<<有限自动机及在密码学中的应用>>

图书基本信息

书名：<<有限自动机及在密码学中的应用>>

13位ISBN编号：9787302175308

10位ISBN编号：7302175306

出版时间：2008-9

出版时间：清华大学出版社 Springer-Verlag出版社

作者：陶仁骥

页数：406

内容概要

本书主要研究有限自动机的可逆性理论及其在密码学上的应用。
此外，也讨论自治有限自动机和拉丁阵，它们与有限自动机单钥密码的标准形有关。
有限自动机是被认为是密码的自然模型。
本书作者提出并发展了RaRb风变换方法，用它彻底解决了有限域上（拟）线性有限自动机的结构问题。
与经典的线性系统“传输函数方法”不同，RaRb变换方法可推广到非线性有限自动机；大量弱可逆有限自动机及其弱逆可用它产生，这就导致基于有限自动机的公开钥密码（简记为FAPKC）的提出。
本书可用作计算机科学和数学专业高年级和研究生课程的参考书。

作者简介

陶仁骥，工作于中国科学院软件研究所，中国密码学界学术带头人。
1985年，基于有限自动机可逆性领域的工作，陶仁骥先生和陈世华先生开创性地提出了FAPKC，有限自动机公开钥密码体系。
该体系是目前世界上不多的投入实际使用的公钥密码体系之一。
该体系在国际上被称作Tao-Chen体制，在经典教科书《应用密码学》中有所介绍。

<<有限自动机及在密码学中的应用>>

书籍目录