(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 101742236 B
(45)授权公告日 2015.06.10

(21)申请号 200910311992.9
(22)申请日 2009.12.22
(73)专利权人 山东泰信电子股份有限公司
地址 250101 山东省济南市高新区新泺大街2008号银荷大厦1-501-1
(72)发明人 陶圣华
(74)专利代理机构 济南圣达知识产权代理有限公司 37221
代理人 张勇
(51)Int.Cl.
H04N 21/4367(2011.01)
H04N 21/4623(2011.01)
(56)对比文件
CN 1279861 A,2001.01.10,
CN 101282456 A,2008.10.08,
佚名 泰信电子.对数字加密电视体系CAS安全性的探讨.《2007国际有线电视技术研讨会论文集》.2007,
审查员 李靖

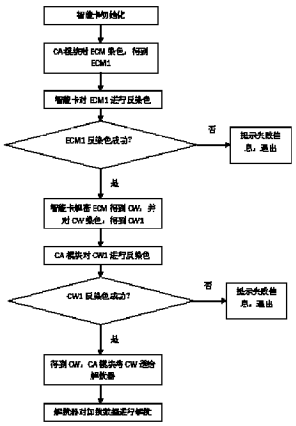
权利要求书1页 说明书6页 附图1页

(54)发明名称

一种预防和反制智能卡共享的方法

(57)摘要

本发明涉及一种预防和反制智能卡共享的方法，步骤为：(1)智能卡初始化，智能卡和机顶盒通信；(2)机顶盒接收数字电视信号，得到ECM并送给CA模块，CA模块对ECM进行染色，得到ECM1，并将ECM1送给智能卡；(3)智能卡对ECM1进行反染色，得到ECM，并对ECM进行解密，得到CW；(4)智能卡对CW进行染色，得到CW1，并将CW1送给CA模块；(5)CA模块对CW1进行反染色，得到CW，并将CW送给解扰器；(6)解扰器利用CW对加扰的音视频数据进行解扰。本发明可以有效防止智能卡的CW共享，在得知智能卡被共享后可以很容易的采取反制措施。



CN 101742236 B

1. 一种预防和反制智能卡共享的方法，其特征在于，它的流程为：

(1) 智能卡初始化，智能卡和机顶盒通信；

(2) 机顶盒接收数字电视信号，通过解复用器得到EMM信息和ECM信息并送给CA模块，CA模块对ECM信息进行染色，染色后的ECM标记为ECM1，并将ECM1送给智能卡；所述CA模块对ECM信息进行染色，是指CA模块先将ECM和机顶盒信息按照设定的规则进行组合，然后再利用密钥rskey1对组合后的信息进行加密，得到ECM1；

(3) 智能卡对接收到的ECM1进行反染色，若反染色失败，则提示失败信息，退出流程；若反染色成功，则得到还原的ECM，并对ECM进行解密，得到CW；所述智能卡对接收到的ECM1进行反染色，是指智能卡先利用密钥rskey1对ECM1进行解密，然后再对解密后的数据进行解析，进而得到ECM和机顶盒信息；

(4) 智能卡再对ECM解密得到的CW进行染色，染色后的CW标记为CW1，并将CW1送给机顶盒的CA模块；所述智能卡再对ECM解密得到的CW进行染色，是指智能卡先将CW和智能卡信息按照设定的规则进行组合，然后再利用密钥rskey2对组合后的信息进行加密；

(5)CA模块对接收到的CW1进行反染色，若反染色失败，则提示失败信息，退出流程；若反染色成功，则得到还原的CW，并将CW送给解扰器；所述CA模块对接收到的CW1进行反染色，是指CA模块先利用密钥rskey2对CW1进行解密，然后再对解密后的数据进行解析，进而得到CW和智能卡信息；

(6) 解扰器利用CW对加扰的音视频数据进行解扰，并将解扰后的数据送给播放模块播放。

2. 如权利要求1所述的预防和反制智能卡共享的方法，其特征在于，所述步骤(1)中，智能卡和机顶盒通信时，智能卡将能够唯一标识智能卡的智能卡信息和染色CW过程中用的密钥rskey2发送给机顶盒，同时，机顶盒将能够唯一标识机顶盒的机顶盒信息和染色ECM过程中用的密钥rskey1发送给智能卡。

