基于属性的多授权中心身份认证方案

唐飞[1,2]，包佳立[1]，黄永洪[2]，黄东[3]，王惠莅[4,5]

（1. 重庆邮电大学计算机科学与技术学院，重庆 400065；2. 重庆邮电大学网络空间安全与信息法学院，重庆 400065；
3. 重庆机电职业技术大学信息工程学院，重庆 402760；4. 中国电子技术标准化研究院信息安全研究中心，北京 100076；
5. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071）

摘 要：针对现有的基于属性的身份认证方案均是基于单授权中心实现的，存在密钥托管问题，即密钥生成中心知道所有用户的私钥，提出了一种基于属性的多授权中心的身份认证方案。所提方案结合分布式密钥生成技术实现用户属性私钥的(t,n)门限生成机制，可以抵抗最多来自 $t-1$ 个授权中心的合谋攻击。利用双线性映射构造了所提方案，分析了所提方案的安全性、计算开销和通信开销，并与同类型方案做比较。最后，以多因子身份认证为例，分析了所提方案在电子凭据应用场景中的可行性。分析结果表明，所提方案具有更优的综合性能。

关键词：身份认证；属性密码；多授权中心；分布式密钥生成

中图分类号：TP309

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021047

Multi-authority attribute-based identification scheme

TANG Fei[1,2], BAO Jiali[1], HUANG Yonghong[2], HUANG Dong[3], WANG Huili[4,5]

1. College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
3. Information Engineering Institute, Chongqing Vocational and Technical University of Mechatronics, Chongqing 402760, China
4. Information Security Research Center, China Electronic Technology Standardization Institute, Beijing 100076, China
5. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

Abstract: Based on the problem that the existing attribute-based identification scheme is all based on one single authority, which has a key escrow problem, that is, the key generation center knows all users' private keys, an multi-authority attribute-based identification scheme was proposed. Distributed key generation technology was integrated to realize the (t,n) threshold generation mechanism of the user's private key, which could resist collusion attacks from at most $t-1$ authorities. Utilizing bilinear mapping, a specific multi-authority attribute-based identification scheme was constructed. The security, computation cost and communication cost of the proposed scheme was analyzed, and it was compared with the same type of schemes. Finally, taking multi-factor identification as an example, the feasibility of the proposed scheme in the application scenario of electronic credentials was analyzed.The result shows that the proposed scheme has better comprehensive performance.

Keywords: identification, attribute-based cryptography, multi-authority, distributed key generation

收稿日期：2020−10−13；**修回日期**：2021−01−05

基金项目：国家重点研发计划基金资助项目（No.2018YFB0803905）；国家自然科学基金资助项目（No.61702067）；重庆市自然科学基金资助项目（No.cstc2017jcyjAX0201, No.cstc2020jcyj-msxmX0343）

Foundation Items: The National Key Research and Development Program of China (No.2018YFB0803905), The National Natural Science Foundation of China (No.61702067), The Natural Science Foundation of Chongqing (No.cstc2017jcyjAX0201, No.cstc2020jcyj-msxmX0343)

1　引言

身份认证技术作为网络空间安全的第一道关口，是网络空间环境确认操作者身份的有效方法，保证了用户与其数字身份的绑定关系。身份认证方案是一种交互过程，使持有私钥的证明者能够向持有相应公钥的验证者证明其合法身份。

身份认证方案的概念由 Fiat 等[1]提出，方案中存在一个可信中心核实用户身份信息并为其生成私钥，用户可以利用该私钥向其他用户证明其身份的真实性。Schnorr[2]方案是经典的身份认证方案之一，其安全性依赖于离散对数的困难性。随后，Guillou 等[3]基于 RSA（Rivest-Shamir-Adleman）问题提出了一种高效的身份认证方案。

为了简化传统公钥基础设施中的证书管理工作，Shamir[4]提出了基于身份的密码方案概念。在基于身份的密码方案中，将实体用户的身份信息作为公钥，并由一个可信的密钥生成中心（KGC, key generation center）生成用户的密钥。Kurosawa 等[5]根据 BB04 签名方案[6]构建了一种基于身份的身份认证方案，并证明了方案在随机预言模型下的安全性。Chin 等[7]提出了一种在标准模型下可证明安全的身份认证方案。Barapatre 等[8]根据基于身份的密钥封装机制提出了一种基于身份的身份认证方案通用框架，并构造了一种具体的认证方案。

在基于身份的密码方案基础上，Sahai 等[9]进一步提出了基于属性的密码方案概念。以属性加密[9]为例，用户的密钥和密文都被标记了一个属性集合，当用户拥有的属性个数超过加密者预设的门限值时，用户可以对密文进行解密。属性密码提供了更加灵活的操作关系，受到了国内外学者的广泛研究，例如基于属性的加密方案[10-11]、基于属性的签名方案[12-15]、基于属性的密钥交换协议[16-17]等。基于属性密码的优良性质，显然可以考虑其在身份认证领域的应用。Anada 等[18]将属性密码推广到身份认证方案中，定义了证明者策略和验证者策略 2 类基于属性的身份认证方案，并基于属性密钥封装机制实现了属性身份认证方案的通用构造，给出了一种具体的实现方案。

