

# 基于忆阻器交叉阵列的低开销存内加法器及加解密电路设计\*

罗丽<sup>1)2)3)</sup> 石绍田<sup>1)</sup> 张凤运<sup>1)2)3)†</sup> 段书凯<sup>1)2)3)‡</sup>

1) (西南大学人工智能学院, 重庆 400715)

2) (智能传动和控制技术国家地方联合工程研究中心, 重庆 400715)

3) (类脑计算与智能芯片重庆市重点实验室, 重庆 400715)

(2026 年 5 月 12 日收到; 2026 年 5 月 28 日收到修改稿)

针对传统冯·诺依曼架构存算分离导致的存储墙瓶颈, 以及现有忆阻器全加器方案存在器件开销大、运算步骤多、硬件复杂度高问题, 本文基于忆阻器交叉阵列开展新型存内加法器设计. 首先, 提出一种低开销、少步骤的 1 位全加器, 仅需 6 个忆阻器和 2 步操作即可完成求和与进位输出, 在器件数量与运算效率上优于现有方案. 其次, 基于该全加器构建存内加解密电路, 实现存储、运算与加解密功能的一体化融合, 可满足安全敏感应用场景的需求. 进一步, 通过全加器设计  $n$  位行波进位加法器, 经品质因数 (figure of merit, FoM) 评估, 在  $FoM_B$  (步骤数和器件数同等权重) 和  $FoM_S$  (侧重步骤数) 指标下性能改进分别达到  $1.37 \times -12.18 \times$  和  $1.80 \times -41.98 \times$ . 本文设计为基于忆阻器的存算一体加法电路的高效实现提供了可行方案.

**关键词:** 忆阻器, 存内计算, 全加器, 加解密电路**DOI:** 10.7498/aps.75.20260679**CSTR:** 32037.14.aps.75.20260679

## 1 引言

全球数据量呈指数级暴涨, 传统存算分离的计算系统存在显著性能瓶颈, 不仅限制了计算速度, 更导致系统高功耗、高时延等问题<sup>[1-3]</sup>. 存内计算作为后摩尔时代计算新范式的研究热点, 被认为是极具潜力的革命性技术, 其核心是实现计算单元与存储单元的深度融合, 在完成数据存储的同时直接执行计算操作, 从而彻底消除冯·诺依曼架构中数据频繁搬移带来的额外开销与时延, 大幅提升运算效率, 实现计算与存储的高效节能<sup>[4-8]</sup>.

新型纳米忆阻器具备双稳态/多稳态电阻、非易失性、纳米级尺寸、低功耗及可三维堆叠等独特

特性, 兼具高效计算能力与高密度存储能力, 成为适配未来以数据为中心计算需求的核心候选器件<sup>[9-13]</sup>. 尤为重要的是, 忆阻器可在同一器件内同步实现数据存储与逻辑运算, 其天然的存算一体特性与存内计算架构高度契合, 为加法器等基础算术单元的设计提供了颠覆性的实现路径, 也为基于忆阻器交叉阵列构建高效存内计算系统奠定了基础<sup>[14-16]</sup>. 加法器作为现代微处理器、加密电路等系统中的核心算术部件, 其运算速度、面积开销、功耗表现直接决定了整个系统的性能, 因此优化加法器性能、提升其集成度与效率具有重要意义<sup>[17,18]</sup>.

目前, 基于忆阻器的全加器设计已成为研究热点<sup>[19-21]</sup>, 相关成果不断涌现, Miao 等<sup>[22]</sup> 基于与 (AND)、或 (OR)、异或 (XOR) 基本逻辑门, 实现

\* 重庆市自然科学基金 (批准号: CSTB2024NSCQ-MSX0586, CSTB2024NSCQ-MSX0302) 和国家自然科学基金 (批准号: 62576291, 62306246) 资助的课题.

† 通信作者. E-mail: zhangfy24@swu.edu.cn

‡ 通信作者. E-mail: duansk@swu.edu.cn

了1位全加器,需6个忆阻器、1个电阻和6个操作步骤. Dias等<sup>[23]</sup>提出了“积之和”形式的状态逻辑计算范式,实现1位全加器同样需要6个忆阻器、1个电阻和6个步骤. Wang等<sup>[24]</sup>基于 $V$ (电压)/ $R$ (电阻)- $R$ 逻辑设计了2-1多路选择器(multiplexer, MUX),以XOR和MUX作为逻辑原语,需4步操作实现1位全加器,但该设计中逻辑级联需额外引入 $R$ - $V$ 转换电路,不可避免地增加了系统功耗、延迟与设计复杂度. Luo等<sup>[25]</sup>基于可重构布尔逻辑运算构建1位全加器,采用9个忆阻器,需7个操作步骤. Kim等<sup>[26]</sup>以蕴含非(inverse implication, NIMP)和AND逻辑门为基础,用8个忆阻器、6步操作实现了1位全加器.

现有忆阻器全加器方案多采用分立基础逻辑门级联的设计思路,通过XOR, AND, OR, NIMP等门电路组合实现全加器和与输出进位,不仅依赖大量忆阻器,还需多步操作完成运算,存在器件数量多、运算步长长、传输延迟高、硬件面积开销大等问题,难以满足高速数据处理与实时加密运算的应用需求,也限制了忆阻器存内计算架构在安全加解密、多位并行运算场景的工程落地. 针对上述不足,本文面向存内计算与硬件图像加解密应用需求,开展基于忆阻器交叉阵列的新型存内加法器设计. 首先设计低器件开销、少运算步数的忆阻器阵列1位全加器;在此基础上构建基于全加器的存内加解密硬件电路;进一步基于1位全加器,实现 $n$ 位行波进位存内加法器. 在精简器件规模与操作步骤的同时,提升存内加法运算效率与硬件安全加密能力,为忆阻器存算一体安全电路的设计与应用提供新的可行方案.

## 2 基于忆阻器交叉阵列的全加器设计与分析

### 2.1 全加器电路设计

本节设计了一种基于忆阻器交叉阵列的全加器电路,将两个一位二进制数与来自低位的进位相加,输出和与进位,如图1所示,该电路包括输入忆阻器 $M_1$ 、输入忆阻器 $M_2$ 、输入忆阻器 $M_3$ 、辅助忆阻器 $M_4$ 、输出忆阻器 $M_5$ 和输出忆阻器 $M_6$ ,其中忆阻器 $M_1$ —忆阻器 $M_6$ 的顶电极分别与位线 $BL_1$ — $BL_6$ 相连,各忆阻器的底端电极均连接在同一字线(word line, WL)上. 图1全加器电路中采

用的是同种类型忆阻器,不同颜色忆阻器用于区分不同功能,其中蓝色表示用作输入的忆阻器,紫色表示用作辅助计算的忆阻器,绿色表示用作输出的忆阻器. 忆阻器的置位(SET)和复位(RESET)电压分别为 $V_{SET}$ 和 $V_{RES}$  ( $2|V_{RES}| < V_{SET}$ ),忆阻器包括高阻态 $R_H$ 和低阻态 $R_L$ ,分别定义为逻辑0和1. 忆阻器 $M_1$ 、忆阻器 $M_2$ 和忆阻器 $M_3$ 的阻态分别表示全加器的被加数 $a$ 、加数 $b$ 和输入进位 $c_{in}$ ,忆阻器 $M_5$ 和忆阻器 $M_6$ 的阻态分别表示全加器的和 $s$ 与输出进位 $c_o$ . 进行运算之前,将忆阻器 $M_1$ 、忆阻器 $M_2$ 和忆阻器 $M_3$ 分别置为被加数 $a$ 、加数 $b$ 和输入进位 $c_{in}$ 逻辑值所对应的阻态,忆阻器 $M_4$ 、忆阻器 $M_5$ 和忆阻器 $M_6$ 的初始状态都为低阻态. 基于忆阻器交叉阵列的全加器具体操作步骤如下.

步骤1: 给位线 $BL_1$ 施加电压 $V_{A1}$ ,位线 $BL_2$ 施加电压 $V_{B1}$ ,位线 $BL_3$ 施加电压 $V_{CIN1}$ ,位线 $BL_4$ 施加电压 $V_{AS1}$ ,而位线 $BL_5$ 接地( $G$ ),位线 $BL_6$ 悬空( $F$ ),得到全加器的输出进位 $c_o$ ,同时存储在忆阻器 $M_5$ 中;

步骤2: 在上一步操作基础上,给位线 $BL_1$ 施加电压 $V_{A2}$ ,位线 $BL_2$ 施加电压 $V_{B2}$ ,位线 $BL_3$ 施加电压 $V_{CIN2}$ ,位线 $BL_4$ 施加电压 $V_{AS2}$ ,位线 $BL_5$ 施加电压 $V_{CO}$ ,而位线 $BL_6$ 接地,得到全加器的和 $s$ ,同时存储在忆阻器 $M_6$ 中.

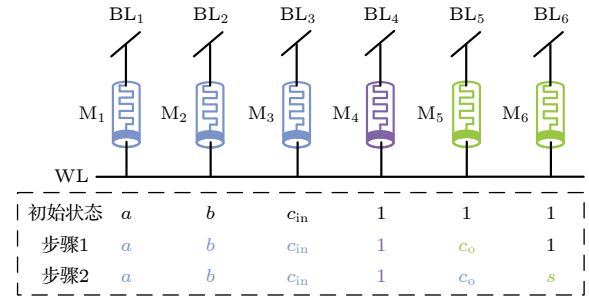


图1 基于忆阻器交叉阵列的全加器电路示意图

Fig. 1. Circuit schematic of a full adder based on memristor crossbar array.

