(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 103929312 A
(43)申请公布日 2014.07.16

(21)申请号 201410178720.7

(22)申请日 2014.04.29

(71)申请人 深圳市中兴移动通信有限公司
地址 518000 广东省深圳市南山区高新区北环大道9018号大族创新大厦A区10楼

(72)发明人 李琳

(74)专利代理机构 广东广和律师事务所 44298
代理人 章小燕

(51)Int.Cl.
H04L 9/32(2006.01)
G06F 21/31(2013.01)

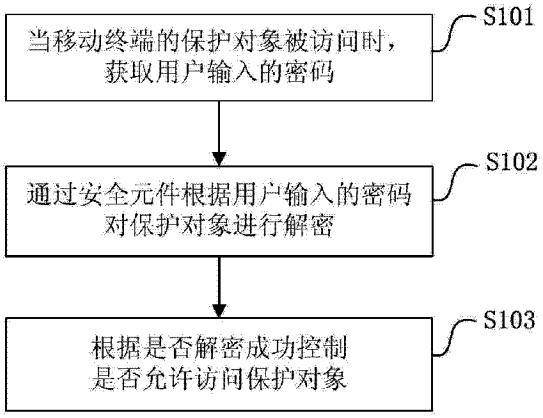
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种移动终端及其个人信息保护方法和系统

(57)摘要

本发明公开了一种移动终端及其个人信息保护方法和系统，属于移动终端领域。该方法包括：当移动终端的保护对象被访问时，获取用户输入的密码；通过安全元件根据用户输入的密码对保护对象进行解密；根据是否解密成功控制是否允许访问保护对象。采用本发明，将移动支付终端上的SE应用到用户个人信息的保护上，充分利用SE是具有高安全性的CPU加密机的特性对个人信息进行加密和解密，不仅能防止恶意软件获取个人信息，并且能在移动终端丢失或者被盗时，保护对象因被加密而不会被泄露，从而能提高用户个人信息的安全性。



CN 103929312 A

1. 一种个人信息保护方法，应用于包括安全元件的移动终端，其特征在于，所述方法包括：

当移动终端的保护对象被访问时，获取用户输入的密码；

通过所述安全元件根据所述用户输入的密码对所述保护对象进行解密；

根据是否解密成功控制是否允许访问所述保护对象。

2. 根据权利要求 1 所述的个人信息保护方法，其特征在于，所述方法之前还包括：

移动终端接收到用户预设的保护对象和密码后，通过所述安全元件建立参考签名信息，并对所述保护对象进行加密；

其中，所述参考签名信息包括加密密钥。

3. 根据权利要求 2 所述的个人信息保护方法，其特征在于，通过所述安全元件建立参考签名信息，并对所述保护对象进行加密包括：

安全元件接收移动终端传送的用户预设的保护对象和密码；

根据所述密码和预设的加密算法计算加密密钥，并建立参考签名信息存储在安全元件的存储空间；

根据所述参考签名信息对所述保护对象进行加密。

4. 根据权利要求 2 所述的个人信息保护方法，其特征在于，通过所述安全元件根据所述用户输入的密码对所述保护对象进行解密包括：

安全元件根据所述用户输入的密码和所述预设的加密算法计算解密密钥；判断所述解密密钥与所述参考签名信息的加密密钥是否配对，如果配对，则输出解密之后的保护对象，否则解密失败；或者

安全元件根据所述参考签名信息的加密密钥和预设的解密算法计算解密密码；判断所述解密密码与所述用户输入的密码是否配对，如果配对，则输出解密之后的保护对象，否则解密失败。

5. 根据权利要求 1 所述的个人信息保护方法，其特征在于，所述根据是否解密成功控制是否允许访问所述保护对象包括：当不允许访问所述保护对象时，隐藏所述保护对象、弹出要求用户输入密码或者无权访问的提示界面、以乱码的形式显示所述对象、和 / 或屏蔽所述对象的权限。

