基于相变存储器的非易失内存数据机密性保护

赵 鹏 朱龙云
(清华大学计算机科学与技术系 北京 100084)

摘 要 相变存储器(Phase-Change Memory)是计算机体系结构中的下一代内存技术,具有高密度、低功耗、非易失等优点,具备替代现有 DRAM 内存的实力,但非易失的自然属性会带来一系列潜在计算机数据隐私方面的隐患.比如掉电后内存中依然保留了很多明文形式的敏感数据,同时相变存储器的存储单元还有写次数有限的问题.文中提出一种基于加密技术和减少相变存储器写次数的方法.它能保护基于相变存储器的内存中的数据,即使在系统断电的状态下内存中的敏感数据也不能被攻击者获取,同时极大延长了系统内存的使用寿命,加强了非易失内存的机密性和可靠性.实验结果表明,增加处理单元后,整体系统性能只下降 3.6%,同时在加密操作的条件下相变内存的寿命平均延长 2.6 倍,所提设计方案可以很好地达到预期目的.

关键词 相变存储器;加密内存;机密性;写操作
中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.02114

A Scheme for Protecting Confidentiality of No-volatile Main Memory Based on Phase-Change Memory

ZHAO Peng ZHU Long-Yun
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract Phase-Change Memory(PCM) is a computer architecture in the next-generation memory technology. As its high density, low power, nonvolatile, etc., it has ability to replace the existing DRAM memory. But the natural properties of non-volatile computer will bring a range of potential data privacy risks, such as after power-down memory still retains a lot of sensitive data in plain text, and phase-change memory storage unit has issues of limited number writing. Proposed design based on encryption technology and reducing the number of phase-change memory write can protect the data in the phase-change memory, even when the system power off, memory sensitive data can not be obtained by the attacker. While it can greatly extend the life of system memory to enhance the confidentiality and reliability of the non-volatile memory. The results show that increasing the processing unit, the overall system performance is only down 3.6%, while adding the encryption operation on the phase-change memory, the life of whole memory can be extended 2.6 times the average, the proposed design can achieve the desired good.

Keywords phase change memory; encryption memory; confidentiality; write operation

1 引 言

随着计算机体系结构的发展,计算机的运算能力显著提高,同时系统对内存的要求也越来越高.目前所使用的动态随机存储器(DRAM)的发展逐渐遇到了瓶颈,片载容量和能耗问题日益突出,研究人员开始寻找能解决问题的替代产品.相变存储器技

收稿日期:2011-08-29;最终修改稿收到日期:2011-09-19.本课题得到国家自然科学基金(61103020)资助.**赵 鹏**,男,1985 年生,博士研究生,中国计算机学会(CCF)学生会员,主要研究方向为新型内存体系结构、操作系统、系统安全.E-mail: p-zhao07@mails.tsinghua.edu.cn. **朱龙云**,男,1986 年生,硕士研究生,主要研究方向为新型内存体系结构、操作系统。

术(Phase-Change Memory)以下简称 PCM，作为一种新型的存储技术正日趋成熟. 由于 PCM 的读写速度和 DRAM 的读写速度相近，和 DRAM 相比，既节约能耗，片载密度又高，所以 PCM 成为一种很好的 DRAM 替代品，成为下一代内存技术的主要候选对象.

PCM 尽管拥有众多优点，但要作为计算机系统的内存依然面临很多挑战. PCM 的一个重要特性是非易失性，保存在 PCM 存储单元中的信息在没有电力供给的情况下可以永久保持，拥有同磁盘、Flash 闪存等一样的数据非易失特性. PCM 不仅可以替代 DRAM，也可以替代磁盘或 Flash 闪存. 由于在现代计算机体系架构中，内存占有核心地位，即使在外存或网络传输中对数据进行了加密保护，一旦数据要进行处理，就要被调入内存. 当处于内存中的数据要进行处理时都会脱离原来的保护，比如从密文转换为明文参与运算处理. 这就给攻击者带来了可乘之机. 攻击者可以直接对内存数据进行扫描然后进行数据分析，寻找他们感兴趣的数据，比如用户的银行账户和密码，用户的个人隐私数据等. 即使系统断电之后，攻击者仍然可以获得数据. 文献[1]采用了 cold boot 攻击，在系统关机掉电后，用液氮来冷冻 DRAM 内存，原本掉电后消失的数据还会长时间保存在 DRAM 中，攻击者将冷冻的 DRAM 内存插入到自己的计算机中，就可以拷贝内存数据并进行数据分析进而获得共享密钥等信息. 当 PCM 作为内存时，自身的非易失特性决定了即使掉电后内存中的数据也不会消失，这就更方便了攻击者. 攻击者只需将掉电后的 PCM 内存插入到自己的计算机中就可以按部就班地完成剩下的数据获取步骤. 这会给计算机系统造成极大的安全隐患.