为了得到输出进位,操作电压 $V_{A1}$ ,  $V_{B1}$ ,  $V_{CIN1}$ ,  $V_{AS1}$ 大小设置在 $[0, V_X]$ 范围内. 为了避免输入忆阻器发生SET切换,  $V_X$ 应小于忆阻器的SET电压 $V_{SET}$ . 当给全加器电路施加操作电压时,输出忆阻器 $M_5$ 根据输入 $a$ ,  $b$ 和 $c_{in}$ 进行条件RESET切换. 也就是说,对于特定的逻辑输入,忆阻器 $M_5$ 两端的电压 $V_{M5}$  ( $V_{M5} = V_{WL} - G = V_{WL}$ , 其中 $V_{WL}$ 是字线WL处的结点电压)大于RESET电压绝对值

$|V_{\text{RES}}|$ , 将忆阻器  $M_5$  从低阻态  $R_L$  切换到高阻态  $R_H$ ; 而对于其他逻辑输入, 忆阻器  $M_5$  两端的电压  $V_{M5}$  小于  $|V_{\text{RES}}|$ , 忆阻器  $M_5$  保持在低阻态  $R_L$  不变. 根据基尔霍夫定律, 可得到下式:

$$\frac{V_{A1} - V_{WL}}{R_{M1}} + \frac{V_{B1} - V_{WL}}{R_{M2}} + \frac{V_{\text{CIN1}} - V_{WL}}{R_{M3}} + \frac{V_{AS1} - V_{WL}}{R_{M4}} = \frac{V_{WL}}{R_{M5}}, \quad (1)$$

其中,  $R_{M1}$ ,  $R_{M2}$ ,  $R_{M3}$ ,  $R_{M4}$  和  $R_{M5}$  分别是忆阻器  $M_1$ 、忆阻器  $M_2$ 、忆阻器  $M_3$ 、忆阻器  $M_4$  和忆阻器  $M_5$  的阻值. 将  $R_{M4} = R_{M5} = R_L$  代入 (1) 式可得到:

$$V_{WL} = \left( \frac{1}{R_{M1}} + \frac{1}{R_{M2}} + \frac{1}{R_{M3}} + \frac{2}{R_L} \right)^{-1} \times \left( \frac{V_{A1}}{R_{M1}} + \frac{V_{B1}}{R_{M2}} + \frac{V_{\text{CIN1}}}{R_{M3}} + \frac{V_{AS1}}{R_L} \right). \quad (2)$$

根据 (2) 式和表 1 全加器真值表中输入、输出情况, 可得到操作电压  $V_{A1}$ ,  $V_{B1}$ ,  $V_{\text{CIN1}}$ ,  $V_{AS1}$  的确认条件, 具体为

$$V_{WL1} = \left( \frac{3}{R_H} + \frac{2}{R_L} \right)^{-1} \left( \frac{V_{A1}}{R_H} + \frac{V_{B1}}{R_H} + \frac{V_{\text{CIN1}}}{R_H} + \frac{V_{AS1}}{R_L} \right) > |V_{\text{RES}}|, \quad (3)$$

$$V_{WL2} = \left( \frac{2}{R_H} + \frac{3}{R_L} \right)^{-1} \left( \frac{V_{A1}}{R_H} + \frac{V_{B1}}{R_H} + \frac{V_{\text{CIN1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) > |V_{\text{RES}}|, \quad (4)$$

$$V_{WL3} = \left( \frac{2}{R_H} + \frac{3}{R_L} \right)^{-1} \left( \frac{V_{A1}}{R_H} + \frac{V_{B1}}{R_L} + \frac{V_{\text{CIN1}}}{R_H} + \frac{V_{AS1}}{R_L} \right) > |V_{\text{RES}}|, \quad (5)$$

$$V_{WL4} = \left( \frac{1}{R_H} + \frac{4}{R_L} \right)^{-1} \left( \frac{V_{A1}}{R_H} + \frac{V_{B1}}{R_L} + \frac{V_{\text{CIN1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) < |V_{\text{RES}}|, \quad (6)$$

$$V_{WL5} = \left( \frac{2}{R_H} + \frac{3}{R_L} \right)^{-1} \left( \frac{V_{A1}}{R_L} + \frac{V_{B1}}{R_H} + \frac{V_{\text{CIN1}}}{R_H} + \frac{V_{AS1}}{R_L} \right) > |V_{\text{RES}}|, \quad (7)$$

$$V_{WL6} = \left( \frac{1}{R_H} + \frac{4}{R_L} \right)^{-1} \left( \frac{V_{A1}}{R_L} + \frac{V_{B1}}{R_H} + \frac{V_{\text{CIN1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) < |V_{\text{RES}}|, \quad (8)$$

$$V_{WL7} = \left( \frac{1}{R_H} + \frac{4}{R_L} \right)^{-1} \left( \frac{V_{A1}}{R_L} + \frac{V_{B1}}{R_L} + \frac{V_{\text{CIN1}}}{R_H} + \frac{V_{AS1}}{R_L} \right) < |V_{\text{RES}}|, \quad (9)$$

$$V_{WL8} = \left( \frac{5}{R_L} \right)^{-1} \left( \frac{V_{A1}}{R_L} + \frac{V_{B1}}{R_L} + \frac{V_{\text{CIN1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) < |V_{\text{RES}}|. \quad (10)$$

其中,  $V_{WL1}$ ,  $V_{WL2}$ ,  $V_{WL3}$ ,  $V_{WL4}$ ,  $V_{WL5}$ ,  $V_{WL6}$ ,  $V_{WL7}$ ,  $V_{WL8}$  分别表示全加器输入  $abc_{\text{in}}$  为 000, 001, 010, 011, 100, 101, 110, 111 的结点电压. 为了简化操作电压确认条件, 操作电压  $V_{A1}$ ,  $V_{B1}$ ,  $V_{\text{CIN1}}$  可选取相同大小的电压  $V_{\text{CM1}}$ , 于是,  $V_{WL2} = V_{WL3} = V_{WL5}$ ,  $V_{WL4} = V_{WL6} = V_{WL7}$ , 因而操作电压确认条件可简化为 4 个:

$$\left( \frac{3}{R_H} + \frac{2}{R_L} \right)^{-1} \left( \frac{3V_{\text{CM1}}}{R_H} + \frac{V_{AS1}}{R_L} \right) > |V_{\text{RES}}|, \quad (11)$$

$$\left( \frac{2}{R_H} + \frac{3}{R_L} \right)^{-1} \left( \frac{2V_{\text{CM1}}}{R_H} + \frac{V_{\text{CM1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) > |V_{\text{RES}}|, \quad (12)$$

$$\left( \frac{1}{R_H} + \frac{4}{R_L} \right)^{-1} \left( \frac{V_{\text{CM1}}}{R_H} + \frac{2V_{\text{CM1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) < |V_{\text{RES}}|, \quad (13)$$

$$\left( \frac{5}{R_L} \right)^{-1} \left( \frac{3V_{\text{CM1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) < |V_{\text{RES}}|. \quad (14)$$

进而为了避免输入忆阻器  $M_1$ — $M_3$  和辅助忆阻器  $M_4$  的阻态被破坏, 以便能够多次使用. 在输出忆阻器  $M_5$  发生 RESET 切换情况下, 处于低阻态的输入忆阻器  $M_1$ — $M_3$  以及辅助忆阻器  $M_4$  两端电压都应小于  $|V_{\text{RES}}|$ . 于是, 电压  $V_{\text{CM1}}$  和  $V_{AS1}$  增加如下选择约束:

$$\left( \frac{4}{R_H} + \frac{1}{R_L} \right)^{-1} \left( \frac{3V_{\text{CM1}}}{R_H} + \frac{V_{AS1}}{R_L} \right) - V_{AS1} < |V_{\text{RES}}|, \quad (15)$$

$$\left( \frac{3}{R_H} + \frac{2}{R_L} \right)^{-1} \left( \frac{2V_{\text{CM1}}}{R_H} + \frac{V_{\text{CM1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) - V_{\text{CM1}} < |V_{\text{RES}}|, \quad (16)$$

$$\left( \frac{3}{R_H} + \frac{2}{R_L} \right)^{-1} \left( \frac{2V_{\text{CM1}}}{R_H} + \frac{V_{\text{CM1}}}{R_L} + \frac{V_{AS1}}{R_L} \right) - V_{AS1} < |V_{\text{RES}}|. \quad (17)$$

根据 (11)—(17) 式即可确认操作电压  $V_{\text{CM1}}$  和  $V_{AS1}$  的大小. 为了计算  $V_{\text{CM1}}$  和  $V_{AS1}$ , 将参数  $V_{\text{SET}} = 0.78 \text{ V}$ ,  $V_{\text{RES}} = -0.21 \text{ V}$ ,  $V_X = 0.6 \text{ V}$ ,  $R_H = 616 \text{ k}\Omega$  和  $R_L = 530 \text{ }\Omega$  代入 (11)—(17) 式, 这些值来自用于电路仿真的忆阻器模型参数, 仿真实验情

况将在 2.2 节讨论. 图 2 显示了用于全加器输出进位的操作电压  $V_{CM1}$  和  $V_{AS1}$  的确认条件可视化图, 洋红色阴影区域表示适用于全加器输出进位  $V_{CM1}$  和  $V_{AS1}$  的有效范围, 例如, 可选择  $V_{CM1} = 0.14$  V 和  $V_{AS1} = 0.52$  V 来进行全加器输出进位操作.

表 1 1 位全加器真值表  
Table 1. One-bit full adder truth table.

| 输入  |     |          | 输出    |     |
|-----|-----|----------|-------|-----|
| $a$ | $b$ | $c_{in}$ | $c_o$ | $s$ |
| 0   | 0   | 0        | 0     | 0   |
| 0   | 0   | 1        | 0     | 1   |
| 0   | 1   | 0        | 0     | 1   |
| 0   | 1   | 1        | 1     | 0   |
| 1   | 0   | 0        | 0     | 1   |
| 1   | 0   | 1        | 1     | 0   |
| 1   | 1   | 0        | 1     | 0   |
| 1   | 1   | 1        | 1     | 1   |

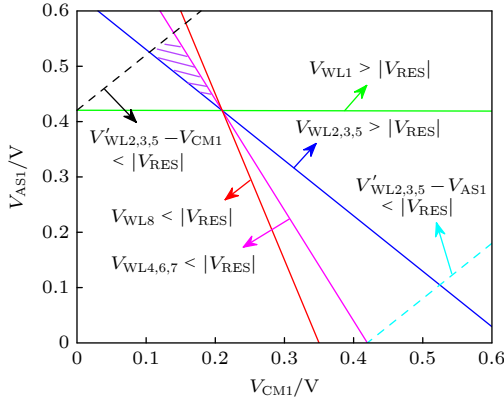


图 2 实现全加器输出进位操作电压  $V_{CM1}$  和  $V_{AS1}$  选择  
Fig. 2. Voltage selection of  $V_{CM1}$  and  $V_{AS1}$  for full adder carry-out operation.

