[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/32
H04L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 200410058214.0

[43] 公开日 2005 年 12 月 28 日

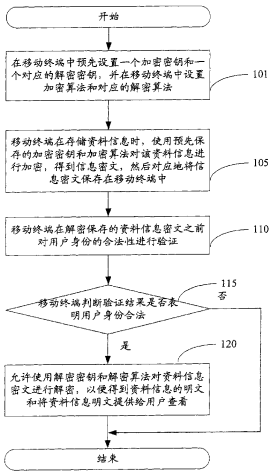
[11] 公开号 CN 1713756A

[22] 申请日 2004.8.17
[21] 申请号 200410058214.0
[30] 优先权
[32] 2004.6.23 [33] CN [31] 200410049696.3
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 王正伟 吴古政
[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 罗正云 宋志强
权利要求书 5 页 说明书 17 页 附图 4 页

[54] 发明名称 一种移动终端内存储的资料信息的安全保障方法

[57] 摘要

本发明公开了一种移动终端内存储的资料信息的安全保障方法。 在该方法中，首先在移动终端中设置一个加密密钥和一个对应的解密密钥，并设置一个加密算法和一个对应的解密算法。 移动终端在接收到用户输入的资料信息后，通过加密密钥和加密算法对用户输入的资料信息进行加密，然后将加密后的信息密文存储在移动终端中。 当用户希望查看移动终端内存储的资料信息时，首先对移动终端的用户身份进行合法性验证；如果通过合法性验证，则允许通过解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，否则不允许对信息密文进行解密。 通过本发明可以保证移动终端内存储的资料信息只提供给合法用户查看，从而保障了资料信息的安全性。



ISSN1008-4274

1. 一种移动终端内存储的资料信息的安全保障方法，至少包括如下步骤：

a. 在移动终端中设置一个加密密钥和一个对应的解密密钥，并设置一个加密算法和一个对应的解密算法；

b. 在接收到用户输入的资料信息后，通过所述加密密钥和加密算法对所述资料信息进行加密，然后将加密后的信息密文存储在移动终端中；

c. 在解密信息密文之前对移动终端的用户身份进行合法性验证；如果通过合法性验证，允许通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，否则结束本流程。

2. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，该方法进一步包括在一个验证设备中保存一个对应于该移动终端的验证密钥和移动终端信息之间的对应关系，并在该移动终端中保存所述验证密钥，步骤 c 所述对移动终端的用户身份进行合法性验证包括：

移动终端向验证设备发送一个用于获取验证设备中保存的验证密钥的验证请求消息，所述请求消息包含移动终端信息；

验证设备根据移动终端信息获取保存的对应于该移动终端的验证密钥，并将所述验证密钥返回给移动终端；

移动终端判断接收自验证设备的验证密钥和自身保存的验证密钥是否一致。

3. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，该方法进一步包括在一个验证设备中保存一个对应于该移动终端的验证密钥和移动终端信息之间的对应关系，并在该移动终端中保存所述验证密钥，步骤 c 所述对移动终端的用户身份进行合法性验证包括：

移动终端向验证设备发送一个用于获取验证设备中保存的验证密钥的验证请求消息，所述请求消息包含移动终端信息和一个随机数；

验证设备根据移动终端信息获取保存的对应于该移动终端的验证密钥，并

对获取的验证密钥和得到的随机数进行计算，将计算结果发送给移动终端；

移动终端对自身生成的随机数和自身保存的验证密钥进行相同或对应的计算，得到一个计算结果；

移动终端判断接收自验证设备的计算结果和自身得到的计算结果是否相同或者满足预定对应关系。

4. 根据权利要求 2 或 3 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述移动终端信息是移动终端内部的用户识别卡信息。

5. 根据权利要求 2 或 3 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述移动终端信息是移动终端特征信息。

6. 根据权利要求 5 所述的移动终端内存储的资料信息的安全保障方法，其特征是，进一步包括验证设备在接收到一个停止移动终端服务通知后，删除对应于该移动终端的验证密钥和移动终端信息之间的对应关系或锁定对所述对应关系的访问操作。

7. 根据权利要求 2 或 3 所述的移动终端内存储的资料信息的安全保障方法，其特征是，进一步包括在移动终端中设置一个访问控制密码的步骤，在步骤 c 之前进一步包括判断移动终端是否能够连接到网络，如果能连接到网络，直接执行步骤 c，否则执行下述步骤：

移动终端提示用户输入访问控制密码，并在接收到用户输入的访问控制密码后，通过比较用户输入的访问控制密码和移动终端预先保存的访问控制密码确定用户输入是否正确，如果正确，允许通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，否则结束本流程。

8. 根据权利要求 2 或 3 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述验证设备是归属位置寄存器 HLR、鉴权中心 AC 和设备识别寄存器 EIR 中的一种。

9. 根据权利要求 2 或 3 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述验证设备是电子钥匙，该方法进一步包括在移动终端和电子钥

匙中分别设置一个无线收发模块，移动终端和电子钥匙通过该无线收发模块建立无线通信连接。

10. 根据权利要求 2 或 3 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述验证设备是电子钥匙，该方法进一步包括在移动终端和电子钥匙中分别设置一个数据通信线接口，移动终端和电子钥匙通过连接在所述两个接口之间的数据通信线建立有线通信连接。

11. 根据权利要求 2 或 3 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述验证设备是用户卡，在验证设备向移动终端返回信息之前进一步包括：验证用户卡自身的合法性，如果验证通过，则执行向移动终端返回信息的步骤，否则，直接结束本流程，或者返回一个失败信息，然后结束本流程。

12. 根据权利要求 11 所述的移动终端内存储的资料信息的安全保障方法，其特征是，进一步包括在用户卡和网络侧相关设备中保存一个业务密钥，所述验证用户卡自身的合法性包括：

用户卡产生一个随机数，然后发送给网络侧相关设备；

网络侧相关设备根据随机数和自己保存的业务密钥进行计算，得到一个计算结果，然后将该计算结果返回给用户卡；

用户卡根据随机数和自己保存的业务密钥进行相应的计算，得到一个计算结果，并比较自己计算得到的结果和来自网络侧相关设备的计算结果是否一致。

13. 根据权利要求 12 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述业务密钥是用户卡的根密钥。

14. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，进一步包括移动终端在接收到来自移动通信网络的一个停止服务通知后，禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，并锁定保存在移动终端内存中的已经解密的资料信息的明文。

15. 根据权利要求 14 所述的移动终端内存储的资料信息的安全保障方法，

其特征是，移动通信网络在向移动终端发送一个停止服务通知后进一步包括：在判断出所述通知没有被移动终端所接收时，移动通信网络保存所述通知并在移动终端重新登陆网络后发送所述通知。

16. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，该方法进一步包括在移动终端中设置一个访问控制密码，并进一步包括移动终端在接收到表示该短消息是一个用于禁止进行解密并携带有访问控制密码的命令短消息后，判断所述访问控制密码和自己保存的访问控制密码是否相同，如果是，禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，并锁定保存在移动终端内存中的已经解密的资料信息的明文，否则不执行任何处理。

17. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，进一步包括移动终端在和网络的连接断开预定时间之后，禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，并锁定保存在移动终端内存中的已经解密的资料信息的明文；移动终端在重新登陆网络后允许通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，并解锁保存在移动终端内存中的已经解密的资料信息的明文。

18. 根据权利要求 1 或 17 所述的移动终端内存储的资料信息的安全保障方法，其特征是，该方法进一步包括在移动终端中设置一个访问控制密码，在禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文之前或之后进一步包括：

移动终端提示用户输入访问控制密码，并在接收到用户输入的访问控制密码后，通过比较用户输入的访问控制密码和移动终端预先保存的访问控制密码确定用户输入是否正确，如果正确，允许通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，否则执行禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文或者直接关闭移动终端的步骤。

19. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，进一步包括在移动终端中设置一个访问控制密码的步骤，步骤 c 所述对移动终端的用户身份进行合法性验证包括:

移动终端提示用户输入访问控制密码，并在接收到用户输入的访问控制密码后，比较用户输入的访问控制密码和移动终端预先保存的访问控制密码是否相同。

20. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述步骤 c 是在移动终端开机之后进行，或者是在移动终端连接到网络之后进行，或者是在接收到用户读取存储在移动终端的资料信息的指令后进行。

21. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述加密密钥和解密密钥保存在一个单独设置的位于移动终端内的集成电路 IC 芯片中。

22. 根据权利要求 1 所述的移动终端内存储的资料信息的安全保障方法，其特征是，所述加密算法和解密算法由一个单独设置的位于移动终端内的 IC 芯片实现，或者由移动终端程序实现。

一种移动终端内存储的资料信息的安全保障方法

技术领域

本发明涉及无线通信的信息安全技术，具体涉及一种移动终端内存储的资料信息的安全保障方法。

背景技术

随着诸如移动电话等移动终端应用越来越广泛，在移动终端上保存的信息也越来越丰富多样，例如为了拨打电话的方便，用户经常在移动电话上保存有电话簿信息，该电话簿里存储了和用户相关的家人、亲人、朋友等的电话号码和其他联系方式。除了电话号码信息之外，移动电话上还可能存储有普通短消息（SMS）或多媒体短消息（MMS），并且，在带有摄像头的移动电话上还可能保存有用户拍摄的图片或视频，在具有个人助理功能的移动电话上还保存有用户的一些其它资料信息，这些信息的存储给用户带来了工作和生活上的方便。移动终端中保存的以上这些信息一般都是用户的一些隐私信息，用户一般不希望这些信息泄漏给他人。但是，所有的这些信息目前都是直接保存在移动终端上的，没有经过任何加密措施。

而我们知道，目前移动电话因为疏忽或者被盗抢而丢失的情况比比皆是，一旦其它人得到了用户的移动电话，那么可以轻易地得到移动电话里储存的例如电话号码、SMS、MMS、图片或视频等等信息。由于这些信息绝大多数都是用户的隐私，这些信息一旦被暴露，用户可能因此蒙受物质上的巨大损失和精神上的巨大伤害，因此用户不希望这些信息被别人知晓，特别是不熟悉的人所知晓。但是，目前由于没有任何针对移动终端内部信息的加密措施或者安全保障措施，因此由于用户隐私的泄漏而对用户造成影响的情况依然时有发生。这不但给移动终端的用户带来了消极影响，也阻碍了移动

终端中更多需要得到信息安全保障的功能的开发。因此，如何保障移动终端内部存储的信息的安全性，成为目前一个迫切需要解决的问题。

发明内容

有鉴于此，本发明的主要目的是提供一种移动终端内存储的资料信息的安全保障方法，以有效保障移动终端内部信息的安全，避免移动终端内部信息的泄漏给用户造成的物质上的损失和精神上的伤害。

本发明的上述目的是通过如下的技术方案予以实现的：

一种移动终端内存储的资料信息的安全保障方法，至少包括如下步骤：

a. 在移动终端中设置一个加密密钥和一个对应的解密密钥，并设置一个加密算法和一个对应的解密算法；

b. 在接收到用户输入的资料信息后，通过加密密钥和加密算法对资料信息进行加密，然后将加密后的信息密文存储在移动终端中；

c. 在解密信息密文之前对移动终端的用户身份进行合法性验证；如果通过合法性验证，允许通过解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，否则结束本流程。

上述方法可以进一步包括在一个验证设备中保存一个对应于该移动终端的验证密钥和移动终端信息之间的对应关系，并在该移动终端中保存所述验证密钥，步骤 c 中对移动终端的用户身份进行合法性验证包括：

移动终端向验证设备发送一个用于获取验证设备中保存的验证密钥的验证请求消息，所述请求消息包含移动终端信息；

验证设备根据移动终端信息获取保存的对应于该移动终端的验证密钥，并将所述验证密钥返回给移动终端；

移动终端判断接收自验证设备的验证密钥和自身保存的验证密钥是否一致。

或者，步骤 c 中对移动终端的用户身份进行合法性验证包括：

移动终端向验证设备发送一个用于获取验证设备中保存的验证密钥的验证

请求消息，所述请求消息包含移动终端信息和一个随机数；

验证设备根据移动终端信息获取保存的对应于该移动终端的验证密钥，并对获取的验证密钥和得到的随机数进行计算，将计算结果发送给移动终端；

移动终端对自身生成的随机数和自身保存的验证密钥进行相同或对应的计算，得到一个计算结果；

移动终端判断接收自验证设备的计算结果和自身得到的计算结果是否相同或者满足预定对应关系。

上述验证设备可以是归属位置寄存器，可以是鉴权中心，也可以是设备识别寄存器。

上述验证设备还可以是电子钥匙，此时该方法进一步包括在移动终端和电子钥匙中分别设置一个无线收发模块，移动终端和电子钥匙通过该无线收发模块建立无线通信连接；或者该方法进一步包括在移动终端和电子钥匙中分别设置一个数据通信线接口，移动终端和电子钥匙通过连接在所述两个接口之间的数据通信线建立有线通信连接。

上述验证设备还可以是用户卡，此时在验证设备向移动终端返回信息之前进一步包括：验证用户卡自身的合法性，如果验证通过，则执行向移动终端返回信息的步骤，否则，直接结束本流程，或者返回一个失败信息，然后结束本流程。这里验证用户卡自身的合法性包括：

用户卡产生一个随机数，然后发送给网络侧相关设备；

网络侧相关设备根据随机数和自己保存的业务密钥进行计算，得到一个计算结果，然后将该计算结果返回给用户卡；

用户卡根据随机数和自己保存的业务密钥进行相应的计算，得到一个计算结果，并比较自己计算得到的结果和来自网络侧相关设备的计算结果是否一致。

上述业务密钥较佳地是用户卡的根密钥，也就是 AK 或者 AKEY 信息。

这里的移动终端信息是诸如国际移动用户识别（IMSI）信息的移动终端内部的用户识别卡信息或者是诸如国际移动设备识别（IMEI）信息的移动终端特

征信息。在后一种情况下，该方法进一步包括验证设备在接收到一个停止移动终端服务通知后，删除对应于该移动终端的验证密钥和移动终端信息之间的对应关系或锁定对所述对应关系的访问操作。

