支持敏感属性保护的ABS-OSBE协议

张 斌 李冬辉 熊厚仁 费晓飞
(解放军信息工程大学 郑州 450001)

摘 要 针对基于属性访问控制模型中敏感属性容易泄露的问题,提出了基于属性签名的无记忆签名信封(ABS-OSBE)协议。ABS-OSBE协议使用基于属性的签名机制,给出属性协商双方交互信息时所使用的参数计算方法,以确保只有满足属性访问树结构的用户才能通过计算,从而获得敏感属性。通过扩展属性的描述方式,验签者定义的属性访问树结构能支持描述"非"关系。给出了"非"关系的匹配规则,最后证明了ABS-OSBE协议的安全性。

关键词 敏感属性,ABS,OSBE,访问树
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.2.026

ABS-OSBE Protocol Supporting Sensitive Attributes Protection

ZHANG Bin LI Dong-hui XIONG Hou-ren FEI Xiao-fei
(PLA Information Engineering University, Zhengzhou 450001, China)

Abstract In order to protect the sensitive attribute in attribute-based access control, an ABS-based OSBE protocol was put forward. ABS-OSBE protocol integrates the ABS algorithm into OSBE, and provides the computational method to both attribute negotiated sides for exchanging information, ensuring the users that meet the access tree structure can obtain sensitive attributes. By extending the description of attributes, the access tree structure can exactly describe "NOT" threshold. A matching method of "NOT" threshold was proposed. Finally, the security of ABS-OSBE protocol was demonstrated.

Keywords Sensitive attributes, ABS, OSBE, Access tree

1 引言

属性信息是属性访问控制模型(ABAC)的授权依据,如何防止敏感属性信息的泄露[1]成为近年来研究的一个热点。自动信任协商[2]通过规范敏感信息的交换,已成为防止敏感信息泄露的重要手段。OSBE[3]是信任协商系统中信息保护及防止敏感信息泄露的典型技术,具有以下优点:(1)提供一种使用签名防止信息泄露的框架,能够支持不同的应用场景,采用不同的签名方案;(2)与签名算法有相同的安全级别;(3)网络传输开销少,协商效率高。以上特点使得OSBE得到广泛研究。

针对ABAC中敏感属性信息的保护问题,文献[4,5]深入研究了隐藏证书技术,并对访问控制模型进行了扩展,用于对敏感属性信息的保护,隐藏证书技术中的属性协商过程需要进行4次信息交互。文献[6]提出的基于RSA算法的OSBE协议只需进行两次信息交互就能防止敏感信息的泄露,但基于PKI的公钥密码体制存在公私钥的管理负担比较重的问题。

在ABS[7,8]算法中,验签者通过规定一个属性访问树结构,当且仅当签名方的属性信息满足此访问树所规定的属性信息时,签名方签名成功。ABS具有公私钥管理成本低、不用暴露用户具体身份信息且与ABAC模型一样以属性信息为依据等特点。文献[9,10]提出的ABS算法能灵活地支持属性访问树中的"与"关系和"或"关系,但不支持"非"关系的描述。

针对现有研究在解决敏感属性信息泄露时存在协商效率低、密钥管理成本高等问题,本文提出基于ABS的OSBE协议。该协议利用属性拥有方发送的签名信息时,对请求的属性信息进行加密,仅当属性请求方具有的属性信息满足属性发送方规定的属性访问树结构,拥有正确的签名信息时,才能通过计算得到密钥,进而解密获得所请求的属性信息。同时,通过使用属性类型和属性值共同描述属性信息,使ABS中的访问树支持"非"关系的描述,扩展了访问树结构的描述方式。

2 基于扩展访问树的ABS签名

在基于属性的签名体制中,用户从属性中心获得一组属性私钥并利用该属性私钥进行签名。用户能否签名成功由其所拥有的属性集合决定,若属性集合能够满足访问结构,用户签名成功,否则签名失败。属性访问树结构是访问结构中的一个主要发展方向[8],扩展访问树结构并丰富访问树对属性关系的描述是ABS签名研究的一个热点。因此,通过扩展属性信息的描述方法,可扩展属性访问树结构的描述范围。

