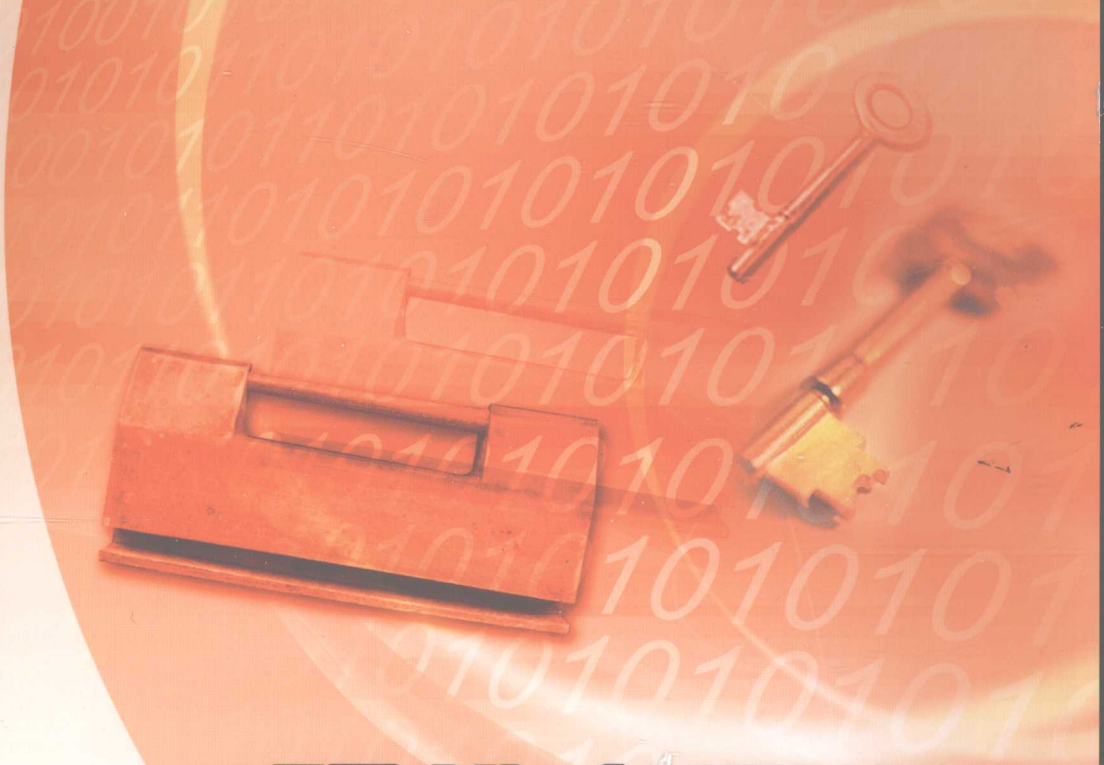

现代密码学：理论、方法与研究前沿

李顺东　王道顺　著

科学出版社
www.sciencep.com

现代密码学：

理论、方法与研究前沿

李顺东　王道顺　著

国家863高技术发展计划项目(2005AA114160、2008AA01Z419)
国家自然科学基金(60673065、60873249、90304014)
国家博士后基金(2004036248)
陕西省科技攻关计划(2008K01-58)
陕西师范大学优秀学术著作出版基金

科学出版社

北京

内 容 简 介

本书是一本现代密码学的入门书，书中系统地讲解了现代密码学研究所需要的预备知识、基础理论与研究中使用的理论工具、证明方法、协议构造方法，以及现代密码学研究的若干前沿领域。全书分 10 章， 内容包括预备知识、理论计算机科学基础、数论与代数基础、传统密码学协议的设计与分析、单向散列函数与随机性、公开密钥算法与数字签名、数字承诺、零知识证明与不经意传输、多方保密计算、量子密码学等。

本书可作为数学、计算机科学与技术、信息安全、通信等专业科研人员的参考书，也可供相关的教师、研究生参考。

图书在版编目(CIP)数据

现代密码学：理论、方法与研究前沿/李顺东，王道顺著. —北京：科学出版社, 2009

ISBN 978-7-03-023635-7

I. 现… II. ① 李… ② 王… III. 密码-理论 IV. TN918.1

中国版本图书馆 CIP 数据核字(2008) 第 195053 号

责任编辑：余 丁／责任校对：陈丽珠
责任印制：赵 博／封面设计：耕 者

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

新蕾印刷厂印刷

科学出版社发行 各地新华书店经销

*

2009 年 2 月第 一 版 开本：B5(720×1000)
2009 年 2 月第一次印刷 印张：18
印数：1—3 000 字数：344 000

定价：50.00 元

(如有印装质量问题，我社负责调换〈新蕾〉)

