(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 111355588 A
(43)申请公布日 2020.06.30

(21)申请号 202010102830.0

(22)申请日 2020.02.19

(71)申请人 武汉大学
地址 430072 湖北省武汉市武昌区珞珈山武汉大学

(72)发明人 刘树波 朱厚望 蔡朝晖 涂国庆 熊星星

(74)专利代理机构 武汉科皓知识产权代理事务所(特殊普通合伙) 42222
代理人 罗飞

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)

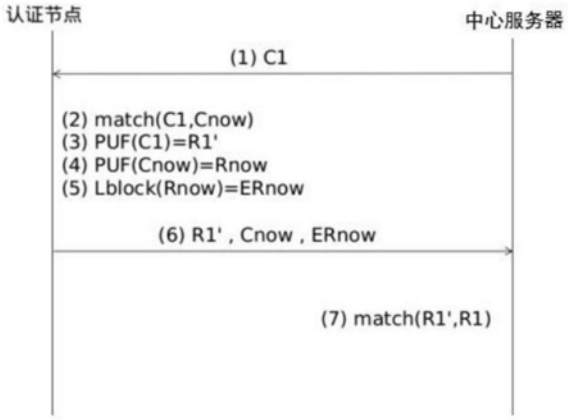
权利要求书2页 说明书8页 附图4页

(54)发明名称

一种基于PUF与指纹特征的可穿戴设备双因子认证方法及系统

(57)摘要

本发明提出一种基于PUF(物理不可克隆函数)和指纹生物特征的双因子认证方法,本方法基于对指纹生物特征匹配特点的分析,通过结合PUF认证方法,设计了一种新型的双因子认证方法。该认证方法利用设备物理特性和用户生物特征的双重唯一性,有效地增强了认证的安全性。



CN 111355588 A

1.一种基于PUF与指纹特征的可穿戴设备双因子认证方法,其特征在于,包括:

S1:认证节点利用弱PUF生成密钥,将密钥发送至中心服务器进行存储;

S2:认证节点采集用户的第一指纹特征值,并基于第一指纹特征值和强PUF生成第一响应,通过预设加密算法Lblock和密钥对第一响应进行加密,再将第一指纹特征值和加密后的第一响应发送至中心服务器,以使中心服务器通过密钥对加密后的第一响应进行解密,得到第一响应,并存储第一指纹特征值和第一响应;

S3:认证节点接收中心服务器发送的第一指纹特征值,并将第一指纹特征值与采集的当前第二指纹特征值进行匹配,当匹配成功时,利用第一指纹特征值生成第二响应,将第二响应和第二指纹特征值发送至中心服务器,以使中心服务器基于第一响应与第二响应之间的关系,判定是否认证成功。

2.如权利要求1所述的方法,其特征在于,认证节点包括节点ID,中心服务器根据节点ID对与节点对应的密钥进行存储,在S2之前,所述方法还包括:

认证节点向中心服务器发起注册请求,注册请求中包括节点ID,以使中心服务器在接收到注册请求后,根据认证节点的节点ID判断其激励响应对是否为空,进而判定是否进行注册,其中,激励响应对为与该认证节点对应的指纹特征值以及响应。

3.如权利要求1所述的方法,其特征在于,S2具体包括:

S2.1:认证节点采集用户的第一指纹特征值;

S2.2:认证节点将第一指纹特征值作为强PUF的输入,生成第一响应;

S2.3:认证节点重新产生密钥,作为预设加密算法Lblock的密钥输入,对第一响应进行加密,获得加密后的第一响应;

S2.4:认证节点将第一指纹特征值和加密后的第一响应发送至中心服务器,以使中心服务器通过存储的密钥对加密后的第一响应进行解密,获得第一响应,并对认证节点的激励响应对进行存储,认证节点的激励响应对为第一指纹和加密后的第一响应。

4.如权利要求1所述的方法,其特征在于,S3具体包括:

S3.1:认证节点接收中心服务器发送的第一指纹特征值,其中,第一指纹特征值由中心服务器检索后向对应的认证节点发送;

S3.2:认证节点采集用户当前的第二指纹特征值;

S3.3:认证节点将第一指纹特征值与采集的当前第二指纹特征值进行匹配,当匹配成功时,则执行S3.4,否则向中心服务器发送匹配失败,认证流程结束;

S3.4:认证节点将第一指纹特征值作为PUF的激励,生成第二响应;

S3.5:认证节点将第二响应和第二指纹特征值发送至中心服务器,以使中心服务器基于第一响应与第二响应之间的关系,判定是否认证成功。

5.如权利要求4所述的方法,其特征在于,在S3.4之后,所述方法还包括:

认证节点将第二指纹特征值作为PUF的激励,生成第三响应;

认证节点基于密钥和预设加密算法Lblock,对第三响应进行加密,获得加密后的第三响应,并将加密后的第三响应发送至中心服务器。

6.如权利要求5所述的方法,其特征在于,S3.5具体包括:

中心服务器比较第一响应与第二响应之间的汉明距离,当汉明距离小于指定阈值时,则认证成功,否则,认证失败。

7.如权利要求6所述的方法，其特征在于，在认证成功之后，所述方法还包括：

中心服务器删除之前存储的第一指纹特征值和第一响应；

采用密钥对加密后的第三响应进行解密，得到第三响应，并存储第二指纹特征值和第三响应。

8.一种基于PUF与指纹特征的可穿戴设备双因子认证方法，其特征在于，包括：

出厂模块，用于认证节点利用弱PUF生成密钥，将密钥发送至中心服务器进行存储；

注册模块，用于认证节点采集用户的第一指纹特征值，并基于第一指纹特征值和强PUF生成第一响应，通过预设加密算法Lblock和密钥对第一响应进行加密，再将第一指纹特征值和加密后的第一响应发送至中心服务器，以使中心服务器通过密钥对加密后的第一响应进行解密，得到第一响应，并存储第一指纹特征值和第一响应；

认证模块，用于认证节点接收中心服务器发送的第一指纹特征值，并将第一指纹特征值与采集的当前第二指纹特征值进行匹配，当匹配成功时，利用第一指纹特征值生成第二响应，将第二响应和第二指纹特征值发送至中心服务器，以使中心服务器基于第一响应与第二响应之间的关系，判定是否认证成功。

9.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被执行时实现如权利要求1至7中任一项权利要求所述的方法。

10.一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求1至7中任一项权利要求所述的方法。

一种基于PUF与指纹特征的可穿戴设备双因子认证方法及系统

技术领域

[0001] 本发明涉及信息安全隐私保护技术领域,具体涉及一种基于PUF与指纹特征的可穿戴设备双因子认证方法及系统。

背景技术

[0002] 可穿戴设备是置于用户身上的智能化微型设备,能从用户身上收集健康数据并分析,为用户提供健康服务。然而,由于可穿戴设备涉及用户隐私与数据安全,在无线体域网的开放式结构下,系统必须在节点设备与中心服务器之间提供一种安全认证机制。用于医疗的健康数据信息非常敏感,若其被非授权用户恶意盗取或篡改,会威胁到用户的数据安全甚至生命。

[0003] 为了解决穿戴设备资源受限的问题,基于物理不可克隆函数(PUF, Physically Unclonable Function)的认证方法被提出。PUF利用硅基器件固有的不可克隆物理特性提供激励(输入)到响应(输出)的唯一映射。基于PUF 的认证方法具有易实现与低消耗的优点,多应用于资源受限的嵌入式系统中的设备身份认证。

[0004] 本申请发明人在实施本发明的过程中,发现现有技术的方法,至少存在如下技术问题:

[0005] 目前已有多种基于生物特征的认证方法与密钥协商方案,但仅仅考虑到了用户生物特征的唯一性,忽略了物理设备特征的唯一性,使其容易收到假冒攻击。PUF认证方法也仅考虑了设备物理特征的唯一性,使其容易收到妥协攻击。此外,现有的PUF认证方法为了抵抗重放攻击,只能进行有限次数的认证,注册大量 CRP的同时增加了中心服务器的负担。

[0006] 也就是说,现有技术中存在安全性不高的技术问题。

发明内容

[0007] 有鉴于此,本发明提供了一种基于PUF与指纹特征的可穿戴设备双因子认证方法及系统,用以解决或者至少部分解决现有技术中存在的安全性不高的技术问题。

[0008] 为了解决上述技术问题,本发明第一方面提供了一种基于PUF与指纹特征的可穿戴设备双因子认证方法,包括:

[0009] S1:认证节点利用弱PUF生成密钥,将密钥发送至中心服务器进行存储;

[0010] S2:认证节点采集用户的第一指纹特征值,并基于第一指纹特征值和强PUF 生成第一响应,通过预设加密算法Lblock和密钥对第一响应进行加密,再将第一指纹特征值和加密后的第一响应发送至中心服务器,以使中心服务器通过密钥对加密后的第一响应进行解密,得到第一响应,并存储第一指纹特征值和第一响应;

[0011] S3:认证节点接收中心服务器发送的第一指纹特征值,并将第一指纹特征值与采集的当前第二指纹特征值进行匹配,当匹配成功时,利用第一指纹特征值生成第二响应,将第二响应和第二指纹特征值发送至中心服务器,以使中心服务器基于第一响应与第二响应

之间的关系，判定是否认证成功。

[0012] 在一种实施方式中，认证节点包括节点ID，中心服务器根据节点ID对与节点对应的密钥进行存储，在S2之前，所述方法还包括：

[0013] 认证节点向中心服务器发起注册请求，注册请求中包括节点ID，以使中心服务器在接收到注册请求后，根据认证节点的节点ID判断其激励响应对是否为空，进而判定是否进行注册，其中，激励响应对为与该认证节点对应的指纹特征值以及响应。

[0014] 在一种实施方式中，S2具体包括：

[0015] S2.1：认证节点采集用户的第一指纹特征值；

[0016] S2.2：认证节点将第一指纹特征值作为强PUF的输入，生成第一响应；

[0017] S2.3：认证节点重新产生密钥，作为预设加密算法Lblock的密钥输入，对第一响应进行加密，获得加密后的第一响应；

[0018] S2.4：认证节点将第一指纹特征值和加密后的第一响应发送至中心服务器，以使中心服务器通过存储的密钥对加密后的第一响应进行解密，获得第一响应，并对认证节点的激励响应对进行存储，认证节点的激励响应对为第一指纹和加密后的第一响应。

