(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 102088443 B
(45)授权公告日 2015.04.01

(21)申请号 200910241440.5
(22)申请日 2009.12.02
(73)专利权人 北大方正集团有限公司
地址 100871 北京市海淀区成府路298号中关村方正大厦5层
专利权人 北京方正阿帕比技术有限公司
北京大学
(72)发明人 黄肖俊 汤帜
(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
代理人 陈源 罗建民
(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/10(2013.01)
H04L 29/08(2006.01)

(56)对比文件
CN 1571331 A,2005.01.26, 全文.
US 2003/0161473 A1,2003.08.28, 全文.

审查员 杨凯鹏

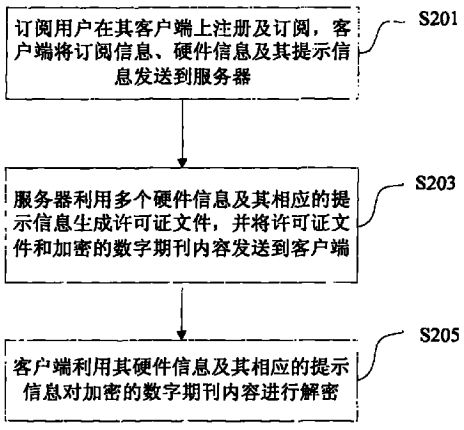
权利要求书5页 说明书9页 附图6页

(54)发明名称

一种带版权保护的数字期刊订阅方法和系统

(57)摘要

本发明提供了一种带版权保护的数字期刊订阅方法及系统，其中，服务器利用注册的每个客户端的硬件信息作为加密密钥对用于加密数字期刊内容的保护密钥进行加密，之后将其与相应的提示信息生成一个授权许可，再将多个授权许可合并生成一个许可证文件，在每个发行日，将许可证文件和加密的数字期刊内容一起推送到客户端。接收到许可证文件的客户端根据许可证文件和硬件信息及其相应的提示信息对加密的数字期刊内容进行解密。通过本发明生成的许可证文件限定仅在指定的硬件设备上获得加密的数字期刊内容，并且一个许可证文件可在订阅用户注册的多个硬件设备上使用，并且在硬件设备发生部分变化的时候，许可证文件仍然可以正常使用，大大方便了用户。



CN 102088443 B

1. 一种带版权保护的数字期刊订阅方法，该方法包括：

步骤 1、订阅用户在其客户端上向服务器注册并订阅数字期刊，服务器接收订阅用户所注册的多个客户端的注册信息和订阅信息，所述注册信息包括客户端设备的硬件信息及与所述硬件信息相应的提示信息，所述提示信息为客户端设备的设备名称或用户输入的名称，所述订阅信息包括订阅用户信息、订阅的期刊名及其订阅起止期；

步骤 2、服务器利用保护密钥对订阅的数字期刊内容进行加密，并且对于发行日在其订阅起止期之内的订阅用户，根据保护密钥和从其客户端接收的注册信息中的硬件信息及与所述硬件信息相应的提示信息生成许可证文件，然后将许可证文件和加密的数字期刊内容推送到该订阅用户的客户端；和

步骤 3、接收到许可证文件和加密的数字期刊内容的客户端根据该许可证文件和注册时所使用的硬件信息及与所述硬件信息相应的提示信息对加密的数字期刊内容进行解密；

所述步骤 2 中服务器生成许可证文件的步骤包括：

利用注册的每个客户端设备的硬件信息生成加密密钥对保护密钥进行加密，形成一个加密信息；

将该加密信息及其相应的提示信息一起生成一个授权许可，所述相应的提示信息指的是该客户端注册时注册信息中的提示信息；

将生成的多个授权许可合并生成一个许可证文件，以使得多个客户端能够共用所述许可证文件；

所述步骤 3 包括：

根据所述客户端注册时使用的提示信息找到许可证文件中相应的授权许可；

利用该客户端设备的硬件信息生成解密密钥对该授权许可中的加密信息进行解密，得到保护密钥；

利用该保护密钥对加密的数字期刊内容进行解密。

2. 根据权利要求 1 所述的方法，其特征在于，所述步骤 1 包括：

订阅用户分别在其多个客户端上注册并订阅数字期刊，这些客户端分别采集各自设备的硬件信息及与所述硬件信息相应的提示信息，并将该硬件信息及与所述硬件信息相应的提示信息以及订阅信息一起发送到服务器。

3. 根据权利要求 1 所述的方法，其特征在于，所述步骤 1 包括：

订阅用户在其一个客户端上注册并订阅数字期刊，该客户端采集自身设备的硬件信息和该订阅用户所注册的其它客户端设备的硬件信息以及与这些硬件信息相应的提示信息，并将这些硬件信息及与所述硬件信息相应的提示信息与订阅信息一起发送到服务器。

4. 根据权利要求 1 所述的方法，其特征在于，所述服务器利用注册的硬件信息生成加密密钥的步骤包括：

利用消息摘要算法对客户端设备的硬件信息进行变换，并利用变换后得到的信息生成加密密钥。

5. 根据权利要求 4 所述的方法，其特征在于，所述客户端利用消息摘要算法对客户端设备的硬件信息进行变换，并利用变换后得到的信息生成解密密钥进行解密。

6. 根据权利要求 1 所述的方法，其特征在于，所述保护密钥使用随机密钥算法生成。

7. 根据权利要求 1 所述的方法，其特征在于，所述提示信息为相应客户端的设备名称或者用户输入的名称。

8. 根据权利要求 7 所述的方法，其特征在于，在订阅用户注册并订阅数字期刊时，如果注册的提示信息重复，则允许订阅用户修改提示信息。

9. 根据权利要求 1 所述的方法，其特征在于，所述订阅信息还包括根据不同的订阅条件所获得的使用权利，包括对解密的数字期刊内容的转发、下载、复印、打印操作的权利以及注册客户端的数量限定，所述订阅条件包括收费条件。

10. 根据权利要求 1 所述的方法，其特征在于，服务器将许可证文件和加密的数字期刊内容合并成一个文件推送到订阅用户的客户端。

11. 根据权利要求 1 所述的方法，其特征在于，还包括 ：

订阅用户从其已经注册的多个客户端中的任何一个向服务器发送删除设备的请求，该删除请求中包括发送该删除请求的设备的硬件信息及与所述硬件信息相应的提示信息以及待删除设备的提示信息，

服务器在接收到删除请求之后，从原来的注册信息中删除待删除设备的硬件信息及与所述硬件信息相应的提示信息，从而得到更新的注册信息，并利用该更新的注册信息和所述保护密钥生成许可证文件，然后将该许可证文件和加密的数字期刊内容推送到该订阅用户的注册客户端。

12. 根据权利要求 11 所述的方法，其特征在于，还包括 ：客户端对所述删除请求进行加密和串接以将其作为参数发送到服务器。

13. 根据权利要求 1 所述的方法，其特征在于，还包括 ：

订阅用户从其已经注册的多个客户端中的任何一个向服务器发送增加设备的请求，该增加请求中包括发送该增加请求的设备的硬件信息及与所述硬件信息相应的提示信息以及待增加设备的硬件信息及与所述硬件信息相应的提示信息，所述待增加设备的硬件信息及与所述硬件信息相应的提示信息由发送该增加请求的客户端设备采集，

服务器在接收到增加请求之后，在原来的注册信息中增加待增加设备的硬件信息及与所述硬件信息相应的提示信息，从而得到更新的注册信息，并利用该更新的注册信息和所述保护密钥生成许可证文件，然后将该许可证文件和加密的数字期刊内容推送到该订阅用户的注册客户端。

14. 根据权利要求 13 所述的方法，其特征在于，还包括 ：客户端对所述增加请求进行加密和串接以将其作为参数发送到服务器。

15. 根据权利要求 1 所述的方法，其特征在于，每个客户端设备的硬件信息包括该客户端设备的 n 个相关硬件配置的特征信息，其中包括该客户端设备上不存在的 n_0 个相关硬件配置的特征信息。

16. 根据权利要求 15 所述的方法，其特征在于，所述步骤 2 中服务器生成许可证文件的步骤包括 ：

根据接收的硬件信息，选择 (t,n) 门限方案中的门限参数 t 的值 ：$t \in [\left[\frac{n+n_0}{2}\right]+1, n)$，其中，t 表示有效子密钥的数量的阈值 ；

将所述保护密钥分成 n 个共享子密钥 ；

对于每个客户端设备，将这 n 个共享子密钥与该设备的硬件配置绑定，即利用接收的该设备的 n 个硬件配置的特征信息生成 n 个加密密钥，分别用于对这 n 个共享子密钥或者这 n 个共享子密钥逐个进行变换后得到的 n 个信息串进行加密，同时生成各个共享子密钥的有效性校验信息；将门限参数 t 的值、加密的共享子密钥及其有效性校验信息形成一个加密信息；将该加密信息及解密该加密信息的提示信息一起生成一个授权许可；

