

(12) 发明专利申请

(10) 申请公布号 CN 102075802 A

(43) 申请公布日 2011.05.25

(21) 申请号 201010601052.6

(22) 申请日 2011.03.08

(71) 申请人 广东爱科数字科技有限公司

地址 510000 广东省广州市番禺区小谷围中
一路数字家庭孵化基地 B401

(72) 发明人 叶灿才 卢林发

(51) Int. Cl.

H04N 21/41 (2011.01)

H04N 21/418 (2011.01)

H04L 9/32 (2006.01)

H04L 9/30 (2006.01)

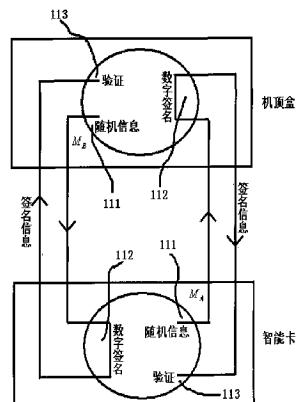
权利要求书 2 页 说明书 5 页 附图 4 页

(54) 发明名称

一种机顶盒和智能卡安全通信的方法

(57) 摘要

本发明公开了一种智能卡和机顶盒安全通信的方法，该方法包括：机顶盒和智能卡都拥有一对非对称密钥，机顶盒和智能卡相互配对。机顶盒和智能卡在交换控制字之前先互相进行身份验证，验证通过后交换的信息都采用对方的公钥进行加密再发送，接收方可以用自己的私钥进行解密。通过机顶盒和智能卡之间的相互认证机制，可以防止非法的机顶盒（或智能卡）与合法的智能卡（或机顶盒）进行通信交换密钥。机顶盒与智能卡的通信交换的信息加密处理，可以有效地防止智能卡和机顶盒间的连接被攻击，从而保证了交换过程的安全性。



1. 一种实现机顶盒和智能卡安全通信的方法,其特征在于,机顶盒和智能卡各具有一对非对称密钥,机顶盒和智能卡互相配对,记录对方公钥;

所述的安全通信的方法的包括如下步骤:

步骤一、所述的机顶盒和所述的智能卡先进行身份验证,所述的身份验证方法是采用互相认证机制,所述的身份验证采用向对方发送的随机信息,要求对方使用密钥进行数字签名,通过数字签名来验证对方身份;

步骤二、身份验证通过后,所述的机顶盒和所述的智能卡方才可进行解密控制字的解密通信过程;机顶盒和智能卡在执行所述的解密通信过程中,要向对方发送信息时,必须先采用对方密钥对息信进行加密后,再发送给对方,加密时采用非对称加密方式加密;

步骤三、所述的身份验证过程中的数字签名与步骤二所述的解密通信过程中的加密都使用非对称密钥执行,其所采用的算法为同一个算法体系,其所使用的非对称密钥都采用同一对非对称密钥,其运行时使用共同的装置。

2. 根据权利要求 1 所述的安全通信方法,其特征在于:所述的步骤一的身份验证采用互相验证机制,机顶盒对智能卡进行身份验证同时智能卡对机顶盒进行身份验证;所述的身份验证使数字签名的算法来执行,通过发送的随机信息,要求对方使用密钥进行数字签名来验证对方身份;所述的数字签名算法与所述的非对称加密算法使用同一算法体系并使用同一对非对称密钥;

所述的身份验证还包括以下流程:

步骤四、机顶盒产生随机信息 M_B ,发送给智能卡;智能卡产生随机信息 M_A 发送到机顶盒;

步骤五、智能卡使用自己的非对称密钥对 M_B 进行数字签名,返回给机顶盒;机顶盒使用自己的非对称密钥对 M_A 进行数字签名,返回给智能卡;

