



(12) 发明专利申请

(10) 申请公布号 CN 103150524 A

(43) 申请公布日 2013. 06. 12

(21) 申请号 201310035090. 3

(22) 申请日 2013. 01. 30

(71) 申请人 华中科技大学

地址 430074 湖北省武汉市洪山区珞瑜路
1037 号

(72) 发明人 刘政林 詹鑫 刘世生 张瑞
邹雪城

(74) 专利代理机构 华中科技大学专利中心
42201

代理人 朱仁玲

(51) Int. Cl.

G06F 21/76(2013. 01)

G06F 21/64(2013. 01)

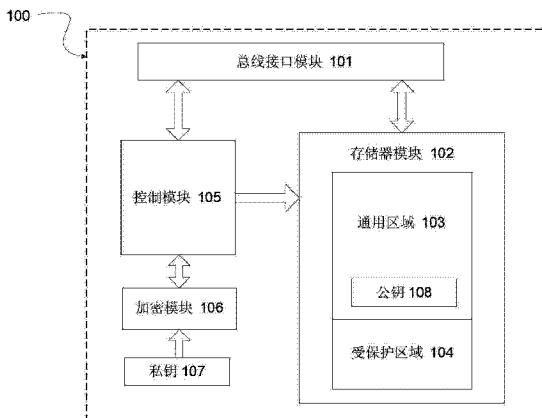
权利要求书2页 说明书6页 附图3页

(54) 发明名称

一种安全存储器芯片、系统及其认证方法

(57) 摘要

本发明公开了一种安全存储器芯片、系统及其认证方法；该安全存储器芯片包括总线接口模块、存储器模块、控制模块、加密模块和私钥；控制模块和存储器模块共用一个总线接口模块，加密模块和存储器模块均与控制模块相连，私钥与加密模块相连；存储器模块的存储区域包括通用区域和受保护区域，通用区域用于存储软件程序，受保护区域用于存储敏感数据；公钥存储于通用区域内。本发明提供的安全存储器芯片具备更高的安全性；安全存储器芯片中的存储区域分为通用区域和受保护区域，由同一种存储介质构成，具有统一的地址空间，方便微处理器的访问；既保证了敏感数据的安全性，又提高了系统的运行速度。



1. 一种安全存储器芯片，其特征在于，包括总线接口模块(101)、存储器模块(102)、控制模块(105)、加密模块(106)和私钥(107)；控制模块(105)和存储器模块(102)共用一个总线接口模块(101)，加密模块(106)和存储器模块(102)均与控制模块(105)相连，私钥(107)与加密模块(106)相连；存储器模块(102)的存储区域包括通用区域(103)和受保护区域(104)，通用区域(103)用于存储软件程序，受保护区域(104)用于存储敏感数据；公钥(108)存储于通用区域(103)内。

2. 如权利要求1所述的安全存储器芯片，其特征在于，所述通用区域(103)定义为访问不受限制的区域；受保护区域(105)定义为只有通过认证后才可访问的区域；敏感数据定义为用户需要保护的关键数据。

3. 如权利要求1所述的安全存储器芯片，其特征在于，所述安全存储器芯片(100)产生质询并发送给外部的微处理器(200)，微处理器(200)采用公钥(108)对质询进行加密，并将加密后的质询传回安全存储器芯片(100)；安全存储器芯片(100)采用私钥(107)对加密的质询进行解密，并将解密结果与原质询进行比较；当解密结果与原质询相同时，允许微处理器(200)访问安全存储器芯片(100)的受保护区域(104)；当解密结果与原质询不同时，禁止微处理器(200)访问安全存储器芯片(100)的受保护区域(104)。

4. 如权利要求1所述的安全存储器芯片，其特征在于，微处理器(200)产生质询并采用公钥(108)对质询进行加密，将加密后的质询发送给安全存储器芯片(100)；安全存储器芯片(100)采用私钥(107)对加密后的质询进行解密，并将解密后的质询发送给微处理器(200)；微处理器(200)将安全存储器芯片(100)解密后的质询和原质询进行比较；当解密后的质询与原质询相同时，微处理器(200)继续执行程序；当解密后的质询与原质询不同时，微处理器(200)终止执行程序。

5. 如权利要求1所述的安全存储器芯片，其特征在于，所述加密模块(107)采用非对称加密算法对质询进行加密。

6. 一种安全存储器系统，包括安全存储器芯片，微处理器和用于所述微处理器与所述安全存储器芯片之间数据交换的总线，其特征在于，所述安全存储器芯片为权利要求1-5任一项所述的安全存储器芯片。