在使用验证设备判断用户身份合法性的情况下，可以进一步包括在移动终端中设置一个访问控制密码的步骤，在步骤 c 之前进一步包括判断移动终端是否能够连接到网络，如果能连接到网络，直接执行步骤 c，否则执行下述步骤：

移动终端提示用户输入访问控制密码，并在接收到用户输入的访问控制密码后，通过比较用户输入的访问控制密码和移动终端预先保存的访问控制密码确定用户输入是否正确，如果正确，允许通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，否则结束本流程。

另外，移动终端在接收到来自移动通信网络的一个停止服务通知后，禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，并锁定保存在移动终端内存中的已经解密的资料信息的明文。如果移动通信网络得知通知没有被移动终端所接收时，移动通信网络保存通知并在移动终端重新登陆网络后发送该通知。

另外也可以在移动终端中设置一个访问控制密码，并进一步包括移动终端在接收到表示该短消息是一个用于禁止进行解密并携带有访问控制密码的命令短消息后，判断所述访问控制密码和自己保存的访问控制密码是否相同，如果是，禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，并锁定保存在移动终端内存中的已经解密的资料信息的明文，否则不执行任何处理。

在移动终端在和网络的连接断开预定时间之后，移动终端禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，并锁定保存在移动终端内存中的已经解密的资料信息的明文；移动终端在重新登陆网络后允许通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，并解锁保存在移动终端内存中的已经解密的资料信息的明文。

在这种情况下，该方法进一步包括在移动终端中设置一个访问控制密码，在禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文之前或之后进一步包括：

移动终端提示用户输入访问控制密码，并在接收到用户输入的访问控制密码后，通过比较用户输入的访问控制密码和移动终端预先保存的访问控制密码确定用户输入是否正确，如果正确，允许通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文，否则执行禁止通过所述解密密钥和解密算法对信息密文进行解密以得到资料信息的明文或者直接关闭移动终端的步骤。

除了通过验证设备来验证用户身份之外，可以通过访问控制密码来进行验证，此时进一步包括在移动终端中设置一个访问控制密码的步骤，步骤 c 中对移动终端的用户身份进行合法性验证包括：

移动终端提示用户输入访问控制密码，并在接收到用户输入的访问控制密码后，比较用户输入的访问控制密码和移动终端预先保存的访问控制密码是否相同。

本发明中步骤 c 是在移动终端开机之后进行，或者是在移动终端连接到网络之后进行，或者是在接收到用户读取存储在移动终端的资料信息的指令后进行。

较佳地，加密密钥和解密密钥保存在一个单独设置的位于移动终端内的集成电路 IC 芯片中。加密算法和解密算法也由该 IC 芯片实现，或者由移动终端程序实现。

从本发明的技术方案可以看出，本发明首先在移动终端中设置一个加密密钥和一个对应的解密密钥，并设置一个加密算法和一个对应的解密算法；然后在接收到用户输入的资料信息后，通过加密密钥和加密算法对资料信息进行加密，然后将加密后的信息密文存储在移动终端中。当用户需要查看移动终端内部的资料信息时，首先需要对用户的身份进行合法性验证，并且仅

仅对通过合法性验证的用户使用解密密钥和解密算法对信息密文进行解密，得到资料信息的明文，而对于没有通过合法性验证的用户则不进行解密，这样该用户也就不可能看到移动终端内部存储的资料信息了。

可以看出，本发明通过对用户合法性的验证能有效地保证合法的用户才能看到移动终端内部资料信息，有效地提高了移动终端内部存储的资料信息的安全性，极大地避免了移动终端内部信息的泄漏给用户造成的物质上的损失和精神上的伤害。并且本发明设置密钥和算法的步骤，以及进行用户合法性验证的步骤都非常简单，不会给用户带来任何不便，也不会降低系统效率。

附图说明

图 1 是本发明的总体流程图。

图 2 是本发明的第一实施例的流程图。

图 3 是本发明的第二实施例的流程图。

图 4 是本发明的第三实施例的流程图。

具体实施方式

下面结合附图和具体实施例对本发明进行详细说明。

本发明通过在移动终端中设置一个加密密钥和对应的解密密钥，并设置一个加密算法和对应的解密算法，对于所有保存在移动终端内部的资料信息在保存之前进行加密计算得到信息密文，保存的资料信息是以密文的形式保存的，然后在读取资料信息之前首先对用户身份进行验证，如果验证通过，对信息密文进行对应的解密计算，得到信息明文，从而让用户可以像目前那样方便地查看资料信息，如果验证未通过，则不向用户提供资料信息，从而增强了移动终端内部资料信息的安全性。

图 1 是本发明的总体流程图。如图 1 所示，本发明至少包括如下步骤：

在步骤 101，在移动终端中预先设置一个加密密钥和一个对应的解密密钥，并在移动终端中设置加密算法和对应的解密算法。

在步骤 105，移动终端在存储诸如电话号码、SMS、MMS、图片或视频等资料信息时，使用预先保存的加密密钥和加密算法对该资料信息进行加密，得到信息密文，然后对应地将信息密文保存在移动终端，例如电话号码保存在电话簿存储区域，SMS 和 MMS 保存在短消息存储区域等等。

在步骤 110，移动终端在解密保存的资料信息密文之前，移动终端对用户身份的合法性进行验证。

在步骤 115，移动终端判断验证结果是否表明用户身份合法。如果用户身份合法，执行步骤 120，也就是允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看等等。如果用户身份不合法，结束流程，也就是不允许对资料信息密文进行解密，当然也就不会向用户提供解密后的明文。

在本发明中，密钥和算法可以通过移动终端的程序进行保存，但是较佳地，加密密钥和解密密钥由一个单独设置在移动终端内部的 IC 芯片来保存。这是因为作为硬件的 IC 芯片能对存储在其中的数据提供更高级别的安全性，从而提高本发明能实现的安全效果。使用一个单独的 IC 芯片来存储加密密钥和解密密钥，例如运用移动终端的用户识别卡安全技术等，对于本领域技术人员来说是一个公知常识，因此这里不再赘述。

在加密密钥和解密密钥由一个单独的 IC 芯片来保存的情况下，加密算法和解密算法依然可以通过移动终端程序来实现，此时进行加密计算或解密计算是移动终端程序从 IC 芯片获取相应的加密密钥或解密密钥。但是较佳地，加密算法和解密算法也同样可以在该 IC 芯片中实现，可以理解这样安全性将会更高。在这种情况下，所有的加密计算和解密计算也可以在该 IC 芯片中进行。

为了进一步提高本发明的执行效率，在步骤 110 可以是在移动终端连接到网络之后立即执行验证过程，这样可以预先将所有的资料信息解密得到明文，移动终端用户在查看时直接查看即可，不会影响用户的查看效率。当然，

也可以是用户希望查看某一个具体资料信息时对用户指定的资料信息进行解密和显示。

在本发明的第一实施例中，验证操作是向验证设备发送一个验证请求，验证设备然后向移动终端发送验证请求响应信息，移动终端执行用户身份合法性的验证处理。具体地说，第一实施例包括如图 2 所示的如下步骤。

