基于信号传输理论的 Glitch 物理不可克隆函数电路设计

张跃军 汪鹏君* 李 刚 钱浩宇
(宁波大学电路与系统研究所 宁波 315211)

摘 要：通过对信号传输理论、竞争-冒险现象和物理不可克隆函数(Physical Unclonable Functions, PUF)电路的研究，论文提出一种基于信号传输理论的“毛刺”型物理不可克隆函数电路(Glitch Physical Unclonable Functions, Glitch-PUF)方案。该方案首先根据偏差延迟的信号传输理论，推导出获得稳定“毛刺”输出的电路级数；然后利用组合逻辑电路的传播延迟差异，结合“1”冒险和“0”冒险获得具有“毛刺”的输出波形，采用多级延迟采样电路实现 Glitch-PUF 的输出响应。由于“毛刺”信号具有显著的非线性特性，将其应用于 PUF 电路可有效解决模型攻击等问题。最后在 TSMC 65 nm CMOS 工艺下，设计 128 位数据输出的电路结构，Monte Carlo 仿真结果表明 Glitch-PUF 电路具有良好的随机性。

关键词：信息安全；物理不可克隆函数电路；信号传输理论；Glitch 型物理不可克隆函数
中图分类号： TP331 **文献标识码**： A **文章编号**：1009-5896(2016)09-2391-06
DOI: 10.11999/JEIT151312

Design of Glitch Physical Unclonable Functions Circuit Based on Signal Transmission Theory

ZHANG Yuejun WANG Pengjun LI Gang QIAN Haoyu
(*Institute of Circuits and Systems*, *Ningbo University*, *Ningbo* 315211, *China*)

Abstract: In this paper, a Glitch-PUF circuit technique is proposed by taking into consideration various aspects i.e. the signal transmission theory, race and hazard phenomenon, and Physical Unclonable Functions (PUF). First and foremost, the glitch circuit is obtained under the signal transmission theory. Using the combinational logic circuit propagation delay difference which causes 1-hazard and 0-hazard, this feature is used to form output glitch waveform. This glitch is sampled by multistage delay sampling circuit. Due to the nonlinear characteristics of the Glitch, Glitch-PUF can thwart the modeling attack. Finally, under the TSMC 65 nm CMOS technology, a 128-bit output data Glitch-PUF circuit is designed. Monte Carlo simulation results show that the Glitch PUF circuit has better randomness.

Key words: Information security; Physical Unclonable Functions (PUF) circuit; Signal transmission theory; Glitch-PUF

1 引言

在现代信息安全系统中，物理不可克隆函数(Physical Unclonable Functions, PUF)电路已经被广泛用来作为身份认证和防伪手段，如智能卡、信用卡、电子标签(Radio Frequency Identification Devices, RFID)、手机、安全摄像机和游戏设备等等。PUF 电路属于芯片特征识别电路，具有唯一性、随机性和不可克隆性，通过提取芯片制造过程中无法避免引入的工艺偏差，产生无限多个特有的数据信息。将 PUF 电路应用到安全设备中，可以有效防御传统的攻击模式，如数学攻击、病毒攻击、差分功耗攻击以及碰撞攻击等等。国际上许多研究机构，包括美国、奥地利、日本和法国等国家，都对 PUF 电路展开了深入研究，并取得一定的研究成果。在 PUF 电路概念模型方面，文献[1]依据光学操作原理提出物理单向函数(Physical One-Way Functions, POWFs)的概念，并将其用于武器控制条约的战略武器识别中。在延迟型 PUF 电路的实现方面[2−5]，文献[2]采用 CMOS 工艺参数偏差实现随机函数的

收稿日期：2015-11-25；改回日期：2016-04-27；网络出版：2016-07-04
*通信作者：汪鹏君 wangpengjun@nbu.edu.cn
基金项目：浙江省自然科学基金(LQ14F040001)，国家自然科学基金(61404076, 61474068, 61274132)，浙江省科技厅公益技术应用研究(2015C31010)
Foundation Items: The Zhejiang Provincial Natural Science Foundation of China (LQ14F040001), The National Natural Science Foundation of China (61404076, 61474068, 61274132), The S&T Plan of Zhejiang Provincial Science and Technology Department (2015C31010)

