(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 107766061 A
(43)申请公布日 2018.03.06

(21)申请号 201711153403.X

(22)申请日 2017.11.20

(71)申请人 烽火通信科技股份有限公司
地址 430000 湖北省武汉市东湖高新技术开发区高新四路6号

(72)发明人 王能 祝振东

(74)专利代理机构 武汉智权专利代理事务所(特殊普通合伙) 42225
代理人 张凯

(51)Int.Cl.
G06F 8/61(2018.01)
G06F 21/51(2013.01)

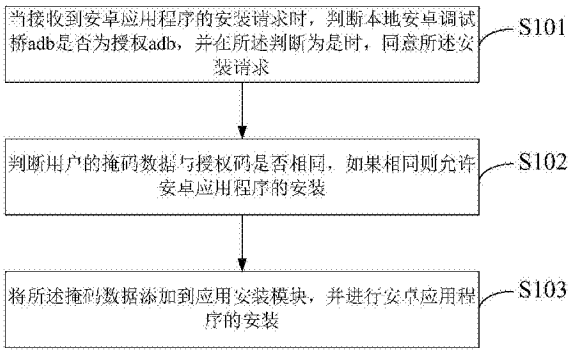
权利要求书2页 说明书4页 附图3页

(54)发明名称

一种安卓应用程序的安装方法和安装系统

(57)摘要

本发明适用于数据处理领域，提供了一种安卓应用程序的安装方法和安装系统，所述安装方法包括：当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在所述判断为是时，同意所述安装请求；判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装；将所述掩码数据添加到应用安装模块，并进行安卓应用程序的安装。实施本发明实施例，安卓应用程序在安装过程中，会经过adb和掩码的验证，可以保证安装应用程序的安全安装。



CN 107766061 A

1.一种安卓应用程序的安装方法,其特征在于,所述安装方法包括:

当接收到安卓应用程序的安装请求时,判断本地安卓调试桥adb是否为授权adb,并在所述判断为是时,同意所述安装请求;

判断用户的掩码数据与授权码是否相同,如果相同则允许安卓应用程序的安装;

将所述掩码数据添加到应用安装模块,并进行安卓应用程序的安装。

2.如权利要求1所述的安装方法,其特征在于,所述判断本地adb是否为授权adb,并在判断为是时,同意所述安装请求,包括:

接收授权主机发送的签名报文;

通过预设的adb公钥对所述签名报文进行解密;

将所述经过解密的签名报文与本地的令牌进行比对,如果所述经过解密的签名报文与所述令牌相同,则所述本地adb为授权adb。

3.如权利要求1所述的安装方法,其特征在于,所述判断用户的掩码数据与授权码是否相同,如果相同则允许安卓应用程序的安装,包括:

获取安卓应用程序调用升级接口传递的掩码;

对所述掩码进行分拆处理,并对原接口标识位进行过滤处理,根据所述过滤处理提取对应的bit位数据,通过预设的对比算法对所述bit位数据进行计算获取要传入安装模块的数值;

将所述数值与授权码进行比较,如果所述数值与授权码相同,则允许安卓应用的安装。

4.如权利要求1～3任一项所述的安装方法,其特征在于,在所述将所述掩码数据添加到应用安装模块,并进行安卓应用程序的安装的步骤之后,所述安装方法还包括:

显示所述安卓应用程序的安装结果。

5.如权利要求4所述的安装方法,其特征在于,所述安装结果包括:adb开启结果、安卓应用程序显示结果。

6.一种安卓应用程序的安装系统,其特征在于,所述安装系统包括:

adb判断单元,用于当接收到安卓应用程序的安装请求时,判断本地安卓调试桥adb是否为授权adb,并在所述判断为是时,同意所述安装请求;

授权码判断单元,用于判断用户的掩码数据与授权码是否相同,如果相同则允许安卓应用程序的安装;

安装单元,用于将所述掩码数据添加到应用安装模块,并进行安卓应用程序的安装。

7.如权利要求6所述的安装系统,其特征在于,所述adb判断单元,包括:

接收子单元,用于接收授权主机发送的签名报文;

解密子单元,用于通过预设的adb公钥对所述签名报文进行解密;

比对子单元,用于将所述经过解密的签名报文与本地的令牌进行比对,如果所述经过解密的签名报文与所述令牌相同,则所述本地adb为授权adb。

8.如权利要求6所述的安装系统,其特征在于,所述授权码判断单元,包括:

掩码获取子单元,用于获取安卓应用程序调用升级接口传递的掩码;

数值获取子单元,用于对所述掩码进行分拆处理,并对原接口标识位进行过滤处理,根据所述过滤处理提取对应的bit位数据,通过预设的对比算法对所述bit位数据进行计算获取要传入安装模块的数值;

比较子单元，用于将所述数值与授权码进行比较，如果所述数值与授权码相同，则允许安卓应用的安装。

9.如权利要求6～8任一项所述的安装系统，其特征在于，所述安装系统还包括：

显示单元，用于显示所述安卓应用程序的安装结果。

10.如权利要求9所述的安装系统，其特征在于，所述安装结果包括：adb开启结果、安卓应用程序显示结果。

一种安卓应用程序的安装方法和安装系统

技术领域

[0001] 本发明属于数据处理领域，尤其涉及一种安卓应用程序的安装方法和安装系统。

背景技术

[0002] Android是Google公司和开放手持联盟领导及开发的基于Linux平台的一套操作系统。该平台包括操作系统、中间件、用户界面和应用程序。由于源码开放，Android可以被移植到不同的硬件平台上。

[0003] 伴随着Android技术发展的同时，海量android应用程序(一般称为apk)也诞生出来。由于用户对技术细节的不了解，随意安装apk的行为为一些盗版、恶意的应用程序带来有机可趁的机会。通常这些apk会开机自动启动并常驻后台，消耗了大量的系统资源，以及窃取用户隐私、篡改系统等。

[0004] 因此，在上述背景情况下，基于对android系统安全和保护用户隐私的考虑，如何管控apk的安装，及防止用户未经授权安装apk，成了必须要解决的问题。

发明内容

[0005] 本发明实施例的目的在于提供一种安卓应用程序的安装方法和安装系统，以解决现有技术在安装安卓应用程序时不安全的问题。

[0006] 本发明实施例是这样实现的，一种安卓应用程序的安装方法，所述安装方法包括：

[0007] 当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在所述判断为是时，同意所述安装请求；

[0008] 判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装；

[0009] 将所述掩码数据添加到应用安装模块，并进行安卓应用程序的安装。

[0010] 本发明实施例的另一目的在于提供一种安卓应用程序的安装系统，所述安装系统包括：

[0011] adb判断单元，用于当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在所述判断为是时，同意所述安装请求；

[0012] 授权码判断单元，用于判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装；

[0013] 安装单元，用于将所述掩码数据添加到应用安装模块，并进行安卓应用程序的安装。

[0014] 本发明实施例，当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在判断为是时，同意安装请求，判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装，将掩码数据添加到应用安装模块，并进行安卓应用程序的安装，经过adb和掩码的验证，可以保证安装应用程序的安全安装。

附图说明

[0015] 图1为本发明一示例性实施例示出的一种安卓应用程序的安装方法的流程图；

[0016] 图2为本发明另一示例性实施例示出的一种安卓应用程序的安装方法的流程图；

[0017] 图3为本发明再一示例性实施例示出的一种安卓应用程序的安装方法的流程图；

[0018] 图4为本发明一示例性实施例示出的一种安卓应用程序的安装系统的结构图；

[0019] 图5为本发明另一示例性实施例示出的一种安卓应用程序的安装系统的结构图；

[0020] 图6为本发明再一示例性实施例示出的一种安卓应用程序的安装系统的结构图。

具体实施方式

[0021] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，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。

[0022] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0023] 如图1所示为本发明一示例性实施例示出的一种安卓应用程序的安装方法的流程图，所述安装方法包括：

[0024] 步骤S101，当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在所述判断为是时，同意所述安装请求。

