[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710179936.5

[43] 公开日 2008 年 8 月 27 日

[11] 公开号 CN 101252432A

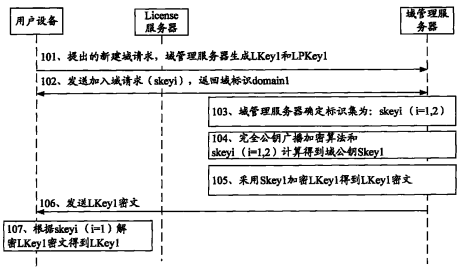
[22] 申请日 2007.12.19
[21] 申请号 200710179936.5
[71] 申请人 北大方正集团有限公司
地址 100871 北京市海淀区成府路 298 号中关村方正大厦 513
共同申请人 北京方正阿帕比技术有限公司
北京大学
[72] 发明人 高 飞 俞银燕 汤 帜 洪献文
[74] 专利代理机构 北京同达信恒知识产权代理有限公司
代理人 郭润湘
权利要求书 4 页 说明书 9 页 附图 3 页

[54] 发明名称

一种基于域的数字权限管理方法、域管理服务器及系统

[57] 摘要

本发明公开了一种基于域的数字权限管理方法、域管理服务器及系统，为了解决 License 解密密钥密文不能在域内设备间拷贝使用的问题，通过多元素加密单元素解密的加密算法，利用设备标识集计算得到域公钥，加密 License 解密密钥得到 License 解密密钥密文，任一域设备可使用本身标识恢复 License 解密密钥，非域设备则不可。 由于使用多元素加密单元素解密的加密算法，直接从设备标识集计算域公钥来保护 License 密钥，License 解密密钥密文对于任一域设备可共享使用，保证了 License 解密密钥能且仅能在域内设备间拷贝使用，解决了不方便联网设备获取 License 解密密钥不便的问题。



1、一种基于域的数字权限管理方法，其特征在于，包括:

域管理服务器建立域，生成使用证书解密密钥，并将至少两用户设备加入到域中;

域管理服务器获取用户设备标识集，所述用户设备标识集为加入到域中的全部用户设备的用户设备标识的集合;

域管理服务器通过多元素加密单元素解密的加密算法和用户设备标识集计算得到域公钥;

域管理服务器采用域公钥加密使用证书解密密钥得到使用证书解密密钥密文，并发送给用户设备;

域中的任一用户设备根据其用户设备标识，解密使用证书解密密钥密文得到使用证书解密密钥。

2、如权利要求 1 所述的方法，其特征在于，所述由多元素加密单元素解密的加密算法为完全公钥广播加密算法。

3、如权利要求 2 所述的方法，其特征在于，域管理服务器随机生成反单向函数链，从中取出一个密钥作为使用证书解密密钥。

4、如权利要求 3 所述的方法，其特征在于，

域管理服务器建立域，生成使用证书解密密钥，并将至少两用户设备加入到域中的步骤后还包括:

域管理服务器根据使用证书解密密钥生成使用证书加密密钥;

用户设备向使用证书服务器请求获取用于加密数字内容的内容密钥;

使用证书服务器向域管理服务器请求获取使用证书加密密钥;

使用证书服务器根据使用证书加密密钥加密内容密钥得到内容密钥密文;

使用证书服务器将内容密钥密文发送给用户设备;

在域中的任一用户设备根据其用户设备标识，解密使用证书解密密钥密文得到使用证书解密密钥的步骤后还包括:

用户设备采用使用证书解密密钥解密内容密钥密文得到内容密钥;

用户设备使用内容密钥解密内容密文获得数字内容。

5、如权利要求 1 至 4 中任一权利要求所述的方法，其特征在于，当有新的临时用户设备加入域时，使用该临时用户设备标识加密使用证书解密密钥，得到使用证书解密密钥临时密文;

设定使用证书解密密钥临时密文在临时设备中的使用时限;

临时用户设备根据其用户设备标识解密使用证书解密密钥临时密文得到使用证书解密密钥;

当使用时限到达后，使用证书解密密钥临时密文被无效，临时用户设备退出域。

6、如权利要求 1 至 4 中任一权利要求所述的方法，其特征在于，当有新的非临时用户设备加入域时，域管理服务器更新用户设备标识集并重新计算域公钥。

7、如权利要求 3 或 4 所述的方法，其特征在于，当有非临时用户设备退出域时，域管理服务器更新用户设备标识集并重新计算域公钥;

域管理服务器从反单向函数链中取出下一个密钥更新使用证书解密密钥;

