



(12)发明专利

(10)授权公告号 CN 109714167 B

(45)授权公告日 2020.08.25

(21)申请号 201910197222.X

(22)申请日 2019.03.15

(65)同一申请的已公布的文献号
申请公布号 CN 109714167 A

(43)申请公布日 2019.05.03

(73)专利权人 北京邮电大学
地址 100876 北京市海淀区西土城路10号

(72)发明人 徐国爱 王菲菲 郭燕慧

(74)专利代理机构 北京同立钧成知识产权代理
有限公司 11205

代理人 张子青 刘芳

(51)Int.Cl.

H04L 9/08(2006.01)

(续)

(56)对比文件

CN 109412790 A,2019.03.01

CN 109088888 A,2018.12.25

CN 107483195 A,2017.12.15

US 10158636 B2,2018.12.18

US 2019074982 A1,2019.03.07

Tanmoy Maitra et al.《Security

analysis and design of an efficient ECC-based two-factor password authentication scheme》.《SECURITY AND COMMUNICATION NETWORKS》.2016,第9卷(第17期),

Tanmoy Maitra et al.《Security analysis and design of an efficient ECC-based two-factor password authentication scheme》.《SECURITY AND COMMUNICATION NETWORKS》.2016,第9卷(第17期),

Yanrong Lu et al.《Robust anonymous two-factor authenticated key exchange scheme for mobile client-server environment》.《SECURITY AND COMMUNICATION NETWORKS》.2016,第9卷(第11期),

(续)

审查员 陈燕

权利要求书3页 说明书17页 附图8页

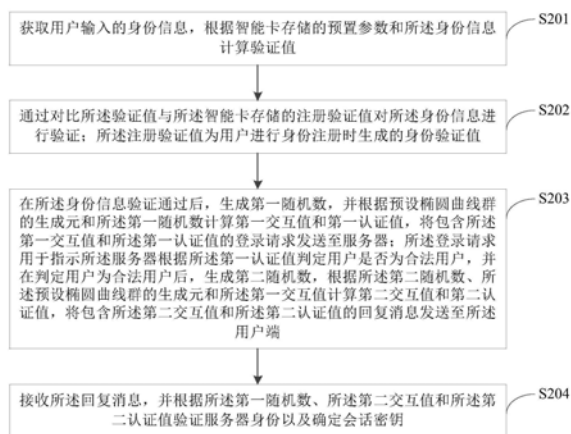
(54)发明名称

适用于移动应用签名的身份认证与密钥协商方法及设备

(57)摘要

本发明实施例提供一种适用于移动应用签名的身份认证与密钥协商方法及设备,该方法包括获取用户输入的身份信息,根据智能卡存储的预置参数和所述身份信息计算验证值;通过对比所述验证值与所述智能卡存储的注册验证值对所述身份信息进行验证;在所述身份信息验证通过后,生成第一随机数,并根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值,将包含所述第一交互值和所述第一认证值的登录请求发送至服务器;接收回复消息,并根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话

密钥。本发明实施例能够提高移动应用签名身份认证与密钥协商的安全性。



CN 109714167 B

[接上页]

(51) Int.Cl.

H04L 9/30(2006.01)

H04L 9/32(2006.01)

(56) 对比文件

SK Hafizul Islam et al..《DYNAMIC ID-BASED REMOTE USER MUTUAL AUTHENTICATION SCHEME WITH SMARTCARD USING ELLIPTIC

CURVE CRYPTOGRAPHY》.《JOURNAL OF ELECTRONICS (CHINA)》.2014,第31卷(第5期),

Min Luo et al..《A secure and efficient identity-based mutual authentication scheme with smart card using elliptic curve cryptography》.《International Journal of COMMUNICATION SYSTEMS》.2017,第30卷(第16期),

1. 一种适用于移动应用签名的身份认证与密钥协商方法,其特征在于,应用于用户端,包括:

获取用户输入的身份信息,根据智能卡存储的预置参数和所述身份信息计算验证值;

通过对比所述验证值与所述智能卡存储的注册验证值对所述 ([信息进行验证;所述注册验证值为 ([信息进行身份注册时生成的身份验证值;

在所述身份信息验证通过后,生成第一随机数,并根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值,将包含所述第一交互值和所述第一认证值的登录请求发送至服务器;所述登录请求用于指示所述服务器根据所述第一认证值判定用户是否为合法用户,并在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值,将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端;

接收所述回复消息,并根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥;

其中,所述预置参数包括预置随机数和预置整数,所述身份信息包括身份标识及身份密码;

所述根据智能卡存储的预置参数和所述身份信息计算验证值,包括:

根据所述预置参数、所述身份信息和第一公式计算所述验证值;所述第一公式为:

$$V_i^* = h(ID_i^* \parallel PW_i^* \parallel N_i) \bmod n$$

其中, V_i^* 为所述验证值, $h()$ 为哈希函数, ID_i^* 为所述身份标识, PW_i^* 为所述身份密码, N_i 为所述预置随机数, n 为所述预置整数。

2. 根据权利要求1所述的方法,其特征在于,所述预置参数包括服务器预置参数和用户端预置参数,在所述获取用户输入的身份信息之前,还包括:

获取用户输入的待注册身份信息;所述待注册身份信息包括待注册身份标识及待注册身份密码;

生成第三随机数,并根据所述待注册身份信息和所述第三随机数计算哈希值,将包含所述待注册身份标识和所述哈希值的注册请求发送至服务器;所述注册请求用于指示所述服务器根据私钥、所述待注册身份标识和所述哈希值确定服务器预置参数,将所述服务器预置参数存储到所述智能卡;

根据所述哈希值和所述服务器预置参数计算所述注册验证值,将所述第三随机数和所述注册验证值作为所述用户端预置参数存储到所述智能卡。

3. 根据权利要求1所述的方法,其特征在于,所述预置参数包括预置公钥和第一预置值;

所述根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值,将包含所述第一交互值和所述第一认证值的登录请求发送至服务器,包括:

根据所述预设椭圆曲线群的生成元、第一随机数及第二公式计算所述第一交互值;所述第二公式为:

$$R_i = N_i P$$

其中, R_i 为所述第一交互值, N_i 为所述第一随机数, P 为所述预设椭圆曲线群的生成元;

根据所述第一交互值和第三公式计算所述第一认证值;所述第三公式为:

$$D_i = h(A_i^* \parallel R_i)$$

其中, D_i 为所述第一认证值, $A_i^* = B_i \oplus F_i^*$, B_i 为所述第一预置值, $F_i^* = h(ID_i^* \parallel PW_i^* \parallel N_i)$;

根据所述第一随机数和第四公式计算加密密钥;所述第四公式为:

$$C_i = h(N_i P_{\text{PUB}})$$

其中, C_i 为所述加密密钥, P_{PUB} 为所述预置公钥;

根据所述加密密钥和高级加密标准算法对所述身份标识和所述第一认证值加密得到密文;

生成时间戳,将包含所述密文、所述时间戳和所述第一交互值的登录请求发送至所述服务器。

4. 根据权利要求3所述的方法,其特征在于,所述根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥,包括:

根据所述第一随机数、所述第二交互值和第五公式计算会话密钥;所述第五公式为:

$$SK = h(K'_i \parallel A_i^*)$$

其中, SK 为所述会话密钥, $K'_i = N_i * Z_i$, Z_i 为所述第二交互值;

根据第六公式计算所述第二认证值对应的验证值;所述第六公式为:

$$X'_i = h(Z_i \parallel A_i^* \parallel C_i \parallel SK)$$

其中, X'_i 为所述第二认证值对应的验证值;

若所述第二认证值对应的验证值与所述第二认证值相等,则判定服务器合法,并将所述会话密钥作为所述用户端与所述服务器之间的会话密钥。

5. 根据权利要求3所述的方法,其特征在于,还包括:

在所述身份信息验证通过后,获取用户输入的新身份密码;

根据所述新身份密码和第七公式计算新注册认证值;所述第七公式为:

$$V_i^{\text{new}} = h(ID_i^* \parallel PW_i^{\text{new}} \parallel N_i) \bmod n$$

其中, V_i^{new} 为所述新注册认证值, PW_i^{new} 为新身份密码;

根据第八公式计算新第一预置值;所述第八公式为:

$$B_i^{\text{new}} = B_i \oplus h(ID_i^* \parallel PW_i^* \parallel N_i) \oplus h(ID_i^* \parallel PW_i^{\text{new}} \parallel N_i)$$

其中, B_i^{new} 为所述新第一预置值;

将所述存储卡中存储的注册认证值替换为所述新注册认证值,将所述存储卡中存储的所述第一预置值替换为所述新第一预置值。

6. 一种适用于移动应用签名的身份认证与密钥协商方法,应用于服务器,其特征在于,包括:

接收用户端发送的包含第一交互值和第一认证值的登录请求;所述第一交互值和所述第一认证值为所述用户端根据预设椭圆曲线群的生成元和第一随机数计算得到;

根据所述第一认证值判定用户是否为合法用户；

在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值；

将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端；所述回复消息用于指示所述用户端根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥；

其中,所述登录请求包括对第一认证值和身份标识加密得到的密文、所述第一交互值以及时间戳；

所述根据所述第一认证值判定用户是否为合法用户包括：

判定所述时间戳是否有效；

若所述时间戳有效,则根据私钥、所述第一交互值和第九公式计算解密密钥；所述第九公式为：

$$C'_i = h(xR_i)$$

其中, C'_i 为所述解密密钥, $h()$ 为哈希函数, x 为所述私钥, R_i 为所述第一交互值；

根据所述解密密钥和高级加密标准算法对所述密文进行解密得到解密出的第一认证值和解密出的身份标识；

根据第十公式计算所述第一认证值对应的验证值；所述第十公式为：

$$D''_i = h(A'_i || R_i)$$

其中, D''_i 为所述第一认证值对应的验证值, $A'_i = h(x || ID'_i)$, ID'_i 为所述解密出的身份标识；

若所述第一认证值对应的验证值与所述第一认证值相等,则判定用户为合法用户。

7. 一种适用于移动应用签名的身份认证与密钥协商设备,其特征在于,包括:至少一个处理器和存储器；

所述存储器存储计算机执行指令；

所述至少一个处理器执行所述存储器存储的计算机执行指令,使得所述至少一个处理器执行如权利要求1至5任一项所述的身份认证与密钥协商方法。

8. 一种适用于移动应用签名的身份认证与密钥协商设备,其特征在于,包括:至少一个处理器和存储器；

所述存储器存储计算机执行指令；

所述至少一个处理器执行所述存储器存储的计算机执行指令,使得所述至少一个处理器执行如权利要求6所述的身份认证与密钥协商方法。

9. 一种计算机可读存储介质,其特征在于,所述计算机可读存储介质中存储有计算机执行指令,当处理器执行所述计算机执行指令时,实现如权利要求1至5任一项所述的适用于移动应用签名的身份认证与密钥协商方法。

