<<中国密码学发展报告2010>>

图书基本信息

书名：<<中国密码学发展报告2010>>

13位ISBN编号：9787121140402

10位ISBN编号：7121140403

出版时间：2011-9

出版时间：电子工业出版社

作者：中国密码学会 编

页数：237

<<中国密码学发展报告2010>>

内容概要

本书从密码学的最新进展出发，以探索的眼光审视密码学最新、最活跃的研究方向。
在密码学深度发展的同时，新的应用和新的思想激发了密码学的新方向。
本书主要抗量子密码体制的研究现状、视觉密码学研究进展、零知识证明理论研究进展、生物特征密码学研究进展、DNA密码研究综述、轻量级分组密码研究进展、同态密码学研究进展、安全多方计算、密码算法征集评估及标准化发展概况等。

<<中国密码学发展报告2010>>

书籍目录

章节摘录

零知识协议是一个两方协议，它有两个参与方，即证明者和验证者。
参与方之间一般进行成员归属命题的证明或者知识证明。
零知识协议首先是一个证明（论据）系统，即该系统要满足完备性和可靠性。
完备性是指，对于属于语言集合的输入实例，任意的诚实证明者都能够以1的概率使得验证者相信该实例属于该语言集合。
可靠性是指，对于不属于语言集合的输入实例，即使恶意的证明者也不能以不可忽略的概率使得验证者相信该实例属于语言集合。
另外，零知识协议还需要满足零知识性，即恶意的验证者只知道输入实例确实属于语言集合与否，却获取不到其他的一切有用信息。
零知识性的形式化刻画，是要求对于任意的有效验证者，其和诚实证明者交互过程中的一切观察，存在一个期望概率多项式时间模拟器，其不和证明者进行通信，仍能模拟出同样的观察。
隐藏在定义中的思想是，验证者在和证明者交互过程中学习到的任何信息，它都可以自己产生（即运行模拟器）。
……

编辑推荐

《抗量子密码体制的研究现状》重点介绍了：基于Hash函数的数字签名、基于纠错码的公钥密码体制、基于格的密码体制，以及多变量公钥密码体制等抗量子密码体制，并指出了一系列值得研究的公开问题。

《视觉密码学研究进展》详细介绍了视觉密码的原理机制、评价标准，并讨论了当今流行的几种构造方案及各个热点的研究进展。

《零知识证明理论研究进展〉从零知识协议的可合成性、可重置性、并发零知识、精确零知识，以及非交互零知识等方面对零知识证明的最新研究进展进行了介绍。

《生物特征密码学研究进展》介绍了生物特征加密中的一些主流技术及其应用，并对该技术的未来发展进行了展望。

《DNA密码研究综述》介绍了DNA：计算的基本原理及DNA密码的基本概念，界定了DNA密码和生物特征密码的区别。

《轻量级分组密码研究进展》介绍了轻量级分组密码的研究进展，并重点介绍了自主设计的“鲁班锁”轻量级分组密码算法。

《同态密码学研究进展》讲述了全同态加密方案在云计算等新环境中的应用是传统密码方案无法比拟的特性。

《安全多方计算》述了安全多方计算的基本理论及研究进展。

《密码算法征集评估及标准化发展概况》概括地介绍了国际上开展的系列密码算法征集活动。

<<中国密码学发展报告2010>>

版权说明