



基于 SRAM PUF 稳定性处理的 RFID 标签密钥生成方案

潘畚稣¹, 张继军^{1,2}, 张钊锋²

(1. 上海大学 材料科学与工程学院, 上海 201900; 2. 中国科学院上海高等研究院, 上海 200120)

摘 要: 物理不可克隆函数 (PUF) 以其不可预测、不可克隆等特性提高了 RFID 通信系统的安全性, 然而 PUF 响应的稳定性处理给资源、计算力等受限标签带来较大挑战。为此, 利用 SRAM 部分非稳定单元相邻的特性, 提出一种基于条件概率的预选位方法, 结合反向模糊提取器设计 SRAM PUF 稳定性处理方案, 在计算力和面积都较小的情况下仍能稳定生成密钥。实验结果表明, 在平均错误率为 0.14 的条件下, 该方法仅需 686 个 SRAM PUF 单元即可得到失败率为 4.5×10^{-5} 的 64 bit 密钥。

关键词: 射频识别; 物理不可克隆函数; 预选位; 反向模糊提取器; 密钥生成

开放科学 (资源服务) 标志码 (OSID):



中文引用格式: 潘畚稣, 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): 149-153, 162.

英文引用格式: PAN Shesu, ZHANG Jijun, ZHANG Zhaofeng. Key generation scheme for RFID tag based on SRAM PUF stability processing [J]. Computer Engineering, 2020, 46(9): 149-153, 162.

Key Generation Scheme for RFID Tag Based on SRAM PUF Stability Processing

PAN Shesu¹, ZHANG Jijun^{1,2}, ZHANG Zhaofeng²

(1. School of Material Science and Engineering, Shanghai University, Shanghai 201900, China;

2. Shanghai Advanced Research Institute, Chinese Academy of Sciences, Shanghai 200120, China)

[Abstract] Physical Unclonable Function (PUF) improves the security of the RFID communication system because of its unpredictable and unclonable characteristics. However, the stability of PUF response brings great challenges to tags with limited resources and computing power. In order to solve the problem, this paper proposes a pre-selection method based on conditional probability using the property that some unstable elements of SRAM are adjacent, and designs a SRAM PUF stability processing scheme based on the reverse fuzzy extractor. The key can still be generated stably when the computational power and area are small. Experimental results show that on condition of average error rate of 0.14, the proposed method only needs 686 SRAM PUF units to generate a 64 bit key with a failure rate of 4.5×10^{-5} .

[Key words] Radio Frequency Identification (RFID); Physical Unclonable Function (PUF); pre-selection; reverse fuzzy extractor; key generation

DOI: 10.19678/j.issn.1000-3428.0055974

0 概述

随着 RFID 技术的不断发展和广泛应用, 用户隐私密钥泄露等安全问题变得越来越重要。传统 RFID 通信系统应用对称加密时, 标签将密钥信息存储在非易失性存储器中, 但这种方式容易被窃取或恶意篡改。物理不可克隆函数 (Physical Unclonable Function, PUF) 以其不可克隆的理想特性, 被认为是

一种具有应用前景的安全构建模块, 可用于各种认证和识别应用的密钥。PUF 信息是电路在制造过程由工艺造成的差异产生的, 电路下电后其响应信息自动湮灭, 不容易被攻击^[1-2]。

近年来, 国内外学者对 PUF 在安全通信方面的应用进行了深入研究^[3-5], 但多数研究均没有考虑到 PUF 在实际使用过程中的稳定性处理问题。因为相同的 PUF 在每次响应时往往还存在一定差异, 所以

基金项目: 国家自然科学基金 (51472155, 11675099)。

作者简介: 潘畚稣 (1996—), 女, 硕士研究生, 主研方向为 PUF 密钥生成、RFID 安全通信; 张继军, 副研究员、博士; 张钊锋 (通信作者), 研究员、博士。

