



(12) 发明专利

(10) 授权公告号 CN 111817851 B

(45) 授权公告日 2020.12.08

(21) 申请号 202010944227.7

H04L 9/32 (2006.01)

(22) 申请日 2020.09.10

(56) 对比文件

(65) 同一申请的已公布的文献号

WO 2014006618 A1, 2014.01.09

申请公布号 CN 111817851 A

CN 104025504 A, 2014.09.03

(43) 申请公布日 2020.10.23

审查员 陈晓伟

(73) 专利权人 北京深思数盾科技股份有限公司

地址 100193 北京市海淀区西北旺东路10

号院东区5号楼5层510

(72) 发明人 刘书深 孙吉平 念龙龙

(74) 专利代理机构 北京山允知识产权代理事务

所(特殊普通合伙) 11741

代理人 胡冰

(51) Int. Cl.

H04L 9/08 (2006.01)

H04L 9/06 (2006.01)

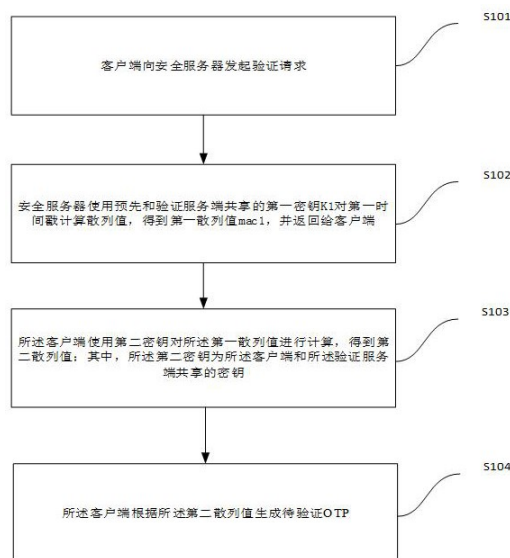
权利要求书3页 说明书10页 附图4页

(54) 发明名称

OTP生成方法、验证方法、终端、服务器、芯片和介质

(57) 摘要

本发明提出一种OTP生成方法、验证方法、终端、服务器、芯片和介质,其中,密码OTP生成方法包括:客户端向安全服务器发起验证请求;所述客户端从所述安全服务器接收第一散列值;其中,所述第一散列值由所述安全服务器使用第一密钥对第一时间戳计算得到,所述第一密钥为所述安全服务器与验证服务端共享的密钥,所述第一时间戳用于指示所述客户端发起所述验证请求的时间;所述客户端使用第二密钥对所述第一散列值进行计算,得到第二散列值;其中,所述第二密钥为所述客户端和所述验证服务端共享的密钥;所述客户端根据所述第二散列值生成待验证OTP。本发明使得客户端和验证端都在用户侧的使用环境中,OTP的生成和验证过程都是安全的。



1. 一种一次性密码OTP的生成方法,其特征在于,包括:  
客户端向安全服务器发起验证请求;  
所述客户端从所述安全服务器接收第一散列值;其中,所述第一散列值由所述安全服务器使用第一密钥对第一时间戳计算得到,所述第一密钥为所述安全服务器与验证服务端共享的密钥,所述第一时间戳用于指示所述客户端发起所述验证请求的时间;  
所述客户端使用第二密钥对所述第一散列值进行计算,得到第二散列值;其中,所述第二密钥为所述客户端和所述验证服务端共享的密钥;  
所述客户端根据所述第二散列值生成待验证OTP。
2. 根据权利要求1所述的方法,其特征在于,所述第一密钥的安全等级高于所述第二密钥的安全等级。
3. 根据权利要求1所述的方法,其特征在于,所述第二密钥以在所述客户端设置的密码作为密钥种子生成。
4. 根据权利要求1-3任一项所述的方法,其特征在于,  
当存在多个验证服务端时,每个所述验证服务端分别与所述安全服务器共享一个第一密钥,或者,所述多个验证服务端与所述安全服务器共享同一个第一密钥。
5. 根据权利要求4所述的方法,其特征在于,当所述多个验证服务端与所述安全服务器共享同一个第一密钥时,所述第一散列值由所述安全服务器使用随机盐值以及所述第一密钥对第一时间戳计算得到。
6. 根据权利要求1-3任一项所述的方法,其特征在于,  
所述第一时间戳由所述客户端获取,所述验证请求携带所述第一时间戳;或者,所述第一时间戳由所述安全服务器获取。
7. 根据权利要求1-3任一项所述的方法,其特征在于,  
所述安全服务器包括加密机,所述第一密钥存储于所述加密机中,所述第一散列值在所述加密机中计算得到。
8. 一种一次性密码OTP的验证方法,其特征在于,包括:  
验证服务端接收待验证OTP;  
所述验证服务端基于第二时间戳确定时间窗口;其中,所述第二时间戳用于指示所述验证服务端开始验证所述待验证OTP的时间,所述第二时间戳处于所述时间窗口内,并且,所述时间窗口包含至少两个时间点;  
所述验证服务端使用第一密钥,分别对每个时间点进行计算,得到与每个时间点对应的第一比较散列值;其中,所述第一密钥为所述验证服务端与安全服务器共享的密钥;  
所述验证服务端使用第二密钥,分别对每个所述第一比较散列值进行计算,得到与每个所述第一比较散列值对应的第二比较散列值;其中,所述第二密钥为所述验证服务端和客户端共享的密钥;  
所述验证服务端根据所述第二比较散列值,生成与所述至少两个时间点对应的至少两个比较OTP;  
如果所述至少两个比较OTP中包含所述待验证OTP,则所述验证服务端确定验证通过。
9. 根据权利要求8所述的方法,其特征在于,所述第一密钥的安全等级高于所述第二密钥的安全等级。

10. 根据权利要求8所述的方法, 其特征在于, 所述第二密钥以在所述客户端设置的密码作为密钥种子生成。

11. 根据权利要求8-10任一项所述的方法, 其特征在于,

当存在多个验证服务端时, 每个所述验证服务端分别与所述安全服务器共享一个第一密钥, 或者, 所述多个验证服务端与所述安全服务器共享同一个第一密钥。

12. 根据权利要求11所述的方法, 其特征在于, 当所述多个验证服务端与所述安全服务器共享同一个第一密钥时, 所述验证服务端使用第一密钥, 分别对每个时间点进行计算, 得到与每个时间点对应的第一比较散列值的步骤, 包括:

所述验证服务端使用随机盐值以及所述第一密钥, 分别对每个时间点进行计算, 得到与每个时间点对应的第一比较散列值; 其中, 所述随机盐值为所述验证服务端与所述安全服务器共享的数据。