[0025] 在本发明实施例中，安卓应用程序在安装时可以通过adb(Android DebugBriage，安卓调试桥)的形式绕开安卓系统本身的防护机制，因此需要对安卓系统的adb进行判断，判断adb是否为经过授权的adb。

[0026] 如图2所示为本发明另一示例性实施例示出的一种安卓应用程序的安装方法的流程图，所述判断本地adb是否为授权adb，并在判断为是时，同意所述安装请求，具体为：

[0027] 步骤S201，接收授权主机发送的签名报文；

[0028] 步骤S202，通过预设的adb公钥对所述签名报文进行解密；

[0029] 步骤S203，将所述经过解密的签名报文与本地的令牌进行比对，如果所述经过解密的签名报文与所述令牌相同，则所述本地adb为授权adb。

[0030] 在本发明实施例中，在进行授权判断时，授权主机会向安卓设备发送一随机令牌，该随机令牌被签名报文进行了加密，安卓设备中预先保存有授权主机发送的adb公钥，通过该adb公钥可以对签名报文进行解密，将解密后获取的随机令牌与预先存储在安卓设备本地的令牌进行比对，即可判断本地的adb是否为授权adb，如果相同，则为授权adb，可以进行后续的安装流程，如果不同，则为未授权adb，断开adb连接。

[0031] 步骤S102，判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装。

[0032] 在本发明实施例中，安卓应用程序在安装时通常会调用系统PM工具中的install接口，进而调用系统的安装服务。因此，对系统PM的install命令的入口参数进行扩展，增加一-m选项，通过该-m选项可以实现掩码数据的传递。在安装校验模块中，该掩码会与通过其他方式确定的标志位进行运算，其运算结果会作为调用安装服务方法的标志位参数传入，若参数符合要求则进入安装模式，若不符合则拒绝安装。

[0033] 如图3所示为本发明再一示例性实施例示出的一种安卓应用程序的安装方法的流程图，所述判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装，

包括：

[0034] 步骤S301，获取安卓应用程序调用升级接口传递的掩码；

[0035] 步骤S302，对所述掩码进行分拆处理，并对原接口标识位进行过滤处理，根据所述过滤处理提取对应的bit位数据，通过预设的对比算法对所述bit位数据进行计算获取要传入安装模块的数值；

[0036] 步骤S303，将所述数值与授权码进行比较，如果所述数值与授权码相同，则允许安卓应用的安装。

[0037] 步骤S103，将所述掩码数据添加到应用安装模块，并进行安卓应用程序的安装。

[0038] 在本发明实施例中，掩码校验结果为相同则表示安卓应用程序为安全的，可以进行安卓应用程序的安装。

[0039] 本发明实施例，当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在判断为是时，同意安装请求，判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装，将掩码数据添加到应用安装模块，并进行安卓应用程序的安装，经过adb和掩码的验证，可以保证安装应用程序的安全安装。

[0040] 作为本发明的一个可选实施例，在所述将所述掩码数据添加到应用安装模块，并进行安卓应用程序的安装的步骤之后，所述安装方法还包括：

[0041] 显示所述安卓应用程序的安装结果。

[0042] 在本发明实施例中，在安装完安卓应用程序之后，设备还可以将安卓应用程序的安装结果呈现给用户，所述安装结果包括但不限于：adb开启结果、安卓应用程序显示结果等。

[0043] 如图4所示为本发明一示例性实施例示出的一种安卓应用程序的安装系统的结构图，所述安装系统包括：

[0044] adb判断单元401，用于当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在所述判断为是时，同意所述安装请求。

[0045] 在本发明实施例中，安卓应用程序在安装时可以通过adb(Android DebugBriage，安卓调试桥)的形式绕开安卓系统本身的防护机制，因此需要对安卓系统的adb进行判断，判断adb是否为经过授权的adb。

