(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102932341 B
(45)授权公告日 2016.01.13

(21)申请号 201210413895.2

(22)申请日 2012.10.25

(73)专利权人 小米科技有限责任公司
地址 100085 北京市海淀区清河中街 68 号
华润五彩城购物中心二期 13 层

(72)发明人 万钰臻 孙鹏 林俊琦

(51)Int.Cl.
H04L 29/06(2006.01)
H04M 1/725(2006.01)

(56)对比文件
CN 102497635 A,2012.06.13, 权利要求 1-5.

审查员 裴广坤

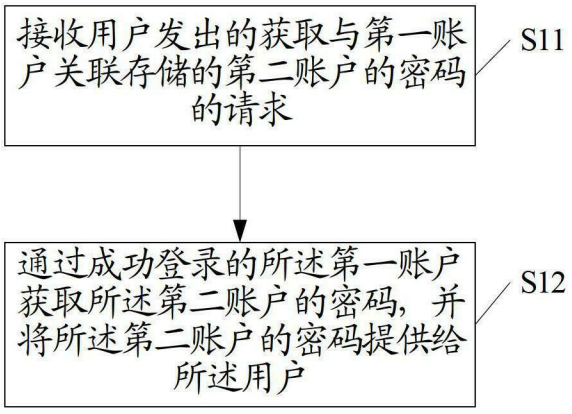
权利要求书2页 说明书9页 附图5页

(54)发明名称

一种密码处理方法、装置及设备

(57)摘要

本发明公开了一种密码处理方法、系统及设备，信息处理技术领域。该方法包括以下步骤：接收用户发出的获取与第一账户关联存储的第二账户的密码的请求；通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。本发明实施例提出的密码处理方法使得用户只要将注册的其他账户密码与第一账户关联存储，便可以只记得一个第一账户的密码，通过登录第一账户获取多个其他账户的密码，免去了需要用户记忆密码的不便。



CN 102932341 B

1. 一种密码处理方法，其特征在于，包括以下步骤：

接收用户为第二账户设置的密码，或接收所述用户发出的生成所述第二账户的密码的请求，根据所述请求为所述第二账户生成密码；

将所述第二账户、所述第二账户的密码以及第一账户关联存储至移动终端本地预设路径或服务器；

接收用户发出的获取与第一账户关联存储的第二账户的密码的请求；

通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户；

所述通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户，包括：

在所述移动终端不能与所述服务器通信时，通过成功登录的所述第一账户，从所述移动终端的本地预设路径获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户；

在所述移动终端能与所述服务器通信时，通过成功登录的所述第一账户，从所述服务器获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。

2. 根据权利要求 1 所述的方法，其特征在于，所述请求中包括所述第二账户的密码的类型和 / 或强度。

3. 根据权利要求 1 所述的方法，其特征在于，当所述第二账户、所述第二账户的密码以及所述第一账户关联存储至服务器时，所述通过成功登录的所述第一账户获取所述第二账户的密码的步骤包括：

将用户发出的获取与第一账户关联存储的第二账户的密码的请求发送至服务器，以使服务器通过登陆成功的所述第一账户查找第二账户的密码；

接收服务器返回的所述第二账户的密码。

4. 根据权利要求 1 所述的方法，其特征在于，所述将所述第二账户的密码提供给所述用户，采用如下方式：

将所述第二账户的密码显示在预设区域中；或者

将所述第二账户的密码填充至密码输入区域中。

5. 根据权利要求 1 所述的方法，其特征在于，通过成功登录的所述第一账户获取所述第二账户的密码的步骤之前，所述方法还包括：

接收并向服务器转发所述用户输入的登陆所述第一账户的请求，以便于所述服务器完成所述第一账户的登录；

接收所述服务器返回的所述第一账户登录成功的指示消息；

其中，所述登陆所述第一账户的请求中携带有所述第一账户的账户名和密码。

6. 一种密码处理系统，其特征在于，包括移动终端；

所述移动终端包括：

第一接收模块，用于接收用户发出的获取与第一账户关联存储的第二账户的密码的请求；

第一获取密码模块，用于通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户；

所述移动终端还包括 :

第一设置密码模块,用于接收所述用户为所述第二账户设置的密码,或接收所述用户发出的生成所述第二账户的密码的请求,根据所述请求为所述第二账户生成密码 ;将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至本地预设路径 ;

所述第一获取密码模块,还用于在所述移动终端不能与服务器通信时,通过成功登录的所述第一账户,从所述移动终端的本地预设路径获取所述第二账户的密码,并将所述第二账户的密码提供给所述用户 ;

所述系统还包括服务器,

所述服务器包括 :

第二设置密码模块,用于接收所述用户为所述第二账户设置的密码,或接收所述用户发出的生成所述第二账户的密码的请求,根据所述请求为所述第二账户生成密码 ;将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至服务器 ;

所述第一获取密码模块用于 :在所述移动终端能与所述服务器通信时,将用户发出的获取与第一账户关联存储的第二账户的密码的请求发送至服务器,接收所述服务器返回的所述第二账户的密码 ;

所述服务器还包括 :

第二获取密码模块,用于接收所述移动终端发送的获取与第一账户关联的第二账户的密码的请求,通过登陆成功的所述第一账户查找第二账户的密码,将查找到的第二账户的密码发送至移动终端。

7. 根据权利要求 6 所述的系统,其特征在于,所述请求中包括密码的类型和 / 或强度。

8. 根据权利要求 6 所述的系统,其特征在于,所述第一获取密码模块还用于 :将所述第二账户的密码显示在预设区域中 ;或者将所述第二账户的密码填充至密码输入区域中。

9. 根据权利要求 6 所述的系统,其特征在于,所述移动终端还包括 :

登陆第一账户模块,用于接收并向服务器转发所述用户输入的登陆所述第一账户的请求,以便于所述服务器完成所述第一账户的登录 ;接收所述服务器返回的所述第一账户登录成功的指示消息 ;其中,所述登陆所述第一账户的请求中携带有所述第一账户的账户名和密码。

