(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103186723 A
(43)申请公布日 2013.07.03

(21)申请号 201110457870.8

(22)申请日 2011.12.30

(71)申请人 北京大学
地址 100871 北京市海淀区颐和园路 5 号
申请人 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 邱勤 汤帜 俞银燕

(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 孔凡红

(51)Int.Cl.
G06F 21/10(2013.01)

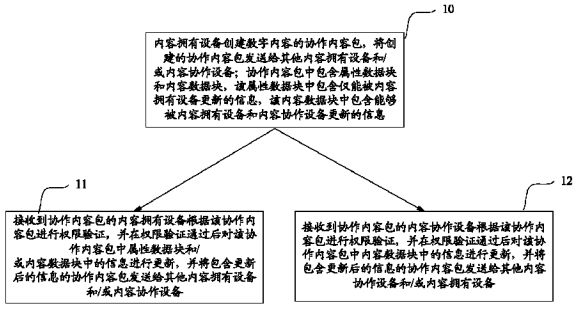
权利要求书3页 说明书16页 附图4页

(54)发明名称

数字内容安全协作的方法和系统

(57)摘要

本发明实施例公开了一种数字内容安全协作的方法和系统，涉及数字内容安全技术领域，用于提高在内容协作过程中数字内容的安全性。本发明中，内容拥有设备创建的协作内容包中包含仅能被内容拥有设备更新的属性数据块以及能够被内容拥有设备和内容协作设备更新的内容数据块；内容拥有设备在进行权限验证后，对属性数据块和/或内容数据块中的信息进行更新，内容协作设备在进行权限验证后，仅能对内容数据块中的信息进行更新。采用本发明，提高了数字内容的安全性。



CN 103186723 A

1. 一种数字内容安全协作的方法，其特征在于，该方法包括：

内容拥有设备创建数字内容的协作内容包，将创建的协作内容包发送给其他内容拥有设备和/或内容协作设备；所述协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息；

接收到协作内容包的内容拥有设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和/或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和/或内容协作设备；

接收到协作内容包的内容协作设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容协作设备和/或内容拥有设备。

2. 如权利要求1所述的方法，其特征在于，所述属性数据块中包含所述数字内容的属性信息和属性签名，所述内容数据块中包含内容密文、该协作内容包的封装信息和内容包签名；所述属性签名是所述属性信息的数字签名；所述内容密文是使用内容密钥加密所述数字内容生成的密文；所述内容包签名是所述内容密文、所述封装信息与所述属性信息的数字签名，或者是所述内容密文、所述封装信息与所述属性签名的数字签名。

3. 如权利要求2所述的方法，其特征在于，所述接收到协作内容包的内容拥有设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和/或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和/或内容协作设备，具体包括：

接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后对该协作内容包中的属性信息、封装信息、属性签名和内容包签名进行更新，并将包含更新后的属性信息、封装信息、属性签名和内容包签名、以及更新前的内容密文的协作内容包，发送给其他内容拥有设备和/或内容协作设备；或者，

接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后使用所述内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；并对该协作内容包中的封装信息和内容包签名进行更新，将包含更新后的内容密文、封装信息和内容包签名、以及更新前的属性信息和属性签名的协作内容包，发送给其他内容拥有设备和/或内容协作设备；或者，

接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后对该协作内容包中的属性信息进行更新；使用所述内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；并对该协作内容包中的封装信息、属性签名和内容包签名进行更新，将包含更新后的属性信息、属性签名、内容密文、封装信息和内容包签名的协作内容包，发送给其他内容拥有设备和/或内容协作设备。

4. 如权利要求3所述的方法，其特征在于，所述接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，具体包括：

接收到协作内容包的内容拥有设备使用私钥对该协作内容包中的属性信息进行签名，

并将该签名与该协作内容包中的属性签名进行对比，以实现对属性签名的验证；

接收到协作内容包的内容拥有设备根据该协作内容包中的封装信息，确定封装该协作内容包的设备，并使用该设备对应的公钥和该协作内容包中的内容密文、封装信息、以及属性信息或属性签名，对该协作内容包中的内容包签名进行验证。

5. 如权利要求 2 所述的方法，其特征在于，在内容拥有设备创建数字内容的协作内容包之后，进一步包括：

创建协作内容包的内容拥有设备自身或通过可信第三方，将创建的协作内容包的协作许可证签发给内容协作设备；所述协作许可证中包含授权信息和授权签名；该授权信息包含该协作内容包中的属性信息和内容密钥密文；该内容密钥密文是使用被绑定硬件保存或生成的密钥加密所述内容密钥生成的密文；该授权签名是内容拥有设备对该授权信息的数字签名。

6. 如权利要求 5 所述的方法，其特征在于，所述接收到协作内容包的内容协作设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容协作设备和 / 或内容拥有设备，具体包括：

接收到协作内容包的内容协作设备对所述协作许可证中的授权签名以及该协作内容包中的属性签名和内容包签名进行验证，在验证通过后，确定所述协作许可证中的属性信息与该协作内容包中的属性信息是否一致，在确定为是时：

获取所述被绑定硬件保存或生成的密钥，使用该密钥对所述协作许可证中的内容密钥密文进行解密，使用解密得到的内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；对该协作内容包中的封装信息和内容包签名进行更新，将包含更新后的内容密文、内容包签名和封装信息、以及更新前的属性信息和属性签名的协作内容包，发送给其他内容协作设备和 / 或内容拥有设备。

7. 如权利要求 6 所述的方法，其特征在于，所述接收到协作内容包的内容协作设备对所述协作许可证中的授权签名以及该协作内容包中的属性签名和内容包签名进行验证，具体包括：

接收到协作内容包的内容协作设备根据签发所述协作许可证的设备的公钥和协作许可证中的授权信息，对所述协作许可证中的授权签名进行验证；

接收到协作内容包的内容协作设备根据该协作内容包中的封装信息，确定封装该协作内容包的设备，并使用该设备对应的公钥和协作内容包中的内容密文、封装信息、以及属性信息或属性签名对该协作内容包中的内容包签名进行验证；还根据该协作内容包中的属性信息确定内容拥有设备，并使用确定的内容拥有设备对应的公钥和协作内容包中的属性信息对该协作内容包中的属性签名进行验证。

8. 如权利要求 6 所述的方法，其特征在于，生成所述内容密钥密文时使用的密钥为所述被绑定硬件保存或生成的公钥时，内容协作设备对所述协作许可证中的内容密钥密文进行解密时使用的密钥为所述被绑定硬件保存或生成的私钥；或者，

生成所述内容密钥密文时使用的密钥为所述被绑定硬件保存或生成的对称密钥时，内容协作设备对所述协作许可证中的内容密钥密文进行解密时使用的密钥为该对称密钥。

9. 如权利要求 5 所述的方法，其特征在于，所述授权信息还包含权利信息，该权利信息是用于申明内容协作设备能够对协作内容包进行的处理操作的信息。

10. 如权利要求 5 所述的方法，其特征在于，所述被绑定硬件是位于指定区域内的硬件或属于被授权的内容协作设备的硬件。

11. 如权利要求 2 所述的方法，其特征在于，进一步包括：

创建协作内容包的内容拥有设备接收到内容协作设备或其他内容拥有设备发来的协作内容包后，对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后使用所述内容密钥对该协作内容包中的内容密文进行解密，在用户对解密得到的内容明文进行审核确认后，根据审核确认后的内容明文创建用于正式发布的数字内容包。

12. 如权利要求 2-11 中任一所述的方法，其特征在于，所述属性信息包括：所述数字内容的内容标识和内容拥有设备标识；

所述封装信息包括：封装者标识和封装时间信息。

13. 一种数字内容安全协作的系统，其特征在于，该系统包括：

内容拥有设备，用于创建数字内容的协作内容包，将创建的协作内容包发送给其他内容拥有设备和 / 或内容协作设备；所述协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息；以及，

在接收到协作内容包后，根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和 / 或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和 / 或内容协作设备；

内容协作设备，用于在接收到协作内容包后，根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容协作设备和 / 或内容拥有设备。

数字内容安全协作的方法和系统

技术领域

[0001] 本发明涉及数字内容安全技术领域，尤其涉及一种数字内容安全协作的方法和系统。

背景技术

[0002] 随着电子设备的普及和互联网应用的发展，越来越多的普通用户成为了数字内容的主动生产者，基于网络的人际协作也逐渐增多。内容协作已经成为人们日常生活中非常普遍的行为，典型的场景包括多位作者共同完成数字作品的创作，以及专家帮助作者修改完善数字作品。

