



(12) 发明专利申请

(10) 申请公布号 CN 105631299 A

(43) 申请公布日 2016. 06. 01

(21) 申请号 201511006294. X

(22) 申请日 2015. 12. 29

(71) 申请人 惠州 TCL 移动通信有限公司

地址 516006 广东省惠州市仲恺高新区和畅七路西 86 号

(72) 发明人 孔亦亮

(74) 专利代理机构 深圳市君胜知识产权代理事务所 44268

代理人 王永文 刘文求

(51) Int. Cl.

G06F 21/35(2013. 01)

H04L 9/30(2006. 01)

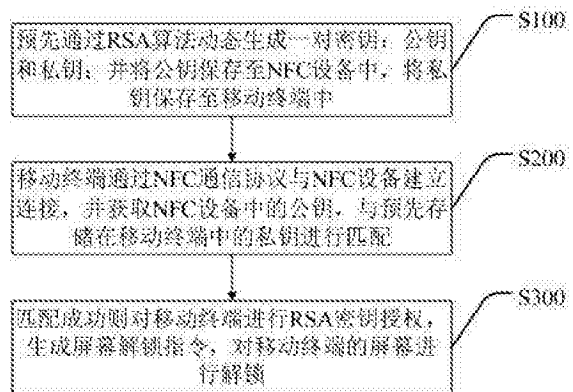
权利要求书2页 说明书4页 附图2页

(54) 发明名称

一种移动终端的智能解锁方法及系统

(57) 摘要

本发明公开一种移动终端的智能解锁方法及系统,其将移动终端的解锁方式设置为 NFC 解锁,另外还采用 RSA 算法动态生成一对密钥,通过对移动终端和 NFC 设备进行加密配对,使得在 NFC 设备靠近移动终端并且 NFC 设备中的公钥能与移动终端中的私钥配对成功后,实现快速解锁的目的,并且本发明所述智能解锁方法简单易实现,其安全性高,为用户提供极大的便利。



1. 一种移动终端的智能解锁方法,其特征在于,包括以下步骤:

A、预先通过RSA算法动态生成一对密钥:公钥和私钥;并将公钥保存至NFC设备中,将私钥保存至移动终端中;

B、移动终端通过NFC通信协议与NFC设备建立连接,并获取NFC设备中的公钥,与预先存储在移动终端中的私钥进行匹配;

C、匹配成功则对移动终端进行RSA密钥授权,生成屏幕解锁指令,对移动终端的屏幕进行解锁。

2. 根据权利要求1所述移动终端的智能解锁方法,其特征在于,还包括以下步骤:

D、匹配不成功则退出解锁界面或返回手动解锁界面。

3. 根据权利要求2所述移动终端的智能解锁方法,其特征在于,还包括以下步骤:

E、重新通过RSA算法动态生成一对新的密钥:公钥和私钥;并重新将公钥保存至NFC设备中,将私钥保存至移动终端中。

4. 根据权利要求3所述移动终端的智能解锁方法,其特征在于,所述NFC设备为穿戴式NFC设备,包括智能手表、智能手环以及智能眼镜中的任一种。

5. 根据权利要求4所述移动终端的智能解锁方法,其特征在于,所述步骤B具体包括:

B1、预先将移动终端的解锁方式设置为NFC解锁,并通过NFC通信协议与NFC设备建立连接;

B2、判断移动终端中是否存在私钥;当是时,则进入步骤B3,当否时,则重新生成私钥,并保存至移动终端中;

B3、移动终端获取建立连接的NFC设备中的公钥,并与预先存储在移动终端中的私钥进行匹配。

6. 一种移动终端的智能解锁系统,其特征在于,所述智能解锁系统包括:

预先设定模块、用于预先通过RSA算法动态生成一对密钥:公钥和私钥;并将公钥保存至NFC设备中,将私钥保存至移动终端中;

建立与匹配模块、用于移动终端通过NFC通信协议与NFC设备建立连接,并获取NFC设备中的公钥,与预先存储在移动终端中的私钥进行匹配;

屏幕解锁模块、用于匹配成功则对移动终端进行RSA密钥授权,生成屏幕解锁指令,对移动终端的屏幕进行解锁。

7. 根据权利要求6所述移动终端的智能解锁系统,其特征在于,所述智能解锁系统还包括:

退出解锁模块、用于匹配不成功则退出解锁界面或返回手动解锁界面。

8. 根据权利要求7所述移动终端的智能解锁系统,其特征在于,所述智能解锁系统还包括:

重新设定模块、用于重新通过RSA算法动态生成一对密钥:公钥和私钥;并重新将公钥保存至NFC设备中,将私钥保存至移动终端中。

9. 根据权利要求8所述移动终端的智能解锁方法,其特征在于,所述建立与匹配模块具体包括:

建立单元、用于预先将移动终端的解锁方式设置为NFC解锁,并通过NFC通信协议与NFC设备建立连接;

判断单元、用于判断移动终端中是否存在私钥；当是时，则与NFC设备中的公钥进行匹配，当否时，则重新生成私钥，并保存至移动终端中；

匹配单元、用于移动终端获取建立连接的NFC设备中的公钥，并与预先存储在移动终端中的私钥进行匹配。

## 一种移动终端的智能解锁方法及系统

### 技术领域

[0001] 本发明涉及移动终端解锁领域,尤其涉及一种移动终端的智能解锁方法及系统。

### 背景技术

[0002] 目前智能手机已经有了很多的解锁方式,比如滑动解锁,九宫图解锁,指纹解锁,声纹解锁。但是这些方式多多少少都有一定局限性,比如滑动解锁和九宫图解锁虽然简单但是安全性却是问题,指纹则需要加入指纹模块,声纹解锁也有一定的难度,比如声音的仿生,判断算法的准确率和效率都有一些问题。

[0003] 因此,现有技术还有待于改进和发展。

### 发明内容

[0004] 鉴于上述现有技术的不足,本发明的目的在于提供一种移动终端的智能解锁方法及系统,旨在解决现有技术中移动终端解锁不够便利的问题。

[0005] 本发明的技术方案如下:

一种移动终端的智能解锁方法,其中,包括以下步骤:

A、预先通过RSA算法动态生成一对密钥:公钥和私钥;并将公钥保存至NFC设备中,将私钥保存至移动终端中;

B、移动终端通过NFC通信协议与NFC设备建立连接,并获取NFC设备中的公钥,与预先存储在移动终端中的私钥进行匹配;

C、匹配成功则对移动终端进行RSA密钥授权,生成屏幕解锁指令,对移动终端的屏幕进行解锁。

[0006] 所述移动终端的智能解锁方法,其中,还包括以下步骤:

D、匹配不成功则退出解锁界面或返回手动解锁界面。

[0007] 所述移动终端的智能解锁方法,其中,还包括以下步骤:

E、重新通过RSA算法动态生成一对新的密钥:公钥和私钥;并重新将公钥保存至NFC设备中,将私钥保存至移动终端中。

[0008] 所述移动终端的智能解锁方法,其中,所述NFC设备为穿戴式NFC设备,包括智能手表、智能手环以及智能眼镜中的任一种。

[0009] 所述移动终端的智能解锁方法,其中,所述步骤B具体包括:

B1、预先将移动终端的解锁方式设置为NFC解锁,并通过NFC通信协议与NFC设备建立连接;

B2、判断移动终端中是否存在私钥;当是时,则进入步骤B3,当否时,则重新生成私钥,并保存至移动终端中;

B3、移动终端获取建立连接的NFC设备中的公钥,并与预先存储在移动终端中的私钥进行匹配。

[0010] 所述移动终端的智能解锁方法,其中,所述建立与匹配模块具体包括:

建立单元、用于预先将移动终端的解锁方式设置为NFC解锁,并通过NFC通信协议与NFC设备建立连接;

判断单元、用于判断移动终端中是否存在私钥;当是时,则与NFC设备中的公钥进行匹配,当否时,则重新生成私钥,并保存至移动终端中;

匹配单元、用于移动终端获取建立连接的NFC设备中的公钥,并与预先存储在移动终端中的私钥进行匹配。

[0011] 有益效果:本发明一种移动终端的智能解锁方法及系统,其将移动终端的解锁方式设置为NFC解锁,另外还采用RSA算法动态生成一对密钥,通过对移动终端和NFC设备进行加密配对,使得在NFC设备靠近移动终端并且NFC设备中的公钥能与移动终端中的私钥配对成功后,实现快速解锁的目的,并且本发明所述智能解锁方法简单易实现,其安全性高,为用户提供极大的便利。

