(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 106295314 A
(43)申请公布日 2017.01.04

(21)申请号 201510268973.8

(22)申请日 2015.05.22

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区科技南路55号

(72)发明人 王小松 卫伟 张家明

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 江舟 李灵洁

(51)Int.Cl.
G06F 21/46(2013.01)

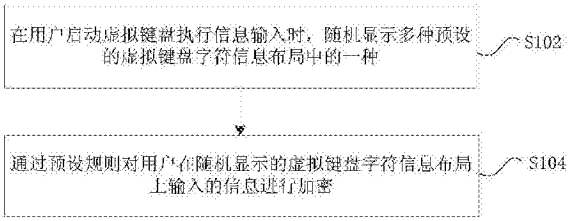
权利要求书1页 说明书7页 附图3页

(54)发明名称

基于虚拟键盘的加密方法及装置

(57)摘要

本发明提供了一种基于虚拟键盘的加密方法及装置，其中，该方法包括：在用户启动虚拟键盘执行信息输入时，随机显示多种预设的虚拟键盘字符信息布局中的一种；通过预设规则对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密。通过本发明，使得用户在在线支付时更加安全，解决了相关技术中移动客户端在线支付不够安全的问题。



CN 106295314 A

1.一种基于虚拟键盘的加密方法，其特征在于，包括：

在用户启动虚拟键盘执行信息输入时，随机显示多种预设的所述虚拟键盘字符信息布局中的一种；

通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密。

2.根据权利要求1所述的方法，其特征在于，所述字符信息包括：字母和数字信息、符号信息以及功能键信息，则随机显示多种预设的所述虚拟键盘字符信息布局中的一种包括：

将所述符号信息中指定常用的符号信息和所述功能键信息在所述字符信息布局的指定位置上显示；

将所述字母和数字信息在所述字符信息布局上随机显示。

3.根据权利要求2所述的方法，其特征在于，所述数字信息为中文数字信息。

4.根据权利要求1所述的方法，其特征在于，通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密包括：

通过RSA公钥加密算法对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密。

5.根据权利要求1所述的方法，其特征在于，在通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密之后，所述方法还包括：

将加密后信息发送到第三平台进行校验。

6.一种基于虚拟键盘的加密装置，其特征在于，包括：

显示模块，用于在用户启动虚拟键盘执行信息输入时，随机显示多种预设的所述虚拟键盘字符信息布局中的一种；

加密模块，用于通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密。

7.根据权利要求6所述的装置，其特征在于，所述字符信息包括：字母和数字信息、符号信息以及功能键信息，则所述显示模块包括：

第一显示单元，用于将所述符号信息中指定常用的符号信息和所述功能键信息在所述字符信息布局的指定位置上显示；

第二显示单元，用于将所述字母和数字信息在所述字符信息布局上随机显示。

8.根据权利要求7所述的装置，其特征在于，所述数字信息为中文数字信息。

9.根据权利要求6所述的装置，其特征在于，

所述加密模块，还用于通过RSA公钥加密算法对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密。

10.根据权利要求6所述的装置，其特征在于，在通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密之后，所述装置还包括：

发送模块，用于将加密后信息发送到第三平台进行校验。

基于虚拟键盘的加密方法及装置

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种基于虚拟键盘的加密方法及装置。

背景技术

[0002] 随着互联网迅速发展，网上购物成为现在人们生活的主题，如淘宝、京东以及各大网购网站，并且随着智能手机的普及，人们的生活渐渐成为掌上生活，移动支付应运而生，这是对传统面对面资金交易的转变。所以能否快捷并安全的支付成为目前资金转移的重要问题。

[0003] 目前手机系统大都是 Android 和 IOS 系统，但是目前各个客户端软件均没有非常严密的保护措施，使得用户完全信赖自己的资金安全，所以制约了移动支付的蓬勃发展。

[0004] 目前移动支付技术使用的键盘均是普通键盘、类似普通键盘或乱序的虚拟键盘，然后对用户输入的支付密码进行加密，普通虚拟键盘容易造成密码被旁观者偷窥，乱序的虚拟键盘可以有效的防止这一点，以最前沿的乱序的虚拟键盘为例，该虚拟键盘在使用上趋向于个人设备 PC 端应用，对键盘布局和数字键的处理没有涉及，采用同原有键盘具有一一映射关系，形成映射表存储于 PC 端，原键盘为 QWER，如生成的乱序键盘为 ERPY…，若用户输入的字符为 Q，则映射为 E，然后采用预设的加密算法，对用户输入进行加密。该方法一定程度上解决了密码安全问题，但是还不够理想。

