



(12)发明专利申请

(10)申请公布号 CN 110298181 A

(43)申请公布日 2019.10.01

(21)申请号 201910398621.2

(22)申请日 2019.05.14

(71)申请人 北京航空航天大学

地址 100191 北京市海淀区学院路37号

(72)发明人 康旺 张留洋 赵巍胜

(74)专利代理机构 北京三友知识产权代理有限公司 11127

代理人 王涛 任默闻

(51)Int.Cl.

G06F 21/60(2013.01)

G06F 21/78(2013.01)

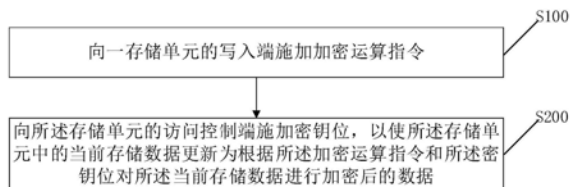
权利要求书1页 说明书8页 附图5页

(54)发明名称

数据加密存储方法、数据解密方法以及加密存储器芯片

(57)摘要

本发明提供的数据加密存储方法、数据解密方法以及加密存储器芯片,通过向一存储单元的写入端施加加密/解密运算指令;向该存储单元的访问控制端施加密钥位,以使该存储单元中的当前存储数据更新为根据该加密/解密运算指令和该密钥位对该当前存储数据进行加密/解密后的数据,基于存内计算原理直接利用非易失性存储器的存储单元对数据进行加密存储,通过正常的数据读写过程即可实现,不需要额外的加解密模块,进而减小存储器的面积,适应小型化集成化的需求。



1. 一种数据加密存储方法,其特征在于,包括:
向一存储单元的写入端施加加密运算指令;
向所述存储单元的访问控制端施加加密密钥,以使所述存储单元中的当前存储数据更新为根据所述加密运算指令和所述密钥位对所述当前存储数据进行加密后的数据。
2. 根据权利要求1所述的数据加密存储方法,其特征在于,还包括:
将待加密数据按位写入至少一个存储单元中,所述存储单元的个数等于所述待加密数据的位数。
3. 根据权利要求1所述的数据加密存储方法,其特征在于,还包括:
根据加密算法获取各存储单元的加密运算指令。
4. 根据权利要求1所述的数据加密存储方法,其特征在于,还包括:
根据密钥获取各存储单元的密钥位。
5. 根据权利要求1至4任一项所述的数据加密存储方法,其特征在于,所述写入端为存储单元的位线,所述访问控制端为存储单元的字线。
6. 根据权利要求2所述的数据加密存储方法,其特征在于,在所述将待加密数据按位写入至少一个存储单元中之前,还包括:
对欲写入待加密数据的存储单元进行初始化。
7. 根据权利要求1所述的数据加密存储方法,其特征在于,所述根据所述加密运算指令和所述密钥位对所述当前存储数据进行加密后的数据 B_{i+1} :

$$B_{i+1} = AC + \bar{A}B_i,$$

其中,A表示密钥位,C表示加密运算指令, B_i 表示当前存储数据。

8. 一种数据解密方法,其特征在于,包括:
向一存储单元的写入端施加解密运算指令;
向所述存储单元的访问控制端施加加密密钥,以使所述存储单元中的当前存储数据更新为根据所述解密运算指令和所述密钥位对所述当前存储数据进行解密后的数据。
9. 根据权利要求8所述的数据解密方法,其特征在于,还包括:
根据解密算法获取各存储单元的解密运算指令。
10. 根据权利要求8所述的数据解密方法,其特征在于,还包括:
根据密钥获取各存储单元的密钥位。
11. 根据权利要求8至10任一项所述的数据解密方法,其特征在于,所述写入端为存储单元的位线,所述访问控制端为存储单元的字线。
12. 根据权利要求11所述的数据解密方法,其特征在于,所述根据所述解密运算指令和所述密钥位对所述当前存储数据进行解密后的数据 B'_{i+1} :

$$B'_{i+1} = A'C' + \bar{A}B'_i,$$

其中, A' 表示密钥位, C' 表示解密运算指令, B'_i 表示当前存储数据。

13. 一种加密存储器芯片,其特征在于,包括:存储单元阵列、写入电路、行列译码器,所述加密存储器芯片应用如权利要求1至7任一项所述的数据加密存储方法的步骤对数据进行加密存储或应用如权利要求8至12任一项所述的数据解密方法的步骤进行数据解密。

