SDL PUF：高可靠自适应偏差锁定PUF电路

张 源 罗静茹 张吉良*
(湖南大学半导体学院(集成电路学院) 长沙 410000)

摘 要：物理不可克隆函数(Physical Unclonable Function, PUF)作为一种新的硬件安全原语，通过提取工艺偏差产生唯一的响应序列为计算系统提供可信根。然而现有基于现场可编辑门阵列(Field Programmable Gate Array, FPGA)的PUF难以在较宽的温度和电压范围内实现高可靠性。该文提出一种基于自定时环(Self-Timed Ring，STR)的自适应偏差锁定PUF(Self-adaption Deviation Locking PUF, SDL PUF)，首先利用STR延迟引起的振荡频率差产生PUF响应；然后通过在初始化阶段自适应配置，有效扩大STR环内的事件到达时间偏差，从而显著提高PUF的可靠性；最后进一步提出一种对比混淆策略，通过提取工艺偏差自动生成随机比特配置并混淆比较器，以抵抗侧信道攻击。在Xilinx Virtex-6 FPGA上实验结果表明， SDL PUF在0～80°C的温度范围和0.85～1.15V的电压范围内误码率为0， 唯一性和均匀性分别为49.29%和49.84%。

关键词：物理不可克隆函数；自定时环；FPGA；可靠性
中图分类号：TN402 **文献标识码**：A **文章编号**：1009-5896(2024)05-2274-07
DOI: 10.11999/JEIT231313

SDL PUF: A High Reliability Self-Adaption Deviation Locking PUF

ZHANG Yuan LUO Jingru ZHANG Jiliang
(*College of Semiconductors* (*College of Integrated Circuits*), *Hunan University*, *Changsha* 410000, *China*)

Abstract: As a novel hardware security primitive, Physical Unclonable Function (PUF) extracts process deviations to generate a unique response sequence, providing a root of trust for computing systems. However, existing PUFs based on Field Programmable Gate Arrays (FPGAs) cannot maintain high reliability over a wide range of temperatures and voltages. In this work, we propose a Self-Timed Ring (STR) based Self-adaption Deviation Locking PUF (SDL PUF). Firstly, the PUF response is generated utilizing the oscillation frequency difference caused by the STR delay. Secondly, the adaptive configuration in the initialization stage can effectively expand the deviation of the event arrival time in the STR, substantially enhancing the reliability of PUF. Finally, a comparator obfuscation strategy is proposed, automatically configuring the comparator by extracting the process deviation to resist the side-channel attack. The proposed structure is implemented on a Xilinx Virtex-6 FPGA. Experimental results show that the proposed SDL PUF achieves 0 bit error rate in the temperature range of 0°C～80°C and the voltage range of 0.85～1.15V, and ensures 49.29% uniqueness and 49.84% uniformity while maintaining high reliability.

Key words: Physical unclonable function; Self-timed ring; FPGA; Reliability

1 引言

物联网是继计算机、互联网和移动通信之后又一新的信息科学技术，并已深入到工业生产、家居生活以及军事国防等各个方面。根据IHS预测[1]，全球物联网设备的安装基数将从2015年的154亿增长到2020年的307亿，2025年这一数字更将达到754亿。

在物联网早期阶段，人们更关注基础理论和应用研究，然而随着物联网的迅猛发展，安全问题得以凸显，引起了人们的高度重视。到2025年，全球物联网安全市场规模预计将达到98.8亿美元，在预测期内以29.7%的复合年增长率发展[2]。安全问题已成为制约物联网可持续发展的核心问题之一。在物联网安全中，密钥和认证是其两大核心关键技术[3]。密钥系统是安全的基础，是实现感知信息隐私保护的手段之一。认证则是物联网安全中最直接

收稿日期：2023-11-29；改回日期：2024-05-21；网络出版：2024-05-23
*通信作者： 张吉良 zhangjiliang@hnu.edu.cn
基金项目：国家自然科学基金(U20A20202, 62122023)
Foundation Items: The National Natural Science Foundation of China(U20A20202, 62122023)

也是最前沿的一道防线。传统的安全机制将密钥存储在电可擦写可编程只读存储器(Electrically Erasable Programmable Read Only Memory, EEPROM)或电池供电的非易失性静态随机存储器(Static Random Access Memory, SRAM)中，结合以密码学为理论基础的加密算法，实现信息加解密和身份认证。但是物联网设备资源通常有限，比如计算能力弱、存储资源小和能耗有限。传统的密钥生成和认证技术很难适用于资源受限的物联网环境，因此开发新的轻量级密钥生成和设备认证机制成为当前物联网安全研究的热点。