[0019] 在一种实施方式中，S3具体包括：

[0020] S3.1：认证节点接收中心服务器发送的第一指纹特征值，其中，第一指纹特征值由中心服务器检索后向对应的认证节点发送；

[0021] S3.2：认证节点采集用户当前的第二指纹特征值；

[0022] S3.3：认证节点将第一指纹特征值与采集的当前第二指纹特征值进行匹配，当匹配成功时，则执行S3.4，否则向中心服务器发送匹配失败，认证流程结束；

[0023] S3.4：认证节点将第一指纹特征值作为PUF的激励，生成第二响应；

[0024] S3.5：认证节点将第二响应和第二指纹特征值发送至中心服务器，以使中心服务器基于第一响应与第二响应之间的关系，判定是否认证成功。

[0025] 在一种实施方式中，在S3.4之后，所述方法还包括：

[0026] 认证节点将第二指纹特征值作为PUF的激励，生成第三响应；

[0027] 认证节点基于密钥和预设加密算法Lblock，对第三响应进行加密，获得加密后的第三响应，并将加密后的第三响应发送至中心服务器。

[0028] 在一种实施方式中，S3.5具体包括：

[0029] 中心服务器比较第一响应与第二响应之间的汉明距离，当汉明距离小于指定阈值时，则认证成功，否则，认证失败。

[0030] 在一种实施方式中，在认证成功之后，所述方法还包括：

[0031] 中心服务器删除之前存储的第一指纹特征值和第一响应；

[0032] 采用密钥对加密后的第三响应进行解密，得到第三响应，并存储第二指纹特征值和第三响应。

[0033] 基于同样的发明构思，本发明第二方面提供了一种基于PUF与指纹特征的可穿戴设备双因子认证系统，包括：

[0034] 出厂模块，用于认证节点利用弱PUF生成密钥，将密钥发送至中心服务器进行存储；

[0035] 注册模块，用于认证节点采集用户的第一指纹特征值，并基于第一指纹特征值和

强PUF生成第一响应,通过预设加密算法Lblock和密钥对第一响应进行加密,再将第一指纹特征值和加密后的第一响应发送至中心服务器,以使中心服务器通过密钥对加密后的第一响应进行解密,得到第一响应,并存储第一指纹特征值和第一响应;

[0036] 认证模块,用于认证节点接收中心服务器发送的第一指纹特征值,并将第一指纹特征值与采集的当前第二指纹特征值进行匹配,当匹配成功时,利用第一指纹特征值生成第二响应,将第二响应和第二指纹特征值发送至中心服务器,以使中心服务器基于第一响应与第二响应之间的关系,判定是否认证成功。

[0037] 基于同样的发明构思,本发明第三方面提供了一种计算机可读存储介质,其上存储有计算机程序,该程序被执行时实现第一方面所述的方法。

[0038] 基于同样的发明构思,本发明第四方面提供了一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现如第一方面所述的方法。

[0039] 本申请实施例中的上述一个或多个技术方案,至少具有如下一种或多种技术效果:

[0040] 本发明提供的一种基于PUF与指纹特征的可穿戴设备双因子认证方法,在出厂阶段,认证节点利用弱PUF生成密钥,将密钥发送至中心服务器进行存储;在注册阶段,认证节点采集用户的第一指纹特征值,并基于第一指纹特征值和强 PUF生成第一响应,通过预设加密算法Lblock和密钥对第一响应进行加密,再将第一指纹特征值和加密后的第一响应发送至中心服务器,以使中心服务器通过密钥对加密后的第一响应进行解密,得到第一响应,并存储第一指纹特征值和第一响应;在认证阶段,认证节点接收中心服务器发送的第一指纹特征值,并将第一指纹特征值与采集的当前第二指纹特征值进行匹配,当匹配成功时,利用第一指纹特征值生成第二响应,将第二响应和第二指纹特征值发送至中心服务器,以使中心服务器基于第一响应与第二响应之间的关系,判定是否认证成功。

[0041] 由于本发明提出了一种新颖的双因子(PUF与指纹特征)认证方法来保证物理特征和用户生物特征的双重唯一性,提升了假冒攻击的难度,增强了认证方法的安全性。该安全认证方法考虑了用户在非安全环境条件下的使用情形,在保护用户隐私数据安全的同时,增强了该安全认证方法的可用性。

附图说明

[0042] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0043] 图1为强PUF生成CRP(Challenge Response Pair,激励响应对)示意图;

[0044] 图2为一种实施例中双因子认证方法的出厂阶段流程示意图;

[0045] 图3为一种实施例中双因子认证方法的注册阶段流程示意图;

[0046] 图4为一种实施例中双因子认证方法的认证阶段流程示意图;

[0047] 图5为本发明实施例中一种基于PUF与指纹特征的可穿戴设备双因子认证系统的结构框图;