7. 一种安全存储器的认证方法，其特征在于，包括下述步骤：

S301：安全存储器芯片(100)中的控制模块(105)生成一个质询M1并发送给微处理器(200)；

S302：微处理器(200)采用公钥(108)对质询M1进行加密并获得加密后的质询C1；微处理器(200)将加密后的质询C1发送给安全存储器芯片(100)；

S303：安全存储器芯片(100)采用私钥(107)对加密后的质询C1进行解密并获得解密后的质询M1'；

S304：安全存储器芯片(100)将解密后的质询M1'与原质询M1进行比较，当解密后的质询M1'与原质询M1相同时进入步骤305；当解密后的质询M1'与原质询M1不同时结束；

S305：安全存储器芯片(100)赋予微处理器(200)访问受保护区域(104)的权限。

8. 如权利要求7所述的认证方法，其特征在于，还包括下述步骤：

S401：微处理器(200)生成一个质询M2并对质询M2进行加密后获得加密后的质询C2；微处理器(200)将加密后的质询C2发送给安全存储器芯片(100)；

S402 :安全存储器芯片(100)采用私钥(107)对加密后的质询 C2 进行解密并获得解密后的质询 M2' ;安全存储器芯片(100)将解密后的质询 M2' 发送给微处理器(200)；

S403 :微处理器(200)将解密后的质询 M2' 与原质询 M2 进行比较,当解密后的质询 M2' 与原质询 M2 相同时进入步骤 S404,当解密后的质询 M2' 与原质询 M2 不同时,微处理器(200)终止执行软件程序；

S404 :微处理器(200)继续执行软件程序。

9. 一种安全存储器的认证方法,其特征在于,包括下述步骤 :

S401 :微处理器(200)生成一个质询 M2 并对质询 M2 进行加密后获得加密后的质询 C2 ;微处理器(200)将加密后的质询 C2 发送给安全存储器芯片(100)；

S402 :安全存储器芯片(100)采用私钥(107)对加密后的质询 C2 进行解密并获得解密后的质询 M2' ;安全存储器芯片(100)将解密后的质询 M2' 发送给微处理器(200)；

S403 :微处理器(200)将解密后的质询 M2' 与原质询 M2 进行比较,当解密后的质询 M2' 与原质询 M2 相同时进入步骤 S404,当解密后的质询 M2' 与原质询 M2 不同时,微处理器(200)终止执行软件程序；

S404 :微处理器(200)继续执行软件程序。

10. 如权利要求 9 所述的认证方法,其特征在于,还包括 :

S301 :安全存储器芯片(100)中的控制模块(105)生成一个质询 M1 并发送给微处理器(200)；

S302 :微处理器(200)采用公钥(108)对质询 M1 进行加密并获得加密后的质询 C1 ;微处理器(200)将加密后的质询 C1 发送给安全存储器芯片(100)；

S303 :安全存储器芯片(100)采用私钥(107)对加密后的质询 C1 进行解密并获得解密后的质询 M1' ；

S304 :安全存储器芯片(100)将解密后的质询 M1' 与原质询 M1 进行比较,当解密后的质询 M1' 与原质询 M1 相同时进入步骤 305 ;当解密后的质询 M1' 与原质询 M1 不同时结束；

S305 :安全存储器芯片(100)赋予微处理器(200)访问受保护区域(104)的权限。

一种安全存储器芯片、系统及其认证方法

技术领域

[0001] 本发明属于数字集成电路领域,更具体地,涉及一种安全存储器芯片、系统及其认证方法。

背景技术

[0002] 随着集成电路芯片技术的飞速发展,电子产品设计业也越来越开放,很多硬件解决方案已经成为公开的资料,产品设计者的核心技术往往集中在嵌入式软件内。许多公司,不仅一些“地下”公司或者说是“山寨”公司,而且一些大公司,也会对竞争对手销量大的产品进行研究破解其知识产权。实力强的公司在研究破解的基础上进行升级或者进行相关的创新,以提高产品性能,增强自身产品的竞争力,击败对手。实力一般的“山寨”公司,则是直截了当的对别人产品进行破解、翻造、冠名自己公司的名字后直接上市,以比同类产品价格低廉且功能俱全的优势,从而在市场上占有一定份额。这种竞争不仅损害了原产品公司的知识产权和经济利益,更为重要的是严重扰乱了市场秩序。当今我国大力提倡科技创新、技术创新,显然像上述那样互相抄袭,或单方面盗版的现象应该绝对的杜绝。

[0003] 在行业竞争日益激烈的今天,如何保护自己的产品设计方案以提高产品的市场占有率,如何在产品技术转让时有一个理想的、可以量化的计量标准已经成为很多公司和产品设计者日益关切的问题。一般人们比较容易想到的是用软件实现加密系统来对自身进行保护。这种方法成本较低、也比较容易实现,但是具有占用主机系统资源较多、核心模块容易被跟踪和替换、密钥管理难度较大等缺点;再加上嵌入式系统空间有限、资源宝贵,用纯软件办法对产品进行保护对于大部分嵌入式系统来讲并不实用。

