[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/16 (2008.01)
H04H 60/23 (2008.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710172886.8

[43] 公开日 2008 年 6 月 11 日

[11] 公开号 CN 101198014A

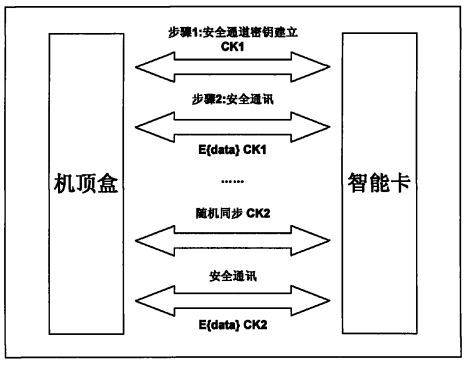
[22] 申请日 2007.12.25
[21] 申请号 200710172886.8
[71] 申请人 天栢宽带网络科技（上海）有限公司
地址 201103 上海市宜山路 2016 号合川大厦 9 楼
[72] 发明人 吕 品 陈德钊
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 陈 亮
权利要求书 1 页 说明书 4 页 附图 3 页

[54] 发明名称

一种防范智能卡共享 CA 的方法

[57] 摘要

本发明公开了防范智能卡共享条件访问的方法，防止用户通过共享智能卡，同时用多台机顶盒收看数字电视节目。 其技术方案为：方法包括在智能卡初始化时，机顶盒向该智能卡发送命令请求建立安全通道密钥；该智能卡产生随机安全密钥，作为该安全通道密钥回传给该机顶盒，其中该安全通道密钥在该智能卡的每一次初始化时都不相同；该机顶盒与该智能卡之间建立随机序列的安全的握手通讯；该机顶盒与该智能卡之间的通讯信息通过该安全通道密钥进行加密；在后续的数据通讯中，该智能卡和该机顶盒通过随机同步机制建立新的安全通道密钥以替换之前的安全通道密钥。 本发明应用于数字电视领域中。



1、一种防范智能卡共享条件访问的方法，包括：

（1）在智能卡初始化时，机顶盒向该智能卡发送命令请求建立安全通道密钥；

（2）该智能卡产生随机安全密钥，作为该安全通道密钥回传给该机顶盒，其中该安全通道密钥在该智能卡的每一次初始化时都不相同；

（3）该机顶盒与该智能卡之间建立随机序列的安全的握手通讯；

（4）该机顶盒与该智能卡之间的通讯信息通过该安全通道密钥进行加密；

（5）在后续的数据通讯中，该智能卡和该机顶盒通过随机同步机制建立新的安全通道密钥以替换之前的安全通道密钥。

2、根据权利要求1所述的防范智能卡共享条件访问的方法，其特征在于，该智能卡初始化是在机顶盒开机或者智能卡被插入或拔除的时候。

3、根据权利要求1所述的防范智能卡共享条件访问的方法，其特征在于，该方法还包括：

将指令的数据长度设为可变化。

一种防范智能卡共享CA的方法

技术领域

本发明涉及一种防范智能卡共享CA（Conditional Access，有条件访问）的方法，尤其涉及一种通过智能卡与机顶盒之间的对数据通讯的随机加密实现防止用户通过对智能卡进行共享以用一张智能卡同时在多台机顶盒上收看数字电视节目的情况的发生。

背景技术

在目前的数字电视系统中，CA就是其中的加密认证。利用CA系统对数字化处理后的节目流进行加密处理，并辅助以加密控制信息，这样可以按照用户的付费情况来分别设置用户的收看权限，利用用户端的机顶盒内放置智能卡来实现收看付费电视的功能，从而达到可以实现按频道收费、按节目付费、按收费次数收费的目的，同时也保证非法用户、不付费用户不能收看到收费电视。

在机顶盒内通常设有特殊的处理器，用于执行解译密钥、消息以及内容的操作功能。在智能卡方式中，解密装置是分布在机顶盒和可插拔的智能卡之间，另一个安全电路和固件嵌入在机顶盒内。当机顶盒接收到来自智能卡的消息时，即可实现内容的解密操作。

