(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102497465 A
(43)申请公布日 2012.06.13

(21)申请号 201110329692.0

(22)申请日 2011.10.26

(71)申请人 潘铁军
地址 315100 浙江省宁波市鄞州区钟公庙街道钱湖南路 8 号

(72)发明人 潘铁军

(51)Int.Cl.
H04M 1/725(2006.01)
H04L 9/32(2006.01)
G06F 21/00(2006.01)

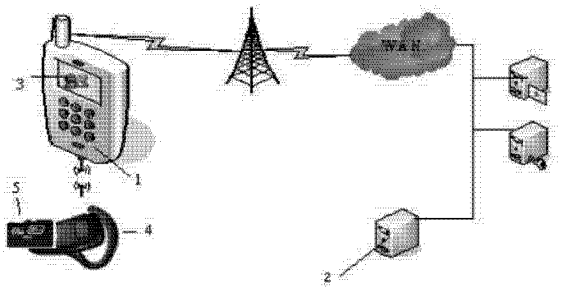
权利要求书 2 页　说明书 6 页　附图 5 页

(54)发明名称

一种分布式密钥的高保密移动信息安全系统及安全方法

(57)摘要

本发明公开了一种分布式密钥的高保密移动信息安全系统及安全方法，包括安装在移动电话上与服务器通讯的客户端和设置在耳机中与移动电话通讯的安全设备，其特征在于所述的耳机通过接口连接有基于硬件加密或生物特征识别的安全设备，所述的安全设备存储标识用户的密钥、口令、数字证书、生物特征信息的至少一种。优点利用耳机作为基于硬件加密的移动信息安全设备，为手机用户提供高强度的信息安全保护，同时，采用基于并行计算的安全设备不仅能够满足对上层应用的单指令调用，而且能满足多业务对大量数据存储、高效处理的安全保障；多重签约信息的鉴权和交叉校验大大提高了系统的安全性。



CN 102497465 A

1. 一种移动信息安全系统的安全装置，包括安装在移动电话上与服务器通讯的客户端和设置在耳机中与移动电话通讯的安全设备，其特征在于所述的耳机通过接口连接有基于硬件加密或生物特征识别的安全设备，所述的安全设备存储标识用户的密钥、口令、数字证书、生物特征信息的至少一种。

2. 如权利要求 1 所述的一种移动信息安全系统的安全装置，其特征在于所述的接口为总线、SDIO、USB、数据线接口的至少一种。

3. 如权利要求 1 所述的一种移动信息安全系统的安全装置，其特征在于所述的安全设备是一种基于硬件加密或生物特征识别的安全设备，支持 SWP 协议、PBOC 规范、QPBOC 协议中的至少一种，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备中至少一种两两结合。

4. 一种用于移动信息安全保护的 NFC 耳机，包括安装在一壳体内的单片机以及通过接口模块分别与单片机相连的耳机模块、用于移动信息安全保护的安全设备、用于与外界通讯的 NFC 模块、用于接收外界 NFC 信号并获得工作能量的天线、电源，其特征在于所述的安全设备是一种基于硬件加密或生物特征识别的安全设备，支持 SWP 协议、PBOC 规范、QPBOC 协议中的至少一种，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备中至少一种两两结合，所述的接口模块支持总线、SDIO、USB、数据线接口的至少一种，所述天线连接至所述 NFC 模块。

5. 如权利要求 4 所述的一种用于移动信息安全保护的 NFC 耳机，其特征在于所述的安全设备是支持 SWP 协议、CUPMobile 银行卡应用规范和 CUPMobile 智能 SD 卡应用接口规范的 TF 卡，所述的接口模块是安装 TF 卡的 TF 卡座，所述 TF 卡座具有实现安装在所述 TF 卡座上的 TF 卡的 SWP 协议信号传输的 SWP 触点以及为安装在所述 TF 卡座上的 TF 卡的 SWP 模块供电的 Vcc 触点，所述 SWP 触点和 Vcc 触点可分别与 TF 卡上的 SWP 触点和 Vcc 触点相连接。

6. 一种用于移动信息安全保护的蓝牙耳机，包括安装在一壳体内的单片机以及通过接口模块分别与单片机相连的蓝牙耳机模块、用于移动信息安全保护的安全设备、用于与外界通讯的 NFC 模块、用于接收外界 NFC 信号并获得工作能量的天线、电源，其特征在于所述的安全设备是一种基于硬件加密或生物特征识别的安全设备，支持 SWP 协议、PBOC 规范、QPBOC 协议中的至少一种，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备中至少一种两两结合，所述的接口模块支持总线、SDIO、USB、数据线接口的至少一种，所述天线连接至所述 NFC 模块。

7. 如权利要求 6 所述的一种用于移动信息安全保护的蓝牙耳机，其特征在于所述的安全设备是支持 SWP 协议、CUPMobile 银行卡应用规范和 CUPMobile 智能 SD 卡应用接口规范的 TF 卡，所述的接口模块是安装 TF 卡的 TF 卡座，所述 TF 卡座具有实现安装在所述 TF 卡座上的 TF 卡的 SWP 协议信号传输的 SWP 触点以及为安装在所述 TF 卡座上的 TF 卡的 SWP 模块供电的 Vcc 触点，所述 SWP 触点和 Vcc 触点可分别与 TF 卡上的 SWP 触点和 Vcc 触点相连接。

8. 一种用于移动信息安全保护的安全设备，包括指令存储器 IM（Instruction Memory）、阵列处理器 AP（Array Processor）和数据阵列存储器 DAM（Data/Instruction Array Memory），其特征在于所述的安全设备基于 SIMD（Single Instruction Multiple Data stream）体系结构，一条专用的指令 SI（Single Instruction）可以使阵列处理器 AP 重构并转换成并行计算的多指令流 MI（Multiple Instruction）和多数据流 MD(Multiple

Data stream)，以完成多业务的安全保护；所述的数据阵列存储器 DAM，也作为指令阵列存储器使用，不仅能完成数据的并行读写，而且也能完成指令的并行读写；所述的阵列处理器 AP 中的处理元(PE，Processing Element)之间互连是采用局部路由器实现。

9. 一种基于分布式密钥的安全方法，其特征在于包括以下步骤：

①用户持本人相关证件和携带安装有基于硬件加密或生物特征识别安全设备的耳机在相关部门填写签约信息，所述的签约信息包括但并不限于用来标识用户的身份证号码、银行卡号、智能卡标识、国际移动用户识别码 IMSI、国际移动设备身份码 IMEI、移动用户综合业务数字网号码 MSISDN、IP 地址、用户名、密码、生物识别特征、数字证书、密钥和申请的业务种类及其安全策略、授信额度和风险等级；

