doi:10.3969/j.issn.1000-436x.2013.z1.019

基于属性的可净化签名方案

刘西蒙[1]，马建峰[2]，熊金波[2]，马骏[2]，李琦[2]
(1. 西安电子科技大学 通信工程学院，陕西 西安 710071；2. 西安电子科技大学 计算机学院，陕西 西安 710071)

摘 要：针对云环境下文件的敏感信息隐藏问题，提出基于属性的可净化签名方案。将可净化的思想引入到基于属性的签名中，有效解决了敏感信息隐藏，保证签名者隐私性的同时提供细粒度访问控制。具体构造了该方案并在 CDH 假设下证明该方案在标准模型下是不可伪造的。分析表明，与已有方案相比，所提方案适用于云环境下文件的敏感信息隐藏。

关键词：属性；访问控制；签名；可净化；标准模型
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0148-08

Attribute based sanitizable signature scheme

LIU Xi-meng[1], MA Jian-feng[2], XIONG Jin-bo[2], MA Jun[2], LI Qi[2]
(1. School of Telecommunication Engineering, Xidian University, Xi'an 710071, China;
2. School of Computer Science and Technology , Xidian University, Xi'an 710071, China)

Abstract: Sensitive information in the document needs to be hidden in cloud computing environment, and attribute based sanitizable signature (ABSS) scheme was proposed to solve this problem. The ABSS scheme brings the character of sanitizable into ABS in order to hide sensitive information, ensure signer's anonymity and achieve fine-grained access control. Under the CDH assumption, the ABSS scheme constructed was proved to be unforged in the standard model. Compared with existing schemes, the proposed ABSS scheme is more appropriate for cloud computing environment.

Key words: attribute based; access control; signature; sanitizable; standard model

1 引言

云计算是一种非常有前景的计算模式，可以减少企业的花销以及基础设施的建设，云端用户可灵活定制相应的服务、应用及资源，并且云具有强大的计算和存储能力，近年来受到学术界以及工业界的广泛关注[1]。尽管云计算给学术界及工业界带来了巨大的好处，安全问题却对云计算在未来的大规模使用产生了阻碍。首要的安全问题为保证云存储服务器上数据的完整性及数据拥有者的隐私性。在云计算环境中，用户将数据提交给云服务提供商进行存储和计算，但云服务提供商通常是一个商业公司，并不是完全可信的。由于数据对于任何一个组织来说都是一个重要的资产，将其暴露在不可信的环境下对任何组织来说都是不利的。因此，保证用户数据的完整性及数据拥有者的隐私性变成一个重要的问题。

近些年来，由于云计算等新兴技术的发展，基于属性的密码学广受关注，其不仅可以保证数据的完整性，也可以为数据提供细粒度的访问控制。基于属性签名 (ABS, attribute based signature)[2]将原有基于身份的签名中身份串扩展为一个属性集，非常适用于匿名认证系统。ABS 为用户提供了一个强有力的工具来保护用户隐私：签名者可以依据其所

收稿日期：2013-07-02
基金项目：长江学者和创新团队发展计划基金资助项目（IRT1078）；国家自然基金委员会—广东联合基金重点基金资助项目（U1135002）；国家科技部重大专项基金资助项目（2011ZX03005-002）；中央高校基本科研业务费基金资助项目（JY10000903001）
Foundation Items: Supported by Program for Changjiang Scholars and Innovative Research Team in University(IRT1078); The Key Program of NSFC-Guangdong Union Foundation (U1135002); Major national S&T program(2011ZX03005-002); The Fundamental Research Funds for the Central Universities(JY10000903001)

在的场景选择与自己相关的属性集签署消息，如果验证者的属性集包含了签名者的属性，就可以验证该消息。在某些情况下，文件中包含部分敏感信息与用户的私人信息，这些信息是不能向公众展示的。处理该问题的一个方法是对需要公开的文件进行信息的修改，也就是说对已经签名的文件进行改动，使之隐私部分不再呈现，该方法称为“净化”。可净化的数字签名(sanitizable signatures)可以保证文件部分的完整性，其允许一个叫做净化者的指定方在原始消息被签名者签署后，不与原始签名者进行多次交互来对原始消息进行修改，依然可以保证数字签名的有效性。本文提出了一种基于属性的可净化签名(ABSS, attribute based sanitizable signatures)方案，不仅可以保证签名者的隐私性，并且可以使半可信方对已签名的消息进行修改而不与原始签名者进行多次交互。综上所述，该方案非常适用于云计算环境中。相关工作介绍如下。

基于属性的加密(ABE, attribute based encryption)[3,4]作为模糊身份加密(FIBE, fuzzy identity based encryption)的一个重要应用，在文献[5]中被首次提出，其主要思想为用户加密所用的属性集与用户解密所用的属性集相交超过门限值就可以解密，因此，FIBE 方案也被称作门限属性加密方案。文献[6]使用了密钥策略的属性基加密(KP-ABE, key-policy attribute based encryption)方案运用于云环境下，实现了安全可扩展地将数据外包给云数据服务器进行存储。相对应与 FIBE 方案，YANG 在文献[7]中首次构造并提出模糊身份签名（FIBS）方案。为了支持大规模属性集与小规模属性集，由于在 FIBS 中，签名者不能控制其隐私，文献[8]提出了一种支持小规模属性集与大规模属性集门限属性签名方案。为了实现签名的强不可伪造性，文献[9]提出了基于属性的签名方案，为签名者提供强隐私保护与签名的强不可伪造性。为了有效地压缩开销签名大小与减小验证时间，文献[10]提出了一种用灵活门限谓词构造的一种新的 ABS 方案。由于属性签名有明显的优势，有很多与属性签名相关的签名被提出，比如，基于属性的群签名[11]，基于属性的环签名[12]。