3. 如权利要求2所述的预防和反制智能卡共享的方法，其特征在于，所述的密钥rskey1是机顶盒中的CA模块随机生成的密钥；所述的密钥rskey2是智能卡随机生成的密钥。

4. 如权利要求2所述的预防和反制智能卡共享的方法，其特征在于，所述的密钥rskey1和密钥rskey2均由智能卡随机生成或者由CA模块随机生成。

5. 如权利要求4所述的预防和反制智能卡共享的方法，其特征在于，所述密钥rskey1和密钥rskey2均由智能卡随机生成时，在每次智能卡初始化的时候都要进行重新生成。

一种预防和反制智能卡共享的方法

技术领域

[0001] 本发明涉及数字电视技术领域（包含有线、卫星、地面、移动数字电视和IPTV等），尤其涉及一种预防和反制智能卡共享的方法。

背景技术

[0002] 条件接收（ConditionalAccess简称CA）系统是指用来控制用户对数字电视业务进行接收的系统，即用户只能收看经过授权的数字电视节目（含音频、视频、数据等），其基本目的是运营商在电视系统中对用户进行授权控制及授权管理，从而实现数字电视系统的有偿服务。条件接收系统是数字电视系统中的一个基本的，也是最重要的组成部分。

[0003] 目前的数字电视条件接收系统主要基于10多年前欧洲的DVB标准，其主要原理是：经过前端加密的数字电视信号里有一对周期变更的密钥，叫做控制字，简称CW。条件接收系统负责对CW加密并安全地传输到数字电视接收端的解密器里，同时授予某些接收端的解密器解密的权限。这些有权限的解密器解密出CW，然后将其传输到解扰器中，解扰器利用CW解出音视频数据流供播放模块播放。当时在制定该标准的时候，只是考虑到如何将CW安全地送到接收端，而没有考虑到在接收端得到解密的CW后可以利用网络技术进行扩散共享CW，被盗版者利用。这在当前网络技术很发达的情况下，就成了这种系统的一个严重的漏洞，并被许多盗版者利用，给运营商带来严重的损失。

[0004] 现有的采用智能卡条件接收系统的接收端，解密算法就在智能卡中，解密过程是将加密的数据送到智能卡中，智能卡将解密后的CW传到接收端中，再通过接收端中的CA模块传输到解扰器中。CA模块作为一个独立的部分嵌入在机顶盒软件框架里。这种技术在多个地方可以截取CW，在安全上造成了隐患。图1指示出了CW的泄露点。

[0005] 第一个泄露点是智能卡和接收端之间的通讯点。

[0006] 第二个泄露点是CA模块和解扰器之间。

[0007] 第三个泄露点是CA模块和内存RAM之间的通讯过程。

[0008] 在上述的第二和第三个泄露点获取CW相对比较困难。但是，在第一个泄露点获得CW比较容易，使用简单的仪器就可以实现。一旦CW被获取，利用网络技术，CW可以被网络上的多台接收端使用，只使用一张智能卡就可以实现很多台接收端免费收视收费节目。更糟的情况是，即使运营商知道了智能卡被共享，也没有办法确定被用于共享的智能卡的卡号，没办法对这种CW共享进行反制。CW网络共享将会给运营商造成严重的经济损失。

发明内容

[0009] 本发明的目的就是为了解决目前的利用智能卡和接收端之间的通讯点获取CW，并将CW用于网络共享以及在得知智能卡被用于CW共享后无法采取反制措施等问题，提出了一种预防和反制智能卡共享的方法。

[0010] 为了实现上述目的，本发明采用如下技术方案：

[0011] 一种预防和反制智能卡共享的方法，它的流程为：

[0012] (1) 智能卡初始化，智能卡和机顶盒通信；

[0013] (2) 机顶盒接收数字电视信号，通过解复用器得到 EMM 信息和 ECM 信息并送给 CA 模块，CA 模块对 ECM 信息进行染色，染色后的 ECM 标记为 ECM1，并将 ECM1 送给智能卡；