[0003] 数字版权保护技术通过一系列手段使得内容拥有设备能够限定谁能够如何使用数字内容，是一种重要的内容保护方式。现有的数字版权保护(Digital Rights Management，DRM)机制主要用于对正式发布后的数字内容进行保护，确保只有获得合法授权的用户能够根据其所获权限使用数字内容。一般而言，内容拥有设备将数字内容密文和完整性验证信息封装在数字内容包中，以防止内容受到非法访问和篡改。只有获得授权的内容使用设备能够在成功验证内容包的完整性后根据许可证中的信息解密、使用数字内容包中的数字内容。

[0004] 现有的DRM机制通常假定数字内容在正式发布前所处的环境是安全可控的，几乎不考虑为数字内容在正式发布前的创作过程中提供保护。然而在内容协作的场景中，创作过程涉及多个参与方，在各方交互的过程中，数字内容的安全性是不确定和不可控的。如果数字内容在内容协作过程中不受保护，数字内容很容易被窃听者或者被恶意的内容协作设备非法使用和传播，从而给版权所有者的权益造成损害。

发明内容

[0005] 本发明实施例提供一种数字内容安全协作的方法和系统，用于提高在内容协作过程中数字内容的安全性。

[0006] 一种数字内容安全协作的方法，该方法包括：

[0007] 内容拥有设备创建数字内容的协作内容包，将创建的协作内容包发送给其他内容拥有设备和/或内容协作设备；所述协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息；

[0008] 接收到协作内容包的内容拥有设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和/或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和/或内容协作设备；

[0009] 接收到协作内容包的内容协作设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容协作设备和/或内容拥有设备。

[0010] 一种数字内容安全协作的系统，该系统包括：

[0011] 内容拥有设备，用于创建数字内容的协作内容包，将创建的协作内容包发送给其他内容拥有设备和/或内容协作设备；所述协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息；以及，

[0012] 在接收到协作内容包后，根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和/或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和/或内容协作设备；

[0013] 内容协作设备，用于在接收到协作内容包后，根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容协作设备和/或内容拥有设备。

[0014] 本方案中，内容拥有设备创建的协作内容包中包含仅能被内容拥有设备更新的属性数据块以及能够被内容拥有设备和内容协作设备更新的内容数据块；内容拥有设备在进行权限验证后，可以对属性数据块和内容数据块中的信息进行更新，内容协作设备在进行权限验证后，仅能对内容数据块中的信息进行更新。通过将协作内容包划分为仅能被内容拥有设备更新的属性数据块以及能够被内容拥有设备和内容协作设备更新的内容数据块，确保了内容协作设备对协作内容包的加工处理和重新封装不会更改数字内容的属性，从而提高了数字内容的安全性。

附图说明

[0015] 图 1A 为本发明实施例的应用场景示意图；

[0016] 图 1B 为本发明实施例提供的方法流程示意图；

[0017] 图 1C 为本发明实施例的协作内容包的结构示意图；

[0018] 图 2A 为本发明实施例一的流程示意图；

[0019] 图 2B 为本发明实施例二的流程示意图；

[0020] 图 3 为本发明实施例提供的设备结构示意图；

[0021] 图 4 为本发明实施例提供的另一设备结构示意图。

具体实施方式

[0022] 为了提高在内容协作过程中数字内容的安全性，本发明实施例提供一种数字内容安全协作的方法，本方法中，内容拥有设备创建的协作内容包中包含仅能被内容拥有设备更新的属性数据块以及能够被内容拥有设备和内容协作设备更新的内容数据块；内容拥有设备在进行权限验证后，可以对属性数据块和内容数据块中的信息进行更新，内容协作设备在进行权限验证后，仅能对内容数据块中的信息进行更新。

[0023] 本发明方法的应用场景如图 1A 所示，包括内容拥有设备、内容协作设备和内容使用设备。参与内容协作的设备包括至少一个内容拥有设备和若干内容协作设备，其可以对内容进行多方、多次加工处理（包括内容编辑、添加批注等等），且加工处理后的所有版本的内容都与原始内容具有相同的基本属性和权限设置。其中：

[0024] 内容拥有设备是数字内容的版权所有人，对数字内容有绝对的操控权，可以对数

字内容进行创建、设置属性信息、加工处理、授权等操作。在协作中，可能存在多个内容拥有设备，多个内容拥有设备都具有同等的最高地位，可利用已有技术手段进行关键信息（包括内容密钥和签名私钥）的安全协商。

[0025] 内容协作设备获得与硬件绑定的协作许可证后，能够在使用被绑定硬件的状态下，对受保护的数字内容（包括所有版本）进行加工处理。被绑定硬件可以是具有计算或者安全存储功能的电子设备，例如单位配备的计算机、经过认证的 U 盾、或者智能密钥设备。

[0026] 除了参与内容协作的人员外，系统用户还包括内容使用设备，他们获得使用授权后，能够对协作完成、正式发布的数字内容进行使用。

[0027] 参见图 1B，本发明实施例提供的数字内容安全协作的方法，包括以下步骤：

[0028] 步骤 10：内容拥有设备创建数字内容的协作内容包，将创建的协作内容包发送给其他内容拥有设备和 / 或内容协作设备；创建的协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息；

[0029] 步骤 11：接收到协作内容包的内容拥有设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和 / 或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和 / 或内容协作设备；

[0030] 步骤 12：接收到协作内容包的内容协作设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容协作设备和 / 或内容拥有设备。

[0031] 步骤 10 中，如图 1C 所示，协作内容包中的属性数据块包含数字内容的属性信息和属性签名；内容数据块中包含内容密文、该协作内容包的封装信息和内容包签名；

[0032] 属性签名是内容拥有设备对属性信息的数字签名；内容密文是内容拥有设备使用内容密钥加密所述数字内容生成的密文；内容包签名是内容拥有设备对内容密文、封装信息与属性信息的数字签名，或者是内容拥有设备对内容密文、封装信息与属性签名的数字签名。属性签名的生成过程如下：内容拥有设备使用消息摘要函数得到属性信息的摘要，然后使用自己的私钥以及数字签名算法得到该摘要的数字签名。同样的，内容包签名的生成过程如下：内容拥有设备使用消息摘要函数得到内容密文、封装信息与属性信息（或者内容密文、封装信息与属性签名）的摘要，然后使用自己的私钥以及数字签名算法得到该摘要的数字签名。

[0033] 属性信息可以包括：数字内容的内容标识和内容拥有设备标识；协作内容包中的封装信息可以包括：封装者标识和封装时间信息。封装者标识是封装当前的协作内容包的设备的标识。封装时间信息用于区分协作内容包的不同版本，可以是协作内容包的封装时间或者版本序列号。

[0034] 相应的，步骤 11 的具体实现可以有如下三种方式：

[0035] 第一，接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后对该协作内容包中的属性信息、封装信息、属性签名和内容包签名进行更新，并将包含更新后的属性信息、封装信息、属性签名和内容包签名、以及更新前的内容密文的协作内容包，发送给其他内容拥有设备和 / 或内容协作设备；

[0036] 其中，更新后的封装信息包含当前的封装者标识和封装时间信息；更新后的属性

签名是内容拥有设备对更新后的属性信息的数字签名，其生成方法与前面描述的属性签名的生成方法类似；更新后的内容包签名是内容拥有设备对更新后的属性信息（或属性签名）与更新后的封装信息、更新前的内容密文的数字签名，其生成方法与前面描述的内容包签名的生成方法类似；

[0037] 第二，接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后使用所述内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；并对该协作内容包中的封装信息和内容包签名进行更新，将包含更新后的内容密文、内容包签名和封装信息、以及更新前的属性信息和属性签名的协作内容包，发送给其他内容拥有设备和／或内容协作设备；

[0038] 其中，各内容拥有设备可以预先对加密数字内容时使用的所述内容密钥进行共享。更新后的封装信息包含当前的封装者标识和封装时间信息；更新后的内容包签名是内容拥有设备对更新前的属性信息（或属性签名）与更新后的封装信息、更新后的内容密文的数字签名，其生成方法与前面描述的内容包签名的生成方法类似；

[0039] 第三，接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后对该协作内容包中的属性信息进行更新；使用所述内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；并对该协作内容包中的封装信息、属性签名和内容包签名进行更新，将包含更新后的属性信息、属性签名、内容密文、封装信息和内容包签名的协作内容包，发送给其他内容拥有设备和／或内容协作设备。

