(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102111681 A
(43)申请公布日 2011.06.29

(21)申请号 200910243800.5

(22)申请日 2009.12.24

(71)申请人 航天信息股份有限公司
地址 100097 北京市海淀区杏石口路甲 18 号

(72)发明人 郭宝安 张飚 于志强 唐凌 叶松 丁瑶 王杰斌 吴渊 鲁昱

(74)专利代理机构 北京科龙寰宇知识产权代理有限责任公司 11139
代理人 孙皓晨 朱世定

(51)Int.Cl.
H04N 21/6334(2011.01)
H04L 9/08(2006.01)

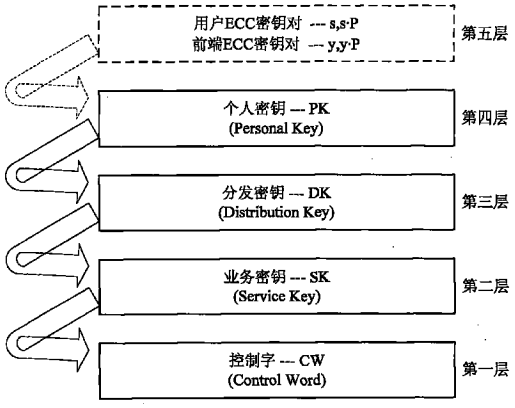
权利要求书 2 页 说明书 6 页 附图 2 页

(54)发明名称

一种用于数字电视广播条件接收系统的密钥体系

(57)摘要

本发明提供一种用于数字电视广播条件接收系统的密钥体系，其包括五层密钥，所述的五层密钥为四层对称密钥及一层非对称密钥，所述的四层对称密钥包括控制字 CW、业务密钥 SK、分发密钥 DK 及个人密钥 PK，所述的一层非对称密钥为 ECC 密钥对。本发明中的密码算法全部采用国家密码管理局指定的密码算法，符合国家商用密码管理政策的要求。密码算法的强度高，能有效抵御基于数字电视广播网络的暴力攻击。



CN 102111681 A

1. 一种用于数字电视广播条件接收系统的密钥体系，其特征在于，其包括五层密钥，所述的五层密钥为四层对称密钥及一层非对称密钥，所述的四层对称密钥包括控制字 CW、业务密钥 SK、分发密钥 DK 及个人密钥 PK，所述的一层非对称密钥为 ECC 密钥对。

2. 根据权利要求 1 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的控制字 CW 为最底层密钥，用于加扰节目内容。

3. 根据权利要求 1 或 2 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的控制字 CW 采用国密 SM5 序列对称加密算法，密钥长度采用 128Bit。

4. 根据权利要求 3 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述控制字 CW 采用快变策略，按不到 2 秒的周期更新，并随授权控制信息 ECM 发送到用户终端。

5. 根据权利要求 1 或 2 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的业务密钥 SK 为第二层密钥，用于加密保护所述控制字 CW，还用于控制业务使用权限。

6. 根据权利要求 5 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的业务密钥 SK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit，所述的业务密钥 SK 随授权管理信息 EMM 发送到用户终端。

7. 根据权利要求 5 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的业务密钥 SK 用于针对一个节目或针对一组具有共同授权信息的多个节目。

8. 根据权利要求 7 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，当针对多个节目时，不同的节目或节目组有着不同的业务密钥，所述的业务密钥 SK 的有效期与节目播放的时间一致，相关节目的业务密钥 SK 只有在节目播放周期内才起作用，节目播放结束后自动失效。

9. 根据权利要求 1 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的分发密钥 DK 为第三层密钥，用于加密保护业务密钥 SK。

10. 根据权利要求 9 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的分发密钥 DK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit，所述的分发密钥 DK 随授权管理信息 EMM 发送到用户终端，并可以在不同的运营商之间进行漫游。

11. 根据权利要求 1 或 9 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的分发密钥 DK 与用户申请的业务使用周期密切相关，用来控制用户的节目收视权限，即实现授权控制。

