

<<CPK公钥体制与标识鉴别>>

图书基本信息

书名：<<CPK公钥体制与标识鉴别>>

13位ISBN编号：9787115231925

10位ISBN编号：7115231923

出版时间：2013-4

出版时间：南湘浩 人民邮电出版社 (2013-04出版)

作者：南湘浩

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>

<<CPK公钥体制与标识鉴别>>

内容概要

《CPK公钥体制与标识鉴别——自主管理技术基础》公布了CPK最新版本v7.0。CPK(v7.0)建立在线性复杂度理论的基础上，解决规模化标识鉴别和抗量子计算攻击的难题。《CPK公钥体制与标识鉴别——自主管理技术基础》将鉴别逻辑从相信逻辑、信任逻辑提升到真值逻辑，讨论了在接入鉴别、代码鉴别、交易鉴别、物流鉴别等领域，标识鉴别和实体鉴别的应用，也讨论了信息系统与非信息系统互通的新一代信息安全概念和未来绿色网络的发展方向。

<<CPK公钥体制与标识鉴别>>

书籍目录

目 录第一篇 鉴别技术第1章 几个概念1.1 物理世界和网际世界 41.2 无序世界和有序世界	
51.3 它证系统和自证系统 61.4 证明链和信任链 71.5 集中式管理和分散式管理 81.6 物理特征与逻辑特征 9第2章 鉴别逻辑2.1 鉴别逻辑的发展 132.2 相信逻辑 142.2.1 建立模型	
142.2.2 形式化证明 152.2.3 相信逻辑特点 152.3 信任逻辑 152.3.1 直接级信任 152.3.2 推理级信任 162.3.3 公理级信任 162.3.4 基于行为的信任 172.4 真值逻辑 182.4.1 真值逻辑要点 182.4.2 真值逻辑内容 192.4.3 真值逻辑特点 202.5 鉴别协议 202.5.1 国际标准签名协议	
202.5.2 国际标准鉴别协议 202.5.3 CPK鉴别协议 212.6 鉴别系统 232.6.1 PKI认证系统 232.6.2 CPK鉴别系统 24第3章 标识鉴别3.1 网际安全的兴起 273.2 网际安全的内容 273.3 通信标识鉴别 283.4 软件标识鉴别 303.5 交易标识鉴别 313.6 标签标识鉴别 323.7 标识鉴别与网络秩序 333.8 标识鉴别与整体方案 34第二篇 密码体制第4章 CPK组合公钥(v6.0)4.1 引言 384.2 映射序列 384.3 密钥的计算 394.3.1 标识密钥的计算 394.3.2 分割密钥的计算 394.3.3 通用密钥的计算 404.3.4 地区密钥的计算 404.4 数字签名和密钥传递 404.4.1 数字签名 404.4.2 密钥传递 414.5 安全性 41第5章 标识鉴别体制5.1 标识鉴别 445.1.1 CPK标识鉴别 445.1.2 IBC标识鉴别 455.1.3 PKI标识鉴别 455.1.4 mRSA标识鉴别 475.1.5 IB-RSA标识鉴别 475.2 密钥交换体制 495.2.1 IBE密钥传递 495.2.2 CPK密钥传递 495.2.3 PKI密钥交换 505.2.4 mRSA密钥交换 515.2.5 性能比较 515.3 信任根的讨论 52第6章 字节加密6.1 编码结构 546.1.1 置换表disk 546.1.2 代替表subst 556.1.3 密钥结构 556.2 作业流程 576.2.1 给定条件 576.2.2 密钥派生 576.2.3 数据展开 576.2.4 数据和密钥的结合 576.2.5 左向累加 576.2.6 置换变换 586.2.7 右向累加 586.2.8 数据集中 586.2.9 单代变换 586.2.10 数据与密钥再次结合 586.3 安全性考虑 59第三篇 CPK系统第7章 密钥管理7.1 鉴别网络 647.2 密钥分类 647.2.1 通信密钥 647.2.2 分级密钥 657.3 密钥分发 657.3.1 证书体 667.3.2 变量体 667.4 密钥交换 677.4.1 CPK一对一密钥交换 677.4.2 CPK一对多密钥交换 677.4.3 ElGamal密钥交换 687.5 数据加密 687.6 密钥保护 697.6.1 口令验证 697.6.2 口令更换 69第8章 ID card管理8.1 密钥管理机构 728.2 注册部 728.3 生产部 738.4 发行部 75第9章 CPK Chip设计9.1 背景技术 779.2 主要技术 779.3 Chip结构 789.4 Chip的功能 829.4.1 签名功能 829.4.2 加密功能 83第四篇 代码鉴别第10章 软件代码鉴别10.1 技术背景 8810.2 工作原理 8910.3 代码鉴别流程 9010.3.1 签名模块(SM) 9010.3.2 验证模块(VM) 9110.4 代码鉴别的特点 93第11章 WINDOWS代码鉴别11.1 概述 9511.2 PE文件 9511.3 微过滤驱动 9611.3.1 NT I/O子系统 9611.3.2 文件过滤驱动 9611.3.3 微过滤驱动 9811.4 Windows代码鉴别的实现 9811.4.1 系统架构 9811.4.2 特征值提取 99第12章 Linux代码鉴别12.1 概述 10112.2 ELF文件 10112.3 Linux安全模块(LSM)框架 10212.4 Linux代码鉴别的实现 103第五篇 接入鉴别第13章 手机接入鉴别13.1 基本技术 10813.2 连接过程 10913.3 加密过程 11013.4 脱密过程 111第14章 套接层接入鉴别14.1 信息网络通信层 11314.2 安全套接层(SSL) 11414.3 可信套接层(TSL) 11614.4 TSL基本技术 11714.5 TSL工作流程 11814.6 SSL和TSL比较 120第15章 路由器接入鉴别15.1 路由器工作原理 12315.2 可信连接的要求 12415.3 基本技术 12515.4 始发地址鉴别 12615.5 加密功能 12815.5.1 加密过程 12915.5.2 脱密过程 12915.6 分组头格式要求 12915.7 可信计算环境 13015.7.1 软件代码的证明 13015.7.2 软件代码的鉴别 13015.7.3 结论 131第六篇 交易鉴别第16章 电子票据鉴别16.1 基本技术 13616.2 票据的申请 13716.3 票据的流通 13816.4 票据的验证 139第17章 电子取款鉴别17.1 背景技术 14217.2 柜面网络 14317.3 主要环节 14317.4 基本技术 14417.5 柜员机鉴别流程 14517.5.1 ATM机上的作业 14517.5.2 ATM和门户通信 14617.6 电子银行的优点 147第七篇 物流鉴别第18章 防伪鉴别18.1 背景技术 15218.2 工作原理 15218.3 实施例(一) 15418.4 实施例(二) 155第19章 Mywallet设计(v1.0)19.1 两种鉴别思路 15819.2 系统配置 15919.3 TAG结构1 6019.3.1 数据区结构 16019.3.2 控制区结构 16119.4 TAG数据生成与鉴别 16219.4.1 KMC 16219.4.2 Enterprise 16219.4.3 Writer和Reader 16219.5 协议设计 163第八篇 存储文件鉴别第20章 文件安全管理20.1	

