



(12) 发明专利申请

(10) 申请公布号 CN 102255917 A

(43) 申请公布日 2011. 11. 23

(21) 申请号 201110233869. 7

(22) 申请日 2011. 08. 15

(71) 申请人 北京宏基恒信科技有限责任公司
地址 100044 北京市海淀区中关村南大街
56 号首都体育馆首体宾馆西配楼

(72) 发明人 潘斌 陈孟英

(74) 专利代理机构 北京清亦华知识产权代理事
务所(普通合伙) 11201
代理人 张大威

(51) Int. Cl.

H04L 29/06(2006. 01)

H04L 9/32(2006. 01)

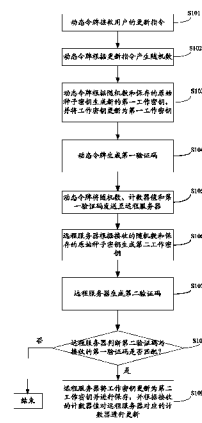
权利要求书 2 页 说明书 6 页 附图 2 页

(54) 发明名称

动态令牌的密钥更新及同步方法、系统及装置

(57) 摘要

本发明提出一种动态令牌的密钥更新及同步方法、系统及装置。其中,方法包括以下步骤:动态令牌根据用户发送的更新指令生成随机数,再根据随机数和原始种子密钥生成第一工作密钥以及生成第一验证码,并将动态令牌的工作密钥更新为第一工作密钥,然后将随机数、计数器值和第一验证码发送至远程服务器;远程服务器根据接收到的随机数和远程服务器中保存的原始种子密钥生成第二工作密钥以及生成第二验证码,再对第一验证码和第二验证码进行比对,并在验证码匹配时,将服务器的工作密钥更新为第二工作密钥,将服务器对应的计数器值更新为接收到的计数器值。本发明保证动态令牌的密钥安全性和动态令牌与服务器的同步性。



1. 一种动态令牌的密钥更新及同步方法,其特征在于,包括以下步骤:

动态令牌接收用户的更新指令;

所述动态令牌根据所述更新指令产生随机数;

所述动态令牌根据所述随机数和所述动态令牌中的原始种子密钥生成新的第一工作密钥,并将所述动态令牌的工作密钥更新为所述第一工作密钥;

所述动态令牌生成第一验证码;

将所述随机数、所述动态令牌中的计数器值和所述第一验证码发送至远程服务器;

所述远程服务器根据接收的随机数和所述远程服务器保存的原始种子密钥生成第二工作密钥,其中,所述远程服务器中第二工作密钥的生成算法和原始种子密钥分别与所述动态令牌中的第一工作密钥的生成算法和原始种子密钥相同;

所述远程服务器生成第二验证码,其中所述远程服务器中第二验证码的生成算法与所述动态令牌中第一验证码的生成算法相同;

所述远程服务器对所述第二验证码和接收的第一验证码进行验证;

如果所述第一验证码与所述第二验证码匹配,则将所述远程服务器的工作密钥更新为所述第二工作密钥并进行保存,并根据接收到的计数器值对所述远程服务器对应的计数器进行更新以使所述远程服务器与所述动态令牌同步。

2. 如权利要求1所述的动态令牌的密钥更新及同步方法,其特征在于,其中,所述动态令牌根据所述第一工作密钥和所述动态令牌中的计数器值生成所述第一验证码,所述远程服务器根据所述第二工作密钥和所述接收到的动态令牌的计数器值生成所述第二验证码。

3. 如权利要求1所述的动态令牌的密钥更新及同步方法,其特征在于,所述计数器值为计数器的当前值或计数器的尾数。

4. 如权利要求1所述的动态令牌的密钥更新及同步方法,其特征在于,所述动态令牌具有更新功能,所述用户通过特定的按键操作发送所述更新指令。

5. 一种动态令牌的密钥更新及同步系统,其特征在于,包括:

动态令牌,用于接收用户的更新指令,并根据所述更新指令产生随机数,以及根据所述随机数和所述动态令牌中的原始种子密钥生成新的第一工作密钥,并将动态令牌的工作密钥更新为所述第一工作密钥,以及生成第一验证码,并显示所述随机数、所述计数器值和所述第一验证码;和