12. 根据权利要求 1 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的个人密钥 PK 为第四层密钥，用于加密保护所述分发密钥 DK 的分发。

13. 根据权利要求 1 或 12 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述的个人密钥 PK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit，所述的个人密钥 PK 的更新间隔时间要求为 1 至 2 年，或与所述分发密钥 DK 同时更换。

14. 根据权利要求 1 所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，当前端需要发送个人密钥 PK 时，前端个人密钥 PK 发生器运行密钥协商发送方算法产

生个人密钥PK、个人密钥PK的动态参数R1和验证参数S1，后两个参数随授权管理信息EMM发送到用户终端。

15. 根据权利要求1所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，所述ECC密钥对为第五层密钥，用于参与用户基于ECC的个人密钥PK的协商，必要时可用于在用户注册期间实现终端同前端系统之间的相互认证，并可在今后条件接收系统扩展到双向系统时用于双向身份认证。

16. 根据权利要求1或15所述的一种用于数字电视广播条件接收系统的密钥体系，其特征在于，用户的ECC公私钥对在终端解密模块初始化时写入，采用国密SM2-2密钥协商算法。

一种用于数字电视广播条件接收系统的密钥体系

技术领域

[0001] 本发明涉及一种密钥体系，特别涉及一种用于数字电视广播条件接收系统的密钥体系。

背景技术

[0002] 近年来，数字电视成为全球高新技术产业竞争的一个重点。随着数字电视技术的成熟，许多运营商开始考虑或者着手建设数字化的广播电视网络。数字网络提供了丰富的增值服务机会，为传统广电行业带来新的发展机会。而数字电视发展的出路是以多元化的收费方式来促进电视的发展，这其中条件接收 (CA，conditional access) 系统在数字电视的应用平台中扮演了很重要的角色。

[0003] 数字电视广播条件接收系统的主要工作原理是：在数字电视前端系统对音视频信息和广播数据进行加密传输，同时对用户终端的解密密钥和解密过程进行控制，从而确保只有付费用户才能收看所选节目。

[0004] 密钥是数字电视条件接收系统安全的关键因素，其有效性和安全性直接决定了整个条件接收系统的安全性。传统的条件接收系统采用三密钥体系：最底层为用于加扰节目内容的控制字 CW(Control Word)；中间层为业务密钥 SK(Service Key)，用于对控制字 CW 进行加密形成授权控制信息 ECM(EntitlementControl Message)；最上层为个人分配密钥 PDK(Personal Distributed Key)，用于加密 SK 形成授权管理信息 EMM(Entitlement Management Message)。授权管理信息 EMM、授权控制信息 ECM 和节目内容密文数据经过复用形成传输流 TS，它通过单向广播的方式传送给用户终端，用户终端按照相反的顺序进行解密，最终取出控制字 CW 完成对节目内容的解扰。

[0005] 近年来，计算机技术与数字技术的迅猛发展，为数字电视产业的发展带来机遇的同时，数字电视系统的安全性和业务的多样性也向条件接收系统提出了更高的要求，传统的基于三层密钥体系的条件接收系统逐渐变得不能适应数字电视产业的发展。

[0006] 因此，如何将上述问题加以解决，即为本领域技术人员所欲研究的方向所在。

发明内容

[0007] 本发明的主要目的是提供一种用于数字电视广播条件接收系统的密钥体系，以解决现有技术中所存在的问题，适应数字电视产业的发展。

[0008] 为了达到上述目的，本发明提供一种用于数字电视广播条件接收系统的密钥体系，其包括五层密钥，所述的五层密钥为四层对称密钥及一层非对称密钥，所述的四层对称密钥包括控制字 CW、业务密钥 SK、分发密钥 DK 及个人密钥 PK，所述的一层非对称密钥为 ECC 密钥对。

