

基于FPGA的新型强弱混合型PUF电路设计

连佳娜^{1,2}, 汪鹏君¹, 李刚¹, 马雪娇³, 翟官宝¹

(1. 温州大学电气与电子工程学院, 浙江 温州 325000;

2. 温州大学计算机与人工智能学院, 浙江 温州 325000;

3. 温州大学瓯江学院, 浙江 温州 325000)

摘要: 物理不可克隆函数 (PUF, physically unclonable function) 通过提取芯片制造过程中无法避免引入的工艺偏差, 可产生具有随机性、唯一性和防篡改特性的特征密钥。通过对 PUF 电路结构和工作原理的研究, 提出一种基于现场可编程门阵列 (FPGA, field-programmable gate array) 的新型强弱混合型 PUF (SWPUF, strong and weak PUF) 电路设计方案。该 PUF 可根据激励的汉明重量 (HW, hamming weight) 灵活地配置为强 PUF 和弱 PUF 两种拓扑结构, 解决强/弱 PUF 分立实现的局限性。此外, 利用异或去相关技术进一步优化输出密钥的统计特性。所提 PUF 采用 Xilinx Artix-7 FPGA (28 nm 工艺) 实现, 利用 Matlab 结合 MicroBlaze 微控制器构建内建自测试平台 (self-built test platform)。实验结果表明, 该 PUF 具有良好的随机性 (96.98%)、唯一性 (99.64%) 和可靠性 (常温常压下 96.6%)。逻辑回归分析进一步显示, 在 HW 较小的情况下所提 SWPUF 比传统的 Arbiter-PUF 具有更好的抗攻击能力, 可广泛应用于信息安全领域, 如密钥存储 (针对弱 PUF) 和设备认证 (针对强 PUF)。

关键词: 强弱混合型; 物理不可克隆函数; 现场可编程门阵列; 电路设计

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021028

Novel hybrid strong and weak PUF design based on FPGA

LIAN Jiana^{1,2}, WANG Pengjun¹, LI Gang¹, MA Xuejiao³, ZHAI Guanbao¹

1. College of Electrical and Electronic Engineering, Wenzhou University, Wenzhou 325000, China

2. College of Computer Science and Artificial Intelligence, Wenzhou University, Wenzhou 325000, China

3. Oujiang College, Wenzhou University, Wenzhou 325000, China

Abstract: Physically unclonable function (PUF) can produce intrinsic keys with characteristics of randomness, uniqueness and tamper-proof by exploiting the process deviations which can not be avoided in the chip

收稿日期: 2020-11-15; 修回日期: 2021-02-22

通信作者: 汪鹏君, wangpengjun@wzu.edu.cn; 李刚, ligang@wzu.edu.cn

基金项目: 国家重点研发计划 (2018YFB2202100); 国家自然科学基金 (61874078, 61904125); 温州市基础性科研项目 (G20190006, G20190003)

Foundation Items: The National Key R&D Program of China (2018YFB2202100), The National Natural Science Foundation of China (61874078, 61904125), Basic Scientific Research Project of Wenzhou (G20190006, G20190003)

论文引用格式: 连佳娜, 汪鹏君, 李刚, 等. 基于FPGA的新型强弱混合型PUF电路设计[J]. 网络与信息安全学报, 2021, 7(2): 94-103.

LIAN J N, WANG P J, LI G, et al. Novel hybrid strong and weak PUF design based on FPGA[J]. Chinese Journal of Network and Information Security, 2021, 7(2): 94-103.

manufacturing process. A novel hybrid strong and weak PUF (SWPUF) circuit design based on field-programmable gate array(FPGA) was proposed after the investigation of the PUF circuit structures and principles. To address the limitation of designing strong-PUF and weak-PUF discretely, SWPUF could be configured into two topologies conveniently depending on the Hamming Weight (HW) of the challenges. In addition, the statistical characteristics of the responses could be further improved by a XOR-decorrelation technique. The proposed SWPUF was implemented on a Xilinx Artix-7 FPGA (28nm technology), and a self-built test platform was set up by using Matlab and MicroBlaze microcontroller. Experimental results show that the SWPUF has good performances of randomness (96.98%), uniqueness (99.64%) and reliability (96.6%). Logic register analysis also shows that the SWPUF has a better anti-attack capability than the traditional Arbiter-PUF in the case of with small HW, and can be used in the information security, such as key storage (especially to weak PUF) and device authentication (especially to strong PUF).

Keywords: hybrid strong and weak, physically unclonable function, FPGA, circuit design

1 引言

随着第四次技术革命的到来,人类社会进入万物感知、万物互联的全新时代,信息安全已从传统的政治、经济、军事、外交等领域逐步扩展到日常生活中,如防伪标签、身份认证、汽车防盗、金融收费、物流跟踪等。物理不可克隆函数(PUF, physically unclonable function)是一种极具应用前景的硬件安全原语,最早由 Pappu 等^[1]研究人员提出。PUF 通过捕获集成电路制造过程中无法避免引入的工艺偏差,可产生具有随机性、唯一性以及防篡改特性的特征密钥,非常适合应用于信息安全领域,如知识产权保护^[2-3]、密钥存储^[4-6]、设备认证^[7-8]、物联网安全防护^[4,9-10]等。PUF 根据产生激励响应对(CRP, challenge response pair)的能力不同,可分为弱 PUF^[11-17]和强 PUF^[18-26]两大类。弱 PUF 仅能产生有限数量的 CRP,因此主要用于密钥生成^[4-6]。典型的弱 PUF 主要包括涂层 PUF^[15]、SRAM PUF^[11-13]、蝶形 PUF^[14]、锁存器 PUF (latch PUF)^[16]等。强 PUF 通过硬件资源重构可产生大量的 CRP,因此强 PUF 主要用于设备认证^[7-8]和状态证明^[23]。典型的强 PUF 主要包括光学 PUF^[1]、仲裁器 PUF^[20-21,26](APUF)、环形振荡器 PUF (RO-PUF)^[18]、算数逻辑单元 PUF 等。

