

采用全局互连线随机模型的硅物理 不可克隆函数的设计

吴志安, 段成华

(中国科学院研究生院 信息科学与工程学院, 北京 100049)

摘 要: 物理不可克隆函数(PUF)是一种新颖的从复杂物理系统中提取“秘密”的技术方法,有望在移动设备身份鉴别、密钥的生成和存储等诸多领域得到广泛应用. 现有的硅 PUF 电路仅考虑了片上逻辑器件延时,而忽视了已经作为时序模型主导因素的全局互连延时,不符合物理电路的实际. 本文在 PUF 的构造中考虑到 IC 加工工艺的变化性并结合互连延时模型,提出了一种新型的 PUF 电路. 仿真实验是在 Synopsys Hspice C-2010 模拟设计平台上完成的,测量了 PUF 电路的片间差异和片内差异参数,评估了 128 位的 PUF 电路的性能. 实验结果表明所设计的 PUF 电路是可行的,有望应用于移动计算身份鉴别和核心芯片防护.

关键词: 物理不可克隆函数;器件延时;互连延时;片间差异;片内差异

中图分类号: TN47

文献标识码: A

文章编号: 1000-7180(2012)12-0036-07

Design of Silicon Physical Unclonable Functions using Global Interconnect Stochastic Model

WU Zhi-an, DUAN Cheng-hua

(School of Information Science and Engineering, Graduate University of Chinese
Academy of Sciences, Beijing 100049, China)

Abstract: Physical unclonable function (PUF) is a novel method to extract “secret” from complex physical systems. It is expected to be widely used in many fields such as mobile device authentication, key generation and storage. But existing silicon PUF circuits consider only on-chip logic device delay and ignore global interconnect delay that has already become the dominant factor of timing model, thus behaving differently with corresponding physical circuits. In this paper, a new silicon PUF circuit is proposed by considering state-of-the-art IC manufacturing process variations and incorporating global interconnect delay model into PUF building. Experiments are conducted on Synopsys Hspice C-2010 analog design platform, on which PUF circuits' parameters of inter-chip and intra-chip variations are measured for evaluating the performance of a 128-bit PUF. Experiment results show that this PUF circuit is effective and is expected to support applications of identity authentication in mobile computing and of protecting core chips from intrusive attack.

Key words: physical unclonable function; device delay; interconnect delay; inter-chip variation; intra-chip variation

1 引言

在许多领域,包括光学、硅制造及其他纳米器件制造工艺中都存在许多随机的或统计的物理现象. 这些物理现象的变化性都是随机产生的^[1-2],但对于处在一个特定未知状态的系统,其探查与系统间

的交互是唯一的,系统具有不可克隆性,而这些特性可以用于构造物理不可克隆函数.

物理不可克隆函数有多种实现方式. MIT 的 R. S. Pappu 率先于 2001 年提出了光学物理不可克隆函数(Optical PUFs)^[3],利用激光照射到晶片上产生的斑点图案作为芯片的独有特征. J. Guajar-

do 等人提出了 FPGA 本征的物理不可克隆函数^[4], 利用 FPGA 中静态随机存储器上电时的原始值作为独有特征. MIT 的 Lee 提出了基于仲裁器的 PUF 电路^[5], 利用硅的物理特征和 IC 加工工艺的变化性, 唯一表征每一块硅芯片.

纳米尺度 CMOS 制造工艺的发展, 不仅缩小了器件的尺寸, 同时也缩短了信号在器件中的传输时间. 但是加工工艺的进步使导线电阻横截面缩小, 线边沿粗糙不易控制等因素增加, 导致全局互连延时已经超过了器件延时, 成为时序模型的主导因素. 现有的 PUF 电路都是基于器件延时实现的, 没有考虑全局互连延时的影响^[6-9]. 互连线作为电路的一部分也存在着大量的随机性, 导线的长度、宽度以及高度都不可能精确的控制, 同时其形状也是不规则的, 可能存在着大量的毛边. 这些因素都将会影响导线的电阻值和电容值, 从而影响全局互连延时.