<<CPK公钥体制与标识鉴别>>

安全要求 17020.2 基本技术 17120.3 文件上传协议 17220.4 文件下传协议 17320.5 存储数据的加密 17420.5.1 密钥文件的建立 17420.5.2 密钥文件的存储 17420.5.3 文献库加密 17520.5.4 关系库加密 175第21章 文件保险箱21.1 背景 17921.2 系统架构 17921.3 系统特点 18021.4 系统实现 181第22章 密级印章22.1 技术背景 18522.2 主要技术 18522.3 作业流程 18722.4 具体实施 18822.5 标记解释 189第九篇 移动文件鉴别第23章 电子邮件鉴别23.1 基本技术 19823.2 发送过程 19923.3 接收过程 20123.4 回执过程 202第24章 数字版权鉴别24.1 技术背景 20424.2 工作原理 20424.3 厂家的版权 20524.4 企业的运营权 20724.5 客户的使用权 208第十篇 网络连接鉴别第25章 内联网网哨25.1 技术背景 21425.2 主要技术 21425.3 内联网网哨 21625.3.1 网哨的配置 21625.3.2 网哨的工作流程 21625.4 个人网哨 21825.5 安全策略 218第26章 网络地址鉴别26.1 引言 22126.2 技术路线 22126.2.1 地址真实性证明 22226.2.2 路由协议和报头格式 22326.2.3 可信计算环境 22326.3 功能样机 224第十一篇 最新进展第27章 抗穷举攻击27.1 穷举能力 22827.2 基本看法 22927.3 主要目标 22927.4 技术路线 23027.5 功能实现 231第28章 CPK组合公钥(v7.0)引言 23328.1 标识密钥 23328.2 分割密钥 23528.3 合成密钥 23528.4 公网与专网密钥 23628.5 CPK数字签名协议 23628.6 CPK密钥传递协议 23728.7 安全性 23828.7.1 系统密钥的安全 23828.7.2 个人密钥的安全 238第29章 CPK私钥分发协议第30章 Mywallet设计(v2.0)30.1 技术要求 24430.1.1 两种鉴别关系 24430.1.2 两种鉴别网络 24530.2 系统结构 24630.2.1 密钥配置 24630.2.2 数据区结构TAG结构 24730.2.3 控制器结构 24830.3 协议设计 24930.3.1 鉴别协议 24930.3.2 脱密与验证协议 24930.3.3 加密与签名协议 250附录 253后记 283参考文献 287索引 289

<<CPK公钥体制与标识鉴别>>

编辑推荐

第一次解决标识鉴别的课题，这一直是世界性的难题，比如通信中防止非法接入问题，就要靠标识认证才能解决，由于还没有标识认证技术，一直没能得到解决。

因此，不可能有类似的文章。

作者为我国著名的密码学专家，完成了CPK芯片开发，使其达到实用化要求，民生银行利用这一系统对电子票据签章，效果良好。

作者还将此项技术延伸到移动通信领域，开发出可包括用于3G系统等高端安全认证手机，实现保密通信要求。

<<CPK公钥体制与标识鉴别>>

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>