



(12)发明专利申请

(10)申请公布号 CN 108564361 A

(43)申请公布日 2018.09.21

(21)申请号 201810394687.X

(22)申请日 2018.04.27

(71)申请人 北京华大智宝电子系统有限公司

地址 100015 北京市朝阳区高家园一号

(72)发明人 周飞

(74)专利代理机构 北京集佳知识产权代理有限公司

公司 11227

代理人 王雪 王宝筠

(51)Int.Cl.

G06Q 20/32(2012.01)

G06Q 20/40(2012.01)

H04L 29/06(2006.01)

H04W 12/06(2009.01)

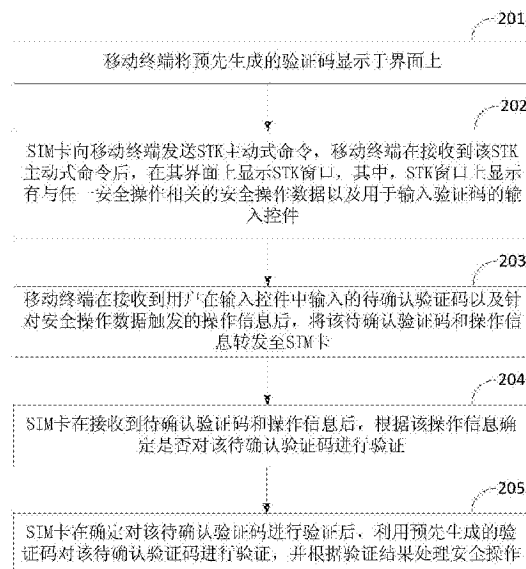
权利要求书2页 说明书11页 附图6页

(54)发明名称

一种信息处理方法、装置及设备

(57)摘要

本发明公开一种信息处理方法、装置及设备,所述方法包括:装在移动终端上的SIM卡通过STK主动式命令在移动终端的界面上显示STK窗口,该STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;SIM卡接收到移动终端从输入控件中获取到的待确认验证码以及针对安全操作数据触发的操作信息后,根据操作信息确定是否对待确认验证码进行验证;SIM卡在确定对待确认验证码进行验证后,利用预先生成的验证码对待确认验证码进行验证,并根据验证结果处理安全操作。所以,本申请通过在处理安全操作的过程中增加用户输入随机的验证码的方式来防止他人通过伪造确认信息的方式对用户信息安全造成威胁,一定程度上保证了用户信息的安全性,也提高了安全操作的安全性。



1. 一种信息处理方法,其特征在于,所述方法应用于安装在移动终端上的SIM卡,所述方法包括:

所述SIM卡通过STK主动式命令在所述移动终端的界面上显示STK窗口,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

所述SIM卡接收到所述移动终端从所述输入控件中获取到的待确认验证码以及针对所述安全操作数据触发的操作信息后,根据所述操作信息确定是否对所述待确认验证码进行验证;

所述SIM卡在确定对所述待确认验证码进行验证后,利用预先生成的验证码对所述待确认验证码进行验证,并根据验证结果处理所述安全操作。

2. 根据权利要求1所述的方法,其特征在于,所述SIM卡通过STK主动式命令在所述移动终端的界面上显示STK窗口之前,还包括:

所述SIM卡与所述移动终端建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

3. 根据权利要求2所述的方法,其特征在于,所述利用预先生成的验证码对所述待确认验证码进行验证之前,还包括:

基于所述安全连接,所述SIM卡与所述移动终端通过预设算法生成验证码,所述验证码用于对所述待确认验证码进行验证。

4. 根据权利要求1所述的方法,其特征在于,所述根据所述操作信息确定是否对所述待确认验证码进行验证,包括:

如果所述操作信息为确定信息,则所述SIM卡确定对所述待确定验证码进行验证;

相应的,所述利用预先生成的验证码对所述待确认验证码进行验证,并根据验证结果处理所述安全操作,包括:

所述SIM卡将预先生成的验证码与所述待确认验证码进行匹配,如果匹配成功,则执行所述安全操作;否则,终止所述安全操作。

5. 根据权利要求1所述的方法,其特征在于,所述根据所述操作信息确定是否对所述待确认验证码进行验证,包括:

如果所述操作信息为取消信息,则所述SIM卡确定对所述待确认验证码不进行验证;

相应的,所述方法还包括:

如果所述SIM卡确定对所述待确认验证码不进行验证,则终止所述安全操作。

6. 一种信息处理方法,其特征在于,所述方法应用于安装有SIM卡的移动终端,所述方法包括:

所述移动终端将预先生成的验证码显示于界面上,以及在接收到来自所述SIM卡的STK主动式命令后,在界面上显示STK窗口;其中,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

所述移动终端在接收到所述输入控件中的待确认验证码以及针对所述安全操作数据触发的操作信息后,将所述待确认验证码和所述操作信息转发至所述SIM卡,以便所述SIM卡根据所述操作信息确定是否对所述待确认验证码进行验证,以及根据验证结果处理所述安全操作。

7. 根据权利要求6所述的方法,其特征在于,所述移动终端将预先生成的验证码显示于

界面上,以及在接收到来自所述SIM卡的STK主动式命令后,在界面上显示STK窗口之前,还包括:

所述移动终端与所述SIM卡建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

8.根据权利要求7所述的方法,其特征在于,所述移动终端将预先生成的验证码显示于界面上之前,还包括:

基于所述安全连接,所述移动终端与所述SIM卡通过预设算法生成验证码,所述验证码用于对所述待确认验证码进行验证。

9.根据权利要求6所述的方法,其特征在于,所述移动终端将预先生成的验证码显示于界面上之前,还包括:

所述移动终端对预先生成的验证码进行处理后,得到处理后验证码;

相应的,所述移动终端将预先生成的验证码显示于界面上,具体为:

所述移动终端将所述处理后验证码显示于界面上。

10.一种信息处理装置,其特征在于,所述装置应用于安装在移动终端上的SIM卡,所述装置包括:

命令发送单元,用于向所述移动终端发送STK主动式命令,以便在所述移动终端的界面上显示STK窗口,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

确定单元,用于接收到所述移动终端从所述输入控件中获取到的待确认验证码以及针对所述安全操作数据触发的操作信息后,根据所述操作信息确定是否对所述待确认验证码进行验证;

验证及处理单元,用于在确定对所述待确认验证码进行验证后,利用预先生成的验证码对所述待确认验证码进行验证,并根据验证结果处理所述安全操作。

11.一种信息处理装置,其特征在于,所述装置应用于安装有SIM卡的移动终端,所述装置包括:

显示单元,用于将预先生成的验证码显示于界面上,以及在接收到来自所述SIM卡的STK主动式命令后,在界面上显示STK窗口;其中,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

转发单元,用于在接收到所述输入控件中的待确认验证码以及针对所述安全操作数据触发的操作信息后,将所述待确认验证码和所述操作信息转发至所述SIM卡,以便所述SIM卡根据所述操作信息确定是否对所述待确认验证码进行验证,以及根据验证结果处理所述安全操作。

