计算机工程 2011, 37(24) 136-137 DOI: 10.3969/j.issn.1000-3428.2011.24.045 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于COS的Hash接口设计与实现

郑 斌，李 峥，王瑞蛟

(信息工程大学电子技术学院，郑州 450004)

摘要： 基于片上操作系统(COS)的Hash函数可扩展性较差。针对该问题，提出一种可重构的Hash接口方法。该方法引入面向对象的概念，由Hash算法接口与Hash算法设置接口2个部分组成，利用存储在EEPROM中的Hash算法设置接口对Hash算法接口进行实例化，使之具备密码服务功能。验证结果表明，该方法具有较强拓展性，能够达到预期设计目标。

关键词： Hash算法 可重构 密码服务 算法接口

Design and Implementation of Hash Interface Based on COS

ZHENG Bin, LI Zheng, WANG Rui-jiao

(Electronic Technology Institute, Information Engineering University, Zhengzhou 450004, China)

Abstract: To solve the problem of the Hash algorithm expansibility based on the Chip Operating System(COS), a flexible Hash interface is designed. The interface which takes the object-oriented thought is made up by Hash algorithm interface and Hash algorithm setting interface. The Hash algorithm interface is set by the Hash algorithm setting interface, which is stored in the EEPROM, to be an instance and has the capability to provide the cryptographic service. The results of experiment show that Hash interface has good expansibility to add other algorithms, and get the purpose to design it.

Keywords: Hash algorithm reconfigurable cryptographic service algorithm interface

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.1000-3428.2011.24.045

基金项目:

国家自然科学基金资助项目(61072047)；现代通信国家重点实验室基金资助项目(9140C1106021006)；郑州市创新型科技人才队伍建设工程基金资助项目(096SYJH21099)

通讯作者:

作者简介: 郑 斌(1985－)，男，硕士，主研方向：密码学，软件工程；李 峥，副教授、博士；王瑞蛟，硕士

通讯作者E-mail: countsinbad@163.com

参考文献：

[1] ISO/IEC. 7816-4-1996 Identification Cards Integrated Circuit(s) Cards with Contacts Part4: Interindustry Commands for Inter- change[S]. 1996.

[2] ISO/IEC. 7816-8-1999 Identification Cards Integrated Circuit(s) Cards with Contacts

Part8: Security Related Interindustry Com- mands[S]. 1999.

[5] 史肖燕, 熊 璋, 蒲菊华. 智能卡操作系统-BHCOS的设计和实现[J].计算机工程.2003, 29(2):207-209

[6] 金晨辉, 郑浩然, 张少武, 等. 密码学[M]. 北京: 高等教育出版社, 2009.

本刊中的类似文章

1. 叶晓敏, 王侃文, 陈佳临, 周学功, 王伶俐.优化的可重构多常数乘法器生成算法[J]. 计算机工程, 2012,38(3): 228-233
2. 刘杰, 吴强, 赵全伟.面向可重构计算系统的模块映射算法[J]. 计算机工程, 2012,38(3): 276-279,283
3. 谭一匡, 邝继顺, 凌纯清, 周颖波, 尤志强.基于改进ESLA算法的可重构资源管理[J]. 计算机工程, 2012,38(04): 221-223
4. 刘沙, 周学功, 王颖, 王伶俐.可重构系统在线任务预约重调度算法[J]. 计算机工程, 2011,37(8): 271-274
5. 许新达, 徐成, 刘彦, 李仁发.基于可重构系统的亚可抢占任务调度算法[J]. 计算机工程, 2011,37(6): 239-241
6. 褚有睿, 王志远, 欧阳旦.基于可重构密码模块的VPN安全网关[J]. 计算机工程, 2011,37(5): 152-154
7. 宋庆增, 顾军华.稀疏矩阵向量乘的FPGA设计与实现[J]. 计算机工程, 2011,37(23): 214-216
8. 杨敏, 吴艳霞, 顾国昌, 孙延腾.面向可重构编译技术的RAM访问优化算法[J]. 计算机工程, 2011,37(2): 284-285
9. 聂彧, 刘亮, 叶凡, 任俊彦.基于信道分析的动态可重构MIMO检测器[J]. 计算机工程, 2011,37(18): 243-245
10. 王福焕, 曾国荪.基于随机Petri网的可重构核心单元分析[J]. 计算机工程, 2011,37(17): 1-6

文章评论

反馈人		邮箱地址	
反馈标题		验证码	6475