自 Science 上发表光学 PUF^[1]以来,先后出现了多种不同类型的 PUF。对于弱 PUF, Shifman 等^[11]通过分析 SRAM 单元的决策电压提出一种基于 65nm 工艺可产生两位独立响应的 SRAM

PUF。Li 等^[12]利用双稳态 PUF 单元共享和随机字级读取策略,提出一种单元特征尺寸仅为 $215F^2$ 、比特不稳定性为 2.05% 的双稳态轻量型 PUF 电路。Lu 等^[13]通过配置 SRAM 单元选择顺序提出一种可配置的 SRAM PUF 以扩大 CRP 空间。Li 等^[17]基于电压受控型反相器最大增益点偏差,提出一款多工作模式、动态可配置、稳定性自主筛选的低功耗 PUF 电路。对于强 PUF,李雪营等^[18]通过引入并行输入串行输出移位寄存器提出一种基于现场可编程门阵列(FPGA, field-programmable gate array)的 RO-PUF,该 PUF 仅利用 4 位激励能产生 16 位随机响应,增大了 CRP 空间,与其他产生相同 CRP 空间的 PUF 电路相比减小了硬件开销。Gao 等^[19]将有限状态机与 APUF 相结合提出一种受控的强 PUF,在无须使用纠错编码以及辅助数据的前提下能实现更高的安全性。Dubrova 等^[20]为了缩短密钥更新周期,利用 4×4 开关模块代替传统 2×2 开关模块,提出一种可重构的新型 APUF。Wen 等^[21]基于两路传播信号的时延差与仲裁器建立时间的关系,提出一种具有选择功能的 APUF 以避免仲裁器处于亚稳态,从而增强 PUF 的可靠性和唯一性。Gu 等^[22]利用触发器和多路选择器的工艺偏差提出一种基于触发器的 FF-APUF 电路,该 PUF 结构紧凑,有良好的唯一性和可靠性。

对于弱 PUF,PUF 单元通常只产生一位输出响应,因此输出响应间相互独立,适用于密钥生成等场景;对于强 PUF,工艺敏感单元的重构,使生成的响应间必然存在相关性。因此,与强 PUF

相比,弱 PUF 具有更好的抗建模攻击和机器学习攻击的能力。但弱 PUF 在实际应用中也存在不足,如需要生成指数多个输出响应时,其硬件开销随输出响应的长度呈指数增长关系。强 PUF 和弱 PUF 在信息安全领域皆有其各自的应用场景,研究人员通常采用分立方式实现两种不同的 PUF,即弱 PUF 与强 PUF 单独设计无法整合在一个统一的拓扑结构中。本文通过对强弱 PUF 电路结构和设计思想的研究,结合两者优势并利用异或去相关技术,提出一种强弱混合型 PUF (SWPUF, strong and weak PUF),使同一 PUF 电路既能产生弱 PUF 的 CRP,又能产生强 PUF 的 CRP。且在仅需少量 CRP 的场景中(如密钥生成),该 PUF 配置为弱 PUF 拓扑结构,作为弱 PUF 使用;在需要大量 CRP 的场景中(如设备认证),该 PUF 配置为强 PUF,从而兼顾两者优势,拓展单个 PUF 的适用场景。因此,所提 PUF 利用相同的电路拓扑结构,通过输入激励汉明重量(HW, hamming weight)变化可实现强 PUF 和弱 PUF 的有机统一。最后,采用 Xilinx Artix-7 开发板对所提 PUF 进行 FPGA 实现,并搭建内建自测试平台。实验结果表明,所提 PUF 具有良好的随机性、唯一性和可靠性。在不引入非线性和增加电路复杂度的前提下实现所提 PUF 比传统 APUF 具有更强的抗攻击能力。

2 传统 APUF 电路分析

传统的 APUF 电路结构如图 1 所示,通过在电路中构造两条完全对称的信号传输路径,并在末端设置一个仲裁器,通过比较同一信号经过两条对称路径到达仲裁器的先后顺序,判决输出响应“0”或“1”。理论上两条路径上的信号应该同时到达仲裁器,但由于时延路径不可避免地存在工艺偏差,导致两条路径上信号的时延不同,从而产生不可预测的响应“0”或“1”。组成 APUF 的开关单元主要用于选择不同的时延路径,激励信号 $C=C_1, C_2, \dots, C_n$ 用于选择传输路径是直接通过还是交叉通过。此外,APUF 电路中的仲裁器通常采用 D 触发器构成。文献[27]表明当两条路径信号的时延差小于仲裁器的建立时间时,仲裁器的输出响应一般不发生变化,然而采用基于 D

触发器的仲裁器会在电路中引入大约 10% 的 0/1 偏向性。改进的 APUF 仲裁器通常由交叉耦合的与非门构成,若第一条路径上升沿信号先到达仲裁器,则输出为逻辑“1”,反之则为逻辑“0”。

传统 APUF 电路通常可表示为一个线性时延模型^[28]。总时延为每一级开关单元传播时延的累加和,可表示为

$$\Delta = \vec{\omega}^T \vec{\Phi} \quad (1)$$

其中 $\vec{\omega}$ 表示 APUF 中每一个多路选择器传播时延的特征向量。 N 位激励 C 的函数表达式用 $\vec{\Phi}$ 表示。

$$\vec{\Phi}(\vec{C}) = (\Phi_1(\vec{C}), \Phi_2(\vec{C}), \Phi_3(\vec{C}), \dots, \Phi_n(\vec{C}), 1)^T \quad (2)$$

