医疗社交网络中基于云计算的属性基签密方案

牛淑芬[①] 周思玮*[①] 吕锐曦[②] 闫 森[①] 张美玲[①] 王彩芬[①②③]

[①](西北师范大学计算机科学与工程学院 兰州 730070)

[②](西北师范大学数学与统计学院 兰州 730070)

[③](深圳技术大学大数据与互联网学院 深圳 518118)

摘 要：移动医疗社交网络的出现为患者之间互相交流病情提供了极大的便利，促进了患者之间高效、高质量的沟通与交流，但与此同时也产生了患者数据的保密性和隐私性问题。针对此问题，该文提出一种基于云计算的属性基签密方案，能够有效地保护患者数据的隐私性。患者将自己的病情信息签密后上传至云服务器，当数据用户要访问患者的信息时，云服务器帮助数据用户进行部分解密并验证数据的完整性，这在一定程度上减少了数据用户的计算量。同时，在随机预言机模型下，证明了该方案满足选择消息攻击下的不可伪造性、选择密文攻击下的不可区分性以及属性隐私安全性。理论分析和数值模拟实验结果表明，该方案在签密和解签密阶段比现存的方案有更高的效率。

关键词：属性基签密；云服务器；医疗社交网络；云辅助验证

中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2023)03-0884-10

DOI: 10.11999/JEIT220070

Attribute-Base Signcryption Scheme Based on Cloud Computing in Mobile Medical Social Network

NIU Shufen[①] ZHOU Siwei[①] LÜ Ruixi[②] YAN Sen[①]

ZHANG Meiling[①] WANG Caifen[①②③]

[①](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[②](*College of Mathematics and Statistics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[③](*College of Big Data and Internet*, *Shenzhen University of Technology*, *Shenzhen* 518118, *China*)

Abstract: The emergence of mobile medical social networks has greatly facilitated the communication of patients' conditions to each other, promoting efficient and high-quality communication and exchange between patients. However, it also causes problems of confidentiality and privacy of patient data. To solve this problem, an attribute-based signcryption scheme based on cloud-assisted verification is proposed, which can effectively protect the privacy of patient data. Patients signcrypt their health information and upload it to the cloud server. When the data user wants to access the patient's information, the cloud server helps the data user partially decrypt and verify the integrity of the data, which reduces the amount of calculation of the data user to a certain extent. At the same time, under the random oracle model, it is proved that the scheme satisfies the unforgeability under the adaptive selection message, the indistinguishability under the adaptive selection ciphertext attack, and the attribute privacy security. Theoretical analysis and numerical simulation experimental results show that the scheme is more efficient than the existing schemes in the signcryption and unsigncryption phases.

Key words: Attribute-based signcryption; Cloud server; Medical social network; Cloud-assisted verification

收稿日期：2022-01-14；改回日期：2022-06-13；网络出版：2022-07-19

*通信作者： 周思玮 zsw7angel@163.com

基金项目：国家自然科学基金(62241207, 61862058, 61662069)

Foundation Items: The National Natural Science Foundation of China (62241207, 61862058, 61662069)

1　引言

随着医疗信息技术的快速发展，智慧医疗[1]的概念应运而生。移动医疗社交网络平台通过使用无线传感设备[2]实时收集患者的健康信息，拥有相同病症的患者成为一个社交群体，彼此之间相互交流自己的健康信息、身体的健康状态和分享彼此的经验。相较于传统的医疗模式，移动医疗社交网络具有更强的关联性与交互性，更有助于实时收集患者的数据，能进行更及时的治疗。随着云计算的不断发展，移动医疗得到广泛应用并趋于多样化[3]，越来越多的医疗机构采用移动医疗社交网络平台，将患者的数据上传至云端进行存储。基于云的存储系统比传统的存储系统具有更多的优势，使患者通过更便捷的服务[4]维护数据。

基于属性的密码体制能够更好地保证患者数据的隐私性和安全性，与传统的基于身份的密码体制相比，实现了一对多的细粒度的访问控制，提升了数据发送方的效率[5]。属性基密码体制源于Sahai等人[6]提出的模糊身份基加密体制。近年来，基于属性的加密思想广泛应用于云计算的环境下，文献[7]提出一种可撤销的属性基加密方案，并结合外包计算的思想，将部分运算量大的计算外包给云服务器处理，使得用户本地端执行解密操作的效率大幅提高。文献[8]将可搜索加密技术应用于属性基中，提出一种智慧医疗环境中的属性基可搜索加密方案，实现了细粒度访问控制。文献[9]提出“云-雾-端”的3层系统模型，将属性基加密算法应用到雾计算中，并支持属性撤销和外包计算，进一步实现了数据用户的隐私保护。文献[10]提出了基于多机构的属性基代理重加密方案，分析了云存储医疗数据安全访问与共享机制的研究现状。

传统的“先加密后签名”思想的计算开销和通信成本较高，针对此问题，文献[11]首次提出了签密的概念和方案，同时保证消息的机密性和不可伪造性。近年来，众多学者对属性基签密做了大量的研究，提升了其计算效率，文献[12]在属性基加密算法基础上提出了一个属性基签密方案，实现了数据外包解密并支持属性撤销，确保了消息的完整性与机密性。文献[13]在体域网中提出基于属性的在线\离线签密方案，将大部分解签密运算外包给云服务器，减轻了数据用户的计算负担。文献[14,15]，用属性基签密机制，使用过滤器隐藏访问策略，保护了病患信息的隐私；为了进一步提高医疗社交网络的可用性，文献[16,17]提出了可追踪的属性基签密方案，该方案能够追踪到发布恶意信息用户的身份信息。文献[18,19]都提出支持数据完整性验证的属性基签密方案，文献[18]支持访问策略更新，文献[19]实现细粒度访问控制保证数据的隐私性、询问结果的完整性以及不可伪造性。文献[20]在云计算的基础上引入雾节点，提出云雾辅助的属性基签密方案，形成了“云-边-端”的3层模型，将更多的数据运算外包给雾节点进行，进一步提升了算法的效率。

本文提出了一种基于属性的签密方案，将云计算和属性基签密技术相结合，进一步提高了数据的细粒度访问控制，云服务器因其强大的计算和存储能力，为数据的存储提供了良好的平台，同时帮助数据用户部分解密并验证数据的完整性，一定程度上减少了数据用户的计算量。并且属性基签密技术能实现对用户数据的保护，从而保证数据分享的安全性和患者的隐私性，并分别从不可区分性、不可伪造性、隐私性方面证明数据用户使用数据的安全性。相对于现有方案，本文创新点有以下3个方面：

(1)本文方案使用基于属性的签密技术在一定程度上减少了证书验证的开销，密文有两部分，分别用于数据用户解密和云服务器验证。在此方案中云服务器帮助数据用户解密并验证，减少了数据用户的计算负担。

(2)结合智慧医疗平台采用无线身体传感设备实时收集患者的健康信息，通过无线传感网络可定期将患者信息上传至云服务器存储，为患者间的相互交流提供了便利。

(3)本文方案实现了数据的可追踪性。当有恶意用户在此平台上发布虚假信息给其他患者时，PKG和云服务器可联合追踪到发布虚假信息用户的身份。PKG从他保存的私钥映射表里得到签名者的属性的签名，然后将此签名发送给云服务器，云服务器在查询他所保存的属性签名表之后就可以输出签名者的身份。

2　预备知识

2.1　访问结构

假定$P=\{P_1,P_2,\cdots,P_n\}$为n个数据使用者组成的集合，存在一个集合$W\subseteq 2^P$，且此集合是单调的，对于任意的集合B和C，当且仅当$B\in W$，$B\subseteq C$则$C\in W$。如果集合W是P的非空子集，即ω_1且单调，那么W就是一个访问结构，包含在W中的集合称为授权子集，否则为非授权子集。

