[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
G11B 20/00 (2006.01)
G06F 21/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480006804.7

[45] 授权公告日 2010 年 2 月 24 日

[11] 授权公告号 CN 100592683C

[22] 申请日 2004.3.12
[21] 申请号 200480006804.7
[30] 优先权
[32] 2003.3.14 [33] EP [31] 03100658.8
[86] 国际申请 PCT/IB2004/050242 2004.3.12
[87] 国际公布 WO2004/082201 英 2004.9.23
[85] 进入国家阶段日期 2005.9.13
[73] 专利权人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 M·沃克莱尔
[56] 参考文献
CN1306663A 2001.8.1
US2003/0021420A1 2003.1.30
EP1176827A2 2001.1.30
WO01/05150A1 2001.1.18
审查员 郭风顺
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 刘 杰

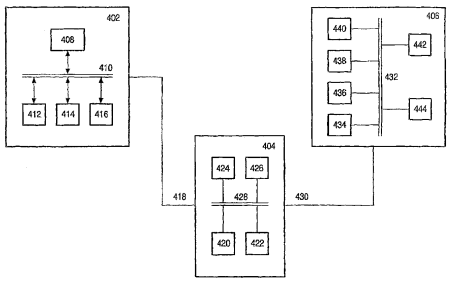
权利要求书 2 页 说明书 6 页 附图 3 页

[54] 发明名称

来自数字权利管理加密解密器的受保护的返回路径

[57] 摘要

公开了一种用于在防篡改装置(404)和信宿装置(406)之间提供安全通信的方法、设备和系统。在防篡改装置(404)处接收来自信源装置(402)的经加密的内容，其中已经使用第一密钥加密了该内容。使用已解密的第一密钥来解密该内容。在防篡改装置(404)处接收来自信宿装置(406)的第二密钥，其中使用防篡改装置(404)的公共密钥来加密第二密钥。使用防篡改装置(404)的专有密钥来解密第二密钥。使用第二密钥对所述内容进行重新加密。重新加密的内容被发送给信宿装置(406)。



1. 一种用于在防篡改装置和信宿装置之间提供安全通信的方法，该方法包括如下步骤：

在防篡改装置处从信源装置接收加密的内容，其中已经使用第一密钥加密了所述内容；

使用第一密钥，解密该内容；

在防篡改装置处从信宿装置接收第二密钥，其中使用防篡改装置的公共密钥加密第二密钥；

使用防篡改装置的专有密钥，解密第二密钥；

使用所述第二密钥，重新加密该内容；和

将所述重新加密的内容发送给所述信宿装置。

2. 根据权利要求 1 的方法，其中所述加密的内容被编码。

3. 根据权利要求 2 的方法，还包括如下步骤：

在所述信宿装置中使用所述第二密钥来解密所述加密的内容；

解码该解密的内容；

显示所述内容。

4. 根据权利要求 1 的方法，其中所述防篡改装置是智能卡或加密解密器。

5. 根据权利要求 1 的方法，其中所述第二密钥用于填装第一伪随机数生成器，并且将该生成器的输出与防篡改装置中解密的数据进行异或。

6. 根据权利要求 5 的方法，其中所述信宿装置将接收到的加密的内容与利用第二密钥填装的第二伪随机数生成器的输出进行异或。

7. 根据权利要求 1 的方法，其中所述内容是多媒体内容。

8. 根据权利要求 1 的方法，其中所述信源装置和所述防篡改装置各生成相同的第一密钥。

9. 根据权利要求 1 的方法，其中所述第一密钥被发送给防篡改装置。

10. 根据权利要求 9 的方法，其中使用所述防篡改装置的公共密钥来加密第一密钥，以及其中在使用第一密钥对所述内容进行解密之前，所述加密的第一密钥从所述信源装置被发送到所述防篡改装置。

11. 一种用于在防篡改装置和信宿装置之间提供安全通信的设备，

该设备包括:

用于在防篡改装置（404）处从信源装置（402）接收（404）加密的内容的装置，其中已经使用第一密钥加密了所述数据;

用于使用解密的第一密钥来解密（420）该内容的装置;