在基于属性的密码方案中，也需要一个可信的密钥生成中心来生成用户的私钥。因此，用户需要相信中心不会泄露用户私钥。此外，单个密钥生成中心也面临攻击风险过高和负担过重等问题。事实上，Chase[19]于 2007 年就提出了多授权中心属性加密方案的概念。在他的方案中，用户私钥的生成由多个授权中心共同完成，但方案仍需要一个可信中心对用户身份信息进行统一认证以防多用户的合谋攻击。为了解决这一问题，Lin 等[20]结合分布式密钥生成技术[21]提出了一种不依赖任何可信中心的门限多授权中心属性加密方案。

针对无可信中心环境下的属性身份认证需求问题，在 Anada 等[18]所提出的基于属性的身份认证框架基础上，本文提出多授权中心的属性身份认证方案。本文主要贡献如下。

1) 定义了基于属性的多授权中心身份认证方案的概念，具体包括初始化算法、密钥生成算法和认证协议 3 个部分。与单授权中心属性身份认证的不同之处在于，用户的私钥由 n 个授权中心中的至少 t 个共同完成，且方案最多可以抵抗来自 $t-1$ 个授权中心的合谋攻击，具有较高的安全性。

2) 基于双线性映射构造了一种属性身份认证方案。该方案支持门限谓词策略，即证明者的属性集与验证策略属性集的交集个数至少需要满足预定的门限值。分析了方案在分布式密钥生成环境下的安全性，并从计算开销、通信开销等方面分析了方案的效率。此外，与同类型认证方案的比较结果表明，所提方案具有更优良的综合性能。

3) 以多因子身份认证为例，分析所提方案在电子凭据应用场景中的可行性。以口令、邮箱、生物特征等因子构成用户的属性集，用户获得属性集相关的私钥。在身份认证过程中，验证者指定验证策略属性集，并规定验证者需满足的属性个数门限值，从而实现基于用户多因子的身份认证机制。

2　预备知识

2.1　双线性对

定义 1　令 G 和 G_T 是 2 个阶为大素数 p 的乘法循环群，其中 g 是群 G 的生成元。双线性对 $e: G\times G\to G_T$ 是满足如下性质的映射。

1) 双线性。对于任意 $a,b\in Z_p$，有 $e(g^a,g^b)=e(g,g)^{ab}$。

2) 非退化性。存在 $g^c,g^d\in G$，使 $e(g^c,g^d)\neq 1_{G_T}$，其中 1_{G_T} 代表群 G_T 的单位元。

3) 可计算性。存在有效的算法对任意 $a,b\in Z_p$，可计算 $e(g^a,g^b)$。

2.2 方案定义

基于属性的多授权中心身份认证方案包括 3 种算法或者协议，分别是初始化（Setup）算法、密钥生成（Key-generation）算法和认证协议。其中，初始化算法根据安全参数得到系统公开参数；密钥生成算法根据用户的属性集生成相应的属性密钥；认证协议由证明者 P 和验证者 V 共同完成。基于属性的多授权中心身份认证方案的具体定义如下。

初始化。输入安全参数 λ 和属性全集 U，生成系统公开参数 params。同时，每个授权中心 P_i 根据系统参数 params 进行相应的初始化，得到自己的主密钥 sk_i。

密钥生成。输入系统参数 params 和用户属性集合 I，如果用户有资格获得这些属性，则向至少 t 个授权中心 P_i 请求生成部分密钥，用户在获得至少 t 个部分密钥之后，合成自己的属性密钥集 D_j，其中 $j \in I$。

认证协议。证明者 P 拥有参数 $(\mathrm{params}, I, D_I)$ 作为输入，验证者 V 拥有参数 (params, I^*) 作为输入，其中 I^* 是 V 选择的验证策略属性集。如果 $|I \cap I^*| \geqslant k$，则 P 能正确证明其身份信息，V 输出 1；否则，V 输出 0。其中，k 为策略所规定的门限值。

2.3 安全模型

基于属性的身份认证方案需满足不可仿冒性和匿名性。

1) 不可仿冒性

在不可仿冒性定义中，敌手首先与诚实证明者运行认证协议，随后尝试向第三方仿冒其为一个合法证明者。Anada 等[18]称这类针对属性身份识别方案的攻击为中间人攻击。

初始化阶段。挑战者 C 输入安全参数 λ，运行 Setup 算法得到系统参数 params，并将 params 发送给敌手 A。同时，根据 params 对所有授权中心 $T_1, \cdots, T_n$ 进行初始化。

询问阶段。敌手 A 可以发起如下询问。

① 密钥生成询问。在接收到系统参数 params 后，敌手 A 向挑战者 C 发出属性集合 I 密钥生成请求，C 返回相应属性密钥 D_I。询问密钥生成的属性集合 I 不能满足攻击目标属性集合 I^* 的要求，即 $|I \cap I^*| < k$。

② 交互训练。敌手 A 作为恶意验证者 V* 和诚实证明者 P 交互运行认证协议。

挑战阶段。敌手 A 作为恶意证明者 P* 和任意的诚实验证者 V 进行交互，试图说服验证者接受。

如果任意多项式时间敌手 A 都不能以不可忽略的优势使诚实验证者接受，则称基于属性的多授权中心身份认证方案具有不可仿冒性。

2) 匿名性

基于属性的多授权中心身份认证方案的匿名性表示拥有属性集 I 的证明者在向验证者证明后，除了会泄露 $|I \cap I^*| \geqslant k$ 这一事实外，不会泄露其他任何属性信息。基于属性的多授权中心身份认证方案的匿名性的具体定义如下。

初始化阶段。挑战者 C 输入安全参数 λ，运行 Setup 算法得到系统参数 params，并将 params 发送给敌手 A。同时，根据 params 对所有授权中心 $P_1, \cdots, P_n$ 进行初始化。