物理不可克隆函数(Physical Unclonable Function, PUF)作为一种新型轻量级硬件安全原语，已受到学术界与工业界的广泛研究[4–7]。从技术角度看，现场可编程门阵列(Field Programmable Gate Array, FPGA)已经成为热门的主流集成平台，与专用集成电路(Application-Specific Integrated Circuits, ASIC)相比，FPGA 成本更低且更为灵活，并且基于FPGA的PUF具有高唯一性、低开销和灵活性等优势。然而， FPGA PUF的输出容易受到温度、电压和老化等因素的影响[8–10]，可靠性问题已成为制约其产业化最重要的问题之一。

为了提高基于FPGA PUF的可靠性，文献[8]提出了一种基于NAND SR锁存器的PUF结构，通过将SR锁存器的配置和复位信号均置0来激励完全对称的电路，以生成PUF响应，该结构资源开销较低，在标准工作环境下实现了良好的唯一性和可靠性，但当电压和温度发生变化时，可靠性会显著降低。文献[9]提出了一种基于FPGA的RO PUF，该结构通过LUT的自比较改善唯一性，同时提出一种实时测量响应稳定性的自适应计数器时间周期调优方案提高其可靠性。但随着工作温度的升高，其可靠性仍会出现大幅波动。文献[10] 提出了一种基于FPGA中XOR门的轻量级RO PUF，利用两个交叉耦合的XOR门在单个可配置逻辑块(Configurable Logic Block, CLB)中实现4个PUF响应位，但此结构的可靠性对于电压变化较为敏感。文献[11]提出一种基于动态可寻址移位寄存器的可调PUF设计，通过调整移位寄存器的参数，可以调整PUF内部的信号延迟，从而在不同环境下生成可靠PUF响应，但该设计会产生额外硬件开销，且在高温环境中可靠性下降明显。上述工作均无法在宽温度和电压范围内保持高可靠性。

本文提出一种基于自定时环(Self-Timed Ring, STR)的PUF结构(Self-adaption Deviation Locking PUF, SDL PUF)，能够在初始化阶段自适应地配置STR的状态，显著偏移由制造工艺导致的频率差，从而有效提高其在温度、电压等环境条件变化下的可靠性。本文贡献如下：

(1) 提出一种基于STR的PUF方案，通过提取STR内由工艺偏差引起的事件到达时间差生成PUF响应，同时给出了可靠性提升的相关原理分析。

(2) 基于STR PUF提出一种能够自适应重配置的高可靠性SDL PUF，通过对每个环的事件到达时间进行自适应配置，从而显著提升不同工作环境下的PUF可靠性。

(3) 提出一种对比混淆方案，通过提取特定工艺偏差，为每一对STR提供独特的比较策略以抵抗侧信道攻击，并对其效果进行了理论分析。

(4) 在Xilinx Virtex-6 FPGA上实现了SDL PUF，响应结果分别获得了49.29%的唯一性以及49.84%的均匀性，并且在0.85～1.15V电压范围和0°C～80°C温度范围内实现0误码，具有良好唯一性和均匀性的同时表现出对环境变化的高度可靠性。

2　预备知识

2.1　基于延迟的PUF

由于工艺偏差的影响，延迟型PUF利用脉冲信号在电路中传播速度的不同而生成唯一响应。该类PUF可靠性高且更为灵活，如仲裁器PUF(Arbiter-PUF, APUF)[12,13]、毛刺 PUF(Glitch-PUF)[14] 、环形振荡器(Ring Oscillator, RO)PUF[15–18]，适用于物联网或嵌入式设备等硬件平台。其中，RO PUF具有较好的唯一性，且无需严格对称设计，易于在FPGA中例化实现。我们以RO PUF为实例来介绍延迟型PUF的工作原理。图1展示了传统RO PUF[19]的电路结构，由于存在工艺偏差，相同结构的RO_1～RO_n振荡频率不一致。因此，多路选择器(MUltipleXer, MUX)MUX1与MUX2成对地选择其中两个RO，计数器CNT1与CNT2分别对其频率进行采集，比较器通过将计数值进行对比而生成二进制PUF响应位。现有RO PUF研究具有良好的唯一

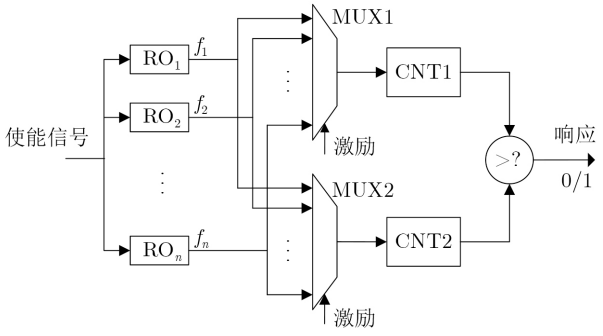


图 1 传统RO PUF结构

性[9,15–18]，但它们对环境变化的抵抗能力较弱，在不同环境下容易出现误码现象。而在系统认证中，PUF响应出现一位误码就会导致整个认证过程的失败。因此，不可靠的PUF会严重影响系统安全。