一种密码处理方法、装置及设备

技术领域

[0001] 本发明涉及信息处理技术领域，更具体地，涉及一种密码处理方法、装置及设备。

背景技术

[0002] 随着互联网的发展，以及移动终端（例如手机、平板电脑等）智能化程度越来越高，移动终端具有越来越多的功能，尤其是在移动终端中，各种应用越来越多，例如社交类的应用程序、记事类应用程序、拍照类应用程序、购物类应用程序等等。一些应用程序由于具有社交功能、支付功能或联网功能，需要用户向该应用的服务器申请账号并设置密码，例如邮箱、社区、微博等，还有一些应用程序需要保护用户隐私，也可以为用户设置账号和密码，以上这些设置账号和密码都是为了验证用户的权限，很好地保护了需要访问的应用程序的安全性，从而也保护了用户的隐私。

[0003] 但是，面对越来越多的应用，用户需要记住越来越多的账号和密码，并且要将账号和密码一一对应地记住，这对于用户来说很不方便。

发明内容

[0004] 有鉴于此，本发明实施例的目的是提出一种密码处理方法、装置及设备，能够提供便捷的密码获取方式，为用户提供便利。

[0005] 为了达到上述目的，本发明实施例提出一种密码处理方法，包括以下步骤：

[0006] 接收用户发出的获取与第一账户关联存储的第二账户的密码的请求；

[0007] 通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。

[0008] 本发明实施例提出的密码处理方法使得用户只要将注册的其他账户密码与第一账户关联存储，便可以只记得一个第一账户的密码，通过登录第一账户获取多个其他账户的密码，免去了需要用户记忆密码的不便。

[0009] 作为上述技术方案的优选，所述接收用户发出的获取与第一账户关联存储的第二账户的密码的请求之前，还包括：

[0010] 接收所述用户为所述第二账户设置的密码，或

[0011] 接收所述用户发出的生成所述第二账户的密码的请求，根据所述请求为所述第二账户生成密码；

[0012] 将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至本地预设路径或服务器。

[0013] 本方案给出第二账户密码的生成方法。

[0014] 作为上述技术方案的优选，所述请求中包括所述第二账户的密码的类型和/或强度。

[0015] 该方案可以生成符合第二账户的密码要求的密码。

[0016] 作为上述技术方案的优选，当所述第二账户、所述第二账户的密码以及所述第一

账户关联存储至服务器时，所述通过成功登录的所述第一账户获取所述第二账户的密码的步骤包括：

[0017] 将用户发出的获取与第一账户关联存储的第二账户的密码的请求发送至服务器，以使服务器通过登陆成功的所述第一账户查找第二账户的密码；

[0018] 接收服务器返回的所述第二账户的密码。

[0019] 本方案给出了通过服务器获取第二账户的密码的方法。

[0020] 作为上述技术方案的优选，所述将所述第二账户的密码提供给所述用户，采用如下方式：

[0021] 将所述第二账户的密码显示在预设区域中；或者

[0022] 将所述第二账户的密码填充至密码输入区域中。

[0023] 该方案可以对获得的密码进行进一步的处理，方便了用户的使用。

[0024] 作为上述技术方案的优选，通过成功登录的所述第一账户获取所述第二账户的密码的步骤之前，所述方法还包括：

[0025] 接收并向服务器转发所述用户输入的登陆所述第一账户的请求，以便于所述服务器完成所述第一账户的登录；

[0026] 接收所述服务器返回的所述第一账户登录成功的指示消息；

[0027] 其中，所述登陆所述第一账户的请求中携带有所述第一账户的账户名和密码。

[0028] 本方案进一步限定了通过服务器来登陆第一账户的技术方案。

[0029] 本发明实施例还提出一种密码处理系统，包括移动终端；

[0030] 所述移动终端包括：

[0031] 第一接收模块，用于接收用户发出的获取与第一账户关联存储的第二账户的密码的请求；

[0032] 第一获取密码模块，用于通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。

[0033] 作为上述技术方案的优选，所述移动终端还包括：

[0034] 第一设置密码模块，用于接收所述用户为所述第二账户设置的密码，或接收所述用户发出的生成所述第二账户的密码的请求，根据所述请求为所述第二账户生成密码；将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至本地预设路径。

[0035] 作为上述技术方案的优选，所述系统还包括服务器，

[0036] 所述服务器包括：

[0037] 第二设置密码模块，用于接收所述用户为所述第二账户设置的密码，或接收所述用户发出的生成所述第二账户的密码的请求，根据所述请求为所述第二账户生成密码；将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至服务器；

[0038] 所述第一获取密码模块用于：将用户发出的获取与第一账户关联存储的第二账户的密码的请求发送至服务器，接收所述服务器返回的所述第二账户的密码；

[0039] 所述服务器还包括：

[0040] 第二获取密码模块，用于接收所述移动终端发送的获取与第一账户关联的第二账户的密码的请求，通过登陆成功的所述第一账户查找第二账户的密码，将查找到的第二账户的密码发送至移动终端。

[0041] 作为上述技术方案的优选，所述请求中包括密码的类型和 / 或强度。

[0042] 作为上述技术方案的优选，所述第一获取密码模块还用于 ：将所述第二账户的密码显示在预设区域中 ；或者将所述第二账户的密码填充至密码输入区域中。

[0043] 作为上述技术方案的优选，所述移动终端还包括 ：

[0044] 登陆第一账户模块，用于接收并向服务器转发所述用户输入的登陆所述第一账户的请求，以便于所述服务器完成所述第一账户的登录 ；接收所述服务器返回的所述第一账户登录成功的指示消息 ；其中，所述登陆所述第一账户的请求中携带有所述第一账户的账户名和密码。