[0040] 其中，各内容拥有设备可以预先对加密数字内容时使用的所述内容密钥进行共享。更新后的属性签名是内容拥有设备对更新后的属性信息的数字签名，其生成方法与前面描述的属性签名的生成方法类似；更新后的封装信息包含当前的封装者标识和封装时间信息；更新后的内容包签名是内容拥有设备对更新后的属性信息（或属性签名）与更新后的封装信息、更新后的内容密文的数字签名，其生成方法与前面描述的内容包签名的生成方法类似。

[0041] 上述接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，其具体实现可以如下：

[0042] 接收到协作内容包的内容拥有设备使用创建该协作内容包的内容拥有设备在生成该协作内容包中的属性签名时使用的私钥，对该属性签名进行验证；具体验证方法为，使用该私钥对该协作内容中的属性信息重新做签名，若得到的新的属性签名与该协作内容中的属性签名一致，则验证通过，否则，验证失败；各内容拥有设备可以预先对生成协作内容包中的属性签名时使用的私钥进行共享。

[0043] 接收到协作内容包的内容拥有设备根据该协作内容包中的封装信息，确定封装该协作内容包的设备，并使用该设备对应的公钥对该协作内容包中的内容包签名进行验证；具体验证方法为，使用该公钥对该协作内容包中的内容包签名进行解密，得到摘要，并使用消息摘要函数得到该协作内容包中的属性信息（或属性签名）与内容密文、封装信息的摘要，若该摘要与解密得到的摘要一致，则验证通过，否则，验证失败。

[0044] 进一步的，在内容拥有设备创建数字内容的协作内容包之后，创建协作内容包的

内容拥有设备自身或通过可信第三方，将创建的协作内容包的协作许可证签发给内容协作设备；该协作许可证中包含授权信息和授权签名；该授权信息包含该协作内容包中的属性信息和内容密钥密文；该内容密钥密文是使用被绑定硬件保存或生成的密钥加密所述内容密钥生成的密文；该授权签名是授权者对该授权信息的数字签名，授权签名的生成过程如下：授权者使用消息摘要函数得到授权信息的摘要，然后使用自己的私钥以及数字签名算法得到该摘要的数字签名。

[0045] 上述授权信息还可以包含权利信息，该权利信息是用于申明内容协作设备能够对协作内容包进行的处理操作的信息。被绑定硬件可以是位于指定区域内的硬件或属于被授权的内容协作设备的硬件。

[0046] 相应的，步骤 12 的具体实现可以如下：

[0047] 接收到协作内容包的内容协作设备对协作许可证中的授权签名以及该协作内容包中的属性签名和内容包签名进行验证，在验证通过后，确定协作许可证中的属性信息与该协作内容包中的属性信息是否一致，在确定为是时：

[0048] 在使用被绑定硬件的状态下获取被绑定硬件保存或生成的密钥，使用获取到的密钥对协作许可证中的内容密钥密文进行解密，使用解密得到的内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；对该协作内容包中的封装信息和内容包签名进行更新，将包含更新后的内容密文、内容包签名和封装信息、以及更新前的属性信息和属性签名的协作内容包，发送给其他内容协作设备和 / 或内容拥有设备。

[0049] 其中，更新后的封装信息包含当前的封装者标识和封装时间信息；更新后的内容包签名是更新前的属性信息（或属性签名）与更新后的封装信息、更新后的内容密文的数字签名，其生成方法与前面描述的内容包签名的生成方法类似。

[0050] 上述接收到协作内容包的内容协作设备对协作许可证中的授权签名以及该协作内容包中的属性签名和内容包签名进行验证，具体实现可以如下：

[0051] 接收到协作内容包的内容协作设备根据签发协作许可证的设备的公钥，对协作许可证中的授权签名进行验证；具体验证方法为，使用该公钥对协作许可证中的授权签名进行解密，得到摘要，并使用消息摘要函数得到该协作许可证中的授权信息的摘要，若该摘要与解密得到的摘要一致，则验证通过，否则，验证失败。

[0052] 接收到协作内容包的内容协作设备根据该协作内容包中的封装信息，确定封装该协作内容包的设备，并使用该设备对应的公钥对该协作内容包中的属性签名和内容包签名进行验证。对属性签名的具体验证方法为，使用该公钥对该协作内容包中的属性签名进行解密，得到摘要，并使用消息摘要函数得到该协作内容包中的属性信息的摘要，若该摘要与解密得到的摘要一致，则验证通过，否则，验证失败。对内容包签名的具体验证方法为，使用该公钥对该协作内容包中的内容包签名进行解密，得到摘要，并使用消息摘要函数得到该协作内容包中的属性信息（或属性签名）与内容密文、封装信息的摘要，若该摘要与解密得到的摘要一致，则验证通过，否则，验证失败。

[0053] 上述生成内容密钥密文时使用的密钥为被绑定硬件保存或生成的公钥时，内容协作设备对协作许可证中的内容密钥密文进行解密时使用的密钥为被绑定硬件保存或生成的私钥；或者，生成内容密钥密文时使用的密钥为被绑定硬件保存或生成的对称密钥时，内

容协作设备对协作许可证中的内容密钥密文进行解密时使用的密钥为对称密钥。

[0054] 进一步的，在经过内容拥有设备和 / 内容协作设备的至少一次的协作内容包的更新后，创建协作内容包的内容拥有设备接收到内容协作设备或其他内容拥有设备发来的更新后的协作内容包后，可以对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后使用所述内容密钥对该协作内容包中的内容密文进行解密，在用户对解密得到的内容明文进行审核确认后，根据审核确认后的内容明文创建用于正式发布的数字内容包。具体实现可以采用如下两种方式：

[0055] 第一，创建并发布的数字内容包与协作内容包的格式相同，包含数字内容的属性信息、属性信息的数字签名即属性签名、使用内容密钥对审核确认后的内容明文进行加密得到的数字内容密文、该数字内容包的封装信息、数字内容包签名，该数字内容包签名是该内容拥有设备对该数字内容密文、该封装信息与该属性信息（或属性签名）的数字签名；以及，

[0056] 在创建并发布用于正式发布的数字内容包之后，创建协作内容包的内容拥有设备自身或通过可信第三方，将数字内容包的使用许可证签发给内容使用设备；该使用许可证中包含许可信息和许可签名，该许可信息包含数字内容包中的属性信息和数字内容密钥密文；该数字内容密钥密文是使用内容使用设备的公钥加密所述内容密钥生成的密文；该许可签名是授权者（创建协作内容包的内容拥有设备自身或可信第三方）对该许可信息的数字签名；

[0057] 内容使用设备对使用许可证中的许可签名以及内容数字包中的内容包签名和属性签名进行验证，在验证通过后使用自己的私钥解密使用许可证中的数字内容密钥密文，使用解密得到的内容密钥对内容数字包中的数字内容密文进行解密，并使用解密得到的内容。

[0058] 第二，创建并发布的数字内容包中包含数字内容的属性信息、使用内容密钥对审核确认后的内容明文进行加密得到的数字内容密文、数字内容包签名，该数字内容包签名是该内容拥有设备对该数字内容密文与该属性信息的数字签名；以及，

[0059] 在创建并发布用于正式发布的数字内容包之后，创建协作内容包的内容拥有设备自身或通过可信第三方，将数字内容包的使用许可证签发给内容使用设备；该使用许可证中包含许可信息和许可签名，该许可信息包含数字内容包中的属性信息和数字内容密钥密文；该数字内容密钥密文是使用内容使用设备的公钥加密所述内容密钥生成的密文；该许可签名是授权者（创建协作内容包的内容拥有设备自身或可信第三方）对该许可信息的数字签名；

[0060] 内容使用设备对使用许可证中的许可签名以及所述内容数字包中的内容包签名和属性签名进行验证，在验证通过后使用自己的私钥解密使用许可证中的数字内容密钥密文，使用解密得到的内容密钥对所述内容数字包中的数字内容密文进行解密，并使用解密得到的内容。

[0061] 下面结合具体实施例对本发明进行说明：

[0062] 实施例一：

[0063] 本实施例针对某公司的项目经理与助理合作撰写项目报告的场景提出数字内容安全协作的具体方法，内容协作设备为公司分配的计算机设备，正式发布的数字内容包的

结构与协作内容包的结构相同。内容拥有设备是经理所使用设备A，内容协作设备是助理所使用设备B，内容使用设备是公司总经理所使用设备C。各设备通过可靠的DRM软件进行相关的安全操作，包括生成并保存密钥，创建、更新、或解析内容包，创建或解析许可证，根据权限加工处理或使用内容等等。本实施例中的对称加密机制具体可采用高级加密标准AES、国际数据加密算法IDEA等；消息摘要函数可采用MD5、SHA-1等；数字签名可采用RSA、DSS等算法。