到稿日期:2014-03-10 返修日期:2014-07-04 本文受河南省基础研究计划项目(142300413201)资助。
张 斌(1969-),男,博士,教授,主要研究方向为网络信息安全,E-mail:dhlee999@126.com;李冬辉(1988-),男,硕士生,主要研究方向为网络访问控制;熊厚仁(1986-),男,博士生,主要研究方向为授权管理与访问控制;费晓飞(1977-),男,博士,主要研究方向为SOA安全。

2.1 访问树的扩展

使用单一属性值描述属性的方式，所定义的属性访问树结构准确地描述了“与”关系和“或”关系[9,10]，但在描述“非”关系时易造成混淆。例如，对于访问树中“不是经理”这一“非”关系，满足此“非”关系的用户符合访问树规则，某用户的属性集是(硕士，工程师)，用户的属性集与访问树进行匹配时，由于硕士不等于经理，工程师不等于经理，得出的结论是用户符合访问树中“非”关系的定义。而此访问树中“非”关系的实际意义是“用户的职位不是经理”，从“非”关系的实际意义可知用户的属性集并不一定能满足。因此，根据单一属性值描述属性的匹配和“非”关系的实际意义上得出的结论不一致。需要通过扩展属性信息的描述方法，将原来的单一属性值描述方法扩展为由属性类型和属性值共同描述，使属性访问树结构能支持“非”关系。

设 T 为一个访问树，树中的非叶子节点代表由其阈值所描述的门限，叶子节点代表属性信息。设(w_x，Num_x | $0\leqslant w_x\leqslant Num_x$)分别表示节点 x 的阈值和子节点的数目，($Att\_t(T)$，$Att\_v(T)$)表示叶子节点中的属性类型集和属性值集。属性类型 $att\_t(T)$($att\_t(T)\in Att\_t(T)$)和属性值 $att\_v(T)$($att\_v(T)\in Att\_v(T)$)分别表示某类具体属性信息的统称和主体(客体或环境)的某种属性类型的具体值。

图 1 是一个包含“或”关系、“与”关系和“非”关系的访问树结构示例，当 $w_x=1$ 时，表示“或”关系，当 $w_x=Num_x$ 时，表示“与”关系，当 $w_x=0$ 时，表示“非”关系。

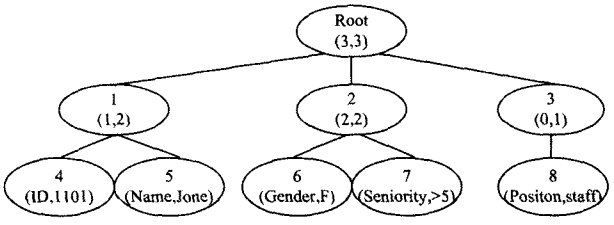

图 1 访问树结构示例

设 T_x 表示根为 x 的子树，用户 s 的属性集{$Att(s)$ | ($Att\_t(s)$，$Att\_v(s)$)}中的某属性满足 T_x 时，返回 $T_x(s)=1$，否则返回 $T_x(s)=0$。文献[9]给出了属性访问树中“或”关系和“与”关系的匹配方法，但不支持表示“非”关系，本文对此加以扩展，使访问树可表示“非”关系。属性访问树中出现“非”关系时，应遵循如下的匹配规则：

$$\left.\begin{array}{l}(att\_t(T)=att\_t(s))\wedge\\(att\_v(T)\neq att\_v(s))\end{array}\right\}\Rightarrow T_x(s)=1$$

$$\left.\begin{array}{l}(att\_t(T)=att\_t(s))\wedge\\(att\_v(T)=att\_v(s))\end{array}\right\}\Rightarrow T_x(s)=0$$

$$(att\_t(T)\neq att\_t(s))\Rightarrow T_x(s)=0$$

其中，($att\_t(T)$，$att\_v(T)$)表示属性访问树“非”关系中的一个属性的属性类型和属性值，($att\_t(s)$，$att\_v(s)$)是用户某个属性的属性类型和属性值。

图 1 中，“非”关系的含义可表示为“Position”不是“staff”，与之匹配的主体属性必须满足拥有“Position”这个属性类型，且属性值不为“staff”，此时与该“非”关系匹配成功；否则，不满足此“非”关系。

