(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 107733899 B
(45)授权公告日 2020.06.09

(21)申请号 201710989345.8

(22)申请日 2017.10.23

(65)同一申请的已公布的文献号
申请公布号 CN 107733899 A

(43)申请公布日 2018.02.23

(73)专利权人 北卡科技有限公司
地址 350108 福建省福州市闽侯县科技东路福州高新区海西高新技术产业园创新园10#楼1层132室

(72)发明人 陈明志 刘川葆 董晨 许春耀 杨小权 林伟宁

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04M 1/725(2006.01)
H04W 4/80(2018.01)
G06K 7/10(2006.01)
G06Q 10/08(2012.01)
G07F 17/12(2006.01)

(56)对比文件
CN 204904335 U,2015.12.23,
CN 104217318 A,2014.12.17,
CN 106296049 A,2017.01.04,
CN 203995189 U,2014.12.10,
CN 104123624 A,2014.10.29,
CN 104268731 A,2015.01.07,
CN 106339744 A,2017.01.18,
US 2012246075 A1,2012.09.27,
马秀,何家辉,孙秀扬,关瑜.基于二维码和NFC加密的快递签收系统.《中国科技信息》.2016,(第19期),55-58页.
Sha Liu;Junyu Wang.A security-enhanced express delivery system based on NFC.《2016 13th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)》.2016,第1-3页.

审查员 蔡红

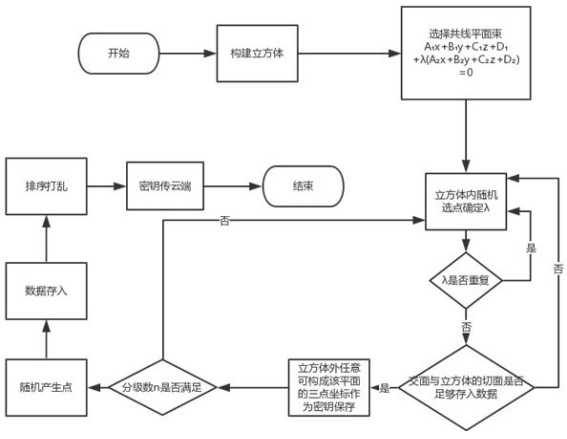
权利要求书2页 说明书12页 附图3页

(54)发明名称

一种基于NFC的快递面单隐私保护的加密方法

(57)摘要

本发明涉及一种基于NFC的快递面单隐私保护的加密方法。通过将快递单信息分为N个部分信息,而后采用基于三维点阵的切面加密方法将快递单信息分为N个切面加密,即形成包括N个阶段加密信息的,以此实现了快递的揽收、中转、收件三个过程的快递信息保密。本发明有效保护了用户的隐私,由于不是使用纸质面单,而是通过NFC设备处理使用的是无线通信,所以不会存在肉眼可以识别获得用户个人信息的问题;而通过加密的方式保存数据,因此快递员工即使获得了数据,也无法分析破解获取到用户个人信息。



CN 107733899 B

1.一种基于NFC的快递面单隐私保护的加密方法,其特征在于:包括如下步骤,

(1)揽件过程:

S1、寄件人通过具有NFC功能的手机下载快递APP,并在快递APP上填写快递单信息,而后快递APP将填写后的快递单信息发送给云端;

S2、云端通过基于三维点阵的切面加密方法加密快递单信息,生成加密数据,并将加密数据发送给快递APP;基于三维点阵的切面加密方法加密快递单信息时,将快递单信息分为N个切面加密,即加密数据包括N个阶段加密信息,其中,N为大于1的自然数;

S3、快递APP将收到的加密数据通过手机NFC输入至快递NFC设备,快递NFC设备完成数据更新后,将快递NFC设备置于快递箱中,完成揽件;

(2)中转过程

S4、快递员将揽件后的快递箱运输至快递网点,在快递网点分拣流水线上,由NFC阅读器发送快递单编号查询讯号至快递箱中的快递NFC设备,快递NFC设备接收后返回快递单编号至NFC阅读器;

S5、NFC阅读器收到快递单编号以及阶段代码发送至后台服务器,后台服务器根据快递单编号及阶段代码提取出对应的阶段信息密钥并发送给NFC阅读器;

S6、NFC阅读器将阶段信息密钥发给快递NFC设备,快递NFC设备使用阶段信息密钥解密加密数据对应阶段信息,并将数据反馈发给NFC阅读器,而后快递网点分拣流水线依据数据反馈结果对快递箱进行分拣;

(3)派送过程:

S7、通知收件人阶段:派送员使用NFC阅读器对快递箱内的快递NFC设备发出快递单编号查询讯号,快递NFC设备将快递单编号发回给NFC阅读器,NFC阅读器将快递单编号以及取件信息发送给云端,云端通过快递单编号查询确认信息密钥,再发送通知信息以及确认信息密钥给收件人的快递APP;

S8、收件人签收阶段:收件人通过快递APP使用手机NFC功能把确认信息密钥发送给快递NFC设备,快递NFC设备使用确认信息密钥进行解密,提取出确认信息,并通过手机NFC发送给快递APP,快递APP把确认信息发送给云端服务器,完成认证过程;而后,云端发送确认收件的通知给派送员,派送员回收快递NFC设备,签收完成;

所述步骤S2中,云端通过基于三维点阵的切面加密方法加密快递单信息,生成加密数据的具体实现方式如下,

S21、将快递单信息分为N个部分数据,设分级数n＝0,设置各个部分的密钥集合为Φ,初始为空集;

S22、根据快递单信息划分的N个部分数据,预测各个切面加入数据的大小,构建立方体;再选择一个共线在立方体之外的共线平面束:$A1x+B1y+C1z+D1+\lambda(A2x+B2y+C2z+D2)=0$,其中A1、B1、C1、D1、A2、B2、C2、D2为一次随机生成的常量,λ是变量;

S23、随机选择立方体内的一个点,确定λ的值,由此得到一个确定的平面方程,此平面方程是立方体的一个切面方程;

S24、检查λ是否有重复,若λ已经被使用过,则返回步骤S23;

S25、判断切面内点x的范围是否足够长,以能存入该部分信息为准,若长度不足,则返回步骤S23;

S26、记录下λ的值，即λn＝λ，λn作为密钥保存；分级数n＝n+1；

S27、检查分级数n是否达到N，若否，则返回步骤S23；

S28、随机产生大量的点；

S29、对前面产生的N个切面依次进行数据存入：在第n个切面，算得切面的x的范围为x1到x2，再对步骤S28中生成的点中所有属于切面内的点(m,n,k)做如下判断：

若数据的二进制编码中第m-x1位为1，则保留该点，若为0，则删除该点，若存在二进制编码中为1的位置p，却没有任何点与之对应，则生成满足x＝p+x1且在切面上的随机点；

S30、对生成的点的排列顺序进行打乱，构成密文

S31、将A1、B1、C1、D1、A2、B2、C2、D2和密钥集合Φ进行保存。

2.根据权利要求1所述的一种基于NFC的快递面单隐私保护的加密方法，其特征在于：所述步骤S3中，快递NFC设备完成数据更新后，还需反馈信息至云端后，云端计算相应的收费信息并通过快递APP将收费信息告知用户，用户完成收费后，快递APP将收费确认反馈云端后，再将快递NFC设备置于快递箱中。

