

基于忆阻器的 SIMON 轮函数电路设计

陈鑫辉, 张会红, 张跃军*

(宁波大学 电路与系统研究所, 浙江 宁波 315211)

摘要: 忆阻器由磁通量、电荷、电压、电流之间关系对称性推导得出, 被认为是继电阻、电容、电感之后的第四大无源元件, 具有记忆功能和非易失性等特点. 通过对忆阻器工作原理和电路模型的研究, 提出了基于忆阻器的 SIMON 轮函数电路设计方案. 该方案首先分析忆阻器模型结构和 SIMON 算法, 设计基于忆阻器的与、或、非门电路; 并在此基础上实现基于忆阻器的 SIMON 轮函数电路, 利用忆阻器的非易失性特性实现断点记忆功能; 最后在 Cadence Virtuoso 环境下, 仿真验证所设计电路的断电保存功能. 与传统 CMOS 电路比较, 基于忆阻器的 SIMON 轮函数电路减少了 27.8% 的元器件数量, 低功耗特性明显.

关键词: 忆阻器; SIMON 轮函数; 断点记忆; 逻辑门电路

中图分类号: TP331

文献标志码: A

文章编号: 1001-5132 (2018) 06-0001-06

忆阻器由蔡少棠教授于 1971 年提出, 是一种具有记忆功能的非易失性电阻^[1]. 目前国内对忆阻器的探索处于起步阶段, 鉴于忆阻材料种类繁多, 相关理论缺少电路验证, 电学性质未被系统概括, 所提出的忆阻模型忆阻效果一般, 无法实现商业化. 因此探索忆阻器模型结构, 并设计出具有应用价值的忆阻器电路已成为当前研究热点^[2-3], 尤其是在 2008 年惠普实验室提出 MIM(Metal Insulator Metal)结构的模型^[4], 引起学术界的广泛关注.

惠普实验室提出用 2 块金属铂电极夹住极薄二氧化钛的忆阻器模型^[5]. 该模型中二氧化钛由 2 个区域组成, 一个区域是正常的二氧化钛, 称为非掺杂区(可等效为高电阻); 另一区域是少氧原子的二氧化钛, 称为掺杂区(可等效为低电阻). 当电流从“掺杂区”流向“非掺杂区”时, 在电场作用下, “掺杂区”会逐步向“非掺杂区”移动, 致使掺杂区部分占二氧化钛比重增加, 阻值也随之降低. 当电流从“非掺杂区”流向“掺杂区”时, 在电场作用下少氧掺杂物往“掺杂区”移动, 致使阻值增加, 忆阻值呈非线性变化. 忆阻器的记忆效应表现为

能“记住”流经的电荷量的改变, 并以忆阻值的改变来反映. 忆阻值定义为电流或电压关于时间的导数, 具有非易失性, 且忆阻值随施加于忆阻器的电压或电流而变动, 且这种变化是持续的.

近年来, 密码算法有着良好的发展, 从 AES (Advanced Encryption Standard)^[6]、RSA(Rivest Shamir Adleman)、RC4(Rivest Cipher 4)^[7]到 SIMON 算法^[8], 在加密电路领域有着广泛的应用. 但基于传统 CMOS(Complementary Metal Oxide Semiconductor)设计的密码电路在运行时, 忽然断电会导致数据丢失. 鉴此, 本文将忆阻器与传统 CMOS 电路融合, 利用忆阻器的记忆功能和非易失性特征设计基于忆阻器的断点记忆 SIMON 轮函数电路, 并在 Cadence Virtuoso 环境完成仿真验证.

1 忆阻器模型与单元门电路

1.1 忆阻器模型分析

忆阻器分磁控型^[9]和荷控型^[10], 图 1(a)为忆阻器模型. 荷控型忆阻器由金属铂和二氧化钛构成, 二氧化钛分为掺杂区和非掺杂区, 掺杂区等效为

收稿日期: 2018-02-01.

宁波大学学报(理工版) 网址: <http://journalg.nbu.edu.cn/>

基金项目: 浙江省自然科学基金 (LY18F040002); 国家自然科学基金 (61871244, 61874078); 浙江省公益项目 (2016C31078); 横向项目 (HK2017000135); 宁波大学研究生科研创新基金.

