(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 11 月 15 日 (15.11.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/205263 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/084174

(22) 国际申请日: 2017 年 5 月 12 日 (12.05.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 深圳大学(SHENZHEN UNIVERSITY) [CN/CN]; 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。

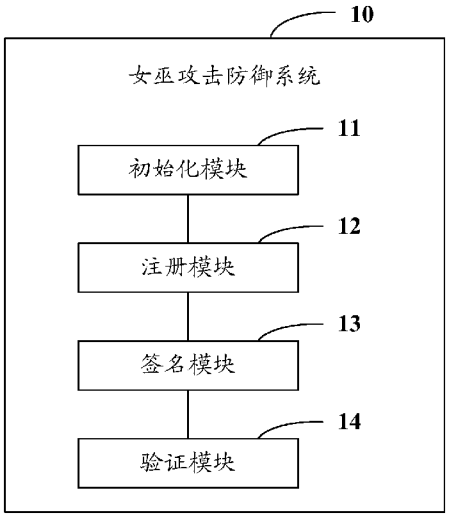
(72) 发明人: 张鹏(ZHANG, Peng); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。 喻建平(YU, Jianping); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。 张霞飞(ZHANG, Xiafei); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。

(74) 代理人: 深圳市恒申知识产权事务所(普通合伙) (HENSEN INTELLECTUAL PROPERTY FIRM); 中国广东省深圳市福田区南园路68号上步大厦10H, Guangdong 518000 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM,

(54) **Title:** SYBIL ATTACK DEFENSE METHOD AND SYSTEM

(54) 发明名称: 一种女巫攻击防御方法及其系统



10 Sybil attack defense system
11 Initialization module
12 Registration module
13 Signature module
14 Verification module

图 2

(57) **Abstract:** Provided are a Sybil attack defense method. The method comprises: an initialization step: according to a known security parameter λ and a global attribute set U, using the secret key generation center to operate a pre-set setting algorithm so as to generate a master secret key MSK = {S} and publish a public parameter pp; a registration step: submitting a registration application to the secret key generation center by means of the user, the secret key generation center operating a pre-set secret key generation algorithm to generate a user private key SKS, and distributing the user private key SKS to the user by means of a secret channel; a signature step: the user signing a signature by means of operating a pre-set signature algorithm; and a verification step: the user verifying, after signing a signature, the signature by means of operating a pre-set verification algorithm. Also provided is a Sybil attack defense system. The technical solution provided in the present invention can effectively defend a Sybil attack, so that data security is improved.

WO 2018/205263 A1

[见续页]

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本发明提供一种女巫攻击防御方法，其中，所述方法包括：初始化步骤：根据已知安全参数λ和全局属性集U，利用所述秘钥生成中心运行预设的设置算法以生成主密钥MSK＝{S}并公布公共参数pp；注册步骤：通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥SK_S，并通过秘密通道将所述用户私钥SK_S分发至所述用户；签名步骤：所述用户通过运行预设的签名算法进行签名；验证步骤：所述用户在签名后通过运行预设的验证算法对签名进行验证。本发明还提供一种女巫攻击防御系统。本发明提供的技术方案能有效防御女巫攻击，提高数据的安全性。

一种女巫攻击防御方法及其系统

技术领域

本发明涉及网络通信中的数据认证技术领域，尤其涉及一种女巫攻击防御方法及其系统。

背景技术

近年来，可穿戴智能设备日益普及，云计算发展趋于成熟，移动互联网用户规模逐年增长，大数据价值加速凸显，医疗服务由信息化向移动化、网络化发展，移动医疗网络逐渐形成。其中，可穿戴设备采集居民健康信息，并依托云平台对采集数据进行分析与处理，后提供至医院、医生进行健康监测与临床诊断。移动医疗网络能改善患者的就医体验，提高医生的诊断与治疗效率，降低医疗服务的社会成本，进而有效改善居民健康状况与社会医疗环境。

移动医疗网络可向用户提供社交网络服务，如转发健康信息、分享健身体验、交流治疗经历等。然而，移动医疗社交网络容易遭受恶意攻击。当一个攻击者伪装成多个合法用户的身份，或者非法声明多个伪造的用户身份时，社交网络遭受到女巫攻击。女巫攻击会降低网络性能、中断程序、篡改数据或恶意欺骗他人，因此会对移动医疗社交网络性能造成巨大的破坏。

在移动医疗健康社交网络中，不可避免的会向公众开放一些健康数据。与

此同时，由于存在的隐私泄露风险，用户不愿意再使用其真实身份互相交流。事实上，任何身份信息泄漏都可能侵犯用户隐私，甚至导致生命和财产损失。身份隐私保护使得防御女巫攻击变得更加困难。

发明内容

有鉴于此，本发明的目的在于提供一种女巫攻击防御方法及其系统，旨在解决现有技术中移动医疗社交网络容易受到女巫攻击的问题。

本发明提出一种女巫攻击防御方法，应用于由秘钥生成中心、云服务提供商、用户组成的移动医疗社交网络，其中，所述方法包括：

初始化步骤：根据已知安全参数λ和全局属性集U，利用所述秘钥生成中心运行预设的设置算法以生成主密钥$MSK=\{\mathbf{S}\}$并公布公共参数pp；

注册步骤：通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥SK_S，并通过秘密通道将所述用户私钥SK_S分发至所述用户；

签名步骤：所述用户通过运行预设的签名算法进行签名；

验证步骤：所述用户在签名后通过运行预设的验证算法对签名进行验证。

优选的，在所述初始化步骤中，所述设置算法为$Setup(\lambda,U)$算法，其中，运行预设的所述$Setup(\lambda,U)$算法的步骤具体包括：

输入所述安全参数λ和所述全局属性集$U=\{1,2,\ldots,t\}$，并定义缺省属性集$U^*=\{t+1,t+2,\ldots,2t\}$；

选择随机矩阵 $\mathbf{S}=(\mathbf{s}_1,\mathbf{s}_2)^t\in\mathcal{R}_{2q}^{2\times1}$ ；

挑选一个随机矩阵 $\mathbf{A}=(\mathbf{a},q-2)\in\mathcal{R}_{2q}^{1\times2}$ 使得 $\mathbf{AS}=q \bmod 2q$ ；

定义 ζ 使得 $\zeta\cdot(q-2)=1 \bmod 2q$ ；

计算 $\zeta\mathbf{A}=(\zeta\mathbf{a},1)$ 以及 $\zeta\mathbf{AS}=\zeta\mathbf{as}_1+\mathbf{s}_2=\zeta q \bmod 2q$ ；

输出主密钥 $MSK=\{\mathbf{S}\}$ 和公共参数 $PP=\{\mathbf{A},\zeta,U,U^*\}$ 。

优选的，在所述注册步骤中，所述秘钥生成算法为 $KeyGen(PP,MSK,S)$ 算法，其中，运行预设的所述 $KeyGen(PP,MSK,S)$ 算法的步骤具体包括：

随机选择 $t-1$ 次多项式 $f_j(x)\in\mathcal{R}_{2q}[x]$ 使得对于每个 j 都有 $f_j(0)=\mathbf{s}_j$ ；

对于每个 $i\in S\cup U^*$ ，令 $\mathbf{S}_i\leftarrow(f_1(i),f_2(i))^t\in\mathcal{R}_{2q}^{2\times1}$ ；

输出所述用户私钥 $SK_S=(\mathbf{AS}_i,i\in S\cup U^*)$ 。

优选的，在所述签名步骤中，所述签名算法为 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法，其中运行预设的所述 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法的步骤具体包括：

定义一个 k 元素的属性集 $S'\subseteq S\cap S^*$ ；

定义缺省属性集 $U'\subset U^*$ ，其中 $\left|U'\right|=t-k$ ；

对于 $i\in S^*\cup U'$ ，从标准差为 σ 的分布 $D_{\mathbb{Z}^n,\sigma}^n$ 选择 m 维向量 $\mathbf{y}_{1i},\mathbf{y}_{2i}$ ，定义 $\mathbf{Y}=(\mathbf{y}_{1i},\mathbf{y}_{2i})^t$ ，并计算 $\mathbf{u}_i=\zeta\mathbf{AY}=\zeta\cdot\mathbf{a}\cdot\mathbf{y}_{1i}+\mathbf{y}_{2i} \bmod 2q$ 以及 $\mathbf{c}=H([\sum_{i\in S^*\cup U'}\mathbf{Au}_i]_d \bmod p,\mu)$ ，其中， $p=[2q/2^d]$ ， $2q=p\cdot2^d+2q \bmod 2^d$ ；

