doi:10.3969/j.issn.1000-436x.2014.z2.028

知识安全研究初探

闫世杰[1]，闵乐泉[1]，范修斌[2]
（1. 北京科技大学 自动化学院，北京 100083；2. 北京博文广成信息安全技术有限公司，北京 100095）

摘 要：在借鉴有关文献的基础上，给出了数据、大数据、信息以及知识的形式化定义，提出了知识安全的机密性、完整性、可用性、可控性、可认证性、可传承性以及抗白化性等 7 大属性。给出了 7 大属性的形式化描述和各属性的相关保护技术。讨论了大数据与中心极限定理的关系，提出了安全知识系统的概念。
关键词：数据；大数据；信息；知识；知识安全；安全知识系统
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0203-10

Research on the knowledge security

YAN Shi-jie[1], MIN Le-quan[1], FAN Xiu-bin[2]
(1.School of Automation and Electrical Engineering , University of Science and Technology Beijing, Beijing 100083, China;
2. Beijing Bowen Guangcheng Information Security Technology Ltd., Beijing 100039, China)

Abstract: Based on previous researches, the formal definitions of data, huge data, information and knowledge is given, seven attribute for knowledge security are proposed: confidentiality, integrity, availability, controllability, verifiability, inheritability, and anti- whiteness and related prevention technology, the relation between huge data and the center limit theorem is discussed, the concept of secure knowledge system is introduced.
Key words: data; big data; information; knowledge; knowledge security; secure knowledge system

1 引言

当前网络空间已成为人类知识发现、知识共享、知识交流、知识传递、知识学习、知识创新、知识利用、知识传承等最大的平台。通过进行知识的发布、查询、获取以及评议成为包括草根阶层在内的异质性知识行动者通达知识的新路径[1]。但由于网络空间的特性以及潜在的安全隐患，进而给现代社会的正常发展带来了一系列前所未有的知识安全问题。

知识工程[2]以知识为处理对象，主要研究知识系统的知识发现、知识获取、知识表示、知识处理、知识应用等，知识系统包括专家系统、知识库系统、智能决策系统等；知识管理[3]是对知识获取、存储、学习、共享与创新等进行管理过程；知识安全[4]则是研究知识工程与知识管理过程中的安全问题。近年来，知识工程领与知识管理领域的发展十分迅速，取得了许多新的重要成果，但知识安全领域的研究还处于比较新的研究领域。2007 年美国出版的《知识安全管理》中指出知识安全研究是知识管理与信息安全相互交叉的热点领域（如图 1 所示）[4]，应该像对待信息安全一样重视知识安全的问题。中国科学院大学吕述望教授多年从事知识安全的研究，在文献[5, 6]中指出当前网络空间中存在知识表达、知识创新、知识传承、知识传递、知识存储、知识利用、知识挖掘、知识泯灭等方面的安全问题。如果不充分重视知识安全，将带来知识白化、公民丑化、知识创新产权失控、国家资源不清、知识恶性使用、知识退化、知识失传等严重的问题。面对上述问题，仅靠数据安全与信息安全已有的安全属性（如机密性、完整性、可用性、可控性、可认证性等）是不能解决的，例如解决不了知识的失传、

收稿日期：2014-11-28
基金项目：国家自然科学基金资助项目（61074192, 61170037）
Foundation Item: The National Natural Science Foundation of China (61074192, 61170037)

知识的白化等问题。信息安全传统的安全属性主要是侧重语法安全的，因此有必要把语法安全延伸到语义安全的范畴即知识安全的研究，这是当前迫切之需求。

图 1 知识安全—知识管理与信息安全的交集

知识安全是网络空间继数据安全、信息安全、网络安全后一个新的安全需求，由于知识的重要性、特殊性，已有的数据保护技术与信息安全保障技术已无法满足知识安全的要求。当前人们往往把数据、信息、知识混为一谈，知识安全也在一些学者的著作中不加定义地被直接使用。网络空间中信息、知识是抽象的，数据是具体的，数据是信息与知识的载体，大数据是知识发现的重要资源，因此数据安全是信息安全知识安全之基础，研究知识安全需以数据及数据安全为基础。南开大学曾伟忠博士在其论文中讲到，知识安全学科交叉性、边缘性强，应用领域面宽，是一个庞大的学科群体系，它是一个以知识安全为核心，以知识技术学、知识工程学和知识管理学为支撑，以国家和社会各领域知识安全防护为应用方向的跨学科的交叉学科群体系[7]。本研究在已有数据定义的基础上给出了数据、大数据及数据安全的形式化定义，并讨论了大数据与中心极限定理的关系；试图在数据安全、信息安全、知识工程、知识管理、知识理论等的基础上给出知识安全的微观、中观、宏观研究内容。

2 数据与数据安全

文献[8]指出，对数据进行分析的最重要目的就是获得知识、利用知识。由于大数据中蕴含大量的原始、真实信息，对网络空间中的大数据进行分析，能够有效地摒弃个体差异，帮助人们透过现象，更准确地把握事物背后的规律，基于挖掘出的知识，可以更准确地对自然或社会现象进行预测，同时更好地为人类社会发展所服务。网络空间中数据是信息、知识的载体，是知识处理的核心。数据支撑着运算、推理、比较、分析以及决策等理性活动，应用非常广泛。由此可以看出网络空间数据安全真实性、完整性是知识安全之基础。当前越来越多的组织认识到数据安全特别是大数据安全的重要性。

2.1 数据的定义

当前，计算机数据主要有 2 种类型：即静态数据（存储数据）、动态数据（计算数据）[9]。在计算机和信息科学不同分支领域的理论研究者和实际工作者以各自不同的方式理解和使用着“数据”这个词，对其定义还没有形成一致的意见。在大多数论述数据的场合中都不提及数据的定义，而是笼统的使用它。也有些人把它看作是信息的同义词。尽管如此，由于数据本身的重要性和广泛性，人们还是给出了多种定义。本文在文献[10, 11]的基础上，从概率论、数理统计出发，给出大数据的形式化定义。

定义 1（随机变量[12]）一个概率空间$(\Omega,\mathcal{F},p)$中的概率可测函数X，即为一个随机变量，其中$\mathcal{F}$是一个σ-代数，p是概率侧度。