其中 $\Phi_j(\vec{C}) = \prod_{i=j}^n (1 - C_i)$, $j=1, 2, 3, \dots, k$ 。如果 $\Delta > 0$, APUF 的输出响应为 1, 否则为 0。为了简化计算,常使用 $t=2 \times r - 1$ ($t \in \{-1, 1\}$) 代替式(3)中的输出响应 t , t 可表示为

$$t = \text{sgn}(\Delta) = \text{sgn}(\vec{\omega}^T \vec{\Phi}) \quad (3)$$

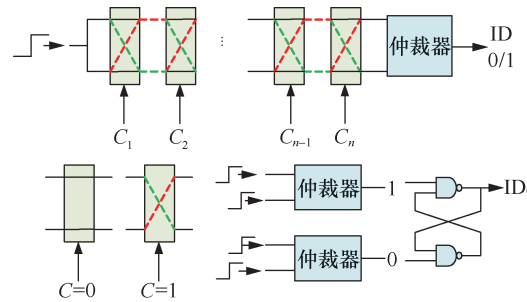
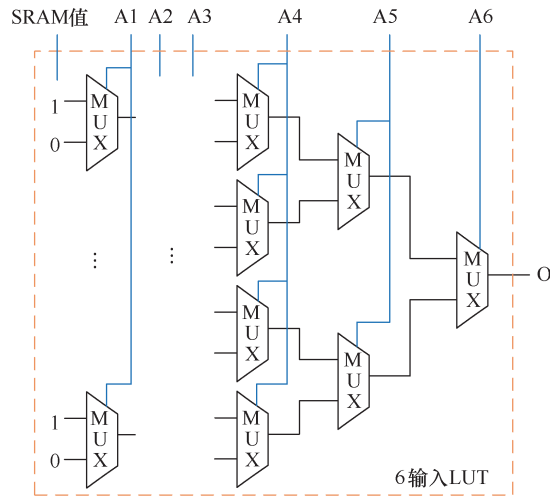


图 1 仲裁器 PUF 电路结构
Figure 1 Circuit structure of arbiter-PUF

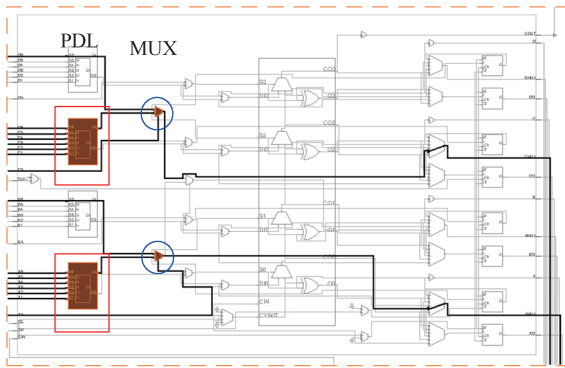
3 新型 SWPUF 电路设计

3.1 强弱混合型 PUF 电路结构

通过对 APUF 结构和工作原理的研究,本节提出一种基于时延模块的新型开关单元结构,其中时延模块由 FPGA 片内 6 输入查找表(LUT, look-up-table)实现,如图 2(a)所示。LUT 利用输入端控制信号传输路径,其中 A1 端口用于信号输入, A2 ~ A6 端口用于控制传输路径。所提新型开关单元由两个时延模块和两个多路选择器(MUX)构成,该结构可在一个 Slice 中实现。经 Vivado 软件布局布线后其内部拓扑结构如图 2(b)所示。所提强弱混合型 PUF 电路由 N 级新型开关



(a) 时延模块结构



(b) 开关单元实现

图2 新型开关单元结构以及实现

Figure 2 Structure and implementation of novel switch unit

单元和仲裁器构成，形成两条完全对称的时延路径，整体电路结构如图3所示。所提PUF在运行过程中，可以根据输入激励的HW变化灵活地配置为两种不同的类型（强PUF和弱PUF）。工作原理如下：输入激励 C 为一串二进制序列，传输信号会根据激励选择相应MUX的导通路径。当 $C_i=1$ 时，脉冲信号选通有时延模块的MUX路径，反之选通无时延模块的MUX路径，最后通过仲

裁器判决上下两条时延信号到达的先后顺序，从而产生输出响应“0”或“1”。根据运行过程中是否选通时延模块，将PUF电路中的开关单元分为有效（选通时延模块）和无效（不选通时延模块）两种状态。此时输入激励的HW映射到电路中表现为有效开关单元数量。对于弱PUF，电路运行中仅有1个有效开关单元参与，如表1所示。输入激励的HW=1，共有 N 组激励，每次脉冲信号在上下两条路径中仅选通一个时延模块，最后两条路径信号通过仲裁器输出响应。与弱PUF不同，强PUF电路的时延路径中有多个有效开关单元参与信号传输过程（输入激励的HW大于1），此时所提PUF配置为强PUF结构。

表1 由 N 级开关单元组成的弱PUF的激励（HW=1）
Table 1 Challenge of weak PUF composed of N switch units (HW=1)

激励	C_0	C_1	C_2	C_3	...	C_n
激励 1	1	0	0	0	...	0
激励 2	0	1	0	0	...	0
激励 3	0	0	1	0	...	0
激励 4	0	0	0	1	...	0
...	...	...	...	...	...	...
激励 N	0	0	0	0	...	1

由于输入激励的HW不同，该PUF传输路径中实际选通的时延模块数量也不同，因此可根据HW变化将 N 位SWPUF的CRP空间划分为 N 个子空间。以64级开关单元为例，不同HW对应的CRP数量如图4所示，其中横坐标表示激励响应数量，纵坐标表示输入激励的HW。在HW为1时所提PUF配置为弱PUF，仅产生64个CRP，