第一作者: 陈鑫辉 (1995-), 男, 浙江温州人, 在读硕士研究生, 主要研究方向: 忆阻器电路研究设计. E-mail: 465998670@qq.com

*通信作者: 张跃军 (1982-), 男, 浙江宁波人, 博士/副教授, 主要研究方向: 集成电路抗老化设计等. E-mail: zhangyuejun@nbu.edu.cn

电阻 R_{on} , 非掺杂区等效为电阻 R_{off} . p 和 n 分别表示输入和输出端口, w_{pos} 表示掺杂区位置. 当有效电阻为 R_{on} 时, 忆阻器为短路; 有效电阻为 R_{off} 时, 忆阻器为开路. 图 1(b)为等效模型, 图 1(c)为忆阻器元件符号.

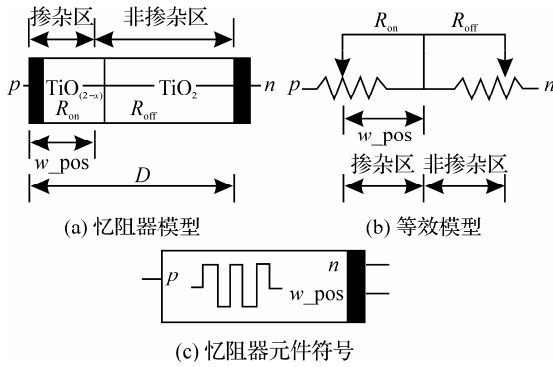


图 1 忆阻器模型和元件符号

忆阻器在电流作用下, 通过离子漂移方式改变掺杂区长度, 从而改变忆阻值, 其电流和电压的关系可用式(1)表示^[11]:

$$v(t) = \left[R_{on} \frac{w(t)}{D} + R_{off} \left(1 - \frac{w(t)}{D} \right) \right] i(t), \quad (1)$$

$$\frac{dw(t)}{dt} = \mu_v \frac{R_{on}}{D} i(t), \quad (2)$$

其中, $w(t)$ 为掺杂区长度随时间的变化函数; μ_v 为器件内部离子漂移速率; D 为忆阻器的总长度. 对式(2)两边积分可得:

$$w(t) = w_0 + \mu_v \frac{R_{on}}{D} \int_0^t i(t) dt = w_0 + \mu_v \frac{R_{on}}{D} q(t), \quad (3)$$

其中, w_0 表示掺杂区初始长度; $q(t)$ 为电荷量关于时间的函数. 将式(3)代入式(1)可得:

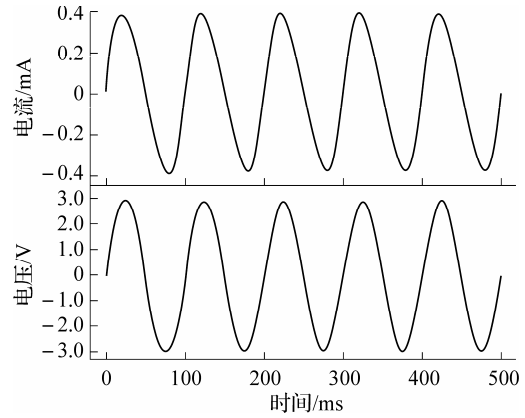
$$M(t) = R_{off} \left[1 + \frac{w_0}{D} \left(\frac{R_{on}}{R_{off}} - 1 \right) - \frac{\mu_v R_{on}}{D^2} \left(1 - \frac{R_{on}}{R_{off}} \right) q(t) \right]. \quad (4)$$

因为 $R_{on} \ll R_{off}$, $R_{on} / R_{off} \approx 0$, 且设 $w_0 = 0$, 故式(4)可化简为:

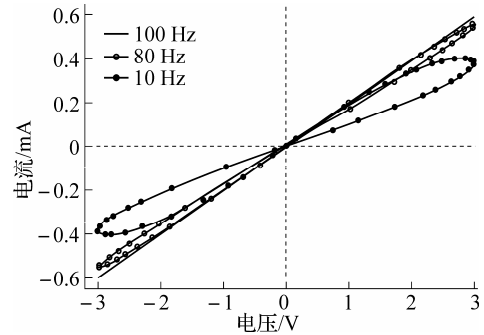
$$M(t) = R_{off} \left(1 - \frac{\mu_v R_{on}}{D^2} q(t) \right). \quad (5)$$