步骤六、机顶盒对智能卡返回的数字签名进行验证;智能卡对机顶盒返回的数字签名进行验证。

3. 根据权利要求 1 所述的安全通信方法,其特征在于:步骤二所述的解密控制字的解密通信过程必须在相互身份验证通过后才会被执行;所述的解密通信过程必须先采用密钥对息信进行加密后,再发送给对方;所述的对息信进行加密都是采用非对称加密方法,用对方的公钥进行加密,解密时必须用到对应的私钥,所述的非对称加密算法和所述的数字签名算法使用同一算法体系并使用同一对非对称密钥;

所述的解密控制字的解密通信过程还包括如下的步骤:

步骤七、机顶盒先释出前端加密的控制字 CW_1 ;

步骤八、机顶盒使用智能卡的公钥将 CW_1 加密为 CW_2 ,将 CW_2 发送到智能卡中;

步骤九、智能卡使用私钥从 CW_2 解密出 CW_1 ;

步骤十、智能卡使用 CA 系统的解密算法从 CW_1 中解密出原始的控制字 CW ;

步骤十一、智能卡使用机顶盒的公钥将 CW 加密为 CW_3 ,并将 CW_3 发送机顶盒中;

步骤十二、机顶盒使用自己的私钥将 CW_3 解密为 CW ;

步骤十三、机顶盒的解扰器用 CW 解扰出原始节目流。

4. 根据权利要求 1、2、3 所述的安全通信方法,其特征在于:所述的数字签名与所述的非对称加密都使用非对称密钥执行,其所采用的算法都为同一个算法体系,其所使用的非

对称密钥都采用同一对非对称密钥,其运行时使用共同的装置。

一种机顶盒和智能卡安全通信的方法

技术领域

[0001] 本发明涉及数字家庭通讯技术,尤其涉及机顶盒和智能卡之间安全通信和密钥交换领域。

背景技术

[0002] 数字电视条件接收 (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。其基本目的是运营商在电视系统中对用户进行授权管理,从而实现数字电视的有偿服务。

[0003] 现在的数字电视条件接收系统主要是基于欧洲的 DVB 标准,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,称为控制字 (CW)。条件接收系统负责对 CW 进行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。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。现在的条件接收系统接收端采用智能卡,解密算法存放在智能卡中,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,再通过接收端的 CA 模块传到解扰器中。

[0004] 条件接收系统中有两个引起广泛关注的安全问题:

[0005] 一:机顶盒和智能卡之间的连接对于攻击是非常脆弱的。如果智能卡将解密出的控制字 CW 以明文的形式传送给机顶盒,攻击者可以通过监测智能卡与机顶盒之间的通信获得控制字,然后通过网络将控制字发给未授权用户,使得他们能够免费收看节目。

[0006] 二:互相认证机制的缺乏。这将允许一个伪造的机顶盒(例如带黑客智能卡读卡器的计算机)从智能卡中获得控制字,为盗版提供可能;或者一张伪造的智能卡在机顶盒中使用访问受保护的内容。

[0007] 在信息安全领域,有一个非对称密钥加密法。非对称密钥加密法是一种使用一对非对称密钥的非对称加密手段。公钥用于加密,私钥用于解密。公钥可以让所有人知道,而私钥却必须保密。想从公钥推导出私钥在计算上是不可行的。拥有公钥的人可以加密信息却不能将其解密,只有拥有对应私钥的人才能解密信息。非对称加密法的算法体系可以修改成数字签名算法,从而应用于数字签名领域。

发明内容

[0008] 本发明旨在解决条件接收 (CA) 系统在解密控制字过程中的安全问题,提出一种采用密钥控制的机顶盒和智能卡的安全通信方法。为防止使用仿冒的机顶盒或智能卡的接入,本发明加入了机顶盒和智能卡的相互身份验证机制,为防止机顶盒和智能卡之间的连接被攻击,防止非法用户在终端在解密控制字的解密通信过程中截取控制字,本发明的智能卡和机顶盒之间交换的通信信息都是先经过加密,再进行通信交换,从而保证了信息的安全性。