前　言

战争年代保密通信对于战争的胜负起着十分关键的作用。第二次世界大战中，美军正是凭借破译日本的高级密码“紫密”，击毙了日本海军大将山本五十六，扭转了美军在太平洋战场上的被动局面。同样在欧洲战场上也因为盟军破译了法西斯德国的恩尼格马密码而掌握了欧洲战场的主导权。有军事科学研究者和历史学家说：没有恩尼格马密码的破译，欧洲战场上的第二次世界大战至少还要再持续 2 年，还要再付出 2000 万人生命的代价。第二次世界大战中两个密码的破译已成为众所皆知的密码攻防战中的范例。

保密通信不仅在军事等领域发挥着独特作用，而且对当今的社会发展也日渐重要。网络信息安全问题是随着网络的发展而产生和发展的。最初设计互联网的目的是为使用者提供一种弹性、快速的通信方式。初期互联网的使用者都是一些知识层次较高，具有一定身份的人群。因为网络信息有限，网络用户比较单一，使用目的也比较单纯，所以最初的网络并不存在明显的安全问题。20 世纪 90 年代，由于商业的进入与应用的推动，互联网获得了迅猛的发展，现在网络已经无处不在、无时不在、无孔不入，人类产生了严重的互联网依赖，信息处理依靠计算机，信息通信依靠互联网，各行各业都严重依赖互联网。网络中的内容越来越丰富，网络中信息的价值也越来越大。网络用户变得异常复杂，不法之徒可能出于经济的目的、政治的目的、个人的目的等利用网络中的各种漏洞对网络实施攻击，达到自己不可告人的目的，并且造成网络瘫痪、丧失机密、丢失数据、服务质量下降等网络安全事故，造成国家、机构、组织、个人等严重的经济、政治、社会及组织形象等方面的损失。敌对国家可能通过瘫痪一个国家的通信指挥系统、经济系统，攻破保密通信系统而达到战胜、控制一个国家的目的。

因此网络安全不仅仅是一个技术问题，更是一个经济、政治问题。是否能保证网络信息安全足以影响一个国家的国家安全、经济发展、社会稳定。因此信息保障能力已经成为国家综合国力的重要组成部分，成为未来国际竞争、企业竞争的杀手锏，是国家的头等大事。没有信息安全就没有真正意义上的政治安全，就没有稳固的经济安全和军事安全，就没有完整意义上的国家安全。包括网络安全在内的信息安全问题，成为世界各国所面临的共同难题。

因为信息安全的理论基础是密码学，解决网络安全难题的根本出路在于加强密码学基础研究。加强密码学基础研究，需要培养一批既掌握密码学基本理论知识、基本研究方法，又了解密码学前沿，并能迅速进入密码学研究前沿的高级研究

人才。掌握密码学基本理论知识、基本研究方法，了解密码学研究前沿，对于刚刚进入研究的硕士研究生、博士研究生的学习和科研选题有重要的意义。

而目前，这些基础知识、研究方法与基本技能知识分散在一系列密码学基础与应用的国外学术著作与学术论文中，国内尚没有一本专门的著作进行全面的介绍。更麻烦的是这些基础知识都使用高度抽象的数学语言来叙述的，很像是数学的教科书，是大量的数学符号的堆积，没有生动具体的例子，使初学者尤其是电子信息学科的初学者理解起来非常困难，更无法体会到这些知识的思想精髓，也无法做到灵活运用。这对于繁荣我国的密码学与信息安全研究是非常不利的。要把这些知识系统总结出来，即使对于经过完整的学习、研究、提高过程历练的研究人员也需要花费数年的时间。这对于视时间如生命的科研人员来说，是一种巨大的浪费，是无可挽回的损失。由于时间的限制，这对于硕士研究生、博士研究生来说是完全不现实的。

