利用震荡环频率特性提取多位可靠信息熵的物理不可克隆函数研究

孙子文*①② 叶 乔①
①(江南大学物联网工程学院 无锡 214122)
②(物联网技术应用教育部工程研究中心 无锡 214122)

摘 要：针对传统物理不可克隆函数(PUF)产生信息熵少、易受环境因素干扰等问题，该文设计一种产生多位稳定信息熵的PUF方案。该方案通过对FPGA上环形震荡器所产生频率数据的分析，从每个震荡环中提取能够代表震荡环特性的特征位作为信息熵。通过对逆变器温度特性的研究，利用电流饥饿逆变器和常规逆变器组成新的震荡环来降低温度对产生的信息熵的可靠性的影响。通过Cadence IC仿真和进行赛灵思zynq 7000系列FPGA开发平台上的实验，结果表明改进的PUF结构使用相同数量的震荡环产生更多的信息熵，并且其可靠性、唯一性均得到提升。

关键词：FPGA；物理不可克隆函数；环形震荡器；信息熵；逆变器
中图分类号：TN911.7; TP331 **文献标识码**：A **文章编号**：1009-5896(2021)01-0234-08
DOI: 10.11999/JEIT191013

Study on the Physical Unclonable Function of the Reliable Information Entropy Extracted by the Frequency Characteristic of Oscillating Ring

SUN Ziwen①② YE Qiao①
①(*School of Internet of Things, Jiangnan University, Wuxi* 214122, *China*)
②(*Engineering Research Center of Internet of Things Technology Applications Ministry of Education, Wuxi* 214122, *China*)

Abstract: Considering the problem of information entropy being low and easily disturbed by environmental factors in the traditional Physical Unclonable Function (PUF), a PUF scheme is designed to generate multiple stable information entropy. By analyzing the frequency data generated by the ring oscillator on the FPGA, the feature bits representing the characteristics of the ring are extracted from each ring as information entropy. By studying the temperature characteristics of the inverter, a new oscillating ring is formed by the current hungry inverter and the conventional inverter to reduce the influence of temperature on the reliability of the generated information entropy. Through Cadence IC simulation and experiments on zynq7000 series FPGA development platform, the results show that the improved PUF structure can generate more information entropy with the same number of oscillatory rings, and its reliability and uniqueness are improved.

Key words: FPGA; Physically Unclonable Function (PUF); Ring oscillator; Information entropy; Inverter

1 引言

随着物联网(Internet of Things, IoT)技术的发展，无线射频识别(Radio Frequency IDentification, RFID)技术也受到广泛关注[1]。其中，关于RFID用户隐私信息的安全问题已经引发消费者的重点关注。由于体积、资源、功耗等方面的限制，传统的高级加密标准、椭圆加密算法等加密算法应用于RFID时存在局限性[2]。物理不可克隆函数(Physically Unclonable Function, PUF)利用集成芯片制造工艺的差异，实现对不同的激励产生特定的激励响应对(Challenge Response Pairs, CRPs)[3]。作为一种轻量级的安全原语，PUF所产生的不可预测性的CRPs可有效地解决RFID、智能卡等物理实体的安全问题[4]。

围绕不同PUF产生机制的研究较为成熟。目前比较常见的PUF类型有：SRAM PUF[5]、触发器

收稿日期：2019-12-19；改回日期：2020-05-30；网络出版：2020-06-26
*通信作者： 孙子文 sunziwen@jiangnan.edu.cn
基金项目：国家自然科学基金(61373126)，江苏省自然科学基金(BK20131107)，中央高校基本科研业务费用专项资金(JUSRP51310A)
Foundation Items: The National Natural Science Foundation of China (61373126), The Natural Science Foundation of Jiangsu Province (BK20131107), The Special Funds for Basic Scientific Research Expenses of Central Universities (JUSRP51310A)

PUF[6]、锁存PUF[7]、蝴蝶PUF[8]、仲裁器PUF[9,10]、环形震荡器PUF (Ring-Oscillator PUF, RO PUF)[11–13]以及毛刺PUF[14]。其中，RO PUF相比较其他各种PUF，更容易在FPGA上进行布局实现，并且具有优良的性能，所以被广泛的使用[3]。RO PUF中比较有代表性的是Suh等人[11]提出的PUF方案，该方案拥有比较简单的熵评价标准并且很方便在FPGA上进行设计。

Suh等人[11]提出的RO PUF的原理通过比较两个随机选取的震荡环的频率值大小产生信息熵。这种方案每次一组环形震荡器只能产生1位信息熵，随着RO PUF需要生产的随机信息数量的增加，所消耗的资源也将成倍地增加[15]。同时，工作温度对频率的影响很大，当a震荡环在一个温度下比b震荡环频率高，而在另一个温度下比b震荡环频率低时，这种频率交叉变化会使这对环形震荡器产生的信息熵不可靠。ROPUF存在环形震荡器提取的信息熵数量少，以及信息熵的可靠性易受温度影响等问题。