[0045] 本发明实施例还提出一种设备，所述设备包括 ：

[0046] 一个或多个处理器 ；

[0047] 存储器 ；和

[0048] 一个或多个模块，所述一个或多个模块存储于所述存储器中并被配置成由所述一个或多个处理器执行，其中，所述一个或多个模块具有如下功能 ：

[0049] 接收用户发出的获取与第一账户关联存储的第二账户的密码的请求 ；

[0050] 通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。

[0051] 本发明实施例的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明实施例而了解。本发明实施例的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

[0052] 下面通过附图和实施例，对本发明实施例的技术方案做进一步的详细描述。

附图说明

[0053] 附图用来提供对本发明实施例的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明实施例，并不构成对本发明实施例的限制。在附图中 ：

[0054] 图 1 是本发明优选实施例提出的密码处理方法的流程图 ；

[0055] 图 2 是本发明一具体实施例提出的密码生成方法的流程图 ；

[0056] 图 3 是本发明一具体实施例提出的密码获取方法的流程图 ；

[0057] 图 4 是本发明另一具体实施例提出的密码生成方法的流程图 ；

[0058] 图 5 是本发明另一具体实施例提出的密码获取方法的流程图 ；

[0059] 图 6 是本发明优选实施例提出的密码处理系统的结构示意图 ；

[0060] 图 7 是本发明一具体实施例提出的密码处理系统的结构示意图。

具体实施方式

[0061] 以下结合附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明实施例，并不用于限定本发明实施例。

[0062] 如图 1 所示为本发明优选实施例提出的一种密码处理方法，包括 ：

[0063] 步骤 S11 ：接收用户发出的获取与第一账户关联存储的第二账户的密码的请求 ；

[0064] 步骤 S12 ：通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。

[0065] 本发明实施例提出的密码处理方法是将用户的第二账户的密码与第一账户关联存储，当用户需要第二账户的密码时，只需登陆第一账户就能获得第二账户的密码，因此，免去了需要用户记忆密码的不便。

[0066] 在本发明实施例中，密码处理可以包括密码生成和密码获取两个过程，下面通过具体实施例来对本发明提出的密码生成及获取方法分别进行详细说明。

[0067] 具体实施例一

[0068] 如图 2 所示，本实施例提供了一种密码生成方法，在该实施例中，以在服务器侧生成密码为例对一种密码处理方法进行说明，且在本实施例中，以第一账户为主账户、第二账户为主账户的子账户为例进行说明，包括以下步骤：

[0069] 步骤 S21：用户通过向服务器注册获得主账户；

[0070] 例如，用户可以通过手机中安装的浏览器登录预定网址进行主账户的注册。需要说明的是，在当前用户已具有可提供子账户密码生成及密码获取服务的主账户的情况下，本步骤 S21 不是必选步骤。

[0071] 步骤 S22：用户登录主账户；

[0072] 登录时需要通过主账户的账户名、密码等认证，另外，也可选取其他登录方式，例如，通过动态密码认证、短消息认证等，本发明实施例中不做限定。

[0073] 步骤 S23：用户打开手机中的应用程序 A，弹出应用程序 A 的注册页面；

[0074] 在本实施例中，应用程序 A 需要用户注册，并通过用户名和密码验证合法后才可以使用程序 A。

[0075] 步骤 S24：用户在应用程序 A 的注册页面中输入欲注册使用的账户名，该欲注册使用的账户即为子账户；

[0076] 其中，用户可以根据应用程序 A 的要求输入子账户名，例如，应用程序 A 可能要求用户用电子邮箱地址、手机号码、用户名等信息注册。

[0077] 步骤 S25：用户向服务器发出生成密码的请求，请求中带有欲注册使用的子账户的名称；

[0078] 这里，如果仅将用户名作为用户的主账户下的一个子账户，可能会出现以下情况：该用户名与主账户名一致，也就是子账户与主账户相同，更或者，会出现多个应用程序的用户名相同，或与主账户名相同，例如，为同一邮件地址，因此，优选地，可以将该应用程序的名称和子账户的名称一起作为子账户，因为，一个应用程序可能会出现多个账户的情况，例如，邮件应用程序中允许多个邮件账户同时存在，因此，一个应用程序可能具有多个用户名以及对应的密码，所以，将应用程序的名称和子账户的名称一起作为子账户能更好的进行区别；

[0079] 优选地，在该请求中，还可以携带该应用程序对密码的类型的要求以及用户对密码强度的要求，其中，类型例如可以包括：密码的位数、密码的组合（例如数字和字母）等等。这样，服务器可以根据该要求生成可用的密码，例如：当用户需要一个至少八位的密码时，为用户生成八位以上的密码；当用户需要至少一个八位且为数字与字母的组合的密码时，则可生成一个八位的数字与字母组合的密码；当用户需要使用一个 128bit（比特）的密码对数据进行加密用时，则生成一个 128bit 的密码；

[0080] 更近一步地，该步骤还可以扩展为：用户欲使用一个密码作为密钥加密数据，也可

向服务器发起生成密码的请求，该请求中包括加密数据的名称，将该加密数据的名称作为子账户。

[0081] 步骤 S26 ：服务器接收该请求，为该子账户生成密码，需要说明的是，子密码的生成算法，这里不做限定。例如，可以为任意一个随机数生成算法。

[0082] 步骤 S27 ：服务器将该子账户的密码与用户的主账户及子账户关联存储。

[0083] 步骤 S28 ：服务器将该子账户的密码发送至用户 ；

[0084] 优选地，服务器可通过安全通道发送密码给终端，例如，终端与服务器建立的为传输控制协议（Transmission Control Protocol，简称 TCP）链接，则可使用安全的超文本传输协议（Hypertext Transfer Protocol over Secure Socket Layer，简称 https）通道进行子密码的发送。