2.2　困难问题假设

(1)λ Diffie-Hellman指数问题(λ-DHE)[15]：已知两个循环群G_1和G_2，生成元为g，阶为大素数p，并且存在双线性映射：$e:G_1\times G_1\to G_2$，给定

$(g, g^a, \cdots, g^{a^l}, g^{a^{l+2}}, \cdots, g^{a^{2l}}, h)$，$h \in G_2$，并随机选择$a \in Z_p$，判断$h = e(g,g)^{a^{\lambda+1}}$是否成立。

(2)判定性双线性Diffie-Hellman问题(DBDH)[18]：G_1和G_2是阶为p的循环群$e: G_1 \times G_1 \to G_2$为一个双线性映射，给定2个元组$(g, g^a, g^b, g^c, e(g,g)^{abc})$和$(g, g^a, g^b, g^c, e(g,g)^z)$，对随机的$a, b, c, z \in Z_p^*$，不存在概率多项式时间的攻击者以不可忽略的优势区分$e(g,g)^{abc}$和$e(g,g)^z$。

3 系统模型和安全模型

3.1 系统模型

本文方案系统模型如图1所示，主要由密钥生成中心PKG、云服务器、数据拥有者Alice、数据使用者Bob和无线传感基站构成，各实体具体说明如下：

密钥生成中心PKG：PKG作为整个系统的可信第三方来提供服务，它的主要职责是根据每个用户的属性集合，为每个用户生成并颁发私钥；

云服务器：云服务器在整个系统中是一个半可信的第三方平台。由于其强大的存储量和计算能力，它的主要职责是实现用户数据的存储，并辅助数据使用者进行验证工作；

数据拥有者Alice：Alice作为数据拥有者并不是指一个人，而是代表一个数据拥有者群体。他将自己的隐私信息进行签密上传至云服务器存储；

数据使用者Bob：Bob作为数据使用者并不是指一个人，而是代表一个数据使用者群体。当他想要查看数据拥有者的病症信息时，对存储在云服务器上的数据进行解签密获得数据；

无线传感基站：在此系统中为每个患者配有无线身体感知设备，用于实时收集患者的健康信息，通过此基站来接收患者可穿戴设备实时收集到的数据。

下面对本文所提的方案进行简单示例说明：图1中，数据拥有者Alice首先将自己的隐私信息进行签密，并上传至云服务器存储，Alice所签密的隐私信息包括自己的性别、年龄、病症以及由可穿戴设备实时收集到的健康信息等。在此医疗社交网络中，当有一个数据使用者Bob想要查看Alice的隐私信息时，Alice将自己加密的部分隐私信息发送给Bob，Bob解签密得到消息m，与此同时，云服务器辅助验证Bob得到的消息m是否被篡改。若未被篡改，则Bob可以利用消息m与用户Alice联系；若被篡改，则Bob丢弃该消息。系统模型如图1所示。

3.2 形式化定义

本文提出的医疗社交网络中基于属性的签密方案由以下算法组成：

系统初始化：$\text{Setup}(1^\lambda) \to (\text{PP})$，该算法由PKG执行，输入安全参数$\lambda$，初始化算法并输出公共参数PP。

密钥提取：$\text{Extract}(W_\text{s}, \text{mk}, \text{Sig}(W_\text{s})) \to \text{sk}_\text{u}$，该算法由PKG执行，输入数据发送者的属性集合$W_\text{s}$及他的签名$\text{Sig}(W_\text{s})$和主密钥mk，算法输出私钥$\text{sk}_\text{u}$。

签密：$\text{Signcrypt}(m, W_\text{e}, \Gamma_{\text{k},W_*}(\cdot), \text{sk}_\text{u}) \to \sigma$，该算法由拥有属性集合$W_\text{e}$的数据发送者执行，输入消息$m$、属性集合$W_\text{e}$、签名谓词$\Gamma_{\text{k},W_*}(\cdot)$和数据发送者的私钥$\text{sk}_\text{u}$，最终输出密文$\sigma$。

解签密：$\text{Unsigncrypt}(\sigma, \Gamma_{\text{k},W_*}(\cdot), W_\text{d}, \text{sk}'_\text{u}) \to m$，

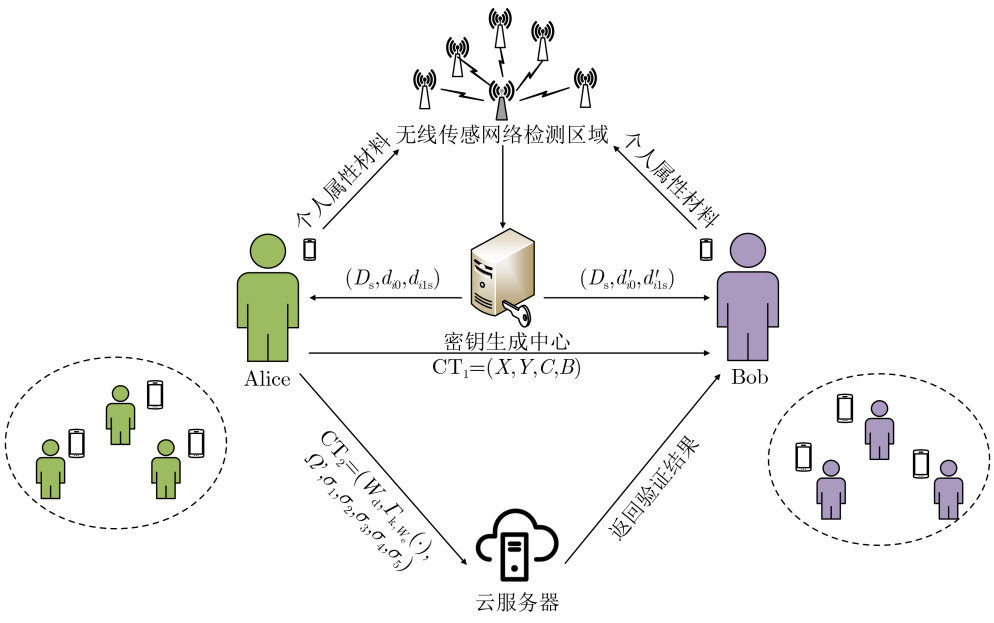

图 1 系统模型

该算法由拥有属性集合W_{d}的数据使用者执行，输入密文σ、签名谓词$\Gamma_{\mathrm{k},W_*}(\cdot)$、属性集合$W_{\mathrm{d}}$和数据使用者的私钥$\mathrm{sk}'_{\mathrm{u}}$，最终得到消息$m$。

3.3 安全模型

通过多项式时间模拟敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间的游戏来定义选择消息攻击下的不可伪造性安全，适应性选择密文攻击下不可区分性安全。

游戏1 选择消息攻击下不可伪造性。

定义1　对于任何具有多项式时间能力的敌手$\mathcal{A}$，如果在下面的选择谓词游戏中没有以不可忽略的优势获胜，则称基于属性的签密算法在选择消息攻击下具有不可伪造性。

初始化：敌手$\mathcal{A}$将部分用户签名属性集合W_{s}^*和一个签名谓词$\Gamma_{W_{\mathrm{s}}^*}^*(\cdot)$给挑战者$\mathcal{C}$，在这里$|W_{\mathrm{s}}^*|<d$，并且采用$W_{\mathrm{s}}^*$来对明文进行加密。

系统建立：$\mathcal{C}$选择系统参数PP，并且执行初始化算法。$\mathcal{C}$的参数选择仅意味着$\mathcal{A}$不能访问挑战明文。

询问阶段：$\mathcal{A}$发起预言询问，挑战者$\mathcal{C}$对询问做出响应。

(1)密钥提取询问：$\mathcal{A}$生成一个用户的签密属性集合W_{s}和一个门限值k，$\mathcal{C}$执行密钥提取算法，提取发送者的私钥$\mathrm{sk}_{W_{\mathrm{s}}^*,k}=\mathrm{KeyExtraction}(\mathrm{pp},\mathrm{mk},W_{\mathrm{s}}^*,k)$并将它发送给$\mathcal{A}$。然后$\mathcal{A}$选择他的部分用户的解签密属性集合$W_{\mathrm{r}}$和一个门限值$d$，$\mathcal{C}$提取接收者的私钥$\mathrm{sk}_{W_{\mathrm{r}},d}=\mathrm{KeyExtract}(\mathrm{pp},\mathrm{mk},W_{\mathrm{r}},d)$并将它发送给$\mathcal{A}$。