收稿日期: 2019-09-10

修回日期: 2019-10-22

E-mail: panshesu@sari.ac.cn

不能直接作为密钥使用。针对 PUF 响应的稳定性处理问题,文献[6-7]提出一种利用模糊提取器得到稳定输出,该方法虽然能够有效纠正 PUF 的错误响应,但是运算量较大,不适用于计算力、面积与功耗等受限的标签。文献[8]提出将 PUF 响应行为看作布尔函数,并与傅里叶变换分析相结合,该方案的运算量较纠错码方案减小了很多,然而,利用 8 kB 的 SRAM 生成 128 bit 的密钥对于标签而言成本较高。文献[9]提出的反向模糊提取器虽然可以大幅降低标签的负担,但是当 PUF 片间距离较大时,硬件开销也会随之增加。为了降低 PUF 的片间距离,以减小 ECC 纠错负担,文献[10-12]提出各种预选位方法,以选择最稳定的 PUF 单元,但各种预选位方法都需要在大量的 PUF 源中进行测试挑选,造成多数 PUF 单元被浪费。

本文通过对 SRAM PUF 进行研究,利用其非稳定且总是相邻的特点,提出基于条件概率的预选位方法。结合反向模糊提取器设计了应用于 RFID 标签密钥生成的 SRAM PUF 处理模块,以在非正常工作条件下达到较小失败率。

1 SRAM PUF 介绍

硅 PUF 由于原理和结构的不同存在基于时延的仲裁 PUF、环形振荡器 PUF、基于失配的 SRAM PUF、蝶形 PUF 以及基于电流的 PUF 等各种类型。

SRAM 作为传统存储器被普遍嵌入各种电子产品。每个 SRAM 单元都具有优先上电状态,而优先上电状态对于不同 SRAM 单元和不同芯片都各不相同,这种上电模式可以作为 PUF。SRAM PUF 是目前最受欢迎的硅 PUF 之一,它无需硬件修改和额外硬件开销即可作为 PUF 模块^[13-14]。因此,本文采用 SRAM 作为标签的 PUF 源,并以此展开研究。

2 稳定性设计

2.1 反向模糊提取器

PUF 测量物理电路特性以产生响应,然而与任何物理测量一样,SRAM PUF 的响应值不可避免地受到热噪声和不同环境条件的影响,因此,PUF 响应的复制不是完全稳定的^[15]。为了稳定噪声响应得以在加密协议中使用,需要引入模糊提取器提取 PUF 响应的稳定部分并生成密钥。

基于 code-offset 的模糊提取器结构如图 1 所示^[16],其通过注册和重现 2 个阶段产生 SRAM PUF 密钥。在注册阶段,通过 Gen() 产生辅助数据 W,该辅助数据在重现阶段用来通过 Rep() 恢复响应。Gen() 和 Rep() 分别为相应纠错码的编码和解码函数,汉明距离在纠错码的纠错范围内的带噪响应可以被正确纠正。KDF() 为密钥派生函数,用来生成强密钥。

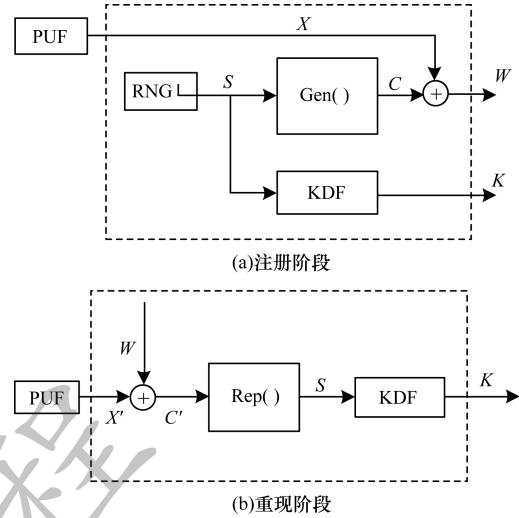


图 1 基于 code-offset 的模糊提取器结构

Fig. 1 Fuzzy extractor structure based on code-offset

通常在模糊提取器的设置中,服务器存储在注册阶段,执行 Gen() 函数后生成辅助数据,在重现阶段将辅助数据发送给 PUF 设备,由 PUF 设备纠错修正 Rep() 函数生成的带噪响应。然而,由于 Rep() 函数的计算量远大于 Gen() 函数,文献[9]提出将 Gen() 函数放在资源受限的设备中,由服务器负责执行 Rep() 函数修正存储值,该方法称为反向模糊提取器。考虑到标签对面积、功耗等的要求远高于读写器,本文选择基于 code-offset 的反向模糊提取器作为标签的 PUF 响应处理,以轻量海绵结构的哈希函数作为 KDF。