[0048] 图6为本发明实施例中一种计算机可读存储介质的结构框图；

[0049] 图7为本发明实施例中计算机设备的结构图。

具体实施方式

[0050] 为了解决现有基于单一PUF的认证方法与生物特征认证方法的局限性本发明提出了一种基于PUF与指纹生物特征的安全认证方法。与现有的方案相比，本方法能利用自身设备的物理特征有效地阻止假冒攻击和重放攻击，进一步增强认证方法的安全性。

[0051] 本发明的主要构思如下：

[0052] 对于同一指纹，每次提取的指纹特征值并不完全相同，但能两两匹配。基于这一特点，本发明提出一种基于PUF(物理不可克隆函数)和指纹生物特征的双因子认证方法，本方法基于对指纹生物特征匹配特点的分析，通过结合PUF认证方法，设计了一种新型的双因子认证方法。该认证方法利用设备物理特性和用户生物特征的双重唯一性，有效地增强了认证的安全性。

[0053] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0054] 实施例一

[0055] 本实施例提供了一种基于PUF与指纹特征的可穿戴设备双因子认证方法，该方法包括：

[0056] S1:认证节点利用弱PUF生成密钥，将密钥发送至中心服务器进行存储；

[0057] 具体来说，中心服务器与认证节点(可穿戴设备)组成一个网络系统，参与双方分别为中心服务器和认证节点。每个设备节点都是被认证方，中心服务器为认证方。该认证方法包括出厂、注册与认证三个阶段。出厂阶段在安全环境下进行，注册与认证阶段为用户的实际使用环境(非安全环境)。

[0058] 基于PUF的认证方法利用存储好的激励响应对(CRP,Challenge Response Pairs)实现。首先，需要从设备节点获取CRP并存储于后台数据库。认证时，认证节点根据数据库中的某条CRP记录的激励，生成对应的响应。若生成的响应与CRP记录中的响应一致，节点认证成功，否则认证失败。为抵抗重放攻击，每条CRP记录在认证完成后需要删除。

[0059] 在具体的实施过程中，激励信号(指纹特征)作用于PUF产生响应(输出) 如图1所示。PUF bits表示由FPGA生成的弱PUF，PUFbits输入至MUX2(二选一选择器)，由激励信号选择后，结果作为XOR(异或器)的输入，此XOR 的输出即为强PUF的响应。

[0060] 出厂阶段流程如图2所示。在安全环境下，认证节点利用FPGA生成80bit 的弱PUF，作为Lblock的加密密钥，以备注册与认证阶段使用，发送至中心服务器。

[0061] S2:认证节点采集用户的第一指纹特征值，并基于第一指纹特征值和强PUF 生成第一响应，通过预设加密算法Lblock和密钥对第一响应进行加密，再将第一指纹特征值和加密后的第一响应发送至中心服务器，以使中心服务器通过密钥对加密后的第一响应进行解密，得到第一响应，并存储第一指纹特征值和第一响应。

[0062] 具体来说，注册阶段，假设认证节点A要向中心服务器注册。则节点A采集用户的第

一指纹特征值C1,C1作为强PUF的输入(激励),经过PUF生成第一响应(输出)R1。为了避免重放攻击,节点A重新生成密钥Ka,将Ka作为 Lblock(一种轻量级对称加密算法)的加密密钥,利用Lblock将R1加密生成加密后的第一响应ER1。最后将(C1,ER1)发送至中心服务器,中心服务器将ER1 解密后得到R1。

[0063] S3:认证节点接收中心服务器发送的第一指纹特征值,并将第一指纹特征值与采集的当前第二指纹特征值进行匹配,当匹配成功时,利用第一指纹特征值生成第二响应,将第二响应和第二指纹特征值发送至中心服务器,以使中心服务器基于第一响应与第二响应之间的关系,判定是否认证成功。

[0064] 具体来说,例如认证节点A要向中心服务器认证。中心服务器取出节点A 对应的激励C1,发送至节点A。此时节点A采集用户当前的第二指纹特征值 Cnow,将Cnow与C1进行匹配(若C1＝＝Cnow则认证失败,因为每次采集同一指纹的特征并不一致)。若匹配失败,则向中心服务器返回失败标识码,中心服务器判定认证失败,若Cnow与C1匹配成功,则节点A利用C1经过PUF生成第二响应R1'。

[0065] 在一种实施方式中,认证节点包括节点ID,中心服务器根据节点ID对与节点对应的密钥进行存储,在S2之前,所述方法还包括:

[0066] 认证节点向中心服务器发起注册请求,注册请求中包括节点ID,以使中心服务器在接收到注册请求后,根据认证节点的节点ID判断其激励响应对是否为空,进而判定是否进行注册,其中,激励响应对为与该认证节点对应的指纹特征值以及响应。

[0067] 具体来说,认证节点有多个,每个认证节点具有唯一标识符节点ID,从而中心服务器可以根据节点ID对每个认证节点的信息进行存储。

[0068] 在一种实施方式中,S2具体包括:

[0069] S2.1:认证节点采集用户的第一指纹特征值;

