基于访问树的属性基签名算法

马春光[1,2]，石 岚[1]，汪 定[1]

(1. 哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001; 2. 电子科技大学网络与数据安全四川省重点实验室 成都 611731)

【摘要】提出了一种基于访问树的属性基签名算法，签名算法采用访问树结构有效地解决了门限属性基签名方案中阈值对签名算法的限制。该算法无需限定属性个数，可以灵活地设定签名策略。算法安全性证明基于标准模型而不是随机预言机模型，在标准模型中将算法的安全性归约到判定BDH困难假设。

关 键 词 访问树; 属性基; 判定BDH; 签名; 标准模型

中图分类号 TP309 **文献标志码** A doi:10.3969/j.issn.1001-0548.2013.03.018

Attribute-Based Signature with AT

MA Chun-guang[1,2], SHI Lan[1], and WANG Ding[1]

(1.College of Computer Science and Technology, Harbin Engineering University Harbin 150001;

2. Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China Chengdu 611731)

Abstract An attribute-based signature with access tree (AT) is presented in this paper. By building AT access control structure, the new scheme can solve the shortage that signature algorithms are always limited by the threshold in threshold attribute-based signature schemes. Our scheme need not constrain the number of attribute set and provides more flexibility in signature strategy. The security of our scheme is proved under the standard model rather than random oracle model.

Key words access tree; attribute-based; decisional bilinear Diffie-Hellman; signature; standard model

ABS是一个新的密码学原语，它将属性引入密码算法中，扩展了身份基签名(identity-based signature，IBS)。在ABS体制中，用户的身份用一系列属性描述，而不是IBS中单一的身份串。在ABS中，当且仅当签名者的属性集合满足断言时才能进行正确的签名。ABS体制可用于当消息接收者需要认证消息发送者身份信息，但发送者又不愿意暴露过多属性的场景，此时，发送者只需应用ABS签名，并用自己的属性生成满足接收者断言的签名即可。

ABS一直是密码学研究的热点问题。ABS具体的签名方案也相继被提出。文献[1]提出了一个断言支持“与”、“或”和“门限”的ABS方案，但是其安全性较弱，其安全性证明是基于一般的群模型。文献[2]提出了基于计算Diffie-Hellman难题，在标准模型下可证安全的ABS方案，但该方案只考虑了(n,n)门限，其中n是签名断言所要求的属性个数。文献[3]对文献[2]提出的ABS方案进行了改进，使其支持(k,n)门限。但是，无论是文献[2]还是文献[3]中所提的方案在效率方面都存在不足，因为在方案中对一个消息的签名需要用到签名者的所有属性。

本文构造了一个断言可由访问树表示的ABS签名，能灵活地支持“与”和“或”门，并基于判定BDH难题，在标准模型下证明了其安全性。

1 相关研究

文献[4]提出了身份基密码体制(identity-based cryptography，IBC)，解决了公钥密码体制中公钥证书分发和管理的不足。在IBC中，用户的公钥可以是任意标识用户的二进制串，如电子邮件地址等，从而可容易地实现实体身份与公钥的绑定。文献[4]同时提出了一个IBS方案。随后，一些IBS方案被相继提出[5-8]，这些体制大多基于因子分解问题(IFP)、离散对数问题(DLP)或二次剩余问题(QRP)，但其安全性都未经过严格的形式化证明。文献[9]使用双线性对技术提出了第一个安全的IBC方案，在随机预言模型下(ROM)可抵抗自适应选择密文攻击。以后，使

收稿日期：2012 – 06 – 29; 修回日期： 2012 – 08 – 17
基金项目：国家自然科学基金(61170241)；四川省重点实验室开放课题基金；黑龙江省自然科学基金面上项目(F201229)
作者简介：马春光 (1974 –)，男，博士，教授，主要从事密码学、信息安全、传感网与物联网等方面的研究.