数据加密存储方法、数据解密方法以及加密存储器芯片

技术领域

[0001] 本发明涉及数据存储技术领域,尤其涉及一种数据加密存储方法、数据解密方法以及加密存储器芯片。

背景技术

[0002] 存储器(Memory)是现代信息技术中用于保存信息的记忆设备,其主要功能是存储程序和各种数据。其中,为了保障数据存储安全性,需要对存储的数据进行加密。

[0003] 对于目前的存储器,如果需要对数据进行加密存储,通常需要特定的加解密模块,以对待存数据进行加密后存储,在数据读出时,通过解密模块进行解密后再进行后续应用,如图1所示,当输入数据(即:待存数据,也可称为明文)需要加密存储在存储器中时,首先,通过加密模块根据特定的加密算法与密钥对输入数据进行加密,然后把加密后的数据(通常称密文)再存储到存储器当中;当读取数据时,被加密的数据被解密模块根据特定的解密算法与密钥进行解密,恢复出原文再输出。

[0004] 现有数据加密存储方法和解密方法由于需要设置加密模块和解密模块或加解密一体模块对数据进行加密和解密,加密模块和解密模块增加了存储器的面积,不能适应小型化集成化的需求。

发明内容

[0005] 有鉴于此,本发明提供一种数据加密存储方法、数据解密方法以及加密存储器芯片,用于非易失性存储存储器,基于存内计算原理直接利用非易失性存储器的存储单元对数据进行加密存储,不需要额外的加解密模块,进而减小存储器的面积,适应小型化集成化的需求。

[0006] 为了实现上述目的,本发明采用如下技术方案:

[0007] 第一方面,提供一种数据加密存储方法,包括:

[0008] 向一存储单元的写入端施加加密运算指令;

[0009] 向该存储单元的访问控制端施加密钥位,以使该存储单元中的当前存储数据更新为根据该加密运算指令和该密钥位对该当前存储数据进行加密后的数据。

[0010] 进一步地,还包括:

[0011] 将待加密数据按位写入至少一个存储单元中,该存储单元的个数等于该待加密数据的位数。

[0012] 进一步地,还包括:

[0013] 根据加密算法获取各存储单元的加密运算指令。

[0014] 进一步地,还包括:

[0015] 根据密钥获取各存储单元的密钥位。

[0016] 进一步地,该写入端为存储单元的位线,该访问控制端为存储单元的字线。

[0017] 进一步地,在该将待加密数据按位写入至少一个存储单元中之前,还包括:

[0018] 对欲写入待加密数据的存储单元进行初始化。

[0019] 进一步地,该根据该加密运算指令和该密钥位对该当前存储数据进行加密后的数据 B_{i+1} :

$$[0020] \quad B_{i+1} = AC + \bar{A}B_i,$$

[0021] 其中,A表示密钥位,C表示加密运算指令, B_i 表示当前存储数据。

[0022] 第二方面,提供一种数据解密方法,包括:

[0023] 向一存储单元的写入端施加解密运算指令;

[0024] 向该存储单元的访问控制端施加密钥位,以使该存储单元中的当前存储数据更新为根据该解密运算指令和该密钥位对该当前存储数据进行解密后的数据。

[0025] 进一步地,还包括:

[0026] 根据解密算法获取各存储单元的解密运算指令。

[0027] 进一步地,还包括:

[0028] 根据密钥获取各存储单元的密钥位。

[0029] 进一步地,该写入端为存储单元的位线,该访问控制端为存储单元的字线。

[0030] 进一步地,该根据该解密运算指令和该密钥位对该当前存储数据进行解密后的数据 B'_{i+1} :

$$[0031] \quad B'_{i+1} = A'C' + \bar{A}'B'_i,$$

[0032] 其中, A' 表示密钥位, C' 表示解密运算指令, B'_i 表示当前存储数据。

[0033] 第三方面,提供一种加密存储器芯片,包括:存储单元阵列、写入电路、行列译码器,所述加密存储器芯片应用上述的数据加密存储方法的步骤对数据进行加密存储或应用上述的数据解密方法的步骤进行数据解密。

[0034] 本发明提供的数据加密存储方法、数据解密方法以及加密存储器芯片,通过向一存储单元的写入端施加加密/解密运算指令;向该存储单元的访问控制端施加密钥位,以使该存储单元中的当前存储数据更新为根据该加密/解密运算指令和该密钥位对该当前存储数据进行加密/解密后的数据,基于存内计算原理直接利用非易失性存储器的存储单元对数据进行加密存储,通过正常的读写过程即可实现,不需要额外的加解密模块,进而减小存储器的面积,适应小型化集成化的需求。

