大脑密码学的三旋数学模型

王德奎

王德奎 (Wang Dekui), 绵阳日报社, 绵阳, 四川 621000, 中国, y-tx@163.com

摘要：从某种意义上说，自然界的物质和大脑的物质都是一种圈群结耦有限自动机结构。建筑在类圈体三旋模型基础上的“大脑密码学”，正是沿着从白箱来分析黑箱的道路，去探索大脑的智能与结构的。在大脑密码学模型里，大脑是硬件与软件合一的密码机。

[王德奎. 大脑密码学的三旋数学模型. *Academ Arena* 2025;17(7):32-36]. ISSN 1553-992X (print); ISSN 2158-771X (online). http://www.sciencepub.net/academia. 03. doi:10.7537/marsaaj170725.03

关键词：大脑密码学；三旋理论；神智结构；密码体制；拓扑学

【0、引言】

美国杰出的神经外科医生伯格兰德，在他的《神智的结构》一书中对传统的理论提出质疑。因为两百多年来，人们一直认为，一切信息都是由电信号沿着神经系统传递到人脑的；而人脑，就象一台计算机那样，再将电信号处理成各种思想意识。

伯格兰德却认为，人脑实际只是一个腺体，其功能作用取决于激素和分子的变换结构。人的语言是化学性的而非电学性的，人脑中的电脉冲仅是表层信息。对于向人脑传送的信号来说，它并不像激素那么重要。

【1、意识的现代数理结构】

以上理论，不仅为人脑研究领域开拓了新的广阔前景，而且也为新型智能机的设计开拓了广阔的前景。

其一，它将大大丰富电子计算机的传输媒介。当代电子计算机普遍以电流作传输信号，这正如人类普遍使用语言、文字思维一样。

然而人类的思维却不限于语言和文字，而是按全方位信息处理的，语言只是其中最主要的一种。对这种多因素的信息处理，只靠单元性的电讯编码，即使其容量和形式是大量的，也还是不够的。

而思维的化学递质的多元性理论的提出，便为新一代电子计算机全方位信息编码处理，提供了理论基础。

其二，当今电子计算机系统正面临着“病毒”的威胁。所谓病毒，是指一个作怪的小小程序，能够不知不觉地污染连结各计算机的电子网络，而使系统陷于瘫痪：把受污染的磁盘装入机中，这种病毒就会传播，并且继续留在计算机数据库里，破坏插入的其它磁盘；而排除这种病毒必须付出昂贵的代价。为此，大脑密码学愿为设计新型的全方位信息处理，并为对付“病毒”的电子计算机，寻找一条出路。

大脑密码学，是在三旋数学破译物质的夸克结构、微观向宏观进化的圈群组装、大脑思维的魔方模拟模型之后提出来的。这三者，也是我们认定大脑与物质具有合一性的基础，它能阐释大脑这种生态位为什么会在自然进化中出现，以及意识怎样构成人脑的机能与属性等问题。密码学最基本的概论，如“明文”与“密文”，“密文中高频字母群”与“明文中高频字母群”，“密码机”与“密码体制”，“加密”、“密钥”、与“解密”、“破译”等，对大脑密码学来说，是很容易联想的。我们可以把一切显秩序，都看成是明文，即把我们人类能观感到的东西都可以看成是明文，这样我们平常用的语言和文字，仅是明文字母中的特殊部分。相反隐秩序、体内解，也可以看成是密文。

从某一种意义上说，人类的大脑密码体制并不十分复杂，但却十分优越、和谐和统一。而且人和动物的密码体制的建构原理并没有什么不同，也许仅是密钥不同之分。

当然，密码学还仅能体现我们大脑工作情况的一部分，但从这一部分，我们也能窥视大脑的创造力与分析力的一些机制。为了说明大脑的密码学模型，我们先来看看大脑的智能控制模型。