用双线性对技术研究IBC[10-12]越来越多。

无论是公钥密码体制还是IBC，其加密-解密都是“一对一”的模型，即用一个公钥加密的消息只能用其对应的私钥解密，并且加密者必须知道解密者的身份。为了解决上述问题，2005年，文献[13]提出了基于属性加密(attribute-based encrypt，ABE)的概念。在ABE中，加密者无需知道解密者的详细身份信息，只需掌握解密者的一系列描述属性，在加密过程中用属性定义访问规则，当且仅当用户的密钥与密文在这个访问规则下相“匹配”时，解密用户才可以解密此密文，它是一种“多对多”的密码体制。由于ABE能实现灵活的访问控制策略，在现实生活中具有广泛的应用，如远程文件管理、有目的的广播加密等。从ABE体制提出开始，出现了许多有关ABE体制[14-16]的研究。

ABS扩展了IBS，用户的身份信息用一系列属性，而非身份串描述。签名者的权力由其所拥有的属性集合决定。验证者通过验证该签名，只能确定该签名满足某个访问结构，但不知道签名者是如何满足这个访问结构。ABS在细粒度访问控制的匿名认证系统中具有重要的应用价值。

2　背景知识

本文给出基本概念的形式化定义，以及安全性证明中要使用的数学难题和安全模型。

2.1　秘密共享

秘密共享(secret share，SS)方案是将秘密分散到多方，每一方的秘密称为子秘密。一个(t,n)门限秘密共享方案，其中n是共享者(参与者)的数目，t是门限值，不少于t个参与者子集可以恢复出要保护的秘密，而少于t个参与者则得不到任何关于原秘密的信息。

2.2　访问结构

假定$\{P_1,P_2,\cdots,P_n\}$是参与方的集合，$P=2^{\{P_1,P_2,\cdots,P_n\}}$；访问结构$\mathsf{A}$是$\{P_1,P_2,\cdots,P_n\}$的非空子集，即$\mathsf{A}\subseteq P\setminus\{\varnothing\}$；若访问结构$\mathsf{A}$是单调的，则$\forall B$，$C$，若$B\in\mathsf{A}$且$B\subseteq C$，则$C\in\mathsf{A}$；并且在$\mathsf{A}$中的集合称为授权集合，否则称为非授权集合。文献[17]将访问结构一般化为树状的结构，其中每个结点都是一个带有门限值表示的门。

2.3　双线性映射

设G_1和G_2是两个有限循环群，阶均为$p\in\mathsf{Z}$，具有如下性质的映射$e:G_1\times G_1\to G_2$称为双线性对：1) 双线性性：对$\forall u,v\in G_1$，$\forall a,b\in\mathsf{Z}_p$，存在$e(u^a,v^b)=e(u,v)^{ab}$。2) 非退化性：$\exists g\in G_1$，使$e(g,g)\neq 1$。3) 可计算性：$\forall u,v\in G_1$，存在一个有效的算法计算$e(u,v)$。$e(*,*)$是对称操作，即$e(u^a,v^b)=e(u,v)^{ab}=e(u^b,v^a)$。

2.4　安全模型

首先给出本文的安全证明中使用的复杂性假设，即判定BDH问题。

判定BDH问题[10]为：随机选择$a,b,c,z\in Z_p^*$、$g\in G_1$是生成员，在多项式时间内，不存在算法S能以不可忽略的优势判定出$(g^a,g^b,g^c,e(g,g)^{abc})$与$(g^a,g^b,g^c,e(g,g)^z)$，算法$\mathsf{S}$优势的定义为：

$$|\Pr[\mathsf{S}(g^a,g^b,g^c,e(g,g)^{abc})=0]-\Pr[\mathsf{S}(g^a,g^b,g^c,e(g,g)^z)=0]|$$

