文章编号：2095-4980(2025)07-0748-07

基于延时可控的双边沿APUF电路设计

江佳琳，周子宇，李　刚，汪鹏君*

(温州大学 电气与电子工程学院，浙江 温州 325006)

摘　要：物理不可克隆函数(PUF)是一种实用性极强的硬件安全原语，广泛应用于物联网设备认证等信息安全领域。然而强PUF的输入输出之间关联性较强，易受到机器学习(ML)算法的攻击。为此，通过对延时可控单元和双边沿触发机理的研究，提出一种基于延时可控的双边沿仲裁器PUF(APUF)电路。通过延时可控开关电路，优化APUF的路径，调节电路延迟偏差以降低激励响应对(CRP)间的相关性；采用上升沿和下降沿仲裁器分别采集PUF电路双边沿延时响应，成倍提高APUF的CRP数量，以提高信息熵利用率；基于TSMC 65 nm CMOS工艺及Cadence Virtuoso设计平台，全定制设计电路与版图。实验结果表明：电路的逻辑功能正确，PUF的唯一性和可靠性分别为51.01%和0.025 57，且对应逻辑回归(LR)、支持向量机(SVM)、人工神经网络(ANN)和轻量梯度提升机(Light GBM)算法的ML攻击预测率为59.71%、62.75%、86.00%和80.92%，相较APUF抗ML能力显著提升。

关键词：物理不可克隆函数；延时可控；双边沿触发；机器学习；物联网安全

中图分类号：TN47　　**文献标志码：**A　　**DOI：**10.11805/TKYDA2024129

Dual-edge APUF circuit design based on controllable delay time

JIANG Jialin，ZHOU Ziyu，LI Gang，WANG Pengjun*

(Institute of Electrical and Electronic Engineering，Wenzhou University，Wenzhou Zhejiang 325006，China)

Abstract：Physical Unclonable Function(PUF) is a highly practical hardware security primitive that can be widely used in information security fields such as IoT device authentication. However, the strong PUF has strong correlation between inputs and outputs, which makes it vulnerable to attacks by Machine Learning(ML) algorithms. In view of this, a delay-controllable dual-edge Arbiter PUF(APUF) circuit based on the delay-controllable unit and dual-edge triggering mechanism is proposed. Firstly, a delay-controllable switching circuit is employed to optimize the path of the conventional APUF and adjust the circuit delay deviation to reduce the correlation between the Challenge-Response Pair(CRP). Secondly, a rising-edge arbiter and a falling-edge arbiter are employed to capture the dual-edge delay response of the PUF circuit respectively, which double increases the number of pairs of CRP of the PUF. Finally, a dual-edge arbiter PUF circuit is proposed based on the TSMC 65 nm CMOS process and the Cadence Virtuoso design platform, the circuit and layout are realized in a fully customized way. The experimental results show that the logic function of the circuit is correct, the uniqueness and reliability of the PUF are 51.01% and 0.025 57 respectively. And the prediction rates of ML attacks corresponding to Logistic Regression(LR), Support Vector Machine(SVM), Artificial Neural Network(ANN) and Light Gradient Boosting Machine(Light GBM) algorithms are 59.71%, 62.75%, 86.00% and 80.92%, the resistance to ML attack is significantly improved.

收稿日期：2024-03-07；**修回日期：**2024-03-19

基金项目：国家自然科学基金资助项目(62234008；62374117)

***通信作者：**汪鹏君　email:wangpengjun@wzu.edu.cn

引用格式：江佳琳,周子宇,李刚,等. 基于延时可控的双边沿APUF电路设计[J]. 太赫兹科学与电子信息学报，2025,23(7):748-754. DOI:10.11805/TKYDA2024129.

Citation format：JIANG Jialin,ZHOU Ziyu,LI Gang,et al. Dual-edge APUF circuit design based on controllable delay time[J]. Journal of Terahertz Science and Electronic Information Technology，2025,23(7):748-754. DOI:10.11805/TKYDA2024129.

