



(12) 发明专利

(10) 授权公告号 CN 101908112 B

(45) 授权公告日 2013. 04. 17

(21) 申请号 201010241690. 1

(22) 申请日 2010. 07. 30

(73) 专利权人 上海华岭集成电路技术股份有限公司

地址 201203 上海市张江郭守敬路 351 号 2 号楼 1 楼

(72) 发明人 祁建华 汤雪飞 王锦 徐惠
刘远华 方华 张杰 凌俭波
叶建明

(74) 专利代理机构 上海思微知识产权代理事务
所(普通合伙) 31237

代理人 郑玮

(51) Int. Cl.

G06F 21/57(2013. 01)

(56) 对比文件

WO 2006/027308 A2, 2006. 03. 16, 全文.

CN 201054140 Y, 2008. 04. 30, 全文.

CN 1702593 A, 2005. 11. 30, 说明书第 2 页
18-21 行, 说明书第 3 页第 7 行至第 6 页第 18 行.

CN 1702593 A, 2005. 11. 30, 说明书第 2 页
18-21 行, 说明书第 3 页第 7 行至第 6 页第 18 行.

徐艳平. TPM 系统 RNG 模块的设计实现. 《中
国优秀硕士学位论文全文数据库(信息科技
辑)》. 2009, 第 4. 4 部分.

徐艳平. TPM 系统 RNG 模块的设计实现. 《中
国优秀硕士学位论文全文数据库(信息科技
辑)》. 2009, 第 4. 4 部分.

审查员 胡雅娟

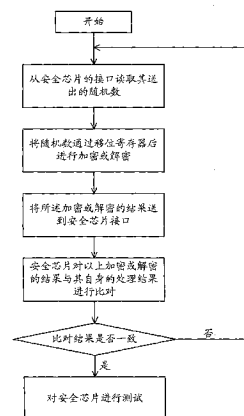
权利要求书 1 页 说明书 5 页 附图 4 页

(54) 发明名称

安全芯片的测试方法与系统

(57) 摘要

本发明揭示了一种安全芯片的测试方法与系统, 利用移位寄存器将芯片内的随机数实时取出进行寄存, 而后独立对移位寄存器内所存储的随机数进行加解密操作。从而, 大大简化了芯片测试平台的设计要求, 降低了测试成本。另外, 移位寄存器可以自动将随机数进行实时完整的寄存, 保证了测试实时性的要求, 提高了安全芯片测试的可操作性与测试效率。以上方法包括: 从安全芯片的接口读取其送出的随机数; 将所述随机数通过移位寄存器后进行加密或解密; 将所述加密或解密的结果送到所述安全芯片接口; 所述安全芯片对所述加密或解密的结果与其自身的处理结果进行比对, 比对结果一致, 则通过身份确认, 对所述安全芯片进行测试。



1. 一种安全芯片的测试方法,其特征是,采用一种安全芯片的测试系统,
所述测试系统包括:

测试平台,以放置所述安全芯片,并将所述安全芯片的接口引出,所述测试平台在芯片测试过程中保持安全芯片处于工作状态;

移位寄存器,与所述测试平台信号连接,读取所述安全芯片的接口送出的随机数;

加解密发生器,信号连接于所述移位寄存器与测试平台,获取所述移位寄存器所接收到的随机数,并对所述随机数进行加密或解密,并将所述加密或解密的结果送到所述安全芯片的接口;

所述安全芯片的测试方法包括:

从所述安全芯片的接口读取其送出的随机数;

将所述随机数通过移位寄存器后进行加密或解密;

将所述加密或解密的结果送到所述安全芯片的接口;

所述安全芯片对所述加密或解密的结果与其自身的处理结果进行比对,比对结果一致,则通过身份确认,对所述安全芯片进行测试;

在以上测试过程中,保持所述安全芯片处于工作状态。

2. 一种安全芯片的测试系统,其特征是,包括:

测试平台,以放置所述安全芯片,并将所述安全芯片的接口引出,所述测试平台在芯片测试过程中保持安全芯片处于工作状态;

移位寄存器,与所述测试平台信号连接,读取所述安全芯片的接口送出的随机数;

加解密发生器,信号连接于所述移位寄存器与测试平台,获取所述移位寄存器所接收到的随机数,并对所述随机数进行加密或解密,并将所述加密或解密的结果送到所述安全芯片的接口,所述加解密发生器包括控制单元以及分别与所述控制单元信号连接的存储单元、算法运算单元和接口单元,其中,

所述存储单元存储算法运算单元运算所需的密钥;

所述算法运算单元在所述控制单元的控制下,通过所述接口单元获取所述随机数,并获取所述存储单元内的密钥,并对所述随机数进行加密或解密运算,并将所述加密或解密的结果通过所述接口单元送到所述安全芯片的接口。