10. 一种计算机可读存储介质,其特征在于,所述计算机可读存储介质中存储有计算机执行指令,当处理器执行所述计算机执行指令时,实现如权利要求6所述的适用于移动应用签名的身份认证与密钥协商方法。

适用于移动应用签名的身份认证与密钥协商方法及设备

技术领域

[0001] 本发明实施例涉及网络安全技术领域,尤其涉及一种适用于移动应用签名的身份认证与密钥协商方法及设备。

背景技术

[0002] 身份认证与密钥协商目的是在复杂的、非安全的网络环境中实现通信参与各方的身份认证与通信安全。身份认证包括服务器对用户的身份的确认以及用户对服务器合法性的确认,根据双方共享的认证信息判断通信方身份的真实性。而密钥协商在开放的网络通信环境中,允许多个参与成员在由攻击者完全控制通信信道的情况下通过信息交换,联合生成一个共享的会话密钥,用于加密用户和服务器的通信消息。

[0003] 随着移动应用的快速发展,针对移动应用的各种攻击事件也层出不穷,攻击者可能通过对原始应用进行篡改、植入病毒或恶意程序,从而达到插入恶意广告或非法收集用户信息的目的。尤其是针对一些与用户财产密切相关的敏感软件,例如银行手机客户端软件、理财APP,如果攻击者通过仿冒原始软件,进而捕获用户的用户名与密码,从而非法使用或转移用户财产,这将给用户带来非常大的损失,因此亟需对移动应用进行安全认证。应用商店作为移动应用下载服务的提供者目前已成为移动应用的主要获取渠道。由应用商店对所提供移动应用进行安全认证是切实可行的,并将大大提高用户使用该应用商店的信心。应用商店首先对各个应用的安全性检测,对通过安全检测的应用通过数字签名的方式认证该应用的安全性,用户通过验证签名的合法性,确认该应用的安全性。在这一过程中,不仅涉及用户与应用商店之间的身份认证,同时为保证签名结果、签名者的公钥等信息通过公有网络安全传输,还需为签名及应用商店公钥证书的安全传递协商会话密钥。

[0004] 现有的针对移动应用签名的认证与密钥协商方案存在着各种各样的安全缺陷,抗攻击能力弱,安全性差。

发明内容

[0005] 本发明实施例提供一种适用于移动应用签名的身份认证与密钥协商方法及设备,以解决目前针对移动应用签名的认证与密钥协商方案安全性差的问题。

[0006] 第一方面,本发明实施例提供一种适用于移动应用签名的身份认证与密钥协商方法,应用于用户端,包括:

[0007] 获取用户输入的身份信息,根据智能卡存储的预置参数和所述身份信息计算验证值;

[0008] 通过对比所述验证值与所述智能卡存储的注册验证值对所述身份信息进行验证;所述注册验证值为用户进行身份注册时生成的身份验证值;

[0009] 在所述身份信息验证通过后,生成第一随机数,并根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值,将包含所述第一交互值和所述第一认证值的登录请求发送至服务器;所述登录请求用于指示所述服务器根据所述第一认证值判定

用户是否为合法用户,并在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值,将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端;

[0010] 接收所述回复消息,并根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。

[0011] 第二方面,本发明实施例提供一种适用于移动应用签名的身份认证与密钥协商方法,应用于服务器,包括:

[0012] 接收用户端发送的包含第一交互值和第一认证值的登录请求;所述第一交互值和所述第一认证值为所述用户端根据预设椭圆曲线群的生成元和第一随机数计算得到;

[0013] 根据所述第一认证值判定用户是否为合法用户;

[0014] 在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值;

[0015] 将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端;所述回复信息用于指示所述用户端根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。

[0016] 第三方面,本发明实施例提供一种适用于移动应用签名的身份认证与密钥协商设备,包括:至少一个处理器和存储器;

[0017] 所述存储器存储计算机执行指令;

[0018] 所述至少一个处理器执行所述存储器存储的计算机执行指令,使得所述至少一个处理器执行如上第一方面以及第一方面各种可能的实施方式所述的身份认证与密钥协商方法,或者执行如上第二方面以及第二方面各种可能的实施方式所述的身份认证与密钥协商方法。

[0019] 第四方面,本发明实施例提供一种计算机可读存储介质,所述计算机可读存储介质中存储有计算机执行指令,当处理器执行所述计算机执行指令时,实现如上第一方面以及第一方面各种可能的实施方式所述的身份认证与密钥协商方法,或者实现如上第二方面以及第二方面各种可能的实施方式所述的身份认证与密钥协商方法。

[0020] 本实施例提供的适用于移动应用签名的身份认证与密钥协商方法及设备,用户端获取用户输入的身份信息,根据智能卡存储的预置参数和所述身份信息计算验证值;通过对比所述验证值与所述智能卡存储的注册验证值对所述身份信息进行验证;所述注册验证值为用户进行身份注册时生成的身份验证值;在所述身份信息验证通过后,生成第一随机数,并根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值,将包含所述第一交互值和所述第一认证值的登录请求发送至服务器;所述登录请求用于指示所述服务器根据所述第一认证值判定用户是否为合法用户,并在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值,将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端;接收所述回复消息,并根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。本发明实施例通过注册阶段生成的身份验证值能够确认用户身份,通过用户端与服务器之间的传递的第一交互值和第二交互值进行会话密钥协商,使得生成的会话密钥具有高安全性,从而提高移动应用签名身份认证与密钥协商

的安全性。

附图说明

[0021] 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一简单地介绍,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性的前提下,还可以根据这些附图获得其他的附图。

[0022] 图1为本发明实施例提供的适用于移动应用签名的身份认证与密钥协商系统的架构示意图;

[0023] 图2为本发明一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的流程示意图;

[0024] 图3为本发明又一实施例提供的适用于移动应用签名的身份认证与密钥协商方法中身份注册的流程示意图;

[0025] 图4为本发明另一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的流程示意图;

[0026] 图5为本发明再一实施例提供的适用于移动应用签名的身份认证与密钥协商方法中修改密码的流程示意图;

[0027] 图6为本发明下一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的流程示意图;

[0028] 图7为本发明还一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的流程示意图;

[0029] 图8为本发明一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的交互信令图;

[0030] 图9为本发明一实施例提供的适用于移动应用签名的身份认证与密钥协商装置的结构示意图;

[0031] 图10为本发明又一实施例提供的适用于移动应用签名的身份认证与密钥协商装置的结构示意图;

[0032] 图11为本发明另一实施例提供的适用于移动应用签名的身份认证与密钥协商装置的结构示意图;

[0033] 图12为本发明一实施例提供的适用于移动应用签名的身份认证与密钥协商设备的硬件结构示意图。

具体实施方式

[0034] 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作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。

[0035] 图1为本发明实施例提供的适用于移动应用签名的身份认证与密钥协商系统的架构示意图。本实施例提供的适用于移动应用签名的身份认证与密钥协商系统包括用户端11

和服务器12。用户端11可以为手机、平板、电脑等终端设备,在此不作限定。用户可以通过用户端11进行身份认证,并通过用户端11与服务器12之间的信息交互实现会话密钥协商。例如,对于移动应用签名场景,用户端11为移动终端,服务器12可以为提供应用下载服务的应用商店服务器。

[0036] 图2为本发明一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的流程示意图。本实施例的执行主体为用户端,如图2所示,该方法包括:

[0037] S201、获取用户输入的身份信息,根据智能卡存储的预置参数和所述身份信息计算验证值。

[0038] 在本实施例中,用户的身份信息可以包括但不限于身份标识、身份密码、生物识别特征等中的一个或多个,在此不作限定。例如,身份信息可以包括用户在应用商店注册的账户名称和账户密码。智能卡可以为单独的一张存储卡,也可以为用户端中指定的一个存储空间,在此不作限定。用户端和服务器均可以向智能卡写入或读取数据。智能卡存储的预置参数为用户在进行身份注册过程中用户端和/或服务器写入到智能卡的参数。

[0039] 用户端可以获取用户输入的身份信息,从智能卡读取存储的预置参数,根据智能卡存储的预置参数和身份信息计算验证值。验证值用于对用户输入的身份信息进行验证。

[0040] S202、通过对比所述验证值与所述智能卡存储的注册验证值对所述身份信息进行验证;所述注册验证值为用户进行身份注册时生成的身份验证值。

[0041] 在本实施例中,智能卡存储有用户进行身份注册时生成的注册验证值,该注册验证值为根据用户注册时的身份信息计算得到。用户端从智能卡读取注册验证值,对比验证值与智能卡存储的注册验证值,若验证值与智能卡存储的注册验证值相同,则身份信息验证通过;若验证值与智能卡存储的注册验证值不同,则身份信息验证未通过。

[0042] S203、在所述身份信息验证通过后,生成第一随机数,并根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值,将包含所述第一交互值和所述第一认证值的登录请求发送至服务器;所述登录请求用于指示所述服务器根据所述第一认证值判定用户是否为合法用户,并在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值,将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端。

[0043] 在本实施例中,预设椭圆曲线群的生成元为预先设定的椭圆曲线群和指定的生成元,该椭圆曲线群和该生成元为服务器和终端都能够获取到的信息。第一认证值用于服务器判断用户端当前的用户是否为合法用户,第二认证值用于用户端判断服务器是否为合法服务器。第一交互值和第二交互值用于用户端和服务器进行密钥协商。

[0044] 在身份信息通过验证后,用户端生成一个随机数作为第一随机数,然后根据预设椭圆曲线群的生成元和第一随机数计算第一交互值和第一认证值,将包含第一交互值和第一认证值的登录请求发送至服务器。服务器接收该登录请求,根据第一认证值判定用户是否为合法用户。服务器在判定用户为合法用户后,生成第二随机数,并根据第二随机数、预设椭圆曲线群的生成元和第一交互值计算第二交互值和第二认证值,将包含第二交互值和第二认证值的回复消息发送至用户端。

[0045] S204、接收所述回复消息,并根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。

[0056] 图4为本发明另一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的流程示意图。本实施例在图2实施例的基础上,对本实施例的具体实现过程进行了详细说明。如图4所示,该方法可以包括:

[0057] S401、获取用户输入的身份信息,根据所述预置参数、所述身份信息和第一公式计算所述验证值;所述第一公式为:

$$[0058] \quad V_i^* = h(ID_i^* \parallel PW_i^* \parallel N_i) \bmod n \quad (1)$$

[0059] 其中, V_i^* 为所述验证值, $h()$ 为哈希函数, ID_i^* 为所述身份标识, PW_i^* 为所述身份密码, N_i 为所述预置随机数, n 为所述预置整数。

[0060] 在本实施例中,所述预置参数包括预置随机数和预置整数,所述身份信息包括身份标识及身份密码。预置随机数为用户在身份注册阶段生成的一个随机数,并将该随机数写入到智能卡中。预置整数为服务器在系统初始化阶段生成的一个整数值,并将该整数值写入到智能卡。哈希函数可以为预先选取一个安全的哈希函数。

[0061] S402、通过对比所述验证值与所述智能卡存储的注册验证值对所述身份信息进行验证;所述注册验证值为用户进行身份注册时生成的身份验证值。

[0062] 在本实施例中,S402与图2实施例中的S202类似,此处不再赘述。

[0063] S403、在所述身份信息验证通过后,生成第一随机数,根据所述预设椭圆曲线群的生成元、第一随机数及第二公式计算所述第一交互值;所述第二公式为:

$$[0064] \quad R_i = N_1 P \quad (2)$$

[0065] 其中, R_i 为所述第一交互值, N_1 为所述第一随机数, P 为所述预设椭圆曲线群的生成元。

[0066] S404、根据所述第一交互值和第三公式计算所述第一认证值;所述第三公式为:

$$[0067] \quad D_i = h(A_i^* \parallel R_i) \quad (3)$$

[0068] 其中, D_i 为所述第一认证值, $A_i^* = B_i \oplus F_i^*$, B_i 为所述第一预置值, $F_i^* = h(ID_i^* \parallel PW_i^* \parallel N_i)$ 。

[0069] 在本实施例中,预置参数包括预置公钥和第一预置值。其中预置公钥为服务器根据私钥和预设椭圆曲线群的生成元计算得到的公钥,并由服务器写入到智能卡中。第一预置值为服务器在用户身份注册时由私钥和待注册身份信息得到的一个预置值,并写入到智能卡中。

[0070] S405、根据所述第一随机数和第四公式计算加密密钥;所述第四公式为:

$$[0071] \quad C_i = h(N_1 P_{\text{PUB}}) \quad (4)$$

[0072] 其中, C_i 为所述加密密钥, P_{PUB} 为所述预置公钥。

[0073] S406、根据所述加密密钥和高级加密标准算法对所述身份标识和所述第一认证值加密得到密文。

[0074] 在本实施例中,可以通过AES (Advanced Encryption Standard, 高级加密标准) 算法对身份标识和所述第一认证值进行加密。

[0075] S407、生成时间戳,将包含所述密文、所述时间戳和所述第一交互值的登录请求发

送至所述服务器。所述登录请求用于指示所述服务器根据所述第一认证值判定用户是否为合法用户,并在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值,将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端。

[0076] 在本实施例中,S407与图2实施例中的S203类似,此处不再赘述。

[0077] S408、接收所述回复消息,根据所述第一随机数、所述第二交互值和第五公式计算会话密钥;所述第五公式为:

$$[0078] \quad SK = h(K'_i \| A_i^*) \quad (5)$$

[0079] 其中,SK为所述会话密钥, $K'_i = N_i * Z_i$, Z_i 为所述第二交互值。

[0080] S409、根据第六公式计算所述第二认证值对应的验证值;所述第六公式为:

$$[0081] \quad X'_i = h(Z_i \| A_i^* \| C_i \| SK) \quad (6)$$

[0082] 其中, X'_i 为所述第二认证值对应的验证值。

[0083] S410、若所述第二认证值对应的验证值与所述第二验证值相等,则判定服务器合法,并将所述会话密钥作为所述用户端与所述服务器之间的会话密钥。

[0084] 传统的身份认证和密钥协商方法,并不能满足移动应用签名的需求。首先,已有的认证与密钥协商方案,存在着许多安全缺陷,或是不能抵抗离线密码猜测攻击、拒绝服务攻击、智能卡丢失攻击、离线密码猜测攻击、用户模拟攻击、内部特权攻击、重放攻击的一种或多种攻击,或是不能满足前向安全性、用户匿名性。这些方案不能为移动应用签名提高安全可靠的服务保障。其次,方案的效率不能满足移动应用签名的需求。在用户获取网络服务时,服务器的响应时间对用户来说是非常重要的,这就要求认证与密钥协商方案要有高效率,才能保证良好的用户体验。

[0085] 相对于传统的身份认证和密钥协商方法,本实施例提供的身份认证和密钥协商方法具有以下优点:

[0086] 1. 基于椭圆曲线密码体制设计认证与密钥协商方案,该方法具有强安全性的优点,同时具有抗攻击性强、CPU占用少、内容使用少、网络消耗低、加密速度快等优点。

[0087] 2. 高效安全的实现了用户端与服务器之间的认证与会话密钥协商,同时方案满足用户匿名性、前向安全性等良好的安全特性。采用对称加密的方式传递用户身份实现了用户匿名性,加密密钥随着用户选取的随机数而改变,每次加密的结果都不相同,保证了用户行为不被追踪。服务器在注册阶段安全的分发给用户一个认证信息,在登陆与认证阶段用户端和服务器通过对认证信息的验证从而确认通信方的真实身份。通过椭圆曲线Diffie-Hellman密钥交换的方式协商用户端与服务器的会话密钥,生成的会话密钥具有高安全性:满足前向安全性,甚至在一方临时秘密值泄露的情况下会话密钥的安全性也不受影响,攻击者通过各种攻击方法无法揭露本方案的会话密钥,为用户端与服务器的通信安全提供了保障。

[0088] 3. 该方法满足移动应用签名场景的安全要求及效率要求。方案能够抵抗各种网络攻击与密码分析,能够抵抗离线密码猜测攻击、拒绝服务攻击、内部特权攻击、用户模拟攻击、服务器模拟攻击、重放攻击等攻击,满足移动应用签名的高安全需求。同时方案具有高效率,在用户认证与密钥协商过程中方案的计算开销5个点乘、3个AES加解密、10个哈希运

算,相比传统方案在效率上有明显提升,能够满足移动应用签名场景的需求。

[0089] 图5为本发明再一实施例提供的适用于移动应用签名的身份认证与密钥协商方法中修改密码的流程示意图。本实施例在图2实施例的基础上,对本实施例的密码修改过程进行了详细说明。如图5所示,该方法还可以包括:

[0090] S501、在所述身份信息验证通过后,获取用户输入的新身份密码。

[0091] 在本实施例中,用户可以在用户端申请修改密码。用户端获取用户输入修改前的身份信息,对身份信息进行验证。在身份信息验证通过后,用户端获取用户输入的新身份密码。

[0092] S502、根据所述新身份密码和第七公式计算所述新注册认证值;所述第七公式为:

$$[0093] \quad V_i^{new} = h(ID_i^* \parallel PW_i^{new} \parallel N_i) \bmod n \quad (7)$$

[0094] 其中, V_i^{new} 为所述新注册认证值, PW_i^{new} 为新身份密码。

[0095] S503、根据第八公式计算新第一预置值;所述第八公式为:

$$[0096] \quad B_i^{new} = B_i \oplus h(ID_i^* \parallel PW_i^* \parallel N_i) \oplus h(ID_i^* \parallel PW_i^{new} \parallel N_i) \quad (8)$$

[0097] 其中, B_i^{new} 为所述新第一预置值。

[0098] S504、将所述存储卡中存储的注册认证值替换为所述新注册认证值,将所述存储卡中存储的所述第一预置值替换为所述新第一预置值。

[0099] 在本实施例中,用户修改密码时,用户端通过将存储卡中存储的注册认证值替换为新注册认证值,将存储卡中存储的第一预置值替换为新第一预置值,不用与服务器进行通信就能实现密码修改,方便快捷。用户端本地更新密码,效率较高,节省了通信开销与服务器的计算开销。

[0100] 图6为本发明下一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的流程示意图。本实施例的执行主体为服务器,本实施例的具体实施方式与上述图2所示的以用户端为执行主体的实施例类似,因此下文仅简要叙述,不赘述。如图6所示,该方法包括:

[0101] S601、接收用户端发送的包含第一交互值和第一认证值的登录请求;所述第一交互值和所述第一认证值为所述用户端根据预设椭圆曲线群的生成元和第一随机数计算得到。

[0102] 在本实施例中,在用户登录阶段,用户端根据预设椭圆曲线群的生成元和第一随机数计算得到第一交互值和第一认证值,将包含第一交互值和第一认证值的登录请求发送到服务器。服务器接收该登录请求。

[0103] S602、根据所述第一认证值判定用户是否为合法用户。

[0104] S603、在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值。

[0105] 在本实施例中,服务器根据第一认证值判定用户是否为合法用户。服务器在判定用户为合法用户后,生成第二随机数,根据第二随机数、预设椭圆曲线群的生成元和第一交互值计算第二交互值和第二认证值。

[0106] S604、将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端;所述回复信息用于指示所述用户端根据所述第一随机数、所述第二交互值和所述第二认证

值验证服务器身份以及确定会话密钥。

[0107] 在本实施例中,服务器将包含第二交互值和第二认证值的回复消息发送至用户端。用户端根据第一随机数、第二交互值和第二认证值验证服务器身份以及确定会话密钥。

[0108] 图7为本发明还一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的流程示意图。本实施例在图6实施例的基础上,对本实施例的具体实现过程进行了详细说明。如图7所示,该方法可以包括:

[0109] S701、接收用户端发送的包含第一交互值和第一认证值的登录请求;所述第一交互值和所述第一认证值为所述用户端根据预设椭圆曲线群的生成元和第一随机数计算得到。

[0110] 在本实施例中,登录请求包括对第一认证值和身份标识加密得到的密文、所述第一交互值以及时间戳。在本实施例中,S701与图6实施例中的S601类似,此处不再赘述。