[0009] 本发明的相互身份验证过程采用了经过个修改的数字签名算法,将数字签名的算

法应用于机顶盒和智能卡的身份验证领域。本发明解密控制字的解密通信过程对通信信息的加密采用修改的非对称加密算法体系，将非对称加密算法应用于机顶盒和智能卡的安全通信领域。本发明的数字签名算法和非对称加密算法使用同一个密钥算法体体系，使得本发明在实施时能使用相同的一对非对称，使用相同的算法装置，从而在实施时更加简单容易。

[0010] 本发明通过下述技术方案实现：

[0011] 机顶盒在生产时分配一对非对称密钥，包括公钥和私钥，所述的非对称密的公钥对外公开，私钥保密。

[0012] 智能卡在生产时分配一对非对称密钥，包括公钥和私钥，所述的非对称密的公钥对外公开，私钥保密。

[0013] 在使用安装时广播运营商将所述的机顶盒和智能卡进行互相配对，记录对方的公钥。

[0014] 本发明的技术方案包括以下主要流程：

[0015] 110 机顶盒和智能卡进行身份验证，所述的身份验证采用互相认证机制；身份验证时向对方发送的随机信息，要求对方使用密钥进行数字签名，用用对方公钥和数字签名的结果来验证对方身份；

[0016] 120 步骤 101 所述的身份验证通过后，机顶盒和智能卡方可进行解密控制字的解密通信过程，解密通信过程必须先采用密钥对息信进行加密后，再发送给对方；

[0017] 所述的主要流程的 110 步骤（身份验证）采用互相认证机制。在用户收看节目时，智能卡和机顶盒必须先进行身份互相认证，即机顶盒对智能卡进行身份验证，同时智能卡对机顶盒进行身份验证。所述的身份验证使数字签名的算法来执行，将数字签名的算法应用于机顶盒和智能卡的身份验证领域。身份验证过程通过向对方发送随机信息，要求对方使用密钥进行数字签名，用对方公钥和数字签名的结果来验证对方身份。认证通过后才进行解密控制字的解密通信过程。

[0018] 所述的身份认证步骤如下：

[0019] 111 机顶盒产生随机信息 M_B ，发送给智能卡；智能卡产生随机信息 M_A ，发送到机顶盒；

[0020] 112 智能卡使用自己的密钥对 M_B 进行数字签名，返回给机顶盒；机顶盒使用自己的密钥对 M_A 进行数字签名，返回给智能卡；

[0021] 113 机顶盒使用智能卡公钥对智能卡返回的数字签名进行验证；智能卡使用机顶盒的公钥对机顶盒返回的数字签名进行验证。

[0022] 身份认证通过后机顶盒和智能卡才会执行解密控制字的 120 步骤解密控制字的解密通信过程。解密通信过程必须先采用密钥对息信进行加密后，再发送给对方。解密控制字的解密通信过程对通信信息的加密采用修改过的非对称加密算法，将非对称加密算法应用于机顶盒和智能卡的安全通信领域。解密通信过程，用对方的公钥进行加密，解密时必须用到对应的私钥。