同理, 为了实现加法运算的和, 操作电压  $V_{A2}$ ,  $V_{B2}$ ,  $V_{CIN2}$ ,  $V_{AS2}$ ,  $V_{CO}$  大小设置在  $[0, V_X]$  ( $V_X < V_{SET}$ ) 范围内. 当给全加器电路施加操作电压时, 输出忆阻器  $M_6$  根据  $a$ ,  $b$ ,  $c_{in}$  和  $c_o$  组合情况进行条件 RESET 切换. 也就是说, 对于特定的组合情况 ( $abc_{in}c_o = 0000, 0111, 1011, 1101$ ), 忆阻器  $M_6$  两端的电压  $V_{M6}$  ( $V_{M6} = V_{WL} - G = V_{WL}$ ) 大于  $|V_{RES}|$ , 将忆阻器  $M_6$  从低阻态  $R_L$  切换到高阻态  $R_H$ ; 而对于其他组合情况, 忆阻器  $M_6$  两端的电压  $V_{M6}$  小于  $|V_{RES}|$ , 忆阻器  $M_6$  保持在低阻态  $R_L$  不变. 根据基尔霍夫定律, 可得到:

$$\frac{V_{A2} - V_{WL}}{R_{M1}} + \frac{V_{B2} - V_{WL}}{R_{M2}} + \frac{V_{CIN2} - V_{WL}}{R_{M3}} + \frac{V_{AS2} - V_{WL}}{R_{M4}} + \frac{V_{CO} - V_{WL}}{R_{M5}} = \frac{V_{WL}}{R_{M6}}, \quad (18)$$

其中,  $R_{M6}$  是忆阻器  $M_6$  的阻值. 将  $R_{M4} = R_{M6} = R_L$  代入 (18) 式可得到:

$$V_{WL} = \left( \frac{1}{R_{M1}} + \frac{1}{R_{M2}} + \frac{1}{R_{M3}} + \frac{1}{R_{M5}} + \frac{2}{R_L} \right)^{-1} \times \left( \frac{V_{A2}}{R_{M1}} + \frac{V_{B2}}{R_{M2}} + \frac{V_{CIN2}}{R_{M3}} + \frac{V_{CO}}{R_{M5}} + \frac{V_{AS2}}{R_L} \right). \quad (19)$$

根据 (19) 式和表 1 全加器真值表中输入、输出情况, 可得到操作电压  $V_{A2}$ ,  $V_{B2}$ ,  $V_{CIN2}$ ,  $V_{AS2}$ ,  $V_{CO}$  的确认条件, 具体为

$$V_{WL1} = \left( \frac{4}{R_H} + \frac{2}{R_L} \right)^{-1} \left( \frac{V_{A2}}{R_H} + \frac{V_{B2}}{R_H} + \frac{V_{CIN2}}{R_H} + \frac{V_{CO}}{R_H} + \frac{V_{AS2}}{R_L} \right) > |V_{RES}|, \quad (20)$$

$$V_{WL2} = \left( \frac{3}{R_H} + \frac{3}{R_L} \right)^{-1} \left( \frac{V_{A2}}{R_H} + \frac{V_{B2}}{R_H} + \frac{V_{CIN2}}{R_L} + \frac{V_{CO}}{R_H} + \frac{V_{AS2}}{R_L} \right) < |V_{RES}|, \quad (21)$$

$$V_{WL3} = \left( \frac{3}{R_H} + \frac{3}{R_L} \right)^{-1} \left( \frac{V_{A2}}{R_H} + \frac{V_{B2}}{R_L} + \frac{V_{CIN2}}{R_H} + \frac{V_{CO}}{R_H} + \frac{V_{AS2}}{R_L} \right) < |V_{RES}|, \quad (22)$$

$$V_{WL4} = \left( \frac{1}{R_H} + \frac{5}{R_L} \right)^{-1} \left( \frac{V_{A2}}{R_H} + \frac{V_{B2}}{R_L} + \frac{V_{CIN2}}{R_L} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L} \right) > |V_{RES}|, \quad (23)$$

$$V_{WL5} = \left( \frac{3}{R_H} + \frac{3}{R_L} \right)^{-1} \left( \frac{V_{A2}}{R_L} + \frac{V_{B2}}{R_H} + \frac{V_{CIN2}}{R_H} + \frac{V_{CO}}{R_H} + \frac{V_{AS2}}{R_L} \right) < |V_{RES}|, \quad (24)$$

$$V_{WL6} = \left( \frac{1}{R_H} + \frac{5}{R_L} \right)^{-1} \left( \frac{V_{A2}}{R_L} + \frac{V_{B2}}{R_H} + \frac{V_{CIN2}}{R_L} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L} \right) > |V_{RES}|, \quad (25)$$

$$V_{WL7} = \left( \frac{1}{R_H} + \frac{5}{R_L} \right)^{-1} \left( \frac{V_{A2}}{R_L} + \frac{V_{B2}}{R_L} + \frac{V_{CIN2}}{R_H} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L} \right) > |V_{RES}|, \quad (26)$$

$$V_{WL8} = \left( \frac{6}{R_L} \right)^{-1} \left( \frac{V_{A2}}{R_L} + \frac{V_{B2}}{R_L} + \frac{V_{CIN2}}{R_L} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L} \right) < |V_{RES}|. \quad (27)$$



为了简化操作电压确认条件, 操作电压  $V_{A2}$ ,  $V_{B2}$ ,  $V_{CIN2}$  可选取相同大小的电压  $V_{CM2}$ , 于是,  $V_{WL2} = V_{WL3} = V_{WL5}$ ,  $V_{WL4} = V_{WL6} = V_{WL7}$ , 因而操作电压确认条件可简化为 4 个:

$$\left(\frac{4}{R_H} + \frac{2}{R_L}\right)^{-1} \left(\frac{3V_{CM2}}{R_H} + \frac{V_{CO}}{R_H} + \frac{V_{AS2}}{R_L}\right) > |V_{RES}|, \quad (28)$$

$$\left(\frac{3}{R_H} + \frac{3}{R_L}\right)^{-1} \left(\frac{2V_{CM2}}{R_H} + \frac{V_{CM2}}{R_L} + \frac{V_{CO}}{R_H} + \frac{V_{AS2}}{R_L}\right) < |V_{RES}|, \quad (29)$$

$$\left(\frac{1}{R_H} + \frac{5}{R_L}\right)^{-1} \left(\frac{V_{CM2}}{R_H} + \frac{2V_{CM2}}{R_L} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L}\right) > |V_{RES}|, \quad (30)$$

$$\left(\frac{6}{R_L}\right)^{-1} \left(\frac{3V_{CM2}}{R_L} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L}\right) < |V_{RES}|. \quad (31)$$

为了避免输入忆阻器  $M_1$ — $M_3$ 、辅助忆阻器  $M_4$  和输出忆阻器  $M_5$  的阻态被破坏, 在输出忆阻器  $M_6$  发生 RESET 切换情况下, 处于低阻态的输入忆阻器  $M_1$ — $M_3$ 、输出忆阻器  $M_5$  以及辅助忆阻器  $M_4$  两端电压都应小于  $|V_{RES}|$ . 于是, 电压  $V_{CM2}$  和  $V_{AS2}$  增加如下选择约束:

$$\left(\frac{5}{R_H} + \frac{1}{R_L}\right)^{-1} \left(\frac{3V_{CM2}}{R_H} + \frac{V_{CO}}{R_H} + \frac{V_{AS2}}{R_L}\right) - V_{AS2} < |V_{RES}|, \quad (32)$$

$$\left(\frac{2}{R_H} + \frac{4}{R_L}\right)^{-1} \left(\frac{V_{CM2}}{R_H} + \frac{2V_{CM2}}{R_L} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L}\right) - V_{CM2} < |V_{RES}|, \quad (33)$$

$$\left(\frac{2}{R_H} + \frac{4}{R_L}\right)^{-1} \left(\frac{V_{CM2}}{R_H} + \frac{2V_{CM2}}{R_L} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L}\right) - V_{CO} < |V_{RES}|, \quad (34)$$

$$\left(\frac{2}{R_H} + \frac{4}{R_L}\right)^{-1} \left(\frac{V_{CM2}}{R_H} + \frac{2V_{CM2}}{R_L} + \frac{V_{CO}}{R_L} + \frac{V_{AS2}}{R_L}\right) - V_{AS2} < |V_{RES}|. \quad (35)$$

根据 (28)—(35) 式即可确认操作电压  $V_{CM2}$ ,  $V_{AS2}$  和  $V_{CO}$  的大小. 因而, 全加器和的操作电压的确认条件是关于  $V_{CM2}$ ,  $V_{AS2}$  和  $V_{CO}$  的不等式, 可通过如图 3 所示的三维图确定, 如选择  $V_{CM2} = 0.1$  V,  $V_{AS2} = 0.45$  V 和  $V_{CO} = 0.45$  V.

## 2.2 基于忆阻器交叉阵列的全加器仿真实现

为了验证所提出的忆阻器全加器设计, 在 Cadence Virtuoso 中进行 SPICE (simulation program with integrated circuit emphasis) 仿真验证. 本文采用文献 [25] 中改进的模型对全加器进行仿真实验, 利用 MATLAB 基于该模型对 Cu/CuI/Pt 忆阻器  $I$ - $V$  特性曲线 (由半导体测试系统 B1500A 测得) 进行拟合, 图 4(a) 所示为拟合结果, 图 4(b) 列出了具体的拟合参数  $V_L$ ,  $V_H$ ,  $R_L$ ,  $R_H$ ,  $A_L$ ,  $A_H$ ,  $x_L$ ,  $x_H$ ,  $\alpha_L$  和  $\alpha_H$ , 其中  $V_{SET} = V_L$ ,  $V_{RES} = V_H$ . 基于拟合得到的参数, 构建 Verilog-A 模型, 用于后续的 SPICE 电路仿真. 根据 2.1 节给出的操作步骤和得到的操作电压, 第一步, 给位线  $BL_1$ ,  $BL_2$

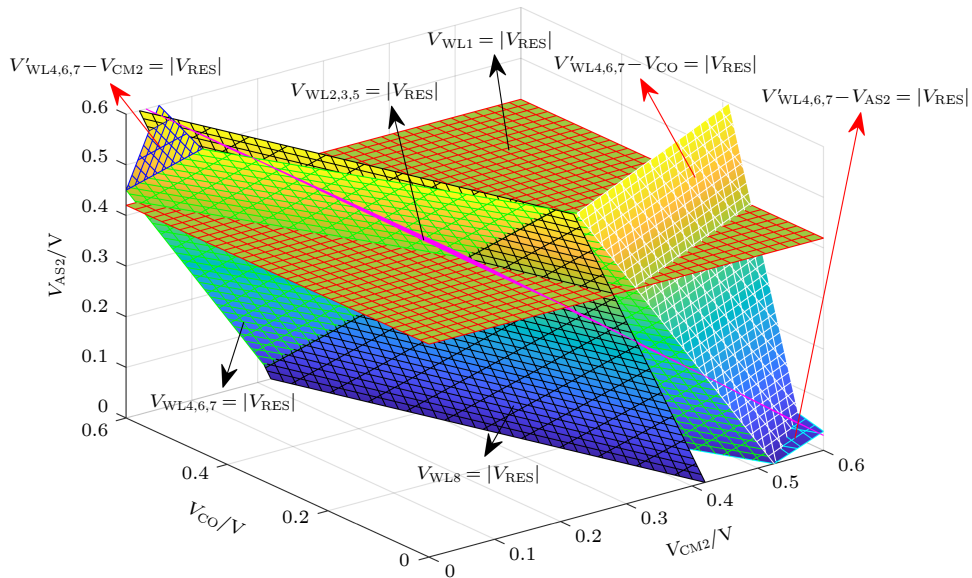


图 3 实现全加器和的操作电压  $V_{CM2}$ ,  $V_{AS2}$  及  $V_{CO}$  选择

Fig. 3. Voltage selection of  $V_{CM2}$ ,  $V_{AS2}$ , and  $V_{CO}$  for the full adder sum.