还有一个 PCM 需要面对的挑战是本身写次数有限的问题. 每个 PCM 存储单元目前的可写次数大约是 10^8 次，作为内存的存储单元中的数据更新会很频繁，当写次数达到上限后，该存储单元会失效进而造成数据丢失，这在一定程度上降低了 PCM 内存自身的稳定性.

本文在分析了 PCM 内存在数据保护方面所面临的挑战后，提出一种基于加密技术和减少相变存储器写次数的方法. 该方法既能保护基于相变存储器的内存中的数据，即使在系统断电的状态下内存中的敏感数据也不能被攻击者获取，同时极大延长了系统内存的使用寿命，从而加强了非易失内存数据的机密性和可靠性.

本文第 2 节介绍相关工作；第 3 节介绍整体解决方案，并分别从数据保护、数据加密对数据写回的影响及有效减少写次数的方法三个方面详细介绍解决方案；第 4 节给出本文所提方案的一些实验结果并进行了相关比较；第 5 节做了总结和展望.

2　相关工作

2.1　相变存储器技术

传统 DRAM 存储单元使用 1 个电容存储 1 比特信息. 而一个相变存储单元使用含有一种或多种氧族元素的玻璃材质来存储 1 比特信息. 这种介质可以稳定地存在两种状态：非晶体状态和晶体状态. 可以用来代表逻辑上的‘0’和‘1’. 两种状态可以通过加热来进行状态转换. 当温度达到结晶温度以上并小于熔点时，材质由非晶体状态转变为晶体状态(‘1’). 当加热温度超过熔点温度后，材质又变为非晶体状态(‘0’). 这种材质还可以通过加热温度的不同来形成多种可以区分的状态来存储更多的信息. 图 1 为利用相变存储单元构成的 PCM 存储阵列，可以像 DRAM 那样存储多位数据.

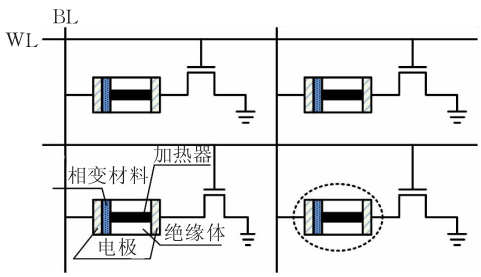

图 1　PCM 存储阵列[2]

2.2　延长 PCM 写寿命技术

目前延长 PCM 写寿命的方法主要分为两大类：

(1) 减少数据的写次数

由于 PCM 可以按位寻址，所以最小的写操作单位是比特位. Cache line 级别的写回策略[3]只把修改过的 cache line 写回，而不是把整个页写回 PCM 内存. 同样，部分写的方法(partial writes)[4]是当 cache line 被替换时，只把包含修改过比特位的脏字写回 PCM 内存. Redundant bit-write removal[2]设计了一个硬件电路，会将现有数据和新的将要写入的数据进行对比，仅仅将那些不同的数据位写回. Flip-N-write[5]将修改的数据位数控制在 50% 以内.

(2) 磨损均衡

磨损均衡的目的是使写操作均匀分布到各个存

储单元. Segment swapping[2] 当一个段的擦写次数过多时,将其与其它擦写次数少的段进行交换. Start-gap[6] 当写操作次数达到一定程度时,通过一个空闲 cache line 来对存储块进行调整,同时改变逻辑地址和物理地址的对应关系来达到磨损均衡.

这两类技术均可以有效地解决 PCM 的写寿命问题,通常可以混合使用.

2.3 存储加密技术

为了防止被攻击者轻易看到明文数据,通常采用对数据进行加密的方法来保证数据的机密性. 最简单的方式是采用直接加密的方式,也就是直接用密钥通过对称加密的分组加密算法对明文信息进行加密. 但这样做的一个很大的缺点是性能不好,很大程度地降低了系统的数据处理能力. 另外一种通用的方法是采用基于计数器的加密方式[7] 来提高加密性能. 它利用计数器和对称加密算法生成一个一次一密的加密块,然后加密块和数据进行异或处理. 这样加密过程和数据获取过程可以并行执行从而提高性能.

