**专利名称：一种支持位置隐私保护的双向匿名认证方案**

**申请人 ：南京邮电大学**

**发明人：柯昌博、朱泽江**

**第一发明人身份证号：**

本发明公开了一种支持位置隐私保护的双向匿名认证方案，解决了智能医疗环境中身份安全和位置隐私泄露的问题。该方案可以使患者用户匿名检查医疗雾节点的合法性，也可以使医疗雾节点匿名检查患者用户的合法性，同时在雾节点端和用户端对数据进行保护，避免敌手模拟患者用户提供虚假的数据，以及防止敌手修改雾节点中的报告内容。考虑到患者用户在发生紧急状况时需要向医疗中心报告自己的地理位置，以得到及时的救助。本发明利用可信中心TC对用户的地理位置信息进行匿名加密，让只有通过身份认证的医疗雾节点才能正确解密用户的真实地理位置信息，避免了在传输数据的过程中患者用户隐私位置信息被泄露。



1.一种支持位置隐私保护的双向匿名认证方案，包括以下步骤：

步骤 1）系统初始化，本发明通过第三方可信中心TC来管理和引导整个系统的运行，首先选取随机数作为私钥，并计算公钥，之后选取三个阶数为*q*的乘法循环群和用以构造双线性对。同时引入JPBC函数库，调用函数来生成系统参数，之后将系统参数发送给所有经过注册的用户智能终端和雾节点设备。

步骤 2）设备注册，用户将自己的真实身份和地理位置的经纬坐标GC发送给可信中心TC，TC接收到后计算其私钥和公钥，之后选取随机数计算用户的匿名身份及其对应的跟踪参数，最后将追踪列表和系统参数返回给用户。雾节点将自己的真实身份发送给可信中心TC，TC接收到后在计算其私钥和公钥，之后选取随机数计算雾节点的匿名身份及其对应的跟踪参数，接着选择两个安全加密密钥用来加密和解密位置经纬坐标，最后将追踪列表和返回给雾节点。

步骤 3）用户匿名认证，用户需要生成匿名的身份证书（AIC）来向对应的雾节点证明其合法性，生成后需要对其进行哈希加密，得到加密结果，之后结合当前的时间戳，计算匿名认证消息。为防止用户的匿名认证消息被敌手攻击并篡改，需要通过计算匿名签名来对认证消息进行签名操作，然后用户将签名过后的认证消息发送给雾节点。雾节点接收到后，首先对签名进行验证以保证认证消息的完整性，之后利用中的伪装认证参数还原出真实的认证参数，并计算用户的身份令牌。最后将和中的进行比较，如果两者相等，则雾节点认为发送认证消息的用户为可信用户，否则认证失败。

步骤 4）雾节点匿名认证，为生成匿名认证消息，雾节点首先利用匿名身份以及对应的跟踪参数计算认证参数，在参数计算完成后，利用公钥，匿名身份和系统参数通过哈希加密计算得到身份令牌。之后雾节点将结合当前的时间戳发送给用户，当用户在时刻接收到匿名认证消息后，首先检查时间戳和的差值以防止敌手的重试攻击，之后计算来验证雾节点的合法性。

步骤 5）位置隐私加密，为保护用户的位置隐私安全，可信中心TC不能直接向可信雾节点返回用户的真实坐标，TC需要对真实的坐标信息进行加密，并由雾节点端进行解密。首先用户向可信中心提交自己的真实地理坐标，之后利用匿名身份和追踪参数计算身份参数，在雾节点通过匿名身份认证后，将加密后的身份参数发送给雾节点。雾节点将接收到的身份参数转发给可信中心TC，TC从中还原出用户的身份，并其对应的地理坐标加密后返回给雾节点。最后，雾节点利用密钥还原出真实地理坐标。

其中所述步骤1）具体如下：

步骤11）可信中心TC选取一个安全参数*C*，通过运行生成器生成双线性参数*,,G,,*，其中*G*和均为循环群，为循环群*G*的阶数，为循环群*G*的生成元，示一种映射关系。

步骤 12）选取随机数作为主密钥，随机数作为私钥。之后可信中心TC计算对应的公钥，以及认证参数。最终可信中心TC选取一个安全的哈希加密函数，并发布系统参数。

所述步骤 2）具体如下：

步骤21）用户将自己的真实身份和地理位置的经纬坐标GC同过安全的加密通道（如SSL协议）发送给可信中心TC，TC在接收到后选择一个随机数，并计算该用户的私钥，以及对应的公钥。