将生成的多个授权许可合并生成一个许可证文件。

17. 根据权利要求 16 所述的方法，其特征在于，所述步骤 3 包括：

根据所述客户端注册时使用的提示信息找到许可证文件中相应的授权许可；

提取该客户端设备的 n 个相关硬件配置的特征信息，并利用这些特征信息生成 n 个解密密钥，分别用于对该授权许可中的加密信息中的 n 个共享子密钥或者 n 个信息串进行解密；

根据各个共享子密钥的有效性校验信息和 (t, n) 门限方案，对解密的各个共享子密钥进行有效性校验，如果存在 t 个及以上的有效共享子密钥，则根据这些有效子密钥恢复数字期刊内容的保护密钥，并利用该保护密钥对加密的数字期刊内容进行解密，否则密钥恢复失败。

18. 一种带版权保护的数字期刊订阅系统，该系统包括：

多个客户端，用于订阅用户在其上向服务器注册并订阅数字期刊，然后将注册信息和订阅信息发送到服务器，所述注册信息包括客户端设备的硬件信息及与所述硬件信息相应的提示信息，所述提示信息为客户端设备的设备名称或用户输入的名称，所述订阅信息包括订阅用户信息、订阅的期刊名及其订阅起止期；当从服务器接收到许可证文件和加密的数字期刊内容时，根据该许可证文件和注册时所使用的硬件信息及与所述硬件信息相应的提示信息对加密的数字期刊内容进行解密；和

服务器，用于利用保护密钥对订阅的数字期刊内容进行加密，并且对于发行日在其订阅起止期之内的订阅用户，根据保护密钥和从其客户端接收的注册信息中的硬件信息及与所述硬件信息相应的提示信息生成许可证文件，然后将许可证文件和加密的数字期刊内容推送到该订阅用户的客户端；

所述服务器包括：

订阅处理单元，用于从客户端接收注册信息和订阅信息，并将注册信息和订阅信息发送给期刊加密及授权单元；

期刊加密及授权单元，用于利用保护密钥对数字期刊内容进行加密，并且对于发行日在其订阅起止期之内的订阅用户，根据保护密钥和从其客户端接收的注册信息中的硬件信息及与所述硬件信息相应的提示信息生成许可证文件；和

推送单元，用于将许可证文件和加密的数字期刊内容推送到客户端；

所述期刊加密及授权单元包括：

期刊内容单元，用于利用保护密钥对数字期刊内容进行加密，并将保护密钥发送给加密密钥单元，将加密的数字期刊内容发送给推送单元；

加密密钥单元，用于利用从订阅处理单元接收的硬件信息生成加密密钥对从期刊内容单元接收的保护密钥进行加密，形成一个加密信息，并将该加密信息发送给许可证文件生成单元，将加密密钥发送给订阅客户端信息单元；

订阅客户端信息单元，用于生成从订阅处理单元接收的提示信息与从加密密钥单元接收的加密密钥的相应关系；

许可证文件生成单元，用于利用从订阅客户端信息单元接收的相应关系、从订阅处理单元接收的提示信息和从加密密钥单元接收的加密信息生成一个授权许可，并将生成的多个授权许可合并生成一个许可证文件，然后将该许可证文件发送给推送单元；

所述客户端包括：

采集单元，采集该客户端自身设备的硬件信息及与所述硬件信息相应的提示信息，并将该硬件信息和提示信息作为一个注册信息发送到注册单元；

注册单元，订阅用户通过该注册单元注册并订阅数字期刊，并将订阅信息和注册信息发送到服务器；

接收单元，用于接收从服务器推送的许可证文件和加密的数字期刊内容，并将许可证文件发送给保护密钥单元，将加密的数字期刊内容发送给解密数字期刊单元；

保护密钥单元，用于根据注册时使用的提示信息找到许可证文件中相应的授权许可，并利用该客户端的硬件信息生成解密密钥对该授权许可中的加密信息进行解密，得到保护密钥，并将保护密钥发送给解密数字期刊单元；和

解密数字期刊单元，利用从保护密钥单元接收的保护密钥对从接收单元接收的加密的数字期刊内容进行解密；

所述保护密钥单元包括：

许可证提取单元，用于根据注册时使用的提示信息在从接收单元接收的许可证文件中找到相应的授权许可，从该授权许可中获取相应的加密信息，并将该加密信息发送给解密保护密钥单元；

解密保护密钥单元，利用该客户端的硬件信息生成解密密钥对从许可证提取单元接收的加密信息进行解密，得到保护密钥。

19. 根据权利要求 18 所述的系统，其特征在于，所述采集单元采集其自身设备的硬件信息和订阅用户所注册的其它客户端设备的硬件信息以及与这些硬件信息相应的提示信息，并将这些硬件信息和提示信息作为一个注册信息发送给注册单元。

20. 根据权利要求 18 所述的系统，其特征在于，服务器将许可证文件和加密的数字期刊内容合并成一个文件推送到该订阅用户的客户端。

21. 根据权利要求 18 所述的系统，其特征在于，订阅用户从其已经注册的多个客户端中的任何一个向服务器发送删除设备的请求，该删除请求中包括发送该删除请求的设备的硬件信息及与所述硬件信息相应的提示信息以及待删除设备的提示信息，

服务器在接收到删除请求之后，从原来的注册信息中删除待删除设备的硬件信息及与所述硬件信息相应的提示信息，从而得到更新的注册信息，并利用该更新的注册信息和所述保护密钥生成许可证文件，然后将该许可证文件和加密的数字期刊内容推送到该订阅用户的注册客户端。

22. 根据权利要求 21 所述的系统，其特征在于，客户端对所述删除请求进行加密和串接以将其作为参数发送到服务器。

23. 根据权利要求 18 所述的系统，其特征在于，订阅用户从其已经注册的多个客户端中的任何一个向服务器发送增加设备的请求，该增加请求中包括发送该增加请求的设备的

硬件信息及与所述硬件信息相应的提示信息以及待增加设备的硬件信息及与所述硬件信息相应的提示信息，所述待增加设备的硬件信息及与所述硬件信息相应的提示信息由发送该增加请求的设备采集，

服务器在接收到增加请求之后，在原来的注册信息中增加待增加设备的硬件信息及与所述硬件信息相应的提示信息，从而得到更新的注册信息，并利用该更新的注册信息和所述保护密钥生成许可证文件，然后将该许可证文件和加密的数字期刊内容推送到该订阅用户的注册客户端。

24. 根据权利要求 23 所述的系统，其特征在于，客户端对所述增加请求进行加密和串接以将其作为参数发送到服务器。

25. 根据权利要求 18 所述的系统，其特征在于，每个客户端设备的硬件信息包括该客户端设备的 n 个相关硬件配置的特征信息，其中包括该客户端设备上不存在的 n_0 个相关硬件配置的特征信息。

26. 根据权利要求 25 所述的系统，其特征在于，服务器生成许可证文件的步骤包括：

根据接收的硬件信息，选择 (t,n) 门限方案中的门限参数 t 的值：$t \in [\left[\frac{n+n_0}{2}\right]+1, n)$，其中，t 表示有效子密钥的数量的阈值；

将所述保护密钥分成 n 个共享子密钥；

对于每个客户端设备，将这 n 个共享子密钥与该设备的硬件配置绑定，即利用接收的该设备的 n 个硬件配置的特征信息生成 n 个加密密钥，分别用于对这 n 个共享子密钥或者这 n 个共享子密钥逐个进行变换后得到的 n 个信息串进行加密，同时生成各个共享子密钥的有效性校验信息；将门限参数 t 的值、加密的共享子密钥及其有效性校验信息形成一个加密信息；将该加密信息及解密该加密信息的提示信息一起生成一个授权许可；

将生成的多个授权许可合并生成一个许可证文件。

27. 根据权利要求 26 所述的系统，其特征在于，服务器执行以下解密步骤：

根据所述客户端注册时使用的提示信息找到许可证文件中相应的授权许可；

提取该客户端设备的 n 个相关硬件配置的特征信息，并利用这些特征信息生成 n 个解密密钥，分别用于对该授权许可中的加密信息中的 n 个共享子密钥或者 n 个信息串进行解密；

根据各个共享子密钥的有效性校验信息和 (t，n) 门限方案，对解密的各个共享子密钥进行有效性校验，如果存在 t 个及以上的有效共享子密钥，则根据这些有效子密钥恢复数字期刊内容的保护密钥，并利用该保护密钥对加密的数字期刊内容进行解密，否则密钥恢复失败。

一种带版权保护的数字期刊订阅方法和系统

技术领域

[0001] 本发明涉及数字期刊领域，具体涉及一种带版权保护的数字期刊订阅方法和系统。

背景技术

[0002] 目前数字期刊订阅的主要方式，是将期刊内容做成一个不加密的文件（如 pdf），然后做为附件通过 email 分发到订阅用户的计算机上，无法实现对数字内容的版权保护。而现有的数字版权保护技术，主要涉及电子图书等单行本的保护，并且都是通过网站进行下载的方式进行，对数字期刊这样的连续出版物使用起来并不方便。

