DOI:10.19651/j.cnki.emt.2105822

一种基于 BCH 算法的 SRAM PUF 芯片的设计、测试与分析*

张家梁[1,2] 宋贺伦[1,2]
(1.中国科学技术大学 纳米技术与纳米仿生学院 合肥 230026; 2.中国科学院 苏州纳米技术与纳米仿生研究所 苏州 215123)

摘 要: 物理不可克隆功能是一种新型的信息安全硬件,在物联网、消费电子等领域得到了越来越广泛的应用。基于 SRAM 的 PUF 是工业上应用最广泛的一种类型。基于华宏 0.11 μm CMOS 工艺的 SRAM PUF,通过引入 BCH 算法解决了 SRAM 的不稳定性造成的误码率问题。通过设计单片机测试电路和 PUF 芯片测试板,对 PUF 芯片的片内汉明距离、片间汉明距离和稳定性等关键指标进行了详细的测试和分析。测试结果表明,PUF 的片间汉明距离达到 42.2%,片内汉明距离达到 20.0%,并且具有很好地电压稳定性与温度稳定性。在 BCH 算法纠错机制运行的情况下芯片片内汉明距离降为 0,很好地解决了 PUF 实现过程中的误码率问题。基于本项研究可知,通过 BCH 算法与 SRAM 单元相结合的方式可以很好地解决 PUF 常出现的不稳定性的问题。BCH 算法与 SRAM 单元相结合的 PUF 芯片可以很好地满足识别、电子标签等应用的需要。

关键词: STM32F4 单片机;SRAM;PUF;BCH 算法;串口通信;芯片测试
中图分类号: TN432 **文献标识码**: A **国家标准学科分类代码**: 510.1010

The design, test and analysis of a SRAM PUF chip based on BCH algorithm

Zhang Jialiang[1,2] Song Helun[1,2]
(1.School of Nano Technology and Nano Bionics, University of Science and Technology of China, Hefei 230026, China;
2.Suzhou Institute of Nano-Tech and Nano-Bionics, Chinede Academy of Science, Suzhou 215123, China)

Abstract: PUF(physically unclonable functions) is a new type of information security hardware, which has been widely used in the fields of Internet of things, consumer electronics and so on. SRAM based PUF is one of the most widely used types in industry. The SRAM PUF, based on Huahong 0.11 μm CMOS process, solves the error rate problem caused by SRAM instability by introducing a BCH algorithm. Through the design of MCU test circuit and PUF chip test board, the key indexes such as in-chip hamming distance, inter-chip hamming distance and stability of PUF chip are tested and analyzed in detail. According to the test results, the hamming distance between the PUF films is 42.2% and the hamming distance within the films is 20.0%. When the error correction mechanism of the BCH algorithm is running, the hamming distance in the chip is reduced to 0, which solves the error rate problem in the process of PUF implementation. This study shows that the problem of instability can be solved by combining BCH algorithm with SRAM unit. The PUF chip combined with BCH algorithm and SRAM unit can meet the needs of recognition, electronic label and other applications.

Keywords: MCU STM32F4; SRAM; PUF; BCH algorithm; serial communication; chip testing

0 引 言

随着物联网技术以及相关设备的发展,微电子元件几乎在每个领域都被广泛使用。由于芯片制造过程中固有的变异性,每颗芯片都是唯一的。微电子元件的这种物理唯一性可以用来为每个芯片分配签名。这些签名可以用来识别芯片,并解决微电子领域出现的许多问题。

物理不可克隆函数(physical unclonable functions,

收稿日期:2021-02-20
*基金项目:中国科学院科技服务网络计划(KFJ-STS-QYZX-061)、纳米真空互联试验站(2018-000052-73-01-000356)、"十三五"国家密码发展基金(MMJJ20180112)项目资助

PUF)使这种唯一性得以实现和应用。物理不可克隆函数是利用制造过程中的可变性来生成设备特定输出的实体,其产生的输出通常是二进制数。文献[1]给出了物理不可克隆函数的其他不同定义。PUF 由几个参数确定的组件组成。PUF 将这些参数组合、比较或直接读出,生成二进制输出。由于不能从外部控制组件变化,因此不能复制 PUF。PUF 是输出信号取决于输入的函数。输入(挑战)变化会改变 PUF 组件的内部组合,从而改变输出(响应)。输入还可以决定由哪些组件生成输出。也可以使用 HASH 函数来组合输入和 PUF 输出以生成特定的序列。理论上 PUF 的定义为:PUF 是一个利用难以克隆的物理结构产生输出值的物理实体。使用 PUF 方法加密不需要复杂的密码算法,减小了通信过程中的计算量。文献[2]提出了一种基于 PUF 的物理层安全认证方法。对 PUF 安全性的研究可以参考文献[3]提出的基于 PUF 安全协议研究。

