CPK密码体制与网际安全

CPK-Crypotosystem and Cyber Security

南湘浩 著

国防工业出版社
National Defense Industry Press

CPK密码体制与网际安全

CPK-Cryptosystem and Cyber Security

[illegible] 著

CPK 密码体制与网际安全

CPK Cryptosystem and Cyber Security

南湘浩　著

国防工业出版社

·北京·

图书在版编目(CIP)数据

CPK 体制与网际安全/南湘浩著. —北京:国防工业出版社,2008.12

ISBN 978-7-118-05939-7

Ⅰ.C... Ⅱ.南... Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2008)第 136550 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号　邮政编码 100048)

国防工业出版社印刷厂印刷

新华书店经售

*

开本 850×1168　1/32　**印张** 7⅞　**字数** 200 千字

2008 年 12 月第 1 版第 1 次印刷　**印数** 1—4000 册　**定价** 35.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)68428422　　发行邮购:(010)68414474

发行传真:(010)68411535　　发行业务:(010)68472764

前　言

2005 年美国总统信息技术顾问委员会(PITAC)提交的一篇《网际安全—优先项目危机》的报告,标志着网际(网络世界或社会)安全新时代的到来。如果说网络安全的主要任务是以堵漏洞、打补丁为主的被动防护的话,那么网际安全的主要任务则是以建立可信系统为主的主动管理。主动管理的核心内容是建立证明系统,将信息安全建立在证明系统的基础之上,这就是所谓的可信系统(trusting system)。这是一项新的任务,过去由于没有合适的示证系统和验证系统,信息安全的原则只能采用“出于好意”,或者采用主体可信的前提假设之上,而网际安全则不同,它建立在“互相怀疑”的基础之上,不允许前提假设下的证明或验证。

这种主要任务和基本原则的变化,首先影响安全的基础理论。过去以“出于好意”的所有安全协议和标准,需要以“互相怀疑”的基点上重新考虑,如:通信协议和标准、可信计算(包括代码认证)协议和标准等,不得不引起革命性的变化。

今年欧洲密码年会上,James Hughes (2004 年国际密码年会执行主席)和北京大学博士研究生关志向大会介绍了基于标识的组合公钥(CPK: Combned Public Key)体制,与会权威专家肯定了 CPK 体制是新型基于标识的体制。基于标识的体制,代表着现代密码体制发展的新趋势,受到全世界密码界的关注。CPK 体制和标识认证系统得到了我国高层领导的高度重视,也得到了国家保密局、国家知识产权局等有关部门的大力支持。国务院信息办和安标委已将 CPK 体制作为国家标准的基础项目,正式纳入标准化研究计划,国家工业和信息化部给予了企业发展基金补助。SUN 公司已决定,将 CPK 体制作为 Solaris 操作系统的一部分。在广东

省科技厅和信息产业厅的支持下成立了广东南方信息安全研究院,并由南方信息安全产业基地公司和 SUN 公司签订了战略合作意向,共同推动 CPK 的国际标准。在北京市科委的支持下,成立了北京易恒信公司,开发了相关产品,在中国民生银行票据认证系统中得到应用。

CPK 体制的研究一直在进行,不断得到新的进展。CPK 密码体制在私钥之间存在的线性相关性一直是重点攻关的课题。2007 年初,James Hughes 等国内外专家又提出能否实现签名私钥由个人生成,保护个人隐私的问题。在集中式管理的模式下,这似乎是不好解决的难题。周仲义、陈华平、裴定一、吕述望、翟起滨、袁文恭、司常玉、吕海民、陈钟、陆浪如、李益发等研究员或教授,唐文、关志、陈瑞川、郭文嘉、陈宇、田文春、李维刚等博士或研究生先后参与了本课题研究。最后,由陈华平研究员正式提出和形成了标识密钥和随机密钥复合的双因子组合公钥(TF - CPK)的思路,解决了私钥可以由个人定义的难题,并消除了私钥间的线性关系。