功能，结合互联线和晶体管的延迟偏差实现 Arbiter-PUF 电路；文献[4]提出可配置逻辑结构的 RO-PUF 电路；文献[5]提出在 FPGA 上实现 PUF 电路的功能。在存储型 PUF 电路实现方面[6–10]，文献[6]在 0.13 μm 工艺下实现有效长度为 128 位、能量效率为 1.6 pJ/bit、稳定性达到 96%的 SRAM-PUF 电路；文献[7]提出采用 Power-up PUF 电路实现芯片硬件指纹的认证；文献[8]在 TSMC 65 nm CMOS 工艺下提出可重构多端口 PUF 电路设计。针对新型、功能强大的 PUF 电路的研究越来越多[11–14]。

同时，研究人员也发现 PUF 电路存在被攻击的威胁，已经成功采用多种攻击方法对 PUF 电路实施攻击[15–17]。其中，文献[15]采用机器学习方法成功攻击物理不可克隆函数，并系统分析 PUF 电路模型攻击，成功攻击 Arbiter-PUF 和前反馈 Arbiter-PUF 等电路。随着攻击模式的增加，严重影响 PUF 电路的实用化进程。PUF 电路被攻击的主要原因是不具备足够的非线性特性，如何有效增强 PUF 电路的非线性特性，将成为下一代 PUF 电路的主要研究方向。鉴此，本文提出一种基于信号传输理论的 Glitch-PUF 电路结构，该电路利用 Glitch 的非线性特性，可以达到 PUF 电路防御模型攻击的目的。首先根据信号传输理论，推导出获得稳定 Glitch 的延迟树电路结构；然后利用组合逻辑电路的门传播延迟差异，并结合“1”冒险和“0”冒险获得具有 Glitch 的输出波形，通过多级延迟采样电路实现 Glitch-PUF 的输出响应。该 PUF 电路利用 Glitch 的非线性特性，解决延迟型 PUF 电路的模型攻击等问题。最后在 TSMC 65 nm CMOS 工艺下，设计 128 位数据输出的 Glitch-PUF 电路。Monte Carlo 仿真结果表明所设计的 PUF 电路具有良好的随机性。

2 信号传输理论和 Glitch 的产生

2.1 信号传输理论

组合逻辑电路通常由与、或、非3种基本门电路组成，采用信号传输概率理论，即可以从输入信号的概率逐级计算电路中各结点的信号概率，直至电路输出。首先，我们定义在一段足够长的时间内测得信号 $x=1$ 的时间与总的测量时间之比被称为信号 $x=1$ 的概率，并记作 $P(x)$。对图1(a)所示的反相器，输入信号 $x=1$ 的概率为 P_1，输出信号的概率为 $1-P_1$；对图1(b)所示的与门，输入信号的概率为 P_2 和 P_3，且输入信号之间互相独立，则输出信号的概率为 $P_2 \cdot P_3$；对图1(c)所示的或门，输入信号的概率为 P_4 和 P_5，且输入信号之间互相独立，输出信号的概率为 $P_4+P_5-P_4 \cdot P_5$。

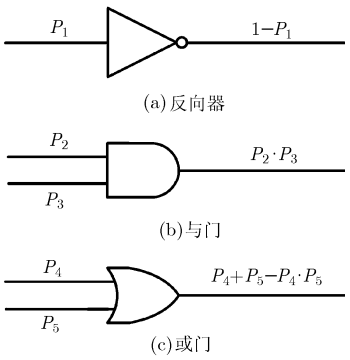


图 1 信号概率传输模型

2.2 Glitch 的产生

信号在器件内部通过连线和逻辑单元时，都有一定的延时。信号的高低电平转换也需要一定的过渡时间。由于存在这两方面因素，多路信号的电平值发生变化时，在信号变化的瞬间，组合逻辑的输出有先后顺序，并不是同时变化，往往会出现一些不正确的尖峰信号，这些尖峰信号称为“Glitch”。在逻辑函数表达式中，若某个变量同时以原变量和反变量两种形式出现，就具备了竞争条件。去掉其它变量，留下有竞争能力的变量，如果表达式为：$F=A \cdot A'$，就会产生“0”冒险，如图 2(a)所示；$F=A+A'$，就会产生“1”冒险，如图 2(b)所示。此外，还存在动态结构产生 Glitch 的电路，如图 2(c)所示。在动态 Glitch 电路中，当输入信号 A 和 B 通过门电路产生 Glitch 信号，还需要满足输入信号 C 从 0 变换 1 之后才能将 Glitch 传输到 F 端[18]。