[0014] (3) 智能卡对接收到的 ECM1 进行反染色，若反染色失败，则提示失败信息，退出流程；若反染色成功，则得到还原的 ECM，并对 ECM 进行解密，得到 CW；

[0015] (4) 智能卡再对 ECM 解密得到的 CW 进行染色，染色后的 CW 标记为 CW1，并将 CW1 送给机顶盒的 CA 模块；

[0016] (5)CA 模块对接收到的 CW1 进行反染色，若反染色失败，则提示失败信息，退出流程；若反染色成功，则得到还原的 CW，并将 CW 送给解扰器；

[0017] (6) 解扰器利用 CW 对加扰的音视频数据进行解扰，并将解扰后的数据送给播放模块播放。

[0018] 所述步骤 (1) 中，智能卡和机顶盒通信时，智能卡将能够唯一标识智能卡的智能卡信息和染色 CW 过程中用的密钥 rskey2 发送给机顶盒，同时，机顶盒将能够唯一标识机顶盒的机顶盒信息和染色 ECM 过程中用的密钥 rskey1 发送给智能卡。

[0019] 所述的密钥 rskey1 是机顶盒中的 CA 模块随机生成的密钥；所述的密钥 rskey2 是智能卡随机生成的密钥。

[0020] 所述的密钥 rskey1 和密钥 rskey2 均由智能卡随机生成或者由 CA 模块随机生成。

[0021] 所述密钥 rskey1 和密钥 rskey2 均由智能卡随机生成时，在每次智能卡初始化的时候都要进行重新生成。

[0022] 所述步骤 (2) 中的 CA 模块对 ECM 进行染色，是指 CA 模块先将 ECM 和机顶盒信息按照设定的规则进行组合，然后再利用密钥 rskey1 对组合后的信息进行加密，得到 ECM1。

[0023] 所述步骤 (3) 的智能卡对 ECM1 进行反染色，是指智能卡先利用密钥 rskey1 对 ECM1 进行解密，然后再对解密后的数据进行解析，进而得到 ECM 和机顶盒信息。

[0024] 所述步骤 (4) 的智能卡对 CW 进行染色，是指智能卡先将 CW 和智能卡信息按照设定的规则进行组合，然后再利用密钥 rskey2 对组合后的信息进行加密。

[0025] 所述步骤 (5) 的 CA 模块对 CW1 进行反染色，是指 CA 模块先利用密钥 rskey2 对 CW1 进行解密，然后再对解密后的数据进行解析，进而得到 CW 和智能卡信息。

[0026] 本发明所述方法中，分别对 ECM 和 CW 进行染色和反染色。这样即使 CW 通过智能卡和机顶盒之间的通讯点被泄露了，由于此处泄露的是染色后的 CW，没有智能卡的共享客户端机顶盒由于没有 CW 反染色过程中使用的密钥 rskey2 将无进行正常收视；另外，由于共享客户端机顶盒没有 ECM 染色过程中使用的 rskey1 密钥，无法对 ECM 进行正常染色，智能卡将拒绝为共享客户端机顶盒发送的 ECM 解析出 CW。即使 rskey1 和 rskey2 被共享客户端机顶盒伪造，由于 ECM 染色过程中将 ECM 和能唯一标识机顶盒的机顶盒信息进行了组合，智能卡也将拒绝为共享客户端机顶盒发送的 ECM 解析出 CW；另外，由于 CW 染色过程中将 CW 和能够唯一标识智能卡的智能卡信息进行了组合，共享客户端机顶盒在不知道智能卡信息的情况下也将无法进行共享。因此，只要能保证 ECM 染色过程中使用的密钥 rskey1、CW 染色过程中使用的密钥 rskey2、插有智能卡做共享服务端的机顶盒的机顶盒信息和智能卡信息四个中有一个是安全的，没有被共享客户端机顶盒获知，智能卡将无法被用于共享。即使密钥 rskey1、密钥 rskey2、智能卡信息和共享服务端机顶盒的机顶盒信息都被共享客户端

机顶盒获知了，客户端机顶盒可以共享智能卡了，由于共享客户端机顶盒接收到的是经过染色的 CW，经过染色的 CW 包含有智能卡信息，通过任意一台共享客户端机顶盒都可以获知智能卡的信息，进而可以通过条件接收系统前端取消对被用于共享的智能卡的授权，进行共享反制。

