一种基于动态环形振荡器物理不可克隆函数统计模型的频率排序算法

徐金甫 吴 缙*

(解放军信息工程大学 郑州 450001)

摘 要：针对现有环形振荡器物理不可克隆函数(ROPUF)设计存在的可靠性和唯一性不高，导致在应用时安全性较差的问题，该文提出面向ROPUF的统计模型，定量分析了可靠性和唯一性的影响因素，发现增大延迟差能够提高可靠性，减小环形振荡器(RO)单元间的工艺差异可以提高唯一性。根据该模型结论，设计了基于mesh拓扑结构的动态RO单元，结合RO阵列频率分布特性，设计了一种新的频率排序算法，以增大延迟差和减小RO单元的工艺差异，从而提高ROPUF的可靠性和唯一性。结果表明，与其他改进设计的ROPUF相比，所提设计的可靠性和唯一性具有显著优势，可达到99.642%和49.1%，且受温度变化的影响最小。安全性分析证明，该文的设计具有很强的抗建模攻击能力。

关键词：信息安全；物理不可克隆函数；统计模型；频率排序

中图分类号：TP331; TP309 **文献标识码**：A **文章编号**：1009-5896(2019)03-0717-08

DOI: 10.11999/JEIT180405

Frequency Sorting Algorithm Based on Dynamic Ring Oscillator Physical Unclonable Function Statistical Model

XU Jinfu WU Jin

(*The PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: The existing Ring Oscillator (RO) Physical Unclonable Function (ROPUF) design has low reliability and uniqueness, resulting in poor application security. A statistical model for ROPUF is proposed, the factors of reliability and uniqueness are quantitatively analyzed, it is found that the larger delay difference can improve the reliability, and the lower process difference between RO units can improve the uniqueness. According to the conclusion of the model, a dynamic RO unit is designed based on the mesh topological structure. In combination with the frequency distribution characteristics of the RO array, a new frequency sorting algorithm is designed to increase the delay difference and reduce the process variation of the RO unit, thereby improving the reliability and uniqueness of ROPUF. The results show that compared with other improved ROPUF designs, the reliability and uniqueness of the proposed design has significant advantages, which can reach 99.642% and 49.1%, and temperature changes affect minimally them. It is verified by security analysis that the proposed design has strong anti-modeling attack capabilities.

Key words: Information security; Physical Unclonable Function (PUF); Statistical model; Frequency sorting

1 引言

物理不可克隆函数(Physical Unclonable Function, PUF)的引入为解决信息安全问题提供了新的思路。在数字电路PUF中，环形振荡器物理不可克隆函数(Ring Oscillator Physical Unclonable Function, ROPUF)不仅突破了仲裁器PUF高对称性布局布线的限制[1]，并且能够克服SRAM PUF每次生成响应值都要求重启电路的缺陷[2]，能够灵活地应用于安全防护[3]。因此，对ROPUF进行深入研究具有重要意义。

为提高ROPUF的安全性，国内外学者主要研究影响ROPUF性能的关键因素，提出了许多改进的ROPUF结构[4,5]和频率排序方案[6−8]。文献[4]提出了一种选择相邻位置RO单元进行频率比较的方法来补偿系统工艺差异对ROPUF唯一性产生的不利影响，并设计了一种可配置的环形振荡器(Configurable Ring Oscillator, CRO)结构来配合1-out-of-k降噪方法。该方法增加了ROPUF结构的约束，减少了可产生的激励响应对(Challenge-Response Pairs, CRP)数量。文献[5]提出了一种基于动态RO单元设计的性能优化算法，但并没有考虑环境因素对ROPUF性能指标的影响，而其改进的RO单元结构所产生频率数少，CRP空间增大效

收稿日期：2018-04-28；改回日期：2018-09-21；网络出版：2018-10-22
*通信作者： 吴缙 woshi57890@163.com

率不高。文献[6]针对传统ROPUF应用于密钥产生时响应噪声大、熵密度低等缺陷，提出了一种基于Lehmer格雷编码的频率排序方案，在提取PUF响应过程中频率集合的后处理模块占用了大量资源，对于资源受限的物理实体应用适用性差。文献[7]统计分析了RO阵列的频率分布特性，提出了两种新的振荡频率比较策略。但这两种频率比较策略均不能兼顾响应熵密度和CRP空间大小。文献[8]分析了当ROPUF处于可变的温度条件下对称和非对称RO比较策略的统计特性，提出了能够提高ROPUF可靠性的基于频率比的计数提取方案，但并没有考虑对唯一性等性能的影响，其应用范围受到限制。

针对以上问题，为了提高ROPUF的安全性，本文提出了基于延迟变量和环境变化的ROPUF统计模型。在该模型下，定量分析可靠性和唯一性的关键影响因子，找到了ROPUF结构的优化方向。然后结合可配置RO单元设计思想和RO阵列频率分布特性，指导频率排序算法设计，这是本文优化设计的思路和理论支撑。

2 ROPUF的统计模型

2.1 模型参数定义

ROPUF中环形振荡器是由同构的硬宏单元组成。但由于制造时存在着不可控的工艺偏差，环形振荡器之间会有微小的差异。根据统计静态时序分析(Statistical Static Timing Analysis, SSTA)[9]的结果，晶体管参数的制造工艺差异符合高斯分布。