在步骤 200，在移动终端中设置一个用于验证用户身份合法性的验证密钥，并单独设置一个验证设备，并在该验证设备中保存对应于该移动终端的验证密钥和对应于用户的用户信息之间的对应关系。这里的用户信息可以是用户识别卡的卡号，也就是 IMSI 信息。实际当中，验证密钥可以是加密密钥，也可以是解密密钥，也可以是一个单独密钥。

在步骤 201，在移动终端单独设置的一个 IC 芯片上保存验证密钥、加密密钥、解密密钥，并由该 IC 芯片实现加密算法和解密算法。

在步骤 205，移动终端在存储资料信息时，由 IC 芯片调用加密算法，利用保存的加密密钥对资料信息进行加密，然后将经过加密得到的资料信息密文保存在相应的位置，例如将一条电话号码记录密文保存在电话簿存储区域。

在步骤 210，移动终端在解密存储在自身内的资料信息之前，移动终端向验证设备发送一个验证请求消息，也就是请求验证设备存储的验证密钥，该验证请求消息携带有移动终端用户的用户信息，例如用户的用户识别卡卡号等等。

在步骤 211，验证设备在接收到来自移动终端的验证请求之后，根据移动终端用户的用户信息从步骤 200 建立的对应关系中确定对应于该移动终端的验证密钥。

在步骤 212，验证设备将所确定的验证密钥作为验证响应消息发送给该移动终端的 IC 芯片。

在步骤 215，IC 芯片比较接收自验证设备的验证密钥和自己保存的验证

密钥是否一致，如果是，在步骤220允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看。如果接收自验证设备的验证密钥不正确，直接结束流程，也就是不允许进行解密，当然也就不会向用户提供解密后的明文。

在该实施例中可以预先在移动终端中设置一个表示是否允许进行解密的标志，在步骤215如果判断两个验证密钥一致，在步骤220设置该标志的值为表示允许进行解密，通过这种方式来允许使用解密密钥和解密算法对资料信息密文进行解密。在步骤215如果判断两个验证密钥不一致，则设置该标志的值为表示禁止进行解密，从而不允许进行解密。在设置了标志的值后，在需要对资料信息密文进行解密时，移动终端会首先读取该标志的值，如果该标志的值表示允许进行解密，则进行解密；否则不进行解密。

在此实施例中，由于加密算法和解密算法都由IC芯片实现，因此由IC芯片执行步骤205和215。可以理解，如果加密算法和解密算法有移动终端程序来实现，则由移动终端程序来执行步骤205和215。

当然，步骤212之后，如果在预定时间内IC芯片没有接收到验证设备返回的响应信息，则可以直接判断验证不通过。

在这一实施例中，验证设备直接将验证密钥传送给移动终端，在这个传送的过程中验证密钥很容易泄露，因此，为了提高验证密钥的安全性，在步骤210，移动终端在向验证设备发送验证请求消息时可以同时携带一个自己产生的随机数；在步骤212，验证设备并不直接将所确定的验证密钥作为验证响应消息发送给该移动终端，而是利用该验证密钥和接收自移动终端的随机数进行计算得到一个计算结果，将该计算结果作为验证响应消息发送给该移动终端；在步骤215，移动终端并不是比较接收自验证设备的验证密钥和自己保存的验证密钥是否一致，而是利用自己产生的随机数和自己保存的验证密钥进行相应的计算，得到一个计算结果，移动终端通过比较接收自验证设备的验证响应信息和自己计算得到的计算结果是否匹配来判断用户合法

性。这里移动终端所进行的相应计算可以和验证设备所进行的计算相同或者具有一个对应关系，这样移动终端比较两个计算结果是否匹配也就是比较两个计算结果是否相同或者满足预定对应关系。

在第一实施例中，验证设备中保存对应于该移动终端的验证密钥和对应于用户的用户信息之间的对应关系，这样，如果合法用户的带有用户卡的移动终端丢失后，合法用户只需要通知网络运营商停止自己的用户卡，这样得到该移动终端的人因为无法使用原来的用户卡而不能对移动终端进行任何操作，当然也就不能解密保存在移动终端中的资料信息。如果得到该移动终端的人换一张用户卡插入该移动终端，那么验证设备中没有保存该用户卡的用户信息和验证密钥的对应关系，这样移动终端就不能从验证设备处得到正确的验证响应信息，从而在验证用户合法性的步骤中将确定用户是一个不合法用户，这样不会向该用户提供解密后的信息明文，从而实现了本发明保护移动终端内部资料信息的目的。

在第一实施例中，验证设备中也可以保存对应于该移动终端的验证密钥和对应于移动终端的移动终端特征信息之间的对应关系，这样，在步骤 210，移动终端向验证设备发送的验证请求消息中将携带有移动终端的移动终端特征信息；相应地，在步骤 211，验证设备在接收到来自移动终端的验证请求之后，根据移动终端的移动终端特征信息从步骤 200 建立的对应关系中确定对应于该移动终端的验证密钥。这里的移动终端特征信息例如可以是移动终端的 IMEI 信息。

在验证设备中保存对应于该移动终端的验证密钥和对应于移动终端的移动终端特征信息之间的对应关系情况下，合法用户在丢失移动终端之后，通知系统运营商自己的移动终端丢失，并提供移动终端特征信息。系统运营商可以在验证设备中删除该移动终端与验证密钥的对应关系，也可以对其设置一个表示该移动终端已经丢失的标记，拒绝移动终端获取该移动终端的验证密钥相关的验证信息。这样得到该移动终端的非法用户希望使用该移动终

端查看资料信息时，将会由于得不到正确的验证响应信息而不能进行相应操作，从而保证了移动终端内部存储的资料信息的安全性。

当然，这里的验证密钥也可以是一个简单的访问控制密码，由于访问控制密码应该方便于人们的记忆和输入，因此经常被限定为 4 个字符或 6 个字符，更经常地是被限定为 4 个数字或 6 个数字。

在第一实施例中需要通过验证设备来进行用户身份合法性的检查，在实际情况下也可以通过验证用户输入的访问控制密码是否正确来进行用户身份合法性的检查。为此本发明提出了如图 3 所示的第二实施例。

在步骤 301，在移动终端单独设置的一个 IC 芯片上保存访问控制密码、加密密钥、解密密钥，并由该 IC 芯片实现加密算法和解密算法。

在步骤 305，移动终端在存储资料信息时，由 IC 芯片调用加密算法，利用保存的加密密钥对资料信息进行加密，然后将经过加密得到的资料信息密文保存在相应的位置，例如将一条电话号码记录密文保存在电话簿存储区域。

在步骤 310，移动终端在解密存储在自身内的资料信息之前，移动终端通过输出单元向用户发送输入访问控制密码的提示消息。这里的提示可以通过显示屏幕或者通过声音等方式。

在步骤 311，移动终端在接收到用户输入的访问控制密码后，将该访问控制密码传送给 IC 芯片。

在步骤 315，IC 芯片比较用户输入的访问控制密码和自己保存的访问控制密码是否一致，如果是，在步骤 320 允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看；否则直接结束本流程，也就是不允许进行解密，当然也就不会向用户提供解密后的明文。

