(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114726647 B
(45)授权公告日 2022.08.12

(21)申请号 202210512136.5

(22)申请日 2022.05.12

(65)同一申请的已公布的文献号
申请公布号 CN 114726647 A

(43)申请公布日 2022.07.08

(73)专利权人 知安视娱(北京)科技有限公司
地址 100176 北京市大兴区北京经济技术开发区宏达北路12号A幢3层310室(北京自贸试验区高端产业片区亦庄组团)

(72)发明人 张海永

(74)专利代理机构 北京弘权知识产权代理有限公司 11363
专利代理师 逯长明 许伟群

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 9/06(2006.01)

(56)对比文件
CN 113111360 A,2021.07.13
CN 103873233 A,2014.06.18
CN 111080299 A,2020.04.28
CN 111601117 A,2020.08.28
CN 113886860 A,2022.01.04
WO 2015133829 A1,2015.09.11

审查员 方婷

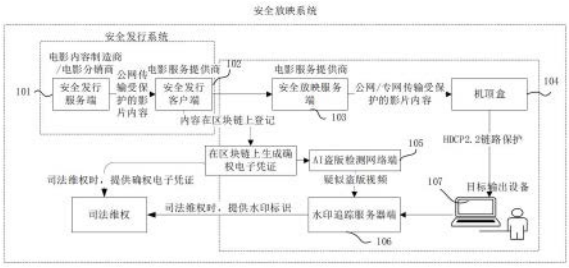
权利要求书4页 说明书15页 附图5页

(54)发明名称

一种4K影片内容的安全发行方法、系统及安全放映系统

(57)摘要

本申请公开一种4K影片内容的安全发行方法、系统及安全放映系统，属于数字版权保护技术领域，该方法包括：生成随机AES密钥和密钥偏移量IV；使用随机AES密钥对影片内容加密，使用安全发行客户端的TPM RSA公钥对随机AES密钥加密，生成密钥文件；使用安全发行服务端的TPM RSA私钥解密加密的第一请求验证信息；对密钥请求文件进行第二映射处理，得到第二请求验证信息；验证密钥请求文件是否被篡改；如果密钥请求文件未被篡改，则将加密后的影片内容以及密钥文件发送至安全发行客户端。该安全发行方法基于AES加解密算法和TPM可信任环境的公钥体系，同时满足ECP要求和支持国密算法，能够实现4K影片内容从电影内容制造商到电影服务提供商的安全发行交付。



CN 114726647 B

1.一种4K影片内容的安全发行方法,其特征在于,所述方法应用于安全发行服务端,所述方法包括:

响应安全发行客户端的影片内容发行请求,生成随机AES密钥和密钥偏移量IV;

使用随机AES密钥对影片内容加密;

在TPM可信任环境下,使用所述安全发行客户端的TPM RSA公钥对所述随机AES密钥加密,生成密钥文件,其中,所述密钥文件中还包括所述密钥偏移量IV;

如果接收到所述安全发行客户端发送的密钥请求,所述密钥请求包括密钥请求文件和加密的第一请求验证信息,则在TPM可信任环境下,使用所述安全发行服务端的TPM RSA私钥解密所述加密的第一请求验证信息,得到解密后的第一请求验证信息,其中,所述第一请求验证信息是指通过所述安全发行客户端对所述密钥请求文件进行第一映射处理后得到的信息;

对所述密钥请求文件进行第二映射处理,得到第二请求验证信息,其中,所述第一映射处理与所述第二映射处理的处理方法相同;

通过所述第一请求验证信息和所述第二请求验证信息,验证所述密钥请求文件是否被篡改;

如果所述密钥请求文件未被篡改,则将加密后的影片内容以及所述密钥文件发送至所述安全发行客户端。

2.根据权利要求1所述的4K影片内容的安全发行方法,其特征在于,如果所述密钥请求文件未被篡改,还包括:

对所述密钥文件进行第三映射处理,得到第一密钥验证信息;

使用所述安全发行客户端的TPM RSA公钥对所述第一密钥验证信息加密,得到加密的第一密钥验证信息;

将所述密钥文件和所述加密后的第一密钥验证信息发送至所述安全发行客户端。

3.根据权利要求1所述的4K影片内容的安全发行方法,其特征在于,所述第一映射处理为散列运算或Base64编码;如果所述第一映射处理为散列运算,则所述第一请求验证信息为第一哈希值,所述第二请求验证信息为第二哈希值;

则通过所述第一请求验证信息和所述第二请求验证信息,验证所述密钥请求文件是否被篡改,包括:

对比所述第一哈希值与所述第二哈希值是否相同;

如果所述第一哈希值与所述第二哈希值相同,则确定所述密钥请求文件未被篡改;

如果所述第一哈希值与所述第二哈希值不相同,则确定所述密钥请求文件被篡改。

4.根据权利要求1所述的4K影片内容的安全发行方法,其特征在于,还包括在所述影片内容中插入第一水印标识的步骤,所述第一水印标识用于标识所述影片内容的发行信息,所述发行信息包括接收所述影片内容的安全发行客户端信息以及发行所述影片内容的安全发行服务端信息。

5.根据权利要求1所述的4K影片内容的安全发行方法,其特征在于,还包括:

将加密后的影片内容以及所述密钥文件封装在安全发行包中;

如果所述密钥请求文件未被篡改,则将所述安全发行包发送至所述安全发行客户端。

6.一种4K影片内容的安全发行方法,其特征在于,所述方法应用于安全发行客户端,所

述方法包括：

生成密钥请求文件；

对所述密钥请求文件进行第一映射处理，生成第一请求验证信息；

使用安全发行服务端的TPM RSA公钥对所述第一请求验证信息加密，得到加密后的第一请求验证信息；

将所述密钥请求文件和所述加密后的第一请求验证信息发送至所述安全发行服务端；

如果接收到所述安全发行服务端发送的加密后的影片内容以及密钥文件，则在TPM可信任环境下，使用所述安全发行客户端的TPM RSA私钥解密所述密钥文件，得到随机AES密钥和密钥偏移量IV；

在TPM可信任环境下，使用所述随机AES密钥和所述密钥偏移量IV解密所述加密后的影片内容。

7.根据权利要求6所述的4K影片内容的安全发行方法，其特征在于，还包括：

接收所述安全发行服务端发送的密钥文件和加密后的第一密钥验证信息，其中，所述第一密钥验证信息是指通过所述安全发行服务端对所述密钥文件进行第三映射处理后得到的信息；

对所述密钥文件进行第四映射处理，得到第二密钥验证信息，其中，所述第三映射处理与所述第四映射处理的处理方法相同；

使用安全发行客户端的TPM RSA私钥解密加密后的第一密钥验证信息，得到解密后的所述第一密钥验证信息；

通过所述第一密钥验证信息和所述第二密钥验证信息，验证所述密钥文件是否被篡改；

如果所述密钥文件未被篡改，则执行所述在TPM可信任环境下，使用所述安全发行客户端的TPM RSA私钥解密所述密钥文件，得到随机AES密钥的步骤及后续步骤。

8.根据权利要求7所述的4K影片内容的安全发行方法，其特征在于，所述第三映射处理为散列运算或Base64编码；如果所述第三映射处理为散列运算，则所述第一密钥验证信息为第三哈希值，所述第二密钥验证信息为第四哈希值；

则通过所述第一密钥验证信息和所述第二密钥验证信息，验证所述密钥文件是否被篡改，包括：

对比所述第三哈希值与所述第四哈希值是否相同；

如果所述第三哈希值与所述第四哈希值相同，则确定所述密钥文件未被篡改；

如果所述第三哈希值与所述第四哈希值不相同，则确定所述密钥文件被篡改。

9.根据权利要求6所述的4K影片内容的安全发行方法，其特征在于，所述生成密钥请求文件包括：

采集所述安全发行客户端的密钥请求信息，所述密钥请求信息包括所述安全发行客户端的硬件信息、用户信息以及所请求的影片内容信息；

根据所述密钥请求信息，生成所述密钥请求文件。

10.根据权利要求6所述的4K影片内容的安全发行方法，其特征在于，使用所述随机AES密钥和所述密钥偏移量IV解密所述加密后的影片内容后，还包括：

在区块链上登记安全发行内容，所述安全发行内容包括所述安全发行服务端向所述安

全发行客户端发送的影片内容信息、所述安全发行服务端的信息、以及所述安全发行客户端的信息，其中，所述区块链由电影服务商和电影分销商创建，所述区块链用于所述电影服务商和所述电影分销商之间的影片内容安全发行交易；

根据所述安全发行内容，生成确权电子凭证；

将所述确权电子凭证发送至AI盗版检测网络端。

11.一种4K影片内容的安全发行系统，其特征在于，包括安全发行服务端和安全发行客户端；

所述安全发行服务端，用于响应安全发行客户端的影片内容发行请求，生成随机AES密钥和密钥偏移量IV；使用随机AES密钥对所述影片内容加密；在TPM可信任环境下，使用所述安全发行客户端的TPM RSA公钥对所述随机AES密钥加密，生成密钥文件，其中，所述密钥文件中还包括所述密钥偏移量IV；如果接收到所述安全发行客户端发送的密钥请求，所述密钥请求包括密钥请求文件和加密的第一请求验证信息，则在TPM可信任环境下，使用所述安全发行服务端的TPM RSA私钥解密所述加密的第一请求验证信息，得到解密后的第一请求验证信息，其中，所述第一请求验证信息是指通过所述安全发行客户端对所述密钥请求文件进行第一映射处理后得到的信息；对所述密钥请求文件进行第二映射处理，得到第二请求验证信息，其中，所述第一映射处理与所述第二映射处理的处理方法相同；通过所述第一请求验证信息和所述第二请求验证信息，验证所述密钥请求文件是否被篡改；如果所述密钥请求文件未被篡改，则将加密后的影片内容以及所述密钥文件发送至所述安全发行客户端；

所述安全发行客户端，用于生成密钥请求文件；对所述密钥请求文件进行第一映射处理，生成第一请求验证信息；使用安全发行服务端的TPM RSA公钥对所述第一请求验证信息加密，得到加密后的第一请求验证信息；将所述密钥请求文件和所述加密后的第一请求验证信息发送至所述安全发行服务端；如果接收到所述安全发行服务端发送的加密后的影片内容以及密钥文件，则在TPM可信任环境下，使用所述安全发行客户端的TPM RSA私钥解密所述密钥文件，得到随机AES密钥和密钥偏移量IV；在TPM可信任环境下，使用所述随机AES密钥和所述密钥偏移量IV解密所述加密后的影片内容。

