(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 4 月 16 日 (16.04.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/073206 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01) *G06F 21/00* (2013.01)

(21) 国际申请号: PCT/CN2018/109537

(22) 国际申请日: 2018 年 10 月 9 日 (09.10.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华 为 技 术 有 限 公 司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 蔡 恒 (**CAI, Heng**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (**LONGSUN LEAD IP LTD.**); 中国北京市海淀区北清路68号院3号楼101, Beijing 100094 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

(54) **Title:** CHIP, METHOD FOR GENERATING PRIVATE KEY, AND METHOD FOR TRUSTED VERIFICATION

(54) **发明名称**: 芯片、生成私钥的方法和可信证明的方法

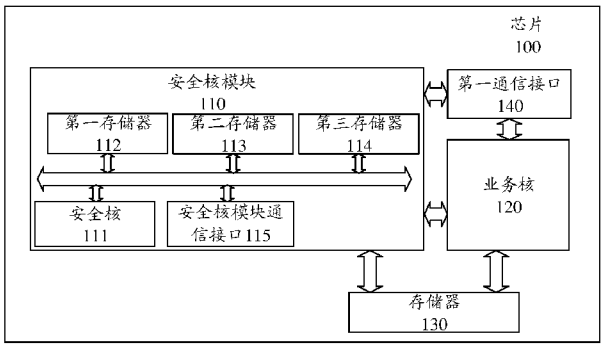

图1

100 Chip
110 Security kernel module
111 Security kernel
112 First memory
113 Second memory
114 Third memory
115 Security kernel module communication interface
120 Service kernel
130 Memory
140 First communication interface

(57) **Abstract:** A chip (700), a method for generating a private key, and a method for trusted verification. The chip (700) comprises a security kernel module (710); the security kernel module (710) comprises a security kernel (711) and a memory (712); the security kernel module (710) performs access isolation on the external modules of the chip (700) other than the security kernel module (710), and the security kernel module (710) performs access isolation on the external devices other than the chip (700); the memory (712) is used for storing a first root public key hash and a unique device secret (UDS) of the chip (700); the security kernel (711) is used for generating a layer-1 public key and a layer-1 private key according to the first root public key hash and the UDS; the memory (712) is used for storing the layer-1 private key. The solution can reduce the possibility that an attacker obtains the layer-1 private key, and performs trusted verification on tampered firmware or information by using the layer-1 private key.

(57) **摘要**: 一种芯片（700）、生成私钥的方法和可信证明的方法，该芯片（700）包括安全核模块（710），该安全核模块（710）包括：安全核（711）和存储器（712），其中，该安全核模块（710）对于该芯片（700）的除该安全核模块（710）外的外部模块访问隔离，且该安全核模块（710）对于该芯片（700）以外的外部设备访问隔离；该存储器（712），用于保存第一根公钥哈希和该芯片（700）的唯一设备秘密UDS；该安全核（711），用于根据该第一根公钥哈希和该UDS生成层1公钥和层1私钥；该存储器（712），用于保存该层1私钥。本方案可以减少攻击者获取到层1私钥，并利用层1私钥对篡改后的固件或信息进行可信证明的可能性。

WO 2020/073206 A1

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

芯片、生成私钥的方法和可信证明的方法

技术领域

本申请涉及信息技术领域，更具体地，涉及芯片、生成私钥的方法和可信证明的方法。

背景技术

计算机设备中的一些芯片对于安全性的要求较高。一旦这些芯片运行的操作系统和/或应用程序（application，APP）被植入恶意代码。攻击者就可以轻易的获取该计算机设备的控制权或者获取该计算机设备中的数据。

例如，服务器中的基板管理控制器（baseboard management controller，BMC）就是这样一种对安全性要求较高的芯片。BMC 通过网络接口提供服务器的远程维护、监控服务器的运行状态等功能。BMC 还可以获取服务器的中央处理器（central processing unit，CPU）的运行状态信息。BMC 还可以管理服务器的基本输入输出系统（basic input output system，BIOS）。一旦攻击者利用 BMC 侧的漏洞，植入恶意的 BMC 固件，就可以轻易地获取服务器的控制权或者该服务器中的数据。

目前业界利用挑战设备验证芯片运行的各层固件的证书方式来确保该芯片运行的固件是可信的。目前业界采用的可信证明流程有如下缺陷：如果私钥发生泄漏，攻击者就可以利用私钥对加入了恶意代码的固件进行签名。因此，需要一种方式可以保证私钥的安全性。

发明内容

本申请提供一种芯片、生成私钥的方法和可信证明的方法，可以减少攻击者获取到私钥，并利用私钥对篡改后的固件或信息进行可信证明的可能性。

第一方面，本申请实施例提供一种芯片，该芯片包括安全核模块，该安全核模块包括：安全核和存储器，其中，该安全核模块对于该芯片的除该安全核模块外的外部模块访问隔离，且该安全核模块对于该芯片以外的外部设备访问隔离；该存储器，用于保存第一根公钥哈希和该芯片的唯一设备秘密 UDS；该安全核，用于根据该第一根公钥哈希和该 UDS 生成层 1 公钥和层 1 私钥；该存储器，用于保存该层 1 私钥。上述技术方案中，由于层 1 私钥被保存在安全核模块内的存储器中，且安全核模块对外访问隔离，这就使得安全核模块外的组件无法访问到保存该层 1 私钥的存储器。这样可以减少攻击者获取到层 1 私钥，并利用层 1 私钥对篡改后的固件或信息进行可信证明的可能性。此外，由于安全核模块集成在芯片中，因此生产该芯片的成本较低，并且对设置有该芯片的电路板的布局空间要求较低。

结合第一方面，在第一方面的一种可能的实现方式中，该安全核模块的地址在该外部模块和该外部设备能够访问的地址范围之外。通过上述技术方案可以实现安全核模块内的各个组件无法被安全核模块外的组件访问。

结合第一方面，在第一方面的一种可能的实现方式中，该存储器还用于保存第二根公钥哈希；该安全核还用于根据该第二根公钥哈希和该 UDS，生成层 2 公钥和层 2 私钥；该存储器还用于保存该层 2 私钥；该安全核，还用于使用该层 1 私钥对层 2 证书进行签名，其中该层 2 证书中包括该层 2 公钥。上述技术方案中，安全核固件只包括层 1 固件和层 2 固件，运行环境简单，但是仍然能够实现固件或数据的可信证明流程。

结合第一方面，在第一方面的一种可能的实现方式中，该安全核，还用于在使用该层 1 私钥对层 2 证书进行签名后，将该层 1 私钥删除。这样可以防止由于层 1 私钥泄漏导致的伪造层 2 证书的情况发生。

结合第一方面，在第一方面的一种可能的实现方式中，该安全核还用于在接收到挑战设备发送的针对目标数据的验证请求信息时，运行安全固件，以根据该层 2 私钥对该目标数据进行签名，并将签名后的目标数据发送给该挑战设备，以便于该挑战设备根据该层 2 公钥对该签名后的目标数据进行验证。这样，可以利用该安全核实现可信证明。

结合第一方面，在第一方面的一种可能的实现方式中，该安全核还用于在接收到挑战设备发送的针对目标数据的验证请求信息时，运行安全固件，以根据该层 1 私钥对该目标数据进行签名，并将签名后的目标数据发送给该挑战设备，以便于该挑战设备根据该层 1 公钥对该签名后的目标数据进行验证。这样，可以利用该安全核实现可信证明。

结合第一方面，在第一方面的一种可能的实现方式中，该芯片还包括业务核，用于运行业务核固件。换句话说，该芯片中业务核保持原有功能不变。这样对于芯片改动较小。

结合第一方面，在第一方面的一种可能的实现方式中，该芯片还包括第一输入输出接口和第二输入输出接口，该第一输入输出接口耦合至该安全核模块，该第二输入输出接口耦合至该业务核。这样，安全核模块和业务核直接没有公用的通信接口，可以进一步隔离该安全核和该业务核。

第二方面，本申请实施例提供一种生成私钥的方法，由芯片中的安全核执行，该安全核位于该芯片的安全核模块中，该安全核模块还包括用于存储第一根公钥哈希和该芯片的唯一设备秘密 UDS 的存储器，该安全核模块对于该芯片的除该安全核模块外的外部模块访问隔离，且该安全核模块对于该芯片以外的外部设备访问隔离，该方法包括：该安全核从存储器中获取该第一根公钥哈希和该 UDS；该安全核根据该第一根公钥哈希和该 UDS 生成层 1 公钥和层 1 私钥；该安全核将该层 1 私钥写入到该存储器中。上述技术方案中，由于层 1 私钥被保存在安全核模块内的存储器中，且安全核模块对外访问隔离，这就使得安全核模块外的组件无法访问到保存该层 1 私钥的存储器。这样可以减少攻击者获取到层 1 私钥，并利用层 1 私钥对篡改后的固件或信息进行可信证明的可能性。

结合第二方面，在第二方面的一种可能的实现方式中，该存储器还用于存储第二根公钥哈希，该方法还包括：该安全核从该存储器中获取该第二根公钥哈希；该安全核根据该第二根公钥哈希和该 UDS，生成层 2 公钥和层 2 私钥；该安全核将该层 2 私钥写入到该存储器中；该安全核使用该层 1 私钥对层 2 证书进行签名，其中该层 2 证书中包括该层 2 公钥。上述技术方案中，安全核固件只包括层 1 固件和层 2 固件，运行环境简单，但是仍然能够实现固件或数据的可信证明流程。

结合第二方面，在第二方面的一种可能的实现方式中，该方法还包括：该安全核在使用该层 1 私钥对层 2 证书进行签名后，将该层 1 私钥删除。这样可以防止由于层 1 私钥泄

漏导致的伪造层 2 证书的情况发生。

结合第二方面，在第二方面的一种可能的实现方式中，该方法还包括：该安全核获取挑战设备发送的针对目标数据的验证请求信息；该安全核根据该层 2 私钥对该目标数据进行签名；该安全核将签名后的目标数据发送给该挑战设备，以便于该挑战设备根据该层 2 公钥对该签名后的目标数据进行验证。这样，可以利用该安全核生成的私钥实现可信证明。

结合第二方面，在第二方面的一种可能的实现方式中，该方法还包括：该安全核获取挑战设备发送的针对目标数据的验证请求信息；该安全核根据该层 1 私钥对该目标数据进行签名；该安全核将签名后的目标数据发送给该挑战设备，以便于该挑战设备根据该层 1 公钥对该签名后的目标数据进行验证。这样，可以利用该安全核生成的私钥实现可信证明。

第三方面，本申请实施例提供一种可信证明的方法，该方法包括：芯片的安全核模块内的安全核获取挑战设备发送的针对目标数据的验证请求信息，其中，该安全核模块对于该芯片的除该安全核模块外的外部模块访问隔离，且该安全核模块对于该芯片以外的外部设备访问隔离；该安全核根据该安全核模块的存储器中保存的私钥对该目标数据进行签名；该安全核向该挑战设备发送签名后的目标数据。上述技术方案中可以利用安全核模块内保存的私钥进行可信证明。并且上述技术方案中，由于用于可信证明的私钥被保存在安全核模块内的存储器中，且安全核模块对外访问隔离，这就使得安全核模块外的组件无法访问到保存该私钥的存储器。这样可以减少攻击者获取到私钥，并利用该私钥对篡改后的固件或信息进行可信证明的可能性。

结合第三方面，在第三方面的一种可能的实现方式中，该芯片的安全核模块内的安全核获取挑战设备发送的验证请求信息，包括：该安全核读取保存在该芯片的存储器中特定存储空间的该验证请求信息。

结合第三方面，在第三方面的一种可能的实现方式中，在该安全核读取保存在该芯片的存储器中的该验证请求信息之前，该方法还包括：该安全核接收该芯片的业务核发送的指示信息，该指示信息用于指示该安全核读取该芯片的存储器的特定存储空间。

结合第三方面，在第三方面的一种可能的实现方式中，该目标数据的类型包括：目标设备中的硬件运行的固件、该目标设备中的硬件运行的固件的哈希、该目标设备运行过程中生成的数据、该目标设备保存的数据，其中该目标设备为设置有该芯片的设备。

附图说明

图 1 是根据本申请实施例提供的一种芯片的结构框图。

图 2 是根据本申请实施例提供的一种对层 1 固件的可信身份进行构建的示意性流程图。

图 3 是根据本申请实施例提供的一种对层 1 固件进行校验的示意性流程图。

图 4 是根据本申请实施例提供的一种生成层 1 私钥和层 1 公钥的示意性流程图。

图 5 是根据本申请实施例提供的一种可信证明流程的示意图。

图 6 是根据本申请实施例提供的另一种可信证明流程的示意图。

图 7 是根据本申请实施例提供的一种芯片的结构框图。

图 8 示出了本申请提供的一种服务器的结构示意图。

图 9 示出了本申请提供的一种终端设备的结构示意图。

图 10 示出了本申请提供的一种网络设备的结构示意图。

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 的情况，其中 A，B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下中的至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a，b 或 c 中的至少一项（个），可以表示：a、b、c、a-b、a-c、b-c、或 a-b-c，其中 a、b、c 可以是单个，也可以是多个。另外，在本申请的实施例中，“第一”、“第二”等字样并不对数量和执行次序进行限定。

需要说明的是，本申请中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其他实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。

为了帮助本领域技术人员更好地理解本申请的技术方案，首先先对本申请实施例中所涉及到的一些概念进行介绍。

本申请实施例中所称的“核”例如是中央处理器（central processing unit，CPU）的核，即，算术逻辑运算单元（arithmetic logic unit，ALU）。

固件（firmware）可以有不同的定义，在计算机领域内的合理解释都适用于本申请。例如，可以有如下解释。以下解释仅为举例说明，而不应被认为是对本申请的技术方案的限定。

固件可以被解释为：预安装到硬件产品内部的只读存储器，与硬件产品捆绑匹配的程序。例如，计算机的基本输入输出系统（basic input output system，BIOS）即属于固件的一种。

