计算机工程 2011, 37(24) 103-105 DOI: 10.3969/j.issn.1000-3428.2011.24.034 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于生物密钥系统的能量攻击分析

姚剑波 [1]，**张 涛** [2]

(1. 遵义师范学院计算机科学系，贵州 遵义 563002；2. 中国电子科技集团公司第三十研究所卫士通公司，成都 610041)

摘要： 为评估生物密钥系统在侧信道攻击下的安全性能，在分析生物密钥系统结构和特点的基础上，将用户的击键生物特征和秘密共享方案相结合，设计一个基于击键的安全生物密钥系统，并通过差分能量攻击技术测量安全生物密钥系统的功耗泄漏。仿真分析表明，攻击者借助少量的功耗泄露就可以破解生物密钥系统的信息。

关键词： 生物密钥系统 侧信道攻击 差分能量攻击 功耗泄漏

Power Attack Analysis Based on Biometric Cryptosystem

YAO Jian-bo [1], ZHANG Tao [2]

(1. Department of Computer Science, Zunyi Normal College, Zunyi 563002, China; 2. Westone Corporation of No.30 Research Institute, China Electronics Technology Group Corporation, Chengdu 610041, China)

Abstract: To assess the biometric cryptosystem performance in possible side-channel attacks, on the basis of analysis of the biometric cryptosystem structure and characteristics, a secure biometric cryptosystem based on the keystroke is designed by the combination of the user's keystroke biological characteristics and secret sharing scheme. Power consumption leakage of the safe biometric cryptosystem is measured with the Differential Power Attack(DPA). Simulation analysis shows the biometric cryptosystem can be extracted with bits of power leakages.

Keywords: biometric cryptosystem side-channel attack Differential Power Attack(DPA) power consumption leakage

收稿日期 2011-06-21 **修回日期** **网络版发布日期** 2011-12-20

DOI: 10.3969/j.issn.1000-3428.2011.24.034

基金项目:

贵州省科学技术基金资助项目(黔科合J字2009(2275))

通讯作者:

作者简介: 姚剑波(1965－)，男，博士、CCF高级会员，主研方向：信息安全；张 涛，博士

通讯作者E-mail: yaojianbo007@gmail.com

参考文献：

[1] Jain A K, Ross A, Pankanti S. Biometrics: A Tool for Information Security[J].IEEE Transactions on Information Forensics and Security.2006, 1(2):125-143

[3] 杜之波, 陈 运, 吴 震, 等. 防范边信道攻击的逆伪操作实现算法[J].计算机工程.2010, 36(3):131-133 浏览

本刊中的类似文章

1. 常小龙, 丁国良, 武翠霞, 王创伟.抗电磁侧信道攻击的AES S盒设计[J]. 计算机工程, 2011,37(17): 93-95
2. 李宗秀;鲍皖苏;汪 翔.基于Brier-Joye的Elgamal 椭圆曲线密码体制研究[J]. 计算机工程, 2006,32(23):

扩展功能

本文信息

Supporting info

PDF(277KB)

[HTML] 下载

参考文献[PDF]

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

引用本文

Email Alert

文章反馈

浏览反馈信息

本文关键词相关文章

生物密钥系统

侧信道攻击

差分能量攻击

功耗泄漏

本文作者相关文章

姚剑波

张涛

PubMed

Article by Tao, J. B.

Article by Zhang, C.

153-155,
3. 杜育松;王大星;沈 静.一种对AES-128的差分错误分析原理[J]. 计算机工程, 2006,32(23): 174-176

文章评论

反馈人		邮箱地址	
反馈标题		验证码	2740