<<完全映射及其密码学应用>>

图书基本信息

书名：<<完全映射及其密码学应用>>

13位ISBN编号：9787312021169

10位ISBN编号：7312021166

出版时间：2008-12

出版时间：中国科学技术大学出版社

作者：吕述望　等著

页数：267

<<完全映射及其密码学应用>>

内容概要

本书对完全映射相关理论进行了系统的总结，在此基础上，进一步介绍了两类完全映射：正形置换与全向置换，书中给出了主要面向密码算法设计的几种正形置换发生器的研究结果，为完全映射在密码学中的具体应用做好了准备。

为阐述完全映射理论在密码算法设计中的应用，本书进一步给出了sP网络密码算法、Fleistel网络密码算法的线性与差分安全性分析技术，并介绍了上述两种算法与正形置换之间的关系。

在上述工作的基础上，本书进一步介绍了P逻辑密码算法，并给出了其线性与差分安全性分析技术，从而使正形置换理论得到了比较系统的应用。

本书是专著《序列密码的设计与分析》(北京中软电子出版社，2003年1月)的姊妹篇。

本书可供信息安全、密码设计与分析等相关领域的研究和工作人员使用、参考。

<<完全映射及其密码学应用>>

书籍目录

章节摘录

第1章　引论　　随着计算机网络和通信技术的迅速发展与普及，信息安全在现代信息社会中占据着越来越重要的地位。
信息安全已经成为国家安全、经济发展和社会稳定的重要保障和基本组成部分。
然而，要构建安全的信息系统，必须使用密码技术，密码技术是安全信息系统的核心。
密码技术主要由密码设计技术和密码分析技术两个分支组成。
密码设计和密码分析都必须以一定的数学理论为基础，这在现代密码的设计与分析中表现尤为突出。
由密码设计和密码分析的相互作用而逐渐发展和完善起来的密码设计理论具有极其丰富的内涵，其中密码函数的选取标准和设计技术是密码设计理论中讨论尤为广泛和持久的一类课题，它构成了密码设计理论的重要组成部分。
设计一个密码并不难，难的是如何分析清楚密码抗分析的复杂度。
一个好的密码算法需要以构建好的密码函数为基础，密码体制或密码组件的设计是密码设计理论研究的基本内容。
在这些基本内容的研究中，密码学安全性分析总是建立在各个密码组件的安全性分析基础之上的，因此，基本密码学映射或置换的研究对于构建好的密码算法具有重要意义。
本章将从密码函数与置换、密码学对置换的需求等几个方面来讨论密码学中的有关置换理论。

<<完全映射及其密码学应用>>

版权说明