文献[13]利用变色龙哈希函数[14]，不可否认签名[15]的相关概念上提出了可净化签名方案，方案允许指定的半可信方（称为净化者）更改文件中指定的部分，并且产生一个对于修改后文件的有效签名，并且该过程不需要与原始签名者进行多次交互。透明性是净化签名方案[13,15]的一个性质，方案[16]给出了一个强透明性的净化签名方案，强透明方案要求验证者不知道消息能否被净化，并且该方案是在标准模型下构造的。文献[17]给出了一种多签名者与多净化者的方案代替现有单签名者与单净化者的方案。文献[18]指出了文献[19]所提安全模型的不足，并给出了更强的安全模型，并且减少了验证时间与存储开销。

2　预备知识

2.1　双线性对

令 $\mathbb{G}$ 和 $\mathbb{G}_{\mathrm{T}}$ 是以素数阶为 p 的循环群，设 g 是 $\mathbb{G}$ 的生成元并且 e 为双线性映射 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_{\mathrm{T}}$。双线性映射有以下的性质。

1) 双线性性：对于所有的 $u,v\in\mathbb{G}$ 和 $a,b\in Z_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$。

2) 非退化性：$e(g,g)\neq 1$。

如果对于群 $\mathbb{G}$ 中的运算和双线性运算 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_{\mathrm{T}}$ 都可以有效的计算，那么称 $\mathbb{G}$ 是双线性群。注意到 $e(*,*)$ 是对称操作，也就是说，$e(u^a,v^b)=e(u,v)^{ab}=e(u^b,v^a)$。

2.2　困难性假设

定义 1　计算性 Diffie-Hellman(CDH) 问题为，给定对于未知随机选取的值 $x,y\in Z_{p^*}$。如果 $\left|\Pr[A(g,g^a,g^b)=g^{ab}]\right|\geqslant\epsilon$，称敌手 $\mathcal{A}$ 至少为 ϵ。如果没有 t 时间的敌手以至少 ϵ 的优势解决上述游戏，称 (t,ϵ)-CDH 假设成立。

2.3　灵活门限谓词

在本文中，应用了包含门限的谓词 Υ。所有的谓词 $\Upsilon_{k,\omega^*}(\cdot)$ 都与属性集 ω^* 和门限 k 相关。如果属性集合 $\omega'\cap\omega^*$ 中属性的数量超过门限 k，那么输出为 1，否则输出为 0。表示如下：

$$Y_{k,\omega^*}(\omega')=\begin{cases}1, & |\omega'\cap\omega^*|\geqslant k\\ 0, & \text{其他}\end{cases}$$

3　算法框架与安全模型

3.1　算法框架

系统建立：该算法由密钥生成中心执行，输入为安全参数与全体属性集。输出为公共参数 *params* 与主密钥 *MK*。密钥生成中心将公共参数 *params* 发布，将主密钥 *MK* 保密。

密钥生成：将属性集 ω，主密钥 *MK* 与公共参数 *params* 输入到该算法中。算法生成一个与属性集 ω 相关的私钥。密钥生成中心应用该算法产生私钥并将相对应的私钥通过秘密信道分配给参与到方案中的参与方。

签名：将消息 m，签名者的属性 ω_a 与私钥 d，净化者的属性集 ω_b 与公共参数 *params* 输入到算法中。签名者应用该算法对消息 m 签名，其中，$m = m_1 m_2 \cdots m_n \in \{0,1\}^n$，定义 m_i 为消息 m 的第 i 个比特。令 $I_S \subseteq \{1,\cdots,n\}$ 为净化者允许修改的消息的标号。

算法输出为消息 m 的签名，并将签名者的秘密消息 *SI* 通过安全信道发送给净化者。

净化签名：该算法由净化者执行，输入为消息 m、公共参数 *params*、与 m 相关的签名 σ、净化者的属性集 ω_b 和由签名者发送来的秘密消息 *SI*。算法输出为消息 m' 与净化签名 σ'。

验证：该算法由验证者执行，输入为未净化的消息签名对 (m,σ) 或者是经过净化的消息签名对 (m',σ')、公开参数 *params*、签名者的属性集 ω_a 与净化者的属性集 ω_b。其算法输出为 accept 或者 reject。强透明性要求验证者不能发现消息是否被净化，也就是说，验证过程对于净化与非净化的签名者都是相同的。

3.2 安全模型

3.2.1 不可伪造性

定义不可伪造性的游戏 $\mathrm{Exp}_{\mathrm{unf}}$，具体如下。

系统建立：模拟器 $\mathcal{B}$ 运行系统建立算法产生公开参数与属性集，并将此交给敌手 $\mathcal{A}$。

询问：敌手 $\mathcal{A}$ 可以进行多项式次询问，每一次询问为可以为以下之一。

私钥询问：敌手 $\mathcal{A}$ 可以自适应的对 $\mathcal{B}$ 进行关于属性集 ω_j 的私钥的询问，使对于所有 j 有 $|\omega_j \cap \omega^*| < k$。挑战者 $\mathcal{B}$ 运行密钥生成算法获得私钥并将私钥结果送给 $\mathcal{A}$。

签名询问：敌手自适应地选择签名者的属性集与净化者的属性集，利用密钥生成算法生成签名者的私钥，挑战者 $\mathcal{B}$ 利用签名者的私钥，消息与净化者的属性集通过签名算法生成签名，并将其发送给 $\mathcal{A}$。