当 $i\in S'\cup U'$ 时，计算 $\mathbf{z}_{1i}=\mathbf{A}((\Delta_1 f_1(i)\mathbf{c}+\mathbf{y}_{1i})$ ，当 $i\in S^*\setminus S'$ 时，计算 $\mathbf{z}_{1i}=\mathbf{Ay}_{1i}$ ，当 $i\in S'\cup U'$ 时，计算 $\mathbf{z}_{2i}=\mathbf{A}((\Delta_2 f_2(i)\mathbf{c}+\mathbf{y}_{2i})$ ，当 $i\in S^*\setminus S'$ 时，计算 $\mathbf{z}_{2i}=\mathbf{Ay}_{2i}$ ；

输出概率为 $1/(M\exp(\frac{-2\langle \mathbf{z}_i, \mathbf{S}_i\mathbf{c}\rangle + \|\mathbf{S}_i\mathbf{c}\|^2}{2\|\mathbf{A}\|^2\sigma^2}))$ ；

计算 $\mathbf{z}_{2i}^{\dagger} \leftarrow ([\mathbf{A}\mathbf{u}_i]_d - [\mathbf{A}\mathbf{u}_i - \mathbf{z}_{2i}]_d) \bmod p$ ；

输出签名 $Sig = (\{\mathbf{z}_{1i}, \mathbf{z}_{2i}^{\dagger}\}_{i\in S^*\cup U'}, \mathbf{c}\}$ 。

优选的，在所述验证步骤中，所述验证算法为 $Verify(PP, \mu, Sig, \gamma_{k,S^*}(\cdot))$ 算法，其中运行预设的所述 $Verify(PP, \mu, Sig, \gamma_{k,S^*}(\cdot))$ 算法的步骤具体包括：

输入用户 μ 的签名 $Sig = (\{\mathbf{z}_{1i}, \mathbf{z}_{2i}^{\dagger}\}_{i\in S^*\cup U'}, \mathbf{c}\}$ ，并定义 $\mathbf{B}$ 使得 $\mathbf{A} \bmod q = 2\mathbf{B}$ ；

如果 $\|\mathbf{z}_{1i} \| 2^d \cdot \mathbf{z}_{2i}^{\dagger}\| > \|\mathbf{B}\|$ ，则拒绝签名；

如果 $\|\mathbf{z}_{1i} \| 2^d \cdot \mathbf{z}_{2i}^{\dagger}\|_{\infty} > \|\mathbf{B}\|_{\infty}$ ，则拒绝签名；

如果 $\mathbf{c} = H([\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i} + \zeta\cdot q\cdot\mathbf{A}\cdot\mathbf{c}]_d + \sum_{i\in S^*\cup U'}\mathbf{z}_{2i}^{\dagger} \bmod p, \mu)$ ，则接受签名。

另一方面，本发明还提供一种女巫攻击防御系统，应用于由秘钥生成中心、云服务提供商、用户组成的移动医疗社交网络，其中，所述系统包括：

初始化模块，用于根据已知安全参数 λ 和全局属性集 U ，利用所述秘钥生成中心运行预设的设置算法以生成主密钥 $MSK = \{\mathbf{S}\}$ 并公布公共参数 pp ；

注册模块，用于通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥 SK_S ，并通过秘密通道将所述用户私钥 SK_S 分发至所述用户；

签名模块，用于所述用户通过运行预设的签名算法进行签名；

验证模块，用于所述用户在签名后通过运行预设的验证算法对签名进行验证。

优选的，所述设置算法为 $Setup(\lambda,U)$ 算法，其中，运行预设的所述 $Setup(\lambda,U)$ 算法的步骤具体包括：

输入所述安全参数 λ 和所述全局属性集 $U=\{1,2,\ldots,t\}$，并定义缺省属性集 $U^*=\{t+1,t+2,\ldots,2t\}$；

选择随机矩阵 $\mathbf{S}=(\mathbf{s}_1,\mathbf{s}_2)^t\in\mathcal{R}_{2q}^{2\times 1}$；

挑选一个随机矩阵 $\mathbf{A}=(\mathbf{a},q-2)\in\mathcal{R}_{2q}^{1\times 2}$ 使得 $\mathbf{AS}=q \bmod 2q$；

定义 ζ 使得 $\zeta\cdot(q-2)=1 \bmod 2q$；

计算 $\zeta\mathbf{A}=(\zeta\mathbf{a},1)$ 以及 $\zeta\mathbf{AS}=\zeta\mathbf{a}\mathbf{s}_1+\mathbf{s}_2=\zeta q \bmod 2q$；

输出主密钥 $MSK=\{\mathbf{S}\}$ 和公共参数 $PP=\{\mathbf{A},\zeta,U,U^*\}$。

优选的，所述秘钥生成算法为 $KeyGen(PP,MSK,S)$ 算法，其中，运行预设的所述 $KeyGen(PP,MSK,S)$ 算法的步骤具体包括：

随机选择 $t-1$ 次多项式 $f_j(x)\in\mathcal{R}_{2q}[x]$ 使得对于每个 j 都有 $f_j(0)=\mathbf{s}_j$；

对于每个 $i\in S\cup U^*$，令 $\mathbf{S}_i\leftarrow(f_1(i),f_2(i))^t\in\mathcal{R}_{2q}^{2\times 1}$；

输出所述用户私钥 $SK_S=(\mathbf{AS}_i,i\in S\cup U^*)$。

优选的，所述签名算法为 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法，其中运行预设的所述 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法的步骤具体包括：

定义一个 k 元素的属性集 $S'\subseteq S\cap S^*$；

定义缺省属性集 $U'\subset U^*$，其中 $\left|U'\right|=t-k$；

对于 $i\in S^*\cup U'$，从标准差为 σ 的分布 $D_{\mathbb{Z}^n,\sigma}^n$ 选择 m 维向量 $\mathbf{y}_{1i},\mathbf{y}_{2i}$，定义

$\mathbf{Y}=(\mathbf{y}_{1i},\mathbf{y}_{2i})^t$，并计算$\mathbf{u}_i=\zeta\mathbf{AY}=\zeta\cdot\mathbf{a}\cdot\mathbf{y}_{1i}+\mathbf{y}_{2i}\bmod 2q$以及$\mathbf{c}=H([\sum_{i\in S^*\cup U'}\mathbf{Au}_i]_d \bmod p,\mu)$，其中，$p=[2q/2^d]$，$2q=p\cdot 2^d+2q\bmod 2^d$；

当$i\in S'\cup U'$时，计算$\mathbf{z}_{1i}=\mathbf{A}((\Delta_1 f_1(i)\mathbf{c}+\mathbf{y}_{1i})$，当$i\in S^*\setminus S'$时，计算$\mathbf{z}_{1i}=\mathbf{Ay}_{1i}$，当$i\in S'\cup U'$时，计算$\mathbf{z}_{2i}=\mathbf{A}((\Delta_2 f_2(i)\mathbf{c}+\mathbf{y}_{2i})$，当$i\in S^*\setminus S'$时，计算$\mathbf{z}_{2i}=\mathbf{Ay}_{2i}$；

输出概率为$1/(M\exp(\frac{-2\langle\mathbf{z}_i,\mathbf{S}_i\mathbf{c}\rangle+\|\mathbf{S}_i\mathbf{c}\|^2}{2\|\mathbf{A}\|^2\sigma^2}))$；

计算$\mathbf{z}_{2i}^{\dagger}\leftarrow([\mathbf{Au}_i]_d-[\mathbf{Au}_i-\mathbf{z}_{2i}]_d)\bmod p$；

输出签名$Sig=(\{\mathbf{z}_{1i},\mathbf{z}_{2i}^{\dagger}\}_{i\in S^*\cup U'},\mathbf{c}\}$。

优选的，所述验证算法为$Verify(PP,\mu,Sig,\gamma_{k,S^*}(\cdot))$算法，其中运行预设的所述$Verify(PP,\mu,Sig,\gamma_{k,S^*}(\cdot))$算法的步骤具体包括：

输入用户μ的签名$Sig=(\{\mathbf{z}_{1i},\mathbf{z}_{2i}^{\dagger}\}_{i\in S^*\cup U'},\mathbf{c}\}$，并定义$\mathbf{B}$使得$\mathbf{A}\bmod q=2\mathbf{B}$；

