



(12) 发明专利申请

(10) 申请公布号 CN 101729558 A

(43) 申请公布日 2010. 06. 09

(21) 申请号 200910225395. 4

H04L 9/08 (2006. 01)

(22) 申请日 2006. 04. 25

G06F 21/00 (2006. 01)

(30) 优先权数据

10-2005-0065669 2005. 07. 20 KR

60/674, 333 2005. 04. 25 US

(62) 分案原申请数据

200680014085. 2 2006. 04. 25

(71) 申请人 三星电子株式会社

地址 韩国京畿道水原市

(72) 发明人 金奉禅 金明宣 韩声休 尹映善

李善男 李栽兴

(74) 专利代理机构 北京铭硕知识产权代理有限公司 11286

代理人 郭鸿禧 李娜娜

(51) Int. Cl.

H04L 29/06 (2006. 01)

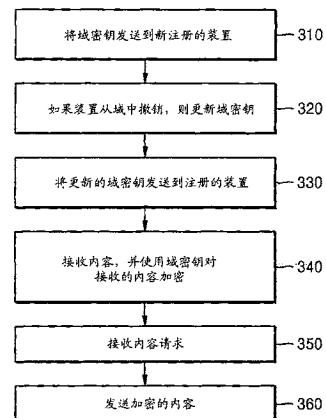
权利要求书 1 页 说明书 7 页 附图 10 页

(54) 发明名称

域管理的方法和设备

(57) 摘要

提供一种域管理的方法和设备。如果在域中注册的装置从所述域撤销，则将在所述装置撤销之前在所述域中使用的域密钥更新为不能由所述装置使用的域密钥；和将未暴露给所述装置的域密钥发送到当前在域中注册的多个装置，从而仅当前注册的装置具有最新域密钥。因此，可以防止未在域中注册的装置和先前在所属域中注册但又从所属域中撤销的装置使用当前在域中共享的数字内容。此外，已经从所属域中撤销的曾经注册的装置可以使用在其从域中撤销之前合法地从所属域中下载的数字内容。



1. 一种在域中注册装置的方法,包括:
向域管理设备发出在域中注册装置的请求;和
接收使用装置的公有密钥加密的所述域的当前域密钥和所有域密钥。
2. 如权利要求1所述的方法,还包括将装置的公有密钥发送到域管理设备。

域管理的方法和设备

[0001] 本申请是申请日为 2006 年 4 月 25 日、申请号为 200680014085.2、题为“域管理的方法和设备”的专利申请的分案申请。

技术领域

[0002] 根据本发明的设备和方法涉及域管理,更具体的说,涉及保护域中的数字内容。

背景技术

[0003] 近年来,经诸如因特网、陆地波、线缆和卫星的各种通信媒体的数字内容传输的频率已经迅速增长,诸如压缩盘 (CD) 和数字多用盘 (DVD) 的具有大存储容量的记录介质上的数字内容的出售和租赁也迅速增长。因此,作为数字内容版权保护方案的数字权限管理受到了比以往更高的关注。具体来说,已经大力地进行了对这样一种方法的开发研究,即,所述方法允许经属于所属域 (home domain) 的装置为该所属域的合法用户自由地提供各种内容服务。根据这种方法,属于相同域的装置 (例如,数字电视和 PDA) 可彼此共享他们的内容。

[0004] 期望的是通过以下方式来保护域中的内容,即,仅允许在域内注册的装置使用内容,防止未在域内注册的装置或者曾经在域内注册但已经从域中撤销的装置使用内容,以及允许曾经注册的装置使用在其从域中撤销之前已经合法地从域中下载的内容。然而,还没有开发出以这种方式保护域中的内容的技术。

发明内容

[0005] 本发明提供以下所述的一种域管理设备和方法,所述设备和方法能够仅使当前在域中注册的装置使用在域中共享的数字内容,并能够使曾经在域内注册但已经从域中撤销的装置使用在其从域中撤销之前已经合法地从域中下载的数字内容。

[0006] 根据本发明,通过仅在当前在所属域中注册的装置之间共享域密钥可以防止尚未在所属域中注册的装置使用在所属域中共享的数字内容,并且先前在所属域中注册但已经从所属域中撤销的装置仅可以使用在其从所属域中撤销之前已经合法地从所述所属域中下载的数字内容。因此,可以仅在当前注册的装置之间共享数字内容的方式对域进行有效管理。

[0007] 根据本发明的一方面,提供了一种域管理方法,所述域管理方法管理使用作为由在所属域中注册的多个装置共享的解密密钥的域密钥的至少一个装置。所述域管理方法包括:如果在所属域中注册的装置从所属域撤销,则将在所述装置撤销之前曾经使用的第一域密钥更新为未暴露给所述装置的第二域密钥;和将第二密钥发送到在域中注册的多个装置。

[0008] 域管理方法还可包括,在更新步骤之后如果从域的外部接收到内容,则以只能使用第二域密钥对加密的内容解密的方式来对所述内容加密;和将加密的内容发送到请求所述内容的装置。

[0009] 域管理方法还可包括，在更新步骤之后将第一域密钥和第二域密钥发送到在所属域中注册的装置。

[0010] 根据本发明的另一方面，提供了一种存储用于执行所述域管理方法的计算机程序的计算机可读记录介质。

[0011] 根据本发明的另一方面，提供了一种域管理设备，所述域管理设备使用作为由在所属域中注册的多个装置共享的解密密钥的域密钥的至少一个装置。所述域管理设备包括：域密钥更新单元，如果在所属域中注册的装置从所属域撤销，则将在所述装置撤销之前使用的第一域密钥更新为未暴露给所述装置的第二域密钥；和域密钥发送单元，如果域密钥更新单元更新所述域密钥，则域密钥发送单元将更新的域密钥发送到在域中注册的多个装置。

附图说明

[0012] 图 1 是示出根据本发明示例性实施例的链接信息的格式的示图；

[0013] 图 2 是示出根据本发明示例性实施例的内容信息的格式的示图；

[0014] 图 3 是示出根据本发明示例性实施例的域管理方法的流程图；

[0015] 图 4 是示出根据本发明示例性实施例的当第一装置在所属域中注册时的信息流的示图；

[0016] 图 5 是示出根据本发明示例性实施例的当第二装置在所属域中注册时的信息流的示图；

[0017] 图 6 是示出根据本发明示例性实施例的方法的示图，通过所述方法根据本发明示例性实施例的域管理设备接收第一内容，并将第一内容提供给在所属域中注册的装置；

[0018] 图 7 是示出根据本发明示例性实施例的当在所属域中注册的第一装置从所属域中撤销时的信息流的示图；

[0019] 图 8 是示出根据本发明示例性实施例的方法的示图，通过所述方法域管理设备接收第二内容，并将该内容提供给还在所属域中注册的第二装置；

[0020] 图 9 是示出根据本发明示例性实施例的当第三装置在所属域中注册时的信息流的示图；

[0021] 图 10 是示出根据本发明示例性实施例的当第四装置在所属域中注册时的信息流的示图；

[0022] 图 11 是示出根据本发明示例性实施例的域管理设备的框图。

具体实施方式

[0023] 图 1 是示出根据本发明示例性实施例的链接信息的格式的示图。

[0024] 根据本发明示例性实施例的域管理设备使用多个在所属域中注册的装置的每一个的基于公开密钥基础设施 (PKI) 的公有密钥对作为在所属域中共享的解密密钥的域密钥加密，从而产生链接信息。此后，域管理设备存储链接信息，并将所述链接信息发送到在所属域中注册的装置。参照图 1，链接信息包括：有效性比特字段 110、主 (major) 版本字段 120、次 (minor) 版本字段 130 和链接数据字段 140。有效性比特字段 110 指示该链接信息是否是最新的链接信息。通过确定包括在链接数据 140 中的域密钥是否正在传播中来确定