本文在器件延时随机模型的基础上, 利用互连延时模型并考虑 IC 加工工艺的变化性, 建立全局互连延时随机模型. 通过修改台积电 (TSMC) 65nm 低 K 电介质工艺器件模型参数, 并考虑互连延时随机特征, 提出全局互连式 PUF 电路的设计方案.

2 基本原理与电路实现

在大规模集成电路芯片生产过程中, 不同芯片间的差异性是不可控制的, 随机因素越来越多, 这就为硅物理不可克隆函数的研究应用提供了一个基本平台. 图 1 显示的是一个硅工艺下由数据选择器和仲裁器构成的 PUF 电路^[7].

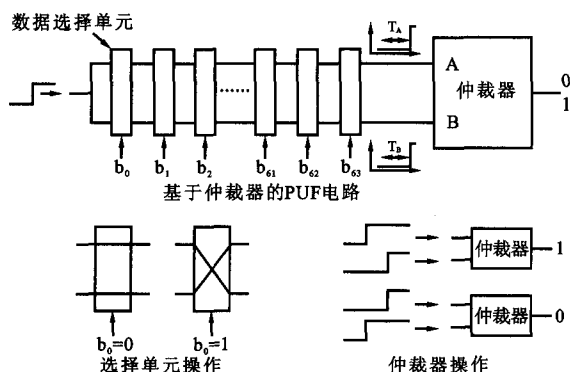


图 1 PUF 电路原理图

电路的左侧输入端输入信号是一个由低电平到高电平的上升沿信号, 经过两条不同的时延路径后到达仲裁器的输入端. 时延路径的选择是由数据选择器决定的, 通过控制信号 b_i 进行控制. 例如, 当 b_0 为 '0' 时, b_0 上方的数据选择器中的输入信号直接

直线输出; 而当 b_0 为 '1' 时, b_0 上方的数据选择器中的输入信号交叉传输至输出端口. 通过改变控制信号 b_i 的值, 可以控制信号的传输路径, 从而对于每一组 b_i 都可以获得一对时延路径. 这样上升沿信号就会在输入端分成两个信号经由两条不同的时延路径到达最后一个数据选择器的两个输出端口. 由于两条时延路径存在差异性, 到达最后一个数据选择单元输出时, 两个输出信号就会存在时间差. 如果 b_{63} 数据选择器上端口的输出信号快于下端口输出信号, 仲裁器的输出信号即为 '1'; 反之, 输出信号即为 '0'. 所以对于每一组的 b_i , 仲裁器都有一个与之对应的输出信号.

3 互连线建模

3.1 门延时与互连延时

互连设计作为芯片设计中的一个必要程序, 其重要性在过去一段时间没有得到应有的重视. 随着工艺节点的不断缩小, 不断增加的导线电阻使得互连延时日益显著, 而门延时却在不断缩小. 国家半导体行业协会曾发布过一张互连与门延时预测图, 如图 2 所示. 随着硅技术加工工艺的不断进步发展, 门电路的速度将越来越快, 而电路中导线速度却相对的越来越慢了.

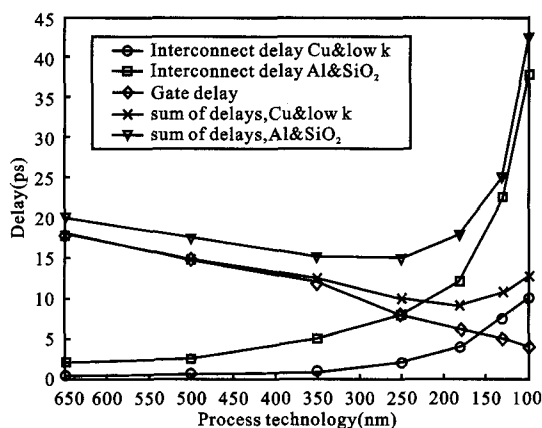


图 2 互连与门延时预测图

在工艺节点在一百纳米以下时, 互连延时和门延时之间的差距会进一步增大. 此时, 互连延时已经成为时序模型主导因素, 这就要求对互连线进行准确的建模分析.

