[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04N 7/16
H04N 7/167

[12] 发明专利说明书

[21] ZL 专利号 97193565.3

[45] 授权公告日 2004 年 1 月 7 日

[11] 授权公告号 CN 1134161C

[22] 申请日 1997.3.21 [21] 申请号 97193565.3
[30] 优先权
[32] 1996. 4. 3 [33] EP [31] 96200907.2
[86] 国际申请 PCT/EP97/01557 1997.3.21
[87] 国际公布 WO97/38530 英 1997.10.16
[85] 进入国家阶段日期 1998.9.30
[71] 专利权人 耶德托存取公司
地址 荷兰霍夫多普
[72] 发明人 西蒙·鲍尔·阿什利·里克斯
安德鲁·格拉斯普尔
多纳德·瓦茨·戴维斯
审查员 郑 直

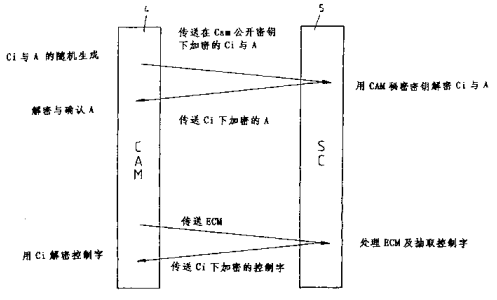
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 杨国旭

权利要求书 5 页 说明书 4 页 附图 2 页

[54] 发明名称 在两个设备之间提供安全通信的方法及使用该方法的设备

[57] 摘要

在两个设备之间提供安全通信的方法中，第一设备生成随机密钥(C_i)并在采用公开密钥加密的第一报文中将这一密钥传送给第二设备。第二设备用对应的秘密密钥解密第一加密报文以获取该随机密钥(C_i)并用这一随机密钥来加密与解密这两个设备之间的所有传输。在收费电视系统的解码器中，包含条件接入模块及智能卡，应用这一方法来提供控制接入模块与智能卡之间与/或解码器与条件接入模块之间的安全通信。



ISSN1008-4274

1.在两个设备之间提供安全通信的方法，其中，第一设备生成随机密钥(C_i)并在用公开密钥加密的第一报文中将所述密钥传送给第二设备，其中所述第二设备用对应的秘密密钥解密第一加密报文以获取所述随机密钥(C_i)，其中利用所述随机密钥来加密与解密所述设备之间的传输。

2.按照权利要求1的方法，其中解密了所述加密的报文之后，所述第二设备首先在带有认证的第二加密报文中返回所述随机密钥(C_i)给所述第一设备。

3.按照权利要求2的方法，其中为了提供所述认证，所述第一设备还生成随机数（A）并在所述第一加密报文中将这一随机数（A）与所述随机密钥（C_i）一起传送给第二设备，其中该第二设备利用所述随机数（A）供在第二加密报文中认证。

4.按照权利要求3的方法，其中所述第二设备在所述随机密钥(C_i)下加密所述随机数（A）来获得所述第二加密报文。

5.一种用于收费电视系统的解码器中的方法，其中所述解码器包括条件接入模块（CAM）及智能卡（SC），其中该条件接入模块（CAM）产生一个随机密钥（Ci）并且把所述密钥中使用公开密钥加密的第一报文中传送到该智能卡，其中该智能卡（SC）通过一个相应的秘密密钥来解密该第一加密报文，以获得所述随机密钥（Ci），其中所述随机密钥被用于加密和解密所述设备之间的传输。

6.按照权利要求5的方法，其中在解密所述加密报文之后，所述智能卡（SC）首先在带有认证的第二加密报文中把所述随机密钥（Ci）返回到所述条件接入模块（CAM）。

7. 按照权利要求6的方法，其中为了提供所述认证，所述条件接入模块（CAM）进一步产生一个随机数（A），并且把该随机数（A）与所述随机密钥（Ci）一同在所述第一加密报文中传送

到该智能卡（SC），其中该智能卡（SC）使用所述随机数（A），用于在第二加密报文中的认证。

8. 按照权利要求 7 的方法，其中所述智能卡用所述随机密钥（Ci）加密所述随机数（A），以获得所述第二加密密钥。

9. 一种用于收费电视系统的解码器中的方法，其中所述解码器包括条件接入模块（CAM）及智能卡（SC），其中该解码器产生随机密钥（Ci）并且在使用公开密钥加密的第一报文中把所述密钥传送到该条件接入模块(CAM)，其中该条件接入模块(CAM)通过一个相应的秘密密钥对该第一加密报文解密，以获得所述随机密钥（Ci），其中所述随机密钥被用于加密和解密所述设备之间的传输。