伪造：最终，敌手输出消息 m^*，属性值 ω_a^* 与 ω_b^* 与签名值 σ^*。如果下面的条件成立，敌手输出 succeed。

1) 将 m^*，属性值 ω_a^* 与 ω_b^* 与签名值 σ^* 输入验证算法，验证算法输出 accept。

2) 没有对 ω_a^* 进行私钥询问。

3) 没有对 m^*，属性值 ω_a^* 与 ω_b^* 进行签名询问。

定义 2 如果不存在 t 时间的敌手进行 q_e 次密钥询问与 q_S 次私钥询问，并以不超过 ϵ 的优势赢得上述游戏，基于属性的净化签名是 (t,q_e,q_S,ϵ)-安全的。

3.2.2 不变性

对于不变性，定义以下游戏 $\mathrm{Exp}_{\mathrm{imm}}$。其中，令 I_S 为净化者允许修改消息比特的位置。这里，敌手为一个净化者试图修改 I_S 以外的比特。

初始化：$\mathcal{A}$ 声称挑战集合 I_S，I_S 为允许净化消息的比特的位置。

系统建立：模拟器 $\mathcal{B}$ 运行系统建立算法产生公开参数与属性集，并将此交给敌手 $\mathcal{A}$。

询问：敌手 $\mathcal{A}$ 可以自适应地进行多项式 q_e 次密钥询问与 q_S 次签名询问，密钥询问和签名询问与 $\mathrm{Exp}_{\mathrm{unf}}$ 中类似。假定在签名询问的第 j 次中，输入的消息为 $m_j = m_{j,1} m_{j,2} \cdots m_{j,n}$，通过签名询问产生关于消息 m_j 的签名 σ_j。

输出：最终，$\mathcal{A}$ 输出消息 $m^* = m_1^* m_2^* \cdots m_n^*$ 的签名 σ^*，其中，对于任意的 $j \in \{1,\cdots,q_S\}$，不存在 $i \in I_S$，使 $m_{j,i} = m_i^*$。

如果签名 σ^* 与消息 m^* 通过验证，说 $\mathcal{A}$ 赢得了上述游戏，敌手赢得以上游戏的优势就定义为：$Adv_{\mathcal{A}} = Pr[\mathcal{A}\ \text{succeed}]$。

定义 3 如果不存在敌手以不超过 ϵ 的优势赢得上述游戏，基于属性的净化签名是 ϵ-不变的。

4 方案构造

在本节中，给出了 ABSS 的具体构造。ABSS 包含 5 个算法：系统建立、密钥生成算法、签名、净化、验证。

系统建立：算法定义全体属性集 U，其所有的元素都在 Z_p 中。选择 $d-1$ 个默认属性集 $\Omega = \{\Omega_1, \Omega_2, \cdots, \Omega_{d-1}\}$。选择 g 为群 $\mathbb{G}$ 的生成元。选择一个随机数 $\alpha \in Z_p^*$ 并且计算 $g_1 = g^\alpha \in \mathbb{G}$。选择一个随机元素 g_2 并且计算 $A = (g_1, g_2)$。随机的从 $\mathbb{G}$ 中选择元素 $t_1,\cdots,t_{n+1}$ 并且令 N 为集合 $\{1,\cdots,n+1\}$，计算函数 T 为

$$T(x) = g_2^{x^n} \prod_{j=1}^{n+1} t_j^{\Delta_{j,N}(x)}$$

随机从 Z_p 中选择 y' 并且从 Z_p^k 中随机选择

$\boldsymbol{y}=(y_1,y_2,\cdots,y_k)$，计算 $u'=g^{y'}$，$\boldsymbol{U}=(u_1,u_2,\cdots,u_k)=(g^{y_1},g^{y_2},\cdots,g^{y_k})$。

算法输出公开参数

$$params=(\mathbb{G},\mathbb{G}_T,e,g,g_1,g_2,t_1,\cdots,t_{n+1},\boldsymbol{U},A),$$

主密钥为

$$MSK=\alpha$$

密钥生成算法:该算法生成一个与属性集 ω 的私钥。首先，算法随机选择一个 $d-1$ 阶的多项式使得 $q(0)=\alpha$；其次生成一个新的属性集合 $\hat{\omega}=\omega\cup\Omega$。对于 $i\in\hat{\omega}$，选择 $r_i\in Z_p$ 并且计算 $d_{i0}=g_2^{q(i)}\cdot T(i)^{r_i}$ 和 $d_{i1}=g^{r_i}$；最终，算法输出 $D_i=(d_{i0},d_{i1})_{i\in\hat{\omega}}$ 作为私钥。

签名：算法输入与属性集相关的签名者的私钥，消息 m，谓词 $\Upsilon_{m,\omega'}(\cdot)$。为了用谓词对消息 m 进行签名，算法从子集合 $\omega'\subseteq\omega\cap\omega^*$ 中选择 k 个元素，算法执行如下过程。

1) 首先，算法选择一个默认的属性子集合 $\Omega'\subseteq\Omega$ 使 $|\Omega'|=d-k$。对于 $i\in\omega^*\cup\Omega'$，从 Z_p 中选择 $n+d-k$ 个随机元素 $r_i'\in Z_p$。

2) 算法计算 $\sigma_0=[\prod_{i\in\omega_b^*\cup\Omega_a'}d_{i0}^{\Delta_{i,S}(0)}][\prod_{i\in\omega_b^*\cup\Omega_a'}T(i)^{r_i'}]\cdot[\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{r_i''}](u'\prod_{j=1}^{k}u_j^{m_j})^{r_s}$，$\{\sigma_{ai}=d_{i1}^{\Delta_{i,S}(0)}g^{r_i'}\}_{i\in\omega_a'\cup\Omega_a'}$，$\{\sigma_{ai}=g^{r_i'}\}_{i\in\omega_a^*/\Omega_a'}$，$\{\sigma_{bi}=g^{r_i'}\}_{i\in\omega_b^*\cup\Omega_b'}$ $\sigma_m=g^{r_s}$。

