

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2018 年 6 月 28 日 (28.06.2018)



(10) 国际公布号
WO 2018/113708 A1

- (51) 国际专利分类号:
H04L 12/58 (2006.01) **H04L 29/06** (2006.01)
- (21) 国际申请号: PCT/CN2017/117564
- (22) 国际申请日: 2017 年 12 月 20 日 (20.12.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201611190140.5 2016 年 12 月 21 日 (21.12.2016) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。
- (72) 发明人: 曾溪泉(ZENG, Xiquan); 中国北京市朝阳区酒仙桥路6号院2号楼, Beijing 100015 (CN)。
- (74) 代理人: 北京市隆安律师事务所 (BEIJING LONGAN LAW FIRM); 中国北京市朝阳区建

国门外大街 21 号北京国际俱乐部 188 室, Beijing 100020 (CN)。

- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

(54) Title: MAIL SENDING, READING, AND READ CONTROL METHOD, AND APPARATUS FOR SAME

(54) 发明名称: 一种邮件发送、查看、查看控制方法及其设备

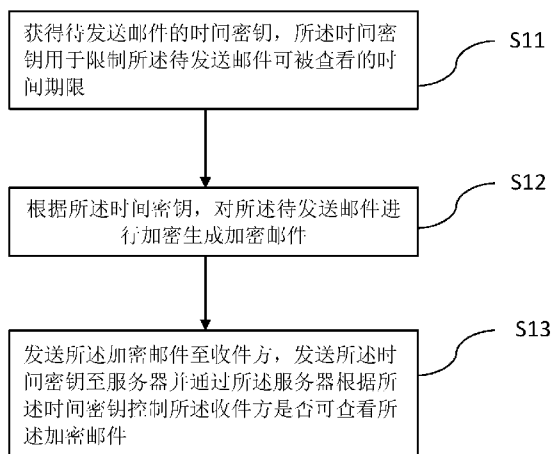


图 1

- S11 Acquire a time key of a mail to be sent; the time key is used to restrict a time period of the mail to be sent available for reading
- S12 Encrypt, according to the time key, the mail to be sent to generate an encrypted mail
- S13 Send to a receiving party the encrypted mail, send the time key to a server, and control, by means of the server and according to the time key, whether the receiving party can read the encrypted mail

(57) Abstract: Disclosed in the present invention are a mail sending, reading, and read control method, and apparatus for same. The method comprises: acquiring a time key of a mail to be sent, the time key being used to restrict a time period of the mail to be sent available for reading; encrypting, according to the time key, the mail to be sent to generate an encrypted mail; and sending to a receiving party the encrypted mail, sending the time key to a server, and controlling, by means of the server and according to the time key, whether the receiving party can read the encrypted mail. The present invention provides expiration protection of mails to improve mail security and enable mails to be time sensitive, thus broadening applications of encryption.

(57) 摘要: 本发明公开了一种邮件发送、查看、查看控制方法及其设备。该方法包括: 获得待发送邮件的时间密钥, 所述时间密钥用于限制所述待发送邮件可被查看的时间期限; 根据所述时间密钥, 对所述待发送邮件进行加密生成加密邮件; 发送所述加密邮件至收件方, 发送所述时间密钥至服务器并通过所述服务器根据所述时间密钥控制所述收件方是否可查看所述加密邮件。本发明为邮件提供了过期失效的保障, 使邮件的安全性、时效性更高, 加密范围更广。

本国际公布：

- 包括国际检索报告(条约第21条(3))。

一种邮件发送、查看、查看控制方法及其设备

技术领域

5 本发明涉及通信技术领域，尤其涉及一种邮件发送、查看、查看控制方法及其设备。

背景技术

随着科技的发展，电子邮件的应用范围越来越广,电子邮件(ElectronicMail,Email)是人们日常工作常用的办公通信工具，技术人员在工作过程中会频繁利用办公电脑、个人电脑、手机等电子产品收发电子邮件，因此，电子邮件的信息安全就变得尤其重要，然而在目前邮件的使用过程中，通常是设置复杂的邮箱帐户密码以求邮件的安全。

事实上，这种通过邮箱账户密码来收发邮件的方式只实现了邮件通讯加密，并不能实现电子邮件内容的全程加密，目前，市场上也有使用对电子邮件内容进行加密的方法，采取的加密方法是用证书和公钥来加密，知晓公钥对应的私钥才能解密该邮件内容并浏览，无论是通过邮箱账户密码来对邮件通讯进行加密还是通过证书和公钥来对邮件内容进行加密，不足之处在于：加密邮件不具有时效性，易于破解。

发明内容

20 鉴于上述问题，本发明提出了一种克服上述问题或者至少部分地解决上述问题的邮件发送、查看、查看控制方法及其设备，具体技术方案是：

本申请实施例提供一种邮件发送方法，所述方法包括：

获得待发送邮件的时间密钥，所述时间密钥用于限制所述待发送邮件可被查看的时间期限；

25 根据所述时间密钥，对所述待发送邮件进行加密生成加密邮件；

发送所述加密邮件至收件方，发送所述时间密钥至服务器并通过所述服务器根据所述时间密钥控制所述收件方是否可查看所述加密邮件。

本发明还提供一种邮件查看方法，应用于邮件接收端，所述方法包括：

30 接收根据时间密钥进行加密的加密邮件，所述时间密钥用于限制所述加密邮件可被查看的时间期限；

响应查看所述加密邮件的查看操作，生成并发送密钥请求至服务器，所述密钥

请求用于获取所述加密邮件的所述时间密钥;

接收所述服务器响应所述密钥请求的反馈信息, 所述反馈信息由所述服务器根据所述密钥请求的请求时间和发送端发送的所述时间密钥生成, 当所述请求时间超出所述时间密钥对应的时间范围时所述反馈信息为表征所述加密邮件无效的信息,

5 当所述请求时间在所述时间密钥对应的时间范围内时所述反馈信息为所述时间密钥;

解析所述反馈信息, 根据解析结果响应所述查看操作。

本发明还提供一种邮件查看控制方法, 应用于服务器, 所述方法包括:

接收邮件接收端发送的获取加密邮件时间密钥的密钥请求;

10 将所述邮件接收端请求所述时间密钥的请求时间与所述时间密钥对应的时间范围进行比较;

如果所述请求时间超出所述时间范围, 拒绝向邮件接收端发放所述时间密钥, 使得邮件接收端无法对加密邮件进行解密及查看;

15 如果所述请求时间未超出所述时间范围, 向邮件接收端发放所述时间密钥, 使得邮件接收端根据所述时间密钥对加密邮件进行解密并查看。

本发明还提供一种邮件发送端, 包括:

获取单元: 用于获得待发送邮件的时间密钥, 所述时间密钥用于限制待发送邮件可被查看的时间期限;

加密单元: 用于根据所述时间密钥, 对所述待发送邮件进行加密生成加密邮件;

20 第一发送单元: 用于发送所述加密邮件至收件方, 发送所述时间密钥至服务器并通过所述服务器根据所述时间密钥控制所述收件方是否可查看所述加密邮件。

本发明还提供一种邮件接收端, 包括:

第一接收单元: 用于接收根据时间密钥进行加密的加密邮件, 所述时间密钥用于限制所述加密邮件可被查看的时间期限;

25 响应请求单元: 用于响应查看所述加密邮件的查看操作, 生成并发送密钥请求至服务器, 所述密钥请求用于获取所述加密邮件的所述时间密钥;

第二接收单元: 用于接收所述服务器响应所述密钥请求的反馈信息, 所述反馈信息由所述服务器根据所述密钥请求的请求时间和发送端发送的所述时间密钥生成, 当所述请求时间超出所述时间密钥对应的时间范围时所述反馈信息为表征所述加密邮件无效的信息, 当所述请求时间在所述时间密钥对应的时间范围内时所述反
30 馈信息为所述时间密钥;