一种信息处理方法、装置及设备

技术领域

[0001] 本申请涉及数据处理领域,具体涉及一种信息处理方法、装置及设备。

背景技术

[0002] 现有的手机SIM(Subscriber Identity Module,客户识别模块)卡可以支持各种安全应用的装载,可以通过安全应用提供数字签名、加解密等安全功能。由于SIM卡不存在显示设备和物理按键,所以,在提供上述安全功能时一般采用STK(SIM Card Tool Kit,用户识别应用发展工具)的主动式命令实现信息的显示以及物理按键的“确认”和“取消”按键。

[0003] 但是,由于采用STK的主动式命令实现信息的显示和物理按键功能是依赖于手机系统内置应用来实现的,一旦手机系统被强行提升权限(通常称为root),则恶意软件有机会伪装成手机系统内置应用处理信息的显示和物理按键功能,使得本应弹出STK窗口由用户进行信息确认的步骤被恶意软件篡改,对用户的信息安全造成威胁。

发明内容

[0004] 有鉴于此,本申请实施例提供一种信息处理方法、装置及设备,以解决现有技术中用户的信息存在安全风险的问题。

[0005] 为解决上述问题,本申请实施例提供的技术方案如下:

[0006] 第一方面,本申请提供了一种信息处理方法,应用于安装在移动终端上的SIM卡,该方法包括:

[0007] 所述SIM卡通过STK主动式命令在所述移动终端的界面上显示STK窗口,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

[0008] 所述SIM卡接收到所述移动终端从所述输入控件中获取到的待确认验证码以及针对所述安全操作数据触发的操作信息后,根据所述操作信息确定是否对所述待确认验证码进行验证;

[0009] 所述SIM卡在确定对所述待确认验证码进行验证后,利用预先生成的验证码对所述待确认验证码进行验证,并根据验证结果处理所述安全操作。

[0010] 在一种可选的实现方式中,所述SIM卡通过STK主动式命令在所述移动终端的界面上显示STK窗口之前,还包括:

[0011] 所述SIM卡与所述移动终端建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

[0012] 在一种可选的实现方式中,所述利用预先生成的验证码对所述待确认验证码进行验证之前,还包括:

[0013] 基于所述安全连接,所述SIM卡与所述移动终端通过预设算法生成验证码,所述验证码用于对所述待确认验证码进行验证。

[0014] 在一种可选的实现方式中,所述根据所述操作信息确定是否对所述待确认验证码

进行验证,包括:

[0015] 如果所述操作信息为确定信息,则所述SIM卡确定对所述待确定验证码进行验证;

[0016] 相应的,所述利用预先生成的验证码对所述待确认验证码进行验证,并根据验证结果处理所述安全操作,包括:

[0017] 所述SIM卡将预先生成的验证码与所述待确认验证码进行匹配,如果匹配成功,则执行所述安全操作;否则,终止所述安全操作。

[0018] 在一种可选的实现方式中,所述根据所述操作信息确定是否对所述待确认验证码进行验证,包括:

[0019] 如果所述操作信息为取消信息,则所述SIM卡确定对所述待确认验证码不进行验证;

[0020] 相应的,所述方法还包括:

[0021] 如果所述SIM卡确定对所述待确认验证码不进行验证,则终止所述安全操作。

[0022] 第二方面,本申请提供了一种信息处理方法,应用于安装有SIM卡的移动终端,该方法包括:

[0023] 所述移动终端将预先生成的验证码显示于界面上,以及在接收到来自所述SIM卡的STK主动式命令后,在界面上显示STK窗口;其中,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

[0024] 所述移动终端在接收到所述输入控件中的待确认验证码以及针对所述安全操作数据触发的操作信息后,将所述待确认验证码和所述操作信息转发至所述SIM卡,以便所述SIM卡根据所述操作信息确定是否对所述待确认验证码进行验证,以及根据验证结果处理所述安全操作。

[0025] 在一种可选的实现方式中,所述移动终端将预先生成的验证码显示于界面上,以及在接收到来自所述SIM卡的STK主动式命令后,在界面上显示STK窗口之前,还包括:

[0026] 所述移动终端与所述SIM卡建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

[0027] 在一种可选的实现方式中,所述移动终端将预先生成的验证码显示于界面上之前,还包括:

[0028] 基于所述安全连接,所述移动终端与所述SIM卡通过预设算法生成验证码,所述验证码用于对所述待确认验证码进行验证。

[0029] 在一种可选的实现方式中,所述移动终端将预先生成的验证码显示于界面上之前,还包括:

[0030] 所述移动终端对预先生成的验证码进行处理后,得到处理后验证码;

[0031] 相应的,所述移动终端将预先生成的验证码显示于界面上,具体为:

[0032] 所述移动终端将所述处理后验证码显示于界面上。

[0033] 第三方面,本申请提供了一种信息处理装置,所述装置应用于安装在移动终端上的SIM卡,所述装置包括:

[0034] 命令发送单元,用于向所述移动终端发送STK主动式命令,以便在所述移动终端的界面上显示STK窗口,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

[0035] 确定单元,用于接收到所述移动终端从所述输入控件中获取到的待确认验证码以及针对所述安全操作数据触发的操作信息后,根据所述操作信息确定是否对所述待确认验证码进行验证;

[0036] 验证及处理单元,用于在确定对所述待确认验证码进行验证后,利用预先生成的验证码对所述待确认验证码进行验证,并根据验证结果处理所述安全操作。

[0037] 在一种可选的实现方式中,所述装置还包括:

[0038] 安全连接建立单元,用于与所述移动终端建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

[0039] 在一种可选的实现方式中,所述装置还包括:

[0040] 生成单元,用于基于所述安全连接,与所述移动终端通过预设算法生成验证码,所述验证码用于对所述待确认验证码进行验证。

[0041] 在一种可选的实现方式中,所述确定单元包括:

[0042] 第一确定子单元,用于如果所述操作信息为确定信息,则确定对所述待确定验证码进行验证;

[0043] 相应的,所述验证及处理单元包括:

[0044] 匹配子单元,用于将预先生成的验证码与所述待确认验证码进行匹配,如果匹配成功,则执行所述安全操作;否则,终止所述安全操作。

[0045] 在一种可选的实现方式中,所述确定单元包括:

[0046] 第二确定子单元,用于如果所述操作信息为取消信息,则确定对所述待确认验证码不进行验证;

[0047] 相应的,所述装置还包括:

[0048] 终止单元,用于如果确定对所述待确认验证码不进行验证,则终止所述安全操作。

[0049] 第四方面,本申请提供了一种信息处理装置,所述装置应用于安装有SIM卡的移动终端,所述装置包括:

[0050] 显示单元,用于将预先生成的验证码显示于界面上,以及在接收到来自所述SIM卡的STK主动式命令后,在界面上显示STK窗口;其中,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

