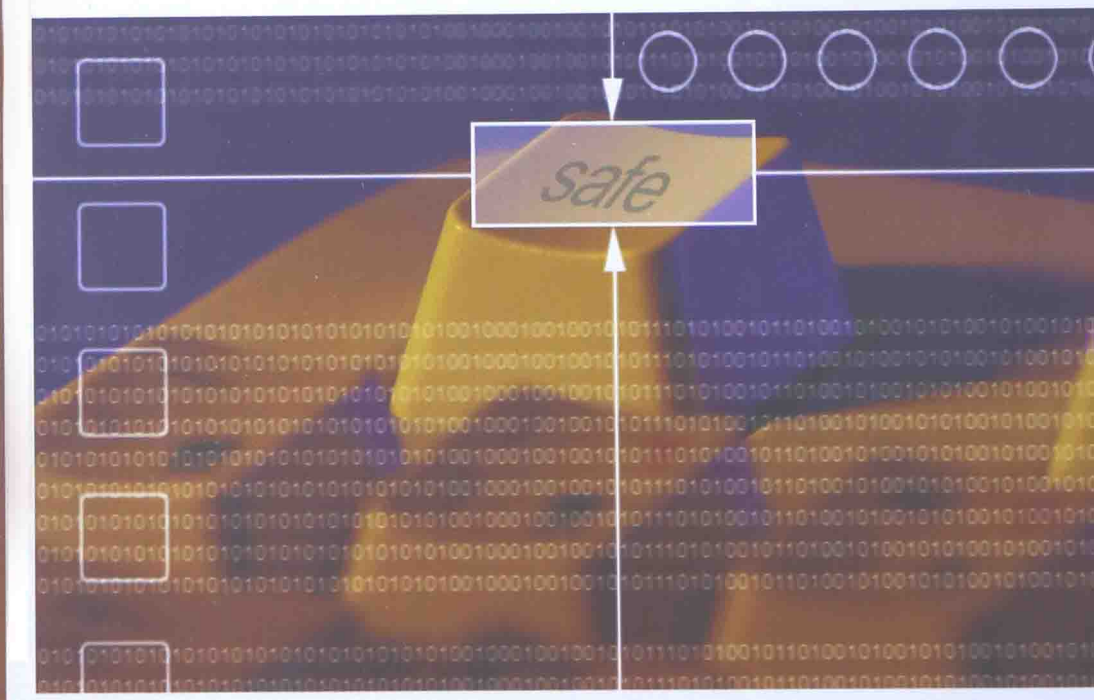
陈志德 黄欣沂 许力 著

身份认证安全协议
理论与应用



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

身份认证安全协议理论与应用

陈志德　黄欣沂　许力　著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书内容围绕近年来身份密码体制的研究热点和难点展开。本书分为基础篇、密码篇、签名篇、RFID篇、应用篇五部分，重点介绍和分析多身份及可变身份下的身份密码体制、具有等级结构的身份密码体制、在线/离线签名验证的加速机制、基于属性签名的自适应匿名认证、无线射频认证系统安全协议、基于身份密码体制的隐私匹配及其在自组织网络中的应用及无线 Mesh 网络对密钥建立方案。第一部分对身份密码安全协议的理论和技术发展进行综述；第二部分从多身份密码系统构造、可变身份签名构造、基于等级身份加密密钥共享方案等多个方面分析身份密码体制的设计；第三部分从在线/离线的可验证的签名方案、基于属性签名自适应匿名认证 SA^3 系统、基于属性签名的用户撤销等方面描述和分析了基于身份密码体制的签名机制；第四部分从轻量级 RFID 认证协议与可靠统计机制、SKRAP 安全认证协议、SECRAP 安全认证协议研究、ESAP 安全认证协议研究等多个方面阐述了基于身份密码的 RFID 安全机制；第五部分从基于身份加密的多方隐私匹配、基于身份加密的隐私匹配在自组织网络中的应用、无线 Mesh 网络中基于矩阵的对密钥建立方案等方面阐述和分析了身份加密安全协议在自组织网络和无线 Mesh 网络中的应用。

本书可供计算机网络与信息安全、通信与信息系统、电子与信息系统等研究人员、相关专业教师、研究生以及高年级本科生参考。

图书在版编目（CIP）数据

身份认证安全协议理论与应用 / 陈志德，黄欣沂，许力著. —北京：电子工业出版社，2015.1

ISBN 978-7-121-25124-5

Ⅰ. ①身… Ⅱ. ①陈… ②黄… ③许… Ⅲ. ①计算机网络—身份认证—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2014）第 294357 号

