基于双线性对的新型门限签名方案

吕 鑫 王志坚 许 峰
(河海大学计算机与信息学院 南京 210098)

摘 要 针对当前电子商务对数字签名方案提出的新要求,在改进后的短签名方案的基础上,提出了一种基于双线性对的新型门限签名方案,使得单个签名成员可高效地完成签名。分析表明,方案具有不可冒充性和可审计性,同时可以动态地增删成员,较之已有的门限签名方案其具有密钥分发简单、签名过程执行高效等优势。

关键词 门限签名,双线性对,概率签名,秘密共享
中图法分类号 TP309 **文献标识码** A

New Threshold Signature Scheme Based on Bilinear Pairings

LU Xin WANG Zhi-jian XU Feng
(College of Computer and Information Science, Hohai University, Nanjing 210098, China)

Abstract To meet the new requirements droven by nowadays E-commerce for the signature schemes, a new threshold signature scheme was proposed from bilinear pairings based on improved short signature scheme, in which a single signing member can accomplish signature efficiently. The analysis shows that the scheme serves properties of non-masquerading and auditing, the members can be added and revoked dynamically. Compared with the existing threshold signature scheme, our scheme is more convenient in secret key distribution and more efficient in signing process.

Keywords Threshold signature, Bilinear pairings, Probabilistic signature, Secret sharing

数字签名是实现身份认证、数据完整性和反抵赖的基础,在电子商务等方面有着重要应用。而门限签名是数字签名的重要研究内容,它是由 Desmedt[1] 首次提出的。在门限签名中,密钥管理者将签名密钥分发给多人管理,并且要求必须有足够多的成员参与才能产生正确的签名,从而实现了签名权力的分配,避免了职权滥用。近年来,国内外专家学者不断提出各种门限签名协议[2-6],其中 Shoup 于 2000 年提出的门限签名方案[3]是目前认为最有效的 RSA 门限签名方案之一。随着门限签名技术的发展,人们对它的实用性提出了越来越高的要求,如在保证安全性的前提下,数字签名尽可能占用少的存储空间,密钥尽可能地短;能够有效地防止管理员和成员的欺骗行为;能够方便、有效地增删签名成员。

针对上述要求,人们进行了不懈的研究。2001 年 Boneh 等人提出了基于双线性对的短签名方案[7],方案具有签字短、安全、高效等特点,所以一经提出就引起了广泛关注。文献[8]在 Hess 签名方案[9]的基础上,提出了一个可验证的门限签名方案,方案虽然通过门限技术提高了签名密钥的安全性,但其签名过程复杂、效率较低。2004 年钱海峰、曹珍富等在文献[10]中对短签名方案进行了改进,提出了一个概率签名方案,此方案在不降低安全性的情况下,增加了概率签名的特性。2006 年,Zhang 等人利用双线性对提出了一种新型签名方案[11],该方案在标准模型下具有不可伪造性。此外,人们还提出了一些基于双线性对的具有特殊性质的签名方案。文献[12]提出了一种前向安全的门限签名方案,并在随机预言机模型中证明了方案的鲁棒性和前向安全性;文献[13]结合 Schnorr 签名方案[14]提出了一种基于身份的轻量签名方案,该方案具有较高的效率。

现在让我们考虑数字签名在电子商务中的一种应用场景。假设买卖双方已签订买卖合同,汇款方通过电子银行汇款,任何一位银行当值人员都应能及时地签发出有效、合法的银行电子支票,而无须和其它工作人员合作签名,同时银行可以从工作记录中了解受理这笔业务的工作人员的编号。这就要求签名方案在赋予成员独立签名权利的同时又能审计成员的签名行为。

本文针对门限签名方案的实用性要求以及上述应用场景的应用需求,在文献[10]中的概率签名方案的基础上,提出了一种基于双线性对的新型门限签名方案。在该方案中,密钥管理中心采用了特殊的密钥分配方式向成员和签名中心分发子密钥,在保证可审计性等安全属性的前提下,实现了单个成员即可独立完成签名(成员对外不暴露身份),并使得系统可以动态地增删成员;同时方案的签名过程简单,加之以双线性对为构造工具,使得签名长度和密钥长度相比于用其它方法构造的签名要短。

到稿日期:2010-05-17 返修日期:2010-08-10 本文受国家自然科学基金(60903018),河海大学中央高校基本科研业务费项目(2009B20514,2010B16314)资助。