2.2 STR

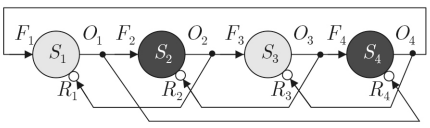
STR作为一种数字熵源，它通过异步握手协议并根据不同的事件到达时间产生振荡信号[19]。如图2所示，组成STR基本单元的S_i由一个穆勒门和一个反相器组成。

其中，输出O_i与正向输入F_i相同，与反向输入R_i相反。当F_i和R_i相同时，O_i状态保持不变。如果S_i的输出O_i与前一级的输出O_{i-1}一致，则称为Bubble(B，用灰色表示)。否则，如果S_i的输出O_i与前一级的输出O_{i-1}相反，则称为Token(T，用黑色表示)。当满足式(1)时，T从S_i传播到S_{i+1}，而B从S_i传播到S_{i-1}。

$$O_i \neq O_{i-1},\ O_i = O_{i+1} \tag{1}$$

根据B和T的分布，STR将处于两种不同振荡模式，如图3所示。为了实现PUF熵源的高效提取，通过使T均匀地放置于B中，将STR环置于均匀振荡模式。值得注意的是，环的传播延迟取决于两个模拟效应[19]：(1)Charlie效应：Charlie效应与输入端事件之间的分离时间有关，即事件分离时间越短，级间传播延迟越长；(2)Drafting效应：输出事件的时延越短，门级传播延迟越短。Drafting效应在ASIC中较强，但在FPGA中相对较弱，以至于可以完全忽略[20]。由此可知，能通过利用事件传播延迟与B和T的关系来控制频率。当达到最大频率时满足式(2)

$$\frac{\mathrm{NT}}{\mathrm{NB}} \simeq \frac{D_{\mathrm{ff}}}{D_{\mathrm{rr}}} \tag{2}$$



F_i	R_i	O_i
0	0	O_i^{-1}
0	1	0
1	0	1
1	1	O_i^{-1}

图 2 一个STR的基本结构和真值表

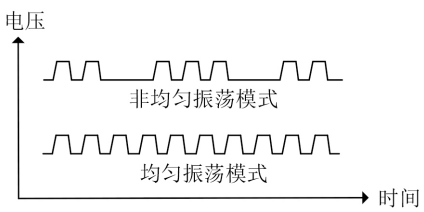


图 3 在STRs中的非均匀振荡和均匀振荡的传播模式

其中NT和NB分别为环中T和B的数量，D_{ff}和D_{rr}分别为静态正向传播延迟和静态反向传播延迟。因此，可以通过调整B与T在事件传播链中的分布情况，在不增加额外硬件开销的情况下实现STR环振荡频率的偏移。

3 基于STR的SDL PUF设计

本节首先给出了SDL PUF的总体架构。然后介绍了基于STR的偏差自锁定方案，并且详细分析了可靠性提升原理。最后，提出一种对比混淆策略。

3.1 总体架构和执行过程

图4展示了所提SDL PUF的总体架构。该架构采用相同结构的STR作为PUF的熵源阵列，以产生振荡信号并传递给MUX。MUX选择处于均匀振荡模式的STR对，其振荡信号由计数器模块(CNT)收集，并记录单位时间内振荡次数。当比较器(CMP)接收由CNT传入的计数值后，对比选中的两个STR频率大小，以生成1位响应。由于工艺偏差的存在，最终的比较结果反映PUF响应值。控制器收集第1次输出响应R1以混淆比较器。第2次生成的响应R2用于配置每个相应的STR，以实现自适应偏差锁定。

SDL PUF的工作流程分为以下3个阶段：首先是混淆阶段，每个STR环给予相同配置，通过顺序对比生成响应R1，并且控制器根据第一次生成的输出R1随机配置CMP，对下一次的响应生成进行对比混淆；然后为注册阶段，通过控制MUX实现STR环从顺序对比转换为等间距对比，在对比混淆方案的作用下生成响应R2，并通过配置器自适应配置每个STR，以实现频率偏差锁定；最后是执行阶段，通过输入激励信号使SDL PUF输出高可靠性的响应数据。后续如需此PUF进行密钥生成或认证操作，只需重复执行阶段，生成所需PUF响应。各阶段均需在STR中产生一次均匀振荡信号，每个阶段的实现细节见本章后续小节。