所述链接信息是否是最新的链接信息。

[0025] 主版本字段 120 指示包括在链接数据 140 中的域密钥的版本。每当装置从所属域中撤销时主版本字段 120 的值增加。次版本字段 130 也指示包括在链接数据 140 中的域密钥的版本。每当装置在所属域中注册时次版本字段 130 的值增加。因此,根据本发明示例性实施例的域管理设备可参照多条链接信息的次版本字段值来确定具有相同主版本字段值的多条链接信息中的哪一条是最新的链接信息。

[0026] 链接数据 140 包括使用当前在所属域中注册的多个装置的公有密钥的每一个加密的域密钥。因此,当前在所属域中注册的装置可通过接收链接数据 140 并使用其各自的私有密钥对链接数据 140 解密来恢复域密钥。每当主版本字段 120 的值或者次版本字段 130 的值改变时,即,每当除了当前在所属域中注册的装置之外的装置在所属域中注册,或者每当当前在所属域中注册的装置之一从所属域中撤销时,根据本发明示例性实施例的域管理设备根据主版本字段 120 或者次版本字段 130 中的改变更新所有链接信息,并随后将更新的链接信息发送到当前在所属域中注册的装置的每一个,从而保持最新的关于当前在所属域中注册的装置的装置信息和域密钥信息。

[0027] 图 2 是示出根据本发明示例性实施例的内容信息的格式的示图。参照图 2,内容信息包括:版本字段 210 和内容字段 220。版本字段 210 与图 1 的主版本字段 120 相似,指示域密钥的版本。当根据本发明示例性实施例的域管理设备从外部源接收数字内容时,将接收数字内容时正在传播中的所属域密钥的版本记录在版本字段 210 中。内容字段 220 包括通过对数字内容加密获得并可使用所属域密钥解密的加密数据。因此,合法装置可通过接收内容信息并使用所属域密钥对包括在内容信息的内容字段 220 中的加密数据解密来恢复数字内容。

[0028] 图 3 是示出根据本发明示例性实施例的域管理方法的流程图。参照图 3,在操作 310,当装置在所属域中注册时,根据本发明示例性实施例的域管理设备通过使用新注册装置的公有密钥对当前域密钥加密来产生链接信息,并将链接信息发送到新注册的装置。在操作 310,如果存在低于当前域密钥的版本的域密钥(以下称为前域密钥),则域管理设备还可将前域密钥与当前域密钥一起发送到新注册的装置,从而使新注册的装置能够使用存储在域管理设备中的所有数字内容。

[0029] 在操作 320,如果在所属域中注册的多个装置中的一个从所属域中撤销,则域管理设备更新当前域密钥,并在操作 330 将更新的域密钥发送到其余的注册装置,从而在注册的装置中保持最新的当前域密钥。此后,在操作 340,如果域管理设备从外部源接收数字内容,则域管理设备使用在接收数字内容时正在传播中的域密钥对所述数字内容加密。在操作 350,如果注册的装置向域管理设备发出对数字内容的请求,则在操作 360 域管理设备将加密的数字内容发送到所述注册的装置。随后,注册的装置可使用该注册的装置持有的域密钥对加密的数字内容解密。

[0030] 图 4 是示出根据本发明示例性实施例的当装置 A(410) 被注册在所属域中时的信息流的示图。参照图 4,装置 A(410) 通过将装置 A(410) 的公有密钥 pub_conf_dev_A 发送到域管理设备(400) 向域管理设备 400 发出在所属域中注册装置 A(410) 的请求。随后,域管理设备 400 使用公有密钥 pub_conf_dev_A 对域密钥 priv_shar_user1 加密,并产生装置 A 的链接信息,所述链接信息包括:有效性比特字段,其中记录了字符“C”,指示加密的域

密钥 priv_shar_user1 是最新的域密钥 ; 和主版本字段, 其中将值 1 记录为加密的域密钥 priv_shar_user1 的版本信息。域管理设备 400 将所述链接信息发送到装置 A(410), 装置 A(410) 接收并存储所述链接信息。因此, 只能由装置 A(410) 使用装置 A(410) 的私有密钥对加密的域密钥 priv_shar_user1 解密。

[0031] 图 5 是示出根据本发明示例性实施例的当在装置 A(410) 已经在所属域中注册之后装置 B(420) 在所属域中注册时的信息流的示图。参照图 5, 装置 B(420) 通过将装置 B(420) 的公有密钥 pub_conf_dev_B 发送到域管理设备 400 来向域管理设备 400 发出在所属域中注册的请求。然后, 域管理设备 400 产生装置 B(420) 的链接信息。随后, 域管理设备 400 将装置 B(420) 的链接信息添加到装置 A(410) 的链接信息, 并同时将装置 A(410) 的链接信息和装置 B(420) 的链接信息的次版本字段值增加 1。简短来说, 根据本发明的当前实施例, 当装置在域中注册时, 链接信息的主版本字段值和域密钥不改变 ; 只有链接信息的次版本字段值增加。此后, 域管理设备 400 将装置 A(410) 的链接信息和装置 B(420) 的链接信息发送到所有注册的装置 (即, 装置 A(410) 和装置 B(420))。因此, 装置 B(420) 也可使用装置 B(420) 的私有密钥对加密的域密钥 priv_shar_user1 解密。

[0032] 图 6 是示出根据本发明示例性实施例的域管理设备 400 接收第一内容 401 并将第一内容 401 提供给所有注册的装置 (即, 装置 A(410) 和装置 B(420)) 的方法的示图。参照图 6, 域管理设备 400 从外部源接收第一内容 401, 使用作为第一内容 401 的对称密钥的内容密钥 Key_content1 对第一内容 401 加密, 并使用加密密钥 pub_shar_user1 对内容密钥 Key_content1 加密, 从而产生内容信息 402。这里, 仅可使用当接收第一内容 401 时在传播中的所属域密钥 (即, 域密钥 priv_shar_user1) 对加密密钥 pub_shar_user1 解密。如上所述, 内容信息 402 的版本与域密钥 priv_shar_user1 的版本相同, 因此所述版本为 1。

[0033] 此后, 当装置 A(410) 和装置 B(420) 请求时, 域管理设备 400 将内容信息 402 发送到装置 A(410) 和装置 B(420)。因此, 所有注册的装置 (即, 装置 A(410) 和装置 B(420)) 可通过使用装置 A(410) 和装置 B(420) 的私有密钥分别对包括在装置 A(410) 的链接信息和装置 B(420) 的链接信息中的加密的域密钥 priv_shar_user1 解密, 使用解密的域密钥 priv_shar_user1 对加密的内容密钥 pub_shar_user1 解密, 和使用解密的内容密钥 pub_shar_user1 对加密的第一内容 401 解密, 来恢复第一内容 401。