定义 1 设反相器的标称延迟为μ，延迟变化的标准方差σ，则每一级反相器的延迟为

$$D_i \sim N\left(\mu, \sigma^2\right) \tag{1}$$

设RO级数为m，其总延迟D_t可表示为$N\left(m\mu, m\sigma^2\right)$。而激励所选取的环形振荡器对的延迟差为

$$\Delta_c = D_t^a - D_t^b \sim N\left(0, 2m\sigma^2\right) \tag{2}$$

对于传统ROPUF，产生的响应依赖于所选环形振荡器对的延迟差。在实际PUF电路中，将延迟差模拟量转化为数字量的过程并不是理想的，存在着偏斜效应，会导致ROPUF的唯一性降低[7]。设偏斜阈值为s，则输出的响应比特为

$$R = \operatorname{sign}\left(\Delta_c\right) = \begin{cases} 1, & \Delta_c \geq s \\ 0, & \Delta_c < s \end{cases} \tag{3}$$

根据式(3)可推导输出的响应比特等于1的概率为

$$\begin{aligned} P(R=1) &= P(\Delta_c \geq s) \\ &= \int_s^{\infty} \frac{1}{\sqrt{2\pi 2m\sigma^2}} \exp\left(\frac{-x^2}{4m\sigma^2}\right) \mathrm{d}x \\ &= \frac{1}{2} - \frac{1}{2}\operatorname{erf}\left(\frac{s}{\sqrt{4m\sigma^2}}\right) \end{aligned} \tag{4}$$

定义 2 设在相同激励作用下单个响应比特的翻转概率为P_s，每一级反相器的噪声符合均值为0的高斯分布$N\left(0, \sigma^2\right)$[10]。设$n_i$和$n'_i$表示不同环境状态的噪声，响应比特的翻转概率为

$$P_s = P\left[\operatorname{sign}\left(\Delta_c + \sum_{i=1}^{M} n_i\right) \neq \operatorname{sign}\left(\Delta_c + \sum_{i=1}^{M} n'_i\right)\right] \tag{5}$$

定义 3 设不同PUF实例在相同激励作用下产生不同响应比特的概率为P_d，则

$$\begin{aligned} P_d &= P(R=1)\,P(R=0) + P(R=0)\,P(R=1) \\ &= 2P(R=1)\left(1 - P(R=1)\right) \end{aligned} \tag{6}$$

2.2 统计模型建立

下面通过对ROPUF的可靠性和唯一性进行统计建模，分析影响这两个性能指标的关键因子。

(1) 可靠性P_R：考虑环境噪声的影响。因为每个反相器都符合独立一致性的高斯分布，所以片内差异概率P_s等于单个反相器的片内差异概率，根据式(5)可得

$$P_s = P[\operatorname{sign}\left(\Delta D_i + n_i\right) \neq \operatorname{sign}\left(\Delta D_i + n'_i\right)] \tag{7}$$

其中，$\Delta D_i = D_i^a - D_i^b$, ΔD_i的方差等于$2\sigma^2$。因为延迟差的制造工艺差异和环境噪声都符合均值为0的高斯分布，它们的概率密度函数为

$$\left.\begin{aligned} f_a(a) &= \frac{1}{\sqrt{2\pi\sigma_a^2}} \exp\left(-\frac{a^2}{2\sigma_a^2}\right) \\ f_n(n) &= \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp\left(-\frac{n^2}{2\sigma_n^2}\right) \end{aligned}\right\} \tag{8}$$

其中，$\sigma_a^2 = 2\sigma^2$。根据式(7)和式(8)，可计算ROPUF的片内差异概率

$$\begin{aligned} P_s &= P[\operatorname{sign}\left(\Delta D_{\text{inv}} + n_i\right) \neq \operatorname{sign}\left(\Delta D_{\text{inv}} + n_i'\right)] \\ &= 4\int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_a^2}} \exp\left(-\frac{a^2}{2\sigma_a^2}\right) \int_{-\infty}^{-a} \frac{1}{\sqrt{2\pi\sigma_n^2}} \\ &\quad \cdot \exp\left(-\frac{n^2}{2\sigma_n^2}\right) \mathrm{d}n \int_{-a}^{-\infty} \frac{1}{\sqrt{2\pi\sigma_n^2}} \\ &\quad \cdot \exp\left(-\frac{n'^2}{2\sigma_n^2}\right) \mathrm{d}n' \mathrm{d}a \\ &= 4\int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_a^2}} \exp\left(-\frac{a^2}{2\sigma_a^2}\right) \\ &\quad \cdot \left(\frac{1}{4} - \frac{1}{4}\operatorname{erf}^2\left(\frac{a}{\sqrt{2\sigma_n^2}}\right)\right) \mathrm{d}a \\ &= \frac{1}{2} - \frac{1}{\pi}\arctan\left(\sqrt{\frac{\sigma_a^4}{2\sigma_a^2\sigma_n^2 + \sigma_n^4}}\right) \end{aligned} \tag{9}$$

根据式(9)可知，通过增大制造工艺差异与环境噪声的比值，片内差异可以减小至接近于0。对于给定激励产生响应的P_s，可以得到条件概率

$$P[\mathrm{sign}\left(\Delta D_i+n_i\right)\neq\mathrm{sign}\left(\Delta D_i+n_i'\right)|\Delta D_i]=\frac{1}{2}-\frac{1}{2}\mathrm{erf}^2\left(|\Delta D_i|\Big/\sqrt{2\sigma_n^2}\right) \tag{10}$$