吕 鑫(1983—),男,博士生,主要研究方向为可信计算、信息安全等,E-mail:lvxin.gs@163.com;王志坚(1958—),男,博士,教授,博士生导师,主要研究方向为并行分布计算、软件自动化等;许 峰(1975—),男,博士,副教授,主要研究方向为可信计算、信息安全等。

1 预备知识

1.1 双线性映射和 GDH 群

设 G_1 和 G_2 分别是阶数为素数 q 的加法循环群和乘法循环群，P 为 G_1 的一个生成元。假设 G_1 和 G_2 这两个群中的离散对数问题都是困难问题。双线性映射 $e:G_1\times G_1\to G_2$ 满足如下特性：

1)双线性性：$\forall P,Q\in G_1$，$a,b\in Z$，有 $e(aP,bQ)=e(P,Q)^{ab}$；

2)非退化性：若 $e(P,Q)=1$，$\forall Q\in G_1$，则 P 是 G_1 的生成元；

3)可计算性：对所有的 $P,Q\in G_1$，存在有效算法可以计算 $e(P,Q)$。

群 G_1 可取有限域上超奇异椭圆曲线或超椭圆曲线，双线性对可将该曲线上的 Weil 对或 Tate 对加以改进后得以实现。

设群 G_1 是具有以上性质的加法群，我们可以在群 G_1 上定义以下密码学问题：

离散对数(DL)问题：给定 $P,Q\in G_1$，计算整数 n，满足 $Q=nP$，若这样的 n 存在。

计算 Diffie-Hellman(CDH)问题：对 $a,b\in Z_q^*$，给定三元组 $(P,aP,bP)\in G_1^3$，计算 abP。

判定 Diffie-Hellman(DDH)问题：对 $a,b,c\in Z_q^*$，给定四元组 $(P,aP,bP,cP)\in G_1^4$，判断 $c\equiv ab \bmod q$ 是否成立。

Gap Diffie-Hellman(GDH)问题：一类 CDHP 困难而 DDHP 容易的问题。

Gap Diffie-Hellman(GDH)群是 CDH 问题困难而 DDH 问题容易的群。

1.2 新型概率签名方案[10]

该方案是在 GDH 短签名方案[7]的基础上做出的改进，增加了概率签名的特性，使其对同一消息 M 的重复签名可以产生不同的签名，避免了攻击者通过收集若干签名对 (M_i,σ_i) 而发起的攻击。

1.2.1 概率签名方案

系统初始化：设群 G_1 和 G_2 的阶数为素数 q。令 P 为 GDH 群 G_1 的生成元，$e:G_1\times G_1\to G_2$ 为一个安全的双线性映射。选择两个 Hash 函数 $H_1:\{0,1\}^*\times G_1\to Z_q^*$；$H_2:\{0,1\}^*\to G_1\backslash 1$。

密钥生成：从 Z_q^* 中随机选取 x，计算 $Y\leftarrow xP$，返回 $(pk=(Y,P,G_1,H_1,H_2),sk=x)$，这里 pk 和 sk 分别为公钥和私钥。

签名过程：给定消息 $M\in\{0,1\}^*$，随机选取 $r\in_R Z_q^*$，计算 $U=rP$。令 $h=H_1(M,U)$，$Q=H_2(M)$，计算 $V=(r+hx)Q$，消息 M 的签名为 $\sigma=(U,V)$。

验证过程：验证消息 M 的签名 $\sigma=(U,V)$，我们检查以下等式是否成立：$e(P,V)=e(U+hY,Q)$，成立则返回 1，否则返回 0。

1.2.2 方案分析

正确性：签名验证过程的正确性可由如下方程给出：

$$e(P,V)=e(P,(r+hx)Q)=e((r+hx)P,Q)=e(U+hY,Q)$$

故签名的验证过程是正确的。

安全性：该签名方案的安全性至少不低于 GDH 短签名方案。

证明过程见文献[7]。

下面我们将提出基于此方案的新型门限签名方案。

2 基于双线性对的新型门限签名方案

签名方案是基于可信中心的，它包含 3 类实体：密钥管理中心、签名中心、n 个团体成员。密钥管理中心生成团体公私钥、签名中心密钥、成员公私钥。它首先生成一组密钥 $(S_0,S_1,\cdots,S_n)$，然后将 $S_i(i=1,2,\cdots,n)$ 进一步分解为 $(S_{i0},S_{i1})(i=1,2,\cdots,n)$。最后，将 S_0 和 $S_{i0}(i=1,2,\cdots,n)$ 分发给签名中心，$S_{i1}(i=1,2,\cdots,n)$ 发送给各个成员作为其签名密钥。密钥分发如图 1 所示。