策划编辑：董亚峰
责任编辑：夏平飞　　特约编辑：郭茂威
印　　刷：北京天宇星印刷厂
装　　订：北京天宇星印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：17　字数：385 千字
版　　次：2015 年 1 月第 1 版
印　　次：2015 年 1 月第 1 次印刷
定　　价：46.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言

近年来，随着信息技术的发展，网络活动越来越受欢迎。网络信息和服务在给授权用户带来便利的同时，也使得非法用户有机可乘。在网络技术应用中，要抵制非法用户的入侵，首先必须正确地识别通信双方的身份。身份认证是一个实体确认通信的另一个实体满足它所声明的属性的过程，是验证实体真实性的过程。基于身份密码安全协议在电子医疗、云计算、车载网、物联网等领域具有广泛的应用。

本书是作者在福建师范大学网络安全与密码技术重点实验室工作期间与所指导的研究生合作成果的基础上，经整理、修改而成的。本书的主要目的就是紧随信息安全中的身份密码这一主题，对于多年来的研究成果进行归纳总结，希望对从事该领域研究的研究生、教师以及对该领域感兴趣的其他方面的专家学者起到一定的参考和引导作用。

本书的内容共分为 25 章。第 1 章，引言：分别介绍了身份认证的研究背景与现状，以及国内外的研究现状、隐私匹配的研究背景和现状、无线 Mesh 网络节点间密钥建立方案的研究背景和现状、无线射频认证（RFID）系统。第 2 章：基础知识，主要介绍了身份密码安全协议所需要的数学理论和一些密码学的基本工具。第 3 章：多身份加密构造，在传统的身份加密系统中，一个密钥仅能对应唯一的一个公钥，在本章所构造的多身份加密系统中，一个密钥可以对应于不同的公钥，这种特殊的身份加密系统有利于简化用户管理密钥。第 4 章，可变身份签名构造：在该方案中，公钥由一公开信息及 n 个隐私信息组成，且验证的公钥内容是可变化的，即在验证过程中验证者仅能获取一个隐私信息。第 5 章，基于等级身份加密的密钥共享方案：在传统的等级身份加密中，每一等级的主密钥由一个 KGC 管理，如果该 KGC 不可信任了，那么它将泄露一些密钥信息。第 6 章，基于等级身份加密的密钥门限方案：该方案提出了等级身份加密中一种有效的密钥管理机制，实现了密钥分发的门限方案。在该方案中，当进行运算的 KGC 数量达到门限值时才能进行有效的密钥计算，而且个别 KGC 的失效不会影响系统的正常运行。第 7 章，在线/离线身份加密：首先将 Guo 等人提出的在线/离线身份加密技术扩展到等级身份加密，然后提出了一个有效的在线/离线等级身份加密（HIBOOE）方案，实现该技术的目的在于提高在线加密的效率，它在计算能