(2)签密询问：$\mathcal{A}$选择一个消息m，一个加密属性集合W_{e}和一个门限值k，挑战者$\mathcal{C}$根据密钥提取算法提取出$\mathrm{sk}_{W_{\mathrm{s}}^*,k}$，然后发送询问结果给$\mathcal{A}$。

伪造：$\mathcal{A}$输出一个根据消息m和加密属性集合W_{e}伪造的密文，若密文有效，则敌手赢得游戏。

游戏2 自适应选择密文攻击下不可区分性。

定义2　在概率多项式时间内，如果敌手$\mathcal{A}$没有以不可忽略的优势在如下游戏中获胜，则基于属性签密方案在适应性选择密文攻击下具有不可区分性。

初始化：$\mathcal{C}$执行初始化算法，利用系统安全参数λ产生公共参数PP和系统密钥α，将PP发布给敌手$\mathcal{A}$，保留α作为秘密值。

询问阶段1：$\mathcal{A}$发起适应性预言询问，挑战者$\mathcal{C}$对询问做出响应。

(1)Hash询问：$\mathcal{A}$可以询问任意输入的Hash值。

(2)密钥提取询问：$\mathcal{A}$选择一个属性集ω_i，根据系统参数PP和主密钥α，$\mathcal{C}$计算用户私钥sk_{ω_i}，并将它发送给$\mathcal{A}$。

(3)签密询问：$\mathcal{A}$选择加密属性集合ω_i，ω_j和明文m，ω_i用于签名，ω_j用于加密。挑战者$\mathcal{C}$对ω_i进行密钥提取询问，并计算$\sigma=\mathrm{Signcrypt}(\omega_i,\omega_j,\mathrm{sk}_{\omega_i},m)$，将密文$\sigma$发送给$\mathcal{A}$。

在询问阶段1，$\mathcal{A}$可以根据之前的询问结果进行自适应询问。最后，$\mathcal{A}$选择两个等长的明文m_0，m_1和两个挑战的属性集ω_A^*，ω_B^*，ω_A^*用于签名，ω_B^*用于加密，且ω_B^*没有被执行过私钥提取询问。

挑战：$\mathcal{C}$随机选择ε'，计算$\sigma_c^*=\mathrm{Signcrypt}(\omega_A^*,\omega_B^*,\mathrm{sk}_{\omega_A}^*,m_c^*)$，返回密文$\sigma_c^*$给$\mathcal{A}$。

询问阶段2：与阶段1询问相同。但不允许对ω_B^*进行私钥提取询问，不允许询问$\omega_A^*,\omega_B^*,\sigma_c^*$的明文。

猜测：最后$\mathcal{A}$输出$c'\in\{0,1\}$，如果$c'=c$，则$\mathcal{A}$在游戏中获胜。定义$\mathcal{A}$在游戏中获胜的的优势为$\mathrm{Adv}(\mathcal{A})=|\mathrm{pr}[c'=c]-\dfrac{1}{2}|$。

若对于多项式时间的敌手$\mathcal{A}$，$\mathrm{Adv}(\mathcal{A})$可忽略，则称方案满足自适应选择密文攻击下不可区分性安全。

定义3　签密者属性隐私安全性：定义全局属性集合U、谓词Γ、消息m以及一个由两者之一生成的有效密文CT。如果属性集$\omega\subset U$，则$\Gamma(\omega)=1$。如果给定消息m，签名属性集合ω_1，ω_2和密文CT，且$\Gamma(\omega_1)=\Gamma(\omega_2)=1$，任何一个多项式时间的敌手$\mathcal{A}$不能区分密文CT是由哪一个属性集合产生的，如果他没有同时破解云服务器和PKG，那么就可以认为此方案满足签密者属性隐私性安全性。

4　具体方案

本文方案由5个多项式时间算法组成，即PKG初始化、密钥生成、签密、解签密、验证，具体如下：

PKG初始化：(1)给定安全参数λ和全局属性集合U，首先PKG选择两个阶为p的双线性群G和G_{T}，g_1和g_2为群G的两个生成元。令双线性映射为$e:G\times G\to G_{\mathrm{T}}$，选择两个抗碰撞的哈希函数$H_1:G_{\mathrm{T}}\to\{0,1\}^{n_1}$，$H_2:\{0,1\}^{n_1}\times G_{\mathrm{T}}\times G\to Z_{\mathrm{p}}^*$。在这里$n_1$代表消息的比特长度，然后PKG计算$g_1=g^{\alpha}$和$Z=e(g_1,g_2)^{\alpha}$。

(2)假定属性集合U的长度为$b=|U|$，并且令$U=\{1,2,\cdots,b\}$。为了实现一个灵活的可变门限值d，选择一个$d-1$阶的默认属性集合，记为$\Omega=\{b+1,b+2,\cdots,b+d-1\}$。然后PKG随机选择$v',v_1,v_2,\cdots,v_n$、$\mu'$，$\mu_1,\mu_2,\cdots,\mu_{n_2}\in G$，$n_2$表示发送者属性集合的长度。对于每个发送者$u=(u[1],u[2],\cdots,u[n_2])\in\{0,1\}^{n_2}$以及消息$m=(m[1],m[2],\cdots,m[n_1])\in\{0,1\}^{n_1}$，定义两个函数分别为：$W(u)=\mu'\prod_{i=1}^{n_2}{\mu_i}^{u[i]}$和$V(m)=v'\prod_{i=1}^{n_1}{v_i}^{m[i]}$。

(3)PKG 公布$\mathrm{PP}=\{G,G_{\mathrm{T}},e,p,g_1,g_2,Z,H_1,H_2,U,M\}$，其中$M=(v',v_1,v_2,\cdots,v_{n_1})$, $U=(\mu',\mu_1,\mu_2,\cdots,\mu_{n_2})$，主密钥$\mathrm{mk}=\alpha$。

密钥生成：PKG执行此算法，以主密钥mk和数据发送者属性集合W_{s}作为输入，为每位患者生成私钥。随机选择一个$d-1$阶的多项式L_U，且L_U，选择$s\in Z_{\mathrm{p}}^*$，计算$D_{\mathrm{s}}={g_1}^s$。对于每个$i\in W_{\mathrm{s}}\cup\Omega$，PKG随机选择$r_1,r_2,\cdots,r_i\in Z_{\mathrm{p}}^*$，计算$d_{i0}={g_2}^{q(i)}H_1(i)^{r_i}W(u)^s$, $d_{i1}={g_1}^{r_i}$。对于每个$i\in W_{\mathrm{r}}\cup W_{\mathrm{d}}$，PKG随机选择$r_1,r_2,\cdots,r_i\in Z_{\mathrm{p}}^*$，计算$d'_{i0}={g_2}^{q(i)}H_1(i)^{r_i}$, $d'_{i1}=g^{r_i}$。PKG保存一个私钥映射表，记录从$e(g_1,g_1^{\mathrm{s}})$到$\mathrm{Sig}(W_{\mathrm{s}})$的映射关系，最后输出私钥$\mathrm{sk_u}=(D_{\mathrm{s}},d_{i0},d_{i1})$。

