云计算环境下基于属性的可净化签名方案

刘西蒙*① 马建峰② 熊金波② 贺 拓① 李 琦②
①(西安电子科技大学通信工程学院 西安 710071)
②(西安电子科技大学计算机学院 西安 710071)

摘 要：基于属性的签名近年来由于云计算的大规模应用而备受关注。为了有效保护云计算环境下数据中的敏感信息，该文将可净化的思想引入基于属性的签名中，提出云计算环境下基于属性的可净化签名的方案。该方案中的签名者可以指定净化者对已经签名的文件进行改动，使之隐私部分不再呈现，可以有效解决云端数据中敏感信息隐藏与签名者隐私性的问题。方案在标准模型下证明基于属性的可净化签名方案是不可伪造的。分析表明，所提方案可以解决云计算环境下数据的敏感信息隐藏问题。

关键词：云计算；属性；访问控制；签名；可净化；标准模型
中图分类号：TP393; TP309 **文献标识码**：A **文章编号**：1009-5896(2014)07-1749-06
DOI: 10.3724/SP.J.1146.2013.01154

Attribute Based Sanitizable Signature Scheme in Cloud Computing

Liu Xi-meng① Ma Jian-feng② Xiong Jin-bo② He Tuo② Li Qi②
①(*School of Telecommunications Engineering, Xidian University, Xi'an* 710071, *China*)
②(*School of Computer Science and Technology, Xidian University, Xi'an* 710071, *China*)

Abstract: Attribute signature attracts much attention due to the large-scale applications of cloud computing. Sensitive information in the document needs to be hidden in cloud computing environment, and Attribute Based Sanitizable Signature (ABSS) scheme in cloud computing environment is proposed to solve this issue. The ABSS scheme brings the character of sanitizable into Attribute Based Signature (ABS) in order to hide sensitive information, ensure signer's anonymity and achieve fine-grained access control. The ABSS scheme constructed in this paper is proved to be unforged in the standard model. Analysis shows that the proposed ABSS scheme is more appropriate for cloud computing environment to hide the sensitive information of the data.

Key words: Cloud computing; Attribute; Access control; Signature; Sanitizable; Standard model

1 引言

云计算是一种前沿的计算模式，其具有强大的存储与计算能力，并可以有效地减少工业界对于基础设施的建设，成为学术界以及工业界的关注的焦点[1]。尽管云计算对于工业界有极大的推动作用，但是其面临很多关键性技术问题，安全问题首当其冲。首要的安全问题为保证云存储服务器上数据的完整性，数据拥有者的隐私性以及保证数据敏感信息隐藏。但在云存储环境中，云终端用户需要将数据提交给云服务提供商进行存储，但云服务提供商通常是一个商业公司，并不完全可信。由于数据对于任何组织来说都是重要的资产，将数据中的敏感信息暴露在不可信的环境下对任何组织来说都是不利的。并且云环境下，也需要保护数据拥有者身份的隐私性。因此，如何有效地保证数据的完整性，同时保证数据拥有者身份的隐私性，隐藏数据中敏感信息变成了关键的问题。

近年来由于云计算的发展，基于属性的密码学(Attribute Based Cryptography, ABC)受到了学术界与工业界的广受关注，其保证数据机密性，并为数据提供细粒度的访问控制。基于属性的加密(Attribute-Based Encryption, ABE)[2,3]作为模糊身份加密(Fuzzy Identity Based Encryption, FIBE)[4]的一个重要应用，最早源于基于身份的加密[5]，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]给出了一种基于属性集合分等级的加密方案以实现用户可以灵活可扩展地将数据安全外包给云服务器进行存储。文献[7]利用多授权中心的基于属性加密方案加密个

2013-07-31 收到，2014-02-14 改回
长江学者和创新团队发展计划项目(IRT1078)，国家自然科学基金(U1135002, 61370078)，国家科技部重大专项(2011ZX03005-002)和中央高校基本科研业务费项目(JY10000903001)资助课题
*通信作者：刘西蒙 snbnix@gmail.com