13. 一种一次性密码OTP的生成方法, 其特征在于, 包括:

安全服务器接收客户端发起的验证请求;

所述安全服务器利用第一密钥对第一时间戳进行计算, 得到第一散列值; 其中, 第一密钥为所述安全服务器与验证服务端共享的密钥, 所述第一时间戳用于指示所述客户端发起所述验证请求的时间;

所述安全服务器将所述第一散列值发送给所述客户端, 以使所述客户端利用第二密钥对所述第一散列值进行计算, 得到第二散列值, 以及根据所述第二散列值生成待验证OTP; 其中, 所述第二密钥为所述客户端和所述验证服务端共享的密钥。

14. 根据权利要求13所述的方法, 其特征在于,

所述安全服务器包括加密机, 所述第一密钥存储于所述加密机中, 所述第一散列值在所述加密机中计算得到。

15. 根据权利要求13所述的方法, 其特征在于, 所述第一密钥的安全等级高于所述第二密钥的安全等级。

16. 根据权利要求13-15任一项所述的方法, 其特征在于,

当存在多个验证服务端时, 每个所述验证服务端分别与所述安全服务器共享一个第一密钥, 或者, 所述多个验证服务端与所述安全服务器共享同一个第一密钥。

17. 根据权利要求16所述的方法, 其特征在于, 当所述多个验证服务端与所述安全服务器共享同一个第一密钥时, 所述第一散列值由所述安全服务器使用随机盐值以及所述第一密钥对第一时间戳计算得到。

18. 一种客户端, 包括存储器、处理器以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1-7中任一项所述的方法。

19. 一种验证服务端, 包括存储器、处理器以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8-12中任一项所述的方法。

20. 一种芯片, 包括至少一个处理器和接口, 其特征在于, 所述接口用于接收代码指令, 并传输至所述至少一个处理器; 所述至少一个处理器运行所述代码指令, 实现如权利要求8-12中任一所述的方法。

21. 一种安全服务器,包括至少一个处理器,其特征在于,所述至少一个处理器运行代码指令,实现如权利要求13-17中任一所述的方法。

22. 一种计算机可读存储介质,其上存储有计算机程序或指令,其特征在于,当所述计算机程序或指令在电子设备上运行时,使所述电子设备执行权利要求1-17任一项所述的方法。

## OTP生成方法、验证方法、终端、服务器、芯片和介质

### 技术领域

[0001] 本申请涉及验证技术,更具体地,涉及一种一次性密码OTP的生成方法、验证方法、用户终端、服务器、芯片和存储介质。

### 背景技术

[0002] 一次性密码(One Time Password,简称OTP),指的是只能使用一次的密码。常规的OTP技术,涉及到两个交互端,一个是用户侧的客户端,另一个是非用户侧的服务器。客户端和服务器的具有一个共享的密钥。客户端执行生成待验证的OTP的过程,服务器执行验证待验证的OTP的过程。

[0003] 现有的OTP技术都是由服务器来完成验证的过程。然而,在某些应用场景中,验证过程需要由用户侧的另一个客户端来实现。将现有的OTP技术,直接挪用到这样的场景来使用,会影响到OTP的安全性。因为,共享的密钥放在客户端和另一个用户侧的客户端(以下称为验证端),而相对于服务器,客户端和验证端的安全性保障能力很低,存放在客户端或验证端的密钥如果泄露,则影响到验证的安全性。

### 发明内容

[0004] 针对现有技术中的问题,本申请提出一次性密码OTP的生成方法,包括:

[0005] 客户端向安全服务器发起验证请求;

[0006] 所述客户端从所述安全服务器接收第一散列值;其中,所述第一散列值由所述安全服务器使用第一密钥对第一时间戳计算得到,所述第一密钥为所述安全服务器与验证服务端共享的密钥,所述第一时间戳用于指示所述客户端发起所述验证请求的时间;

[0007] 所述客户端使用第二密钥对所述第一散列值进行计算,得到第二散列值;其中,所述第二密钥为所述客户端和所述验证服务端共享的密钥;

[0008] 所述客户端根据所述第二散列值生成待验证OTP。

[0009] 可选地,所述第一密钥的安全等级高于所述第二密钥的安全等级。

[0010] 可选地,所述第二密钥以在所述客户端设置的密码作为密钥种子而生成。

[0011] 可选地,所述第一时间戳由所述客户端获取,所述验证请求携带所述第一时间戳;或者,所述第一时间戳由所述安全服务器获取。

[0012] 可选地,当存在多个验证服务端时,每个所述验证服务端分别与所述安全服务器共享一个第一密钥,或者,所述多个验证服务端与所述安全服务器共享同一个第一密钥。

[0013] 可选地,当所述多个验证服务端与所述安全服务器共享同一个第一密钥时,所述第一散列值由所述安全服务器使用随机盐值以及所述第一密钥对第一时间戳计算得到。

[0014] 可选地,所述安全服务器包括加密机,所述第一密钥存储于所述加密机中,所述第一散列值在所述加密机中计算得到。

[0015] 另一方面,本申请还提出一种一次性密码OTP的验证方法,包括:

[0016] 验证服务端接收待验证OTP;

[0017] 所述验证服务端基于第二时间戳确定时间窗口；其中，所述第二时间戳用于指示所述验证服务端开始验证所述待验证OTP的时间，所述第二时间戳处于所述时间窗口内，并且，所述时间窗口包含至少两个时间点；

[0018] 所述验证服务端使用第一密钥，分别对所述每个时间点进行计算，得到与每个时间点对应的第一比较散列值；其中，所述第一密钥为所述验证服务端与安全服务器共享的密钥；

[0019] 所述验证服务端使用第二密钥，分别对每个所述第一比较散列值进行计算，得到与每个所述第一比较散列值对应的第二比较散列值；其中，所述第二密钥为所述验证服务端和客户端共享的密钥；

[0020] 所述验证服务端根据所述第二比较散列值，生成与所述至少两个时间点对应的至少两个比较OTP；

[0021] 如果所述至少两个比较OTP中包含所述待验证OTP，则所述验证服务端确定验证通过。

[0022] 可选地，所述第一密钥的安全等级高于所述第二密钥的安全等级。

[0023] 可选地，所述第二密钥以在所述客户端设置的密码作为密钥种子生成。

[0024] 可选地，当存在多个验证服务端时，每个所述验证服务端分别与所述安全服务器共享一个第一密钥，或者，所述多个验证服务端与所述安全服务器共享同一个第一密钥。