[0064] 本实施例的交互流程如图2A所示：

[0065] 步骤一：用户注册；

[0066] 某公司为保证重要资料的安全，在每位员工的计算机上安装了DRM软件，保证只有获得授权的员工能够在指定的计算机上创建、加工或读取资料。用户注册阶段，每一名员工在自己的计算机上打开DRM软件的注册界面，输入自己的员工号作为用户标识，DRM软件提取员工计算机的设备参数信息，生成一对设备公私钥对，然后将用户的员工号和生成的设备公钥上传到公司服务器，服务器经过检查确认后，将所有员工的员工号和对应的设备公钥公开。

[0067] 步骤二：A创建原始的协作内容包；

[0068] 使用A的用户撰写项目报告草稿，然后选择DRM软件上的“创建协作内容包”功能，设置内容状态标志为“创作中”，A为报告创建初始化的协作内容包CPO。DRM客户端软件从系统设置中提取A的员工号ID(A)，为该报告生成唯一的内容标识i，随机的内容密钥CEK，最终生成CPO。CPO中，属性信息包括内容标识i、内容拥有设备标识ID(A)、以及内容状态标志“创作中”，属性签名用A的设备私钥对属性信息的摘要做签名生成，内容密文是用CEK对称加密报告明文生成，封装者标识是ID(A)，封装时间信息是当前的系统时间，内容包签名是用A的设备私钥对属性签名、内容密文和封装时间信息的摘要做签名生成。

[0069] 步骤三：A为B授权；

[0070] A通过DRM软件为B创建协作许可证，其中包含了内容标识i，拥有者标识ID(A)，内容密钥密文，授予B的权利信息和用A的设备私钥对上述信息摘要做的签名。其中内容密钥密文用B的设备公钥加密CEK生成。

[0071] 步骤四：B加工内容，更新协作内容包；

[0072] A将协作内容包CPO和协作许可证通过电子邮件发送给B，要求B对报告内容进行补充、完善。

[0073] B获得协作许可证和CPO后，B的DRM软件首先验证协作许可证中A的签名和CPO中的内容包签名和属性签名，然后确认CPO中的内容标识i与协作许可证中的内容标识i一致，且CPO中的内容状态标志为“创作中”。验证成功后，B的DRM软件根据设备信息生成设备私钥，用设备私钥解密协作许可证中的内容密钥密文，再用获得的内容密钥CEK解密CPO中的内容密文，呈现内容明文，使用B的用户根据所获权限对内容明文进行加补充、完善。

[0074] 当使用B的用户完成加工处理操作后，B的DRM软件用从协作许可证中提取的内容密钥CEK加密更新后的报告明文，生成更新后的内容密文，然后创建更新后的协作内容包CP1，其中CP1的属性信息与CPO中的属性信息相同，CP1的属性签名与CPO中的属性签名相同，CP1的内容密文为更新后的内容密文，CP1的封装者标识为B的用户标识ID(B)，CP1的

封装时间为当前的系统时间，CP1 的内容包签名是用 B 的设备私钥对 CP1 的属性签名、CP1 的内容密文和 CP1 的封装时间信息的摘要做的签名。

[0075] 步骤五 :A 审核内容并发布正式内容包 ;

[0076] B 将 CP1 通过电子邮件发送给 A。A 通过 DRM 软件验证 CP1 的内容包签名和属性签名。下一步，A 用 CEK 解密 CP1 中的内容密文，使用 A 的用户对内容明文进行审核确认，并根据实际情况对内容明文进行调整，形成最终确定的内容明文 M。确认完成后，A 创建正式内容包 CP :A 先将 CP1 中的内容标识 i、拥有者标识 ID(A)、和用 CEK 加密 M 形成的内容密文存放到 CP 的对应项中，然后将 CP 属性信息中的内容状态标志设置为“正式发布”，并用自己的设备私钥对 CP 中的属性信息的摘要签名，生成 CP 的属性签名 ;进一步，A 设置封装者标识为自己的用户标识 ID(A)，封装时间信息为当前的系统时间，并用自己的设备私钥对 CP 的属性签名、内容密文和封装时间信息的摘要做签名，生成内容包签名。

[0077] 步骤六 :A 授权 C 使用正式发布的内容 ;

[0078] A 为 C 创建使用许可证，其中包含了内容标识 i、内容密钥密文、C 的使用权利信息和 A 用设备私钥对上述信息摘要的签名 ;所述内容密钥密文是 A 用 C 的设备公钥加密内容密钥 CEK 生成的。完成许可证创建后，A 将正式发布的数字内容包 CP 和使用许可证通过电子邮件发送给 C。

[0079] 使用受保护的项目报告前，C 首先验证 CP 中的内容包签名和属性签名，并确认 CP 中的内容拥有设备标识和封装者标识一致，且内容状态标志为“正式发布”。若验证失败，C 放弃使用 CP 中的内容。若验证成功，C 继续验证使用许可证的完整性，然后用自己的设备私钥解密使用许可证中的内容密钥密文，用获得的内容密钥 CEK 解密 CP 中的内容密文，最后使用 C 的用户根据授予的权限使用 CP 中的项目报告。

[0080] 实施例二 :

[0081] 本实施例针对作家在助手的协作下完成数字作品的创作、并通过数字内容经销商销售数字作品的场景提出数字内容安全协作的具体方法。本实施例中，内容协作设备只能在使用经过认证的被绑定硬件的状态下进行协作，正式发布的数字内容包的结构与协作内容包的结构不同。内容拥有设备是网络作家使用的设备 A，内容协作设备是插图绘制人使用的设备 B1 和编辑使用的设备 B2，内容使用设备是消费者使用的设备 C，另外，系统中还有一个可信的内容经销商 D，负责运行具有 DRM 功能的内容协作管理平台和内容销售平台，职责包括用户认证和许可证签发。本实施例中的对称加密机制具体可采用高级加密标准 AES、国际数据加密算法 IDEA 等 ;消息摘要函数可采用 MD5、SHA-1 等 ;数字签名可采用 RSA、DSS 等算法。

[0082] 在进行内容协作前需要进行用户注册，具体的 :

[0083] D 负责运行具备 DRM 功能的内容协作管理平台和内容销售平台。其通过权威的认证中心获得一对公私钥对，并公开自己的公钥证书。

[0084] A、B1、B2 到 D 运行的内容协作管理平台上分别注册用户标识 ID(A)、ID(B1)、ID(B2)，并在认证中心授权的 D 的注册登记处领取存储了自己公私钥的 U 盾，U 盾中的微型智能卡处理器能够根据存储的用户私钥进行解密和数字签名等操作。D 在内容协作管理平台上公布注册用户的公钥列表。

[0085] C 到 D 运行的内容销售平台注册用户标识 ID(C)，并通过 DRM 客户端提取并上传自

己的设备特征信息，进行设备注册。为了保护版权所有人的权利，销售平台对用户能够注册的设备数进行了限制，例如允许用户最多注册 6 台设备。C 完成设备注册后，D 能够根据 C 的设备信息生成 D 的设备密钥，使得 C 在获得授权后，能且仅能在已注册设备上使用数字内容。

[0086] 本实施例的基本流程如图 2B 所示：

[0087] 步骤 1：A 初始化协作内容包，并上传内容密钥密文；

[0088] 使用 A 的用户完成作品初稿创作后，通过 DRM 客户端软件选择“封装协作内容包”功能。DRM 客户端软件为该作品生成唯一的内容标识 i，随机的内容密钥 CEK，并要求 A 插入 U 盾，为 A 生成初始化的协作内容包 CPO。CPO 中，属性信息包括内容标识 i 和内容拥有设备标识 ID(A)；属性签名由 A 的 U 盾用 A 的私钥对属性信息的摘要做签名生成；内容密文是 DRM 客户端软件用 CEK 对称加密作品明文生成；封装者标识是 ID(A)，封装时间信息是版本序列号 0；内容包签名由 A 的 U 盾用 A 的私钥对属性信息、内容密文和封装时间信息的摘要做签名生成。

[0089] 初始化的协作内容包 CPO 创建完成后，A 通过 DRM 客户端软件用 D 的公钥加密 CEK，并将 CPO 和 CEK 的密文上传到协作管理平台。D 通过协作管理平台获得上述信息后，用私钥解密 CEK 的密文，并在与内容 i 相对应的数据项中安全地保存 CEK。