12.一种4K影片内容的安全放映系统，其特征在于，所述安全放映系统包括如权利要求11所述的4K影片内容的安全发行系统，以及安全放映服务端、机顶盒、AI盗版检测网络端和水印追踪服务器端；

所述安全放映服务端，用于接收安全发行客户端发送的解密后的影片内容；对所述影片内容进行二次加密处理；将二次加密后的影片内容发送至机顶盒；

所述机顶盒，用于确定目标输出设备是否支持HDCP2.2；如果确定所述目标输出设备支持HDCP2.2，则向安全放映服务端发送影片内容密钥请求；如果接收到安全放映服务端发送的二次加密后的影片内容，则解密所述安全放映服务端二次加密后的影片内容，并在解密后的影片内容中插入第二水印标识，所述第二水印标识用标识机顶盒信息；将解密后的影片内容发送至所述目标输出设备；

所述机顶盒，还用于如果确定所述目标输出设备不支持HDCP2.2，则向所述目标输出设备发送第一指示信息，所述第一指示信息用于指示所述目标输出设备不支持HDCP2.2；

所述AI盗版检测网络端，用于接收安全发行客户端发送的确权电子凭证后，根据所述

确权电子凭证,检索疑似盗版视频;如果检索到疑似盗版视频,则将所述疑似盗版视频发送至所述水印追踪服务器端;

所述水印追踪服务器端,用于在接收到所述AI盗版检测网络端发送的所述疑似盗版视频后,提取所述疑似盗版视频中的水印标识;如果从所述疑似盗版视频中提取出水印标识,则将所述水印标识与用于存储第一水印标识的数据库以及用于存储第二水印标识的数据库比对,确定所述水印标识对应的信息是否属于第一水印标识或第二水印标识;如果所提取的水印标识对应的信息属于第一水印标识或第二水印标识,则向所述安全放映服务端发送第二指示信息,所述第二指示信息用于指示疑似盗版视频的转播来源对应的机顶盒信息,所述第二指示信息包括与所述水印标识对应的机顶盒信息;

所述安全放映服务端,还用于在接收到所述水印追踪服务器端发送的第二指示信息后,停止对所述疑似盗版视频的转播来源对应的机顶盒的授权许可。

13.根据权利要求12所述的4K影片内容的安全放映系统,其特征在于,所述机顶盒预先烧写与所述机顶盒相关的密钥证书到所述机顶盒基于高安芯片的TEE下。

14.根据权利要求13所述的4K影片内容的安全放映系统,其特征在于,所述机顶盒上安装有终端管理系统和DRM平台,其中,所述DRM平台基于四级密钥体系构建信任体系;

其中,所述四级密钥体系中第一级密钥为硬件信任根,所述硬件信任根包括可读取数据SN和不可读取数据IN;所述第一级密钥,用于所述机顶盒开机认证时,进行所述机顶盒与所述终端管理系统的双向认证;

所述四级密钥体系中第二级密钥为会话密钥R1,所述会话密钥R1由所述机顶盒在开机认证时生成,并经所述终端管理系统认证;

所述四级密钥体系中第三级密钥为终端密钥DK,所述终端密钥DK包括终端私钥和终端证书,所述终端证书包括终端公钥和证书链接;所述会话密钥R1,用于在所述DRM平台初始化时,对所述终端私钥加密,其中,所述终端证书和加密后的终端私钥保存在所述机顶盒的TEE中;

所述四级密钥体系中第四级密钥为内容密钥CK,所述内容密钥CK由所述终端公钥加密,所述内容密钥CK,用于加密内容。

一种4K影片内容的安全发行方法、系统及安全放映系统

技术领域

[0001] 本申请属于数字版权保护技术领域，尤其涉及一种4K影片内容的安全发行方法、系统及安全放映系统。

背景技术

[0002] 4K影片内容是指具有4K分辨率的影片内容，4K分辨率是指水平方向每行像素值达到或者接近4096个，4K分辨率属于超高清分辨率。而根据使用范围的不同，4K分辨率也有各种各样的衍生分辨率，例如Full Aperture 4K的4096×3112、Academy 4K的3656×2664以及UHDTV标准的3840×2160等，都属于4K分辨率的范畴。在此分辨率下，观众将可以看清画面中的每一个细节，每一个特写，从而为用户带来更好的视听体验。

[0003] 如果想将好莱坞4K影片内容引入国内，则不仅要满足好莱坞的内容保护标准(MovieLabs Specification for Enhanced Content Protection，ECP)要求，还要满足国内的中华人民共和国广播电视行业GY/T 277-2019规范要求。其中，ECP要求所有好莱坞片商在输出 UHD (超高清)片源时，在终端上实现基于芯片的硬件级别 DRM 保护，且在可信执行环境(TEE，Trusted Execution Environment)下运行；中华人民共和国广播电视行业GY/T 277-2019规范要求支持国密算法。

[0004] 但是，目前尚没有一种能够同时满足ECP要求和支持国密算法的技术方案，来保证电影分销商(或电影制片商)到电影服务提供商的安全发行交付。

发明内容

[0005] 为解决上述技术问题，本申请提供一种4K影片内容的安全发行方法、系统及安全放映系统。

[0006] 第一方面，本申请提供一种4K影片内容的安全发行方法，所述方法应用于安全发行服务端，所述方法包括：响应安全发行客户端的影片内容发行请求，生成随机AES密钥和密钥偏移量IV；使用随机AES密钥对所述影片内容加密；在TPM可信任环境下，使用所述安全发行客户端的TPM RSA公钥对所述随机AES密钥加密，生成密钥文件，其中，所述密钥文件中还包括所述密钥偏移量IV；如果接收到所述安全发行客户端发送的密钥请求，所述密钥请求包括密钥请求文件和加密的第一请求验证信息，则在TPM可信任环境下，使用所述安全发行服务端的TPM RSA私钥解密所述加密的第一请求验证信息，得到解密后的第一请求验证信息，其中，所述第一请求验证信息是指通过所述安全发行客户端对所述密钥请求文件进行第一映射处理后得到的信息；对所述密钥请求文件进行第二映射处理，得到第二请求验证信息，其中，所述第一映射处理与所述第二映射处理分处理方法相同；通过所述第一请求验证信息和所述第二请求验证信息，验证所述密钥请求文件是否被篡改；如果所述密钥请求文件未被篡改，则将加密后的影片内容以及所述密钥文件发送至所述安全发行客户端。

[0007] 一种可能的实现方式中，如果所述密钥请求文件未被篡改，还包括：对所述密钥文件进行第三映射处理，得到第一密钥验证信息；使用所述安全发行客户端的TPM RSA公钥对

所述第一密钥验证信息加密，得到加密的第一密钥验证信息；将所述密钥文件和所述加密后的第一密钥验证信息发送至所述安全发行客户端。

[0008] 一种可能的实现方式中，所述第一映射处理为散列运算或Base64编码；如果所述第一映射处理为散列运算，则所述第一请求验证信息为第一哈希值，所述第二请求验证信息为第二哈希值；则通过所述第一请求验证信息和所述第二请求验证信息，验证所述密钥请求文件是否被篡改，包括：对比所述第一哈希值与所述第二哈希值是否相同；如果所述第一哈希值与所述第二哈希值相同，则确定所述密钥请求文件未被篡改；如果所述第一哈希值与所述第二哈希值不相同，则确定所述密钥请求文件被篡改。

[0009] 一种可能的实现方式中，还包括在所述影片内容中插入第一水印标识的步骤，所述第一水印标识用于标识所述影片内容的发行信息，所述发行信息包括接收所述影片内容的安全发行客户端信息以及发行所述影片内容的安全发行服务端信息。

[0010] 一种可能的实现方式中，还包括：将加密后的影片内容以及所述密钥文件封装在安全发行包中；如果所述密钥请求文件未被篡改，则将所述安全发行包发送至所述安全发行客户端。

[0011] 第二方面，本申请提供一种4K影片内容的安全发行方法，所述方法应用于安全发行客户端，所述方法包括：生成密钥请求文件；对所述密钥请求文件进行第一映射处理，生成第一请求验证信息；使用安全发行服务端的TPM RSA公钥对所述第一请求验证信息加密，得到加密后的第一请求验证信息；将所述密钥请求文件和所述加密后的第一请求验证信息发送至所述安全发行服务端；如果接收到所述安全发行服务端发送的加密后的影片内容以及密钥文件，则在TPM可信任环境下，使用所述安全发行客户端的TPM RSA私钥解密所述密钥文件，得到随机AES密钥和密钥偏移量IV；在TPM可信任环境下，使用所述随机AES密钥和所述密钥偏移量IV解密所述加密后的影片内容。

[0012] 一种可能的实现方式中，还包括：接收所述安全发行服务端发送的密钥文件和加密后的第一密钥验证信息，其中，所述第一密钥验证信息是指通过所述安全发行服务端对所述密钥文件进行第三映射处理后得到的信息；对所述密钥文件进行第四映射处理，得到第二密钥验证信息，其中，所述第三映射处理方法与所述第四映射处理方法相同；使用安全发行客户端的TPM RSA私钥解密加密后的第一密钥验证信息，得到解密后的所述第一密钥验证信息；通过所述第一密钥验证信息和所述第二密钥验证信息，验证所述密钥文件是否被篡改；如果所述密钥文件未被篡改，则执行所述在TPM可信任环境下，使用所述安全发行客户端的TPM RSA私钥解密所述密钥文件，得到随机AES密钥的步骤及后续步骤。

[0013] 一种可能的实现方式中，所述第三映射处理为散列运算或Base64编码；如果所述第三映射处理为散列运算，则所述第一密钥验证信息为第三哈希值，所述第二密钥验证信息为第四哈希值；则通过所述第一密钥验证信息和所述第二密钥验证信息，验证所述密钥文件是否被篡改，包括：对比所述第三哈希值与所述第四哈希值是否相同；如果所述第三哈希值与所述第四哈希值相同，则确定所述密钥文件未被篡改；如果所述第三哈希值与所述第四哈希值不相同，则确定所述密钥文件被篡改。

[0014] 一种可能的实现方式中，所述生成密钥请求文件包括：采集所述安全发行客户端的密钥请求信息，所述密钥请求信息包括所述安全发行客户端的硬件信息、用户信息以及所请求的影片内容信息；根据所述密钥请求信息，生成所述密钥请求文件。