远程服务器,用于根据接收的随机数和所述远程服务器保存的原始种子密钥生成第二工作密钥,并生成第二验证码,其中所述远程服务器中的原始种子密钥、第一工作密钥的生成算法、第一验证码的生成算法分别与所述动态令牌中的原始种子密钥、第二工作密钥的生成算法、第二验证码的生成算法相同,以及对所述第二验证码和接收的所述第一验证码进行验证,且在所述第二验证码与所述第一验证码匹配时,将远程服务器的工作密钥更新为所述第二工作密钥并保存,并根据接收的计数器值对所述远程服务器对应的计数器进行更新以使所述远程服务器与所述动态令牌同步。

6. 如权利要求5所述的动态令牌的密钥更新及同步系统,其特征在于,其中,所述动态令牌根据所述第一工作密钥和所述动态令牌中的计数器值生成所述第一验证码,所述远程服务器根据所述第二工作密钥和所述接收到的动态令牌的计数器值生成所述第二验证码。

7. 如权利要求5所述的动态令牌的密钥更新及同步系统,其特征在于,所述计数器值

为计数器的当前值或计数器的尾数。

8. 如权利要求 5 所述的动态令牌的密钥更新及同步系统,其特征在于,所述动态令牌具有更新功能,所述用户通过特定的按键操作发送所述更新指令。

9. 一种动态令牌,其特征在于,包括:

更新指令接收模块,用于接收用户的更新指令;

随机数产生模块,用于根据所述更新指令产生随机数;

计数器,用于进行时间计数或事件计数;

存储器,用于保存原始种子密钥和工作密钥;

工作密钥生成模块,用于根据所述随机数和所述原始种子密钥生成新的工作密钥,并将所述存储器中保存的工作密钥更新为所述新的工作密钥;

验证码生成模块,用于根据所述新的工作密钥和所述计数器的计数器值生成验证码;
和

显示器,用于显示所述随机数、所述计数器值和所述验证码。

10. 如权利要求 9 所述的动态令牌,其特征在于,所述计数器值为所述计数器的当前值或所述计数器的尾数。

11. 如权利要求 9 所述的动态令牌,其特征在于,还包括:

更新按键,所述用户通过特定的按键操作发送所述更新指令。

12. 一种远程服务器,其特征在于,包括:

接收模块,用于接收动态令牌生成的随机数、所述动态令牌中的计数器值和所述动态令牌生成的第一验证码;

计数器,用于进行时间计数或事件计数;

存储器,用于保存原始种子密钥和工作密钥,其中,所述远程服务器中保存的原始种子密钥与所述动态令牌中保存的原始种子密钥相同;

验证模块,用于根据接收的随机数和所述存储器保存的原始种子密钥生成新的工作密钥,并根据所述新的工作密钥和接收的所述计数器值生成第二验证码,以及对所述第二验证码和接收的第一验证码进行验证,其中所述工作密钥的生成算法和第二验证码的生成算法分别与动态令牌中的工作密钥的生成算法和第一验证码的生成算法相同;

种子密钥更新模块,用于在所述第二验证码与所述第一验证码匹配时,将所述存储器中存储的工作密钥更新为所述新的工作密钥并进行保存;和

同步模块,用于根据接收的计数器值对所述远程服务器对应的计数器进行更新以使所述远程服务器与所述动态令牌同步。

13. 如权利要求 12 所述的远程服务器,其特征在于,所述计数器值为所述计数器的当前值或所述计数器的尾数。

动态令牌的密钥更新及同步方法、系统及装置

技术领域

[0001] 本发明涉及信息安全技术领域,特别涉及一种动态令牌的密钥更新及同步方法、系统及装置。

背景技术

[0002] 身份认证是电子商务和电子政务等各种关键业务应用的安全基础。身份认证技术包括:静态口令认证、动态口令认证、生物技术认证、通过第三方发放的数字证书认证等。

[0003] 静态口令认证存在的问题是,由于静态口令的静态特性和重复实用性,其容易被窃取、猜测或破解,这样黑客就可以冒充合法身份进入个人账户,盗取关键资料,对用户造成严重的损失。