[0034] 加密密钥 pub_shar_user1 可以是基于 PKI 的公有密钥, 域密钥 priv_shar_user1 可以是相应于加密密钥 pub_shar_user1 的基于 PKI 的私有密钥。然而, 本发明不限于此。换句话说, 本发明可被应用于加密密钥 pub_shar_user1 与域密钥 priv_shar_user1 相同的情况, 即, 域密钥 priv_shar_user1 是对称密钥。

[0035] 图 7 是示出根据本发明示例性实施例的当图 6 所示的在所属域中注册的装置 A(410) 从所述所属域中撤销时的信息流的示图。参照图 7, 当装置 A(410) 从所属域中撤销时, 域管理设备 400 删除装置 A(410) 的链接信息, 并更新域密钥 priv_shar_user1, 从而获得域密钥 priv_shar_user2。

[0036] 域管理设备 400 将仍为在所属域中注册的装置 B(420) 的链接信息的有效性比特字段中记录的字符“C”替换为字符“P”, 字符“P”指示装置 B(420) 的链接信息已经不再是最新的链接信息, 并使用装置 B(420) 的公有密钥 pub_conf_dev_B 对域密钥 priv_shar_user2 加密, 从而产生装置 B(420) 的新的链接信息。因此, 将字符“C”记录在装置 B(420) 的新的

链接信息的有效性比特字段中。因为域密钥 `priv_shar_user1` 被更新为域密钥 `priv_shar_user2`, 所以装置 B 的新的链接信息的主版本字段值是 2, 简短来说, 根据本发明当前示例性实施例, 每当注册的装置从域中撤销时, 链接信息的主版本字段值增加 1, 而链接信息的次版本字段值被重设为 0。

[0037] 域管理设备 400 将装置 B(420) 的新的链接信息发送到装置 B(420), 并且装置 B(420) 用装置 B(420) 的新的链接信息替换装置 B(420) 的旧的链接信息。

[0038] 结果, 因为可以将第一内容 401 解密的域密钥 `priv_shar_user1` 是使用装置 A(410) 的公有密钥 `pub_conf_dev_A` 加密的, 所以即使装置 A(410) 从所属域中撤销, 其仍可使用从所属域中合法下载的数字内容 (即, 第一内容 401)。然而, 因为其他数字内容以仅可使用具有主版本字段值为 2 的域密钥 `priv_shar_user2` 解密的方式来加密, 所以装置 A(410) 不能使用在装置 A(410) 从所属域中撤销之后新接收的数字内容。另一方面, 因为装置 B(420) 持有包括加密的域密钥 `priv_shar_user1` 的装置 B(420) 的旧的链接信息和包括加密的域密钥 `priv_shar_user2` 的装置 B(420) 的新的链接信息, 所以装置 B(420) 不仅可以自由地使用第一内容 401, 还可以使用通过使用域密钥 `priv_shar_user2` 加密的其他数字内容。

[0039] 图 8 是示出根据本发明示例性实施例的在图 7 所示的情况下域管理设备 400 接收第二内容 403, 并将第二内容 403 提供给装置 B(420) 的方法的示图。参照图 8, 域管理设备 400 接收第二内容 403, 使用作为第二内容 403 的对称密钥的内容密钥 `Key_content2` 对第二内容 403 加密, 并使用加密密钥 `pub_shar_user2` 对内容密钥 `Key_content2` 加密, 以使用当接收到第二内容 403 时在传播中的域密钥 (即, 域密钥 `priv_shar_user2`) 对加密的内容密钥 `Key_content2` 解密, 从而产生内容信息 404。内容信息 404 的版本字段值与链接信息 (即, 当接收到第二内容 403 时的最新链接信息) 的主版本字段值相同, 因此所述内容信息 404 的主版本字段值为 2。当装置 B(420) 请求时, 域管理设备 400 将内容信息 404 发送到装置 B(420)。随后, 装置 B(420) 不仅可以使用第一内容 401, 还可以通过使用包括在最新链接信息中的域密钥 `priv_shar_user2` 来使用第二内容 403。

[0040] 这里, 装置 B(420) 可参照内容信息的版本字段值来确定需要域密钥 `priv_shar_user1` 还是域密钥 `priv_shar_user2` 来使用内容信息。例如, 为了使用具有版本字段值为 2 的加密的第二内容 403, 对具有主版本字段值为 2 的链接信息进行搜索, 并且使用装置 B(420) 的私有密钥对包括在发现的链接信息中的加密的域密钥 `priv_shar_user2` 解密。此后, 使用解密的域密钥 `priv_shar_user2` 对加密的内容密钥 `Key_content2` 解密, 然后使用解密的内容密钥 `Key_content2` 对加密的第二内容 403 解密。

[0041] 图 9 是示出根据本发明示例性实施例的在图 8 所示的情况下当装置 C(430) 在所属域中注册时的信息流的示图。参照图 9, 装置 C(430) 向域管理设备 400 发出在所属域中注册装置 C(430) 的请求。随后, 域管理设备 400 更新存储在域管理设备 400 中的所有链接信息, 并将更新的链接信息发送到装置 B(420) 和装置 C(430)。

[0042] 此时, 域管理设备 400 通过使用装置 C(430) 的公有密钥对当前域密钥 (即, 域密钥 `priv_shar_user2`) 加密和前域密钥 (即, 域密钥 `priv_shar_user1`) 加密来产生链接信息。因此, 由于域密钥 `priv_shar_user1` 不是当前域密钥, 所以根据域密钥 `priv_shar_user1` 的版本, 链接信息具有为 1 的主版本字段值, 并且字符 “P” 被记录在链接信息的有效

性比特字段中。此后，域管理设备(400)将所述链接信息发送到装置C(430)。因此，装置C(430)不仅可以通过向域管理设备400发出请求来使用第一内容401和第二内容403，还可以使用其他内容。

[0043] 图10是示出根据本发明示例性实施例的在图9所示的情况下当装置D(440)在所属域中注册时的信息流的示图。参照图10，如参照图9所述，装置D(440)向所属域发出注册装置D(440)的请求，并且域管理设备400更新所有链接信息。因此，当装置D(440)在所属域中注册时包含最新域密钥的链接信息的次版本值从1改变为2。因为在装置D(440)在所属域中注册之前没有在所属域中注册的装置从所述所属域中撤销，所以链接信息的主版本字段值(即，最新域密钥)没有被更新。因此，装置D(440)不仅可以使用第一内容401和第二内容403，还可以使用其他内容。

[0044] 图11是示出根据本发明示例性实施例的域管理设备400的框图。参照图11，域管理设备400包括：I/O接口510、域密钥更新单元520、域密钥发送单元530、内容处理单元540和存储单元550。域密钥发送单元530包括：链接信息产生器531、加密单元532和发送器533。内容处理单元540包括：第一加密单元541、第二加密单元542和内容信息发送器543。

[0045] I/O接口510能够使域管理设备400向所属域外部或者内部的装置发送数据，或者从所属域外部或者内部的装置接收数据。存储单元550存储链接信息、域密钥和内容。

[0046] 当注册的装置从所属域中撤销时，域密钥更新单元520产生更新的域密钥。域密钥更新单元520将更新的域密钥发送到域密钥发送单元530。

[0047] 域密钥发送单元530的发送器533将包括域密钥的链接信息发送到新注册的装置。当域密钥被更新时，域密钥发送单元530的发送器533将包括更新的域密钥的链接信息发送到所有注册的装置。如果需要将域密钥发送到新注册的装置并且该域密钥至少被更新过一次，则域密钥发送单元530的发送器533将所述域密钥和所有先前的域密钥一起发送到新注册的装置，从而该新注册的装置可以使用所属域中所有可用的内容。