[0003] 在申请号为 02815591.2 的中国专利“用于订阅数字权利管理的方法和系统”中，提出了一种可用于数字期刊订阅的管理方法。在该方法中，存储有包括与订阅用户相关的公钥的订阅清单，许可证服务器通过检查订阅用户的公钥是否在订阅清单上来提交许可证，在许可证中定义了与多个受保护内容相关的使用权利及其使用条件和状态变量等。在从许可证服务器获取许可证之后，分发点（比如，商家）将其与多个受保护内容一起预打包，发送给订阅用户，从而订阅用户能够根据许可证中定义的使用权利及其使用条件来访问多个受保护内容，而不必独立激活与每个受保护内容相关的每个许可证。但是，由于这种方法是通过根据每个订阅用户的公钥生成许可证，即，为每个订阅用户生成许可证来达到对订阅内容的控制，所以无法控制订阅内容仅在指定的多个硬件设备上使用。也就是说，这种方法主要是依据与订阅用户相关的信息（比如，域账号信息），而不是其多台硬件设备的信息，所以在任何一个硬件设备上只要用域账号登录就允许访问，而不能控制仅限于在指定的硬件设备上访问。简而言之，这种方式只能实现对人的控制，而不能实现对硬件设备的控制，特别是对一个订阅用户多台设备的控制的情况。

发明内容

[0004] 为了解决上述问题，本发明提供一种带版权保护的数字期刊订阅方法和系统，从而避免数字期刊发行过程中被随意转发的问题，并且仅可在订阅用户指定的多个硬件设备上获得加密的数字期刊内容。

[0005] 为了实现以上目的，本发明提供的带版权保护的数字期刊订阅方法包括以下步骤：步骤 1、订阅用户在其客户端上向服务器注册并订阅数字期刊，服务器接收订阅用户所注册的多个客户端的注册信息和订阅信息，所述注册信息包括客户端设备的硬件信息及其相应的提示信息，所述订阅信息包括订阅用户信息、订阅的期刊名及其订阅起止期；步骤 2、服务器利用保护密钥对订阅的数字期刊内容进行加密，并且对于发行日在其订阅起止期之内的订阅用户，根据保护密钥和从其客户端接收的注册信息中的硬件信息及其相应的提示信息生成许可证文件，然后将许可证文件和加密的数字期刊内容推送到该订阅用户的客户端；和步骤 3、接收到许可证文件和加密的数字期刊内容的客户端根据该许可证文件和注册时使用的硬件信息及其相应的提示信息对加密的数字期刊内容进行解密。

[0006] 可通过以下两种方式来执行步骤 1 :订阅用户分别在其多个客户端上注册并订阅数字期刊,这些客户端分别采集各自设备的硬件信息及其相应的提示信息,并将该硬件信息及其相应的提示信息与订阅信息一起发送到服务器 ;或者,订阅用户在其一个客户端上注册并订阅数字期刊,该客户端采集自身设备的硬件信息和该订阅用户所注册的其它客户端设备的硬件信息以及与这些硬件信息相应的提示信息,并将这些硬件信息及其相应的提示信息与订阅信息一起发送到服务器。

[0007] 步骤 2 中服务器生成许可证文件的步骤包括 :利用注册的每个客户端的硬件信息生成加密密钥对保护密钥进行加密,形成一个加密信息 ;将该加密信息及其相应的提示信息一起生成一个授权许可 ;将生成的多个授权许可合并生成一个许可证文件。其中,服务器可利用消息摘要算法对客户端设备的硬件信息进行变换,并利用变换后得到的信息生成加密密钥。

[0008] 步骤 3 包括 :根据注册时使用的提示信息找到许可证文件中相应的授权许可 ;利用该客户端的硬件信息生成解密密钥对该授权许可中的加密信息进行解密,得到保护密钥 ;利用保护密钥对加密的数字期刊内容进行解密。其中,客户端可利用消息摘要算法对客户端设备的硬件信息进行变换,并利用变换后得到的信息生成解密密钥进行解密。

[0009] 优选地,本发明还可通过以下方法删除多余的设备 :订阅用户从其已经注册的多个客户端中的任何一个向服务器发送删除设备的请求,该删除请求中包括发送该删除请求的设备的硬件信息及其相应的提示信息以及待删除设备的提示信息。服务器在接收到删除请求之后,从原来的注册信息中删除待删除设备的硬件信息及其相应的提示信息,从而得到更新的注册信息,并利用该更新的注册信息和所述保护密钥生成许可证文件。

[0010] 优选地,可通过以下方法增加注册设备 :订阅用户从其已经注册的多个客户端中的任何一个向服务器发送增加设备的请求,该增加请求中包括发送该增加请求的设备的硬件信息及其相应的提示信息以及待增加设备的硬件信息及其相应的提示信息,所述待增加设备的硬件信息及其相应的提示信息由发送该增加请求的设备采集。服务器在接收到增加请求之后,在原来的注册信息中增加待增加设备的硬件信息及其相应的提示信息,从而得到更新的注册信息,并利用该更新的注册信息和所述保护密钥生成许可证文件。更优选地,本发明可通过密钥共享机制,结合用户设备的硬件配置情况,采用具有硬件适应性的数字期刊与硬件绑定的方法来保证在硬件设备中的部分硬件配置发生变更时仍可正常使用许可证文件。

[0011] 相应地,本发明提供的一种带版权保护的数字期刊订阅系统包括 :多个客户端,用于订阅用户在其上向服务器注册并订阅数字期刊,然后将注册信息和订阅信息发送到服务器,当从服务器接收到许可证文件和加密的数字期刊内容时,根据该许可证文件和注册时使用的硬件信息及其相应的提示信息对加密的数字期刊内容进行解密 ;和服务器,用于利用保护密钥对订阅的数字期刊内容进行加密,并且对于发行日在其订阅起止期之内的订阅用户,根据保护密钥和从其客户端接收的注册信息中的硬件信息及其相应的提示信息生成许可证文件,然后将许可证文件和加密的数字期刊内容推送到该订阅用户的客户端。

[0012] 在本发明中,服务器利用订阅用户注册的硬件信息作为加密密钥对用于对数字期刊内容进行加密的保护密钥进行加密,并将加密的保护密钥与其相应的提示信息一起生成相应的授权许可,从而使得只能在发行日在其订阅起止期内的订阅用户指定的多个客户端

上获得订阅内容，实现对硬件设备的控制。此外，服务器将多个授权许可合并起来生成一个许可证文件，从而使得可在订阅用户注册的多个硬件设备上共用这一个许可证文件，而且在硬件设备中的部分硬件配置发生变更时仍可正常使用许可证文件，大大方便了用户。另外，本发明还可在已经注册的客户端上删除或增加设备，提高了数字期刊订阅的灵活性。

附图说明

[0013] 图 1 是根据本发明的第一实施方式的带版权保护的数字期刊订阅系统的结构示意图；

[0014] 图 2 是根据本发明的第一实施方式的带版权保护的数字期刊订阅方法的流程示意图；

[0015] 图 3 是图 1 所示系统中的服务器的具体结构示意图；

[0016] 图 4 是图 1 所示系统中的客户端的具体结构示意图；

[0017] 图 5 是根据本发明的第二实施方式的带版权保护的数字期刊订阅系统的结构示意图；

[0018] 图 6 是根据本发明的具体实施例的许可证文件的示意图。

具体实施方式

[0019] 本发明提供了一种带版权保护的数字期刊订阅方法和系统，用于对数字期刊内容在订阅和发行过程中进行保护和控制，避免数字期刊发行过程中被随意转发的问题，并且可以支持一个许可证文件在订阅用户所注册的多个硬件设备中使用。

[0020] 下面将结合附图和实施例对本发明进行详细说明。

[0021] （第一实施方式）

[0022] 图 1 是根据本发明的第一实施方式的带版权保护的数字期刊订阅系统的结构示意图。如图 1 所示，该系统包括：服务器 11 和多个客户端 12A、多个客户端 12B（及更多的客户端 12C、12D……，图中未示出），其中多个客户端 12A 属于同一个订阅用户 A，多个客户端 12B 属于同一个订阅用户 B。以下，以客户端 12A 与服务器 11 之间的交互为例进行说明。

[0023] 图 2 是根据本发明的第一实施方式的带版权保护的数字期刊订阅方法的流程图。如图 2 所示，该方法包括以下步骤：

[0024] 步骤 S201、订阅用户注册及订阅步骤

[0025] 在该步骤中，订阅用户在其客户端上向服务器注册并订阅数字期刊，客户端将注册信息和订阅信息发送到服务器，所述注册信息客户端设备的硬件信息及其相应的提示信息，所述订阅信息包括订阅用户信息、订阅的期刊名及其订阅起止期。服务器接收订阅用户所注册的多个客户端的注册信息和订阅信息。