ABS体制应满足正确性、匿名性和不可伪造性等安全需求：

1) 正确性：指一个签名者生成的有效签名，一定可以被验证者的验证算法所接受的，即验证成功的概率应为1。

2) 匿名性：基于选择消息攻击的ABS的匿名性可以定义为以下敌手A和挑战者C的游戏：① 系统建立阶段。敌手A输出挑战属性断言T和两个要挑战的属性集合ω_1和ω_2。② 询问查询阶段。挑战者C输入安全参数λ，运行建立算法得到系统参数PK和主密钥MK，挑战者发送系统参数给敌手A，并秘密保存主密钥MK。③ 挑战阶段。敌手A决定何时请求最后的挑战。敌手A继续询问成员的属性私钥和签名。最后，C随机选择$b\in\{0,1\}$并用属性集合ω_b签名。④ 输出阶段。敌手A输出$b'\in\{0,1\}$，如果$b=b'$，则表示敌手成功区分出签名，否则攻击失败。

一个ABS系统是基于选择消息匿名的，则对于任何多项式时间内的敌手，A在只能做p次特定成员属性私钥查询和q次特定成员的签名查询情况下，在上述游戏中获胜的概率是可以忽略的，即有：

$$\mathrm{Adv}_{\mathrm{ABS,A}}^{\mathrm{anom}}(k)\leqslant\varepsilon$$

式中，$\mathrm{Adv}_{\mathrm{ABS,A}}^{\mathrm{anom}}(k)$为敌手能赢得上述游戏的概率。

3) 不可伪造性：多项式时间内，用不满足断言的属性集构造出正确签名的概率是可以忽略的。

3　算法描述

本文介绍了访问树的相关知识，给出了ABS的具体算法。

3.1 访问树

1) 访问树 T。树 T 代表一个访问结构，每个非叶结点都由孩子个数和门限值表示。num_x 表示孩子个数，k_x 表示门限值并有 $0<k_x<\text{num}_x$。$k_x=1$ 时，表示“或”门；$k_x=\text{num}_x$ 时，表示“与”门。每个叶结点都表示一个属性并且其门限值 $k_x=1$。

为了方便，本文定义以下几个函数。首先用 $\text{parent}(x)$ 表示结点 x 的父结点，当且仅当 x 是叶结点时，函数 $\text{att}(x)$ 返回与 x 相关联的属性。树 T 为每个结点的孩子结点定义了顺序，让其从1～num编号。函数 $\text{index}(x)$ 返回与 x 相关联的编号。

2) 满足访问树。设访问树 T 的根结点为 r。标记 T_x 表示根结点为 x 的子树，则访问树 T 同样可以记为 T_r。一个属性集合 ω 满足访问树结构 T_x，则标记 $T_x(\omega)=1$。以递归的方式计算 $T_x(\omega)$，如果 x 是非叶结点，计算 x 的每个孩子结点 x' 的 $T_{x'}(\omega)$ 的值。当且仅当至少 k_x 个孩子结点返回1值时，$T_x(\omega)=1$。当 x 是叶结点时，当且仅当 $\text{att}(x)\in\omega$ 时，$T_x(\omega)=1$。

3.2 具体算法

1) 建立阶段(setup)。定义属性集合 $\mathsf{U}=\{1,2,\cdots,n\}$，对每一个属性 $i\in\mathsf{U}$，从 Z_p 中随机选择 t_i。最后随机选择 $y\in\mathsf{Z}_p$，则公开的公共参数PK为 $T_1=g^{t_1},g^{t_2},\cdots,T_{|\mathsf{U}|}=g^{t_{|\mathsf{U}|}}$，$Y=e(g,g)^y$，主密钥MK为 $t_1,t_2,\cdots,t_{|\mathsf{U}|},y$。

2) 私钥提取阶段(extract)。用户属性集合为 ω，当且仅当 ω 满足访问树，即 $T(\omega)=1$ 时，该算法生成用户相应的私钥。私钥提取过程如下：对访问树 T 中的每一结点 x，用自顶向下的方法从根结点开始生成一个多项式 q_x。其中 q_x 的阶 d_x 为每个结点的门限值减一，即 $d_x=k_x-1$。对于根结点 r，设 $q_r(0)=y$，并随机选择其他的 d_r 个点，生成多项式 q_r。对于其他的结点 x，设 $q_x(0)=q_{\text{parent}(x)}(\text{index}(x))$，并随机选择其他的 d_x 个点用来生成 q_x。多项式生成后，对于每个叶结点生成如下的私钥 $D_x=g^{q_x(0)/t_i}$，$i=\text{att}(x)$。

