(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
2019 年 2 月 14 日 (14.02.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/029393 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2018/097717

(22) 国际申请日: 2018 年 7 月 30 日 (30.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710671465.3 2017年8月8日 (08.08.2017) CN

(71) 申请人: 杭州中天微系统有限公司 (C-SKY MICROSYSTEMS CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼, Zhejiang 310012 (CN)。

(72) 发明人: 杨军 (YANG, Jun); 中国浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼, Zhejiang 310012 (CN)。 王洁 (WANG, Jie); 中国浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼, Zhejiang 310012 (CN)。

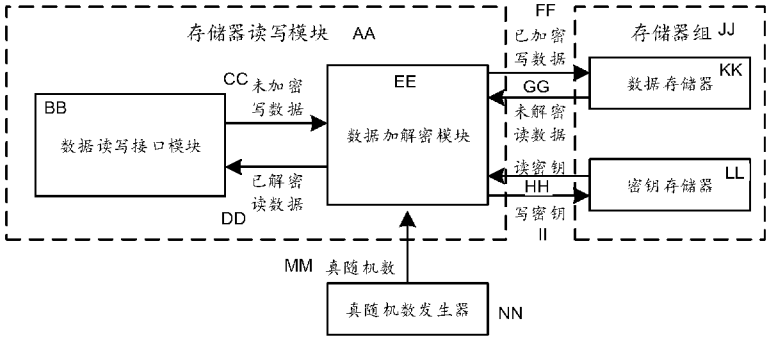
(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街35号国际企业大厦A座16层, Beijing 100033 (CN)。

(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,

WO 2019/029393 A1

(54) **Title:** STORAGE DATA ENCRYPTION AND DECRYPTION DEVICE AND METHOD

(54) **发明名称:** 一种存储数据加解密装置及方法



AA Memory read-write module
BB Data read-write interface module
CC Unencrypted write data
DD Decrypted read data
EE Data encryption and decryption module
FF Encrypted write data
GG Undecrypted read data
HH Read key
II Write key
JJ Memory bank
KK Data memory
LL Secrete key memory
MM True random number
NN True random number generator

图 1

(57) **Abstract:** Provided in the present invention is a storage data encryption and decryption method, comprising: step 1: providing a true random number generator used for generating a plurality of secret keys; step 2: providing a data memory used for storing data and a secret key memory used for storing the secret keys, and writing the secret keys into the secret key memory; and step 3: providing a data read-write interface module used for reading and writing data, and providing a data encryption and decryption module used for reading the secret keys and carrying out an encryption and decryption operation, wherein the data encryption and decryption module encrypts

[见续页]

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))。

data written in from the data read-write interface module and then writes the data into the data memory, and the data encryption and decryption module decrypts data read from the data memory and then reads the data into the data read-write interface module. Also provided in the present invention is a storage data encryption and decryption device. The present invention may effectively enhance the security of data.

(57) 摘要：本发明提供一种存储数据加解密方法，其中包括：步骤一、提供真随机数发生器，用于产生多个密钥；步骤二、提供用于存储数据的数据存储器以及用于存储密钥的密钥存储器，将密钥写入密钥存储器；步骤三、提供用于数据读写的数据读写接口模块，提供用于读取密钥并进行加解密操作的数据加解密模块；从数据读写接口模块写入的数据由数据加解密模块进行加密后写入到数据存储器，从数据存储器读出的数据由数据加解密模块进行解密后读出到数据读写接口模块。本发明还提供一种存储数据加解密装置。本发明能够有效增强数据的安全性。

一种存储数据加解密装置及方法

技术领域

本发明涉及计算机设备科学技术领域，尤其涉及一种存储数据加解密装置及方法。

背景技术

伴随全球信息化步伐的加快，网络和移动互联网设备已经与人们的生活紧密相连，成为现代社会中信息交换不可或缺的载体。随着移动智能设备性能的大幅提升以及高速移动互联网的覆盖范围不断扩大，移动办公和移动金融交易随之大规模展开。但是，办公数据和金融交易数据也越来越面临更多的威胁。