用于在防篡改装置处从信宿装置（406）接收（404）第二密钥的装置，其中使用防篡改装置的公共密钥来加密第二密钥;

用于使用防篡改装置的专有密钥来解密（420）第二密钥的装置;

用于使用所述第二密钥来重新加密（422）所述内容的装置；和

用于将所述重新加密的内容发送（404）给所述信宿装置的装置。

12. 一种用于在防篡改装置和信宿装置之间提供安全通信的系统，该系统包括:

用于发送加密的内容的信源装置，其中已经使用第一密钥加密了所述内容;

防篡改装置，从信源装置接收加密的内容，和

该防篡改装置使用第一密钥来解密（420）该内容;

该防篡改装置还从信宿装置（406）接收（404）第二密钥，其中使用该防篡改装置的公共密钥来加密第二密钥;

该防篡改装置使用该防篡改装置的专有密钥来解密（420）该第二密钥;

该防篡改装置使用所述第二密钥来重新加密（422）该内容；和

该防篡改装置将所述重新加密的内容发送（404）给所述信宿装置。

来自数字权利管理加密解密器的受保护的返回路径

本发明涉及保护数据传输，尤其涉及一种用于保护在防篡改装置和信宿装置之间的数据传输的方法、设备和系统。

在计算机和诸如因特网之类的网络的使用方面的爆炸性发展已导致在因特网上发送的数据和信息的知识产权保护方面的问题。这些问题是数字信息能够被容易地发送和拷贝的结果。以数字的形式，诸如视频、音乐、游戏、软件等等之类的信息能够以很难区分信息的原始版本和拷贝版本的高质量而被拷贝。结果，数字形式的信息成为黑客的非常诱人的目标。

为了抗击对数字信息的非法拷贝，已经开发了各种形式的保护。例如，当一个信源装置发送数字多媒体内容给信宿装置时，可以在将该内容从信源装置发送到信宿装置之前以某种方式对该内容进行加密以便保护该数字内容免于被偷盗或者被不适当地拷贝。如图1中所示，多媒体内容106从信源装置102被发送给信宿装置104以用于显示。多媒体内容106首先被编码器108编码。编码的内容然后由加密装置110使用一个加密密钥加密。加密的数据然后被发送给信宿装置。信宿装置104利用解密装置114、使用所述加密密钥来解密所述加密的内容。解密的内容然后被解码器116解码。解码的内容然后被呈现装置120呈现并被显示在输出装置122上。这种解决方案的一个问题是：在加密的内容能够被解密之前，信宿装置需要知道加密密钥。因此，内容分发者必须确保每个合法的顾客拥有加密密钥。这对于大的内容分发者来说会成为一个后勤问题。此外，攻击者在试图找到加密密钥时将有许多可作为攻击目标的源。

已被开发来抗击这个问题的一个系统是使用非对称的密钥。信源装置102和信宿装置104各可以具有非对称的密钥，所述非对称的密钥包括一个公共密钥和一个专有密钥。用公共密钥加密的信息只能被专有密钥解密，反之亦然。

在信源装置102和信宿装置104之间的易受攻击的链路上对内容的加密防止了对内容的有害数字拷贝。可是，攻击者仍然能够尝试攻击

信宿装置104以获得解密密钥，并从而能够使用该内容。为了抗击这种攻击，如图2所示，对内容的解密可以由附着到信宿装置104上或者作为信宿装置104的一部分的诸如智能卡或加密解密器（dongle）之类的防篡改装置来执行。在这个方案中，使用一个加密密钥来加密内容，并且使用该防篡改装置的公共密钥来加密所述加密密钥本身。当该防篡改装置接收到加密的内容和密钥时，使用该防篡改装置的专有密钥来解密该被加密的加密密钥。专有密钥被安全地储存在防篡改装置201内部，因此攻击者不能使用该专有密钥。所接收到的加密内容被解密装置203使用所储存的已解密的加密密钥来解密。解密的内容被发送给解码器116，并且如上参考图1所述的那样被处理。这种系统的一个缺点是：以一种无保护的格式将内容从所述防篡改装置发送到信宿装置104。结果，通过在信宿装置104和防篡改装置201之间插入一个探测器（sniffer）装置，仍然能够获得该内容的未经授权的数字拷贝。结果，需要一种用于保护在信宿装置和防篡改装置之间的链路的方法和系统。