又一个重要进展是在标识认证基础上建立了可信逻辑的理论,将传统的相信逻辑提高到可信逻辑。基于标识认证的可信逻辑,不同于传统的基于数据认证的相信逻辑。可信逻辑由主体认证、客体认证、行为认证构成,能够做到“事前验证”,即事件发生之前验证,进而有效防止非法事件的发生;而传统的相信逻辑只做到客体认证,做不到“事前认证”,只能是事件发生后才能认证,因而很难防止非法事件的发生。规模化鉴别技术是建立可信世界的核心技术。CPK 体制正好能够解决这个国际性难题。可信系统的关键问题是怎样证明实体的真实性,即鉴别技术。在鉴别技术中遇到的难题有二:一是认证的规模性,二是认证的直接性。规模性要求不是万级,而是万亿级,直接性要求不能依赖外部而要自身当场验证。

本书系统介绍了可信系统主要领域的解决方案,这些领域包括过去无法解决的很多课题,现在却变得容易解决了,如:通信的非法接入、非法软件的运行、印章鉴别系统等。通过应用举例,读

者可以发现由于解决了标识认证这一核心课题，使过去无法解决的很多难题都容易得到解决。因此，“标识认证”是网际安全的“纲”，起到“纲举目张”的作用。

CPK 密码体制、标识认证、可信逻辑作为可信系统的基础理论和技术，越来越显现其意义。在酝酿成立国际 CPK 行业联盟，推进国际标准之际，本书的出版具有特殊意义。希望本书满足国内外读者的要求，对国际联盟和国际标准有所帮助，并以此促进信息安全从网络安全到网际安全的过渡。

著 者

2008 年 7 月 11 日

目　录

第 1 章　基本概念 …… 1
1.1　物理世界和网际世界 …… 1
1.2　无序世界和有序世界 …… 2
1.3　有证书系统和无证书系统 …… 3
1.4　基于标识的证明和基于第三方的证明 …… 4
1.5　证明链和信任链 …… 5
1.6　集中式管理和分散式管理 …… 6
1.7　手写签名和数字签名 …… 7
1.8　生物特征和逻辑特征 …… 9
第 2 章　鉴别逻辑 …… 11
2.1　信任关系 …… 11
2.2　相信逻辑 …… 13
2.3　标识认证 …… 14
2.4　可信逻辑 …… 21
第 3 章　组合公钥(CPK) …… 23
3.1　ECC 密钥复合定理 …… 23
3.2　标识密钥 …… 24
3.3　密钥复合 …… 25
3.4　数字签名 …… 26
3.5　密钥交换 …… 26
3.6　安全性分析 …… 27
第 4 章　体制的探讨 …… 29
4.1　体制的需求 …… 29
4.2　体制的发展 …… 30

4.3 数字签名机制 …… 31
4.4 密钥交换机制 …… 34
4.5 信任根的讨论 …… 35
第5章 系统设计 …… 38
5.1 认证网络 …… 38
5.2 证书定义 …… 39
5.3 数字签名协议 …… 41
5.4 密钥交换协议 …… 42
5.5 口令协议 …… 43
5.6 数据加密协议 …… 44
5.7 签名格式协议 …… 45
5.8 证书生成协议 …… 46
5.9 证书使用协议 …… 47
第6章 证书管理 …… 49
6.1 密钥管理机构 …… 49
6.2 行政管理 …… 53
第7章 CPK芯片 …… 55
7.1 技术背景 …… 55
7.2 主要技术 …… 55
7.3 具体实施方式 …… 57
第8章 ID证书 …… 68
8.1 技术背景 …… 68
8.2 主要技术 …… 68
8.3 具体实施方式 …… 70
第9章 电子邮件认证 …… 76
9.1 电子邮件的证书 …… 76
9.2 电子邮件作业过程 …… 77
第10章 手机通信认证 …… 81
10.1 手机证书 …… 81
10.2 手机认证通信 …… 82

