

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200510125539.0

[43] 公开日 2006 年 12 月 27 日

[11] 公开号 CN 1885227A

[22] 申请日 2005.11.25

[21] 申请号 200510125539.0

[30] 优先权

[32] 2005. 6. 23 [33] JP [31] 2005 - 183465

[71] 申请人 株式会社东芝

地址 日本东京都

[72] 发明人 柳田将 江尻正仁

[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 李德山

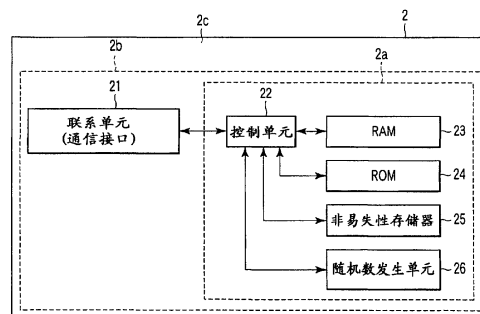
权利要求书 3 页 说明书 11 页 附图 5 页

[54] 发明名称

便携式电子设备及其数据输出方法

[57] 摘要

在 IC 卡(2)中,当对应于用于输出数据的命令的所有的处理被正常地执行时,监视标志的值在 IC 芯片(2a)的存储器中被设置为作为预定值的初始值。基于对应于用于输出数据的命令的各个处理的执行状态,设置监视标志的值。当先于数据输出的这些处理被完成时,要输出的数据根据监视标志的值被屏蔽,并且利用通信接口(21)输出该屏蔽的数据。



1.一种便携式电子设备，其特征在于包括：

设置单元，其在当从外部设备提供用来输出数据的命令时执行相应于该命令的所有处理的状态下设置作为预定值的监视信息的初始值；

改变监视信息的改变单元，该监视信息的初始值由设置单元基于所执行的处理来设置；

保护单元，其根据由改变单元基于所执行的处理而改变的监视信息来保护将被输出的数据；以及

输出单元，其将由保护单元所保护的数据输出给外部设备。

2.根据权利要求1的设备，其特征在于进一步包括：

包括设置单元、改变单元、保护单元、以及输出单元的模块，以及

模块隐藏于其中的外壳。

3.根据权利要求1的设备，其特征在于，

保护单元根据由改变单元基于所执行的处理而改变的监视信息，对要输出的数据执行预定计算处理，以及

输出单元将作为由保护单元执行的计算处理的结果所得到的数据输出到外部设备。

4.根据权利要求1的设备，其特征在于，根据任意数据以及由改变单元基于所执行的处理所改变的监视信息，保护单元保护将被输出的数据。

5.根据权利要求4的设备，其特征在于，

根据任意数据以及由改变单元基于所执行的处理所改变的监视信息，保护单元对要输出的数据执行预定计算处理，以及

输出单元将作为由保护单元执行的计算处理的结果所得到的数据输出到外部设备。

6.根据权利要求1的设备，其进一步地包括产生随机数数据的随

机数发生单元, 以及

其特征在于根据由改变单元基于所执行的处理所改变的监视信息, 以及由随机数数据生成单元所产生的随机数数据, 保护单元保护将被输出的数据。

7.根据权利要求6的设备, 其特征在于,

根据由改变单元基于所执行的处理所改变的监视信息, 以及由随机数数据生成单元所产生的随机数数据, 保护单元对要输出的数据执行预定计算处理, 以及

输出单元将作为由保护单元执行的计算处理的结果所得到的数据输出到外部设备。

8. 根据权利要求1的设备, 其进一步地包括其中存储对于便携式电子设备唯一的数据的存储器, 以及

其特征在于, 根据由改变单元基于所执行的处理所改变的监视信息, 以及存储在存储器中的该唯一数据, 保护单元保护将被输出的数据。

9.根据权利要求8的设备, 其特征在于,

根据由改变单元基于所执行的处理所改变的监视信息, 以及存储在存储器中的该唯一数据, 保护单元对要输出的数据执行预定计算处理, 并且输出单元将作为由保护单元所执行的计算处理的结果所得到的数据输出到外部设备。

10.根据权利要求1的设备, 其进一步地包括一存储器, 当输出单元输出数据时, 其存储被保护单元用于保护数据的监视信息, 以及

其特征在于, 根据由改变单元基于所执行的处理所改变的监视信息, 以及存储在存储器中的该监视信息, 保护单元保护将被输出的数据。

11.根据权利要求10的设备, 其特征在于,

根据由改变单元基于所执行的处理所改变的监视信息, 以及存储在存储器中的该监视信息, 保护单元对要输出的数据执行预定计算处理, 以及

输出单元将作为由保护单元执行的计算处理的结果所得到的数据输出到外部设备。

12.一种用于便携式电子设备的数据输出方法，其特征在于包括：
在当从外部设备提供用来输出数据的命令时执行相应于该命令的所有处理的状态下设置作为预定值的监视信息的初始值；