Keywords：Physical Unclonable Function(PUF)；delay-controllable；dual-edge triggering；Machine Learning(ML)；internet of things security

随着通信技术和集成电路技术的飞速发展，人类社会进入万物感知、万物互联的全新时代，而信息与隐私安全问题愈发受到关注。PUF是一种新兴的信息安全技术[1]，可应用于安全密钥生成与低成本认证等领域[2-3]。多数传统的加密方式依赖于存储在闪存或非易失性存储器中的安全密钥，并通过对比完成解密，此方法容易受到物理探针、侧信道、逆向工程等攻击而泄露信息。PUF通过读取硬件制造时产生的微小差异，以非存储的方式生成不可预测的安全信息，故极大降低信息泄露风险。PUF输入信号称为激励，输出信号称为响应，对于两个结构相同的PUF，同一激励作用产生的响应信号依旧差异明显。PUF根据产生不同量级激励响应对(CRP)的能力，可分为弱PUF[4-5]和强PUF[6]两大类。由于弱PUF仅能产生有限少量CRP，故主要用于密钥生成，而强PUF通过硬件资源重构可产生大量CRP，适用于设备认证和状态证明等方面。

然而，强PUF因输入输出间存在相关性，易受到机器学习(ML)攻击。常用ML算法如逻辑回归(LR)、支持向量机(SVM)、人工神经网络(ANN)和LightGBM等都对其有巨大威胁。攻击者通过收集强PUF的CRP数据构建数学模型，即可预测任意激励信号的响应。一旦激励和响应之间的映射关系被建模，密钥就将被盗取。为提升PUF电路的安全性能，近年来学者们相继提出诸多防御技术。文献[7]提出一种基于纳米级晶体管陷阱发射概率的强PUF，通过在响应中混合随机比特的方式减少CRP空间，解决PUF抗ML攻击能力弱、存储开销高、可靠性低等问题。文献[8]提出一种轻量级密钥管理方案，通过新型的双层网格部署模型并采用双阶段的密钥信息分配算法，大幅提高电力信息网络的抗捕获性能。文献[9]针对强PUF抗攻击电路硬件开销大的问题，通过响应预处理激励并利用S-box执行深度非线性混淆，实现高度可靠和安全的轻量级PUF，降低硬件开销。上述抗ML攻击方法只对激励或响应进行预处理操作，虽可在一定程度上增强PUF的抗ML攻击能力，但攻击者窃取PUF电路对CRP的预处理方式后，可逆向推导出原激励响应并实施有效ML攻击。

鉴此，本文提出一种基于延时可控的双边沿仲裁器PUF(APUF)电路，通过优化后的开关组件逐级调节电路延迟偏差，以降低激励响应间的线性度。此外利用双边沿采样，成倍增加PUF电路的CRP数量，以提高信息熵利用率。

1　传统APUF原理分析

APUF电路如图1所示，延时结构主要由n级路径选择延时单元构成，同一级的两个延时单元共享一个激励信号，激励信号的“0”或“1”分别决定信号路径为平行传输或交叉传输。触发信号通过对称路径的传输延时相同，但实际生产过程工艺偏差会导致单元电路延时不一致，触发信号经过不同延时路径累积后先后到达仲裁器端，经仲裁器判决输出响应0或1。将APUF上下路径之间的最终延迟差Δ定义为$\Delta=\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{\phi}$，其中$\boldsymbol{\omega}$表示APUF每级路径选择模块中传播延迟的特征向量$\{\omega^1,\omega^2,\cdots,\omega^n,\omega^{n+1}\}$，$\omega^1=(\sigma_1^0-\sigma_1^1)/2$，$\omega^i=(\sigma_{i-1}^0-\sigma_{i-1}^1+\sigma_i^0-\sigma_i^1)/2$，$i=2,3,\cdots,n$，$\omega^{n+1}=(\sigma_n^0-\sigma_n^1)/2$，$\sigma_i$表示第$i$级路径选择模块的延迟，$\sigma_i^0$表示信号并行通传输，$\sigma_i^1$表示信号交叉传输。向量$\boldsymbol{\phi}$通过激励$\boldsymbol{C}=c_1,c_2,c_3,\cdots,c_n$进行组合运算得到$\boldsymbol{\phi}(\boldsymbol{C})=\{\phi^1(\boldsymbol{C}),\phi^2(\boldsymbol{C}),\cdots,\phi^n(\boldsymbol{C}),1\}^{\mathrm{T}}$，其中向量$\phi^j(\boldsymbol{C})$表示为：