[0015] 一种可能的实现方式中，使用所述随机AES密钥和所述密钥偏移量IV解密所述加密后的影片内容后，还包括：在区块链上登记安全发行内容，所述安全发行内容包括所述安全发行服务端向所述安全发行客户端发送的影片内容信息、所述安全发行服务端的信息、以及所述安全发行客户端的信息，其中，所述区块链由电影服务商和电影分销商创建，所述区块链用于所述电影服务商和所述电影分销商之间的影片内容安全发行交易；根据所述安全发行内容，生成确权电子凭证；将所述确权电子凭证发送至AI盗版检测网络端。

[0016] 第三方面，本申请提供一种4K影片内容的安全发行系统，包括安全发行服务端和安全发行客户端；所述安全发行服务端，用于响应安全发行客户端的影片内容发行请求，生成随机AES密钥和密钥偏移量IV；使用随机AES密钥对所述影片内容加密；在TPM可信任环境下，使用所述安全发行客户端的TPM RSA公钥对所述随机AES密钥加密，生成密钥文件，其中，所述密钥文件中还包括所述密钥偏移量IV；如果接收到所述安全发行客户端发送的密钥请求，所述密钥请求包括密钥请求文件和加密的第一请求验证信息，则在TPM可信任环境下，使用所述安全发行服务端的TPM RSA私钥解密所述加密的第一请求验证信息，得到解密后的第一请求验证信息，其中，所述第一请求验证信息是指通过所述安全发行客户端对所述密钥请求文件进行第一映射处理后得到的信息；对所述密钥请求文件进行第二映射处理，得到第二请求验证信息，其中，所述第一映射处理方法与所述第二映射处理方法相同；通过所述第一请求验证信息和所述第二请求验证信息，验证所述密钥请求文件是否被篡改；如果所述密钥请求文件未被篡改，则将加密后的影片内容以及所述密钥文件发送至所述安全发行客户端；所述安全发行客户端，用于生成密钥请求文件；对所述密钥请求文件进行第一映射处理，生成第一请求验证信息；使用安全发行服务端的TPM RSA公钥对所述第一请求验证信息加密，得到加密后的第一请求验证信息；将所述密钥请求文件和所述加密后的第一请求验证信息发送至所述安全发行服务端；如果接收到所述安全发行服务端发送的加密后的影片内容以及密钥文件，则在TPM可信任环境下，使用所述安全发行客户端的TPM RSA私钥解密所述密钥文件，得到随机AES密钥和密钥偏移量IV；在TPM可信任环境下，使用所述随机AES密钥和所述密钥偏移量IV解密所述加密后的影片内容。

[0017] 第四方面，本申请提供一种4K影片内容的安全放映系统，所述放映系统包括如第三方面所述的4K影片内容的安全发行系统，以及安全放映系统；所述安全放映系统包括安全放映服务端、机顶盒、AI盗版检测网络端和水印追踪服务器端；所述安全放映服务端，用于接收安全发行客户端发送的解密后的影片内容；对所述影片内容进行二次加密处理；将二次加密后的影片内容发送至机顶盒；所述机顶盒，用于确定目标输出设备是否支持HDCP2.2；如果确定所述目标输出设备支持HDCP2.2，则向安全放映服务端发送影片内容密钥请求；如果接收到安全放映服务端发送的二次加密后的影片内容，则解密所述安全放映服务端二次加密后的影片内容，并在解密后的影片内容中插入第二水印标识，所述第二水印标识用标识机顶盒信息；将解密后的影片内容发送至所述目标输出设备；所述机顶盒，还用于如果确定所述目标输出设备不支持HDCP2.2，则向所述目标输出设备发送第一指示信息，所述第一指示信息用于指示所述目标输出设备不支持HDCP2.2；所述AI盗版检测网络端，用于接收安全发行客户端发送的确权电子凭证后，根据所述确权电子凭证，检索疑似盗版视频；如果检索到疑似盗版视频，则将所述疑似盗版视频发送至所述水印追踪服务器端；所述水印追踪服务器端，用于在接收到所述AI盗版检测网络端发送的所述疑似盗版视频

后,提取所述疑似盗版视频中的水印标识;如果从所述疑似盗版视频中提取出水印标识,则将所述水印标识与用于存储第一水印标识的数据库以及用于存储第二水印标识的数据库比对,确定所述水印标识对应的信息是否属于第一水印标识或第二水印标识;如果所提取的水印标识对应的信息属于第一水印标识或第二水印标识,则向所述安全放映服务端发送第二指示信息,所述第二指示信息用于指示疑似盗版视频的转播来源对应的机顶盒信息,所述第二指示信息包括与所述水印标识对应的机顶盒信息;所述安全放映服务端,还用于在接收到所述水印追踪服务器端发送的第二指示信息后,停止对所述疑似盗版视频的转播来源对应的机顶盒的授权许可。

[0018] 一种可能的实现方式中,所述机顶盒的芯片上预先烧写有与所述机顶盒相关的密钥证书。

[0019] 一种可能的实现方式中,所述机顶盒上安装有终端管理系统和DRM平台,其中,所述DRM平台基于四级密钥体系构建信任体系;其中,所述四级密钥体系中第一级密钥为硬件信任根,所述硬件信任根包括可读取数据SN和不可读取数据IN;所述第一级密钥,用于所述机顶盒开机认证时,进行所述机顶盒与所述终端管理系统的双向认证;所述四级密钥体系中第二级密钥为会话密钥R1,所述会话密钥R1由所述机顶盒在开机认证时生成,并经所述终端管理系统认证; 所述四级密钥体系中第三级密钥为终端密钥DK,所述终端密钥DK包括终端私钥和终端证书,所述终端证书包括终端公钥和证书链接;所述会话密钥R1,用于在所述DRM平台初始化时,对所述终端私钥加密,其中,所述终端证书和加密后的终端私钥保存在所述机顶盒的TEE中;所述四级密钥体系中第四级密钥为内容密钥CK,所述内容密钥CK由所述终端公钥加密,所述内容密钥CK,用于加密内容。

[0020] 综上,本申请提供的4K影片内容的安全发行方法、系统及安全放映系统,安全发行系统基于AES加解密算法和TPM可信任环境的公钥体系,同时满足ECP要求和支持国密算法,能够实现4K影片内容(电影原始母版介质)从电影分销商或电影内容制造商到电影服务提供商的安全发行交付;电影服务提供商在将影片内容分发前,在区块链上登记生成确权电子凭证,确权电子凭证可以为快速维权提供版权证明。安全放映系统,基于高安芯片的TEE机顶盒,限制机顶盒输出影片内容至支持HDCP2.2的输出设备,从而实现机顶盒到显示设备之间的链路保护;AI盗版检测网络端和水印追踪服务器端,可以实现从疑似盗版视频中提取水印标识,提取的水印标识也可以作为电子证据。因此,本申请实施例提供的4K影片内容的安全放映系统,不仅满足引入好莱坞4K内容的安全技术要求,电影服务提供商作为版权方在确认盗版后,还可以通过网络法院司法维权,司法维权时可调取区块链确权电子凭证以及水印标识作为电子证据。

附图说明

[0021] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍,显而易见地,下面描述中的附图是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0022] 图1为本申请实施例提供的一种4K影片内容的安全放映系统的结构框图;

[0023] 图2为本申请实施例提供的一种4K影片内容的安全发行系统的结构框图;

[0024] 图3A为本申请实施例提供的一种4K影片内容的安全发行方法的工作流程图；

[0025] 图3B为本申请实施例提供的又一种4K影片内容的安全发行方法的工作流程图；

[0026] 图4为本申请实施例提供的一种密钥请求文件的验证流程示意图；

[0027] 图5A为本申请实施例提供的一种联盟链的架构图；

[0028] 图5B为本申请实施例提供的一种注册创建部署联盟链的流程示意图；

[0029] 图5C为本申请实施例提供的一种内容版权交易登记的流程示意图；

[0030] 图6为本申请实施例提供的一种DRM平台的四级密钥体系的结构框图。

[0031] 附图标记说明

[0032] 101-安全发行服务端,102-安全发行客户端,103-安全放映服务端,104-机顶盒,105- AI盗版检测网络端,106-水印追踪服务器端,107-目标输出设备；

[0033] 201-证书服务系统,202-Peer节点,203-客户端,204-链码,205-共识网络,2051-Order节点,2052-背书Peer节点,2053-记账Peer节点。

具体实施方式

[0034] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0035] 参见图1,图1为本申请实施例提供的一种4K影片内容的安全放映系统,安全放映系统包括安全发行系统以及安全放映服务端103、机顶盒104、AI盗版检测网络端105和水印追踪服务器端106。其中,安全发行系统,用于保障电影内容制造商与电影服务提供商,或者,电影分销商与电影服务提供商之间影片内容的安全发行交付;安全放映服务端103、机顶盒104、AI盗版检测网络端105和水印追踪服务器端106,用于保障电影服务提供商与用户机顶盒之间影片内容的安全放映。

[0036] 下面首先结合附图对本申请实施例提供的安全发行系统进行说明。

[0037] 参见图2,图2为本申请实施例提供的一种4K影片内容的安全发行系统的结构框图。安全发行系统包括安全发行服务端101和安全发行客户端102,其中,安全发行服务端101是指电影内容制造商或电影分销商的安全发行服务端,安全发行客户端102是指电影服务提供商的安全发行客户端。

[0038] 本申请中安全发行服务端101和安全发行客户端102可以是诸如电脑、平板、智能手机等电子设备。

[0039] 在影片内容安全发行过程中,安全发行服务端101和安全发行客户端102,可以采用本申请实施例提供的4K影片内容的安全发行方法,该方法基于AES加解密算法和TPM可信任环境的公钥体系,实现4K影片内容(电影原始母版介质)从电影分销商或电影内容制造商到电影服务提供商的安全发行交付。

[0040] 下面分别以安全发行服务端101和安全发行客户端102为执行主体,对本申请实施例提供的4K影片内容的安全发行方法进行说明。

[0041] 首先以安全发行客户端102为执行主体,介绍本申请实施例提供的4K影片内容的安全发行方法,如图3A所示,包括以下步骤：

[0042] 步骤S101、生成密钥请求文件。

[0043] 一种可实现方式中，生成密钥请求文件，可以采用按照下述方式实现：先采集安全发行客户端102的密钥请求信息，其中，密钥请求信息可以包括安全发行客户端的硬件信息、用户信息以及所请求的影片内容信息；之后，根据密钥请求信息，生成密钥请求文件。

[0044] 步骤S102、对密钥请求文件进行第一映射处理，生成第一请求验证信息。

[0045] 一种可实现方式中，对密钥请求文件进行第一映射处理，可以采用按照下述方式实现：如图4所示，对密钥请求文件进行散列运算，生成第一哈希值，以第一哈希值作为第一请求验证信息。