2.2 熵泄露分析及参数选择

由图 1 可知,生成的密钥由随机数种子 S 经过 KDF() 函数后生成,而辅助数据 W 是公开的,因此,为保证安全性需要保证在 W 已知情况下, S 仍具有足够的熵。S 为长度为 k 的随机数种子,因此, $H_{\infty}(S) = \text{length}(S) = k$ 。用条件熵 $H_{\infty}(S|W)$ 表示已知 W 时 S 的剩余熵,具体如式(1)所示:

$$H_{\infty}(S|W) = H_{\infty}(S) - I(S, W) \quad (1)$$

其中:

$$\begin{aligned} I(S, W) &= I(S, X \oplus SG) = H_{\infty}(S) - H_{\infty}(X) + H_{\infty}(XH^T) = \\ &= k - H_{\infty}(X) + H_{\infty}(XH^T) \\ H_{\infty}(XH^T) &\leq |XH| = n - k \\ H_{\infty}(X) &= nh(p_b) \\ h(p_b) &= -\text{lb}(\max(p_b, 1 - p_b)) \end{aligned} \quad (2)$$

最终可得:

$$H_{\infty}(S|W) = H_{\infty}(X) - H_{\infty}(XH^T) \geq k - n(1 - h(p_b)) \quad (3)$$

其中, n 为纠错码码长, p_b 为 PUF 响应的偏置(响应值出现 1 的概率), $h()$ 为最小熵密度函数, H 为相应纠错码的校验矩阵。为提高纠错效率,采用 BCH

码 C_2 作为外码,重复码 C_1 作为内码, L 个 (n_2, k_2, t) 结构的 BCH 码和 $(n_1, 1, n_1)$ 重复码级联后, $H_\infty(XH^T)$ 可由式(4)表示^[16-18]:

$$H_\infty(XH^T) \leq L \cdot (n_2 \cdot H_\infty(X_{1:n_1}H_1^T) + H_\infty(X_{1:n_2}H_2^T)) = L \cdot (n_1 n_2 - k_2) \quad (4)$$

因此,级联后的剩余熵下限如式(5)所示,并以该下限值作为设计最终所得密钥熵。

$$H_\infty(S|W) \geq L - (n_1 n_2 h(p_b) - n_1 n_2 + k_2) \quad (5)$$

假设 PUF 响应每比特出现的错误概率为 e ,级联码的纠错失败率可由式(6)表示:

$$\begin{aligned} p_1 &= \sum_{i=0}^{n_1/2} C_{n_1}^i e^i (1-e)^{n_1-i} \\ p_2 &= \sum_{i=0}^L C_{n_2}^i (1-p_1)^i p_1^{(n_2-i)} \\ p_{\text{fail}} &= 1 - p_2^L \end{aligned} \quad (6)$$

其中, p_1 和 p_2 分别为经过重复码译码和 BCH 码译码后的成功率。对于给定 BCH (n_2, k_2, t) 码,生成熵为 k 的密钥需要 $L = (k/H_\infty(S|W))$ 个块, p_{fail} 为最终密钥生成失败率。

对 1 kB ISSI SRAM 上电初始值进行统计,得到片内距离均值为 0.075,该值可作为每比特发生错误的平均概率 e , p_b 为 0.51。当偏置 p_b 范围为 $[0.42, 0.58]$ 时,增加初始响应长度可得到所需密钥熵^[19],因此,本文设计通过增加初始长度而不额外增加针对密钥泄露的处理部分。考虑到标签的面积和计算力制约,根据式(5)、式(6)设计生成熵为 64 bit 的密钥,不同纠错码的结果比较如表 1 所示。从表 1 可以看出,相较于 RM 码和 Golay 码, BCH 码的效果更好。

表 1 不同纠错码级联结果比较
Table 1 Comparison of cascade results of different error correction codes