考虑非理想情况下延迟差转化为响应过程中偏斜效应的影响。令变量$x\sim N\left(-s/\sqrt{m},\sigma_a^2\right)$, P_s可表示为

$$\begin{aligned}P_s&=P\left[\mathrm{sign}\left(\sum_{i=1}^{M}\left(\Delta D_i+n_i\right)-s\right)\neq\mathrm{sign}\left(\sum_{i=1}^{M}\left(\Delta D_i+n_i'\right)-s\right)\right]=P[\mathrm{sign}\left(x+n_i\right)\neq\mathrm{sign}\left(x+n_i'\right)]\\&=2\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi\sigma_a^2}}\exp\left(-\left(x+\frac{s}{\sqrt{m}}\right)^2\Big/2\sigma_a^2\right)\left(\frac{1}{4}-\frac{1}{4}\mathrm{erf}^2\left(\frac{|x|}{\sqrt{2\sigma_n^2}}\right)\right)\mathrm{d}x\\&\approx2\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi\sigma_a^2}}\exp\left(-x^2/2\sigma_a^2\right)\left(1-\frac{s}{\sigma_a^2\sqrt{m}}x\right)\left(\frac{1}{4}-\frac{1}{4}\mathrm{erf}^2\left(\frac{|x|}{\sqrt{2\sigma_n^2}}\right)\right)\mathrm{d}x\\&=\frac{1}{2}-\frac{1}{\pi}\arctan\left(\sqrt{\frac{\sigma_a^4}{2\sigma_a^2\sigma_n^2+\sigma_n^4}}\right)-\frac{s}{\sqrt{2\pi m\sigma_a^2}}\left(1-\frac{2}{\pi}\sqrt{\frac{\sigma_a^2}{\sigma_a^2+\sigma_n^2}}\arctan\left(\sqrt{\frac{\sigma_a^2}{\sigma_a^2+\sigma_n^2}}\right)\right)\end{aligned} \tag{11}$$

则ROPUF的可靠性指标可表示为

$$P_R=1-P_s=\frac{1}{2}+\frac{1}{\pi}\arctan\left(\sqrt{\frac{\sigma_a^4}{2\sigma_a^2\sigma_n^2+\sigma_n^4}}\right)+\frac{s}{\sqrt{2\pi m\sigma_a^2}}\left(1-\frac{2}{\pi}\sqrt{\frac{\sigma_a^2}{\sigma_a^2+\sigma_n^2}}\arctan\left(\sqrt{\frac{\sigma_a^2}{\sigma_a^2+\sigma_n^2}}\right)\right) \tag{12}$$

(2) 唯一性P_u：为了在相同数学模型中计算片间工艺差异，需要比较不同PUF实例的响应。若不同PUF实例生成的响应是完全独立的，那么式(6)可以简单表示为

$$P_d=2P(R=1)\,P(R=0)=2\left(\frac{1}{2}-\frac{1}{2}\mathrm{erf}\left(\frac{s}{\sqrt{2m\sigma_a^2}}\right)\right)\left(\frac{1}{2}+\frac{1}{2}\mathrm{erf}\frac{H}{\sqrt{m}}\right)=\frac{1}{2}-\frac{1}{2}\mathrm{erf}^2\left(\frac{s}{\sqrt{2m\sigma_a^2}}\right) \tag{13}$$

则ROPUF的唯一性指标可表示为

$$\begin{aligned}P_u&=\frac{1}{2}-\left|P_d-\frac{1}{2}\right|=2P(R=1)\left(1-P(R=1)\right)\\&=\frac{1}{2}-\frac{1}{2}\mathrm{erf}^2\left(\frac{s}{\sqrt{2m\sigma_a^2}}\right)\end{aligned} \tag{14}$$

2.3 模型分析

从模型可知，ROPUF的性能指标与RO级数m，延迟差的标准方差σ_a，环境噪声的标准方差σ_n和偏斜阈值s有关。本文中将偏斜阈值s看作可配常量。首先，讨论参数m, σ_a, σ_n对可靠性P_R的影响。根据式(10)可知，在$\Delta D_i=0$时，$P[\mathrm{sign}\left(\Delta D_i+n_i\right)\neq\mathrm{sign}\left(\Delta D_i+n'_i\right)|\Delta D_i]$取最大值。根据式(12)可知，因为

$$(2/\pi)\sqrt{\sigma_a^2/\left(\sigma_a^2+\sigma_n^2\right)}\arctan\left(\sqrt{\sigma_a^2/\left(\sigma_a^2+\sigma_n^2\right)}\right)<1 \tag{15}$$

在其他参数保持不变时，P_R随着RO级数m的增大而减小。当σ_a/σ_n较大时，$\sigma_a^2/\left(\sigma_a^2+\sigma_n^2\right)$接近于1，$1-2/\pi\sqrt{\sigma_a^2/\left(\sigma_a^2+\sigma_n^2\right)}\arctan\left(\sqrt{\sigma_a^2/\left(\sigma_a^2+\sigma_n^2\right)}\right)$近似为0，故RO级数$m$对$P_R$的影响可以忽略不计。因为$\sigma_a$受到制造工艺水平限制，不作为唯一性指标的主要考虑因素，当环境变化剧烈，即σ_n增大时，响应翻转概率P_s将变差。所以根据式(9)，式(10)，式(12)可知，如果$\Delta_c\approx0$，片内差异概率将较大；而Δ_c比较大时，制造工艺差异将成为决定响应比特的主要因素，环境噪声将很难翻转响应比特。