[0023] 解密控制字的解密通信过程的步骤如下：

[0024] 121 机顶盒从信号源释出前端加密的控制字 CW_1 。

[0025] 122 机顶盒使用智能卡公钥对前端加密控制字 CW_1 再次加密为 CW_2 ，然后将 CW_2 发

送到智能卡

- [0026] 123 智能卡先用私钥从 CW_2 中解密出前端加密控制字 CW_1 。
- [0027] 124 智能卡使用 (CA) 系统的解密算法从前端加密控制字 CW_1 中解密出原始明码控制字 CW 。
- [0028] 125 智能卡使用机顶盒的公钥将原始明码控制字 CW 加密为 CW_3 , 再将 CW_3 发送回机顶盒中。
- [0029] 126 机顶盒使用私钥从 CW_3 解密出原始明码控制字 CW 。
- [0030] 127 机顶盒的解扰器用 CW 解扰节目流。
- [0031] 所述的身份认证过程使用的数字签名和所述的解密通信过程使用非对称加密都通过非对称密钥执行, 其所采用的算法为同一个算法体系。即从一个算法体系扩展修改形成的适用于机顶盒和智能卡之间安全通信领域的, 用于相互身份验证的数字签名算法和用于相互安全通信的非对称加密算法。因此, 其所使用的非对称密钥可以采用同一对非对称密钥, 其运行时可以使用共同的装置。
- [0032] 通过本发明, 可以保证在智能卡与机顶盒之间的控制字信息安全地交换。通过机顶盒和智能卡之间的相互认证机制, 可以防止伪造的机顶盒(或智能卡)与合法的智能卡(或机顶盒)进行通信交换密钥, 防止非法人员使用非法的机顶盒或智能卡(带有黑客功能)进行破解。同时机顶盒与智能卡的通信信息都经过加密处理, 可以有效地防止智能卡和机顶盒间的连接被攻击, 即使交换的信息被非法导出也能保证安全, 从而保证了控制字交换的安全性。
- [0033] 本发明的身份认证过程的数字签名算法和解密通信过程的非对称加密算法使用同一个钥匙密算法体系, 因而可以使同一对密钥, 并且可以使用共同的装置, 从而在生产实施时更为方便且节约成本。
- [0034] 本发明使用非对称密钥算法, 并且同时为机顶盒和智能卡都分配了密钥以识别, 机顶盒和智能卡的密钥无需在生时互通信息, 可以分别由不同的生产商进行生产分配, 符合机卡分离标准, 利于机顶盒和智能卡的批量规模生产。

附图说明

- [0035] 图 1 : 身份验证示意图 ;
- [0036] 图 2 : 解密通信示意图 ;
- [0037] 图 3 : 实施例身份验证示意图 ;
- [0038] 图 4 : 实施例解密通信示意图。

具体实施方式

- [0039] 下面将给出本发明的具体实施例和附图, 以便对本发明作进一步的说明。
- [0040] 本实施方式采用 ELGama1 算法密码体制, ELGama1 算法是基于求解离散对数问题的困难性来保证安全的, 普遍认为其具有可靠的安全性, 而且 ELGama1 算法有广泛的应用。
- [0041] 本实施方式通过如下技术方案实现 :
- [0042] 首先, 机顶盒在生产制造时分配一对非对称密钥, 包括公钥 Y_A , g_A , p_A 和私钥 X_A , 所述的非对称密的公钥对外公开, 私钥保密。