[0004] 其他的身份认证技术如生物认证、数字认证等,可以提供更高的安全强度,但是由于成本较高、使用难度大、环境要求复杂等问题,用户接受程度较低。

[0005] 动态口令认证由于每次产生的口令是变化的,因此有效地避免了被猜测和破解等,成为主要的认证技术之一,广泛应用于电子商务、远程访问、内部系统访问等身份认证。动态口令的技术实现包括软件方式(如安装在电脑、手机上)、短信方式、读卡器方式(将智能卡插入专用读卡器)、易携带的专用动态令牌等。由于动态令牌具有与携带、内部密钥不可读、使用方便等特性,成为当前主要的动态口令认证技术。

[0006] 目前,动态令牌存在的问题是,通常在动态令牌出厂时将种子密钥灌装至动态令牌之中,在用户使用后该种子密钥将不再变化,因此就可能会造成种子密钥在工厂灌装时的不安全。一旦种子密钥被获知,则该动态令牌的保密性将不复存在,因此动态令牌的安全性存在隐患。

发明内容

[0007] 本发明的目的旨在至少解决上述技术缺陷之一,特别是提出一种动态令牌的密钥更新及同步方法、系统及装置。

[0008] 为达到上述目的,本发明一方面提出一种动态令牌的密钥更新及同步方法,包括以下步骤:动态令牌接收用户的更新指令;所述动态令牌根据所述更新指令产生随机数;所述动态令牌根据所述随机数和所述动态令牌中的原始种子密钥生成新的第一工作密钥,并将所述动态令牌的工作密钥更新为所述第一工作密钥;所述动态令牌生成第一验证码;将所述随机数、所述动态令牌中的计数器值和所述第一验证码发送至远程服务器;所述远程服务器根据接收的随机数和所述远程服务器保存的原始种子密钥生成第二工作密钥,其中,所述远程服务器中第二工作密钥的生成算法和原始种子密钥分别与所述动态令牌中的第一工作密钥的生成算法和原始种子密钥相同;所述远程服务器生成第二验证码,其中所述远程服务器中第二验证码的生成算法与所述动态令牌中第一验证码的生成算法相同;所述远程服务器对所述第二验证码和接收的第一验证码进行验证;如果所述第一验证码与所述第二验证码匹配,则将所述远程服务器的工作密钥更新为所述第二工作密钥并进行保

存,并根据接收到的计数器值对所述远程服务器对应的计数器进行更新以使所述远程服务器与所述动态令牌同步。

[0009] 根据本发明实施例的动态令牌的密钥更新及同步方法,通过动态令牌产生随机数,根据该随机数生成工作密钥和验证码,并将随机数、验证码和动态令牌中的计数器值发送至远程服务器以进行验证从而进行更新和同步,保证动态令牌的密钥安全性,同时保证动态令牌和远程服务器的同步。而且,该更新及同步方法操作简单,便于使用。

[0010] 在本发明的一个实施例中,所述动态令牌根据所述第一工作密钥和所述动态令牌中的计数器值生成所述第一验证码,所述远程服务器根据所述第二工作密钥和所述接收到的动态令牌的计数器值生成所述第二验证码。

[0011] 在本发明的一个实施例中,所述计数器值为计数器的当前值或计数器的尾数。

[0012] 在本发明的一个实施例中,所述动态令牌具有更新功能,所述用户通过特定的按键操作发送所述更新指令。

[0013] 本发明另一方面还提出一种动态令牌的密钥更新及同步系统,包括:动态令牌,用于接收用户的更新指令,并根据所述更新指令产生随机数,以及根据所述随机数和所述动态令牌中的原始种子密钥生成新的第一工作密钥,并将动态令牌的工作密钥更新为所述第一工作密钥,以及生成第一验证码,并显示所述随机数、所述计数器值和所述第一验证码;和远程服务器,用于根据接收的随机数和所述远程服务器保存的原始种子密钥生成第二工作密钥,并生成第二验证码,其中所述远程服务器中的原始种子密钥、第一工作密钥的生成算法、第一验证码的生成算法分别与所述动态令牌中的原始种子密钥、第二工作密钥的生成算法、第二验证码的生成算法相同,以及对所述第二验证码和接收的所述第一验证码进行验证,且在所述第二验证码与所述第一验证码匹配时,将远程服务器的工作密钥更新为所述第二工作密钥并保存,并根据接收的计数器值对所述远程服务器对应的计数器进行更新以使所述远程服务器与所述动态令牌同步。

