(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106409336 A
(43)申请公布日 2017.02.15

(21)申请号 201610819091.0

(22)申请日 2016.09.13

(71)申请人 天津大学
地址 300072 天津市南开区卫津路92号

(72)发明人 赵毅强 辛睿山 赵公元 王佳 李跃辉

(74)专利代理机构 天津市北洋有限责任专利代理事务所 12201
代理人 刘国威

(51)Int.Cl.
G11C 16/04(2006.01)
G11C 16/14(2006.01)
G11C 16/34(2006.01)

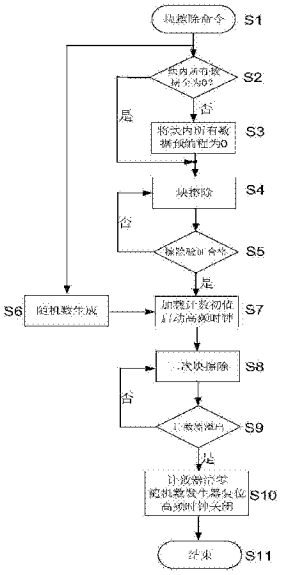
权利要求书1页 说明书4页 附图2页

(54)发明名称

基于随机时间的非易失性存储器数据安全擦除方法

(57)摘要

本发明涉及数据安全领域，为提出非易失性存储器数据安全擦除方法，利用随机数发生器、计数器与高频时钟结构，调控数据擦除时间，使得擦除时间随机，进而使得浮栅单元残余电子数随机，大大增加了数据恢复难度，保障了存储器芯片的数据安全。为此，本发明采用的技术方案是，基于随机时间的非易失性存储器数据安全擦除方法，具体步骤如下：利用随机数发生器、计数器与高频时钟结构，调控数据擦除时间，使得擦除时间随机，进而使得浮栅单元残余电子数随机。本发明主要应用于数据安全。



CN 106409336 A

1.一种基于随机时间的非易失性存储器数据安全擦除方法，其特征是，具体步骤如下：

步骤S1中，非易失性存储器的命令接收模块接收芯片输入信息，包括擦写命令和起始地址，命令解析模块对接收到的输入信息进行解析，向预编程模块发送解析后的命令和相关数据，从而启动块擦除状态机，下一步将进行步骤S2；同时，命令解析模块还产生随机数生成器启动信号，下一步同时进行步骤S6；

步骤S6中，经步骤S1，随机数生成器将启动，此后随机数生成器将生成一个指定位宽的随机数，该随机数据将用于步骤S7中作为计数器初值；

步骤S2中，将进行块内数据的预判断操作，若块内所有存储空间的存储数据都为“0”，则无需进行预编程，下一步进入块擦除操作S4；若块内存在数据不为“0”的地址空间，则下一步进入预编程操作S3；

步骤S3中，进行预编程操作，预编程操作模块根据步骤S1中命令解析模块传递的块擦写命令以及起始地址，对相应地址的存储块内所有地址空间进行预编程，完成整块的预编程操作后，当前块内的所有地址空间存储数据都为“0”，下一步进入步骤S4；

步骤S4中，将根据块地址，对相应的块进行擦除操作，当完成一次块擦除操作后，将进入擦除验证步骤S5；

步骤S5中，进行块擦除结果验证，若当前块内某一地址空间存储的数据不为“1”，则擦除操作未完成，返回步骤S4，继续进行擦除操作；若当前块内所有地址空间存储数据都为“1”，则块擦除验证完成，进入步骤S7；

步骤S7中，计数器读取步骤S6中随机数生成器生成的随机数值，作为计数器初始值，并启动高频时钟，每个高频时钟上升沿，计数器计数值加1，当计数器开始计数时，进入步骤S8；

步骤S8中，对当前块进行一次额外的擦除操作，该擦除操作同步骤S4中块擦除操作类似，只是相比于S4中块擦除，该擦除将一直持续，在擦除持续过程中，将一直判断计数器是否溢出，进入步骤S9；