3. 根据权利要求2所述的安全芯片的测试系统,其特征是,所述加解密发生器与所述移位寄存器集成在一起。

4. 一种安全芯片的测试系统,其特征是,包括:

测试平台,以放置所述安全芯片,并将所述安全芯片的接口引出,所述测试平台在芯片测试过程中保持安全芯片处于工作状态;

移位寄存器,与所述测试平台信号连接,读取所述安全芯片的接口送出的随机数;

加解密工作站,信号连接于所述移位寄存器,获取所述移位寄存器所接收到的随机数,并对所述随机数进行加密或解密,并将所述加密或解密的结果送到所述安全芯片的接口,所述加解密工作站为计算机,其内设置有存储器,且所述存储器内存储有加解密运算程序与密钥,且

所述计算机通过其接口接收所述移位寄存器所接收到的随机数,并调用存储器内的加解密运算程序与密钥,对所述随机数进行加密或解密,并将所述加密或解密的结果送到所述安全芯片的接口。

安全芯片的测试方法与系统

技术领域

[0001] 本发明涉及信息安全技术领域,特别是涉及半导体测试领域中的一种安全芯片的测试方法与系统。

背景技术

[0002] 随着信息时代的到来,特别是随着计算机和网络技术的发展,信息安全技术日益凸显其重要性。传统的信息安全措施是以防火墙技术为代表的被动防卫型方案,但是,目前 PC 平台存在的不安全问题,绝大多数都是因为 PC 和操作系统在体系结构上存在着设计弱点,因此传统安全措施这种治标不治本的做法,使得众多的安全问题多年以来一直没有很好的解决。为了从根本上解决安全问题,可信计算机联盟 (TCPA) 提出了可信赖平台模块 (TPM) 的概念。

[0003] 1999 年,由 Intel、IBM、HP、Microsoft 等发起的可信计算机联盟 (TCPA) 组织在推动构建一个可信赖的计算环境,这个组织定义了一个平台设备认证的构架,以及嵌入在主板上的可信赖平台模块 (TPM) 和上层软件中间件 (TSS) 的规范。2003 年 TCPA 重组为可信计算机组 (TCG),对 TPM 和 TSS 进行完善补充。

[0004] 具体,请参考图 1,其为一种 TCG 要求的安全芯片体系的结构示意图。

[0005] 如图所示,该芯片包括用于控制的微处理器 (MCU) 模块 10、加解密模块 20、存储模块 30、输入输出 (I/O) 接口模块 40 和用于检测安全芯片电源的电源检测模块 50,这些模块通过芯片内部的总线 60 相互连接。其中,微处理器模块 10 根据从 I/O 接口模块 40 收到的指令对加解密模块 20 进行控制,根据接收到的指令将指令处理结果传送给 I/O 接口模块 40,或者直接从存储模块 30 中取出密钥等传送给 I/O 接口模块 40。加解密模块 20 在微处理器模块 10 的控制下,从存储模块 30 内获取密钥,应用密钥对接收到的数据进行加解密,并将加解密后的数据通过 I/O 接口模块 40 传输给外部设备。I/O 接口模块 40 用于传输芯片和外部设备之间的数据或指令。

[0006] 通常,加解密模块 20 由算法模块 21、随机数发生器模块 22 和密钥生成模块 23 组成,其中随机数发生器模块 22 在微处理器模块 10 的控制下,生成随机数以便产生随机密钥;密钥生成模块 23 利用随机数发生器模块 22 产生的随机数,生成算法模块 21 进行运算所需的密钥;算法模块 21 在微处理器模块 10 的控制下,对接收到的数据进行相应的算法运算,并将计算结果传送给 I/O 接口模块 40。例如,如果算法模块 21 为 RSA 模块,则对接收到的数据进行 RSA 运算,如果是 3DES 模块,则对接收到的数据进行 3DES 运算。存储模块 30 往往由用于存储密钥数据、用户数据和程序的非易失性存储器和用于存储临时数据和临时程序的易失性存储器构成。

[0007] 可见,TPM 安全芯片实际上是一个含有密码运算部件和存储部件的小型片上系统,通过提供密钥管理和配置管理等特性,完成计算平台的可靠性认证、用户身份认证、数字签名、信任链的建立等功能,为各种安全应用提供了功能性强大的平台。可以说,TPM 技术在其应用中体现了巨大的优势,然而,却为半导体测试带来了困难。