询问阶段。敌手 A 可以发起密钥生成询问。在接收到系统参数 params 后，敌手 A 向挑战者 C 发出属性集合 I 密钥生成请求，C 返回相应属性密钥 D_I。

挑战阶段。敌手 A 与挑战者 C 进行如下操作。

① 敌手选择 3 个属性集 (I_0, I_1, I^*)，其中 I_0 和 I_1 表示 2 个证明者身份属性集，I^* 表示用于挑战的验证策略属性集，且 $|I_0 \cap I^*| \geqslant k$，$|I_1 \cap I^*| \geqslant k$。

② 挑战者运行密钥生成算法生成密钥 D_{I_0} 和 D_{I_1}，并将 2 个私钥发送给敌手。

③ 挑战者随机选择 $b \in \{0,1\}$，并充当证明者 P 使用私钥 D_{I_b} 与敌手交互运行认证协议。

④ 最后，敌手输出猜测值 b'，如果 $b' = b$，则表示敌手猜测成功。

本文将上述游戏中敌手的成功优势定义为 $|\Pr[b' = b] - 1/2|$。如果任意多项式时间敌手 A 都不能以不可忽略的优势区分证明者 P 用的是私钥 D_{I_0} 还是 D_{I_1}，则称基于属性的多授权中心身份认证方案具有匿名性。

3 具体方案

本文方案主要借鉴了 Li 等[22]的属性签名方案。Li 等[22]构造了一种支持门限谓词的中心化属性签名方案。为了实现无可信中心环境下的用户属性密钥生成，本文采用分布式密钥生成（DKG, distributed

key generation）技术[21]。分布式密钥生成技术是门限密码系统的主要组成部分，主要通过多方参与的形式来计算共享的公钥和私钥集，不需要依赖任何可信第三方，其核心思想是(t,n)门限秘密共享。秘密共享用于在一组参与者中共享一个秘密，每个参与者都有关于秘密的部分信息。门限秘密共享意味着n个参与者之间的至少t个参与就可以重建秘密值。在 DKG 协议中，参与者共同选择并生成一个随机秘密共享值s。每个参与者P_i选择一个随机共享值s_i，然后至少t个参与者参与就可以恢复出秘密共享值s，并公开值$y=g^s$。本文将系统的主密钥当成秘密共享值s，只要有t个参与者就可以重建主密钥，同时在系统中公开系统主公钥$y=g^s$。

由阈值门组成所有谓词γ。具体地，支持阈值k为 $1\sim d^2$ 的所有谓词$\gamma_{k,I^*}(\cdot)\to 0/1$，其中$\gamma_{k,I^*}=\begin{cases}1, & \left|I'\cap I^*\right|\geqslant k\\ 0, & \text{其他}\end{cases}$。

回顾关于拉格朗日插值的知识，给定$d-1$次多项式上的d个点$q(1),\cdots,q(d)$，则可以利用拉格朗日插值公式来计算$q(i)$，其中$i\in Z_p$。设S为d元素集，在$q(i)$的计算中，将$q(j)$的拉格朗日系数$\Delta_{j,S}(i)$定义为

$$\Delta_{j,S}(i)=\prod_{\eta\in S,\eta\neq j}\frac{i-\eta}{j-\eta}$$

3.1　详细过程

本节将描述基于属性的多授权中心身份认证方案，该方案由以下 3 个阶段组成。

初始化（Setup），系统初始化阶段。

1) 根据安全参数λ生成素数阶p。选择 2 个阶为素数p的乘法循环群G和G_T，g是群G的生成元，双线性映射$e:G\times G\to G_T$。定义属性全集为U，默认属性集A中有$a-1$个属性元素。选取哈希函数为$H:\{0,1\}^*\to G$。系统公共参数为

$$\text{params}=\{p,g,G,G_T,H,U,A,a,k,n,t\}$$

其中，属性门限值为$k\in[1,a]$，n为授权中心的个数，t为用户属性密钥生成的门限值。

2) 生成系统主密钥。

Step1　P_i选择一个$t-1$阶的多项式

$$f_i(x)=c_{i0}+c_{i1}x+\cdots+c_{i(t-1)}x^{t-1}\tag{1}$$

然后，P_i分别计算并广播$C_{ik}=g^{c_{ik}}\pmod p$，其中$k=0,\cdots,t-1$。接着P_i计算秘密值$y_{ij}=f_i(P_j)$，其中$j=1,\cdots,n$，并将其发送给P_j，其中$j\neq i$。

Step2　P_j验证等式$g^{y_{ij}}=\prod_{k=0}^{t-1}(C_{ik})^{P_j^k}$是否成立，如果成立，则认为$P_i$为诚实的中心；否则，$P_j$要求$P_i$重新广播$y_{ij}$。

Step3　由此，可以得到系统的主密钥

$$s=\sum_{i=1}^{n}c_{i0}=\sum_{i=1}^{n}\sum_{j\in S}f_i(j)\Delta_{j,S}(0)\tag{2}$$

其中，S表示参与密钥生成的t个中心。从而得到系统主公钥$y=g^s$。

3) 系统中的所有授权中心根据系统参数共同生成参数$g_2\in G$。

Step1　P_i选择一个$n-1$阶的多项式

$$h_i(x)=b_{i0}+b_{i1}x+\cdots+b_{i(n-1)}x^{n-1}\tag{3}$$

然后，P_i分别计算并广播$B_{ik}=g^{b_{ik}}\pmod p$，其中$k=0,\cdots,n-1$。接着P_i计算秘密值$t_{ij}=h_i(P_j)$，其中$j=1,\cdots,n$，并将其发送给P_j，其中$i\neq j$。