解析响应单元：用于解析所述反馈信息，根据解析结果响应所述查看操作。

本发明还提供一种邮件服务器，包括：

第三接收单元：用于接收邮件接收端发送的获取加密邮件时间密钥的密钥请求；

5 验证单元：用于将所述邮件接收端请求所述时间密钥的请求时间与所述时间密钥对应的时间范围进行比较；

第二发送单元：用于如果所述请求时间超出所述时间范围，拒绝向邮件接收端发放所述时间密钥，使得邮件接收端无法对加密邮件进行解密及查看；

如果所述请求时间未超出所述时间范围，向邮件接收端发放所述时间密钥，使得邮件接收端根据所述时间密钥对加密邮件进行解密并查看。

10 本发明还提供一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据如上述的邮件发送方法，或者执行如上述的邮件查看方法，或者执行如上述的邮件查看控制方法。

本发明还提供一种计算机可读介质，其中存储了如上所述的计算机程序。

本申请实施例中提供的技术方案，至少具有如下技术效果或优点：

15 与传统的加密方法相比，本发明的加密方法在于利用时间密钥对待发送邮件进行加密，该时间密钥用于限制待发送邮件可被查看的时间期限，即过了该时间期限，邮件将不能再被查看，保证了邮件的时效性；同时，用于加密邮件的时间密钥是发送至服务器，由服务器来管理密钥的发放，以此来控制加密邮件能否被查看，确保了邮件传输以及使用过程中信息的高度安全性和邮件的时效性，解决了现有技术中
20 加密邮件不具有时效性、易于破解的技术问题。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

25 附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

30 图 1 示出了根据本发明一个实施例的一种邮件发送方法流程图；

图 2 示出了根据本发明一个实施例的一种邮件查看方法流程图；

图 3 示出了根据本发明一个实施例的一种邮件查看控制方法流程图；

图 4 示出了根据本发明一个实施例的一种邮件发送端的示意图；

图 5 示出了根据本发明一个实施例的一种邮件接收端的示意图；

图 6 示出了根据本发明一个实施例的一种邮件服务器的示意图；

5 图 5 示意性地示出了用于执行根据本发明的方法的计算设备的框图；以及

图 6 示意性地示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元。

具体实施例

10 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

15 本发明实施例提供一种邮件发送、查看、查看控制方法及其设备，用以解决现有技术中加密邮件不具有时效性、易于破解的技术问题。

请参考图 1，本申请实施例提供的一种邮件发送的方法，该方法包括以下步骤：

S11：获得待发送邮件的时间密钥，所述时间密钥用于限制所述待发送邮件可被查看的时间期限；

S12：根据所述时间密钥，对所述待发送邮件进行加密生成加密邮件；

20 S13：发送所述加密邮件至收件方，发送所述时间密钥至服务器并通过所述服务器根据所述时间密钥控制所述收件方是否可查看所述加密邮件。

需要说明的是，在具体实施过程中，本申请提供的上述邮件发送方法可应用于使用 IMAP(Internet Mail Access Protocol，交互式邮件存取协议) /POP3(Post Office Protocol 3，邮局协议的第 3 个版本)/SMTP(Simple Mail Transfer Protocol，简单邮件传输协议) /ESMTP(Extended SMTP，扩展 SMTP)等协议收发电子邮件的邮件客户端，且该邮件客户端可以搭建各种邮件服务器来使用，只需按照相关邮件服务器地址完成配置即可，举例来说明，如某邮件客户端要使用 SINA 邮件服务器，可配置接收邮件服务器地址(POP3)为：pop.sina.com.cn 或：pop3.sina.com.cn，发送邮件服务器地址(SMTP)为：smtp.sina.com.cn，即可使用，该方法应用广泛，操作方便。

30 下面，结合图 1 详细介绍本邮件发送方法的具体实现步骤：

步骤 S11，获得待发送邮件的时间密钥，所述时间密钥用于限制所述待发送邮件

可被查看的时间期限。

具体包括：

S111：获得待发送邮件的失效时间，所述失效时间为所述邮件发送后过期失效的时间；

5 S112：根据所述失效时间得到时间密钥；

其中步骤 S111，获得待发送邮件的失效时间，所述失效时间的生成可以采用以下方式：

第一种方式：失效时间由发件人设定。

具体方法为：邮件发送端为发件人在编辑新邮件发送前，设定有输入失效时间指令的入口，比如，发件人可以通过这个入口手动录入或者手动选择失效时间，比如手动录入或选择的时间为“2016-8-1 11:30”，即邮件的失效时间为“2016-8-1 11:30”。
10

第二种方式：失效时间由发送端系统自动生成。

具体方法为，所述失效时间是由邮件发送端的发送邮件的时间加上一个固定的期限自动生成，比如说，发送邮件的时间为“2016-8-1 11:30”，固定的期限为 30 天，那么所述失效时间为“2016-8-31 11:30”。所述固定期限的设定为邮件系统开发时的功能集成。关于失效时间的生成方式，本发明不做限制。
15

步骤 S112：根据所述失效时间得到时间密钥。

具体的时间密钥可以为利用标识密码算法计算得到的时间公钥 ID，至少有以下两种方法：

20 第一种方法：可以使用对称加密的方法对原始邮件数据加密，对称加密算法的原理是：数据发信方将明文(原始数据)和加密密钥一起经过加密算法处理后，使其变成复杂的加密密文发送出去。收信方收到密文后，若想解读原始数据，则需要使用加密用过的密钥及相同加密算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密，对称加密算法的优点在于加解密的高速度和使用长密钥时的难破解性。
25

第二种方法：时间密钥还可以用非对称加密算法得到，非对称加密算法需要两个密钥：公开密钥(publickey)和私有密钥(privatekey)。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。非对称密码体制的特点在于：
30 加密解密速度较对称加密慢，但加密算法强度复杂、安全性高。

步骤 S12, 根据所述时间密钥, 对所述待发送邮件进行加密生成加密邮件;

步骤 S12 具体的可以采用方法一实现: 用所述时间密钥对所述待发送邮件进行加密生成所述加密邮件;

具体在本实施例中, 此处可以采用对称加密的方法对原始邮件数据加密, 具体

5 加密内容如下:

$\text{EncrpytBySym}(\text{邮件数据密文}) = \text{fx_encryptBySym}(\text{ori}(\text{邮件内容}), \text{ID}(\text{时间密钥}))$, ori 为 EML 的所有内容 (包含邮件头、邮件体), 采用的是二进制数据格式, EncrpytBySym 即为加密获得的邮件数据密文, 加密使用的加密强度为 AES256。

步骤 S12 也可以采用方法二实现: 生成会话密钥, 用所述时间密钥和所述会话
10 密钥的组合对所述待发送邮件进行加密生成所述加密邮件;

具体在本实施例中, 举例说明, 生成会话密钥的算法为根据随机数生成一段会话密钥, 如 $\text{SessionPassword} = \text{fx_randomSession}("1234567890")$, SessionPassword= 会话密钥, 1234567890 即为一个随机数, 通过生成会话密钥的算法即生成一段会话密钥。然后, 用所述会话密钥对待发送邮件进行加密, 生成所述加密邮件中的邮件
15 数据密文, 具体方法是:

$\text{EncrpytBySym}(\text{邮件数据密文}) = \text{fx_encryptBySym}(\text{ori}(\text{邮件内容}), \text{SessionPassword}, \text{ID})$, EncrpytBySym 即为用所述时间密钥和所述会话密钥的组合对所述待发送邮件进行加密生成的邮件数据密文。

接下来, 用所述时间密钥对所述会话密钥进行加密, 生成所述加密邮件中的会
20 话密钥密文; 具体方法可以是:

会话密钥密文 $\text{id1_encryptdata} = \text{fx_encryptByIBC}(\text{SessionPassword}(\text{会话密钥}), \text{ID}(\text{时间密钥}))$, 此加密算法采用 sm9 加密算法, 加密强度是 RSA3072。

进一步的, 其中的加密邮件具体可以是在发送前将由所述邮件数据密文和会话
密钥密文进行封装后生成的封装包; 对邮件数据密文和会话密钥密文进行 P7 格式封
25 装, 结合本实施例, 具体封装为 XXX 邮件系统格式如下:

```
P7Data=SEQUENCE{
  加密类型=XXXsmail
  加密算法=id-ibc-enc-kem-sok-esbdh
  摘要类型=aes256
  30 编码类型=dem-dem3, hmacSHA
  可解密时间信息={
```

可解密时间标识=yyyymmddhhnnsszzz

域=360jiamiyou_olym

版本=1

会话密钥密文(id1_encryptdata)

}

数据密文(EncryptBySym)