[0046] 一种可实现方式中，对密钥请求文件进行第一映射处理，还可以采用按照下述方式实现：对密钥请求文件进行Base64编码，生成编码后的密钥请求文件，以编码后的密钥请求文件作为第一请求验证信息。

[0047] 步骤S103、使用安全发行服务端101的TPM RSA公钥对所述第一请求验证信息加密，得到加密后的第一请求验证信息。

[0048] 需要说明的是，TPM(Trusted Platform Module，可信任平台模块)是一种基于硬件的安全标准，该标准要求设备配备专用的防损芯片，以此提升设备的安全性。本申请中将这种防损芯片称为TPM 芯片。

[0049] TPM 芯片是一种安全的加密处理器，旨在执行加密操作。TPM芯片包含多重物理安全机制，具有防篡改功能，恶意软件无法篡改TPM的安全功能。TPM RSA作为非对称密钥，TPM RSA私钥已刻录到TPM 芯片中受到硬件安全级别的严密保护，故TPM RSA公钥无需考虑泄露问题，电影分销商和电影服务提供商已预先知晓彼此TPM RSA公钥。

[0050] 以安全发行服务端101和安全发行客户端102为电脑为例，本申请中安全发行服务端101和安全发行客户端102上安装有TPM芯片，这样，TPM芯片可以提供TPM可信任环境，使电脑更加安全地进行解码密钥的生成、储存和认证等，从而可以提升电脑的安全性。

[0051] 本申请中安全发行客户端102使用安全发行服务端101的TPM RSA公钥对第一请求验证信息加密，得到加密后的第一请求验证信息。

[0052] 应理解，如果第一请求验证信息为第一哈希值，则加密后的第一请求验证信息为对第一哈希值加密后的信息；如果第一请求验证信息为编码后的密钥请求文件，则加密后的第一请求验证信息为对编码后的密钥请求文件加密后的信息。

[0053] 步骤S104、将密钥请求文件和加密后的第一请求验证信息发送至安全发行服务端101。

[0054] 这样，本申请实施例提供的4K影片内容的安全发行方法，可以基于对密钥请求文件的验证，保障密钥请求文件在网络上的传输安全。

[0055] 进一步的，安全发行服务端101接收到安全发行客户端102发送的密钥请求文件和加密后的第一请求验证信息后，安全发行服务端101首先对密钥请求文件进行验证，以确认密钥请求文件是否在网络上安全传输、未经篡改。

[0056] 如果安全发行服务端101确认密钥请求文件没有被篡改，则安全发行服务端101可以根据安全发行客户端102的密钥请求文件，将加密的影片内容和密钥文件发送给安全发行客户端102。如果安全发行客户端102接收到安全发行服务端101发送的加密后的影片内容以及密钥文件，则安全发行客户端102执行如下步骤S105和步骤S106。

[0057] 步骤S105、在TPM可信任环境下，使用安全发行客户端102的TPM RSA私钥解密密钥文件，得到随机AES密钥和密钥偏移量IV。

[0058] 步骤S106、在TPM可信任环境下，使用随机AES密钥和密钥偏移量IV解密加密后的影片内容。

[0059] 接下来以安全发行服务端101为执行主体，本申请实施例提供的4K影片内容的安全发行方法，如图3B所示，包括以下步骤：

[0060] 步骤S201、响应安全发行客户端102的影片内容发行请求，生成随机AES密钥和密钥偏移量IV。

[0061] 步骤S202、使用随机AES密钥对所述影片内容加密。

[0062] 步骤S203、在TPM可信任环境下，使用安全发行客户端102的TPM RSA公钥对随机AES密钥加密，生成密钥文件，其中，密钥文件中还包括密钥偏移量IV。

[0063] 安全发行客户端102可以向安全发行服务端101发送影片内容发行请求，其中，影片内容发行请求中可以包括请求发行的影片内容信息以及安全发行客户端102自己的物理信息等。

[0064] 这样，安全发行服务端101接收到影片内容发行请求后，执行步骤S201至步骤203以实现对影片内容的加密处理。本申请实施例中，安全发行服务端101和安全发行客户端102对影片内容，采用AES加解密算法。其中，AES(Advanced Encryption Standard，高级加密标准)密钥，是一种对称密钥。

[0065] 进一步，安全发行服务端101对安全发行客户端102发送的密钥请求文件和加密后的第一请求验证信息进行验证，如果经安全发行服务端101验证，确认安全发行客户端102发送的密钥请求文件未被篡改，则安全发行服务端101将加密后的影片内容以及所述密钥文件发送至安全发行客户端102。

[0066] 以下通过步骤S204至步骤S206对验证密钥请求文件是否被篡改的方法进行说明。

[0067] 步骤S204、在TPM可信任环境下，使用所述安全发行服务端101的TPM RSA私钥解密所述加密的第一请求验证信息，得到解密后的第一请求验证信息。

[0068] 步骤S205、对所述密钥请求文件进行第二映射处理，得到第二请求验证信息，其中，第一映射处理方法与第二映射处理方法相同。

[0069] 其中，第一映射处理方法与第二映射处理方法相同，例如，第一映射处理方法与第二映射处理均为采用散列运算，又例如，第一映射处理方法与第二映射处理均为Base64编码。

[0070] 步骤S206、通过所述第一请求验证信息和所述第二请求验证信息，验证所述密钥请求文件是否被篡改。

[0071] 一种可实现方式中，通过第一请求验证信息和第二请求验证信息，验证密钥请求文件是否被篡改，可以采用按照下述方式实现：如果第一映射处理方法与第二映射处理均为采用散列运算，则第一请求验证信息为第一哈希值，第二请求验证信息为第二哈希值；进而对比对比第一哈希值与所述第二哈希值是否相同；如果第一哈希值与第二哈希值相同，则确定密钥请求文件未被篡改，表明密钥请求文件在网络上的传输是安全的；如果第一哈希值与第二哈希值不相同，则确定密钥请求文件被篡改，表明密钥请求文件在网络上的传输不是安全的。

[0072] 类似的，如果第一请求验证信息和第二请求验证信息为编码后的密钥请求文件，则对比两个编码后的密钥请求文件是否相同，如果相同，则确定密钥请求文件未被篡改，表明密钥请求文件在网络上的传输是安全的；如果不相同，则确定密钥请求文件被篡改，表明密钥请求文件在网络上的传输不是安全的。

[0073] 步骤S207、如果所述密钥请求文件未被篡改，则将加密后的影片内容以及所述密钥文件发送至所述安全发行客户端。

[0074] 一种可实现方式中，加密后的影片内容和密钥文件可以分别单独发送至安全发行客户端102；另一种可实现方式中，也可以先将加密后的影片内容和密钥文件封装在安全发行包中；然后将安全发行包发送至安全发行客户端102。

[0075] 另外，本申请中安全发行服务端101还可以在影片内容中插入水印标识，以下将安全发行服务端101插入在影片内容中水印标识称为第一水印标识。第一水印标识可以用于标识影片内容的发行信息，发行信息可以包括接收所述影片内容的安全发行客户端信息以及发行所述影片内容的安全发行服务端信息。第一水印标识可以在版权纠纷中提供确权证据。

[0076] 接下来，安全发行客户端102接收到安全发行服务端101发送的加密后的影片内容和密钥文件后，便可以执行上述步骤S105至步骤S106，对加密后的影片内容进行解密，从而获得解密后的影片内容。

[0077] 综上，本申请提供的4K影片内容的安全发行方法，基于AES加解密算法和TPM可信任环境的公钥体系，同时满足ECP要求和支持国密算法，能够实现4K影片内容(电影原始母版介质)从电影分销商或电影内容制造商到电影服务提供商的安全发行交付。

[0078] 上述实施例中通过对密钥请求文件的验证过程，保证用于验证的密钥请求文件在网络上的传输安全。进一步的，为保证密钥文件的安全传输，本申请还可以在确定密钥请求文件未被篡改后，先验证密钥文件传输是否安全，如果确认密钥文件传输安全，安全发行客户端102才执行步骤S105和步骤S106。

[0079] 下面对验证密钥文件传输是否安全的方法进行说明。

[0080] 一种可实现方式中，验证密钥文件传输是否安全，可以采用按照下述方式实现：请参见图4，如果安全发行服务端101确认密钥请求文件未被篡改，则安全发行服务端101先对密钥文件进行第三映射处理，得到第一密钥验证信息；之后，使用安全发行客户端102的TPM RSA公钥对第一密钥验证信息加密，得到加密的第一密钥验证信息；最后，将密钥文件和加密后的第一密钥验证信息发送至安全发行客户端102。

[0081] 一种可实现方式中，安全发行服务端101先对密钥文件进行第三映射处理，得到第一密钥验证信息，可以采用按照下述方式实现：对密钥文件进行散列运算，生成第三哈希值，以第三哈希值作为第一密钥验证信息。

[0082] 一种可实现方式中，安全发行服务端101先对密钥文件进行第三映射处理，得到第一密钥验证信息，还可以采用按照下述方式实现：对密钥文件进行Base64编码，生成编码后的密钥文件，以编码后的密钥文件作为第一密钥验证信息。

[0083] 这样，安全发行客户端102接收到安全发行服务端101发送的密钥文件和加密后的第一密钥验证信息后，安全发行客户端102首先对密钥文件进行验证，以确认密钥文件是否在网络上安全传输、未经篡改。

[0084] 一种可实现方式中，安全发行客户端102验证密钥文件是否被篡改，可以采用按照下述方式实现：安全发行客户端102对密钥文件进行第四映射处理，得到第二密钥验证信息；使用安全发行客户端102的TPM RSA私钥解密加密后的第一密钥验证信息，得到解密后的第一密钥验证信息；最后，通过第一密钥验证信息和第二密钥验证信息，验证密钥文件是否被篡改。其中，第三映射处理方法与第四映射处理方法相同。例如，第三映射处理方法与第四映射处理均为采用散列运算，又例如，第三映射处理方法与第四映射处理均为Base64编码。

[0085] 一种可实现方式中，安全发行客户端102通过第一密钥验证信息和第二密钥验证信息，验证密钥文件是否被篡改，可以采用按照下述方式实现：如果第三映射处理方法与第四映射处理均为采用散列运算，则第一密钥验证信息为第三哈希值，第二密钥验证信息为第四哈希值；进而安全发行客户端102对比第三哈希值与第四哈希值是否相同；如果所述第三哈希值与所述第四哈希值相同，则确定密钥文件未被篡改，表明密钥文件在网络上的传输是安全的；如果所述第三哈希值与所述第四哈希值不相同，则确定密钥文件被篡改，表明密钥文件在网络上的传输不是安全的。

