基于忆阻器 -CMOS 的通用逻辑电路及其应用

杨辉^{1,2}, 段书凯^{1,2*}, 董哲康^{3,4}, 王丽丹^{1,2}, 胡小方⁵, 尚柳汀^{1,2}

1. 西南大学电子信息工程学院, 重庆 400715

2. 西南大学非线性电路重庆市重点实验室, 重庆 400715

3. 浙江大学电气工程学院, 杭州 310027

4. 香港理工大学电机工程系, 香港 999077

5. 西南大学计算机科学与信息科学学院, 重庆 400715

* 通信作者. E-mail: duansk@swu.edu.cn

收稿日期: 2018-09-10; 修回日期: 2019-01-02; 接受日期: 2019-03-21; 网络出版日期: 2020-02-12

国家重点研发计划 (批准号: 2018YFB1306600)、国家自然科学基金 (批准号: 61571372, 61672436, 61601376)、重庆市基础科学与前沿技术研究专项重点项目 (批准号: cstc2017jcyjBX0050, cstc2016jcyjA0547)、中央高校基本科研业务费 (批准号: XDJK2016A001, XDJK2017A005) 和西南大学博士基金 (批准号: SWU116005) 资助项目

摘要 忆阻器是一种具有阻值开关特性的信息存储器件. 由于忆阻器件具有可变电导性, 其组合电路可应用与逻辑运算. 本文提出了一种新的忆阻器 -CMOS 逻辑电路, 能够在同一电路中同时实现 AND-OR-XOR-XNOR 4 种基本的逻辑操作. 相较于 MAD Gates, MRL, IMPLY 逻辑电路, 忆阻器数量和功耗均有大幅降低, 电路性能更优, 电路效率大幅提高. 在此基础上设计了一种新的全加电路及二值图像加密电路. 与现有忆阻器逻辑加法电路相比, 本文设计的加法电路在元件数量上同样具有极大的优势. 本文设计的二值图像加密电路能够用两种不同的加密方式实现图像加密, 密钥与电路相互独立, 提高了加密结果的可靠性.

关键词 忆阻器, 逻辑运算, 忆阻器 -CMOS 逻辑, 全加电路, 二值图像加密

1 引言

1971 年, Chua^[1] 根据电路完备性理论提出了除电容、电感、电阻之外的第 4 种基本电路元件, 称其为忆阻器, 理论上定义了忆阻器, 描述了其物理特性. 然而, 忆阻器物理实物一直没有被研制出来, 所以并没有引起研究学者太多的关注. 直到忆阻器实物的出现^[2,3] 及忆阻器的 SPICE 仿真模型的提出^[4,5], 立即引起了研究人员以及工业界的广泛关注. 忆阻器具有掉电后信息非易失特性且阻值的二值性明显, 因此在信息存储及逻辑运算等领域有巨大的应用潜能. Emara 等^[6] 和 Shaarawy 等^[7] 将忆阻器与二极管相结合, 提出了 1T2M, 2T2M 存储结构替代原有的由 6 个二极管构成的随机存储单元.

引用格式: 杨辉, 段书凯, 董哲康, 等. 基于忆阻器 -CMOS 的通用逻辑电路及其应用. 中国科学: 信息科学, 2020, 50: 289–302, doi: 10.1360/N112018-00247
Yang H, Duan S K, Dong Z K, et al. A memristor-CMOS-based general-logic circuit and its applications (in Chinese). Sci Sin Inform, 2020, 50: 289–302, doi: 10.1360/N112018-00247

Sarwar 等^[8]将忆阻器与 CMOS 器件组成 3T2M 混合结构, 实现非易失随机存储. Duan 等^[9~12]用忆阻器构成随机阻变存储器, 用于信息的存储及图像处理. Luo 等^[13]对忆阻器不同的串并联结构进行了分析. Dong 等^[14, 15]提出了一种忆阻器 -CMOS 混合逻辑电路, 实现 AND, OR, NAND 逻辑, 该电路不用对忆阻器进行初始化, 大幅减少了电路时延. Zhang 等^[16, 17]研究人员用忆阻器构成基础逻辑门电路, 并基于此构建 4M1M 存储单元, 用于信息存储. Lehtonen 等^[18]和 Broghetti 等^[19]提出忆阻蕴含逻辑 (IMPLY), 真正实现了忆阻器存储计算相融合, 并且使用蕴含逻辑实现 16 种完备布尔逻辑. Kvatinsky 等^[20]改进蕴含逻辑, 减少了忆阻器个数及操作步骤. Kvatinsky 等^[21]提出 memristor ratioed logic (MRL), 并基于其逻辑电路实现半加及全加电路. Guckert 等^[22]将电阻与忆阻器结合, 提出了忆阻驱动门 (MAD Gates) 逻辑电路, 实现了半加器以及全加器. Teimoory 等^[23~26]基于 MRL 逻辑将忆阻器与 CMOS 器件结合, 构建 Hybrid-CMOS 逻辑电路.

然而, 现有的大多数的忆阻逻辑电路都有其自身的局限性. 如 memristor-as-drivers gates (MAD Gates), 在电路设计时会受到开关阈值电压的约束; 且由于其电路本身结构, 导致逻辑响应会有两步的时延, 大大增加电路响应时间. IMPLY 逻辑电路实现逻辑功能需要多步操作, 增大了电路时延; 其输入输出均为忆阻器阻值, 级联特性一般.

以上基于忆阻器构建的逻辑电路有其相应的局限性, 本文主要贡献如下:

(1) 提出了一种新的逻辑电路, 称之为多逻辑融合通用电路 (以下称通用逻辑电路). 该电路能够在同一电路中同时实现 OR-AND-XOR-XNOR 4 种逻辑, 同时所需元件进一步减少, 电路中忆阻器数量减少 70% 以上, 电路功耗进一步降低.

