[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06K 17/00 (2006.01)

[12] 实用新型专利说明书

专利号 ZL 200620041014.9

[45] 授权公告日 2007 年 5 月 9 日

[11] 授权公告号 CN 2898953Y

[22] 申请日 2006.4.13
[21] 申请号 200620041014.9
[73] 专利权人 上海复旦微电子股份有限公司
地址 200433 上海市国泰路 127 号
共同专利权人 上海公共交通卡股份有限公司
[72] 设计人 俞 军 谢志刚 张 弛

[74] 专利代理机构 上海正旦专利代理有限公司
代理人 姚静芳

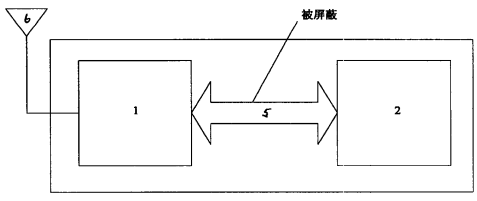
权利要求书 1 页 说明书 3 页 附图 2 页

[54] 实用新型名称

集成安全加密认证功能的非接触卡读写装置

[57] 摘要

本实用新型提供了一种用于非接触 IC(集成电路)卡操作的读写装置，该装置将非接触卡读写功能模块和安全认证模即 SAM 模块集成于一个完整封装模块中，模块间的连线被封装屏蔽不外露。 该读写装置不仅集成了通常的非接触 IC 卡的读写功能，而且集成了实现安全加密用的 SAM(安全认证模块)卡功能，可以减小非接触卡读写器的大小，并解决非接触逻辑加密卡存在的安全隐患，对于目前大量使用逻辑加密非接触卡的应用有重要的实用价值。



1、一种非接触 IC 卡的读写装置，由非接触卡读写功能模块（1）和安全认证模块即 SAM 模块(2)组成，其特征是非接触卡读写功能模块(1)与安全认证模块即 SAM 模块(2)连接且上述两个模块集成在一个完整封装模块中，两个模块间的连线被封装所屏蔽不外露。

2、如权利要求 1 所述的非接触 IC 卡的读写装置，其特征是非接触卡读写功能模块是读写器专用芯片(4)，安全认证模块(2)是高性能 CPU 芯片(3)。

3、如权利要求 2 所述的非接触 IC 卡的读写装置，其特征是读写器专用芯片(4)和高性能 CPU(3)集成为单个芯片。

集成安全加密认证功能的非接触卡读写装置

技术领域

本实用新型涉及一种新型非接触卡的读写器装置和应用。

背景技术

随着我国信息化的发展，非接触 IC 卡的应用领域不断扩展，卡片的应用环境不断改善，用户对非接触卡读写器的形式提出了各种要求，其中大部分涉及小型化和安全性的要求，特别是在涉及金钱交易的领域。目前大部分的非接触卡市场采用了逻辑加密的非接触卡，该类卡片技术成熟，价格较低，同时具有较强的安全性，其采用的三重认证和通信加密方式的安全性也得到了业界的认可。但是由于目前采用的该类非接触 IC 卡的读写器装置上一般采用独立读写芯片（或读写模块）和 SAM 卡的结构，不但体积较大，而且价格较高，同时在卡片读写过程中，SAM 卡产生的卡片读写密钥需要通过读写器控制 CPU 导入读写模块，存在被外界截取的可能性，因此有安全隐患。

发明内容

本实用新型的目的是获得一种小型化、安全性能好的集成安全加密认证功能的非接触卡读写装置。

非接触 IC 卡作为新型的 IC 卡，具有携带使用方便，操作简便，使用寿命长等特点，应用领域越来越广，已经成为了 IC 卡的主要形式。作为读写该类卡片的非接触 IC 卡读写器而言，形式更是多种多样，比如在公交应用中有公交 POS 机，出租车 POS 机，地铁 POS 机，充值机，手持 POS 机等等。但通常 POS 机均包括非接触 IC 卡读写模块（或集成电路芯片）和 SAM（安全认证模块），其中非接触 IC 卡读写模块（或集成电路芯片）负责与非接触 IC 卡通信，而 SAM 负责安全认证和产生加密通信采用的加密密钥。在目前的读卡器对非接触逻辑加密卡的操作流程中，采用读取非接触逻辑加密卡的一些初始化信息和卡片认证码，采用 SAM 的功能进行卡片的合法性认证，同时利用 SAM 卡产生与卡片相关的读写密钥，该密钥导入读写器中的读写模块，即可以对非接触逻辑加密卡进行操作。由于在该密钥导入读写器中的读写模块时，该密钥会以明码形式出现在读写器中读写模块的数据连接线上，可以使用诸如逻辑分析仪等设备截取该密码数据，从而得到操作非接触逻辑加密卡的密码，如果该密码被非法使用，就存在安全性的隐患。

