[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200510080573.0

[43] 公开日 2007 年 1 月 3 日

[11] 公开号 CN 1889420A

[22] 申请日 2005.6.30
[21] 申请号 200510080573.0
[71] 申请人 联想（北京）有限公司
地址 100085 北京市海淀区上地信息产业基地创业路 6 号
[72] 发明人 刘永华

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 王 琦 程殿军

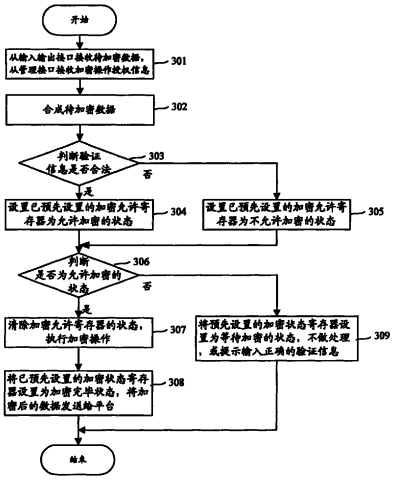
权利要求书 3 页 说明书 10 页 附图 2 页

[54] 发明名称

一种实现加密的方法

[57] 摘要

本发明公开了一种实现加密的方法，关键是，加密装置接收来自输入输出接口的待加密数据，以及来自管理接口的加密操作授权信息后，获取正确且完整的待加密数据，之后，对待加密数据执行加密操作，并将加密后的信息传送给平台。 应用本发明，防止了冒充签名或篡改签名内容的情况。 本发明可以广泛用于银行、证券相关的网上交易系统、电子支付密码系统，以及公文电子签章、邮件签名系统等。 其对于加密装置的持有人和加密信息的接收方都是安全可信赖的。



1、一种实现加密的方法，用于具有输入输出接口及管理接口的加密装置进行加密的情况，其特征在于，该方法包括以下步骤：

加密装置接收来自输入输出接口的待加密数据，以及来自管理接口的加密操作授权信息后，获取正确且完整的待加密数据，之后，对待加密数据执行加密操作，并将加密后的信息传送给平台。

2、根据权利要求 1 所述的方法，其特征在于，所述来自输入输出接口的待加密数据为完整的待加密数据，所述来自管理接口的加密操作授权信息为根据安全需求设置的约束条件；

所述获取正确且完整的待加密数据的过程包括以下步骤：

根据预设的格式要求判断待加密数据是否在约束条件所约束的范围之内，如果是，则来自输入输出接口的待加密数据为正确且完整的待加密数据，否则不做处理或提示输入正确的待加密数据。

3、根据权利要求 1 所述的方法，其特征在于，所述来自输入输出接口的待加密数据为部分待加密数据，所述来自管理接口的加密操作授权信息为待加密数据要素；

所述获取正确且完整的待加密数据的过程包括以下步骤：

从加密操作授权信息中提取出待加密数据要素，将该待加密数据要素与接收到的部分待加密数据进行组合，所合成完整的待加密数据为正确且完整的待加密数据。

4、根据权利要求 1 所述的方法，其特征在于，所述来自输入输出接口的待加密数据为部分待加密数据，所述来自管理接口的加密操作授权信息为根据安全需求设置的约束条件以及待加密数据要素；

所述获取正确且完整的待加密数据的过程包括以下步骤：

从加密操作授权信息中提取出待加密数据要素，将该待加密数据要素与接收到的部分待加密数据进行组合，合成完整的待加密数据；然后根据预设的格

式要求判断待加密数据是否在约束条件所约束的范围之内，如果是，则获得正确且完整的待加密数据，否则不做处理或提示输入正确的待加密数据。

5、根据权利要求 3 或 4 所述的方法，其特征在于，所述从加密操作授权信息中提取出待加密数据要素后，进一步包括：将待加密数据要素转换为显示装置所要求的格式后，通过管理接口输出到外部已设置的显示装置；

在加密装置接收到的来自管理接口的验证信息后，再执行加密操作；

所述外部的显示装置为显示器或打印机或扬声器，或者所述三者的任意组合。

6、根据权利要求 2 或 3 或 4 所述的方法，其特征在于，

所述获取正确且完整的待加密数据后，进一步包括：将完整的待加密数据转换为显示装置所要求的格式后，通过管理接口输出到外部已设置的显示装置，在加密装置接收到的来自管理接口的验证信息后，再执行加密操作；所述外部的显示装置为显示器或打印机或扬声器，或者所述三者的任意组合。