[0005] 针对相关技术中移动客户端在线支付不够安全的问题，目前尚未提出有效的解决方案。

发明内容

[0006] 本发明的主要目的在于提供一种基于虚拟键盘的加密方法及装置，以至少解决相关技术中移动客户端在线支付不够安全的问题。

[0007] 根据本发明的一个方面，提供了一种基于虚拟键盘的加密方法，包括：在用户启动虚拟键盘执行信息输入时，随机显示多种预设的所述虚拟键盘字符信息布局中的一种；通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密。

[0008] 进一步地，所述字符信息包括：字母和数字信息、符号信息以及功能键信息，则随机显示多种预设的所述虚拟键盘字符信息布局中的一种包括：将所述符号信息中指定常用的符号信息和所述功能键信息在所述字符信息布局的指定位置上显示；将所述字母和数字信息在所述字符信息布局上随机显示。

[0009] 进一步地，所述数字信息为中文数字信息。

[0010] 进一步地，通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密包括：通过 RSA 公钥加密算法对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密。

[0011] 进一步地，在通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密之后，所述方法还包括：将加密后信息发送到第三平台进行校验。

[0012] 根据本发明的另一个方面，提供了一种基于虚拟键盘的加密装置，包括：显示模块，用于在用户启动虚拟键盘执行信息输入时，随机显示多种预设的所述虚拟键盘字符信息布局中的一种；加密模块，用于通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密。

[0013] 进一步地，所述字符信息包括：字母和数字信息、符号信息以及功能键信息，则所述显示模块包括：第一显示单元，用于将所述符号信息中指定常用的符号信息和所述功能键信息在所述字符信息布局的指定位置上显示；第二显示单元，用于将所述字母和数字信息在所述字符信息布局上随机显示。

[0014] 进一步地，所述数字信息为中文数字信息。

[0015] 进一步地，所述加密模块，还用于通过 RSA 公钥加密算法对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密。

[0016] 进一步地，在通过预设规则对用户在随机显示的所述虚拟键盘字符信息布局上输入的信息进行加密之后，所述装置还包括：发送模块，用于将加密后信息发送到第三平台进行校验。

[0017] 通过本发明，采用在用户启动虚拟键盘执行信息输入时，在终端的界面随机显示一种虚拟键盘字符信息的布局，也就是说在终端显示的键盘字符信息并只是只有一种布局方式，然后在随机显示的虚拟键盘字符信息布局上对用户输入的信息进行加密，通过本实施例，使得用户在在线支付时更加安全，解决了相关技术中移动客户端在线支付不够安全的问题。

附图说明

[0018] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0019] 图 1 是根据本发明实施例的基于虚拟键盘的加密方法的流程图；

[0020] 图 2 是根据本发明实施例的基于虚拟键盘的加密装置的结构框图；

[0021] 图 3 是根据本发明实施例的基于虚拟键盘的加密装置的可选结构框图一；

[0022] 图 4 是根据本发明实施例的基于虚拟键盘的加密装置的可选结构框图二；

[0023] 图 5 是根据本发明可选实施例的实现快捷支付的安全键盘的系统结构框图；

[0024] 图 6 是根据本发明可选实施例的安全键盘的布局图一；

[0025] 图 7 是根据本发明可选实施例的安全键盘的布局图二；

[0026] 图 8 是根据本发明可选实施例的实现快捷支付的安全键盘的方法的流程图；

[0027] 图 9 是根据本发明可选实施例的密码处理模块内部的操作过程的流程图。

具体实施方式

[0028] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本发明。

[0029] 本实施例提供了一种基于虚拟键盘的加密方法，图 1 是根据本发明实施例的基于虚拟键盘的加密方法的流程图，如图 1 所示，该方法的步骤包括：

[0030] 步骤 S102：在用户启动虚拟键盘执行信息输入时，随机显示多种预设的虚拟键盘

字符信息布局中的一种；

[0031] 步骤 S104：通过预设规则对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密。

[0032] 通过本实施例，采用在用户启动虚拟键盘执行信息输入时，在终端的界面随机显示一种虚拟键盘字符信息的布局，也就是说在终端显示的键盘字符信息并只是只有一种布局方式，然后在随机显示的虚拟键盘字符信息布局上对用户输入的信息进行加密，通过本实施例，使得用户在在线支付时更加安全，解决了相关技术中移动客户端在线支付不够安全的问题。