域管理服务器使用新计算的域公钥加密新的使用证书解密密钥，生成新的使用证书解密密钥密文。

8、如权利要求 1 至 4 中任一权利要求所述的方法，其特征在于，域管理服务器设置使用证书解密密钥生命期，当使用证书解密密钥的存在时间超过所设置的生命期时，域管理服务器更新使用证书解密密钥。

9、如权利要求 4 所述的方法，其特征在于，域管理服务器建立至少两个域，对应每个域生成使用证书解密密钥、使用证书加密密钥和域标识;

将域标识与使用证书解密密钥密文关联后发送给用户设备;

用户设备向使用证书服务器请求获取用于加密数字内容的内容密钥的过程中，将该用户设备的域标识发送给使用证书服务器;

使用证书服务器根据该用户设备的域标识，向域管理服务器请求获取具有该用户设备域标识域的使用证书加密密钥。

10、如权利要求 9 所述的方法，其特征在于，所述用户设备标识集为具有相同域标识的全部用户设备标识的集合。

11、如权利要求 1 所述的方法，其特征在于，用户设备被动接收域管理服务器发送的使用证书解密密钥密文，并解密得到使用证书解密密钥；或

用户设备主动从域管理服务器下载使用证书解密密钥密文，并解密得到使用证书解密密钥；或

用户设备共享使用其它用户设备的使用证书解密密钥密文，并解密得到使用证书解密密钥。

12、如权利要求 1 所述的方法，其特征在于，用户设备共享使用其它用户设备的使用证书解密密钥密文具体为：

用户设备从其他设备拷贝使用证书解密密钥密文。

13、一种基于域的数字权限管理域管理服务器，其特征在于，包括：

域建立模块：用于建立域，生成使用证书解密密钥，并将至少两用户设备加入到域中；

标识集获取模块：用于获取用户设备标识集，所述用户设备标识集为加入到域中的全部用户设备的用户设备标识的集合；

域公钥计算模块：用于通过由多元素加密单元素解密的加密算法和用户设备标识集计算得到域公钥；

解密密钥加密模块：用于采用域公钥加密使用证书解密密钥得到使用证书解密密钥密文，并发送给用户设备。

14、一种基于域的数字权限管理系统，其特征在于，包括：

域建立模块：用于建立域，生成使用证书解密密钥，并将至少两用户设备加入到域中；

标识集获取模块：用于获取用户设备标识集，所述用户设备标识集为加入

到域中的全部用户设备的用户设备标识的集合;

域公钥计算模块：用于通过由多元素加密单元素解密的加密算法和用户设备标识集计算得到域公钥;

解密密钥加密模块：用于采用域公钥加密使用证书解密密钥得到使用证书解密密钥密文，并发送给用户设备;

解密密钥解密模块：用于域中的任一用户设备根据其用户设备标识，解密使用证书解密密钥密文得到使用证书解密密钥。

一种基于域的数字权限管理方法、域管理服务器及系统

技术领域

本发明属于DRM（digital right management）数字权限管理系统领域，特别涉及一种基于域的数字权限管理方法、域管理服务器及系统。

背景技术

DRM的用户易用性一直是阻碍DRM广泛应用的很大障碍，而这个障碍很大程度又体现在由于加密内容同设备的绑定带来的用户多设备方便共享问题上。因此出现了基于域（即将用户的多设备、甚至多用户的多设备视为一个域）的解决方案。

但现有基于域的方案存在以下问题：域证书中的License（使用证书）解密密钥密文不能在域内设备间拷贝使用，给不方便联网设备获取License解密密钥密文带来不便。

发明内容

为了解决域证书中的License解密密钥密文不能在域内设备间拷贝使用，给不方便联网设备获取License解密密钥密文带来不便的问题，本发明实施例提供了一种基于域证书共享的数字权限管理方法，包括：

