基于纠错码模糊提取器的 SRAM-PUF 设计方法

徐太忠[1] 杨天池[2] 程 娟[2] 邵奇峰[2]
(国家计算机网络应急技术处理协调中心 北京 100029)[1] (信息工程大学 郑州 450000)[2]

摘 要 物理不可克隆函数(Physical Unclonable Function,PUF)是新型的硬件安全技术,利用芯片的"物理指纹"特征实现密钥生成和身份认证等不同功能。提出了一种基于纠错码技术的模糊提取器,用于提高 SRAM 类 PUF 的鲁棒性。模糊提取器工作分为生成阶段和重构阶段,生成阶段利用 BCH 编码产生与 PUF 响应相关的辅助数据,重构过程利用辅助数据和 BCH 码的纠错功能重建 PUF 的稳定响应输出。模糊提取器在 ATSAMV70J19 处理器上进行实验,在不同的工作温度条件下,其一致性指标可达到 99.9%,验证了该方法的有效性。

关键词 物理不可克隆函数,模糊提取器,纠错码,密码生成,身份认证
中图法分类号 TP331 **文献标识码** A

Design Method of SRAM-PUF Based on Error Correcting Code Fuzzy Extractor

XU Tai-zhong[1] YANG Tian-chi[2] CHENG Juan[2] SHAO Qi-feng[2]
(National Computer Network Emergency Response Technical Team/Coordination Center,Beijing 100029,China)[1]
(The PLA Information Engineering University,Zhengzhou 450000,China)[2]

Abstract Physical unclonable function is a new kind of hardware security technology. The physical fingerprint characteristics of the chip are used in many fields such as key generation and identity authentication. The fuzzy extractor based on error correcting code was proposed in this paper to improve the robustness of PUF of SRAM. The working process of fuzzy extractor can be divided into two stages,generation stage and reconfiguration stage. The supplementary data of PUF is created by using BCH encoder method in generation stage. And the stable response output of PUF is created by using supplementary data and the error correcting ability of BCH encoder in reconfiguration stage. The fuzzy extractor experiment is running on ATSAMV70J19 CPU platform and the consistency reaches 99.9% under different operating temperatures. The result of experiment verifies the excellent performance of this method.

Keywords Physical unclonable function,Fuzzy extractor,Error correcting code,Key generation,Identity authentication

1 引言

随着信息技术的发展,嵌入式设备越来越多地应用在人们的日常生活中,并带来了极大的便利,同时嵌入式系统的安全也越发引起人们的重视。将信息技术与密码技术紧密结合,如集成 AES、DES、SM3 等密码运算模块,增加内存访问保护单元[1]等防护手段,可提高系统的安全强度。

但是总体来说嵌入式系统的安全,仍可视作"唯密钥安全",即只有密钥安全了,才可以保证系统的安全。密钥大多以密文或明文分割方式存储于非易失性存储器之中,在应用时对密码进行转换或合成,这种方式常常面临字典攻击[2]、穷举攻击、旁路攻击[3]的威胁。

芯片的"物理指纹"是在芯片生产制作过程中的随机特征,物理指纹具有唯一性和不可复制特性,如时延、频率和电压等。物理不可克隆函数(Physical Unclonable Function,PUF)是内置于芯片内部的"物理指纹"差异识别的功能单元函数。PUF 最主要的工作特性即为其唯一性和不可复制特性,每一个输入激励对应一个输出响应,不同的电路的输出是不可预测的,即"激励-响应对"CRPs。CRPs 只在激励输入的情况下才产生,激励失效则响应输出也不存在。并且 PUF 具有天然的抗剖皮攻击的特性,一旦对芯片进行剖皮后,其物理特性将会发生变化,则 CRPs 也同样产生变化,利用芯片在制作过程中的随机偏差,将产生的多个具有随机性、唯一性的 PUF 输出作为密码算法的密钥无疑更加具有安全的优势。