[0033] 对于本实施例涉及到的字符信息可以包括：字母和数字信息、符号信息以及功能键信息，基于此，本实施例中步骤 S102 中随机显示多种预设的虚拟键盘字符信息布局中的一种的方式，可以通过如下方式来实现：

[0034] 步骤 S11：将符号信息中指定常用的符号信息和功能键信息在字符信息布局的指定位置上显示；

[0035] 步骤 S12：将字母和数字信息在字符信息布局上随机显示。

[0036] 对于上述步骤 S11 和步骤 S12，在本实施例的一个应用场景中，虚拟键盘的布局可以是：常规键盘的布局包含 49 个按键，在本实施例中顶部是收起键（功能键）、常用的 6 个字符键（指定常用的符号键）和删除键（功能键），接着一排是从零到九的数字按键，中间区域是 26 个字母键，下侧左边分布大写切换和小写切换转换键（功能键），下侧右边分布符号切换和确认键（功能键），正中最下侧是空格键（功能键）。可见，在本实施例中功能键和指定常用的符号键分布在固定的位置，而字母和字符键只是在固定区域，而在这个固定区域内字母和字符键的顺序是随机的。

[0037] 在本实施例的另一个可选实施方式中，对于本实施例涉及到的数字信息为可选为中文数字信息。虽然数字键用中文键表示，但在后台处理输入的密码时依然按阿拉伯数字 0-9 来处理，这样做的目的是保障用户输入的安全，别人看到的输入和后台实际存储的输入有差别，同时键盘上输入和后台存储又有关联，易于用户理解自己的输入，既方便了用户的输入又保障了用户输入的安全。

[0038] 而对于本实施例涉及到的步骤 S104 中通过预设规则对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密方式，在本实施例的一个可选实施方式，可以通过如下方式来实现：通过 RSA 公钥加密算法对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密。需要说明的是 RSA 公钥加密算法是 RSA 公开密钥密码体制，该公开密钥密码提示就是使用不同的加密密钥与解密密钥，是一种“由一致加密密钥推导出解密密钥在计算上不可行的”密码体制，此外，该 RSA 算法仅仅是用来进行举例说明，并不构成本发明的限定，其他可以用来进行加密的算法也是在本发明的保护范围之内的。

[0039] 而在本实施例的通过预设规则对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密之后，本实施例的方法还可以包括：将加密后信息发送到第三平台进行校验。

[0040] 在本实施例中还提供了一种基于虚拟键盘的加密装置，该装置用于实现上述实施例及可选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”“单元”可以实现预定功能的软件和 / 或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来

实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0041] 图 2 是根据本发明实施例的基于虚拟键盘的加密装置的结构框图，如图 2 所示，该装置包括：显示模块 22，用于在用户启动虚拟键盘执行信息输入时，随机显示多种预设的虚拟键盘字符信息布局中的一种；加密模块 24，与显示模块 22 耦合连接，用于通过预设规则对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密。

[0042] 图 3 是根据本发明实施例的基于虚拟键盘的加密装置的可选结构框图一，如图 3 所示，字符信息包括：字母和数字信息、符号信息以及功能键信息，则显示模块 22 包括：第一显示单元 32，用于将符号信息中指定常用的符号信息和功能键信息在字符信息布局的指定位置上显示；第二显示单元 34，与第一显示单元 32 耦合连接，用于将字母和数字信息在字符信息布局上随机显示。

[0043] 可选地，对于本实施例中涉及到的述数字信息为中文数字信息。

[0044] 可选地，加密模块 24，还用于通过 RSA 公钥加密算法对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密。

[0045] 图 4 是根据本发明实施例的基于虚拟键盘的加密装置的可选结构框图二，在通过预设规则对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密之后，该装置还包括：发送模块 42，与加密模块 24 耦合连接，用于将加密后信息发送到第三平台进行校验。

[0046] 下面结合本发明的可选实施例对本发明进行举例说明；

[0047] 本可选实施例，提供了一种实现快捷支付的安全键盘方法，其中，安全键盘布局部分包含 49 个按键，顶部是收起键、常用的 6 个字符键和删除键，接着一排是中文从零到九的按键，中间区域是 26 个字母或字符键，下侧左边分布大写切换和小写切换转换键，下侧右边分布符号切换和确认键，正中最下侧是空格键。