[0025] 可选地，当所述多个验证服务端与所述安全服务器共享同一个第一密钥时，所述验证服务端使用第一密钥，分别对所述每个时间点进行计算，得到与每个时间点对应的第一比较散列值的步骤，包括：

[0026] 所述验证服务端使用随机盐值以及所述第一密钥，分别对所述每个时间点进行计算，得到与每个时间点对应的第一比较散列值；其中，所述随机盐值为所述验证服务端与所述安全服务器共享的数据。

[0027] 在另一方面，本申请提出一种一次性密码OTP的生成方法，包括：

[0028] 安全服务器接收客户端发起的验证请求；

[0029] 所述安全服务器利用第一密钥对第一时间戳进行计算，得到第一散列值；其中，第一密钥为所述安全服务器与验证服务端共享的密钥，所述第一时间戳用于指示所述客户端发起所述验证请求的时间；

[0030] 所述安全服务器将所述第一散列值发送给所述客户端，以使所述客户端利用第二密钥对所述第一散列值进行计算，得到第二散列值，以及根据所述第二散列值生成待验证OTP；其中，所述第二密钥为所述客户端和所述验证服务端共享的密钥。

[0031] 可选地，所述安全服务器包括加密机，所述第一密钥存储于所述加密机中，所述第一散列值在所述加密机中计算得到。

[0032] 可选地，所述第一密钥的安全等级高于所述第二密钥的安全等级。

[0033] 可选地，当存在多个验证服务端时，每个所述验证服务端分别与所述安全服务器共享一个第一密钥，或者，所述多个验证服务端与所述安全服务器共享同一个第一密钥。

[0034] 可选地，当所述多个验证服务端与所述安全服务器共享同一个第一密钥时，所述第一散列值由所述安全服务器使用随机盐值以及所述第一密钥对第一时间戳计算得到。

[0035] 本申请还提出一种用户终端，包括存储器、处理器以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本申请任一实施例中所述的OTP的生成方法。

[0036] 本申请还提出一种用户终端,包括存储器、处理器以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本申请任一实施例中所述的OTP的验证方法。

[0037] 本申请还提出一种芯片,包括至少一个处理器和接口;所述接口用于接收代码指令,并传输至所述至少一个处理器;所述至少一个处理器运行所述代码指令,实现本申请任一实施例中所述的OTP的验证方法。

[0038] 本申请还提出一种安全服务器,包括至少一个处理器,所述至少一个处理器运行代码指令,实现本申请任一实施例中所述的OTP的生成方法。

[0039] 本申请还提出一种计算机可读存储介质,其上存储有计算机程序或指令,当所述计算机程序或指令在电子设备上运行时,使所述电子设备执行本申请任一实施例中所述的OTP的生成方法或验证方法。

[0040] 本申请的有益效果包括:提供一种安全的OTP生成方法和验证方法,在客户端和验证端都在用户侧的使用环境中,保障了OTP的生成和验证过程的安全性。

## 附图说明

[0041] 为了更容易理解本发明,将通过参照附图中示出的具体实施方式更详细地描述本发明。这些附图只描绘了本发明的典型实施方式,不应认为对本发明保护范围的限制。

[0042] 图1为本发明的方法的一个实施例的应用架构图。

[0043] 图2为本发明的OTP的生成方法一个实施方式的流程图。

[0044] 图3为本发明的OTP的验证方法一个实施方式的流程图。

[0045] 图4为本发明的OTP的生成方法一个实施方式的流程图。

[0046] 图5为本发明的方法另一个实施例的应用架构图。

## 具体实施方式

[0047] 下面参照附图描述本申请的实施方式,其中相同的部件用相同的附图标记表示。在不冲突的情况下,下述的实施例及实施例中的技术特征可以相互组合。

[0048] 第一实施方式

[0049] 图1显示了本申请的方法的一个实施例的应用架构图。本申请实施例的方法涉及三个设备:客户端、验证服务端(用户侧的终端)和安全服务器。图2为本申请的OTP的生成方法的示意性流程图,图3为本申请的OTP的验证方法的示意性流程图。下面参照图1-3来描述本申请实施例的方案,需要说明的是,本申请的方法不受图2-3中所示的步骤顺序的限制。

[0050] S101,客户端向安全服务器发起验证请求。

[0051] S102,安全服务器使用预先和验证服务端共享的第一密钥K1对第一时间戳计算散列值,得到第一散列值mac1,并返回给客户端。

[0052] 第一时间戳用于指示客户端发起验证请求的时间。第一时间戳能够指示出客户端发起验证请求的时间即可,其可以是客户端发起验证请求前后的某一个时间点,也可以是客户端发起验证请求那一刻的时间点,本申请对此不作限定。

[0053] 获取第一时间戳可以有多种不同的实现方式,第一时间戳可以是由客户端获取,也可以是由安全服务器获取。例如,客户端可以将接收到用户的触发指令(用于触发客户端发起验证请求)的时间点,确定为第一时间戳。又例如,客户端可以将接收到用户的触发指令的时间点至发送验证请求的时间点之间的某一个时间点,确定为第一时间戳。还例如,安全服务器可以将接收到客户端发送的验证请求的时间点,确定为第一时间戳。还例如,安全服务器可以将接收到客户端发送的验证请求的时间点至计算第一散列值的时间点之间的某一个时间点,确定为第一时间戳。

[0054] 可选地,当客户端或安全服务端生成所述第一时间戳时,可以采用如下方式:客户端或安全服务端获取当前时间,然后按照预设的步长取整,得到第一时间戳。例如,客户端在接收到用户的触发指令(用于触发客户端发起验证请求)之后,客户端取当前时间(09:04:05),然后对其按照一个预设的步长(例如30s)取整,得到第一时间戳(09:04:00)。

[0055] 所述第一散列值的计算有很多方法,例如MD5(Message Digest Algorithm)、SHA-1(Secure Hash Algorithm 1)、MAC(Message Authentication Codes)、HMAC(Hash-based Message Authentication Code)等。示例性地,在本实施例中,前述第一散列值可以是安全服务器采用MAC算法对第一时间戳进行计算得到的,记为mac1。

[0056] 可选地,上述的方法中安全服务器可以使用加密机来保护第一密钥K1的安全。可选地,第一散列值mac1的计算过程可以在加密机中完成。采用这样的实现方式,可以进一步提高一次性密码OTP的安全性。