[0086] 类似的，如果第一密钥验证信息和第二密钥验证信息为编码后的密钥文件，则对比两个编码后的密钥文件是否相同，如果相同，则确定密钥文件未被篡改，表明密钥文件在网络上的传输是安全的；如果不相同，则确定密钥文件被篡改，表明密钥文件在网络上的传输不是安全的。

[0087] 另外，请继续参见图1，本申请在安全发行服务端101与安全发行客户端102之间每完成一次4K影片内容的安全发行后，安全发行客户端102都可以在区块链上登记此次安全发行内容，其中，安全发行内容包括所述安全发行服务端101向所述安全发行客户端102发送的影片内容信息、所述安全发行服务端101的信息、以及所述安全发行客户端102的信息，其中，所述区块链由电影服务商和电影分销商创建，所述区块链用于所述电影服务商和所述电影分销商之间的影片内容安全发行交易；之后，根据安全发行内容，生成确权电子凭证；最后，将生成分确权电子凭证发送至AI盗版检测网络端105。这样，一方面，AI盗版检测网络端105接收到安全发行客户端101发送的确权电子凭证后，可以根据确权电子凭证，检索疑似盗版视频；另一方面，在需要司法维权时，本申请中的确权电子凭证可以作为有力的确权证据。

[0088] 其中，在区块链上登记安全发行内容，也可称为内容版权交易登记。

[0089] 下面对本申请提供的安全发行客户端102在区块链上进行内容版权交易登记的方法进行说明。

[0090] 本申请对区块链技术的实现方式不进行限定，一种可实现方式中，本申请采用符合Hyperledger Fabric协议规范的联盟链。如图5A所示，图5A为联盟链的架构图。联盟链架构中包括证书服务系统201、记账节点(Peer节点202)、客户端203、链码204和共识网络205。

[0091] 其中，证书服务系统201主要提供会员注册和证书颁发功能，Fabric系统的参与方都必须经过授权，比如排序服务节点(Order节点2051)、Peer节点202、客户端203等都需要拥有受信任的证书，证书一方面用于系统接入，另一方面用于交易签名。

[0092] 会员证书又分为注册证书和交易证书，注册证书与会员信息关联在一起，用于标识会员的身份，在必要的时候，还可以支持监管和审计；交易证书用于交易签名，交易证书

可以申请多份,使用不同的证书可以避免信息泄露(如多笔交易之间的关联关系)。

[0093] 一个区块链网络是一个联盟,一个联盟由多个组织组成。参见图5B,注册创建部署联盟链,可以通过以下方式实现:首先,电影服务提供商在证书服务系统中填写类型、组织名称、组织域名等信息创建组织,其中,组织可以以成员身份加入已经创建的联盟(电影分销商为盟主创建的联盟),也可以创建联盟成为盟主邀请其他组织(电影分销商),盟主邀请并批准其他组织加入联盟;之后,创建确权业务通道,其中通道主要用于实现区块链网络中业务的隔离,一个联盟中可以有多个通道,每个通道代表一项业务,并且对应一套账本,这意味着联盟链除了可以开展内容登记确定版权拥有者(即确权)的业务外,后期还有能力扩展其他业务;然后安装链码,安装好链码后,可以进行业务应用访问。

[0094] 请结合图5A和图5C,链码即智能合约,使用计算机语言编写内容版权交易(登记)法律合同中的条款,然后将编写的程序部署到区块链上去执行,同时其在代码中存储一份相应的内容版权交易(登记)法律合同文本文件以应对法律效力问题。链码204主要用于操作账本上的数据,运行于隔离的Docker容器中,在链码204部署的时候会自动生成合约的Docker镜像,使用获取状态(GetState)接口/存储状态(PutState)接口和Peer节点202通信存取账本数据(key-val状态数据库)。

[0095] 完整的区块链应用包含客户端203和链码204两部分。客户端203通过链码204与账本数据进行交互,客户端203通过区块链网络中部署的Peer节点202调用链码204,链码204通过区块链网络的Peer节点202来操作账本数据。

[0096] 如图5C所示,在安全发行服务端101与安全发行客户端102之间每完成一次4K影片内容的安全发行后,客户端都会构造一次内容版权交易登记提案。具体的,客户端发起构造内容版权交易登记提案,并发送给一个或多个背书Peer节点2052,其中,交易提案中可以包含本次提案要调用的合约标识、合约方法和参数信息以及客户端签名等;背书Peer节点2052收到内容版权交易登记提案后,会模拟执行并将原始内容版权交易登记提案和执行结果打包到一起,进行签名并发回给客户端203,其中,在模拟执行期间产生的数据修改不会写到账本上。客户端203收到各个背书Peer节点2502的响应后,将各个背书Peer节点2502的响应信息打包到一起,组成一个交易并签名,然后发送给Order节点2051。Order节点2051对接收到的交易进行共识排序,然后按照区块生成策略,将一批交易打包到一起,生成新的区块,发送给记账Peer节点2053;记账Peer节点2053收到区块后,会对区块中的每笔交易进行同步校验,检查交易依赖的输入输出是否符合当前区块链的状态,完成后将区块写入账本并修改账本数据。

[0097] 需要说明的是,如图5A至图5C中的客户端可以是本申请中安全发行客户端102。

[0098] 下面结合附图对本申请实施例提供的安全放映系统进行说明。

[0099] 参见图1,本申请实施例中的安全放映系统还包括安全放映服务端103、机顶盒104、AI盗版检测网络端105和水印追踪服务器端106。其中,安全放映服务端103是指电影服务提供商的安全放映服务端。

[0100] 安全发行客户端102获取到解密后的影片内容后,可以将解密后的影片内容发送给安全放映服务端103,这样,如果有用户请求播放影片内容,则安全放映服务端103和机顶盒104可以通过以下交互过程,将影片内容安全输出至用户的目标输出设备107。

[0101] 安全放映服务端103和机顶盒104的交互过程为:如果机顶盒104接收到目标输出

设备107的播放请求，机顶盒104首先确定目标输出设备107是否支持HDCP2.2，如果确定目标输出设备107支持HDCP2.2，则向安全放映服务端103发送影片内容密钥请求。如果确定目标输出设备107不支持HDCP2.2，机顶盒104会向目标输出设备107发送第一指示信息，第一指示信息用于指示目标输出设备107不支持HDCP2.2，对应的，在目标输出设备107会显示第一指示信息，如：在目标输出设备107显示文字“当前设备不支持HDCP2.2”。其中，HDCP为高带宽数字内容保护技术，用来保证传输的高清晰信号不会被非法录制，HDCP2.2是指HDCP的2.2版本。

[0102] 安全放映服务端103接收到机顶盒104发送的影片内容密钥请求后，首先将影片内容进行二次加密处理，然后，将二次加密后的影片内容发送给机顶盒104。

[0103] 机顶盒104接收到安全放映服务端103发送的加密后的影片内容后，解密所述安全放映服务端103二次加密后的影片内容，并在解密后的影片内容中插入第二水印标识，所述第二水印标识用标识机顶盒信息；之后，机顶盒104将解密后的影片内容发送至目标输出设备107。

[0104] 需要说明的是，本申请中安全发行服务端101对影片内容的加密处理也可以称为一次加密处理，安全放映服务端103对影片内容的加密处理称为二次加密处理。其中，二次加密处理的方法与一次加密处理的方法可以相同也可以不同。

[0105] 一种可实现方式中，本申请安全放映服务端103对影片内容的二次加密处理方法可以采用以下方式实现，安全放映服务端103接收到机顶盒104发送的影片内容播放请求后，依次使用内容加密密钥对影片内容进行加密、使用会话密钥对内容加密密钥进行加密、使用非对称密钥对用会话密钥加密后的信息进行加密；之后，将会话密钥和用会话密钥加密后的信息封装在内容授权许可中，用会话密钥加密后的信息是指用所述会话密钥对内容加密密钥加密后的信息；最后，安全放映服务端103向机顶盒104发送内容授权许可和加密的影片内容。

[0106] 对应的，机顶盒104接收到安全放映服务端103发送的内容授权许可和二次加密后的影片内容后，可以采用如下方法对二次加密后的影片内容进行解密：使用非对称密钥解密加密的内容授权许可，得到会话密钥；使用会话密钥解密用会话密钥加密后的信息，得到内容加密密钥，使用内容加密密钥解密所述加密的影片内容。

[0107] 还需要说明的是，本申请中机顶盒104为基于高安芯片的TEE机顶盒。本申请预先将与机顶盒104相关的密钥证书烧写到了机顶盒104的基于高安芯片的可信执行环境(Trusted Execution Environment，TEE)下，也就是说，本申请中，与机顶盒104相关的密钥证书在机顶盒104出厂时就烧写在机顶盒104的TEE安全存储区域。其中，高安芯片的TEE机顶盒是指在机顶盒中嵌入一个具有高级安全功能的芯片，在这个芯片中嵌入一个一次性写入(OTP)存储区域，在芯片封装之前将与机顶盒104相关的密钥证书写到这个存储区域，这样，密钥不容易被读取，从而提高机顶盒104安全性。

[0108] 这样，一方面，相比于现有的无法在线将相关的密钥证书烧写到TEE下的存量机顶盒，本申请提供的基于高安芯片的TEE机顶盒可以提供硬件安全级别保护，并可以通过限定目标输出设备必须为支持HDCP2.2的显示设备，来实现机顶盒到显示设备之间的链路保护；另一方面，使用本申请实施例提供的基于高安芯片的TEE机顶盒，能够满足播放4K影片内容的需求。

[0109] 还需要说明的是,本申请实施例中的机顶盒104上还可以安装终端管理系统和DRM平台。

[0110] 如图6所示,DRM平台为基于四级密钥体系构建信任体系,其中,四级密钥体系中第一级密钥为硬件信任根,所述硬件信任根包括可读取数据SN和不可读取数据IN;所述第一级密钥,用于所述机顶盒开机认证时,进行所述机顶盒与所述终端管理系统的双向认证;所述四级密钥体系中第二级密钥为会话密钥R1,所述会话密钥R1由所述机顶盒在开机认证时生成,并经所述终端管理系统认证;所述四级密钥体系中第三级密钥为终端密钥DK,所述终端密钥DK包括终端私钥和终端证书,所述终端证书包括终端公钥和证书链接;所述会话密钥R1,用于在所述DRM平台初始化时,对所述终端私钥加密,其中,所述终端证书和加密后的终端私钥保存在所述机顶盒的TEE中;所述四级密钥体系中第四级密钥为内容密钥CK,所述内容密钥CK由所述终端公钥加密,所述内容密钥CK,用于加密内容。

