多频率段物理不可克隆函数

项群良 张培勇* 欧阳冬生 冯忱晖
(浙江大学超大规模集成电路设计研究所 杭州 310027)

摘 要：物理不可克隆函数(Physical Unclonable Functions, PUF)是一种用于保护集成电路芯片安全的新方法。传统的基于振荡器的 PUF 在产生响应过程中振荡器的振荡频率固定不变，因此存在着被攻击的隐患。该文提出一种新的利用多频率段的 PUF(Multiple Frequency Slots based PUF, MFS-PUF)来解决这个问题，通过可配置的振荡器，每产生一位响应，振荡器的振荡频率便发生转移。在每一种振荡频率下，由于不可避免地制造差异，振荡器之间的频率会有微小差别，这些略有差异的频率组成了一个频率段(frequency slot)，整个系统中则存在着多个频率段。各个频率段之间随机转变，相比于传统的基于振荡器的 PUF，系统输入输出响应对(Challenge-Response Pairs, CRPs)的值更大，也更加不可预测，这使得攻击者使用建模攻击的复杂度大大增加，在保证了自身性能的同时增强了本身的安全性。

关键词：安全芯片；物理不可克隆函数；多频率段
中图分类号：TN402 **文献标识码**： A **文章编号**：1009-5896(2012)08-2007-06
DOI: 10.3724/SP.J.1146.2011.01249

Multiple Frequency Slots Based Physical Unclonable Functions

Xiang Qun-liang Zhang Pei-yong Ouyang Dong-sheng Feng Chen-hui
(*Institute of VLSI Design*, *Zhejiang University*, *Hangzhou* 310027, *China*)

Abstract: Physical Unclonable Functions (PUF) is a new method for the safety of Integrated Circuit (IC) products. Nowadays, the Ring Oscillator (RO) based puf is under the shadow of being attacked because of RO's constant frequency. A new construct(Multiple Frequency Slots based PUF,MFS-PUF) is proposed to solve this problem. All the ROs are configurable, each RO's frequency changes from one to another after generating one response bit. In each frequency, ROs differ from each other because of the uncontrollable difference in manufacture and there exists a frequency slot. In the whole system, many frequency slots exist and the transfer between them are unpredictable, this makes us get more Challenge-Response Pairs (CRPs for short), what's more, the system is more unpredictable. Compared with the traditional RO based PUF, it is more difficult for the attacker to model this system. This architecture not only ensures the uniqueness, but also increases the safety of itself.

Key words: Security chip; Physical Unclonable Functions (PUF); Multiple Frequency Slots (MFS)

1 引言

物理不可克隆函数(Physical Unclonable Functions, PUF)通过物理设备来实现，它利用了制造设备过程中所固有的必然引入的随机性，具有不可克隆性，可用于产生不可复制的密钥，并且这种密钥只在芯片上电的时候存在，因此大大加强了其安全性，可广泛用于智能卡，信用卡等安全领域[1]。

PUF 的种类很多[1−4]，对于广泛研究的硅 PUF 有基于仲裁器的 PUF(Arbiter-based PUF)[2,5]和基于振荡器的 PUF(RO based PUF)[3]。前者强调布局的对称性，在制造上实现难度较大，后者对于对称性的要求不高，应用更加广泛，而且易于在 FPGA 上实现，本文主要研究基于振荡器的 PUF。

传统的基于振荡器的 PUF 存在着被建模攻击的隐患[6]。由于 PUF 自身的特殊性，传统的物理攻击对其无效，因为对电路物理结构一点点的破坏都很有可能破坏整个电路的布局，核心的延时电路也有可能遭到破坏，从而使其失效[1]。现有的对其最有效的攻击方式是根据输入输出响应对的关系，利用数学建模的方式来进行攻击[1,6]。为了解决这个问题，本文提出了一种新的结构，通过可配置的振荡器，每产生一位响应，每个振荡器的频率便转移。由于不可避免的制造差异，整个系统中存在着多个频率