显然，常量是随机变量的特例。

定义 2（样本[13]）随机变量的一次取值称为样本。

借鉴文献[12]，给出关于数据的如下定义。

定义 3（数据）数据是随机变量的样本的数字刻画。

如果随机变量的取值空间就是数字空间，则随机变量的样本即为数据。在不至于混淆的情况下，给出如下定义。

定义 4（数据）数据即为随机变量的样本。

由定义 2 以及定义 4，给出大数据的数学刻画。

在上述概念的基础上，结合文献[14~16]，给出“大数据”的刻画。

定义 5（比特流数据）设$X=(X_0,X_1,X_2,\cdots,X_{n-1})$，其中，$X_i$是取值于二元域[17,18]$F_2$的随机变量序列，设其一个样本为

$$(X=x)=(X_0=x_0,X_1=x_1,X_2=x_2,\cdots,X_{n-1}=x_{n-1})$$

则称X为比特流数据。

由于比特是计算机最小的编码单元，因此任何计算机数据都可以比特数据流化。

定义 6（大数据）设$X=(X_0,X_1,X_2,\cdots,X_{n-1})$，其中，$X_i$是取值于二元域[17,18] F_2的随机变量序列，设其一个样本为

$$(X=x)=(X_0=x_0,X_1=x_1,X_2=x_2,\cdots,X_{n-1}=x_{n-1})$$

如果$n\geqslant 8\times 1\,024\times 2^{40}=2^{53}$ bit，则称该数据为大数据。其中，8 为字节数，8×2^{40}是一个 T 的数据，1 024 是指千 T 以上的数据。

当前天河二号的每秒比特计算量为 $(10^8)^2 = 10^{16} \approx 10\times 2^{50} \approx 2^{53.3}$，也就是说大数据的下限与当今世界最快超算量级是对应的。超算与大数据时空上的匹配性，应该不是巧合。

2.2　大数据与中心极限定理

随着云计算、云存储、4G 网络、物联网、移动通信网的发展，大数据时代已经到来。面对大数据，虽然使数据挖掘工程专家面临计算复杂度的挑战，但是为概率统计专家提供了广阔的天地。究其重要的原因之一即为中心极限定理。

定义 7[19]　设 $F_n(x)(n=1,2,\cdots)$，$F(x)$ 分别为随机变量 $\xi_n(n=1,2,\cdots)$ 及 ξ 的分布函数，若对于 $F(x)$ 的任一连续点 x 有 $\lim\limits_{n\to\infty}F_n(x)=F(x)$，则称随机序列 $\{\xi_n\}$ 依分布收敛于 ξ，并称 $F(x)$ 为 $\{F_n(x)\}$ 的极限分布函数。

定义 8[19]　设 $\xi_n(n=1,2,\cdots)$ 为相互独立的随机变量序列，有有限的数学期望和方差 $E(\xi_k)=a_k$，$D(\xi_k)=\sigma_k^2(k=1,2,\cdots)$。

令

$$\left.\begin{aligned} B_n^2 &= \sum_{k=1}^{n} D(\xi_K) \\ \eta_n &= \sum_{k=1}^{n}\frac{\xi_k - a_k}{B_n} \end{aligned}\right\}(n=1,2,\cdots)$$

若对于 $x\in R_1$ 有

$$\lim_{n\to\infty} P\{\eta_n < x\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} \mathrm{e}^{-\frac{1}{2}y^2}\,\mathrm{d}y$$

则称随机序列 $\{\xi_n\}$ 服从中心极限定理。

定理 1[19]　设 $\xi_n(n=1,2,\cdots)$ 为相互独立同分布的随机序列，且

$$\mathrm{E}(\xi_k)=a$$

$$D(\xi_k)=\sigma^2<\infty(\sigma^2\neq 0)$$

$$k=1,2,\cdots$$

则 $\{\xi_n\}$ 服从中心极限定理。

定理 2　（Beery-Esseen 不等式[20,21]）设 $\xi_n: n\geqslant 1$ 相互独立同分布的随机变量

$$\mathrm{E}(\xi_n)=0, \mathrm{E}(\xi_n^2)=\sigma^2, \mathrm{E}(|\xi_n|^3)<\infty$$

则

$$\sup_{-\infty<x<\infty}\left|P\left\{\frac{1}{\sigma\sqrt{n}}\sum_{k=1}^{n}\xi_k<x\right\}-\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}\mathrm{e}^{-\frac{1}{2}y^2}\mathrm{d}y\right|\leqslant A_2\frac{\mathrm{e}}{\sqrt{n}}$$

其中，A_2 是小于等于 0.788 2 的正常数。

由上述定理以及大数据的定义 6，易得如下性质。

性质 1　设 $X=(X_0,X_1,X_2,\cdots,X_{n-1})$，$X_i$ 是取值于二元域 F_2 上的相互独立均匀分布的随机变量序列，且 $n\geqslant 8\times 1\,024\times 2^{40}=2^{53}$ bit，令 $\xi_i=(-1)^{X_i}$，$0\leqslant i\leqslant n-1$，则

$$\sup_{-\infty<x<\infty}\left|P\left\{\frac{1}{\sqrt{n}}\sum_{k=1}^{n}\xi_k<x\right\}-\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}\mathrm{e}^{-\frac{1}{2}y^2}\,\mathrm{d}y\right|$$

$$\leqslant A_2\frac{\mathrm{e}}{\sqrt{n}}\leqslant 0.788\,2\frac{\mathrm{e}}{\sqrt{2^{53}}}$$

由性质 1 可知，在大数据条件下，若是相互独立均匀分布的随机变量序列的样本，统计量 $\frac{1}{\sqrt{n}}\sum_{k=1}^{n}\xi_k$ 是以不超过 $0.788\,2\frac{\mathrm{e}}{\sqrt{2^{53}}}$ 的误差一致接近标准正态分布的。也就是说在大数据条件下，在进行知识挖掘时，为消除噪声以及波动影响，提供了坚实的基础。

2.3　数据安全属性形式化

数据安全机密性（confidentiality）是指限定能够观看数据的合法对象，或者说，数据的内容对非合法对象是不能获取或即使获取也是不能理解的[22]。比如，机密性保护措施应当能够防范攻击者通过截获总线信号而理解总线数据所表达的具体内容。通常，机密性保护是一种“阻断”措施，即阻止攻击者对数据的非法获得与理解。其形式化描述如下。