为消除温度对PUF的信息熵可靠性的影响，Maiti等人[12]提出可配置的RO PUF(Configurable RO PUF, CRO PUF)。CRO PUF通过在FPGA上频率差异最大的区域布置CRO，然后选取一对CRO产生信息熵。此方法在一定程度上降低了温度的影响，不过在温度变化较大的情况下依然会存在比特跳变[16]，可靠性不能得到完全的保证。同时，为了选取频率差异较大的区域布置CRO，导致所能部署的CRO数量极大地减少，进而影响了CRO PUF一次所能产生随机数据的数量。因此，为了保证CRO PUF一次产生足够长的可靠的随机数据，解决一对CRO提取信息熵的数量少和震荡器易受温度的影响等问题仍然是关键。

为了解决RO PUF和CRO PUF方案存在的震荡环单元提取信息熵位数少、易受温度影响等问题，本文采用一种提取多位可靠信息熵的PUF方案ME-ROPUF(Muitibit Entropy RO PUF)。ME-ROPUF方案中，通过对FPGA中震荡环频率数据的分析，采用提取震荡环的频率特征位产生信息熵的方法来替代RO PUF比较频率大小产生信息熵的方法，有效地提高PUF产生信息熵的数量；此外，通过对逆变器时延受温度影响的分析，ME-ROPUF方案中环形震荡器采用由电流饥饿逆变器[17]和传统逆变器组成的混合可配置环形震荡器(Hybrid CRO, HCRO)[16]单元,从而减小温度对环形震荡器频率的影响，降低不同温度下PUF信息熵的跳变率,提高ME-ROPUF的可靠性。

2　PUF方案改进的理论基础

ME-ROPUF采用提取多位信息熵方法以及HCRO单元产生多位可靠信息熵，其中，提取多位信息熵方法是基于对FPGA震荡环特征的研究，而HCRO是基于对逆变器温度特性的研究。

2.1　震荡环的频率特征

环形震荡器在FPGA上是由同构的硬宏单元组成，但由于集成芯片制造工艺的差异，环形震荡器的时延会有一定的差异[17]。结合Maiti等人[12]提出的震荡环的时延模型，并且将时延数据转化成频率时，其转化过程会存在偏斜效应[18]，这种偏斜效应会使在同一制造工艺、同一位置的环形震荡器多次测量的频率存在偏差。那么，环形震荡器的频率组成成分表示为式(1)

$$f_{\mathrm{Loop}} = f_{\mathrm{avg}} + f_{\mathrm{various}} + f_{\mathrm{convert}} \tag{1}$$

其中，f_{Loop}表示震荡环的频率，f_{avg}表示同构震荡环的标准频率，f_{various}表示制造工艺产生的随机频率，f_{convert}表示由延迟模拟量转化位数字量时的偏斜差异所产生的偏斜频率。在FPGA上，相邻震荡环频率受空间布局的影响最小[12]，选取5个相邻震荡环，每个震荡环200次测量的频率分布如图1所示。

图1中同一曲线表示同一环形震荡器200次测量的频率分布，不同的曲线表示不同环形震荡器的频率分布。从图1可知，f_{Loop}中f_{convert}分量和f_{various}分量影响频率的范围不同，采用量级$2^i(i=0, 1, \cdots, 23)$定量描述各频率分量对f_{Loop}的影响程度，如当$f_{\mathrm{convert}}<2^i$时，只会影响前i位二进制数据。震荡环的偏斜频率所能影响的位数较少，而随机频率所能影响的位数较多，采用式(2)和式(3)表示两种影响之间的关系

$$f_{\mathrm{convert}} < 2^{\mathrm{low}},\ \mathrm{low} \in (0, 23) \tag{2}$$

$$2^{\mathrm{low}} < f_{\mathrm{various}} < 2^{\mathrm{high}},\ \mathrm{high} \in (0, 23) \tag{3}$$

当所有震荡环的f_{various}, f_{convert}都满足式(2)和式(3)时，对于同一环形震荡器的频率f_{Loop}具有相

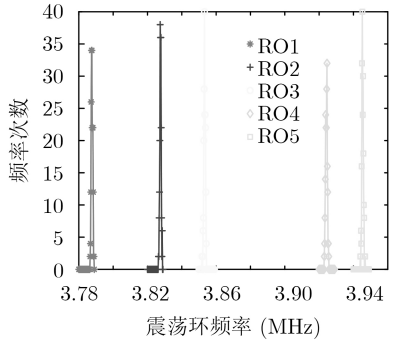

图 1 不同RO的频率分布图

同的f_{various}分量，其频率差异来自于f_{convert}分量，即同一环形震荡器多次测量的频率二进制数据在(low, 23)之间的数据操持不变；而对于不同的震荡环的频率f_{Loop}具有不同的f_{various}分量，其频率差异主要来自于f_{various}分量，即不同环形震荡器多次测量的频率二进制数据在(high, 23)之间的数据保持不变。所以，对于同一环形震荡器(low, high)之间的数据多次测量保持不变，不同环形震荡器(low, high)之间的数据多次测量会变化，即每个环形震荡器(low, high)之间的数据唯一。

