

(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
2018 年 5 月 17 日 (17.05.2018)



(10) 国际公布号
WO 2018/086469 A1

- (51) 国际专利分类号:
G06F 21/79 (2013.01) **H04L 9/08** (2006.01)
- (21) 国际申请号: PCT/CN2017/108254
- (22) 国际申请日: 2017 年 10 月 30 日 (30.10.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610998449.0 2016 年 11 月 11 日 (11.11.2016) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 付颖芳 (FU, Yingfang); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, 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))。

(54) **Title:** DATA STORAGE METHOD UTILIZED IN NON-VOLATILE STORAGE SPACE IN INTEGRATED CIRCUIT, AND TRUSTED INTEGRATED CIRCUIT

(54) 发明名称: 芯片中非易失性存储空间的数据存储方法和可信芯片



(57) **Abstract:** A data storage method utilized in a non-volatile storage space in an integrated circuit (IC), and a trusted integrated circuit. The data storage method comprises: creating, in the integrated circuit, the non-volatile storage space (S302); wherein the non-volatile storage space has attributes including a parameter representing storage of owner data in the non-volatile storage space, and a storage address range of the owner data; and the storage address range of the owner data represents a maximum data length allowable for requesting data from the integrated circuit. The method resolves a technical issue in the prior art in which when reading, from a non-volatile space of a trusted IC, the raw data, the read raw data has low accuracy.

(57) **摘要:** 一种芯片中非易失性存储空间的数据存储方法和可信芯片。其中, 该方法包括: 在芯片中创建非易失性存储空间 (S302), 其中, 非易失性存储空间的属性至少包括: 用于表征在非易失性存储空间中存储属主数据的参数, 属主数据的存储地址范围; 其中, 属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。该方法解决了现有技术从可信安全芯片的非易失空间中读取原始数据时, 读取到的原始数据准确性差的技术问题。



WO 2018/086469 A1

芯片中非易失性存储空间的数据存储方法和可信芯片

本申请要求 2016 年 11 月 11 日递交的申请号为 201610998449.0、发明名称为“芯片中非易失性存储空间的数据存储方法和可信芯片”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明涉及数据存储领域，具体而言，涉及一种芯片中非易失性存储空间的数据存储方法和可信芯片。

10 背景技术

用户可以在可信安全芯片中创建非易失空间，可以为非易失空间赋予如表 1 所示的属性：

表 1

Nv_index	User_name	Password	Nv_Size	Nv_F&L_adress	Data
非易失空间编号	非易失空间属主名称	非易失空间授权使用密码	非易失空间大小	非易失空间始末物理地址范围	属主数据

图 1 示出了根据现有技术的一种用户获取非易失空间数据的交互示意图，如图 1 所示，具体包括如下步骤：

15

(1) 属主 C 向可信芯片 T 发起访问非易失空间请求；

(2) 可信芯片 T 响应属主 C 请求，要求其反馈密码口令、非易失空间编号以及数据长度；

(3) 属主 C 回传口令、要访问的非易失空间编号、非易失数据长度给可信芯片 T；

20

(4) 可信芯片 T 验证口令和非易失空间索引编号的正确性，以及非易失空间的数据长度 L 是否满足下式：

$$L \leq | \text{Last\_adress} - \text{First\_adress} | \quad (1)$$

上式中，First_adress 表示非易失空间初始物理地址，Last_adress 表示非易失空间末位物理地址。

25

如果口令和非易失空间编号正确，其获取的数据长度 L 也满足公式 (1)，则可信芯片返回属主 C 要访问的数据，流程结束。否则，直接终止流程。

现有国际 TCG 标准安全芯片规范了可信安全芯片的非易失空间的固定大小、访问授

权，该规范中其状态标识数据默认为 0，容易与属主数据 0 相混淆，导致用户获取数据时，获取到的部分数据可能是状态标识数据 0，而非用户真正存储的数据 0。例如，属主 C 申请了 6 字节的非易失空间，其存放了 4 个字节的数据，如表 2 所示：属主空间编号为 1，属主名称为 C，属主空间编号对应的非易失空间的大小为 6 字节，即数据长度最大可为 6 字节，其对应的物理地址为 FFFFF0~FFFFF6，在其物理地址中存放了 4 字节，属主写入的数据为“1101”，TCG 标准默认没有写入数据的两字节为 00，即属主数据为 1101**00**（加粗斜体的数字表示状态数据，不加粗的数字表示属主数据，如表 1 所示的属主数据）。

表 2

Nv_index	User_name	Password	Nv_Size	Nv_F&L_adress	Data
1	C	****	6	FFFFF0~FFFFF6	1101 00

当存储数据较长，且经常变更时，属主 C 不一定能记住自己存了多长，且存了什么数据，比如当属主 C 并当属主向用户获取数据长度 5 时，且响应可信芯片要求反馈的信息：用户输入正确的口令****，Nv_index 编号 1，可信芯片接到信息后，验证口令和 Nv 索引编号的正确性，也验证其长度 5<6,是其可允许的范围，因此返回给属主 C 数据长度为 1101**0**，这样属主 C 的原始数据由 1101 变成了 1101**0**，造成了数据的错误。

针对上述现有技术从可信安全芯片的非易失空间中读取原始数据时，读取到的原始数据准确性差的技术问题，目前尚未提出有效的解决方案。

发明内容

本发明实施例提供了一种芯片中非易失性存储空间的数据存储方法和可信芯片，以至少解决现有技术从可信安全芯片的非易失空间中读取原始数据时，读取到的原始数据准确性差的技术问题。

根据本发明实施例的一个方面，提供了一种芯片中非易失性存储空间的数据存储方法，包括：在芯片中创建非易失性存储空间，其中，非易失性存储空间的属性至少包括：用于表征在非易失性存储空间中存储属主数据的参数，属主数据的存储地址范围；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

根据本发明实施例的另一方面，还提供了一种获取存储在芯片中的数据的方法，包括：接收用于访问芯片的非易失性存储空间的访问请求；响应访问请求，得到验证信息和需要请求的数据长度；在验证验证信息通过的情况下，判断需要请求的数据长度是否

处于非易失性存储空间中预先设置的属主数据的存储地址范围之内；如果需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回属主数据的内容；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

根据本发明实施例的另一方面，还提供了一种可信芯片，包括：存储器，包括非易失性存储空间，其中，非易失性存储空间的属性至少包括：用于表征在非易失性存储空间中存储属主数据的参数，属主数据的存储地址范围；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

根据本发明实施例的另一方面，还提供了一种获取存储在芯片中的数据的系统，包括：访问设备端，用于发出用于访问芯片的非易失性存储空间的访问请求；可信芯片，与访问设备端通信，用于响应访问请求，获取访问设备端返回的验证信息和需要请求的数据长度，在验证验证信息通过的情况下，如果需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回属主数据的内容；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

根据本发明实施例的另一方面，还提供了一种获取存储在芯片中的数据的装置，包括：接收模块，用于接收用于访问芯片的非易失性存储空间的访问请求；响应模块，用于响应访问请求，得到验证信息和需要请求的数据长度；判断模块，用于在验证验证信息通过的情况下，判断需要请求的数据长度是否处于非易失性存储空间中预先设置的属主数据的存储地址范围之内；控制模块，用于如果需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回属主数据的内容；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

在本发明实施例中，采用限定属主数据的存储地址范围的方式，通过在芯片中创建非易失存储空间之后，向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围，根据属主数据的大小和属主数据的存储地址范围返回属主需要获取的数据，达到了准确获取属主数据的目的，从而实现了保证属主获取原始数据的正确性的技术效果，进而解决了现有技术从可信安全芯片的非易失空间中读取原始数据时，读取到的原始数据准确性差的技术问题。

