计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190700131

大属性可公开追踪的密文策略属性基加密方案

马潇潇[1]　黄　艳[2]
1 郑州信息科技职业学院　郑州 450046
2 河南省煤田地质局四队　郑州 450016

摘　要　密文策略属性基加密可以灵活实现“一对多”加密，尤其是大属性的属性基加密，可以支持任意的属性全集，因此在云计算、物联网、大数据等领域有广泛应用前景。然而，密文策略属性基加密中同一个解密私钥可以对应多个不同的用户，于是恶意用户敢于共享其(部分)私钥以获取非法利益。针对用户恶意共享解密私钥的问题，为实现公开追踪并验证泄露私钥拥有者身份的目的，文中提出一个支持大属性的可公开追踪的密文策略属性基加密方案，该方案可以支持任意单调的访问结构。并且，除了固定长度的系统公开参数外，不花费额外的存储代价就可以对泄露密钥的用户身份进行公开验证。

关键词：属性基加密；追踪性；公开验证性；大属性；密文策略；云计算
中图法分类号　TP309

Publicly Traceable Accountable Ciphertext Policy Attribute Based Encryption Scheme Supporting Large Universe

MA Xiao-xiao[1] and HUANG Yan[2]
1 Zhengzhou Vocational University of Information and Technology, Zhengzhou 450046, China
2 The Fourth Team, Henan Bureau of Coal Geological Exploration, Zhengzhou 450016, China

Abstract　Ciphertext policy attribute-based encryption can achieve one-to-many encryption flexibly. Especially, the large universe attribute-based encryption can support unbounded attribute universe, and has extensive applications in cloud computing, big data, etc. However, owing to the fact that a private decryption key may correspond to different users, thus malicious users dare to share their decryption privileges to others for profits. To solve this problem and publicly verify the identity of a leaked secret key, this paper proposes an accountable attribute based encryption scheme that supports large universe. The proposed scheme can support LSSS realizable access structures. In addition to the fixed-length system public parameters, the identity of the user who leaks the encryption key can be publicly verified without considering the constant storage cost.

Keywords　Attribute based encryption, Traceability, Public verifiability, Large universe, Ciphertext policy, Cloud computing

1　引言

随着云计算、大数据等新型网络服务的兴起，在分布、开放的计算环境中进行数据共享和数据处理的需求与日俱增，越来越多的公司或个人将数据存放在第三方数据服务机构中或者由第三方进行数据处理。然而，恶意攻击者和不完全可信的第三方数据服务机构的存在，使得安全性问题日益凸显。

2005 年 Sahai 等[1]提出属性基加密的思想，用描述性的属性集合代替用户的身份，用户私钥与属性集(访问结构)相关，由属性集和访问结构之间的匹配关系确定用户的解密能力，从而达到通过灵活的访问结构实现细粒度解密权限控制的目的。而根据访问策略位置的不同，属性基加密分为密钥策略属性基加密(KP-ABE)和密文策略属性基加密(CP-ABE)两类。本文着重考虑 CP-ABE，在 CP-ABE 方案中用户属性集合嵌入在私钥里，发送者选定访问策略并与密文相结合，只有属性集合满足密文的访问策略的用户才能进行解密。

围绕效率、安全性、访问结构等 3 个重要指标，许多属性基加密方案被提出[2-11]。2013 年，Rouselakis 等[12]提出一个支持大属性的属性基加密方案。一般来说，属性基加密可以分为小属性和大属性两类。所谓小属性是指属性全集在系统建立阶段就确立，属性个数是多项式有限的，并且公开参数的长度与属性个数线性正比。而大属性属性基加密中，属性全集在系统建立阶段不需要具体化，属性个数可以无限多。因此大属性的属性基加密更适合于实际应用。

然而，CP-ABE 系统中用户只能访问其属性集合满足的访问结构对应的加密密文，用户之间存在共享各自私钥以获得更大解密权限的动机。加之一个属性集合可能对应多个不同用户，这意味着这些用户具有相同的解密私钥。即使用户的私钥泄露，也很难准确找到哪个用户泄露的私钥。这一缺点使得属性基加密系统从理论走向实际应用的过程中受到了极大的限制，因此有必要对泄露密钥的来源进行追踪。