3 设计方案

3.1 整体设计框架

如图 2 所示,将计算机系统分为两个区域:信任区域和不信任区域,在信任区域可以使用明文来直接对数据进行操作;在不信任区域数据均为加密形式. 本设计方案的主要内容是增加了一个安全处理区域,位于缓存和内存之间,来完成对数据的加解密和减少写操作的处理.

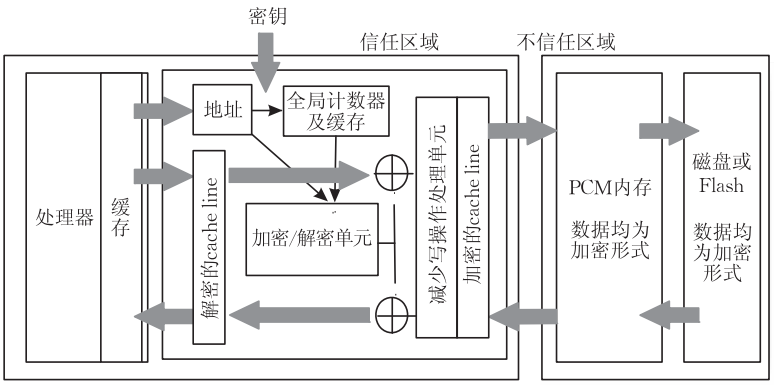

图 2 数据处理流程设计图

数据从 PCM 内存中读取. 在 PCM 内存中,数据以加密形式存在. 当处理器调用内存数据时,调用到的加密数据将进入到安全处理区域. 首先通过减少写操作的处理单元,进行数据预处理. 然后同加密/解密单元中生成的加密块做异或操作,完成数据解密过程. 最后明文数据进入缓存.

数据写回 PCM 内存. 当数据发生改变被缓存换出时,需要将数据写回 PCM 内存中. 按照读取数据的逆过程,对数据进行异或加密处理后再进行减少写操作的处理形成加密数据,写回到 PCM 内存.

设计方案的重点和难点在于如何生成安全的加密块,也就是如何选择加密算法种子实现加密块的唯一性,从而保证数据的机密性. 这将在 3.2 小节中进行详细叙述. 研究发现,由于加密算法的扩散效应会导致数据的改动很大,这就给有写次数限制的 PCM 内存带来了考验. 为了降低加密对 PCM 内存的影响,延长 PCM 使用寿命,本方案中增加了减少写操作的处理单元,有效地缓解了加密带来的影响.

3.2 数据机密性保护

首先分析一下在计数器加密模式下的安全性. 加密算法通过加密种子数据来生成一个加密块,然后要加密的数据同加密块做异或运算生成加密数据. 这种加密方式的安全性关键在于要确保每次加密时的加密块不能重复,也就是要保证种子数据的唯一性.

假定两个明文数据块分别为 P_1 和 P_2,加密后的数据块为 C_1 和 C_2,对两个数据块采用相同的种子数据 $Seed_1 = Seed_2$,由于分组加密算法是一对一映射函数,那么它们产生的加密块也相同.

两边经过异或运算,得到

$$E_{key}(Seed_1) = E_{key}(Seed_2),$$

$$C_1 = P_1 \text{ XOR } E_{key}(Seed_1),$$

$$C_2 = P_2 \text{ XOR } E_{key}(Seed_2).$$

根据异或的运算性质最后可以得到

$$C_1 \text{ XOR } C_2 = (P_1 \text{ XOR } E_{key}(Seed_1)) \text{ XOR } (P_2 \text{ XOR } E_{key}(Seed_2)).$$

从最后得到的公式可以看到如果知道任意 3 个

未知数的值，另外一个未知数也可以计算得到.

很多情况下，攻击者可以得到加密过的数据，然后通过一些手段可以获得一个明文数据，那么最后一个未知数将会被破解. 所以在这种加密模式中要达到安全性就要求种子数据必须是唯一的、不可重复的.