## 附图说明

[0012] 图1为本发明所述移动终端的智能解锁方法的步骤流程图。

[0013] 图2为本发明所述移动终端的智能解锁方法中步骤S200的流程图。

[0014] 图3为本发明所述移动终端的智能解锁系统的结构模块图。

[0015] 图4为本发明所述移动终端的智能解锁系统中建立与匹配单元的单元图。

## 具体实施方式

[0016] 本发明提供一种移动终端的智能解锁方法及系统,为使本发明的目的、技术方案及效果更加清楚、明确,以下对本发明进一步详细说明。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。

[0017] 如图1所示,本发明提供一种移动终端的智能解锁方法,其包括以下步骤:

S100、预先通过RSA算法动态生成一对密钥:公钥和私钥;并将公钥保存至NFC设备中,将私钥保存至移动终端中;

S200、移动终端通过NFC通信协议与NFC设备建立连接,并获取NFC设备中的公钥,与预先存储在移动终端中的私钥进行匹配;

S300、匹配成功则对移动终端进行RSA密钥授权,生成屏幕解锁指令,对移动终端的屏幕进行解锁。

[0018] 本发明实施例中通过将移动终端的解锁方式设置为NFC解锁,并采用RSA算法动态生成一对密钥分别存储到移动终端和与其建立连接的NFC设备中,通过对移动终端和NFC设备进行加密配对,使得在NFC设备靠近移动终端并且NFC设备中的公钥能与移动终端中的私钥配对成功后,实现快速解锁的目的。

[0019] 首先对本发明中的NFC通信协议和RSA算法进行解释。NFC通信协议全称为Near Field Communication,是一种短距高频的无线电技术,在13.56MHz频率下,有效运行于20厘米距离内。本发明正是基于NFC技术,实现移动终端的自动解锁。应当理解地是,本发明采用的NFC技术,不采用上述标准,可对NFC进行定义,如NFC的感应距离,即移动终端与NFC设备处于设定的距离内即可建立连接,所述设置的距离为1m、0.5m、0.3m或直接接触等。而RSA算法是第一个既能用于数据加密也能用于数字签名的算法,该算法的名字

以发明者的名字命名:Ron Rivest, Adi Shamir 和Leonard Adleman。在本发明中采用RSA算法是为了动态生成一对密钥来实现对数据加密的,这样使得只有在密钥配对成功时才能实现解锁,大大提高了移动终端的安全性。

[0020] 在步骤S100中,预先通过RSA算法动态生成一对密钥:公钥和私钥;并将公钥保存至NFC设备中,将私钥保存至移动终端中,即将公钥保存在NFC设备的客户端中,而私钥保存在移动终端的服务端中。本发明中采用RSA进行加、解密方式是私钥加密、公钥验证。需要说明的是,一台NFC设备对应有一个公钥,但可以设置有多台NFC设备对移动终端进行解密,因此可以生成一个密钥和多个公钥,这样我们就可以选择一台或者多台NFC设备对移动终端进行解锁。另外,还可以在一段时间后重新生成新的一对密钥,这样即使被别人捡到公钥也无需担心移动终端被盗取解锁了。

[0021] 而在步骤S200中,因为移动终端的解锁方式设置为NFC解锁,因此其可以通过NFC通信协议与NFC设备建立连接,并获取NFC设备中的公钥,与预先存储在移动终端中的私钥进行匹配。当然,本发明中所述移动终端内部需设置有NFC模块才能实现本技术方案,优选地,所述移动终端指的是智能手机、IPAD等具有NFC模块的智能设备。

[0022] 下面对所述步骤S200的具体操作过程阐述如下:S201、预先将移动终端的解锁方式设置为NFC解锁,并通过NFC通信协议与NFC设备建立连接;S202、判断移动终端中是否存在私钥;当是时,则进入步骤S203,当否时,则重新生成私钥,并保存至移动终端中;S203、移动终端获取建立连接的NFC设备中的公钥,并与预先存储在移动终端中的私钥进行匹配。

[0023] 随后进入步骤S300,即当NFC设备中的公钥与移动终端中的私钥匹配成功后,NFC设备对移动终端进行RSA密钥授权,生成屏幕解锁指令,对移动终端的屏幕进行解锁。

[0024] 较佳实施例中,本发明还包括以下步骤:S400、匹配不成功则退出解锁界面或返回手动解锁界面。需要说明的是,本发明所述智能解锁方法能够和其他屏幕解锁程序配合使用,例如可以用手动解锁中的迷宫解锁、密码解锁等配合使用,这样,即使用户因某种原因无法使用 NFC 设备进行解锁的情况下,也可采用其它解锁方式对屏幕进行解锁,不影响对移动终端的使用。