力有限的设备中是非常有用的。第 8 章，在线/离线签名的批验证：提出一个非常高效的在线/离线签名方案能够实现 multi-signer 批验证，该方案是基于 CHP 方案并且在随机预言模型下证明了它的安全性。第 9 章，可分在线/离线签名方案：首先给出了可分在线/离线签名方案的一般构造方法，并且以 Boneh、Lynn 和 Shacham（BLS）的短签名作为一个例子，然后描述一个有效的 DOS 签名，长度只有 320 比特，且在随机预言模型下被证明是安全的。第 10 章，在线/离线验证签名方案：首先定义了在线/离线验证的新概念及其安全模型，然后提出了一个非常有效和实用的在线/离线验证签名方案，且证明了该方案在标准模型下是安全的，最后通过借助双陷门变色龙哈希的适当转换发现现存的短签名方案都能在随机或非随机模型下转化为本章所提出的方案。第 11 章，基于属性签名自适应匿名认证 SA^3 系统：首先针对不同认证策略情形，设计一个自适应匿名身份认证的通用模型和安全需求，然后应用一个具体的签名工具——基于属性的签名来实现动态匿名认证，最后应用 PBD 库，针对 10 个不同的认证策略，在 ubuntu 的环境下仿真认证过程，最后获得认证的时间。第 12 章，基于属性签名的用户撤销：针对基于属性签名算法的用户撤销问题设计出一个高效的用户撤销算法。第 13 章，自适应匿名身份认证的用户撤销：在自适应匿名身份认证系统的应用中，一个必须解决的问题就是如何有效地撤销系统的用户。本章进一步完善自适应匿名认证系统，运用基于属性签名用户撤销方案，从而设计出一个 SA^3 中有效的用户撤销方案。第 14 章，轻量级 RFID 双向认证协议：基于现有的 HB 类协议来设计一个安全有效的 RFID 认证协议，其困难性是基于 LPN 问题。第 15 章，RFID 标签所有权转换安全协议：提出了一个实现 RFID 标签所有权完全转换的有效方案，通过“一交换两更新”的 3 步骤实现协议，该协议能达到保护原、新所有者的隐私，抵御一些不法参与方的恶意行为和保障交易方尤其是新所有者的权益的目的。第 16 章，RFID 标签隐私可靠统计机制设计：基于 RFID 技术所设计的一个隐私数据统计系统机制，该机制实现了既保障 RFID 标签的隐私，又很好地保证了统计结果的可靠。第 17 章，SKRAP 安全认证协议研究：在分析已有的 SKRAP 安全协议的基础上，提出了一种基于 SKRAP 的改进协议，通过对其分析可知，改进的协议 ISKRAP 能够抵抗重放攻击、监听攻击、去同步化攻击和追踪攻击，是一种比较安全的认证协议，在实际环境中有一定的使用价值。第 18 章，SECRAP 安全认证协议研究：介绍了一种基于椭圆曲线密码的 RFID 安全协议，发现其不能抵抗去同步化攻击的安全漏洞，通过在服务器和标签都存储两份的共享密钥来使协议能够抵抗去同步化攻击，进而完全随机化阅读器发出的证据，修改后的协议也能够抵抗伪造攻击。第 19 章，ESAP 安全认证协议研究：通过对 RFID 安全认证协议 ESAP 的分析得出，它存在不能抵抗追踪攻击的弱点，从而通过修改服务器端的回复消息，使得每条认证消息更加不可分辨，从而达到抵抗追踪攻击的效果。第 20 章，基于身份加密的隐私匹配：提出一个基于身份加密隐私匹配的简单方案，并给出了该方案所能抵抗的攻击。第 21 章，基于身份加密的多方隐私匹配：通过使用布隆过滤器解决基于身份加密的多方隐私匹配的计算量巨大的问题，然后从可信和安全

性分析，所给出的基于身份加密的多方隐私匹配方案是可行的。第 22 章，基于身份加密的隐私匹配在自组织网络中的应用：尝试将基于身份加密的多方隐私匹配方案应用到实际环境中加以检验其实用性。第 23 章，无线 Mesh 网络中基于矩阵的对密钥建立方案，改进了 Blom 方案，提出了一种新的无线 Mesh 网络中基于矩阵的对密钥建立方案，实现了能量受限的 Mesh 客户端只需要消耗极少的通信代价、存储代价就可以建立对密钥。第 24 章，无线 Mesh 网络中基于矩阵和利用部署信息的对密钥建立方案：基于 Mesh 网络中存在大量的能力受限的 Mesh 客户端且这些 Mesh 客户端之间需要在短时间内建立对密钥，提出两个方案来为 Mesh 客户端之间建立对密钥。第 25 章，无线 Mesh 网络中基于多项式的对密钥建立方案：在传感器节点通过 Mesh 路由器与 Internet 连接的网络模型下，提出一个基于多项式的对密钥建立方案。

参加本书撰写的还有福建师范大学数学与计算机科学学院、福建师范大学网络安全与密码技术重点实验室的研究生郭福春、吴忠生、刘中仁、张一镰、陈友勤、连燕玲、张跃欣、蒋德山，陈志德对全书进行了统稿和审定。另外，电子科技大学计算机科学与工程学院的陈建章博士对全书的排版和校对也做出了贡献并且帮助整理了全书的参考文献。

本书的出版得到了国家自然科学基金（61202450，U1405255）和教育部博士点新教师类基金（20123503120001）的资助。福建师范大学数学与计算机科学学院、福建师范大学网络安全与密码技术重点实验室对本书的撰写给予了大力支持，在此深表感谢。