定义 9　（数据安全机密性属性形式化）

若 $\forall a\in A, C(d,a)=1, \forall b\in \bar{A}, C(d,b)=0$，其中，$A$ 是数据 d 的授权可读集合，C 是机密性度量，则称数据 d 满足数据安全机密性属性。

在数据的产生、传输、存储、应用等方面，都要保证 $C(d,a)=1, C(d,b)=0$，才能实现数据机密性属性。数据安全机密性属性保护物理技术，主要有防侦收（是对手侦收不到有用的信息）、防辐射（防止有用信息以各种途径辐射出去）、限制、隔离、掩蔽等措施。数据安全机密性属性保护密码技术，主要有序列密码、对称密码、公钥密码等。可参照国家给出的相应具体密码算法标准。数据安全机密性属性保护访问控制技术，主要有 BLP 模型[23~26]、防隐蔽信道技术等。

数据安全完整性（integrity）是指要求数据不在未经授权的情况下被修改或者丢弃[27]。即数据的接收者能够验证数据在存储或传输过程中数据的安

全性，防止数据被非授权用户篡改，使数据保持原始性和真实性。其形式化描述如下。

定义 10 （数据安全完整性属性形式化）

$I(S(d))=I(d)$，则称数据 d 满足数据安全完整性属性，其中 S 是指对数据 d 的任何处理算子，包括：传输、备份、复制、应用等，I 是数据 d 的完整性度量。

数据安全完整性属性要求数据不致受到各种原因的破坏。影响网络空间数据安全完整性的主要因素有设备故障、误码（传输、处理和存储过程中各种干扰源造成的误码）、人为攻击、计算机病毒等。保障数据安全完整性的主要技术有协议、纠错编码方法、密码校验和方法、数字签名、公证等。数据安全完整性属性保护访问控制技术主要有 Biba 模型[28,29]等。

数据安全可用性（availability）是数据可被授权实体访问并按需求使用的特性[30]。其形式化描述为如下。

定义 11 （数据安全可用性属性形式化）

$\forall n\in N, A(n,d)=1$，其中 N 是用户的对数据 d 应用需求集合，则称数据 d 满足数据安全可用性属性。若 $\exists n\in N, A(n,d)=0$，则称数据 d 不满足可用性，其中 A 为对数据 d 可用性度量。支持数据安全可用性的常用技术包括访问控制技术、负载均衡技术、身份鉴别技术、防病毒木马技术、异地备份技术等。

综上所述，静态数据在存储过程中不需要参与运算，数据的机密性、完整性、可靠性以及隐私保护等是用户对于存储数据关注的核心安全问题。目前，对静态数据的保护主要基于密码学技术；动态数据则仅利用加密技术保护十分困难，目前对密文数据直接操作的“全同态加密”执行效率距离实际可用相差很远，因此，数据在运算时依然要解密驻留在内存中，很难利用密码学技术进行完整的保护。对动态数据的保护多基于安全策略模型和机制进行，例如访问控制模型和机制、沙箱机制等。

3 信息与信息安全

3.1 信息的定义

信息作为一个科学术语被提出和使用，可追溯到 1928 年维哈特利在《信息传输》一文中的描述：信息是指有新内容、新知识的消息。1948 年，香农博士在《通信的数学理论》[31]中给出了信息定义，是信息科学发展史上的里程碑。香农在进行信息的定量计算的时候明确地把信息定量为随机不确定性之差。这表明了香农应用信息定义，减少随机不确定性，他还用了一个专门的词语“熵”来定义不确定性。香农的定义也可以表述为信息就是能够使熵减少的东西。事实上，不确定性是香农定义中最重要的一个特征。根据这一思想，法裔美国科学家 L.Brillouin 在他的名著《科学与信息论》中就直接指出：信息就是负熵。1950 年，控制论的奠基人维纳（Winner）出版的《控制论与社会》[32]一书中也曾经指出，正如熵是无组织程度的度量一样，消息集合所包含的信息就是组织程度的度量。事实上，完全可以将消息所包含的信息解释为负熵。本文借鉴上述思想，给出如下信息定义。

定义 12 （信息）信息是一个随机变量蕴含的另一个随机变量的确定性。也就是说，随机变量的样本即数据，蕴含变量之间的互信息，这是知识挖掘的理论基石。

定义 13[33] （信息熵）设 X 为取值于非空有限集合 S 的随机变量，则其随机性度量即信息熵

$$H(X)=-\sum_{i\in S}P(X=i)\mathrm{lb}(P(X=i))$$

定义 14[33] （联合熵定义）

$$H(X,Y)=-\sum_{i,j}P(X=i,Y=j)\mathrm{lb}P(X=i,Y=j)$$

定义 15[33] （条件熵）

$$H(Y\mid X)=\sum_{i}P(X=i)H(Y\mid X=i)$$

当 2 个随机变量有关系时，已知一个随机变量的取值后，另一个随机量熵一般是变小的，也就是说，另一个变量的确定性增加。

定义 16 （互信息熵）

$$p(X=i,Y=j)\mathrm{lb}I(Y;X)=\sum_{i}\sum_{j}\left(\frac{p\left(X=i,Y=j\right)}{p\left(X=i\right)p\left(Y=j\right)}\right)$$

由互信息熵可知，利用一个随机变量的取值，可平均得到另一个随机变量的多少信息。

性质 2[33] （熵之间的关系）

$$I(X;Y)=H(X)-H(X\mid Y)$$
$$I(X;Y)=H(Y)-H(Y\mid X)$$
$$I(X;Y)=H(X)+H(Y)-H(X,Y)$$
$$I(X;Y)=I(Y;X)$$
$$I(X;X)=H(X)$$

设 Y 也是概率空间 $(\Omega,\mathcal{F},p)$ 上一个随机变量，

是要从比特数据流样本

$$(X=x)=(X_0=x_0,X_1=x_1,X_2=x_2,\cdots,X_{n-1}=x_{n-1})$$

要挖掘的信息的随机变量，则能够得到的信息，有定义 12，即为 X 中包含的关于 Y 的信息，即定义 16 中的互信息。但是由样本 $(X=x)=(X_0=x_0,X_1=x_1,X_2=x_2,\cdots,X_{n-1}=x_{n-1})$ 挖掘 Y 的信息的算法复杂度一般是 NP 的，也就是说一般的挖掘算法所能挖掘出的关于 Y 信息是小于等于上界，即 $I(X,Y)$ 的；当然该信息是条件信息的数学期望，在一定的附加条件下，可能会大于平均值，此即为条件熵 $I(Y,X\mid Z)$。