[0048] 加密单元532使用注册的装置的公有密钥对域密钥加密。链接信息产生器531通过将有效性比特字段、主版本字段和次版本字段添加到加密的域密钥来产生链接信息。发送器533将链接信息发送到所有注册的装置，从而能够使注册的装置获得域密钥。

[0049] 内容处理单元540以使加密的数字内容仅可使用在接收到数字内容时在传播中的域密钥解密的方式来加密数字内容。此后，内容处理单元540将加密的数字内容发送到请求该数字内容的装置。具体来说，第一加密单元541使用作为数字内容的对称密钥的内容密钥对数字内容加密，第二加密单元542通过以使加密的数字内容仅可使用在接收到数字内容时在传播中的域密钥解密的方式来加密内容密钥来产生内容信息。随后，内容信息发送器543将内容信息发送到已经求求数字内容的装置。

[0050] 域密钥发送单元530将域密钥与域密钥的更新版本信息一起发送到注册的装置，并且内容处理单元540将加密的数字内容与将加密的数字内容解密所需的域密钥的更新版本信息一起发送到注册的装置，从而即使当注册的装置同时接收到两个或者多个数字内容时，也能够容易地搜索适用于特定数字内容的域密钥。

[0051] 本发明可被实现为写在计算机可读记录介质上的计算机可读代码。所述计算机可读记录介质可以为任何类型的以计算机可读的方式存储数据的记录装置。所述计算机可读

记录介质的例子包括 :ROM、RAM、CD-ROM、磁带、软盘、光学数据存储装置和载波（例如，经互联网的数据传输）。

[0052] 尽管已经参照本发明示例性实施例具体显示和描述了本发明，但是本领域普通技术人员将理解，在不脱离由权利要求限定的本发明的精神和范围的情况下，可在形式和细节上做出各种改变。

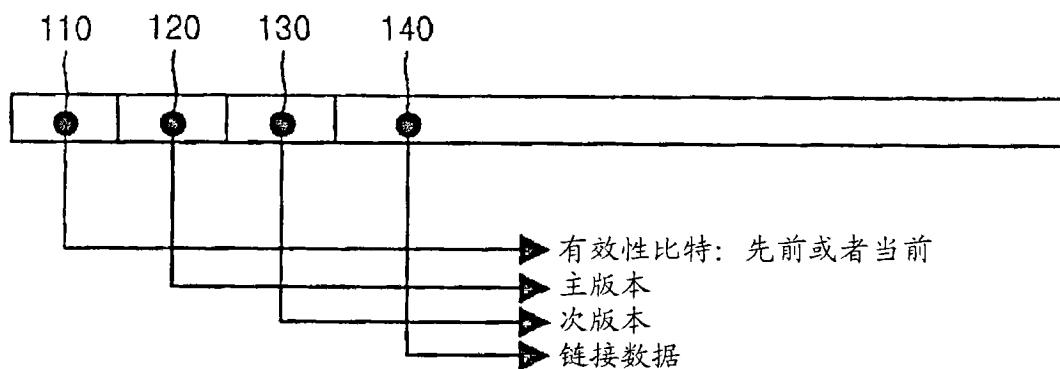


图 1

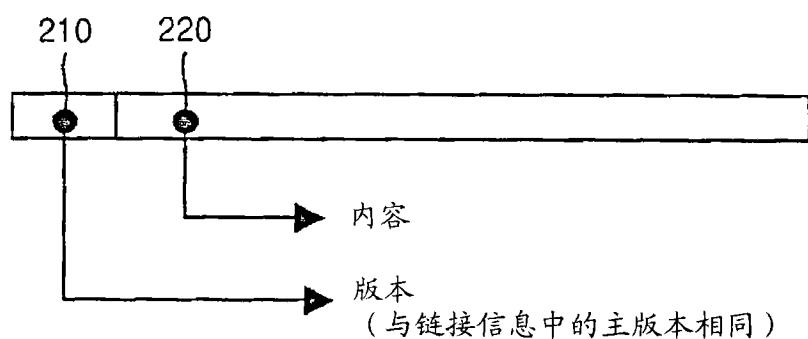
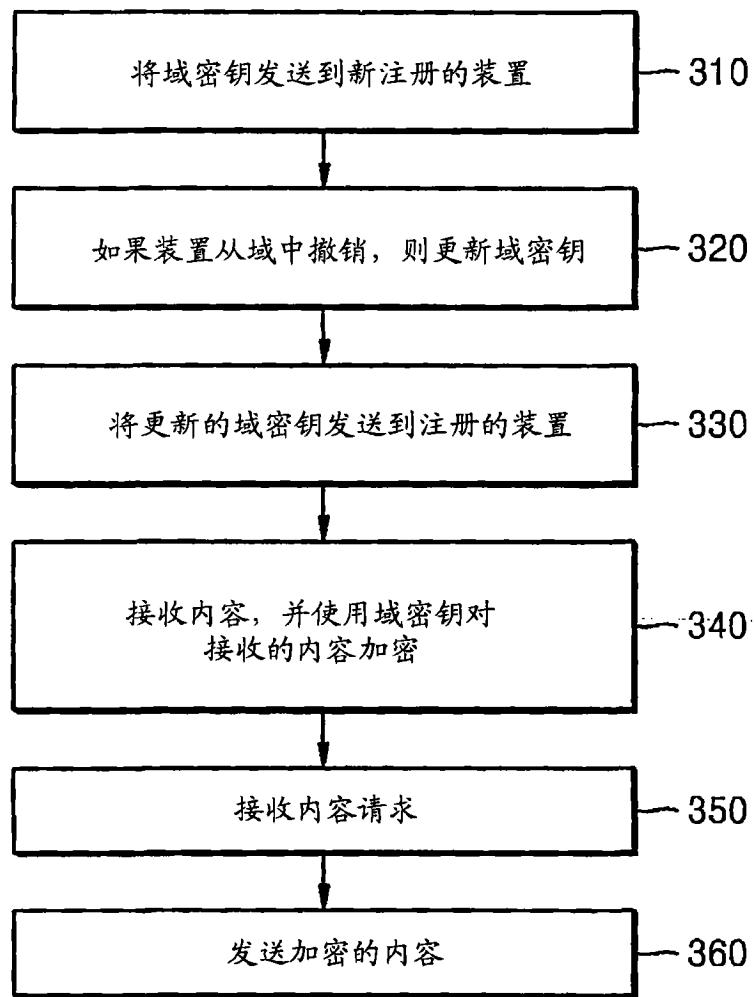


