计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.181202390

# 自动纠错 CRO PUF 密钥生成方案

张向阳[1]　孙子文[1,2]
1 江南大学物联网工程学院　江苏 无锡 214122
2 江南大学物联网技术应用教育部工程研究中心　江苏 无锡 214122
(xiangyangz@126.com)

**摘　要**　针对射频识别(Radio Frequency Identification,RFID)安全问题中的加密技术,设计了自动纠错 CRO PUF 密钥生成方案。该方案将数字通信系统中重复码的纠错思想应用到可配置环形振荡器物理不可克隆函数(Configurable Ring-oscillator Physical Unclonable Function,CRO PUF)结构中,对相邻 CRO 的最终振荡频率进差行分运算得到 3 位输出响应值,然后对输出响应值进行纠错处理,得到一位自动纠错 CRO PUF 输出信息,从而实现 CRO PUF 电路自动纠错;利用模糊提取器中注册阶段和重构阶段的纠错码编解码技术的纠错特性来纠正复现输出信息向量存在的比特跳变误差,然后使用 Hash 模块对纠错后的 PUF 复现输出信息向量进行数据加密以生成密钥。基于 Linux 系统,利用 Cadence virtuoso 中 specture 环境下的 TSMCO 0.18um,1.8V CMOS0 工艺库对自动纠错 CRO PUF 电路进行 Monte Carlo 模拟仿真,使用 MATLAB 对 PUF 电路复现输出信息向量进行模糊提取器处理。由仿真实验数据可得,自动纠错 CRO PUF 电路在电源电压影响下的最高、最低可靠性分别为 98.96%和 92.71%;在温度影响下的最高、最低可靠性分别为 99.10%和 93.75%。实验结果表明,相对于 CRO PUF 电路,自动纠错 CRO PUF 的可靠性与均匀性有了明显提高;从整体情况看,自动纠错 CRO PUF 与 CRO PUF 电路的唯一性没有一方处于明显的优势或劣势,但对两组数据进行方差计算和比较后发现,自动纠错 CRO PUF 的唯一性与标准值 50%之间有着更好的逼近效果。经模糊提取器处理后的 PUF 复现输出响应向量的可靠性进一步提高,且高达 99.8%,其受环境因素干扰非常小,可直接用作密钥。

**关键词**:CRO PUF;模糊提取器;纠错码;重复码;Hash 模块
**中图法分类号**　TP331

## Automatic Error Correction CRO PUF Key Generation Scheme

ZHANG Xiang-yang[1] and SUN Zi-wen[1,2]
1 School of Internet of Things Engineering,Jiangnan University,Wuxi,Jiangsu 214122,China
2 Engineering Research Center of Internet of Things Technology Applications,Ministry of Education,Jiangnan University,Wuxi,Jiangsu 214122,China

**Abstract**　For the encryption technology in the radio frequency identification security problem,this paper designed an automatic error correction CRO PUF key generation scheme. The error correction idea of the repeated code in the digital communication system is applied to the Configurable Ring-oscillator Physical Unclonable Function structure,and a 3-bit output value is obtained by performing a differential operation on the final oscillation frequency of adjacent CRO. The output response value is subjected to error correction processing to obtain an automatic error correction CRO PUF output information,thereby realizing automatic error correction of the CRO PUF circuit. The error correction characteristics of the error correction code encoding and decoding technology in the registration phase and the reconstruction phase of the fuzzy extractor are used to correct the bit hopping error of the reproduced output information vector,and the error-corrected vector encrypted by PUF reproduction output information vector uses the Hash module to generate a secret key. In the Linux system,the Monte Carlo simulation of the automatic error correction CRO PUF circuit is carried out by using the TSMCO 0.18um,1.8V CMOS0 process library in the spectrum environment of Cadence virtuoso,and the output information vector of the PUF circuit is reproduced by using MATLAB for fuzzy extractor processing. The simulation results show that the highest reliability of the automatic error correction CRO PUF circuit under the influence of power supply voltage is 98.96%,the lowest reliability is 92.71%. The highest reliability under the influence of temperature is 93.75%,the lowest reliability is 84.90%. The uniformity of the automatic error correction CRO PUF is significantly

到稿日期:2018-11-23　返修日期:2019-01-25　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61373126);中央高校基本科研业务费专项资金(JUSRP51510);江苏省自然科学基金(BK20131107)
This work was supported by the National Natural Science Foundation of China (61373126),Fundamental Research Funds for the Central Universities of Ministry of Education of China (JUSRP51510) and Natural Science Foundation of the Higher Education Institutions of Jiangsu Province,China (BK20131107).
通信作者:孙子文(sunziwen@jiangnan.edu.cn)

improved compared with the CRO PUF. As a whole, the uniqueness of the automatic error correction CRO PUF and CRO PUF is not in a distinct advantage or disadvantage, but the automatic error correction CRO PUF has a better approximation effect with the standard value of 50% after the variance calculation being performed on the two groups of data. The reliability of the PUF reproduced output response vector processed by the fuzzy extractor is further improved, up to 99.8%, which is almost immune to environmental factors and can be directly used as a key.

**Keywords** CRO PUF, Fuzzy extractor, Error correcting code, Repeated code, Hash module

## 1 引言

高速发展的物联网(Internet of Things，IoT)技术在给社会带来巨大经济效益的同时，也导致了诸多信息安全问题。RFID 作为物联网应用中的一种重要技术，同样存在亟待解决的安全问题。加密技术是保护 RFID 系统安全的关键技术，密钥的生成方案成为了近些年的研究热点。物理不可克隆函数(Physical Unclonable Function，PUF)由于其独有的不可克隆特性，成为了目前研究生成 RFID 密钥的一种全新方法。

