一种具有近内存移位旋转功能和 42.6 GB/s 读取带宽的 22 纳米 1 Mb 1024 位读取数据保护 STT-MRAM 宏，适用于安全感知移动设备

邱彦程, 张东成, 李俊颖, 洪哲民, 张光堂, 薛承鑫, IEEE 研究生会员, 吴思妍, 高慧瑶, 陈鹏 □ , 黄晓瑜, 滕世熙, 罗杰普 □ , 施宜君 □ , IEEE 会员, 池育德, IEEE 会员, 张宗永, IEEE 会士, 金毅 ⊕ , IEEE 高级会员, 张孟凡 ⊕ , IEEE 会士

摘要——使用宽输入输出 (IO) 非易失性存储器 (NVM) 开发安全感知移动设备的进展受到高峰值电流、高读取带宽 (BWR) 所需的大面积开销以及 NVM 与逻辑块之间数据传输的显著能耗的阻碍。此外，存储在 NVM 中的数据容易受到逆向工程攻击。本工作提出了一种高 BWR 安全感知的近内存计算自旋转移矩磁性随机存取存储器 (STT-MRAM) 宏，采用多位电流模式感测放大器 (MB-CSA) 来降低宽 IO 访问的峰值电流和能耗，结合 MB-CSA 的近内存移位和旋转功能 (NSRF) 以减少面积开销，并在单个周期内完成读取和逻辑操作，以及一种基于 XOR 的逆向工程防护内存数据保护器，以保护存储在 NVM 中的数据免受逆向工程攻击。采用代工厂嵌入式 22 纳米 STT-MRAM 制造的 1-Mb 1024 位读取 STT-MRAM 宏，本工作实现了 42.67 GB/s 的 BWR 和 0.23 pJ/b 的能耗。包含 NSRF 电路将面积开销减少了 33.3%，而延迟仅增加了 170 ps。

关键词——高带宽，近内存计算 (NMC)，安全感知移动设备，自旋转移矩磁性随机存取存储器 (STT-MRAM)。

I. 引言

许多使用安全哈希算法 (SHA) 或高级加密标准 (AES) 进行数据加密的安全意识移动设备需要宽输入输出 (IO) 非易失性存储器 (NVM)[1]-[12] 来存储用户 ID、固件代码和计算参数。这些设备还需要短的读取访问时间 (t_{AC})、高读取带宽 (BWR) 以及移位/旋转功能。自旋转移矩磁性随机存取存储器 (STT-MRAM) 是先进工艺节点的主要片上 NVM [13]-[17]；然而，它需要小偏移感测放大器 (SAs)[18]-[20] 来针对小的隧道磁阻 (TMR) 比率进行稳健的读取操作，这大大增加了面积开销和读取能量 (E_{RD})。如图 1 所示，为安全相关应用设计 STT-MRAM 宏面临四个主要挑战。

1) 使用大量 SAs 进行宽并行 IO 读取以实现短的 t_{AC} 会导致高峰值电流 (I_{PEAK}) 和大的面积开销。使用较少的 SAs 进行顺序宽 IO 读取可以减少 I_{PEAK} 和面积开销；然而，这会导致长的 t_{AC} 和低的 BWR。

2) 具有高 I_{PEAK} 的 MRAM 宏可能会降低电源电压 (VDD) 的完整性，通常会导致同一芯片中噪声敏感模块的故障。

3) 传统的存储器-逻辑分离方案在基于 NVM 的安全逻辑操作中会引入长延迟 (两个周期: 宽 IO 存储器读取 + 触发器 (FF) 移位/旋转)。

4) 旨在保护 NVM 数据的传统逻辑锁定方案容易受到逆向工程攻击，导致安全密钥的泄露。

本文介绍了一种 22 纳米 1 兆比特 STT-MRAM 宏单元，具有双模式操作 [宽 IO 存储器和近存储器计算 (NMC)] 以及抗逆向工程攻击的特性。所提出的 1 兆比特宏单元在使用 0.85 V 供电电压的情况下，实现了最大数量的数据输出操作 (1024 位)，t_{AC} 为 2.75 纳秒。在存储器模式下，该工作在 BWR(42.67 GB/s) 和 E_{RD} (0.23pJ/b) 方面优于所有已报道的非易失性存储器宏单元。该工作还首次展示了具有 NMC 功能的 MRAM 宏单元，逻辑面积减少了 33.3%，并且在非易失性存储器访问后，1 位移位/旋转操作的延迟仅为 170 皮秒。所提出的基于 XOR 的抗逆向工程存储器数据保护器还采用了逻辑混淆方案来保护电路免受逆向工程攻击，同时在面积、计算速度和能耗方面仅带来 2% 的损失。

稿件于 2021 年 5 月 8 日收到，2021 年 8 月 9 日修订，2021 年 9 月 2 日接受。发表日期为 2021 年 9 月 29 日，当前版本日期为 2022 年 5 月 26 日。本文由副主编 Vivek De 批准。本工作部分由台积电联合开发项目 (JDP)、台湾半导体研究所 (TSRI) 以及台湾科技部 (MOST) 支持。(通讯作者: 张孟凡。)

邱彦程、张东成、李俊颖、洪哲民、张光堂、薛承鑫、吴思妍、高慧瑶、陈鹏、黄晓瑜和邓世希就职于国立清华大学电机工程系，地址: 台湾新竹市 30013(电子邮件:ppkkp00032@gapp.nthu.edu.tw)。

罗杰普、施宜君、池育德和张宗永就职于台湾积体电路制造公司 (TSMC)，地址: 台湾新竹市 30075。

金毅就职于佛罗里达大学电气与计算机工程系，地址: 美国佛罗里达州盖恩斯维尔市 32611(电子邮件:yier.jin@ece.ufl.edu)。

张孟凡就职于国立清华大学电机工程系，地址: 台湾新竹市 30013，同时就职于台湾积体电路制造公司 (TSMC)，地址: 台湾新竹市 30075(电子邮件:mfchang@ee.nthu.edu.tw)。

本文中一幅或多幅图的彩色版本可在 https://doi.org/10.1109/JSSC.2021.3112182 获取。

数字对象标识符 10.1109/JSSC.2021.3112182

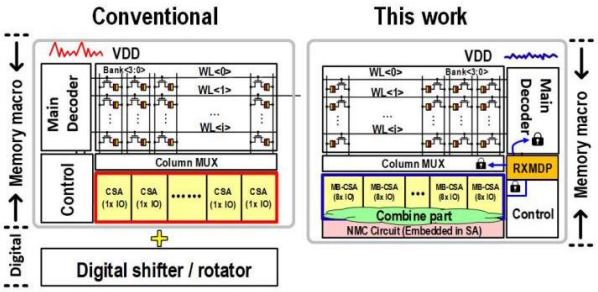


图 1. 所提出的 1Mb STT-MRAM 宏的概述。

本文的其余部分组织如下。第二部分描述了所提出的高带宽多位电流模式感测放大器 (MB-CSA)。第三部分描述了所提出的近存移位和旋转功能 (NSRF)。第四部分描述了所提出的基于 XOR 的安全反工程防护内存数据保护器 (RXMDP)。第五部分展示了性能和测量结果。第六部分总结了本工作。

II. 用于高带宽 STT-MRAM 宏的所提出的多位电流模式感测放大器

A. 高带宽读取方案

图 3(a) 展示了所提出的 MB-CSA 的概念以及两种传统的多位数据读取方案: 并行感测和顺序感测。每个传统的电流模式感测放大器 (CSA) 需要一个参考电流 (I_{REF}) 来感测 1 位数据。并行感测方案需要八个 I_{REF} 和八个 CSA 来感测 8 位数据。顺序感测方案需要八个周期来感测 8 位数据。相比之下，所提出的 MB-CSA 仅使用两个参考电流 (I_{REF_P} 和 I_{REF_AP})，并且仅需一个周期即可感测 8 位数据。

存储单元电流定义为当无读取干扰电压施加到单元时流过 STT-MRAM 单元的电流。I_{REF_AP} 和 I_{REF_P} 是在复制单元阵列 (RCA) 中使用多个 STT-MRAM 单元 (本工作中为八个单元) 生成的。I_{REF_P} 表示 P 状态下八个 MRAM 单元的平均单元电流，而 I_{REF_AP} 表示 AP 状态下八个 MRAM 单元的平均单元电流。平均效应降低了 I_{REF_AP} 和 I_{REF_P} 对与 MRAM 单元电阻相关的工艺变化的敏感性。

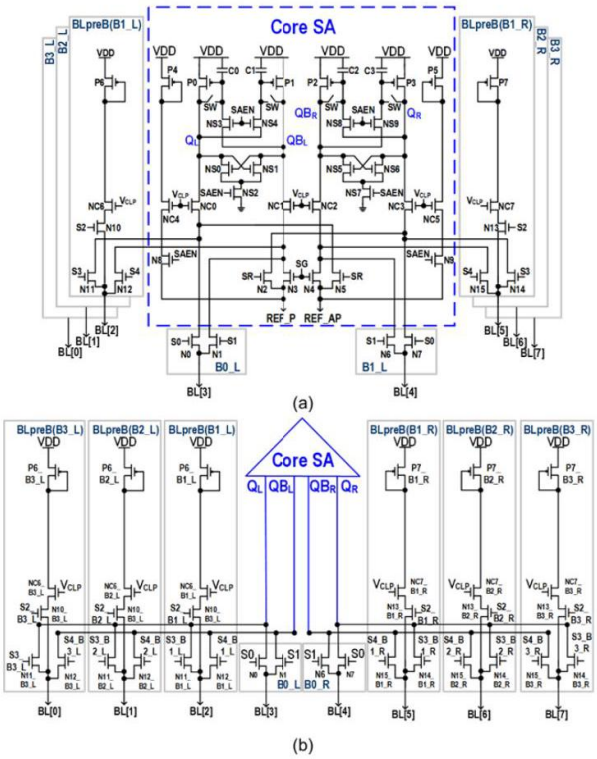


图 2. 所提出的 MB-CSA 的 (a) 核心 SA 和 (b) 分支 (B0-3_R 和 B0-3_L) 的电路结构。

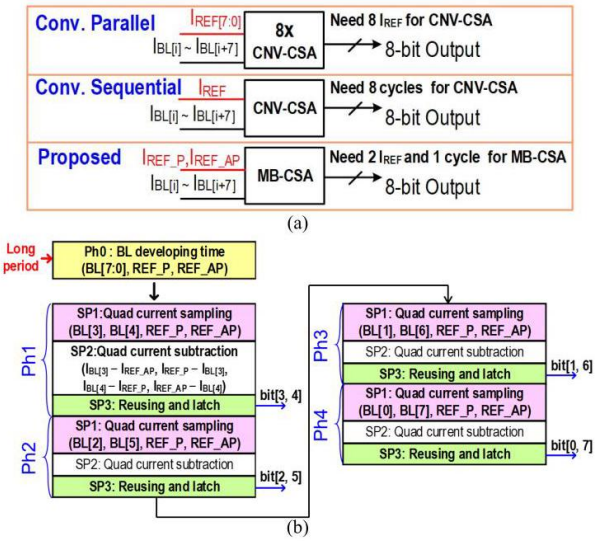


图 3. 所提出的 MB-CSA 的概念。(a) 传统并行、传统顺序和所提出的多位传感方案的概念。(b) 所提出的 MB-CSA 的操作流程。

许多 CSA [2], [25], [26] 已被开发出来，旨在提高读取性能。在 [25] 中，使用电流采样来减少输入偏移。在 [26] 中，使用两个参考电流和距离竞赛来增加传感裕度。在 [2] 中，使用电流采样和电流路径切换来同时加倍传感裕度并减少输入偏移。然而，需要注意的是，这些工作仅专注于提高 1 位传感性能。对于涉及宽 IO 读取操作的应用，这些方法仍然依赖于传统的并行或顺序传感方案，这些方案在读取 8 位数据时会消耗大量面积或导致长延迟。