图 2



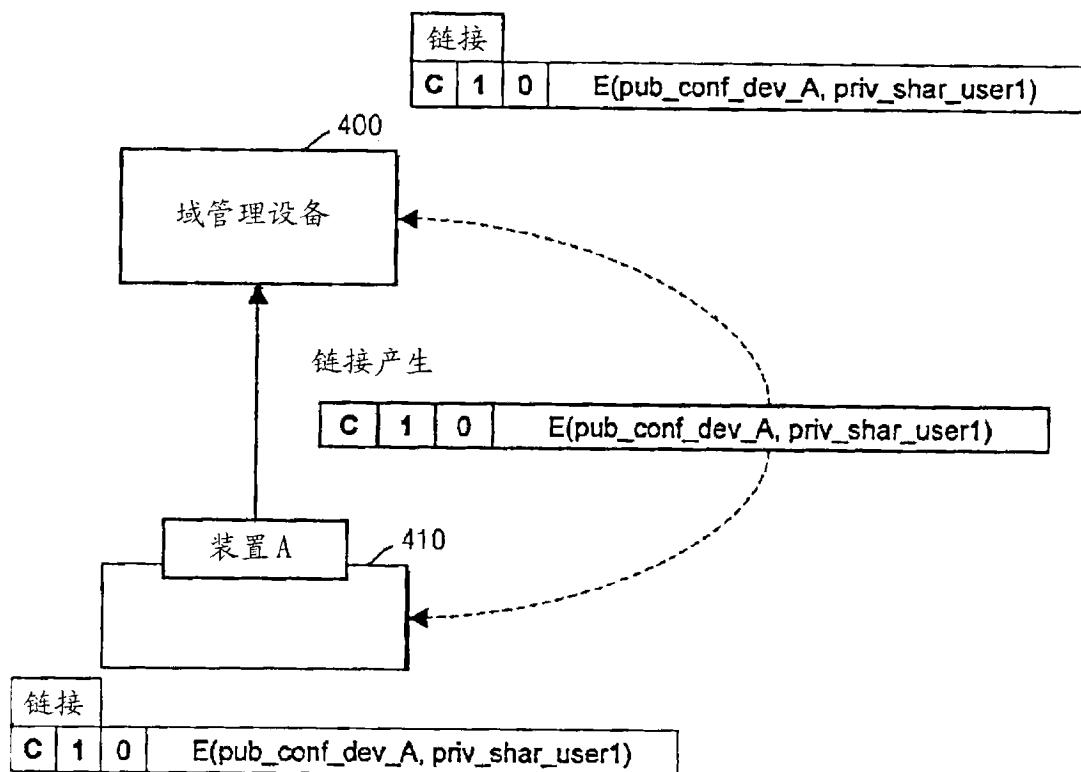


图 4

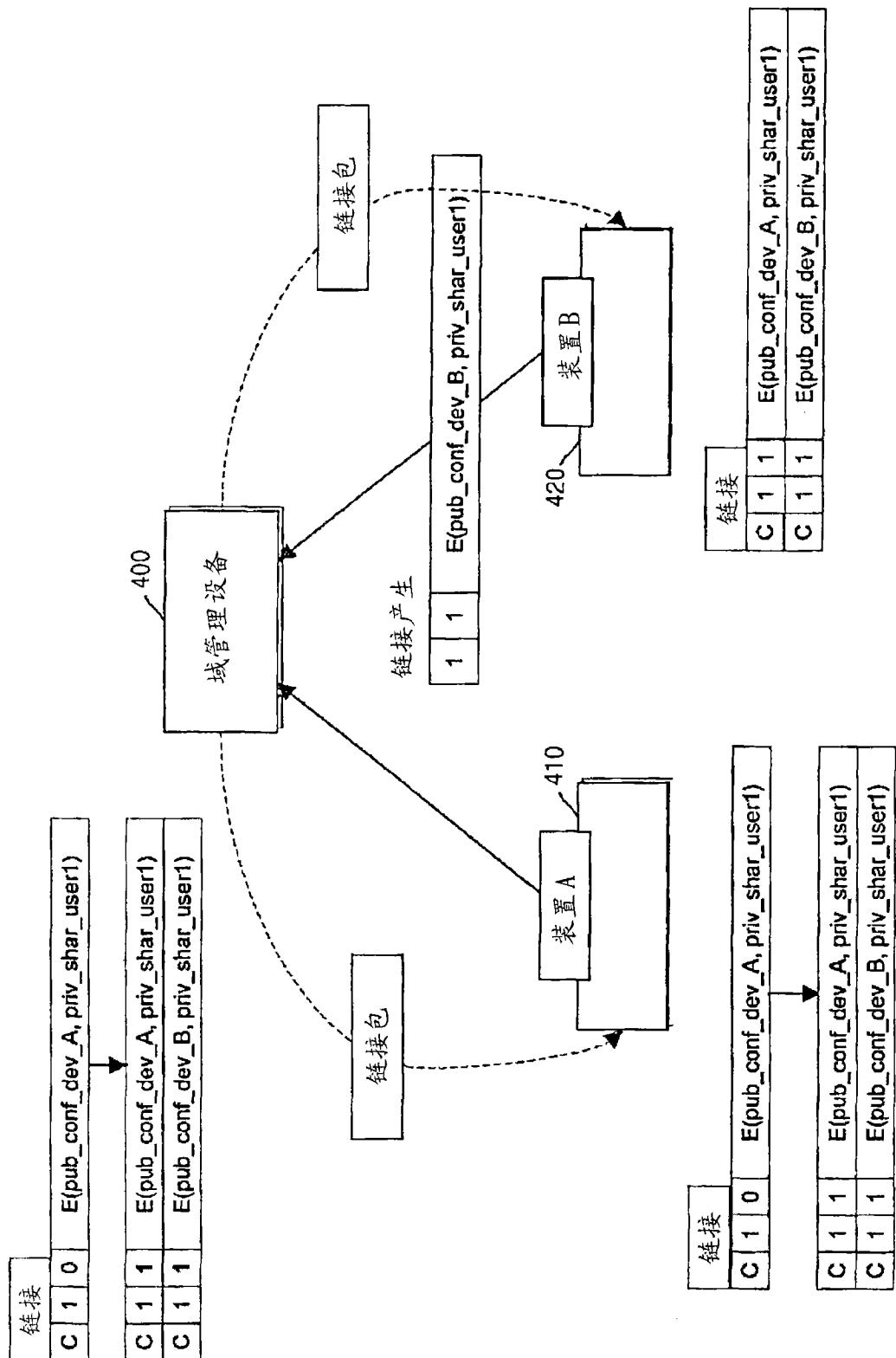