Pappu 等[1]首次提出单向物理函数(Physical One-way Function)，且得出单向物理函数不依赖数学理论知识，而是通过物理介质传输理论来获得唯一的、不可克隆和不可预测的二进制标识符的方法。此后，Gassend 等[2]提出了 PUF，利用制造过程中工艺的随机偏差来产生独有的标识符。PUF 的种类众多，如基于仲裁器 PUF[3]、环形振荡器 PUF[4]、蝴蝶 PUF[5]、SRAM PUF[6]等。在环境因素(电源电压、温度等)的影响下，相对于其他 PUF，环形振荡器物理不可克隆函数(Ring-oscillator Physical Unclonable Function，RO PUF)产生的误差较小，且其制造简单，因此被广泛用于生成密钥[7]。

RO PUF 作为一种强 PUF，利用芯片在制造过程中产生的物理差异来生成独一无二的标志符，具有较高的抵抗模型构建攻击的能力[8]。但一个 RO PUF 电路只能产生一组激励响应对(Challenge Response Pairs，CRPs)，且电路在受到环境干扰时其可靠性较低。Maiti 等[9]提出的 CRO PUF 在 RO PUF 的基础上采用可配置环形振荡器(Configurable Ring-oscillator，CRO)代替环形振荡器(Ring-oscillator，RO)，以解决 RO PUF 中 CRPs 过少的问题。但 CRO PUF 在相同激励的多次作用下生成的复现输出信息向量存在比特跳变现象，其可靠性还有较大的提升空间。Suh 等[10]提出的 $K$($K$ 一般为 8)选 1 RO PUF，在 RO PUF 的基础上采用 $K$ 选 1 结构，在一定程度上提高了 RO PUF 的可靠性；但 $K$ 选 1 RO PUF 通过牺牲大量硬件资源也只一定程度地提高了可靠性，其在生成复现输出信息向量时仍然存在比特跳变误差。可见，文献[9-10]两种形式的 PUF 电路的输出信息向量存在不同程度的比特跳变误差，不能直接用作密钥。为了消除 PUF 电路复现输出信息向量存在的比特跳变误差，文献[11]提出使用模糊提取器对 PUF 的输出信息向量进行数据处理，使得经过数据处理的 PUF 电路的输出信息序列能够直接用作密钥。模糊提取器于 2004 年由 Dodis 等[12]首次提出，它利用纠错码对数据中存在的误差进行纠错。纠错码[13]作为一种检测和纠错的编解码技术，有线性分组码、完备码、RM 码和 BCH[13]码等多种类型。文献[11]中的模糊提取器选用 BCH 码来进行纠错，但由于 PUF 复现输出信息向量的误差较大，以至于纠错码码字较长，纠错效率较低。

为了提高 PUF 电路输出信息向量的可靠性，缩短模糊提取器中纠错码码字的长度并提高纠错效率，本文设计了自动纠错 CRO PUF 密钥生成方案。将数字通信系统中重复码的纠错思想应用到 CRO PUF 结构中，以实现 PUF 电路的自动纠错功能；使用模糊提取器对自动纠错 CRO PUF 电路生成的输出信息向量进行数据处理，以进一步提高 PUF 电路的可靠性，使最终生成的密钥可直接用于加密技术中。

## 2 CRO PUF 及其可靠性问题

CRO PUF 的基本原理是通过测量 CRO 的振荡频率差异来提取 CRPs。CRO PUF 由 $n$ 个 CRO 阵列、$2n$ 个计数器(Counter)和 $n$ 个比较器组成[7]，其基础结构如图 1 所示。

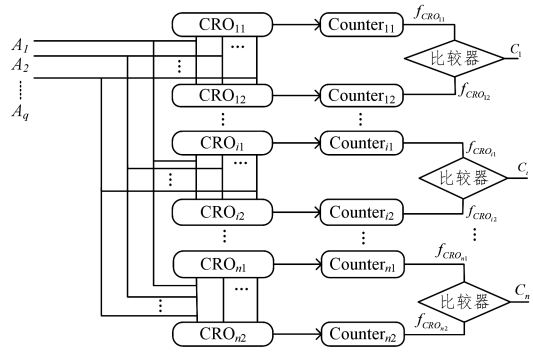


图 1 CRO PUF 结构

Fig. 1 CRO PUF structure

CRO PUF 中所有 CRO 的设计和布局完全一致，CRO 由 $q$ 个反相器对级联构成，其结构如图 2 所示。$(A_1, A_2, \cdots, A_q)$ 作为 CRO PUF 的激励，通过 $(A_1, A_2, \cdots, A_q)$ 的取值来选择 CRO 的导通方式，当 $A_1=0$ 时，$A_1$ 对应反相器对中的上反相器导通，当 $A_1=1$ 时，反相器对中的下反相器导通，$A_2$ 到 $A_q$ 对应反相器对的导通规则与 $A_1$ 相同。

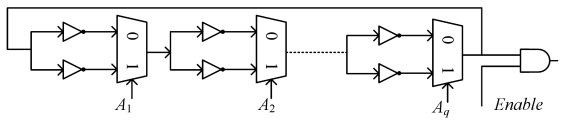


图 2 CRO 结构

Fig. 2 CRO structure

CRO 作为以特定频率振荡的集成电路，其振荡频率[14]取决于导通反相器的个数 $q$(奇数)和导通反相器的延迟时间 $t_{\text{delay}}$。CRO 振荡频率的计算如式(1)所示：

$$f_{CRO_{is}}=\frac{1}{2*t_{\text{delay}}*q} \tag{1}$$

其中，$i\in\{1,2,3,\cdots,n\}$ 表示 CRO PUF 中的第 $i$ 个 $CRO_i$ 阵列；$s\in\{1,2\}$ 表示 $CRO_i$ 阵列中的第 $s$ 个 CRO；$f_{CRO_{is}}$ 表示第 $i$ 个 $CRO_i$ 阵列中的第 $s$ 个 CRO 的振荡频率。

CRO PUF 在比较器中对相邻 CRO 的振荡频率进行比较，得到 CRO PUF 输出信息序列中的第 $i$ 位信息 $C_i$，如式(2)所示：

$$C_i=\begin{cases}1, & f_{CRO_{i1}}>f_{CRO_{i2}}\\ 0, & \text{其他}\end{cases} \tag{2}$$

