信息安全系列丛书

TONGXIN XITONG ANQUAN

通信系统安全

张焕炯 编著

- 以通信系统的安全问题为研究对象
- 以信息论和系统论为基本工具
- 对各种通信模式的安全问题进行深入讨论

国防工业出版社
National Defense Industry Press

通信系统安全

张焕炯　编著

国防工业出版社
·北京·

内 容 简 介

本书以通信系统中的安全问题为研究对象，尝试以信息论等为研究问题的基本工具，对于各种通信模式的安全问题进行了深入的讨论。全书共分6章：第1章从信息安全和通信系统的基本概念出发，阐述了通信系统安全这一学科的基本特征和研究方法；第2章从概率论的角度出发，系统地介绍了信息论中的自信息和互信息这两个基本概念，这些概念对于解决通信安全问题有直接的指导作用。第3章则着重介绍加密算法和认证技术；第4章简要地介绍了各种通信网，并为通信网络中的安全通信问题做了必要的准备；第5章介绍通信网络的安全通信技术；第6章介绍通信系统安全中的非技术因素对安全的影响。这样建构成一个相对完整的知识体系，把通信系统安全中的最基本的处理问题的理论、方法、技巧等进行较系统的梳理和总结。

本书既可以作为高等院校的教材，也可以作为通信类和信息安全类的相关参考书。此外，对于想较深入地了解信息理论和网络理论的读者来说，本书也不失为一本能窥探门径的专著。

图书在版编目（CIP）数据

通信系统安全/张焕炯编著. —北京：国防工业出版社，2012.9

ISBN 978-7-118-08342-2

Ⅰ. ①通… Ⅱ. ①张… Ⅲ. ①通信系统—安全管理 Ⅳ. ①TN914

中国版本图书馆CIP数据核字（2012）第186289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）

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 12¼ **字数** 275千字

2012年9月第1版第1次印刷 **印数** 1—3000册 **定价** 32.00元

（本书如有印装错误，我社负责调换）

国防书店：（010）88540777 发行邮购：（010）88540776

发行传真：（010）88540755 发行业务：（010）88540717

前　言

信息安全，顾名思义是关于信息进行安全地传输和存储等处理的理论和技术的总和，在信息化时代，涉及信息安全的领域已不仅仅局限于传统的政治、军事、经济等方面了，它有了非常广泛的拓展，几乎到了无所不包含的程度，在生物信息学、医学信息、图书信息管理、市场、信息经济学理论等方面都离不开信息安全。由于它几乎涉及社会和个人的方方面面，人们对它的重视程度也越来越高，相关的研究和技术应用等也已经提升到了一个前所未有的高度。目前，信息安全已经成为研究的热点，相关的文献大量涌现，信息安全的理论和技术正处在飞速发展的状态之中。

但是信息安全的发展在很大程度上源于通信技术的发展，香农在对通信系统的研究中，提出了基于统计意义上的信息理论，在通信系统的优化指标中首次提出了安全性指标，并就保密通信等展开了卓有成效的研究，并以信息论为研究信息安全的基础，得到了著名的香农保密定理等。他的关于通信系统信息安全的研究成果成为了信息论理论体系中的重要组成部分，香农的研究工作非常重要，它的重要性至少包含以下几点：一是通过通信系统中保密性等的研究，引进了密码学等学科，使得原本仅是一种方法和经验的保密工程实践成长为有严格理论支持的科学；二是找到了信息安全理论的最实用的应用领域，或可称为找到了应用的核心领域；三是为如何进行信息安全的研究提供了成功的范例，具有方法论上的深刻含义；四是为进一步的更宽广范围上的信息安全的研究指明了方向，为确立通信系统安全学科的理论做了奠基性的工作。

所以，以通信系统为基本的着眼点，来研究信息安全技术，或是在通信系统领域进行信息安全的应用研究，它形成了一个非常重要的研究和应用方向，更成为展现通信特色的一个重要手段。

现今，通信系统的模式已经有了很多的种类，既有传统的通信模式，更有以网络为基本支撑的通信模式，针对不同的通信系统模型，对应的信息安全策略和方法也不尽相同；同时，对于安全协议等的研究也展现了多样性的特点，相应的材料日益丰富，通信系统安全问题的总结也自然到了水到渠成的程度，通信系统安全这一交叉性的学科也已经基本形成。