Step2　P_j验证等式$g^{t_{ij}}=\prod_{k=0}^{n-1}(B_{ik})^{P_j^k}$是否成立，如果成立，则认为$P_i$为诚实的中心；否则，要求$P_i$重新广播$t_{ij}$。

Step3　经过上面的交互，每个授权中心都可以计算参数

$$g_2=\prod_{i=1}^{n}B_{i0}=g^{b_{10}+\cdots+b_{n0}}\tag{4}$$

然后，生成参数$Z=e(y,g_2)$。

4) 公开系统参数$\text{params}=\{p,g,g_1,Z,G,G_T,H,U,A,a,k,n,t\}$，其中，属性门限值$k\in[1,a]$，$n$为授权中心的个数。

密钥生成（Key-generation），为属性$i\in I$生成相应的属性私钥D_i。

1) 生成一个新的属性集$\hat{I}=I\cup A$。对于每个$j\in\hat{I}$，P_i选择一个随机值$r_{ij}\in Z_p$，并计算

$$d_{j1}^{(i)}=g^{r_{ij}}\tag{5}$$

$$d_{j0}^{(i)}=g_2^{f_i(j)\Delta_{i,S}(j)}H(j)^{r_{ij}}\tag{6}$$

并将$d_{j0}^{(i)}$和$d_{j1}^{(i)}$安全地发送给用户。

2) 用户收到t个中心发来的部分密钥后，计算自己的属性私钥

$$d_{j0}=\prod_{i=1}^{t}d_{j0}^{(i)}=g_2^{\sum_{i=1}^{t}f_i(j)\Delta_{i,S}(j)}H(j)^{\sum_{i=1}^{t}r_{ij}} \tag{7}$$

$$d_{j1}=\prod_{i=1}^{t}g^{r_{ij}}=g^{\sum_{i=1}^{t}r_{ij}} \tag{8}$$

由此得到每个属性 $j\in\hat{I}$ 的私钥 $D_j=(d_{j0},d_{j1})$。

认证协议。为了完成身份认证过程，即证明用户拥有验证策略属性集 I^* 中的至少 k 个属性。首先，用户选择一个含有 k 个属性的属性子集 $I'\subseteq I\cap I^*$，并进行以下操作。

1) 用户选择一个默认属性子集 $A'\subseteq A$，其中 $|A'|=a-k$ 并且选择 $m+a-k$ 个随机值 $r_i'\in Z_p$，其中 $i\in I^*\cup A'$，并随机选择 $x\in Z_p$，计算

$$\{\sigma_i=d_{i1}^{\Delta_{i,S}(0)}g^{r_i'}\}_{i\in I'\cup A'} \tag{9}$$

$$\{\sigma_i=g^{r_i'}\}_{I^*/I'} \tag{10}$$

$$\sigma_0'=g^x \tag{11}$$

然后，将 (σ_i,σ_0') 发送给验证者。

2) 验证者随机选择 $c\in Z_p$，并发送给用户。

3) 用户收到 c 后，计算

$$\sigma_0=\left[\prod_{i\in I'\cup A'}d_{i0}^{\Delta_{i,S}(0)}\right]\left[\prod_{i\in I^*\cup A'}H(i)^{r_i'}\right]c^x \tag{12}$$

并将 σ_0 发送给验证者。

4) 验证者在收到用户发来的值后，验证等式 $\dfrac{e(g,\sigma_0)}{\left[\prod_{i\in I^*\cup A'}e(H(i),\sigma_i)\right]e(c,\sigma_0')}=Z$ 是否成立，如果等式成立，则通过认证；否则认证失败。

3.2 正确性分析

首先，所提方案的系统初始化和密钥生成 2 个算法的正确性可通过分布式密钥生成技术的正确性得以保证。其次，交互验证协议的正确性如下。

$$\frac{e(g,\sigma_0)}{\left[\prod_{i\in I^*\cup A'}e(H(i),\sigma_i)\right]e(c,\sigma_0')}=$$

$$\frac{e\left(g,\prod_{i\in I'\cup A'}d_{i0}^{\Delta_{i,S}(0)}\right)e\left(g,\prod_{i\in I^*\cup A'}H(i)^{r_i'}\right)e(g,c^x)}{\left[\prod_{i\in I^*\cup A'}e(H(i),\sigma_i)\right]e(c,g^x)}=$$

$$\frac{e(g,\prod_{i\in I'\cup A'}d_{i0}^{\Delta_{i,S}(0)})e(g,\prod_{i\in I^*\cup A'}H(i)^{r_i'})}{\left[\prod_{i\in I'\cup A'}e(H(i),\sigma_i)\right]\left[\prod_{i\in I^*/I'}e(H(i),\sigma_i)\right]}=$$

$$\frac{\left[\prod_{i\in I'\cup A'}e(g,d_{i0}^{\Delta_{i,S}(0)})\right]\left[\prod_{i\in I'\cup A'}e(g,H(i)^{r_i'})\right]\left[\prod_{i\in I^*/I'}e(g,H(i)^{r_i'})\right]}{\left[\prod_{i\in I'\cup A'}e(H(i),d_{i1}^{\Delta_{i,S}(0)}g^{r_i'})\right]\left[\prod_{i\in I^*/I'}e(H(i),g^{r_i'})\right]}=$$