7、根据权利要求 1 所述的方法，其特征在于，进一步包括：所述加密装置接收来自输入输出接口的个人身份码 PIN 码，判断该 PIN 码与自身预先保存的 PIN 码是否一致，如一致加密装置再接收来自输入输出接口的待加密数据，否则不做处理或提示输入正确的 PIN 码。

8、根据权利要求 2、3 或 4 所述的方法，其特征在于，进一步包括：加密装置接收来自管理接口的验证信息，

当加密装置获取正确且完整的待加密数据后，进一步包括：

加密装置判断接收到的来自管理接口的验证信息是否合法，如果合法，则执行加密操作，加密操作完成后将加密后的数据传送给平台，否则不做处理或提示输入正确的验证信息。

9、根据权利要求 8 所述的方法，其特征在于，

所述验证信息为电平信号；

所述判断加验证信息是否合法的过程为：判断接收到的电平信号是否为预设的高电平或低电平，如果是，则该加密操作授权信息合法，否则不合法。

10、根据权利要求 8 所述的方法，其特征在于，

所述验证信息为字符串；

所述判断验证信息是否合法的过程为：判断接收到的字符串与自身预先保存的字符串是否相同，如果相同，则该验证信息合法，否则不合法。

11、根据权利要求 8 所述的方法，其特征在于，所述验证信息是否合法，由预先设置的用于表示验证信息是否合法的标志位的状态来指示，所述加密操作是否完毕，由用于表示加密操作是否完毕的标志位的状态来指示。

12、根据权利要求 11 所述的方法，其特征在于，所述用于表示验证信息是否合法的标志位和用于表示加密操作是否完毕的标志位的不同状态由两个的寄存器的不同状态来表示。

一种实现加密的方法

技术领域

本发明涉及信息安全技术领域，特别是指适用于具有输入输出接口、执行单元以及管理接口的加密装置，实现加密的方法。

背景技术

现今社会中，网络非常普及，为以下叙述方便，先对几个术语进行描述。

“平台”，包括包含数据处理能力装置的任何产品，其中包含数据处理能力装置可以是一个或多个封装或者未封装的集成电路。各种类型平台的实例包括但不局限于或限定于计算机，例如：个人数字助理、笔记本、台式机、工作站、服务器；任何与计算机关联的外围设备，例如：打印机、数码相机、数码摄像机；无线通信装置，例如：电话手机、智能手机；网络终端，例如：ATM 机、POS 机、KIOSK 信息查询终端；电视机机顶盒等。

“链路”被广泛地定义为逻辑的或者物理通信的通道，例如：电线、光纤、线缆、总线（如：USB 接口、1394 接口、串行通讯口、并行打印口、内部 LPC）、PS2 接口、硬盘接口(ATAPI、SATA\SCSI)，红外线/蓝牙/Zigbee/WLAN、射频（RF）或者其它任何无线信令机构的无线信道。

“公共网络环境”，其泛指处于与其它平台存在不可信赖“链路”的情形，包括但不限于局域网络，如：公司内部的以太网络、网吧网络等；因特网，如家用电脑拨号上网、ADSL/LAN/Cable 上网等；手机网络，如 GPRS/CDMA/3G 等；以及平台的蓝牙/WLAN 装置打开的时候。

随着网络、电子商务的普及，推动了电子加密装置及系统的多样化，如电子公文流转相关的电子印章，网络支付相关的专业版证书等。其中，“公共网络环境”中的“平台”上，使用的电子签名装置在关键技术方面，主要

集中于带 CPU 的智能卡。基于 CPU 的智能卡，通常完美地支持公开密钥基础设施（PKI）技术，其安全性得到了广泛的认可和肯定。另外，在电脑内的安全芯片（TPM）也具有与智能卡类似的功能。在此，将所有具有基于 CPU 智能卡或 TPM 的芯片统称为加密装置。