[0051] 转发单元,用于在接收到所述输入控件中的待确认验证码以及针对所述安全操作数据触发的操作信息后,将所述待确认验证码和所述操作信息转发至所述SIM卡,以便所述SIM卡根据所述操作信息确定是否对所述待确认验证码进行验证,以及根据验证结果处理所述安全操作。

[0052] 在一种可选的实现方式中,所述装置还包括:

[0053] 安全连接建立单元,用于与所述SIM卡建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

[0054] 在一种可选的实现方式中,所述装置还包括:

[0055] 生成单元,用于基于所述安全连接,与所述SIM卡通过预设算法生成验证码,所述验证码用于对所述待确认验证码进行验证。

[0056] 在一种可选的实现方式中,所述装置还包括:

[0057] 处理单元,用于对预先生成的验证码进行处理后,得到处理后验证码;

[0058] 相应的,所述显示单元包括:

[0059] 第一显示子单元,用于将所述处理后验证码显示于界面上。

[0060] 第五方面,本申请提供了一种信息处理设备,所述设备包括存储器和处理器,

[0061] 所述存储器用于存储程序代码,并将所述程序代码传输给所述处理器;

[0062] 所述处理器用于根据所述程序代码中的指令,执行上述第一方面和第二方面提供的任一项所述的信息处理方法。

[0063] 在本申请中,安装在移动终端上的SIM卡通过STK主动式命令在移动终端的界面上显示STK窗口,其中,STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;接着,SIM卡在接收到移动终端从输入控件中获取到的待确认验证码以及针对安全操作数据触发的操作信息后,根据该操作信息确定是否需要对该待确认验证码进行验证;在确定需要对待确认验证码进行验证后,SIM卡利用预先生成的验证码对待确认验证码进行验证,并根据验证结果处理安全操作。因此,本申请通过在处理安全操作的过程中增加用户输入随机的验证码的方法来防止他人通过伪造确认信息的方式对用户信息安全造成威胁,一定程度上保证了用户信息的安全性,也提高了安全操作的安全性。

附图说明

[0064] 为了更清楚地说明本申请实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请的一些实施例,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。

[0065] 图1为本申请实施例提供的示例性应用场景的框架示意图;

[0066] 图2为本申请实施例提供了一种信息处理方法实施例的流程图;

[0067] 图3为本申请实施例提供的App通过安全连接通道与Applet协商验证码的方法的交互流程图;

[0068] 图4为本申请实施例提供了一种验证码显示方式的示意图;

[0069] 图5为本申请实施例提供的信息处理方法实施例的交互流程图;

[0070] 图6为本申请实施例提供了一种信息处理装置的结构示意图之一;

[0071] 图7为本申请实施例提供了一种信息处理装置的结构示意图之二;

[0072] 图8为本申请实施例提供一种信息处理设备的结构示意图。

具体实施方式

[0073] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,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,都属于本申请保护的范围。

[0074] 为了便于理解本申请提供的技术方案,下面先对本申请在实际中的应用场景进行介绍。

[0075] 参见图1,为本申请在实际应用中的场景示例图,如图1所示,本申请提供的信息处理方法可以在安装了SIM卡101的移动终端102中得以实现;其中,SIM卡101也称用户身份识

别卡、智能卡,实际是装有微处理器的芯片卡,其内部存储了数字移动电话客户的信息,加密的密钥以及用户的电话簿等内容,可供全球移动通信系统(Global System for Mobile Communication,GSM)网络客户身份进行鉴别,并对客户通话时的语音信息进行加密。如手机中安装的手机卡、银行卡内置的SIM芯片等;移动终端102是指可以在移动中使用的计算机设备,能够安装SIM卡和客户端等,并正在从简单的通话工具变为一个综合信息处理平台,如具有多种应用功能的智能手机以及平板电脑等。

[0076] 如图1所示,在实际应用中,当用户在移动终端102上触发了任一安全操作时,比如通过移动终端进行转账或者缴费等,移动终端将该安全操作的类型发送给SIM卡,本申请利用安装在移动终端102上的SIM卡101向移动终端102发送STK主动式命令,移动终端将预先生成的验证码显示于界面上,在接收到STK主动式命令后,在其界面上显示包含安全操作数据以及输入控件的STK窗口103。接着,移动终端102将从输入控件中获取用户输入的待确认验证码以及针对安全操作数据触发的操作信息,并发送至SIM卡101,以便于SIM卡101根据该操作信息确定是否对该待确认验证码进行验证,进而根据验证结果处理该安全操作。

[0077] 可见,本申请提供的该方法在处理安全操作的过程中增加了用户输入随机的验证码进行检验,防止了他人伪造用户的确认信息,提高了交易的安全性。

[0078] 基于以上应用场景,本申请实施例提供了一种信息处理方法,以下将结合附图对该方法进行详细说明。

[0079] 参见图2,其示出了本申请实施例提供的一种信息处理方法的流程图,该方法可以应用于安装在移动终端上的SIM卡,如图2所示,该方法包括:

[0080] 步骤201:移动终端将预先生成的验证码显示于界面上。

[0081] 步骤202:SIM卡向移动终端发送STK主动式命令,移动终端在接收到该STK主动式命令后,在其界面上显示STK窗口,其中,STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件。

[0082] 在实际应用中,当用户需要利用移动终端上安装的应用程序进行交易签名时,为了确保用户交易的安全性,往往需要通过SIM卡和移动终端的交互,来验证用户身份的真实性,实现安全交易。在本申请中的SIM卡指的是支持多种通信通道的SIM卡,例如蓝牙SIM卡等。在SIM卡和移动终端的交互过程中,SIM卡响应于用户在移动终端上触发的安全操作,例如,用户利用移动终端上安装的手机银行应用程序(Application,简称App)进行转账交易时,用户需要在终端界面上触发转账交易按钮这一安全操作来实现转账交易,一旦SIM卡获知安全操作被触发后,首先向移动终端发送STK主动式命令,其中,STK命令是一种SIM卡与移动终端的交互指令,而SIM卡向移动终端发送STK主动式命令指的是通过该STK主动式命令,SIM卡可以指示移动终端执行显示STK窗口的行为,在STK窗口上显示有与用户任一安全操作相关的安全操作数据,其中,安全操作是指涉及用户安全信息的操作,如转账等,与用户任一安全操作相关的安全操作数据指的是与该安全操作相关的需要用户进行交易签名的操作数据,例如,用户利用某银行的手机App进行转账交易时,在需要用户进行交易签名的界面,显示本次交易相关的操作数据,如用户转入转出的银行卡信息、交易金额等,都属于与用户对这一转账交易进行交易签名时的相关的安全操作数据。

[0083] 在步骤201中,移动终端将预先生成的验证码显示于界面上,其中,预先生成的验证码是当App需要进行安全操作时,为了验证用户身份,而与SIM卡共同协商出来并通过安