$$\phi^j(\boldsymbol{C})=\prod_{i=j}^{n}(1-2C_i),j=1,2,\cdots,n \tag{1}$$

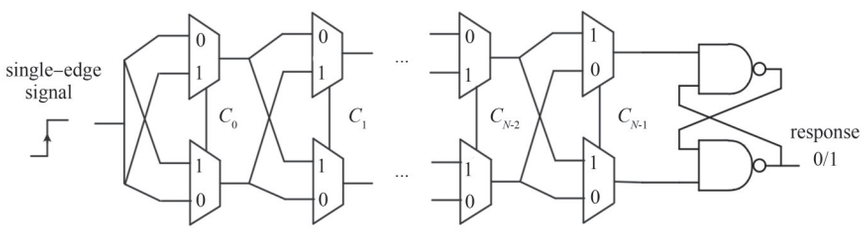


Fig.1 Schematic diagram of APUF circuit structure
图1 APUF电路结构原理图

2　延时可控单元电路设计

APUF电路总延时为各级延时的累加，因此，控制各级延时的激励信号与表示总延时特征的响应信号之间有

很强的线性关系。为抵御ML攻击，需削弱各级路径延迟与最终响应间的相关性。延时可控单元通过调节偏置电压改变各路径的延迟时间，可有效降低各路径模块间的相关性，以及由激励控制的路径与最终响应间的相关性。延时可控的开关电路由P沟道金属氧化物半导体(P-channel Metal-Oxide-Semiconductor，PMOS)晶体管网络和N沟道金属氧化物半导体(N-channel Metal-Oxide-Semiconductor，NMOS)晶体管网络组成，包含偏置单元和延时单元，其中偏置单元可调节路径中信号经反相器的延时至合适的范围内。如图2所示，激励控制延时单元实现对加载输入信号的平行传输或交叉传输的信号传输模式转换，同时，偏置单元受偏置电压U_{BIAS}控制，实现对输入信号的延时调控。在开关组件电路中，各级晶体管最终构成两条理论相等的路径延时单元。随着偏置单元反相器输出端口电压值升高，延时单元电路的NMOS管不完全导通，呈关断趋势，其流经电流也随之下降。同时，该门电路的PMOS管从完全关断状态逐渐变为开启状态，流经PMOS管电流逐渐增大，触发信号经门电路传输得到增强。与传输门结构相比，受制造噪声影响造成的单位延时偏差更为显著。

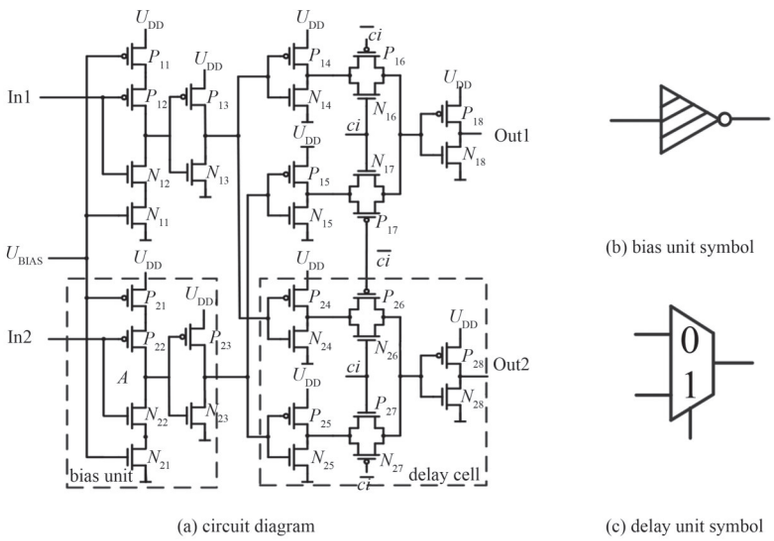


Fig.2 Delay time controllable unit circuit

图2 延时可控单元电路

路径单元的延时受偏置电压影响，随着偏置电压的变化呈现不同工作状态[10]。为导通下拉网络NMOS器件，其栅源电压需大于阈值电压U_{th}。此处$U_{\mathrm{GS-22}}=U_{\mathrm{In2}}-U_{\mathrm{DS-21}}$，$U_{\mathrm{GS-21}}=U_{\mathrm{BIAS}}$。由于体效应的缘故，晶体管$N_{22}$的阈值电压将高于晶体管$N_{21}$。下拉网络NMOS器件阈值电压为：

$$U_{\mathrm{th2}}=U_{\mathrm{th0}}+\gamma\left(\left(\sqrt{\left|2\Phi_{\mathrm{f}}\right|+U_{\mathrm{SB}}}\right)-\sqrt{\left|2\Phi_{\mathrm{f}}\right|}\right) \tag{2}$$