现有的加密装置通常有两种结构，参见图 1 和图 2。

图 1 所示为现有的一种加密装置的结构示意图。该加密装置中至少包括输入输出接口 101 和执行单元 102。其中，输入输出接口 101 是加密装置与平台之间的接口，用于接收来自平台的待加密数据，并将该待加密数据传输给执行单元 102；或者，接收来自执行单元 102 的加密后的数据，将该加密后的数据传送给平台；执行单元 102 则用来对接收到的数据进行加密操作。执行单元内通常包括算法引擎、存储器、密钥生成单元和具有 RAM 空间的核心处理单元。当然，输入输出接口 101 还可以接收来自平台的个人身份码（PIN 码），并将该 PIN 码传送给执行单元 102，执行单元 102 会首先验证该 PIN 码是否合法，如果是，再对接收到的待加密数据进行加密操作，否则不做处理或提示输入正确的 PIN 码。

例如，日常经常用到的 USBKey，以及公开号为“CN1509546A”，发明名称为“一种用于安全发送授权数据的平台和方法”的中国专利申请中所提到的 TPM，就是利用图 1 所示装置的具体实现方式。

应用图 1 所示装置执行加密操作时，所有的控制环节均是在平台上完成，而在现有的公共网络环境中，网络中的黑客可以远程监控或记录你在平台上面的一切行为，比如：按键输入、手写输入、语音输入、屏幕显示，以及平台与加密装置之间的所有通信过程；黑客也有可能远程暗中操作或使用你的平台。可见，由于签名操作即加密操作的控制都是在平台完成，在加密装置与平台相连的期间，也就是加密装置插入平台的期间，可能出现冒充用户签名或篡改用户签名内容的情况。

图 2 所示为现有的另一种加密装置的结构示意图，该加密装置中至少包括输入输出接口 101、执行单元 102 和管理接口 201。该装置中的输入输出

接口 101、执行单元 102 的功能与图 1 所示装置完全相同，该装置中的管理接口 201 主要用于加密控制，即只有执行单元 102 接收到来自管理接口 201 的加密控制信息并验证该加密控制信息正确后，才执行加密操作，否则执行单元 102 不执行加密操作。该加密控制信息可以是指纹、或电平信号或密码等。例如，公开号为“CN2609069Y”，发明名称为“指纹数字签名器”的中国专利申请中 ，提出了将指纹传感器、指纹识别装置、加密装置和密钥发生器一体化的加密装置，其即是利用图 2 所示装置的一种实现方式。

应用图 2 所示装置执行加密操作时，虽然需要输入加密控制信息，加强了控制环节，但由于公共网络环境中的平台是不可信赖的，仍然可能出现冒充用户签名或篡改用户签名内容的情况。

另外，无论基于上述哪种加密装置，用户最多只能看到输入的信息，是不可能看到具体的待加密内容的，这样，就有可能在真正加密前，黑客将实际加密的内容进行掉包。由此可见，现有的加密方法都不能避免冒充签名或篡改签名内容的情况。而目前还没有解决冒充签名或者篡改签名内容的方法。

发明内容

有鉴于此，本发明的目的在于提供一种实现加密方法，以防止冒充签名或篡改签名内容的情况。

为达到上述目的，本发明的技术方案是这样实现的：

一种实现加密的方法，用于具有输入输出接口及管理接口的加密装置进行加密的情况，该方法包括以下步骤：

加密装置接收来自输入输出接口的待加密数据，以及来自管理接口的加密操作授权信息后，获取正确且完整的待加密数据，之后，对待加密数据执行加密操作，并将加密后的信息传送给平台。

较佳地，所述来自输入输出接口的待加密数据为完整的待加密数据，所述来自管理接口的加密操作授权信息为根据安全需求设置的约束条件；

所述获取正确且完整的待加密数据的过程包括以下步骤:

根据预设的格式要求判断待加密数据是否在约束条件所约束的范围之内,如果是,则来自输入输出接口的待加密数据为正确且完整的待加密数据,否则不做处理或提示输入正确的待加密数据。

较佳地,所述来自输入输出接口的待加密数据为部分待加密数据,所述来自管理接口的加密操作授权信息为待加密数据要素;

所述获取正确且完整的待加密数据的过程包括以下步骤:

从加密操作授权信息中提取出待加密数据要素,将该待加密数据要素与接收到的部分待加密数据进行组合,所合成完整的待加密数据为正确且完整的待加密数据。

较佳地,所述来自输入输出接口的待加密数据为部分待加密数据,所述来自管理接口的加密操作授权信息为根据安全需求设置的约束条件以及待加密数据要素;

所述获取正确且完整的待加密数据的过程包括以下步骤:

从加密操作授权信息中提取出待加密数据要素,将该待加密数据要素与接收到的部分待加密数据进行组合,合成完整的待加密数据;然后根据预设的格式要求判断待加密数据是否在约束条件所约束的范围之内,如果是,则获得正确且完整的待加密数据,否则不做处理或提示输入正确的待加密数据。

较佳地,所述从加密操作授权信息中提取出待加密数据要素后,进一步包括:将待加密数据要素转换为显示装置所要求的格式后,通过管理接口输出到外部已设置的显示装置;

在加密装置接收到的来自管理接口的验证信息后,再执行加密操作;

所述外部的显示装置为显示器或打印机或扬声器,或者所述三者的任意组合。

较佳地,所述获取正确且完整的待加密数据后,进一步包括:将完整的待加密数据转换为显示装置所要求的格式后,通过管理接口输出到外部已设

置的显示装置，在加密装置接收到的来自管理接口的验证信息后，再执行加密操作；所述外部的显示装置为显示器或打印机或扬声器，或者所述三者的任意组合。

较佳地，进一步包括：所述加密装置接收来自输入输出接口的个人身份码 PIN 码，判断该 PIN 码与自身预先保存的 PIN 码是否一致，如一致加密装置再接收来自输入输出接口的待加密数据，否则不做处理或提示输入正确的 PIN 码。

较佳地，进一步包括：加密装置接收来自管理接口的验证信息，

当加密装置获取正确且完整的待加密数据后，进一步包括：

加密装置判断接收到的来自管理接口的验证信息是否合法，如果合法，则执行加密操作，加密操作完成后将加密后的数据传送给平台，否则不做处理或提示输入正确的验证信息。

较佳地，所述验证信息为电平信号；

所述判断加验证信息是否合法的过程为：判断接收到的电平信号是否为预设的高电平或低电平，如果是，则该加密操作授权信息合法，否则不合法。

较佳地，所述验证信息为字符串；

所述判断验证信息是否合法的过程为：判断接收到的字符串与自身预先保存的字符串是否相同，如果相同，则该验证信息合法，否则不合法。

较佳地，所述验证信息是否合法，由预先设置的用于表示验证信息是否合法的标志位的状态来指示，所述加密操作是否完毕，由用于表示加密操作是否完毕的标志位的状态来指示。

较佳地，所述用于表示验证信息是否合法的标志位和用于表示加密操作是否完毕的标志位的不同状态由两个的寄存器的不同状态来表示。

本发明提供了一种实现加密的方法，关键是，加密装置接收来自输入输出接口的待加密数据，以及来自管理接口的加密操作授权信息后，获取正确且完整的待加密数据，之后，对待加密数据执行加密操作，并将加密后的信息传送给平台。应用本发明，防止了冒充签名或篡改签名内容的情况。

来自输入输出接口的待加密数据为是完整的待加密数据，来自管理接口的加密操作授权信息为根据安全需求设置的约束条件；或者，来自输入输出接口的待加密数据为部分待加密数据，来自管理接口的加密操作授权信息为待加密数据要素；或者，来自输入输出接口的待加密数据为部分待加密数据，来自管理接口的加密操作授权信息为根据安全需求设置的约束条件以及待加密数据要素；应用本发明，能够保证黑客不能通过平台篡改待加密数据内容，或能够及时地发现待加密数据被篡改的问题。

再有，在执行加密操作前，加密装置可以通过再次检查验证信息保证待加密数据的安全。

另外，在执行加密操作前，用户可以通过输出装置对待加密数据要素或完整的待加密数据再次验证，从而，更进一步地避免了冒充签名或篡改签名内容的情况。本发明可以广泛用于银行、证券相关的网上交易系统、电子支付密码系统，以及公文电子签章、邮件签名系统等，其对于加密装置的持有人和加密信息的接收方都是安全可信赖的。

附图说明

图 1 所示为现有的一种加密装置的结构示意图；

图 2 所示为现有的另一种加密装置的结构示意图；

图 3 所示为应用本发明的实现加密的流程示意图。

具体实施方式

下面结合附图及具体实施例对本发明再做进一步地详细说明。

图 3 所示为应用本发明的实现加密的流程示意图。

步骤 301，加密装置从输入输出接口接收部分待加密数据，从管理接口接收包含待加密数据要素的加密操作授权信息。上述部分待加密数据通常为明文。

步骤 302，加密装置内的执行单元从加密操作授权信息中提取待加密数

据要素，将该待加密数据要素与接收到的部分待加密数据组合，合成完整的待加密数据。

当然，在加密操作授权信息中可以进一步包括根据安全需求设置的约束条件，该约束条件包括但不限于数据的数值范围或某些特定的文本等，当加密装置内的执行单元根据预设的格式要求，确认加密操作授权信息中包含约束条件后，首先判断该待加密数据要素是否在约束条件所约束的范围之内，例如是否为约束条件所限定的数据范围和/或是否为约束条件所限定的文本等，如果是，再执行合成操作，从而合成完整的待加密数据，否则，不做处理或提示输入的该待加密数据要素有误，并结束。