文献[4]首次提出 PUF 概念,通过光反射不同特性,设计实现了光学 PUF 检测系统,从此 PUF 朝着多样化的方向发展,如基于仲裁器的 PUF[5,6]、蝴蝶 PUF(Butter-Fly PUF)[7]、增加图层的 PUF(Coating-PUF)[8]和基于振荡环路的 PUF(RO-PUF)[9]等。PUF 的输出可以应用于密钥生成[10]、IP 保护[11]和身份认证[12-14]等多种领域。

虽然 PUF 的设计越来越多地呈现多元化的趋势,但是均需要额外的 PUF 生成和识别电路来实现,即这些 PUF 的通用型难以满足,给实际应用带来不便。因此本文提出了一种基于 SRAM 的 PUF 设计方法,更具有实用价值。

徐太忠(1977-),男,工程师,主要研究方向为信息安全、网络安全等,E-mail:xtz@cert.org.cn;杨天池(1978-),男,讲师,主要研究方向为 SOC 安全、物理安全防护等,E-mail:yang_tch@163.com;程 娟(1979-),女,讲师,主要研究方向为嵌入式系统、信号处理等,E-mail:cheng_j@163.com;邵奇峰(1978-),男,讲师,主要研究方向为信息安全、安全操作系统等,E-mail:sqf.ice@163.com。

2 SRAM-PUF 基本原理

SRAM 是嵌入式芯片设备中常见的随机存储器，典型的 SRAM 存储单元结构如图 1 所示。

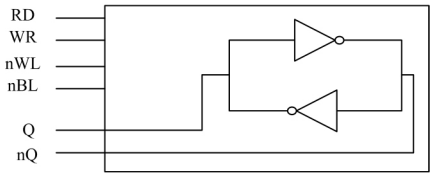


图 1 SRAM 存储单元结构图

nWL 和 nBL 控制信号分别为线使能和位使能信号，只有当 SRAM 单元的 nWL 和 nBL 同时有效时，对应的单元才被选中。WR 和 RD 分别为读写信号，在本文不参与讨论。Q 和 nQ 为 SRAM 的状态位，表示其逻辑状态处于“0”或者“1”。

由图 1 所示，SRAM 的单元结构为典型的交叉耦合回路，即一个逻辑单元由两个首尾相连的反相器构成。在无源条件下，Q，nQ 处于逻辑“00”状态；但是上电后的一段时间内，由于 WR，RD，nWL 以及 nBL 均处于无效状态，因此，Q，nQ 的输出可能处于“01”，“10”（短暂的振荡状态最终将收敛于“01”或“10”）。每个逻辑单元在上电后的状态都是不可预知的，这与制造过程中的工艺和工作环境紧密相关。

上电过程中，由于制造工艺的差异，在 SRAM 存储矩阵上，将会得到一系列不同的响应，进而形成了一组相当大规模的“激励-响应对”CRPs，因此我们可以制定系列的策略，选取 CRPs 中的特征位作为密钥，进而实现 SRAM-PUF 的密钥生成过程。

3 基于 ECC 的 SRAM-PUF 提取方法

上节阐述了 SRAM-PUF 的基本原理，然而在实际应用中，SRAM-PUF 作为密钥生成器存在下列问题：1）工作环境敏感，即使同一颗芯片上的 SRAM-PUF 在不同的工作温度、电压等条件下工作时，CRPs 也会存在一些差异；2）CRPs 的初值分布随机性能并不均匀。

为解决上述问题，本文提出了基于纠错编码的 SRAM-PUF 模糊提取方法（Fuzzy Extractor）。

3.1 模糊提取器模型

模糊提取器的基本思想是，同一激励作用于同一 SRAM-PUF 时，如果输出响应存在微小变化，可以利用数据后处理的方法，对 SRAM-PUF 的响应进行误差纠正，保持输出响应的稳定不变。