[0009] 较佳的实施方式中，所述的控制字 CW 为最底层密钥，用于加扰节目内容。

[0010] 较佳的实施方式中，所述的控制字 CW 采用国密 SM5 序列对称加密算法，密钥长度采用 128Bit。

[0011] 较佳的实施方式中，所述控制字 CW 采用快变策略，按不到 2 秒的周期更新，并随授权控制信息 ECM 发送到用户终端。

[0012] 较佳的实施方式中，所述的业务密钥 SK 为第二层密钥，用于加密保护所述控制字 CW，还用于控制业务使用权限。

[0013] 较佳的实施方式中，所述的业务密钥 SK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit，所述的业务密钥 SK 随授权管理信息 EMM 发送到用户终端。

[0014] 较佳的实施方式中，所述的业务密钥 SK 用于针对一个节目或针对一组具有共同授权信息的多个节目。

[0015] 较佳的实施方式中，当针对多个节目时，不同的节目或节目组有着不同的业务密钥，所述的业务密钥 SK 的有效期与节目播放的时间一致，相关节目的业务密钥 SK 只有在节目播放周期内才起作用，节目播放结束后自动失效。

[0016] 较佳的实施方式中，所述的分发密钥 DK 为第三层密钥，用于加密保护业务密钥 SK。

[0017] 较佳的实施方式中，所述的分发密钥 DK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit，所述的分发密钥 DK 随授权管理信息 EMM 发送到用户终端，并可以在不同的运营商之间进行漫游。

[0018] 较佳的实施方式中，所述的分发密钥 DK 与用户申请的业务使用周期密切相关，用来控制用户的节目收视权限，即实现授权控制。

[0019] 较佳的实施方式中，所述的个人密钥 PK 为第四层密钥，用于加密保护所述分发密钥 DK 的分发。

[0020] 较佳的实施方式中，所述的个人密钥 PK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit，所述的个人密钥 PK 的更新间隔时间要求为 1 至 2 年，或与所述分发密钥 DK 同时更换。

[0021] 较佳的实施方式中，当前端需要发送个人密钥 PK 时，前端个人密钥 PK 发生器运行密钥协商发送方算法产生个人密钥 PK、个人密钥 PK 的动态参数 R1 和验证参数 S1，后两个参数随授权管理信息 EMM 发送到用户终端。

[0022] 较佳的实施方式中，所述 ECC 密钥对为第五层密钥，用于参与用户基于 ECC 的个人密钥 PK 的协商，必要时可用于在用户注册期间实现终端同前端系统之间的相互认证，并可在今后条件接收系统扩展到双向系统时用于双向身份认证。

[0023] 较佳的实施方式中，用户的 ECC 公私钥对在终端解密模块初始化时写入，采用国密 SM2-2 密钥协商算法。

[0024] 与现有技术相比，本发明的有益效果在于：

[0025] 本发明中，密码算法全部采用国家密码管理局指定的密码算法，符合国家商用密码管理政策的要求。密码算法的强度高，能有效抵御基于数字电视广播网络的暴力攻击。

[0026] 本发明提出的密钥体系中的四层对称密钥，控制字 CW 与加扰数据相关联，业务密钥 SK 与受保护的节目（业务）相关联，分发密钥 DK 与用户对节目（业务）的使用权限相关联，个人密钥 PK 与用户相关联，这四层密钥通过高层密钥对低层密钥（节目数据）加密的层层保护机制，保护节目数据和密钥的安全性，实现有条件接收；一层非对称密钥，用于基

于 ECC 的 PK 协商，提高了 PK 使用的安全性。这样的层次划分，不仅增加了系统的安全性，还为运营商开展多样性业务和进行系统的双向改造提供了技术支撑。

附图说明

[0027] 图 1 为本发明密钥体系结构框图；

[0028] 图 2 为本发明条件接收系统的示意框图。

具体实施方式

[0029] 以下结合附图，对本发明上述的和另外的技术特征和优点作更详细的说明。

[0030] 如图 1 所示，为本发明密钥体系结构框图，本发明提供一种用于数字电视广播条件接收系统的密钥体系，其包括五层密钥，所述的五层密钥为四层对称密钥及一层非对称密钥，所述的四层对称密钥包括控制字 CW(Control Word)、业务密钥 SK(Service Key)、分发密钥 DK(Distribution Key) 及个人密钥 PK(Personal Key)，所述的一层非对称密钥为 ECC 密钥对。