2002 年,文献[4]提出了一种通过比较相同制造流程的两个晶体管的漏电流产生芯片唯一数据的方法。该方法使用自动归零比较器测量电阻器上的不同晶体管之间的电位差实现 PUF,是物理不可克隆函数的首次实现。文献[5]提出了一种光学 PUF,根据透明光学介质的衍射图样产生唯一输出。文献[6]提出了环形振荡器 PUF,利用测量制造过程中引起的环形振荡器频率的差异实现 PUF,并且该方法可以在 FPGA 上实现。文献[7]在 2021 年发表了一种可调可重构的环形振荡器物理不可克隆函数。文献[8]利用延时调节模块控制不同路径的延时大小在 2020 年设计了一种基于延时控制的 Glitch PUF。2020 年,文献[9]提出了一种基于 RSRAM 延时单元的 PUF 设计,该方法利用延时单元将 RSRAM 的阻值输出到方向器中,形成脉冲的延迟,最后通过判决器判断两路脉冲达到顺序并编码为“0”和“1”。2020 年,文献[10]针对基于不可逆变换的虹膜模板保护在进行虹膜识别时面临特征模板泄露的问题,提出一种结合局部置乱和双随机相位编码双虹膜身份模板保护方法。以上 PUF 的实现方法均存在不稳定性较大以及资源占用较多等问题。

SRAM PUF 使用 SRAM 模块生成芯片的特定数据。电路上电后,存储单元稳定在一个晶体管失配状态,每个 SRAM 单元输出一位数据。SRAM PUF 由文献[11-12]提出。SRAM PUF 方法也可以通过 FPGA 或微控制器[13]来实现。

PUF 的不稳定问题是制约 PUF 发展和应用的主要问题。并且 PUF 对于空间和功耗资源的占用也是制约其在数字系统中应用的主要原因。本文选择占用资源较少的 SRAM PUF 芯片进行研究,并通过 BCH 算法进一步提升 PUF 芯片数据的稳定性。本项研究自主设计了通过 BCH 算法进行纠错的 SRAM PUF。设计了基于 STM32F4 单片机的测试系统,采集并处理分析 SRAM PUF 的相关数据。针对 SRAM PUF 芯片的唯一性、鲁棒性、均匀性等关键性能进行评估,分别计算 SRAM PUF 芯片的片内汉明距离、片间汉明距离、均匀性、误码率。同时完成不同电压不同温度下的 SRAM PUF 芯片的数据采集工作。评估 SRAM PUF 芯片在不同电压不同温度下的性能。最后提出了本项研究中 SRAM PUF 芯片的应用领域以及应用时的注意事项。

1　SRAM PUF 理论基础

SRAM 电路结构简单,通常仅由几个晶体管组成,晶体管尺寸小失配较大。SRAM 电路的这些特点非常适用于 PUF 方面的应用。

一个 SRAM 单元通常由 6 个晶体管组成,其电路原理如图 1 所示。

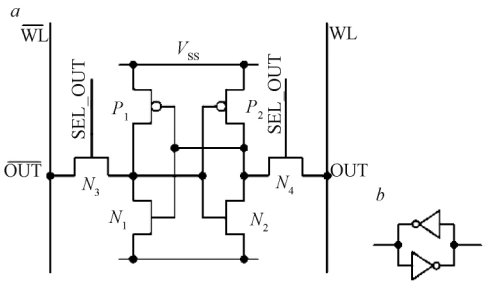
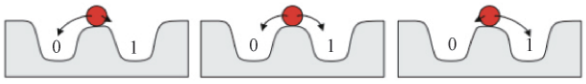


图 1　SRAM 单元电路模型

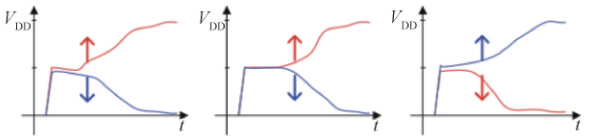
其物理模型如图 2 所示。图 2(b)是一个完全平衡系统,小球向左移动的概率与小球向右移动的概率相同。图 2(a)、(c)展示的是不平衡的系统,图 2(a)中系统偏向于状态“0”,图 2(c)中系统更偏向于状态“1”。



(a) 平衡系统趋向于“0”　(b) 平衡系统趋向于“0”“1”概率相同　(c) 平衡系统趋向于“1”

图 2　SRAM 单元物理模型

SRAM 单元的电压曲线如图 3 所示。SRAM 单元的偏置主要由 PMOS 晶体管的失配来产生。偏置状态决定了电路上电后 SRAM 单元的状态。



(a) 平衡系统趋向于“0”　(b) 平衡系统趋向于“0”“1”概率相同　(c) 平衡系统趋向于“1”

图 3　SRAM PUF 电压曲线

对于 SRAM 电路的进一步研究可以参考文献[14]发表的一种改进的 SRAM 随机故障注入技术。

2　SRAM PUF 芯片介绍

文献[15]提出一种基于 SRAM PUF 稳定性处理的 RFID 标签密钥生成方案。利用 SRAM 部分不稳定位相邻的特点提出基于条件概率的预选位方法。采用该方法去除容易连续出错的不稳定位。但是位置信息的存储在一定程度上增加了 SRAM PUF 的应用成本。而且由于去除了不稳定位，SRAM PUF 芯片可用的数据资源减少且不可预估。本方案通过将纠错算法集成在芯片内部降低了芯片的应用成本。而且通过纠错算法可以保证芯片能够持续稳定的输出有效数据。