大脑密码学要解决的根本问题是意识问题，从某种意义上说，人类仍然是一种物质，但它何来的意识与智能呢？虽然大脑能充分利用和发挥物质类圈的各种层次上的结构与功能，但智能控制论运用控制原理和方法，不是也能研究人脑神经系统的功能，模拟和放大人的智能，设计和建造智能控制系统吗？

1943 年美国科学家麦卡洛克和匹茨，提出一种神经元模型，以二值（1 与 0）逻辑刻画神经细胞的兴奋与抑制的双态工作。

由这种形式的神经元构成神经网络的形式化系统，它在一定程度上也能模拟人脑的功能，并沿着神经网络模型的方向发展，形成称之为脑模型的专门

领域，建成既有感知、识别和学习的脑模型，又有用计算机，进行的模拟实验。对这一模型加以改进，以之模拟简单的思维过程，可以实现三段论式的推理和简单归纳逻辑。

当然这还仅是智能控制论的一个方面，另一个更为全面的方面是人工智能的研究，强调机器能思维，从而沿着以计算机为支持手段的智能模拟方向发展。它的特点，是从软件方面考虑机器行为与人脑功能的相似，而不从硬件方面追究机器构件与脑内结构的等同性。

因此，人工智能主要是编制智能软件，采用算法或启发式方法进行程序设计，使计算机具有智能。目前这方面已有不少成果，用机器证明定理、发现定理，用机器下棋、绘画、翻译和模式识别，均已成为现实；而运用知识工程方法研究的化学专家系统、医学专家系统、探矿专家系统已被应用于实践；智能机器人，开始走出了实验室。

但目前的智能控制论，尽管成就突出，而其基本方法仍未超出黑箱范围。即使操作功能有些已超过了活脑，但意识的实际结构，仍然无从揭示。三旋数学认为，从黑箱不能完全分析白箱，从灰箱也不能完全分析白箱；那么能不能从白箱来分析黑箱呢？

建筑在类圈体三旋模型基础上的“大脑密码学”，正是沿着从白箱来分析黑箱的道路，去探索大脑的智能与结构的。在大脑密码学模型里，大脑是硬件与软件合一的密码机。

这种密码、译码，不是说像气味这类无形的东西对人体的嗅觉、大脑的影响，或者像人体使用气味交流信息，以及像气味是由细菌在皮肤上分泌的作用而产生那样，作解释就可以了事的。大脑的密码功能具有拓扑特性，这可以从视知觉的拓扑特性看出。

1982 年我国科学家陈霖报道，用 5 毫秒的速示仪提供图形刺激，通过对一批受试者的测试统计，发现在接近阀值的条件下，在拓扑学意义上不同的图形对（圆盘--环等）的正确判别概率，总是高于拓扑学意义上相同而几何学意义上不同的图形对（圆盘--正方形；圆盘--三角形等）。这说明拓扑学意义上不同的图形对有更大的可判别性，这是由视觉系统对拓扑结构的敏感性决定的。

在大脑接收的信息总量中，视觉比例最大，而拓扑信息量与类圈体模型的信息编码相关极大，这正反映出大脑功能注意信息拓扑量是与类圈体模型联系在一起的。如类圈体的三旋排列跟光子跃迁的联系，就涉及到大脑化学递质的编码与译码结构。

沿着这思路，我们来看看密码学的内容。目前的密码编制已经实现了机械化，密码分析实现了数学化。传统密码编制的最基本方式是代替和换位，而代替密码是按一定规则，用密文代替明文字母的。

从明文字母表 X 到密文字母表 Y 的一一映射的序列 K=（f_1，f_2，f_3，……），称为代替密码体制的密钥。由密钥 K 决定一个密码变换 T_k 。它按照公式 $y_i=f_i(x_i)$,（其中 i=1，2，3 …），将明文字母序列 $X_1X_2X_3\cdots$ 变换为密文字母序列 $Y_1Y_2Y_3\cdots$。解密过程是按照公式 $X_i=f_i^{-1}(Y_i)$,(其中 i=1，2，3，…)，将密文恢复为明文 $X_1X_2X_3\cdots$。这里 f_i^{-1} 表示 f_i 的逆映射。当 $f_1=f_2=f_3=\cdots$时 ，称 T_K 为单表代替，否则称 T_K 为多表代替。