[0027] 本发明的有益效果是：可以有效的预防因智能卡和接收端之间的通讯点泄露 CW 而导致的智能卡共享，并且可以在得知智能卡被共享后快速简单的采取反制措施，安全性高。

附图说明

[0028] 图 1 是采用智能卡条件接收系统的接收端的 CW 泄漏点示意图；

[0029] 图 2 是本发明所述的一种预防和反制智能卡共享的方法的流程图。

具体实施方式

[0030] 下面结合附图与实施例对本发明做进一步说明。

[0031] 此处所说明的附图用来提供对本发明的进一步理解，构成本发明的一部分，本发明的示意实施例及其说明用于解释本发明，并不够成对本发明的不当限定。

[0032] 图 1 是采用智能卡条件接收系统的接收端的 CW 泄漏点示意图，主要包括三个泄漏点：第一个泄露点是智能卡和接收端之间的通讯点；第二个泄露点是 CA 模块和解扰器之间；第三个泄露点是 CA 模块和内存 RAM 之间的通讯过程。在上述的第二和第三个泄露点获取 CW 相对比较困难。但是，在第一个泄露点获得 CW 比较容易，使用简单的仪器就可以实现。

[0033] 图 2 是本发明所述的一种预防和反制智能卡共享的方法的流程图，它包括：

[0034] (1) 智能卡初始化，智能卡和机顶盒通信；

[0035] (2) 机顶盒接收数字电视信号，通过解复用器得到 EMM 信息和 ECM 信息并送给 CA 模块，CA 模块对 ECM 信息进行染色，染色后的 ECM 标记为 ECM1，并将 ECM1 送给智能卡；

[0036] (3) 智能卡对接收到的 ECM1 进行反染色，若反染色失败，则提示失败信息，退出流程；若反染色成功，则得到还原的 ECM，并对 ECM 进行解密，得到 CW；

[0037] (4) 智能卡再对 ECM 解密得到的 CW 进行染色，染色后的 CW 标记为 CW1，并将 CW1 送给机顶盒的 CA 模块；

[0038] (5)CA 模块对接收到的 CW1 进行反染色，若反染色失败，则提示失败信息，退出流程；若反染色成功，则得到还原的 CW，并将 CW 送给解扰器；

[0039] (6) 解扰器利用 CW 对加扰的音视频数据进行解扰，并将解扰后的数据送给播放模块播放。

[0040] 实施例 1：

[0041] 结合附图 2，一种预防和反制智能卡共享的方法的流程为：

[0042] (1) 智能卡初始化，智能卡生成随机密钥 rskey2 用于 CW 染色和反染色过程中的加解密，智能卡将能唯一标识一张智能卡的智能卡号和密钥 rskey2 发送给机顶盒，机顶盒将收到的智能卡号和密钥 rskey2 再发送给智能卡以确保数据发送成功；同时，机顶盒中的 CA 模块生成随机密钥 rskey1 用于 ECM 染色和反染色过程中的加解密，机顶盒将能唯一标识机

顶盒的机顶盒号和密钥 rskey1 发送给智能卡，智能卡将收到机顶盒号和密钥 rskey1 再发送回机顶盒以确保数据发送成功；

[0043] (2) 机顶盒接收数字电视信号，通过解复用器得到 ECM 信息，并将 ECM 信息送给 CA 模块，CA 模块将机顶盒号和 ECM 信息按照顺序排列组合，然后利用密钥 rskey1 对组合后的数据进行加密，得到 ECM1，并将 ECM1 发送给智能卡；

[0044] (3) 智能卡接收 ECM1，利用密钥 rskey1 对 ECM1 进行解密，如果解密失败，提示错误并退出流程；如果 ECM1 解密成功，则判断解密后的数据中的机顶盒号和智能卡初始化过程中接收到的机顶盒号是否匹配，如果不匹配，也提示错误并退出；如果机顶盒号匹配，则 ECM1 反染色成功，智能卡对反染色得到的 ECM 进行解密，得到 CW；

[0045] (4) 智能卡将智能卡号和 CW 按照顺序排列的方式进行组合，然后利用密钥 rskey2 对组合后的数据进行加密，得到 CW1，并将 CW1 发给机顶盒中的 CA 模块；

