(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 101404573 B
(45)授权公告日 2014.11.19

(21)申请号 200810225208.8
(22)申请日 2008.10.27
(73)专利权人 北京大学
地址 100871 北京市海淀区颐和园路 5 号
专利权人 北大方正集团有限公司
北京方正阿帕比技术有限公司
(72)发明人 汤帜 高飞 洪献文
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
(56)对比文件
CN 101252432 A,2008.08.27,
CN 1530791 A,2004.09.22,

审查员 阎洁

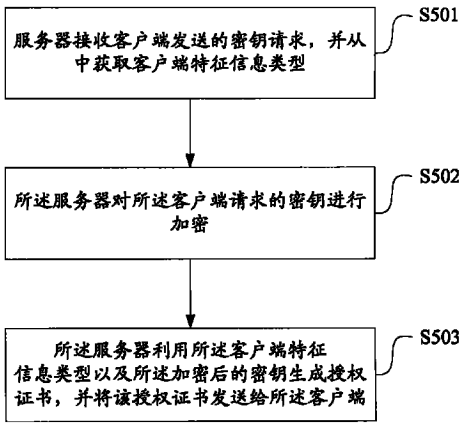
权利要求书4页 说明书9页 附图3页

(54)发明名称

一种授权方法、系统及装置

(57)摘要

本发明公开了一种授权方法、系统及装置，用以实现对客户端关于获取密钥的动态授权，并且使得更多的客户端获得用于访问相关内容的密钥，满足用户在多个客户端能够获得同一密钥的需求。本发明提供的一种授权方法包括：服务器接收客户端发送的密钥请求，并从中获取客户端特征信息类型；所述服务器对所述客户端请求的密钥进行加密；所述服务器利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端。本发明还提供了一种密钥获取方法及装置。



CN 101404573 B

1. 一种授权方法，其特征在于，该方法包括：

服务器接收一个客户端发送的密钥请求，并从中获取一个客户端特征信息，以及一个客户端特征信息类型；或者，服务器接收多个客户端发送的密钥请求，并从中获取每一客户端特征信息，以及每一客户端特征信息类型；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；

所述服务器利用所述客户端特征信息，或者利用所述客户端特征信息和所述客户端特征信息类型，对所述客户端请求的密钥进行加密；

所述服务器利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端；

其中，所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息。

2. 根据权利要求 1 所述的方法，其特征在于，当所述服务器接收到多个客户端请求的密钥相同时，所述服务器利用该多个客户端的客户端特征信息，或者利用该多个客户端特征信息和所述多个客户端发送的客户端特征信息类型对该多个客户端请求的同一密钥进行加密；

所述服务器利用所述多个客户端提交的客户端特征信息和客户端特征信息类型生成所述授权证书。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述服务器利用所述客户端特征信息和客户端特征信息类型对所述客户端请求的密钥进行加密的步骤包括：

所述服务器利用所述客户端特征信息和所述客户端特征信息类型生成加密密钥，采用该加密密钥对所述客户端请求的密钥进行加密。

4. 根据权利要求 1 所述的方法，其特征在于，所述服务器进一步从所述客户端发送的密钥请求中获取加密密钥，利用该加密密钥对所述客户端请求的密钥进行加密。

5. 根据权利要求 4 所述的方法，其特征在于，所述的加密密钥是利用客户端特征信息，或者利用该客户端特征信息和客户端特征信息类型生成的。

6. 根据权利要求 1 所述的方法，其特征在于，所述客户端请求的密钥为域密钥或数字内容的保护密钥。

7. 一种密钥获取方法，其特征在于，该方法包括：

服务器只有一个客户端时，该客户端从服务器下发的授权证书中获取一个客户端特征信息类型和经过加密的密钥；服务器有多个客户端时，所述多个客户端中每一个客户端从服务器下发的授权证书中获取所述多个客户端中每一个客户端的特征信息类型和经过加密的密钥；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；

所述客户端根据所述客户端特征信息类型提取客户端特征信息，并利用该客户端特征信息，或者利用该客户端特征信息和客户端特征信息类型对所述密钥解密，得到解密后的密钥；

其中，所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息。

8. 根据权利要求 7 所述的方法，其特征在于，所述客户端从所述授权证书中获取所述客户端特征信息类型和密钥之前，该方法还包括：

所述客户端根据用户请求按照预先设定的客户端特征信息类型的优先级选定客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息；

所述客户端将所述客户端特征信息以及所述选定的客户端特征信息类型发送给所述服务器。

9. 根据权利要求 8 所述的方法，其特征在于，所述客户端根据用户请求提取自身的设备类型，按照预先设定的设备类型与客户端特征信息类型的对应关系，获取自身设备类型所对应的备选的客户端特征信息类型；

所述客户端按照预先设定的客户端特征信息类型的优先级，从所述备选的客户端特征信息类型中选定客户端特征信息类型。

10. 根据权利要求 8 或 9 所述的方法，其特征在于，当所述客户端提取与所述选定的客户端特征信息类型相对应的客户端特征信息失败时，所述客户端根据所述客户端特征信息类型的优先级重新选定客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息。

11. 根据权利要求 7 所述的方法，其特征在于，所述客户端从所述授权证书中获取的客户端特征信息类型包括多种客户端特征信息类型；

所述客户端从所述多种客户端特征信息类型中选择一种客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，如果提取失败，则从所述多种客户端特征信息类型中选择另一种客户端特征信息类型，直到提取客户端特征信息成功。