其中，$i\in\{1,2,3,\cdots,n\}$ 表示 CRO PUF 输出信息向量中的第 $i$ 位信息。

理论上，两个 CRO 的振荡频率因环境因素导致的变化应该一致，如图 3(a)所示，此时环境因素并不足以导致 CRO PUF 的输出信息发生比特跳变；但实际上两个 CRO 振荡频率因环境因素导致的变化并不一致，如图 3(b)所示，此时 CRO 振荡频率在环境因素的影响下产生随机性偏差，导致 CRO PUF 电路的输出信息向量在相同激励的多次作用下出现比特跳变的现象，降低了 CRO PUF 电路的可靠性。

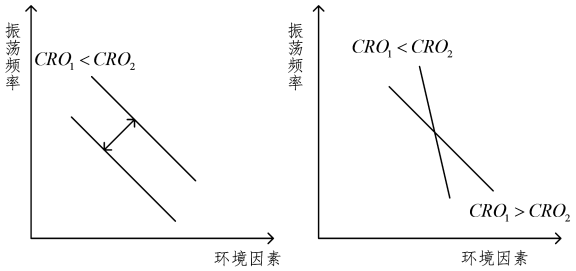


图 3 振荡频率受环境因素影响的变化

Fig. 3 Oscillation frequency affected by environmental factors

## 3 自动纠错 CRO PUF 密钥生成方案

本文通过改进 CRO PUF 结构得到自动纠错 CRO PUF，并经模糊提取器对后续 PUF 输出进行数据处理，设计自动纠错密钥生成方案，并生成长度为 $n$ 的 CRO PUF 密钥。本方案由自动纠错 CRO PUF、数据库和模糊提取器构成，其中，自动纠错 CRO PUF 用于实现 PUF 电路的自动纠错，提高 PUF 电路的部分可靠性；数据库用于存储模糊提取器在注册阶段生成的辅助数据和随机数；模糊提取器[15]用于处理自动纠错 CRO PUF 电路产生的输出信息向量，消除自动纠错 CRO PUF 复现输出信息向量存在的误差，并产生的密钥。

### 3.1 自动纠错 CRO PUF

(1)自动纠错 CRO PUF 的组成结构

自动纠错 CRO PUF 的结构如图 4 所示。它由 $n$ 个自动纠错 $CRO_i$ 阵列组成，每一个自动纠错 $CRO_i$ 阵列在激励($A_1$，$A_2$，…，$A_q$)的作用下生成一位 PUF 输出信息，$n$ 个自动纠错 $CRO_i$ 阵列生成 $n$ 位输出信息，组成 PUF 输出信息序列。

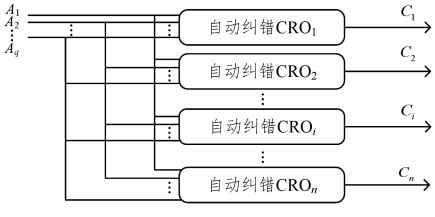


图 4 自动纠错 CRO PUF 的组成结构

Fig. 4 Composition chart of automatic error correction CRO PUF

自动纠错 CRO PUF 中的一个 $CRO_i$ 阵列结构如图 5 所示。每个 $CRO_i$ 阵列由 4 个 CRO 并联组成，阵列中所有 CRO 的结构布局完全一致。在激励($A_1$，$A_2$，…，$A_q$)的作用下，每个 CRO 的计数器计算对应 CRO 的最终振荡频率，对相邻两个 CRO 的最终振荡频率依次进行差分运算得到 3 位输出响应值，并对输出响应值进行纠错处理得到一位 PUF 输出信息 $C_i$。每个阵列输出一位信息，$n$ 个阵列共输出 $n$ 位 PUF 信息位。

下文讨论中，($A_1$，$A_2$，…，$A_q$)取值不变，且所有 CRO 导通都相同。

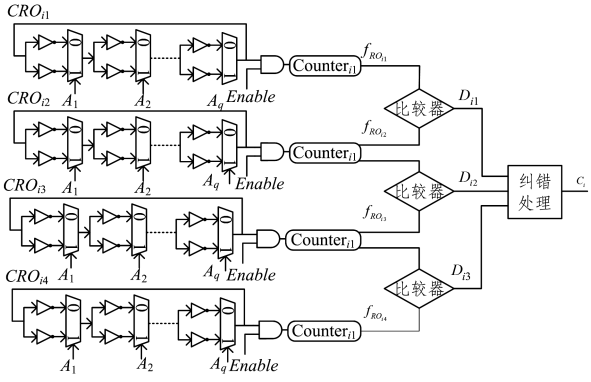


图 5 自动纠错 $CRO_i$ 的结构

Fig. 5 Structure of automatic error correction $CRO_i$

(2)CRO 输出响应值生成规则

CRO 的最终振荡频率由 3 部分组成：理论振荡频率、制造工艺误差振荡频率延迟和系统误差振荡频率延迟[8]。

$$f_{CRO_{ij}}=f_{CTOY_{ij}}+f_{CRAN_{ij}}+f_{CSYT_{ij}} \tag{3}$$

其中，$i\in\{1,2,3,\cdots,n\}$ 表示第 $i$ 个自动纠错 $CRO_i$ 阵列；$j\in\{1,2,3,4\}$ 表示第 $j$ 个 CRO，即 $CRO_{ij}$ 为第 $i$ 个自动纠错阵列 $CRO_i$ 中的第 $j$ 个 CRO；$f_{CRO_{ij}}$ 为 $CRO_{ij}$ 的最终振荡频率；$f_{CTOY_{ij}}$ 为 $CRO_{ij}$ 的理论振荡频率，结构布局完全一致的 CRO 的 $f_{CTOY_{ij}}$ 值应一致；$f_{CRAN_{ij}}$ 为 $CRO_{ij}$ 的制造工艺误差振荡频率延迟，该延迟由 CRO 制造生成过程中的工艺误差引起，$f_{CRAN_{ij}}$ 的值是随机的；$f_{CSYT_{ij}}$ 表示 $CRO_{ij}$ 的系统误差振荡频率延迟，该延迟由 $CRO_{ij}$ 的位置差异导致。

