(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103546767 B
(45)授权公告日 2017.01.25

(21)申请号 201210246709.0

(22)申请日 2012.07.16

(65)同一申请的已公布的文献号
申请公布号 CN 103546767 A

(43)申请公布日 2014.01.29

(73)专利权人 航天信息股份有限公司
地址 100195 北京市海淀区杏石口路甲18号航天信息园

(72)发明人 罗世新 郭宝安

(74)专利代理机构 北京工信联合知识产权代理事务所(普通合伙) 11266
代理人 黄晓军

(51)Int.Cl.
H04N 21/2389(2011.01)
H04N 21/254(2011.01)
H04N 21/262(2011.01)
H04N 21/435(2011.01)
H04N 21/4385(2011.01)
H04N 21/462(2011.01)
H04N 21/6334(2011.01)

(56)对比文件
CN 101626488 A,2010.01.13,
CN 101902611 A,2010.12.01,
CN 1822165 A,2006.08.23,
CN 101790735 A,2010.07.28,
CN 101076109 A,2007.11.21,
CN 101409592 A,2009.04.15,
CN 101505400 A,2009.08.12,
CN 1549595 A,2004.11.24,
CN 102238422 A,2011.11.09,
JP 4801515 B2,2011.10.26,

审查员 张鑫垚

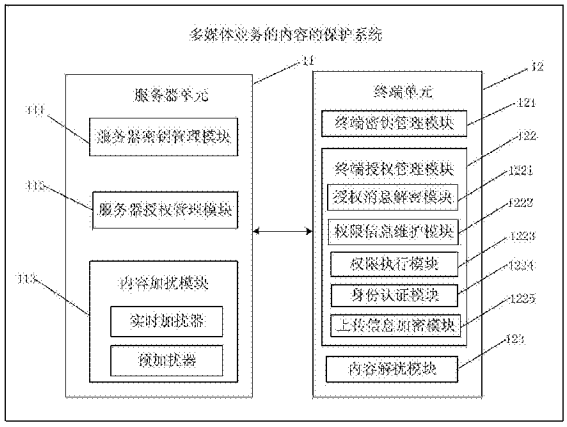
权利要求书4页 说明书10页 附图3页

(54)发明名称

多媒体业务的内容保护方法和系统

(57)摘要

本发明提供了一种多媒体业务的内容保护方法和系统。基于对多媒体业务的节目内容在网络传输时对视音频流的保护需要,对实时节目流采用身份密钥TIK、个人密钥或域密钥PK/DK、业务密钥SK和控制字CW四层密钥体系,对非实时节目流采用身份密钥TIK、个人密钥或域密钥PK/DK和内容加密密钥CEK三层密钥体系,通过对多媒体业务实时流四层密钥和非实时流三层密钥的授权和管理控制解决应用安全问题;并且本发明使用国家自主知识产权的密码算法,引入了身份认证机制,是安全灵活可靠、易于推广实施的。



CN 103546767 B

1.一种多媒体业务的内容保护系统,其特征在于,包括:

服务器单元,用于完成对多媒体业务的节目内容的加密、密钥管理和终端用户授权管理,并实现与终端交互信息的认证;

终端单元,用于完成多媒体业务的节目内容、各级密钥或权限的解密,实现终端与服务器的交互认证,执行终端用户的权限对应的业务内容;所述的服务器单元包括:

服务器密钥管理模块,用于实现本系统所使用密钥的产生、存储、更新和发放,所述密钥包括对称密钥和非对称密钥,所述对称密钥包括:个人密钥PK或域密钥DK、业务密钥SK、控制字密钥CW和内容加密密钥CEK,所述非对称密钥包括:服务器和终端的错误检查和纠正ECC公私钥对和相关参数;

服务器授权管理模块,用于实现终端用户认证和终端用户的权限信息管理,根据终端用户的权限授予终端用户相应节目的许可和使用权限,产生和发送终端用户的授权消息,所述终端用户认证包括:终端用户接入认证、在线注册认证、在线业务申请认证,所述终端用户的权限包括:给终端用户提供直播、点播的权限或者终端用户下载业务的权限;

内容加扰模块,用于实现对直播节目、点播或下载节目的加扰与安全控制,并按照指定格式封装节目码流;

所述的服务器密钥管理模块,还用于对直播业务采用如下的四层密钥管理体系:

第1层:服务器的身份密钥SIK和终端用户的身份密钥TIK,用于保护PK或DK在线分发和实现终端用户与服务器端之间的身份认证;

第2层:PK或DK,其中PK用于实现终端用户的授权管理和保护终端用户的SK在线分发,DK用于实现终端用户组的授权管理和保护终端用户组的SK在线分发;

第3层:SK,用于实现分类业务、独立业务或业务组的控制授权和保护CW实时发放;

第4层:CW,用于实现媒体内容的传输保护,随节目流信息定时在线分发;

对点播或下载业务采用如下的三层密钥体系:

第1层:服务器的身份密钥SIK和终端用户的身份密钥TIK,用于保护PK或DK在线分发和实现终端用户与服务器端之间的身份认证;

第2层:PK或DK,其中PK用于实现终端用户的授权管理和保护终端用户的内容加密密钥CEK在线分发,DK用于实现终端用户组的授权管理和保护终端用户组的CEK在线分发;

第3层:CEK,用于实现点播媒体流和下载媒体内容的加密。

2.根据权利要求1所述的多媒体业务的内容保护系统,其特征在于:

所述的服务器密钥管理模块,还用于在系统初始化或终端安全模块初始化时,以离线方式将所述终端用户的ECC密钥对分发给终端;

在终端用户注册时,在所述终端用户的ECC公钥加密保护下通过在线或离线的方式将所述终端用户的PK或DK分发给终端;

在终端申请业务时,在所述终端用户的PK或DK加密保护下将所述终端用户的SK分发给所述终端;

在系统广播加密的节目内容时,在所述终端用户的SK加密保护下将所述终端用户的CW随被加扰的节目内容一起分发给所述终端;

在终端申请非实时业务授权时,在所述终端用户的PK或DK加密保护下将所述终端用户的CEK分发给所述终端。

3.根据权利要求1所述的多媒体业务的内容保护系统，其特征在于，所述的内容加扰模块包括：

实时加扰器，用于在密码算法和CW的作用下实现对直播节目的加扰；

预加扰器，用于在密码算法、CEK作用下实现对点播节目和下载节目的预加扰，预加扰后的节目内容存入节目服务器。

4.根据权利要求1至3任一项所述的多媒体业务的内容保护系统，其特征在于，所述终端单元包括：

终端密钥管理模块，用于完成终端用户的各种密钥和相关参数的存储和管理，所述密钥包括：ECC密钥、对称密钥；

终端授权管理模块，用于完成授权消息解密、权限信息维护、权限执行、身份认证和上传信息加密处理；

内容解扰模块，用于在所述终端密钥管理模块、终端授权管理模块的控制下，采用与服务器的节目内容加扰处理对应的方法完成直播、点播或下载媒体节目内容的解扰处理。

5.根据权利要求4所述的多媒体业务的内容保护系统，其特征在于，所述终端授权管理模块包括：

授权消息解密模块，用于根据接收的权限管理消息和授权控制消息完成终端用户的各层密钥和权限信息的解密，提取出终端用户的收视条件信息，该收视条件信息包括密钥、有效期、播放控制参数；