附图说明

此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

图 1 是根据现有技术的一种用户获取非易失空间数据的交互示意图；

图 2 是根据本发明实施例的一种可选的计算机终端的硬件结构框图；

图 3 是根据本发明实施例的一种芯片中非易失性存储空间的数据存储方法流程图；

图 4 是根据本发明实施例的一种可选的芯片中非易失性存储空间的数据存储方法流

5 程图；

图 5 是根据本发明实施例的一种可选的访问非易失性存储空间的属主数据的方法流程图；

图 6 是根据本发明实施例的一种可选的 TCG 信任链的结构示意图；

图 7 是根据本发明实施例的一种获取存储在芯片中的数据的方法流程图；

10 图 8 是根据本发明实施例的一种可信芯片的结构示意图；

图 9 是根据本发明实施例的一种获取存储在芯片中的数据的系统结构示意图；

图 10 是根据本发明实施例的一种获取存储在芯片中的数据的装置结构示意图；以及

图 11 是根据本发明实施例的一种可选的计算机终端的结构框图。

15 具体实施方式

为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保

20 护的范围。

需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变

25 形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

首先，在对本申请实施例进行描述的过程中出现的部分名词或术语适用于如下解释：

非易失存储（Non-volatile memory，简称为 Nv），作为一种存储技术，其可以保证

30 在设备掉电的时候，设备中存储的数据不会丢失，常用来保护用户非常敏感的数据。

属主数据，指用户向存储设备中存储的数据，其中，属主指对数据进行操作的主体。

可信，指一个实体一直以一种可预期的方式为特定的目标运行。

可信计算（Trusted computing），是在计算和通信系统中广泛使用的基于硬件安全模块支持下的可信计算平台，使用该可信计算平台可以提高系统整体的安全性。其核心机制是通过信任链机制构建可信计算环境。

可信安全芯片，是一种具有产生加解密密钥功能的芯片，可信安全芯片也能够进行高速的资料加密和解密，以及充当保护基本输入输出系统和操作系统不被修改的辅助处理器。

实施例 1

根据本发明实施例，还提供了一种芯片中非易失性存储空间的数据存储方法的方法实施例。

本申请实施例 1 所提供的方法实施例可以在移动终端、计算机终端或者类似的运算装置中执行。图 2 示出了一种用于实现芯片中非易失性存储空间的数据存储方法的计算机终端（或移动设备）的硬件结构框图。如图 2 所示，计算机终端 10（或移动设备 10）可以包括一个或多个（图中采用 102a、102b，……，102n 来示出）处理器 102（处理器 102 可以包括但不限于微处理器 MCU 或可编程逻辑器件 FPGA 等的处理装置）、用于存储数据的存储器 104、以及用于通信功能的传输模块 4。除此以外，还可以包括：显示器、输入/输出接口（I/O 接口）、通用串行总线（USB）端口（可以作为 I/O 接口的端口中的一个端口被包括）、网络接口、电源和/或相机。本领域普通技术人员可以理解，图 2 所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，计算机终端 10 还可包括比图 2 中所示更多或者更少的组件，或者具有与图 2 所示不同的配置。

应当注意到的是上述一个或多个处理器 102 和/或其他数据处理电路在本文中通常可以被称为“数据处理电路”。该数据处理电路可以全部或部分的体现为软件、硬件、固件或其他任意组合。此外，数据处理电路可为单个独立的处理模块，或全部或部分的结合到计算机终端 10（或移动设备）中的其他元件中的任意一个内。如本申请实施例中所涉及到的，该数据处理电路作为一种处理器控制（例如与接口连接的可变电阻终端路径的选择）。

存储器 104 可用于存储应用程序的软件程序以及模块，如本发明实施例中的芯片中非易失性存储空间的数据存储方法对应的程序指令/数据存储装置，处理器 102 通过运行存储在存储器 104 内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实

现上述的应用程序的漏洞检测方法。存储器 104 可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 104 可进一步包括相对于处理器 102 远程设置的存储器，这些远程存储器可以通过网络连接至计算机终端 10。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

此处需要说明的是，在一些可选实施例中，上述图 2 所示的计算机设备（或移动设备）可以包括硬件元件（包括电路）、软件元件（包括存储在计算机可读介质上的计算机代码）、或硬件元件和软件元件两者的结合。应当指出的是，图 2 仅为特定具体实例的一个实例，并且旨在示出可存在于上述计算机设备（或移动设备）中的部件的类型。

在上述运行环境下，本申请提供了如图 3 所示的芯片中非易失性存储空间的数据存储方法。图 3 是根据本发明实施例 1 的芯片中非易失性存储空间的数据存储方法的流程图，包括如下步骤：

步骤 S302，在芯片中创建非易失性存储空间，其中，非易失性存储空间的属性至少包括：用于表征在非易失性存储空间中存储属主数据的参数，属主数据的存储地址范围；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

在上述步骤 S302 所限定的技术方案中，上述非易失性存储空间的存储模式可以采用大端模式和小端模式，大端模式是指数据的高字节保存在内存的低地址中，而数据的低字节保存在内存的高地址中；而小端模式是指数据的高字节保存在内存的高地址中，而数据的低字节保存在内存的低地址中，该存储模式可以将地址的高低和数据有位权有效结合起来，高地址部分数据的权值高，低地址部分数据的权值低。

需要说明的是，非易失性存储空间的属性之一属主数据为用户存入到非易失性存储空间的数据，例如，用户存储的数据为“1101”，则该数据即为存储到非易失性存储空间的属主数据；非易失性存储空间的另一个属性属主数据的存储地址范围的长度为允许用户读取非易失性存储空间的最大数据长度，例如，属主数据的存储地址范围为：FFFFF0~FFFFF6，则允许用户向芯片请求数据时的最大数据长度为 7。此外，在芯片中创建非易失性存储空间可以保证在设备掉电时，存储在芯片中的数据不会丢失，从而可以用来存储比较重要的数据。

基于上述实施例步骤 S302 所公开的方案中，可以获知在芯片中创建非易失性存储空间，可以保证用户存储在芯片中的数据在设备掉电时，不会丢失，进而提高了数据存储的安全性。

可选的，非易失性存储空间的属性至少还包括如下至少之一：空间编号、空间属主名称、空间授权密码、空间大小和空间物理地址范围。

在一种可选的实施例中，表 3 为已经写入属主数据的非易失性存储空间的属性表，如表 3 所示。

5

表 3

Nv_index	User_name	Password	Nv_Size	First_address Last_address	Data	Max_address Min_address
空间编号	空间属主名称	空间授权密码	空间大小	空间物理地址范围	属主数据	属主数据块的存储地址范围
1	C	****	6	FFFFF0~ FFFFF6	1101	FFFFF1~ FFFFF4

在表 3 中，属主的空间编号为 1，空间属主名称为 C，属主空间编号为 1 的属主空间大小为 6 字节，即数据长度最大可为 6 字节，其对应的空间物理地址范围为 FFFFF0~FFFFF6，在其物理地址中存放了 4 字节，其存储地址范围为 FFFFF1~FFFFF4，写入的属主数据为“1101”。

10

可选的，图 4 示出了在芯片中创建非易失性存储空间之后，芯片中非易失性存储空间的数据存储方法的流程示意图，如图 4 所示，该方法还包括如下步骤：

步骤 S304，向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围，其中，通过属主数据的数据块的初始存储地址和末尾存储地址来确定存储地址范围。

15

在一种可选的实施例中，在属主数据的存储模式为小端模式的情况下，假设属主数据的大小为 L，属主数据的数据块的初始存储地址，即属主数据的低字节所在的内存地址为 Min_adress，属主数据的数据块的末尾存储地址，即属主数据的高字节所在的内存地址为 Max_adress，则 L、Min_adress 和 Max_adress 满足下式：

$$L \leq \text{Max\_adress} - \text{Min\_adress} + 1 \quad (2)$$

20

因此，根据属主数据的大小 L 以及属主数据的初始存储地址 Min_adress 可以确定属主数据的末尾地址 Max_adress，进而可以确定属主数据的存储地址范围。例如，向非易失性存储空间写入的属主数据为“1101”，该属主数据的大小为 4 字节，则该属主数据的存储地址范围的长度也为 4 字节，如果此时属主数据的初始存储地址为 FFFFF1，则该属主数据的末尾地址为 FFFFF4，属主数据的数据块的存储地址范围为 FFFFF1~FFFFF4。

25

可选的，图 5 示出了在向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围之后，访问非易失性存储空间的属主数据的方法流程图，

如图 5 所示，该方法包括如下步骤：

步骤 S502，接收用于访问非易失性存储空间的访问请求；

步骤 S504，响应访问请求，得到验证信息和需要请求的数据长度；

5 步骤 S506，在验证验证信息通过的情况下，判断需要请求的数据长度是否处于属主数据的存储地址范围之内；

步骤 S508，如果需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回属主数据的内容。

作为一种可选的实施例，访问设备端向可信芯片发起访问非易失性空间请求，可信芯片接收到访问设备端发送的非易失性空间请求后，响应访问设备端的请求，并要求访问设备端反馈验证信息以及属主数据的长度信息；访问设备端向可信芯片发送验证信息以及属主数据的长度信息，例如，访问的属主数据的长度为 4 字节；可信芯片验证访问设备端返回的验证信息是否符合要求，在验证信息符合要求的情况下，判断需要请求的数据长度是否处于属主数据的存储地址范围之内，例如，需要请求的数据长度为 4 字节，属主数据的存储地址范围为 FFFFF1~FFFFF4，属主数据的最大存储长度为 4 字节，请求的数据长度满足公式（2），因此，可信芯片允许访问属主数据，并返回存储地址范围为 FFFFF1~FFFFF4 的属主数据。