限于作者的水平，书中错漏之处在所难免，恳请国内同行和广大读者不吝赐教。

陈志德　黄欣沂　许力

2014 年 12 月 5 日

福建师范大学数学与计算机科学学院

福建师范大学网络安全与密码技术重点实验室

目 录

基 础 篇

应 用 篇

基础篇

第 1 章

引 言

1.1 身份认证的研究背景和现状

随着科学技术的发展，接入网络的用户越来越多，第 32 次中国互联网发展状况统计报告指出，截至 2013 年上半年，中国互联网用户数量达到 5.91 亿，互联网普及率为 44.1%。然而，网络是一把双刃剑，网络的信息和服务在给授权用户带来便利的同时，也给非法用户提供了可乘之机。近年来，大到国家军事政治等机密数据的安全，小到商业企业或个人用户，都面临着不法用户破坏、更改、泄露等造成的安全威胁。因此，在网络世界里如何保护信息的安全，成为迫切需要解决的问题。

身份认证是防护网络信息的第一道关口。在网络中，要保证通信的可信和可靠，必须正确地识别通信双方的身份，防止非法用户假冒合法用户，给合法用户造成经济上的损失。身份认证分为用户与主机的认证和主机与主机的认证，是一个实体确认通信的另一个实体具有它所声明的属性的过程，是验证实体真实性的过程。在真实世界，认证一个实体的身份可以通过：（1）实体所知道的东西，如口令、密码等；（2）实体拥有的东西，如印章、智能卡等；（3）实体所特有的生物特征，如指纹、虹膜、声音等。在网络世界中，身份认证的手段和真实世界一致。

公钥密码学中的数字签名可以设计身份认证协议。数字签名类似手写的签名，是给电子文档进行签名的一种电子方法，具有与手写签名一样的法律效力。在数字签名策略中，用户拥有一对公私钥，在签名中使用私钥对消息进行签名，利用公钥对签名进行验证。由于私钥为用户所特有，因此签名具有认证性、完整性和不可否认性。在公钥密码学中，为保证公钥的真实性和有效性，公钥可以与用户的公钥证书相绑定，一个简单的证书包括证书拥有者的公钥、名称及证书中心 CA（Certification Authority）的数字签名。也可以将用

户的身份（如身份证号码、电话号码和邮件地址等与用户的身份具有直接而天然的联系）直接作为用户的公钥，如基于身份签名技术的应用。

无论是基于公钥证书或是基于身份的签名技术，都有一个共同点，即用户的真实身份对于认证服务器是公开的。然而，如果用户在每次认证时都公开自己的身份，一些网络商家可以分析用户的网上习惯，获取他们需要的信息。而信息一旦泄露，造成的损失会不可计数，特别是金融企业。具有隐私保护的身份认证是近年来迅速发展的安全问题，越来越多学者从事隐私保护方面的研究。隐私保护认证技术是指在认证的过程中不泄露实体真实身份的一种认证技术，可以满足一些特殊场合的需求，在电子医疗、云计算、车载网、物联网等领域得到了广泛的应用。据波士顿咨询公司的一项调查，隐私比成本、易用性和安全性等更为用户所关心[1]。目前存在几种匿名认证技术，包括群签名[2,3,4]、环签名[5,6,7]、盲签名、假名技术[8,9,10,11,12,13,14]和基于属性的签名[15,16]等。数字签名的理论与应用还在不断发展中，随着新体制（如基于格的密码系统）的出现，将会有更安全、更高效、更易硬件实现的数字签名方案被提出。安全而高效的短签名能够快速发展是因为双线性映射（Bilinear Pairing）被引入到签名系统构造中。它的出现马上成为研究的热点，很多原先难以解决的密码问题都得以解决。自 2001 年 Boneh、Lynn 和 Shacham 提出可证明的基于双线性对短签名以来[17]，又有好几个基于双线性对短签名被提出。Boneh 等人的短签名长度只有 160 比特，而且它的安全性是基于困难问题 co-CDH 假定的，它的主要不足是基于随机预言模型下安全证明；2004 年，Boneh 和 Boyen 提出了一个在非随机预言模型下是安全的短签名方案[18]，签名长度是 320 比特。它的不足是基于困难问题 q-SDH 假定下，这个困难问题假定中输入量很大，将导致方案的安全性降低。2005 年，Waters 提出另一个在非随机预言模型下是安全的短签名方案[19]，它的签名长度与 Boneh-Boyen 方案的相同，而且它的安全性是在标准困难问题 CDH 假定下进行证明的，这个困难问题的输入参数长度比 q-SDH 困难问题要短很多。但是，该方案的不足是需要输入一个很长的公钥参数且安全归约不够紧。2009 年，Hohenberger 和 Waters 又提出一个在非随机预言模型下而且在标准困难问题 CDH 下进行证明的短签名方案[20]，它的不足是签名长度为 640 比特而且引入了一个状态信息（如计数器），增加了操作的复杂性。许多学者对这些经典短签名方案进行了深入的讨论和研究，提出了很多改进方案和具有附加性质的签名方案。