在实际情况下，有可能出现用户希望查看移动终端内部的资料信息而移动终端不能连接到网络的情况，例如用户位于移动信号不能覆盖的山区，为

了不影响合法用户的正常使用，本发明结合第一实施例的方便性和第二实施例的可靠性提出了如图 4 所示的第三实施例。

在步骤 400，设置一个验证设备，并在该验证设备中保存对应于该移动终端的验证密钥和对应于用户的用户信息之间的对应关系。当然，这里的验证密钥可以是加密密钥，可以是解密密钥，可以是访问控制密码，也可以是一个单独密钥。

在步骤 401，在移动终端单独设置的一个 IC 芯片上保存加密密钥、解密密钥、验证密钥、访问控制密码，并由该 IC 芯片实现加密算法和解密算法。

在步骤 405，移动终端在存储资料信息时，由 IC 芯片调用加密算法，利用保存的加密密钥对资料信息进行加密，然后将经过加密得到的资料信息密文保存在相应的位置。

在步骤 410，移动终端在解密存储在移动终端内的资料信息之前，移动终端判断此时是否能连接到移动通信网络，如果是，在步骤 411 向验证设备发送一个验证请求消息，也就是请求对应于验证设备保存的验证密钥的验证信息，该验证请求消息携带有移动终端用户的用户信息，例如用户识别卡的卡号等等，同时还携带一个随机数；否则执行步骤 450 及其后续步骤。

在步骤 412，验证设备在接收到来自移动终端的验证请求消息之后，根据移动终端用户的用户信息从步骤 400 建立的对应关系中确定对应于该移动终端的验证密钥。

在步骤 413，验证设备使用得到的验证密钥和接收自移动终端的随机数进行计算，得到一个计算结果，并将计算结果作为验证响应信息发送给移动终端。

在步骤 414，移动终端在接收到计算结果后，对自身保存的验证密钥和自身生成的随机数进行相应的计算，得到一个计算结果。

在步骤 415，移动终端比较接收自验证设备的计算结果和自己计算得到

的计算结果是否匹配，如果是，在步骤 420 允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看。如果接收自验证设备的计算结果不正确，直接结束流程，也就是不允许进行解密，当然也就不会向用户提供解密后的明文。

在步骤 450，移动终端通过输入/输出单元提示用户输入访问控制密码。

在步骤 455，移动终端在得到用户输入的访问控制密码之后，判断用户输入的访问控制密码和移动终端预先保存的访问控制密码是否相同。如果相同，执行步骤 420，也就是允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看；否则直接结束流程，也就是不允许解密，当然也就不会向用户提供解密后的明文。这里对应用户输入的访问控制密码正确性的判断在 IC 芯片内部进行。

当然可以理解，在第三实施例中也可以不使用随机数而是直接发送验证密钥。

在第三实施例中，在移动终端能连接到网络时通过验证设备来判断用户身份的合法性，在移动终端不能连接到网络时通过用户输入的访问控制密码来判断用户身份的合法性，因此该实施例同时具有方便性和可靠性。

在第一和第三实施例中，如果移动终端连接不到验证设备，则可以直接判断验证不通过。如果移动终端在向验证设备发送一个验证请求消息后的设定时间内没有接收到验证设备相应的响应信息，则移动终端重复向验证设备发送一个验证请求消息，或直接判断验证不通过。在移动终端判断验证不通过后，也可以不直接禁止对资料信息的解密，而是进一步执行步骤 350 及其后续步骤，也就是给用户提供一个通过输入访问控制密码来获取资料信息的机会。

在上述实施例中，如果用户的移动终端丢失，用户可以向系统运营商要求停止用户卡业务，此时系统运营商会通过移动通信网络向移动终端发送一个停止服务通知，在接收到该通知后，移动终端可以关闭解密功能，即禁止

解密移动终端保存的资料信息的操作，并锁定保存在移动终端内存中的已经解密的资料信息的明文，或者移动终端直接关机。这样即使非法用户在合法用户要求停止用户卡业务之前已经查看用户资料，通过锁定已经解密的资料信息的明文或者直接关机的方式也可以防止非法用户进一步查看，从而将合法用户的损失降低到最小。和第一实施例相似，这里也可以预先在移动终端中设置一个表示验证是否通过的标志，关闭解密功能也就是将该标志的值设置为表示禁止进行解密。

还可以设置关闭解密功能的短消息命令，通过向丢失移动终端发送一个关闭解密功能的短消息来使移动终端执行关闭解密功能。在该短消息中用一个特殊的标识来区分该短消息是一个关闭解密功能的命令短消息，并在所述特殊标识后，存放验证密码信息，一般情况下，该验证密码应该采用访问控制密码。这样，被盗终端接收到该短消息后，根据所述特殊标识判断出该短消息为关闭解密功能的命令后，将携带的验证密钥传送给 IC 芯片，IC 芯片判断短消息携带的验证密码是否正确，如果正确，则直接执行关闭解密功能操作，否则，不作任何处理。这样，用户丢失移动终端后，可以迅速给丢失的移动终端发送一个关闭解密功能的命令短消息，以便能够及时关闭该丢失移动终端的解密功能，而后再向运营商报失，以便由运营商从网络侧再次执行关闭丢失的移动终端的解密功能，从而，通过双重的安全方式，最大限度地保证用户资料的安全性。

另外，如果移动终端和网络连接断开之后，例如移动终端进入一个信号覆盖不到的区域，用户向系统运营商要求停止用户卡业务之后，移动终端可能无法接收网络侧通过移动通信网络向移动终端发送的停止服务通知，此时可以由移动终端自动检测和网络的连接是否断开，并在检测到断开并经过一个预定时间之后，移动终端关闭解密功能，同时锁定保存在移动终端内存中的已经解密的资料信息的明文，防止拥有该移动终端的人继续查看移动终端的资料信息。这时如果用户需要查看移动终端内部的资料信息，移动终端将

提示用户输入访问控制密码，只有在访问控制密码正确后，才打开解密功能，并允许移动终端用户查看资料信息，并在一个设定的时间之后，继续关闭解密功能，同时锁定保存在移动终端内存中的已经解密的资料信息的明文。这样即使移动终端和网络的连接断开，也会有效防止非法用户继续查看移动终端内部存储的资料信息，进一步提高了本发明的安全性。

需要再次说明的是，移动终端打开解密功能的情况有两种，一种是如第一实施例通过从网络获取验证响应信息来驱动移动终端打开解密功能，另一种是如第二实施例通过用户从终端输入相应的访问控制密码来驱动移动终端打开解密功能。对于前一种情况，移动终端在进入一个信号无法覆盖区域后，应该设置较短的时间就执行关闭解密功能，同时锁定保存在移动终端内存中的已经解密的资料信息的明文。而对于后一种情况，移动终端在进入一个信号无法覆盖区域后，应该设置相对较长的时间才执行关闭解密功能等等操作，这样不会使得移动终端要求用户频繁地输入访问控制密码，从而不会给用户带来不便。