[0090] 步骤 2：A 通过 D 为 B1、B2 授权；

[0091] 使用 A 的用户通过协作管理平台将 B1 和 B2 添加为内容 i 的内容协作设备，并设置分配给 B1 的权限是为作品添加插图，分配给 B2 的权限是在 B1 完成插图后，检查并修改作品内容。D 通过协作管理平台为 B1、B2 分别创建协作许可证，其中包含了内容标识 i，拥有者标识 ID(A)，内容密钥密文，A 授予 B1 或 B2 的权利信息，D 的标识和 D 用自己的私钥对上述信息摘要做的签名。其中内容密钥密文是 D 用 B1 或 B2 的公钥加密 CEK 生成。

[0092] 步骤 3：A 与 B1、B2 协作修改内容；

[0093] D 将初始化内容包 CPO 和协作许可证通过系统消息发送给 B1、B2。

[0094] B1 获得协作许可证和 CPO 后，通过 DRM 客户端软件首先验证协作许可证中 D 的签名和 CPO 中的内容包签名和属性签名，然后确认 CPO 中的内容标识 i 与协作许可证中的内容标识 i 一致。验证成功后，B1 的 DRM 客户端软件要求 B1 插入 U 盾，U 盾用 B1 的私钥解密协作许可证中的内容密钥密文，再通过安全信道将获得的内容密钥 CEK 传送给 B1 的 DRM 客户端软件，用于解密 CPO 中的内容密文，呈现内容明文，使用 B1 的用户根据所获权限为作品添加插图。

[0095] 当使用 B1 的用户完成加工处理操作后，B1 的 DRM 客户端软件用从协作许可证中提取的内容密钥 CEK 加密更新后的作品明文，生成更新后作品的内容密文，然后创建更新后的协作内容包 CP1，其中 CP1 的属性信息与 CPO 中的属性信息相同，CP1 的属性签名与 CPO 中的属性签名相同，CP1 的内容密文为更新后的内容密文，CP1 的封装者标识为 B1 的用户标识 ID(B1)，CP1 的封装时间信息是版本序列号 1，CP1 的内容包签名是 B1 的 U 盾用 B1 的私钥对 CP1 的属性信息、CP1 的内容密文和 CP1 的封装时间信息的摘要做的签名。

[0096] B1 完成 CP1 的封装后，通过协作管理平台的系统消息将 CP1 发送给 B2。B2 通过 DRM 客户端软件首先验证协作许可证中 D 的签名和 CP1 中的内容包签名和属性签名，然后确认 CP1 中的内容标识 i 与协作许可证中的内容标识 i 一致。验证成功后，B2 的 DRM 客户端

软件要求 B2 插入 U 盾用 B2 的私钥解密协作许可证中的内容密钥密文，U 盾通过安全信道将获得的内容密钥 CEK 传递给 DRM 客户端软件，DRM 客户端软件用 CEK 解密 CP1 中的内容密文，呈现内容明文，使用 B2 的用户根据所获权限对作品进行检查和修改。

[0097] 当使用 B2 的用户完成加工处理操作后，B2 的 DRM 客户端软件用从协作许可证中提取的内容密钥 CEK 加密更新后的作品明文，生成更新后作品的内容密文，然后创建更新后的协作内容包 CP2，其中 CP2 的属性信息与 CP1 中的属性信息相同，CP2 的属性签名与 CP1 中的属性签名相同，CP2 的内容密文为更新后的内容密文，CP2 的封装者标识为 B2 的用户标识 ID(B2)，CP2 的封装时间信息为当前的版本序列号 2，CP2 的内容包签名是 B2 的 U 盾用 B2 的私钥对 CP2 的属性信息、CP2 的内容密文和 CP2 的封装时间信息的摘要做的签名。

[0098] 步骤 4 :A 审核内容并生成正式的数字内容包 ;

[0099] B2 将 CP2 通过系统消息发送给 A。A 通过 DRM 客户端软件验证 CP2 的内容包签名和属性签名。下一步，A 用 CEK 解密 CP2 中的内容密文，使用 A 的用户对内容明文进行审核确认，并根据实际情况对内容明文进行调整，或者要求 B1、B2 重复完成协作工作，直到形成最终确定的内容明文 M。确认完成后，A 通过 DRM 客户端软件随机生成新的内容密钥 CEK’，创建正式的数字内容包 CP。CP 中包含内容标识 i、拥有者标识 ID(A)、用 CEK’加密 M 形成的内容密文，以及 A 的 U 盾用 A 的私钥对这些信息的摘要做的签名。

[0100] 步骤 5 :A 通过 D 销售正式内容包 ;

[0101] A 用 D 的公钥加密 CEK’，然后将 CP 和 CEK’的密文上传到协作管理平台，并选择平台上的“正式发布”功能，请求 D 替代其进行 CP 中数字作品的销售。D 用私钥解密 CEK’的密文，获取并安全保存 CEK’。

[0102] 步骤 6 :D 授权 C 使用正式发布的内容。

[0103] D 在销售平台上发布 CP 的商品信息，当用户 C 成功购买并下载 CP 后，D 为 C 创建使用许可证，其中包含了内容标识 i、内容密钥密文、C 的使用权利信息和 D 用私钥对上述信息摘要的签名 ;所述内容密钥密文由 D 用 C 的设备密钥加密内容密钥 CEK’生成。完成许可证创建后，D 将使用许可证发送到 C 的设备上。

[0104] 使用受保护的数字作品前，C 首先分别验证 CP 和使用许可证中的签名，并确认 CP 和使用许可证中的内容标识一致。若验证失败，C 向 D 发送错误信息，请求 D 重新发送 CP 或者使用许可证。若验证成功，C 在注册设备上通过 DRM 客户端软件提取设备信息，生成设备密钥，用设备密钥解密使用许可证中的内容密钥密文，用获得的内容密钥 CEK’解密 CP 中的内容密文，最后使用 C 的用户根据授予的权限使用 CP 中的数字作品。

[0105] 仍参见图 1A，本发明实施例还提供一种数字内容安全协作的系统，该系统包括 :

[0106] 内容拥有设备，用于创建数字内容的协作内容包，将创建的协作内容包发送给其他内容拥有设备和 / 或内容协作设备 ;所述协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息 ;以及，

[0107] 在接收到协作内容包后，根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和 / 或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和 / 或内容协作设备 ;

[0108] 内容协作设备，用于在接收到协作内容包后，根据该协作内容包进行权限验证，并

在权限验证通过后对该协作内容包中内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容协作设备和 / 或内容拥有设备。

[0109] 进一步的，所述属性数据块中包含所述数字内容的属性信息和属性签名，所述内容数据块中包含内容密文、该协作内容包的封装信息和内容包签名；所述属性签名是所述属性信息的数字签名；所述内容密文是使用内容密钥加密所述数字内容生成的密文；所述内容包签名是所述内容密文、所述封装信息与所述属性信息的数字签名，或者是所述内容密文、所述封装信息与所述属性签名的数字签名。

[0110] 进一步的，所述内容拥有设备用于：

[0111] 在接收到协作内容包后，对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后对该协作内容包中的属性信息、封装信息、属性签名和内容包签名进行更新，并将包含更新后的属性信息、封装信息、属性签名和内容包签名、以及更新前的内容密文的协作内容包，发送给其他内容拥有设备和 / 或内容协作设备；或者，

[0112] 接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后使用所述内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；并对该协作内容包中的封装信息和内容包签名进行更新，将包含更新后的内容密文、封装信息和内容包签名、以及更新前的属性信息和属性签名的协作内容包，发送给其他内容拥有设备和 / 或内容协作设备；或者，

[0113] 接收到协作内容包的内容拥有设备对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后对该协作内容包中的属性信息进行更新；使用所述内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；并对该协作内容包中的封装信息、属性签名和内容包签名进行更新，将包含更新后的属性信息、属性签名、内容密文、封装信息和内容包签名的协作内容包，发送给其他内容拥有设备和 / 或内容协作设备。

[0114] 进一步的，所述内容拥有设备用于：按照如下方法对该协作内容包中的属性签名和内容包签名进行验证：

[0115] 使用私钥对该协作内容包中的属性信息进行签名，并将该签名与该协作内容包中的属性签名进行对比，以实现对属性签名的验证；

[0116] 根据该协作内容包中的封装信息，确定封装该协作内容包的设备，并使用该设备对应的公钥和该协作内容包中的内容密文、封装信息、以及属性信息或属性签名，对该协作内容包中的内容包签名进行验证。