10. 按照权利要求 9 的方法，其中在解密所述加密报文之后，所述条件接入模块（CAM）首先在带有认证的第二加密报文中把所述随机密钥（Ci）返回到所述解码器。11. 按照权利要求 10 的方法，其中为了提供所述认证，所述解码器进一步产生一个随机数（A），并且把该随机数（A）与所述随机密钥（Ci）一同在所述第一加密报文中传送到条件接入模块（CAM），其中该条件接入模块（CAM）使用所述随机数（A），用于在第二加密报文中的认证。

12. 按照权利要求 11 的方法，其中所述条件接入模块(CAM)用所述随机密钥（Ci）加密所述随机数（A），以获得所述第二加密密钥。13.收费电视系统的解码器，包括条件接入模块（4）及智能卡（5），所述条件接入模块包括用于生成随机密钥(C_i)的装置（8）、利用公开密钥加密方法在第一加密报文中加密所述密钥的装置（8）、传送所述第一加密报文到智能卡的装置（8），所述智能卡（5）包括用于接收与解密所述第一加密报文以获得所述随机密钥的装置（10）、用于在所述随机密钥下加密对条件接入模块的传输的装置（10），所述条件接入模块（4）具有解密从智能卡接收的所述传输的装置（8）。

14.按照权利要求13的解码器，其中所述智能卡包括用于在带有认证的第二加密报文中将所述随机密钥返回给条件接入模块的装置（10）。

15.按照权利要求8的解码器，其中条件接入模块（4）的所述生成装置（8）还生成包含在所述第一加密报文中的随机数，其中该智能卡（5）适应于采用所述随机数作为第二加密报文中的认证。

16.收费电视系统的解码器，包括条件接入模块（4）及智能卡（5），其中所述解码器包括用于生成随机密钥（Ci）的装置（6）、用于采用公开密钥加密方法在第一加密报文中加密所述密钥的装置（6）、用于传送所述第一加密报文到条件接入模块（4）的装置（6），所述条件接入模块包括用于接收与解密所述第一加密报文以获取所述随机密钥的装置（8）、用于在所述随机密钥下加密对解码器的传输的装置（8），所述解码器具有解密从条件接入模块接收的所述传输的装置（6）。

17.按照权利要求16的解码器，其中所述条件接入模块（4）包括用于在带有认证的第二加密报文中返回所述随机密钥给解码器的装置（8）。

18.按照权利要求17的解码器，其中解码器的所述生成装置（6）还生成包含在所述第一加密报文中的随机，数其中该条件接入模块（4）适应于利用所述随机数作为第二加密报文中的认证。

19. 一种在收费电视系统中提供安全通信的装置，该装置包括包含至少一个微处理器的第一设备，该第一设备包括：从第二设备接收第一报文的装置，该第一报文包括一个随机密钥并且使用公开密钥加密；通过相应的密钥来解密第一加密的报文以获得所述随机密钥的装置；在带有认证的第二加密报文中把所述随机密钥返回到所述第二设备的装置；以及把所述随机密钥用于所述第一设备和所述第二设备之间的加密传输中的装置。

20. 按照权利要求19的装置，其中所述第一设备包括：

与所述随机密钥一同接收在所述第一加密报文中的随机数的装置，以及

在该第二加密报文中使用所述随机数进行认证的装置。

21. 按照权利要求 20 的装置，其中所述第一设备包括使用所述随机密钥加密所述随机数以获得所述加密报文的装置。

22. 按照权利要求 19-21 中的任何一项所述的装置，其中所述第一设备是用于收费电视系统中的智能卡。

23. 按照权利要求 19-22 中的任何一项所述的装置，其中所述第一设备包括从第二设备接收包含加密的控制字的授权控制报文的装置、处理所接收的授权控制报文的装置、提取该控制字的装置、以及在用随机密钥加密的返回报文中把解密的控制字返回到第二设备的装置。