[0111] S702、判定所述时间戳是否有效。

[0112] S703、若所述时间戳有效,则根据私钥、所述第一交互值和第九公式计算解密密钥;所述第九公式为:

$$[0113] \quad C'_i = h(xR_i) \quad (9)$$

[0114] 其中, C'_i 为所述解密密钥, $h()$ 为哈希函数, x 为所述私钥, R_i 为所述第一交互值。

[0115] S704、根据所述解密密钥和高级加密标准算法对所述密文进行解密得到解密出的第一认证值和解密出的身份标识。

[0116] 在本实施例中,服务器根据AES算法对密文进行解密得到解密出的第一认证值和解密出的身份标识。

[0117] S705、根据第十公式计算所述第一认证值对应的验证值;所述第十公式为:

$$[0118] \quad D''_i = h(A'_i || R_i) \quad (10)$$

[0119] 其中, D''_i 为所述第一认证值对应的验证值, $A'_i = h(x || ID'_i)$, ID'_i 为所述解密出的身份标识。

[0120] S706、若所述第一认证值对应的验证值与所述第一验证值相等,则判定用户为合法用户。

[0121] S707、在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值。

[0122] 可选地,S707可以包括:

[0123] 根据所述第二随机数和第十一公式计算所述第二交互值;所述第十一公式为:

$$[0124] \quad Z_i = N_2 P \quad (11)$$

[0125] 其中, Z_i 为所述第二交互值, N_2 为所述第二随机数, P 为所述预设椭圆曲线群的生成元;

[0126] 根据所述第二随机数和第十二公式计算所述第二认证值;所述第十二公式为:

$$[0127] \quad X_i = h(Z_i || A'_i || C'_i || SK) \quad (12)$$

[0128] 其中, X_i 为所述第二认证值, SK 为会话密钥, $SK = h(K_i || A'_i)$, $K_i = N_2 * R_i$ 。

[0129] S708、将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端;所述回复信息用于指示所述用户端根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。

[0130] 在本实施例中,S708与图6实施例中的S604类似,此处不再赘述。

[0131] 图8为本发明一实施例提供的适用于移动应用签名的身份认证与密钥协商方法的交互信令图。如图8所示,该方法可以包括:

[0132] S801、用户端获取用户输入的待注册身份信息。

[0133] S802、用户端生成第三随机数,并根据待注册身份信息和第三随机数计算哈希值。

[0134] S803、用户端将包含待注册身份标识和哈希值的注册请求发送至服务器。

[0135] S804、服务器根据私钥、待注册身份标识和哈希值确定服务器预置参数,将服务器预置参数存储到存储卡。

[0136] S805、用户端根据哈希值和服务器预置参数计算注册验证值,将第三随机数和注册验证值作为用户端预置参数存储到存储卡。

[0137] S806、用户端获取用户输入的身份信息,根据智能卡存储的预置参数和身份信息计算验证值,通过对比验证值与智能卡存储的注册验证值对身份信息进行验证。

[0138] S807、用户端在身份信息验证通过后,生成第一随机数,并根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值。

[0139] S808、用户端将包含第一交互值和第一认证值的登录请求发送至服务器。

[0140] S809、服务器根据第一认证值判定用户是否为合法用户,并在判定用户为合法用户后,生成第二随机数,根据第二随机数、预设椭圆曲线群的生成元和第一交互值计算第二交互值和第二认证值。

[0141] S810、服务器将包含第二交互值和第二认证值的回复消息发送至用户端。

[0142] S811、用户端根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。

[0143] 本实施例的具体实施方式与上述图2及图3所示的实施例类似,此处不再赘述。

[0144] 作为本发明的一个实施示例,该身份认证与会话密钥协商方法可以包括系统初始化、用户注册阶段、认证与密钥协商、用户密码更新四部分,具体如下:

[0145] 第一部分,系统初始化。该部分包含以下步骤:

[0146] 步骤1.1、选择一个椭圆曲线群 E_p 以及它的一个生成元 P 。

[0147] 步骤1.2、选择一个随机数 x ,计算公钥 $P_{pub} = xP$ 。

[0148] 步骤1.3、选取整数 n ,满足 $2^8 \leq n < 2^{10}$ 。

[0149] 步骤1.4、选择一个安全的哈希函数 $h()$ 。

[0150] 步骤1.5、选取高级加密标准算法(Advanced Encryption Standard, AES) $E_{key}()$, key 是算法的密钥,在该方法执行过程中生成,不预先设定。

[0151] 步骤1.6、服务器秘密保存 x ,公布 $\{E_p, P, P_{pub}, n\}$ 。

[0152] 第二部分:用户注册。该部分包含以下步骤:

[0153] 步骤2.1、用户端生成注册请求消息。

[0154] 用户选择它的身份 ID_i 及密码 PW_i ,用户端生成一个随机数 N_i ,计算 $F_i = h(ID_i || PW_i || N_i)$,通过安全信道发送注册请求消息 $\{ID_i, F_i\}$ 给服务器。

[0155] 步骤2.2、服务器为用户分发智能卡。

[0156] 服务器收到注册请求后,计算 $A_i = h(x || ID_i)$, $B_i = A_i \oplus F_i$ 。服务器把参数 $\{B_i, P_{pub}, n\}$ 存入一张智能卡,并把智能卡安全的分发给用户。

[0157] 步骤2.3、用户收到智能卡后,计算 $V_i = F_i \bmod n$,把 V_i, N_i 存入智能卡中。

[0158] 第三部分,认证与密钥协商。该部分包含以下步骤:

[0159] 步骤3.1、用户端验证用户身份密码的有效性,并为用户生成登陆请求消息。

[0160] 步骤3.1.1、用户把智能卡放入用户端,输入他的身份以及密码,用户端计算 $F_i^* = h(ID_i^* \| PW_i^* \| N_i)$, $V_i^* = F_i^* \bmod n$,验证 V_i^* 与 V_i 是否相等,若相等,代表用户输入的身份与密码是正确的,则执行下一步,否则,方案终止,认证失败。

[0161] 步骤3.1.2、用户端产生一个随机数 N_1 ,计算 $R_i = N_1 P$, $C_i = h(N_1 P_{PUB})$, $A_i^* = B_i \oplus F_i^*$, $D_i = h(A_i^* \| R_i)$ 。以 C_i 为加密密钥运行AES算法加密用户身份及认证值 D_i ,得到密文 $L_i = E_{C_i}(ID_i^* \| D_i)$ 。生成时间戳 T_i ,把 $\{L_i, R_i, T_i\}$ 作为登陆请求送给服务器。

[0162] 步骤3.2、服务器处理用户的登陆请求消息,若确认用户合法,则返回一个回复消息,该回复消息包含服务器的认证信息。

[0163] 步骤3.2.1、服务器收到用户的登陆请求后,首先验证 T_i 的有效性,若 T_i 有效,则执行下一阶段,否则,方案终止,认证失败。

[0164] 步骤3.2.2、服务器计算 $C'_i = h(x R_i)$,以 C'_i 为密钥解密 L_i 得到 $(ID'_i \| D'_i) = D_{C'_i}(L_i)$ 。计算 $A'_i = h(x \| ID'_i)$, $D''_i = h(A'_i \| R_i)$,验证 D''_i 与 D'_i 是否相等,若相等,则相信其为合法用户,执行下一步骤;否则,方案终止,认证失败。

[0165] 步骤3.2.3、服务器生成随机数 N_2 ,计算 $Z_i = N_2 P$, $K_i = N_2 * R_i$,计算会话密钥 $SK = h(K_i \| A'_i)$,计算认证值 $X_i = h(Z_i \| A'_i \| C'_i \| SK)$ 。把消息 $\{Z_i, X_i\}$ 返回给用户。

[0166] 步骤3.3、用户端对服务器回复的消息进行确认,验证服务器的身份,若服务器身份合法,则根据用户端以及服务器选取的随机数生成其椭圆曲线 Diffie-Hellman 密钥交换的值,以及认证阶段服务器通过智能卡分发给用户的认证信息 A_i ,生成会话密钥,并返回一个确认消息给服务器。

[0167] 步骤3.3.1、收到服务器的回复消息后,用户端计算 $K'_i = N_1 * Z_i$,计算会话密钥 $SK = h(K'_i \| A_i^*)$,计算认证值 $X'_i = h(Z_i \| A_i^* \| C_i \| SK)$,验证 X'_i 与 X_i 是否相等。若相等,用户端认为服务器是合法的,并确信它与服务器协商了会话密钥 SK ;否则,方案终止,认证失败。

[0168] 第四部分用户密码更新。该部分包含以下步骤:

[0169] 步骤4.1、验证用户身份及密码的有效性。

[0170] 用户把智能卡插入终端,并输入他的身份及密码,用户端计算 $F_i^* = h(ID_i^* \| PW_i^* \| N_i)$, $V_i^* = F_i^* \bmod n$,验证 V_i^* 与 V_i 是否相等。若相等,说明用户拥有正确的身份与密码。要求用户输入他的新密码 PW_i^{new} 。

[0171] 步骤4.2、用户输入新密码后,用户端根据新密码更新智能卡中对应的参数。

[0172] 客户端计算 $B_i^{new} = B_i \oplus h(ID_i^* \| PW_i^* \| N_i) \oplus h(ID_i^* \| PW_i^{new} \| N_i)$, $V_i^{new} = h(ID_i^* \| PW_i^{new} \| N_i) \bmod n$,把 B_i^{new} , V_i^{new} 存入智能卡,并从智能卡中删除失效的 B_i, V_i 。

[0173] 本实施例提供的身份认证及密钥协商方法具有以下优点：

[0174] 1. 在用户端对用户输入的身份与密码采用模糊验证的方式，在智能卡中存储 V_i 而非 F_i ，避免因智能卡中存储 F_i 而导致的离线密码猜测攻击。若智能卡中存有 F_i ，则在攻破智能卡的情况下，可利用 F_i 验证猜测的用户身份与密码的正确性而最终试出用户的身份与密码。而所提算法采用模糊验证的方式，在用户与密码为32位时， n 为 2^8 时，有 2^{56} 个猜测的身份密码对满足 $V_i^* = h(ID_i^* \| PW_i^* \| N_i) \bmod n$ ，从而无法确定用户真实的身份与密码。

[0175] 2. 实现用户与服务器双方身份认证，服务器在注册阶段安全的分发给用户一个认证信息 A_i ，在登陆与认证阶段用户和服务器通过对认证信息 A_i 的验证从而确认通信方的真实身份。

[0176] 3. 实现安全会话密钥协商，用户和服务器经过交互协商得到会话密钥 $SK = h(K'_i \| A_i^*)$ ， A_i^* 为只有用户与服务器知道的认证信息， K'_i 是用户与服务器通过椭圆曲线Diffie-Hellman密钥交换生成的， K'_i 保证了生成的会话密钥的前向安全性。 A_i^* 保证了生成的会话密钥能够抵抗临时秘密值丢失攻击(N_1 或 N_2 泄露)。