然后，讨论参数m, σ_a对唯一性P_u的影响。根据式(14)可知，s看作常量，m保持不变，当σ_a增大时，$\mathrm{erf}^2\left(s/\sqrt{2m\sigma_a^2}\right)$会减小，导致$P_u$增大。ROPUF的环形振荡器组通常排列成2维网格模型[7]，布局在相邻位置的RO单元的工艺差异最小，延迟差的标准方差σ_a最大。因此，选择相邻位置的RO单元进行比较可获得高唯一性。

从以上分析可知，为获得更高的可靠性P_R，可增加用于比较的RO单元的延迟差Δ_c；为增大ROPUF的唯一性P_u，应减小所选RO单元的工艺差异。此结论将指导基于MC-RO单元的动态PUF的设计。

3 基于MC-RO单元的动态PUF设计

3.1 基于mesh拓扑结构的可配置RO单元设计

根据统计模型结论，需要设计一种可配置RO单元以产生多种RO级数，采用不同RO级数的环形振荡器进行比较来增大延迟差Δ_c，以提高

PUF的可靠性。为了不消耗更多的芯片资源，在同一个RO单元中产生尽可能多的振荡频率，本文设计了基于mesh拓扑结构的可配置RO单元(Mesh Configurable-RO, MC-RO)，其逻辑电路结构如图1所示。MC-RO单元包括MC-RO和死锁矫正模块两个部分。MC-RO是通过控制奇数个反相单元间的信号传输，来产生多个不同的振荡频率。死锁矫正模块对MC-RO的状态位$S[0..4]$进行控制，来防止MC-RO的信号传输发生冲突。

图1右侧虚线框内为多路输出选择器deMUX和数据选择器MUX结构，并定义了deMUX和MUX的输入输出端口。考虑到路径逻辑的合理性，对MC-RO单元中MUX3和每个deMUX的控制信号进行了适当的配置，配置原因如下所述。

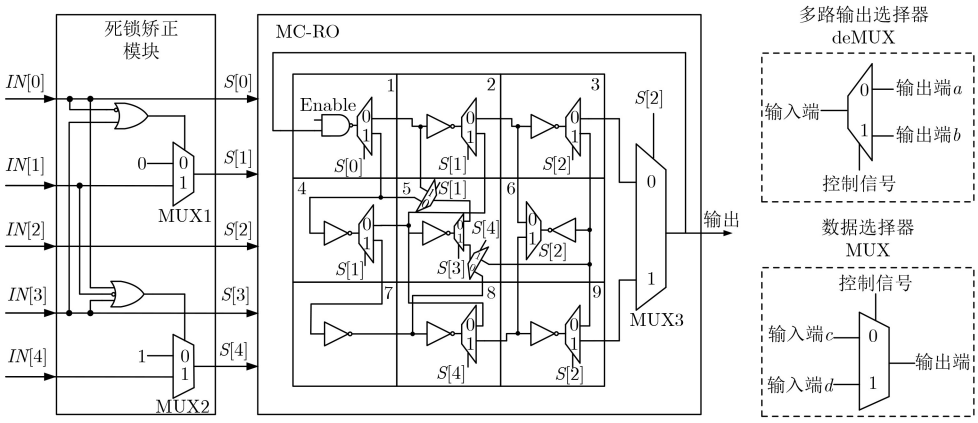


图 1 MC-RO单元的逻辑电路

(1) 分块1的路径选择应是随机的，单独配置为$S[0]$；

(2) 分块2和4位置对称，都配置为$S[1]$；

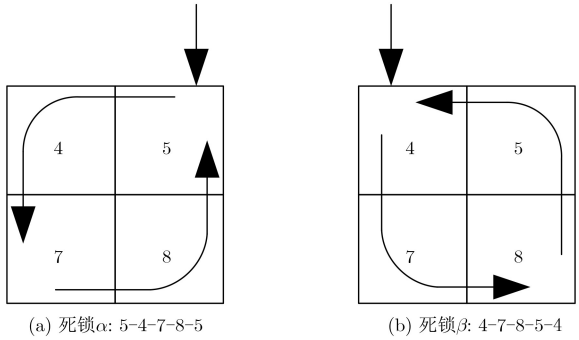
(3) 分块3, 6, 9之间按由上至下或由下至上的路径方向传播，且分块3, 9的输出端与反馈模块的输入端相连接，故分块3, 6, 9和MUX3都配置为$S[2]$；

(4) 分块5与分块2, 4, 8之间的连接是双向的，与(3)中情况相同，分块2, 4, 5间是按一致性方向传播，分块5, 8间也是如此，所以分块5配置了3个状态选择位$S[1]$, $S[3]$和$S[4]$；