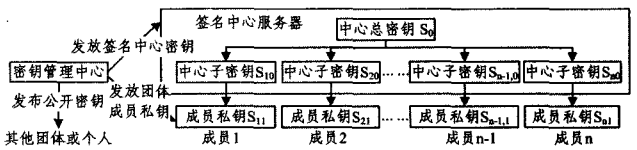

图 1 密钥分发示意图

签名思想是基于 1.2.1 节的概率签名方案。不同的是，我们的是门限式签名方案，签名过程需要签名中心与某一位成员共同参与完成。签名中心是独立于密钥管理中心的，可以设置在公共的服务器上。

2.1 密钥生成与分发

设有 n 个团体成员，系统公开参数同 1.2.1 节的概率签名方案 $\{G_1,G_2,q,P,e,H_1,H_2\}$。密钥管理中心选取 $S\in Z_q^*$ 作为团体密钥，计算 $Y_S\leftarrow SP$ 为团体公钥，并按如下步骤分发密钥：

1)任选 $a_0\in Z_q^*$，构造一次多项式 $f(x)=S+a_0x$；

2)任选 $x_0\in Z^+$，计算签名中心总密钥 $S_0=f(x_0)$；

3)任选 n 个 $x_i\in Z^+(i=1,2,\cdots,n)$，计算 $S_i=a_{i0}=f(x_i)$；任选 n 个 $a_{i1}\in Z_q^*(i=1,2,\cdots,n)$，构造 n 个一次多项式 $f_i(x)=a_{i0}+a_{i1}x(i=1,2,\cdots,n)$；

4)任选 n 个 $x_{i1}\in Z^+(i=1,2,\cdots,n)$，计算 n 个团体成员的私钥 $S_{i1}=f_i(x_{i1})$；

5)任选 n 个 $x_{i0}\in Z^+(i=1,2,\cdots,n)$，计算 n 个签名中心子密钥(与成员私钥一一对应)$S_{i0}=f_i(x_{i0})$；

6)向每个成员公开密钥生成参数 $x_0,x_i,x_{i0},x_{i1}\mid i=1,\cdots,n$，将中心总密钥 S_0 和子密钥 $S_{i0}(i=1,2,\cdots,n)$ 保存在签名中心，将成员私钥 $S_{i1}(i=1,2,\cdots,n)$ 安全地发送给相应的成员。

2.2 签名生成

当某个成员 i 要对消息 M 签名，他首先将 M 提交到签名中心，签名中心记录下成员的身份，与其联合执行如下步骤：

2.2.1 联合生成随机数

签名中心和成员 i 执行 Joint-Shamir-RSS 方案[15]联合共享一个随机数 r：

1)签名中心选取两个随机数 $r_1,r_2\in_U Z_q^*$，构造两个二次多项式 $R_1(x)=r_1+b_1x+a_1x^2$，$R_2(x)=r_2+b_2x+a_2x^2$。成员 i 选取一个随机数 $r_3\in_U Z_q^*$，构造一个二次多项式 $R_3(x)=r_3+b_3x+a_3x^2$。各多项式系数均随机选取于 Z_q^*。

2)签名中心计算 $R_1(x),R_2(x),x\in\{x_0,x_{i0},x_{i1}\}$，将 R_1

(x_{i1})，$R_2(x_{i1})$发送给成员 i。同时成员 i 计算 $R_3(x)$，$x\in\{x_0,x_{i0},x_{i1}\}$，将 $R_3(x)$，$x\in\{x_0,x_{i0}\}$发送给签名中心。

3)令 $R(x)=\sum_{i=1}^{3}R_i(x)$，签名中心计算 $R(x_0)=(\sum_{i=1}^{3}R_i(x_0))$，$R(x_{i0})=(\sum_{i=1}^{3}R_i(x_{i0}))$。同时成员 i 计算 $R(x_{i1})=(\sum_{i=1}^{3}R_i(x_{i1}))$，并广播 $R(x_{i1})P$。

4)令 $r=\sum_{i=1}^{3}r_i$，签名中心计算并公开

$$U=rP=R(x_0)\frac{-x_{i0}}{x_0-x_{i0}}\frac{-x_{i1}}{x_0-x_{i1}}P+R(x_{i0})\frac{-x_0}{x_{i0}-x_0}\frac{-x_{i1}}{x_{i0}-x_{i1}}P+R(x_{i1})\frac{-x_0}{x_{i1}-x_0}\frac{-x_{i0}}{x_{i1}-x_{i0}}P$$

