Information & Communication

信息与通信创新学术专著

·通信加密技术与系统·

消息鉴别与生物认证

Message Authentication and Biometric Authentication

王志芳 著

人民邮电出版社
POSTS & TELECOM PRESS

Informatic Communication

信息与通信创新学术专著

·通信加密技术与系统·

消息鉴别与生物认证

Message Authentication and Biometric Authentication

■ 王志芳 著

人民邮电出版社

北京

图书在版编目（CIP）数据

消息鉴别与生物认证 / 王志芳著. -- 北京 : 人民邮电出版社, 2015.2
（信息与通信创新学术专著. 通信加密技术与系统）
ISBN 978-7-115-37297-0

Ⅰ. ①消… Ⅱ. ①王… Ⅲ. ①通信保密－研究 Ⅳ. ①TN918

中国版本图书馆CIP数据核字(2014)第243930号

内 容 提 要

消息鉴别是对信息的真实性、完整性进行认证的技术，既有基于密码学算法的消息鉴别方法，也有近年来发展起来的以生物测量学（Biometrics）为基础的新方法，如生物识别、生物密钥等。站在认证性需求的角度系统地归纳相关的技术基础和最新进展，是本书写作的最初动机，这种视角和结构安排也体现了笔者关于信息安全内涵的理解和一些相关的工作。对于信息系统中来源真实性、内容真实性及内容完整性的认证鉴别需求，本书给出了基于密码学方法和生物测量学方法的若干技术途径，可供相关研究人员参考。

◆ 著　　王志芳
责任编辑　代晓丽
责任印制　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
◆ 开本：700×1000　1/16
印张：18　　2015 年 2 月第 1 版
字数：352 千字　　2015 年 2 月北京第 1 次印刷

定价：85.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序　言

按香农（Claude Shannon）的信息论定义，信息是通信信道容量的度量，是系统传输和处理的对象，它载荷于语言、文字、图像、数据等消息（Message）之中。在日常生活、工农业生产、科学研究以及战争等活动中，一切都离不开消息传递和信息流动。

随着信息化的飞速发展，信息安全（Information Security）越来越成为整个社会和民生发展中不可回避的重要问题，是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略问题。从信息安全的本质上看，可以体现在两个层面，一个是信息来源的真实性、可信性和可靠性，另一个是信息自身的完整性、可用性、保密性和可靠性；从信息安全的技术观点上看，则体现在信息载体（消息）的安全与保护。

笔者从信息安全的本质和技术出发，以经典的应用密码学的角度，讨论了消息鉴别（Message Authentication）的概念、基于加密的消息鉴别、基于对称密码的消息鉴别、基于公钥密码的消息鉴别、基于散列函数和认证码的消息鉴别等关键技术问题，为读者系统地捋清了上述各项技术对于消息的完整性与消息的真实性认证的思路、方法与手段。

经典的应用密码学最大的问题（不论是其协议或算法）在于只研究消息（信息）自身的安全性，而忽略消息（信息）使用者的安全性问题。密码学中最经典的一句话就是“This session is not about securing: People (sorry), cables, typewriters and computers (?!)”。就是说，任何人或用户掌握了密钥或设备资源，那么信息就是属于这个人的，密码学也无能为力。生物信息识别与认证（Biometric Identification and Authentication）技术，就是试图从信息使用者的安全性出发，解决信息归属的安全问题。《消息鉴别与生物认证》中笔者的最为难能可贵的地方就是，将信息自身的完整性与真实性问题和信息拥有者（使用者）的完整性与真实性问题系统地整合在一起，同时，还把其多年的研究成果呈现在本书中，比如，

基于感觉信息的多模态生物特征融合、基于知觉信息的多模态生物识别、基于感觉—知觉信息的多模态生物特征融合、生物密钥与生物模板保护等技术和方法，这些无疑为读者全面系统地了解和掌握信息安全的本质、技术和方法，提供了极好的学习与研究平台。