本书以通信系统中的安全问题为研究对象，以信息论和系统论为研究问题的基本工具，对于各种通信模式的安全问题进行了深入的讨论，试图从中寻找到它们内在的共同规律，以期对通信系统理论和通信模式有更深刻的认知，并希望成为通信系统安全这一学科的专著。

最后，殷切地希望读者提出宝贵意见，以便进一步改进和提高。

张焕炯

2012 年 7 月于杭州

目 录

第1章 绪 论

1.1 信息安全与通信系统

顾名思义，安全（Security）就是没有事故或危险。而信息安全，则可理解为关于信息进行安全地传输和存储的理论、技术、方法和规范等的总和，它实际上是对信息的一种安全性的保护，信息安全业已成为具有非常宽泛含义的一个概念或术语，它几乎涉及所有的方面。过去，信息安全往往与密码理论与技术等相关联，甚至是互相不作区分，但是，近年来随着计算机技术、信息处理技术、通信技术的迅猛发展及网络和通信等的相对普及，以信息的传输和存储为基本模式的诸如电子邮件、电子商务、电子政务、网络金融等业务的广泛开展，由安全引起的诸如信息被篡改、窃取、破坏等问题越来越严重，解决这些安全问题的基本方法就是采用切实有效的信息安全保障，这些安全保障包括相应的理论和技术、硬件设施和政策法规等。随着人们对信息安全认知的日益深入，不仅把这个概念扩充为一门具有严谨结构的学科，更给这个概念赋予了基本的含义。信息安全的一般定义：为达到信息在存储、传输、管理等处理过程中的安全指标要求而所采用的一切设备保障、政策法规、管理手段、技术处理及相应理论指导等的总和。使信息安全的过程以及结果都满足信息的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）准则的同时，确保系统本身和使用者有效规避事故和危险。这三大准则从不同的角度来规范信息安全的目标要求，但它们构成一个完整的整体，记为“大三角”。

通信系统，可理解为能用来实现通信目的的设备等的总和，它是以最基本的“输入—处理—输出”模式为基础的，它拥有相对的独立性、鲁棒性等特性，它的模式在不断的发展之中，已从单纯的“信源—信道—信宿”模式发展成为具有广泛互联的通信网络。通信系统不仅成为具有举足轻重的影响力的基础设施，也成为人们日常生活中用于沟通交流的必备工具。它的技术水准在很大程度上是展现一个国家或地区的科技水平的重要指标，更成为一个国家和地区的科技创新的重要策动力量。

人们历来重视在通信系统上的信息安全的研究和应用，但往往是以信息流的安全为主要研究对象，而把通信系统作为信息安全的应用领域。这种观点虽作为主流观点影响了很长时间，但随着通信系统和安全技术各自的进一步发展，各种研究成果大量涌现，人们的观点也发生了改变。开始把通信系统和信息流的安全作为整体来考虑，由此逐步形成了“通信系统安全”这样一门学科，进而极大地拓展了通信系统信息安全的范围。通信系统安全至少应该包括以下安全概念：一是传统的针对通信系统中以数据形式等的信息安全；二是包括通信系统设备等在内的系统安全，它涉及系统的可用性以及系统的正常运行、维护和维修等；三是还包括使用通信系统的用户的安全，用户的安全不仅仅

指一个个具体直接使用系统者的安全，还包括所在的地区和相应的国家主权等方面的安全等。

目前，有关信息安全的研究层出不穷，信息安全的应用更是到了无处不在的地步，相关的研究及应用文献大量涌现；同时，通信系统的理论和技术发展也非常迅猛，把它们的理论和技术进行融合，构成既具有学科交叉的，又包含鲜明特色的通信系统安全是发展的必然结果。