24. 一种提供安全通信的装置，该装置包括包含至少一个微处理器的第一设备，该第一设备包括：

产生随机密钥的装置；

用第二设备的公开密钥把所述随机密钥加密在第一报文中的装置；

把所述第一报文传送到第二设备的装置；

从第二设备接收第二加密报文，返回带有认证的所述随机密钥的装置；

验证该认证是否正确的装置；以及

如果该认证为正确，则使用所述随机密钥来解密从所述第二设备发送到所述第一设备的内容。

25. 按照权利要求 24 的装置，其中为了提供所述认证，所述第一设备被构造为：

产生一个随机数；以及

把该随机数与所述随机密钥一同在所述第一加密报文中传送到该第二设备。

26. 按照权利要求 25 的装置，其中所述第一设备被构造为使

用所述随机密钥来解密所述第二加密报文。

27. 按照权利要求 24-26 中的任何一项所述的装置，其中所述第一设备是在收费电视系统中的一个条件接入模块。

28. 按照权利要求 24-27 中的任何一项所述的装置，其中所述第一设备被构造为把包含加密的控制字的授权控制报文转发到第二设备；

从第二设备接收用随机密钥加密的包含该控制字的一个返回报文；以及

使用该随机密钥解密该返回报文。

29. 按照权利要求 28 的装置，其中第一设备进一步包括一个破密器，其被设置为使用该控制字对被加密的数字数据流进行破密。

在两个设备之间提供安全通信的方法及使用该方法的设备

技术领域

本发明涉及在两个设备之间，特别是在收费电视系统中所使用的设备之间，提供安全通信的方法。

背景技术

在收费电视系统中，各用户通常具有用于破密源分量信号的解码器，其中所述解码器包括用于解密权利控制报文及权利管理报文的条件接入模块及智能卡。为了防止将解码器的未授权操作用于破密源分量信号，例如防止在授权与未授权的智能卡之间转换是重要的。

EP－A－0428252公开了用于在两个设备之间提供安全通信的方法及这一方法在收费电视系统中的应用。在这一已知方法中，第二设备，即智能卡，的认证是由第一设备检验的。

US－A－5029207公开了用于在两个设备之间提供安全通信的方法及这一方法在收费电视系统中的应用。在这一已知方法中，在加密报文中将第一密钥从编码器传输给解码器，及解码器解密这一报文来获取第一密钥来解密节目信号。秘密的序列号用于加密与解密。从解码器到编码器没有传输。

发明内容

本发明旨在提供上述类型的方法，其中以这样的方式来配置诸如控制接入模块与智能卡或解码器与条件接入模块这两个设备之间的通信，使得授权与未授权的设备之间的转换是不可能的。

按照本发明，提供了一种方法，其中第一设备生成随机密钥（C_i）并在用公开密钥加密的第一报文中将所述密钥传送给第二设备，其中所述第二设备利用对应的秘密密钥解密该第一加密报文来获得所述随机密钥（C_i），其中所述随机密钥用于加密与解密从所述第二设备到所述

第一设备的进一步传输。

按照本发明，这一方法能应用在收费电视系统的解码器中，其中所述解码器包括条件接入模块及智能卡，其中应用所述方法来提供控制接入模块与智能卡之间或解码器与条件接入模块之间的安全通信。

公开密钥算法在1995年出版的Schneier，B.所著的“应用加密技术（Applied Cryptography）”，第二版，第4页中描述。并且进一步设计公开密钥算法，使得用于加密的密钥不同于用于解密的密钥。另外，该解密密钥不能够（至少在任何合理的时间段内）从该加密密钥计算而得出。该算法被称为“公开密钥算法”，因为该加密密钥可以被公开：任何人可以使用该加密密钥来加密一个报文，但是仅仅具有解密密钥的特定人可以解密该报文。在这些系统中，加密密钥通常被称为公开密钥，而解密密钥通常被称为秘密密钥。

上述教科书中还在第52页中讨论了认证的技术。认证使得报文的接收者可能确定该报文的来源；入侵者不能够伪装成另一个人而发送该报文。通常，用密码技术解决该认证问题。登录到主计算机的用户输入其密码，并且该主机确认该密码的正确性。该用户和主机都已知该密码，并且在该用户每次登录时，主机要求该用户输入密码。

本发明进一步提供用于收费电视系统的解码器，包括条件接入模块及智能卡，所述条件接入模块包括用于生成随机密钥（C_i）的装置、用于在使用公开密钥加密方法的第一加密报文中加密所述密钥的装置、用于将所述第一加密报文传送到智能卡的装置，所述智能卡包括用于接收与解密所述第一加密报文来获得所述随机密钥的装置、用于在所述随机密钥下加密对条件接入模块的传输的装置，所述条件接入模块具有解密来自该智能卡所接收的所述传输的装置。