步骤S9中，需要判断计数器是否溢出，若未溢出，则返回步骤S8，继续进行擦除操作。若计数器溢出，则额外的擦除操作完成，进入步骤S10；

步骤S10中，计数器清零，随机数发生器复位，高频时钟关闭。进入步骤S11；

步骤S11中，此次块擦除操作结束。

2.如权利要求1所述的基于随机时间的非易失性存储器数据安全擦除方法，其特征是，擦除操作具体步骤是，控制栅接地，源端接12V的高电压，漏端悬空，由于控制栅和浮栅之间的电容耦合效应，因此在浮栅与源区之间形成强电场，浮栅上的电子直接穿过隧道氧化层的势垒到达源区，使得浮栅上的负电荷减少，浮栅晶体管的阈值电压降低。

基于随机时间的非易失性存储器数据安全擦除方法

技术领域

[0001] 本发明涉及数据安全领域，尤其涉及一种基于擦除时间随机改变的非易失性存储器数据安全擦除方法。

背景技术

[0002] 随着微电子技术的快速发展，存储器芯片作为各类数据和程序的唯一载体，越来越多地受到外部攻击，对用户的自主知识产权、敏感信息造成巨大威胁。其中，以FLASH存储器为代表的非易失性存储器，以其容量大、体积小、传输速率快等优点，在社会各个领域都得到了广泛的应用。

[0003] 但是，现有非易失性存储器存在数据残留现象，完全清除残留在其中的关键数据将面临巨大挑战，即使经过物理上的擦除或者覆盖，非易失性存储单元(浮栅单元)上仍然存在残留电子，使得攻击者能够通过一定的攻击手段，以一定的概率恢复有用的数据，从而导致关键数据泄露。剑桥大学的Sergei Skorobogatov和David Samyde证明了在某些Flash样品中，即使经过多次擦除，数据仍然能够被恢复出来[1]。研究表明，非易失性存储器中浮栅残留电子数与其擦除电压、擦除时间、擦除次数、器件自身参数等都存在联系[2]。其中，擦除时间作为可控因素之一，对于提高非易失性存储器擦除效果具有重要的意义。在一定的擦除时间内，浮栅残留电子数与擦除时间成反比。但是，在实际使用中，擦除时间不可无限延长。另外，由于现有非易失性存储器的擦除时间固定，经过擦除操作后，浮栅残留电子数固定，其阈值电压固定。攻击者通过测量器件阈值电压，存在一定概率恢复有效数据。为提高擦除安全性，可以使擦除时间具有一定的随机性，从而使得残留电子具有随机性，增加了攻击者恢复数据的难度。

[0004] 经过专利检索，还未有中国专利提出类似基于随机擦除时间的非易失性存储器数据安全擦除方法。为此，本专利提出一种适用于非易失性存储器的数据安全擦除方法，该方法利用随机数发生器与计数器调控擦除时间，使得存储器各区块擦除时间不同，从而使得攻击者无法恢复有效数据。

[0005] 参考文献

[0006] 1、Samyde D,Skorobogatov S,Anderson R,et al.On a new way to read data from memory[C]//Security in Storage Workshop,2002.Proceedings.First International IEEE.IEEE,2002:65-69。

[0007] 2、Skorobogatov S.Data remanence in flash memory devices[C]//International Workshop on Cryptographic Hardware and Embedded Systems.Springer Berlin Heidelberg,2005:339-353。

发明内容

[0008] 为克服现有技术的不足，本发明旨在提出提出非易失性存储器数据安全擦除方法，利用随机数发生器、计数器与高频时钟结构，调控数据擦除时间，使得擦除时间随机，进

而使得浮栅单元残余电子数随机，大大增加了数据恢复难度，保障了存储器芯片的数据安全。为此，本发明采用的技术方案是，基于随机时间的非易失性存储器数据安全擦除方法，具体步骤如下：

[0009] 步骤S1中，非易失性存储器的命令接收模块接收芯片输入信息，包括擦写命令和起始地址，命令解析模块对接收到的输入信息进行解析，向预编程模块发送解析后的命令和相关数据，从而启动块擦除状态机，下一步将进行步骤S2；同时，命令解析模块还产生随机数生成器启动信号，下一步同时进行步骤S6；

[0010] 步骤S6中，经步骤S1，随机数生成器将启动，此后随机数生成器将生成一个指定位宽的随机数，该随机数据将用于步骤S7中作为计数器初值；

[0011] 步骤S2中，将进行块内数据的预判断操作，若块内所有存储空间的存储数据都为“0”，则无需进行预编程，下一步进入块擦除操作S4；若块内存在数据不为“0”的地址空间，则下一步进入预编程操作S3；