权限信息维护模块，用于根据接收到的授权消息，保存、更新、维护终端用户的权限信息；

权限执行模块，用于根据接收到的权限信息控制密钥接收、密钥使用和控制机卡之间密钥的传递，达到控制节目解密和播放的目的；

身份认证模块，用于实现终端和服务器之间交互数据的签名或验证运算；

上传信息加密模块，用于完成终端向服务器提交的交互信息产生和加密处理。

6.一种多媒体业务的内容保护方法，其特征在于，包括：

服务器完成对多媒体业务的节目内容的加密、密钥管理和终端用户授权管理，并实现与终端交互信息的认证；

终端完成多媒体业务的节目内容、各级密钥或权限的解密，实现终端与服务器的交互认证，执行终端用户的权限对应的业务内容；所述的方法还包括：

所述服务器对直播业务采用如下的四层密钥管理体系：

第1层：服务器的身份密钥SIK和终端用户的身份密钥TIK，用于保护PK或DK在线分发和实现终端用户与服务器端之间的身份认证；

第2层：PK或DK，其中PK用于实现终端用户的授权管理和保护终端用户的SK在线分发，DK用于实现终端用户组的授权管理和保护终端用户组的SK在线分发；

第3层：SK，用于实现分类业务、独立业务或业务组的控制授权和保护CW实时发放；

第4层：CW，用于实现媒体内容的传输保护，随节目流信息定时在线分发；

所述服务器对点播或下载业务采用如下的三层密钥体系：

第1层：服务器的身份密钥SIK和终端用户的身份密钥TIK，用于保护PK或DK在线分发和实现终端用户与服务器端之间的身份认证；

第2层:PK或DK,其中PK用于实现终端用户的授权管理和保护终端用户的内容加密密钥CEK在线分发,DK用于实现终端用户组的授权管理和保护终端用户组的CEK在线分发;

第3层:CEK,用于实现点播媒体流和下载媒体内容的加密。

7.根据权利要求6所述的多媒体业务的内容保护方法,其特征在于,所述的方法还包括:

所述服务器在系统初始化或终端安全模块初始化时,以离线方式将所述终端用户的ECC密钥对分发给终端;

所述服务器在终端用户注册时,在所述终端用户的ECC公钥加密保护下通过在线或离线的方式将所述终端用户的PK或DK分发给终端;

所述服务器在终端申请业务时,在所述终端用户的PK或DK加密保护下将所述终端用户的SK分发给所述终端;

所述服务器在系统广播加密的节目内容时,在所述终端用户的SK加密保护下将所述终端用户的CW随被加扰的节目内容一起分发给所述终端;

所述服务器在终端申请非实时业务授权时,在所述终端用户的PK或DK加密保护下将所述终端用户的CEK分发给所述终端。

8.根据权利要求7所述的多媒体业务的内容保护方法,其特征在于,所述的方法还包括:

所述服务器产生所述终端用户的PK或DK和与PK或DK关联的权限信息$C_{P或D}$,将所述终端用户的PK或DK和$C_{P或D}$进行保存;

所述服务器产生权利管理消息$RMM_{P或D}$

$RMM_{P或D}=PE_{TIKpub}(PK或DK\|C_{P或D})\|PE_{SIKpri}(H(PK或DK\|C_{P或D}))$,将所述$RMM_{P或D}$加密后发送到终端用户的终端,所述PE为非对称密码算法SM2,所述H为使用SM3算法进行的Hash运算,所述||为链接;

所述终端接收到所述$RMM_{P或D}$后,使用终端用户的私钥TIK_{pri}解密所述$RMM_{P或D}$,得到所述PK或DK和$C_{P或D}$明文,并利用所述服务器的公钥SIK_{pub}验证所述$RMM_{P或D}$的有效性,如果验证确认所述$RMM_{P或D}$有效,则保存所述解密得到的PK或DK和$C_{P或D}$;否则,丢弃所述解密得到的PK或DK和$C_{P或D}$。

9.根据权利要求7所述的多媒体业务的内容保护方法,其特征在于,所述的方法还包括:

所述服务器随机产生所述终端用户的SK和与SK关联的权限信息C_S,用所述终端用户的PK或DK对SK和C_S进行加密,得到SK的权利消息RMM_S:

$RMM_S=E_{PK或DK}(SK\|C_S)\|H(SK\|C_S)$

所述E表示对称密码算法SM1;

所述服务器将RMM_S以指定的授权方式发送到所述终端;

所述终端接收到所述RMM_S后,用所述终端用户的PK或DK解密RMM_S得到$SK\|C_S$,计算$H(SK\|C_S)$,将计算出的$H(SK\|C_S)$与解密后的RMM_S中包含的$H(SK\|C_S)$值比较,如果所述比较结果为相等,则所述终端接受所述解密得到的SK和C_S;否则,拒绝接受所述解密得到的SK和C_S。

10.根据权利要求7所述的多媒体业务的内容保护方法,其特征在于,所述的方法还包括:

所述服务器随机产生所述终端用户的CW，并产生使用该CW的控制参数P，用所述终端用户的SK对所述终端用户的CW进行加密并计算HASH，获得授权控制消息ECM：

$ECM = E_{SK}(CW \| P) \| H(CW \| P)$

所述服务器将所述ECM随节目流发送到终端；

所述终端接收到所述ECM后，用自己的SK解密所述ECM，获取解密后的ECM中包含的CW和P，计算H(CW‖P)，将计算出的H(CW‖P)与解密后的ECM中包含的H(CW‖P)值比较，如果所述比较结果为相等，则所述终端接受所述解密得到的CW和P；否则，拒绝接受所述解密得到的CW和P。

11.根据权利要求7所述的多媒体业务的内容保护方法，其特征在于，所述的方法还包括：

所述终端通过交互信道向服务器发送交互业务授权请求REQ_T

$REQ_T = E_{PK或DK}(TID \| CID \| W \| r) \| PE_{TIKpri}(H(TID \| CID \| W \| r))$

所述CID为节目标识信息，所述W为申请业务的消费需求信息，

所述服务器接收到所述REQ_T后，用所述终端用户的PK或DK解密所述REQ_T，用所述终端用户的身份密钥公钥TIK_{pub}验证所述REQ_T的签名的有效性；

所述服务器在验证所述REQ_T的签名有效后，发送点播或下载文件授权消息RES_S

$RES_S = RMM_c = E_{PK或DK}(CEK \| CC \| r) \| H(CEK \| CC \| r)$

所述CC为授予的申请节目权限信息；

所述终端接收到所述RES_S后，用自己的PK或DK解密所述RES_S，获取解密后的RES_S中包含的CEK‖CC‖r，计算H(CEK‖CC‖r)，将计算出的H(CEK‖CC‖r)与解密后的RES_S中包含的H(CEK‖CC‖r)值比较，如果所述比较结果为相等，则所述终端接受所述解密得到的CEK，按照权限信息CC，用CEK对点播或下载文件进行解密；否则，拒绝接受所述解密得到的CEK。

多媒体业务的内容保护方法和系统

技术领域

[0001] 本发明涉及多媒体技术领域，尤其涉及一种多媒体业务的内容保护方法和系统。

背景技术

[0002] 手机电视，指以手机等便携式手持终端为设备，传播视听内容的一项技术或应用。目前，手机电视业务的实现方式主要有两种：第一种是通信方式，利用移动通信技术、通过无线通信网向手机点对点提供多媒体服务；第二种是广播方式，利用数字广播电视技术，通过地面或卫星广播电视覆盖网向手机、PDA、MP3、MP4、数码相机、笔记本电脑以及在车船上的小型接收终端点对面提供广播电视节目。