[0048] 本可选实施例中安全键盘具备数字键始终在第二排且随机分布，字母键和字符键每次展现或切换布局均进行重新排列，仅有收起、删除、大写、小写、符号、空格和确认键布局不会改变。

[0049] 需要说明的是，收起键用于收起安全软键盘，删除键用于删除输入的密码中的单个字符，大写键用于切换键盘上的小写字母至大写字母，小写键用于切换键盘上的大写字母至小写字母，符号键用于将软键盘上的小写字母区域切换成字符区域，空格键用于输入单个空格字符，确认键用于密码的加密并传输到服务器。

[0050] 本可选实施例还提供了一种实现快捷支付的安全键盘的系统，该系统包括以下部分：

[0051] 1) 在终端上提供独特的虚拟键盘布局，布局中包含字母、中文数字展示、字符和必要的功能按键；其中，该功能按键用于提供乱序的字母、中文数字和字符键盘，每次展示虚拟键盘布局局部重新改变，后台随机排序字母、中文数字和字符并在键盘的不同区域进行展现；

[0052] 2) 提供密码输入模块，用于输入用 * 显示的用户密码输入，输入后的密码在输入框并进行加密处理，期间可以进行大小写切换、符号切换等满足用户输入的需要，密码采集模块通过监听键盘来获取每个键盘的值并得到输入的密码，乱序后键盘的每个按键具有一个码值，该码值唯一且与按键一一对应，监听每个按键获取用户的输入；

[0053] 3) 中文数字处理模块，用于当监听到中文数字按键操作时，后台按对应阿拉伯数字作为用户输入；

[0054] 4) 功能按键处理模块，用于监听功能按键，当功能按键操作时，触发相应的功能，如当大小写切换功能触发时，切换字母区域的大小写字母；

[0055] 5) 密码加密模块，用于将输入的密码进行加密处理，使用 RSA 进行加密；

[0056] 6) 传输模块，用于将生成的密文传输到第三方平台进行校验；

[0057] 可见，本可选实施例从功能上分主要分为四大模块：安全键盘布局模块、安全键盘输入模块、密码处理模块、密文传输模块。安全键盘布局模块展示合理按键布局，安全键盘输入模块主要处理密码输入和各种切换，密码处理模块是对密码进行加密处理，密文传输模块实现密文与第三方平台对接。

[0058] 下面结合本可选实施例的方法及上述模块，对本可选实施例进行相关说明；

[0059] 首先，对于本可选实施例中的键盘包括：个性化虚拟键盘，封装系统自带键盘，重新布局键盘，并对本可选实施例中的安全键盘分为汉字数字键、字母键、符号键和功能键。

[0060] 其中，重写或自定义功能键的实现，自定义收起键盘方法，实现点击安全键盘收起键能收起安全键盘、重写大小写切换键，实现切换大写键随机展示大写字母键盘，切换小写键随机展示小写字母键盘，重写符号键，实现点击符号键随机展示符号键盘，自定义删除键，实现点击删除键能删除密码框中的一个密码，自定义确认键，实现点击确认键，实现密码加密并传输。

[0061] 然后，在密码输入中文数字处理时，监听中文数字输入，对于中文数字键在后台以阿拉伯数字处理。密码输入完毕后，调用密码加密算法完成密码的加密操作。加密完成后，密文传输给第三方平台

[0062] 采用本可选实施例与相关技术相比，可以有效识别资金操作的使用者，保障用户资金的安全并且方便用户网上支付。解决了相关技术中的移动支付存在的安全隐患，从而确保用户资金安全。

[0063] 本可选实施例可以应用于：(1) 支付宝，支付宝的密码支付可以使用本发明中的方法，当用户在网上淘宝或转账时可以使用具有本发明安全键盘来保障你的资金安全，达到方便使用、快捷使用和安全有保障的效果。(2) 手机网银，手机网银在密码输入时可以调用本发明的安全键盘，用户在用手机进行资金操作时可以用安全键盘输入密码，避免密码被他人查看与泄露，同时密码加密处理，双重保障。(3) 理财应用，手机上的理财应用可以对登陆密码和支付密码进行安全键盘的使用，来保障资金安全。(4) 火车购票，手机在登陆 12306 购票时登陆密码可以使用安全键盘，可以保护用户的密码不被泄露，保障用户购票信息以及个人信息的安全。