6. 根据权利要求 1-5 任意一项权利要求所述的个人信息保护方法，其特征在于，

所述被保护对象包括：文件夹、文件、存储空间、数据库、数据库中的数据、应用软件、和 / 或操作系统调度接口；

所述密码包括：符号、用户生物特征信息、或用户特定的体感动作。

7. 一种个人信息保护系统，其特征在于，所述个人信息保护系统包括访问控制装置和安全装置，其中：

所述访问控制装置，用于当移动终端的保护对象被访问时，获取用户输入的密码；以及根据所述安全装置解密是否成功控制是否允许访问所述保护对象；

所述安全装置，设置于安全元件上，包括用于根据所述用户输入的密码对所述保护对象进行解密的对象解密模块。

8. 根据权利要求 7 所述的个人信息保护系统，其特征在于，所述安全装置还包括：

参考签名信息建立模块，用于接收访问控制装置传送的用户预设保护对象和密码，根

据所述密码和预设的加密算法计算加密密钥，并建立参考签名信息存储在安全元件的存储空间；

对象加密模块，用于根据所述参考签名信息对所述保护对象进行加密。

9. 根据权利要求 7 所述的个人信息保护系统，其特征在于，所述对象解密模块具体用于：

根据所述用户输入的密码和所述预设的加密算法计算解密密钥；判断所述解密密钥与所述参考签名信息的加密密钥是否配对，如果配对，则输出解密之后的保护对象，否则解密失败；或者

根据所述参考签名信息的加密密钥和预设的解密算法计算解密密码；判断所述解密密码与所述用户输入的密码是否配对，如果配对，则输出解密之后的保护对象，否则解密失败。

10. 根据权利要求 7 所述的个人信息保护系统，其特征在于，所述访问控制装置还用于：当不允许访问所述保护对象时，隐藏所述保护对象、弹出要求用户输入密码或者无权访问的提示界面、以乱码的形式显示所述对象、和 / 或屏蔽所述对象的权限。

11. 一种移动终端，其特征在于，该移动终端包括权利要求 7-10 任意一项权利要求所述的个人信息保护系统。

一种移动终端及其个人信息保护方法和系统

技术领域

[0001] 本发明涉及移动通信技术领域，尤其涉及将 SE(Secure Element，安全元件）应用到个人信息安全性上的一种移动终端及其个人信息保护方法和系统。

背景技术

[0002] 随着移动终端的智能化和移动互联网的发展，移动终端逐渐成为人们生活中不可缺少的工具，用户的个人信息安全问题也日益成为人们关注的焦点。一方面，移动终端存储、链接到与个人信息相关的机构网络，各种各样的软件能够快速访问个人终端，获取个人信息，个人信息随时有泄露的风险。另一方面，在移动终端丢失或者被盗时，由于存储的信息是以明文的方式存储在移动中的存储空间，个人信息自然会被泄露。目前，现有技术没有很好地解决移动终端的用户个人信息安全性不高的问题。

发明内容

[0003] 有鉴于此，本发明要解决的技术问题是提供一种个人信息保护方法、装置和移动终端，以解决移动终端的用户个人信息安全性不高的技术问题。

[0004] 本发明解决上述技术问题所采用的技术方案如下：

[0005] 根据本发明的一个方面，提供的一种个人信息保护方法，应用于包括安全元件的移动终端，该方法包括：

[0006] 当移动终端的保护对象被访问时，获取用户输入的密码；

[0007] 通过安全元件根据用户输入的密码对保护对象进行解密；

[0008] 根据是否解密成功控制是否允许访问保护对象。

[0009] 优选的，该方法之前还包括：

[0010] 移动终端接收到用户预设的保护对象和密码后，通过安全元件建立参考签名信息，并对保护对象进行加密；其中，参考签名信息包括加密密钥。

[0011] 优选的，通过安全元件建立参考签名信息，并对保护对象进行加密包括：

[0012] 安全元件接收移动终端传送的用户预设的保护对象和密码；

[0013] 根据密码和预设的加密算法计算加密密钥，并建立参考签名信息存储在安全元件的存储空间；

[0014] 根据参考签名信息对保护对象进行加密。

[0015] 优选的，通过安全元件根据用户输入的密码对保护对象进行解密包括：

[0016] 安全元件根据用户输入的密码和预设的加密算法计算解密密钥；判断解密密钥与参考签名信息的加密密钥是否配对，如果配对，则输出解密之后的保护对象，否则解密失败；或者

