科学通报

密码学的新领域——DNA密码

肖国镇, 卢明欣, 秦磊 and 来学嘉

Citation: 科学通报 **51**, 1139 (2006); doi: 10.1360/csb2006-51-10-1139

View online: http://engine.scichina.com/doi/10.1360/csb2006-51-10-1139

View Table of Contents: http://engine.scichina.com/publisher/scp/journal/CSB/51/10

Published by the 《中国科学》杂志社

密码学的新领域——DNA 密码

肖国镇[①]　卢明欣[①*]　秦 磊[②]　来学嘉[③]

(① 西安电子科技大学综合业务网国家重点实验室, 西安 710071; ② Cancer Research Institute, Queen's University, 10 Stuart St Kingston, ON K7L 3N6, Canada; ③ 上海交通大学计算机科学与工程系, 上海 200030. * 联系人, E-mail: seulmx@126.com)

摘要　DNA 密码是近年来伴随着 DNA 计算的研究而出现的密码学新领域, 其特点是以 DNA 为信息载体, 以现代生物技术为实现工具, 挖掘 DNA 固有的高存储密度和高并行性等优点, 实现加密、认证及签名等密码学功能. 本文简要介绍了 DNA 计算原理, 总结了当前 DNA 密码的研究现状以及存在的若干问题, 对 DNA 密码、传统密码和量子密码的发展状况、安全性以及适用领域进行了分析对比, 探讨了 DNA 密码未来发展的趋势. DNA 密码与传统的密码以及研制中的量子密码相比各有优势, 在未来的应用中可以互相补充. 实现 DNA 密码面临的主要困难是缺乏有效的安全理论依据和简便的实现方法, 当前研究的主要目的是充分发掘 DNA 可用于信息领域的优良特性, 建立起相关的理论依据, 探寻 DNA 密码可能的发展方向, 寻找实现 DNA 密码的简便方法, 为 DNA 密码的未来发展奠定基础.

关键词　密码　**DNA** 密码　**DNA** 计算

DNA 所具有的超大规模并行性、超高容量的存储密度以及超低的能量消耗正被人们开发出来用于分子计算、数据储存以及密码学等领域, 这方面的研究有可能最终导致新型计算机、新型数据存储器和新型密码系统的诞生, 引发一场新的信息革命. DNA 密码就是在这种背景下、随着对 DNA 计算(也称为分子计算或生物计算)的研究而诞生的. 传统的密码随着电子技术的发展在 20 世纪得到了巨大的发展, 也是当前实际使用的密码系统; 量子密码诞生于 20 世纪 70 年代, 近年来有了一定的发展, 但是距离实际应用尚有距离; DNA 密码是在 1994 年 Adleman 提出 DNA 计算之后才开始得到关注的, 目前已成为国际密码学研究的前沿领域. DNA 密码、传统的密码和量子密码各自以大不相同的方式, 实现着共同的目的——信息安全, 它们有可能成为未来密码学的三大主要领域. 本文对 DNA 密码的研究背景、研究进展和未来的发展趋势进行评述, 以期为这一前沿领域的进一步研究服务.

1　DNA 计算

DNA 密码的发展, 首先得益于 DNA 计算(也称为分子计算或者生物计算)的研究进展. 一方面, 密码系统与相应的计算模式总是有着或多或少的关联. 另一方面, DNA 计算中使用的一些生物技术, 在 DNA 密码系统中也得到了一定的应用.

1994 年, Adleman[1]进行了世界上第一次DNA计算, 标志着信息时代的一个新阶段开始了. 在随后的研究中发现, DNA计算具有超大规模并行性, 超低的能量消耗和超高密度的信息存储能力[1~5]. 2002 年, Adleman领导的一个小组利用一台简单的DNA计算机, 采取穷举搜索的方法解决了一个有 100 万种可能的 3-SAT问题[6]. 2005 年, 文献[7]报道了由Keinan领导的小组实现了用很少的DNA和酶进行 10 亿次的并行运算. Adleman这样评价DNA计算: "几千年以来, 人类社会一直使用各种人造的设备提高自己的计算能力. 但是只有在 60 年前电子计算机出现以后, 人类社会的计算能力才有了质的飞跃. 现在, 分子设备的使用使得人类的计算能力能够获得第二次飞跃[6]".

