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

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

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.