2.2 “非”关系的优势分析

某一属性的属性类型表示为 att_t，其属性类型对应的属性值集合表示为(att_v_1，att_v_2，…，att_v_n，att_v_{n+1}，…，att_v_{n+k})($k\geqslant 1$)，属性访问树的描述语义为用户属性的属性类型是 att_t，其属性值只需满足(att_v_1，att_v_2，…，att_v_n)中的任意一个，用户能够满足此属性访问树的定义。访问树结构中的“或”关系、“非 att”表示方法与本文提出的“非”关系表示分别如图 2(a)、(b)、(c)所示。

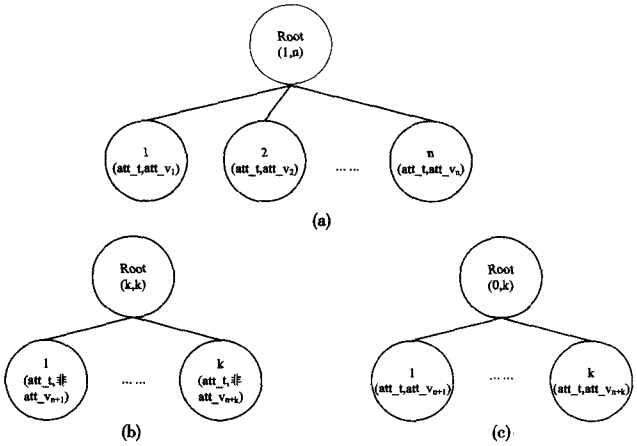

图 2 同一语义的 3 种表示方式

判断某用户属性($att\_t(s)$，$att\_v(s)$)是否满足该访问结构，假设访问树中每个节点匹配成功的概率是 α，匹配失败的概率为 β，且 $\alpha+\beta=1$。

其中图 2(a)采用“或”关系表示方式，其访问树结构是单调的。图 2(b)采用“非 att”的表示方法所构建的访问树，其语义与图 2(a)中访问树所描述的一样，将“非 att”作为一个新的属性添加到属性访问树结构的表示中，其访问结构是非单调的。属性访问树所表示的属性集合数量会增加一倍，降低整个签名系统的效率[11]。因此，在属性访问树的构造中通常不考虑这种情况。图 2(c)采用“非”关系表达方式，且不增加访问结构所表示的属性集合数量，表示“非”关系，其描述的语义与图 2(a)、图 2(b)相同。

用户的某一属性与属性访问树匹配次数的概率如表 1 所列。

表 1 访问树匹配次数概率表

匹配次数	1	2	3	…	n−1	n
概率	α	$\alpha\cdot\beta$	$\beta^2\cdot\alpha$	…	$\beta^{n-2}\cdot\alpha$	β^{n-1}

通过计算可得，用户属性与图 2(a)中所示访问树的匹配次数的期望为：$E_1=\alpha+2\alpha\beta+\cdots+(n-1)\alpha\beta^{n-2}+n\beta^{n-1}$($n$ 为自然数)，用户属性与访问树中的属性匹配成功，用户属性满足访问树，匹配结束。

同理可得，用户属性与图 2(c)所示访问树的匹配次数期望为：$E_2=\alpha+2\alpha\beta+\cdots+(k-1)\alpha\beta^{k-2}+k\beta^{k-1}$($k$ 为自然数)，利用提出的“非”关系匹配规则，用户属性与访问树中的属性匹配成功，则用户属性不能够满足访问树，匹配结束。

当 $n>k$ 时，$E_1-E_2=k\alpha\beta^{k-1}+\cdots+n\beta^{n-1}-k\beta^{k-1}$，由于当 $x>1$ 时，函数 $f(x)=x\beta^{x-1}$ 是单调递增的，因此 $n\beta^{n-1}-k\beta^{k-1}>0$，$E_1-E_2>0$，此时，使用提出的“非”关系结构能够提高访问树的匹配效率。当 $n<k$ 时，使用“或”关系比“非”关系的访问树结构节点少。

因此，根据实际请情况灵活地选用一种表达方式，以提高属性签名算法的效率。

2.3 基于属性签名算法(ABS)