(2) 简化了全加电路逻辑表达式, 基于通用逻辑电路设计了一种新的全加电路. 与现有忆阻器全加电路相比, 忆阻器数量减少 50% 以上, 进一步提高了硬件可实现性.

(3) 基于提出的通用逻辑电路设计了二值图像加密电路, 该加密电路能够在同一电路中可选择不同的加密方式对二值图像进行加密, 且密钥和加密电路是相互独立的, 进一步提高了加密结果的可靠性. 与软件加密算法相比, 极大地减少了耗时.

2 忆阻器模型

HP 忆阻器是由夹在两个铂片电极之间的两层 TiO_2 组成. 其中一层缺失部分氧原子, 称为掺杂层, 另一层为纯 TiO_2 , 称为未掺杂层. 电流流过时, 氧空位区移动, 掺杂层与未掺杂层改变, 导致忆阻器阻值改变; 忆阻器是一种有极性的器件, 对 HP 忆阻器, 当其负极接高电平时, 忆阻值减小. 负极接低电平, 忆阻值增大.

忆阻器两端的电压与电流满足欧姆定律. 定义 R_{OFF} 和 R_{ON} 是忆阻器阻值的极限值; $\omega(t)$ 是掺杂区厚度的变化率, D 为薄膜厚度, 则非掺杂区厚度为 $D-\omega(t)$, μ_V 为掺杂区掺杂物的平均迁移率. 则 HP 忆阻器阻值 $R(t)$ 可以定义为

$$v(t) = R(t)i(t), \quad (1)$$

$$R(t) = R_{\text{OFF}} + (R_{\text{OFF}} - R_{\text{ON}}) \frac{\omega(t)}{D}, \quad (2)$$

$$\frac{d\omega(t)}{dt} = (R_{\text{ON}} \times \mu_V) \frac{i(t)}{D}. \quad (3)$$

HP 忆阻器其模型经典, 结构简单, 二值特性明显, 广泛用于逻辑电路. 文献 [15, 16] 采用 HP 忆阻器模型实现 AND, OR, NOT 逻辑门电路, 本文在电路设计时同样选取该模型.

图 1 本文提出的通用逻辑电路
Figure 1 Proposed general logic circuits

3 通用逻辑电路设计

根据 MRL 逻辑的 AND 和 OR 逻辑门电路, 本文设计了一种新的忆阻器 -CMOS 逻辑电路, 该电路能够在同一电路中同时实现 AND, OR, XOR, XNOR 逻辑, 而只需要 4 个忆阻器和 4 个 MOSFET.

本文提出的通用逻辑电路如图 1 所示, a 和 b 分别为电路的两个输入. M_1, M_2, M_3, M_4 为器件参数一致的相同忆阻器. M_1 和 M_2 实现 OR 逻辑. M_3 和 M_4 实现 AND 逻辑. X_1, X_2, X_3 和 X_4 为 4 个输出节点. I_1 和 I_2 为 CMOS 反相器, I_1 的输入为 AND 逻辑的输出, I_1 的上端接 OR 逻辑的输出, I_1 的下端接低电平, 输出为 XOR 逻辑. I_2 的输入为 OR 逻辑的输出, I_2 的下端接 AND 逻辑的输出, I_2 的上端接高电平, 输出为 XNOR 逻辑.

3.1 电路实现

本文提出的通用逻辑电路中输入分为 4 种情况, 对应能够得到 AND-OR-XOR-XNOR 逻辑门输出电压, 其中 AND 和 OR 逻辑实现与 MRL 逻辑同理. XOR 和 XNOR 逻辑输出结果如表 1 所示.

由表 1 中可知, XOR 和 XNOR 输入输出有以下 4 种情况:

(1) 输入 $V_a = 0, V_b = 0$ 时, OR 逻辑的输出节点 X_1 电压为低电平, AND 逻辑的输出节点 X_2 为低电平. 反相器 I_1 和 I_2 的上端导通, 可以得到 XOR 逻辑的输出节点 X_3 电压为低电平, 即逻辑“0”; XNOR 逻辑的输出节点 X_4 电压为高电平, 即逻辑“1”.

(2) 输入 $V_a = 0, V_b = 1$ 时, OR 逻辑的输出节点 X_1 电压为高电平, AND 逻辑的输出节点 X_2 电压为低电平. 反相器 I_1 的上端导通, I_2 下端导通, 可得 XOR 逻辑输出节点 X_3 为高电平, 即逻辑“1”; XNOR 逻辑输出节点 X_4 为低电平, 即逻辑“0”.

(3) 输入 $V_a = 1, V_b = 0$ 时, 与情况 (2) 相同, 可得 XOR 逻辑输出节点 X_3 为高电平, 即逻辑“1”; XNOR 逻辑输出节点 X_4 为低电平, 即逻辑“0”.

(4) 输入 $V_a = 1, V_b = 1$ 时, OR 逻辑输出节点 X_1 电压为高电平, AND 逻辑输出节点 X_2 为高电平. 反相器 I_1 下端导通, I_2 下端导通. 可得 XOR 逻辑输出节点 X_3 为低电平, 即逻辑“0”; XNOR 逻辑输出节点 X_4 为高电平, 即逻辑“1”.