作者经历了从初学者到高级研究人员的成长过程，称得上是一位经历了学习、总结、提高、应用等完整历练过程的密码学工作者。在这个过程中逐渐领悟了一些密码学思想的精髓，掌握了密码学的基础知识，学会了基本的研究方法。在这个成长过程中曾得到国家 863 高技术发展计划项目 (2005AA114160、2008AA01Z419)、国家自然科学基金 (60673065、60873249、90304014)、国家博士后基金 (2004036248)、陕西省科技攻关计划 (2008K01-58)、陕西师范大学优秀学术著作出版基金、安全部科研项目、北京师范大学青年基金等项目的支持。在此向 863 高技术发展计划项目、国家自然科学基金、国家博士后基金、陕西省科技攻关计划等表示衷心的感谢。作者曾就读于西安交通大学、四川大学，并在清华大学做博士后研究，博士后出站曾在清华大学工作，先后在北京师范大学、陕西师范大学从事教学与科研工作，得到了许多密码学前辈的帮助和指导，得到我的博士生导师覃征教授 (西安交通大学)、杨路教授 (中国科学院成都计算机应用研究所)、齐东旭教授 (北方工业大学)、博士后合作导师戴一奇教授，以及清华大学、北京师范大学、陕西师范大学的各位老师的指导和帮助，在此对他们表示衷心的感谢。

在这个成长过程中，作者积累了许多研究的基础理论、基本方法、基本技能方面的知识、心得，作者愿意认真总结并配以生动具体的例子或者故事作为著作出版，作为密码学研究的入门书，与密码学研究者分享。计算机出身的研究者在看到密码学书籍中许多形式化描述时往往感到恐惧，为了使他们不再恐惧，本书在引入密码学中常见的形式化描述之前，都先给出形式化描述简明的物理解释。根据作者的经验，一旦了解了形式化表示的背景和物理意义，再理解形式化表示就是非常容易的事了。此外本书用生动的语言和有趣的故事介绍深奥的数学原理，既保持理论的严谨性，又使得读者更容易理解。为了使读者对密码学基础知识、基本方法不但知其然，更知其所以然，本书力求在对概念进行形式化叙述时，首先给出问题的背

景、概念的直观意义，提出这个概念的初衷以及它在实际中的应用，给出数学表述的物理解释，使形式化的描述更易于理解。相信本书的出版对于密码学的初学者、初级研究人员的成长有一定的帮助，对于密码学知识的普及，对于我国信息安全人才的培养，对于保证我国的信息安全具有一定的意义。

本书可作为密码学、应用数学、计算机、信息安全等专业的研究生教材，也可以作为有关研究人员的参考书。本书特别适合计算机专业的本科生、研究生学习现代密码学的需要。由于时间和作者的水平所限，书中不妥之处在所难免，恳请读者提出宝贵意见。

目　录

第1章 预备知识

现代密码学主要是建立在理论计算机科学、数论、代数、函数论与概率论等基本科学的基础上的。由于密码学所需要的理论计算机科学 (或者称为可计算性与计算复杂性理论) 和数论的知识比较系统，也比较多一点，所以专门用两章的篇幅介绍这两方面的知识。而需要的其他方面的知识虽然比较杂但都不多，所以将这些知识合起来放在第 1 章进行介绍。本章主要包括集合、函数、概率论和证明方法的内容。

1.1 集合、元组与数制

1.1.1 集合与元组

集合是现代科学中一个非常重要的概念。集合就是任何一个有明确定义的对象的整体。这些对象称为集合的元素或者成员。有明确定义是指能够确定一个具体的对象是否属于该整体。几乎所有的数学对象，不管它可能有什么附加的性质，它们首先都是集合。因此从某种意义上说，集合论实际上成为构建一切数学知识的基础。描述一个集合的最直观的方法就是在一对括号内列出集合的所有元素，比如所有小于 4 的正整数的集合可以用 $\{1,2,3\}$ 来表示。

用列出集合中所有元素的方法来描述一个集合，有时是极不方便的或是不可能的 (比如要用这种方法列出所有自然数的集合)。于是引入另一种有用的方法，通过详细说明集合的元素所具有的某种共同性质来定义一个集合，例如 $Z^+ = \{x|x是正整数\}$。用 $a \in S$ 表示 a 是 S 的元素，用 $a \notin S$ 表示 a 不是 S 的元素，或者说 a 不属于 S。没有任何元素的集合称为空集。$R = S$ 表示两个集合恰好有相同的元素。如果 R 的每个元素也是 S 的元素，那么称 R 是 S 的子集，记作 $R \subseteq S$。如果 R 是 S 的子集，S 也是 R 的子集，即 $R \subseteq S$ 且 $S \subseteq R$，那么就说 $R = S$。证明两个集合 $R = S$ 的方法首先要证明 R 的任何一个元素 x 都是集合 S 的元素，接着再证明 S 的任何一个元素 y 都是集合 R 的元素。