式中：U_{Th0}为U_{SB}=0时的阈值电压；Φ_{f}为硅衬底费米势；γ为体效应系数。同时，亚阈值电流随过驱动电压升高指数增加。亚阈值电流随源漏电压U_{DS}增大而增加，亚阈值电流为：

$$I_{\mathrm{DS}}=I_0\mathrm{e}^{\frac{U_{\mathrm{BIAS}}-U_{\mathrm{S}}-U_{\mathrm{th}}}{nkT/q}}\left(1-\mathrm{e}^{-\frac{U_{\mathrm{DS}}}{kT/q}}\right) \tag{3}$$

式中：I_0为预设常数，$I_0\propto k'W/L$，W/L为晶体管的长宽比；k'为工艺跨导参数，$k'=\mu C_{\mathrm{ox}}=\mu\varepsilon_{\mathrm{ox}}/t_{\mathrm{ox}}$，$\mu$为迁移率；$C_{\mathrm{ox}}$为栅氧的单位面积电容；$\varepsilon_{\mathrm{ox}}$=3.97×$\varepsilon_{\mathrm{o}}$=3.5×$10^{-11}$F/m为氧化层的介电常数，$t_{\mathrm{ox}}$为氧化层厚度；$n$为亚阈值栅耦合系数，常用值为1.4~1.5；$k$为玻尔兹曼常数；$T$为工作温度；$T$(K)=273.15+$t$(℃)；$q$为电子电量。

当U_{DS}>>kT/q时，源漏电流I_{DS}为：

$$I_{\mathrm{DS}}=I_0\mathrm{e}^{\frac{U_{\mathrm{BIAS}}-U_{\mathrm{S}}-U_{\mathrm{th}}}{nkT/q}} \tag{4}$$

当U_{BIAS}为低电压且输入电压U_{in}均为0时，处于PMOS网络的晶体管同时导通，此时U_{BIAS}对于PMOS管作用更明显，PMOS管驱动能力强于NMOS管驱动能力，PMOS管导通电流更大，PMOS网络充电能力强于NMOS网络放电能力，触发信号上升速度始终快于下降速度，信号A上升沿延迟时间t_{u}减少，信号OUT下降沿延迟时间t_{d}减少。当U_{BIAS}为亚阈值电压时，偏置晶体管在亚阈值区工作，偏置单元互补CMOS网络因处于弱导通状态进入电流饥饿型反相器工作模式，此时PMOS管驱动能力与NMOS管驱动能力平衡，PMOS管和NMOS管导通电流相

近，PMOS 网络充电能力与 NMOS 网络放电能力相近，触发信号上升速度与下降速度相近，信号 A 和信号 OUT 上升沿延迟时间 t_u 与下降沿延迟时间 t_d 接近。当 U_{BIAS} 为高电压且输入电压 U_{in} 均为 1 时，处于 NMOS 网络的晶体管同时导通，此时 U_{BIAS} 对于 NMOS 管作用更明显，NMOS 管驱动能力强于 PMOS 管驱动能力，NMOS 管导通电流更大，NMOS 网络放电能力强于 PMOS 网络充电能力，触发信号下降速度始终快于上升速度，信号 A 下降沿延迟时间 t_d 减少，信号 OUT 上升沿延迟时间 t_u 减少。每级偏置单元的下降沿延迟时间为：

$$t_d = \frac{C_d U_{DD}}{\eta I_{DS}} \tag{5}$$

式中：C_d 为总负载电容；U_{DD} 为电源电压；ηI_{DS} 为平均电流，η 为给定反相器的固定参数，每级偏置单元的下降沿延迟时间与上升沿时间成反比。

3　双边沿 APUF 电路设计

强 PUF 在物联网认证协议中常作为反映身份信息的密钥使用，根据密钥长度需提供对应数量的 CRP 以保证系统的运行。所需 CRP 越多，攻击者能采集到的 CRP 信息越多，抗攻击能力越弱[11]。故在同一激励作用下，若能产生更多的响应，所需 CRP 数量则更少，攻击者能采集到的 CRP 数量更少，PUF 的抗攻击能力更强。APUF 电路通过单个仲裁器采集信号上升沿延时，故一组激励只对应一位响应。由于路径模块相互独立，分别采集同一激励的不同路径差产生的响应，可实现响应数目翻倍的效果。采用双边沿采样技术[12]，触发信号送至 PUF 输入端，通过调节偏置电压源的输入改变 PUF 电路充放电时间，进而调节 PUF 响应端双边沿信号的延迟时间，生成有效双边沿响应，并引入两类仲裁器采集成倍输出的 PUF 响应。