3.2　信息安全属性形式化

信息安全机密性是指信息对于授权用户或实体是能够获得并确定的。对于非授权用户是不能获得或即使获得也不能理解信息内容的。根据数据安全机密性属性形式化描述，信息安全机密性属性形式化描述如下。

定义 17　（信息安全机密性属性形式化）

若 $\forall a\in A,C(i,a)=1,\forall b\notin A,C(i,b)=0$，则称信息 i 满足信息安全机密性属性，其中 A 是信息 i 的授权可读集合，C 是信息的机密性量。

信息的产生、传输、存储、应用等方面，都要保证 $C(i,a)=1,C(i,b)=0$，才能实现信息机密性属性。

信息安全完整性（integrity）是指要求信息不在未经授权的情况下被修改或者丢弃[27]。

借鉴数据安全完整性形式化描述，给出信息安全完整性形式化描述为

定义 18　（信息安全完整性属性形式化）

$I(S(i))=I(i)$，则称信息 i 满足信息安全完整性属性，其中 S 是指对信息 i 的任何处理算子，包括传输、备份、复制、应用等，I 是信息 i 的完整性度量。

信息安全可用性是信息可被授权实体访问并按需求使用的特性[30]。

借鉴数据安全可用性形式化描述，给出信息安全可用性形式化描述如下。

定义 19　（信息安全可用性属性形式化）

$\forall n\in N,A(n,i)=1$，其中 N 是用户的对信息 i 应用需求集合，则称信息 i 满足信息安全可用性属性。若 $\exists n\in N,A(n,i)=0$，则称信息 i 不满足可用性。A 为可用性度量。

信息安全可控性（controllability）是指能够对信息进行监控的属性[30]。形式化描述如下。

定义 20　（信息安全可控性属性形式化）

若 $CT(I)=1$，则称信息 I 满足信息安全控制可控性属性；若 $CT(I)=0$，则称信息 I 不满足可控性属性。其中 CT 是对信息 I 的监控度量，所谓监控是指能够控制授权范围内的信息流向、传播及行为方式，控制信息资源的使用及使用资源的人或实体的使用方式。信息安全可控性常用技术有信息流向监控技术、信息资源使用监控技术、内存监控技术等。

可认证性（verifiability）是指通信的双方不能否认通信行为，即事后发送者不能否认其发送的信息，接收方也不能否认其接收到的信息[30]。形式化描述如下。

定义 21　（信息安全可认证性属性形式化）

若 $V_F(F(i))=1$，其中 $\forall F\in\{s,r\}$，s 为对信息 i 的发送，r 为对信息 i 的接收，则称对于信息 i 是双向可认证的。否则若 $\exists F,V_F(F(i))=0$，则称对于信息 i 是不能双向认证的。若满足双向认证，则称满足信息安全可认证性属性。若 $V_s(s(i))=1$，称信息 i 满足发方可认证性属性；若 $V_s(s(i))=0$，则称发方不满足可认证性。若 $V_r(r(i))=1$，称信息 i 满足收方可认证性属性；若 $V_r(r(i))=0$，则称收方不满足可认证性。

信息安全可认证性具体实现技术主要有数字签名认证算法等，例如 PKI(public key infrastructure)[34]、IBE(identity-based encryption)[35,36]、CFL[37] 等。PKI 是用公钥概念和技术实施的，支持公开密钥的管理并提供真实性、保密性、完整性以及可追究性等安全服务并具有普适性的网络安全基础设施。虽然目前已有了证书认证和标识认证 2 种认证技术，但是由于网络的复杂性以及认证技术的安全性，网络认证技术仍是当前网络安全的重要研究课题。

4　知识与知识安全

4.1　知识的定义

《布莱克维尔哲学指南》[38]与《西方认识论简史》[39]中都指出知识的概念是哲学认识论领域最为重要的一个概念，是哲学的一个分支，它探求知识的性质、来源和有效性以及研究知识的性质及前提和基础，以及对知识所要求的一般可靠性。知识如何定义？经验主义、理性主义、实用主义、历史主义等流派各有自己的观点，哲学、逻辑学、科学学、社会学、管理学、信息学等学科的定义也各有自己

的深度和广度。奥地利的赫尔穆特[40]将知识定义为某种心理的东西，在人类的心理之外知识是不存在的。每一种知识都是个体人的知识，知识有一个对象客体，也就是人们知道的东西，信息则是一种事态（sachverhait）。

通过对文献[41~43]知识分类比较分析，网络空间知识的分类以显性知识与隐性知识分类更便于知识安全研究的进行，网络空间知识又可分为科学知识和非科学知识，而非科学知识中的主要构成成分是常识知识。知识的分类是非常复杂的问题，已有的分类方法多样，出于研究论述的方便，只通过上述知识分类来澄清和说明网络空间知识的类别和性质。

在哲学界，人们把知识的定义问题称之为“泰阿泰德问题”。这个问题最早是由柏拉图提出，在该“问题”中对于构成知识的条件给出了经典型解说，所谓的知识必须能够满足如下 3 个条件：信念的条件、真的条件以及证实的条件。由此得出结论，即一条陈述能称得上是知识必须满足 3 个条件，它一定是被验证过的、正确的，而且被人们相信的。知识是个集合概念，它即指知识总体，也指知识个体[44]。本文在借鉴文献[44~46]基础上，给出如下形式定义。

定义 22 （相容知识体）假设一个多条陈述的集合为 K_i，其中的各条陈述形式可以划分为 2 类，一类为公理或原理，另一类为由公理或原理逻辑推导出的结论，且任何条陈述之间逻辑上无矛盾。称这样的 K_i 为一个相容知识体。

根据定义 22，给出如下的相容知识体的性质。

性质 3 一个相容知识体 $K_i = C_i \cup A_i \cup T_i$，其中 C_i 是 K_i 中的概念的集合，A_i 是 K_i 的公理或原理，T_i 是由 A_i（人工或机器）推导出的结论集合；且 C_i、A_i、T_i 都是 K_i 的子集合。