12. 根据权利要求 11 所述的方法，其特征在于，所述客户端根据预先设置的客户端特征信息类型的优先级，从所述多种客户端特征信息类型中选择客户端特征信息类型。

13. 根据权利要求 7 所述的方法，其特征在于，所述客户端获取的密钥为域密钥或数字内容的保护密钥。

14. 一种服务器，其特征在于，该服务器包括：

接收请求单元，用于接收一个客户端发送的密钥请求，并从中获取一个客户端特征信息，以及一个客户端特征信息类型；或者，用于接收多个客户端发送的密钥请求，并从中获取每一客户端特征信息，以及每一客户端特征信息类型；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；所述由客户端按照预先

设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息；

加密单元，用于利用所述客户端特征信息，或者利用所述客户端特征信息和所述客户端特征信息类型，对所述客户端请求的密钥进行加密；

发送授权证书单元，用于利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端。

15. 一种客户端，其特征在于，该客户端包括：

授权证书单元，用于在服务器只有一个客户端时，从服务器下发的授权证书中获取一个客户端特征信息类型和经过加密的密钥；或者，用于在服务器有多个客户端时，从服务器下发的授权证书中获取所述多个客户端中每一个客户端的特征信息类型和经过加密的密钥；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息；

密钥获取单元，用于根据所述客户端特征信息类型提取客户端特征信息，并利用该客户端特征信息，或者利用该客户端特征信息和客户端特征信息类型对所述密钥解密，得到解密后的密钥。

16. 根据权利要求 15 所述的客户端，其特征在于，该客户端还包括：

信息提取单元，用于根据用户请求按照预先设定的客户端特征信息类型的优先级选定客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息；

加密密钥单元，用于利用所述客户端特征信息，或者利用所述客户端特征信息以及所述选定的客户端特征信息类型生成加密密钥；

发送单元，用于将所述选定的客户端特征信息类型，以及所述加密密钥或者所述客户端特征信息发送给所述服务器。

17. 一种授权系统，其特征在于，该系统包括：

服务器，用于接收一个客户端发送的密钥请求，并从中获取一个客户端特征信息，以及获取一个客户端特征信息类型；或者，用于接收多个客户端发送的密钥请求，并从中获取每一客户端特征信息，以及每一客户端特征信息类型；利用所述客户端特征信息，或者利用所述客户端特征信息和所述客户端特征信息类型，对所述客户端请求的密钥进行加密；利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类

型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息；

客户端，用于从所述服务器下发的授权证书中获取客户端特征信息类型和经过加密的密钥；通过客户端特征信息生成的密钥，或者通过该客户端特征信息和所述客户端特征信息类型生成的密钥对所述授权证书中的密钥解密，得到解密后的密钥。

18. 根据权利要求 17 所述的系统，其特征在于，所述客户端包括：

信息提取单元，用于按照预先设定的客户端特征信息类型的优先级选定客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息；

发送单元，用于将所述客户端特征信息以及所述选定的客户端特征信息类型发送给所述服务器；

授权证书单元，用于从服务器下发的授权证书中获取客户端特征信息类型和经过加密的密钥；

密钥获取单元，用于根据所述客户端特征信息类型提取客户端特征信息，并利用该客户端特征信息生成的密钥，或者通过该客户端特征信息和所述客户端特征信息类型生成的密钥对所述授权证书中的密钥解密，得到解密后的密钥。

19. 根据权利要求 17 或 18 所述的系统，其特征在于，所述服务器包括：

接收请求单元，用于接收客户端发送的密钥请求，并从中获取客户端特征信息和客户端特征信息类型；

加密单元，用于利用所述客户端特征信息，或者利用所述客户端特征信息和所述客户端特征信息类型，对所述客户端请求的密钥进行加密；

发送授权证书单元，用于利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端。

一种授权方法、系统及装置

技术领域

[0001] 本发明涉及数字版权保护技术领域，尤其涉及一种授权方法、系统及装置。

背景技术

[0002] 随着网络技术的发展和普及，音频、视频、图片、文档等数字内容的数量越来越多，使用也越来越广泛，数字内容的传播和共享变的更加方便和快捷。但是，由于数字内容具有易于复制和传播的特点，导致数字内容非法流通，使得利用大量成本和人力来制作的数字内容很容易在未经许可的情况下被非法复制和传播，从而损害了数字内容权利人的利益，影响数字内容创作者的积极性，从而阻碍数字内容行业的发展。

[0003] 为了有效防止数字内容的非法复制、传播和使用而出现的技术，称为数字版权管理 (DRM，Digital Rights Management) 技术。在 DRM 应用中，通常会通过将数字内容同客户端的特征信息相绑定来保证数字内容的下载使用的安全性。

[0004] 将数字内容与客户端绑定的方案有很多种，包括将数字内容与一个客户端、一个客户端中的一个或多个硬件相绑定等等。但是在实际应用中，一个 DRM 系统通常仅采用一种绑定方案。例如，应用于手机设备的 DRM 系统仅将数字内容与手机号相绑定，应用于 PC 设备的 DRM 系统仅将数字内容与 PC 硬盘的绑定。