本发明还进一步包括，网络侧判断向移动终端发送的停止服务通知没有到达移动终端时，例如没有接收到移动终端返回的接收到停止服务通知的响应消息，则保存该通知；移动终端重新执行连接和登录网络的操作后，例如移动终端在进入一个信号无法覆盖区域后又重新进入一个有信号覆盖区域时，网络在判断移动终端重新连接到网络后，如果发现有相应的停止服务通知没有通知到该移动终端，则重新尝试将该停止服务通知发送给该移动终端。对于移动终端来说，在重新连接网络并经过一个设定的时间后，自动打开解密功能，并解锁保存在内存中的已经解密的资料信息，并在接收到停止服务通知时，关闭解密功能，同时锁定保存在移动终端内存中的已经解密的资料信息的明文的操作。

在本发明中，为了简化 IC 芯片的设计，对于使用 IC 芯片保存加密密钥、解密密钥、验证密钥或访问控制密码的情况，加密算法和解密算法也可以不

在 IC 芯片中实现，而是由移动终端程序来实现，这样，在对移动终端的用户身份进行合法性验证通过时，IC 芯片允许访问保存的加密密钥和解密密钥信息，否则，如果没有通过验证时，禁止访问保存的加密密钥和解密密钥信息。这样，由于加解密密钥保存在 IC 芯片里，而加解密算法又是由移动终端程序实现，这样，移动终端程序得到 IC 芯片存储的加解密密钥时，即可进行相应的加解密操作。相应地，移动终端程序得不到 IC 芯片存储的加解密密钥时，就无法进行相应的加解密操作。

在本发明中，验证设备可以是增加了支持本发明移动终端验证功能的归属位置寄存器（HLR）或者鉴权中心（AC）或者设备识别寄存器（EIR）。

验证设备也可以是一个电子钥匙，在这种情况下，在移动终端和电子钥匙中分别设置一个无线收发模块，移动终端和电子钥匙通过该无线收发模块建立无线通信。或者，在移动终端和电子钥匙中分别设置一个数据通信线接口，当需要对移动终端进行认证时，使用一根数据通信线连接两个接口，移动终端和电子钥匙通过该数据通信线建立有线通信连接。

验证设备也可以是移动终端内部的用户卡，例如 GSM 网络中的 SIM 卡或者 CDMA 网络中的 UIM 卡。在这种情况下，用户卡在验证移动终端的用户身份的合法性之前进一步包括验证用户卡自身的合法性，如果验证通过，则将验证密钥或计算结果返回给移动终端，否则，不返回验证密钥或者计算结果，或者返回一个失败信息给移动终端。

上述用户卡对自身合法性进行验证具体包括：在用户卡中预先设置一个业务密钥，并将该业务密钥保存在网络侧相关设备中，例如鉴权中心或者电子钥匙中，用户卡对自身合法性进行验证时，首先产生一个随机数，然后发送给网络侧相关设备；网络侧相关设备根据随机数和自己保存的业务密钥进行计算，得到一个计算结果，然后将该计算结果返回给用户卡；用户卡也根据随机数和自己保存的业务密钥进行相应的计算，得到一个计算结果，并比较自己计算得到的结果和来自所述网络侧相关设备的计算结果是否一致，如果一致，则认证

成功，否则，认证失败。这里的业务密钥可以直接是用户卡里的根密钥，具体地说，对于 GSM 的 SIM 卡来说，就是 AK；对于 CDMA 的 UIM 卡来说，就是 AKEY。

本发明中提到的移动终端内存储的资料信息包括移动终端本身存储的资料信息，也包括移动终端内的用户卡上存储的资料信息。

因此可以理解，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，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。

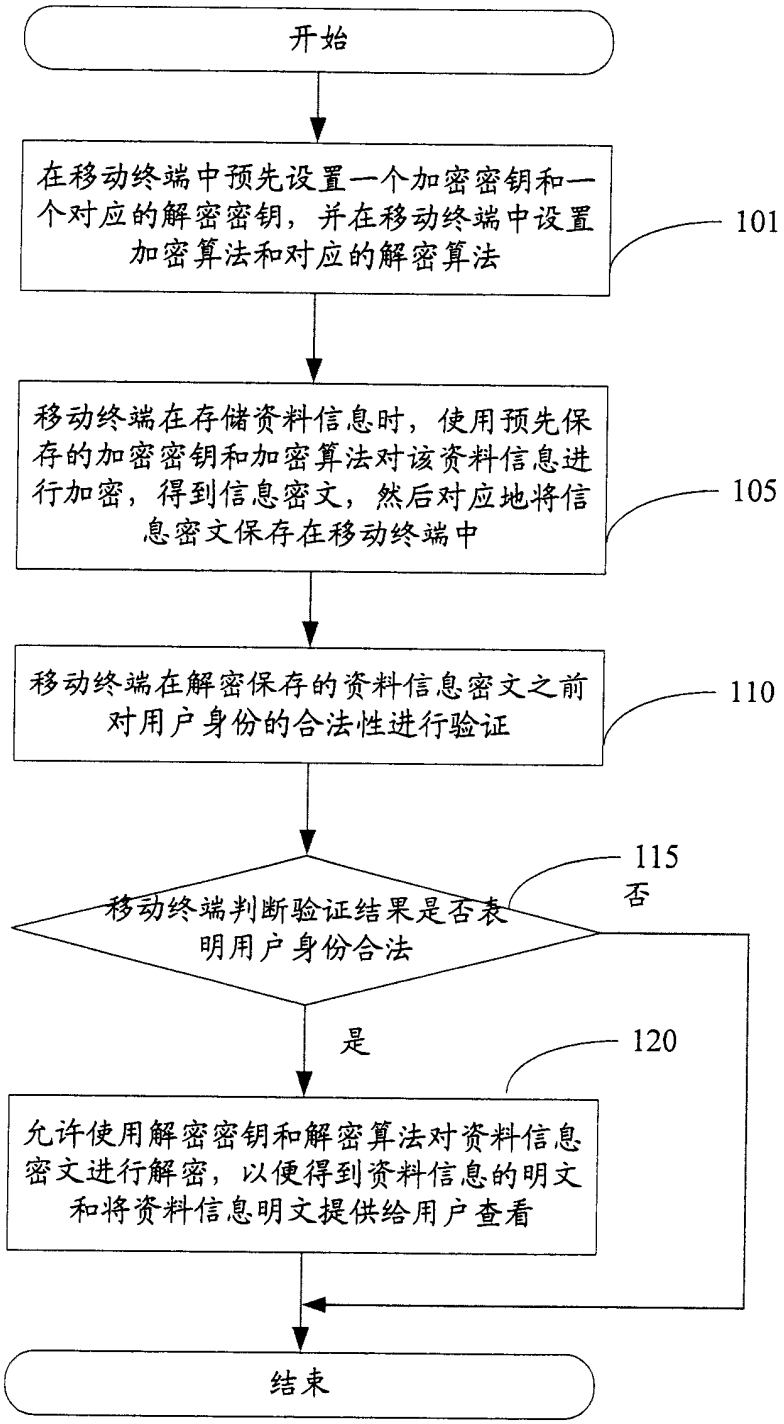

开始
在移动终端中预先设置一个加密密钥和一个对应的解密密钥，并在移动终端中设置加密算法和对应的解密算法
101
移动终端在存储资料信息时，使用预先保存的加密密钥和加密算法对该资料信息进行加密，得到信息密文，然后对应地将信息密文保存在移动终端中
105
移动终端在解密保存的资料信息密文之前对用户身份的合法性进行验证
110
移动终端判断验证结果是否表明用户身份合法
115
否
是
120
允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看
结束