DNA计算的理论研究也取得了一定的进展, 提出了多个可行的计算模型, 如Adleman[1]于 1994 年使用的模型(本文称为汉密尔顿路径模型), 文献[7,8]中利用DNA芯片进行计算的模型, 以及Adleman等提出的粘贴模型(sticker model)[9]. 下面简略介绍汉密尔顿路径模型和粘贴模型.

1.1　汉密尔顿路径模型

1994 年, Adleman[1]利用DNA计算解决了一个有向汉密尔顿路径问题, 该计算模型也同样被Lipton[10]用于解决 3-SAT问题. 所谓汉密尔顿路径问题, 就是在有向图(图 1)上找出一条经过所有顶点一次且仅一次的有向路径来. 图中的每一个顶点i可用一个随机的长度为 20-mer的寡核苷酸(DNA短链)表示. 寡核苷酸片段是有方向的, 一端称为 5′端, 一端称为 3′端. 下面的O_2, O_3和O_4分别表示顶点 2, 3 和 4, 所有这些

寡核苷酸片段的方向都是 5′到 3′.

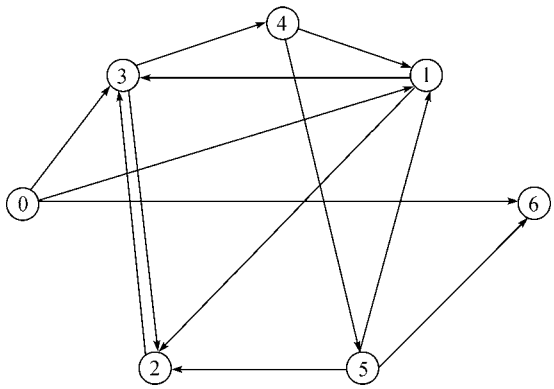

图 1 有向图

$$O_2 = \text{TATCGGATCGGTATATCCGA},$$
$$O_3 = \text{GCTATTCGAGCTTAAAGCTA},$$
$$O_4 = \text{GGCTAGGTACCAGCATGCTT}$$

图 1 中的每一条边 $i \to j$ 所对应的核苷酸 $O_{i\to j}$, 是由 O_i 3′端的 10-mer 寡核苷酸和 O_j 5′端的 10-mer 寡核苷酸组成. 对于图中的每一个顶点, $\bar{O}_i$ 是 O_i 的 Watson-Crick 互补配对. 除了顶点 $\bar{O}_3$ 以外, 下面所有寡核苷酸片段的方向都是 5′→3′.

$$O_{2\to 3} = \text{GTATATCCGAGCTATTCGAG},$$
$$O_{3\to 4} = \text{CTTAAAGCTAGGCTAGGTAC},$$
$$\bar{O}_3 = \text{CGATAAGCTCGAATTTCGAT}.$$

实验中, 对于图中的每一个顶点 i (起点和终点除外)和每一条边 $i \to j$, 在一个连接反应体系中将大量的代表顶点 O_i 的互补 DNA 序列 $\bar{O}_i$ 和代表边 $O_{i\to j}$ 的寡核苷酸片段混合在一起, 这样, 通过“逐步的 PCR”反应, 将生成相关联的、代表边连接起来所形成路径的寡核苷酸片段(图 2). $\bar{O}_i$ 的作用是通过互补原理, 将两条有向边连接起来.

反应结束后, 首先通过 PCR 扩增出那些始于起点并止于终点的路径, 然后通过电泳去除长度不符合要求的边, 再用磁珠分离技术, 依次去掉不通过某些顶点的边. 如果最后有 DNA 序列存在, 就说明有满足要求的汉密尔顿路径存在.