1.2 通信系统中的安全问题

通信系统实现了信息的传输和存储等处理功能，在这个体系中，还有用来提升系统安全性能的安全处理，以突出安全处理为特点的基本模型如图 1-1 所示。

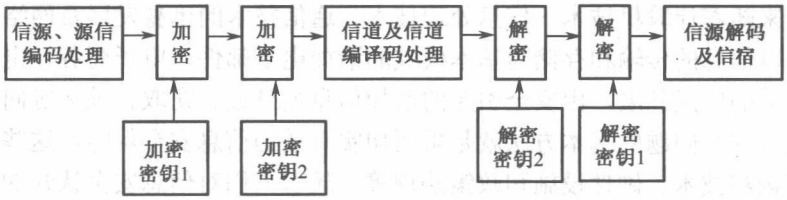

图 1-1 通信系统的结构模型

从模型中不难看出，通信系统最基本的要素为信源、信道和信宿，这三要素能实现通信系统中的信息发送、传输、存储及接收等功能。但是，因为环境的复杂性以及技术的局限性等因素，如何实现“好”的通信是一个十分现实的大问题，它至少涉及如下三个方面：首先，需确定用来描述系统好坏的具体指标；其次，给出所确定的具体指标的定量表述；最后，在不能达到技术指标要求的前提下，采用何种行之有效的技术手段来克服具体的困难，也就是采用何种有效的手段对系统性能指标进行有效的优化。香农根据自己的长期研究，提出了“好”的通信系统的具体指标，它们分别为有效性、可靠性和安全性。有效性表现为有用的信息占总的传输信息的比例多少的问题，它需要尽可能地减少冗余来提高系统的有效性。可靠性则是体现在所传输的信息的正确率的问题，它以误码率或误比特率来表示。在很多时候，人们看到，要提高系统的有效性，则很可能需要牺牲系统的可靠性，它们是一对矛盾体，类同于通常所谓的精度与速度之间的矛盾。但是，必须也要看到，在某种条件下，它们事实上也是相辅相成的，在传输总量确定的前提下，若通信系统在信息传输过程中出现错误越多，这不仅表现在系统的可靠性越差，同时也表现在系统的有效性也是越差的。因此，提高系统的有效性与提高系统的可靠性得到了内在的统一。

分析上面的通信系统不难发现，所需传输的信息必定要有专门的接收对象，无论是广播模式、组播模式还是一对一的点对点模式，概莫例外。对于接收者，根据它是否为所期望的接收者这一条件，可以分为合法用户和非法用户或期望用户和非期望用户。信息的发送方总是希望安全地把信息发送给合法用户，且不被非法接收者所窃听，这就需

要提供如何防窃听的技术和手段。一种可行的办法就是选定专门的信道，以确保从发送到接收整个过程不被破坏。但一般的通信系统是一种语义透明的公共信道，成为专门信道的条件显然不能达到，因此需要在通信系统中采用相应的处理技术来防窃听，构成通信系统中防泄漏的安全问题。同样的道理，以信息接收者为参考对象，它既需要接收到完整的信息，更需要接收到期望发送者的信息。它所面临的一个主要问题是如何防止非期望发送者伪造身份进行虚假信息发送，这构成通信系统中防伪造的问题。同样需要专门的技术处理来克服这个难题，通常所采用的是认证技术。认证是一个过程，通过一系列的推演等步骤的处理，能够验证发送者的身份是真实可信的或是伪造的。所以对于一个通信系统来说，它的安全问题既涉及具体的防窃听的问题，也涉及具体的防伪造的问题，以及这些问题的交错混合所构成的复杂安全问题。通信系统为解决相应的安全问题，同时提升或优化系统的安全性能，所采用的技术不仅需要有防窃听的加、解密技术，还需要防伪造的认证技术，以及包含它们的综合性的技术措施。

随着通信技术的发展，单纯的通信系统向着网络化方向发展，针对网络的安全技术成为了通信系统安全的重要组成部分，而且它的重要性更可谓是与日俱增。人们发现，网络中的安全问题层出不穷，不仅有针对不同网络种类的安全问题，也有针对网络分层中不同层的安全问题。例如，数据链路层、网络层、传送层以及应用层中的安全问题。而如何更加有效地解决通信网络中的安全问题，更成为了安全问题中的重中之重。除了采用传统的密码技术和认证技术外，需要有更加针对性的综合技术来解决通信网络中的安全问题，这个针对性的综合技术就是设计安全通信协议。而安全通信协议的实质就是为实现信息安全交换等目标，各通信方之间的某种约定和采取相应步骤的总和。现在，人们越来越认识到实现通信网络安全的核心是“密码和安全协议”。所以对网络安全协议的研究和应用成为通信网络安全的主要组成部分，通信安全协议及相关的理论和技术构成通信系统安全的重要内容。