换位密码是将明文字母的正常次序打乱，即按密钥所确定的顺序得到密文。例如，周期为 e 的换位是将明文字母划分为组，每组 e 个字母，密钥是 1，2，…e 的一个置换 f。然后按照公式 $Y_i+n_e=X_{f(i)}+n_e$，（其中 i=1，…e；n=0，1，…）将明文 $X_1X_2X_3\cdots$加密为密文 $Y_1Y_2Y_3\cdots$。解密过程则按照下式进行：$X_j+n_e=Yf^{-1}{}_{(j)}+n_e$，（其中 j=1，…e；n=0，1…）。

由此可见，各种简单的和复杂的密码体制，都是代数密码体制的非常特殊的情况。如果把大脑密码也转化为数学问题，那么，我们便可改进计算机设备的弱点，并依靠数学技巧，而获得全新的破译大脑创造性思维的方法。

【2、从智能模型到密码学模型】

解剖开人的大脑，所见无非是脑细胞和各种有机物质，却找不到人们认识世界所留下的表象。其间的隐秩序，即我们不能观感到的大脑里的体内解，恰与密文对应；而显秩序，即我们的意识随时都能反映的外部事物及其联系，正与明文对应。

大脑密码学正是将意识与大脑内部组织相分离，而通过明文与密文对应把它们联系在一起，以此揭示大脑的结构。这样，我们将发现，人和动植物的密码体制的建构原理并无不同，只不过密钥不同罢了。

从反应与记忆看，人和动植物的机体相同，作为生命物质，都由细胞、DNA 构成，都有信息接收和反应表现，都有充分利用类圈体结构与功能的特性。若从密码机和密码体制来看，其最低级层次上都有类似光谱频率变换的三旋密码编译机制。

但随着动植物高级程度的不同，体外解性质的不同，这种密码机和密码体制的复杂程度也不同。这不仅符合它们的进化过程，也符合它们生存活动需要。以语言、文字及其对应的具体事物为例，这些明文字母在人类大脑中能够转换为密文编码，当它再作为明文转译反映出来时，我们发现每个人的“密码机”虽然形式、结构、原理相同，但结果却存在差异。这从传统密码的破译方法上，便可以理解。

传统密码的破译通常使用统计分析的方法，分析字母的频率和连缀关系。以英文字母的单表代替为例，破译者首先统计密文中每个字母的频率及连缀关系，然后与一般英文中各个字母的出现频率对

照，即将密文中高频字母群和明文中高频字母群对应，再根据连缀关系进行探测，就可能破译密码。

又如破译有周期密钥的多表代替密码，也是通过计算重码之间的距离，并将这些数分解成因子，根据出现频率最高的因子测定密钥的周期。一旦周期被确定，破译多表代替密码就可归结为用频率法破译各单表代替密码。由于每个人是硬件与软件相结合的密码机与密码体制共振的独立系统，因此在接受各种明文时，通常带有独特的处理方法，反映在大脑译出的明文中，便是各具特色。

这类似于几个人同译一本英文小说，英文的明文是早定下的，翻译规则也大致相同，但因互不沟通信息，因而各人所译便大不相同。

数理语言学家正是利用这种不同，来分析考证作品的地方色彩与个性风格，从而确定它的时代与作者等问题的。如有人把《红楼梦》一百二十回当成一个整体，以回为单位，从中挑选出 47 个常用字，由于字的使用频率与作家的大脑密码编译直接相关，因此将这些字输入计算机，并将其使用频率绘成图纸，从星云状和阶梯状的图形，便可以直观地看出几大群落，一一显示不同作者的大脑密码风格。

据此有人提出，《红楼梦》成书，可能经过轶名作者作《石头记》，曹雪芹以所作《风月宝鉴》插入其中，“披阅十载，增删五次”，定名为《红楼梦》；再经程伟元、高鄂，整理形成全书。

