(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110247881 A
(43)申请公布日 2019.09.17

(21)申请号 201810195543.1

(22)申请日 2018.03.09

(71)申请人 山东量子科学技术研究院有限公司
地址 250101 山东省济南市高新区新泺大街1768号齐鲁软件园大厦B座7层

(72)发明人 赵勇 刘春华

(74)专利代理机构 济南圣达知识产权代理有限公司 37221
代理人 黄海丽

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)

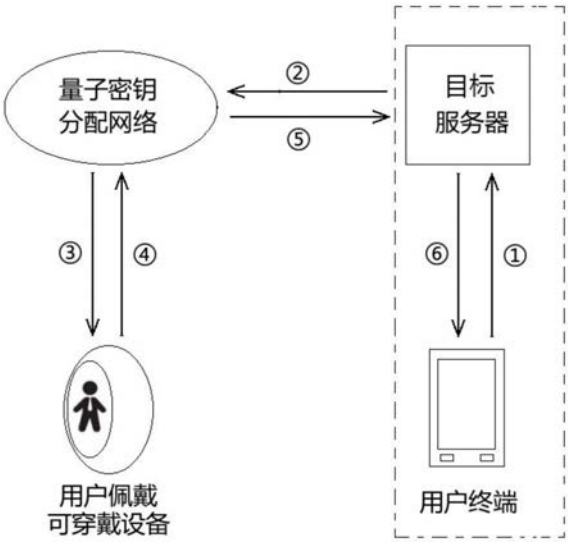
权利要求书5页 说明书14页 附图2页

(54)发明名称

基于可穿戴设备的身份认证方法及系统

(57)摘要

本发明公开了一种基于可穿戴设备的身份认证方法及系统，所述方法包括：用户终端向目标服务器发起认证请求并提供用户终端的设备信息，所述目标服务器接收认证请求并生成临时会话，将临时会话ID和所述设备信息发送至量子密钥分配网络；量子密钥分配网络查找与所述用户终端绑定的可穿戴设备，将所述临时会话ID发送至所述可穿戴设备；所述可穿戴设备采集用户的生物识别信息，将生物识别信息发送至量子密钥分配网络；量子密钥分配网络将生物识别信息与预存的生物识别信息进行匹配，若匹配成功则说明此次身份认证通过，将认证结果发送至所述目标服务器，继而发送至所述用户终端。本发明的技术方案提高了身份认证的安全性和可靠性。



CN 110247881 A

1.一种基于可穿戴设备的身份认证方法,其特征在于,包括以下步骤:

S1:用户终端向目标服务器发起认证请求并提供所述用户终端的设备信息,所述目标服务器接收所述认证请求并生成临时会话,将临时会话ID和所述设备信息发送至量子密钥分配网络;

S2:所述量子密钥分配网络接收所述临时会话ID和设备信息,查找与所述用户终端绑定的可穿戴设备,将所述临时会话ID发送至所述可穿戴设备;

S3:所述可穿戴设备接收所述临时会话ID,采集用户的生物识别信息,将所述生物识别信息发送至所述量子密钥分配网络;

S4:所述量子密钥分配网络接收所述生物识别信息,并将所述生物识别信息与预存的生物识别信息进行匹配,若匹配成功则说明所述临时会话ID对应的此次身份认证通过,将认证结果发送至所述目标服务器,继而发送至所述用户终端。

2.如权利要求1所述的一种基于可穿戴设备的身份认证方法,其特征在于,所述设备信息是所述用户终端的设备ID或量子身份号,所述量子身份号是所述量子密钥分配网络为注册入网的所述可穿戴设备分配的全网唯一的身份标识,所述可穿戴设备与所述用户终端建立绑定关系后,所述量子身份号由所述可穿戴设备及与其绑定的所述用户终端所共享。

3.如权利要求2所述的一种基于可穿戴设备的身份认证方法,其特征在于,当所述设备信息是所述用户终端的设备ID时,所述步骤S2中查找与所述用户终端绑定的可穿戴设备包括:首先根据所述用户终端的设备ID在所述量子密钥分配网络查找到相应的量子身份号,然后查找具备该量子身份号的可穿戴设备,即为与所述用户终端绑定的可穿戴设备;若不能查找到则身份认证失败;其中,所述量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的所述可穿戴设备的量子身份号,以及与这些可穿戴设备绑定的所述用户终端的设备ID。

4.如权利要求2所述的一种基于可穿戴设备的身份认证方法,其特征在于,当所述设备信息是量子身份号时,所述步骤S2中查找与所述用户终端绑定的可穿戴设备包括:根据所述用户终端的量子身份号,在所述量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备,即为目标可穿戴设备;若不能查找到,则此次身份认证失败;其中,所述量子密钥分配网络中预存的设备信息应至少包含注册到所述量子密钥分配网络的所述可穿戴设备的量子身份号。

5.如权利要求1所述的一种基于可穿戴设备的身份认证方法,其特征在于,所述步骤S4中所述与预存的生物识别信息匹配成功之后还包括:进一步查找所述量子密钥分配网络中存储的该条生物识别信息所绑定的设备信息,判断所述设备信息是否与自所述目标服务器接收到的设备信息相一致;和/或

判断接收自所述可穿戴设备的临时会话ID是否与自所述目标服务器接收到的临时会话ID相一致,其中接收自所述可穿戴设备的临时会话ID是所述可穿戴设备向所述量子密钥分配网络发送所述生物识别信息的同时发送的;

若判断结果为一致,则认证通过;其中,所述量子密钥分配网络中预存的信息应至少包含事先注册到本网络上的设备信息和与所述设备信息绑定的生物识别信息。

6.如权利要求1所述的一种基于可穿戴设备的身份认证方法,其特征在于,所述用户的生物识别信息包括以下一种或几种:指纹信息、心跳信息、血压信息、视网膜信息、虹膜信

息、声纹信息、静脉信息、面部信息、笔迹签名信息。

7.如权利要求1所述的一种基于可穿戴设备的身份认证方法，其特征在于，所述量子密钥分配网络与所述目标服务器中均预存第一共享密钥，用于二者之间通信数据的加密和解密。

8.如权利要求1-7任一项所述的一种基于可穿戴设备的身份认证方法，其特征在于，所述可穿戴设备与所述量子密钥分配网络中均预存第二共享密钥，用于二者之间通信数据的加密和解密。

9.如权利要求1所述的一种基于可穿戴设备的身份认证方法，其特征在于，所述可穿戴设备与所述用户终端的连接方式为无线或有线连接。

10.一种基于可穿戴设备的身份认证系统，其特征在于，包括：

用户终端，用于向目标服务器发起认证请求并提供所述用户终端的设备信息，以及接收所述目标服务器发送的认证结果；

目标服务器，用于接收所述认证请求并生成临时会话，将临时会话ID和所述设备信息发送至量子密钥分配网络，以及接收所述量子密钥分配网络发送的所述认证结果，继而发送至所述用户终端；

量子密钥分配网络，用于接收所述临时会话ID和设备信息，查找与所述用户终端绑定的可穿戴设备，向所述可穿戴设备发送所述临时会话ID，以及接收所述可穿戴设备发送的生物识别信息，并将其与预存的生物识别信息进行匹配，若匹配成功则所述临时会话ID对应的此次身份认证通过，将所述认证结果发送至所述目标服务器；

可穿戴设备，用于接收所述临时会话ID，采集用户的生物识别信息，并将所述生物识别信息发送至所述量子密钥分配网络。

11.如权利要求10所述的一种基于可穿戴设备的身份认证系统，其特征在于，所述设备信息是所述用户终端的设备ID或量子身份号，所述量子身份号是所述量子密钥分配网络为注册入网的所述可穿戴设备分配的全网唯一的身份标识，所述可穿戴设备与所述用户终端建立绑定关系后，所述量子身份号由所述可穿戴设备及与其绑定的所述用户终端所共享。

12.如权利要求11所述的一种基于可穿戴设备的身份认证系统，其特征在于，当所述设备信息是所述用户终端的设备ID时，所述查找与所述用户终端绑定的可穿戴设备包括：首先根据所述用户终端的设备ID在所述量子密钥分配网络查找到相应的量子身份号，然后查找具备该量子身份号的可穿戴设备，即为与所述用户终端绑定的可穿戴设备；若不能查找到则身份认证失败；其中，所述量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的所述可穿戴设备的量子身份号，以及与这些可穿戴设备绑定的所述用户终端的设备ID。

