<<中国密码学发展报告2009>>

图书基本信息

书名：<<中国密码学发展报告2009>>

13位ISBN编号：9787121112379

10位ISBN编号：712111237X

出版时间：2010-8

出版时间：电子工业出版社

作者：中国密码学会 编

页数：380

前言

经过大家的努力，第三期《中国密码学发展报告》终于要与读者见面了。
2009年恰逢美国数学家C. Shannon发表现代密码学中具有里程碑意义的论文“保密系统的通信理论”60周年，所以这期编辑的中国密码学发展报告也可以算做对Shannon工作的纪念。

1949年，Shannon在他的文章中用信息论的观点对信息保密问题作了全新的诠释，他以概率统计为工具对消息源、密钥源及接收、截获的密文作了严格的数学描述和分析，用不确定性和唯一解距离给出了密码的安全性度量，并且证明了通信系统达到理想的完善保密性的条件。

Shannon理论的意义在于，不仅仅是得到了一些具体的密码设计理论、方法和安全准则，更重要的是第一次将密码学的研究置于严格的数学理论之上。
同时，Shannon论文中涉及的概率统计、信息论、伪随机序列、计算复杂度、布尔逻辑、代数系统，等等，这些也成为研究现代密码理论的重要手段。

现代密码学在形成之初，就与数学有着千丝万缕的密切联系。
本期报告的主题就是“数学密码学”，我们邀请有关专家就相关问题进行了系统深入的探讨，共收集的12篇论文，从不同的角度展现给读者密码学与相关数学分支的内在联系，读者可以了解到密码学与数学“水乳交融”的共存、共生的过程。
不只是数学为密码学奠定了可靠的逻辑基础、提供了有效的研究工具，同时，密码学的发展也丰富了数学理论的内容，为数学家提出了许多有挑战性的课题。

<<中国密码学发展报告2009>>

内容概要

《中国密码学发展报告2009》是中国密码学会成立以来的第三期《中国密码学发展报告》。本期报告的主题是“数学密码学”，我们邀请了有关专家就相关问题进行了系统深入的探讨，共收集12篇论文，从不同的角度展现给读者密码学与相关数学分支的内在联系，读者可以了解到密码学与数学“水乳交融”的共存、共生的过程：不只是数学为密码学奠定了可靠的逻辑基础、提供了有效的研究工具；同时，密码学的发展也丰富了数学理论的内容，为数学家提出了许多有挑战性的课题。内容包括：信息论与密码学、序列与密码学、布尔函数与密码学、组合数学与密码学、代数数论在编码和密码学中的应用、RSA密码体制的安全性分析综述、国内超椭圆曲线密码体制的研究、概率统计与密码学、基于复杂性理论的密码学若干问题探讨、符号计算与密码学、编码理论与密码学、非线性系统与密码学。

《中国密码学发展报告2009》可供国内从事密码学和信息安全领域工作的研究人员参考。对掌握密码学最新进展和最新发展动态具有重要的参考价值。

作者简介

中国密码学会是由从事密码学术研究的知名专家、学者和部分大专院校、科研院所共同发起成立的非营利性社会团体组织。
旨在凝聚密码学术人才，开展密码学术理论研究，提供密码学术交流平台。

学会开展多种形式的国内外密码学术交流活动，出版、发行密码学术刊物，举办相关培训班，积极促进密码技术的应用与发展。

<<中国密码学发展报告2009>>

书籍目录

章节摘录

有两种刻画并发不可锻造性的定义方法： 方法1：简单地说，我们说一个密码协议是并发不可锻造安全的，如果证明者部分的并发交互并没有给予并发中间人敌手任何实质性的利益，以使得其在验证者部分证明一个定理但却不知道该定理的证据或者该定理本身就是错误的。
这可以简单地形式化为：对于任意一个多项式时间的并发中间人敌手A，存在另外一个多项式时间的算法S，满足A通过并发中间人攻击所有能得到的信息都实质上可以由S单独模拟出来。
并且，对所有A在验证者部分成功证明的定理，S也输出相应的证据。
方法2：在并发中间人环境中，虽然我们不知道这个恶意敌手具体使用什么样的策略以获得他的利益，但是有两个极端的策略被认为是无害的或者是无法避免的。
第一种极端策略是传递（relaying）策略：使用这种策略，恶意敌手只是在诚实证明者与诚实验证者之间如实地传递信息。
也就是说，使用这种极端策略的敌手对于协议的诚实参与者而言是透明的。
另外一种极端策略是阻塞（blocking）策略：使用这种极端策略，恶意敌手在证明者部分的并发交互与恶意敌手在验证者部分的并发交互是完全独立的。
很显然，使用这两种极端策略的中间人攻击不会给恶意敌手带来任何利益，因此被认为是无害的。
同时，由于对于并发不可锻造安全性而言，所有的通信信道被假设为没有任何的认证（authentication）机制，因此使用以上两种极端策略的中间人攻击也是无法避免的。
直观地说，我们说一个密码协议是并发不可锻造的，如果恶意中间人使用任何潜在恶意策略所能得到的利益都可以使用上述两种无害的极端策略得到。
在并发中间人攻击中，如果所有在证明者部分由诚实证明者证明的定理事先确定（即并发中间人不可以作任何修改），这种假设下的并发不可锻造安全性称为静态并发不可锻造安全性；若在证明者部分由诚实证明者证明的定理可以由并发中间人来设定，但是必须在每一次协议执行（即会话session）之前设定，这种假设下的并发不可锻造安全性称为部分并发不可锻造安全性；若对并发中间人在设定证明者部分的定理上没有任何限制（特别地，并发中间人可以在每一个会话的任何时间点上设定该会话所需证明的定理），则这种最强的并发不可锻造安全性称为动态不可锻造安全性。

<<中国密码学发展报告2009>>

版权说明