哈尔滨工业大学　牛夏牧

前　言

信息安全是一个由来已久的话题，在数字化信息系统（Internet 尤具代表性）出现之后，信息的获取更加便利、流转更加通畅，但同时也带了信息的不受控传播、可信性及可用性等方面的问题，这些不安全因素除了影响信息的正常使用，还可能引起信息系统的故障甚至瘫痪，因为信息系统本身的运作也依赖于各种不同形式的消息所承载的信息。这些问题在现实中的表现就是常常听到的窃取信息、非法访问、数字欺诈、系统瘫痪等令人不安的各种信息安全问题。随着信息安全问题对人们工作、生活的影响越来越大，关于信息安全的研究也逐渐成为热点，信息安全本身也逐渐发展成为一门系统性的学科。那么，在信息安全领域中，各种安全需求、安全技术以及安全协议之间是怎样一种关系呢？下图试图对这个问题进行梳理。

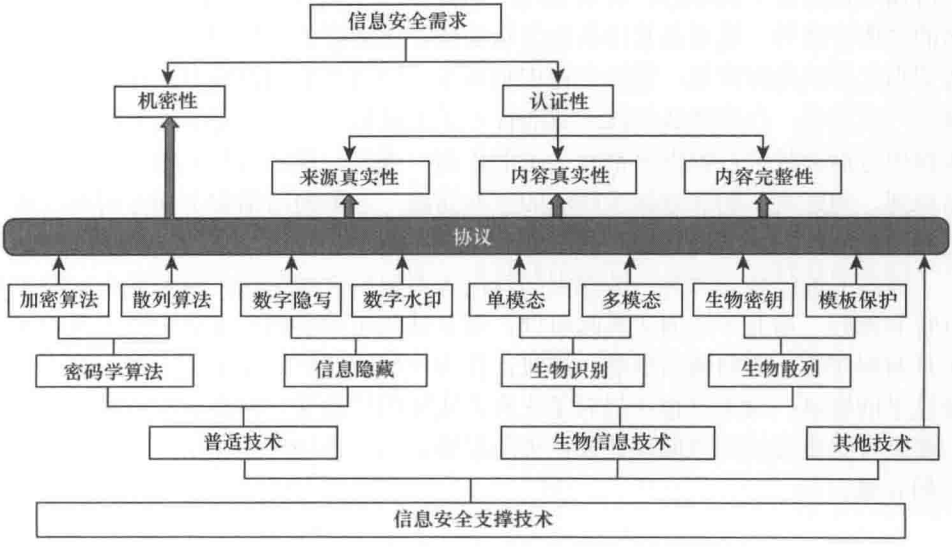

图 1　信息安全需求与信息安全技术

如上图所示，实际信息系统中关于安全的需求有各种表述方式，但是本质上归结起来无外乎机密性与认证性两个方面的安全需求，其中认证性又包括来源真实、内容真实及内容完整 3 个侧面。而在现实世界中，这些需求的表现方式千变万化，所用到的技术也多种多样，它们到底是什么关系呢？笔者试图从这样一个视角去理解：信息安全领域中的各种基本技术、算法都可以认为是信息安全支撑技术，这些技术在协议的组织下，构成了针对特定安全业务的方案与实现，这些方案与实现用来满足这个安全业务背后所体现的信息安全需求。上图就是在试图以这样一种视角来理解信息安全领域中的诸多概念。

基于上述分析可以看到，对于一种安全支撑技术，一般很难说它是解决某种安全需求问题的，比如，加密算法既可以用来加密数据实现机密性保证，也可以基于某种协议实现真实性或者完整性的认证；反过来，满足某种安全需求的技术方案往往也不是唯一的，比如，可以通过数字签名的方式进行来源真实性认证，也可以通过数字水印的方式达到同样的目的。因此，关于信息安全技术的书籍由于出发点不同，其表述方式也有很大差别，如果没有理解上述事实，就很容易“只见树木不见森林”，无法在真正的问题面前找到有效的解决方案。