[0004] 针对嵌入式系统的特殊性,市场上出现了很多基于对称密码体制的具有安全认证功能的硬件安全芯片。采用硬件安全芯片的系统一般由微处理器、存储器芯片、硬件安全芯片和其它外围电路组成,其中存储器芯片用于存储软件,硬件安全芯片则用于存储敏感数据。主机执行程序的过程中通过对硬件安全芯片的认证后才可访问敏感数据,从而达到保护软件的目的。在硬件安全芯片内部一般集成了加密算法引擎,这样可以大大提高安全性和认证速度。这种程序保护方式将大部分的计算工作放在硬件安全芯片内部,不影响系统的整体性能,所以更适合于嵌入式软件的保护。但是,在对称密码体制中,任何一方的密钥被盗,整个系统就相当于被破解了。相对于存储在硬件安全芯片中的密钥,存储器软件中的密钥较容易被读出,极大地限制了系统的安全性。另外,由于使用了两种存储介质(存储器芯片如 Flash,硬件安全芯片如 EEPROM)和地址空间的不统一,使用不便,且当微处理器需要和硬件安全芯片频繁交换敏感数据时,会严重影响系统的吞吐率。

发明内容

[0005] 针对现有技术的缺陷,本发明的目的在于提供一种安全存储器芯片,旨在解决现有技术中存储器存储密钥不安全以及微处理器和硬件安全芯片频繁交换敏感数据会严重影响系统的吞吐率的问题。

[0006] 为实现上述目的,本发明提供了一种安全存储器芯片,包括总线接口模块、存储器模块、控制模块、加密模块和私钥;控制模块和存储器模块共用一个总线接口模块,加密模块和存储器模块均与控制模块相连,私钥与加密模块相连;存储器模块的存储区域包括通用区域和受保护区域,通用区域用于存储软件程序,受保护区域用于存储敏感数据;公钥存储于通用区域内。

[0007] 更进一步地,所述通用区域定义为访问不受限制的区域;受保护区域定义为只有通过认证后才可访问的区域;敏感数据定义为用户需要保护的关键数据。

[0008] 更进一步地,所述安全存储器芯片产生质询并发送给外部的微处理器,微处理器采用公钥对质询进行加密,并将加密后的质询传回安全存储器芯片;安全存储器芯片采用私钥对加密的质询进行解密,并将解密结果与原质询进行比较;当解密结果与原质询相同时,允许微处理器访问安全存储器芯片的受保护区域;当解密结果与原质询不同时,禁止微处理器访问安全存储器芯片的受保护区域。

[0009] 更进一步地,微处理器产生质询并采用公钥对质询进行加密,将加密后的质询发送给安全存储器芯片;安全存储器芯片采用私钥对加密后的质询进行解密,并将解密后的质询发送给微处理器;微处理器将安全存储器芯片解密后的质询和原质询进行比较;当解密后的质询与原质询相同时,微处理器继续执行程序;当解密后的质询与原质询不同时,微处理器终止执行程序。

[0010] 更进一步地,所述加密模块采用非对称加密算法对质询进行加密。

[0011] 本发明还提供了一种安全存储器系统,包括安全存储器芯片,微处理器和用于所述微处理器与所述安全存储器芯片之间数据交换的总线,所述安全存储器芯片为上述的安全存储器芯片。

[0012] 本发明还提供了一种安全存储器的认证方法,包括下述步骤:

[0013] S301:安全存储器芯片中的控制模块生成一个质询M1并发送给微处理器;

[0014] S302:微处理器采用公钥对质询M1进行加密并获得加密后的质询C1;微处理器将加密后的质询C1发送给安全存储器芯片;

[0015] S303:安全存储器芯片采用私钥对加密后的质询C1进行解密并获得解密后的质询M1';

[0016] S304:安全存储器芯片将解密后的质询M1'与原质询M1进行比较,当解密后的质询M1'与原质询M1相同时进入步骤305;当解密后的质询M1'与原质询M1不同时结束;

[0017] S305:安全存储器芯片赋予微处理器访问受保护区域的权限。

[0018] 更进一步地,还包括下述步骤:

[0019] S401:微处理器生成一个质询M2并对质询M2进行加密后获得加密后的质询C2;微处理器将加密后的质询C2发送给安全存储器芯片;

[0020] S402:安全存储器芯片采用私钥107对加密后的质询C2进行解密并获得解密后的质询M2';安全存储器芯片将解密后的质询M2'发送给微处理器;

[0021] S403:微处理器将解密后的质询M2'与原质询M2进行比较,当解密后的质询M2'与原质询M2相同时进入步骤S404,当解密后的质询M2'与原质询M2不同时,微处理器终止执行软件程序;