签密：此算法输入加密属性集合W_{e}和签名谓词$\Gamma_{\mathrm{k},W_*}(\cdot)$，这代表发送者必须证明他在属性集合$W_{\mathrm{e}}$中至少有$k$个属性，数据接收者也得确保他在属性集合$W_{\mathrm{d}}$中至少有$d$个属性，这样才能确保签密的消息只能由他自己进行解签密。给定消息$m=(m[1],m[2],\cdots,m[n_1])\in\{0,1\}^{n_1}$，数据发送者对消息进行签密：选择一个$k$阶属性子集$W'_{\mathrm{s}}\subseteq(W_{\mathrm{s}}\cap W_{\mathrm{e}})$以及一个$d-k$阶的默认属性子集$\Omega'\subseteq\Omega$，然后生成一个新的$d$阶子集，将其记为$S=W'_{\mathrm{s}}\cup\Omega'$，且$(|S|=d)$；随机选择$x\in Z_{\mathrm{p}}^*$并且计算：$X={g_1}^x$, $Y=Z^x=e(g_1,g_2)^{\alpha x}$, $C=m\oplus H_2(Y)$, $B=H_1(i)$, $i\in S$，最终输出$\mathrm{CT}_1=(X,Y,C,B)$。随机选择$t'\in Z_p^*$并且计算：$\sigma_1={d_{i1}}^{\sum_{i\in S}\Delta_{i,S}(0)}$，$\sigma_2={D_{\mathrm{s}}}^{\sum_{i\in S}\Delta_{i,S}(0)}$，$\sigma_3=d_{i0}\cdot V(m)^{t'}$，$\sigma_4={g_1}^{t'\sum_{i\in S}\Delta_{i,S}(0)}$，$\sigma_5={g_1}^{\sum_{i\in S}\Delta_{i,S}(0)}$，最终输出$\mathrm{CT}_2=(W_{\mathrm{d}},\Gamma_{\mathrm{k},W_{\mathrm{e}}}(\cdot),\Omega',\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$。数据拥有者将$\mathrm{CT}_1$发送给数据使用者，将$\mathrm{CT}_2$发送给云服务器。

解签密：数据使用者执行此算法，输入密文$\mathrm{CT}_1=(X,Y,C,B)$，$\mathrm{CT}_2=(W_{\mathrm{d}},\Gamma_{\mathrm{k},W_{\mathrm{e}}}(\cdot),\Omega',\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$，计算$Y=\prod_{i\in W'_{\mathrm{r}}}\left(\frac{e(d'_{i0},X)}{e(B^x,d'_{i1})}\right)^{\Delta_{i,W'_{\mathrm{r}}}(0)}$，然后从中恢复出消息$m=C\oplus H_2(Y)$。

上述正确性证明如下：已知数据接收者的私钥$(D_{\mathrm{s}},d'_{i0},d'_{i1})$，给定消息$m\in\{0,1\}^{n_1}$的密文$\mathrm{CT}_1=(X,Y,C,B)$，$\mathrm{CT}_2=(W_{\mathrm{d}},\Gamma_{\mathrm{k},W_{\mathrm{e}}}(\cdot),\Omega',\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$，解签密过程为

$$
\begin{aligned}
Y&=\prod_{i\in W'_{\mathrm{r}}}\left(\frac{e(d'_{i0},X)}{e(B^x,d'_{i1})}\right)^{\Delta_{i,W'_{\mathrm{r}}}(0)}=\prod_{i\in W'_{\mathrm{r}}}\left(\frac{e({g_2}^{q(i)}H_1(i)^{r_i},g_1^x)}{e(H_1(i)^x,g_1^{r_i})}\right)^{\Delta_{i,W'_{\mathrm{r}}}(0)}\\
&=\prod_{i\in W'_{\mathrm{r}}}\left(\frac{e({g_2}^{q(i)},g_1^x)\cdot e(H_1(i)^{r_i},g_1^x)}{e(H_1(i)^x,g_1^{r_i})}\right)^{\Delta_{i,W'_{\mathrm{r}}}(0)}\\
&=\prod_{i\in W'_{\mathrm{r}}}e({g_2}^{q(i)},g_1^x)^{\Delta_{i,W'_{\mathrm{r}}}(0)}\\
&=e(g_1,g_2)^{\sum_{i\in W'_{\mathrm{r}}}x\cdot\Delta_{i,W'_{\mathrm{r}}}(0)\cdot q(i)}\\
&=Y
\end{aligned}
$$

验证：云服务器辅助数据使用者验证恢复得到的消息m是否被篡改，若未被篡改，则等式成立且返回1。否则，则返回$\perp$。验证等式：$\frac{e(\sigma_3,\sigma_5)}{e(V(m),\sigma_4)\cdot e(W(u),\sigma_2)\cdot e(\sigma_1,B)}=Z$。 证毕

上述正确性证明如下：验证过程为

$$
\begin{aligned}
&\frac{e(\sigma_3,\sigma_5)}{e(V(m),\sigma_4)\cdot e(W(u),\sigma_2)\cdot e(\sigma_1,B)}\\
&=\frac{e(d_{i0}\cdot V(m)^{t'},{g_1}^{\sum_{i\in S}\Delta_{i,S}(0)})}{e(V(m),{g_1}^{t'\sum_{i\in S}\Delta_{i,S}(0)})\cdot e(W(u),{D_s}^{\sum_{i\in S}\Delta_{i,S}(0)})\cdot e({d_{i1}}^{\sum_{i\in S}\Delta_{i,S}(0)},H_1(i))}\\
&=\frac{e({g_2}^{q(i)}H_1(i)^{r_i}W(u)^sV(m)^{t'},{g_1}^{\sum_{i\in S}\Delta_{i,S}(0)})}{e(V(m),{g_1}^{t'\sum_{i\in S}\Delta_{i,S}(0)})\cdot e(W(u),{g_1}^{s\sum_{i\in S}\Delta_{i,S}(0)})\cdot e({g_1}^{r_i\sum_{i\in S}\Delta_{i,S}(0)},H_1(i))}\\
&=\frac{e({g_2}^{q(i)},{g_1}^{\sum_{i\in S}\Delta_{i,S}(0)})\cdot e(H_1(i)^{r_i},{g_1}^{\sum_{i\in S}\Delta_{i,S}(0)})\cdot e(W(u)^s,{g_1}^{\sum_{i\in S}\Delta_{i,S}(0)})\cdot e(V(m)^{t'},{g_1}^{\sum_{i\in S}\Delta_{i,S}(0)})}{e(V(m),{g_1}^{t'\sum_{i\in S}\Delta_{i,S}(0)})\cdot e(W(u),{g_1}^{s\sum_{i\in S}\Delta_{i,S}(0)})\cdot e({g_1}^{r_i\sum_{i\in S}\Delta_{i,S}(0)},H_1(i))}\\
&=e(g_1,g_2)^{q(i)\sum_{i\in S}\Delta_{i,S}(0)}=e(g_1,g_2)^{\alpha}=Z
\end{aligned}
$$

算法输入消息m、它的签名σ以及签名谓词$\Gamma_{\mathrm{k},W_*}(\cdot)$，然后PKG计算：$e(g,{\sigma_2}^{q(i)})=e(g_1,{g_1}^s)$。最后，PKG可以从他保存的私钥映射表里得到签名者的属性的签名，然后将此签名发送给云服务

器，云服务器在查询他所保存的属性签名表之后就可以输出签名者的身份，这样就实现了追踪的功能。

证毕

5　安全性证明

本文基于DBDH困难问题及λ-DHE指数问题假设，证明了本文方案在安全模型定义中的安全目标和随机预言模型下的安全性。

5.1 自适应选择消息攻击下不可伪造性

定理1　若在多项式时间t内，敌手$\mathcal{A}$以不可忽略的优势ε赢得游戏1，则挑战者$\mathcal{C}$能够以不可忽略的优势ε'伪造签名。

假设敌手$\mathcal{A}$以不可忽略的优势ε通过至多q_{k}次的密钥生成询问和q_{s}次的签密询问伪造一个合法签名，则可以构建算法$\mathcal{F}$，能以不可忽略的优势ε'解决λ-DHE困难性问题，即：$\varepsilon' \geq \varepsilon/4q_s(q_k+q_s)(n_1+1)(n_2+1)$，其中，$n_1$代表消息的比特数，$n_2$代表患者身份信息ID的比特数。