3.2 互连电阻 R

图 3 为互连线示意图, W 为互连线宽度, H 互连线高度, 互连线的长度为 L , 则未考虑趋肤效应的互连线电阻可用下式表示:

$$R = \frac{\sigma \cdot L}{H \cdot W} \quad (1)$$

式中, σ 是互连材料的电阻率(单位 $\Omega \cdot \text{m}$).

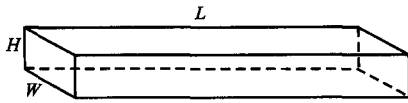


图 3 互连线示意图

3.3 互连电容 C

互连电容最简单的模型是平行板电容器模型, 如图 4 所示. 如果互连线的宽度明显大于绝缘材料, 那么就可以假设电场线垂直作用于电容板级, 它的电容可以用平板电容模型来表示, 如下:

$$C_{\text{int}} = \frac{\epsilon_{\text{ox}}}{t_{\text{di}}} WL \quad (2)$$

式中, W 和 L 分别为互连线的宽度与长度, t_{di} 和 ϵ_{ox} 表示绝缘层的厚度和介电常数. $\epsilon_{\text{ox}} = \epsilon_r \epsilon_0$, 其中 $\epsilon_0 = 8.854 \times 10^{-12} \text{ F/m}$ 是真空的介电常数, ϵ_r 是绝缘材料的相对介电常数.

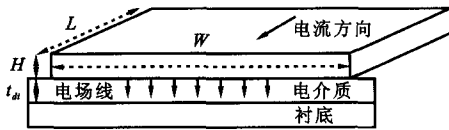


图 4 互连线平行板电容模型

为减少模型复杂度, 有效提取互连线的电容参数, 采用了如图 5 所示的模型模拟互连线结构. 对于纳米级 CMOS 工艺而言, 边缘电容在互连线电容中的比重越来越大, 参考 BPTM 模型的 CMOS 工艺互连寄生电容提取方法, 考虑边沿电容后互连线的电容表达式为:

$$c_g = \epsilon_{\text{ox}} \left[\frac{W}{T} + 2.22 \left(\frac{S}{S+0.70T} \right)^{3.19} + 1.17 \left(\frac{S}{S+1.51T} \right)^{0.76} \right] \times \left(\frac{H}{H+4.53T} \right)^{0.12} \quad (3)$$

其中 W 为互连线宽度, H 为互连线高度, 互连线的长度为 L , S 为互连线之间的间距, T 为顶层互连线与下层互连线之间的介质厚度, ϵ_{ox} 为介质材料的介电常数. 括号内的第一项表示互连线和下层互连线的平板电容, 后两项则表示互连线的边缘电容. 纳米级集成电路中的耦合电容也很明显, 同样参考 BPTM 模型的 CMOS 工艺互连寄生电容提取方法, 相邻互连线之间的耦合电容的表达式为:

$$c_c = \epsilon_{\text{ox}} \left[1.44 \frac{H}{S} \left(\frac{T}{T+0.70S} \right)^{0.09} + 0.74 \left(\frac{W}{W+1.59S} \right)^{1.14} + 1.16 \left(\frac{W}{W+1.87S} \right)^{0.16} \right]$$

$$\times \left(\frac{T}{T+0.98S} \right)^{1.18} \quad (4)$$

所以单位长度互连线的总电容为:

$$c = c_g + 2c_c \quad (5)$$

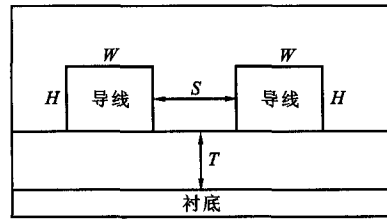


图 5 互连线结构模型

3.4 PUF 电路互连线建模

基于仲裁器的物理不可克隆函数电路设计过程中, 为了简化 PUF 电路的建模仿真, 没有考虑互连线对电路的影响. 但这对于在 65 nm 工艺下实现的 PUF 电路来说, 有着极大的缺陷. 根据国家半导体行业协会互连与门延时预测图显示, 百纳米级以下的工艺互连延时已经远远地超过了逻辑门的延时, 而 PUF 电路的基本原理就是利用电路本身内部的不可预测的不确定延时, 所以互连线延时已经是 PUF 电路中不可忽视的重要影响因素.