需要说明的是，上述验证信息可以用来验证访问设备端是否有访问的权限以及确定访问设备端访问数据的位置，从而可以进一步提高访问数据的准确性。

20 可选的，如果需要请求的数据长度处于属主数据的存储地址范围之外，则中止获取属主数据的流程，和/或输出用于表征请求失败的提示信息。

作为一种可选的实施例，在可信芯片验证访问设备端返回的验证信息符合要求的情况下，可信芯片进一步判断需要请求的数据长度是否处于属主数据的存储地址范围之内，如果需要请求的数据长度处于属主数据的存储地址范围之外，例如，需要请求的数据长度为 4 字节，而属主数据的存储地址范围为 FFFFF1~FFFFF3，属主数据的最大存储长度为 3 字节，请求的数据长度不满足公式（2），因此，可信芯片不允许访问属主数据，直接终止流程，并输出此次请求失败的提示信息。

可选的，验证信息至少包括如下至少之一：需要访问的空间编号、密码口令。

作为一种可选的实施例，验证上述需要访问的空间编号可以确认可信芯片中是否存在该空间编号，进一步验证密码口令可以确认当前访问的用户是否有访问权限，从而可以进一步提高访问数据的准确性。

可选的，在验证验证信息失败的情况下，返回无法获取属主数据的提示信息。

在一种可选的实施例中，用户需要访问的空间编号为 2，但可信芯片中不存在空间编号为 2 的属主数据，在这种情况下，中止获取属主数据的流程，并向访问设备端发送提示信息，提示不存在空间编号为 2 的属主数据。在另一种可选的实施例中，用户需要访问的空间编号为 2，可信芯片中存在空间编号为 2 的属主数据，当检测到密码口令不对，在这种情况下，同样会中止获取属主数据的流程，并向访问设备端发送提示信息，提示密码口令不正确，并要求其再次操作。

在一种优选的实施例中，属主 C 申请了 6 字节的非易失性空间，其存放了 4 个字节的数据，如表 4 所示：属主空间编号 Nv_index 为 1，空间属主名称 User_name 为 C，属主空间编号 1 对应的空间大小 Nv_Size 为 6 字节，即数据长度最大可为 6 字节；其对应的物理地址为 FFFFF0~FFFFF6，在物理地址中存放了 4 字节，属主写入的数据为“1101”，TCG 标准默认没有写入的属主数据 Data 为 **00**，即 Data 数据项数据为 1101**00**（加粗斜体的数字表示状态数据，不加粗的数字表示属主数据，如表 4 所示的属主数据）。

表 4

Nv_index	User_name	Password	Nv_Size	First_address Last_address	Data	Max_address Min_address
1	C	****	6	FFFFF0~ FFFFF6	1101 00	FFFFF1~ FFFFF4

当存储的数据较长且经常变更时，属主可能不记得在存储空间中存储数据长度为多长的数据，例如，当属主要求向可信芯片获取数据的长度为 5，并响应了可信芯片要求反馈的信息，包括：属主输入的正确的密码口令****，以及空间编号 Nv_index 1 后，可信芯片接到上述验证信息后，验证密码口令和空间编号反馈正确，并验证其要求获取的数据长度 5 大于属主数据的长度 4，由于请求数据长度不在其允许访问的范围内，因此可信芯片提示请求数据超出预存范围，终止获取属主数据的流程。

可信计算能够在计算运算的同时进行安全防护，使计算结果总是与预期一致，计算全程可测可控，不被干扰。

可信计算的核心要素是可信链与可信根，其中，可信计算可以通过信任链机制构架可信计算环境。在可信根为包含有非易失性存储空间的可信芯片的情况下，存在另一种可选的实施例，具体如下：

目前可信计算有国内可信平台控制模块（Trusted Platform Control Module，TPCM）和国际 TCG 标准组织的可信平台模块(Trusted Platform Module,TPM)两种技术路线。

可信计算的核心要素是可信链与可信根，TCG 规范中的可信平台模块(Trusted Platform Module,TPM)是可信计算平台的硬件可信根，TPM 是提供受保护的安全存储、密码运算能力的安全芯片。TPM 通过物理方式与计算平台相连并通过外部总线连接到 CPU 上，例如 PC 机平台上采取直接固化在主板上的方式并通过 LPC 总线连接。

5 TCG 规范中给出了对可信 (trusted) 的定义：一个实体一直以一种可预期的方式为特定的目标运行。可信计算的核心机制是通过信任链机制构建可信计算环境，目前运行实体是否可信是建立系统前一运行过程是否可信的基础上。基于这种信任关系，如果系统从一个初始的信任根出发，在平台计算环境的每一次转换时，这种信任可以通过传递的方式维持下去，从而在计算平台上建立了一级验证一级，一级信任一级的可信链，该
10 计算环境就始终是可信的，它能够被本地用户或远程实体信任。图 6 示出了 TCG 信任链的结构示意图，如图 6 所示，图中实线箭头表示可信度量连接，虚线箭头表示可信报告连接，加粗实线箭头表示可信存储连接，加粗虚线箭头表示可信网络连接。

可信计算的关键技术包括可信度量，可信报告，可信存储和可信网络连接等几部分。

可信平台控制模块 TPCM 实现了可信平台模块的基本功能，其功能组成和与 TPM
15 基本相同，但由于 TPM 的核心度量根 CRTM 处于基本输入输出系统 BIOS 中，不受 TPM 的保护，因此，TPCM 提出新的可信度量根设计，解决了可信度量根的起始度量点问题，改变了启动和度量顺序，在此基础上，建立了以该芯片为信任根的信任链度量流程，实现了由该芯片控制整个系统的启动，I/O 接口控制以及系统配置等，体现了该芯片对系统可信性的控制作用。

20 在计算平台的运行控制传递过程中，可信根 TPCM 判断其下一级执行代码的真实性和完整性是否被篡改，如果没有，系统将运行控制权传递到下一级可信执行代码，系统的可信范围因扩大到下一级功能代码；同理，这种系统控制权不断传递，就可以实现信任链的建立和传递过程，最终实现系统范围可信构建。一个完整的系统可信传递过程要从可信根开始，系统控制权顺序由可信平台控制模块传递到可信的 BIOS，再传递到可信
25 的操作系统装载器，从可信的操作系统装载器传递到可信的操作系统，再从可信的操作系统传递到可信的应用。

可信安全芯片具有产生加解密密钥的功能，也能够进行高速的资料加密和解密，以及充当保护 BIOS 和操作系统不被修改的辅助处理器。

TPM 安全芯片用途十分广泛，配合专用软件可以实现以下用途：

30 (1) 存储、管理 BIOS 开机密码以及硬盘密码。以往这些事务都是由 BIOS 做的，

玩过的朋友可能知道，忘记了密码只要取下 CMOS 电池，给 CMOS 放电就清除密码了。如今这些密钥实际上是存储于固化在芯片的存储单元中，即便是掉电其信息亦不会丢失。相比于 BIOS 管理密码，TPM 安全芯片的安全性要大为提高。

(2) TPM 安全芯片可以进行范围较广的加密。TPM 安全芯片除了能进行传统的开机加密以及对硬盘进行加密外，还能对系统登录、应用软件登录进行加密。比如 MSN、QQ、网游以及网上银行的登录信息和密码，都可以通过 TPM 加密后再进行传输，这样就不用担心信息和密码被人窃取。

(3) 加密硬盘的任意分区。可以加密本本上的任意一个硬盘分区，也可以将一些敏感的文件放入该分区以策安全。比如有些本本厂商采用的一键恢复功能，就是该用途的集中体现之一（其将系统镜像放在一个 TPM 加密的分区中）。还有一些大型商业软件公司(如：Microsoft)也会利用其作为加密分区的手段(如：著名的 BitLocker)。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，计算机，服务器，或者网络设备等）执行本发明各个实施例的方法。

实施例 2

根据本发明实施例，还提供了一种获取存储在芯片中的数据的方法实施例。

本申请提供了如图 7 所示的获取存储在芯片中的数据的方法。图 7 是根据本发明实施例 2 的获取存储在芯片中的数据的方法流程图。包括如下步骤：

步骤 S702，接收用于访问芯片的非易失性存储空间的访问请求；

步骤 S704，响应访问请求，得到验证信息和需要请求的数据长度；

步骤 S706，在验证验证信息通过的情况下，判断需要请求的数据长度是否处于非易失性存储空间中预先设置的属主数据的存储地址范围之内；

步骤 S708, 如果需要请求的数据长度处于属主数据的存储地址范围之内, 则允许返回属主数据的内容; 其中, 属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