同一阵列中相邻两个 CRO 的最终振荡频率的差分结果是生成输出响应的依据。为此，计算 $CRO_i$ 阵列中的第 $j$ 个和第 $j+1$ 个 CRO 的最终振荡频率的差值：

$$\begin{aligned}\Delta f_{CRO_{i(j,j+1)}}&=f_{CRO_{ij}}-f_{CRO_{i(j+1)}}\\&=(f_{CTOY_{ij}}+f_{CRAN_{ij}}+f_{CSYT_{ij}})-(f_{CTOY_{i(j+1)}}+\\&\quad f_{CRAN_{i(j+1)}}+f_{CSYT_{i(j+1)}})\\&\approx f_{CRAN_{ij}}-f_{CRAN_{i(j+1)}}\end{aligned} \tag{4}$$

可见，由于相邻 CRO 的系统误差振荡频率延迟近似相等[8]，相邻 CRO 的最终振荡频率的差分运算消除了 CRO 中的系统误差振荡频率的延迟差异，因此最终振荡频率差值仅来源于制造工艺误差引起的振荡频率延迟。

比较器通过相邻 CRO 之间的最终振荡频率差值得到一位输出响应值。$CRO_i$ 阵列的第 $j$ 位输出响应值 $D_{ij}$ 取决于 $CRO_{ij}$ 与 $CRO_{i(j+1)}$ 的最终振荡频率差值，规则如下：

$$D_{ij}=\begin{cases}1, & \Delta f_{CRO_{i(j,j+1)}}>0\\ 0, & \Delta f_{CRO_{i(j,j+1)}}\leqslant 0\end{cases} \tag{5}$$

其中，$j=1,2,3$。

为便于描述，$CRO_i$ 阵列在无环境干扰条件下由激励 $(A_1,A_2,\cdots,A_q)$ 作用得到的由 3 位标准输出响应值组成的标准输出响应向量用上标 0 表示，$CRO_i$ 在有环境干扰条件下由激励 $(A_1,A_2,\cdots,A_q)$ 作用得到的由 3 位复现输出响应值组成的复现输出响应向量不带上标，分别如式(6)、式(7)所示：

$$\boldsymbol{D}_i^0=(D_{i1}^0,D_{i2}^0,D_{i3}^0) \tag{6}$$

$$\boldsymbol{D}_i=(D_{i1},D_{i2},D_{i3}) \tag{7}$$

每个 $CRO_i$ 阵列对应一个标准输出响应向量和一个复现输出响应向量，$n$ 个阵列共生成 $n$ 个标准输出响应向量 $\boldsymbol{D}_i^0(i=1,2,\cdots,n)$ 和 $n$ 个复现输出响应向量 $\boldsymbol{D}_i(i=1,2,\cdots,n)$。

(3)PUF 输出信息生成规则

设自动纠错 CRO PUF 在无环境干扰条件下由激励 $(A_1,A_2,\cdots,A_q)$ 作用生成的标准输出信息向量 $\boldsymbol{C}^0$ 为：

$$\boldsymbol{C}^0=(C_1^0,C_2^0,\cdots,C_i^0,\cdots,C_n^0) \tag{8}$$

其中，各信息位 $C_i^0$ 直接由标准输出响应向量 $\boldsymbol{D}_i^0$ 中的 $D_{i1}^0$ 得到：

$$C_i^0=D_{i1}^0 \tag{9}$$

设自动纠错 CRO PUF 在有环境干扰条件下由激励 $(A_1,A_2,\cdots,A_q)$ 作用生成的复现输出信息向量 $\boldsymbol{C}$ 为：

$$\boldsymbol{C}=(C_1,C_2,\cdots,C_i,\cdots,C_n) \tag{10}$$

其中，复现输出信息向量 C 中的各信息位由复现输出响应向量进行纠错处理后得到，C 中第 $i$ 位信息 $C_i$ 由对应的复现输出响应向量 $\boldsymbol{D}_i$ 纠错得到。

环境干扰的存在，导致复现输出响应向量中元素的值可能存在比特跳变现象，以至于 PUF 电路生成的复现输出响应向量可能出现差错。因此，利用自动纠错 $CRO_i$ 的标准输出响应向量 $\boldsymbol{D}_i^0=(D_{i1}^0,D_{i2}^0,D_{i3}^0)$ 对复现输出响应向量 $\boldsymbol{D}_i=(D_{i1},D_{i2},D_{i3})$ 的比特跳变进行纠错。根据重复编码纠错思想，采用标准输出响应向量 $\boldsymbol{D}_i^0$ 为复现输出响应向量 $\boldsymbol{D}_i$ 构造一个与输出信息向量中的信息位 $C_i$ 相关的重复编码：

$$\boldsymbol{Q}_i=(\boldsymbol{Q}_{i1},\boldsymbol{Q}_{i2},\boldsymbol{Q}_{i3}) \tag{11}$$

各元素的编码规则为：

$$Q_{ij}=\begin{cases}D_{i1}, & j=1\\ D_{ij}\oplus D_{ij}^0\oplus D_{i1}^0, & j>1\end{cases} \tag{12}$$

其中，$j=1,2,3$。

由式(12)可知，重复编码是通过将标准输出响应向量 $\boldsymbol{D}_i^0$ 中的元素与复现输出响应向量 $\boldsymbol{D}_i$ 中的元素进行异或得到的，所以 $\boldsymbol{Q}_i$ 中的大部分元素值为 $D_{i1}^0$，即标准输出信息向量 $\boldsymbol{C}^0$ 中的 $C_i^0$，因此，可通过重复解码的思想对 $\boldsymbol{Q}_i$ 进行解码得到正确的 $C_i$，从而达到纠错的目的。