[0064] 下面结合附图对本发明可选实施例进行详细说明；

[0065] 图 5 是根据本发明可选实施例的实现快捷支付的安全键盘的系统结构框图，如图 5 所示，本可选实施的系统包括：安全键盘布局模块，安全键盘输入模块，密码处理模块和密码传输模块。其中安全键盘布局模块对虚拟键盘布局进行设计，最上排是常用字符，接着是一排中文数字布局，中间区域为字母展示区域可以切换为大写字母或字符，周围布局实用的功能键；安全键盘输入模块用于完成输入的各种操作，包含切换大小写，切换字符，每次展示键盘的内容重新布局，以及收起安全键盘和删除输入的一个字符；密码处理模块主

要完成用户输入的密码进行 RSA 加密操作，获得加密后的用户密码；密码传输模块完成密文的传输给第三方服务器。

[0066] 图 6 是根据本发明可选实施例的安全键盘的布局图一，图 7 是根据本发明可选实施例的安全键盘的布局图二，图 6 展示了字母键盘的布局，图 7 展示了符号键盘的布局，这种布局在 Android 平台通过用 xml 文件写好布局文件，在 Res 下新建两个 xml 文件，分别为 qwerty.xml 和 symbols.xml，qwerty.xml 是图 6 的布局文件，symbols.xml 是图 7 的布局文件。该布局文件实现软键盘的布局，每个按键都有一个 codes 值，即布局中的每个键盘按键有个 code 码值与之一一对应，如按键 a 对应的码值为 97，通过 code 值来监听每一个按键，代码中需要对现有的 Android 平台的 keyBoard 进行封装，使用原有的 keyBoard 的方法，对于特殊需要的功能需要重新一些方法或自定义一些方法来实现，对于 IOS 平台，通过获取系统键盘所在的 view，然后自定义一个 view 覆盖在系统键盘 view 上，接着加入个性化实现的方法。

[0067] 图 8 是根据本发明可选实施例的实现快捷支付的安全键盘的方法的流程图，如图 8 所示，该流程的步骤包括：

[0068] 步骤 S802：启动安全键盘；

[0069] 步骤 S804：密码输入处理；

[0070] 步骤 S806：密码加密；

[0071] 步骤 S808：密码传输；

[0072] 步骤 S810：判断密码是否正确；在判断为是时，执行步骤 S812，在判断为否时，执行步骤 S814；

[0073] 步骤 S812：支付成功；

[0074] 步骤 S814：支付失败。

[0075] 也就是说，上述步骤 S802 至步骤 S814 整个过程为：启动安全键盘，此时会弹出本发明自定义的安全键盘布局，在安全键盘上进行操作，输入密码，因每次弹出的安全键盘中键盘内容的布局不一样，从而避免输入密码的泄露，后台根据每个按键的 code 进行监听，对于点击中文数字时后台进行判断按阿拉伯数字进行处理，接着系统会对用户输入的密码使用 RSA 方法进行加密，并且使用该算法加密的结果在 java 平台上给定密钥和密文后后可以解密出明文，将加密后的密文传输给服务端数据库进行比对，判断密码的正确性，若密码不对直接支付失败返回，若密码比对正确，跳转到支付成功界面，提示用户的支付操作成功完成。

[0076] 图 9 是根据本发明可选实施例的密码处理模块内部的操作过程的流程图，如图 9 所示，该流程的步骤包括：

[0077] 步骤 S902：输入密码；

[0078] 步骤 S904：密码 RSA 加密；

[0079] 步骤 S906：输出加密后的密码。

[0080] 该过程的详细过程为：密码处理采用 1024 位 RSA 算法，首先生成公钥和私钥，用户的密码根据公钥加密成密文输出，传送到服务端时，服务端用私钥和密文进行解密，若解密的结果和数据库中存储的结果一致，则说明密码输入正确，否则密码输入有误。

[0081] 在另外一个实施例中，还提供了一种软件，该软件用于执行上述实施例及优选实

施方式中描述的技术方案。

[0082] 在另外一个实施例中，还提供了一种存储介质，该存储介质中存储有上述软件，该存储介质包括但不限于：光盘、软盘、硬盘、可擦写存储器等。

[0083] 显然，本领域的技术人员应该明白，上述本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0084] 上述仅为本发明的可选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