在定义 22 的基础上给出知识的定义。

定义 23 （知识）$K = \bigcup_{i \in I} K_i$，其中 $\forall i \in I, K_i$ 都是一个相容知识体。

由上述定义可知，知识创新有高低 2 个层次：低层次创新是指一个相容知识体内的知识创新；高层次的创新是指新的相容知识体的产生。

根据定义 12，信息是一个随机变量蕴含的另一个随机变量的确定性。根据定义 23，知识是相容知识体的集合。从这 2 个定义可以看出，信息是知识发现的基础，知识发现的作用之一就是能够消除信息的不确定性，消除了“不确定性”的信息也就所追求的知识，即知识是确定的信息。把在传统信息系统中添加一定相容知识体集合后的信息系统称为知识系统。

4.2 知识安全

正如文献[7]所述，知识安全是信息安全之后的一个自然过渡。关于知识安全的具体定义目前还没有相关的研究。本文在借鉴数据安全与信息安全定义的基础上分别给出知识安全微观、中观与宏观的研究内容。

知识安全微观研究内容。对于知识来说，只有作为表象的概念还不足够。知识还与用逻辑句子表达的事态有关。除了主观构成物之外，还存在着客观逻辑句子，它反映了一种具体的事态。网络空间由于事态缺失、逻辑证明不严谨进而导致知识的可信性无法衡量。A N Kolmogorow 提出了描述信息复杂性的概念[47]，知识的数学本质和复制性问题是知识科学 2 个基本的问题。从数学的观点看，知识是什么？那么，对知识复杂性应如何描述？知识的基本单位是什么？知识有哪些功能？网络空间知识的边界如何来定义？知识安全的微观定义主要研究的是事态可信度与逻辑推理的过程，即知识可信度度量的过程—知识生命周期可信度进行分析的结果。知识的生命周期知识发现、知识表示、知识存储、知识集成、知识共享、知识应用、知识创新、知识进化等。

知识安全宏观研究内容。网络空间知识系统是由无数个由知识构成物库（知识构成物库中提供陈述、陈述复合体、知识模型等）、术语资料库、事实库、方法库构成的知识库（或者知识系统，该知识库包含了资料源的一种证据）与网络空间基础设施构成的。由此可见知识安全宏观研究内容是围绕构建安全知识系统展开的研究。

知识安全中观研究内容。当今网络空间中的知识退化、知识白化，也不是信息安全的五大属性能够解决的。为此在信息安全的五大属性的基础上，外加可传承性、抗白化性，构成知识安全的 7 大属性，其形式化描述如下。

知识安全机密性是指知识对于授权用户或实体是能够获得并确定的。对于非授权用户是不能获得或即使获得也不能理解知识内容的。

根据信息安全机密性属性形式化描述，知识安

全机密性属性形式化描述如下。

定义 24　（知识安全机密性属性形式化）

若 $\forall a\in A, C(k,a)=1, \forall b\in \overline{A}, C(k,b)=0$，$C$ 是机密性度量，则称知识 k 满足知识安全机密性属性，其中，A 是知识 $k\in K_i$ 的授权可读集合。

知识安全完整性是指要求知识不在未经授权的情况下被修改或者丢弃。

借鉴信息安全完整性形式化描述，给出知识安全完整性形式化描述所示。

定义 25　（知识安全完整性属性形式化）

若 $I(S(k))=I(k)$，则称知识 k 满足知识安全完整性属性，其中，S 是指对知识 $k\in K_i$ 的任何处理算子，包括传输、备份、复制、应用等，I 是知识 k 的完整性度量。

知识安全可用性是知识可被授权实体访问并按需求使用的特性。

借鉴信息安全可用性形式化描述，给出知识安全可用性形式化描述如下。

定义 26　（知识安全可用性属性形式化）

$\forall n\in N, A(n,k)=1$，则称知识 k 满足知识安全可用性属性；若 $\exists n\in N, A(n,k)=0$，则称知识 k 不满足可用性。其中 N 是用户的对知识 $k\in K_i$ 应用需求集合，A 为知识安全可用性度量。

知识安全可控性是指能够对知识活动进行监控的属性。

形式化描述如下。

定义 27　（知识安全可控性属性形式化）

$k\in K_i$，若 $CT(k)=1$，则称知识 k 满足知识安全可控性属性；若 $CT(k)=0$，则知识 k 不满足可控性。其中 CT 是对知识 k 的监控度量，所谓监控是指能够控制授权范围内的知识流向、传播及行为方式，控制知识资源的使用及使用资源的人或实体的使用方式。

知识安全可认证性是指通信的双方不能否认通信行为，即事后发送者不能否认其发送的知识，接收方也不能否认其接收到的知识。

其形式化描述如下。

定义 28　（知识安全可认证性属性形式化）

$k\in K_i$，若 $\forall F\in (s,r), V_F(F(k))=1$，则称知识 k 满足知识安全可认证性属性，其中 s 为对知识 k 的发送方，r 为对知识 k 的接收方。

若 $V_s(s(k))=1$，称知识 k 满足发方可认证性；若 $V_s(s(k))=0$，则称发方不满足可认证性。

若 $V_r(r(k))=1$，称知识 k 满足收方可认证性；若 $V_r(r(k))=0$，则称收方不满足可认证性。

知识安全可认证性具体实现技术主要应有数字签名认证算法等，可同样使用 PKI[31]、IBE[32~36]、CFL[37]等。

知识安全可传承性（inheritability）是指知识可以由拥有该知识的人传授给别人。

其形式化描述如下。

定义 29　（知识安全可传承性属性形式化）

$k\in K_i, a(k)\to b$，则称知识 k 满足由 a 到 b 的知识安全可传承性属性，其中 a 为拥有知识 k 的人或实体，b 为被 a 传授知识 k 的人或实体。