②相关部门根据国家商密办指定的加密算法，将加密过的用户签约信息、电子商务安全基础平台中涉及的安全信息返写到所述的安全设备上对应的 IC 卡应用文件和相关部门的服务器；

③ 所述客户端可以通过 OTA(Over The Air) 的方式安装在移动电话上并进行软件更新和业务下载；所述客户端为用户提供操作界面，将用户需要保护的信息根据不同的安全等级传送到所述安全设备依据不同的安全策略进行安全保护；根据检测到的风险等级动态调整安全等级，风险升高时，将相应安全等级提高，风险降低时，将安全等级恢复正常；

④所述的客户端与所述服务器、所述安全设备、所述耳机根据签约信息进行相互认证和交叉校验，如果签约信息不一致则认证不成功，允许用户重试，重试失败后结束业务流程；对短时间内多次频繁重试的用户，所述的安全设备、所述服务器对该用户的业务自动锁定并列入黑名单，只有通过相关部门来解锁；认证成功，所述的客户端将用户需要保护的信息，通过安全设备进行安全保护后，发送到所述服务器完成业务。

10. 一种基于分布式密钥的安全方法，其特征在于包括以下步骤：

①用户通过客户端将个人安全信息写入基于硬件加密或生物特征识别安全设备中，所述的个人安全信息包括但并不限于用来标识用户的身份证号码、银行卡号、智能卡标识、国际移动用户识别码 IMSI、国际移动设备身份码 IMEI、移动用户综合业务数字网号码 MSISDN、IP 地址、用户名、密码、超级用户口令、生物识别特征、数字证书、密钥、好友列表和安全策略；所述的安全设备是一种 IC 卡设备，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备、手机耳机中至少一种两两结合；所述的个人安全信息存储在所述的安全设备上对应的 IC 卡应用文件；

②所述客户端可以通过 OTA(Over The Air) 的方式安装在移动电话上并进行软件更新和业务下载；所述客户端为用户提供操作界面，将用户需要保护的信息根据不同的安全等级传送到所述安全设备依据不同的安全策略进行安全保护；根据检测到的风险等级动态调整安全等级，风险升高时，将相应安全等级提高，风险降低时，将安全等级恢复正常；

③所述的客户端、所述安全设备根据所述的个人安全信息进行相互认证和交叉校验，如果签约信息不一致则认证不成功，允许用户重试，重试失败后结束安全流程；对短时间内多次频繁重试的用户，所述的安全设备、所述客户端对该用户的操作自动锁定，通过超级用户或延时来解锁；认证成功，所述的客户端将用户需要保护的信息，通过安全设备进行安全保护后，进行存储或发送。

一种分布式密钥的高保密移动信息安全系统及安全方法

技术领域

[0001] 本发明涉及一种移动信息安全系统，尤其是涉及一种分布式密钥的高保密移动信息安全系统及安全方法。

[0002]

背景技术

[0003] 随着第三代移动通信系统(The Third-Generation Mobile Communication System, 3G)时代的到来，无线移动业务空前繁荣，将智能手机、掌上电脑和其它移动设备结合到标准的商业活动中将成为3G的“Killer Application”，移动应用迎来了飞速发展的黄金时代，移动应用迎来了飞速发展的黄金时代，但安全问题至今仍然是制约移动业务“井喷”的关键瓶颈。国内外学者试图在计算能力和资源严重受限的手机内部寻求解决方案，但在手机病毒日益猖獗和SIM卡克隆机的攻击下，安全防护形同虚设，这也是目前移动业务仅限于小额支付或定向支付的原因。另外，由于我国对金融混业经营的严格管制，银行和移动运营商、SP、制造商的利益冲突，使手机这个天然的无线个域网平台未能充分发挥改变人们生活模式的巨大潜在影响。

[0004] 由于移动设备提供了越来越多的重要功能，移动信息安全逐渐成为影响终端产品推广和移动业务增值的关键因素，是未来市场竞争力的重要体现。由于移动信息安全技术主要被国外组织和企业垄断，需付出大量的外汇，具有潜在的战略和商业威胁，这对研发具有自主知识产权的移动信息安全技术是一个发展机遇。目前iphone4等手机的用户越来越多，但由于手机没有SD卡插槽等原因，依靠基于外部安全设备金融安全SD卡的移动支付模式不能实现，本发明将耳机作为载体，将基于硬件加密的安全模块作为IC模块嵌入到耳机内或作为耳机的插件插入耳机来为手机提供安全保护，能够有效增强手机的信息安全性能，达到金融安全级的安全保护。2001年12月5日公开的01138250.3号中国发明专利公开了具有信息安全管理单元的安全计算机，提出一种具有信息安全管理单元的安全计算机。所述安全计算机包括身份信息输入设备接口，信息安全管理单元，安全控制执行单元，开机电路单元，计算机外设开关电路单元，以及计算机主板单元，安全计算机中的安全管理单元还可做成安全模块(ELM) 。其优点在于：具有自检，验证，从底层硬件控制管理信息，从而解决和改善了计算机信息的安全保护问题。该方案适用于专用的计算机，而对智能手机不适合，因为需要对手机进行改造，实施复杂，成本高，不可行，不能满足用户移动信息安全的需求。而本发明在不改造手机硬件的条件下，就能满足人们对高保密移动信息安全功能的需求。

[0005] 随着移动通信技术的迅猛发展，移动终端(手机、PDA等)已逐渐成为个人商务平台，采用基于硬件加密的移动信息安全设备成为大势所趋，对phone手机用户，他们有移动信息安全保护的强烈愿望，如何将耳机改造为高保密的移动信息安全设备成为一个迫切的问题。

[0006]

发明内容

[0007] 本发明所要解决的技术问题是提供一种高保密的移动信息安全系统及安全方法。

[0008] 一种移动信息安全系统的安全装置，包括安装在移动电话上与服务器通讯的客户端和设置在耳机中与移动电话通讯的安全设备，其特征在于所述的耳机通过接口连接有基于硬件加密或生物特征识别的安全设备，所述的安全设备存储标识用户的密钥、口令、数字证书、生物特征信息的至少一种。所述的接口为总线、SDIO、USB、数据线接口的至少一种。所述的安全设备是一种基于硬件加密或生物特征识别的安全设备，支持 SWP (Single Wire Protocol，单线协议）协议、PBOC 规范、QPBOC 协议中的至少一种，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备中至少一种两两结合。