2011-11-30 收到，2012-05-07 改回
国家科技重大专项(2009ZX02023-004-1)，国家自然科学基金(61002003)和浙江省自然科学基金(Z1111051)资助课题
*通信作者：张培勇 zhangpy@vlsi.zju.edu.cn

段(frequency slot)[7]。各个频率段之间随机转变，相比于传统的基于振荡器的 PUF，系统更加不可预测，这使得攻击者使用建模攻击的复杂度大大增加，在保证了自身性能的同时增强了本身的安全性。

本文结构如下：第 2 节介绍了传统基于 RO 的 PUF 的工作原理以及安全隐患；第 3 节提出了新的基于多频率段的 PUF(Multiple Frequency Slots based PUF, MFS-PUF)；同时分析了新结构的安全性和它的实现方式，第 4 节是实验结果分析；第 5 节为总结。

2 传统的基于振荡器的 PUF

2.1 工作原理

传统的基于振荡器的 PUF 的基本结构如图 1 所示[5,8,9]。

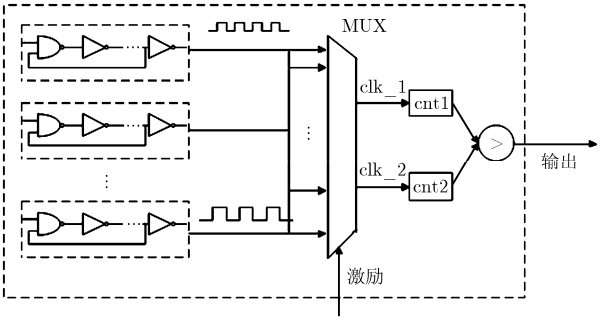

图 1 基于振荡器的 PUF 的结构框图

图 1 中的振荡器都由同一个硬宏单元例化而来，因此每个振荡器都完全相同。但是由于制造上的不可控性，振荡器之间的振荡频率并不完全一致，而是存在着微小的差别，利用这些随机差异可以用来产生响应。在激励作用下，每次会有两个振荡器被选择，它们分别触发一个计数器，当计数周期足够长时，振荡器之间微小的频率差别会被放大，因此很容易得到两者的快慢比较结果，该结果作为一位响应输出。这些输出完全由制造上的随机性决定，因此哪怕给予了精确的制造工艺也很难复制出相同的电路[1]。

由于制造上的不可控性，上述结构在不同电路上实现会得到不同的结果，这个特性可以用于产生不可复制的密钥，用来制作身份鉴别的安全芯片。

2.2 安全隐患

文献[6]中提出了对于传统的基于振荡器的 PUF 的攻击方式。

对于传统的基于振荡器的 PUF，输入输出之间的关系可以表示为

$$R = H(C, F) \tag{1}$$

其中 R 表示输出响应，C 表示输入的激励，F 表示各个振荡器的振荡频率所组成的频率段，H 表示输入输出之间的转变函数。

由于这种 PUF 在产生响应的过程中，振荡器的振荡频率固定不变，因此 F 相当于是一个常数，输入输出之间的关系可以简化成：

$$R = H(C) \tag{2}$$

攻击者只需要适当地施加激励，最多施加 $k(k-1)/2$ 个便可以得到各个振荡器之间的频率快慢顺序 $F = (f_1, f_2, \cdots, f_k)$，根据 F 和 H 就可以准确预测出任意激励下的响应。

3 基于多频率段的 PUF

为了避免被建模方式攻击以提高 PUF 自身的安全性，本文提出了基于多频率段的 PUF(Multiple Frequency Slots based PUF, MFS-PUF)。

