

<<伪随机序列的设计及其密码学应用>>

图书基本信息

书名：<<伪随机序列的设计及其密码学应用>>

13位ISBN编号：9787561541890

10位ISBN编号：7561541899

出版时间：2011-12

出版时间：厦门大学出版社

作者：陈智雄

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>

## <<伪随机序列的设计及其密码学应用>>

### 内容概要

序列密码的安全性完全依赖于密钥序列的随机性，构造具有密码学特殊性质的序列是序列密码的关键技术。

《伪随机序列的设计及其密码学应用》主要介绍椭圆曲线序列生成器、有限域上逆函数序列生成器、费马商数序列生成器、模 $pq$ 的广义割圆序列生成器等构造，并采用数论中的指数理论和有限域理论讨论相应序列的分布性质、相关值性质、线性复杂度性质等密码学指标。

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>