[0026] 具体地讲，在本发明的第一实施方式中，订阅用户 A 在多个客户端 12A 上分别注册并订阅数字期刊，包括注册用户信息、选定订阅的期刊名以及订阅起止期等。然后，这些客户端 12A 提取客户端 12A 的设备名称（例如，计算机名称）作为与其相应的提示信息，并将其硬件信息和相应的提示信息作为注册信息与订阅信息一起发送到服务器 11，如上所述，订阅信息包括订阅用户信息、订阅的期刊名及其订阅起止期。或者，也可让用户输入一个名称作为与每个客户端 12A 的硬件信息相应的提示信息。为了使提示信息与每个客户端 12A

的硬件信息一一相应，如果注册的提示信息重复，比如设备名称重复，则允许订阅用户 A 修改提示信息，即，重新输入一个不重复的名称。

[0027] 步骤 S203、服务器加密及授权步骤

[0028] 在该步骤中，服务器利用保护密钥对订阅的数字期刊内容进行加密，并且对于发行日在其订阅起止期之内的订阅用户，根据保护密钥和从其客户端接收的注册信息中的硬件信息及其相应的提示信息生成许可证文件，然后将许可证文件和加密的数字期刊内容推送到该订阅用户的客户端。

[0029] 具体地讲，在数字期刊的发行日，服务器 11 使用密钥生成算法，比如随机密钥算法生成保护密钥，并利用该保护密钥对数字期刊内容进行加密，然后检查每一个订阅用户，如果当前发行日在其订阅起止期之内，则根据保护密钥和从该订阅用户的多个客户端接收的注册信息中的硬件信息及其相应的提示信息生成许可证文件，然后将许可证文件和加密的数字期刊内容推送到该订阅用户的多个客户端。其中，服务器生成许可证文件的步骤进一步包括：

[0030] 利用注册的每个客户端 12A 的硬件信息生成加密密钥对保护密钥进行加密，形成一个加密信息，其中，可利用消息摘要算法对客户端的硬件信息进行变换，并利用变换后得到的信息生成加密密钥；

[0031] 将该加密信息及其相应的提示信息一起生成一个授权许可；

[0032] 将生成的多个授权许可合并生成一个许可证文件。

[0033] 步骤 S205、客户端解密步骤

[0034] 在该步骤中，接收到许可证文件和加密的数字期刊内容的客户端 12A 根据该许可证文件和注册时使用的硬件信息及其相应的提示信息对加密的数字期刊内容进行解密。具体地讲，该步骤包括以下步骤：

[0035] 根据注册时所使用的提示信息找到许可证文件中相应的授权许可；

[0036] 利用该客户端 12A 的硬件信息生成解密密钥对找到的授权许可中的加密信息进行解密，得到保护密钥，其中，在服务器 11 利用消息摘要算法将多个客户端 12A 的硬件信息变换得到加密密钥的情况下，客户端 12A 相应地利用消息摘要算法对其硬件信息进行变换，利用变换后得到的信息生成解密密钥；

[0037] 利用解密得到的保护密钥对加密的数字期刊内容进行解密。

[0038] 通过这种订阅方法，订阅用户可以定期在其指定的多个客户端设备上接收到许可证文件和带版权保护的数字期刊内容，从而不仅保障了期刊社的利益，而且还可实现对硬件设备的控制。在订阅用户每次需要访问数字期刊内容时，其客户端利用注册时使用的设备名称或者输入的其它名称信息作为提示信息从许可证文件中找到相应的授权许可，并利用该客户端设备的硬件信息生成解密密钥，对该授权许可中的加密信息进行解密，从而获得保护密钥，然后利用该保护密钥对数字期刊内容进行解密。解密之后，订阅用户可以立即离线使用，大大提高了订阅用户使用的便捷程度。

[0039] 相比于每次获取订阅内容都需要重新发送申请的解决方案，本发明采用订阅方案，不需要每次等到发行数字期刊时由客户端发起请求，而是由服务器直接主动生成许可证文件，并将许可证文件推送到订阅用户限定的多个客户端，因而，可避免重放攻击的问题。

[0040] 此外，根据本发明生成的许可证文件不仅限定仅在订阅用户制定的几个客户端设备上使用，而且在这多个客户端设备上可共用这一个许可证文件，而不必分别为各个客户端生成多个许可证文件。因此，订阅用户可以非常简单方便地获取数字期刊。

[0041] 图 3 和图 4 分别是实现图 2 所示方法的服务器和客户端的具体结构图。

[0042] 如图 3 所示，服务器 11 具体包括：订阅处理单元 31，用于从客户端接收注册信息和订阅信息，并将注册信息和订阅信息发送给期刊加密及授权单元 32；期刊加密及授权单元 32，用于利用保护密钥对数字期刊内容进行加密，并且对于发行日在其订阅起止期之内的订阅用户，根据保护密钥和从其客户端接收的注册信息中的硬件信息及其相应的提示信息生成许可证文件；和推送单元 33，用于将许可证文件和加密的数字期刊内容推送到客户端。

[0043] 其中，期刊加密及授权单元 32 进一步包括：期刊内容单元 321，用于利用保护密钥对数字期刊内容进行加密，并将保护密钥发送给加密密钥单元 322，将加密的数字期刊内容发送给推送单元 33；加密密钥单元 322，用于利用从订阅处理单元 31 接收的硬件信息生成加密密钥对从期刊内容单元 321 接收的保护密钥进行加密，形成一个加密信息，并将该加密信息发送给许可证文件生成单元 324，将加密密钥发送给订阅客户端信息单元 323；订阅客户端信息单元 323，用于生成从订阅处理单元 31 接收的提示信息与从加密密钥单元 322 接收的加密密钥的相应关系；许可证文件生成单元 324，用于利用从订阅客户端信息单元 323 接收的相应关系、从订阅处理单元 31 接收的提示信息和从加密密钥单元 322 接收的加密信息生成一个授权许可，并将生成的多个授权许可合并生成一个许可证文件，然后将该许可证文件发送给推送单元 33。然后，推送单元 33 将许可证文件和加密的数字期刊内容推送到订阅用户 A 的多个客户端 12A。

[0044] 如图 4 所示，客户端 12A 具体包括：采集单元 40，采集该客户端 12A 自身的硬件信息及其相应的提示信息，并将该硬件信息和提示信息作为一个注册信息发送到注册单元 41；注册单元 41，订阅用户通过该注册单元注册并订阅数字期刊，并将订阅信息和注册信息发送到服务器 11；接收单元 42，用于接收从服务器 11 推送的许可证文件和加密的数字期刊内容，并将许可证文件发送给保护密钥单元 43，将加密的数字期刊内容发送给解密数字期刊单元 44；保护密钥单元 43，用于根据注册时使用的提示信息找到许可证文件中相应的授权许可，并利用该客户端 12A 的硬件信息生成解密密钥对该授权许可中的加密信息进行解密，得到保护密钥，并将该保护密钥发送给解密数字期刊单元 44；和解密数字期刊单元 44，利用从保护密钥单元 43 接收的保护密钥对从接收单元 42 接收的加密的数字期刊内容进行解密。

[0045] 其中，保护密钥单元 43 进一步包括：许可证提取单元 431，用于根据注册时使用的提示信息从接收单元 42 接收的许可证文件中找到相应的授权许可，从该授权许可中获取相应的加密信息，并将该加密信息发送给解密保护密钥单元 432；解密保护密钥单元 432，利用该客户端 12A 的硬件信息生成解密密钥对从许可证提取单元 431 接收的加密信息进行解密，得到保护密钥。

[0046] 以上参考图 1 至图 4 描述了根据本发明的第一实施方式的订阅方法和系统，但是应该理解，本发明方法并不仅限于该实施方式中公开的步骤和单元，还可包括其他优化方案。

[0047] 比如，为了增加安全性，客户端 12A 在向服务器 11 发送注册信息和订阅信息时，可对注册信息和订阅信息进行加密传送，服务器 11 接收到注册信息和订阅信息之后首先要利用相应的解密方法对其进行解密。而且，订阅用户 A 还可仅在一个客户端 12A 上进行订阅和注册，其它客户端 12A 上仅进行注册，而不必再进行订阅。

[0048] 又比如，在订阅用户 A 订阅数字期刊时，可根据不同的订阅条件，比如，不同的收费标准获得不同的使用权利，包括对解密的数字期刊内容的转发、下载、复印、打印等操作的权利，并且还可根据不同的收费标准限定注册客户端 12A 的数量。相应地，在许可证文件中的每个授权许可中，除了第一实施方式中所公开的加密信息及其相应的提示信息之外，还应包括这些订阅条件和使用权利。