基于属性的签名主要包括系统建立、密钥生成、签名生成等3个阶段。本文采用文献[11]提出的ABS签名算法。

(1)系统建立

选择双线性对 $e:G_1\times G_2\rightarrow G(G_1,G_2$ 和 G 是阶为 p 的乘法循环群)和 G_1、G_2 的生成元 $g_1\in G_1$、$g_2\in G_2$;选择一个公开的Hash函数 $H:\{0,1\}^*\rightarrow\mathbb{Z}_p^*$;定义属性空间 $A=\{1,2,\cdots n\}$,对于任意的 $i\in A$,随机选择 $k_i\in\mathbb{Z}_p^*$,$l\in\mathbb{Z}_p^*$,计算 $L=g_2^l$。

生成系统的主私钥:$MK=(\{k_i\}_{i\in A},l)$,公开参数:$PK=(g_1,g_2,e,H,\{P_i=L^{1/k_i}\}_{i\in A},L)$。

(2)密钥生成

(a)生成用户 i 私钥 $KeyGen_{private}(sk_i,\chi_i)$:拥有属性集 χ_i 的主体颁发私钥。对于属性 $j\in\chi_i$,$x_i\in\mathbb{Z}_p^*$,计算 $B_i=g_1^{1/(l+x_i)}$,$T_{i,j}=B_i^{k_j}$。主体 i 的私钥:$SK=(x_i,B_i,\{T_{i,j}\}_{j\in ATT})$。

(b)生成公开参数 $KeyGen_{public}(T)$:客体选择访问树 T,选择 $s\in\mathbb{Z}_p^*$,计算 $Q=L^s$,访问树 T 中的叶子节点集合 χ_T。对于树中的每个非叶子节点 x 设定其多项式 f_x 的次数是 $d_x=q_x-1$。对于根节点 r,有 $f_x(0)=s$,其它节点 $f_x(0)=f_{parent(x)}(index(x))$,通过递归方法构造控制树的多项式。对于每个叶子节点 x,计算 $D_x=P_i^{f_{i'}(0)/k_i}$,i'是叶子节点的属性,访问树的公开参数:$PK=(D_{i'})_{i'\in\chi_T},Q)$。

(3)签名生成

签名者根据生成的私钥和消息 M 随机选择 $a,b\in\mathbb{Z}_p^*$,$R_1=B_i^a$,$R_2=(Lg_2^{x_i})^{1/a}$,$R_3=g_1^a$,$R_4=g_1^b$,$\lambda=H(R_1,R_2,R_4,M)$,计算 $r_b=b+\lambda a$。选择主体的签名属性 $\delta\subseteq\chi_i$,如果属性 δ 是满足访问树结构的属性子集,计算某叶子节点的值为 $e(T_{i,j}^a,D_j)$,则通过递归得到根节点 r 的值为:$F_r=e(B_i^a,L)^s$。签名 $\sigma=(R_1,R_2,R_3,\lambda,r_b,F_r,M,Q,T)$。

3 ABS-OSBE协议

OSBE通过检查用户提交的数字签名是否为指定证书的签名,决定用户是否有权获取信息。在基于属性访问控制模型中,对于主体属性、客体属性和环境属性的调用没有给出相应的保护机制,容易造成敏感属性的泄露。将OSBE引入到属性信息的请求和响应过程中,保证只有拥有正确证书签名的用户才能获得相对应的属性信息。鉴于ABS签名具有公私钥管理成本低、不会暴漏用户具体身份信息且与ABAC模型一样以属性信息为依据等特点,提出基于ABS算法的OSBE协议,并将该协议应用到基于属性访问控制模型中属性信息的调用过程,实现对敏感属性信息的保护。

3.1 ABS-OSBE协议

ABS-OSBE协议包括系统建立、信息交互和解密获得属性信息3个阶段。

(1)系统建立

向主体 S 和客体 O 公布ABS签名算法的所有公开参数,所请求的属性信息 m,两个同阶的安全参数 $t_1,t_2(t_1=t_2=128\text{bit})$。同时给出一个用于生成对称加密密钥的安全的Hash函数 $h':\mathbb{Z}_p\rightarrow\{0,1\}^*$。主体 S 持有ABS签名 $\sigma=(R_1,R_2,R_3,\lambda,r_b,F_r,M,Q,T)$,客体 O 具有属性信息 m。