3.根据权利要求1所述的一种基于NFC的快递面单隐私保护的加密方法，其特征在于：后台服务器根据快递单编号及阶段代码提取出对应的阶段信息密钥并发送给NFC阅读器，NFC阅读器将阶段信息密钥发给快递NFC设备，快递NFC设备使用阶段信息密钥解密加密数据对应阶段信息的具体实现方式如下，

S61、根据需要解密的阶段信息k，0≤k≤N-1，提取出阶段信息密钥λk，随机选取出不在同一直线上且满足A1x+B1y+C1z+D1+λk(A2x+B2y+C2z+D2)＝0的三个点，构建平面方程组{A3x+B3y+C3z＝D3，A4x+B4y+C4z＝D4}作为阶段信息密钥；

S62、将平面方程组{A3x+B3y+C3z＝D3，A4x+B4y+C4z＝D4}发送给快递NFC设备；

S63、计算平面方程组{A3x+B3y+C3z＝D3，A4x+B4y+C4z＝D4}与立方体的8条棱的交点，获得平面方程组{A3x+B3y+C3z＝D3，A4x+B4y+C4z＝D4}与立方体构成的切面的所有点的x的取值范围，为x1到x2；同时生成一个数组M，长度为x2-x1+1，编号从0位到x2-x1位；

S64、将加密数据所有的点(xm,ym,zm)代入平面方程组{A3x+B3y+C3z＝D3，A4x+B4y+C4z＝D4}判断是否满足平面方程，若满足，则标记数组M的xm-x1位为1，不满足的则跳过；

S65、遍历完所有的点后，数组M即为该阶段信息明文的二进制编码，即解得明文。

一种基于NFC的快递面单隐私保护的加密方法

技术领域

[0001] 本发明涉及一种基于NFC的快递面单隐私保护的加密方法。

背景技术

[0002] 传统国家邮政局发布《2016年中国快递发展指数报告》显示中国的快递量已经超过300亿件，中国快递发展指数(CEDI)同比提高40.8%，快递业务亦居世界首位[1]。从整体的趋势上看，我国快递的发展还将保持着相当长时间的增长，以及相当大的一个体量。从服务上看，各大快递公司也将提高服务质量作为重点，当前的重点主要是集中在如何提高物流速度，对快递的“最后一公里”投入较大等方面。但提高服务质量也势必需要考虑到如何缩减填单揽件的时间耗费，以及收件时如何确保安全无误地交托到客户手中，当快递业务集中繁忙的时候，如何快速地完成快递签收的问题，在整个过程中，如何保护客户的个人身份信息，隐私信息不被泄露的问题。

[0003] 随着社会的发展，人们越来越重视个人的隐私。而快递面单上有丰富的个人隐私的相关信息，如个人的住址，姓名，联系电话等等。在快递中，人们有时候也不想让别人知道快递的内容物是什么，来自哪里，来自何人等等，比如，快递来自各种旗舰店，即可以根据旗舰店出售货物的类型进行广告的推送等等[2]。由于这些个人信息具有一定的价值，这种售卖个人隐私的市场一直存在着。多家快递公司的面单在网络上公然出售，价格从0.4元到2元不等，交易量数千上万[3]。

[0004] 现阶段使用的快递面单主要是由纸质面单为主。纸质面单上的个人信息全部是暴露在外的，通过人工肉眼即可以辨认，而如果是打印的纸质面单则更容易获得个人信息，通过拍摄成照片就可以通过软件提取出文字信息，效率很高，技术也已经相当成熟[4]。在快递揽件，中转，派送过程中，由于快递员的基本素质不强，流动性大，若是有利益，极有可能出卖用户个人信息。快递员撕下的快递回执，上面也有个人信息，也可能造成个人隐私的泄露。签收后用户对快递箱的处理，通常是直接丢弃到垃圾箱，快递面单通常是不做处理的，而快递箱可以被收垃圾人回收再利用，这可能造成泄露信息。因此使用纸质面单的方式，在保护用户个人信息的方面，有很多安全隐患[5]。

[0005] 知名调研机构Frost&Sullivan曾公布数据，到2015年，欧洲出售的手机中38%将配备近场通信(Near Field Communication,NFC)功能[6]。美国科技研究公司In-Stat 曾发布报告，到2015年，全球NFC市场将增长30%，达到3.75亿用户，出库芯片12亿个[7]。具有NFC设备的手机和使用NFC设备的用户越来越多，使用NFC设备可以对快递用户个人信息数据进行加密，保证安全，能提高分拣速度，揽收速度等，通过NFC设备来替代纸质面单是极具潜力的。

[0006] 针对快递纸质面单在用户个人信息保护，快递揽件中转派送效率上的问题，本文提出一种基于NFC的一种快递面单加密方法。方案采用基于三维点阵的切面加密方法，对NFC设备内的用户个人信息进行加密，从而防止在快递过程中用户个人信息被非法获取，有效保护用户个人信息安全，从而保护用户个人隐私，并通过NFC设备，能节省快递揽件、中

转、派送的时间，提高效率，也能更好地防止快递冒领的问题。

[0007] 1、RFID与NFC

[0008] 无线射频识别技术(RFID)是一种使设备与设备之间能够进行无线通信的技术[8]。其中，设备可以是与云端或后台数据库相连的阅读器(如POS机)或支持NFC功能的设备(如支持NFC功能的手机)。NFC是一种短距高频的无线射频识别技术[9]，使用的频段为13.56MHz，传输距离在20cm以内[10]。传统NFC设备的安全性依赖于底层的一个硬件设备——SE(Secure Element)模块，基于该模块的应用需要基于可信服务管理(Trusted Service Management，TSM)。

[0009] SE模块本身是一个小型的智能芯片，能进行一些数据处理，如对短小数据的加密等[11]，因此通常把用于身份认证的相关信息，如云端分配给个人的唯一编码、个人信息等，存放在SE模块的存储单元中，以达到使身份认证的相关信息与设备系统(如手机系统)的数据相隔离的目的，从而保证身份认证的相关信息不受其他系统数据的干扰以实现相对安全。通过SE模块对进出数据进行独立的加密解密，使得数据的传输过程相对安全[12]。

[0010] 2、RFID在快递领域的应用

[0011] 我国现在的快递分拣主要是手工分拣，使用大量的人力来完成分拣的工作，其次是半自动分拣，通过传送带将快递箱传送到分拣员手中，再进行人工识别，来完成分拣，最后是全自动分拣[13]。由于大量使用人力，在这个过程中，对从业人员的素质难以把握，从而使得用户的隐私和快递安全性也有所牺牲。随着劳动力成本的逐渐提高，快递行业势必会逐步走向自动化分拣。

[0012] 在使用自动化分拣的过程中，有许多种方案。文献[14]中介绍了对条形码进行图像识别来完成自动化分拣的方案，而进行识别时候，容易出现图形弯折，扭曲，污染，条形码位置偏移，条形码定位困难，识别困难等实际问题。文献[15]提供了ZigBee的方案进行快递分拣，文献[16]提出的使用RFID+条形码的方案，以无线网络的方式对快件进行识别，识别率已经99.9%，高于条形码方案的90%识别率，分拣的速度也有进一步的提高。总体上看，以RFID为代表的无线网络的方案更加适用于自动化分拣，进一步提高效率，因此，以RFID方案替代纸质面单具有足够的前景。然而，存入RFID设备内的用户信息，以明文的方式保存，依然有被泄露的风险，因此为了保护用户的隐私，仍然需要进行加密。