注意到集合中的元素没有任何顺序的限制，因此 $\{a,b,c\} = \{c,b,a\} = \{b,a,c\}$，也就是说可以选择任意的顺序写出集合中的元素。当顺序比较重要时，把它说成是 n 元组或者表。n 元组用小括号而不是用大括号表示，即

$$(a_1, a_2, \cdots, a_n)$$

集合与元组的区别是集合中不能有相同的元素，n 元组中的元素则可以相同。

如果 $S_1, S_2, \cdots, S_n$ 是给定的集合，则用 $S_1 \times S_2 \times \cdots \times S_n$ 表示由所有 n 元组 $(a_1, a_2, \cdots, a_n)$ 组成的集合，其中 $a_1 \in S_1, a_2 \in S_2, \cdots, a_n \in S_n$。有时称 $S_1 \times S_2 \times \cdots \times S_n$ 为 $S_1, S_2, \cdots, S_n$ 的笛卡儿集。

1.1.2 函数

函数的概念在纯数学与应用数学的每个分支中都是非常重要的，在现代密码学中也是最重要的概念。函数有很多种定义方式，中学所学习的函数的定义是大家都熟悉的函数定义，高等数学中函数的定义与中学数学中函数的定义有很大的不同，也是大家所熟悉的函数的定义。离散数学从集合论的角度研究函数，将函数定义为一种特殊的关系，自变量与因变量的取值范围也扩展到某两个具体的集合。这也是每个学习计算机科学与技术的读者都熟悉的函数定义。这里从计算机理论的角度给出一个新的函数的定义，这里的定义比数学中的函数概念的外延要广泛得多。

定义 1.1　函数 f 就是一个集合，它的所有元素都是满足下面的特殊性质的一个有序对

$$(a,b) \in f \text{ 且 } (a,c) \in f \text{ 蕴含 } b = c \tag{1.1}$$

直观上，将有序对看作一个表的两行更好理解一些。如果这样看待，那么就成为中学所学的函数列表法表示。对于函数 $(a,b) \in f$，人们一般习惯于用 $f(a) = b$ 来表示。根据函数的定义对于每一个 a 至多存在一个这样的 b 使得 $b = f(a)$。使 $f(a)$ 有定义的所有 a 的集合称作函数 f 的定义域。对于 f 的定义域中的所有 a，所有的 $f(a)$ 组成的集合称为 f 的值域。理论计算机只研究数论函数，即定义域为自然数的集合的函数。而密码学研究的函数是定义在某些字符串的集合上的函数。

在计算机科学中研究的函数通常用从 a 到 $f(a)$ 的过程的算法来确定。确定一个具体的函数的方法在计算机科学中非常重要。然而，有时完全可能有一个算法，它规定了一个函数，但是却不能确定函数的定义域。在这种情况下，为了方便研究工作引入部分函数的概念。集合 S 上的部分函数是以 S 的子集为定义域的函数。理论计算研究的函数都是在 N 上的函数，但很多并不是在整个 N 上都有定义，而只是在 N 的某个子集上有定义。例如作为数论函数 $g(n) = \sqrt{n}$ 是集合 N 上的部分函数，其定义域是完全平方数的集合。如果 f 是集合 S 上的部分函数，而且 $a \in S$，用 $f(a)\downarrow$ 表示 a 在 f 的定义域中，并且说 $f(a)$ 是有定义的。如果 a 不在 f 的定义域中，则记作 $f(a)\uparrow$，并且说 $f(a)$ 没有定义。如果 S 上的部分函数的定义域是 S 则称它是全函数。对于函数 $(a,b) \in f$，由 a 计算 b 的过程称为函数的计算过程，而如果给定 b，根据函数 f 计算 a 的过程，称为函数的求逆过程，记作 $b = f^{-1}(b)$。