[0046] 如图5所示为本发明另一示例性实施例示出的一种安卓应用程序的安装系统的结构图，所述adb判断单元401，包括：

[0047] 接收子单元4011，用于接收授权主机发送的签名报文；

[0048] 解密子单元4012，用于通过预设的adb公钥对所述签名报文进行解密；

[0049] 比对子单元4013，用于将所述经过解密的签名报文与本地的令牌进行比对，如果所述经过解密的签名报文与所述令牌相同，则所述本地adb为授权adb。

[0050] 在本发明实施例中，在进行授权判断时，授权主机会向安卓设备发送一随机令牌，该随机令牌被签名报文进行了加密，安卓设备中预先保存有授权主机发送的adb公钥，通过该adb公钥可以对签名报文进行解密，将解密后获取的随机令牌与预先存储在安卓设备本地的令牌进行比对，即可判断本地的adb是否为授权adb，如果相同，则为授权adb，可以进行后续的安装流程，如果不同，则为未授权adb，断开adb连接。

[0051] 授权码判断单元402，用于判断用户的掩码数据与授权码是否相同，如果相同则允

许安卓应用程序的安装。

[0052] 在本发明实施例中，安卓应用程序在安装时通常会调用系统PM工具中的install接口，进而调用系统的安装服务。因此，对系统PM的install命令的入口参数进行扩展，增加一-m选项，通过该-m选项可以实现掩码数据的传递。在安装校验模块中，该掩码会与通过其他方式确定的标志位进行运算，其运算结果会作为调用安装服务方法的标志位参数传入，若参数符合要求则进入安装模式，若不符合则拒绝安装。

[0053] 如图6所示为本发明再一示例性实施例示出的一种安卓应用程序的安装系统的结构图，所述授权码判断单元402，包括：

[0054] 掩码获取子单元4021，用于获取安卓应用程序调用升级接口传递的掩码；

[0055] 数值获取子单元4022，用于对所述掩码进行分拆处理，并对原接口标识位进行过滤处理，根据所述过滤处理提取对应的bit位数据，通过预设的对比算法对所述bit位数据进行计算获取要传入安装模块的数值；

[0056] 比较子单元4023，用于将所述数值与授权码进行比较，如果所述数值与授权码相同，则允许安卓应用的安装。

[0057] 安装单元403，用于将所述掩码数据添加到应用安装模块，并进行安卓应用程序的安装。

[0058] 在本发明实施例中，掩码校验结果为相同则表示安卓应用程序为安全的，可以进行安卓应用程序的安装。

[0059] 本发明实施例，当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在判断为是时，同意安装请求，判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装，将掩码数据添加到应用安装模块，并进行安卓应用程序的安装，经过adb和掩码的验证，可以保证安装应用程序的安全安装。

[0060] 作为本发明的一个可选实施例，所述安装系统还包括：

[0061] 显示单元，用于显示所述安卓应用程序的安装结果。

[0062] 在本发明实施例中，在安装完安卓应用程序之后，设备还可以将安卓应用程序的安装结果呈现给用户，所述安装结果包括但不限于：adb开启结果、安卓应用程序显示结果等。

[0063] 本领域普通技术人员可以理解为上述实施例所包括的各个单元只是按照功能逻辑进行划分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本发明的保护范围。

[0064] 本领域普通技术人员还可以理解，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指令相关的硬件来完成，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，包括ROM/RAM、磁盘、光盘等。

[0065] 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、等同替换和改进等，均应包含在本发明的保护范围之内。

