(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103124256 B
(45)授权公告日 2017.03.29

(21)申请号 201110371266.3

(22)申请日 2011.11.21

(65)同一申请的已公布的文献号
申请公布号 CN 103124256 A

(43)申请公布日 2013.05.29

(73)专利权人 国民技术股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园区深圳软件园3栋301、302

(72)发明人 艾俊 付月朋 王正鹏

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 杨立

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/06(2006.01)

(56)对比文件
CN 102082665 A,2011.06.01,说明书第[0053]段、第[0075]-[0078]段.
CN 102082665 A,2011.06.01,说明书第[0053]段、第[0075]-[0078]段.
CN 1393081 A,2003.01.22,说明书第2页第14行至第3页第17行.
CN 101281575 A,2008.10.08,全文.
KR 20060081338 A,2006.07.12,全文.
CN 101018129 A,2007.08.15,全文.
CN 101217374 A,2008.07.09,全文.

审查员 郑红萍

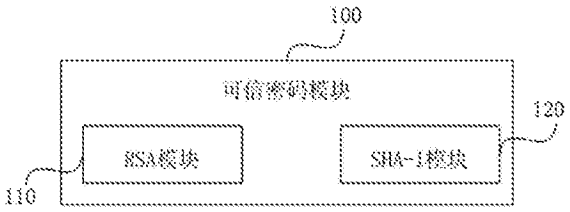
权利要求书1页 说明书6页 附图4页

(54)发明名称

可信密码模块及可信计算方法

(57)摘要

本发明涉及一种可信密码模块及可信计算方法。其中,可信密码模块包括:RSA模块,用于根据RSA算法对数据进行处理;SHA-1模块,用于接收所述RSA模块输出的数据,根据哈希算法SHA-1对数据进行处理。本发明的可信计算方法用于上述的可信密码模块,该可信计算方法包括:根据RSA算法对数据进行第一处理;在所述第一处理后,根据哈希算法SHA-1对数据进行第二处理。本发明的可信密码模块及可信计算方法,能够支持PKI应用体系,从而扩大了可信密码模块的应用范围。



CN 103124256 B

1.一种可信密码模块,其特征在于,包括:

RSA模块,用于根据RSA算法对数据进行处理;所述RSA模块包括:RSA密钥处理模块,用于根据RSA算法创建RSA密钥,以及使用所述RSA密钥对数据进行处理;RSA算法库,用于对数据实现RSA算法;

SHA-1模块,用于接收所述RSA模块输出的数据,根据哈希算法SHA-1对数据进行处理;所述SHA-1模块包括:SHA-1计算模块,用于根据哈希算法SHA-1计算所述RSA密钥的公钥的哈希值,以及根据所述哈希值建立所述RSA密钥的索引;SHA-1算法库,用于对数据实现哈希算法SHA-1;

所述RSA密钥处理模块包括修改单元,用于对RSA密钥的授权数据进行修改;修改RSA密钥授权数据的执行过程为:验证存储主密钥SMK的授权数据;根据RSA密钥的公钥哈希数据获取该RSA密钥信息并验证RSA密钥的授权数据;修改RSA密钥的授权数据为新的授权数据;按照命令修改所述RSA密钥授权数据命令的输出参数的格式,返回命令数据。

2.根据权利要求1所述的可信密码模块,其特征在于,所述RSA密钥处理模块包括:

创建单元,用于根据RSA算法创建RSA密钥;

解密单元,用于使用RSA密钥对待解密数据进行解密;

签名单元,用于使用RSA密钥对待签名数据进行签名。

3.根据权利要求1所述的可信密码模块,其特征在于,所述RSA密钥处理模块还包括写单元,用于将RSA证书写入到存储区域中。

4.根据权利要求1所述的可信密码模块,其特征在于,所述RSA密钥处理模块还包括证书获取单元,用于获取RSA证书。

5.根据权利要求1所述的可信密码模块,其特征在于,所述RSA密钥处理模块还包括公钥获取单元,用于获取RSA密钥的公钥。

6.一种可信计算方法,其特征在于,用于权利要求1所述的可信密码模块,该可信计算方法包括:

根据RSA算法对数据进行第一处理:根据RSA算法创建RSA密钥,以及使用所述RSA密钥对数据进行处理,对数据实现RSA算法;

在所述第一处理后,根据哈希算法SHA-1对数据进行第二处理:包括根据哈希算法SHA-1计算所述RSA密钥的公钥的哈希值,以及根据所述哈希值建立所述RSA密钥的索引,对数据实现哈希算法SHA-1;

还包括修改RSA密钥的授权数据的步骤:验证存储主密钥SMK的授权数据;根据RSA密钥的公钥哈希数据获取该RSA密钥信息并验证RSA密钥的授权数据;修改RSA密钥的授权数据为新的授权数据;按照命令修改所述RSA密钥授权数据命令的输出参数的格式,返回命令数据。