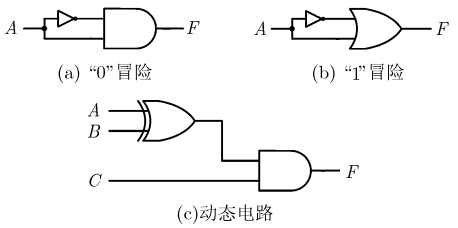


图 2 Glitch产生电路

在实际电路中，信号延迟大小与连线长短和逻辑单元数目有关，同时还受器件制造工艺、工作电压、温度等的影响。在 TSMC 65 nm CMOS 工艺，TT 工艺角(Typical NMOS Typical PMOS, TT)、1.2 V 电源电压、温度 25℃ 的工作条件下，仿真二输入门产生 Glitch 需要的信号延迟差，统计结果如表 1 所示。

当 Glitch 在组合逻辑电路中产生后，还会沿着信号路径往下一级逻辑电路传输。以二输入与门 AND 为例分析 Glitch 的传输过程，如图 3 所示。

表 1 二输入门电路产生 Glitch 信号延迟差(ns)

门电路	信号延迟差	门电路	信号延迟差
AN2D0	0.025	GOR2D1	0.045
AN2D1	0.030	GOR2D2	0.045
AN2D2	0.035	GXOR2D1	0.040
AN2D4	0.035	GOR2D2	0.040
AN2D8	0.040	AN2XD1	0.025

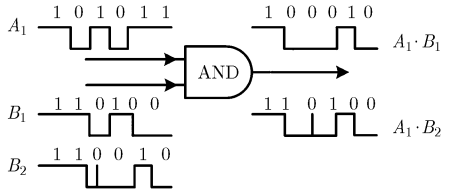


图 3 门电路Glitch传输

A_1为与门的一个输入端信号，B_1为与门的无Glitch的输入信号，B_2为与门的有Glitch的输入信号。当A_1和B_1作与操作时，输出信号为$A_1\cdot B_1$，输出无Glitch；当A_1和B_2作与操作，且Glitch出现的时刻A_1信号为高电平时，输出信号为$A_1\cdot B_2$，输出有Glitch。A_1和B_2作与操作的过程可以实现Glitch在组合逻辑电路的传输。

此外，有效Glitch还应满足脉冲高度和宽度的要求。脉冲高度由与门电路的延迟和负载电容决定，脉冲幅值大于10% Vdd。脉冲宽度由采样电路中的D触发器决定，脉冲宽度大于D触发器的数据输入到数据稳定输出的时间CTQ，即满足建立和保持时间(setup time and hold time)。采样D触发器的建立时间和保持时间如表2所示，其中工作环境分别为FF, TT和SS (FF：电压为1.32 V，工艺角为Fast NMOS Fast PMOS，温度为−40℃; TT：电压为1.2 V，工艺角为Typical NMOS Typical PMOS，温度为25 ℃; SS：电压为1.08 V，工艺角为Slow NMOS Slow PMOS，温度为125 ℃)，建立和保持时间之和为CTQ (t_{PLH}：低电平到高电平转换，t_{PHL}：高电平到低电平转换)。Glitch的宽度必须大于D触发器的建立和保持时间才有可能被采样，即为有效Glitch。

表 2　D 触发器的建立和保持时间(ns)

工作环境	CTQ	
	t_{PLH}	t_{PHL}
FF	0.105	0.124
TT	0.174	0.204
SS	0.338	0.394

2.3 基于信号传输理论的 Glitch 概率估计

通常采用信号传输理论的开关活动性来估计电路的功耗，其中包括理想的开关活动性功耗估计和考虑电路延时的开关活动性功耗估计等。考虑延时的情况下估计的电路功耗会大于理想的功耗估计，增加部分的功耗由电路延时产生 Glitch 造成，即增加的开关活动性为 Glitch 的数量。因此，我们可以采用信号传输理论估计逻辑电路的 Glitch 概率。电路延时由实际电路确定，在电路逻辑级设计中可以采用数学模型进行估计。一般利用单位延时模型估计电路延时，即将电路的每个多输入门分解成二输入门，将二输入门的传输延时大小定为一个单位时间。分解后的电路网络，可用 $G(U)$表示，U 为节点集合，每个节点代表一个二输入门。此外，G 的延时为关键路径上节点传输延时之和，且对于任意节点 j，其输出延时可表示为