和  $BL_3$  施加 0.14 V 电压, 位线  $BL_4$  施加 0.52 V 电压, 而位线  $BL_5$  接地, 位线  $BL_6$  悬空; 第二步, 给位线  $BL_1$ ,  $BL_2$  和  $BL_3$  施加 0.1 V 电压, 位线  $BL_4$  和  $BL_5$  施加 0.45 V 电压, 而位线  $BL_6$  接地.

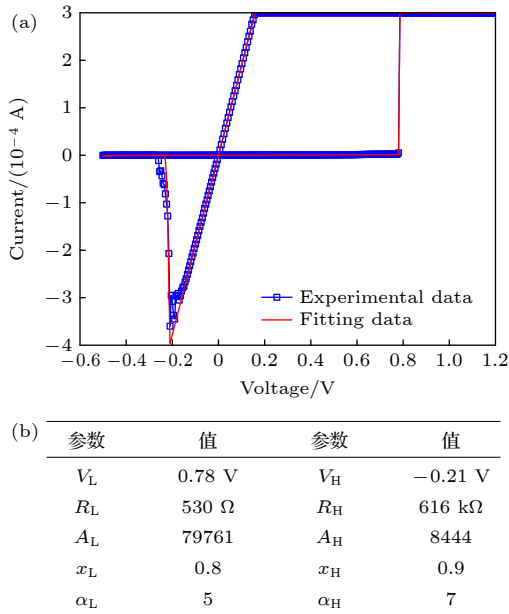


图 4 Cu/CuI/Pt 忆阻器拟合 (a) 电流-电压特性曲线; (b) 拟合器件参数

Fig. 4. Fitting of Cu/CuI/Pt memristor: (a) Current-voltage characteristic curves; (b) parameter fitting.

图 5 为 1 位全加器的所有 8 种输入情况的仿真结果, 其中浅紫色 (530.0  $\Omega$ ) 表示低电阻  $R_L$  (逻辑 1), 深紫色 (616.0 k $\Omega$ ) 表示高阻态  $R_H$  (逻辑 0). 图 5 从左往右的每一列依次显示被加数  $a$ 、加数  $b$ 、输入进位  $c_{in}$ 、辅助忆阻器、输出进位  $c_o$  以及和  $s$  对

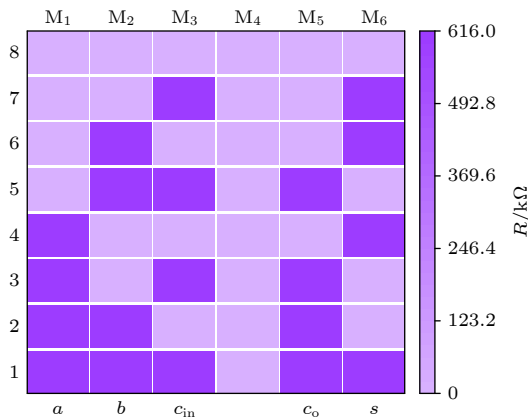


图 5 基于忆阻器的 1 位全加器所有 8 种输入情况下的仿真结果

Fig. 5. Simulation results for all 8 input cases of the memristor-based 1-bit full adder.

应的阻态, 每一行显示 1 位全加器的一种输入情况 (即  $abc_{in}$ ) 及其对应的输出 ( $c_o s$ ). 从下往上的每一行的输入组合依次为 000, 001, 010, 011, 100, 101, 110 和 111, 根据图 5, 得到的对应输出为 00, 01, 01, 10, 01, 10, 10 和 11, 该结果与表 1 所列的 1 位全加器真值表一致, 说明所设计的基于忆阻器的全加器电路有效.

### 2.3 忆阻器阻态变化对全加器运算性能的影响

在所提出的全加器中, 结点电压  $V_{WL}$  是实现正确运算的关键, 而该电压受忆阻器电阻窗口 ( $R_H/R_L$ ) 波动的影响. 图 6(a) 和图 6(b) 分别展示了计算输出进位  $c_o$  和本位和  $s$  时, 电阻窗口从 10 增大到 10000 的过程中结点电压  $V_{WL}$  的变化情况. 对于所有输入组合, 结点电压  $V_{WL}$  随电阻窗口的波动均较小, 尤其当  $R_H/R_L$  大于 500 时, 结点电压  $V_{WL}$  趋于稳定. 进一步由图 6(a) 可知, 当输入  $abc_{in}$  为 000, 001, 010, 100 时, 结点电压  $V_{WL1,2,3,5}$  始终大于

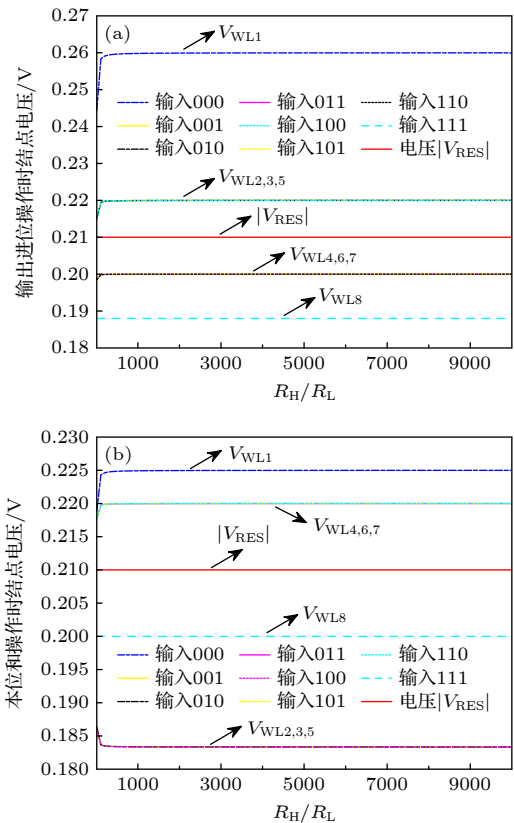


图 6 全加器结点电压随忆阻器电阻窗口的变化 (a) 计算输出进位  $c_o$  时; (b) 计算本位和  $s$  时

Fig. 6. Variation of full adder node voltage with memristor resistance window: (a) For the output carry  $c_o$  calculation; (b) for the sum  $s$  calculation.

RESET 电压绝对值  $|V_{\text{RES}}|$ , 对应输出进位  $c_0 = 0$ ; 其余输入组合下结点电压  $V_{\text{WL}4,6,7,8}$  始终小于  $|V_{\text{RES}}|$ , 对应  $c_0 = 1$ . 类似地, 图 6(b) 表明, 当输入  $abc_{\text{in}}$  为 000, 011, 101, 110 时, 结点电压  $V_{\text{WL}1,4,6,7}$  始终大于  $|V_{\text{RES}}|$ , 本位和  $s = 0$ ; 其余输入组合下结点电压  $V_{\text{WL}2,3,5,8}$  始终小于  $|V_{\text{RES}}|$ , 对应  $s = 1$ . 由此可见, 在  $R_{\text{H}}/R_{\text{L}}$  从 10 到 10000 的范围内, 结点电压  $V_{\text{WL}}$  与参考电压  $|V_{\text{RES}}|$  的相对关系始终保持不变, 全加器计算正确, 该设计对忆阻器阻态波动具有优异的鲁棒性.

## 2.4 基于忆阻器的全加器对比分析

本文设计的基于忆阻器交叉阵列的 1 位全加器突破了传统逻辑门组合设计思路, 其性能优势通过与现有基于忆阻器的全加器设计<sup>[23-27]</sup>的对比得到充分验证, 如图 7 所示. 操作步骤方面, 本文设计的全加器仅需 2 步即可完成运算, 相较于文献<sup>[23]</sup> (6 步)、文献<sup>[24]</sup> (4 步)、文献<sup>[25]</sup> (7 步)、文献<sup>[27]</sup> 串行架构 (13 步)、文献<sup>[27]</sup> 半串行架构 (15 步) 及文献<sup>[26]</sup> (6 步), 操作步骤显著减少, 步骤效率分别提升 200%, 100%, 250%, 550%, 650%, 200%. 器件开销方面, 本文设计的全加器仅需 6 个忆阻器即可实现运算功能, 无需额外辅助电阻器件, 而文献<sup>[23,24]</sup> 的设计除忆阻器外, 还需额外搭配无源电阻, 增加了硬件面积开销; 文献<sup>[25-27]</sup> 虽仅采用忆阻器, 但器件数量均多于本文方案, 其中文献<sup>[25]</sup> 需 9 个忆阻器、文献<sup>[27]</sup> 串行架构需 15 个忆阻器、文献<sup>[27]</sup> 半串行架构需 21 个忆阻器、文献<sup>[26]</sup> 需 8 个忆阻器. 综上, 本文设计的 1 位全加器在操作步骤与器件开销两方面均具备显著优势,

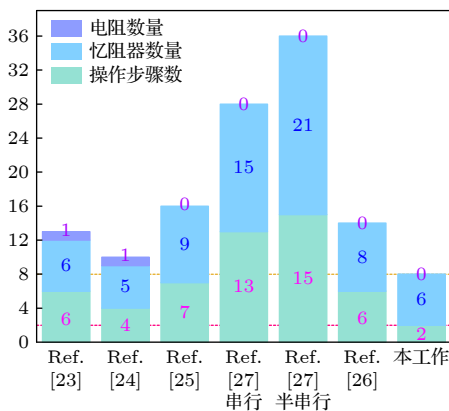


图 7 本工作设计的 1 位全加器与之前的设计比较

Fig. 7. Comparison of the proposed 1-bit full adder with prior designs.