因此，我们需要通过算法$\mathcal{F}$得到ε和ε'之间的关系。此不等式意味着：如果存在一个攻击者能够以概率ε攻击本文的方案，那么算法$\mathcal{F}$就能以概率ε'解决λ-DHE问题，但是这个假设是不成立的，因为解决λ-DHE问题是困难的，所以本文提出的方案满足不可伪造性。

证明　$\mathcal{A}$攻击本文方案的概率为ε，$\mathcal{F}$为一个能够解决λ-DHE问题的算法，攻击者给算法$\mathcal{F}$用户一部分签密属性集W_s^*和一个谓词$\Gamma_{k,W_s^*}^*(\cdot)$。接下来，算法$\mathcal{F}$从缺省属性集$\Omega$中选择$d-k$个元素属性，使得$\Omega'^* = \{l+1,\cdots,l+d-k\} \subseteq \Omega$。

初始化阶段：算法$\mathcal{F}$令$g_1{=}g$,$g_2 = g^a$，然后$\mathcal{F}$生成主密钥$\alpha{=}a^\lambda$,得到$Z = e(g_1,g_2)^\alpha = e(g^{a^\lambda}, g^a)$。$\mathcal{F}$令$l_\mu{=}2(q_k+q_s)$，$l_m = 2q_s$，并且随机地选择两个整数$k_\mu$和$k_m(0 \leq k_\mu \leq l_\mu,\ 0 \leq k_m \leq l_m)$。对于给定的数值$q_k$,$q_s$,$n_1$和$n_2$，假设$l_\mu(n_2+1) < p$以及$l_m(n_1+1) < p$。$\mathcal{F}$选择$a_0{\in}_R Z_{l_\mu}$和长度为$n_2$的向量$\boldsymbol{A} = (a_i)$，$a_i$为集合$Z_{l_\mu}$里的随机整数。同时，$\mathcal{F}$选择$b_0{\in}_R Z_{l_m}$和一个长度为$n_1$的向量$\boldsymbol{B} = (b_i)$，$b_i$为集合$Z_{l_m}$里的随机整数。另外，$\mathcal{F}$选择$w_0, v_0{\in}_R Z_{\mathrm{p}}$。对于所有的$i$和$j$来说，$\mathcal{F}$选择两个随机向量分别为$\boldsymbol{W} = (w_i)$和$\boldsymbol{V} = (v_j)$，长度分别为$n_2$和$n_1$，其中$w_i \in Z_{\mathrm{p}}$，$v_j \in Z_{\mathrm{p}}$。为了表述的简洁，本文分别对身份$u$定义两个函数$F(u)$和$J(u)$，对消息$m$定义两个函数$K(m)$和$L(m)$，其表达形式为

$$F(u){=}a_0{+}\sum_{i=1}^{n_2} a_i u[i] - l_\mu k_\mu, J(u){=}w_0{+}\sum_{i=1}^{n_2} w_i u[i],$$
$$K(m){=}b_0{+}\sum_{i=1}^{n_1} b_i m[i] - l_m k_m,$$
$$L(m) = v_0 + \sum_{i=1}^{n_1} v_i m[i]$$

$\mathcal{F}$构造一些公共参数，表达形式为

$$\mu' = (g^{a^\lambda})^{a_0 - l_\mu k_\mu} g^{w_0}, \mu_i = (g^{a^\lambda})^{a_i} g^{w_i}, 1 \leq i \leq n_2,$$
$$v' = (g^{a^\lambda})^{b_0 - l_m k_m} g^{v_0}, v_i = (g^{a^\lambda})^{b_i} g^{v_i}, 1 \leq i \leq n_1$$

对于任意的身份u和消息m，可以得到：$V(m){=}v'\prod_{i=1}^{n_1} v_i{}^{m[i]}{=}(g^{a^\lambda})^{K(m)} g^{L(m)}$，$W(u){=}\mu' \prod_{i=1}^{n_2} \mu_i{}^{v[i]}{=}(g^{a^\lambda})^{F(u)} g^{J(u)}$，最终，$\mathcal{F}$将系统参数$\mathrm{PP} = \{G, G_{\mathrm{T}}, e, p, g_1, g_2, Z, H_1, H_2, U, M\}$发送给敌手$\mathcal{A}$。其中$M = (v', v_1, v_2, \cdots, v_{n_1})$、$U = (\mu', \mu_1, \mu_2, \cdots, \mu_{n_2})$。

询问阶段：$\mathcal{A}$发起适应性预言询问，挑战者$\mathcal{C}$对询问做出响应。

(1)密钥提取询问：$\mathcal{A}$生成一个用户的签密属性集合W_{s}和一个门限值k，$\mathcal{C}$提取发送者的私钥$\mathrm{sk}_{W_{\mathrm{s}}^*,k} = \mathrm{KeyExtraction}(\mathrm{pp}, \mathrm{mk}, W_{\mathrm{s}}^*, k)$并将它发送给$\mathcal{A}$。然后$\mathcal{A}$选择他的部分用户的解签密属性集合$W_{\mathrm{r}}$和一个门限值$d$，$\mathcal{C}$提取接收者的私钥$\mathrm{sk}_{W_{\mathrm{r}},d} = \mathrm{KeyExtraction}(\mathrm{pp}, \mathrm{mk}, W_{\mathrm{r}}, d)$并将它发送给$\mathcal{A}$。

(2)签密询问：$\mathcal{A}$选择一个消息m，一个加密属性集合W_e和一个门限值k，挑战者$\mathcal{C}$根据密钥提取算法提取出$\mathrm{sk}_{W_{\mathrm{s}}^*,k}$，然后发送询问结果给$\mathcal{A}$。

伪造阶段：最后，对于给定的身份$u^* = (u^*[1], u^*[2], \cdots, u^*[n_2])$和消息$m^* = (m^*[1], m^*[2], \cdots, m^*[n_1])$，攻击者输出了一个伪造的密文$\mathrm{CT}^* = (W_{\mathrm{e}}, \Gamma_{\mathrm{k},W_{\mathrm{s}}^*}^*(\cdot), \Omega'^*, X, C^*, \sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*)$。

如果$F(u^*) \neq 0 \bmod p$或$K(m^*) \neq 0 \bmod p$，则$\mathcal{F}$终止，否则$\mathcal{F}$就能解决上述的λ-DHE问题，根据解签密阶段，可以得到：$e(\sigma_3^*, \sigma_5^*)/e(V(m^*), \sigma_4^*) \cdot e(W(u^*), \sigma_2^*) \cdot e(\sigma_1^*, H_1(i)) = e(g_1, g_2)^\alpha$，因此，伪造的签密结果$\mathrm{CT}^*$是有效的。

证毕

5.2 自适应选择密文攻击下不可区分性

定理2　若DBDH困难问题成立，则本文所提签密方案满足适应性选择密文攻击不可区分性。

证明　设置系统参数λ，$d \in {}_R Z_q^*$，缺省属性集$\Omega = \{b+1, b+2, \cdots, b+d-1\}$，$\mathcal{A}$输出预挑战的用于签名的属性集合$\omega_1^*$以及门限$1 \leq k \leq d$，用于加密的属性集合$\omega_2^*$以及门限$1 \leq k' \leq d$，设签名谓词为$\Gamma_{k,\omega_1^*}(\cdot)$。挑战者$\mathcal{C}$随机选择缺省属性集$\Omega'^*_1 \subseteq \Omega$，$|\Omega'^*_1| = d-k$，$\Omega'^*_2 \subseteq \Omega$，$|\Omega'^*_2| = d-k'$。