13.如权利要求11所述的一种基于可穿戴设备的身份认证系统，其特征在于，当所述设备信息是量子身份号时，所述查找与所述用户终端绑定的可穿戴设备，是在所述量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备，即为目标可穿戴设备；若不能查找到，则此次身份认证失败；其中，所述量子密钥分配网络中预存的设备信息应至少包含注册到所述量子密钥分配网络的所述可穿戴设备的量子身份号。

14.如权利要求10所述的一种基于可穿戴设备的身份认证系统，其特征在于，所述与预存的生物识别信息进行匹配成功之后还包括：进一步查找所述量子密钥分配网络中存储的

该条生物识别信息所绑定的设备信息，判断所述设备信息是否与自所述目标服务器接收到的设备信息相一致；和/或

判断接收自所述可穿戴设备的临时会话ID是否与自所述目标服务器接收到的临时会话ID相一致，其中接收自所述可穿戴设备的临时会话ID是所述可穿戴设备向所述量子密钥分配网络发送所述生物识别信息的同时发送的；

若判断结果为一致，则认证通过；其中，所述量子密钥分配网络中预存的信息应至少包含事先注册到本网络上的设备信息和与所述设备信息绑定的生物识别信息。

15.如权利要求10所述的一种基于可穿戴设备的身份认证系统，其特征在于，所述用户的生物识别信息包括以下一种或几种：指纹信息、心跳信息、血压信息、视网膜信息、虹膜信息、声纹信息、静脉信息、面部信息、笔迹签名信息。

16.如权利要求10所述的一种基于可穿戴设备的身份认证系统，其特征在于，所述量子密钥分配网络与所述目标服务器中均预存第一共享密钥，用于二者之间通信数据的加密和解密。

17.如权利要求10-16任一项所述的一种基于可穿戴设备的身份认证系统，其特征在于，所述可穿戴设备与所述量子密钥分配网络中均预存第二共享密钥，用于二者之间通信数据的加密和解密。

18.如权利要求10所述的一种基于可穿戴设备的身份认证系统，其特征在于，所述可穿戴设备与所述用户终端的连接方式为无线或有线连接。

19.一种用于身份认证的量子密钥分配网络，其特征在于：

接收用户终端的设备信息；

查找与所述用户终端绑定的可穿戴设备；

接收所述可穿戴设备采集并发送的生物识别信息，并将其与预存的生物识别信息进行匹配，若匹配成功则认证通过。

20.如权利要求19所述的一种用于身份认证的量子密钥分配网络，其特征在于，所述设备信息是用户终端向目标服务器发起认证请求时提供的。

21.如权利要求20所述的一种用于身份认证的量子密钥分配网络，其特征在于，所述量子密钥分配网络还接收所述目标服务器接收所述认证请求生成的临时会话ID，继而发送至所述可穿戴设备。

22.如权利要求19所述的一种用于身份认证的量子密钥分配网络，其特征在于，所述设备信息是所述用户终端的设备ID或量子身份号，所述量子身份号是所述量子密钥分配网络为注册入网的所述可穿戴设备分配的全网唯一的身份标识，所述可穿戴设备与所述用户终端建立绑定关系后，所述量子身份号由所述可穿戴设备及与其绑定的所述用户终端所共享。

23.如权利要求22所述的一种用于身份认证的量子密钥分配网络，其特征在于，当所述设备信息是所述用户终端的设备ID时，所述查找与所述用户终端绑定的可穿戴设备包括：首先根据所述用户终端的设备ID在所述量子密钥分配网络查找到相应的量子身份号，然后查找具备该量子身份号的可穿戴设备，即为与所述用户终端绑定的可穿戴设备；若不能查找到则身份认证失败；其中，所述量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的所述可穿戴设备的量子身份号，以及与这些可穿戴设备绑

定的所述用户终端的设备ID。

24.如权利要求22所述的一种用于身份认证的量子密钥分配网络，其特征在于，当所述设备信息是量子身份号时，所述查找与所述用户终端绑定的可穿戴设备包括：根据所述用户终端的量子身份号，在所述量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备，即为与所述用户终端绑定的可穿戴设备；若不能查找到，则此次身份认证失败；其中，所述量子密钥分配网络中预存的设备信息应至少包含注册到所述量子密钥分配网络的所述可穿戴设备的量子身份号。

25.如权利要求19所述的一种用于身份认证的量子密钥分配网络，其特征在于，所述与预存的生物识别信息进行匹配成功之后还包括：进一步查找所述量子密钥分配网络中存储的该条生物识别信息所绑定的设备信息，判断所述设备信息是否与自所述目标服务器接收到的设备信息相一致；和/或

判断接收自所述可穿戴设备的临时会话ID是否与自所述目标服务器接收到的临时会话ID相一致，其中接收自所述可穿戴设备的临时会话ID是所述可穿戴设备向所述量子密钥分配网络发送所述生物识别信息的同时发送的；

若判断结果为一致，则认证通过；其中，所述量子密钥分配网络中预存的信息应至少包含事先注册到本网络上的设备信息和与所述设备信息绑定的生物识别信息。

26.如权利要求19所述的一种用于身份认证的量子密钥分配网络，其特征在于，所述量子密钥分配网络与所述目标服务器中均预存第一共享密钥，用于二者之间通信数据的加密和解密。

27.如权利要求19-26任一项所述的一种用于身份认证的量子密钥分配网络，其特征在于，所述可穿戴设备与所述量子密钥分配网络中均预存第二共享密钥，用于二者之间通信数据的加密和解密。

28.一种用于身份认证的可穿戴设备，与用户终端绑定，其特征在于：

采集用户的生物识别信息；

将所述生物识别信息发送至所述量子密钥分配网络进行认证。

29.如权利要求28所述的一种用于身份认证的可穿戴设备，其特征在于，所述可穿戴设备采集用户生物识别信息是在接收到临时会话ID/设备信息之后；所述临时会话ID是目标服务器接收所述用户终端发起的认证请求生成的，并由所述目标服务器发送至所述量子密钥分配网络；所述设备信息是用户终端向目标服务器发起认证请求时提供的，在目标服务器接收所述认证请求后发送至量子密钥分配网络。

30.如权利要求28所述的一种用于身份认证的可穿戴设备，其特征在于，所述可穿戴设备在所述量子密钥分配网络注册并存储有全网独一无二的量子身份号，具有密钥存储及数据加解密和数据收发功能。

31.如权利要求28-30任一项所述的一种用于身份认证的可穿戴设备，其特征在于，所述可穿戴设备与所述量子密钥分配网络中均预存第二共享密钥，用于二者之间通信数据的加密和解密。

32.一种目标服务器，其特征在于：

接收用户终端发送的认证请求以及所述用户终端的设备信息，将所述设备信息发送至量子密钥分配网络；

将所述量子密钥分配网络发送的认证结果发送至所述用户终端。

33.如权利要求32所述的一种目标服务器，其特征在于，所述目标服务器接收用户终端发送的认证请求后还将生成的临时会话ID发送至量子密钥分配网络。

34.如权利要求32所述的一种目标服务器，其特征在于，所述目标服务器兼具身份认证功能和为所述用户终端提供业务访问的功能；或仅具备身份认证功能，若所述目标服务器身份认证通过，由其他服务器为所述用户终端提供业务访问功能。