为此本实用新型如权利要求 1 所述，该装置如图 1 所示，集成了非接触卡读写功能模块（1）和 SAM(安全认证模块)（2）的功能，由于上述两个模块集成在一个完整封装模块

中，两个模块间的连线被封装所屏蔽而不外露，那么就可以避免在导入密钥时被非法截取。

本实用新型的装置可以是采用如权利要求 2 中的非接触读写芯片即读写器专用芯片和高性能 CPU 连接组成，非接触卡读写功能和安全认证模块的功能由非接触读写芯片和高性能 CPU 共同完成。读写器芯片可以采用上海复旦微电子股份有限公司的 FM17 系列读卡器芯片，或 Philips 公司的 RC500 系列芯片，高性能 CPU 可以采用 8051 系列的高速 CPU 或 Philips 公司的 ARM 系列 CPU 等。该 CPU 可以完成 SAM 卡的认证和密钥功能外，还可以解决对非接触逻辑加密卡的流程操作。

通过集成电路设计，可以把上述的读写器专用芯片和高性能 CPU 集成为单个芯片，如此可以彻底解决由于连线外露而导致的安全性问题。此方案即为本实用新型的权利要求 3 的内容。

本实用新型获得了一种小型化的集成非接触卡读写功能和 SAM 卡功能为一体的非接触 IC 卡读写器装置，它可以减小读写器装置的体积，最重要的是可以解决逻辑加密非接触卡读写器的安全隐患问题。

附图说明

图 1 是本实用新型装置的结构示意图。

图 2 是本实用新型装置具体结构示意图。

图 3 是本实用新型实施例的结构示意图。

上述图中 1 是非接触卡读写功能模块，2 是 SAM 卡功能模块，3 是高性能 CPU，4 是读写器专用芯片，5 是连接线，6 是天线，7 是射频电路，8 是读写器单元，9 是数据处理单元。

具体实施方式

如图 3 所示的非接触 IC 卡读写模块，该模块采用 FM17XX 系列 IC 卡读写芯片和高性能的 MCU 处理器，实现 RF 卡读卡器和 SAM 卡的双重功能。支持 13.56MHz 频率下的 Type A、Type B 和 15693 标准的协议，操作距离可达 6cm 以上。模块可以通过串口通信进行输入/输出。

该模块具有如下的特点：

1. 集 IC 读写器和 SAM 卡的功能于一身，体积小，非常适于用对体积敏感的手持设备，并且很容易嵌入到应用系统的其它设备中。

2. 支持将消费密钥经加密处理后导入模块，导入的密钥是外部不可读取的，这一过程由读写器发行方操作完成，保证了安全性。

3. 模块程序可以方便地更新，软件的升级换代灵活性高。

4.具有方便灵活的RS232接口，可与任意COM端口连接，如显示设备等。还可以根据用户的需求对输出的数据进行加密和格式转换等处理。

硬件构成

模块硬件由射频电路、FM17XX、数据处理单元及接口电路组成。整个模块按照DIP28方式封装，尺寸为38mm×19mm。数据处理单元是由高性能的MCU组成，是对IC卡操作、数据处理的硬件基础。FM17XX是复旦微电子公司设计的基于ISO14443和15693标准的非接触卡读卡机专用芯片，它支持13.56MHz频率下的Type A、Type B和15693方式的通信协议和加密算法。

软件功能

模块的软件部分包括嵌入式软件和工具软件两部分，嵌入式软件是嵌入模块中MCU的软件，工具软件是PC上的软件，用作模块发行时的密钥导入。嵌入式软件实现了对IC卡数据存贮的操作、数据处理、数据输入输出及SAM的功能，工具软件由模块发行方操作，实现从SAM卡母卡中导出密钥，对密钥进行加密处理，然后把经加密处理后的密钥导入模块。