如果$\|\mathbf{z}_{1i}\|2^d\cdot\mathbf{z}_{2i}^{\dagger}\|>\|\mathbf{B}\|$，则拒绝签名；

如果$\|\mathbf{z}_{1i}\|2^d\cdot\mathbf{z}_{2i}^{\dagger}\|_\infty>\|\mathbf{B}\|_\infty$，则拒绝签名；

如果$\mathbf{c}=H([\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i}+\zeta\cdot q\cdot\mathbf{A}\cdot\mathbf{c}]_d+\sum_{i\in S^*\cup U'}\mathbf{z}_{2i}^{\dagger}\bmod p,\mu)$，则接受签名。

本发明提供的技术方案适用于移动医疗社交网络，提出了一个匿名认证协议，该协议使用用户的多个属性而不是单个身份来访问服务，从而防止潜在的女巫攻击和身份隐私泄漏，提高数据的安全性。

附图说明

图 1 为本发明一实施方式中女巫攻击防御方法流程图；

图 2 为本发明一实施方式中女巫攻击防御系统 10 的内部结构示意图；

图 3 为本发明一实施方式中防御方案中的签名算法的运行时间示意图；

图 4 为本发明一实施方式中防御方案中的验证算法的运行时间示意图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

本发明具体实施方式提供了一种女巫攻击防御方法，应用于由秘钥生成中心、云服务提供商、用户组成的移动医疗社交网络，其中，所述方法包括：

初始化步骤：根据已知安全参数 λ 和全局属性集 U ，利用所述秘钥生成中心运行预设的设置算法以生成主密钥 $MSK=\{\mathbf{S}\}$ 并公布公共参数 pp；

注册步骤：通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥 SK_S ，并通过秘密通道将所述用户私钥 SK_S 分发至所述用户；

签名步骤：所述用户通过运行预设的签名算法进行签名；

验证步骤：所述用户在签名后通过运行预设的验证算法对签名进行验证。

本发明提供的一种女巫攻击防御方法，适用于移动医疗社交网络，提出了一个匿名认证协议，该协议使用用户的多个属性而不是单个身份来访问服务，从而防止潜在的女巫攻击和身份隐私泄漏，提高数据的安全性。

以下将对本发明所提供的一种女巫攻击防御方法进行详细说明。

请参阅图 1，为本发明一实施方式中女巫攻击防御方法流程图。

在本实施方式中，该女巫攻击防御方法应用于由秘钥生成中心（Key Generation Center，KGC）、云服务提供商（Cloud Server Provider，CSP）、用户（包括签名者和验证者）组成的移动医疗社交网络，通常，KGC 用于设置系统并发出私钥给合法用户，CSP 向用户提供医疗健康数据的存储服务，也是潜在的女巫攻击者篡改或伪造用户的健康数据，用户使用某些终端（例如智能手机，笔记本电脑等）和应用来定期访问社交平台，签名者是指想要分享存储在 CSP 中的健康数据的用户，验证者是指与签名者有社交关系的用户。

在步骤 S1 中，初始化步骤：根据已知安全参数λ和全局属性集U，利用所述秘钥生成中心运行预设的设置算法以生成主密钥$MSK=\{\mathbf{S}\}$并公布公共参数pp。在本实施方式中，初始化步骤用于建立注册系统。

在本实施方式中，在所述初始化步骤中，所述设置算法为$Setup(\lambda,U)$算法，其中，运行预设的所述$Setup(\lambda,U)$算法的步骤具体包括：

输入所述安全参数λ和所述全局属性集$U=\{1,2,\ldots,t\}$，并定义缺省属性集$U^{*}=\{t+1,t+2,\ldots,2t\}$；

选择随机矩阵$\mathbf{S}=(\mathbf{s}_1,\mathbf{s}_2)^{t}\in\mathcal{R}_{2q}^{2\times1}$；

挑选一个随机矩阵$\mathbf{A}=(\mathbf{a},q-2)\in\mathcal{R}_{2q}^{1\times2}$使得$\mathbf{AS}=q \bmod 2q$；

定义ζ使得$\zeta\cdot(q-2)=1 \bmod 2q$；

计算 $\zeta\mathbf{A}=(\zeta\mathbf{a},1)$ 以及 $\zeta\mathbf{AS}=\zeta\mathbf{as}_1+\mathbf{s}_2=\zeta q \bmod 2q$ ；

输出主密钥 $MSK=\{\mathbf{S}\}$ 和公共参数 $PP=\{\mathbf{A},\zeta,U,U^*\}$。

在步骤 S2 中，注册步骤：通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥 SK_S，并通过秘密通道将所述用户私钥 SK_S 分发至所述用户。

在本实施方式中，如果一个具有属性集 S 的合法用户（如病人或医生）想访问社交平台，则必须执行此操作。

在本实施方式中，在所述注册步骤中，所述秘钥生成算法为 $KeyGen(PP,MSK,S)$ 算法，其中，运行预设的所述 $KeyGen(PP,MSK,S)$ 算法的步骤具体包括：

随机选择 $t-1$ 次多项式 $f_j(x)\in\mathcal{R}_{2q}[x]$ 使得对于每个 j 都有 $f_j(0)=\mathbf{s}_j$ ；

对于每个 $i\in S\cup U^*$，令 $\mathbf{S}_i\leftarrow(f_1(i),f_2(i))^t\in\mathcal{R}_{2q}^{2\times1}$ ；

输出所述用户私钥 $SK_S=(\mathbf{AS}_i,i\in S\cup U^*)$。

在步骤 S3 中，签名步骤：所述用户通过运行预设的签名算法进行签名。

在本实施方式中，假设医生具有属性集 S 的私钥 SK_S，例如“医院 A，儿科，主任医师”，为了防御女巫攻击和保护身份隐私，医生运行 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法来证明他是一个有效的用户。在本实施方式中，设 d 是我们想要在 $\mathbb{Z}_2$ 中降低的位数，为了减少签名的长度，本发明引入 x 的高阶位 $[x]_d$，本发明定义在长度为 n 和权重为 k 的二进制向量集合 $\mathbb{B}_k^n$ 上具有均匀输出的哈希函数 H，为了证明签

名者在属性集S^*中至少拥有k个属性，签名者执行$Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$算法。

在本实施方式中，在所述签名步骤中，所述签名算法为$Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$算法，其中运行预设的所述$Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$算法的步骤具体包括：

定义一个k元素的属性集$S^{'}\subseteq S\cap S^*$；

定义缺省属性集$U^{'}\subset U^*$，其中$\left|U^{'}\right|=t-k$；

对于$i\in S^*\cup U^{'}$，从标准差为σ的分布$D^n_{\mathbb{Z}^n,\sigma}$选择$m$维向量$\mathbf{y}_{1i},\mathbf{y}_{2i}$，定义$\mathbf{Y}=(\mathbf{y}_{1i},\mathbf{y}_{2i})^t$，并计算$\mathbf{u}_i=\zeta\mathbf{AY}=\zeta\cdot\mathbf{a}\cdot\mathbf{y}_{1i}+\mathbf{y}_{2i}\bmod 2q$以及$\mathbf{c}=H([\sum_{i\in S^*\cup U^{'}}\mathbf{Au}_i]_d\bmod p,\mu)$，其中，$p=[2q/2^d]$，$2q=p\cdot 2^d+2q\bmod 2^d$；

当$i\in S^{'}\cup U^{'}$时，计算$\mathbf{z}_{1i}=\mathbf{A}((\Delta_1 f_1(i)\mathbf{c}+\mathbf{y}_{1i})$，当$i\in S^*\setminus S^{'}$时，计算$\mathbf{z}_{1i}=\mathbf{Ay}_{1i}$，当$i\in S^{'}\cup U^{'}$时，计算$\mathbf{z}_{2i}=\mathbf{A}((\Delta_2 f_2(i)\mathbf{c}+\mathbf{y}_{2i})$，当$i\in S^*\setminus S^{'}$时，计算$\mathbf{z}_{2i}=\mathbf{Ay}_{2i}$；

输出概率为$1/(M\exp(\frac{-2\langle\mathbf{z}_i,\mathbf{S}_i\mathbf{c}\rangle+\|\mathbf{S}_i\mathbf{c}\|^2}{2\|\mathbf{A}\|^2\sigma^2}))$；