改变监视信息，该监视信息的初始值基于所执行的处理来设置；
根据基于所执行的处理而改变的监视信息来保护将被输出的数据；以及

将所保护的数据输出给外部设备。

13.根据权利要求12的方法，其特征在于保护将被输出的数据包括根据任意数据以及基于所执行的处理所改变的监视信息，保护将被输出的数据。

14.根据权利要求12的方法，其进一步地包括产生随机数数据，
以及

其特征在于，保护将被输出的数据包括根据基于所执行的处理所改变的监视信息，以及产生的随机数数据，保护将被输出的数据。

15.根据权利要求12的方法，其特征在于，

保护将被输出的数据包括保护将被输出的数据包括根据基于所执行的处理所改变的监视信息，以及对便携式电子设备唯一的数据，
保护将被输出的数据。

16.根据权利要求12的方法，其进一步包括存储当输出数据时用于保护数据的监视信息，以及

其特征在于，保护将被输出的数据包括根据基于所执行的处理所改变的监视信息，以及存储在存储器中的监视信息，保护将被输出的数据。

便携式电子设备及其数据输出方法

技术领域

本发明涉及诸如 IC 卡的便携式电子设备，包括与外部设备的通信接口，存储数据的存储器，用于执行处理程序的 CPU，并涉及用于便携式电子设备的数据输出方法。

背景技术

通常,在作为便携式电子设备的IC卡中，响应为读出数据而从外部设备发出的读出命令输出存储在存储器中的数据。在常规的IC卡中，当接收到来自外部设备的读出命令时，执行输出数据所需的各个步骤。此时，在IC卡中，监视标志监视输出数据所需的各个步骤的执行状态。因此，在IC卡中，在实际数据输出之前检查监视标志。当确定监视标志作为检查步骤的结果是正常时，数据从IC卡输出。如上所述，在常规的IC卡中，利用监视标志来监视处理内容。因此，在常规的IC卡中，禁止欺骗输出数据。

然而，打算从上述IC卡中窃取数据的带有恶意的人(欺骗性访问者)试图通过对IC卡进行各种攻击来破解(读出)IC卡中的数据。例如，欺骗性访问者有时通过给IC卡增加外部噪声来制造程序错误工作。在该情况下，在IC卡中，可以使上述处理中监视标志的检查功能失效，并且可以从IC卡中输出数据。即，在常规的IC卡中，当有人故意地通过增加外部噪声等等来制造程序错误工作时，内部数据可以被输出，因而造成了一个问题。

发明内容

本发明的目的是提供一个便携式电子设备，其可以通过保护要输出到外部设备的数据以具有高安全性而改善安全性，以及用于该便携式电子设备的控制方法。

根据本发明的一个方面，便携式电子设备包括：设置单元，其在

当从外部设备提供用来输出数据的命令时执行相应于该命令的所有处理的状态下设置作为预定值的监视信息的初始值；改变监视信息的改变单元，该监视信息的初始值由设置单元基于所执行的处理来设置；保护单元，其根据由改变单元基于所执行的处理而改变的监视信息来保护要输出的数据；以及输出单元，其将由保护单元所保护的数据输出给外部设备。

根据本发明的另一个方面，用于便携式电子设备的数据输出方法包括：在当从外部设备提供用来输出数据的命令时执行相应于该命令的所有处理的状态下设置作为预定值的监视信息的初始值；改变监视信息，该监视信息的初始值基于所执行的处理来设置；根据基于所执行的处理而改变的监视信息来保护要输出的数据；以及将所保护的数据输出给外部设备。

本发明的其它目的和优点将在随后的描述中阐明，并且部分地从描述中将会很清楚，或可由本发明的实施获悉。本发明的目的和优点可通过特别地在下文中所指出的手段和组合来实现并达到。

附图说明

并入并组成说明书的一部分的附图图解了本发明的实施例，并结合上面所给出的概述以及如下的实施例的具体实施方式，用来解释本发明的原理。

图1是一个方框图，根据本发明的实施例示意地显示了作为便携式电子设备的IC卡，以及作为与IC卡通信的外部设备的IC卡处理设备的结构例子；

图2是一个显示IC卡结构例子的方框图；

图3是用于解释当用于读出数据的读出命令被接收时的过程的流程图；

图4是用于解释当用于读出该数据的该读出命令被接收时的过程的流程图；

图5是一个流程图，用于解释图3以及4所示的过程的修改；以及

图6是一个流程图，用于解释图3以及4中所示过程的修改。

具体实施方式

下面将参考附图详细描述本发明的实施例。

图1是一个方框图，根据本发明的实施例，示意地显示了作为外部设备的终端系统1(IC卡处理设备)的结构例子，其具有与作为便携式电子设备的IC卡2通信的功能。

如图1所示，终端系统1包括终端设备11、显示设备12、键盘13、卡读取器/写入器14等。

终端设备11控制整个终端系统1的操作。终端设备11包括CPU、各种存储器、各种接口等。例如，终端设备11具有通过卡读取器/写入器14发送用于处理IC卡2的命令的功能，以及根据从IC卡2接收的数据执行各种处理的功能。

例如，终端设备11通过卡读取器/写入器14发送用来在IC卡2上写入数据的写入命令。当接收到写入命令时，IC卡2将数据写入IC卡2的存储器中。并且，终端设备11也通过卡读取器/写入器14发送用来从IC卡2读出数据的读出命令。当接收到读出命令时，存储在IC卡2的存储器中的数据被读出，并且读出的数据被送给终端设备11。

显示设备12是在终端设备11控制下显示各个类型的信息的显示设备。键盘13是由终端系统1的操作员操作的操作单元。该操作员利用键盘13输入各种操作指令及数据。卡读取器/写入器14是用来与IC卡2通信的接口设备。通过卡读取器/写入器14，可以对IC卡进行供电、时钟提供、复位控制、数据发送/接收等。即，卡读取器/写入器14在终端设备11的控制下激活IC卡2。卡读取器/写入器14发送各个命令给被激活的IC卡2，并接收针对所发送命令的响应。

当从诸如IC卡处理设备1的高阶设备接收供电时，IC卡2被激活(变成可操作的)。例如，当IC卡2与终端系统1按照接触通信方案通信时，即，当IC卡2是接触IC卡时，通过经由作为通信接口的接触单元21从IC卡处理设备1接收工作功供电电压和操作时钟来激活IC卡2。

当IC卡2利用非接触的通信方案与终端系统1通信时，即，当IC

卡2是非接触IC卡时，IC卡2的接触单元21包括作为通信接口的天线，通信控制单元等。在这种情况下，IC卡2经由包括在作为通信接口的接触单元21内的天线、通信控制单元等，接收来自IC卡处理设备的无线电波。IC卡2利用供电单元(未显示)由所接收的无线电波产生工作供电电压和操作时钟，并且被激活。