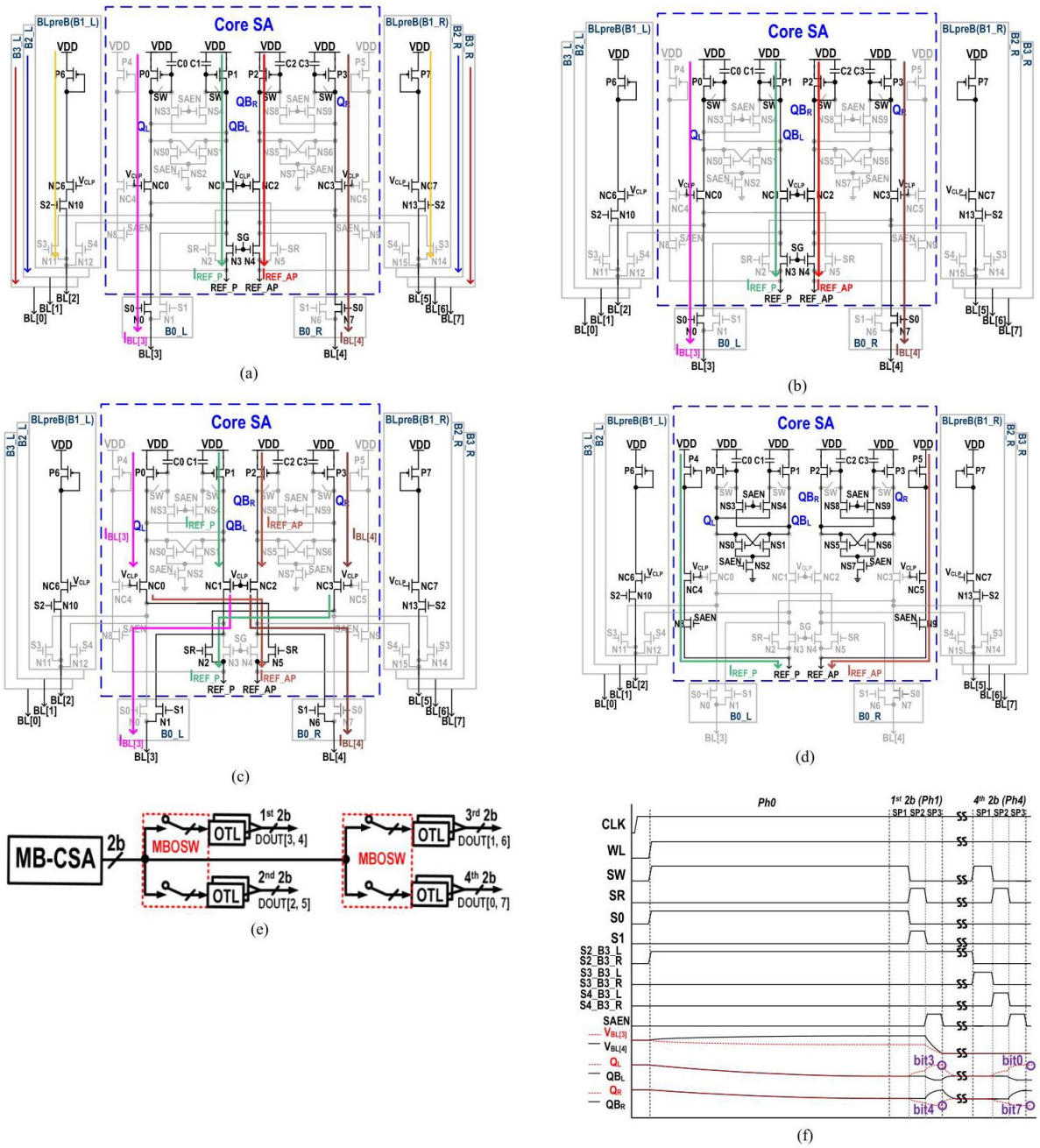


图 4. MB-CSA 的逐阶段操作:(a) Ph0，BL 发展，(b) SP1，四重电流采样 (旧)，(c) SP2，四重电流减法，(d) SP3，重用和锁存，(e) MB-CSA 与输出锁存器之间的连接，以及 (f) MB-CSA 操作波形。

B. 所提出的 MB-CSA 的结构

图 2 展示了所提出的 MB-CSA 的结构，该结构能够在单个内存访问周期内实现 8 位输出。MB-CSA 包括一个核心比较器 (CMP) 和一个六分支位线预充电器 (BLpreB)。核心 CMP 包含四个 PMOS (P0-P3)、两对电容器 (C0 和 C1 以及 C2 和 C3)、两个门控 (SAEN 控制) 交叉耦合 *N* 锁存器 (NS0-NS2 和 NS5-NS7)、两个非门控 *N* 锁存器 (NS3 和 NS4 以及 NS8 和 NS9)、四个位线 (BL) 电压钳位晶体管 (NC0-NC3) 以及八个 NMOS 路径开关 (N0-N7)。每个 BLpreB(例如 B1_L) 包括一个预充电 PMOS (P6_b1_L)、一个钳位 NMOS (NC6) 和三个路径开关 (N11 和 N12)，通过确保八个 BL 的位线预充电任务在同一周期内完成 (与传统感测方案相同) 来减少时序开销。

C. 所提出的 MB-CSA 的操作

图 3(b) 展示了 MB-CSA 的操作，包括一个 BL 开发阶段 (Ph0) 和四个重复阶段 (Ph1-Ph4) 以生成 8 位输出。每个阶段通过三个短周期子阶段 (SP1-SP3) 生成 2 位输出。在 Ph1 阶段，开关 S0 和 S1 开启，使 MB-CSA 能够同时感知 BL[3] 和 BL[4]。在 Ph2 阶段，开关 S3_B1_L 和 S3_B1_R 开启，使 MB-CSA 能够感知 BL[2] 和 BL[5]。在 Ph3 阶段，开关 S3_B2_L 和 S3_B2_R 开启，使 MB-CSA 能够感知 BL[1] 和 BL[6]。在 Ph4 阶段，开关 S3_B3_L 和 S3_B3_R 开启，使 MB-CSA 能够感知 BL [0] 和 BL [7] 。

在下文中，我们描述了 Ph0 和 Ph1 在感知 BL[3] $\left(I_{\mathrm{BL}[3]}\right)$ 和 BL[4] ($I_{\mathrm{BL}[4]}$) 的 BL 电流以进行前 2-b 输出的操作。图 4(a)-(f) 展示了 MB-CSA 的操作和波形。每个读取操作在相位 0 (Ph0) 期间启动，在此期间预充电 PMOS(P0-P3、P6_B3_L、P6_B2_L、P6_B1_L、P7_B3_R、P7_B2_R 和 P7_B1_R) 同时将 BL[7:0] 预充电到目标 BL 读取电压 (V_{BLRD})，以便进行电流模式传感，与传统 CSA 相同。需要注意的是，Ph0 具有较长的 BL 发展时间 (T_{BLD})，并且在 BL 长度较长的情况下通常主导读取访问时间 (t_{AC})。参考输入节点 (REF_P 和 REF_AP) 处的 $I_{\mathrm{REF\_P}}$ 和 $I_{\mathrm{REF\_AP}}$ 由 RCA 使用电流镜像电路提供。在 Ph1, SW = ON 和 SG = S0 = 1 的子相位 1(SP1，四倍电流采样) 中。

PMOS 晶体管 (P0-P3) 的栅源电压用于电流采样操作 [18]，以抑制给定位线电流 ($I_{\mathrm{BL}[3]}$ 和 $I_{\mathrm{BL}[4]}$) 和参考电流 ($I_{\mathrm{REF\_AP}}$ 和 $I_{\mathrm{REF\_P}}$) 的输入偏移。在 SP2(四电流减法) 中，SW = OFF, SG = S0 = 0 和 S1 = SR = 1 。节点 $\mathrm{Q_L}$ 随后连接到 P0 $\left(I_{\mathrm{BL}[3]}\right)$ 和 NC0 $\left(I_{\mathrm{REF\_AP}}\right)$，节点 $\mathrm{Q_{BL}}$ 连接到 P1 $\left(I_{\mathrm{REF\_P}}\right)$ 和 NC1 $\left(I_{\mathrm{BL}[3]}\right)$，节点 $\mathrm{Q_{BR}}$ 连接到 P2 $\left(I_{\mathrm{REF\_AP}}\right)$ 和 NC2 $\left(I_{\mathrm{BL}[4]}\right)$，节点 $\mathrm{Q_R}$ 连接到 P3 $\left(I_{\mathrm{BL}[4]}\right)$ 和 NC3 $\left(I_{\mathrm{REF\_P}}\right)$。在给定周期 T_{SP2}, the voltage swings on nodes $\mathrm{Q_L}$ $\left(\Delta V_{\mathrm{QL}}\right)$ 和 $\mathrm{Q_{BL}}$ $\left(\Delta V_{\mathrm{QBL}}\right)$ 中，$T_{\mathrm{SP2}} \times \left(I_{\mathrm{BL}[3]} - I_{\mathrm{REF\_AP}}\right) / C_{\mathrm{QL}}$ 和 $T_{\mathrm{SP2}} \times \left(I_{\mathrm{REF\_P}} - I_{\mathrm{BL}[3]}\right) / C_{\mathrm{QBL}}$，而节点 $\mathrm{Q_R}$ $\left(\Delta V_{\mathrm{QR}}\right)$ 和 $\mathrm{Q_{BR}}$ $\left(\Delta V_{\mathrm{QBR}}\right)$ 上的电压摆幅为 $T_{\mathrm{SP2}} \times \left(\mathrm{I}_{\mathrm{BL}[4]} - I_{\mathrm{REF\_P}}\right) / C_{\mathrm{QR}}$ 和 $T_{\mathrm{SP2}} \times \left(I_{\mathrm{REF\_AP}} - I_{\mathrm{BL}[4]}\right) / C_{\mathrm{QBR}}$. $C_{\mathrm{QL}} / C_{\mathrm{QBL}} / C_{\mathrm{QR}} / C_{\mathrm{QBR}}$，表示节点 $\mathrm{Q_L}/\mathrm{Q_{BL}}/\mathrm{Q_R}/\mathrm{Q_{BR}}$ 的寄生电容。在 SP3, S1 = SR = 0 和 SAEN = 1 中。随后，开关 NS3、NS4、NS8 和 NS9 被打开以形成两个锁存器 (锁存器 1:NS0-P0 和 NS1-P1；锁存器 2:NS5-P2 和 NS6-P3)，根据 $\mathrm{Q_L} - \mathrm{Q_{BL}}$ $\left(\Delta V_{\mathrm{QL-QBL}}\right)$ 和 $\mathrm{Q_R} - \mathrm{Q_{BR}}$ $\left(\Delta V_{\mathrm{QR-QBR}}\right)$ 之间的电压差生成两个差分数字输出 ($\mathrm{Q_L}/\mathrm{Q_{BL}}$ 和 $\mathrm{Q_R}/\mathrm{Q_{BR}}$。两个 MB-CSA 输出开关 (MBOSW [3, 4]) 被打开，将 $\mathrm{Q_L}/\mathrm{Q_{BL}}$ 和 $\mathrm{Q_R}/\mathrm{Q_{BR}}$ 值传递到两个相应的输出锁存器 (OTL；即 OTL[3, 4])，这些锁存器也用于传统的内存宏。从阶段 2 到阶段 4，相同的 SP1-SP3 操作重复进行 BL [2, 5] (第二次 2 位读取操作)、BL[1, 6](第三次 2 位读取操作) 和 BL[0, 7](第四次 2 位读取操作)。