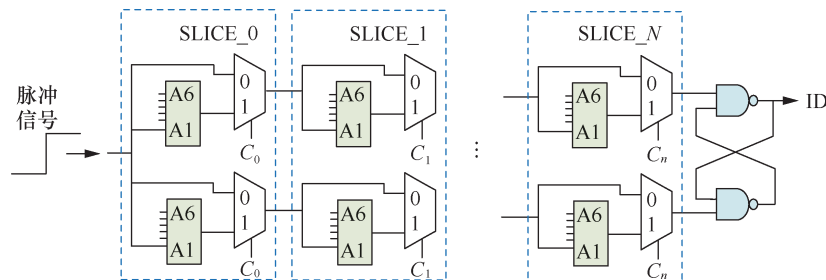


图3 基于FPGA的新型强弱混合型PUF电路结构

Figure 3 Circuit structure of novel hybrid strong weak PUF based on FPGA

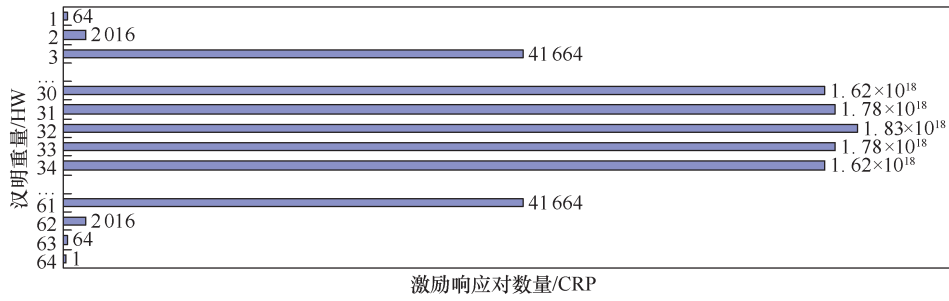


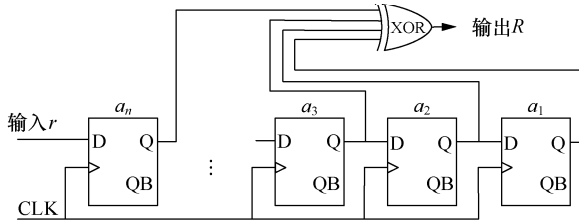
图 4 不同 HW 对应的 CRP 数量 (以 64 级开关单元为例)

Figure 4 Counts of CRPs with different HWs with 64 switch units

其余 63 个子空间都为强 PUF 产生的 CRP。

3.2 后处理电路

为增强输出密钥的随机性以及降低密钥之间的相关性, 引入移位寄存器模块, 并采用异或 (XOR) 去相关对原始序列进行处理。后处理电路结构如图 5 所示, 由 N 个 D 触发器和 1 个 XOR 门构成, D 触发器用于存储 0/1, XOR 门用于对 N 个 D 触发器的输出进行异或操作。

图 5 N 位 XOR 移位寄存器后处理电路Figure 5 Post processing circuit of N -bit XOR shift register

当前时刻 N 个 D 触发器的状态构成该 XOR 移位寄存器的当前状态 S , 可用 N 位序列 $a_1, a_2, \dots, a_n$ 表示。在时钟脉冲周期区间内, 每一级触发器 a_i 都将其状态向下一级 a_{i-1} 传递, 并将输入序列 $r_1, r_2, \dots, r_n$ 的下一个值 r_i 作为 a_n 下一时刻的输入。在时钟脉冲作用下, XOR 移位寄存器的状态可表示为

$$S_i = (a_i, a_{i+1}, \dots, a_{i+n-1}) \quad (4)$$

在输入序列 r_i 的驱动下, XOR 移位寄存器的每一位数据向前移动一位, 下一时刻状态 S_{i+1} 可表示为

$$S_{i+1} = (a_{i+1}, a_{i+2}, \dots, a_{i+n-1}, r_i) \quad (5)$$

则最终异或输出结果为

$$R_i = a_{i+1} \oplus a_{i+2} \oplus \dots \oplus a_{i+n-1} \oplus r_i \quad (6)$$

由此得到一串二进制序列 $R_1, R_2, \dots, R_n$, 即为 XOR 移位寄存器的输出序列 R 。XOR 移位寄存器 ($n=4$) 的工作状态如表 2 所示, 这里假定输入序列为 10010110, 寄存器的初值为 0101。

表 2 4 位 XOR 移位寄存器工作状态
Table 2 Status of 4-bit XOR shift register

时钟 脉冲	输入 序列值	状态 S (初值为 0101)				输出 R
		a_1	a_2	a_3	a_4	
1	1	1	0	1	1	1
2	0	0	1	1	0	0
3	0	1	1	0	0	0
4	1	1	0	0	1	0
5	0	0	0	0	1	0
6	1	1	0	1	0	1
7	1	1	1	0	1	1
8	0	0	0	1	1	0

对于寄存器位数的选择, 设 X 和 Y 分别为两位随机数, 其期望值 $E(X)=E(Y)=u$, p 表示它们的相关性, 则当 u 接近 0.5 时, 式(7)可表示为

$$E(X \oplus Y) \approx 0.5(1 - p) \quad (7)$$

由式(7)可知, 若 X 和 Y 相互独立 (即 $p=0$), 则 $E(X \oplus Y) \approx 0.5$ 。若有 n 位彼此独立的随机数进行异或, 则其对应的期望值为

$$0.5 + (-2)^{n-1}(u - 0.5)^n = 0.5(1 + (-2m)^n) \quad (8)$$

其中, $m=u-0.5$ 。由式(8)可知, 期望值随着位数 n 的增大趋于 0.5。后处理电路输出响应的随机性随移位寄存器位数 n 和数据异或间隔位数变化的统计特性如表 3 所示。

通过分析表 3, 并综合考虑电路实现过程中

的硬件开销,选择彼此间隔 1 位的 12 位移位寄存器作为后处理电路,其电路结构如图 6 所示。

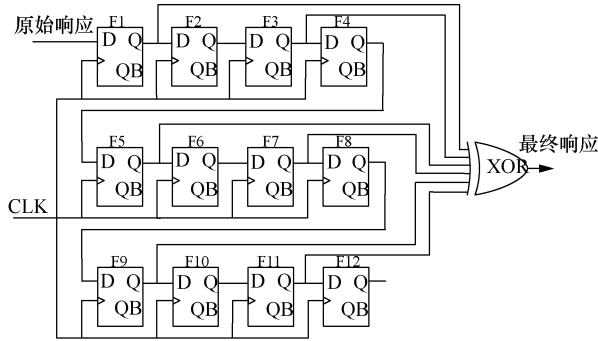


图 6 XOR 移位寄存器电路结构 ($n=12$)
Figure 6 Circuit structure of the XOR shift register ($n=12$)