[0035] 另外,由于摒弃了现有技术中的加解密算法的运算过程,采用边存储边加密的方式对数据进行加密存储,或者,采用边读取边解密的方式对数据进行解密,进而能够降低数据访存的时延,提高了数据加密存储速度。

[0036] 再者,本发明实施例利用存内计算原理对数据进行加解密,加密过程灵活,更改方便。

[0037] 为了让本发明的上述和其他目的、特征和优点能更明显易懂,下文特举较佳实施例,并配合所附图式,作详细说明如下。

附图说明

[0038] 为了更清楚地说明本申请实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图是本申请

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他的附图。在附图中:

[0039] 图1为示出了现有加密存储架构;

[0040] 图2为应用本发明实施例提供的数据加密存储方法或数据解密方法的存储器的电路示意图;

[0041] 图3为应用本发明实施例提供的数据加密存储方法或数据解密方法的存储器的存储单元结构示意图;

[0042] 图4示出了本发明实施例数据加密存储方法的流程图一;

[0043] 图5示出了采用本发明实施例提供的数据加密存储方法利用存储单元对数据进行加密存储的计算原理;

[0044] 图6示出了本发明实施例数据加密存储方法的流程图二;

[0045] 图7示出了采用本发明实施例提供的数据加密存储方法利用存储单元对数据进行加密存储的真值表;

[0046] 图8示出了本发明实施例数据解密方法的流程图。

具体实施方式

[0047] 为了使本技术领域的人员更好地理解本申请方案,下面将结合本申请实施例中的附图,对本申请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申请一部分的实施例,而不是全部的实施例。基于本申请中的实施例,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,都应当属于本申请保护的范围。

[0048] 需要说明的是,本申请的说明书和权利要求书及上述附图中的术语“包括”和“具有”以及他们的任何变形,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。

[0049] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0050] 现有数据加密存储方法和解密方法由于需要设置加密模块和解密模块或加解密一体模块对数据进行加密和解密,加密模块和解密模块增加了存储器的面积,不能适应小型化集成化的需求。

[0051] 为解决现有技术中存在上述技术问题,本发明实施例提供一种数据加密存储方法和数据解密方法,通过向一存储单元的写入端施加加密/解密运算指令;向该存储单元的访问控制端施加密钥位,以使该存储单元中的当前存储数据更新为根据该加密/解密运算指令和该密钥位对该当前存储数据进行加密/解密后的数据,基于存内计算原理直接利用非易失性存储器的存储单元对数据进行加密存储,通过正常的数据读写过程即可实现,不需要额外的加解密模块,进而减小存储器的面积,适应小型化集成化的需求。

[0052] 值得说明的是,为解决现有技术中存在的上述技术问题,发明人在对现有非易失性存储器的存储原理和工作流程进行了深入地分析和研究后,通过大量的推理验证,发现了利用非易失性存储器的存储单元能够实现逻辑计算的特性能够进行数据加密

存储和数据解密,以解决现有技术中存在的技术问题。

[0053] 图2为应用本发明实施例提供的数据加密存储方法或数据解密方法的存储器的电路示意图。参见图2,对于新型非易失性存储器,例如阻变存储器(ReRAM)、自旋转移矩磁性随机存储器(STT-MRAM)、相变存储器(PCRAM)等,包括多个闪存单元,典型存储单元由一个用于对存储单元进行访问控制的晶体管(记为T)和一个用于存储二进制数据的非易失性存储器件(记为R)组成,称为1T1R存储单元(如图3所示),多个存储单元通过字线、位线、源线以阵列形式组织在一起。

[0054] 另外,该非易失性存储器件还有配套的行译码器、列译码器、写入电路、读取电路以及控制器等。

[0055] 该控制器可以通过控制行译码器、列译码器、写入电路以及读取电路,来实现本发明实施例提供的数据加密存储方法和数据解密方法。

[0056] 其中,非易失性存储器件的阻值可以有两种状态,一种为高阻状态,一种为低阻状态,分别代表数据比特“0”和“1”,或者反之。晶体管的栅极接字线,漏极经非易失性存储器件后接位线,源极接源线,源线一般接地。通过控制字线的电压即可控制晶体管的开闭,从而控制存储单元的选择与否。更具体地,当字线为高电平时,晶体管处于导通状态,存储单元可访问,可对其进行读写操作;而当字线为低电平时,晶体管处于非导通状态,存储单元不可访问。

[0057] 对于1T1R存储单元,通常需要施加两个信号:(1)访问控制信号(通常从字线施加),用于对存储单元进行访问控制;(2)写入信号(通常从位线施加,可以是电流或电压)。

