吉林大学学报(理学版) 2012, 50(02) 305-308 DOI: ISSN: 0412-1961 CN: 21-1139/TG

计算机科学

基于可编程逻辑器件的单向壳核函数构造方法

李蕴奇

吉林省经济信息中心, 长春 130061

摘要:

针对构造公钥密码时出现函数单向性和陷门性矛盾的问题, 通过引入单向壳核函数新型公钥密码体制, 根据可编程逻辑器件PLD的设计思想和结构
特征, 给出一种单向壳核函数的构造方法, 其安全性等同于一次一密. 与传统公钥密码体制相比, 单向壳核函数具有更广的包容性和更高的安全性, 是一种灵活性更强的公钥密码体制.

关键词: 公钥密码; 单向壳核函数; 可编程逻辑器件

Construction Method of One Way Shell Core Function Based on Programmable Logic Device

LI Yun qi

Center of Economic and Information in Jilin Province, Changchun 130061, China

Abstract:

In view of the contradiction between one way and trapdoor occured on constructing public key cryptography , the author introduced a new type of public key cryptography that is one way shell core function. According to the designing ideas and structural characteristics of programmable logic device (PLD), the paper presents a scheme of one way shell core function and shows that its security is equal to that of one time pad. Compared with the traditional public key cryptography, one way shell core function has the characteristics of wider inclusivity, more change and higher security. The function provides people with a public key cryptography of more flexibility.

Keywords: public key cryptography; one way shell core function; programmable logic device

收稿日期 2011-03-19 修回日期 网络版发布日期

DOI:

基金项目:

通讯作者: 李蕴奇

作者简介:

作者Email: li__yunqi@sina.com

参考文献:

本刊中的类似文章

文章评论

反馈人		邮箱地址	
反馈标题		验证码	7391