域管理服务器建立域，生成使用证书解密密钥，并将至少两用户设备加入到域中；

域管理服务器获取用户设备标识集，所述用户设备标识集为加入到域中的全部用户设备的用户设备标识的集合；

域管理服务器通过多元素加密单元素解密的加密算法和用户设备标识集计算得到域公钥；

域管理服务器采用域公钥加密使用证书解密密钥得到使用证书解密密钥密文，并发送给用户设备；

域中的任一用户设备根据其用户设备标识，解密使用证书解密密钥密文得到使用证书解密密钥。

同时本发明实施例还提供一种基于域的数字权限管理域管理服务器，包括：

域建立模块：用于建立域，生成使用证书解密密钥，并将至少两用户设备加入到域中；

标识集获取模块：用于获取用户设备标识集，所述用户设备标识集为加入到域中的全部用户设备的用户设备标识的集合；

域公钥计算模块：用于通过由多元素加密单元素解密的加密算法和用户设备标识集计算得到域公钥；

解密密钥加密模块：用于采用域公钥加密使用证书解密密钥得到使用证书解密密钥密文，并发送给用户设备。

同时本发明实施例还提供一种基于域的数字权限管理系统，包括：

域建立模块：用于建立域，生成使用证书解密密钥，并将至少两用户设备加入到域中；

标识集获取模块：用于获取用户设备标识集，所述用户设备标识集为加入到域中的全部用户设备的用户设备标识的集合；

域公钥计算模块：用于通过由多元素加密单元素解密的加密算法和用户设备标识集计算得到域公钥；

解密密钥加密模块：用于采用域公钥加密使用证书解密密钥得到使用证书解密密钥密文，并发送给用户设备；

解密密钥解密模块：用于域中的任一用户设备根据其用户设备标识，解密使用证书解密密钥密文得到使用证书解密密钥。

由上述本发明提供的具体实施方案可以看出，正是由于通过多元素加密单

元素解密的加密算法，直接利用域内各个用户设备的标识信息计算域公钥，进而利用该公钥加密License解密密钥，得到License解密密钥密文的解决方案，使得任一域设备可使用本身标识信息恢复License解密密钥，非域设备则不可。通过多元素加密单元素解密的加密算法，从域内各个成员设备的标识信息计算域公钥来加密License解密密钥，保证了License解密密钥密文可在域内设备间拷贝使用，解决了不方便联网设备获取License解密密钥密文不便的问题。

附图说明

图 1 为 DRM 系统整体结构图；

图 2 为本发明提供的第一实施例方法流程图；

图 3 为本发明提供的第二实施例方法流程图；

图 4 为本发明提供的第三实施例域管理服务器结构图；

图 5 为本发明提供的第四实施例系统结构图。

具体实施方式

DRM 系统整体结构如图 1 所示，包括 License 服务器（使用证书服务器）、内容服务器、域管理服务器和用户设备，它们之间通过网络连接，其中用户设备包括用户甲的 PC 以及便携式阅读器，用户乙的笔记本电脑。其中域管理服务器用于实现域管理功能，包括域的建立、更新、域公钥的产生、更新等。所述域管理服务器需要能同 license 服务器进行通讯。该域管理服务器可独立于 DRM 系统，并对一个或多个 DRM 系统提供可信的域管理服务。

本发明提供的第一实施例是一种基于域证书共享的数字权限管理方法，方法流程如图 2 所示，包括：

步骤 101：域管理服务器接收到用户甲通过其 PC 提出的新建域请求，并产生一个唯一的域标识 domain1（若域管理服务器只管理一个域则不需要域标识），并随机生成反单向函数链，从中取出第一个数作为该域的 License 解密密钥 LKey1，根据 LKey1 产生相应的 License 加密密钥 LPKey1。然后进一步根

据与用户的协商建立相应的域规则，如：允许加入域的用户设备数为 4、变更次数为 3、临时设备数为 2 等等。

域管理服务器在接收到新建域请求后，为用户甲分配一个用户名：user1，和一个密码：123456，该新建域操作也可在用户将设备第一次添加到域时完成。

随机生成反单向函数链，从中取出第一个数作为该域的 License 解密密钥 LKey1，只是生成 License 解密密钥 LKey1 的一个优选的方案，在本实施例中也可采用其它方式生成 License 解密密钥，如：随机生成一个密钥作为 License 解密密钥 LKey1，同样根据 LKey1 产生相应的 License 加密密钥 LPKey1。

步骤 102：将 PC 以及便携式阅读器注册（通过用户特征设备，如智能卡等）到域管理服务器，即执行发送加入域请求。域管理服务器将 PC 以及便携式阅读器加入到 domain1 域中。注册时将根据 PC 机的主板号、CPU 号和硬盘号产生的 PC 机的标识 skeyi （i=1）发送给域管理服务器，同时将便携式阅读器的标识 skeyi （i=2），发送给域管理服务器。

具体实施时，用户甲通过 PC 机上的注册软件输入用户名：user1，和对应密码：123456，请求将 PC 机加入 domain1 域，管理服务器验证用户名 user1 和密码 123456 通过后将 PC 加入到 domain1 域中，并将 domain1 域的域标识 domain1 告知 PC。