3) 签名阶段(sign)。该算法对于输入消息 $M\in\mathsf{G}_2$，生成有效的签名。随机选择 $s\in\mathsf{Z}_p$，并对每个属性随机选择 $r_i,i\in\mathsf{U}$，并生成签名 $\sigma=\{\sigma_1,\sigma_2,\sigma_3\}$，其中，$\sigma_2=\{\sigma_{2i}=T_i^{sr_i}\}_{i\in\omega}$，$\sigma_3=\text{MY}^s$，$\sigma_1=\{\sigma_{1i}=D_x^{1/r_i},\ i=\text{att}(x)\}$。

4) 验证阶段(verify)。首先定义一个递归的算法 $\text{Verify}(\sigma_1,\sigma_2,x)$，该算法输入 σ_1、σ_2 和树的结点 x，输出 G_2 中的元素或者 $\perp$。

设 $i=\text{att}(x)$，如果 x 为叶结点时，有：

$$\text{Verify}(\sigma_1,\sigma_2,x)=\begin{cases}e(\sigma_{1i},\sigma_{2i})=e(D_x^{1/r_i},T_i^{sr_i})\\ e(g^{\frac{q_x(0)}{r_it_i}},g^{st_ir_i})\\ e(g,g)^{sq_x(0)} & i\in\gamma\\ \perp & \text{否则}\end{cases}$$

当 x 非叶结点时，首先对 x 的所有孩子结点 z 执行 $\text{Verify}(\sigma_1,\sigma_2,z)$，并把得到的结果记为 F_z，然后选择 $F_z\neq\perp$ 的 k_x 个孩子结点集合 S_x。如果不存在这样的集合则验证算法失败，否则执行如下运算：

$$F_x=\prod_{z\in S_x}F_z^{\Delta_{i,s'x}(0)}=\prod_{z\in S_x}(e(g,g)^{sq_x(0)})^{\Delta_{i,S'x}(0)}=$$

$$\prod_{z\in S_x}(e(g,g)^{sq_{\text{parent}(z)}(\text{index}(z))})^{\Delta_{i,S'x}(0)}=$$

$$\prod_{z\in S_x}e(g,g)^{sq_x(i)\Delta_{i,S_x'}(0)}=e(g,g)^{sq_x(0)}$$

$$i=\text{index}(z)\qquad S_x'=\{\text{index}(z):z\in S_x\}$$

定义了上述算法后，就可进行签名的验证。验证是否成立，则有：

$$\frac{\sigma_3}{\text{Verify}(\sigma_1,\sigma_2,r)}=M$$

如果成立则验证成功，否则验证失败。

4 安全性和效率分析

4.1 正确性

当用户的属性集合 ω 的一个子集 γ 满足访问树，即 $T(\gamma)=1$ 时，该算法的正确性证明如下：

$$\frac{\sigma_3}{\text{Verify}(\sigma_1,\sigma_2,r)}=\frac{MY^s}{e(g,g)^{sq_r(0)}}=$$

$$\frac{MY^s}{e(g,g)^{sy}}=\frac{MY^s}{Y^s}=M$$

4.2 匿名性

定理 1 如果一个敌手攻破签名者的隐私保护，则存在一个模拟器，能以不可忽略的优势解决判定BDH难题。

证明：假设存在一个多项式时间的敌手 A，能以不可忽略的优势 ε 攻破签名者的隐私保护性，则能构造一个模拟器 B，以 $\varepsilon/2$ 的优势解决判定BDH难题，模拟过程如下：

1) 挑战者设定两个群阶为 p 的 G_1和G_2 及在其上的双线性映射 e。挑战者在不让模拟器 B 知道的情况下随机选取 $\mu\in\{0,1\}$。当 $\mu=0$ 时，挑战者设定 $(A,B,C,Z)=(g^a,g^b,g^c,e(g,g)^{abc})$；否则有 $(A,B,C,Z)=(g^a,g^b,g^c,e(g,g)^z)$，其中 a、b、c、z 都是随机选择的。

