

适用于 SRAM-PUF 的纠错码研究

冯志华¹, 张 苗², 邹雪城², 刘政林²

(1 北京计算机技术及应用研究所, 北京 100854; 2 华中科技大学 光学与电子信息学院, 湖北 武汉 430074)

摘 要: 物理不可克隆函数(Physical Uncloneable Functions, PUFs)能够产生、存储密钥, 可以抵御侵入攻击的威胁. 利用 SRAM PUF 进行密钥提取时, 需用纠错编码来恢复密钥源数据, 通常采用 BCH 纠错码, 但是 BCH 的迭代译码算法复杂, 单纯地利用 BCH 编码使得硬件开销大. 本文提出一种级联编码方案, 将较长码字分成两个较短码字逐级编译码, 仿真结果表明本文所提的级联编码方案能够满足 SRAM-PUF 纠错率的要求.

关键词: 物理不可克隆函数; 密钥; 纠错编码; 级联编码

中图分类号:

文献标识码: A

文章编号: 1000-7180(2016)06-0011-03

Study on Error Correcting Code Applied to SRAM-PUF

FENG Zhi-hua¹, ZHANG Miao², ZOU Xue-cheng², LIU Zheng-lin²

(1 Beijing Institute of Computer Technology and Applications, Beijing 100854, China; 2 School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: Physical Unclonable Function(PUF) can generate and store security keys in a way that can prevent them from assaulting attacks. When deploying PUF to extract the keys, we have to apply Error Correcting Code where the BCH code is the most often used to reconstruct the source data of security key. But the decoding algorithm of BCH is complex, making it hardware-inefficient when using BCH code only. This paper proposed a concatenated construction by splitting a longer code into two shorter codes and then decoding in two steps. The results of simulation show the construction based on concatenate codes can meet the need of SRAM-PUF's error rate.

Key words: PUF; security keys; error correcting code; concatenated codes

1 引言

密码系统的安全性依赖于密钥的安全性. 密钥的泄漏往往意味着整个安全机制的失效, 而物理侵入攻击对密钥安全有着致命的威胁. 物理非克隆函数(PUF)是一种能有效抵抗物理攻击的密钥产生办法, 与传统密码学的密钥产生方案不同, PUF 使用激励和响应对的方法生成密钥, 激励和响应之间的映射关系仅由设备个体的某些物理差异决定. IC 制造过程中的无法预测、复制和控制的细微差异产生了这些物理差异. 任何潜在物理攻击将破坏设备个体的物理差异, PUF 的激励和响应之间的映射关系也会发生变化. 因此, PUF 密钥具备物理决定、稳

定唯一、随用随取、不用保存、难以事先预测和容易测量的优点, 能提供安全、稳定和低成本的密钥. SRAM-PUF 的激励响应对是存储单元地址和对应地址单元的上电初始值, 它不需要额外地搭建硬件电路, 易于实现且可以降低成本.

使用 SRAM-PUF 提取密钥存在两个问题: (1) 由于存在环境噪声的影响, 上电初值不是稳定不变的, 而有一些微小的变化; (2) SRAM 上电初值不是均匀分布的. 由此提出让 HDA (Helper Data Algorithm) 对 SRAM-PUF 提取的数据进行处理. HDA 又叫模糊提取器 (Fuzzy Extractor). 在 Fuzzy Extractor 结构下, 使用图 1 所示的具体方式来处理 SRAM-PUF 数据, 以获得满足要求的密钥, 模糊提

取器通过注册 (Enrollment) 和密钥重构 (Key Reconstruction) 两个阶段来产生 SRAM-PUF 密钥。

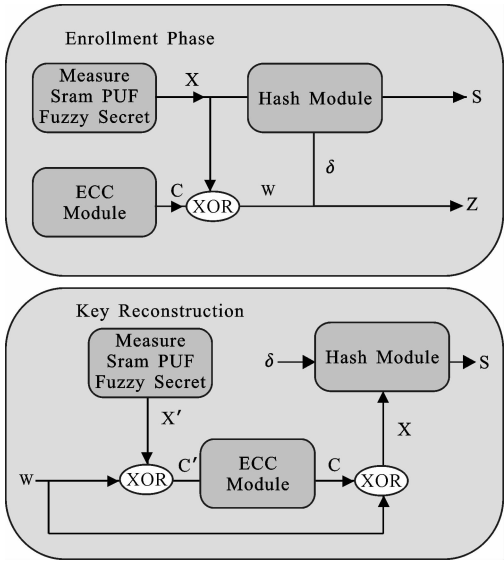


图 1 数据返回控制

用级联方案处理 ECC 模块时,可供考虑的码类有:重复码、一阶 RM 码、格雷码和 BCH 码. LDPC 码只有在码长较长的情况下接近香浓极限才有较好的纠错效果,在这里不适用,所以在此就不考虑 LDPC 码. 在研究纠错编码方案时,先做以下假设:

- (1) 要从 PUF 响应中提取 128 位密钥,而 SRAM 的 secrecy rate 为 0.76^[1],则需要得到 128/0.76=171 bits 的“无错”信息位通过哈希得到 128 位密钥;
- (2) 每个 SRAM 单元的出错概率相等,均为 0.15. 因为在实验统计 SRAM 单元的出错率时发现最大值也是 0.12,因此提出 0.15 是较保守的^[1];
- (3) 允许的最大译码出错率(纠错失败率/FRR)设为 10⁻⁶^[1].

在文献[2]中,作者已经提出了大量的仅用一种码类进行纠错所得到的各种码参数,其中结果最为理想的是缩短的 BCH[1020, 43, 439]*,其需要的 SRAM 单元数为 4 080,因此问题是能不能找到更好的编码方案使得需要的 SRAM 单元数小于 4 080. 早在 1966 年,Forney 就在文献[3]中提出简单短码的级联方案,所以本文提出基于 BCH、一阶 RM 码、格雷码和重复码的其中两种码的级联,给出了各种级联码参数下的误码率 P_{total} (下文中的 P_1) 和提取 128 位密钥所需的 SRAM 单元数.

2 SRAM-PUF 对纠错的要求

同一 SRAM 相同环境下不同次数读出数据存

在一定的误差,不同环境下的读出的数据也存在误差. 这里选择的 ECC 编码应该能够满足各种情况下的数据纠错的需要,同时考虑处理器的运算能力,编码的纠错能力不应过强. 因此,应该选择一种合适的纠错编码来作为使用的算法. 一般纠错能力强的,其译码复杂度高,硬件开销大,比如 BCH 码. 纠错码的选择主要是在纠错能力和硬件开销两者之间折中. 在密钥提取系统中,要保证纠错失败率小于 10⁻⁶. 对于 SRAM 上电初始值来说,假定其出现错误的位置是随机的,出现错误的概率为 p ,那么,在 n 位 SRAM 上电初始值中发生 i 位错误的概率就是: $p_i = C_n^i p^i (1-p)^{n-i}$.

设 t 为所选纠错码的纠错容限,那么只有当同片 SRAM 上电初始值实际发生错误不大于 t 时,纠错码才能成功纠正发生的错误,恢复出 SRAM 识别码 ID,故能成功纠错的概率可表示为

$$p_{success} = \sum_0^t p_i = \sum_0^t C_n^i p^i (1-p)^{n-i}.$$

根据本设计所要求的纠错失败率,则 $P_{success} \geq 0.999\ 999$.

3 重复码、二进制格雷码、一阶 RM 码、和 BCH 码的特点

(1) 重复码

重复编码是一种简单的信道编码方法,其实质就是将每个要发送的符号重复发送,或者说是将原来的每一个信源符号编成多个相同的码元符号,其值与原来的符号取值相同. 比如(3, 1)二元重复码,其编码方法就是将原来二进制序列中的每一个“0”编成“000”,将每一个“1”编成“111”. 其特点是:译码简单,但是编码效率低,若将每个比特重复 n 次,则构成一个码长为 n 信息为长度为 1 的 $(n, 1)$ 重复码,其编码效率码只有 $1/n$.

(2) 二进制格雷码

二元格雷码是一类特殊的线性分组码, Golay 码是线性(23, 12)码,最小码距为 7,是能纠 3 位错误的完备码. 将其增加一个全校验位扩展为二元线性(24, 12)码,最小码距为 8,可以检测到 4 位错误、纠正 3 位错误. 其编译码是基于查找表 LUT.

(3) 一阶 RM 码

RM(r, m),其中 r 为阶数,则码字长度为 2^m ,最小码距 $d = 2^{m-r}$,信息长度 $k = \sum_{i=0}^r \binom{m}{i}$ 一阶形式下为 RM($2^m, m+1, 2^{m-1}$),其一般用大数逻辑实现译码.

(4) BCH(n, k, t)

BCH 码是一类纠错能力较强的循环码^[4],且其纠错能力可控,即在码字长度 n 一定的条件下,根据纠错数 t 的不同,信息位 k 跟着变化(n 一定, t 越大, k 越小). 由于是循环码的子类,所以编码可以用循环码通用的线性反馈移位寄存器 LFSR 实现,其最新的译码方法是 BM 迭代算法,译码相对较复杂些.