用三旋、九连环套和魔方的模式，我们不难理解意识的密码学结构。换句话说，大脑对体外体内的信息处理，都采用了有限自动机密码体制的编码程序，予以接收转译释放。至于通信，已用到现代密码学中正在研制的却是：“公开密钥密码体制”。

所谓公钥体制，是讲该体制的加密算法和加密密钥，均可以公布于众，供加密者选择使用。而解密密钥，由用户 A 自行秘密保管。

当用户 B 向 A 用密码的形式发送消息 M 时，B 首先要从密钥记录表（相当于电话簿）中找到 A 的公开算法和公开加密密钥 E_A，并用它来加密信息 M，即 $C_1=E_A（M）$，然后在 A、B 之间的公共信道上传送（由 B 发给 A）；当 A 接收到 B 所发来的密文信息 C_1 后，就用 A 所秘密保存着的解密密钥 D_A 解密，$D_A（C_1）= D_A[E_A（M）]=M$，恢复出明文信息 M。当然 B 也可用自己保管的秘密密钥 D_B 作变换，$C_2=D_B（M）$，那么，当 A 接到信息 C_2 后，可用 B 的公开密钥 E_B 作逆变换，$E_B（C_2）= E_B[D_B（M）]=M$，恢复原来的信息 M。

也许一切显秩序，即我们认为是明文的事情，其实它们和人类的大脑之间，早就在用密码进行通信，并且实行的都是公钥体制。

因为从大脑与物质的合一性研究，这种双方的公开密钥是很好理解的，就是物质的类光谱变换的三旋自然密码机制，和九连环套式的伪随机序列编码机制。而主要的公共信道，是光波传送。

至于各自的解密密钥，无生命物质一般都是这两种公开的密钥形式，而有意识活动的人或高等生命，解密密钥便多了一层魔方式对应的密钥穷尽搜索机制。因为大脑工作机构所面对的外部事物有着无穷的密文，要破译这种有限自动机产生和释放的密文，便不能不利用大脑密钥穷尽搜索机制。大脑潜意识活动的这种公钥解密过程，实际已经适合有物质手征的光学活性选择，即包含了对内外有关的熵能量分流的处理。在这里，物质与大脑公钥的合一性，是自然界的伟大创造，它减少了自然界的混乱和复杂，又加强了生物的发展进化。

而人类又以生育递归迭代方式，强化和增质这种密钥穷尽机器。此外，人类还有不同于机械的密钥穷尽搜索机器。即社会思维的群体大脑性、耦连性，可以看作第二级的密钥穷尽搜索机，这是大脑密码学模型不同于人工智能控制模型的地方。也是人脑和人脑信息网络，并不完全同于电子计算机和电子计算机的网络的地方。

【3、大脑创造性思维的密码学机制】

现在再看大脑密码学与经济、军事活动中，人工创造的密码机和智能机的联系。不管是智能控制论中的神经元二值逻辑模式，还是密码学的编译模式，都还不能包罗大脑创造性思维的全部功能。

对此，人们提出了种种设想，例如，采用模糊数学逻辑来模拟大脑对模糊信息的处理，发展模糊计算机。认知科学、思维科学与神经控制论、心理控制论的相互渗透，在智能控制论的基础上，创建思维控制论等等。其实，大脑类圈体三旋转座子机制，不但与物质的结构性统一在一起，而且还把密码机功能与创造性和模糊识别思维能力结合在一起。这里不妨对大脑的密钥穷尽搜索机功能，与它的创造性思维的结合情况，作一探讨。

第二次世界大战广泛使用的转轮密码机，大多是一部打字机外带几个转轮，实现的是一种周期密钥多表代替密码。由于数学方法在密码学中的应用，使得这种复杂密码体制还是被破译了。

当时日本使用的转轮密码机一一九七式欧文印字机发报的密码，被美国密码专家佛里德曼等人破译，就显示了数学工具（其中包括群论、数论、统计学）的威力。1948 年香农建立了信息论，次年他发表了将信息论用于密码的文章，从理论上探明了有效的破译密码，应当具有的密文字母数量，提出破译的起码要求是有充分数量的密文。