可信密码模块及可信计算方法

技术领域

[0001] 本发明涉及可信计算领域，尤其涉及一种可信密码模块及可信计算方法。

背景技术

[0002] 可信计算是指在PC(个人计算机)硬件平台引入安全芯片架构，通过其提供的安全特性来提高终端系统的安全性，从而在根本上实现对各种不安全因素的主动防御。可信计算因此成为信息安全的主要发展趋势之一，也是IT产业发展的主要方向。

[0003] 可信计算技术体系理念的提出是在二十世纪末。1999年开始，国际上一批IT巨头组成了一个可信计算工作组，来推相关的一个技术标准，到2003年一个比较成熟的TCG(Trusted Computing Group，可信计算组织)形成了。TCG组织的成员几乎包括IT行业各个层次的巨头，数量已达到将近200家。

[0004] TCG组织从标准规范入手，来影响这一产业的发展。TCG组织对未来IT产业的影响力、未来的发展目标也是非常宏大的。他们建立的标准，借助硬件芯片TPM(Trusted Platform Module，可信平台模块)。可以说TPM是未来基础设施中的基础部件，今后会影响到整个IT产业的各个方面，包括各种产品形态、终端、服务器、存储系统、软件、网络接入、手机等。

[0005] 中国和国际上其他组织几乎是同步在进行可信计算的研究和部署工作。其中，我国部署的可信计算体系中，密码技术是最重要的核心技术。具体的方案是以密码算法为突破口，依据嵌入芯片技术，完全采用我国自主研发的密码算法和引擎，来构件一个安全芯片，称之为TCM(Trusted Cryptography Module，可信密码模块)。

[0006] PKI(Public Key Infrastructure，公钥基础设施)是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI技术是信息安全技术的核心，也是电子商务的关键和基础技术。