[0058] 图4示出了本发明实施例数据加密存储方法的流程图一。如图4所示,该数据加密存储方法可以包括以下内容:

[0059] 步骤S100:向一存储单元的写入端施加加密运算指令。

[0060] 其中,该存储单元为待加密的存储单元,该存储单元中可以存储待加密的数据中的一个二进制位,也可以存储经过加密后的一个二进制位,针对第一种情况,实现待加密数据的第一次加密,针对第二种情况,实现加密后的数据的再次加密(即多重加密)。本领域技术人员可以理解的是,通过多重加密技术,能够实现更复杂的加密,能够进一步提高数据存储安全性。

[0061] 另外,存储单元中存储的数据为一个二进制数的一个二进制位。

[0062] 再者,该写入端可为存储单元的位线。

[0063] 值得说明的是,该加密运算指令可以看做逻辑功能选择信号,决定了逻辑计算的功能函数,可为数据比特“0”或“1”。

[0064] 步骤S200:向所述存储单元的访问控制端施加密钥位,以使所述存储单元中的当前存储数据更新为根据所述加密运算指令和所述密钥位对所述当前存储数据进行加密后的数据。

[0065] 其中,该访问控制端可为存储单元的字线。

[0066] 另外,该密钥位是指密钥中对应该存储单元的一位数据,可为数据比特“0”或“1”。

[0067] 值得说明的是,在实际应用中,一般是对一个由多个二进制位组成的二进制数进行加密,此时,该二进制数的多个二进制位分别存储在对应的多个存储单元中。密钥可为一个由多个二进制位组成的二进制数,密钥中的二进制位称为密钥位,密钥的长度可与待加

密数据的长度相同,也可以小于待加密数据的长度。当密钥的长度小于待加密数据的长度时,可通过利用一定的扩展规则扩展该密钥,使得扩展后的密钥的长度与待加密数据的长度相同。密钥和待加密数据的各个位一一对应,以利用密钥位对对应的待加密数据位进行加密,加密的算法由对应的加密运算指令限定。多个存储单元对应的多个加密运算指令组合形成加密算法。

[0068] 图5示出了采用本发明实施例提供的数据加密存储方法利用存储单元对数据进行加密存储的计算原理。参见图5,根据加密运算指令和密钥位对所述当前存储数据进行加密后的数据 B_{i+1} :

$$[0069] \quad B_{i+1} = AC + \bar{A}B_i,$$

[0070] 其中,A表示密钥位,C表示加密运算指令, B_i 表示当前存储数据。

[0071] 当C等于“0”、“1”或“ \bar{B}_i ”时,存储单元下一个存储的数据 B_{i+1} 分别等于 $\bar{A}B_i$ (“与”逻辑), $A+B_i$ (“或”逻辑)或 $A \oplus B_i$ (“异或”逻辑),实现了密钥位与当前存储数据的逻辑运算(即加密过程)。最终计算的结果(即 B_{i+1})直接存储在存储单元内。其逻辑计算操作与存储器的正常书写读写操作基本一致。其他逻辑计算功能可以通过如上三种逻辑功能函数进行组合而成。

[0072] 另外,本领域技术人员可以理解的是,在执行完步骤S200之后,可以返回步骤S100,改变或不改变密钥位和加密运算指令,实现多轮加密,即可实现任意复合的加密算法。

[0073] 通过上述技术方案可以得知,本发明提供的数据加密存储方法,基于存内计算原理直接利用非易失性存储器的存储单元对数据进行加密存储,通过正常的数据读写过程即可实现,不需要额外的加解密模块,进而减小存储器的面积,适应小型化集成化的需求。另外,由于摒弃了现有技术中的加解密算法的运算过程,采用边存储边加密的方式对数据进行加密存储,进而能够降低数据访存的时延,提高了数据加密存储速度。再者,本发明实施例利用存内计算原理对数据进行加解密,加密过程灵活,更改方便。

[0074] 在一个可选的实施例中,该数据加密存储方法还可以包括以下内容(参见图6):

[0075] 步骤S10:将待加密数据按位写入至少一个存储单元中,所述存储单元的个数等于所述待加密数据的位数。

[0076] 其中,当对一待加密数据进行第一轮加密之前,需要将该待加密数据按位写入至少一个存储单元中。

[0077] 在一个可选的实施例中,在将待加密数据按位写入至少一个存储单元中之前,还可以对欲写入待加密数据的存储单元进行初始化。

[0078] 在一个可选的实施例中,该数据加密存储方法还可以包括以下内容:

[0079] 根据加密算法获取各存储单元的加密运算指令。

[0080] 根据密钥获取各存储单元的密钥位。

[0081] 本领域技术人员可以理解的是,本发明实施例提供的数据加密存储方法,可以不需要加解密模块,也可以在现有拓扑的基础上,对经过加密模块加密后的数据利用本发明实施例提供的数据加密方法再次进行加密,由此,也能够提高数据安全性以及兼容性,适应范围广。

[0082] 下面以图7中示出的采用本发明实施例提供的数据加密存储方法利用存储单元对数据进行加密存储的真值表为例,对本发明实施例提供的数据加密存储方法进行详细说明。

[0083] 假设待加密数据为二进制数【00110011】,密钥为【01010101】,加密算法为将待加密数据的前4位与密钥的前4位相与,将待加密数据的后4位与密钥的后4位相或。

[0084] (1) 首先,将8个二进制位【0,0,1,1,0,0,1,1】分别写入8个存储单元中,作为当前表示当前存储数据B₁、B₂、B₃、B₄、B₅、B₆、B₇、B₈。

[0085] (2) 根据该密钥【01010101】获取到对应上述8个存储单元的8个密钥位【0,1,0,1,0,1,0,1】。

[0086] (3) 根据该加密算法获取到对应上述8个存储单元的8个加密运算指令【0,0,0,0,1,1,1,1】。

[0087] 其中,上述步骤1~3没有先后限制,可以按照任何顺序逐个进行,也可以2个步骤同步进行。

[0088] (4) 向8个存储单元的写入端分别施加8个加密运算指令【0,0,0,0,1,1,1,1】,同时,向8个存储单元的访问控制端分别施加8个密钥位【0,1,0,1,0,1,0,1】,由此,在8个存储单元中存储的数据将变为【0,0,1,0,0,1,1,1】。

[0089] 当然,本领域技术人员可以理解的是,在上述加密流程完成以后,还可以根据对数据存储安全性的要求,对加密后的数据采用相同或不同的密钥和加密算法再次进行加密,直至多轮加密,实现复杂的加密算法和加密机制,进一步提高数据存储的安全性。其中,对机密后的数据再次进行加密的过程参见步骤2至步骤4,在此不再赘述。

[0090] 基于同一发明构思,本申请实施例还提供了一种数据解密方法,该数据解密方法的原理与数据加密存储方法的原理相同,解密算法与加密算法匹配,解密密钥与加密密钥匹配,解密过程即为上述加密过程的逆过程,可以参见上述数据加密存储方法的实施,重复之处不再赘述。

[0091] 图8示出了本发明实施例数据解密方法的流程图,如图8所示,该数据解密方法可以包括以下内容:

[0092] 步骤S1000:向一存储单元的写入端施加解密运算指令。

[0093] 其中,该存储单元为待解密的存储单元。

[0094] 另外,存储单元中存储的数据为一个二进制数的一个二进制位。

[0095] 再者,该写入端可为存储单元的位线。

[0096] 值得说明的是,该解密运算指令可以看做逻辑功能选择信号,决定了逻辑计算的功能函数,可为数据比特“0”或“1”。另外,当加密时采用了多重加密,则解密时要需要进行多重解密。

[0097] 步骤S2000:向所述存储单元的访问控制端施加密钥位,以使所述存储单元中的当前存储数据更新为根据所述解密运算指令和所述密钥位对所述当前存储数据进行解密后的数据。

[0098] 其中,所述访问控制端为存储单元的字线。

[0099] 另外,该密钥位是指解密密钥中对应该存储单元的一位数据,可为数据比特“0”或“1”。

[0100] 值得说明的是,在实际应用中,一般是对一个由多个二进制位组成的二进制数进行解密,此时,该二进制数的多个二进制位分别存储在对应的多个存储单元中。密钥可为一个由多个二进制位组成的二进制数,密钥中的二进制位称为密钥位,密钥的长度可与待解密数据的长度相同,也可以小于待解密数据的长度。当密钥的长度小于待解密数据的长度时,可通过利用一定的扩展规则扩展该密钥,使得扩展后的密钥的长度与待解密数据的长度相同。密钥和待解密数据的各个位一一对应,以利用密钥位对对应的待解密数据位进行解密,解密的算法由对应的解密运算指令限定。多个存储单元对应的多个解密运算指令组合形成解密算法。

[0101] 通过上述技术方案可以得知,本发明提供的数据解密方法,通过正常的读写过程即可实现,不需要额外的加解密模块,进而减小存储器的面积,适应小型化集成化的需求。