固件还可以被解释为：运行在“非控制处理器”中的程序，上述“非控制处理器”指不直接运行操作系统的处理器，例如外设中的处理器，上述“非控制处理器”也可以指被用于裸金属（bare metal）虚拟机系统的处理器中的一些核。

固件还可以被解释为一种特殊的计算机软件。固件可以为计算机设备的特定硬件提供低等级的控制。例如，固件可以为计算机设备中更复杂的软件提供运行环境。又如，对于不太复杂的计算机设备，固件可以充当该计算机设备的完成操作系统，执行所有控制、监视和数据操作功能。该计算机设备的不同功能可以由不同的固件实现。例如操作系统固件可以用于实现操作系统的运行，u-boot 固件可以用于实现引导操作系统固件启动运行。APP 固件用于实现运行在操作系统上的 APP 的运行，不同的 APP 可以由不同的 APP 固件实现。计算机设备内的核通过运行固件的代码实现固件的运行。

在本申请中，安全芯片指的是能够执行可信证明流程以验证外部固件的安全性的芯片，上述外部固件指的是存储在安全芯片的安全核模块之外的固件，该外部固件可以存储在芯片上的存储器中，也可以存储在芯片之外的存储器中。本申请实施例图 1 和图 7 所示

的芯片可以被认为是安全芯片。

由安全核运行的固件可以称为安全核固件。本申请实施例图 1 至图 7 实施例中所称的层 1 固件和层 2 固件都是安全核固件。由业务核运行的固件可以称为业务核固件。相对于业务核固件，安全核固件比较精简，功能单一，因此安全核固件的安全性更高。

唯一设备秘密（unique device secret，UDS）是设备的一个秘密信息，为一段随机数，一旦初始化后，设备生命周期内不可更改；唯一设备秘密（必须）具有访问权限控制，仅支持DICE访问，可升级代码不能读取到唯一设备秘密的值。

设备标识组合引擎（Device Identifier Composition Engine，DICE）：遵循信任计算组（Trusted Computing Group，TCG）发布的 DICE 规范，实现设备组合身份（compound device identifier，CDI）计算的软硬件引擎。

层 1 固件（Layer1 Firmware），也可以称为第一级可变代码、层 1 代码，是核（core）开始执行的第一级/第一级非固化软件代码，该代码的存储介质内容能够被改写。需要说明的是，一些场景将层 0 固件定义为第一级非固化代码。本申请实施例中将层 1 固件定义为第一级非固化代码。

单向函数（One-way function）是一种具有下述特点的单射函数：对于每一个输入，函数值都容易计算（多项式时间），但是给出一个随机输入的函数值，算出原始输入却比较困难。

作为示例而非限定，本申请的可信证明可以根据固件的层数执行，例如，假设芯片中运行有四层固件，则芯片启动后，会生成层 1 私钥、层 2 私钥、层 3 私钥和层 4 私钥；使用层 1 私钥对层 2 固件的证书（以下简称层 2 证书）进行签名，得到签名后的层 2 证书；使用层 2 私钥对层 3 固件的证书（以下简称层 3 证书）进行签名，得到签名后的层 3 证书；使用层 3 私钥对层固件的证书（以下简称层 4 证书）进行签名，得到签名后的层 4 证书；签名后的层 1 证书至层 4 证书组成证书链，其中证书链中每层证书中包括每层固件的哈希以及每层公钥，例如层 1 证书中包括层 1 固件的哈希和层 1 公钥，层 2 证书中包括层 2 固件的哈希和层 2 公钥，以此类推，其中层 1 证书是证书授权（Certificate Authority，CA）中心使用 CA 私钥进行签名的。该芯片在接收到挑战设备发送的随机数（nounce）后，使用层 4 私钥对证书链（即层 1 至层 4 证书）和该随机数进行签名，并将签名后的数据发送至该挑战设备。该挑战设备中可以计算出或者保存层 1 至层 4 固件的哈希。该挑战设备中还可以保存 CA 公钥以及层 4 公钥。该挑战设备接收到签名后的数据后，利用层 4 公钥对该签名后的数据进行解密，得到签名后的层 1 证书、签名后的层 2 证书、签名后的层 3 证书和签名后的层 4 证书；利用 CA 公钥，对签名后的层 1 证书进行解密，得到层 1 固件的哈希和层 1 公钥；利用层 1 的公钥，对签名后的层 2 证书进行解密，得到层 2 固件的哈希和层 2 公钥，以此类推。该挑战设备如果无法使用一层的公钥对下一层签名后的证书进行解密，则表示证书链被篡改。挑战设备如果成功对证书链中的全部签名后的证书进行解密，则比较解密得到的固件的哈希与该挑战设备保存的固件的哈希是否一致，如果一致，则证明该芯片运行的各个固件没有被篡改，如果不一致，则表明该芯片运行的固件被篡改。

图 1 是根据本申请实施例提供的一种芯片的结构框图。如图 1 所示，芯片 100 包括：安全核模块 110、业务核 120、存储器 130、第一通信接口 140。当然，芯片 100 还可以包括除了上述组件以外的其他组件，在此就不必一一列出。为便于描述，以下假设芯片 100

是设置在服务器中的一个芯片。

应理解，图 1 所示的芯片的结构仅为示例性说明，本申请并未限定于此，例如，芯片 100 也可以不包括业务核 120。此情况下，该业务核 120 的功能可以由与该芯片 100 配置在同一计算设备中的芯片（具体地说，是芯片中能够运行业务固件的核）提供。或者，该业务核 120 的功能可以由与配置有该芯片 100 的计算设备联合使用的计算设备(具体地说，是计算设备中能够运行业务固件的核）提供。又如，芯片 100 可以包括多个业务核或者多个存储器。不同的业务核可以执行不同的业务核固件，以实现相应的功能。

图 1 所示的芯片是对安全性要求较高的芯片，例如，服务器中的 BMC，终端设备的系统级（System-on-a-Chip，SoC）芯片；网络设备中的 SoC 芯片。

业务核 120 可以执行业务核固件，以实现该芯片的相应功能。例如，若芯片 100 为 BMC，则业务核 120 可以通过执行业务核固件，以实现 BMC 能够实现的功能，例如提供服务器的远程维护、监控服务器的运行状态、获取 CPU 的运行状态信息等功能。

又如，若芯片 100 为终端设备的 SoC 芯片，则业务核 120 可以通过执行业务核固件，以实现终端设备的 SoC 芯片能够实现的功能，例如对通信协议以及通信数据进行处理，以及对整个终端设备进行控制，执行软件程序，处理软件程序的数据等功能。

又如，若芯片 100 为网络设备的 SoC 芯片，则业务核 120 可以通过执行业务核固件，以实现网络设备的 SoC 芯片能够实现的功能，例如假设该网络设备为基站，该业务核 120 可以通过执行业务核固件能够实现在基带单元（baseband unit，BBU）（也可称为数字单元（digital unit，DU））启动时为 BBU 提供安全启动保障

安全核模块 110 与存储器 130 之间通过内部连接通路互相通信，传递控制和/或数据信号。

业务核 120 与存储器 130 之间通过内部连接通路互相通信，传递控制和/或数据信号。

存储器 130 是允许被多次擦写的非易失性存储器。例如，电可擦除可编程只读存储器（Electrically-Erasable Programmable Read-Only Memory，EEPROM）、快闪存储器（Flash memory）等。

安全核模块 110 包括：安全核 111、第一存储器 112、第二存储器 113、第三存储器 114 和安全核模块通信接口 115。安全核 111 与第一存储器 112、第二存储器 113、第三存储器 114 之间可以通过内部连接通路互相通信。例如，安全核 111 可以读取保存在第一存储器 112、第二存储器 113 和第三存储器 114 中的信息，或者将信息发送至第二存储器 113 和第三存储器 114，第二存储器 113 和第三存储器 114 可以将接收到的信息进行保存。安全核 111 与安全核模块通信接口 115 也可以通过内部链接通路互相通信，可以通过安全核模块通信接口 115 将信息发送至其他组件、设备或装置或者接收其他组件、设备或装置发送的信息。

安全核模块 110 与业务核 120 之间可以通过内部连接通路互相连接。安全核 111 能够访问安全核模块 110 外的各个组件。安全核模块 110 对外访问隔离。具体地，安全核模块 110 对于芯片 100 的除安全核模块 110 外的外部模块访问隔离，且安全核模块 110 对于芯片 100 以外的外部设备访问隔离。

安全核模块 110 对于芯片 100 的除安全核模块 110 外的外部模块访问隔离是芯片 100 的除安全核模块 110 外的模块无法访问安全核模块 110 内的各个组件。例如，业务核 120

无法访问安全核模块 110 内的各个组件，例如业务核 120 无法访问安全核模块 110 内的第一存储器 112、第二存储器 113 或第四存储器 114。

安全核模块 110 对于芯片 100 以外的外部设备访问隔离是芯片 100 外的外部设备无法访问安全核模块 110 内的各个组件。例如，服务器内的 CPU 无法访问安全核模块 110 内的各个组件，例如服务器内的 CPU 无法访问安全核模块 110 内的第一存储器 112、第二存储器 113 或第四存储器 114。

安全核 111 能够访问安全核模块 110 外的各个组件。例如，安全核 111 能够访问业务核 120 的存储空间以获取业务核 120 运行的固件。又如，安全核 111 能够访问存储器 130，以获取存储器 130 保存的数据或者将要保存至存储器 130 的数据发送至存储器 130。又如，安全核 111 能够访问芯片 100 外的存储器，例如服务器的存储器，以获取该存储器保存的数据或者将希望保存至该存储器的数据发送至该存储器。

可选的，在一些实施例中，业务核 120 在非安全模式时，安全核模块 110 对于业务核 120 访问隔离。业务核 120 在安全模式时，可以访问安全核模块 110 内的组件。在安全模式下，业务核运行的是经过一些有限的代码，这些代码都是经过验证过的安全的代码。业务核在安全模式时访问安全核模块 110 内的组件不会篡改安全核模块 110 中保存的数据，也不会将安全核模块 110 中保存的数据泄露给攻击者。因此，业务核在安全模式时访问安全核模块 110 内部的组件是安全的。

可选的，在一些实施例中，安全核模块 110 在任何时候都对于安全核模块 110 外的组件访问隔离。这样，可以保证业务核 120 与安全核模块 110 完全隔离，避免利用业务核 120 来访问第一存储器 112、第二存储器 113 和第三存储器 114。

安全核模块 110 内的组件（即安全核 111、第一存储器 112、第二存储器 113 和第三存储器 114 等）的属性为主组件，从组件，和主从属性的组件。所有带从属性组件，仅安全核内部有主属性组件有能力访问。外部组件（即外部设备和外部模块）不能访问。安全核模块 110 内部的带从属性组件的地址不在外部组件能够访问的地址范围内。

具体地，安全核模块 110 中与芯片 100 内的其他组件进行通信的安全核模块通信接口 115 只有主（master）接口，没有从（slave）接口。因此，安全核模块 110 可以对外发起主访问，但是安全核模块 110 外的组件，例如业务核 120，无法对安全核模块 110 内的组件发起主访问。在此情况下，安全核模块 110 以外的组件的地址在安全核模块 110 能够访问的地址空间范围内，而安全核模块 110 内部各个组件（例如安全核 111、第一存储器 112 等）的地址不在安全核模块 110 以外的组件能够访问的地址空间范围内。因此，安全核模块 110 可以利用安全核模块通信接口 115 与安全核模块 110 以外的组件进行通信，而安全核模块 110 外的组件（例如业务核 120 或者芯片 100 外的组件）无法访问安全核模块 110 内部的组件，例如安全核模块 110 内的各个存储器。

安全核模块 110 内带有从属性的组件可以是安全核模块 110 内部的存储器，例如第一存储器 112、第二存储器 113 和第三存储器 114。安全核模块 110 内部属性为主组件的组件可以是安全核 111。

可选的，在一些实施例中，第一存储器 112，用于存储芯片 100 的 UDS。第一存储器 112 中保存的该 UDS 无法被删除或更改。换句话说，第一存储器 112 中保存的该 UDS 在任何时候均无法被删除或更改。如果希望更改芯片 100 内的第一存储器 112 中保存的 UDS，

只能通过更换新的第一存储器实现。该 UDS 用于生成层 1 私钥和层 1 公钥。因此，如果该 UDS 被篡改，则会导致层 1 私钥和层 1 公钥发生错误。因此，第一存储器 112 中保存的 UDS 无法被更改或删除可以提高芯片 100 的安全性。该第一存储器 112 中保存的 UDS 可以通过烧写锁定的方式实现该 UDS 无法被更改。换句话说，第一存储器 112 中保存的 UDS 被锁定烧写。

可选的，在一些实施例中，第一存储器 112 保存的该 UDS 在芯片 100 每次上电后仅允许被读取一次。例如，芯片 100 上电后，可以将该 UDS 读取到第三存储器 114，除非芯片 100 复位，否则不再读取该 UDS。使用完该 UDS 后，可以将该 UDS 从第三存储器 114 删除。该 UDS 只允许在生成层 1 公钥和层 1 私钥密钥的时候被读取一次。这样，可以防止该 UDS 泄漏造成的攻击者可能利用 UDS 伪造层 1 私钥和层 1 公钥的情况发生。

第一存储器 112 可以是一次性可编程非易失存储器（One-time programmable non-volatile memory，OTP NVM）。OTP NVM 也可以称为可编程只读存储器（Programmable read-only memory，PROM）、一次性可编程（One-time programmable，OTP）存储器。电子熔丝（eFuse）是一种典型的 OTP 存储器。

OTP 存储器是一种特殊类型的非易失性存储器（NVM），它允许将数据仅写入存储器一次。写入到 OTP 存储器中的数据可以通过烧写锁定的方式禁止删除或修改。换句话说，若第一存储器 112 为 OTP 存储器，则可以在芯片制造阶段将该 UDS 写入到该第一存储器 112，并进行烧写锁定，这样写入到第一存储器 112 中的该 UDS 无法被删除或者更改。