[0013] 3、加密方案

[0014] 对RFID设备的加密方案多是使用伪随机加密为主的方案，如文献[17]中的以伪随机数为基础的加密方式，特点是轻小，功耗低，速度快。文献[18]提出以AES为基础的加密方案，但此类传统的强加密算法，其代价都相对较高。

[0015] 由于快递业务的特点，揽件，中转，派送的各个部分中，并不需要知道全部的信息，为了防止超需信息引起的信息泄露，需要针对各个部分所需的信息分开加密，即表示，快递业务中的使用的加密方案需要有能按需获得信息的特点。现有的RFID加密方案，大多是对数据进行整体加密的，使用一个密钥能解开全部的数据。

[0016] 针对快递业务这种，需要对信息进行分段解密的，主要思路有以下几种：第一种，数据分段后，对各个分段数据使用同一种加密方式。第二种，数据分段后，各段数据使用不同的加密方案，如文献[19]，这样需要使用多套加密解密的系统。而我们希望，数据分段后，通过一定的手段，使数据产生变形，如混淆，替换等，之后能通过密钥对进行特定部分的数

据进行解密恢复，而剩余的部分不被发现，这样数据看上去依然是完整的，没有明显区分，特定密钥只能恢复特定的内容，从而达到按需获得信息特点。

发明内容

[0017] 本发明的目的在于提供一种基于NFC的快递面单隐私保护的加密方法，该方法有效保护了用户的隐私，由于不是使用纸质面单，而是通过NFC设备处理使用的是无线通信，所以不会存在肉眼可以识别获得用户个人信息的问题；而通过加密的方式保存数据，因此快递员工即使获得了数据，也无法分析破解获取到用户个人信息。

[0018] 为实现上述目的，本发明的技术方案是：一种基于NFC的快递面单隐私保护的加密方法，包括如下步骤，

[0019] (1)揽件过程：

[0020] S1、寄件人通过具有NFC功能的手机下载快递APP，并在快递APP上填写快递单信息，而后快递APP将填写后的快递单信息发送给云端；

[0021] S2、云端通过基于三维点阵的切面加密方法加密快递单信息，生成加密数据，并将加密数据发送给快递APP；基于三维点阵的切面加密方法加密快递单信息时，将快递单信息分为N个切面加密，即加密数据包括N个阶段加密信息，其中，N为大于1的自然数；

[0022] S3、快递APP将收到的加密数据通过手机NFC输入至快递NFC设备，快递NFC设备完成数据更新后，将快递NFC设备置于快递箱中，完成揽件；

[0023] (2)中转过程

[0024] S4、快递员将揽件后的快递箱运输中快递网点，在快递网点分拣流水线上，由NFC阅读器发送快递编号查询讯号至快递箱中的快递NFC设备，快递NFC设备接收后返回快递单编号至NFC阅读器；

[0025] S5、NFC阅读器收到快递单编号以及阶段代码发送至后台服务器，后台服务器根据快递单编号及阶段代码提取出对应的阶段信息密钥并发送给NFC阅读器；

[0026] S6、NFC阅读器将阶段信息密钥发给快递NFC设备，快递NFC设备使用阶段信息密钥解密加密数据对应阶段信息，并将数据反馈发给NFC阅读器，而后快递网点分拣流水线依据数据反馈结果对快递箱进行分拣；

[0027] (3)派送过程：

[0028] S7、通知收件人阶段：派送员使用NFC阅读器对快递箱内的快递NFC设备发出快递单编号查询讯号，快递NFC设备将快递单编号发回给NFC阅读器，NFC阅读器将快递单编号以及取件信息发送给云端，云端通过快递单编号查询确认信息密钥，再发送通知信息以及确认信息密钥给收件人的快递APP；

[0029] S8、收件人签收阶段：收件人通过快递APP使用手机NFC功能把确认信息密钥发送给快递NFC设备，快递NFC设备使用确认信息密钥进行解密，提取出确认信息，并通过手机NFC发送给快递APP，快递APP把确认信息发送给云端服务器，完成认证过程；而后，云端发送确认收件的通知给派送员，派送员回收快递NFC设备，签收完成。

[0030] 在本发明一实施例中，所述步骤S3中，快递NFC设备完成数据更新后，还需反馈信息至云端后，云端计算相应的收费信息并通过快递APP将收费信息告知用户，用户完成收费后，快递APP将收费确认反馈云端后，再将快递NFC设备置于快递箱中。

[0031] 在本发明一实施例中，所述步骤S2中，云端通过基于三维点阵的切面加密方法加密快递单信息，生成加密数据的具体实现方式如下，

[0032] S21、将快递单信息分为N个部分数据，设分级数n=0，设置各个部分的密钥集合为λ_n，初始为空集；

[0033] S22、根据快递单信息划分的N个部分数据，预测各个切面加入数据的大小，构建立方体；再选择一个共线在立方体之外的共线平面束：A1x+B1y+C1z+D1+λ(A2x+B2y+C2z+D2)=0，其中A1、B1、C1、D1、A2、B2、C2、D2为一次随机生成的常量，λ是变量；

[0034] S23、随机选择立方体内的一个点，确定λ的值，由此得到一个确定的平面方程，此平面方程是立方体的一个切面方程；

[0035] S24、检查λ是否有重复，若λ已经被使用过，则返回步骤S23；

[0036] S25、判断切面内点x的范围是否足够长，以能存入该部分信息为准，若长度不足，则返回步骤S23；

[0037] S26、记录下λ的值，即$\lambda_n=\lambda$，λ_n作为密钥保存；分级数n=n+1；

[0038] S27、检查分级数n是否达到N，若否，则返回步骤S23；

[0039] S28、随机产生大量的点；

[0040] S29、对前面产生的N个切面依次进行数据存入：在第n个切面，算得切面的x的范围为x1到x2，再对步骤S28中生成的点中所有属于切面内的点(m,n,k)做如下判断：

[0041] 若数据的二进制编码中第m-x1位为1，则保留该点，若为0，则删除该点，若存在二进制编码中为1的位置p，却没有任何点与之对应，则生成满足x=p+x1且在切面上的随机点；

[0042] S30、对生成的点的排列顺序进行打乱，构成密文

[0043] S31、将A1、B1、C1、D1、A2、B2、C2、D2和密钥集合λ_n进行保存。

[0044] 在本发明一实施例中，后台服务器根据快递单编号及阶段代码提取出对应的阶段信息密钥并发送给NFC阅读器，NFC阅读器将阶段信息密钥发给快递NFC设备，快递NFC设备使用阶段信息密钥解密加密数据对应阶段信息的具体实现方式如下，

[0045] S61、根据需要解密的阶段信息k，$0\le k\le N-1$，提取出阶段信息密钥λ_k，随机选取出不在同一直线上且满足A1x+B1y+C1z+D1+λ_k(A2x+B2y+C2z+D2)=0的三个点，构建平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}作为阶段信息密钥；

[0046] S62、将平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}发送给快递NFC设备；

[0047] S63、计算平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}与立方体的8条棱的交点，获得平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}与立方体构成的切面的所有点的x的取值范围，为x1到x2；同时生成一个数组M，长度为x2-x1+1，编号从0位到x2-x1位；

[0048] S64、将加密数据所有的点(xm,ym,zm)代入平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}判断是否满足平面方程，若满足，则标记数组M的xm-x1位为1，不满足的则跳过；