本发明的一个目的是通过加密在防篡改装置和信宿装置之间发送的内容来克服上述缺陷。

根据本发明的一个实施例，公开了一种用于在防篡改装置和信宿装置之间提供安全通信的方法、设备和系统。在防篡改装置处接收来自信源装置的加密内容，其中该内容已经使用第一密钥被加密。使用已解密的第一密钥来解密该内容。在防篡改装置处接收来自信宿装置的第二密钥，其中使用防篡改装置的公共密钥来加密第二密钥。使用防篡改装置的所述专有密钥来解密第二密钥。使用该第二密钥对所述内容进行重新加密。重新加密的内容被发送给信宿装置。

本发明的这些以及其他方面将从此后描述的实施例中变得明显并被阐明。

现在将参考附图举例来描述本发明，附图中：

图1是用于发送媒体内容的已知传输系统的方框示意表示；

图2是用于发送媒体内容的已知传输系统的方框示意表示；

图3说明了根据本发明一个实施例在信源装置、防篡改装置和信宿

装置之间的数据和加密密钥流；和

图4是根据本发明一个实施例的用于发送媒体内容的传输系统的方框示意表示。

根据本发明的一个实施例，信源装置、防篡改装置和信宿装置各被分配一个非对称公共－专有密钥对，该密钥对可用于向其它装置验证每个装置，并且所述密钥对还用于执行各个装置之间的受保护的信息交换。与上述已知系统不同，本发明使用公共－专有密钥对来加密所述加密密钥，其中所述加密密钥被用于加密在信源装置和防篡改装置之间的链路以及在防篡改装置和信宿装置之间的链路上的内容。简要地说，被信源装置使用来加密所述内容的第一加密密钥由信源装置发送给防篡改装置，其中该第一加密密钥是用防篡改装置的公共密钥加密（被加密的密钥透明地发送通过信宿装置）。这个密钥是永久性的，并且附着到所述内容上。信宿装置不知道这个密钥。另外，被防篡改装置使用来加密在防篡改装置和信宿装置之间发送的内容的第二加密密钥本身是使用防篡改装置的公共密钥而被加密的，并且被从信宿装置发送给防篡改装置。或者，如将在下面更详细描述的那样，代替第二加密密钥，可以将一个加扰密钥从信宿装置发送给防篡改装置。

现在将参考图3更详细地解释在上面简要描述的数据和加密密钥流。如图所示，信源装置301经由一条传输链路302连接到防篡改装置303，并且防篡改装置303经由一条传输链路304连接到信宿装置305。本领域技术人员应该理解：传输链路可以是能够发送数字信息的任何种类的通信链路，无线或有线均可。信源装置301具有一个公共密钥1和一个专有密钥1。防篡改装置303具有一个公共密钥2和一个专有密钥2。信宿装置305具有一个公共密钥3和一个专有密钥3。各装置以一种已知的方式使用公共和专有密钥来彼此验证它们自身。虽然图3中示出的装置各具有一个公共/专有密钥对，但是本领域技术人员应该理解：并不是所有这些装置（例如信宿装置）都需要一个公共/专有密钥对来实践本发明。

正如将在下面更详细地解释的那样，信源装置301使用第一加密密钥306来加密多媒体内容，并经由传输链路302将该加密的内容发送给

防篡改装置303。另外，信源装置301使用防篡改装置303的公共密钥2对加密密钥306进行加密，并经由传输链路302将已加密的该加密密钥发送给防篡改装置303。简要地说，防篡改装置303然后使用专有密钥2对该已加密的加密密钥306进行解密。防篡改装置303然后使用已解密的该加密密钥306对被加密的内容进行解密。或者，信源装置301和防篡改装置303能够在协议的验证阶段交换密钥素材。在链路两侧交换的密钥素材然后被分组并被使用于一个数学过程，以便产生一个密钥生成器，如果要以一定时间相隔更新、修改加密密钥的话，该密钥生成器在链路两侧递送相同的密钥或者相同的密钥流。在这个方案中，防篡改装置将产生密钥并解码从信源装置301接收的内容。