[0005] 由此可见，现有对客户端授予访问数字内容的权利的技术存在以下两点不足 ：

[0006] 一、客户端的特征信息具有唯一性，从而可能导致 DRM 系统所限定的唯一的数字内容授权方式失效，从而造成客户端无法使用数字内容的问题。例如，某 DRM 系统是利用 PC 的硬盘序列号和网卡号绑定数字内容，然而并非所有 PC 设备的硬盘都能顺利读取到自身的序列号，如果 PC 设备没有网卡或者网卡号也无法获取，那么该 DRM 系统将不能应用于该 PC 设备上，造成用户无法使用需要的数字内容。

[0007] 二、随着数字内容应用的发展，用户往往需要一个 DRM 系统可以支持多种客户端的数字内容授权方案，然而现有技术中一个 DRM 系统仅能对一种客户端实现数字内容授权。例如，对于某电子书的 DRM 系统来说，用户购买该电子书后，用户可能希望既能够在 PC 设备上阅读电子书，又能够在手机上阅读该电子书，然而该电子书的 DRM 系统只能支持一种客户端设备的数字内容授权，无法同时支持 PC 设备和手机设备的数字内容授权。

[0008] 综上所述，现有实现对客户端关于获取用于访问相关内容的密钥的技术不够灵活，造成有些客户端无法获得用于访问相关内容的密钥，以及无法满足用户希望在多个客户端都能够获得用于访问相同内容的同一密钥的需求。

发明内容

[0009] 本发明实施例提供了一种授权方法、系统及装置，用以实现对客户端关于获取密钥的动态授权，并且使得更多的客户端获得用于访问相关内容的密钥，满足用户在多个客户端能够获得同一密钥的需求。

[0010] 本发明实施例提供的一种授权方法包括 ：

[0011] 服务器接收一个客户端发送的密钥请求，并从中获取一个客户端特征信息，以及一个客户端特征信息类型；或者，服务器接收多个客户端发送的密钥请求，并从中获取每一客户端特征信息，以及每一客户端特征信息类型；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；

[0012] 所述服务器利用所述客户端特征信息，或者利用所述客户端特征信息和所述客户端特征信息类型，对所述客户端请求的密钥进行加密；

[0013] 所述服务器利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端；

[0014] 其中，所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息。

[0015] 本发明实施例提供的一种密钥获取方法包括：

[0016] 服务器只有一个客户端时，该客户端从服务器下发的授权证书中获取一个客户端特征信息类型和经过加密的密钥；服务器有多个客户端时，所述多个客户端中每一个客户端从服务器下发的授权证书中获取所述多个客户端中每一个客户端的特征信息类型和经过加密的密钥；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；

[0017] 所述客户端根据所述客户端特征信息类型提取客户端特征信息，并利用该客户端特征信息，或者利用该客户端特征信息和客户端特征信息类型对所述密钥解密，得到解密后的密钥；

[0018] 其中，所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息。

[0019] 本发明实施例提供的一种服务器包括：

[0020] 接收请求单元，用于接收一个客户端发送的密钥请求，并从中获取一个客户端特征信息，以及一个客户端特征信息类型；或者，用于接收多个客户端发送的密钥请求，并从中获取每一客户端特征信息，以及每一客户端特征信息类型；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特

征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息；

[0021] 加密单元，用于利用所述客户端特征信息，或者利用所述客户端特征信息和所述客户端特征信息类型，对所述客户端请求的密钥进行加密；

[0022] 发送授权证书单元，用于利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端。

[0023] 本发明实施例提供的一种客户端包括：

[0024] 授权证书单元，用于在服务器只有一个客户端时，从服务器下发的授权证书中获取一个客户端特征信息类型和经过加密的密钥；或者，用于在服务器有多个客户端时，从服务器下发的授权证书中获取所述多个客户端中每一个客户端的特征信息类型和经过加密的密钥；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息；

[0025] 密钥获取单元，用于根据所述客户端特征信息类型提取客户端特征信息，并利用该客户端特征信息，或者利用该客户端特征信息和客户端特征信息类型对所述密钥解密，得到解密后的密钥。

[0026] 本发明实施例提供的一种授权系统包括：

[0027] 服务器，用于接收一个客户端发送的密钥请求，并从中获取一个客户端特征信息，以及一个客户端特征信息类型；或者，用于接收多个客户端发送的密钥请求，并从中获取一个或多个客户端特征信息，以及一个或多个客户端特征信息类型；利用所述客户端特征信息，或者利用所述客户端特征信息和所述客户端特征信息类型，对所述客户端请求的密钥进行加密；利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端；其中，所述客户端特征信息类型，是由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型；所述由客户端按照预先设定的客户端特征信息类型的优先级，从与用户请求的客户端的设备类型相对应的客户端特征信息类型中选定的客户端特征信息类型，包括：客户端按照预先设定的客户端特征信息类型的优先级，首先选择优先级高的客户端特征信息类型，并根据该客户端特征信息类型提取对应的客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到成功提取到客户端特性信息；

[0028] 客户端，用于从所述服务器下发的授权证书中获取客户端特征信息类型和经过加

密的密钥；通过客户端特征信息生成的密钥，或者通过该客户端特征信息和所述客户端特征信息类型生成的密钥对所述授权证书中的密钥解密，得到解密后的密钥。

[0029] 本发明实施例，通过服务器接收客户端发送的密钥请求，并从中获取客户端特征信息类型；所述服务器对所述客户端请求的密钥进行加密；所述服务器利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端，从而实现了服务器对客户端关于获取密钥的动态授权，使得更多的客户端能够获得用于访问相关内容的密钥，并且能够满足用户在多个客户端获得用于访问相同内容的同一密钥的需求。