[0102] 根据所述解密运算指令和所述密钥位对所述当前存储数据进行解密后的数据 B'_{i+1} :

$$[0103] \quad B'_{i+1} = A'C' + \bar{A}B'_i,$$

[0104] 其中, A' 表示密钥位, C' 表示解密运算指令, B'_i 表示当前存储数据。

[0105] 在一个可选的实施例中,该数据解密方法还可以包括以下步骤:

[0106] 根据解密算法获取各存储单元的解密运算指令。

[0107] 根据解密密钥获取各存储单元的密钥位。

[0108] 本发明实施例还提供一种加密存储器芯片,包括:用于寄存输入数据的输入寄存器堆、用于加密存储数据的存储单元阵列、用于将数据写入所述闪存单元阵列中的闪存单元的写入电路、用于进行行列译码的行列译码器、用于读取所述闪存单元阵列中的数据的读取电路以及控制上述电路工作的控制器,所述控制器执行上述的数据加密存储方法对数据进行加密存储或执行上述的数据解密方法的对闪存单元中的数据进行解密。

[0109] 特别地,根据本发明的实施例,上文参考流程图描述的过程可以被实现为计算机软件程序。例如,本发明的实施例包括一种计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现上述方法的步骤。

[0110] 上述实施例阐明的装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。

[0111] 为了描述的方便,描述以上装置时以功能分为各种单元分别描述。当然,在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0112] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0113] 本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于系统实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0114] 以上所述仅为本申请的实施例而已,并不用于限制本申请。对于本领域技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在本申请的权利要求范围之内。