[0057] S103,客户端使用和验证服务端共享的第二密钥K2,对安全服务器返回的第一散列值mac1值计算散列值,得到第二散列值mac2。

[0058] 可选地,第一密钥K1和第二密钥K2可以相同,也可以不同。如果二者不同,可以进一步提高OTP的安全性。

[0059] 可选地,第一密钥K1可以采用相对复杂的、安全等级相对较高的密钥(比如密钥包含的字符位数更长、包含的字符种类更多、更加没有规律性),第二密钥K2可以采用相对简单的、安全等级相对较低的密钥。示例性地,第二密钥可以以用户在客户端设置的密码作为密钥种子而生成。这样的密钥种子相对简单,更加便于用户记忆和使用。相应地,以其作为密钥种子生成的第二密钥也相对简单,具有一定的安全性,但安全等级相对较低。在本实施例中,将第一密钥K1和第二密钥K2设置为不同的安全等级,可以更好地兼顾安全性和用户使用时的便利性。

[0060] 可选地,所述第二散列值的计算方法也有很多方法,例如MD5、SHA-1、MAC、HMAC等。示例性地,在本实施例中,前述第二散列值可以是安全服务器采用MAC算法对第一散列值进行计算得到的,记为mac2。

[0061] 需要说明的是,计算第一散列值和计算第二散列值采用的算法可以相同,也可以不同,本申请对此不作限定。

[0062] S104,客户端从第二散列值mac2中计算出本次的待验证OTP。

[0063] 其中,使用第二散列值mac2中计算本次OTP所采用的算法可以根据需要来选择。例如,在一种实现方式中,客户端可以使用第二散列值mac2的最前面三个字节和最后面三个字节拼成字符串,再进行base64编码,从而得到待验证OTP。又例如,在另一种实现方式中,客户端可以取第二散列值mac2中间几个字节,再进行base64编码,从而得到待验证OTP。



[0064] 可选地,如果作为登录密码,待验证OTP的字符长度可以设置在一个合适的长度阈值范围内。例如,上述合适的长度阈值范围可以为6-8个字符,也可以采用其他长度。可选地,待验证OTP中每一个字符均为可打印字符,即,上述待验证OTP为可打印的字符串。采用上述实现方式,待验证OTP就可以通过显示设备显示给用户,用户查看到该待验证OTP之后,也可以较方便地手动将其输入到验证服务端中。即,采用上述实现方式可以便于用户查看和输入待验证OTP。

[0065] 可选地,客户端也可以不采用算法,直接将第二散列值作为待验证OTP。这可以视为客户端根据第二散列值生成待验证OTP的一种特殊情况。

[0066] 需要说明的是,本申请对于待验证OTP的长度,以及是否能够打印,均不作限定。在不同的应用场景中,可以采用不同的实现方式。例如,当客户端将待验证OTP直接发送给验证服务端,无需显示给用户或者让用户手动输入时,即便待验证OTP的长度很长或者不能打印,也不影响本申请实施例中方法的正常执行。

[0067] 如图3所示,验证服务端收到待验证OTP后,开始对该OTP进行验证。

[0068] S201,验证服务端接收待验证OTP。

[0069] 可选地,验证服务端可以从客户端接收待验证OTP,也可以由用户直接输入(见第二实施方式中门锁的实施例)至验证服务端。所述用户可以是使用客户端的用户,也可以是使用验证服务端的用户。即,在实际的应用场景中,使用客户端的用户和使用验证服务端的用户,可以是同一个用户,也可以是不同的用户,本申请对此不作限定。

[0070] S202,验证服务端基于第二时间戳确定时间窗口。其中,所述第二时间戳用于指示所述验证服务端开始验证所述待验证OTP的时间,所述第二时间戳处于所述时间窗口内,并且所述时间窗口包含至少两个时间点。

[0071] 上述第二时间戳可以采用验证服务端接收到待验证OTP时,验证服务端当前的时间点,也可以采用这前后的某一个时间点,只要能够指示出验证服务端开始验证待验证OTP的时间即可,本申请对其具体的取值方式不作限定。

[0072] 第二时间戳与第一时间戳类似,其指示出验证服务端开始验证待验证OTP的时间,可以采用验证服务端收到待验证OTP时验证服务端当前的时间点,也可以采用该时间点前后的其他能够指示出前述信息的时间点。

[0073] 在一种实现方式中,验证服务端可以基于第二时间戳来确定时间窗口,使得时间窗口包含第二时间戳,即以第二时间戳为一个时间点。并且,除了第二时间戳以外,时间窗口还包含至少一个其他的时间点。

[0074] 可选地,在一个示例中,验证服务端取当前时间(09:05:38),然后对其按照一个预设的步长(例如30s)取整,得到第二时间戳(09:05:30)。

[0075] 可选地,时间窗口的长度可以根据需要设置,本申请对于其具体取值不作限定。例如,时间窗口的长度设置为5min,将第二时间戳(09:05:30)向前推3min,向后推2min,得到上述第二时间戳对应的时间窗口为(09:02:30-09:07:30)。

[0076] 在一种实现方式中,第二时间窗口中包含的时间点,可以根据预设步长对第二时间窗做划分而得到。例如,沿用前述的时间窗口(09:02:30-09:07:30)的例子,在这个时间段中,假设预设步长为30s,以每30s为一个时间点,可以确定出11个时间点:09:02:30,09:03:00,09:03:30,09:04:00,09:04:30,09:05:00,09:05:30,09:06:00,09:06:30,09:07:

00,09:07:30。

[0077] 需要说明的是,一般地,在划分时间点时,采用的预设步长与前面步骤S102中确定第一时间戳时取整所采用的步长,以及前述确定第二时间戳时取整所采用的步长,三者保持一致。

[0078] 以上取时间戳、确定时间窗口以及划分时间点的方法,可以根据需要进行不同的变化。

[0079] S203,验证服务端用第一密钥K1,分别对所述每个时间点进行计算,得到与每个时间点对应的第一比较散列值 $mac1'$ 。

[0080] 其中,验证服务端计算第一比较散列值 $mac1'$ 的算法,和安全服务器计算第一散列值 $mac1$ 的算法一致,例如可以为MD5、SHA-1、MAC、HMAC。

[0081] S204,验证服务端用第二密钥K2分别对每个所述第一比较散列值 $mac1'$ 进行计算,得到与每个所述第一比较散列值 $mac1'$ 对应的第二比较散列值 $mac2'$ 。

[0082] 其中,验证服务端计算第二比较散列值 $mac2'$ 的算法,和客户端计算第二散列值 $mac2$ 的方法一致,例如可以为MD5、SHA-1、MAC、HMAC。