下面将描述IC卡2的结构例子。

图2是一个示意地显示IC卡2内部结构的方框图。如图2所示，IC卡2包括接触单元(通信接口) 21、控制单元22、RAM 23、ROM 24、非易失性存储器25等。例如，控制单元22、RAM 23、ROM 24、以及非易失性存储器25被包括在一个IC芯片2a中。更进一步地，IC芯片2a和通信接口21被集成为一个模块2b。模块2b被埋藏在IC卡2的外壳2c中。

接触单元21作为与终端系统的卡读取器/写入器14的通信接口。当IC卡2被作为接触IC卡实现时，接触单元21作为用于与终端系统1的卡读取器/写入器14接触地发送/接收信号的接口。当IC卡2被作为非接触IC卡实现时，接触单元21作为用于针对终端系统1的卡读取器/写入器14发送到/接收无线电波的接口。

控制单元22控制整个IC卡2的操作。控制单元22根据存储在ROM 24或非易失性存储器25中的处理程序进行操作。RAM 23是作为工作存储器的作用的易失性存储器。RAM 23作为暂时保存例如由控制单元22当前处理的数据的缓冲器。例如，RAM 23暂时地保存经由接触单元21接收自IC卡处理设备1的数据。

ROM 24是其中控制程序和控制数据被预先存储的非易失性存储器。ROM 24在IC卡2的制造阶段被并入IC卡2中。存储在ROM 24中的控制程序根据IC卡2的规格被预设置。

非易失性存储器25是诸如EEPROM或快擦写ROM、能写入/重写数据的非易失性存储器。在非易失性存储器25中，根据IC卡2的应用目的定义程序文件和数据文件，并且数据被写入指定文件中。另外，在非易失性存储器25中，存储用于认证IC卡的认证信息，或对于IC卡

唯一的数据。随机数发生单元26产生随机数数据。

下面将描述在具有上述结构的IC卡2中的处理。

图3和4是用于解释在IC卡2中的处理例子的流程图。

首先，终端系统1经由卡读取器/写入器14输出用于读出数据的读出命令到IC卡2。另一方面，IC卡2经由接触单元21接收来自终端系统1的读出命令(步骤S11)。当从终端系统1接收读出命令时，IC卡2的控制单元22响应所接收的命令设置(初始化)监视标志(监视信息)(步骤S12)。

监视标志是用来监视对应于所接收命令的处理的执行状态的信息。即，监视标志是用来识别是否已可靠执行对应于命令的各个处理的信息。在IC卡2的存储器中设置监视标志。例如，监视标志可被存储在控制单元22的内存储器(未显示)、RAM 23、或非易失性存储器25中。

当这个监视标志被初始化时，IC卡2的控制单元22根据所接收的命令顺序地执行各个处理，并根据这些处理的执行结果在预定定时设置监视标志(即，改变监视标志的值)(步骤S13到S20)。即，当根据所接收的读出命令的处理被正常地执行时，控制单元22根据设置监视标志的处理改变监视标志的值。

当完成先于数据输出(紧接在数据输出前)的各个处理时，监视标志的值(初始值)被如此设置，以便成为一个预定值("0")。在IC卡2中，根据所接收的命令确定要执行的各个处理(处理内容)。因此，根据所接收的命令的预定初始值被设置在监视标志中。根据所接收的命令预置用于设置监视标志的定时(处理检查点)。

图3和4示出了在加密和输出数据的情况下的一般处理内容的例子，以及用于设置监视标志的多个定时。作为数据输出的详细例子，下面参照附图3和4描述加密和输出数据的处理。注意，在该实施例中，设置监视标志的定时也称作“处理检查点”。

即，当从终端系统1接收到用于加密和输出数据的命令时，首先，响应于该命令，控制单元22根据处理检查点的数目设置监视标志的初

始值(步骤S12)。注意,在图3和4所示的例子中,处理检查点的数目是四。因此,在图3和4所示的例子中,例如,"4"被设置为监视标志的初始值。

当监视标志被初始化时,控制单元22作为第一处理而检查安全状态(步骤S13)。该安全状态检查处理是检查被设置为安全状态的项目的处理。作为该安全状态检查处理,例如,执行作为命令发送源的终端系统1的认证,或所接收的命令的认证。

当作为第一处理的安全状态检查处理正常地结束时,控制单元22确定其为第一处理检查点。第一处理检查点是与第一处理相应的用于设置监视标志的定时。当如上所述确定其为第一处理检查点时,即,当确定作为第一处理的安全状态检查处理正常地结束时,控制单元22设置监视标志。例如,当监视标志的值在第一处理检查点处逐一递减时,控制单元22通过从监视标志的当前值(初始值)减一来设置监视标志。

当监视标志在第一处理检查点被设置时,控制单元22作为第二处理而验证认证方(authenticator)数据(步骤S15)。认证方数据验证处理是一个验证认证方数据的有效性的处理。当作为第二处理的认证方数据验证处理正常地结束时,控制单元22确定该结束为第二处理检查点。第二处理检查点是与第二处理相应的用于设置监视标志的定时。

当确定该结束为如上所述的第二处理检查点时,即,当确定作为第二处理的认证方数据验证处理正常地结束时,控制单元22设置监视标志(步骤S16)。例如,当监视标志的值在第二处理检查点处逐一递减时,控制单元22通过从监视标志的当前值减一来设置监视标志。

当监视标志在第二处理检查点被设置时,控制单元22执行作为第三处理的加密处理(步骤S17)。在该加密处理中,加密要输出的数据。当作为第三处理的加密处理正常地结束时,控制单元22确定该结束为第三处理检查点。第三处理检查点是与第三处理本应的用于设置监视标志的定时。

当如上所述确定该结束为第三处理检查点时,即,当确定作为第

三处理的加密处理正常地结束时，控制单元22设置监视标志(步骤S18)。例如，当监视标志的值在第三处理检查点处逐一递减时，控制单元22通过从监视标志的当前值减一来设置监视标志。