笔者从博士课题开始进入信息安全研究领域，10 年来有幸目睹了信息安全在我国逐渐引起重视、在大学设立专业、建立研究机构直至国家成立专门机构的过程，在这个过程中笔者所在的研究团队也从多个角度努力探寻信息安全这个学科的内涵、规律及本质，本书在一定程度上体现了笔者及其合作伙伴对于信息安全的理解及在相关领域的一些工作。之所以起名为“消息鉴别与生物认证”，就是基于前述对信息安全的理解，着重关注信息认证性保障的方法。除了基于密码学算法的经典方法外，笔者及其团队在生物认证方面从事了多年的研究工作，站在模式识别之外的角度审视、理解生物识别技术，同时将生物识别方法在信息安全领域进一步推进，在生物认证技术方面投入了大量精力，特别是生物密钥、生物模板保护方面的研究在国内外都有一定的影响。因此，这本书从生物认证的角度重新梳理、阐述了生物信息技术领域的一些问题，把生物识别和生物密钥对应到消息源的真实性鉴别和消息的完整性鉴别两个方面。

这本书的结构安排和一些观点与目前大多数信息安全相关的书籍相比似乎有点特立独行，这并不是为了挑起争议，而是试图在理解信息安全学科内涵的基础上重新阐述对一些问题的理解。同时，作为一种连接信息安全需求与信息安全支撑技术的尝试，这本书也许能对于正在为实际的信息安全问题寻找解决方案的人们提供一些更直接的帮助和建议，如果能够起到一点这样的作用，那将是我们最大的欣慰。

作者

2014 年 10 月

目　录

第1章
消息鉴别概述

1.1 信息安全与消息鉴别

随着信息化在社会各个方面的普及，人们的生活、社会的生产以及社会的秩序与信息系统的关系越来越密切，一般意义上的信息系统包括从巨型计算机到手机终端等各种信息处理设备构成的庞大的体系，从国家安全到个人生活服务，无不依赖于各种数字化的信息。人们看到的、看不到的各种各样的设备之所以都能够被归结到所谓的信息系统，是因为信息系统的实质在于处理信息而非其外在形态，换句话讲，信息系统中最有价值的资产是其中无形的信息。随着人们对信息化认识的深入，人们对“信息安全”的重视程度也越来越高，从某种意义上讲，失去了安全保障的信息系统基本上也就失去了其使用价值，因此，近年来信息安全的保障已经上升到国家战略的层面[1]。

信息安全的核心问题是保护信息的两个关键属性：机密性和认证性。所谓机密性，就是信息对于未授权的用户而言是不可理解的，一般包括两种技术手段：一是信息加密，二是信息隐藏；所谓认证性，就是对于信息（包括其来源）的真实性、完整性进行确认，保障信息认证性的过程在信息安全的专业术语中一般称为“消息鉴别”，消息鉴别涉及的技术手段比较多，方式、方法也比较多样化，除了保障机密性用到的加密、隐藏等技术手段外，还可以使用散列函数（包括多媒体感知散列）、模式识别（特别是生物识别）等技术配合特定的协议进行消息鉴别。本书旨在介绍围绕消息鉴别问题的一系列理论、方法及其最新进展，为信息安全领域中相关应用提供理论化、系统化的指导和建议。

关于信息机密性的保护不是本书讨论的重点，这里仅对其原理和方法做一个简要的介绍，更多的细节请参考密码学和信息隐藏方面的书籍。从狭义的角度讲，保证信息的机密性就是指信息加密，加密后的信息只有持有密钥的人才能看到有

意义的内容，否则看到的都是无意义的密文。但是，近年来随着数字隐写技术的发展，信息隐藏方法也成为保证信息机密性的手段之一，从而扩充了信息机密性的内涵。基于信息隐藏的方法的特点是只有合法的用户才能看到相应的信息，其他人甚至不知道是否存在这些信息、这些信息在哪里存在。因此，从“只让指定的人看到指定的信息”的角度讲，信息加密和信息隐藏都是保证信息机密性的方法。

本书重点讨论“消息鉴别”的原理和方法，也即如何保证信息的认证性。信息认证性的内涵有两个方面：真实性认证和完整性认证，而真实性认证又包括内容真实性与来源真实性，所谓认证就是对这 3 种“性”进行鉴别。有的参考文献中还提到诸如“可用性”、“不可抵赖性”等，其实大都相当于上述某一种或多种基本属性结合特定的应用背景或约定（协议）的概念延伸，比如“不可抵赖性”就是在一定语义前提下的来源真实性问题，“可用性”认证在多数场合相当于信息的完整性及其内容真实性的鉴别。因此，笔者认为，信息安全最为核心的内涵就是保证信息的机密性、内容真实性、来源真实性及完整性等属性，后面 3 个属性也可以统称为认证性，实现认证性的技术过程一般称为消息鉴别。消息鉴别的方法相对而言更加多样化，可以基于信息加密算法，也可以基于信息隐藏算法，另外对于来源真实性问题，还逐渐形成了基于生物特征识别的一系列方法。