[0046] (5)CA 模块接收到 CW1，利用密钥 rskey2 对 CW1 进行解密，如果解密失败，提示错误并退出流程；如果 CW1 解密成功，则判断解密后的数据中的智能卡号和智能卡初始化过程中机顶盒接收到的智能卡号是否匹配，如果不匹配，则提示错误并退出流程；如果智能卡号匹配，则 CW1 反染色成功，CA 模块得到解密加扰音视频数据使用的 CW，并将 CW 送给解扰器；

[0047] (6) 解扰器接收 CW，利用 CW 解扰音视频数据，并将解扰后的音视频数据发送给播放模块，进而在电视上播放加扰的电视节目。

[0048] 实施例 1 中，ECM 染色、ECM 反染色、CW 染色和 CW 反染色过程中必须使用密钥 rskey1、密钥 rskey2、智能卡号和机顶盒号，可见只要密钥 rskey1、密钥 rskey2、智能卡号和机顶盒号四个中有一个是安全的，智能卡就无法实现共享。即使密钥 rskey1、密钥 rskey2、智能卡号和机顶盒号都被泄露了，由于机顶盒中的 CA 模块收到的是 CW1（染色后的 CW），CW1 包含有智能卡号，通过任意一台共享的机顶盒都可以获知用于共享的智能卡的卡号，可以很容易的通过条件接收系统前端对用于共享的智能卡进行反制。

[0049] 实施例 2：

[0050] 结合附图 2，一种预防和反制智能卡共享的方法的流程为：

[0051] (1) 智能卡初始化，智能卡生成随机密钥 rskey，rskey 用于 CW 染色和反染色过程中的加解密以及 ECM 染色和反染色过程中的加解密，智能卡将能唯一标识一张智能卡的智能卡号和密钥 rskey 发送给机顶盒，机顶盒将收到的智能卡号和密钥 rskey 再发送给智能卡以确保数据发送成功；同时，机顶盒中的 CA 模块不生成染色和反染色使用的密钥，机顶盒将能唯一标识机顶盒的机顶盒号和密钥 rskey 发送给智能卡，智能卡将收到机顶盒号和密钥 rskey 再发送回机顶盒以确保数据发送成功；

[0052] (2) 机顶盒接收数字电视信号，通过解复用器得到 ECM 信息，并将 ECM 信息送给 CA 模块，CA 模块将机顶盒号和 ECM 信息按照顺序排列组合，然后利用密钥 rskey 对组合后的数据进行加密，得到 ECM1，并将 ECM1 发送给智能卡；

[0053] (3) 智能卡接收 ECM1，利用密钥 rskey 对 ECM1 进行解密，如果解密失败，提示错误并退出流程；如果 ECM1 解密成功，则判断解密后的数据中的机顶盒号和智能卡初始化过程中接收到的机顶盒号是否匹配，如果不匹配，也提示错误并退出；如果机顶盒号匹配，则 ECM1 反染色成功，智能卡对反染色得到的 ECM 进行解密，得到 CW；

[0054] (4) 智能卡将智能卡号和 CW 按照顺序排列的方式进行组合，然后利用密钥 rskey 对组合后的数据进行加密，得到 CW1，并将 CW1 发给机顶盒中的 CA 模块；

[0055] (5)CA 模块接收到 CW1，利用密钥 rskey 对 CW1 进行解密，如果解密失败，提示错误并退出流程；如果 CW1 解密成功，则判断解密后的数据中的智能卡号和智能卡初始化过程中机顶盒接收到的智能卡号是否匹配，如果不匹配，则提示错误并退出流程；如果智能卡号匹配，则 CW1 反染色成功，CA 模块得到解密加扰音视频数据使用的 CW，并将 CW 送给解扰器；