有效解决了传统方案延迟高、面积开销大的缺陷, 实现了低开销、高效率的原位加法运算, 充分验证了所提的全加器在存内算术运算中的优势.

## 3 新型存内加解密电路构建与分析

### 3.1 基于全加器的存内加解密电路设计

传统加密需要频繁在内存与加密运算单元之间搬运图像、大数据等海量数据, 传输功耗占比极高. 硬件存算加密原位存储、原位运算, 减少数据搬运, 大幅降低传输功耗与延迟, 能效远高于传统 CPU (central processing unit)/GPU (graphics processing unit) 软件加密, 适配图像加密、边缘终端、物联网轻量化场景. 利用第 2 节设计的 1 位全加器操作方法, 基于忆阻器 (one-memristor, 1M) 交叉阵列可构建新型存内加解密电路, 充分发挥阵列的并行计算优势, 提升加解密速度. 但多行多列 1M 交叉阵列存在潜通路问题, 一晶体管一忆阻器 (one-transistor-one-memristor, 1T1M) 结构可有效解决该问题. 图 8(a) 所示的 1T1M 交叉阵列由晶体管和忆阻器构建, 每个交叉点包含一个 NMOS (N-metal-oxide-semiconductor) 晶体管和一个忆阻器, 同一列忆阻器的顶电极连接到位线 (bit line, BL), 同一列晶体管的栅极连接到栅线 (gate line, GL), 同一行晶体管的源极连接到字线 (WL). 所提 1 位全加器设计仍适用于 1T1M 结构, 其计算实现方式为: 向选定 GLs 施加电压  $V_G$  以导通对应晶体管 (等效闭合开关), 未选择 GLs 接地则对应晶体管不导通 (等效断开开关); 同时向选定 BLs 施加操作电压, 未选择 BLs 与选定 WLs 悬空, 并向未选择 WLs 施加电压  $V_{\text{iso}}$  以隔离未选择行.

存内加解密单元 (encryption-decryption unit, EDU) 由一位全加器构成 (如图 8(a) 所示), 其中 A, B, C, S 分别对应全加器的被加数  $a$ 、加数  $b$ 、输入进位  $c_{\text{in}}$  及和  $s$ , 单个加解密电路包含  $m \times n$  个 EDU 单元. 为实现图像加解密, 电路中 A, B, C 分别表示原始/加密图像、密钥 1、密钥 2, S 则输出加密/解密图像, 其核心原理为: 原始图像对应的二值矩阵 (1 对应忆阻器低阻态、0 对应高阻态) 与随机生成的密钥 1、密钥 2 矩阵相加得到加密图像, 加密图像与两密钥矩阵再次相加即可完成解密. 提出两种加解密方式: 第一种为半并行式, 如图 8(b) 所示, 由  $m \times n$  个 EDU 构成加解密交叉阵列, 每次



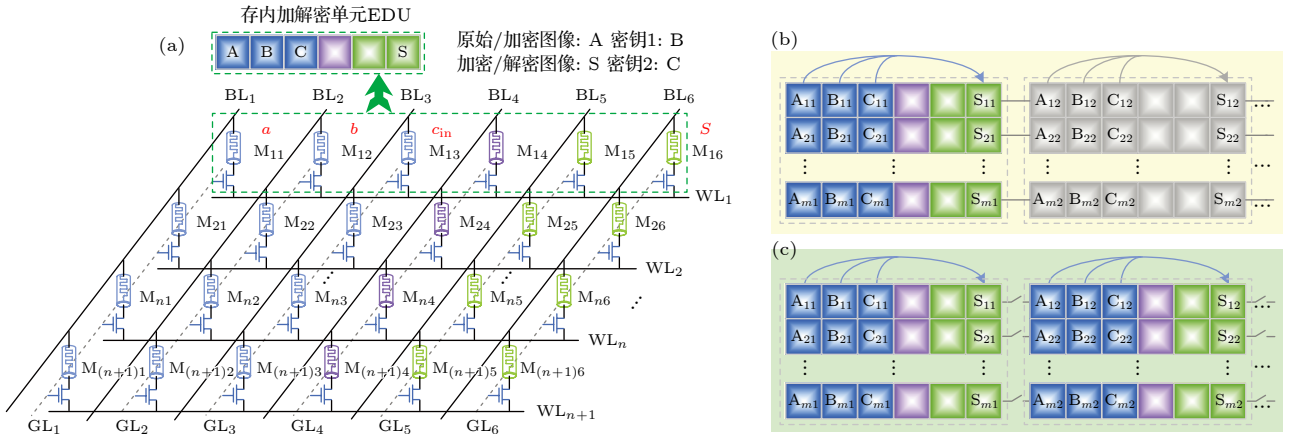


图 8 基于全加器的存内加解密电路图 (a) 基于全加器的加解密单元; (b) 半并行加解密电路结构示意图; (c) 全并行加解密电路结构示意图

Fig. 8. Full-adder-based in-memory encryption/decryption circuits: (a) Full-adder-based encryption/decryption unit; (b) semi-parallel architecture schematic; (c) fully-parallel architecture schematic.



图 9 图像二值化示意图

Fig. 9. Schematic diagram of image binarization.

仅用一列 EDU 并行处理图像某一列所有像素, 逐列依次完成加密 (解密), 处理  $m \times n$  二值图像需  $2n$  步操作; 第二种为全并行式, 如图 8(c) 所示, 通过开关断开交叉阵列各列, 使不同列 EDU 可同时处理图像所有列像素, 仅需 2 步即可完成全部加密 (解密) 操作。

### 3.2 图像加解密实验

为验证方案有效性, 选用  $256 \times 256$  图像 (见图 9) 开展实验. 首先通过 MATLAB 的 `rgb2gray` 函数灰度化、`imbinarize` 函数二值化, 得到对应二进制矩阵; 随后创建两个与该矩阵尺寸一致的随机密钥矩阵; 采用图 8(c) 所示的全并行方式对三个矩阵进行加法运算, 得到加密矩阵以完成加密; 最终将加密矩阵与两密钥矩阵相加, 得到解密图像, 如图 10 所示. 对比加解密前后图像可知, 该基于全加器的存内加解密电路可成功实现图像加解密. 硬件存内加密突破了传统软件加密的性能瓶颈, 从

物理底层构建了信息安全防护体系, 在图像加密、边缘物联网、隐私计算等领域具有重要理论与工程应用价值, 是后摩尔时代信息安全硬件化的重要发展方向。

## 4 $n$ 位行波进位加法器设计与分析

### 4.1 基于全加器的 $n$ 位行波进位加法器设计

利用 1 位全加器可实现  $n$  位行波进位加法器, 须在 1T1M 交叉阵列内执行复制 (COPY) 逻辑运算, 以将一个忆阻器的阻态复制到另一个忆阻器. 图 11 所示为基于 1T1M 阵列的 COPY 逻辑电路图, 包含三个 1T1M 单元, 其中橘色、蓝色、紫色忆阻器分别为输入、输出及辅助忆阻器. 其实现方法为: 向参与逻辑运算忆阻器所在列的 GL 施加电压  $V_G$ , 向输入、输出、辅助忆阻器所在行的 WL 分别施加电压  $0.8V_{CP}$ ,  $V_{CP}$ ,  $0.1V_{CP}$  (满足  $2|V_{RES}| < V_{CP} < V_{SET}$ ), 未选择的 GLs 接地, 所有 BLs 与未选择 WLs



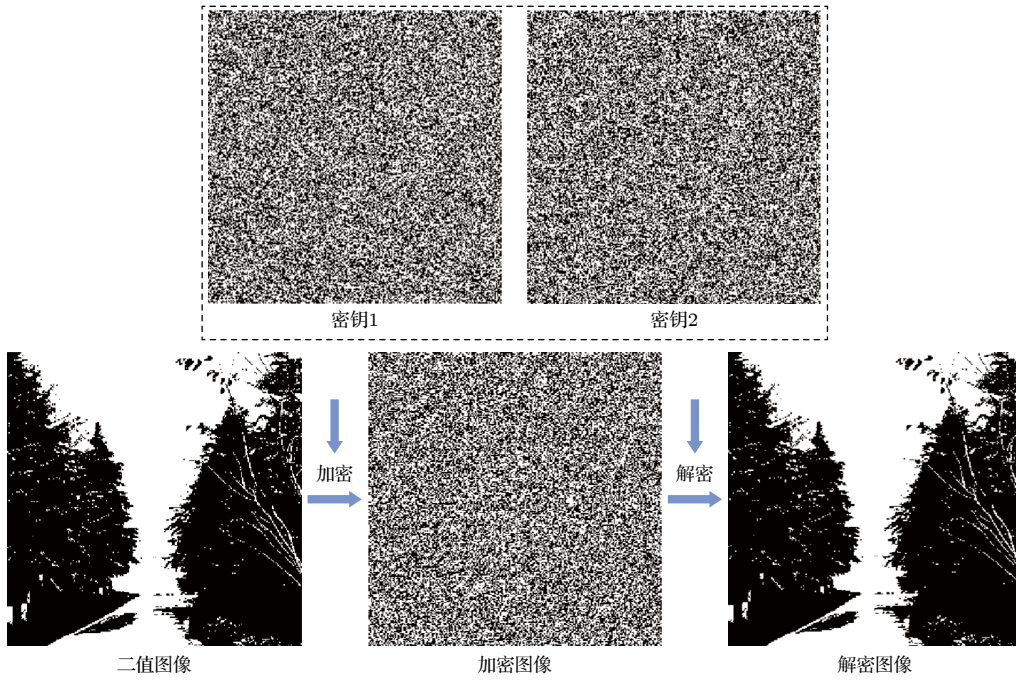


图 10 二值图像加解密

Fig. 10. Encryption and decryption of the binary image.

