<<安全协议的建模与分析>>

图书基本信息

书名：<<安全协议的建模与分析>>

13位ISBN编号：9787111157212

10位ISBN编号：7111157214

出版时间：2005-1

出版时间：机械工业出版社

作者：[英] Peter Rya

页数：235

字数：381000

<<安全协议的建模与分析>>

内容概要

本书主要介绍了安全协议的一种建模与分析方法：CSP（Communica-ting Sequential Processes，通信顺序进程）方法。
本书共有11章和3个附录，主要内容包括：安全协议概述、CSP方法介绍、安全协议的CSP建模方法、协议目标描述、FDR概述、Casper介绍、为FDR进行协议和入侵者编码、分析结果的定理证明、协议的简化转换、其他的安全协议分析方法以及安全协议分析所存在的问题与发展趋势。
附录包括：密码学背景知识、具体实例及第8章的详细证明过程。
　本书可作为高等院校信息安全、计算机、通信等专业的教学参考书，也可供从事相关专业的教学、科研和工程技术人员参考。

<<安全协议的建模与分析>>

书籍目录

<<安全协议的建模与分析>>

版权说明