}

上述工作完成后,就可以进行步骤 S13: 发送所述加密邮件至收件方,发送所述时间密钥至服务器并通过所述服务器根据所述时间密钥控制所述收件方是否可查看所述加密邮件。关于服务器如何根据所述时间密钥控制所述收件方是否可查看所述加密邮件的方法将在后面内容作详细描述。

请参考图 2: 本申请实施例提供的一种邮件查看方法,应用于邮件接收端,所述方法包括:

S21: 接收根据时间密钥进行加密的加密邮件,所述时间密钥用于限制所述加密邮件可被查看的时间期限;

S22: 响应查看所述加密邮件的查看操作,生成并发送密钥请求至服务器,所述密钥请求用于获取所述加密邮件的所述时间密钥;

S23: 接收所述服务器响应所述密钥请求的反馈信息,所述反馈信息由所述服务器根据所述密钥请求的请求时间和发送端发送的所述时间密钥生成,当所述请求时间超出所述时间密钥对应的时间范围时所述反馈信息为表征所述加密邮件无效的信息,当所述请求时间在所述时间密钥对应的时间范围内时所述反馈信息为所述时间密钥;

S24: 解析所述反馈信息,根据解析结果响应所述查看操作;

所述根据解析结果响应所述查看操作,包括:

当解析结果为所述加密邮件无效时,执行步骤 S241: 响应所述查看操作,提示用户所述加密邮件已过期无法被查看;

当解析结果为所述时间密钥时,执行步骤 S242: 响应所述查看操作,根据所述时间密钥解密所述加密邮件,获得邮件数据并显示;

在执行步骤 S242 中,所述根据所述时间密钥解密所述加密邮件,可以采用两种办法:

方法一: 用所述时间密钥解密所述加密邮件,得到邮件数据;

或者方法二：解析所述加密邮件的封装包得到所述加密邮件中的会话密钥密文；用所述时间密钥解密所述会话密钥密文，得到会话密钥；用所述会话密钥解密所述加密邮件中的邮件数据密文，得到邮件数据。

下面，结合图 2 详细介绍本申请实施例中邮件查看方法的具体实现步骤：

5 S21：接收根据时间密钥进行加密的加密邮件，所述时间密钥用于限制所述加密邮件可被查看的时间期限；

时间密钥可以为利用标识密码算法计算得到的时间公钥 ID，至少有以下两种方法：

10 第一种方法：可以使用对称加密的方法对原始邮件数据加密，对称加密算法的原理是：数据发信方将明文(原始数据)和加密密钥一起经过加密算法处理后，使其变成复杂的加密密文发送出去。收信方收到密文后，若想解读原始数据，则需要使用加密用过的密钥及相同加密算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密，对称加密算法的优点在于加解密的高速度和使用长密钥时的难破
15 解性。

第二种方法：时间密钥还可以用非对称加密算法得到，非对称加密算法需要两个密钥：公开密钥(publickey)和私有密钥(privatekey)。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。非对称密码体制的特点在于：
20 加密解密速度较对称加密慢，但加密算法强度复杂、安全性高。

S22：响应查看所述加密邮件的查看操作，生成并发送密钥请求至服务器，所述密钥请求用于获取所述加密邮件的所述时间密钥；

所述邮件接收端向服务器发送密钥请求获得时间密钥，所述时间密钥是服务器通过验证所述邮件接收端申请时间密钥的时间是否在时间密钥对应的时间范围内来
25 发放的，此处服务器一般为 CA 服务器；所谓 CA，即为数字证书认证中心（CertificateAuthority,CA），是整个网上电子交易安全的关键环节。它主要负责产生、分配并管理所有参与网上交易的实体所需的身份认证数字证书。

S23：接收所述服务器响应所述密钥请求的反馈信息，所述反馈信息由所述服务器根据所述密钥请求的请求时间和发送端发送的所述时间密钥生成，当所述请求时间超出所述时间密钥对应的时间范围时所述反馈信息为表征所述加密邮件无效的信息，当所述请求时间在所述时间密钥对应的时间范围内时所述反馈信息为所述时间
30

密钥。

具体在本实施例中，举例说明：

5 邮件接收端向服务器发送密钥请求的请求时间是 2016-8-20 10:10:10，而邮件发送端发送的时间密钥对应的时间是 2016-8-10 10:10:10，则请求时间超出所述时间密钥对应的时间范围，服务器给邮件接收端的反馈信息即为加密邮件无效，邮件发送端发送的时间密钥对应的时间是 2016-8-30 10:10:10，则请求时间在所述时间密钥对应的时间范围内，此时服务器给邮件接收端的反馈信息为时间密钥。

S24: 解析所述反馈信息，根据解析结果响应所述查看操作；

所述根据解析结果响应所述查看操作，包括：

10 当解析结果为所述加密邮件无效时，执行步骤 S241：邮件接收端响应所述查看操作，提示用户所述加密邮件已过期无法被查看；

当解析结果为所述时间密钥时，执行步骤 S242：邮件接收端响应所述查看操作，根据所述时间密钥解密所述加密邮件，获得邮件数据并显示；

15 在执行步骤 S242 中，所述根据所述时间密钥解密所述加密邮件，可以采用两种办法：

方法一：用所述时间密钥解密所述加密邮件，得到邮件数据；

或者方法二：解析所述加密邮件的封装包得到所述加密邮件中的会话密钥密文；用所述时间密钥解密所述会话密钥密文，得到会话密钥；用所述会话密钥解密所述加密邮件中的邮件数据密文，得到邮件数据；

20 具体的，邮件接收端在得到时间密钥后，会用所述时间密钥解析所述会话密钥密文，得到所述会话密钥。在本实施例中，通过解析会话密钥密文(id1_encryptdata)，得到会话密钥 SessionPassword 为“1234567890”，然后通过会话密钥 SessionPassword 来解析邮件数据密文，如在加密时，EncrpytBySym（邮件数据密文）=fx_encryptBySym(ori（邮件内容）,SessionPassword（会话密钥）)，解密后，最后得
25 到邮件数据 ORI。

此处的封装包如前述邮件发送方法中所述的生成的 P7 格式封装数据，具体封装数据如下：

P7Data=SEQUENCE{

加密类型=360smail

30 加密算法=id-ibc-enc-kem-sok-esbdh

摘要类型=aes256

编码类型=dem-dem3, hmacSHA

可解密时间信息={

可解密时间标识=yyyymmddhhnnsszzz

域=360jiamiyou_olym

5 版本=1

会话密钥密文(id1_encryptdata)

}

数据密文(EncryptBySym)

}。

10 通过对 P7 格式封装包解析,可从中得到会话密钥密文 id1_encryptdata 和失效时间 yyyymmddhhnnsszzz。

请参考图 3:一种邮件查看控制方法,应用于服务器,方法包括:

S31:接收邮件接收端发送的获取加密邮件时间密钥的密钥请求;

15 S32:将所述邮件接收端请求所述时间密钥的请求时间与所述时间密钥对应的时间范围进行比较;

如果所述请求时间超出所述时间范围,执行 S321:拒绝向邮件接收端发放所述时间密钥,使得邮件接收端无法对加密邮件进行解密及查看;

如果所述请求时间未超出所述时间范围,执行 S322:向邮件接收端发放所述时间密钥,使得邮件接收端根据所述时间密钥对加密邮件进行解密并查看。

20 步骤 S32 的具体原理和操作方法与步骤 S23 相对应。

步骤 S321 和步骤 S322 的具体原理和操作方法分别与 S241 和 S242 相对应。

作为对应于上述加密方法的邮件系统,采用前述的方法进行邮件的加密发送、解密接收和查看控制,该邮件系统包括前述的邮件发送端、邮件接收端和服务器。

其中,邮件发送端,如图 4 所示,包括:

25 获取单元 21:用于获得待发送邮件的时间密钥,所述时间密钥用于限制待发送邮件可被查看的时间期限;

加密单元 22:用于根据所述时间密钥,对所述待发送邮件进行加密生成加密邮件;

30 第一发送单元 23:用于发送所述加密邮件至收件方,发送所述时间密钥至服务器并通过所述服务器根据所述时间密钥控制所述收件方是否可查看所述加密邮件。

获取单元 21,包括:

时间获取子单元，一种可选实施例，时间获取子单元用于获得待发送邮件的失效时间，所述失效时间为所述邮件发送后过期失效的时间；

另一种可选实施例，所述时间获取子单元，用于获得将所述待发送邮件的发送时间加上固定期限生成所述失效时间。

5 密钥获取子单元，用于根据所述失效时间得到时间密钥。加密单元 22，包括：

第一加密子单元，用于用所述时间密钥对所述待发送邮件进行加密生成所述加密邮件；或者

第二加密子单元；

10 一种可选实施例，第二加密子单元用于生成会话密钥，用所述时间密钥和所述会话密钥的组合对所述待发送邮件进行加密生成所述加密邮件。

另一种可选实施例，第二加密子单元，用于：

用所述会话密钥对待发送邮件进行加密，生成所述加密邮件中的邮件数据密文；

用所述时间密钥对所述会话密钥进行加密，生成所述加密邮件中的会话密钥密文。

15 邮件接收端，如图 5 所示，包括：

第一接收单元 31：用于接收根据时间密钥进行加密的加密邮件，所述时间密钥用于限制所述加密邮件可被查看的时间期限；

响应请求单元 32：用于响应查看所述加密邮件的查看操作，生成并发送密钥请求至服务器，所述密钥请求用于获取所述加密邮件的所述时间密钥；

20 第二接收单元 33：用于接收所述服务器响应所述密钥请求的反馈信息，所述反馈信息由所述服务器根据所述密钥请求的请求时间和发送端发送的所述时间密钥生成，当所述请求时间超出所述时间密钥对应的时间范围时所述反馈信息为表征所述加密邮件无效的信息，当所述请求时间在所述时间密钥对应的时间范围内时所述反馈信息为所述时间密钥；

25 解析响应单元 34：用于解析所述反馈信息，根据解析结果响应所述查看操作。

具体的，解析响应单元 34，用于：

当解析结果为所述加密邮件无效时，响应所述查看操作，提示用户所述加密邮件已过期无法被查看；

30 当解析结果为所述时间密钥时，响应所述查看操作，根据所述时间密钥解密所述加密邮件，获得邮件数据并显示；

所述解析响应单元 34，包括：

第一解析响应子单元，用于用所述时间密钥解密所述加密邮件，得到邮件数据；
或者

第二解析响应子单元，用于解析所述加密邮件的封装包得到所述加密邮件中的
会话密钥密文；用所述时间密钥解密所述会话密钥密文，得到会话密钥；用所述会
5 话密钥解密所述加密邮件中的邮件数据密文，得到邮件数据。

邮件服务器，如图 6 所示，包括：

第三接收单元 41：用于接收邮件接收端发送的获取加密邮件时间密钥的密钥请
求；

验证单元 42：用于将所述邮件接收端请求所述时间密钥的请求时间与所述时间
10 密钥对应的时间范围进行比较；

第二发送单元 43：用于在所述请求时间超出所述时间范围时，拒绝向邮件接收
端发放所述时间密钥，使得邮件接收端无法对加密邮件进行解密及查看；在所述请
求时间未超出所述时间范围，向邮件接收端发放所述时间密钥时，使得邮件接收端
根据所述时间密钥对加密邮件进行解密并查看。

15 与传统的加密方法相比，本发明的加密方法在于利用时间密钥对待发送邮件进
行加密，该时间密钥用于限制待发送邮件可被查看的时间期限，即过了该时间期限，
邮件将不能再被查看，保证了邮件的时效性；同时，用于加密邮件的时间密钥是发
送至服务器，由服务器来管理密钥的发放，以此来控制加密邮件能否被查看，确保
了邮件传输以及使用过程中信息的高度安全性和邮件的时效性，解决了现有技术中
20 加密邮件不具有时效性、易于破解的技术问题。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。
各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统
所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，
可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的
25 描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的
实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知
的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，
30 在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单
个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下

意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

5 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非
10 另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中
15 所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行
20 的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的邮件发送端、邮件接收端和邮件服务器中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站服务器上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

25 例如，图 7 示出了用于执行根据本发明的方法的计算设备的框图。该计算设备传统上包括处理器 710 和以存储器 720 形式的计算机程序产品或者计算机可读介质。存储器 720 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 720 具有存储用于执行上述方法中的任何方法步骤的程序代码 731 的存储空间 730。例如，用于程序代码的存储空间 730 可以
30 包括分别用于实现上面的方法中的各种步骤的各个程序代码 731。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品

中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为例如图 8 所述的便携式或者固定存储单元。该存储单元可以具有与图 7 的计算设备中的存储器 720 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元存储有用于执行根据本发明的方法步骤的计算机可读程序代码 731’，即可以由诸如 710 之类的处理器读取的程序代码，当这些程序代码由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1、一种邮件发送方法，包括：

获得待发送邮件的时间密钥，所述时间密钥用于限制所述待发送邮件可被查看的时间期限；

5 根据所述时间密钥，对所述待发送邮件进行加密生成加密邮件；

发送所述加密邮件至收件方，发送所述时间密钥至服务器并通过所述服务器根据所述时间密钥控制所述收件方是否可查看所述加密邮件。

2、如权利要求 1 所述的方法，其特征在于，所述获得待发送邮件的时间密钥，包括：

10 获得待发送邮件的失效时间，所述失效时间为所述邮件发送后过期失效的时间；

根据所述失效时间得到时间密钥。

3、如权利要求 1 所述的方法，其特征在于，所述根据所述时间密钥，对所述待发送邮件进行加密生成加密邮件，具体方法包括：

15 用所述时间密钥对所述待发送邮件进行加密生成所述加密邮件；或者

生成会话密钥，用所述时间密钥和所述会话密钥的组合对所述待发送邮件进行加密生成所述加密邮件。

4、如权利要求 3 所述的方法，其特征在于，所述用所述时间密钥和所述会话密钥的组合对所述待发送邮件进行加密，包括：

20 用所述会话密钥对待发送邮件进行加密，生成所述加密邮件中的邮件数据密文；

用所述时间密钥对所述会话密钥进行加密，生成所述加密邮件中的会话密钥密文。

25 5、如权利要求 4 所述的方法，其特征在于，所述加密邮件具体是：在发送前将由所述邮件数据密文和会话密钥密文进行封装后生成的封装包。

6、如权利要求 1~5 任一所述的方法，其特征在于，所述时间密钥为利用标识密码算法计算得到的时间公钥。

7、如权利要求 2 所述的方法，其特征在于，所述获得待发送邮件的失效时间，包括：

30 将所述待发送邮件的发送时间加上固定期限生成所述失效时间。

8、一种邮件查看方法，应用于邮件接收端，包括：

接收根据时间密钥进行加密的加密邮件，所述时间密钥用于限制所述加密邮件可被查看的时间期限；

响应查看所述加密邮件的查看操作，生成并发送密钥请求至服务器，所述密钥请求用于获取所述加密邮件的所述时间密钥；

接收所述服务器响应所述密钥请求的反馈信息，所述反馈信息由所述服务器根据所述密钥请求的请求时间和发送端发送的所述时间密钥生成，当所述请求时间超出所述时间密钥对应的时间范围时所述反馈信息为表征所述加密邮件无效的信息，当所述请求时间在所述时间密钥对应的时间范围内时所述反馈信息为所述时间密钥；

解析所述反馈信息，根据解析结果响应所述查看操作。

9、如权利要求 8 所述的方法，其特征在于，所述加密邮件为：

用所述时间密钥加密生成的邮件；或者

用所述时间密钥和所述会话密钥的组合进行加密生成的邮件。

10、如权利要求 8 或权利要求 9 所述的方法，其特征在于，所述根据解析结果响应所述查看操作，包括：

当解析结果为所述加密邮件无效时，响应所述查看操作，提示用户所述加密邮件已过期无法被查看；

当解析结果为所述时间密钥时，响应所述查看操作，根据所述时间密钥解密所述加密邮件，获得邮件数据并显示。

11、如权利要求 10 所述的方法，其特征在于，所述根据所述时间密钥解密所述加密邮件，包括：

用所述时间密钥解密所述加密邮件，得到邮件数据；或者

解析所述加密邮件的封装包得到所述加密邮件中的会话密钥密文；用所述时间密钥解密所述会话密钥密文，得到会话密钥；用所述会话密钥解密所述加密邮件中的邮件数据密文，得到邮件数据。