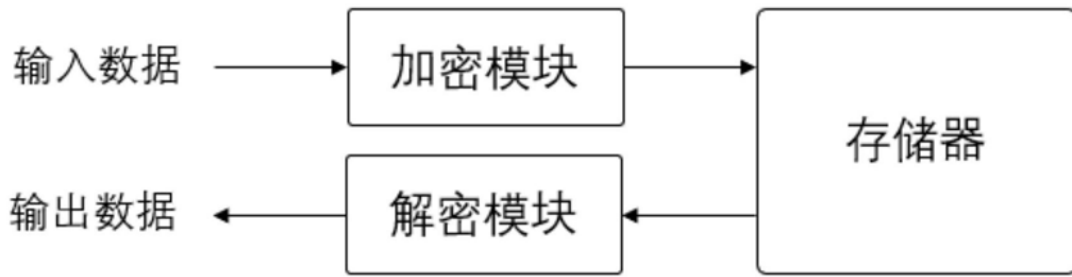


图1

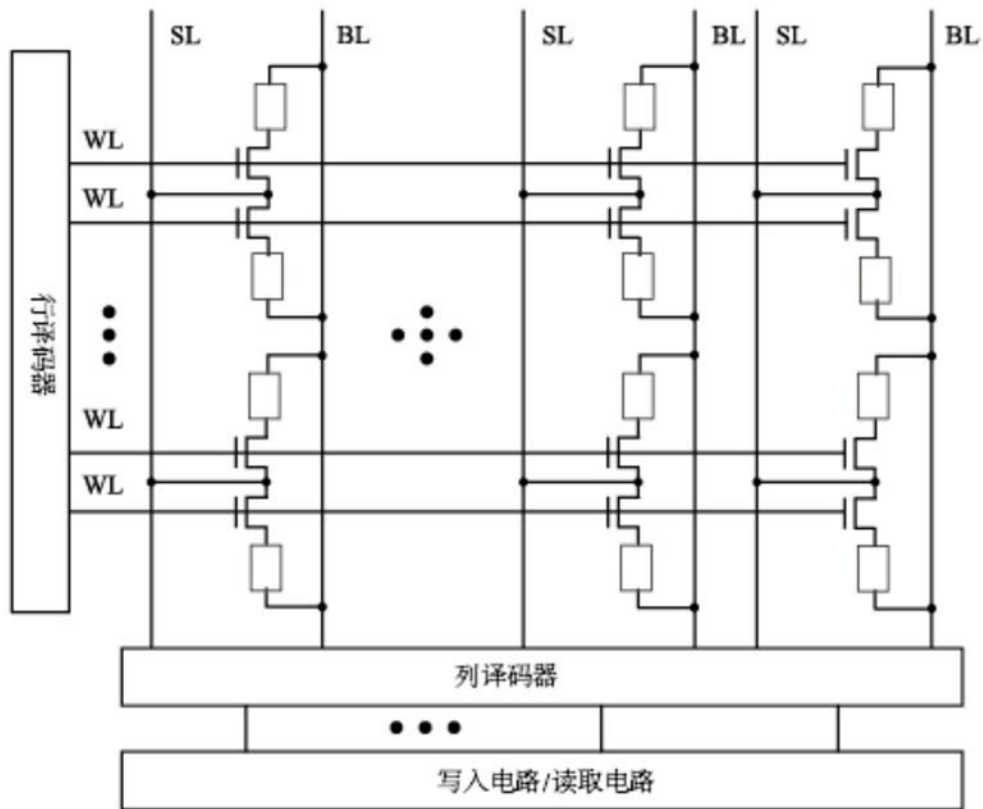


图2

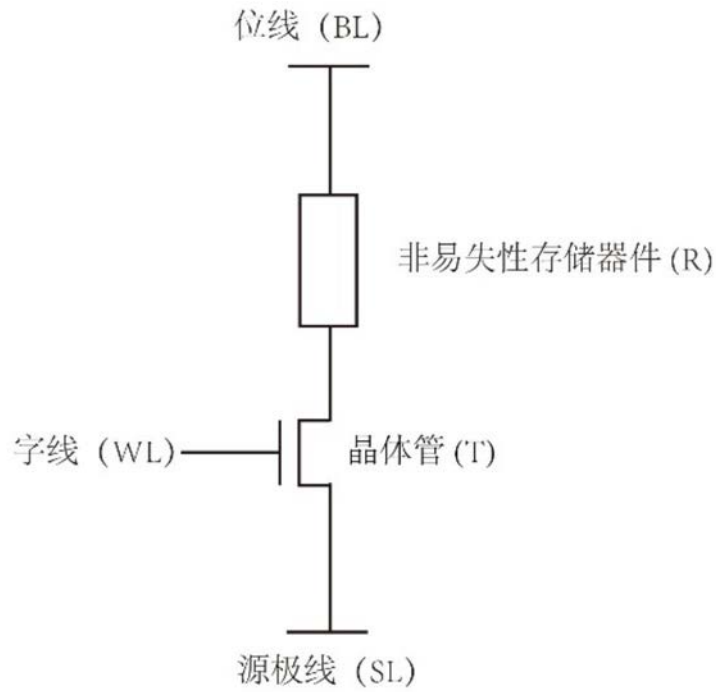


图3

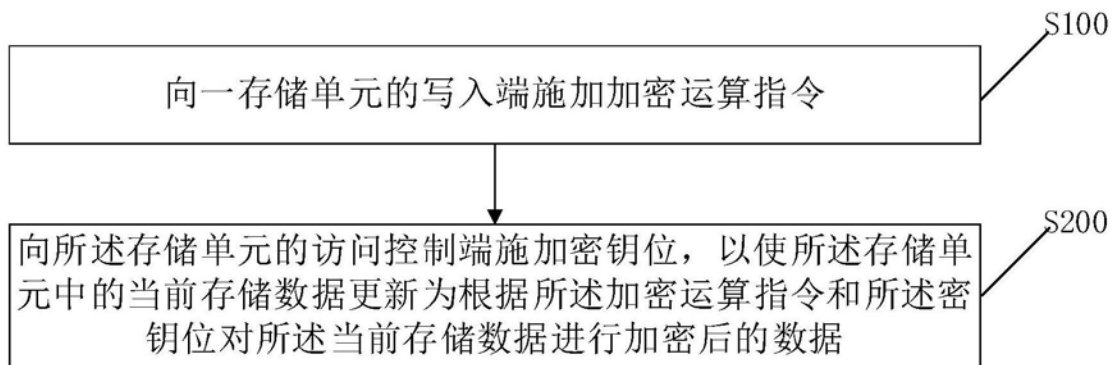


图4