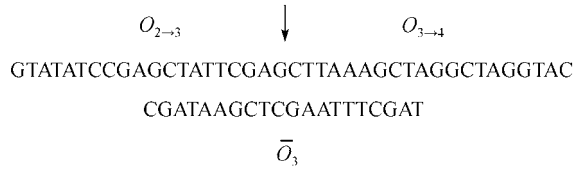

图 2 连接过程

1.2 粘贴模型

粘贴模型和汉密尔顿路径模型都是基于 Watson-Crick 互补模式, 所不同的是, 在汉密尔顿路径模型中, 一开始是短链, 然后通过退火逐步形成作为解答的长链. 而在粘贴模型中, 一开始是长的 DNA 单链, 短的粘贴链通过退火粘贴在长链上. 在文献[6]和[11]中, 用的都是粘贴模型. 粘贴模型主要包括存储结构以及组合、分离、设置位和清除位四种操作. 关于粘贴模型的详细介绍参见文献[9], 图 3 是文献[9]中粘贴模型的存储结构.

DNA 计算在理论和实践中取得了一定的成就, 但是, 人们还远未揭开细胞内的所有奥秘, 研究这些奥秘的时候极有可能会发现新的计算原理. 所以, 当前 DNA 计算的成就似乎还是非常初级的. 正如 Gifford[12]所述, 转录控制以及其他基因机制在细胞的行为中起着极为重要的作用, 但是在这简单的生物过程中, 似乎还隐藏着其他的计算机制.

2 DNA 密码的研究现状及面临的主要问题

2.1 研究现状

DNA 密码是新生的密码, 其特点是以 DNA 为信息载体, 以现代生物学技术为实现工具, 挖掘 DNA

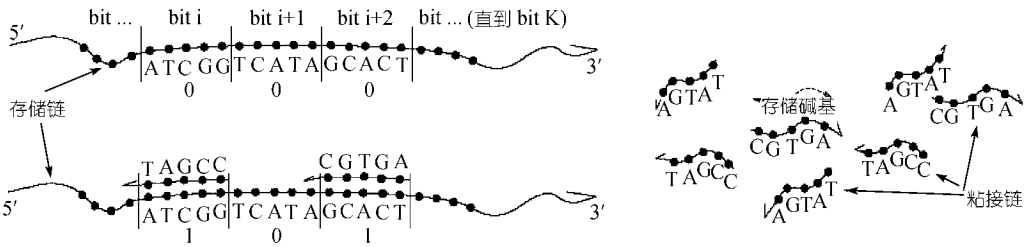

图 3 粘贴模型

固有的高存储密度和高并行性等优点，实现加密、认证及签名等密码学功能．虽然DNA计算的研究对DNA密码的发展有一定的贡献，但这种贡献是间接的，Adleman等提出的DNA计算并不能直接成为DNA密码．DNA计算是用DNA技术解决计算难题，而在DNA密码中，各种生物学难题被研究并用作DNA密码系统的安全依据．DNA密码的加密和解密过程可以看作是计算的过程，而并不是所有的DNA计算都与保密有关．此外，DNA密码也不同于遗传密码．遗传密码属于基因工程领域，涉及DNA在生物遗传方面的作用．目前，DNA密码在国际上刚刚起步，有效的DNA密码方法较少[13~15]．下面介绍两个提出较早并且具有代表性的DNA密码方案．第一个方案体现了DNA的超高存储密度，但实现困难．第二个方案实现相对容易，其用PCR技术解密的方法既与DNA计算相关联，又在后续的DNA密码研究中得到了广泛应用．第二个方案虽然也被称为隐写术，但从其实现系统安全的方式看，该方案称为一个以加密为主，并具有部分信息隐藏功能的系统更贴切．