2008 年，Hinek 等[13]首先提出一个密钥可追踪的系统，

基金项目：国家自然科学基金项目(61602512)；河南省重点研发与推广专项(科技攻关)项目(182102210575，192102310005)；国家开放大学项目(G18A24166Q)
This work was supported by the National Natural Science Foundation of China (61602512), Key Science and Technology Research Projects of Henan Province (182102210575, 192102310005) and National Open University Project(G18A24166Q).
通信作者：马潇潇(mxx1010@126.com)

但该系统要求解密时解密者与第三方机构进行交互。2009年，Li等[14]提出一个可公开验证的可追踪ABE方案，但是该方案仅支持“与门”的访问策略，不适于实际应用。2011年，Katz等[15]提出谓词加密的可追踪性，并给出一个可追踪的内积谓词加密系统，其追踪代价与系统中的用户数量呈线性关系。2013年，Liu等[16]给出一个支持单调访问结构的白盒可追踪CP-ABE系统，但该方案需要维护一个记录用户的列表来实现白盒可追踪。2015年，Ning等[17]提出一个无需维护列表的白盒可追踪CP-ABE系统。

但是，追踪到密钥泄露者身份之后，为了挽回密钥泄露造成的损失，需要追究泄露者的责任。显而易见，泄露者会想方设法否定其恶意行为。用户以及追踪机构产生分歧，追踪机构需要提供给第三方可以公开验证的证据，由第三方权威机构进行仲裁，即实现对恶意用户的责任认定，达到可追踪的公开验证性或者恶意用户的不可抵赖性。文献[16-17]给出的方案虽然支持高表达能力，但是不能满足公开验证性，无法对泄露者进行公开追踪。文献[14]给出的方案可以提供公开验证性，但其仅支持小属性以及“与门”的访问策略，实用性和表达能力不强。

本文为实现泄露密钥拥有者身份的公开验证性，通过对密钥的身份进行签名的方式，提出一个可追踪的大属性的属性基加密方案。该方案的具体优势如下：

(1)支持对泄露私钥拥有者身份的公开验证性，在仅知道系统公开参数的情况下，任何第三方可以公开验证泄露私钥的身份，从而实现对恶意泄露者的身份追踪。

(2)支持大属性的属性基加密，不但支持任意的加密属性全集，而且系统的公开参数与属性个数无关，即公开参数是固定长度的，又由于公开验证只需要知道系统公开参数，因此实现公开验证的存储代价也是固定的，不随属性个数增加。

(3)灵活的访问控制，支持线性秘密共享方案可实现的任意单调的访问结构，实现灵活的一对多的加密。

2 基础知识

2.1 线性秘密共享方案(LSSS)

$P=\{P_1,\cdots,P_k\}$表示参与者的集合，$(\mathbb{A},\rho)$表示一个访问结构，其中$\mathbb{A}$表示ℓ行k列的矩阵，ρ表示$\{1,2,\cdots,\ell\}$到$P=\{P_1,\cdots,P_k\}\oplus$的映射。$\mathbb{Z}_p$上的线性秘密共享方案由以下两个算法组成。

(1)秘密共享算法：假设$s\in\mathbb{Z}_p$为共享的秘密值，随机选取$(v_2,\cdots,v_k)\in_R\mathbb{Z}_p^*$，构造向量$\vec{v}=(s,v_2,\cdots,v_n)$，则$\rho(i)$分享的子秘密值为$\lambda_i=A_i\cdot\vec{v}$，其中$A_i$表示矩阵$\mathbb{A}$第$i$行对应的向量。