[0009] 一种用于移动信息安全保护的 NFC 耳机，包括安装在一壳体内的单片机以及通过接口模块分别与单片机相连的耳机模块、用于移动信息安全保护的安全设备、用于与外界通讯的 NFC 模块、用于接收外界 NFC 信号并获得工作能量的天线、电源，其特征在于所述的安全设备是一种基于硬件加密或生物特征识别的安全设备，支持 SWP 协议、PBOC 规范、QPBOC 协议中的至少一种，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备中至少一种两两结合，接口模块支持总线、SDIO、USB、数据线接口的至少一种，天线连接至所述 NFC 模块。安全设备是支持 SWP 协议、CUPMobile 银行卡应用规范和 CUPMobile 智能 SD 卡应用接口规范的 TF 卡，接口模块是安装 TF 卡的 TF 卡座，TF 卡座具有实现 TF 卡的 SWP 协议信号传输的 SWP 触点以及为安装在 TF 卡座上的 TF 卡的 SWP 模块供电的 Vcc 触点，SWP 触点和 Vcc 触点可分别与 TF 卡上的 SWP 触点和 Vcc 触点相连接。

[0010] 一种用于移动信息安全保护的蓝牙耳机，包括安装在一壳体内的单片机以及通过接口模块分别与单片机相连的蓝牙耳机模块、用于移动信息安全保护的安全设备、用于与外界通讯的 NFC 模块、用于接收外界 NFC 信号，并获得工作能量的天线、用于电压检测的低压检测模块，其特征在于所述的安全设备是一种基于硬件加密或生物特征识别的安全设备，支持 SWP 协议、PBOC 规范、QPBOC 协议中的至少一种，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备中至少一种两两结合。所述的接口模块支持总线、SDIO、USB、数据线接口的至少一种。所述天线连接至所述 NFC 模块。所述的安全设备是支持 SWP 协议、CUPMobile 银行卡应用规范和 CUPMobile 智能 SD 卡应用接口规范的 TF 卡，所述的接口模块是安装 TF 卡的 TF 卡座，所述 TF 卡座具有实现安装在所述 TF 卡座上的 TF 卡的 SWP 协议信号传输的 SWP 触点以及为安装在所述 TF 卡座上的 TF 卡的 SWP 模块供电的 Vcc 触点，所述 SWP 触点和 Vcc 触点可分别与 TF 卡上的 SWP 触点和 Vcc 触点相连接。

[0011] 一种用于移动信息安全保护的安全设备，包括指令存储器 IM (Instruction Memory)、阵列处理器 AP (Array Processor) 和数据阵列存储器 DAM (Data/Instruction Array Memory)，其特征在于所述的安全设备基于 SIMD (Single Instruction Multiple Data stream) 体系结构，一条专用的指令 SI (Single Instruction) 可以使阵列处理器 AP 重构并转换成并行计算的多指令流 MI (Multiple Instruction) 和多数据流 MD(Multiple Data stream)，以完成多业务的安全保护；所述的数据阵列存储器 DAM，也作为指令阵列存储器使用，不仅能完成数据的并行读写，而且也能完成指令的并行读写；所述的阵列处理器 AP 中的处理元 (PE，Processing Element) 之间互连是采用局部路由器实现。

[0012] 一种基于分布式密钥的安全方法，其特征在于包括以下步骤：

①用户持本人相关证件和带有安全设备的耳机在相关部门填写签约信息，所述的签约信息包括但并不限于用来标识用户的身份证号码、银行卡号、智能卡标识、IMSI、IMEI、IP地址、用户名、密码、生物识别特征、数字证书、密钥和申请的业务种类、授信额度和风险等级。②相关部门根据国家商密办指定的加密算法，将加密过的用户签约信息、电子商务安全基础平台中涉及的安全信息返写到所述的安全设备上对应的IC卡应用文件和所述的服务器。③所述客户端可以通过OTA(Over The Air)的方式安装在移动电话上并进行软件更新和业务下载。所述客户端为用户提供操作界面，将用户需要保护的信息传送到所述安全设备进行安全保护；④所述的客户端与所述服务器、所述安全设备、所述耳机根据签约信息进行两两认证和交叉校验，如果签约信息不一致则认证不成功，允许用户重试，重试失败后结束业务流程。对短时间内多次频繁重试的用户，所述的安全设备、所述服务器对该用户的业务自动锁定，只有通过相关部门来解锁。认证成功，所述的客户端将用户需要保护的信息，通过安全设备进行安全保护后，发送到所述服务器完成业务。

[0013] 一种基于分布式密钥的安全方法，其特征在于包括以下步骤：

①用户通过客户端将个人安全信息写入基于硬件加密或生物特征识别安全设备中，所述的个人安全信息包括但并不限于用来标识用户的身份证号码、银行卡号、智能卡标识、IMSI、IMEI、IP地址、用户名、密码、超级用户口令、生物识别特征、数字证书、密钥、好友列表和安全策略；所述的安全设备是一种IC卡设备，可以与SIM卡、Micro SD卡、TF卡、USB设备、手机耳机中至少一种两两结合。所述的个人安全信息存储在所述的安全设备上对应的IC卡应用文件；②所述客户端可以通过OTA(Over The Air)的方式安装在移动电话上并进行软件更新和业务下载。所述客户端为用户提供操作界面，将用户需要保护的信息传送到所述安全设备进行安全保护；③所述的客户端、所述安全设备根据所述的个人安全信息进行两两认证和交叉校验，如果签约信息不一致则认证不成功，允许用户重试，重试失败后结束安全流程。对短时间内多次频繁重试的用户，所述的安全设备、所述客户端对该用户的操作自动锁定，通过超级用户或延时来解锁。认证成功，所述的客户端将用户需要保护的信息，通过安全设备进行安全保护后，进行存储或发送。

[0014] 与现有技术相比，本发明的优点在于利用耳机作为基于硬件加密的移动信息安全设备，为iphone等手机用户提供高强度的信息安全保护，同时，采用基于并行计算的安全设备不仅能够满足对上层应用的单指令调用，而且能满足多业务对大量数据存储、高效处理的安全保障；多重签约信息的鉴权和交叉校验大大提高了系统的安全性；通过OTA的方式可以方便地对移动信息安全系统进行业务更新和升级，因此可扩展性更强。随着第三代移动通信网络的到来，移动电话、PDA逐渐发展成为功能强大的个人商务平台，本发明可以在不改变手机硬件的情况下，为移动业务提供高保密的移动信息安全保障。