附图说明

[0030] 图 1 为本发明实施例提供的一种授权系统的结构示意图；

[0031] 图 2 为本发明实施例提供的一种服务器的结构示意图；

[0032] 图 3 为本发明实施例提供的一种客户端的结构示意图；

[0033] 图 4 为本发明实施例提供的授权证书中的利用三种客户端特征信息生成的用于加密数字内容的保护密钥的密钥的示意图；

[0034] 图 5 为本发明实施例提供的一种授权方法的流程示意图；

[0035] 图 6 为本发明实施例提供的一种密钥获取方法的流程示意图。

具体实施方式

[0036] 本发明实施例提供了一种授权方法、系统及装置，用以实现对客户端关于获取密钥的动态授权，并且使得更多的客户端获得用于访问相关内容的密钥，满足用户在多个客户端能够获得同一密钥的需求。

[0037] 本发明实施例所述的客户端请求的用于访问相关内容的密钥可以为各种密钥，例如域密钥、数字内容（如电子书等）的保护密钥。

[0038] 本发明实施例预先在客户端设置客户端特征信息类型和客户端特征信息的对应关系，例如，客户端特征信息类型为硬盘，则对应的客户端特征信息为硬盘的序列号。进一步还可以设置客户端设备类型和客户端特征信息类型的对应关系，使得客户端通过检测得知自身的设备类型后，可以找到相应的客户端特征信息类型，从而根据该客户端特征信息类型提取相应的客户端特征信息。如果某一客户端的设备类型对应多个客户端特征信息类型，则按照预先设定的客户端特征信息类型的优先级选定一种客户端特征信息类型。所述的客户端特征信息就是用于标识该客户端的特征信息。当然，进一步还可以在服务器中预先设置上述对应关系。

[0039] 下面结合附图对本发明实施例进行详细说明。

[0040] 参见图 1，本发明实施例提供的一种授权系统包括：服务器 11 和至少一个客户端 12。

[0041] 服务器 11，用于接收客户端 12 发送的密钥请求，并从中获取客户端特征信息类型；对所述客户端 12 请求的密钥进行加密；利用该客户端特征信息类型以及加密后的密钥生成授权证书，并将该授权证书发送给所述客户端 12。

[0042] 客户端 12，用于根据用户请求从所述服务器 11 下发的授权证书中获取客户端特

征信息类型和经过加密的密钥；通过客户端特征信息生成的密钥，或者通过该客户端特征信息和所述客户端特征信息类型生成的密钥对所述授权证书中的密钥解密，得到解密后的密钥。

[0043] 较佳地，所述服务器 11 进一步从所述客户端 12 发送的密钥请求中获取客户端特征信息，利用该客户端特征信息和 / 或所述客户端特征信息类型对所述客户端 12 请求的密钥进行加密。当所述服务器 11 接收到多个客户端 12 请求的密钥相同时，所述服务器 11 利用该多个客户端 12 的客户端特征信息和 / 或所述客户端特征信息类型对该多个客户端 12 请求的同一密钥进行加密；利用所述多个客户端 12 提交的客户端特征信息和客户端特征信息类型生成授权证书。

[0044] 较佳地，所述服务器 11 采用一定算法（如消息摘要算法等）对客户端特征信息处理后生成加密密钥；或者，采用一定算法对客户端特征信息和客户端特征信息类型进行处理后生成加密密钥；

[0045] 所述服务器 11 采用加密密钥对所述客户端 12 请求的密钥进行加密。

[0046] 较佳地，所述服务器 11 进一步从所述客户端 12 发送的密钥请求中获取加密密钥，利用该加密密钥对所述客户端 12 请求的密钥进行加密。也就是说，所述客户端 12 采用一定算法对客户端特征信息处理后生成加密密钥；或者，采用一定算法对客户端特征信息和客户端特征信息类型进行处理后生成加密密钥，将生成的加密密钥发送给服务器 11。

[0047] 较佳地，客户端 12，根据用户请求按照预先设定的客户端特征信息类型的优先级选定客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息；将该客户端特征信息以及选定的客户端特征信息类型发送给服务器 11。

[0048] 较佳地，服务器 11 利用多个客户端 12 的客户端特征信息采用完全公钥广播加密等算法对同一数字内容的保护密钥进行加密，使得其中任一客户端 12 可以利用自身的客户端特征信息对从授权证书中获取的密钥进行解密；服务器 11 利用加密后的密钥，以及多个客户端 12 提交的客户端特征信息类型生成授权证书，也就是说，授权证书中包括了加密后的密钥以及请求同一密钥的所有客户端提交的客户端特征信息类型。

[0049] 较佳地，客户端 12 选定客户端特征信息类型之前，先提取自身的设备类型，获取自身设备类型所对应的客户端特征信息类型，在自身设备类型对应多个客户端特征信息类型的情况下，按照预先设定的客户端特征信息类型的优先级选定一种客户端特征信息类型，并根据该客户端特征信息类型提取客户端特征信息，如果提取失败，则根据客户端特征信息类型的优先级选定次优的客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息，直到提取客户端特征信息的操作成功。