步骤 22）可信中心TC为用户生成匿名身份来保护用户的真实身份信息，使得敌手在认证过程中即使捕获到该认证消息也无法获取用户真正的身份信息。

步骤 23）可信中心TC为用户的匿名身份生成跟踪参数，并与该用户的私钥、公钥和匿名身份组成跟踪列表存储到本地进行维护。例如可信中心TC可以对信誉度低的用户跟踪列表进行删除。

步骤 24）可信中心TC计算用户真实身份的哈希结果，并利用该结果对跟踪列表进行异或加密得到。之后将加密结果通过安全传输通道返回给用户，用户接收到后通过计算还原出跟踪列表。

步骤 25）雾节点将自己的真实身份通过安全加密通道发送给可信中心TC，TC收到雾节点的注册请求后选取一个随机数，计算其私钥以及对应的公钥。

步骤 26）可信中心TC为雾节点生成匿名身份及其跟踪参数，并将参数作为跟踪列表保存在本地进行管理。

步骤 27）可信中心TC为雾节点选择两个安全加密密钥用来加密和解密认证用户的隐私位置经纬坐标，其中。

步骤 28）可信中心TC计算雾节点真实身份的哈希结果，并利用该结果对跟踪列表和安全密钥进行异或加密。之后将加密结果通过安全传输通道返回给雾节点，雾节点接收到后通过计算还原出跟踪列表和密钥。

所述步骤 3）具体如下：

步骤 31）用户的智能终端首先选取四个随机数作为加密密钥，并计算身份认证参数，其中为用户的短生命周期私钥，为其对应的公钥。然后对进行哈希加密结算得到身份令牌，同时计算伪装身份认证参数。接着利用伪装身份认证参数计算匿名身份证书，并对进行哈希加密得到结果。最后结合当前的时间戳，计算匿名认证消息。

步骤 32）为防止用户的匿名认证消息被敌手攻击并篡改，需要对进行签名操作。用户的智能终端利用密钥和的哈希加密结果计算其匿名签名，然后将发送给雾节点。在雾节点接收到后，利用消息中的哈希加密结果、公钥和签名计算，如果等式成立，则雾节点认为该认证消息是完整的并接收，否则将拒绝。

步骤 33）雾节点在验证完匿名认证消息的完整性后，首先检查接收到的时间戳和当前的时间戳的差值以防止敌手的重试攻击，其中是双方约定的时间延迟。然后雾节点分别利用装身份认证参数以及公钥还原出真实的认证参数，计算，，。被计算完成后，接着计算，之后比较是否等于接收到的，如果相等，则雾节点认为发送认证消息的用户为可信用户。

所述步骤 4）具体如下：

步骤 41) 为生成雾节点的匿名身份证书，雾节点首先利用匿名身份以及对应的跟踪参数计算参数。在参数计算完成后，利用公钥，匿名身份和系统参数通过哈希加密计算身份令牌。

步骤 42）雾节点生成匿名认证消息，并将和当前的时间戳发送给用户，当用户在时刻接收到匿名认证消息后，首先检查时间戳和的差值以防止敌手的重试攻击，之后计算来验证雾节点的合法性。