双边沿 APUF 电路由 m 级路径单元和双边沿仲裁器组成，电路结构如图 3 所示。其中 m 级路径单元构成延时路径，可在 m 位激励作用下实现不同延时功能。双边沿仲裁器采用两个与非门和两个或非门构成的 RS(Reset/Set) 触发器结构，分别负责判决、采集该 PUF 上升沿、下降沿的延迟偏差。当路径延迟偏差达到识别阈值时，若上级信号先到达响应端，判决结果为响应 R=1，若下级信号先到达响应端，判决结果为响应 R=0。在实际应用中，每个开关组件都作为一个独立 PUF 单元，以上级延时信号和激励作为输入，延时后的信号作为输出，最终得到路径的总延时差。在双边沿 APUF 电路结构中，信号沿两种路径传输至仲裁器端存在不同延迟偏差，经双边沿仲裁器分别得到两倍响应，无需增加熵源即可提升响应数量。

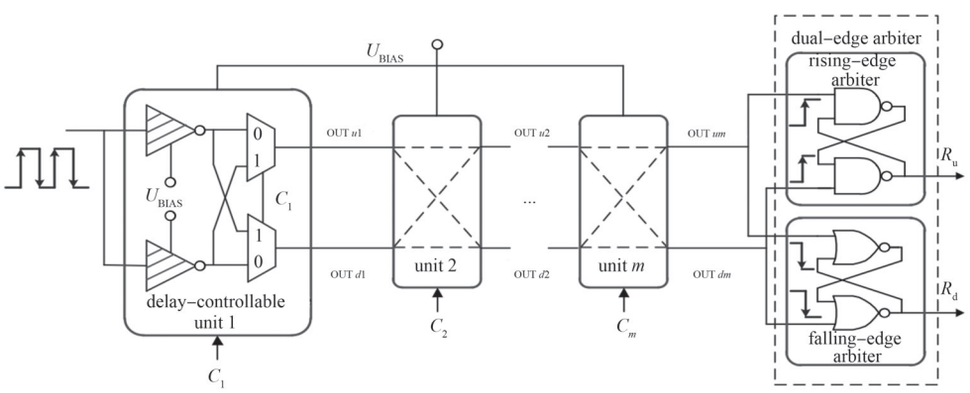


Fig.3 Dual−edge APUF circuit with controllable delay time
图 3　延时可控的双边沿 APUF 电路

4　实验结果与分析

本文利用蒙特卡罗仿真评估延时可控的双边沿 APUF 电路性能，分析 PUF 电路的输出响应唯一性、可靠性和抗 ML 攻击能力。采用台积电 65 nm 互补金属氧化物半导体(Complementary Metal−Oxide−Semiconductor，CMOS)工艺设计，使用 Calibre 软件提取寄生参数，Spectre 仿真器进行前仿和后仿，Cadence Virtuoso 设计平台验证逻辑功能正确。

4.1　抗攻击能力

由于基于路径延时的强 PUF 激励信号与响应信号之间存在一一对应的函数关系，且响应信号通常只有 0 或

1 两种情况。因此针对典型强 PUF 结构进行 ML 建模攻击，主要根据响应信号值的不同对激励信号进行分类，并依据两者之间关系构建模型，在经过一定数量 CRP 的训练之后，优化模型参数以达到最好效果。得到分类函数即预测模型后，将测试用 CRP 代入此模型可判断是否正确分类，最终预测率为预测正确的 CRP 数与总测试 CRP 数的比值，预测率越高表明攻击性能越好[12]。

通过 ML 方法测试延时可控的双边沿 APUF 电路抗攻击能力。图 4 给出当训练集达到 50 000 组时，对应 LR、SVM、ANN 和 LightGBM 算法攻击的结果，APUF 的预测率分别为 98.18%、97.31%、97.72% 和 96.41%，而所设计双边沿 PUF 的最高预测率仅分别为 59.71%、62.75%、86.00% 和 80.92%，较 APUF 抗 ML 攻击能力明显提升。VBPUF 表示可变偏置 PUF。