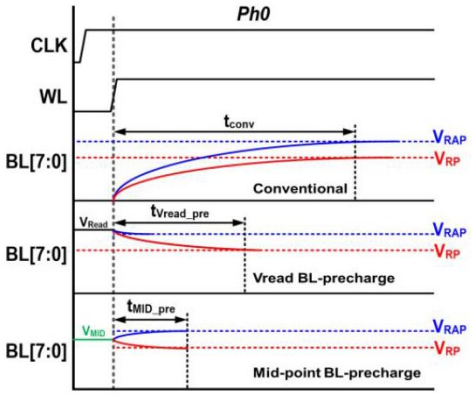
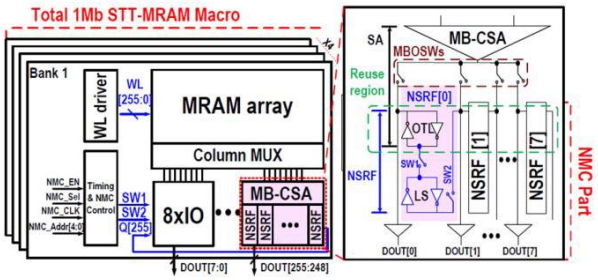


图 5. 传统选择预充电 (BL-SP)、位线初始高电平 (BL-IH) 和所提出的 MP-BLV 方案的概念波形。

D. 中点位线初始电压方案

本研究开发的中点位线初始电压 (MP-BLV) 方案旨在缩短读取延迟。图 5 展示了所提出的 MP-BLV 方案与传统选择预充电 (BL-SP) 和位线初始高电平 (BL-IH) 方案的波形对比概念图 [21]。基于典型的 RC 行为，位线发展时间 (T_{BLD}) 随着电压的增加而增加。由于隧道磁阻比 (TMR) 较小，执行电流模式读取操作的 STT-MRAM 的位线电压 (V_{RD}) 必须足够准确和稳定，以确保稳健的电流模式传感操作。当使用选择预充电 (SP) 方案进行传统的电流模式读取操作时，所有位线在待机模式下初始处于 0 V，并且在启用电流传感放大器 (CSA) 之前，选定位线 (即 BL[0]) 从地 (0V) 充电至 V_{RD}。因此，当位线长度较长时，选择预充电方案会遭受较长的位线发展时间 (T_{BLD})。注意，$V_{\mathrm{RD-AP}}$ 指的是位线发展阶段 (Ph0) 结束时稳定的 V_{RD}，此时被读取的单元处于反平行 (AP) 状态，而 $V_{\mathrm{RD-P}}$ 指的是位线 Ph0 结束时稳定的 V_{RD}，此时被读取的单元处于平行状态 (P)。在待机模式下将初始位线电压设置为 V_{RD} 是抑制 T_{BLD} 的直接方法，作为传统选择预充电读取方案的替代方案。然而，需要注意的是，如果 BL-IH 方案选择 $V_{\mathrm{RD}} = V_{\mathrm{RD-AP}}$，则在读取 AP 单元时 T_{BLD} 为零，但在读取 P 单元时则显著。这是由于 RC 的充放电特性导致位线电压 (V_{BL}) 从

$V_{RD\text{-}AP}$ 摆动到 $V_{RD\text{-}P}$ 所需的长时间稳定时间。同样，如果 BL-IH 方案选择 $V_{RD} = V_{RD\text{-}P}$，则 T_{BLD} 受到位线电压从 V_{RD-P} 摆动到 V_{RD-AP} 所需的长时间稳定时间的影响。在所提出的 MP-BLV 方案下，所有位线在位线发展阶段 (Ph0) 之前被设置为 V_{RAP} 和 V_{RP} 之间的中点电压 (V_{MID})。位线电压从 V_{MID} 摆动到 V_{RAP} 的发展时间几乎与从 V_{MID} 摆动到 V_{RP} 的时间相同。因此，所提出的 MP-BLV 方案中的 T_{BLD} 比传统的 BL-SP 和 BL-IH 方案中的更短。



(a)

Shift / Rotate table				
Mode	NMC_EN	NMC_Sel	NMC_Addr[4:0]	Operation
Wide-IO	0	X	X	Normal SA data out
Shift	1	1	00000	No shift
			00001	Shift 1 bit
			⋮	⋮
			11111	Shift 31 bits
Rotate	1	0	00000	No rotate
			00001	Rotate 1 bit
			⋮	⋮
			11111	Rotate 31 bits

(b)

图 6. (a) 所提出的 NSRF 的框图和电路结构。(b) NSRF 的操作表。

III. 支持移位和旋转操作的 NSRF 方案

A. 安全应用中的逻辑操作

诸如 AES 和 HASH 等安全算法使用了大量的多位移位和旋转操作。例如，AES-128 算法 [27] 在 ShiftRow 操作中需要 8 位、16 位和 24 位的旋转。SHA-256 算法 [28] 在将 16 个 32 位字扩展为 64 个 32 位字时，需要 7 位、17 位、18 位和 19 位的旋转操作，以及 3 位和 10 位的移位操作。它还在主计算循环中使用了 2 位、6 位、11 位、13 位、22 位和 25 位的旋转操作。

在之前的工作 [29]-[31] 中，移位和旋转操作所需的大量多路复用器 (MUX) 和广泛的布线导致了相当大的面积开销，并且缺乏许多安全相关算法所需的可配置性。

所提出的 NSRF 通过在 D 触发器 (DFF) 链中使用输出缓冲器中的 OTL 作为主锁存器，支持低功耗和低面积开销的数字电路进行多位移位和旋转配置。

B. 所提出的 NSRF

图 6(a) 展示了所提出的 NSRF 的框图和电路结构。每个存储体包含 256 个 NSRF 和 32 个 MB-CSA。每个 MB-CSA 连接了总共 8 个 NSRF。NSRF 在输出缓冲器中复用 OTL 作为 DFF 链中的主锁存器，用于 NSRF 中的可配置移位器/旋转器。因此，每个 NSRF 仅包含一个从锁存器 (LS) 和两个开关 (SW1 和 SW2)。该 NSRF 除了存储器模式外还包括其他控制信号: 用于移位/旋转位数 (k) 的 NMC_Addr、用于 DFF 时序的 NMC_CLK 以及用于选择移位和旋转功能的 NMC_Sel。在存储器模式下，NMC_EN = 0 且 SW1 = SW2 = OFF，以将 LS 与常规输出缓冲器的 OTL 断开。因此，NSRF 不会影响常规的存储器读取操作。如图 6(b) 所示，NMC_EN 在计算模式下被激活。当 NMC_SEL = 1 时，NSRF 能够根据信号 NNC_Addr[4:0] 的设置执行 1-31 位移位操作。当 NMC_Addr[4:0] = 11111 时，NSRF 执行 31 位移位操作。当 NMC_SEL = 0 时，NSRF 能够执行 1-31 位旋转操作。与移位操作类似，当信号 NNC_Addr[4:0] = 11111 时，NSRF 执行 31 位旋转操作。图 7 展示了 NSRF 的移位和旋转操作。每个 NSRF 操作分两步实现。对于 1 位 NSRF 移位操作，步骤 1(SW1 = ON 且 SW2 = OFF) 涉及将存储在 OTL 中的数据 (Q)(从 MBCSA 读取的数据) 移动到同一 NSRF 的 LS 中。步骤 2(SW1 = OFF 且 SW2 = ON) 涉及将位于 LS(即 NSRF[0]) 的数据 Q 传递到其相邻 NSRF(即 NSRF[1]) 的 OTL，同时 0 V 被应用到 NSRF[0] 的 LS。对于 4 位移位操作，上述 1 位移位操作重复四次。如图 7(b) 中的示例所示，NSRF 操作开始时 DOUT[7:0] = 10100011，经过四次短 NSRF 操作后

变为 DOUT[7:0] = 00110000。旋转操作与移位操作类似；然而，NSRF[0] 的 OTL 的输入来自同一存储体的 NSRF[255] 或另一个 IO。相同的两步 NSRF 过程可以重复 k 次以移位或旋转 k 位。

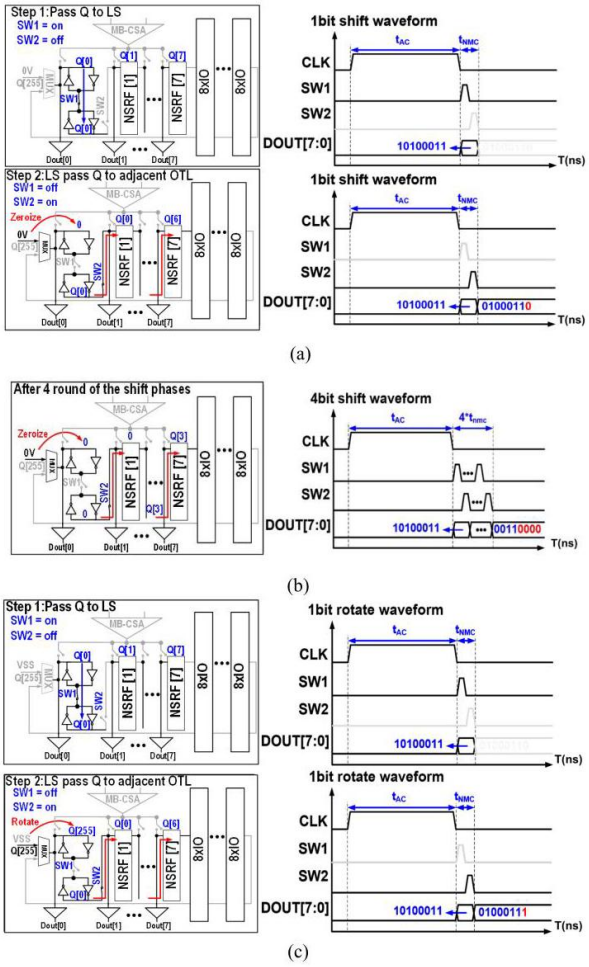


图 7. (a) 1 位移位 (旧)、(b) 4 位移位和 (c) 1 位旋转操作的详细操作和波形。

IV. 提出的 RXMDP

A. RXMDP 的背景与结构

本研究提出了一种 RXMDP 来保护存储在 STT-MRAM 中的数据。先前的逻辑锁定电路 [22]-[24] 主要针对功能块内的计算逻辑电路，以确保仅在提供正确的外部 KEY 信息时才能准确计算数据。然而，这种方法可能无法直接应用于存储器控制器，因为典型存储器宏中使用的解码器的电路和功能已被广泛理解。这使得有经验的工程师能够追踪存储器宏中添加的逻辑锁定电路，以获取与 KEY 相关的信息。在典型的存储器宏中，用于读写控制、地址和数据 IO 的引脚是明确定义的。任何用于输入 KEY 数据的额外引脚都可能泄露逻辑锁定功能的使用。这给那些希望使用数据保护的独立存储器芯片来修改预先设计的系统 [即印刷电路板 (PCB)] 的工程师带来了额外的负担。在当前的研究中，我们通过让所提出的 RXMDP 对解码器以及 IO 电路应用基于 XOR 的加密和解密逻辑来加密访问的存储器位置和数据，从而实现了确保安全性所需的长 KEY 长度。为了防止数据保护器使用特征的泄露，RXMDP 重用了存储器宏的原始引脚来输入 KEY 数据。图 8 显示了所提出的 RXMDP 的块结构，该结构在所提出的 STT-MRAM 宏中实现。RXMDP 包括 KEY 控制中心 (KCC)、基于 XOR 的预解码器 (XOR-PD)、基于 XOR 的数据处理单元 (XOR-DPU)、KEY 存储单元 (KSU) 和 m 位 KEY 输入信号。KCC 包括一个 KEY 控制单元 (KCU) 和 m 个路径切换单元 (PSU)。请注意，$m (m = N_{\mathrm{WIO}} + N_{\mathrm{ADR}}$ 的值等于读写电路中的 IO 位计数 (N_{WIO}) 和输入地址位计数 (N_{ADR}) 的总和。KSU 由用于 XOR-PD 的 N_{ADR} 个 D 型触发器 (K-DFF-PD) 和用于 XOR-DPU 的 N_{WIO} 个 DFF (K-DFF-DPU) 组成。