[0056] (6) 解扰器接收 CW，利用 CW 解扰音视频数据，并将解扰后的音视频数据发送给播放模块，进而在电视上播放加扰的电视节目。

[0057] 实施例 2 中，ECM 染色、ECM 反染色、CW 染色和 CW 反染色过程中必须使用密钥 rskey、智能卡号和机顶盒号，可见只要密钥 rskey、智能卡号和机顶盒号中有一个是安全的，智能卡就无法实现共享。即使密钥 rskey、智能卡号和机顶盒号都被泄露了，由于机顶盒中的 CA 模块收到的是 CW1（染色后的 CW），CW1 包含有智能卡号，通过任意一台共享的机顶盒都可以获知用于共享的智能卡的卡号，可以很容易的通过条件接收系统前端对用于共享的智能卡进行反制。

[0058] 实施例 3：

[0059] 结合附图 2，一种预防和反制智能卡共享的方法的流程为：

[0060] (1) 智能卡初始化，智能卡不生成染色和反染色过程中用的密钥，智能卡将能唯一标识一张智能卡的智能卡号发送给机顶盒，机顶盒将收到的智能卡号再发送给智能卡以确保数据发送成功；同时，机顶盒中的 CA 模块生成随机密钥 rskey，用于 ECM 染色和反染色过程中的加解密以及 CW 染色和反染色过程中的加解密，机顶盒将能唯一标识机顶盒的机顶盒号和密钥 rskey 发送给智能卡，智能卡将收到机顶盒号和密钥 rskey 再发送回机顶盒以确保数据发送成功；

[0061] (2) 机顶盒接收数字电视信号，通过解复用器得到 ECM 信息，并将 ECM 信息送给 CA 模块，CA 模块将机顶盒号和 ECM 信息按照顺序排列组合，然后利用密钥 rskey 对组合后的数据进行加密，得到 ECM1，并将 ECM1 发送给智能卡；

[0062] (3) 智能卡接收 ECM1，利用密钥 rskey 对 ECM1 进行解密，如果解密失败，提示错误并退出流程；如果 ECM1 解密成功，则判断解密后的数据中的机顶盒号和智能卡初始化过程中接收到的机顶盒号是否匹配，如果不匹配，也提示错误并退出；如果机顶盒号匹配，则 ECM1 反染色成功，智能卡对反染色得到的 ECM 进行解密，得到 CW；

[0063] (4) 智能卡将智能卡号和 CW 按照顺序排列的方式进行组合，然后利用密钥 rskey 对组合后的数据进行加密，得到 CW1，并将 CW1 发给机顶盒中的 CA 模块；

[0064] (5)CA 模块接收到 CW1，利用密钥 rskey 对 CW1 进行解密，如果解密失败，提示错误并退出流程；如果 CW1 解密成功，则判断解密后的数据中的智能卡号和智能卡初始化过程中机顶盒接收到的智能卡号是否匹配，如果不匹配，则提示错误并退出流程；如果智能卡号匹配，则 CW1 反染色成功，CA 模块得到解密加扰音视频数据使用的 CW，并将 CW 送给解扰器；

[0065] (6) 解扰器接收 CW，利用 CW 解扰音视频数据，并将解扰后的音视频数据发送给播放模块，进而在电视上播放加扰的电视节目。

[0066] 实施例 3 中，ECM 染色、ECM 反染色、CW 染色和 CW 反染色过程中必须使用密钥 rskey、智能卡号和机顶盒号，可见只要密钥 rskey、智能卡号和机顶盒号中有一个是安全

的，智能卡就无法实现共享。即使密钥rskey、智能卡号和机顶盒号都被泄露了，由于机顶盒中的CA模块收到的是CW1（染色后的CW），CW1包含有智能卡号，通过任意一台共享的机顶盒都可以获知用于共享的智能卡的卡号，可以很容易的通过条件接收系统前端对用于共享的智能卡进行反制。