为了解决数据安全的问题，必须提高计算机技术、密码学理论和网络应用水平。目前，信息安全防护已经从传统的单点信息加密，发展到构建以芯片级硬件防护为基础，覆盖全网络系统的信息保障体系。并且，低成本、小体积、高性能、抗破解并且具备信息安全保护机制的芯片化设计已经成为必然趋势，由此，片上系统（SoC, System on Chip）芯片设计逐渐成为嵌入式系统发展的新方向，芯片设计者通常在一个 SoC 芯片中集成加解密算法与信息安全协议，并且保证足够的安全等级。但是，现有技术中的 SoC 芯片集成加解密算法对不同芯片或者同一芯片的不同存储区域采用相同密钥进行加解密，不能够有效地进行数据保护。

因此，亟需设计一种存储数据加解密装置及方法，能够对不同芯片以及同一芯片不同存储区域中的数据采用不同密钥进行加解密，并且更有效地完成数据存储和读写操作。

发明内容

本发明提供的存储数据加解密装置和方法，能够针对现有技术的不足，对不同芯片以及同一芯片不同存储区域中的数据采用不同密钥进行加解密，高效完成数据存储和读写操作。

第一方面，本发明提供一种存储数据加解密方法，其中，包括：

步骤一、提供真随机数发生器，用于产生多个密钥；

步骤二、提供用于存储数据的数据存储器以及用于存储密钥的密钥存储器，将所述密钥写入所述密钥存储器；

步骤三、提供用于数据读写的数据读写接口模块，提供用于读取所述密钥并进行加

解密操作的数据加解密模块；

从所述数据读写接口模块写入的数据由所述数据加解密模块进行加密后写入到所述数据存储器，从所述数据存储器读出的数据由所述数据加解密模块进行解密后读出到所述数据读写接口模块。

可选地，上述步骤三还包括对是否分隔所述数据存储器中的数据进行判断：

如果判断是，将所述数据存储器划分为逻辑多个数据存储区域，对所述多个数据存储区域的数据选择性进行加解密操作；

如果判断否，对所述数据存储器不划分数据存储区域，对整块数据存储区域的数据进行加解密操作。

可选地，对上述多个数据存储区域的数据选择性进行加解密操作所使用的每个数据存储区域的密钥均不相同；对所述整块数据存储区域的数据进行加解密操作使用统一密钥。

可选地，对不同芯片的所述多个数据存储区域中的相同数据存储区域进行加解密操作所使用的密钥均不相同；对不同芯片的所述的整块数据存储区域的数据进行加解密操作所使用的密钥均不相同。

可选地，上述数据加解密模块使用的加解密算法在单周期内完成。

可选地，上述数据加解密模块使用的加解密算法包括异或、序列重排。

可选地，上述数据加解密模块在系统芯片启动时自动通过硬件获取所述密钥存储器中的密钥。

可选地，上述数据存储器和所述密钥存储器位于同一物理介质上。

可选地，上述方法还包括在系统受到攻击时，所述密钥存储器中存储的密钥可以被清除。

再一方面，本发明提供一种使用上述方法的存储数据加解密的装置，其中包括：

真随机数发生器，用于产生多个密钥；

存储器组，所述存储器组包括用于存储数据的数据存储器和用于存储所述多个密钥的密钥存储器；

存储器读写模块，所述存储器读写模块包括用于数据读写的数据读写接口模块和用于读取所述多个密钥并对数据进行加解密操作的数据加解密模块。

本发明实施例提供的存储数据加解密装置及方法，能够在一个时钟周期内完成对不同芯片或同一芯片不同存储区域中的数据的加密，安全高效地完成数据存储和读写操作。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

图1为本发明一实施例的存储数据加解密装置结构示意图；

图2为本发明一实施例的存储数据加解密流程图；

图 3 为本发明一实施例的存储数据加解密方法的步骤示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，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，都属于本发明保护的范围。

本发明提供一种存储数据加解密装置，图1示出了本发明一实施例的存储数据加解密装置结构示意图。如图所示，所述存储数据加解密装置包括存储器模块、存储器组、真随机数发生器。具体的，所述存储器模块用于支持数据和密钥读写以及对经过该模块的数据进行加解密操作，所述存储器组用于支持数据和密钥存储功能，所述真随机数发生器用于生成密钥。

存储器读写模块负责将写数据加密后写入到存储器组，以及将从存储器组读取的读数据解密。存储器读写模块由一个数据读写接口模块和一个数据加解密模块组成。其中，数据读写接口模块用于对数据进行读写；数据加解密模块则用于对数据进行加密和解密。