[0003] 目前，手机电视业务等多媒体业务受到许多移动运营商、广电公司的关注，纷纷开展各种承载技术的试验，手机电视商用业务已经出现在世界各地。手机电视业务的承载技术多样化，且地域特征明显，很难形成统一的手机电视标准。不同地域或者不同国家的运营商在部署手机电视业务时倾向于使用基于本地区、本国家的数字电视标准发展而来的手机电视标准。

[0004] 手机电视的媒体内容是经数字化处理后的数字媒体，易于存储、无损复制与传播，特别是点播节目和供终端用户下载的媒体文件，可以方便地下载、存储、批量复制，由此滋生的大量盗版及不规范的使用行为，对手机电视产业将造成巨大的冲击。因此，开发一种对手机电视等多媒体业务内容进行有效保护的方法是十分必要的。

发明内容

[0005] 本发明的实施例提供了一种多媒体业务的内容保护方法和系统，以实现对手机电视等多媒体业务内容进行有效的保护。

[0006] 一种多媒体业务的内容保护系统，包括：

[0007] 服务器单元，用于完成对多媒体业务的节目内容的加密、密钥管理和终端用户授权管理，并实现与终端交互信息的认证；

[0008] 终端单元，用于完成多媒体业务的节目内容、各级密钥或权限的解密，实现终端与服务器的交互认证，执行终端用户的权限对应的业务内容。

[0009] 一种多媒体业务的内容保护方法，包括：

[0010] 服务器完成对多媒体业务的节目内容的加密、密钥管理和终端用户授权管理，并实现与终端交互信息的认证；

[0011] 终端完成多媒体业务的节目内容、各级密钥或权限的解密，实现终端与服务器的交互认证，执行终端用户的权限对应的业务内容。

[0012] 由上述本发明的实施例提供的技术方案可以看出，本发明实施例通过对直播业务采用四层密钥体系，对点播或下载业务采用三层密钥体系，并且由于所有密码算法本身都是安全的，密码使用流程中密钥信息和密文信息都是安全的，所有需要用密码保护的信息均被有效保护，从而有效地保证了手机电视等多媒体业务的节目内容的安全。

附图说明

[0013] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅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性的前提下，还可以根据这些附图获得其他的附图。

[0014] 图1为本发明实施例一提供的多媒体业务的内容保护系统的具体结构图；

[0015] 图2为本发明实施例一提供的多媒体业务的内容保护系统的密钥体系结构图；

[0016] 图3为本发明实施例一提供的多媒体业务的内容保护系统中的直播业务保护密钥的分发流程图；

[0017] 图4为本发明实施例一提供的多媒体业务的内容保护系统中的点播或下载业务保护密钥的分发流程图；

[0018] 图5为本发明实施例二提出的多媒体业务的内容保护方法的处理流程图。

具体实施方式

[0019] 为便于对本发明实施例的理解，下面将结合附图以几个具体实施例为例做进一步的解释说明，且各个实施例并不构成对本发明实施例的限定。

[0020] 实施例一

[0021] 本发明用到的符号说明如下：

[0022] ‖：链接。如C=A‖B，表示将B作为C的低段数据，将A作为C的高段数据，C的比特长度为A和B的比特长度之和。

[0023] E：对称密码算法SM1(SHANGMI1)。

[0024] PE：非对称密码算法SM2(SHANGMI2)。

[0025] EK：使用SM1算法和密钥K进行的加或解密运算。

[0026] PEK：使用SM2算法和密钥K进行的加密或解密或签名或解签名运算。

[0027] H：使用SM3(SHANGMI3)算法进行的Hash运算。

[0028] R、r：均为随机数

[0029] P：代表与CW(Control Word，控制字密钥)关联的控制参数。

[0030] 本发明可以应用于手机电视业务等多媒体业务，下面以手机电视业务为例来说明本发明实施例。

[0031] 该实施例提供的一种多媒体业务的内容保护系统的具体结构如图1所示，包括：

[0032] 服务器单元11，用于完成对手机电视等多媒体业务的节目内容的加密、密钥管理和终端用户授权管理，并实现与终端交互信息的认证；

[0033] 终端单元12，用于完成多媒体业务的节目内容、各级密钥或权限的解密，实现终端与服务器的交互认证，执行终端用户的权限对应的业务内容，从而实现对节目内容的保护和消费行为的控制。

[0034] 所述服务器单元11包括：服务器密钥管理模块111、服务器授权管理模块112和内容加扰模块113。

[0035] 所述服务器密钥管理模块111，用于实现本系统所使用密钥的产生、存储、更新、发

放等功能。包括：

[0036] 对称密钥管理：PK(Personal Key，个人密钥)或DK(Domain Key，域密钥)、SK(Service Key，业务密钥)、CEK(Content Encryption Key，内容加密密钥)、CW等密钥产生、加密存储、安全分发、安全更换等。

[0037] 非对称密钥管理：通过发卡系统实现，包括系统中服务器和终端的所有ECC公私钥对和相关参数等的产生、分发、更新或发布，以及建立和更新ECC黑表目录、终端用户信息记录审计等。

[0038] 本系统采用的主体密钥体系如图2所示，通过对直播业务四层密钥和点播或下载业务三层密钥的授权和管理控制解决应用安全问题。所述服务器密钥管理模块111还用于：

[0039] 1)对直播业务采用四层密钥体系：

[0040] 第1层：服务器单元的身份密钥SIK(Service Identity Key)和终端用户的身份密钥TIK(TerminaI Identity Key)。ECC密钥对分别为SIK_{pri}或SIK_{pub}和TIK_{pri}或TIK_{pub}，用于保护PK或DK在线分发和实现终端用户注册等应用时与机构之间的身份认证。该密钥是离线产生和写卡。

[0041] 第2层：PK或DK，分别用于实现终端用户或终端用户组的授权管理和保护SK在线分发。

[0042] 第3层：SK，用于实现分类业务、独立业务或业务组的控制授权和保护CW实时发放。

[0043] 第4层：CW，用于实现媒体内容的传输保护，随节目流信息定时在线分发。

[0044] 2)对点播或下载业务采用三层密钥体系：

[0045] 第1层：服务器单元和终端用户的身份密钥，ECC密钥对分别为SIK_{pri}或SIK_{pub}和TIK_{pri}或TIK_{pub}，该层密钥与直播的第1层ECC密钥共用，用于实现交互应用下终端用户与服务器端之间的双向身份认证和保护PK或DK在线分发。