$$t_j = 1 + \max(t_{j\_a}, t_{j\_b}) \tag{1}$$

其中，t_j是节点 j 的输出延时，t_{j_a}和 t_{j_b}是节点 j 的输入延时，$j \in U$。五变量表达式 $f(x_4,x_3,x_2,x_1,x_0)=x_4x_3 \oplus x_2x_1x_0$，其电路示意图如图 4 所示。其中，$x_4$, x_3, x_2,x_1 和 x_0 为输入信号，m, n 和 w 为电路内部节点，d 为电路内部节点的单位延迟时间，y 为输出信号。则带延迟的函数可用式(2)表示，其中 $x_0(t-d)$ 为在 t 时刻的输入信号 x_0 经过一级内部节点到达输出端 $y, x_1(t-2d), x_2(t-2d), x_3(t-d)$ 和 $x_4(t-d)$ 的含义与上述相同。

$$\begin{aligned} f(y) = F(x_0,x_1,x_2,x_3,x_4,t) &= x_0(t-d)x_1(t-2d) \\ &\cdot x_2(t-2d)x_3(t-d)x_4(t-d) \end{aligned} \tag{2}$$

由文献[19]可知，逻辑电路的开关活动性估计问题可按照以下方法进行转换。假设逻辑电路采用门级网络和惯性延迟表示，则该电路可等同为 f 函数的同步时序电路，当输入信号满足门电路的建立和保持时间(setup time 和 hold time)时候，开关活动性可用所有类型电路信号的相关性来估计。结合开关活动性和 Glitch 概率的关系，可用零延迟电路与延迟电路信号相关性的差来表示电路 Glitch 概率。零延迟电路信号相关性模型为[19]

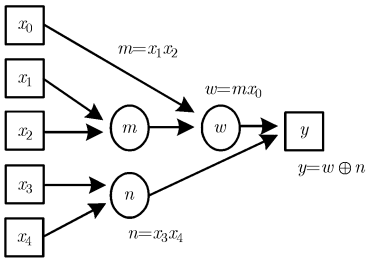


图 4　$f(x_4,x_3,x_2,x_1,x_0)=x_4x_3 \oplus x_2x_1x_0$的电路示意图

$$TC_{kl,mn}^{x_1x_2}=\frac{P(x_1(t-T)=k\wedge x_1(T)=l\wedge x_2(t-T)=m\wedge x_2(T)=n)}{P(x_1(t-T)=k\wedge x_1(T)=l)\cdot P(x_2(t-T)=m\wedge x_2(T)=n)} \tag{3}$$

其中，x_1x_2为输入信号；$P(x)$为信号概率；T为输入信号的周期；k, l, m, n为二值信号0或1; kl, $mn\in\{00, 01, 10, 11\}$; $\wedge$表示条件连接符； $P(x_1(t-T)=k\wedge x_1(t)=l)$ 表示状态k跳变到状态l的概率。延迟信号相关性模型为[19]

$$TC_{kl,mn}^{x_1x_2}(t_1,t_2)=\frac{P(x_1(t_1-1)=k\wedge x_1(t_1)=l\wedge x_2(t_2-1)=m\wedge x_2(t_2)=n)}{P(x_1(t_1-1)=k\wedge x_1(t_1)=l)\cdot P(x_2(t_2-1)=m\wedge x_2(t_2)=n)} \tag{4}$$

其中，t_1和 t_2为信号传输的起止时间。由式(3)和式(4)，可得组合逻辑电路的 Glitch 概率估计模型：

$$G(t_1,t_2)=TC_{kl,mn}^{x_1x_2}(t_1,t_2)-TC_{kl,mn}^{x_1x_2} \tag{5}$$

3 基于信号传输理论的 Glitch-PUF 电路设计

通过上述分析，稳定 Glitch 输出需要级联一定级数的门电路偏差，并且产生的 Glitch 信号可以随着电路进行传输。因此，我们可以利用延迟树结构的电路，构建“1”冒险和“0”冒险电路，获得具有 Glitch 的输出波形，然后通过多级采样电路实现 Glitch-PUF 的输出响应。