35.如权利要求32-34任一项所述的一种目标服务器，其特征在于，所述量子密钥分配网络与所述目标服务器中均预存第一共享密钥，用于二者之间通信数据的加密和解密。

基于可穿戴设备的身份认证方法及系统

技术领域

[0001] 本发明涉及信息安全认证领域，具体涉及一种基于可穿戴设备的身份认证方法及系统。

背景技术

[0002] 随着移动互联网的迅速发展，企事业单位内部业务网站也逐步向移动终端方向发展，为了便于工作人员随时了解工作内容，用户希望能够通过便携的移动终端来访问单位内部网站服务器。若身份认证存在漏洞会导致数据的泄露，会为企业带来不可挽回的后果，因此，安全可靠的登录认证方法是非常必要的。现有的对移动终端的认证方式主要有：通过账号和密码登录认证、通过动态口令认证、通过将设备标识信息与认证服务器中预存的用户设备信息比对进行认证等，但账号密码、动态口令和设备ID都存在被截获或泄露的可能。随着可穿戴设备的普及，已有很多将可穿戴设备引入到身份认证技术中的相关技术，有将普通密码技术与可穿戴设备的结合的认证技术，也有生物识别技术与可穿戴设备的结合认证技术。例如《一种可穿戴设备的认证方法》(申请号：201510598684.4)，该方法引入伪随机函数、异或运算和单向认证函数等轻量级算子实现智能手机与可穿戴设备的相互认证，在智能手机与可穿戴设备交互过程中，可穿戴设备的伪身份标识符和预共享密值等敏感数据通过匿名的方式进行传输，保证交互数据的安全性，同时引入动态更新机制，提高了会话周期的新鲜性和随机性，避免恶意攻击者进行重放、假冒等攻击；《通过穿戴式设备进行认证的方法和穿戴式设备》(申请号：201310190418.9)根据生物特征获取用户的身份认证信息，并通过穿戴式设备将身份认证信息发送至终端进行认证；还有《基于可穿戴设备的认证支付方法以及支付认证系统》(申请号：201410295802.X)也是通过增加对可穿戴设备的认证进一步提高支付的安全性。

[0003] 但是，现有的基于可穿戴设备的认证方式通常应用于与用户终端交互过程中的身份认证；并且现有的可穿戴设备认证方式在信息传输过程中往往使用基于数学算法复杂度的加密方式，而基于数学算法的保密机制容易被越来越快速发展的计算技术所破解，新的算法漏洞被不断发现，在未来的量子计算机面前更是非常脆弱，使得现有的基于可穿戴设备的认证方式存在严重的安全隐患，难以适应较高安全要求的身份认证场合。

[0004] 因此，如何在借助可穿戴设备的条件下，提高移动终端登录目标服务器的身份认证安全性是目前需要本领域技术人员迫切解决的技术问题。

发明内容

[0005] 为了解决上述问题，本发明提供了一种基于量子密钥与可穿戴设备的认证方法，用于账户管理及访问身份认证，构建了从使用者到用户终端、再到目标服务器的可靠认证链条，提出了一种高安全性的认证机制。

[0006] 本发明的技术方案为一种基于可穿戴设备的身份认证方法，包括以下步骤：

[0007] S1：用户终端向目标服务器发起认证请求并提供所述用户终端的设备信息，所述

目标服务器接收所述认证请求并生成临时会话，将临时会话ID和所述设备信息发送至量子密钥分配网络；

[0008] S2：所述量子密钥分配网络接收所述临时会话ID和设备信息，查找与所述用户终端绑定的可穿戴设备，将所述临时会话ID发送至所述可穿戴设备；

[0009] S3：所述可穿戴设备接收所述临时会话ID，采集用户的生物识别信息，将所述生物识别信息发送至所述量子密钥分配网络；

[0010] S4：所述量子密钥分配网络接收所述生物识别信息，并将所述生物识别信息与预存的生物识别信息进行匹配，若匹配成功则说明所述临时会话ID对应的此次身份认证通过，将认证结果发送至所述目标服务器，继而发送至所述用户终端。

[0011] 进一步地，所述设备信息是所述用户终端的设备ID或量子身份号，所述量子身份号是所述量子密钥分配网络为注册入网的所述可穿戴设备分配的全网唯一的身份标识，所述可穿戴设备与所述用户终端建立绑定关系后，所述量子身份号由所述可穿戴设备及与其绑定的所述用户终端所共享。

[0012] 进一步地，当所述设备信息是所述用户终端的设备ID时，所述步骤S2中查找与所述用户终端绑定的可穿戴设备包括：首先根据所述用户终端的设备ID在所述量子密钥分配网络查找到相应的量子身份号，然后查找具备该量子身份号的可穿戴设备，即为与所述用户终端绑定的可穿戴设备；若不能查找到则身份认证失败；其中，所述量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的所述可穿戴设备的量子身份号，以及与这些可穿戴设备绑定的所述用户终端的设备ID。

[0013] 进一步地，当所述设备信息是量子身份号时，所述步骤S2中查找与所述用户终端绑定的可穿戴设备包括：根据所述用户终端的量子身份号，在所述量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备，即为目标可穿戴设备；若不能查找到，则此次身份认证失败；其中，所述量子密钥分配网络中预存的设备信息应至少包含注册到所述量子密钥分配网络的所述可穿戴设备的量子身份号。

[0014] 进一步地，所述步骤S4中所述与预存的生物识别信息匹配成功之后还包括：进一步查找所述量子密钥分配网络中存储的该条生物识别信息所绑定的设备信息，判断所述设备信息是否与自所述目标服务器接收到的设备信息相一致；和/或

[0015] 判断接收自所述可穿戴设备的临时会话ID是否与自所述目标服务器接收到的临时会话ID相一致，其中接收自所述可穿戴设备的临时会话ID是所述可穿戴设备向所述量子密钥分配网络发送所述生物识别信息的同时发送的；

[0016] 若判断结果为一致，则认证通过；其中，所述量子密钥分配网络中预存的信息应至少包含事先注册到本网络上的设备信息和与所述设备信息绑定的生物识别信息。

[0017] 进一步地，所述用户的生物识别信息包括以下一种或几种：指纹信息、心跳信息、血压信息、视网膜信息、虹膜信息、声纹信息、静脉信息、面部信息、笔迹签名信息。

[0018] 进一步地，所述量子密钥分配网络与所述目标服务器中均预存第一共享密钥，用于二者之间通信数据的加密和解密。

[0019] 进一步地，所述可穿戴设备与所述量子密钥分配网络中均预存第二共享密钥，用于二者之间通信数据的加密和解密。

[0020] 进一步地，所述可穿戴设备与所述用户终端的连接方式为无线或有线连接。

[0021] 根据本发明的第二方面，本发明还提供了一种基于可穿戴设备的身份认证系统，包括：

[0022] 用户终端，用于向目标服务器发起认证请求并提供所述用户终端的设备信息，以及接收所述目标服务器发送的认证结果；

[0023] 目标服务器，用于接收所述认证请求并生成临时会话，将临时会话ID和所述设备信息发送至量子密钥分配网络，以及接收所述量子密钥分配网络发送的所述认证结果，继而发送至所述用户终端；

[0024] 量子密钥分配网络，用于接收所述临时会话ID和设备信息，查找与所述用户终端绑定的可穿戴设备，向所述可穿戴设备发送所述临时会话ID，以及接收所述可穿戴设备发送的生物识别信息，并将其与预存的生物识别信息进行匹配，若匹配成功则所述临时会话ID对应的此次身份认证通过，将所述认证结果发送至所述目标服务器；

[0025] 可穿戴设备，用于接收所述临时会话ID，采集用户的生物识别信息，并将所述生物识别信息发送至所述量子密钥分配网络。

[0026] 进一步地，所述设备信息是所述用户终端的设备ID或量子身份号，所述量子身份号是所述量子密钥分配网络为注册入网的所述可穿戴设备分配的全网唯一的身份标识，所述可穿戴设备与所述用户终端建立绑定关系后，所述量子身份号由所述可穿戴设备及与其绑定的所述用户终端所共享。

[0027] 进一步地，当所述设备信息是所述用户终端的设备ID时，所述查找与所述用户终端绑定的可穿戴设备包括：首先根据所述用户终端的设备ID在所述量子密钥分配网络查找到相应的量子身份号，然后查找具备该量子身份号的可穿戴设备，即为与所述用户终端绑定的可穿戴设备；若不能查找到则身份认证失败；其中，所述量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的所述可穿戴设备的量子身份号，以及与这些可穿戴设备绑定的所述用户终端的设备ID。

[0028] 进一步地，当所述设备信息是量子身份号时，所述查找与所述用户终端绑定的可穿戴设备，是在所述量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备，即为目标可穿戴设备；若不能查找到，则此次身份认证失败；其中，所述量子密钥分配网络中预存的设备信息应至少包含注册到所述量子密钥分配网络的所述可穿戴设备的量子身份号。