计算$\mathbf{z}^{\dagger}_{2i}\leftarrow([\mathbf{Au}_i]_d-[\mathbf{Au}_i-\mathbf{z}_{2i}]_d)\bmod p$；

输出签名$Sig=(\{\mathbf{z}_{1i},\mathbf{z}^{\dagger}_{2i}\}_{i\in S^*\cup U^{'}},\mathbf{c}\}$。

在本实施方式中，$Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$算法中使用的私钥与医生的属性而不是他的身份有关，所以他的身份隐私被保护免于泄漏。同时，随着访问结构的使用和公开，身份合法性得到保证。

在步骤S4中，验证步骤：所述用户在签名后通过运行预设的验证算法对签名进行验证。

在本实施方式中，在所述验证步骤中，所述验证算法为$Verify(PP,\mu,Sig,\gamma_{k,S^*}(\cdot))$

算法，其中运行预设的所述$Verify(PP,\mu,Sig,\gamma_{k,S^*}(\cdot))$算法的步骤具体包括：

输入用户μ的签名$Sig=(\{\mathbf{z}_{1i},\mathbf{z}_{2i}^{\dagger}\}_{i\in S^*\cup U'},\mathbf{c}\}$，并定义$\mathbf{B}$使得$\mathbf{A}\bmod q=2\mathbf{B}$；

如果$\left\|\mathbf{z}_{1i}\|2^d\cdot\mathbf{z}_{2i}^{\dagger}\right\|>\|\mathbf{B}\|$，则拒绝签名；

如果$\left\|\mathbf{z}_{1i}\|2^d\cdot\mathbf{z}_{2i}^{\dagger}\right\|_{\infty}>\|\mathbf{B}\|_{\infty}$，则拒绝签名；

如果$\mathbf{c}=H([\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i}+\zeta\cdot q\cdot\mathbf{A}\cdot\mathbf{c}]_d+\sum_{i\in S^*\cup U'}\mathbf{z}_{2i}^{\dagger}\bmod p,\mu)$，则接受签名。

在本实施方式中，如签名通过验证，签名者的属性满足访问结构中定义的策略，所以验证者认为签名者是合法的。否则签名者的属性可能不能满足访问结构，或者有女巫攻击者篡改或伪造信息，所以验证者应该拒绝它。

在本实施方式中，签名的正确性验证描述如下：

$$\sum_{i\in S^*\cup U'}(\mathbf{Au}_i-\mathbf{z}_{2i})]_d$$

$$=[\sum_{i\in S^*\cup U'}(\zeta\cdot\mathbf{A}\cdot\mathbf{a}\cdot\mathbf{y}_{1i}-\mathbf{Ay}_{2i}-(\Delta_2 f_2(i)\mathbf{Ac}-\mathbf{Ay}_{2i})]_d$$

$$=[\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{Ay}_{1i}-\sum_{i\in S'\cup U'}\Delta_2 f_2(i)\cdot\mathbf{Ac}]_d$$

$$=[\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i}-\sum_{i\in S'\cup U'}(\zeta\cdot\mathbf{a}\cdot\Delta_1 f_1(i)+\Delta_2 f_2(i))\cdot\mathbf{Ac})]_d$$

$$=[(\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i}-\zeta\cdot\mathbf{AS}\cdot\mathbf{Ac})]_d$$

$$=[(\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i}-\zeta\cdot q\cdot\mathbf{Ac})]_d$$

因此，

$$[\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i}+\zeta\cdot q\cdot\mathbf{A}\cdot\mathbf{c}]_d+\sum_{i\in S^*\cup U'}\mathbf{z}_{2i}^{\dagger}\bmod p$$

$$=([\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i}+\zeta\cdot q\cdot\mathbf{A}\cdot\mathbf{c}]_d+\sum_{i\in S^*\cup U'}[\mathbf{Au}_i]_d-[\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^*\cup U'}\mathbf{z}_{1i}+\zeta\cdot q\cdot\mathbf{Ac}]_d)\bmod p$$

$$=[\sum_{i\in S^*\cup U'}\mathbf{Au}_i]_d\bmod p。$$

本发明提供的一种女巫攻击防御方法，适用于移动医疗社交网络，提出了一个匿名认证协议，该协议使用用户的多个属性而不是单个身份来访问服务，

从而防止潜在的女巫攻击和身份隐私泄漏，提高数据的安全性。

本发明具体实施方式还提供一种女巫攻击防御系统 10，应用于由秘钥生成中心、云服务提供商、用户组成的移动医疗社交网络，其中，所述系统包括：

初始化模块 11，用于根据已知安全参数 和全局属性集 ，利用所述秘钥生成中心运行预设的设置算法以生成主密钥 并公布公共参数 pp；

注册模块 12，用于通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥 ,并通过秘密通道将所述用户私钥 分发至所述用户；

签名模块 13，用于所述用户通过运行预设的签名算法进行签名；

验证模块 14，用于所述用户在签名后通过运行预设的验证算法对签名进行验证。

本发明提供的一种女巫攻击防御系统 10，适用于移动医疗社交网络，提出了一个匿名认证协议 ,该协议使用用户的多个属性而不是单个身份来访问服务，从而防止潜在的女巫攻击和身份隐私泄漏，提高数据的安全性。

请参阅图 2，所示为本发明一实施方式中女巫攻击防御系统 10 的结构示意图。

在本实施方式中，女巫攻击防御系统 10，主要包括初始化模块 11、注册模块 12、签名模块 13 和验证模块 14。

初始化模块 11，用于根据已知安全参数λ和全局属性集U，利用所述秘钥

生成中心运行预设的设置算法以生成主密钥 $MSK=\{\mathbf{S}\}$ 并公布公共参数 pp。

在本实施方式中，所述设置算法为 $Setup(\lambda,U)$ 算法，其中，运行预设的所述 $Setup(\lambda,U)$ 算法的步骤具体包括：

输入所述安全参数 λ 和所述全局属性集 $U=\{1,2,\ldots,t\}$，并定义缺省属性集 $U^*=\{t+1,t+2,\ldots,2t\}$；

选择随机矩阵 $\mathbf{S}=(\mathbf{s}_1,\mathbf{s}_2)^t\in\mathcal{R}_{2q}^{2\times1}$；

挑选一个随机矩阵 $\mathbf{A}=(\mathbf{a},q-2)\in\mathcal{R}_{2q}^{1\times2}$ 使得 $\mathbf{AS}=q \bmod 2q$；

定义 ζ 使得 $\zeta\cdot(q-2)=1 \bmod 2q$；

计算 $\zeta\mathbf{A}=(\zeta\mathbf{a},1)$ 以及 $\zeta\mathbf{AS}=\zeta\mathbf{as}_1+\mathbf{s}_2=\zeta q \bmod 2q$；

输出主密钥 $MSK=\{\mathbf{S}\}$ 和公共参数 $PP=\{\mathbf{A},\zeta,U,U^*\}$。

注册模块 12，用于通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥 SK_S，并通过秘密通道将所述用户私钥 SK_S 分发至所述用户。

在本实施方式中，所述秘钥生成算法为 $KeyGen(PP,MSK,S)$ 算法，其中，运行预设的所述 $KeyGen(PP,MSK,S)$ 算法的步骤具体包括：

随机选择 $t-1$ 次多项式 $f_j(x)\in\mathcal{R}_{2q}[x]$ 使得对于每个 j 都有 $f_j(0)=\mathbf{s}_j$；

对于每个 $i\in S\cup U^*$，令 $\mathbf{S}_i\leftarrow(f_1(i),f_2(i))^t\in\mathcal{R}_{2q}^{2\times1}$；

输出所述用户私钥 $SK_S=(\mathbf{AS}_i,i\in S\cup U^*)$。

签名模块 13，用于所述用户通过运行预设的签名算法进行签名。

在本实施方式中，所述签名算法为 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法，其中运行预设的所述 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法的步骤具体包括：