加入域的过程中，用户甲不容易联网的便携式阅读器，将 PC 机作为便携式阅读器的注册代理，通过 PC 机上的注册软件输入用户名：user1，和对应密码：123456，请求将 PC 机代理的便携式阅读器加入 domain1 域，或者对于用户甲不容易联网的便携式阅读器可以产生一个 ticket，通过 PC 机将 ticket 提交，来代替注册请求，至于通过 ticket 的具体实现方法属于现有技术，此处不再赘述。

加入域的过程中，域管理服务器在收到 PC 机以及便携式阅读器加入域请求后，验证该请求是否满足域规则，如是否已达到域允许的设备数上限 4，因为 PC 机和便携式阅读器分别为第一个和第二个申请加入域的设备，判断它们

满足规则再进行后续步骤。

步骤 103：域管理服务器确定标识集为：skeyi （i=1,2）。

步骤 104：域管理服务器通过多元素加密单元素解密的加密算法和 skeyi（i=1,2）计算得到域公钥 Skey1。多元素加密单元素解密的加密算法在本实施例中优选使用完全公钥广播加密算法。多元素加密单元素解密的加密算法就是加密时使用多个元素而解密时只使用其中的一个元素解密，如使用 A、B 和 C 三个元素加密，解密时只使用 A、B 或 C 任意之一进行解密。典型的算法为完全公钥广播加密算法。

步骤 105：域管理服务器采用 Skey1 加密 LKey1 得到 LKey1 密文。

步骤 106：域管理服务器根据 LKey1 密文制作域证书 v1.0，将域证书 v1.0 发送给 PC 机，域证书 v1.0 中包含 LKey1 密文等。

步骤 107：PC 机根据 skeyi （i=1）解密 LKey1 密文得到 LKey1。

上述步骤中具体实施时 PC 机可以被动接收域管理服务器发送的域证书 v1.0，并解密 LKey1 密文得到 LKey1，PC 机还可以主动从域管理服务器下载域证书 v1.0，并解密 LKey1 密文得到 LKey1，对于便携式阅读器前面步骤类同，只是在步骤 106 中，可以通过拷贝 PC 机得到的 LKey1 密文的方式获取 LKey1 密文（当然也可以不拷贝 PC 机得到的 LKey1 密文，而是通过与 PC 机相连直接使用 PC 机上的 LKey1 密文，只要能达到共享使用的目的就可以）。之后步骤 107 中通过便携式阅读器的用户标识 skeyi （i=2）解密 LKey1 密文得到 LKey1。当然便携式阅读器也可以通过 PC 机连接域管理服务器（或其它方式连接域管理服务器），以下载的方式获取域证书 v1.0。

本发明提供的第二实施例是一种基于域证书共享的数字权限管理方法，方法流程如图 2 所示，其中步骤 201-步骤 207 与实施例一中的步骤 101-步骤 107 相同，还包括：

步骤 208：用户甲通过 PC 从内容服务器购买经过内容密钥 Ckey 加密的数字内容文档 1 得到内容密文 1。该步骤只要在步骤 209 之前执行即可。

步骤 209: 用户甲通过 PC 向 License 服务器发送获取内容密钥 Ckey 请求，请求获取携带 Ckey 的使用证书（即 License），用于解密使用数字内容文档 1。

步骤 210: License 服务器根据该获取 Ckey 请求向用户甲索取 PC 所在域的域标识。

步骤 211: 用户甲通过 PC 向 License 服务器发送域标识 domain1（域标识 domain1 也可在请求 license 时一同发出，则步骤 210 和步骤 211 可以省略）。

步骤 212: License 服务器向域管理服务器请求 domain1 域的 License 加密密钥（License 加密密钥与解密密钥可相同-用对称加密方法，也可不同-用非对称加密方法）。

步骤 213: 域管理服务器将 domain1 域的 License 加密密钥 LPKey1 告知 License 服务器。（此步骤也可包含对 License 服务器的验证）

步骤 214: License 服务器根据 LPKey1 加密 Ckey 构成 Ckey 密文，得到文档 1 的使用证书 license（包括 Ckey 密文）。

步骤 215: License 服务器将文档 1 的使用证书 license 返回给 PC 机。

步骤 216: PC 机通过 LKey1 解密 Ckey 密文得到 Ckey。

步骤 217: PC 机通过 Ckey 解密内容密文 1 得到数字内容文档 1。

对于便携式阅读器前面步骤类同，步骤 215 中 PC 机将 license 自由拷贝到便携式阅读器使用，或便携式阅读器通过 PC 机。这样无需便携式阅读器重新获取新的 license。