在本发明的又一实施例中，所述解码器包括条件接入模块及智能卡，其中所述解码器包括用于生成随机密钥（C_i）的装置、用于在使用公开密钥加密方法的第一加密报文中加密所述密钥的装置、用于将所述第一加密报文传送到该条件接入模块的装置，所述条件接入模块包括用于接收及解密所述第一加密报文来获得所述随机密钥的装置、用于在所

述随机密钥下加密对解码器的传输的装置，所述解码器具有解码从条件接入模块接收的所述传输的装置。

附图说明

通过参照在其中说明应用在收费电视系统中的本发明的方法的实施例的附图，进一步说明本发明。

图 1 示出按照本发明的解码器的实施例的方框图。

图 2 示出本发明的方法的实施例的步骤序列。

具体实施方式

参见图 1，其中以非常示意性的方式示出了用于收费电视系统的解码器的方框图，其中按照诸如 Eurocrypt 标准用控制字扰频数字信息信号。在本实施例中，解码器包括解调器 1、信号分离器 2 及解压单元 3。解码器还包括条件接入模块或 CAM 4 及智能卡 5，后者能插入条件接入模块 4 的连接槽中。此外解码器还设置有用于配置与控制目的的微处理器 6。

条件接入模块 4 设置有破密器单元 7 及具有存储器 9 的微处理器 8。智能卡 5 包括具有存储器 11 的微处理器 10。

由于解码器的上述部件的操作不是本发明的一部分，将不详细描述这一操作。通常，解调器 1 所接收的信号为在 950 MH_z 与 2050 MH_z 之间的经过调制的数据流。解调器 1 的输出为提供给 CAM 4 的加密数字数据流，而假定已插入了授权的智能卡且用户有权接收节目，便允许破密器 7 破密这一加密数据流。信号分离器 2 分离破密后的数据流信号并由解压单元 3 将其解压及转换成原来的模拟音频与视频信号。

在收费电视系统中，破密所需的控制字是在用服务密钥加密的包含该控制字的所谓授权控制报文中传送给用户的。这一服务密钥是用诸如称作授权管理报文下载到智能卡 5 的存储器 11 中的。操作期间，CAM 4 将授权控制报文传送到智能卡 5 的微处理器 10，使得微处理器 10 能处理该授权控制报文并抽取控制字。此后，智能卡 5 将解密的控制字返回到 CAM 4，从而允许破密器 7 破密从解调器 1 接收的数字数据流。

为了防止结合 CAM 4 使用未授权的智能卡 5，提供 CAM 4 与智能

卡 5 之间的安全通信是重要的。按照本发明，采用了下述方法来提供这一安全通信。图 2 中示出这一方法的步骤。当将智能卡插入解码器中时，CAM 4 的微处理器 8 生成两个随机数 C_i 与 A。微处理器 8 在 CAM 4 的公开密钥下在第一报文中加密随机数 C_i 与 A。将这样得出的第一报文传送给智能卡 5 而微处理器 10 用 CAM 4 的秘密密钥解密这一第一报文。此后微处理器 10 返回第二报文给 CAM 4，所述第二报文为在用作密钥的数 C_i 下加密的随机数 A。CAM 4 的微处理器 8 解密这一第二报文并检验随机数 A 是否正确。假定随机数 A 是正确的，因此可以认为插入的智能卡 5 是授权的智能卡，这时 CAM 4 将包含加密的控制字的授权控制制报文提交给智能卡 5，后者以传统方式处理该授权控制报文并抽取该控制字。然而，在对 CAM 4 的返回报文中，智能卡将提交在密钥 C_i 下加密的所抽取的控制字，而这些加密的控制字则由微处理器 8 用相同的密钥 C_i 解密。一旦有人试图用其它智能卡替代插入的智能卡 5，例如通过从授权的智能卡 5 转换到非授权的智能卡，由于新的智能卡不知道密钥 C_i 而 CAM 4 立即觉察这一改变，从而 CAM 不再能破密包含控制字的返回报文。从而使破密单元 7 不能工作。

能以相同的方式利用上述方法来提供 CAM 4 与解码器之间的安全通信，其中遵守图 2 中所示的相同协议。

简言之，可以理解如果将新的 CAM 4 连接到其它解码器部件上，解码器的微处理器 6 将生成这两个随机数 C_i 与 A，并且在微处理器 6 解密了从 CAM 4 的微处理器 8 所接收的第二报文并检验出随机数 A 为正确的时，便立即在 CAM 4 与微处理器 6 之间的所有传输中使用密钥 C_i。