通信系统是由人设计和制造的系统，“人”的因素在每一个环节都起着重要的作用。对于通信系统的安全来说，同样需要“人”遵循相应的原则和规范。这些规范既有面向技术的，也有面向非技术的，如操作规范、道德守则和法律法规等。遵循这些规范同样能有效地规避相关的风险，对通信系统安全有很好的保障和促进作用。

1.3 通信系统的发展与信息安全理论与实践的关系

通信系统的安全性能是表征通信系统优劣的重要指标之一，通信系统的安全问题以及解决该问题的所有技术和策略构成了通信系统安全的核心内容。但同时也必须看到，信息安全是一个相对宽泛的，具有鲜明特色的学科，要认清通信系统的发展与信息安全的理论创新与实践的关系。

一方面，从通信系统的发展历程来看，它从单纯的点到点的模式到网络化的模式，从单纯的话音业务到以数据业务为主的综合业务，更从面向单机和数据到面向数据共享的模式，所对应的对系统的安全也有了更高的要求。系统的安全已经不仅仅是解决某一个

具体问题或漏洞那么简单，而是对面向数据和用户的安全属性赋予新的内涵的同时，强调了面向系统的安全属性，构成了综合的面向数据、面向系统和面向用户的立体型的信息安全新概念。从面向数据的角度来看安全的概念，它最直接的体现就是信息的保密性、完整性和可用性，也就是信息安全的 C.I.A 准则；而面向系统的安全概念所涉及的是实现系统的可用性、可控性、稳健性和可再生、恢复等特性；面向用户的安全概念是以用户为主体，实现该主体的可操作性和自然法人等的特性，具体包括对实体的认证、访问控制、授权和服务性等实践等的相应功能。进一步，随着通信系统和技术的发展，新的安全问题更是层出不穷，这为密码学和信息安全的理论和技术提出了全新的挑战。它促使人们对信息安全作更精深的研究，同时为信息安全的理论创新和技术创新提供良好的契机和应用领域。从这种意义上来看，通信系统的发展是促进安全技术创新的重要因素，也是展示安全新技术的重要领域，更是检验具体的安全技术和方法的先进性的重要场所。

另一方面，密码学等信息安全的理论和技术的发展，为顺利解决通信系统的安全问题提供理论的准备和实际的实现方法。信息安全作为一门严谨的学科，它具有自己内在发展脉络和轨迹，具有相对完整的自我完善的特性。新的加密算法的出现，新的加密技术标准的颁布，新颖的认证算法等的出现，或已有的加密算法的破译等。不仅能推动信息安全理论和技术自身的巨大发展，更能有力地推动通信系统的发展，尤其对通信系统的安全性能指标的优化产生巨大的促进作用。例如，RSA 公钥制理论的提出、DES 和 AES 标准的颁布、基于椭圆曲线难解问题的数字认证方案的公布、用于电子邮件安全的 PGP 协议的公开、针对 TCP/IP 协议模型的安全通信协议的设计等，这些信息安全的理论和技术都能有力地提升通信系统的相应的安全能力。因此，密码学等信息安全的理论和技术的发展能极大地促使通信系统的安全性能的长足提升，是通信系统发展的重要推进力量。

此外，还必须看到，在很多时候，相关的通信技术本身能有效提高通信系统的安全，这方面最典型的莫过于扩频技术。在通信中，采用扩频技术能有效降低对信噪比的要求，同时由于信噪比的降低，能很好地起到信息的隐藏等效果，这就实现了安全理论和技术与通信系统的理论和技术的内在统一，它从一个方面也说明了两者内在的可融合性。