初始化：$\mathcal{C}$设置$g_1 = g^x$，$g_2 = g^y$。

询问阶段1：$\mathcal{A}$创建列表L_U并初始化为空。

(1)H_1询问：如果对i进行H_1询问，$\mathcal{C}$检查L_U，如果能在L_U中找到i，则返回其对应的值；如果$i \in \omega_2^* \cup \Omega'^*_2$，选择$\beta_i{\in}_R Z_{\mathrm{p}}^*$，返回$H_1(i){=}g^{\beta_i}$,并记录

于L_U；否则，选择$\beta_i,\gamma_i\in_R Z_p^*$，返回$H_1(i)=g_1{}^{-\beta_i}g^{\gamma_i}$，并记录于$L_U$。

(2)密钥提取询问：如果对属性集ω_i，满足$|\omega_i\cap\omega_2^*|<k^{'}$，则进行私钥提取询问。定义3个集合$\Gamma$,$\Gamma$',$S$，满足$\Gamma=(\omega_i\cap\omega_2^*)\cup\Omega_i'$，$\Gamma\subseteq\Gamma'\subseteq S$，$|\Gamma'|=d-1$，$S=\Gamma'\cup\{0\}$。

对于$i\in\Gamma'$，挑战者$\mathcal{C}$令$D_i=(g_2^{t_i}H_1(i)^{r_i}W(u)^s, g^{r_i})$，其中$t_i,r_i\in_R Z_q^*$。相当于隐式选择了一个$d-1$次多项式$q(x)$，且$q(i)=t_i$，且$q(0)=\alpha$。对于$i\notin\Gamma'$，设$r_i=\dfrac{\Delta_{0,S}(i)}{\beta_i}y+r_i'$, $q(i)=\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)+\Delta_{0,S}(i)q(0)$，因为$g_2^{t_i}H_1(i)^{r_i}$·

$W(u)^s=g_2^{\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)+\Delta_{0,S}(i)q(0)}(g_1{}^{-\beta_i}g^{\gamma_i})^{\frac{\Delta_{0,S}(i)}{\beta_i}y+r_i'}$，$W(u)^s=g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}+\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)}(g_1^{-\beta_i}g^{\gamma_i})^{r_i'}$，$g^{r_i}=g^{\frac{\Delta_{0,S}(i)}{\beta_i}y+r_i'}=g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}}g^{r_i'}$，可以计算出$D_i=\{g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}+\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)}(g_1^{-\beta_i}g^{\gamma_i})^{r_i'}W(u)^s, g_2^{\frac{\Delta_{0,S}(i)}{\beta_i}}g^{r_i'}\}_{i\in\omega_i}$，所以对$\mathcal{A}$来说，$D_i$是一个合法的私钥。如果$|\omega_i\cap\omega_2^*|\geq k'$，则挑战者$\mathcal{C}$不能进行密钥提取询问。

(3)签密询问：$\mathcal{A}$请求在属性集合ω_A和谓词$\Gamma_{k,\omega_1^*}(\cdot)$，$\Gamma_{k,\omega_2^*}(\cdot)$下的消息$m$的签密询问。

如果$|\omega_A\cap\omega_2^*|<k'$，则$\mathcal{C}$通过密钥提取询问生成$\omega_A$的私钥$D_{Ai}=(d_{i0},d_{i1})$，并且按照签名算法产生密文并返回给$\mathcal{A}$。否则，$\mathcal{C}$从缺省属性集$\Omega$随机选择由$d-k$个元素构成的子集$\Omega_1'$，从属性集$\Omega$随机选取$d-k'$个缺省属性构成缺省属性集$\Omega_2'$，设$\omega_A\cup\Omega_1'=\{i_1,i_2,\cdots,i_d\}$，计算$c_i=m_i\oplus H_2(Y)$，因为$\mathcal{A}$不能对$\omega_B$，$|\omega_B\cap\omega_2^*|\geq k'$进行密钥提取询问，因此密文$c_i$对于敌手$\mathcal{A}$来说是合法的。

挑战：$\mathcal{C}$随机选择$c\in\{0,1\}$，选取k个属性构成的属性集$\omega_A^{'*}\subseteq\omega_1^*$，$\mathcal{C}$进行密钥提取询问，获得与$\omega_A^{'*}$相关的私钥$d_{i0},d_{i1}$，执行签密算法。

询问阶段2：与阶段1询问相同。不允许对ω_2^*进行密钥提取询问。

猜测：如果$c'=c$，敌手$\mathcal{A}$赢得游戏并输$c'\in\{0,1\}$，$\mathcal{A}$在游戏中获胜的优势为$\mathrm{Adv}(\mathcal{A})=|\mathrm{pr}[c=c']-\dfrac{1}{2}|$。

若对于多项式时间的敌手$\mathcal{A}$，$\mathrm{Adv}(\mathcal{A})$可忽略，则称方案满足自适应选择密文攻击下不可区分性安全。 证毕

5.3 签密者属性隐私安全性

定理3 本文所提签密方案满足签密者属性隐私安全性。

证明 根据本文的相关定义，对于本文所提出的方案隐私性的证明可以分为两部分。

首先，我们需要证明的是，如果只给定一个密文，任何人都不能区分出哪一个属性是被签名者用于签密过程的。$\mathcal{C}$选择系统参数PP并生成主密钥$\mathrm{mk}=\alpha$，攻击者选择一个默认的属性集Ω，两个属性子集ω_1和ω_2，并且让$\widehat{\omega_1}=\omega_1\cup\Omega$，$\widehat{\omega_2}=\omega_2\cup\Omega$。$\mathcal{C}$生成私钥$\mathrm{sk}_{i1}=\{g_1^s,g_2^{q(i)}H_1(i)^{r_i}W(u)^s,g^{r_i}\}$，$i\in\widehat{\omega_1}$和$\mathrm{sk}_{i2}=\{g_1^s,g_2^{q(i)}H_1(i)^{r_i}W(u)^s,g^{r_i}\}$，$i\in\widehat{\omega_2}$。然后攻击者输出消息$m^*$，属性子集$\omega^*=\{i_1,i_2,\cdots,i_k\}\subseteq\overline{\omega}$，$|\omega^*|\leq d$，并且请求$\mathcal{C}$在$\omega^*$下用$\mathrm{sk}_{i1}$或者$\mathrm{sk}_{i2}$对消息$m^*$进行签密。于是就可以得到密文$(X,C,\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$，在这里$i\in\omega_1'\cup\Omega'$，且$\omega_1'$是属于$\omega_1$的一个$k$阶子集，$\Omega'$是属于$\Omega$的一个$d-k$阶子集。所以根据拉格朗日插值定理，密文能够被私钥$\mathrm{sk}_{i1}$或者$\mathrm{sk}_{i2}$解密，但是攻击者不能分辨出密文是由哪个集合生成的。

其次，只有当云服务器和PKG联合起来，本文提出的方案才能够根据给出的签名获得签名者的真实身份，因为从$e(g_1,g_1^s)$到签名者ID的映射关系被存储在两个不同的表项里，这两个表分别被云服务器和PKG所持有，所以尽管任何人都可以根据追踪算法计算得到$e(g_1,g_1^s)$的值，但是他们却得不到签名者的ID。由此可见本文的方案满足签密者属性隐私安全性。 证毕

5.4 移动医疗社交网络的特点

移动医疗社交网络作为一个发展前景广阔的移动健康监测系统得到了越来越多的关注。本文所提的移动医疗社交网络与传统的医疗模式不同，移动医疗社交网络通过患者身上的可穿戴的无线感知节点来感知患者的健康信息，由无线传感基站进行数据收集，并将收集到的数据通过无线通信发送至患者的智能终端，最终由智能终端对数据进行整合、分析等操作。在此社交网络中的用户具有更好的移动性和社交性。

(1)移动性：假设每个用户都可以自由移动，比如可以出门散步等，这与传统的卧病在床的患者不同。正是由于其移动性，当附近有无线传感监测基站时，患者的健康信息就可以被收集。