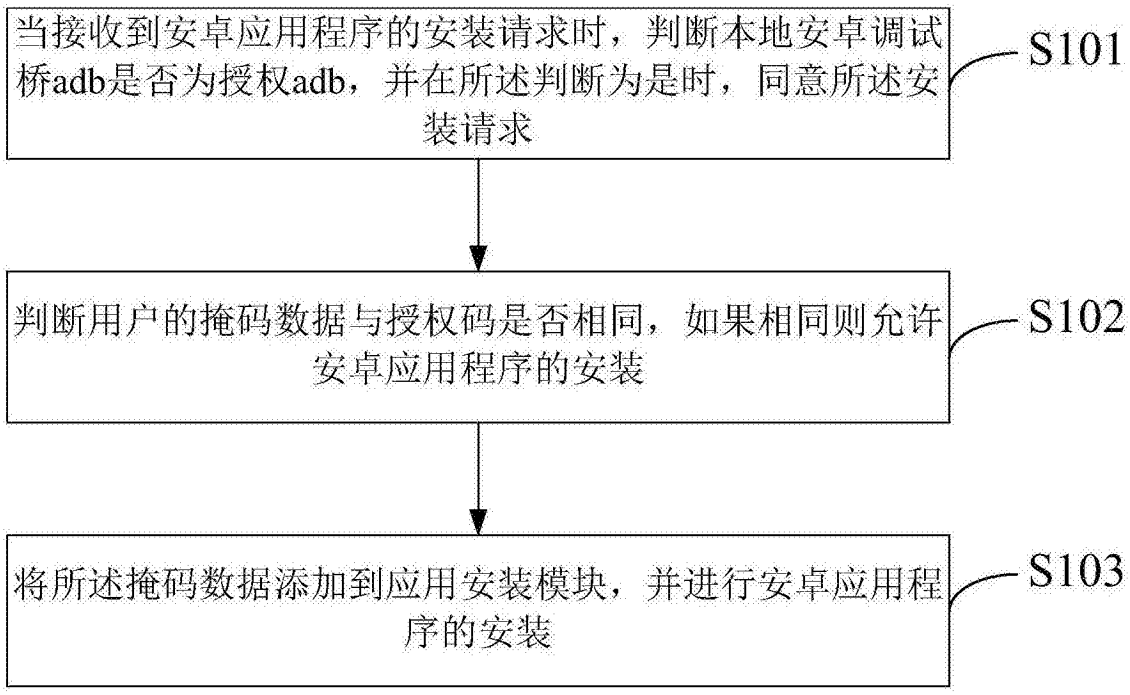

当接收到安卓应用程序的安装请求时，判断本地安卓调试桥adb是否为授权adb，并在所述判断为是时，同意所述安装请求
S101
判断用户的掩码数据与授权码是否相同，如果相同则允许安卓应用程序的安装
S102
将所述掩码数据添加到应用安装模块，并进行安卓应用程序的安装
S103