3.1 MFS-PUF 的结构

MFS-PUF 的结构如图 2 所示。

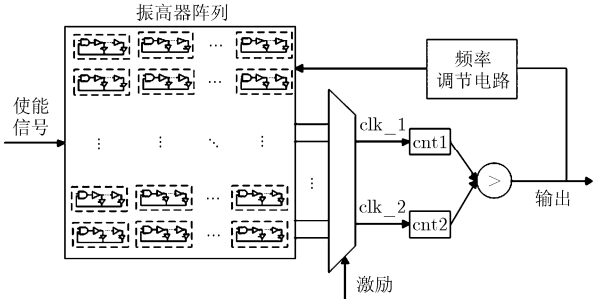

图 2 MFS-PUF 结构图

图 2 中，多个由同一硬宏单元例化的振荡器组成了振荡器阵列(RO arrays)，选择器每次从这个振荡器阵列中按一定规则选择两个振荡器进行计数，比较两者频率的大小，比较结果在输出的同时经过一个频率调节电路(frequency modulate circuit)反馈到振荡器阵列以改变振荡器的振荡频率。频率调节电路产生的输出称为跳频码。

振荡器作为该结构的核心，本文设计了如图 3 所示的可配置的振荡器。

图 3 中，带有使能信号(enable)的与门(A)控制该振荡器的启动与关闭，缓冲器($U_1, U_2, \cdots, U_n$)和三

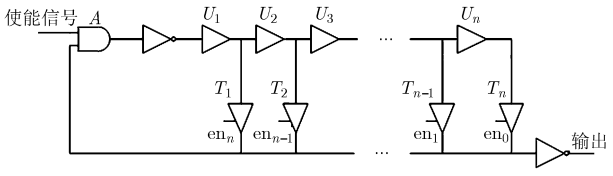

图 3 可配置的振荡器结构图

态缓冲器 $(T_1,T_2,\cdots,T_n)$ 构成了延时电路，三态缓冲器的使能信号连接到跳频码，跳频码通过控制三态缓冲器的开关来选择延时电路的延时长短，从而改变振荡器的振荡频率。在正常工作状态下，振荡器每次只有一个选择位有效。三态缓冲器和缓冲器组成的电路越长，该电路所能产生的振荡频率种数也就越多。

这种振荡器在产生响应过程中以几种频率在振荡，在每一种振荡频率下，由于制造上的随机性，振荡器之间的频率会有微小差别，假设有 k 个振荡器，它们的频率按照快慢顺序组成了一个集合，可以用下式表示：

$$F=(f_1,f_2,\cdots,f_k) \tag{3}$$

这可以称为一个频率分布段，在整个 RO 阵列中，每一种振荡频率下都存在着一个频率段，假设电路中共有 M 种振荡频率，那么系统中便存在如式(4)所示的 M 个频率段：

$$\left.\begin{aligned} F_1&=(f_1^1,f_2^1,\cdots,f_k^1)\\ F_2&=(f_1^2,f_2^2,\cdots,f_k^2)\\ &\vdots\\ F_M&=(f_1^M,f_2^M,\cdots,f_k^M) \end{aligned}\right\} \tag{4}$$

不同于传统的基于振荡器的 PUF，该结构中，当前输出的响应位不仅与当前的输入激励和当前的频率段有关，而且与上一个输出响应位也有关，它们之间的关系可以用式(5)表示。

$$R=H(C,F,R_{n-1}) \tag{5}$$

其中 H 表示它们之间的转变函数，C 是当前输入的激励，F 是当前振荡器振荡频率所组成的频率段，R_{n-1} 表示上一位响应输出，它用来决定当前的频率段。

振荡器的振荡频率在产生响应的过程中不断变化，每产生一个输出位，当前频率段便转移到下一个频率段，转移的关系由 R_{n-1} 经过一个频率调节电路之后产生的跳频码来决定，可以由式(6)表示。

$$F=G(R_{n-1}) \tag{6}$$

在得到 R_{n-1} 之后，在产生下一位输出的过程中，输入输出之间的关系可以简化成与之前传统的基于振荡器的 PUF 一样的公式，即 $R=H(C,F)$，但是由于制造上的随机差异，在不同的频率段下，振荡器之间的振荡频率快慢顺序会不一样，因此在整个过程中，F 不再是一个常数，这相当于增大了输入输出响应比的值，而且，对于相同的激励 C，在不同的频率段下，$R_i=H(C,F_i)$ 会得到不同的响应值。