除了上述的一元函数 $f(x)$ 外，还有二元函数 $f(x,y)$ 与多元函数 $f(x_1,\cdots,x_n)$，这些函数在密码学中都有应用。密码学的所有内容都与函数有密切的关系，密码学的各种应用都是建立在对函数的特性充分理解、巧妙运用的基础上的。

信息的加密最初就是一种一元函数 $y=f(x)$ 运算，将要加密的信息作为自变量，而函数的输出作为加密的结果。用这样的加密过程，如果要保证消息的机密性，就必须保证函数 f 的机密。但这样的方法有许多缺点，如何改进这样的加密方法，密码学家们从二元函数的 $f(x,y)$ 的性质找到了解决方案。这是因为 $f(x,y)$ 的值是由 x 和 y 共同决定的，如果要计算 $f(x,y)$ 的值，必须同时提供两个输入 x 和 y。在这样的函数中把要加密的消息作为输入 x，另一个输入 y 用密钥来代替，这样计算 $f(x,y)$ 的过程就变成是具有密钥的加密。加密用的函数必须是可逆的，只有这样才能够在接收方解密出相应的消息进行阅读。要解密出相应的消息 x，必须提供 y。这样如果不知道 y 的值，即使知道 f 的表达式或者计算的程序，也不能解密相应的消息。因此函数以及表示该函数的相应算法就可以公开。这就是现代密码学的基本思想。

有的函数 $f(x)$ 具有这样的性质，给定 x 计算 $f(x)$ 的值非常容易，而给定 $f(x)$ 的值，要求对应的 x 则非常困难。这样的函数一般称为单向函数，单向函数是密码学中一个主要的研究课题，在消息的完整性保护、消息认证、数字签名等方面都有重要的应用。有的单向函数如果提供某一个额外的参数，单向函数的求逆就变得非常容易。这就是所谓的限门单向函数，密码学中的公开密钥加密、数字签名等都是利用函数的这种性质。

1.1.3　谓词

定义 1.2　集合 S 上的谓词 (predicate) 或者布尔函数，是指 S 上的全函数 P，对于每个 $a\in S$ 有

$$P(a)=\text{TRUE}\ \text{ 或者 }\ P(a)=\text{FALSE}. \tag{1.2}$$

其中 TRUE 和FALSE是一对称作真值的不同对象。当 $P(a)$ =TRUE 时，就说 $P(a)$ 为真；而当 $P(a)$ =FALSE时，则说 $P(a)$ 为假。如果令TRUE=1，FALSE=0，那么谓词就变成在 N 中取值的一类特殊函数。

如果 P,Q 是集合 S 上的谓词，那么 $\neg P, P\vee Q, P\wedge Q$ 也是集合 S 上的谓词。恰好当 P 为假时，$\neg P$ 为真。当 P,Q 同时为真时，$P\wedge Q$ 为真。当 P 为真或 Q 为真，或 P,Q 同时为真时，$P\vee Q$ 为真。

1.1.4　数制与字符串

字母表是称作符号的对象的有穷非空集合 $A=\{s_1,s_2,\cdots,s_m\}$。A 中符号的 n 元组 $(a_1,a_2,\cdots,a_n)$ 称作 A 上的字或字符串。把 $(a_1,a_2,\cdots,a_n)$ 简单地写作

$a_1a_2\cdots a_n$。如果 $u=a_1a_2\cdots a_n$，则称 u 的长度为 n 并记作 $|u|=n$。字母表 A 上所有字组成的集合记作 A^*。A^* 的任何子集称为 A 上的语言或字母表为 A 的语言。如果 $u,v\in A^*$，则用 uv 表示将字符串 v 放在字符串 u 后所得到的字符串。

字符串和数字有非常密切的关系，我们遇到的数制有十进制、二进制、六十进制、二十四进制等。在十进制数中如果令字母表 $A=\{0,1,2,3,4,5,6,7,8,9\}$，那么所有的十进制数实际上都是该字母表上的字符串。同理二进制数都是字母表 $A=\{0,1\}$ 上的字符串。而日常生活中都用十进制数，在计算机科学中都用二进制数。那么字符串和数有什么关系呢，当字母表确定以后，字符串和自然数可以就建立起一一对应的关系。这种一一对应提供了很大的方便，使得研究者能够把文字同数字一样进行处理，而处理数字则是计算机的优势。