[0031] 其中，控制字 CW 用来加扰节目内容，业务密钥 SK 用来加密保护所述的控制字 CW，所述的分发密钥 DK 用来加密保护所述的业务密钥 SK，所述的个人密钥 PK 用来加密保护所述的分发密钥 DK，所述的 ECC 密钥对用于所述个人密钥 PK 的密钥协商。

[0032] 由图 1 可以得知，所述的控制字 CW 为最底层密钥，即第一层密钥，用于加扰节目内容。所述的控制字 CW 采用国密 SM5 序列对称加密算法，密钥长度采用 128Bit，控制字 CW 采用快变策略，按不到 2 秒的周期更新，并随授权控制信息 ECM(Entitlement Control Message) 发送到用户终端。

[0033] 所述的业务密钥 SK 为第二层密钥，用于加密保护所述控制字 CW，还用于控制业务使用权限。业务密钥 SK 可以针对一个节目，也可以针对一组具有共同授权信息的多个节目，不同的节目或节目组有着不同的业务密钥，业务密钥 SK 的有效期与节目播放的时间一致，相关节目的业务密钥 SK 只有在节目播放周期内才起作用，节目播放结束后自动失效。业务密钥 SK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit。业务密钥 SK 随授权管理信息 EMM 发送到用户终端。

[0034] 所述分发密钥 DK 为第三层密钥，用于加密保护所述业务密钥 SK。所述的分发密钥 DK 与用户申请的业务使用周期密切相关，用来控制用户的节目收视权限，即实现授权控制。分发密钥 DK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit。分发密钥 DK 随授权管理信息 EMM 发送到用户终端，并可以在不同的运营商之间进行漫游。

[0035] 所述个人密钥 PK 为第四层密钥，用于加密保护分发密钥 DK 的分发。个人密钥 PK 的更新间隔时间要求为 1 至 2 年，或与分发密钥 DK 同时更换。个人密钥 PK 采用国密 SM1 分组对称加密算法，分组长度为 128Bit，密钥长度为 128Bit。前端需要发送个人密钥 PK 时，前端个人密钥 PK 发生器运行密钥协商发送方算法产生个人密钥 PK、个人密钥 PK 的动态参数 R1 和验证参数 S1，后两个参数随 EMM 发送到用户终端。

[0036] 所述 ECC 密钥对为第五层密钥，用于参与用户基于 ECC 的个人密钥 (PK) 协商，必要时可用于在用户注册期间实现终端同前端系统之间的相互认证，并可在今后条件接收系统扩展到双向系统时用于双向身份认证。用户的 ECC 公私钥对在终端解密模块初始化时写

入，采用国密 SM2-2 密钥协商算法。

[0037] 本发明在具体实施的时候，对于对称密钥，要求完全以硬件形式实现 SM5 和 SM1 的完整算法，在保障满足应用性能的同时，可以抵抗目前已知的针对对称密码硬件实现的所有攻击。SM5 的实现要考虑与加解扰模块的接口，保障 SM5 模块调用的方便性和安全性。考虑到技术发展和各种系统的性能要求，要求 SM5 实现的速度要达到 100-200Mbps。SM1 可以用硬件形式完全实现 ECB(ElectronicCodebook Mode)、CBC(Cipher Block Chaining Mode) 和 CTR(Counter Mode) 三种模式，也可以只用硬件形式实现 ECB 模式，但必须考虑对 CBC 和 CTR 模式的支持。SM1 实现要考虑与其他模块的接口，保障 SM1 模块调用的方便性和安全性。要求 SM1 在前端实现的加密速率≥ 200Mbps，在终端实现的解密速率≥ 30Kbps。