步骤 43）用户计算的=，如果等式成立，则与匿名认证消息中的相等，并认为该雾节点为可信节点。

所述步骤 5）具体如下所示：

步骤 51）用户利用匿名身份和追踪参数计算身份参数，并利用私钥对身份参数进行加密，得到加密结果。当雾节点通过匿名身份认证后，用户将发送给雾节点。

步骤 52）雾节点利用自己的匿名身份将发送给可信中心TC，可信中心TC接收到后计算，得到用户的匿名身份。

步骤 53）可信中心TC通过用户的匿名身份找到本地存储的对应经纬坐标之后利用雾节点的加密密钥，计算加密参数。然后选择两个随机数，使满足，。

步骤 54）可信中心TC利用加密参数和随机数生成匿名坐标，其中，。然后将匿名坐标返回给雾节点。

步骤 55）雾节点在接收到匿名坐标后，利用本地的加密密钥计算，还原出真实的经纬坐标。

**一种支持隐私保护的双向匿名认证方案**

**技术领域**

本发明提出一种在智能医疗中支持保护患者用户位置隐私的双向匿名认证方案，属于雾计算、隐私保护和身份认证等交叉技术领域。

**背景技术**

随着无线技术的不断发展，各种可穿戴设备和智能移动终端通过蓝牙、WIFI等技术组成了用户的个人身体局域网络（WBANs）。这些低功耗的医疗传感器收集患者的血压、心跳、脉搏等实时生理信息，然后通过数据接收器等移动设备将信息发送到远程医疗雾服务器。这些远程医疗雾服务器由医疗中心部署在患者用户的周围，医生可以通过医疗雾节点中的数据为用户进行远程诊断或者及时提供医疗救治。由于用户的智能移动终端和医疗雾节点中存放着用户的敏感身体信息（BI），因此隐私保护对患者来说是一个重要的问题。为保证BI在存储和传输过程中的私密性和安全性，需要一种支持对用户和雾节点匿名保护的双向认证方案来验证数据接收和发送方的合法性。

目前国内外研究者对匿名认证协议的研究大多是在现有的安全协议基础上进行改进和优化，包括协议的灵活性、高效性、节能性和隐私保护等。其中主要的技术原理包括双线性映射、椭圆曲线加密（ECC）和数字签名等。

椭圆曲线密码系统和双线性映射技术可以构造基于伪装身份的匿名认证方法，采用匿名通信的方式可以隐藏敏感节点的身份信息，从而实现节点位置的隐私保护。另外，在智能医疗环境中，通过双向的匿名认证可以使患者用户验证医疗雾节点的合法性的同时，同样允许医疗雾节点验证用户的合法性，实现了隐私数据的双向保护。

数字签名是一种基于哈希算法和非对称加密算法实现的数据保护技术，数字签名的主要目的是保证数据接受者能够确认数据来源的准确性和数据本身的完整性。其本质特征是只有签名者使用自己的私钥以及其他私有信息才能生成签名。数字签名流程由签署和验证两个部分组成，可以用五元组表示。其中元素表示签名消息，元素表示签名集合，元素表示有限密钥空间，元素表示验证算法，元素表示签署算法。

基于上述研究成果，本发明针对智能医疗中患者用户的位置和身份隐私保护问题，提出一种支持位置隐私保护的双向匿名认证方案，旨在帮助用户得到安全可靠的医疗雾计算服务。

**发明内容**

**技术问题：**发明所要解决的技术问题是设计一种支持位置隐私保护的双向匿名认证方案，以有效地降低智能医疗网络中患者隐私数据泄露的风险。

**技术方案：**本发明的一种支持位置隐私保护的双向匿名认证方案包括以下步骤：

步骤 1）系统初始化，本发明通过第三方可信中心TC来管理和引导整个系统的运行，首先选取随机数作为私钥，并计算公钥，之后选取三个阶数为*q*的乘法循环群和用以构造双线性对。同时引入JPBC函数库，调用函数来生成系统参数，之后将系统参数发送给所有经过注册的用户智能终端和雾节点设备。

步骤 2）设备注册，用户将自己的真实身份和地理位置的经纬坐标GC发送给可信中心TC，TC接收到后计算其私钥和公钥，之后选取随机数计算用户的匿名身份及其对应的跟踪参数，最后将追踪列表和系统参数返回给用户。雾节点将自己的真实身份发送给可信中心TC，TC接收到后在计算其私钥和公钥，之后选取随机数计算雾节点的匿名身份及其对应的跟踪参数，接着选择两个安全加密密钥用来加密和解密位置经纬坐标，最后将追踪列表和返回给雾节点。

步骤 3）用户匿名认证，用户需要生成匿名的身份证书（AIC）来向对应的雾节点证明其合法性，生成后需要对其进行哈希加密，得到加密结果，之后结合当前的时间戳，计算匿名认证消息。为防止用户的匿名认证消息被敌手攻击并篡改，需要通过计算匿名签名来对认证消息进行签名操作，然后用户将签名过后的认证消息发送给雾节点。雾节点接收到后，首先对签名进行验证以保证认证消息的完整性，之后利用中的伪装身份认证参数还原出真实的认证参数，并计算用户的身份令牌。最后将和中的进行比较，如果两者相等，则雾节点认为发送认证消息的用户为可信用户，否则认证失败。

步骤 4）雾节点匿名认证，为生成匿名认证消息，雾节点首先利用匿名身份以及对应的跟踪参数计算认证参数，在参数计算完成后，利用公钥，匿名身份和系统参数通过哈希加密计算得到身份令牌。之后雾节点将结合当前的时间戳发送给用户，当用户在时刻接收到匿名认证消息后，首先检查时间戳和的差值以防止敌手的重试攻击，之后计算来验证雾节点的合法性。