[0017] 安全元件根据参考签名信息的加密密钥和预设的解密算法计算解密密码；判断解密密码与用户输入的密码是否配对，如果配对，则输出解密之后的保护对象，否则解密失败。

[0018] 优选的，根据是否解密成功控制是否允许访问保护对象包括：当不允许访问保护对象时，隐藏保护对象、弹出要求用户输入密码或者无权访问的提示界面、以乱码的形式显示对象、和 / 或屏蔽对象的权限。

[0019] 优选的，被保护对象包括：文件夹、文件、存储空间、数据库、数据库中的数据、应用软件、和 / 或操作系统调度接口；密码包括：符号、用户生物特征信息、或用户特定的体感动作。

[0020] 根据本发明的另一个方面，提供的一种个人信息保护系统包括访问控制装置和安全装置，其中：

[0021] 访问控制装置，用于当移动终端的保护对象被访问时，获取用户输入的密码；以及根据安全装置解密是否成功控制是否允许访问保护对象；

[0022] 安全装置，设置于安全元件上，包括用于根据用户输入的密码对保护对象进行解密的对象解密模块。

[0023] 优选的，安全装置还包括：

[0024] 参考签名信息建立模块，用于接收访问控制装置传送的用户预设保护对象和密码，根据密码和预设的加密算法计算加密密钥，并建立参考签名信息存储在安全元件的存储空间；

[0025] 对象加密模块，用于根据参考签名信息对保护对象进行加密。

[0026] 优选的，对象解密模块具体用于：

[0027] 根据用户输入的密码和预设的加密算法计算解密密钥；判断解密密钥与参考签名信息的加密密钥是否配对，如果配对，则输出解密之后的保护对象，否则解密失败；或者

[0028] 根据参考签名信息的加密密钥和预设的解密算法计算解密密码；判断解密密码与用户输入的密码是否配对，如果配对，则输出解密之后的保护对象，否则解密失败。

[0029] 优选的，访问控制装置还用于：当不允许访问保护对象时，隐藏保护对象、弹出要求用户输入密码或者无权访问的提示界面、以乱码的形式显示对象、和 / 或屏蔽对象的权限。

[0030] 根据本发明的再一个方面，提供的一种移动终端包括上述技术方案中的个人信息保护系统。

[0031] 本发明提供的移动终端及其个人信息保护方法和系统，将移动支付终端上的 SE 应用到用户个人信息的保护上，充分利用 SE 是具有高安全性的 CPU 加密机的特性对需要保护的个人信息进行加密和解密，不仅能防止恶意软件获取个人信息，并且能在移动终端丢失或者被盗时，保护对象因被加密而不会被泄露，从而能提高用户个人信息的安全性。

附图说明

[0032] 图 1 为本发明实施例提供的一种个人信息保护方法的流程图。

[0033] 图 2 为本发明优选实施例提供的一种个人信息保护方法的流程图。

[0034] 图 3 为本发明实施例提供的一种个人信息保护系统的模块结构图。

具体实施方式

[0035] 为了使本发明所要解决的技术问题、技术方案及有益效果更加清楚、明白，以下结

合附图和实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0036] 实施例一

[0037] 如图 1 所示，本发明实施例提供的一种个人信息保护方法，应用于包括安全元件的移动终端，该方法包括：

[0038] S101、当移动终端的保护对象被访问时，获取用户输入的密码。

[0039] 具体的，保护对象是加密过的文件，以密文的方式存储在移动终端的存储空间的，当用户访问保护对象时，移动终端通过人机界面提示用户输入密码作为保护对象访问的解密密码。用户输入的密码包括但不限于以下任一种：一是用户在界面上输入相应符号作为密码；二是通过移动终端的传感器采集用户的生物特征信息，提取生物特征信息的关键特征信息作为密码，三是移动终端的传感器采集用户特定的体感动作（如手势动作），提取体感动作关键特征信息作为密码。安全元件接收到预设的密码后，根据预设的加密算法计算加密密钥，并建立参考签名信息存储在安全元件存储空间内。