[0008] 具体而言,在对安全芯片进行性能测试时,由于 TPM 的存在,无法绕开身份确认这一环节。即使有些安心芯片加入了常规测试可以绕开身份确认这一环节的设计,但是对于充分测试而言,身份确认始终是无法绕开的。对于,现有的测试设备,由于无法进行身份确认而无法对安全芯片进行测试。而高档设备为了配合安全芯片内的加密机制,不得不增加设许多软硬件设施,来构建测试平台,而芯片内的随机数发生器每次产生的随机数都是不同的,这些测试平台往往难以满足实时性的要求,因此测试效率比较低。

发明内容

[0009] 本发明的目的在于提供一种安全芯片的测试方法与系统,以对安全芯片进行测试,且满足其身份确认实时性的需求,提高测试效率。

[0010] 为解决以上技术问题,本发明提供一种安全芯片的测试方法,包括:从所述安全芯片的接口读取其送出的随机数;将所述随机数通过移位寄存器后进行加密或解密;将所述加密或解密的结果送到所述安全芯片接口;所述安全芯片对所述加密或解密的结果与其自身的处理结果进行比对,比对结果一致,则通过身份确认,对所述安全芯片进行测试。

[0011] 进一步的,在以上测试过程中,保持所述安全芯片处于工作状态。

[0012] 本发明另提供一种安全芯片的测试系统,其包括:测试平台,以放置所述安全芯片,并将所述安全芯片的接口引出;移位寄存器,与所述测试平台信号连接,读取所述安全芯片的接口送出的随机数;加解密发生器,信号连接于所述移位寄存器与测试平台,获取所述移位寄存器所接收到的随机数,并对所述随机数进行加密或解密,并将所述加密或解密的结果送到所述安全芯片接口。

[0013] 进一步的,所述测试平台在芯片测试过程中保持安全芯片处于工作状态。

[0014] 进一步的,所述加解密发生器与所述移位寄存器集成在一起。

[0015] 进一步的,所述加解密发生器包括控制单元以及分别与所述控制单元信号连接的存储单元、算法运算单元和接口单元,其中,所述存储单元存储算法运算单元运算所需的密钥;所述算法运算单元在所述控制单元的控制下,通过所述接口单元获取所述随机数,并获取所述存储单元内的密钥,并对所述随机数进行加密或解密运算,并将所述加密或解密的结果通过所述接口单元送到所述安全芯片接口。

[0016] 本发明还提供一种安全芯片的测试系统,其包括:测试平台,以放置所述安全芯片,并将所述安全芯片的接口引出;移位寄存器,与所述测试平台信号连接,读取所述安全芯片的接口送出的随机数;加解密工作站,信号连接于所述移位寄存器,获取所述移位寄存器所接收到的随机数,并对所述随机数进行加密或解密,并将所述加密或解密的结果送到所述安全芯片接口。

[0017] 进一步的,所述测试平台在芯片测试过程中保持安全芯片处于工作状态。

[0018] 进一步的,所述加解密工作站为计算机,其内设置有存储器,且所述存储器内存储有加解密运算程序与密钥,且所述计算机通过其接口接收所述移位寄存器所接收到的随机数,并调用存储器内的加解密运算程序与密钥,对所述随机数进行加密或解密,并将所述加密或解密的结果送到所述安全芯片接口。

[0019] 综上所述,以上安全芯片测试方法与系统,利用移位寄存器将芯片内的随机数实时取出进行寄存。而后独立对移位寄存器内所存储的随机数进行加解密操作。从而,大大

简化了芯片测试平台的设计要求,甚至可以在原有测试平台上进行测试,从而无需改进测试平台,降低了测试成本。另外,每一次对芯片开始新的测试,都无需操作人员考虑芯片所产生的随机数的随机性问题,移位寄存器可以自动将随机数进行实时完整的寄存,保证了测试实时性的要求,提高了安全芯片测试的可操作性与测试效率。

附图说明

- [0020] 图 1 为一种 TCG 要求的安全芯片体系的结构示意图 ;
- [0021] 图 2 为本发明实施列一所提供的安全芯片的测试系统的结构示意图 ;
- [0022] 图 3 为本发明实施列二所提供的安全芯片的测试系统的结构示意图 ;
- [0023] 图 4 为本发明实施列二所提供的安全芯片的测试系统另一种实现方式的结构示意图 ;
- [0024] 图 5 为本发明实施列二所提供的安全芯片的测试系统的加解密发生器的结构示意图 ;
- [0025] 图 6 为本发明一实施列所提供的移位寄存器的安全芯片测试方法的流程示意图。

具体实施方式

[0026] 为使本发明的目的、特征更明显易懂,下面结合附图对本发明的具体实施方式作进一步的说明。

[0027] 实施列一 :