当在第三处理检查点设置监视标志时，控制单元22作为第四处理而处理认证方数据(步骤S19)。认证方数据处理是向要输出的加密数据加入认证方数据的处理。当作为第四处理的认证方数据处理正常结束时，控制单元22确定该结束为第四处理检查点。第四处理检查点是与第四处理相应的用于设置监视标志的定时。

当如上所述确定该结束为第四处理检查点时，即，当确定作为第四处理的认证方数据处理正常地结束时，控制单元22设置监视标志(步骤S20)。例如，当在第四处理检查点处从监视标志的值减一时，控制单元22通过从监视标志的当前值减一来设置监视标志。

在图3和4所示的例子中，在第一、第二、第三和第四处理中必须先于数据输出执行处理。因此，当监视标志在第四处理检查点被设置时，控制单元22确定将响应所接收的读出命令而在数据输出之前执行的各个处理完全结束。当确定将先于数据输出而执行的各个处理结束时，控制单元22产生屏蔽数据(步骤S21和S22)。

屏蔽数据是用于保护要输出的数据的数据。在该实施例中，步骤S23中(稍后将被描述)，利用屏蔽数据对要输出的数据执行计算处理。即，上述的屏蔽数据当监视标志被设置为预定值时不改变要屏蔽的数据，而当监视标志不是该预定值时则改变要屏蔽的数据。

例如，屏蔽数据可利用监视标志的值。屏蔽数据也可基于监视标志的值和随机数数据(任意数据)、监视标志的值和IC卡唯一数据、或过去和当前处理中监视标志的值来产生。在本情况下，假定屏蔽数据是基于监视标志的值和随机数数据产生的。

在本情况中，作为产生屏蔽数据的处理，控制单元22通过随机数发生单元26产生随机数数据(步骤S21)。当该随机数数据由随机数发生单元26产生时，控制单元22基于所产生的随机数数据和监视数据的值产生屏蔽数据(步骤S22)。然后，控制单元22通过在随机数数据和监视

标志的值之间执行预定计算处理来产生屏蔽数据。作为屏蔽数据产生处理的详细例子,可进行根据监视标志的值针对所产生的随机数数据的移位计算处理,以及在计算结果和随机数数据之间的异或操作。

当产生该屏蔽数据时,控制单元22利用所产生的屏蔽数据屏蔽(保护)要输出的数据(步骤S23)。更明确地说,控制单元22在所产生的屏蔽数据和要输出的数据之间执行预定计算处理(步骤S23)。即,为保护要输出的数据,控制单元22利用屏蔽数据针对要输出的数据执行计算处理。例如,作为利用屏蔽数据针对要输出的数据的计算处理,控制单元22在屏蔽数据和要输出的数据之间执行异或操作。作为步骤S23中的计算处理,针对屏蔽数据和要输出的数据可执行或操作、加法或移位计算。

当利用屏蔽数据屏蔽要输出的数据时,作为对所接收的读出命令的响应,控制单元22经由通信接口21向终端系统1输出利用屏蔽数据屏蔽的要输出数据(步骤S25)。因此,作为对所发送的读出命令的响应,终端系统1从IC卡获得数据。

作为步骤S22到S24中的详细例子,将描述一个实例,其中,步骤S22中执行随机数数据和利用随机数数据通过按照监视标志的值进行移位而获得的数据之间的异或操作,以及步骤S23中执行屏蔽数据和要输出的数据之间的异或操作。

在本实例中,当监视标志的值为"0"时,不考虑随机数数据的值,作为步骤S22中的计算结果的屏蔽数据变成"0"。因此,如果屏蔽数据为"0",要输出的数据在步骤S23的计算处理中不被篡改。从而,如果监视标志为"0",该屏蔽数据也变成"0"。因此,步骤S24中,要输出的数据作为正常数据被输出。

与此相反,如果监视标志的值不是"0",作为步骤S22中的计算结果的屏蔽数据不是"0"。因此,如果屏蔽数据不是"0",在步骤S23的计算处理中要输出的数据被篡改。即,如果监视标志的值为"0",则该屏蔽数据不是"0"。因此,步骤S24中,输出通过篡改要输出的数据而获得的异常数据。

如上所述,在根据该实施例的IC卡中,当所有的处理正常结束时,监视对应于用于输出数据的命令的各个处理的执行状态的监视标志被设置为作为预定值的初始值。另外,根据所执行的处理改变(设置)监视标志的值,当完成数据输出之前的处理时根据监视标志的值屏蔽要输出的数据,并输出所屏蔽的数据。

因而,在IC卡中,监视标志不必被检查,并且当处理为异常时,可以阻止输出正常数据。例如,当程序由于干扰而错误工作,并且一个特定的处理被跳过时,监视标志的值变为异常。从而,基于监视标志而屏蔽的输出数据也变为异常。因此,在上述实施例中,可以保护IC卡中的数据,并且实现具有高安全性的IC卡。

更进一步地,在上述的IC卡中,在要输出的数据和屏蔽数据之间执行根据预定规则的诸如异或操作,或操作,加法以及移位计算的计算。该计算结果作为输出数据被输出。因此,当监视标志的值不是预定值时,实际输出数据为不同于要输出数据的异常数据。从而,可以保护IC卡中的数据。

更进一步地,当由监视标志监视的所有处理结束时,在IC卡中,基于监视标志的值和随机数数据产生屏蔽数据,并且基于所产生的屏蔽数据屏蔽并输出要输出的数据。从而,在IC卡中,要输出的数据可以被随机屏蔽。从而,参考屏蔽的数据(输出数据)不能预测正确数据,因此实现具有高安全性的IC卡。