[0177] 4. 实现用户身份匿名，用户选取随机数 N_1 ，计算 $R_i = N_1P$ ， $C_i = h(N_1P_{PUB})$ ，其中 P_{PUB} 为服务器的公钥，只有拥有 N_1 的用户 U_i 或拥有服务器私钥的合法服务器才能计算出 C_i 。加密密钥 C_i 随着用户选取的随机数而改变，每次加密的结果都不相同，保证了用户身份的不可追踪性。在用户端以 C_i 为AES算法的密钥对用户身份加密，得到 $L_i = E_{C_i}(ID_i^* \| D_i)$ ，服务器通过计算 $C'_i = h(xR_i)$ ，并解密 L_i 得到用户的真实身份。

[0178] 本发明实施例中，用户端获取用户输入的身份信息，根据智能卡存储的预置参数和所述身份信息计算验证值；通过对比所述验证值与所述智能卡存储的注册验证值对所述身份信息进行验证；所述注册验证值为用户进行身份注册时生成的身份验证值；在所述身份信息验证通过后，生成第一随机数，并根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值，将包含所述第一交互值和所述第一认证值的登录请求发送至服务器；所述登录请求用于指示所述服务器根据所述第一认证值判定用户是否为合法用户，并在判定用户为合法用户后，生成第二随机数，根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值，将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端；接收所述回复消息，并根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。本发明实施例通过注册阶段生成的身份验证值能够确认用户身份，通过用户端与服务器之间的传递的第一交互值和第二交互值进行会话密钥协商，使得生成的会话密钥具有高安全性，从而提高移动应用签名认证与密钥协商的安全性。

[0179] 图9为本发明一实施例提供的适用于移动应用签名的身份认证与密钥协商装置的结构示意图。如图9所示，该身份认证与密钥协商装置90应用于用户端，包括：获取模块901、身份验证模块902、交互认证模块903及会话密钥确定模块904。

[0180] 获取模块901，用于获取用户输入的身份信息，根据智能卡存储的预置参数和所述身份信息计算验证值。

[0181] 身份验证模块902，用于通过对比所述验证值与所述智能卡存储的注册验证值对

所述身份信息验证;所述注册验证值为用户进行身份注册时生成的身份验证值。

[0182] 交互认证模块903,用于在所述身份信息验证通过后,生成第一随机数,并根据预设椭圆曲线群的生成元和所述第一随机数计算第一交互值和第一认证值,将包含所述第一交互值和所述第一认证值的登录请求发送至服务器;所述登录请求用于指示所述服务器根据所述第一认证值判定用户是否为合法用户,并在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值,将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端。

[0183] 会话密钥确定模块904,用于接收所述回复消息,并根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。

[0184] 本发明实施例中,用户端获取用户输入的身份信息,根据智能卡存储的预置参数和所述身份信息计算验证值;通过对比所述验证值与所述智能卡存储的注册验证值对所述 ([0185] 图10为本发明又一实施例提供的适用于移动应用签名的身份认证与密钥协商装置的结构示意图。如图10所示,本实施例提供的身份认证与密钥协商装置90在图9所示实施例提供的身份认证与密钥协商装置的基础上,还包括:身份注册模块905和密码修改模块906。

[0185] 图10为本发明又一实施例提供的适用于移动应用签名的身份认证与密钥协商装置的结构示意图。如图10所示,本实施例提供的身份认证与密钥协商装置90在图9所示实施例提供的身份认证与密钥协商装置的基础上,还包括:身份注册模块905和密码修改模块906。

[0186] 可选地,所述身份注册模块905用于:

[0187] 获取用户输入的待注册身份信息;所述待注册身份信息包括待注册身份标识及待注册身份密码;

[0188] 生成第三随机数,并根据所述待注册身份信息和所述第三随机数计算哈希值,将包含所述待注册身份标识和所述哈希值的注册请求发送至服务器;所述注册请求用于指示所述服务器根据私钥、所述待注册身份标识和所述哈希值确定服务器预置参数,将所述服务器预置参数存储到所述存储卡;

[0189] 根据所述哈希值和所述服务器预置参数计算所述注册验证值,将所述第三随机数和所述注册验证值作为所述用户端预置参数存储到所述存储卡。

[0190] 可选地,所述预置参数包括预置随机数和预置整数,所述身份信息包括身份标识及身份密码;所述获取模块901用于:

[0191] 根据所述预置参数、所述身份信息和第一公式计算所述验证值;所述第一公式为:

$$[0192] \quad V_i^* = h(ID_i^* \| PW_i^* \| N_i) \bmod n$$

[0193] 其中, V_i^* 为所述验证值, $h()$ 为哈希函数, ID_i^* 为所述身份标识, PW_i^* 为所述身份密码, N_i 为所述预置随机数, n 为所述预置整数。

[0194] 可选地, 所述预置参数包括预置公钥和第一预置值; 所述交互认证模块 903 用于:

[0195] 根据所述预设椭圆曲线群的生成元、第一随机数及第二公式计算所述第一交互值; 所述第二公式为:

$$[0196] \quad R_i = N_i P$$

[0197] 其中, R_i 为所述第一交互值, N_i 为所述第一随机数, P 为所述预设椭圆曲线群的生成元;

[0198] 根据所述第一交互值和第三公式计算所述第一认证值; 所述第三公式为:

$$[0199] \quad D_i = h(A_i^* \| R_i)$$

[0200] 其中, D_i 为所述第一认证值, $A_i^* = B_i \oplus F_i^*$, B_i 为所述第一预置值, $F_i^* = h(ID_i^* \| PW_i^* \| N_i)$;

[0201] 根据所述第一随机数和第四公式计算加密密钥; 所述第四公式为:

$$[0202] \quad C_i = h(N_i P_{\text{PUB}})$$

[0203] 其中, C_i 为所述加密密钥, P_{PUB} 为所述预置公钥;

[0204] 根据所述加密密钥和高级加密标准算法对所述身份标识和所述第一认证值加密得到密文;

[0205] 生成时间戳, 将包含所述密文、所述时间戳和所述第一交互值的登录请求发送至所述服务器。

[0206] 可选地, 所述会话密钥确定模块 904 用于:

[0207] 根据所述第一随机数、所述第二交互值和第五公式计算会话密钥; 所述第五公式为:

$$[0208] \quad SK = h(K_i' \| A_i^*)$$

[0209] 其中, SK 为所述会话密钥, $K_i' = N_i * Z_i$, Z_i 为所述第二交互值;

[0210] 根据第六公式计算所述第二认证值对应的验证值; 所述第六公式为:

$$[0211] \quad X_i' = h(Z_i \| A_i^* \| C_i \| SK)$$

[0212] 其中, X_i' 为所述第二认证值对应的验证值;

[0213] 若所述第二认证值对应的验证值与所述第二验证值相等, 则判定服务器合法, 并将所述会话密钥作为所述用户端与所述服务器之间的会话密钥。

[0214] 可选地, 所述密码修改模块 906 用于:

[0215] 在所述身份信息验证通过后, 获取用户输入的新身份密码;

[0216] 根据所述新身份密码和第七公式计算所述新注册认证值; 所述第七公式为:

$$[0217] \quad V_i^{\text{new}} = h(ID_i^* \| PW_i^{\text{new}} \| N_i) \bmod n$$

[0218] 其中, V_i^{new} 为所述新注册认证值, PW_i^{new} 为新身份密码;

[0219] 根据第八公式计算新第一预置值;所述第八公式为:

$$[0220] \quad B_i^{new} = B_i \oplus h(ID_i^* \parallel PW_i^* \parallel N_i) \oplus h(ID_i^* \parallel PW_i^{new} \parallel N_i)$$

[0221] 其中, B_i^{new} 为所述新第一预置值;

[0222] 将所述存储卡中存储的注册认证值替换为所述新注册认证值,将所述存储卡中存储的所述第一预置值替换为所述新第一预置值。

[0223] 本发明实施例提供的身份认证与密钥协商装置,可用于执行上述以用户端为执行主体的方法实施例,其实现原理和技术效果类似,本实施例此处不再赘述。

[0224] 图11为本发明另一实施例提供的适用于移动应用签名的身份认证与密钥协商装置的结构示意图。如图11所示,该身份认证与密钥协商装置110应用于服务器,包括:接收模块1101、判定模块1102、计算模块1103及发送模块1104。

[0225] 接收模块1101,用于接收用户端发送的包含第一交互值和第一认证值的登录请求;所述一交互值和所述第一认证值为所述用户端根据预设椭圆曲线群的生成元和第一随机数计算得到。

[0226] 判定模块1102,用于根据所述第一认证值判定用户是否为合法用户。

[0227] 计算模块1103,用于在判定用户为合法用户后,生成第二随机数,根据所述第二随机数、所述预设椭圆曲线群的生成元和所述第一交互值计算第二交互值和第二认证值。

[0228] 发送模块1104,用于将包含所述第二交互值和所述第二认证值的回复消息发送至所述用户端;所述回复信息用于指示所述用户端根据所述第一随机数、所述第二交互值和所述第二认证值验证服务器身份以及确定会话密钥。

[0229] 可选地,所述登录请求包括对第一认证值和身份标识加密得到的密文、所述第一交互值以及时间戳;所述判定模块1102用于:

[0230] 判定所述时间戳是否有效;

[0231] 若所述时间戳有效,则根据私钥、所述第一交互值和第九公式计算解密密钥;所述第九公式为:

$$[0232] \quad C'_i = h(xR_i)$$

[0233] 其中, C'_i 为所述解密密钥, $h()$ 为哈希函数, x 为所述私钥, R_i 为所述第一交互值;

[0234] 根据所述解密密钥和高级加密标准算法对所述密文进行解密得到解密出的第一认证值和解密出的身份标识;

[0235] 根据第十公式计算所述第一认证值对应的验证值;所述第十公式为:

$$[0236] \quad D''_i = h(A'_i \parallel R_i)$$

[0237] 其中, D''_i 为所述第一认证值对应的验证值, $A'_i = h(x \parallel ID'_i)$, ID'_i 为所述解密出的身份标识;