[0015] 附图说明

图1为本发明实施例一的结构示意图；

图2为本发明实施例二的结构示意图；

图3为本发明实施例三的结构示意图；

图4为本发明实施例四的结构示意图；

图5为本发明实施例五的结构示意图；

图 6 为本发明实施例六的结构示意图；

图 7 为本发明实施例七的结构示意图。

具体实施方式

[0016]

以下结合附图实施例对本发明作进一步详细描述。

[0017] 实施例一：一种移动信息安全系统的安全装置，如图 1 中所示，包括安装在移动电话 1 上与服务器 2 通讯的客户端 3 和设置在耳机 4 中与移动电话 1 通讯的安全设备 5，其特征在于所述的耳机 4 通过 SDIO 接口连接有基于硬件加密或生物特征识别的安全设备 5，安全设备 5 存储标识用户的密钥、口令、数字证书、生物特征信息的至少一种，支持 SWP 协议、PBOC 规范、QPBOC 协议，和 TF 卡整合为一。

[0018] 实施例二：一种用于移动信息安全保护的 NFC 耳机，如图 2 中所示，包括安装在一壳体 1 内的 ARM Cortex A8 单片机 2 以及通过 UART 接口模块 3 与单片机 2 相连的耳机模块 4、通过 PIO 接口模块 3 与单片机 2 相连的并用于移动信息安全保护的 ESAM 安全设备 5、用于与外界通讯的 NFC 模块 6、用于接收外界 NFC 信号并获得工作能量的天线 7、电源 8，天线 7 连接至 NFC 模块 6。ESAM 安全设备 5 是一种基于硬件加密的嵌入式安全模块，支持 SWP 协议、PBOC 规范、QPBOC 协议，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备中至少一种两两结合。

[0019] 实施例三：一种用于移动信息安全保护的 NFC 耳机，如图 3 中所示，包括安装在一壳体 1 内的 ARM Cortex A8 单片机 2 以及通过 UART 接口模块 3 与单片机 2 相连的 BF10 耳机模块 4、通过 TF 卡座接口模块 3 与单片机 2 相连的并用于移动信息安全保护的 TF 卡信息安全设备 5、用于与外界通讯的 NFC 模块 6、用于接收外界 NFC 信号并获得工作能量的天线 7、用于供电的电源模块 8，天线 7 连接至 NFC 模块 6。TF 卡信息安全设备 5 是基于硬件加密的智能卡与 TF 卡集成的信息安全卡，支持 SWP 协议、PBOC 规范、QPBOC 协议、CUPMobile 银行卡应用规范和 CUPMobile 智能 SD 卡应用接口规范。TF 卡座 3 通过其上的 SWP 触点实现与插入的 TF 卡信息安全设备 5 的 SWP 协议信号传输，通过其上的 Vcc 触点为插入的 TF 卡信息安全设备 5 的 SWP 模块供电，TF 卡座 3 上额 SWP 触点和 Vcc 触点可分别与 TF 卡信息安全设备 5 上的 SWP 触点和 Vcc 触点相连接。

[0020] 实施例四：一种用于移动信息安全保护的蓝牙耳机，如图 4 中所示，包括安装在一壳体 1 内的 ARM Cortex A8 单片机 2 以及通过 UART 接口模块 3 与单片机 2 相连的 BF10 蓝牙耳机模块 4、通过 PIO 接口模块 3 与单片机 2 相连的并用于移动信息安全保护的 ESAM 安全设备 5、用于与外界通讯的 NFC 模块 6、用于接收外界 NFC 信号并获得工作能量的天线 7、用于供电的电源模块 8，天线 7 连接至 NFC 模块 6。ESAM 安全设备 5 是一种基于硬件加密的嵌入式安全模块，支持 SWP 协议、PBOC 规范、QPBOC 协议，可以与 SIM 卡、Micro SD 卡、TF 卡、USB 设备中至少一种两两结合。

[0021] 实施例五：一种用于移动信息安全保护的蓝牙耳机，如图 5 中所示，包括安装在一壳体 1 内的 ARM Cortex A8 单片机 2 以及通过 UART 接口模块 3 与单片机 2 相连的 BF10 蓝牙耳机模块 4、通过 TF 卡座接口模块 3 与单片机 2 相连的并用于移动信息安全保护的 TF 卡信息安全设备 5、用于与外界通讯的 NFC 模块 6、用于接收外界 NFC 信号并获得工作能量的

天线 7、用于供电的电源模块 8，天线 7 连接至 NFC 模块 6。TF 卡信息安全设备 5 是基于硬件加密的智能卡与 TF 卡集成的信息安全卡，支持 SWP 协议、PBOC 规范、QPBOC 协议、CUPMobile 银行卡应用规范和 CUPMobile 智能 SD 卡应用接口规范。TF 卡座 3 通过其上的 SWP 触点实现与插入的 TF 卡信息安全设备 5 的 SWP 协议信号传输，通过其上的 Vcc 触点为插入的 TF 卡信息安全设备 5 的 SWP 模块供电，TF 卡座 3 上额 SWP 触点和 Vcc 触点可分别与 TF 卡信息安全设备 5 上的 SWP 触点和 Vcc 触点相连接。

[0022] 实施例六：一种用于移动信息安全保护的蓝牙耳机，如图 6 中所示，包括安装在一壳体 1 内的 ARM Cortex A8 单片机 2 以及通过 UART 接口模块 3 与单片机 2 相连的 BF10 蓝牙耳机模块 4、通过 TF 卡座接口模块 3 与单片机 2 相连的并用于移动信息安全保护的 TF 卡信息安全设备 5。TF 卡信息安全设备 5 是基于硬件加密的智能卡与 TF 卡集成的信息安全卡，支持 SWP 协议、PBOC 规范、QPBOC 协议、CUPMobile 银行卡应用规范和 CUPMobile 智能 SD 卡应用接口规范。TF 卡信息安全设备 5 上集成了用于与外界通讯的 NFC 模块、用于接收外界 NFC 信号并获得工作能量的天线、天线连接至 NFC 模块。