在DNA加密方面，Reif 等[13]利用DNA实现了一次一密的加密方式．他认为，一次一密的使用之所以受限制，是因为保存一个巨大的一次一密乱码本非常困难．DNA具有体积小，存储量大的优点，1 克DNA就包含有 10^{21} 个碱基，或者说 10^{8} TB，几克DNA 就能够储存世界上现有的所有数据．所以，DNA 非常适合用作存储一次一密乱码本．Reif 的方法考虑到了 DNA 的高容量存储特性，具有潜在的使用价值，也许会成为解决一次一密乱码本存储的有效方法．不过，制备一个能够方便地分离并读取出数据的大规模 DNA 一次一密乱码本非常困难．对于发送者和接收者来说，都要进行目前看来还有些复杂的生物学实验，需要在一个装备精良的实验室里才能实现，因此加密和解密的成本也很高．今后很多年内，上述问题都会严重限制 Reif 方案的可行性．

在DNA信息隐藏方面，Celland等[14]成功地把“June 6 invasion: Normandy”隐藏在DNA微点中，从而实现了基于DNA的信息隐藏．他们的方法如下:

(1) 编码方式．他们没有采用传统的二进制编码方式，而是把核苷酸看作是四进制编码，用 3 位核苷酸表示 1 个字母．譬如字母 A 用核苷酸序列 CGA 表示，字母 B 用核苷酸序列 CCA 表示……

(2) 合成消息序列．把需要传送的消息按上面的编码方式编成相应的 DNA 序列，如 AB 用CCGCCA 表示．编码结束以后，人工合成相应的有69 个核苷酸的 DNA 序列，并在 DNA 序列前后各链接上有 20 个核苷酸的 5′和 3′引物．这样，需要隐藏的DNA 消息序列就准备好了．

(3) 信息隐藏．用超声波把人类基因序列粉碎成长度为 50~100 的核苷酸双链，并变性成单链，作为冗余的 DNA 使用，再把含有信息的 DNA 序列混杂到冗余的 DNA 序列中，喷到信纸上形成无色的微点，就可以通过普通的非保密途径传送了．

(4) 信息读取．接收方和发送方的共享秘密是编码方式和引物．接收方收到含有消息 DNA 微点的信纸后，提取出微点中的 DNA．由于接收方预先通过安全的途径得到了引物，所以他可以用已有的引物对 DNA 微点中的消息序列进行 PCR 扩增，通过测序得出消息 DNA 序列，然后根据预先约定的编码方式恢复出消息(明文)．

图 4 是文献[14]中信息隐藏方法的基本流程．需要指出的是，图 4 中仅把编码方式作为加密钥的说法并不准确，真正的密钥应该是引物和编码方式．

2.2　当前面临的主要问题

从国际上的研究现状可以看出，现有的 DNA 密码方法主要面临下面的问题:

(1) 缺乏相关的理论支持． 1949 年，Shannon[16]在《保密系统的通信理论》中提出了现代保密通信的基本模型和发展方向．其后，20 世纪 70 年代提出用计算复杂度作为设计密码算法的工具，促进了公钥密码体制的产生[17]．随后，RSA，EIGamal，DES和AES等相继诞生，形成了比较完善的体系[18~21]．相比之下，DNA密码还没有建立起相应的理论，DNA密码的实现模型是什么，安全性依据在哪里，具体应该如何实现，这些问题都还没有解决．也正因为相关理论的缺乏，导致现阶段难以产生优秀的DNA密码方案．

(2) 实现困难，应用代价高昂． 已有的方法，在加密和解密阶段往往需要人工合成消息 DNA 序列，进行 PCR 扩增，对 DNA 序列进行测序等生物学实验．在现有的技术水平下，上述工作只能在一个装备精良的实验室完成，这使得 DNA 密码在实际使用中很不方便，无法与现在使用的密码系统竞争．幸运的是，最近 20 年来，现代生物学发展迅速，很多过去实现困难且代价高昂的实验现在已经成了常规的实验．