[0046] 第2层：PK或DK，该层密钥与直播的第2层PK或DK密钥共用，用于实现终端用户或终端用户组授权管理和保护CEK在线分发。

[0047] 第3层：CEK，实现点播媒体流和下载媒体内容的加密。

[0048] 所述的服务器密钥管理模块111，还用于在系统初始化或终端安全模块初始化时，以离线方式将所述终端用户的ECC密钥对分发给终端；

[0049] 在终端用户注册时，在所述终端用户的ECC公钥加密保护下通过在线或离线的方式将所述终端用户的PK或DK分发给终端；

[0050] 在终端申请业务时，在所述终端用户的PK或DK加密保护下将所述终端用户的SK分发给所述终端；

[0051] 在系统广播加密的节目内容时，在所述终端用户的SK加密保护下将所述终端用户的CW随被加扰的节目内容一起分发给所述终端；

[0052] 在终端申请非实时业务授权时，在所述终端用户的PK或DK加密保护下将所述终端用户的CEK分发给所述终端。

[0053] 所述服务器授权管理模块112，用于实现终端用户认证和终端用户权限信息管理，根据终端用户的权限授予终端用户相应节目的许可和使用权限。包括：

[0054] 权限管理：提供直播、点播或下载业务的权限管理，包括终端用户权限信息产生和维护。

[0055] 授权消息产生:授权消息包含密钥和权限信息,它与密钥管理、内容管理以及终端用户管理关联产生授权消息。本系统有两类授权消息:RMM(权利管理消息,Right Management Message)和ECM(授权控制消息,Entitle Control Message)。

[0056] 授权消息(含密钥)加密,包括RMM加密器和ECM加密器。

[0057] 终端用户认证:如终端用户接入认证、在线注册认证、在线业务申请认证等,包含签名或验证、公钥加或解密模块。

[0058] 授权消息权利分发和交付。

[0059] 所述内容加扰模块113,分别实现对直播节目和点播或下载节目的加扰与安全控制,并按照指定格式封装码流。包括:

[0060] 实时加扰器:在密码算法和密钥CW的作用下实现对直播节目内容流的加扰。

[0061] 预加扰器:在密码算法、密钥CEK作用下实现对点播节目和下载文件内容流的预加扰,预加扰后的内容存入节目服务器。

[0062] 所述终端单元12包括:终端密钥管理121、终端授权管理模块122和内容解扰模块123。

[0063] 所述终端密钥管理模块121,用于完成终端用户的各种密钥如ECC密钥、对称密钥和相关参数的存储和管理;

[0064] 所述终端授权管理模块122,用于完成授权消息解密、权限信息维护、权限执行、身份认证和上传信息加密等处理过程。具体包括:

[0065] 授权消息解密模块1221,用于根据接收的RMM和ECM完成终端用户的各层密钥和权限信息的解密,提取出终端用户的收视条件如密钥、有效期、播放控制参数等。

[0066] 权限信息维护模块1222,用于依据接收的授权消息,保存、更新、维护终端用户的权限信息。

[0067] 权限执行模块1223,依据接收的权限信息控制密钥接收、密钥使用和控制机卡之间密钥的传递,达到控制节目解密和播放的目的。

[0068] 身份认证模块1224,实现交互数据的签名或验证运算。

[0069] 上传信息加密模块1225,完成终端向服务器提交的交互信息产生和加密等。

[0070] 所述内容解扰模块123,用于在所述密钥管理模块121的控制下,采用与服务器对应的方法完成直播、点播和下载媒体节目内容的解扰。在密码算法和密钥CW的作用下实现对直播节目内容流的解扰。在密码算法、密钥CEK作用下实现对点播节目和下载文件内容流的解扰。

[0071] 图3为上述系统中的直播业务保护密钥的分发流程图,图4为上述系统中的点播或下载业务保护密钥的分发流程图。参照图3和图4,在本发明中,密钥分发与保护的原则是,不仅要保障密钥的机密性,还要保障密钥的完整性和来源的可靠性,分发的所有密钥都必须确保只有认证合法的授权终端用户才能够获得。

[0072] 本发明中所有密钥都是采用逐层保护方式分发,即采用上层密钥加密下层密钥的分发方式,除了个人密钥(PK)和域密钥(DK)是通过ECC算法保护外,其之下的其它密钥都是由对称密码算法SM1加密保护。同时,每一个密钥都与使用条件一起捆绑后加密分发,终端用户只能够按照指定规则(用C_X表示)使用密钥。具体如下:

[0073] $RMM_{P或D}=PE_{TIKpub}(PK或DK\|C_{P或D})\|PE_{SIKpri}(H(PK或DK\|C_{P或D}))$

[0074] $RMM_S=E_{PK或DK}(SK\|C_S)\|H(SK\|C_S)$

[0075] $RMM_C=E_{PK或DK}(CEK\|C_C)\|H(CEK\|C_C)$

[0076] $ECM=E_{SK}(CW\|P)\|H(CW\|P)$

[0077] 各密钥的分发是分步完成的。其中，ECC密钥对在系统初始化或终端安全模块初始化时以离线方式完成分发；个人密钥PK或域密钥DK是终端用户注册时，在终端用户的ECC公钥加密保护下通过在线或离线的方式分发给终端用户；业务密钥SK采用PK或DK加密保护，是在终端用户申请业务时分发给终端；CW采用SK加密，在系统广播加密的节目内容时随流实时分发；CEK采用PK或DK加密保护，在终端用户申请非实时业务授权时在线分发给指定终端。

[0078] 除了传输控制字CW是随被加扰的节目内容一起分发外，其它密钥都是独立于节目内容分发。

[0079] 当系统中同时存在多个同类密钥时，密钥分发消息中要指定密钥标识符KID，并且节目内容中也要包含用于加密该内容的密钥标识符KID。

[0080] 在本发明中，终端用户持终端用户智能卡向运营商申请注册时，由于系统的初始化是安全可靠的，运营商和终端用户卡在进行注册前都已经可信地获得了对方的公钥，双方对注册过程中交互的信息均进行了签名，因此攻击者是无法通过替换或篡改这些信息的，使得双方在接收到伪造信息的情况下仍能够注册成功。一旦终端用户注册成功，就具备了分发$RMM_{P或D}$即个人密钥PK和域密钥DK的条件。

[0081] 参照图3和图4，在本发明中，服务器密钥管理模块产生个人密钥PK和域密钥DK，并将其保存在存储介质中。服务器单元计算$RMM_{P或D}=PE_{TIKpub}(PK或DK\|C_{P或D})\|PE_{SIKpri}(H(PK或DK\|C_{P或D}))$，将$RMM_{P或D}$随授权管理信息RMM经复用发送到终端。经解复用，终端密钥管理模块计算$(PK或DK\|C_{P或D})'=PE_{TIKpri}(PE_{TIKpub}(PK或DK\|C_{P或D}))$，并验证$RMM_{P或D}$的有效性(计算$PE_{SIKpub}(PE_{SIKpri}(H(PK或DK\|C_{P或D})))$，并与计算出的$H((PK或DK\|C_{P或D})')$值比较，相等则认为解密的$(PK或DK)'==PK或DK$)，终端密钥管理模块只接受合法的PK或DK和$C_{P或D}$，并将其存储于终端密钥管理模块的安全区域。

[0082] 参照图3，在本发明中，服务器密钥管理模块产生业务密钥SK，并将其保存在存储介质中。服务器单元计算$RMM_S=E_{PK或DK}(SK\|C_S)\|H(SK\|C_S)$，将$RMM_S$随授权管理信息经复用发送到终端。经解复用，终端密钥管理模块计算$(SK\|C_S)'=E_{PK或DK}(E_{PK或DK}(SK\|C_S))$，并验证$SK\|C_S$的完整性(计算$h((SK\|C_S)')$，并与接收的$h(SK\|C_S)$值比较，相等则认为解密的SK'==SK)，终端密钥管理只接受合法的SK和C_S，并将其存储于终端密钥管理模块的安全区域。