(2)信息交互

(a)S 给 O 发送 σ',$\sigma'=(\eta,\mu)$,其中,$\eta=(R_1,R_2,R_3,r_b,M,Q,T)$,$\mu=(\phi,\lambda')$,$\phi=F_r^{t'}\bmod p$,$\lambda'=(\lambda+t)\bmod p$,$t,t'\in[1\cdots 2^{t_1}p]$。

(b)当 O 接收到 σ' 时,根据用户发送的消息 σ',通过 $u=[e(R_1,Q)^{t'+\lambda'}e(R_1,Q)^{-h(R_1,R_2,g_1^{r_b}R_3^{-\lambda},M)}]^{t''}\bmod p$ 计算得到密钥参数,$v=F_r^{t''}$,$t''\in[1\cdots 2^{t_2}p]$,利用密钥 $h'(u)$ 对消息 m 进行加密得到密文 $D=E_{h'(u)}(m)$,然后将 (v,D) 发送给 S。

(3)解密获得属性信息 m

当 S 收到 (v,D) 后,得出解密密钥参数 $u'=v^{t+t'}\bmod p$,然后使用 $h'(u')$ 对 D 进行解密获得消息 m。

由于以下推导过程成立:

$$\begin{aligned}u&=[e(R_1,Q)^{t'+\lambda'}e(R_1,Q)^{-h(R_1,R_2,g_1^{r_b}R_3^{-\lambda},M)}]^{t''}\bmod p\\&=[e(R_1,Q)^{t'+(t+\lambda)-h(R_1,R_2,g_1^{r_b}R_3^{-\lambda},M)}]^{t''}\bmod p\\&=\{[e(B_i^a,L^s)]^{t'+(t+\lambda)-h(R_1,R_2,g_1^{r_b}R_3^{-\lambda},M)}\}^{t''}\bmod p\\&=\{[e(B_i^a,L)^s]^{t'+(t+\lambda)-h(R_1,R_2,g_1^{b+\lambda a}g_1^{-\lambda a},M)}\}^{t''}\bmod p\\&=(F_r^{t'+(t+\lambda)-h(R_1,R_2,R_4,M)})^{t''}\bmod p\\&=(F_r^{t'+t})^{t''}\bmod p\\&=(F_r^{t''})^{t'+t}\bmod p\\&=v^{t'+t}\bmod p=u'\end{aligned}$$

因此,拥有正确签名的用户可以通过计算获得密钥参数 u。

3.2 安全性分析

OSBE协议的安全性[13]需要满足匿名性、有效性和语义安全性。ABS-OSBE协议是将扩展访问树结构的ABS算法应用于OSBE协议,同样需要满足以上3个安全性条件。此外,安全的ABS-OSBE协议还应具有抵御截获攻击风险的特性。因此,ABS-OSBE协议的安全性从匿名性、有效性、语义安全性和能否抵御截获攻击4个方面进行分析。

(1)匿名性:信息发送方无法判断信息请求方的身份信息。

对于任意用户 S' 发送 $\sigma'=(\eta',\mu')$,其中 η' 可以与 η 相同,μ' 如下所示:

$$\begin{aligned}\mu'&=(\phi',\lambda'')\\&=\begin{cases}\phi'=F_r'^{t_1'}\bmod p(F_r'\in\mathbb{Z}_p^*,t_1'\in[1\cdots 2^{t_1}p])\\\lambda''=t_2'\bmod p(t_2'\in[1\cdots 2^{t_1}p])\end{cases}\\\mu&=(\phi,\lambda')\\&=\begin{cases}\phi=F_r^{t'}\bmod p(F_r\in\mathbb{Z}_p^*,t'\in[1\cdots 2^{t_1}p])\\\lambda'=(t+\lambda)\bmod p(t\in[1\cdots 2^{t_1}p])\end{cases}\end{aligned}$$