本申请对 UDS 如何写入到该第一存储器 112 的实现方式并不限定。例如，该 UDS 可以是在设备生产过程中，通过硬件接口或软件接口写入到该第一存储器 112 中的固化的随机数，不同设备的 UDS 不一样。因此，UDS 具有随机性。设备生产过程可以是将芯片 100 加工到电路板的过程。或者该 UDS 也可以是利用物理层防克隆功能（physical unclonable function，PUF）技术，在芯片 100 生产阶段，由专用设备生成并写入到第一存储器 112 中的。

可选的，在一些实施例中，第一存储器 112，用于存储芯片 100 的 UDS。第一存储器 112 中保存的该 UDS 在芯片 100 的工作过程中无法被删除或更改。换句话说，第一存储器 112 可以是需要特定设备才能将第一存储器 112 中保存的数据进行删除或修改的存储器。例如，第一存储器 112 可以是可擦除可编程只读存储器（Erasable Programmable Read Only Memory，EPROM）。EPROM 封装中包含有玻璃窗，通过强紫外线照射该玻璃窗可以将 EPROM 中的数据删除。通常，写入数据后的 EPROM 的玻璃窗会被盖住，以防止遭受阳光直射。因此，芯片 100 在工作过程中，EPROM 中的数据无法被删除或更改。

可选的，在一些实施例中，第一存储器 112 可以包括一个安全启动指示位。当完成对第一存储器 112 中的数据写入后，该安全启动指示位为被置为使能。例如，若该安全启动指示位的值为 0，则表示该安全启动指示位未使能。在此情况下，第一存储器 112 中的数据尚未写入完成。若安全启动指示位的值为 1，则表示该安全启动指示位使能。在此情况下，第一存储器 112 中的数据已经写入完成。

第一存储器 112 中还可以存储第一校验信息。该第一校验信息是用于对层 1 固件进行校验的相关信息，

可选的，在一些实施例中，该第一校验信息可以包括第一根公钥哈希（hash）、第一吊销标识信息、第一安全版本号信息。

可选的，在一些实施例中，该第一存储器 112 中可以只存储该第一根公钥哈希。该第一吊销标识信息和/或该第一安全版本号信息可以存储在第二存储器 113 中。

可选的，在另一些实施例中，该第一校验信息中的所有内容都可以存储在该第一存储器 112 中。

与存储在第一存储器 112 中的 UDS 类似，存储在第一存储器 112 中的第一根公钥哈希不允许被删除和修改。具体地，该第一根公钥哈希在写入到第一存储器 112 后，进行烧写锁定。换句话说，写入到第一存储器 112 中的第一根公钥哈希被锁定烧写。这样可以避免因第一根公钥哈希被修改造成的无法对层 1 固件进行校验。

与存储在第一存储器 112 中的 UDS 类似，在一些实施例中，存储在第一存储器 112 中的第一根公钥哈希在芯片 100 工作的过程中不允许被删除或更改。

若第一存储器 112 中还存储该第一吊销标识信息，则该第一吊销标识信息可以被更改，更改的方式是可以将该第一吊销标识信息中 0 更改为 1。但是，不能将该第一吊销标识信息中的 1 更改为 0。例如，10 是该第一吊销标识信息中包括的一个吊销标识，10 可以被修改为 11，但是不能被修改为 00 或 01。

若第一存储器 112 中还存储该第一安全版本号信息，则该第一安全版本号信息可以被更改，更改的方式是可以将该第一安全版本号信息中 0 更改为 1。但是，不能将该第一安全版本号信息中的 1 更改为 0。例如，10 是该第一安全版本号信息中包括的一个安全版本号，10 可以被修改为 11，但是不能被修改为 00 或 01。

可选的，在一些实施例中，该第一校验信息可以只包括该第一根公钥哈希。

可选的，在另一些实施例中，该第一校验信息可以包括该第一根公钥哈希，该第一校验信息还可以包括该第一吊销标识信息和该第一安全版本号信息中一个。

第二存储器 113，用于保存引导（Boot-Rom）代码。

第二存储器 113 是非易失性存储器（non-volatile memory，NVM），例如，第二存储器 113 可以是只读存储器（read-only memory，ROM），也可以是 PROM、EPROM、OTP NVM、EEPROM、快闪存储器等。

第三存储器 114 是可读写存储器，即允许被多次擦写的存储器。例如第三存储器 114 可以是随机存储器（Random-Access Memory），例如静态随机存取存储器（Static Random-Access Memory，SRAM）、动态存储存取存储器（Dynamic Random Access Memory，DRAM）。第三存储器还可以是 EEPROM、快闪存储器等允许被多次擦写的存储器。

NVM 包括 OTP NVM。因此，在一些实施例中，第一存储器 112 与第二存储器 113 可以由同一个存储器实现。该存储器可以实现第一存储器 112 和第二存储器 113 的功能，即该存储器可以用于存储 UDS、该第一校验信息以及引导代码。当然，本申请实施例也并不排除可以使用两个 OTP NVM 分别实现第一存储器 112 的功能和第二存储器 113 的功能。

一些 NVM，例如 EEPROM 和快闪存储器等，也允许被多次擦写。因此，在一些实施例中，第二存储器 113 与第三存储器 114 也可以由同一个存储器实现。该存储器允许被多次擦写的 NVM。该存储器可以实现第二存储器 113 和第三存储器 114 的功能，即该存储

器可以用于存储引导代码以及保存复制的层 1 固件。当然，本申请实施例也并不排除可以使用两个允许被多次擦写的 NVM 分别实现第二存储器 113 的功能和第三存储器 114 的功能。

安全核 111 可以用于执行如图 2 所示的方法完整对层 1 固件的可信身份的构建。

图 2 是根据本申请实施例提供的一种对层 1 固件的可信身份进行构建的示意性流程图。

201，安全核 111 对层 1 固件进行校验。

若安全核 111 对层 1 固件进行校验通过，则执行步骤 202。安全核 111 对层 1 固件进行校验的过程可以参见图 3 所示的流程图。

可选的，在一些实施例中，若安全核 111 对层 1 固件校验失败，则安全核 111 停止运行，发送校验失败指示消息，提醒用户安全核 111 层 1 固件校验失败。

可选的，在另一些实施例中，若安全核 111 对层 1 固件校验失败，则安全核 111 可以对备用层 1 固件进行校验。若安全核 111 对备用层 1 固件进行校验通过，则执行步骤 202。若继续校验失败，则停止运行，发送校验失败指示消息，提醒用户安全核 111 层 1 固件校验失败。

202，安全核 111 生成层 1 私钥和层 1 公钥。

安全核 111 生成层 1 私钥和层 1 公钥的过程可以参见图 4 所示的流程图。

图 3 是根据本申请实施例提供的一种对层 1 固件进行校验的示意性流程图。

安全核 111 通过执行第二存储器 113 保存的 Boot-Rom 代码实现如图 3 所示的对层 1 固件的校验流程。

具体地，安全核 111 根据第一校验信息、层 1 固件校验相关信息，对层 1 固件进行校验。

层 1 固件校验相关信息包括第一根公钥、二级密钥公钥的签名结果、二级密钥公钥、层 1 固件与层 1 固件版本号的签名结果。层 1 固件校验相关信息还可以包括以下信息中的任一个或多个：二级密钥标识（ID）、层 1 固件版本号。

本申请实施例对用于保存层 1 固件和层 1 固件校验相关信息的存储器并不限定。例如，在一些实施例中，层 1 固件和层 1 固件校验相关信息可以保存在第二存储器 113 中。在另一些实施例中，层 1 固件和层 1 固件校验相关信息可以保存在安全核模块 110 外的存储器中。例如，层 1 固件和层 1 固件校验相关信息可以保存到存储器 130 中。又如，层 1 固件和层 1 固件校验相关信息可以保存在芯片 100 外的存储器中，例如服务器的存储器。

可选的，在一些实施例中，安全核 111 可以将层 1 固件复制到第三存储器 114。这样，在安全核 111 对层 1 固件进行校验时，安全核 111 可以直接从第三存储器 114 读取该层 1 固件，而无需从安全核模块 110 外的存储器读取该层 1 固件。安全核 111 访问第三存储器 114 的速度要快于访问安全核 110 外的存储器的访问速度。因此，将该层 1 固件复制到第三存储器 114 可以加快对层 1 固件进行校验的速度。类似的，安全核 111 也可以将层 1 固件校验相关信息复制到第三存储器 114 中，从而加快对层 1 固件进行校验的速度。换句话说，安全核 111 是对保存在第三存储器 114 中的层 1 固件进行校验。

可选的，在另一些实施例中，安全核 111 可以在对层 1 固件校验通过后将层 1 固件复制到第三存储器 114。换句话说，安全核 111 是对保存在安全核模块 110 外的存储器中的

层 1 固件进行校验。

安全核 111 可以根据信息头确定层 1 固件校验相关信息以及层 1 固件在存储器中的位置。信息头可以指示层 1 固件校验相关信息中的各个信息在存储器中的偏移位置和大小。例如信息头可以指示第一根公钥在存储器内的偏移位置和大小、二级密钥公钥的签名结果在存储器内的偏移位置和大小等。该信息头还可以指示层 1 固件在存储器内的偏移位置和大小。上述信息头的作用仅是举例说明，信息头还可以指示其它内容。

安全核 111 根据第一校验信息、层 1 固件校验相关信息，对层 1 固件进行校验流程如下：

301，若第一存储器 112 中包括安全启动指示位，则先判断该安全启动指示位是否使能。若该安全启动指示位使能，则利用第一存储器 112 中保存的第一根公钥哈希对层 1 固件校验相关信息中的第一根公钥进行校验。若该安全启动指示位未使能，则无需进行固件校验。此时，可以认为层 1 固件校验成功。

具体地，利用第一根公钥哈希对层 1 固件相关信息中的第一根公钥进行校验过程如下：计算该第一根公钥的哈希，比较计算出的第一根公钥的哈希与第一储器 112 保存的第一根公钥哈希是否一致。如果一致，则该第一根公钥校验成功，进行步骤 302；如果不一致，则校验失败。若第一存储器 112 中不包括安全启动指示位，则可以直接利用第一存储器 112 中保存的第一根公钥哈希对该第一根公钥进行校验。

302：利用第一根公钥对层 1 固件校验相关信息中的二级密钥公钥的签名结果进行签名校验，若签名校验通过，则执行步骤 303；若校验不通过，则校验失败。

由于步骤 302 是在第一根公钥校验成功后执行的，因此可以保证步骤 302 中使用的第一根公钥是可信的。

具体地，待校验的二级密钥公钥的签名结果是通过以下方式生成的：首先对二级密钥公钥进行哈希运算，得到二级密钥公钥的哈希，然后使用第一根私钥对二级密钥公钥的哈希进行加密（即签名处理），得到二级密钥公钥的签名结果。

利用第一根公钥对二级密钥公钥的签名结果进行签名校验的过程如下：首先利用该第一根公钥对该二级密钥公钥的签名结果进行解密，得到一个哈希；对该二级密钥公钥进行哈希计算可以得到另一个哈希；比较这两个哈希是否相同，若相同，则对二级密钥公钥的签名结果的签名校验通过；若不相同则校验不通过。

303：根据第一存储器 112 中保存的第一吊销标识信息，确定层 1 固件校验相关信息中的二级密钥标识（ID）是否已吊销，若该二级密钥标识未吊销，则执行步骤 304；若该二级密钥标识已吊销，则校验失败。

可选的，在一些实施例中，该第一吊销标识信息中可以包括已吊销的二级密钥标识。在此情况下，若该第一吊销标识信息中不包括该二级密钥标识，则确定该二级密钥标识未吊销；若该第一吊销标识信息中包括该二级密钥标识，则确定该二级密钥标识已吊销。

可选的，在另一些实施例中，该第一吊销标识信息中可以包括未吊销的二级密钥标识。在此情况下，若该第一吊销标识信息中包括该二级密钥标识，则确定该二级密钥标识未吊销；若该第一吊销标识信息中不包括该二级密钥标识，则确定该二级密钥标识已吊销。

可选的，在一些实施例中，可以不执行步骤 303。换句话说，在一些实施例中，无需确定二级密钥标识是否已经被吊销。在此情况下，该层 1 固件相关信息中无需包括二级密

钥标识，相应的，该第一校验信息中也不需要包括该第一吊销标识信息。可以理解，若不需要执行步骤 303，则步骤 302 中签名校验通过后可以直接执行步骤 304。

304：使用二级密钥公钥对层 1 固件与层 1 固件版本号的签名结果进行签名校验，若签名校验通过，则执行步骤 305；若校验不通过，则校验失败。

具体地，待校验的层 1 固件与层 1 固件版本号的签名结果可以通过以下两种方式生成：

方式 1，首先对层 1 固件与层 1 固件版本号进行哈希运算，得到一个哈希；然后使用二级密钥私钥对这个哈希进行加密（即签名处理），得到层 1 固件与层 1 固件版本号的签名结果。

方式 2，首先对层 1 固件进行哈希运算，得到层 1 固件的哈希；然后对层 1 固件的哈希和层 1 固件版本号进行哈希运算，得到一个哈希；然后使用二级密钥私钥对这个哈希进行加密（即签名处理），得到层 1 固件与层 1 固件版本号的签名结果。

若层 1 固件与层 1 固件版本号的签名结果使用的是上述方式 1 确定的，则使用二级密钥公钥对层 1 固件与层 1 固件版本号的签名结果进行签名校验过程如下：使用二级密钥公钥对层 1 固件与层 1 固件版本号的签名结果进行解密，得到一个哈希；对层 1 固件与层 1 固件版本号进行哈希运算，得到一个哈希；比较这两个哈希是否相同，若相同，则对层 1 固件与层 1 固件版本号的签名结果进行签名校验通过，若不相同，则校验不通过。