将模型参数设为 $R_{on} = 100 \Omega$, $R_{off} = 20 \text{ k}\Omega$, $D = 3 \text{ nm}$, $\mu_v = 10^{-15} \text{ m}^2 \cdot (\text{s} \cdot \text{V})^{-1}$. 图 2(a)为 $w \in [0, D]$, $M \in [R_{on}, R_{off}]$ 时, 在 Cadence Virtuoso 环境下仿真忆阻器的电流—电压关系曲线. 根据图 2(a)数据拟

合出忆阻器的伏安特性曲线, 得到图形如图 2(b)所示. 在 10, 80, 100 Hz 工作频率下, 伏安特性曲线均关于原点对称, 呈倒 ‘8’ 字形回滞曲线.



(a) 10 Hz 下输出电流和电压

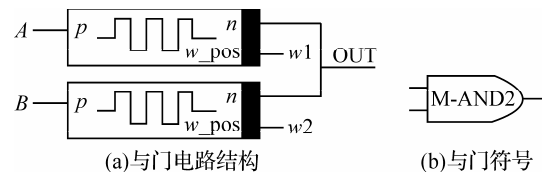


(b) 多个频率下 $I-V$ 特性曲线

图 2 忆阻器 $I-V$ 曲线绘制

1.2 基于忆阻器的基本逻辑门设计

采用忆阻器设计逻辑与门和或门^[12]. 如图 3(a)所示, 当输入端 A 和 B 电压相同时, 忆阻器 $M1$ 和 $M2$ 上电流抵消, 此时输出端 OUT 电压等于输入电压; 当输入端 A 和 B 电压不同时, 忆阻器 $M1$ 和 $M2$ 有电流流经, 电路输入端 A 和 B 中较低电平端口可视作接地, 两者中高电平端口使忆阻值增加. 与门由 2 个忆阻器采用 $n-n$ 端相连方式组成. 与门输出端为 2 个忆阻器的连接端口, 输出端口电压值为 2 个忆阻器输入端 A 和 B 分压的结果. 图 3(b)为与门符号, 图 3(c)为与门仿真波形. 其中 U_1 为忆阻器与门波形, U_2 为忆阻器和 CMOS 与门波形.



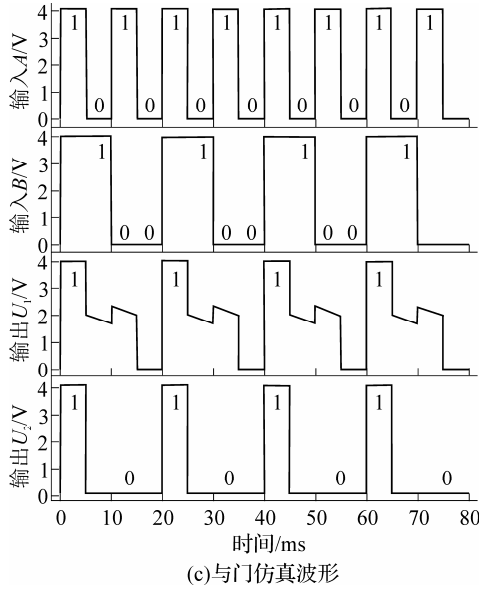


图 3 忆阻器与门电路图及仿真波形

如图 4(a)所示, 或门由 2 个忆阻器采用 $p-p$ 端相连方式构成. 当输入端 A 和 B 电压相同时, 忆阻器 $M1$ 和 $M2$ 上电流抵消, 此时输出端 OUT 电压等于输入电压; 当输入端 A 和 B 电压不同时, 忆阻器 $M1$ 和 $M2$ 有电流流经, 电路输入端 A 和 B 中较低电平端口可视为接地, 两者中高电平端口使忆