[0007] 由于可信密码模块TCM只支持我国自主研发的密码算法，因此目前的可信密码模块TCM无法支持采用国际算法的PKI应用体系。

发明内容

[0008] 本发明所要解决的技术问题是提供一种可信密码模块及可信计算方法，能够支持PKI应用体系，扩大可信密码模块的应用范围。

[0009] 为解决上述技术问题，本发明提出了一种可信密码模块，包括：

[0010] RSA模块，用于根据RSA算法对数据进行处理；

[0011] SHA-1模块，用于接收所述RSA模块输出的数据，根据哈希算法SHA-1对数据进行处理。

[0012] 进一步地，上述可信密码模块还可具有以下特点，所述RSA模块包括：

[0013] RSA密钥处理模块，用于根据RSA算法创建RSA密钥，以及使用所述RSA密钥对数据

进行处理；

[0014] RSA算法库，用于对数据实现RSA算法。

[0015] 进一步地，上述可信密码模块还可具有以下特点，所述SHA-1模块包括：

[0016] SHA-1计算模块，用于根据哈希算法SHA-1计算所述RSA密钥的公钥的哈希值，以及根据所述哈希值建立所述RSA密钥的索引；

[0017] SHA-1算法库，用于对数据实现哈希算法SHA-1。

[0018] 进一步地，上述可信密码模块还可具有以下特点，所述RSA密钥处理模块包括：

[0019] 创建单元，用于根据RSA算法创建RSA密钥；

[0020] 解密单元，用于使用RSA密钥对待解密数据进行解密；

[0021] 签名单元，用于使用RSA密钥对待签名数据进行签名。

[0022] 进一步地，上述可信密码模块还可具有以下特点，所述RSA密钥处理模块还包括修改单元，用于对RSA密钥的授权数据进行修改。

[0023] 进一步地，上述可信密码模块还可具有以下特点，所述RSA密钥处理模块还包括写单元，用于将RSA证书写入到存储区域中。

[0024] 进一步地，上述可信密码模块还可具有以下特点，，所述RSA密钥处理模块还包括证书获取单元，用于获取RSA证书。

[0025] 进一步地，上述可信密码模块还可具有以下特点，所述RSA密钥处理模块还包括公钥获取单元，用于获取RSA密钥的公钥。

[0026] 为解决上述技术问题，本发明提出了一种可信计算方法，用于前述的可信密码模块，包括：

[0027] 根据RSA算法对数据进行第一处理；

[0028] 在所述第一处理后，根据哈希算法SHA-1对数据进行第二处理。

[0029] 进一步地，上述可信计算方法还可具有以下特点，

[0030] 根据RSA算法对数据进行第一处理包括：

[0031] 根据RSA算法创建RSA密钥，以及使用所述RSA密钥对数据进行处理；

[0032] 在所述第一处理后，根据哈希算法SHA-1对数据进行第二处理包括：

[0033] 根据哈希算法SHA-1计算所述RSA密钥的公钥的哈希值，以及根据所述哈希值建立所述RSA密钥的索引。

[0034] 本发明的可信密码模块及可信计算方法，能够支持PKI应用体系，从而扩大了可信密码模块的应用范围。

附图说明

[0035] 图1为本发明实施例中可信密码模块的结构框图；

[0036] 图2为图1中RSA模块110的一种结构框图；

[0037] 图3为图1中SHA-1模块120的一种结构框图；

[0038] 图4为图2中RSA密钥处理模块111的一种结构框图；

[0039] 图5为本发明实施例中可信密码模块的一种具体结构图。

具体实施方式

[0040] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0041] 图1为本发明实施例中可信密码模块的结构框图。如图1所示，本实施例中，可信密码模块100包括RSA模块110和SHA-1模块120。其中，RSA模块110用于根据国际加密算法RSA算法对数据进行处理。SHA-1模块120用于接收RSA模块110输出的数据，根据哈希算法SHA-1对数据进行处理。当然，可信密码模块100中必然包括现有TCM的基本组成模块，这些基本组成模块是现有技术。

[0042] 其中，RSA模块110和SHA-1模块120可以置于TCM的固件中。可信密码模块100通过在TCM固件中扩展对国际加密算法RSA和哈希算法SHA-1的支持来支持PKI应用体系。

[0043] 图2为图1中RSA模块110的一种结构框图。如图2所示，本实施例中，RSA模块110可以包括RSA密钥处理模块111和RSA算法库112。RSA密钥处理模块111用于根据国际加密算法RSA算法创建RSA密钥，以及使用该RSA密钥对数据进行处理。RSA算法库112用于对数据实现国际加密算法RSA算法。

[0044] 图3为图1中SHA-1模块120的一种结构框图。如图3所示，本实施例中，SHA-1模块120可以包括SHA-1计算模块121和SHA-1算法库122。其中，SHA-1计算模块121用于根据哈希算法SHA-1计算RSA密钥的公钥的哈希值，以及根据该哈希值建立RSA密钥的索引。SHA-1算法库122用于对数据实现哈希算法SHA-1。

[0045] 图4为图2中RSA密钥处理模块111的一种结构框图。如图4所示，本实施例中，RSA密钥处理模块111可以包括创建单元1111、解密单元1112和签名单元1113。创建单元1111用于根据国际加密算法RSA算法创建RSA密钥。解密单元1112用于使用RSA密钥对待解密数据进行解密。签名单元1113用于使用RSA密钥对待签名数据进行签名。

[0046] 其中，创建单元1111执行创建RSA密钥命令。创建RSA密钥命令的输入参数包括命令标识、命令长度、创建RSA密钥命令码、RSA密钥授权使用数据、授权会话句柄、SMK(Storage Master Key，存储主密钥)授权数据、命令防重放攻击序列。创建RSA密钥命令的输出参数包括命令标识、命令长度、返回码、创建RSA密钥命令码、密钥的公钥哈希数据、授权会话句柄、授权数据的摘要值、命令防重放攻击序列。

[0047] 在可信密码模块TCM中，创建RSA密钥命令的执行过程如下：

[0048] 步骤a1，验证SMK的授权数据，若授权失败返回授权失败信息TCM_AuthFail，若授权成功则执行步骤a2；

[0049] 步骤a2，验证密钥参数，如果密钥的使用方式不是加密密钥或签名密钥，返回密钥使用方式无效信息TCM_INVALID_KEYUSAGE，如果密钥的长度不是1024或2048位，返回密钥特征错误信息TCM_BAD_KEY_PROPERTY；若密钥的使用方式是加密密钥或签名密钥，且密钥的长度是1024或2048位，则执行步骤a3；

[0050] 步骤a3，根据RSA密钥的参数调用RSA算法生成RSA密钥；

[0051] 步骤a4，使用新生成的RSA密钥填充包裹的密钥结构；

[0052] 步骤a5，使用SMK加密保存RSA密钥的私钥部分

[0053] 步骤a6，计算RSA密钥的公钥数据的摘要，按照创建RSA密钥命令的输出参数的格式返回命令数据。

[0054] 其中，解密单元1112执行RSA解密命令。RSA解密命令的输入参数包括命令标识、命

令长度、RSA解密命令码、密钥的公钥哈希数据、解密数据长度、解密数据、随机序列、授权会话句柄、授权数据。RSA解密命令的输出参数包括命令标识、命令长度、返回码、RSA解密命令码、解密后数据的长度、解密数据、随机序列、授权会话句柄、授权数据的摘要值。