(2)秘密重构算法：对于任一授权集S，令$I=\{i:\rho(i)\in S\}$，那么存在多项式时间算法计算得到系数$\{w_i\in\mathbb{Z}_p\}_{i\in I}$，使得$\sum_{i\in I}w_iA_i=(1,0,\cdots,0)$成立，然后恢复秘密值$s=\sum_{i\in I}w_iA_i\cdot\vec{v}=\sum_{i\in I}w_i\lambda_i$。对于非授权集，上述系数不存在，但存在多项式时间算法计算得到向量$\vec{w}=(w_1,\cdots,w_k)\in\mathbb{Z}_p^k$使得$w_1=-1$，并且$A_i\cdot\vec{w}=\sum_{i\in I}w_iA_i=(0,0,\cdots,0)$，$i\in I$。

2.2 双线性对

假设$\mathbb{G}$，$\mathbb{G}_T$是p阶乘法循环群，其中是p大素数，g是群$\mathbb{G}$的一个生成元。那么$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$为双线性映射，如果$e$满足以下3条性质：

(1)双线性：对于任意的$a,b\in\mathbb{Z}_p$，都有$e(g^a,g^b)=e(g^b,g^a)=e(g,g)^{ab}$。

(2)非退化性：如果$e(g^a,g^b)=1$当且仅当$ab=0(\mathrm{mod}\ p)$。

(3)有效性：对任意$P,Q\in\mathbb{G}$，存在多项式时间算法有效计算$e(p,Q)$。

$(e,\mathbb{G},\mathbb{G}_T,g)$称为双线性对，本文方案的不可伪造性基于双线性群$(e,\mathbb{G},\mathbb{G}_T,g)$中的弱计算性Diffie-Hellman难题(w-CDHP)，即给定$(g,g^a,g^b,v^b)\in\mathbb{G}^4$，其中$v\in_R\mathbb{G}^*$，$a,b\in_R\mathbb{Z}_p^*$，计算$g^{ab}$的值。

3 大属性可追踪的属性基加密

3.1 算法组成

大属性可追踪的属性基加密由以下算法组成。

系统建立算法：输入安全参数λ，输出系统主密钥MSK和公开参数PP。

密钥生成算法：输入身份ID、加密属性集S、主密钥MSK、系统公开参数PP，输出解密私钥$SK_{ID,S}$。

加密算法：输入系统公开参数PP、加密访问结构$\mathbb{A}$、消息M，输出相应的密文CT。

解密算法：输入系统公开参数PP、私钥$SK_{ID,S}$、密文CT，输出原始消息M或者解密失败符号$\perp$。

公开验证算法：输入系统公开参数PP、私钥$SK_{ID,S}$，输出无效符号$\perp$，或者身份ID。

3.2 安全模型

大属性可追踪的属性基加密安全性主要考虑两个方面：密文的机密性以及泄露私钥拥有者身份的公开验证性。其中后者来源于私钥的不可伪造性。

(1)机密性

密文策略的属性基加密的适应性选择密文攻击的安全模型，可以由敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间的一系列游戏来刻画：

承诺：敌手$\mathcal{A}$选择一个加密属性集合S^*用来生成挑战密文，将S^*发送给挑战者。

系统建立：挑战者$\mathcal{C}$运行系统初始化算法，得到主密钥MSK和系统公开参数PP，并秘密保存主密钥MSK，将公开参数PP发送给$\mathcal{A}$。

询问阶段1：$\mathcal{A}$可以进行多项式次数的适应性私钥提取询问和解密询问，$\mathcal{C}$进行回答。

1)私钥提取询问：敌手任意选择身份ID'、加密属性集S'，$\mathcal{C}$输出私钥$SK_{ID',S'}$。

2)解密询问：敌手任意选择访问结构$\mathbb{A}'$、密文CT'，$\mathcal{C}$输出CT'对应的明文消息M'。

挑战阶段：$\mathcal{A}$向提交$\mathcal{C}$两个等长的消息(M_0,M_1)以及相应的访问结构$\mathbb{A}^*$，其中要求已经执行私钥提取询问的加密属性集合S'都不能满足访问结构$\mathbb{A}^*$。随机选择$\beta\in\{0,1\}$，对访问结构$\mathbb{A}^*$、消息M_β加密，将挑战密文CT'发送给敌手。

询问阶段2：$\mathcal{A}$继续执行多项式次数的适应性私钥提取询问和解密询问，但是不能对满足访问结构$\mathbb{A}^*$的任意加密属性集合S'执行私钥提取询问，不能对CT^*执行解密询问。