人健康病历(Personal Health Record, PHR)，并将其外包给云服务器进行存储，实现对 PHR 进行细粒度，可伸缩的访问控制。相对于基于属性的加密方案，基于属性签名(Attribute Based Signature, ABS)[8]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在的场景选择使用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。对应与 FIBE 方案，ABS 最早源于文献[9]中的模糊身份签名(FIBS)方案。文献[9]首次构造并提出 FIBS 方案。由于在 FIBS 方案中，签名者不能控制其隐私，并且为了支持小规模属性集与大规模属性集，文献[10]提出了一种支持小规模属性集与大规模属性集的门限属性签名方案。为了在 ABS 方案中实现签名的强不可伪造性，文献[11]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。文献[12]提出了一种用灵活门限谓词构造的一种新的 ABS 方案，可以有效地压缩开销签名大小与减小验证时间，更适用实际应用。由于现有签名长度是随着属性的增长而增长的，文献[13]给出了一种固定签名长度的基于属性的签名方案，有效地解决了这个问题。文献[14]利用门限谓词同样给出了两种固定签名长度的基于属性的签名方案。为了减少现有 ABS 运行签名算法时的开销，文献[15]给出了一种基于属性签名的安全外包方案，可以将用户端的计算开销外包给云服务器从而减小了用户端的签名时候的开销。文献[16]给出了一种前向安全基于属性的加密，有效地解决了密钥泄漏的问题。

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，该方法称之为“净化”。 文献[17]利用变色龙哈希函数[18]，在不可否认签名[19]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，并且产生对于修改后文件的一个有效的签名，并且该过程不需要与原始签名者进行多次交互，依然可以保证数字签名的有效性。透明性是净化签名方案[17, 19]的一个性质，文献[20]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[21]给出了一种多签名者与多净化者的方案来代替现有单签名者与单净化者的方案。文献[22]给出了一种基于属性的可净化签名方案，但是该文献并没有给出应用场景下的系统模型，并没有对文献中所提方案进行效率分析。本文提出了一种在云环境下的基于属性的可净化签名(Attribute Based Sanitizable Signatures, ABSS)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。文中给出了基于属性加密的系统级与算法级方案，该方案非常适用于云计算环境中。

2 云计算系统框架与安全模型

2.1 系统框架

本文提出的机制中包括 5 个参与方： 数据提供者(签名者)，数据净化者，可信授权中心，云存储服务器和云端用户。

系统模型如图 1 所示。系统描述如下：在系统中，数据提供者与数据净化者都需要从可信授权中心获得系统公开参数与私钥。当数据需要上传到云端服务器进行保存时，下载者下载好云端数据时需要对数据进行完整性验证。由于基于属性的净化签名可以保证数据提供者身份的隐私性与对敏感信息的隐藏，因此需要用基于属性的净化签名对数据进行签名。数据提供者签名后将数据连同其对应的签名上传至云存储服务器。当数据中有敏感信息需要进行隐藏时，净化者从数据提供者获得数据并验证数据的完整性，对消息中敏感信息的比特位改动后，不需要与原始的数据提供者进行多次的交互，对改动后的数据进行基于属性的净化签名，并上传到云端服务器。当云端用户需要下载该数据时，需要对该数据的真实性与完整性进行验证，通过使用公开参数与属性集合，对数据进行完整性验证。当一个新的云端用户加入系统时，授权中心针对用户的私钥申请请求，对用户所提交的属性集合生成密钥。如果云端用户私钥中的属性集合满足签名中的门限谓词结构时，则可以对数据的完整性与真实性进行验证。

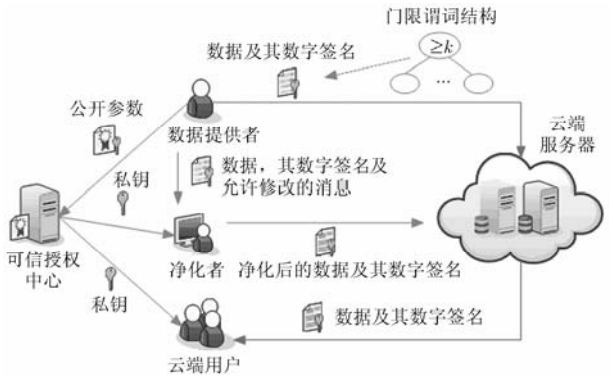

图 1 系统模型

2.2 安全模型

不可区分性游戏与不变性游戏与文献[20]类似，本文不再赘述。文中所使用的不可伪造性游戏与文献[23]类似，在此仅仅给出定义 1。

定义 1　如果不存在 t 时间的敌手进行多项式 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，那么称基于属性的净化签名是 (t,q_e,q_S,ϵ)-安全的。

