基于 RRAM 延时单元的 PUF 设计

杨 轩[1],叶文强[2],崔小乐[2]
(1. 北京环境特性研究所,北京 100854; 2. 北京大学深圳研究生院,广东深圳 518055)

摘 要: 随着技术的发展,信息安全受到了很大挑战. 物理不可克隆函数(Physically Unclonable Function,PUF)电路是一种新型的密钥生成电路,阻变存储器(Resistive Random Access Memory,RRAM)可以为其提供物理随机熵源,这使得 PUF 在物理上不可被攻击. 但目前在基于 RRAM 的 PUF 设计方案中,RRAM 延时单元的测试响应对(Challenge Response Pair,CRP)效率并不够高. 本文提出一种基于 RRAM 延时单元的 PUF 结构,延时单元将 RRAM 的阻值输出到反向器中,形成脉冲的延迟,最后通过判决器判断两路脉冲达到顺序并编码为"0"和"1",这就是 PUF 的输出位. 基于 RRAM 延时单元,本文设计了 8 位、16 位、32 位、64 位 PUF,这些 PUF 在保证良好的随机性、稳定性、唯一性的前提下,大大提高了 PUF 的 RRAM 单元效率. 实验结果表明:该设计能够有效的提高 RRAM 使用效率,使得 PUF 能够更好地防止外界的攻击.

关键词: 物理不可克隆函数; 阻变存储器; CRP (Challenge Response Pair) 效率
中图分类号: TN47 **文献标识码:** A **文章编号:** 0372-2112(2020)08-1565-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.08.015

PUF Design Based on RRAM Delay Unit

YANG Xuan[1], YE Wen-qiang[2], CUI Xiao-le[2]
(1. *Beijing Institute of Environmental Features*, *Beijing* 100854, *China*;
2. *Peking University Shenzhen Graduate School*, *Shenzhen*, *Guangdong* 518055, *China*)

Abstract: With the development of technology, information security has been greatly challenged. The Physical Unclonable Function (PUF) circuit is a new type of key generation circuit. Resistive Random Access Memory (RRAM) can provide a source of physical random entropy, which makes the PUF physically impossible be attacked. However, in the RRAM-based PUF design, the RRAM delay unit's test response pair (Challenge Response Pair, CRP) efficiency is not high enough. In this paper, a PUF structure based on RRAM delay unit is proposed. The delay unit outputs the resistance of the RRAM to the inverter to form a delay of the pulse. Finally, the determiner determines that the two pulses are in sequence and is coded as "0" and "1", this is the output bit of the PUF. Based on the RRAM delay unit, this paper designs 8-bit, 16-bit, 32-bit, 64-bit PUF. These PUFs greatly improve the efficiency of PUF RRAM cells under the premise of ensuring good randomness, stability and uniqueness. The experimental results show that the design can effectively improve the efficiency of RRAM, so that PUF can prevent external attacks better.

Key words: physical unclonable function; resistive memory; CRP efficiency

1 引言

传统的软件加密算法通常需要将密钥保存在存储器中,密钥易受存储器读写攻击,攻击者可以通过读写存储器内容获取或破坏密钥,存在信息安全隐患. 因此产生了一种物理加密的方法,即 PUF[1],物理不可克隆函数,这一概念最早由 Pappu[2] 于 2001 年首先提出,并利用光学设计实现了 PUF 的系统认证等应用. PUF 电路利用电路自身的参数波动性来产生密钥,具有良好的随机性、唯一性和可靠性,攻击者无法通过传统方法获取 PUF 所产生的保密信息.

目前,大多数 PUF 电路是利用工艺波动实现的,主流设计方案包括环形振荡器(RO-Ring Oscillator)型 PUF,仲裁器(Arbiter)型 PUF 和存储器型 PUF. 由于 PUF 的构建基于无法控制的制造过程中物理参数的变化,因此 PUF 电路即使在知晓所有电路细节以及工艺环境的情况下,也不可能制作出完全相同的 PUF 电路,

收稿日期:2019-11-21; 修回日期:2020-02-20;责任编辑:马兰英
基金项目:深圳市学科布局项目(No. JCYJ20170412150411676)

因此 PUF 电路可以阻止物理攻击[3].

一个输入激励(Challenge)提交给一个 PUF 电路时,PUF 会产生相应的输出响应(Response). 这个响应是由以上提到的复杂的物理函数实现的,而这个物理函数针对每个设备都是唯一的. 一组 CRP 可以作为 PUF 以及相应的集成电路或设备的指纹(如图 1 所示).

