<<中国密码学发展报告2011>>

图书基本信息

书名：<<中国密码学发展报告2011>>

13位ISBN编号：9787121179495

10位ISBN编号：7121179490

出版时间：2012-9

出版时间：电子工业出版社

作者：中国密码学会 编

页数：283

字数：400000

前言

《中国密码学发展报告2011》终于可以与读者见面了。
自2007年开始组织编写“密码学发展报告”，通过介绍国际密码学界最新发展动态，宣传推广国内学者在密码学各个方面的研究成果，促进了密码学研究、应用的交流，取得了较好的社会影响。
在已经出版的几期报告中，分别从不同的角度对密码学及其相关信息安全领域的研究现状、研究进展、应用情况等做了较为全面的分析和介绍，这就为后续的发展报告打下很好的基础。
我们希望不断推出题材新颖、内容丰富的“密码学发展报告”，奉献给读者。
在过去的几年中，计算机网络技术又有了新的发展。
物联网、云计算无疑是非常时髦且充满诱惑的概念，这些网络新技术和新的网络服务模式，对网络和信息安全会造成哪些影响？
而这些新技术的挑战又会给密码学研究带来什么样的变化？
本期报告围绕“密码学新动向”展开，我们特别邀请了几位专家对最近几年密码研究领域一些新的研究热点问题进行分析讨论，希望能够引起读者的共鸣并带来有意义的思考。
本期报告共包括9篇特邀文章。
华南师范大学马昌社、暨南大学翁健合写的文章通过介绍2010年“三大密码会”发表的论文，可以让我们看到国际密码学研究前沿的一些基本动向。
首先，在抗泄露的密码方案构造技术以及格上加密方案的构造技术等方面取得了突破性的进展；以云计算为代表的新的网络应用模式对密码学研究产生了很大推动，比如同态加密的发展、属性加密的改进等。
其次，尽管格上密码有了长足的发展，但是密钥规模过大和密文扩张过多限制了它的应用。
因此，如何设计规避这两个问题的新型算法将是未来格上密码需要攻克的主要问题，同时格上的数字签名方案有待进一步的研究。
最后，传统意义上的知识证明协议、多方计算协议等在可应用性方面仍需要在效率方面有所提高。
2012年2月，由于发现RSA算法在实际应用中大量存在共模数现象，一时间人们关注的焦点又回到了RSA。
这仅仅是使用RSA算法时随机生成参数的不慎，还是RSA这个被认为最好的公钥算法存在某些内在的短板？
中国科学院DCS中心吕克伟的文章，系统讨论了相关的RSA/Rabin函数的明文比特安全性。
近几年的研究已经对RSA函数的单个比特安全性有了定论，但所得到的结论更多的是理论上的意义，缺少实际可应用性。
因此，如何构造出更具实用性的方法，是一个值得探讨的问题。
另外，关于明文比特块的同时安全性则需要进一步讨论，特别是，能够得到的最大同时安全的比特块是多大？
这方面的任何进展将对于构造高效的伪随机生成器产生影响。
随着网络多媒体的广泛应用，如何解决条件接收、数字产品的版权保护是迫切需要解决的问题。基于公钥的广播加密技术为网络多媒体应用安全提供了一条有效的解决思路。
西安电子科技大学胡予濮等人的文章介绍了公钥广播加密的研究背景、进展及设计要求和特点；给出了几种代表性的方案。
与对称广播加密相比，基于公钥的广播加密还有很多问题亟待解决。
但无论如何，广播加密都是一个值得投入和深入研究的密码学分支。
广播加密在解决网络多媒体应用安全方面可以发挥作用，但是在现实中有一个问题始终困扰着人们：不论是对称广播加密还是基于公钥的广播加密，其密码运算和工作环境并不安全，通过侧信道攻击甚至通过监测内存，加密算法和加密密钥都可能被攻击者获得。
为此，一个新的解决方案“白盒密码”应运而生，即一种变形的密码算法，即使攻击者可能监测密码系统的内部运行，并完全掌控执行环境，仍可以保证安全。

上海交通大学来学嘉的文章，就给出关于白盒密码比较全面的介绍，包括白盒密码的基本思想，对白盒密码的攻击模型和应用背景等，总结了白盒密码常用的设计方法，并通过几个白盒密码算法实现为例，说明目前的白盒密码算法在效率和安全性上仍然存在不足。