[0029] 进一步地，所述与预存的生物识别信息进行匹配成功之后还包括：进一步查找所述量子密钥分配网络中存储的该条生物识别信息所绑定的设备信息，判断所述设备信息是否与自所述目标服务器接收到的设备信息相一致；和/或

[0030] 判断接收自所述可穿戴设备的临时会话ID是否与自所述目标服务器接收到的临时会话ID相一致，其中接收自所述可穿戴设备的临时会话ID是所述可穿戴设备向所述量子密钥分配网络发送所述生物识别信息的同时发送的；

[0031] 若判断结果为一致，则认证通过；其中，所述量子密钥分配网络中预存的信息应至少包含事先注册到本网络上的设备信息和与所述设备信息绑定的生物识别信息。

[0032] 进一步地，所述用户的生物识别信息包括以下一种或几种：指纹信息、心跳信息、血压信息、视网膜信息、虹膜信息、声纹信息、静脉信息、面部信息、笔迹签名信息。

[0033] 进一步地，所述量子密钥分配网络与所述目标服务器中均预存第一共享密钥，用

于二者之间通信数据的加密和解密。

[0034] 进一步地,所述可穿戴设备与所述量子密钥分配网络中均预存第二共享密钥,用于二者之间通信数据的加密和解密。

[0035] 进一步地,所述可穿戴设备与所述用户终端的连接方式为无线或有线连接。

[0036] 根据本发明的第三方面,本发明还提供了一种用于身份认证的量子密钥分配网络:

[0037] 接收用户终端的设备信息;

[0038] 查找与所述用户终端绑定的可穿戴设备;

[0039] 接收所述可穿戴设备采集并发送的生物识别信息,并将其与预存的生物识别信息进行匹配,若匹配成功则认证通过。

[0040] 进一步地,所述设备信息是用户终端向目标服务器发起认证请求时提供的。

[0041] 进一步地,所述量子密钥分配网络还接收所述目标服务器接收所述认证请求生成的临时会话ID。

[0042] 进一步地,所述设备信息是所述用户终端的设备ID或量子身份号,所述量子身份号是所述量子密钥分配网络为注册入网的所述可穿戴设备分配的全网唯一的身份标识,所述可穿戴设备与所述用户终端建立绑定关系后,所述量子身份号由所述可穿戴设备及与其绑定的所述用户终端所共享。

[0043] 进一步地,当所述设备信息是所述用户终端的设备ID时,所述查找与所述用户终端绑定的可穿戴设备包括:首先根据所述用户终端的设备ID在所述量子密钥分配网络查找到相应的量子身份号,然后查找具备该量子身份号的可穿戴设备,即为与所述用户终端绑定的可穿戴设备;若不能查找到则身份认证失败;其中,所述量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的所述可穿戴设备的量子身份号,以及与这些可穿戴设备绑定的所述用户终端的设备ID。

[0044] 进一步地,当所述设备信息是量子身份号时,所述查找与所述用户终端绑定的可穿戴设备包括:根据所述用户终端的量子身份号,在所述量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备,即为与所述用户终端绑定的可穿戴设备;若不能查找到,则此次身份认证失败;其中,所述量子密钥分配网络中预存的设备信息应至少包含注册到所述量子密钥分配网络的所述可穿戴设备的量子身份号。

[0045] 进一步地,所述与预存的生物识别信息进行匹配成功之后还包括:进一步查找所述量子密钥分配网络中存储的该条生物识别信息所绑定的设备信息,判断所述设备信息是否与自所述目标服务器接收到的设备信息相一致;和/或

[0046] 判断接收自所述可穿戴设备的临时会话ID是否与自所述目标服务器接收到的临时会话ID相一致,其中接收自所述可穿戴设备的临时会话ID是所述可穿戴设备向所述量子密钥分配网络发送所述生物识别信息的同时发送的;

[0047] 若判断结果为一致,则认证通过;其中,所述量子密钥分配网络中预存的信息应至少包含事先注册到本网络上的设备信息和与所述设备信息绑定的生物识别信息。

[0048] 进一步地,所述量子密钥分配网络与所述目标服务器中均预存第一共享密钥,用于二者之间通信数据的加密和解密。

[0049] 进一步地,所述可穿戴设备与所述量子密钥分配网络中均预存第二共享密钥,用

于二者之间通信数据的加密和解密。

[0050] 根据本发明的第四方面，本发明还提供了一种用于身份认证的可穿戴设备，与用户终端绑定：

[0051] 采集用户的生物识别信息；

[0052] 将所述生物识别信息发送至所述量子密钥分配网络进行认证。

[0053] 进一步地，所述可穿戴设备采集用户生物识别信息是在接收到临时会话ID/设备信息之后；所述临时会话ID是目标服务器接收所述用户终端发起的认证请求生成的，并由所述目标服务器发送至所述量子密钥分配网络；所述设备信息是用户终端向目标服务器发起认证请求时提供的，在目标服务器接收所述认证请求后发送至量子密钥分配网络。

[0054] 进一步地，所述可穿戴设备在所述量子密钥分配网络注册并存储有全网独一无二的量子身份号，具有密钥存储及数据加解密和数据收发功能。

[0055] 进一步地，所述可穿戴设备与所述量子密钥分配网络中均预存第二共享密钥，用于二者之间通信数据的加密和解密。

[0056] 根据本发明的第五方面，本发明还提供了一种目标服务器：

[0057] 接收用户终端发送的认证请求以及所述用户终端的设备信息，将所述设备信息发送至量子密钥分配网络；

[0058] 将所述量子密钥分配网络发送的认证结果发送至所述用户终端

[0059] 进一步地，所述目标服务器接收用户终端发送的认证请求后还将生成的临时会话ID发送至量子密钥分配网络。

[0060] 进一步地，所述目标服务器兼具身份认证功能和为所述用户终端提供业务访问的功能；或仅具备身份认证功能，若所述目标服务器身份认证通过，由其他服务器为所述用户终端提供业务访问功能。

[0061] 进一步地，所述量子密钥分配网络与所述目标服务器中均预存第一共享密钥，用于二者之间通信数据的加密和解密。

[0062] 本发明的有益效果：

[0063] 本发明提供了一种用户终端访问第三方目标服务器的身份认证方法，该方法基于量子密钥分配网络，它向第三方目标服务器提供认证服务接口，以代替传统的基于数学算法的认证方式，采用量子密钥加密，提升了身份认证过程中的安全性。

[0064] 本发明在身份认证过程中加入了可穿戴设备，相比于用户终端，可穿戴设备与具体使用者的身份绑定更加紧密，安全性更高；另外，可穿戴设备使用方便，能有效提高用户体验。

[0065] 本发明中关键认证环节被量子密码所保护，因此具有极强的抗冒充身份、抗破译的功能。

[0066] 本发明将生物身份认证与量子密钥进行有机结合，极大增强了设备与设备之间、人和设备之间的身份认证的可靠性，解决了设备本身带来的安全隐患，铺平了从远程业务服务器到使用者的“最后一公里”。

附图说明

[0067] 构成本申请的一部分的说明书附图用来提供对本申请的进一步理解，本申请的示

意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。

[0068] 图1为本发明基于可穿戴设备的身份认证方法流程图。

[0069] 图2为本发明身份认证过程示意图。

[0070] 图3为本发明量子密钥分配网络进行生物信息识别匹配的方法示意图。

具体实施方式

[0071] 应该指出，以下详细说明都是示例性的，旨在对本申请提供进一步的说明。除非另有指明，本文使用的所有技术和科学术语具有与本申请所属技术领域的普通技术人员通常理解的相同含义。

[0072] 需要注意的是，这里所使用的术语仅是为了描述具体实施方式，而非意图限制根据本申请的示例性实施方式。如在这里所使用的，除非上下文另外明确指出，否则单数形式也意图包括复数形式，此外，还应当理解的是，当在本说明书中使用术语“包含”和/或“包括”时，其指明存在特征、步骤、操作、器件、组件和/或它们的组合。

[0073] 本发明中所称的移动终端包括但不限于手机、平板，能够进行网络连接的电子设备均适用于本发明的移动终端；本发明中所述的可穿戴设备包括但不限于智能戒指、智能手环、智能手表、智能项链等与人体接触及随身携带的小型设备。