这种能够对微小变化（即模糊）进行误差纠正的设计方法称为模糊提取器。

图 2 为模糊提取器的抽象模型：

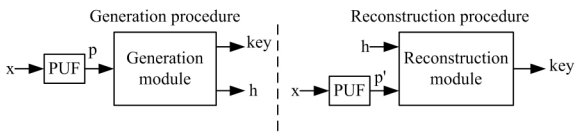


图 2 模糊提取器的抽象模型

模糊提取器划分为两个部分，分别为生成过程（generation procedure）和重建过程（reconstruction procedure）。

生成过程用于密钥的初始生成过程，在此过程中，激励 x 作用于 PUF 模块产生响应 p，p 作为生成模块的输入产生两个不相关的输出，分别为辅助数据（supplementary data）h 和密钥 key。辅助数据 h 可以作为公共数据保存在非易失性载体中，用于在重建过程中进行误差纠正；而 key 则为 x 所产生的密钥，暂存在设备缓存中，使用完毕后立即清除。

重建过程是应用于密钥使用过程中，由激励 x 作用于 PUF 模块，由于受到环境等其他因素的影响，PUF 输出具有一定噪声差异的 p'，而 p' 辅助数据 h 重构模块，可以正确地重建密钥 key。

设计生成模块和重建模块的逻辑结构是模糊提取器的重点。

3.2 基于纠错编码的模糊提取器

ECC 是一种能够错误检测和纠正的编解码技术，能够对输入数据序列中存在的微小差异进行纠错，利用 ECC 进行错误的检测与纠正的特性，可提高 SRAM-PUF 的鲁棒性，保持稳定的输出。

基于 ECC 纠错编码的模糊提取器结构如图 3 所示，分别为生成过程和重建过程。

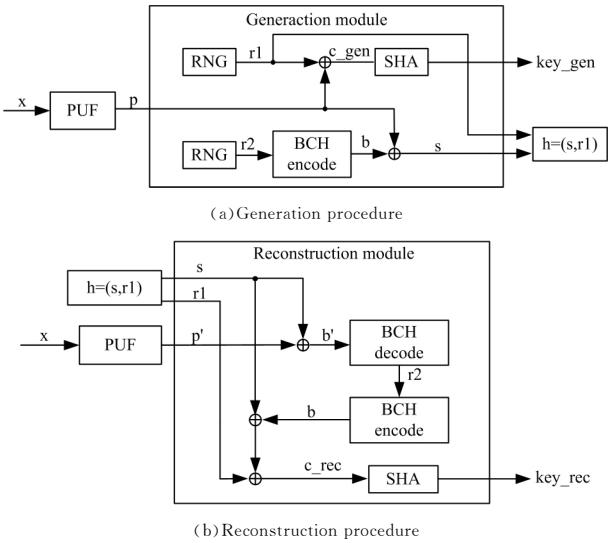


图 3 基于纠错编码的模糊提取器结构图

生成过程用于 SRAM-PUF 的注册阶段，激励 x 作用于某个 PUF 单元，生成响应 p，生成模块内部产生两个随机数序列 $r1$ 和 $r2$。$r1$ 与 p 异或操作后，进行杂凑运算 $SHA()$，生成 key_gen，key_gen 作为生成的密钥。

随机数序列 $r2$ 进行 BCH[15] 编码后，与 p 进行异或生成 s，s 和 $r1$ 共同构成辅助数据 h，其运算关系如下所示：

$$key\_gen = SHA(c\_gen) = SHA(p \oplus r1) \tag{1}$$

$$s = b \oplus p \tag{2}$$

$$b = BCH\_ENC(r2) \tag{3}$$

其中，$SHA()$ 表示杂凑运算，$BCH\_ENC()$ 表示 BCH 编码运算，$\oplus$ 为异或运算。辅助数据 $h=(s,r1)$ 存储在 FLASH 中，在 SRAM-PUF 重建过程中使用。由于辅助数据由 s 无法逆推出 p，从而也无法得到 key_gen 的数值。

在密钥重建时，辅助数据已经包含有密钥重建分量 $r1$，另外一个密钥重建分量 p 则可以由激励 x 作用于同一 PUF 生成，进而得到重建密钥 key_gen。但是在实际应用过程中，

重建分量 p 是存在微小的错误比特位的，用 p' 与 $r1$ 则无法重建出正确的密钥 key_gen。而辅助数据中 s 分量包含有 p 的信息，因此可以由 p' 和 s 利用 ECC 编解码的纠错特性，恢复出无误差的密钥重建分量 p。