复现输出信息向量 $\boldsymbol{C}$ 中信息位 $C_i$ 的生成规则采用重复编码纠错规则：

$$C_i=decode(\boldsymbol{Q}_i) \tag{13}$$

其中，$i=1,2,\cdots,n$；$decode(\ )$ 为重复码解码算法，将 $C_i$ 解码为 $\boldsymbol{Q}_i$ 中出现次数最多的元素。

### 3.2 模糊提取器

自动纠错 CRO PUF 在一定程度上可提高 PUF 可靠性，但当自动纠错 CRO PUF 的复现输出响应向量存在的比特跳变误差超过重复码的纠错范围时，自动纠错 CRO PUF 生成的复现输出信息向量 $\boldsymbol{C}$ 仍会存在一定的比特跳变误差。针对此问题，采用模糊提取器(fuzzy extractor)[15] 对自动纠错 CRO PUF 的复现信息向量 $\boldsymbol{C}$ 进行数据处理，以进一步消除复现输出信息向量 $\boldsymbol{C}$ 中的比特跳变误差，使自动纠错 CRO PUF 密钥生成方案的最终输出数据可以直接用作密钥。

模糊提取器结构如图 6 所示，它由注册阶段、重构阶段和 Hash 模块[11] 组成。模糊提取器的纠错能力取决于注册阶段和重构阶段的纠错码。纠错码作为一种检测和纠正错误的编解码技术，将信息码元与监督码元建立关系，根据编码规则判断复现信息是否存在误差，若存在误差，则按照解码规则纠正。

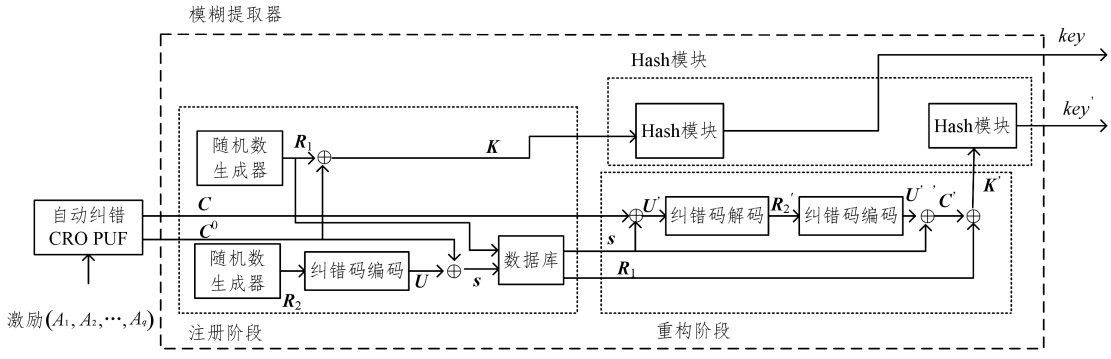


图 6 模糊提取器结构

Fig. 6 Structure diagram of fuzzy extractor

注册阶段：1)生成包含有标准输出信息向量 $\boldsymbol{C}^0$ 的辅助数据 $\boldsymbol{S}$，将 $\boldsymbol{S}$ 与随机数生成器生成的随机数 $\boldsymbol{R}_1$ 一起存储在数据库中，$\boldsymbol{S}$ 和 $\boldsymbol{R}_1$ 在重构阶段被调用；2)将标准输出信息向量 $\boldsymbol{C}^0$ 与随机数 $\boldsymbol{R}_1$ 异或，得到加密后的标准输出信息向量 $\boldsymbol{K}$。

模糊提取器中注册阶段的过程如图 6 所示，注册阶段生成的辅助数据 $\boldsymbol{S}$ 如式(14)所示：

$$\boldsymbol{S}=\boldsymbol{C}^0\oplus\boldsymbol{U} \tag{14}$$

其中，$\boldsymbol{S}=(S_1,S_2,\cdots,S_n)$，$\boldsymbol{U}=(U_1,U_2,\cdots,U_n)$。$\boldsymbol{U}$ 为 $\boldsymbol{R}_2$ 经纠错码编码后产生的输出值，如式(15)所示：

$$\boldsymbol{U}=enc(\boldsymbol{R}_2) \tag{15}$$

其中，$\boldsymbol{R}_2=(R_{21},R_{22},\cdots,R_{2l})$ 为 $l$ 位二进制随机数，$l$ 的大小取决于纠错码[16] 的选择及构造，$enc()$ 为纠错码编码过程。

自动纠错 CRO PUF 的标准输出信息向量 $\boldsymbol{C}^0$ 进行加密：

$$\boldsymbol{K}=\boldsymbol{C}^0\oplus\boldsymbol{R}_1 \tag{16}$$

其中，$\boldsymbol{K}=(K_1,K_2,\cdots,K_n)$，$\boldsymbol{R}_1=(R_{11},R_{12},\cdots,R_{1n})$。

重构阶段：1)利用注册阶段生成的辅助数据 $\boldsymbol{S}$ 对复现输出信息向量 $\boldsymbol{C}$ 进行纠错重构，得到 $\boldsymbol{C}'$；2)将 $\boldsymbol{C}'$ 与随机数 $\boldsymbol{R}_1$ 异或，得到加密后的复现输出信息向量 $\boldsymbol{K}'$。

模糊提取器中重构阶段的过程如图 6 所示，其中纠错码解码的输入如式(17)所示：

$$\boldsymbol{U}'=\boldsymbol{C}\oplus\boldsymbol{S} \tag{17}$$

其中，$\boldsymbol{U}'=(U_1',U_2',\cdots,U_n')$。

由式(14)反推得到：$\boldsymbol{U}=\boldsymbol{C}^0\oplus\boldsymbol{S}$。结合式(17)可知，复现输出信息向量 $\boldsymbol{C}$ 与标准输出信息向量 $\boldsymbol{C}^0$ 之间的比特跳变误差的位置和数量，可以转化为 $\boldsymbol{U}$ 与 $\boldsymbol{U}'$ 之间的差异。