- [0043] 密钥按如下方法产生：
- [0044] 先选定一个足够大的素数 p_A 和 $GF(p_A)$ 上的本原元素 g_A , 再选取定一个随机数作为私钥 X_A ,
- [0045] 计算 : $Y_A = g_A^{X_A} \bmod p$
- [0046] 则 Y_A, g_A, p_A 作为公钥对外公布, X_A 作为私钥保密
- [0047] 智能卡在生产制造时也分配一对非对称密钥, 公钥 Y_B, g_B, p_B 对外公布, 私钥 X_B 保密
- [0048] 其中 : $Y_B = g_B^{X_B} \bmod p_B$
- [0049] 安装用户端时机顶盒和智能卡配对, 机顶盒记录智能卡的公钥 Y_B, g_B, p_B , 智能卡记录机顶盒的公钥 Y_A, g_A, p_A
- [0050] 210. 机顶盒和智能卡在执行解密控制字的解密通信过程之前, 必须先进行身份认证。认证通过后才执行行解密控制字的解密通信过程密钥交换通信。身份认证采用互相认证机制, 机顶盒对智能卡进行身份验证, 同时智能卡对机顶盒进行身份验证。
- [0051] 机顶盒和智能卡的身份验证步骤如下 :
- [0052] 211 机顶盒产生随机数 M_B 作为随机信息, 将 M_B 发送到智能卡中, 要求智能卡对其进行数字签名。智能卡产生随机数 M_A 作为随机信息发送到机顶盒中, 要求机顶盒对其进行数字签名。
- [0053] 212 智能卡对 M_B 进行数字签名, 签名方法如下 :
- [0054] 智能卡选择随机数 k_B 满足 $GCD(k_B, p_B - 1) = 1$
- [0055] 计算 $K_B = g_B^{k_B} \bmod p_B$ $S_B = [k_B^{-1} (M_B - X_B \square K_B)] \bmod (p_B - 1)$
- [0056] 则数字签名为 (K_B, S_B) , 返回 (K_B, S_B) 给机顶盒。
- [0057] 机顶盒对 M_A 进行数字签名 :
- [0058] 机顶盒产生随机数 k_A , 满足 $GCD(k_A, p_A - 1) = 1$
- [0059] 计算 $K_A = g_A^{k_A} \bmod p_A$, $S_A = [k_A^{-1} (M_A - X_A \square K_A)] \bmod (p_A - 1)$
- [0060] 则数字签名为 : (K_A, S_A) , 返回 (K_A, S_A) 给智能卡。
- [0061] 213 对数字签名进行验证 :
- [0062] 机顶盒计算等式 $Y_A^{K_A} K_A^{S_A} \bmod p_A = g_A^{M_A} \bmod p_A$ 两边的值, 若值相等则对智能卡验证通过, 否则不通过。
- [0063] 智能卡计算等式 $Y_B^{K_B} K_B^{S_B} \bmod p_B = g_B^{M_B} \bmod p_B$ 两边的值, 若值相等则对机顶盒验证通过, 否则不通过。
- [0064] 互相验认通过后机顶盒和智能卡才可以进行加密解密通信。
- [0065] 220. 身份认证通过后机顶盒和智能卡会执行解密控制字的解密通信过程。机顶盒和智能卡的通信信息都会先使用使用对方的公钥加密进行, 再发送给对方。
- [0066] 机顶盒和智能卡的解密控制字的解密通信过程的步骤好下 :
- [0067] 221 机顶盒从信号源释出前端加密的控制字 CW_1 。
- [0068] 222 机顶盒使用随机数 x_1 和智能卡的公钥 Y_B, g_B, p_B 加密 CW_1 得到 CW_2 即 (C_1, C_2) , 将 CW_2 发送到机顶盒中。
- [0069] 其中加密方法为 : $C_1 = g_B^{x_1} \bmod p_B$ $C_2 = Y_B^{x_1} \square CW_1 \bmod p_B$

[0070] 223 智能卡收到 CW₂ 后使用私钥解密出 CW₁, 解密算法如下：

[0071]

$$CW_1 = C_1^{-x_B} \square C_2 \bmod p_B$$

[0072] 224 智能卡再使用 CA 系统的解密算法从 CW₁ 中解密出原始的控制字 CW

[0073] 225 智能卡使用随机数 x₂ 和机顶盒的公钥 Y_A, g_A, p_A 加密 CW 得到 CW₃ 即 (D₁, D₂), 并将 CW₃ 发送机顶盒中。其中：

$$D_1 = g_A^{x_2} \bmod p_A, D_2 = Y_A^{x_2} \square CW \bmod p_A$$

[0075] 226 机顶盒收到 CW₃ 后, 使用自己的私钥进行解密, 得到 CW。其中解密算法如下：

$$CW = D_1^{-x_A} \square D_2 \bmod p_A$$

[0076] 227 机顶盒的解扰器再用 CW 解扰节目流。

[0077] 上述实施例是供本领域普通技术人员实现和使用本发明的, 本领域的普通技术人员可以在不脱离本发明的发明思想的情况下, 对实施例作出种种变化。因而本发明的保护范围不应受实施例所限, 而应该是符合权利要求书提到的新颖性特征的最大范围。

