

<<中国密码学发展报告2008>>

图书基本信息

书名：<<中国密码学发展报告2008>>

13位ISBN编号：9787121090516

10位ISBN编号：7121090511

出版时间：2009-8

出版时间：电子工业出版社

作者：中国密码学会 编

页数：360

字数：450000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<中国密码学发展报告2008>>

内容概要

本书是中国密码学会成立以来的第二期《中国密码学发展报告》。

本发展报告侧重于应用密码学和密码学应用两方面的内容，共收录论文11篇。

内容包括：基于身份的密码体制的研究综述、数字签名技术、密码协议的可证明安全性、安全协议的形式化分析方法及其发展现状、密码体系中的密钥管理方案概述、密码与网络安全处理系统的芯片实现研究、侧信道攻击理论与技术、无线移动通信安全技术、多媒体安全、数字水印及其中版权和内容保护应用中的进展、可信计算技术研究进展。

本书可供国内从事密码学和信息安全领域的研究人员参考。

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。

<<中国密码学发展报告2008>>

书籍目录

基于身份的密码体制的研究综述 数字签名技术 密码协议的可证明安全性 安全协议的形式化分析方法及其发展现状 密码体系中的密钥管理方案概述 密码与网络安全处理系统的芯片实现研究 侧信道攻击理论与技术 无线移动通信安全技术 多媒体安全 数字水印及其在版权和内容保护应用中的进展 可信计算技术研究进展

章节摘录

基于身份的密码体制的研究综述 1.引言 1976年,美国密码学家Diffie和Hellman提出了公钥密码体制的思想,这是密码学上一个重要的里程碑。

公钥密码体制不仅具有加密的功能,同时还有认证的功能。

在公钥体制架构下,用户Alice无论是向另一个用户Bob传送加密信息,还是在收到用户Bob发来的某个签名.消息对后验证签名,都需要使用Bob的公钥来完成。

在此,很关键的一点是用户Alice必须对用户Bob的公钥进行认证,即确认他所使用的公钥的确是用户Bob的公钥。

在传统的公钥体制架构下,公钥与私钥对的产生是符合一定规则的,并不是任何信息都可以用作公钥和私钥信息的,其形式是一些看起来随机的数字信息,与用户的身份没有任何联系。

在使用某个用户的公钥进行加密或验证签名时,一定要确认所使用的公钥的确属于那个宣称拥有它的用户。

这需要一个可信赖的第三方CA (certificate Authority), 又称证书机构,向系统中的各个用户发行公钥证书。

公钥证书上CA的签名可把用户的身份和他的公钥紧密地联系起来。

在这种架构下,CA机构是一个重要部门,负责用户公钥证书生命周期的每一个环节:生成、签发、存储、维护、更新、撤销等。

我们把这种需要证书的密码体制称为基于证书的公钥密码体制 (Pied)。

.....

<<中国密码学发展报告2008>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>