[0022] S404:微处理器继续执行软件程序。

- [0023] 本发明还提供了一种安全存储器的认证方法,包括下述步骤:
- [0024] S401:微处理器生成一个质询M2并对质询M2进行加密后获得加密后的质询C2;微处理器将加密后的质询C2发送给安全存储器芯片;
- [0025] S402:安全存储器芯片采用私钥107对加密后的质询C2进行解密并获得解密后的质询M2';安全存储器芯片将解密后的质询M2'发送给微处理器;
- [0026] S403:微处理器将解密后的质询M2'与原质询M2进行比较,当解密后的质询M2'与原质询M2相同时进入步骤S404,当解密后的质询M2'与原质询M2不同时,微处理器终止执行软件程序;
- [0027] S404:微处理器继续执行软件程序。
- [0028] 更进一步地,还包括:
- [0029] S301:安全存储器芯片中的控制模块生成一个质询M1并发送给微处理器;
- [0030] S302:微处理器采用公钥对质询M1进行加密并获得加密后的质询C1;微处理器将加密后的质询C1发送给安全存储器芯片;
- [0031] S303:安全存储器芯片采用私钥对加密后的质询C1进行解密并获得解密后的质询M1';
- [0032] S304:安全存储器芯片将解密后的质询M1'与原质询M1进行比较,当解密后的质询M1'与原质询M1相同时进入步骤305;当解密后的质询M1'与原质询M1不同时结束;
- [0033] S305:安全存储器芯片赋予微处理器访问受保护区域的权限。
- [0034] 本发明采用了非对称的密码体制,即使软件程序中的公钥被盗,没有与之唯一对应的私钥,软件程序也无法正常运行,这使得破解系统的难度由攻击软件中的密钥提升到了攻击硬件安全环境中的私钥。考虑到对芯片进行物理攻击来获取私钥的成本较高,该安全存储器芯片显然具备更高的安全性。安全存储器芯片中的存储区域分为通用区域和受保护区,由同一种存储介质构成,具有统一的地址空间,方便微处理器的访问。其中通用区域存储软件程序,微处理器可直接访问。受保护区存储敏感数据,微处理器只有通过安全认证之后才可访问。这样既保证了敏感数据的安全性,又提高了系统的运行速度。与传统方案相比,将存储器功能和安全认证功能集成在同一块芯片上,还具有使用方便,节省PCB面积,成本更低的优点。

附图说明

- [0035] 图1是本发明实施例提供的安全存储器系统的模块结构示意图;
- [0036] 图2是本发明实施例提供的安全存储器芯片的模块结构示意图;
- [0037] 图3是本发明实施例提供的安全认证方法中安全存储器芯片认证微处理器的流程图;
- [0038] 图4是本发明实施例提供的安全认证方法中微处理器认证安全存储器芯片的流程图。

具体实施方式

- [0039] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并

不用于限定本发明。

[0040] 本发明实施例提供的安全存储器芯片同时具有存储功能和安全认证功能,认证采用非对称密码体制,且软件和敏感数据存储在同一介质上;既保证了敏感数据的安全性,又提高了系统的运行速度。

[0041] 图1示出了本发明实施例提供的安全存储器系统的模块结构;安全存储器系统包括安全存储器芯片100,微处理器200和用于微处理器与安全存储器芯片之间数据交换的总线150。其中,微处理器200和其间交换数据的总线150可以采用SPI、IIC或并口等。

[0042] 本发明实施例提供的安全存储器系统安全性更高、系统运行速度更快、PCB面积更小。

[0043] 安全存储器芯片100的模块结构如图2所示,安全存储器芯片100包括:总线接口模块101、存储器模块102、控制模块105、加密模块106和私钥107;控制模块105和存储器模块102共用一个总线接口模块101和微处理器进行数据交互,控制模块105与加密模块106和存储器模块102相连,私钥107只供加密模块106访问;存储器模块102被划分为通用区域103和受保护区域104,软件程序存储于通用区域103,敏感数据存储于受保护区域104;公钥108设置在通用区域103的软件程序中。

[0044] 本发明通过基于非对称加密算法的双向认证来实现安全存储。一方面,安全存储器芯片100需要认证微处理器200来开放受保护区域104的访问权限,以实现对敏感数据的保护。这个过程中安全存储器芯片100产生质询,发送给微处理器200用公钥108进行加密,把加密的质询传回安全存储器芯片100;安全存储器芯片100用私钥107对加密的质询解密,将结果和原质询进行比较。若相同,则说明微处理器200合法,允许其访问安全存储器芯片100的受保护区域104;否则,禁止其访问安全存储器芯片100的受保护区域104。另一方面,微处理器200需要认证安全存储器芯片100来确定其合法性,对于非法的存储器芯片,程序中止执行。这个过程中微处理器200产生质询,用公钥108进行加密,并加密的质询发送给安全存储器芯片100;安全存储器芯片100用私钥107对加密的质询解密,将恢复得到的质询发送给微处理器200;微处理器200将安全存储器芯片解密得到的质询和原质询进行比较。若相同,则说明安全存储器芯片100合法,程序继续执行;否则,程序执行中断。