$$\frac{\prod_{i\in I'\cup A'}e(g,d_{i0}^{\Delta i,S(0)})}{\prod_{i\in I'\cup A'}e(H(i),d_{i1}^{\Delta_{i,S}(0)})}=$$

$$\frac{\prod_{i\in I'\cup A'}e\left(g,g_2^{\sum_{i=1}^{t}f_i(j)\Delta_{i,S}(j)}H(j)^{\sum_{i=1}^{t}r_{ij}}\right)^{\Delta_{i,S}(0)}}{\prod_{i\in I'\cup A'}e\left(H(i),g^{\sum_{i=1}^{t}r_{ij}}\right)^{\Delta_{i,S}(0)}}=$$

$$\prod_{i\in I'\cup A'}e\left(g,g_2^{\sum_{i=1}^{t}f_i(j)\Delta_{i,S}(j)}\right)=e(g,g_2)^s=Z \tag{13}$$

4 方案分析

4.1 安全性分析

本文方案采用的是 Gennaro 等[21]的分布式密钥生成方法，该方法已经被证明是抗合谋的。因此，本文方案可以最多抵抗来自 $t-1$ 个授权中心的合谋攻击。此外，分布式密钥生成技术核心在于以一种隐式的方式恢复系统主密钥 s，从而得到用户的属性私钥。因此，不同于 Chase[19]的各授权中心负责一个或多个属性密钥生成，基于分布式密钥生成技术的用户属性密钥生成机制可以抵抗来自用户的合谋攻击。

如前所述，本文方案主要基于文献[14]的单授权中心属性签名方案。借鉴文献[22]的混合证明思路，可以将本文方案的不可仿冒性和匿名性分别规约到文献[14]方案的不可仿冒性和签名者隐私性上。规约方法具体如下，首先定义如下 3 个游戏。

1) 游戏 Game_0。与不可仿冒性和匿名性安全定义一样，所有参与方均诚实执行相关算法或协议。

2) 游戏 Game_1。将系统主密钥定义为 $y=g^{as}$，其中，指数 a 是文献[14]方案中 CDH（computational Diffie-Hellman）问题的一个挑战实例；指数 s 是所有授权中心联合生成的随机秘密值，但所有授权中心均不知道 s 的具体值，除非至少 t 个授权中心发起合谋攻击。

3) 游戏 Game_2。在该游戏中，系统主密钥依然为 $y=g^{as}$，与 Game_1 的区别在于，在 Game_2 中，挑战者充当授权中心角色，知道秘密值 s。

由此，可以证明任意多项式时间敌手的优势在

上述 3 个游戏中是计算不可区分的。

引理 1　如果文献[21]的分布式密钥生成技术是安全的，则敌手在游戏 Game_0 与 Game_1 中的优势是计算不可区分的。

证明　根据分布式密钥生成技术[21]的安全性结论可知，即便 $t-1$ 个参与者发起合谋攻击，依然不能区分元素 $y=g^s\in G$ 是由 n 个参与者协作生成的还是从群 G 中随机选择得到的。因此，任意多项式时间敌手都无法区分元素 $y:=g^s\in G$ 和 $y:=g^{as}\in G$，其中 s 是分布式密钥生成技术的真实值，a 是 CDH 问题实例中的指数，且 a 与 s 是相互独立的。因此，对任意多项式敌手而言，其在游戏 Game_0 与 Game_1 中的优势是计算不可区分的。

证毕。

引理 2　任意多项式敌手在游戏 Game_1 与 Game_2 中的优势是计算不可区分的。

证明　注意，在 2 个游戏中，系统主公钥均为 $y=g^{as}$，其中 s 是分布式密钥生成技术的真实值，a 是 CDH 问题实例中的指数，且 a 与 s 是相互独立的。因此，尽管挑战者知道值 s，但是 $y=g^{as}$ 依然是群 G 中的一个随机元素，对敌手而言挑战者是否知道 s 并不会影响敌手的攻击。

证毕。

基于上述 2 个引理，可以分别证明本文方案的不可仿冒性和匿名性。

1) 不可仿冒性

首先证明引理 3。

引理 3　如果文献[14]的属性签名方案具有不可仿冒性，则任意多项式时间的仿冒攻击敌手在游戏 Game_2 中的优势是可忽略的。

证明　将本文方案记为 ABI，仿冒攻击敌手为 A，挑战者为 C；将文献[14]的单授权中心的属性签名方案记为 ABS，伪造敌手记为 A'，挑战者记为 C'。将 ABI 方案的不可仿冒性规约到 ABS 的不可仿冒性，ABI 的挑战者 C 同时也充当 ABS 方案的敌手 A'，C 尝试利用敌手 A 仿冒攻击 ABS 方案的安全性。具体证明过程如下。

初始化阶段。挑战者 C 输入安全参数 λ，运行 Setup 算法得到系统参数 params。同时，根据参数 params 运行分布式密钥生成算法生成 $y=g^s$。此外，从挑战者 C' 处获得 CDH 问题挑战实例 (g^a,g^b)。最后，将系统主公钥设置为 $y=g^{as}$，并将系统公开参数发送给敌手 A。

询问阶段。敌手 A 可以发起如下询问。

①密钥生成询问。敌手 A 向挑战者 C 发出属性集合 I 密钥生成请求。收到请求后，C 将属性集合 I 发送给 ABS 的挑战者 C'。根据 ABS 方案的不可仿冒性证明，C' 会返回相应的属性密钥 D_I。C 直接将 D_I 返回给敌手 A 即可。