图 5

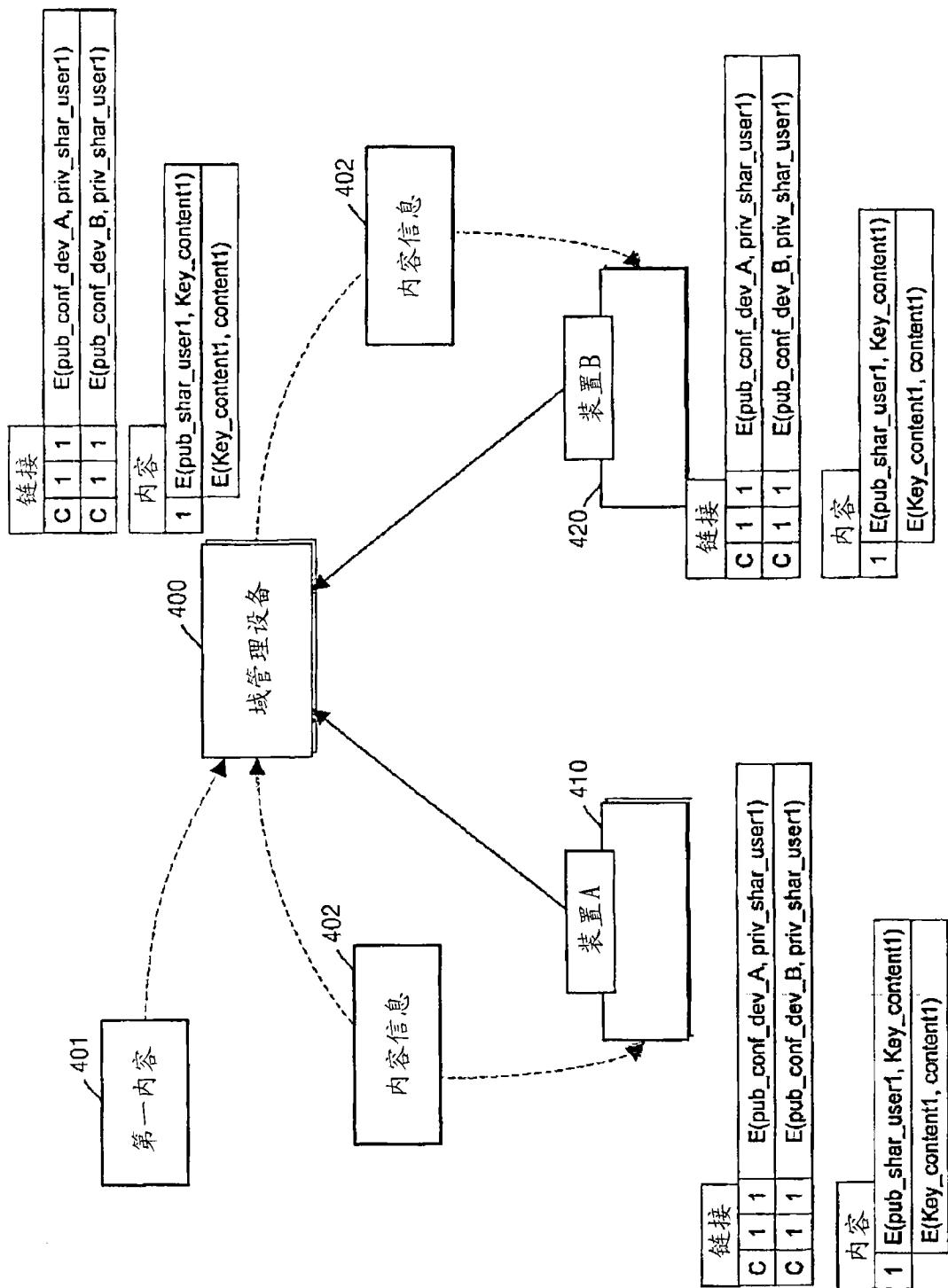


图 6

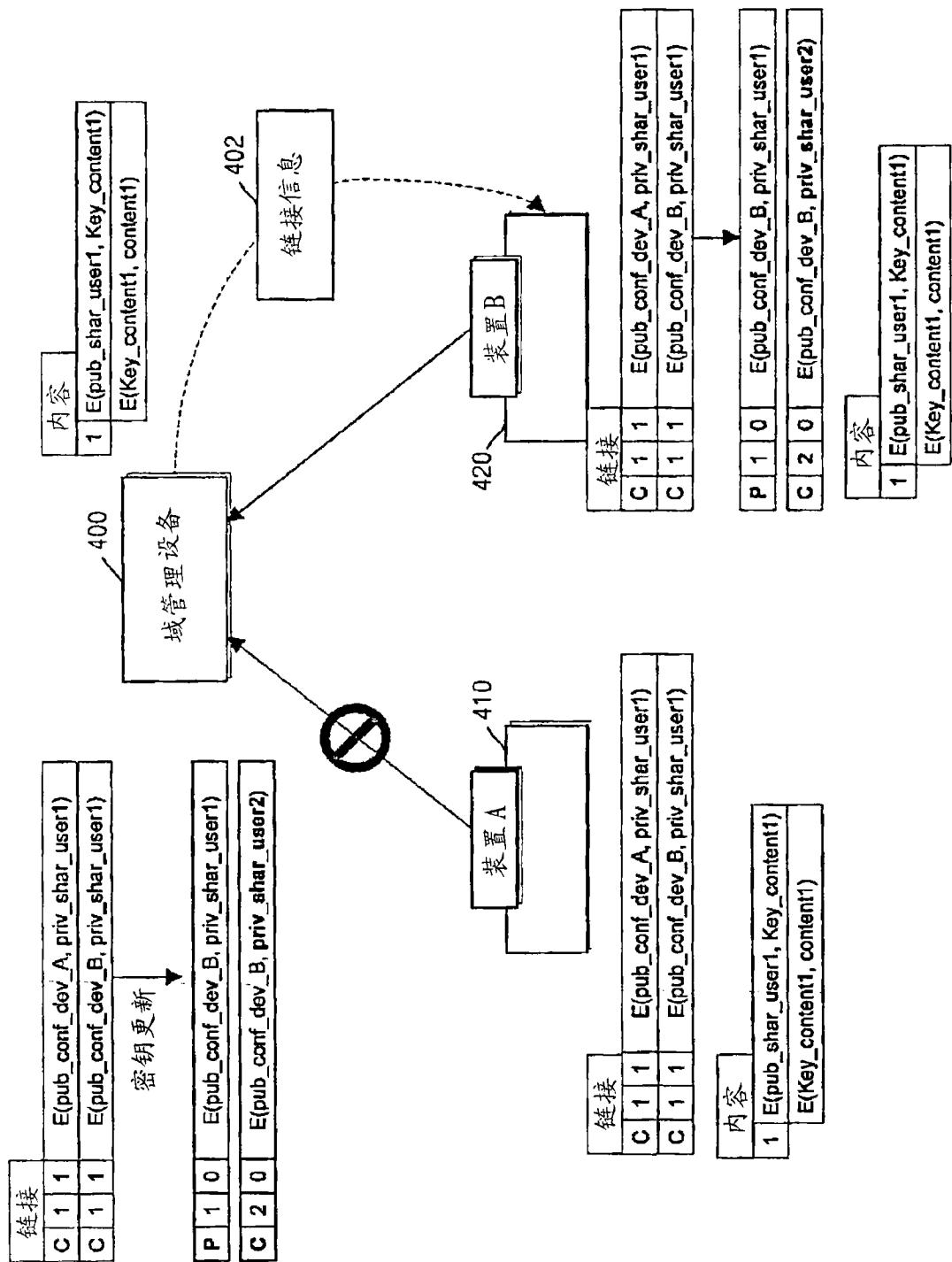