1.4 通信系统安全的研究方法

在过去，研究密码学等信息安全理论的人们不大关注通信理论的研究，同样地，专注于通信理论等方面的研究者也不大关注信息安全等的问题。例如，他们设计通信系统及其各种规制时往往对安全问题的考虑不是非常充分，等系统在实际使用时，碰到了具体的安全挑战后，再来补强相关的安全举措，这似乎已经形成了一个传统。但随着人们对信息安全的重要性的认识越来越深入，人们认识到通信系统安全是一门综合的交叉于通信理论和安全理论的学科，并着手寻找最佳的深入研究的途径，总结和归纳合乎通信系统安全学科本身内在规律的研究方法。

香农是创立信息论的伟大先贤，他关于通信系统中的安全问题的研究成果业已成为信

息论的重要组成部分，他的关于通信系统的安全问题的研究方法也能堪称经典。其中最有特色的是一方面能抓住问题的本质的前提下，对安全问题进行有效的简约；另一方面，他引进了描述不确定性的信息熵的概念，通过对通信系统处理前后不同状态下的信息熵的定量表述，引进了诸如唯一解距离等新概念的同时，堪称完美地给出并证明了保密定理，为密码学和信息安全的学科的确立奠定了重要的基础。分析他的研究方法，不难发现，他自觉地把通信系统安全问题纳入了信息处理的具体范畴，把加密、解密等安全处理看作信息处理器模块的功能实现，因此它也遵循信息处理的基本原理和准则。而迄今，所采用的信息处理的方法和手段都不外乎来自如 Weiner 等所创立的控制论（Cybernatics）和香农等所创立的信息论（Information Theory）等的相关理论。控制论和信息论是信息与信号处理的所有方法的理论基础，当然它们也是信息安全处理的理论基础，所以通信系统安全的基本处理方法应该是以系统论和信息论为指引的能有效提升安全性能的方法。也就是说，通信系统安全的研究方法不能背离系统论和信息论的基本原则和要求。这种基本的研究方法可以用图 1-2 作直观的表示。

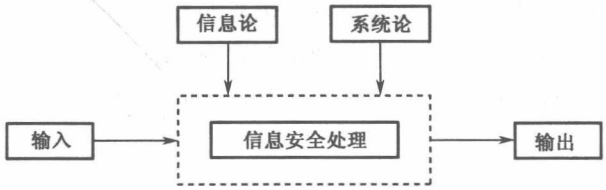

图 1-2　通信系统安全处理方法示意图

随着通信网络的发展，针对网络的安全问题的研究方法也呈现出新的特点。虽然人们越来越认识到“密码和安全协议是网络安全的核心”，比较专注于从密码学和通信安全协议的设计等方面着手进行通信系统的安全的处理，但是本质上还是没有跳过以信息论和系统论为基本理论依据的信息处理的方法。

另外，因为通信与普通人们的生活息息相关，通信系统的安全实际上就是普通人安全的重要组成部分。关于通信系统安全的研究要把具体的理论与大众的具体实践相结合，更要有很好的推广。这方面，Philip Zimmermann 的研究方法可以看成是一种榜样，他致力于把公钥制的 RSA 算法带到普通人的生活中，尤其把它应用到网络用户都要使用的电子邮件的安全防范中，起到了很好的作用。

当然，关于“通信系统安全”的研究方法是多姿多彩的，这些各有特色的方法和相应的研究成果都成为这门学科日益完善的重要资料。

1.5 小　结

本章重点论述了通信系统安全这一交叉学科的几个基本问题：通信系统安全的基本定义，这门学科的主要内容，通信系统技术的相关理论和信息安全等的相关理论与技术发展对该学科的影响，该学科方向的特点，以及对该学科方向的研究所应坚持的基本方法

等，试图从这些方面来展现通信系统安全这一学科的本质特点。

思 考 题

1．通信系统安全的基本描述是什么？
2．描述通信系统性能指标有哪些？
3．C.I.A 具体指什么？
4．结合信号与系统和信息论等课程，分析如何认知信息论方法和系统论方法？