[0074] 实施例1

[0075] 本实施例提供了一种基于可穿戴设备的身份认证方法，其采用了生物信息识别技术，如图1所示，包括以下步骤：

[0076] S1：用户终端向目标服务器发起认证请求并提供所述用户终端的设备信息，目标服务器接收所述认证请求并生成临时会话，并将临时会话ID和设备信息发送至量子密钥分配网络；

[0077] S2：量子密钥分配网络接收所述临时会话ID和设备信息，查找与用户终端绑定的可穿戴设备，将所述临时会话ID发送至所述可穿戴设备；

[0078] S3：所述可穿戴设备接收所述临时会话ID，采集用户的生物识别信息，将所述生物识别信息发送至量子密钥分配网络；

[0079] S4：所述量子密钥分配网络接收所述生物识别信息，并将所述生物识别信息与预存的生物识别信息进行匹配，若匹配成功则说明所述临时会话ID对应的此次身份认证通过，将认证结果发送至目标服务器，继而发送至用户终端。

[0080] 所述目标服务器可以兼具所述身份认证功能和为用户终端提供业务访问功能；也可以仅具备身份认证功能，若所述目标服务器身份认证通过，由其他服务器为用户终端提供业务访问功能。

[0081] 量子密钥分配网络为目标服务器提供接口，与其建立通信，向自身和所述目标服务器分发统一的第一共享密钥，所述第一共享密钥用于量子密钥分配网络与目标服务器之间通信数据的加密和解密；可选地，二者间也可以通过其他形式实现密钥共享，例如量子密钥分配网络先生成量子密钥，再用其他相对可靠的介质(如VPN专网、移动存储介质)传递到目标服务器实现共享。

[0082] 可穿戴设备注册到量子密钥分配网络，量子密钥分配网络为自身和可穿戴设备分配第二共享密钥，所述第二共享密钥用于量子密钥分配网络与可穿戴设备之间通信数据的

加密和解密。

[0083] 其中,注册方式是:可穿戴设备持有者(可以是个人,或可穿戴设备的生产设备商、销售商)首先去量子密钥分配网络的运营机构办理注册入网的相关手续,量子密钥分配网络的运营机构负责审核用户的入网申请,如审核通过,则为每一台申请入网的可穿戴设备颁发一个由量子密钥分配网络分配的全网内独一无二的量子身份号,该量子身份号被存储在申请入网的可穿戴设备的永久存储介质中。由于每次身份认证过程中所传递的信息很少,因此即使采用一次一密,可穿戴设备上在注册时预存的与量子密钥分配网络间的共享密钥也可以使用很长时间。如果出于提高安全性的考虑,可以定期更换存储在可穿戴设备上的共享密钥。一种方法是量子密钥分配网络生成新密钥,并用旧的共享密钥加密新的共享密钥,下发到可穿戴设备上。

[0084] 可穿戴设备与用户终端的连接方式为无线或有线连接。

[0085] 由于执行此过程时用户终端与可穿戴设备的距离很近,二者可以通过蓝牙方式进行绑定和信息传输,在更加严苛的安全环境要求下,也可以通过有线方式进行信息传输。

[0086] 为了防止重放攻击,使用量子密钥进行保密通信的两个设备之间信息传输时(例如量子密钥分配网络和可穿戴设备之间、量子密钥分配网络和目标服务器之间),都要携带一个随机码,该随机码取自与对端设备共享的量子密钥,而且只用一次。只有当两边的随机码一致时,本段通信才是合法有效的。

[0087] 可选地,可以将可穿戴设备注册到量子密钥分配网络中,获取所述可穿戴设备的量子身份号,当所述可穿戴设备与一个用户终端实现绑定时,所述量子身份号也被所述用户终端共享,并且绑定关系存储在量子密钥分配网络中。可穿戴设备可以向量子密钥分配网络申请解除与用户终端的绑定关系,也可以申请与另外的用户终端建立新的绑定关系。

[0088] 优选地,所述设备信息可以是用户终端的设备ID,也可以是量子身份号。

[0089] 所述步骤S1中将该临时会话ID和设备信息发送至量子密钥分配网络前还包括:目标服务器将临时会话ID和设备信息采用第一共享密钥进行加密;所述第一共享密钥为目标服务器与量子密钥分配网络之间的共享密钥。

[0090] 所述步骤S2中量子密钥分配网络接收所述临时会话ID和设备信息还包括:采用第一共享密钥对其进行解密。

[0091] 当发起认证时提供的设备信息为设备ID时,所述步骤S2中查找与用户终端绑定的可穿戴设备,如图3所示,具体包括:首先根据用户终端的设备ID在量子密钥分配网络查找到相应的量子身份号,然后查找具备该量子身份号的可穿戴设备,即为与所述用户终端绑定的可穿戴设备;若不能查找到则身份认证失败。其中,量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的可穿戴设备的量子身份号,以及与这些可穿戴设备绑定的用户终端的设备ID。

[0092] 当发起认证时提供的设备信息为设备量子身份号时,所述步骤S2中查找与用户终端绑定的可穿戴设备,是在量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备,即为与所述用户终端绑定的可穿戴设备;若不能查找到则身份认证失败。其中,量子密钥分配网络中预存的设备信息应至少包含注册到量子密钥分配网络的可穿戴设备的量子身份号。

[0093] 所述步骤S2中向所述可穿戴设备发送所述临时会话ID前还包括:将所述临时会话

ID采用第二共享密钥进行加密;所述第二共享密钥为可穿戴设备与量子密钥分配网络之间的共享密钥。

[0094] 所述步骤S3中可穿戴设备接收所述临时会话ID还包括:采用第二共享密钥对其进行解密。

[0095] 所述步骤S3中用户的生物识别信息包括以下一种或几种:指纹信息、心跳信息、血压信息、视网膜信息、虹膜信息、声纹信息、静脉信息、面部信息、笔迹签名信息。

[0096] 所述步骤S3中将所述生物识别信息发送至量子密钥分配网络前还包括:可穿戴设备将所述生物识别信息采用第二共享密钥进行加密。

[0097] 所述步骤S4中所述量子密钥分配网络接收所述生物识别信息还包括:量子密钥分配网络将加密后的生物识别信息采用第二共享密钥进行解密。

[0098] 所述步骤S4中预存的生物识别信息包括以下一种或几种:指纹信息、心跳信息、血压信息、视网膜信息、虹膜信息、声纹信息、静脉信息、面部信息、笔迹签名信息。

[0099] 所述步骤S4中与预存的生物识别信息进行匹配的方式可以为:将自可穿戴设备接收的生物识别信息与量子密钥分配网络中预存的生物识别信息逐个对比,若查找到一致的生物识别信息则匹配成功,反之匹配失败,本次身份认证失败;也可以是量子密钥分配网络在本网络内存储的生物识别信息中检索自可穿戴设备接收的生物识别信息,如果检索到结果则说明认证请求发起者确为已经注册到量子密钥分配网络的合法用户,匹配成功,如果检索失败则匹配失败,本次身份认证失败。

[0100] 可选地,如图3所示,为了进一步提高认证过程中的安全性,匹配过程中在匹配过生物识别信息之后还对设备信息进行进一步验证,即,所述步骤S4中与预存的生物识别信息进行匹配的过程具体包括:

[0101] S41:量子密钥分配网络在本网络内存储的生物识别信息中检索可穿戴设备发送上来的生物识别信息,如果检索失败则本次身份认证失败。

[0102] S42:如果检索成功,则进一步查找量子密钥分配网络中存储的该条生物识别信息所绑定的设备信息(量子身份号或设备ID,图3中以量子身份号为例),如图3所示,根据所述生物识别信息可以唯一确定与其绑定的可穿戴设备的量子身份号,以及与所述可穿戴设备绑定的用户终端的设备信息(设备ID或与可穿戴设备共享的量子身份号)。

[0103] S43:检查所述设备信息是否与步骤S2中来自目标服务器的设备信息相符。

[0104] S44:所述可穿戴设备向量子密钥分配网络发送生物识别信息的同时还发送了所述临时会话ID,所述量子密钥分配网络检查来自可穿戴设备的临时会话ID是否与步骤S2中来自目标服务器的临时会话ID相符。

[0105] S45:如果均相符,说明认证请求发起者的声称身份确实与现场采集到的实际身份相符,且属于同一次认证过程,匹配成功。

[0106] 可选地,可以仅验证所述设备信息是否与步骤S2中来自目标服务器的设备信息相符,或者仅验证来自可穿戴设备的临时会话ID是否与步骤S2中来自目标服务器的临时会话ID相符。