$C_1(n_1, 1, n_1)$	$C_2(n_2, k, t)$	p_{fail}	SRAM PUF 大小
Rep(3, 1, 3)	BCH(127, 78, 15)	1.1×10^{-3}	381
Rep(5, 1, 5)	BCH(127, 85, 13)	6.4×10^{-7}	635
Rep(3, 1, 3)	RM(16, 5, 8)	1.9×10^{-3}	864
Rep(3, 1, 3)	RM(31, 6, 16)	5.0×10^{-7}	1 860
Rep(3, 1, 3)	Golay(24, 12, 8)	3.8×10^{-3}	504
Rep(5, 1, 5)	Golay(24, 12, 8)	1.6×10^{-5}	960

2.3 基于条件概率的预选位方法

上述实验结果是在正常工作条件下得到的,当标签老化或处于较极端外界环境下(高温、高压等)时,实验的失败率会相应增加,如果仅靠纠错码进行纠错,硬件开销和计算复杂度也会随之增加。图 2 为 $0^\circ\text{C} \sim 100^\circ\text{C}$ 下, 1 kB SRAM 经过 100 次测试得到的平均错误率,当温度为 100°C 时,平均错误率 e 上升

至 0.14,用表 1 中效果最好的 Rep(5, 1, 5) 与 BCH(127, 85, 13) 纠错码级联只能得到约为 0.02 的失败率。因此,可以通过预选位减小 SRAM PUF 的片内距离,在不增加纠错码复杂度的条件下降低密钥生成失败率。

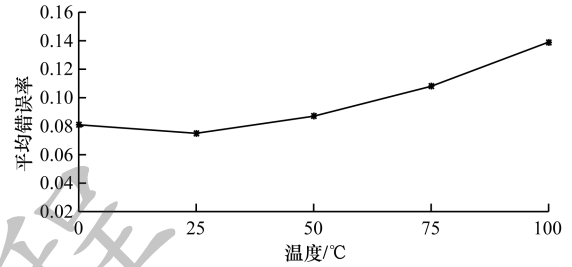


图 2 不同温度下 SRAM 的平均错误率
Fig. 2 Average error rate of SRAM at different temperatures

通过对 SRAM PUF 响应分析发现,与其他 PUF 不同的是,其具有大量的稳定位,此外,由于低面积和低功耗的需求,相邻 SRAM 单元的物理距离相应减小,从而增加了耦合电容产生的电容串扰,因此 SRAM 单元的稳定性会受其相邻位的影响^[12]。图 3 为相邻 100 bit 的 SRAM PUF 响应测量 100 次得到的错误率分布。从图 3 可以看出,每比特错误率分布不均,且稳定位和非稳定位总是各自相邻。基于 SRAM 单元非稳定位的相邻特性,提出在反向模糊提取器纠错的基础上去除少量连续出错概率较高的非稳定位,以提高纠错成功率。

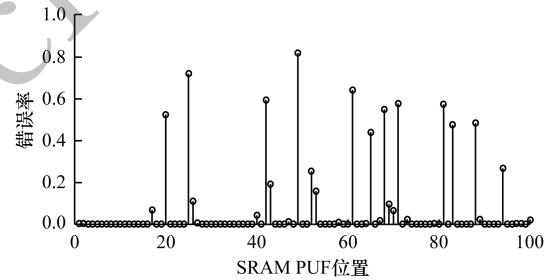


图 3 相邻 100 bit 的 SRAM PUF 错误率分布
Fig. 3 Error rate distribution of SRAM PUF of adjacent 100 bit

为去除连续出错概率较高的非稳定位,实验使用条件概率描述 SRAM 单元对相邻单元稳定性的依赖,具体如式(7)所示:

$$P(A|B) = \frac{P(A, B)}{P(B)} \quad (7)$$

其中, $P(A)$ 表示测试位发生错误的概率,由于实验选用 Rep(5, 1, 5) 作为内码进行测试比较, $P(B)$ 则表示窗长度为 5 时,该测试位的窗内邻近位发生 2 个及以上错误的概率,当测试位条件概率 $P(A|B)$ 大于阈值 T 时,则弃用该 SRAM 单元。由于 SRAM PUF 进行