2.2 逆变器的温度特性

环形震荡器的时延取决于震荡器中逆变器的时延t_{d}[19]，由式(4)表示

$$t_{\text{d}} = \frac{C_{\text{o}} V_{\text{dd}}}{\eta I_{\text{DS}}} \tag{4}$$

其中，C_{o}是逆变器的总电容，V_{dd}是逆变器的电源电压，ηI_{DS}是逆变器的均值电流，η是逆变器的一个固定常数，I_{DS}是逆变器中MOS管的漏极电流。

当MOS管处于饱和区时，MOS管的漏极电流与阈值电压、反转层电荷迁移率的关系如式(5)[20]

$$I_{\text{DS, sat}} = \frac{\mu W C_{\text{ox}}}{2L} \left(V_{\text{GS}} - V_{\text{th}}\right) \tag{5}$$

其中，C_{ox}表示MOS管的栅极电容，W, L分别表示MOS管的有效通道的长和宽，阈值电压V_{th}和反转层电荷迁移率$\boldsymbol{\mu}$随温度的变换如式(6)和式(7)所示[20]

$$V_{\text{th}}(T) = V_{\text{th0}} + \sigma (T - T_0) \tag{6}$$

$$\mu = \mu_0 \left(\frac{T_0}{T}\right)^b \tag{7}$$

其中，T, T_0分别表示当前温度和参考温度，V_{th0}, μ_0分别表示在参考温度下的阈值电压和反转层电荷迁移率，σ表示阈值温度系数，b表示反转层电荷迁移率温度系数。

由式(5)—式(7)，得出MOS管处于饱和区时的漏极电流的温度系数TCC_{sat}如式(8)所示

$$\text{TCC}_{\text{sat}} = \frac{1}{I_{\text{DS, sat}}} \frac{\text{d}I_{\text{DS, sat}}}{\text{d}T} = \frac{1}{\mu}\frac{\text{d}\mu}{\text{d}T} - \frac{2}{V_{\text{GS}} - V_{\text{th}}} \frac{\text{d}V_{\text{th}}}{\text{d}T} \tag{8}$$

此时，$\text{d}V_{\text{th}}/\text{d}T > 0$，而$\text{d}\mu/\text{d}T < 0$，因此$\text{TCC}_{\text{sat}} < 0$，即MOS管的电流与温度呈负相关。

当MOS管处于截止区域时，其漏极电流与阈值电压、反转层电荷迁移率的关系为[20]

$$I_{\text{DS, sub}} = \frac{\mu W C_{\text{ox}}}{L} \left(\frac{K_{\text{B}} T}{q}\right)^2 \frac{C_{\text{s}} + C_{\text{it}}}{C_{\text{ox}}} \text{e}^{\frac{q}{nK_{\text{B}}T}(V_{\text{GS}} - V_{\text{th}})} \cdot \left(1 - \text{e}^{-\frac{qV_{\text{GS}}}{K_{\text{B}}T}}\right) \tag{9}$$

其中，K_{B}是温度常数，q是反转层电荷数，C_{s}为半导体电容，C_{it}是通道电容，V_{GS}表示栅极到源极的电压。

结合式(6)、式(7)、式(9)可得出MOS管处于截止区时的漏极电流的温度系数TCC_{sub}

$$\text{TCC}_{\text{sub}} = \frac{1}{I_{\text{DS, sub}}} \frac{\text{d}I_{\text{DS, sub}}}{\text{d}T} = \frac{1}{\mu}\frac{\text{d}\mu}{\text{d}T} + \frac{2}{T} + \frac{q}{nK_{\text{B}}T} \cdot \left(\frac{\text{d}V_{\text{th}}}{\text{d}T} - \frac{V_{\text{GS}} - V_{\text{th}}}{T}\right) \tag{10}$$

此时，阈值电压受温度影响成为主要的影响因素，TCC_{sub}是一个正值，即漏极电流与温度呈正相关。

由于MOS管处于不同区域时，漏极电流与温度的关系呈现相反的状态，这就为构建一种能够降低温度影响的环形震荡器提供了可能。

3 ME-ROPUF方案

ME-RO PUF整体结构如图2，主要由8个5阶的HCRO单元、9个24位计数器和一个特征位提取器组成，其中特征位提取器实现的功能是从24位频率数据中选出指定的几位数据。ME-ROPUF的激励数据作为激励信号配置5阶的HCRO单元，计数器和HCRO单元受到触发信号开始工作。当计数器1的计数值达到参考值时所有计数器停止计数，然后特征位提取器从计数器2～9所产生的24位二进制频率数据中分别选取频率特征位区域组成响应数据输出。

ME-ROPUF为了降低温度对环形震荡器频率的影响，使用HCRO单元产生震荡频率；为了提高从环形震荡器中提取多位信息熵，采用提取频率特征位的方法产生信息熵。

3.1 HCRO结构

环形震荡器的时延主要取决于组成环形震荡器的逆变器的时延，由于逆变器的时延会受到温度的影响，所以环形震荡器的频率也会受到温度影响。常规逆变器的MOS管是工作于饱和区，逆变器的时延与温度呈现正相关变化。为了降低温度对环形震荡器频率的影响，可根据电流饥饿逆变器的MOS管是工作在截止区且其时延与温度呈现负相关变化的特性，将环形震荡器的部分常规逆变器替换成电流饥饿逆变器。饥饿逆变器和常规逆变器组成的HCRO单元的结构如图3所示。