[0117] 进一步的，所述内容拥有设备还用于：

[0118] 在创建数字内容的协作内容包之后，通过自身或可信第三方，将创建的协作内容包的协作许可证签发给内容协作设备；所述协作许可证中包含授权信息和授权签名；该授权信息包含该协作内容包中的属性信息和内容密钥密文；该内容密钥密文是使用被绑定硬件保存或生成的密钥加密所述内容密钥生成的密文；该授权签名是内容拥有设备对该授权信息的数字签名。

[0119] 进一步的，所述内容协作设备用于：

[0120] 对所述协作许可证中的授权签名以及该协作内容包中的属性签名和内容包签名

进行验证，在验证通过后，确定所述协作许可证中的属性信息与该协作内容包中的属性信息是否一致，在确定为是时：

[0121] 获取所述被绑定硬件保存或生成的密钥，使用该密钥对所述协作许可证中的内容密钥密文进行解密，使用解密得到的内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；对该协作内容包中的封装信息和内容包签名进行更新，将包含更新后的内容密文、内容包签名和封装信息、以及更新前的属性信息和属性签名的协作内容包，发送给其他内容协作设备和/或内容拥有设备。

[0122] 进一步的，所述内容协作设备用于：按照如下方法对所述协作许可证中的授权签名以及该协作内容包中的属性签名和内容包签名进行验证：

[0123] 根据签发所述协作许可证的设备的公钥和协作许可证中的授权信息，对所述协作许可证中的授权签名进行验证；

[0124] 根据该协作内容包中的封装信息，确定封装该协作内容包的设备，并使用该设备对应的公钥和协作内容包中的内容密文、封装信息、以及属性信息或属性签名对该协作内容包中的属性签名和内容包签名进行验证；还根据该协作内容包中的属性信息确定内容拥有设备，并使用确定的内容拥有设备对应的公钥和协作内容包中的属性信息对该协作内容包中的属性签名进行验证。

[0125] 进一步的，在生成所述内容密钥密文时使用的密钥为所述被绑定硬件保存或生成的公钥时，所述内容协作设备对所述协作许可证中的内容密钥密文进行解密时使用的密钥为所述被绑定硬件保存或生成的私钥；或者，

[0126] 生成所述内容密钥密文时使用的密钥为所述被绑定硬件保存或生成的对称密钥时，所述内容协作设备对所述协作许可证中的内容密钥密文进行解密时使用的密钥为该对称密钥。

[0127] 进一步的，所述授权信息还包含权利信息，该权利信息是用于申明内容协作设备能够对协作内容包进行的处理操作的信息。

[0128] 进一步的，所述被绑定硬件是位于指定区域内的硬件或属于被授权的内容协作设备的硬件。

[0129] 进一步的，所述内容拥有设备还用于：

[0130] 接收到内容协作设备或其他内容拥有设备发来的协作内容包后，对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后使用所述内容密钥对该协作内容包中的内容密文进行解密，在用户对解密得到的内容明文进行审核确认后，根据审核确认后的内容明文创建用于正式发布的数字内容包。

[0131] 进一步的，所述属性信息包括：所述数字内容的内容标识和内容拥有设备标识；所述封装信息包括：封装者标识和封装时间信息。

[0132] 参见图 3，本发明实施例还提供一种内容拥有设备，该设备包括：

[0133] 创建单元 30，用于创建数字内容的协作内容包；所述协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息；

[0134] 发送单元 31，用于将创建的协作内容包发送给其他内容拥有设备和/或内容协作

设备。

[0135] 进一步的，该内容拥有设备还包括：

[0136] 协作单元 32，用于接收到协作内容包后，根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和 / 或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和 / 或内容协作设备。

[0137] 进一步的，所述属性数据块中包含所述数字内容的属性信息和属性签名，所述内容数据块中包含内容密文、该协作内容包的封装信息和内容包签名；所述属性签名是内容拥有设备对所述属性信息的数字签名；所述内容密文是内容拥有设备对使用内容密钥加密所述数字内容生成的密文；所述内容包签名是内容拥有设备对所述内容密文、所述封装信息与所述属性信息的数字签名，或者是所述内容密文、所述封装信息与所述属性签名的数字签名。

[0138] 进一步的，所述协作单元 32 用于：

[0139] 对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后对该协作内容包中的属性信息、封装信息、属性签名和内容包签名进行更新，并将包含更新后的属性信息、封装信息、属性签名和内容包签名、以及更新前的内容密文的协作内容包，发送给其他内容拥有设备和 / 或内容协作设备；或者，

[0140] 对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后使用所述内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；并对该协作内容包中的封装信息和内容包签名进行更新，将包含更新后的内容密文、封装信息和内容包签名、以及更新前的属性信息和属性签名的协作内容包，发送给其他内容拥有设备和 / 或内容协作设备；或者，

[0141] 对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后对该协作内容包中的属性信息进行更新；使用所述内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；并对该协作内容包中的封装信息、属性签名和内容包签名进行更新，将包含更新后的属性信息、属性签名、内容密文、封装信息和内容包签名的协作内容包，发送给其他内容拥有设备和 / 或内容协作设备。

[0142] 进一步的，所述协作单元 32 用于：

[0143] 按照如下方法对该协作内容包中的属性签名和内容包签名进行验证：

[0144] 使用私钥对该协作内容包中的属性信息进行签名，并将该签名与该协作内容包中的属性签名进行对比，以实现对属性签名的验证；

[0145] 根据该协作内容包中的封装信息，确定封装该协作内容包的设备，并使用该设备对应的公钥和该协作内容包中的内容密文、封装信息、以及属性信息或属性签名，对该协作内容包中的内容包签名进行验证。

[0146] 进一步的，该内容拥有设备还包括：

[0147] 授权单元 33，用于通过自身或可信第三方，将创建的协作内容包的协作许可证签发给内容协作设备；所述协作许可证中包含授权信息和授权签名；该授权信息包含该协作内容包中的属性信息和内容密钥密文；该内容密钥密文是使用被绑定硬件保存或生成的密

钥加密所述内容密钥生成的密文；该授权签名是内容拥有设备对该授权信息的数字签名。

[0148] 进一步的，该内容拥有设备还包括：

[0149] 发布单元 34，用于接收到内容协作设备或其他内容拥有设备发来的协作内容包后，对该协作内容包中的属性签名和内容包签名进行验证，在验证通过后使用所述内容密钥对该协作内容包中的内容密文进行解密，在用户对解密得到的内容明文进行审核确认后，根据审核确认后的内容明文创建用于正式发布的数字内容包。

[0150] 参见图 4，本发明实施例还提供一种内容协作设备，该设备包括：

[0151] 验证单元 40，用于接收到协作内容包后，根据该协作内容包进行权限验证；该协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息；

[0152] 更新单元 41，用于在权限验证通过后对该协作内容包中内容数据块中的信息进行更新；

[0153] 发送单元 42，用于将包含更新后的信息的协作内容包发送给其他内容协作设备和 / 或内容拥有设备。

[0154] 进一步的，所述属性数据块中包含所述数字内容的属性信息和属性签名，所述内容数据块中包含内容密文、该协作内容包的封装信息和内容包签名；所述属性签名是内容拥有设备对所述属性信息的数字签名；所述内容密文是内容拥有设备或其他内容协作设备对使用内容密钥加密所述数字内容生成的密文；所述内容包签名是内容拥有设备或其他内容协作设备对所述内容密文、所述封装信息与所述属性信息的数字签名，或者是所述内容密文、所述封装信息与所述属性签名的数字签名。

[0155] 进一步的，该内容协作设备还包括：

[0156] 授权接收单元 43，用于接收内容拥有设备自身或通过可信第三方签发的协作内容包的协作许可证；所述协作许可证中包含授权信息和授权签名；该授权信息包含该协作内容包中的属性信息和内容密钥密文；该内容密钥密文是使用被绑定硬件保存或生成的密钥加密所述内容密钥生成的密文；该授权签名是该内容拥有设备对授权信息的数字签名；

[0157] 相应的，所述验证单元 40 用于：

[0158] 对所述协作许可证中的授权签名以及该协作内容包中的属性签名和内容包签名进行验证，在验证通过后，确定所述协作许可证中的属性信息与该协作内容包中的属性信息是否一致；

[0159] 所述更新单元 41 用于：

[0160] 在确定一致时，获取所述被绑定硬件保存或生成的密钥，使用该密钥对所述协作许可证中的内容密钥密文进行解密，使用解密得到的内容密钥对该协作内容包中的内容密文进行解密，对解密得到的内容明文进行更新，使用所述内容密钥对更新后的内容明文进行加密，得到更新后的内容密文；对该协作内容包中的封装信息和内容包签名进行更新；