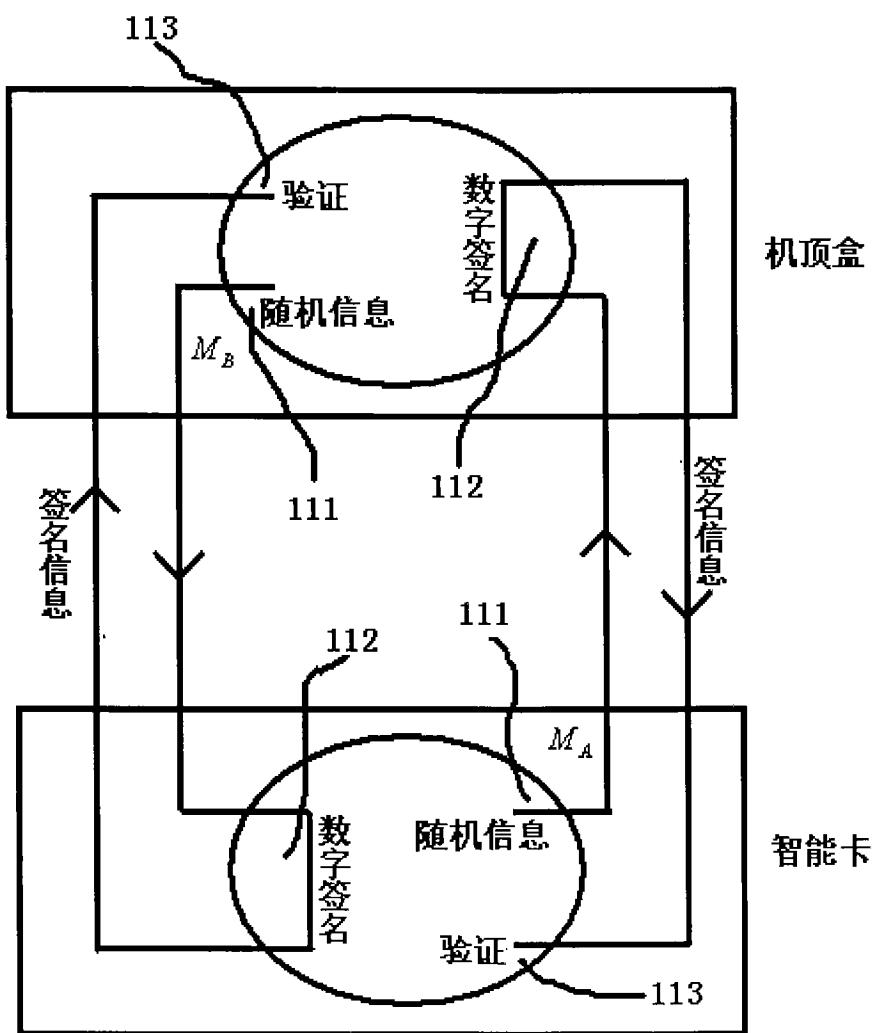


图 1