3.2 基于STR的自适应偏差锁定

本节首先分析所提可靠性提升原理。延迟型PUF的可靠性可以用式(3)来表示

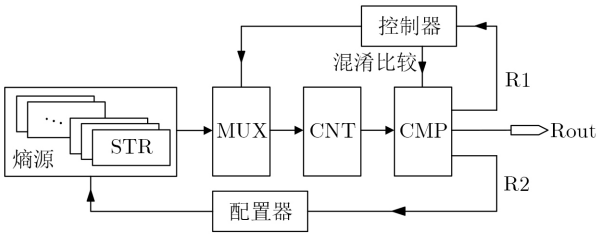


图 4 SDL PUF的总体架构

$$\text{Reliability}=1-\frac{1}{k}\sum_{j=1}^{k}\sum_{i=1}^{n}\frac{\text{HD}(R_i,R_{i,j})}{n}\times 100\% \quad (3)$$

其中，n为PUF响应的位数，k为样本数量，$\text{HD}(R_i,R_{i,j})$是输出R_i和第j个采样$R_{i,j}$之间的汉明距离。提高PUF的可靠性需要降低$\text{HD}(R_i,R_{i,j})$。而R_i的值由$f_{i,a}$和$f_{i,b}$之间的关系决定，如式(4)所示

$$R_i=\begin{cases}1, & f_{i,a}>f_{i,b}\\ 0, & f_{i,a}\le f_{i,b}\end{cases} \quad (4)$$

其中，$f_{i,a}$和$f_{i,b}$分别表示用于产生第i次响应的两个环的振荡频率。我们用d表示每个响应频率偏差的极值，则$\text{HD}(R_i,R_{i,j})$的表达式如下所示

$$\text{HD}(R_i,R_{i,j})=\text{HW}\left(d_i(f_{i,\text{a}}-f_{i,\text{b}})\oplus d_i(f_{i,\text{a},j}-f_{i,\text{b},j})\right) \quad (5)$$

为了有效提升PUF的可靠性，需要使式(5)的值最小化，其推导如下

$$\begin{cases}f_{i,\text{a},j}-f_{i,\text{a}}-(f_{i,\text{b},j}-f_{i,\text{b}})>-(f_{i,\text{a}}-f_{i,\text{b}}), R_i=1\\ f_{i,\text{b},j}-f_{i,\text{b}}-(f_{i,\text{a},j}-f_{i,\text{a}})>-(f_{i,\text{b}}-f_{i,\text{a}}), R_i=0\end{cases}$$
$$=\begin{cases}\Delta f_{i,\text{a}}-\Delta f_{i,\text{b}}<f_{i,\text{a}}-f_{i,\text{b}}, R_i=1\\ \Delta f_{i,\text{a}}-\Delta f_{i,\text{b}}<f_{i,\text{b}}-f_{i,\text{a}}, R_i=0\end{cases} \quad (6)$$

其中，$\Delta f_{i,\text{a}}$和$\Delta f_{i,\text{b}}$分别表示改变外部环境时频率的变化值。由于$\Delta f_{i,\text{a}}$和$\Delta f_{i,\text{b}}$不可预测且无法控制，因此，需要通过增加上述不等式右侧的值，即扩大环与环之间的频率差，来降低环境波动条件下的误码率。由于STR具有振荡模式可变性，通过配置STR的振荡模式偏移事件到达时间来实现频率差的扩大。

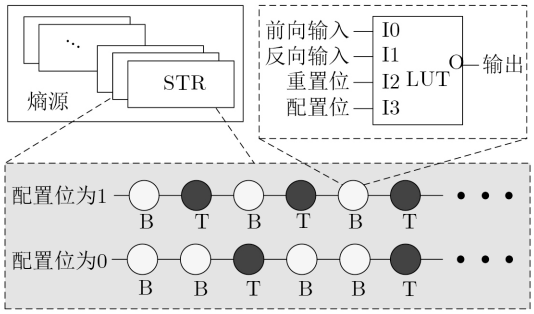
基于上述理论分析，本文提出了自适应偏差锁定方案。图5(a)展示了SDL PUF 的熵源结构，首先将STR置于均匀振荡模式，即T均匀分布于B中。由于不同的配置位决定STR中B和T的分布状态，配置位为1相对于配置位为0，STR具有更短的事件到达时间，振荡频率更高。为了实现自适应偏差锁定，如图5(b)所示，首先将所有STR环的配置位设为0，测试并生成初始PUF响应R_1。设定图中上路STR频率大于下路STR时，对应的响应位输出为1。因此将响应1反馈至上路STR的配置端，响应0反馈至下路STR的配置端。从而，在不改变最终响应结果的情况下，该配置方案大幅提升两环之间的事件到达时间差，从而使最终输出的PUF响应能够容忍环境变化所引起的频率偏移。因此，所提自适应偏差锁定方案能够显著提高PUF的可靠性。