目前出现了一种以多机共享一卡的共享系统，使消费者通过该系统可以使家庭中的主机和副机共享主机上的合法智能卡，通过主副机之间的共享通道，达到一张卡两台盒子共用的目的，这样就意味着，消费者完全可以通过此种方式逃避副机所产生的智能卡及月租费用，使运营商的利益蒙受损失，目前尚没有很好的解决方法。

发明内容

本发明的目的在于提供了一种防范智能卡共享条件访问的方法，防止用户通过共享智能卡，同时用多台机顶盒收看数字电视节目。

本发明的技术方案为：本发明揭示了一种防范智能卡共享条件访问的方法，包括：

（1）在智能卡初始化时，机顶盒向该智能卡发送命令请求建立安全通道密钥；

（2）该智能卡产生随机安全密钥，作为该安全通道密钥回传给该机顶盒，其中该安全通道密钥在该智能卡的每一次初始化时都不相同；

（3）该机顶盒与该智能卡之间建立随机序列的安全的握手通讯；

（4）该机顶盒与该智能卡之间的通讯信息通过该安全通道密钥进行加密；

（5）在后续的数据通讯中，该智能卡和该机顶盒通过随机同步机制建立新的安全通道密钥以替换之前的安全通道密钥。

上述的防范智能卡共享条件访问的方法，其中，该智能卡初始化是在机顶盒开机或者智能卡被插入或拔除的时候。

上述的防范智能卡共享条件访问的方法，其中，该方法还包括：

将指令的数据长度设为可变化。

本发明对比现有技术，有如下的有益效果：本发明通过在智能卡和机顶盒之间建立安全通道密钥，并在通讯过程中根据随机同步机制建立新的安全通道密钥，还通过将指令设置为数据长度可变，有效防止用户通过共享智能卡实现多台机顶盒同时收看数字电视节目的问题。

附图说明

图 1 是本发明的机顶盒和智能卡之间的安全通道密钥的验证原理示意图。

图 2 是本发明的机顶盒端的流程图。

图 3 是本发明的智能卡端的流程图。

具体实施方式

下面结合附图和实施例对本发明作进一步的描述。

图 1 示出了本发明的机顶盒与智能卡之间的验证原理。请参见图 1，首先在智能卡初始化时，机顶盒和智能卡之间建立安全通道密钥（即图示的步骤 1）。具体地说，在机顶盒开机或者智能卡被插入或拔除时智能卡被初始化，由机顶盒先向智能卡发送命令请求建立安全通道密钥，然后智能卡产生随机安全密

钥，作为安全通道密钥 CK1 回传给机顶盒，其中安全通道密钥在智能卡的每次初始化时都是不同的。

机顶盒与智能卡之间根据前一步骤的安全通道密钥 CK1 建立起随机序列的握手通讯（即图示的步骤 2）。之后机顶盒与智能卡之间的数据通讯通过安全通道密钥 CK1 进行加密。

在后续的数据通讯中，智能卡和机顶盒通过随机同步机制建立新的安全通道密钥 CK2 以替换原来的安全通道密钥 CK1，之后的数据通讯通过安全通道密钥 CK2 进行加密。依此类推，智能卡和机顶盒之间还可以建立安全通道密钥 CK3 以替换 CK2 等。

在数据通讯中，将指令设置成数据长度可变。例如，机顶盒 A 发送指令给智能卡和智能卡回复命令给机顶盒 B，它们的数据长度在每一个时间点都是不同的，如表一所示。

命令	从 STB 发送命令到 Smart Card 的数据长度	从 Smart Card 发送命令到 STB 的数据长度
Command A STB →SC	10	
Command B STB ←SC		20
Command A STB →SC	12	
Command B STB ←SC		18