[0049] 又比如，除了第一实施方式中所采用的推送方式之外，服务器 11 还可仅将许可证文件在发行日推送给订阅用户 A 所注册的多个客户端 12A。在这种情况下，接收到许可证文件的客户端 12A 首先根据该许可证文件从服务器 11 下载加密的数字期刊内容，并根据该许可证文件和注册信息对下载的加密的数字期刊内容进行解密。由于数字期刊内容已被加密，所以可通过任何渠道供用户下载，比如，公开地或者以特定密码等方式发布加密的数字期刊内容。此外，服务器 11 也可事先根据接收到的注册信息和订阅信息准备好随机保护密钥和许可证文件，在每期数字期刊内容制作完成之后，利用该随机保护密钥对其进行加密，然后定期（比如，在发行日或其它临近日期）将许可证文件等推送到注册的客户端 12A。或者，服务器还可将许可证文件和加密的数字期刊内容合并成一个文件，然后定期推送到该订阅用户的客户端。

[0050] （第二实施方式）

[0051] 在第二实施方式中，与第一实施方式的不同之处在于，不是分别在订阅用户 A 的每个客户端 12A 上注册，而是仅在其一个客户端 12A 上进行注册和订阅，通过该客户端 12A 采集订阅用户 A 所注册的所有客户端设备的硬件信息以及与这些硬件信息相应的提示信息。具体的采集方法可以通过网络连接、其它接口连接或者在本机上采集信息加密后发送或复制到正进行注册的客户端设备上。

[0052] 图 5 是实现以上方法的系统的示意图。如图 5 所示，在订阅用户 A 通过注册单元 41 注册并订阅数字期刊时，采集单元 40 采集其自身设备的硬件信息和订阅用户 A 所注册的其它客户端设备的硬件信息以及与这些硬件信息相应的提示信息，并将这些硬件信息和提示信息作为一个注册信息发送给注册单元 41。

[0053] 通过这种实施方式，订阅用户 A 仅需要在其一个客户端（比如，电脑）上进行注册和订阅，就可在该用户的其它客户端（比如，手机）上直接接收和观看数字期刊，而不需要在其它客户端上重新注册。

[0054] （具体实施例）

[0055] 以下将通过一个具体的实施例来对本发明进行进一步的说明。

[0056] 在该实施例中，假设，一期刊发行单位需要对一本每月 1 日发行的月刊进行带版权保护的订阅，一个订阅用户张三订阅了该期刊，订阅起止期为从 2009 年 1 月到 2009 年 12 月，并且需要在 N 台计算机（或手机、手持设备）上接收和阅读这份期刊。

[0057] 首先，张三在其一个客户端上向服务器注册用户并进行支付，并在 N 台计算机（或手机、手持设备）上分别向服务器注册硬件信息 HINFOi(i ＝ 1…N)（如 PC 机的主板号、CPU

号、硬盘号；Windows Mobile 的手持设备通过 GetDeviceUniqueID() 获取到的设备唯一编号），并分别提取相应的计算机名 CNAMEi(i = 1…N) 作为提示信息，例如，可以在 windows 平台使用 GetComputerName() 函数获取计算机名称，在 Linux 平台用 sys_gethostname() 函数获取计算机名称，在 Windows Mobile 平台 (Pocket PC 和 SmartPhone) 中使用 System.Net.Dns.GetHostName() 属性获取相关名称，在手持移动阅读设备上可以通过与计算机相连时的设备驱动程序获取设备的名称。然后，将获取到的硬件信息 HINFOi(i = 1…N) 和计算机名称 CNAMEi(i = 1…N) 作为注册信息与订阅信息（包括订阅用户信息、订阅的期刊名和订阅起止期）一起发送到服务器端。在发送注册信息和订阅信息时，通过加密传送硬件信息和计算机名，例如，用服务器公钥 K，分别对 HINFOi 和 CNAMEi 进行加密，并串接一起 K(HINFOi)+K(CNAMEi) 作为参数发送（串接方法可以通过增加分隔符如“||空格||”的办法进行）。

[0058] 接着，服务器通过与公钥 K 相应的私钥 P 进行解密；每月 1 日，首先准备好该月刊的数字期刊内容文件 CF，然后使用随机密钥生成器产生一个随机密钥作为保护密钥 KC，对内容文件 CF 进行对称加密得到加密的内容文件 KC(CF)。服务器检查到张三订阅了本期刊，于是用消息摘要算法 Hash() 对张三的 N 台设备的硬件信息进行变换后得到 Hash(HINFOi)(i = 1…N) 作为加密密钥，用于加密保护密钥 KC，得到加密信息 KHi(i = 1…N)。服务器在与该设备相应的授权许可中添加加密信息（即，已加密的保护密钥）KHi(i = 1…N) 以及解密该加密信息的提示信息，即，相应的加密信息与提示信息的相应关系。

[0059] 图 6 是该实施例中所生成的许可证文件 FLic 的示意图。如图 6 所示，<Permission> 标签中 ClientName 属性中的“zhangsanPC”信息即为提示信息，<info> 标签中的“akeo832mj294bkjhk”的信息即为加密信息，即，加密的保护密钥。

[0060] 接着，服务器将生成的许可证文件 FLic 与加密好的数字期刊内容文件 KC(CF) 一起，通过 email 发送到张三的邮箱中。

[0061] 张三收到邮件后，在张三的 N 台客户端设备上打开许可证文件 FLic，客户端首先获取本机的设备名称信息 CNAMEi 后，在许可证文件中找到 ClientName 与 CNAMEi 相同的 Permission 节点，获取其加密信息，即，<info> 节点中的信息。然后，利用本设备的硬件信息 HINFOi 经过消息摘要算法 Hash(HINFOi) 进行变换后得到解密密钥，解密出数字期刊内容的保护密钥 KC，并用该保护密钥 KC 解密数字期刊内容文件 KC(CF)，从而获得最终的该数字月刊内容 CF。

[0062] （第三实施方式）

[0063] 第三实施方式与以上实施方式相比，增加了允许删除多余的设备和增加新设备的功能。

[0064] 在某些情况下（如设备丢失、损坏或另做它用），订阅用户需要删除不再使用的多余的设备。可采用以下方法删除多余设备：订阅用户 A 从其已经注册的多个客户端 12A 中的任何一个向服务器 11 发送删除多余设备 12A’的请求，该删除请求中可包括如下相关参数：发送删除请求的设备 12A 的硬件信息 HINFOn 及其相应的提示信息 CNAMEn、以及待删除设备 12A’的提示信息 CNAMEm。这种方法不限定提出申请的设备为待删除的设备，这样可以保证即使某设备灭失，仍可在其它注册设备上向服务器发送删除请求，从而将该灭失的设备删除。

[0065] 此外，为了增强删除设备过程的安全性，可使用服务器 11 的公钥 K 对删除请求进行加密，并进行串接 K(HINFOn)+K(CNAMEn)+K(CNAMEm) 以作为参数发送（串接方法可以通过增加分隔符如“||空格||”的办法进行）。

[0066] 服务器 11 在接收到删除请求之后，从原来的注册信息中删除待删除设备 12A’的硬件信息及其相应的提示信息，从而得到更新的注册信息，并利用更新的注册信息和保护密钥生成许可证文件。然后，将该许可证文件和加密的数字期刊内容推送到订阅用户 A 的注册客户端 12A（此时，不包括已删除的客户端 12A’）。

[0067] 关于增加设备的功能，可通过以下方法来实现：订阅用户 A 可从其已经注册的多个客户端 12A 中的任何一个向服务器 11 发送增加设备 Am 的请求，该增加请求中包括发送增加请求的设备 12A 的硬件信息 HINFOn 及其相应的提示信息 CNAMEn 以及待增加设备 Am 的硬件信息 HINFOm 及其相应的提示信息 CNAMEm，其中，待增加设备 Am 的硬件信息 HINFOm 及其相应的提示信息 CNAMEm 由发送增加请求的设备 12A 采集。如上所述，具体的采集方法可以通过网络连接、其他接口连接或在本机 Am 上采集信息加密后发送或复制到正进行增加注册的客户端 12A 上。与删除设备过程一样，为了增强增加设备过程的安全性，使用服务器 11 的公钥 K 对增加请求进行加密，并进行串接 K(HINFOm)+K(CNAMEm)+K(HINFOn)+K(CNAMEn) 以作为参数发送（串接方法可以通过增加分隔符如“||空格||”的办法进行）。

[0068] 服务器 11 在接收到增加请求之后，在原来的注册信息中增加待增加设备 Am 的硬件信息及其相应的提示信息，从而得到更新的注册信息，并利用更新的注册信息和保护密钥生成许可证文件，然后，将该许可证文件和加密的数字期刊内容推送到订阅用户 A 的注册客户端 12A 和 Am。

[0069] （第四实施方式）

[0070] 第四实施方式与以上实施方式的不同之处在于，增加了对硬件设备中部分硬件配置变更的适应性功能，即，当硬件设备中的部分硬件配置（比如，主板、CPU、硬盘等）发生变更（包括更换、删除、增加等）时，仍然可正常使用生成的许可证文件来获取加密的数字期刊内容。