通过分析 PUF 电路的原理图(图 1), 发现电路中的互连线主要有两部分, 一是数据选择单元内部的互连线, 主要是逻辑门之间的连线; 二是数据选择单元之间的互连线, 即 b_i 与 b_{i+1} 之间的连线. 为了简化互连线的建模仿真, 对互连线采用了 RC 模型, 电路原理图如图 6 所示的.

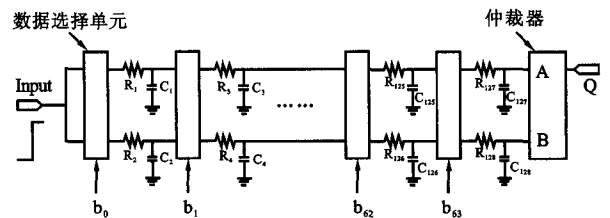


图 6 Arbiter PUF 原理图

4 随机仿真的建立

4.1 MOS 管随机延时模型建立

CMOS 工艺节点的减小, 导致相同的电路单元在不同的芯片上存在微小的性能差异, 即使在同一块芯片上放置在不同物理位置的相同电路单元, 也存在着这种差异. 而 PUF 电路的设计正是利用信号在器件和互连线中传输的时延差, 提取时延信息这一在芯片制造过程中产生的不可预测的内在固有性质, 作为其“秘密”信息.

在 CMOS 逻辑电路中, 对时延影响相对比较大

的参数就是 MOS 管的阈值电压(V_t),文献[7]中测量得到 MOS 管阈值电压在 30%(标准差/平均值)的差幅内变化,该变化将对逻辑门(反相器,与非门等)的传输时延产生 5%的影响.而在众多的影响因素中,对阈值电压产生主要影响的有随机掺杂波动(RDF)、线边沿粗糙程度(line edge roughness)以及栅氧化层厚度的变化(T_{ox} variations),其中线边沿粗糙程度和栅氧化层厚度的变化对阈值电压的影响相对于随机掺杂波动而言是非常小的,并指出随机掺杂波动是符合随机正态分布的,将阈值电压在随机掺杂波动影响下的标准差定义为:

$$\sigma_{V_t, RDF} = 3.19 \times 10^{-8} \frac{T_{ox} N_d^{0.4}}{\sqrt{W_{eff} L_{eff}}} \quad (6)$$

其中 T_{ox} 为栅极氧化层厚度, N_d 为随机掺杂浓度, W_{eff} 和 L_{eff} 为有效沟道宽度和长度.

表 1 为 CMOS 工艺节点的电压特性^[7],由此可以根据式(7),在 MATLAB 中产生一组符合随机正态分布的 MOS 管阈值电压.

$$V_{th} = V_t + \sigma \cdot \text{randn}(m, n) \quad (7)$$

表 1 CMOS 工艺节点电压特性

Node[nm]	V_{dd} [V]	V_t [V]	σ [mV]
250	2.5	0.55	12
180	1.8	0.50	13
130	1.3	0.36	15
90	1.2	0.35	21
65	1.0	0.30	28
45	0.6	0.25	40
32	0.5	0.23	58

在仿真实验中,采用的器件库是 TSMC 的 65nm 逻辑硅化低 K 金属间电介质工艺器件库,其中 NMOS 管的零偏阈值电压 $V_t = 0.31703V$, PMOS 管的零偏阈值电压 $V_t = -0.29638894V$. 实验中总共采用了 2002 个 NMOS 管和 2002 个 PMOS 管,取 $m = 2002$, $n = 1$,并参考表 1 可知 65nm 工艺下阈值电压的标准差 $\sigma = 28mV$,分别代入式(7),得到两组阈值电压(2002 个 NMOS 阈值电压和 2002 个 PMOS 阈值电压分别符合各自的随机正态分布).将 MATLAB 生成的随机阈值电压逐个写入电路代码中,即可模拟 PUF 电路中的 MOS 管因 RDF 效应影响而导致其阈值电压发生随机变化的情形.