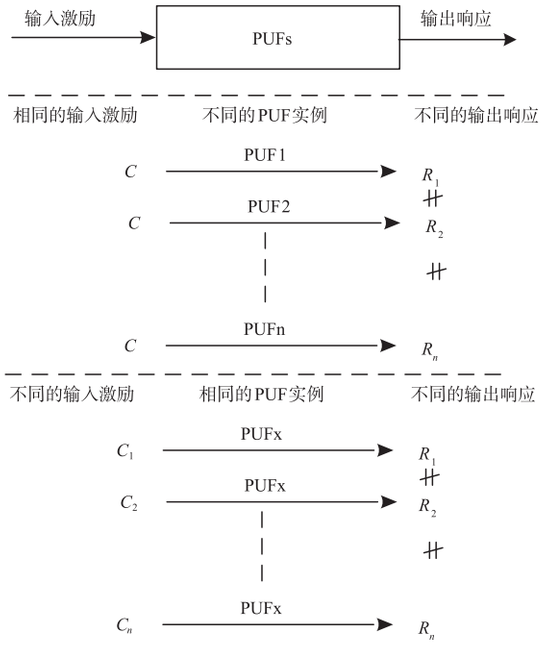


图1 PUF的输入激励与输出响应

RRAM[4,5]概念最早是由蔡少堂于 1971 年提出[6],并于 2008 年由惠普在《Nature》[7]杂志上首次发表报道找到了 RRAM 器件. RRAM 的高阻态和低阻态的阻值都具有一定的随机性,这在存储器本身的应用上存在一定的缺陷,但却为物理不可克隆函数的应用提供了物理熵源. RRAM 在工艺上制备简便并且兼容 CMOS 工艺. 阻变材料的 I-V 特性曲线如图 2 所示,可以看出其具有典型的回滞特性. 该回滞曲线一共分为 4 个区域:低阻态区、高阻态区和两个转换区域,只有当电压幅度超过一定阈值后才可以对阻变材料进行复位或编程.

RRAM 虽然存在高阻态和低阻态两个稳定状态,但其高低阻态的阻值却存在随机性[9]. 图 3 是对 100 个 RRAM 单元进行测量得到其高低阻态的阻值分布情况,从图中可以看出 RRAM 的高阻态比低阻态阻值随机分布范围更大[10].

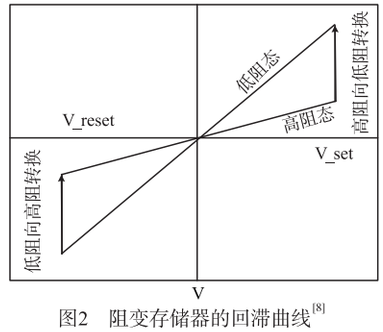


图2 阻变存储器的回滞曲线[8]

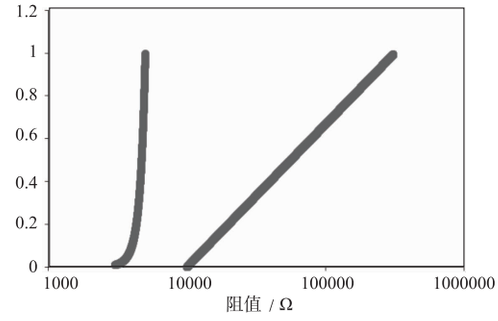


图3 RRAM高低阻态阻值分布[10]

RRAM 的阻值随机特性在信息安全领域的研究受到了广泛的关注. 目前使用 RRAM 设计 PUF 的思路包括高阻实现方式、阈值电压操作方式、数字化分级实现方式、平行 RRAM 实现方式等. 在高阻实现方式上,Yangsong Gao[11]等人提出了一种通过电流镜控制的环形振荡器(CM-RO)型 PUF,在 40×40 的 RRAM 阵列上仅实现了 31200 个 CRP;Pai-Yu Chen[12]等人提出列电流和比较输出的设计方案,在 1024×1024 的 RRAM 阵列上实现了 107 数量级的 CRP,但增加了输入逻辑电路的复杂度;Karsten Beckman[13]等人就提出了将 RRAM 单元与电容并联构成延时单元的方法进行 PUF 设计. 在阈值电压操作方式上,Chen[14]利用当 RRAM 单元切换电压在阈值电压时,RRAM 会被随机设置为高阻或低阻来进行 PUF 设计. Wenjie Che[15]提出了一种通过数字化分级的 PUF 设计方案,方案在 40×40 的阵列上总共实现了 1600 个 CRP. Daniel Arumi[16]等人设计了一种改造的 1T1R 阵列,通过平行 RRAM 实现 PUF 设计的方案,在 256×512 的阵列上实现了 65536 个 CRP.

2 基于 RRAM 延时单元的 PUF 设计

由于 RRAM 的高阻态阻值比低阻态阻值分布范围更广,所以我们在 PUF 设计当中选用 RRAM 的高阻态作为电路的随机性来源.