表一

因此，对于同样的指令，其数据长度不是固定不变的，黑客不能根据命令长度确定是哪一条指令或者进行简单的逆向工程进行破解。

图 2 示出了机顶盒端的流程。请参见图 2，下面是对流程中各个步骤的说明。

步骤 S10：机顶盒开机。

步骤 S12：等待智能卡初始化。

步骤 S14：机顶盒发送命令请求建立安全通道密钥（CK）。

步骤 S16：接收智能卡产生并回传的安全通道密钥（CK）。

步骤 S18：机顶盒与智能卡之间的通讯信息通过安全密钥（CK）进行加密。

在通讯过程中，机顶盒可以请求智能卡重新产生新的随机安全通道密钥。若需产生新的随机安全通道密钥，则返回步骤 S14 的运作。

图 3 示出了智能卡端的流程。请参见图 3，下面是对流程中各个步骤的说明。

步骤 S20：智能卡初始化。智能卡在两处会被初始化，一处是在机顶盒开机的时候，一处是在智能卡插入或拔除的时候。

步骤 S21：等待机顶盒发出指令。

步骤 S22：判断通讯数据是否已被安全通道密钥（CK）加密，如果已被加密则进入步骤 S23，否则进入步骤 S26。

步骤 S23：判断是否要求新的安全通道密钥（CK）。如果是则进入步骤 S24，否则进入步骤 S25。

步骤 S24：根据随机同步机制产生新的安全通道密钥并发送给机顶盒，流程结束。

步骤 S25：进行智能卡译码操作，通过数据命令进行解码，流程结束。

步骤 S26：中断通讯，流程结束。

这些步骤中每次都产生不同值的安全通道密钥，亦即安全通道密钥的值是随机的。

由于安全通道密钥是智能卡随机产生的，当机顶盒 A 请求变换安全通道密钥时，密钥将被智能卡产生并回应给机顶盒 A。然后机顶盒 A 与智能卡利用这个密钥建立进一步的通讯。如果另一个机顶盒 B 用另外一个安全通道密钥发送命令给智能卡，智能卡将阻止这个通讯。因此，即使黑客复制了同样存储内存的另一台机顶盒，当智能卡检测安全通道密钥不是自己所要的密钥时，系统将停止工作以预防恶意破解，可以阻止黑客通过任何破解行为获取机顶盒 A 与智能卡之间的数据包。

上述实施例是提供给本领域普通技术人员来实现或使用本发明的，本领域普通技术人员可在不脱离本发明的发明思想的情况下，对上述实施例做出种种修改或变化，因而本发明的保护范围并不被上述实施例所限，而应该是符合权利要求书提到的创新性特征的最大范围。