步骤 303，接收来自管理接口的验证信息，并判断该验证信息是否合法，如果合法则执行步骤 304，否则执行步骤 305。

如果验证信息为电平信号，则判断验证信息是否合法的过程为：判断接收到的电平信号是否为预设的高电平或低电平，如果是，则该验证信息合法，否则不合法。

例如，在实际应用时，可预先设置一按钮，并设置该按钮按下的状态所产生的电平为验证信息，也就是说，当按钮被按下时，才允许执行步骤 304，这样，加密装置通过判断接收到的电平是否为预设的电平，即可知道按钮是否被按下。当然，在实际应用中需要添加一些防抖动的处理，避免摁一次，加密操作多于一次的问题。

如果所述验证信息为字符串，则判断验证信息是否合法的过程为：判断接收到的字符串与预先保存在在存储器内的字符串是否相同，如果相同，则该验证信息合法，否则不合法。当然，所述字符串是可以更改的。

例如，在实际应用时，可预先设置一密码输入装置，并在加密装置的存储器预设一密码，将该密码作为验证信息，也就是说，只有用户输入正确的密码后，才允许执行步骤 303，这样，加密装置通过判断接收到的密码是否与自身存储器中预先保存的密码是否一致，即可知道用户输入的密码是否正确。当然，在实际应用中会添加一些防抖动的处理，以避免匹配一次，加密

操作多于一次的问题。

步骤 304，设置已预先设置的用于表示验证信息是否合法的标志位为允许加密的状态，然后执行步骤 306。在本实施例中，该用于表示验证信息是否合法的标志位由寄存器来实现，即将该寄存器的状态设置为允许加密的状态，以下为叙述方便，将该寄存器称为加密允许寄存器。

步骤 305，设置已预先设置的加密允许寄存器的状态为不允许加密的状态，然后执行步骤 306。

步骤 306，加密装置检测加密允许寄存器的状态，判断是否为允许加密的状态，如果是，执行步骤 307，如果是不允许加密的状态，则执行步骤 309。

步骤 307，清除加密允许寄存器的状态，即将其设置为不允许加密的状态，执行加密操作。

该加密操作的算法可以是公开密码算法，如 RSA 算法，椭圆曲线算法，或是对称密码算法，如：DES 算法，AES 算法，或是杂凑算法，如：SHA1，HMAC，还可以是以上所有算法的任意组合，以上仅是举例，在实际应用中不限与此。另外，由于 SHA1 算法中没有密码，因此最好不要单独使用。

步骤 308，加密操作执行完毕后将已预先设置的用于表示加密操作是否完毕的标志位设置为加密完毕的状态，然后将加密后的数据传送给平台，结束。

在本实施例中，该用于表示加密操作是否完毕的标志位由另一寄存器来实现，即将该寄存器的状态设置为加密完毕的状态，以下为叙述方便，将该寄存器称为加密状态寄存器，结束。

步骤 309，将已预先设置的加密状态寄存器设置为等待加密的状态，之后，不做处理，或提示输入正确的验证信息。

也就是说，只要加密装置内的执行单元检测到加密允许寄存器的状态为允许加密，则将加密状态寄存器设置为不允许加密状态，之后进行加密操作，并在加密完成后将加密状态寄存器设置为加密完毕的状态；而只要加密装置内的执行单元检测到加密允许寄存器的状态为不允许加密的状态，则将加密

状态寄存器设置为等待加密的状态。

当然，在上述实现流程中也可以不设置任何标志位，只要加密装置内的执行单元检测出验证信息合法，就对接收到的待加密数据执行加密操作；只要检测到验证信息不合法，就不做处理，或提示输入正确的验证信息。同样地，加密操作结束后，即可直接结束，而不再设置寄存器的状态。