2.1　SRAM PUF 架构

本项研究选择华宏集团 110 nm 加工平台。该研究的 SRAM PUF 芯片模块组成，物理版图以及芯片实物如图 4～6 所示。

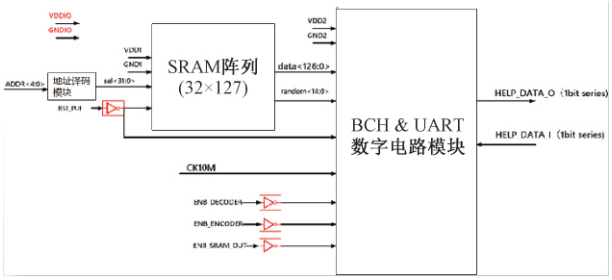


图 4　SRAM PUF 芯片各模块组成

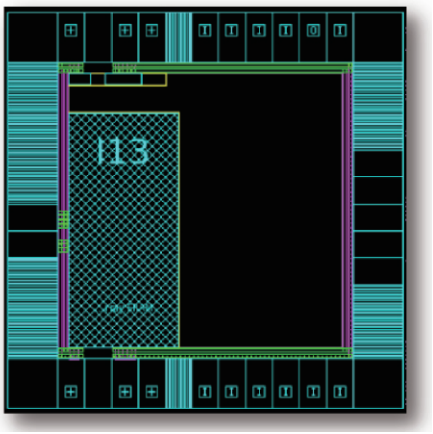


图 5　SRAM PUF 芯片物理版图

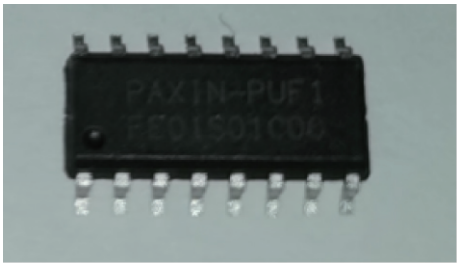


图 6　SRAM PUF 芯片实物

本款 SRAM 芯片主要由 4 部分模块组成，地址解码模块、SRAM 模块、BCH 算法数字模块和串口信号发送接收模块。地址解码模块将 5 位地址输入解码为 32 位的数据选择信号。SRAM 模块是 32×127 的数据阵列，根据 32 位的输入输出其对应的 127 位输出。由于相同地址的 127 位输出在两次向外输出的过程中存在误码率的问题，所以需要通过 BCH 算法纠错模块对 127 进行编码生成辅助数据并通过发送模块以串口通信的协议向外发送辅助数据，这进行的是 BCH 算法模块的编码功能。要获得最终的 PUF 数据时，需要通过 BCH 算法纠错模块将 127 位的 SRAM 数据与接收到的辅助数据进行译码，并将译码的结果通过串口通信协议向外发送。编码与译码功能的选择将由指定的引脚控制。对芯片进行控制的时序要求将在以下各节进行介绍。

半导体器件和集成电路的制造工艺中，引线与封装具有重要的地位。一个半导体器件，如果没有良好的、牢固的封装管壳来保护管芯，则管芯的性能就要受外部环境所影响，如高温、低温、急剧的温度变化、潮气、低气压、盐环境以及震动、冲击、离心作用等都会强烈地影响管芯的性能，甚至可能使器件失效。同时，半导体器件还须借助于管壳来散热，对于大功率器件来说，尤其是这样。如图 6 所示，根据应用需求以及芯片实际设计情况，本项研究制造的 SRAM PUF 芯片采用 SOP16 塑料封装。

2.2　SRAM PUF 各引脚及功能介绍

本项研究制造的 SRAM PUF 芯片设计了 16 个引脚，如图 7 所示。引脚名称分别为 VDD，VSS，VDDH，VSSH，CLK，RST，ADD[0]，ADD[1]，ADD[2]，ADD[3]，ADD[4]，SRAMOUT，ENCODE，DECODE，HELPDATA_O，HELPDATA_I。各引脚功能如下所述。

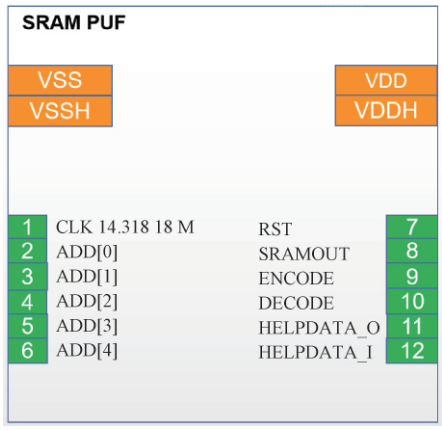


图 7　SRAM PUF 芯片引脚示意图

VDD-VSS：VDD 接 1.5 V，VSS 接地。为芯片内部的标准逻辑单元供电。

VDDH-VSSH：VDDH 接 3.3 V，VSSH 接地。为芯片 I/O Pad 供电。

CLK：接标准电平为 3.3 V，时钟频率为 14.318 18 M

的时钟。

RST:复位功能,3.3 V 高电平复位。

ADD:芯片内部 SRAM 阵列的地址,作为 SRAM 数据的选择信号。

SRAMOUT:此引脚作为方便芯片测试与分析的附加引脚。在大于一个时钟周期的 3.3 V 脉冲后,芯片即通过 HELPDATA_O 以串口协议的方式发送地址相对应的 SRAM 数据。

ENCODE:此引脚为芯片的编码使能引脚。在大于一个时钟周期的 3.3 V 脉冲后,芯片即通过 HELPDATA_O 以串口协议的方式发送地址相对应的 SRAM 数据的编码结果,作为后续纠错译码的辅助数据。