12、一种邮件查看控制方法，应用于服务器，包括：

接收邮件接收端发送的获取加密邮件时间密钥的密钥请求；

将所述邮件接收端请求所述时间密钥的请求时间与所述时间密钥对应的时间范围进行比较；

如果所述请求时间超出所述时间范围，拒绝向邮件接收端发放所述时间密钥，使得邮件接收端无法对加密邮件进行解密及查看；

如果所述请求时间未超出所述时间范围，向邮件接收端发放所述时间密钥，使得邮件接收端根据所述时间密钥对加密邮件进行解密并查看。

5 13、一种邮件发送端，包括：

获取单元：用于获得待发送邮件的时间密钥，所述时间密钥用于限制待发送邮件可被查看的时间期限；

加密单元：用于根据所述时间密钥，对所述待发送邮件进行加密生成加密邮件；

10 第一发送单元：用于发送所述加密邮件至收件方，发送所述时间密钥至服务器并通过所述服务器根据所述时间密钥控制所述收件方是否可查看所述加密邮件。

14、如权利要求 13 所述邮件发送端，其特征在于：所述获取单元，包括：

15 时间获取子单元，用于获得待发送邮件的失效时间，所述失效时间为所述邮件发送后过期失效的时间；

密钥获取子单元，用于根据所述失效时间得到时间密钥。

15、如权利要求 13 所述的邮件发送端，其特征在于，所述加密单元，包括：

20 第一加密子单元，用于用所述时间密钥对所述待发送邮件进行加密生成所述加密邮件；或者

第二加密子单元，用于生成会话密钥，用所述时间密钥和所述会话密钥的组合对所述待发送邮件进行加密生成所述加密邮件。

16、如权利要求 15 所述的邮件发送端，其特征在于，所述第二加密子单元，用于：

25 用所述会话密钥对待发送邮件进行加密，生成所述加密邮件中的邮件数据密文；

用所述时间密钥对所述会话密钥进行加密，生成所述加密邮件中的会话密钥密文。

30 17、如权利要求 16 所述的邮件发送端，其特征在于，所述加密邮件具体是：在发送前将由所述邮件数据密文和会话密钥密文进行封装后生成的封装

包。

18、如权利要求 13~17 任一所述的邮件发送端，其特征在于，所述时间密钥为利用标识密码算法计算得到的时间公钥。

19、如权利要求 14 所述的邮件发送端，其特征在于，所述时间获取子单元，用于：

将所述待发送邮件的发送时间加上固定期限生成所述失效时间。

20、一种邮件接收端，包括：

第一接收单元：用于接收根据时间密钥进行加密的加密邮件，所述时间密钥用于限制所述加密邮件可被查看的时间期限；

10 响应请求单元：用于响应查看所述加密邮件的查看操作，生成并发送密钥请求至服务器，所述密钥请求用于获取所述加密邮件的所述时间密钥；

第二接收单元：用于接收所述服务器响应所述密钥请求的反馈信息，所述反馈信息由所述服务器根据所述密钥请求的请求时间和发送端发送的所述时间密钥生成，当所述请求时间超出所述时间密钥对应的时间范围时所述反
15 馈信息为表征所述加密邮件无效的信息，当所述请求时间在所述时间密钥对应的时间范围内时所述反馈信息为所述时间密钥；

解析响应单元：用于解析所述反馈信息，根据解析结果响应所述查看操作。

21、如权利要求 20 所述的邮件接收端，其特征在于，所述加密邮件为：
20 用所述时间密钥加密生成的邮件；或者
用所述时间密钥和所述会话密钥的组合进行加密生成的邮件。

22、如权利要求 20 或权利要求 21 所述的邮件接收端，其特征在于，解析响应单元，用于：

当解析结果为所述加密邮件无效时，响应所述查看操作，提示用户所述
25 加密邮件已过期无法被查看；

当解析结果为所述时间密钥时，响应所述查看操作，根据所述时间密钥解密所述加密邮件，获得邮件数据并显示。

23、如权利要求 22 所述的邮件接收端，其特征在于，所述解析响应单元，包括：

30 第一解析响应子单元，用于用所述时间密钥解密所述加密邮件，得到邮

件数据；或者

第二解析响应子单元，用于解析所述加密邮件的封装包得到所述加密邮件中的会话密钥密文；用所述时间密钥解密所述会话密钥密文，得到会话密钥；用所述会话密钥解密所述加密邮件中的邮件数据密文，得到邮件数据。

5 24、一种邮件服务器，包括：

第三接收单元：用于接收邮件接收端发送的获取加密邮件时间密钥的密钥请求；

验证单元：用于将所述邮件接收端请求所述时间密钥的请求时间与所述时间密钥对应的时间范围进行比较；

10 第二发送单元：用于在所述请求时间超出所述时间范围时，拒绝向邮件接收端发放所述时间密钥，使得邮件接收端无法对加密邮件进行解密及查看；在所述请求时间未超出所述时间范围时，向邮件接收端发放所述时间密钥，使得邮件接收端根据所述时间密钥对加密邮件进行解密并查看。

15 25、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-7 中的任一个所述的邮件发送方法，或者，执行根据权利要求 8-11 中的任一个所述的邮件查看方法，或者，执行根据权利要求 12 所述的邮件查看控制方法。