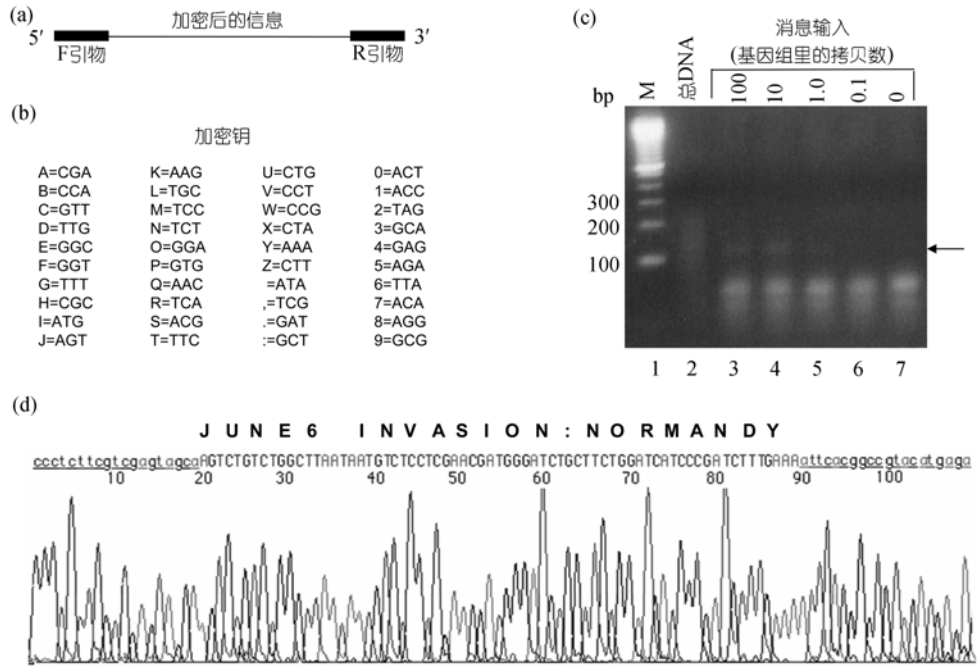

图 4 信息隐藏方法

(a) 合成的消息序列; (b) 编码方式; (c) PCR 扩增结果; (d) PCR 扩增后通过测序得到的消息序列以及对应的明文

随着生物技术的进一步发展和更好的 DNA 密码设计方案的出现, 实现困难和代价高昂的问题应该可以解决.

3 DNA 密码、传统密码和量子密码的比较

3.1 发展状况

传统密码可以追溯到 2000 多年前的凯撒密码甚至更早, 已经基本建立了比较完善的理论体系, 目前实际使用的密码都可以算是传统的密码. 量子密码诞生于 20 世纪 70 年代, 已经有相当的理论基础, 但在实现上困难较多, 还基本没有投入实际应用. DNA 密码只有不到 10 年的历史, 理论尚处于探索阶段, 使用代价也比较高昂.

3.2 安全性

传统的密码除了一次一密以外, 都只具有计算安全性. 也就是说, 如果攻击者有无限的计算能力, 理论上就可以破译这些密码系统. 研究表明, 量子计算机具有惊人的计算潜力[22~24]. 虽然目前还不能完全确定量子计算机的计算能力, 但是存在这样的可能性, 即在未来的量子计算机攻击下, 传统的密码中将只有一次一密仍然是安全的. 量子密码是在现有的理论上不可破译的密码, 它的安全性建立在海森堡测不准定理之上, 物理法则保证了这个量子信道的安全性. 即使窃听者能够做他想做的任何事情, 并且有无限的计算资源, 甚至P=NP, 他都不能破译量子密码. 任何对量子密码的窃听都会造成密码的改变从而被发现; 攻击者无法复制出一个和他所截获的量子完全一样的量子, 所以要想不被发现的篡改也是不可能的[25~29]. 因此, 通过量子密码进行密钥协商, 具有无条件的安全性. DNA密码主要是以生物学技术的局限性为安全依据, 与计算能力无关, 因此对量子计算机的攻击也是免疫的. 但是这种安全性有多么高, 能够保持多久, 还有待于研究.