[0161] 所述发送单元 42 用于：

[0162] 将包含更新后的内容密文、内容包签名和封装信息、以及更新前的属性信息和属性签名的协作内容包，发送给其他内容协作设备和 / 或内容拥有设备。

[0163] 进一步的，所述验证单元 40 用于：

[0164] 按照如下方法对所述协作许可证中的授权签名以及该协作内容包中的属性签名

和内容包签名进行验证 ：

[0165] 根据签发所述协作许可证的设备的公钥和协作许可证中的授权信息，对所述协作许可证中的授权签名进行验证 ；

[0166] 根据该协作内容包中的封装信息，确定封装该协作内容包的设备，并使用该设备对应的公钥和协作内容包中的内容密文、封装信息、以及属性信息或属性签名对该协作内容包中的属性签名和内容包签名进行验证 ；还根据该协作内容包中的属性信息确定内容拥有设备，并使用确定的内容拥有设备对应的公钥和协作内容包中的属性信息对该协作内容包中的属性签名进行验证。

[0167] 进一步的，生成所述内容密钥密文时使用的密钥为所述被绑定硬件保存或生成的公钥时，所述更新单元 41 对所述协作许可证中的内容密钥密文进行解密时使用的密钥为所述被绑定硬件保存或生成的私钥 ；或者，

[0168] 生成所述内容密钥密文时使用的密钥为所述被绑定硬件保存或生成的对称密钥时，所述更新单元 41 对所述协作许可证中的内容密钥密文进行解密时使用的密钥为该对称密钥。

[0169] 综上，本发明的有益效果包括 ：

[0170] 本发明实施例提供的方案中，内容拥有设备创建的协作内容包中包含仅能被内容拥有设备更新的属性数据块以及能够被内容拥有设备和内容协作设备更新的内容数据块 ；内容拥有设备在进行权限验证后，可以对属性数据块和内容数据块中的信息进行更新，内容协作设备在进行权限验证后，仅能对内容数据块中的信息进行更新。本发明通过将协作内容包划分为仅能被内容拥有设备更新的属性数据块以及能够被内容拥有设备和内容协作设备更新的内容数据块，确保了内容协作设备对协作内容包的加工处理和重新封装不会更改数字内容的属性，从而提高了数字内容的安全性。并且内容拥有设备和获得授权的内容协作设备对所有版本的协作内容包的权限保持不变，这免除了对各个版本分别管理、授权的开销。

[0171] 其次，本发明通过将协作许可证与硬件绑定，限制内容协作设备工作的范围，防止内容协作设备滥用权利、恶意散播受保护的内容。再者，只有经过内容拥有设备审核确认的内容才能够最终正式发布，从而确保内容拥有设备对内容发布的可控性。此外，本发明不限定协作的具体交互流程，可灵活地应用于多种协作模式。因此，本发明能够为数字内容的协作过程提供安全保障，且具有良好的易用性和灵活性。

[0172] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

[0173] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或

多个方框中指定的功能。

[0174] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

[0175] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0176] 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。

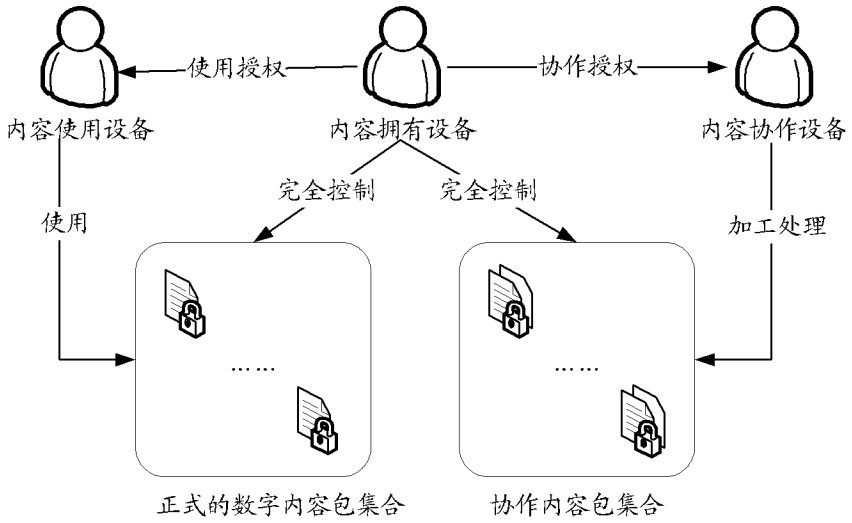

使用授权
协作授权
内容使用设备
内容拥有设备
内容协作设备
完全控制
完全控制
使用
加工处理
……
……
正式的数字内容包集合
协作内容包集合

图 1A

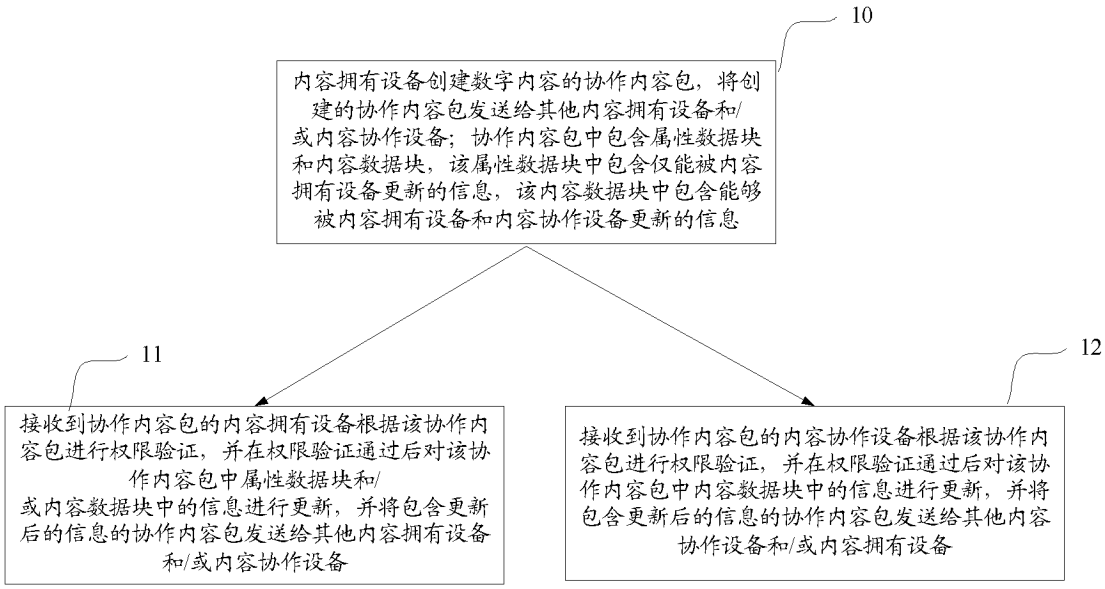

10
内容拥有设备创建数字内容的协作内容包，将创建的协作内容包发送给其他内容拥有设备和/或内容协作设备；协作内容包中包含属性数据块和内容数据块，该属性数据块中包含仅能被内容拥有设备更新的信息，该内容数据块中包含能够被内容拥有设备和内容协作设备更新的信息
11
接收到协作内容包的内容拥有设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中属性数据块和/或内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容拥有设备和/或内容协作设备
12
接收到协作内容包的内容协作设备根据该协作内容包进行权限验证，并在权限验证通过后对该协作内容包中内容数据块中的信息进行更新，并将包含更新后的信息的协作内容包发送给其他内容协作设备和/或内容拥有设备

图 1B

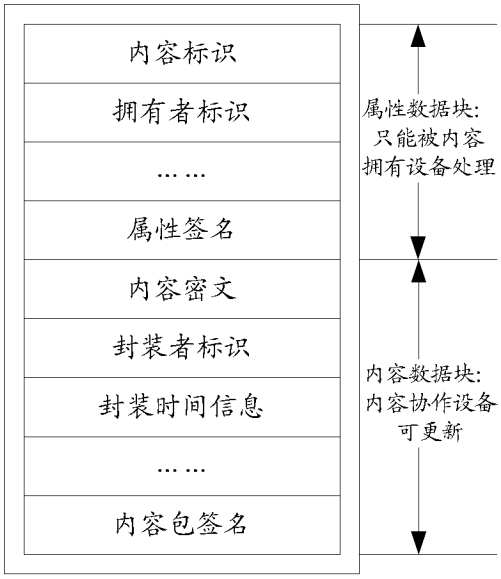

内容标识
拥有者标识
……
属性签名
内容密文
封装者标识
封装时间信息
……
内容包签名
属性数据块:
只能被内容
拥有设备处理
内容数据块:
内容协作设备
可更新