[0111] 上述四级密钥体系可以保护电视运营商发行的机顶盒的安全。

[0112] 进一步的,本申请实施例提供的安全放映系统还可以包括AI盗版检测网络端105和水印追踪服务器端106。

[0113] 请继续参见图1,AI盗版检测网络端105在接收到安全发行客户端102发送的确权电子凭证后,可以根据确权电子凭证,检索疑似盗版视频;如果检索到疑似盗版视频,则将疑似盗版视频发送至水印追踪服务器端106。

[0114] 需要说明的是,本申请对AI盗版检测网络端105的检索方法不进行限定,例如,AI盗版检测网络端105可以使用互联网搜索引擎,在网络上根据关键字(如电影名)检索疑似盗版视频、并可以对搜索结果采用现有NLP技术模型Transformer对搜索结果进行识别筛选。

[0115] 水印追踪服务器端106在接收到AI盗版检测网络端105发送的疑似盗版视频后,提取疑似盗版视频中的水印标识。如果从疑似盗版视频中提取出水印标识,则将提取出的水印标识与用于存储第一水印标识的数据库以及用于存储第二水印标识的数据库比对,确定提取出的水印标识对应的信息是否属于第一水印标识或第二水印标识。如果提取出的水印标识能够与第一水印标识匹配,则可以确定该疑似盗版视频的发行信息(如发行疑似盗版视频的安全发行服务端的信息以及安全发行客户端的信息);如果提取出的水印标识能够与第二水印标识匹配,则可以确定该疑似盗版视频的转播来源对应的机顶盒信息。

[0116] 需要说明的是,水印追踪服务器端106可能从疑似盗版视频提取出一个或多个水印标识,如果提取出多个水印标识可以一一与第一水印标识和第二水印标识匹配,其中,第一水印标识和第二水印标识分别存储在各自对应的数据库中。

[0117] 进一步的,为了防止非法转播事件的进一步扩大,尤其是对于直播视频的非法转播事件,一旦水印追踪服务器端106确定所提取的水印标识对应的信息属于第一水印标识或第二水印标识,则水印追踪服务器端106可以向安全放映服务端103发送第二指示信息,第二指示信息用于指示疑似盗版视频的转播来源对应的机顶盒信息,第二指示信息包括与所述水印标识对应的机顶盒信息。

[0118] 这样,在司法维权阶段,本申请中水印追踪服务器端106可以提供水印标识作为维权证据。

[0119] 综上,本申请实施例提供的安全发行服务端101,用于响应安全发行客户端的影片

内容发行请求，生成随机AES密钥和密钥偏移量IV；使用随机AES密钥对所述影片内容加密；在TPM可信任环境下，使用所述安全发行客户端的TPM RSA公钥对所述随机AES密钥加密，生成密钥文件，其中，所述密钥文件中还包括所述密钥偏移量IV；如果接收到所述安全发行客户端发送的密钥请求，所述密钥请求包括密钥请求文件和加密的第一请求验证信息，则在TPM可信任环境下，使用所述安全发行服务端的TPM RSA私钥解密所述加密的第一请求验证信息，得到解密后的第一请求验证信息，其中，所述第一请求验证信息是指通过所述安全发行客户端对所述密钥请求文件进行第一映射处理后得到的信息；对所述密钥请求文件进行第二映射处理，得到第二请求验证信息，其中，所述第一映射处理方法与所述第二映射处理方法相同；通过所述第一请求验证信息和所述第二请求验证信息，验证所述密钥请求文件是否被篡改；如果所述密钥请求文件未被篡改，则将加密后的影片内容以及所述密钥文件发送至所述安全发行客户端。

[0120] 本申请实施例提供的安全发行客户端102，用于生成密钥请求文件；对所述密钥请求文件进行第一映射处理，生成第一请求验证信息；使用安全发行服务端的TPM RSA公钥对所述第一请求验证信息加密，得到加密后的第一请求验证信息；将所述密钥请求文件和所述加密后的第一请求验证信息发送至所述安全发行服务端；如果接收到所述安全发行服务端发送的加密后的影片内容以及密钥文件，则在TPM可信任环境下，使用所述安全发行客户端的TPM RSA私钥解密所述密钥文件，得到随机AES密钥和密钥偏移量IV；在TPM可信任环境下，使用所述随机AES密钥和所述密钥偏移量IV解密所述加密后的影片内容。

[0121] 本申请实施例提供的安全放映服务端103，用于接收安全发行客户端发送的解密后的影片内容；对所述影片内容进行二次加密处理；将二次加密后的影片内容发送至机顶盒。

[0122] 本申请实施例提供的机顶盒104，用于确定目标输出设备是否支持HDCP2.2；如果确定所述目标输出设备支持HDCP2.2，则向安全放映服务端发送影片内容密钥请求；如果接收到安全放映服务端发送的二次加密后的影片内容，则解密所述安全放映服务端二次加密后的影片内容，并在解密后的影片内容中插入第二水印标识，所述第二水印标识用标识机顶盒信息；将解密后的影片内容发送至所述目标输出设备；还用于如果确定所述目标输出设备不支持HDCP2.2，则向所述目标输出设备发送第一指示信息，所述第一指示信息用于指示所述目标输出设备不支持HDCP2.2。

[0123] 本申请实施例提供的AI盗版检测网络端105，用于接收安全发行客户端发送的确权电子凭证后，根据所述确权电子凭证，检索疑似盗版视频；如果检索到疑似盗版视频，则将所述疑似盗版视频发送至所述水印追踪服务器端。

[0124] 本申请实施例提供的水印追踪服务器端106，用于在接收到所述AI盗版检测网络端发送的所述疑似盗版视频后，提取所述疑似盗版视频中的水印标识；如果从所述疑似盗版视频中提取出水印标识，则将所述水印标识与用于存储第一水印标识的数据库以及用于存储第二水印标识的数据库比对，确定所述水印标识对应的信息是否属于第一水印标识或第二水印标识；如果所提取的水印标识对应的信息属于第一水印标识或第二水印标识，则向所述安全放映服务端发送第二指示信息，所述第二指示信息用于指示疑似盗版视频的转播来源对应的机顶盒信息，所述第二指示信息包括与所述水印标识对应的机顶盒信息；

[0125] 本申请实施例提供的安全放映服务端，还用于在接收到所述水印追踪服务器端发

送的第二指示信息后，停止对所述疑似盗版视频的转播来源对应的机顶盒的授权许可。

[0126] 这样，本申请实施例提供的4K影片内容的安全放映方法及系统中，安全发行系统基于AES加解密算法和TPM可信任环境的公钥体系，同时满足ECP要求和支持国密算法，能够实现4K影片内容(电影原始母版介质)从电影分销商或电影内容制造商到电影服务提供商的安全发行交付；电影服务提供商在将影片内容分发前，在区块链上登记生成确权电子凭证，确权电子凭证可以为快速维权提供版权证明。基于高安芯片的TEE机顶盒，限制机顶盒输出影片内容至支持HDCP2.2的输出设备，从而实现机顶盒到显示设备之间的链路保护；AI盗版检测网络端和水印追踪服务器端，可以实现从疑似盗版视频中提取水印标识，提取的水印标识也可以作为电子证据。因此，本申请实施例提供的4K影片内容的安全放映方法及系统，不仅满足引入好莱坞4K内容的安全技术要求，电影服务提供商作为版权方在确认盗版后，还可以通过网络法院司法维权，司法维权时可调取区块链确权电子凭证以及水印标识作为电子证据。

[0127] 在一个可能的设计中，安全发行服务端包括处理器和存储器，其中，所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令供所述处理器调用执行；所述处理器用于：响应安全发行客户端的影片内容发行请求，生成随机AES密钥和密钥偏移量IV；使用随机AES密钥对所述影片内容加密；在TPM可信任环境下，使用所述安全发行客户端的TPM RSA公钥对所述随机AES密钥加密，生成密钥文件，其中，所述密钥文件中还包括所述密钥偏移量IV；如果接收到所述安全发行客户端发送的密钥请求，所述密钥请求包括密钥请求文件和加密的第一请求验证信息，则在TPM可信任环境下，使用所述安全发行服务端的TPM RSA私钥解密所述加密的第一请求验证信息，得到解密后的第一请求验证信息，其中，所述第一请求验证信息是指通过所述安全发行客户端对所述密钥请求文件进行第一映射处理后得到的信息；对所述密钥请求文件进行第二映射处理，得到第二请求验证信息，其中，所述第一映射处理方法与所述第二映射处理方法相同；通过所述第一请求验证信息和所述第二请求验证信息，验证所述密钥请求文件是否被篡改；如果所述密钥请求文件未被篡改，则将加密后的影片内容以及所述密钥文件发送至所述安全发行客户端。

[0128] 本发明实施例提供了一种计算机存储介质，所述计算机存储介质存储有一条或多条计算机指令，所述计算机指令被执行时实现4K影片内容的安全发行的方法。

[0129] 在另一个可能的设计中，安全发行客户端包括处理器和存储器，其中，所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令供所述处理器调用执行；所述处理器用于：生成密钥请求文件；对所述密钥请求文件进行第一映射处理，生成第一请求验证信息；使用安全发行服务端的TPM RSA公钥对所述第一请求验证信息加密，得到加密后的第一请求验证信息；将所述密钥请求文件和所述加密后的第一请求验证信息发送至所述安全发行服务端；如果接收到所述安全发行服务端发送的加密后的影片内容以及密钥文件，则在TPM可信任环境下，使用所述安全发行客户端的TPM RSA私钥解密所述密钥文件，得到随机AES密钥和密钥偏移量IV；在TPM可信任环境下，使用所述随机AES密钥和所述密钥偏移量IV解密所述加密后的影片内容。

[0130] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本发明的一般性原理并包括本发明未公开的本技术领域中的公知常识

或惯用技术手段。说明书和实施例仅被视为示例性的，本发明的真正范围和精神由所附的权利要求指出。

[0131] 应当理解的是，本发明并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本发明的范围仅由所附的权利要求来限制。