以上 4 种情况与表 1 中输入输出一一对应, 在同一电路中同时实现 AND-OR-XOR-XNOR 4 种

表 1 通用逻辑电路实现过程
Table 1 Implementation process of proposed general logic circuit

Logic	Truth table	Input		Node voltage	Output
		<i>a</i>	<i>b</i>		
AND	0 0→0	V_L	V_L	$X_1 \rightarrow V_L, X_2 \rightarrow V_L, X_3 \rightarrow V_L, X_4 \rightarrow V_H$	$V_L \rightarrow \text{Logic "0"}$
	0 1→0	V_L	V_H	$X_1 \rightarrow V_H, X_2 \rightarrow V_L, X_3 \rightarrow V_H, X_4 \rightarrow V_L$	$V_L \rightarrow \text{Logic "0"}$
	1 0→0	V_H	V_L	$X_1 \rightarrow V_H, X_2 \rightarrow V_L, X_3 \rightarrow V_H, X_4 \rightarrow V_L$	$V_L \rightarrow \text{Logic "0"}$
	1 1→1	V_H	V_H	$X_1 \rightarrow V_H, X_2 \rightarrow V_H, X_3 \rightarrow V_L, X_4 \rightarrow V_H$	$V_H \rightarrow \text{Logic "1"}$
OR	0 0→0	V_L	V_L	$X_1 \rightarrow V_L, X_2 \rightarrow V_L, X_3 \rightarrow V_L, X_4 \rightarrow V_H$	$V_L \rightarrow \text{Logic "0"}$
	0 1→1	V_L	V_H	$X_1 \rightarrow V_H, X_2 \rightarrow V_L, X_3 \rightarrow V_H, X_4 \rightarrow V_L$	$V_H \rightarrow \text{Logic "1"}$
	1 0→1	V_H	V_L	$X_1 \rightarrow V_H, X_2 \rightarrow V_L, X_3 \rightarrow V_H, X_4 \rightarrow V_L$	$V_H \rightarrow \text{Logic "1"}$
	1 1→1	V_H	V_H	$X_1 \rightarrow V_H, X_2 \rightarrow V_H, X_3 \rightarrow V_L, X_4 \rightarrow V_H$	$V_H \rightarrow \text{Logic "1"}$
XOR	0 0→0	V_L	V_L	$X_1 \rightarrow V_L, X_2 \rightarrow V_L, X_3 \rightarrow V_L, X_4 \rightarrow V_H$	$V_L \rightarrow \text{Logic "0"}$
	0 1→1	V_L	V_H	$X_1 \rightarrow V_H, X_2 \rightarrow V_L, X_3 \rightarrow V_H, X_4 \rightarrow V_L$	$V_H \rightarrow \text{Logic "1"}$
	1 0→1	V_H	V_L	$X_1 \rightarrow V_H, X_2 \rightarrow V_L, X_3 \rightarrow V_H, X_4 \rightarrow V_L$	$V_H \rightarrow \text{Logic "1"}$
	1 1→0	V_H	V_H	$X_1 \rightarrow V_H, X_2 \rightarrow V_H, X_3 \rightarrow V_L, X_4 \rightarrow V_H$	$V_L \rightarrow \text{Logic "0"}$
XNOR	0 0→1	V_L	V_L	$X_1 \rightarrow V_L, X_2 \rightarrow V_L, X_3 \rightarrow V_L, X_4 \rightarrow V_H$	$V_H \rightarrow \text{Logic "1"}$
	0 1→0	V_L	V_H	$X_1 \rightarrow V_H, X_2 \rightarrow V_L, X_3 \rightarrow V_H, X_4 \rightarrow V_L$	$V_L \rightarrow \text{Logic "0"}$
	1 0→0	V_H	V_L	$X_1 \rightarrow V_H, X_2 \rightarrow V_L, X_3 \rightarrow V_H, X_4 \rightarrow V_L$	$V_L \rightarrow \text{Logic "0"}$
	1 1→1	V_H	V_H	$X_1 \rightarrow V_H, X_2 \rightarrow V_H, X_3 \rightarrow V_L, X_4 \rightarrow V_H$	$V_H \rightarrow \text{Logic "1"}$

逻辑. 通过 SPICE 搭建仿真电路, 分别选用 PWRMOS 模型库中型号为 M2N6782 场效应管, 其导通电压为 0~1 V, 型号为 M2N6851 场效应管, 其导通电压为 3.5~5 V, 构建 CMOS 反相器. 设定忆阻器参数 $R_{\text{OFF}} = 20 \text{ K}$, $R_{\text{ON}} = 100$, $D = 10 \text{ n}$, $\mu_V = 10 \text{ f}$, 令 0~0.5 V 为低电平, 4~5 V 为高电平.

通用逻辑电路仿真结果如图 2 所示. 当 $V_a = V_L = "0"$, $V_b = V_L = "0"$ 时, 结果如图 2(a) 所示, 电路在 $t = 3 \mu\text{s}$ 时达到稳定, $V_{\text{OR}} = 0.5 \text{ V} = V_L$, $V_{\text{AND}} = 0.2 \text{ V} = V_L$, $V_{\text{XOR}} = 0.5 \text{ V} = V_L$, $V_{\text{XNOR}} = 4.5 \text{ V} = V_H$; 当 $V_a = V_L = "0"$, $V_b = V_H = "1"$ 时, 结果如图 2(b) 所示, $V_{\text{OR}} = 4.5 \text{ V} = V_H$, $V_{\text{AND}} = 0.5 \text{ V} = V_L$, $V_{\text{XOR}} = 4.5 \text{ V} = V_H$, $V_{\text{XNOR}} = 0.5 \text{ V} = V_L$; 当 $V_a = V_H = "1"$, $V_b = V_L = "0"$ 时, 结果如图 2(c) 所示, $V_{\text{OR}} = 4.5 \text{ V} = V_H$, $V_{\text{AND}} = 0.5 \text{ V} = V_L$, $V_{\text{XOR}} = 4.5 \text{ V} = V_H$, $V_{\text{XNOR}} = 0.5 \text{ V} = V_L$; 当 $V_a = V_H = "1"$, $V_b = V_H = "1"$ 时, 结果如图 2(b) 所示, $V_{\text{OR}} = 4.8 \text{ V} = V_H$, $V_{\text{AND}} = 4.6 \text{ V} = V_H$, $V_{\text{XOR}} = 0.5 \text{ V} = V_L$, $V_{\text{XNOR}} = 4.5 \text{ V} = V_H$; 整个电路输入输出与表 1 中真值表一致, 验证了本文提出的通用逻辑电路的有效性.