他将所需密文的最小量，称为“唯一解点”或“唯一解码量”。香农研究了破译密码的统计方法的本质，提出两种抗统计分析的密码设计方法：分散法和混乱法。分散法是使多余度扩散到大范围的统计中，以

迫使破译者增大工作量。混乱法是使描述统计量和密钥关系的方程，变得更加错综复杂，以此达到抗统计分析的目的。

1977 年美国商业部国家标准局，公布了 DES 密码，这是实现香农理论的产物。DES 密码，对 64 位二进制数字加密，产生 64 位密文数字；所用密钥也是 64 位（除去 8 位奇偶校验位，实只 56 位）。

前面提到的转轮密码机，只是有限自动机中的一种，输入和输出运用的是字母。20 世纪五十年代由于晶体管的发展，到六十年代初，商用数字通信系统开始投入使用，原有转轮密码机已不能适应，因而出现采用移位寄存器产生的伪随机序列来加密和解密的密码体制。这与生物中性漂变中假性密码基因，有很多相似之处。

笔者曾经用九连环套式的密码编制类比，对物质圈态结耦作过解释，这也类似一个移位寄存器。

而这种编码是设被传送的明文是二元序列 X_0 X_1…（X_i 取 0 或 1），用一个二元伪随机序列 Z_0 Z_1… 作为密钥，并按照公式 $Y_i=X_i \oplus Z_i$(其中 i=0，1，…) 加密得到密文 Y_0 Y_1…。解密时，把同样的伪随机序列叠加到密文上，即得到明文 X_0 X_1…；$X_i = Y_i \oplus Z_i$（其中 i=0，1，…）。这里⊕表示模 2 加法。以一个 4 级移位寄存器为例，它产生周期为 $2^4-1=15$ 的伪随机序列 111100010011010111100010011010…。这种移位寄存器序列尽管是周期性的，但它具有良好的统计性质，与白噪声接近，因此被称为伪噪声或伪随机序列。用它作密钥时，一般将 n 取得相当大，使序列的周期 2^n-1 充分大，因此这种密码能抵抗统计分析。

如果把生物进化程度愈高，看成 n 愈大，这不是可以看作它的密码破译程度愈困难吗？有限自动机是一个数学概念，它可以作为大脑的类圈体群落结耦编码的数学模型。一般说来，用移位寄存器序列加密和解密的这种有限自动机密码体制，超出了周期密钥多表代替密码体制，而近似于理论上不可破的一次一密体制。因此即使结构已经暴露，用“状态识别”试验的方法来破译仍是困难的。

如果用穷尽密文和开始状态的所有可能的取值进行尝试，由于周期较大，工作量也十分惊人。其次，由于函数的系数个数是变元个数的指数函数，这样的方程更是难解。如 DES 二进制数字有限自动机，它自公布以来，研究者们至今没有找到有效破译方法。

但也有认为 56 位密钥长度还不够，建议制造专用机，由给定的密文和对应的明文片断，对 258 种可能的密钥进行尝试检查。

1976 年 8 月美国国家标准局，计算机科学技术研究还专门召开会议，讨论建造这种密钥穷尽搜索机器的可行性问题，但得出的结论是，平均每天找出一个密钥的机器，大概在 1990 年前不可能建造，而且这种机器的造作达几千万美元。

从某种意义上说，自然界的物质和大脑的物质都是一种圈群结耦有限自动机结构。人类体外信息也是十分混乱和分散的，再加上用光波作公共信道加密来反射，更类似白噪声，具有抗统计分析的效应。