第 2 章　信息论基础

信息安全可以看作是信息论理论的一个具体分支，它的相应的理论和技术应用虽然构成相对独立的体系，但与信息理论有着非常密切的关系。信息论的具体描述：对量化了的信息进行一系列地诸如传递、存储等的处理，致使信息量变化规律等研究的总和，它是通信系统安全的重要理论基础。信息论的创立，使得加密方法等针对工程实践的技术，提升到了具体的理论高度，它不仅体现在用信息理论进行定量地分析通信系统的安全指标和安全性能，从而获得理论上的成果，更是借用信息理论，为具体设计通信系统的安全体系提供理论指导，更重要的意义还在于：针对通信系统的安全性的理论成果是信息论本身的重要组成部分，是构成经典香农信息论的重要分支，同时它为从信息理论的观点出发，自觉地用信息论的观点和方法来解决具体的实际问题。

本章重点讲述信息论中与保密通信有关的基本概念以及香农的保密定理等内容。

2.1　信息的特征

2.1.1　信息名称的历史沿革

信息（information）是一个难以确切定义的物理量，它不等同于“物质”和“能量”，但它总是与“物质”和“能量”等相伴随；它也不等同于“信号”和“消息”，但信号与消息等又与它关系密切。在不同的领域，人们对它的认知也不一样，但人人都能切切实实地感受到它的存在。一种较普遍能接受的见解就是把它写成了 information，information 是 inform 的名词形式，它的最基本的含义为“告知、通知”，这就是作为 object 的一方，有被告知相关的事情的内容情报等的含义，突出了作为 object 一方从未知某事到通过某种的作用而得到相关事情的内容情报和消息等的过程转化，这一点深刻地显示了作为信息的一个基本的特征。而近年来，把 information 翻译成中文的信息，也体现出它的合理性。首先，它非常直接地显示了与“消息”和“信号”等的区别和差异；其次，“信息”不是为翻译 information 所专门生造的，而是在传统的中文中业已出现过的词汇。这个词汇可在晚唐诗人李中的诗句中找到，他的“梦断美人沉信息，目穿长路依楼台”诗句中的信息这个词汇，就含有“音信”和“消息”的意思，这与 information 的含义就很贴切。

“信息”虽难以被确切定义，致使它作为概念的外延难以明确界定。表面看来，这是一个不小的缺陷，但实际上，正因为它的这个特点，反倒使之成为能囊括各种相关情况的一个统一而全面的表述形式，体现了该概念的开放性特征。另外，之所以把它统一地表述为信息，它必定有内在的一种独一无二的特性，这个特性可表达为事件的不确定性。

从本质上说，它是用来度量事物不确定性的一个物理量，通过信息的量度，不仅反映出事物不确定的量值的大小，更是反映出事物运动变化过程中的不确定性的变化程度的多少。除此之外，它还能表征事物差异性，具有鉴别事物本质的属性，这一点也具有根本的重要性。总之，把信息量统一地论述为用来定量描述事物的不确定性的状态和变化的物理量，由于事件的不确定性是事物本身所固有的特性，所以，信息是事物本身所具有的属性之一，与事物的本身是不可分离的。

2.1.2 信息量的描述

信息量这个概念虽早在 20 世纪 20 年代由 Fisher 所提出，但到它被真正确立并广泛传播已是香农撰写并发表了“通信的数学问题”一文以后的事了。自从信息论由香农等人创立以来，虽关于信息量的概念已有诸多的发展，但从本质上来看，信息量还没有超越自信息量、互信息量和鉴别信息量这三个基本的概念和范畴。之所以这么认定：一是在理论研究中，相比较于这三者，有关信息量的新概念迄今尚未有巨大的本质突破；二是这三者具有最广泛的应用，尤其在现代非线性信号处理中，鉴别信息准则等已经成为一种非常重要的研究方法。另一个典型的应用例子是，香农利用信息处理的研究方法，对保密通信进行了深入研究，得出了香农保密定理，并由此确定了密码学的理论基础，使传统的加密技术和工艺上升为具有严格体系的科学理论。