注册阶段前预选位的测试次数会影响到开发的时间和成本,实验在不同工作条件下(具体如表 2 所示)对非稳定定位的条件概率超过 0.5 的比例进行比较。实验结果发现,在高温、高压条件下,SRAM PUF 相邻非稳定定位的比例最高,具体如图 4 所示,这说明了在该工作环境下,SRAM 单元对相邻单元依赖性最高。因此,该工作条件可作为预选位时的测试环境,高效去除了由于外界环境影响最容易出现连续不稳定的 SRAM 单元。

表 2 工作环境参数

Table 2 Working environment parameters

测试条件	温度/℃	电压/V
高温、高压 (HTHV)	100	3.4
高温 (HT)	100	3.2
低温 (LT)	0	3.2
高压 (HV)	25	3.4
低压 (TV)	25	3.0

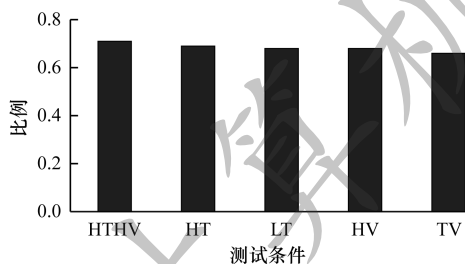


图 4 不同测试条件下不稳定定位条件概率超过 0.5 的比例

Fig.4 The ratio of the conditional probability of unstable position exceeding 0.5 under different test conditions

Rep(5,1,5)与 BCH(127,85,13)级联作为反向模糊提取器中的纠错码,图 5 为采用上述预选位方法在不同阈值下生成 64 bit 密钥,并测试 5 万次的失败率以及相应丢弃的位数,图 6 为在相同丢弃位数下,本文方法与丢弃最高错误率 SRAM 单元方法的失败率比较。当阈值 $T=0.3$ 时,仅去除 51 个非稳定 SRAM 单元可以达到 4.6×10^{-5} 的失败率,比丢弃相同数量的最高错误率单元方法下降了约 2 个数量级。

表 3 不同稳定性处理方法性能比较

Table 3 Performance comparison of different stability treatment methods

方法	Block 数量(L)	Codes Type	内码 $C_1(n_1, 1, n_1)$	外码 $C_2(n_2, k_2, t)$	SRAM PUF 大小	失败率 P_{fail}
文献[9]方法	1	Rep + BCH	(5,1,5)	(127,85,13)	635	2.0×10^{-2}
	2	Rep + BCH	(5,1,5)	(127,57,23)	1 270	5.3×10^{-5}
文献[10]方法	1	BCH	—	(127,71,19)	852	5.6×10^{-5}
文献[11]方法	4	BCH	—	(31,16,3)	992	3.9×10^{-5}
Hard RM ^[20]	22	Rep + RM(Hard)	(15,1,15)	(8,4,4)	2 640	8.7×10^{-5}
Soft RM ^[20]	22	Rep + RM(Soft)	(9,1,9)	(8,4,4)	1 584	8.5×10^{-5}
本文方法	1	Rep + BCH	(5,1,5)	(127,85,13)	686	4.6×10^{-5}

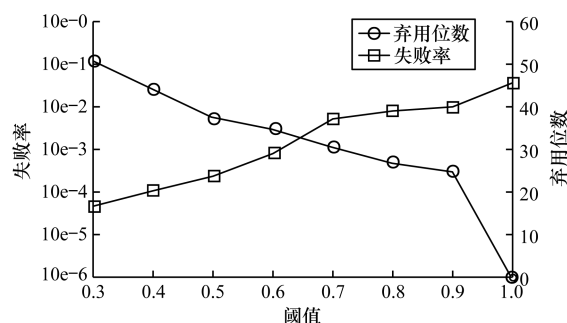


图 5 不同阈值下 SRAM 单元弃用位数与失败率

Fig.5 The number of discarded bits and failure rate of SRAM cells under different thresholds