[0070] S2.2:认证节点将第一指纹特征值作为强PUF的输入,生成第一响应;

[0071] S2.3:认证节点重新产生密钥,作为预设加密算法Lblock的密钥输入,对第一响应进行加密,获得加密后的第一响应;

[0072] S2.4:认证节点将第一指纹特征值和加密后的第一响应发送至中心服务器,以使中心服务器通过存储的密钥对加密后的第一响应进行解密,获得第一响应,并对认证节点的激励响应对进行存储,认证节点的激励响应对为第一指纹和加密后的第一响应。

[0073] 具体的实施过程中,注册阶段流程如图3所示,具体包括如下步骤:

[0074] Step1认证节点向中心服务器发起注册请求。

[0075] Step2中心服务器根据认证节点的ID判断其CRP(激励相应对)是否为空。若CRP为空,则应答同意注册;否则拒绝认证(为了避免一个设备绑定多个用户的情况,保证物理特征与用户生物特征的双重唯一性),认证流程结束。

[0076] Step3认证节点采集用户的第一指纹特征值C1。

[0077] Step4认证节点将C1作为PUF的激励(输入),使用图1的所示的PUF(C1) 生成响应第一响应R1。

[0078] Step5认证节点重新产生密钥Ka(其中,Ka是一个弱PUF,与出厂阶段的密钥相同,本发明可以无需存储,需要要用时再生成,从而提高了安全性),作为Lblock的密钥输入,R1经Lblock加密,通过Lblock(R1)变换生成加密后的第一响应:密文ER1(从而避免重放攻

击)。

[0079] Step6认证节点将C1和ER1发送至中心服务器。

[0080] Step7中心服务器将ER1解密得到R1,存储认证节点的C1与ER1,注册完成。

[0081] 在一种实施方式中,S3具体包括:

[0082] S3.1:认证节点接收中心服务器发送的第一指纹特征值,其中,第一指纹特征值由中心服务器检索后向对应的认证节点发送;

[0083] S3.2:认证节点采集用户当前的第二指纹特征值;

[0084] S3.3:认证节点将第一指纹特征值与采集的当前第二指纹特征值进行匹配,当匹配成功时,则执行S3.4,否则向中心服务器发送匹配失败,认证流程结束;

[0085] S3.4:认证节点将第一指纹特征值作为PUF的激励,生成第二响应;

[0086] S3.5:认证节点将第二响应和第二指纹特征值发送至中心服务器,以使中心服务器基于第一响应与第二响应之间的关系,判定是否认证成功。

[0087] 在一种实施方式中,在S3.4之后,所述方法还包括:

[0088] 认证节点将第二指纹特征值作为PUF的激励,生成第三响应;

[0089] 认证节点基于密钥和预设加密算法Lblock,对第三响应进行加密,获得加密后的第三响应,并将加密后的第三响应发送至中心服务器。

[0090] 具体来说,当第二指纹特征值Cnow与第一指纹特征值C1匹配成功,则认证节点A利用第一指纹特征值C1经过PUF生成第二响应R1',同时利用第二指纹特征值Cnow经过PUF并加密生成ERnow(加密后的第三响应)。将(R1',Cnow, ERnow)发送至中心服务器。中心服务器比对R1'与R1的汉明距离,若小于设定阈值,则判定认证成功并将ERnow解密得到Rnow,删除已有的CRP记录 (C1,R1),增加CRP记录(Cnow,Rnow);若R1'与R1的汉明距离大于设定阈值,判定认证失败。

[0091] 在一种实施方式中,S3.5具体包括:

[0092] 中心服务器比较第一响应与第二响应之间的汉明距离,当汉明距离小于指定阈值时,则认证成功,否则,认证失败。

[0093] 在一种实施方式中,在认证成功之后,所述方法还包括:

[0094] 中心服务器删除之前存储的第一指纹特征值和第一响应;

[0095] 采用密钥对加密后的第三响应进行解密,得到第三响应,并存储第二指纹特征值和第三响应。

[0096] 在具体的实施过程中,认证阶段流程如图4所示。

[0097] Step1中心服务器检索出认证节点的第一指纹特征值C1,并将C1发送至认证节点。

[0098] Step2认证节点收到C1,并采集用户的第二指纹特征值Cnow(若C1＝＝Cnow 则认证失败,因为每次所采集同一指纹的特征并不一致),匹配(match)C1与 Cnow的相似度,具体可以根据现有的指纹识别算法实现,若C1与Cnow匹配成功,则继续下一步step3;否则给中心服务器应答匹配失败,认证流程结束。

[0099] Step3认证节点将第一指纹特征值C1作为PUF的激励(输入),经PUF(C1) 生成PUF第二响应R1'。

[0100] Step4认证节点将第二指纹特征值Cnow作为PUF的激励(输入),经PUF (Cnow)生成PUF第三响应Rnow。

[0101] Step5 Rnow经Lblock加密生成密文ERnow(避免重放攻击)。

[0102] Step6认证节点将R1'、Cnow、ERnow发送至中心服务器

[0103] Step7中心服务器比较R1与R1'的汉明距离,若小于指定阈值,则认证成功,同时删除C1与R1,并解密ERnow得到Rnow,存储Cnow与Rnow;若R1与 R1'的汉明距离大于指定阈值,则认证失败。