进一步在上述过程中，在用户设备加入域时，首先判断是否是临时设备的加入请求，经判断 PC 机和便携式阅读器不是临时设备，将 PC 机的 skeyi（i=1）保存到域管理服务器数据库，并与域标识 domain1 关联。然后根据 domain1 域的标识集 skeyi （i=1，2）和完全公钥广播加密算法计算出相应的公钥 Skey1，进而得到 domain1 域的 License 解密密钥密文，生成包含 License 解密密钥密文和域标识 domain1 等信息的域证书 v1.0，将域证书 v1.0 返回给 PC 机。

进一步，用户甲还有一个不是临时设备的 PDA 希望加入该域，需重新确

定用户设备标识集，重新确定的用户设备标识集，PDA 的用户设备标识 skeyi（i=3）则重新确定的用户设备标识集为：skeyi（i=1,2,3），根据 skeyi（i=1,2,3）利用完全公钥广播加密算法重新计算出相应的域公钥 Skey2，此时 License 解密密钥 Lkey1 不做更新，利用域公钥 Skey2 加密 Lkey1 得到新的 License 解密密钥密文。该 PDA 可直接拷贝 PC 机由 License 服务器获取文档 1 的使用证书 license。使用 skeyi （i=3）解密新的 License 解密密钥密文得到 LKey1，之后得到文档 1。PDA 的加入对 PC 机和便携式阅读器的使用不会带来任何影响。进一步，用户甲的便携式阅读器退出域，重新确定的用户设备标识集，重新确定的用户设备标识集为：skeyi （i=1, 3），根据 skeyi （i=1, 3）利用完全公钥广播加密算法重新计算出相应的域公钥 Skey3，选取对应反单向函数链的下一个数（第二个）作为新的 License 解密密钥 Lkey2 并替换现有的 License 解密密钥 Lkey1，其余步骤和上述过程类同，此处不再赘述。由于采用反单向函数链的方式获得 Lkey2，因此 Lkey2 可解密 LPKey1，这样对之前获得的 Ckey 密文还可以继续解密使用。若采用随机生成一个密钥作为 License 解密密钥 LKey1 的方式，则域管理服务器需要将原 License 解密密钥 LKey1 和新生成的 License 解密密钥 LKey2 一同发送给 PDA，这样 PDA 就可以解密原 License 加密密钥 LKey1。

由于便携式阅读器的退出将导致 License 解密密钥 Lkey1 更新为 Lkey2，对于更新后产生的数字内容文档 2 使用 license，旧的域证书 v1.0 中的 License 解密密钥密文将不能适用，PC 机将给予提醒，该 PC 自动完成域证书的更新，更新为 v2.0。PDA 可通过拷贝的方式将新证书 v2.0 导入。为了避免新旧证书互相导入造成混乱，证书的新旧由版本号（v1.0 为旧版本号，v2.0 为新版本号）决定。在导入证书时，域证书 v2.0 覆盖域证书 v1.0。即在已有域证书 v2.0 的情况下，域证书 v1.0 将不能导入。

进一步，若用户甲还在用他人的 PC 上网，用户甲告知域管理服务器此 PC 是临时设备，则产生一个具有时间限制的临时证书，使用临时 PC 的用户设备

标识 skeyi （i=4）加密现有的 Lkey1 生成 License 解密密钥临时密文，并将包括 License 解密密钥临时密文的临时证书返回给临时 PC。临时 PC 根据 skeyi（i=4）解密 License 解密密钥临时密文得到 Lkey1。

临时 PC 的临时证书到达时限后，临时设备由于证书有时间限制，从本地删除证书即可，无需执行退出域操作。

进一步，域管理服务器接收到用户乙通过其笔记本电脑新建域请求，产生一个唯一的域标识 domain2，随机生成一个新的反单向函数链，从中取出第一个密钥作为 domain2 域的 License 解密密钥 LKey1'，笔记本电脑申请注册到 domain2 域中，管理服务器将笔记本电脑加入到 domain2 域中。后续的加解密过程与前述过程类同此处不再赘述。

本发明提供的第三实施例是一种基于域的数字权限管理域管理服务器，其结构如图 4 所示，包括:

域建立模块 310: 用于建立域，生成 License 解密密钥，并将至少两用户设备加入到域中;

标识集获取模块 320: 用于获取用户设备标识集，所述用户设备标识集为加入到域中的全部用户设备的用户设备标识的集合;