[0085] 步骤 S29 ：用户使用该密码完成子账户的注册。

[0086] 优选地，在该步骤中，当终端接收到子密码后，可以在预设的显示区域显示该密码，以便用户进行使用 ；也可以直接填充到密码区域，而不显示出来，比如显示为黑点 ；或者当用户使用该密码当作密钥时，可直接使用该密码完成数据的加密。

[0087] 作为另一种实施方式，步骤 S27 还可以被替换为 ：

[0088] 服务器将该子账户的密码发送至终端，终端将用户的子账户、该子账户的密码保存在终端的预设位置，优选地，该预设位置只有具有 root 权限的账户（root 是超级管理员用户帐户，该帐户拥有整个系统至高无上的权力）才可查看。

[0089] 在上述实施例中，步骤 S22 也可放在步骤 S24 之后执行，只要服务器验证用户的主账户后，才会为用户的子账户生成密码。

[0090] 与上述服务器生成密码的方法对应的获取密码的方法如图 3 所示，包括 ：

[0091] 步骤 S31 ：用户登录主账户，且服务器对主账户认证通过 ；

[0092] 用户登陆主账户的具体方法可以如下 ：

[0093] 接收并向服务器转发所述用户输入的登陆所述主账户的请求，以便于所述服务器完成所述主账户的登录 ；

[0094] 接收所述服务器返回的所述主账户登录成功的指示消息 ；

[0095] 其中，所述登陆所述主账户的请求中携带有所述主账户的账户名和密码。

[0096] 步骤 S32 ：用户打开应用程序 A，执行登录操作，输入子账户名。

[0097] 步骤 S33 ：向服务器发送获取该子账户（与应用程序 A 对应的账户）的密码的请求 ；

[0098] 较佳地，获取密码的请求中携带有子账户的名称 ；

[0099] 需要说明的是，步骤 S31 也可以在步骤 S33 之后执行，服务器需保证用户的主账户认证通过后，才会为用户的子账户查找对应的密码。

[0100] 步骤 S34 ：服务器根据该用户的子账户名查找该子账户对应的密码。

[0101] 步骤 S35 ：服务器向用户发送该子账户的密码 ；

[0102] 优选地，服务器可通过安全通道发送子密码给终端，例如，终端与服务器建立的为 TCP 链接，则可使用 https 通道进行子密码的发送。

[0103] 步骤 S36 ：用户使用该密码完成子账户的登录。

[0104] 优选地，在该步骤中，当终端接收到子密码后，可以在预设的显示区域显示该密码，以便用户进行使用 ；也可以直接填充到密码区域，而不显示出来，比如显示为黑点 ；或

者当用户使用该密码当作密钥时，可直接使用该密码完成数据的解密。

[0105] 在该实施例中，生成密码和获取密码的方法在服务器端实现，需要注意的是，在可选的步骤 S27 的另一种实施方式中，终端已将用户的子账户、该子账户的密码保存在终端的只有具有 root 权限的账户才可查看的位置(例如终端本身的 ROM(Read-Only Memory，只读内存))，因此，在获取密码时，如果当时终端没有联网，不能与服务器通信，那么，也可以从终端中获取密码。

[0106] 具体实施例二

[0107] 如图 4 所示，为一种密码生成方法，在该实施例中，以在终端侧生成密码、从终端侧获取密码为例对一种密码处理方法进行说明，且在本实施例中，以第一账户为主账户、第二账户为主账户的子账户为例进行说明，包括以下步骤：

[0108] 步骤 S41：用户通过注册获得主账户；

[0109] 在本实施例中，主账户既可以为建立在本地的账户，也可以为建立在服务器的账户。

[0110] 在手机不能联网的情况下，优选地使用建立在本地的账户，将主账户的账户名和密码存储在本地，在用户登录主账户时，在本地即可完成主账户认证。

[0111] 步骤 S42：用户登录主账户；

[0112] 登录时需要通过主账户名、密码等认证。

[0113] 步骤 S43：判断登陆用户是否具有 root 权限。

[0114] 步骤 S44：用户打开手机中的应用程序 A，弹出应用程序 A 的注册页面。

[0115] 步骤 S45：用户在应用程序 A 的注册页面中输入欲注册使用的账户名，该欲注册使用的账户即为子账户。

[0116] 步骤 S46：用户请求生成密码，该请求中带有欲注册使用的子账户的名称。

[0117] 步骤 S47：终端生成密码，并将该密码与用户的主账户及子账户关联存储；

[0118] 优选地，可以存储在终端中的预设位置，该预设位置只有具有 root 权限的用户才可访问，以此保证密码的安全性。

[0119] 步骤 S48：用户使用该密码完成子账户的注册。

[0120] 优选地，在该步骤中，当终端接收到子密码后，可以在预设的显示区域显示该密码，以便用户进行使用；也可以直接填充到密码区域，而不显示出来，比如显示为黑点；或者当用户使用该密码当作密钥时，可直接使用该密码完成数据的加密。

[0121] 与上述终端生成密码的方法对应的获取密码的方法如图 5 所示，包括以下步骤：

[0122] 步骤 S51：用户成功登录主账户；

[0123] 步骤 S52：用户打开应用程序 A，执行登录操作，输入子账户名；

[0124] 步骤 S53：用户发送获取该应用程序(子账户)的密码的请求；获取密码的请求中携带有子账户的名称；

[0125] 步骤 S54：判断登陆用户是否具有 root 权限，若是，则继续执行步骤 S55；若否，则结束；

[0126] 步骤 S55：终端在预设位置查找得到该子账户对应的密码。

[0127] 步骤 S56：用户使用密码完成子账户的登录。

[0128] 优选地，在该步骤中，当终端接收到子账户的密码后，可以在预设的显示区域显示

该密码，以便用户进行使用；也可以直接填充到密码区域，而不显示出来，比如显示为黑点；或者当用户使用该密码当作密钥时，可直接使用该密码完成数据的解密。

[0129] 在本实施例中，在终端中实现了本发明提出的根据用户的请求自动生成密码及获取密码的方法，而且进一步地，将密码存储在需要 root 权限才能访问的位置，保证了密码的安全性。