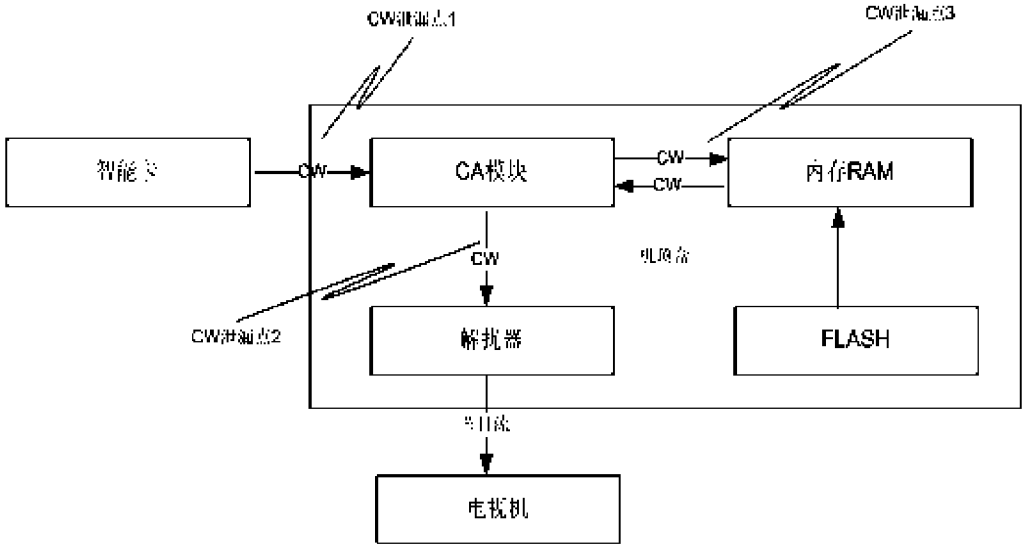

CW泄漏点1
CW泄漏点3
智能卡
CW
CA模块
CW
CW
内存RAM
CW
电源
CW泄漏点2
解扰器
FLASH
电视机

图 1

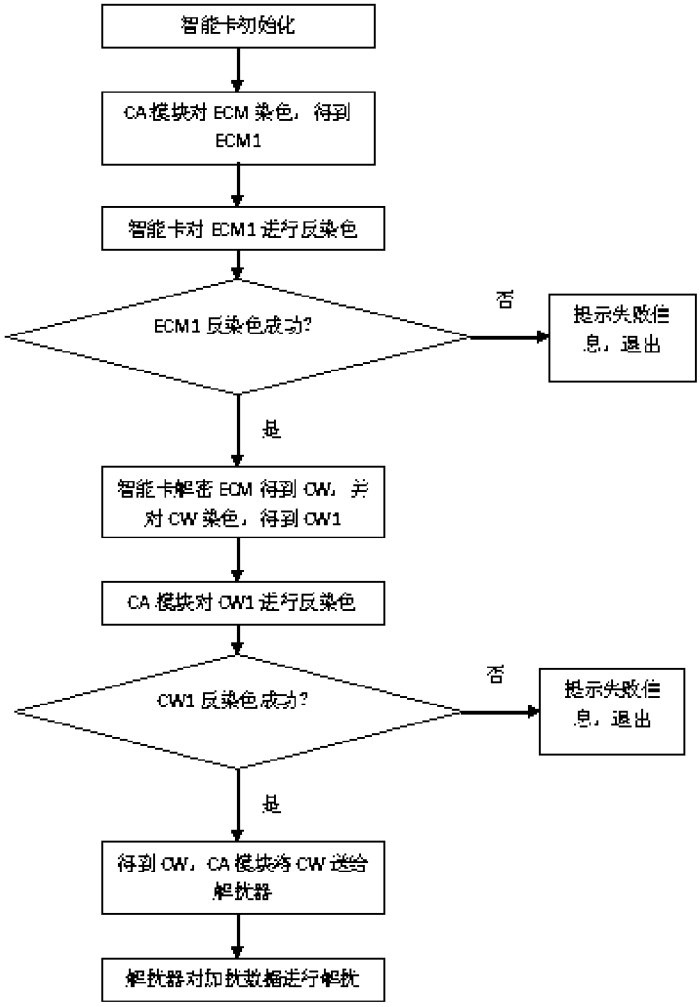

智能卡初始化
CA模块对 ECM 染色，得到 ECM1
智能卡对 ECM1 进行反染色
ECM1 反染色成功?
否
提示失败信息，退出
是
智能卡解密 ECM 得到 CW，并对 CW 染色，得到 CW1
CA 模块对 CW1 进行反染色
CW1 反染色成功?
否
提示失败信息，退出
是
得到 CW，CA 模块将 CW 送给解扰器
解扰器对加扰数据进行解扰

图 2