[0028] 请参考图 2,其为本发明实施列一所提供的安全芯片的测试系统的结构示意图,如图所示。该系统包括测试平台 10 以及与测试平台 10 信号连接的移位寄存器 20 和加解密工作站 30,其中测试平台 10 用以放置待测试的安全芯片 40,并将安全芯片 40 的接口信号引出,以便于在测试时实时获取安全芯片 40 的接口送出的信号。移位寄存器 20 读取安全芯片 40 的接口送出的随机数,将其暂存于其中 ;加解密工作站 30 获取移位寄存器 20 所接收到的随机数,并对该随机数进行加密或解密,并将所述加密或解密的结果送到安全芯片的接口。其中,测试平台 10 在芯片测试过程中保持安全芯片 40 处于工作状态。

[0029] 这样,安全芯片在接收到以上加密或解密结果时,会自动与其内加解密模块的处理结果进行比对,如果比对结果一致,则通过身份确认,利用对安全芯片进行测试。可见,以上安全芯片的测试系统仅需加设一移位寄存器,以将安心芯片产生的随机数进行寄存,而后只要保证芯片处于工作状态,便可以独立对移位寄存器内所存储的随机数进行加解密操作。这样,大大简化了芯片测试平台的设计要求,降低了测试成本。而移位寄存器的引入,又避免了安全芯片内随机数产生的随机性对测试带来的影响。这是因为移位寄存器中的数据可以在移位脉冲的作用下一次逐位右移或左移,这样,可以实时将芯片内所产生的随机数完整取出,满足了测试实时性的要求,提高了测试效率。另外,移位寄存器的输入或输出可以是串行也可以是并行,因此,可以灵活配合芯片随机数的输出形式与加解密工作站 30 所需的输入形式。

[0030] 在本实施列中,加解密工作站 30 为计算机,通过软件方式来实现加解密运算,具体,该计算机 30 内设置有存储器,且存储器内存储有加解密运算程序与密钥,且计算机 30 通过其接口接收移位寄存器 20 所接收到的随机数,并调用存储器内的加解密运算程序与

密钥,对所述随机数进行加密或解密,并将加密或解密的结果送到安全芯片接口。需要说明的是,计算机 30 与测评平台 10 和移位寄存器 20 之间的连接方式不限于有线或者无线,本领域技术人员可根据需要选取。

[0031] 为了进一步降低成本,可以利用 FPGA 技术将以上测试系统硬件化。具体请参考以下实施列。

[0032] 实施列二:

[0033] 请参考图 3,其为本发明实施列二所提供的安全芯片的测试系统的结构示意图,如图所示。该系统包括测试平台 10 以及与测试平台 10 信号连接移位寄存器 20 以及加解密发生器 50。其中测试平台 10 用以放置待测试的安全芯片 40,并将安全芯片 40 的接口信号引出,以便于在测试时实时获取安全芯片 40 的接口送出的信号。移位寄存器 20 读取安全芯片 40 的接口送出的随机数,将其暂存于其中;加解密发生器 50 获取移位寄存器 20 所接收到的随机数,并对该随机数进行加密或解密,并将所述加密或解密的结果送到安全芯片 40 的接口。其中,测试平台 10 在芯片测试过程中保持安全芯片 40 处于工作状态。

[0034] 这样,安全芯片在接收到以上加密或解密结果时,会自动与其内加解密模块的处理结果进行比对,如果比对结果一致,则通过身份确认,利用对安全芯片进行测试。可见,以上安全芯片的测试系统仅需加设一移位寄存器,以将安心芯片产生的随机数进行寄存,而后只要保证芯片处于工作状态,便可以独立对移位寄存器内所存储的随机数进行加解密操作。这样,大大简化了芯片测试平台的设计要求,降低了测试成本。而移位寄存器的引入,又避免了安全芯片内随机数产生的随机性对测试带来的影响。这是因为移位寄存器中的数据可以在移位脉冲的作用下一次逐位右移或左移,这样,可以实时将芯片内所产生的随机数完整取出,满足了测试实时性的要求,提高了测试效率。另外,移位寄存器的输入或输出可以是串行也可以是并行,因此,可以灵活配合芯片随机数的输出形式与加解密发生器 50 所需的输入形式。

[0035] 在本实施列中,加解密发生器 50 是利用硬件方式来实现的,具体请参考图 5,其给出了加解密发生器 50 的一种实现方式。如图所示,该加解密发生器 50 包括控制单元 510 以及分别与控制单元 510 信号连接的存储单元 520、算法运算单元 530 和接口单元 540。其中,存储单元 520 用以存储算法运算单元 530 运算所需的密钥;算法运算单元 530 则在控制单元的控制下,通过接口单元 540 获取移位寄存器 20 所接收到的随机数,并获取存储单元 520 内的密钥,并利用密钥对随机数进行加密或解密运算,并将加密或解密的结果通过接口单元 540 送到安全芯片 40 的接口。