[0083] S205,验证服务端根据所述第二比较散列值 $mac2'$ ,生成与所述至少两个时间点对应的至少两个比较OTP。

[0084] 示例性地,沿用前述的从时间窗口中确定出11个时间点的例子,验证服务端通过执行S203的步骤,可以分别得到11个对应的第一比较散列值 $mac1'$ (1), $mac1'$ (2)…… $mac1'$ (10), $mac1'$ (11)。然后执行S204的步骤,可以分别得到11个对应的第一比较散列值 $mac2'$ (1), $mac2'$ (2),…… $mac2'$ (10), $mac2'$ (11)。再执行S206的步骤,可以分别得到11个对应的比较OTP:比较OTP(1),比较OTP(2)……比较OTP(10),比较OTP(11)。通过以上步骤,验证服务端针对第二时间戳对应的时间窗口内的每个时间点(至少两个),计算得到对应的至少两个比较OTP。

[0085] 需要说明的是,验证服务端生成比较OTP时所采用的方法,与前述步骤中客户端生成待验证OTP时所采用的方法,应保持一致。

[0086] S206,如果所述至少两个比较OTP中包含所述待验证OTP,则所述验证服务端确定验证通过。

[0087] 也就是说,比对计算得到的多个比较OTP以及待验证OTP,如果其中有任何一个比较OTP与待验证OTP相匹配,则验证服务端可以确认验证通过。

[0088] 示例性地,沿用前述11个比较OTP的例子,验证服务端将接收到的待验证OTP,分别与比较OTP(1),比较OTP(2)……比较OTP(10),比较OTP(11)进行比对。一旦发现其中某一个比较OTP与待验证OTP相匹配,例如,OTP(4)与待验证OTP二者相同,则验证服务端判断验证通过。

[0089] 另外,本申请实施例的方法还可以适用于多个验证服务端的应用场景。

[0090] 在一种实现方式中,当有多个验证服务端时,安全服务器可以和每个验证服务分别共享一个第一密钥K1。如此,多个验证服务端之间相互独立,彼此不影响,安全性更高。

[0091] 在另一种实现方式中,安全服务器也可以和这多个验证服务端使用共同的第一密钥K1。相比于各自对应一个第一密钥,采用共用第一密钥的方案覆盖性更好,使同一个客户端生成的OTP能够通过多个验证服务端的验证。例如,在一种应用场景中,安全服务器与

多个验证服务端共享同一个第一密钥,客户端可以绑定这多个验证服务端。通过安全服务器和客户端生成一次待验证OTP,该待验证OTP可以被发送给多个验证服务端,从而同时或者在一个比较短的时间段内,通过多个验证服务端的验证,进而实现联动开锁。

[0092] 优选地,当安全服务器与多个验证服务端使用共同的第一密钥K1时,安全服务器可以在计算第一散列值mac1时加入一个随机盐值(salt),用于增强安全性。

[0093] 例如,在一种实现方式中,安全服务器在对第一时间戳计算得到mac1之前,先生成一个随机的盐值。该盐值存储在安全服务器中。在计算第一散列值mac1时,安全服务器先将第一时间戳与盐值拼接在一起,然后计算拼接结果的散列值,得到第一散列值mac1。安全服务器将该盐值也传递给验证服务端,以便验证服务端在计算mac1'之前,采用相同的盐值来加盐。

[0094] 可选地,安全服务器将盐值传递给验证服务端,可以在安全服务器与验证服务端配置共享的第一密钥K1的时候同步进行。示例性地,在配置时,安全服务器可以将盐值和第一密钥K1携带在同一个消息中,发送给验证服务器。

[0095] 将常规的OTP生成和验证的方法直接挪用到客户端和验证端都在用户侧的应用场景中,会影响到OTP的安全性。具体来说,客户端和验证端之间具有一个共享的密钥,客户端采用该密钥来生成待验证OTP,验证端采用该密钥来验证待验证OTP。一旦该密钥泄露,则将无法保障OTP的安全使用。

[0096] 本申请实施例的方案中,除了客户端与验证服务端之间共享的密钥(即第二密钥)之外,还引入了安全服务器,使安全服务器和验证服务端之间共享的一个密钥(即第一密钥)。基于此,在本申请提供的OTP生成方法中,在生成待验证OTP时,不再仅由客户端使用一个密钥来生成待验证OTP,而是先由安全服务器使用第一密钥来生成第一散列值,然后由客户端使用第二密钥对第一散列值进行计算,得到第二散列值,再基于第二散列值来生成待验证OTP。与之相对应地,验证待验证OTP的过程,则由验证服务端利用第一密钥和第二密钥来验证待验证OTP。通过这样的方式,即便存储在客户端或验证服务端的第二密钥发生泄露,由于待验证OTP的生成和验证都还涉及到第一密钥,因此可以继续保障使用OTP的安全性。即便客户端被攻击导致存储在客户端的密钥都泄露了,由于第一密钥存储在安全性保障能力更高的安全服务器上,并不存储在客户端上,计算第一散列值的过程也在安全服务器上执行,因此采用本申请提供的方法也可以继续保障OTP的使用安全性。

[0097] 此外,常规的OTP生成和验证的方法还存在便利性较差的问题。为了保障OTP的使用安全,客户端和验证端之间共享的密钥往往需要采用安全等级较高的密钥。如果要变更这样的密钥,需要通过厂商才能实现。例如,在智能门锁的应用场景中,生成OTP的客户端为用户的手机,验证OTP的验证端为用户家里的智能门锁。智能门锁与手机共享的密钥是在安装智能门锁时,由厂商为用户配置的安全等级较高的密钥。一旦后续用户的手机丢失了,用户就需要找厂商为智能门锁和用户的新手机重新配置共享的密钥,这降低了用户使用的便利性。

[0098] 在本申请提供的OTP生成方法和验证方法中,第一密钥为安全服务器与验证服务端共享的密钥,这个密钥可以由厂家为用户来配置;第二密钥为客户端和验证服务端共享的密钥,由于客户端和验证服务端都在用户侧,第二密钥可以由用户自己来进行变更,不需要厂家的参与。例如,在前述智能门锁的应用场景中,即使用户的手机丢失了,由于仅涉及

第二密钥,不涉及第一密钥,故而用户可以将新的手机与智能门锁绑定之后,自己变更第一密钥,从而提高了用户使用的便利性。即便用户的手机并没有丢失,用户也可以常常自己变更第一密钥,避免长时间使用同一个第一密钥,影响使用OTP的安全性。

[0099] 因此,本申请实施例提供的OTP生成方法和验证方法,在客户端和验证端都在用户侧的使用环境中,能够较好地保障OTP的使用安全性的同时,也提高了用户的便利性。

[0100] 下面参照图4描述安全服务器完成的一次性密码OTP的生成方法,包括:

[0101] S301,安全服务器接收客户端发起的验证请求。

[0102] S302,所述安全服务器利用第一密钥对第一时间戳进行计算,得到第一散列值;其中,第一密钥为所述安全服务器与验证服务端共享的密钥,所述第一时间戳用于指示所述客户端发起所述验证请求的时间。