[0049] S65、遍历完所有的点后，数组M即为该阶段信息明文的二进制编码，即解得明文。

[0050] 相较于现有技术，本发明具有以下有益效果：

[0051] 首先，通过app填单的方式，有效地节省了填单所花费的时候；对于个人用户，需要手动进行单据的填写，很多时候存在字迹不清晰，填写不规范等问题，对于快递单的分拣投

递造成一定难度，通过app填单可以避免遇到这种情况造成的影响；对于商业用户，可以通过与淘宝的合作等方式进行改进，使得app能够进行自动填单，再通过人工核对，减少手动输入快递面单的耗时过程，以及疏忽大意引起的输入错误等问题；

[0052] 其次，有效保护了用户的隐私；因为不是使用纸质面单，而是通过NFC设备处理使用的是无线通信，所以不会存在肉眼可以识别获得用户个人信息的问题；而通过加密的方式保存数据，因此快递员工即使获得了数据，也无法分析破解获取到用户个人信息；

[0053] 最后，对于用户来说，不需要向快递员工出示身份信息，不需要将身份证提交给快递员工核定，可以避免重要的证件丢失，被拍摄记录等风险；对于收件人来说，由于需要使用手机NFC进行签收，可以很大程度上防止冒领，意外被人领走，如果需要替领，收件人也可以通过app对信得过的人进行授权，云端只需要把领取密钥发给授权人即可，领取人信息和情况也可以通过app进行确认，从而保证快递能到合法的人手中。

附图说明

[0054] 图1为本发明方法加密流程图。

[0055] 图2为快递业务过程。

[0056] 图3为揽件过程。

[0057] 图4为中转过程。

[0058] 图5为派送过程。

具体实施方式

[0059] 下面结合附图，对本发明的技术方案进行具体说明。

[0060] 本发明的一种基于NFC的快递面单隐私保护的加密方法，包括如下步骤，

[0061] (1)揽件过程：

[0062] S1、寄件人通过具有NFC功能的手机下载快递APP，并在快递APP上填写快递单信息，而后快递APP将填写后的快递单信息发送给云端；

[0063] S2、云端通过基于三维点阵的切面加密方法加密快递单信息，生成加密数据，并将加密数据发送给快递APP；基于三维点阵的切面加密方法加密快递单信息时，将快递单信息分为N个切面加密，即加密数据包括N个阶段加密信息，其中，N为大于1的自然数；

[0064] S3、快递APP将收到的加密数据通过手机NFC输入至快递NFC设备，快递NFC设备完成数据更新后，将快递NFC设备置于快递箱中，完成揽件；

[0065] (2)中转过程

[0066] S4、快递员将揽件后的快递箱运输中快递网点，在快递网点分拣流水线上，由NFC阅读器发送快递编号查询讯号至快递箱中的快递NFC设备，快递NFC设备接收后返回快递单编号至NFC阅读器；

[0067] S5、NFC阅读器收到快递单编号以及阶段代码发送至后台服务器，后台服务器根据快递单编号及阶段代码提取出对应的阶段信息密钥并发送给NFC阅读器；

[0068] S6、NFC阅读器将阶段信息密钥发给快递NFC设备，快递NFC设备使用阶段信息密钥解密加密数据对应阶段信息，并将数据反馈发给NFC阅读器，而后快递网点分拣流水线依据数据反馈结果对快递箱进行分拣；

[0069] (3)派送过程：

[0070] S7、通知收件人阶段：派送员使用NFC阅读器对快递箱内的快递NFC设备发出快递单编号查询讯号，快递NFC设备将快递单编号发回给NFC阅读器，NFC阅读器将快递单编号以及取件信息发送给云端，云端通过快递单编号查询确认信息密钥，再发送通知信息以及确认信息密钥给收件人的快递APP；

[0071] S8、收件人签收阶段：收件人通过快递APP使用手机NFC功能把确认信息密钥发送给快递NFC设备，快递NFC设备使用确认信息密钥进行解密，提取出确认信息，并通过手机NFC发送给快递APP，快递APP把确认信息发送给云端服务器，完成认证过程；而后，云端发送确认收件的通知给派送员，派送员回收快递NFC设备，签收完成。

[0072] 在本发明中，所述步骤S3中，快递NFC设备完成数据更新后，还需反馈信息至云端后，云端计算相应的收费信息并通过快递APP将收费信息告知用户，用户完成收费后，快递APP将收费确认反馈云端后，再将快递NFC设备置于快递箱中。

[0073] 在本发明中，所述步骤S2中，云端通过基于三维点阵的切面加密方法加密快递单信息，生成加密数据的具体实现方式如下，

[0074] S21、将快递单信息分为N个部分数据，设分级数n=0，设置各个部分的密钥集合为λ_n，初始为空集；

[0075] S22、根据快递单信息划分的N个部分数据，预测各个切面加入数据的大小，构建立方体；再选择一个共线在立方体之外的共线平面束：A1x+B1y+C1z+D1+λ(A2x+B2y+C2z+D2)=0，其中A1、B1、C1、D1、A2、B2、C2、D2为一次随机生成的常量，λ是变量；

[0076] S23、随机选择立方体内的一个点，确定λ的值，由此得到一个确定的平面方程，此平面方程是立方体的一个切面方程；

[0077] S24、检查λ是否有重复，若λ已经被使用过，则返回步骤S23；

[0078] S25、判断切面内点x的范围是否足够长，以能存入该部分信息为准，若长度不足，则返回步骤S23；

[0079] S26、记录下λ的值，即$\lambda_n=\lambda$，λ_n作为密钥保存；分级数n=n+1；

[0080] S27、检查分级数n是否达到N，若否，则返回步骤S23；

[0081] S28、随机产生大量的点；

[0082] S29、对前面产生的N个切面依次进行数据存入：在第n个切面，算得切面的x的范围为x1到x2，再对步骤S28中生成的点中所有属于切面内的点(m,n,k)做如下判断：

[0083] 若数据的二进制编码中第m-x1位为1，则保留该点，若为0，则删除该点，若存在二进制编码中为1的位置p，却没有任何点与之对应，则生成满足x=p+x1且在切面上的随机点；

[0084] S30、对生成的点的排列顺序进行打乱，构成密文

[0085] S31、将A1、B1、C1、D1、A2、B2、C2、D2和密钥集合λ_n进行保存。

[0086] 在本发明中，后台服务器根据快递单编号及阶段代码提取出对应的阶段信息密钥并发送给NFC阅读器，NFC阅读器将阶段信息密钥发给快递NFC设备，快递NFC设备使用阶段信息密钥解密加密数据对应阶段信息的具体实现方式如下，

[0087] S61、根据需要解密的阶段信息k，$0\leq k\leq N-1$，提取出阶段信息密钥λ_k，随机选取出不在同一直线上且满足A1x+B1y+C1z+D1+λ_k(A2x+B2y+C2z+D2)=0的三个点，构建平面

方程组{ A3x+B3y+C3z=D3,A4x+B4y+C4z=D4}作为阶段信息密钥；

[0088] S62、将平面方程组{ A3x+B3y+C3z=D3,A4x+B4y+C4z=D4}发送给快递NFC设备；

[0089] S63、计算平面方程组{ A3x+B3y+C3z=D3,A4x+B4y+C4z=D4}与立方体的8条棱的交点，获得平面方程组{ A3x+B3y+C3z=D3,A4x+B4y+C4z=D4}与立方体构成的切面的所有点的x的取值范围，为x1到x2；同时生成一个数组M，长度为x2-x1+1，编号从0位到x2-x1位；