3) 最终，输出签名为 $\sigma=(\sigma_0,\{\sigma_i\}_{i\in\omega_a^*\cup\Omega_a'},\{\sigma_i\}_{i\in\omega_b^*\cup\Omega_b'},\sigma_m)$。

净化：净化者获得签名 $\sigma=(\sigma_0,\{\sigma_{ai}\}_{i\in\omega_a^*\cup\Omega_a'},\{\sigma_{bi}\}_{i\in\omega_b^*\cup\Omega_b'},\sigma_0')$ 与从签名者获得的秘密消息 $u_i^r,\forall i\in I_S$。首先，运行验证算法来检查签名是否是合法的。定义集合 $I\subseteq I_S$ 为 m' 与消息 m 信息位置不同标识的集合，定义集合 $I_1=\{i\in I:m_i=0,m_i'=1\}$，$I_2=\{i\in I:m_i=1,m_i'=0\}$. 净化者首先选择随机数 $\tilde{r}_i',\tilde{r}_i'',\tilde{r}_s\in Z_p$，并且计算净化签名为

$$\sigma'=(\sigma_0',\{\sigma_{ai}'\}_{i\in\omega_a'\cup\Omega_a'},\{\sigma_{bi}'\}_{i\in\omega_b^*\cup\Omega_b'},\sigma_m')$$

$$\sigma_0'=\sigma_0[\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{\tilde{r}_i'}][\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{\tilde{r}_i''}]\cdot\frac{\prod_{i\in I_1}u_i^r}{\prod_{i\in I_2}u_i^r}\left(u'\prod_{i\in\mathcal{M}}u_i^{m_i'}\right)^{\tilde{r}_s}$$

$$\sigma_{ai}'=\sigma_{ai}g^{\tilde{r}_i'},\sigma_{bi}'=\sigma_{bi}g^{\tilde{r}_i''}\ \sigma_m'=\sigma_m g^{\tilde{r}_s}$$

验证：为了验证签名的正确性，需要验证等式

$$\frac{e(g,\sigma_0)\cdot e(u'\prod_{j=1}^{k}u_j^{m_j},\sigma_m)^{-1}}{\left[\prod_{i\in\omega_a^*\cup\Omega_a'}e(T(i),\sigma_{ai})\right]\left[\prod_{i\in\omega_b^*\cup\Omega_b'}e(T(i),\sigma_{bi})\right]}=A$$

验证算法不仅适用于净化消息，并且适用于非净化消息。

5　安全性分析

5.1　正确性

对于给定消息 m，验证签名 σ 通过等式

$$\frac{e(g,\sigma_0)e(u'\prod_{j=1}^{k}u_j^{m_j},\sigma_m)^{-1}}{\left[\prod_{i\in\omega_a^*\cup\Omega_a'}e(T(i),\sigma_i)\right]\left[\prod_{i\in\omega_b^*\cup\Omega_b'}e(T(i),\sigma_i)\right]}$$

$$=e(g,[\prod_{i\in\omega_a'\cup\Omega_a'}d_{i0}^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{r_i'}][\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{r_i''}](u'\prod_{j=1}^{k}u_j^{m_j})^{r_s})[\prod_{i\in\omega_a'\cup\Omega_a'}e(T(i),\sigma_i)]^{-1}\cdot\left[\prod_{i\in\omega_b^*\cup\Omega_b'}e(T(i),g^{r_i''})\right]^{-1}e(u'\prod_{j=1}^{k}u_j^{m_j},g^{r_s})^{-1}$$

$$=\frac{e(g,[\prod_{i\in\omega_a'\cup\Omega_a'}d_{i0}^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{r_i'}])}{\left[\prod_{i\in\omega_a'\cup\Omega_a'}e(T(i),d_{i1}^{\Delta_{i,S}(0)}g^{r_i'})\right]\left[\prod_{i\in\omega_a^*/\Omega_a'}e(T(i),g^{r_i'})\right]}$$

$$=e(g,g_2^{\alpha})=e(g_1,g_2)=A$$

因此，正确的签名是可以通过验证的等式。

净化性：当获得净化签名 $\sigma'=(\sigma_0',\{\sigma_{ai}'\}_{i\in\omega_a'\cup\Omega_a'},\{\sigma_{bi}'\}_{i\in\omega_b^*\cup\Omega_b'},\sigma_m')$ 时，其中

$$\sigma_0'=\sigma_0[\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{\tilde{r}_i'}][\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{\tilde{r}_i''}]\cdot\frac{\prod_{i\in I_1}u_i^r}{\prod_{i\in I_2}u_i^r}\left(u'\prod_{i\in\mathcal{M}}u_i^{m_i'}\right)^{\tilde{r}_s}$$

$$\sigma_{ai}'=\sigma_{ai}g^{\tilde{r}_i'},\sigma_{bi}'=\sigma_{bi}g^{\tilde{r}_i''},\sigma_m'=\sigma_m g^{\tilde{r}_s}$$