若层 1 固件与层 1 固件版本号的签名结果使用的是上述方式 2 确定的，则使用二级密钥公钥对层 1 固件与层 1 固件版本号的签名结果进行签名校验过程如下：使用二级密钥公钥对层 1 固件与层 1 固件版本号的签名结果进行解密，得到一个哈希；对层 1 固件的哈希与层 1 固件版本号进行哈希运算，得到一个哈希；比较这两个哈希是否相同，若相同，则对层 1 固件与层 1 固件版本号的签名结果进行签名校验通过，若不相同，则校验不通过。

305：根据第一存储器 112 保存的第一安全版本号信息，确定该层 1 固件版本号是否为安全版本号。若该层 1 固件版本号是安全版本号，则执行步骤 306；若该层 1 固件版本号不是安全版本号，则校验失败。

可选的，在一些实施例中，该第一安全版本号信息中可以包括安全版本号。在此情况下，若该第一安全版本号信息中包括该层 1 固件版本号，则该层 1 固件版本号是安全版本号；若该第一安全版本号信息中不包括该层 1 固件版本号，则该层 1 固件版本号不是安全版本号。

可选的，在另一些实施例中，该第一安全版本号信息中可以包括非安全版本号。在此情况下，若该第一安全版本号信息中不包括该层 1 固件版本号，则该层 1 固件版本号是安全版本号；若该第一安全版本号信息中包括该层 1 固件版本号，则该层 1 固件版本号不是安全版本号。

可选的，在一些实施例中，可以不执行步骤 305。换句话说，在一些实施例中，无需确定层 1 固件版本号是否是安全版本号。在此情况下，该层 1 固件相关信息中无需包括层 1 固件版本号，相应的，该第一校验信息中也不需要包括该第一安全版本号信息。可以理解，若不需要执行步骤 305，则步骤 304 中签名校验通过后可以直接执行步骤 306。进一步，若层 1 固件相关信息中不包括层 1 固件版本号，则层 1 固件校验相关信息应包括层 1 固件的签名结果而非是层 1 固件与层 1 固件版本号的签名结果。相应的，步骤 304 中校验的对象是层 1 固件的签名结果而非是层 1 固件与层 1 固件版本号的签名结果。

306：对层 1 固件进行哈希计算，得到层 1 固件的哈希，并与 304 中签名校验过层 1 固件的哈希进行比较，若两个层 1 固件的哈希一致，则对层 1 固件校验通过；若两个层 1 固件的哈希不一致，则校验失败。

安全核 111 在对层 1 固件进行校验成功的情况下，可以执行如图 4 所示的方法生成层 1 私钥和层 1 公钥。

图 4 是根据本申请实施例提供的一种生成层 1 私钥和层 1 公钥的示意性流程图。

401，安全核 111 在根据该第一校验信息对层 1 固件校验通过的情况下，继续执行第二存储器 113 保存的 Boot-Rom 代码，生成 CDI。

具体地，安全核 111 可以根据该 UDS 和该层 1 固件的哈希，确定 CDI，并将该 CDI 传递至层 1 固件，以便层 1 固件根据该 CDI 确定层 1 私钥和公钥。传递该 CDI 的方式可以是将该 CDI 保存至第三存储器 114 中。

安全核 111，可以用于根据该 UDS 和该层 1 固件的哈希，利用单向函数进行单向计算生成该 CDI。用于进行单向计算单向函数可以是散列消息认证码（Hash-based message authentication code，HMAC）、安全散列算法（Secure Hash Algorithms，SHA）-256、SHA-512、MD5 消息摘要算法（MD5 Message-Digest Algorithm）等。

例如，安全核 111 可以用于通过计算 HMAC（UDS，Hash（Layer1））生成该 CDI，其中 UDS 表示第一存储器 112 中保存的 UDS，Hash（Layer1）表示对层 1 固件的哈希。HMAC（UDS，Hash(Layer1)）表示以 UDS 为密钥对层 1 固件的哈希进行 HMAC 签名，得到的签名就是该 CDI。

402，在计算出该 CDI 后，安全核 111 可以运行层 1 固件，生成层 1 私钥和层 1 公钥，并将生成的该层 1 私钥保存在第三存储器 114 中。该层 1 的公钥可以保存至安全核模块 110 外的存储器中，例如，存储器 130 或者芯片 100 外的存储器中，例如服务器的存储器。

用于生成该层 1 公钥和该层 1 私钥的非对称加密算法可以是李维斯特-萨莫尔-阿德曼（Rivest–Shamir–Adleman，RSA）加密算法，例如 RSA-2048、RSA-3072、RSA-4096 等，也可以是椭圆曲线密码学（elliptic curve cryptography，ECC）算法，例如 ECC256、ECC384、ECC512 等。

可选的，在一些实施例中，第一存储器 112 保存的该 UDS 在芯片 100 每次上电后仅允许被读取一次。

如上所述，安全核模块 110 以外的其他任何设备都无法访问安全核模块 110 内的各个组件或者只有业务核 120 在安全模式的情况下才可以访问安全核模块 110 内的各个组件，这样保存在第三存储器 114 内的层 1 私钥无法被泄漏。这样可以避免利用层 1 私钥伪造层 2 证书的风险。

进一步，在芯片 100 的生产阶段，安全核 111 还可以通过安全核模块通信接口 115 将层 1 证书信息发送至证书颁发设备并通过安全核模块通信接口 115 接收该证书颁发设备发送的使用 CA 私钥签名的层 1 证书信息（以下简称“CA 签名层 1 证书”）。

该层 1 证书信息可以是包含有层 1 公钥的各种信息。可选的，在另一些实施例中，该层证书信息中除了包括该层 1 公钥外，还可以包括层 1 固件的标识。该层 1 固件的标识可以是层 1 固件的哈希。

可选的，在一些实施例中，该层 1 证书信息可以是由安全核 111 生成的层 1 证书。该

层 1 证书中包括层 1 公钥。该层 1 证书中还可以包括层 1 固件的标识，层 1 固件的标识可以是层 1 固件的哈希。

可选的，在另一些实施例中，该层 1 证书信息可以是由安全核 111 进行自签名后得到的自签名证书。具体地，安全核 111 可以生成层 1 证书，使用层 1 私钥对层 1 证书进行签名，得到该自签名证书。因此，该自签名证书中包括层 1 公钥。该自签名证书中还可以包括层 1 固件的标识，层 1 固件的标识可以是层 1 固件的哈希。通过使用层 1 私钥对层 1 证书进行签名，可以保证层 1 证书的完整性，即若层 1 证书中某些字节在传递过程中被修改，这些修改也可以被识别。

可选的，在另一些实施例中，该层 1 证书信息可以是证书签名请求（certificate signing request，CSR），该 CSR 中包括安全核 111 生成的层 1 证书。因此，该 CSR 中包括层 1 公钥。该 CSR 中还可以包括层 1 固件的标识，层 1 固件的标识可以是层 1 固件的哈希。

相应的，该 CA 签名层 1 证书中包括层 1 公钥。若该层 1 证书信息中还包括层 1 固件的标识，则该 CA 签名层 1 证书中还可以包括该层 1 固件的标识。

具体地，在芯片 100 的生产阶段，安全核 111 可以执行如图 2 所示的方法生成层 1 私钥和层 1 公钥，并根据该层 1 公钥生成该层 1 证书信息。芯片 100 可以连接至证书颁发设备，将该层 1 证书信息发送至该证书颁发设备。该证书颁发设备将该层 1 证书信息发送至 CA 中心。CA 中心使用 CA 私钥对该层 1 证书信息进行签名，得到 CA 签名层 1 证书，并将 CA 签名层 1 证书发送至该证书颁发设备，该证书颁发设备将接收到 CA 签名层 1 证书发送至芯片 100 的安全核模块 110。

可选的，在一些实施例中，安全核模块 110 可以与第一通信接口 140 通过内部连接通路互相通信。在此情况下，该层 1 证书信息可以直接通过芯片 100 的第一通信接口 140 发送至该证书颁发设备。

此外，如上所述，安全核 111 能够访问安全核模块 110 外的各个组件。因此，在另一些实施例中，该层 1 证书信息可以通过业务核 120 发送至该证书颁发设备。具体地，安全核 111 可以通过安全核模块通信接口 115 将该层 1 证书信息发送至业务核 120。业务核 120 可以通过第一通信接口 140 将该层 1 证书信息发送至该证书颁发设备。

虽然安全核模块 110 对于安全核模块 110 外的组件访问隔离，但是安全核模块 110 外的组件可以向安全核模块 110 发送一些信息。因此，在一些实施例，第一通信接口 140 接收到的该证书颁发设备发送的 CA 签名层 1 证书可以直接发送至安全核模块通信接口 115。安全核 111 获取安全核模块通信接口 111 接收到的该 CA 签名层 1 证书。

可选的，在一些实施例中，第一通信接口 140 可以将接收到的 CA 签名层 1 证书发送至业务核 120。业务核 120 可以将接收到的 CA 签名层 1 证书写入至存储器 130 的特定存储空间。该特定存储空间是业务核 120 和安全核 111 共享的存储空间。换句话说，业务核 120 与安全核 111 都可以访问该存储空间，读取该存储空间内保存的数据或者将数据写入到该存储空间。安全核 111 可以通过安全核模块通信接口 115 周期性地访问该特定存储空间。若安全核 111 确定该存储空间内存储有该 CA 签名层 1 证书，则通过安全核模块通信接口 115 获取该 CA 签名层 1 证书。

虽然安全核模块 110 对安全核模块 110 外的组件访问隔离，但是业务核 120 可以向安全核 111 发送一些指示信息。因此，在另一些实施例中，第一通信接口 140 可以将接收到

的CA签名层1证书发送至业务核120。业务核120可以将接收到的CA签名层1证书写入至存储器130的特定存储空间，然后向安全核111发送一个指示信息，该指示信息用于指示安全核111读取该特定存储空间。安全核111在接收到该指示信息后，通过安全核模块通信接口115读取该特定存储空间，获取该CA签名层1证书。

可选的，在一些实施例中，芯片100还可以包括第二通信接口（图中未示出）。业务核120可以与第二通信接口通过内部连接通路互相通信。但是，业务核120与第一通信接口140无法互相通信。换句话说，芯片100可以包括两个与芯片外设备进行通信的通信接口。安全核模块110可以通过两个通信接口中的一个（例如第一通信接口）与芯片外设备进行通信，业务核120可以通过另一个通信接口（例如第二通信接口）与芯片外设备进行通信。安全核模块110与第二通信接口之间没有连接通路，业务核120与第一通信接口之间也没有连接通路。在此情况下，安全核模块110与业务核120之间没有共用的通信接口。这样，安全核模块110与业务核120之间可以实现进一步的隔离，可以进一步提升安全核模块110的安全性。

安全核111可以通过安全核通信接口115将CA签名层1证书发送至存储器。该存储器保存接收到的CA签名层1证书。该存储器是一个非易失性存储器，例如可以是存储器130，也可以是在生产芯片100过程中的，设置与芯片100外的，芯片100能够访问的一个存储器。

可选的，在一些实施例中，在安全核固件只有层1固件的情况下，安全核111还可以在生成该层1公钥和该层1私钥之后，删除第三存储器114中保存的CDI。在删除第三存储器114中保存的CDI后，层1固件的可信身份构建成功。在层1固件的可信身份构建成功的情况下，第三存储器114中保存有层1私钥。该层1私钥可以被应用于可信证明。

此外，在安全核固件只有层1固件的情况下，获取CA签名层1证书的过程（包括生成层1证书信息，向证书颁发设备发送该层1证书信息，接收该CA签名层1证书，将该CA签名层1证书写入存储器）是通过运行层1固件实现的。

可选的，在另一些实施例中，在安全核固件包括层2固件的情况下，层1固件还可以用于对层2固件进行校验、生成层2私钥、层2证书以及层2公钥。

在生成层2私钥、层2证书以及层2公钥前，安全核111还需要对层2固件进行校验，校验通过后才能够生成层2私钥、层2证书以及层2公钥。

安全核111可以用于执行层1固件代码，完成对层2固件的校验。用于对层2固件进行校验的第二校验信息可以包括第二根公钥哈希、第二吊销标识信息和第二安全版本号信息。层2固件校验相关信息包括第二根公钥、二级密钥公钥的签名结果、二级密钥公钥、层2固件与层2固件版本号的签名结果。层2固件校验相关信息还可以包括以下信息中的任一个或多个：二级密钥标识（ID）、层2固件版本号。层2固件的校验流程可以参考层1固件的校验流，在此就不必赘述。

需要说明的是，第二根公钥与第一根公钥可以相同。因此第一根公钥哈希与第二根公钥哈希可以相同。用于对层2固件与层2固件版本号的进行签名处理的二级密钥私钥与对层1固件与层1固件版本号进行签名处理的二级密钥私钥也可以相同。在此情况下，在对层2固件进行校验的过程中则无需执行层1固件校验过程中的步骤301至步骤303，直接从步骤304开始执行即可。

安全核 111 还在根据该层 2 固件校验通过的情况下，根据该 CDI 和层 2 固件的哈希，确定层 2 加密信息，将该层 2 加密信息保存在该第三存储器 114。

具体地，安全核 111 可以根据该 CDI 和层 2 固件的哈希，利用单向函数进行单向计算生成该层 2 加密信息。用于进行单向计算的单向函数可以是 HMAC、SHA-256、SHA-512、MD5 消息摘要算法（MD5 Message-Digest Algorithm）等。

例如，安全核 111 可以通过计算 HMAC（CDI，Hash（Layer2））生成该层 2 加密信息，其中 CDI 可以是第三存储器 114 中保存的 CDI 或者是第三存储器 114 保存的 CDI 和其他数据进行运算后得到的一个值，Hash（Layer2）表示对层 2 固件的哈希。HMAC（CDI，Hash(Layer2)）表示以 CDI 为密钥对层 2 固件的哈希进行 HMAC 签名，得到的签名就是该层 2 加密信息。