本发明不限于上述实施例而能在权利要求书的范围内以多种方式变化。作为另一实施例的示例，该 CAM（即破密器）可以是解码器的一部分。解码器这时会查问智能卡来证明它自己以获得智能卡与解码器之间的安全通信。

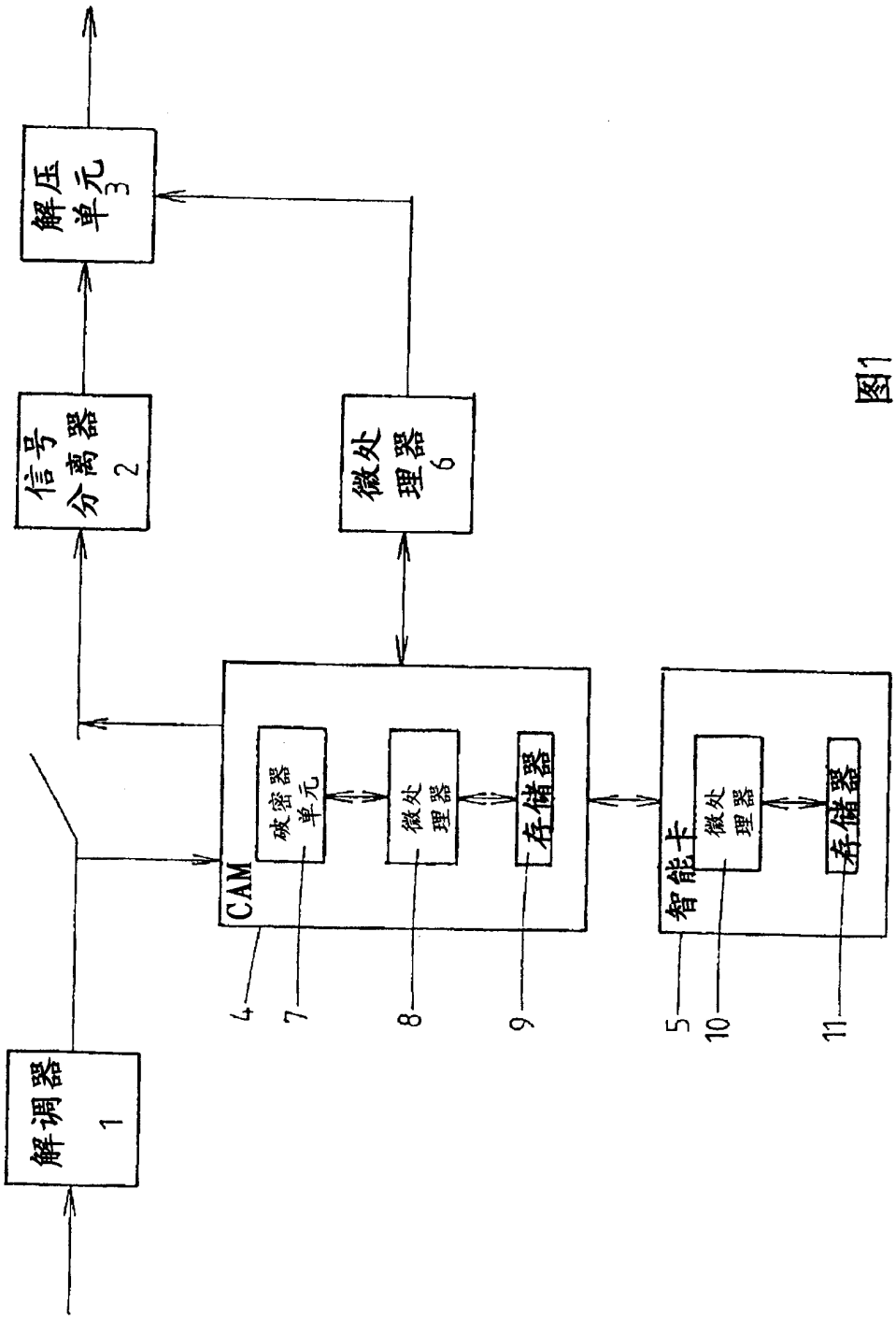

解调器
1
信号
分离器
2
解压
单元
3
微处
理器
6
CAM
破密器
单元
微处
理器
存储器
智能卡
微处
理器
存储器
4
7
8
9
5
10
11