3.2 频率跳变图

MFS-PUF 在产生响应过程中，频率段之间的转变顺序可以由图 4 所示的频率跳变图来描述：

如图 4 所示，在第 1 个时间段内，振荡器振荡在第 3 个频率段，在第 2 个时间段内，振荡器振荡在 5 个频率段，第 k 个时间段内，振荡器振荡在第 n 个频率段，频率段的变化是由频率调节电路产生的跳频码来决定。由于 R_{n-1} 是 0 或是 1 完全由制造上的不可控因素决定，它是由一个物理现象产生的真随机数[10]，于是跳频码的转变不可预测，频率段之间的转移便如图 4 所示的一样无规律。设计者也必须在完成设计并且经过实际测试之后才能得到这个图。由于物理制造上不可避免的差异，同一个布局下得到的 PUF 生成的频率跳变图也会不一样。

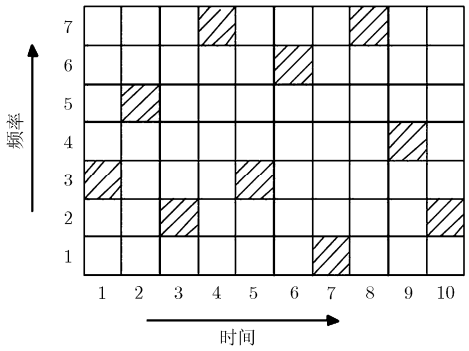

图 4 频率跳变图

进一步分析频率跳变图可知，图中涉及跳频的频率数目越多，跳频码的周期越长，即时间和频率的乘积越大，该图所能容纳的随机图案也就越多，其本身的随机性越大，这个图案也就越难以被破解。

3.3 频率调节电路的设计

跳频码的设计至关重要。由图 3 可知，跳频码的每一位都连接到一个三态缓冲器的使能输入端，振荡器振荡的时候每次都只有一个三态缓冲器有效，因此跳频码以 one-hot 编码的形式存在。为了得到一个理想的频率调节电路，各个跳频码之间的转换应该随机化，不可预测。

由图 4 可知，为了使设计的系统的安全性更高，振荡器应有较多的振荡频率，因此振荡器中的三态缓冲器数量会比较多，跳频码的长度也会相应地变得很长。直接对这些 one-hot 形式的跳频码进行设计的难度会因为振荡器级数的增加而加大，并且也很难直接定义一个两个 one-hot 码之间的随机转换关系。这里，本文提出了一种新方法，即先生成一个随机序列发生器，然后对这个随机序列进行译码得到想要的 one-hot 码。对于一个 N 位的 one-hot 码，其对应的随机序列元素只需要 $\log_2 N$ 位即可，这样不仅可以保证随机性，而且相对于直接控制 one-hot 码来说也更容易实现。

LFSR 作为一种很好的伪随机数发生器，可以被用来实现这个频率调节电路，并且其可以很容易在 FPGA 上实现。为了得到随机性更强的序列，本文利用了两种相同规格的 LFSR 函数和相应的译码电路来实现频率调节电路，如图 5 所示。

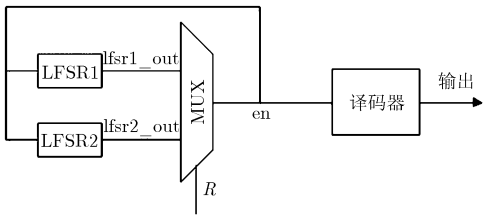

图 5 频率调节电路

该频率调节电路使用了两种相同规格的LFSR。这里利用的是整个 LFSR 序列而不是其当前的输出位。这两个 LFSR 函数产生的元素相同，但是由于产生机制不一样，相同元素在排列顺序上有所差别。一个 2 选 1 的选择器决定了输出的 en 信号，可以用下式表示：

$$\text{en} = \begin{cases} \text{lfsr1\_out1}, & R=1 \\ \text{lfsr2\_out}, & R=0 \end{cases} \tag{7}$$