图 7

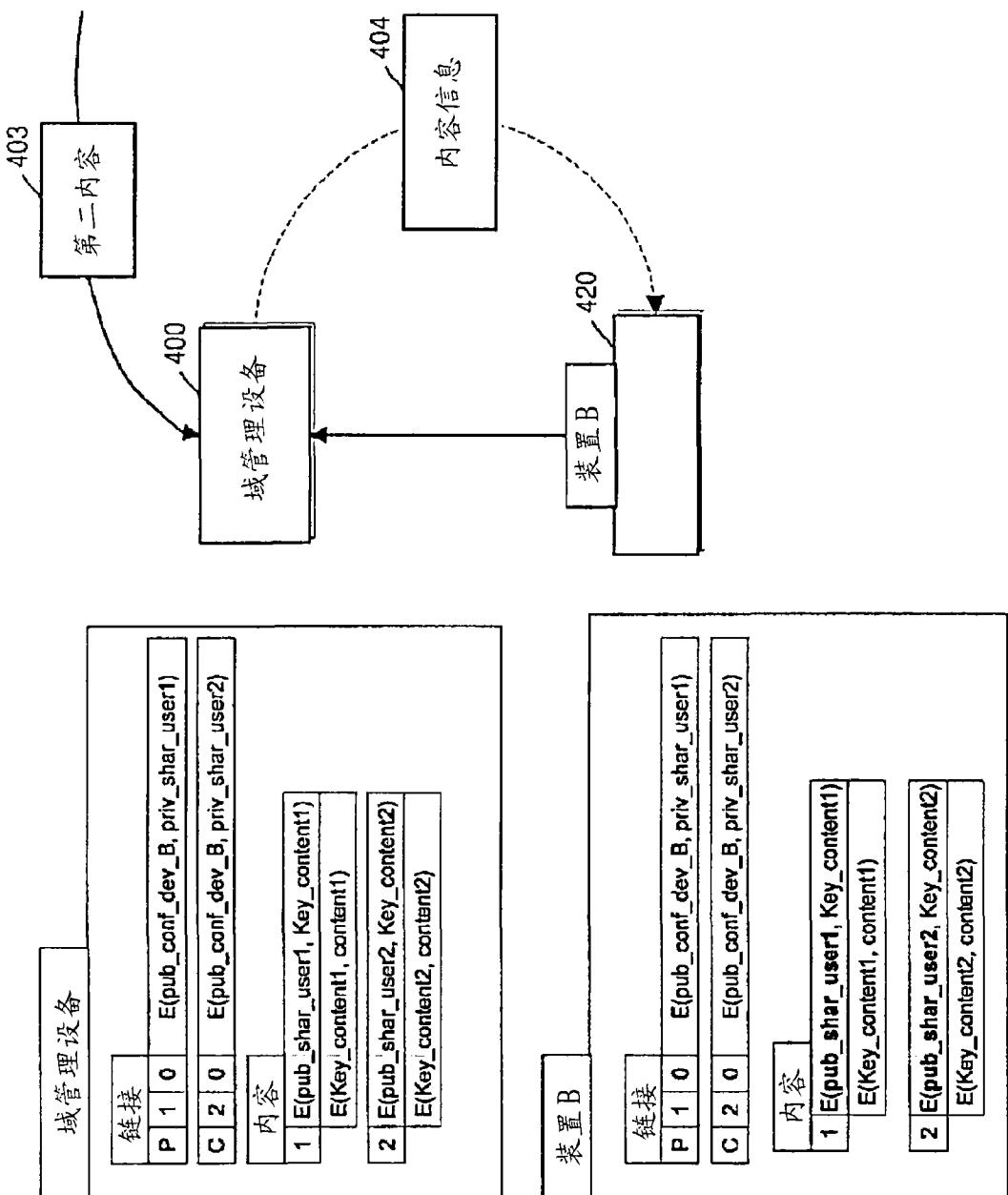
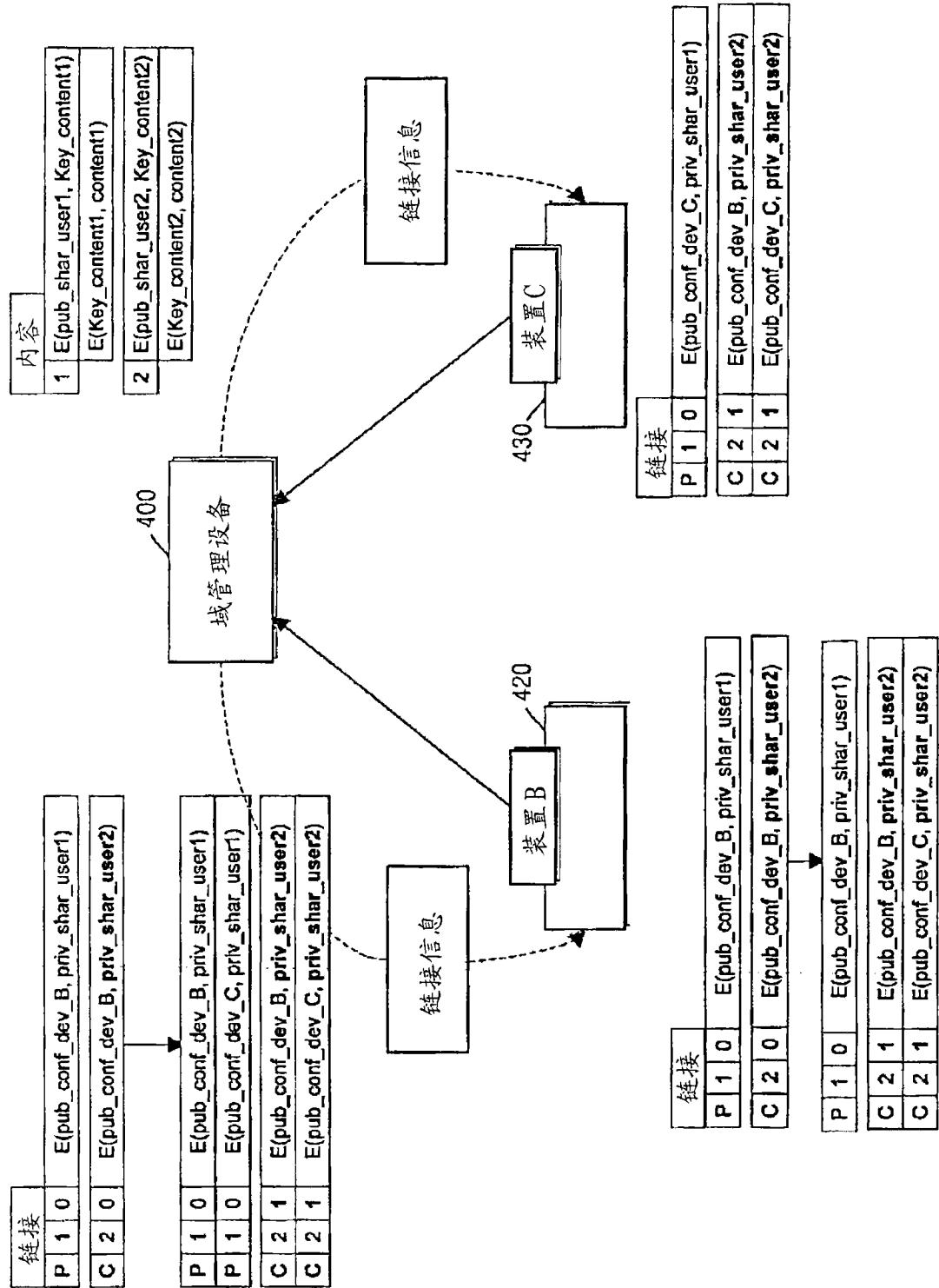