注意,在IC卡中,在所有处理被正常地执行时,监视标志的值可被设置为初始值,以变成"0",并且对于每个特定的处理可递减监视标志的值。在本实例中,当由监视标志所监视的所有处理正常地结束时,监视标志的值在IC卡中变成"0"。因此,作为屏蔽处理,当监视标志的值为"0"时,执行计算处理以防止改变要输出的数据。从而,在IC卡中,当所有处理正常地结束时,即使要输出的数据被屏蔽也无数据改变,因此改善了安全性。

在IC卡中,步骤S24中无论何时输出数据,对IC卡唯一的数据可被保持在非易失性存储器中,并且步骤S21到S23中基于该唯一的数据

及监视标志的值可产生该屏蔽数据。在本实例中，当由监视标志所监视的所有处理结束时，在IC卡中，基于监视标志的值和对于IC卡唯一的数据产生屏蔽数据。然后基于所产生的屏蔽数据屏蔽并输出要输出的数据。从而，在IC卡中，基于IC卡的唯一数据可以屏蔽要输出的数据，因此改善了安全性。

此外，在IC卡中，用于在上述所有处理中屏蔽输出数据(即，每当输出步骤S24中被屏蔽的数据时)的监视标志的值可被存储在非易失性存储器25中，并且基于监视标志的过去和当前值可产生屏蔽数据。在本实例中，当由监视标志所监视的所有处理结束时，在IC卡中，相加存储在非易失性存储器中的监视标志的当前和过去值。然后，基于随机数数据和利用该随机数数据通过按相加的值而进行移位所获得的数据产生屏蔽数据。因此，基于所产生的屏蔽数据屏蔽并输出要输出的数据。从而，因为保存了监视标志的值，即使当程序在相同的位置总是错误工作时，也可以改善安全性。

下面将描述上述处理的修改。

图5和6是用于解释在IC卡2中的处理例子的流程图。

注意，图5和6是用于解释图3和4所示的处理的修改的流程图。因此，与图3和4中相同的参考符号在图5和6中表示相同的步骤，并由此忽略其详细描述。通过给图3和4所示的流程图增加步骤S31和S32而获得图5和6所示的流程图。

即，当确定要在数据输出之前执行的各个处理(第一、第二、第三、和第四处理)完成时，控制单元22确定监视标志的值是否是预定值(例如，"0") (步骤S31)。如果基于确定结果确定监视标志的值不是预定值，则控制单元22输出一个错误状态(步骤S32)，并且该处理结束。可选地，当基于确定结果确定监视标志的值是预定值时，控制单元22前进到步骤S21。

因此，在图5和6所示的修改中，当确定监视标志的值不是预定值("0")时，控制单元22输出错误状态但不输出数据，并且对应于读出命令的处理结束。可选地，当确定监视标志的值是预定值("0")时，控制

单元22产生屏蔽数据，并输出被所产生的屏蔽数据所屏蔽的数据。

即，如在该修改中那样，当基于监视标志的检查结果确定监视标志的值不是预定值时，可以通知错误状态，但不输出数据。即使当监视标志检查处理被跳过时，利用基于监视标志的值的屏蔽数据可以屏蔽要输出的数据。

换言之，当监视标志的值由于普通错误而不是预定值时，IC卡可以通知错误已发生。当监视标志检查处理被欺骗性地跳过时，如果监视标志的值不是预定值，要输出的数据可被篡改并输出。

上述实施例中，在对应于用于输出数据的命令的所有处理被正常地执行时，监视标志的值被设置为初始值，以成为预定值。根据对应于用于输出数据的命令的各个处理的执行状态，设置监视标志的值。当先于数据输出的这些处理被完成时，根据监视标志的值屏蔽要输出的数据，并且输出屏蔽的数据。

如上所述，在该实施例中，即使当处理程序错误工作时，在IC卡中的数据也可以被保护，从而实现具有高安全性的IC卡。

本领域技术人员将容易地想到其他的优点和修改。因此，在其广泛的方面本发明不局限于此处所显示和描述的特定细节和典型的实施例。因此，在不背离如所附权利要求书和其等同表述所定义的总的发明构思的实质或范围的前提下，可做各种修改。