信宿装置305选择第二加密或加扰密钥307。信宿装置然后使用防篡改装置303的公共密钥2来加密该第二加密或加扰密钥307。被加密的第二加密或加扰密钥307然后经由传输链路304被发送给防篡改装置303。防篡改装置303使用该专有密钥2来解密该第二加密或加扰密钥307。防篡改装置303然后使用该第二加密或加扰密钥307加密来自信源装置301的已解密内容，并经由传输链路304把经重新加密的内容发送给信宿装置305。

现在将参考图4更详细地描述本发明。如图所示，多媒体内容被从信源装置402发送到信宿装置406以用于显示。信源装置402除了其它元件之外尤其包括：存储器装置408、总线410、编码器412、加密装置414和用于控制信源装置402的操作的处理器416。应该理解：信源装置可以包含其它元件，并且所列出的元件中的一些可以被合并在单个元件中。所储存的多媒体内容首先可选地被编码器412编码。（已编码的）内容然后被加密装置414使用第一加密密钥加密。第一加密密钥然后被加密装置414使用防篡改装置404的公共密钥加密。已加密内容和经加密的第一加密密钥然后经由传输链路418被发送给防篡改装置404。正如在上面相对于图3所述的那样，信源装置301和防篡改装置303或者可以在验证阶段期间交换密钥素材来使彼此能够生成相同的第一加密密钥。在这个方案中，信源装置402将生成第一加密代码并加密所述内容，其中该内容被发送给防篡改装置404。

防篡改装置404除了其它元件之外尤其包括：解密装置420、加密装置422、存储器装置424、总线428和用于控制该防篡改装置的操作的

处理器426。防篡改装置首先使用储存在存储器424中的它的专有密钥来解密第一加密密钥。一旦该加密密钥已经被解密装置420解密，则解密装置420现在使用该已解密的加密密钥来解密从信源装置402中接收到的加密的内容。或者，防篡改装置404能够生成该第一加密密钥并解密该加密的内容。

信宿装置406除了其它元件之外尤其包括：总线432、加密/解密装置434、解码器436、呈现装置438、输出装置440、存储器442和用于控制信宿装置406的操作的处理单元444。信宿装置406选择将被用来保护在防篡改装置404和信宿装置406之间的传输链路上发送的内容的第二加密密钥。加密/解密装置434使用防篡改装置404的公共密钥对第二加密密钥进行加密，并通过传输链路430将被加密的加密密钥发送给防篡改装置。

解密装置420使用防篡改装置404的专有密钥对经加密的第二加密密钥进行解密。所述加密装置现在可以使用第二加密密钥对来自信源装置402的解密的内容进行加密。然后通过传输链路430将该重新加密的内容发送给信宿装置406。

信宿装置406利用加密/解密装置434、使用第二加密密钥来解密从防篡改装置404中接收到的经加密的内容。然后可选地由解码器436解码解密后的内容。解码后的内容然后被进一步处理，例如它被呈现装置120呈现并被显示在输出装置440上。

第二加密密钥可以采用许多形式。例如，第二加密密钥可以是一个加扰密钥，它被用来例如在加密装置422中填装（prime）一个伪随机数生成器，其中对该伪随机数生成器的输出与防篡改装置中的明文内容进行异或。信宿装置406然后必须例如把所接收的数据与例如在加密/解密装置434中的由同一第二加密密钥填装的它自己的伪随机数生成器的输出进行异或。本领域技术人员应该理解：任何安全的流密码技术都适用于这个操作，并且本发明不限制于此。

第二加密密钥是短暂的，并且只是在防篡改装置404和信宿装置406之间的数据传送期间被使用。在添加到信宿装置406上的密码设施强制实施一个链路层保护的同时，防篡改装置404强制实施一个应用层保护。该方法被设计成使得信宿装置406的预期密码性能被保持在最小限度。

应该理解：本发明的不同实施例不限制于上述步骤的精确顺序，因为一些步骤的定时可以互换而不影响本发明的总体操作。此外，术语“包括”不排除其它元件或步骤，术语“一个”不排除多个，并且单个处理器或者其它单元可以实现权利要求中引述的几个单元或电路的功能。