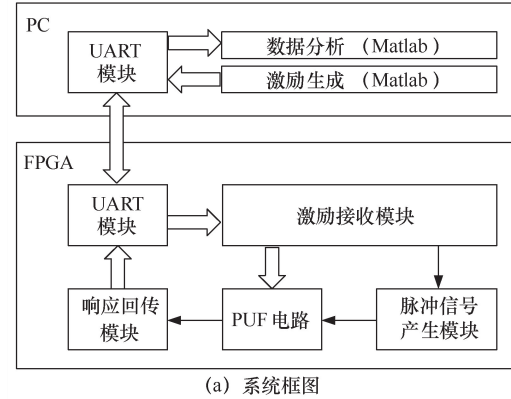
表 3 随机性随移位寄存器数和间隔位数变化的统计特性
Table 3 Statistical characteristics of randomness with the counts of shift register and XOR

移位寄存器 位数 n	异或间隔位数			
	0	1	2	3
4	46.94%	41.53%	—	—
6	49.65%	47.25%	50.82%	—
8	51.84%	48.48%	38.62%	38.52%
10	49.97%	49.67%	38.64%	38.62%
12	50.14%	50.29%	49.65%	49.89%
14	49.06%	48.91%	38.55%	38.64%
16	50.16%	50.11%	48.81%	50.07%
18	51.92%	51.29%	50.64%	38.65%
20	50.74%	50.15%	38.74%	50.81%

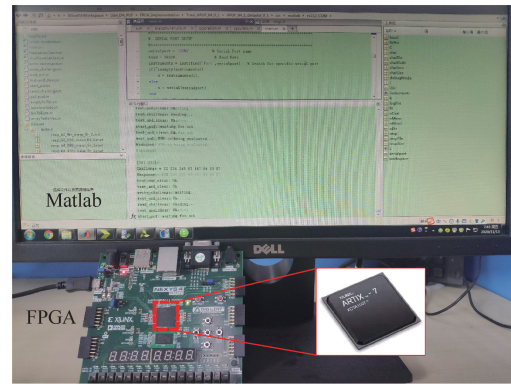
4 实验结果与分析

本文所提 PUF 采用 Xilinx Artix-7 (28nm 工艺) FPGA 开发板实现,测试系统框架及平台如图 7 所示。首先,PC 端利用 Matlab 并结合 MicroBlaze 微控制器构建内建自测试平台 (self-built test platform) 并通过 UART 模块发送随机激励至 FPGA;其次,利用 FPGA 实现脉冲信号产生、激励接收、PUF 电路、响应回传和 UART 等模块(脉冲产生模块用于产生脉冲信号,激励接收模块用于接收 PC 端发送的 N 位随机激励,PUF 电路用于产生响应,UART 模块用于激励接收及响应回传),当响应回传模块接收到响应并将其打包后,UART 模块将响应发送至 PC 端;

最后,PC 端再次利用 UART 模块接收响应,并通过 Matlab 对随机选取的输出响应进行随机性、唯一性及可靠性分析。



(a) 系统框图



(b) 测试平台

图 7 本文所提 PUF 测试系统框架与平台
Figure 7 Test system framework and platform of proposed PUF

4.1 随机性

随机性主要通过观察 PUF 电路输出响应中逻辑 0 和逻辑 1 的概率统计分布来衡量。理想情况下,逻辑 0 和逻辑 1 均匀分布,都接近 50%^[29],随机性可表示为

$$\text{Randomness} = (1 - |2P(R=1) - 1|) \times 100\% \quad (9)$$

PUF 随机性通常由灰度图来直观表示。随机选取一个 PUF,输出响应的灰度映射如图 8(a)所示,其中白色像素代表逻辑 0,黑色像素代表逻辑 1,输出响应中逻辑 0 和逻辑 1 分别为 51.51% 和 48.49%,对应的随机性为 96.98% (接近理想值 100%,无明显逻辑偏向性)。此外,其余 99 个 PUF 也获得了类似的统计结果。100 个 PUF 输出响应的平均灰度映射如图 8(b)所示,可以发现平均灰度值在 0.5 附近波动,且无明显的空间相关性。

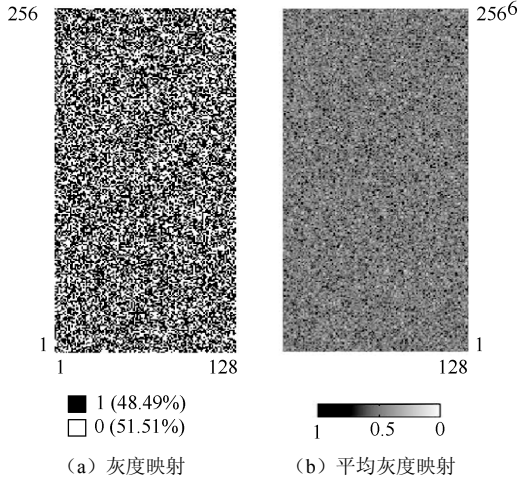


图8 PUF 输出响应分布
Figure 8 Distribution of the output responses

相关性用于衡量 PUF 输出响应之间的相关程度,其中相关值越小,输出响应的相关性越低。本文使用自相关函数 (ACF, autocorrelation function) 对所提 PUF 的输出响应进行自相关分析,结果如图9所示。测试结果表明,在95%置信区间内,所提 PUF 的 ACF 值为 0.02 (接近理想值 0),因此具有良好的空间独立性。综上所述,所提 PUF 具有良好的随机性。