[0012] 步骤S3中，进行预编程操作，预编程操作模块根据步骤S1中命令解析模块传递的块擦写命令以及起始地址，对相应地址的存储块内所有地址空间进行预编程，完成整块的预编程操作后，当前块内的所有地址空间存储数据都为“0”，下一步进入步骤S4；

[0013] 步骤S4中，将根据块地址，对相应的块进行擦除操作，当完成一次块擦除操作后，将进入擦除验证步骤S5；

[0014] 步骤S5中，进行块擦除结果验证，若当前块内某一地址空间存储的数据不为“1”，则擦除操作未完成，返回步骤S4，继续进行擦除操作；若当前块内所有地址空间存储数据都为“1”，则块擦除验证完成，进入步骤S7；

[0015] 步骤S7中，计数器读取步骤S6中随机数生成器生成的随机数值，作为计数器初始值，并启动高频时钟，每个高频时钟上升沿，计数器计数值加1，当计数器开始计数时，进入步骤S8；

[0016] 步骤S8中，对当前块进行一次额外的擦除操作，该擦除操作同步骤S4中块擦除操作类似，只是相比于S4中块擦除，该擦除将一直持续，在擦除持续过程中，将一直判断计数器是否溢出，进入步骤S9；

[0017] 步骤S9中，需要判断计数器是否溢出，若未溢出，则返回步骤S8，继续进行擦除操作。若计数器溢出，则额外的擦除操作完成，进入步骤S10；

[0018] 步骤S10中，计数器清零，随机数发生器复位，高频时钟关闭。进入步骤S11；

[0019] 步骤S11中，此次块擦除操作结束。

[0020] 擦除操作具体步骤是，控制栅接地，源端接12V的高电压，漏端悬空，由于控制栅和浮栅之间的电容耦合效应，因此在浮栅与源区之间形成强电场，浮栅上的电子直接穿过隧道氧化层的势垒到达源区，使得浮栅上的负电荷减少，浮栅晶体管的阈值电压降低。

[0021] 本发明的特点及有益效果是：

[0022] 本发明可以满足非易失性存储器正常的数据存储与读取，又能防止已擦除数据被恶意读出。通过随机改变非易失性存储器的擦除时间，使得存储器浮栅单元擦除后的残余电子数随机，增加了数据被恶意恢复的难度，从而保障了非易失性存储器的数据安全。

附图说明：

[0023] 图1基于随机时间的安全擦除方法流程图；

[0024] 图2非易失性存储单元擦除操作原理图。

具体实施方式

[0025] 本发明旨在提出一种基于随机时间的非易失性存储器数据安全擦除方法，该方法利用随机数发生器、计数器与高频时钟结构，调控数据擦除时间，使得擦除时间随机，进而使得浮栅单元残余电子数随机，大大增加了数据恢复难度，保障了存储器芯片的数据安全。

[0026] 本发明针对非易失性存储器一般擦除方法存在数据残留的问题，提出一种基于随机时间的数据擦除方法，该方法先进行一次一般擦除，再进行一次特殊的随机时间擦除，从而使得整体擦除时间随机，保障了非易失性存储器数据无法恢复。

[0027] 为使本发明的目的、技术方案更加清楚，以下将结合图1所示安全擦除方法流程图进行详细说明，具体步骤如下：

[0028] 步骤S1中，非易失性存储器的命令接收模块接收芯片输入信息，包括擦写命令和起始地址，命令解析模块对接收到的输入信息进行解析，向预编程模块发送解析后的命令和相关数据，从而启动块擦除状态机，下一步将进行步骤S2。同时，命令解析模块还产生随机数生成器启动信号，下一步同时进行步骤S6。

[0029] 步骤S6中，经步骤S1，随机数生成器将启动，此后随机数生成器将生成一个指定位宽的随机数。该随机数据将用于步骤S7中作为计数器初值。

[0030] 步骤S2中，将进行块内数据的预判断操作。若块内所有存储空间的存储数据都为“0”，则无需进行预编程，下一步进入块擦除操作S4。若块内存在数据不为“0”的地址空间，则下一步进入预编程操作S3。