[0050] 较佳地，客户端 12 从授权证书中获取的客户端特征信息类型包括多种客户端特征信息类型；从该多种客户端特征信息类型中选择一种客户端特征信息类型，并从自身提取与该客户端特征信息类型相对应的客户端特征信息，如果提取失败，则从多种客户端特征信息类型中选择另一种客户端特征信息类型，直到提取客户端特征信息成功。其中，在从授权证书中的多种客户端特征信息类型中选择一种客户端特征信息类型时，可以根据预先设置的客户端特征信息类型的优先级进行选择。

[0051] 下面给出上述服务器 11 和客户端 12 的具体结构说明。

[0052] 参见图 2，较佳地，所述服务器 11 包括：

[0053] 接收请求单元 21，用于接收客户端 12 发送的密钥请求，并从中获取客户端特征信息和客户端特征信息类型。

[0054] 加密单元 22，用于利用客户端特征信息对客户端 12 请求的密钥进行加密。

[0055] 发送授权证书单元 23，用于利用客户端特征信息类型以及加密后的密钥生成授权证书，并将该授权证书发送给客户端 12。

[0056] 参见图 3，较佳地，所述客户端 12 包括：

[0057] 信息提取单元 31，用于根据用户请求按照预先设定的客户端特征信息类型的优先级选定客户端特征信息类型，并提取与该客户端特征信息类型相对应的客户端特征信息。

[0058] 加密密钥单元 32，用于利用所述客户端特征信息，或者利用所述客户端特征信息以及所述选定的客户端特征信息类型生成加密密钥。

[0059] 发送单元 33，用于将所述选定的客户端特征信息类型，以及所述加密密钥或者所述客户端特征信息发送给所述服务器 11。

[0060] 授权证书单元 34，用于根据用户请求从服务器 11 下发的授权证书中获取客户端特征信息类型和经过加密的密钥。

[0061] 密钥获取单元 35，用于根据客户端特征信息类型提取客户端特征信息，并利用该客户端特征信息对所述密钥解密，得到解密后的密钥。

[0062] 下面给出几个具体的实施例。

[0063] 实施例 1：

[0064] 某电子阅读器厂商需要在一批没有扩展存储卡的阅读器中预置受 DRM 保护的数字内容。首先在通用阅读器客户端和授权服务器中预置多项授权方案。优先级较高的授权方案是：将电子阅读器的设备号和可扩展存储卡的卡号同时与数字内容绑定，优先级较低的授权方案是：将数字内容仅同设备号绑定。授权服务器根据该批客户端的特征信息对数字内容的保护密钥进行加密；随后在授权证书中描述该批客户端的特征信息的类型和加密后的内容密钥。该授权证书即可供该批电子阅读器使用。

[0065] 实施例 2：

[0066] 预先在一授权服务器上和多个 PC 设备上设置具有不同优先级的设备特征信息类型及其对应的设备特征信息，使得某个电子书 DRM 保护系统可以支持这些特殊的 PC 设备。由于在 PC 机上，通常供绑定的硬件，如显卡、网卡等设备都有可能不存在，硬盘序列号也可能检测不出来，因此需要针对这些特点在客户端软件上预置多套具备优先级的特征信息提取方案。如优先提取硬盘、网卡、显卡，其次提取主板、CPU、内存，再其次，利用能提取到的上述 6 种设备号，应用诸如“硬件适应性方法”进行绑定。例如，当某用户 PC 不含网卡时，用户通过该 PC 购买电子书。在获得 RO 凭证之后，客户端通过检测设备类型得知设备为 PC，根据预置方案得知 PC 设备对应的客户端特征信息类型，并选取优先级较高的客户端特征信息类型（如为硬盘、网卡、显卡），并检测获取相应的客户端特征信息，此次获取失败，则选取 PC 设备对应的优先级次优的客户端特征信息类型（如为主板、CPU、内存），并检测获取相应的客户端特征信息，此次获取成功。将该客户端特征信息和特征信息类型的摘要值、客户端特征信息类型（如标识为：PC 硬件绑定类型 2），同 RO 凭证一起发送给 RO 授权服务器。RO 服务器在判断 RO 凭证有效后，使用客户端特征信息和特征信息类型作为参数，通过生成密钥的算法（如消息摘要算法）计算出加密密钥 K1，并用该加密密钥 K1 对数字内容的

保护密钥 Kc 进行加密，生成 K2。再在授权证书中描述客户端特征信息类型和利用 K1 加密后的保护密钥 K2，如下所示：

[0067] <bindtype>PC 硬件绑定类型 2</bindtype>

[0068] <ECK>K2</ECK>

[0069] RO 服务器将该授权证书返回给客户端。客户端获得该授权证书后，将其保存。当用户准备使用电子书时，客户端检测到该授权证书，并获取到相应的客户端特征信息类型以及利用客户端特征信息加密后的保护密钥；客户端根据客户端特征信息类型获取相应的客户端特征信息，使用客户端特征信息生成解密密钥，并对保护密钥 K2 进行解密得到 Kc。再利用 Kc 解密电子书，从而使得用户可以阅读电子书。