[0038] 对于非对称密钥，考虑到其算法实现的复杂性和实现环境的资源约束，可以用硬件形式完全实现 SM2-2，但也可以只用硬件形式实现 SM2-2 所基于的基础运算（如：大整数运算、点加、点倍和点乘），SM2-2 协议部分用软件实现。要求 SM2-2 在前端实现的 PK 生成速率≥ 1000 次 / 秒；在终端实现的 PK 生成速率≥ 8 次 / 秒。

[0039] 参阅图 2，为本发明条件接收系统的示意框图，通过此系统来介绍密钥体系中各密钥的使用情况，首先将所用到的符号定义如下：

[0040] 1、IDT 表示用户卡的唯一标识号；

[0041] 2、“·”表示椭圆曲线上的点乘运算；

[0042] 3、椭圆曲线参数、P、y·P 和 s·P 都是系统可公开的参数；

[0043] 4、C1、C2 为系统对用户的控制因子（如用户信息、卡的有效期、运营商控制信息、本次分发专用控制信息等，均应可量化为字母数字串）；

[0044] 5、“||”表示两个串的组合，组合方式应使得组合后的结果可满足椭圆曲线密码体制的计算需要；

[0045] 6、EK(X)/DK(X) 分别表示用密钥 K 对 X 进行加密 / 解密。

[0046] 7、HMAC(X) 表示对 X 计算无密钥的消息验证码 (MAC)，在这里采用国密 SM3 计算 MAC，即 HMAC(X) = SM3(X) 的低 128 位。

[0047] 下面，通过条件接收系统的工作流程来介绍密钥体系中各密钥的使用情况。

[0048] 1) 发用户卡时

[0049] A. 用户卡生成用户的 ECC 密钥对 s 和 s·P。

[0050] B. 用户卡与运营商交换公钥。

[0051] 2) 当用户注册时

[0052] A. 用户持用户卡向运营商申请注册。

[0053] B. 运营商审查用户资料，为用户卡产生用户控制信息 C1（包含用户个人信息和有效期等），用前端私钥 y 对 C1 签名，并将 C1 及其签名写入用户卡。

[0054] C. 用户卡以前端公钥 y·P 验证运营商对 C1 签名的有效性，如签名无效则注册以失败结束，如签名有效则用户卡向运营商返回 IDT||C1 以及用用户卡私钥 s 对 IDT||C1 的签名。

[0055] D. 运营商根据 IDT 从数据库中提取用户卡公钥 s·P 验证用户卡对 IDT||C1 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 IDT||C1 及用户卡对 IDT||C1 的签名记录入数据库，注册成功。

[0056] 3) 前端系统在需要发布个人密钥 PK 时

[0057] A. 针对指定用户（通过用户卡的 IDT 标识）产生运营商控制信息 C2（如运营商代号、授权机构等）。

[0058] B. 前端 PK 发生器运行密钥协商发送方算法产生 PK、PK 的动态参数 R1 = H(r||C2)·P 和 PK 的验证参数 S1，r 为随机数。

[0059] C. 将 R1||S1 随 EMM 发送到用户终端。

[0060] 4) 用户终端接收 PK 时

[0061] 用户终端接收到 R1||S1 后，其 PK 发生器运行密钥协商接收方算法验证 R1||S1 的有效性，如有效则计算 PK，无效则不计算 PK（协商失败）。