3.2 与其他逻辑电路对比

根据电路仿真结果可知, 本文提出的通用逻辑电路能够在同一电路同时实现 4 种不同的逻辑. 与文献 [19~22] 中逻辑电路相比较, 极大地减少了所需元器件, 电路功耗进一步降低, 且性能更优. 为提高不同逻辑电路实验结果的可对比性, 文中电路及数值仿真均使用 HP 忆阻器模型 [4]. 结果如表 2 所示.

根据表 2 对比可知, 同时实现 AND-OR-XOR-XNOR 4 种逻辑功能, 本文提出的通用逻辑电路只需要 4 个忆阻器及 4 个 MOSFET, 与 MAD Gates 逻辑电路相比, 忆阻器数量减少 69.2%, 功耗降低 63.1%; 与 MRL 逻辑电路相比, 忆阻器数量减少 75%, MOSFET 数量减少 60%, 功耗降低 74.8%; 与

图 2 (网络版彩图) 通用逻辑电路仿真结果

Figure 2 (Color online) The simulation result of proposed general logic circuit. (a) $V_a = V_L = "0"$, $V_b = V_L = "0"$; (b) $V_a = V_L = "0"$, $V_b = V_H = "1"$; (c) $V_a = V_H = "1"$, $V_b = V_L = "0"$; (d) $V_a = V_H = "1"$, $V_b = V_H = "1"$

表 2 实现 AND-OR-XOR-XNOR 通用逻辑电路与几种逻辑电路性能对比

Table 2 Several logic circuits' performance for implementation of AND-OR-XOR-XNOR logic

Logic circuits	Components	Generalized	Power estimation	Circuit design constraints	Cascading
Proposed general logic circuit	4 memristors 4 MOSFETs	Excellent	1.592 mW	Low	Excellent
MAD Gates	13 memristors 13 resistors 7 switches	Normal	4.306 mW	High	Normal
MRL	16 memristors 10 MOSFETs	Normal	6.312 mW	Low	Excellent
IMPLY	18 memristors 4 resistors	Normal	12.490 mW	High	Normal
Hybrid CMOS	8 memristors 4 MOSFETs	Good	3.183 mW	Low	Excellent

IMPLY 逻辑电路相比, 忆阻器数量减少 77.8%, 功耗降低 87.2%, MOSFET 数量略有增加; 与 Hybrid CMOS 逻辑电路相比, 忆阻器数量减少 50%, 功耗降低 49.9%. 从电路元件组成来看, 本文提出的通用逻辑电路极大地减少了元件的需求, 电路功耗上具有较大的优势.

表 2 中电路设计约束是指电路对电压是否有幅度限制. MAD Gates^[21] 逻辑电路中阈值开关电压被设定为 0.5 V, 当作用于阈值开关的电压 V_{apply} 满足 $16/220 \text{ V} < V_{\text{apply}} < 16/121 \text{ V}$ 时, 实现 OR 逻辑.

通用性是指逻辑电路能够实现多种功能. MAD Gates, MRL, IMPLY 逻辑电路功能单一, 一种电路结构只能实现一种逻辑功能; Hybrid-CMOS 逻辑电路同一电路中可以实现 3 种逻辑功能. 而本文提出的通用逻辑电路能够在同一电路中同时实现 4 种功能, 在电路功能性上优势明显. MRL, Hybrid-CMOS 及通用逻辑电路的输入输出均为电压信号, 级联特性优异, 而 MAD Gates, IMPLY 逻辑输入输出则为忆阻器阻值, 而忆阻器阻值作为电路输出时不能够直接读取; IMPLY 逻辑忆阻器阻值作为电路输入时, 首先需要将忆阻值进行初始化, 设定成相应的阻值. 由此 MAD Gates, IMPLY 电路级联特性一般.

根据以上对比可知, 本文提出的通用逻辑电路能够用更少的元件, 更低的功耗, 在同一电路中实现更多逻辑功能, 同时具有更为优异的电路通用性及级联特性.

4 基于通用逻辑电路的设计

本节将现有全加逻辑表达式进行简化, 根据图 1 所示的通用逻辑电路, 设计了一种新的全加电路. 其次设计了一种新的二值图像加密电路, 在加密电路中可以选择不同的加密方式, 通过对二值图像像素点进行逻辑运算, 实现图像加密解密.

4.1 全加电路设计

4.1.1 全加电路实现

现有全加电路逻辑表达式为

$$V_{\text{sum}} = V_A \text{ XOR } V_B \text{ XOR } V_{\text{cin}}, \quad (4)$$

$$V_{\text{cout}} = (V_A \text{ AND } V_B) \text{ OR } (V_B \text{ AND } V_{\text{cin}}) \text{ OR } (V_A \text{ AND } V_{\text{cin}}). \quad (5)$$

对加法电路逻辑表达式简化之后, 可得到以下关系式:

当 $V_{\text{cin}} = 0$ (“0”表示低电平, 即 V_L):

$$V_{\text{sum}} = V_A \text{ XOR } V_B, \quad (6)$$

$$V_{\text{cout}} = V_A \text{ AND } V_B; \quad (7)$$

当 $V_{\text{cin}} = 1$ (“1”表示高电平, 即 V_H):

$$V_{\text{sum}} = V_A \text{ XNOR } V_B, \quad (8)$$

$$V_{\text{cout}} = V_A \text{ OR } V_B, \quad (9)$$

其中 V_{cin} 为全加电路中进位信号.