B. 所提出的 RXMDP 的操作流程

所提出的 RXMDP 具有三种操作模式: 密钥更新模式、安全访问模式和密钥重置模式。在密钥更新模式下，用户提供的密钥数据通过 PSU 和内存宏中的常规控制和数据输入引脚插入到 KSU 中。在安全访问模式下，所提出的 XOR-DPU 和基于 XOR 的预解码器 (XOR-PD) 使用存储在 K-DFF-DPU 和 K-DFF-PD 中的密钥数据进行安全写入 (加密操作) 或读取 (解密操作)。在密钥重置模式下，存储在 K-DFF-PD 和 K-DFF-DPU 中的密钥数据被擦除并重置为设计者确定的模式 (在本工作中为全 KEY $=0$)。此操作确保在内存宏完成安全模式访问后，KEY 数据不会保留在 KSU 中。接下来将详细介绍这三种模式中使用的操作和相应电路。图 9 展示了所提出的 RXMDP 的高级流程图。内存写入操作包括一个密钥更新周期以获取用户提供的写入密钥 (即 KEY-W)，至少一个安全写入访问周期以基于 KEY-W 加密写入数据，以及一个密钥重置周期以擦除与密钥相关的信息。内存读取操作与写入操作类似，包括一个密钥更新周期以获取用户提供的读取密钥 (KEY-R)，至少一个安全读取访问周期以基于 KEY-R 解密输出数据，以及一个密钥重置周期以擦除与密钥相关的信息。如果 KEY-R 与 KEY-W 不同，则读取的数据将不会与在安全写入访问期间写入内存的数据匹配。

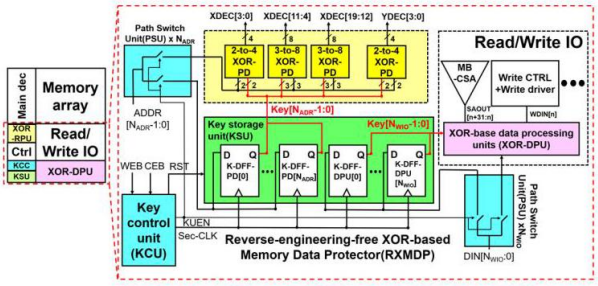


图 8. 所提出的 RXMDP 的框图和电路结构。

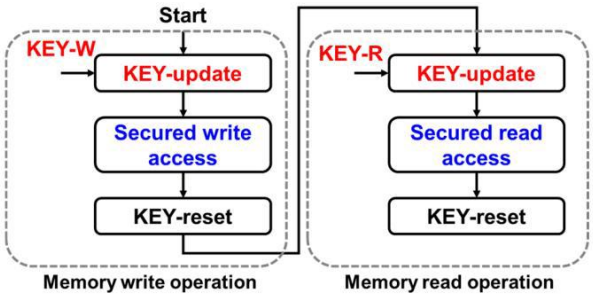


图 9. 所提出的 RXMDP 的高级流程图。

C. 密钥更新: 电路与操作

所提出的 RXMDP 重用了数据输入 (DIN) 和输入地址 (ADDR) 的引脚，用于将密钥数据传输到密钥存储单元 (KSU)。为了避免需要额外的引脚并保持安全功能的隐蔽性，我们仅在通过控制命令引脚 (例如 CEB 和 WEB) 提供预设计模式时允许访问密钥更新模式。图 10 显示了密钥更新模式下的操作波形，其中 CEB $=1$ 用于禁用常规内存访问。在密钥更新操作开始时，选定的输入控制信号根据预设计模式进行切换，以激活密钥控制单元 (KCU) 块并传输密钥更新使能 (KUEN $=1$) 信号。KUEN 信号使能电源单元 (PSU)，创建从 DIN 引脚到 K-DFF-DPU 数据输入以及从 ADDR 到 K-DFF-RPD 数据输入的路径。同时，从 DIN 引脚到写入电路的路径以及从输入地址引脚到 XOR-RPD 的路径被禁用。在 KUEN 信号上升沿开始的预定延迟周期后，安全时钟 (Sec-CLK) 从 0 上升到 1，以将数据传递到 DFF(K-DFF-RPD 和 K-DFF-DPU)。

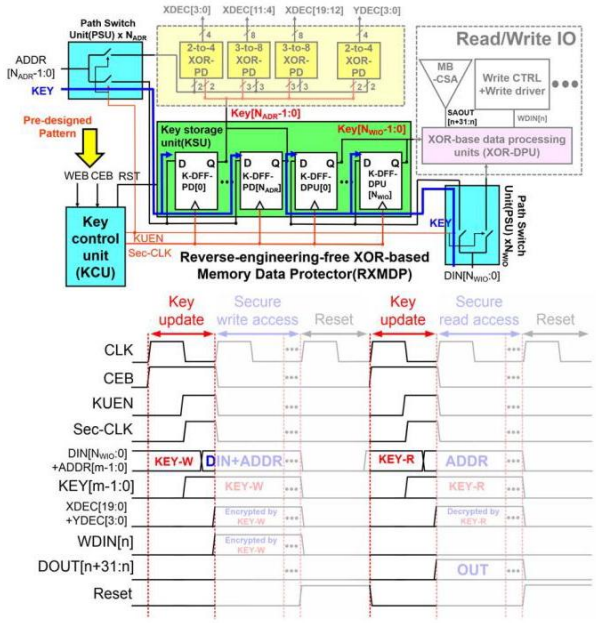
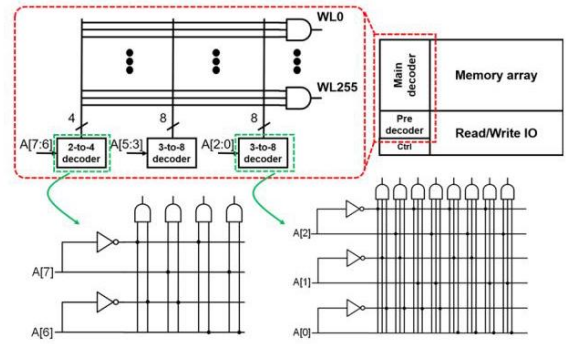


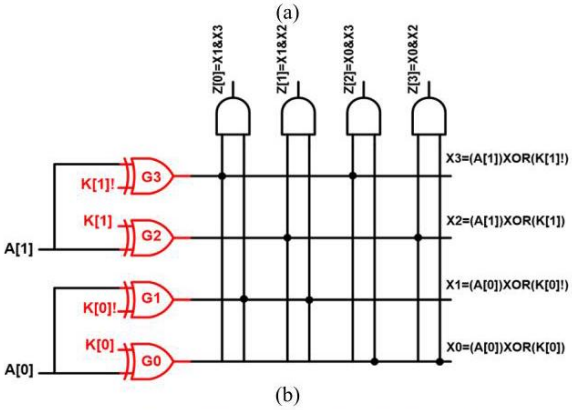
图 10. 密钥更新操作的电路激活和波形。

D. 安全访问: 基于异或的预解码器电路与操作

多级解码方案通常用于存储器宏中的行地址解码，如图 11(a) 所示。例如，256 行 (8 位行地址) 的解码可以通过在主控制区域使用两个 3-8 解码器和一个 2-4 解码器作为第一级预解码器来实现。在 RXMDP 方案下，我们在常规地址预解码器的输入端插入异或门和密钥信息，以创建异或预解码器 (XOR-PD)。如图 11(b) 所示，在典型的 2-4 预解码器 (AND0-AND3) 中增加了四个异或门 (XR1-XR4) 和两个密钥输入 (K1 和 K0)。每对异或门 (例如，XR0 和 XR1) 连接到一个地址信号 (例如，A[0])、一个密钥数据 (例如，K[0]) 以及密钥数据的补码值 (例如，KB[0])。地址 A [0] 和 K0 的异或结果连接到 AND3 和 AND2，而地址 A[0] 与 K0 的补码 (KB0) 的异或结果连接到 AND1 和 AND0 的输入端。XOR-PD 保留了典型行预解码器的相同功能；然而，解码输出模式根据密钥数据 (K[1:0]) 的值而有所不同。



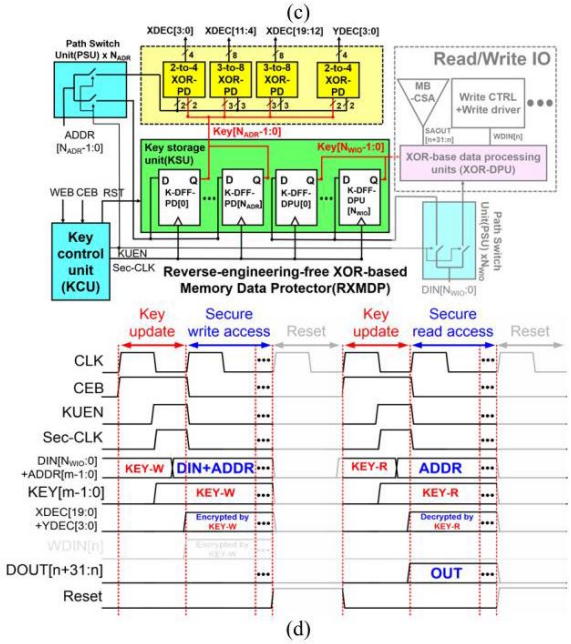
(a)



(b)

Ex:[A0:A1]=00	[K0:K1]=00	[K0:K1]=00	[K0:K1]=00	[K0:K1]=00
Z0	1	0	0	0
Z1	0	1	0	0
Z2	0	0	1	0
Z3	0	0	0	1

(c)



(d)