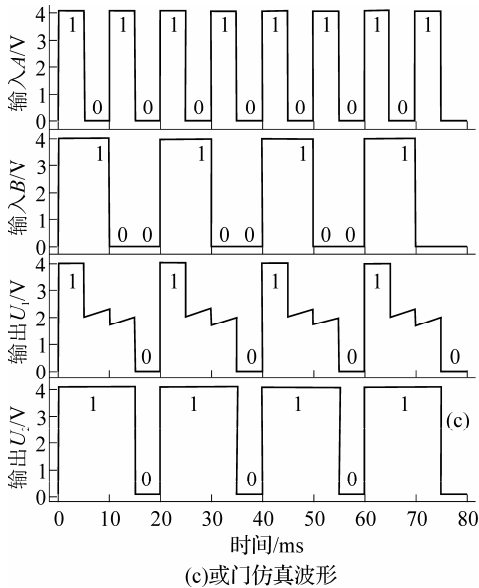
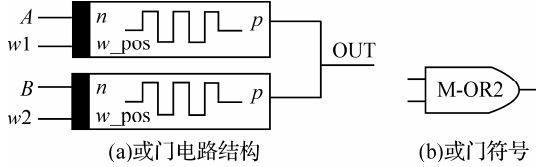


图 4 忆阻器或门电路图及仿真波形

阻值减小. 或门输出端为 2 个忆阻器的连接端口, 输出端口的电压值为 2 个忆阻器输入端 A 和 B 分压的结果. 图 4(b)为或门符号, 图 4(c)为或门仿真波形. 其中, U_1 为忆阻器或门波形, U_2 为忆阻器和 CMOS 或门波形.

2 忆阻器的 SIMON 轮函数电路设计

轻量级 SIMON 密码算法于 2013 年由 Beaulieu 等提出^[13], 属于高度优化的分组轻量密码系列, 可以在硬件和软件环境中提供优异的性能. 文献[13]表明, 每个 SIMON 算法都优于主流硬件算法(在相同吞吐量下的面积开销)和主流软件算法(代码复杂度和内存开销). SIMON 算法整体框图如图 5 所示.

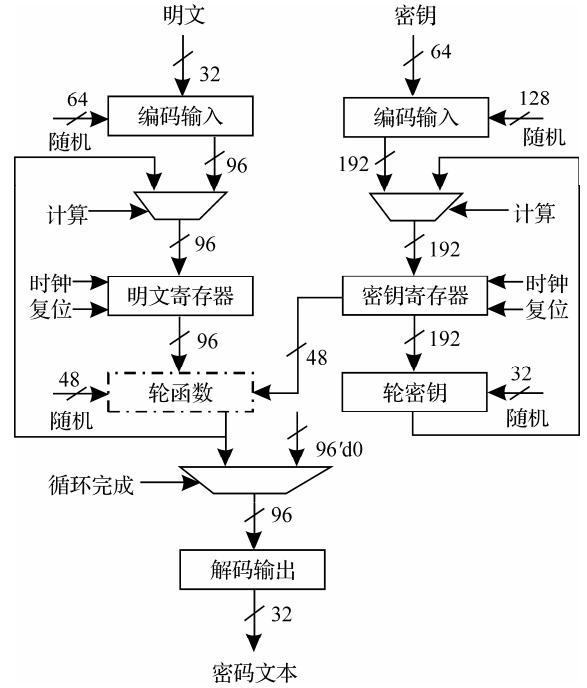


图 5 SIMON 算法结构框

SIMON 算法由轮函数(循环函数)和轮密钥组成, 可通过移位运算、与运算和异或运算来实现. 图 5 中点划线虚框为本文设计的轮函数, 定义见式(6)~(8). 式中, M_{RW} 和 M_{LW} 分别代表明文的低位部分和高位部分, i 为循环轮数, K_m 为第 m 位密钥, S^j 为左移 j 位操作. 式(6)~(8)对应轮函数的实现方式如图 6 所示.