[0014] 在本发明的一个实施例中,所述动态令牌根据所述第一工作密钥和所述动态令牌中的计数器值生成所述第一验证码,所述远程服务器根据所述第二工作密钥和所述接收到的动态令牌的计数器值生成所述第二验证码。

[0015] 在本发明的一个实施例中,所述计数器值为所述计数器的当前值或所述计数器的尾数。

[0016] 在本发明的一个实施例中,所述动态令牌具有更新功能,所述用户通过特定的按键操作发送所述更新指令。

[0017] 根据本发明实施例的动态令牌的密钥更新及同步系统,通过动态令牌产生随机数,根据该随机数生成工作密钥和验证码,并将随机数、验证码和动态令牌中的计数器值发送至远程服务器以进行验证从而进行更新和同步,保证动态令牌的密钥安全性,同时保证动态令牌和远程服务器的同步。而且,该更新及同步系统操作简单,便于使用。

[0018] 本发明又一方面还提出一种动态令牌,包括:更新指令接收模块,用于接收用户的更新指令;随机数产生模块,用于根据所述更新指令产生随机数;计数器,用于进行时间计数或事件计数;存储器,用于保存原始种子密钥和工作密钥;工作密钥生成模块,用于根据所述随机数和所述原始种子密钥生成新的工作密钥,并将所述存储器中保存的工作密钥更新为所述新的工作密钥;验证码生成模块,用于根据所述新的工作密钥和所述计数器的计

计数器值生成验证码 ;和显示器,用于显示所述随机数、所述计数器值和所述验证码。

[0019] 在本发明的一个实施例中,所述计数器值为计数器的当前值或计数器的尾数值。

[0020] 在本发明的一个实施例中,所述动态令牌还包括更新按键,所述用户通过特定的按键操作发送所述更新指令。

[0021] 根据本发明实施例的动态令牌,通过产生随机数以生成工作密钥和验证码从而进行验证和更新,保证了动态令牌密钥的安全性。

[0022] 本发明再一方面还提出一种远程服务器,包括:接收模块,用于接收动态令牌生成的随机数、所述动态令牌中的计数器值和所述动态令牌生成的第一验证码;计数器,用于进行时间计数或事件计数;存储器,用于保存原始种子密钥和工作密钥,其中,所述远程服务器中保存的原始种子密钥与所述动态令牌中保存的述原始种子密钥相同;验证模块,用于根据接收的随机数和所述存储器保存的原始种子密钥生成新的工作密钥,并根据所述工作密钥和接收的所述计数器值生成第二验证码,以及对所述第二验证码和接收的第一验证码进行验证;种子密钥更新模块,用于在所述第二验证码与所述第一验证码匹配时,将所述存储器中保存的工作密钥更新为所述新的工作密钥并进行保存;和同步模块,用于根据接收的计数器值对所述远程服务器对应的计数器进行更新以使所述远程服务器与所述动态令牌同步。

[0023] 在本发明的一个实施例中,所述计数器值为所述计数器的当前值或所述计数器的尾数值。

[0024] 根据本发明实施例的远程服务器,通过接收动态令牌生成的验证码进行比对以判断是否更新工作密钥,并且在更新工作密钥的同时更新计数器,保证了动态令牌的安全性,同时保证了动态令牌和远程服务器的同步性。

[0025] 本发明附加的方面和优点将在下面的描述中部分给出,部分将从下面的描述中变得明显,或通过本发明的实践了解到。

附图说明

[0026] 本发明上述的和 / 或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解,其中:

[0027] 图 1 为本发明实施例的动态令牌的密钥更新及同步方法的流程图;

[0028] 图 2 为本发明实施例的动态令牌的密钥更新及同步系统的结构示意图;

[0029] 图 3 为本发明实施例的动态令牌的结构示意图;以及

[0030] 图 4 为本发明实施例的远程服务器的结构示意图。

具体实施方式

[0031] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,仅用于解释本发明,而不能解释为对本发明的限制。

[0032] 如图 1 所示,根据本发明实施例的动态令牌的密钥更新及同步方法,包括以下步骤:

[0033] 步骤 S101,动态令牌接收用户的更新指令。

[0034] 动态令牌具有更新功能,用户可通过特定的按键操作发送更新指令。例如,在动态令牌上可设有更新按键,用户可通过长时间按压该更新按键发送更新指令。

[0035] 步骤 S102,动态令牌根据更新指令产生随机数。

[0036] 在本发明的一个实施例中,随机数 r 为 8 字节的随机数据。

[0037] 应理解,为了保证数据传输的安全性,随机数的字节长度越长越好,一般来说,字节长度为 24 位时可保证其安全性。

[0038] 步骤 S103,动态令牌根据随机数和动态令牌中的原始种子密钥生成新的第一工作密钥,并将动态令牌的工作密钥更新为生成的第一工作密钥。

[0039] 动态令牌在灌装时灌装有原始种子密钥,该原始种子密钥可为 20 或 32 字节的随机数据。

[0040] 步骤 S104,动态令牌生成第一验证码。

[0041] 具体地,动态令牌可根据第一工作密钥和动态令牌中的计数器值生成第一验证码,其中,计数器值可为计数器的当前值,也可为计数器的尾数。

[0042] 步骤 S105,将随机数、动态令牌中的计数器值和第一验证码发送至远程服务器。

[0043] 具体地,上述随机数、动态令牌中的计数器值和第一验证码可在动态令牌的显示器上进行显示,然后用户可通过柜台等将随机数、计数器值和第一验证码输入至服务器。

[0044] 应理解,随机数、动态令牌中的计数器值和第一验证码可以按顺序排列显示,也可以交错显示以提高数据安全性。

[0045] 步骤 S106,远程服务器根据接收的随机数和远程服务器保存的原始种子密钥生成第二工作密钥。

[0046] 远程服务器中保存的原始种子密钥与动态令牌中保存的原始种子密钥相同,远程服务器中第二工作密钥的生成算法与动态令牌中第一工作密钥的生成算法相同。

[0047] 步骤 S107,远程服务器生成第二验证码。

[0048] 远程服务器中第二验证码的生成算法与动态令牌中第一验证码的生成算法相同,由此保证密码验证的可行性。

[0049] 具体地,远程服务器可根据接收到的计数器值和第二工作密钥生成第二验证码。

[0050] 步骤 S108,远程服务器对生成的第二验证码和接收的第一验证码进行验证。

[0051] 也就是说,远程服务器对生成的第二验证码和接收的第一验证码进行比对以判断其生成的第二验证码与动态令牌生成的第一验证码是否匹配。

[0052] 步骤 S109,如果第二验证码与第一验证码匹配,则将远程服务器的工作密钥更新为第二工作密钥并进行保存,并根据接收的计数器值对远程服务器对应的计数器进行更新以使远程服务器与动态令牌同步。

[0053] 如果动态令牌生成的第一验证码与远程服务器生成的第二验证码匹配,则动态令牌通过了验证可以进行正常使用。此时,如果远程服务器对应的计数器的计数值与接收到的计数值不相同,则强制将远程服务器的值更新为接收到的计数值以保证远程服务器与动态令牌的同步,从而保证动态令牌的正常使用。

[0054] 如果动态令牌生成的第一验证码与远程服务器生成的第二验证码不匹配,则动态令牌未通过验证不能正常使用。

[0055] 需要说明的是,该更新操作可多次执行,因而在远程服务器数据泄密后,可以通过

再次更新动态令牌密钥使得动态令牌在保密状态下工作。

[0056] 根据本发明实施例的动态令牌的密钥更新及同步方法,通过动态令牌产生随机数,根据该随机数生成工作密钥和验证码,并将随机数、验证码和动态令牌中的计数器值发送至远程服务器以进行验证从而进行更新和同步,保证动态令牌的密钥安全性,同时保证动态令牌和远程服务器的同步。而且,该更新及同步方法操作简单,便于使用。

[0057] 为实现上述实施例,本发明还提出一种动态令牌的密钥更新及同步系统。如图 2 所示,该系统包括:动态令牌 1 和远程服务器 2。

[0058] 动态令牌 1 接收用户的更新指令,并根据更新指令产生随机数,再根据随机数和保存的原始种子密钥生成新的第一工作密钥,以及生成第一验证码,并显示随机数、计数器值和第一验证码。

[0059] 远程服务器 2 接收随机数、计数器值和第一验证码,根据接收到的随机数和保存的原始种子密钥生成第二工作密钥,以及生成第二验证码,然后对第二验证码和接收到的第一验证码进行验证,在第二验证码与第一验证码匹配时,将保存的工作密钥更新为第二工作密钥并保存,同时根据接收到的计数器值对远程服务器 2 对应的计数器进行更新以使远程服务器 2 与动态令牌 1 同步。