[0104] 由上可见,认证节点在生成PUF响应的同时生成了新的注册信息(CRP),将认证信息与注册信息一同发往中心服务器。若认证成功,则新的CRP会取代该次认证所使用的CRP,以此达到一次注册多次认证。

[0105] 本发明基于对指纹特征与PUF认证方法的分析,提出了一种新颖的双因子认证方法来保证物理特征和用户生物特征的双重唯一性,提升了假冒攻击的难度,增强了认证方法的安全性。该安全认证方法考虑了用户在非安全环境条件下的使用情形,在保护用户隐私数据安全的同时,增强了该安全认证方法的可用性。

[0106] 与现有方案相比有如下有益的改进:

[0107] 1.同时确保了物理特征与用户生物特征的双重唯一性,增加了隐私数据的安全系数。

[0108] 2.一次注册,多次认证,在认证的同时生成注册信息,在防止重放攻击的基础上增加了可用性,更符合实际使用场景。

[0109] 3.解决了PUF认证方法需在安全环境下进行注册的局限性,本双因子认证方法的注册阶段可在用户使用环境(非安全环境)下进行,增加了方法的实用性。

[0110] 实施例二

[0111] 基于同样的发明构思,本实施例提供了一种基于PUF与指纹特征的可穿戴设备双因子认证系统,请参见图5,该系统包括:

[0112] 出厂模块201,用于认证节点利用弱PUF生成密钥,将密钥发送至中心服务器进行存储;

[0113] 注册模块202,用于认证节点采集用户的第一指纹特征值,并基于第一指纹特征值和强PUF生成第一响应,通过预设加密算法Lblock和密钥对第一响应进行加密,再将第一指纹特征值和加密后的第一响应发送至中心服务器,以使中心服务器通过密钥对加密后的第一响应进行解密,得到第一响应,并存储第一指纹特征值和第一响应;

[0114] 认证模块203,用于认证节点接收中心服务器发送的第一指纹特征值,并将第一指纹特征值与采集的当前第二指纹特征值进行匹配,当匹配成功时,利用第一指纹特征值生成第二响应,将第二响应和第二指纹特征值发送至中心服务器,以使中心服务器基于第一响应与第二响应之间的关系,判定是否认证成功。

[0115] 由于本发明实施例二所介绍的系统,为实施本发明实施例一中基于PUF与指纹特征的可穿戴设备双因子认证方法所采用的系统,故而基于本发明实施例一所介绍的方法,本领域所属人员能够了解该系统的具体结构及变形,故而在此不再赘述。凡是本发明实施例一的方法所采用的系统都属于本发明所欲保护的范围。

[0116] 实施例三

[0117] 请参见图6,基于同一发明构思,本申请还提供了一种计算机可读存储介质 300,其上存储有计算机程序311,该程序被执行时实现如实施例一中所述的方法。

[0118] 由于本发明实施例三所介绍的计算机可读存储介质为实施本发明实施例一中基于PUF与指纹特征的可穿戴设备双因子认证方法所采用的计算机可读存储介质，故而基于本发明实施例一所介绍的方法，本领域所属人员能够了解该计算机可读存储介质的具体结构及变形，故而在此不再赘述。凡是本发明实施例一中方法所采用的计算机可读存储介质都属于本发明所欲保护的范围。

[0119] 实施例四

[0120] 基于同一发明构思，本申请还提供了一种计算机设备，请参见图7，包括存储401、处理器402及存储在存储器上并可在处理器上运行的计算机程序403，处理器402执行上述程序时实现实施例一中的方法。

[0121] 由于本发明实施例四所介绍的计算机设备为实施本发明实施例一中基于 PUF与指纹特征的可穿戴设备双因子认证方法所采用的计算机设备，故而基于本发明实施例一所介绍的方法，本领域所属人员能够了解该计算机设备的具体结构及变形，故而在此不再赘述。凡是本发明实施例一中方法所采用的计算机设备都属于本发明所欲保护的范围。

[0122] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0123] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0124] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0125] 显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的精神和范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