重构阶段中对复现输出信息向量 $\boldsymbol{C}$ 进行纠错重构：

$$\boldsymbol{R}_2'=dec(\boldsymbol{U}') \tag{18}$$

$$\boldsymbol{U}''=enc(\boldsymbol{R}_2') \tag{19}$$

$$\boldsymbol{C}'=\boldsymbol{U}''\oplus\boldsymbol{S} \tag{20}$$

其中，$\boldsymbol{R}_2'=(R_{21}',R_{22}',\cdots,R_{2l}')$，$dec()$ 为纠错码解码过程，$\boldsymbol{U}''=(U_1'',U_2'',\cdots,U_n'')$ 由 $\boldsymbol{R}_2'$ 经纠错码编码得到，$\boldsymbol{C}'=(C_1',C_2',\cdots,C_n')$ 为纠错重构后的复现输出信息向量。

将复现输出信息向量 $\boldsymbol{C}'$ 与随机数 $\boldsymbol{R}_1$ 异或，然后对其进行加密得到 $\boldsymbol{K}'$，如式(21)所示：

$$\boldsymbol{K}'=\boldsymbol{C}'\oplus\boldsymbol{R}_1 \tag{21}$$

其中，$\boldsymbol{K}'=(K_1',K_2',\cdots,K_n')$。

Hash 模块使用 Hash 函数对加密后的标准输出信息向量 $\boldsymbol{K}$ 和纠错重构后的复现输出信息向量 $\boldsymbol{K}'$ 进行进一步加密，以生成自动纠错 CRO PUF 密钥生成方案的标准密钥 $key$ 和复现密钥 $key'$，如式(22)、式(23)所示：

$$key=Hash(\boldsymbol{K}) \tag{22}$$

$$key'=Hash(\boldsymbol{K}') \tag{23}$$

## 4 性能指标

理论上，设计布局完全一致的 CRO，其振荡频率也应完全一致；但实际上，由于集成电路在制造生产过程中存在着不可避免和不可控的制造工艺误差，CRO 内部元器件的某些参数在一定程度上产生了随机性抖动偏差，使得 CRO 的振荡频率发生了改变。CRO 的输出响应值取决于其振荡频率，由于振荡频率的误差具有随机性，因此 PUF 的输出信息序列也应具有随机性，但由于现实中存在不可控的因素，需要从 3 个方面去度量 PUF 的性能[8]：可靠性、唯一性和均匀性。

### 4.1 可靠性

可靠性描述的是 PUF 实例在同一个激励的作用下产生的输出信息序列受到环境(电源电压、温度等)干扰的大小。理想情况下，PUF 的可靠性为 100%，即 PUF 的输出信息序列不受环境干扰；但在实际情况下，PUF 的输出信息序列在环境干扰条件下会产生比特跳变现象。

采用平均片内距离与输出信息序列位数的百分比来度量 CRO PUF 的可靠性[8]。片内距离为相同激励作用于同一个 PUF 实例所生成的输出信息序列的汉明距离。可靠性的计算如式(24)所示：

$$u_o=100\%-\frac{1}{M_{\text{time}}}\sum_{x=1}^{M_{\text{time}}}\frac{HD(\boldsymbol{C}^0,\boldsymbol{C}_x)}{n}\times100\% \tag{24}$$

其中，$\boldsymbol{C}_x$ 表示同一个 PUF 电路在相同激励的第 $x$ 次作用下生成的复现输出信息向量；$HD()$ 为汉明距离：

$$HD(\boldsymbol{C}^0,\boldsymbol{C}_x)=\sum_{i=1}^{n}C_i^0\oplus C_i \tag{25}$$

PUF 电路的可靠性取决于 $u_o$ 的大小，$u_o$ 值越大，PUF 电路的可靠性越高；$u_o$ 值越小，PUF 电路的可靠性越低。

### 4.2 唯一性

唯一性是指不同 PUF 实例在相同环境和激励下生成复现输出信息序列的区别度。若唯一性达到要求，不同 PUF 实例生成的复现输出信息序列将不同。

采用平均片间距离与输出信息序列位数的百分比来衡量 CRO PUF 的唯一性[8]。片间距离为相同激励作用于不同 PUF 实例产生的输出信息序列的汉明距离。唯一性的计算如式(26)所示：

$$u_n=\sum_{a=1}^{N_{\text{puf}}-1}\sum_{b=a+1}^{N_{\text{puf}}}\frac{2HD(\boldsymbol{C}_a,\boldsymbol{C}_b)}{N_{\text{puf}}(N_{\text{puf}}-1)\cdot n}\times100\% \tag{26}$$

其中，$N_{\text{puf}}$ 表示一组 PUF 中 PUF 实例的个数；$\boldsymbol{C}_a$ 和 $\boldsymbol{C}_b$ 表示两个不同 PUF 实例在相同环境及激励下的复现输出信息序列。

PUF 电路的唯一性取决于 $u_n$ 的大小，当 $u_n$ 值越靠近理想值 50%时，PUF 电路的唯一性越好。

### 4.3 均匀性

均匀性为 PUF 输出响应序列中 0 和 1 所占的比例。理论上，均匀性标准值为 50%，它的计算如式(27)所示：

$$u_k=\frac{1}{n}\sum_{i=1}^{n}C_i\times100\% \tag{27}$$

PUF 电路的均匀性取决于 $u_k$ 的大小，当 $u_k$ 值越靠近理想值 50%时，PUF 电路的均匀性越好。

## 5 实验仿真与分析

仿真实验在 Linux 系统下进行，利用 Cadence virtuoso 中 specture 环境下的 TSMC0.18 um，1.8 V CMOS0 工艺库，对本文设计的自动纠错 CRO PUF 电路进行 Monte Carlo 模拟，创建 100 个 PUF 电路实例。

通过改变 Cadence virtuoso 中温度和电源电压的参数设置，来模拟环境因素对 PUF 可靠性的影响。对同一个 PUF 电路实例使用相同激励作用 100 次得到 100 组 32 位数据，对 100 个 PUF 电路使用相同激励作用一次得到 100 组 32 位数据，这两次实验数据分别用来计算 PUF 电路的唯一性和均匀性。