[0025] 较佳实施例中,本发明还包括以下步骤:S500、重新通过RSA算法动态生成一对新的密钥:公钥和私钥;并重新将公钥保存至NFC设备中,将私钥保存至移动终端中。即每次解锁成功或不成功后,都会重新生成新的一对密钥,这样可以有效提高移动终端解锁的安全性。

[0026] 具体而言,本发明实施例中所述NFC设备为穿戴式NFC设备,包括智能手表、智能手环以及智能眼镜中的任一种,所述智能眼镜可以是谷歌眼镜。例如,本发明采用智能手表作为NFC设备,当需要对移动终端进行解锁时,则只需将智能手表靠近移动终端或轻轻触碰移动终端,并通过其内部的密钥配对,来实现解锁目的,其方法简单易实现,具有极高的便利性。

[0027] 另外,如图3所示,本发明还提供一种移动终端的智能解锁系统,其中所述智能解锁系统包括:

预先设定模块100、用于预先通过RSA算法动态生成一对密钥:公钥和私钥;并将公钥保存至NFC设备中,将私钥保存至移动终端中;

建立与匹配模块200、用于移动终端通过NFC通信协议与NFC设备建立连接,并获取NFC

设备中的公钥,与预先存储在移动终端中的私钥进行匹配;

屏幕解锁模块300、用于匹配成功则对移动终端进行RSA密钥授权,生成屏幕解锁指令,对移动终端的屏幕进行解锁。

[0028] 进一步地,所述智能解锁系统还包括:

退出解锁模块400、用于匹配不成功则退出解锁界面或返回手动解锁界面。

[0029] 更进一步地,所述智能解锁系统还包括:

重新设定模块500、用于重新通过RSA算法动态生成一对密钥:公钥和私钥;并重新将公钥保存至NFC设备中,将私钥保存至移动终端中。

[0030] 较佳实施例中,如图4所示,所述建立与匹配模块200具体包括:

建立单元201、用于预先将移动终端的解锁方式设置为NFC解锁,并通过NFC通信协议与NFC设备建立连接;

判断单元202、用于判断移动终端中是否存在私钥;当是时,则与NFC设备中的公钥进行匹配,当否时,则重新生成私钥,并保存至移动终端中;

匹配单元203、用于移动终端获取建立连接的NFC设备中的公钥,并与预先存储在移动终端中的私钥进行匹配。

[0031] 本发明所述移动终端的智能解锁系统的模块实现途径与上述智能解锁方法的步骤相同,在此不再赘述。

[0032] 上述模块的划分仅用以举例说明,在实际应用中,可以根据需要将上述模块的功能分配由不同的功能模块来完成,即划分成不同的功能模块,来完成上述描述的全部或部分功能。

[0033] 本领域普通技术人员可以理解上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件完成,所述的计算机程序可存储于一计算机可读取存储介质中,程序在执行时,可包括上述各方法的实施例的流程。其中的存储介质可以为磁碟、光盘、只读存储记忆体(ROM)或随机存储记忆体(RAM)等。

[0034] 综上所述,本发明一种移动终端的智能解锁方法及系统,其将移动终端的解锁方式设置为NFC解锁,另外还采用RSA算法动态生成一对密钥,通过对移动终端和NFC设备进行加密配对,使得在NFC设备靠近移动终端并且NFC设备中的公钥能与移动终端中的私钥配对成功后,实现快速解锁的目的,并且本发明所述智能解锁方法简单易实现,其安全性高,为用户提供极大的便利。

[0035] 应当理解的是,本发明的应用不限于上述的举例,对本领域普通技术人员来说,可以根据上述说明加以改进或变换,所有这些改进和变换都应属于本发明所附权利要求的保护范围。