第 11 章　电子银行认证 …… 87
11.1　技术背景 …… 87
11.2　主要技术 …… 88
11.3　具体实施方式 …… 91
第 12 章　电子票据认证 …… 100
12.1　票据的申请 …… 100
12.2　票据的流通 …… 100
第 13 章　通信标签认证 …… 104
13.1　技术背景 …… 104
13.2　主要技术 …… 107
13.3　具体实施方式 …… 109
第 14 章　出入网关认证 …… 115
14.1　技术背景 …… 115
14.2　主要技术 …… 115
14.3　具体实施方式 …… 117
第 15 章　软件代码认证 …… 121
15.1　技术背景 …… 121
15.2　主要内容 …… 122
15.3　具体实施方式 …… 123
第 16 章　电子标签认证 …… 127
16.1　背景技术 …… 127
16.2　主要技术 …… 127
16.3　实施方式 …… 130
第 17 章　电子印章认证 …… 136
17.1　技术背景 …… 136
17.2　主要技术 …… 136
17.3　实施方式 …… 138
第 18 章　数字版权认证 …… 150
18.1　技术背景 …… 150
18.2　主要技术 …… 150

18.3 实施方式 …… 153
附件1:走出神秘的“黑屋” …… 158
附件2:标识认证打开信息安全新天地 …… 163
附件3:CPK Cryptosystem …… 170
附件4:我国解决世界难题的“电子身份证”引起国际关注 … 174
附件5:CPK体制走向国际 …… 179
附件6:关于CPK若干问题的说明 …… 183
附件7:寻找安全“银弹” …… 192
附件8:基于CPK体制的标识认证 …… 201
附件9:WebIBC:Identity Based Cryptography for Client Side Security in Web Applications …… 210
参考文献 …… 231
后记:浅谈信息安全发展新动向 …… 233

Contents

1 Basic Concepts 1
1.1 Physical World and cyber World 1
1.2 Ordered World and Disordered World 2
1.3 System with or without Certificate 3
1.4 Identity-Based and Third Party-Based Certification 4
1.5 Certificate Chain and Trust Chain 5
1.6 Centralized and Decentralized Management 6
1.7 Written Signature and Digital Signature 7
1.8 Physical Feature and Logical Feature 9
2 Authentication Logic 11
2.1 About Trust 11
2.2 Belief Logic 13
2.3 Identity Authentication 14
2.4 Trust Logic 21
3 CPK Cryptosystem 23
3.1 Compound Theorem 23
3.2 Identity-key 24
3.3 Compound Key 25
3.4 Digital Signature Scheme 26
3.5 Key Exchange Scheme 26
3.6 Security 27
4 Discussions on Crypto-system 29
4.1 Requirenments for Crypoto-system 29

4.2 The History of System Development 30
4.3 Digital Signature Systems 31
4.4 Key Exchage Systems 34
4.5 Discussion on Trust Root 35
5 System Design 38
5.1 Key Configuration 38
5.2 Definition of Certificate 39
5.3 Authentication Protocols 41
5.4 Key Exchange Protocols 42
5.5 Password Protocols 43
5.6 Data Encryption Protocols 44
5.7 Transmition Protocols 45
5.8 Certificate Generation Protocols 46
5.9 Operation Protocals 47
6 Certificate Management 49
6.1 Key management Center 49
6.2 Administration 53
7 CPK Chip Design 55
7.1 Background Technique 55
7.2 Main Contents 55
7.3 Implementation 57
8 ID-Certificate 68
8.1 Background Technique 68
8.2 Main Contents 68
8.3 Implementation 70
9 e-Mail Authentication 76
9.1 Certificate for e-Mail 76
9.2 Procedure of Authentication 77
10 Cell-phone Authentication 81
10.1 Certificate for Cell-phone 81

10.2 Procedure of Authentication 82
11 e-Banking Authentication 87
11.1 Background Technique 87
11.2 Main Contents 88
11.3 Implementation 91
12 e-Cheque Authentication 100
12.1 Application for e-Cheque 100
12.2 Circulation of e-Cheque 100
13 Communition Tag Authentication 104
13.1 Background Technique 104
13.2 Main Contents 107
13.3 Implementation 109
14 Gateway Authentication 115
14.1 Background Technique 115
14.2 Main Contents 115
14.3 Implementation 117
15 Software Tag Authentication 121
15.1 Background Technique 121
15.2 Main Contents 122
15.3 Implementation 123
16 RFID Tag Authentication 127
16.1 Background Technique 127
16.2 Main Contents 127
16.3 Implementation 130
17 e-Seal Authentication 136
17.1 Background Technique 136
17.2 Main Contents 136
17.3 Implementation 138
18 Digital Right Authentication 150
18.1 Background Technique 150