白盒密码本质上是一种对现有密码算法的修正技术，使其在执行过程中能够抗泄露攻击。

华东师范大学李祥学、郁昱等人的文章，则从安全模型、可证明安全的角度讨论如何保证密码算法抗泄露的问题。

传统意义上的密码可证明安全性主要针对只能看到输入输出的攻击者，忽略了算法硬件显示时出现的物理信息泄露，这导致了很多理论上“牢不可破”的密码学算法在现实中被轻易破解。

抗泄露密码学就是要在理论层面设计对抗旁路攻击的可证明安全的密码学算法。

从加密与签名的综合效率角度考虑，一次逻辑执行就完成加密和签密两种密码学操作的签密方案无疑在通信中优势明显，因此签密体制在应用中是不错的选择。

保密通信重点实验室和成都电子科技大学的祝世雄、李发根等人的文章介绍了签密方案的研究背景，分析了经典的签密方案、签密的安全性模型、签密的不可否认性质、混合签密、基于身份的签密、无证签密以及签密的应用等，并提出一些未来值得研究的工作。

在现实社会中，人们经常需要将自己的签名权委托给他人，让他人代替自己行使签名权力。

随着信息化社会各种网络应用模式的多样化，也同样需要通过代理人行使加密和签名操作。

代理多签名是代理签名的一种特殊形式，是多个原始签名人将自己的签名权限委托给某个代理签名人并让其代理这些原始签名人行使签名权力的行为。

南京航空航天大学王箭等人的文章，针对代理多签名方案及其困难问题，分别介绍了基于离散对数、基于椭圆曲线、基于双线性对以及基于身份的代理多签名方案。

涉及到密码系统安全，我们总是假定密码使用者会看管好自己的密钥而不丢失。

但在实际应用中，特别是移动终端用户，丢失密码设备造成密钥泄露的情况几乎难以避免。

对于多数密码体制，一旦密钥泄露似乎还可以选择更换密钥；而一些新型密码体制，如基于身份的密码，由于公钥与用户身份信息绑定，根本不能接受更换密钥。

因此，必须有一种针对密钥泄露的解决方案，使因为密钥泄露而造成的风险降到最低。

青岛大学于佳等人的文章讨论了通过密钥演化技术来降低密钥泄露危害的机制，如周期性地更新密钥，包括前向安全、密钥隔离、入侵容忍等手段，同时还指出了一些值得研究的问题。

传统意义上的密码学，主要涉及数学和计算等理论。

虽然对量子密码、量子计算的研究早已展开，但是早期很少有人相信物理学的理论最终可能撼动并影响业已成熟的现代密码学。

这一切自从Shor给出了基于量子计算的整数分解多项式算法而改变。

南京航空航天大学袁家斌等人的文章讨论了量子计算的原理以及相关量子算法，分析了量子计算模型在速度上超越图灵机模型的原因。

对于大多数读者来说，通过本文可以对量子计算和量子算法有一个初步的了解。

本研究发展报告得到了国家自然科学基金项目（61133014和60970111）资助，同时也得到了保密通信重点实验室和上海市可扩展计算与系统重点实验室的支持，在此一并表示感谢。

最后，还要对中国密码学会学术工作委员会的同事王鲲鹏博士、毕宁策划编辑等表示感谢，他们为本期研究报告的组稿、联络、编辑和出版等付出了大量辛苦的工作。

中国密码学会学术工作委员会主任　　陈克非　　2012年4月

<<中国密码学发展报告2011>>

内容概要

中国密码学会组编的《中国密码学发展报告(2011)》是第五期的《中国密码学发展报告》，全书共9篇文章，对最近几年密码研究领域一些新的研究热点问题进行分析讨论。
包括2010年“三大密码会”的评述，以及RsA
共模问题、广播加密、白盒密码、签密和代理签名、密钥演化、量子计算等方面的研究进展，希望能够引起读者的共鸣并带来有意义的思考。

《中国密码学发展报告(2011)》可供国内从事密码学和信息安全领域的研究人员参考，对了解和掌握密码学最新发展动态有参考价值。

<<中国密码学发展报告2011>>

书籍目录

<<中国密码学发展报告2011>>

版权说明