[0036] 需要说明的是,加解密发生器 50 与移位寄存器 20 可以集成在一起。具体请参考图 4,此时,加解密发生器 50 与移位寄存器 20 可以共用一个接口单元 60,来与测试平台 10 进行通信。

[0037] 从以上两个实施列可以看出,由于移位寄存器的引入,可以将安全芯片所产生的随机数进行寄存,而后只要保证芯片处于工作状态,便可以独立对移位寄存器内所存储的随机数进行加解密操作。从而,大大简化了芯片测试平台的设计要求,降低了测试成本。另外,每一次对芯片开始新的测试,都无需操作人员考虑芯片所产生的随机数的随机性问题,移位寄存器可以自动将随机数进行实时完整的寄存,保证了测试实时性的要求,提高了安全芯片测试的可操作性与测试效率。

[0038] 下面结合图 6, 来详细描述引入了移位寄存器的安全芯片测试方法。如图所示, 本实施例提供了一种安全芯片的测试方法, 其包括如下步骤:

[0039] S1: 从安全芯片的接口读取其送出的随机数;

[0040] S2: 将随机数通过移位寄存器后进行加密或解密;

[0041] S3: 将所述加密或解密的结果送到安全芯片接口;

[0042] S4: 安全芯片对以上加密或解密的结果与其自身的处理结果进行比对, 比对结果一致, 则通过身份确认, 如此, 便可以对安全芯片进行测试。

[0043] 其中, 在以上测试过程中, 保持安全芯片处于工作状态。

[0044] 综上所述, 以上安全芯片测试方法与系统, 利用移位寄存器将芯片内的随机数实时取出进行寄存。而后独立对移位寄存器内所存储的随机数进行加解密操作。从而, 大大简化了芯片测试平台的设计要求, 甚至可以在原有测试平台上进行测试, 从而无需改进测试平台, 降低了测试成本。另外, 每一次对芯片开始新的测试, 都无需操作人员考虑芯片所产生的随机数的随机性问题, 移位寄存器可以自动将随机数进行实时完整的寄存, 保证了测试实时性的要求, 提高了安全芯片测试的可操作性与测试效率。

[0045] 以上显示和描述了本发明的基本原理、主要特征和本发明的优点。本领域的技术人员应该了解, 本发明不受上述实施例的限制, 上述实施例和说明书中描述的只是本发明的原理, 在不脱离本发明精神和范围的前提下本发明还会有各种变化和改进, 这些变化和进步都落入要求保护的本发明的范围内。本发明要求的保护范围由所附的权利要求书及其等同物界定。