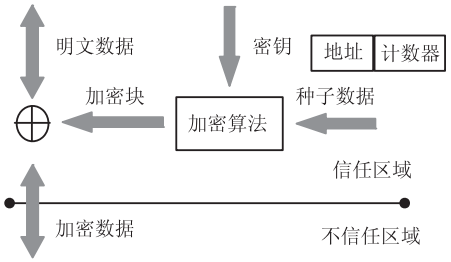

图 3　加密过程

为了保证种子数据的唯一性，我们借鉴了文献[7]中的设计思路. 将数据的虚拟地址和计数器结合来构成种子数据. 利用内存数据块的虚拟地址来保证在空间上的唯一性，利用计数器来保证时间上的唯一性. 利用这种方式可以避免在同一地址上写回不同的种子数据，达到种子数据的全局唯一的目的.

在安全处理区域中增加一个全局的 64 位非易失寄存器作为全局计数器. 采用大位数的寄存器可以保证计数器不轻易溢出，从而排除相同种子的可能. 当需要对内存进行写操作时，计数器自动加 1，即使掉电，计数器也不会丢失数据. 当数据写回内存后，数据加密时所对应的计数器同样写入内存的特定区域. 当解密时，需要将数据对应的计数器读入安全处理区域，为了提高运算性能，在安全处理区域中设计了 8 MB 的计数器缓存，可以缓存 1 MB 计数器的数值，从而提高处理性能.

此外，分组加密算法采用标准的 AES 加密，密钥是 AES 加密引擎自身提供的私有密钥或是外部提供的可信任的私有密钥，每个引擎的密钥均不同.

当数据 P 写回内存时：

$$seed=VA(P)+GlobalCounter,$$

$$C=P\ \text{XOR}\ AES_{\text{key}}(seed),$$

$$LocalCounter=GlobalCounter,$$

GlobalCounter 是全局计数器中的当前值，*LocalCounter* 随数据 P 一同写入内存.

当数据 P 从内存读取时，首先从计数器缓存中查找相应的计数器是否存在. 若命中，直接调用；若缺失，则需从内存中读取：

$$seed=VA(P)+LocalCounter,$$

$$P=C\ \text{XOR}\ AES_{\text{key}}(seed).$$

3.3　分析数据加密对数据写回的影响

在上面所设计的数据保护方案中，当数据需要被写回 PCM 内存时，数据将进行加密操作，加密后的数据和内存中原来的数据差别越大，意味着需要修改的 PCM 存储单元越多. 为了延长 PCM 存储单元寿命，修改的位数越少越好. 下面通过一个简单的实验来分析数据加密对数据写回的影响.

假定采用 AES 算法进行数据加密，分组大小和密钥长度均为 128 位. 需要加密的数据为 00000000000000000000000000000000，修改后的数据 00000000000000000000000000000001. 密钥为 0123456789ABCDEF0123456789ABCDEF. 所列数据均为十六进制表示.

如图 4 所示，一个数据块在未采用加密方式时只修改了一位，当采用加密方式后，由于加密算法所具有的扩散效应使多位数据产生变化，从图 4 中的例子中看到原始数据需要修改 63 位，占到了数据块的一半. 这加快了对 PCM 内存存储单元的磨损.

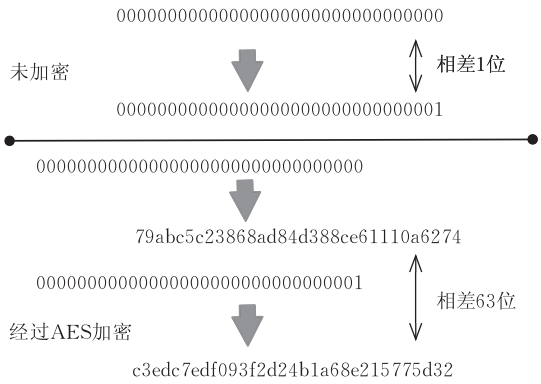

图 4　数据加密对数据的影响

3.4　减少 PCM 写次数

当写回的 cache line 数据经过加密处理后，数据的改动就不会是局部性的变动，而是分散到了多个位上. 上一节的实验中可以看到这一现象. 由于 PCM 存在存储单元写次数受限的问题，为了减小加密操作对 PCM 内存寿命的伤害，我们设计增加了一种减少 PCM 写次数的处理单元来延长 PCM 存储单元的寿命.