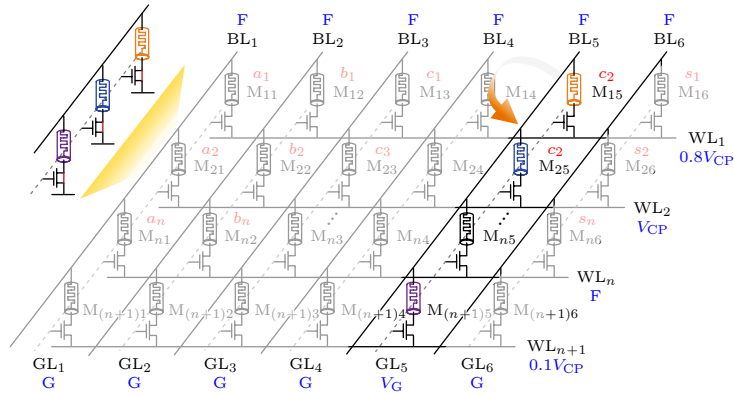


图 11 基于 1T1M 的交叉阵列及其 COPY 逻辑运算实现示意图

Fig. 11. Schematic diagram of a 1T1M-based crossbar array and its COPY logic operation implementation.

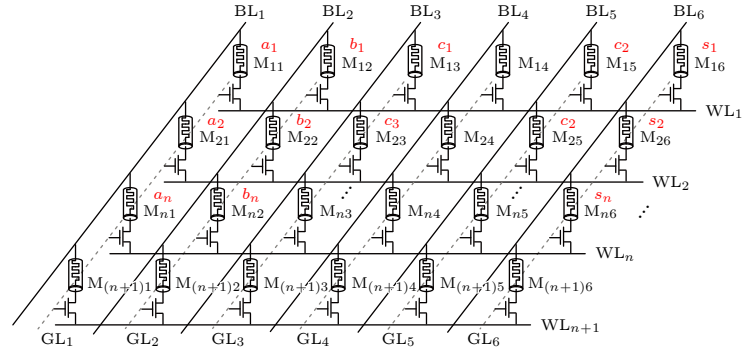
悬空, 如图 11 所示, 即可将忆阻器  $M_{15}$  中存储的数据  $c_2$  复制到忆阻器  $M_{25}$  中。

图 12 所示为基于 1T1M 交叉阵列的  $n$  位行波进位加法器, 被加数  $a_i$  和加数  $b_i$  ( $i = 1, 2, 3, \dots, n$ ) 分别存储于 1T1M 交叉阵列第一列和第二列忆阻器中, 最低位输入进位  $c_1$  存储于忆阻器  $M_{13}$  中。计算前, 假设所有输入已预存于对应忆阻器中, 阵列中其余忆阻器均设为低阻态。由于第  $i$  位输出进位  $c_{i+1}$  与第  $i-1$  位输出进位  $c_i$  相关, 需串行计算每一位输出进位, 即先计算第  $i-1$  位输出进位  $c_i$ , 再将  $c_i$  复制到同列第  $i$  行忆阻器, 重复该串行计算与 COPY 操作, 直至得到所有输出进位; 随后, 分

别并行计算奇数位和  $s_i$  ( $i = 1, 3, 5, \dots$ ) 与偶数位和  $s_i$  ( $i = 2, 4, 6, \dots$ )。该  $n$  位行波进位加法器的完整操作过程如表 2 所述, 共需  $2n + 1$  个操作步骤。

## 4.2 4 位行波进位加法器实验

以 4 位行波进位加法器为例, 根据表 2, 实现 4 位加法器需要 9 步, 图 13 给出了操作示意图, 其中一个圆圈表示一个 1T1M 单元, 蓝色、绿色、紫色和灰色圆圈分别表示输入、输出、辅助和未选择单元。图 14 所示为 4 位行波进位加法器的 SPICE 仿真结果, 为清晰展示时序变化与忆阻器阻态特性, 仿真单步操作时长设为 1 s, 该时间并非忆阻器实际响应时间。图 14(a) 所示为 4 位行波进位加法

图 12 基于 1T1M 交叉阵列的  $n$  位行波进位加法器示意图Fig. 12. Schematic of an  $n$ -bit ripple-carry adder using a 1T1M crossbar array.表 2 基于 1T1M 交叉阵列实现  $n$  位行波进位加法器的操作算法Table 2. Operation algorithm for  $n$ -bit ripple carry adder implemented on a 1T1M crossbar array.

输入: 被加数  $a_i (i = 1, 2, 3, \dots, n)$  存储在  $BL_1$  的  $M_{i1}$  中, 加数  $b_i$  存储在  $BL_2$  的  $M_{i2}$  中, 输入进位  $c_1$  存储在  $M_{13}$ ; 输出: 第  $i$  位的输入进位  $c_i$ 、输出进位  $c_{i+1}$  存储在  $BL_3$  的  $M_{i3}$  或者  $BL_5$  的  $M_{i5}$  中; 和  $s_i$  存储在  $BL_6$  的  $M_{i6}$  中.

Begin

$i = 1$ ;

//串行计算

for 每个输入  $a_i, b_i, c_i$  do

if  $i$  为奇数 then

对  $M_{i1}, M_{i2}, M_{i3}, M_{i4}, M_{i5}$  进行输出进位操作, 同时得到的输出进位结果  $c_{i+1}$  存储在  $M_{i5}$  中;

if ( $i < n$ ) then

对  $M_{i5}, M_{(i+1)5}, M_{(n+1)5}$  进行 COPY 逻辑运算, 同时运算结果  $c_{i+1}$  存储在  $M_{(i+1)5}$ ;

end if

else

对  $M_{i1}, M_{i2}, M_{i3}, M_{i4}, M_{i5}$  进行输出进位操作, 同时得到的输出进位结果  $c_{i+1}$  存储在  $M_{i3}$  中;

if ( $i < n$ ) then

对  $M_{i3}, M_{(i+1)3}, M_{(n+1)3}$  进行 COPY 逻辑运算, 同时运算结果  $c_{i+1}$  存储在  $M_{(i+1)3}$ ;

end if

end if

$i = i + 1$ ;

end for

//并行计算

for 奇数位的操作数  $a_i, b_i, c_i, c_{i+1}$  do

对阵列的  $BL_1, BL_2, BL_3, BL_4, BL_5$  和  $BL_6$  并行进行奇数位的和操作, 得到所有奇数位的  $s_i$ , 同时  $s_i$  存储在  $BL_6$  的  $M_{i6}$  中;

end for

for 偶数位的操作数  $a_i, b_i, c_i, c_{i+1}$  do

对阵列的  $BL_1, BL_2, BL_3, BL_4, BL_5$  和  $BL_6$  并行进行偶数位的和操作, 得到所有偶数位的  $s_i$ , 同时  $s_i$  存储在  $BL_6$  的  $M_{i6}$  中;

end for

return  $c_{i+1}$  和  $s_i$ ;

end

器的输入, 其中表示  $a_4, a_3, a_2, a_1, b_4, b_3, b_2, b_1$  和  $c_1$  的忆阻器电阻状态分别为  $R_L, R_L, R_L, R_L, R_H, R_H, R_H, R_L$  和  $R_H$ , 意味着被加数、加数和最低位输入进位分别为 1111, 0001 和 0. 从图 14(a) 可知, 在逻辑操作期间, 表示输入的忆阻器电阻状态一直保持不变. 图 14(b) 所示为 4 位行

波进位加法器的输出, 表示  $c_5, c_4, c_3, c_2, s_4, s_3, s_2$  和  $s_1$  的忆阻器电阻状态分别为  $R_L, R_L, R_L, R_L, R_H, R_H, R_H$  和  $R_H$ , 得到输出进位 1111 及和 0000, 这与 1111, 0001 和 0 相加的理论结果一致, 验证了所提出的  $n$  位行波进位加法器在 1T1M 阵列中的可行性.

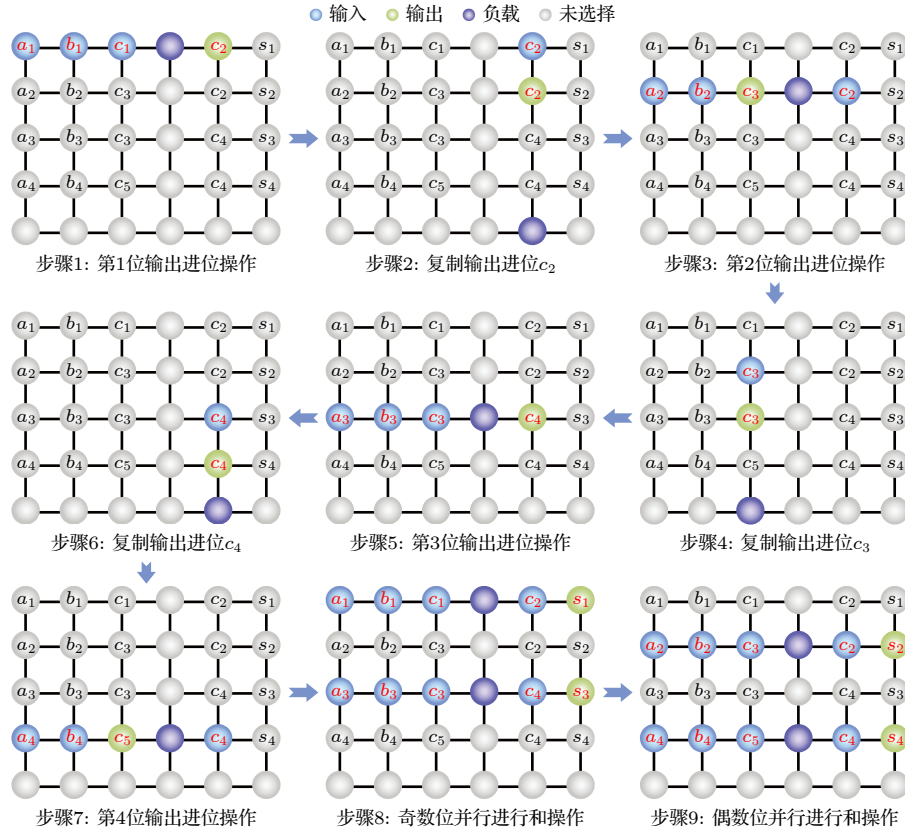


Fig. 13. Operation schematic of a 4-bit ripple carry adder.