域公钥计算模块 330: 用于通过由多元素加密单元素解密的加密算法和用户设备标识集计算得到域公钥;

解密密钥加密模块 340: 用于采用域公钥加密 License 解密密钥得到 License 解密密钥密文，并发送给用户设备。

本发明提供的第四实施例是一种基于域的数字权限管理系统，其结构如图 5 所示，包括:

域建立模块 310: 用于建立域，生成 License 解密密钥，并将至少两用户设备加入到域中;

标识集获取模块 320: 用于获取用户设备标识集，所述用户设备标识集为加入到域中的全部用户设备的用户设备标识的集合;

域公钥计算模块 330：用于通过由多元素加密单元素解密的加密算法和用户设备标识集计算得到域公钥；

解密密钥加密模块 340：用于采用域公钥加密 License 解密密钥得到 License 解密密钥密文，并发送给用户设备；

解密密钥解密模块 350：用于域中的任一用户设备根据其用户设备标识，解密 License 解密密钥密文得到 License 解密密钥。

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。

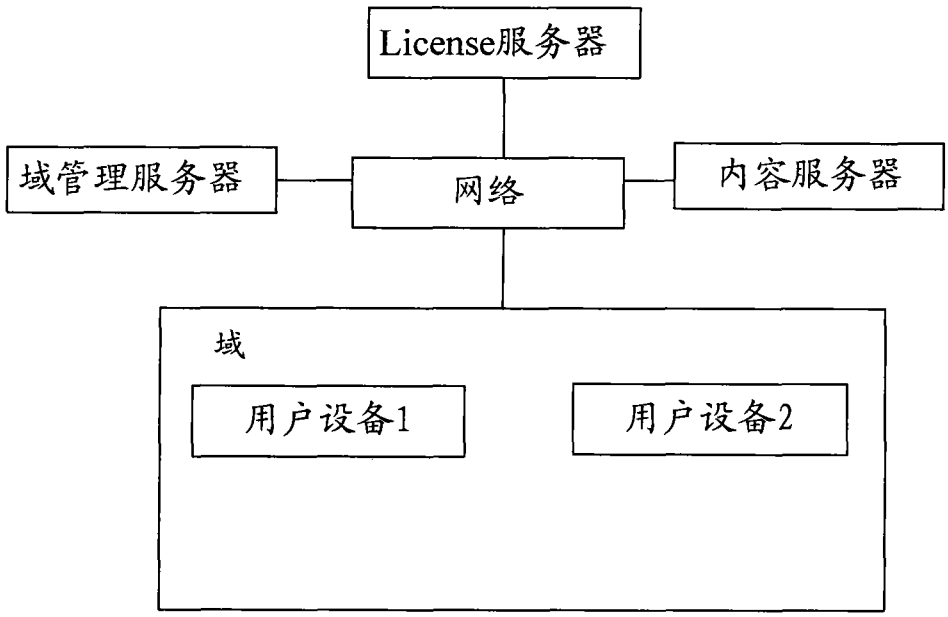

License服务器
域管理服务器
网络
内容服务器
域
用户设备1
用户设备2

图 1

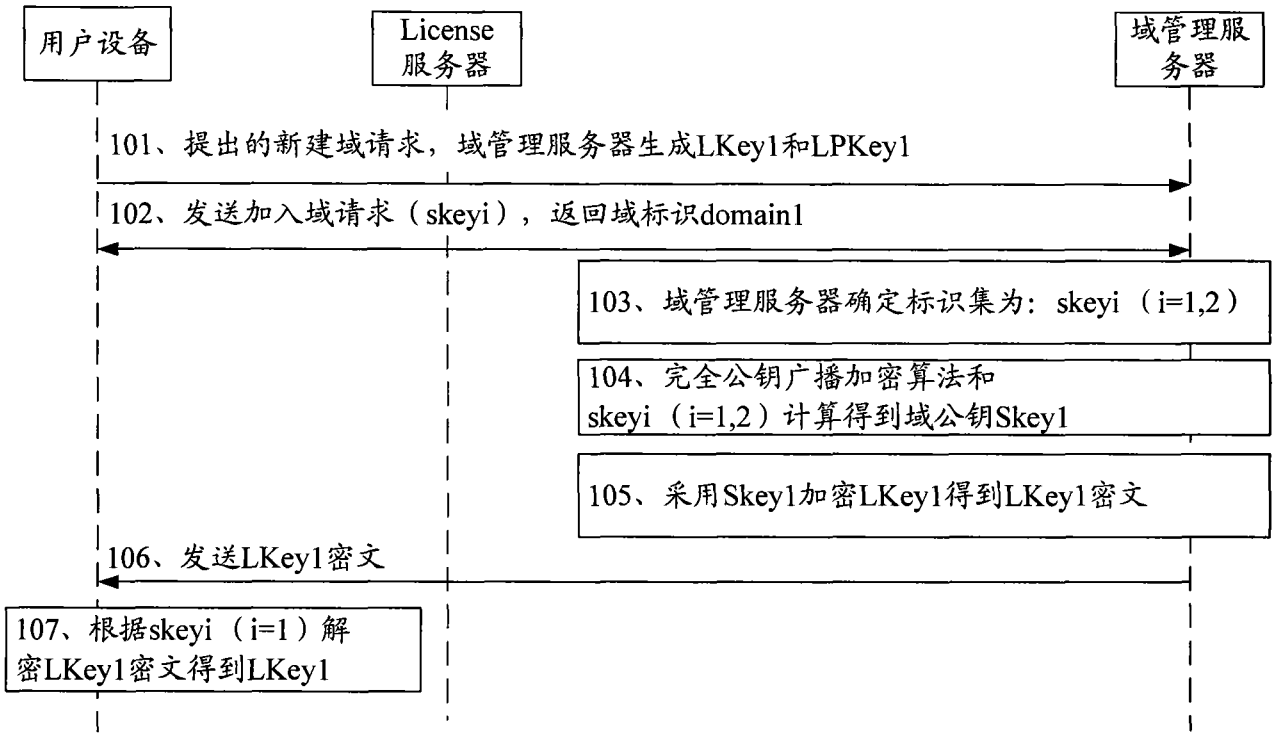

用户设备
License 服务器
域管理服务器
101、提出的新建域请求，域管理服务器生成LKey1和LPKey1
102、发送加入域请求（skeyi），返回域标识domain1
103、域管理服务器确定标识集为：skeyi （i=1,2）
104、完全公钥广播加密算法和 skeyi （i=1,2）计算得到域公钥Skey1
105、采用Skey1加密LKey1得到LKey1密文
106、发送LKey1密文
107、根据skeyi （i=1）解密LKey1密文得到LKey1