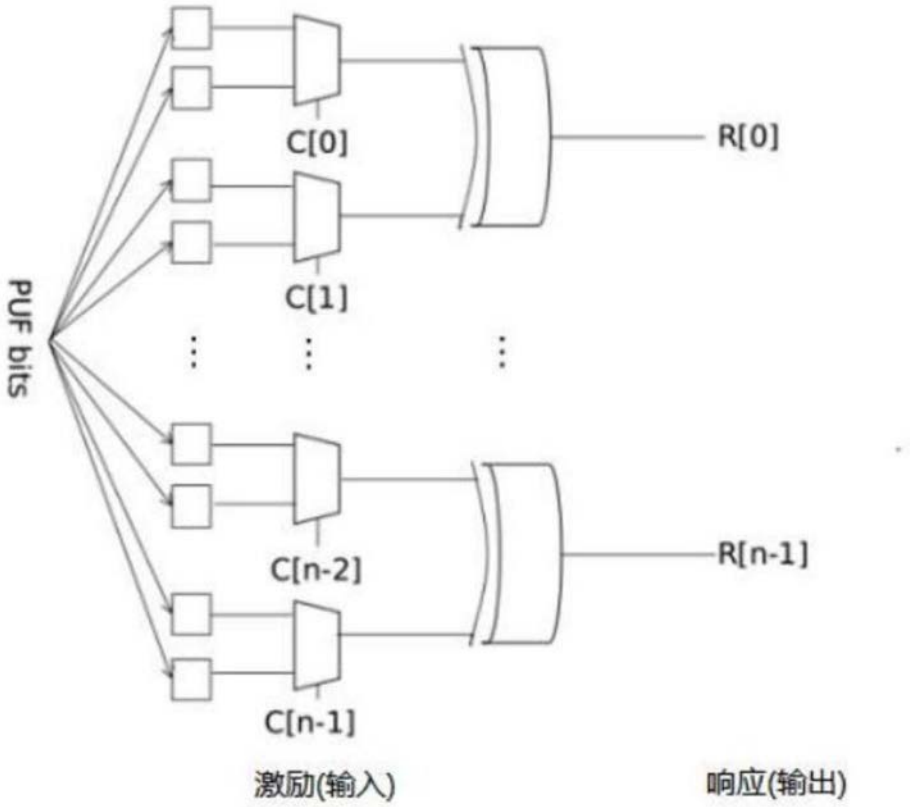


图1

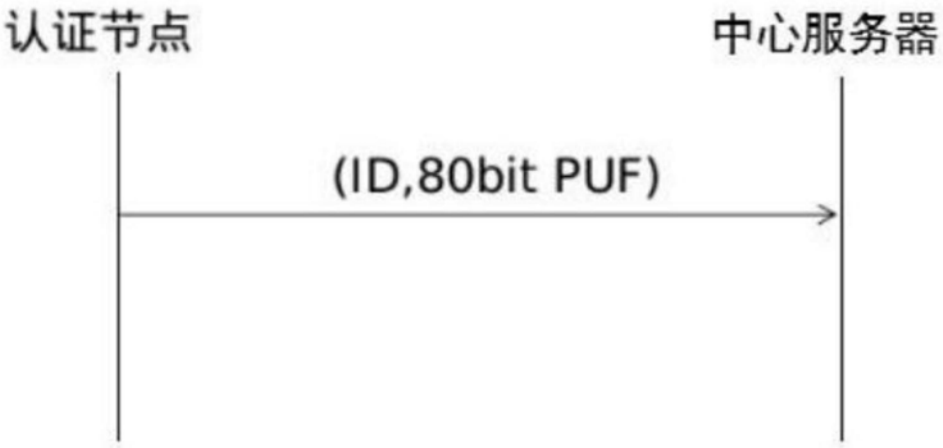


图2

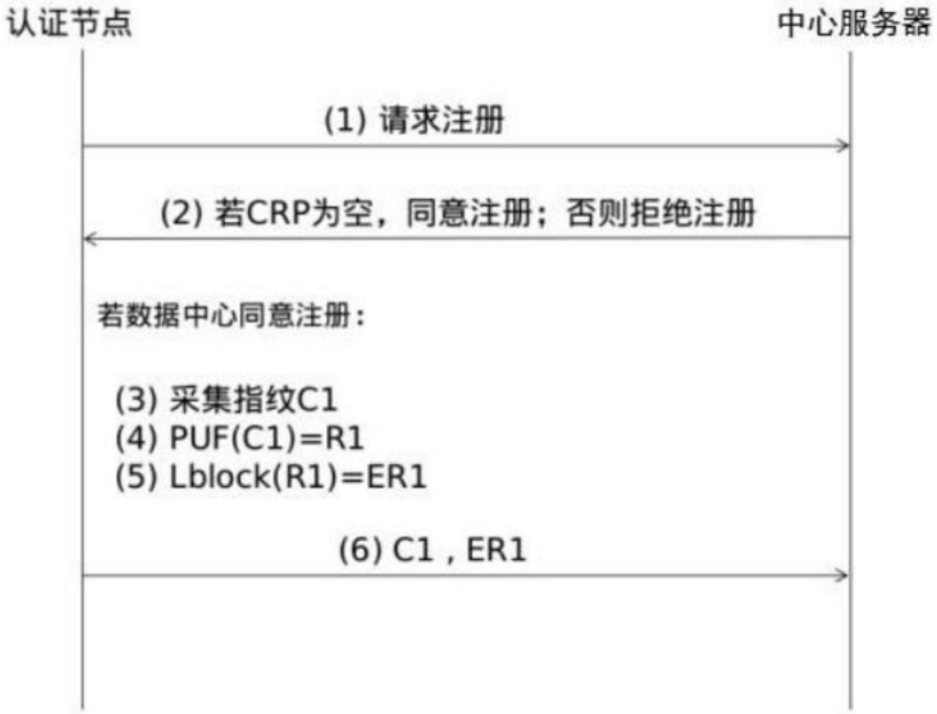

认证节点
中心服务器
(1) 请求注册
(2) 若CRP为空，同意注册；否则拒绝注册
若数据中心同意注册：
(3) 采集指纹C1
(4) PUF(C1)=R1
(5) Lblock(R1)=ER1
(6) C1 , ER1