[0107] 其中,量子密钥分配网络中至少预存事先注册到本网络上的设备信息,以及与所述设备信息绑定的生物识别信息。

[0108] 所述步骤S4中将认证结果发送至目标服务器,继而发送至用户终端包括:量子密

钥分配网络将认证结果采用第一共享密钥进行加密，发送至目标服务器，目标服务器接收加密后的认证结果，采用第一共享密钥对其进行解密，继而发送至用户终端。

[0109] 为了更清楚的阐述本发明，下面通过一实例描述本实施例，如图2所示：

[0110] ①用户终端访问目标服务器，将自己身份告知服务器。目标服务器为此次登陆生成一个临时会话。

[0111] ②目标服务器向量子密钥分配网络申请授权认证，并将此次临时会话的相关信息以及用户终端身份用与量子密钥分配网络间的共享量子密钥加密之后，发送到量子密钥分配网络。量子密钥分配网络收到后解密还原信息。

[0112] ③量子密钥分配网络在内部查找登陆者身份，并向拥有该身份的可穿戴设备发送此次临时会话的相关信息，该信息使用与可穿戴设备间预置的共享量子密钥加密后下发。可穿戴设备收到后解密还原信息。

[0113] ④可穿戴设备采集用户的生物信息特征并以量子密钥加密方式上传到量子密钥分配网络。量子密钥分配网络解密后得到用户上传的生物信息特征。

[0114] ⑤量子密钥分配网络比对用户上传的生物信息特征与原本存储的生物信息特征，决定本次登陆认证是否通过，并以量子密钥加密方式传回目标服务器。目标服务器解密后得到认证结果。

[0115] ⑥目标服务器向用户终端告知此次认证结果。

[0116] 本发明的身份认证尤其适合于复杂应用场合。例如同一个用户终端在一个较短的时间段内发出两次或者多次认证请求(比如先申请对目标服务器A的授权，再马上接着申请对目标服务器B的授权)，对于量子密钥分配网络，此时就可能出现前一次认证尚未完成，后一次认证就接着到来的情况，采用临时会话ID来区分两次不同的认证过程保证的身份认证的准确性。

[0117] 作为本实施例的简化方案，用户终端发起认证请求，在该认证请求得到响应之前(即认证通过或不通过之前)，不能发起另一次认证请求，即，在一个时间段内，一个用户设备仅会有一次认证请求，不需要采用临时会话ID来进行标识。此时，只需要采用用户终端的设备信息来标识在此次临时会话的身份即可。具体地，包括以下步骤：

[0118] S1：用户终端向目标服务器发起认证请求并提供所述用户终端的设备信息，目标服务器接收所述认证请求并生成临时会话，将设备信息发送至量子密钥分配网络；

[0119] S2：量子密钥分配网络接收所述设备信息，查找与用户终端绑定的可穿戴设备，将所述设备信息发送至所述可穿戴设备；

[0120] S3：所述可穿戴设备接收所述设备信息，采集用户的生物识别信息，将所述生物识别信息发送至量子密钥分配网络；

[0121] S4：所述量子密钥分配网络接收所述生物识别信息，并将所述生物识别信息与预存的生物识别信息进行匹配，若匹配成功则此次身份认证通过，将认证结果发送至目标服务器，继而发送至用户终端。

[0122] 实施例2

[0123] 基于实施例1的身份认证方法，本发明还提供了一种基于可穿戴设备的身份认证系统，包括：

[0124] 用户终端，用于向目标服务器发起认证请求并提供所述用户终端的设备信息，以

及接收目标服务器发送的认证结果；

[0125] 目标服务器，用于接收所述认证请求并生成临时会话，将临时会话ID和设备信息发送至量子密钥分配网络，以及接收量子密钥分配网络发送的认证结果，继而发送至用户终端；

[0126] 量子密钥分配网络，用于接收所述临时会话ID和设备信息，查找与所述用户终端绑定的可穿戴设备，向所述可穿戴设备发送所述临时会话ID，以及接收可穿戴设备发送的生物识别信息，并将其与预存的生物识别信息进行匹配，若匹配成功则所述临时会话ID对应的此次身份认证通过，将认证结果发送至目标服务器；

[0127] 可穿戴设备，用于接收所述临时会话ID，采集用户的生物识别信息，并将所述生物识别信息发送至量子密钥分配网络。

[0128] 所述目标服务器可以兼具所述身份认证功能和为用户终端提供业务访问功能；也可以仅具备身份认证功能，若所述目标服务器身份认证通过，由其他服务器为用户终端提供业务访问功能。

[0129] 可选地，所述设备信息是用户终端的设备ID或量子身份号，所述量子身份号是量子密钥分配网络为注册入网的可穿戴设备分配的全网唯一的身份标识，可穿戴设备与用户终端建立绑定关系后，量子身份号由可穿戴设备及与其绑定的用户终端所共享。

[0130] 可选地，所述查找与用户终端绑定的可穿戴设备的一种方式为：首先根据用户终端的设备ID在量子密钥分配网络查找到相应的量子身份号，然后查找具备该量子身份号的可穿戴设备，即为与所述用户终端绑定的可穿戴设备；若不能查找到则身份认证失败。其中，量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的可穿戴设备的量子身份号，以及与这些可穿戴设备绑定的用户终端的设备ID。

[0131] 可选地，所述查找与用户终端绑定的可穿戴设备的另一种方式为：根据用户终端的量子身份号，在量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备，即为目标可穿戴设备；若不能查找到，则此次身份认证失败。其中，量子密钥分配网络中预存的设备信息应至少包含注册到量子密钥分配网络的可穿戴设备的量子身份号。

[0132] 可选地，所述用户的生物识别信息包括以下一种或几种：指纹信息、心跳信息、血压信息、视网膜信息、虹膜信息、声纹信息、静脉信息、面部信息、笔迹签名信息。

[0133] 所述与预存的生物识别信息进行匹配的方式可以为：将自可穿戴设备接收的生物识别信息与量子密钥分配网络中预存的生物识别信息逐个对比，若查找到一致的生物识别信息则匹配成功，反之匹配失败，本次身份认证失败；也可以是量子密钥分配网络在本网络内存储的生物识别信息中检索自可穿戴设备接收的生物识别信息，如果检索到结果则说明认证请求发起者确为已经注册到量子密钥分配网络的合法用户，匹配成功，如果检索失败则匹配失败，本次身份认证失败。

[0134] 可选地，如图3所示，为了进一步提高认证过程中的安全性，匹配过程中在匹配过生物识别信息之后还对设备信息进行进一步验证，即，与预存的生物识别信息进行匹配的过程具体包括：

[0135] S41：量子密钥分配网络在本网络内存储的生物识别信息中检索可穿戴设备发送上来的生物识别信息，如果检索失败则本次身份认证失败。

[0136] S42：如果检索成功，则进一步查找量子密钥分配网络中存储的该条生物识别信息

所绑定的设备信息(量子身份号或设备ID,图3中以量子身份号为例),如图3所示,根据所述生物识别信息可以唯一确定与其绑定的可穿戴设备的量子身份号,以及与所述可穿戴设备绑定的用户终端的设备信息(设备ID或与可穿戴设备共享的量子身份号)。

[0137] S43:检查所述设备信息是否与来自目标服务器的设备信息相符。

[0138] S44:所述可穿戴设备向量子密钥分配网络发送生物识别信息的同时还发送了所述临时会话ID,所述量子密钥分配网络检查来自可穿戴设备的临时会话ID是否与来自目标服务器的临时会话ID相符。

[0139] S45:如果均相符,说明认证请求发起者的声称身份确实与现场采集到的实际身份相符,且属于同一次认证过程,匹配成功。

[0140] 可选地,可以仅验证所述设备信息是否与来自目标服务器的设备信息相符,或者仅验证来自可穿戴设备的临时会话ID是否与来自目标服务器的临时会话ID相符。

[0141] 其中,量子密钥分配网络中至少预存事先注册到本网络上的设备信息,以及与所述设备信息绑定的生物识别信息。

[0142] 可选地,各设备间的通信连接方式为:

[0143] 用户终端访问目标服务器。

[0144] 量子密钥分配网络与目标服务器中均预存第一共享密钥,用于二者之间通信数据的加密和解密。

[0145] 可穿戴设备与量子密钥分配网络中均预存第二共享密钥,用于二者之间通信数据的加密和解密。

[0146] 作为本实施例的简化方案,用户终端发起认证请求,在该认证请求得到响应之前(即认证通过或不通过之前),不能发起另一次认证请求,即,在一个时间段内,一个用户设备仅会有一次认证请求,不需要采用临时会话ID来进行标识。此时,只需要采用用户终端的设备信息来标识在此次临时会话的身份即可。具体地,所述基于可穿戴设备的身份认证系统,包括:

[0147] 用户终端,用于向目标服务器发起认证请求并提供所述用户终端的设备信息,以及接收目标服务器发送的认证结果;

[0148] 目标服务器,用于接收所述认证请求并生成临时会话,将设备信息发送至量子密钥分配网络,以及接收量子密钥分配网络发送的认证结果,继而发送至用户终端;

[0149] 量子密钥分配网络,用于接收所述设备信息,查找与所述用户终端绑定的可穿戴设备,向所述可穿戴设备发送所述设备信息,以及接收可穿戴设备发送的生物识别信息,并将其与预存的生物识别信息进行匹配,若匹配成功则身份认证通过,将认证结果发送至目标服务器;

[0150] 可穿戴设备,用于接收所述设备信息,采集用户的生物识别信息,并将所述生物识别信息发送至量子密钥分配网络。

[0151] 实施例3

[0152] 基于实施例1的身份认证方法,本实施例还提供了一种用于身份认证的量子密钥分配网络,包括:

[0153] 接收用户终端向目标服务器发起认证请求时提供的设备信息,以及目标服务器接收所述认证请求生成的临时会话ID;

[0154] 查找与所述用户终端绑定的可穿戴设备，向所述可穿戴设备发送所述临时会话ID；

[0155] 接收所述可穿戴设备采集并发送的生物识别信息，并将其与预存的生物识别信息进行匹配，若匹配成功则认证通过，将认证结果发送至目标服务器。

[0156] 可选地，所述设备信息是用户终端的设备ID或量子身份号，所述量子身份号是量子密钥分配网络为注册入网的可穿戴设备分配的全网唯一的身份标识，可穿戴设备与用户终端建立绑定关系后，量子身份号由可穿戴设备及与其绑定的用户终端所共享。

[0157] 其中，所述查找与用户终端绑定的可穿戴设备的一种方式包括：首先根据用户终端的设备ID在量子密钥分配网络查找到相应的量子身份号，然后查找具备该量子身份号的可穿戴设备，即为与所述用户终端绑定的可穿戴设备；若不能查找到则身份认证失败。其中，量子密钥分配网络中预存的设备信息应至少包含事先注册到所述量子密钥分配网络上的可穿戴设备的量子身份号，以及与这些可穿戴设备绑定的用户终端的设备ID。

[0158] 所述查找与用户终端绑定的可穿戴设备的另一种方式包括：根据用户终端的量子身份号，在量子密钥分配网络中预存的设备信息中查找具备该量子身份号的可穿戴设备，即为与所述用户终端绑定的可穿戴设备；若不能查找到，则此次身份认证失败。其中，量子密钥分配网络中预存的设备信息应至少包含注册到量子密钥分配网络的可穿戴设备的量子身份号。

[0159] 所述与预存的生物识别信息进行匹配之后还包括：进一步查找量子密钥分配网络中存储的该条生物识别信息所绑定的设备信息，判断所述设备信息是否与自目标服务器接收到的设备信息相一致；和/或

[0160] 判断接收自可穿戴设备的临时会话ID是否与自目标服务器接收到的临时会话ID相一致，其中接收自可穿戴设备的临时会话ID是所述可穿戴设备向量子密钥分配网络发送生物识别信息的同时发送的；

[0161] 若判断结果为一致，则认证通过；其中，量子密钥分配网络中至少预存事先注册到本网络上的设备信息和与所述设备信息绑定的生物识别信息。

[0162] 可选地，量子密钥分配网络与目标服务器中均预存第一共享密钥，用于二者之间通信数据的加密和解密。

[0163] 可选地，可穿戴设备与量子密钥分配网络中均预存第二共享密钥，用于二者之间通信数据的加密和解密。

[0164] 作为本实施例的简化方案，用户终端发起认证请求，在该认证请求得到响应之前(即认证通过或不通过之前)，不能发起另一次认证请求，即，在一个时间段内，一个用户设备仅会有一次认证请求，不需要采用临时会话ID来进行标识。此时，只需要采用用户终端的设备信息来标识在此次临时会话的身份即可。具体地，所述用于身份认证的量子密钥分配网络，包括：

[0165] 接收用户终端向目标服务器发起认证请求时提供的设备信息；

[0166] 查找与所述用户终端绑定的可穿戴设备，向所述可穿戴设备发送所述设备信息；

[0167] 接收所述可穿戴设备采集并发送的生物识别信息，并将其与预存的生物识别信息进行匹配，若匹配成功则认证通过，将认证结果发送至目标服务器。

[0168] 实施例4

[0169] 基于实施例1的身份认证方法，本实施例还提供了一种用于身份认证的可穿戴设备，与用户终端绑定，包括：

[0170] 接收量子密钥分配网络发送的临时会话ID，采集用户的生物识别信息，并将所述生物识别信息发送至量子密钥分配网络进行认证；所述临时会话ID是目标服务器接收所述用户终端发起的认证请求生成的，并由目标服务器发送至量子密钥分配网络。

[0171] 所述可穿戴设备在量子密钥分配网络注册并存储有全网独一无二的量子身份号，具有密钥存储及数据加解密和数据收发功能。

[0172] 可选地，可穿戴设备与量子密钥分配网络中均预存第二共享密钥，用于二者之间通信数据的加密和解密。

[0173] 作为本实施例的简化方案，用户终端发起认证请求，在该认证请求得到响应之前(即认证通过或不通过之前)，不能发起另一次认证请求，即，在一个时间段内，一个用户设备仅会有一次认证请求，不需要采用临时会话ID来进行标识。此时，只需要采用用户终端的设备信息来标识在此次临时会话的身份即可。具体地，所述用于身份认证的可穿戴设备，与用户终端绑定，包括：

[0174] 接收量子密钥分配网络发送的用户终端设备信息，采集用户的生物识别信息，并将所述生物识别信息发送至量子密钥分配网络进行认证；所述设备信息是用户终端向目标服务器发起认证请求时提供的，在目标服务器接收所述认证请求后发送至量子密钥分配网络。

[0175] 实施例5

[0176] 基于实施例1的身份认证方法，本实施例还提供了一种目标服务器，包括：

[0177] 接收用户终端发送的认证请求以及所述用户终端提供的设备信息，生成临时会话，并将临时会话ID和设备信息发送至量子密钥分配网络；

[0178] 将量子密钥分配网络发送的认证结果发送至所述用户终端。

[0179] 其中，所述目标服务器兼具身份认证功能和为用户终端提供业务访问的功能；或仅具备身份认证功能，若所述目标服务器身份认证通过，由其他服务器为用户终端提供业务访问功能。

[0180] 可选地，量子密钥分配网络与目标服务器中均预存第一共享密钥，用于二者之间通信数据的加密和解密。

[0181] 作为本实施例的简化方案，用户终端发起认证请求，在该认证请求得到响应之前(即认证通过或不通过之前)，不能发起另一次认证请求，即，在一个时间段内，一个用户设备仅会有一次认证请求，不需要采用临时会话ID来进行标识。此时，只需要采用用户终端的设备信息来标识在此次临时会话的身份即可。具体地，所述目标服务器，包括：

[0182] 接收用户终端发送的认证请求以及所述用户终端提供的设备信息，并将设备信息发送至量子密钥分配网络；

[0183] 将量子密钥分配网络发送的认证结果发送至所述用户终端。

[0184] 本发明对用户身份的认证，以一次一密的对称量子密钥取代了基于数学算法复杂度的加密方式，提高了安全性；将可穿戴设备介入目标服务器的登录认证，增强了用户体验；将量子密码技术、生物识别技术和可穿戴设备进行有机结合，极大提高了设备与设备之间、人和设备之间的身份认证的可靠性。由此，建立了一条从人(使用者)到远程业务服务器