3.1 采用延迟树结构的 1 位输出 Glitch-PUF 电路

为了在电路中实现更多稳定输出的 Glitch，结合“1”冒险和“0”冒险电路，设计的延迟树结构电路如图 5 所示，图中所示的基本门电路可以采用相同功能的组合逻辑电路模块来替换。在延迟树结构中，基本门电路与、或、非门都采用最小尺寸的标准单元，且相同类型的电路结构完全相同。在延迟树结构中，由于工艺偏差的存在 OR1 和 OR2 门电路的延迟会有差别，输入信号传输到节点 m 和 n 的时间不同。当节点 m 和 n 的时间差达到 AND1 门的 Glitch 产生时间，则会在节点 q 产生 Glitch。同理，由于工艺偏差的存在，Path1 和 Path2 的延迟时间存在差异，输入信号传输到节点 s 和 t 的时间不同，则会在 XOR 的输出节点 Y 产生 Glitch。为了防止前一级产生的 Glitch 被后一级门电路吸收，采用延迟路径中插入奇数个反相器来实现，如图 5 中的 INV1 和 INV2，有效避免“1”冒险和“0”冒险相互吸收的问题。为了满足有效 Glitch 的宽度要求，图 5 所示的基本门电路可用具有相同逻辑功能的组合逻辑模块进行替换。图 6 为 Glitch 信号产生电路在电压为 1.2 V，工艺角为 TT，温度为 25 ℃的工作条件下的仿真结果。

在获得有效的Glitch信号后，需要设计采样电路，将不同的Glitch信号转换为Glitch-PUF的二进制输出数据，工作过程可分为延迟和采样两个阶段。首先，在延迟阶段，带Glitch的输入信号通过一串的延迟单元，单元的延迟时间与D触发器的建立时间

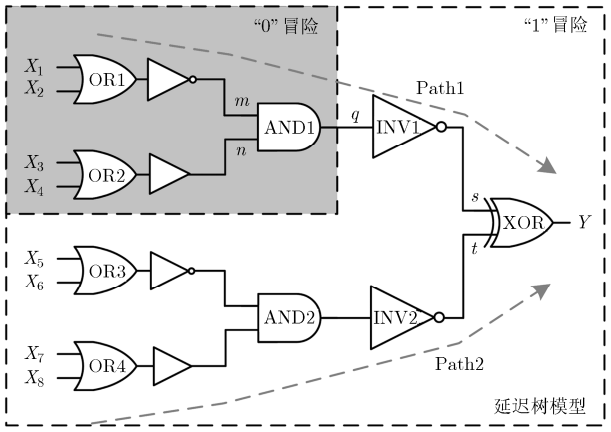


图 5 Glitch信号产生电路

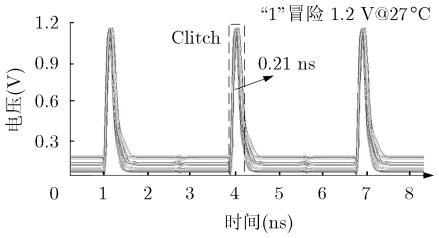


图 6 Glitch信号的仿真结果

保持一致，每级延迟电路都引出一个输出端口。然后，在采样阶段，在采样时钟的控制下，每个D触发器对延迟链的多个输出端口进行采样，实现串联信号的并行化处理，采样结果暂存在内部寄存器中。延迟采样电路结构如图7所示。如输入不包含有效Glitch信号，则采样输出为0111100, 0和1相对集中分布，如图8(a)所示；如输入包含有效Glitch信号，则采样输出为0111101, 0和1分布比较离散，如图8(b)所示。其中，图8(b)中最后一位出现1的即为有效Glitch信号。对采样结果进行Glitch信号统计，就可以获得Glitch-PUF的输出数据。