根据简化之后的逻辑式, 设计了一种新的忆阻器 -CMOS 全加电路. 如图 3 所示, A 和 B 为全加电路输入. M_1, M_1, M_3, M_4 为器件参数一致的相同忆阻器. I_1, I_2, I_3, I_4 为 CMOS 反相器, 其中反相器 I_1, I_2, I_3 输入为高电平时, 其下端导通; 输入为低电平时, 其上端导通; 反相器 I_4 反之. I_3 的上端接反相器 I_1 的输出, 下端接 I_2 的输出. I_4 的上端接 M_1, M_1 构成的 OR 逻辑门电路的输出, 下端接 M_3, M_4 构成的 AND 逻辑门电路的输出. 进位信号 V_{cin} 为反相器 I_3, I_4 的输入, 控制其导通. I_3 和 I_4 的输出则分别为全加电路的输出 V_{sum} 和 V_{cout} . 全加电路真值表如表 3 所示.

图 3 忆阻器 -CMOS 全加电路
Figure 3 Proposed memristor-CMOS hybrid full adder

表 3 全加电路真值表
Table 3 The truth table of full adder

Carry voltage	Input		Output
	V_A	V_B	
$V_{cin} \rightarrow V_L$	V_L	V_L	$V_{sum} \rightarrow V_L, V_{cout} \rightarrow V_L$
	V_L	V_H	$V_{sum} \rightarrow V_H, V_{cout} \rightarrow V_L$
	V_H	V_L	$V_{sum} \rightarrow V_H, V_{cout} \rightarrow V_L$
	V_H	V_H	$V_{sum} \rightarrow V_L, V_{cout} \rightarrow V_H$
$V_{cin} \rightarrow V_H$	V_L	V_L	$V_{sum} \rightarrow V_H, V_{cout} \rightarrow V_L$
	V_L	V_H	$V_{sum} \rightarrow V_L, V_{cout} \rightarrow V_H$
	V_H	V_L	$V_{sum} \rightarrow V_L, V_{cout} \rightarrow V_H$
	V_H	V_H	$V_{sum} \rightarrow V_H, V_{cout} \rightarrow V_H$

根据表 3 可知, 当进位信号 $V_{cin} = 0$ 时, 反相器 I_3 的上端导通, I_4 的下端导通, 此时电路响应有以下 4 种情况:

- (1) 输入 $V_A = 0, V_B = 0$ 时, 电路中 OR 和 AND 逻辑门电路输出均为低电平 V_L , 反相器 I_1, I_2 均为上端导通, 则 I_1 的输出为 V_L , I_2 的输出为 V_H , 可以得到 I_3, I_4 输出均为 V_L , 即 $V_{sum} = V_{cout} = V_L$.
- (2) 输入 $V_A = 0, V_B = 1$ 时, OR 逻辑门输出为高电平 V_H , AND 逻辑门电路输出为低电平 V_L , 反相器 I_1 上端导通, 其输出为 V_H ; I_2 下端导通, 其输出为 V_L . 可以得到 $V_{sum} = V_H, V_{cout} = V_L$.
- (3) 输入 $V_A = 1, V_B = 0$ 时, 与情况 (2) 相同, 可得到输出 $V_{sum} = V_H, V_{cout} = V_L$.
- (4) 输入 $V_A = 1, V_B = 1$ 时, OR 和 AND 逻辑门电路的输出均为高电平 V_H , 反相器 I_1, I_2 均为下端导通. 反相器 I_1 的输出为 V_L , I_2 的输出为 V_H . 可以得到 $V_{sum} = V_L, V_{cout} = V_H$.

当进位信号 $V_{cin}=1$ 时, 同理可以得到输出电压与真值表一致.

4.1.2 电路仿真结果及对比

本文使用 HP 忆阻器的 SPICE 模型, 搭建仿真电路. 设定忆阻器参数 $R_{OFF} = 20\text{ K}$, $R_{ON} = 100$, $D = 10\text{ n}$, $\mu_V = 10\text{ f}$, 令 $0\sim 0.5\text{ V}$ 为低电平, $4\sim 5\text{ V}$ 为高电平. 当 $V_{cin} = V_L$ 仿真结果如图 4 所示, 当 $V_{cin} = V_H$ 仿真结果如图 5 所示.

由图 4(a) 可知, 当 $V_A = V_L, V_B = V_L$ 时, 电路中输出电压 $V_{sum} = V_L, V_{cout} = V_L$; 图 4(b) 中, 当 $V_A = V_L, V_B = V_H$ 时, 可得 $V_{sum} = V_H, V_{cout} = V_L$; 图 4(c) 中, 当 $V_A = V_H, V_B = V_L$ 时, 可得

图 4 (网络版彩图) $V_{\text{cin}} = V_L$ 时, 忆阻器 -CMOS 全加电路仿真结果

Figure 4 (Color online) The simulation results of memristor-CMOS hybrid full adder when $V_{\text{cin}} = V_L$. (a) $V_A = V_L$, $V_B = V_L$; (b) $V_A = V_L$, $V_B = V_H$; (c) $V_A = V_H$, $V_B = V_L$; (d) $V_A = V_H$, $V_B = V_H$