$$M_{RW}^i = M_{LW}^{i-1}, \quad (6)$$

$$M_{LW}^i = M_{RW}^{i-1} \oplus F(M_{LW}^{i-1}) \oplus K^{i-1}, \quad (7)$$

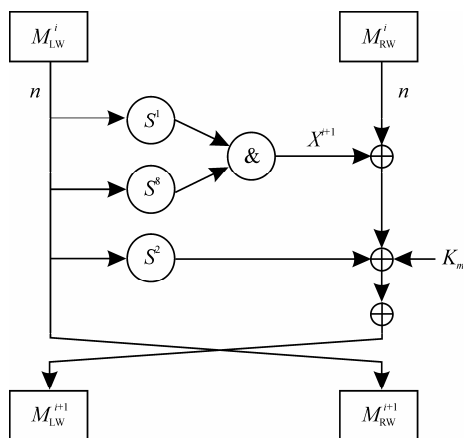


图6 轮函数算法

$$F(X) = ((X \ll 1) \& (X \ll 8)) \oplus (X \ll 2), \quad (8)$$

在与、或、非3种基本逻辑门基础上,设计与非门、或非门和异或电路门等,再实现SIMON轮函数电路所需与门链和异或门链。以与门链为例,64位输入,需32个与门构成与门链。图7是根据SIMON算法轮函数式(6)~(8)设计的最终电路结构图。

3 实验结果与分析

实验的仿真验证环境包括服务器型号 Intel

Xeon(R) Dual-Core CPU 2.0GHZ、6G RAM、Cadence Virtuoso IC617 以及 Israel Institute of Technology 的忆阻器模型。

表1中 j 为与门器件的序列号(采用随机算法抽取8组), A_j, B_j 为第 j 个与门的输入(采用随机算法抽取8组状态), $R_{out,1}, R_{out,2}$ 分别为前两轮异或加密的结果, R_{out} 为一轮轮函数最后的加密结果。在Cadence Virtuoso 环境下,仿真验证基于忆阻器的SIMON轮函数电路。

表1 SIMON 轮函数的部分输出真值表

j	A_j	B_j	$R_{out,1}$	$R_{out,2}$	R_{out}
2	1	0	1	0	1
4	1	0	1	1	0
9	0	1	0	1	1
16	1	1	0	1	0
20	0	0	0	0	0
25	1	0	1	0	1
27	0	1	1	1	1
31	0	0	0	0	0