3.2 多位输出 Glitch-PUF 电路

多位 Glitch-PUF 电路的结构框图，如图 9 所示。128 位输出 PUF 电路方案包括 Glitch 产生模块、译码器、输入模块和移位寄存器。

每个Glitch产生模块由多级“1”冒险和“0”冒险电路组成，译码器分为两个阶段3-8译码和2-4译码。首先，将输入信号通过输入接口存储在输入模

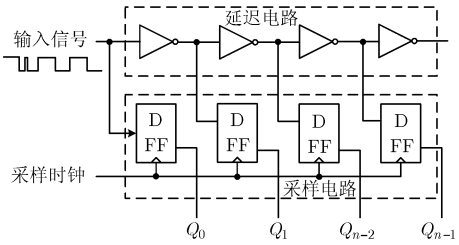


图 7 延迟采样电路结构

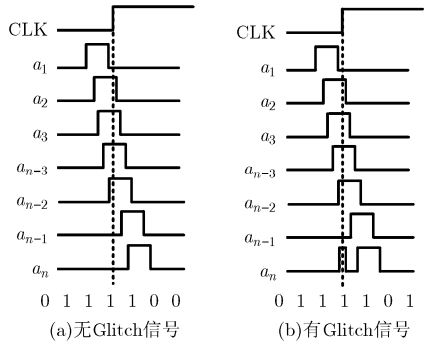


图 8 延迟采样电路工作情况分析

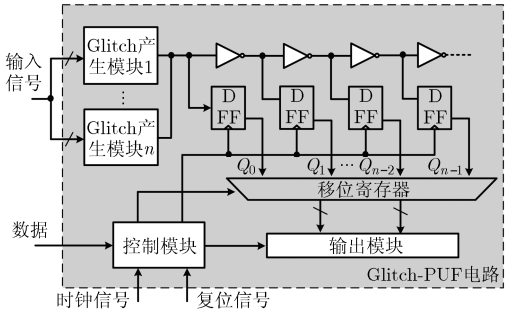


图 9 多位输出Glitch-PUF电路

块中，包括地址信息和控制信息；然后，通过控制电路模块，在时钟信号控制下将控制信息存储到移位寄存器中；其次，运行延迟电路，分别将带Glitch信号输入到C_i端口，输入信号依次通过各级延迟电路，采样电路裁决出PUF电路的输出数据；最后，将数据输出到输出模块，作为Glitch-PUF电路的输出数据。

4　实验结果与分析

采用 TSMC 65 nm CMOS 工艺，设计基于信号传输理论的 Glitch-PUF 电路。与门、或门和反相器分别为标准单元 AN2D0, OR2D0, INVD0。涉及的晶体管尺寸分别为 NMOS 管 260 nm/60 nm, PMOS 管 195 nm/60 nm。为验证 Glitch-PUF 电路的随机性，图 10 给出 Monte Carlo 仿真情况。图 10(a)和图 10(b)分别表示电路工作在“1”冒险和“0”冒险下的仿真情况，证明所设计的 PUF 电路输出响应具有良好的随机性。

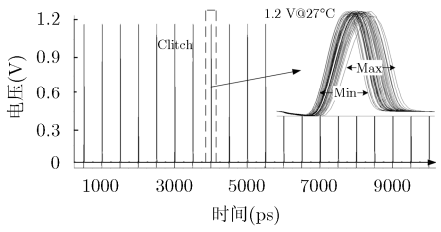
基于信号传输理论的 Glitch-PUF 电路与相关论文比较如表 3 所示。所设计的 PUF 电路的非线性特性大大提高，可以有效地实现延迟型 PUF 电路防御模型攻击，随机性达到 98%以上。由于使用采样电路复用技术，降低整体 PUF 电路的硬件成本。

表 3 与相关文献的比较结果

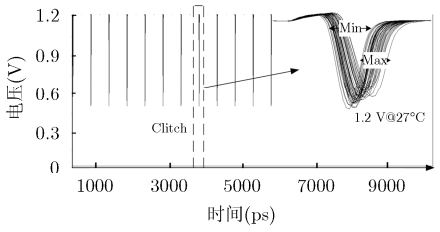
文献	PUF 类型	制造工艺	防御模型攻击	随机性 (%)
VLSI [2]	Arbiter-PUF	180 nm	否	95.8
JSSC[7]	SRAM-PUF	130 nm	是	89
IEICE[8]	RM-PUF	65 nm	是	–
TIFS[10]	STT-PUF	Magnetic	否	73.8
DATA[13]	Strong PUF	65 nm	否	97.2
TCASI [17]	SC-PUF	180 nm	是	–
本文	Glitch-PUF	65 nm	是	98

5　结论

本文设计了一种基于信号传输理论的 Glitch-PUF 电路。通过延迟树 Glitch 产生模块、译码器、采样模块和移位寄存器，实现 Glitch-PUF 电路多位数据输出。分析 Glitch 的产生、传输以及采样等过程，给出有效 Glitch 必须满足信号传输条件和采样条件，采用延迟树结构实现 Glitch 的“1”冒险电路和“0”冒险电路等。在 TSMC 65 nm CMOS 工艺下，设计 128 位 Glitch-PUF 电路。实验结果表明所设计的 Glitch-PUF 电路逻辑功能正确，具有良好的随机性。该 Glitch-PUF 电路可应用于密钥产生等信息安全领域。



(a) “1”冒险



(b) “0”冒险

图 10 蒙特卡洛仿真结果

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] 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.