3.3 对比混淆方案

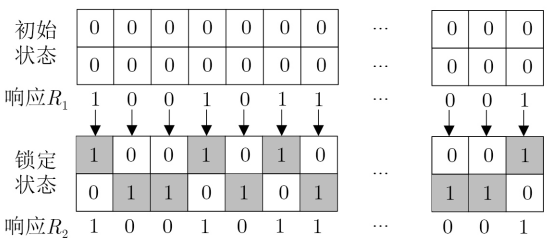
在PUF电路中，由制造工艺引起的偏差量越大，可靠性越高，但也更容易受侧信道攻击。本文采用的自适应偏差锁定方案能有效提升可靠性，但显著的频率差异也会使侧信道攻击变得更容易。为了解决此问题，本文提出了一种对比混淆方案，即通过随机数据对STR的环级对比进行混淆，并且在不同阶段采用不同的对比次序，如图6所示。首先，在混淆阶段，MUX将S_i与S_{i+1}按顺序逐次对比振荡频率，其中S_i表示STR阵列中第i个振荡环。通过两两对比产生n位响应$r_1\sim r_n$，以此作为配置数据来重配置CMP实现对比混淆，此时比较器的具体对比方式如式(7)所示：

$$R_i=\begin{cases}1, r_i=1, S_i>S_{n+i}\\ 0, r_i=1, S_i\le S_{n+i}\\ 0, r_i=0, S_i>S_{n+i}\\ 1, r_i=0, S_i\le S_{n+i}\end{cases} \quad (7)$$

其中，R_i为混淆后输出的第i位响应。在注册阶段，通过MUX的选取改变对比次序，按照等间距将S_i与S_{i+n}依次进行对比，被混淆的CMP通过对比振荡频率产生相应的PUF响应R_i。然后，STR按照上节所述方案实现自适应偏差锁定。最后，在执行阶段，通过再次激励SDL PUF，输出已经过频率偏移的高可靠性响应。通过在注册阶段和执行阶段采用的对比混淆策略，使得攻击者难以通过侧信道来预测PUF响应结果，一定程度上提高了PUF抗侧信道攻击的能力。综上，SDL PUF通过自己



(a) SDL PUF 的熵源结构



(b) 自适应配置过程

图 5 SDL PUF 的熵源结构和自适应配置过程

的特定响应数据作为随机密钥来实现不同PUF实例之间唯一的混淆对比策略，以实现更高的安全性。

4 实验结果和分析

我们在Xilinx Virtex-6 FPGA上实现了提出的SDL PUF，并生成了500个64 bit PUF响应。本节通过测试和分析唯一性、可靠性和均匀性来对所提出的PUF进行性能评估，并对该PUF的安全性进行分析。

4.1 均匀性

均匀性用于评估PUF响应中0和1的分布。理想情况下，PUF的每个输出位应具有相同的0/1生成概率。因此，均匀性越接近理想值50%，PUF的随机性越强。

为了准确地测试不同PUF电路输出响应的均匀性，本文提取了PUF电路生成的10组64位输出响应数据进行统计计算。测试结果如图7所示，对于本文提出的PUF，‘1’的最大位数是33，最小位数是31。最终的均匀性结果为49.84%，非常接近50%的理想值。实验结果表明，本文提出的SDL PUF具有良好的均匀性。

4.2 唯一性

唯一性是指将同一组激励输入到不同的PUF电路中所得到的响应间差异，也称为片间差异。由于工艺偏差的存在，一般来说，当相同的激励输入到不同PUF电路时，响应结果应该是不同的，即每个PUF电路的响应是唯一的。唯一性通常通过计算PUF不同输出响应之间的汉明距离来衡量，理想值为50%。我们通过式(8)对其进行评估：

$$\text{Uniqueness}=\frac{2}{k(k-1)}\sum_{i=1}^{k-1}\sum_{j=i+1}^{k}\frac{\text{HD}(r_i,r_j)}{n}\times 100\% \tag{8}$$

其中，k是电路样本数量，r_i和r_j分别为第i个和第j个PUF响应，n为响应序列的长度，$\text{HD}(r_i,r_j)$为相同激励下第i个与第j个PUF响应之间的汉明距离。

我们在常温常压下测试了12组64位SDL PUF的输出响应，实验结果如图8所示，其中片间汉明距离呈现高斯分布，平均片间汉明距离为31.546。因此，SDL PUF的唯一性达到49.29%，接近理想值。

4.3 可靠性

可靠性是考察PUF响应稳定程度的一种特征指标。理想情况下，PUF在输入相同激励时，响应应该完全一致。而在不同环境下，由于温度、电压等外界条件的改变，会对PUF的可靠性造成一定的影响。我们通过等式(9)来对可靠性进行计算：

$$\text{Reliability}=1-\frac{1}{m}\sum_{j=1}^{m}\frac{\text{HD}(r,r_j)}{n}\times 100\% \tag{9}$$