[0055] 在可信密码模块TCM中，RSA解密命令的执行过程如下：

[0056] 步骤b1，根据RSA密钥的公钥哈希数据获取RSA密钥信息并验证RSA密钥的授权数据；

[0057] 步骤b2，验证密钥的属性，如果密钥不是加密密钥，返回密钥属性无效信息TPM_INVALID_KEYUSAGE，如果解密数据长度是0，返回参数错误信息TPM_BAD_PARAMETER，如果密钥是加密密钥且解密数据长度不是0，则执行步骤b3；

[0058] 步骤b3，使用SMK密钥解密RSA密钥的私钥部分；

[0059] 步骤b4，利用RSA密钥的私钥解密；

[0060] 步骤b5，按照RSA解密命令的输出参数的格式返回命令数据。

[0061] 其中，签名单元1113执行RSA签名命令。RSA签名命令的输入参数包括命令标识、命令长度、RSA签名命令码、密钥的公钥哈希数据、签名数据长度、签名数据、随机序列、授权会话句柄、授权数据。RSA签名命令的输出参数包括命令标识、命令长度、返回码、RSA签名命令码、签名后数据的长度、签名数据、随机序列、授权会话句柄、授权数据。

[0062] 在可信密码模块TCM中，RSA签名命令的执行过程如下：

[0063] 步骤c1，根据RSA密钥公钥的哈希数据获取该RSA密钥信息并验证RSA密钥的授权数据；

[0064] 步骤c2，验证密钥的属性，如果密钥不是签名密钥，则返回密钥用途错误信息TCM_INVALID_KEYUSAGE，如果签名数据长度是0，返回参数错误信息TCM_BAD_PARAMETER，如果密钥是签名密钥且签名数据长度不是0，则执行步骤c3；

[0065] 步骤c3，使用SMK密钥解密RSA密钥的私钥部分；

[0066] 步骤c4，验证签名模式，签名模式包括如下三种：

[0067] a)哈希签名模式，对应的签名标识为TCM_SS_RSASSAPKCS1v15_SHA1；

[0068] b)编码签名模式，对应的签名标识为TCM_SS_RSASSAPKCS1v15_DER；

[0069] c)填充签名模式，对应的签名标识为TCM_SS_RSASSAPKCS1v15_INFO；

[0070] 步骤c5，利用RSA密钥的私钥对数据进行签名；

[0071] 步骤c6，按照RSA签名命令的输出参数的格式返回命令数据。

[0072] 再如图4所示，RSA密钥处理模块111还可以包括修改单元1114。修改单元1114用于对RSA密钥的授权数据进行修改。

[0073] 修改单元1114执行修改RSA密钥授权数据命令。修改RSA密钥授权数据命令的输入参数包括命令标识、命令长度、修改RSA密钥授权数据命令码、新的授权数据、密钥的公钥哈希数据、SMK授权会话随机序列、SMK密钥的授权句柄、SMK密钥的授权数据、密钥授权会话随机序列、密钥授权会话随机序列、密钥的授权数据。修改RSA密钥授权数据命令的输出参数包括命令标识、命令长度、返回码、修改RSA密钥授权数据命令码、SMK密钥授权会话随机序列、SMK密钥的授权句柄、SMK密钥的授权数据、密钥授权会话随机序列、密钥授权会话随机序列、密钥的授权数据。

[0074] 在可信密码模块TCM中，修改RSA密钥授权数据命令的执行过程如下：

[0075] 步骤d1，验证SMK的授权数据；

[0076] 步骤d2，根据RSA密钥的公钥哈希数据获取该RSA密钥信息并验证RSA密钥的授权数据；

[0077] 步骤d3，修改RSA密钥的授权数据为新的授权数据；

[0078] 步骤d4，按照命令修改所述RSA密钥授权数据命令的输出参数的格式，返回命令数据。

[0079] 再如图4所示，RSA密钥处理模块111还可以包括写单元1115。写单元1115用于将RSA证书写入到存储区域中。

[0080] 写单元1115执行写RSA证书命令。写RSA证书命令的输入参数包括命令标识、命令长度、写RSA证书命令码、密钥的公钥哈希数据、证书数据长度、证书数据。写RSA证书命令的输出参数包括命令标识、命令长度、返回码。

[0081] 在可信密码模块TCM中，写RSA证书命令的执行过程如下：

[0082] 步骤e1，验证命令标识，如果命令标识不是TCM_TAG_RQU_COMMAND，返回命令标识错误信息TCM_BADTAG。

[0083] 步骤e2，将RSA证书和密钥的公钥哈希数据根据一对一的关系写入DATAFLASH中。

[0084] 步骤e3，按照命令输出参数的格式返回命令数据。

[0085] 再如图4所示，RSA密钥处理模块111还可以包括证书获取单元1116。证书获取单元1116用于获取RSA证书。

[0086] 获取单元1116获取RSA证书命令。获取RSA证书命令的输入参数包括命令标识、命令长度、获取RSA证书命令码、密钥的公钥哈希数据。获取RSA证书命令的输出参数包括命令标识、命令长度、获取RSA证书命令码、RSA证书数据长度、RSA证书数据。