图 1

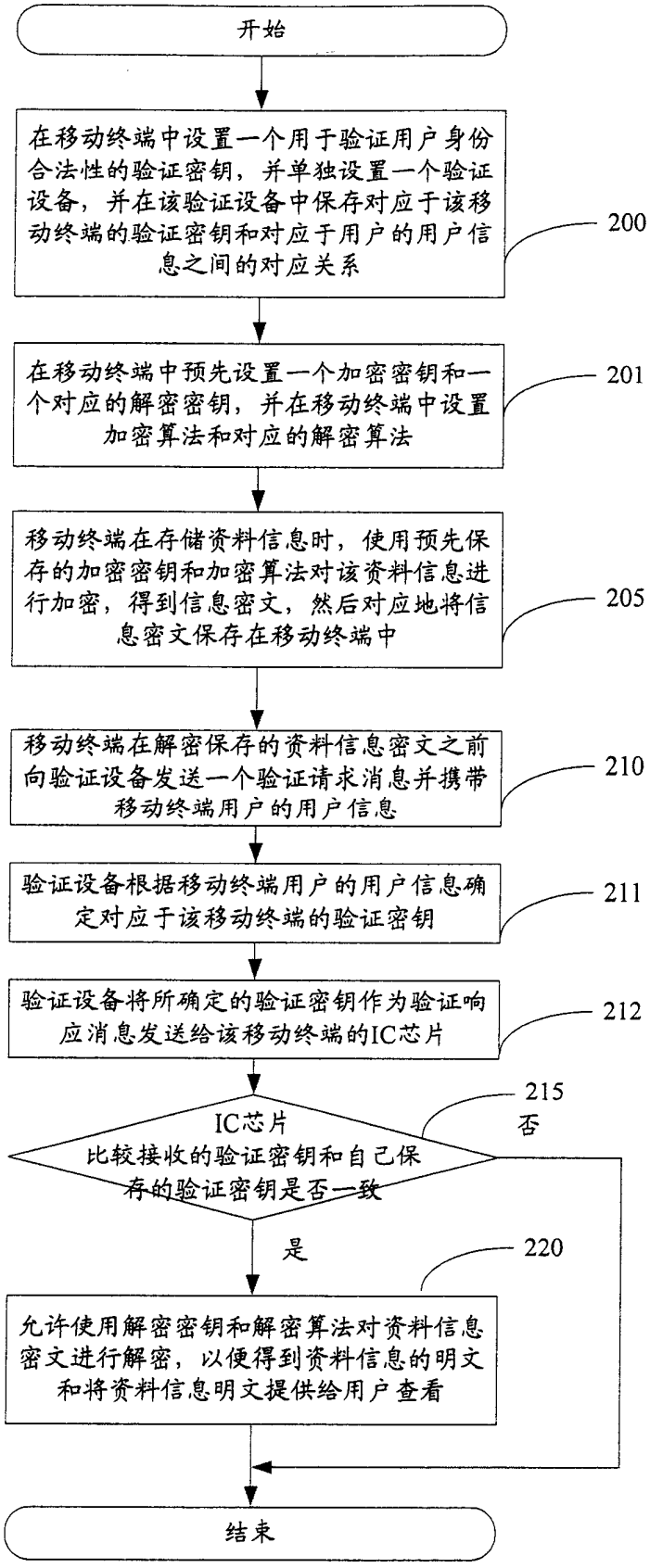

开始
在移动终端中设置一个用于验证用户身份合法性的验证密钥，并单独设置一个验证设备，并在该验证设备中保存对应于该移动终端的验证密钥和对应于用户的用户信息之间的对应关系
200
在移动终端中预先设置一个加密密钥和一个对应的解密密钥，并在移动终端中设置加密算法和对应的解密算法
201
移动终端在存储资料信息时，使用预先保存的加密密钥和加密算法对该资料信息进行加密，得到信息密文，然后对应地将信息密文保存在移动终端中
205
移动终端在解密保存的资料信息密文之前向验证设备发送一个验证请求消息并携带移动终端用户的用户信息
210
验证设备根据移动终端用户的用户信息确定对应于该移动终端的验证密钥
211
验证设备将所确定的验证密钥作为验证响应消息发送给该移动终端的IC芯片
212
IC芯片比较接收的验证密钥和自己保存的验证密钥是否一致
215
否
是
220
允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看
结束