知识安全抗白化性（anti-whitability）是指保证知识的真实性。

其形式化描述如下。

定义 30　（知识安全抗白化性属性形式化）

$k\in K_i, AW(k)=1$，则称知识 k 满足知识安全抗白化属性，否则若 $AW(k)=0$，则该知识 k 不满足抗白化性。

在当前网络环境下应有意识地大力发展知识抗白化性技术，例如支持实名制的数字签名验证技术、网络追溯技术、网络取证技术，制定相应的法律法规等。知识安全完整性与抗白化性区别在于知识 k 是完整的，但有可能是白化的知识。通过抗白化性技术等，可防止当今网络的知识白化[7]、公民丑化；利用可控性技术等，可防止当今网络知识恶性使用；利用机密性、完整性、可用性、可控性、可认证性等技术，可防止当今网络环境中的知识创新产权失控；利用可传承性、完整性等技术，可防止当今网络环境中的知识泯灭。

5　安全知识系统中的知识系统构建

在知识系统 $K=\bigcup_{i\in I} K_i$ 中，$\forall k\in K_i$，如何保证这条知识的安全性呢，下面对其进行知识安全 7 大属性结构化保护。

5.1　安全知识系统中每条知识的结构化

在建立一个安全知识系统时，首先在管理层面上，要建立安全知识系统管理中心，成立该类知识领域专家组、成立提供每条知识的专业人员团队等。

安全知识系统管理中心领导负责协调组织领域专家组、专业人员团队的日常工作；专业人员团队成员负责提供每条知识，领域专家组成员要对提供的每条知识进行核查，保证每条知识的抗白化性。为确保每条知识的可认证性，要对每条知识本身、提供者、核查者进行基于标识的证书认证。每条知识具体结构化如下。

定义 31 （每条知识的结构）

每条短程的结构为

$$y_0\ \ y_1\ \ x_0\ \ x_1\ \ x_2\ \ y_0\,u_0\ \ u_1\ \ v_0\ \ v_1\ \ g_0\ \ g_1$$

其中：

1) y_0 表示该条知识所隶属的相容知识体的序号即 i，其长度足够长且固定为 $l(y_0)$；

2) y_1 为该条知识在相容知识体中的序号，不防设为 j，即在相容知识体 K_i 中的第 j 条知识，其长度足够长且固定为 $l(y_1)$；

3) x_0 为该条知识的内容，其长度为 $l(x_0)$，其为不定长参数，由 $z_0=l(x_0)$ 来标识其长度，$l(z_0)$ 足够长且固定；

4) x_1 为该条知识的阅读器标识，其长度 $l(x_1)$ 足够长且固定；

5) x_2 为该条知识的种类，$x_2=s, s\in\{0,1,2\}$，$s=0$ 是指该条知识属于 K_i，$s=1$ 是指该条知识属于 A_i，$s=2$ 是指该条知识属于 T_i，其长度 $l(x_2)$ 足够长且固定；

6) u_0 为该条知识提供的时间、提供者的姓名、国籍、身份证号、所属单位，其中时间、姓名、国籍、身份证号、所属单位的长度足够长且固定，其长度之和为 $l(u_0)$；

7) u_1 为该条知识提供者的数字签名，其长度足够长且固定为 $l(u_1)$，被签名的内容为 $(y_0y_1x_0x_1x_2z_0u_0)$；

8) v_0 为该条知识的核查时间、核查者的姓名、国籍、身份证号、所属单位，其中时间、姓名、国籍、身份证号、所属单位的长度足够长且固定，其长度之和为 $l(v_0)$；

9) v_1 为该条知识核查者的数字签名，其长度足够长且固定为 $l(v_1)$，被签名的内容为 $(y_0y_1x_0x_1x_2z_0u_0v_0)$；

10) g_0 为安全知识系统管理中心负责人签名时间、安全知识系统拥有者的唯一名称，负责人的姓名、国籍、身份证号，其长度足够长且固定为 $l(g_0)$；

11) g_1 为知识系统管理中心负责人的数字签名，其长度足够长且固定为 $l(g_1)$，被签名的内容为 $(y_0y_1x_0x_1x_2z_0u_0v_0v_1g_0)$。

定义 31 给出了每条知识的结构化。

在每条知识结构化后的基础上，下面给出安全知识系统的条件分析。

5.2 安全知识系统的条件分析

假设某知识系统为 KS，且其中的每条知识 $k\in K_i\subset K$ 都按定义 31 进行了结构化。

首先给出如下假设。

假设 1 假设每条知识在三方(提供者、核查者、管理中心负责人)的数字签名约束下满足抗白化属性。即 $\forall k\in K_i\ AW(k)=1$。

也就是说知识系统 KS 中的每条知识是真的。

假设 2 假设 KS 中的每条知识的结构化过程中的数字签名算法是安全的。

假设 3 假设知识系统 KS 的授权用户集合为 A，满足

$$\forall i\in I,\forall k\in K_i,\forall a\in A,C(k,a)=1,\forall b\in \bar{A},C(k,b)=0$$

在假设 3 下，知识系统 KS 是满足机密性的。

假设 4 假设知识系统 KS 的每条知识在用户使用时满足

$$\forall i\in I,\forall k\in K_i,I(S(k))=I(k)$$

在假设 4 下，知识系统 KS 中的每条结构化的知识作为数据是满足动态完整性的。

假设 5 假设知识系统 KS 满足：$\forall i\in I$, $\forall k\in K_i$, $\forall n\in N, A(n,k)=1$。

在假设 5 下，知识系统 KS 是满足可用性的。

假设 6 假设知识系统 KS 满足 $\forall i\in I$, $\forall k\in K_i$, $CT(k)=1$。

在假设 6 下，知识系统 KS 是满足可控性的。

在假设 2 的基础上，给出如下性质。

性质 7 结构化后的每条知识是满足静态数据完整性属性的。

证明 对于结构化后的每条知识，使用者可根据三方签名对每条知识进行验证，再根据假设 2，故可得 $I(S(k))=I(k)$，因此该性质成立。

在假设 2、假设 4 下由性质 4 可知知识系统 KS 是满足完整性属性的。

在上述假设下分析知识系统 KS 的可传承性问题。

在假设 1、假设 2、假设 4、假设 5 下，有如下性质。

性质 5　A 中的成员可以获得知识系统 KS 中的知识。

证明　由于 A 是知识系统 KS 的授权集合，根据假设 5，因此 A 中的成员可以获取知识系统 KS 中的知识。又根据假设 4 与性质 7，因此 A 中的成员从知识系统 KS 中所获得的知识是完整的。再根据假设 1，A 中的成员所得到的知识是抗白化的。因此该性质成立。