[0087] 在可信密码模块TCM中，获取RSA证书命令的执行过程如下：

[0088] 步骤f1，验证命令标识，如果命令标识不是TCM_TAG_RQU_COMMAND则返回命令标识错误信息TCM_BADTAG，如果命令标识是TCM_TAG_RQU_COMMAND则执行步骤f2；

[0089] 步骤f2，根据RSA密钥的公钥哈希数据获取该密钥对应的证书信息，如果未找到相关信息返回失败；

[0090] 步骤f3，按照获取RSA证书命令的输出参数的格式返回命令数据。

[0091] 再如图4所示，RSA密钥处理模块111还可以包括公钥获取单元1117。公钥获取单元1117用于获取RSA密钥的公钥。

[0092] 公钥获取单元1117执行获取RSA密钥公钥命令。获取RSA密钥公钥命令的输入参数包括命令标识、命令长度、命令码、密钥的公钥哈希数据。获取RSA密钥公钥命令的输出参数包括命令标识、命令长度、返回码、获取RSA密钥公钥命令码、密钥公钥数据。

[0093] 步骤g1，根据RSA密钥公钥的哈希数据获取该密钥信息，如果未找到相关密钥信息返回失败；

[0094] 步骤g2，获取密钥的公钥数据，按照获取RSA密钥公钥命令的输出参数的格式返回命令数据。

[0095] 在具体的应用中，TCM是使用原有的国密算法(例如SMS4算法和SM2算法)对数据进行加解密，还是使用支持PKI的RSA算法和SHA-1算法对数据进行加解密，根据应用需求确定。如果应用需要支持PKI则必须使用RSA算法和SHA-1算法。如果是其它需求则可以任意选

择，只要加解密或签名验签使用的算法相同就行。

[0096] 为了更加直观地说明本发明的可信密码模块与现有可信密码模块的区别，下面将通过具体实例来对本发明可信密码模块作进一步阐述。图5为本发明实施例中可信密码模块的一种具体结构图。如图5所示，本实施例中，可信密码模块包括硬件初始化模块、数据初始化模块、LPC模块、命令解析和预处理模块、命令处理模块。其中，命令处理模块包括数据解析模块、密钥处理模块、授权数据处理模块、Hash计算模块、PCR处理计算模块、NV处理模块、RSA密钥处理模块、SHA-1计算子模块、计数器处理模块、会话/句柄处理模块、Flash处理模块、审计处理模块。而且，可信密码模块中还包括供命令处理模块调用的对称算法引擎、非对称算法引擎、Hash算法引擎、RSA算法库、SHA-1算法库、Flash驱动。其中，命令处理模块中的数据解析模块、密钥处理模块、授权数据处理模块、Hash计算模块、PCR处理计算模块、NV处理模块、计数器处理模块、会话/句柄处理模块、Flash处理模块、审计处理模块，以及供命令处理模块调用的对称算法引擎、非对称算法引擎、Hash算法引擎、Flash驱动，是现有技术中可信密码模块已有的。命令处理模块中的RSA密钥处理模块和SHA-1计算子模块以及供命令处理模块调用的RSA算法库、SHA-1算法库是本发明的可信密码模块具有而现有技术中的可信密码模块不具有的。

[0097] 本发明的可信密码模块，通过在TCM内部添加RSA密钥处理模块和SHA-1计算模块在命令协议层上来支持国际算法，RSA算法引擎和SHA-1算法引擎可以使用软件方法实现。

[0098] 由上可见，本发明的可信密码模块包括支持国际算法的功能模块，能够支持PKI应用体系，从而扩大了可信密码模块的应用范围。

[0099] 本发明还提出了一种可信计算方法，该可信计算方法用于前述的可信密码模块，包括：

[0100] 根据RSA算法对数据进行第一处理；

[0101] 在第一处理后，根据哈希算法SHA-1对数据进行第二处理。

[0102] 在本发明可信计算方法的一个实施例中，根据RSA算法对数据进行第一处理包括：

[0103] 根据RSA算法创建RSA密钥，以及使用该RSA密钥对数据进行处理；

[0104] 在第一处理后，根据哈希算法SHA-1对数据进行第二处理包括：

[0105] 根据哈希算法SHA-1计算RSA密钥的公钥的哈希值，以及根据该哈希值建立RSA密钥的索引。

[0106] 本发明的可信计算方法，能够支持PKI应用体系，从而扩大了可信密码模块的应用范围。

[0107] 以上所述仅为本发明的较佳实施例，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、改进等，均应包含在本发明的保护范围之内。