[0083] 参照图3，在本发明中，服务器密钥管理模块产生控制字CW并计算$ECM=E_{SK}(CW\|P)\|H(CW\|P)$，将ECM随加扰的节目内容一起发送到终端。终端密钥管理模块计算$(CW\|P)'=E_{SK}(E_{SK}(CW\|P))$，并验证CW‖P的完整性(计算$h((CW\|P)')$，并与接收的$h(CW\|P)$值比较，相等则认为解密的CW'==CW)，终端密钥管理模块只接受合法的控制字CW，并将CW和P输出到解扰模块用于内容解扰。

[0084] 参照图4，在本发明中，服务器密钥管理模块产生内容加密密钥CEK并计算$RMM_C=E_{PK或DK}(CEK\|C_C)\|H(CEK\|C_C)$，将$RMM_C$随授权管理信息一起发送到终端。经解复用，终端密钥管理模块计算$(CEK\|C_C)'=EP_{K或DK}(E_{PK或DK}(CEK\|C_C))$，并验证CW‖P的完整性(计算$h(CEK\|C_C)')$，并与接收的$h(CW\|P)$值比较，相等则认为解密的CEK'==CEK)，终端密钥管理模块只接受合法

的内容加密密钥CEK，并将CEK和C_C输出到解扰模块用于内容解扰。

[0085] 参照图3和图4，在本发明中，服务器加扰操作是用对称密码算法和控制字CW或内容加密密钥CEK对视音频流进行加扰，形成加扰后的视音频流；终端解扰操作是用对称密码算法和解密出的控制字CW或内容加密密钥CEK对加扰后的视音频流进行解扰，形成可以观看的明文视音频流。攻击者只有在获得控制字CW或内容加密密钥CEK的前提下，才能利用对称密码算法对加扰后的音视频流进行解扰。

[0086] 在本发明中，采用的对称加密算法、非对称加密算法和杂凑密码算法均为国产算法，其安全性通过了国家主管部门组织的安全性检测，是安全可靠的。

[0087] 在本发明中，在分发PK或DK时，服务器计算PK或DK的消息验证码H(PK或DK)并利用服务器私钥SIK_{pri}进行签名，因此经终端用户智能卡验证过签名和H(PK或DK)有效的PK或DK密文均是可信的，解密出的PK或DK是可信的。

[0088] 在本发明中，在分发SK时，服务器计算SK的消息验证码H(SK)，由于PK或DK和SK是保密的，且PK或DK是可信的，攻击者无法冒充服务器单元计算出H(SK)，因此经终端用户卡验证H(SK)有效的SK密文均是可信的，解密出的SK是可信的。

[0089] 在本发明中，在分发CW时，服务器计算CW的消息验证码H(CW)，由于PK或DK、SK和CW是保密的，且SK是可信的，攻击者无法冒充服务器单元计算出H(CW)，因此经终端用户卡验证H(CW)有效的CW密文均是可信的，解密出的CW是可信的。

[0090] 在本发明中，在分发CEK时，服务器计算CEK的消息验证码H(CEK)，由于PK或DK和CEK是保密的，且PK或DK是可信的，攻击者无法冒充服务器单元计算出H(CEK)，因此经终端用户卡验证H(CEK)有效的CEK密文均是可信的，解密出的CEK是可信的。

[0091] 实施例二

[0092] 本发明提出的多媒体业务的内容保护方法的处理流程如图5所述，包括以下步骤：

[0093] 步骤51、系统初始化和终端用户注册的密码流程和协议。

[0094] I)系统初始化

[0095] 确定系统使用的密码算法：E、PE和H。

[0096] 服务器单元产生ECC密钥对，确定自身的标志SID(服务端标识符，Service Identifier)和椭圆曲线参数及其基点P，并产生服务器单元基于ECC的密钥对(SIK_{pub}，SIK_{pri})。

[0097] TSM(终端安全模块，如智能卡，Terminal Safety Module)初始化

[0098] 为每个TSM产生和分配唯一的TID(终端标识符，Terminal Identifier)；

[0099] 向TSM中写入SID、TID和SIK_{pub}；

[0100] 终端用户基于ECC的密钥对为(TIK_{pub}，TIK_{pri})，并将TIK_{pub}记入系统数据库；

[0101] 运营商向终端用户分发TSM，TSM中包含SM2、SM1、SM3等算法，以及TIK_{pri}、TIK_{pub}、SIK_{pub}、SID和TID。

[0102] 移动终端初始化

[0103] 服务器为终端用户的手机等移动终端加载机卡通信和媒体加解扰用的分组密码算法SM1；

[0104] 服务器单元随机产生TSK(终端安全密钥，Terminal Safety Key)，并写入到移动终端的解扰模块中。

[0105] Ⅱ)终端用户注册

[0106] 终端用户注册的密码流程和协议如下：

[0107] 终端用户持TSM和移动终端向运营商离线或在线申请注册，并说明是个人注册或分组注册。

[0108] 服务器单元为TSM产生TM(终端用户管理信息，Terminal Management)和随机数r，用SIK_{pri}对TM签名，并将TM及其签名写入TSM。即：

[0109] $TM\|r\|PE_{SIKpri}(TM\|r)$

[0110] TSM以SIK_{pub}验证运营商对TM签名的有效性，如签名无效则注册以失败结束，如签名有效则TSM向服务器单元返回TID‖TM以及用TIK_{pri}对TID‖TM的签名，即：

[0111] $TID\|TM\|r\|PE_{TIKpri}(TID\|TM\|r)$

[0112] 服务器单元根据TID从数据库中提取TIK_{pub}验证TSM对TID‖TM签名的有效性，如签名无效则注册以失败结束，如签名有效则将TID‖TM及TSM对TID‖TM的签名记录入数据库。

[0113] 服务器单元向TSM和终端分发TLK(机卡通信连接密钥，Terminal Link Key)。即

[0114] $PE_{TIKpub}(TLK\|r)\|PE_{SIKpri}(PE_{TIKpub}(TLK\|r))$

[0115] 和

[0116] $E_{TSK}(TLK\|r)\|H(TLK\|r)$

[0117] 步骤52、分发$RMM_{P或D}$密码流程和协议。

[0118] 终端用户PK或DK授权消息是在$RMM_{P或D}$里分发，具体密码流程和协议如下：

[0119] 运营商针对指定终端用户或终端用户组产生与PK或DK关联的权限信息$C_{P或D}$，该$C_{P或D}$包括PK或DK密钥有效期、服务器可提供的业务类型、密钥使用规则等。

[0120] 产生$RMM_{P或D}$(权利管理消息，Right Management Message)

[0121] $RMM_{P或D}=PE_{TIKpub}(PK或DK\|C_{P或D})\|PE_{SIKpri}(H(PK或DK\|C_{P或D}))$

[0122] 当$PK或DK\|C_{P或D}$数据大于256bit时，可以使用数字信封产生$RMM_{P或D}$：

[0123] $RMM_{P或D}=EK(PK或DK\|C_{P或D})\|PETIK_{pub}(K)\|PESIK_{pri}(H(K\|C_{P或D}))$

[0124] 将$RMM_{P或D}$发送到终端用户的移动终端。

[0125] 移动终端接收$RMM_{P或D}$、解密PK或DK。终端接收到$RMM_{P或D}$后，使用私钥TIK_{pri}解密$RMM_{P或D}$，得到PK或DK和$C_{P或D}$明文，并利用ECC签名验证模块和服务器单元的公钥SIK_{pub}验证$RMM_{P或D}$的有效性，若有效则保留PK或DK和$C_{P或D}$，无效则放弃解密数据。