电流饥饿逆变器是在常规逆变器上下分别增加1个PMOS管和1个NMOS管，通过偏置电压V_{p}和V_{n}使图4中逆变器的MOS管工作于截止区域。

采用cadence virtuoso中spectrure环境进行蒙特卡洛仿真，比较了常规逆变器CRO、电流饥饿逆

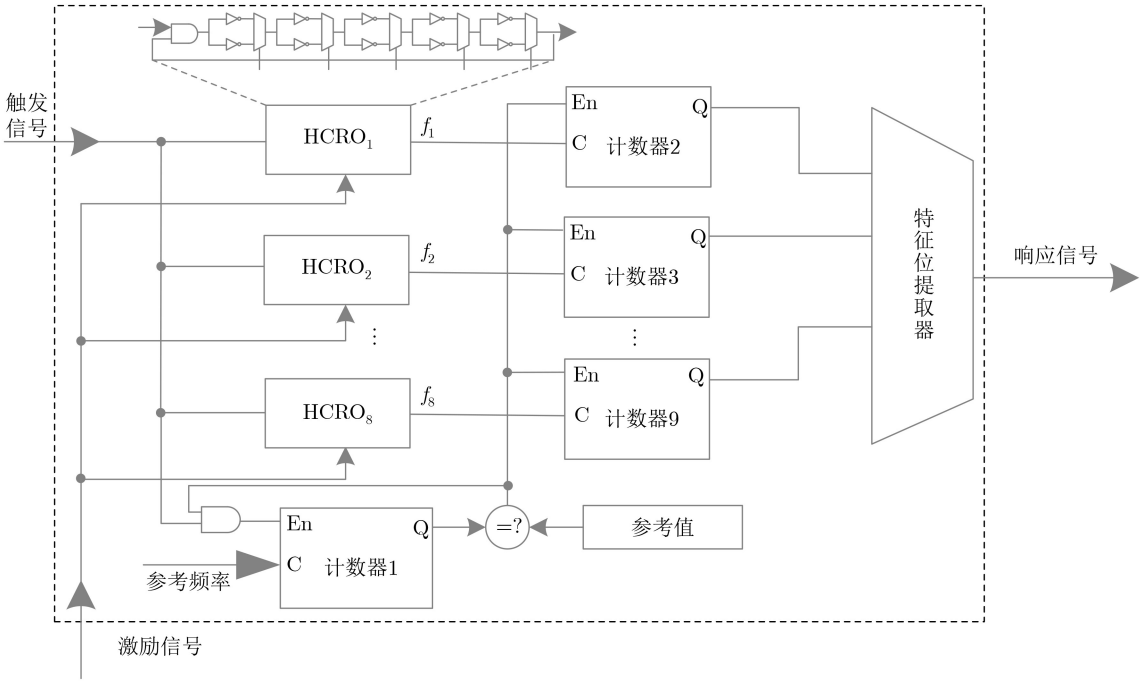

图 2 ME-ROPUF整体框图

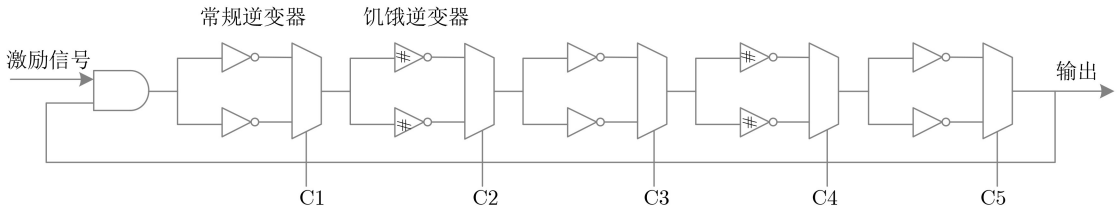

图 3 HCRO结构

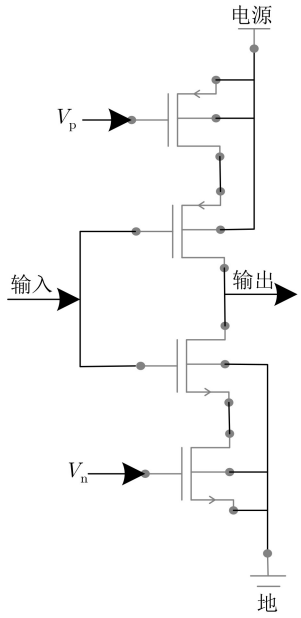

图 4 电流饥饿逆变器

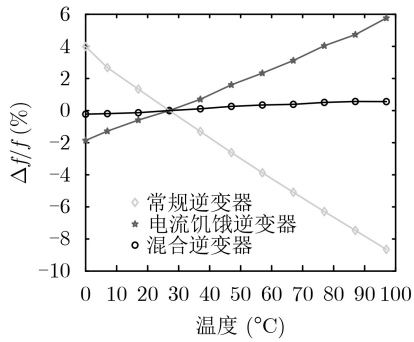

图 5 3种震荡环频率随温度变化图

变器CRO与HCRO的频率受温度影响的变化情况，如图5所示。由图5可知，以27°C作为参考温度，常规逆变器CRO单元所产生的频率随温度升高而减小，电流饥饿逆变器CRO单元所产生的的频率随温度的升高而升高，而由常规逆变器和电流饥饿逆变器组成的HCRO单元所产生的频率基本不会受温度的影响，因此采用HCRO单元的PUF结构拥有很好的抗温度特性。相比较常规逆变器CRO单元和电流饥饿逆变器CRO单元，ME-ROPUF所采用的HCRO单元所受到温度的影响更小，HCRO单元所产生的频率受温度影响的位数处于(0, low)区域，不影响ME-ROPUF所提取的特征位数据，提高ME-ROPUF产生信息熵的可靠性。

3.2 特征位的选取方法

选取合适的特征位是提取多位信息熵的关键。结合式(2)和式(3)，震荡环的f_{convert}分量所影响的频率位区域为(0, low)，即同一震荡环多次测量的(low, 24)区域的频率数据稳定性高；而震荡环的f_{various}分量所影响的频率位数为(0, high)，即不同震荡环的(0, high)区域频率数据随机性大。为了选取代表震荡环频率特性的区域，需要消除f_{convert}分量的影响，体现f_{various}分量的影响，即选取位稳定性高于S_{low}并且位随机性高于R_{high}的区域(low, high)。其选取过程分为两步：特征位预选区域的选择和特征位区域的确定。

3.2.1 特征位预选区域的选择

第1步，计算ME-ROPUF的位稳定性S_i和位随机性R_i，根据所求的S_i和R_i选取几个预选区域(low', high')。震荡环的位稳定性S_i(RO)是衡量同一震荡环多次测量中每位频率数据稳定程度的指标，表示为

$$S_i(\text{RO}) = \begin{cases} P_{\text{S}}(b_i=1), & P_{\text{S}}(b_i=1) \geq 0.5 \\ 1-P_{\text{S}}(b_i=1), & P_{\text{S}}(b_i=1) < 0.5 \end{cases} \tag{11}$$

$$P_{\text{S}}(b_i=1) = \frac{1}{k}\sum_{j=1}^{k} b_{j,i} \tag{12}$$