[0070] 实施例 3：

[0071] 某个电子书 DRM 保护系统除了支持 PC 设备以外还支持手机时，客户端在获得了服务器下发的 RO 凭证之后，通过检测设备类型得知自身设备为手机，并根据预定方案得知手机对应的客户端特征信息类型，并检测获取相应的客户端特征信息（如为 SIM 卡号、手机设备号等），将其同 RO 凭证一起发送给 RO 授权服务器。RO 授权服务器在判断 RO 凭证的有效性后，将根据客户端特征信息对数字内容的保护密钥进行加密处理后，连同客户端特征信息类型一起，添加到生成的授权证书中，并将该授权证书返回给该手机。该手机获得了授权证书后，将其保存。当用户准备使用电子书时，该手机检测到该授权证书，并获取到客户端特征信息类型以及经客户端特征信息加密后的保护密钥；手机根据客户端特征信息类型获取相应的客户端特征信息，使用客户端特征信息对保护密钥进行解密；再利用解密后的保护密钥解密电子书，从而得到用户需要的电子书内容。

[0072] 实施例 4：

[0073] 当用户希望在 2 台 PC 和一台手机上都能阅读同一电子书时。在第一个 PC 上，客户端通过检测设备类型得知设备为 PC，根据预置方案得知优先需要获取的客户端特征信息类型（如为硬盘、网卡），并检测获取相应的客户端特征信息，获取成功，将客户端特征信息、客户端特征信息类型发送给授权服务器；在第二个 PC 上，客户端通过检测设备类型得知设备为 PC，根据预置方案得知优先需要获取的客户端特征信息类型（如为硬盘、网卡），并检测获取相应的客户端特征信息，获取失败，于是再在 PC 对应的预置方案中查找次优的客户端特征信息类型（如为主板、CPU、内存），并检测获取相应的客户端特征信息，获取成功。将该客户端特征信息、客户端特征信息类型发送给授权服务器。在手机上，客户端通过检测设备类型得知设备为手机，根据预置方案得知优先需要获取的客户端特征信息（如为手机设备 ID），并检测获取相应的客户端特征信息，获取成功，将客户端特征信息、客户端特征信息类型发送给授权服务器。授权服务器在获取到这 3 台设备的客户端特征信息及客户端特征信息类型后，用三者的客户端特征信息加密电子书的保护密钥，然后将这三个客户端提交的客户端特征信息类型、加密后的保护密钥分别描述在授权证书中，如图 4 所示，授权服务器将该授权证书传送给用户的这三个客户端设备，从而使得用户可以在这三个设备上通过该授权证书阅读同一电子书。

[0074] 在第一个 PC 上，客户端通过依次检测授权证书上客户端特征信息类型，得知 PC 对应的最优选的客户端特征信息类型为硬盘、网卡，随即获取相应的客户端特征信息，获取成功；使用该客户端特征信息解密得到电子书的保护密钥。

[0075] 在第二个PC上，客户端通过依次检测授权证书上客户端特征信息类型，得知PC对应的最优选的客户端特征信息类型为硬盘、网卡，随即获取相应的客户端特征信息，获取失败；检测PC对应的下一个优选的客户端特征信息类型为主板、CPU、内存，随即获取相应的客户端特征信息，获取成功；使用该客户端特征信息解密得到电子书的保护密钥。

[0076] 在手机上，客户端通过依次检测授权证书上客户端特征信息类型，得知手机对应的最优选的客户端特征信息类型为设备ID，随即获取相应的客户端特征信息，获取成功；使用该客户端特征信息解密得到电子书的保护密钥。

[0077] 显而易见，本发明实施例提供的技术方案还可以应用在其他领域。例如，在域管理过程中，通常需要将域证书同设备绑定。一个域证书需要与特殊的PC设备绑定时，客户端通过检测设备类型得知设备为PC，根据预置方案得知PC对应的最优选的客户端特征信息类型（如为硬盘、网卡），并检测获取相应的客户端特征信息，获取失败，于是选取PC对应的次优选的客户端特征信息类型（如为主板、CPU、内存），并获取相应的客户端特征信息，获取成功。将该客户端特征信息、客户端特征信息类型发送给域管理服务器。域管理服务器使用客户端发送的客户端特征信息对域密钥进行加密；在域证书中描述客户端特征信息类型和利用客户端特征信息加密后的域密钥，如下所示：

[0078] <bindtype>PC硬件适应性绑定</bindtype>

[0079] <EDK>XXX</EDK>

[0080] 域管理服务器将该域证书返回给客户端。客户端获得域证书后，将其保存。当用户需要使用该域证书时，客户端获取该域证书中的客户端特征信息类型以及利用客户端特征信息加密后的域密钥；客户端根据客户端特征信息类型获取相应的客户端特征信息，使用该客户端特征信息对域密钥进行解密。

[0081] 下面介绍一下本发明实施例提供的方法。

[0082] 参见图5，本发明实施例提供的一种授权方法包括步骤：

[0083] S501、服务器接收客户端发送的密钥请求，并从中获取客户端特征信息类型。

[0084] S502、服务器对客户端请求的密钥进行加密。

[0085] S503、服务器利用客户端特征信息类型以及加密后的密钥生成授权证书，并将该授权证书发送给客户端。

[0086] 参见图6，本发明实施例提供的一种密钥获取方法包括步骤：

[0087] S601、客户端根据用户请求从服务器下发的授权证书中获取客户端特征信息类型和经过加密的密钥。

[0088] S602、客户端根据客户端特征信息类型提取客户端特征信息，并利用该客户端特征信息对密钥解密，得到解密后的用于访问相关内容的密钥。

[0089] 综上所述，本发明实施例通过服务器接收客户端发送的密钥请求，并从中获取客户端特征信息类型；服务器对客户端请求的密钥进行加密；服务器利用客户端特征信息类型以及加密后的密钥生成授权证书，并将该授权证书发送给客户端，从而实现了服务器对客户端关于获取密钥的动态授权，使得更多的客户端能够获得用于访问相关内容的密钥，并且能够满足用户在多个客户端获得用于访问相同内容的同一密钥的需求。