[0238] 若所述第一认证值对应的验证值与所述第一验证值相等,则判定用户为合法用户。

[0239] 本发明实施例提供的身份认证与密钥协商装置,可用于执行上述以服务器为执行主体的方法实施例,其实现原理和技术效果类似,本实施例此处不再赘述。

[0240] 图12为本发明一实施例提供的适用于移动应用签名的身份认证与密钥协商设备的硬件结构示意图。如图12所示,本实施例提供的身份认证与密钥协商设备120包括:至少

一个处理器1201和存储器1202。该身份认证与密钥协商设备120还包括通信部件1203。其中,处理器1201、存储器1202以及通信部件1203通过总线1204连接。

[0241] 在具体实现过程中,至少一个处理器1201执行所述存储器1202存储的计算机执行指令,使得至少一个处理器1201执行如上应用于用户端的身份认证与密钥协商方法,或者执行如上应用于服务器的身份认证与密钥协商方法。

[0242] 处理器1201的具体实现过程可参见上述方法实施例,其实现原理和技术效果类似,本实施例此处不再赘述。

[0243] 在上述的图12所示的实施例中,应理解,处理器可以是中央处理单元(英文:Central Processing Unit,简称:CPU),还可以是其他通用处理器、数字信号处理器(英文:Digital Signal Processor,简称:DSP)、专用集成电路(英文:Application Specific Integrated Circuit,简称:ASIC)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。结合发明所公开的方法的步骤可以直接体现为硬件处理器执行完成,或者用处理器中的硬件及软件模块组合执行完成。

[0244] 存储器可能包含高速RAM存储器,也可能还包括非易失性存储NVM,例如至少一个磁盘存储器。

[0245] 总线可以是工业标准体系结构(Industry Standard Architecture,ISA)总线、外部设备互连(Peripheral Component,PCI)总线或扩展工业标准体系结构(Extended Industry Standard Architecture,EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示,本申请附图中的总线并不限定仅有一根总线或一种类型的总线。

[0246] 本申请还提供一种计算机可读存储介质,所述计算机可读存储介质中存储有计算机执行指令,当处理器执行所述计算机执行指令时,实现如上应用于用户端的身份认证与密钥协商方法,或者实现如上应用于服务器的身份认证与密钥协商方法。

[0247] 上述的计算机可读存储介质,上述可读存储介质可以由任何类型的易失性或非易失性存储设备或者它们的组合实现,如静态随机存取存储器(SRAM),电可擦除可编程只读存储器(EEPROM),可擦除可编程只读存储器(EPROM),可编程只读存储器(PROM),只读存储器(ROM),磁存储器,快闪存储器,磁盘或光盘。可读存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0248] 一种示例性的可读存储介质耦合至处理器,从而使处理器能够从该可读存储介质读取信息,且可向该可读存储介质写入信息。当然,可读存储介质也可以是处理器的组成部分。处理器和可读存储介质可以位于专用集成电路(Application Specific Integrated Circuits,简称:ASIC)中。当然,处理器和可读存储介质也可以作为分立组件存在于设备中。

[0249] 本领域普通技术人员可以理解:实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时,执行包括上述各方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0250] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述各实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分或者全部技术特征进