DECODE:此引脚为芯片的译码使能引脚。译码功能的正常实现需要首先通过 HELPDATA_I 引脚向芯片以串口协议发送辅助数据。之后在大于一个时钟周期的 3.3 V 脉冲后,芯片利用辅助数据对 SRAM 数据进行纠错译码并通过 HELPDATA_O 引脚以串口协议的方式发送与地址相对应的 SRAM 数据的纠错译码结果。

HELPDATA_I:数据输入引脚,芯片通过该引脚以串口协议接收数据,芯片保存最近一次接收到的 127 位数据。

HELPDATA_O:数据输出引脚,芯片通过该引脚以串口协议向外输出数据。

2.3　SRAM PUF 时序介绍

这一款 SRAM PUF 芯片有 3 个主要功能:原始数据输出,编码,译码。现就这 3 个功能对芯片的时序做一个简要说明。

原始数据输出功能(如图 8 所示):CLK,SRAM_OUT,HELPDATA_O 时序如下,其他引脚保持不变。SRAM_OUT 在大于一个时钟周期的 3.3 V 脉冲后,芯片即通过 HELPDATA_O 以串口协议的方式发送地址相对应的 SRAM 数据。

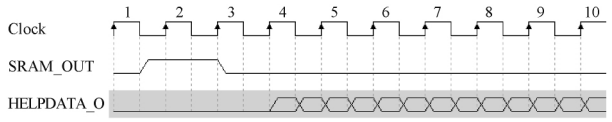


图 8　芯片原始数据输出功能时序图

编码功能(如图 9 所示):CLK,ENCODE,HELPDATA_O 时序如下,其他引脚保持不变。ENCODE 在大于一个时钟周期的 3.3 V 脉冲后,芯片即通过 HELPDATA_O 以串口协议的方式发送地址相对应的 SRAM 编码数据。

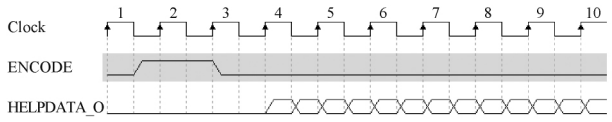


图 9　芯片编码功能时序图

译码功能(如图 10 所示):CLK,HELPDATA_I,DECODE,HELPDATA_O 时序如下,其他引脚保持不变。首先通过 HELPDATA_I 向芯片发送 SRAM 相对应的辅助数据,之后 DECODE 在大于一个时钟周期的 3.3 V 脉冲后,芯片即通过 HELPDATA_O 以串口协议的方式发送地址相对应的 SRAM 译码数据。

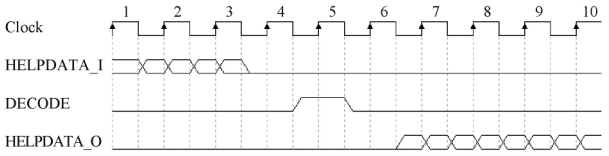


图 10　芯片译码功能时序图

3　SRAM PUF 测试系统设计

3.1　测试系统硬件设计

本测试系统选用 AMS1117 芯片作为电源转换芯片,并外接 10 μF 和 104 电容进行滤波。选择 FSX 14.318 18 M 无源晶振为芯片提供时钟。选择 STM32F4 MUC 作为 SRAM PUF 的驱动芯片。

SRAM PUF 实验测试系统的主要功能设备为 PC、STM32 和 SRAM PUF 芯片,系统正常运转的流程如图 11 所示。

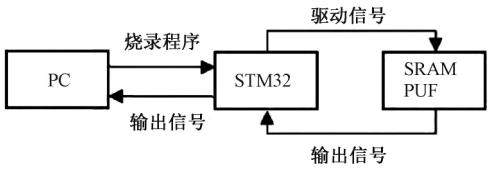


图 11　SRAM PUF 实验测试系统的主要功能设备连接示意图

实验测试时,为了使得 SRAM PUF 芯片正常工作,最重要的是建立 STM32 与 SRAM PUF 芯片的正确通信,并确保 SRAM PUF 芯片的正确触发条件和相应工作环境,比如加载的输入信号是否满足要求,SRAM PUF 芯片的电压是否为工作电压,同时还要确保硬件各个单元组件之间连接无误,首先给 FPGA 配置相关信号参数,然后加载相应信号驱动 SRAM PUF 芯片工作,使其产生输出信号,然后数据传送到 FPGA,通过 USB2.0 完成与电脑的正确通信,在串口助手上观测并保存所需的输出响应数据。本测试系统具各模块化设计的优点,适用于小批量片的快速测试,功耗比较低,可靠性强,实时操作性好,通用性比较强。

3.2　测试系统软件单元及测试流程设计

程序模块包含初始化程序、信号加载程序、串口通信模块、时钟模块等。程序使用 C 语言编写,采用 Keil5 软件对程序进行编译仿真,并完成烧录工作。具体工作模式是首先为 SRAM PUF 芯片提供 14.318 18 M 的时钟,Reset 功能结束后为芯片提供地址选择信号 ADD。SRAMOUT 高电平脉冲后芯片输出地址对应 SRAM 数据。ENCODE 高

电平脉冲后芯片输出编码数据。通过 HELPDATA_I 向芯片发送译码辅助数据，DECODE 高电平脉冲后芯片发送译码数据。

发送和接收数据时采用串口通信，计算机没有串口，本实验采用 USB 转串口进行数据传输，这种转换模式可为计算机提供快速通信的通道，实现计算机 USB 接口到通用串口之间的转换，USB 支持主机与外设之间进行数据传输。