电路结构如图 4 所示,总体分为两个部分:两个传输通路和一个判决模块. 两个传输通路同时传输一个相同的信号,最终通过不同的延时竞争到达判决模块的输入端. 而判决模块则是用来判决传输信号到达的先后顺序,从而判断哪一条延时通路传输信号更快. C_1、C_2,…,$C_{(2n)}$是 PUF 的输入端,而“输出响应”是 PUF 的输出端. 每条传输通路都由 n 个延时模块串联组成,而每级延迟均由 RRAM 单元特性控制.

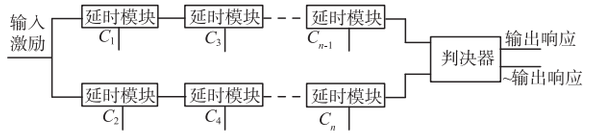


图4　RRAM PUF方案总体结构图

延时模块如图 5 所示,由两个并行的 RRAM 单元构成,通过两个 2 选 1 多路选择器和两个 1 分 2 多路分配器并联起来. 第五个输入信号为 C 的多路选择器用以从两个 RRAM 单元中选出一个投入工作状态. 两个多路选择器共同接入 V_RRAM 和 V_reset,而这两对多路选择器和多路分配器共同拥有同一个控制端 V_ctrl. V_RRAM 是 RRAM 单元的读电压,可对 RRAM 进行非破坏性读出;V_reset 是 RRAM 的重置电压,可将 RRAM 阻值设置为高阻态. 两个多路分配器则在输出端分别接入 GND 和图中的下一个 2 选 1 多路选择器的输入端.

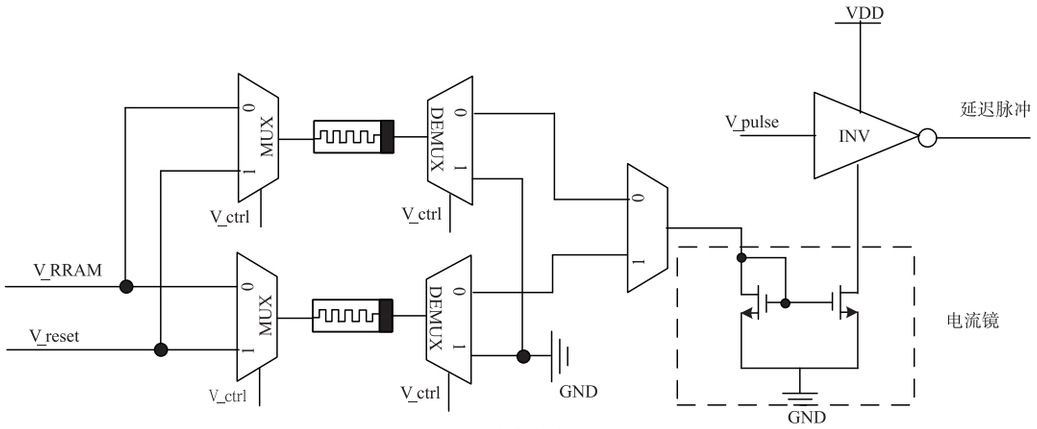


图5　延时模块结构

当 V_ctrl 为“1”时,多路选择器切换到 V_reset 信号,而与此同时多路分配器切换到 GND,重设为高阻态;当 V_ctrl 为“0”时,多路选择器切换到 V_RRAM 信号,而与此同时多路分配器切换到与下一个多路选择器的连接通路上. 而下一个多路选择器的控制端则是输入激励的输入端,当控制端为“1”时选择下端的 RRAM 单元,当控制端为“0”时,选择上面的 RRAM 单元. 由此则将 RRAM 电阻阻值以读电流的方式读出,再接入下一级的延时电路,而此延时电路则由一个电流镜和一个反相器构成. 一方面通过电流镜将 RRAM 读电流信号与反相器接地端相连,另一方面通过设置电流镜的比例,可以将 RRAM 单元读电流放大以增加 RRAM 阻值引起的读电流大小的差异,使输出效果更佳明显,PUF 工作更加稳定. RRAM 单元电阻阻值通过电流镜控制反相器的充放电时间,从而体现其随机性.

多路选择器和多路分配器都是模拟的,由传输门构成,可传输模拟信号而不会像数字多路选择器和数字多路分配器一样将电位拉高到“1”或者“0”,这就保证了信号的 PUF 能够正常工作. 延时单元通过反相器的输入端和输出端依次相连,并形成两条并行的传输通路. 一个相同的脉冲信号则从最左端延时单元的反相器输入端同时输入到两条延时通路,最终输出给判决器模块的输入端. 判决器根据脉冲信号到来的先后顺序得出响应的输出,即 PUF 的输出响应. 如果上端通路脉冲先到达,则判决器输出“1”;反之,则输出“0”. 判决器模块则是由两个与非门构成的触发器构成,通过固定时间采样即可得到 PUF 电路的输出响应.