具体地，数据读写接口模块输出未加密写数据到数据加解密模块，并且从数据加解密模块输入已解密读数据。

特别的，数据加解密模块可以使用单周期加解密算法，这种单周期加解密算法可以但不仅限于异或、序列重排等，采用这种加解密算法的数据加解密模块不影响数据访问效率。

存储器组由数据存储器和密钥存储器组成。其中，数据存储器用于存储数据，密钥

存储器用于存储密钥。典型的，数据存储器和密钥存储器包括但不限于部署在同一物理存储介质上，方便存储高效实现。

具体的，数据存储器中的数据可以被分割为多个数据存储区域，不同存储区域可以采用不同的密钥进行加解密，各存储区域也可以分别选择是否进行加解密，但是相同的存储区域的数据只能使用同一个密钥进行加解密。另外，不同芯片相同数据存储区域采用的密钥也不相同；对不同芯片的所述的整块数据存储区域的数据进行加解密操作所使用的密钥均不相同。密钥存储器中存储多个密钥，分别用于对特定数据存储区域的数据进行加解密操作。

真随机数发生器负责生成密钥，用于提供给数据加解密模块并对数据进行加解密操作。

具体的，存储器读写模块中的数据加解密模块将真随机数发生器生成的真随机数作为密钥输出到存储器组的密钥存储器中，并采用密钥存储器中的密钥对输出到数据存储器中的写数据进行加密，对输入的读数据进行解密。

特别的，数据加解密模块在芯片启动时自动获取存储器组的密钥存储器中的密钥，并对所有经过存储器读写模块的数据使用获取到的密钥进行加解密，密钥获取方式由硬件实现，软件透明。

特别的，存储器读写模块需在数据加解密模块完成密钥获取之后被访问，提前访问请求无法响应。

图 2 示出了本发明一实施例的存储数据加解密流程图。如图所示，系统启动，真随机数发生器产生多个密钥，随后，数据加解密模块将真随机数发生器生成的密钥写入到密钥存储器。对是否分隔数据存储器中的数据进行判断，如果判断是，则在逻辑上将数据存储器划分为多个数据存储区域，对各数据存储区域的数据选择性进行加解密，并采用不同的密钥；如果判断否，则对数据存储器不划分数据存储区域，而采用统一的密钥对整块数据存储区域进行数据加解密。随后，对经过存储区读写模块的数据进行加解密，在本发明的一个实施例中，数据读写接口模块向数据加解密模块传送未加密的写数据，数据加解密模块对数据进行加密后存储与数据存储器，反之，数据存储器向数据加解密模块传送未解密读数据，经过数据加解密模块解密后，向数据读写接口模块传送已解密读数据。随后，判断系统是否受到攻击，如果系统受到攻击，则由数据加解密模块清除密钥存储器中的密钥，从而避免存储器中的数据被攻击获取；如果系统未受到攻击，继续判断系统是否关闭，如果判断是，则启动系统；如果判断否，则继续对经过存储器读

写模块的数据进行加解密。

图 3 示出了本发明一个实施例的存储数据加解密方法步骤示意图。如图所示，S31 提供真随机数发生器，用于产生多个密钥；S32 表示提供用于存储数据的数据存储器以及用于存储密钥的密钥存储器，将密钥写入密钥存储器；S33 表示提供用于数据读写的数据读写接口模块，提供用于读取密钥并进行加解密操作的数据加解密模块；从数据读写接口模块写入的数据由数据加解密模块进行加密后写入到数据存储器，从数据存储器读出的数据由数据加解密模块进行解密后读出到数据读写接口模块。

本发明提供的存储数据加解密装置及方法，通过在同一个芯片中将数据存储器划分为多个存储区域，每个存储区域分别采用特定的密钥，并且在不同芯片中，相同地址的存储区域采用不同的密钥，能够保证数据安全性。另外，当系统遭受数据安全攻击时可以通过擦除密钥存储器中的密钥使存储器中的加密数据不能正确解密，具有较强的抗攻击能力，能够有效完成数据存储和读写操作。

以上所述，仅为本发明的具体实施方式，但本发明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发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

权 利 要 求 书

1、一种存储数据加解密方法，其特征在于，包括：

步骤一、提供真随机数发生器，用于产生多个密钥；

步骤二、提供用于存储数据的数据存储器以及用于存储密钥的密钥存储器，将所述密钥写入所述密钥存储器；

步骤三、提供用于数据读写的数据读写接口模块，提供用于读取所述密钥并进行加解密操作的数据加解密模块；

从所述数据读写接口模块写入的数据由所述数据加解密模块进行加密后写入到所述数据存储器，从所述数据存储器读出的数据由所述数据加解密模块进行解密后读出到所述数据读写接口模块。