在上述实施例中，步骤 303 是可选的，也就是说，可以没有验证信息而在获得完整且正确的待加密数据后，直接对待加密数据进行加密操作，并继续执行后续操作。

在上述实施例中，从输入输出接口接收到的是部分待加密数据，从管理接口接收到的是包含待加密数据要素的加密操作授权信息，或者从管理接口接收到的是包含待加密数据要素以及约束条件的加密操作授权信息。当然，从输入输出接口接收到的也可以是完整的待加密数据，从管理接口接收到的加密操作授权信息仅仅是根据安全需要设置的约束条件。也既保证黑客不能通过平台篡改待加密数据内容，或能够及时发现待加密数据被篡改即可。

如果从输入输出接口接收到的是完整的待加密数据，从管理接口接收到的加密操作授权信息仅仅是根据安全需要设置的约束条件：则加密装置根据预设的格式要求直接判断完整的待加密数据是否在约束条件所约束的范围之内，如果是，则说明来自输入输出接口的待加密数据为正确且完整的待加密数据，可以对该待加密数据执行加密操作，否则不做处理或提示输入正确的待加密数据。

如果来自输入输出接口的待加密数据为部分待加密数据，来自管理接口的加密操作授权信息仅仅为待加密数据要素而不包括约束条件，则加密装置从加密操作授权信息中提取出待加密数据要素，将该待加密数据要素与接收到的部分待加密数据进行组合，所合成完整的待加密数据即为正确且完整的待加密数据。

另外，还可以存在以下两种情况：

情况 1：如果存在一个显示装置与加密装置的管理接口直接相连时，则

在步骤 302 中，从加密操作授权信息中提取出待加密数据要素后，进一步包括：在组合成完整的待加密数据之后，将待加密数据要素转换为显示装置所要求的格式后，通过管理接口输出到外部已设置的显示装置，由显示装置对待加密数据要素进行显示，然后再执行步骤 303；或者，在步骤 302 中合成完整的待加密数据后，进一步包括：将完整的待加密数据转换为显示装置所要求的格式后，通过管理接口输出到外部已设置的显示装置，由显示装置对完整的待加密数据进行显示，然后再执行步骤 303，这样做的好处是进一步保证了待加密数据的正确性。上述外部的显示装置为显示器或打印机或扬声器，或者所述三者的任意组合。

如果既存在约束条件，又需执行显示操作，则确定待加密数据在约束条件所要求的范围内后，再执行显示操作；如果确定待加密数据不在约束条件所要求的范围内，则不执行显示操作，或显示无效数据。

情况 2：在加密装置的存储器内可以预先设置有 PIN 码，加密装置首先接收来自输入输出接口的 PIN 码，并判断该 PIN 码与自身存储器内预先保存的 PIN 码是否一致，如果一致，再执行步骤 301，否则不做处理或提示输入正确的 PIN 码。

上述情况 1 和情况 2 可以分别单独存在于上述所有实施例中，也可以同时存在于上述所有实施例中。

本发明所述方法可以以硬件、固件、软件或其三者的任意组合来实现。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