猜测：最后，$\mathcal{A}$输出对随机比特$\beta\in\{0,1\}$的猜测值β'。

如果敌手给出了正确的猜测值，即$\beta'=\beta$，称$\mathcal{A}$赢得了游

戏。进一步,敌手的优势定义为 $Adv(\mathscr{A})=|\Pr[\beta'=\beta]-1/2|$。

(2)可追踪性

泄露私钥拥有者身份的可追踪性(即身份的公开验证性)是基于密钥的不可伪造性。而适应性选择消息存在性不可伪造的安全模型,可以由敌手 $\mathscr{A}$ 和挑战者 $\mathscr{C}$ 之间的一系列游戏来刻画:

系统建立:$\mathscr{C}$ 运行系统初始化算法,得到主密钥 MSK 和系统公开参数 PP,并秘密保存主密钥 MSK,将公开参数 PP 发送给敌手。

询问阶段 1:$\mathscr{A}$ 可以进行多项式次数的适应性私钥提取询问,敌手任意选择身份 ID'、加密属性集 S',挑战者输出解密私钥 $SK_{ID',S'}$。

伪造阶段:$\mathscr{A}$ 输出加密属性集 S^*、身份 ID^*、私钥 SK_{ID^*,S^*},其中要求不能对 S^*、ID^* 执行私钥提取询问。如果 SK_{ID^*,S^*} 正确,则 $\mathscr{A}$ 赢得游戏。

$\mathscr{A}$ 赢得游戏的优势定义为 $Adv(\mathscr{A})=\Pr[\mathscr{A}\ wins]$。

4 具体方案

基于 Rouselakis 等[11]的支持属性基加密方案,通过对密钥拥有者的身份进行短签名,本文给出一个大属性的可公开追踪的属性基加密方案,记为 LAABE。

系统建立:设 $(\mathbb{G},\mathbb{G}_T)$ 都是阶为素数 p 的乘法群,g 为 $\mathbb{G}$ 的一个生成元,$\varepsilon:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 是一个双线性映射,$H:\{0,1\}^*\to\mathbb{Z}_p^*$ 是一个抗碰撞的 Hash 函数;随机选取 g_1, u, h, w, $v\in_R\mathbb{G}$, $\alpha\in_R\mathbb{Z}_p^*$,令系统主密钥 $MSK=g_1^\alpha$,系统公开参数 $PP=(\mathbb{G},\mathbb{G}_T,g,e,g_1,u,h,w,v,e(g_1,g)^\alpha,H)$。

密钥生成:给定用户的身份 ID 及其加密属性集为 $S=\{A_1,\cdots,A_k\}\subset\mathbb{Z}_p$,随机选取 $r,r_1,\cdots,r_k\in_R\mathbb{Z}_p^*$,计算 $L=g^r$, $K=g_1^\alpha w^r$, $K_{i,0}=g^{r_i}$, $K_{i,1}=g^{r_i}$, $K_{i,2}=(u^{A_i}h)^{r_i}v^{-r}$, $\forall A_i\in S$, $h=H(L,ID)$,用户的私钥 $SK_{ID,S}=(L,K,\{K_{i,0},K_{i,1},K_{i,2}\}_{i=1,\cdots,k})$。

加密:给定消息 $M\in\mathbb{M}$、访问结构 $(\mathbb{W},\rho)$,其中 $\mathbb{X}$ 为 ℓ 规模的矩阵,首先随机选取向量 $\vec{v}=(s,y_2,\cdots,y_l)\in(\mathbb{Z}_p^*)^l$,然后生成 $\{\lambda_{\rho(i)}=\vec{v}\cdot W_i:i\in[l]\}$,其中 W_i 为 $\mathbb{W}$ 的第 i 行。对于任意的 $i\in[l]$,随机选取 $t_1,\cdots,t_l\in\mathbb{Z}_p^*$,计算:

$C=M\cdot e(g,g_1)^\alpha$, $C'=g^s$

$C_{i,1}=w^{\lambda(i)}v^{t_i}$, $C_{i,2}=(u^{A_{\rho(i)}}h)^{-t_i}$, $C_{i,3}=g^{t_i}$

输出密文 $CT_{\mathbb{W}}=(C,C',\{C_{i,1},C_{i,2},C_{i,3}\}_{i=1,\cdots,l})$。

解密:给定密文 $CT_{\mathbb{W}}=(C,C',\{C_{i,1},C_{i,2},C_{i,3}\}_{i=1,\cdots,l})$,如果 A 符合解密访问结构 $(\mathbb{W},\rho)$,令 $I=\{i:A_{\rho(i)}\in A,i\in\{1,\cdots,l\}\}$,通过秘密重构算法得到 $\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$ 使得 $\sum_{i\in I}\omega_iW_i=(1,0,\cdots,0)$,其中 W_i 为 $\mathbb{W}$ 的第 i 行,然后计算:

$$M=C\left(\frac{(\prod_{i\in I}e(C_{i,1},L)e(C_{i,2},K_{\rho(i),1})e(C_{i,3},K_{\rho(i),2}))^{w_i}}{e(C',K)}\right)^{\frac{1}{h}}$$

$h=H(L,ID)$

公开验证:一个正确的私钥 $SK_{ID,S}=(L,K,\{K_{i,0},K_{i,1},K_{i,2}\}_{i=1,\cdots,k})$ 满足以下等式:

$e(K,g)=e(g,g_1)^{\alpha h}e(w,L)$, $h=H(L,ID)$

$e(K_{i,1},L)=e(K_{i,0},g)$, $\forall A_i\in S$

$e(K_{i,2},L)=e(g,v)e(K_{i,0},u^{A_i}h)$, $\forall A_i\in S$

由于私钥拥有者可能只分享部分解密权限,即只泄露部分私钥,其可以对私钥进行部分修改,因此在公开验证泄露密钥拥有者身份时,不用对任意的 $A_i\in S$ 都成立,只需验证存在性即可。

$e(K,g)=e(g,g_1)^{\alpha h}e(w,L)$, $h=H(L,ID)$

$e(K_{i,1},L)=e(K_{i,0},g)$

$e(K_{i,2},L)=e(g,v)e(K_{i,0},u^{A_i}h)$, $\exists A_i\in S$

正确性:

$$M=C\left(\frac{(\prod_{i\in I}e(C_{i,1},L)e(C_{i,2},K_{\rho(i),1})e(C_{i,3},K_{\rho(i),2}))^{w_i}}{e(C',K)}\right)^{\frac{1}{h}}$$

$$=M\cdot e(g,g_1)^{\alpha s}\left(\frac{(\prod_{i\in I}e(w^{\lambda(i)}v^{t_i},g^r)e((u^{A_{\rho(i)}}h)^{-t_i},g^{r_{\rho(i)}})e(g^{t_i},(u^{A_{\rho(i)}}h)^{r_{\rho(i)}}v^{-r}))^{w_i}}{e(g^s,g_1^{\alpha h}w^r)}\right)^{\frac{1}{h}}=M$$

5 效能分析

5.1 安全证明

定理 1 在 w-CDHP 困难的假设下,LAABE 方案中的私钥在随机预言模型下满足适应性选择消息的存在性不可伪造。

证明:假设 g^b,g^c,v^b,其中 $v\in_R\mathbb{G}^*$, $b,c\in_R\mathbb{Z}_p^*$,这是一个 w-CDHP 实例,$\mathscr{C}$ 进行如下攻击游戏模拟。

系统建立:挑战者 $\mathscr{C}$ 令 $g_1=g^b$, $w=g^c$,其他参数按照系统初始化算法正常选取。则公开参数 $PP=(\mathbb{G},\mathbb{G}_T,g,e,g_1,u,h,w,v,e(g_1,g^c),H)$,其中隐式定义 $MSK=g^{bc}$,挑战者也不知道 MSK 的具体值,最后将公开参数 PP 发送给敌手。

询问阶段 1:$\mathscr{C}$ 如下回答敌手 $\mathscr{A}$ 的 Hash 询问、适应性私钥提取询问:

1)Hash 询问:对于 L,ID Hash 的私钥提取询问,$\mathscr{C}$ 随机选取 $h\in_R\mathbb{Z}_p^*$,返回 h。

2)私钥提取询问:对于 $ID,S=\{A_1,\cdots,A_k\}\subset\mathbb{Z}_p^*$ 的私钥提取询问,$\mathscr{C}$ 随机选取 $r,r_1,\cdots,r_k\in_R\mathbb{Z}_p^*$,计算 $L=g^r(g^b)^{-h}$, $K=g^{ar}$, $K_{i,0}=g^{r_i}(g^b)^{-r_i}h$, $K_{i,1}=g^{r_i}$, $K_{i,2}=(u^{A_i}h)^{r_i}(v^b)^{h-r}$, $\forall A_i\in S$,其中 h_i 来自于 Hash 询问,返回私钥 $SK_{ID,S}$。可以验证这样生成的私钥是正确的:

$e(g_1,g^b)^he(w,L)=e(g_1,g^b)^he(g^c,g^r(g^b)^{-h})=e(K,g)$

$e(K_{i,1},L)=e(K_{i,0},g)$, $\forall A_i\in S$

$e(K_{i,2},L)=e(g,v)e(K_{i,0},u^{A_i}h)$, $\forall A_i\in S$

伪造阶段:根据分叉引理[18-19],如果存在适应性选择消息攻击者 $\mathscr{A}$ 以不可忽略的概率 ε 伪造合法的签名,那么挑战者 $\mathscr{C}$ 可以产生两个合法的签名 $ID,L,K,\{K_{i,0},K_{i,1},K_{i,2}\}_{i=1,\cdots,k},h_1$ 和 $ID,L,K',\{K_{i,0},K_{i,1},K_{i,2}\}_{i=1,\cdots,k},h_2$。其中 $h_1\neq h_2$,满足:

$e(K,g)=e(g^c,g_1)^{h_1}e(w,L)$, $h_1=H(L,ID)$

$e(K,g)=e(g^c,g_1)^{h_2}e(w,L)$, $h_2=H(L,ID)$

那么有:

$e(K(K')^{-1},g)e(g_1^{ch_2-ch_1},g)=1$

$\Rightarrow K(K')^{-1}g_1^{ch_2-ch_1}=\mathcal{O}$

$\Rightarrow g^{bc}=(K^{-1}(K'))^{h_1-h_2}$

这意味着可以求解 w-CDHP 难题。

定理 2 在判定 q-PBDHE 困难的假设下,LAABE 方案

满足在选择属性集模型下是 IND-CCA2 安全的。

LAABE 方案的机密性基于 Rouselakis 等[12]提出的属性基加密方案。为了实现密钥拥有者身份的公开验证性，LAABE 方案在 Rouselakis 等[12]的属性基加密方案上进行了一些适应性改变。改变之一是密文中 $C=M\cdot e(g,g)^{as}$ 用 $C=M\cdot e(g_1,g)^{as}$ 代替，其中 $g,g_1\in_R\mathbb{G}$，这对 IND-CCA2 的证明没有影响；改变之二是在密钥部分 $K=g^{ah}w^r$ 用 $K=g_1^{ah}w^r$ 代替，其中 $h=H(L,ID)$，这对 IND-CCA2 的证明没有影响。因此，可以类似地用 Rouselakis 等[12]的方法证明方案的 IND-CCA2 安全。

5.2 效率分析

本节对已有的白盒可追踪的属性基加密[16-17]、可公开追踪属性基加密[14]与本文提出的 LAABE 方案进行了比较。从表 1 可以看出 LAABE 方案可以同时实现白盒可追踪和公开验证性，并且与唯一可以提供公开追踪性的方案[14]相比，本文提出的 LAABE 方案不但可以支持 LSSS 可实现的任意单调访问结构，而且实现公开验证性时仅需要系统公开参数，不增加额外的存储代价，而且由于可以支持大属性，公开参数的长度是固定的，因此只需要固定的存储就可以实现公开验证性。