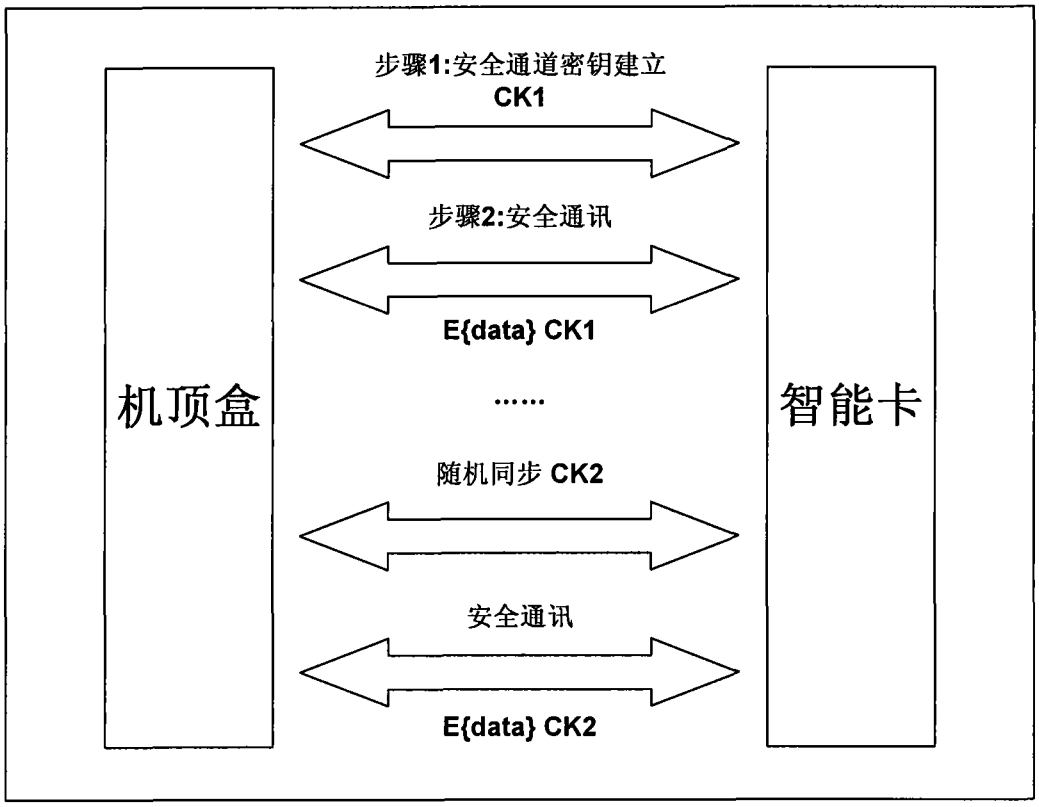

步骤1:安全通道密钥建立
CK1
步骤2:安全通讯
E{data} CK1
.....
随机同步 CK2
安全通讯
E{data} CK2
机顶盒
智能卡

图 1

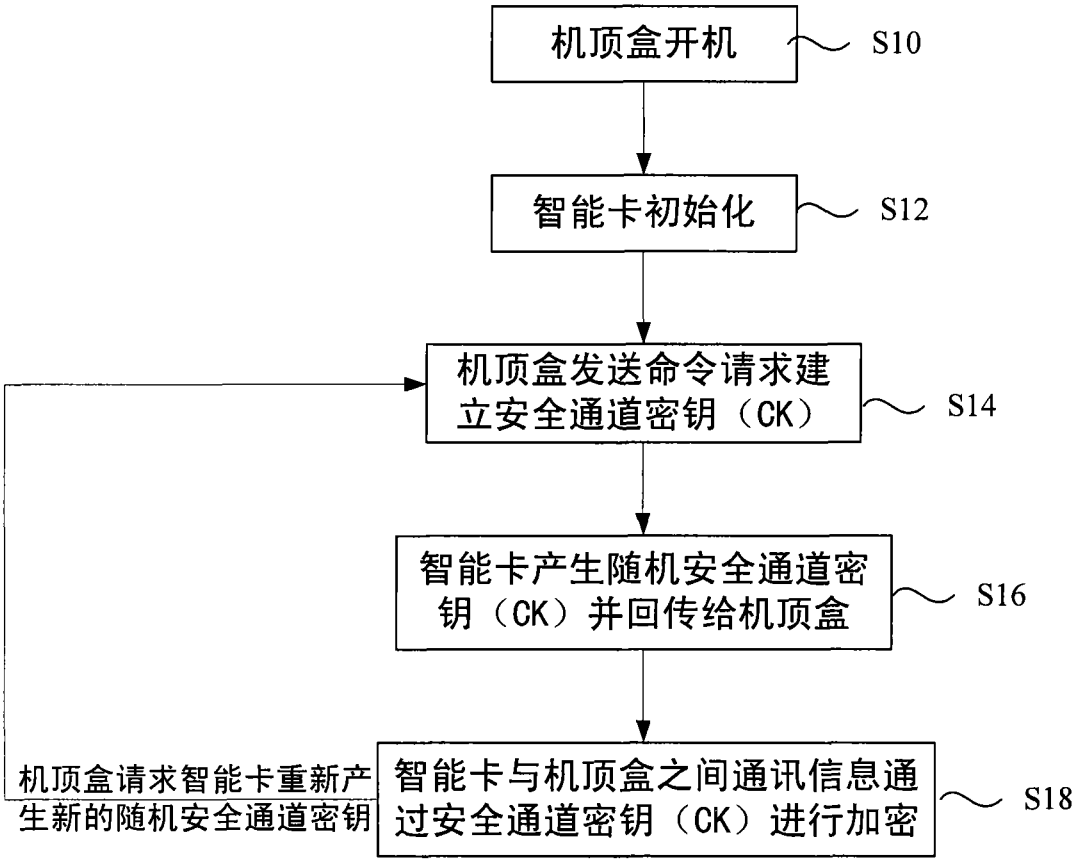

机顶盒开机
S10
智能卡初始化
S12
机顶盒发送命令请求建立安全通道密钥（CK）
S14
智能卡产生随机安全通道密钥（CK）并回传给机顶盒
S16
智能卡与机顶盒之间通讯信息通过安全通道密钥（CK）进行加密
S18
机顶盒请求智能卡重新产生新的随机安全通道密钥