行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。



图1

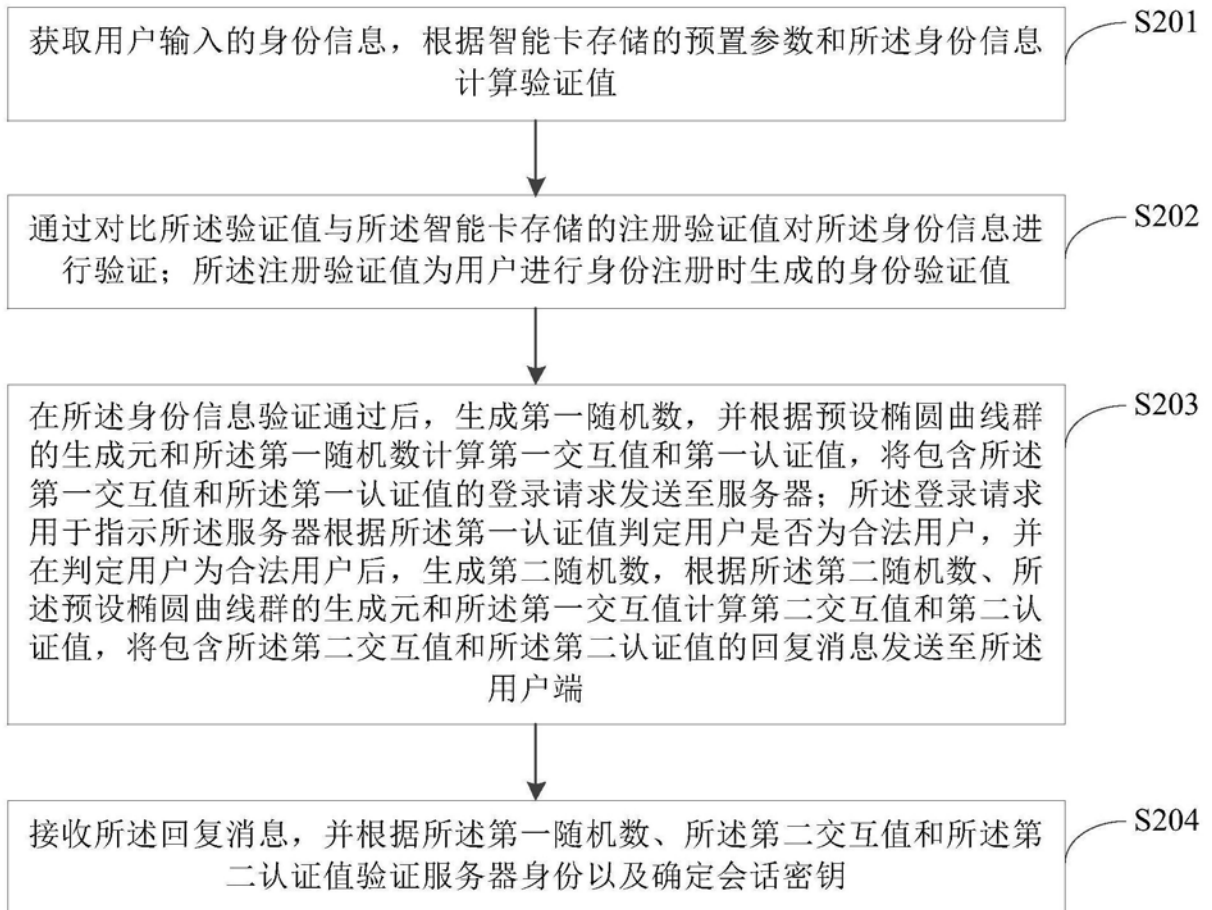


图2

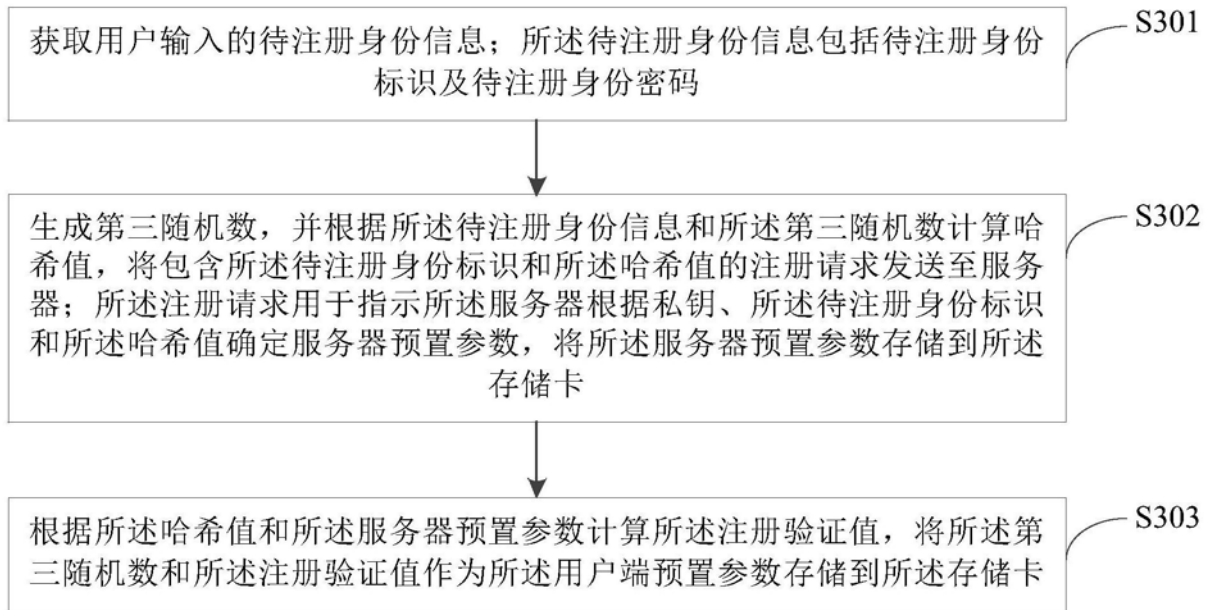


图3

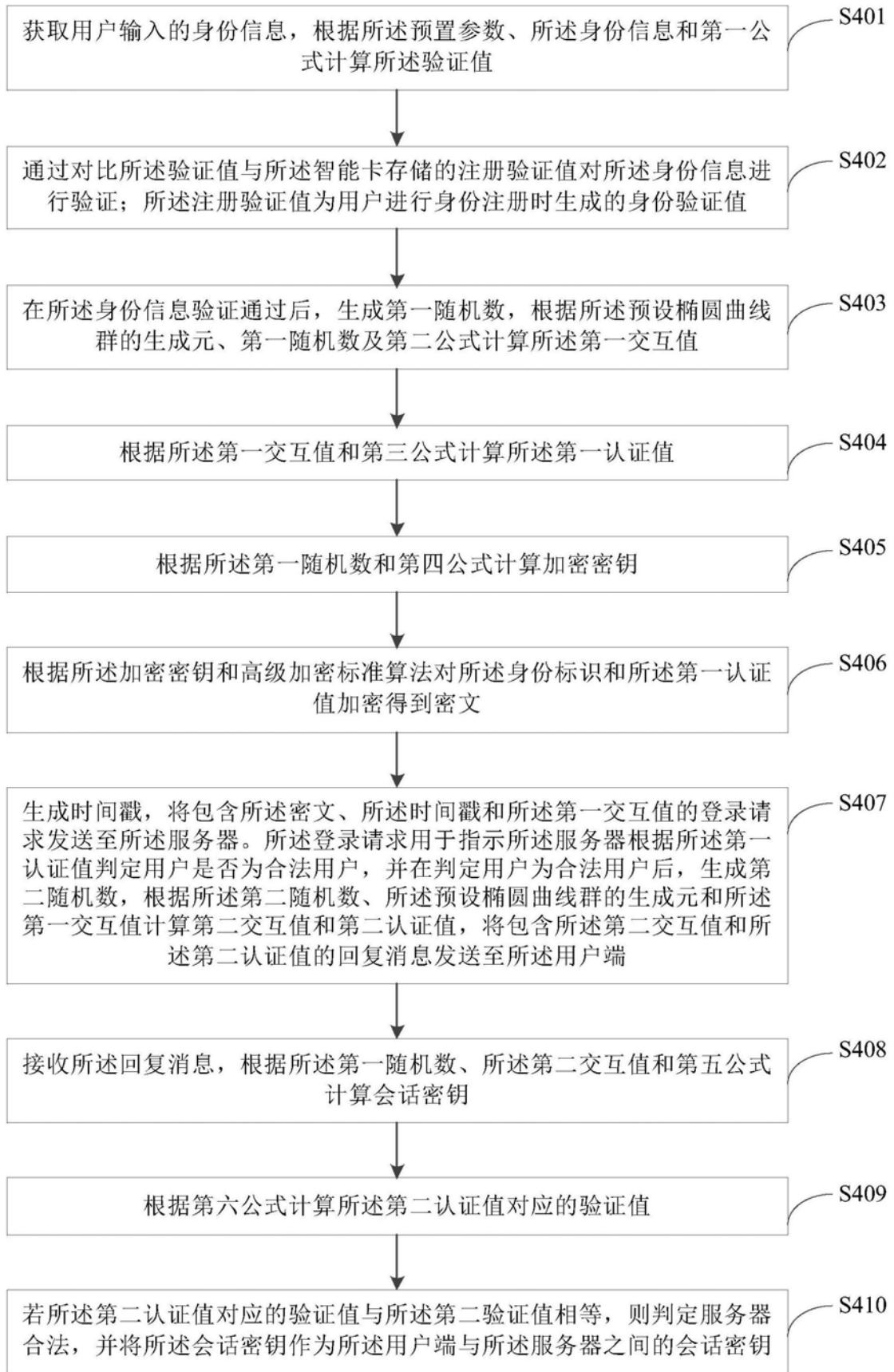


图4

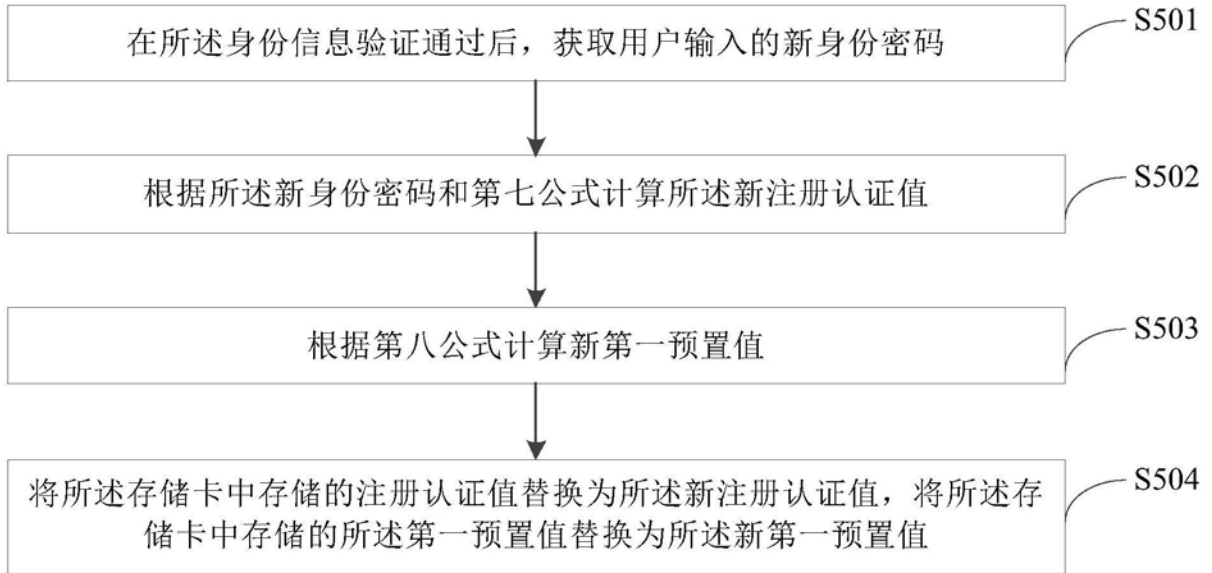


图5

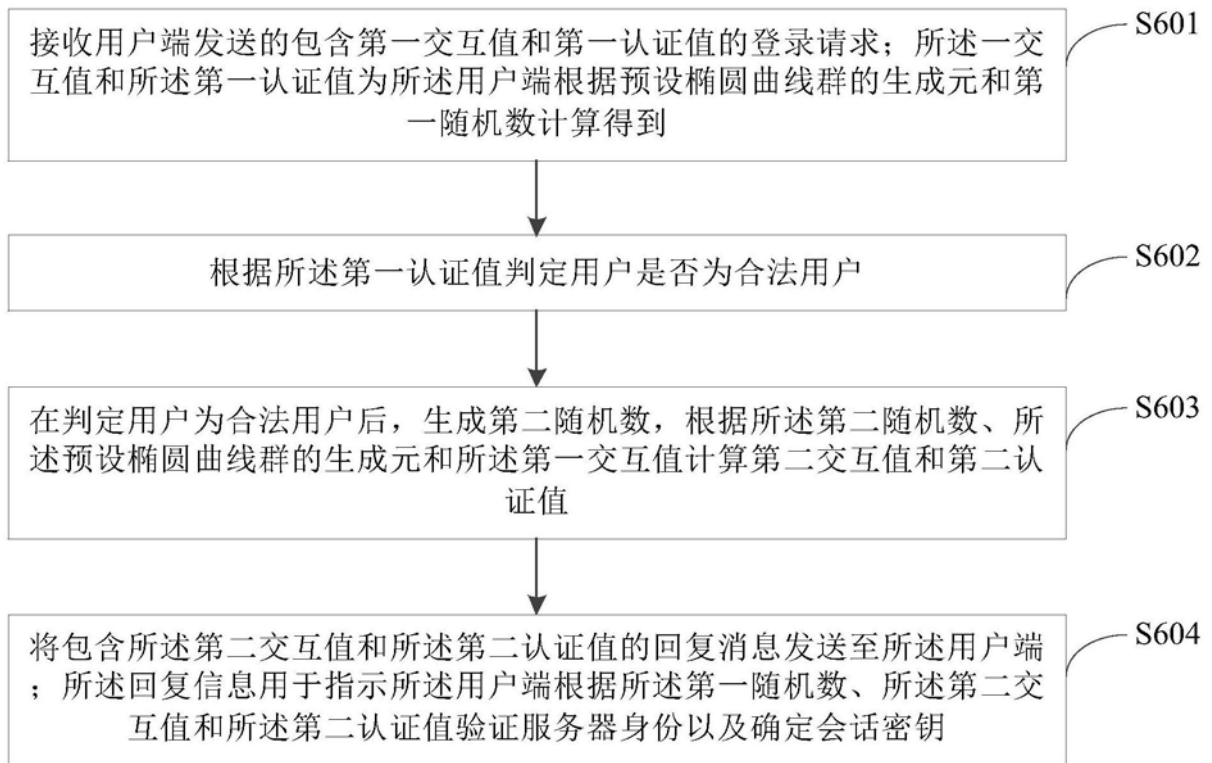