[0060] 具体地,动态令牌 1 可根据第一工作密钥和动态令牌 1 中的计数器值生成第一验证码。远程服务器 2 可根据第二工作密钥和接收到的计数器值生成第二验证码。

[0061] 在本发明的一个实施例中,计数器值可以为计数器的当前值,也可以为计数器的尾数。

[0062] 此外,动态令牌可具有更新功能,用户通过特定的按键操作发送更新指令,例如长时间按键更新按键。

[0063] 根据本发明实施例的动态令牌的密钥更新及同步系统,通过动态令牌产生随机数,根据该随机数生成工作密钥和验证码,并将随机数、验证码和动态令牌中的计数器值发送至远程服务器以进行验证从而进行更新和同步,保证动态令牌的密钥安全性,同时保证动态令牌和远程服务器的同步。而且,该更新及同步系统操作简单,便于使用。

[0064] 为实现上述实施例,本发明还提出一种动态令牌 1。如图 3 所示,该动态令牌 1 包括:更新指令接收模块 110、随机数产生模块 120、计数器 130、存储器 140、工作密钥生成模块 150、验证码生成模块 160 和显示器 170。

[0065] 更新指令接收模块 110 用于接收用户的更新指令。随机数产生模块 120 用于根据更新指令产生随机数。计数器 130 用于进行时间计数或事件计数。存储器 140 用于保存原始种子密钥和工作密钥。工作密钥生成模块 150 用于根据随机数和原始种子密钥生成新的工作密钥,并将存储器 140 中保存的工作密钥更新为新的工作密钥。验证码生成模块 160 用于根据新的工作密钥和计数器的计数器值生成验证码。显示器 170 用于显示随机数、计数器值和验证码。

[0066] 具体地,验证码生成模块 160 和显示器 170 中的计数器值可以为计数器 130 的当前值,也可以为计数器 130 的尾数。

[0067] 在本发明的一个实施例中,该动态令牌 1 还可包括更新按键,用户通过特定的按键操作发送更新指令,例如长时间按压更新按键。

[0068] 根据本发明实施例的动态令牌,通过产生随机数以生成工作密钥和验证码从而进

行验证和更新,保证了动态令牌密钥的安全性。

[0069] 为实现上述实施例,本发明还提出一种远程服务器 2。如图 4 所示,该远程服务器 2 包括:接收模块 210、计数器 220、存储器 230、验证模块 240、种子密钥更新模块 250 和同步模块 260。

[0070] 接收模块 210 用于接收动态令牌 1 生成的随机数、动态令牌 1 中的计数器值和动态令牌 1 生成的第一验证码。计数器 220 用于进行时间计数或事件计数。存储器 230 用于保存原始种子密钥和工作密钥,其中,远程服务器 2 中保存的原始种子密钥与动态令牌 1 中保存的原始种子密钥相同。验证模块 240 用于根据接收的随机数和远程服务器 2 保存的原始种子密钥生成工作密钥,并根据工作密钥和接收的计数器值生成第二验证码,以及对第二验证码和接收的第一验证码进行验证。种子密钥更新模块 250 用于在第一验证码与第二验证码匹配时,将存储器 230 中保存的工作密钥更新成生成的工作密钥进行保存。同步模块 260 用于根据接收的计数器值对远程服务器 2 对应的计数器进行更新以使远程服务器 2 与动态令牌 1 同步。

[0071] 在本发明的一个实施例中,计数器值可以为计数器的当前值也可以为尾数。

[0072] 根据本发明实施例的远程服务器,通过接收动态令牌生成的验证码进行比对以判断是否更新工作密钥,并且在更新工作密钥的同时更新计数器,保证了动态令牌的安全性,同时保证了动态令牌和远程服务器的同步性。

[0073] 尽管已经示出和描述了本发明的实施例,对于本领域的普通技术人员而言,可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型,本发明的范围由所附权利要求及其等同限定。