图 8



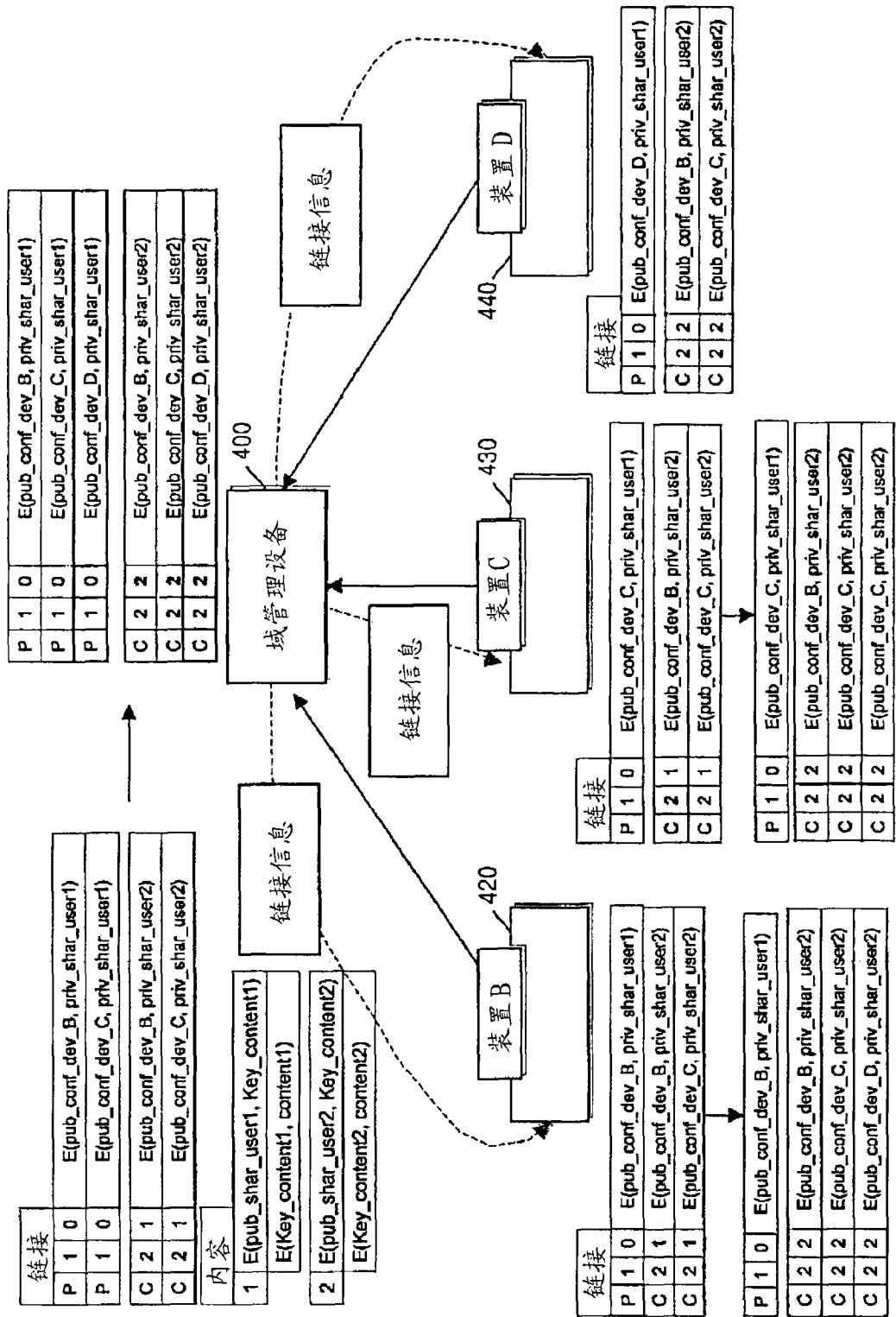


图 10

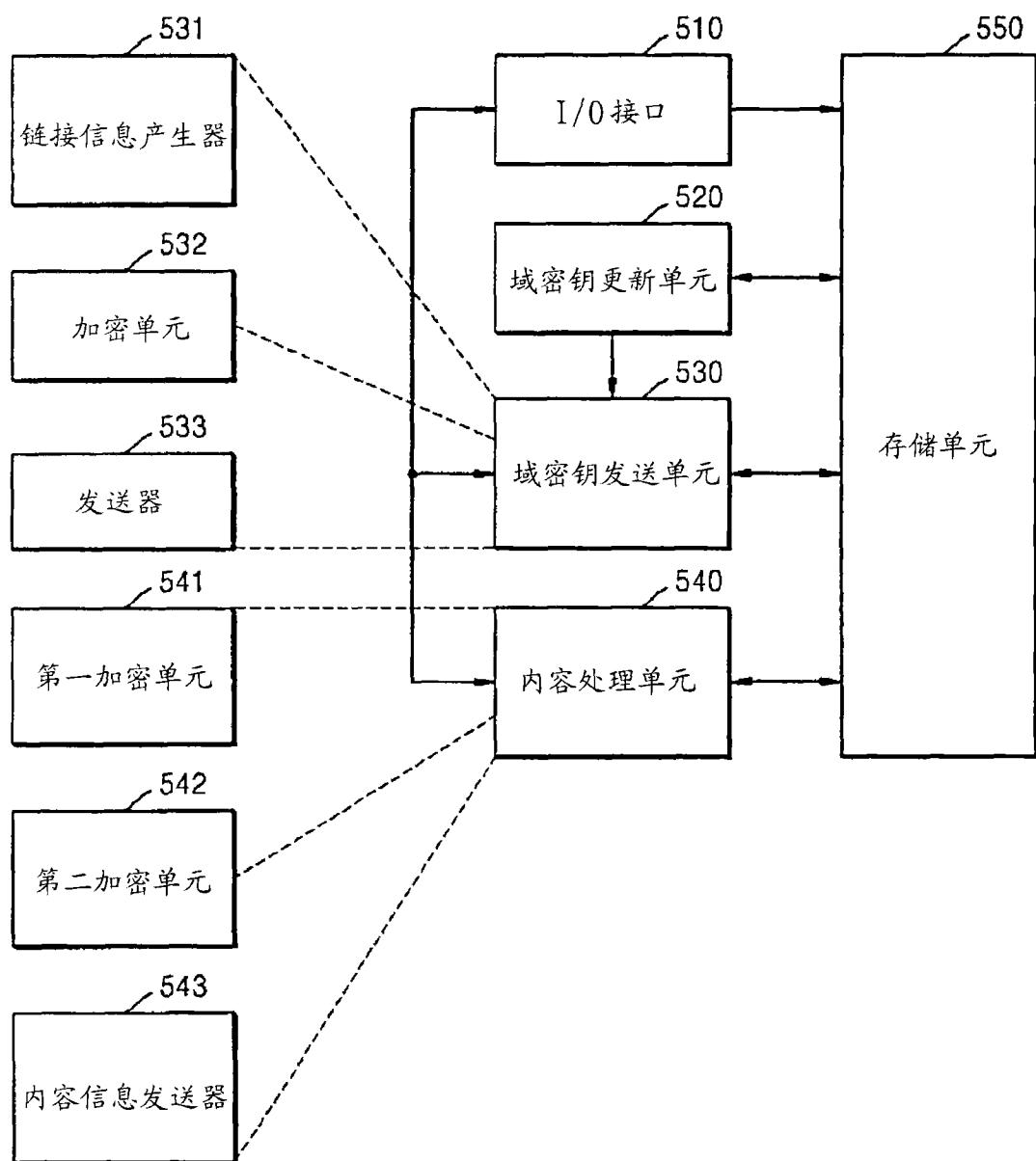


图 11