[0090] S64、将加密数据所有的点(xm,ym,zm)代入平面方程组{ A3x+B3y+C3z=D3,A4x+B4y+C4z=D4}判断是否满足平面方程，若满足，则标记数组M的xm-x1位为1，不满足的则跳过；

[0091] S65、遍历完所有的点后，数组M即为该阶段信息明文的二进制编码，即解得明文。

[0092] 以下为本发明的具体实现过程。

[0093] 1、本发明中采用的基于三维点阵的切面加密方法

[0094] 在纸质快递面单上集中了用户的个人信息，如姓名，电话，家庭住址等等，然而在分拣、运输等过程中实际上并不需要用到全部的个人信息，这些不需要用到的个人信息却具有价值，并且容易泄露，对用户的个人隐私和人身安全造成了一定威胁。因此，设计了基于三维点阵的切面加密方法，将各个过程所需要的信息分别存放在三维点阵的特定切面上，而切面方程系数则作为密钥。假设根据需求，需要把信息分成N个部分，设分级数n=0，设置各个部分的密钥的集合为λ_n，现在为空。加密流程图如图1所示：

[0095] 加密过程：

[0096] (1)需要预测各个切面加入数据的大小，构建立方体(例如，x,y,z的范围为0~100，构成100X100X100的立方体)。再选择一个共线在立方体之外的共线平面束：A1x+B1y+C1z+D1+λ (A2x+B2y+C2z+D2)=0(其中A1、B1、C1、D1、A2、B2、C2、D2为一次随机生成的常量，λ是变量)。

[0097] (2)随机选择立方体内的一个点，确定λ的值，由此得到一个确定的平面方程，此平面方程是立方体的一个切面方程。

[0098] (3)检查λ是否有重复，如果λ已经被使用过，则返回第二步；

[0099] (4)判断切面内点的x的范围是否足够长，能存入该部分的信息(如，要存入的信息为一个数字5，二进制编码101，二进制编码长度是3，则需要3位，若x的范围为4到10，则有7位，因此该切面足够存入信息)。若长度不足，则返回第二步；

[0100] (5)记录下λ的值，即$\lambda_n=\lambda$，λ_n作为密钥保存。分级数n=n+1。

[0101] (6)检查分级数n是否达到N；若否则返回第二步；

[0102] (7)随机产生足够大量的点；

[0103] (8)对前面产生的N个切面依次进行数据存入。操作为：在第n个切面，算得切面的x的范围为x1到x2，再对(7)中生成的点中所有属于切面内的点(m,n,k)做如下判断：若数据的二进制编码中第m-x1位(二进制编码从第0位开始)为1，则保留该点，若为0则，则删除该点(如，存入数据为数字5，二进制编码为101，x的范围为4到10，则保留x=4，x=6且属于切面的点，删除属于该切面的其他点)。若存在二进制编码中为1的位置p，却没有任何点与之对应，则生成满足x=p+x1且在切面上的随机点。

[0104] (9)对生成的点的排列顺序进行打乱。这些点一起构成密文。可以发送出去。

[0105] (10)将A1、B1、C1、D1、A2、B2、C2、D2和密钥集合λ_n进行保存。

[0106] 解密过程：

[0107] (1)根据需要解密的部分k($0 \le k \le N-1$)，提取出λ_k，随机选取出不在同一直线上且满足A1x+B1y+C1z+D1+λ_k(A2x+B2y+C2z+D2)=0的三个点，构建平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}作为阶段信息密钥。

[0108] (2)将平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}发送给解密方。

[0109] (3)计算平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}与立方体的8条棱的交点，可以获得平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}与立方体构成的切面的所有点的x的取值范围，为x1到x2。同时生成一个数组M，长度为x2-x1+1，编号从0位到x2-x1位。

[0110] (4)对密文(即为三维点的数据)所有的点(xm，ym，zm)代入平面方程组{ A3x+B3y+C3z=D3，A4x+B4y+C4z=D4}判断是否满足平面方程，若满足，则标记数组M的xm-x1位为1，不满足的则跳过。

[0111] (5)遍历完所有的点后，数组M即为明文的二进制编码，即解得明文。

[0112] 2、本发明基于NFC的快递面单加密方法

[0113] 本发明将一次快递业务分为三个过程：揽件过程，中转(分拣、运输)过程，派送过程，如图2所示。

[0114] 在揽件过程中，应完成身份认证，信息登记，信息录入快递专用NFC设备的工作。在中转过程，应完成分拣、运输的工作。在派送过程中，应完成通知用户，身份认证，快递专用NFC设备回收的工作。各过程的具体实施方法如下。

[0115] 2.1揽件过程

[0116] 寄件人需要使用特定的快递公司的app，具有NFC功能的手机，并预先注册好，登记身份证号码等有关个人信息。在快递业务中，寄件人在app上进行填写快递单，按照快递公司的要求输入包括寄件人姓名，寄件人地址，寄件人邮编，寄件人联系方式，收件人姓名，收件人地址，收件人邮编，收件人联系方式等相关信息。app将填写好的快递单信息传给云端。云端通过基于三维点阵的切面加密方法生成加密数据，并将加密数据传递给app。app把收到的加密数据通过手机NFC输入到快递专用NFC设备，快递专用NFC设备完成数据的更新后，把确认完成的反馈通过手机NFC传递给app，再由app发送给云端。云端计算好收费信息，并通过app把收费信息告知用户，用户完成收费之后，app把收费确认交给云端登记。快递员确认用户已经付费后，把快递专用NFC设备放入快递箱中，并连同快递箱封装好。从而完成揽件过程，如图3所示。

[0117] 2.2中转过程

[0118] 揽件的快递员将快递箱无差别运输到各个快递网点进行分拣。在流水线上进行分拣时，由NFC阅读器发出快递单编号查询讯号，快递专用NFC设备接收之后将快递单编号发送回NFC阅读器，NFC阅读器将快递单编号以及阶段代码(如，省级阶段，市级阶段，乡镇阶段)发送给后台服务器，后台服务器通过查询快递单编号以及阶段代码，提取出对应的阶段信息密钥并发送给NFC阅读器，NFC阅读器再把阶段信息密钥发给快递专用NFC设备，快递专用NFC设备使用阶段信息密钥对数据进行解密之后，把数据反馈发给NFC阅读器，之后再依据数据反馈结果对快递箱进行分拣，如图4所示。

[0119] 2.3派送过程

[0120] 快递进入派送阶段的时候，需要完成两个过程，一个是通知收件人阶段，一个是收件人签收阶段。

[0121] 在通知收件人阶段，派送员需要使用NFC阅读器对快递箱内的快递专用NFC设备发出快递单编号查询讯号，快递专用NFC设备将快递单编号发回给NFC阅读器，NFC阅读器将快递单编号以及其他信息(如何时何地去何处取件等信息，由派送员决定)发送给云端服务器，云端服务器通过快递单编号查询确认信息密钥，再发送通知信息以及确认信息密钥给收件人的app。

[0122] 在收件人签收阶段，收件人通过app使用自己的手机NFC功能把确认信息密钥发送给快递专用NFC设备，快递专用NFC设备使用确认信息密钥进行解密，提取出确认信息，并通过手机NFC发送给app，app把确认信息发送给云端服务器，完成认证过程。最后，云端服务器发送确认收件的通知给派送员，派送员回收快递专用NFC设备，签收完成，如图5所示。