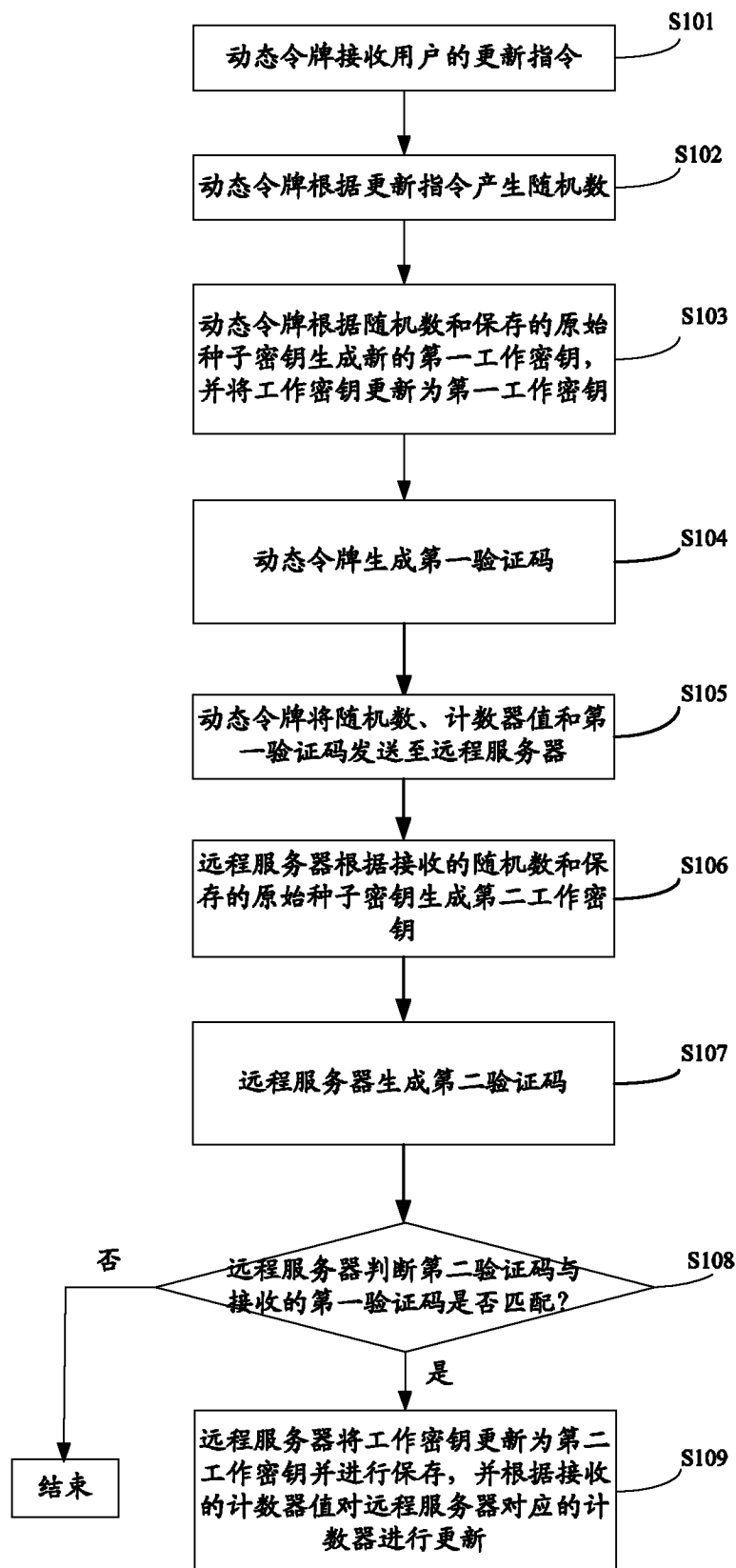


图 1

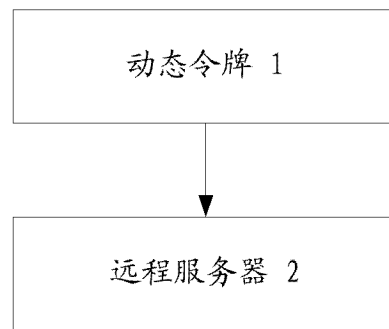


图 2