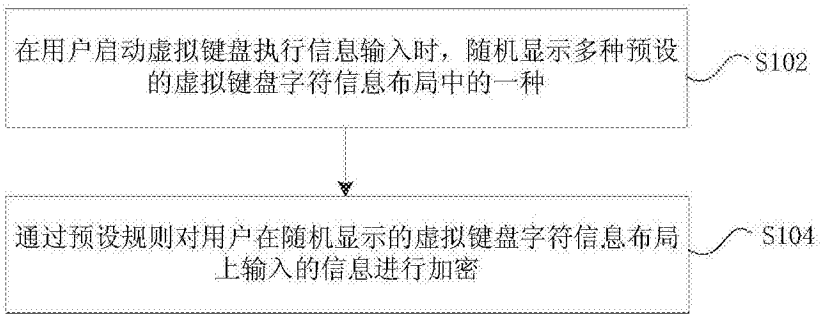

在用户启动虚拟键盘执行信息输入时，随机显示多种预设的虚拟键盘字符信息布局中的一种
S102
通过预设规则对用户在随机显示的虚拟键盘字符信息布局上输入的信息进行加密
S104

图 1


显示模块
22
加密模块
24

图 2

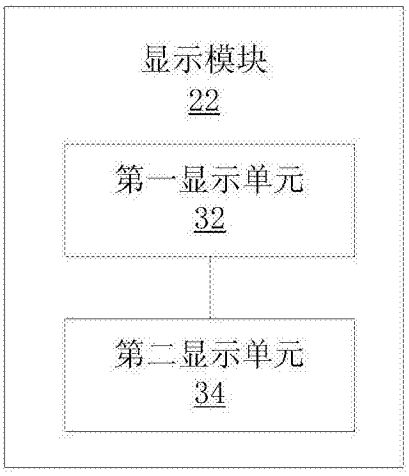

显示模块
22
第一显示单元
32
第二显示单元
34

图 3

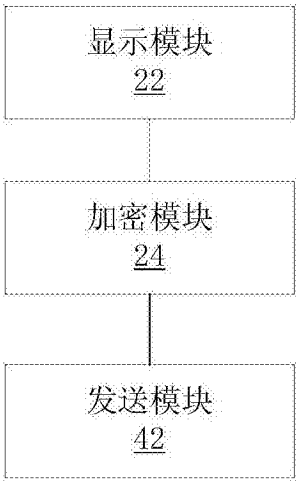

