<<数论及其相关领域>>

图书基本信息

书名：<<数论及其相关领域>>

13位ISBN编号：9787040367751

10位ISBN编号：7040367750

出版时间：2013-3

出版时间：欧阳毅、 等 高等教育出版社 (2013-03出版)

作者：欧阳毅 编

<<数论及其相关领域>>

内容概要

《数论及其相关领域(英文)》内容定位于冯克勤教授作出重要成就及感兴趣的领域，分为两个方面：一方面是数论，包括二次丢番图方程的同余性、代数整数环的K群、整体函数域的L-函数、自守形式以及p-adic表示等，另一方面是这些理论在设计、编码等领域的应用，反映了冯克勤教授在数论及其应用领域的发展所作的贡献和影响。

<<数论及其相关领域>>

书籍目录

章节摘录

版权页： 插图： 6Conclusion We propose the study of a new family of word-oriented LFSR,s with High Efficiency: σ-LFSRs, which might be interesting in the design of modern stream ciphers.By the theory of matrix and polynomial over finite fields, we explore the cryptographic properties of σ-LFSR.s such as minimal polynomial, state graph,coordinate sequences, and several properties of primitive σ-LFSRs etc.We also discuss some principles for choosing σ-LFSR,s suitable for software implementation,and then we offer an algorithm to search for primitive cr-LFSRs and obtain many primitive σ-LFSR.s such as HHZ-1 or HH2-2, etc, which only use few memory and basic instructions.At last, we give two applications in cryptography: constructing RNGs and stream ciphers. These studies implicate that σ-LFSRs may be used as building block in many cryptographic schemes.We believe that as the performance, security and resource consumption be increasingly important, σ-LFSRs will become an important and attractive alternative to traditional bit and byte oriented designs.However, there remain many open problems for future work.Nevertheless we hope that the results and ideas in this paper serve as an initial step in establishing a continuing research on the design of fast and secure word-oriented LFSRs for cryptographic purpose. Acknowledgement.The work is supported by a grant from the National Natural Science Foundation of China （No.61003291）, National Basic Research Program of China （No.2007CB807902）, and Foundation for the Author of National Excellent Doctoral Dissertation of China （No.FANEDD-2007874）.

<<数论及其相关领域>>

编辑推荐

《数论及其相关领域(英文)》不仅是数论及其应用领域专家们有价值的参考书，也是研究生开展研究时极好的入门书。

<<数论及其相关领域>>