重建过程如图 3(b)所示，激励 x 作用于与生成过程对应的同一个 PUF 单元，生成与 p 具有一定差异的响应 p'，p' 与辅助数据 h 共同重构出 key_rec，而 key_rec 即为 key_gen，具体的逻辑关系如下：

$$b'=s \oplus p' \tag{4}$$

其中，b' 与式(2)中 b 的比特位的数量和位置差异等价于 p' 与 p 的差异。当差异不超过 BCH 运算纠错能力时，可以得到：

$$r2=BCH\_DEC(b') \tag{5}$$

$BCH\_DEC()$ 表示解码运算，且可以得到：

$$c\_rec=b\otimes s\otimes r1=b\otimes b\otimes p\otimes r1=p\otimes r1=c\_gen \tag{6}$$

由此，重建过程的输出为：

$$\begin{aligned} key\_rec &= SHA(c\_rec) \\ &= SHA(c\_gen) \\ &= key\_gen \end{aligned} \tag{7}$$

即重建过程的输出与生成过程的输出相同。总的来说，基于纠错编码的模糊提取器在生成过程中构建出辅助数据 h，在重建过程中，通过纠错编解码和辅助数据 h，消除了重建过程中 PUF 响应的噪声误差，从而提高了输出的鲁棒性。

4 实验验证

为了对本文提出的基于纠错编码模糊提取器的性能进行验证，选取了 atmel 公司的 ATSAMV70J19 处理器，该处理器内部集成 384kB 的 RAM、1MB 的 FLASH、真随机数发生器以及 SHA256 运算模块。

在实验过程中，选取处理器最高地址空间的 8kB ram 作为 SRAM-PUF，同时需要确定密钥的输出长度和 BCH() 编解码的纠错能力，由于 ATSAMV70J19 已经内置有 SHA256 硬件加速运算模块，因此模糊提取器的杂凑运算直接选用 SHA256 算法，即输出密钥长度为 256bit。通过统计实验，SRAM-PUF 的输出误差为 6.7%，选择 BCH(127,113)编解码方式，即 113bit 数据输入时，纠错能力为 14bit，满足误差为 6.7%的纠错要求。

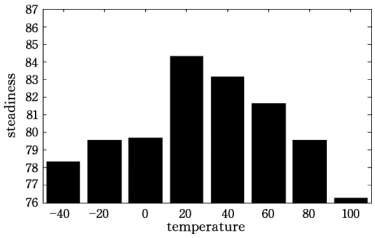
综上所述，每次作用于 SRAM-PUF 的激励 x 产生长度为 113bit 的响应，可以进行 14bit 的纠错，对应的生成密钥 key 的长度为 256bit，如果需要更长的密钥，则可以对多组激励的响应进行组合来实现。

为了统计基于纠错编码性能的有效性，采用一致性[16](steadiness)指标，定义为同一 PUF 实体在同一个激励下产生响应之间的差异。

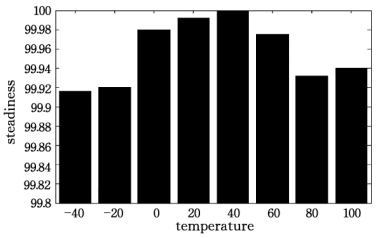
$$\sigma_{steadiness}=\left(1-\frac{1}{M\cdot N\cdot N}\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{N}key_{i,j}\otimes key_{i,k}\right)\times 100\% \tag{8}$$

其中，M 为 SRAM-PUF 响应的比特位数，N 为实验的总次数，$key_{i,j}$ 表示响应的第 i 位的第 j 次输出值。

在不同的温度条件下进行测试，每个温度测试点进行 500 次统计实现，结果如图 4 所示。



(a)无模糊提取器的 SRAM-PUF 一致性统计结果



(b)基于纠错编码的模糊提取器的 SRAM-PUF 一致性统计结果

图 4 SRAM-PUF 的一致性统计结果

图 4(a)表示未加入模糊提取器的 SRAM-PUF 一致性结果，从图中可以看出，即使在 20℃的工作条件下，一致性指标仅能达到 84%，在 100℃时仅有 76%，无法用于密钥的重建。