3　方案构造

3.1 算法级

本小节给出了 ABSS 的具体构造。ABSS 包含 5 个算法：系统建立，密钥生成算法，签名算法，净化算法，验证算法。相比于文献[23]方案，本文运用 g_2h_i 代替文献[23]中所用的函数 $T(i)$，在 4.4 节可以看出本文方案能有效减小验证时的计算开销。构造 ABSS 所需要的双线性对，灵活谓词访问结构，拉格朗日插值法，以及证明需要的计算性 Diffie-Hellman(CDH) 问题在文献[23]中有详细介绍。

系统建立：算法输入为全体属性集 U，属性集合中的所有元素都在 Z_p 中。该算法选择 $d-1$ 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 $A=e(g_1,g_2)$。随机地从 $\mathbb{G}$ 中选择元素 $t_1,t_2,\cdots,t_{n+1}$，并且令 $N=\{1,2,\cdots,n+1\}$。从 $\mathbb{G}$ 中随机选出一个长为 $n+d-1$ 的向量 $\boldsymbol{H}=(h_1,h_2,\cdots,h_{n+d-1})$，并随机从 $\mathbb{G}$ 中选择随机向量 $\boldsymbol{U}=(u_1,u_2,\cdots,u_n)$。

算法输出公开参数：　$PK=(\mathbb{G},\mathbb{G}_T,e,g,g_1,g_2,\boldsymbol{U},\boldsymbol{H},A)$，主密钥为 $\mathrm{MSK}=\alpha$。

密钥生成算法：该算法可以生成一个与属性集 ω 相关联的私钥。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 $d_{i0}=g_2^{q(i)}\cdot(g_2h_i)^{r_i}$ 和 $d_{i1}=g^{r_i}$。最终，将 $D_i=(d_{i0},d_{i1})_{i\in\hat{\omega}}$ 输出作为与属性 ω 相关的私钥。

签名算法：该算法输入公开参数，签名者的私钥，消息 m，谓词 $\Upsilon_{m,\omega^*}(\cdot)$ 与净化者的属性集 ω_b。为了用谓词 $\Upsilon_{k,\omega^*}(\cdot)$ 对消息 m 进行签名，算法从子集合 $\omega'\subseteq\omega\bigcap\omega^*$ 中选择 k 个元素，算法执行过程如下：

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

(2)算法计算

$$\sigma_0=\left[\prod_{i\in\omega_a^{'}\cup\Omega_a^{'}}d_{i0}^{\Delta_{i,S}(0)}\right]\left[\prod_{i\in\omega_a^{*}\cup\Omega_a^{'\prime}}(g_2h_i)^{r_i^{'}}\right]\cdot\left[\prod_{i\in\omega_b^{*}\cup\Omega_b^{'}}(g_2h_i)^{r_i^{''}}\right]\left(u'\prod_{j=1}^{k}u_j^{m_j}\right)^{r_s}$$

$$\{\sigma_{ai}=d_{i1}^{\Delta_{i,S}(0)}g^{r_i'}\}_{i\in\omega_a'\cup\Omega_a'},\ \{\sigma_{ai}=g^{r_i'}\}_{i\in\omega_a^*/\Omega_a'}$$

$$\{\sigma_{bi}=g^{r_i'}\}_{i\in\omega_b^*\cup\Omega_b'},\ \sigma_m=g^{r_s}$$

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

净化算法：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合法。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

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

$$\sigma_0'=\sigma_0\left[\prod_{i\in\omega_a^{*}\cup\Omega_a^{'\prime}}(g_2h_i)^{\tilde{r}_i'}\right]\left[\prod_{i\in\omega_b^{*}\cup\Omega_b^{'}}(g_2h_i)^{\tilde{r}_i''}\right]\cdot\frac{\prod_{i\in I_1}u_i^r}{\prod_{i\in I_2}u_i^r}\left(u'\prod_{i\in\mathcal{M}}u_i^{m_i'}\right)^{\tilde{r}_s}$$

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

验证算法：为了验证签名的正确性，需要验证等式：

$$e(g,\sigma_0)\Big/\left\{\left[\prod_{i\in\omega_a^{*}\cup\Omega_a'}e(g_2h_i,\sigma_{ai})\right]\left[\prod_{i\in\omega_b^{*}\cup\Omega_b^{'}}e(g_2h_i,\sigma_{bi})\right]\cdot e\left(u'\prod_{j=1}^{k}u_j^{m_j},\sigma_m\right)\right\}=A$$