但从自然界的普通物质进化到大脑物质，形成的高级圈群结耦的这种有限自动机结构，对体外体内的信息反应，不仅采用了有限自动机密码体制的编码接收，也采用了这种密码体制转译释放。反过来说，我们人类清醒意识认为是明文的事情，大脑里的工作机构也许认为它是密文；而我们认为大脑密码机里是密文的事情，却是大脑工作机构的明文，在这种情况下我们就不难理解，大脑工作机构面对外部事物存在多少密文啊！在这里，事物机理也是一种密文；而要破译外部事物这种有限自动机（每个人自身也是各自独立的有限自动机）生产和释放的密文，既是大脑创造力与分析力的行为，也是每个个体对付外部密码，不得不还要建造密钥穷尽搜索机器式的大脑的根源。

而建造破译伪噪声高级密钥穷尽搜索机器的可行性，已在生物进化之颠的人类大脑中实现了，这就是大脑的三旋转座子模式。用这种模式，我们不难理解人类的“意会思维”和“言传思维”合一的情况。

而且用三旋转座子的有序图案对应寻找密钥，这又是自然力的一件伟大创造，也是非常之平常和自然的事情。

因为物质的始元，本来就内禀蕴藏着三旋属性。人类大脑的这种三旋转座子密钥穷尽搜索机器，正是人脑的创造力和分析力的根本动力来源，也正是我们说的创造性思维的神力所在。

而且人类生育的递归迭代的方式，也在强化和增质这种密钥穷尽搜索机器，这是人类不同于机械的密钥穷尽搜索机器，即人类社会表现出的自动的群体大脑性、耦联性，也可以看着是第二级的密钥穷尽搜索机；并且这种人类大脑互相间，既出难题又共同组成解答难题的阵线，也是人脑密码学模型不同于人工智能控制模型的地方，即人脑和人脑信息网络，并不完全同于电子计算机和电子计算机的网络。

【4、结束语】

当然人脑和人脑网络，同电脑和电脑网络也有相似之处，特别是将全球网络界的最大创新----因特网以及无线上网映射人体，可以说人体内大脑与其它各个器官，以及与各个细胞之间，都建立有类似电脑与因特网之间的联系。

再类比从地方网络到全球网络，建立的各级新型的大容量系统和以网络为核心的企业重建，涉及整个经济领域所产生的效果，如网络化金融服务带

来的系统升级；网络进一步使证券市场、外汇及其他投机性票据的交易导致的无国界资本的流动，致使金融业成为资本全球化的先驱；以及将因特网技术应用于企业内部的发展，大大超过因特网的发展步伐的这种旨在将局限性很大的传统系统，改造为综合企业网络的趋势，表明各行各业的公司都在努力把因特网当作一种新的、分散的全球信息架的基础等等来看，就更知人体因特网的先进性和完美性。可以说人类社会，还在向自然的进化看齐。

或者说，自然的存在，需要人类社会的科学进步才能得以理解。

因为所谓细胞的全息性、全能性、整体性，从人体因特网的角度，能得到更多更好的阐释。其次，还应该提出的是：大脑密码学建立的泛解概念，对从热力学产生的泛熵学说是一个大挑战。

它进一步揭示了泛熵学说张扬的困境，是由于它自身基立于点体观，而失掉了圈比点更基本而带来的这部分目的性的计量和考虑。

6/2/2025

参考文献

[1]叶眺新，关于大脑密码的思维，延边大学学报（社），1987（4）；
[2]叶眺新等，论大脑密码学的三旋数学模型，上饶师专学报（自），1990（3）；
[3]王德奎，三旋理论初探，四川科学技术出版社，2002 年 5 月；
[4]孔少峰、王德奎，求衡论----庞加莱猜想应用，四川科学技术出版社，2007 年 9 月；
[5]王德奎，解读《时间简史》，天津古籍出版社，2003 年 9 月；
[6]王德奎、林艺彬、孙双喜，中医药多体自然叩问，独家出版社，2020 年 1 月；
[7]叶眺新，自然全息律，潜科学杂志，1982 年第 3 期；
[8]叶眺新，中国气功思维学，延边大学出版社，1990 年 5 月；
[9]王德奎，大脑密码学的三旋数学模型，Academ Arena，December 25, 2023。