在上述步骤 S702 至步骤 S708 所限定的方案中, 上述访问芯片可以为可信芯片, 该可信芯片中包含非易失性存储空间。上述非易失性存储空间的存储模式可以采用大端模式和小端模式, 在属主数据的存储模式为小端模式的情况下, 假设属主数据的大小为 L , 属主数据的数据块的初始存储地址, 即属主数据的低字节所在的内存地址为 Min_adress , 属主数据的数据块的末尾存储地址, 即属主数据的高字节所在的内存地址为 Max_adress , 则 L 、 Min_adress 和 Max_adress 满足下式:

$$L \leq |\text{Max\_adress} - \text{Min\_adress}|$$

在访问设备端向可信芯片发起访问非易失性空间请求, 可信芯片接收到访问设备端发送的非易失性空间请求后, 响应访问设备端的请求, 并要求访问设备端反馈验证信息以及属主数据的长度信息; 访问设备端向可信芯片发送验证信息以及属主数据的长度信息, 例如, 访问的属主数据的长度为 4 字节; 可信芯片验证访问设备端返回的验证信息是否符合要求, 在验证信息符合要求的情况下, 判断需要请求的数据长度是否处于属主数据的存储地址范围之内, 例如, 需要请求的数据长度为 4 字节, 属主数据的存储地址范围为 $\text{FFFFF1} \sim \text{FFFFF4}$, 属主数据的最大存储长度为 4 字节, 请求的数据长度满足公式:

$$L \leq |\text{Max\_adress} - \text{Min\_adress}|$$

因此, 可信芯片允许访问属主数据, 并返回存储地址范围为 $\text{FFFFF1} \sim \text{FFFFF4}$ 的属主数据。

需要说明的是, 上述验证信息可以用来验证访问设备端是否有访问的权限以及确定访问设备端访问数据的位置, 从而可以进一步提高访问数据的准确性。上述非易失性存储空间的存储模式可以采用大端模式和小端模式, 大端模式是指数据的高字节保存在内存的低地址中, 而数据的低字节保存在内存的高地址中; 而小端模式是指数据的高字节保存在内存的高地址中, 而数据的低字节保存在内存的低地址中, 该存储模式可以将地址的高低和数据的位权有效结合起来, 高地址部分数据的权值高, 低地址部分数据的权值低。

基于上述实施例步骤 S702 至步骤 S708 所公开的方案中, 可以获知通过在芯片中创建非易失性存储空间之后, 向非易失性存储空间写入属主数据, 并根据属主数据的大小确定属主数据的存储地址范围, 根据属主数据的大小和属主数据的存储地址范围返回属主需要获取的数据, 达到了准确获取属主数据的目的, 从而实现了保证属主获取原始数据

的正确性的技术效果，进而解决了现有技术从可信安全芯片的非易失空间中读取原始数据时，读取到的原始数据准确性差的技术问题。

可选的，非易失性存储空间的属性至少还包括如下至少之一：空间编号，空间属主名称、空间授权密码、空间大小和空间物理地址范围。

- 5 在一种可选的实施例中，表 5 为已经写入属主数据的非易失性存储空间的属性表，如表 5 所示。

表 5

Nv_index	User_name	Password	Nv_Size	First_adress Last_adress	Data	Max_adress Min_adress
空间编号	空间属主名称	空间授权密码	空间大小	空间物理地址范围	属主数据	属主数据块的存储地址范围
1	C	****	6	FFFFF0~ FFFFF6	1101	FFFFF1~ FFFFF4

- 在表 5 中，属主的空间编号为 1，空间属主名称为 C，属主空间编号为 1 的属主空间大小为 6 字节，即数据长度最大可为 6 字节，其对应的空间物理地址范围为
10 FFFFF0~FFFFF6，在其物理地址中存放了 4 字节，其存储地址范围为 FFFFF1~FFFFF4，写入的属主数据为“1101”。

可选的，在接收用于访问芯片的非易失性存储空间的访问请求之前，方法还包括：向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围，其中，通过属主数据的数据块的初始存储地址和末尾存储地址来确定存储地址范围。

- 15 在一种可选的实施例中，在属主数据的存储模式为小端模式的情况下，假设属主数据的大小为 L，属主数据的数据块的初始存储地址，即属主数据的低字节所在的内存地址为 Min_adress，属主数据的数据块的末尾存储地址，即属主数据的高字节所在的内存地址为 Max_adress，则 L、Min_adress 和 Max_adress 满足下式：

$$L \leq | \text{Max\_adress} - \text{Min\_adress} |$$

- 20 因此，根据属主数据的大小 L 以及属主数据的初始存储地址 Min_adress 可以确定属主数据的末尾地址 Max_adress，进而可以确定属主数据的存储地址范围。例如，向非易失性存储空间写入的属主数据为“1101”，该属主数据的大小为 4 字节，则该属主数据的存储地址范围的长度也为 4 字节，如果此时属主数据的初始存储地址为 FFFFF1，则该属主数据的末尾地址为 FFFFF4，属主数据的数据块的存储地址范围为 FFFFF1~FFFFF4。

- 25 可选的，如果需要请求的数据长度处于属主数据的存储地址范围之外，则中止获取属主数据的流程，和/或输出用于表征请求失败的提示信息。

作为一种可选的实施例，在可信芯片验证访问设备端返回的验证信息符合要求的情况下，可信芯片进一步判断需要请求的数据长度是否处于属主数据的存储地址范围之内，如果需要请求的数据长度处于属主数据的存储地址范围之外，例如，需要请求的数据长度为 4 字节，而属主数据的存储地址范围为 FFFFF1~FFFFF3，属主数据的最大存储长度
5 为 3 字节，请求的数据长度不满足公式 $L \leq | \text{Max\_adress} - \text{Min\_adress} |$ ，因此，可信芯片不允许访问属主数据，直接终止流程，并输出此次请求失败的提示信息。

实施例 3

根据本发明实施例，还提供了一种可信芯片的实施例。

本申请提供了如图 8 所示的可信芯片的结构示意图。图 8 是根据本发明实施例 3 的
10 可信芯片的结构示意图，该可信芯片包括：存储器 801。其中，

存储器 801，包括非易失性存储空间，其中，非易失性存储空间的属性至少包括：用于表征在非易失性存储空间中存储属主数据的参数，属主数据的存储地址范围；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

在上述存储器 801 所限定的技术方案中，上述非易失存储空间的存储模式可以采用
15 大端模式和小端模式，大端模式是指数据的高字节保存在内存的低地址中，而数据的低字节保存在内存的高地址中；而小端模式是指数据的高字节保存在内存的高地址中，而数据的低字节保存在内存的低地址中，该存储模式可以将地址的高低和数据有位权有效结合起来，高地址部分数据的权值高，低地址部分数据的权值低。

需要说明的是，非易失性存储空间的属性之一属主数据为用户存入到非易失性存储
20 空间的数据，例如，用户存储的数据为“1101”，则该数据即为存储到非易失性存储空间的属主数据；非易失性存储空间的另一个属性属主数据的存储地址范围的长度为允许用户读取非易失性存储空间的最大数据长度，例如，属主数据的存储地址范围为：FFFFF0~FFFFF6，则允许用户向芯片请求数据时的最大数据长度为 7。此外，在芯片中创建非易失性存储空间可以保证在设备掉电时，存储在芯片中的数据不会丢失，从而可
25 以用来存储比较重要的数据。

由上可知，在芯片中创建非易失性存储空间，可以保证用户存储在芯片中的数据在设备掉电时，不会丢失，进而提高了数据存储的安全性。

实施例 4

根据本发明实施例，还提供了一种获取存储在芯片中的数据的系统实施例。

本申请提供了如图 9 所示的获取存储在芯片中的数据的系统。图 9 是根据本发明实
30

施例 4 的获取存储在芯片中的数据的系统结构示意图，该系统包括：访问设备端 901 和可信芯片 903。其中，

访问设备端 901，用于发出用于访问芯片的非易失性存储空间的访问请求；

可信芯片 903，与访问设备端通信，用于响应访问请求，获取访问设备端返回的验证信息和需要请求的数据长度，在验证验证信息通过的情况下，如果需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回属主数据的内容；其中，属主数据的存储地址范围用于表征允许向可信芯片请求数据时的最大数据长度。