验证算法不仅适用于净化消息，而且适用于非净化消息。

3.2 系统级

文献[24]给出了云计算下基于密文策略的权重属性加密的系统模型。与此对应，本文给出的系统级方案主要关注于：(1)系统初始化；(2)新文件生成；(3)文件中敏感信息的隐藏；(4)新用户产生；(5)用户撤销；(6)文件访问；(7)文件删除。这些操作调用都是基于属性净化签名的算法级的方案。

(1)系统初始化　数据提供者选择一个安全参数并且调用系统建立算法，输出系统公共参数和系

统主密钥。数据提供者对每一个元素进行签名，然后将系统公共参数和系统主密钥连同签名一起发送给可信授权中心。可信授权中心通过了验证签名，则利用数据提供者所提交的公共参数和系统主密钥为系统新用户分发密钥。

(2)新文件生成　数据拥有者创建一个文件后，为文件定义一个门限谓词结构，调用签名算法对新文件进行签名，新文件连同签名被加密后上传到云端服务器。

(3)文件中敏感信息的隐藏　当文件中有敏感信息需要隐藏时，数据拥有者将数据文件与对应的签名消息与需要修改的消息交给净化者。数据净化者通过调用净化签名算法，不需要与数据拥有者交互多次，对数据文件中敏感信息进行隐藏并产生与其对应的签名。当敏感信息隐藏后，数据净化者将修改后的数据文件连同签名一同上传至云端服务器存储。

(4)新用户产生　当一个用户加入系统的时候，用户对其所拥有的属性集合提交给可信授权中心。可信授权中心将用户所对应的属性集合作为密钥产生算法的输入，用于产生新用户的私钥。可信授权中心将这个私钥发送给新用户。

(5)文件验证与访问　首先用户选择将云端的数据文件与其对应的签名下至本地。首先通过解密获得文件与其签名。云端用户调用签名验证算法对数据文件的完整性进行验证。如果云端用户的属性集满足密文的门限谓词策略，那么可以通过完整性验证，说明文件确实是由数据的拥有者产生或者经过净化者修改的。

(6)用户撤销　一旦用户被撤销，系统要保证被撤销的用户不能再访问云服务器的数据文件，并且要保证未被撤销的用户不受影响。为了使撤销用户无需周期性地更新密钥，本文使用文献[25]提出的一种CP-ABE的密钥更新思路，即可信授权中心给每一个用户的属性一个终止日期，签名中附带时间信息，验证时要求云端用户的属性满足签名消息中的门限谓词，且终止日期在签名附带的时间之后。如用户不满足上面的任意一条，则无法正确验证数据文件的信息。

(7)文件删除　文件删除操作只能由数据提供者发起，数据提供者提供要删除文件与其签名，云存储服务器验证签名，如果通过验证则删除文件。

4　方案分析

本节首先对基于属性的可净化签名进行安全性分析，然后对所提方案进行性能分析。

4.1 不可伪造性

定理 1　本文提出的净化签名是 (t,q_e,q_S,ϵ) 在 (t',ϵ')-CDH 问题下是不可伪造的，当

$$\epsilon' \ge \epsilon \Big/ \left(4\binom{d-1}{d-k}(n_m+1)(q_e+q_S)\right)$$

$$t' = t + O\big((d(q_e+q_S)+n_m q_S)t_m + d(q_e+q_S)t_e\big)$$

其中，t_m 与 t_e 分别为群 $\mathbb{G}$ 中乘法运算与指数运算的时间。

证明方法与概率分析方法与文献[23]中给出的方法类似，不再赘述。

4.2 不可区分性

由于消息 m 相关的正确签名 σ_s 与消息 m_1 相关净化签名 σ_1' 是同分布的。同理，净化者对消息 m_2 产生净化签名 σ_2' 与 σ_s 同分布。因此可以得出，相对于 m_1 净化签名 σ_1' 与相对于 m_2 净化签名 σ_2' 是同分布的。

4.3 不变性

我们需要介绍引理 1 用来证明定理 2，用定理 2 说明不变性。

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 bit 数据。那么存在一个多项式时间算法 $\mathcal{A}$ 以优势 $\epsilon_a \ge \epsilon_b$ 进行不可伪造游戏，其中消息长度为 $n-m$。