$I_1=\{i\in I:m_i=0,m_i'=1\}$，$I_2=\{i\in I:m_i=1,m_i'=0\}$

当 $i\in I_1$ 时，记 $m_i'-m_i$ 为 1；当 $i\in I_2$ 时，$m_i'-m_i$ 的值为 –1，记为 0。

因此，有

$$\sigma_0'=\sigma_0[\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{\tilde{r}_i'}][\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{\tilde{r}_i''}]\cdot\frac{\prod_{i\in I_1}u_i^{r_s}}{\prod_{i\in I_2}u_i^{r_s}}\left(u'\prod_{i\in\mathcal{M}}u_i^{m_i'}\right)^{\tilde{r}_s}$$

$$=[\prod_{i\in\omega_a'\cup\Omega_a'}d_{i0}^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{r_i'}]\cdot[\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{r_i''}](u'\prod_{i\in\mathcal{M}}u_i^{m_i})^{r_s}\cdot$$

$$[\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{\tilde{r}_i'}][\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{\tilde{r}_i''}]$$
$$\left(u'\prod_{i\in\mathcal{M}}u_i^{m_i'-m_i}\right)^{r_s}\left(u'\prod_{i\in\mathcal{M}}u_i^{m_i'}\right)^{\tilde{r}_s}$$
$$=[\prod_{i\in\omega_a'\cup\Omega_a'}d_{i0}^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{r_i'+\tilde{r}_i'}]\cdot$$
$$[\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{r_i''+\tilde{r}_i''}]\left(u'\prod_{i\in\mathcal{M}}u_i^{m_i'}\right)^{r_s+\tilde{r}_s}$$

净化签名的构成为

$$\sigma'=(\sigma_0',\{\sigma_{ai}'\}_{i\in\omega_a'\cup\Omega_a'},\{\sigma_{bi}'\}_{i\in\omega_b^*\cup\Omega_b'},\sigma_m')$$

其中，$\sigma_0'=[\prod_{i\in\omega_a'\cup\Omega_a'}d_{i0}^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{r_i'+\tilde{r}_i'}]\cdot[\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{r_i''+\tilde{r}_i''}]\left(u'\prod_{i\in\mathcal{M}}u_i^{m_i'}\right)^{r_s+\tilde{r}_s}\{\sigma_{ai}'=d_{i1}^{\Delta_{i,S}(0)}g^{r_i'+\tilde{r}'}\}_{i\in\omega_a'\cup\Omega_a'}\{\sigma_{ai}=g^{r_i'+\tilde{r}'}\}_{i\in\omega_a^*/\Omega_a'}$，$\sigma_{bi}=g^{r_i''+\tilde{r}_i''}$。

净化签名的分部与原始签名的分布是一样的，这样，净化签名也可以通过验证等式。

5.2 不可伪造性

定理 1 所提出的净化签名是(t,q_e,q_S,ϵ)不可伪造的在(t',ϵ')-CDH 假设下，当

$$\epsilon'\geqslant\frac{\epsilon}{4\binom{d-1}{d-k}p^{2n}(n_m+1)(q_e+q_S)}\text{时，}$$

$$t'=t+O((d(q_e+q_S)+n_mq_S)t_m+d(q_e+q_S)t_e)$$

其中，t_m为群$\mathbb{G}$中乘法运算的时间，t_e为群G中指数运算的时间。

证明 假设存在敌手$\mathcal{A}$以优势ϵ攻击这个方案。构造一个概率多项式时间的算法$\mathcal{B}$以概率至少为ϵ'解决 CDH 问题。算法$\mathcal{B}$输入一个群G，一个生成元g与元素g^a和g^b。为了用$\mathcal{A}$来解决这个问题，算法$\mathcal{B}$需要为$\mathcal{A}$构造一个挑战者。模拟构造如下。

初始化：对于一个预定义的整数d，定默认的属性集为$\Omega=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$，选择随机数$k\in\{0,\cdots,q\}$，并且在区间$\{0,\cdots,2l-1\}$选择随机数$x',x_1,\cdots,x_q$。然后选择一个随机选择$n$阶多项式$u(x)$使对于任意$x$，当且仅当$x\in\alpha$时，有$u(x)=-x^n$。对于$i$从 1 到$n$，$\mathcal{B}$定义$t_i$为$t_i=g_2^{u(i)}g^{f(i)}$。由于$t_i$的选择是随机的，有

$$T(i)=g_2^{i^n}\prod_{j=1}^{n+1}\left(g_2^{u(j)}g^{f(j)}\right)^{\Delta_{j,N}(i)}=g_2^{i^n+u(i)}g^{f(i)}$$

选择随机的元素$z',z_1,\cdots,z_q\in Z_p$使得对于$1\leqslant k\leqslant q$有

$$u'=g_2^{x'-l_mk_m'}g^{z'},\quad u_k=g_2^{x_k}g^{z_k}$$

为了使表示简单，定义以下 2 个函数$F(m)$、$J(m)$为

$$F(m)=x'-k'l-\sum_j x_jm_j$$

$$J(m)=z'+\sum_j z_jm_j$$

那么，主密钥为$g_2^\alpha=g_2^a=g^{ab}$并且如下的等式成立：

$$u'\prod_{j\in M}u_j^{m_j}=g_2^{F(m)}g^{J(m)}$$

密钥询问：$\mathcal{A}$可以询问关于属性集ω的私钥，使得$|\omega\cap\omega^*|<k$，定义 3 个子集Γ,Γ',S使$\Gamma=(\omega\cap\omega^*)\cup\Omega^*$，$\Gamma\subseteq\Gamma'\subseteq S$，$|\Gamma'|=d-1$。令集合$S=\Gamma'\cup\{0\}$，对于$i\in\Gamma'$，计算$D_i=(g_2^{\lambda_i}T(i)^{r_i},g^{r_i})$，其中$\lambda_i$、$r_i$是从$Z_p$中随机选取的；对于$i\notin\Gamma',D_i$模拟为