[0130] 本发明提出的密码处理方法是将用户的某一应用的账户名作为主账户的子账户，当用户需要注册设置密码时，对应于用户在该应用程序中设置的账户名生成密码供用户使用，当用户使用该应用程序需要输入密码登录时，只需提供该应用程序中使用的账户名就能获得对应的密码。因此，免去了需要用户记忆密码的不便。

[0131] 相应地，如图 6 所示为本发明提出一种密码处理系统，包括移动终端 600：

[0132] 所述移动终端 600 包括：

[0133] 第一接收模块 601，用于接收用户发出的获取与第一账户关联存储的第二账户的密码的请求；

[0134] 第一获取密码模块 602，用于通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。

[0135] 所述移动终端还包括：

[0136] 第一设置密码模块，用于接收所述用户为所述第二账户设置的密码，或接收所述用户发出的生成所述第二账户的密码的请求，根据所述请求为所述第二账户生成密码；将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至本地预设路径。

[0137] 如图 7 所示，所述系统还包括服务器 700，

[0138] 所述服务器 700 包括：

[0139] 第二设置密码模块 701，用于接收所述用户为所述第二账户设置的密码，或接收所述用户发出的生成所述第二账户的密码的请求，根据所述请求为所述第二账户生成密码；将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至服务器。

[0140] 优选地，第一获取密码模块 602 用于：当所述第二账户、所述第二账户的密码以及所述第一账户关联存储至服务器时，将用户发出的获取与第一账户关联存储的第二账户的密码的请求发送至服务器，接收所述服务器返回的所述第二账户的密码；

[0141] 所述服务器还包括：

[0142] 第二获取密码模块 702，用于接收所述移动终端发送的获取与第一账户关联的第二账户的密码的请求，通过登陆成功的所述第一账户查找第二账户的密码，将查找到的第二账户的密码发送至移动终端。

[0143] 优选地，所述请求中包括密码的类型和 / 或强度。

[0144] 所述第一获取密码模块 602 还用于：将所述第二账户的密码显示在预设区域中；或者将所述第二账户的密码填充至密码输入区域中。

[0145] 所述移动终端还包括：

[0146] 登陆第一账户模块，用于接收并向服务器转发所述用户输入的登陆所述第一账户的请求，以便于所述服务器完成所述第一账户的登录；接收所述服务器返回的所述第一账户登录成功的指示消息；其中，所述登陆所述第一账户的请求中携带有所述第一账户的账户名和密码。

[0147] 本发明实施例还提出一种设备，所述设备包括：

[0148] 一个或多个处理器；

[0149] 存储器；和

[0150] 一个或多个模块(programs)，所述一个或多个模块存储于所述存储器中并被配置成由所述一个或多个处理器执行，其中，所述一个或多个模块具有如下功能：

[0151] 接收用户发出的获取与第一账户关联存储的第二账户的密码的请求；

[0152] 通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。

[0153] 优选地，所述一个或多个模块还可以包括如下功能：

[0154] 在所述接收用户发出的获取与第一账户关联存储的第二账户的密码的请求之前，接收所述用户为所述第二账户设置的密码，或接收所述用户发出的生成所述第二账户的密码的请求，根据所述请求为所述第二账户生成密码；将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至本地预设路径或服务器。

[0155] 优选地，所述请求中包括所述第二账户的密码的类型和/或强度。

[0156] 优选地，当所述第二账户、所述第二账户的密码以及所述第一账户关联存储至服务器时，所述通过成功登录的所述第一账户获取所述第二账户的密码包括：

[0157] 将用户发出的获取与第一账户关联存储的第二账户的密码的请求发送至服务器，以使服务器通过登陆成功的所述第一账户查找第二账户的密码；

[0158] 接收服务器返回的所述第二账户的密码。

[0159] 优选地，所述将所述第二账户的密码提供给所述用户，包括：

[0160] 将所述第二账户的密码显示在预设区域中；或者

[0161] 将所述第二账户的密码填充至密码输入区域中。

[0162] 优选地，所述一个或多个模块还可以包括如下功能：

[0163] 在通过成功登录的所述第一账户获取所述第二账户的密码的步骤之前，接收并向服务器转发所述用户输入的登陆所述第一账户的请求，以便于所述服务器完成所述第一账户的登录；

[0164] 接收所述服务器返回的所述第一账户登录成功的指示消息；

[0165] 其中，所述登陆所述第一账户的请求中携带有所述第一账户的账户名和密码。

[0166] 本发明实施例还提供了一种非易失性可读存储介质，该存储介质中存储有一个或多个模块(programs)，该一个或多个模块被应用在具有一个或多个处理器的设备时，可以使得该设备执行如下步骤的指令(instructions)：

[0167] 接收用户发出的获取与第一账户关联存储的第二账户的密码的请求；

[0168] 通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户。

[0169] 优选地，所述一个或多个模块还可以使得该设备执行如下步骤的指令：

[0170] 在所述接收用户发出的获取与第一账户关联存储的第二账户的密码的请求之前，接收所述用户为所述第二账户设置的密码，或接收所述用户发出的生成所述第二账户的密码的请求，根据所述请求为所述第二账户生成密码；将所述第二账户、所述第二账户的密码以及所述第一账户关联存储至本地预设路径或服务器。