易得如下性质。

性质 6　A 中的成员在获得知识系统 KS 中的知识后加以学习掌握，则满足了知识系统 KS 中的知识的可传承性。即满足 $k \in K_i, KS(k) \to b$。其中 b 是知识系统 KS 的被传承者。

由性质 6，易得如下性质。

性质 7　在性质 6 中的条件、及假设 1~假设 6 下，知识系统 KS 满足知识安全的 7 大属性，即机密性、完整性、可用性、可控性、可认证性、可传承性、抗白化性。

定义 32　称满足知识安全 7 大属性的知识系统 KS 为安全知识系统。

根据上述分析，在以后的研究将给出一类安全知识系统的构建方法。

6　结束语

中国科学院王飞跃研究员指出，随着网络空间云计算、大数据等理念和技术的发展预示并已经由面向物理世界的工业自动化，走向基于数据、大数据的网络空间知识自动化[48]。随着网络空间知识自动化时代的到来，网络空间必将掀起知识安全研究的高潮。本研究给出了知识安全的 7 大安全属性及其它们的形式化描述，对解决当前网络空间中存在的知识安全问题具有积极的现实意义。此外，本文给出了知识系统中的每条知识结构化，继而在一定的假设条件下，给出了安全知识系统的概念及分析。下一步的研究中，将会就知识安全的微观定义及其知识安全的可信度度量方法等进行研究，并在此基础上给出面向实际应用的安全知识系统建设的细化设计、实施与安全性分析，并对相应的安全知识系统管理体系进行研究。

参考文献：

[1] 丁大尉, 李正风. 网络信息空间中的知识构建—以维基百科知识生成机制为例[J]. 自然辩证法研究, 2012, 28(5):61-65.
DING D W, LI Z F. Knowledge construction in nnetwork information world-case study of knowledge production machanism of wikipedia[J]. Studies in Dialectics of Nature, 2012,28(5):61-65.

[2] 陆汝铃. 世纪之交的知识工程与知识科学[M]. 北京:清华大学出版社, 2001.
LU R L. Knowledge engineering and knowledge science at the turn of the century [M]. Beijing: Tsinghua University Press ,2001.

[3] 陈文伟, 陈晟.知识工程与知识管理[M]. 北京:清华大学出版社, 2010.
CHEN W W, Chen C. Knowledge Engineering and Knowledge Management[M]. Beijing: Tsinghua University Press, 2010.

[4] DESOUZA K C. Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets[M]. UK: Kogan Page.

[5] 陈雪秀, 吕述望, 孙鹏. 知识安全与可控性[J]. 信息安全与保密通信, 2004,12(4):12-16.
CHEN X X, LV S W, SUN P. Knowledge security and controllability[J]. China Information Security, 2004,12(4):12-16.

[6] 周雪. 吕述望教授谈知识安全与未来网络[J]. 信息安全与保密通信, 2012,12(3):20-22.
ZHOU X. Professor Lv Shuwang talks about the knowledge of safety and the future network[J]. China Information Security, 2012,12(3): 20-22.

[7] 曾伟忠. e-Science 环境下知识控制研究[D]. 南开大学, 2009.
ZENG W Z. Research on Knowledge Control Under e-Science EnviRonment[D]. Nankai University, 2009.

[8] 冯登国, 张敏, 李昊. 大数据安全与隐私保护[J].计算机学报, 2014, 37(1):246-259.
FENG D G, ZHANG M, LI H. Big data security and privacy protection[J]. Chinese Journal of Computers, 2014, 37(1):246-259.

[9] 刘婷婷. 面向云计算的数据安全保护关键技术研究[D]. 郑州：信息工程大学, 2013.
LIU T T. Research on Key Technologies of Data Security towards Cloud Computing[D]. Zhengzhou: PLA Information Engineering University, 2013.

[10] 严慰敏, 吴伟民.数据结构[M].北京:清华大学出版社, 1997.
YAN W M, WU W M. Data Construction[M]. Beijing: Tsinghua University Press, 1997.

[11] JP 1-02. Department of Defence Dictionary of Military and Associated Terms[S]. Washington DC:U.S. Joint Staff, 2010.

[12] 严士健, 王隽骧, 刘秀芳. 概率论基础[M]. 北京：科学出版社, 2007.
YAN S J, WANG J X, LIU X F. Foundations of Probability Theory[M]. Beijing: Science Press, 2007.

[13] 茆诗松, 王静龙, 濮晓龙, 高等数理统计[M]. 北京：高等教育出版社, 2009.
MAO S S, WANG J L, PU X L, Advanced Mathematical Statistics[M]. Beijing: China Higher Education Press, 2009.

[14] BILL F, 黄海, 车皓阳等译. 驾驭大数据[M]. 北京：人民邮电出版社, 2013.
BILL F, HUANG H, CHE H Y, *et al*. Taming the Big Data Tidal Wave[M]. Beijing: Posts & Telecom Press, 2013.

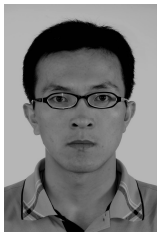
[15] 陆嘉恒. 大数据挑战与 NoSQL 数据库技术[M]. 北京:电子工业出版社, 2013.
LU J H. Large Data Challenge with NoSQL Database Technology[M]. Beijing: Electronic Industry Press.2013.

[16] 赵刚. 大数据技术与应用实践指南[M]. 北京: 电子工业出版社, 2013.
ZHAO G. Big Data Technology and Application of Practice Guidelines[M]. Beijing: Electronic Industry Press, 2013.

[17] EDWARDS, HAROLD M. Galois Theory[M].Springer-Verlag,1984.