在图 4(b)中，一致性指标具有良好的特性，在工作不同温度下，均高于 99.9%，特别是在 20～60℃的范围内，可以达到 99.98%。有效提高了 SRAM-PUF 的鲁棒性。相对于图 4(a)的方法，一致性指标提高 12%以上。

如果要进一步提高一致性指标，可以采取提高纠错能力的 BCH 编码，如 BCH(255,131)，纠错能力为 124 等。

结束语 本文提出了一种基于 SRAM 的 PUF 设计方法，为了提高 SRAM-PUF 的鲁棒性，设计并实现基于纠错编码的 SRAM-PUF 模糊提取器，实验验证结果再次验证了模糊提取器的有效性，极大提高了 SRAM-PUF 的使用性和应用价值。

参 考 文 献

[1] 胡丽辉，张建泉，李楠，等. 带内存保护的 FreeRTOS 在 TMS570 上的移植[J]. 单片机与嵌入式系统应用，2015，15(2)：63-66

[2] 李龙谱，斯雪明，张志鸿，等. 在多 FPGA 上实现基于字典的 ZIP 文档口令恢复[J]. 计算机应用与软件，2015，32(6)：292-295

[3] 李浪，李仁发，童元满，等. 嵌入式加密芯片功耗分析攻击与防御研究进展[J]. 计算机研究与发展，2010，47(4)：595-604

[4] Pappu R，Recht B，Taylor J，et al. Physical one-way functions [J]. Science，2001，297(5589)：2026-2030

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

[6] Machida T，Yamamoto D，et al. A New Mode of Operation for Arbiter PUF to Improve Uniqueness on FPGA[J]. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems，2014，2(3)：871-878

[7] Kumar S S，Guajardo J，et al. Extended abstract：the butterfly PUF protecting IP on every FPGA[C]// IEEE International Workshop on Hardware Oriented Security and Trust. 2008：67-70

[8] Tuyls P, et al. Read-proof hardware from protective coatings[C]// 8th International Workshop, Vokohama, Janpan. October 10-13, 2006:369-383

[9] Cao Yuan, Zhang Le, 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

[10] Masato T G C, Mitsuru S, et al. A stable key generation from PUF responses with a fuzzy extractor for cryptographic authentications[C]// IEEE Global Conference on Consumer Electronics. 2013:525-527

[11] Guajardo J, Kumar S S, Schrijen G J, et al. FPGA Intrinsic PUFs and Their Use for IP Protection[M]. Cryptographic Hardware and Embedded Systems-CHES 2007. Springer Berlin Heidelberg, 2007:63-80

[12] 李晖,夏伟,邓冠阳,等. PUF-HB#:轻量级 RFID 双向认证协议[J]. 北京邮电大学学报,2013,36(6):13-17

[13] Majzoobi M, Rostami M, et al. Devadsa S. Slender PUF protocol: A light weight, robust, and secure authentication by substring matching[J]. IEEE Symposium on Security and Privacy Workshops, 2012:33-44

[14] 向学哲,马昌社. 基于 PPUF 的高效 RFID 隐私认证协议[J]. 华南师范大学学报,2013,45(1):42-46

[15] Canteaut A, Chaband F. A New Algorithm for Finding Minimun-weight Words in a Linear Code: Application to McEliece's Cryptosystem and to BCH codes of length 511[J]. IEEE Transactions on Information Theory, 2010, 44(1):367-378

[16] Hori Y, Yoshida T, et al. Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs[C]// 2010 International Conference on Reconfigurable Computing and FPGAS, Cancun, Quintana Roo, Mexico, 13-15 December 2010:115-120

(上接第 361 页)