(5) 分块7作为拐点，不进行路径分流。

MC-RO单元将9个反相单元和10个多路输出选择器deMUX划分为9个块。使能信号Enable控制单元的启动与关闭。反馈链路将数据选择器MUX3的输出信号传输到分块1，形成环路结构。根据循环通路中的反相单元数量，RO级数可分为3, 5, 7, 9等4种情况。输入不同的$S[0..4]$，使得环形振荡器的RO级数发生改变，所产生的振荡频率不同。例如，当$S[0..4]$=000XX(“X”代表0或1)时，RO电路的路径为1-2-3(“1-2-3”中数字代表分块，数字顺序代表路径传播方向)，RO单元只能产生1种RO级数为3的路径。当$S[0..4]$=001XX时，路径为1-2-3-6-9，在RO单元中一共可以产生9种RO级数为5的路径。以此类推，可以得到不同RO级数的路径产生情况。

为了使MC-RO产生尽可能多的振荡频率，分块间的信号传输并不是指向某一个特定的分块，例如分块5中的3个deMUX有4个输出端口，可将信号传输给分块2, 4, 6, 8中的一个。而分块5的输入信号可以由分块2, 4或8提供，也就可能存在这种情况：分块5传输给其它分块的信号，之后又传输分块5，与之前分块5的输入信号冲突。因此，需要对状态位$S[0..4]$进行约束，来解决可能存在的信号传输冲突问题。通过对MC-RO逻辑电路的信号传输情况的分析发现，分块4, 5, 7, 8之间的信号传输可能存在冲突，在网络拓扑学中这一现象称为路径死锁，RO单元的路径死锁分为5-4-7-8-5和4-7-8-5-4两种情况，分别以死锁α和β表示，如图2所示。死锁α的诱发条件为$S[0..4]$=01000或01100。当$S[0]$=0, $S[3]$=0时，若$S[1]$=1，则$S[4]$只能取值1，若$S[1]$=0，则路径恒为1-2-3，与$S[4]$取值无关。死锁β的诱发条件为$S[0..4]$=11000, 11001, 11100或11101。当$S[0]$=1, $S[3]$=0时，$S[1]$只能取值0，其它



(a) 死锁α: 5-4-7-8-5　　(b) 死锁β: 4-7-8-5-4

图 2 MC-RO电路中的路径死锁

情况下可以任意取0/1。根据路径死锁结构及诱发条件，本文设计了死锁矫正方案来解决这一问题，如表1所示。

表 1　死锁矫正方案

$S[0]$	$S[3]$	$S[1]$	是否存在死锁(是/否)	矫正方案	
				$S[4]$	$S[1]$
0	0	1	是	1	–
0	1	0/1	否	0/1	–
1	0	–	是	–	0
1	1	–	否	–	0/1

根据上述方案设计的死锁矫正模块放置在配置信息$IN[0..4]$与MC-RO单元之间，如图1所示。配置信息$IN[0..4]$可随机取值0或1，但死锁矫正模块可能会对ROPUF响应的随机性造成影响。

选择两个环形振荡器M_i和M_j进行比较，若两者产生的频率f_i高于f_j，则比较结果为1，否则为0。MC-RO单元中不同的RO级数3, 5, 7, 9分别用事件A, B, C, D表示，事件出现概率分别为ρ_{A}, ρ_{B}, ρ_{C}, ρ_{D}。假设相同RO级数的比较结果输出0或1的概率各为50%。M_i和M_j的频率比较结果的概率分布如表2所示。比较结果为1的概率是

$$\begin{aligned}\rho_1 &= \rho_{\mathrm{A}}\times\rho_{\mathrm{A}}\times 50\% + \rho_{\mathrm{A}}\times\rho_{\mathrm{B}} + \rho_{\mathrm{A}}\times\rho_{\mathrm{C}} \\ &\quad + \rho_{\mathrm{A}}\times\rho_{\mathrm{D}} + \rho_{\mathrm{B}}\times\rho_{\mathrm{B}}\times 50\% \\ &\quad + \rho_{\mathrm{B}}\times\rho_{\mathrm{C}} + \rho_{\mathrm{B}}\times\rho_{\mathrm{D}} + \rho_{\mathrm{C}}\times\rho_{\mathrm{C}}\times 50\% \\ &\quad + \rho_{\mathrm{C}}\times\rho_{\mathrm{D}} + \rho_{\mathrm{D}}\times\rho_{\mathrm{D}}\times 50\% \\ &= (\rho_{\mathrm{A}}+\rho_{\mathrm{B}}+\rho_{\mathrm{C}}+\rho_{\mathrm{D}})^2\times 50\% \\ &= 50\% \end{aligned} \tag{16}$$

由式(16)可知，只要相同RO级数的比较结果满足随机性，死锁矫正模块就不会影响ROPUF响应的随机性。

3.2　频率排序算法

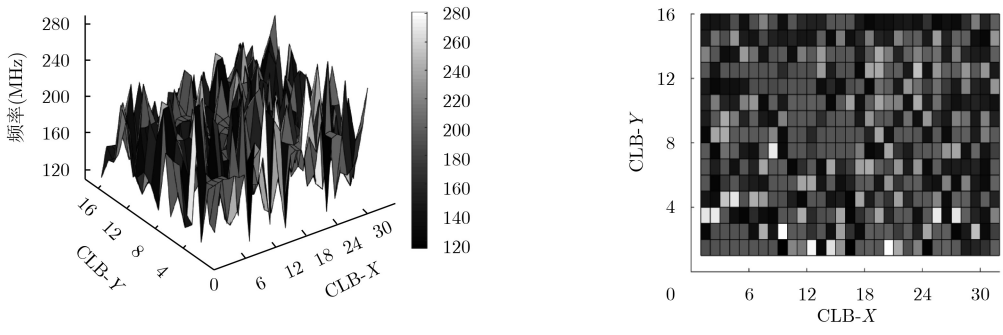
MC-RO单元可产生4种不同RO级数，由该单元组成规模为32×16的RO阵列，其频率分布情况