的完整可靠认证链路，铺平了“最后一公里”的安全。

[0185] 量子密钥的使用方式均为一次一密。但如果降低安全性要求，使得密钥使用方式不再严格遵循一次一密，或者在本实施例的基础上，以其他密钥替代量子密钥，此种变通也应被视为本申请提案的保护范围。

[0186] 本领域技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算机装置来实现，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。本发明不限制于任何特定的硬件和软件的结合。

[0187] 上述虽然结合附图对本发明的具体实施方式进行了描述，但并非对本发明保护范围的限制，所属领域技术人员应该明白，在本发明的技术方案的基础上，本领域技术人员不需要付出创造性劳动即可做出的各种修改或变形仍在本发明的保护范围以内。

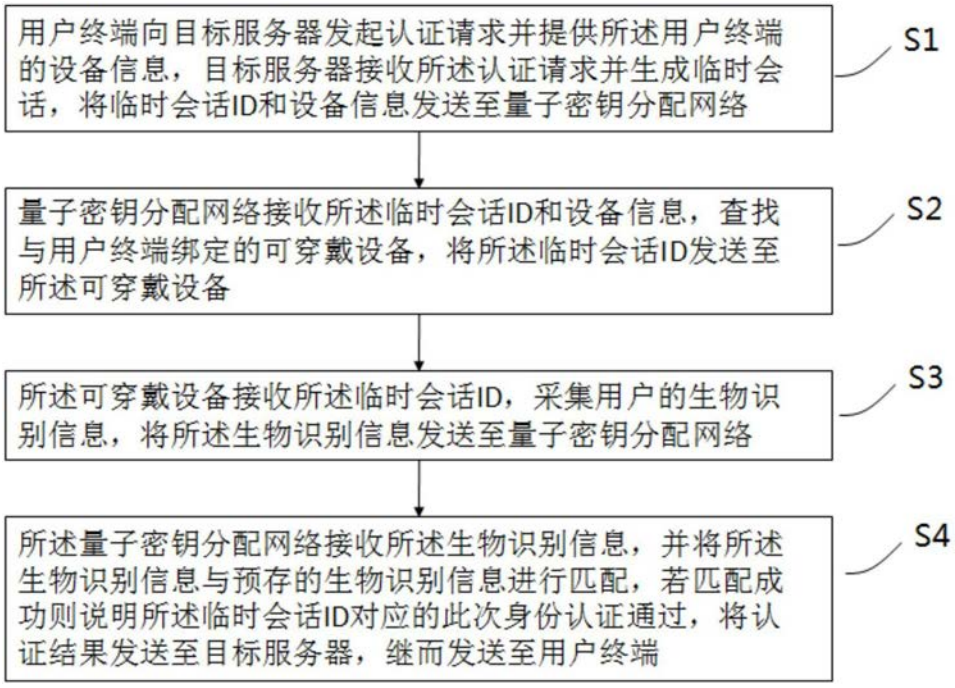

用户终端向目标服务器发起认证请求并提供所述用户终端的设备信息，目标服务器接收所述认证请求并生成临时会话，将临时会话ID和设备信息发送至量子密钥分配网络
S1
量子密钥分配网络接收所述临时会话ID和设备信息，查找与用户终端绑定的可穿戴设备，将所述临时会话ID发送至所述可穿戴设备
S2
所述可穿戴设备接收所述临时会话ID，采集用户的生物识别信息，将所述生物识别信息发送至量子密钥分配网络
S3
所述量子密钥分配网络接收所述生物识别信息，并将所述生物识别信息与预存的生物识别信息进行匹配，若匹配成功则说明所述临时会话ID对应的此次身份认证通过，将认证结果发送至目标服务器，继而发送至用户终端
S4

图1

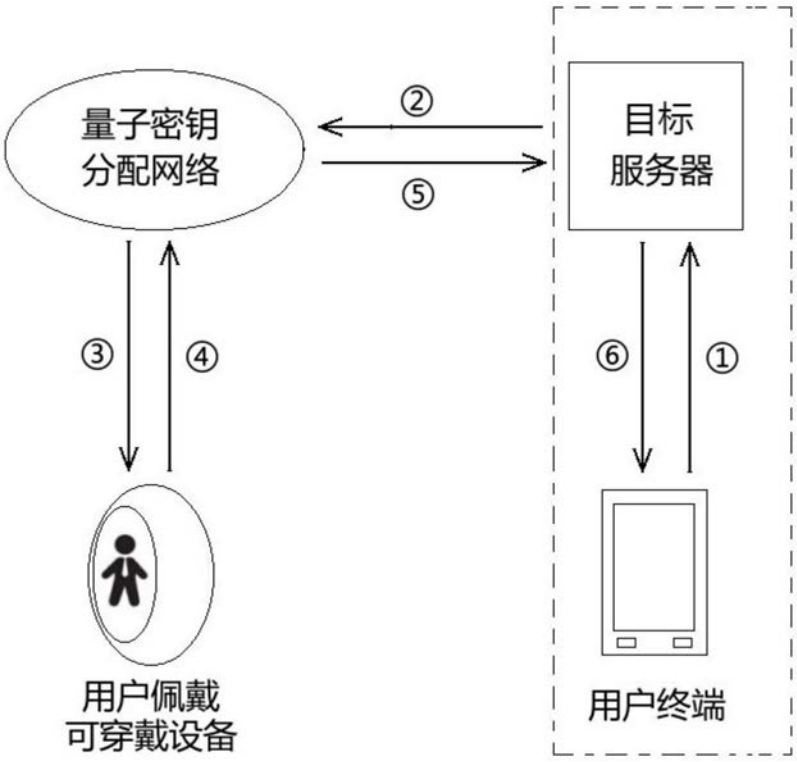

量子密钥分配网络
目标服务器
②
⑤
③
④
⑥
①
用户佩戴可穿戴设备
用户终端

图2

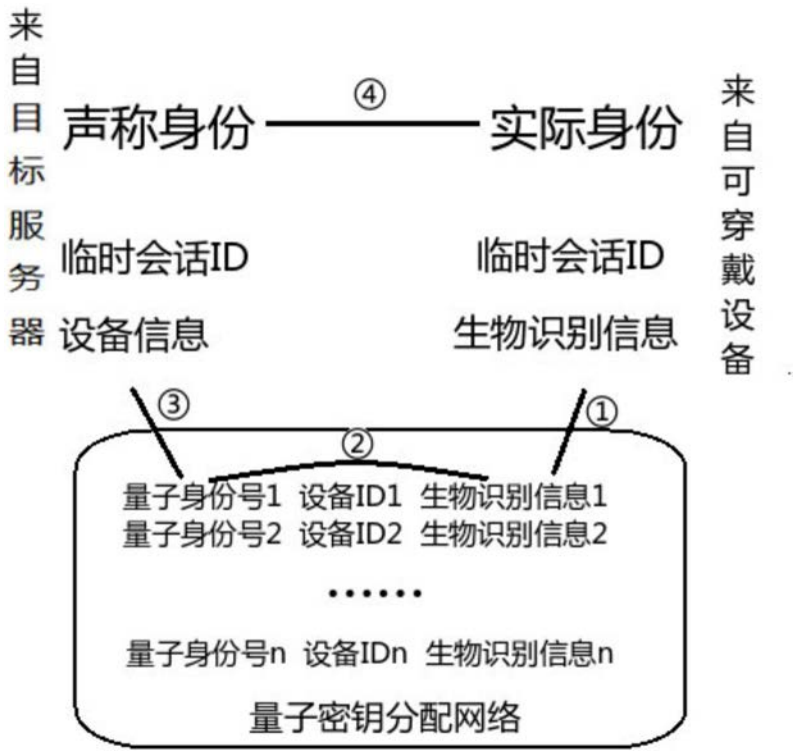

来自目标服务器
声称身份
④
实际身份
来自可穿戴设备
临时会话ID
临时会话ID
设备信息
生物识别信息
③
①
②
量子身份号1 设备ID1 生物识别信息1
量子身份号2 设备ID2 生物识别信息2
.....
量子身份号n 设备IDn 生物识别信息n
量子密钥分配网络

图3