[0045] 在本发明实施例中,通用区域103是指访问不受限制的区域,其功能相当于嵌入式系统中微处理器的存储器。受保护区域105是指只有通过认证后才可访问的区域。软件程序是指微处理器执行的程序主体和存储的数据。敏感数据是指想要保护的关键数据。

[0046] 在本发明实施例中,存储器模块102和控制模块105共用一个总线接口模块101。安全存储器芯片100的总线接口模块101和普通的存储器芯片一致,在嵌入式应用中存储器常用的总线接口有IIC、SPI和并口。在实际应用中,存储器模块102主要由Flash和EEPROM构成,存储区域划分为通用区域103和受保护区域104。通用区域103主要存储软件程序,其中包括公钥108;受保护区域104则存储敏感数据,包含使用者想要保护的数据。微处理器200可直接访问通用区域103,受保护区域104则必须通过控制模块105的认证才可访问,否则访问操作失败。而当控制模块105没能通过微处理器200的认证时,软件程序应当中止执行,从而实现双向认证。控制模块105主要控制加解密过程和数据的搬移。当微处理器200没有通过控制模块105的认证时,屏蔽掉微处理器对受保护区域104的操作。

加密模块 107 主要完成非对称加密算法。私钥 107 存储在独立的非忆失区域内 (EEPROM, OTP 等), 只能由加密模块 106 访问, 对微处理器 200 不可见。

[0047] 在本发明实施例中, 非对称加密算法可以采用 RSA, ECC, NTRU 等。加密算法的具体过程为: 接收方 B 通过计算产生一对密钥(公钥 PKey 和私钥 SKey)。发送方 A 知道 B 的公钥 PKey 和待加密报文 M 的情况下, 计算密文 C : $C=E_{PKey}(M)$ 。接收方 B 使用私钥 SKey 来恢复明文 M' : $M'=D_{SKey}(C)=D_{SKey}(E_{PKey}(M))=M$ 。

[0048] 如图 3 所示, 本发明实施例提供了安全存储器的认证方法中安全存储器芯片认证微处理器的流程; 方法 300 可以被实施于安全存储器芯片 100 和微处理器 200 之间, 以确定安全存储器芯片 100 是否认证了微处理器 200, 以用于安全存储器芯片 100 或供其使用。微处理器 200 和安全存储器芯片 100 通过总线 150 连接在一起, 开机后微处理器 200 加载存储在安全存储器芯片 100 通用区域 103 中的软件程序。

[0049] 该方法具体包括:

[0050] S301: 安全存储器芯片 100 中的控制模块 105 生成一个质询 M1 并发送给微处理器 200;

[0051] S302: 微处理器 200 采用公钥 108 对质询 M1 进行加密并获得加密后的质询 C1; 微处理器 200 将加密后的质询 C1 发送给安全存储器芯片 100;

[0052] S303: 安全存储器芯片 100 采用私钥 107 对加密后的质询 C1 进行解密并获得解密后的质询 M1';

[0053] S304: 安全存储器芯片 100 将解密后的质询 M1' 与原质询 M1 进行比较, 当解密后的质询 M1' 与原质询 M1 相同时进入步骤 305; 当解密后的质询 M1' 与原质询 M1 不同时结束;

[0054] S305: 安全存储器芯片 100 赋予微处理器 200 访问受保护区域 104 的权限。

[0055] 在本发明实施例中, 微处理器 200 采用公钥 108 对质询 M1 加密, 得到密文 C1: $C1=E_{PKey}(M1)$, PKey 是公钥, E_{PKey} 是非对称加密算法中的加密算法。其中, 公钥 108 存储在安全存储器芯片 100 中的通用区域 103 内。微处理器 200 将加密后的质询 C1 通过总线 150 发送给安全存储器芯片 100。

[0056] 在本发明实施例中, 安全存储器芯片 100 采用私钥 107 对加密的质询 C1 进行解密, 恢复出明文质询 M1' : $M1'=D_{SKey}(C1)=D_{SKey}(E_{PKey}(M1))$, SKey 是私钥, D_{SKey} 是非对称加密算法中的加密算法。其中私钥 107 存储在独立的非忆失区域内, 只能由加密模块 106 访问, 保证了私钥 107 的安全性。

[0057] 本发明实施例提供的方法 300 保护了安全存储器芯片 100 中的敏感数据。即使公钥 PKey 被攻击者破解, 存储在存储器模块 102 中的软件程序和敏感数据被盗, 采用方法 400, 由于设置在软件程序中公钥 PKey 和硬件环境中的私钥 SKey 一一对应, 盗取的软件程序和敏感数据也就无法批量应用在嵌入式系统中, 保护了系统的安全。