[0103] S303,所述安全服务器将所述第一散列值发送给所述客户端。

[0104] 客户端在接收到第一散列值之后,可以利用第二密钥对所述第一散列值进行计算,得到第二散列值;再根据所述第二散列值生成待验证OTP。其中,所述第二密钥为所述客户端和所述验证服务端共享的密钥。

[0105] 在一个实施例中,所述安全服务器包括加密机,所述第一密钥存储于所述加密机中,所述第一散列值在所述加密机中计算得到。

[0106] 在一个实施例中,所述第一密钥的安全等级高于所述第二密钥的安全等级。

[0107] 在一个实施例中,可以存在多个验证服务端时,此时,每个所述验证服务端分别与所述安全服务器共享一个第一密钥,或者,所述多个验证服务端与所述安全服务器共享同一个第一密钥。

[0108] 在一个实施例中,当所述多个验证服务端与所述安全服务器共享同一个第一密钥时,所述第一散列值由所述安全服务器使用随机盐值以及所述第一密钥对第一时间戳计算得到。

[0109] 安全服务器完成的其他操作见如上参照图1-3描述的说明书。

[0110] 第二实施方式

[0111] 如图5所示,在一个实施例中,本申请的方法应用于门锁的OTP(一次性密码, One Time Password)开锁。手机APP为客户端,门锁为验证服务端,门锁的应用服务端为安全服务器。

[0112] 在门锁生产时在门锁的应用服务端(安全服务器)和每个门锁(验证服务端)之间共享一个随机的密钥作为第一密钥K1。在门锁安装时使用用户设置的管理员密码做密钥种子生成第二密钥K2。

[0113] 安全服务器和验证服务端之间的密钥(第一密钥K1)采用复杂的、安全等级比较高的密钥;验证服务端和客户端之间共享的密钥(第二密钥K2)则采用相对简单的、安全等级相对较低的密钥,例如以用户在客户端中设置的密码作为密钥种子生成的密钥。这样就可以兼顾安全性和使用便利性。第一密钥K1和第二密钥K2互相不受影响。

[0114] 当用户在手机APP上输入管理员密码生成OTP(开锁密码)时,手机APP向安全服务器发起请求。安全服务器找到对应门锁,并根据当前时间取整30秒(以30秒为一个时间点),得到第一时间戳。安全服务器通过后台的加密机使用第一密钥K1计算出第一密值mac1并返回给手机APP。手机APP使用第二密钥K2计算出第二密值mac2。可选地,手机APP使用第二密

值mac2的最前面三个字节和最后面三个字节拼成字符串,并做base64编码,得到一个6位的字符串,将其作为待验证OTP。

[0115] 门锁接收用户输入的待验证OTP后,根据门锁的当前时间,取整30秒,得到第二时间戳。门锁计算在第二时间窗对应的时间窗口内的每个时间点所对应的比较OTP,计算方法同前述第一密值、第二密值的计算方法。门锁比对用户输入的待验证OTP和多个比较OTP。如果有任何一个比较OTP和用户输入的待验证OTP比对成功,则认为用户输入合法,可以开锁。否则失败,不能开锁。

[0116] 可选地,门锁接收的待验证OTP也可以由客户端直接发送给验证服务端。比如,远程的屋主可以将在手机端生成的待验证OTP通过无线通讯的方式发送给门锁,然后门锁直接验证完成,为保洁人员开门(无需告知保洁人员生成的待验证OTP,也无需保洁人员输入)。在这种情况下,计算出来的待验证OTP,即便长度很长或者不能打印,也不影响本申请实施例中方法的正常执行。

[0117] 第三实施方式

[0118] 本申请实施例提出一种用户终端,包括存储器、处理器以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本申请任一实施例中所述的OTP的生成方法。该用户终端具体可以是手机、平板电脑、个人数字助理(personal digital assistant,PDA)、可穿戴设备等。

[0119] 可选地,该用户终端包括发送器,发送器通过有线或无线方式向安全服务器发起验证请求,处理器执行其他步骤(例如S102-S104的步骤)。

[0120] 本申请实施例还提出一种用户终端,包括存储器、处理器以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本申请任一实施例中所述的OTP的验证方法。该用户终端可以是门锁等智能家居或者安防领域的产品。

[0121] 可选地,该用户终端包括接收器,接收器可以通过有线或无线方式接收客户端发送的待验证OTP,处理器执行其他步骤(例如S202-S206的步骤)。

[0122] 本申请实施例还提出一种芯片,其特征在于,包括至少一个处理器和接口;所述接口用于接收代码指令,并传输至所述至少一个处理器;所述至少一个处理器运行所述代码指令,实现本申请任一实施例中所述的OTP的验证方法。

[0123] 本申请实施例还提出一种安全服务器,包括至少一个处理器,所述至少一个处理器运行代码指令,实现本申请任一实施例中所述的OTP的生成方法。

[0124] 本申请还提出一种计算机可读存储介质,其上存储有计算机程序或指令,当所述计算机程序或指令在电子设备上运行时,使所述电子设备执行本申请任一实施例中所述的OTP的生成方法或验证方法。

[0125] 应理解,本申请实施例可提供方法、产品或计算机程序产品。因此,本申请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,本申请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上实施的计算机程序产品的形式。

[0126] 上述处理器可以是中央处理单元(Central Processing Unit,CPU),还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-

Programmable Gate Array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0127] 上述存储器可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。存储器是计算机可读介质的示例。

[0128] 上述计算机可读介质包括永久性和非永久性、可移动和非可移动存储介质。存储介质可以由任何方法或技术来实现信息存储,信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。