其中，m为样本数量，r为常温和标准电压下的响应，r_j为第j个不同环境下的PUF响应。

我们在温度范围0°C～80°C(步长20°C)和电压范围0.8～1.2V(步长0.05V)下对SDL PUF, RO PUF以及未进行偏差锁定的原始STR PUF分别进行了测试，每种条件下各输出50组64位PUF响应。实验结果如图9所示，与传统RO PUF以及未进行自适应配置的STR PUF相比，我们提出的SDL PUF在0.85～1.15V和0°C～80°C的范围内实现了零误码。当电压为1.2V时，误码率最高为2.41%。实验结果表明SDL PUF对温度和电压的变化具有较高的鲁棒性。

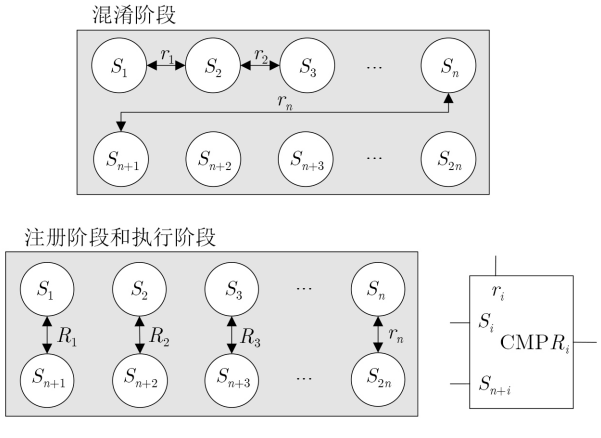


图 6 对比混淆方案

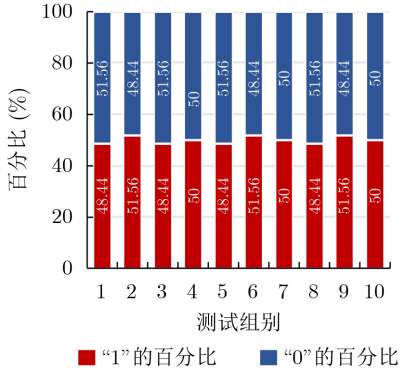


图 7 均匀性测试

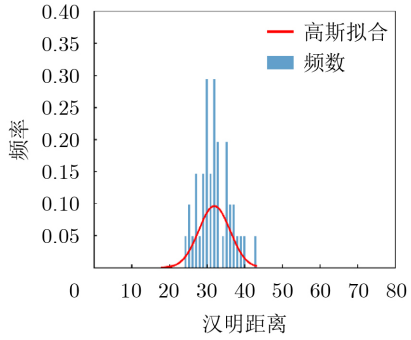
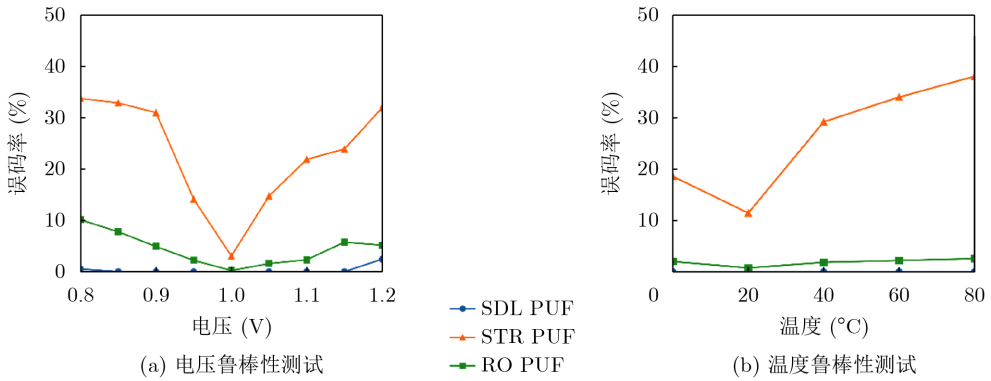


图 8 唯一性测试



(a) 电压鲁棒性测试　　(b) 温度鲁棒性测试

图 9 电压和温度鲁棒性测试

表 1　PUF性能对比

PUF种类	FPGA平台	唯一性(%)	可靠性(%)	是否能实现零误码 (零误码范围)	熵源面积*
文献[6]	Artix-7	49～50	≥99	×	12LUTs, 24MUXs
文献[9]	Spartan-6	49.07	99.80	×	12LUTs
文献[16]	Spartan-7	49.98	98.61	×	12 LUTs, 11MUXs
文献[21]	Artix-7	48.74	98.91	×	12LUTs
文献[22]	Artix-7	47.65	97.36	×	12LUTs
本文SDL PUF	Virtex-6	49.29	99.84	√ (0°C～80°C, 0.85～1.15V)	12 LUTs