2.2.2 子签名的生成

1)签名中心首先计算

$$V_0=(R(x_0)\frac{-x_{i0}}{x_0-x_{i0}}\frac{-x_{i1}}{x_0-x_{i1}}+hS_0\frac{-x_i}{x_0-x_i})Q$$

式中，$h=H_1(M,U)$，$Q=H_2(M)$。

2)签名中心调用与成员 i 私钥 S_{i1} 对应的中心子密钥 S_{i0}，计算

$$V_{i0}=\left(R(x_{i0})\frac{-x_0}{x_{i0}-x_0}\frac{-x_{i1}}{x_{i0}-x_{i1}}+hS_{i0}\frac{-x_{i1}}{x_{i0}-x_{i1}}\frac{-x_0}{x_i-x_0}\right)Q$$

3)签名中心将 V_0，V_{i0}发送给成员 i。

4)成员 i 计算

$$V_{i1}=\left((R(x_{i1})\frac{-x_0}{x_{i1}-x_0}\frac{-x_{i0}}{x_{i1}-x_{i0}}+hS_{i1}\frac{-x_{i0}}{x_{i1}-x_{i0}}\frac{-x_0}{x_i-x_0}\right)Q$$

2.2.3 签名的合成与验证

成员 i 计算 $V=V_0+V_{i0}+V_{i1}$，并输出最终签名 $\sigma=(U,V)$。签名的验证过程与 1.2.1 节中的签名过程一致，即检查等式 $e(P,V)=e(U+hY_S,Q)$是否成立。成立则返回 1，否则返回 0。

签名验证过程的正确性可由如下方程给出：

$$\begin{aligned}V&=V_0+V_{i0}+V_{i1}\\&=[(R(x_0)\frac{-x_{i0}}{x_0-x_{i0}}\frac{-x_{i1}}{x_0-x_{i1}}+R(x_{i0})\frac{-x_0}{x_{i0}-x_0}\frac{-x_{i1}}{x_{i0}-x_{i1}}+R(x_{i1})\frac{-x_0}{x_{i1}-x_0}\frac{-x_{i0}}{x_{i1}-x_{i0}})+(hS_0\frac{-x_i}{x_0-x_i}+(hS_{i0}\frac{-x_{i1}}{x_{i0}-x_{i1}}+hS_{i1}\frac{-x_{i0}}{x_{i1}-x_{i0}})\frac{-x_0}{x_i-x_0})]Q\\&=[r+(hS_0\frac{-x_i}{x_0-x_i}+hS_i\frac{-x_0}{x_i-x_0})]Q=(r+hS)Q\end{aligned}$$

故

$$\begin{aligned}e(P,V)&=e(P,V_0+V_{i0}+V_{i1})=e(P,(r+hS)Q)\\&=e(U+hY_S,Q)\end{aligned}$$

3 安全性分析

该方案的安全性等价于 1.2.1 节的概率签名方案，即在随机预言机模型下是安全的(能够抵抗选择消息攻击)，详细证明见文献[10]。下面首先讨论密钥分发及(门限式)签名过程的安全性。

3.1 签名密钥的安全性

首先，攻击者试图通过公钥信息获取签名密钥等价于求解离散对数困难问题。其次，密钥分发过程将签名密钥进行了两次分割，任何成员试图根据分得的私钥推出签名密钥，等价于求解 2 次门限问题。

3.2 签名过程的安全性

由 2.2.2 节子签名的生成过程可知，子签名 V_0，V_{i0}分别包含 $R(x_0)$，$R(x_{i0})$(签名中心与成员执行 Joint-Shamir-RSS 所得)，对成员来说是随机的。并且签名子密钥隐藏在子签名的指数项中，故成员无法通过子签名得到子密钥。同理，成员虽然合成最终签名，但也无法获得签名密钥。综上所述，整个签名过程没有向成员泄密。

除此之外，该签名方案还具备如下性质：

3.3 不可冒充性

(1) 签名中心无法单独完成签名

由密钥分配过程可知，签名中心虽然拥有主密钥 S_0，n 个子密钥 S_{i0}(来自 n 个不同的多项式)，但仍然无法推出签名密钥或任一成员私钥，故签名中心不能单独完成签名。由此可知，即使签名中心遭受攻击，密钥被窃取，攻击者也无法伪造出合法有效的签名。若攻击者在签名过程中发起攻击，他还能得到子签名和 $R(x_0)$，$R(x_{i0})$，但它们对伪造最终签名以及推出签名密钥毫无用处。

