$，从 $F(m)\neq 0\bmod l_m$ 得出 $F(m)\neq 0\bmod q$。因此，可以推出 $\Pr[E_i]\ge\Pr[E_i^{'}]$，及

$$\begin{aligned}\Pr[E^*] &= \Pr[F(m^*)\equiv 0\bmod q\wedge F(m^*)\equiv 0\bmod l_m]\\ &= \Pr[F(m^*)\equiv 0\bmod l_m]\Pr[F(m^*)\\ &\equiv 0\bmod q\mid F(m^*)\equiv 0\bmod l_m] = \frac{1}{l_m}\frac{1}{n_m+1}\end{aligned}$$

和

$$\begin{aligned}\Pr[\wedge_{i=1}^{q_Q}E_i] &\ge \Pr[\wedge_{i=1}^{q_Q}E_i^{'}] = 1-\Pr[\vee_{i=1}^{q_Q}\neg E_i^{'}]\\ &\ge 1-\sum\nolimits_{i=1}^{q_Q}\Pr[\neg E_i^{'}] = 1-\frac{q_Q}{l_m}\\ &\ge 1-\frac{q_S+q_R}{l_m}(l_m=2(q_S+q_R))\end{aligned}$$

因此，可以得到

$$\begin{aligned}\Pr[\neg\text{abort}] &\ge \Pr[\wedge_{i=1}^{q_Q}E_i]\Pr[E^*]\Pr[E_K]\\ &\ge \frac{1}{l_m(n_m+1)}\cdot\left(1-\frac{q_S+q_R}{l_m}\right)\frac{1}{q_K}\\ &\ge \frac{1}{2(q_S+q_R)(n_m+1)}\cdot\frac{1}{2}\cdot\frac{1}{q_K}\\ &= \frac{1}{4q_K(q_S+q_R)(n_m+1)}\end{aligned}$$

由于 $\Pr[\neg\text{abort}]$ 的值为不可忽略的，因此，B 能成功解决计算 CDH 问题。 证毕

4 结束语

本文利用双线性映射的技术提出了一个盲代理重签名方案，本方案参照盲签名的思想，把消息盲性加入到代理重签名方案中，使重签名代理在对消息转换的过程中无法获知消息的内容。同时，证明了该方案能抵抗伪造签名的攻击。本方案利用标准模型的原理提出，不涉及到随机预言机模型，因而，具有一定的实用性。

参 考 文 献

[1] Blaze M, Bleumer G, and Strauss M. Divertible protocols and atomic proxy cryptography. Proceedings of Advances in Cryptology: EUROCRYPT'98. Helsinki, Finland, 1998, 1403: 127–144.

[2] Ateniese G and Hohenberger S. Proxy re-signatures: New definitions, algorithms and applications. Proceedings of the 12th ACM conference on Computer and communications security , Alexandria, USA, 2005: 310–319.

[3] Sherman C and Raphael P. Proxy re-signatures in the standard model. 11th International Conference on Information Security, Taibei, China , 2008: 260–276.

[4] Jun S, Zhenfu C, Licheng W, and Xiaohui L. Proxy re-Signature schemes without random oracles. Progress in

Cryptology-INDOCRYPT 2007, Chennai, India, 2007, 4859: 197–209.

[5] Kitae K, Ikkwon Y, and Seongan L. Remark on shao et al's bidirectional proxy re-signature scheme in indocrypt'07. *International Journal of Network Security*, 2009, 9(1): 8–11.

[6] Benoit L and Damien V. Multi-use unidirectional proxy re-signatures. http://eprint.iacr.org/2007/371.pdf, 2008,2.

[7] Chaum D. Blind signature for untraceable payments, Advances in Cryptology-Crypto'82, Burg Feuerstein, Germany, 1982: 199–203.

[8] Abe M and Fujisaki E. How to date blind signatures. Advances in Cryptology Asiacrypto' 96, Kyongju, Korea, 1996, 163: 244–251.

[9] Abe M and Okamoto T. Provably secure partially blind signautres. Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology, California, USA, 2000: 271–286.

[10] Maitland G and Boyd C. A provably secure restrictive partially blind signature scheme. Public Key Cryptography PKC 2002, Paris, France, 2002: 99–114.

[11] Canetti R, Goldreich O, and Halevi S. The random oracle methodology, revisited. Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, 1998: 209–218.

[12] Bellare M, Boldyreva A, and Palacio A. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. EUROCRYPT 2004, Interlaken, Switzerland, 2004: 171–188.

[13] Waters B. Efficient Identity-based Encryption Without Random Oracles. EUROCRYPT 2005, Aarhus, Denmark, 2005: 114–127.

[14] Paterson K G and Schuldt J. Efficient identity-based signatures secure in the standard model. ACISP 2006, Melbourne, Australia, 2006: 207–222.

邓宇乔：男，1980年生，博士生，研究方向为数字签名、数字版权管理系统.

杜明辉：男，1964年生，教授，博士生导师，研究方向为图像处理、医学图像处理、模式识别.

尤再来：男，1984年生，硕士生，研究方向为信息安全、多重数字签名.

王晓华：男，1976年生，硕士生，研究方向为Ad hoc网络及网络安全、数字签名.