[0040] S102、通过安全元件根据用户输入的密码对保护对象进行解密。

[0041] 具体的，移动终端将保护对象和用户输入的密码传送到安全元件，比如可以通过 NFC(Near Field Communication) 通道或其他方式传送，NFC 通道是可以用于建立移动终端 CPU 和 SE 之间信息交互的通道，安全元件接收到保护对象和用户输入的密码后，可以通过两种方式进行解密：

[0042] 方式一、安全元件根据用户输入的密码和预设的加密算法计算解密密钥；判断解密密钥与保护对象的加密密钥是否配对，如果配对，则输出解密之后的保护对象，保护对象以明文的方式输出给移动终端进行存储、传输和链接，否则解密失败。

[0043] 方式二、安全元件根据保护对象的加密密钥和预设的解密算法计算解密密码；判断解密密码与用户输入的密码是否配对，如果配对，则输出解密之后的保护对象，保护对象以明文的方式存储、传输和链接，否则解密失败。

[0044] S103、根据是否解密成功控制是否允许访问保护对象。

[0045] 具体的，当安全元件解密成功时，输出解密之后的保护对象，移动终端允许用户访问保护对象，以明文的方式传输和链接保护对象；当安全元件解密失败时，输出解密失败的信息，对象移动终端不允许用户访问保护对象。作为一种优选的方案，当不允许访问保护对象时，隐藏保护对象、弹出要求用户输入密码或者无权访问的提示界面、以乱码的形式显示对象、和 / 或屏蔽对象的权限。

[0046] 上述保护对象包括但不限于文件夹、文件、存储空间、数据库、数据库中的数据、应用软件、操作系统调度接口等，且其可以是移动终端出厂时就预设的，也可以是出厂后由用户自行标识和选择的。

[0047] 实施例二

[0048] 如图 2 所示，本发明优选实施例提供的一种个人信息保护方法包括：

[0049] S201、移动终端接收用户预设的保护对象和密码。

[0050] 具体的，当移动终端开启个人信息保护功能时，用户可以在预设的操作目录下进行预设密码。保护对象可以是移动终端出厂时就预设的，也可以是出厂之后，用户自由标识和选择的需要保护的对象。预设密码的方式可以是以下任一种：一是用户在界面上输入相

应符号作为加密密码；二是通过移动终端的传感器采集用户的生物特征信息，提取生物特征信息的关键特征信息作为加密密码，三是移动终端的传感器采集用户特定的手势动作，提取关键特征信息作为加密密码，移动终端接收到用户预设的保护对象和密码后，将其传送给安全元件进行加密。

[0051] S202、通过安全元件建立参考签名信息，并对保护对象进行加密。

[0052] 具体的，安全元件接收移动终端传送的用户预设的保护对象和密码后，根据密码和预设的加密算法计算加密密钥，并建立参考签名信息存储在安全元件的存储空间，然后根据加密密钥对保护对象进行加密。其中，参考签名信息包括加密密钥，为了让用户能对不同的保护对象设置不同的密码，进一步提高安全性，参考签名信息还可以包括保护对象标识，安全元件可以根据参考签名信息的保护对象对应的加密密钥对用户标识或者输入的保护对象进行加密，并输出加密后的保护对象，加密后的保护对象以密文的形式静态或者动态地存储在移动终端存储器内。