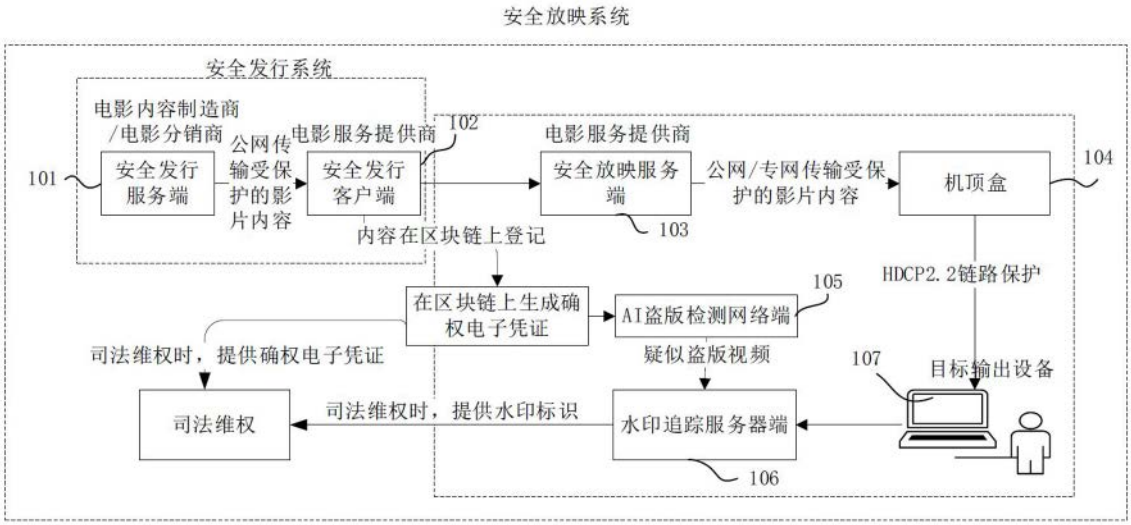

安全放映系统
安全发行系统
电影内容制造商
/电影分销商
101
安全发行
服务端
公网传
输受保
护的影
片内容
电影服务提供商
安全发行
客户端
102
内容在区块链上登记
电影服务提供商
安全放映服务
端
103
公网/专网传输受保
护的影片内容
机顶盒
104
HDCP2.2链路保护
在区块链上生成确
权电子凭证
AI盗版检测网络端
105
疑似盗版视频
司法维权时，提供确权电子凭证
107
目标输出设备
司法维权
司法维权时，提供水印标识
水印追踪服务器端
106

图1

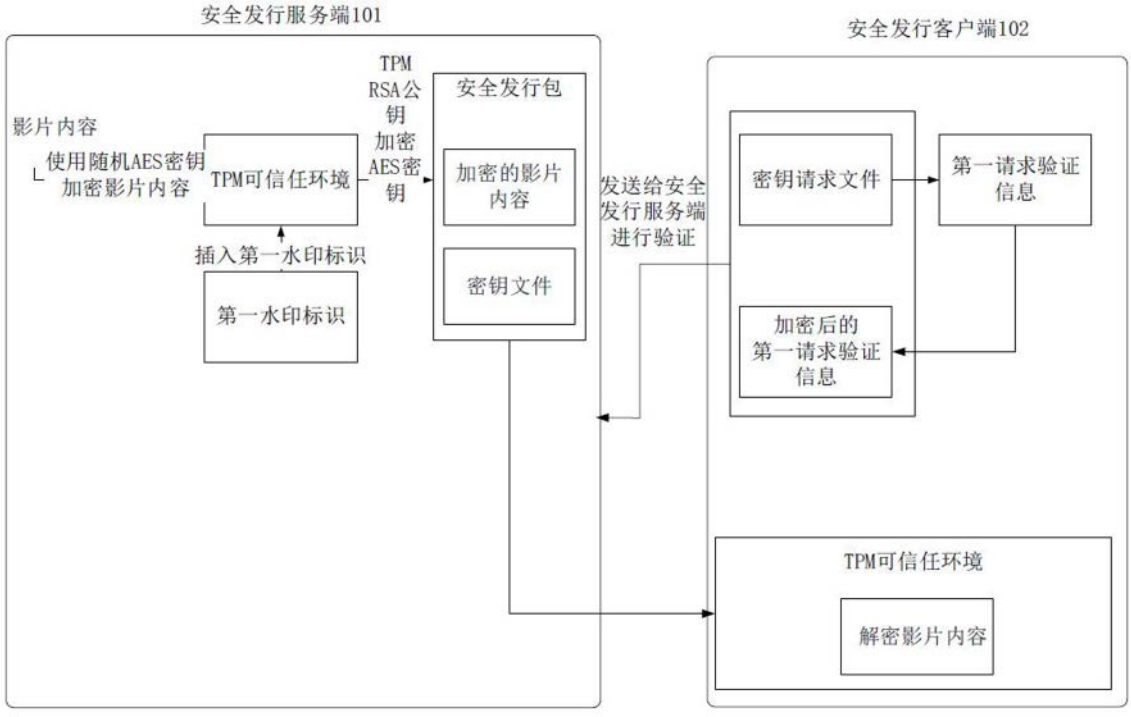

安全发行服务端101
安全发行客户端102
影片内容
使用随机AES密钥
加密影片内容
TPM可信任环境
TPM
RSA公
钥
加密
AES密
钥
安全发行包
加密的影片
内容
密钥文件
插入第一水印标识
第一水印标识
发送给安全
发行服务端
进行验证
密钥请求文件
第一请求验证
信息
加密后的
第一请求验证
信息
TPM可信任环境
解密影片内容

图2

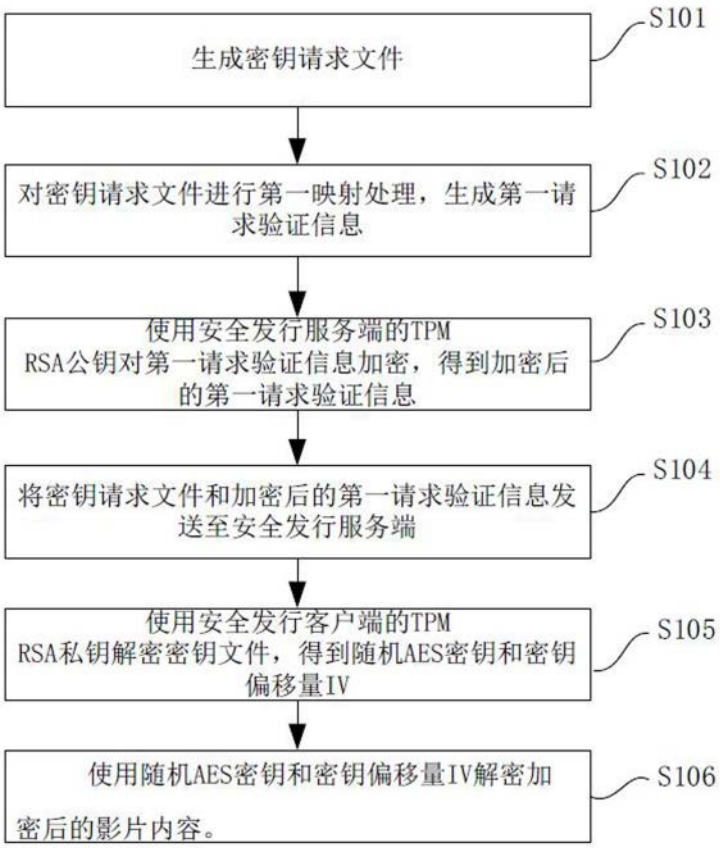

生成密钥请求文件
S101
对密钥请求文件进行第一映射处理，生成第一请求验证信息
S102
使用安全发行服务端的TPM RSA公钥对第一请求验证信息加密，得到加密后的第一请求验证信息
S103
将密钥请求文件和加密后的第一请求验证信息发送至安全发行服务端
S104
使用安全发行客户端的TPM RSA私钥解密密钥文件，得到随机AES密钥和密钥偏移量IV
S105
使用随机AES密钥和密钥偏移量IV解密加密后的影片内容。
S106

图3A

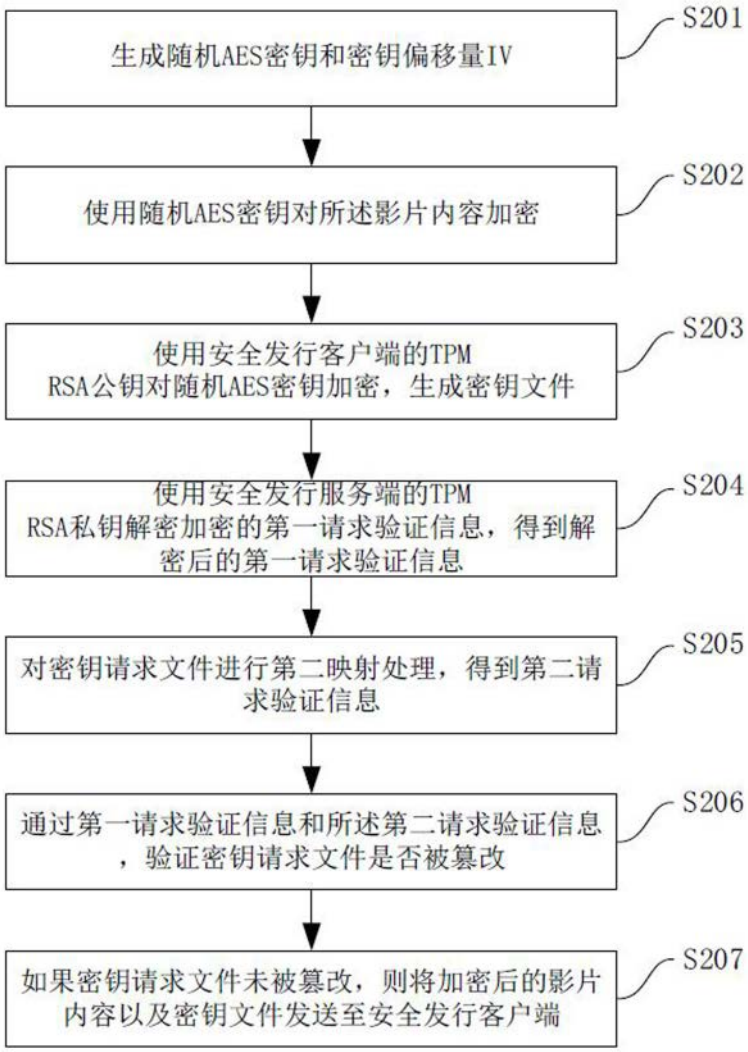

S201
生成随机AES密钥和密钥偏移量IV
S202
使用随机AES密钥对所述影片内容加密
S203
使用安全发行客户端的TPM
RSA公钥对随机AES密钥加密，生成密钥文件
S204
使用安全发行服务端的TPM
RSA私钥解密加密的第一请求验证信息，得到解密后的第一请求验证信息
S205
对密钥请求文件进行第二映射处理，得到第二请求验证信息
S206
通过第一请求验证信息和所述第二请求验证信息，验证密钥请求文件是否被篡改
S207
如果密钥请求文件未被篡改，则将加密后的影片内容以及密钥文件发送至安全发行客户端