图 11. (a) 用于 256 行存储器宏的典型多级解码方案。(b) 提出的 2-4 预解码器的异或预解码器 (XOR-PD) 电路。(c) 提出的 2-4 异或预解码器的解码表。(d) 安全访问模式下与异或预解码器相关的激活电路和波形。

图 11(c) 展示了所提出的 XOR-PD 的真值表。对于给定的行地址模式 $A[1:0] = 00$，当 KEY 数据 K[1:0] 为”00” 时，XOR-PD 的输出 Z[3:0] 为”0001”。当 K[1:0] = 01 时，Z[3:0] 为”0010”。对于每个 KEY 数据，XOR-PD 仅生成一个输出模式。因此，即使攻击者使用逆向工程推导解码器的电路，由于缺乏用户的 KEY 数据输入，攻击者也无法识别正确的行或列地址。图 11(d) 展示了与 XOR-PD 相关的安全读取操作的波形。当 $CEB = 0$ 时，KCU 模块设置信号 $KUEN = 0$，PSU 将输入地址 (ADDR) 发送到 XOR-PD。

在任何内存访问操作之前 (即在时钟上升沿之前的输入建立时间)，存储在 KEY-DFF-PD 中的 KEY 数据被传递到 XOR-PD。请注意，内存访问位置由信号 XDEC[19:0] 和 YDEC[3:0] 决定。

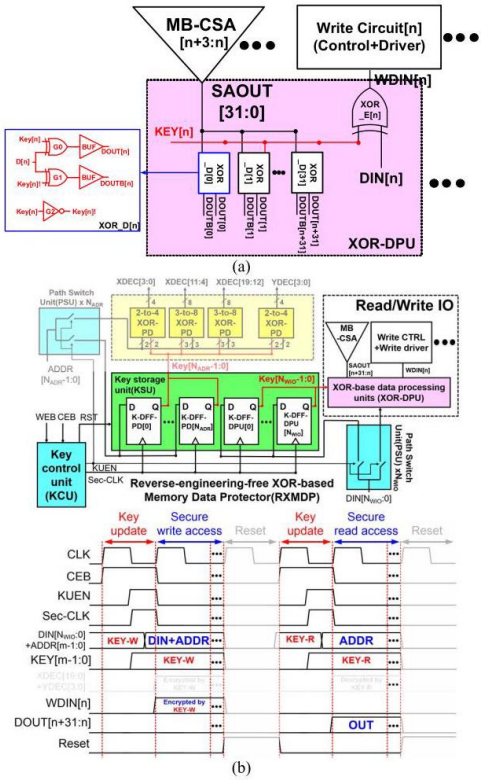


图 12. (a) 所提出的 XOR-DPU。(b) 在安全访问模式下涉及 XOR-DPU 的激活电路和波形。

对于安全写入访问，XOR-PD 中的 XOR 门根据输入地址和存储在 KEY-DFF-PD 中的 KEY 数据 (KEY-W) 改变内存单元阵列中的访问位置。因此，在安全读取访问模式下，只有当 KEY-W = KEY-R 时才能解密内存位置。

E. 安全访问:XOR-DPU 电路与操作

图 12(a) 展示了 RXMDP 中提出的 XOR-DPU。XOR-DPU 在每个 I/O 端口包含一个 XOR 门。每个存储体包含来自 32 个 MB-CSA 的 256 个输出 (DOUT[255:0]) 以及为八个写入电路提供数据的 8 个数据输入 (DIN)。总共有 256 个用于解密输出数据的 XOR 门 (XOR-D) 和 8 个用于加密输入数据的 XOR 门 (XOR-E)，即一个 XOR 门 (XOR-E[n]) 连接到一个写入电路，32 个 XOR 门 (XOR-D $[n+31:n]$) 连接到四个 MB-CSA。这些 XOR 门共享 1 位的 KEY 数据 (KEY[n])。研究发现，攻击者可能通过分析芯片在读取操作期间的功耗特征来获取与正确 KEY 相关的数据。为了降低这种风险，我们在提出的 XOR-DPU 中为每个 XOR_D[n] 添加了一个虚拟 XOR 门 (G1)，以生成互补的数据输出 (DOUTB) [图 12(a)]。互补的 XOR 操作和 DOUTB 的输出缓冲器 (BUF) 旨在减少在不同输入 KEY 下解密操作期间的功耗波动。本质上，包含互补数据输出引脚将允许使用互补数据总线进行芯片布线，从而通过提供对功耗特征分析攻击的免疫力来增强芯片级安全性。图 12(b) 展示了涉及 XOR-DPU 的安全读取操作的工作波形。当 CEB $= 0$ 时，KCU 模块设置 KUEN $= 0$ ，PSU 将数据输入 (DIN 引脚) 连接到 XOR-DPU。

在任何内存访问操作之前 (即在时钟上升沿之前的输入建立时间)，存储在 KEY-DFF-DPU 中的 KEY 数据被传递到 XOR-DPU。在安全写访问期间，内存输入数据 DIN $[n]$ (明文) 通过 XOR-E $[n]$ 使用 KEY $[n]$ 进行加密，生成 WDIN $[n]$ (密文)。然后，写电路将 WDIN $[n]$ 的值写入内存阵列。在安全读访问期间，四个 MB-CSA 输出 SAOUT[31:0]，随后通过 XOR-D $[n+31:n]$ 使用 KEY $[n]$ 进行解密，生成内存宏输出 DOUT $[n+31:n]$ 。只有当 KEY-W = KEY-R 时，才能获得正确的输出数据 (OUT)。

F. KEY-Reset: 电路与操作

如果设计者确定的模式为”0” (KEY[m - 1 : 0] $= 0$) ，地址映射和数据将与没有安全功能的常规内存相同。图 13(a) 显示了 KEY 复位模式下的操作波形，其中 KCC 触发信号复位为 1 并将其传递给 KSU 模块。如

图 13(b) 所示，每个 K-DFF-PD 或 K-DFF-DPU 包括一个反相器 (G5)、一个或非门 (G6)、两个晶体管 (N1 和 P1) 以及一个常规的 DFF(G1-G4, G7, T1 和 T2)。RESET 信号连接到 G5 和 G6 的栅极。当 RST = 1 和 SCLK = 1 (SCLKB = 0) 时，传输门 T1 被禁用，T2 被启用。然后两个晶体管 (N1 和 P1) 被打开，分别强制节点 IN-D1 = 0 和节点 IN-B2 = 1。最后，OUT 节点等于 0，使得 KSU 中的 DFF 将其值 KEY $[m-1:0]$ 复位为设计者确定的模式 (在本例中为 0)。

V. 性能与实验结果

A. 所提出方案的性能

图 14(a) 展示了 MB-CSA 的模拟计算速度、功耗、峰值电流和每比特能耗。在读取模式下，仅使用两个参考电流进行 $8-b$ 感测，使得具有 1024 个 IO 和 256 位 BL 长度的宏的 I_{REF} 数量减少至 6144。与传统的并行读取方案相比，这相当于功耗降低了 53.3%，峰值电流降低了 43.8%。值得注意的是，MBCSA 仅导致延迟 18.2% 增加了 (t_{AC}) 。总体而言，这表示每比特能耗降低了 43%。图 14 还展示了 NSRF 的模拟功耗和面积开销。通过复用输出缓冲器中的锁存器 (OTL)，与传统的外部存储宏数字移位器/旋转器电路相比，NSRF 的面积减少了 33.3%，同时功耗降低了 48.8%。图 14(b) 展示了 MB-CSA 与使用 CL-CSA 的传统串行感测方案的模拟结果对比。与 MB-CSA 相比，使用 CL-CSA 的串行感测将峰值电流值降低了 70%；然而，它也导致读取延迟增加了 554% ，每比特能耗增加了 84.2%。

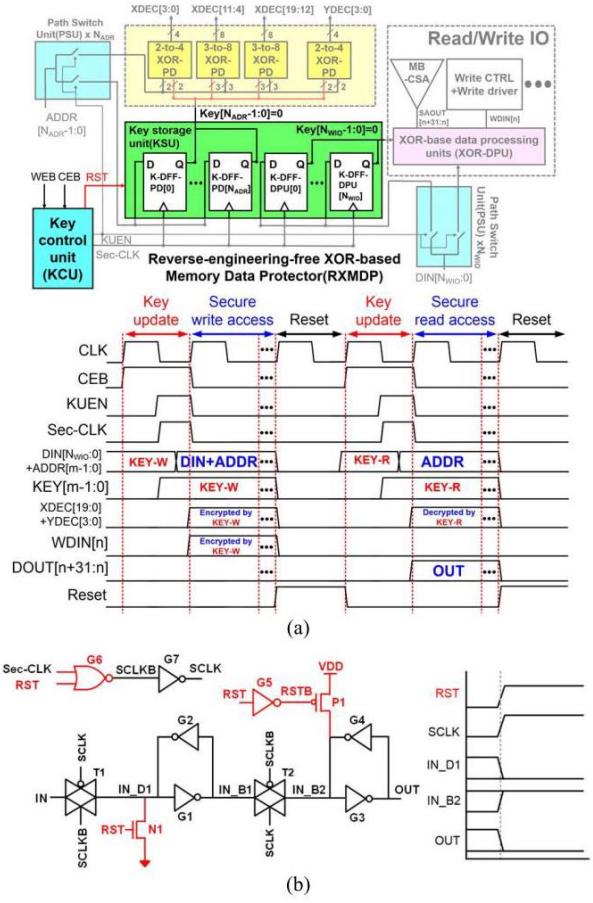


图 13. (a) KEY 复位操作的激活电路和波形。(b) K-DFF-PD 和 K-DFF-DPU 的详细电路和波形。

所提出的 NSRF 还能够在单个周期内完成内存读取和逻辑计算操作，而不是传统的内存-逻辑分离方案所需的两个周期。所提出的 RXMDP 方案对于具有 12 位输入地址和 1024 个 I/O 的 1-Mb 宏，仅增加了 1.11% 的面积开销。如图 15 中的仿真结果所示，RXMDP 增加了延迟

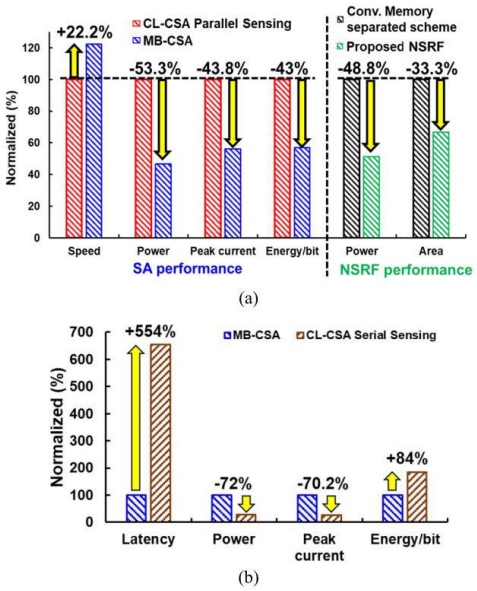


图 14. (a) MB-CSA 与传统方案在计算速度、功耗、峰值电流和每比特能耗方面的比较 (左)，以及 NSRF 与传统方案在功耗和面积开销方面的比较 (右)。(b) MB-CSA 与传统串行传感方案在计算速度、功耗、峰值电流和每比特能耗方面的比较。