2) 初始化阶段。定义属性集合U，敌手A选择要挑战的访问树T，消息M和两个满足访问树的属性集合ω_1、ω_2。

3) 建立阶段。模拟器B设置公共参数$Y=e(A,B)=e(g,g)^{ab}$。对于所有属性$i\in\omega_1\cup\omega_2$，随机选择$r_i\in Z_p$，并使$T_i=g^{r_i}$，则此时有$t_i=r_i$；否则，随机选择$\beta_i\in Z_p$，并设$T_i=g^{b\beta_i}=B^{\beta_i}$，则此时有$t_i=b\beta_i$。最后将公共参数传给敌手A。

4) 询问阶段。敌手A询问属性集合ω^*的私钥和用其属性集合的签名，其中$\omega^*\neq\omega_1$和$\omega^*\neq\omega_2$，并且ω^*可以满足也可以不满足访问树结构。为了生成私钥模拟器B，要为访问树的每个节点生成多项式Q_x。

本文定义两个多项式PolySat和PolyUnsat：

① PolySat(T_x,ω,λ_x)：当$T_x(\omega)=1$时，运行该算法生成子树T_x结点的多项式q_x。对子树T_x的根结点x生成一个d_x阶的多项式q_x，使其满足$q_x(0)=\lambda_x$，并随机选择其他的d_x-1个点生成完整的多项式q_x。然后，x的每个孩子结点x'调用PolySat$(T_{x'},\omega,q_x(\text{index}(x')))$，此时，$x$的每个孩子结点$x'$有$q_{x'}=q_x(\text{index}(x'))$。

② PolyUnsat$(T_x,\omega,g^{\lambda_x})$：当$T_x(\omega)=0$时，运行该算法生成子树$T_x$结点的多项式$q_x$，输入为$g^{\lambda_x}\in G_1$，并$\lambda_x\in Z_p$。为根结点$x$生成$d_x$阶的多项式$q_x$，并使$q_x(0)=\lambda_x$。由于$T_x(\omega)=0$，则$x$没有$d_x$个孩子结点子树被满足。设$h_x\leqslant d_x$是$x$的被满足的孩子结点个数。对于每个被满足的孩子结点$x'$，随机选择$\lambda_{x'}\in Z$，并设$q_x(\text{index}(x'))=\lambda_{x'}$。随机选择$d_x-h_x$个点构成多项多$q_x$。递归生成访问树中的每个结点相对应的多项式。对于$x$的每个孩子结点$x'$，调用PolySat$(T_{x'},\omega,q_x(\text{index}(x')))$，此时$q_x(\text{index}(x'))$的值已知；如果$x'$不是被满足的孩子结点，则调用PolyUnsat$(T_{x'},\omega,g^{q_x(\text{index}(x'))})$。对于$x$的每个孩子结点$x'$都有$q_{x'}(0)=q_x(\text{index}(x'))$。

有了上述的算法，则模拟器能够生成对任意属性集的多项式，无论该属性集合是否满足访问树结构。最后生成私钥，对于访问树的每个结点定义最后的多项式$Q_x(\cdot)=bq_x(\cdot)$，此时有$y=Q_r(0)=ab$。对于每个叶结点其私钥如下：

$$D_x=\begin{cases}g^{\frac{Q_x(0)}{t_i}}=g^{\frac{bq_x(0)}{r_i}}=B^{\frac{q_x(0)}{r_i}} & i\in\omega_1\cup\omega_2\\ g^{\frac{Q_x(0)}{t_i}}=g^{\frac{bq_x(0)}{b\beta_i}}=g^{\frac{q_x(0)}{\beta_i}} & \text{其他}\end{cases}$$

上式使$i=\text{att}(x)$。以上的等式给定了每一个叶结点的私钥，能生成敌手A所询问的属性集合的私钥；并且模拟器B能用私钥按签名算法生成敌手A所询问的签名。