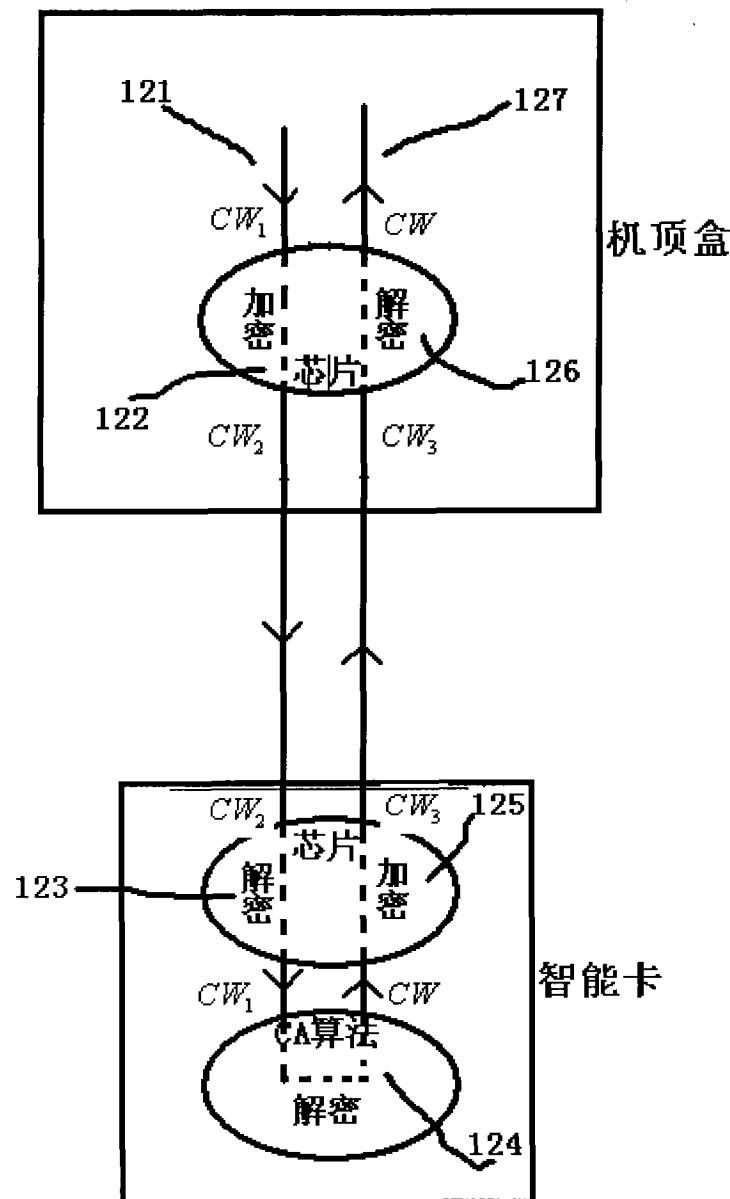


图 2

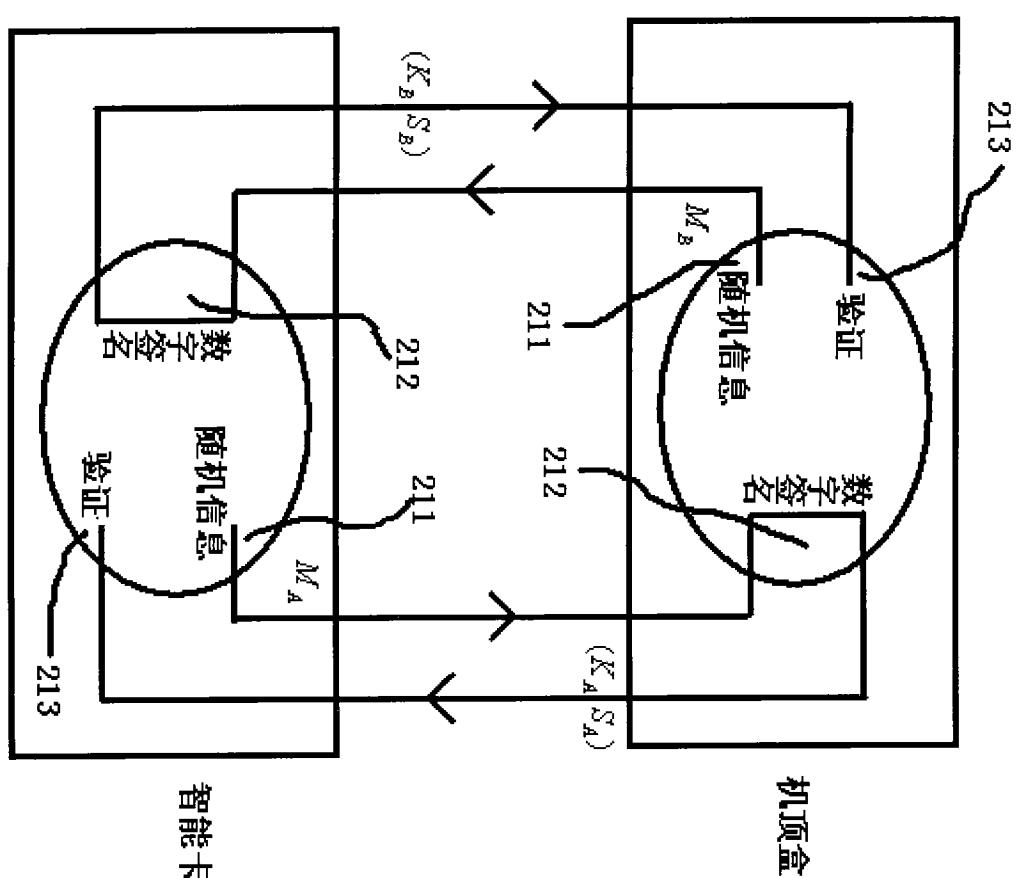