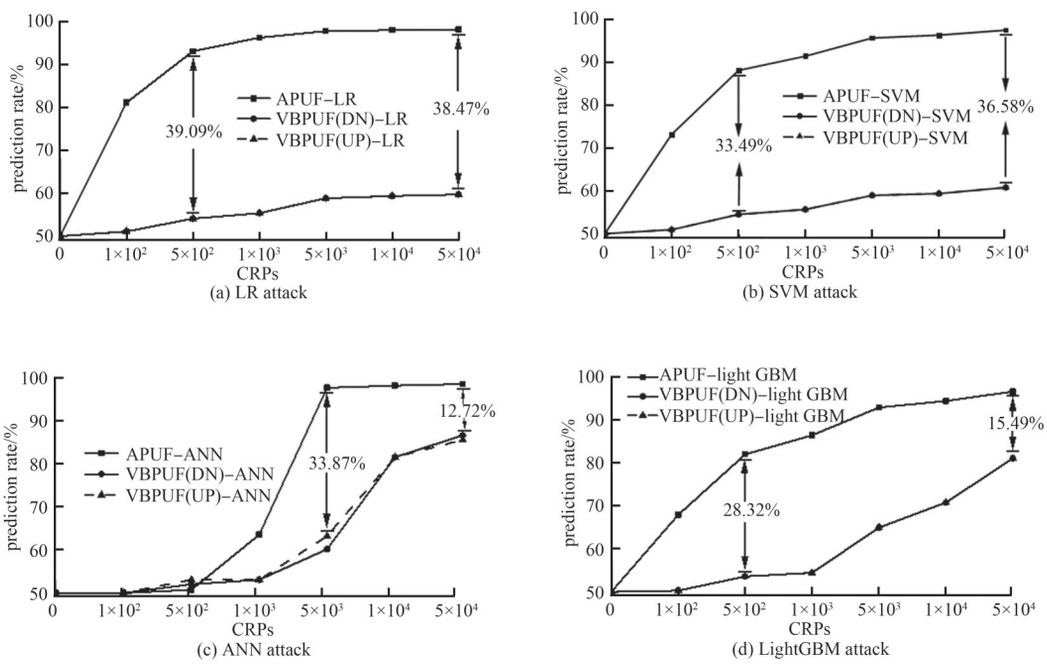


Fig. 4 Prediction rate of ML attack

图4 ML攻击预测率

4.2 随机性

PUF 电路的熵源来自随机噪声，使得电路能生成具有随机性的密钥，密钥随机性越高则所包含的信息量越多。其中，美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)SP800–22 测试常用以评估 PUF 响应的随机性。不同于离散混沌映射的 NIST 测试，本文提出的 PUF 响应并非基于混沌系统连续值序列离散化后的二进制序列，无需依赖 NIST 测试套件中的统计测试对 PUF 响应生成的序列进行随机性检验[13]。将电路生成的 100 000 bit 响应序列作为 NIST 输入，上述响应被分成 10 个独立比特流数据并执行 NIST 测试，结果如表 1 所示。当生成比特流的 P 值大于 0.01 时，表明测试通过。由表 1 可知，该 PUF 生成响应通过大部分测试项，具有良好的随机性。

表1 本文PUF的随机性NIST测试结果

Table1 NIST test results of Randomness for the proposed PUF

test name	P–value	pass rate/(%)
frequency	0.350 485	90
block frequency	0.534 146	100
runs	0.534 146	90
rank	0.213 309	100
longest runs	0.911 413	100
Fast Fourier Transform	0.739 918	100
cumulative sums	0.122 325	100
non–overlapping	0.017 912	100
overlapping template	0.350 485	100
serial	0.350 485	100
approximate entropy	0.002 043	70
linear complexity	0.739 918	90

4.3 唯一性和可靠性

唯一性表示不同 PUF 输出响应之间的差异，可用片间汉明距离(Inter Hamming Distance，Inter HD)衡量。m 组不同 PUF 电路响应的平均片间 HD 可以表示为：

$$E\left(HD_{\text{inter}}\right)=\frac{2}{m(m-1)}\sum_{u=1}^{m-1}\sum_{v=u+1}^{m}\frac{HD\left(R_u,R_v\right)}{n}\times 100\% \quad (6)$$

式中：R_u和R_v分别表示第u和第v个PUF在相同激励作用下生成的n比特响应。分别在U_{BIAS}=400 mV、600 mV，U_{DD}=1.2 V，T=27 ℃条件下，实施20次蒙特卡罗仿真，每次输入10 000组CRP测量上升沿、下降沿的片间HD。如图5所示，该延时可控PUF电路的双边沿片间HD均值为51.01%，接近理想均值50%，具有良好的唯一性。