[0031] 步骤S3中，进行预编程操作。预编程操作模块根据步骤S1中命令解析模块传递的块擦写命令以及起始地址，对相应地址的存储块内所有地址空间进行预编程。完成整块的预编程操作后，当前块内的所有地址空间存储数据都为“0”，下一步进入步骤S4。

[0032] 步骤S4中，将根据块地址，对相应的块进行擦除操作。如图2所示，为非易失性存储单元擦除操作原理图。浮栅单元通过改变浮栅上存储电荷量大小，来改变阈值电压高低，从而实现存储逻辑“0”与逻辑“1”。擦除操作需要电子流出浮栅，使阈值电压降低。其具体过程为：控制栅接地，源端接12V的高电压，漏端悬空，由于控制栅和浮栅之间的电容耦合效应，因此在浮栅与源区之间形成强电场，浮栅上的电子直接穿过隧道氧化层的势垒到达源区，使得浮栅上的负电荷减少，浮栅晶体管的阈值电压降低。当完成一次块擦除操作后，将进入擦除验证步骤S5。

[0033] 步骤S5中，进行块擦除结果验证。若当前块内某一地址空间存储的数据不为“1”，则擦除操作未完成，返回步骤S4，继续进行擦除操作。若当前块内所有地址空间存储数据都为“1”，则块擦除验证完成，进入步骤S7。

[0034] 步骤S7中，计数器读取步骤S6中随机数生成器生成的随机数值，作为计数器初始值，并启动高频时钟，每个高频时钟上升沿，计数器计数值加1。当计数器开始计数时，进入步骤S8。

[0035] 步骤S8中，对当前块进行一次额外的擦除操作，该擦除操作同步骤S4中块擦除操作类似，只是相比于S4中块擦除，该擦除将一直持续。在擦除持续过程中，将一直判断计数

器是否溢出，进入步骤S9。

[0036] 步骤S9中，需要判断计数器是否溢出，若未溢出，则返回步骤S8，继续进行擦除操作。若计数器溢出，则额外的擦除操作完成，进入步骤S10。

[0037] 步骤S10中，计数器清零，随机数发生器复位，高频时钟关闭。进入步骤S11。

[0038] 步骤S11中，此次块擦除操作结束。

[0039] 由步骤S1-S2-S3-S4-S5-S11的擦除操作为一般擦除方法，该方法可以满足一般数据擦除需求，但对于高安全等级的应用情况，无法确保数据完全擦除干净且无法恢复。

[0040] 步骤S6-S7-S8-S9-S10为本发明提出的基于随机时间的特殊擦除步骤，该步骤通过随机数发生器产生某一位宽的随机数，将该随机数作为计数器计数初值，同时启动额外的擦除操作。在高频时钟驱动下，计数器计数值不断增加，直到计数器溢出。计数器溢出后，停止额外的擦除操作。由于随机数发生器每次产生的随机数不同，则每次装入计数器的计数初值随机，则计数器由计数初值到计数溢出所花费的时间为一个随机量，故每次额外擦除操作进行的时间也为一个随机量，使得浮栅单元残余电子数为一个随机值，从而大大增加了数据恢复难度。

[0041] 如图1所示，按照流程图依次进行所有步骤。本发明的保护范围并不以上述实施方式为限，本领域普通技术人员根据本发明所揭示内容所作的等效修饰或变化，皆应纳入保护范围。