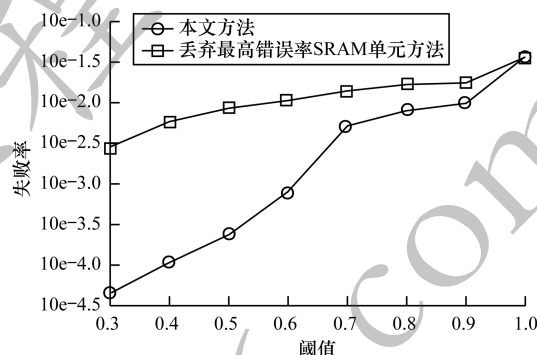


图 6 2 种方法在弃用相同 SRAM 单元数量下的失败率对比

Fig.6 Comparison of failure rates of two methods with the same number of SRAM cells abandoned

3 实验结果与分析

上述方法选择的丢弃位地址可以存储在非易失性存储器中,这是因为位置信息与响应值无关,不会泄露密钥。表 3 为对上述 ISSI SRAM PUF 初始响应进行不同处理方法生成 64 bit 密钥的性能比较,实验均取平均错误率为 0.14, $p_b = 0.51$ 。文献[10-11]只是在大量 PUF 单元内以较高概率选择稳定位,同样需要结合 ECC 纠错,软判决^[20]相较于硬判决所需资源更小,然而由于需要位相关的可靠度信息作为辅助数据以分辨可靠响应,容易受到辅助数据攻击^[21]。本文利用部分不稳定 SRAM 单元相邻的特点,提出的改进方法结合了反向模糊提取器和预选位的优点,相比于其他方案,其能够以较小的 PUF 得到失败率在 10^{-5} 量级的 64 bit 密钥。

表 4 为实现 10^{-5} 量级失败率时,本文预选位方法和文献[9]方法的各模块面积比较。一个标准 SRAM 单元可以看作 1 个等效门 $GE^{[20]}$ 。由于本文设计是针对标签应用的反向模糊提取器,因此不考虑在读写器端执行的 $Rep()$ 重现部分,此外标签的各种通信协议均需要产生随机数,反向模糊提取器中的随机数种子可以通过复用标签自身的随机数发生器得到。

表 4 文献[9]方法与本文方法的模块面积比较

Table 4 Comparison of module area between literature[9] method and the proposed method

方法	SRAM PUF 大小	Gen()	轻量 Hash	控制部分
本文方法	686	2 531	1 094	1 273
文献[9]方法	1 270	7 345	—	—

4 结束语

本文对 SRAM PUF 的响应特征进行研究,利用 SRAM 部分非稳定相邻的特点,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非稳定位,并结合反向模糊提取器设计可应用于标签的 SRAM PUF 稳定性处理方案。实验结果表明,本文方法即使在非正常工作条件下仍能保持 10^{-5} 量级的较低失败率。然而,位置信息的存储在一定程度上增加了标签的存储成本,下一步将对该方案继续改进,在平衡 SRAM PUF 大小、算法复杂度和辅助信息的存储代价的基础上,进一步降低方案的开发成本。