图 2

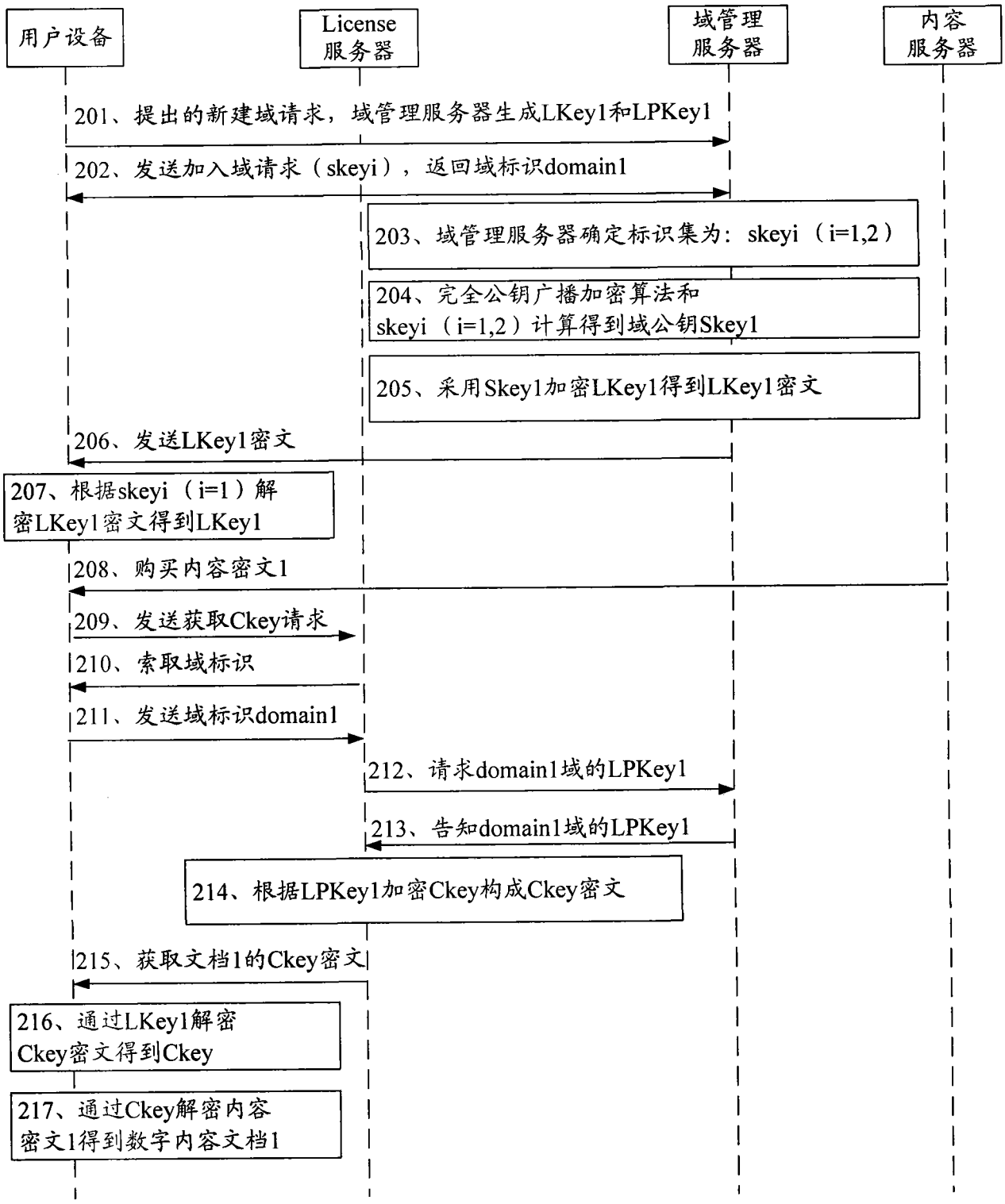

用户设备
License 服务器
域管理 服务器
内容 服务器
201、提出的新建域请求，域管理服务器生成LKey1和LPKey1
202、发送加入域请求（skeyi），返回域标识domain1
203、域管理服务器确定标识集为：skeyi（i=1,2）
204、完全公钥广播加密算法和 skeyi（i=1,2）计算得到域公钥Skey1
205、采用Skey1加密LKey1得到LKey1密文
206、发送LKey1密文
207、根据skeyi（i=1）解密LKey1密文得到LKey1
208、购买内容密文1
209、发送获取Ckey请求
210、索取域标识
211、发送域标识domain1