[0023] 实施例七：一种用于移动信息安全保护的安全设备 TF 信息安全卡，如图 7 中所示，包括指令存储器 IM300、阵列处理器 AP310 和数据阵列存储器 DAM320，TF 信息安全卡基于 SIMD 体系结构，一条专用的移动支付安全指令 SI（Mobile_Payment）可以使阵列处理器 AP 重构并转换成并行计算的多指令流 MI（移动支付鉴权指令 Mobile_Payment_Authorization，移动支付交易指令 Mobile_Payment_Transaction， 移动支付广告指令 Mobile_Payment _Advertisement）和多数据流 MD（移动支付鉴权数据流 Mobile_Payment_Authorization_ Data_Stream，移动支付交易指令数据 Mobile_Payment_Transaction_Data_Stream， 移动支付广告数据流 Mobile_Payment _Advertisement_Data_Stream），以完成多业务的安全保护；数据阵列存储器 DAM320 也作为指令阵列存储器使用，MD（移动支付鉴权指令 Mobile_Payment_Authorization，移动支付交易指令 Mobile_Payment_Transaction， 移动支付广告指令 Mobile_Payment _Advertisement）可存入其中，不仅能完成数据 MD（移动支付鉴权数据流 Mobile_Payment_Authorization_ Data_Stream，移动支付交易指令数据 Mobile_Payment_Transaction_Data_Stream， 移动支付广告数据流 Mobile_Payment _Advertisement_Data_Stream）的并行读写，而且也能完成指令 MD（移动支付鉴权指令 Mobile_Payment_Authorization，移动支付交易指令 Mobile_Payment_Transaction， 移动支付广告指令 Mobile_Payment _Advertisement）的并行读写；阵列处理器 AP310 中的处理元之间互连是采用局部路由器实现。

[0024] 实施例八：一种基于分布式密钥的安全方法，其特征在于包括以下步骤：

①用户持本人身份证和携带安装有基于硬件加密或生物特征识别的 TF 信息安全 IC 卡安全设备的耳机在相关部门填写签约信息，所述的签约信息包括但并不限于用来标识用户的身份证号码、银行卡号、智能卡标识、IMSI、IMEI、MSISDN、IP 地址、用户名、密码、生物识别特征、数字证书、密钥和申请的业务种类及其安全策略、授信额度和风险等级；

②相关部门根据国家商密办指定的加密算法，将加密过的用户签约信息、电子商务安全基础平台中涉及的安全信息返写到所述的安全设备上对应的 IC 卡应用文件和相关部门的服务器；

③所述客户端可以通过 OTA(Over The Air) 的方式安装在移动电话上并进行软件更新

和业务下载。所述客户端为用户提供操作界面，将用户需要保护的信息根据不同的安全等级传送到所述安全设备依据不同的安全策略进行安全保护；根据检测到的风险等级动态调整安全等级，当检测到安全攻击时，客户端根据安全策略迅速将安全等级提高，只有通过更高安全等级的认证和鉴权才能使业务继续进行，否则结束业务流程并记录风险记录供事后分析。当检测到安全攻击消失或已排除安全漏洞后，经过稳定性测试，逐步将安全等级恢复正常；

④所述的客户端与所述服务器、所述安全设备、所述耳机根据签约信息进行相互认证和交叉校验，如果签约信息不一致则认证不成功，允许用户重试，重试失败后结束业务流程。对短时间内多次频繁重试的用户，所述的安全设备、所述服务器对该用户的业务自动锁定并记入黑名单，只有通过相关部门来解锁。认证成功，所述的客户端将用户需要保护的信息，通过安全设备进行安全保护后，发送到所述服务器完成业务。

[0025] 实施例九：一种基于分布式密钥的安全方法，其特征在于包括以下步骤：

①用户通过客户端将个人安全信息写入基于硬件加密或生物特征识别的 TF 智能卡中，个人安全信息包括但并不限于用来标识用户的身份证号码、银行卡号、智能卡标识、IMSI、IMEI、MSISDN、IP 地址、用户名、密码、超级用户口令、生物识别特征、数字证书、密钥、好友列表和安全策略；个人安全信息存储在 TF 智能卡上对应的 IC 卡应用文件；

②客户端可以通过 OTA(Over The Air) 的方式安装在移动电话上并进行软件更新和业务下载。所述客户端为用户提供操作界面，将用户需要保护的信息根据不同的安全等级传送到所述安全设备依据不同的安全策略进行安全保护；根据检测到的风险等级动态调整安全等级，当检测到安全攻击时，客户端根据安全策略迅速将安全等级提高，只有通过更高安全等级的认证和鉴权才能使业务继续进行，否则结束业务流程并记录风险记录供事后分析。当检测到安全攻击消失或已排除安全漏洞后，经过稳定性测试，逐步将安全等级恢复正常；

③客户端、TF 智能卡根据所述的个人安全信息进行相互认证和交叉校验，如果签约信息不一致则认证不成功，允许用户重试，重试失败后结束安全流程。对短时间内多次频繁重试的用户，TF 智能卡、客户端对该用户的操作自动锁定，通过超级用户或延时来解锁。认证成功，客户端将用户需要保护的信息，通过 TF 智能卡进行安全保护后，进行存储或发送。

[0026]