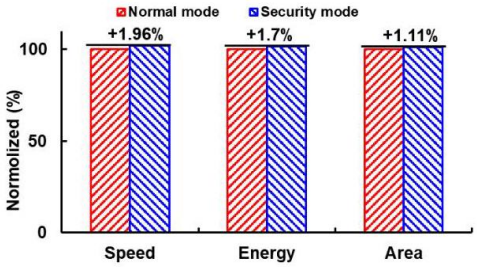


图 15. RXMDP 在正常模式和安全模式下的性能。

与正常模式 (无 RXMDP) 相比，仅增加了 1.96%，而能耗仅增加了 1.7%。此外，RXMDP 的 KEY 长度等于输入地址和内存输入数据 (写 IO) 数量的总和。图 16 比较了所提出的 MP-BLP、传统读取方案 (无预充电) 和具有两个预充电电压的 BL-IH 方案之间的 BL 发展时间 (T_{BLD})。MP-BLP 的 BL 发展时间仅为传统读取方案 (BL-SP) 的 0.27×，BL-IH 的 0.65×，以及 BL-1H 的 0.54×。所提出的 MB-CSA 占宏面积的近 13%。然而，具有 8 位输出的 MB-CSA 的面积开销仅为八个并行感测的单位 CL-CSA 所需面积的 7%。所提出的 SA 偏移在 10k 样本蒙特卡洛模拟下为 5μA，用于采样的四个电容器的值为 2fF。图 17 显示了在 10k 样本蒙特卡洛模拟中考虑工艺变化的电容与 MB-CSA 读取良率的关系。将电容降低到 2fF 以下会降低所提出的 MB-CSA 的读取良率。因此，我们选择 2fF 作为所提出的 MB-CSA 的电容值。图 18 显示了从 MBCSA 在 VDD = 0.85 V 的后布局模拟中提取的时间分解。BL 发展时间 (Ph0) 是最长的阶段，为 1.15 ns。每个重复的 2 位感测阶段 (Ph1-Ph4) 耗时 0.4 ns。注意，在单个 2 位感测阶段 (例如 Ph1) 中，子阶段 1 和 2(SP1 和 SP2) 耗时 0.15 ns，子阶段 3(SP3) 耗时 0.1 ns。在电源电压为 0.85 V 的情况下，BL 发展时间占宏访问时间的近 41%，如图 19 所示。如表 I 所示，所提出的 1-Mb MRAM 宏实现了比之前的 NVM 宏 [2]、[15]、[16]、[20]、[32]-[37] 更高的读取带宽 (42.67 GB/s) 和更低的每比特读取能量 (0.23pJ/b)。

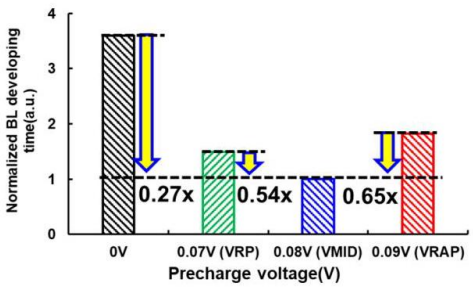


图 16. MP-BLP 与传统方案 (不同预充电电压) 在位线发展时间方面的比较。

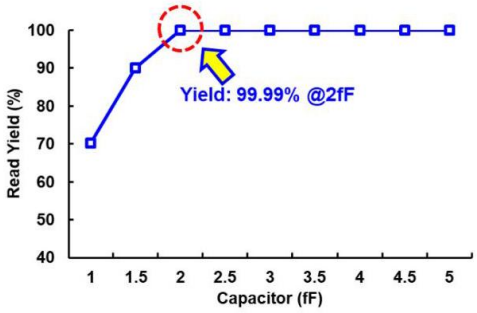


图 17. MB-CSA 的模拟读取良率与 C0-C3 电容的关系。

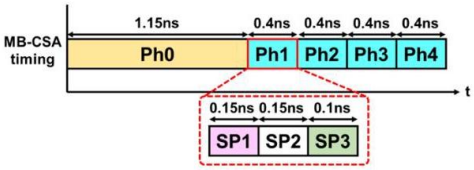


图 18. 所提出的 MB-CSA 在后布局仿真中的时序分解。

B. 实验结果

为了验证所提出方案的有效性，我们基于代工厂 22 纳米 CMOS 逻辑工艺和嵌入式 STT-MRAM 技术，使用 1Mb MRAM 宏制造了一个测试芯片。该测试芯片采用基于 DFF 的路径延迟排除方案实现，以提取与所提出 MARM 宏相关的访问时间 (T_{AC}) 。图 19(a) 展示了芯片照片和芯片摘要。图 19(b) 展示了使用上述 1Mb 宏获得的 Shmoo 图，在存储器模式下，在 0.85 V 的电源电压下实现了 T_{AC} 为 2.75 ns。在这些条件下，BWR(42.67 GB/s) 超过了所有先前报道的 NVM。NSRF 的容量为 256 位移位/旋转操作。图 20(a) 展示了 NSRF 执行 1 位移位和 1 位旋转操作的测量波形。在应用 1 位移位操作后，原始 8 – b 数据 DOUT[7:0] = 10100011 (十进制 163) 变为 DOUT[7:0] = 01000110(十进制 70)。在应用 1 位旋转操作后，原始 8 位数据 DOUT[7:0] = 10100011(十进制 163) 变为 DOUT[7:0] = 01000111(十进制 71)。图 20(b) 展示了 NSRF 在 1-8 位配置下执行移位和旋转操作的测量结果。上图展示了与 8 位移位和 8 位旋转操作相关的捕获波形。下图展示了所有 8 位选项的移位操作和旋转操作的示例。捕获的波形显示，在应用 4 位移位操作后，原始 8 位数据 DOUT[7:0] = 10100011(十进制 163) 变为 DOUT[7:0] = 00110000(十进制 48)。在应用 4 位旋转操作后，原始 8 位数据 DOUT[7:0] = 10100011(十进制 163) 变为 DOUT[7:0] = 00111010(十进制 58)。

TABLE I
已报道的非易失性存储器工作对比表

	本工作	ISSCC'19 [15]	ISSCC'19 [32]	ISSCC'19 [33]	ISSCC'18 [20]	ISSCC'17 [2]	ISSCC' 17 [16]	ISSCC'15 [34]	ISSCC'15 [35]	ISSCC'11 [36]	ISSCC' 07 [37]
存储器类型	MRAM (1T1MTJ)	MRAM (1T1MTJ)	VNAND-TLC	VNAND-TLC	MRAM (1T1MTJ)	闪存 (1T1R)	MRAM (1T1MTJ)	SG-MONOS	MRAM (2T2MTJ)	ReRAM	eNOR
工艺 (nm)	22	22 纳米 FinFET	不适用	不适用	28	90	不适用	28	65	180	130
容量	1 兆字节	7 兆字节	512 吉字节	512 吉字节	1 兆字节	1 兆字节	4 吉字节	4 兆字节	1 兆字节	4 兆字节	17 兆字节
宏数据输出宽度	1024	不适用	不适用	不适用	16	8	1024	276	256	1024	288
宏访问时间	2.75 纳秒	4 纳秒	45 微秒	56 微秒	2.8 纳秒	11 纳秒	50.5 纳秒	5 纳秒	3.3 纳秒	56 纳秒	23.5ns
读取能量/比特 (pJ)	0.23	不适用	不适用	不适用	0.7	2.2	不适用	不适用	0.27	不适用	不适用
位线长度	256	256	不适用	不适用	256	256	8192	不适用	256	不适用	512
读取带宽 (GB/s)	42.67	不适用	1.2	1.066	0.71	0.09	2.53	6.9	9.7	2.3	2
电源电压 (V)	0.85	0.9	Vcc=2.353.6 Vcca=1.2	Vcc=2.33.6 Vcca=1.2. 1.8	1.2	1.2	VDD1=1.8 VDD2=1.2	1.1	1.2	1.8	1.5

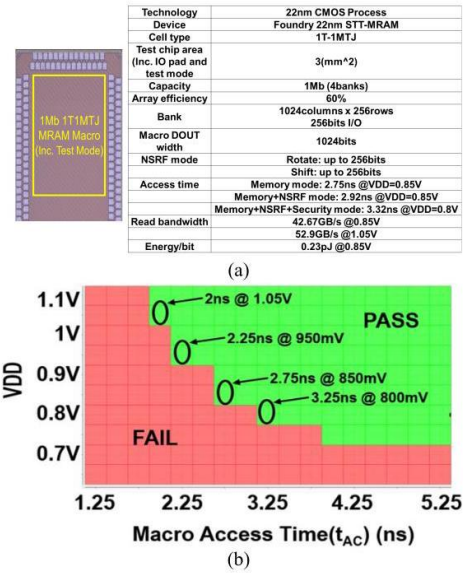


图 19. (a) 芯片总结。(b) 所提出的 MB-CSA 的 Shmoo 图。

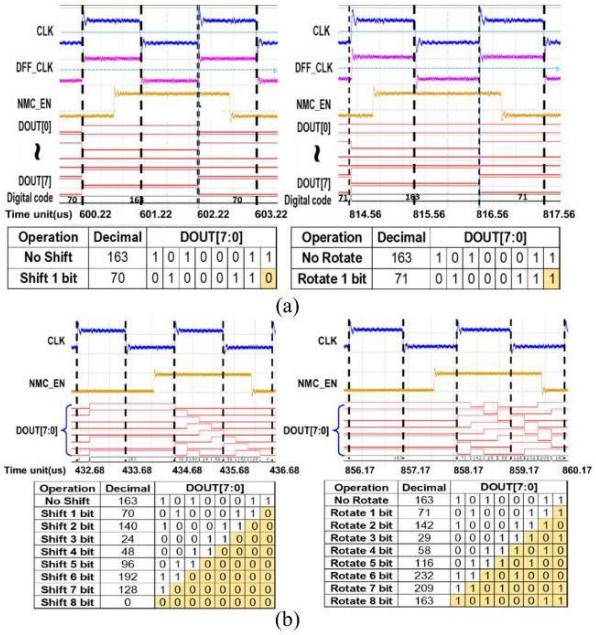


图 20. NSRF 的测量波形:(a) 1 位移位和 1 位旋转操作，(b) 1-8 位配置中的移位和旋转操作。

需要注意的是，图 20(b) 中的表格列出了从 1 到 8 b 的操作测量结果。图 21(a) 展示了使用一个 KEY 进行一次写操作和两个 KEY(正确和错误) 进行两次读操作的 RXMDP 测量波形。在写操作之前，KEY1(所有 KEYs-bit = 高) 被上传到 1-Mb STT-MRAM 宏作为正确的 KEY。在写操作期间, RXMDP 使用 KEY1 对输入数据 (所有 DINs = 高) 进行加密，并激活地址解码器中的逻辑锁定方案。使用 KEY1 的第一次读操作能够从 1-Mb STT-MRAM 宏中获取正确的数据 (所有 douts = 高)。使用错误 KEY2(所有 KEYs-bit = 低) 的第二次读操作导致读取的数据 (所有 Dout = 0) 与原始数据不同。图 21(b) 和 (c) 展示了在电源电压为 0.8 V 时启用 RXMDP 的宏访问时间测量波形。RXMDP 引入的延迟开销 (0.07ns) 远低于未使用 RXMDP 时的宏访问时间。图 22 展示了宏访问时间随 BL 长度变化的测量结果。MB-CSA 引入的并行传感延迟与 CL-CSA 相当；然而，它倾向于随 BL 长度的增加而减少。这是因为 BL 开发时间在宏访问时间中占很大比例，在传统的 CL-CSA 和提出的 MB-CSA 下，BL 开发时间随 BL 长度的增加而增加。图 23(a) 展示了读取存储在单元阵列中的相同 1024 b 数据时，使用两种不同 KEY 和 DOUT 模式的 MRAM 宏电源电压测量结果。电源噪声和电源电压的峰峰值差异分别为 47.1 和 48mV，分别对应 KEY [19 : 0] = 全 1 和 KEY [19 : 0] = 全 0。图 23(b) 展示了 MRAM 宏在十种实验 KEY 模式下的电源噪声测量结果。这十种实验模式为 KEY[19:0] = 全 0,