4.2 互连线随机延时模型建立

PUF 电路作为物理单向函数的一种表现形式,

其主要的有集成电路(IC, integrated circuit)身份鉴别、知识产权(IP, intellectual property)保护以及密钥的生成和存储,而电路本身的时延信息是最重要的“秘密”.为了更好地保护这个“秘密”,可以利用互连线构建类似“鸟巢”的结构,将 PUF 电路本身包裹起来.入侵者为了获取电路的“秘密”,就必须要对电路的时延特性进行研究分析,这就需要深入“鸟巢”内部从而可能会影响甚至破坏外层的互连线结构,而互连线作为电路的一部分,一旦受影响或者破坏,整个电路的时延信息都可能被更改,此时入侵者得到的“秘密”可能就是错误的.为了实现这种“鸟巢”结构,特意增加了互连线的长度,具体参数为:互连线宽度 $W = 0.14 \mu m$,互连线高度 $H = 0.35 \mu m$,互连线的长度为 $L = 500 \mu m$,互连线间距 $S = 0.14 \mu m$.由式(1)(3)(4)(5)可以得到 RC 模型的参数为: $R = 225 \Omega$, $C = 84 fF$.

本实验假设互连线的电阻值和电容值在一定程度上符合随机正态分布,标准差 $\sigma = 3$.由此就可以根据式(8)和式(9),利用 MATLAB 产生两组符合随机正态分布的互连线电阻和电容参数,并将其作为互连线 RC 模型的等效参数.

$$r = R + \sigma \cdot \text{randn}(m, n) \quad (8)$$

$$c = C + \sigma \cdot \text{randn}(m, n) \quad (9)$$

将生成的互连线电阻值和电容值逐个写入电路代码中,模拟互连线在电路中的影响,即可实现本实验对互连线的建模仿真.

4.3 激励(Challenge)的生成

PUF 电路的运行需要输入相应位数的激励,如图 1 的 b).根据激励信号的不同,输入信号在传输过程中切换不同的时延路径.在 PUF 实际应用中,为了保证 PUF 的安全性,通常采用随机生成一定位数的激励,激励的位数越长,PUF 的安全性越好,当然也会消耗更多的资源.文献[1]中提出采用 64 位的激励能较好的满足 PUF 的安全要求,同时消耗较少的资源.

$$b = \text{rand}(m, n) > 0.5 \quad (10)$$

本实验仿真时为了保证激励具有一定的随机性,采用了根据式(10)在 MATLAB 生成的 64 位激励.同时为了保证实验仿真的客观性,生成了 1000 组 64 位的随机激励,对电路进行了 1000 次的测试($m = 1000$, $n = 64$).

5 电路仿真实验及结果

本实验由两部分组成,分别测试 PUF 电路的唯

一性和可靠性^[8]. 实验采用的电路仿真平台为 Synopsys Hspice C-2010. 03, 通过依次输入 1000 组 MATLAB 生成的 64 位随机激励, 以 SR 锁存器的输出信号作为实验的响应输出.

①片间差异测量 (Inter-chip variation): PUF 电路的唯一性主要通过片间差异这个参数来衡量, 即不同的 PUF 电路对于同一组请求生成的响应的差异, 理想状况下应该是 50%. 为此, 本实验同时设计了三个 PUF 电路, 它们的结构完全相同, 存在的差别即是电路中每一段导线的电阻值和电容值以及每一个 MOS 管的阈值电压都是随机生成的. 仿真的环境温度为 25℃, 供电电压为 1.0 V.

②片内差异测量 (Intra-chip variation): 测试 PUF 电路可靠性的衡量参数为片内差异, 即同一个 PUF 电路在外部环境变化时, 对于同一个请求的响应发生的变化差异, 这是对每一个芯片可复制性的一个度量, 也称片内噪声, 理想状况下应该是 0%. 本实验主要考虑温度和供电电压这两个外部环境因素, 实验分别测量了环境温度在 25℃ 和 150℃ 以及供电电压在 +10% 变化时, 同一个 PUF 电路对于同一个请求的输出响应差异, 由此即可验证本实验设计的 PUF 电路的可靠性.