$$\begin{aligned}D_1^{(i)}&=(\prod_{j\in\Gamma'}g_2^{\lambda_j\Delta_{j,S}(i)})(g_1^{-\frac{f(i)}{i^n+u(i)}}(g_2^{i^n+u(i)}g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}\\&=(\prod_{j\in\Gamma'}g_2^{\lambda_j\Delta_{j,S}(i)})(g^{-\frac{af(i)}{i^n+u(i)}}(g_2^{i^n+u(i)}g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}\\&=(\prod_{j\in\Gamma'}g_2^{\lambda_j\Delta_{j,S}(i)})(g_2^a(g_2^{i^n+u(i)}g^{f(i)})^{-\frac{a}{i^n+u(i)}}\cdot\\&\quad(g_2^{i^n+u(i)}g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}\\&=(\prod_{j\in\Gamma'}g_2^{\lambda_j\Delta_{j,S}(i)})\,(g_2^a(g_2^{i^n+u(i)}g^{f(i)})^{r_i'-\frac{a}{i^n+u(i)}})^{\Delta_{0,S}(i)}\\&=(\prod_{j\in\Gamma'}g_2^{\lambda_j\Delta_{j,S}(i)})g_2^{a\Delta_{0,S}(i)}T(i)^{r_i}\\&=g_2^{q(i)}T(i)^{r_i}\end{aligned}$$

$$D_2^{(i)}=(g_1^{\frac{-1}{i^n+u(i)}}g^{r_i'})^{\Delta_{0,S}(i)}=(g^{r_i'-\frac{1}{i^n+u(i)}})^{\Delta_{0,S}(i)}$$

签名询问：此询问是与消息m和属性集ω^*相关。如果$F(m)=0(\mathrm{mod}\,p)$，那么模拟终止。否则，$\mathcal{B}$选择一个随机的集合Λ，使得$|\Lambda|=d-1$。定义$g^{q'(i)}=g^{\lambda_i'}$，其中λ_i'是在Z_p中随机选择的。对于$i\in\omega^*-\Lambda$，计算$g^{q'(i)}=\left(\prod_{k=1}^{d-1}g^{\lambda_k'\Delta_{k,\omega_i^*}(i)}\right)g^{a\Delta_{0,\omega_i^*}(i)}$。$\mathcal{B}$随机选取$r_i',\hat{r}\in Z_p$计算签名为

$$\sigma=(S_1,S_2,S_3,S_4)$$

其中，$S_1=g_1^{-\frac{J(m)}{F(m)}}[\prod_{i\in\omega_a'\cup\Omega_a'}(T(i)^{r_i})^{\Delta_{i,S}(0)}]$
$$[\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{r_i'}][\prod_{i\in\omega_b^*\cup\Omega_b'}T(i)^{r_i''}](g^{J(m)}g_2^{F(m)})^{\tilde{r}_s}$$
$$=g_2^a[\prod_{i\in\omega_a'\cup\Omega_a'}(T(i)^{r_i})^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'}T(i)^{r_i'}]$$

$$[\prod_{i\in\omega_b^*\cup\Omega_b'} T(i)^{r_i''}](g^{J(m)}g_2^{F(m)})^{r_s-\frac{a}{F(m)}}$$

$$= g_2^a[\prod_{i\in\omega_a'\cup\Omega_a'}(T(i)^{r_i})^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'} T(i)^{r_i'}]$$

$$[\prod_{i\in\omega_b^*\cup\Omega_b'} T(i)^{r_i''}](g^{J(m)}g_2^{F(m)})^{r_s}$$

$$= g_2^a[\prod_{i\in\omega_a'\cup\Omega_a'}(T(i)^{r_i})^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'} T(i)^{r_i'}]$$

$$[\prod_{i\in\omega_b^*\cup\Omega_b'} T(i)^{r_i''}](u'\prod_{j=1}^{k} u_j^{m_j})^{r_s}$$

$$=[\prod_{i\in\omega_a'\cup\Omega_a'} d_{i0}^{\Delta_{i,S}(0)}][\prod_{i\in\omega_a^*\cup\Omega_a'} T(i)^{r_i'}]$$

$$[\prod_{i\in\omega_b^*\cup\Omega_b'} T(i)^{r_i''}](u'\prod_{j=1}^{k} u_j^{m_j})^{r_s}$$

$S_2 = \{d_{i1}^{\Delta_{i,S}(0)} g^{r_i'}\}_{i\in\omega'\cup\Omega'}, S_2 = \{g^{r_i'}\}_{i\in\omega^*/\omega}$ ，

$S_3 = \{g^{r_i''}\}_{i\in\omega_b^*\cup\Omega_b'}, S_4 = g_1^{-\frac{1}{F(m)}} g^{r_s}$

伪造：如果 $\mathcal{B}$ 在上述过程中没有终止，$\mathcal{A}$ 将伪造消息 m^* 的签名 σ^*。如果 $F(m^*)\neq 0$ 或者 $\omega_a^*\neq\omega_a'^*$ 或者 $\omega_b^*\neq\omega_b'^*$，那么 $\mathcal{B}$ 终止并且输出 $\perp$。只有当 $F(m^*)=0$ 并且 $\omega_a^*=\omega_a'^*$ 且 $\omega_b^*=\omega_b'^*$，$\mathcal{B}$ 计算并输出

$$\frac{S_1^*}{\prod_{i\in\omega_a^*\cup\Omega_a'}(S_2^*)^{f(i)}\prod_{i\in\omega_b^*\cup\Omega_b'}(S_3^*)^{f(i)}(S_4^*)^{J(m)}} = g^{ab}$$