4　实验测试与分析

4.1　实验设置

本项研究对 SRAM PUF 芯片的测试主要分 3 组，分别为探究电迁移对芯片数据稳定性的影响，电压波动对芯片数据稳定性的影响以及温度涨落对芯片数据稳定性的影响。电迁移对芯片的影响可以通过对比芯片 50 万次上电掉电前后数据的稳定性来分析。常温条件下设置 1.3，1.5 和 1.7 V 电压环境，研究电压对芯片数据稳定性的影响。设置 1.5 V(−40 ℃ −35 ℃ −30 ℃ −25 ℃ −20 ℃ −15 ℃ −10 ℃ −5 ℃ 0℃ 5 ℃ 10 ℃ 15 ℃ 20 ℃ 30 ℃ 40 ℃ 50 ℃ 60 ℃ 65 ℃ 70 ℃ 75 ℃ 80 ℃ 85 ℃ 90 ℃ 95 ℃ 100 ℃ 105 ℃ 115 ℃ 120 ℃ 125 ℃)测试环境进行测试，并对不同温度下芯片数据的稳定性进行分析。

4.2　数据测试及性能分析

PUF 的性能分析主要参考以下几个关键数据。

汉明距离：汉明距离代表相同长度的两个字符串的不同元素的数目。汉明距离也可以以百分比的形式进行表示，具体计算方法为两个字符串的不同元素的数目除以字符串长度乘以 100%。

均值：PUF 的输出应该是随机的。从而，PUF 的输出值中，“1”和“0”出现的概率相同。其计算公式如式(1)所示。理想情况下 SRAM PUF 的均值应满足二项分布。

$$\bar{x}=\frac{1}{n}\sum_{i=1}^{n}x_i \tag{1}$$

式中：n 代表 SRAM PUF 所输出数据的总位数；x 代表 SRAM 单元数值；i 代表 SRAM 单元的序号；$\bar{x}$ 代表 SRAM 单元的平均值。

误码率：PUF 的输出应该在可识别的范围内保持不变。如果相同的数据位在不同的两次输出时其数值不同，则认为该位数据发生了错误，并称该数据位为不稳定位。PUF 芯片的误码率的表示方法如下所述，随机选取一次 SRAM PUF 的输出作为标准数据，重新输出时输出数据与标准数据之间的汉明距离的统计值表示为 SRAM PUF 芯片的误码率。芯片的误码率通常受器件噪声、温度变化和电源稳定性的影响。

SRAM PUF 芯片均值的具体测试方法为选取 10 颗 SRAM PUF 芯片，对每颗芯片进行 100 次上下电，每次上电后将 SRAM PUF 芯片 32 个地址所对应的数据一次输出并保存。通过多次上下电，模拟芯片的实际应用环境。这样每个芯片都对应一个 32×127×100 的数据阵列。对每颗芯片所对应的数据阵列求平均值及为 SRAM PUF 芯片的均值。理想状态下(即每一位数据为“0”与为“1”的概率相同)，芯片均值的概率可以进行如式(2)表示。

$$P\left(\frac{n}{N}\right)=\frac{C_N^n}{2^N} \tag{2}$$

式中：N 为总数据位数；n 为数据中数据“1”的个数。

图 12 将理想状态下数据的概率分布以及 10 颗芯片的均值画在一张图上。从图中可以看出芯片的均值皆分布在理想曲线的均值附近。根据统计学知识，芯片的均值满足随机性要求。

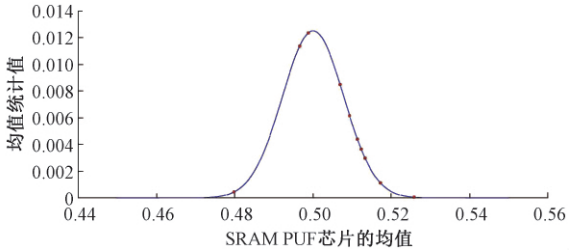


图 12　SRAM PUF 芯片均值的统计结果

SRAM PUF 芯片数据的稳定性可通过比较相同数据位不同次输出的数据之间的汉明距离来表示。本项研究的具体测试方法为，将 10 颗芯片内部的 32 条数据进行 500 次输出并保存其输出的数据。之后通过 Reset 信号为芯片提供 50 万次的高电平脉冲但并不输出数据，对芯片进行 50 万次上电掉电的目的是为了检验芯片在实际应用过程中是否存在由于老化造成的芯片数据的偏移。50 万次上电掉电后再对芯片进行 500 次数据输出，并保存 SRAM PUF 芯片输出的数据。这样每一条数据位都会有 1 000 次输出，通过统计这 1 000 次输出数据之间的汉明距离并做汉明距离的统计结果图即可得到不稳定位位数的统计结果。其具体的计算方法如式(3)所示。

$$HD(C_{i,j}^1,C_{x,y}^n)\quad i=x=1,2,3,\cdots,10;$$
$$j=y=1,2,3,\cdots,32;\quad n=1,2,\cdots,1\,000 \tag{3}$$

