第一图书网, tushu007.com

<<演化密码引论>>

图书基本信息

书名：<<演化密码引论>>

13位ISBN编号：9787307083981

10位ISBN编号：7307083981

出版时间：2010-12

出版时间：武汉大学出版社

作者：张焕国，覃中平　等著

页数：383

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

<<演化密码引论>>

内容概要

密码是信息安全的核心技术。
掌握现代密码技术是世界大国奋力竞争的制高点之一。
发展我国独立自主的密码科学技术，创新是关键。
《演化密码引论(精)》集中介绍了张焕国和覃中平教授的研究小组十年来在演化密码方面的研究成果。
本书的出版将会推进演化密码理论与技术的交流，促进演化密码的深入研究。

<<演化密码引论>>

书籍目录

前言
第1章 信息安全概论
1. 1 信息安全是信息时代永恒的需求
1. 2 信息安全的内涵
1. 3 信息安全的主要研究方向和研究内容
1. 4 信息安全的理论基础
1. 5 信息安全的方法论基础
1. 6 密码是信息安全的关键技术
参考文献
第2章 智能计算概论
2. 1 演化计算与密码问题求解
2. 2 遗传算法
2. 3 模拟退火算法
2. 4 蚁群算法
参考文献
第3章 密码学基础
3. 1 密码体制
3. 2 密码分析
3. 3 完善保密
参考文献
第4章 演化密码基础
4. 1 演化密码的概念
4. 2 演化密码体制的安全性
4. 3 小结
参考文献
第5章 演化DES类密码体制
5. 1 DES的s盒的演化设计
5. 2 演化DES密码体制
5. 3 演化DES密码芯片
5. 4 小结
参考文献
第6章 密码函数的演化设计与分析
6. 1 布尔函数的演化设计与分析
6. 2 Bent函数的演化设计与分析
6. 3 Hash函数的演化设计与分析
6. 4 小结
参考文献
第7章 S盒的设计自动化
7. 1 基于多项式表示的S盒演化设计
7. 2 基于MM类Bent函数的完全非线性s盒的设计
7. 3 基于正形置换的S盒演化设计
7. 4 小结
参考文献
第8章 P置换的设计和生成
8. 1 P置换的构成

8．2 线性正形置换和广义线性正形置换
8．3 有限域上的轮换矩阵
8．4 小结
参考文献
第9章 密码的演化分析
9．1 DES密码的演化分析
9．2 序列密码的演化分析
9．3 小结
参考文献
第10章 椭圆曲线的演化产生
10．1 概述
10．2 Koblitz安全椭圆曲线的演化产生
10．3 大素数域安全椭圆曲线的演化产生
10．4 小结
参考文献
第11章 安全协议的演化设计
11．1 协议的演化设计
11．2 认证协议的演化设计
11．3 非否认协议的演化设计
11．4 小结
参考文献
第12章 演化密码软件系统
12．1 系统结构与功能
12．2 系统功能
12．3 系统介绍
附录1 演化设计的2组(16个)DES的S盒
附录2 演化设计的108个DES的P置换

章节摘录

遗传算法最早在1965年由美国Michigan大学的J.H.Holland教授在其专著《自然系统和人工系统中的自适应》（Adaption in Natural and Artificial Systems）中提出。
遗传算法是模拟生物在自然环境中的遗传和进化过程而形成的一种自适应全局优化概率搜索算法，它把问题的参数用基因表示，把问题的解用染色体表示（二进制码基因编码表示），算法存在一个代表问题潜在解集的种群，从而得到一个由具有不同染色体的个体组成的种群。
该种群由经过基因编码的染色体个体组成。
每个个体携带不同的染色体，染色体作为遗传物质的主要载体表现为某种基因组合，决定了个体性状的外部表现。
这个种群在问题特定的环境里生存竞争，适者有最好的机会生存和产生后代。
后代随机地继承了父代的最好特征，并也在生存环境的控制支配下继续这一过程。
在初代种群产生之后，按照适者生存和优胜劣汰的原理，使用选择算子、交叉算子和变异算子这三种基本遗传操作，演化产生出代表新的解集的种群。
种群像自然进化一样，后代种群的染色体都将逐渐适应环境，不断演化，最后逐代演化收敛到一族最适应环境的个体，即得到问题的最优解。
从数学角度看，遗传算法是一种随机搜索算法；从工程角度看，它是一种自适应的迭代寻优过程。
构成简单遗传算法的要素主要有：染色体编码、个体适应度评价、遗传算子以及遗传参数设置等。
目前的遗传算法已不再局限于二进制编码，将不同的编码策略（即不同的数据结构）与遗传算法的结合称为演化规划EP（Evolution Program）。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com