②交互训练。敌手 A 作为恶意验证者 V^* 和诚实证明者 P 交互运行认证协议，挑战者 C 在这里需要充当证明者 P 向敌手 A 提供认证操作。当敌手发送挑战值 c 给挑战者时，挑战者将 c 充当消息发送给 ABS 方案的挑战者 C'，根据 ABS 方案的不可仿冒性证明，C' 会返回一个合法签名。最后，挑战者 C 将签名作为挑战回复返回给敌手 A。因为签名是有效的，所以其一定能通过验证协议。

挑战阶段。敌手 A 作为恶意证明者 P^* 和任意的诚实验证者 V 进行交互，试图说服验证者接受。在这里，挑战者 C 充当验证者 V，选择挑战值 c^* 发送给敌手 A。

最后，如果敌手 A 能成功打破 ABI 方案的不可仿冒性，则表示其能生成关于挑战值 c^* 的有效验证信息 $(\sigma_i,\sigma_0',\sigma_0)$，使其通过验证等式

$$\frac{e(g,\sigma_0)}{\left[\prod_{i\in I^*\cup A'}e(H(i),\sigma_i)\right]e(c^*,\sigma_0')}=Z \tag{14}$$

因此，挑战者 C 将 c^* 作为挑战消息，并输出 $(c^*,\sigma_i,\sigma_0',\sigma_0)$ 作为 ABS 方案的伪造签名。最后，根据 ABS 方案的不可仿冒性证明可知，C' 会根据 C 的伪造输出值 $T=g^{asb}$，C 计算 $T^{s^{-1}}$ 即可得到给定 CDH 问题实例的解 g^{ab}。

证毕。

根据引理 1～引理 3，即可得到定理 1。

定理 1　如果文献[21]的分布式密钥生成技术是安全的，且文献[14]的单授权中心属性签名方案具有不可仿冒性，则本文方案具有不可仿冒性。

2) 匿名性

匿名性的证明类似于上述不可仿冒性证明，唯一区别是将本文方案的匿名性规约到单授权中心的签名者隐私性上。事实上不难发现，属性身份认证方案的匿名性要求与属性签名方案的签名者隐私性要求是一致的。因此，本文直接给出定理 2。

表 1 方案效率对比

方案	证明计算开销	验证计算开销
文献[24]方案	$(4m+2)T_{\text{exp}}+(m+3)T_{\text{mul}}+T_{\text{mtp}}$	$(m+k+2)T_{\text{par}}+(m+k)T_{\text{exp}}+(k+2)T_{\text{mul}}+T_{\text{mtp}}$
文献[25]方案	$mT_{\text{par}}+(6+k)T_{\text{exp}}+mT_{\text{mul}}$	$(2km+1)T_{\text{par}}+T_{\text{exp}}+T_{\text{mul}}$
文献[26]方案	$(2kl+2)T_{\text{exp}}$	$2klT_{\text{par}}+k\tau T_{\text{exp}}$
本文方案	$(2m+2k+2)T_{\text{exp}}+(m+2k+2)T_{\text{mul}}+(m+1)T_{\text{mtp}}$	$(m+3)T_{\text{par}}+(m+2)T_{\text{mul}}+(m+1)T_{\text{mtp}}$

定理 2 如果文献[21]的分布式密钥生成技术是安全的，且文献[14]的单授权中心属性签名方案具有签名者隐私性，则本文方案具有匿名性。

4.2 效率分析

本节分析本文方案的效率，包括计算开销和通信开销。系统成功建立后，就不会再运行初始化算法。此外，用户获得属性密钥后，也不再需要运行密钥生成算法。因此，本文不考虑初始化算法和密钥生成算法的计算和通信开销。

在基于双线性映射的密码方案中，双线性对运算、map-to-point 运算、群元素指数运算和群元素乘法运算是消耗最大的 4 种运算，因此本文只考虑这 4 种运算的开销。将这 4 种运算的计算开销分别记为 T_{par}、T_{mtp}、T_{exp}、T_{mul}，并基于这 4 种运算考虑本文方案各算法的开销。

将本文方案与同类型的方案进行效率对比。目前，尽管只有一篇基于属性的身份认证方案的文献[18]，但是，基于属性签名方案也可以实现属性身份认证方案。所以，本文也将相关属性签名方案进行对比。本文主要关注多授权中心的属性身份认证方案，因此不比较文献[18]的方案。此外，本文方案基于文献[14]的属性签名方案，所以计算开销和通信开销与文献[14]的方案均一致。事实上，文献[14]也考虑了多授权中心，其方法主要基于 Chase[19]的多授权中心方法，因此需要一个额外的可信中心对用户进行统一认证，以防合谋攻击。文献[23]构造的多授权中心属性签名方案与文献[14]的方案核心技术类似，方案的计算开销与通信开销一致。文献[24-26]的多授权属性签名方案与本文方案采用的技术不一样，因此将本文方案与文献[24-26]的方案进行效率对比，并参考文献[27]的效率分析形式，对比结果如表 1 所示。

表 1 中，m 表示验证策略属性集中的属性个数，k 表示策略门限值，l 表示每个权威的访问结构中包含的属性，τ 表示集合中元素的个数。

接下来，分析本文方案与文献[24-26]方案在传输带宽方面的需求对比，并参考文献[27]的效率分析形式，对比结果如表 2 所示。

表 2 方案通信开销对比

方案	通信开销
文献[24]方案	$(k+2)\lvert G\rvert$
文献[25]方案	$(5+k)\lvert G\rvert+\lvert G_T\rvert$
文献[26]方案	$(k+2)\lvert G\rvert+k\lvert G_T\rvert$
本文方案	$(m+2)\lvert G\rvert$