表 2　频率比较结果的概率分布

RO级数	3	5	7	9	概率
3	0/1	1	1	1	ρ_{A}
5	0	0/1	1	1	ρ_{B}
7	0	0	0/1	1	ρ_{C}
9	0	0	0	0/1	ρ_{D}
概率	ρ_{A}	ρ_{B}	ρ_{C}	ρ_{D}	100%

如图3所示，RO单元对应于平面分布图上的坐标(X, Y)。根据统计模型结论，在2维网格模型的RO阵列中，RO单元间的工艺差异不同，例如，RO1(1, 1)与RO2(1, 2)间的工艺差异小于RO1(1, 1)与RO3(3, 5)间的工艺差异。从制造者角度，通过提高工艺水平可以减少器件参数的失配，从而减小RO单元间的工艺差异[11]。从设计者角度，在器件参数无法改变的情况下，选择相邻位置的RO单元进行比较，能够减小RO单元间的工艺差异，从而设计出具有更高唯一性的ROPUF[12]。

根据频率分布特性可知，通过配置MC-RO单元的状态位，可以增大不同RO单元间的延迟差。采用传统的选择相邻位置的RO单元进行计数和比较，不同芯片的相同PUF中，片间工艺差异导致RO单元频率波动范围将小于延迟差，在相同激励作用下PUF产生的响应几乎完全相同，将大大降低PUF的唯一性。为了克服增大延迟差带来的副作用，本文采用Lehmer格雷编码作为补偿方案[6]。Lehmer格雷编码不要求排序对象的确定数值，可以有效地用于ROPUF的后处理。但是，将其应用在基于MC-RO单元的PUF的频率排序过程，可能会出现两个不同激励所选择频率集合的顺序一致，导致最后输出的响应相同，这违背PUF属性中的不可预测性[13]。本文设计了改进的Lehmer格雷编码方案，将编码中系数集合产生阶段的比较对象由振荡频率换为频率到平均值的距离，使得不同激励选择的频率集合的相对顺序不同，保证了不同CRP之间的独立性。同时，改进的Lehmer格雷编码方案



(a) 频率空间分布图　　(b) 频率平面分布图

图 3 RO阵列频率分布图

是选择相邻位置的两个环形振荡器进行比较，能够提高PUF的唯一性。以规模为$N \times M$的RO阵列为例，具体的频率排序算法伪代码描述见表3的算法1。

表 3 频率排序算法伪代码

算法 1 频率排序算法(FSA)

(1) for C determining CLB-X do
(2) $F = \{f(x,1), f(x,2), \cdots, f(x,N)\}$;
(3) for i=1 to N do
(4) $Z_i = \text{COUNTER}(f(x,i))$;
(5) end for
(6) $\bar{Z} = (Z_1 + Z_2 + \cdots + Z_N)/N$;
(7) for i=1 to N do
(8) $d_i = |Z_i - \bar{Z}|$;
(9) end for
(10) if (x>y) then
(11) $gt(x, y)$=1
(12) else
(13) $gt(x, y)$=0
(14) end if
(15) for k=1 to N–1 do
(16) for j=1 to k do
(17) S_1=0
(18) $L_k = S_j + gt(d_{k+1}, d_j)$;
(19) end for
(20) end for
(21) $R = \text{Gray}(L_1)\,||\text{Gray}(L_2)\,||\cdots||\text{Gray}(L_{N-1})$;
(22) end for
(23) return (R)

频率排序算法可概括为3步：

第1步(1～5行) 激励C决定选取的CLB-X轴坐标x，收集空间坐标(x,i)，$i \in \{1\ 2 \cdots N\}$对应MC-RO的振荡频率，通过计数模块将其映射到一个整数集合$\boldsymbol{Z} = \{Z_1\ \ Z_2\ \cdots\ Z_N\}$。

第2步(6～22行) 对$\boldsymbol{Z}$中元素取平均值$\bar{Z}$，计算每个元素与$\bar{Z}$之间的距离$\boldsymbol{D} = \{d_1\ d_2\ \cdots\ d_N\}$。用系数向量$\boldsymbol{L}^{N-1} = [L_1\ L_2\ \cdots\ L_{N-1}], L_i \in \{1\ 2\ \cdots\ i\}$表示$\boldsymbol{D}$的分类排序，$\boldsymbol{L}^{N-1}$可以取$N$个可能的值。集合$\boldsymbol{D}$的Lehmer系数为