图 2

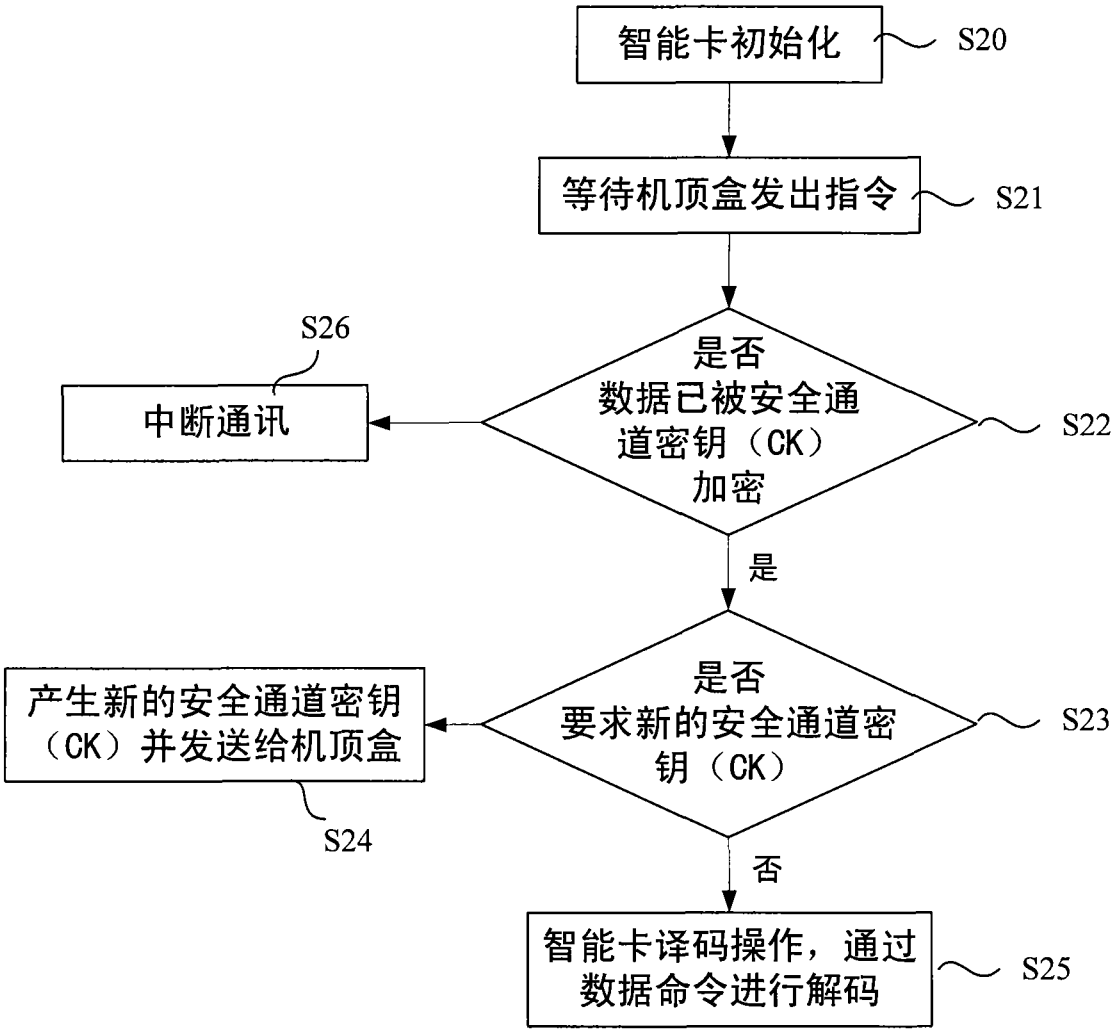

智能卡初始化
S20
等待机顶盒发出指令
S21
是否
数据已被安全通
道密钥（CK）
加密
S22
S26
中断通讯
是
是否
要求新的安全通道密
钥（CK）
S23
产生新的安全通道密钥
（CK）并发送给机顶盒
S24
否
智能卡译码操作，通过
数据命令进行解码
S25

图 3