4 级联码特点以及适用于 SRAM-PUF 的级联方案

级联码的主要思想是:首先用一个很简单的码 C_2 来降低一部分错误,然后用第二种较强码 C_1 来纠正剩下的错误. 如果给定两种纠错码 C_1 和 C_2 ,码参数分别是 (n_1, k_1, d_1) 和 (n_2, k_2, d_2) ,则级联码 $C_c(n_c, k_c, d_c)$ 中 $n_c = n_1 n_2, k_c = k_1 k_2, d_c = d_1 d_2$,这样非常长的码字就拆分成两个更短的码字. 对于纠错失败率的计算,也要分成两步,首先计算 C_2 码译码之后的错误率,得到 P_2 ,再利用 P_2 计算 C_1 码译码后的出错率,即最终的译码错误率 P_1 ,可以将 P_2, P_1 表示为

$$P_2 = 1 - \sum_{i=0}^{t_2} \binom{n_2}{i} p^i (1 - p)^{n_2-i},$$
$$P_1 = 1 - \sum_{i=0}^{t_1} \binom{n_1}{i} p_2^i (1 - p_2)^{n_1-i}.$$

通过实验 Matlab 仿真得到如表 1 所示的各种级联码参数.

表 1 为提取 171 位密钥源泉的级联编码方案

$C_2(n_2, k_2, d_2)$	$C_1(n_1, k_1, d_1)$	P_1	Source bits for 171 bits
Rep[3,1,3]	BCH[127, 29,43]	8.48×10^{-6}	2 247
	RM[64,7, 32]	1.02×10^{-6}	4 691
	BCH[63, 7,31]	8.13×10^{-6}	4 617
Rep[5,1,5]	RM[32,6,16]	1.49×10^{-6}	4 560
	BCH[226, 86,43] *	2.28×10^{-6}	2 247
Rep[7,1,7]	$G_{23}[23, 12,7]$	1.58×10^{-6}	2 295
	$G_{23}[20, 9,7] *$	8.89×10^{-6}	2 660
	BCH[255, 171,23]	8.00×10^{-6}	1 785
	RM[16, 5,8]	3.47×10^{-6}	3 831
Rep[9,1,9]	BCH[113,57, 19] *	1.34×10^{-6}	2 373
	$G_{23}[23,12,7]$	8.00×10^{-6}	2 950
	RM[16, 5,8]	1.70×10^{-6}	4 925
Rep[11,1,11]	$G_{24}[24,13,7]$	5.41×10^{-6}	3 473
	$G_{23}[23,12,7]$	4.52×10^{-6}	3 606

内码 C_2 为重复码,分别重复 3、7、9、11 次,外码

C_1 有 BCH 码、格雷码和一阶 RM 码,

表中最后一栏是重构 171 位信息位所需的 SRAM 单元数(bits),在级联码构造下,它的计算方式^[5]是:

$$\frac{171}{k_1} * n_1 * n_2.$$

5 结束语

本文介绍的级联码是为了解决单独的 BCH 码硬件开销大和单独的简单线性分组码编码效率低(重复码)或纠错能力过小(格雷码)的缺陷而提出的. 结果表明两点,可以不用 BCH 码同时满足以上两方面的要求;综合两方面,最理想的级联方案是重复码 Rep[5,1,5]和缩短的 BCH[226, 86,43]* 级联.

参考文献:

[1]

Jorge Guajardo, Sandeep S Kumar, Pim Tuyls. FPGA intrinsic PUFs and their use for IP protection[C] // Cryptographic Hardware and Embedded Systems CHES 2007. Netherlands, Eindhoven, Springer, 2007 (4727):76-77.

[2]

Biosch C. Efficient fuzzy extractors for reconfigurable hardware. Master’s thesis, chair for system security [R]. Ruhr-University at Bochum,Department of Electrical Engineering and Information Science, 2008 .

[3]

Forney Jrt G D. Concatenated codes[M]. Cambridge, Massachusets, MIT Press,1966,37.

[4]

林舒. 差错控制编码[M]. 2 版. 北京:机械工业出版社,2007.

[5]

Vincent van der Leest. Soft decision error correction for compact memory-based PUFs using a single enrollment, intrinsic-ID[C] // CAES 2012. The Netherlands, Eindhoven,2012.

作者简介:

冯志华 男,(1979-),博士. 研究方向为软硬件协同设计技术、智能信息处理.

张 苗(通讯作者) 女,(1992-),硕士研究生. 研究方向为超大规模集成电路. E-mail:985177857@qq.com.

邹雪城 男,(1962-),教授,博士生导师. 研究方向为超大规模集成电路.

刘政林 男,(1968-),教授,博士生导师. 研究方向为超大规模集成电路.