为了产生一位输出响应,该 PUF 需按以下步骤工作:

(1)编程(reset)阶段:因为 RRAM 的阻值在高阻态的随机分布更为广泛,所以我们在此 PUF 设计中只利用 RRAM 高阻状态的随机性. 所以首先我们需要将 PUF 电路中所有的 RRAM 单元设为高阻,即将 V_ctrl 设为“1”. 这样 RRAM 单元一端接 V_reset,另一端接 GND,则可被 reset 为高阻态. 值得注意的是,这一操作是同时针对所有 RRAM 单元进行操作的,经过此操作后 PUF 中每一个 RRAM 单元的阻值就固定下来了,随后就需要通过一定操作将其阻值的随机分布差异读取出来.

(2)输入激励配置阶段:当所有的 RRAM 单元都被 reset 为高阻态之后,将 V_ctrl 设置为“0”. 这样 RRAM 单元就和编程电压 V_reset 和 GND 断开,转而与读电压 V_RRAM 和下一级多路分配器导通. 在此阶段当中从下一级多路选择器输入激励,每一个延时单元输入口令中的一位,这样输入激励则决定了两条通路上 RRAM 单元的接入情况,并将 RRAM 单元阻值的不同状况体现在每个延时单元的具体延时差异上. 若 PUF 总共消耗 n 个 RRAM 单元,每个延时单元消耗 2 个,则此 PUF 是 $n/4$ 级的,总共拥有 $n/2$ 个延时单元. 一组输入激励选中 PUF 中的 $n/2$ 个 RRAM 单元,即在下一阶段 $n/2$ 个 RRAM 单元

都参与工作,总共拥有 $n/2$ 个输入位. 因此,该 PUF 的 CRP 和 RRAM 单元数量的关系概括为式(1):

$$CRP = 2^{\frac{n}{2}} \tag{1}$$

我们将 RRAM PUF 电路中平均每个 RRAM 单元可产生的 CRP 数量定义为 RRAM 单元 CRP 效率. 本设计方案的 RRAM 单元 CRP 效率为:

$$CRP\ 效率 = \frac{2^{\frac{n}{2}}}{n} \tag{2}$$

(3)输出响应产生阶段:当配置好输入激励,即选中的 RRAM 单元作用到各个延时模块上之后,我们再给两条传输路径的最左端输入一个脉冲信号 V_pulse,V_pulse 通过上下两个并行的延时传输路径之后传递到判决模块的两个输入端,最终得到判决结果,即一位的输出响应. 该过程可将 RRAM 的阻值差异体现为每个 RRAM 单元的读电流差异,再经由电流镜和缓冲器体现为延时单元的延时差异,最终体现在判决结果上. 由于 RRAM 的阻值存在随机性,输出响应也存在其随机性,这就为 PUF 的物理加密功能提供了支撑.

3 实验与讨论

我们使用中芯国际 SMIC65 工艺库,在 Cadence 仿真工具中针对此设计方案各项参数进行了仿真. 本文采用的 RRAM 模型为北京大学康晋峰组和斯坦福大学联合开发的 RRAM Verilog-A 模型[17].

3.1 RRAM 随机性仿真

RRAM 阻值的随机性是该 RRAM PUF 设计的理论基础,因此我们首先对其进行仿真验证. 当导电细丝形成时,RRAM 呈低阻态;而当导电细丝熔断,则 RRAM 呈高阻态[18]. 本文所使用的 RRAM 模型核心就是对导电细丝的形成与熔断进行描述,其随机性是将导电细丝的长度与半径设为随机值得到的.

我们对 2000 个 RRAM 单元同时进行了 RESET 操作,将其全部设为高阻. 先对所有 RRAM 单元施加一个幅度为 -2V 宽度为 20ns 的编程电压,此过程就将 RRAM 设置为高阻态. 再对其施加一个幅度为 100mV 的读电压,读取流过每个 RRAM 的电流值,进行计算之后就可得到 RESET 之后的阻值. 仿真结果如图 6 所示,可以看出 RRAM 单元高阻态的阻值随机分布在 900KΩ ~ 3MΩ,这将成为后续 PUF 设计可靠的物理熵源.