全的方式显示在移动终端界面上的,在本申请中,移动终端终端界面上的STK窗口不仅显示有与任一安全操作相关的安全操作数据,还显示有用于用户输入验证码的输入控件,用户可以根据预先生成并经过处理后显示在移动终端界面上的验证码,在STK窗口的验证码的输入控件中输入待确认验证码,以便于对用户身份的确认。

[0084] 上述步骤202中,在SIM卡向移动终端发送STK主动式命令,以使移动终端在其界面上显示STK窗口之前,本申请还提供了一种可选的实施方式是:

[0085] SIM卡与移动终端建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

[0086] 在具体实现过程中,为了确保SIM卡与移动终端之间的安全通信,在二者之间建立了一个安全连接。基于该安全连接,安装于移动终端上的需要使用SIM卡来完成安全操作的App能够与SIM卡内安装的安全应用Applet进行安全通信。其中,Applet指的是安装在SIM卡上的安全应用,用于接收上位机指令来完成安全操作,并可通过STK主动式命令与移动终端配合完成安全操作信息的展示并获取响应。

[0087] 在建立该安全连接的过程中,首先,移动终端通过其他通道,比如蓝牙、近距离无线通信技术(Near Field Communication,NFC)等,连接到SIM卡,然后,基于该连接,App与Applet之间协商一个信道密钥,并利用该信道密钥对二者之间通信的往来指令进行加密,以便于后续对二者之间通信指令均采用该信道密钥加密后传输,从而在二者之间建立了一个安全连接,进而实现了SIM卡与移动终端之间的安全通信。

[0088] 在SIM卡与移动终端建立安全连接后,为了验证用户身份,本申请还提供了一种可选的实施方式是:

[0089] 基于上述安全连接,SIM卡与移动终端通过预设算法生成验证码,该验证码用于对待确认验证码进行验证。

[0090] 在具体实现过程中,为了验证用户的身份,安装于移动终端上的需要使用SIM卡来完成安全操作的App通过该安全连接通道与Applet进行协商,通过预设算法预先生成验证码,并对该校验码进行安全处理并显示在移动终端的界面上,用于对用户输入的待确认验证码进行验证。

[0091] App通过安全连接通道与Applet协商验证码的方法较多,在此,本申请提供了一种预先生成验证码的方法,具体为:首先,当SIM卡查询到App的当前安全操作指令为交易签名,安全操作的方法是要求通过STK窗口显示关键数据并校验验证码时,Applet内计算随机数R1,并返回特定响应码;App收到该响应码后,生成随机数R2,使用R1对R2进行加密得到密文C1,然后将C1通过验证码协商指令发送给Applet。同时通过特定算法Calc(R1,R2)得到4位验证码M1;Applet接收到C1后,通过R1解密,得到R2,再通过特定的算法Calc(R1,R2)得到4位数字验证码M1,保存在SIM卡中。同时,App通过安全的方式将验证码M1显示在移动终端的界面上。

[0092] 为了便于理解上述生成验证码的方法,参见图3所示,其示出了本申请实施例提供的App通过安全连接通道与Applet协商验证码的方法的交互过程示意图,可以包括以下步骤:

[0093] 步骤301:当SIM卡查询到App的当前安全操作指令为交易签名,SIM卡将查询安全操作列表,以确认交易签名是否需要生成验证码,如需要生成验证码,则SIM卡中安全应用

Applet计算随机数R1。

[0094] 在实际应用中, SIM卡中预先存储有安全操作列表, 且该表中记载了哪些安全操作类型对应需要生成验证码进行用户信息的安全性的验证, 以及哪些安全操作类型不需要生成验证码进行验证, 例如, 若用户触发的安全操作类型为“转账”, 则在安全操作列表中, 可能记载有“转账”是需要生成验证码进行用户信息安全性的验证的; 若用户触发的安全操作类型为“查询”, 则在安全操作列表中, 可能记载了“查询”是不需要生成验证码进行用户信息安全性的验证的。也就是说, SIM卡中存储的安全操作列表记载了用户触发的不同安全操作类型对应的是否需要生成验证码进行用户信息的安全性验证的关系, 具体的安全操作列表可以根据应用需求进行设置。

[0095] 步骤302: Applet将特定响应码返回至App, 此响应码可告知APP当前安全操作需要验证码进行验证, 且该响应码包含R1。

[0096] 步骤303: App收到响应码后, 生成随机数R2, 使用R1对R2进行加密得到密文C1, 同时通过特定算法Calc (R1, R2) 得到4位验证码M1。

[0097] 步骤304: App将C1通过验证码协商指令发送至Applet。

[0098] 步骤305: Applet接收到C1后, 通过R1解密, 得到R2, 再通过特定的算法Calc (R1, R2) 得到4位数字验证码M1, 保存在SIM卡中。

[0099] 步骤306: App通过安全的方式将验证码M1显示在移动终端的界面上。

[0100] 需要说明的是, 上述步骤303和步骤304是同时进行的, 没有先后顺序的区分, 同理, 步骤305和步骤306也同样没有执行顺序的先后区分, 可同时进行。

[0101] 对于上述步骤306中安全的方式, 本申请提出了一种可选的实施方式是, 通过移动终端对预先生成的验证码进行处理后, 得到处理后验证码。则相应的, 所述移动终端将预先生成的验证码显示于界面上, 具体为: 所述移动终端将所述处理后验证码显示于界面上。其中, 对预先生成的验证码进行处理可以包含多种形式, 比如将其转换成图片、图片加扰、转换为数学题等各种方式展示验证码。

[0102] 举例说明, 如图4所示, 假设本申请预先生成验证码为数字5时, 移动终端可将其转换为数学题的方式进行展示, 如在界面上将预先生成的验证码显示为: $3+2=?$ 。

[0103] 利用上述方法, 在SIM卡与移动终端之间建立了安全连接, 基于该安全连接, SIM卡与移动终端通过预设算法生成了验证码, 并且移动终端对该验证码进行处理后, 显示于界面上, 用于对用户输入的待确认验证码进行验证。因此, 本申请中基于该安全连接实现的验证码校验方法使得他人无法通过伪造用户确认信息的方式对用户信息安全造成威胁, 一定程度上保证了用户信息的安全。

[0104] 当用户触发操作信息以及将待确认的验证码输入到移动终端的STK显示窗口后, 执行步骤203。

[0105] 步骤203: 移动终端在接收到用户在输入控件中输入的待确认验证码以及针对安全操作数据触发的操作信息后, 将该待确认验证码和操作信息转发至SIM卡。

[0106] 步骤204: SIM卡在接收到待确认验证码和操作信息后, 根据该操作信息确定是否对该待确认验证码进行验证。

[0107] 在实际应用中, 用户根据显示于移动终端界面的验证码, 在输入控件中输入待确认验证码, 以及根据安全操作数据触发操作信息。当移动终端接收到用户在其界面上输入