*熵源振荡环统一设定为12阶

4.4 安全性分析

侧信道攻击是一种通过探测电路相关物理特性来获取PUF响应的攻击方式，我们提出的PUF设计为了增强可靠性而增大了相互对比的两个STR之间的频率差，如若采用确定性的对比方式会导致攻击者通过预测频率偏差来展开攻击，并获取PUF响应。我们所提出的对比混淆方案通过提取自身工艺偏差对比较器进行随机配置，从而使攻击者即使获取了所有STR振荡频率，也无法通过特定的对比来预测响应结果。这对于n位PUF响应提升了2^n倍的攻击难度，因此对比混淆设计使得SDL PUF具有抗侧信道攻击特性。

4.5 相关性能对比

为了综合评估所提出的PUF电路，本文在唯一性、可靠性、是否实现零误码以及熵源面积等方面与现有设计方案进行对比。如表1所示，文献[6,9, 21]具有较高的可靠性，而文献[6,16]中的熵源结构采用了额外的MUX资源，但这些相关工作都无法实现零误码。相比之下，我们所提出的SDL PUF唯一性为49.29%，非常接近理想值50%；其熵源面积只有12个LUT，在不占用额外资源(如MUX)的情况下，实现了99.84%的高可靠性；并且，该结构在0°C～80°C和0.85～1.15V的环境变化范围内实现零误码，在低误码率方面具有显著优势。综上所述，我们提出的SDL PUF在不占用额外硬件资源的情况下提高了可靠性，且在较宽环境变化范围内实现了零误码。

5　结论

本文利用STR的振荡状态可配置性提出了一种具有高可靠性的自适应偏差锁定PUF。通过在PUF初始化阶段自适应地配置STR，增大环级之间事件到达时间偏差，从而确保其在环境变化的情况下仍能产生相同的PUF响应。同时，所提对比混淆方案通过随机配置比较器的方式，为每比特PUF响应的生成提供唯一的对比策略，使得该结构具备一定的抗侧信道攻击能力。最终，SDL PUF在Xilinx Virtex-6 FPGA上得到实现和验证。实验结果表明该结构唯一性为49.29%，均匀性为49.84%，在电压范围0.85～1.15V和温度范围0°C～80°C内实现零误码，在可靠性方面具有显著优势。

参 考 文 献

[1] 福布斯：2016年物联网预测和市场估算总结[EB/OL]. http://tech.163.com/16/1130/07/C73Q381P00097U7R.html, 2016.

[2] Grand View Research, Inc. IoT security market size worth $9.88 billion By 2025 | CAGR: 29.7%[EB/OL]. https://www.grandviewresearch.com/press-release/global-internet-of-things-iot-security-market, 2018.

[3] 杨庚, 许建, 陈伟, 等. 物联网安全特征与关键技术[J]. 南京邮

电大学学报: 自然科学版, 2010, 30(4): 20–29. doi: 10.3969/j.issn.1673-5439.2010.04.004.
YANG Geng, XU Jian, CHEN Wei, *et al*. Security characteristic and technology in the internet of things[J]. *Journal of Nanjing University of Posts and Telecommunications: Natural Science*, 2010, 30(4): 20–29. doi: 10.3969/j.issn.1673-5439.2010.04.004.

[4] XU Chongyao, ZHANG Jieyun, LAW M K, *et al*. Transfer-path-based hardware-reuse strong PUF achieving modeling attack resilience with200 million training CRPs[J]. *IEEE Transactions on Information Forensics and Security*, 2023, 18: 2188–2203. doi: 10.1109/TIFS.2023.3263621.

[5] 汪鹏君, 连佳娜, 陈博. 基于序列密码的强PUF抗机器学习攻击方法[J]. 电子与信息学报, 2021, 43(9): 2474–2481. doi: 10.11999/JEIT210726.
WANG Pengjun, LIAN Jiana, and CHEN Bo. Sequence cipher based machine learning-attack resistance method for strong-PUF[J]. *Journal of Electronics & Information Technology*, 2021, 43(9): 2474–2481. doi: 10.11999/JEIT210726.

[6] ZHANG Jiliang, SHEN Chaoqun, GUO Zhiyang, *et al*. CT PUF: Configurable tristate PUF against machine learning attacks for IoT security[J]. *IEEE Internet of Things Journal*, 2022, 9(16): 14452–14462. doi: 10.1109/JIOT.2021.3090475.