[0123] 3、效能分析

[0124] 1)基于三维点阵的切面加密方法的可行性

[0125] 基于点阵的切面加密方式，由于任何信息都可以转化为二进制编码，用点的有无可以表示0与1，因此只要长度足够，任何信息都可以通过这种方式存储到这个三维点阵当中。由于是共线平面束，当平面的共线在立方体之外时，每个切面之间的点不会互相干扰，因此存入的信息不会产生冲突，信息完整性得到保证。

[0126] 2)基于三维点阵的切面加密方法的复杂度

[0127] 设立方体的边长为a，基于三维点阵的切面加密方法加密所需要的空间为0到a^3个点集数据。解密过程中，不需要增加任何的数据空间，使用内存空间为一次生成的常量空间。

[0128] 基于三维点阵的切面加密方法加密所需要的时间为一轮n次判断是否满足λn的条件，以及一轮n次每次最坏a次增删除点的操作。时间复杂度为$O(n)$。解密所需要的时间为一次最多a^3的点带入方程计算比较结果，时间复杂度为$O(1)$。

[0129] 3)基于三维点阵的切面加密方法的破译难度

[0130] 基于三维点阵的切面加密方法利用的是理论上三维立体图形的切面无限多这一点。但实际上可构成的切面与加密数据的点数量有关，随着加密数据的冗余点越多，可以构成的切面也就越多。暴力破解需要解出所有切面的数据。而每个切面的数据，只是完整数据的一个部分，要获得完整数据，还需要猜测对明文的分割数量n以及正确的排序方式进行组合，切割越细致，从诸多数据的组合中找到符合语义且为正确的明文数据就越困难。

[0131] 4)基于三维点阵的切面加密方法的优点

[0132] 当一个信息需要分成多个部分，每个部分针对特定类型人群的时候使用，但特定类型人群并不需要知道其他部分信息时可以使用基于三维点阵的切面加密方法。在快递业务中，比起一次性加密方案，采用这种使用方法，可以防止多余的信息被无关人员获取，可以使得密文与明文之间的位置对应关系更加模糊。比起不同部分使用不同加密方案，可以节省成本。由于时空复杂度都比较低，对于类似NFC这样能量和空间都比较有限的系统来说更加有利，更为合适。而且密钥的长度也十分低，长度仅为3个点的数据量，通过一个密钥无法推测出其他密钥，并且可以通过密钥反向推测出是哪个部分泄露了秘密。

[0133] 5)可个性化强

[0134] 在获得切面点的三维数据后，重组还原成二进制编码的方式可以根据企业自身进行再设计，从而加强该方法的安全性。本发明所提出的重组方法只使用了x轴坐标，事实上，可以配合使用y轴坐标与z轴坐标进行更复杂的组合，共同完成对明文相应位置是0还是1的输出控制。

[0135] 6)基于三维点阵的切面加密方法与其他方案的对比

[0136] 对数据进行简单分段后，对各个分段数据使用同一种加密方式的方案，如文献[17]，文献[18]中使用的加密方式，虽然可以沿用传统的RFID的加密方法，但是快递业务中，各个部分的信息并不大，长短不一，这样加密之后数据的分块明显，也需要管理较长的密钥，也容易遭受针对密文攻击。而三维点阵的切面加密方法密钥长度只需要三个三维点坐标即可表示，每个分段隐藏如真假难辨的混淆数据之中，获取真实密文的难度，防止针对密文攻击。

[0137] 文献[19]中提出的方案，分段后使用多套加密解密的系统，按照一定次序使用AES,DES,RC4等多种加密方法，比起始终使用同一种加密方式安全性要高，但是这就意味着要么阅读器必须有所有的解密系统，要么需要在相应的快递业务过程中使用对应的解密系统，这无疑增加了使用成本和使用难度。而基于三维点阵的切面加密方法则始终只需要一套加解密方案，可以灵活地根据需要进行不同阶段的密钥申请和解密。

[0138] 文献[20]，使用的便是利用魔方的思想进行加密，密钥为旋转方式，但通过密钥解密之后，所有的数据也都被解开，而文章作者并没有给出能够只恢复一个部分数据的方法，同时，该加密方法对数据的混淆操作每次需要调动的数据的操作十分复杂，因此并不能满足需求。而基于三维点阵的切面加密方法则始终只需要一套加解密方案，可以灵活地根据需要进行不同阶段的密钥申请和解密。而基于三维点阵的切面加密方法则只需要对点数据进行一次验证性的计算即可，无需反复移动计算，并且能针对特定分段数据进行解密的操作，从而满足快递业务中按需获得信息的特点。

[0139] 7)使用基于NFC的快递面单加密方法对快递业务的优势

[0140] 首先，通过app填单的方式，有效地节省了填单所花费的时候。对于个人用户，需要手动进行单据的填写，很多时候存在字迹不清晰，填写不规范等问题，对于快递单的分拣投递造成一定难度，通过app填单可以避免遇到这种情况造成的影响。对于商业用户，可以通过与淘宝的合作等方式进行改进，使得app能够进行自动填单，再通过人工核对，减少手动输入快递面单的耗时过程，以及疏忽大意引起的输入错误等问题。

[0141] 其次，有效保护了用户的隐私。因为不是使用纸质面单，而是通过NFC设备处理使用的是无线通信，所以不会存在肉眼可以识别获得用户个人信息的问题。而通过加密的方式保存数据，因此快递员工即使获得了数据，也无法分析破解获取到用户个人信息。

[0142] 最后，对于用户来说，不需要向快递员工出示身份信息，不需要将身份证提交给快递员工核定，可以避免重要的证件丢失，被拍摄记录等风险。对于收件人来说，由于需要使用手机NFC进行签收，可以很大程度上防止冒领，意外被人领走，如果需要替领，收件人也可以通过app对信得过的人进行授权，云端只需要把领取密钥发给授权人即可，领取人信息和情况也可以通过app进行确认，从而保证快递能到合法的人手中。

[0143] 参考文献：

[0144] [1]. 中华人名共和国国家邮政局.2016年中国快递发展指数报告出炉

[0145] 快递量全球占比超四成 对世界快递量增长贡献率达60%.Verticals[EB/OL].http://www.spb.gov.cn/xw/dtxx_15079/201703/t20170329_1096784.html

[0146] [2]曾益坤, 戴仁. 新型快递面单的设计与推广分析[J]. 物流技术与应用, 2014, 19(7):144-148.

[0147] [3]邓翔,周游丽,张仁望.新华网.网上公然叫卖圆通、申通快递单 个人隐私仅值4角钱.[EB/OL]http://business.sohu.com/20130729/n382805061.shtml

[0148] [4]Saidane Z,Garcia C,Dugelay J L.图像文本识别图(iTRG)[J]。2011:266-269。

[0149] [5]任民. 一张快递面单能“扒”出多少个人信息[J]. 政府法制, 2017(18):52-53.

[0150] [6]Frost & Sullivan. Promised Market for NFC Effectively Commences in 2011 with Commercial Roll out within All Verticals[EB/OL].http://www.frost.com/prod/servlet/press-release.pag.docid=223107191,2011-1-31.

[0151] [7]腾讯科技.In-Stat:2015年NFC芯片出货量将超12亿[EB/OL].http://tech.qq.com/a/20111025/000145.htm,2011-10-25.

[0152] [8]张玉婷,严承华. 一种基于双向认证协议的RFID标签认证技术研究[J]. 信息网络安全,2016(1):64-69.

[0153] [9]Madlmayr G, Kantner C, Grechenig T. Near Field Communication[J]. Pervasive Computing IEEE, 2014, 4(2):4-7.