图 2

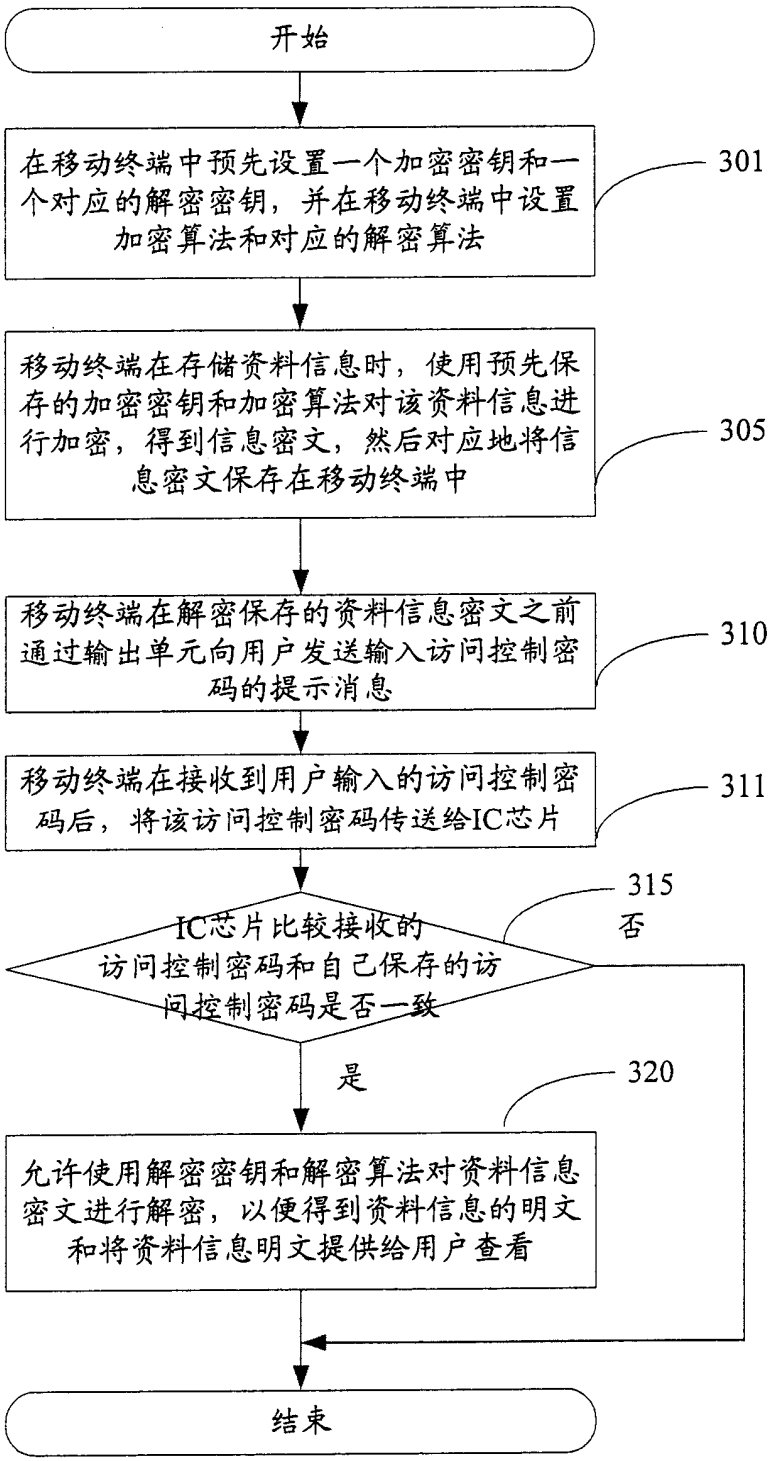

开始
在移动终端中预先设置一个加密密钥和一个对应的解密密钥，并在移动终端中设置加密算法和对应的解密算法
301
移动终端在存储资料信息时，使用预先保存的加密密钥和加密算法对该资料信息进行加密，得到信息密文，然后对应地将信息密文保存在移动终端中
305
移动终端在解密保存的资料信息密文之前通过输出单元向用户发送输入访问控制密码的提示消息
310
移动终端在接收到用户输入的访问控制密码后，将该访问控制密码传送给IC芯片
311
IC芯片比较接收的访问控制密码和自己保存的访问控制密码是否一致
315
否
是
320
允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看
结束

图 3

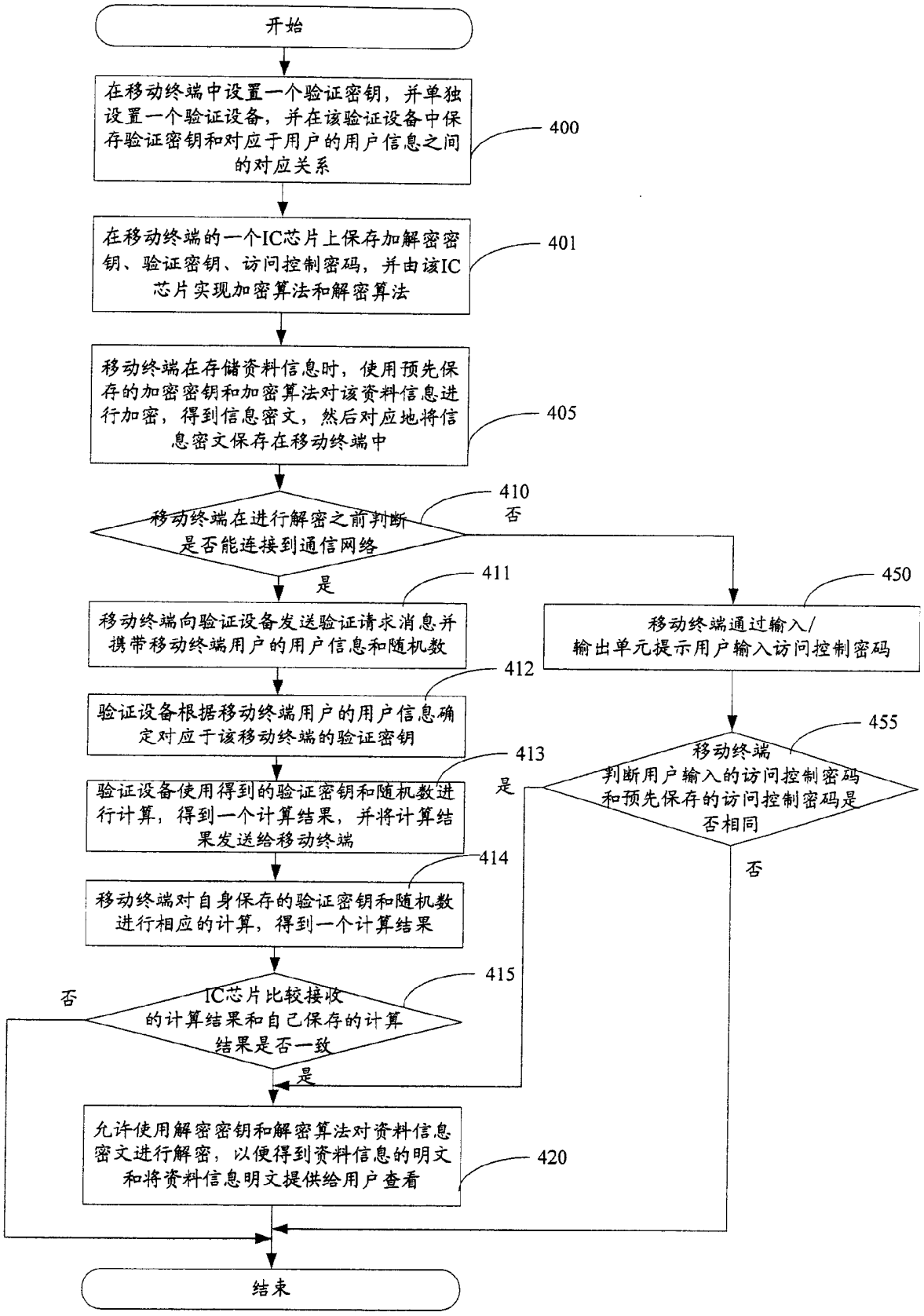

开始
在移动终端中设置一个验证密钥，并单独设置一个验证设备，并在该验证设备中保存验证密钥和对应于用户的用户信息之间的对应关系
400
在移动终端的一个IC芯片上保存加解密密钥、验证密钥、访问控制密码，并由该IC芯片实现加密算法和解密算法
401
移动终端在存储资料信息时，使用预先保存的加密密钥和加密算法对该资料信息进行加密，得到信息密文，然后对应地将信息密文保存在移动终端中
405
移动终端在进行解密之前判断是否能连接到通信网络
410
否
是
移动终端向验证设备发送验证请求消息并携带移动终端用户的用户信息和随机数
411
移动终端通过输入/输出单元提示用户输入访问控制密码
450
验证设备根据移动终端用户的用户信息确定对应于该移动终端的验证密钥
412
移动终端判断用户输入的访问控制密码和预先保存的访问控制密码是否相同
455
是
否
验证设备使用得到的验证密钥和随机数进行计算，得到一个计算结果，并将计算结果发送给移动终端
413
移动终端对自身保存的验证密钥和随机数进行相应的计算，得到一个计算结果
414
IC芯片比较接收的计算结果和自己保存的计算结果是否一致
415
否
是
允许使用解密密钥和解密算法对资料信息密文进行解密，以便得到资料信息的明文和将资料信息明文提供给用户查看
420
结束

图 4