安全核 111 还基于该层 2 加密信息，使用非对称加密算法生成层 2 私钥和层 2 公钥，并将该层 2 私钥保存在第三存储器 114；颁发层 2 证书，使用层 1 私钥对该层 2 证书进行签名，该层 2 证书中包括该层 2 公钥以及层 2 固件标识，该层 2 固件标识可以是层 2 固件的哈希。层 2 固件的哈希可以是对层 2 固件进行哈希运算得到的。

第三存储器 114 中保存有层 1 私钥和层 2 私钥。层 2 公钥以及签名后的层 2 证书可以保存在安全核模块 110 外的存储器中，例如，存储器 130，还可以保存在芯片 100 外的存储器中，例如服务器的存储器。如上所述，安全核模块 110 以外的其他任何设备都无法访问安全核模块 110 内的各个组件或者只有业务核 120 在安全模式的情况下才可以访问安全核模块 110 内的各个组件，这样保存在第三存储器 114 内的层 1 私钥和层 2 私钥无法被泄漏。这样可以避免利用层 1 私钥伪造层 2 证书的风险，以及利用层 2 私钥进行虚假的可信证明的风险。层 2 公钥是用于进行可信证明验证的。因此，层 2 公钥并不需要进行保密。所以保存层 2 公钥的存储器可以是安全核模块 110 外的存储器，以便其他设备获取该层 2 公钥并利用该层 2 公钥进行验证。

用于生成该层 2 公钥和该层 2 私钥的非对称加密算法可以是 RSA 加密算法，例如 RSA-2048、RSA-3072、RSA-4096 等，也可以是 ECC 算法，例如 ECC256、ECC384、ECC512 等。

在一些实施例中，用于生成该层 1 证书的算法可以与用于生成层 2 证书算法相同。

在另一些实施例中，用于生成该层 1 证书的算法可以与用于生成层 2 证书算法不相同。

在一些实施例中，用于生成该层 2 公钥和该层 2 私钥的非对称加密算法可以与用于生成层 1 公钥和层 1 私钥的非对称加密算法相同。

在另一些实施例中，用于生成该层 2 公钥和该层 2 私钥的非对称加密算法也可以与用于生成层 1 公钥和层 1 私钥的非对称加密算法不相同。

可选的，在一些实施例中，安全核 111 还可以在确定该层 2 加密信息之后，删除第三存储器 114 保存的该 CDI；在使用层 1 私钥对层 2 证书进行签名后，删除第三存储器 114 中保存的层 1 私钥。这样，可以防止因层 1 私钥和 CDI 泄漏导致的攻击者可以根据层 1 私钥伪造层 2 证书的情况发生。

此外，在安全核固件还包括层 2 固件的情况下，层 1 固件可以用于实现生成层 1 证书信息并将该层 1 证书信息转递至层 2 固件。该层 2 固件用于实现向证书颁发设备发送该层 1 证书信息，接收该 CA 签名层 1 证书，将该 CA 签名层 1 证书写入存储器。

可选的，在一些实施例中，安全核模块 110 中还可以包括硬件加速引擎（图中未示出），该硬件加速引擎可以加速层 1 固件/层 2 固件校验过程，以及加速确定层 1 私钥、层 1 公钥、层 2 私钥、层 2 公钥和层 2 证书的过程。具体地，该硬件加速引擎可以包括以下至少一种硬件：用于实现层 1 固件校验过程的硬件、用于实现层 2 固件校验过程的硬件、用于实现密码学算法（例如 HMAC、SHA、RSA、或 ECC 等中的至少一个）的硬件。

在安全核固件仅包括层 1 固件且生成了层 1 私钥的情况下，安全核模块 110 内保存有层 1 私钥，存储器中保存有 CA 签名层 1 证书。安全核 111 可以通过运行层 1 固件对需要进行可信证明的数据提供可信证明。具体地，安全核 111 可以获取层 1 私钥，使用层 1 私钥对需要进行可信证明的数据进行签名，以提供可信证明。此外，安全核 111 还可以提供层 1 固件的可信证明（即提供 CA 签名层 1 证书）。

在安全核固件包括层 2 固件且生成了层 2 私钥和层 2 证书的情况下，安全核模块 110 内保存有层 2 私钥，存储器中保存有 CA 签名层 1 证书和使用层 1 私钥签名的层 2 证书。安全核 111 可以通过运行层 2 固件对需要进行可信证明的数据提供可信证明。安全核 111 可以提供层 1 固件的可信证明（即提供 CA 签名层 1 证书）。安全核 111 还可以提供层 2 固件的可信证明（即提供使用层 1 私钥签名的层 2 证书）。安全核 111 还可以利用层 2 私钥对需要进行可信证明的数据进行签名，以提供可信证明。

下面结合图 5 对安全核 111 对需要进行可信证明的数据提供可信证明的流程进行描述。为便于描述，以下将需要提供可信证明的数据称为目标数据。

该目标数据的类型可以包括：该服务器中硬件运行的固件（或代码）、该服务器中运行的固件（或代码）的哈希、该服务器运行过程中生成的数据和/或该服务器中保存的数据。

例如，该目标数据可以是安全核固件中的层 1 固件。该目标数据还可以是安全核固件中的层 2 固件。该目标数据还可以是非安全核固件或代码，例如芯片 100 的业务核运行的通用引导（Universal Boot Loader，U-Boot）代码、操作系统（Operating System，OS）内核（kernel）固件、运行在 OS 中的应用（Application，APP）代码。该目标数据还可以是安全核运行过程中产生的一些数据。该目标数据还可以是服务器中其他硬件运行过程中产生的一些数据，例如服务器的 CPU 产生的一些数据。该目标数据还可以是服务器的存储器中保存的一些数据。

需要说明的是，图 5 所示的实施例是以安全核固件包括层 2 固件为例进行描述的。图 5 所示的实施例是在完成层 2 固件的可信身份构建的基础上执行的。

图 5 是根据本申请实施例提供的一种可信证明流程的示意图。

501，安全核 111 获取挑战设备发送的验证请求信息，该验证请求信息用于获取目标数据的可信证明。

本申请实施例对该挑战设备的具体实现并不限定。只要该挑战设备能够获取到由安全核 111 发送的目标数据的可信证明即可。例如，该挑战设备可以是该服务器内的器件。例如，该挑战设备可以是该服务器内的中央处理器（Central Processing Unit，CPU）、基本输入输出系统（Basic Input Output System，BIOS）等。该挑战设备还可以是服务器外的能够与服务器通信的设备。例如，该挑战设备可以是一个能访问该服务器的终端设备。又如，该挑战设备可以是一个用于验证该服务器是否安全运行的设备。

虽然安全核模块 110 对于安全核模块 110 外的组件访问隔离，但是安全核模块 110 外的组件可以向安全核模块 110 发送一些信息。因此，在一些实施例，第一通信接口 140 接收到的该挑战设备发送的验证请求信息可以直接发送至安全核模块通信接口 115。安全核 111 获取安全核模块通信接口 111 接收到的该验证请求信息。

可选的，在一些实施例中，第一通信接口 140 可以将接收到的验证请求信息发送至业务核 120。业务核 120 可以将接收到的验证请求信息写入至存储器 130 的特定存储空间。该特定存储空间是业务核 120 和安全核 111 共享的存储空间。换句话说，业务核 120 与安全核 111 都可以访问该存储空间，读取该存储空间内保存的数据或者将数据写入到该存储空间。安全核 111 可以通过安全核模块通信接口 115 周期性地访问该特定存储空间。若安全核 111 确定该存储空间内存储有该验证请求信息，则通过安全核模块通信接口 115 获取该验证请求信息。

虽然安全核模块 110 对安全核模块 110 外的组件访问隔离，但是业务核 120 可以向安全核 111 发送一些指示信息。因此，在另一些实施例中，第一通信接口 140 可以将接收到的验证请求信息发送至业务核 120。业务核 120 可以将接收到的验证请求信息写入至存储器 130 的特定存储空间，然后向安全核 111 发送一个指示信息，该指示信息用于指示安全核 111 读取该特定存储空间。安全核 111 在接收到该指示信息后，通过安全核模块通信接口 115 读取该特定存储空间，获取该验证请求信息。

可选的，在一些实施例中，该验证请求信息可以请求提供芯片 100 中的安全核 111 以及业务核 120 运行的全部固件的可信证明。

可选的，在另一些实施例中，该验证请求消息可以请求获取特定固件的可信证明。

可选的，在一些实施例中，该验证请求消息可以请求获取特定数据的可信证明。例如，该特定数据可以是芯片 100 中的业务核生成的一些关键数据。又如，该特定数据可以是该服务器的存储器中存储的一些关键数据。又如，该特定数据可以是该服务器内的 CPU 生成的一些关键数据。

502，安全核 111 确定该目标数据的可信证明。

可选的，在一些实施例中，在该目标数据包括安全核固件的层 1 固件的情况下，该安全核固件的层 1 固件的可信证明为 CA 签名层 1 证书。

可选的，在一些实施例中，在该目标数据包括安全核固件的层 2 固件的情况下，该安全核固件的层 2 固件的可信证明为使用层 1 私钥签名的层 2 证书。

可选的，在一些实施例中，在该目标数据为除安全核固件的层 1 固件与安全核固件的层 2 固件以外的固件（例如业务核固件）的情况下，该目标数据的可信证明为使用层 2 私钥进行签名的固件或固件的证书或固件的哈希。

可选的，在一些实施例中，在该目标数据为特定数据的情况下，该目标数据的可信证明为使用层 2 私钥进行签名的特定数据或该特定数据的哈希。

503，安全核 111 向该挑战设备发送验证反馈信息，该验证反馈信息包括该目标数据的可信证明。

可选的，在一些实施例中，安全核模块 110 可以与第一通信接口 140 通过内部连接通路互相通信。在此情况下，该验证反馈信息可以直接通过芯片 100 的第一通信接口 140 发送至该挑战设备。

此外，如上所述，安全核 111 能够访问安全核模块 110 外的各个组件。因此，在另一些实施例中，该验证反馈信息可以通过业务核 120 发送至该挑战设备。具体地，安全核 111 可以通过安全核模块通信接口 115 将该验证反馈信息发送至业务核 120。业务核 120 可以通过第一通信接口 140 将该验证反馈信息发送至该挑战设备。

504，该挑战设备可以根据保存的验证数据来验证该目标数据的可信证明是否是可信。

若该目标数据为安全核固件的层 1 固件，则该验证数据可以包括 CA 公钥和该层 1 固件（或者层 1 固件的哈希）。若该目标数据为安全核固件的层 2 固件，则该验证数据可以包括层 1 公钥和该层 2 固件（或者层 2 固件的哈希）。若该目标数据是特定数据，则该验证数据可以包括层 2 公钥和该特定数据（或者该特定数据的哈希）。若该目标数据是除安全核固件的层 1 固件与安全核固件的层 2 固件以外的固件，则该验证数据可以包括层 2 公钥和该固件（或者该固件的哈希）。

该验证数据可以是该挑战设备预先获取并保存在该挑战设备中的。例如，该挑战设备可以获取并保存固件的哈希。下面假设该目标数据是芯片 100 的层 3 固件（即业务核的 U-Boot 代码，以下简称层 3 固件），对该挑战设备根据保存的验证信息对可信证明进行验证的过程进行介绍。

安全核 111 使用层 2 私钥对业务核当前运行的层 3 固件的哈希进行签名，得到层 3 固件的哈希的签名结果，并将该层 3 固件的哈希的签名结果作为可信证明发送至该挑战设备。该挑战设备中预先保存有层 2 公钥和层 3 固件的哈希。该挑战设备使用层 2 公钥对接收到的可信证明（即使用层 2 公钥对该层 3 固件的哈希结果的签名得到层 3 固件的哈希的签名结果）进行解密，得到一个哈希。该挑战设备比较该哈希（即使用层 2 公钥对接收到的可信证明进行解密得到的哈希）与该挑战设备中保存的层 3 固件的哈希是否一致，若一致，则该挑战设备可以确定芯片 100 的业务核所运行的层 3 固件是可信的（即未经过篡改的）。可选的，在一些实施例中，该挑战设备还可以保存多个层 3 固件的哈希，不同的层 3 固件的哈希可以对应于不同版本的层 3 固件的哈希。该挑战设备可以确定该哈希（即使用层 2 公钥对接收到的可信证明进行解密得到的哈希）是否是该挑战设备保存的一个层 3 固件的哈希；若是，则该挑战设备可以根据层 3 固件的哈希与层 3 固件的版本的对应关系，确定出该业务核运行的层 3 固件的版本，并且可以确定出业务核所运行的层 3 固件是可信的（即未经过篡改的）；若否（即该挑战设备中并未保存有该哈希），则该挑战设备确定芯片 100 的业务核所运行的层 3 固件是不可信的。

又如，该可信证明是使用层 2 私钥签名后的特定数据。该挑战设备可以使用层 2 公钥对该可信证明进行解密，得到一个特定数据。若该特定数据（即使用层 2 公钥解密得到的特定数据）与该挑战设备接收到的由服务器发送的特定数据，则可以确定该特定数据是由该服务器发送的，并且该特定数据在从该服务器发送至该挑战设备的过程中没有被篡改。

又如，该可信证明是 CA 签名层 1 证书。该挑战设备可以使用 CA 公钥对该 CA 签名层 1 证书进行解密，得到层 1 证书信息。如图 2 所示的安全核 111 生成层 1 私钥和层 1 公钥的流程在芯片 100 每次启动时都会执行。如果层 1 固件没有发生变化，安全核 111 每次执行图 2 所示的方法所生成的层 1 私钥和层 1 公钥都是相同的。该挑战设备确定该层 1 证书信息中的层 1 公钥与安全核 111 在启动时生成的层 1 公钥是否相同，若不同，则表明层 1 固件被篡改；若相同，则表明层 1 固件与芯片 100 生成阶段使用的层 1 固件相同。