图3B

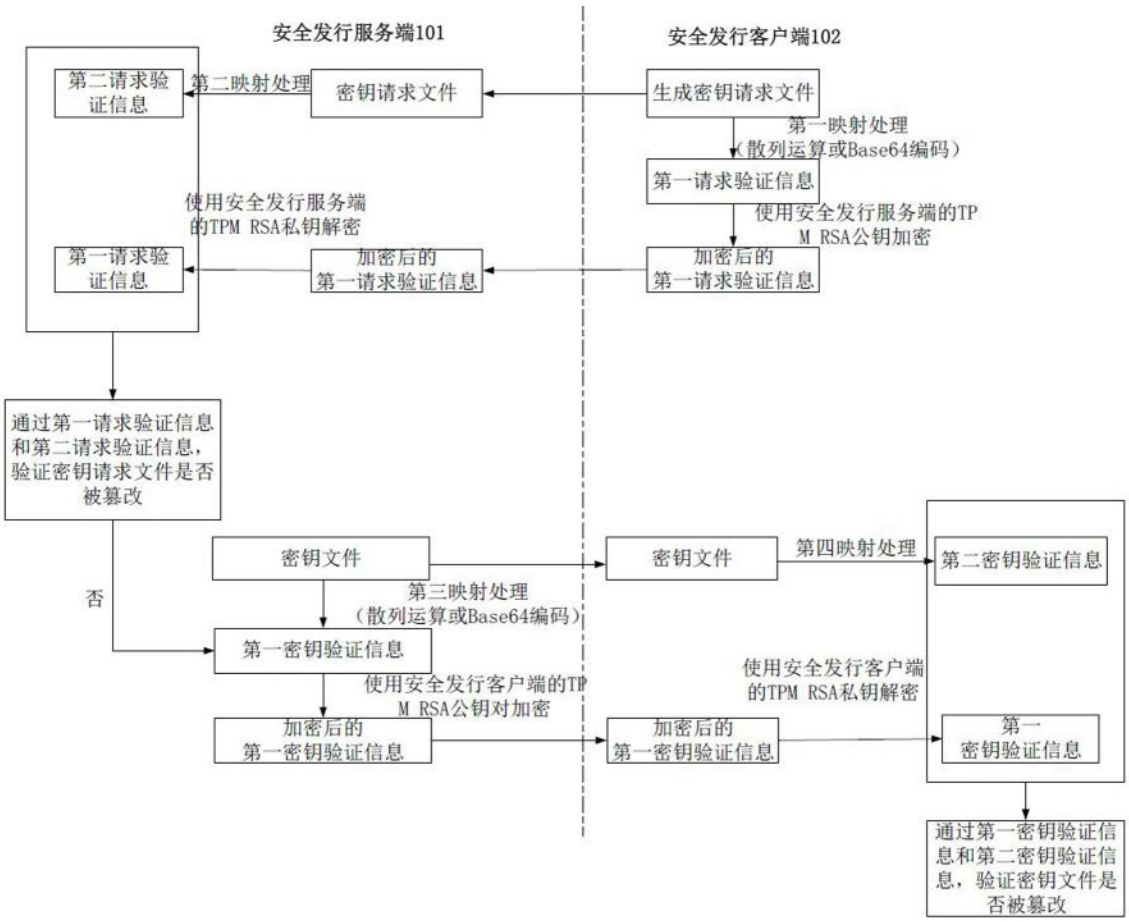

安全发行服务端101
安全发行客户端102
第二请求验证信息
第二映射处理
密钥请求文件
生成密钥请求文件
第一映射处理
（散列运算或Base64编码）
第一请求验证信息
使用安全发行服务端的TPM RSA公钥加密
使用安全发行服务端的TPM RSA私钥解密
第一请求验证信息
加密后的第一请求验证信息
加密后的第一请求验证信息
通过第一请求验证信息和第二请求验证信息，验证密钥请求文件是否被篡改
否
密钥文件
密钥文件
第四映射处理
第二密钥验证信息
第三映射处理
（散列运算或Base64编码）
第一密钥验证信息
使用安全发行客户端的TPM RSA公钥对加密
使用安全发行客户端的TPM RSA私钥解密
加密后的第一密钥验证信息
加密后的第一密钥验证信息
第一密钥验证信息
通过第一密钥验证信息和第二密钥验证信息，验证密钥文件是否被篡改

图4

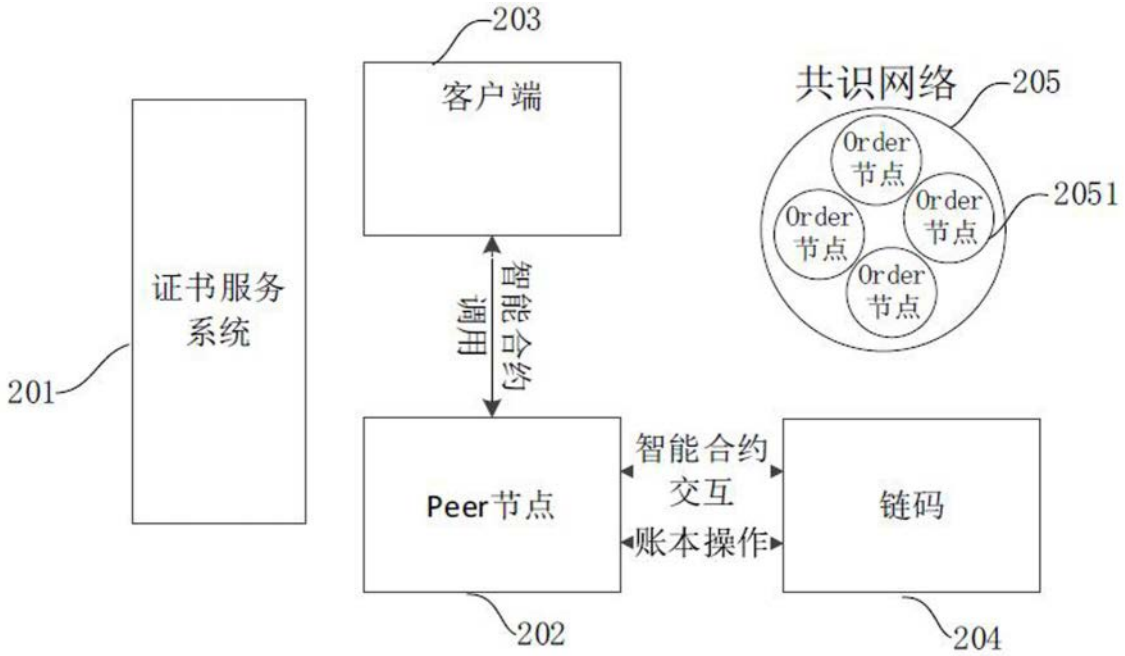

203
客户端
共识网络
205
Order节点
Order节点
Order节点
Order节点
2051
证书服务系统
201
调用
智能合约
Peer节点
智能合约
交互
账本操作
链码
202
204

图5A


电影服务提供商创建组织
创建联盟
邀请组织（电影分销商）加入联盟
创建确权业务通道
安装链码
业务应用访问

图5B

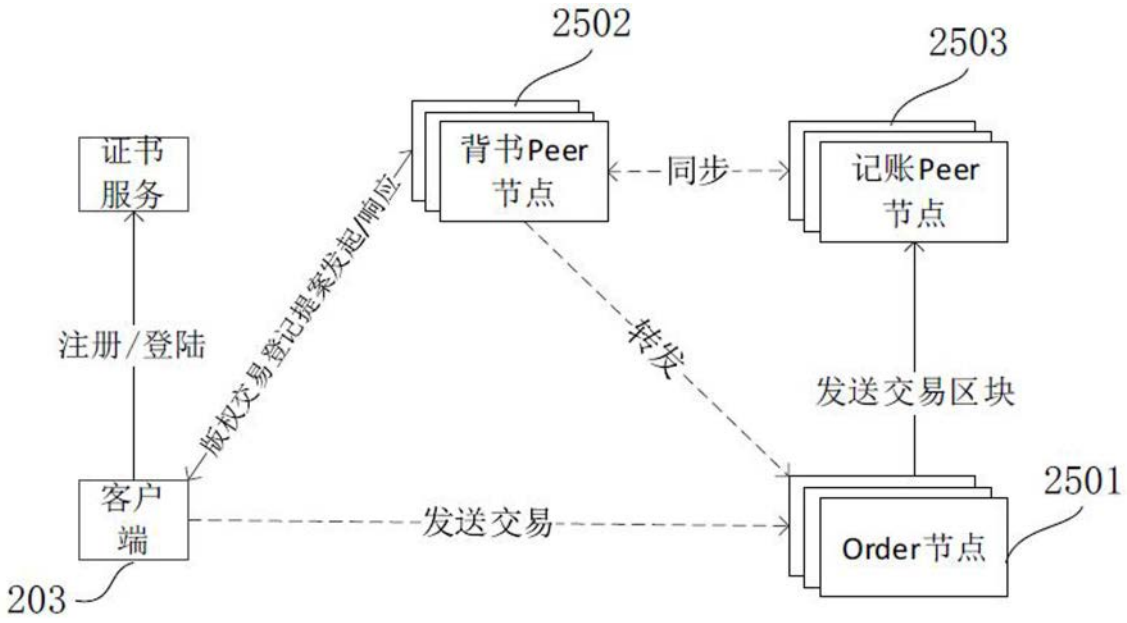

2502
2503
证书服务
背书Peer节点
同步
记账Peer节点
版权交易登记提案发起/响应
转发
注册/登陆
发送交易区块
客户端
发送交易
Order节点
2501
203

图5C

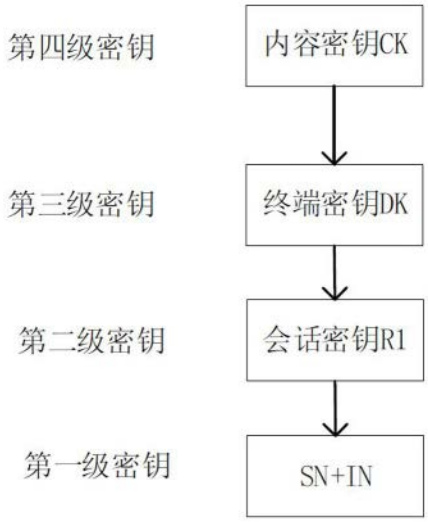

第四级密钥
内容密钥CK
第三级密钥
终端密钥DK
第二级密钥
会话密钥R1
第一级密钥
SN+IN

图6