以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

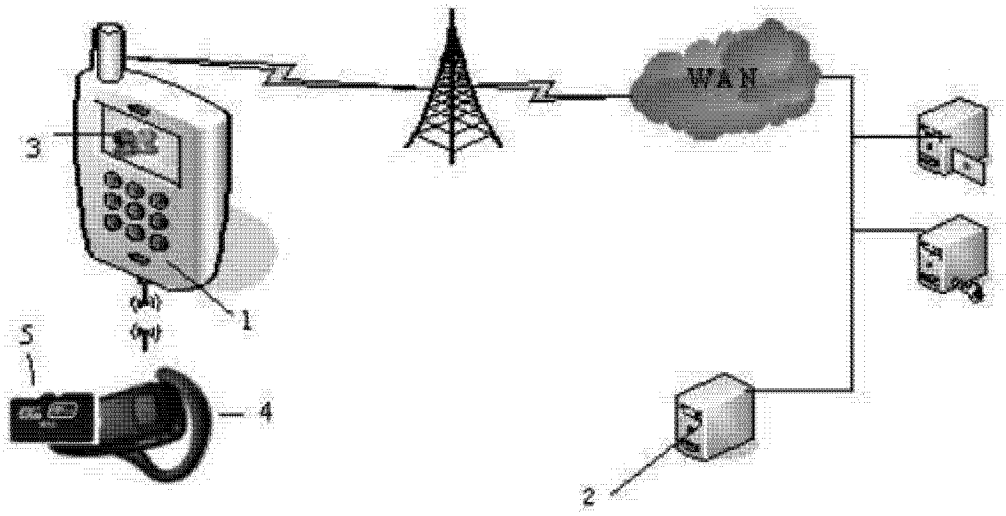

WAN
3
1
5
4
2

图 1

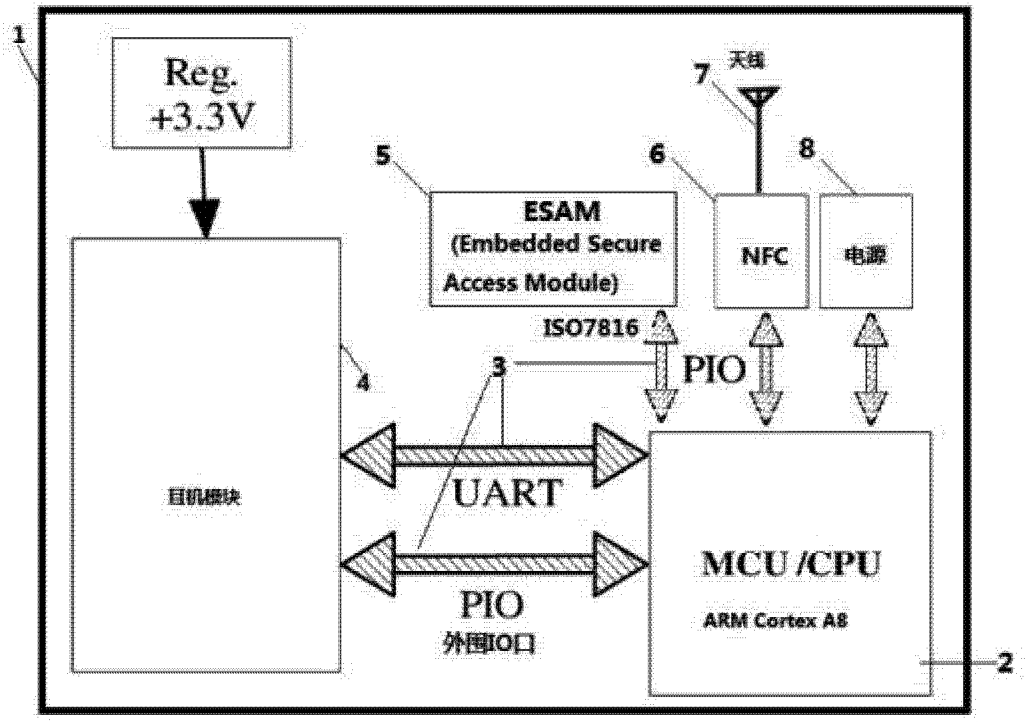

1
Reg.
+3.3V
7
天线
5
6
8
ESAM
(Embedded Secure
Access Module)
NFC
电源
ISO7816
PIO
3
4
目机模块
UART
PIO
外围IO口
MCU /CPU
ARM Cortex A8
2