[0062] 5) 前端系统在需要发布分发密钥 DK 时

[0063] A. 前端产生 DK 并记录入数据库。

[0064] B. 用 PK 对 DK 进行加密，得 C = EPK(DK)||MAC(DK)。

[0065] C. 将 C 随 EMM 发送到用户终端

[0066] 6) 用户终端接收 DK 时

[0067] A. 用 PK 解密 :DK = DPK(EPK(DK))。

[0068] B. 计算 HMAC(DK) 并与 C 中的 HMAC 值比较，相等则接受 DK，否则拒绝接受 DK。

[0069] 7) 在发布和接收业务密钥 SK 时

[0070] A. 前端产生 SK。

[0071] B. 用 DK 对 SK 进行加密，得 C = EDK(SK)||MAC(SK)，C 随 EMM 发送到用户终端。

[0072] C. 用户终端用 DK 解密出 SK，计算 HMAC(SK)，并与 C 中的 MAC 值比较，相等则接受 SK，否则拒绝接受 SK。

[0073] 若一个用户申请了 N 种业务并拥有这 N 项业务的收视权利时，可以 :

[0074] A. 前端 :C = EDK(SK1||SK2||.....SKN)||MAC(SK1||SK2||.....SKN)。

[0075] B. 用户终端 :对于某一业务，只用做与之对应的解密和校验操作。

[0076] 8) 在发布和接收 CW 时

[0077] A. 前端产生 CW。

[0078] B. 用 SK 对 CW 进行加密，得 C = ESK(CW)||HMAC(CW)，C 随 EMM 发送到用户终端。

[0079] C. 用户终端用 SK 解密出 CW，计算 HMAC(CW) 并与 C 中的 HMAC 值比较，相等则接受 CW，否则拒绝接受 CW。

[0080] 9) 在播放节目时

[0081] 用户终端用 CW 对节目内容密文数据解扰。

[0082] 上述密钥流程中 PK 协商采用国家 SM2-2 密钥协商算法标准。这里，PK 协商参数加入了运营商控制信息 C2，实现时可按需要选择确定是否要加进该参数。

[0083] 根据系统需求，上述流程中步骤 3) 和步骤 5) 可以合并进行，如此则步骤 4) 和步骤 6) 也应相应合并。

[0084] 根据需要，用户注册过程可以与发卡过程合并，则工作流程中的步骤 1) 和步骤 2) 可以合并进行，这样就可以简化注册过程。

[0085] 综上所述，本发明的密钥体系具有如下优点 :

[0086] 本发明中，所述的密码算法全部采用国家密码管理局指定的密码算法，符合国家

商用密码管理政策的要求。密码算法的强度高，能有效抵御基于数字电视广播网络的暴力攻击。

[0087] 本发明提出的密钥体系中的四层对称密钥，控制字 CW 与加扰数据相关联，业务密钥 SK 与受保护的节目（业务）相关联，分发密钥 DK 与用户对节目（业务）的使用权限相关联，个人密钥 PK 与用户相关联，这四层密钥通过高层密钥对低层密钥（节目数据）加密的层层保护机制，保护节目数据和密钥的安全性，实现有条件接收；一层非对称密钥，用于基于 ECC 的 PK 协商，提高了 PK 使用的安全性。这样的层次划分，不仅增加了系统的安全性，还为运营商开展多样性业务和进行系统的双向改造提供了技术支撑。

[0088] 以上说明对本发明而言只是说明性的，而非限制性的，本领域普通技术人员理解，在不脱离以下所附权利要求所限定的精神和范围的情况下，可做出许多修改，变化，或等效，但都将落入本发明的保护范围内。