表 4 不同逻辑电路实现 N 位全加电路所需元件对比

	MAD Gates	MRL	IMPLY	Proposed general logic circuit
Components	$8N$ memristors	$18N$ memristors	$7N + 1$ memristors	$4N$ memristors
	$2N + 3$ drivers	$3N$ drivers	$7N$ drivers	$2N + 1$ drivers
	$9N$ resistors	$4N$ MOSFETs	N resistors	$8N$ MOSFETs
	$14N$ switches		$8N - 1$ switches	

$V_{\text{sum}} = V_H$, $V_{\text{cout}} = V_L$; 图 4(d) 中, 当 $V_A = V_H$, $V_B = V_H$ 时, 可得 $V_{\text{sum}} = V_L$, $V_{\text{cout}} = V_H$. 仿真结果与真值表一致.

根据图 4 和 5 的仿真结果可知, $V_{\text{cin}} = V_L$, $V_{\text{cin}} = V_H$ 时, 电路仿真结果均与全加电路真值表一致, 本文提出的基于通用逻辑电路的全加电路的有效性得到验证.

对比 MAD Gates, MRL 等逻辑全加电路, 本文基于通用逻辑电路所设计的全加电路所需的元件大幅减少, 比较结果如表 4 所示.

由表 4 的对比可知, 本文提出的基于通用逻辑电路的 N 位全加电路需要 $4N$ 个忆阻器, $3N$ 个电压源, $8N$ 个 MOSFET. 相比于 MAD Gates 逻辑电路, 忆阻器数量减少 50%, 电压源数量也有所减少. 由此发现, 本文提出的电路在元件数量上优势明显.

相对 MRL 逻辑电路, 其 N 位全加电路需要 $18N$ 个忆阻器, $3N$ 个电源以及 $4N$ 个 MOSFET, 而

图 5 (网络版彩图) $V_{\text{cin}} = V_H$ 时, 忆阻器 -CMOS 全加电路仿真结果

Figure 5 (Color online) The simulation results of memristor-CMOS hybrid full adder when $V_{\text{cin}} = V_L$. (a) $V_A = V_L$, $V_B = V_L$; (b) $V_A = V_L$, $V_B = V_H$; (c) $V_A = V_H$, $V_B = V_L$; (d) $V_A = V_H$, $V_B = V_H$

本文提出的 N 位全加电路只需要 $4N$ 个忆阻器, $2N + 1$ 个驱动单元以及 $8N$ 个 MOSFET, 所需忆阻器的个数减少 78%, 是远小于 MRL 电路, 场效应管个数略多于 MRL 电路。

IMPLY 逻辑 N 位全加电路需要 $7N + 1$ 个忆阻器, $7N$ 个电压源, $8N - 1$ 个开关及 N 个电阻。由此可知, 本文提出的全加电路忆阻器数量减少 42.8%, 电压源数量减少 71.4%。更重要的是, IMPLY 逻辑全加电路每进行一次操作都必须先对忆阻器阻值作初始化, 步骤过多, 使得电路效率降低。

4.2 基于通用逻辑的加密电路设计

数字图像在政治、经济、国防、教育等方面均有广泛应用。对于某些特殊领域, 如军事、商业和医疗, 数字图像还有较高的保密要求。为了实现数字图像保密, 实际操作中一般先将二维图像转换成一维数据, 再采用传统加密算法进行加密。根据图 1 所示的通用逻辑电路, 本文提出了一种新的基于逻辑运算的二值图像加密电路。如图 6 所示基于通用逻辑电路的加密单元 (general logic encryption, GLE)。

本文设计的基于通用逻辑的二值图像加密单元如图 6 所示, 电路中有 3 个输入, 其中 V 是原始图像的输入, K 为密钥输入, V_{choose} 为加密方式选择输入, 可以选 XOR 逻辑或 XNOR 逻辑对图像进行加密。 M_1, M_2, M_3, M_4 为器件参数一致的相同忆阻器。 I_1, I_2, I_3 为 3 个反相器, 其中 I_3 的输入为 V_{choose} , 上端接 I_1 (即 XOR 逻辑) 的输入, 下端接 I_2 (即 XNOR 逻辑) 的输出, V_{choose} 控制 I_3 的导通, 可得到输出 O , 即可完成对单个像素点的运算。

根据图 6 所示的加密单元, 构建加密单元阵列, 即可得到一个 $i \times j$ 的加密单元阵列, 即为基于通用逻辑的二值图像加密电路, 如图 7 所示。

图 6 基于通用逻辑电路的加密单元

Figure 6 Proposed encryption cell based general logic circuit

图 7 二值图像加密电路

Figure 7 Proposed encryption circuit for binary image

加密过程. 以数字“5”为例, 进行加密解密. 首先构建一个 5×5 的二值矩阵和一个同样大小的密钥矩阵, 如图 8 所示.

根据原始图像矩阵和密钥矩阵, 在二值图像加密电路中设置输入, 矩阵中“0”对应低电平, “1”对应高电平. 电路 V_{ij} 为原始图像的输入, K_{ij} 为密钥矩阵输入. 再选择不同的加密逻辑, 对原始图像矩阵和密钥矩阵进行相应的逻辑运算即可对图像进行加密. 如图 9 所示, 对数字“5”的原始矩阵和密钥矩阵中每一个对应的元素进行同或逻辑运算, 即可得到加密后图像矩阵. 将加密后图像矩阵中的每一个元素再与密钥矩阵中对应的元素进行同或逻辑运算, 即可得到解密后图像矩阵. 将解密后图像矩阵与原始图像矩阵进行对比, 可知解密后图像矩阵与原始图像矩阵完全一样.