[0171] 优选地，所述请求中包括所述第二账户的密码的类型和 / 或强度。

[0172] 优选地，当所述第二账户、所述第二账户的密码以及所述第一账户关联存储至服务器时，所述通过成功登录的所述第一账户获取所述第二账户的密码包括 ：

[0173] 将用户发出的获取与第一账户关联存储的第二账户的密码的请求发送至服务器，以使服务器通过登陆成功的所述第一账户查找第二账户的密码 ；

[0174] 接收服务器返回的所述第二账户的密码。

[0175] 优选地，所述将所述第二账户的密码提供给所述用户，包括 ：

[0176] 将所述第二账户的密码显示在预设区域中 ；或者

[0177] 将所述第二账户的密码填充至密码输入区域中。

[0178] 优选地，所述一个或多个模块还可以使得该设备执行如下步骤的指令 ：

[0179] 在通过成功登录的所述第一账户获取所述第二账户的密码的步骤之前，接收并向服务器转发所述用户输入的登陆所述第一账户的请求，以便于所述服务器完成所述第一账户的登录 ；

[0180] 接收所述服务器返回的所述第一账户登录成功的指示消息 ；

[0181] 其中，所述登陆所述第一账户的请求中携带有所述第一账户的账户名和密码。

[0182] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

[0183] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

[0184] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

[0185] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

[0186] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

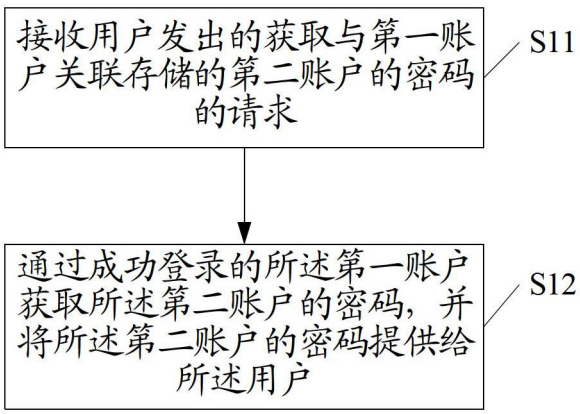

接收用户发出的获取与第一账户关联存储的第二账户的密码的请求
S11
通过成功登录的所述第一账户获取所述第二账户的密码，并将所述第二账户的密码提供给所述用户
S12

图 1

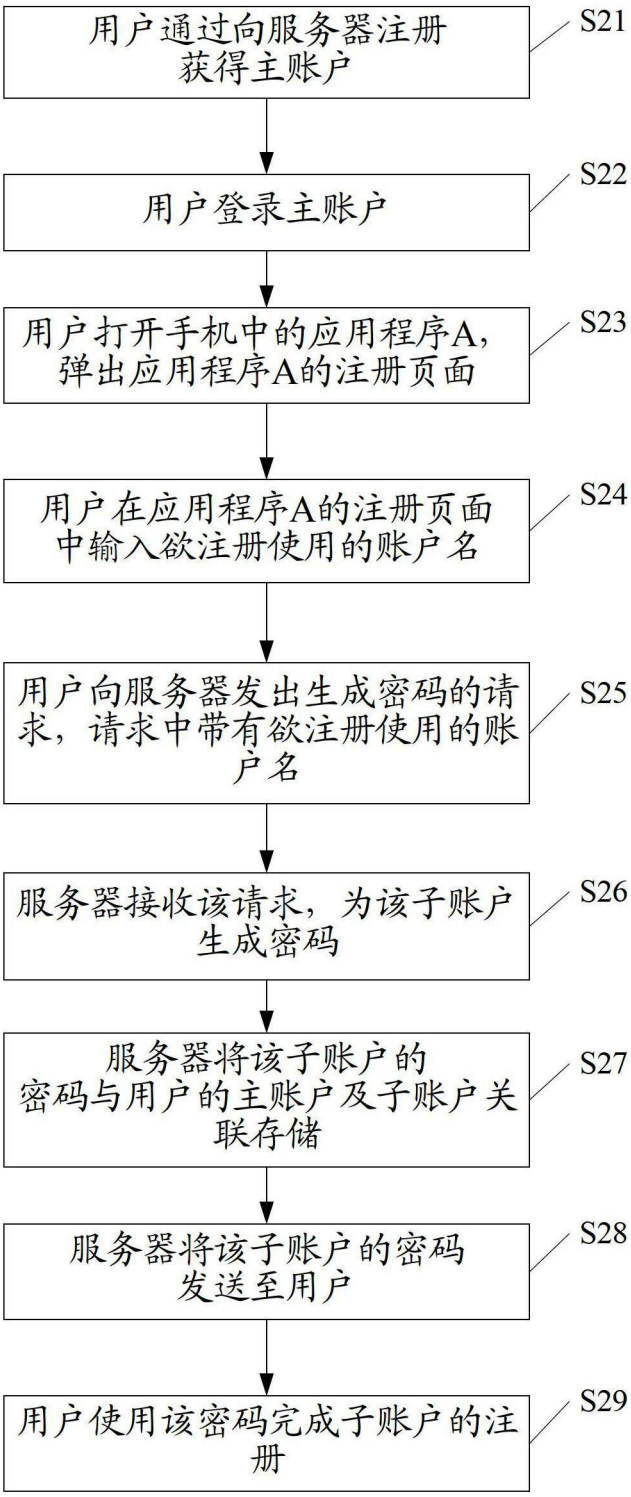

用户通过向服务器注册获得主账户
S21
用户登录主账户
S22
用户打开手机中的应用程序A，弹出应用程序A的注册页面
S23
用户在应用程序A的注册页面中输入欲注册使用的账户名
S24
用户向服务器发出生成密码的请求，请求中带有欲注册使用的账户名
S25
服务器接收该请求，为该子账户生成密码
S26
服务器将该子账户的密码与用户的主账户及子账户关联存储
S27
服务器将该子账户的密码发送至用户
S28
用户使用该密码完成子账户的注册
S29