图 3

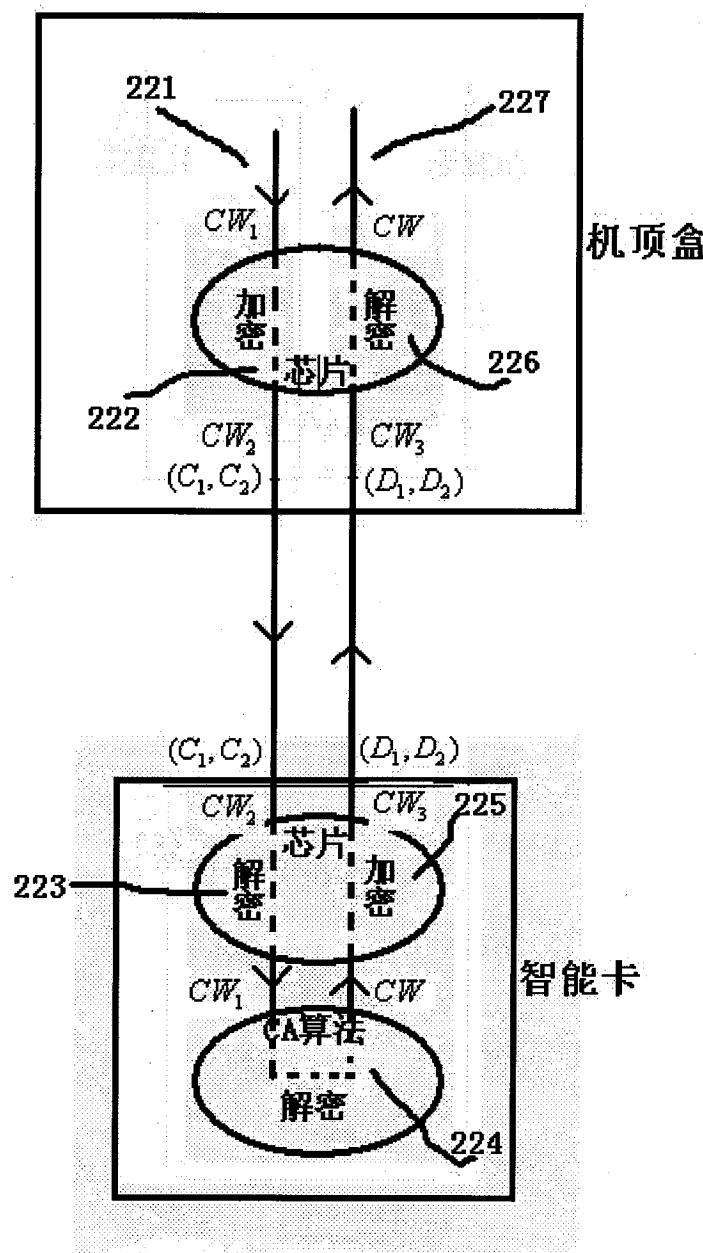


图 4