212、请求domain1域的LPKey1
213、告知domain1域的LPKey1
214、根据LPKey1加密Ckey构成Ckey密文
215、获取文档1的Ckey密文
216、通过LKey1解密 Ckey密文得到Ckey
217、通过Ckey解密内容 密文1得到数字内容文档1

图 3

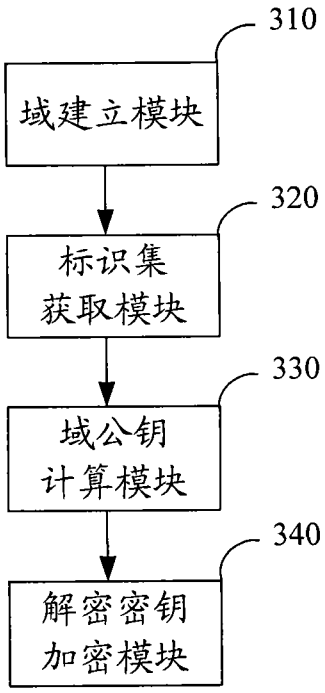

310
域建立模块
320
标识集
获取模块
330
域公钥
计算模块
340
解密密钥
加密模块

图 4

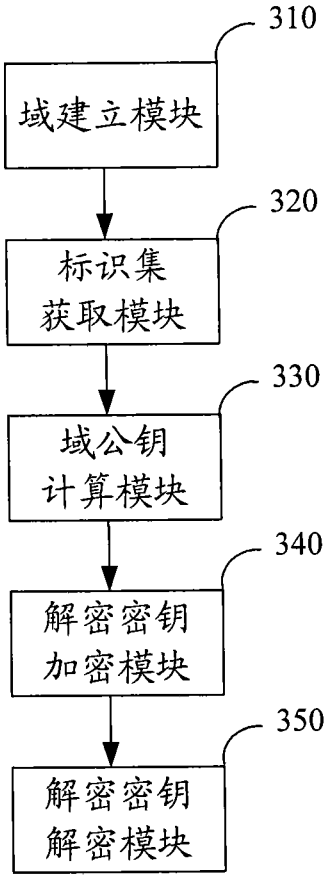

310
域建立模块
320
标识集
获取模块
330
域公钥
计算模块
340
解密密钥
加密模块
350
解密密钥
解密模块

图 5