表1真值表和图8的功能仿真波形表明,所设计的SIMON轮函数电路具有正确的逻辑功能。

图9(a)表示MOS管开启和断开时的电流输出

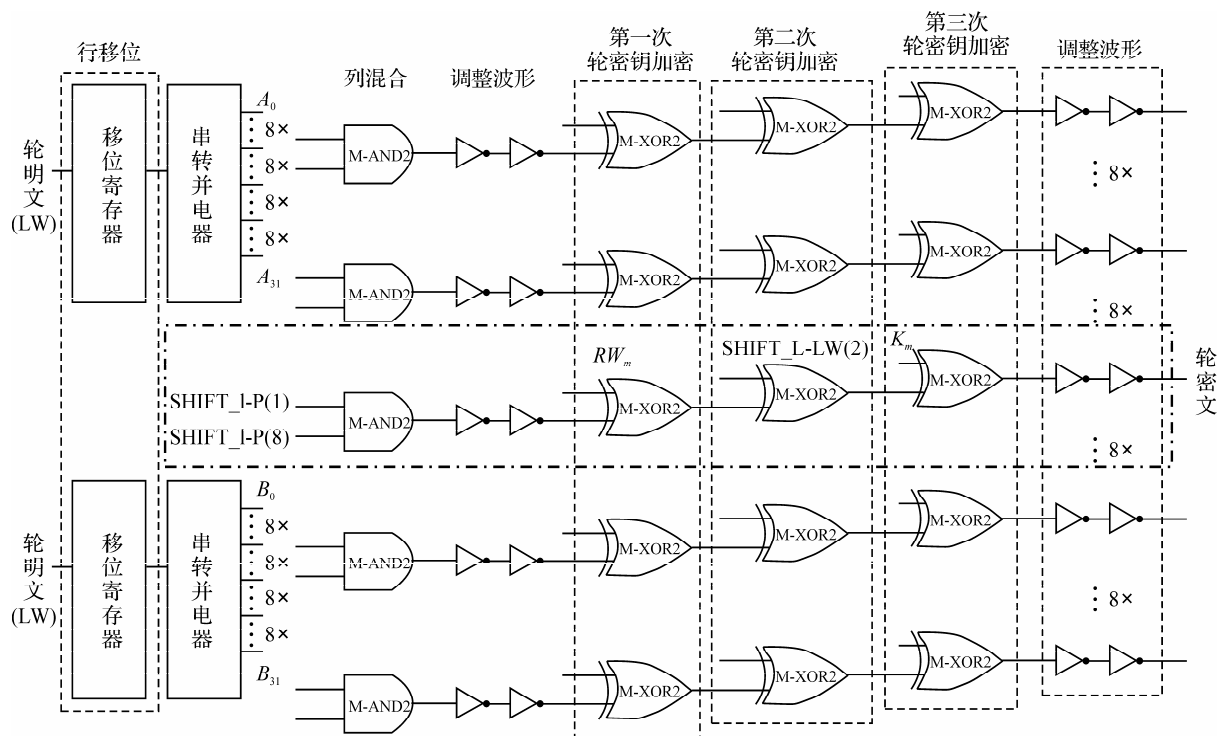
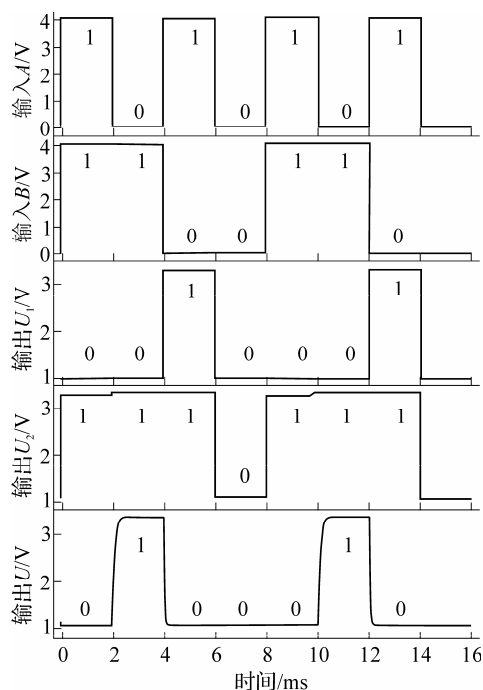
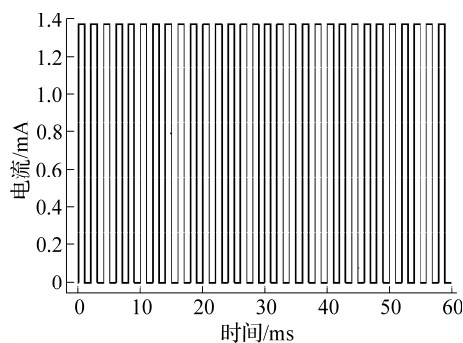
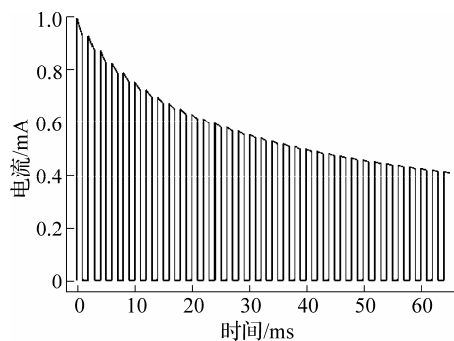


图7 SIMON 算法轮函数电路图

图8 j 取4时的SIMON轮函数功能仿真波形

(a) MOS管的开关特性



(b) 忆阻器电路的非易失性

图9 忆阻器电路与传统CMOS电路非易失性比较

波形,图9(b)表示忆阻器开启和断开时的电流波形,可看到输入为低电平时,忆阻值保持不变;仅在下个脉冲到来时,忆阻值才改变,当电压持续一定时间后,忆阻值达到最值并保持不变.MOS管不具备

非易失性,当输入高电平时,MOS管导通;当输入低电平时,MOS管关断.由忆阻器搭建的电路,在断电后恢复施加电流(电压),会继续在原来忆阻值的基础上工作,而MOS管则需重新从初始状态开始运行.此外,本文所设计的忆阻电路还有以下优点,可以间断性地断电存储信息,进一步降低静态功耗.

随着MOS管尺寸缩小,量子效应、互联寄生效应等将突出,当工艺到5nm左右将达到物理极限.而忆阻器由于自身尺寸小以及功耗低等特性,一个忆阻器的数据处理能力等效于十几个晶体管联合作用的能力,且已经研制出堆叠式多层交叉开关的忆阻器矩阵结构,能够实现更高的集成度.同时,非易失性特性与具体电路结合,使电路记忆特性更突出,与传统CMOS电路比较具有明显的优势,减少了27.8%的元器件数量,具体对比分析结果见表2.