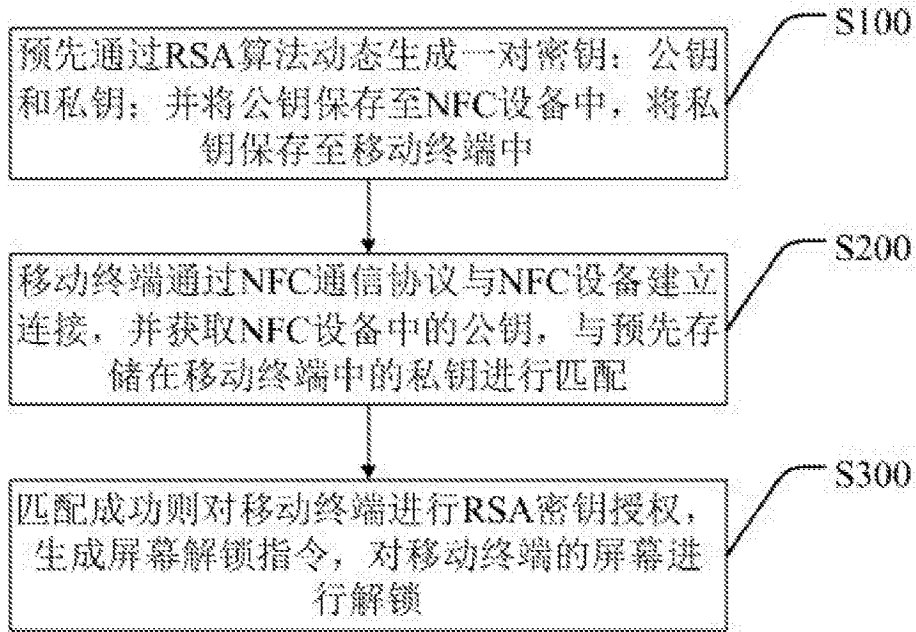


图 1

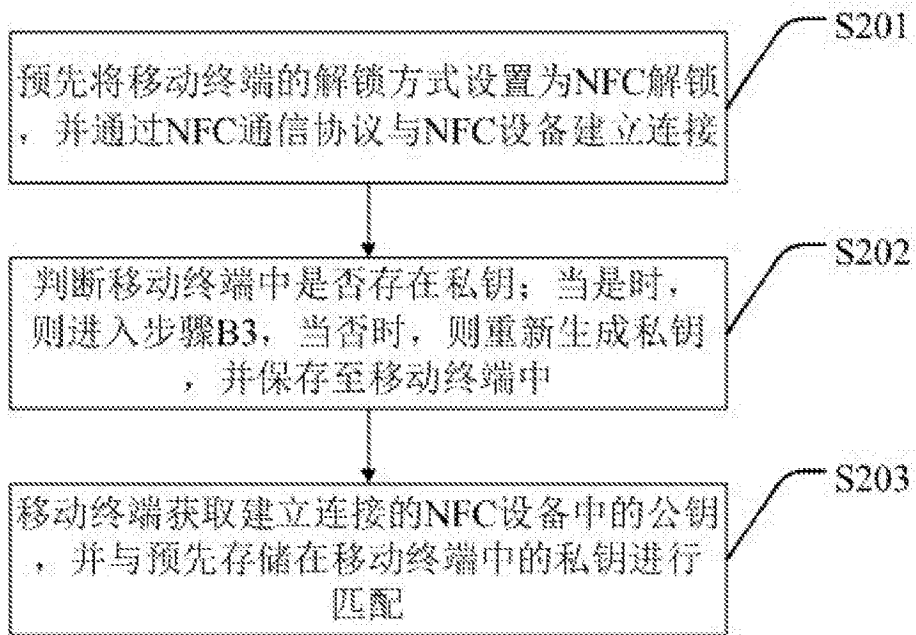


图 2



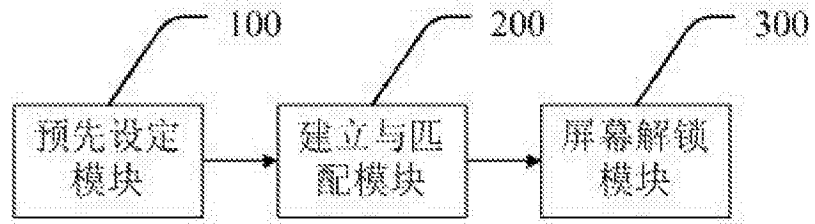


图 3

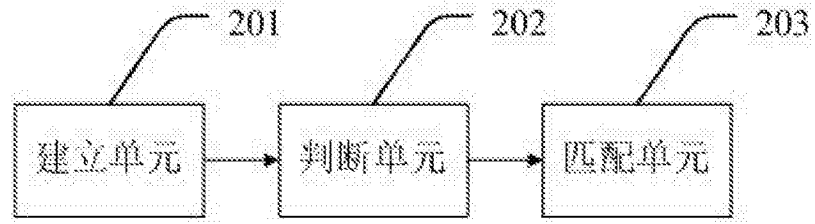


图 4