[0053] S203、当移动终端的保护对象被访问时，获取用户输入的密码。

[0054] S204、根据用户输入的密码对保护对象进行解密。

[0055] 具体的，本步骤可以采用两种方式进行：

[0056] 方式一、安全元件根据用户输入的密码和预设的加密算法计算解密密钥；判断解密密钥与参考签名信息的加密密钥是否配对，如果配对，则输出解密之后的保护对象，否则解密失败。

[0057] 方式二、安全元件根据参考签名信息的加密密钥和预设的解密算法计算解密密码；判断解密密码与用户输入的密码是否配对，如果配对，则输出解密之后的保护对象，否则解密失败。

[0058] S205、判断是否解密成功，如果是，则执行步骤 S206，否则执行步骤 S207。

[0059] S206、允许访问保护对象，转至步骤 S208。

[0060] S207、不允许访问保护对象。

[0061] S208、结束流程。

[0062] 上述保护对象包括但不限于文件夹、文件、存储空间、数据库、数据库中的数据、应用软件、操作系统调度接口等，且其可以是移动终端出厂时就预设的，也可以是出厂后由用户自行标识和选择的。密码包括但不限于符号、用户生物特征信息、或用户特定的体感动作。

[0063] 实施例三

[0064] 如图 3 所示，本发明优选实施例提供的一种个人信息保护系统包括访问控制装置 10 和安全装置 20，其中：

[0065] 访问控制装置 10，用于当移动终端的保护对象被访问时，获取用户输入的密码；以及根据安全装置解密是否成功控制是否允许访问保护对象；

[0066] 安全装置 20，设置于安全元件上，包括用于根据用户输入的密码对保护对象进行解密的对象解密模块 203。

[0067] 作为一种优选的方案，安全装置 20 还包括参考签名信息建立模块 201 和对象加密模块 202，其中：

[0068] 参考签名信息建立模块 201，用于接收访问控制装置传送的用户预设保护对象和

密码，根据密码和预设的加密算法计算加密密钥，并建立参考签名信息存储在安全元件的存储空间；其中，参考签名信息包括加密密钥。

[0069] 对象加密模块 202，用于根据参考签名信息对保护对象进行加密。

[0070] 作为一种优选的方案，对象解密模块 20 具体用于：

[0071] 对象解密模块 20 根据用户输入的密码和预设的加密算法计算解密密钥；判断解密密钥与参考签名信息的加密密钥是否配对，如果配对，则输出解密之后的保护对象，否则解密失败；或者

[0072] 对象解密模块 20 根据参考签名信息的加密密钥和预设的解密算法计算解密密码；判断解密密码与用户输入的密码是否配对，如果配对，则输出解密之后的保护对象，否则解密失败。

[0073] 作为另一种优选的方案，访问控制装置 10 还用于：当不允许访问保护对象时，隐藏保护对象、弹出要求用户输入密码或者无权访问的提示界面、以乱码的形式显示对象、或屏蔽对象的权限。

[0074] 上述保护对象包括但不限于文件夹、文件、存储空间、数据库、数据库中的数据、应用软件、操作系统调度接口等，且其可以是移动终端出厂时就预设的，也可以是出厂后由用户自行标识和选择的。密码包括但不限于符号、用户生物特征信息、或用户特定的体感动作。

[0075] 需要说明的是，上述方法实施例一和二中的技术特征在本实施例的系统中均对应适用，这里不再重述。

[0076] 实施例四

[0077] 本发明还提供了一种移动终端，该移动终端包括 SE，还包括上述实施例三中的个人信息保护系统。

[0078] 具体来说，移动终端开启保护个人信息的功能时，移动终端在预设的操作目录下，提示用户预设密码并标识或者输入相应的需要保护的对象（保护对象也可以出厂时设置），移动终端的访问控制装置将待保护对象输入到 SE 的对象加密模块进行加密，SE 输出加密后的保护对象以密文的形式存储、传输和链接。当用户需要访问被加密的保护对象时，再次提示用户输入密码，其中，接收到的用户输入的密码可能与预设的密码一致，也可能与预设的密码不一致，移动终端接收到用户密码后，将用户输入的密码和被加密的保护对象输入到 SE 的对象解密模块进行解密。当用户密码正确时，SE 输出解密后的保护对象以明文传递给移动终端，移动终端对解密后的明文对象进行显示和传输等操作；当用户密码不正确时，解密失败，移动终端不允许用户访问该保护对象。当不允许用户访问时，当不允许访问保护对象时，隐藏保护对象、弹出要求用户输入密码或者无权访问的提示界面、以乱码的形式显示对象、或屏蔽对象的权限。