图 2

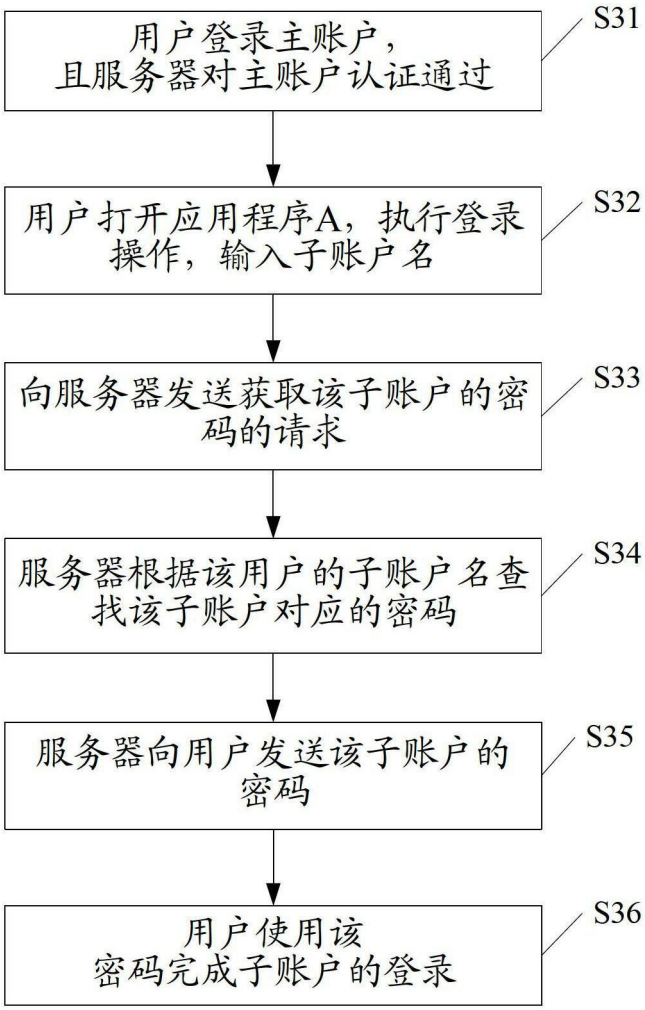

用户登录主账户，
且服务器对主账户认证通过
S31
用户打开应用程序A，执行登录
操作，输入子账户名
S32
向服务器发送获取该子账户的密
码的请求
S33
服务器根据该用户的子账户名查
找该子账户对应的密码
S34
服务器向用户发送该子账户的
密码
S35
用户使用该
密码完成子账户的登录
S36

图 3

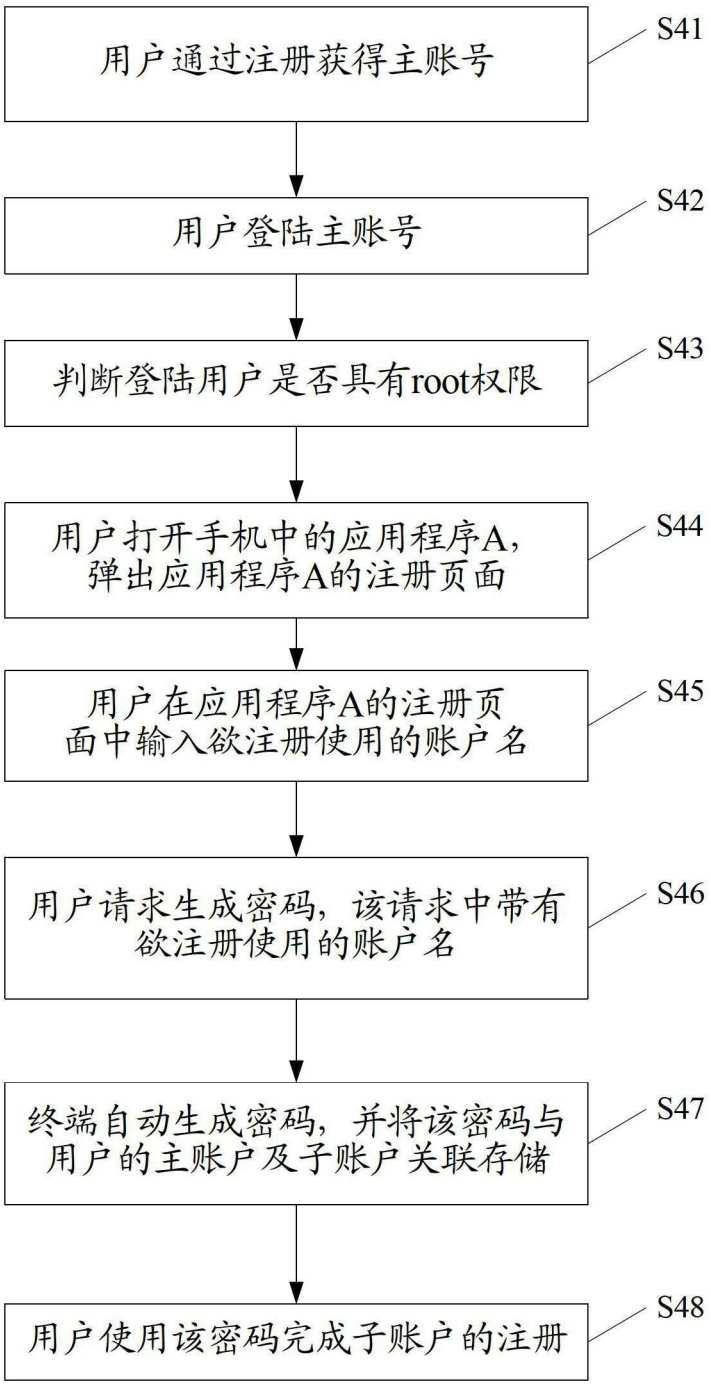

用户通过注册获得主账号
S41
用户登陆主账号
S42
判断登陆用户是否具有root权限
S43
用户打开手机中的应用程序A，
弹出应用程序A的注册页面
S44
用户在应用程序A的注册页
面中输入欲注册使用的账户名
S45
用户请求生成密码，该请求中带有
欲注册使用的账户名
S46
终端自动生成密码，并将该密码与
用户的主账户及子账户关联存储
S47
用户使用该密码完成子账户的注册
S48