[0058] 如图 4 所示, 本发明实施例提供了安全存储器的认证方法中微处理器认证安全存储器芯片的流程, 方法 400 可以被实施于安全存储器芯片 100 和微处理器 200 之间, 以确定微处理器 200 是否认证了安全存储器芯片 100, 以用于微处理器 200 或供其使用。微处理器 200 和安全存储器芯片 100 通过总线 150 连接在一起, 开机后微处理器 200 加载存储在安全存储器芯片 100 通用区域 103 中的软件程序。

[0059] 该方法具体包括：

[0060] S401：微处理器 200 生成一个质询 M2 并对质询 M2 进行加密后获得加密后的质询 C2；微处理器 200 将加密后的质询 C2 发送给安全存储器芯片 100；

[0061] S402：安全存储器芯片 100 采用私钥 107 对加密后的质询 C2 进行解密并获得解密后的质询 M2'；安全存储器芯片 100 将解密后的质询 M2' 发送给微处理器 200；

[0062] S403：微处理器 200 将解密后的质询 M2' 与原质询 M2 进行比较，当解密后的质询 M2' 与原质询 M2 相同时进入步骤 S404，当解密后的质询 M2' 与原质询 M2 不同时，微处理器 200 终止执行软件程序；

[0063] S404：微处理器 200 继续执行软件程序。

[0064] 在本发明实施例中，微处理器 200 用公钥 108 对质询 M 加密，得到密文 C2： $C2 = E_{PKey}(M2)$ ，PKey 是公钥， E_{PKey} 是非对称加密算法中的加密算法。其中，公钥 108 存储在安全存储器芯片 100 中的通用区域 103 内。微处理器 200 将加密后的质询 C2 通过总线 150 发送给安全存储器芯片 100。

[0065] 在本发明实施例中，安全存储器芯片 100 用私钥 107 对加密的质询 C2 进行解密，恢复出明文质询 M2'： $M2' = D_{SKey}(C2) = D_{SKey}(E_{PKey}(M2))$ ，SKey 是私钥， D_{SKey} 是非对称加密算法中的加密算法。其中，私钥 107 存储在独立的非易失区域内，只能由加密模块 106 访问，保证了私钥 107 的安全性。安全存储器芯片 100 通过总线 150 将解密后的质询 M2' 发送给微处理器 200。

[0066] 在本发明实施例中，双向认证方法包括方法 300 和方法 400，可以使方法 300 先执行，再执行方法 400；也可以是先执行方法 400，再执行方法 300。方法 300 和方法 400 构成了基于非对称加密算法的双向认证体系，并且破解系统的难度由攻击软件中的密钥提升到了攻击安全硬件环境中的私钥，提高了嵌入式系统的安全性。

[0067] 本发明提供的安全存储器芯片同时具有存储器功能和安全认证功能。相比市场上采用独立的安全芯片保护系统的做法，由于本发明认证采用非对称密码体制，改善了软件程序中密钥存储的问题，具备更高的安全性。软件程序和敏感数据存储在同一介质上，对其访问通过同一根总线并统一编址，系统的运行速度更快。本发明同时还具有系统集成度更高，PCB 面积更小等优点。

[0068] 本领域的技术人员容易理解，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、等同替换和改进等，均应包含在本发明的保护范围之内。