为了进一步验证提出的加密电路的有效性, 本文选用标准的 Lena 512×512 Grayscale (8-bit) 图像对加密解密过程进行验证.

图 8 (网络版彩图) 原始图像矩阵和密钥矩阵, 其中 (a) 为数字 “5” 矩阵, (b) 为密钥矩阵
Figure 8 (Color online) Original image matrix and key matrix. (a) Numeric “5” matrix; (b) key matrix

图 9 (网络版彩图) 加密解密过程
Figure 9 (Color online) Encryption and decryption process

图 10 原始 Lena 图像和密钥
Figure 10 Original Lena image and key

图 11 对 Lena 图像加密解密过程

Figure 11 Encryption and decryption process for Lena image

首先对 Lena 灰度图像采用 OTSU 阈值分割法^[27]进行阈值分割, 得到 Lena 二值原始图像, 随机生成和原始图像同样大小的密钥矩阵, 如图 10 所示. 将原始图像中每一个像素点与密钥中对应的像素点进行异或 (同或) 逻辑运算, 可得到加密图像, 即为加密过程. 再将加密图像与密钥进行异或 (同或) 逻辑运算可得到解密后图像. 经对比, 可知原始图像与解密后得到的图像完全一样. 可以验证本文提出的加密电路能够对二值图像进行加密解密, 且结果与原始图像保持一致, 如图 11 所示.

电路实现相比于软件算法, 在处理高像素图像时, 电路实现在时间消耗上优势明显. 现今图像像素越来越高, 对处理的速度也要求更高, 电路加密的优势也将日益显著.

5 结论

首先, 本文提出了一种通用逻辑电路, 可以在同一电路中同时实现 4 种逻辑运算. 相比 MAD Gates, MRL, IMPLY 逻辑电路功能单一, 本文电路不仅功能性提高, 且对元器件需求减少 70% 或更高. 电路中不含有电阻、开关等大尺寸元器件, 电路功耗进一步降低, 更加利于大规模集成, 可以实现模块化封装, 通过对模块电路进行不同组合, 能够实现更多逻辑功能, 提高了电路的扩展性能. 其次, 基于提出的通用逻辑电路设计了一种新的全加电路, 该全加电路中只由忆阻器和 MOSFET 构成, 相比于 MAD Gates 等全加电路, 忆阻器数量减少 50% 或更高, 在电路尺寸上同样具有极大的优势, 且通过 SPICE 使用仿真对电路的有效性进行了验证. 最后, 本文将提出的通用逻辑电路用于二值图像的加密解密, 通过实验仿真结果可知加密再解密后图像与原图像保持一致, 验证了该方案的可行性与有效性. 该加密电路可以选择不同的逻辑运算进行加密, 且密钥是独立的, 与电路无关, 提高了加密结果的可靠性.

参考文献

- 1 Chua L O. Memristor-the missing circuit element. *IEEE Trans Circuit Theor*, 1971, 18: 507-519
- 2 Strukov D B, Snider G S, Stewart D R, et al. The missing memristor found. *Nature*, 2008, 453: 80-83
- 3 Williams R. How we found the missing memristor. *IEEE Spectr*, 2008, 45: 28-35
- 4 Biolek Z, Biolek D, Biolkova V, et al. SPICE model of memristor with nonlinear dopant drift. *Radioengineering*, 2009, 18: 210-214
- 5 Vourkas I, Batsos A, Sirakoulis G C. SPICE modeling of nonlinear memristive behavior. *Int J Circ Theor Appl*, 2015, 43: 553-565
- 6 Emara A, Ghoneima M, El-Dessouky M. Differential 1T2M memristor memory cell for single/multi-bit RRAM modules. In: *Proceedings of the 6th Computer Science and Electronic Engineering Conference (CEECE)*, Colchester, 2014. 69-72
- 7 Shaarawy N, Ghoneima M, Radwan A G. 2T2M memristor-based memory cell for higher stability RRAM modules. In: *Proceedings of 2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, Lisbon, 2015. 1418-1421