图 1C

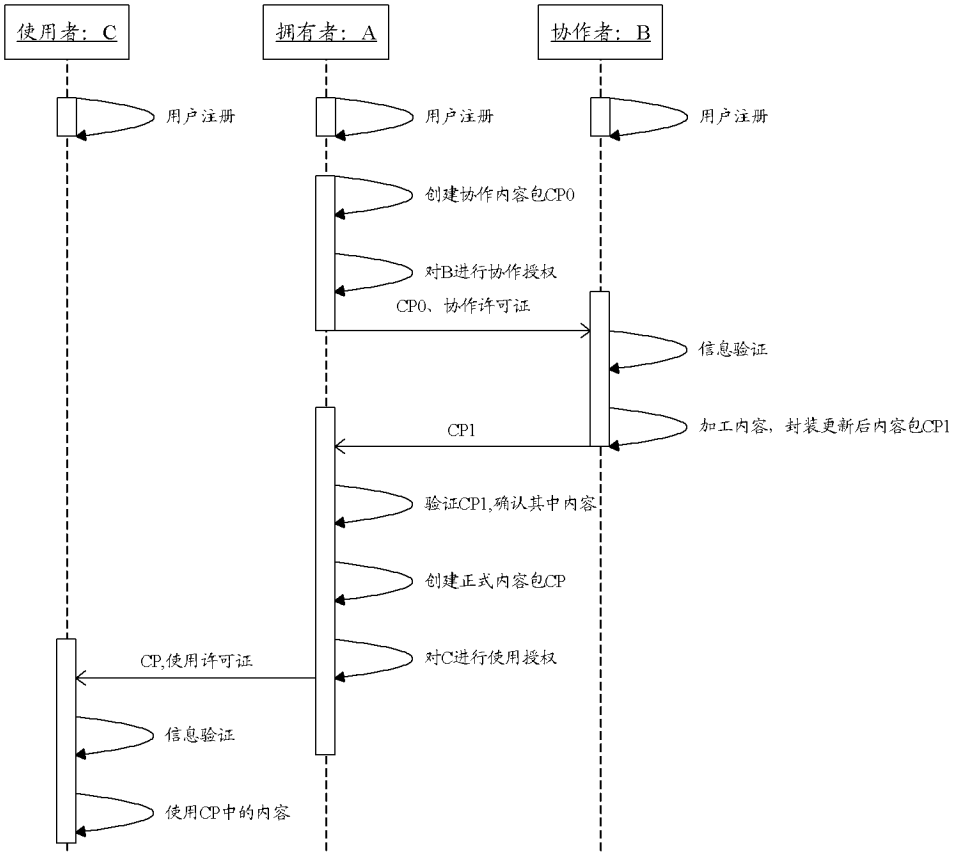

使用者: C
拥有者: A
协作者: B
用户注册
用户注册
用户注册
创建协作内容包CP0
对B进行协作授权
CP0、协作许可证
信息验证
CP1
加工内容，封装更新后内容包CP1
验证CP1,确认其中内容
创建正式内容包CP
CP,使用许可证
对C进行使用授权
信息验证
使用CP中的内容

图 2A

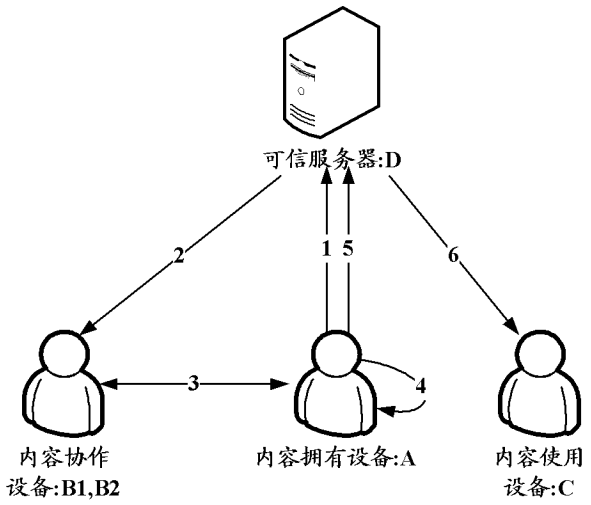

可信服务器:D
2
1 5
6
3
4
内容协作
设备:B1,B2
内容拥有设备:A
内容使用
设备:C

图 2B

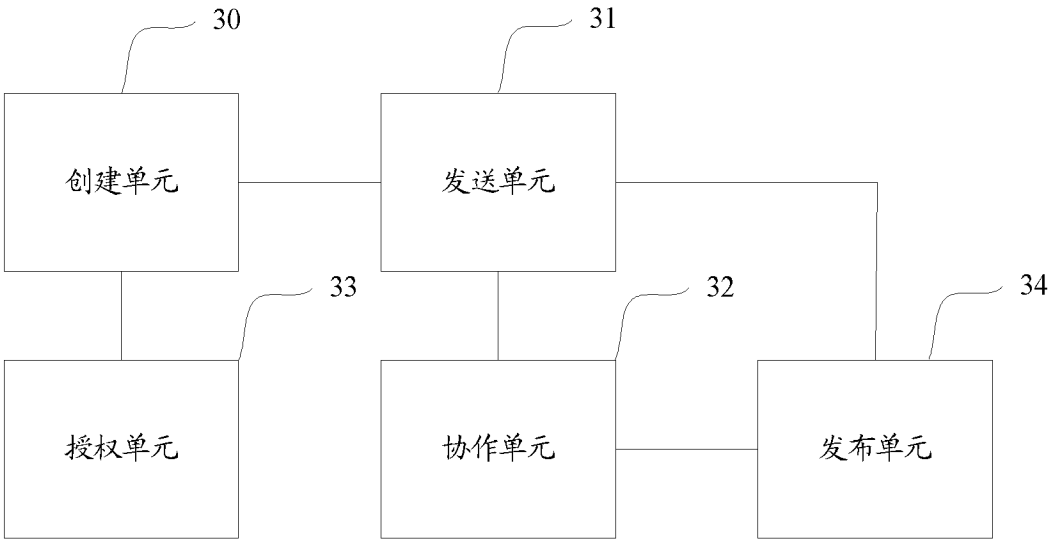

30
31
创建单元
发送单元
33
32
34
授权单元
协作单元
发布单元

图 3

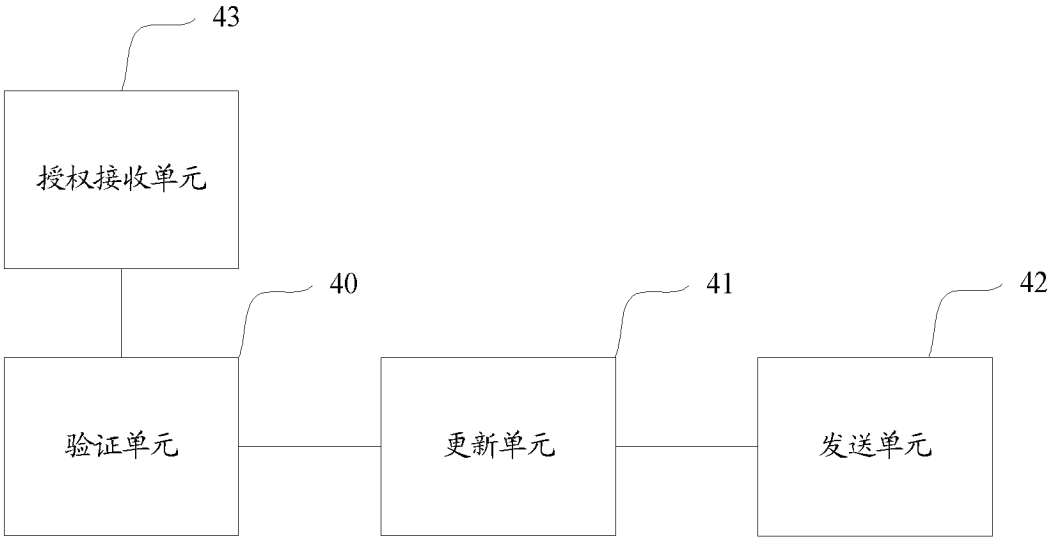


图 4