[0154] [10]Derawi M O, Witte H, Mccallum S, et al. Biometric access control using Near Field Communication and smart phones[C]// Iapr International Conference on Biometrics. IEEE, 2012:490-497.

[0155] [11]杨婷. 基于Android和NFC技术的校园一卡通的关键技术研究[D].北京:北京邮电大学, 2015.

[0156] [12]Chen W D, Mayes K E, Lien Y H, et al. NFC mobile payment with Citizen Digital Certificate[C]// The, International Conference on Next Generation Information Technology. IEEE, 2011:120-126.

[0157] [13]翟龙真. 基于人因工程学的快递分拣作业优化研究[D]. 南华大学, 2016.

[0158] [14]王铁牛. 国内异地快递分拣优化的思路[J]. 物流技术与应用, 2014, 19(10):186-187.

[0159] [15]刘丁, 李新娥, 崔春生,等. 基于ZigBee的快递监管系统[J]. 电子技术应用, 2017, 43(5):11-14.

[0160] [16]林朝波. RFID技术在邮政速递分拣中的应用设计与实现[D]. 北京邮电大学, 2014.

[0161] [17]Luo Y, Chai Q, Gong G, et al. A Lightweight Stream Cipher WG-7 for RFID Encryption and Authentication[C]// Global Telecommunications Conference. IEEE, 2010:1-6.

[0162] [18]Feldhofer M, Dominikus S, Wolkerstorfer J. Strong Authentication for RFID Systems Using the AES Algorithm[J]. Lecture Notes in Computer

Science, 2004, 3156:357-370.

[0163] [19]刘靖, 向敏, 顾方勇. 一种文件分段加密方法及其应用[J]. 指挥信息系统与技术, 2010, 01(4):64-67.

[0164] [20]陈涛, 谢阳群. 基于扩展的N维魔方加密算法的设计与实现[J]. 情报杂志, 2005, 24(2):13-14.。

[0165] 以上是本发明的较佳实施例,凡依本发明技术方案所作的改变,所产生的功能作用未超出本发明技术方案的范围时,均属于本发明的保护范围。

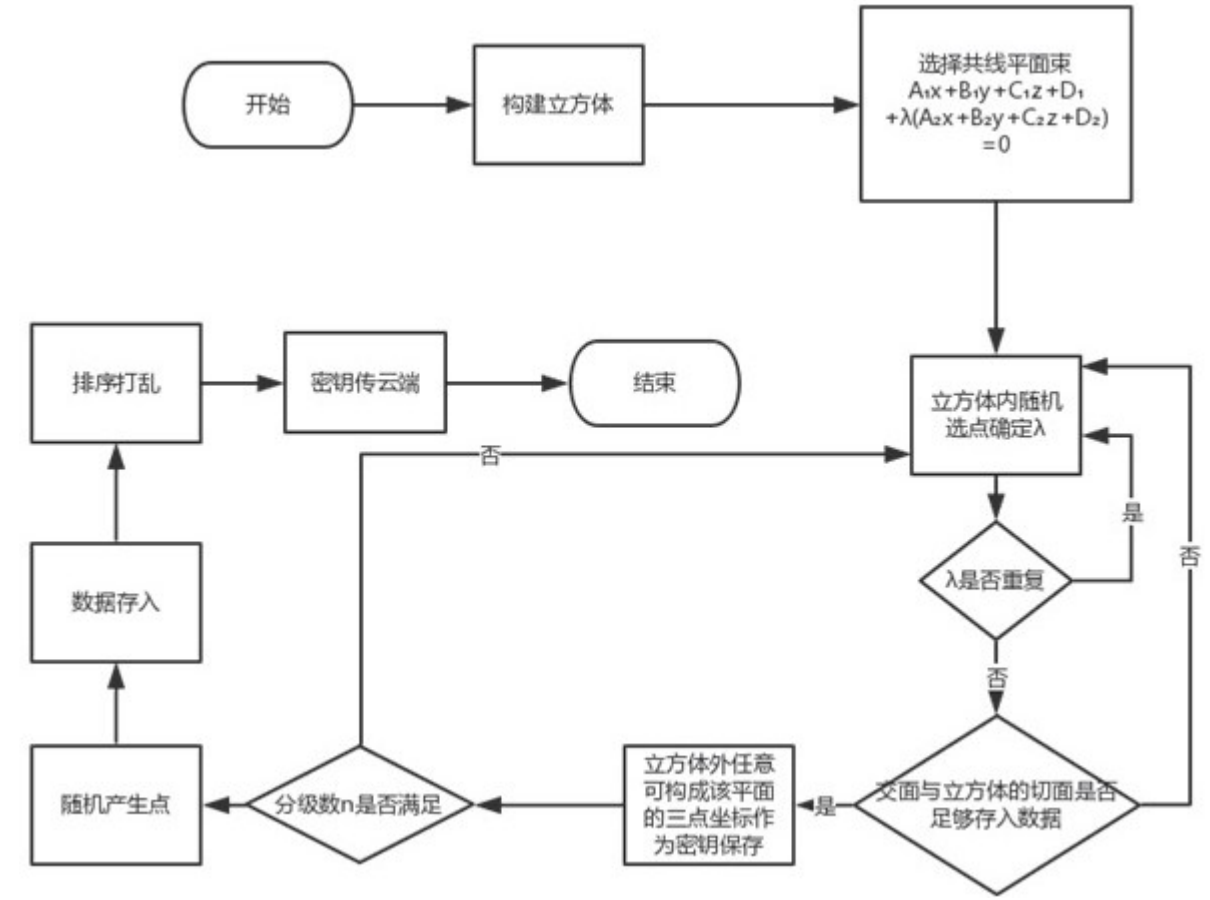

开始
构建立方体
选择共线平面束
$A_1x+B_1y+C_1z+D_1+\lambda(A_2x+B_2y+C_2z+D_2)=0$
排序打乱
密钥传云端
结束
立方体内随机选点确定λ
λ是否重复
是
否
否
数据存入
随机产生点
分级数n是否满足
否
立方体外任意可构成该平面的三点坐标作为密钥保存
是
交面与立方体的切面是否足够存入数据

图1

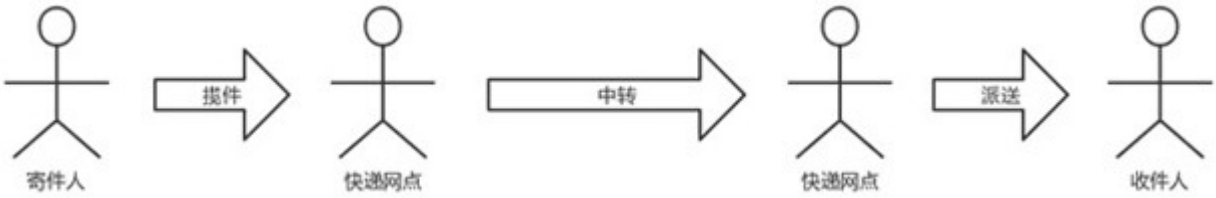

寄件人
揽件
快递网点
中转
快递网点
派送
收件人

图2

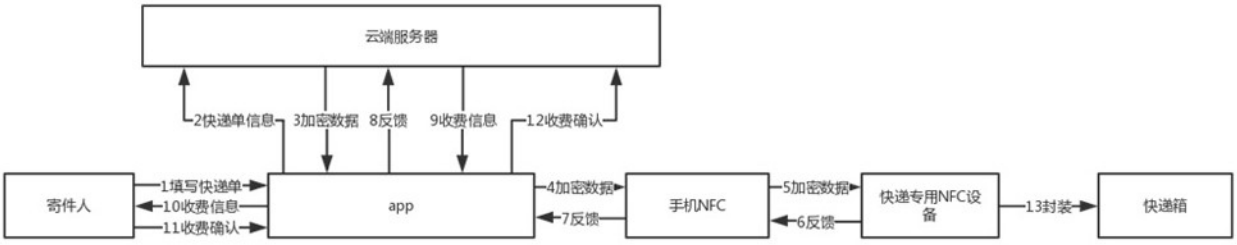

云端服务器
2快递单信息
3加密数据
8反馈
9收费信息
12收费确认
寄件人
1填写快递单
10收费信息
11收费确认
app
4加密数据
7反馈
手机NFC
5加密数据
6反馈
快递专用NFC设备
13封装
快递箱