设计的要点是在 PCM 内存中为每个 cache line 大小的数据块增加两个标志位. 在图 2 中的减少写操作处理单元中增加一个 cache line 大小的只读辅助寄存器，初值为 1010…1010. 下面对数据的读取和写入两个过程详细描述.

3.4.1　数据写入过程

如图 5 所示，数据写入时所经历的过程：

(1)首先需要将写回的数据块进行预处理，分别

进行取反、异或和同或运算；

(2)在运算的同时从 PCM 内存中读取相应的原始数据块；

(3)分别将预处理后的数据同 PCM 内存中读取的原始数据块求汉明距离；

(4)选择汉明距离最小的相应预处理结果写回存储单元，并置相应的标志位；完成写入过程. 2 位标志位可以表示 4 种状态，汉明距离最小表明需要写回的预处理数据同原始数据块的差别最小.

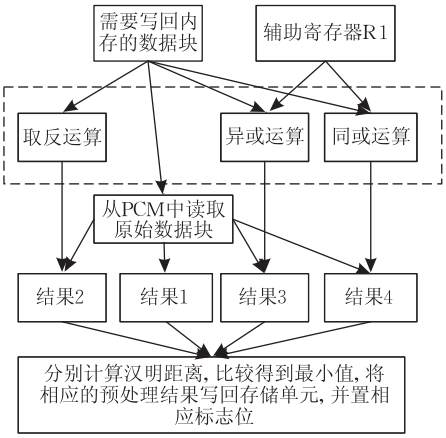

图 5 数据写入过程

3.4.2 数据读取过程

如图 6 所示，数据读取时所经历的过程包括：

(1)首先读取数据块及相应标志位；

(2)通过标志位来判断采取哪种运算，如：标志位为 01，将数据块直接进行取反操作即可得到数据块；若标志位为 10，数据块需要结合辅助寄存器进行异或操作得到需要的数据块；若标志位为 00，则直接读取数据块；若标志位为 11，则结合辅助寄存器进行同或操作得到数据.

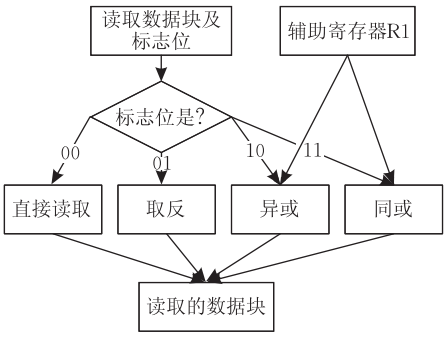

图 6 数据读取过程

4 实验评测

4.1 实验环境

实验采用 GEM5[8] 体系结构模拟器进行. GEM5 可按照指令周期模拟计算机硬件系统运行状况. 按照设计要求对其进行了修改，增加了 PCM 的模拟，构建了 PCM 内存. 表 1 为实验系统的简要配置. 实验所用系统环境包含双核 X86_64 处理器架构、两级 cache 结构、4GB 的 PCM 内存. 部分测试程序选自 SPEC CPU2000&SPEC CPU2006 标准测试程序中的访存密集型程序，实验结果中各程序均运行 1 亿个指令周期. 设置访存延迟为 100 个时钟周期，加解密的访问延迟为 50 个时钟周期.

表 1 测试系统配置情况

参数	配置
处理器参数	2 个乱序执行处理单元，运行频率为 2GHz，X86_64 处理器架构
L1 缓存参数	处理单元私有 L1 缓存，分离式，LRU I-cache 和 D-cache：64KB，4-way，256b/line
L2 缓存参数	共享，4MB，16-way，256b/line，LRU
内存控制器	单内存控制器
内存配置	4GB PCM 内存，1DIMM，4Ranks/DIMM，16Banks/Rank

4.2 系统性能比较

通过在基于 PCM 内存的系统上运行标准测试程序来评测我们的设计方案是否有效. 由于我们的设计方案是在原有计算机系统处理流程中加入了加解密和减少写次数两个处理单元，数据从内存到达 CPU 的时间会产生额外延迟. 此外，在减少写次数的处理单元中需要读取原始数据块进行比较，这也带来了额外系统开销，增加了延迟. 但在处理过程中，数据预处理和读取原始内存数据部分可以并行执行，这在一定程度上减少了系统开销. 图 7 为我们的实验结果. 实验中用无保护措施的系统作为标准，记为 100%. 相应地统计了只有加密单元和加密＋减少写操作同时作用的系统配置下的系统性能情况. 加密单元带来的平均系统延迟时间为 1.6%，减少写次数的处理单元带来的平均系统延迟时间为 2%，系统整体平均增加延迟时间为 3.6%.