(2)社交性：移动医疗社交网络为每个患者提供了社交的机会，在此社交网络中的患者或是活跃或是沉默。活跃的患者可能更乐于与其他具有相同病症的患者分享健康信息，彼此进行交流获得情感寄托和安慰。而沉默的患者也可能借此平台的机会更加积极乐观地接受治疗。

6 性能分析

签密算法相比于传统的签名和加密算法，在一定程度上减少了计算开销和通信开销。在本文所提

出的应用于医疗社交网络中的属性基签密方案，与其他属性基签密方案[14,15]相比，性能上有较明显的提升。对于本文方案、文献[14]方案和文献[15]方案，本节将从功能特性、计算开销和通信开销等方面进行比较。

6.1 功能特性分析

表1将本文与文献[14,15]进行对比，其中访问控制策略有访问树、线性秘密共享方案和门限策略。文献[14]方案运用线性秘密共享访问控制策略，在标准模型下证明了数据的机密性与不可伪造性，也实现了访问策略的隐藏，保护了个人电子病历的隐私性，但是文献[14]方案不能抵抗合谋攻击，存在一定的安全隐患。文献[15]方案提出应用于在线社交网络的属性基签密方案，同样在标准模型下证明了方案的机密性、完整性以及真实性，与文献[14]方案一样也不能抵抗合谋攻击。本文方案可以实现追踪性，当云服务器和PKG联合起来，本文方案能够根据给出的签名获得签名者的真实身份，这在一定程度上可以抵抗合谋攻击，因此本文方案更具功能性。

6.2 理论分析

以下从理论角度分析本文方案与文献[14]方案、文献[15]方案在计算开销和通信开销上的优劣。我们用T_e表示指数运算时间，T_h表示哈希函数运算时间，T_{p}表示执行双线性对映射的时间，T_{m}表示执行乘法运算的时间，$|N|$代表属性集合中属性的个数。

由表2可以看出，在密钥生成阶段，本文方案有多个指数运算，因为PKG要为数据拥有者和数据使用者生成不同的私钥，故在本阶段本文方案的计算效率略低于文献[14]方案和文献[15]方案。在签密和解签密阶段，本文方案效率更高，在解签密阶段，本文方案将一部分运算外包给云服务器进行，减轻了本地端数据用户的计算负担，故本文方案在实际应用中是有效的，对于资源受限的设备来说也是可扩展的，在一定程度上不会带来较大的计算负担。表3对文献[14]方案、文献[15]方案和本文方案进行了通信开销方面的对比，本文主要考虑以下阶段的通信开销：系统公钥生成阶段、系统主密钥生成阶段、用户私钥生成阶段以及加密密文阶段，并定义群G_1, G_{T}, Z_{p}^*中元素的长度为$|G|$, $|G_{\mathrm{T}}|$, $|Z_{\mathrm{r}}|$。在用户私钥生成阶段，随着属性个数的增加，每个方案的通信开销都有一定的增长。对于加密密文阶段的通信开销，由于文献[14]方案具有隐藏访问策略的特点，相对于其他两种方案具有更高的通信开销。

6.3 数值模拟

为了更准确评估方案的实际性能，本文使用PBC[21](Pairing-Based Cryptography)库在签密阶段和解签密阶段进行仿真测试。基于C语言进行编

表 1　功能特性比较

方案	访问控制策略	机密性	不可伪造性	安全模型	抗合谋攻击	其他特点
文献[14]方案	线性秘密共享	√	√	标准模型	×	隐藏访问策略
文献[15]方案	访问树	√	√	标准模型	×	无
本文方案	门限策略	√	√	随机预言机	√	可追踪

注：“×”表示不具有特定功能或未使用某种技术；“√”表示具有特定功能或使用某种技术

表 2　计算开销分析

阶段	文献[14]	文献[15]	本文方案
系统初始化	$3T_{\mathrm{e}}+T_{\mathrm{p}}$	$T_{\mathrm{e}}+\lvert N\rvert T_{\mathrm{m}}$	$2T_{\mathrm{e}}+T_{\mathrm{p}}$
密钥生成	$6T_{\mathrm{e}}+2\lvert N\rvert T_{\mathrm{h}}+2T_{\mathrm{m}}$	$(3\lvert N\rvert)T_{\mathrm{e}}+(\lvert N\rvert+1)T_{\mathrm{m}}$	$(6\lvert N\rvert+1)T_{\mathrm{e}}+2\lvert N\rvert T_{\mathrm{h}}$
签密	$(5\lvert N\rvert+6)T_{\mathrm{e}}+(2\lvert N\rvert+4)T_{\mathrm{m}}$	$(4\lvert N\rvert+4)T_{\mathrm{e}}+T_{\mathrm{p}}$	$8T_{\mathrm{e}}+(\lvert N\rvert+1)T_{\mathrm{h}}+T_{\mathrm{m}}$
解签密	$2\lvert N\rvert T_{\mathrm{e}}+3T_{\mathrm{h}}+\lvert N\rvert T_{\mathrm{m}}$	$(2\lvert N\rvert+1)T_{\mathrm{e}}+(4\lvert N\rvert+3)T_{\mathrm{p}}+T_{\mathrm{h}}$	$\lvert N\rvert T_{\mathrm{e}}+2\lvert N\rvert T_{\mathrm{p}}+T_{\mathrm{h}}$

表 3　通信开销分析

阶段	文献[14]	文献[15]	本文方案
系统公钥	$(\lvert N\rvert+5)\lvert Z_{\mathrm{r}}\rvert+(\lvert N\rvert+5)\lvert G\rvert+\lvert G_{\mathrm{T}}\rvert$	$(3\lvert N\rvert+4)\lvert G\rvert$	$2\lvert Z_{\mathrm{r}}\rvert+3\lvert G\rvert+4\lvert G_{\mathrm{T}}\rvert$
系统主密钥	$\lvert G\rvert$	$\lvert Z_{\mathrm{r}}\rvert+\lvert N\rvert\lvert G\rvert$	$\lvert Z_{\mathrm{r}}\rvert$
用户私钥	$(2\lvert N\rvert+1)\lvert G\rvert+\lvert N\rvert\lvert G_{\mathrm{T}}\rvert$	$2\lvert N\rvert(\lvert N\rvert+1)\lvert G\rvert$	$2\lvert Z_{\mathrm{r}}\rvert+(2\lvert N\rvert+1)\lvert G\rvert$
加密密文	$4\lvert Z_{\mathrm{r}}\rvert+(3\lvert N\rvert+3)\lvert G\rvert+(\lvert N\rvert+1)\lvert G_{\mathrm{T}}\rvert$	$5\lvert G\rvert+2(\lvert N\rvert+1)\lvert G_{\mathrm{T}}\rvert$	$4\lvert Z_{\mathrm{r}}\rvert+6\lvert G\rvert+(\lvert N\rvert+1)\lvert G_{\mathrm{T}}\rvert$

程，在联想笔记本电脑上，Linux操作系统下进行数值模拟。

在本文中，主要通过改变属性数目来测试方案。由图2可以看出，本文方案、文献[14]方案以及文献[15]方案在签密阶段的时间均随属性数目的增加而增长，但本文方案的时间增幅较缓，即随着属性数目的增加，本文方案较文献[14]方案和文献[15]方案更有优势。因此，对于云服务器处理大量数据而言，本文所提方案更能满足实际需求。由图3可以得出，本文方案在数据解签密阶段的运算效率高于文献[14]方案和文献[15]方案，3种方案在解签密阶段的时间开销随着属性数目的增加而增加，但本文方案的时间开销增幅较缓，其在实际应用中云服务器的响应时间更短，更有利于数据使用者访问数据。在解签密阶段，将一部分运算外包给云服务器进行，同时云服务器能够进行辅助验证，减少了大部分的计算开销，并且云服务器因其强大的存储能力，数据所有者可以减轻存储负担。最终可以看出，通过数值模拟得到的性能评估与上述理论分析的结果基本符合。