[0126] 步骤53、分发RMM_S(权利管理消息，Right Management Message)和ECM的密码流程和协议。

[0127] 当终端用户申请了直播流媒体授权后，授权消息分发的密码流程和协议如下：

[0128] I)发布和接收直播节目的业务密钥SK

[0129] 服务器利用SK产生模块随机产生SK，并产生权限信息C_S，该CS包括直播节目的权限信息，如节目有效期、播放条件、使用规则等。

[0130] 服务器单元用PK(或DK)对SK和C_S进行加密，得到SK的权利消息RMM_S：

[0131] $RMM_S=E_{PK或DK}(SK\|C_S)\|H(SK\|C_S)$

[0132] 将RMM_S以指定的授权方式发送到指定的移动终端。

[0133] 移动终端用PK或DK解密RMM_S得到$SK\|C_S$，计算$H(SK\|C_S)$，并与接收的$H(SK\|C_S)$值比较，相等则接受SK，否则拒绝接受SK。

[0134] 若一个终端用户申请了N种业务并拥有该N项业务的收视权利时，可以：

[0135] $RMM_S=E_{PK或DK}(SK_0||SK_1||\cdots SK_{N-1}||C_S)||H(SK_0||SK_1||\cdots SK_{N-1}||C_S)$

[0136] II)发布和接收收直播节目的ECM

[0137] 服务器利用CW产生模块随机产生CW，并产生使用该CW的控制参数P。

[0138] 用SK对CW进行加密并计算HASH，获得ECM：

[0139] $ECM=E_{SK}(CW||P)||H(CW||P)$

[0140] 将ECM随节目流发送到移动终端。

[0141] 移动终端用终端用户的SK解密出CW，计算H(CW||P)并与ECM中的HASH值比较，相等则接受CW，否则拒绝接受CW。

[0142] 在播出节目内容时，终端遵从P和C_S，在权限管理模块控制下，用CW和SM1对广播节目密文流解密。

[0143] 步骤54、终端用户申请点播或下载业务授权RMMc的密码流程和协议。

[0144] 终端用户申请点播业务和下载业务授权时的密码流程和协议如下：

[0145] I)终端用户的移动终端通过交互信道发送REQ_T(交互业务授权请求，Request)

[0146] $REQ_T=E_{PK或DK}(TID||CID||W||r)||PE_{TIKpri}(H(TID||CID||W||r))$

[0147] CID：节目标识信息，如频道、节目名称、节目ID或KID等

[0148] W：申请业务的消费需求等相关信息。

[0149] 服务器接收REQ_T和验证签名

[0150] 服务器接收REQ_T，先用该终端用户的PK或DK解密，再用终端用户的身份密钥公钥TIK_{pub}验证签名的有效性，即计算$PE_{TIKpub}(H(TID||CID||W||r))$。如签名无效则拒绝授权并反馈认证失败信息；如签名有效，再通过授权系统检查终端用户的权限，若符合授权要求则继续，否则反馈授权失败信息。

[0151] Ⅱ)服务器发送点播或下载RES_S(文件授权消息，Response)

[0152] $RES_S=RMM_c=E_{PK或DK}(CEK||CC||r)||H(CEK||CC||r)$

[0153] CC：授予的申请节目权限信息，如有效期，播放条件、使用规则等。其中使用规则规定了终端用户的播放条件。

[0154] Ⅲ)移动终端通过广播或交互信道接收点播或下载文件

[0155] 移动终端用终端用户的PK或DK解密出CEK||CC||r，计算H，并与RES_S中的H值比较，比较r值，都相等则接受CEK，否则拒绝接受CEK。然后，终端按照权限信息CC，用CEK对点播或下载文件进行解密。

[0156] 若一个终端用户申请了N种交互业务并拥有该N项业务的收视权利时，可以一次性分发多个节目的CEK，则上述CEK可以替换为：

[0157] $CEK=CEK_1||CEK_2\cdots||CEK_N$

[0158] 若同一个节目有N个终端用户申请，则需要将同一个CEK分发给若干个终端用户(假定该N个终端用户的收视权限是一样的。)：

[0159] $RMM_c=E_{PK1}(CEK||CC||r)||E_{PK2}(CEK||CC||r)||$

[0160] $\cdots E_{PKN}(CEK||CC||r))||H(CEK||CC||r)$

[0161] 步骤55、终端用户发起授权请求的密码流程和协议。

[0162] 另一种情况是终端用户在密钥广播时未能正确接收，但终端用户却可以向系统主

动指定申请PK、DK或SK，它们在KID和CID中指定。

[0163] I)终端用户的移动终端发送密钥申请

[0164] 终端用户的移动终端通过反向信道向服务器单元的授权管理系统发送密钥和权利请求：

[0165] REQT=PESIKpub(TID‖CID‖W‖r)‖PETIKpri(H(TID‖CID‖W‖r))

[0166] 或

[0167] REQT=EK(TID‖CID‖W‖r)‖PESIKpub(K)

[0168] ‖PETIKpri(H(TID‖CID‖W‖r))

[0169] 其中K和r均为随机数。

[0170] Ⅱ)服务器对终端用户进行签名验证和权限检查。

[0171] Ⅲ)为符合权限的终端用户分发权利

[0172] 依据CID识别终端用户申请，做如下分发：

[0173] PK或DK分发：

[0174] RESS=RMMP或D=PETIKpub(PK或DK‖CP或G‖r)‖PESIKpri(H(PK或DK‖CP或D‖r))

[0175] 或

[0176] RESS=RMMP或D=EKPK或DK‖CP或D‖r)‖PETIKpub1(K)‖PESIKpri(H(K‖CP或G‖r))

[0177] SK分发协议：

[0178] RESS=EPK或DK(SK‖CS‖r)‖H(SK‖CS‖r)

[0179] 系统正确识别终端用户后，向终端用户分发所申请的密钥。

[0180] 步骤56、服务器发起权利分发的密码流程和协议。

[0181] 在直播方式下，终端用户在系统广播密钥时未能够正确接受(如终端用户未开机)，或点播方式下的未正确接收，服务器可以通过点对点方式主动分发指定终端用户的PK、DK、SK或CEK密钥，它们由KID指定。协议如下：

[0182] Ⅰ)服务器单元向终端用户的移动终端发送权利分发提示命令COMS授权管理系统向指定终端用户发送PK或DK分发命令：

[0183] COMS=PETIKpub(SID‖r‖KIDPK或DK)‖PESIKpri(H(SID‖r‖KIDPK或DK))

[0184] 授权管理系统向指定终端用户发送SK或CEK分发命令：

[0185] COMS=EPK或DK(SID‖r‖KIDSK或CEK)‖PESIKpri(H(SID‖r‖KIDSK或CEK))KIDPK或DK:PK或DK的密钥标识。

[0186] KIDSK或CEK:SK或CEK的密钥标识。

[0187] II)终端用户端对系统身份进行认并和发送响应REST

[0188] 终端用户的移动终端接收COMS。解密并验证系统的身份。如签名有效或无效则接受或放弃，反馈认证成功或失败信息。

[0189] PK或DK分发命令确认：

[0190] REST=PESIKpub(TID‖r‖F)‖PETIKpri(H(TID‖r‖F))