其中，$P_{\text{S}}(b_i=1)$表示k次测量中第i位频率数据为1的概率，$b_{j,i}$表示第j次测试所产生的第i位频率数据。

为了保证所求的位稳定性符合所有震荡环，求所有震荡环的位稳定性的均值作为ME-ROPUF的位稳定性S_i, n个震荡环所产生的频率数据第i位的稳定性S_i计算式(13)为

$$S_i = \frac{1}{n}\sum_{m=1}^{n} S_i(\text{RO}_m) \tag{13}$$

震荡环的位随机性R_i(RO)是衡量一次测量中不同震荡环每位频率数据的变化程度的指标，表示为

$$R_i(\text{RO}) = \begin{cases} 1-P_{\text{R}}(b_i=1), & P_{\text{R}}(b_i=1) \geq 0.5 \\ P_{\text{R}}(b_i=1), & P_{\text{R}}(b_i=1) < 0.5 \end{cases} \tag{14}$$

$$P_{\text{R}}(b_i=1) = \sum_{m=1}^{n} b_{m,i} \tag{15}$$

其中，$P_{\text{R}}(b_i=1)$表示n个震荡环第i位频率数据等于1的概率，$b_{m,i}$表示第m个震荡环所产生的第i位。

为了保证所求的位随机性更准确，求k次测量的震荡环位随机性的均值作为ME-ROPUF的位随机性，R_i，计算公式为

$$R_i = \frac{1}{k}\sum_{j=1}^{k} R_{j,i}(\text{RO}) \tag{16}$$

计算得到S_i和R_i，选取S_i>0.990以及R_i>0.490的区域[21]作为预选区域。由于震荡环特征位区域的选取会影响到PUF的可靠性、唯一性以及均匀性，所以对预选特征位区域进行预实验选取准确的特征位区域。

3.2.2 准确特征位区域的确定

第2步，对各预选区域进行预实验，结合PUF的可靠性、唯一性及均匀性，选取准确的特征位区域(low, high)。其中，可靠性S_{puf}衡量的是在不同的操作条件下PUF的CRPs的重现性或稳定性，表示为

$$S_{\text{puf}} = 1 - \frac{1}{k}\sum_{x=1}^{k}\frac{\text{HD}(C_0, C_x)}{l} \times 100\% \tag{17}$$

其中，k表示同一激励下测量的次数，l表示响应数据的位数，C_0是从多次测量的数据中选取的参考响应数据，C_x是第x次测量的响应数据，HD()为两串二进制码的汉明距离。

唯一性U_{puf}是描述不同PUF在相同激励和环境下所产生响应数据的区分度的指标，表示为

$$U_{\text{puf}} = \frac{2}{N(N-1)}\sum_{u=1}^{N-1}\sum_{v=u+1}^{N}\frac{\text{HD}(C_u, C_v)}{l} \times 100\% \tag{18}$$