的待确认验证码以及针对安全操作数据触发的操作信息后,立即将二者转发至SIM卡,而SIM卡在接收到待确认验证码和操作信息后,首先要对用户的操作信息进行判断,再根据判断结果来确定是否需要对待确认验证码进行验证。

[0108] 其中,针对SIM卡对用户的操作信息的判断结果,提供了如下两种可能的实现方式:

[0109] 一种可能的实现方式是,如果SIM卡判断出用户的操作信息为确定信息,则根据该确定信息,SIM卡确定需要对待确认验证码进行验证。

[0110] 另一种可能的实现方式是,如果SIM卡判断出用户的操作信息为取消信息,则根据该取消信息,SIM卡确定对待确认验证码不需要进行验证。例如,如图4所示,如果用户点击的是“取消”按钮,进行了取消转账的操作,则SIM卡判断出用户的操作信息为取消信息,进而不需要对用户输入的待确认验证码进行验证。

[0111] 在SIM卡确定需要对待确认验证码进行验证后,执行步骤205。

[0112] 步骤205:SIM卡在确定对该待确认验证码进行验证后,利用预先生成的验证码对该待确认验证码进行验证,并根据验证结果处理安全操作。

[0113] 在实际应用中,当SIM卡确定对该待确认验证码进行验证后,将利用步骤201中预先生成并保存在SIM卡中的验证码,对该待确认验证码进行验证,并根据该验证结果处理接下来的安全操作。

[0114] 其中,根据SIM卡对该待确认验证码进行验证的结果,处理接下来的安全操作的过程,本申请提供了一种可能的实现方式:

[0115] 如果SIM卡确定对该待确认验证码进行验证后,SIM卡将预先生成的验证码与所述待确认验证码进行匹配,如果匹配成功,则执行安全操作;否则,终止所述安全操作。

[0116] 举例说明,如图4所示,假设预先生成的验证码是数字5,如果SIM卡确定对该待确认验证码进行验证,则SIM卡将预先生成的验证码“5”与用户输入的待确认验证码进行匹配,若用户根据界面显示的验证码转换的数字题,将计算结果“5”作为待确认验证码输入控件,则可以和预先生成的验证码“5”匹配成功,进而可以执行该安全操作,否则,终止该安全操作。

[0117] 在本申请中,安装在移动终端上的SIM卡通过STK主动式命令在移动终端的界面上显示STK窗口,其中,STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;接着,SIM卡在接收到移动终端从输入控件中获取到的待确认验证码以及针对安全操作数据触发的操作信息后,根据该操作信息确定是否需要对该待确认验证码进行验证;在确定需要对待确认验证码进行验证后,SIM卡利用预先生成的验证码对待确认验证码进行验证,并根据验证结果处理安全操作。因此,本申请通过在处理安全操作的过程中增加用户输入随机的验证码的方式来防止他人伪造确认信息,提高了用户信息的安全性,也提高了安全操作的安全性。

[0118] 为了便于理解本申请,参见图5所示,其示出了本申请实施例提供的实现信息处理方法的交互过程示意图,可以包括以下步骤:

[0119] 步骤501:移动终端将预先生成的验证码显示于界面上。

[0120] 步骤502:SIM卡向移动终端发送STK主动式命令。

[0121] 步骤503:移动终端在接收到STK主动式命令后,在界面上显示STK窗口。

[0122] 步骤504:移动终端获取到用户在STK窗口中输入针对安全操作数据触发的操作信息和待确认验证码。

[0123] 步骤505:移动终端将待确认验证码和操作信息转发至SIM卡。

[0124] 步骤506:SIM卡接收到移动终端从输入控件中获取到的待确认验证码以及针对安全操作数据触发的操作信息后,根据操作信息确定是否对所述待确认验证码进行验证,如果是,进入步骤507,如果否,进入步骤509。

[0125] 步骤507:SIM卡利用预先生成的验证码验证待确认验证码是否正确,如果是,进入步骤508,如果否,进入步骤509。

[0126] 步骤508:SIM卡执行安全操作。

[0127] 步骤509:SIM卡终止安全操作。

[0128] 本申请实施例提供的实现信息处理方法,实现了用户在移动终端的App上的安全操作,同时在执行安全操作的过程中验证了用户身份信息,充分保证了用户信息的安全性,也提高了安全操作的安全性。

[0129] 参见图6所示,本申请还提供一种信息处理装置实施例,该装置包括:

[0130] 命令发送单元601,用于向所述移动终端发送STK主动式命令,以便在所述移动终端的界面上显示STK窗口,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

[0131] 确定单元602,用于接收到所述移动终端从所述输入控件中获取到的待确认验证码以及针对所述安全操作数据触发的操作信息后,根据所述操作信息确定是否对所述待确认验证码进行验证;

[0132] 验证及处理单元603,用于在确定对所述待确认验证码进行验证后,利用预先生成的验证码对所述待确认验证码进行验证,并根据验证结果处理所述安全操作。

[0133] 可选地,所述装置还包括:

[0134] 安全连接建立单元,用于与所述移动终端建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

[0135] 可选地,所述装置还包括:

[0136] 生成单元,用于基于所述安全连接,与所述移动终端通过预设算法生成验证码,所述验证码用于对所述待确认验证码进行验证。

[0137] 可选地,所述确定单元602包括:

[0138] 第一确定子单元,用于如果所述操作信息为确定信息,则确定对所述待确定验证码进行验证;

[0139] 相应的,所述验证及处理单元603包括:

[0140] 匹配子单元,用于将预先生成的验证码与所述待确认验证码进行匹配,如果匹配成功,则执行所述安全操作;否则,终止所述安全操作。

[0141] 可选地,所述确定单元602包括:

[0142] 第二确定子单元,用于如果所述操作信息为取消信息,则确定对所述待确认验证码不进行验证;

[0143] 相应的,所述装置还包括:

[0144] 终止单元,用于如果确定对所述待确认验证码不进行验证,则终止所述安全操作。

[0145] 参见图7所示,本申请还提供一种信息处理装置实施例,该装置包括:

[0146] 显示单元701,用于将预先生成的验证码显示于界面上,以及在接收到来自所述SIM卡的STK主动式命令后,在界面上显示STK窗口;其中,所述STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;

[0147] 转发单元702,用于在接收到所述输入控件中的待确认验证码以及针对所述安全操作数据触发的操作信息后,将所述待确认验证码和所述操作信息转发至所述SIM卡,以便所述SIM卡根据所述操作信息确定是否对所述待确认验证码进行验证,以及根据验证结果处理所述安全操作。

[0148] 可选地,所述装置还包括:

[0149] 安全连接建立单元,用于与所述SIM卡建立安全连接,其中,所述安全连接用于所述SIM卡与所述移动终端之间的安全通信。

[0150] 可选地,所述装置还包括:

[0151] 生成单元,用于基于所述安全连接,与所述SIM卡通过预设算法生成验证码,所述验证码用于对所述待确认验证码进行验证。

[0152] 可选地,所述装置还包括:

[0153] 处理单元,用于对预先生成的验证码进行处理后,得到处理后验证码;

[0154] 相应的,所述显示单元701包括:

[0155] 第一显示子单元,用于将所述处理后验证码显示于界面上。

[0156] 在本申请中,安装在移动终端上的SIM卡通过STK主动式命令在移动终端的界面上显示STK窗口,其中,STK窗口上显示有与任一安全操作相关的安全操作数据以及用于输入验证码的输入控件;接着,SIM卡在接收到移动终端从输入控件中获取到的待确认验证码以及针对安全操作数据触发的操作信息后,根据该操作信息确定是否需要对该待确认验证码进行验证;在确定需要对待确认验证码进行验证后,SIM卡利用预先生成的验证码对待确认验证码进行验证,并根据验证结果处理安全操作。因此,本申请通过在处理安全操作的过程中增加用户输入随机的验证码的方式来防止他人伪造确认信息,提高了用户信息的安全性,也提高了安全操作的安全性。

[0157] 相应的,本发明实施例还提供一种信息处理设备,参见图8所示,可以包括:

[0158] 处理器801、存储器802、输入装置803和输出装置804。信息处理设备中的处理器801的数量可以一个或多个,图8中以一个处理器为例。在本发明的一些实施例中,处理器801、存储器802、输入装置803和输出装置804可通过总线或其它方式连接,其中,图8中以通过总线连接为例。

[0159] 存储器802可用于存储软件程序以及模块,处理器801通过运行存储在存储器802的软件程序以及模块,从而执行信息处理设备的各种功能应用以及数据处理。存储器802可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序等。此外,存储器802可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。输入装置803可用于接收输入的数字或字符信息,以及产生与信息处理设备的用户设置以及功能控制有关的信号输入。

[0160] 具体在本实施例中,处理器801会按照如下的指令,将一个或一个以上的应用程序

的进程对应的可执行文件加载到存储器802中,并由处理器801来运行存储在存储器802中的应用程序,从而实现上述信息处理方法中的各种功能。

[0161] 对于装置实施例而言,由于其基本对应于方法实施例,所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[0162] 需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0163] 以上对本申请实施例所提供的一种信息处理方法、装置及设备进行了详细介绍,本文中应用了具体个例对本申请的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本申请的方法及其核心思想;同时,对于本领域的一般技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本申请的限制。