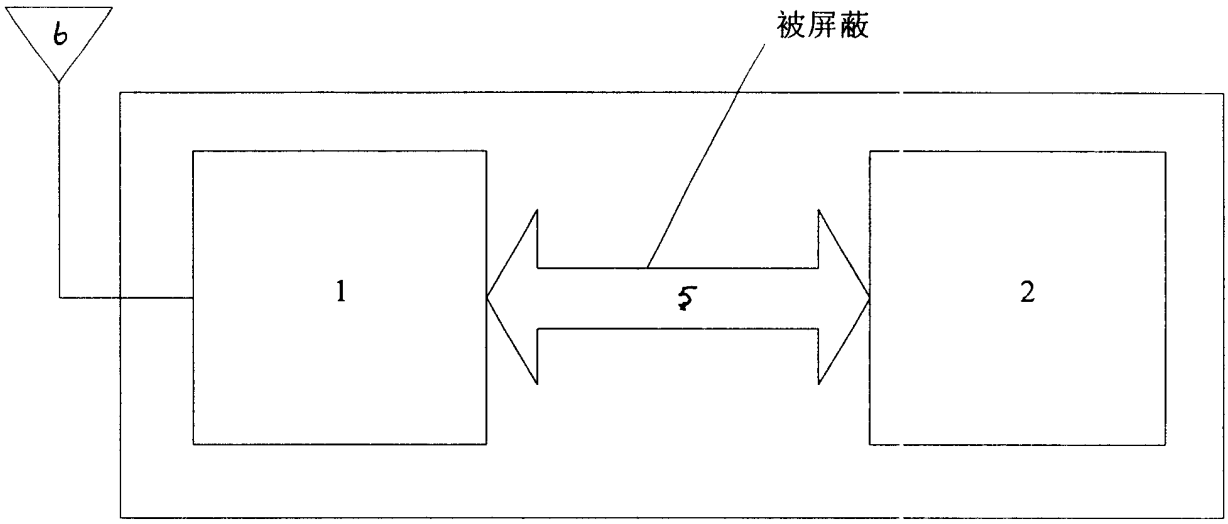


图 1

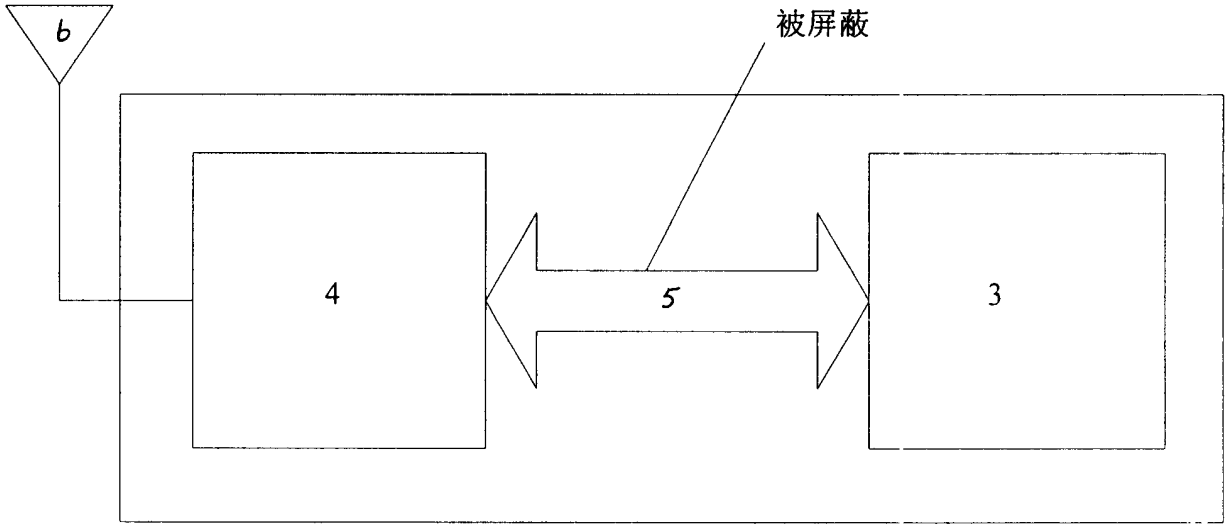


图 2

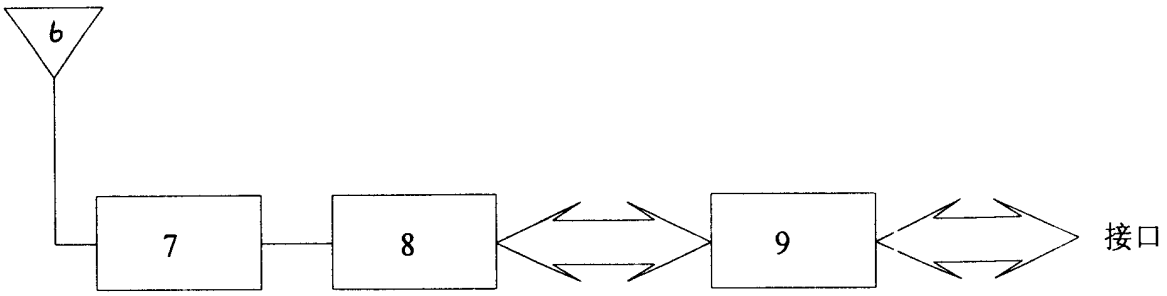


图 3