在一种可选的实施例中，上述可信芯片中包含非易失性存储空间。上述非易失性存储空间的存储模式可以采用大端模式和小端模式，在属主数据的存储模式为小端模式的情况下，假设属主数据的大小为 L ，属主数据的数据块的初始存储地址，即属主数据的低字节所在的内存地址为 Min_adress ，属主数据的数据块的末尾存储地址，即属主数据的高字节所在的内存地址为 Max_adress ，则 L 、 Min_adress 和 Max_adress 满足下式：

$$L \leq |\text{Max\_adress} - \text{Min\_adress}|$$

在访问设备端向可信芯片发起访问非易失性空间请求，可信芯片接收到访问设备端发送的非易失性空间请求后，响应访问设备端的请求，并要求访问设备端反馈验证信息以及属主数据的长度信息；访问设备端向可信芯片发送验证信息以及属主数据的长度信息，例如，访问的属主数据的长度为 4 字节；可信芯片验证访问设备端返回的验证信息是否符合要求，在验证信息符合要求的情况下，判断需要请求的数据长度是否处于属主数据的存储地址范围之内，例如，需要请求的数据长度为 4 字节，属主数据的存储地址范围为 $\text{FFFFF1} \sim \text{FFFFF4}$ ，属主数据的最大存储长度为 4 字节，请求的数据长度满足公式：

$$L \leq |\text{Max\_adress} - \text{Min\_adress}|$$

因此，可信芯片允许访问属主数据，并返回存储地址范围为 $\text{FFFFF1} \sim \text{FFFFF4}$ 的属主数据。

需要说明的是，上述验证信息可以用来验证访问设备端是否有访问的权限以及确定访问设备端访问数据的位置，从而可以进一步提高访问数据的准确性。上述非易失性存储空间的存储模式可以采用大端模式和小端模式，大端模式是指数据的高字节保存在内存的低地址中，而数据的低字节保存在内存的高地址中；而小端模式是指数据的高字节保存在内存的高地址中，而数据的低字节保存在内存的低地址中，该存储模式可以将地址的高低和数据的位权有效结合起来，高地址部分数据的权值高，低地址部分数据的权值低。

由上可知，通过在芯片中创建非易失性存储空间之后，向非易失性存储空间写入属主

数据，并根据属主数据的大小确定属主数据的存储地址范围，根据属主数据的大小和属主数据的存储地址范围返回属主需要获取的数据，达到了准确获取属主数据的目的，从而实现了保证属主获取原始数据的正确性的技术效果，进而解决了现有技术从可信安全芯片的非易失空间中读取原始数据时，读取到的原始数据准确性差的技术问题。

- 5 可选的，可信芯片 903 还用于向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围，其中，通过属主数据的数据块的初始存储地址和末尾存储地址来确定存储地址范围。

实施例 5

- 10 根据本发明实施例，还提供了一种用于实施上述实施例 2 的获取存储在芯片中的数据的装置，如图 10 所示，该装置包括：接收模块 1001、响应模块 1003、判断模块 1005 和控制模块 1007。其中，

接收模块 1001，用于接收用于访问芯片的非易失性存储空间的访问请求；

响应模块 1003，用于响应访问请求，得到验证信息和需要请求的数据长度；

- 15 判断模块 1005，用于在验证验证信息通过的情况下，判断需要请求的数据长度是否处于非易失性存储空间中预先设置的属主数据的存储地址范围之内；

控制模块 1007，用于如果需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回属主数据的内容；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

- 20 上述访问芯片可以为可信芯片，该可信芯片中包含非易失性存储空间。上述非易失性存储空间的存储模式可以采用大端模式和小端模式，在属主数据的存储模式为小端模式的情况下，假设属主数据的大小为 L，属主数据的数据块的初始存储地址，即属主数据的低字节所在的内存地址为 Min_adress，属主数据的数据块的末尾存储地址，即属主数据的高字节所在的内存地址为 Max_adress，则 L、Min_adress 和 Max_adress 满足下式：

$$L \leq |Max\_adress - Min\_adress|$$

- 25 在访问设备端向可信芯片发起访问非易失性空间请求，可信芯片接收到访问设备端发送的非易失性空间请求后，响应访问设备端的请求，并要求访问设备端反馈验证信息以及属主数据的长度信息；访问设备端向可信芯片发送验证信息以及属主数据的长度信息，例如，访问的属主数据的长度为 4 字节；可信芯片验证访问设备端返回的验证信息是否符合要求，在验证信息符合要求的情况下，判断需要请求的数据长度是否处于属主数据的存储地址范围之内，例如，需要请求的数据长度为 4 字节，属主数据的存储地址
- 30

范围为 FFFFF1~FFFFF4, 属主数据的最大存储长度为 4 字节, 请求的数据长度满足公式:

$$L \leq | \text{Max\_adress} - \text{Min\_adress} |$$

因此, 可信芯片允许访问属主数据, 并返回存储地址范围为 FFFFF1~FFFFF4 的属主数据。

- 5 需要说明的是, 上述验证信息可以用来验证访问设备端是否有访问的权限以及确定访问设备端访问数据的位置, 从而可以进一步提高访问数据的准确性。上述非易失存储空间的存储模式可以采用大端模式和小端模式, 大端模式是指数据的高字节保存在内存的低地址中, 而数据的低字节保存在内存的高地址中; 而小端模式是指数据的高字节保存在内存的高地址中, 而数据的低字节保存在内存的低地址中, 该存储模式可以将地址的高低和数据的位权有效结合起来, 高地址部分数据的权值高, 低地址部分数据的权值低。

10 由上可知, 通过在芯片中创建非易失存储空间之后, 向非易失性存储空间写入属主数据, 并根据属主数据的大小确定属主数据的存储地址范围, 根据属主数据的大小和属主数据的存储地址范围返回属主需要获取的数据, 达到了准确获取属主数据的目的, 从而实现了保证属主获取原始数据的正确性的技术效果, 进而解决了现有技术从可信安全芯片的非易失空间中读取原始数据时, 读取到的原始数据准确性差的技术问题。

15 此处需要说明的是, 上述接收模块 1001、响应模块 1003、判断模块 1005 和控制模块 1007 对应于实施例 2 中的步骤 S702 至步骤 S708, 四个模块与对应的步骤所实现的实例和应用场景相同, 但不限于上述实施例 2 所公开的内容。需要说明的是, 上述模块作为装置的一部分可以运行在实施例 1 提供的计算机终端 10 中。

20 可选的, 非易失性存储空间的属性至少还包括如下至少之一: 空间编号, 空间属主名称、空间授权密码、空间大小和空间物理地址范围。

在一种可选的实施例中, 表 6 为已经写入属主数据的非易失性存储空间的属性表, 如表 6 所示。

表 6

Nv_index	User_name	Password	Nv_Size	First_adress Last_adress	Data	Max_adress Min_adress
空间编号	空间属主名称	空间授权密码	空间大小	空间物理地址范围	属主数据	属主数据块的存储地址范围
1	C	****	6	FFFFF0~ FFFFF6	1101	FFFFF1~ FFFFF4

25 在表 6 中, 属主的空间编号为 1, 空间属主名称为 C, 属主空间编号为 1 的属主空间大小为 6 字节, 即数据长度最大可为 6 字节, 其对应的空间物理地址范围为

FFFFFF0~FFFFFF6，在其物理地址中存放了 4 字节，其存储地址范围为 FFFFFF1~FFFFFF4，写入的属主数据为“1101”。

可选的，如图 10 所示，上述获取存储在芯片中的数据还包括：写入模块 1009，用于向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围，其中，通过属主数据的数据块的初始存储地址和末尾存储地址来确定存储地址范围。

在一种可选的实施例中，在属主数据的存储模式为小端模式的情况下，假设属主数据的大小为 L ，属主数据的数据块的初始存储地址，即属主数据的低字节所在的内存地址为 $Min\_address$ ，属主数据的数据块的末尾存储地址，即属主数据的高字节所在的内存地址为 $Max\_address$ ，则 L 、 $Min\_address$ 和 $Max\_address$ 满足下式：

$$L \leq |Max\_address - Min\_address|$$

因此，根据属主数据的大小 L 以及属主数据的初始存储地址 $Min\_address$ 可以确定属主数据的末尾地址 $Max\_address$ ，进而可以确定属主数据的存储地址范围。例如，向非易失性存储空间写入的属主数据为“1101”，该属主数据的大小为 4 字节，则该属主数据的存储地址范围的长度也为 4 字节，如果此时属主数据的初始存储地址为 FFFFFF1，则该属主数据的末尾地址为 FFFFFF4，属主数据的数据块的存储地址范围为 FFFFFF1~FFFFFF4。