图6

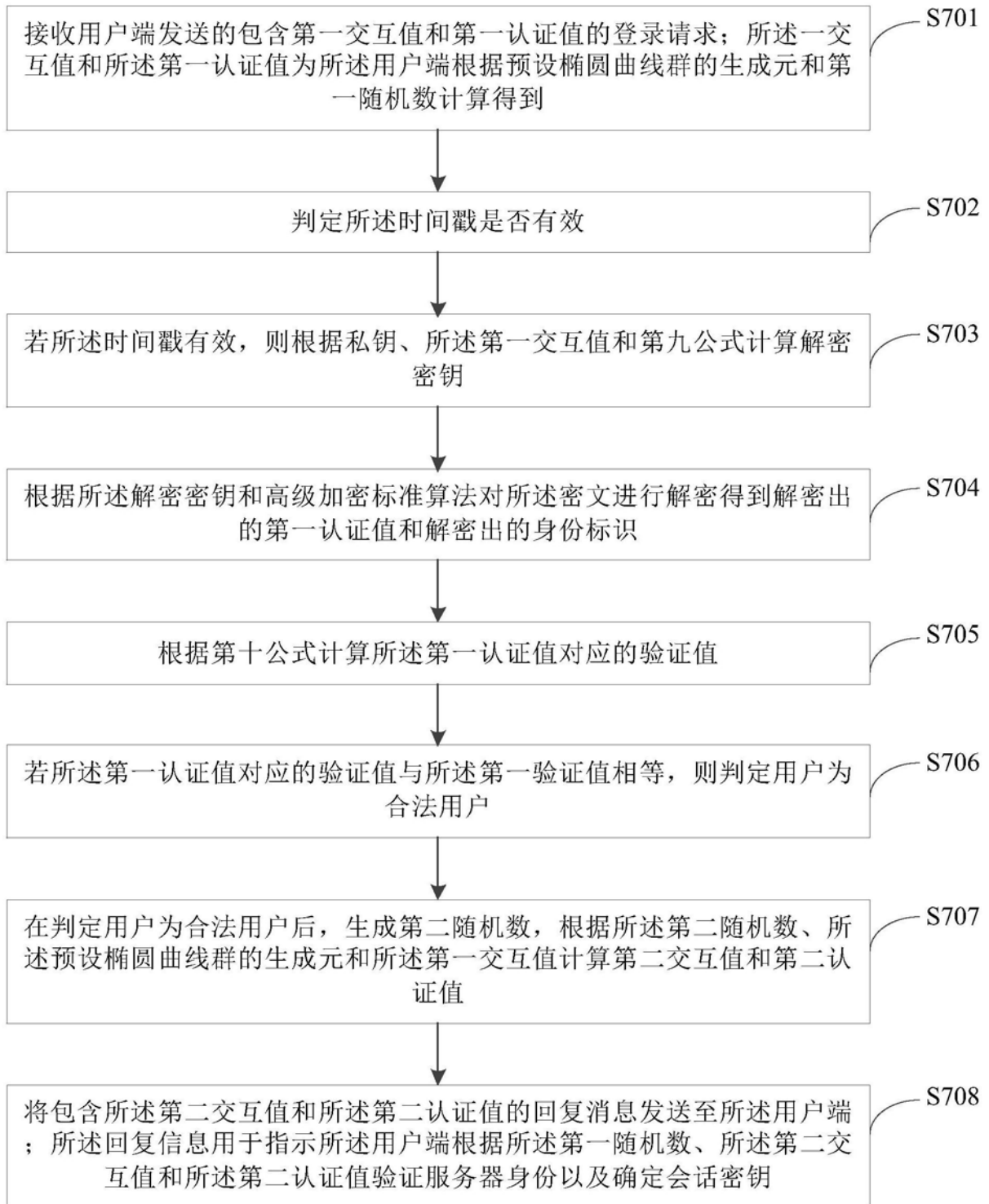


图7

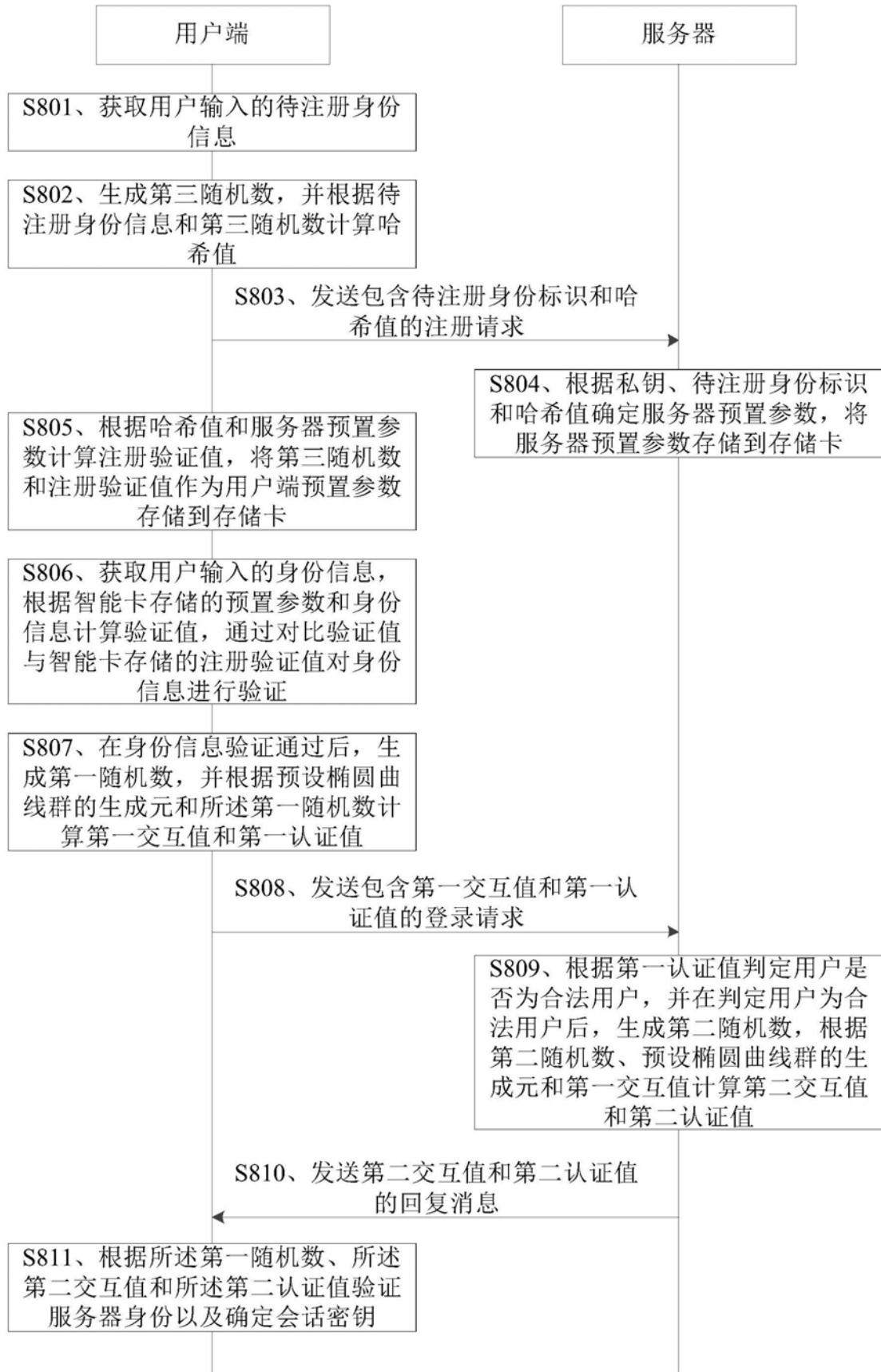


图8

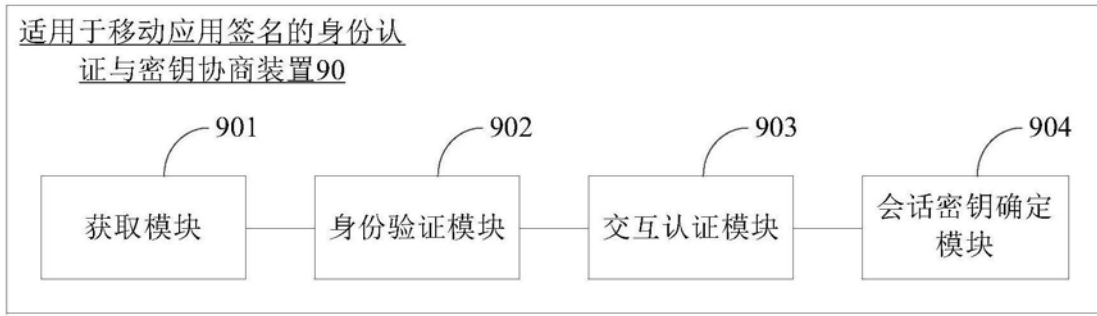


图9

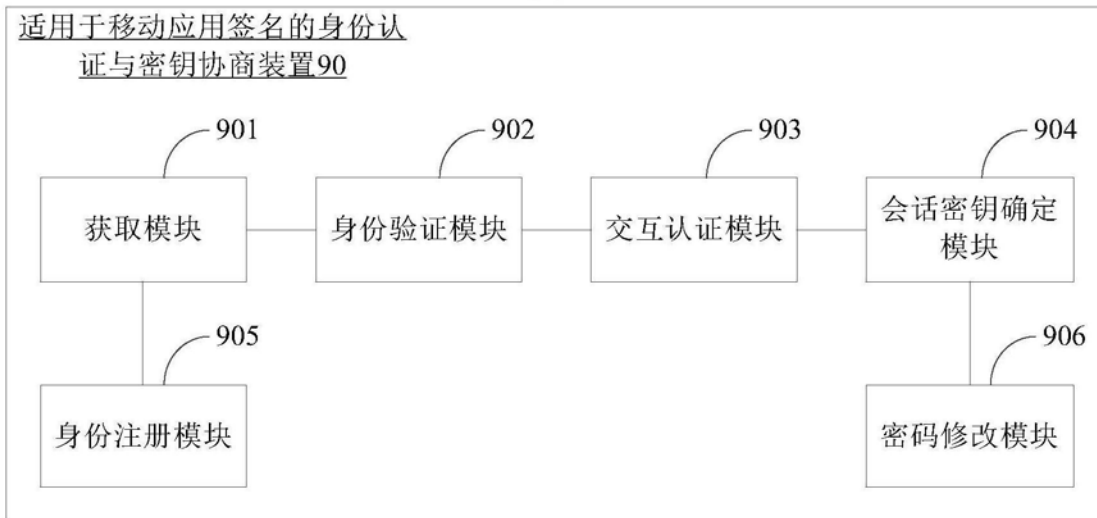


图10

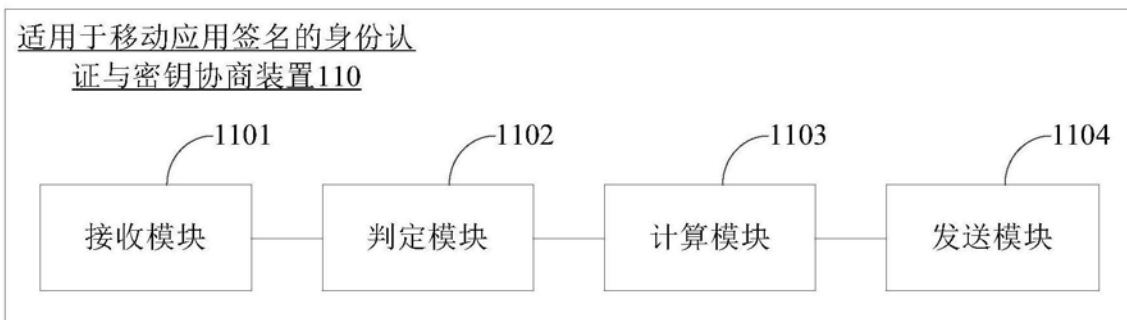


图11

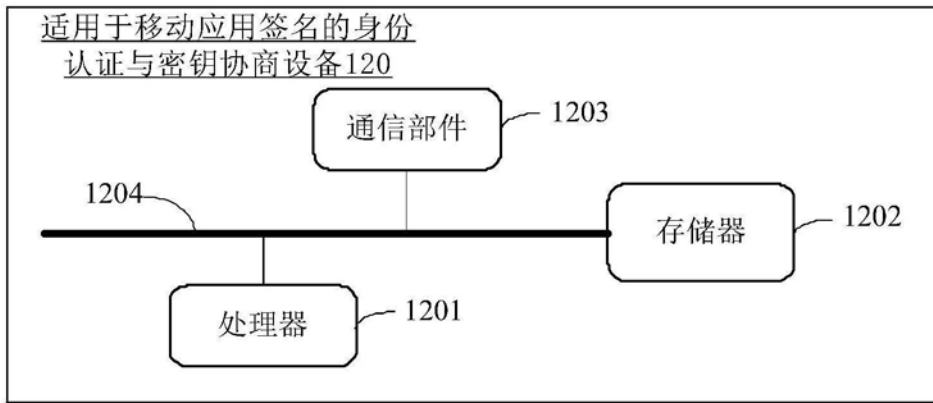


图12