2、根据权利要求 1 所述的方法，其特征在于，所述步骤三还包括对是否分隔所述数据存储器中的数据进行判断：

如果判断是，将所述数据存储器划分为逻辑多个数据存储区域，对所述多个数据存储区域的数据选择性进行加解密操作；

如果判断否，对所述数据存储器不划分数据存储区域，对整块数据存储区域的数据进行加解密操作。

3、根据权利要求 2 所述的方法，其特征在于，对所述多个数据存储区域的数据选择性进行加解密操作所使用的每个数据存储区域的密钥均不相同；对所述整块数据存储区域的数据进行加解密操作使用统一密钥。

4、根据权利要求 3 所述的方法，其特征在于，对不同芯片的所述多个数据存储区域中的相同数据存储区域进行加解密操作所使用的密钥均不相同；对不同芯片的所述的整块数据存储区域的数据进行加解密操作所使用的密钥均不相同。

5、根据权利要求 1 所述的方法，其特征在于，所述数据加解密模块使用的加解密算法在单周期内完成。

6、根据权利要求 5 所述的方法，其特征在于，所述数据加解密模块使用的加解密算法包括异或、序列重排。

7、根据权利要求 1 所述的方法，其特征在于，所述数据加解密模块在系统芯片启动时自动通过硬件获取所述密钥存储器中的密钥。

8、根据权利要求 1 所述的方法，其特征在于，所述数据存储器和所述密钥存储器位于同一物理介质上。

9、根据权利要求 1 所述的方法，其特征在于，所述方法还包括在系统受到攻击时，所述密钥存储器中存储的密钥可以被清除。

10、一种使用权利要求 1 所述方法的装置，其特征在于，包括：

真随机数发生器，用于产生多个密钥；

存储器组，所述存储器组包括用于存储数据的数据存储器和用于存储所述多个密钥的密钥存储器；

存储器读写模块，所述存储器读写模块包括用于数据读写的数据读写接口模块和用于读取所述多个密钥并对数据进行加解密操作的数据加解密模块。

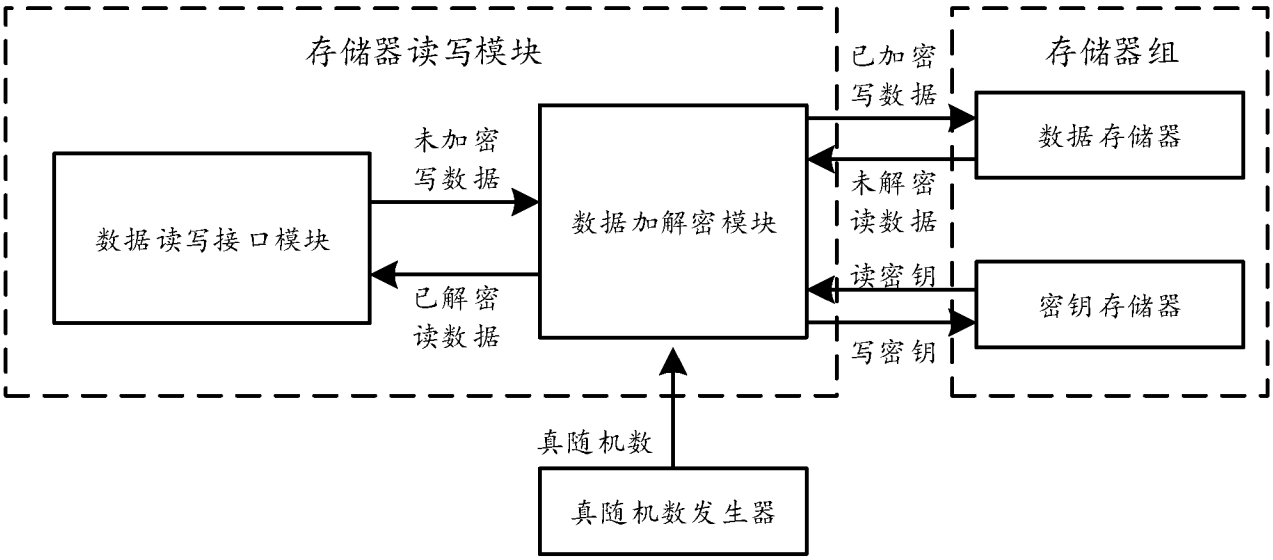

存储器读写模块
存储器组
已加密
写数据
数据存储器
未加密
写数据
数据读写接口模块
数据加解密模块
未解密
读数据
读密钥
密钥存储器
已解密
读数据
写密钥
真随机数
真随机数发生器