其中，N表示PUF实例的个数，C_u, C_v分别表示第u个和第v个PUF实例所产生的响应数据。

均匀性R_{puf}是衡量不同激励下PUF所产生响应数据的0,1分布均匀程度，表示为

$$R_{\text{puf}} = \frac{1}{k}\sum_{j=1}^{k}\sum_{i=1}^{n}\frac{b_{j.i}}{l} \tag{19}$$

其中，k表示不同激励数据的测量次数，l表示响应数据的位数，$b_{j.i}$表示第j次测量下第i位响应数据，通过实验发现，当R_{puf}>0.45时，RO PUF具有好的安全性能。

通过对各预选区域进行小规模的实验计算对应的PUF的可靠性S_{puf}、唯一性U_{puf}以及均匀性R_{puf}，然后计算各预选区域的可靠性和唯一性的均值V_{puf}

$$V_{\text{puf}} = 0.5 \times S_{\text{puf}} + 0.5 \times U_{\text{puf}} \tag{20}$$

选择预选区域中V_{puf}最大且R_{puf}>0.45的区域作为准确的特征区域(low, high)。

4 仿真与实验

基于仿真和实验两个层面，对本文采用的方法的有效性从不同的角度进行了验证和分析。在linux系统下，采用cadence virtuoso中spectrure环境进行蒙特卡洛仿真，用于验证采用HCRO单元的

ME-ROPUF结构的可靠性；使用赛灵思synq7000系列的FPGA开发板，进一步通过实验验证ME-ROPUF提取信息熵方法的有效性以及所提取信息熵的唯一性和均匀性。

4.1 仿真和实验环境介绍

linux系统下的仿真的器件工艺库选择的是TSMC0.18 μm, 1.8 V CMOS工艺库。实验使用verilog语言进行PUF结构设计，为了防止电路被优化，采用xilinx官方提供的原语操作和XDC Macro技术在FPGA的SLICEL逻辑单元中配置LUT单元和数据选择器组成震荡环，每个震荡环采用9个LUT和4个数据选择器，具体的布局如图6所示。采用vivado自带的ila逻辑分析仪对实验数据进行辅助分析。

4.2 实验和仿真结果分析

整个实验和仿真用来验证ME-ROPUF提取信息熵方法的有效性以及对ME-ROPUF的可靠性、唯一性和均匀性的分析。

4.2.1 ME-ROPUF提取信息熵方法的有效性

在27°环境温度下，在FPGA上对ME-ROPUF提取信息熵方法进行验证。ME-ROPUF产生信息熵的方法是选取准确的频率特征位，选取准确的震荡环特征位分为两步。第1步，根据式(13)和式(16)求得震荡环的S_i和R_i的分布如图7所示，满足S_i>0.990且R_i>0.490条件的预选区域为(13, 17)的各子区域。第2步，根据式(17)—式(20)计算不同预选区域对应的S_{puf}, U_{puf}, R_{puf}以及V_{puf}，结果如表1所示。

由表1可知，(14, 17)的V_{puf}最大且R_{puf}>0.45，所以选取(14, 17)作为ME-ROPUF的特征位区域，即ME-ROPUF每个震荡环产生4位信息熵。而RO PUF使用两个震荡环进行比较频率大小产生1位信息熵，故ME-ROPUF使用相同的LUT资源得到ROPUF8倍的信息熵。

4.2.2 ME-ROPUF的可靠性

采用cadence virtuoso中spectrure环境进行蒙特卡洛仿真ME-ROPUF的可靠性，并与ROPUF[11], CROPUF[12]、使用CRO单元的ME-ROPUF以及使用HCRO单元的ME-ROPUF的可靠性进行了对比。根据式(17)—式(20)，以室温27°为参考温度，仿真了实验温度在0°～100°范围内变化过程中ME-ROPUF的可靠性，其结果如图8所示。由图8可知，采用HCRO单元的ME-ROPUF方案的可靠性在98.062%～99.592%之间浮动，而RO PUF, CRO PUF以及采用CRO的ME-ROPUF方案的可靠性分别在95.017%～98.142%, 96.121%～98.768%和95.809%～99.542%之间浮动。使用HCRO单元的ME-ROPUF方案的可靠性明显高于采用CRO单元的可靠性；可靠性随温度变化的浮动程度也明显小于RO PUF, CRO PUF以及采用CRO的ME-ROPUF方案，表明采用HCRO单元的ME-ROPUF方案能有效降低温度对可靠性的影响。

4.2.3 ME-ROPUF的唯一性和均匀性

采用FPGA实验对ME-ORPUF的唯一性和均匀性进行性能验证，并与ROPUF[11], CRO PUF[12]和使用CRO的ME-ROPUF的唯一性和均匀性进行了对比实验，实验在27°下进行，结果如图9所示。由图9可知，ME-ROPUF的唯一性在49.897%～50.176%之间浮动，均匀性在46.290%～48.378%之间浮动，而RO PUF, CRO PUF以及采用CRO的