表 2 为 PUF 电路在输入 1000 组请求后得到响应的位分布, RDF 表示仅考虑 RDF 效应对 PUF 电路的影响, RC 表示在 RDF 效应的影响下再增加互连线对电路的影响. 由表中的数据可知, 加入互连线影响因子的三个 PUF 电路的输出响应中的逻辑“1”的占有率都在 50% 左右, 平均值为 51.77%. 实验结果表明本实验设计的 PUF 电路的响应输出具有良好的均匀性, 偏差微小.

表 2 PUF 电路的输出分布

电路序号	测试次数	RDF	RC
1	1000	522	491
2	1000	482	459
3	1000	521	603

表 3 为 PUF 电路的片间差异测试结果. 由表中的数据可知, 本实验的三个 PUF 电路之间的输出响应差异在 48% 左右, 平均值为 48.13%, 与理想状况 50% 差距很小. 实验结果表明所设计的 PUF 电路的输出响应比之前的 RDF 电路具有更大的差异性, 能较好的达到实验要求的片间差异要求, 具有良好的唯一性.

表 3 PUF 电路的片间差异

比较电路序号	测试次数	RDF 片间差异 (%)	RC 片间差异 (%)
1 vs 2	1000	46.50	48.2
1 vs 3	1000	44.30	50.0
2 vs 3	1000	43.80	46.2

表 4 为 PUF 电路的片内差异测试结果. 本实验主要考虑环境温度和供电电压这两个外部环境因素, 实验分别测量了环境温度在 25℃ 和 150℃ 以及供电电压在 +10% 变化时的输出响应. 由表中的实验数据可知, 三个 PUF 电路各自的输出响应差异在 3% 左右, 平均值为 3.4%, 与理想状况 0% 差距较小. 实验结果表明所设计的 PUF 电路的输出响应相比之前的 RDF 电路, 片内差异性有所增大, 但是幅度很小, PUF 电路受外部环境 (外部温度和供电电压) 的影响仍然较小, 抗环境干扰能力强, 能较好的达到实验要求的片内差异要求, 具有良好的可靠性.

表 4 PUF 电路的片内差异

比较电路序号	测试次数	RDF 片内差异 (%)	RC 片内差异 (%)
1 vs 2	1000	3.1	5.0
1 vs 3	1000	2.3	2.7
2 vs 3	1000	3.0	2.4

6 128 位 PUF 电路设计分析

如前所诉, PUF 电路主要的应用有移动设备身份鉴别、知识产权保护以及密钥的生成和存储等^[6]. IC 身份鉴别是 PUF 电路的基本应用, 但本实验设计的 1 位输出响应 PUF 电路不能直接的用于 IC 身份鉴别, 需要对输出响应进行扩充处理, 以获得更好的安全性能. 现在主要有两种方法可以将 PUF 电路的一位输出响应信号 Q 扩展为 N 位的响应. 第一种就是复制 N 个 PUF 电路, 让这些电路同时工作, 从而得到 N 位的输出信号 Q; 第二种就是将输出信号 Q 作为其中一个数据选择器控制信号 b_i , 让电路运行 N 次, 得到 N 位的输出信号 Q.

文献[8]提出 PUF 电路的输出响应位数对于芯片身份鉴别至关重要, 其中有两个参数将决定着芯片身份鉴别的成功率: 假阳性 (False-positive), 即将不同芯片鉴别为同一块芯片的错误鉴别统计概率; 假阴性 (False-negative), 即将同一块芯片鉴别为两块不同芯片的错误鉴别统计概率. 128 位的 PUF 电路输出响应能较好的权衡假阳性与假阴性之间的概

率分布^[1].

基于以上分析,本实验采用了 128 位输出响应的 PUF 电路,即复制 128 个 PUF 电路,让这些电路同时工作,输入同一组请求,从而得到 128 位的输出信号 Q_i ,电路示意图如图 7 所示.