式中：$HD(C_{i,j}^1,C_{x,y}^n)$ 代表芯片片间汉明距离；(i,j)、(x,y) 用来确定数据的位置；i、x 表示芯片的序号取值范围为 1～10；j、y 表示芯片中的地址序号取值范围为 1～32；n 代表该数据位的第 n 次输出芯片误码率的统计结果如图 13 所示。从图中可以看出 SRAM PUF 芯片不稳定位的统计结果的峰值在两位附近最大不稳定位为 8 位。考虑到本项研究所制造的 SRAM PUF 芯片一次输出的数据位数为127 位，在芯片发生最多错误及 8 位错误的情况下仍能够通过汉明距离识别出不同的数据，所以从稳定性的角度看芯片可以满足实际应用过程中的稳定性要求。

SRAM PUF 芯片通过片间汉明距离来衡量 PUF 芯片的安全性，防止在实际应用的过程中出现无法区分两块 SRAM PUF 芯片的情况。通过统计不同的数据位之间的

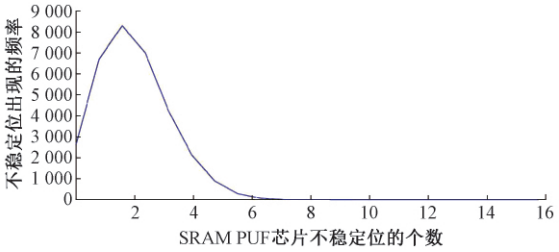


图 13　SRAM PUF 芯片误码率的统计结果

汉明距离,并与芯片的不稳定位进行比较,则可以判断出芯片的安全性能。芯片片间汉明距离的计算方法如式(4)所示。

$$HD(C_{i,j},C_{x,y})$$
$$i,x=[1,\cdots,10];j,y=[1,\cdots,32] \tag{4}$$

式中:$HD(C_{i,j},C_{x,y})$ 代表芯片片间汉明距离值;i,x 代表芯片的序号;j,y 代表芯片内部地址的序号。

本项测试选取 10 颗芯片共有 320 条输出数据,有 320×320 个计算出来的汉明距离,对这些汉明距离做其统计分布图,如图 14 所示。图中横轴代表汉明距离与一次输出的总数据位数的百分比,纵轴代表一定汉明距离所出现的频率。从图中可以看出 SRAM PUF 的片间汉明距离的统计结果绝大多数分布在 0.5 左右。汉明距离的最小值为 0.25,0.25 乘以一次输出的位数 127 及得到其汉明距离为 31,其结果远大于每一条数据的最大不稳定位。所以从安全性上看,足以对不同的数据输出进行区分。

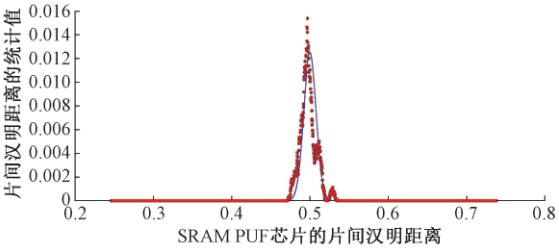


图 14　SRAM PUF 芯片片间汉明距离的统计结果

李森森等[16]提出了一款基于物理不可克隆函数的蓝牙密钥生成器。该方法采用可重构环形振荡器和映射模块实现 PUF。图 15 为该方法实现的 PUF 汉明距离的统计分布图。从图中可以看出通过环形振荡器实现的 PUF 在收敛性上明显差于 SRAM PUF。

SRAM PUF 芯片在 1.3 V 条件下的均值统计分布如图 16 所示。SRAM PUF 芯片在 1.5 V 条件下的均值统计分布如图 17 所示。SRAM PUF 芯片在 1.7 V 条件下的均值统计分布如图 18 所示。从图中可以看出这 5 颗芯片的均值皆分布在 0.56 附近,其均值并没有随电压发生较大的变化。说明本项研究所采用的工艺条件下,在 1.3～1.7 V 之间其均值都是稳定的。