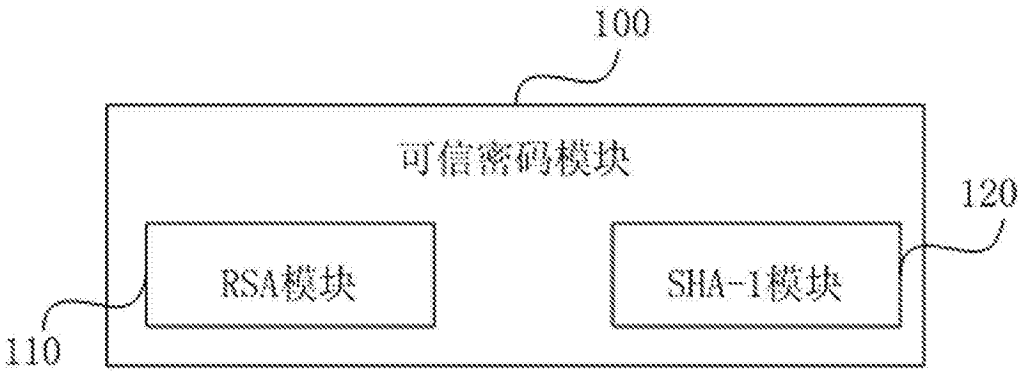

100
可信密码模块
120
RSA模块
SHA-1模块
110

图1

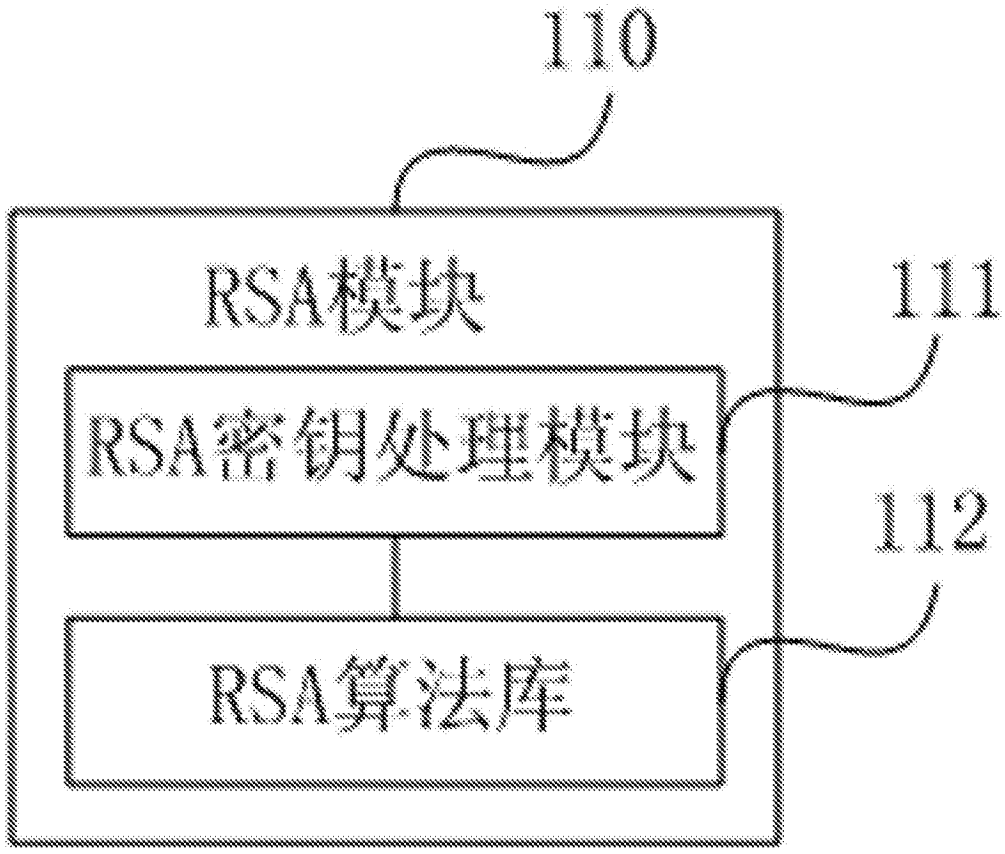

110
RSA模块
111
RSA密钥处理模块
112
RSA算法库

图2

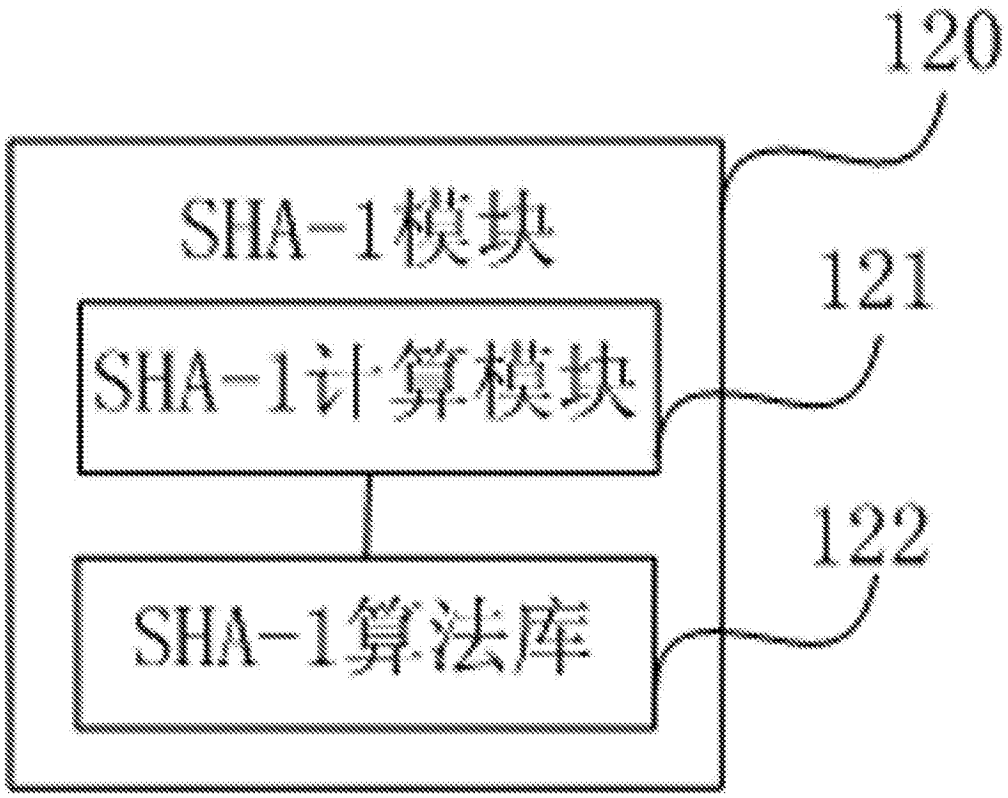