表 2 中，$\lvert G\rvert$ 表示群 G 中的元素长度，$\lvert G_T\rvert$ 表示群 G_T 中的元素长度。

5 多因子身份认证应用

本节考虑本文方案在电子凭据中的多因子身份认证应用。

正如文献[28]所说，随着“互联网+”时代的到来以及电子商务的快速发展，纸质凭据的成本高、难以管理等问题越来越明显，电子凭据以其高效、成本低廉和绿色环保等优点受到人们的青睐。凭据是日常生活中被用作证明物品的东西，包括电子发票等。电子凭据作为纸质凭据的一种电子化产物，具有相同的效用。

电子凭据的流程包括电子凭据的开具、查验以及查询等业务，不同的业务所需的操作权限等级不同。同时，电子凭据涉及用户大量的敏感信息，保护用户敏感信息是对电子凭据业务所提出的挑战。为了保证电子凭据相关业务的正确执行，确保电子凭据生成和使用的合理性，需要确认操作者的权限，并对操作者进行身份认证。

众所周知，单因子身份认证具有不灵活、不支持细粒度身份认证等问题。为了解决这一问题，张敏等[29]提出将生物特征、口令、邮箱 3 种因子或者任意其中 2 种结合进行身份认证，形成多因子的身

份认证方案。多因子身份认证方案的提出提高了认证方案的安全性。

文献[28]针对电子凭据业务中身份认证的需求，提出了多元认证方案。在该方案中，根据用户提交的身份信息、应用场景描述、所需权限描述等，系统为其分配不同类型的认证方式，例如口令认证、指纹识别、人脸识别等。本文方案根据用户口令、邮箱、生物特征、访问权限等因子构成用户的属性集，通过属性谓词策略判断用户属性集是否满足验证策略要求，以此来完成身份认证，从而可以实现基于属性的细粒度认证方式。基于本文方案的电子凭据中的身份认证模型如图 1 所示，具体过程如下。

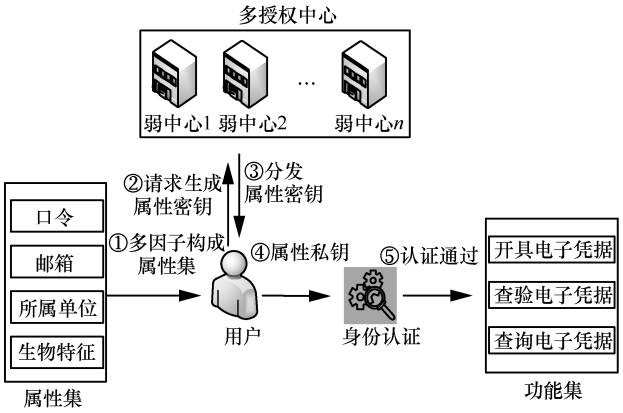


图 1　基于本文方案的电子凭据中的身份认证模型

1) 电子凭据管理系统中的用户根据口令、邮箱、所属单位、职务、角色、生物特征等因子构成自己的属性集。

2) 用户根据属性集向 n 个授权中心中的至少 t 个授权中心发出属性密钥生成请求。授权中心在收到用户发出的请求后，根据所提交的属性集为属性集中的属性生成相应的部分密钥，并将其发送给用户。

3) 用户在收到来自 t 个授权中心发送来的部分密钥后，自己合成属性私钥。

4) 用户利用属性私钥通过认证协议证明自己身份的合法性，即拥有对电子凭据进行某操作的权限，例如，开具电子凭据、查验电子凭据或者查询电子凭据。在认证协议中，电子凭据系统需要指定进行不同电子凭据操作所需要的验证策略属性集，并规定所需要满足的属性个数门限值。如果用户所提交的属性集与需要进行某项操作所指定的验证策略属性集的交集的属性个数达到属性个数门限值，则用户身份合法，身份认证成功；否则，身份认证失败。

5) 身份认证成功后，用户可以进行相应操作。例如用户需要查询电子客票信息时，提供相应的属性私钥通过身份认证即可查询电子凭据。

6　结束语

本文定义了基于属性的多授权中心的身份认证的概念，并基于双线性映射构造了一种高效的属性身份认证方案。在该方案中，根据用户的身份属性信息构成用户的属性集合，结合分布式密钥生成技术实现用户属性私钥的生成，并通过门限谓词策略规定认证机制，分析了所提方案的安全性、不可仿冒性和匿名性。此外，还考虑了基于属性身份认证方案在电子凭据中的多因子认证应用。

参考文献：

[1] FIAT A, SHAMIR A. How to prove yourself: practical solutions to identification and signature problems[C]//Advances in Cryptology-CRYPTO' 86. Berlin: Springer, 1987: 186-194.

[2] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.

[3] GUILLOU L C, QUISQUATER J J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory[C]// Workshop on Advances in Cryptology-Eurocrypt. Berlin: Springer, 1988: 123-128.

[4] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//International Cryptology Conference. Berlin: Springer, 1985: 47-53.

[5] KUROSAWA K, HENG S. Identity-based identification without random oracles[C]//International Conference on Computational Science and Its Applications. Berlin: Springer, 2005: 603-613.

[6] BONEH D, BOYEN X. Short signatures without random oracles[C]//Theory and Application of Cryptographic Techniques. Berlin: Springer, 2004: 56-73.