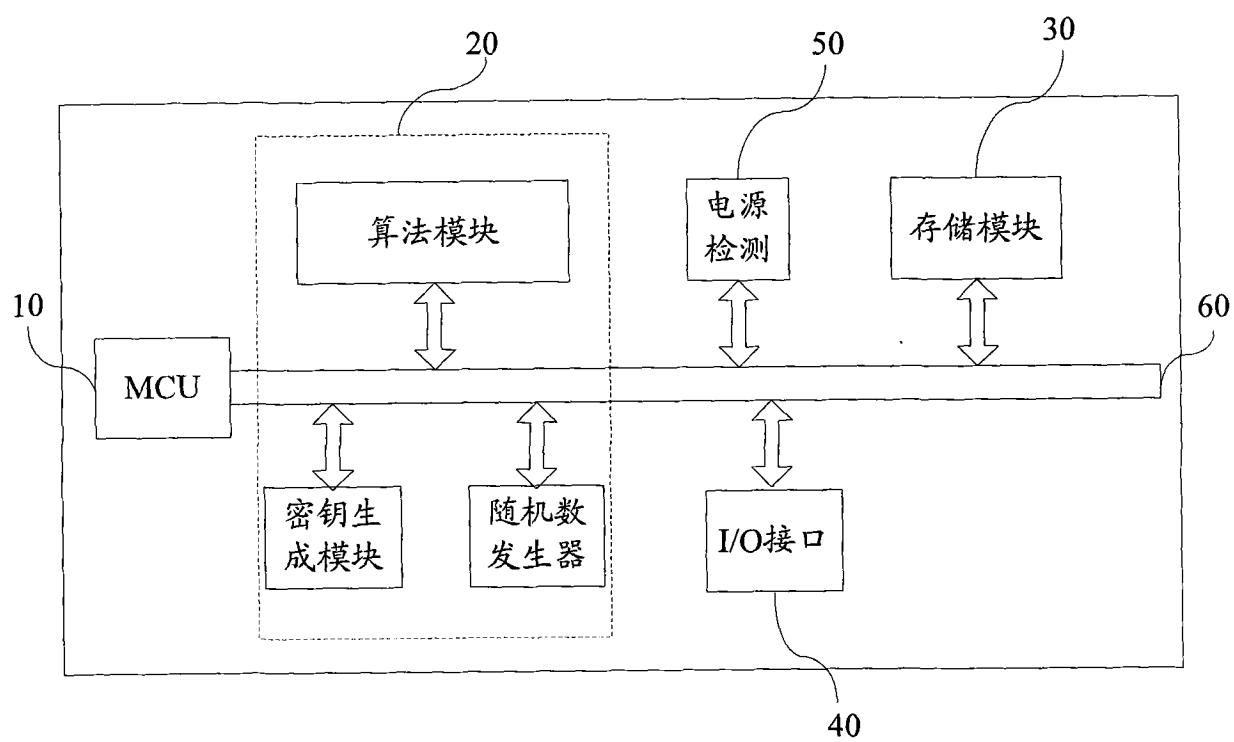


图 1

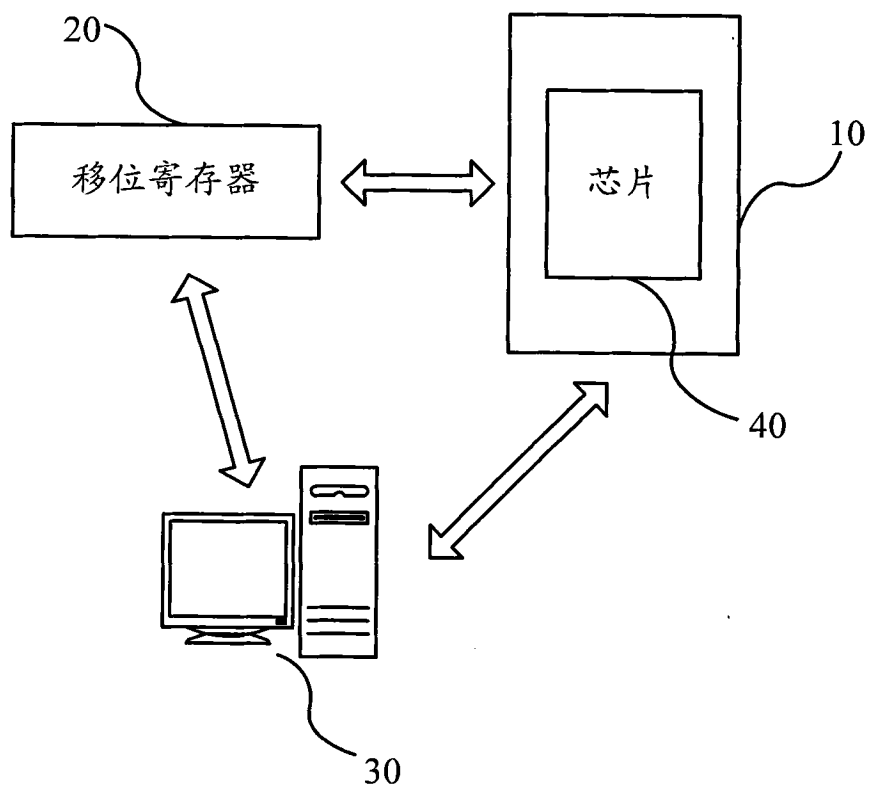


图 2