[0090] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围

之内，则本发明也意图包含这些改动和变型在内。

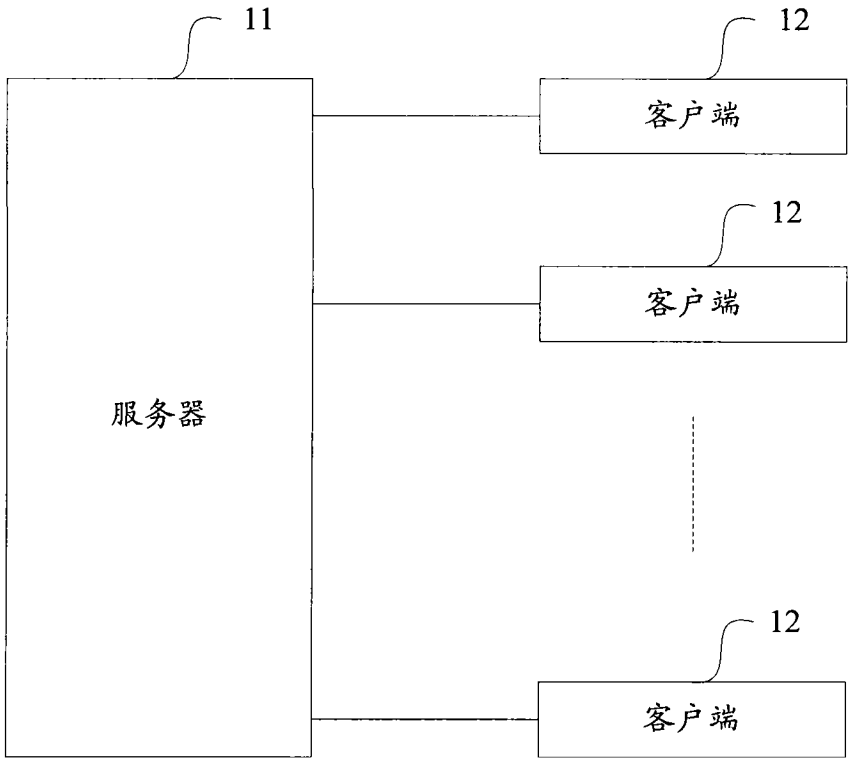

11
12
客户端
12
客户端
服务器
12
客户端

图 1

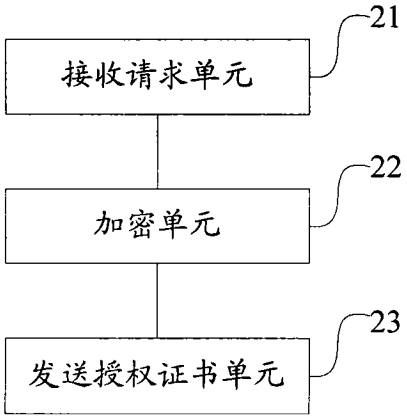

21
接收请求单元
22
加密单元
23
发送授权证书单元

图 2

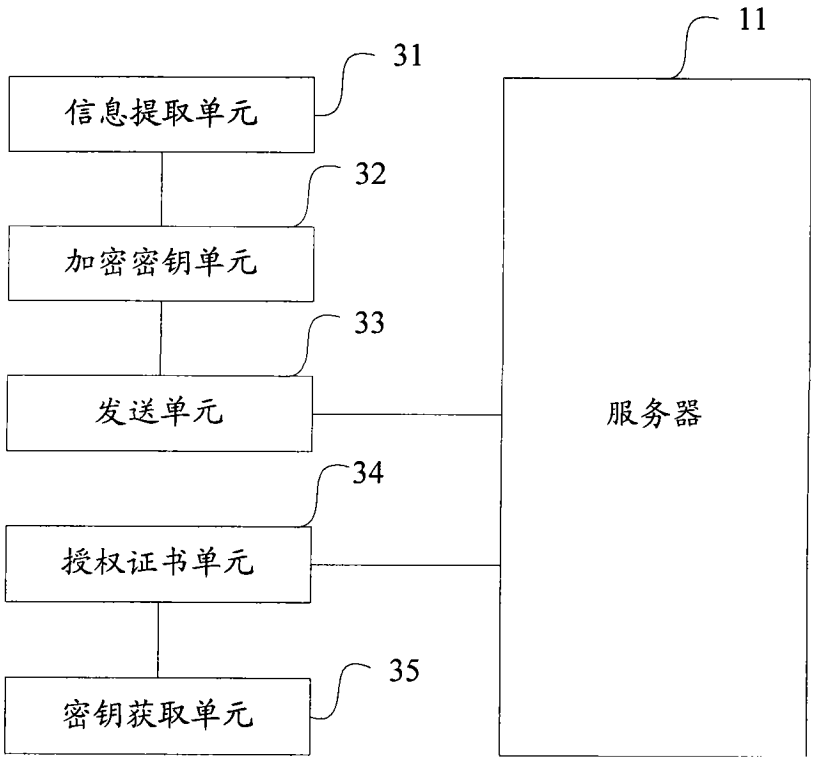

11
31
信息提取单元
32
加密密钥单元
33
发送单元
服务器
34
授权证书单元
35
密钥获取单元

图 3

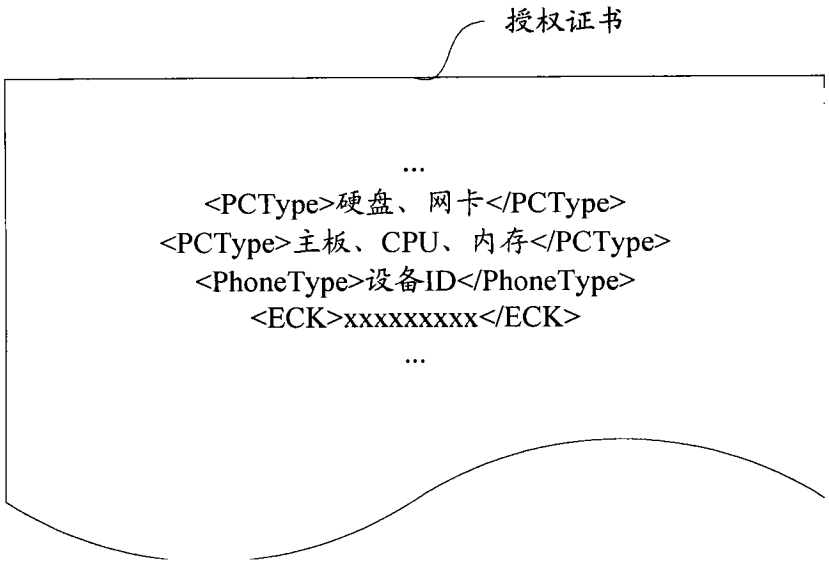

授权证书
...
<PCType>硬盘、网卡</PCType>