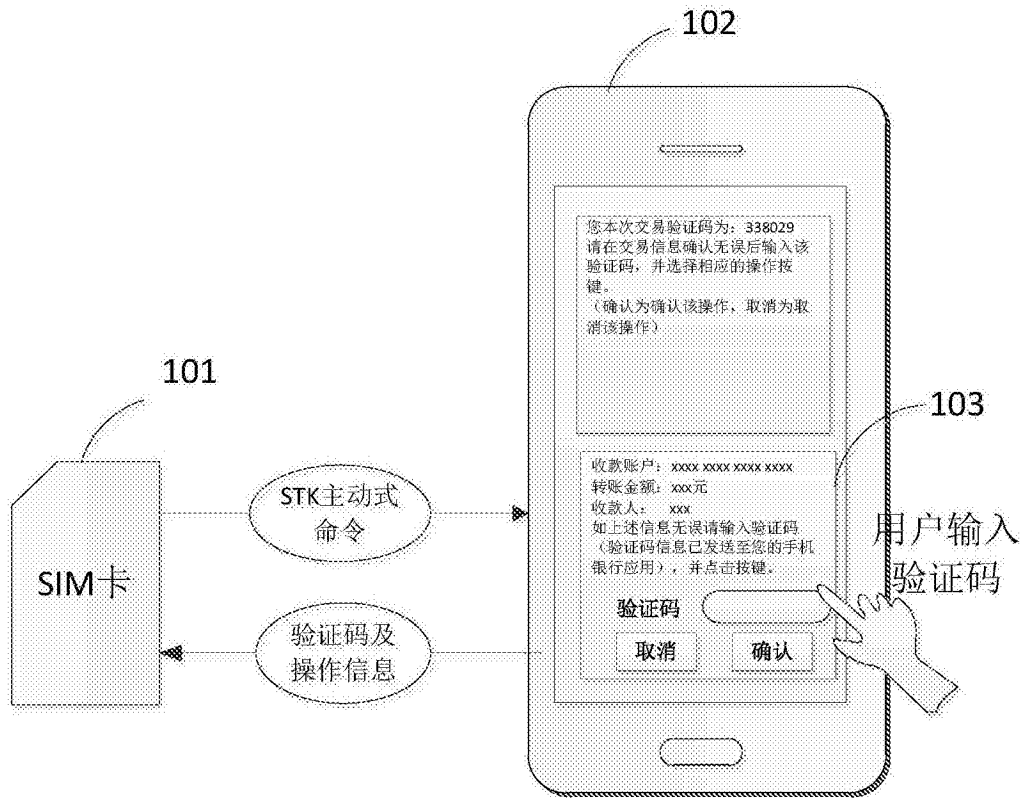


图1

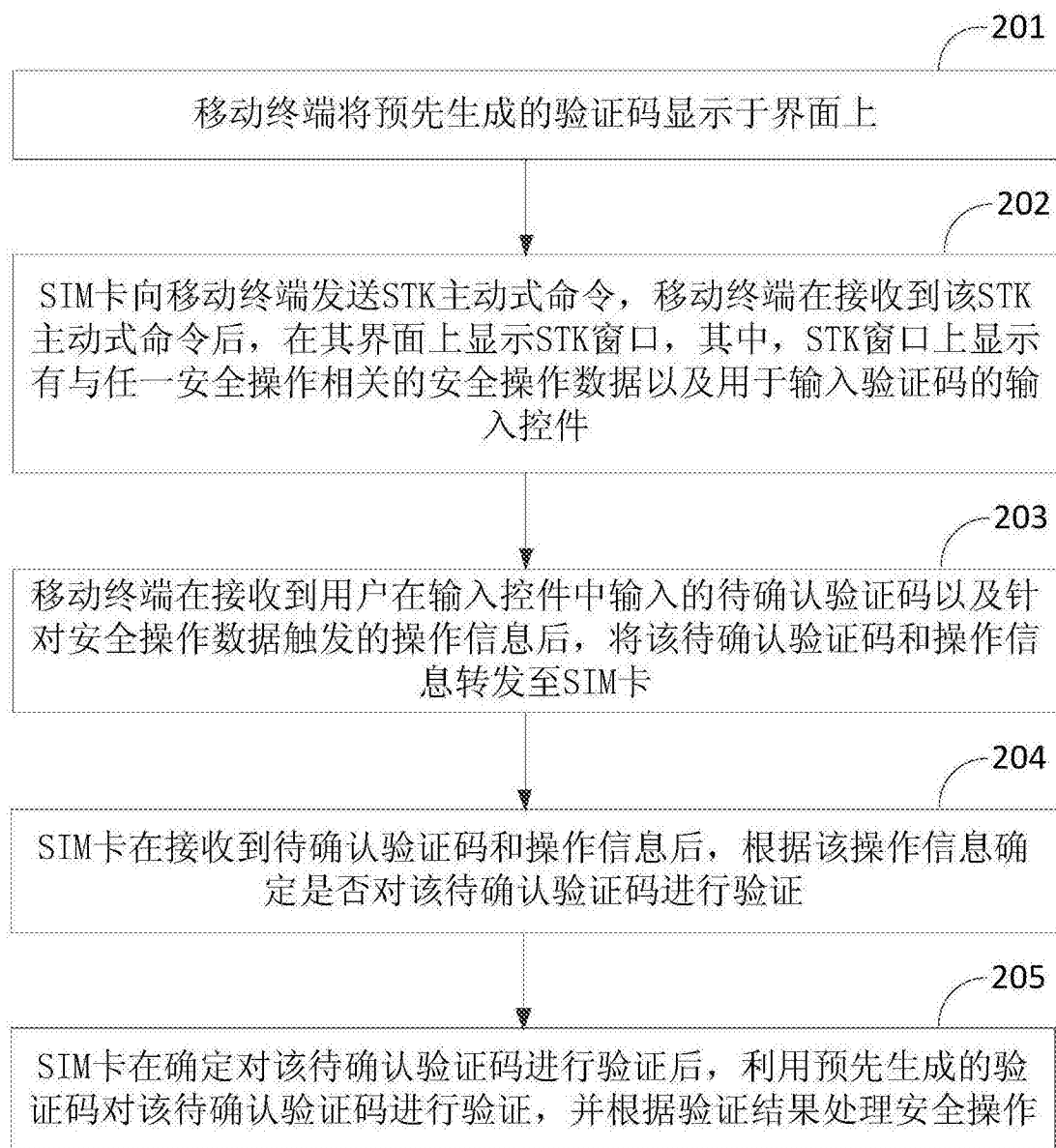


图2

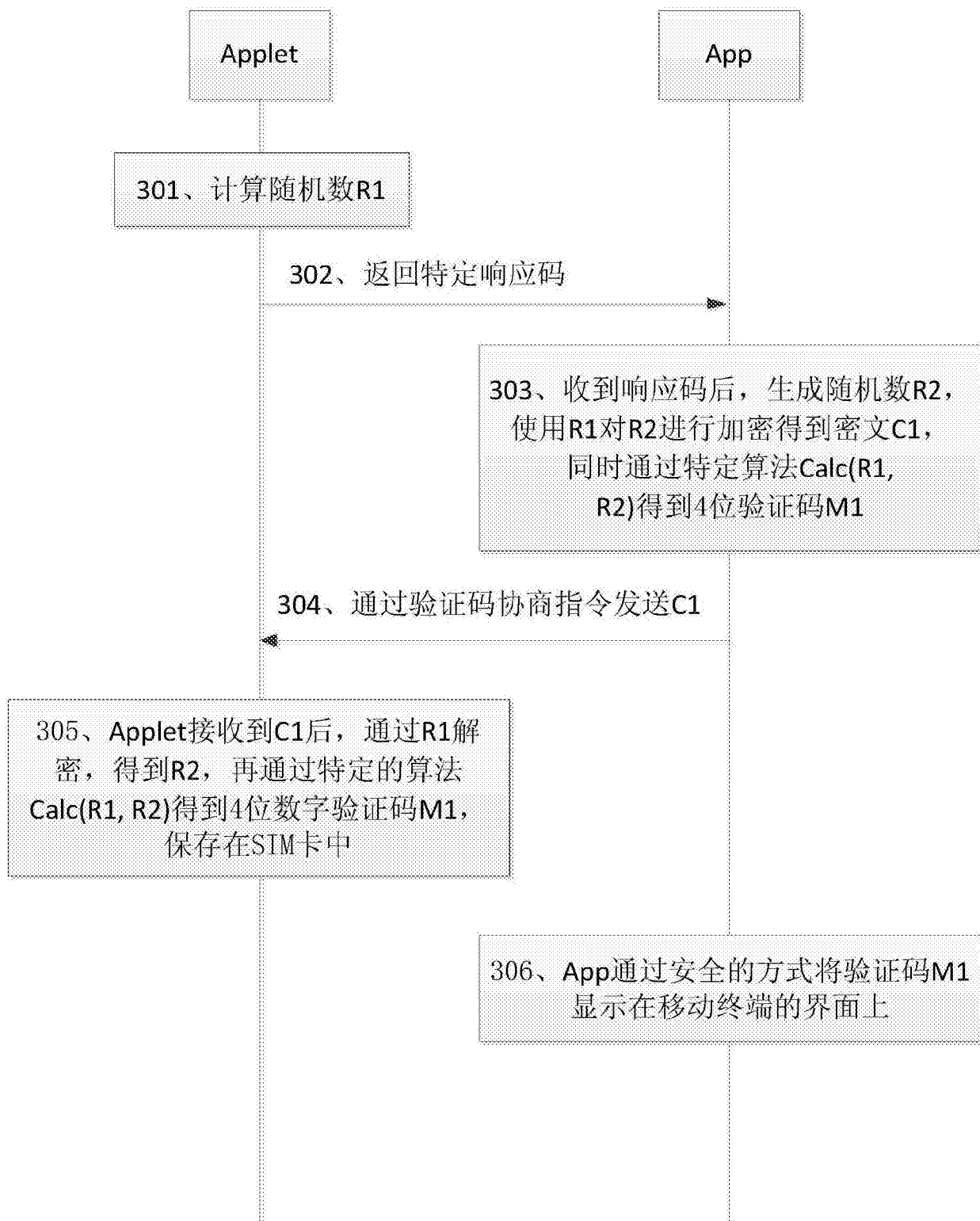


图3

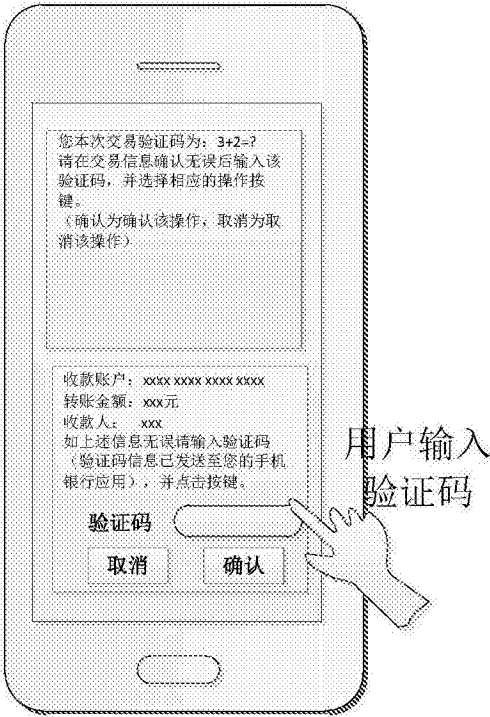


图4