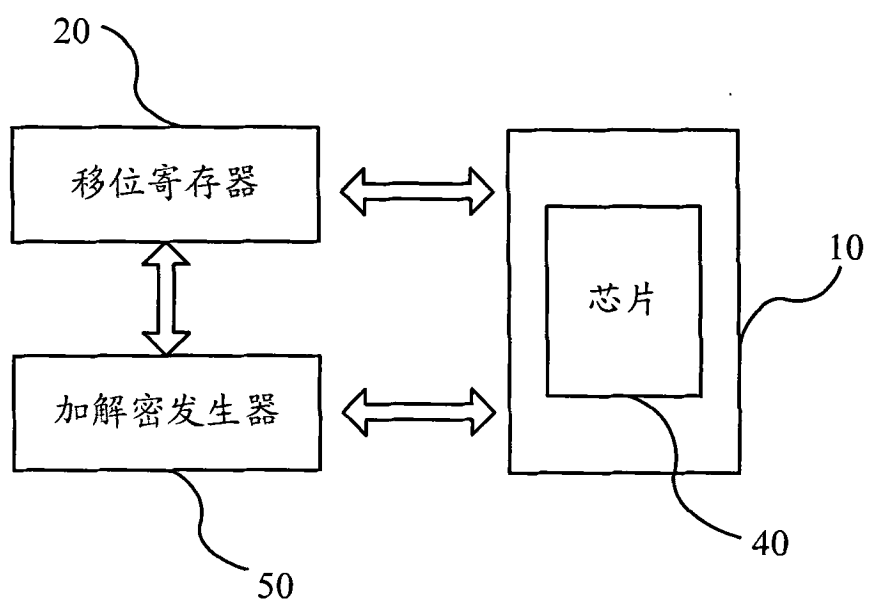


图 3

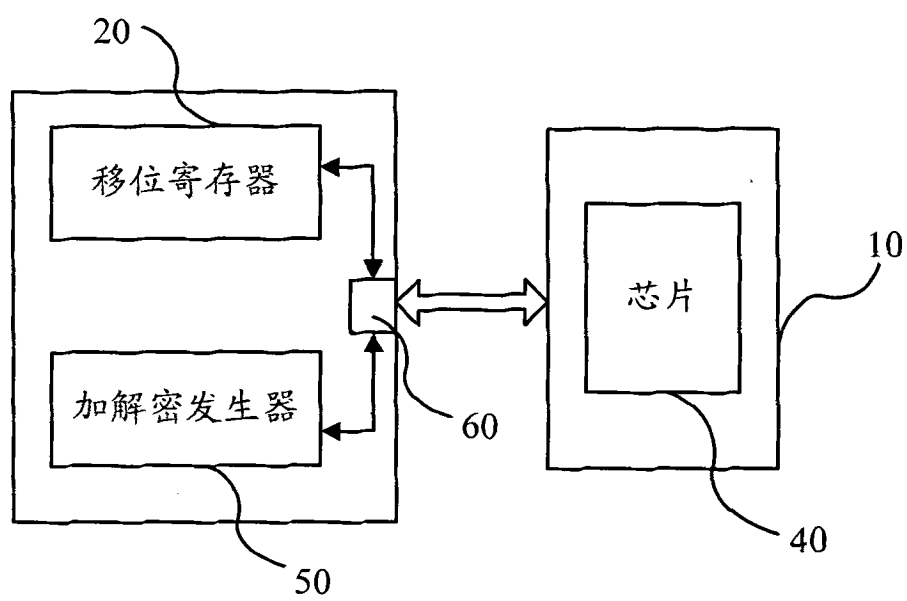


图 4