3.2 延时单元功能仿真

延时单元核心是由一个反相器和电流镜构成,结构如图 7 所示. 我们将 RRAM 单元替换成单纯的电阻并对不同阻值状态下的延时情况进行测试. 因为经过前文测试我们所使用的 RRAM 模型高阻态阻值随机分布范围在 900KΩ ~ 3MΩ,所以我们将电阻设置为步进

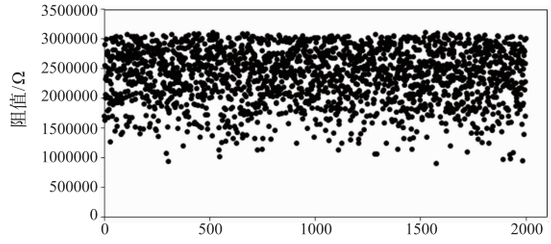


图6 RRAM随机性仿真图

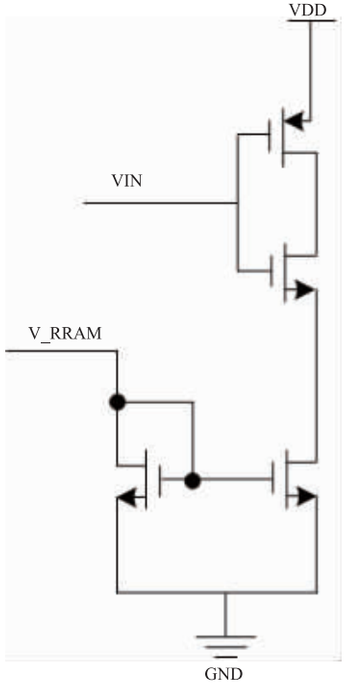


图7 延时单元电路图

100KΩ 从 900KΩ 到 3MΩ,并将电流镜比例设置为 1∶3 对其功能进行测试.

测试结果如图 8 所示,从结果中可以看出,当电阻从 900KΩ 以步进 100KΩ 增加到 3MΩ 的过程中,延迟时间在 1ns 到 3.1ns 之间,其中图上两个邻近曲线之间的延时差在十几皮秒到百皮秒等级. 阻值每提高 100KΩ,延时则约提高几十皮秒. V1 为一个高度为 1V 的上升沿脉冲,V3 为 0.7V 的 RRAM 读电压.

3.3 随机性

随机性描述的是一个 PUF 电路在输出响应中得到“0”和“1”的比例是不是均等,在理想情况下出现“0”和“1”的机会是均等的. 用 $r_{i,1}$ 表示具有 p 位输出响应的 PUF 实例的第 1 个输出向量的第 i 位的二进制值. 随机性如式(3)所示:

$$Randomness = \frac{1}{p \times q}\sum_{l=1}^{q}\sum_{i=1}^{p} r_{i,l} \times 100\% \tag{3}$$

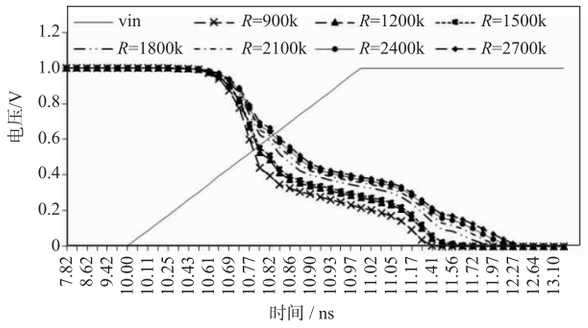


图8　延时仿真结果

理想情况下,这个参数的值是 50%.

p:PUF 实例输出响应向量的位数;

q:PUF 实例输入向量的总个数.

64 位 PUF 针对一个输入激励的一个输出响应结果作为举例,从图 9 可以看出其输出响应分布具有一定随机性.

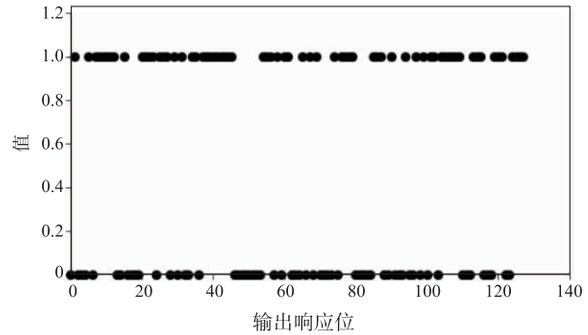


图9　64位PUF随机性仿真结果

对不同位数的随机性仿真数据最终计算结果如表 1 所示.

表 1　不同位数 PUF 的随机性仿真结果

数位	8	16	32	64
随机性	50.20%	50.10%	50.15%	50.17%

随机性代表了 PUF 输出响应中出现“0”和“1”的几率,不能偏“0”或者偏“1”,否则容易被攻击者猜测出响应结果,所以他的理想值应该是50%,从表中可以看出该 RRAM PUF 方案“0”和“1”的出现几率均在 50% 左右,偏差不超过 0.2%. 该种设计方案能够保持良好的随机性.