图1

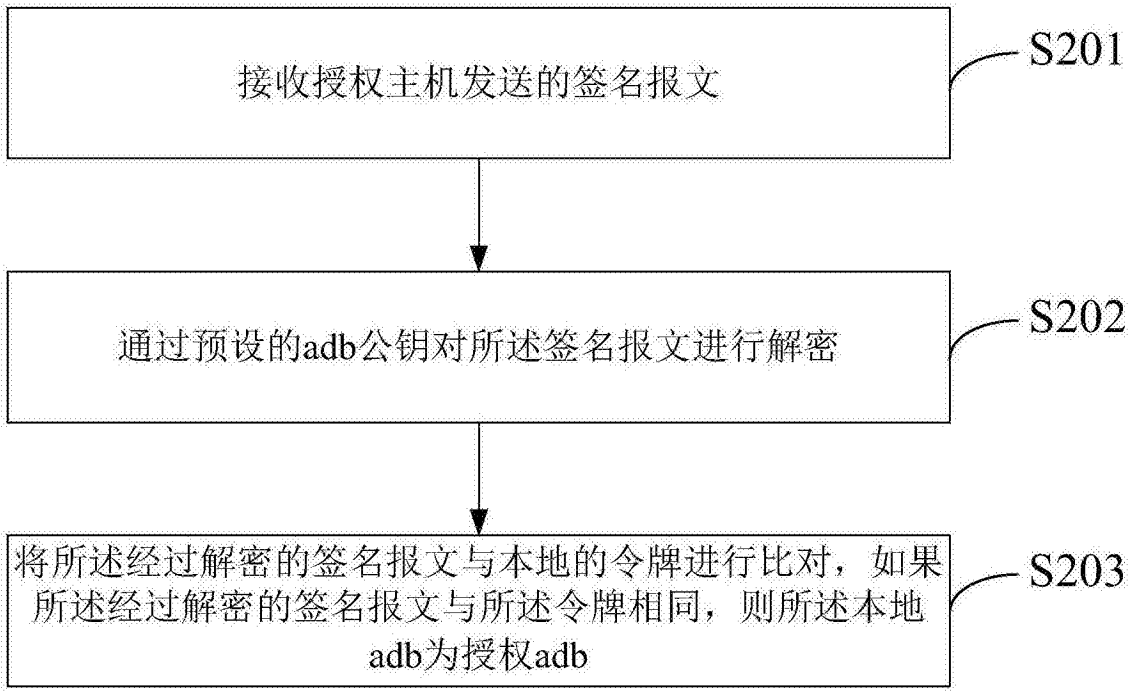

接收授权主机发送的签名报文
S201
通过预设的adb公钥对所述签名报文进行解密
S202
将所述经过解密的签名报文与本地的令牌进行比对，如果所述经过解密的签名报文与所述令牌相同，则所述本地adb为授权adb
S203

图2

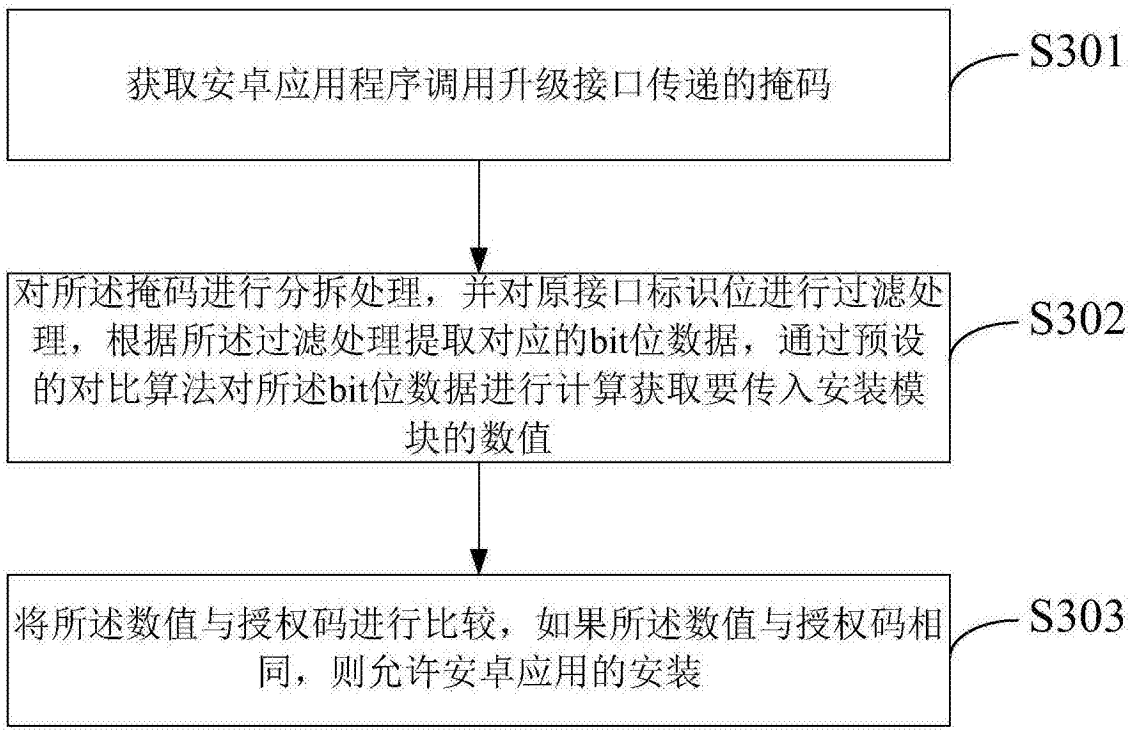

获取安卓应用程序调用升级接口传递的掩码
S301
对所述掩码进行分拆处理，并对原接口标识位进行过滤处理，根据所述过滤处理提取对应的bit位数据，通过预设的对比算法对所述bit位数据进行计算获取要传入安装模块的数值
S302
将所述数值与授权码进行比较，如果所述数值与授权码相同，则允许安卓应用的安装
S303