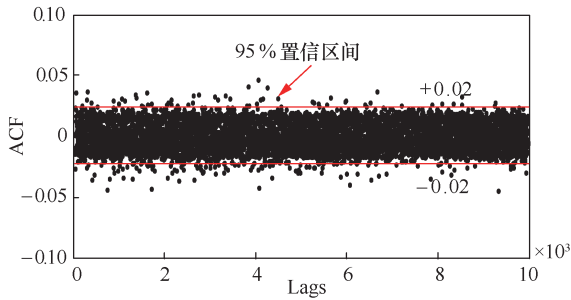


图9 SWPUF 的自相关性
Figure 9 Autocorrelation of SWPUF

4.2 唯一性

唯一性用来标识不同 PUF 个体之间的区分度,通常采用平均片间汉明距离 (HD, hamming distance) 来衡量。 P_{inter} 表示对 K 个不同的 PUF 个体施加相同的激励,输出响应之间不同位数的统计概率。 K 个不同 PUF 个体的平均片间 HD 可表示为

$$P_{\text{inter}} = \frac{2}{K(K-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^K \frac{HD(R(i), R(j))}{L} \times 100\% \quad (10)$$

由此,唯一性可表示为^[29]

$$\text{Uniqueness} = (1 - |2P_{\text{inter}} - 1|) \times 100\% \quad (11)$$

所提 PUF 平均 HD 的统计直方图 (包含拟合曲线) 如图 10 所示,归一化平均片内和片间 HD 分别为 0.034 3 和 0.501 8 (对应的唯一性为 99.64%, 接近理想值 100%)。因此,本文所提 PUF 具有良好的唯一性。

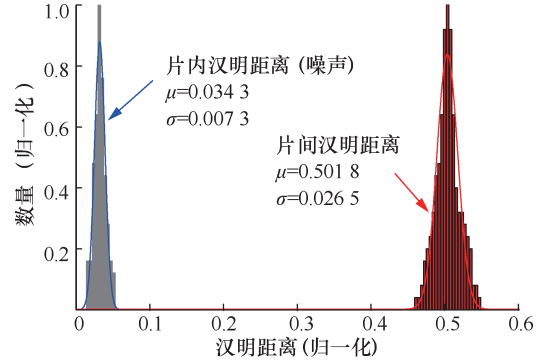


图10 片内汉明距离与片间汉明距离统计直方图
Figure 10 Statistical histogram of inter- and intra-PUF HD

4.3 可靠性

可靠性通常采用平均片内 HD 来衡量,即通过同一 PUF 在不同环境下 (相同激励) 输出响应的片内 HD 统计特性来衡量。这里用 P_{intra} 表示在多次实验中输出响应位发生翻转的概率,即整个 L 位输出响应的片内 HD 变化。平均片内 HD 的期望值可表示为

$$P_{\text{intra}} = \frac{1}{m} \sum_{i=1}^m \frac{HD(R, R')}{L} \times 100\% \quad (12)$$

可靠性可表示为

$$\text{Reliability} = (1 - P_{\text{intra}}) \times 100\% \quad (13)$$

平均片内 HD 统计直方图如图 9 所示,归一化片内 HD 为 0.034 3 (对应的可靠性为 96.6%, 接近理想值 100%)。因此所提 PUF 具有良好的可靠性。

此外,该 PUF 在常温常压下 5 000 次循环读取,其输出响应的最大、最小和平均误码率的统计特性如图 11 所示。可以发现,平均误码率和最大误码率在 1 000 次评估后开始平稳,并随着评估次数增大趋于稳定,最终分别稳定在 3.4% 和 4.8%。而最小误码率随着评估次数增大逐渐减小,在评估次数足够大的情况下接近 0。

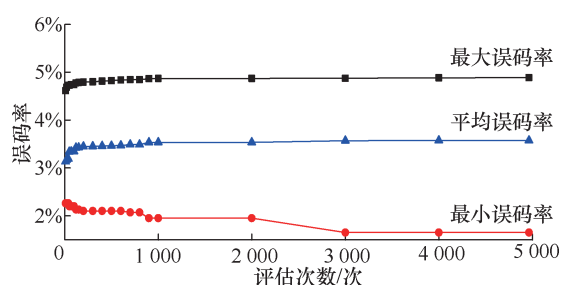


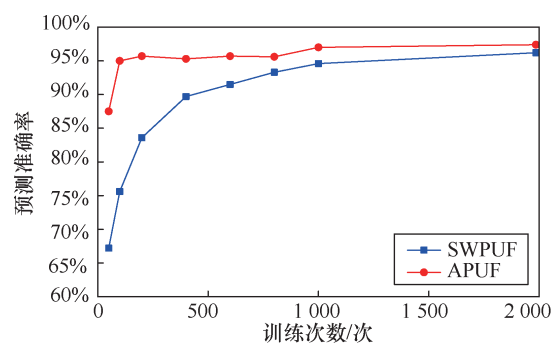
图11 误码率与评估次数的关系
Figure 11 Relationship between BER and evaluations

4.4 抗攻击能力

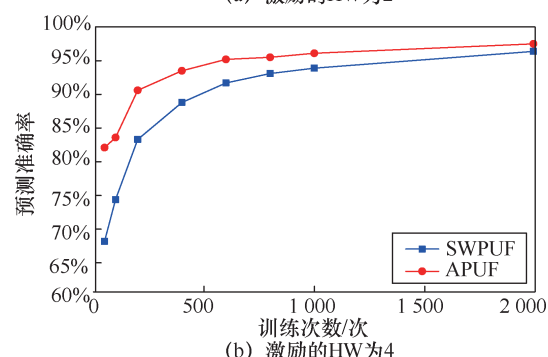
随着研究人员对 PUF 的深入探索, 针对 PUF 的攻击技术越来越多, 如侧信道攻击、建模攻击、机器学习攻击等。其中, 通常使用基于机器学习的建模攻击来分析 PUF 电路的抗攻击能力。通过这一方法攻击者首先收集部分 CRP 来建立 PUF 预测模型, 接着利用训练集中的响应与预测响应得到预测准确率, 最后判断 PUF 电路的安全性。常见的机器学习分析方法主要包括逻辑回归 (LR, logic register)、支持向量机、随机森林、神经网络等^[22]。