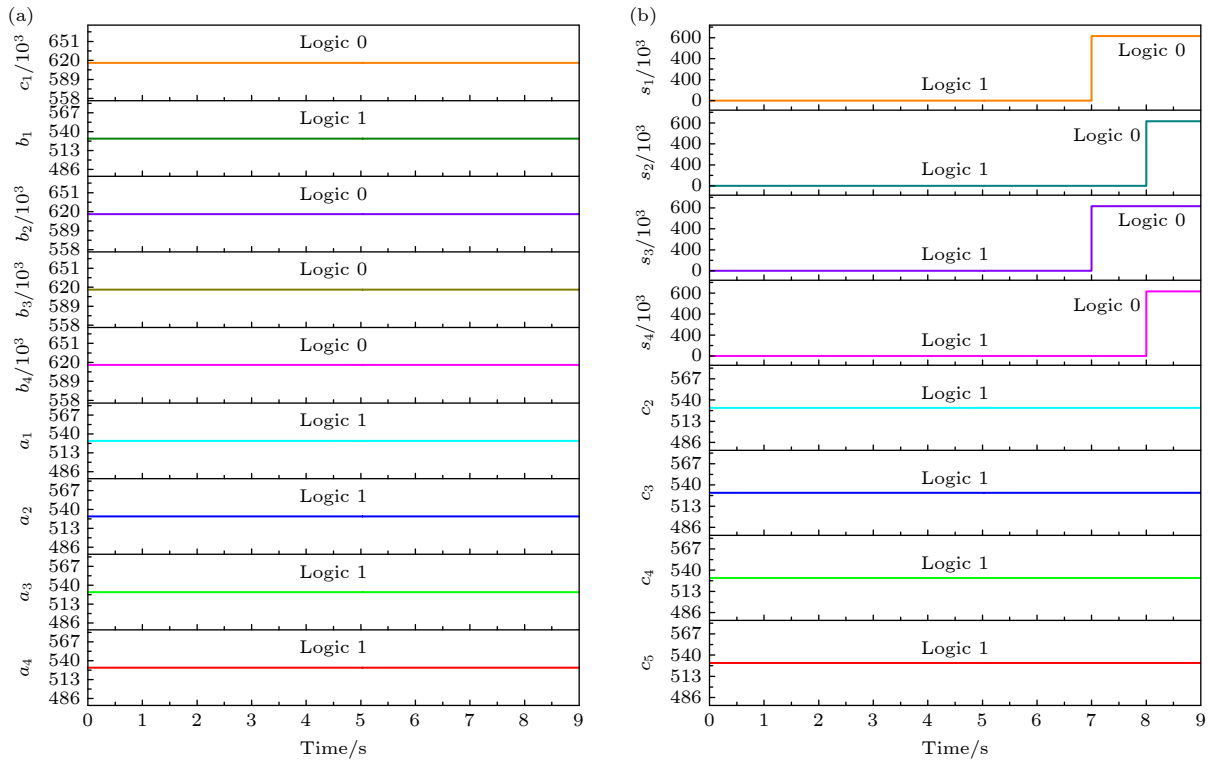


Fig. 14. SPICE simulation results of a 4-bit ripple carry adder based on a memristor array: (a) Augend  $a_4a_3a_2a_1$  (1111), addend  $b_4b_3b_2b_1$  (0001), and least significant bit input carry  $c_1$  (0); (b) output carries  $c_5c_4c_3c_2$  (1111) and sum  $s_4s_3s_2s_1$  (0000).

### 4.3 $n$ 位加法器对比分析

为客观评价本文所设计行波进位加法器的综合性能, 采用文献 [28] 提出的品质因数 (FoM) 作为评价指标, 该指标综合考量操作步骤数量 ( $N_S$ ) 与所需忆阻器数量 ( $N_M$ ) 两个核心性能参数, 其中,  $FoM_B$  为  $N_S$  与  $N_M$  同等权重下的品质因数, 其计算方式如 (36) 式所示;  $FoM_S$  则侧重于对加法器操作步骤数的全面评估, 计算方式如 (37) 式所示.

$$FoM_B = \frac{1}{N_S N_M}, \quad (36)$$

$$FoM_S = \frac{1}{N_S^2 N_M}. \quad (37)$$

为清晰展示本文加法器的性能改进效果, 图 15 给出了本文设计与现有方案 [22,25-27,29] 中 64 位行波进位加法器的综合性能对比, 其中  $IMP_B$  表示本文  $FoM_B$  与现有对应设计  $FoM_B$  的比值 (即性能改进幅度),  $IMP_S$  表示本文  $FoM_S$  与现有对应设计  $FoM_S$  的比值. 由图 15 可知, 无论基于  $FoM_B$  还是  $FoM_S$  指标, 本文设计均优于现有设计方案 [22,25-27,29]. 在  $FoM_B$  指标下, 性能改进幅度范围为  $1.37 \times -12.18 \times$ ; 在  $FoM_S$  指标下, 性能改进幅度范围为  $1.80 \times -41.98 \times$ . 这表明, 无论在操作步骤数与忆阻器数同等重要的场景, 还是侧重操作步骤数优化的场景, 本文所设计的行波进位加法器均具备显著的综合性能优势.

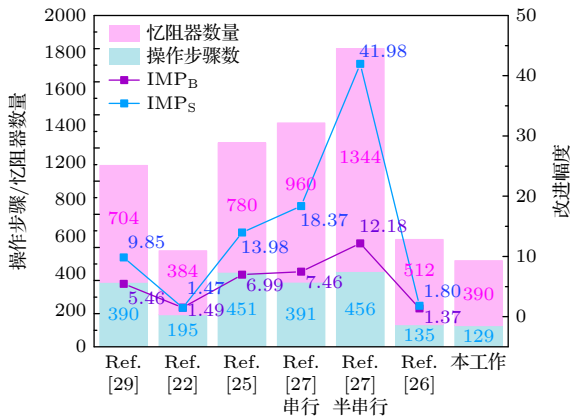


图 15 本工作 64 位加法器与现有设计比较

Fig. 15. Comparison of our 64-bit adder with prior designs.

## 5 结 论

本文提出了一种基于忆阻器交叉阵列的存内加法器设计方案, 完成了存内加解密电路及  $n$  位行

波进位加法器的设计与验证. 与现有方案对比表明, 所设计的 1 位全加器仅需 6 个忆阻器和 2 步操作, 在器件开销与运算效率方面均具有显著优势; 基于该全加器构建的存内加解密电路实现了存储、运算与加解密功能的一体化融合, 能够适配安全敏感应用场景; 设计的  $n$  位行波进位加法器经品质因数评估, 在  $FoM_B$  与  $FoM_S$  指标下, 性能改进幅度分别达到  $1.37 \times -12.18 \times$  和  $1.80 \times -41.98 \times$ , 综合性能优于现有设计. 研究结果表明, 本文设计方案有效突破了传统忆阻器加法器的性能瓶颈, 兼顾了运算效率和硬件开销, 为忆阻器交叉阵列在存算一体中的应用奠定了理论基础并提供了技术参考.

## 参考文献

- [1] He Y, Ma C, Jia Z, Su Y, Tang J 2026 *Nat. Rev. Electr. Eng.* **3** 139
- [2] Yan A, Yan J, Shen P, et al. 2026 *Nature* **649** 1165
- [3] Mannocci P, Zucchelli C, Andreoli I, Pezzoli A, Melacarne E, Pedretti G, Sancandi F, Villa C, Sun Z, Spagnolini U 2026 *Nature Electronics* **9** 200
- [4] Zhao L, Gao S F, Zhang S B, Qiu X, Yang F, Li J, Chen Z Z, Zhao Y 2022 *Sci. China Inf. Sci.* **52** 176 (in Chinese) [赵亮, 高世凡, 张圣波, 邱翔, 杨帆, 李杰, 陈泽志, 赵毅 2022 *中国科学: 信息科学* **52** 176]
- [5] Ortner T, Petschenig H, Vasilopoulos A, Renner R, Brglez Š, Limbacher T, Piñero E, Linares-Barranco A, Pantazi A, Legenstein R 2025 *Nat. Commun.* **16** 1243
- [6] Ansari M H R, El-Atab N 2024 *IEEE Trans. Electron Devices* **71** 1879
- [7] Ji X, Dong Z, Han Y, Lai C S, Qi D 2023 *IEEE Trans. Circuits Syst. Video Technol.* **33** 7928
- [8] Zheng H, Liu H W, Fang Y X, Fan D Y, Han Y H, Hou C Y, Liu W, Xia Z L, Huo Z L 2025 *Acta Phys. Sin.* **74** 248502 (in Chinese) [郑好, 刘慧雯, 方语萱, 范冬宇, 韩玉辉, 侯春源, 刘威, 夏志良, 霍宗亮 2025 *物理学报* **74** 248502]
- [9] Kim S, Shin D H, Choi W, et al. 2026 *Adv. Mater.* **38** e10635
- [10] Lanza M, Pazos S, Aguirre F, et al. 2025 *Nature* **640** 613
- [11] Wang Z, Song W, Wang T, et al. 2025 *Sci. Adv.* **11** ead3436
- [12] Gao S, Ding S, Ho-Ching Iu H, Erkan U, Toktas A, Simsek C, Wu R, Xu X, Cao Y, Mou J 2025 *Chaos* **35** 073105
- [13] Zhu Y Y, Yang Z Y, Yang S N, Zhang Y F, Zhang M, Wang X, Wang H J, Xu J 2025 *Acta Phys. Sin.* **74** 217301 (in Chinese) [朱媛媛, 杨梓怡, 杨淑宁, 张云飞, 张苗, 王鑫, 王红军, 徐静 2025 *物理学报* **74** 217301]
- [14] You J, Hu Y, Yang D, Lin Y, Meng W, Xu N, Sun L 2025 *Adv. Electron. Mater.* **11** 2500221
- [15] Gao K, Sun B, Cao Z, Duan X, Yan W, Tong G, Zhou G, Chen X, Shao J 2024 *Advanced Functional Materials* **34** 2401132
- [16] Tun T T T, Mitra S, Su H, Huo J, Zheng H, Bosman M, Ang Y S, Ang K W 2026 *Adv. Funct. Mater.* **36** e28751
- [17] Wind L, Maierhofer M, Fuchsberger A, Sistani M, Weber W M 2024 *IEEE Electron Device Lett.* **45** 724
- [18] Seiler F, TaheriNejad N 2024 *IEEE Trans. Circuits Syst. Regul. Pap.* **71** 5141
- [19] Yao L, Wu J, Liu P, Lam S K 2026 *IEEE Trans. Circuits*