(2) 抵抗成员合谋攻击

设有 u 个成员 $2\leqslant u\leqslant n$ 试图通过各自的私钥合谋伪造签名。但即使是 n 个成员合谋，由于各自的私钥来自不同的多项式，对推出上一级密钥没有任何帮助，他们试图推出签名密钥仍然等价于求解 2 次门限问题。

(3) 任何成员无法冒充其他成员签名

任一成员 i 的私钥 S_{i1} 均与签名中心的子密钥 S_{i0} 一一对应，只有两者合作才能推出上一级密钥并最终完成签名。故成员在签名过程中，必须提交真实身份，签名中心方能调用相应的子密钥，协助成员完成签名。因此，任何成员无法冒充其他成员签名。

综上所述，签名中心、攻击者、合法成员都无法冒充他人完成签名。

3.4 可审计性

该方案的最终签名者是某一个成员，系统必须对其签名行为作出审计。首先，某一成员(设成员 i)必须与签名中心合作才能完成签名，并且为了协助成员 i 生成有效的签名，服务器必须调用与其私钥 S_{i1} 对应的 S_{i0}；其次，由 3.3 节的讨论可知，任何人不能冒充成员 i 利用 S_{i0} 完成签名。于是，签名中心便可通过保留 S_{i0} 的使用记录，来审计各个成员的签名情况。

3.5 稳定性

3.5.1 成员的动态删除

因为成员可能由于种种原因(离任、被攻击者收买等)不能履行签名职责，系统能够方便、有效地删除成员显得很重要。在该方案中，可以通过删除保存在签名中心中与成员 i 对应的子密钥 S_{i0} 来删除成员。

定理 1 (1) 删除的成员不能签名；(2) 某个成员的删除不会影响其他成员签名。

证明：(1) 设成员 i 已被系统删除。当其再次请求签名时，签名中心与成员执行完 Joint-Shamir-RSS 后，找不到对应的子密钥 S_{i0} 生成 V_{i0}，从而成员 i 无法完成最终签名。

(2) 删除成员 i 只是从签名中心中删除了 S_{i0}，并不影响其他成员的密钥和公共签名参数，因此不会影响其他成员签名。

由定理 1 知，成员的删除是安全、有效的。

3.5.2 成员的动态增加

在该方案中，当团体中成员不足以应付繁多的签名需求

时，可以执行以下步骤来方便、有效地添加成员。添加成员的过程参照 2.1 节，设此时存在 t 个成员，添加步骤如下：

1)任选 $x_{t+1}\in Z^+$，不同于 2.1 节第 3)步中已选的 $x_i(i=1,2,\cdots,t)$；

2)构造一个一次多项式 $f_{t+1}(x)=a_{t+1,0}+a_{t+1,1}x$，其中 $a_{t+1,0}=f(x_{t+1})$，$a_{t+1,1}\in_U Z_q^*$；

3)任选 $x_{t+1,0}$，$x_{t+1,1}\in Z^+$；

4)计算新增成员私钥 $S_{t+1,1}=f_{t+1}(x_{t+1,1})$；

5)计算与新增成员私钥对应的签名中心子密钥 $S_{t+1,0}=f_{t+1}(x_{t+1,0})$；

6)公开$(x_{t+1,0},x_{t+1,1})$。

由添加过程可知，添加成员 $t+1$，只需添加成员 $t+1$ 所需的签名参数，并没有影响其他成员的密钥和公共签名参数，因此不会影响其他成员签名。

4 效率分析

4.1 空间复杂度

设本文中群 G_1 上的一个点需要 $2L_c$ 位二进制表示(这里 2 意味着椭圆曲线上点的横、纵坐标)，其余参数需要 L_q 位二进制表示。密钥的生成与分发过程需要公开 2 个椭圆曲线上的点(P,Y_S)以及 $3n+2$ 个密钥生成参数，同时保密 $2n+1$ 个签名中心密钥，共需要空间 $4L_c+(5n+3)L_q$。签名过程中，签名中心最多需要 $3L_c+6L_q$，成员最多需要 $2L_c+3L_q$，则总共需要空间 $9L_c+(5n+12)L_q$。由此可见，我们的方案在存储代价方面可行。