其中，

$$S_1^* = g_2^a\prod_{i\in\omega_a^*\cup\Omega_a'} T(i)^{r_i\Delta_{i,S}(0)+r_i'}\cdot \prod_{i\in\omega_b^*\cup\Omega_b'} T(i)^{r_i''}(u'\prod_{j=1}^{k} u_j^{m_j})^{r_s}$$

$$= g_2^a\prod_{i\in\omega_a^*\cup\Omega_a'}(g^{f(i)r_i\Delta_{i,S}(0)}g^{f(i)r_i'}) \prod_{i\in\omega_b^*\cup\Omega_b'} g^{r_i''}(g^{J(m)})^{r_s}$$

$$S_2^* = g^{r_{ki}\Delta_{i,S}(0)+r_{ki}'}, S_3^* = g^{r_i''},\ S_4^* = (g)^{r_s}$$

因此，这个算法可以成功地计算并解决 CDH 问题。

5.3　概率分析

需要分析在描述整个模拟过程中，$\mathcal{B}$ 没有终止的概率。若要 $\mathcal{B}$ 在模拟的过程中不发生终止，则需要以下情况发生。

定义事件为 A_k, A^*, B, C 使在密钥生成询问，签名询问中不终止。

$A_k : F(m_k)\neq 0(\mathrm{mod}\, l_u)$

$A^* : F(m^*) = 0(\mathrm{mod}\, p)$

$B : \omega_a^*=\omega_a'^*$

$C : \omega_b^*=\omega_b'^*$

$$Pr[\mathrm{Not-abort}] \geqslant Pr[\bigwedge\nolimits_{k=1}^{q_I} A_k \wedge A^* \wedge B \wedge C]$$

$$Pr[A^*] = Pr[F(m^*)=0(\mathrm{mod}\, p)\wedge F(m^*)=0(\mathrm{mod}\, l_m)]$$

$$= Pr[F(m^*)=0(\mathrm{mod}\, l_m)]$$

$$Pr[F(m^*)=0(\mathrm{mod}\, p)\wedge F(m^*)=0(\mathrm{mod}\, l_m)]$$

$$= \frac{1}{l_m(n_m+1)}$$

$$Pr[\wedge_{k=1}^{q_I} A_k \mid A^*] = \sum_{k=1}^{q_I} Pr[A_k \mid A^*] \geqslant \frac{1}{l_m(n_m+1)}\left(1-\frac{q_e+q_s}{l_m}\right)$$

那么，整个模拟不终止的概率为

$$Pr[notabort] \geqslant Pr[\wedge_{k=1}^{q_I} A_k \wedge A^* \wedge B \wedge C] \geqslant Pr[\wedge_{k=1}^{q_I} A_k \wedge A^*]Pr[B]Pr[C] \geqslant \frac{1}{4(n_m+1)(q_e+q_s)}\cdot\frac{1}{p^n}\cdot\frac{1}{p^n}$$

如果仿真没有终止，从 $d-1$ 个集合 Ω 中正确 $d-k$ 个子集合 Ω^* 的概率为 $1/\binom{d-1}{d-k}$。因此，解决 CDH 问题的概率为

$$\epsilon' \geqslant \frac{\epsilon}{4\binom{d-1}{d-k}p^{2n}(n_m+1)(q_e+q_S)}$$

其中，$t' = t + O((d(q_e+q_S)+n_m q_S)t_m + d(q_e+q_S)t_e)$

5.4　不可区分性

在正确性小节曾指出，有签名者产生与消息 m 相关的正确签名 σ_s 与净化者对消息 m_1 产生的净化签名 σ_1' 是同分布的。同理，净化者对消息 m_2 产生的净化签名 σ_2' 是与 σ_s 同分布的。因此有，净化签名 σ_1' 与净化签名 σ_2' 是同分布的。

5.5　不变性

证明下面的定理来说明不变性。

为了定理 2，需要介绍引理 1 来证明定理 2。

引理 1　对于任意的随机多项式算法 $\mathcal{B}$，其在不变性的游戏 $\mathrm{Exp}_{\mathrm{imm}}$ 中的优势为 ϵ_b，可以访问消息长度为 n，净化在位置 I_S 的 m 比特数据。那么存在一个多项式时间算法 $\mathcal{A}$ 在不可伪造游戏的 $\mathrm{Exp}_{\mathrm{unf}}$ 以优势 $\epsilon_a \geqslant \epsilon_b$，其中消息长度为 $n-m$。

证明　引理 1 的详细证明在文献[15]中给出。

定理 2　提出的基于属性的净化签名是 ϵ-不变

的在ϵ'-CDH 假设下，其中，存在一个整数l，使$\epsilon \leqslant l\epsilon'$。

证明　证明净化者不能修改关于位置$I_S \subseteq \{1,\cdots,n\}$以外的数据，仅能修改$\{u_i^r : i \in I_S\}$。由定理 1 可知，赢得不可伪造游戏$\mathrm{Exp}_{\mathrm{unf}}$任何概率多项式算法的优势在 CDH 假设下是可忽略的。通过应用引理 1，可知赢得不变性游戏$\mathrm{Exp}_{\mathrm{imm}}$任何概率多项式算法的优势在CDH假设下也是可忽略的。这就证明了定理 2。