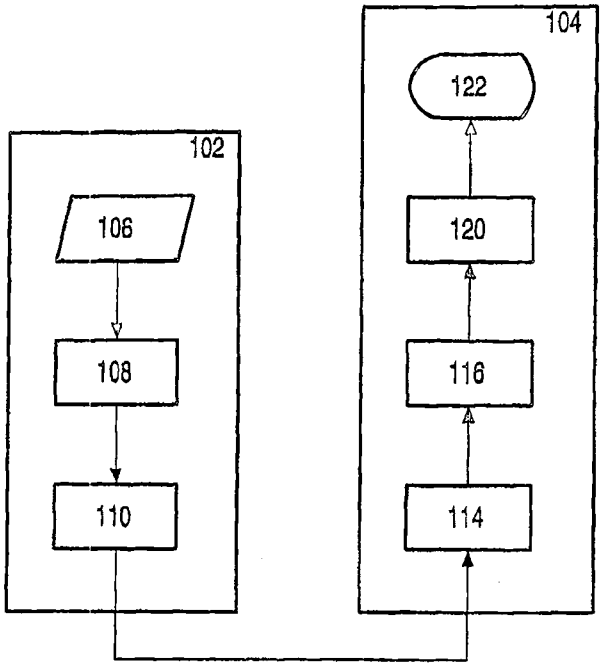

104
122
102
106
120
108
116
110
114

图 1

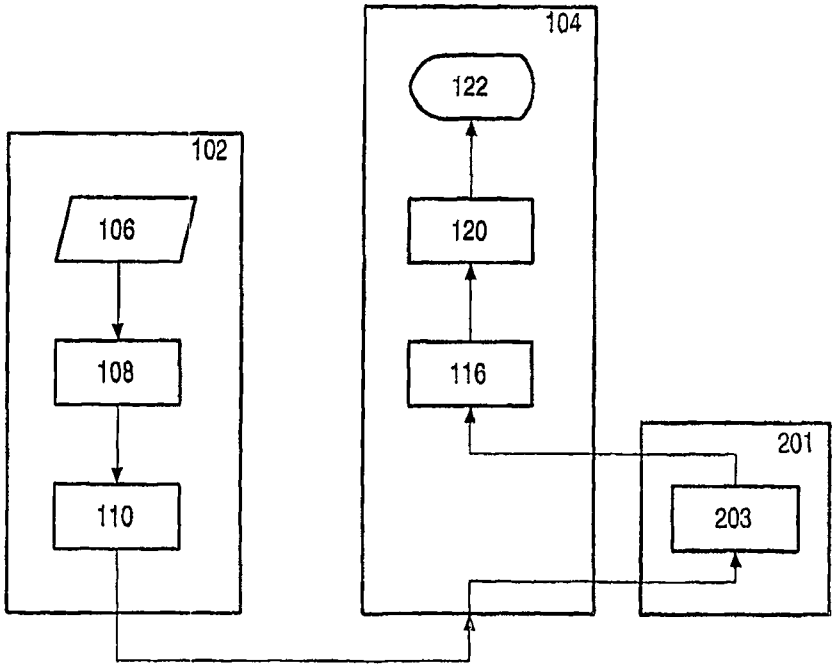

104
122
102
106
120
108
116
201
110
203

图 2