但是相比有限域上的模、加、幂等运算，双线性对的运算开销是很大的。这就限制了这类签名的使用范围，如智能卡、无线设备等。1989 年，在线/离线签名方案概念由 Even、Goldreich 和 Micali 提出来[21]，他们提供了一个通用的方法来将任何签名方案转变为在线/离线签名方案，但是由于被转换的签名方案长度太大而不实用。2001 年，Shamir 和 Taurnan 提出了一种新的在线/离线签名方案，该方案通过一个 hash-sign-switch 模式将任何签名方案转变为在线/离线签名方案[22]。新方案加强了签名的安全性，因为用户在离线签名的时候使用的是一个随机生成的字符串，文献[22]中新的方案对选择明文攻击免疫，而文献[21]中的方案不具有这种对选择明文攻击免疫功能。

在线/离线签名的思想就是将签名分成两个阶段，第一个是离线阶段：待签署的信息还未被确定，签名者做一些预处理工作；第二个阶段是在线阶段：一旦待签署的信息被确定，签名者利用预处理的结果，并使用非常短的时间完成签名。在线/离线方案很有用，在许多应用中签名者需要在有限的时间内进行签名，他需要花费大多数计算在签名前的准备上，签名的算法也需要花费很多计算量。特别在智能卡上，由于其有限的计算量，这种方法很有效，离线的时候进行后台计算，在线签名的时候，利用离线时计算出来的结果进行在线签名。这种在线签名速度很快，因为其不需要做复杂的双线性对或者模幂运算，通常只要做简单的异或乘法或者加法即可。这样，即使在计算量很低的处理器上也可以进行签名。考虑到现今智能卡被广泛应用，这种在线/离线方案具有广泛的应用前途。在线/离线签名方面的相关工作还有文献[23～29]。

与此同时，新一代网络对身份认证协议的设计提出了新的要求，包括：（1）认证规则的多样性。新一代网络中设备和服务的多样性必然会导致认证规则的多样性。（2）认证规则的多变性。网络自身的复杂性和各种突发的事件会导致认证规则变得复杂又难以预测，即使在同样网络服务/设备中，身份协议的认证规则也需要根据实时的网络状况进行调整。

在传统的认证系统中，由于用户的身份是公开的，所以无论策略如何变化，网络服务器可以直接判断用户的身份是否符合认证策略。然而，在具有隐私保护的认证系统中，动态认证有一定的困难性。如何认证用户使其满足动态变化的认证规则，同时确保用户身份隐私，成为迫切需要解决的问题。

基于属性的密码体制是基于身份的密码体制的延伸，很多方面与基于身份的密码体制相比有着更为灵活、广泛的应用，可以实现匿名身份认证。基于属性的密码体制将用户的身份看成是一系列属性的集合，验证的时候只要确定用户给出的几个属性满足所声明的认证规则，并不泄露用户的具体身份。因此基于属性的签名可以提供较强的隐私保护。例如，李四拥有属性集合{“外资企业 A”，“经理”，“年薪 30 万元”，“本科学历”}，李四想向政府揭露 A 企业的产品不合格，李四用“外资企业 A”、“经理”这两个属性进行签名，匿名向政府举报。政府在接收到举报信息后，可以验证此消息的真实性，确定消息是来自外资企业 A 的经理。由于具有这两个属性的人不止一个，李四可以将自己的身份掩盖，达到匿名举报的效果。在发布其他消息时，李四根据具体认证策略的要求，采用另外的属性进行签名。基于属性的签名满足：（1）抗伪造性，签名只能由拥有能满足声明的属性的用户所产生，而不能由几个用户把他们的属性放在一起合谋产生。如果张三的属性是{“外资企业”，“员工”，“年薪 30 万元”，“本科学历”}，王五的属性是{“私营企业”，“经理”，“年薪 30 万元”，“本科学历”}，那么他们两个人不能合谋通过外资企业经理的验证。（2）隐私保护性，即签名只揭示所给的属性满足签名声明，而不知道具体怎么满足、用户是谁、用户有几个属性。

面对复杂多变的网络环境，探讨具有隐私保护特性的基于属性的密码体制在身份认证