图 1

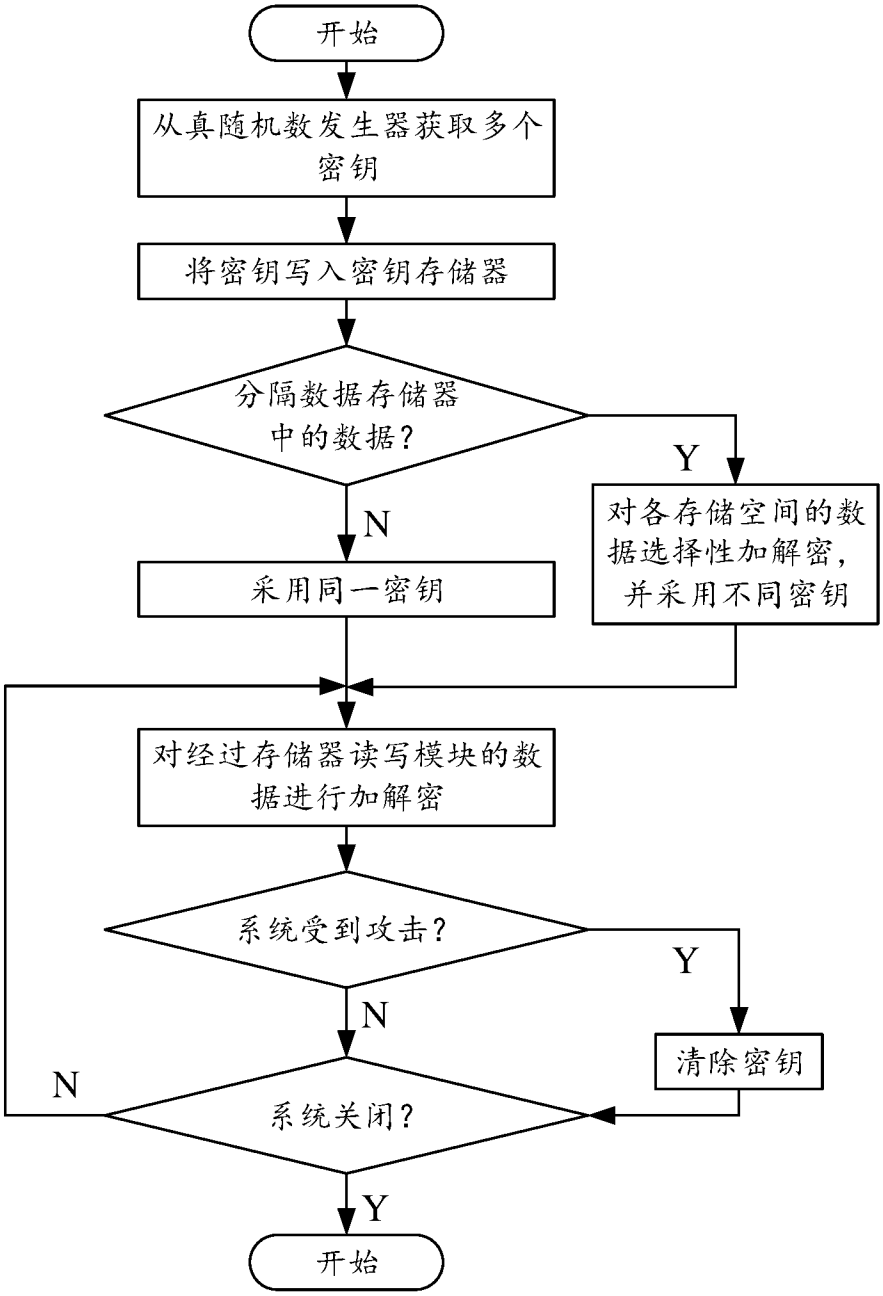

开始
从真随机数发生器获取多个密钥
将密钥写入密钥存储器
分隔数据存储器中的数据？
Y
对各存储空间的数据选择性加解密，并采用不同密钥
N
采用同一密钥
对经过存储器读写模块的数据进行加解密
系统受到攻击？
Y
清除密钥
N
N
系统关闭？
Y
开始