SRAM PUF 芯片在 1.3 V 条件下不稳定位的统计分布如图 19 所示。SRAM PUF 芯片在 1.5 V 条件下不稳定

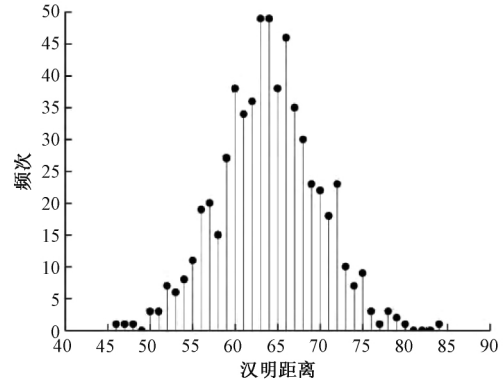


图 15　一种利用可重构环形振荡电路实现的 PUF 汉明距离分布

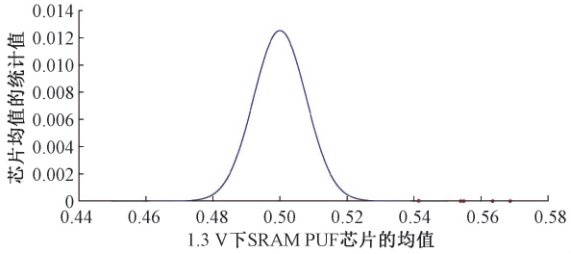


图 16　1.3 V 下 SRAM PUF 芯片的均值

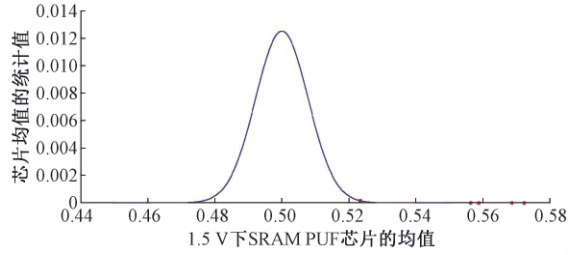


图 17　1.5 V 下 SRAM PUF 芯片的均值

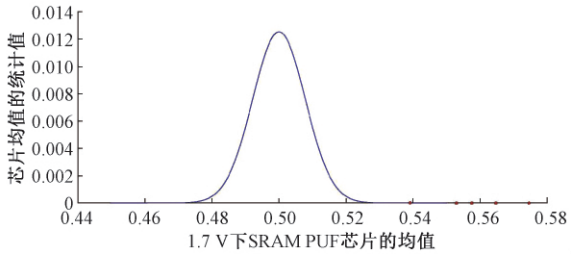


图 18　1.7 V 下 SRAM PUF 芯片的均值

位的统计分布如图 20 所示。SRAM PUF 芯片在 1.7 V 条件下不稳定位的统计分布如图 21 所示。从图中可以看出这 5 颗芯片的不稳定位的峰值皆为 2,其不稳定位的统计结果随电压升高不稳定位较多的统计值较大反之则较小。说明在芯片使用过程中应尽量避免电压较高的情况出现。

本项测试选取的温度范围为－40 ℃～125 ℃,图 22 为不同温度下均值的散点图,随着温度的变化 SRAM PUF

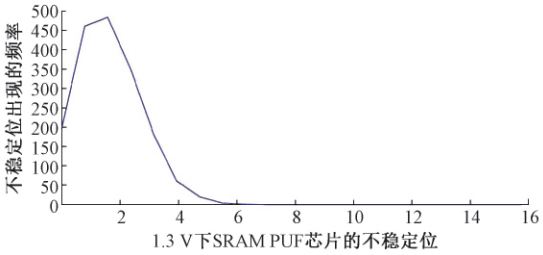


图 19　1.3 V 下 SRAM PUF 芯片的误码率

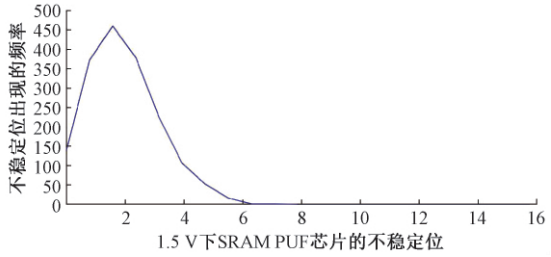


图 20　1.5 V 下 SRAM PUF 芯片的误码率

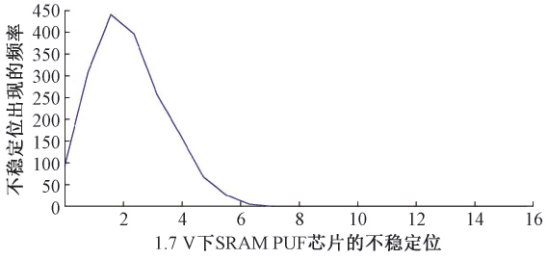


图 21　1.7 V 下 SRAM PUF 芯片的误码率

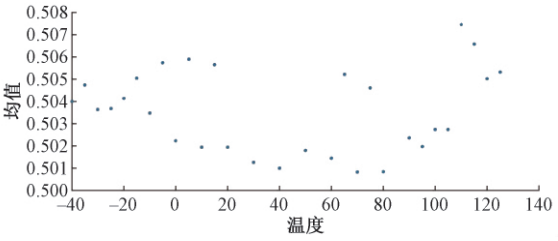


图 22　不同温度条件下 SRAM PUF 的均值分布

的均值相对均匀的分布在 0.5～0.508 之间。说明在 −40 ℃～125 ℃之间温度对 SRAM PUF 芯片的均值影响较小。

图 23 所示为 SRAM PUF 芯片不稳定位统计曲线随温度的变化，从图中可以看出 100 ℃～125 ℃（图中“——”表示）之间芯片不稳定位为 8 位左右且不稳定位的统计曲线变宽。从统计结果可以看出随着温度的升高芯片的不稳定位开始增多，对于工作在饱和区的长沟道 MOS 器件的沟道噪声可以用一个连接在漏源两端的电流源来模拟，$I_n^2=4kT\gamma g_m$，随着温度升高 CMOS 电路的器件噪声增大，降低了制造过程中工艺偏差对器件的影响，导致 SRAM PUF 芯片不稳定位增加。

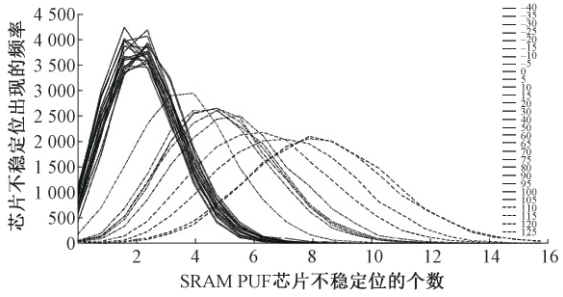


图 23　不同温度条件下 SRAM PUF 的误码率统计分布

5　结　　论

PUF 是一种利用难以克隆的物理结构产生输出值的物理实体。可用于标识、身份验证和密钥生成。随着物联网技术以及相关设备的发展，微电子元件几乎在每个领域都被广泛使用，对 PUF 的需求也快速上升。由于 PUF 的随机性无法人为加以控制，相较于传统的加密方法安全性得到大幅提升。但是 PUF 的不稳定性以及应用中对于外部资源的占用阻碍了 PUF 的大规模应用。