可靠性是指电路在不同工作条件下获得相同输出的能力，可通过片内HD量化，m组PUF电路响应的片内HD可表示为：

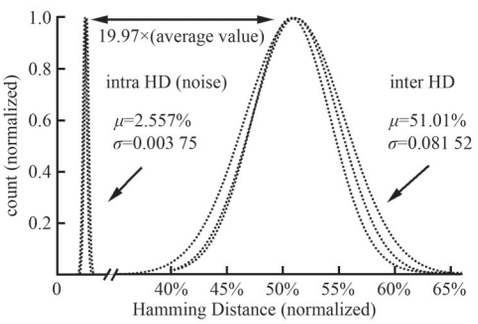


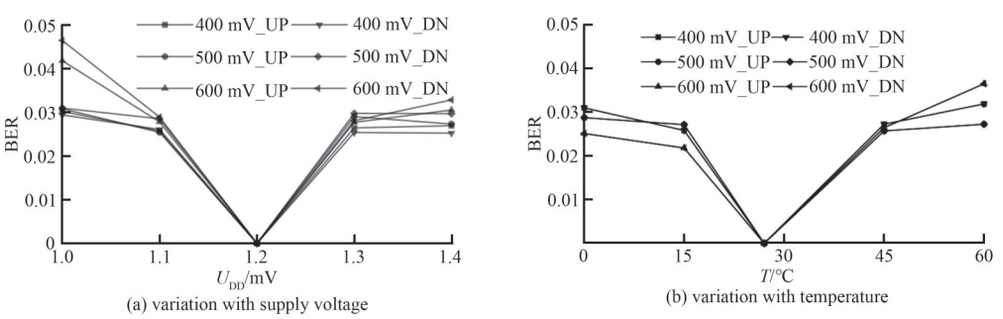
Fig.5 Distribution curves of inter-slice HD and intra-slice HD
图5 片间HD和片内HD分布曲线

$$E\left(HD_{\text{intra}}\right)=\frac{1}{m}\sum_{i=1}^{m}\frac{HD\left(R_{g,i}R_{e,i}\right)}{n}\times 100\% \quad (7)$$

式中：$R_{g,i}$和$R_{e,i}$分别表示同一个PUF在相同激励作用下生成的n bit响应；m为重复次数。分别在U_{BIAS}=400 mV、600 mV，U_{DD}=1.2 V，T=27 ℃条件下，实施20次蒙特卡罗仿真，添加6 MHz噪声，每次输入4 000组CRP测量片内HD。如图5所示，该延时可控PUF电路的双边沿片内HD均值为0.025 57，接近理想均值0，具有良好的可靠性。

4.4 稳定性

除了环境温度的变动和电压的波动会对实际的PUF响应产生影响之外，本文设计的PUF引入偏置电压以调节PUF路径的延迟偏差，使得影响PUF稳定性的因素更为复杂多样。因此在评估其稳定性时，本文不仅采用片内汉明距离作为指标，还进一步采用误码率(Bit Error Rate，BER)以更精细地表现稳定性。为了更准确地衡量BER与稳定性的关系，采用控制变量法，分别针对温度、电压以及偏置电压这3个关键因素进行实验。通过绘制各变量与BER之间的曲线图，直观地展现本文设计的PUF在不同条件下的稳定性表现。实验采用控制变量法，分别以偏置电压U_{BIAS}、电源电压U_{DD}和温度T为变量，每组实验设置10 000组CRP。当变量为配置偏置电压U_{BIAS}，其配置为400 mV、500 mV、600 mV，响应R的基准电源电压U_{DD}=1.2 V，温度T=27 ℃。当变量为电源电压U_{DD}，其配置为：1 V、1.1 V、1.2 V、1.3 V、1.4 V。当变量为温度T，实验设置其值为0 ℃、15 ℃、27 ℃、45 ℃、60 ℃，响应R的基准电源电压为U_{DD}=1.2 V，温度T=27 ℃。将基准状态所得的响应R与不同变量条件所测的响应R进行对比，得到误码率BER。图6所示分别为不同变量的稳定性测试结果。当U_{BIAS}为600 mV时，由于双边沿延迟时间相近，电路充电时间与电路放电时间相等，与APUF的稳定性状况相似，稳定性随变量变化而线性变化，因此稳定性接近理想状态。当U_{BIAS}为400 mV时，双边沿延迟差最大，电路充电时间远长于放电时间，因此稳定性不随变量变化而线性变化。