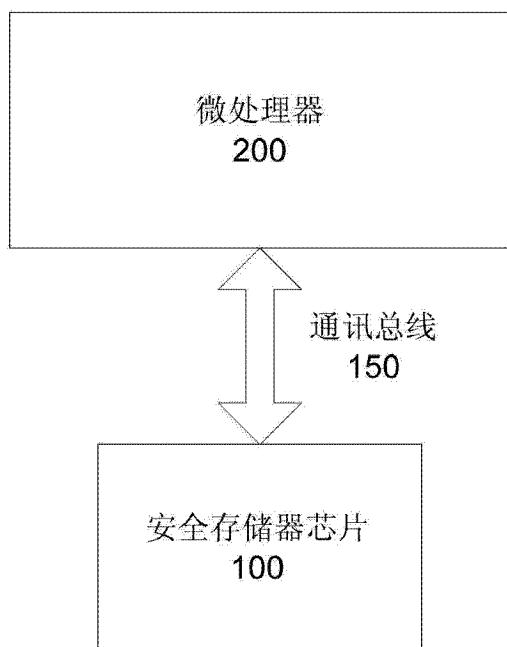


图 1

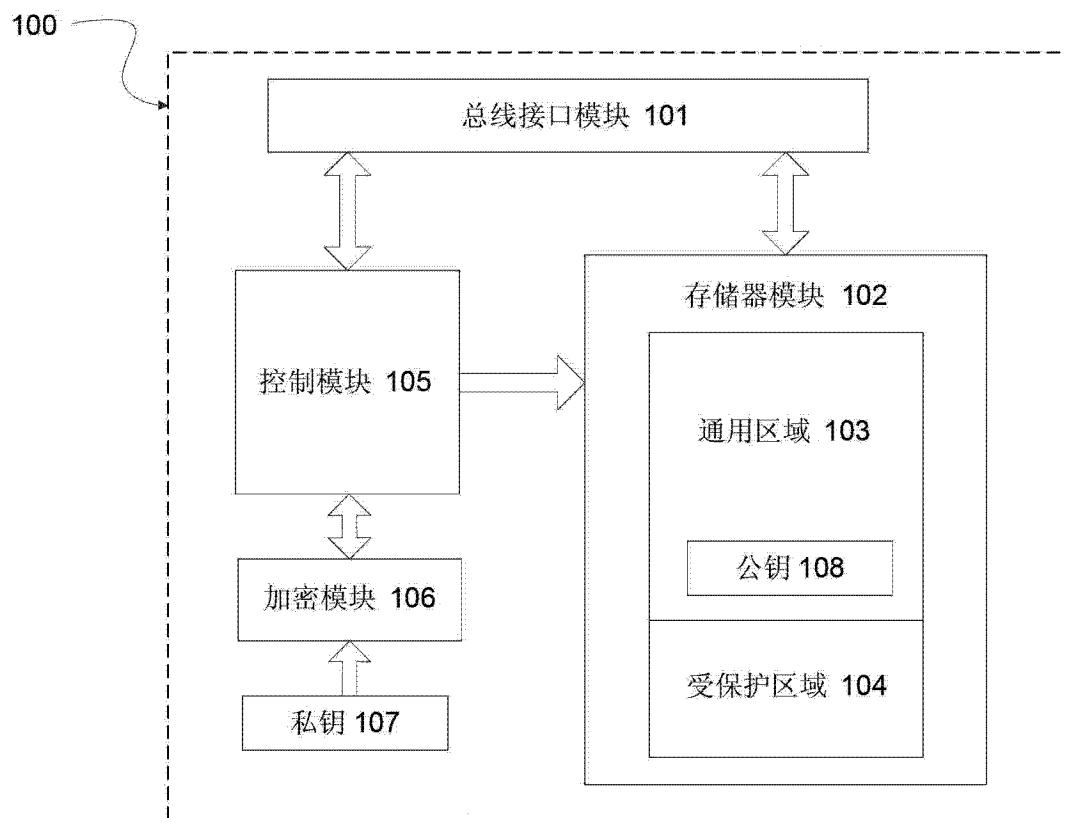


图 2