KEY[19:0] = 00111111111111111111, 00001111111111111111, 00000011111111111111, 0000000 0111111111111, 00000000011111111111, 0000000000001 1111111, 00000000000000111111, 00000000000000001111, 和 KEY [19 : 0] = 全 1。从宏的角度来看，这十种不同 KEY 模式下的电源噪声波动小于电源电压 (VDD = 0.8 V) 的 1mV, 0.125% 。

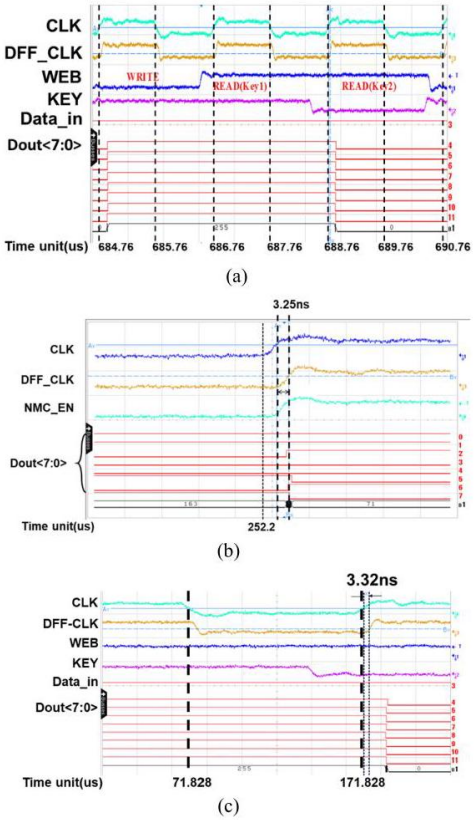


图 21. (a) RXMDP 操作的测量波形，(b) RXMDP 禁用读取操作的测量波形，以及 (c) RXMDP 启用读取操作的测量波形。

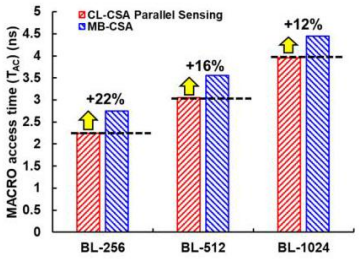


图 22. 测量的宏访问时间与 BL 长度的函数关系。

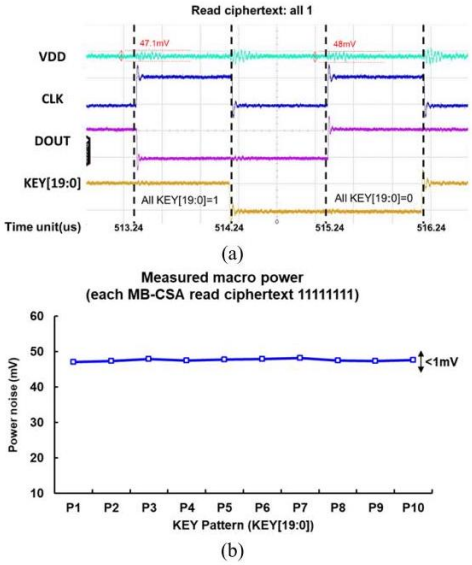


图 23. 存储在单元阵列中的相同数据的测量电源噪声结果。(a) 测量波形。(b) 十个不同 KEY 模式下的测量电源噪声。

VI. 结论

本研究解决了开发具有高读取带宽、快速计算能力和数据保护的安全感知移动设备 STT-MRAM 宏的挑战。所提出的 MBCSA 被证明可以减少高带宽读取操作的面积开销、峰值电流和能耗。所提出的近 NSRF 在紧凑的区域内实现了宏内多位移位和旋转操作，且延迟较短。此外，提出了一种名为 RXMDP 的安全方案，以保护数据和内存访问位置免受逆向工程攻击，而无需额外的引脚。一个 22 纳米 1-Mb STT-MRAM 宏验证了所提出方案的有效性。

参考文献

[1] G. De Sandre 等，” 一种具有 90 nm4Mb 读取访问时间和 1MB/s 写入吞吐量的 1.2 V12 ns 嵌入式相变存储器，” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要，美国加利福尼亚州旧金山，2010 年 2 月，第 268-269 页。

[2] Q. Dong 等，” 一种具有 39μW 编程功率的 1Mb 嵌入式 NOR 闪存，适用于毫米级高温传感器节点，” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要，2017 年 2 月，第 198-199 页。

[3] C. X. Xue 等, ” 一种 22 nm2Mb 用于多比特 MAC 计算的 ReRAM 存内计算宏单元，在微型 AI 边缘设备中实现 121-28TOPS/W 的性能,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 2020 年 2 月, 第 244-245 页。

[4] C. X. Xue 等, ” 一种 1Mb 多比特 ReRAM 存内计算宏单元，在基于 CNN 的 AI 边缘处理器中实现 14.6ns 并行 MAC 计算时间,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 2019 年 2 月, 第 388-389 页。

[5] H. Noguchi 等, ” 一种基于 4Mb STT-MRAM 的缓存，具有内存访问感知的功耗优化和写-验证-写/读-修改-写方案,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 2016 年 1 月/2 月, 第 132-133 页。

[6] H. Maejima 等, ” 一种基于 96 字线层技术的 512Gb 3b/单元 3D 闪存,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 美国加利福尼亚州旧金山, 2018 年 2 月, 第 336-338 页。

[7] C.-X. Xue 等, ” 一种基于电阻式随机存取存储器的 CMOS 集成存内计算宏单元，用于 AI 边缘设备,” 《自然电子》, 第 4 卷, 第 1 期, 第 81-90 页, 2021 年 1 月。

[8] W.-H. Chen 等, ” 用于 AI 边缘处理器的 CMOS 集成忆阻非易失性存内计算,” 《自然电子》, 卷 2, 页 420-428, 2019 年 8 月.

[9] Y. Chiu 等, ” 一种采用自动形成和自动写入方案的 40 nm2Mb ReRAM 宏, 形成时间减少 85% , 页面写入时间减少 99%,” 《VLSI 技术研讨会论文集》, 日本京都, 2019 年 6 月, 页 T232-T233.

[10] T.-C. Chang 等, ” 一种具有 42.6 GB/s 读取带宽的 22 nm1Mb1024 b 读取和近存计算双模式 STT-MRAM 宏, 适用于安全感知移动设备,” 《IEEE 国际固态电路会议 (ISSCC) 技术论文摘要》, 美国旧金山, 2020 年 2 月, 页 224-226.

[11] Z. Li 等, ”RRAM-DNN: 一种由 RRAM 和模型压缩赋能的全权重片上 DNN 加速器,” 《IEEE 固态电路杂志》, 卷 56, 期 4, 页 1105-1115, 2021 年 4 月.

[12] J. Hung 等, ” 开发用于智能边缘设备的非易失性存储器赋能计算芯片的挑战与趋势,” 《IEEE 电子器件汇刊》, 卷 67, 期 4, 页 1444-1453, 2020 年 4 月.

[13] T.-H. Yang 等, ” 一款采用 28 nm 工艺的 32Kb 嵌入式 2T2MTJ STT-MRAM 宏单元，具有 1.3 ns 读取访问时间，适用于快速可靠的读取应用,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 2018 年 2 月, 第 480-481 页。

[14] Y. Chih 等, ” 一款采用 22 nm 工艺的 32Mb 嵌入式 STT-MRAM，具有 10ns 读取速度、1M 次写入耐久性、150°C 下 10 年数据保持能力以及高抗磁场干扰能力,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 美国加利福尼亚州旧金山, 2020 年 2 月, 第 222-224 页。

[15] L. Wei 等, ” 一款采用 22FFL FinFET 工艺的 7Mb STT-MRAM，使用写入-验证-写入方案和偏移消除传感技术，在 0.9 V 下实现 4ns 读取传感时间,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 美国加利福尼亚州旧金山, 2019 年 2 月, 第 214-216 页。

[16] K. Rho 等, ” 一款 4Gb LPDDR2 STT-MRAM，采用紧凑的 9F2 1T1MTJ 单元和分层位线架构,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 美国加利福尼亚州旧金山, 2017 年 2 月, 第 396-397 页。

[17] Y. J. Song 等, ” 高度功能化且可靠的 8Mb STT-MRAM 嵌入 28 nm 逻辑,” 发表于 IEDM 技术文摘, 美国加利福尼亚州旧金山, 2016 年 12 月, 第 27 页.

[18] M.-F. Chang 等, ” 一种适用于亚 100nA 单元电流非易失性存储器的偏移容忍电流采样型感测放大器,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术文摘, 美国加利福尼亚州旧金山, 2011 年 2 月, 第 206-208 页.

[19] C. Kim 等, ” 一种用于具有 1t1mtj 共源线结构阵列的 STT-MRAM 的共价键交叉耦合电流模式感测放大器,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术文摘, 2015 年 2 月, 第 1-3 页.

[20] Q. Dong 等, ” 一种 1Mb 28 nm STT-MRAM, 采用单电容偏移消除感测放大器和原位自写终止, 在 1.2 V VDD 下实现 2.8ns 读取访问时间,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术文摘, 美国加利福尼亚州旧金山, 2018 年 2 月, 第 480-481 页.

[21] C. Chou 等, ” 一种 N40 256K ×44 嵌入式 RRAM 宏, 采用 SL 预充电 SA 和低压限流器以提高读写性能,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术文摘, 美国加利福尼亚州旧金山, 2018 年 2 月, 第 478-480 页.

[22] J. Rajendran, M. Sam, O. Sinanoglu, 和 R. Karri, ” 集成电路伪装的安全性分析,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2013, pp. 709-720.

[23] K Shamsi, M. Li, T. Meade, Z. Zhao, D. Z. Pan, 和 Y. Jin, ” 用于创建 SAT 不可解析电路的循环混淆,” in Proc. Great Lakes Symp. VLSI, May 2017, pp. 173-178.

[24] J. A. Roy, F. Koushanfar, 和 I. L. Markov, ” 终结集成电路盗版,” Computer, vol. 43, no. 10, pp. 30-38, 2010.

[25] M.-F. Chang 等, ” 一种适用于亚 100nA 单元电流非易失性存储器的偏移容忍电流采样感应放大器,” in IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers, San Francisco, CA, USA, Feb. 2011, pp. 206-208.

[26] C. Kim, K. Kwon, C. Park, S. Jang, 和 J. Choi, ” 一种用于具有 1T1MTJ 共源线结构阵列的 STT-MRAM 的共价键交叉耦合电流模式感应放大器,” in IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers, Feb. 2015, pp. 1-3.