[0191] SK或CEK分发命令确认：

[0192] REST=EPK或DK(TID‖r‖F)‖PETIKpri(H(TID‖r‖F))

[0193] F:认证成功或失败等标志。

[0194] r:已接收系统发来的随机数。

[0195] Ⅲ)服务器向终端用户的移动终端分发权利

[0196] 服务器向终端用户的移动终端分发权利的密码协议与前述“权利分发”部分基本相同,即:

[0197] RMMP或D=PETIKpub(PK或DK||CP或G||r)||PESIKpri(H(PK或DK||CP或D||r))

[0198] 或

[0199] RMMP或D=EK(PK或DK||CP或G||r)||PETIKpub(K)||PESIKpri(H(K||CP或D||r))

[0200] RMMS=EPK或DK(SK||CS||r)||H(SK||CS||r)

[0201] RMMc=EPK或DK(CEK||CC||r)||H(CEK||CC||r)

[0202] 综上所述,本发明实施例通过对直播业务采用四层密钥体系,对点播或下载业务采用三层密钥体系,并且由于所有密码算法本身都是安全的,密码使用流程中密钥信息和密文信息都是安全的,所有需要用密码保护的信息均被有效保护。在整个手机电视等多媒体业务流程(从系统初始化到加扰节目的传输和收看)中,攻击者既无法获取秘密信息以窃看节目,也无法用伪造的密钥相关信息或节目信息欺骗终端用户智能卡,从而有效地保证了手机电视等多媒体业务的节目内容的安全,维护媒体内容或电视节目制作者、提供商、运营商、服务商及其合法终端用户的利益,提高媒体内容制作者的积极性,制作出质量更高、更丰富的节目,保证手机电视等多媒体业务的持续、健康发展。

[0203] 在本发明实施例中,系统采用的密钥CW、SK、PK或DK可以按照需要按照一定的周期和策略进行更新,以提高系统的安全性。终端用户的TIK更新间隔时间约为2年。终端用户个人密钥PK或域密钥DK随终端用户或域终端用户收视权限的存在而有效,在权利连续期内其更新间隔时间为1-2年。直播节目业务密钥SK的更新可以是一天或一个月,由运营商决定SK的有效期。控制字CW的更新间隔时间间隔由服务器单元自定,一般可为30-90秒。而CEK同权利要求的文件有效期一致,一般不需要更新,随被加密文件的有效期存在而存在。

[0204] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random Access Memory,RAM)等。

[0205] 以上所述,仅为本发明较佳的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到的变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应该以权利要求的保护范围为准。

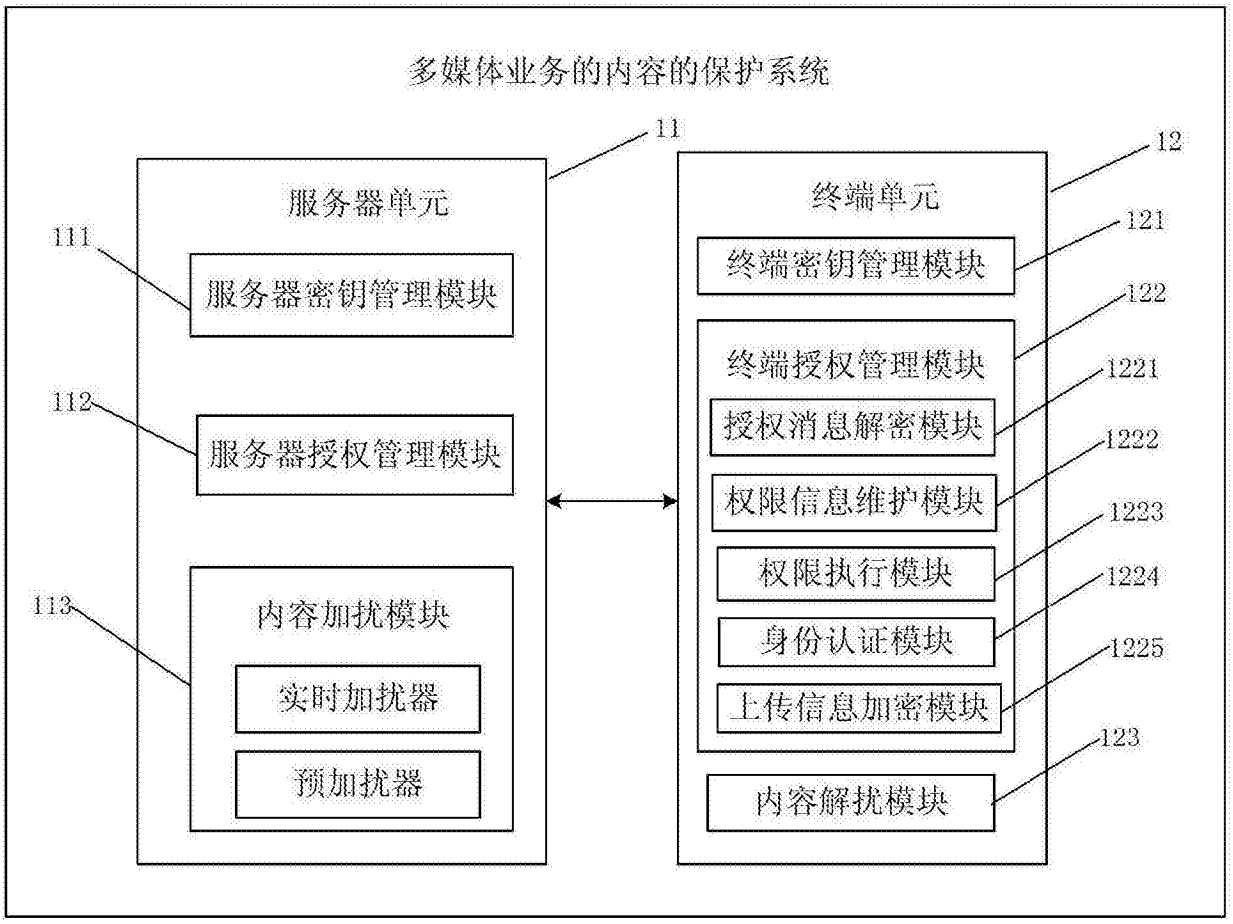

多媒体业务的内容的保护系统
11
服务器单元
111
服务器密钥管理模块
112
服务器授权管理模块
113
内容加扰模块
实时加扰器
预加扰器
12
终端单元
121
终端密钥管理模块
122
终端授权管理模块
1221
授权消息解密模块
1222
权限信息维护模块
1223
权限执行模块
1224
身份认证模块
1225
上传信息加密模块
123
内容解扰模块