本文采用 LR 算法对 SWPUF 的抗攻击能力进行分析, 并与 APUF 进行比较。为显示该 PUF 在不同汉明重量下的抗攻击能力优势, 实验选取不同汉明重量下的 CRP 进行训练, 预测精度与训练次数的关系如图 12 所示。当训练次数较少时, SWPUF 预测准确率远低于 APUF。HW=2 时, SWPUF 与 APUF 的预测准确率分别为 67.2% 和 87.5%; HW=4 时, 分别为 68.2% 和 82.1%。然而,

随着训练次数逐渐增加, SWPUF 的优势逐渐减小。可见在训练次数和汉明重量较小的情况下, SWPUF 的预测准确性明显低于 APUF, 具有更好的抗攻击能力。



(a) 激励的HW为2



(b) 激励的HW为4

图12 不同HW和训练次数下SWPUF与APUF的预测准确率
Figure 12 Comparison of prediction accuracy of SWPUF and APUF with different HW

4.5 性能比较

本文所提 SWPUF 的测试性能与其他相关工作对比如表 4 所示, 该 PUF 在随机性、唯一性和可靠

表4 SWPUF 性能与相关文献比较
Table 4 Comparison of SWPUF and related literatures

对比文献	随机性	唯一性	可靠性	响应位数	实现方式	工艺/nm
Racing APUF ^[30]	92.6%	—	91.6%	—	FPGA	65
multi-line APUF ^[31]	99.4%	93%	99.9%	64	FPGA	65
APUF ^[32]	90.4%	92.8%	99.3%	64	FPGA	65
DAPUF ^[32]	91.4%	82.6%	90.2%	64	FPGA	65
XRBR PUF ^[33]	—	81.34%	98.22%	—	FPGA	45
XRRO PUF ^[33]	—	97.52%	97.72%	—	FPGA	45
RO PUF ^[18]	84.58%	96.02%	98.25%	1024	FPGA	28
Zhang PUF ^[34]	89.8%	99.2%	96.3%	64	FPGA	28
基于延迟的 PUF ^[35]	90.8%	99.4%	96.8%	64	FPGA	28
FF-APUF ^[36]	80%	83.06%	97.1%	64	FPGA	28
本文所提 SWPUF	96.98%	99.64%	96.6%	256	FPGA	28

注：“—”表示无法获得。

性（常温常压下）方面均具有一定优势^[18,30-36]。其中，随机性、唯一性和可靠性的理想值均为 100%。与文献[32]相比，所提 PUF 在随机性和唯一性上分别提高了 6.58%和 6.84%。与文献[34]相比，相同工艺下所提 PUF 在随机性、唯一性和可靠性上分别提高了 7.18%、0.44%和 0.3%。与文献[35]和文献[36]相比，所提 PUF 在随机性上具有明显优势，分别提高了 16.18%和 16.98%。与文献[35]和文献[36]相比，唯一性分别提高了 0.24%和 16.58%。

5 结束语

通过分析强、弱 PUF 在具体设计时存在的不足，提出一种基于 FPGA 的新型强弱混合型 SWPUF 电路设计方案。该 PUF 可根据输入激励的 HW，在电路运行过程中选择不同的开关单元数，利用同一 PUF 电路拓扑结构实现强、弱 PUF 有机统一。实验结果表明，所提 PUF 具有良好的随机性、唯一性和可靠性（常温常压下）。使用基于 LR 的攻击方法对所提 PUF 进行抗攻击能力分析，在训练集和 HW 较小的情况下 SWPUF 具有比传统 APUF 更好的抗攻击能力。该 PUF 克服了传统强、弱 PUF 分立设计的不足，一定程度上扩展了 PUF 电路的应用范围。

参考文献

- [1] PAPPU R, RECHT B, TAYLOR J, et al. Physical one-way functions[J]. *Science*, 2002, 297(5589): 2026-2030.
- [2] ZHANG J. A practical logic obfuscation technique for hardware security[J]. *IEEE Transactions on Very Large Scale Integration Systems*, 2016, 24(3): 1193-1197.
- [3] ZHANG J, LIN Y, YU Y, et al. A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing[J]. *IEEE Transactions on Information Forensics & Security*, 2017, 10(6): 1137-1150.
- [4] CHEN B, WILLEMS J. Secret key generation over biased physical unclonable functions with polar codes[J]. *IEEE Internet of Things Journal*, 2019, 6(1), 435-445.
- [5] USMANI M A, KESHAVER S, MATTHEWS E, et al. Efficient PUF-based key generation in FPGAs using per-device configuration[J]. *IEEE Transactions on Very Large Scale Integration Systems*, 2019, 27(2): 1-12.
- [6] KARPINSKY B, LEE Y, CHOI Y, et al. 8.7 Physically unclonable function for secure key generation with a key error rate of $2e-38$ in 45nm smart-card chips[C]//Solid-state Circuits Conference. 2016: 158-160.
- [7] TEHRANIPOOR F, KARIMIAN N, YAN W, et al. DRAM-based intrinsic physically unclonable functions for system-level security and authentication[J]. *IEEE Transactions on Very Large Scale Integration Systems*, 2017, 25(3): 1085-1097.
- [8] YAN W, TEHRANIPOOR F, CHANDY J. PUF-based fuzzy authentication without error correcting codes[J]. *IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems*, 2017, 36(9): 1445-1457.
- [9] AMAN M, TANEJA S, SIKDAR B, et al. Token-based security for the internet of things with dynamic energy-quality tradeoff[J]. *IEEE Internet of Things Journal*, 2019, 6(2): 2843-2859.
- [10] BAIBHAB C, DEBAYAN D, SHO VAN M, et al. RF-PUF: enhancing IoT security through authentication of wireless nodes using in-situ machine learning[J]. *IEEE Internet of Things Journal*, 2019, 6(1): 388-398.
- [11] SHIFMAN Y, MILLER A, WEIZMAN Y, et al. An SRAM PUF with 2 independent bits cell in 65nm[C]. 2019 IEEE International Symposium on Circuits and Systems (ISCAS), 2019: 1-5.
- [12] LI G, WANG P, MA X, et al. A 215-F² bistable physically unclonable function with an ACF of <0.005 and a native bit instability of 2.05% in 65-nm CMOS process[J]. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2020, 28(11): 2290-2299.
- [13] LU L, KIM T. A sequence-dependent configurable PUF based on 6T SRAM for enhanced challenge response space[C]//2019 IEEE International Symposium on Circuits and Systems (ISCAS). 2019: 1-5.
- [14] KUMAR 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. 2008: 67-70.
- [15] TUYLS P, SCHRIJEN J, SKORIC B, et al. Read-proof hardware from protective coatings[C]//Cryptographic Hardware and Embedded Systems (CHES). 2006: 369-383.
- [16] DAI Y, SAKIYAMA K, IWAMOTO M, et al. Uniqueness enhancement of PUF responses based on the locations of random outputting RS latches[C]//Cryptographic Hardware & Embedded Systems-International Workshop. 2011: 390-406.
- [17] LI G, WANG P, MA X, et al. A multimode configurable physically unclonable function with bit-instability-screening and power-gating strategies[J]. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*.
- [18] 李雪莹, 李磊, 胡剑浩, 等. 基于 RO 电路变化 PUF 的 FPGA 实现[J]. *电子技术应用*, 2018, 44(5): 39-42.
- [19] LI X, LI L, HU J, et al. An RO-PUF design based on FPGA[J]. *Application of Electronic Technique*, 2018, 44(5): 39-42.
- [19] GAO Y, MA H, AL-SARAWI F, et al. PUF-FSM: a controlled strong PUF[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2018, 37(5): 1104-1108.
- [20] DUBROVA E. A reconfigurable arbiter PUF with 4×4 switch blocks[C]//2018 IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL). 2018: 31-37.
- [21] WEN J, HUANG M, CHEN Z, et al. A multi-line arbiter PUF with improved reliability and uniqueness[C]//2019 IEEE 4th International Conference on Signal and Image Processing (ICSIP). 2019: 641-648.
- [22] GU C, LIU W, CUI Y, et al. A flip-flop based arbiter physical unclonable function (APUF) design with high entropy and uniqueness for FPGA implementation[J]. *IEEE Transactions on Emerging Topics in Computing*, 2019.