[0071] 对于这种功能，本发明采用具有硬件适应性的数字内容与硬件绑定的方法（参见专利号为 200410004751.7 的中国专利“具有硬件适应性的数字内容与硬件绑定的方法”）来实现。在这种方法中，主要采用密钥共享机制，结合订阅用户的客户端的硬件配置情况来实现硬件适应性，从而使得一定范围内硬件设备中的硬件配置的变更，不会影响数字内容的合法使用。具体地讲，将数字期刊的保护密钥分成 n 个共享子密钥，并根据客户端设备中的多个硬件配置生成分别对这 n 个共享子密钥进行加密的 n 个加密密钥。当在该客户端设备中有少于 n-t 个硬件配置发生变更时，即，当该客户端设备中有 t 个及以上的硬件配置保持有效时，仍能正常使用许可证文件来获取加密的数字内容，否则将无法继续使用数字内容。在该专利中，定义一个门限方案 (t，n) 来实现以上方法，其中，t 为有效子密钥（对应于保持有效的硬件配置）的数量的阈值。

[0072] 在本发明中，当订阅用户 A 在客户端 12A 上进行注册时，在第一实施方式的情况下，正在注册的客户端 12A 的采集单元 40 采集该硬件设备自身的 n 个相关硬件配置的特征信息（比如，编号），其中包括该客户端设备上不存在的 n_0 个相关硬件配置的特征信息；在采用第二实施方式的情况下，正在注册的客户端 12A 的采集单元 40 采集订阅用户 A 所注册

的全部客户端设备 12A 的相关硬件配置的特征信息，每个客户端设备采集 n 个相关硬件配置的特征信息（包括该客户端设备上不存在的 n_0 个相关硬件配置的特征信息）。此时，客户端 12A 向服务器 11 发送的硬件信息包括通过采集单元 40 采集的这些特征信息。

[0073] 服务器 11 接收到这样的硬件信息之后，按照以下步骤生成许可证文件：

[0074] 根据接收的硬件信息，选择 (t, n) 门限方案中的门限参数 t 的值：$t \in [\left[\frac{n+n_0}{2}\right]+1, n)$；

[0075] 将数字期刊的保护密钥分成 n 个共享子密钥；

[0076] 对于每个客户端设备，将这 n 个共享子密钥与该设备的硬件配置绑定，即利用接收的该设备的 n 个硬件配置的特征信息生成 n 个加密密钥，分别用于对 n 个共享子密钥或者这 n 个共享子密钥逐个进行变换后的 n 个信息串进行加密，同时生成各个共享子密钥的有效性校验信息；将门限参数 t 的值、加密的共享子密钥及其有效性校验信息形成一个加密信息；将该加密信息及其相应的提示信息一起生成一个授权许可；

[0077] 将生成的多个授权许可合并生成一个许可证文件。

[0078] 客户端 12A 接收到许可证文件之后，执行以下解密步骤：

[0079] 根据客户端 12A 注册时使用的提示信息找到许可证文件中相应的授权许可；

[0080] 提取该客户端 12A 的 n 个相关硬件配置的特征信息，并利用这些特征信息生成 n 个解密密钥，分别用于对该授权许可中的加密信息中的 n 个共享子密钥进行解密；

[0081] 根据各个共享子密钥的有效性校验信息和 (t, n) 门限方案，对各个共享子密钥进行有效性校验，如果存在 t 个及以上的有效共享子密钥，则根据这些有效子密钥恢复数字期刊内容的保护密钥，并利用该保护密钥对加密的数字期刊内容进行解密，否则密钥恢复失败。

[0082] 通过这种实施方式，硬件设备中一定范围内的硬件配置变更不会影响数字期刊的合法使用，生成的许可证文件仍可继续正常使用，而不需重新申请，大大方便了用户。

[0083] 此外，优选地，所形成的加密信息中还可包括其它信息，比如，加密算法信息等，即，将门限参数 t 的值、加密的共享子密钥及其有效性校验信息以及其它信息（比如，加密算法信息）形成一个加密信息。另外，在许可证文件中还可包括其它需要的信息，比如许可证文件完整性校验信息等。此时，客户端在接收到许可证文件之后，首先需要对许可证文件的完整性和有效性进行校验。

[0084] 从以上实施例可看出，根据本发明的订阅方法，订阅用户可以定期在其指定的多个客户端设备上接收到许可证文件，然后根据该许可证文件对加密的数字期刊内容进行解密，从而不仅避免了重放攻击的问题，而且还可实现对硬件设备的控制。此外，一个许可证可以在订阅用户的多个设备上使用，而不必分别生成和发送，而且在硬件设备中的部分硬件配置发生变更时，仍可正常使用许可证文件，从而大大方便了用户。另外，订阅用户可在已经注册的客户端上删除或增加设备，提高了数字期刊订阅的灵活性。

[0085] 以上参考附图和实施例详细描述了本发明。但是，本领域的技术人员应该理解，本发明并不限于所公开的具体实施例，任何本领域的普通技术人员在此基础之上能够想到的类似的修改、替换和变形都应包括在本发明的保护范围内。