2.1.3 事件不确定性的概率描述

在介绍信息量的基本概念之前，先就事件的不确定性属性作些说明。首先，在概率论中，就可用连续的随机过程或离散的随机变量来表示具有不确定性的事件，而相应的不确定性就可以对应地用概率分布函数或概率密度函数来具体定量描述。因此，在确定相应的定义域后，把具体的事件和对应的概率分布函数或概率密度函数构成一个矩阵，则这种具有矩阵形式的表示方式可以形象地称为概率场。具体地，离散状况下的概率场可表示为

$$\begin{bmatrix} X \\ P \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ P_1 & P_2 & \cdots & P_n \end{bmatrix} \tag{2-1}$$

式中：$P_i \geqslant 0, \sum_{i=1}^{n} P_i = 1$，而当事件为连续的情况，这时的概率场可表示为

$$\begin{bmatrix} X \\ f(x) \end{bmatrix} = \begin{bmatrix} \mathbb{C} \\ f(x) \end{bmatrix} \tag{2-2}$$

式中：$f(x) \geqslant 0, \int_{\mathbb{C}} f(x)\mathrm{d}x = 1$。

特别地，当一维的连续状况时，则相应的概率场可表示为

$$\begin{bmatrix} X \\ f(x) \end{bmatrix} = \begin{bmatrix} [a,b] \\ f(x) \end{bmatrix} \tag{2-3}$$

其中：也需满足 $f(x) \geqslant 0, \int_{a}^{b} f(x)\mathrm{d}x = 1$。

对于多维情况时的离散状况，事件可以用随机序列和矢量来表示为$[X_1\ X_2\ \cdots\ X_L]$，其中每一个分量X_l中的元素x_l的取值为$x_l \in \{a_1,a_2,\cdots,a_n\},(l=1,2,\cdots,L)$，则对应的概率场可表示为$\begin{bmatrix}[X_1\ X_2\ \cdots\ X_L] \\ P\end{bmatrix}$，概率需要满足对应的归一性和非负性要求。

特别地，当序列长度$L=2$时，相应的描述事件不确定性的概率场可表示为

$$\begin{bmatrix}X \\ P\end{bmatrix}=\begin{bmatrix}(a_1,a_1) & (a_1,a_2) & \cdots & (a_n,a_n) \\ P(a_1,a_1) & P(a_1,a_2) & \cdots & P(a_n,a_n)\end{bmatrix} \tag{2-4}$$

式中：$P(a_i,a_j)\geqslant 0$，$\sum\limits_{i,j=1}^{n}P(a_i,a_j)=1$。

从形式上看，离散状况时和连续状况时的概率场的表示方式有所不同，但实质上它们是一致的。连续状况下的概率场表示，可以用离散状态的概率场逼近甚至转换，这一点也可以理解为连续函数离散化的一种表示方式，在数字化过程中非常重要。为了说明这个问题，举一个最简单的一维状况的例子：设$\mathbb{C}=[a,b]$，把该区间进行n等分的划分后就可以表示为$[a,b]=[a,x_1)\cup[x_1,x_2)\cup\cdots\cup[x_{n-2}.x_{n-1})\cup[x_{n-1},b]$，从而对应的概率场表示为

$$\begin{bmatrix}X \\ f(x)\end{bmatrix}=\begin{bmatrix}[a,b] \\ f(x)\end{bmatrix}\rightarrow\begin{bmatrix}[a,x_1] & (x_1,x_2] & \cdots & (x_{n-1},b] \\ \int_a^{x_1}f(x)\mathrm{d}x & \int_{x_1}^{x_2}f(x)\mathrm{d}x & \cdots & \int_{x_{n-1}}^{b}f(x)\mathrm{d}x\end{bmatrix} \tag{2-5}$$

进一步，当所取的n值足够大时，均分后的每一个小区间的长度为$\Delta,\Delta n=b-a$，每一小区间用一个值来代表，所对应的值分别记为$a_1,a_2,\cdots,a_n$，并应用积分中值定理，则连续时的概率场可完全转化为

$$\begin{bmatrix}X \\ f(x)\end{bmatrix}\rightarrow\begin{bmatrix}[a,x_1] & (x_1,x_2] & \cdots & (x_{n-1},b] \\ \int_a^{x_1}f(x)\mathrm{d}x & \int_{x_1}^{x_2}f(x)\mathrm{d}x & \cdots & \int_{x_{n-1}}^{b}f(x)\mathrm{d}x\end{bmatrix}\rightarrow\begin{bmatrix}a_1 & a_2 & \cdots & a_n \\ f(a_1)\Delta & f(a_2)\Delta & \cdots & f(a_n)\Delta\end{bmatrix} \tag{2-6}$$