选择器的输入控制位连到上一位 PUF 的输出 R_{n-1}。由于 R_{n-1} 是一个真随机数[10]，于是 LFSR1 和 LFSR2 之间的选择不可预测，输出的值也随机。同时，这个选择器的输出值又反馈回这两个 LFSR 的输入口作为下一次 LFSR 的输入值。这样的结构比单纯的 LFSR 结构更复杂，产生的序列更长，在不知道具体电路结构的前提下，攻击者无法准确预测序列发生器下一个输出的是什么。

译码电路主要用来生成符合延时电路选择位格式的跳频码。

3.4 对 MFS-PUF 的安全性分析

MFS-PUF 能有效地避免攻击者采用建模的方法来攻击。

由图 6 可知，采用建模方式攻击只在有限的时间域内是正确的，假设攻击者认为的振荡频率是在第 5 个频率段内，他只有在第 2 个时间段内正确，因此即使攻击者已经破解了当前频率段下各个振荡器之间振荡频率的快慢顺序 F_5，其只可以正确得到当前时刻下的输出位，但是在其他的时间段，频率段已经转变，振荡器之间的快慢顺序也不会与 F_5 中的一致，因此得不到正确的结果。

如文献[6]所述，尽管攻击者仍然可以在得到一定数量的输入输出响应对之后得出一个振荡器之间

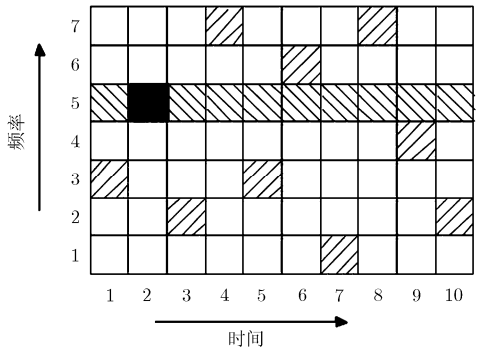

图 6 对传统的攻击方式的分析

频率的快慢关系 $F'=(f_1^{'},f_2^{'},\cdots,f_k^{'})$，但是这个频率并不在涉及的任何一个频率段之内，采用这个结果来进行预测不会得到正确的结果，因此这样的攻击方式无效。

现在假设攻击者知道该 PUF 内的振荡器频率可变且知道其内存在着 M 种频率，由于无法通过物理攻击的方式获得序列发生器的结构，因此在没有任何其他信息的条件下他无法得到振荡频率段的转移顺序。同时，由于振荡器的频率一直在变，攻击者无法知道当前输入下所处的频率段，也不知道下一个频率段是什么，因此无法用之前所述的方式来得到各个频率段下各个振荡器频率的快慢顺序。

如果用穷举的方式来破解这个电路，对于 $k+1$ 个振荡器，每个频率段下的快慢顺序均有 $(k+1)!$ 种，而对于 M 个频率段，攻击者可以先假定其处于某个频率段，这共有 M 种可能性，产生第 1 位输出后，根据频率跳变图，频率段转移到剩下的 $M-1$ 个频率段中的任意一个，但是其无法知晓，同样，之后每产生一位输出，下一个频率段还是 $M-1$ 种可能性。假设该 PUF 共输出 k 位，输出过程中频率段的快慢顺序均有 $(k+1)!$ 种，产生第 1 位输出时频率段有 M 种可能，产生之后的 $k-1$ 位时频率段均有 $M-1$ 种可能，所以所有可能的情况有 $M\cdot(M-1)^{k-1}\cdot[(k+1)!]^M$ 种，每一种被取到的可能性都为 $(M\cdot(M-1)^{k-1}\cdot[(k+1)!]^M)^{-1}$，攻击成功所需尝试的次数的数学期望为

$$\begin{aligned} N &= \frac{1}{M\cdot(M-1)^{k-1}\cdot[(k+1)!]^M}(1+2+\cdots \\ &\quad + M\cdot(M-1)^{k-1}\cdot[(k+1)!]^M) \\ &= \frac{1+M\cdot(M-1)^{k-1}\cdot[(k+1)!]^M}{2} \end{aligned} \tag{8}$$