用户 S 发送的信息 μ 与用户 S' 发送的信息 μ' 在分布上无法区分[8],因此对于接受者 O 而言,在不验证签名的情况下无法辨别发送者 S 与 S'。因此,ABS-OSBE协议中信息请求方的身份信息无法被信息发送方获得。

(2)有效性:具有正确签名的用户能够通过计算得到解密密钥 u',获得消息 m。

S 持有正确的签名 $\sigma=(R_1,R_2,R_3,\lambda,r_b,F_r,M,Q,T)$,计算解密密钥 $u'=u=[e(R_1,Q)^{t'+\lambda'}e(R_1,Q)^{-h(R_1,R_2,g_1^{r_b}R_3^{-\lambda},M)}]^{t''}\bmod p=v^{t'+t}\bmod p$。

可知,S 可以通过计算获得密钥解密 u',$D=E_{h'(u)}(m)$,获得属性信息 m。因此,ABS-OSBE协议中具有正确签名的信息请求方能够获得发送方返回的加密信息。

(3)语义安全性：不持有对消息 M 正确签名的用户不能计算出密钥 u。

假设用户 S' 收到 O 发送的消息 (υ, D)，并且根据计算能够获得密钥 $u=[e(R_1,Q)^{t'+\lambda'}e(R_1,Q)^{-h(R_1,R_2,g_1^{r_b}R_3^{-\lambda},M)}]^{t''} \bmod p$。

由 ABS-OSBE 协议的分析可知获得正确的签名就能获得密钥 u，而在基于属性的签名中，获得签名的关键是具有与访问树 T 相匹配的属性信息。由文献[11]针对属性签名的安全性分析可知：S' 要计算出属性签名需要伪造出访问树 T 的 F_r 值，而安全性分析结果表明，不满足访问树结构定义的用户无法伪造出 F_r 值，因此，用户 S' 无法获得正确的签名信息，在获得消息 (υ, D) 后，无法解密获得属性信息。

(4)抵御截获攻击：截获攻击者不能恢复 ABS-OSBE 方案的密钥 u。

非法用户 S' 可以得到 $\sigma'=(\eta,\mu)$ 和 (υ, D)，但是不知道 F_r 和 λ。

根据给出的 $\eta=(R_1,R_2,R_3,r_b,M,Q,T)$ 和 $\mu'=(\phi=F_r' \bmod p, \lambda'=(\lambda+t) \bmod p)$，计算 $u=(F_r'F_r^{\lambda'-\lambda})^{t''} \bmod p$。

S' 知道 $F_r' \bmod p$，λ' 和 $F_r'' \bmod p$，因为 $\lambda=H(R_1,R_2,R_4,M)$，S' 可以计算出 λ，S' 可以获得 $\lambda'-\lambda=t$，计算 $u=(F_r'^{t''}F_r''^{t''}) \bmod p$，$F_r''^{t''} \bmod p$ 可以计算获得，而 $F_r'^{t''} \bmod p$ 在已知 $F_r' \bmod p$ 和 $F_r'' \bmod p$ 的情况下，是一个 CDH 问题[7]，无法计算获得。所以，截获攻击者不能够获得加密的属性信息。

因此，ABS-OSBE 协议能够满足匿名性、有效性、语义安全性的要求，并能有效抵御截获攻击。

3.3 协议的性能分析

本文提出的 ABS-OSBE 协议与文献[4]提出的基于隐藏证书技术的 XACML 访问控制扩展模型中的隐藏证书协议和文献[6]提出的 RSA-OSBE 协议在信息交互次数、算法复杂度和控制灵活性这 3 个方面进行比较。

ABS-OSBE 协议与隐藏证书和 RSA-OSBE 协议三者的性能对比如表 2 所列(其中，z_1 和 z_2 分别为椭圆双曲线算法和对称加密算法的密钥长度，z_1' 为 RSA 签名算法的密钥长度)，在相同的安全强度下，椭圆双曲线算法所需要的密钥长度和系统参数比 RSA 算法要小，并且在私钥的处理速度上，椭圆双曲线的计算量更小，处理速度更快。

表 2 协议的性能分析对比

	信息交互次数	算法复杂度	控制灵活性
隐藏证书	4	$O(z_1 \cdot z_2)$	证书级
RSA-OSBE	2	$O(z_1' + z_2)$	证书级
ABS-OSBE	2	$O(z_1+z_2)$	属性级