常温常压条件下芯片的均值皆分布在理想曲线的均值附近。根据统计学知识，芯片的均值满足随机性要求。最大不稳定位为 8 位，SRAM PUF 芯片在发生 8 位错误的情况下仍能够通过汉明距离识别出不同的数据，所以从稳定性的角度看芯片可以满足实际应用过程中的稳定性要求。芯片汉明距离的最小值为 0.25 及 31 位，其结果远大于每一条数据的最大不稳定位。所以从安全性上看，足以对不同的数据输出进行区分。5 颗芯片的不稳定位的峰值皆为 2，随电压升高不稳定位较多反之则较少。芯片在使用过程中应尽量避免电压较高的情况出现。−40 ℃～125 ℃之间温度对 SRAM PUF 芯片的均值影响较小。随着温度的升高 CMOS 电路的器件噪声增大，SRAM 的不稳定位开始增多。

在芯片纠错功能运行的情况下芯片均能够输出稳定的数据。常温条件下，在不运行芯片纠错功能的情况下任能够满足芯片识别的需求。在本项研究的工艺条件下，电压对芯片数据稳定性影响较小。随着芯片运行的环境温度升高，当温度超过 100 ℃时芯片的不稳定位达到 8～10 位存在与片间汉明距离发生冲突的可能性，所以必须运行纠错功能芯片才能正常使用。由于本款芯片纠错功能设计的纠错能力为 27 位，所以在纠错功能运行的情况下皆可以解决以上问题。但是由于本芯片选用位数固定的 SRAM 阵列产生 PUF 数据，SRAM PUF 芯片数据的输出位数固定，对芯片的应用场景有一定的限制。之后可以针对芯片的这个特点通过应用软件的设计扩展 SRAM PUF 的应用。

参考文献

[1]　BHARGAVA M, CAKIR C, MAI K. Attack resistant sense amplifiifier based PUFS (SA-PUF) with

deterministic and controllable reliability of puf responses [J]. IEEE International Symposium on Hardware-oriented Security and Trust(HOST),2010,10(11):106-111.

[2] 胡蝶,马东堂,龚旻,等.一种基于 PUF 的物理层安全认证方法[J]. 技术研究,2020,1(1):61-66.

[3] 罗敏,宋佳雯,戴欢. 基于 PUF 的安全协议研究[J]. 江西科学,2019,37(5):762-770.

[4] LOFSTROM K, DAASCH W, TAYLOR D. IC identifification circuit using device mismatch[J].IEEE International Solid-State Circuits Conference, 2000, 10(12):372-373.

[5] PAPPU R, RECHT R, TAYLOR J, et al. Physical one-way functions [J]. Science, 2002, 297 (5589): 2026-2030.

[6] GASSEND B. Physical random functions[J]. Master's Thesis, Massachusetts Institute of Technology, 2003, 13(12):21-39.

[7] 麻超方,叶靖,李晓维,等. 可调可重构的环形振荡器物理不可克隆函数[J]. 计算机辅助设计与图形学学报,2021,33:1-6.

[8] 董永兴,徐金甫,李军伟. 基于延时控制的 Glitch PUF 电路设计[J].计算机应用与软件,2020,37(11):311-333.

[9] 杨轩,叶文强,崔小乐. 基于 RSRAM 延时单元的 PUF 设计[J]. 电子学报,2020,8:1565-1571.

[10] 刘笑楠,张文云,高艳娜. 局部置乱结合双随机相位编码的双虹膜身份模板保护方法[J].仪器仪表学报,2020,41(6):233-239.

[11] GUAJARDO J, KUMAR S, SCHRIJEN G J, et al. Fpga intrinsic pufs and their use for ip protection[J]. Paillier P, Verbauwhede I (eds) Cryptographic Hardware and Embedded Systems-CHES 2007, 2007, 42(27):63-80.

[12] HOLCOMB D, BURLESON W, FU K. Power-up SRAM state as an identifying fifingerprint and source of true random numbers[J]. IEEE Trans Comput, 2009,58(9):1198-1210.

[13] BOHM C, HOFER M, PRIBYL W.A microcontroller sram-puf[J].International Conference on Network and System Security(NSS), 2011,10(9):269-273.

[14] 蔡志匡,王荧,周正,等. 一种改进的 SRAM 随机故障注入技术[J]. 南京邮电大学学报,2020,40(4):31-36.

[15] 潘畲稣,张继军,张钊锋. 基于 SRAM PUF 稳定性处理的 RFID 标签密钥生成方案[J]. 计算机工程,2020,46(9):149-162.

[16] 李森森,黄一才,郁滨,等. 基于物理不可克隆函数的蓝牙密钥生成器[J]. 电子测量与仪器学报,2018,32(2):137-145.

作者简介

张家梁,理学硕士,主要研究方向为微电子学与固体电子学。

E-mail:jlzhang2019@sinano.ac.cn

宋贺伦(通信作者),博士,研究员,主要研究方向为半导体器件集成技术及应用。

E-mail:hlsong2008@sinano.ac.cn