可选的，如果需要请求的数据长度处于属主数据的存储地址范围之外，则中止获取属主数据的流程，和/或输出用于表征请求失败的提示信息。

作为一种可选的实施例，在可信芯片验证访问设备端返回的验证信息符合要求的情况下，可信芯片进一步判断需要请求的数据长度是否处于属主数据的存储地址范围之内，如果需要请求的数据长度处于属主数据的存储地址范围之外，例如，需要请求的数据长度为 4 字节，而属主数据的存储地址范围为 FFFFFF1~FFFFFF3，属主数据的最大存储长度为 3 字节，请求的数据长度不满足公式 $L \leq |Max\_address - Min\_address|$ ，因此，可信芯片不允许访问属主数据，直接终止流程，并输出此次请求失败的提示信息。

实施例 6

本发明的实施例可以提供一种计算机终端，该计算机终端可以是计算机终端群中的任意一个计算机终端设备。可选地，在本实施例中，上述计算机终端也可以替换为移动终端等终端设备。

可选地，在本实施例中，上述计算机终端可以位于计算机网络的多个网络设备中的至少一个网络设备。

可选地，图 11 是根据本发明实施例的一种计算机终端的结构框图。如图 11 所示，该计算机终端 A 可以包括：一个或多个（图中仅示出一个）处理器 1103 以及存储器 1101。

其中，存储器可用于存储软件程序以及模块，如本发明实施例中的安全漏洞检测方法和装置对应的程序指令/模块，处理器通过运行存储在存储器内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的系统漏洞攻击的检测方法。存储器可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器可进一步包括相对于处理器远程设置的存储器，这些远程存储器可以通过网络连接至终端 A。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

处理器可以通过传输装置调用存储器存储的信息及应用程序，以执行下述步骤：在芯片中创建非易失性存储空间，其中，非易失性存储空间的属性至少包括：用于表征在非易失性存储空间中存储属主数据的参数，属主数据的存储地址范围；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

可选的，上述处理器还可以执行如下步骤的程序代码：向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围，其中，通过属主数据的数据块的初始存储地址和末尾存储地址来确定存储地址范围。

可选的，上述处理器还可以执行如下步骤的程序代码：接收用于访问非易失性存储空间的访问请求；响应访问请求，得到验证信息和需要请求的数据长度；在验证验证信息通过的情况下，判断需要请求的数据长度是否处于属主数据的存储地址范围之内；如果需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回属主数据的内容。

可选的，上述处理器还可以执行如下步骤的程序代码：如果需要请求的数据长度处于属主数据的存储地址范围之外，则中止获取属主数据的流程，和/或输出用于表征请求失败的提示信息。

采用本发明实施例，提供了一种获取存储在芯片中的数据的方案的方案，通过在芯片中创建非易失存储空间之后，向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围，根据属主数据的大小和属主数据的存储地址范围返回属主需要获取的数据，达到了准确获取属主数据的目的，从而实现了保证属主获取原始数据的正确性的技术效果，进而解决了现有技术从可信安全芯片的非易失空间中读取原始数据时，读取到的原始数据准确性差的技术问题。

本领域普通技术人员可以理解，图 11 所示的结构仅为示意，计算机终端也可以是智

能手机（如Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices, MID）、PAD 等终端设备。图 11 其并不对上述电子装置的结构造成限定。例如，计算机终端 11 还可包括比图 11 中所示更多或者更少的组件（如网络接口、显示装置等），或者具有与图 11 所示不同的配置。

- 5 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（Read-Only Memory, ROM）、随机存取器（Random Access Memory, RAM）、磁盘或光盘等。

实施例 7

- 10 本发明的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以用于保存上述实施例 2 所提供的获取存储在芯片中的数据的方法所执行的程序代码。

可选地，在本实施例中，上述存储介质可以位于计算机网络中计算机终端群中的任意一个计算机终端中，或者位于移动终端群中的任意一个移动终端中。

- 15 可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：接收用于访问芯片的非易失性存储空间的访问请求；响应访问请求，得到验证信息和需要请求的数据长度；在验证验证信息通过的情况下，判断需要请求的数据长度是否处于非易失性存储空间中预先设置的属主数据的存储地址范围之内；如果需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回属主数据的内容；其中，属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

- 20 可选地，在本实施例中，存储介质被设置为存储还用于执行以下步骤的程序代码：向非易失性存储空间写入属主数据，并根据属主数据的大小确定属主数据的存储地址范围，其中，通过属主数据的数据块的初始存储地址和末尾存储地址来确定存储地址范围。

- 25 可选地，在本实施例中，存储介质被设置为存储还用于执行以下步骤的程序代码：如果需要请求的数据长度处于属主数据的存储地址范围之外，则中止获取属主数据的流程，和/或输出用于表征请求失败的提示信息。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

- 30 在本申请所提供的几个实施例中，应该理解到，所揭露的技术内容，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如单元的划分，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，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

5 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。

10 另外，在本发明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。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

15 集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可为个人计算机、服务器或者网络设备等）执行本发明各个实施例方法的全部或部分步骤。而前述的存储介质包括：U 盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

20 以上仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权利要求书

1.一种可信芯片，其特征在于，包括：

存储器，包括非易失性存储空间，其中，所述非易失性存储空间的属性至少包括：
用于表征在所述非易失性存储空间中存储属主数据的参数，和所述属主数据的存储地址
5 范围；

其中，所述属主数据的存储地址范围用于表征允许向芯片请求数据时的最大数据长度。

2.一种获取存储在芯片中的数据的系统，其特征在于，包括：

访问设备端，用于发出用于访问芯片的非易失性存储空间的访问请求；

10 可信芯片，与所述访问设备端通信，用于响应所述访问请求，获取所述访问设备端返回的验证信息和需要请求的数据长度，在验证所述验证信息通过的情况下，如果所述需要请求的数据长度处于属主数据的存储地址范围之内，则允许返回所述属主数据的内容；

15 其中，所述属主数据的存储地址范围用于表征允许向所述可信芯片请求数据时的最大数据长度。

3.一种芯片中非易失性存储空间的数据存储方法，其特征在于，包括：

在芯片中创建非易失性存储空间，其中，所述非易失性存储空间的属性至少包括：
用于表征在所述非易失性存储空间中存储属主数据的参数，所述属主数据的存储地址范围；

20 其中，所述属主数据的存储地址范围用于表征允许向所述芯片请求数据时的最大数据长度。

4.根据权利要求3所述的方法，其特征在于，所述非易失性存储空间的属性至少还包括如下至少之一：空间编号、空间属主名称、空间授权密码、空间大小和空间物理地址范围。

25 5.根据权利要求3或4所述的方法，其特征在于，在芯片中创建非易失性存储空间之后，所述方法还包括：向所述非易失性存储空间写入所述属主数据，并根据所述属主数据的大小确定所述属主数据的存储地址范围，其中，通过所述属主数据的数据块的初始存储地址和末尾存储地址来确定所述存储地址范围。

30 6.根据权利要求5所述的方法，其特征在于，在向所述非易失性存储空间写入所述属主数据，并根据所述属主数据的大小确定所述属主数据的存储地址范围之后，所述方

法还包括：

接收用于访问所述非易失性存储空间的访问请求；

响应所述访问请求，得到验证信息和需要请求的数据长度；

5 在验证所述验证信息通过的情况下，判断所述需要请求的数据长度是否处于所述属主数据的存储地址范围之内；

如果所述需要请求的数据长度处于所述属主数据的存储地址范围之内，则允许返回所述属主数据的内容。

7.根据权利要求 6 所述的方法，其特征在于，如果所述需要请求的数据长度处于所述属主数据的存储地址范围之外，则中止获取所述属主数据的流程，和/或输出用于表征
10 请求失败的提示信息。

8.根据权利要求 6 所述的方法，其特征在于，所述验证信息至少包括如下至少之一：需要访问的空间编号、密码口令。

9.根据权利要求 6 所述的方法，其特征在于，在验证所述验证信息失败的情况下，返回无法获取所述属主数据的提示信息。

15 10.一种获取存储在芯片中的数据的方法，其特征在于，包括：

接收用于访问芯片的非易失性存储空间的访问请求；

响应所述访问请求，得到验证信息和需要请求的数据长度；

在验证所述验证信息通过的情况下，判断所述需要请求的数据长度是否处于所述非易失性存储空间中预先设置的属主数据的存储地址范围之内；

20 如果所述需要请求的数据长度处于所述属主数据的存储地址范围之内，则允许返回所述属主数据的内容；

其中，所述属主数据的存储地址范围用于表征允许向所述芯片请求数据时的最大数据长度。

11.根据权利要求 10 所述的方法，其特征在于，所述非易失性存储空间的属性至少
25 还包括如下至少之一：空间编号，空间属主名称、空间授权密码、空间大小和空间物理地址范围。