7 结束语

针对在医疗社交网络中存在的用户信息隐私保护的迫切需求，本文提出了一种基于属性的签密方案，在医疗社交网络平台下，用户可以最大化地增强彼此之间的联系和交流，以此来相互鼓舞，减轻彼此的精神压力，消除孤独感，实现了数据拥有者和数据使用者之间通信数据的机密性与完整性。同时该方案能够实现追踪的功能，云服务器的辅助验证减轻了数据拥有者的计算量。最后在随机预言模型下证明了该方案的安全性，通过与之前的属性基签密方案进行分析比较，本文方案在计算效率方面有更好的优势，同时更适用于医疗社交网络。

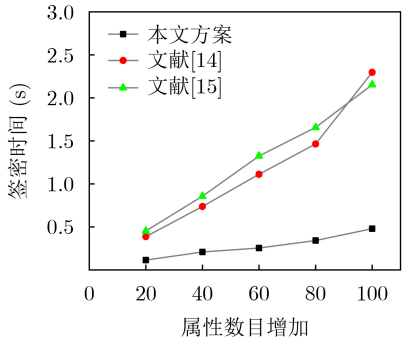

图 2 签密算法的时间成本

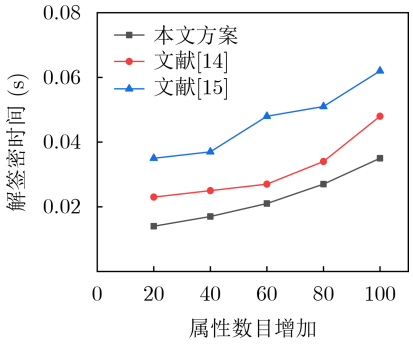

图 3 解签密算法的时间成本

参 考 文 献

[1] DENG Fuhu, WANG Yali, PENG Li, *et al*. Revocable cloud-assisted attribute-based signcryption in personal health system[J]. *IEEE Access*, 2019, 7: 120950–120960. doi: 10.1109/ACCESS.2019.2933636.

[2] ARFAOUI A, BOUDIA O R M, KRIBECHE A, *et al*. Context-aware access control and anonymous authentication in WBAN[J]. *Computers & Security*, 2020, 88: 101496. doi: 10.1016/j.cose.2019.03.017.

[3] XU Chang, WANG Jiachen, ZHU Liehuang, *et al*. Enabling privacy-preserving multi-level attribute based medical service recommendation in eHealthcare systems[J]. *Peer-to-Peer Networking and Applications*, 2021, 14(4): 1841–1853. doi: 10.1007/s12083-021-01075-9.

[4] 牛淑芬, 刘文科, 陈俐霞, 等. 基于代理重加密的电子病历数据共享方案[J]. 计算机工程, 2021, 47(6): 164–171. doi: 10.19678/j.issn.1000-3428.0058229.

NIU Shufen, LIU Wenke, CHEN Lixia, *et al*. Data sharing scheme of electronic medical record based on proxy Re-encryption[J] *Computer Engineering*, 2021, 47(6): 164–171. doi: 10.19678/j.issn.1000-3428.0058229.

[5] 聂旭云, 鲍阳阳, 孙剑飞, 等. 一个多授权中心的属性基签密方案[J]. 信息安全学报, 2018, 3(5): 15–24. doi: 10.19363/J.cnki.cn10-1380/tn.2018.09.02.

NIE Xuyun, BAO Yangyang, SUN Jianfei, *et al*. A multi-authority attribute-based signcryption scheme[J]. *Journal of Cyber Security*, 2018, 3(5): 15–24. doi: 10.19363/J.cnki.cn10-1380/tn.2018.09.02.

[6] SAHAI A and WATERS B. Fuzzy identity-based encryption[C]. The 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

[7] GE Chunpeng, SUSILO W, BAEK J, *et al*. Revocable attribute-based encryption with data integrity in clouds[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 19(5): 2864–2872. doi: 10.1109/TDSC.2021.3065999.

[8] 牛淑芬, 宋蜜, 方丽芝, 等. 智慧医疗中基于属性加密的云存储数据共享[J]. 电子与信息学报, 2022, 44(1): 107–117. doi: 10.11999/JEIT210858.

NIU Shufen, SONG Mi, FANG Lizhi, *et al*. Cloud storage data sharing based on attribute encryption in smart

healthcare[J]. *Journal of Electronics & Information Technology*, 2022, 44(1): 107–117. doi: 10.11999/JEIT210858.

[9] TU Shanshan, WAQAS M, HUANG Fengming, *et al*. A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing[J]. *Computer Networks*, 2021, 195: 108196. doi: 10.1016/J.COMNET.2021.108196.

[10] CHALLAGIDAD P S and BIRJE M N. Efficient multi-authority access control using attribute-based encryption in cloud storage[J]. *Procedia Computer Science*, 2020, 167: 840–849. doi: 10.1016/j.procs.2020.03.423.

[11] ZHENG Yuliang. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption)[C]. The 17th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 1997: 165–179. doi: 10.1007/BFb0052234.

[12] DENG Ningzhi, DENG Shaojiang, HU Chunqiang, *et al*. An efficient revocable attribute-based signcryption scheme with outsourced unsigncryption in cloud computing[J]. *IEEE Access*, 2020, 8: 42805–42815. doi: 10.1109/ACCESS.2019.2963233.

[13] LIU Suhui, CHEN Liquan, WANG Huaqun, *et al*. O3HSC: Outsourced online/offline hybrid signcryption for wireless body area networks[J]. *IEEE Transactions on Network and Service Management*, 2022, 19(3): 2421–2433. doi: 10.1109/TNSM.2022.3153485.

[14] MING Yang and ZHANG Tingting. Efficient privacy-preserving access control scheme in electronic health records system[J]. *Sensors*, 2018, 18(10): 3520. doi: 10.3390/s18103520.

[15] HAN Yiliang and LU Wanyi. Attribute based generalized signcryption for online social network[C]. 2015 34th Chinese Control Conference (CCC), Hangzhou, China, 2015: 6434–6439. doi: 10.1109/ChiCC.2015.7260653.

[16] LU Yanfei, WANG Xu, HU Chunqiang, *et al*. A traceable threshold attribute-based signcryption for mHealthcare social network[J]. *International Journal of Sensor Networks*, 2018, 26(1): 43–53. doi: 10.1504/IJSNET.2018.088384.

[17] BOUCHAALA M, GHAZEL C, and SAIDANE L A. TRAK-CPABE: A novel traceable, revocable and accountable ciphertext-policy attribute-based encryption scheme in cloud computing[J]. *Journal of Information Security and Applications*, 2021, 61: 102914. doi: 10.1016/j.jisa.2021.102914.

[18] BELGUITH S, KAANICHE N, HAMMOUDEH M, *et al*. PROUD: Verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IOT applications[J]. *Future Generation Computer Systems*, 2020, 111: 899–918. doi: 10.1016/j.future.2019.11.012.

[19] OBIRI I A, XIA Qi, XIA Hu, *et al*. Personal health records sharing scheme based on attribute based signcryption with data integrity verifiable[J]. *Journal of Computer Security*, 2022, 30(2): 291–324. doi: 10.3233/JCS-210045.

[20] YU Jiguo, LIU Suhui, WANG Shengling, *et al*. LH-ABSC: A lightweight hybrid attribute-based signcryption scheme for cloud-fog-assisted IoT[J]. *IEEE Internet of Things Journal*, 2020, 7(9): 7949–7966. doi: 10.1109/JIOT.2020.2992288.

[21] PBC Library. The pairing-based cryptography library[EB/OL]. http://crypto.stanford.edu/pbc/, 2015.

牛淑芬：女，博士，副教授，研究方向为云计算和大数据网络的隐私保护.

周思玮：女，硕士生，研究方向为网络与信息安全.

张美玲：女，硕士生，研究方向为网络与信息安全.

王彩芬：女，博士，教授，研究方向为密码学与信息安全.

责任编辑：马秀强