26、一种计算机可读介质，其中存储了如权利要求 25 所述的计算机程序。

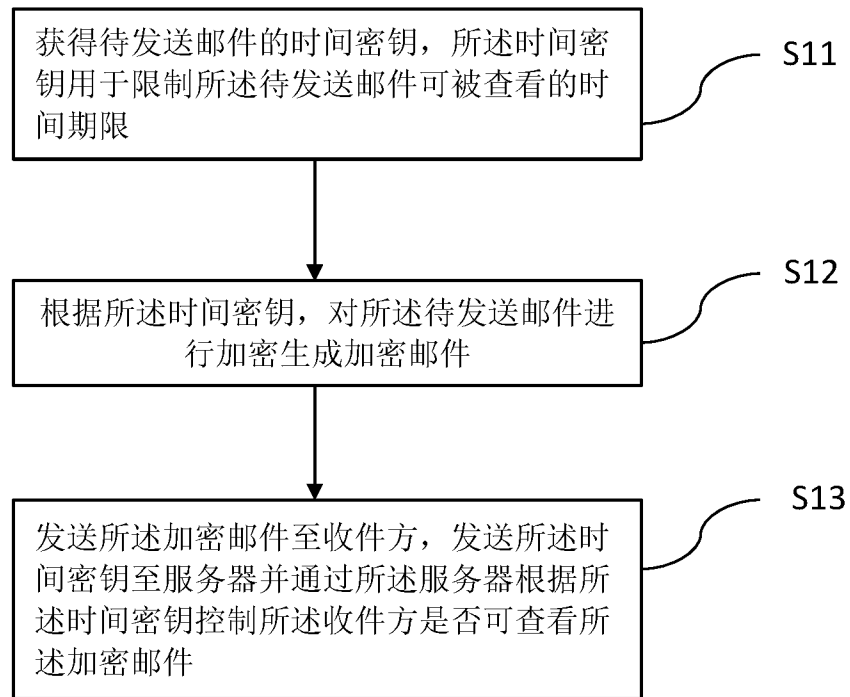


图 1

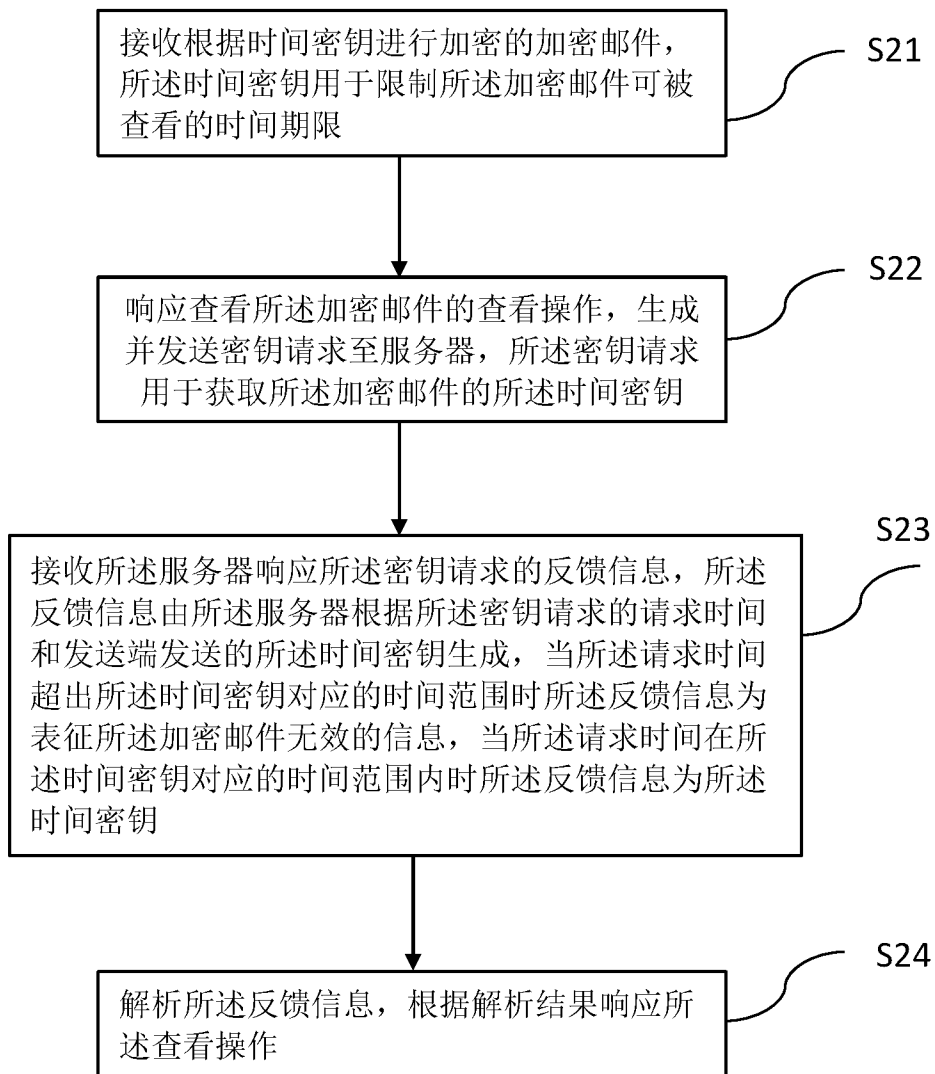


图 2

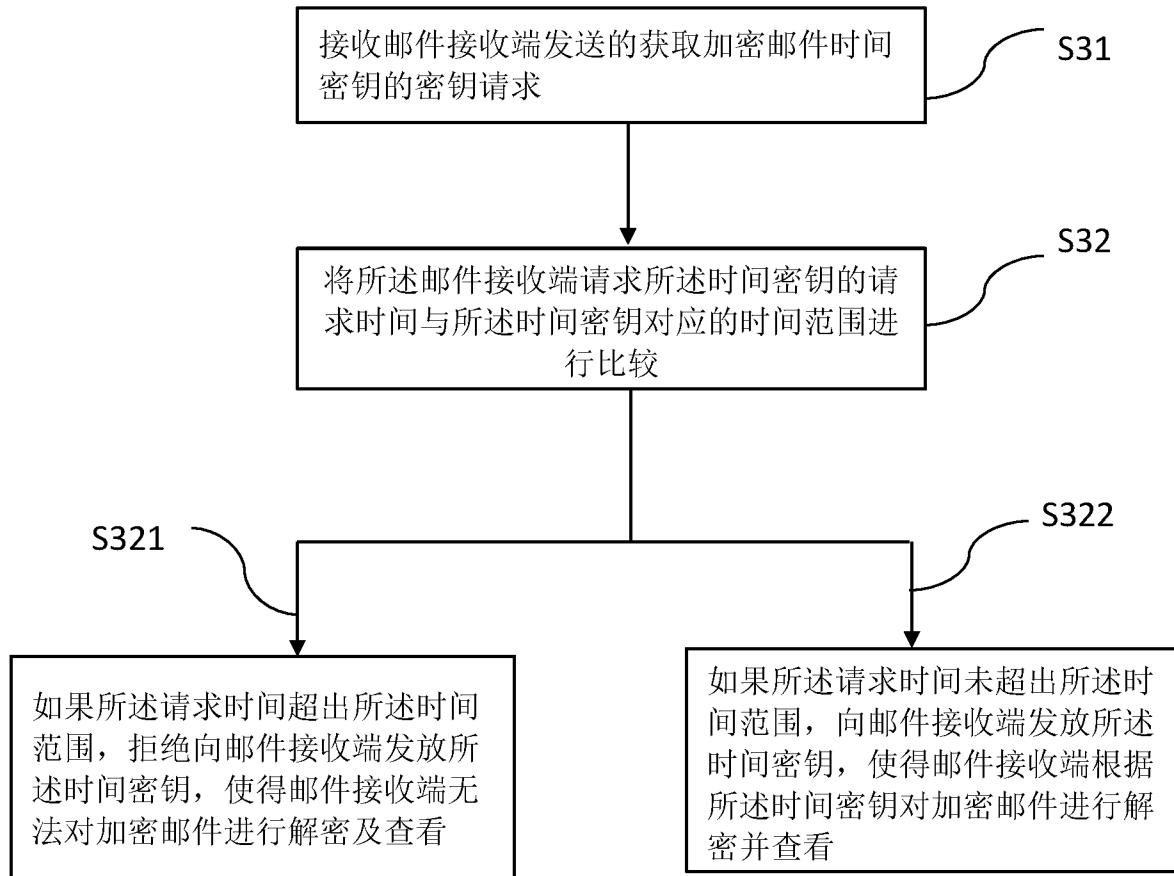


图 3

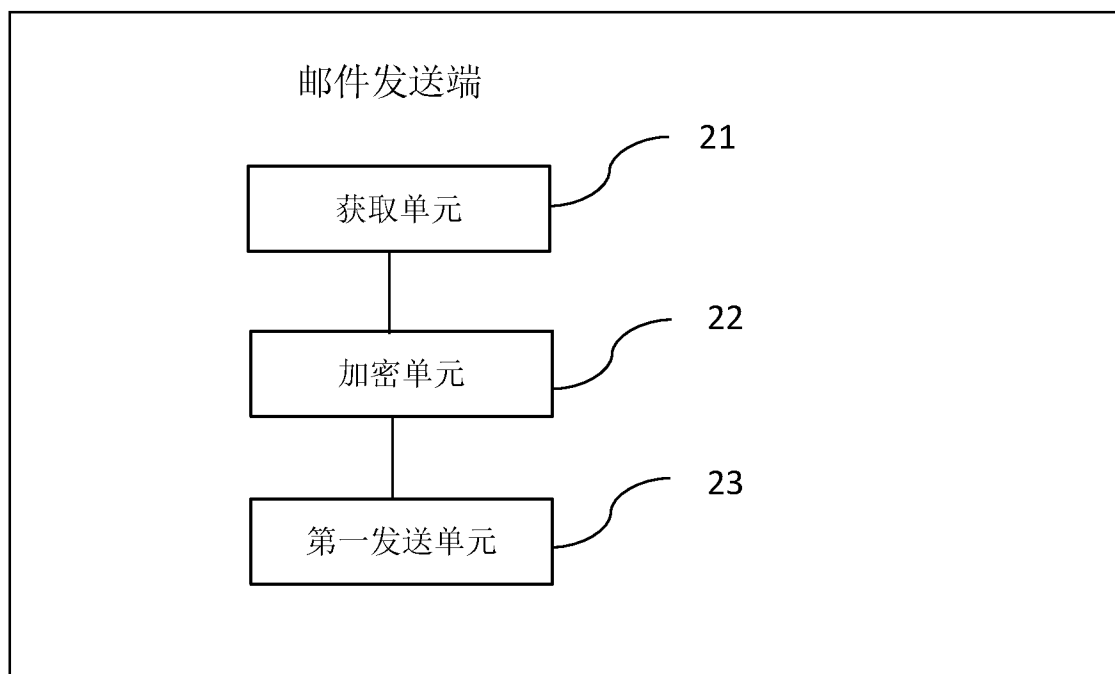


图 4

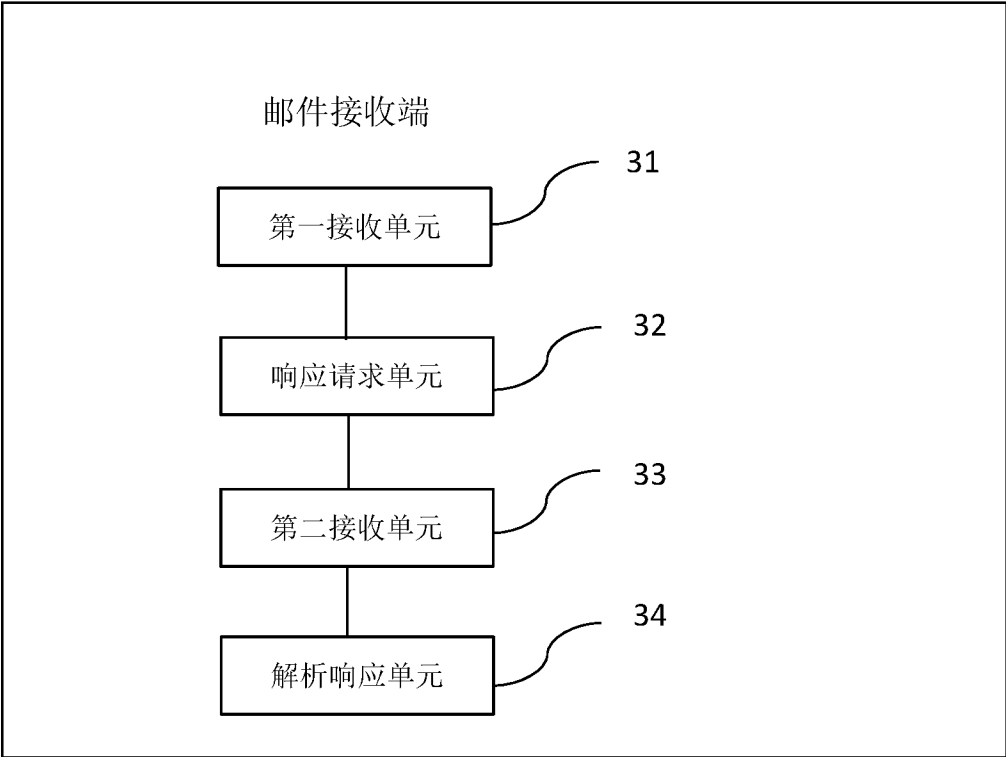


图 5

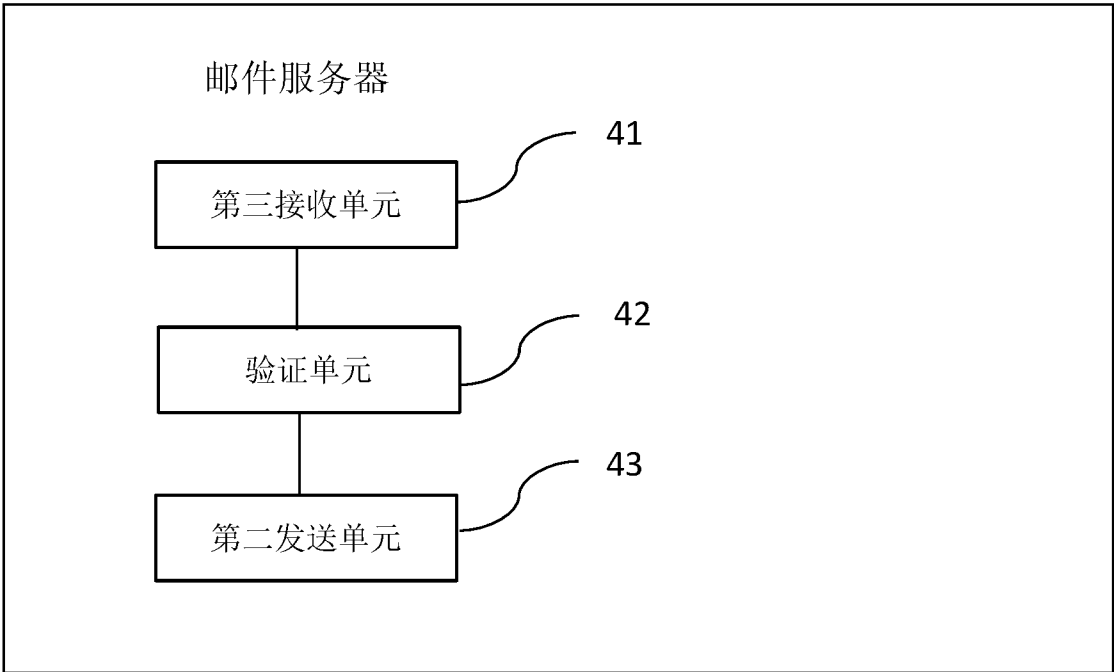


图 6

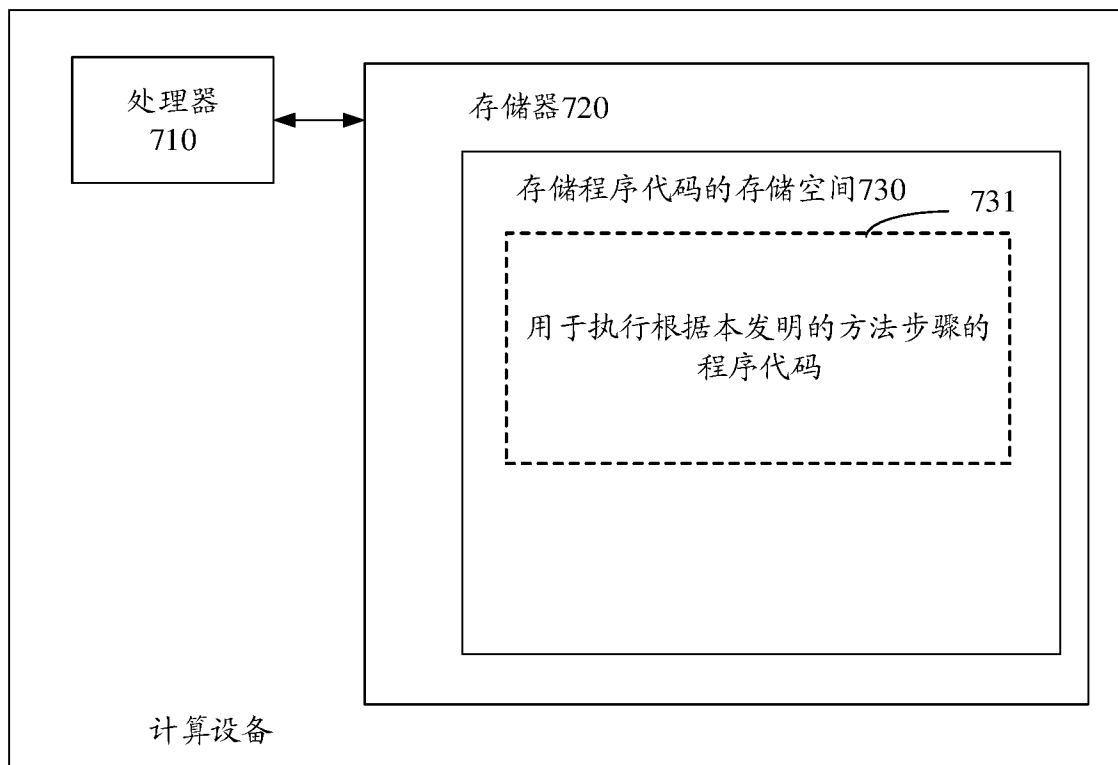


图 7

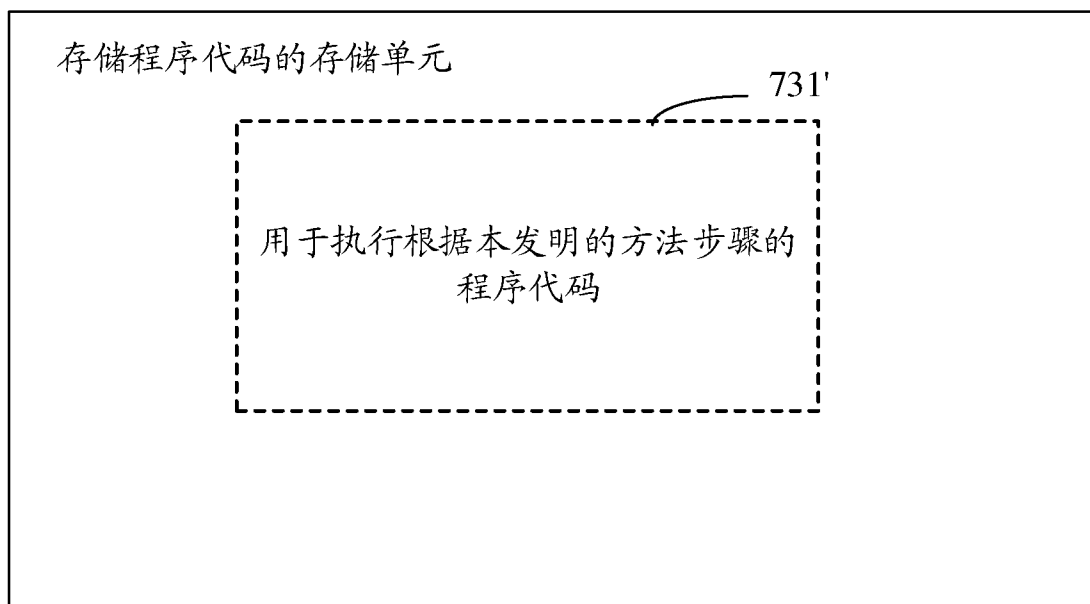


图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/117564

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/58 (2006.01) i; H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNXTX; CNABS; CNKI; VEN: 时间, 日期, 有效, 失效, 截止, 剩余, 到期, 有效期, 时限, 期限, 过期, 邮件, 消息, 加密, 密钥; time, date, overdue, end, residual, available, expire, limit, mail, email, message, IM, encrypt, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106603388 A (BEIJING QIHOO TECHNOLOGY CO., LTD.), 26 April 2017 (26.04.2017), description, paragraphs [0088]-[0291]	1-26
PX	CN 106453069 A (BEIJING QIHOO TECHNOLOGY CO., LTD.), 22 February 2017 (22.02.2017), description, paragraphs [0087]-[0296]	1-26
Y	CN 101677300 A (INTERNATIONAL BUSINESS MACHINES CORPORATION), 24 March 2010 (24.03.2010), description, page 4, line 18 to page 9, line 26 and page 18, lines 10-28	1-26
Y	CN 102195989 A (CHINA TELECOM CORPORATION LIMITED), 21 September 2011 (21.09.2011), description, paragraphs [0025]-[0055], and figure 2	1-26
A	CN 104660589 A (ZTE CORP.), 27 May 2015 (27.05.2015), entire document	1-26
A	US 2014013103 A1 (FUTUREWEI TECHNOLOGIES INC.), 09 January 2014 (09.01.2014), entire document	1-26

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 31 January 2018	Date of mailing of the international search report 12 February 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LI, Meili Telephone No. (86-10) 62089957

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/117564