[7] CHIN J J, HENG S H, GOI B M. An efficient and provable secure identity-based identification scheme in the standard model[C]//Public Key Infrastructure, 5th European PKI Workshop: Theory and Practice, EuroPKI. Berlin: Springer, 2008: 60-73.

[8] BARAPATRE P, RANGAN C P. Identity-based identification schemes from ID-KEMs[C]//International Conference on Security. Berlin: Springer, 2013: 111-129.

[9] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457-473.

[10] GOVAL 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. New York: ACM Press, 2006: 89-98.

[11] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE Symposium on Security and Pri-

vacy. Piscataway: IEEE Press, 2007: 321-334.
[12] MAJI H, PRABHAKARAN M, ROULEK M. Attribute-based signatures[C]//Topics in Cryptology-CT-RSA. Berlin: Springer, 2011: 376-392.
[13] TANG F, LI H, LIANG B. Attribute-based signatures for circuits from multilinear maps[C]//International Conference on Information Security. Berlin: Springer, 2014: 54-71.
[14] LI J, AU M H, SUSILO W, et al. Attribute-based signature and its applications[C]//ACM Symposium on Information. New York: ACM Press, 2010: 60-69.
[15] OKAMOTO T, TAKASHIMA K. Efficient attribute-based signatures for non-monotone predicates in the standard model[J]. IEEE International Conference on Cloud Computing Technology and Science, 2014, 2(4): 409-421.
[16] YONEYANAMA K. Strongly secure two-pass attribute-based authenticated key exchange[C]//International Conference on Pairing-Based Cryptography. Saarland: DBLP, 2010: 147-166.
[17] TANG F, ZHANG R, LI H. Attribute-based non-interactive key exchange[J]. Science China Information Sciences, 2017, 60(2): 206.
[18] ANADA H, ARITA S, HANDA S, et al. Attribute-based identification: definitions and efficient constructions[C]//Australasian Conference on Information Security and Privacy. Berlin: Springer, 2013: 168-186.
[19] CHASE M. Multi-authority attribute based encryption[C]//Theory of Cryptography Conference. Berlin: Springer, 2007: 515-534.
[20] LIN H, CAO Z, LIANG X, et al. Secure threshold multi authority attribute based encryption without a central authority[J]. Information Sciences, 2010, 180(13): 2618-2632.
[21] GENNARO R, JARECKI S, KRAWCZYK H, et al. Secure distributed key generation for discrete-log based cryptosystems[C]//Theory and Application of Cryptographic Techniques. Berlin: Springer, 1999: 295-310.
[22] TANG F, MA S, XIANG Y, et al. An efficient authentication scheme for blockchain-based electronic health records[J]. IEEE Access, 2019, 7: 41678-41689.
[23] CAO D, ZHAO B, WANG X, et al. Multi-authority attribute-based signature[C]//Third International Conference on Intelligent Networking and Collaborative Systems. Piscataway: IEEE Press, 2011: 668-672.
[24] LIU X, ZHANG R, XUE R, et al. Multi-central-authority attribute-based signature[C]//Proceedings of the 2012 Fourth International Symposium on Information Science and Engineering. New York: ACM Press, 2012: 173-178.
[25] GUO R, SHI H, ZHAO Q, et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems[J]. IEEE Access, 2018, 6: 11676-11686.
[26] 莫若, 马建峰, 刘西蒙, 等. 支持树形访问结构的多权威基于属性的签名方案[J]. 通信学报, 2017, 38(7): 96-104.
MO R, MA J F, LIU X M, et al. Multi-authority ABS supporting dendritic access structure[J]. Journal on Communications, 2017, 38(7): 96-104.
[27] 张凯, 马建峰, 李辉, 等. 支持高效撤销的多机构属性加密方案[J]. 通信学报, 2017, 38(3): 83-91.
ZHANG K, MA J F, LI H, et al. Multi-authority attribute-based encryption with efficient revocation[J]. Journal on Communications, 2017, 38(3): 83-91.
[28] 路世翠. 电子凭据服务系统的多元身份管理机制研究[D]. 西安电子科技大学, 2019.
LU S C. Research on the multi-identity management mechanism of electronic credential service system[D]. Xi'an: Xidian University, 2019.
[29] 张敏, 何远德, 张阳. 多服务器环境下可实现访问控制的身份认方案[J]. 计算机工程与应用, 2017, 53(17): 123-129.
ZHANG M, HE Y D, ZHANG Y. Authentication scheme for multi-server enviroment based on Chebyshev chaotic map with access control[J]. Computer Engineering and Applications, 2017, 53(17): 123-129.

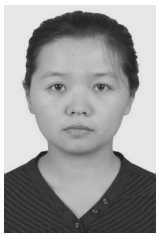
[作者简介]

唐飞（1986– ），男，重庆人，博士，重庆邮电大学副教授、硕士生导师，主要研究方向为公钥密码、隐私保护、区块链等。

包佳立（1994– ），女，重庆人，重庆邮电大学硕士生，主要研究方向为公钥密码、区块链。

黄永洪（1974– ），男，重庆人，重庆邮电大学讲师，主要研究方向为信息安全、密码学等。

黄东（1981– ），男，重庆人，重庆机电职业技术大学教授，主要研究方向为通信安全、公钥密码学等。



王惠莅（1977– ），女，河南清丰人，中国电子技术标准化研究院高级工程师，主要研究方向为信息安全、云计算等。