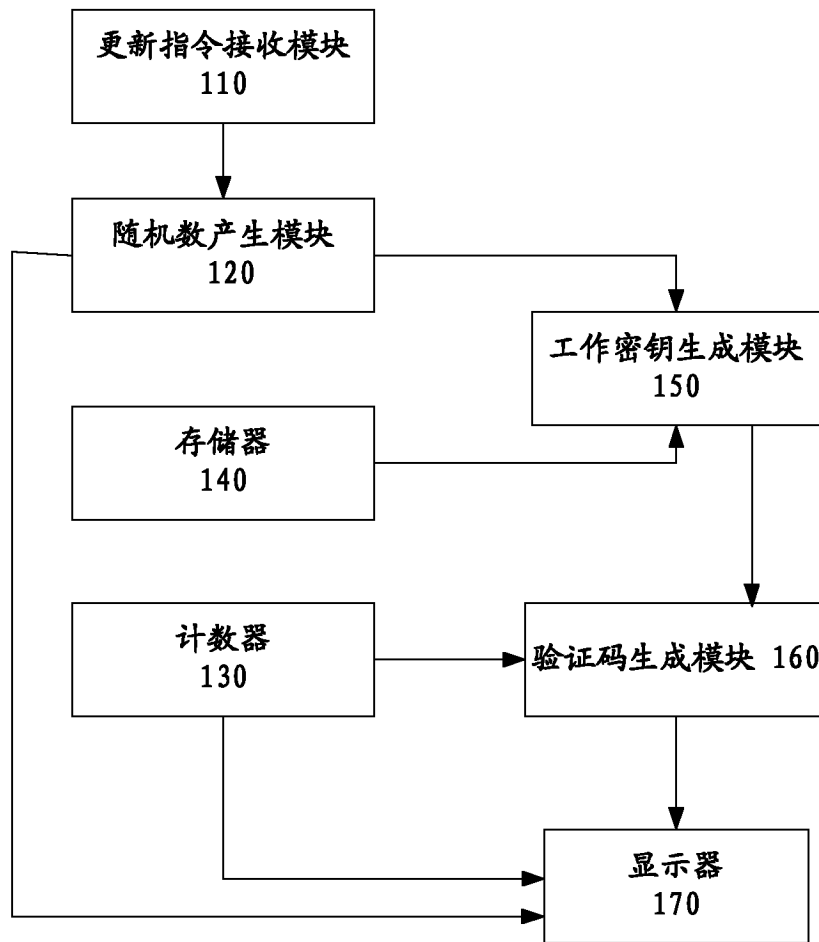


图 3

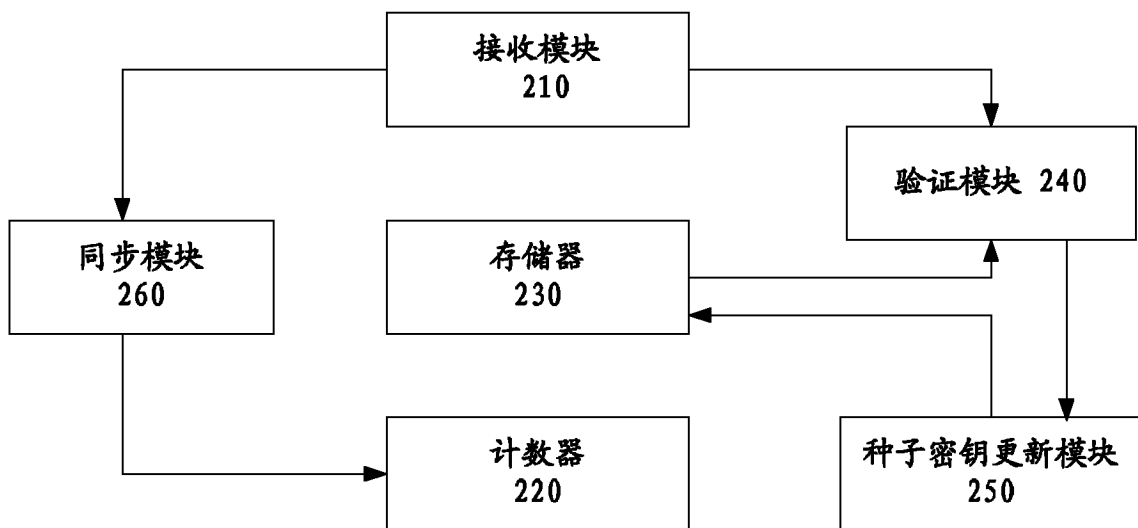


图 4