4.2 时间复杂度

令 Mc,Ac,H,P 分别表示群 G_1 上的乘法和加法运算、散列函数运算以及配对运算。本方案中子签名的生成、签名的合成与验证所需的计算量在表 1 中列出。

表 1 本方案签名与验证过程所需的计算量

	子签名的生成		签名的合成与验证	
运算	签名中心	成员	成员	验证者
Mc	5	2	0	0
Ac	2	0	2	0
H	2	0	0	0
P	0	0	0	2

由表 1 的分析可知，整个签名过程的计算代价较低，并且由计算能力较强的签名中心承担了大多数计算量。同时，对于复杂度较高的配对运算，签名的验证过程仅需 2 次。通过与表 2 的对比，本方案所需的计算量都低于文献[10]中的签名方案，且不随成员个数的增加而增长。因此，我们的方案在效率方面是可行的。

表 2 文献[10]中方案签名与验证过程所需的计算量

运算	子签名的生成	签名的合成与验证
Mc	t	1
Ac	0	2n+t
H	1	1
P	0	2

结束语 本文针对当前电子商务的应用需求和已有门限签名方案存在的问题，提出了一种基于双线性对的新型门限签名方案。方案在具备多种安全属性的前提下，实现了某一成员即可独立完成签名，较好地满足了电子业务快速、安全、高效的要求。同时，本方案的密钥分发简单，签名过程执行高效，并能通过审计成员，使方便、高效的增删成员维护系统正常运行，它是一个安全、有效的数字签名方案，能够在现实的电子票据、电子政务系统中得到应用。

进一步的研究工作将围绕对成员的审计方式，本方案中的审计方式，使得签名中心可以肆意伪造成员的签名证据，我们希望通过改进签名方式让成员在签名过程中自己留下不可抵赖的签名证据，以防止签名权利的滥用。

参 考 文 献

[1] Desmedt Y. Society and group oriented cryptography: a new concept[A]//CRYPTO'87[C]. Santa Barbara, CA, USA, 1987: 20-127

[2] Rabin T. A simplified approach to threshold and proactive RSA [A]//CRYPTO'98[C]. Santa Barbara, CA, USA, 1998: 89-104

[3] Shoup V. *Practical threshold signatures* [A] // EUROCRYPT 2000[C]. Bruges, Belgium, 2000: 207-220

[4] Almansa J, Damgard I, Nielsen J. Simplified threshold RSA with adaptive and proactive security[A]//EUROCRYPT 2006[C]. Petersburg, Russia, 2006: 593-611

[5] Halevis G R, Krawczyk H. Threshold RSA for dynamic and ad-hoc group[A] // EUROCRYPT 2008[C]. Istanbul, Turkey, 2008: 88-107

[6] Chen X F, Zhang F G, Kwangjo K. New ID-based threshold signature scheme from bilinear pairings[A]//Progress in Indocrypt 2004[C]. Berlin: Springer-Verlag, 2004: 371-383

[7] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing[A] // Cryptology Asiacrypt'01[C]. Berlin: Springer-Verlag, 2001: 514-532

[8] Baek J, Zheng Y L. Identity-based threshold signature scheme from the bilinear pairings[A]//ITCC 04[C]. New York: IEEE Computer Society, 2004: 124-128

[9] Hess F. Efficient identity based signature schemes based on pairings[A]//Selected Areas in Cryptography 2002[C]. Berlin: Springer-Verlag, 2002: 310-324

[10] 钱海峰，曹珍富，薛庆水. 基于双线性对的新型门限代理签名方案[J]. 中国科学 E 辑，2004，34(6)：711-720

[11] Zhang F G, Chen X F, Susilo W, et al. A New Signature Scheme Without Random Oracles from Bilinear Pairings[A]//Progress in Cryptology-VIETCRYPT 2006[C]. Berlin: Springer-Verlag, 2006: 67-80

[12] Yu J, Kong F Y, Hao R. Forward Secure Threshold Signature Scheme from Bilinear Pairings[J]. Computational Intelligence and Security, 2007, 4456: 587-597

[13] Galindo D, Garcia F D. A Schnorr-like Lightweight Identity-based Signature Scheme[A] // Progress in Cryptology-AFRICACRYPT 2009[C]. Berlin: Springer-Verlag, 2009: 135-148

[14] Schnorr C P. Efficient Signature Generation by Smart Cards[J]. Journal of Cryptology, 1991, 4: 161-174

[15] Pedersen T. Distributed provers with applications to undeniable signatures[A]//EUROCRYPT91[C]. Brighton, UK, 1991: 221-242