5) 挑战阶段。模拟器B随机选择$\upsilon\in\{0,1\}$，并返回属性集合ω_υ下的签名。签名输出如下：

$$\sigma=\{\sigma_1,\sigma_2,\sigma_3\}$$

其中

$$\sigma_1=\{\sigma_{1x}=D_x^{1/h_i}\quad i=\text{att}(x)\}$$

$$\sigma_2=\{\sigma_{2i}=C^{r_i\cdot h_i}\}_{i\in\omega_i}\quad \sigma_3=MZ$$

$$h_i\in Z_p$$

当$\mu=0$时，$Z=e(g,g)^{abc}$，并使$s=c$，则有$Y^s=(e(g,g)^{ab})^c=e(g,g)^{abc}$，并且$\sigma_{2i}=(g^{r_i})^{ch_i}=C^{r_ih_i}$；否则当$\mu=1$时，$Z=e(g,g)^z$。

敌手A输出$\upsilon'\in\{0,1\}$。如果$\upsilon'=\upsilon$，则模拟器B输出$\mu'=0$表示挑战者给出的是一个有效的BHD对，否则输出$\mu'=1$表示挑战者给出的是一个随机的4元组。

从上面的构造中可以看出，模拟器模拟了一个有效的签名系统。接下分析模拟器B解决判定BDH难题的优势。

当$\mu=1$时，敌手A得不到关于υ的任何信息，则有$\Pr[\upsilon\neq\upsilon'\mid\mu=1]=1/2$。当$\upsilon\neq\upsilon'$时，模拟器B输出的是$\mu'=1$，则得到$\Pr[\mu'=\mu\mid\mu=1]=1/2$；当$\mu=0$时，敌手A以不可忽略的优势$\varepsilon$攻破签名匿名性，则有$\Pr[\upsilon=\upsilon'\mid\mu=0]=1/2+\varepsilon$。当$\upsilon=\upsilon'$时，模拟器B输出的为$\mu'=1$，则得到$\Pr[\mu'=\mu\mid\mu=0]=1/2+\varepsilon$。

模拟器B在判定BDH难题中优势为：

$$\frac{1}{2}\Pr[\mu'=\mu\mid\mu=1]+\frac{1}{2}\Pr[\mu'=\mu\mid\mu=0]-\frac{1}{2}=$$

$$\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\varepsilon$$

4.3 不可伪造性

定理 2 如果一个敌手能伪造一个有效的签名，则存在一个模拟器，能以不可忽略的优势解决判定BDH难题。

证明：可以证明如果有算法在多项式时间内可伪造一个有效的签名，则判定BDH问题以不可忽略的概率解决。

4.4 效率分析

将本文的方案与文献[2-3]的方案进行比较。由于在文献[2]中的方案只考虑到了(n,n)门限，并与文献[3]中的方案运用的技巧相似，所以只将本文的方案与文献[3]中的方案进行比较，比较结果如表1所

示。记U、A、B分别为所有属性集合、用户属性集合和验证属性集合，设k为门限值，N为访问树的所有结点个数，签名长度和签名生成代价分别记为Sig.size和Sig.Gen。设两个方案都利用线性映射$e:G_1\times G_1\to G_2$，记EXP为G_1中的指数运算，P为线性对运算，R用于表示其群中的元素。在本文的方案中，密钥生成需要用所有的属性，则其代价为$|U|R$。签名长度、签名生成代价和认证代价分别为$(|A|+|U|+1)R$、$(|A|+|U|)$EXP和NP。

表1 效率分析

指标	文献[3]方案	本文方案
Key.Size	$(2\|A\|)R$	$\|U\|R$
Sig.Size	$(3\|B\|)R$	$(\|A\|+\|U\|+1)R$
Sig.Gen	$(2\|A\|+3\|B\|)$EXP	$(\|A\|+\|U\|)$EXP
Verfication	$4\|B\|$EXP+$\|B\|P$	NP