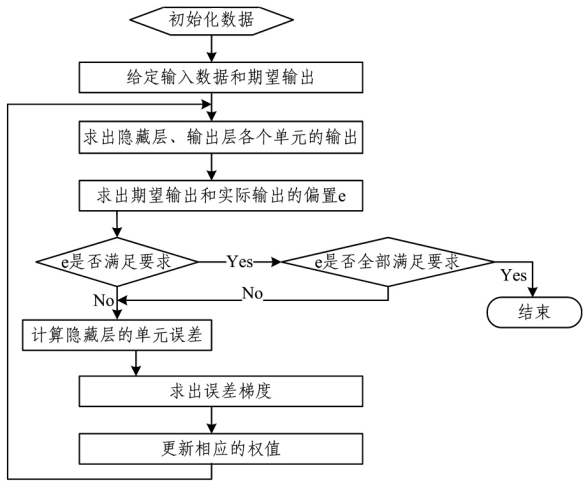


图 5 神经网络算法

结束语 综上所述,可以确定的是网络的体系架构对未来下一代网络的发展方向起着关键性的作用。基于电的分组交换网络和基于光的光交换网之间的紧密联系和数据交换是下一代网络将要研究的对象。我国应该注重组织新的示范网工程,使之达到局部验证成功到大面积推广的效果,这样不仅可以实现更宽的带宽,而且可以在实践中发现问题并可以方便连接各个网络。另外,网络安全是未来下一代网络不可逾越的问题,再加上未来网络速度更快、带宽更宽、运营商的网络规模庞大且结构复杂,网络容易受到攻击的部分也会越来越多,如果采用过去的基于"木桶理论"的安全边界防护体系,这个任务必定是难以完成的。然而使用大数据技术建设下一代网络安全防护体系,就可以利用丰富的检测分析数据迅速发现新的威胁内容;同时深度神经网络的学习也可以预测危险,及时高效地发现网络的安全问题并加以解决。因此未来下一代网络安全的发展将是基于深度神经网络和大数据安全防护的下一代网络安全体系。

参 考 文 献

[1] 程海燕,董见. 下一代网络技术在移动通信网络中的应用[J]. 信息通信,2014(7):210-210

[2] 赵慧玲. 软交换下一代网络的核心[J]. 中国电信业,2001(4):47-49

[3] 于伟. NGN 网络 QoS 的分析和保障[D]. 青岛:山东大学,2009:1-3

[4] 肖勇. 基于服务元网络体系结构的实时通信系统的设计与实现[D]. 成都:电子科技大学,2008

[5] 李国杰. 关于下一代网络的体系结构[J]. 中国工程科学,2002(8):40-43

[6] 樊秀梅,林闯,王忠民. 网边缘可控的 IP QoS 体系结构及其算法[J]. 电子学报,2002,30(12A):2027-2031

[7] ITU. ITU releases annual global ICT data and ICT Development Index country ranking[R]. Geneva, Switzerland, ITU, 2015

[8] Saltzer, et al. End-to-End Arguments in System Design [J]. ACM Transactions in Computer System, 1984, 11(3):277-288

[9] Clark D D, Blumenthal M S. Rethinking the design of the Internet: The end to end arguments vs. the brave new world[J]. ACM Transactions on Internet Technology — TOIT, 2001, 11(1):70-109

[10] 李国杰,徐志伟. 关于下一代网络体系结构和应用模式的思考[J]. 武汉理工大学学报(信息与管理工程版),2002,10(4):1-6

[11] 史凡,姚建锋,陈运清. 下一代互联网络体系架构与现网络演进实践[J]. 电信技术,2011,5(15):67-70

[12] 王璐. 移动互联网用户行为分析[D]. 北京:北京邮电大学,2011

[13] 乐红文. 典型 IPv6 过渡技术的仿真与组网设计[D]. 南昌:南昌大学,2011

[14] 张晓兵. 下一代网络安全解决方案[J]. 电信工程技术与标准化,2014,6(13):59-61

[15] Srihari R K. Situation awareness through concept—based information extraction [EB/OL]. (2012-05-20). http://www.dawnbreaker.com/vas05

[16] Xie Li-xia, Wang Ya-chao, Yu Jin-bo. Network Security Situation Awareness based on Neural Network [J]. Journal of Tsinghua University(Science and Technology), 2013, 53(12):1750-1760