引理 1 的详细证明见文献[20]。

定理 2　本文提出的基于属性的净化签名在 ϵ'-CDH 假设下是 ϵ-不变的，其中，存在一个整数 l，使得 $\epsilon \le l\epsilon'$。

证明　我们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，赢得不可伪造游戏在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，我们知道赢得不变性游戏在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。

4.4 性能分析

在本节中，运用基于对的密码学库(Pairing-Based Cryptography library, PBC library)来测试本文所提方案。仿真中，测试机的配置为频率运行在2.4 GHz的Inter Pentium双核CPU, 6 GB内存，5400转速320 GB硬盘。运行在测试机的操作系统为64位的Ubuntu 12.04 LTS。本文使用PBC库中的Type A对测试方案，其中，Type A对在160 bit的椭圆曲线群上构造基于512 bit有限域上的超奇异曲线 $y^2 = x^3 + x$。在测试机上，首先测试基本的密码学运算的开销。计算双线性对的开销大约为1.389

ms，在$\mathbb{G}$与$\mathbb{G}_T$中指数运算的时间大约为1.994 ms与0.187 ms。在$\mathbb{G}$与$\mathbb{G}_T$中乘法运算时间大约为0.005 ms与0.002 ms。上述所有的运算都运行10000次取均值。运用g_2h_i代替文献[23]中所用的函数$T(i)$。当计算g_2h_i时，本文仅需1次$\mathbb{G}$中的乘法时间，而文献[23]中计算1次$T(i)$需要$\mathbb{G}$中的多次指数运算，随着原始签名者与净化签名者属性变多时候，运算$T(i)$将极大地增加验证所需开销。通过分析本文方案可以得出，签名的长度是随着原始签名者与净化签名者属性的增加而线性增长的。验证所需的时间也与原始签名与净化签名中的属性线性相关。我们在测试机上测试验证者验证签名所需要的时间和原始签名者与净化签名者属性数量之间的关系。在测试中，取$k=20$，原始签名与净化签名中的属性数目分别为0到50。那么测试结果如图2所示。测试结果与我们分析的结果一致。

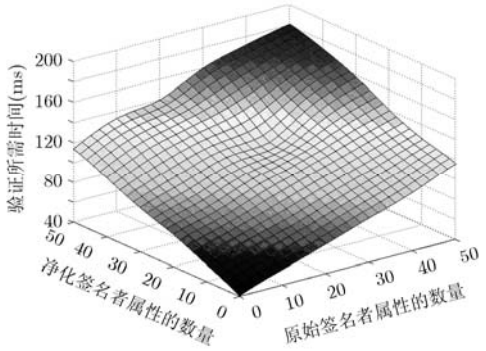

图2 验证所需时间

5 结论

本文提出了一种云计算环境下基于属性的可净化签名，并给出了系统级以及算法级方案。方案保证用户匿名性的同时，有效地解决了对敏感信息隐藏的问题。文中给出了系统框架与算法的安全模型，给出了算法的详细构造，并对基于属性的可净化签名的安全性进行了详细的分析。性能分析表明，基于属性的可净化方案可以有效地解决云环境中敏感信息隐藏的问题。

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] Goyal V, Pandey O, Sahai A, *et al.*. Attribute-based encryption for fine-grained access control of encrypted data[C]. Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 2006: 89–98.

[3] 王海斌, 陈少真. 隐藏访问结构的基于属性加密方案[J]. 电子与信息学报, 2012, 34(2): 457–461.
Wang Hai-bin and Chen Shao-zhen. Attribute-based encryption with hidden access structures[J]. *Journal of Electronics & Information Technology*, 2012, 34(2): 457–461.

[4] Sahai A and Waters B. Fuzzy identity-based encryption[C]. Advances in Cryptology - EUROCRYPT 2005, Aarhus, Denmark, 2005: 557.

[5] Boneh D and Franklin M. Identity-based encryption from the Weil pairing[C]. Advances in Cryptology - CRYPTO 2001, Santa Barbara, California, USA, 2001: 213–229.

[6] Wan Z, Liu J, and Deng R H. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing[J]. *IEEE Transactions on Information Forensics and Security,* 2012, 7(2): 743–754.

[7] Li M, Yu S, Zheng Y, *et al.*. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption[J]. *IEEE Transactions on Parallel and Distributed Systems,* 2013, 24(1): 131–143.

[8] Guo S and Zeng Y. Attribute-based signature scheme[C]. International Conference on Information Security and Assurance, Hanwha Resort Haeundae, Busan, Korea, 2008: 509–511.