3.4　稳定性

稳定性:该参数表示的是对于同一个 PUF 电路实例,在输入激励相同,但不同的运行环境下,输出响应保持稳定的能力. 可靠性可以如式(4)所示:

$$Reliability = 100\% - \frac{1}{q}\sum_{t=1}^{q}\frac{HD(R_i,R_{j,t})}{n}\times 100\% \tag{4}$$

在给定相同输入激励的情况下,假设对于第 i 个 PUF 电路实例,R_i 则表示该电路实例响应的最佳值,此最佳值是在正常环境下测得的,亦即参考环境. 然后保持输入激励不变,在不同的运行环境下测得该 PUF 电路实例的输出响应为 $R_{i,t}$,q 是改变环境测试输出响应向量的总次数. $HD(R_i,R_{j,t})$ 则是输出响应 R_i 和 $R_{j,t}$ 之间的汉明距. 理想情况下,可靠性应该是 100%,即没有比特翻转. 针对稳定性的仿真数据最终计算结果如图 10 所示.

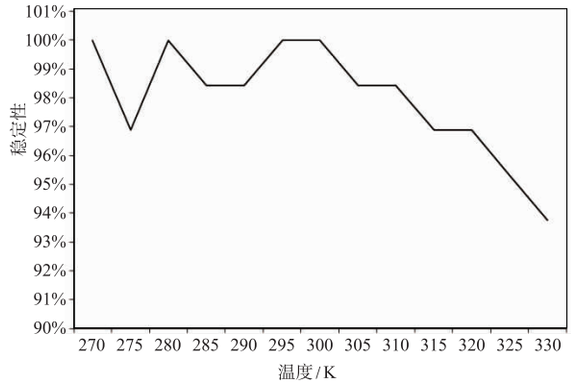


图10　PUF稳定性结果

可以看出该 PUF 稳定性在低温情况下高于高温情况,并在室温正负 20K 左右均能保持在 96% 以上.

3.5　唯一性

唯一性表示的是一个 PUF 实例将自身与其它 PUF 实例区分开来的能力. 当相同的输入激励同时输入到不同的 PUF 实例时,这些 PUF 实例的输出响应应该各不相同,而这个参数则是由不同 PUF 实例的输出响应之间的片间汉明距(inter-Hamming Distance:inter-HD)的平均值来定义的. 理想情况下,唯一性预计为 50%,这意味着在给定相同输入激励的情况下,来自两个或若干个不同 PUF 实例的响应将平均具有一半的不同比特位.

如果 R_i 和 R_j 是两个不同的 PUF 实例的输出响应向量,那么在相同输入激励条件下,唯一性如式(5):

$$Uniqueness = \frac{1}{\binom{k}{2}}\sum_{i=1}^{k-1}\sum_{j=i+1}^{k}\frac{HD(R_i,R_j)}{q}\times 100\% \tag{5}$$

$HD(R_i,R_j)$ 是 R_i 和 R_j 之间的汉明距;

k:PUF 实例的总个数;

q:PUF 实例输出响应向量的位数.

在针对唯一性的仿真中,我们构建十个 PUF 实例对其进行仿真. 分别针对 8 位,16 位,32 位,64 位的 PUF 进行仿真计算. 表 2 是十个 64 位 PUF 在输入激励为 000000 时相互的汉明距,这样的汉明距一共有 64 组,对它们求均值得到最终的唯一性指标.

图 11 统计了 64 位 PUF 实例之间的汉明距的分布情况,而表 3 则是各个不同位数 RRAM PUF 唯一性的

最终计算结果,可以看出该 PUF 方案的唯一性接近 50%,偏差不超过 0.8%,拥有良好的唯一性.

表 2 十个 64 位 PUF 在输入 000000 时的汉明距

	1	2	3	4	5	6	7	8	9	10
1	0	29	37	35	27	31	32	39	35	27
2	0	0	36	64	30	30	37	32	26	28
3	0	0	0	28	34	38	37	28	36	64
4	0	0	0	0	34	34	27	32	38	36
5	0	0	0	0	0	28	31	30	30	30
6	0	0	0	0	0	0	33	34	34	26
7	0	0	0	0	0	0	0	33	31	27
8	0	0	0	0	0	0	0	0	32	36
9	0	0	0	0	0	0	0	0	0	28
10	0	0	0	0	0	0	0	0	0	0

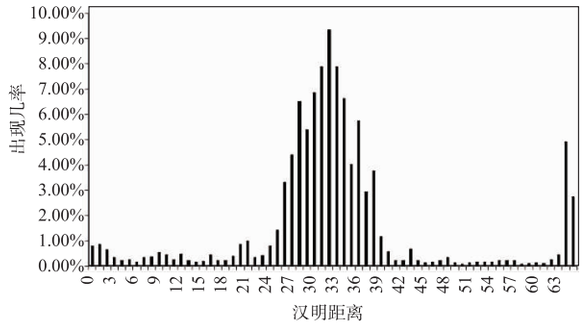


图11 64位PUF唯一性测试中汉明距几率

表 3 不同位数 PUF 的唯一性仿真结果

数位	**8**	**16**	**32**	**64**
唯一性	49.69%	49.48%	50.42%	50.21%

4 CRP 效率对比分析

若本方案所使用的 RRAM 单元数量为 n,由于每个延时单元投入两个 RRAM 单元,根据输入激励的输入情况,在 PUF 的读取过程中每两个单元必定有一个在工作,所以其总共的 CRP 数量为 $2^{n/2}$,以指数增长.