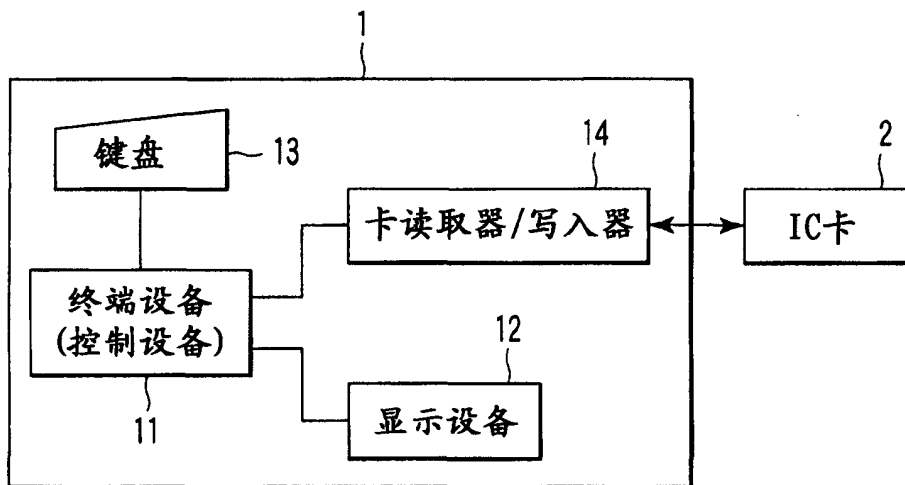


图 1

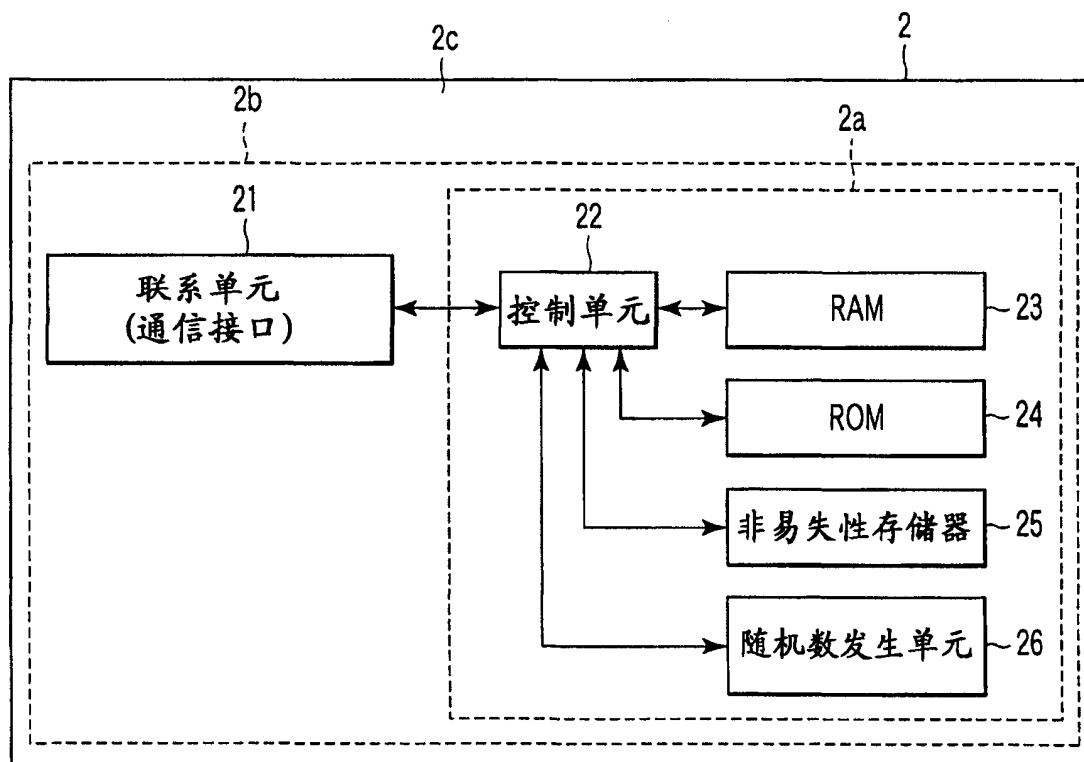


图 2