显示模块
22
加密模块
24
发送模块
42

图 4

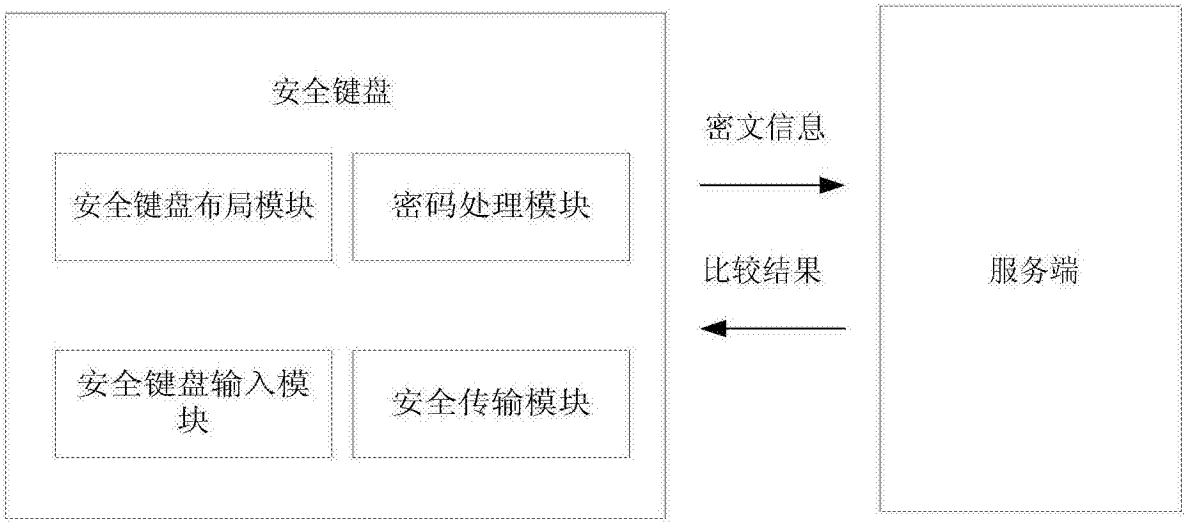

安全键盘
安全键盘布局模块
密码处理模块
安全键盘输入模块
安全传输模块
密文信息
比较结果
服务端

图 5

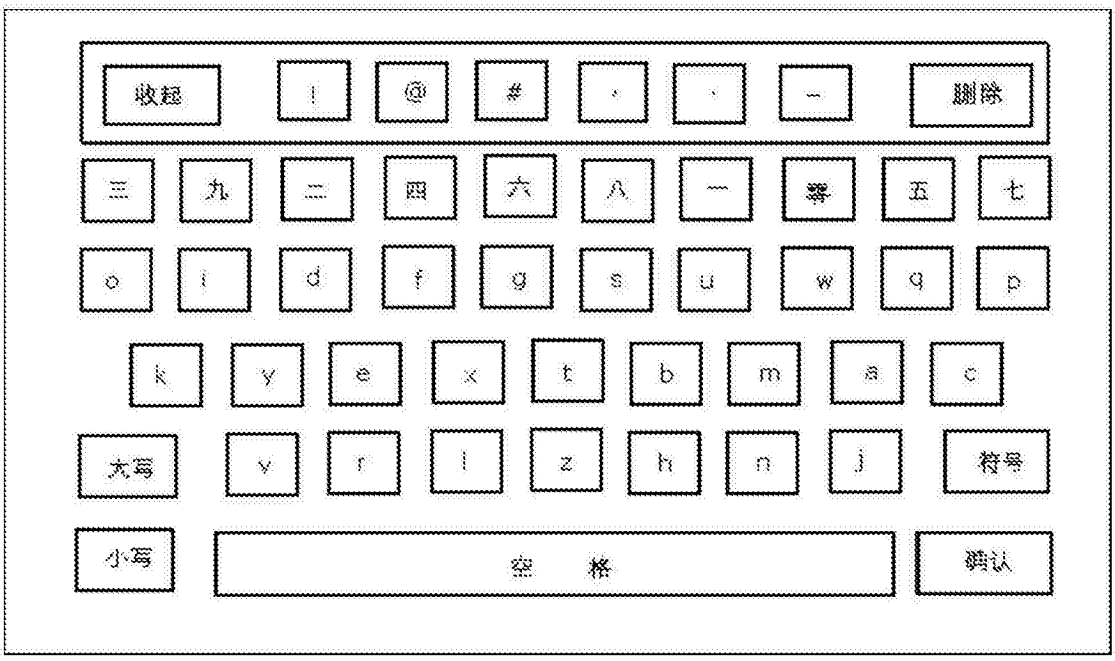

收起
!
@
#
、
、
—
删除
三
九
二
四
六
八
一
零
五
七
o
i
d
f
g
s
u
w
q
p
k
y
e
x
t
b
m
a
c
大写
v
r
l
z
h
n
j
符号
小写
空 格
确认