参考文献

- [1] LIU Weiqiang, CUI Yijun, WANG Chenghua. Design and implementation of a low-cost physical unclonable function and its application in RFID [J]. Acta Electronica Sinica, 2016, 44(7): 1772-1776. (in Chinese)
刘伟强, 崔益军, 王成华. 一种低成本物理不可克隆函数结构的设计实现及其 RFID 应用 [J]. 电子学报, 2016, 44(7): 1772-1776.
- [2] LIU Boya, ZHANG Yue, YANG Yatao, et al. Lightweight mutual authentication protocol based on PUF function [J]. Computer Engineering, 2019, 45(2): 38-41, 52. (in Chinese)
刘博雅, 张悦, 杨亚涛, 等. 基于 PUF 函数的轻量级双向认证协议 [J]. 计算机工程, 2019, 45(2): 38-41, 52.
- [3] MANAMI S, REI U, NAOFUMI H, et al. Efficient fuzzy extractors based on ternary debiasing method for biased physically unclonable functions [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2019, 66(2): 616-629.
- [4] YANG Jianxi, ZHANG Yue, CHI Yaping, et al. Design of cell reselection security protocol based on physical unclonable function [J]. Computer Engineering, 2018, 44(11): 154-157, 164. (in Chinese)
杨建喜, 张悦, 池亚平, 等. 基于物理不可克隆函数的小区重选安全协议设计 [J]. 计算机工程, 2018, 44(11): 154-157, 164.
- [5] PANG Zihan, ZHOU Qiang, GAO Wenchao, et al. Hardware implementation of physical unclonable function on FPGAs [J]. Journal of Computer-Aided Design & Computer Graphics, 2017, 29(9): 1590-1603. (in Chinese)
庞子涵, 周强, 高文超, 等. FPGA 物理不可克隆函数及其实现技术 [J]. 计算机辅助设计与图形学学报, 2017, 29(9): 1590-1603.
- [6] 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.
- [7] MAES R, VAN HERREWEGE A, VERBAUWHEDE I. PUFKY: a fully functional PUF-based cryptographic key generator [C]//Proceedings of the 14th International Conference on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2012: 302-319.
- [8] LIU Wenchao, LU Zhaojun, LIU Hailong, et al. A novel security key generation method for SRAM PUF based on fourier analysis [J]. IEEE Access, 2018, 6: 49576-49587.
- [9] VAN H A, KATZENBEISSER S, MAES R, et al. Reverse fuzzy extractors: enabling lightweight mutual authentication for PUF-enabled RFIDs [M]. Berlin, Germany: Springer, 2012: 374-389.
- [10] EIROA S, CASTRO J, MARTINEZ-RODRIGUEZ M C, et al. Reducing bit-flipping problems in SRAM physical unclonable functions for chip identification [C]//Proceedings of the 19th IEEE International Conference on Electronics, Circuits, and Systems. Washington D. C., USA: IEEE Press, 2012: 392-395.
- [11] YU M D, DEVADAS S. Secure and robust error correction for physical unclonable functions [J]. IEEE Design & Test of Computers, 2010, 27(1): 48-65.
- [12] RAHMAN M T, HOSEY A, GUO Z M, et al. Systematic correlation and cell neighborhood analysis of SRAM PUF for robust and unique key generation [J]. Journal of Hardware and Systems Security, 2017, 1(2): 137-155.
- [13] GAO Y S, SU Y, XU L, et al. Lightweight (reverse) fuzzy extractor with multiple reference PUF responses [J]. IEEE Transactions on Information Forensics and Security, 2019, 14(7): 1887-1901.
- [14] SUTAR S, RAHA A, RAGHUNATHAN V. Memory-based combination PUFs for device authentication in embedded systems [J]. IEEE Transactions on Multi-Scale Computing Systems, 2018, 4(4): 793-810.
- [15] GAO Yansong, SU Yang, YANG Wei, et al. Building secure SRAM PUF key generators on resource constrained devices [C]//Proceedings of 2019 IEEE International Conference on Pervasive Computing and Communications Workshops. Washington D. C., USA: IEEE Press, 2019: 912-917.

(上接第 153 页)

- [16] MAES R, LEEST V, SLUIS E, et al. Secure key generation from biased PUFs [M]. Berlin, Germany: Springer, 2015: 517-534.
- [17] DELVAUX J, GU D W, VERBAUWHEDE I, et al. Efficient fuzzy extraction of PUF-induced secrets: theory and applications [M]. Berlin, Germany: Springer, 2016: 412-431.
- [18] WAN Chao. Design and realization of the security outline of zero information leakage based on PUF [D]. Chengdu: University of Electronic Science and Technology of China, 2018. (in Chinese)
万超. 基于 PUF 的零信息泄露的安全概略的设计与实现 [D]. 成都: 电子科技大学, 2018.
- [19] JEROEN D. Security analysis of PUF-based key generation and entity authentication [D]. Shanghai: Shanghai Jiaotong University, 2017. (in Chinese)
JEROEN D. 基于 PUF 密钥生成和实体认证的安全性分析 [D]. 上海: 上海交通大学, 2017.
- [20] LEEST V, PRENEEL B, SLUIS E. Soft decision error correction for compact memory-based PUFs using a single enrollment [C] // Proceedings of the 14th International Conference on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2012: 268-282.
- [21] BECKER G T. Robust fuzzy extractors and helper data manipulation attacks revisited: theory versus practice [J]. IEEE Transactions on Dependable and Secure Computing, 2019, 16(5): 783-795.

编辑 刘继娟