图 2

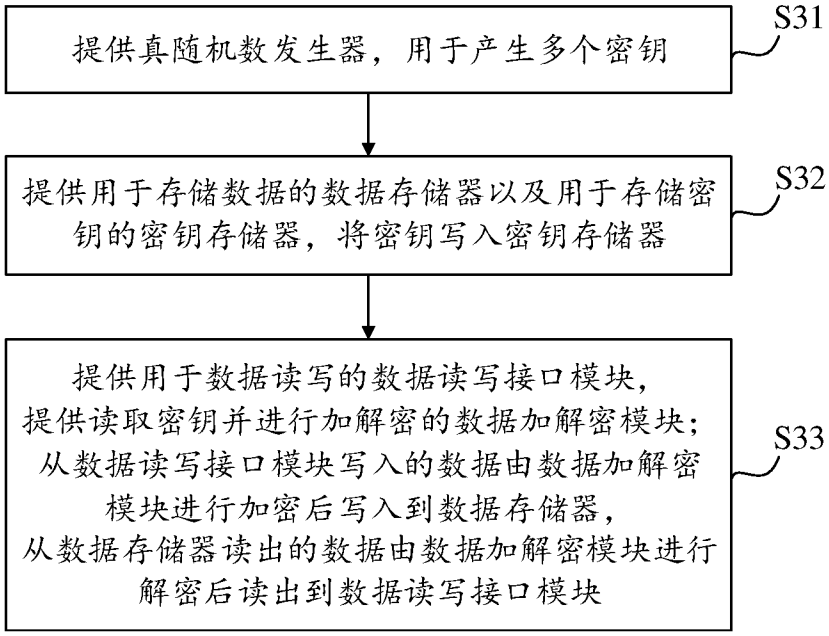

提供真随机数发生器，用于产生多个密钥
S31
提供用于存储数据的数据存储器以及用于存储密钥的密钥存储器，将密钥写入密钥存储器
S32
提供用于数据读写的数据读写接口模块，
提供读取密钥并进行加解密的数据加解密模块；
从数据读写接口模块写入的数据由数据加解密模块进行加密后写入到数据存储器，
从数据存储器读出的数据由数据加解密模块进行解密后读出到数据读写接口模块
S33

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/097717

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(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)

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)

CNABS: 加密, 数据, 芯片, 真随机, 解密, 存储, 随机, encryption, data, chip, true random, decryption, storage, store, random

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 201054140 Y (BEIJING HENGTAI TECHNOLOGIES CO., LTD.) 30 April 2008 (2008-04-30) claims 1 and 4	1-10
X	CN 104918243 A (SHANGHAI JIAO TONG UNIVERSITY) 16 September 2015 (2015-09-16) claims 1 and 5	1-10
PX	CN 107516047 A (C-SKY MICROSYSTEMS CO., LTD.) 26 December 2017 (2017-12-26) entire document	1-10

☐ 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
24 October 2018	**31 October 2018**
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/CN2018/097717

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 201054140 Y	30 April 2008	None	
CN 104918243 A	16 September 2015	CN 104918243 B	10 April 2018
CN 107516047 A	26 December 2017	None	

国际检索报告

国际申请号
PCT/CN2018/097717

A. 主题的分类

G06F 21/60(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)

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））

CNABS:加密，数据，芯片，真随机，解密，存储，随机,encryption, data, chip,true random,decryption, storage,store, random

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
X	CN 201054140 Y (北京华大恒泰科技有限责任公司) 2008年 4月 30日 (2008-04-30) 权利要求1,4	1-10
X	CN 104918243 A (上海交通大学) 2015年 9月 16日 (2015-09-16) 权利要求1,5	1-10
PX	CN 107516047 A (杭州中天微系统有限公司) 2017年 12月 26日 (2017-12-26) 全文	1-10

☐ 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 10月 24日	2018年 10月 31日
ISA/CN的名称和邮寄地址 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	受权官员 王丹 电话号码 62412062

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/097717

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 201054140 Y	2008年 4月 30日	无	
CN 104918243 A	2015年 9月 16日	CN 104918243 B	2018年 4月 10日
CN 107516047 A	2017年 12月 26日	无	