- Syst. Regul. Pap.* **73** 411
- [20] Fu X, Li Q, Wang W, Xu H, Wang Y, Wang W, Yu H, Li Z 2022 *IEEE Trans. Circuits Syst. Express Briefs* **69** 3889
- [21] Wang X Y, Dong C T, Huang J T, Li H, Iu H H C, Kang S M 2026 *Int. J. Circuit Theory Appl.* DOI: 10.1002/cta.70385
- [22] Song Y, Wang X, Wu Q, Yang F, Wang C, Wang M, Miao X 2022 *Adv. Sci.* **9** 2200036
- [23] de Dias C S, de Lima H S, Brum R M, Butzen P F 2025 *IEEE Trans. Circuits Syst. Regul. Pap.* **72** 4686
- [24] Gan Z, Zhang C, Yang F, Zhang D, Ma Y, Huang M, Miao X, Wang X 2025 *IEEE Trans. Electron Devices* **72** 1118
- [25] Luo L, Li B, Wang L, Tan J, Duan S, Zhu C 2024 *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **32** 835
- [26] Park J, Lee J, Youn S, Kim H 2026 *Adv. Intell. Syst.* **8** e202501001
- [27] Senthil S J, Srinivasu B 2025 *38th International Conference on VLSI Design and 2024 23rd International Conference on Embedded Systems (VLSID)* (IEEE), Bangalore, India, January 4–8, 2025 p534
- [28] Radakovits D, TaheriNejad N, Cai M, Delaroche T, Mirabbasi S 2020 *IEEE Trans. Circuits Syst. Regul. Pap.* **67** 1495
- [29] Cheng L, Li Y, Yin K S, Hu S Y, Su Y T, Jin M M, Wang Z R, Chang T C, Miao X S 2019 *Adv. Funct. Mater.* **29** 1905660

# Design of a low-overhead in-memory adder and encryption-decryption circuit based on memristor crossbar array<sup>\*</sup>

LUO Li<sup>1)2)3)</sup> SHI Shaotian<sup>1)</sup> ZHANG Fengyun<sup>1)2)3)†</sup> DUAN Shukai<sup>1)2)3)‡</sup>

1) (College of Artificial Intelligence, Southwest University, Chongqing 400715, China)

2) (National & Local Joint Engineering Research Center of Intelligent Transmission and Control Technology, Chongqing 400715, China)

3) (Chongqing Key Laboratory of Brain-inspired Computing and Intelligent Control, Chongqing 400715, China)

( Received 12 May 2026; revised manuscript received 28 May 2026 )

## Abstract

The adder is a core arithmetic component in modern microprocessors, cryptographic circuits, and other systems. Most existing memristor-based full adders adopt the cascaded discrete basic logic gate approach, which leads to large device overhead and long operation steps, making it difficult to meet the requirements of high-speed data processing and real-time encryption. To address these issues, this paper first designs a low-overhead full adder circuit based on the memristor array, which consists of input memristors, output memristors, and an auxiliary memristor. The entire computation is performed within the memristors, using the high-resistance state and low-resistance state to represent logic 0 and logic 1, respectively. Based on Ohm's law, Kirchhoff's law, and the full adder truth table, a detailed derivation of the circuit is carried out, and the operating voltages are determined. During computation, specific operating voltages are applied to the bit lines of involved memristors, triggering conditional resistance switching of the output memristor determined by inputs. The proposed full adder requires only six memristors and two operation steps to produce the sum and carry, outperforming existing schemes in both device count and operation efficiency.

Based on the above one-bit full adder, this paper further adopts a one-transistor-one-memristor (1T1M) array to construct an in-memory encryption-decryption circuit. The circuit uses a single-bit full adder as the basic unit to form an encryption-decryption unit (EDU), and an  $m \times n$  array of EDUs is integrated to form the encryption-decryption array. For image encryption and decryption applications, two operating modes are developed: 1) Semi-parallel mode: a single column of EDUs is activated at a time to process all pixels in one column of the image in parallel, completing encryption or decryption column by column. Processing an  $m \times n$  binary image requires only  $2n$  operation steps. 2) Fully parallel mode: by disconnecting the columns of the

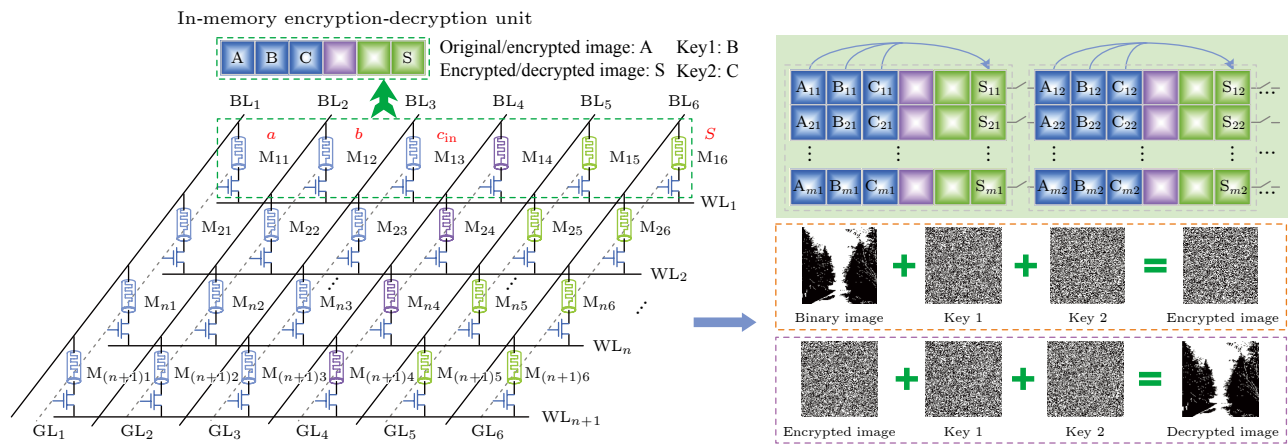
<sup>\*</sup> Project supported by the Natural Science Foundation of Chongqing, China (Grant Nos. CSTB2024NSCQ-MSX0586, CSTB2024NSCQ-MSX0302) and the National Natural Science Foundation of China (Grant Nos. 62576291, 62306246).

<sup>†</sup> Corresponding author. E-mail: zhangfy24@swu.edu.cn

<sup>‡</sup> Corresponding author. E-mail: duansk@swu.edu.cn

array through switches, all columns of EDUs can simultaneously process all columns of pixels, completing the encryption or decryption of the entire image in only 2 steps. Verification using  $256 \times 256$  binary images shows, by comparing the images before and after encryption and decryption, that the proposed encryption-decryption circuit can correctly perform image encryption and decryption.

Finally, this paper proposes a COPY logic operation based on the 1T1M crossbar array, which can copy the resistance state of one memristor to another. By integrating the proposed full adder and COPY gate, an  $n$ -bit ripple-carry adder is designed. Specifically, the output carry  $c_i$  of the  $(i-1)$ -th bit is calculated serially and copied to the memristor at the  $i$ -th row of the same column via COPY operation. This serial computation and copying process is iterated until all carries  $c_{i+1}$  ( $i=1, 2, 3, \dots$ ) are generated. Subsequently, the odd-indexed sums  $s_i$  ( $i=1, 3, 5, \dots$ ) and the even-indexed sums  $s_i$  ( $i=2, 4, 6, \dots$ ) are computed in parallel, respectively. The complete operation of this  $n$ -bit ripple-carry adder requires only  $2n+1$  operation steps. Compared with existing works, the proposed design achieves improvements of  $1.37\times$  to  $12.18\times$  in  $\text{FoM}_B$  (equally weighted by step and device count) and  $1.80\times$  to  $41.98\times$  in  $\text{FoM}_S$  (weighted toward step count), exhibiting distinctly superior overall performance.



**Keywords:** memristor, in-memory computing, full adder, encryption-decryption circuit

**DOI:** [10.7498/aps.75.20260679](https://doi.org/10.7498/aps.75.20260679)

**CSTR:** [32037.14.aps.75.20260679](https://cstr.net.cn/32037.14.aps.75.20260679)

## 基于忆阻器交叉阵列的低开销存内加法器及加解密电路设计

罗丽 石绍田 张凤运 段书凯

## Design of a low-overhead in-memory adder and encryption-decryption circuit based on memristor crossbar array

LUO Li SHI Shaotian ZHANG Fengyun DUAN Shukai

引用信息 Citation: *Acta Physica Sinica*, 75, 120004 (2026) DOI: 10.7498/aps.75.20260679

CSTR: 32037.14.aps.75.20260679

在线阅读 View online: <https://doi.org/10.7498/aps.75.20260679>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

---

### 您可能感兴趣的其他文章

#### Articles you may be interested in

#### 基于忆阻器阵列的下一代储池计算

Next-generation reservoir computing based on memristor array

物理学报. 2022, 71(14): 140701 <https://doi.org/10.7498/aps.71.20220082>

#### 基于非挥发存储器的存内计算技术

Non-volatile memory based in-memory computing technology

物理学报. 2022, 71(14): 148507 <https://doi.org/10.7498/aps.71.20220397>

#### 基于忆阻器的脉冲神经网络硬件加速器架构设计

Memristor based spiking neural network accelerator architecture

物理学报. 2022, 71(14): 148401 <https://doi.org/10.7498/aps.71.20220098>

#### 面向类脑计算的低电压忆阻器研究进展

Recent progress of low-voltage memristor for neuromorphic computing

物理学报. 2024, 73(20): 207302 <https://doi.org/10.7498/aps.73.20241022>

#### 蔡氏结型忆阻器的简化及其神经元电路的硬件实现

Simplification of Chua corsage memristor and hardware implementation of its neuron circuit

物理学报. 2023, 72(7): 070501 <https://doi.org/10.7498/aps.72.20222013>

#### 基于忆阻器的新型混沌系统的动力学、周期轨道及其在图像加密中的应用

Dynamics, periodic orbit, and image encryption of a new four-order memristor chaotic system

物理学报. 2026, 75(2): 070501 <https://doi.org/10.7498/aps.75.20251190>