表 1 比较了 M 和 k 在不同的取值下攻击次数的数学期望，可知，PUF 中振荡器的振荡频率越多，产生的 PUF 输出位数越多，攻击者需要尝试比较的次数以指数级增长，这与频率跳变图上得到的结论

表 1 破解不同规格 PUF 所需攻击次数的比较

M	k	N
3	5	8.96×10^{9}
7	5	1.20×10^{22}
7	15	4.81×10^{104}
15	15	5.37×10^{216}
15	35	2.52×10^{663}

相一致。对于一个小规模的 PUF，当 M 取值为 7，k 为 15 时，破解该系统所需比较的平均次数已经超过 4.81×10^{104}，而传统的基于振荡器的 PUF，当攻击者获得各个振荡器之间的相对频率关系后，其用来攻击成功率为 100%。本文的设计大大提高了安全性。

4　实验结果分析

本文在 10 块不同的 XILINX VIRTEX II-PRO FPGA 板上实现了本文提出的 MFS-PUF。振荡器选择含有 8 个三态缓冲器的电路，因此只需 3 位的 LFSR 来实现跳频码。3 位的 LFSR 共有 3 种实现形式，效果一样，可以任选两种，本文选择的 LFSR 公式如式(9)，式(10)：

$$\text{LFSR1:}\quad f(x)=x^3+x^2+1 \tag{9}$$

$$\text{LFSR2:}\quad f(x)=x^3+x+1 \tag{10}$$

选择器的输出通过一个 3-8 译码器来生成跳频码。振荡器通过 fpga_editor 封装成硬宏单元，这样可以保证每个振荡器完全一样，频率差别完全取决于制造上的差异。整个电路例化了 16 个振荡器，共可以生成 15 位输出。

如图 7 所示，将 16 个振荡器排列成一个 4×4 的矩阵，按图中所示的顺序，每次取相邻的两个进行比较输出。输出的结果如表 2 所示。由表 2 可知，各个 FPGA 板之间的 PUF 输出各不相同。

各个输出之间的汉明距离分布如图 8 所示。图中，横坐标表示两个输出之间汉明距离的大小，纵坐标表示该汉明距离的个数。在理想情况下，各板子之间响应的不同的位数占总响应位数的一半，本

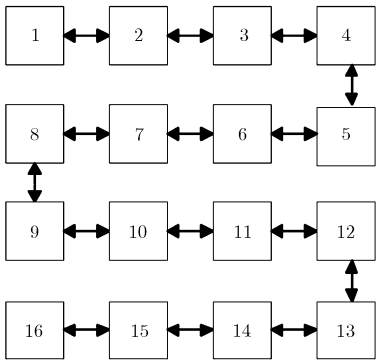

图 7 振荡器的排列及比较方式

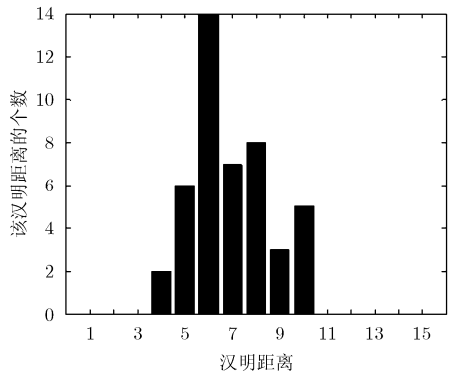

图 8 输出之间汉明码的分布图

表 2 各个 FPGA 板的 PUF 输出值比较

FPGA 板序号	输出值(按位)														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	0	0	1	0	0	1	0	1	0	0	1	1	0	1	1
2	1	0	1	1	0	1	0	0	1	1	1	0	0	1	1
3	1	1	0	1	0	0	0	1	0	0	0	1	0	1	1
4	1	0	1	0	1	0	1	0	0	1	1	1	0	0	0
5	1	0	1	0	1	0	0	1	0	0	0	0	1	1	1
6	0	1	1	0	1	1	0	1	0	0	1	0	1	0	0
7	0	1	0	1	1	0	0	1	1	0	1	0	0	0	1
8	1	0	0	0	1	0	0	1	1	1	1	1	0	0	1
9	0	1	0	0	1	0	1	1	0	1	1	1	0	1	1
10	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1