- 8 Sarwar S S, Saqueeb S A N, Quaiyum F, et al. Memristor-based nonvolatile random access memory: hybrid architecture for low power compact memory design. *IEEE Access*, 2013, 1: 29–34
- 9 Duan S K, Hu X F, Wang L D, et al. Memristor-based RRAM with applications. *Sci Sin Inform*, 2012, 42: 754–769 [段书凯, 胡小方, 王丽丹, 等. 忆阻器阻变随机存取存储器及其在信息存储中的应用, *中国科学: 信息科学*, 2012, 42: 754–769]
- 10 Jiang Z, Duan S, Wang L, et al. A threshold adaptive memristor model analysis with application in image storage. In: *Proceedings of International Conference on Information Science and Technology*, 2015. 449–454
- 11 Duan S K, Hu X F, Wang L D, et al. Memristor-based RRAM with applications. *Sci China Inf Sci*, 2012, 55: 1446–1460
- 12 Hu X F, Duan S K, Wang L D. Memristive multilevel memory with applications in audio signal storage. In: *Artificial Intelligence and Computational Intelligence*. Berlin: Springer, 2011. 228–235
- 13 Luo L, Hu X F, Duan S K, et al. Multiple memristor series-parallel connections with use in synaptic circuit design. *IET Circ Dev Syst*, 2017, 11: 123–134
- 14 Dong Z, Qi D, He Y, et al. Easily cascaded memristor-CMOS hybrid circuit for high-efficiency boolean logic implementation. *Int J Bifurcation Chaos*, 2018, 28: 1850149
- 15 Dong Z K, He Y F, Hu X F, et al. A flexible memristor-based logic unit circuit and its network integration for Boolean logic implementation. *IET Nanodielectrics*, 2019. doi: 10.1049/iet-nde.2018.0027
- 16 Zhang Y, Shen Y, Wang X, et al. A novel design for memristor-based logic switch and crossbar circuits. *IEEE Trans Circ Syst I*, 2015, 62: 1402–1411
- 17 Zhang Y, Shen Y, Wang X, et al. A novel design for a memristor-based OR Gate. *IEEE Trans Circ Syst II*, 2015, 62: 781–785
- 18 Lehtonen E, Laiho M. Stateful implication logic with memristors. In: *Proceedings of IEEE/ACM International Symposium on Nanoscale Architectures, Nanoarch*, 2009. 33–36
- 19 Borghetti J, Snider G S, Kuekes P J, et al. ‘Memristive’ switches enable ‘stateful’ logic operations via material implication. *Nature*, 2010, 464: 873–876
- 20 Kvatinsky S, Satat G, Wald N, et al. Memristor-based material implication (IMPLY) logic: design principles and methodologies. *IEEE Trans VLSI Syst*, 2014, 22: 2054–2066
- 21 Kvatinsky S, Wald N, Satat G, et al. MRL - memristor ratioed logic. In: *Proceedings of IEEE International Workshop on Cellular Nanoscale Networks and Their Applications*, 2012. 1–6
- 22 Guckert L, Swartzlander E E. MAD gates-memristor logic design using driver circuitry. *IEEE Trans Circ Syst II*, 2017, 64: 171–175
- 23 Teimoori M, Ahmadi A, Alirezaee S, et al. A novel hybrid CMOS-memristor logic circuit using memristor ratioed logic. In: *Proceedings of IEEE Electrical and Computer Engineering*, 2016
- 24 Teimoori M, Amirsalemani A, Ahmadi A, et al. A hybrid memristor-CMOS multiplier design based on memristive universal logic gates. In: *Proceedings of IEEE International Midwest Symposium on Circuits and Systems*, 2017. 1422–1425
- 25 Xia Q, Robinett W, Cumbie M W, et al. Memristor-CMOS hybrid integrated circuits for reconfigurable logic. *Nano Lett*, 2009, 9: 3640–3645
- 26 Zhou Y, Li Y, Xu L, et al. A hybrid memristor-CMOS XOR gate for nonvolatile logic computation. *Phys Status Solidi A*, 2016, 213: 1050–1054
- 27 Otsu N. A threshold selection method from gray-level histograms. *IEEE Trans Syst Man Cybern*, 1979, 9: 62–66

A memristor-CMOS-based general-logic circuit and its applications

Hui YANG^{1,2}, Shukai DUAN^{1,2*}, Zhekang DONG^{3,4}, Lidan WANG^{1,2}, Xiaofang HU⁵ & Liuting SHANG^{1,2}

1. College of Electronics and Information Engineering, Southwest University, Chongqing 400715, China;

2. Key Laboratory of Nonlinear Circuits and Intelligent Information Processing of Chongqing, Southwest University, Chongqing 400715, China;

3. College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China;

4. Department of Electrical Engineering, The Hong Kong Polytechnic University, Hong Kong 999077, China;

5. School of Computer and Information Science, Southwest University, Chongqing 400715, China

* Corresponding author. E-mail: duansk@swu.edu.cn

Abstract Memristors are a kind of information-storage device with resistance-switching dynamics. Due to the variable conductivity of memristive devices, their composite circuits can be used for implementation of logic operations. In this paper, a novel hybrid CMOS-memristor-based logic circuit is proposed for use in realizing four basic logic operations (AND, OR, XOR, XNOR) simultaneously within the same circuit. Compared with existing logic implementations (MAD Gates, MRL, IMPLY), the present circuit offers better performance and greater efficiency, owing to the significant reduction in the number of memristors used in the circuit and the power consumption. Thus, a new full-adder circuit and a binary-image-encryption circuit are designed. Unlike previous full-adder circuits, the proposed one has great advantages in terms of the number of circuit elements. In the proposed encryption circuit, there are two available encryption methods and the encryption key is independent of the circuit, which can improve the reliability of encryption results.

Keywords memristor, logic operations, memristor-CMOS hybrid logic, full-adder, binary image encryption

Hui YANG was born in 1994. He received his B.S. degree in electronic and information engineering from Chang'an University, China, in 2016. Currently, he is a graduate student at the College of Electronics and Information Engineering, Southwest University, Chongqing, China. His research interests cover memristors and memristive logical circuits.

Shukai DUAN was born in 1973. He received his Ph.D. in computer-application technology from Chongqing University, China, in 2006. He is a professor with the School of Electronics and Information Engineering, Southwest University, Chongqing. Currently, his research interests cover intelligent information processing, artificial neural networks, chaos, nonlinear circuit theory and applications, memristors and

memristive system.

Zhekang DONG was born in 1990. He received B.E. and M.E. degrees in electronics and information engineering in 2012 and 2015, respectively, from Southwest University, Chongqing, China. Currently, he is a Ph.D. candidate at the College of Electrical Engineering, Zhejiang University, Hangzhou, China. His research interests cover memristor-based circuits and systems, memristor-based logic, neuromorphic-computing systems, and intelligent signals.

Lidan WANG was born in 1976. She received her Ph.D. in computer software and theory from Chongqing University, China, in 2008. Currently, she is a professor with the School of Electronics and Information Engineering, Southwest University, Chongqing. Her research interests include the nonlinear system and chaotic circuits, artificial neural networks and FPGA technology, memristors, and memristive systems.

memristors, and memristive systems.