[3] LAO Y J and PARHI K 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.

[4] CAO Yuan, ZHANG Le, CHANG Chiphong, *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.

[5] WIECZOREK P Z and GOLOFIT K. Metastability occurrence based physical unclonable functions for FPGAs[J]. *Electronics Letters*, 2014, 50(4): 281–283.

[6] YING S, HOLLEMAN J, and OTIS B P. A digital 1.6 pJ/bit chip identification circuit using process variations[J]. *IEEE Journal of Solid-State Circuits*, 2008, 41(3): 69–77.

[7] HOLCOMB D E, BURLESON W P, and FU K. Power-up SRAM state as an identifying fingerprint and source of true random numbers[J]. *IEEE Transactions on Computers*, 2009, 58(9): 1198–1210.

[8] WANG Pengjun, ZHANG Yuejun, HAN Jun, *et al.* Architecture and physical implementation of reconfigurable multi-port physical unclonable functions in 65 nm CMOS[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2013, E96-A(5): 963–970.

[9] ZHANG Le, FONG Xuanyao, CHANG Chiphong, *et al.* Optimizating emerging nonvolatile memories for dual-mode applications: Data storage and key generator[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2015, 34(7): 1176–1187.

[10] ZHANG Le, FONG Xuanyao, CHANG Chiphong, *et al.* Highly reliable spin-transfer torque magnetic RAM-based physical unclonable function with multi-response-bits per cell [J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(8): 1630–1642.

[11] ZHANG Jiliang, LIN Yaping, LYU Yongqiang, *et al.* A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(6): 1137–1150.

[12] 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.* Multiple frequency slots based physical unclonable functions[J]. *Journal of Electronics & Information Technology*, 2012, 34 (8): 2007–2012. doi: 10.3724/SP.J.1146.2011.01249.

[13] BHARGAVE M and MAI K. An efficient reliable PUF-based cryptographic key generator in 65 nm CMOS[C]. Design, Automation and Test in Europe Conference and Exhibition (DATE), Dresden, Germany, 2014: 1–6.

[14] GAO Yansong, RANASINGHE D C, AL-SARAWI S F, *et al.* Memristive crypto primitive for building highly secure physical unclonable functions[J]. *Scientific Reports*, 2015, 5(12785): 1–14.

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

[16] SAHOO D P, NGUYEN P H, MUKHOPADHYAY D, *et al.* A case of lightweight PUF constructions: cryptanalysis and machine learning attacks[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2015, 34(8): 1334–1343.

[17] WAN Meilin, HE Zhangqing, HAN Shuang, *et al.* An invasive-attack-resistant PUF based on switched-capacitor circuit[J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2015, 62(8): 2024–2034.

[18] UNGER S H. Hazards, critical races, and metastability[J]. *IEEE Transactions on Computers*, 1995, 44(6): 754–768.

[19] THEODORIDIS G, THEODORIDIS S, SOUDRIS D, *et al.* Switching activity estimation under real-gate delay using timed Boolean functions[J]. *IEE Proceedings-Computers and Digital Techniques*, 2000, 147(6): 444–450.

张跃军： 男，1982 年生，讲师，研究方向为低功耗、高信息密度集成电路理论和设计、安全芯片理论和设计.

汪鹏君： 男，1966 年生，教授，研究方向为低功耗集成电路理论和设计技术、高信息密度集成电路理论和设计技术、安全芯片理论和设计技术、电路设计综合和优化技术、多媒体技术以及相关理论.

李 刚： 男，1988 年生，博士生，研究方向为低功耗、高信息密度集成电路理论和设计、安全芯片理论和设计.

钱浩宇： 男，1991 年生，硕士生，研究方向为低功耗、高信息密度集成电路理论和设计、安全芯片理论和设计.