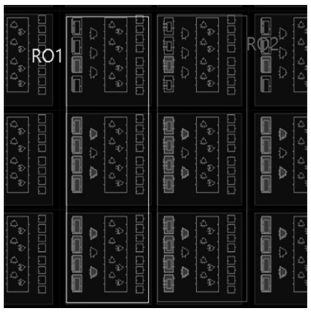

图 6 震荡环在FPGA上的布局图

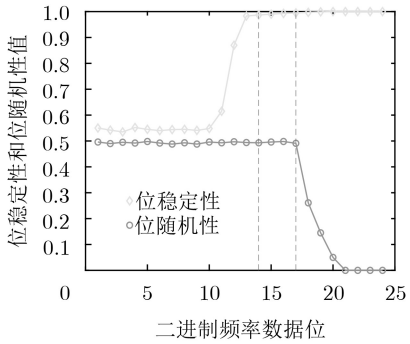

图 7 位稳定性和位随机性分布图

表 1 预选区域性能指标

预选区域	(13, 17)	(14, 17)	(15, 17)	(16, 17)	(13, 16)	(14, 16)	(15, 16)	(13, 15)	(14, 15)
S_{puf}	0.963	0.989	0.986	0.991	0.974	0.982	0.990	0.979	0.981
U_{puf}	0.474	0.492	0.488	0.489	0.482	0.486	0.485	0.487	0.491
R_{puf}	0.464	0.474	0.485	0.476	0.478	0.489	0.481	0.492	0.486
V_{puf}	0.719	0.741	0.737	0.740	0.728	0.734	0.738	0.733	0.736

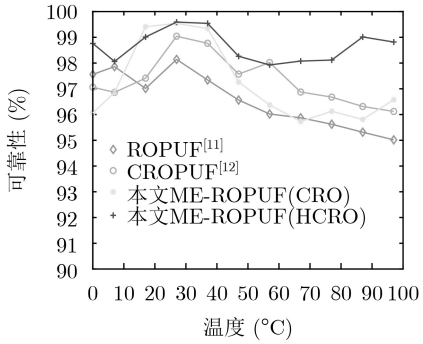

图 8 PUF的可靠性

ME-ROPUF方案的唯一性分别在49.621%～50.369%, 49.604%～50.274%和49.752%～50.238%之间浮动，均匀性分别在46.395%～47.807%, 46.959%～47.809%和46.086%～48.936%之间浮动。表明相对于其他几种方案，ME-ROPUF方案的唯一性都得到了改善，均匀性相差不大。

5 结束语

ROPUF作为一种可靠的硬件加密原语，为低功耗设备不适合使用传统的加密方法提出新的解决方案。但是ROPUF易受到温度的影响且震荡环所产生的信息熵数量少。本文采用的ME-ROPUF方案采用提取震荡环特征位的方法来提取更多信息熵，并采用HCRO单元来降低温度对震荡环频率的影响，从而能够有效的提高PUF的可靠性、唯一性以及信息熵数量。ME-RO PUF可靠性提升到98.062%以上，唯一性在49.621%～50.369%浮动，相同的LUT资源得到8倍的RO PUF信息熵。

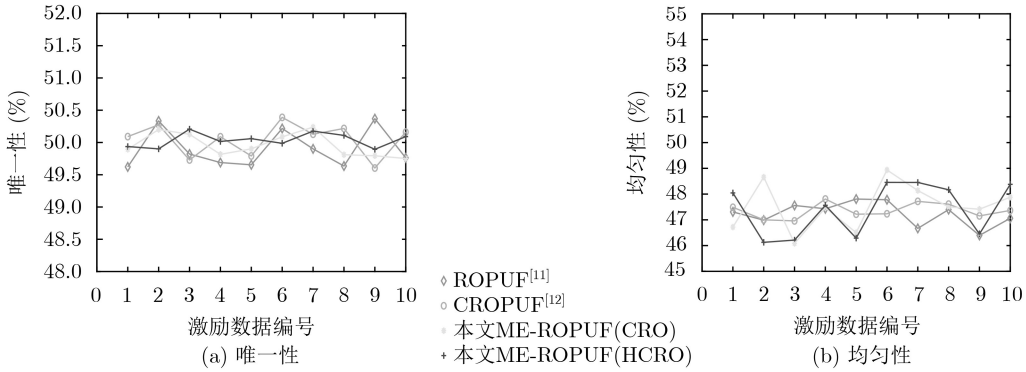

图 9 PUF的唯一性和均匀性

参 考 文 献

[1] SAHOO S R, KUMAR K S, and MAHAPATRA K. A novel current controlled configurable RO PUF with improved security metrics[J]. *Integration*, 2017, 58: 401–410. doi: 10.1016/j.vlsi.2016.11.005.

[2] SANKARAN S, SHIVSHANKAR S, NIMMY K, *et al*. LHPUF: Lightweight hybrid PUF for enhanced security in internet of things[C]. 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), Hyderabad, India, 2018: 175–178. doi: 10.1109/iSES.2018.00066.

[3] GASSEND B, CLARKE D, VAN DIJK M, *et al*. Silicon physical random functions[C]. The 9th ACM Conference on Computer and Communications Security, Washington, USA, 2002. doi: 10.1145/586110.586132.