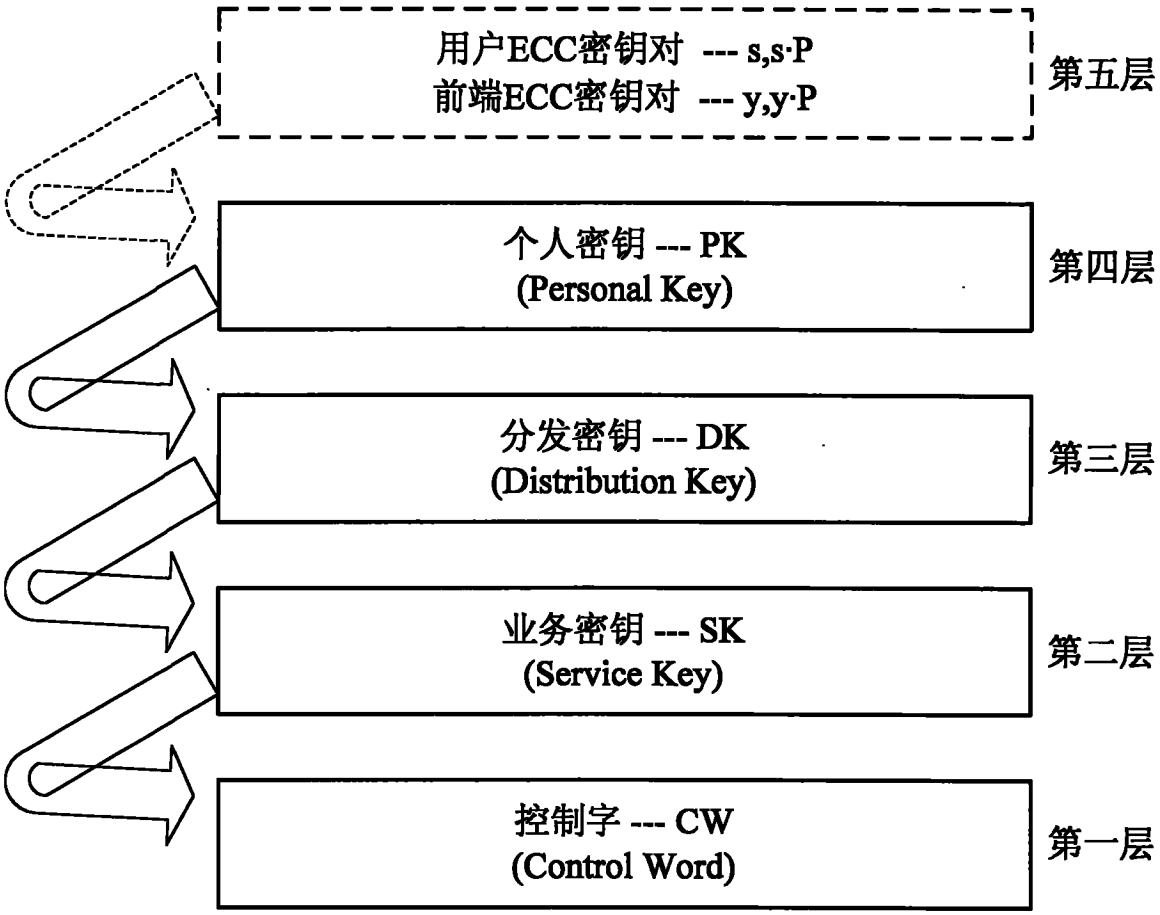

用户ECC密钥对 --- s,s·P
前端ECC密钥对 --- y,y·P
第五层
个人密钥 --- PK
(Personal Key)
第四层
分发密钥 --- DK
(Distribution Key)
第三层
业务密钥 --- SK
(Service Key)
第二层
控制字 --- CW
(Control Word)
第一层