表 1 特征比较

Table 1 Features comparison

方案	公开追踪性	访问结构	大属性
文献[13]	√	AND	×
文献[15]	×	LSSS	×
文献[16]	×	LSSS	√
LAABE	√	LSSS	√

结束语 密文策略属性基加密中，由于一个解密私钥对应多个用户，因此恶意用户敢于共享其私钥以获取非法利益。为解决此问题并追究共享者的责任，本文提出一个大属性可追踪的密文策略属性基加密方案。与 Rouselakis 等[12]的属性基加密相比，其加密和解密的计算代价未增加，并且不用花费额外的存储代价，就可以实现私钥拥有者身份的公开验证。最后，LAABE 方案中的私钥在随机预言模型下满足适应性选择消息的存在性不可伪造，满足在选择属性集标准模型下是 IND-CCA2 安全的。

参 考 文 献

[1] SAHAI A, WATERS B. Fuzzy identity based encryption[C]// Advances in Cryptology-EUROCRYPT 2005. LNCS 3494, Springer-Verlag, 2005: 457-473.

[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. ACM, 2006: 89-98.

[3] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]// Public Key Cryptography-PKC 2011. Springer Berlin Heidelberg, 2011: 53-70.

[4] WANG H B, CHEN S Z. Attribute-based encryption with hidden access structures[J]. Journal of Electronics & Information Technology, 2012, 2: 35.

[5] SHEN X L, LYU Y N. Research on file hierarchy attribute encryption of hidden access structure[J]. Application Research of Computers, 2019, 36(1): 239-242.

[6] LEWKO A, WATERS B. New proof methods for attribute-based encryption: achieving full security through selective techniques[C]// Advances in Cryptology-CRYPTO 2012. Springer-Verlag, 2012: 180-198.

[7] HOHENBERGER S, WATERS B. Online/offline attribute-based encryption[C]// Public-Key Cryptography-PKC 2014. Springer, Berlin, Heidelberg, 2014: 293-310.

[8] LI S B, WANG X R, FU J M, et al. User Key Revocation Method for Multi-cloud Service Providers[J]. JEIT, 2015, 37(9): 2225-2231.

[9] HORVAÁTH M. Attribute-Based Encryption Optimized for Cloud Computing[C]// SOFSEM: Theory and Practice of Computer Science. Springer, Berlin Heidelberg, 2015: 566-577.

[10] QIN B, DENG H, WU Q, et al. Flexible attribute-based encryption applicable to secure e-healthcare records[J]. International Journal of Information Security, 2015(14): 1-13.

[11] ZHOU Z, HUANG D, WANG Z. Efficient Privacy-Preserving Ciphertext-Policy Attribute Based- Encryption and Broadcast Encryption[J]. IEEE Transactions on Computers, 2015, 64(1): 126-138.

[12] ROUSELAKIS Y, WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption [C]// Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security. ACM, 2013: 463-474.

[13] HINEK M J, JIANG S, SAFAVI-NAINI R, et al. Attribute-Based Encryption with Key Cloning Protection[OL]. https://xueshu. baidu. com/usercenter/paper/show? paperid = 46da1dd6833c3a8e6091f3de341d3c46&site=xueshu_se.

[14] LI J, REN K, KIM K. A2BE: Accountable attribute-based encryption for abuse free access control[OL]. https://xueshu. baidu. com/usercenter/paper/show? paperid = febe03db8d8b1a290e65a82cb06b2c05&site=xueshu_se.

[15] KATZ J, SCHRODER D. Tracing insider attacks in the context of predicate encryption schemes[OL]. https:// www. usukita. org/node/ 1779.

[16] LIU Z, CAO Z, WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 76-88.

[17] NING J, DONG X, CAO Z, et al. White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1274-1288.

[18] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signature[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[19] TANG Y L, ZHOU J, LIU K, et al. Lattice-Based Identity-Based Blind Signature Scheme in Standard Model[J]. Journal of Frontiers of Computer Science & Technology, 2017, 3: 29.

MA Xiao-xiao, born in 1984, Ph.D, lecturer. Her main research interests include image processing and information security.