图1

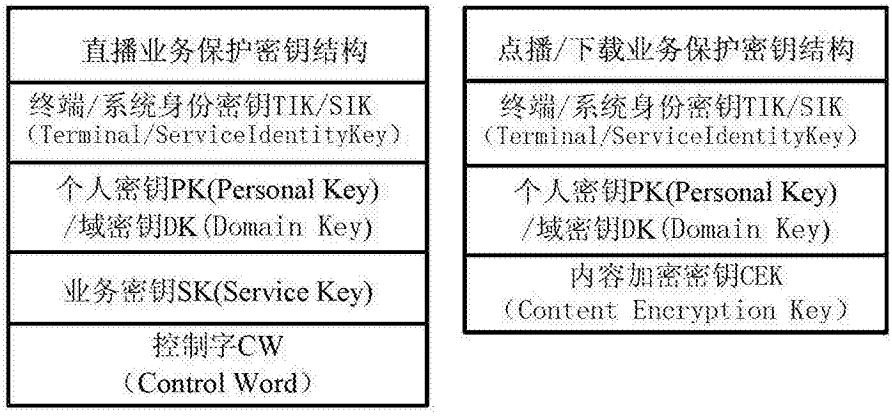

直播业务保护密钥结构
终端/系统身份密钥TIK/SIK
(Terminal/ServiceIdentityKey)
个人密钥PK(Personal Key)
/域密钥DK(Domain Key)
业务密钥SK(Service Key)
控制字CW
(Control Word)
点播/下载业务保护密钥结构
终端/系统身份密钥TIK/SIK
(Terminal/ServiceIdentityKey)
个人密钥PK(Personal Key)
/域密钥DK(Domain Key)
内容加密密钥CEK
(Content Encryption Key)

图2

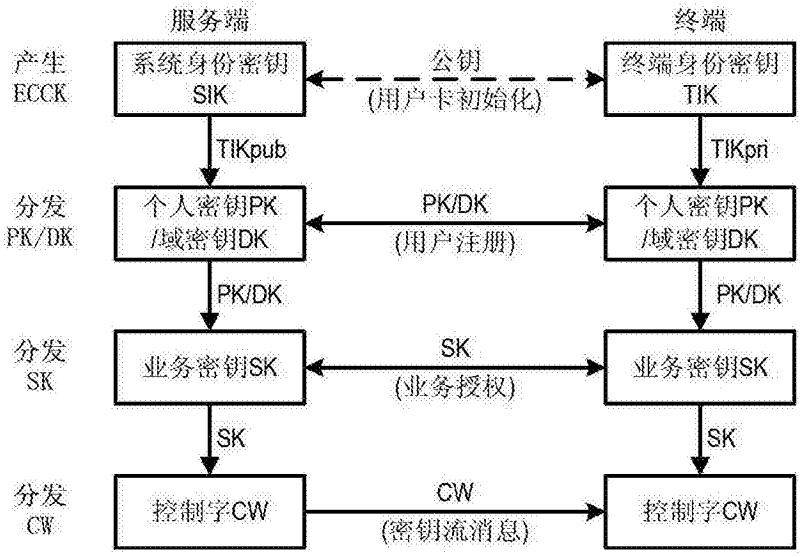

服务端
终端
产生
ECCK
系统身份密钥
SIK
公钥
(用户卡初始化)
终端身份密钥
TIK
TIKpub
TIKpri
分发
PK/DK
个人密钥PK
/域密钥DK
PK/DK
(用户注册)
个人密钥PK
/域密钥DK
PK/DK
PK/DK
分发
SK
业务密钥SK
SK
(业务授权)
业务密钥SK
SK
SK
分发
CW
控制字CW
CW
(密钥流消息)
控制字CW

图3

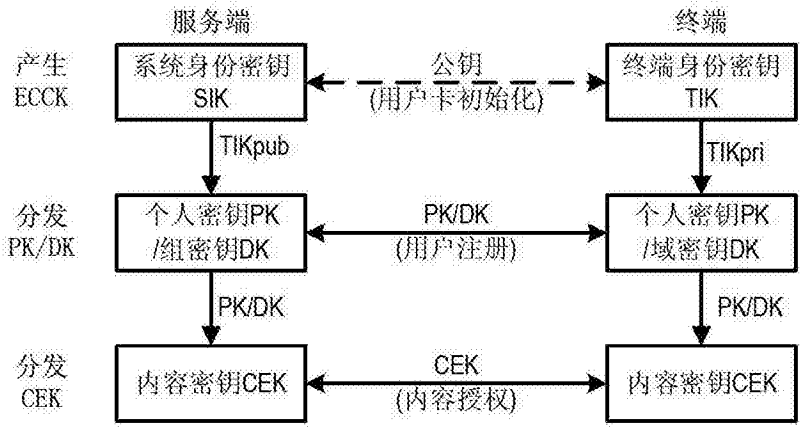

服务端
终端
产生
ECCK
系统身份密钥
SIK
公钥
(用户卡初始化)
终端身份密钥
TIK
TIKpub
TIKpri
分发
PK/DK
个人密钥PK
/组密钥DK
PK/DK
(用户注册)
个人密钥PK
/域密钥DK
PK/DK
PK/DK
分发
CEK
内容密钥CEK
CEK
(内容授权)
内容密钥CEK

图4

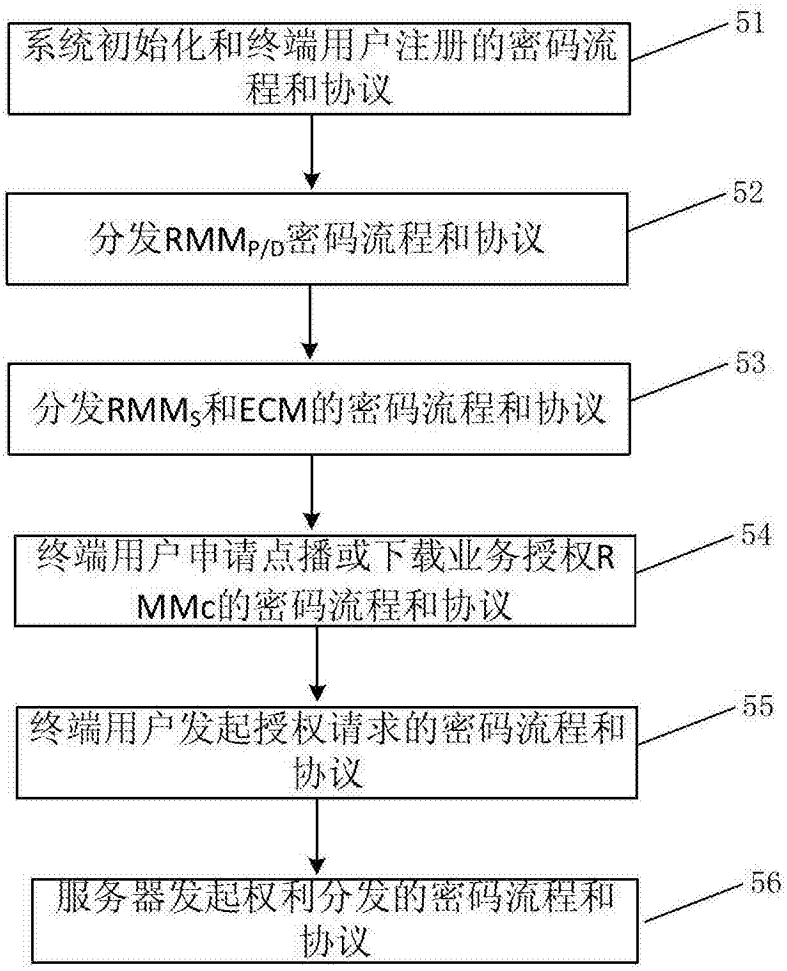

系统初始化和终端用户注册的密码流程和协议
51
分发RMM$_{P/D}$密码流程和协议
52
分发RMM$_S$和ECM的密码流程和协议
53
终端用户申请点播或下载业务授权RMMc的密码流程和协议
54
终端用户发起授权请求的密码流程和协议
55
服务器发起权利分发的密码流程和协议
56

图5