图 4

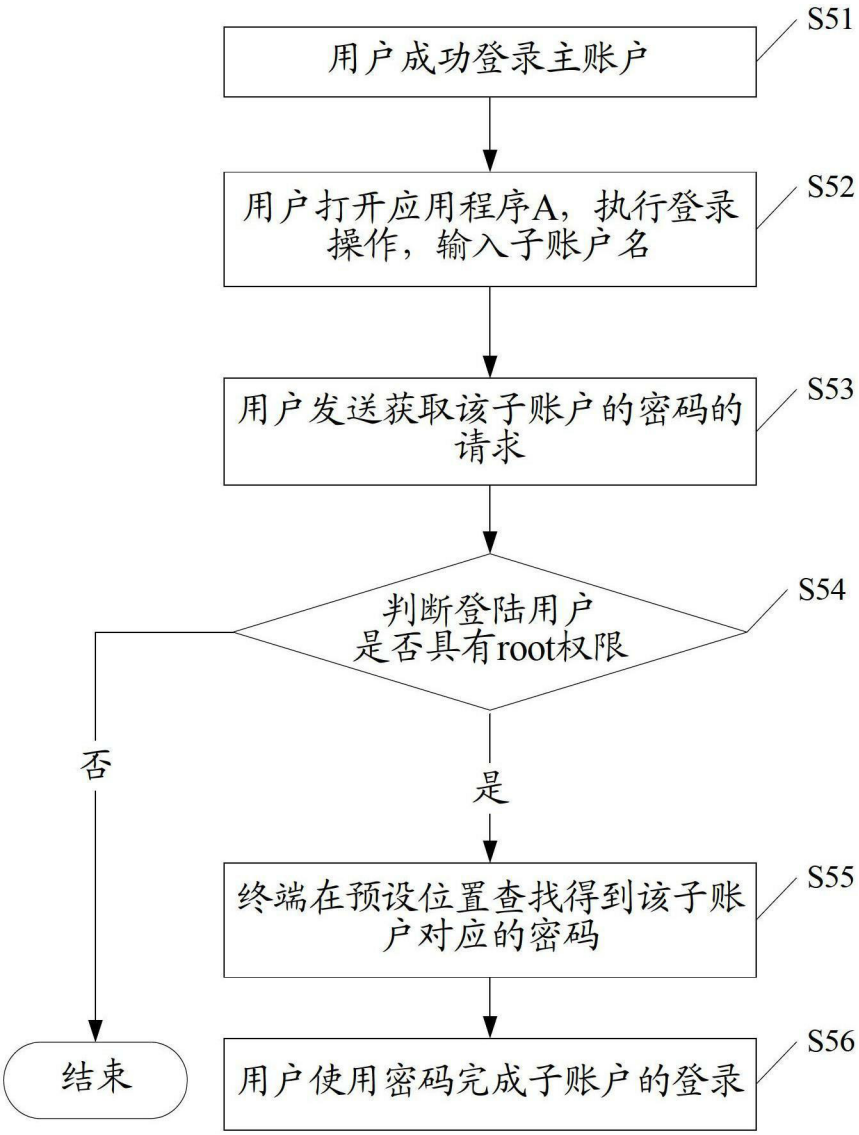

用户成功登录主账户
S51
用户打开应用程序A，执行登录操作，输入子账户名
S52
用户发送获取该子账户的密码的请求
S53
判断登陆用户是否具有root权限
S54
否
是
结束
终端在预设位置查找得到该子账户对应的密码
S55
用户使用密码完成子账户的登录
S56

图 5

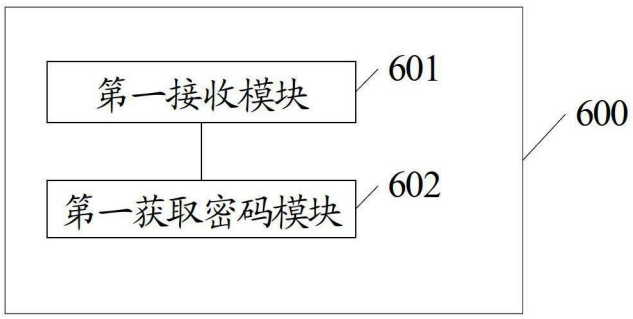

第一接收模块
601
第一获取密码模块
602
600

图 6

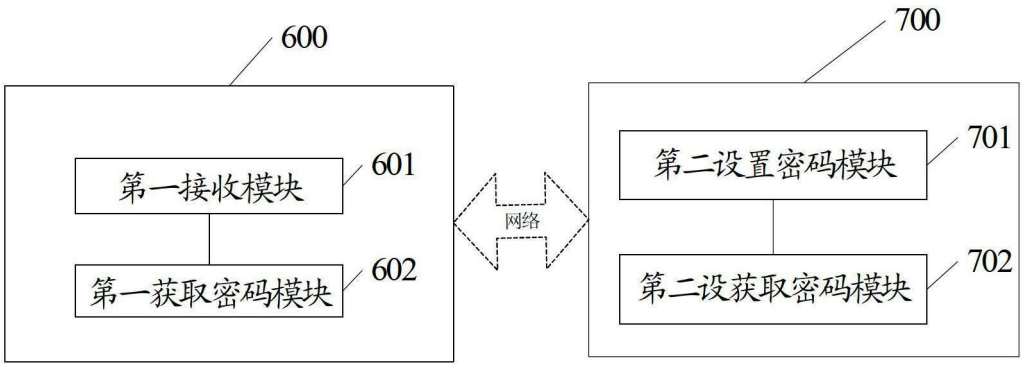

600
700
第一接收模块
601
第一获取密码模块
602
网络
第二设置密码模块
701
第二设获取密码模块
702

图 7