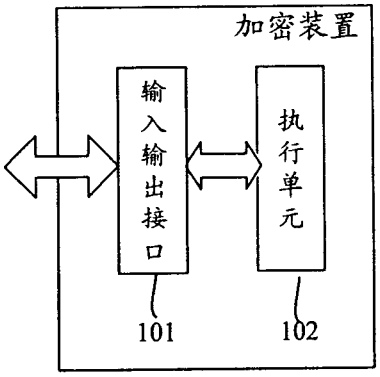


图 1

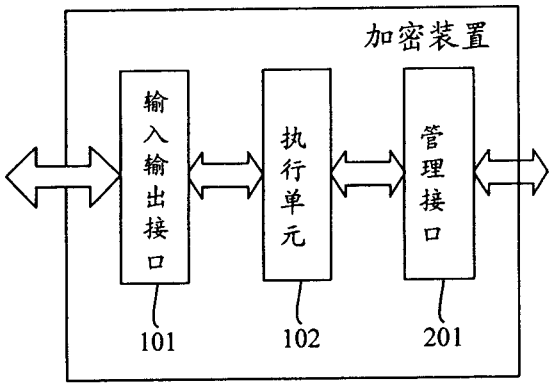


图 2

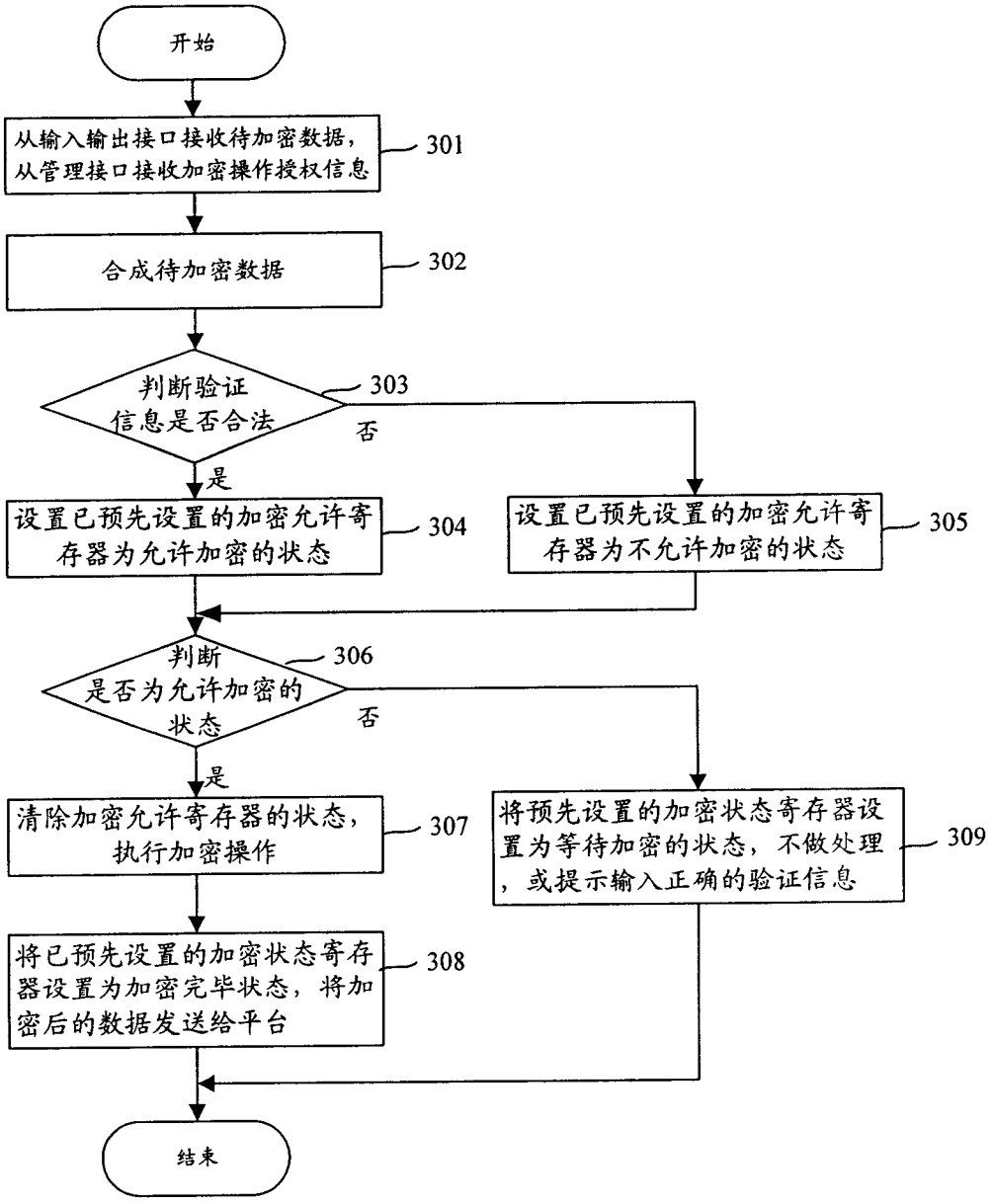

开始
从输入输出接口接收待加密数据，从管理接口接收加密操作授权信息
301
合成待加密数据
302
判断验证信息是否合法
303
否
是
设置已预先设置的加密允许寄存器为允许加密的状态
304
设置已预先设置的加密允许寄存器为不允许加密的状态
305
判断是否为允许加密的状态
306
否
是
清除加密允许寄存器的状态，执行加密操作
307
将预先设置的加密状态寄存器设置为等待加密的状态，不做处理，或提示输入正确的验证信息
309
将已预先设置的加密状态寄存器设置为加密完毕状态，将加密后的数据发送给平台
308
结束

图 3