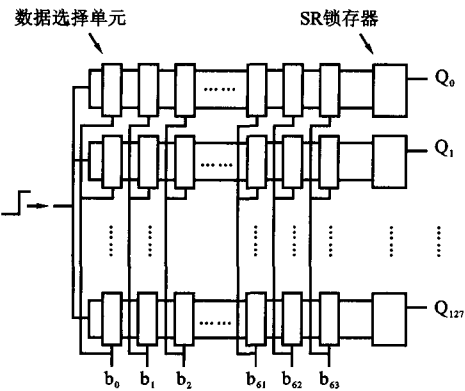


图 7 128 位 PUF 电路原理图

图 8 为 128 位 PUF 电路输出响应海明距离分布图,横坐标为 PUF 电路输出响应差异的位数,纵坐标为响应差异位数所对应的概率.图中带‘○’的实线显示的是考虑连线延时的片间差异变化,带‘□’的实线显示的是仅考虑 RDF 效应的片间差异变化,实验条件为室温 25℃,供电电压 1.0 V.图中虚线显示的是考虑连线延时的片内差异变化,带‘*’的虚线显示的是仅考虑 RDF 效应的片内差异变化,实验条件为 25℃~100℃,供电电压为 0.9 V~1.1 V(±10%).图中带‘☆’的虚线为理想情况下输出响应海明距离曲线.

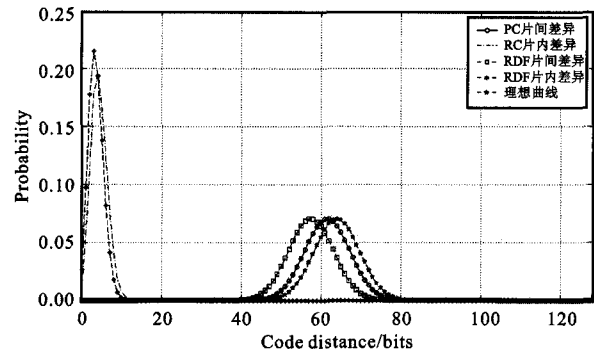


图 8 128 位 PUF 电路输出响应海明距离分布图

由图中可以看到,片间差异主要集中在 45~75 位,而在小于 40 位和大于 80 位的区间概率接近于零,仅考虑 RDF 效应的海明距离的平均值为 57.5 bit,增加考虑连线延时后的海明距离的平均值为 61.6 bit,两者都接近于响应位数的一半(128/2=64),但前者比后者更接近于理想值.文献[8]实测 PUF 电路的片间差异海明距离的平均值为 63.4

位.这表明所设计的考虑连线延时的 PUF 电路的片间差异更大,能更好的区分不同芯片,并且与实测电路参数具有很好的可比性.

图中的虚线和带‘*’的虚线显示的是 PUF 电路由于外部环境的变化而导致输出响应的差异变化,片内差异主要集中在 0~10 bit,而在大于 15 bit 的区间概率接近于零,仅考虑 RDF 效应的海明距离的平均值为 3.6 bit,增加考虑连线延时后的海明距离的平均值为 4.3 bit,分别占响应总长度的 2.8% 和 3.3%.文献[8]实测 PUF 电路的片内差异海明距离的平均值为 11.1 位.虽然考虑连线延时后,片内差异有所增大,但变化很小.这表明所设计的 PUF 电路受到外部环境(温度和电压)的影响较小,片内差异变化较小,具有较好的可靠性,并且与实测电路参数相接近.

由前文分析可知,理想情况下的片间差异和片内差异分别为 50%和 0%,所以 128 位 PUF 电路输出响应海明距离理想曲线为:

$$P_{\text{片间}} = C_{128}^k \cdot p_1^k \cdot (1 - p_1)^{128-k} = C_{128}^k \cdot 0.5^{128} \quad (11)$$

$$P_{\text{片内}} = C_{128}^k \cdot p_2^k \cdot (1 - p_2)^{128-k} = 0 \quad (12)$$

其中, k 为 PUF 电路输出响应差异的位数.

对比图 6 中的实验结果曲线和理想曲线,可以看到两者之间存在一定的差异,但是差异相对较小.综合文献[8]中的实测电路结果,可以发现实验结果与现有的基于样片测试的数据基本吻合.