图1

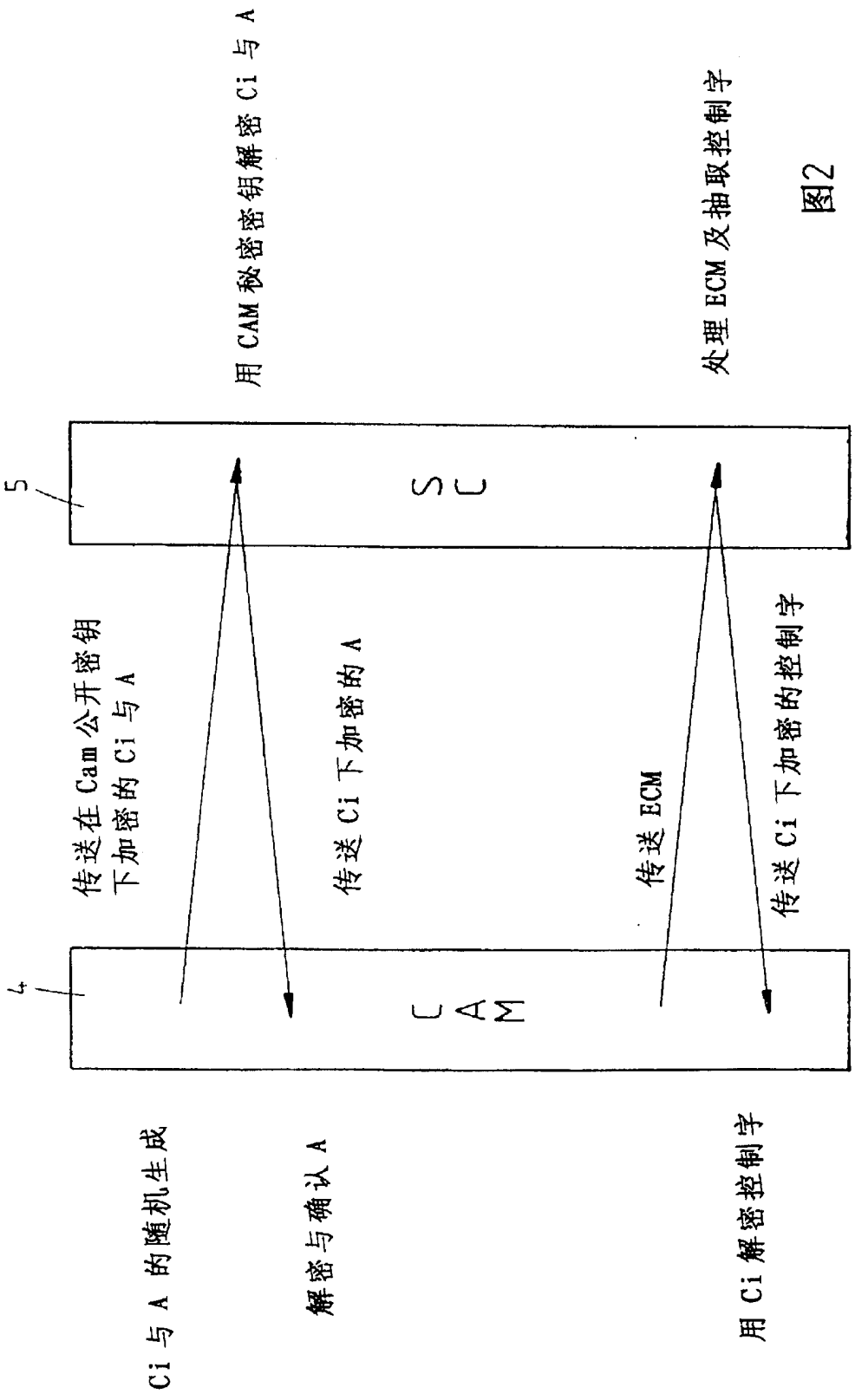

Ci 与 A 的随机生成
解密与确认 A
用 Ci 解密控制字
4
CAM
5
SC
传送在 Cam 公开密钥下加密的 Ci 与 A
传送 Ci 下加密的 A
传送 ECM
传送 Ci 下加密的控制字
用 CAM 秘密密钥解密 Ci 与 A
处理 ECM 及抽取控制字

图2