图3

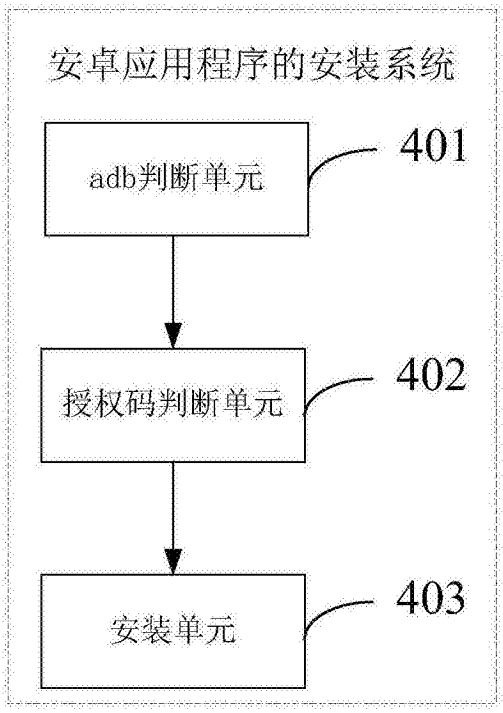

安卓应用程序的安装系统
adb判断单元
401
授权码判断单元
402
安装单元
403

图4

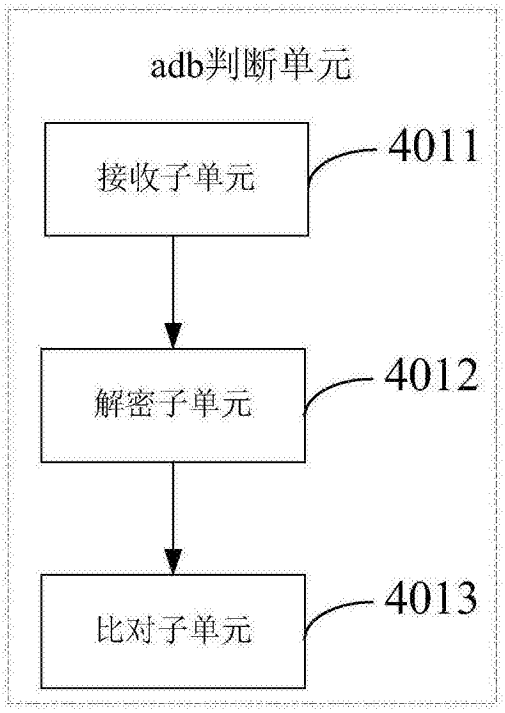

adb判断单元
接收子单元
4011
解密子单元
4012
比对子单元
4013

图5

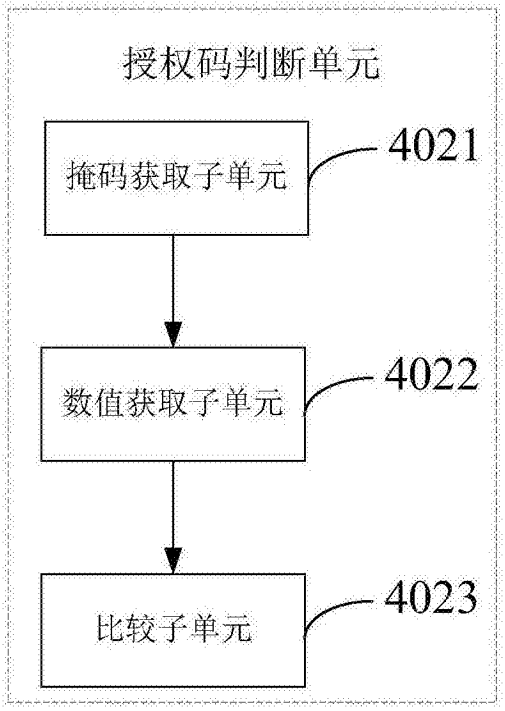

授权码判断单元
掩码获取子单元
4021
数值获取子单元
4022
比较子单元
4023

图6