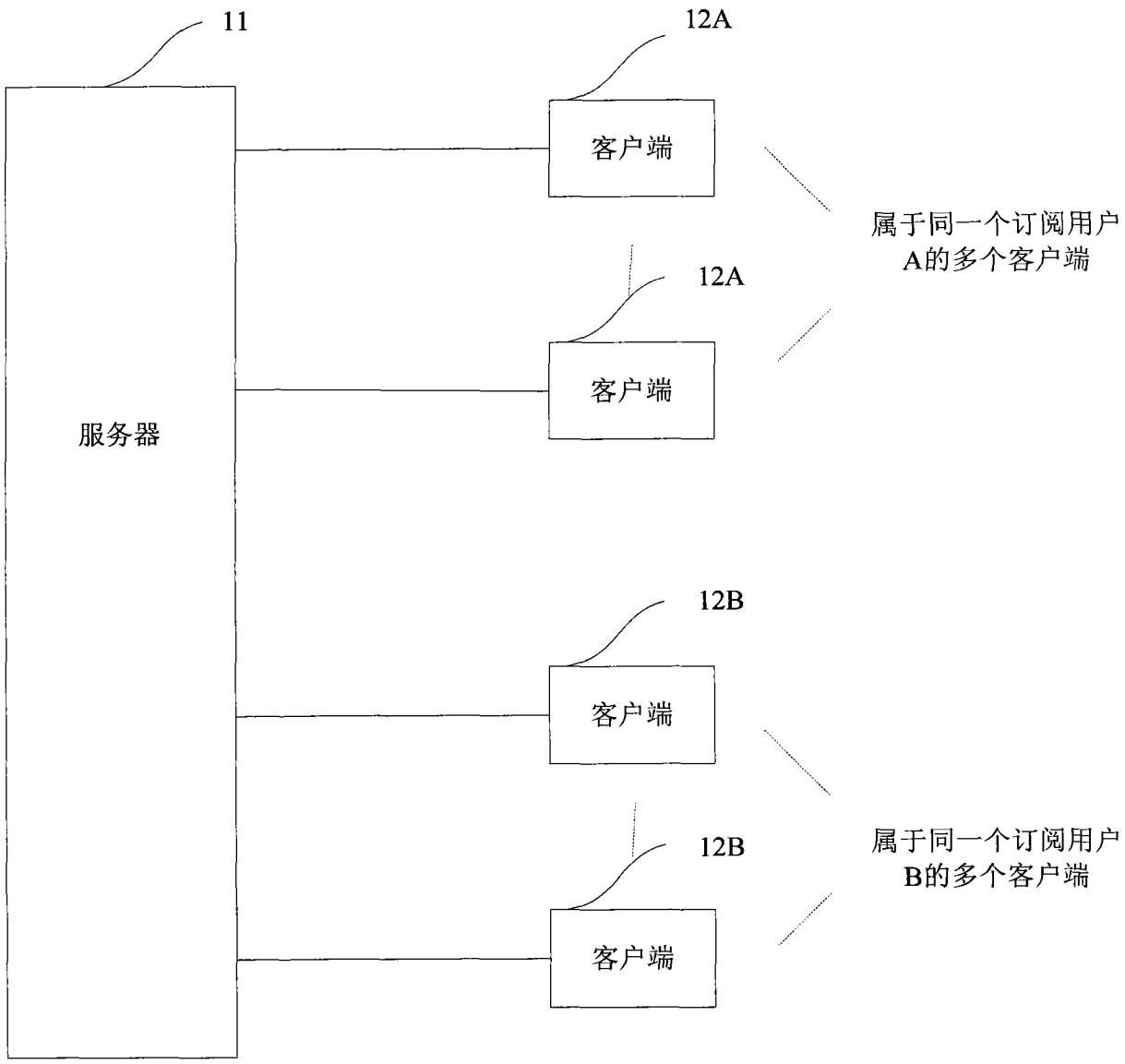

11
12A
客户端
12A
客户端
服务器
属于同一个订阅用户A的多个客户端
12B
客户端
12B
客户端
属于同一个订阅用户B的多个客户端

图 1

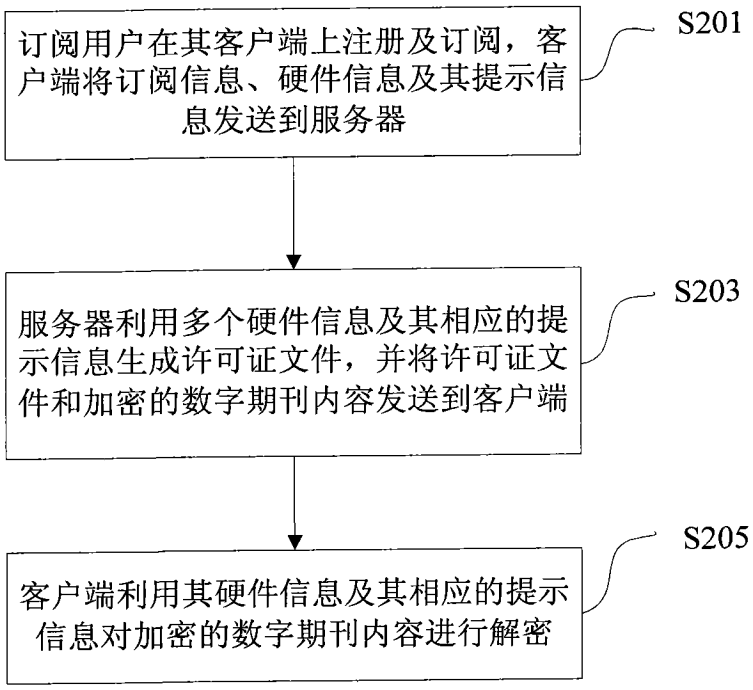

订阅用户在其客户端上注册及订阅，客户端将订阅信息、硬件信息及其提示信息发送到服务器
S201
服务器利用多个硬件信息及其相应的提示信息生成许可证文件，并将许可证文件和加密的数字期刊内容发送到客户端
S203
客户端利用其硬件信息及其相应的提示信息对加密的数字期刊内容进行解密
S205

图 2

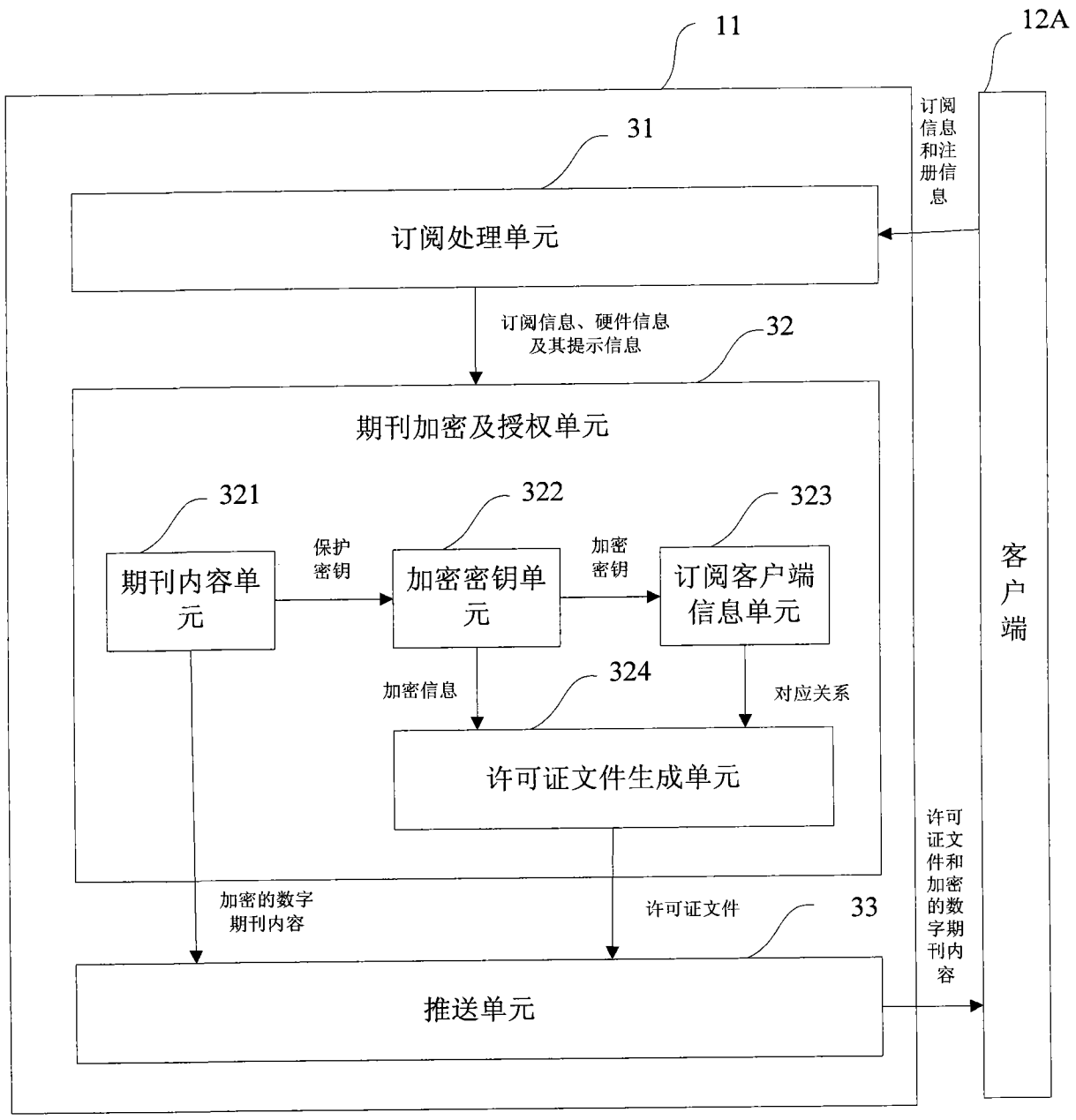

11
12A
31
订阅处理单元
订阅信息和注册信息
订阅信息、硬件信息及其提示信息
32
期刊加密及授权单元
321
期刊内容单元
保护密钥
322
加密密钥单元
加密密钥
323
订阅客户端信息单元
加密信息
324
对应关系
许可证文件生成单元
加密的数字期刊内容
许可证文件
33
推送单元
许可证文件和加密的数字期刊内容
客户端