步骤 5）位置隐私加密，为保护用户的位置隐私安全，可信中心TC不能直接向可信雾节点返回用户的真实坐标，TC需要对真实的坐标信息进行加密，并由雾节点端进行解密。首先用户向可信中心提交自己的真实地理坐标，之后利用匿名身份和追踪参数计算身份参数，在雾节点通过匿名身份认证后，将加密后的身份参数发送给雾节点。雾节点将接收到的身份参数转发给可信中心TC，TC从中还原出用户的身份，并其对应的地理坐标加密后返回给雾节点。最后，雾节点利用密钥还原出真实地理坐标。

其中所述步骤1）具体如下：

步骤11）可信中心TC选取一个安全参数*C*，通过运行生成器生成双线性参数*,,G,,*，其中*G*和均为循环群，为循环群*G*的阶数，为循环群*G*的生成元，示一种映射关系。

步骤 12）选取随机数作为主密钥，随机数作为私钥。之后可信中心TC计算对应的公钥，以及认证参数。最终可信中心TC选取一个安全的哈希加密函数，并发布系统参数。

所述步骤 2）具体如下：

步骤21）用户将自己的真实身份和地理位置的经纬坐标GC同过安全的加密通道（如SSL协议）发送给可信中心TC，TC在接收到后选择一个随机数，并计算该用户的私钥，以及对应的公钥。

步骤 22）可信中心TC为用户生成匿名身份来保护用户的真实身份信息，使得敌手在认证过程中即使捕获到该认证消息也无法获取用户真正的身份信息。

步骤 23）可信中心TC为用户的匿名身份生成跟踪参数，并与该用户的私钥、公钥和匿名身份组成跟踪列表存储到本地进行维护。例如可信中心TC可以对信誉度低的用户跟踪列表进行删除。

步骤 24）可信中心TC计算用户真实身份的哈希结果，并利用该结果对跟踪列表进行异或加密得到。之后将加密结果通过安全传输通道返回给用户，用户接收到后通过计算还原出跟踪列表。

步骤 25）雾节点将自己的真实身份通过安全加密通道发送给可信中心TC，TC收到雾节点的注册请求后选取一个随机数，计算其私钥以及对应的公钥。

步骤 26）可信中心TC为雾节点生成匿名身份及其跟踪参数，并将参数作为跟踪列表保存在本地进行管理。

步骤 27）可信中心TC为雾节点选择两个安全加密密钥用来加密和解密认证用户的隐私位置经纬坐标，其中。

步骤 28）可信中心TC计算雾节点真实身份的哈希结果，并利用该结果对跟踪列表和安全密钥进行异或加密。之后将加密结果通过安全传输通道返回给雾节点，雾节点接收到后通过计算还原出跟踪列表和密钥。

所述步骤 3）具体如下：

步骤 31）用户的智能终端首先选取四个随机数作为加密密钥，并计算身份认证参数，其中为用户的短生命周期私钥，为其对应的公钥。然后对进行哈希加密结算得到身份令牌，同时计算伪装身份认证参数。接着利用伪装身份认证参数计算匿名身份证书，并对进行哈希加密得到结果。最后结合当前的时间戳，计算匿名认证消息。

步骤 32）为防止用户的匿名认证消息被敌手攻击并篡改，需要对进行签名操作。用户的智能终端利用密钥和的哈希加密结果计算其匿名签名，然后将发送给雾节点。在雾节点接收到后，利用消息中的哈希加密结果、公钥和签名计算，如果等式成立，则雾节点认为该认证消息是完整的并接收，否则将拒绝。

步骤 33）雾节点在验证完匿名认证消息的完整性后，首先检查接收到的时间戳和当前的时间戳的差值以防止敌手的重试攻击，其中是双方约定的时间延迟。然后雾节点分别利用装身份认证参数以及公钥还原出真实的认证参数，计算，，。被计算完成后，接着计算，之后比较是否等于接收到的，如果相等，则雾节点认为发送认证消息的用户为可信用户。

所述步骤 4）具体如下：

步骤 41) 为生成雾节点的匿名身份证书，雾节点首先利用匿名身份以及对应的跟踪参数计算参数。在参数计算完成后，利用公钥，匿名身份和系统参数通过哈希加密计算身份令牌。

步骤 42）雾节点生成匿名认证消息，并将和当前的时间戳发送给用户，当用户在时刻接收到匿名认证消息后，首先检查时间戳和的差值以防止敌手的重试攻击，之后计算来验证雾节点的合法性。