图 6

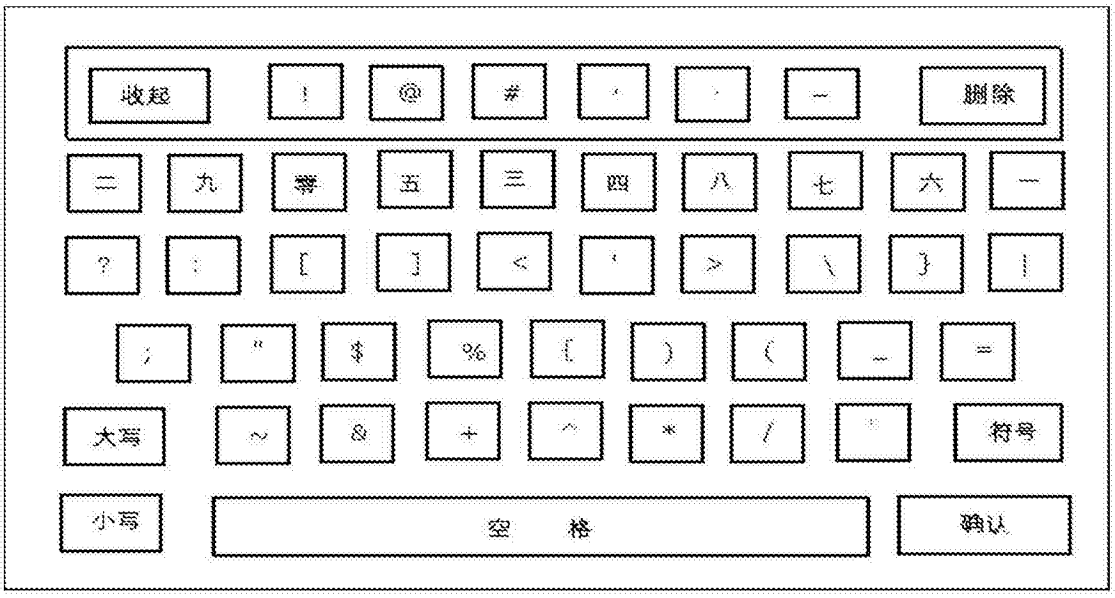

收起
!
@
#
、
、
—
删除
二
九
零
五
三
四
八
七
六
一
?
:
[
]
<
'
>
\
}
|
;
"
$
%
(
)
(
_
=
大写
~
&
+
^
*
/
符号
小写
空 格
确认

图 7

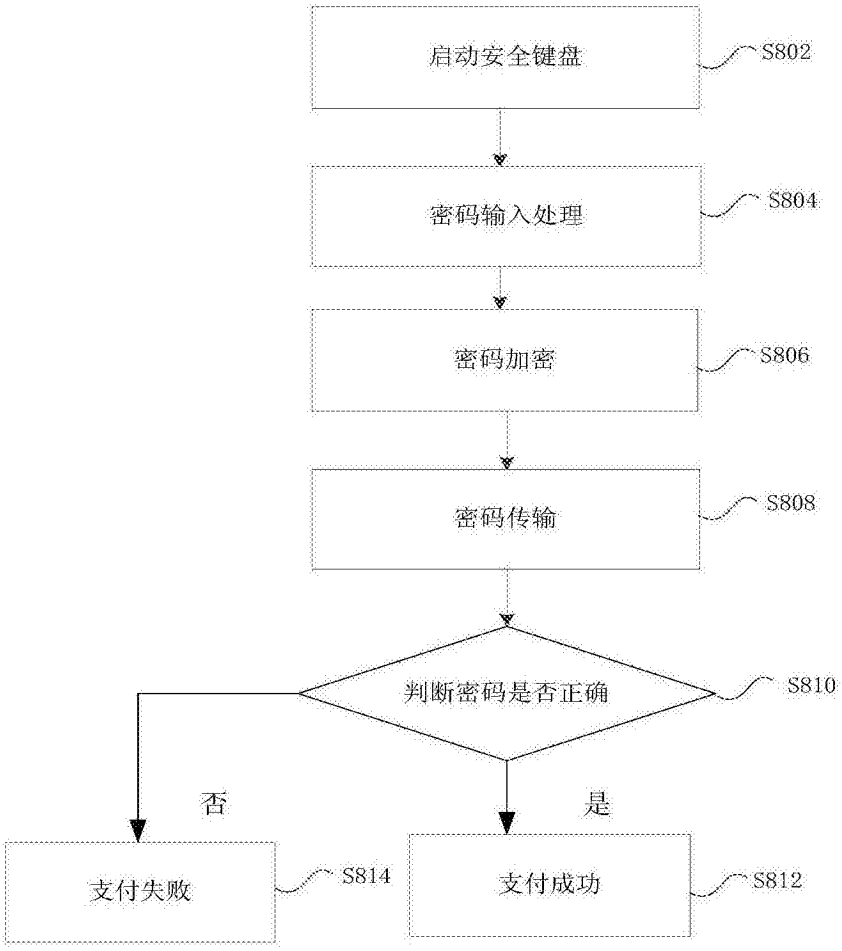

启动安全键盘
S802
密码输入处理
S804
密码加密
S806
密码传输
S808
判断密码是否正确
S810
否
是
支付失败
S814
支付成功
S812

图 8

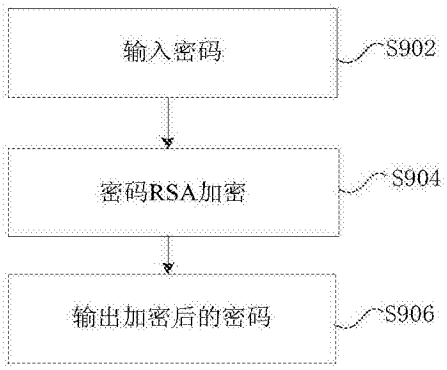

输入密码
S902
密码RSA加密
S904
输出加密后的密码
S906

图 9