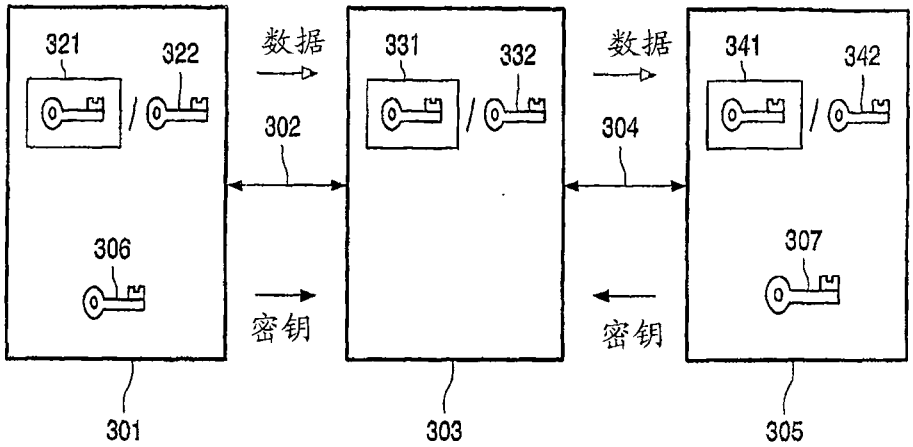


图 3

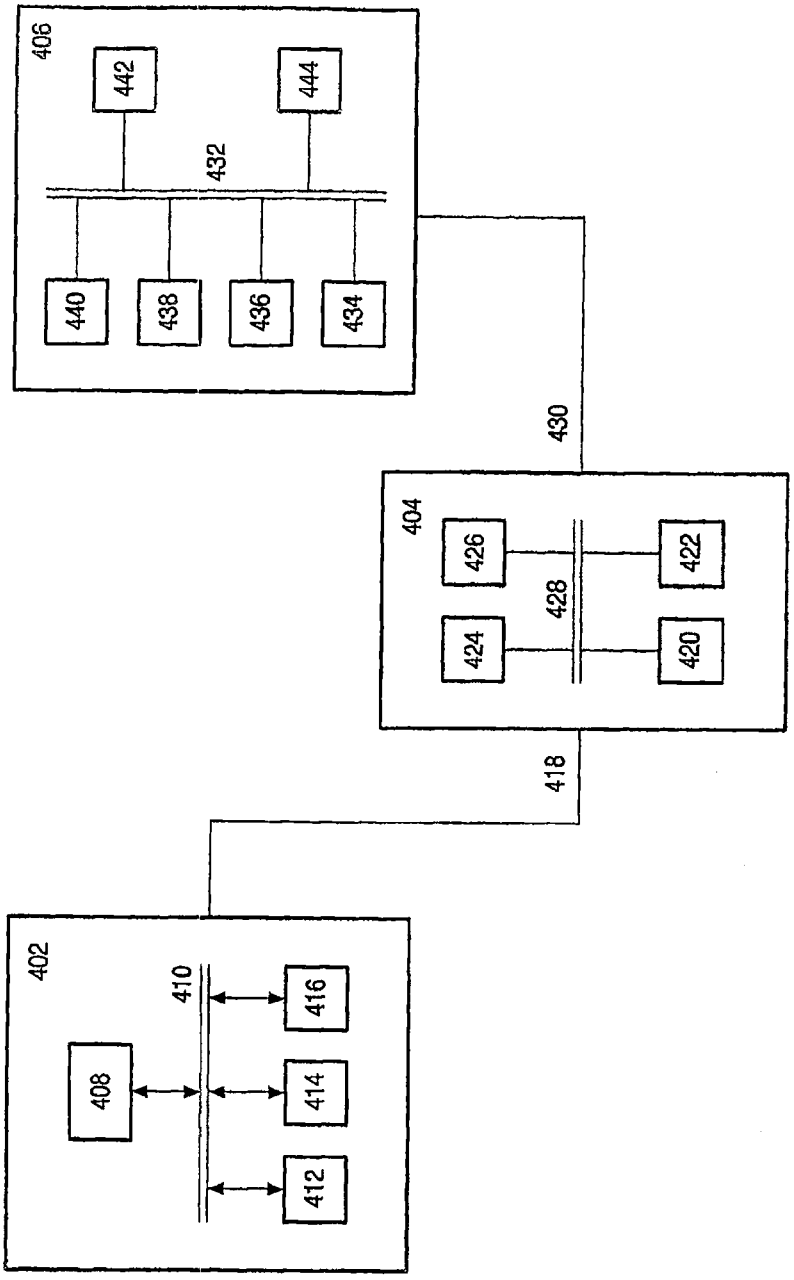

406
442
444
432
440
438
436
434
430
404
426
422
428
424
420
418
402
410
416
408
414
412

图 4