图3

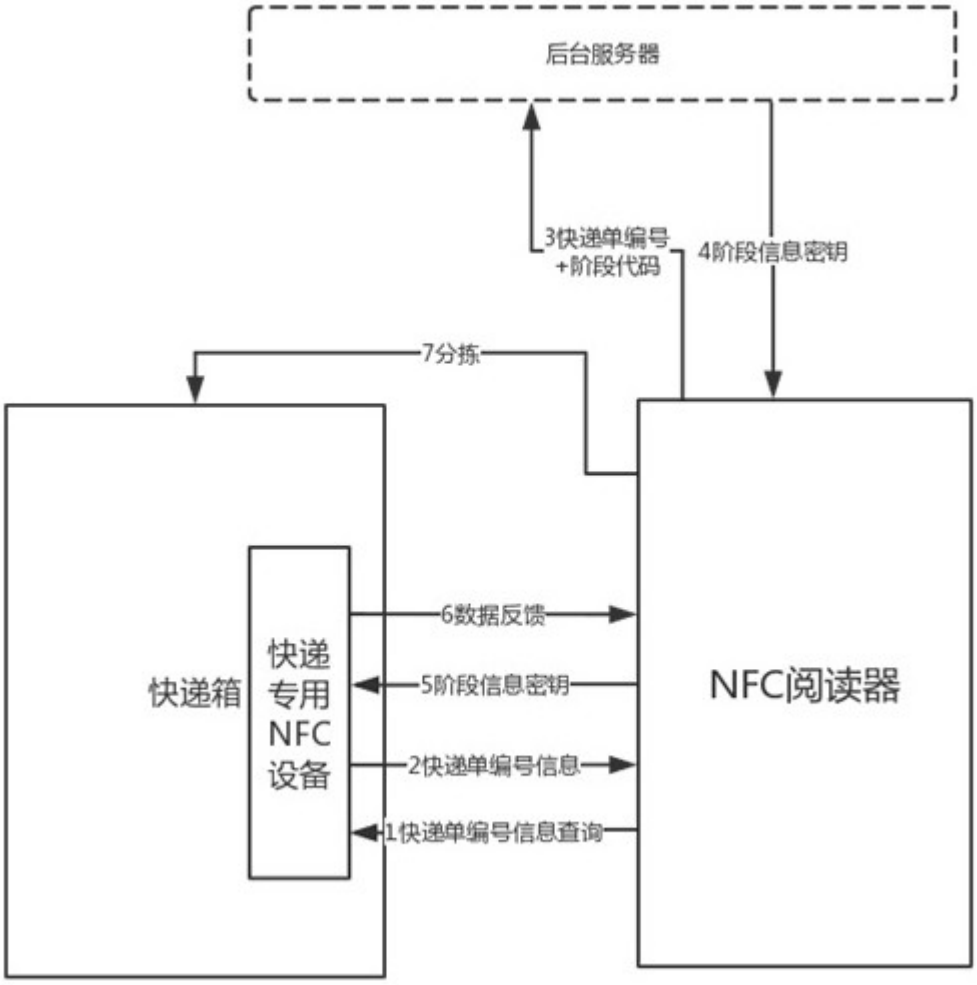

后台服务器
3快递单编号
+阶段代码
4阶段信息密钥
7分拣
快递箱
快递
专用
NFC
设备
6数据反馈
5阶段信息密钥
2快递单编号信息
1快递单编号信息查询
NFC阅读器

图4

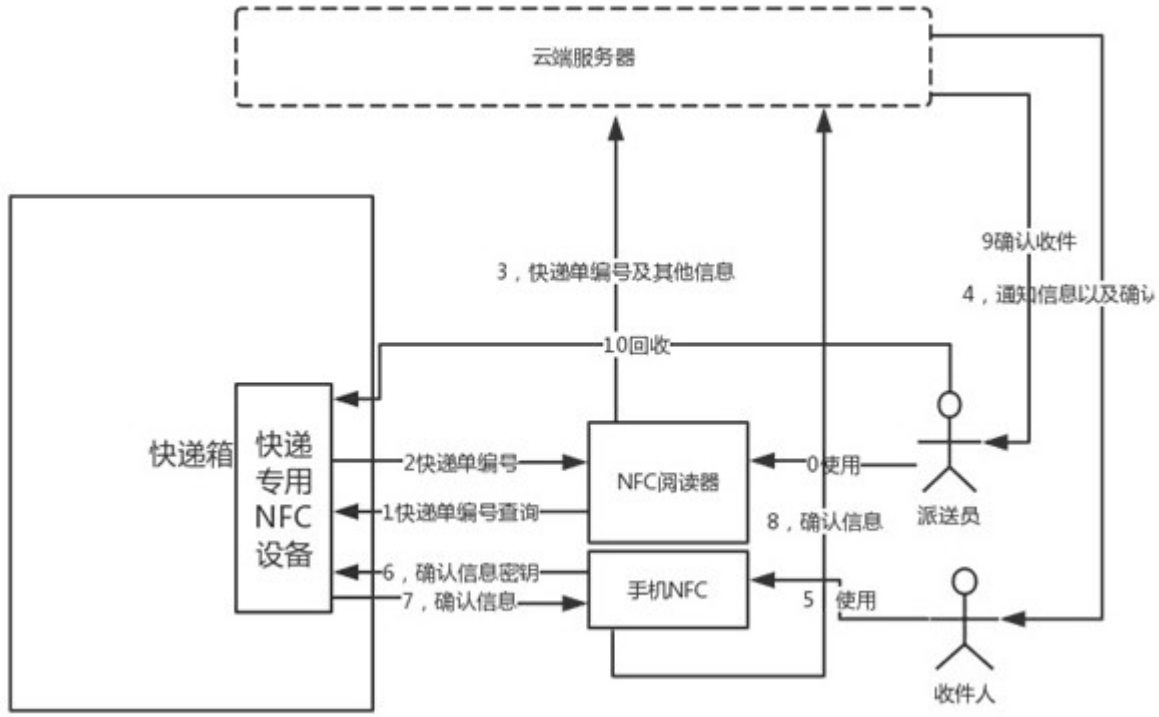

云端服务器
3，快递单编号及其他信息
9确认收件
4，通知信息以及确认
10回收
快递箱
快递专用NFC设备
2快递单编号
1快递单编号查询
6，确认信息密钥
7，确认信息
NFC阅读器
手机NFC
0使用
8，确认信息
派送员
5 使用
收件人

图5