图 1

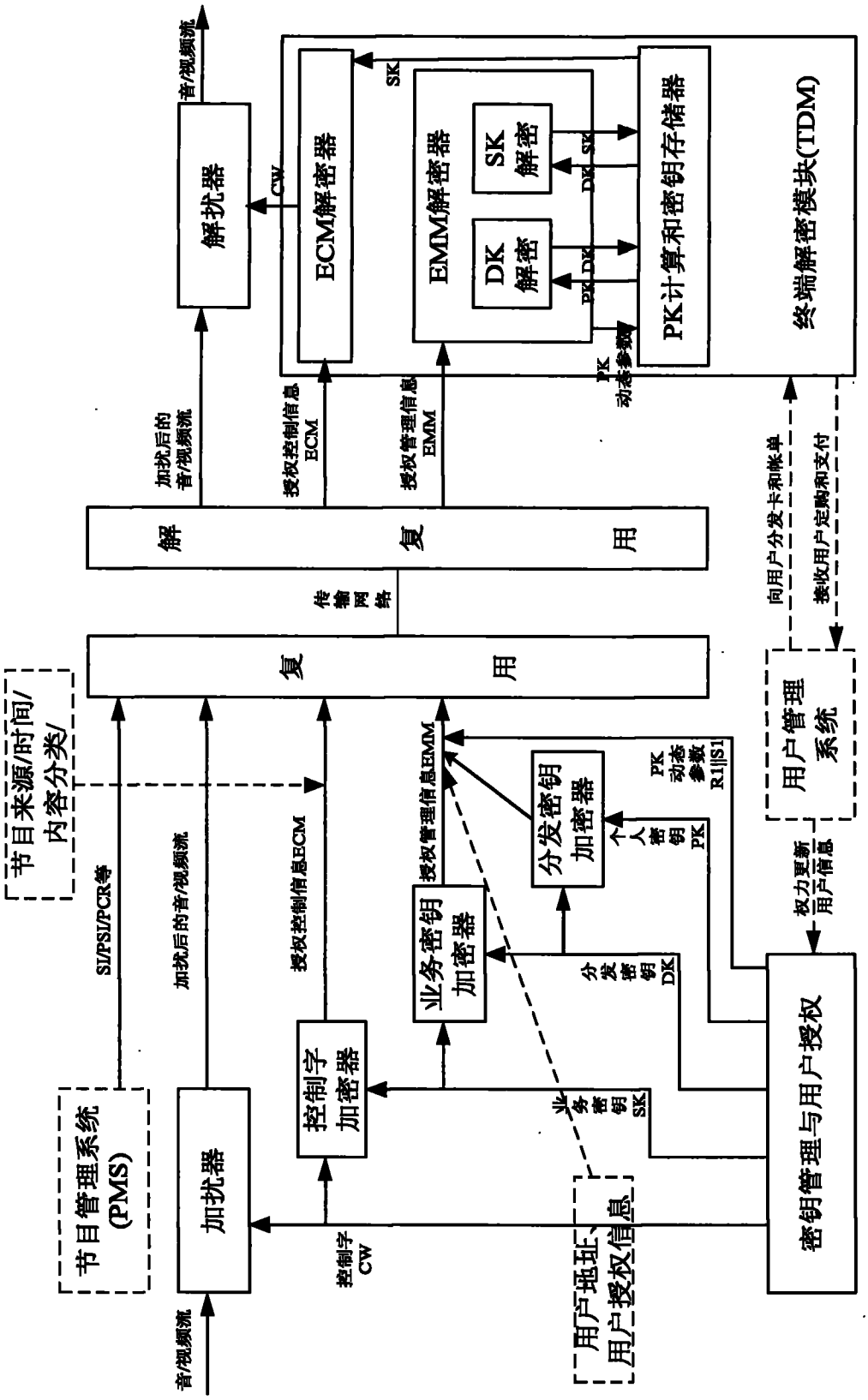

节目来源/时间/内容分类/
节目管理系统(PMS)
SI/PSI/PCR等
音/视频流
加扰器
加扰后的音/视频流
控制字CW
控制字加密器
授权控制信息ECM
业务密钥加密器
授权管理信息EMM
分发密钥加密器
个人密钥PK
PK动态参数R1||S1
分发密钥DK
业务密钥SK
用户地址、用户授权信息
密钥管理与用户授权
权力更新用户信息
用户管理系统
向用户分发卡和帐单
接收用户定购和支付
传输网络
解复用
加扰后的音/视频流
授权控制信息ECM
授权管理信息EMM
解扰器
音/视频流
CW
ECM解密器
EMM解密器
SK解密
DK解密
SK
DK
PK
PK动态参数
PK计算和密钥存储器
终端解密模块(TDM)

图 2