这里为了表述方便，在应用积分中值定理时，把每一个小区间中密度函数所要取的自变量的值与每一小区间的代表元当作同一个值。在实际中，每一小区间中根据中值定理的要求，所得到的元素作为该个小区间的代表元，不失为一种可行的方法。

2.2 信 息 量

2.2.1 自信息量

除了用概率场表征事物的不缺性属性外，用信息量来具体定量地描述更是一种可行的好方法。下面分别从离散和连续两种状况下分别定义信息量。在离散的状况，设有一个事件所表述的概率场为$\begin{bmatrix}a \\ p\end{bmatrix}$，则定义该事件的自信息量为

$$I(a)=\log_a\frac{1}{p(a)},a>1 \tag{2-7}$$

式中：a作为对数的底数，它用来确定信息量的单位：当$a=2$时，对应的信息量的单位为bit；当$a=\mathrm{e}$时，则信息量的单位为奈特（nat）；当$a=10$时，对应的信息量的单位为迪特（det）。虽然信息量的单位各不相同，但它们的实质都是一样的，它们也由对数换底公式可以互相转换，它们的转换关系为

$1\mathrm{nat}=\log_2\mathrm{e}\approx1.43\mathrm{bit}$

$1\mathrm{det}=\log_2 10\approx3.32\mathrm{bit}$

在作为一般性的自信息量表述时，可不考虑a的具体取值，则自信息量可表示为

$$I(a)=\log\frac{1}{p(a)}=-\log p(a) \tag{2-8}$$

定义了单个事件的自信息量以后，还可以定义给定条件下的信息量的表达式：设事件a在给定条件b时的条件概率为$p(a|b)$，则对应的概率场可表示为$\begin{bmatrix}a|b\\p(a|b)\end{bmatrix}$。对应地，反映该种形式的事件的不确定性的量值定义为

$$I(a|b)=\log\frac{1}{p(a|b)} \tag{2-9}$$

在确定了单个事件的自信息量和条件信息量以后，借助于概率论中的求数学期望的方法，就可给出平均自信息量和平均条件自信息量。

设一个具有有限项的序列为$\{a_i\}$，$i=1,2,\cdots,n$，它的概率场为$\begin{bmatrix}a_1&a_2&\cdots&a_n\\P_1&P_2&\cdots&P_n\end{bmatrix}$，其中，$P_i\geqslant0,\sum_{i=1}^{n}P_i=1$，则对应的可以得到该序列的信息量场表示为$\begin{bmatrix}a_1&a_2&\cdots&a_n\\p_1&p_2&\cdots&p_n\\I_1&I_2&\cdots&I_n\end{bmatrix}$，其中$p_i\geqslant0,\sum_{i=1}^{n}p_i=1$，且$I_i=\log\frac{1}{p_i},i=1,2,\cdots,n$，求$E(I_i)$，从而得

$$E(I_i)=\sum_{i=1}^{n}p_i\log\frac{1}{p_i}=-\sum_{i=1}^{n}p_i\log p_i \tag{2-10}$$

所得到的$E(I_i),i=1,2,\cdots,n$，称为该序列的信息熵，记为$H(a)$，它的物理含义可表示为离散序列$\{a_i\}$的平均每个符号所持有的不确定度的量值，反映了一种统计平均条件下的整体不确定性。

条件熵的定义可以通过如下的途径：

首先，定义$\{a_i|b_j\},i=1,2,\cdots,n$，$j$固定值时的条件熵，该类型的概率场为

$$\begin{bmatrix}a_1|b_j&a_2|b_j&\cdots&a_n|b_j\\p(a_1|b_j)|&p(a_2|b_j)&\cdots&p(a_n|b_j)\end{bmatrix} \tag{2-11}$$

式中：$p(a_i|b_j)\geqslant0,\sum_{i=1}^{n}p(a_i|b_j)=1$，则对应的条件信息量场为