- [23] HE Z, WAN M, DENG J, et al. A reliable strong PUF based on switched-capacitor circuit[J]. IEEE Trans Very Large Scale Integr. (VLSI) Syst, 2018, 26(6): 1073-1083.
- [24] ZHANG J. Physical unclonable function-based key sharing for IoT security[J]. IEEE Transactions on Industrial Electronics, 2020, 67(8): 7025-7033.
- [25] 刘伟强, 崔益军, 王成华. 一种低成本物理不可克隆函数结构的设计实现及其 RFID 应用[J]. 电子学报, 2016, 44(7): 1772-1776.
LIU W, CUI Y, WANG C. Design and implementation of a low cost physical unclonable function structure and its RFID application[J]. Acta Electronica Sinica, 2016, 44(7): 1772-1776.
- [26] GU C, LIU W, HANLEY N, et al. A theoretical model to link uniqueness and min-entropy for PUF evaluations[J]. IEEE Transactions on Computers, 2019, 68(2): 287-293.
- [27] LIM D, LEE J, GASSEND B, et al. Extracting secret keys from integrated circuits[J]. IEEE Transactions on Very Large Scale Integration Systems, 2005, 13(10): 1200-1205.
- [28] SHI J, LU Y, ZHANG J. Approximation attacks on strong PUFs[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39(10): 2138-2151.
- [29] LAO Y, PARHI K. Statistical analysis of MUX-based physical unclonable functions[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014, 33(5): 649-662.
- [30] LI Z, ZHU L, HUANG M, et al. Racing APUF: a novel APUF against machine learning attack with high reliability[C]//2019 IEEE 4th International Conference on Signal and Image Processing (IC-SIP). 2019: 722-726.
- [31] WEN J, HUANG M, CHEN Z, et al. A multi-line arbiter PUF with improved reliability and uniqueness[C]//2019 IEEE 4th International Conference on Signal and Image Processing (ICSIP), 2019: 641-648.
- [32] TAKANORI M, DAI Y, MITSUGU I, et al. A new arbiter PUF for enhancing unpredictability on FPGA[J]. The Scientific World Journal, 2015(2015): 1-13.
- [33] LIU W, ZHANG L, ZHANG Z, et al. XOR-based low-cost reconfigurable PUFs for IoT security[J]. ACM Transactions on Embedded Computing Systems. 2019, 18(3): 1-21.
- [34] ZHANG J, WU Q, DING Y, et al. Techniques for design and implementation of an FPGA-specific physical unclonable function[J]. Journal of Computer Science and Technology, 2016, 31(1): 124-136.
- [35] ZHANG J, LIN Y, LYU Y, et al. FPGA IP protection by binding finite state machine to physical unclonable function[C]//2013 23rd International Conference on Field programmable Logic and Applications. 2013: 1-4.
- [36] GU C, CUI Y, HANLEY N, et al. Novel lightweight FF-APUF design for FPGA[C]//2016 IEEE International System-on-Chip Conference (SOCC), 2016: 75-80.

[作者简介]



连佳娜(1996-), 女, 浙江绍兴人, 温州大学硕士生, 主要研究方向为物理不可克隆函数攻击与防御。



汪鹏君(1966-), 男, 浙江宁波人, 温州大学教授、博士生导师, 主要研究方向为低功耗、高信息密度集成电路理论 and 设计技术、电路设计综合和优化技术、安全芯片理论和设计技术。



李刚(1988-), 男, 陕西汉中, 温州大学讲师, 主要研究方向为密码芯片攻击和防御理论及其 VLSI 实现、存储计算、数字电路逻辑综合与优化。



马雪娇(1991-), 女, 河北秦皇岛人, 主要研究方向为数字电路逻辑综合与优化、硬件混淆技术。



翟官宝(1998-), 男, 浙江衢州人, 温州大学硕士生, 主要研究方向为物理不可克隆函数攻击与防御。