[18] RUDOLF L, HARALD N. Finite Fields[M]. Addison-Wesley Publishing Company, 1983.
[19] 梁之舜, 邓集贤, 杨维权等. 概率论及数理统计[M]. 北京: 高等教育出版社, 1992.
LIANG Z S, DENG J X, YANG W Q, *et al*. Probability Theory and Mathematical Statistics[M]. Beijing: China Higher Education Press, 1992.
[20] 陆传荣, 林正炎, 陆传赉. 概率论极限理论引论[M]. 北京:高等教育出版社, 1989.
LU C R, LIN Z Y, LU C J. The Theory of Probability Limit Theory Introduction[M]. Beijing: China Higher Education Press, 1989.
[21] BEEK P, VAN Z. Wahrscheinlichkeits theorie[R]. 1972.
[22] 候方勇. 存储系统数据机密性与完整性保护的关键技术研究[D]. 北京:国防科学技术大学, 2005.
HOU F Y. Research on Key Technologies of Storage System, Data Confidentiality and Integrity Protection[D]. Beijing: National Defense Science and Technology Unviersity, 2005.
[23] BELL D E, LAPADULA L J. Secure Computer Systems: Unified Exposition and Multics Interpretation[M]. Bedford, MA: The MITRE Corporation, 1976.
[24] BELL D E, LAPADULA L J. Secure Computer Systems: Mathematical Foundations[M]. Bedford, MA: Electronic Systems Division, Air Force System Command Corporation, Hanscom AFB,1973.
[25] BELL D E, LAPADULA L J. Secure computer systems: a mathematical model[M]. Bedford, MA: Electronic Systems Division, Air Force System Command Corporation, Hanscom AFB,1973.
[26] 董婵, 范修斌, 李有文等. 应用规律下的 BLP 模型密级赋值方法[J]. 通信学报, 2013, 34(9):142-149.
DONG C, FAN X B, LI Y W, *et al*. Secret level valuation method of BLP model based on some application properties[J]. Journal on Communications, 2013, 34(9):142-149.
[27] 安宝宇. 云存储中数据完整性保护关键技术研究[D]. 北京:北京邮电大学, 2012.
AN BY. Cloud storage of data integrity research on Key Technologies of protection [D]. Beijing: Beijing University of Post & Telecommunication, 2012.
[28] BIBA K J. Integrity considerations for secure computer systems[R]. ESD-TR-76-372, Bedford, MA: USAF Electronic Systems Division, Hanscom Air Force Base, 1977.
[29] 黎琳, 禄凯, 国强等. 基于 Biba 模型的三权分立分析[J]. 北京交通大学学报, 2013, 37(5):1-7.
LI L, LU K, GUO Q, *et al*. Formal analysis of power separation mechanism based on Biba model[J]. Journal of Beijing Jiaotong University, 2013, 37(5):1-7.
[30] 王宇, 卢昱.网络安全与控制技术[M]. 北京: 国防工业出版社,2010.
WANG Y, LU Y. Network security and control technology[M]. Beijing: NationalDefenceIndustryPress,2010.
[31] SHANNON C E. A mathematical theory of communication[J]. Bell Syst.Tech. 1948, 27: 379-423, 623-656.
[32] NOBERT W. The Human Use of Human Beings: Cybernetics and Society[M]. Da Capo Press; New edition, 1988.
[33] THOMAS M, COVER, JOY A. Thomas, Elements of Information Theor[M]. John Wiley & Sons, Inc.2006.
[34] ANDREW N, WILLIAM D, CELIA J, *et al*. PKI Implementing and Managing E-Security[M]. RSA PRSS,2001.
[35] WATERS B. Efficient identity-based encryption without random oracles[J]. Lecture Notes in Computer Science, 2005, 3494:114-127.
[36] GENTRY C. Practical identity-based encryption without random oracles[J]. Lecture Notes in Computer Science, 2006, 4004: 445-464.
[37] 陈华平, 范修斌, 吕述望. 基于标示的证书认证体制 CFL[P]. 2011102500094, 2011.
CHEN H P, FAN X B, LV S W. Mark certification system based on CFL[P]. 2011102500094,2011.
[38] BUNNIN, NICHOLAS E P. The Blackwell Companion to Philosophy[M]. Oxford: Blackwell Publishers Ltd, 2001.
[39] 夏甄陶, 崔建军, 纪虎民. 西方认识论简史[M]. 北京:中国人民出版社, 1987.
XIA Z T, CUI J J, JI H M. The Epistemological History of Westen[M]. Beijing: Beijing People's Press, 1987.
[40] 邱碧华. 术语学、知识论和知识技术[M]. 北京:商务印书馆, 2011.
QIU B H. Terminology, Epistemology and Knowledge Technology[M]. Beijing: the Commercial Press, 2011.
[41] 刘兵,李正风.自然辩证法参考读物[M].北京:清华大学出版社, 2003.
LIU B, LI ZF. Dialectics of Nature of Reference Books[M]. Beijing: Tsinghua University Press, 2003.
[42] 郭元林. 复杂性科学知识论[M]. 中国书籍出版社, 2012.
GUO Y L. Complexity Science Theory[M]. China Book Press, 2012.
[43] 何兆. 哲学问题[M]. 北京:商务印书馆, 2004.
HE Z. Problems of Philosophy[M]. Beijing: the Commercial Press, 2004.
[44] 陈洪澜. 知识分类与知识资源认识论[M]. 北京:人民出版社.2008.
CHEN H L. Knowledge Classification and Knowledge resource epistemology[M].Beijing: Beijing People's Press, 2008.
[45] 史忠植. 知识发现[M].北京:清华大学出版社, 2002.
SHI Z Z. Knowledge Discoverity[M]. Beijing: Tsinghua University Press, 2002.
[46] 许文艳, 刘三阳. 知识库系统的逻辑基础[J]. 计算机学报, 2009(32):11, 2123-2128.
XU W Y, LIU S Y. Logic for knowledgebase systems[J]. Chinese Journal of Computers, 2009(32):11,2123-2128.
[47] LING M, PAUL V. An Introduction to Kolmogorov Complexity and Its Application[M]. Springer-Verlag, 1997.
[48] 王飞跃. 天命唯新:迈向知识自动化—《自动化学报》创刊 50 周年刊序[J]. 自动化学报, 2013, 39(11):1741-1743.
WANG F Y. The destiny: towards knowledge automation—— preface of the special issue for the 50th anniversary of Acta Automatica Sinica[J]. Acta Automatic Sinica, 2013,39(11):1741-1743.

作者简介：



闫世杰（1979-），男，山西交城人，北京科技大学博士生，主要研究方向为网络空间信息安全相关控制技术等。

闵乐泉（1951-），男，北京人，博士，北京科技大学教授，主要研究方向为信息安全密码技术、图像加密技术等。

范修斌（1966-），男，山东新泰人，博士，北京博文广成信息安全技术有限公司研究员，主要研究方向为信息安全密码学等。