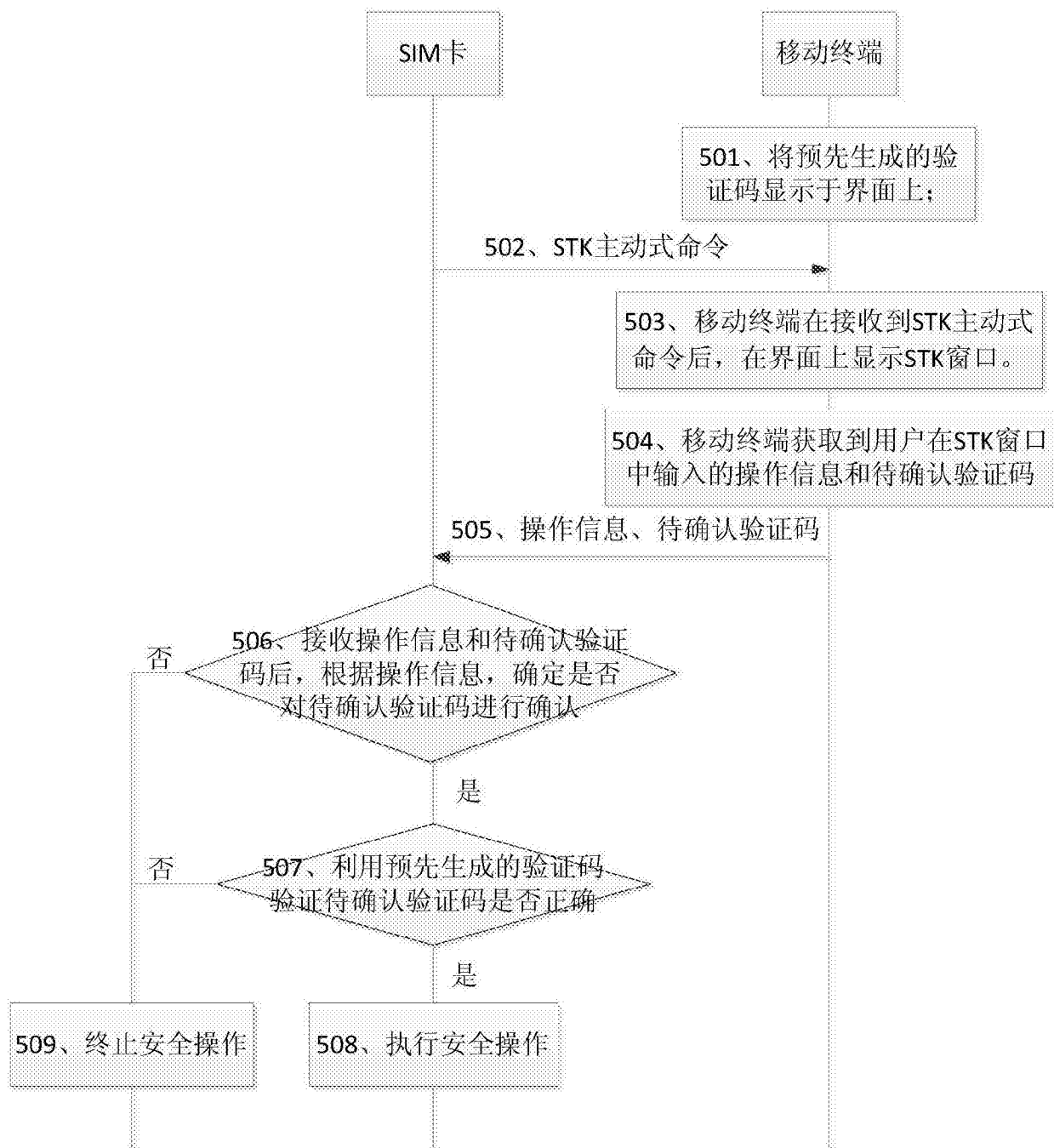


图5

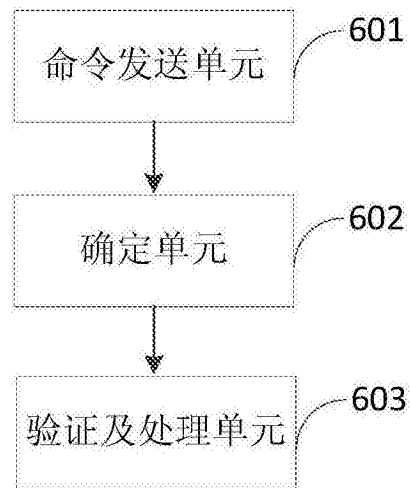


图6

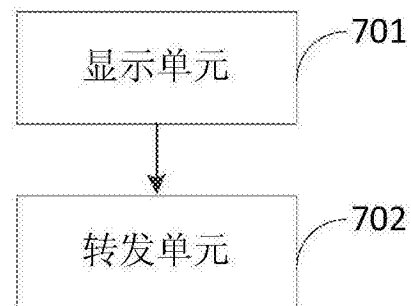


图7

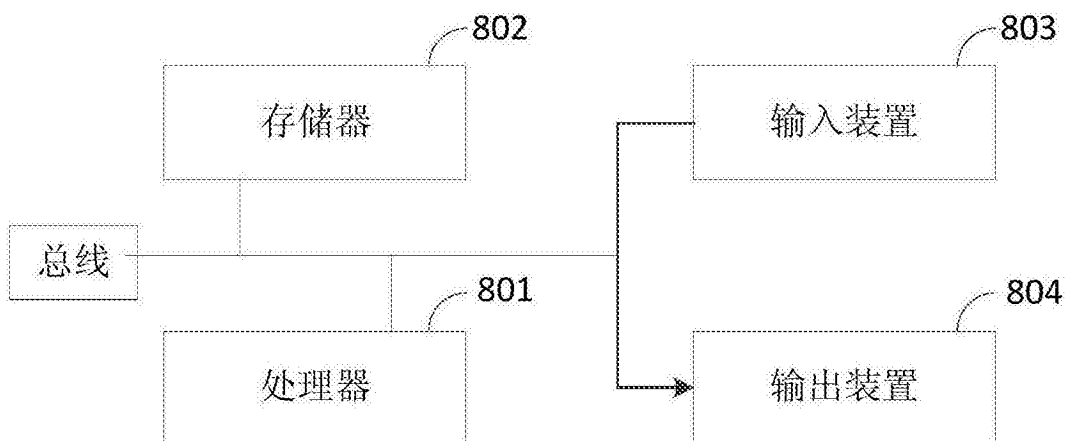


图8