(a) variation with supply voltage　(b) variation with temperature

Fig.6 Trends in stability
图6 稳定性变化趋势图

5 结论

本文利用偏置电压源控制延时可控开关电路影响APUF路径延迟时间，进一步增强结构抗ML攻击能力。同时利用该延时可控APUF响应信号可被双边沿采样的特性，增大熵源利用率以实现CRP数量的提升。实验结果表明，相较于APUF，该PUF电路对于LR、SVM、ANN和LightGBM等攻击方法的抗攻击能力显著提升，平均随

机性、唯一性和稳定性都接近理想值，表明电路具有良好的性能，可广泛应用于信息安全领域。

参考文献：

[1] PAPPU R, RECHT B, TAYLOR J, et al. Physical one-way functions[J]. Science, 2002, 297(5589): 2026-2030. DOI: 10.1126/science.1074376.

[2] CHEN B, 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.

[3] 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.

[4] LI Gang, WANG Pengjun, MA Xuejiao, et al. A 215-F^2 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. DOI:10.1109/TVLSI.2020.3014892.

[5] LI Gang, WANG Pengjun, MA Xuejiao, 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, 2020,29(1): 100-111. DOI:10.1109/TVLSI.2020.3030945.

[6] 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 Jiana,WANG Pengjun,LI Gang,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.) DOI:10.11959/j.issn.2096-109x.2021028.

[7] REN Pengpeng,XUE Yongkang,JING Linglin,et al. A strong physical unclonable function with machine learning immunity for Internet of Things application[J]. Science China Information Sciences, 2024(67):112404. DOI:10.1007/s11432-022-3722-8.

[8] 张卫欣,刘佳林,闫鹏. 电力物联网双层网格抗捕获攻击密钥分配算法[J]. 太赫兹科学与电子信息学报, 2023,21(8):1049-1053. (ZHANG Weixin,LIU Jialin,YAN Peng. Key management method against capture attack in power Internet of things based on double-layer grid model[J]. Journal of Terahertz Science and Electronic Information Technology, 2023, 21(8): 1049-1053.) DOI:10.11805/TKYDA2021104.

[9] MA Xuejiao,WANG Pengjun,LI Gang,et al. Machine learning attacks resistant strong PUF design utilizing response obfuscates challenge with lower hardware overhead[J]. Microelectronics Journal, 2023(142):105977. DOI:10.1016/j.mejo.2023.105977.

[10] 拉拜,钱德拉卡桑,尼科利奇,等. 数字集成电路—电路系统与设计[M]. 周润德,译. 2版. 北京:电子工业出版社, 2017:158-159. (RABAEY J M,CHANDRAKASAN A,NIKOLIC B,et al. Digital integrated circuits: a design perspective[M]. ZHOU Runde, Translated. 2nd ed. Beijing:Publishing House of Electronics Industry, 2017:158-159.)

[11] ZHOU Ziyu, WANG Pengjun, LI Gang. Bagua protocol: a whole-process configurable protocol for iot sensing devices security based on strong PUF[J]. IEEE Internet of Things Journal, 2024,11(1):805-819. DOI:10.1109/JIOT.2023.3285930.

[12] LI Hui, LI Gang, WANG Pengjun, et al. A novel machine learning attack resistant APUF with dual-edge acquisition[C]// Asian Hardware Oriented Security and Trust Symposium. Singapore,Singapore:IEEE, 2022:1-4. DOI:10.1109/AsianHOST56390.2022.10022247.

[13] 刘金梅,屈强. 几类混沌序列的随机性测试[J]. 计算机工程与应用, 2011,47(5): 46-49. (LIU Jinmei,QU Qiang. Randomness tests of several chaotic sequences[J]. Computer Engineering and Applications, 2011,47(5):46-49.) DOI: 10.3778/j.issn.1002-8331.2011.05.016.

作者简介：

江佳琳(1997-)，女，在读硕士研究生，主要研究方向为物理不可克隆函数防御.email:452048579@qq.com.

周子宇(1996-)，男，在读博士研究生，主要研究方向为物理不可克隆函数攻击与防御.

李　刚(1988-)，男，博士，副教授，主要研究方向为集成电路、安全芯片理论和设计技术.

汪鹏君(1966-)，男，博士，教授，主要研究方向为集成电路、安全芯片理论和设计技术.