定义一个 k 元素的属性集 $S^{'}\subseteq S\cap S^*$ ；

定义缺省属性集 $U^{'}\subset U^*$ ，其中 $\left|U^{'}\right|=t-k$ ；

对于 $i\in S^*\cup U^{'}$ ，从标准差为 σ 的分布 $D^n_{\mathbb{Z}^n,\sigma}$ 选择 m 维向量 $\mathbf{y}_{1i},\mathbf{y}_{2i}$ ，定义 $\mathbf{Y}=(\mathbf{y}_{1i},\mathbf{y}_{2i})^t$ ，并计算 $\mathbf{u}_i=\zeta\mathbf{AY}=\zeta\cdot\mathbf{a}\cdot\mathbf{y}_{1i}+\mathbf{y}_{2i}\bmod 2q$ 以及 $\mathbf{c}=H([\sum_{i\in S^*\cup U^{'}}\mathbf{Au}_i]_d\bmod p,\mu)$ ，其中， $p=[2q/2^d]$ ， $2q=p\cdot 2^d+2q\bmod 2^d$ ；

当 $i\in S^{'}\cup U^{'}$ 时，计算 $\mathbf{z}_{1i}=\mathbf{A}((\Delta_1 f_1(i)\mathbf{c}+\mathbf{y}_{1i})$ ，当 $i\in S^*\setminus S^{'}$ 时，计算 $\mathbf{z}_{1i}=\mathbf{Ay}_{1i}$ ，当 $i\in S^{'}\cup U^{'}$ 时，计算 $\mathbf{z}_{2i}=\mathbf{A}((\Delta_2 f_2(i)\mathbf{c}+\mathbf{y}_{2i})$ ，当 $i\in S^*\setminus S^{'}$ 时，计算 $\mathbf{z}_{2i}=\mathbf{Ay}_{2i}$ ；

输出概率为 $1/(M\exp(\frac{-2\langle\mathbf{z}_i,\mathbf{S}_i\mathbf{c}\rangle+\|\mathbf{S}_i\mathbf{c}\|^2}{2\|\mathbf{A}\|^2\sigma^2}))$ ；

计算 $\mathbf{z}^{\dagger}_{2i}\leftarrow([\mathbf{Au}_i]_d-[\mathbf{Au}_i-\mathbf{z}_{2i}]_d)\bmod p$ ；

输出签名 $Sig=(\{\mathbf{z}_{1i},\mathbf{z}^{\dagger}_{2i}\}_{i\in S^*\cup U^{'}},\mathbf{c}\}$ 。

验证模块 14，用于所述用户在签名后通过运行预设的验证算法对签名进行验证。

在本实施方式中，所述验证算法为 $Verify(PP,\mu,Sig,\gamma_{k,S^*}(\cdot))$ 算法，其中运行预设的所述 $Verify(PP,\mu,Sig,\gamma_{k,S^*}(\cdot))$ 算法的步骤具体包括：

输入用户 μ 的签名 $Sig=(\{\mathbf{z}_{1i},\mathbf{z}^{\dagger}_{2i}\}_{i\in S^*\cup U^{'}},\mathbf{c}\}$ ，并定义 $\mathbf{B}$ 使得 $\mathbf{A}\bmod q=2\mathbf{B}$ ；

如果 $\left\|\mathbf{z}_{1i}\|2^d\cdot\mathbf{z}^{\dagger}_{2i}\right\|>\|\mathbf{B}\|$ ，则拒绝签名；

如果 $\left\|\mathbf{z}_{1i}\|2^d\cdot\mathbf{z}^{\dagger}_{2i}\right\|_\infty>\|\mathbf{B}\|_\infty$ ，则拒绝签名；

如果 $\mathbf{c} = H([\zeta \cdot \mathbf{a} \cdot \sum_{i \in S^* \cup U'} \mathbf{z}_{1i} + \zeta \cdot q \cdot \mathbf{A} \cdot \mathbf{c}]_d + \sum_{i \in S^* \cup U'} \mathbf{z}_{2i}^{\dagger} \bmod p, \mu)$ ，则接受签名。

本发明提供的一种女巫攻击防御系统 10，适用于移动医疗社交网络，提出了一个匿名认证协议，该协议使用用户的多个属性而不是单个身份来访问服务，从而防止潜在的女巫攻击和身份隐私泄漏，提高数据的安全性。

本发明提出的女巫攻击防御方案，可以通过仿真分析防御方案的效率，详细的仿真环境描述如下：操作系统是 Ubuntu 12.04，具有英特尔(R)Core(TM) i5-3210M 四核 CPU 处理器，运行速度为 2.50 GHz，内存为 1.6 GB。本发明的程序使用 GMP 6.0.0 大数字库和 NTL 6.0.0 库进行矩阵运算，通过 C ++编程语言在 GCC 平台上实现。为方便起见，本发明将安全参数 λ 设置为 128 位比特和 160 位比特。实验中使用的属性数量为 $l = \{3,5,8\}$。每个测试有 100 次迭代并取其平均值。

其中，表 1 描述了本发明防御方案的参数设置情况，图 3 和图 4 分别显示了本发明防御方案的签名算法和验证算法的运行时间。

表 1　本发明防御方案参数设置

安全参数 λ	128 比特	160 比特
(n, q)	(512,12289)	(512,12289)
主私钥密度 δ_1, δ_2	0.3,0	0.42,0.03
高斯分布标准差 σ	215.73	250.54
$\mathbf{z}_2$ 中丢弃的比特数 d	10	9
验证门限值 B_2, B_∞	12872,2100	16206,1760

值得注意的是，上述实施例中，所包括的各个单元只是按照功能逻辑进行

划分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本发明的保护范围。

另外，本领域普通技术人员可以理解实现上述各实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，相应的程序可以存储于一计算机可读取存储介质中，所述的存储介质，如 ROM/RAM、磁盘或光盘等。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种女巫攻击防御方法，应用于由秘钥生成中心、云服务提供商、用户组成的移动医疗社交网络，其特征在于，所述方法包括：

初始化步骤：根据已知安全参数λ和全局属性集U，利用所述秘钥生成中心运行预设的设置算法以生成主密钥$MSK=\{\mathbf{S}\}$并公布公共参数pp；

注册步骤：通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥SK_S，并通过秘密通道将所述用户私钥SK_S分发至所述用户；

签名步骤：所述用户通过运行预设的签名算法进行签名；

验证步骤：所述用户在签名后通过运行预设的验证算法对签名进行验证。

2. 如权利要求 1 所述的女巫攻击防御方法，其特征在于，在所述初始化步骤中，所述设置算法为$Setup(\lambda,U)$算法，其中，运行预设的所述$Setup(\lambda,U)$算法的步骤具体包括：

输入所述安全参数λ和所述全局属性集$U=\{1,2,\ldots,t\}$，并定义缺省属性集$U^*=\{t+1,t+2,\ldots,2t\}$；

选择随机矩阵$\mathbf{S}=(\mathbf{s}_1,\mathbf{s}_2)^t\in\mathcal{R}_{2q}^{2\times1}$；

挑选一个随机矩阵$\mathbf{A}=(\mathbf{a},q-2)\in\mathcal{R}_{2q}^{1\times2}$使得$\mathbf{AS}=q \bmod 2q$；

定义ζ使得$\zeta\cdot(q-2)=1 \bmod 2q$；

计算$\zeta\mathbf{A}=(\zeta\mathbf{a},1)$以及$\zeta\mathbf{AS}=\zeta\mathbf{as}_1+\mathbf{s}_2=\zeta q \bmod 2q$；

输出主密钥 $MSK=\{\mathbf{S}\}$ 和公共参数 $PP=\{\mathbf{A},\zeta,U,U^*\}$。

3. 如权利要求 2 所述的女巫攻击防御方法，其特征在于，在所述注册步骤中，所述秘钥生成算法为 $KeyGen(PP,MSK,S)$ 算法，其中，运行预设的所述 $KeyGen(PP,MSK,S)$ 算法的步骤具体包括：

随机选择 $t-1$ 次多项式 $f_j(x)\in\mathcal{R}_{2q}[x]$ 使得对于每个 j 都有 $f_j(0)=\mathbf{s}_j$；

对于每个 $i\in S\cup U^*$，令 $\mathbf{S}_i\leftarrow(f_1(i),f_2(i))^t\in\mathcal{R}_{2q}^{2\times1}$；

输出所述用户私钥 $SK_S=(\mathbf{AS}_i,i\in S\cup U^*)$。

4. 如权利要求 3 所述的女巫攻击防御方法，其特征在于，在所述签名步骤中，所述签名算法为 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法，其中运行预设的所述 $Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$ 算法的步骤具体包括：