如上所述，该挑战设备可以是该服务器内的器件。该服务器内的挑战设备可以通过可信证明流程确定该挑战设备周围的运行环境是否是安全的。例如，该目标数据可以是芯片100中的业务核运行的固件（例如OS代码、APP代码）的哈希。通过可信证明流程，可以确定业务核运行的固件代码是否被篡改或者可以确定业务核运行的固件的版本。

如上所述，该挑战设备可以是一个用于验证该服务器是否安全运行的设备。该挑战设备可以通过可信证明流程，确定该服务器所运行的固件是可信的固件。

如上所述，该挑战设备可以是一个能访问该服务器的终端设备。通过该可信流程，挑战设备可以保证从服务器接收到的数据是未经过篡改的。

下面，以服务器为例对可信证明流程进行描述的。本领域技术人员可以理解，任何设置有芯片100的计算机设备都可以实现如图6所示的可信证明流程。

图6是根据本申请实施例提供的另一种可信证明流程的示意图。

601，挑战设备向服务器发送验证请求信息，该验证请求信息用于获取目标数据的可信证明。

如上所述，该服务器是设置有如图1所示芯片100的服务器。该服务器内的芯片100已将完成层2固件的可信身份构建流程。芯片100内的安全核模块内保存有层2私钥。该服务器的存储器存储CA签名层1证书和使用层1私钥签名的层2证书。

具体地，该服务器中的芯片 100 内的安全核模块中的安全核可以获取该验证请求信息。该安全核获取该验证请求信息的具体实现方式可以参加图5所示的实施例，在此就不必赘述。

可选的，在一些实施例中，该验证请求信息可以请求提供芯片100中的安全核以及业务核运行的全部固件的可信证明。

可选的，在另一些实施例中，该验证请求消息可以请求获取特定固件的可信证明。

可选的，在一些实施例中，该验证请求消息可以请求获取特定数据的可信证明。例如，该特定数据可以是芯片100中的业务核生成的一些关键数据。又如，该特定数据可以是该服务器的存储器中存储的一些关键数据。又如，该特定数据可以是该服务器内的CPU生成的一些关键数据。

602，该服务器确定该目标数据的可信证明。具体地，该服务器中的芯片 100 中的安全核可以负责确定该目标数据的可信证明。

可选的，在一些实施例中，在该目标数据包括安全核固件的层1固件的情况下，该安全核固件的层1固件的可信证明为CA签名层1证书。

可选的，在一些实施例中，在该目标数据包括安全核固件的层2固件的情况下，该安全核固件的层2固件的可信证明为使用层1私钥签名的层2证书。

可选的，在一些实施例中，在该目标数据为除安全核固件的层1固件与安全核固件的层2固件以外的固件的情况下，该目标数据的可信证明为使用层2私钥进行签名的固件或固件的证书。

可选的，在一些实施例中，在该目标数据为特定数据的情况下，该目标数据的可信证明为使用层2私钥进行签名的特定数据或该特定数据的哈希。

603，该服务器向该挑战设备发送验证反馈信息，该验证反馈信息包括该目标数据的可信证明。

604，该挑战设备可以根据保存的验证数据来验证该目标数据的可信证明是否是可信。

该挑战设备验证该可信证明的具体实现方式可以参见图 5 所示的实施例，在此就不必赘述。

图 7 是根据本申请实施例提供的一种芯片的结构框图。如图 7 所示，芯片 700 包括安全核模块 710，安全核模块 710 包括安全核 711 和存储器 712。

存储器 712 用于保存第一根公钥哈希和所述芯片的 UDS。安全核 711 用于根据该第一根公钥哈希和该芯片的 UDS，生成层 1 公钥和层 1 私钥。存储器 712 用于保存该层 1 私钥。安全核 711 生成层 1 公钥和层 1 私钥的具体实现方式可以参见图 2 所示的流程图。存储器 712 具体的实现方式可以参见图 1 所示的芯片中的第一存储器、第二存储器和第三存储器的描述，在此就不必赘述。

可选的，在一些实施例中，存储器 712 还用于保存第二根公钥哈希。安全核 711 还用于根据该第二根公钥哈希和该 UDS，生成层 2 公钥和层 2 私钥。存储器 712 还用于保存该层 2 私钥。存储器 712，还用于使用该层 1 私钥对层 2 证书进行签名，其中该层 2 证书中包括该层 2 公钥。具体地，根据该第二根公钥哈希和该 UDS，生成层 2 公钥和层 2 私钥可以是根据第二根公钥和由该 UDS 生成的 CDI，生成层 2 公钥和层 2 私钥。该第二根公钥和第一根公钥可以相同也可以不同。

可选的，在一些实施例中，安全核 711，还用于在使用该层 1 私钥对层 2 证书进行签名后，将该层 1 私钥删除。

可选的，在一些实施例中，安全核 711 还用于在接收到挑战设备发送的针对目标数据的验证请求信息时，运行安全固件，以根据该层 2 私钥对该目标数据进行签名，并将签名后的目标数据发送给该挑战设备，以便于该挑战设备根据该层 2 公钥对该签名后的目标数据进行验证。这里的安全固件是指用于实现可信证明流程的固件。由于该可信证明流程是使用层 2 私钥对该目标数据进行签名，因此该安全固件为层 2 固件。

可选的，在一些实施例中，该安全核还用于在接收到挑战设备发送的针对目标数据的验证请求信息时，运行安全固件，以根据该层 1 私钥对该目标数据进行签名，并将签名后的目标数据发送给该挑战设备，以便于该挑战设备根据该层 1 公钥对该签名后的目标数据进行验证。这里的安全固件是指用于实现可信证明流程的固件。由于该可信证明流程是使用层 1 私钥对该目标数据进行签名，因此该安全固件可以是层 1 固件。当然，若安全核 711 在使用该层 1 私钥对层 2 证书进行签名后，并未将该层 1 私钥删除，则该可信证明流程也可以是由层 2 固件实现。

可选的，在一些实施例中，该芯片还包括业务核（图中未示出），用于运行业务固件。

可选的，在一些实施例中，该芯片还包括第一输入输出接口和第二输入输出接口（图中未示出），该第一输入输出接口耦合至该安全核模块，该第二输入输出接口耦合至该业务核。

图 7 所示实施例中的各个组件的具体功能和有益效果可以参见图 1 至图 5 所示的实施例，在此就不必赘述。

上述实施例均是以服务器作为设置有该芯片的目标设备为例进行描述的。可以理解的是图 1 或图 7 所示的芯片可以应用于各种计算机设备，例如，服务器（例如，存储服务器、数据库服务器、管理服务器等）、终端设备（例如移动终端、个人计算机等）、可穿戴设

备、网络设备（例如路由器、交换机等）等。

图 8 示出了本申请提供的一种服务器的结构示意图。

如图 8 所示，服务器 800 包括处理器 810 和基板管理控制器（baseboard management controller，BMC）820，其中，BMC 820 可以是安全芯片，该安全芯片可以是如图 1 所示的芯片 100 或如图 7 所示的芯片 700，处理器 810 例如是 CPU。

当服务器 800 开机后，BMC 820 可以执行图 2 所示的流程，完成层 1 固件的可信身份构建或者进一步完成层 2 固件的可信身份固件。

BMC 820 还可以与其它组件连接，例如，与第四代双倍速率（double data rata，DDR）存储器（简称为“DDR4”）、寄存器、BMC 闪存、视频接口和物理层芯片（例如，网卡）连接。

DDR4 用于为 BMC 820 或处理器 810 提供运行程序或者代码的空间。

BMC 闪存可以是存储 BMC 自身固件和相关数据的闪存。

视频接口用于连接显示器等外部设备。物理层芯片连接网卡，用于为服务器 800 提供数据收发服务。

BMC 820 和处理器 810 都可以通过开关访问 BIOS，运行 BIOS 闪存中存储的 BIOS，并通过切换开关的方式与 BMC 820 通信。

上述服务器 800 的架构仅是举例说明，而不应被理解为对本申请提供的技术方案的应用限定，本申请提供的技术方案还可以应用于包含更多或者更少的组件的服务器中。

例如，服务器 800 可以是云计算服务器，此时，服务器 800 可以包括多个计算单元，计算单元可以是 CPU、也可以是图形处理器（graphics processing unit，GPU），还可以是数字信号处理器（digital signal processor，DSP）、专用集成电路（application specific integrated circuit，ASIC）、现成可编程门阵列（field programmable gate array，FPGA）、神经网络处理器（neural-network process unit，NPU）或者其它类型的计算单元。该多个计算单元可以组成同构计算（homogenous computing）资源池和/或异构计算（heterogeneous computing）资源池为用户提供服务。

又例如，服务器 800 可以是存储服务器，此时，服务器 800 可以包括多个存储单元，存储单元可以是硬盘驱动器（hard disk drive，HDD）硬盘，也可以是固态硬盘（solid state disk，SSD），还可以是小型计算机系统接口（small computer system interface，SCSI）硬盘或者其它类型的非易失性存储介质。当服务器 800 包括多个硬盘时，该多个硬盘可以组成磁盘阵列（redundant arrays of independent drives，RAID），作为服务器 800 的存储资源池为用户提供服务。

图 9 示出了本申请提供的一种终端设备的结构示意图。

终端设备可被称为接入终端、用户设备（user equipment，UE）、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。接入终端可以是蜂窝电话、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备以及 5G 通信系统中的用户设备。上述各个电子设备仅是对终端设备的举例说明，终端设备还可以是其它电子设备，例如包含 SoC 芯片 901 的汽车或无人机。SoC 芯片 901 可以是如图 1 所示的芯片 100 或如图 7 所示的芯片 700。

如图 9 所示，当终端设备为手机时，手机 900 包括安全芯片 901、闪存 902、控制电路、天线以及输入输出装置。SoC 芯片 901 主要用于对通信协议以及通信数据进行处理，以及对整个终端设备进行控制，执行软件程序，处理软件程序的数据。闪存 902 主要用于存储软件程序和数据。SoC 芯片 901 和闪存 902 用于在手机 900 启动时为手机 900 提供安全启动保障。控制电路主要用于基带信号与射频信号的转换以及对射频信号的处理。控制电路和天线一起也可以叫做收发器，主要用于收发电磁波形式的射频信号。输入输出装置，例如触摸屏、显示屏或键盘，主要用于接收用户输入的数据以及对用户输出数据。

当终端设备开机后，SoC 芯片 901 可以执行图 2 所示的流程，完成层 1 固件的可信身份构建或者进一步完成层 2 固件的可信身份固件。SoC 芯片 901，随后运行 OS，随后读取闪存 902 中的软件程序，解释并执行软件程序的指令，处理软件程序的数据。SoC 芯片 901 可以包括基带芯片，当需要通过无线发送数据时，SoC 芯片 901 的基带芯片对待发送的数据进行基带处理后，输出基带信号至射频电路，射频电路将基带信号进行射频处理后将射频信号通过天线以电磁波的形式向外发送。当有数据发送到终端设备时，射频电路通过天线接收到射频信号，将射频信号转换为基带信号，并将基带信号输出至处理器，处理器将基带信号转换为数据并对该数据进行处理。

本领域技术人员可以理解，为了便于说明，图 9 仅示出了一个存储器（闪存 902）和一个处理器（SoC 芯片 901）。在实际的终端设备中，可以存在多个处理器和多个存储器。存储器也可以称为存储介质或者存储设备等，本申请对此不做限定。

图 10 示出了本申请提供的一种网络设备的结构示意图。

网络设备可以是码分多址（code division multiple access，CDMA）系统中的基站（base transceiver station，BTS），也可以是宽带码分多址（wideband code division multiple access，WCDMA）系统中的基站（node B，NB），还可以是长期演进（long term evolution，LTE）系统中的演进型基站（evolutional node B，eNB），还可以是 5G 通信系统中的基站（gNB），上述基站仅是举例说明，网络设备还可以为中继站、接入点、车载设备、可穿戴设备以及包含安全芯片 1003 的汽车或无人机。

如图 10 所示，当网络设备为基站时，基站 1000 可包括一个或多个射频单元，如远端射频单元（remote radio unit, RRU）1001 和一个或多个基带单元（baseband unit，BBU）（也可称为数字单元（digital unit，DU））1002。所述 RRU 1001 可以称为收发单元、收发机、收发电路、或者收发器等等，其可以包括至少一个天线 1011 和射频单元 1012。RRU 1001 主要用于射频信号的收发以及射频信号与基带信号的转换。BBU 1002 主要用于进行基带处理，对基站 1000 进行控制等。BBU 1002 中的单板上集成有 SoC 芯片 1003 和闪存 1004，SoC 芯片 1003 可以是如图 1 所示的芯片 100 或如图 7 所示的芯片 700。

当基站 1000 开机后，SoC 芯片 1001 可以执行图 2 所示的流程，完成层 1 固件的可信身份构建或者进一步完成层 2 固件的可信身份固件。

SoC 芯片 1003 和闪存 1004 用于在 BBU 1002 启动时为 BBU 1002 提供安全启动保障。RRU 1001 与 BBU 1002 可以是物理上设置在一起的，也可以物理上分离设置的，即分布式基站。

BBU 1002 为基站的控制中心，也可以称为处理单元，主要用于完成基带处理功能，如信道编码，复用，调制，扩频等等。

在一个示例中，BBU 1002 可以由一个或多个单板构成，多个单板可以共同支持单一接入指示的无线接入网（如 LTE 网），也可以分别支持不同接入制式的无线接入网（如 LTE 网，5G 网或其它网）。SoC 芯片 1003 和闪存 1004 可以服务于一个或多个单板。也就是说，可以每个单板上单独设置存储器和处理器。也可以是多个单板共用相同的存储器和处理器。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1、一种芯片，其特征在于，所述芯片包括安全核模块，所述安全核模块包括：安全核和存储器，其中，所述安全核模块对于所述芯片的除所述安全核模块外的外部模块访问隔离，且所述安全核模块对于所述芯片以外的外部设备访问隔离；