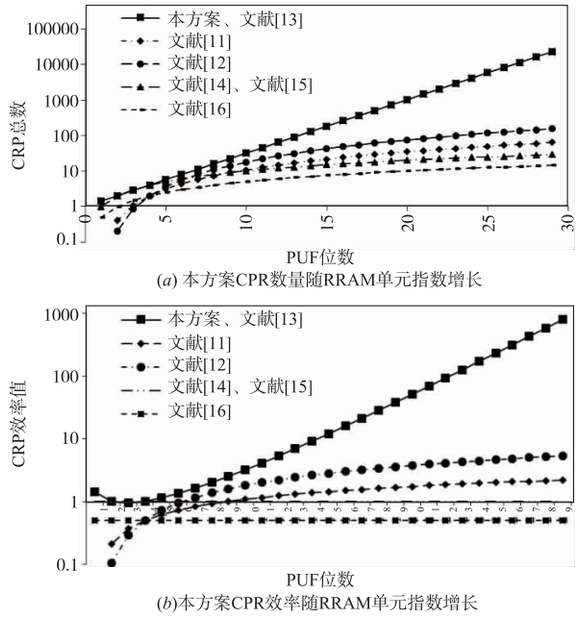
然而在文献[11]中,假设其投入的是一个 $x\times y$ 的 RRAM 阵列,则根据其工作原理,那么相应的 CRP 则是 $x\times y\times(y-1)$,当行列相等时其 CRP 为 $x^2\times(x^{\frac{1}{2}}-1)/2$. 若总的 RRAM 投入数量为 n,则该 PUF 方案的 CRP 为 $n\times(n^{\frac{1}{2}}-1)/2$,即 PUF 电路的 CRP 数量根据 RRAM 单元总数 n,以 3/2 次方进行增长,这个增长速度并不是很高.

同样假设 RRAM 阵列的行列分别为 x 和 y,在文献[12]中提到的在使用 $N\times N$ 阵列时其 CRP 为 $N^2(N-1)\log_2 N/2$,其 CRP 数量可计算为 $[n\times(n^{1/2}-1)\log_2 n^{1/2}]/2$;文献[13]的 CRP 数量为 $2n/2$;文献[14]和[15]的 CRP 数量为 $x\times y$,同样的当行列相等时,若 RRAM 单元总数为 n 时,其 CRP 为 n;文献[16]的 CRP 数量为 $x\times y/2$,按本文的计算方法为 $n/2$. 并将本方案和其他文献中的方案进行对比,对比结果如表 4 所示.

表 4 各方案 CRP 数量与 RRAM 总数 n 之间的关系以及 RRAM 单元 CRP 效率

文献方案	CRP 总数	效率
本方案	$2^{n/2}$	$2^{n/2}/n$
[11]	$n\times(n^{1/2}-1)/2$	$(n^{1/2}-1)/2$
[12]	$[n\times(n^{1/2}-1)\log_2 n^{1/2}]/2$	$[(n^{1/2}-1)\log_2 n^{1/2}]/2$
[13]	$2^{n/2}$	$2^{n/2}/n$
[14][15]	n	1
[16]	$n/2$	1/2

图 12(a)、(b)给出了各个 RRAM 方案 CRP 随 RRAM 单元数量的增长曲线,可以看出当 RRAM 单元数量投入超过 2 个之后本方案的 CRP 数量开始超越所有以往的 RRAM PUF 设计方案,RRAM 单元的 CRP 效率也在 RRAM 数量超过 4 之后处于最高值,尤其在超过 20 个投入数量之后便开始以数量级的规模远远超越以往方案,这样的 RRAM 投入数量在实际应用中是非常常见的. 另一方面,虽然本方案和文献[13]中所实现的 CRP 增长曲线相同,但由于方案[13]需要引入电容,电容的存在会影响 PUF 的随机性,并且电容值也不易控制,所以该方案在设计和实际制造中并不建议使用,三项参数也会剧烈的受到电容的影响.