图3

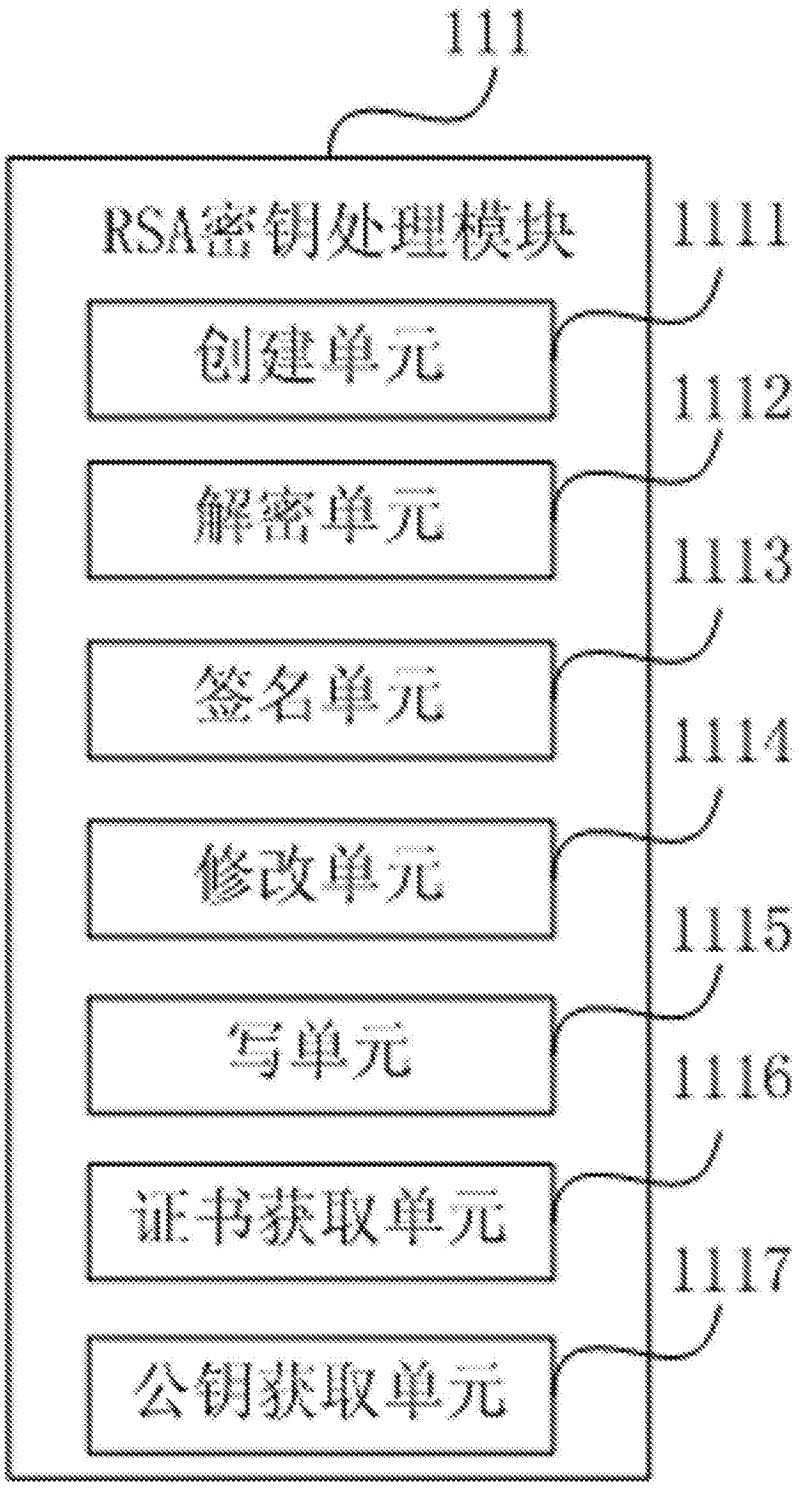

111
RSA密钥处理模块
1111
创建单元
1112
解密单元
1113
签名单元
1114
修改单元
1115
写单元
1116
证书获取单元
1117
公钥获取单元

图4

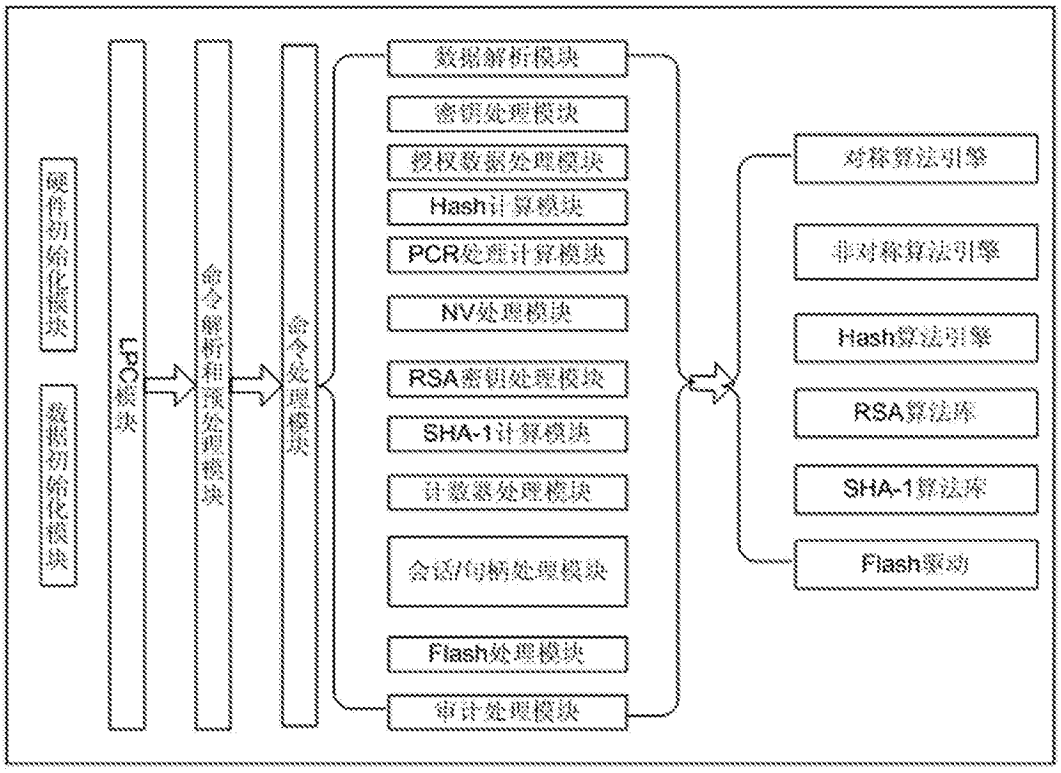

硬件初始化模块
软件初始化模块
LPC模块
命令解析和预处理模块
命令处理模块
数据解析模块
密钥处理模块
授权数据处理模块
Hash计算模块
PCR处理计算模块
NV处理模块
RSA密钥处理模块
SHA-1计算模块
计数器处理模块
会话句柄处理模块
Flash处理模块
审计处理模块
对称算法引擎
非对称算法引擎
Hash算法引擎
RSA算法库
SHA-1算法库
Flash驱动

图5