$$L_j = \sum_{i=1}^{j} gt(d_{j+1}, d_i) \tag{17}$$

第3步(21～23行) 使用二进制格雷码编码Lehmer系数向量$\boldsymbol{L}^{N-1}$，得到响应R。

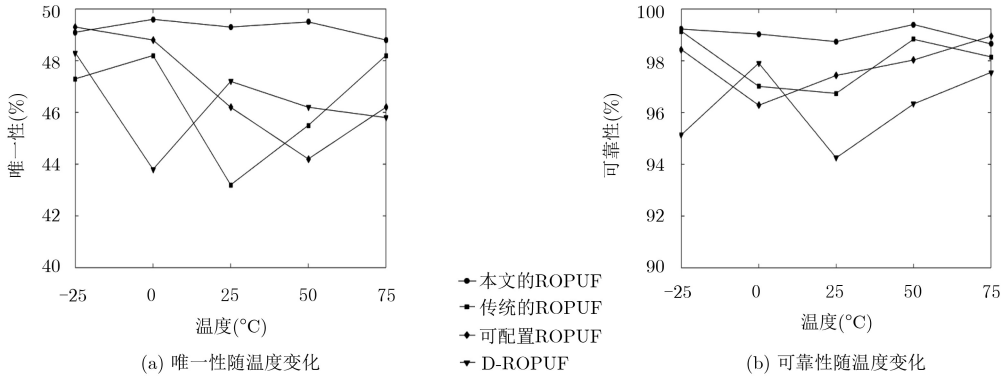
4 性能测试

本文在xilinx公司的Spartan-6 FPGA平台上实现了基于MC-RO单元的PUF设计，采用Verilog语言对MC-RO单元进行了描述，并将其作为硬宏单元在顶层PUF设计中实例化。为了对基于MC-RO单元的PUF的性能指标进行完整评估，在不同温度下和不同频率排序方案下都进行了唯一性和可靠性的测量。

实验测量了基于MC-RO单元的PUF在–25°C, 0°C, 25°C, 50°C, 75°C等温度参数下的平均片间汉明距离和片内汉明距离，如图4所示。根据图中折线变化幅度可看出，相较传统的ROPUF，可配置ROPUF和D-ROPUF设计，本文的ROPUF结构受温度变化影响最小。

基于传统的频率比较方法和基于所设计的频率排序算法，测量了本文的ROPUF的可靠性和唯一性，如表4所示。由表4可知，基于传统的频率比较方法，本文的ROPUF的唯一性随RO级数的增加呈上升趋势，可靠性随RO级数的增加呈下降趋势。基于所设计的频率排序算法，本文的ROPUF的唯一性和可靠性相较其他改进设计具有显著优势，可达到49.1%和99.642%。

不同PUF结构的RO单元资源利用效率如表5所示。以单个RO单元所占LUT数量及可产生频率数



(a) 唯一性随温度变化 (b) 可靠性随温度变化

图 4 PUF在不同温度下的性能对比

为指标，本文的ROPUF的频率产生效率分别是传统ROPUF和D-ROPUF的7.2倍和2.4倍，略低于可配置ROPUF。单从RO单元可产生频率数考虑，所提设计具有更为复杂的激励响应行为，其抗建模攻击能力更高。

从安全性的角度进行分析，假设攻击者采用快速排序方法[14]破解电路。假定该PUF共输出$N-1$位，输出过程中频率排序均有$N!$种，产生每一位输出时振荡频率均有t种可能，故所有可能的情况共有$t^{N-1}[N!]^t$种，每一种被取到的可能性都为$\left(t^{N-1}[N!]^t\right)^{-1}$，

表 4　性能指标分析对比

PUF类型	唯一性(%)	可靠性(%)
传统的ROPUF[2]	47.3	99.140
可配置ROPUF[3]	40.0	98.980
D-ROPUF [4]	46.8	99.059
本文的ROPUF(RO级数为3)	48.4	99.124
本文的ROPUF(RO级数为5)	48.7	99.106
本文的ROPUF(RO级数为7)	48.8	98.994
本文的ROPUF(RO级数为9)	48.9	98.985
本文的ROPUF(频率排序算法)	49.1	99.642

表 5　RO单元资源利用效率对比

指标	传统的ROPUF	可配置ROPUF	D-ROPUF	本文的ROPUF
CLB数量	2	1	1	2
Slice数量	5	3	4	4
LUT数量	6	6	8	15
RO单元可产生频率数	1	8	4	18
抗建模攻击能力	传统的ROPUF<D-ROPUF<可配置ROPUF<本文的ROPUF			

攻击成功所需尝试次数的数学期望为

$$\begin{aligned} Q &= \left(1+2+\cdots+t^{N-1}\left[N!\right]^t\right) t^{N-1}\left[N!\right]^t \\ &= 1+t^{N-1}\left[N!\right]^t 12 \end{aligned} \tag{18}$$

表6比较了t和N在不同取值下攻击次数的数学期望，可知PUF中振荡器的振荡频率越多，产生的PUF输出位数越多，攻击者需尝试的次数呈指数级增长。对于传统ROPUF，当攻击者破解了振荡器间的相对频率关系后，攻击成功率为99.9%[15]。而对于本文设计的PUF，当t取值为18, N为16时，破解所需比较的平均次数已经超过1.99×10^{258}。可配置RO单元能够产生的频率越多，PUF的抗建模攻击能力越强。

表 6　破解不同规格PUF所需攻击次数的比较

t	N	Q
2	8	1.04×10^{11}
18	8	1.35×10^{75}
36	8	2.47×10^{176}
18	16	1.99×10^{258}
36	16	3.85×10^{502}