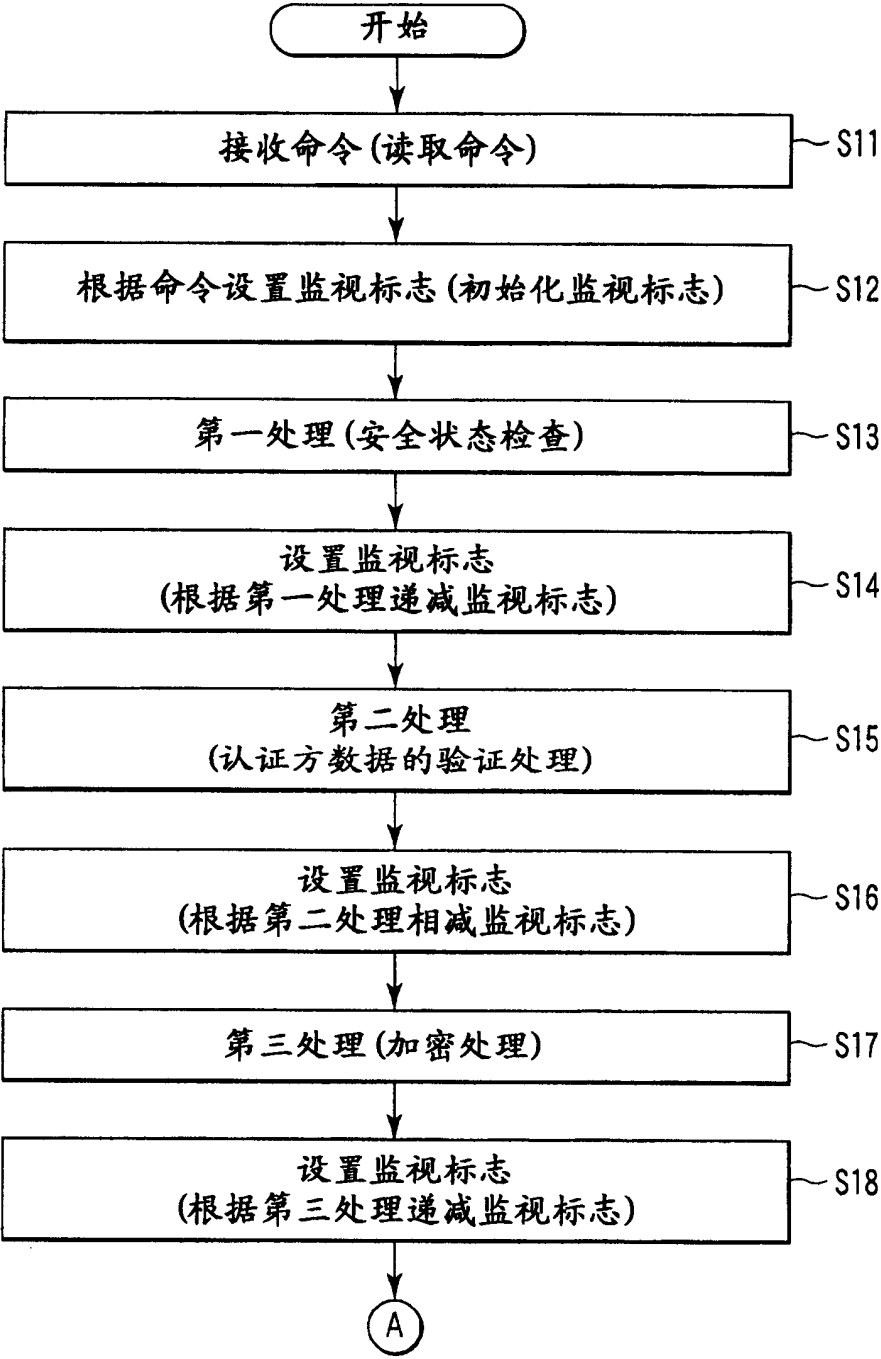


图 3

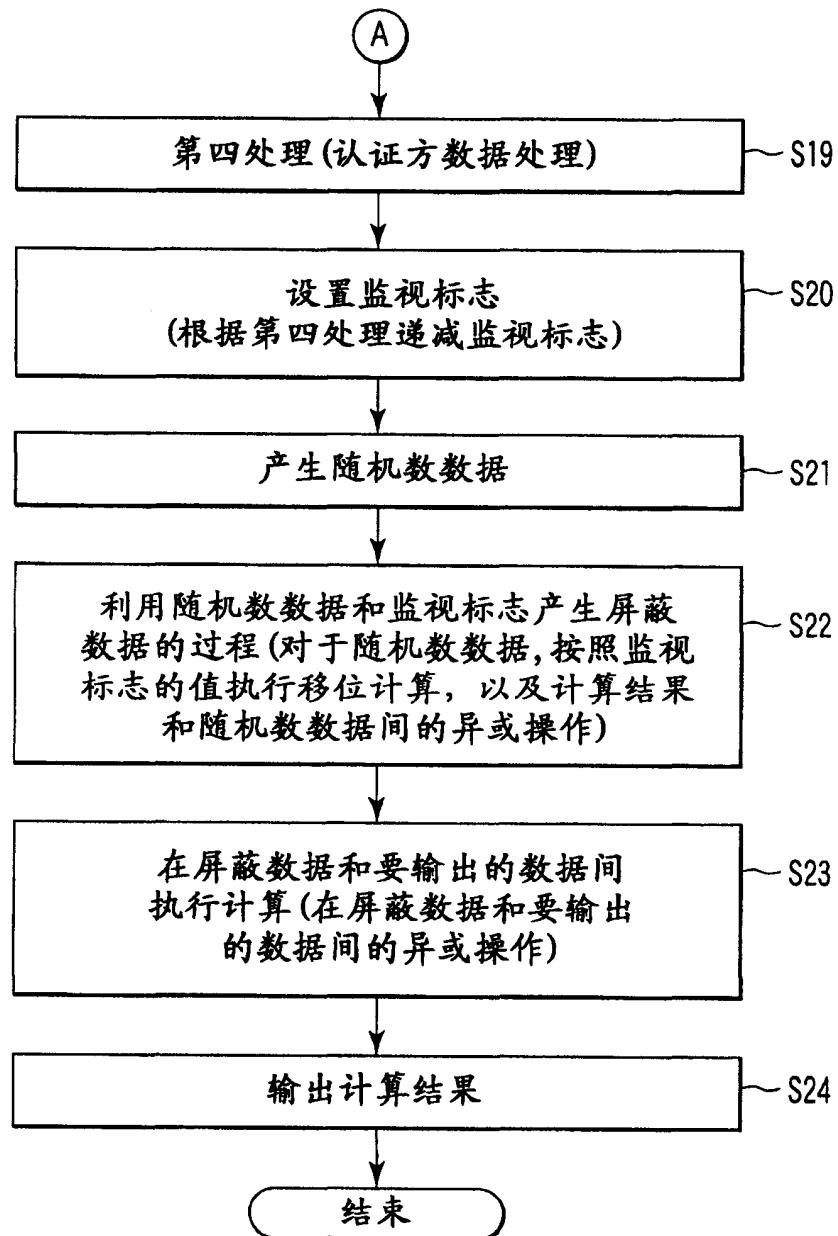


图 4