[27] 宣布高级加密标准 (AES)，联邦信息处理标准出版物，美国国家标准与技术研究院 (NIST)，标准 197，2001 年 11 月。

[28] 安全哈希标准 (SHS)，美国国家标准与技术研究院，标准 FIBS PUB 180-4，2012 年。

[29] Y. Zhang, L. Xu, Q. Dong, J. Wang, D. Blaauw, 和 D. Sylvester, ”Recryptor: 一种用于物联网安全的可重构加密 Cortex-M0 处理器，具有内存内和近内存计算功能,” IEEE 固态电路杂志, 卷 53, 期 4, 页 995-1005, 2018 年 4 月。

[30] L. Sigal 等, ” 用于高性能 CMOS IBM S/390 并行企业服务器 G4 微处理器的电路设计技术,” IBM 研究与开发杂志, 卷 41, 期 4.5, 页 489-503, 1997 年 7 月。

[31] J. Rabaey, 数字集成电路: 设计视角. Englewood Cliffs, NJ, 美国: Prentice-Hall, 1995 年。

[32] D. Kang 等, ” 一款 512Gb 3-bit/单元 3D 6th 代 V-NAND 闪存，具有 82MB/s 写入吞吐量和 1.2Gb/s 接口,” 在 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要中, 2019 年 2 月, 页 216-217。

[33] N. Shibata 等, ” 基于 96 字线层技术的 1.33Tb 4 位/单元 3D 闪存,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 2019 年 2 月, 第 210-211 页。

[34] Y. Taito 等, ” 用于汽车应用的 28 nm 嵌入式 SG-MONOS 闪存宏, 在 200MHz 读取操作和 2.0MB/S 写入吞吐量下实现 Ti, of 170°C ,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 2015 年, 第

132-133 页。
[35] H. Noguchi 等, ” 采用物理消除读取干扰方案和常关存储器架构的 3.3ns 访问时间 71.2μW/MHz1Mb 嵌入式 STT-MRAM,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 美国加州旧金山, 2015 年 2 月, 第 136-137 页。
[36] W. Otsuka 等, ” 具有 2.3GB/s 读取吞吐量和 216MB/s 编程吞吐量的 4Mb 导电桥电阻存储器,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 美国加州旧金山, 2011 年 2 月, 第 210-211 页。
[37] C. Deml 等, ” 用于汽车微控制器的 0.13µm 2.125MB 23.5ns 嵌入式闪存, 具有 2GB/s 读取吞吐量,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 2007 年 2 月, 第 478-479 页。
[38] Y. Chih 等人, ”13.3 一款 22 nm 32Mb 嵌入式 STT-MRAM，具有 10ns 读取速度、1M 次写入耐久性、150°C 下 10 年数据保持能力以及高抗磁场干扰性,” 发表于 IEEE 国际固态电路会议 (ISSCC) 技术论文摘要, 2020 年 2 月, 第 222-224 页。

邱彦程于 2018 年获得台湾新竹国立清华大学电机工程学士学位，目前正在该校电机工程研究所攻读博士学位。
他目前的研究兴趣包括 SRAM 电路设计、存储器安全以及新兴非易失性存储器。

张东成于 2017 年获得台湾桃园国立中央大学电机工程系学士学位，并于 2019 年获得台湾新竹国立清华大学电机工程硕士学位。
他目前任职于台湾新竹的台积电公司，担任工程师。他当前的研究兴趣包括新兴非易失性存储器电路设计、嵌入式存储器以及深度神经网络电路设计。

李俊颖于 2018 年和 2020 年分别获得台湾新竹国立清华大学电机工程系学士和硕士学位。
他的研究兴趣包括新兴非易失性存储器电路设计、嵌入式存储器、高带宽电路、近存计算电路以及深度神经网络电路。

洪哲民于 2019 年获得台湾新竹国立清华大学电机工程与计算机科学学士学位，目前正在该校电子工程研究所攻读博士学位。

他目前的研究兴趣包括新兴非易失性存储器的存内计算。

张光堂于 2019 年获得台湾新竹国立清华大学电子工程硕士学位。

他的研究兴趣包括非易失性存储器的高速感测放大器。

薛承鑫 (IEEE 研究生会员) 于 2015 年和 2017 年分别获得台湾嘉义国立中正大学电气工程系学士和硕士学位。他目前正在台湾新竹国立清华大学电气工程系攻读博士学位。

他目前的研究兴趣包括新兴非易失性存储器、嵌入式存储器和内存计算的电路设计。

吴思妍于 2017 年获得台湾嘉义国立中正大学电子系学士学位。她目前正在台湾新竹国立清华大学电子工程研究所攻读硕士学位。

她目前的研究兴趣包括 SRAM 电路设计和存储器硬件安全。

高慧瑶于 2018 年获得台湾新竹国立清华大学电气工程系学士学位，并于 2020 年获得国立清华大学电子工程研究所硕士学位。

他目前的研究兴趣包括新兴非易失性存储器的电路设计。

陈鹏于 2017 年获得中国哈尔滨东北林业大学电气工程及自动化专业学士学位，并于 2020 年获得台湾新竹国立清华大学电气工程硕士学位。

他的研究兴趣包括内存计算、近内存计算和新兴非易失性存储器的电路设计。

黄晓瑜于 2018 年获得台湾新竹国立清华大学工程与系统科学学士学位，目前正在该校电机工程研究所攻读硕士学位。

她目前的研究兴趣包括存储器安全性和新兴非易失性存储器。

滕世熙于 2019 年获得台湾台南国立成功大学电机工程学士学位，目前正在台湾新竹国立清华大学电机工程研究所攻读硕士学位。

他目前的研究兴趣包括 SRAM 和新兴非易失性存储器的电路设计。

罗杰普分别于 2014 年和 2016 年获得台湾新竹国立清华大学电机工程学士和硕士学位。

他目前是台湾新竹台积电公司的工程师，同时也在国立清华大学任职。他目前的研究兴趣包括新兴存储器电路设计和神经形态电路设计。

施宜君 (IEEE 会员) 分别于 2008 年和 2012 年获得台湾台北国立台湾大学物理学学士学位和光电硕士学位，并于美国华盛顿州西雅图华盛顿大学获得电机工程博士学位。

他目前是台湾新竹台积电公司存储器解决方案部门的技术经理，负责 MRAM 测试平台和嵌入式 MRAM IP 的开发。在加入台积电之前，他曾在美国俄勒冈州希尔斯伯勒英特尔实验室担任研究科学家，专注于集成稳压器和低功耗电路技术的研究。他还曾在新竹旺宏电子担任闪存电路设计师。

尤德志 (IEEE 会员) 于 1988 年获得台湾大学物理学士学位，并于 1992 年获得台湾清华大学电子工程硕士学位。

1992 年至 1997 年，他在台湾积体电路制造公司 (TSMC) 担任数据通信以太网收发器电路设计工程师和 SDRAM 电路设计工程师。1997 年，他加入 TSMC，负责嵌入式非易失性存储器 IP 的开发，包括嵌入式闪存、一次性可编程 (OTP)、多次可编程 (MTP) 和新兴存储器。他是 TSMC 院士，目前担任存储器解决方案部门嵌入式非易失性存储器库部门总监。

张宗永 (IEEE 会士) 于 1990 年获得台湾大学电机工程学士学位，并于 1993 年和 1998 年分别获得美国斯坦福大学电机工程硕士和博士学位。

他曾在美国英特尔公司担任首席工程师，负责企业服务器处理器的二级/三级缓存。目前，他在台湾积体电路制造公司 (TSMC) 担任总监，领导存储器 IP 开发。他负责为先进技术节点提供低功耗、高速应用的 SRAM 编译器、定制 SRAM IP、熔丝和一次性可编程 (OTP)。他在 IEEE 会议或期刊上发表了 30 多篇技术论文，并拥有 25 项嵌入式存储器设计专利。

张博士担任 2019/2020 年 ISSCC 存储器分委会主席，ISSCC 和 VLSI 的技术程序委员会成员，《固态电路杂志》的副主编和客座编辑，以及《IEEE 超大规模集成电路系统汇刊》的副主编。

金毅 (IEEE 高级会员) 于 2005 年和 2007 年分别在中国杭州的浙江大学获得电气工程学士和硕士学位，并于 2012 年在美国康涅狄格州纽黑文的耶鲁大学获得电气工程博士学位。

他目前是美国佛罗里达州盖恩斯维尔的佛罗里达大学电气与计算机工程系的副教授和物联网 Warren B. Nelms 特聘教授。他的研究领域包括硬件安全、嵌入式系统设计与安全、可信硬件知识产权 (IP) 核以及现代计算系统的硬件-软件协同设计。他还对物联网 (IoT) 和可穿戴设备的安全分析感兴趣，特别是在物联网时代的信息完整性和隐私保护方面。

金博士于 2016 年获得美国能源部早期职业奖，并于 2019 年获得美国海军研究局青年研究员奖。他在 DAC 2015、ASP-DAC 2016、HOST 2017、ACM TODAES 2018、GLSVLSI 2018、DATE 2019 和 AsianHOST 2020 上获得了最佳论文奖。他还是 IEEE 电子设计自动化委员会 (CEDA) 的杰出讲师，并担任 IEEE 硬件安全与信任技术委员会 (HSTTC) 的联合主席。

张孟凡 (IEEE Fellow) 于 1996 年获得美国宾夕法尼亚州立大学硕士学位，并于 2005 年获得台湾新竹国立交通大学博士学位。

他目前担任台湾新竹国立清华大学特聘教授，并兼任台湾积体电路制造公司 (TSMC) 新竹企业研究总监。在 2006 年之前，他在工业界工作了十多年。这包括 1996 年至 1997 年在美国 Mentor Graphics 公司

设计存储器编译器，以及 1997 年至 2001 年在 TSMC 设计服务部门设计嵌入式 SRAM 和 Flash 宏单元。2001 年，他在新竹共同创立了 IPLib 公司，开发嵌入式 SRAM 和 ROM 编译器、Flash 宏单元以及平面单元 ROM 产品，直至 2006 年。他的研究兴趣包括易失性和非易失性存储器的电路设计、超低电压系统、3D 存储器、电路与器件相互作用、自旋电子电路、用于神经形态计算的忆阻器逻辑以及用于人工智能的内存计算。

张博士曾获得台湾多项国家级殊荣，包括科技部杰出研究奖、杰出电机工程教授奖、中央研究院年轻学者研究著作奖及吴大猷先生纪念奖。他曾担任 IEEE 固态电路期刊 (JSSC)、IEEE 超大规模集成电路系统汇刊 (VLSI)、IEEE 电路与系统 I 辑: 常规论文汇刊以及 IEEE 集成电路与系统计算机辅助设计汇刊的副编辑，并担任 IEEE JSSC、IEEE 电路与系统 II 辑: 快报以及 IEEE 电路与系统新兴与精选主题期刊 (JETCAS) 的客座编辑。他还曾担任 IEDM 执行委员会委员，以及 ISSCC、IEDM、DAC、ISCAS、VLSI-DAT 和 ASP-DAC 的分委员会主席。他曾担任 IEEE 固态电路学会 (SSCS) 和电路与系统学会 (CASS) 的杰出讲师，CASS 纳米吉咖技术委员会主席，以及 IEEE 纳米技术理事会行政委员会 (AdCom) 成员。他曾担任台湾科技部微电子计划项目主任、IEEE 台北分会主席，以及台湾国家智能电子计划 (NPIE) 及其桥梁计划的副执行主任。