(a) 本方案CPR数量随RRAM单元指数增长

(b)本方案CPR效率随RRAM单元指数增长

图12

5 结论

我们对以往方案 CRP 效率不够高的问题进行了针对性设计,并对 PUF 的各项参数进行了仿真实验与计算. 由以上实验结果可以看出,本方案在拥有良好的随

机性、唯一性、稳定性的前提下,在投入相同数量的 RRAM 单元的条件下,CRP 的增长高于以往方案,并且在强 PUF 应用上尤为明显,这对 PUF 的安全性是一个非常重要的保证.

参考文献

[1] Herder C, Yu M D, Koushanfar F, et al. Physical unclonable functions and applications: A tutorial[J]. Proceedings of the IEEE, 2014, 102(8): 1126 – 1141.

[2] PAPPU RS. Physical one-way function[D]. Boston: Massachusetts Institute of Technology, 2001.

[3] Oliver K, Markus G K. Design principles for tamper-resistant smartcard processors [A]. USENIX Workshop on Smartcard Technology [C]. Chicago: USENIX Association, 1999. 9 – 20.

[4] Li H, Gao B, Chen H Y H, et al. 3-Dresistive memory arrays: from intrinsic switching behaviors to optimization guidelines [J]. IEEE Transactions on Electron Devices, 2015, 62(10): 3160 – 3167.

[5] Jiang Z, Wu Y, Yu S, et al. A Compact model for metal-oxide resistive random access memory with experiment verification[J]. IEEE Transactions on Electron Devices, 2016, 63(5): 1884 – 1892.

[6] Chua L O. Memristor-The missing circuit element[J]. IEEE Transactions on Circuit Theory, 1971, 18(5): 507 – 519.

[7] Strukov, D. B, G. S. Snider, D. R. Stewart, et al. The missing memristor found[J]. Nature, 2008, 453(7191): 80 – 83.

[8] Lewis D L, Lee H H S. Architectural evaluation of 3D stacked RRAM caches[A]. IEEE International Conference on 3d System Integration[C]. San Francisco: IEEE, 2009. 1 – 4.

[9] Jiao B, Deng N, Yu J, et al. Resisitive switching variability study on 1T1R AlOx/WOx-based RRAM array[A]. IEEE International Conference on Electron Devices and Solid-State Circuits[C]. Hong Kong: IEEE, 2013. 1 – 2.

[10] Wei Z, et al. Highly reliable TaOx ReRAM and direct evidence of redox reaction mechanism [A]. IEEE International Electron Devices Meeting [C]. San Francisco: IEEE, 2008. 1 – 4.

[11] Gao Y, Ranasinghe D C, Al-Sarawi S F, et al. mrPUF: Anovel memristive device based physical unclonable function[A]. International Conference on Applied Cryptography and Network Security [C]. New York: Springer, Cham, 2015. 595 – 615.

[12] Chen P Y, Fang R, Liu R, et al. Exploiting resistive cross-point array for compact design of physical unclonable function[A]. IEEE International Symposium on Hardware Oriented Security and Trust[C]. Washington DC: IEEE, 2015. 26 – 31.

[13] Beckmann K, Manem H, Cady N C. Performance enhancement of a time-delay PUF design by utilizing integrated nanoscale ReRAM devices[J]. IEEE Transactions on Emerging Topics in Computing, 2017, 5(3): 304 – 316.

[14] Chen A. Reconfigurable physical unclonable function based on probabilistic switching of RRAM[J]. Electronics Letters, 2015, 51(8): 615 – 617.

[15] Che W, Plusquellic J, Bhunia S. A non-volatile memory based physically unclonable function without helper data [A]. IEEE/ACM International Conference on Computer-Aided Design[C]. Austin: IEEE, 2015. 148 – 153.

[16] Arumi D, Manich S, Rodriguez-Montanes R. RRAM based cell for hardware security applications[A]. IEEE International Verification and Security Workshop[C]. Cantabria: IEEE, 2016. 1 – 6.

[17] Li H, Jiang Z, Huang P, et al. Variation-aware, reliability-emphasized design and optimization of RRAM using SPICE model[A]. Design, Automation & Test in Europe Conference & Exhibition[C]. Grenoble: IEEE, 2015. 1425 – 1430.

[18] Guan W, Long S, Liu Q, et al. Nonpolar nonvolatile resistive switching in Cu doped [J]. IEEE Electron Device Letters, 2008, 29(5): 434 – 437.

作者简介

杨　轩　男,1989 年 3 月出生,河南三门峡人,硕士,主要研究方向:电路设计、IC 测试.
E-mail: yangxuan2698860@sina.com

叶文强　男,1995 年 1 月出生,福建漳州人,硕士在读,主要研究方向:PUF 电路设计与安全.
E-mail: 18041379956@163.com

崔小乐(通讯作者)　男,1975 年 3 月出生,陕西省西安市人,博士,北京大学深圳研究生院教授,博导,主要研究领域:IC 设计与测试,电子系统可靠性与安全性.
E-mail: cuixl@pkusz.edu.cn