隐藏证书技术中的协商过程需要 4 次信息交互过程，而 ABS-OSBE 和 RSA-OSBE 协议是单轮回协议，只需进行 2 次信息交互；文献[4]中提出的隐藏证书的协商协议需要首先利用属性签名算法颁发其证书，然后再对证书和请求的属性信息进行加密，所以其算法复杂度为 $O(z_1 \cdot z_2)$。

RSA-OSBE 协议算法复杂度为 $O(z_1'+z_2)$，其中 z_1' 是 RSA 签名算法的密钥长度，ABS-OSBE 协议的算法复杂度为 $O(z_1+z_2)$。

ABS-OSBE 协议中的签名算法与隐藏证书中的公钥加密算法是基于椭圆双曲线的，RSA-OSBE 协议使用的是 RSA 算法，在相同的安全强度下，$z_1<z_1'$，因此，$O(z_1 \cdot z_2)>O(z_1'+z_2)>O(z_1+z_2)$。

对于用户最终获得敏感属性信息，在隐藏证书中取决于用户是否拥有与策略对应的信任证书，在 RSA-OSBE 协议中取决于用户是否具有正确的证书签名，在 ABS-OSBE 协议中取决于用户属性集中的属性信息能否满足访问树结构，即能否控制到用户的具体属性信息。因此，与隐藏证书和 RSA-OSBE 协议相比，ABS-OSBE 协议可以实现对用户能否获得敏感属性信息进行更灵活的控制。

因此，ABS-OSBE 在信息交互次数、算法复杂度和控制灵活性这 3 个方面性能更好。

结束语 本文提出的基于 ABS 签名的 OSBE 方案，能解决在访问控制过程中敏感属性信息的保护问题。一方面，获得敏感属性信息的属性请求方必须具有某些属性，敏感属性信息发送方根据这些属性建立访问控制树，只有属性请求方的属性信息满足访问树结构，获得正确的签名信息，才能通过计算得到密钥，进而解密获得所请求的属性信息。另一方面，通过扩展属性的描述方式，使访问树结构能够准确描述“非”关系。最后，从匿名性、有效性、语义安全性和能否抵御截获攻击 4 个方面验证了 ABS-OSBE 协议的安全性。

参 考 文 献

[1] 葛维进，胡晓惠. EAEBHCM：一种扩展的基于属性加密的隐藏证书模型[J]. 通信学报，2012，12：85-92

[2] Winsborough W H, seamons K E, Jones V E. Automated trust negotiation[J]. IEEE Computer Society Press, 2012(4): 362-366

[3] 廖振松，金海，李赤松，等. 自动信任协商及其发展趋势[J]. 计算机应用与软件，2006，17(9)：1933-1948

[4] 葛维进，胡晓惠，邓勇. 基于隐藏证书的 XACML 访问控制扩展模型[J]. 计算机应用与软件，2011，28(3)：265-268

[5] Lai J, Deng R H, Li Y. Fully secure cipertext-policy hiding CP-ABE[C]// ISPEC 2011. 2011: 24-39

[6] Yu S C, Ren K, Low W J. Attribute-based on-demand multicast group setup with membership anonymity[J]. Computer Networks, 2010, 54(3): 377-386

[7] 赵春明. 可保护授权隐私性的匿名传输[D]. 西安：西安电子科技大学，2006(9)

[8] Shaniqng G, Yingpei Z. Attribute-based signature scheme[C]// International Conference on Information Security and Assurance(ISA2008). USA: IEEE, 2008: 509-511

[9] 马春光，石岚，汪定. 基于访问树的属性基签名算法[J]. 电子科技大学学报，2013，42(3)：410-414

[10] 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

[11] 陈剑锋. 基于属性签名方案的研究[D]. 广州：中山大学，2010，07

[12] 马春光，石岚，周长利，等. 属性基关系限签名方案及其安全性研究[J]. 电子学报，2013，41(5)：1012-1015

[13] 王继林，陈晓峰，陈德人. 无安全信道的 OSBE 方案[J]. 浙江大学学报，2006，40(4)：590-593