图 2

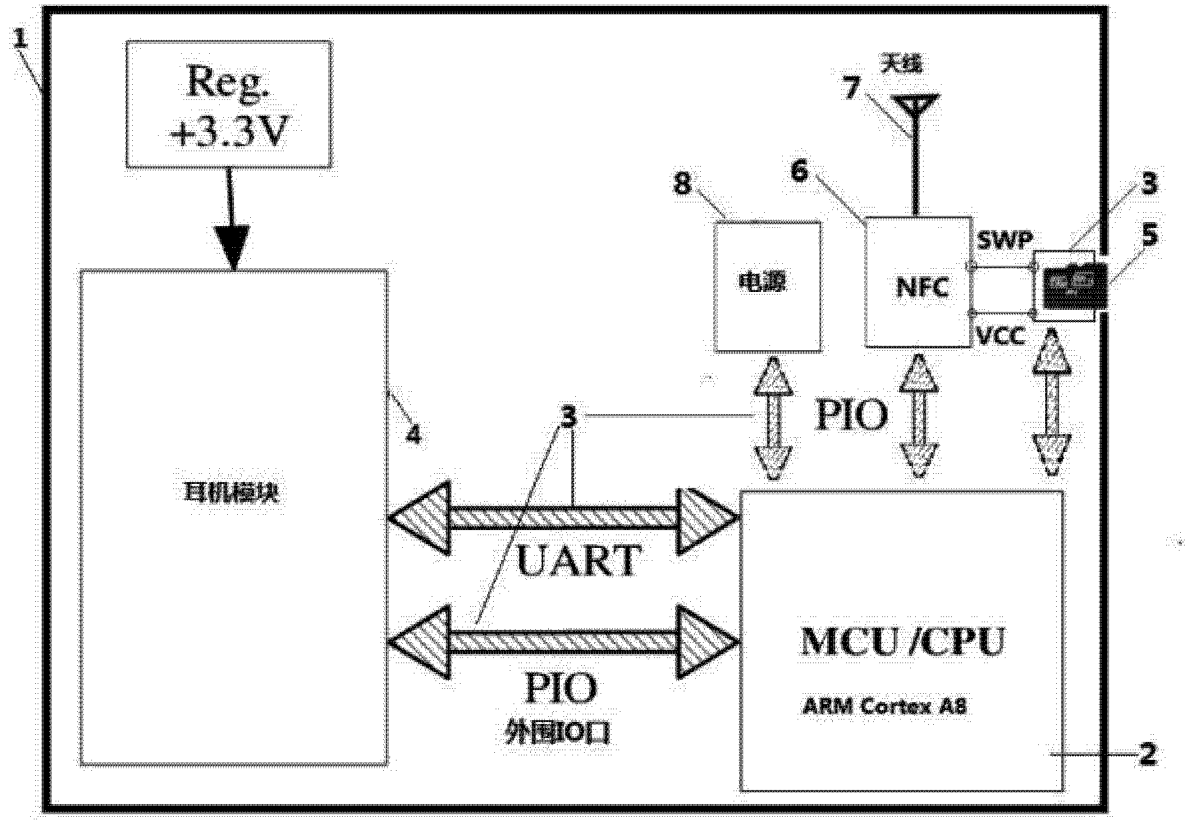

1
Reg.
+3.3V
天线
7
8
6
3
5
电源
NFC
SWP
VCC
PIO
3
4
耳机模块
UART
PIO
外围IO口
MCU /CPU
ARM Cortex A8
2

图 3

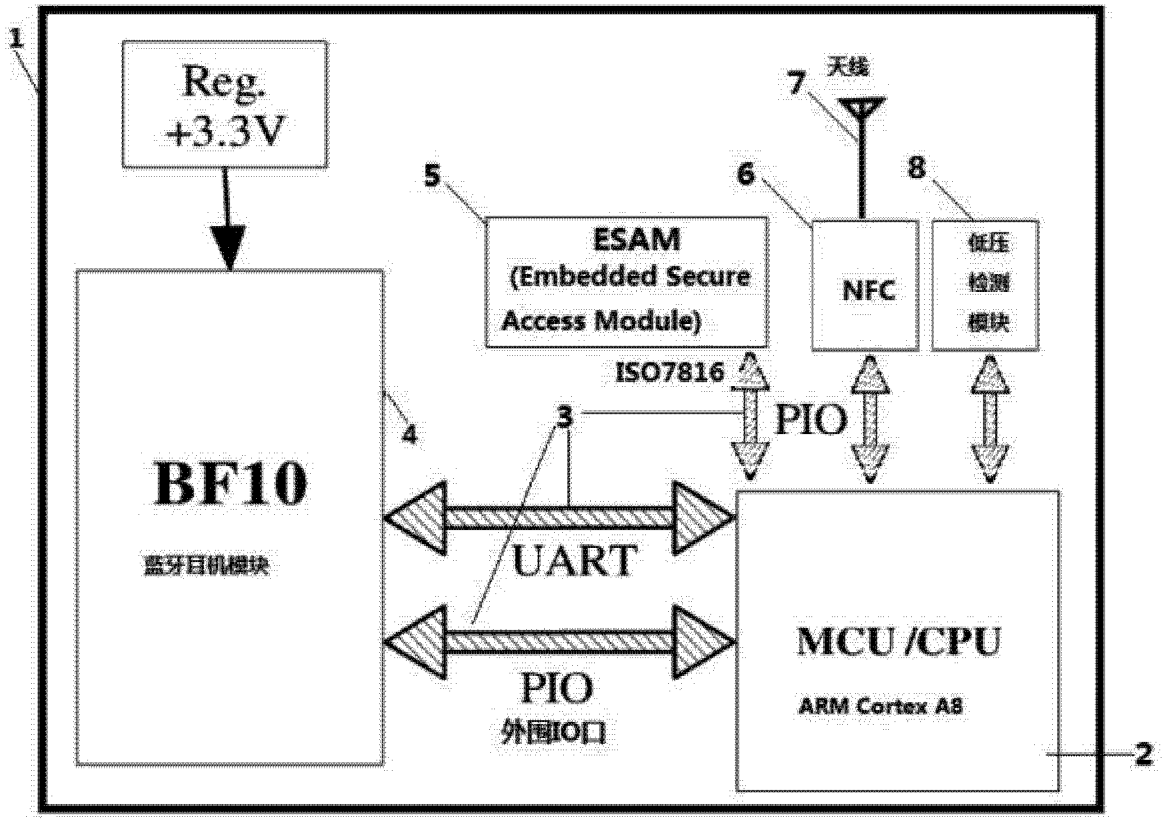

1
Reg.
+3.3V
7
天线
5
6
8
ESAM
(Embedded Secure
Access Module)
NFC
低压
检测
模块
ISO7816
PIO
4
3
BF10
蓝牙耳机模块
UART
MCU /CPU
ARM Cortex A8
PIO
外围IO口
2