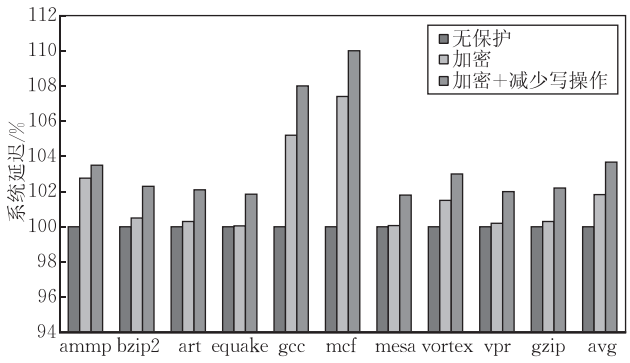

图 7 系统性能比较

4.3　对 PCM 内存写次数的影响

本组实验的目的主要是验证我们提出的减少写操作方法可以极大减少写次数. 对比的是 Flip-N-write 算法. 该算法思想是判断汉明距离是否大于整组数据位数的一半. 若大于，则将数据全部求反，然后再修改内存中的数据. 本组实验的 cache line 长度为 256 位，写回的数据为随机生成的数据集. 两种方法在同一个实验下使用的数据相同. 实验结果如图 8 所示，x 轴为写回内存的次数，y 轴为总共修改的数据位数. 当随机数据写回 PCM 内存 10 000 次时，我们的方法平均只修改了 89 386 比特位，Flip-N-write 方法则在相同随机数据的情况下需要修改 707 333 比特位；当随机数据写回 10 000 000 次时，我们的方法只需要修改 90 107 606 次，而 Flip-N-write 方法则需要修改 707 557 428 次. 由实验数据对比，可以看出我们的方法可以更好地减少 PCM 内存的修改位数，从而提高 PCM 内存的使用寿命.

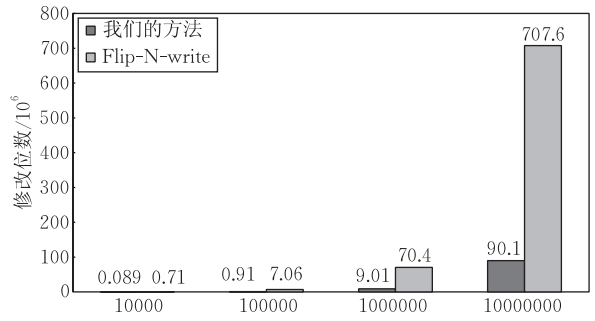

图 8　数据位数修改对比

4.4　与其它算法的比较

数据经过加密操作后，被修改的数据经过扩散作用，需要修改的数据位普遍增多. 很多减少写操作的方法经过加密操作后，效果大打折扣. 图 9 给出了几种算法在带有加密处理的情况下和我们算法的比较. 可以看出我们的算法可以使 4 GB 容量的 PCM 内存平均延长 3 年寿命. 若不加入减少写操作处理，则该内存只能稳定运行将约 2 年时间. 我们的方法可以使该内存延长 2.6 倍的平均使用寿命.

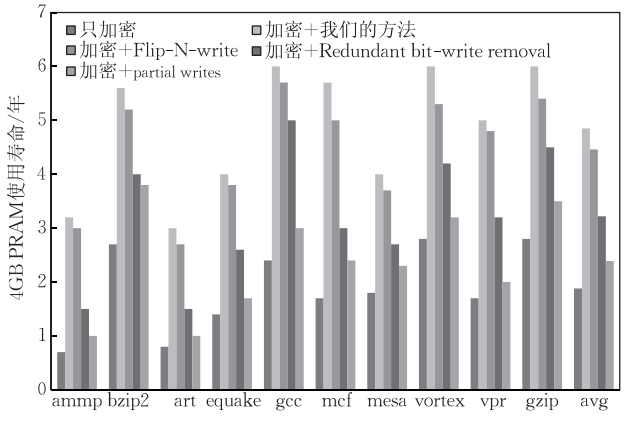

图 9　PRAM 内存使用寿命对比

5　结　论

新型基于相变存储器的内存不仅会具有低功耗、高集成度等诸多优势，同时也会带来安全性隐患. 它的非易失性使系统停机后，内存数据不会消失，别有用心的攻击者会分析提取内存中的数据，获得隐私数据. 本文设计了一个针对相变内存的数据保护方案，主要包括基于计数器的机密单元和减少写操作单元. 实验表明加入加密操作后，性能下降并不多，同时减少写操作的机制可以有效提高 PCM 的写寿命.