所述存储器，用于保存第一根公钥哈希和所述芯片的唯一设备秘密 UDS；

所述安全核，用于根据所述第一根公钥哈希和所述 UDS 生成层 1 公钥和层 1 私钥；

所述存储器，用于保存所述层 1 私钥。

2、如权利要求 1 所述的芯片，其特征在于，所述安全核模块的地址在所述外部模块和所述外部设备能够访问的地址范围之外。

3、如权利要求 1 或 2 所述的芯片，其特征在于，所述存储器还用于保存第二根公钥哈希；

所述安全核还用于根据所述第二根公钥哈希和所述 UDS，生成层 2 公钥和层 2 私钥；

所述存储器还用于保存所述层 2 私钥；

所述安全核，还用于使用所述层 1 私钥对层 2 证书进行签名，其中所述层 2 证书中包括所述层 2 公钥。

4、如权利要求 3 所述的芯片，其特征在于，所述安全核，还用于在使用所述层 1 私钥对层 2 证书进行签名后，将所述层 1 私钥删除。

5、如权利要求 3 或 4 中所述的芯片，其特征在于，所述安全核还用于在接收到挑战设备发送的针对目标数据的验证请求信息时，运行安全固件，以根据所述层 2 私钥对所述目标数据进行签名，并将签名后的目标数据发送给所述挑战设备，以便于所述挑战设备根据所述层 2 公钥对所述签名后的目标数据进行验证。

6、如权利要求 1 至 3 中任一项所述的芯片，其特征在于，所述安全核还用于在接收到挑战设备发送的针对目标数据的验证请求信息时，运行安全固件，以根据所述层 1 私钥对所述目标数据进行签名，并将签名后的目标数据发送给所述挑战设备，以便于所述挑战设备根据所述层 1 公钥对所述签名后的目标数据进行验证。

7、如权利要求 1 至 6 中任一项所述的芯片，其特征在于，所述芯片还包括业务核，用于运行业务核固件。

8、如权利要求 7 所述的芯片，其特征在于，所述芯片还包括第一输入输出接口和第二输入输出接口，所述第一输入输出接口耦合至所述安全核模块，所述第二输入输出接口耦合至所述业务核。

9、一种生成私钥的方法，其特征在于，由芯片中的安全核执行，所述安全核位于所述芯片的安全核模块中，所述安全核模块还包括用于存储第一根公钥哈希和所述芯片的唯一设备秘密 UDS 的存储器，所述安全核模块对于所述芯片的除所述安全核模块外的外部模块访问隔离，且所述安全核模块对于所述芯片以外的外部设备访问隔离，所述方法包括：

所述安全核从存储器中获取所述第一根公钥哈希和所述 UDS；

所述安全核根据所述第一根公钥哈希和所述 UDS 生成层 1 公钥和层 1 私钥；

所述安全核将所述层 1 私钥写入到所述存储器中。

10、如权利要求 9 所述的方法，其特征在于，所述存储器还用于存储第二根公钥哈希，所述方法还包括:

所述安全核从所述存储器中获取所述第二根公钥哈希;

所述安全核根据所述第二根公钥哈希和所述 UDS，生成层 2 公钥和层 2 私钥;

所述安全核将所述层 2 私钥写入到所述存储器中;

所述安全核使用所述层 1 私钥对层 2 证书进行签名，其中所述层 2 证书中包括所述层 2 公钥。

11、如权利要求 10 所述的方法，其特征在于，所述方法还包括:

所述安全核在使用所述层 1 私钥对层 2 证书进行签名后，将所述层 1 私钥删除。

12、如权利要求 10 或 11 所述的方法，其特征在于，所述方法还包括:

所述安全核获取挑战设备发送的针对目标数据的验证请求信息;

所述安全核根据所述层 2 私钥对所述目标数据进行签名;

所述安全核将签名后的目标数据发送给所述挑战设备，以便于所述挑战设备根据所述层 2 公钥对所述签名后的目标数据进行验证。

13、如权利要求 9 或 10 所述的方法，其特征在于，所述方法还包括:

所述安全核获取挑战设备发送的针对目标数据的验证请求信息;

所述安全核根据所述层 1 私钥对所述目标数据进行签名;

所述安全核将签名后的目标数据发送给所述挑战设备，以便于所述挑战设备根据所述层 1 公钥对所述签名后的目标数据进行验证。

14、一种可信证明的方法，其特征在于，所述方法包括:

芯片的安全核模块内的安全核获取挑战设备发送的针对目标数据的验证请求信息，其中，所述安全核模块对于所述芯片的除所述安全核模块外的外部模块访问隔离，且所述安全核模块对于所述芯片以外的外部设备访问隔离;

所述安全核根据所述安全核模块的存储器中保存的私钥对所述目标数据进行签名;

所述安全核向所述挑战设备发送签名后的目标数据。

15、如权利要求 14 所述的方法，其特征在于，所述芯片的安全核模块内的安全核获取挑战设备发送的验证请求信息，包括:

所述安全核读取保存在所述芯片的存储器中特定存储空间的所述验证请求信息。

16、如权利要求 15 所述的方法，其特征在于，在所述安全核读取保存在所述芯片的存储器中的所述验证请求信息之前，所述方法还包括:

所述安全核接收所述芯片的业务核发送的指示信息，所述指示信息用于指示所述安全核读取所述芯片的存储器的特定存储空间。

17、如权利要求 14 至 16 中任一项所述的方法，其特征在于，所述目标数据的类型包括: 目标设备中的硬件运行的固件、所述目标设备中的硬件运行的固件的哈希、所述目标设备运行过程中生成的数据、所述目标设备保存的数据，其中所述目标设备为设置有所述芯片的设备。

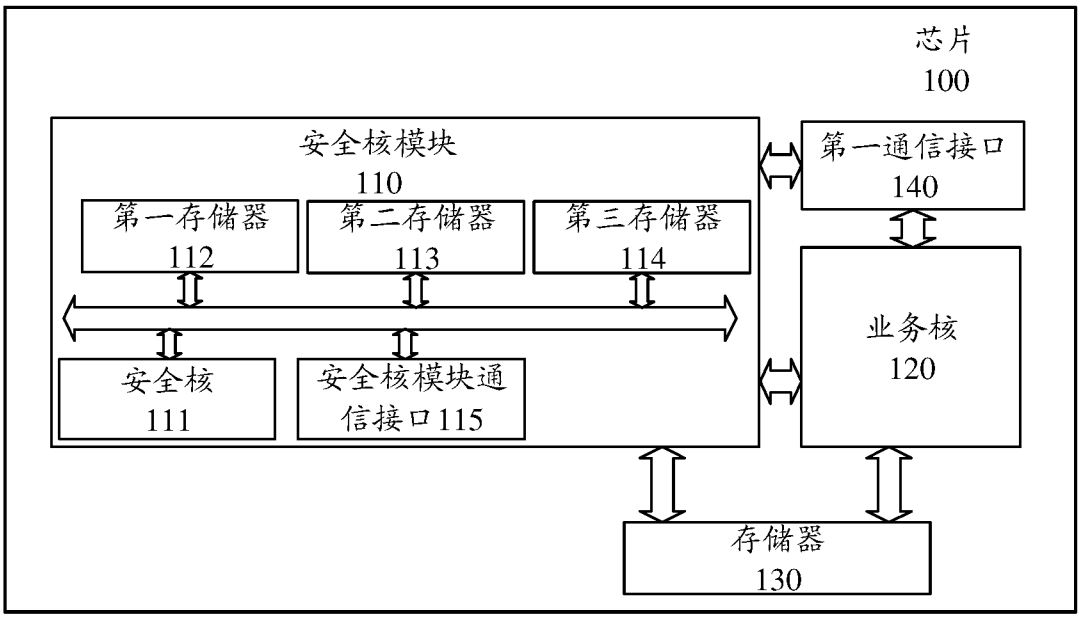
芯片
100
安全核模块
110
第一存储器
112
第二存储器
113
第三存储器
114
安全核
111
安全核模块通信接口115
第一通信接口
140
业务核
120
存储器
130

图1

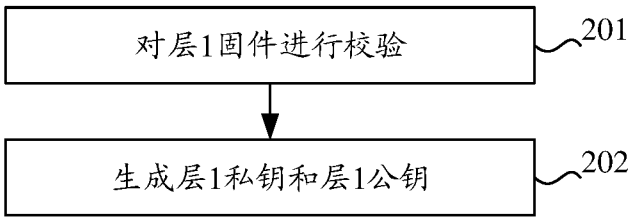
对层1固件进行校验
201
生成层1私钥和层1公钥
202

图2

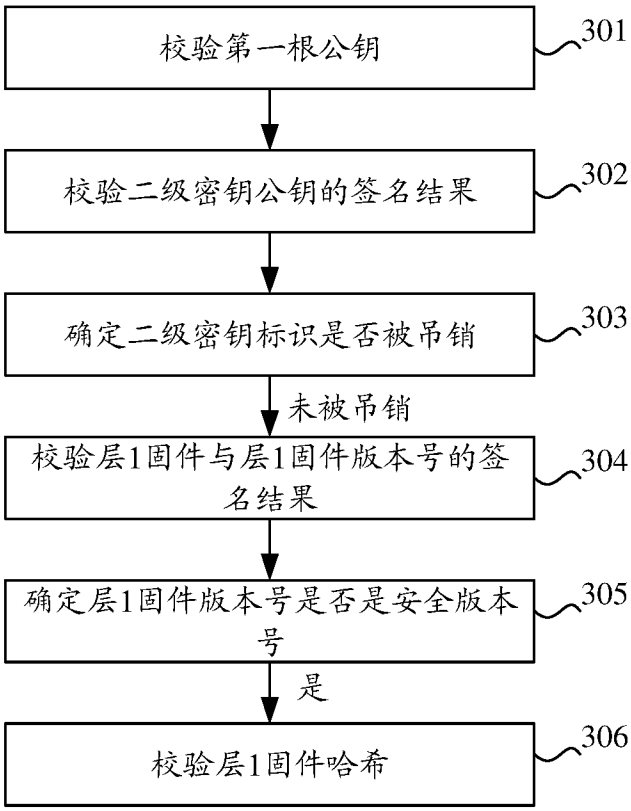
校验第一根公钥
301
校验二级密钥公钥的签名结果
302
确定二级密钥标识是否被吊销
303
未被吊销
校验层1固件与层1固件版本号的签名结果
304
确定层1固件版本号是否是安全版本号
305
是
校验层1固件哈希
306

图3

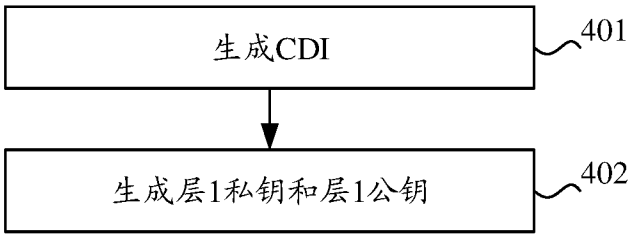
生成CDI
401
生成层1私钥和层1公钥
402

图4

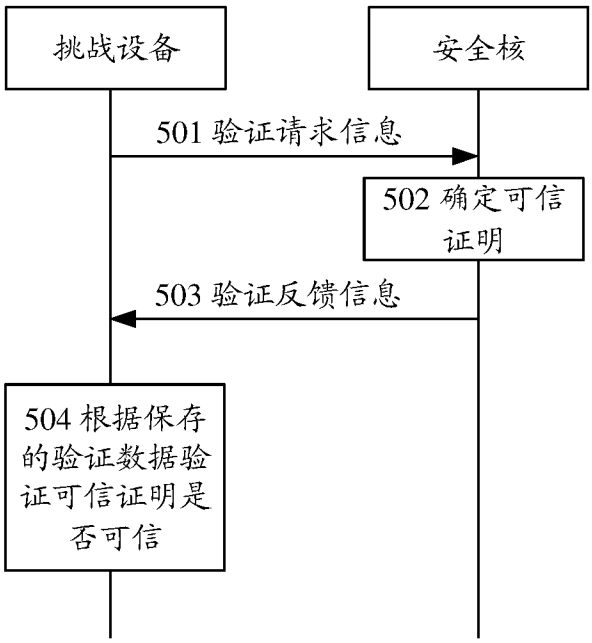
挑战设备
安全核
501 验证请求信息
502 确定可信证明
503 验证反馈信息
504 根据保存的验证数据验证可信证明是否可信

图5

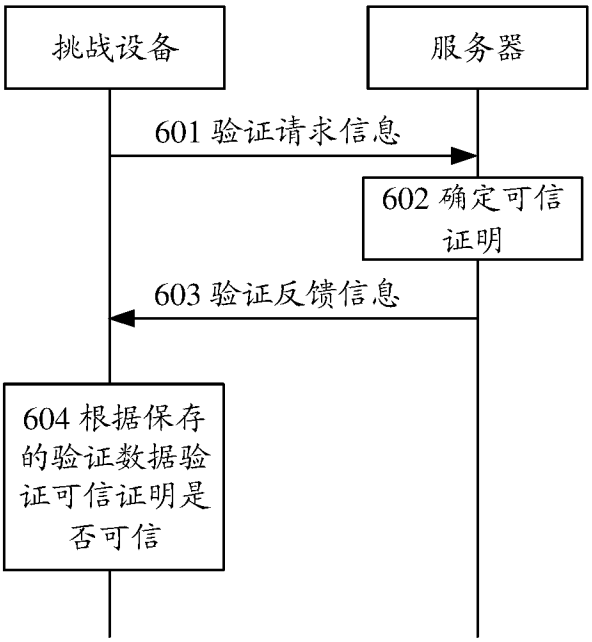
挑战设备
服务器
601 验证请求信息
602 确定可信证明
603 验证反馈信息
604 根据保存的验证数据验证可信证明是否可信