图3

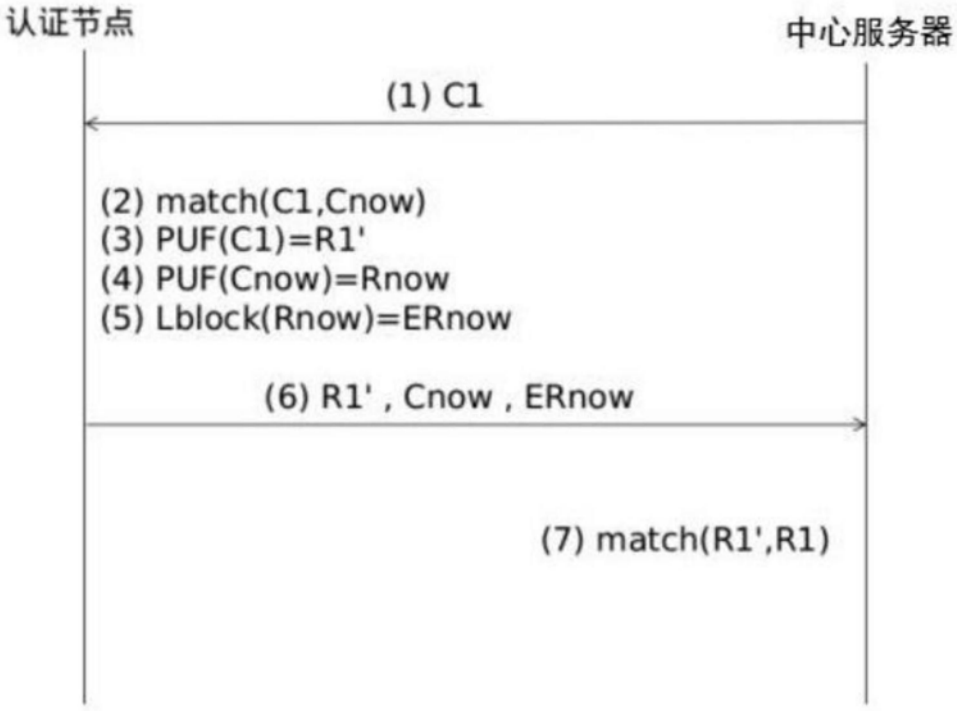

认证节点
中心服务器
(1) C1
(2) match(C1,Cnow)
(3) PUF(C1)=R1'
(4) PUF(Cnow)=Rnow
(5) Lblock(Rnow)=ERnow
(6) R1' , Cnow , ERnow
(7) match(R1',R1)

图4

图5

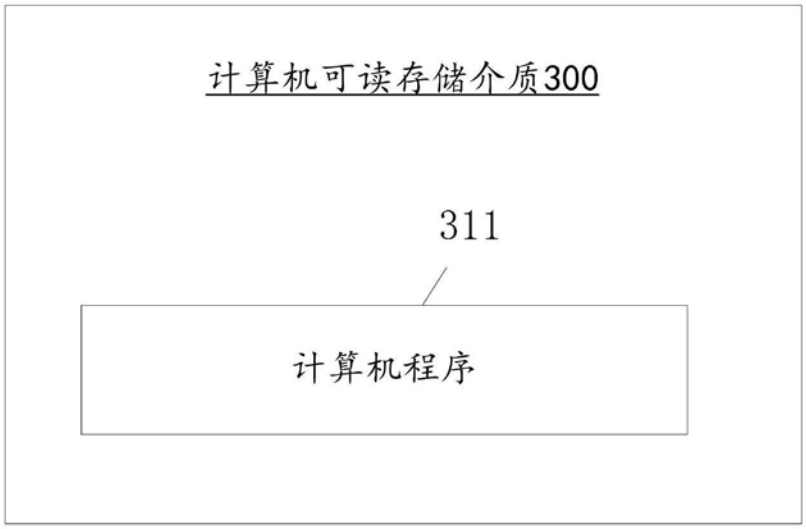


图6

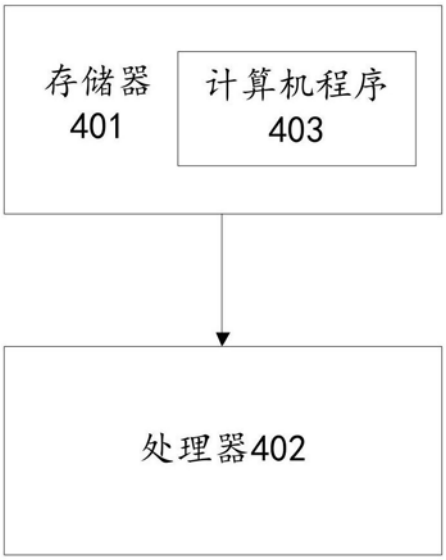


图7