[0079] 本发明提供的移动终端及其个人信息保护方法和系统，将移动支付终端上的 SE 应用到用户个人信息的保护上，充分利用 SE 是具有高安全性的 CPU 加密机的特性对需要保护的个人信息进行加密和解密，不仅能防止恶意软件获取个人信息，并且能在移动终端丢失或者被盗时，保护对象因被加密而不会被泄露，从而能提高用户个人信息的安全性。

[0080] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来控制相关的硬件完成，所述的程序可以在存储于一计算机可读取存储介质中，

所述的存储介质，如 ROM/RAM、磁盘、光盘等。

[0081] 以上参照附图说明了本发明的优选实施例，并非因此局限本发明的权利范围。本领域技术人员不脱离本发明的范围和实质，可以有多种变型方案实现本发明，比如作为一个实施例的特征可用于另一实施例而得到又一实施例。凡在运用本发明的技术构思之内所作的任何修改、等同替换和改进，均应在本发明的权利范围之内。

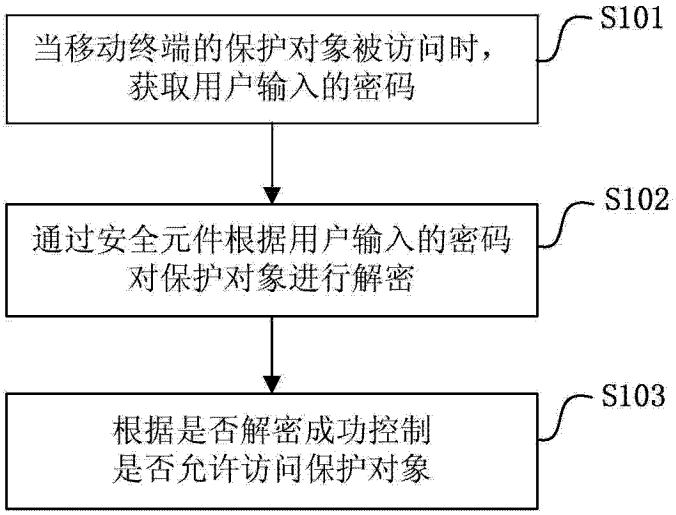

当移动终端的保护对象被访问时，
获取用户输入的密码
S101
通过安全元件根据用户输入的密码
对保护对象进行解密
S102
根据是否解密成功控制
是否允许访问保护对象
S103