图6

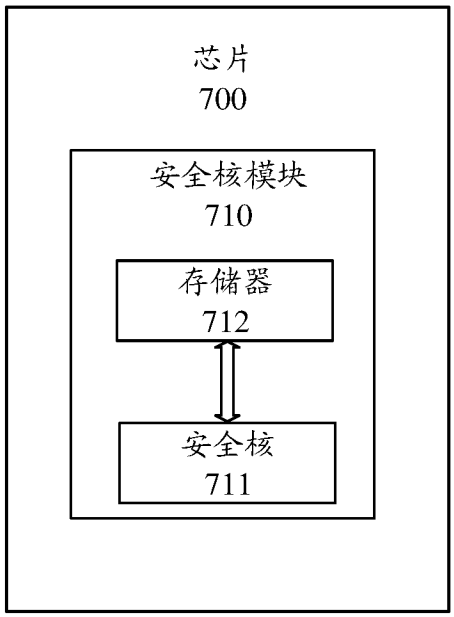

图7

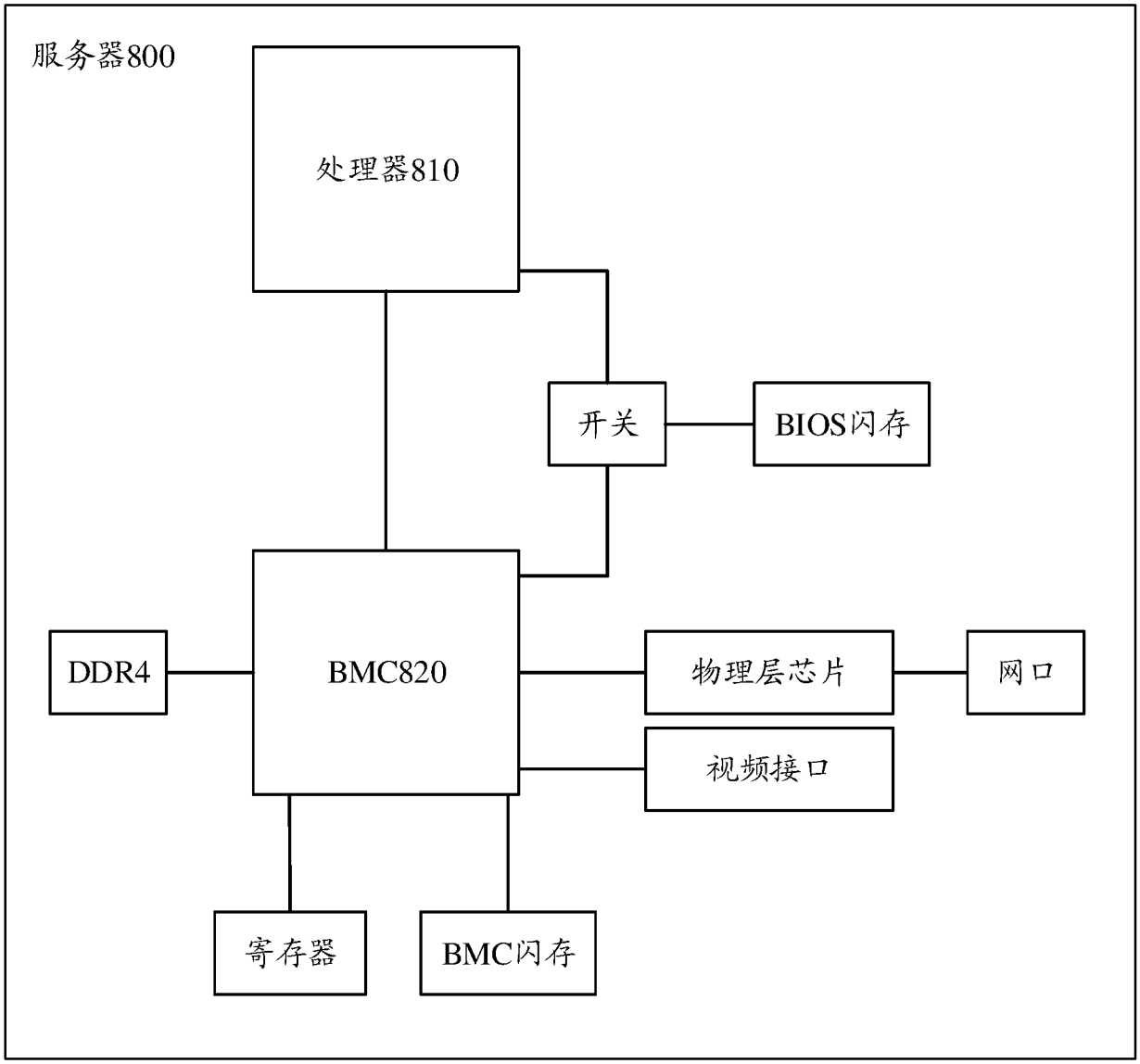

图8

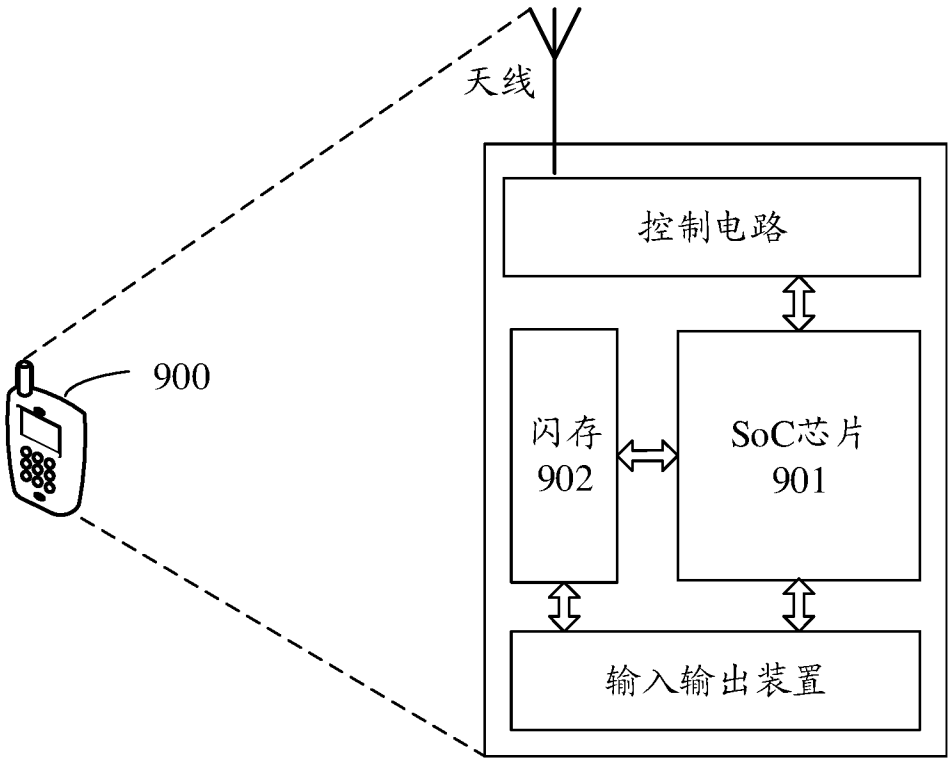

图9

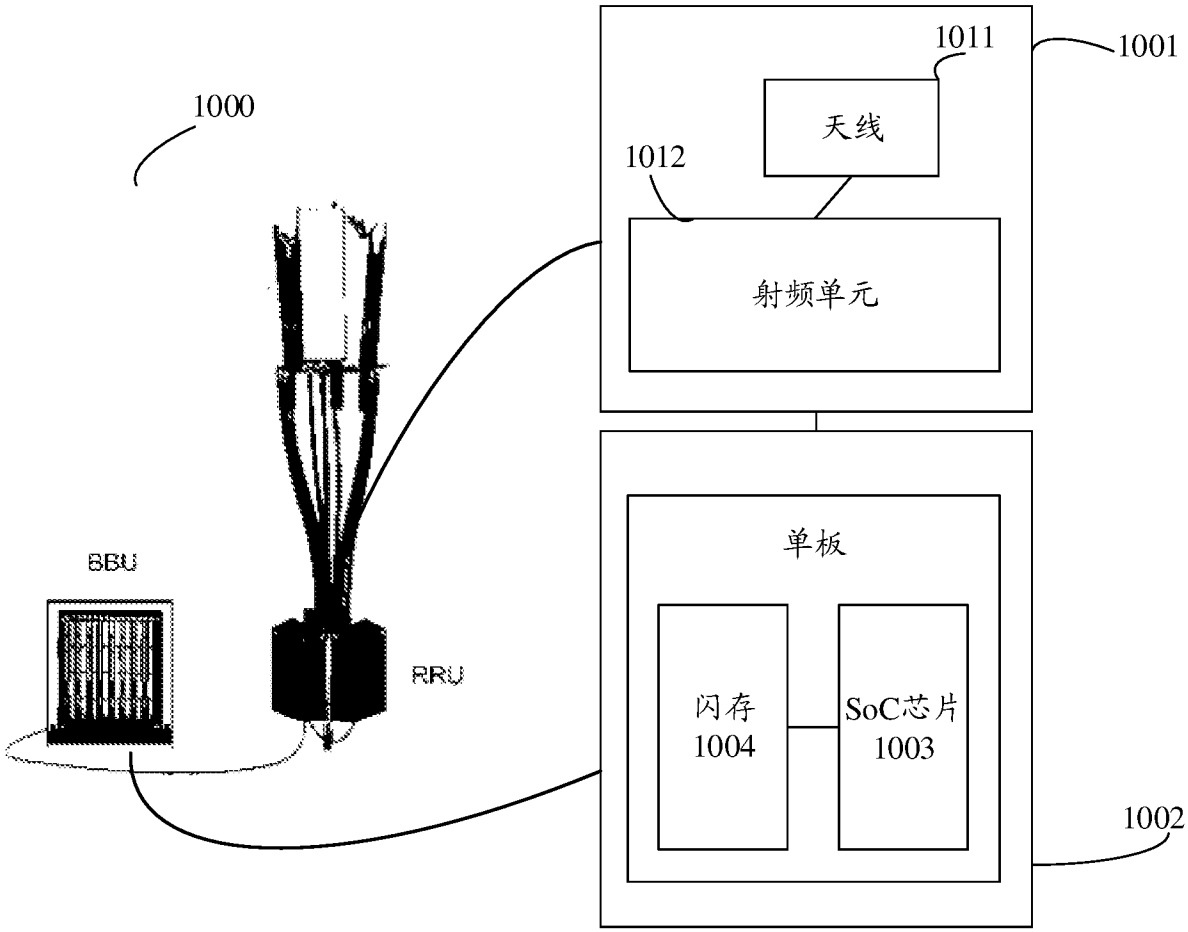

图10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/109537

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00(2006.01)i; G06F 21/00(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI, GOOGLE: 芯片, 安全, 存储器, 隔离, 公钥, 私钥, 密钥, UDS, chip, security, memory, insulate, public key, private key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 1553349 A (LENOVO (BEIJING) CO., LTD.) 08 December 2004 (2004-12-08) description, pages 15-21, and claims 1-25	1-17
A	CN 101430747 A (WUHAN UNIVERSITY) 13 May 2009 (2009-05-13) entire document	1-17
A	CN 108429719 A (HUAWEI TECHNOLOGIES CO., LTD.) 21 August 2018 (2018-08-21) entire document	1-17
A	US 2014010371 A1 (KHAZAN, R.I. ET AL.) 09 January 2014 (2014-01-09) entire document	1-17

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 April 2019	**03 June 2019**
Name and mailing address of the ISA/CN **State Intellectual Property Office of the P. R. China** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/109537

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 1553349 A	08 December 2004	CN 100447763 C	31 December 2008
CN 101430747 A	13 May 2009	CN 101430747 B	07 September 2011
CN 108429719 A	21 August 2018	WO 2018149110 A1	23 August 2018
US 2014010371 A1	09 January 2014	US 2014013123 A1	09 January 2014
		US 2015381659 A1	31 December 2015
		US 2015381592 A1	31 December 2015
		US 9705854 B2	11 July 2017
		WO 2014055148 A2	10 April 2014
		WO 2014055148 A3	02 October 2014

国际检索报告

国际申请号
PCT/CN2018/109537

A. 主题的分类

H04L 9/00(2006.01)i; G06F 21/00(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI, EPODOC, CNPAT, CNKI, GOOGLE: 芯片，安全，存储器，隔离，公钥，私钥，密钥，UDS, chip, security, memory, insulate, public key, private key

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 1553349 A (联想北京有限公司) 2004年 12月 8日 (2004-12-08) 说明书第15-21页，权利要求1-25	1-17
A	CN 101430747 A (武汉大学) 2009年 5月 13日 (2009-05-13) 全文	1-17
A	CN 108429719 A (华为技术有限公司) 2018年 8月 21日 (2018-08-21) 全文	1-17
A	US 2014010371 A1 (KHAZAN, ROGER I. 等) 2014年 1月 9日 (2014-01-09) 全文	1-17

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 4月 9日	2019年 6月 3日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 苏菲 电话号码 86-(10)-53961392

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/109537

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	1553349	A	2004年 12月 8日	CN	100447763	C	2008年 12月 31日
CN	101430747	A	2009年 5月 13日	CN	101430747	B	2011年 9月 7日
CN	108429719	A	2018年 8月 21日	WO	2018149110	A1	2018年 8月 23日
US	2014010371	A1	2014年 1月 9日	US	2014013123	A1	2014年 1月 9日
				US	2015381659	A1	2015年 12月 31日
				US	2015381592	A1	2015年 12月 31日
				US	9705854	B2	2017年 7月 11日
				WO	2014055148	A2	2014年 4月 10日
				WO	2014055148	A3	2014年 10月 2日