[0129] 以上所述的实施例,只是本申请较优选的具体实施方式,本领域的技术人员在本申请技术方案范围内进行的通常变化和替换都应包含在本申请的保护范围内。

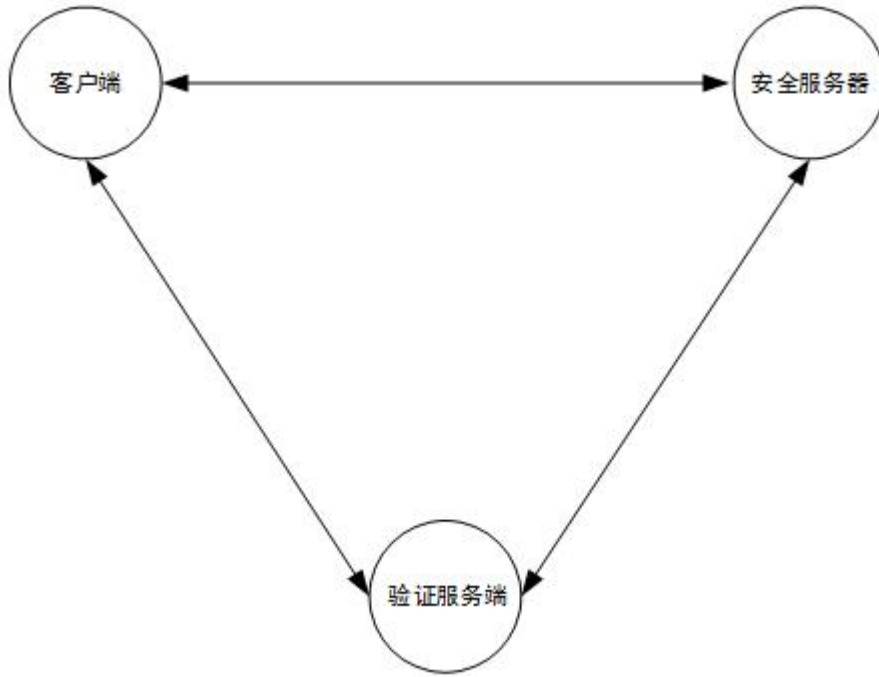


图1

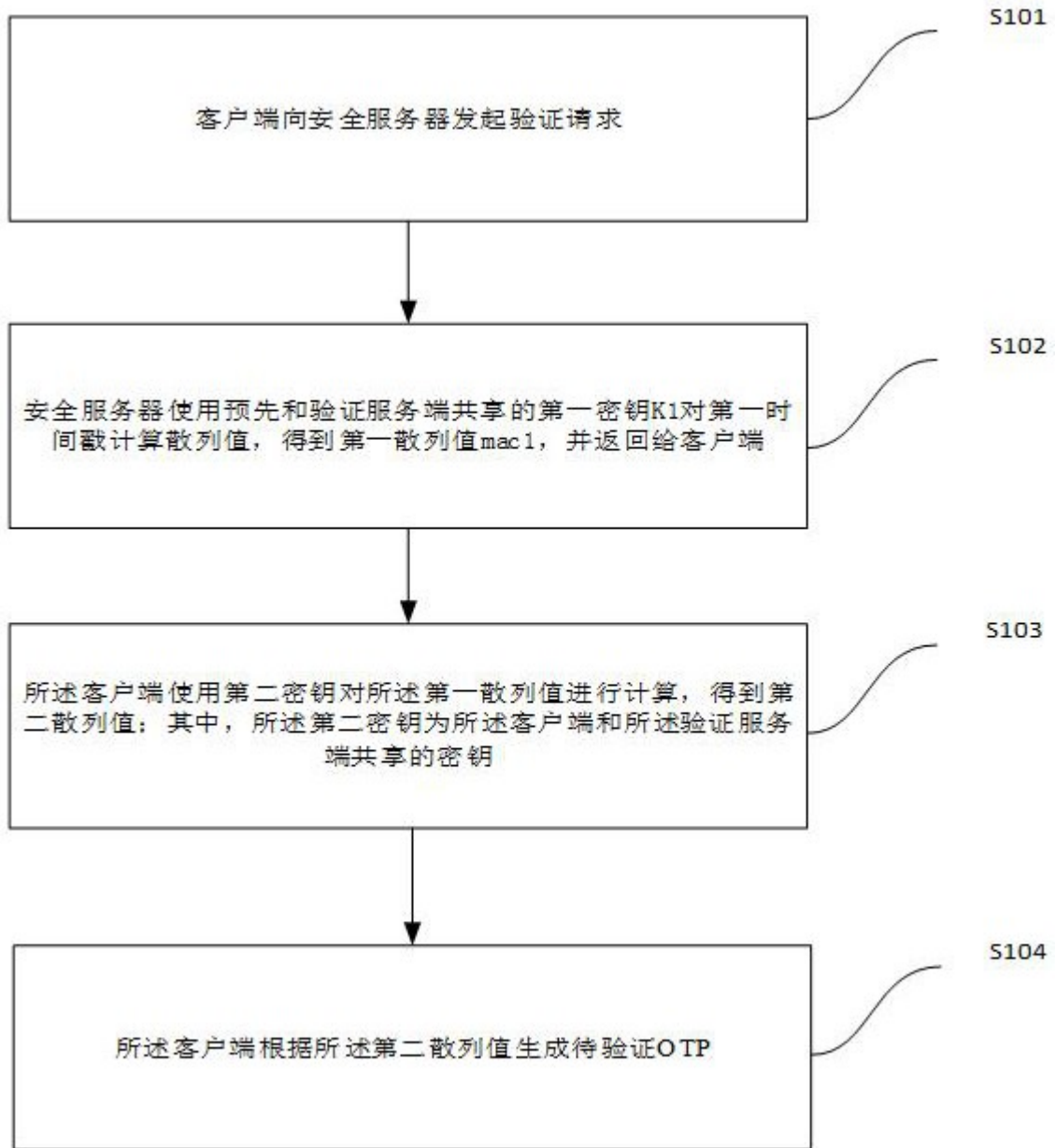