定义一个 k 元素的属性集 $S'\subseteq S\cap S^*$；

定义缺省属性集 $U'\subset U^*$，其中 $\left|U'\right|=t-k$；

对于 $i\in S^*\cup U'$，从标准差为 σ 的分布 $D^n_{\mathbb{Z}^n,\sigma}$ 选择 m 维向量 $\mathbf{y}_{1i},\mathbf{y}_{2i}$，定义 $\mathbf{Y}=(\mathbf{y}_{1i},\mathbf{y}_{2i})^t$，并计算 $\mathbf{u}_i=\zeta\mathbf{AY}=\zeta\cdot\mathbf{a}\cdot\mathbf{y}_{1i}+\mathbf{y}_{2i}\bmod 2q$ 以及 $\mathbf{c}=H([\sum_{i\in S^*\cup U'}\mathbf{Au}_i]_d\bmod p,\mu)$，其中，$p=[2q/2^d]$，$2q=p\cdot2^d+2q\bmod2^d$；

当 $i\in S'\cup U'$ 时，计算 $\mathbf{z}_{1i}=\mathbf{A}((\Delta_1 f_1(i)\mathbf{c}+\mathbf{y}_{1i})$，当 $i\in S^*\setminus S'$ 时，计算 $\mathbf{z}_{1i}=\mathbf{Ay}_{1i}$，当 $i\in S'\cup U'$ 时，计算 $\mathbf{z}_{2i}=\mathbf{A}((\Delta_2 f_2(i)\mathbf{c}+\mathbf{y}_{2i})$，当 $i\in S^*\setminus S'$ 时，计算 $\mathbf{z}_{2i}=\mathbf{Ay}_{2i}$；

输出概率为 $1/(M\exp(\dfrac{-2\langle\mathbf{z}_i,\mathbf{S}_i\mathbf{c}\rangle+\|\mathbf{S}_i\mathbf{c}\|^2}{2\|\mathbf{A}\|^2\sigma^2}))$；

计算 $\mathbf{z}_{2i}^{\dagger}\leftarrow([\mathbf{Au}_i]_d-[\mathbf{Au}_i-\mathbf{z}_{2i}]_d)\bmod p$；

输出签名 $Sig=(\{\mathbf{z}_{1i},\mathbf{z}_{2i}^{\dagger}\}_{i\in S^{*}\cup U'},\mathbf{c}\}$。

5. 如权利要求 4 所述的女巫攻击防御方法，其特征在于，在所述验证步骤中，所述验证算法为 $Verify(PP,\mu,Sig,\gamma_{k,S^{*}}(\cdot))$ 算法，其中运行预设的所述 $Verify(PP,\mu,Sig,\gamma_{k,S^{*}}(\cdot))$ 算法的步骤具体包括：

输入用户 μ 的签名 $Sig=(\{\mathbf{z}_{1i},\mathbf{z}_{2i}^{\dagger}\}_{i\in S^{*}\cup U'},\mathbf{c}\}$，并定义 $\mathbf{B}$ 使得 $\mathbf{A}\bmod q=2\mathbf{B}$；

如果 $\left\|\mathbf{z}_{1i}\,\|\,2^{d}\cdot\mathbf{z}_{2i}^{\dagger}\right\|>\|\mathbf{B}\|$，则拒绝签名；

如果 $\left\|\mathbf{z}_{1i}\,\|\,2^{d}\cdot\mathbf{z}_{2i}^{\dagger}\right\|_{\infty}>\|\mathbf{B}\|_{\infty}$，则拒绝签名；

如果 $\mathbf{c}=H([\zeta\cdot\mathbf{a}\cdot\sum_{i\in S^{*}\cup U'}\mathbf{z}_{1i}+\zeta\cdot q\cdot\mathbf{A}\cdot\mathbf{c}]_{d}+\sum_{i\in S^{*}\cup U'}\mathbf{z}_{2i}^{\dagger}\bmod p,\mu)$，则接受签名。

6. 一种女巫攻击防御系统，应用于由秘钥生成中心、云服务提供商、用户组成的移动医疗社交网络，其特征在于，所述系统包括：

初始化模块，用于根据已知安全参数 λ 和全局属性集 U，利用所述秘钥生成中心运行预设的设置算法以生成主密钥 $MSK=\{\mathbf{S}\}$ 并公布公共参数 pp；

注册模块，用于通过所述用户向所述秘钥生成中心提交注册申请，由所述秘钥生成中心运行预设的秘钥生成算法来生成用户私钥 SK_S，并通过秘密通道将所述用户私钥 SK_S 分发至所述用户；

签名模块，用于所述用户通过运行预设的签名算法进行签名；

验证模块，用于所述用户在签名后通过运行预设的验证算法对签名进行验证。

7. 如权利要求 6 所述的女巫攻击防御系统，其特征在于，所述设置算法为

$Setup(\lambda,U)$算法，其中，运行预设的所述$Setup(\lambda,U)$算法的步骤具体包括：

输入所述安全参数λ和所述全局属性集$U=\{1,2,\ldots,t\}$，并定义缺省属性集$U^*=\{t+1,t+2,\ldots,2t\}$；

选择随机矩阵$\mathbf{S}=(\mathbf{s}_1,\mathbf{s}_2)^t\in\mathcal{R}_{2q}^{2\times1}$；

挑选一个随机矩阵$\mathbf{A}=(\mathbf{a},q-2)\in\mathcal{R}_{2q}^{1\times2}$使得$\mathbf{AS}=q \bmod 2q$；

定义ζ使得$\zeta\cdot(q-2)=1 \bmod 2q$；

计算$\zeta\mathbf{A}=(\zeta\mathbf{a},1)$以及$\zeta\mathbf{AS}=\zeta\mathbf{a}\mathbf{s}_1+\mathbf{s}_2=\zeta q \bmod 2q$；

输出主密钥$MSK=\{\mathbf{S}\}$和公共参数$PP=\{\mathbf{A},\zeta,U,U^*\}$。

8. 如权利要求7所述的女巫攻击防御系统，其特征在于，所述秘钥生成算法为$KeyGen(PP,MSK,S)$算法，其中，运行预设的所述$KeyGen(PP,MSK,S)$算法的步骤具体包括：

随机选择$t-1$次多项式$f_j(x)\in\mathcal{R}_{2q}[x]$使得对于每个$j$都有$f_j(0)=\mathbf{s}_j$；

对于每个$i\in S\cup U^*$，令$\mathbf{S}_i\leftarrow(f_1(i),f_2(i))^t\in\mathcal{R}_{2q}^{2\times1}$；

输出所述用户私钥$SK_S=(\mathbf{AS}_i,i\in S\cup U^*)$。

9. 如权利要求8所述的女巫攻击防御系统，其特征在于，所述签名算法为$Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$算法，其中运行预设的所述$Sign(PP,SK_S,\mu,\gamma_{k,S^*}(\cdot))$算法的步骤具体包括：

定义一个k元素的属性集$S'\subseteq S\cap S^*$；

定义缺省属性集$U'\subset U^*$，其中$\left|U'\right|=t-k$；

对于 $i \in S^* \cup U'$ ，从标准差为 σ 的分布 $D^n_{\mathbb{Z}^n,\sigma}$ 选择 m 维向量 $\mathbf{y}_{1i}, \mathbf{y}_{2i}$ ，定义 $\mathbf{Y} = (\mathbf{y}_{1i}, \mathbf{y}_{2i})^t$ ，并计算 $\mathbf{u}_i = \zeta \mathbf{AY} = \zeta \cdot \mathbf{a} \cdot \mathbf{y}_{1i} + \mathbf{y}_{2i} \bmod 2q$ 以及 $\mathbf{c} = H([\sum_{i \in S^* \cup U'} \mathbf{Au}_i]_d \bmod p, \mu)$ ，其中， $p = [2q / 2^d]$ ， $2q = p \cdot 2^d + 2q \bmod 2^d$ ；

当 $i \in S' \cup U'$ 时，计算 $\mathbf{z}_{1i} = \mathbf{A}((\Delta_1 f_1(i)\mathbf{c} + \mathbf{y}_{1i})$ ，当 $i \in S^* \setminus S'$ 时，计算 $\mathbf{z}_{1i} = \mathbf{Ay}_{1i}$ ，当 $i \in S' \cup U'$ 时，计算 $\mathbf{z}_{2i} = \mathbf{A}((\Delta_2 f_2(i)\mathbf{c} + \mathbf{y}_{2i})$ ，当 $i \in S^* \setminus S'$ 时，计算 $\mathbf{z}_{2i} = \mathbf{Ay}_{2i}$ ；