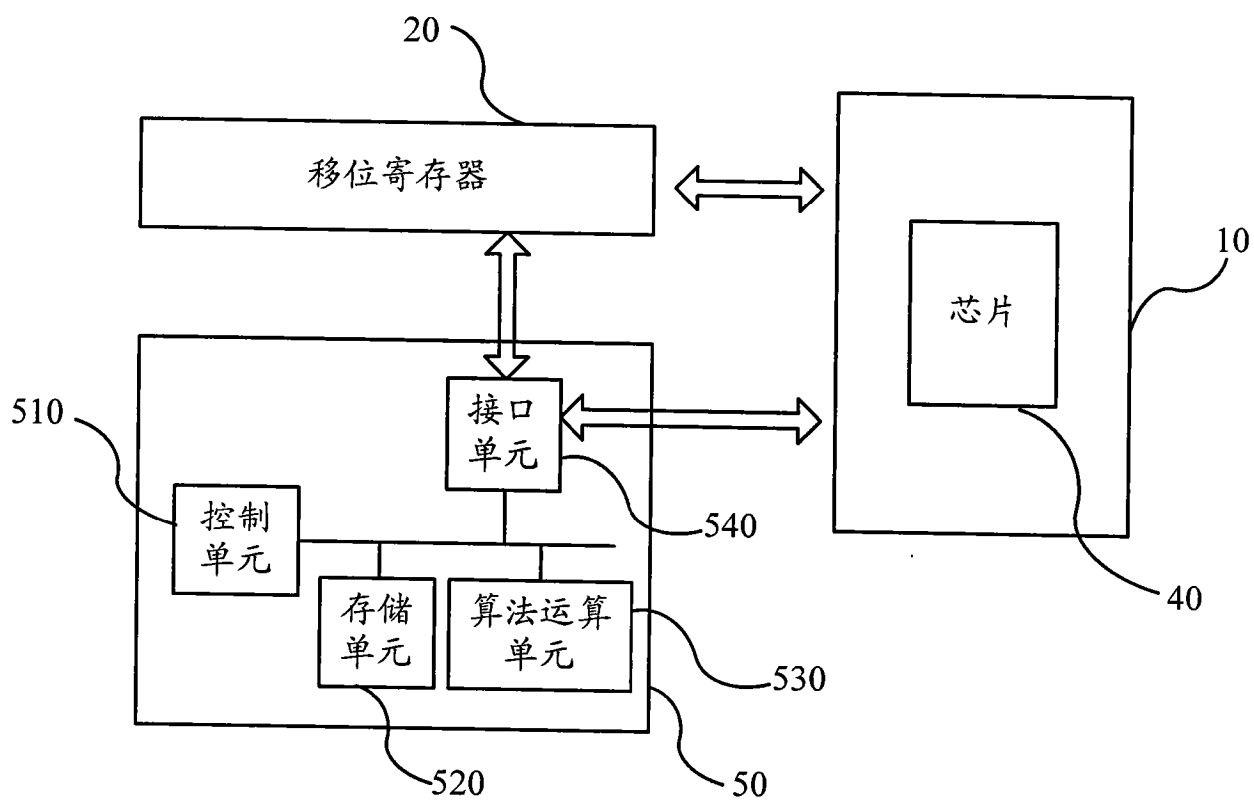


图 5

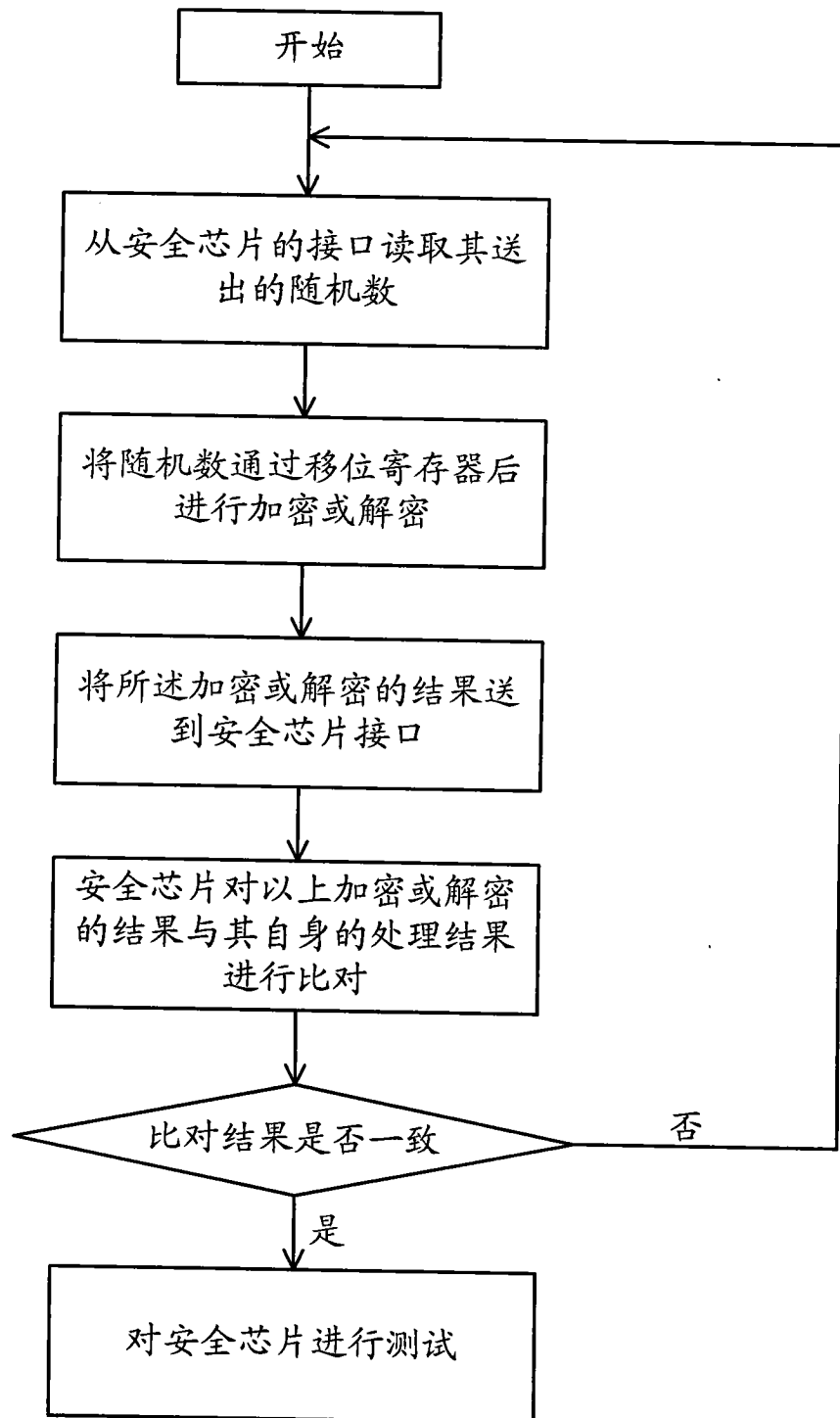


图 6