12.根据权利要求 10 或 11 所述的方法，其特征在于，在接收用于访问芯片的非易失性存储空间的访问请求之前，所述方法还包括：向所述非易失性存储空间写入所述属主数据，并根据所述属主数据的大小确定所述属主数据的存储地址范围，其中，通过所述
30 属主数据的数据块的初始存储地址和末尾存储地址来确定所述存储地址范围。

13.根据权利要求 10 所述的方法，其特征在于，如果所述需要请求的数据长度处于所述属主数据的存储地址范围之外，则中止获取所述属主数据的流程，和/或输出用于表征请求失败的提示信息。

14.一种获取存储在芯片中的数据的装置，其特征在于，包括：

- 5 接收模块，用于接收用于访问芯片的非易失性存储空间的访问请求；
- 响应模块，用于响应所述访问请求，得到验证信息和需要请求的数据长度；
- 判断模块，用于在验证所述验证信息通过的情况下，判断所述需要请求的数据长度是否处于所述非易失性存储空间中预先设置的属主数据的存储地址范围之内；
- 控制模块，用于如果所述需要请求的数据长度处于所述属主数据的存储地址范围之
- 10 内，则允许返回所述属主数据的内容；
- 其中，所述属主数据的存储地址范围用于表征允许向所述芯片请求数据时的最大数据长度。