由表1的效率分析可以看出，当用户的属性集合规模与所有属性集合的规模相差不大时，即$|U|$和$|A|$、$|B|$相差不大时，本文的方案无论在生成密钥时的代价还是在签名，认证时的代价都小于文献[3]提出方案。本文的方案有效率上的优势，因为此时有$2|A|>|U|$、$3|B|>|A|+|U|+1$、$2|A|+3|B|>|A|+|U|$；当所有属性集合的规模大于用户属性规模时，由于本文的方案引进树的结构其验证算法需要使用递归的运算，所以在验证时的运算量比文献[3]中的大。

5 总 结

基于属性密码机制是近几年的研究热点，其研究主要集中在以下方面：1) 设计属性基的匿名签名体制。2) 对签名的安全性进行研究以及提高签名效率等方面。本文提出了一个有效的ABS签名算法，该算法表明由访问树来表示，支持“与”和“或”门。并且在假设判定BDH问题是困难的前提下，证明了该方案的安全性。今后将对能支持“非”门的ABS算法进行研究。

参 考 文 献

[1] MAJI H, PRABHAKARAN M, ROSULEK M. Attribute based signatures: Achieving attribute privacy and collusion-resistance[EB/OL]. [2008-04-15]. http://eprint. iacr. org/2008/328.

[2] LI J, KIM K. Attribute-based ring signatures[EB/OL]. [2008-07-12]. http://eprint. iacr.org/ 2008/394.

[3] SHAHANDASHTI S, SAFAVI-NAINI R. Threshold attribute-based signatures and their application to anonymous credential systems[C]//Progress in Cryptology—AFRICACRYPT. Berlin Heidelberg: Spring, 2009.

[4] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology. Berlin Heidelberg: Spring, 1985.

[5] OKAMOTO T. Provably secure and practical identification schemes and corresponding signature schemes[C]// Advances in Cryptology—CRYPTO’92. Berlin Heidelberg: Springer, 1993.

[6] GUILLOU L, QUISQUATER J J. A “paradoxical” identity-based signature scheme resulting from zero-knowledge[C]//Advances in Cryptology—Crypto’88. New York, USA: Springer-Verlag, 1990.

[7] FIAT A, SHAMIR A. How to prove yourself: Practical solutions to identification and signature problems[C]// Advances in Cryptology—Crypto’86. Berlin Heidelberg: Springer, 1987.

[8] FEIGE U, FIAT A, SHAMIR A. Zero-knowledge proofs of identity[J]. Journal of Cryptology, 1988, 1(2): 77-94.

[9] BONEH D，FRANKLIN M. Identity-based encryption from the weil pairing[C]//Advances in Cryptology—CRYPTO 2001. Berlin Heidelberg: Springer, 2001.

[10] WATERS B. Efficient identity-based encryption without random oracles[C]//Advances in Cryptology—EUROCRYPT 2005. Berlin Heidelberg: Springer, 2005.

[11] CAMENISCH J, LYSYANSKAYA A. Signature schemes and anonymous credentials from bilinear maps[C]// Advances in Cryptology—CRYPTO 2004. Berlin Heidelberg: Springer, 2004.

[12] AU M, LIU J. Identity-based ring signature scheme under standard model[C]//Advances in Information and Computer Security. Berlin Heidelberg: Springer, 2006.

[13] SAHAI A, WATERS B. Fuzzy identity based encryption [C]//Advances in Cryptology—EUROCRYPT 2005. Berlin Heidelberg: Springer, 2005.

[14] GOYAL V, JAIN A. Bounded ciphertext policy attribute based encryption[C]//Languages and Programming Automata. Berlin Heidelberg: Springer, 2008.

[15] PIRRETTI M, TRAYNOR P. Secure attribute-based systems[J]. Journal of Computer Security, 2010, 18(5): 799-837.

[16] EMURA K, MIYAJI A. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]// Information Security Practice and Experience. Berlin Heidelberg: Springer, 2009.

[17] BENALOH J, LEICHTER J. Generalized secret sharing and monotone functions[C]//Advances in Cryptology—CRYPTO’88. New York, USA: Springer, 1990.

编 辑 黄 莘