表2 对比分析

电路	基于忆阻器的 轮函数电路	基于MOS管的 轮函数电路
记忆功能	有	无
元件数	需要640个忆阻器和 1024个MOS管	需要2304个 MOS管
集成度	更高	趋于极限
非易失性	有	无

4 结论

本文设计了一种基于忆阻器的新型SIMON轮函数电路,主要利用忆阻器的忆阻值记忆所流经电流的特点,具有非易失性和记忆性.在Cadence Virtuoso仿真工具下,对基于忆阻器的SIMON轮函数电路进行的验证分析.实验结果表明所设计的电路具有正确的逻辑功能,与传统CMOS电路比较,减少27.8%的元器件数量,且有记忆特性和高集成度等优势,低功耗特性明显.

参考文献:

- [1] Chua L O. Memristor-the missing circuit element[J]. IEEE Transactions on Circuit Theory, 1971, 18(5):507-519.
- [2] 贾旺旺. 忆阻器件及其应用[D]. 成都: 电子科技大学,

- 2016.
- [3] 李心鹏. 基于两层二氧化钛薄膜的新型元器件电路特性及其应用研究[D]. 银川: 宁夏大学, 2015.
- [4] Strukov D B, Snider G S, Stewart D R, et al. The missing memristor found[J]. *Nature*, 2008, 453:80-83.
- [5] Ntinis V, Ascoli A, Tetzlaff R, et al. Transformation techniques applied to a TaO memristor model to enable stable device simulations[C]. 2017 IEEE European Conference on Circuit Theory and Design (ECCTD), 2017:1-4.
- [6] 陶星辰. 基于 AES 加密的无线音视频传输系统设计及应用[D]. 合肥: 合肥工业大学, 2015.
- [7] 张晓燕, 徐允庆. 基于正交拟群的流密码算法[J]. 宁波大学学报(理工版), 2016, 29(2):89-93.
- [8] Dofe J, Reed C, Zhang N, et al. Fault-tolerant methods for a new lightweight cipher SIMON[C]. IEEE 16th International Symposium on Quality Electronic Design (ISQED), 2015:460-464.
- [9] 刘威, 王光义. TiO_2 忆阻器的磁控模型分析及电路实现[J]. 杭州电子科技大学学报(自然科学版), 2015, 35(2): 5-8.
- [10] 谭志平, 杨红姣, 刘奇能, 等. 最简荷控型忆阻器混沌电路的设计及实现[J]. 计算物理, 2015, 32(4):496-504.
- [11] Olufemi A O, Massimo G. Arduino-controlled HP memristor emulator for memristor circuit applications[J]. *Integration, the VLSI Journal*, 2017, 58:438-445.
- [12] 朱平平, 甘朝晖, 蒋旻. 忆阻器实现逻辑门的方法研究[J]. 微电子学与计算机, 2012, 29(12):12-16; 21.
- [13] Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK families of lightweight block ciphers[C]. 2015 Design Automation Conference, 2015:175-180.

Design of a SIMON round function circuit based on memristor

CHEN Xin-hui, ZHANG Hui-hong, ZHANG Yue-jun*

(Institute of Circuits and Systems, Ningbo University, Ningbo 315211, China)

Abstract: As the fourth fundamental circuit element besides resistance, capacitance and inductance, the memristor is derived using the magnetic flux, charge, voltage, electric current symmetry. It contains the memory function and non-volatile. Based on investigating the operating principle and circuit model of memristor, in this paper a scheme of the SIMON round function circuit is presented utilizing the memristor. In the scheme the structure of memristor and SIMON algorithm are first analyzed, followed by designing the circuit of AND OR NOT logic gate based on the use of memristor. The SIMON round function circuit is designed to achieve the function of break-point memory by taking advantage of the non-volatile characteristic of memristor. Under the condition of TSMC 65 nm, the Cadence Virtuoso simulation result shows that the proposed circuit has the correct logic. Compared to the conventional CMOS circuit, the number of components decreases by about 27.8%, and is characterized with low-power consumption.

Key words: memristor; SIMON round function; break-point memory; logic gate circuit

(责任编辑 章践立)