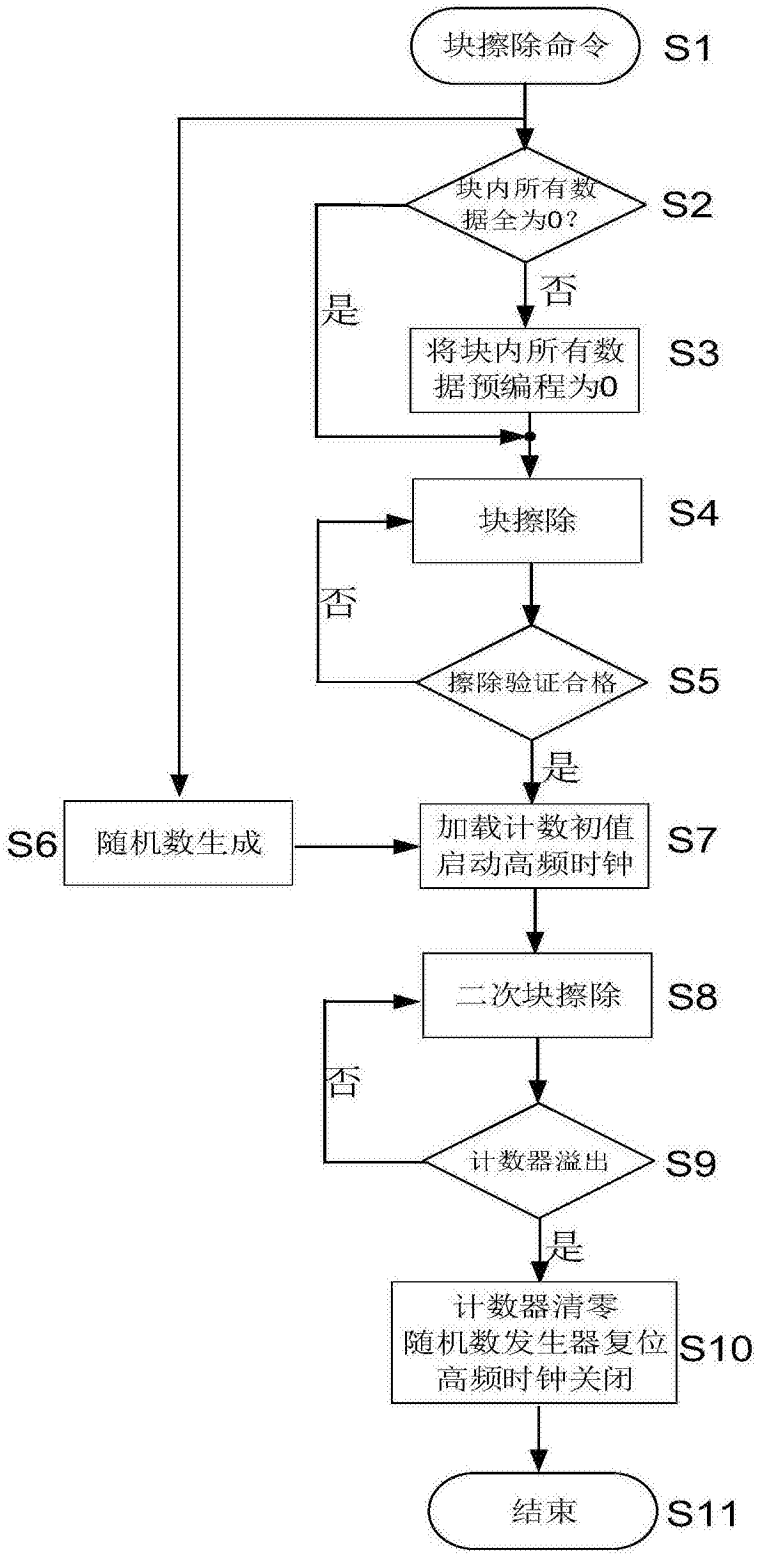

块擦除命令
S1
块内所有数据全为0？
S2
否
是
将块内所有数据预编程为0
S3
块擦除
S4
否
擦除验证合格
S5
是
S6
随机数生成
加载计数初值
启动高频时钟
S7
二次块擦除
S8
否
计数器溢出
S9
是
计数器清零
随机数发生器复位
高频时钟关闭
S10
结束
S11

图1

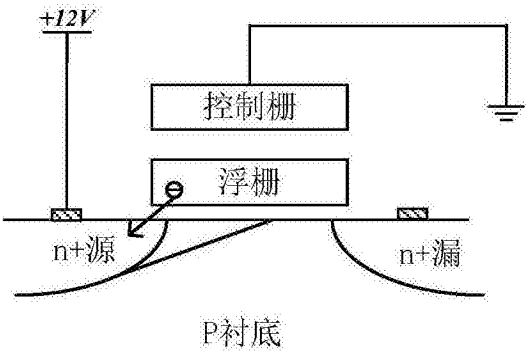


图2