[4] 张跃军, 王佳伟, 潘钊, 等. 基于正交混淆的多硬件IP核安全防护设计[J]. 电子与信息学报, 2019, 41(8): 1847–1854. doi: 10.11999/JEIT180898.

ZHANG Yuejun, WANG Jiawei, PAN Zhao, *et al*. Hardware security for multi IPs protection based on orthogonal obfuscation[J]. *Journal of Electronics & Information Technology*, 2019, 41(8): 1847–1854. doi: 10.11999/JEIT180898.

[5] GAO Yansong, SU Yang, YANG Wei, *et al*. Building secure SRAM PUF key generators on resource constrained devices[C]. 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 2019: 912–917. doi: 10.1109/PERCOMW.2019.8730781.

[6] KUMAR A, MISHRA R S, and KASHWAN K R. Challenge-response generation using RO-PUF with reduced hardware[C]. 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 2016: 1305–1308. doi: 10.1109/ICACCI.2016.7732227.

[7] SU Ying, HOLLEMAN J, OTIS B P, *et al*. A digital 1.6 pJ/bit chip identification circuit using process variations[J]. *IEEE Journal of Solid-State Circuits*, 2008, 43(1): 69–77. doi: 10.1109/JSSC.2007.910961.

[8] KUMAR S S, GUAJARDO J, MAES R, *et al*. Extended abstract: The butterfly PUF protecting IP on every FPGA[C]. 2008 IEEE International Workshop on Hardware-

Oriented Security and Trust, Anaheim, USA, 2008: 67–70. doi: 10.1109/HST.2008.4559053.

[9] LEE J W, LIM D, GASSEND B, *et al*. A technique to build a secret key in integrated circuits for identification and authentication applications[C]. 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525), Honolulu, USA, 2004: 176–179. doi: 10.1109/VLSIC.2004.1346548.

[10] LIM D, LEE J W, GASSEND B, *et al*. Extracting secret keys from integrated circuits[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2005, 13(10): 1200–1205. doi: 10.1109/TVLSI.2005.859470.

[11] SUH G E and DEVADAS S. Physical unclonable functions for device authentication and secret key generation[C]. The 44th ACM/IEEE Design Automation Conference, San Diego, USA, 2007: 9–14.

[12] MAITI A and SCHAUMONT P. Improved ring oscillator PUF: An FPGA-friendly secure primitive[J]. *Journal of Cryptology*, 2011, 24(2): 375–397. doi: 10.1007/s00145-010-9088-4.

[13] CHEN B and WILLEMS F M J. Secret key generation over biased physical unclonable functions with polar codes[J]. *IEEE Internet of Things Journal*, 2019, 6(1): 435–445. doi: 10.1109/JIOT.2018.2864594.

[14] SUZUKI D and SHIMIZU K. The glitch PUF: A new Delay-PUF architecture exploiting glitch shapes[C]. The 12th International Workshop Cryptographic Hardware and Embedded Systems, Santa Barbara, USA, 2010: 366–382. doi: 10.1007/978-3-642-15031-9_25.

[15] USMANI M A, KESHAVARZ S, MATTHEWS E, *et al*. Efficient PUF-Based key generation in FPGAs using per-device configuration[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2019, 27(2): 364–375. doi: 10.1109/TVLSI.2018.2877438.

[16] CAO Yuan, ZHANG Le, CHEN Shoushun, *et al*. A low-power hybrid RO PUF with improved thermal stability for lightweight applications[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2015, 34(7): 1143–1147. doi: 10.1109/tcad.2015.2424955.

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

[18] 徐金甫, 吴缙. 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[J]. 电子与信息学报, 2019, 41(3): 717–724. doi: 10.11999/JEIT180405.

XU Jinfu and WU Jin. Frequency sorting algorithm based on dynamic ring oscillator physical unclonable function statistical model[J]. *Journal of Electronics & Information Technology*, 2019, 41(3): 717–724. doi: 10.11999/JEIT180405.

[19] KUMAR R, PATIL V C, and KUNDU S. On design of temperature invariant physically unclonable functions based on ring oscillators[C]. 2012 IEEE Computer Society Annual Symposium on VLSI, Amherst, USA, 2012: 165–170. doi: 10.1109/ISVLSI.2012.66.

[20] SOCHER E, BEER S M, and NEMIROVSKY Y. Temperature sensitivity of SOI-CMOS transistors for use in uncooled thermal sensing[J]. *IEEE Transactions on Electron Devices*, 2005, 52(12): 2784–2790. doi: 10.1109/TED.2005.859664.

[21] KODÝTEK F, LÓRENCZ R, and BUČEK J. Improved ring oscillator PUF on FPGA and its properties[J]. *Microprocessors and Microsystems*, 2016, 47: 55–63. doi: 10.1016/j.micpro.2016.02.005.

孙子文：女，1968年生，博士，教授，研究方向为模式识别、人工智能、无线传感网络理论与技术、信息安全.

叶　乔：男，1995年生，硕士生，研究方向为物理不可克隆函数及无线射频识别技术等.

责任编辑：余　蓉