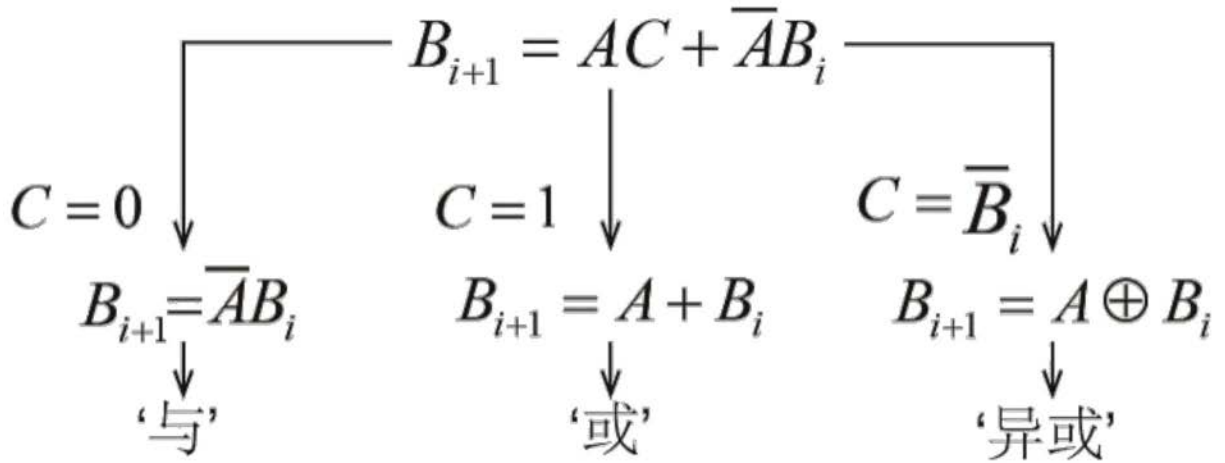


图5

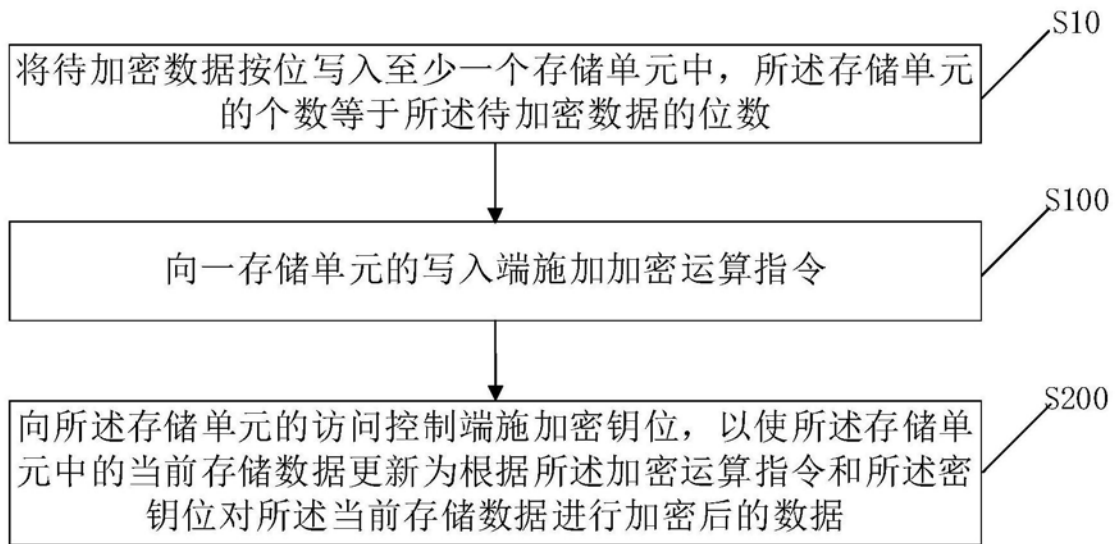


图6

B_i	A	C	B_{i+1}
0	0	0	0
0	1	0	0
1	0	0	1
1	1	0	0
0	0	1	0
0	1	1	1
1	0	1	1
1	1	1	1

图7

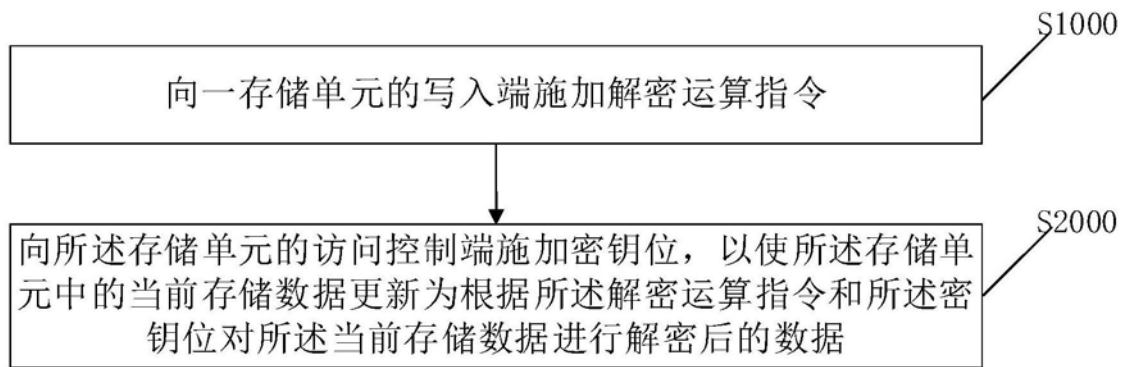


图8