输出概率为 $1/(M \exp(\frac{-2\langle \mathbf{z}_i, \mathbf{S}_i\mathbf{c}\rangle + \|\mathbf{S}_i\mathbf{c}\|^2}{2\|\mathbf{A}\|^2 \sigma^2}))$ ；

计算 $\mathbf{z}^\dagger_{2i} \leftarrow ([\mathbf{Au}_i]_d - [\mathbf{Au}_i - \mathbf{z}_{2i}]_d) \bmod p$ ；

输出签名 $Sig = (\{\mathbf{z}_{1i}, \mathbf{z}^\dagger_{2i}\}_{i \in S^* \cup U'}, \mathbf{c}\}$ 。

10. 如权利要求 9 所述的女巫攻击防御系统，其特征在于，所述验证算法为 $Verify(PP, \mu, Sig, \gamma_{k,S^*}(\cdot))$ 算法，其中运行预设的所述 $Verify(PP, \mu, Sig, \gamma_{k,S^*}(\cdot))$ 算法的步骤具体包括：

输入用户 μ 的签名 $Sig = (\{\mathbf{z}_{1i}, \mathbf{z}^\dagger_{2i}\}_{i \in S^* \cup U'}, \mathbf{c}\}$ ，并定义 $\mathbf{B}$ 使得 $\mathbf{A} \bmod q = 2\mathbf{B}$ ；

如果 $\|\mathbf{z}_{1i} \| 2^d \cdot \mathbf{z}^\dagger_{2i}\| > \|\mathbf{B}\|$ ，则拒绝签名；

如果 $\|\mathbf{z}_{1i} \| 2^d \cdot \mathbf{z}^\dagger_{2i}\|_\infty > \|\mathbf{B}\|_\infty$ ，则拒绝签名；

如果 $\mathbf{c} = H([\zeta \cdot \mathbf{a} \cdot \sum_{i \in S^* \cup U'} \mathbf{z}_{1i} + \zeta \cdot q \cdot \mathbf{A} \cdot \mathbf{c}]_d + \sum_{i \in S^* \cup U'} \mathbf{z}^\dagger_{2i} \bmod p, \mu)$ ，则接受签名。

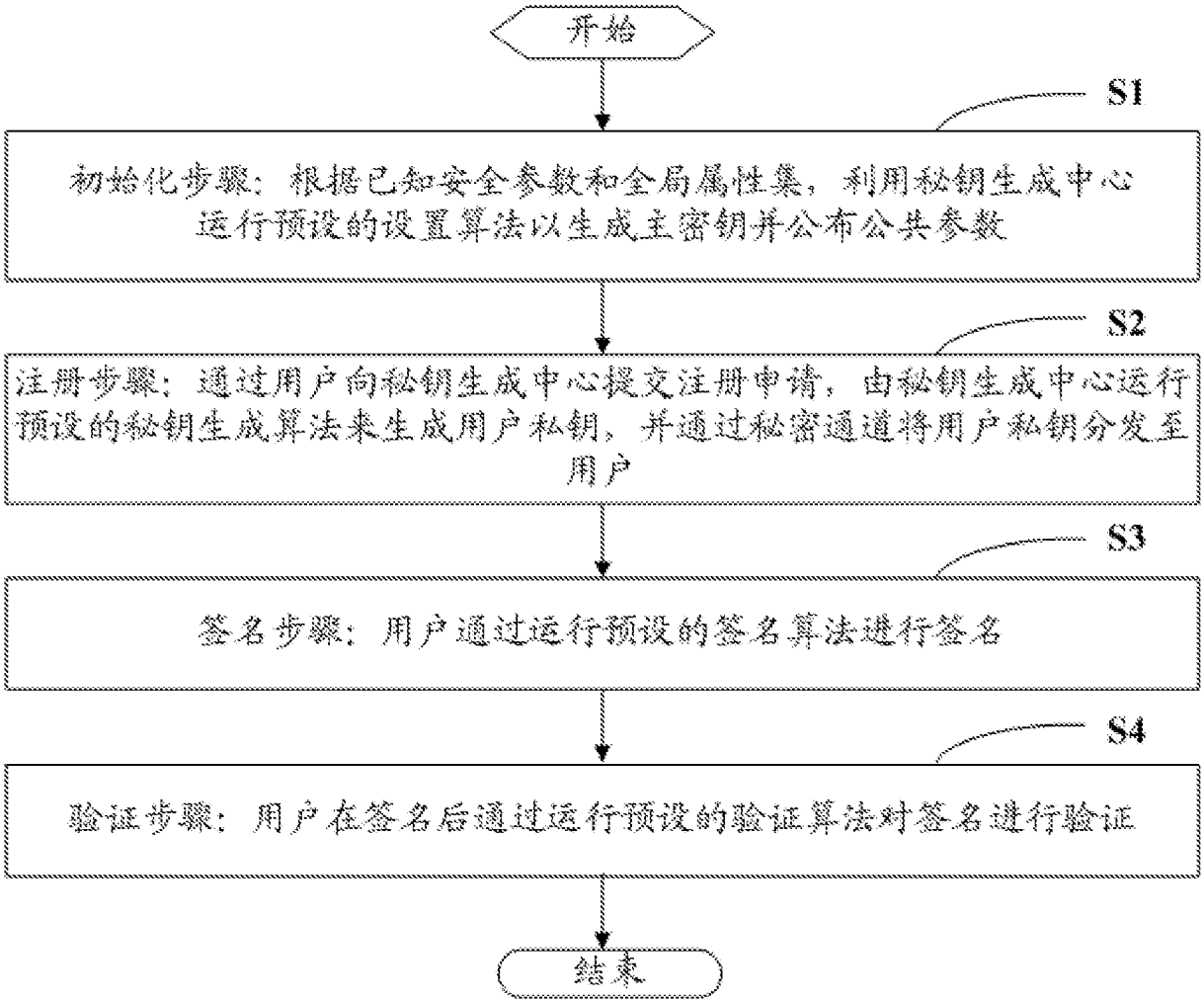

开始
S1
初始化步骤：根据已知安全参数和全局属性集，利用私钥生成中心运行预设的设置算法以生成主密钥并公布公共参数
S2
注册步骤：通过用户向私钥生成中心提交注册申请，由私钥生成中心运行预设的私钥生成算法来生成用户私钥，并通过私密通道将用户私钥分发至用户
S3
签名步骤：用户通过运行预设的签名算法进行签名
S4
验证步骤：用户在签名后通过运行预设的验证算法对签名进行验证
结束