6　方案分析

在云计算环境中，签名方案保护用户数据完整性的同时保证签名者身份的隐私性，并且可以达到细粒度的访问控制。为了解决云计算中敏感信息隐藏的问题，还需要使签名方案具有可净化性。本节，将ABSS与文献[5,9,15,19]的方案进行对比。文献[5]首次给出了在标准模型下的模糊身份签名(FIBS, fuzzy identity based signature)，该方案可以被用在生物学认证中以保证数据的完整性，但是 FIBS 不能保证用户的匿名性与细粒度的访问控制。同时，方案不具有可净化性。文献[9]给出了一种基于属性的签名，该方案保证用户匿名性的同时可以达到细粒度的访问控制，但是，该方案不具有净化性并且方案是在随机寓言机模型下证明是安全的。方案[15]与[19]给出了可净化的数字签名，相比于[19]方案，方案[15]可以实现强透明性，并且方案在标准模型下是可证明安全的。方案[19]不具有透明性并且其构造是基于随机寓言机（RO, random oracle）模型。方案[15,19]都不能实现对用户的匿名性与细粒度访问控制。本文提出的 ABSS 不仅可以具有属性加密中保护用户隐私性与达到细粒度访问控制的性质，并且具有强透明性，在标准模型下可证明是安全的。方案对比如表 1 所示。

表 1　　**方案比较**

	方案[6]	方案[10]	方案[16]	方案[20]	本文方案
数据的完整性	是	是	是	是	是
用户的匿名性	否	是	否	否	是
细粒度访问控制	否	是	否	否	是
安全性假设	CDH	CDH	co-GDH	CDH	CDH
可净化	否	否	是	是	是
透明性	否	否	否	强透明性	强透明性
模型	标准模型	RO 模型	RO 模型	标准模型	标准模型

7　结束语

本文提出了一种基于属性的可净化签名。方案保证用户匿名性的同时，解决了对敏感信息隐藏的问题。文中给出了其安全模型并给出了详细的构造，并对基于属性的可净化签名的安全性进行了详细的分析。通过对本方案与已有的方案对比分析得出，相比于已有的方案，本方案的更适用于云环境中。

参考文献：

[1] ARMBRUST M, FOX A, GRIFFITH R, *et al.* A view of cloud computing[J]. Communications of the ACM, 2010, 53(4):50-58.

[2] SHANIQNG G, YINGPEI Z. Attribute-based signature scheme[A]. Information Security and Assurance[C]. Busan, Korea, 2008. 509-511.

[3] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. Alexandria, Virginia, USA, 2006. 89-98.

[4] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[A]. Public Key Cryptography-PKC 2011[C]. Taormina, Italy, 2011. 53-70.

[5] SAHAI A, WATERS B. Fuzzy identity-based encryption[A], Advances in Cryptology-EUROCRYPT 2005[C]. Aarhus, Denmark, 2005. 457-473.

[6] YANG P, CAO Z, DONG X. Fuzzy identity based signature[EB/OL]. http://eprint.iacr.org/2008/002.pdf.

[7] SHAHANDASHTI S F, SAFAVI-NAINI R. Threshold attribute-based signatures and their application to anonymous credential systems[A]. Progress in Cryptology-AFRICACRYPT 2009[C]. Gammarth, Tunisia, 2009. 198-216.

[8] MAJI H K, PRABHAKARAN M, ROSULEK M. Attribute-based signatures[A]. Topics in Cryptology-CT-RSA 2011[C]. San Francisco, CA, USA, 2011. 376-392.

[9] LI J, AU M H, SUSILO W, *et al*. Attribute-based signature and its applications[A]. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security[C]. Beijing, China, 2010. 60-69.

[10] KHADER D. Attribute based group signatures[EB/OL]. https://eprint.iacr.org/2007/159.pdf.

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

[12] ATENIESE G, CHOU D H, MEDEIROS B D, *et al*. Sanitizable signatures[A]. Computer Security-ESORICS 2005[C]. Milan, Italy, 2005. 159-177.

[13] ATENIESE G, MEDEIROS B. On the key exposure problem in chameleon hashes[A]. 4th International Conference[C]. Amalfi, Italy, 2004. 165-179.

[14] YUEN T H, SUSILO W, LIU J K, *et al*. Sanitizable signatures revisited[A]. 7th International Conference[C]. Hong-Kong, China, 2008. 80-97.

[15] AGRAWAL S, KUMAR S, SHAREEF A, *et al*. Sanitizable signatures with strong transparency in the standard model[A]. 5th International Conference[C]. Beijing, China, 2009. 93-107.

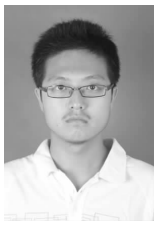
[16] CANARD S, JAMBERT A, LESCUYER R. Sanitizable signatures with several signers and sanitizers[A]. 5th International Conference on Cryptology in Africa[C]. Ifrance, Morocco, 2012. 35-52.

[17] GONG J, QIAN H, ZHOU Y. Fully-secure and practical sanitizable signatures[A]. 6th International Conference[C]. Shanghai, China, 2010. 300-317.

[18] BRZUSKA C, FISCHLIN M, FREUDENREICH T, *et al*. Security of sanitizable signatures revisited[A]. 12th International Conference on Practice and Theory in Public Key Cryptography[C]. Irvine, CA, USA, 2009. 317-336.

[19] IZU T, KUNIHIRO N, OHTA K, *et al*. A sanitizable signature scheme with aggregation[A]. Third International Conference[C]. Hong Kong, China, 2007. 51-64.

作者简介：



刘西蒙（1988-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为公钥密码学与信息安全。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学计算机学院院长、教授、博士生导师，主要研究方向为密码学、计算机网络与信息安全。

熊金波（1981-），男，湖南益阳人，西安电子科技大学博士生，福建师范大学讲师，主要研究方向为访问控制技术与结构化文档安全。

马骏（1981-），男，河北安国人，西安电子科技大学博士生，主要研究方向为无线网络安全。

李琦（1989-），男，江苏淮安人，西安电子科技大学博士生，主要研究方向为基于属性的密码学与访问控制技术。