18.2 Main Contents 150
18.3 Implementation 153
APPENDIX A Farewell to the Mysterjous "Black Chamber" 158
APPENDIX B Identity Authentication open up a new field for Information Security 163
APPENDIX C CPK-Crytosystem 170
APPENDIX D CPK-System is moving toward the World 174
APPENDIX E CPK-System is Moving toward the World 179
APPENDIX F Some Explanations on CPK 183
APPENDIX G Seeking for "Silver Bullet" of Trusing System 192
APPENDIX H Identity Authentication Based on CPK-System 201
APPENDIX I WebIBC: Identity Based Cryptography for Client Side Security in Web Applications 210
Reference 231
Summary New Concept of information Security 233

第1章 基本概念

在认证理论的研究中，首先需要澄清一些基本概念。随着互联网的发展，信息安全和网络安全得到了迅速发展，同时提出或产生了很多新的概念。在新概念形成过程中难免不完善、不全面。概念的不完善或不全面极容易引起误导。如果这种误导影响到国家的决策，则会导致战略性错误。因此，要把有争议的概念提出来，共同讨论、研究、澄清，以求共识。

1.1 物理世界和网际世界

网际世界是IT技术发展的产物，称Cyber。网际世界是新生事物，应该有它自己独特的发展规律，而只有把握了规律才能驾驭网际世界的发展。这个规律的研究则刚刚起步，展示了广阔的研究前景。

认证体系首先在物理世界中产生，已经历了漫长的发展过程，形成了一整套法律、制度、技术、运行的机制。网际世界是新近出现的新生事物，其认证体系的研究则刚刚起步。到目前为止，物理世界还是大世界，而网际世界是小世界，是物理世界的一小部分。然而网际世界在不断扩大，与物理世界越来越融为一体，构成更大空间的新的信息世界。

在认证体系中，物理世界和网际世界之间，有很多相似的地方，但也有很多不同的地方，因此在网络世界认证体系的研究中，首先重视物理世界的各种认证原理、认证方法、认证效果，同时着重研究网际世界与物理世界不同的特点。从一般道理来说，物理世界的认证要用物理方法解决，而网际世界的认证要用逻辑方法

解决，网际世界不可能完全模拟物理世界的认证体系。曾有人提出钞票的真伪用逻辑方法鉴别的想法。很显然钞票是物理的东西，不能用逻辑方法识别真伪。物理的特点是不容易复制，而逻辑的特点是容易复制，因此，在现实生活中，防伪工作都用物理方法来解决。

在物理世界中，政府发布了公告，盖了政府公章。加盖公章的目的首要是“声称”本公文确系本政府的，对公文享有权利和义务。转到网际世界上，政府发布了公告，加盖了公章（比如，政府的数字签名），能否起到物理章一样的作用呢？答案是肯定的。尽管物理章的重点是自己的“声称”，而逻辑章的重点是给对方提供不可否认性，但都同样可以达到对公文的负责性目的。因此可以说，在大部分情况下，逻辑章的应用可以模拟物理章的应用，但并不是形式上的模拟，而是本质上的模拟。

1.2 无序世界和有序世界

无论是物理世界或网络世界都分为无序世界和有序世界。有序世界则是有组织的世界、可组成从属关系和隶属关系的世界、有中心的世界，比如银行系统、国家机关等。无序世界是无组织的世界、不构成从属关系和隶属关系的世界、无中心的世界，例如，一个人到商店买东西的活动一般属于无序世界的活动，因为顾客和商店之间没有任何组织关系，不构成任何从属关系和隶属关系。又如任何一个人对任何一个人，一个人对任何企业，任何独立企业对任何企业，都属于无序世界的活动。

有序世界的认证体系很好建立，因为有序世界是有中心的世界、有边界的世界。这与安全的属性相一致：任何安全都是有它一定的作用域和有效域的。在有序世界中存在从属关系，已具有一般意义上的信任关系，即信任关系注册性和管辖性很容易满足，只证明一体性就建立信任关系。

在无序世界中建立认证体系比较困难，但可能有很多解决办