实验得到的结果符合这个情况。

为了检验我们的设计是否具有唯一性，将上述得到的汉明距离代入式(11)[8]：

$$U = \frac{2}{k(k-1)} \sum_{i=1}^{i=k-1} \sum_{j=i+1}^{j=k} \frac{h_{ij}}{n} \times 100\% \qquad (11)$$

式(11)中，h_{ij} 是两块不同 FPGA 板产生的响应之间的汉明距离，i 和 j 表示不同板子的序号，式(11)的含义是各板子间不同响应的位数的平均数占总响应位数的比例，经计算该值为 46.2%，接近理想情况下的 50%。

5 结束语

PUF 作为保护集成电路芯片安全的新方法正在受到越来越多的关注，对于其安全性的要求也越来越高。传统的基于振荡器的 PUF 由于在产生响应过程中振荡器的振荡频率单一，因此存在着被破解的隐患。本文提出的多频率段物理不可克隆函数(MFS-PUF)采用可配置的振荡器并且引入了一个频率调节电路，将上一位 MFS-PUF 的输出位加载到频率调节电路上得到跳频码并反馈回振荡器组中，使得振荡器频率随输出的变化而相应改变。振荡器振荡频率越多，频率调节电路产生的跳频码周期越长，该结构就越难被攻击。这种改变在保证 PUF 性能的前提下大大提高了其自身的安全性，这将使其得到更加广泛的应用。

参 考 文 献

[1] Gassend B, Clarke D, Van Dijk M, *et al.*. Silicon physical random functions[C]. Proceedings of the 9th ACM Conference on Computer and Communications Security, New York, NY, USA, 2002: 148–160.

[2] Lim Daihyun, 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] Suh G E and Devadas S. Physical unclonable functions for device authentication[C]. Proceedings of the 44th Annual Design Automation Conference, New York, NY, USA, 2007: 9–14.

[4] Anderson Jason H. A PUF design for secure FPGA-based embedded systems[C]. Proceedings of the 2010 Asia and South Pacific Design Automation Conference, IEEE Press Piscataway, NJ, USA, 2010: 1–6.

[5] Li Xiao-xun, Gao Zhi-qiang, and Bai Guo-qiang. Design and FPGA implementation of secure key management[J]. *Lecture Notes in Engineering and Computer Science*, 2011, 2189(1): 1049–1054.

[6] Ührmair U R, Sehnke F, Ölter J S, *et al.*. Modeling attacks on physical unclonable functions[C]. Proceedings of the 17th ACM Conference on Computer and Communications Security, New York, NY, USA, 2010: 237–249.

[7] Dillard R A. Detectability of spread-spectrum signals[J]. *IEEE Transactions on Aerospace and Electronic Systems*. 1979, AES-15(4): 526–537.

[8] Maiti A and Schaumont P. Improving the quality of a physical unclonable function using configurable ring oscillators[C]. International Conference on Field Programmable Logic and Applications, FPL 2009, USA, 2009: 703–707.

[9] Merli D and Eckert C. Improving the quality of ring oscillator PUFs on FPGAs[C]. Proceedings of the 5th Workshop on Embedded Systems Security, New York, NY, USA, 2010: Article No. 9.

[10] Maiti A, Nagesh R, Reddy A, *et al.*. Physical unclonable function and true random number generator: a compact and scalable implementation[C]. Proceedings of the 19th ACM Great Lakes Symposium on VLSI, New York, NY, USA, 2009: 425–428.

项群良： 男，1987 年生，硕士生，研究方向为嵌入式系统可靠性技术.

张培勇： 男，1977 年生，副教授，研究方向为集成电路 CAD 技术.

欧阳冬生： 男，1987 年生，硕士生，研究方向为 VLSI 可测性设计.

冯忱晖： 男，1990 年生，博士生，研究方向为嵌入式系统安全性.