图2



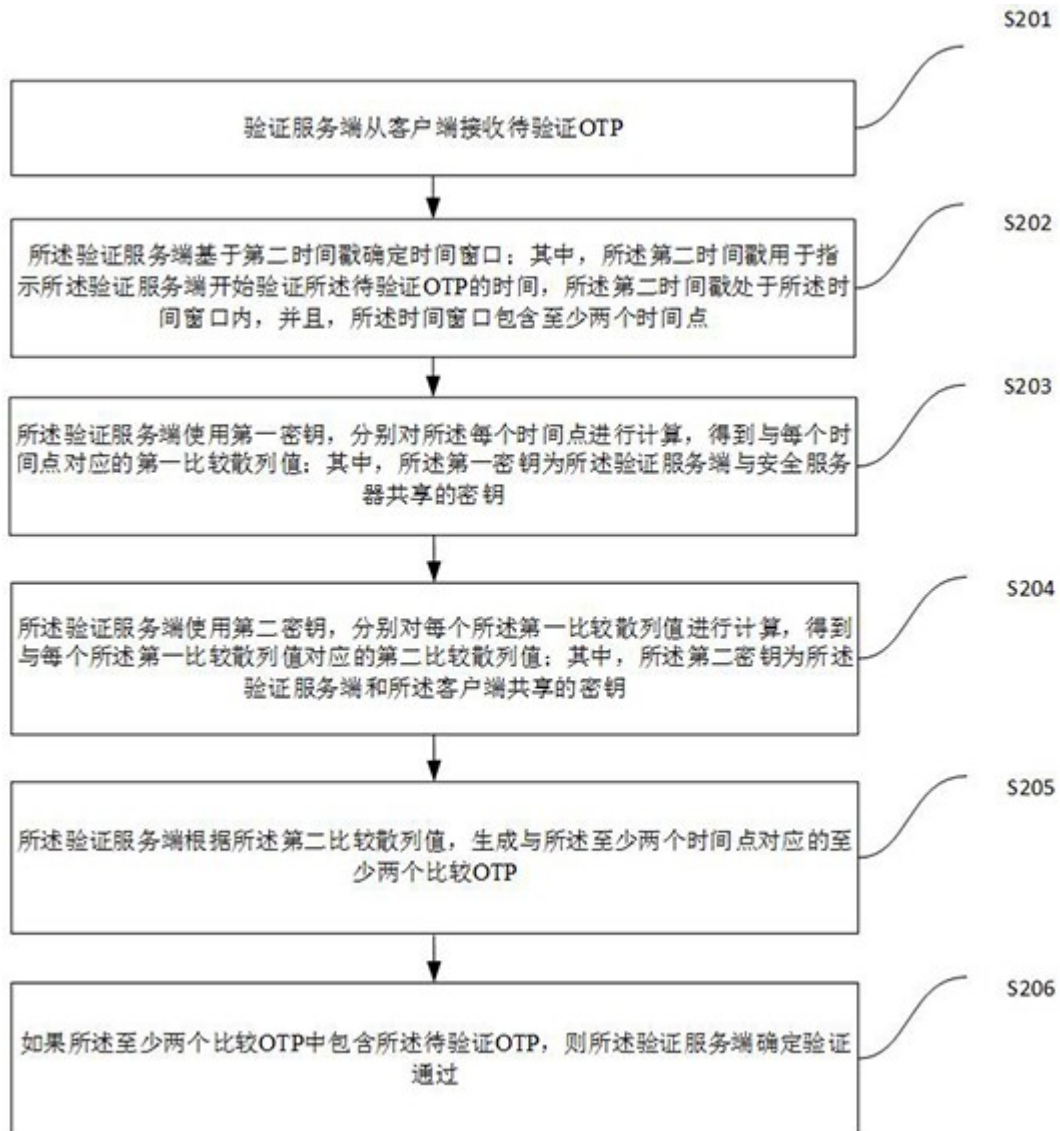


图3

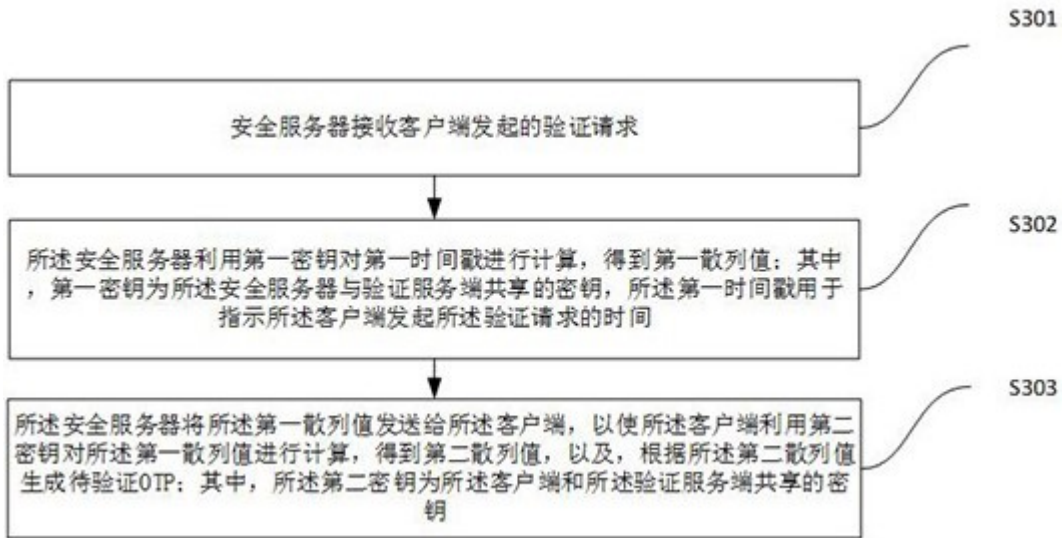


图4

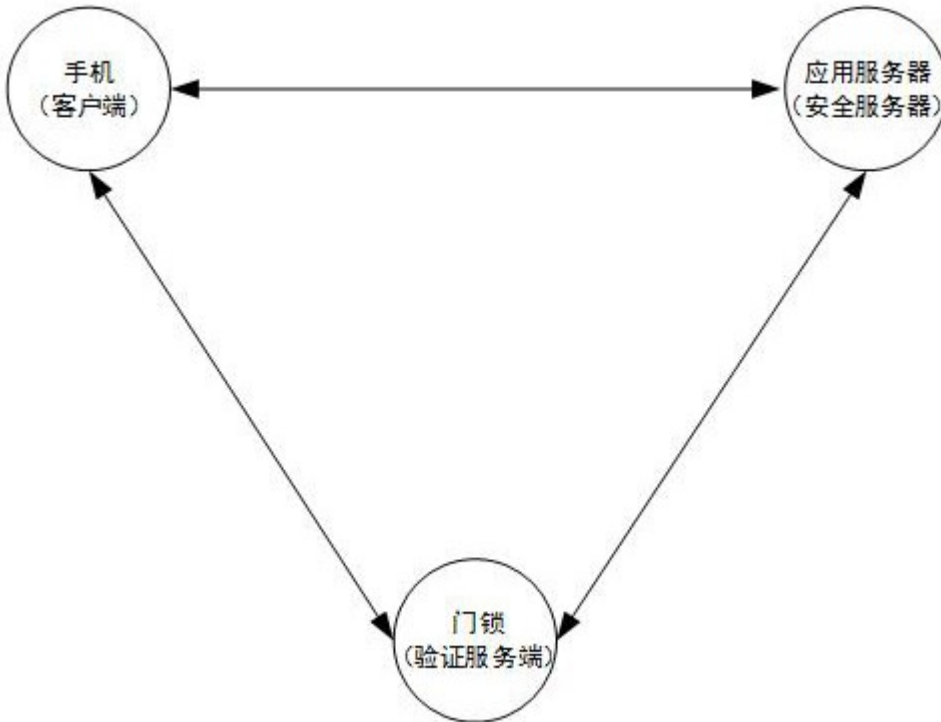


图5