<PCType>主板、CPU、内存</PCType>
<PhoneType>设备ID</PhoneType>
<ECK>xxxxxxxxx</ECK>
...

图 4

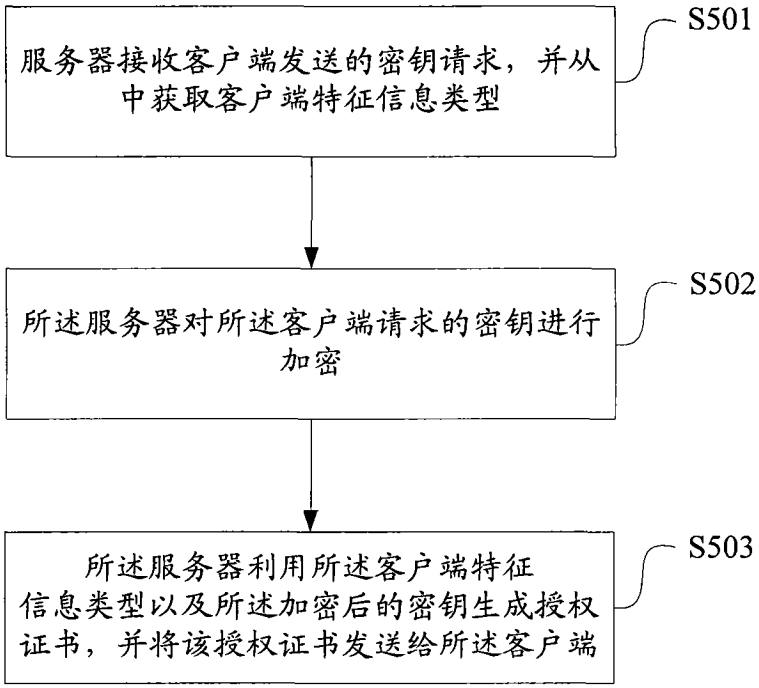

服务器接收客户端发送的密钥请求，并从中获取客户端特征信息类型
S501
所述服务器对所述客户端请求的密钥进行加密
S502
所述服务器利用所述客户端特征信息类型以及所述加密后的密钥生成授权证书，并将该授权证书发送给所述客户端
S503

图 5

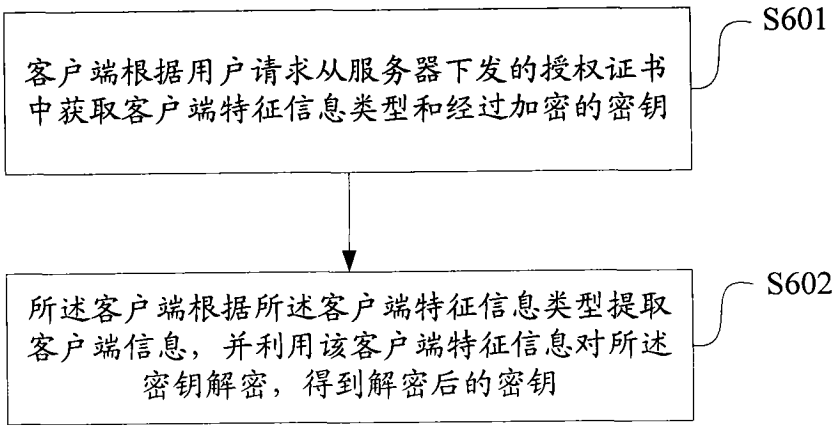

客户端根据用户请求从服务器下发的授权证书中获取客户端特征信息类型和经过加密的密钥
S601
所述客户端根据所述客户端特征信息类型提取客户端信息，并利用该客户端特征信息对所述密钥解密，得到解密后的密钥
S602

图 6