[7] ZHANG Jiliang, DING Lin, CHEN Zhuojun, *et al*. DA PUF: Dual-state analog PUF[C]. The 59th ACM/IEEE Design Automation Conference (DAC), San Francisco, USA, 2022: 73–78. doi: 10.1145/3489517.3530412.

[8] DELLA SALA R and SCOTTI G. A novel FPGA implementation of the NAND-PUF with minimal resource usage and high reliability[J]. *Cryptography*, 2023, 7(2): 18. doi: 10.3390/cryptography7020018.

[9] GAN Jiayan, ZHOU Jun, and WANG Ning. A FPGA-based RO PUF with LUT-based self-compare structure and adaptive counter time period tuning[C]. 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, 2018: 1–5. doi: 10.1109/ISCAS.2018.8351014.

[10] DELLA SALA R, BELLIZIA D, and SCOTTI G. A lightweight FPGA compatible weak-PUF primitive based on XOR gates[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2022, 69(6): 2972–2976. doi: 10.1109/TCSII.2022.3156788.

[11] STREIT F J, KRÜGER P, BECHER A, *et al*. Design and evaluation of a tunable PUF architecture for FPGAs[J]. *ACM Transactions on Reconfigurable Technology and Systems*, 2022, 15(1): 7. doi: 10.1145/3491237.

[12] DUBROVA E. A reconfigurable arbiter PUF with 4 x 4 switch blocks[C]. 2018 IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL), Linz, Austria, 2018: 31–37. doi: 10.1109/ISMVL.2018.00014.

[13] SINGH S, BODAPATI S, PATKAR S, *et al*. PA-PUF: A novel priority arbiter PUF[C]. 2022 IFIP/IEEE 30th International Conference on Very Large Scale Integration (VLSI-SoC), Patras, Greece, 2022: 1–6. doi: 10.1109/VLSI-SoC54400.2022.9939642.

[14] NI Li, WANG Pengjun, ZHANG Yuejun, *et al*. SI PUF: An SRAM and inverter-based PUF with a bit error rate of 0.0053% and 0.073/0.042 pJ/bit[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2024, 71(4): 2339–2343. doi: 10.1109/TCSII.2023.3339296.

[15] YAO Liang, LIANG Huaguo, HUANG Zhengfeng, *et al*. A lightweight configurable XOR RO-PUF design based on Xilinx FPGA[C]. Proceedings of 2021 IEEE 4th International Conference on Electronics Technology (ICET), Chengdu, China, 2021: 83–88. doi: 10.1109/ICET51757.2021.9451016.

[16] RIZK D, RIZK R, RIZK F, *et al*. An economic uniqueness-improved reliable reconfigurable RO PUF for IoT security[C]. 2022 IEEE International Symposium on Circuits and Systems (ISCAS), Austin, USA, 2022: 1680–1684. doi: 10.1109/ISCAS48785.2022.9937931.

[17] LU Yingchun, WANG Xinyu, WANG Yanjie, *et al*. Pure digital scalable mixed entropy separation structure for physical unclonable function and true random number generator[J]. *IEEE Transactions on Very Large scale Integration (VLSI) Systems*, 2021, 29(11): 1922–1929. doi: 10.1109/TVLSI.2021.3116104.

[18] LV Shenglai, HUANG Yangbo, CHEN Lei, *et al*. RO PUF design in FPGAs with frequency-offsetting strategies[C]. 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 2021: 558–562. doi: 10.1109/ICIBA52610.2021.9688287.

[19] WINSTANLEY A and GREENSTREET M. Temporal properties of self-timed rings[C]. Proceedings of the 11th IFIP WG 10.5 Advanced Research Working Conference on Correct Hardware Design and Verification Methods, Scotland, UK, 2001: 140–154. doi: 10.1007/3-540-44798-9_12.

[20] CHERKAOUI A, FISCHER V, AUBERT A, *et al*. Comparison of self-timed ring and inverter ring oscillators as entropy sources in FPGAS[C]. 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 2012: 1325–1330. doi: 10.1109/DATE.2012.6176697.

[21] HUANG Zhengfeng, BIAN Jingchang, LIN Yankun, *et al*. Design guidelines and feedback structure of ring oscillator PUF for performance improvement[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2024, 43(1): 71–84. doi: 10.1109/TCAD.2023.3301386.

[22] BOKE A K, NAKHATE S, and RAJAWAT A. FPGA implementation of PUF based key generator for secure communication in IoT[J]. *Integration*, 2023, 89: 241–247. doi: 10.1016/j.vlsi.2022.12.006.

张 源：男，博士生，研究方向为硬件安全及集成电路设计.
罗静茹：女，硕士生，研究方向为硬件安全.
张吉良：男，教授，博士生导师，研究方向为集成电路硬件安全、安全集成电路设计、后摩尔时代新型计算架构等.

责任编辑：陈 倩