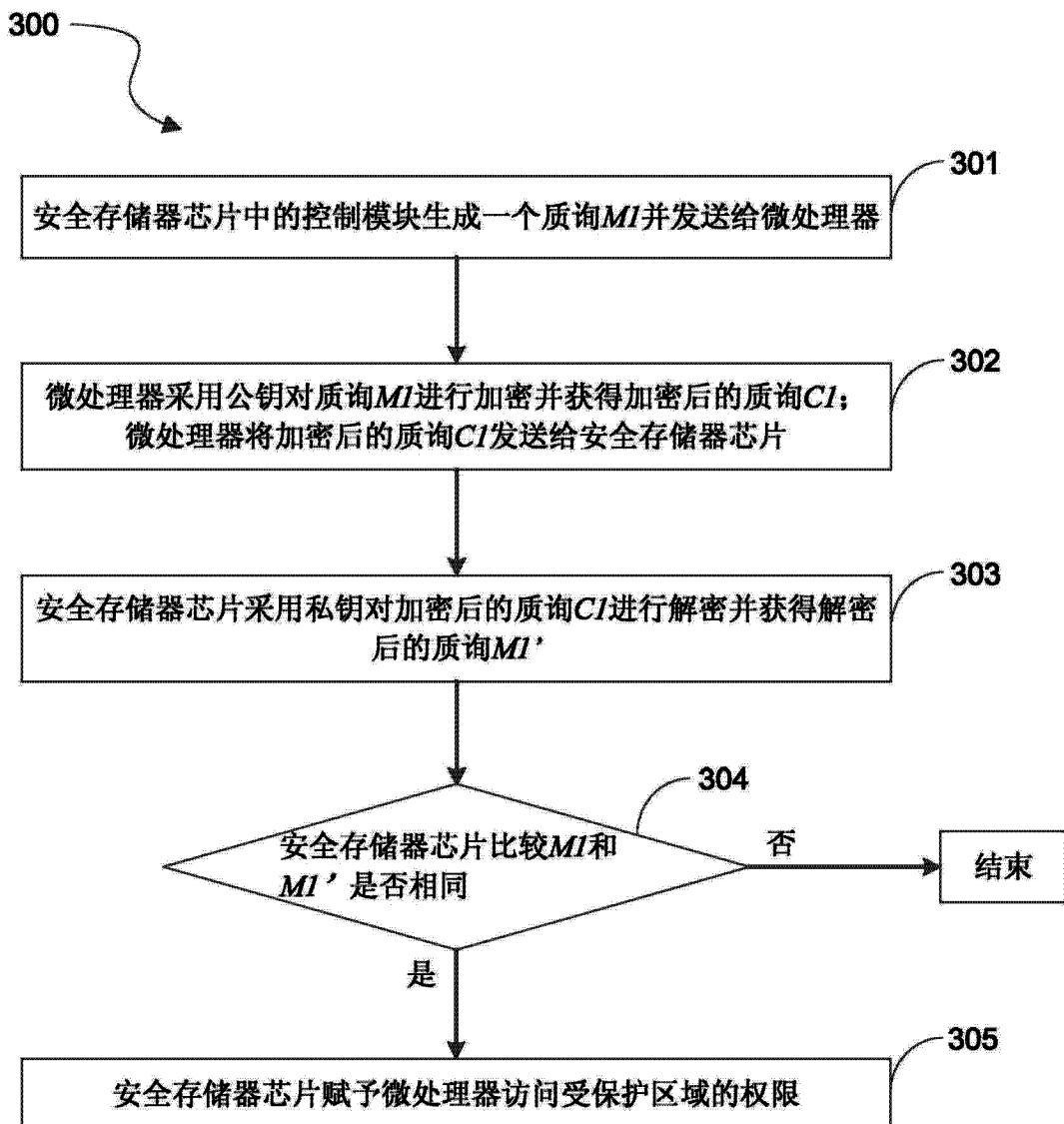


图 3

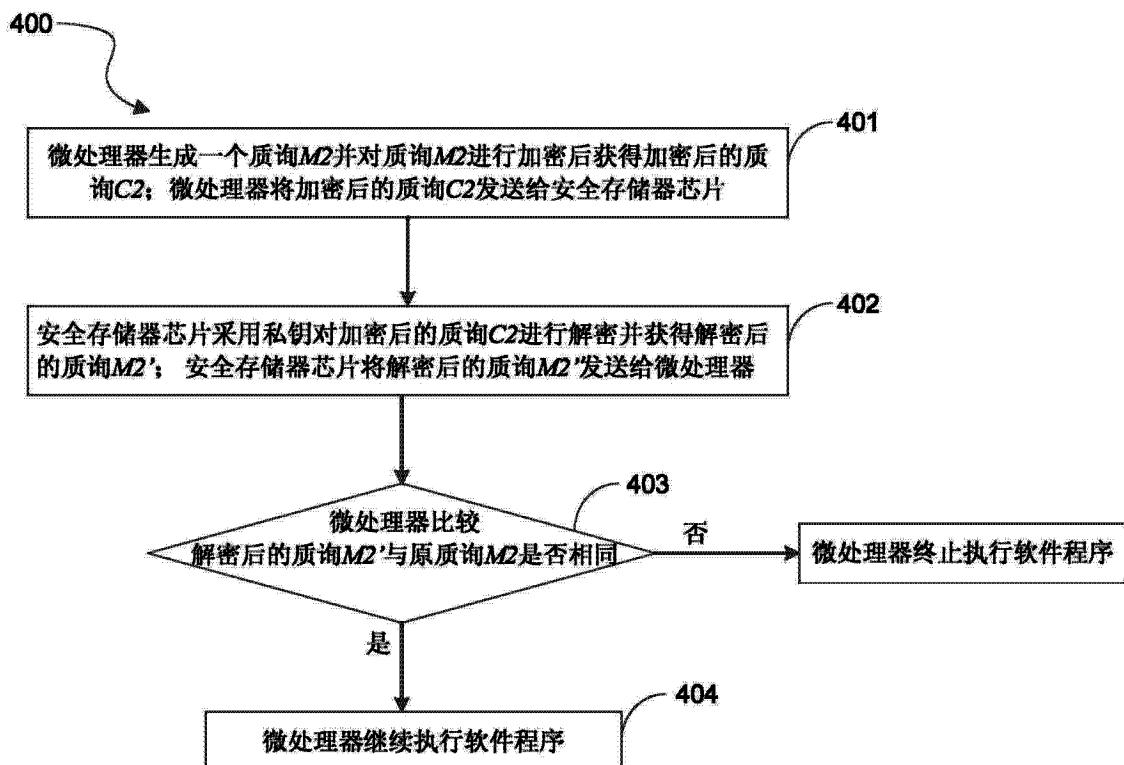


图 4