那么数字和字符串是怎样一一对应的呢？以十进制数为例，众所周知 13852 就表示自然数的 13852，但如果把它看作字母表 $A=\{0,1,2,3,4,5,6,7,8,9\}$ 上的字符串，那么如何计算出这个字符串所表示的数呢？因为这个字符串的字母表有 10 个字符，而

$$2\times10^0+5\times10^1+8\times10^2+3\times10^3+1\times10^4=13852$$

同理二进制数 10010110 是字母表 $\{0,1\}$ 上的字符串，它表示的数是

$$0\times2^0+1\times2^1+1\times2^2+0\times2^3+1\times2^4+0\times2^5+0\times2^6+1\times2^7=150$$

一般来说，假设字母表 $A=\{s_1,s_2,\cdots,s_n\}$ 的顺序是固定不变的，A 上的字符串 $s=a_ka_{k-1}\cdots a_0$ 所表示的数为

$$x=a_k\times n^k+a_{k-1}\times n^{k-1}+\cdots+a_1\times n+a_0 \tag{1.3}$$

字符串 s 称作式 (1.3) 所定义的数 x 的以 n 为底的记法。可以证明这种对应是一一对应的，即给定一个字符串可以利用式 (1.3) 求出该字符串所关联的数，反之给定一个数也可以求出它所对应的字符串。

使用数字的以 n 为底的记法，仅当 $n\geqslant2$ 时才是有用的，而用式 (1.3) 表示数的方法甚至当 $n=1$ 时仍然有效。对于由单个符号 1 组成的字母表，长度为 l 的字符串所表示的数是

$$\sum_{i=0}^{l-1}1\cdot1^i=\sum_{i=0}^{l-1}1=l$$

在实际应用与科学研究中究竟采用以多少为底的记法实际上是有一定随机性的，可以根据方便实用的原则采用任意数为底的记法。因为古代都是屈指计数，运用以十为底的记法就是自然而然的了，这是从方便应用出发来选择数制的。而在计

算机科学中，因为许多物理量可以有两种状态，很容易用这些物理量来表示二进制数，且这样的器件也很容易制造，所以从方便应用出发计算机科学中广泛采用二进制。

在实际应用中，任何以 $n \geqslant 2$ 为底的记法都是合理的，因为这样要表示 x，需要的字符串的长度为 $\log_n x$，这样计算、处理、记录的效率都比较高。以 1 为底的记法是不合理的，因为以 1 为底的表示方法，要表示 x 需要的字符串长度为 x，这样计算、处理、记录都很不方便，效率很低。但是在密码学中有许多地方用一进制来表示一个数，这主要是为了某些叙述的方便。比如说一个算法 A 接受输入 n，在 $\mathrm{poly}(n)$ 步之内停机并输出 $1^{f(x)}$ 就蕴含着 $f(x) \leqslant \mathrm{poly}(n)$，即 $f(x)$ 是多项式时间可计算的。但如果不用一进制表示，要表达这样的意思就很繁琐。

1.2　概 率 基 础

1.2.1　概率的概念

概率论在现代密码学中也起着重要的作用，因为现代密码学的安全定义都是基于计算复杂性方面的定义。现代密码学的一个基本思想是“虽然不能保证有足够计算能力的攻击者无法攻破一个密码系统，但要保证具有有限计算能力限制的攻击者攻破密码系统的概率非常的低。”所以到底攻破系统的概率低到什么程度，这就必须借助于概率论的知识进行分析，故而概率论在密码学中有重要的应用，幸运的是，虽然概率论在密码学中非常重要，但密码学中需要的概率论的知识并不多，只是一些最基本的概念和一些常用的不等式。本小节对这些知识进行简单的整理，罗列如下。

1. 随机试验

在现实中有许多实验的结果是无法控制的，在反复进行试验时无论采用什么办法都无法保证每次实验能够产生相同的结果。例如，如果抛一枚硬币，并不能确定所得到的结果是正面还是反面。这类试验称为随机试验。与此相反，结果能够确定的实验称为确定性试验。

2. 样本空间

一个实验中可能出现的一个结果称为一个样本点。所有可能出现的结果所组成的集合 Ω 称作该试验的样本空间。例如抛一枚硬币的样本空间 $\Omega = \{$ 正面, 反面 $\}$，其中正面和反面各为一个样本点。

3. 事件

样本空间中的任何一个子集称作一个事件。样本空间的每一个元素称为一个