图 1

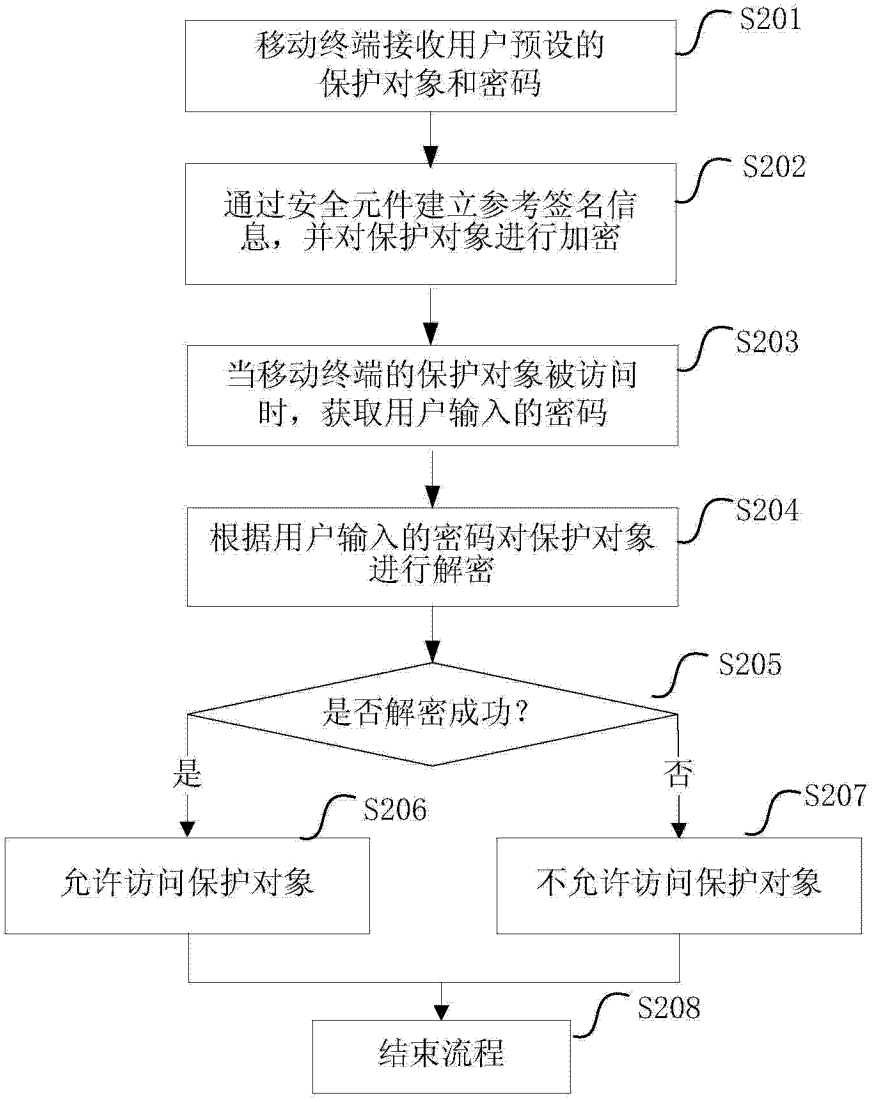

移动终端接收用户预设的保护对象和密码
S201
通过安全元件建立参考签名信息，并对保护对象进行加密
S202
当移动终端的保护对象被访问时，获取用户输入的密码
S203
根据用户输入的密码对保护对象进行解密
S204
是否解密成功？
S205
是
否
允许访问保护对象
S206
不允许访问保护对象
S207
结束流程
S208

图 2

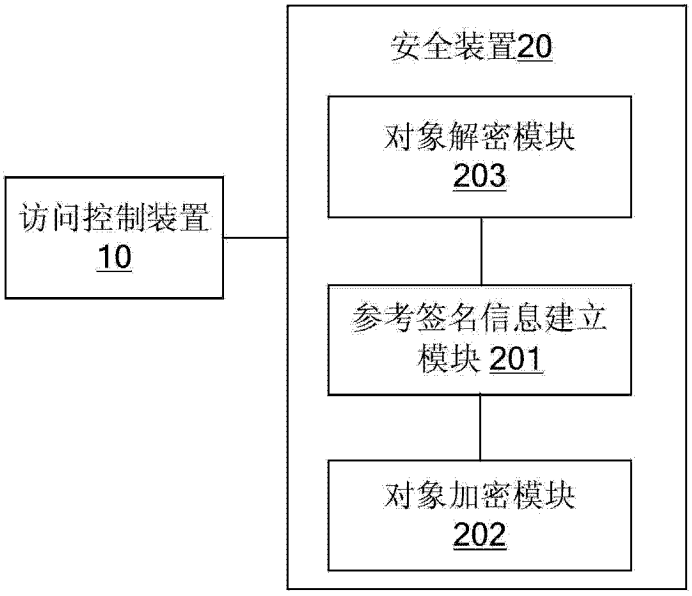


图 3