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106603388 A	26 April 2017	None	
CN 106453069 A	22 February 2017	None	
CN 101677300 A	24 March 2010	None	
CN 102195989 A	21 September 2011	CN 102195989 B	26 March 2014
CN 104660589 A	27 May 2015	US 2017364691 A1	21 December 2017
		EP 3220573 A4	27 December 2017
		KR 20170096164 A	23 August 2017
		EP 3220573 A1	20 September 2017
		WO 2016115889 A1	28 July 2016
US 2014013103 A1	09 January 2014	US 9444794 B2	13 September 2016
		US 2016344706 A1	24 November 2016

国际检索报告

国际申请号

PCT/CN2017/117564

A. 主题的分类 H04L 12/58(2006.01)i; H04L 29/06(2006.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类																							
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) H04L; H04W 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) CNTXT;CNABS;CNKI;VEN:时间, 日期, 有效, 失效, 截止, 剩余, 到期, 有效期, 时限, 期限, 过期, 邮件, 消息, 加密, 密钥; time, date, overdue, end, residual, available, expire, limit, mail, email, message, IM, encrypt, key																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 106603388 A (北京奇虎科技有限公司) 2017年 4月 26日 (2017 - 04 - 26) 说明书第[0088]-[0291]段</td> <td>1-26</td> </tr> <tr> <td>PX</td> <td>CN 106453069 A (北京奇虎科技有限公司) 2017年 2月 22日 (2017 - 02 - 22) 说明书第[0087]-[0296]段</td> <td>1-26</td> </tr> <tr> <td>Y</td> <td>CN 101677300 A (国际商业机器公司) 2010年 3月 24日 (2010 - 03 - 24) 说明书第4页第18行-第9页第26行, 第18页第10-28行</td> <td>1-26</td> </tr> <tr> <td>Y</td> <td>CN 102195989 A (中国电信股份有限公司) 2011年 9月 21日 (2011 - 09 - 21) 说明书第[0025]-[0055]段, 图2</td> <td>1-26</td> </tr> <tr> <td>A</td> <td>CN 104660589 A (中兴通讯股份有限公司) 2015年 5月 27日 (2015 - 05 - 27) 全文</td> <td>1-26</td> </tr> <tr> <td>A</td> <td>US 2014013103 A1 (FUTUREWEI TECHNOLOGIES INC) 2014年 1月 9日 (2014 - 01 - 09) 全文</td> <td>1-26</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 106603388 A (北京奇虎科技有限公司) 2017年 4月 26日 (2017 - 04 - 26) 说明书第[0088]-[0291]段	1-26	PX	CN 106453069 A (北京奇虎科技有限公司) 2017年 2月 22日 (2017 - 02 - 22) 