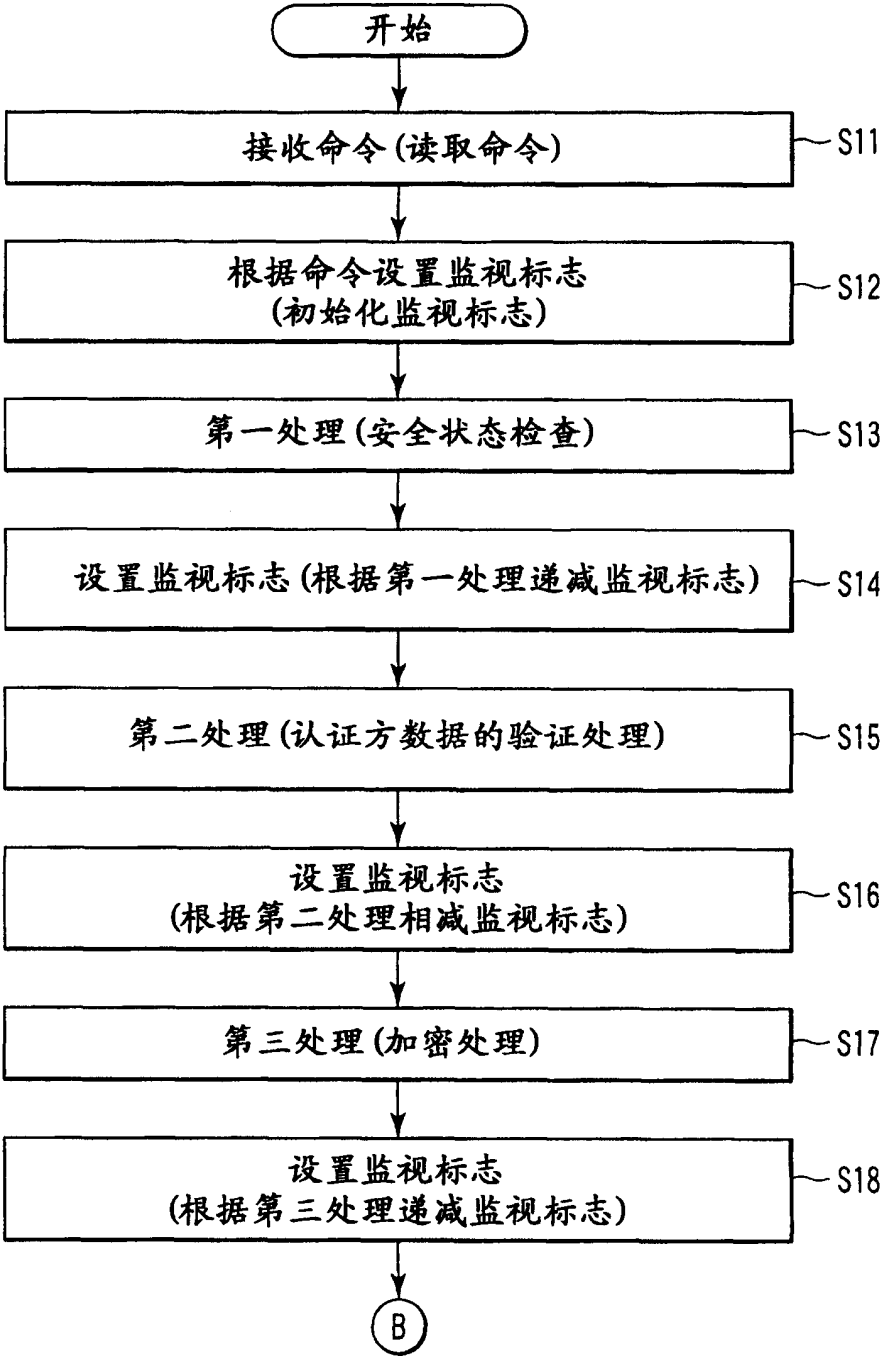


图 5

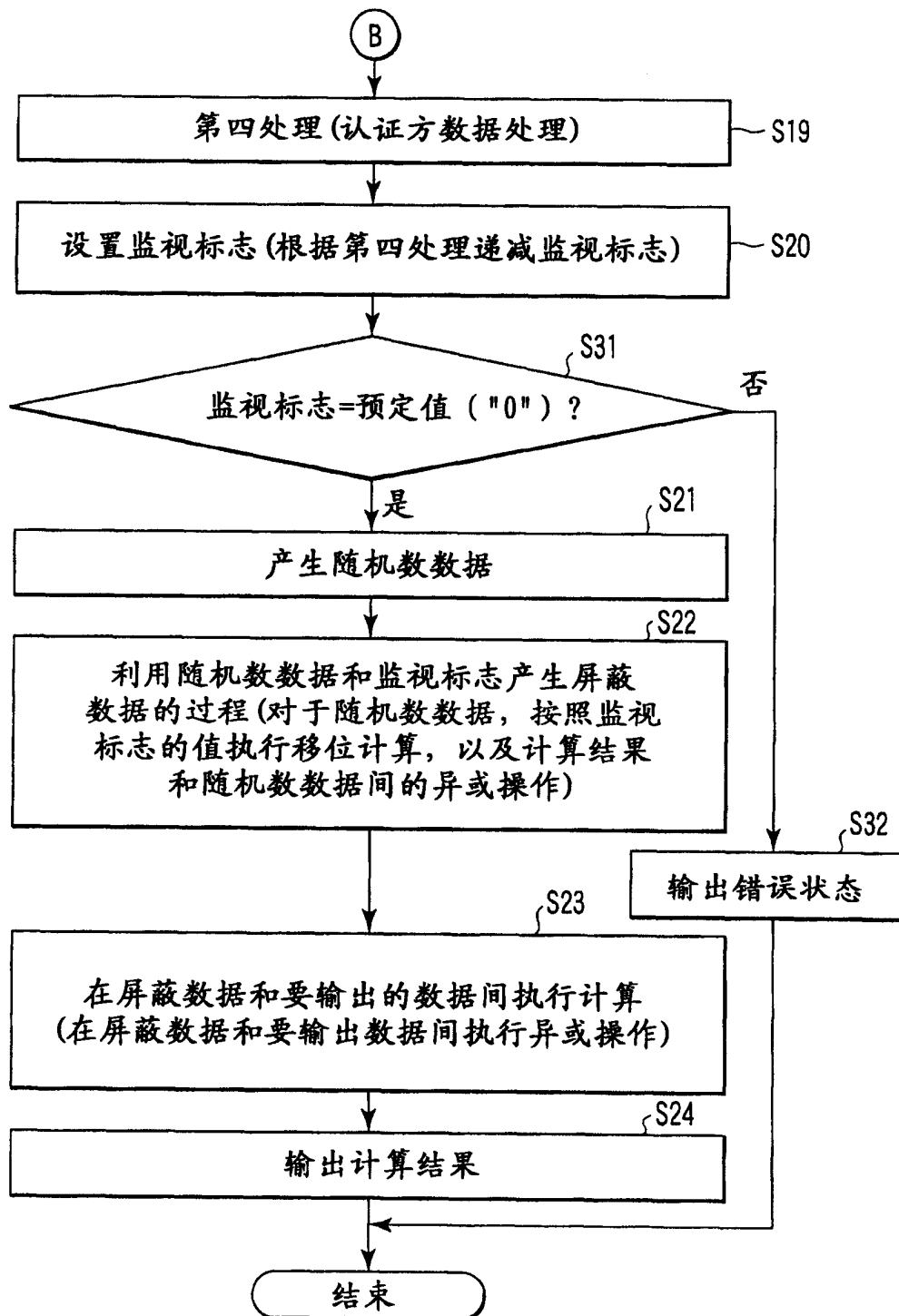


图 6