图 1

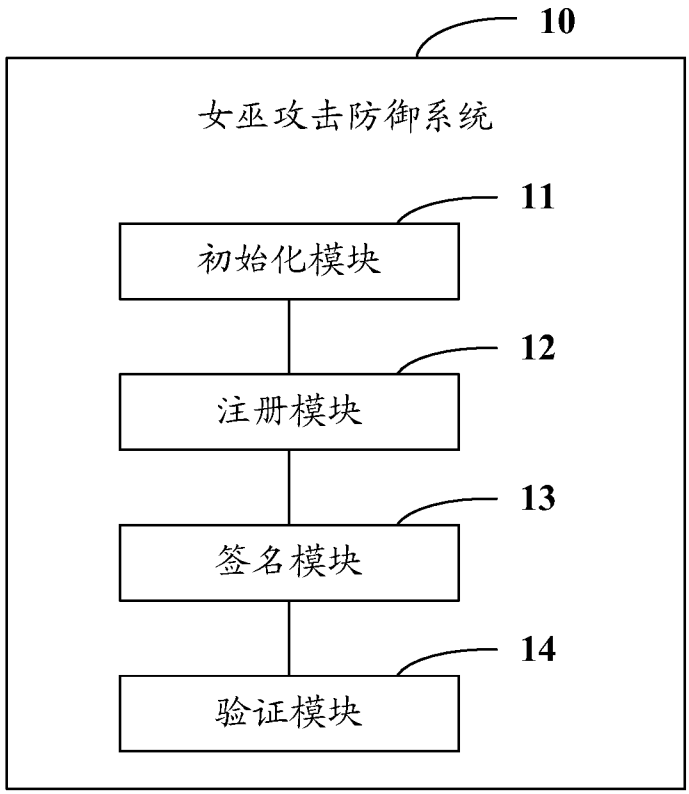


图 2

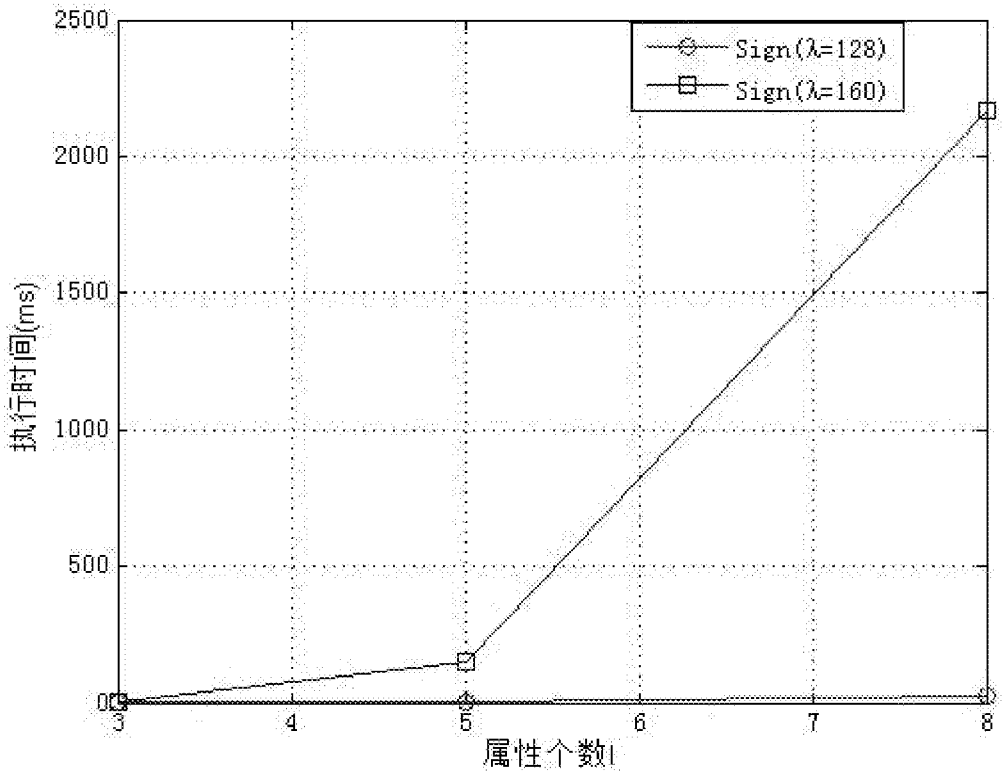

Sign(λ=128)
Sign(λ=160)
2500
2000
1500
1000
500
0
执行时间(ms)
3
4
5
6
7
8
属性个数l

图 3

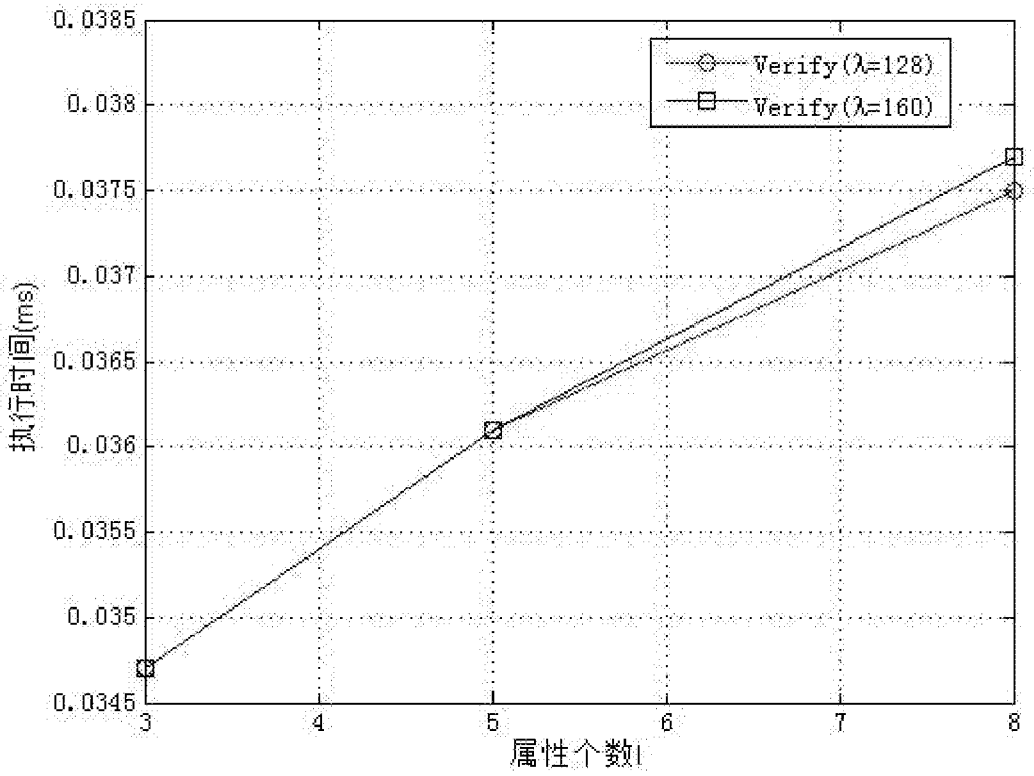

0.0385
0.038
0.0375
0.037
0.0365
0.036
0.0355
0.035
0.0345
执行时间(ms)
3
4
5
6
7
8
属性个数l
Verify(λ=128)
Verify(λ=160)

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/084174

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, IEEE: 女巫, 攻击, 防御, 医疗, 网络, 私钥, 主密钥, 公钥, 参数, 属性, 签名, 验证, 认证, sybil, attack, anti, defense, healthcare, network, master, secret, private, key, public, parameter, attribute, signature, verify, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	CN 107172042 A (SHENZHEN UNIVERSITY), 15 September 2017 (15.09.2017), claims 1-10	1-10
Y	CN 105897742 A (BEIHANG UNIVERSITY), 24 August 2016 (24.08.2016), description, paragraphs 0031-0067	1, 6
Y	CN 104158661 A (ENGINEERING UNIVERSITY OF CAPF), 19 November 2014 (19.11.2014), description, paragraphs 0058-0101	1, 6
A	CN 104506532 A (BEIJING BUSINESS INTELLIGENCE AND COMMUNICATIONS TECH CO., LTD. et al.), 08 April 2015 (08.04.2015), entire document	1-10
A	CHANG, Wei et al. "Sybil Defenses in Mobile Social Networks", 2013 IEEE Global Communications Conference (GLOBECOM), 12 June 2014 (12.06.2014), sections 2-3	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2018	01 February 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer JIN, Jing Telephone No. (86-10) 62414098

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/084174

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 107172042 A	15 September 2017	None	
CN 105897742 A	24 August 2016	None	
CN 104158661 A	19 November 2014	None	
CN 104506532 A	08 April 2015	None	

国际检索报告

国际申请号
PCT/CN2017/084174

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC,IEEE:女巫，攻击，防御，医疗，网络，私钥，主密钥，公钥，参数，属性，签名，验证，认证，sybil, attack, anti, defense, healthcare, network, master, secret, private, key, public, parameter, attribute, signature, verify, authentication

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
E	CN 107172042 A (深圳大学) 2017年 9月 15日 (2017-09-15) 权利要求1-10	1-10
Y	CN 105897742 A (北京航空航天大学) 2016年 8月 24日 (2016-08-24) 说明书第0031-0067段	1,6
Y	CN 104158661 A (中国人民武装警察部队工程大学) 2014年 11月 19日 (2014-11-19) 说明书第0058-0101段	1,6
A	CN 104506532 A (北京智捷伟讯科技有限公司等) 2015年 4月 8日 (2015-04-08) 全文	1-10
A	CHANG, Wei et al. "Sybil Defenses in Mobile Social Networks;" 2013 IEEE Global Communications Conference (GLOBECOM);, 2014年 6月 12日 (2014-06-12), 第2-3节	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 1月 18日	2018年 2月 1日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	靳晶
传真号 (86-10)62019451	电话号码 (86-10)62414098

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/084174

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 107172042 A	2017年 9月 15日	无	
CN 105897742 A	2016年 8月 24日	无	
CN 104158661 A	2014年 11月 19日	无	
CN 104506532 A	2015年 4月 8日	无	