需要说明的是，信息加密是保证信息机密性的手段，但不意味着加密方法只能用来保证信息的机密性，加密算法配合特定的协议，也可以实现消息鉴别，比如双向 MAC、HMAC 等。同样，信息隐藏技术也可以用于构造消息鉴别方案，用于鉴别消息真实性、完整性的信息隐藏方法一般称为数字水印技术，而用来保证信息机密性的信息隐藏方法一般称为数字隐写技术。

总之，信息的机密性和认证性是信息安全的两个本质问题，达到目标的手段有很多种，其中的基本方法或算法不见得就是唯一用来解决机密性问题或认证性问题的，很多时候一些基本算法（如加密算法、信息隐藏算法等）既可以用来保证机密性，又可以用来构造实现消息鉴别的方案。因此，从算法的角度介绍信息安全，常常从“应用密码学”、“信息隐藏”的角度分别介绍；如果从保证信息安全基本需求的角度，则可以按照“信息保密”、“消息鉴别”的分类方式对各种技术方案加以介绍。后者的优点是更加紧密地结合信息安全的现实需求，对实际应用更具有指导意义，本书从后者的分类方法出发，系统介绍目前主流的“消息鉴别”方法及笔者在相关方面的最新研究成果。

1.2 消息鉴别的要求

在一个公开的网络信息系统中，对信息安全的威胁多种多样，典型的攻击包

括以下几种[2]。

① 泄密：将消息透漏给没有合法密钥的任何人或程序。

② 传输分析：分析通信双方的通信模式。在面向连接的应用中，确定连接的频率和持续时间；在面向连接或无连接的环境中，确定双方的消息数量和长度。

③ 伪装：欺诈源向网络中插入一条消息。如攻击者产生一条消息并声称这条消息是来自某合法实体，或者非消息接收方发送的关于收到或未收到消息的欺诈应答。

④ 内容修改：对消息内容的修改，包括插入、删除、转换和修改。

⑤ 顺序修改：对通信双方消息顺序的修改，包括删除和重新排序。

⑥ 计时修改：对消息的延时和重放。在面向连接的应用中，整个消息序列可能是前面某合法消息序列的重放，也可能是消息序列中的一条消息被延时或重放；在面向无连接的应用中，可能是一条消息被延时或重放。

⑦ 发送方否认：发送方否认发送过某消息。

⑧ 接收方否认：接收方否认接收到某消息。

应对前两种攻击的方法属于消息加密范畴，应对③～⑥这 4 种攻击的方法则属于消息鉴别的内容，数字签名可以抵抗第⑦种攻击，第⑧种攻击需要数字签名和相关的协议结合来对付。实际上，消息鉴别就是验证所收到的消息确实是来自真正的发送方且未被修改的消息，也就是消息的真实性和完整性，同时它也可验证消息的顺序和时间性。而数字签名是一种认证技术，通过签名验证可以抵御发送方的否认攻击。

1.3　消息鉴别的手段

大体来说，消息鉴别的手段可以分为 3 类[3~5]：基于加密的消息鉴别、基于散列函数的消息鉴别和基于消息认证码（Message Authentication Code，MAC）的消息鉴别。

（1）基于加密的消息鉴别

根据加密技术的分类，实际上也是现代密码学的分类方法，对称密码体制和非对称密码体制对消息的加密都可作为鉴别的一种手段。在对称密码体制中，又以分组密码为主流，同时结合分组密码工作模式进行加密，用作消息鉴别。这类消息鉴别通过将消息分成若干个分组，然后使用分组密码采用迭代或并行运算的方式计算得到该消息的认证标记。迭代型消息鉴别典型的代表是 CBC-MAC，并行运算结构的消息认证码典型的代表有 PMAC、XOR-MAC。

非对称密码体制，又称公钥密码体制，最主要的一个应用便是数字签名。由