使用 MATLAB 对在环境因素影响下的 100 组数据进行模糊提取器处理，模糊提取器中的纠错码选择 BCH 纠错码，Hash 模块使用 MD5 对纠错后的输出信息向量进行加密。

### 5.1 自动纠错 CRO PUF 的性能分析

#### 5.1.1 可靠性度量

实验以 1.8 V 作为标准电源电压，通过 Monte Carlo 改变电源电压(1.72 V，1.74 V，1.76 V，1.78 V 和 1.82 V)来模拟环境因素的改变，对同一个自动纠错 CRO PUF 电路使用相同激励进行多次作用得到 100 组 32 位数据，根据式(24)得到自动纠错 CRO PUF 的可靠性，并将其与 CRO PUF 的可靠性进

行比较，结果如图 7 所示。

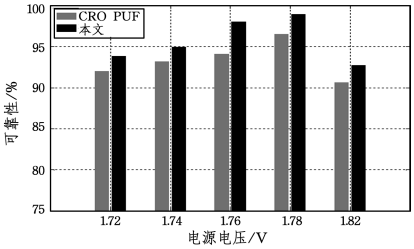


图 7　电源电压对可靠性的影响

Fig. 7　Effect of power supply voltage on reliability

实验以 27℃作为标准温度，通过 Monte Carlo 改变实验温度（10℃，20℃，30℃，40℃ 和 50℃）来模拟环境因素的改变，对同一个自动纠错 CRO PUF 电路使用相同激励进行多次作用得到 100 组 32 位数据，根据式（24）得到自动纠错 CRO PUF 的可靠性，并将其与 CRO PUF 的可靠性进行比较，结果如图 8 所示。

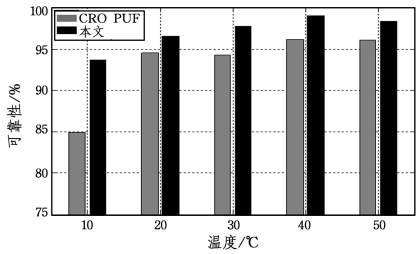


图 8　温度对可靠性的影响

Fig. 8　Temperature impact on reliability

从图 7 中可以看出，与 CRO PUF 可靠性相比，在电源电压干扰下自动纠错 CRO PUF 的可靠性有了很大的提高：CRO PUF 的最小可靠性为 90.63%，最大可靠性为 96.52%；而自动纠错 CRO PUF 的最小可靠性为 92.71%，最大可靠性为 98.96%。从图 8 中可以看出，与 CRO PUF 的可靠性比较，在温度干扰下自动纠错 CRO PUF 的可靠性有了较大的提高：CRO PUF 的最小可靠性为 84.90%，最大可靠性为 96.18%；而自动纠错 CRO PUF 的最小可靠性为 93.75%，最大可靠性为 99.10%。从而可以得出，自动纠错 CRO PUF 在受到环境因素影响下的可靠性较高，输出响应值发生比特跳变的数量减少。

5.1.2　唯一性度量

对 100 个 PUF 实例使用相同激励作用得到 32 位数据，其中激励分别为 10011，10001，11011，11001，11101，分别将其记为标号 1，2，3，4，5，根据式（26）计算自动纠错 CRO PUF 的唯一性，并与 CRO PUF 进行比较，对比结果如图 9 所示。由图 9 可知，自动纠错 CRO PUF 的唯一性在 49.87% 到 50.35% 之间浮动，而 CRO PUF 的唯一性在 49.73% 到 50.24% 之间浮动。从整体情况看，两者的唯一性与标准值 50% 比较，并没有一方处于明显的优势或劣势。但从两组数据的方差来看，自动纠错 CRO PUF 的唯一性数据方差值为 0.02774，CRO PUF 的唯一性数据方差值为 0.17421，可见相对于 CRO PUF，自动纠错 CRO PUF 的唯一性波动较小，与标准值 50% 的效果更加逼近。

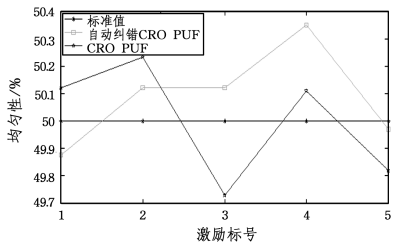


图 9　唯一性对比

Fig. 9　Comparison of uniqueness

5.1.3　均匀性度量

采用唯一性度量实验中的 100 个 PUF 实例生成的 32 位数据，根据式（27）计算得出自动纠错 CRO PUF 的均匀性，并与 CRO PUF 的均匀性进行比较，对比结果如图 10 所示。

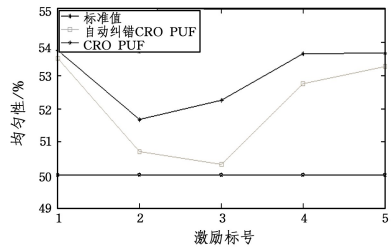


图 10　均匀性对比

Fig. 10　Comparison of uniformity

由图 10 可知，自动纠错 CRO PUF 的均匀性在 50.28% 到 53.43% 之间浮动，而 CRO PUF 的均匀性在 51.69% 到 53.82% 之间浮动，自动纠错 CRO PUF 的均匀性更接近标准值 50%，相对于 CRO PUF，自动纠错 CRO PUF 的均匀性有了一定程度的提高。

### 5.2　模糊提取器处理后的可靠性性能分析

由图 8、图 9 可知，相对于 CRO PUF，自动纠错 CRO PUF 的可靠性有了大幅度提升，但在有环境干扰（电源电压、温度）的情况下还是存在比特跳变误差，不能直接用作密钥。针对自动纠错 CRO PUF 的最低可靠性 92.71%（即自动纠错 CRO PUF 的最大比特跳变误差为 7.29%），采用模糊提取器对复现输出响应序列进行纠错，进一步提高 PUF 可靠性。模糊提取器中的纠错码选择纠错能力较强的 BCH 码[17]，BCH（31，16）纠错码满足最大误差为 7.21% 的纠错要求。