5　结束语

PUF作为安全防护的新方法正在受到越来越多的关注，对其自身性能的要求也越来越高。首先，本文针对现有ROPUF改进设计追求部分性能优化而整体设计存在缺陷的问题，通过ROPUF的统计模型，分析出了增大延迟差能够提高可靠性指标，选择空间位置相近的RO单元是提高唯一性的有效途径。

然后，基于ROPUF的统计模型结论，提出了基于mesh拓扑结构的可配置RO单元的设计思路，并结合RO阵列频率分布特性，设计了一种能够增大延迟差和减小RO单元的工艺差异的频率排序算法。测量评估了本文设计的基于MC-RO单元的PUF的可靠性和唯一性，并与传统的ROPUF、可配置ROPUF和D-ROPUF等改进设计进行性能对比。对比结果表明，本文的ROPUF结构在唯一性和可靠性上具有显著优势。此外，对基于mesh拓扑结构的可配置RO单元进行拓展研究，可进一步提高ROPUF的抗建模攻击能力。

参 考 文 献

[1] GASSEND B, CLARKE D, DEVADAS S, *et al*. Silicon physical random functions[C]. ACM Conference on Computer and Communications Security, Washington, USA, 2002: 148–160. doi: 10.1145/586110.586132.

[2] XU Xiaolin, BURLESON W, and HOLCOMB D E. Using statistical models to improve the reliability of delay-based PUFs[C]. 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, USA, 2016: 547–552. doi: 10.1109/ISVLSI.2016.125.

[3] STANCIU A, MOLDOVEANU F D, and CIRSTEA M. A novel PUF-based encryption protocol for embedded System on Chip[C]. International Conference on Development and

Application Systems, Suceava, Romania, 2016: 158–165. doi: 10.1109/DAAS.2016.7492566.

[4] MAITI A and SCHAUMONT P. Improved ring oscillator PUF: An FPGA-friendly secure primitive[J]. *Journal of Cryptology*, 2004, 24(2): 375–397. doi: 10.1007/s00145-010-9088-4.

[5] AMSAAD F, CHOUDHURY M, CHAUDHURI C R, *et al*. An innovative delay based algorithm to boost PUF security against machine learning attacks[C]. Industrial Electronics, Technology & Automation, Bridgeport City, USA, 2017: 1–6. doi: 10.1109/CT-IETA.2016.7868242.

[6] MAES R, HERREWEGE A V, and VERBAUWHEDE I. PUFKY: A fully functional PUF-based cryptographic key generator[C]. International Conference on Cryptographic Hardware and Embedded Systems, Leuven, Belgium, 2012: 302–319. doi: 10.1007/978-3-642-33027-8_18.

[7] LIU Weiqiang, YU Yifei, WANG Chenghua, *et al*. RO PUF design in FPGAs with new comparison strategies[C]. IEEE International Symposium on Circuits and Systems, Lisbon, Portugal, 2015: 77–80. doi: 10.1109/ISCAS.2015.7168574.

[8] KODYTEK F, LORENCZ R, BUCEK J, *et al*. Temperature dependence of ROPUF on FPGA[C]. Digital System Design, Limassol, Cyprus, 2016: 698–702. doi: 10.1109/DSD.2016.29.

[9] CHANG Hongliang and SACHIN S. Statistical timing analysis considering spatial correlation in a pert-like traversal[C]. International Conference on Computer Aided Design, San Jose, USA, 2003: 621–625. doi: 10.1109/ICCAD.2003.159746.

[10] HADDAD P, FISCHER V, BERNARD F, *et al*. A physical approach for stochastic modeling of TERO-based TRNG[C]. International Conference on Cryptographic Hardware and Embedded Systems, Saint-Malo, France, 2015: 357–372. doi: 10.1007/978-3-662-48324-4_18.

[11] 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. doi: 10.1109/JPROC.2014.2320516.

[12] KODYTEK F, LORENCZ R, and BUCEK J. Improved ring oscillator PUF on FPGA and its properties[J]. *Microprocessors & Microsystems*, 2016, 47(1): 55–63. doi: 10.1016/j.micpro.2016.02.005.

[13] RAHMAN M T, FORTE D, RAHMAN F, *et al*. A pair selection algorithm for robust RO-PUF against environmental variations and aging[C]. IEEE International Conference on Computer Design, New York, USA, 2015: 415–418. doi: 10.1109/ICCD.2015.7357137.

[14] RUHRMAIR U, SOLTER J, SEHNKE F, *et al*. PUF modeling attacks on simulated and silicon data[J]. *IEEE Transactions on Information Forensics & Security*, 2013, 8(11): 1876–1891. doi: 10.1109/TIFS.2013.2279798.

[15] 项群良, 张培勇, 欧阳冬生, 等. 多频率段物理不可克隆函数[J]. 电子与信息学报, 2012, 34(8): 2007–2012. doi: 10.3724/SP.J.1146.2011.01249.

XIANG Qunliang, ZHANG Peiyong, OUYANG Dongsheng, *et al*. An introduction to multi-frequency segment physical unclonable function[J]. *Journal of Electronics & Information Technology*, 2012, 34(8): 2007–2012. doi: 10.3724/SP.J.1146.2011.01249.

徐金甫：男，1965年生，教授，硕士生导师，研究方向为专业集成电路设计技术.

吴 缙：男，1994年生，硕士生，研究方向为专业集成电路设计技术.