图 3

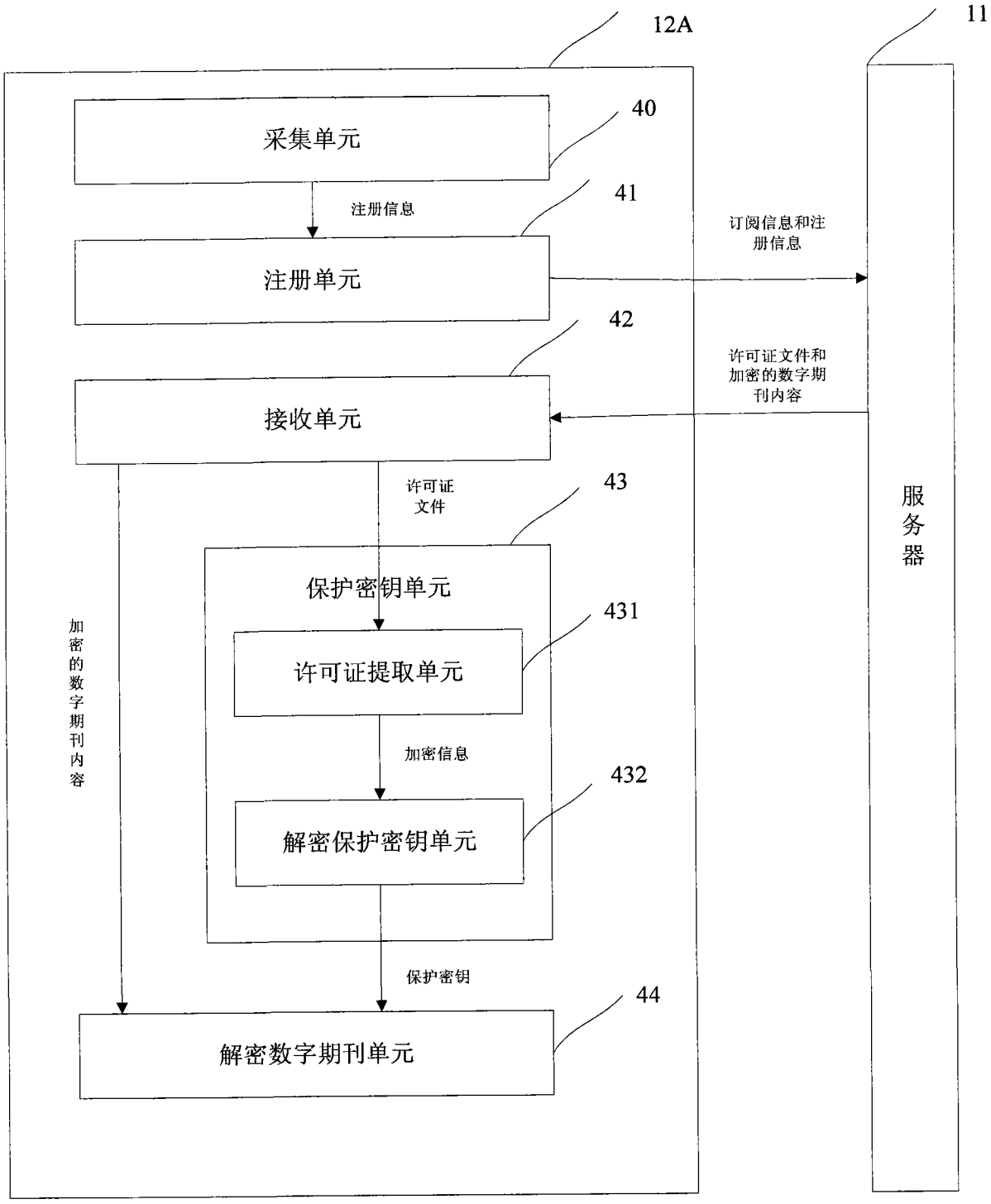

12A
11
采集单元
40
注册信息
41
注册单元
订阅信息和注册信息
42
许可证文件和加密的数字期刊内容
接收单元
许可证文件
43
保护密钥单元
431
许可证提取单元
加密信息
432
解密保护密钥单元
保护密钥
44
解密数字期刊单元
加密的数字期刊内容
服务器

图 4

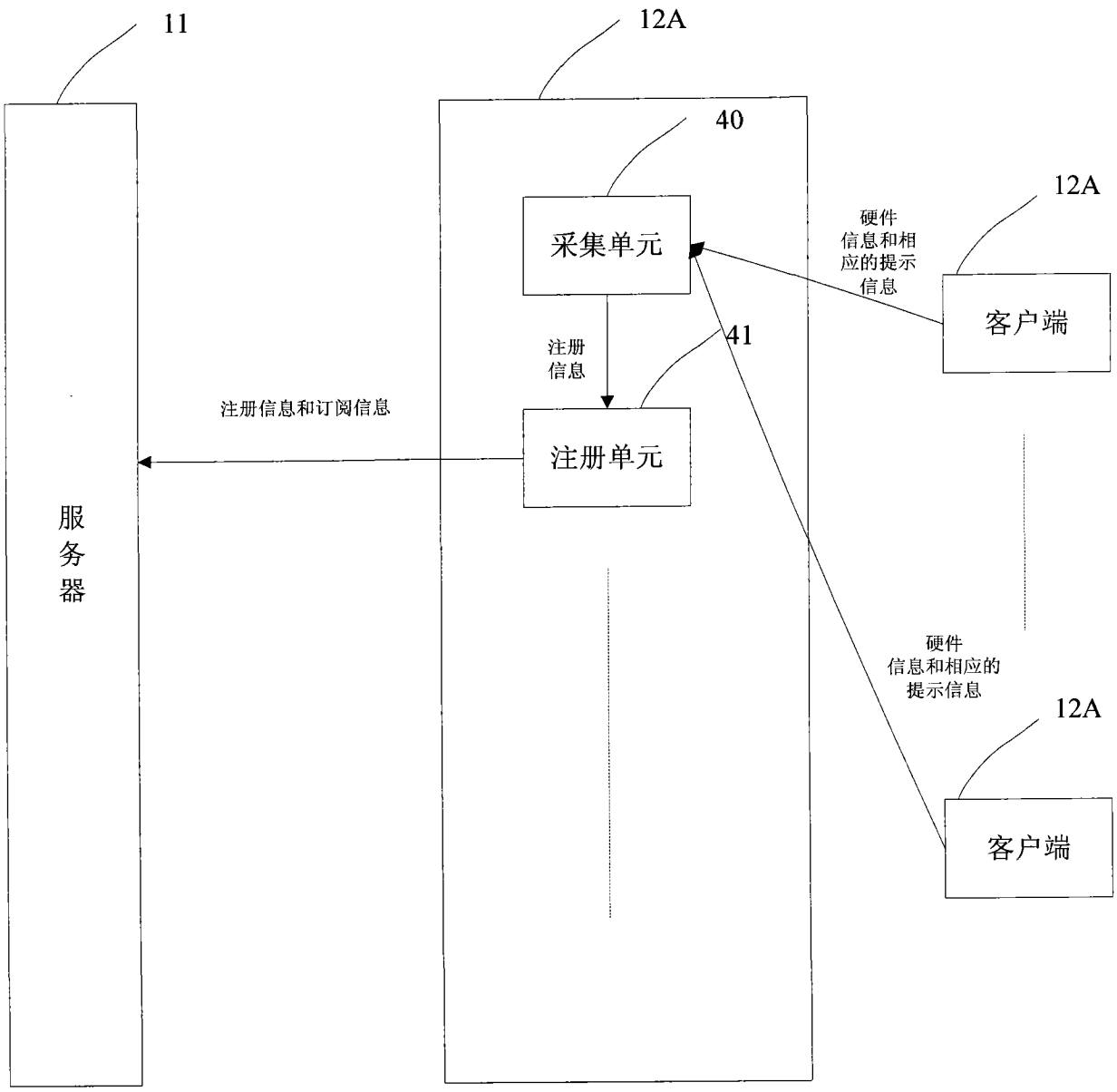

11
12A
40
采集单元
12A
硬件
信息和相
应的提示
信息
客户端
注册
信息
41
注册信息和订阅信息
注册单元
服
务
器
硬件
信息和相应的
提示信息
12A
客户端

图 5

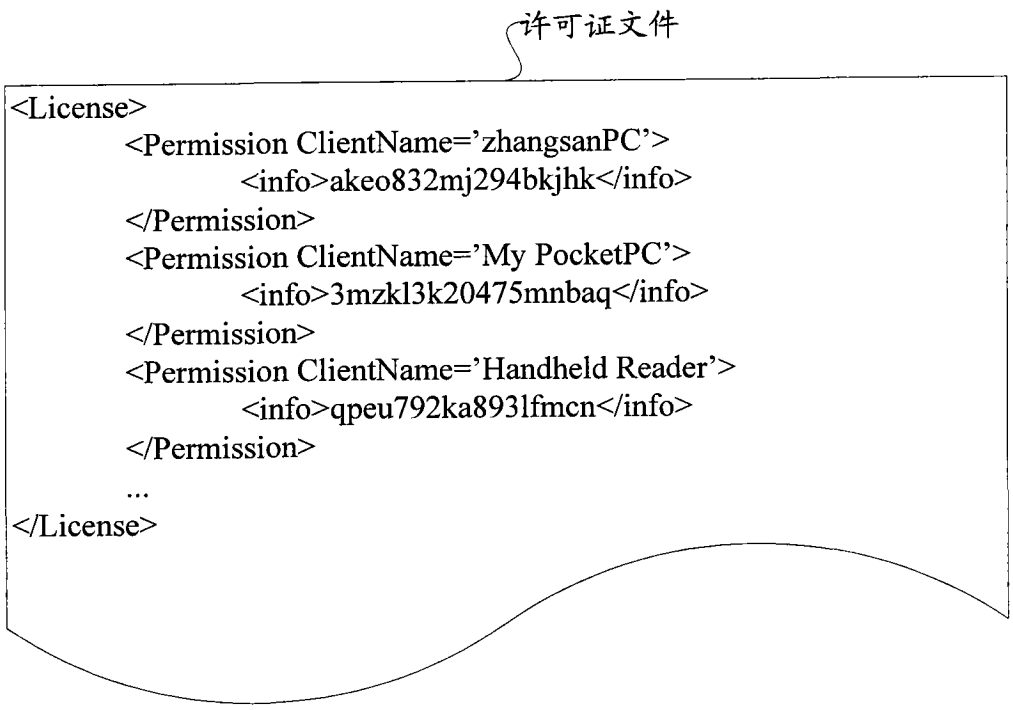

许可证文件
<License>
<Permission ClientName='zhangsanPC'>
<info>akeo832mj294bkjhk</info>
</Permission>
<Permission ClientName='My PocketPC'>
<info>3mzkl3k20475mnbaq</info>
</Permission>
<Permission ClientName='Handheld Reader'>
<info>qpeu792ka893lfmcn</info>
</Permission>
...
</License>

图 6