说明书第[0087]-[0296]段	1-26	Y	CN 101677300 A (国际商业机器公司) 2010年 3月 24日 (2010 - 03 - 24) 说明书第4页第18行-第9页第26行, 第18页第10-28行	1-26	Y	CN 102195989 A (中国电信股份有限公司) 2011年 9月 21日 (2011 - 09 - 21) 说明书第[0025]-[0055]段, 图2	1-26	A	CN 104660589 A (中兴通讯股份有限公司) 2015年 5月 27日 (2015 - 05 - 27) 全文	1-26	A	US 2014013103 A1 (FUTUREWEI TECHNOLOGIES INC) 2014年 1月 9日 (2014 - 01 - 09) 全文	1-26
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
PX	CN 106603388 A (北京奇虎科技有限公司) 2017年 4月 26日 (2017 - 04 - 26) 说明书第[0088]-[0291]段	1-26																					
PX	CN 106453069 A (北京奇虎科技有限公司) 2017年 2月 22日 (2017 - 02 - 22) 说明书第[0087]-[0296]段	1-26																					
Y	CN 101677300 A (国际商业机器公司) 2010年 3月 24日 (2010 - 03 - 24) 说明书第4页第18行-第9页第26行, 第18页第10-28行	1-26																					
Y	CN 102195989 A (中国电信股份有限公司) 2011年 9月 21日 (2011 - 09 - 21) 说明书第[0025]-[0055]段, 图2	1-26																					
A	CN 104660589 A (中兴通讯股份有限公司) 2015年 5月 27日 (2015 - 05 - 27) 全文	1-26																					
A	US 2014013103 A1 (FUTUREWEI TECHNOLOGIES INC) 2014年 1月 9日 (2014 - 01 - 09) 全文	1-26																					
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																							
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																							
国际检索实际完成的日期 2018年 1月 31日		国际检索报告邮寄日期 2018年 2月 12日																					
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 李美丽 电话号码 (86-10)62089957																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/117564

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106603388	A	2017年 4月 26日	无			
CN	106453069	A	2017年 2月 22日	无			
CN	101677300	A	2010年 3月 24日	无			
CN	102195989	A	2011年 9月 21日	CN	102195989	B	2014年 3月 26日
CN	104660589	A	2015年 5月 27日	US	2017364691	A1	2017年 12月 21日
				EP	3220573	A4	2017年 12月 27日
				KR	20170096164	A	2017年 8月 23日
				EP	3220573	A1	2017年 9月 20日
				WO	2016115889	A1	2016年 7月 28日
US	2014013103	A1	2014年 1月 9日	US	9444794	B2	2016年 9月 13日
				US	2016344706	A1	2016年 11月 24日