由表 5 和表 6 更能清楚的看到,所设计的 PUF 电路的输出响应片内差异位数在 15 位以下,而片间差异位数在 45 位以上.由此可以确定假阳性与假阴性之间的冗余区间在 15~45 位.可以在此区间内选取一个值作为鉴别海明距离阈值来鉴别芯片的身份,即差异位数少于阈值的判别为同一芯片,而差异位数多于阈值的判别为不同的芯片.如果将鉴别海明距离阈值定为 24 位,则假阳性概率为 4.47E-12,假阴性概率为 1.60E-12,即芯片鉴别出错的概率低于 4.47E-12,与仅考虑 RDF 效应的 PUF 电路相比,芯片鉴别出错概率降低了一个数量级.

表 5 128 位 PUF 电路片内差异概率

输出响应差异位数	RDF 概率	RC 概率
≤7	0.9719	0.9285
≤8	0.9898	0.9687
≤9	0.9967	0.9876
≤10	0.9991	0.9955
≤11	0.9998	0.9985

表 6 128 位 PUF 电路片间差异概率

输出响应差异位数	RDF 概率	RC 概率
>10	1-2.25E-20	1-4.05E-23
>20	1-1.79E-12	1-1.13E-14
>30	1-3.70E-07	1-8.07E-09
>40	1-1.09E-03	1-1.49E-04

7 结束语

本文提出的 PUF 电路是首次利用全局互连线实现的一种增强式新的硅 PUF 电路. 实验结果表明所设计的 PUF 电路是可行的, 可用于移动计算身份鉴别、核心芯片防护等安全应用领域中.

参考文献:

[1] Soybali, Ors B, Saldamli G. Implementation of a PUF circuit on a FPGA[C] // New Technologies, Mobility and Security (NTMS). Paris, France, 2011:1-5.

[2] Pappu R S, Recht B, Taylor J, et al. Physical one-way functions [J]. Science, 2002, 297 (5589): 2026-2030.

[3] Asenov A, Brown A R, Davies J H, et al. Simulation of intrinsic parameter fluctuations in decananometer and nanometer-scale MOSFETs[J]. IEEE Trans Electron Devices, 2003,50(9):1837-1852.

[4] Guajardo J, Kumar S S, Schrijen G J, et al. FPGA intrinsic PUFs and their use for IP protection[J]. Cryptographic Hardware and Embedded Systems, 2007 (4727):63-80.

[5] Lee J W, Daihyun L, Gassend B, et al. A technique to build a secret key in integrated circuits for idention and authentication applications[J]. IEEE Trans VLSI Circuits, 2004,17-19.

[6] Ozturk E, Hammouri G, Sunar B. Physical unclonable function with tristate buffers[C] // International Symposium on Circuits and Systems (ISCAS). Seattle, USA, 2008:3194-3197.

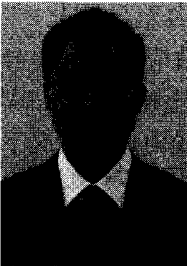
[7] Lin L, Holcomb D, Krishnappa D K, et al, Low-power sub-threshold design of secure physical unclonable functions[C] // ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED). Austin, USA, 2010:43-48.

[8] Devadas S, Suh E, Paral S, et al. Design and implementation of PUF-based unclonable RFID ICs for anti-counterfeiting and security applications[C] // IEEE International Conference on RFID. USA: Las Vegas, 2008:58-64.

[9] Lin L, Holcomb D, Krishnappa D, et al. Design optimization and security validation of sub-threshold PUFs [C]// Secure Component and System Identification Workshop (SECSI). Cologne, Germany, 2010.

[10] Bol D, Ambroise R, Flandre D, et al. Interests and limitations of technology scaling for subthreshold logic [J]. IEEE Trans VLSI Systems, 2009, 17 (10): 1908-1915.

作者简介:



吴志安 男,(1987—),硕士研究生. 研究方向为物理不可克隆函数的设计和评估.

段成华 男,(1962—),教授,博士生导师. 研究方向为大规模集成电路设计、安全处理器设计、信息系统集成等.