步骤 43）用户计算的=，如果等式成立，则与匿名认证消息中的相等，并认为该雾节点为可信节点。

所述步骤 5）具体如下所示：

步骤 51）用户利用匿名身份和追踪参数计算身份参数，并利用私钥对身份参数进行加密，得到加密结果。当雾节点通过匿名身份认证后，用户将发送给雾节点。

步骤 52）雾节点利用自己的匿名身份将发送给可信中心TC，可信中心TC接收到后计算，得到用户的匿名身份。

步骤 53）可信中心TC通过用户的匿名身份找到本地存储的对应经纬坐标之后利用雾节点的加密密钥，计算加密参数。然后选择两个随机数，使满足，。

步骤 54）可信中心TC利用加密参数和随机数生成匿名坐标，其中，。然后将匿名坐标返回给雾节点。

步骤 55）雾节点在接收到匿名坐标后，利用本地的加密密钥计算，还原出真实的经纬坐标。

**有益效果：**本发明采用的以上技术方案与现有技术相比，具有以下技术效果：

本发明在兼顾对患者用户端和医疗雾节点端进行真实身份保护的同时还支持了位置隐私的保护，具体来说：

1. 本发明利用双线性映射技术设计双向的匿名身份认证方案，使得患者用户可以验证医疗雾节点的合法性，同时也使得医疗雾节点可以验证患者用户的合法性。
2. 本发明通过数字签名技术保证了每条认证消息的完整性，以防敌手截取认证消息并对其修改。
3. 本发明利用可信中心TC统一对患者用户的隐私位置信息进行加密，降低了用户智能终端的资源消耗。

**附图说明**

图1是用户匿名身份认证的流程。

图2是雾节点匿名身份认证的流程。

### 具体实施方式

下面结合附图对本发明的技术方案做进一步的详细说明：

在智能医疗领域的具体实施中，假设患者用户在某时刻需要医疗雾节点为其提供计算服务，在进行认证前，第三方可信中心TC首先选取随机数作为主密钥，随机数作为私钥。之后可信中心TC计算对应的公钥，以及认证参数。最终可信中心TC选取一个安全的哈希加密函数，并发布系统参数。用户在注册完成后获得自己的私钥，公钥，匿名身份以及跟踪参数，雾节点在注册完成后获得自己的私钥，公钥，匿名身份及其跟踪参数。

在用户匿名身份认证阶段，如图1所示，用户的智能终端首先选取四个随机数作为加密密钥，并计算身份认证参数，然后对进行哈希加密结算得到身份令牌，同时计算伪装身份认证参数，接着利用伪装身份认证参数计算匿名身份证书，并对进行哈希加密得到结果。最后结合当前的时间戳，计算匿名认证消息。为防止用户的匿名认证消息被敌手攻击并篡改，需要对进行签名操作。用户的智能终端利用密钥和的哈希加密结果计算其匿名签名，然后将发送给雾节点。在雾节点接收到后，利用消息中的哈希加密结果、公钥和签名计算：

如果等式成立，则雾节点认为该认证消息是完整的并接收，否则将拒绝。雾节点在验证完匿名认证消息的完整性后，首先检查接收到的时间戳和当前的时间戳的差值以防止敌手的重试攻击。然后雾节点分别利用装身份认证参数以及公钥还原出真实的认证参数，计算：

被计算完成后，接着计算，之后比较是否等于接收到的，如果相等，则认证成功。

在雾节点匿名认证阶段，如图2 所示，雾节点首先利用匿名身份以及对应的跟踪参数计算参数。在参数计算完成后，利用公钥，匿名身份和系统参数通过哈希加密计算身份令牌，雾节点生成匿名认证消息，并将和当前的时间戳发送给用户。用户计算的=，以及等式：

如果等式成立，则认证成功。

双向匿名认证完成后，患者用户需要将自己的隐私位置报告给医疗雾节点。假设用户的真实经纬坐标为，为方便计算，将经纬度的读数进行取整，得到。可信中心TC通过用户的匿名身份找到本地存储的对应经纬坐标之后利用雾节点的加密密钥，计算加密参数。然后选择两个随机数，使满足，。利用加密参数和随机数生成匿名坐标，其中，。然后将匿名坐标返回给雾节点。雾节点在接收到匿名坐标后，利用本地的加密密钥计算，还原出真实的经纬坐标。



图1 用户匿名认证流程



图2 雾节点匿名认证流程