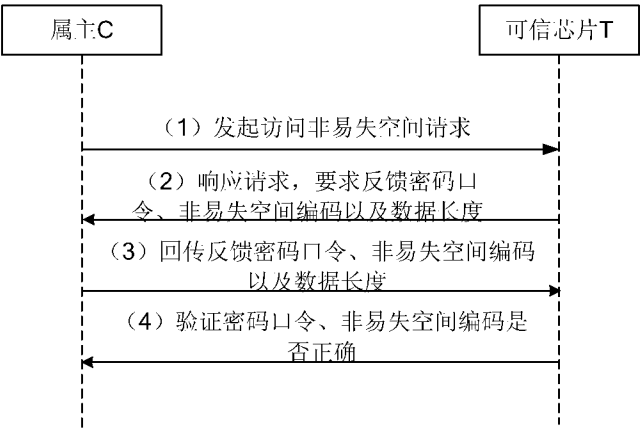


图 1

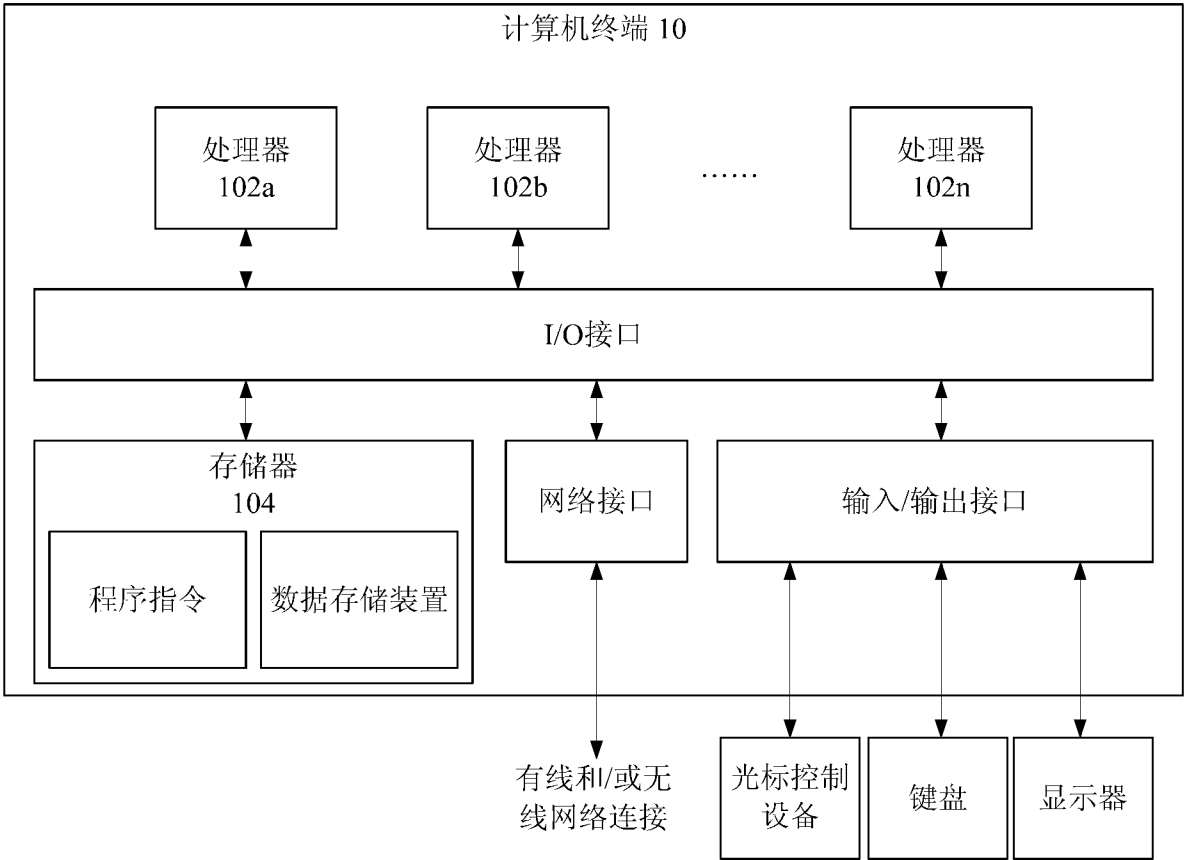


图 2

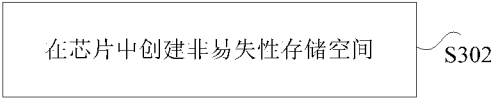


图 3

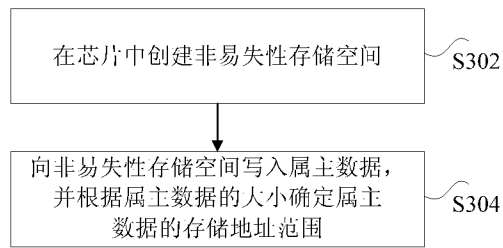


图 4

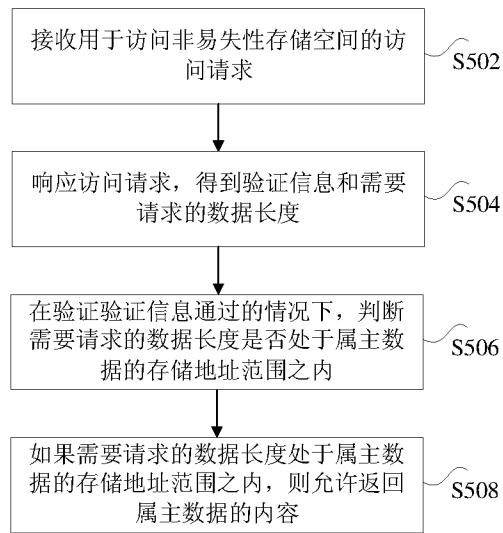


图 5

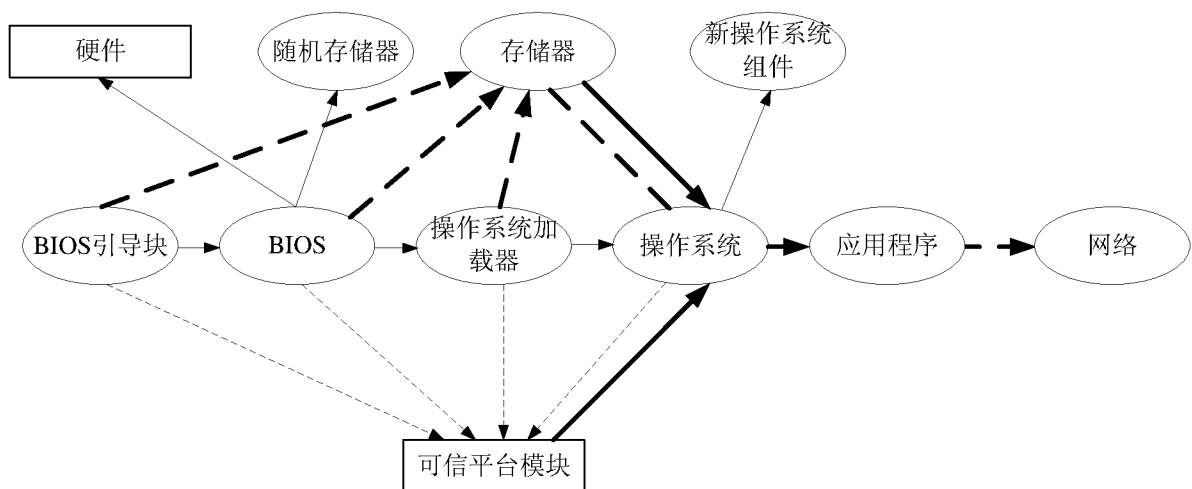


图 6

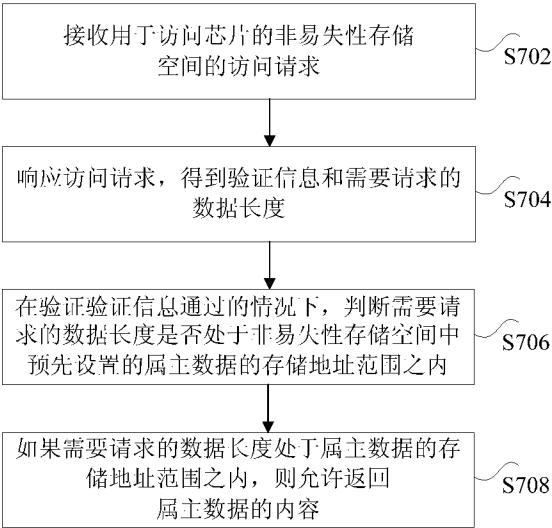


图 7



图 8

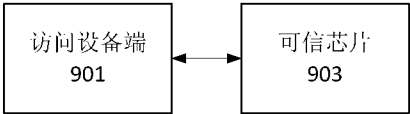


图 9



图 10

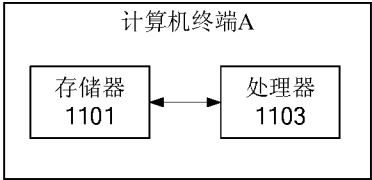


图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/108254

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/79 (2013.01) i; H04L 9/08 (2006.01) 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)

G06F; H04L

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)

CNPAT; EPODOC; WPI; GOOGLE; IEEE; CNKI: 可信, 安全, 属主, 数据, 长度, 地址, 范围, 非易失, 不易失, 不挥发, 非挥发, 存储块, 存储模块, 存储装置, 存储空间, 存储区域, 存储器, 请求, 访问, 超出, 超过, 大于, 密钥, 口令, 密码, 保密, trusted, TPM, TCG, firmware, data, length, range, address, NVM, nonvolatile, memory, non-volatile, store, access+, compar+, key, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 1183198 A (SCIENTIFIC-ATLANTA, INC.), 27 May 1998 (27.05.1998), the abstract, description, page 3, paragraph 5, page 14, paragraph 4 and page 15, paragraph 6 to page 17, paragraph 1, and figures 3-6	1-14
A	US 2016028546 A1 (INTEL CORPORATION), 28 January 2016 (28.01.2016), entire document	1-14
A	US 2013010519 A1 (MICRON TECHNOLOGY, INC.), 10 January 2013 (10.01.2013), entire document	1-14
A	US 2016246964 A1 (DELL PRODUCTS, LP), 25 August 2016 (25.08.2016), entire document	1-14
A	CN 104951405 A (SAMSUNG ELECTRONICS CO., LTD.), 30 September 2015 (30.09.2015), entire document	1-14
A	CN 101986325 A (SHANDONG CHAOYUE NUMERICAL CONTROL ELECTRONIC CO., LTD.), 16 March 2011 (16.03.2011), entire document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 16 January 2018	Date of mailing of the international search report 01 February 2018
Name and mailing address of the ISA 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 OU, Xiaodan Telephone No. (86-10) 53961416

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/108254

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1183198 A	27 May 1998	AU 5432496 A	23 October 1996
		DE 69637517 D1	19 June 2008
		TW 308771 B	21 June 1997
		US 5742677 A	21 April 1998
		EP 0819357 A1	21 January 1998
		WO 9631982 A1	10 October 1996
US 2016028546 A1	28 January 2016	US 9628277 B2	18 April 2017
		US 2014095886 A1	03 April 2014
		US 9152793 B2	06 October 2015
US 2013010519 A1	10 January 2013	TW 200928750 A	01 July 2009
		US 2015280912 A1	01 October 2015
		US 2009121028 A1	14 May 2009
		US 8746578 B2	10 June 2014
		US 8286883 B2	16 October 2012
		US 9088418 B2	21 July 2015
		US 2014229745 A1	14 August 2014
		WO 2009064634 A2	22 May 2009
		EP 2229653 A2	22 September 2010
US 2016246964 A1	25 August 2016	None	
CN 104951405 A	30 September 2015	US 2015278118 A1	01 October 2015
		JP 2015191670 A	02 November 2015
		KR 20150114363 A	12 October 2015
		DE 102015205396 A1	15 October 2015
CN 101986325 A	16 March 2011	None	

国际检索报告

国际申请号

PCT/CN2017/108254

A. 主题的分类 G06F 21/79(2013.01)i; H04L 9/08(2006.01)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) G06F;H04L 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)) CNPAT;EPDOC;WPI;GOOGLE;IEEE;CNKI:可信, 安全, 属主, 数据, 长度, 地址, 范围, 非易失, 不易失, 不挥发, 非挥发, 存储块, 存储模块, 存储装置, 存储空间, 存储区域, 存储器, 请求, 访问, 超出, 超过, 大于, 密钥, 口令, 密码, 保密, trusted, TPM, TCG, firmware, data, length, range, address, NVM, nonvolatile, memory, non-volatile, store, access+, compar+, key, encrypt		
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 1183198 A (亚特兰大科技公司) 1998年 5月 27日 (1998 - 05 - 27) 摘要, 说明书第3页第5段、第14页第4段、第15页第6段-第17页第1段, 图3-6	1-14
A	US 2016028546 A1 (INTEL CORPORATION) 2016年 1月 28日 (2016 - 01 - 28) 全文	1-14
A	US 2013010519 A1 (MICRON TECHNOLOGY, INC.) 2013年 1月 10日 (2013 - 01 - 10) 全文	1-14
A	US 2016246964 A1 (DELL PRODUCTS, LP) 2016年 8月 25日 (2016 - 08 - 25) 全文	1-14
A	CN 104951405 A (三星电子株式会社) 2015年 9月 30日 (2015 - 09 - 30) 全文	1-14
A	CN 101986325 A (山东超越数控电子有限公司) 2011年 3月 16日 (2011 - 03 - 16) 全文	1-14
☐ 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
2018年 1月 16日		2018年 2月 1日
ISA/CN的名称和邮寄地址		受权官员
中华人民共和国国家知识产权局(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		欧晓丹 电话号码 (86-10)53961416

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/108254

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	1183198	A	1998年 5月 27日	AU	5432496	A	1996年 10月 23日
				DE	69637517	D1	2008年 6月 19日
				TW	308771	B	1997年 6月 21日
				US	5742677	A	1998年 4月 21日
				EP	0819357	A1	1998年 1月 21日
				WO	9631982	A1	1996年 10月 10日
US	2016028546	A1	2016年 1月 28日	US	9628277	B2	2017年 4月 18日
				US	2014095886	A1	2014年 4月 3日
				US	9152793	B2	2015年 10月 6日
US	2013010519	A1	2013年 1月 10日	TW	200928750	A	2009年 7月 1日
				US	2015280912	A1	2015年 10月 1日
				US	2009121028	A1	2009年 5月 14日
				US	8746578	B2	2014年 6月 10日
				US	8286883	B2	2012年 10月 16日
				US	9088418	B2	2015年 7月 21日
				US	2014229745	A1	2014年 8月 14日
				WO	2009064634	A2	2009年 5月 22日
				EP	2229653	A2	2010年 9月 22日
US	2016246964	A1	2016年 8月 25日	无			
CN	104951405	A	2015年 9月 30日	US	2015278118	A1	2015年 10月 1日
				JP	2015191670	A	2015年 11月 2日
				KR	20150114363	A	2015年 10月 12日
				DE	102015205396	A1	2015年 10月 15日
CN	101986325	A	2011年 3月 16日	无			