图 4

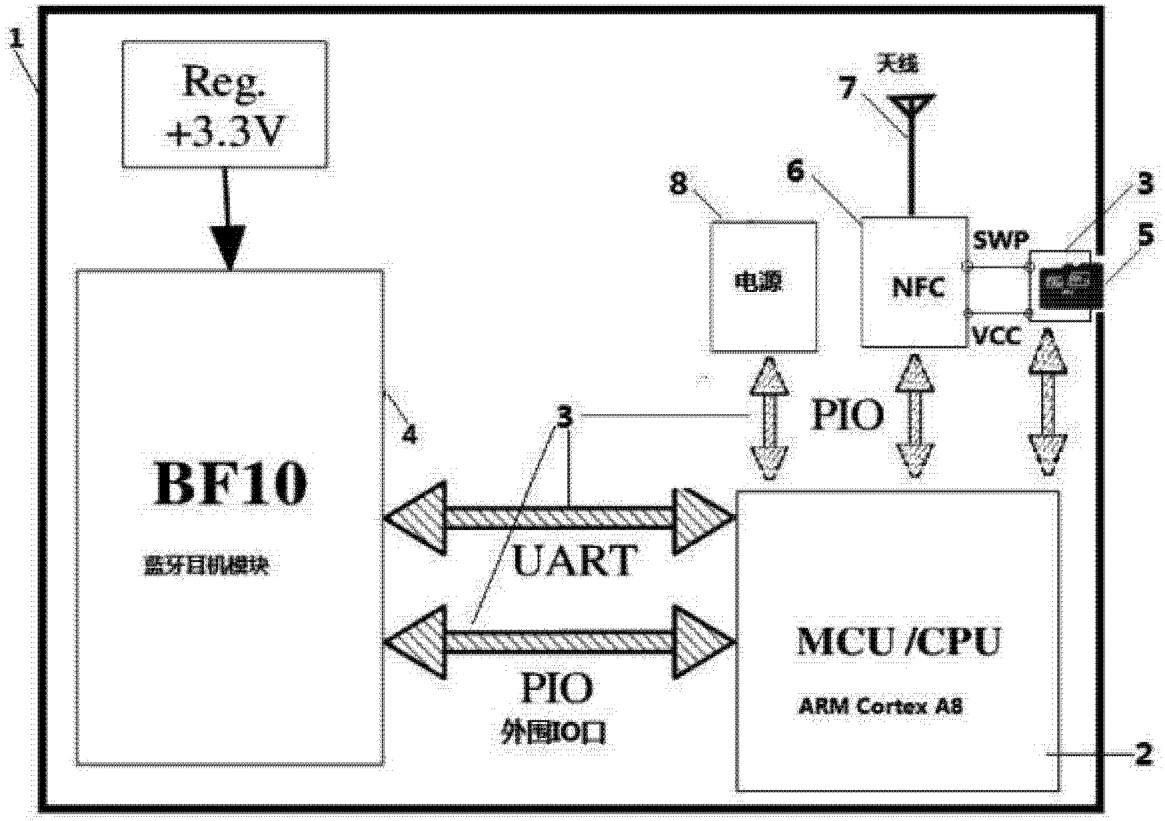

1
Reg.
+3.3V
天线
7
8
6
3
5
电源
NFC
SWP
VCC
PIO
4
3
BF10
蓝牙耳机模块
UART
PIO
外围IO口
MCU /CPU
ARM Cortex A8
2

图 5

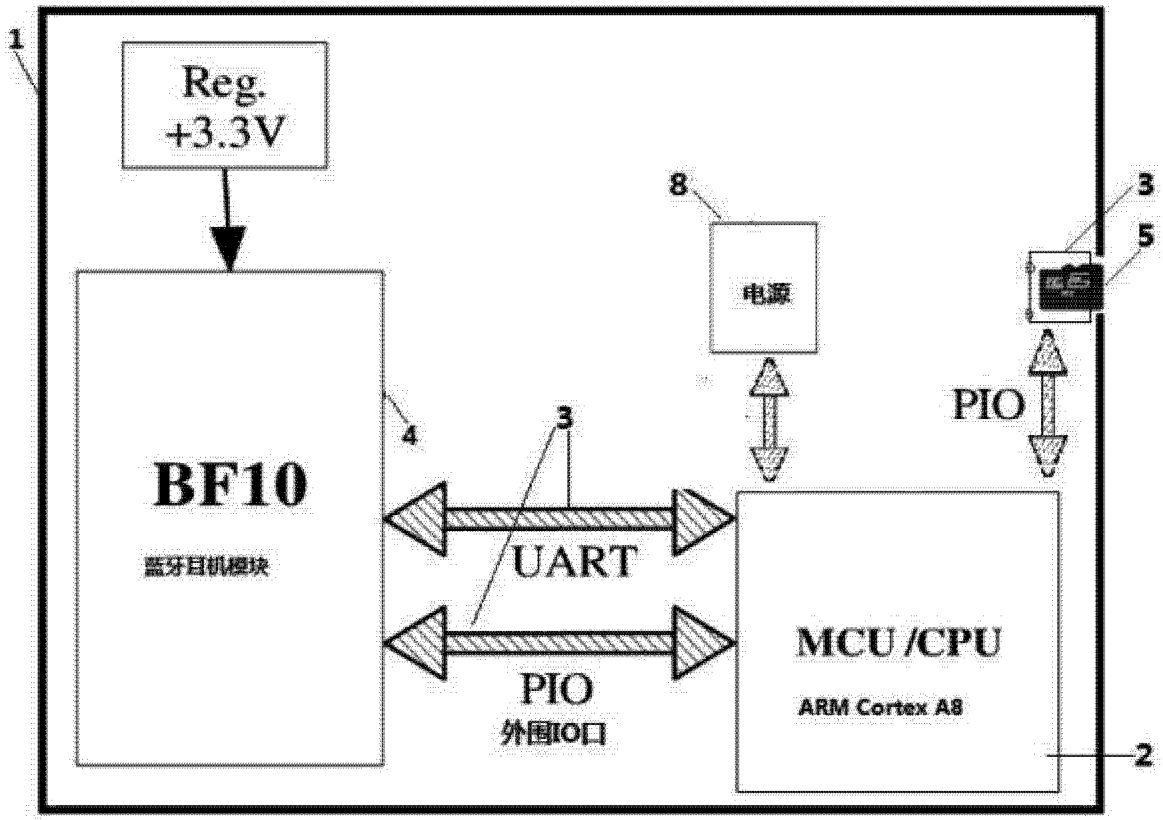

1
Reg.
+3.3V
8
电源
3
5
PIO
4
3
BF10
蓝牙目机模块
UART
PIO
外围IO口
MCU /CPU
ARM Cortex A8
2

图 6

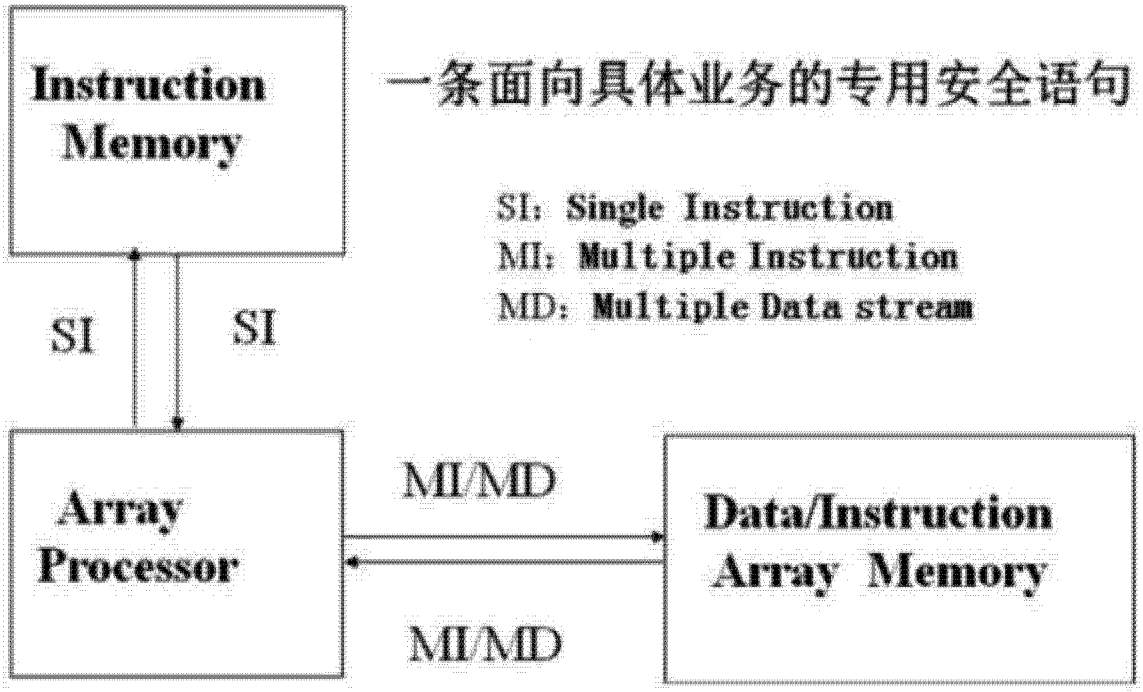

Instruction Memory
一条面向具体业务的专用安全语句
SI: Single Instruction
MI: Multiple Instruction
MD: Multiple Data stream
SI
SI
Array Processor
MI/MD
MI/MD
Data/Instruction Array Memory

图 7