使用模糊提取器对同一 PUF 电路实例在不同环境条件下由相同激励作用生成的 100 组 32 位数据进行处理，并根据式（24）计算得到纠错后的数据的可靠性，然后将其与模糊提取器处理前的平均可靠性进行对比，如表 1 所列。

表 1　模糊提取器纠错前后的可靠性对比

Table 1　Reliability comparison of fuzzy extractor before and after error correction

| | 平均可靠性/% |
|---|---|
| 模糊提取器纠错前 | 96.504 |
| 模糊提取器纠错后 | 99.886 |

由表 1 可以看出，使用模糊提取器进行纠错后的 PUF 的可靠性为 99.886%，而未使用模糊提取器纠错的 PUF 的可靠性为 96.504%。因此，模糊提取器纠错提高了 PUF 电路

的可靠性，降低了环境因素对 PUF 电路的影响，减小了复现输出信息序列的比特跳变误差，使密钥可以直接用作加密。

经模糊提取器纠错后的 PUF 输出数据进入到 Hash 模块，采用 MD5 进行压缩与加密，生成 32 位最终密钥，列举其中 5 组数据，如表 2 所列。表 2 中，密钥由纠错后的 PUF 输出信息向量使用 MD5 加密得到，可以直接用于加密技术中。

表 2 PUF 电路的输出响应向量及密钥

Table 2 PUF circuit output response vector and key

| 激励 | 自动纠错 CRO PUF 输出信息向量 | 密钥 |
|---|---|---|
| 10011 | 10101111101000101000101010100110 | 37D98B099F663F9A19BC945C0964B430 |
| 10001 | 00101111101000101000100110100111 | 6336FF4FB25EDC152998C38A10306C81 |
| 11011 | 00011111001011101101000110100011 | 88079D76DB0D85A7496E151D84A2EA7D |
| 11001 | 10101111101100101000101010100110 | FEEEBC6C83DB9D85F927A100C53EE91D |
| 11101 | 00101111101000101000101010100110 | 1DE0C9535562FCC0C6687A215FBEC2BB |

**结束语** PUF 作为近几年的研究热点，在生成密钥时需从 3 个方面来度量 PUF 的性能：可靠性、唯一性和均匀性。本文设计的自动纠错 CRO PUF 密钥生成方案，通过借鉴重复码的纠错思想改进了 CRO PUF 结构，实现了 PUF 的自动纠错，显著提高了电路的可靠性和均匀性，其唯一性与标准值 50%之间也有较好的逼近效果。自动纠错 CRO PUF 的输出经模糊提取器处理后进一步减小了环境干扰造成的比特跳变误差，最终生成的密钥可直接用于 RFID 的认证协议中。

## 参 考 文 献


[1] PAPPU R, RECHT B, TAYLOR J, et al. Physical One-Way Functions[J]. Science, 2002, 29(5589): 2026-2030.

[2] 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. Washington, USA: ACM, 2002: 148-160.

[3] LEE JW, LIM D, GASSEND B, et al. A technique to build a secret key in integrated circuits for identification and authentication application[C] // Proceedings of the Symposium on VLSI Circuits. Washington, DC: IEEE Computer Society, 2004: 176-159.

[4] CAO Y, ZHANG L, CHANG C H, 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] KUMAR S S, GUAJARDO J, MAES R. Extended abstract: The butterfly PUF protecting IP on every FPGA[J]. IEEE International Workshop on Hardware-oriented Security & Trust, 2008, 6(9): 67-70.

[6] CHEN S, LI B, ZHOU C J. FPGA implementation of SRAM PUFs based cryptographically secure pseudo-random number generator[J]. Microprocessors and Microsystems, 2018, 6(59): 57-68.

[7] RAHMAN M T, FORTE D, FAHRNY J. ARO-PUF: An Aging-Resistant Ring Oscillator PUF Design[J]. Design, Automation & Test in Europe Conference & Exhibition, 2014, 4(21): 1-6.

[8] LI C T, ZHANG Q L, LIU Z B. FROPUF: Extract more entropy from FPGA-based oscillatory ring PUF[J]. Journal of Information Security, 2018, 3(1): 16-30.

[9] MAITI A, SCHAUMONT P. Improved Ring Oscillator PUF: An FPGA-friendly secure primitive[J]. Journal of Cryptology, 2011, 24(2): 375-397.

[10] SUH G E, DEVADAS S. Physical Unclonable Functions for Device Authentication and Secret Key Generation[C]// IEEE Design Automation Conference. San Diego, USA: IEEE, 2007: 9-14.

[11] XU T Z, YANG T C, CHENG J, et al. SRAM-PUF design method based on error correction code fuzzy extractor[J]. Computer Science, 2016, 43(S2): 373-376.

[12] DODIS Y, REYZIN L, SMITH A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[C]// Advances in Cryptology-EUROCRYPT 2004. Germany: Springer, Berlin, Heidelberg, 2004: 523-540.

[13] LIN S. Error Control Coding[M]. Beijing: China Machine Press, 2007.

[14] SAHOO S R, KUMAR K S, MAHAPATRA K. A novel current controlled configurable RO PUF improved security metrics[J]. Integration the Vlsi Journal, 2017, 6(58): 401-410.

[15] DODIS Y, OSTROVSKY R, REYZIN L, et al. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data[J]. SIAM Journal on Computing, 2008, 38(1): 97-139.

[16] ZHANG L L, SUN R Y, ZHOU Y, et al. Key extraction scheme available for SRAM PUF [J]. Journal of Peking University (Natural Science Edition), 2017, 53(6): 997-1002.

[17] LIU Y, LI R, FU Q, et al. Some binary BCH codes with length $n=2^m+1$ [J]. Finite Fields and Their Applications, 2019, 1(55): 109-133.


**ZHANG Xiang-yang**, born in 1995, M. S. candidate. Her main research interests include radio frequency identification and information security.

**SUN Zi-wen**, born in 1968, Ph.D, professor. Her research interests include wireless sensor network theory and technology, information security, pattern recognition.