致　谢　本文作者得到了清华大学计算机科学与技术系操作系统实验室的老师与同学们的许多帮助和有益建议，在此表示感谢！

参　考　文　献

[1] Halderman J A, Schoen S D, Heninger N et al. Lest we remember: Cold-boot attacks on encryption keys//Proceedings of the 17th Conference on Security Symposium. San Jose, CA, 2008: 45-60

[2] Zhou P, Zhao B, Yang J et al. A durable and energy efficient main memory using phase change memory technology//Proceedings of the 36th International Symposium on Computer Architecture. Austin, USA, 2009: 14-23

[3] Qureshi M K, Srinivasan V, Rivers J A et al. Scalable high performance main memory system using phase change memory technology//Proceedings of the 36th International Symposium on Computer Architecture. Austin, USA, 2009: 24-33

[4] Lee B C, Ipek E, Mutlu O et al. Architecting phase change memory as a scalable dram alternative//Proceedings of the 36th International Symposium on Computer Architecture. Austin, USA, 2009: 2-13

[5] Cho S, Lee H. Flip-N-Write: A simple deterministic technique to improve PRAM write performance, energy and endurance//Proceedings of the 42nd Annual IEEE/ACM International Symposium on Microarchitecture, New York, USA, 2009: 347-357

[6] Qureshi M K, Karidis J, Franceschini M et al. Enhancing lifetime and security of PCM-based main memory with start-gap wear leveling//Proceedings of the 42nd Annual IEEE/ACM International Symposium on Microarchitecture. New York, USA, 2009: 14-23

[7] Yang J, Zhang Y, Gao L. Fast secure processor for inhibiting software piracy and tampering//Proceedings of the 36th Annual IEEE/ACM International Symposium on Microarchitecture. San Diego, CA, 2003: 351-361

[8] Binkert N L, Dreslinski R G, Hsu L R et al. The M5 simulator: Modeling networked systems. IEEE Micro, 2006, 26(4): 52-60

ZHAO Peng, born in 1985, Ph. D. candidate. His research interests are emerging memory architecture, operating system, computer security.

ZHU Long-Yun, born in 1986, M. S.. His research interests include emerging memory architecture, operating system.

Background

Phase-change Memory is a emerging memory which has stronger high density, low power consumption, non-volatile, it has such advantages as replaces the existing DRAM Memory. Although have the strength of the numerous advantages, it is still to be faced with many new challenges. An important characteristic of PCM is volatile, stored in PCM storage unit in the information without power supply can remain permanently, like Flash disk with the same data such as non-volatile characteristics. PCM is not only can replace DRAM, also can replace the disk or currently mature Flash memory. As in the modern computer system architecture, memory is the possession of the core position, even if in the hard-disk or network transmission of data encryption method such as the protection, once the data to process, will be a memory, when in data in memory to case from the protection of the original will fall, for example, from cipher text into plaintext participate in computing. This will give the attacker favor. The attacker can directly on the memory scan data and data analysis, looking for interesting data, such as user's bank account and password, user's personal privacy data, etc. Even if the system after power off still can obtain data. When PCM become main memory, the attacker simply after power off memory to insert PCM in the computer can do the rest of the step-by-step data acquisition steps. This will give the computer system caused tremendous security hidden danger.

Another challenge is because itself exists the problem of limited number of writing. Each of the storage unit of the current PCM can write about 10^8 times the number of memory storage unit, as the data update will be very frequently, when writing to cap the number, the storage unit will failure causing the loss of data in a certain degree, the lower the memory of their own stability.

This paper analyzes the existing in PCM data protection challenges faced, put forward a kind of based on encryption technology and reduce the number of phase change memory write method, this method not only can protect based on phase change memory data in memory, even in the power system under the condition of sensitive data in memory and cannot be the attacker get, at the same time greatly extend the service life of the memory system, strengthening the non-volatile memory data confidentiality and reliable protection.