[9] Yang P, Cao Z, and Dong X. Fuzzy identity based signature[EB/OL]. IACR Cryptology ePrint Archive, 2008, 2008: 002. http://eprint.iacr.org/2008/002.

[10] Shahandashti S F and Safavi-naini R. Threshold attribute-based signatures and their application to anonymous credential systems[C]. Progress in Cryptology – AFRICACRYPT 2009, Gammarth, Tunisia, 2009: 198–216.

[11] Maji H K, Prabhakaran M, and Rosulek M. Attribute-based signatures[C]. Topics in Cryptology – CT-RSA 2011, San Francisco, CA, USA, 2011: 376–392.

[12] Li J, Au M H, Susilo W, *et al.*. Attribute-based signature and its applications[C]. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, 2010: 60–69.

[13] Ge A J, Ma C G, and Zhang Z F. Attribute-based signature scheme with constant size signature in the standard model[J]. *IET Information Security*, 2012, 6(2): 47–54.

[14] Herranz J, Laguillaumie F, Libert B, *et al.*. Short attribute-based signatures for threshold predicates[C]. Topics in Cryptology–CT-RSA 2012. San Francisco, CA, USA, 2012: 51–67.

[15] Li J, Chen X, Li J, *et al.*. Secure outsourced attribute-based signatures[EB/OL]. IACR Cryptology ePrint Archive, 2012, 2012: 605. http://eprint.iacr.org/2008/002.

[16] Yuen T H, Liu J K, Huang X, *et al.*. Forward secure attribute-based signatures[C]. International Conference on

Information and Communications Security, Hong Kong, 2012: 167–177.

[17] Ateniese G, Chou D H, De Medeiros B, *et al*.. Sanitizable signatures[C]. 10th European Symposium on Research in Computer Security, Milan, Italy, 2005: 159–177.

[18] Ateniese G and De Medeiros B. On the key exposure problem in chameleon hashes[C]. 4th International Conference on Security in Communication Networks, Milan, Italy, 2004: 165–179.

[19] Yuen T H, Susilo W, Liu J K, *et al*.. Sanitizable signatures revisited[C]. 7th International Conference on Cryptology and Network Security, Hong Kong, 2008: 80–97.

[20] Agrawal S, Kumar S, Shareef A, *et al*.. Sanitizable signatures with strong transparency in the standard model[C]. 5th International Conference on Security and Cryptology, Beijing, China, 2009: 93–107.

[21] Canard S, Jambert A, and Lescuyer R. Sanitizable signatures with several signers and sanitizers[C]. 5th International Conference on Cryptology in Africa, Ifrane, Morocco, 2012: 35–52.

[22] Brzuska C, Fischlin M, Freudenreich T, *et al*.. Security of sanitizable signatures revisited[C]. 12th International Conference on Practice and Theory in Public Key Cryptography, Orange County, California, USA, 2009: 317–336.

[23] 刘西蒙, 马建峰, 熊金波, 等. 基于属性的可净化签名方案[J]. 通信学报, 2013, (Z1): 148–155.
Liu Xi-meng, Ma Jian-feng, Xiong Jin-bo, *et al*.. Attribute based sanitizable signature scheme[J]. *Journal on Communications*, 2013, (Z1): 148–155.

[24] 刘西蒙, 马建峰, 熊金波, 等. 云计算环境下基于密文策略的权重属性加密方案[J]. 四川大学学报(工程科学版), 2013, 45(6): 21–26.
Liu Xi-meng, Ma Jian-feng, Xiong Jin-bo, *et al*.. Ciphertext-policy weighted attribute based encryption scheme in cloud computing[J]. *Journal of Sichuan University: Engineering Science Edition*, 2013, 45(6): 21–26.

[25] Bethencourt J, Sahai A, and Waters B. Ciphertext-policy attribute-based encryption[C]. IEEE Symposium on Security and Privacy, Oakland, California, USA, 2007: 321–334.

刘西蒙： 男，1988 年生，博士生，研究方向为基于属性的密码学、大数据环境下的隐私保护.

马建峰： 男，1963 年生，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： 男，1981 年生，讲师，研究方向为网络与系统安全.

贺 拓： 男，1986 年生，博士生，研究方向为云计算安全、公钥密码学.

李 琦： 男，1989 年生，博士生，研究方向为基于属性的密码学.