3.3 使用功能

传统的密码使用最为方便. 计算过程可以使用电子计算机、DNA 计算机甚至量子计算机; 在传输过程中可以使用电线、光纤、无线信道甚至信使; 储存媒介可以使用光盘、磁介质及 DNA 等任何可以存储数据的媒介. 并且可以实现公钥加密、私钥加密、身份认证和数字签名等诸多功能. 量子密码是在量子信道上实现的, 适用于实时通信, 不适用于安全数据储存, 难以做到像传统密码那样可以轻松实现公钥加密和数字签名等功能. 以目前的技术, DNA 密码只能用物理的方法传送, 但 DNA 所具有的超大规模

并行计算能力、超低的能量消耗和超高密度的信息存储能力，使得 DNA 密码在对实时性要求不高的大规模并行数据加密、安全数据存储，以及身份认证、数字签名和信息隐藏等密码学应用中具有独特的优势. DNA 也可以用来制作难以伪造的商业合同、现金支票以及身份识别卡等.

由于传统密码、DNA 密码和量子密码都还在发展之中，尤其是后两者都还有很多问题没有研究清楚，目前很难准确预测未来密码界的发展. 但从上述分析可以看出，在未来相当长的时间内，这三种密码很可能是互相补充共同发展而不是某一个被彻底淘汰.

4 DNA 密码发展的趋势

DNA 密码的研究还处于探索阶段，准确预测其未来的发展还不太现实. 考虑到生物学技术的发展以及密码学的需求，对今后 DNA 密码的发展提出如下建议:

第一，实现 DNA 密码要以现代生物学为工具，以生物学难题作为主要安全依据，充分发掘 DNA 密码独特的优势.

加密和解密的过程就是对数据进行变换的过程. 在电子计算机和互联网络高速发展的今天，这些变换过程如果能够用数学来描述，常常比物理或者化学变换要容易实现. 其他类型的密码系统能够存在，就应该具备比现有的密码系统更好的安全性或者更高的数据密度等特性，不能或者不易用数学方法和电子计算机来实现. DNA 密码要能够存在和发展，就必须充分挖掘 DNA 密码的优势，利用 DNA 所具有的体积小的特性，实现纳米级的存储；利用 DNA 的超大规模并行特性，实现加密和解密的快速化；利用人类还不能破译但是能够利用的生物学难题，作为 DNA 密码的安全依据，以实现能够抵抗量子攻击的新型密码系统. 由于目前还无法完全确定量子计算机对各种数学难题的威胁，DNA 密码的安全依据也不应完全排斥数学难题. 考虑到 DNA 计算的巨大并行能力，用电子计算机难以实现的加密和解密也许可以用 DNA 计算机轻松实现. 如果这种算法能够抵御量子计算机的攻击，这种计算的安全性就可以用于 DNA 密码中. 所以，DNA 密码与传统的密码并不是完全互相排斥的，有可能把二者结合起来形成混合的密码系统.

第二，安全性要求.

不管DNA密码和传统的密码有多么不同，它同样要遵守密码的共同特性. DNA密码的通信模型仍然是由发送者和接收者组成的，双方通过安全的或认证的途径获得秘钥，然后可以通过不安全或非认证的途径传递密文进行通信. 对于DNA密码的安全性要求也仍然应该以Kerckhoff提出的假设为依据: 一个密码系统之安全性必须仅依赖其解密密钥，亦即在一个密码系统中除解密密钥外，其余的加/解密算法等均应为假设破译者完全知道. 只有在这个假设下，破译者若仍然无法破解密码系统，此系统方有可能称为安全[17]. 具体地说，就是假定破译者知道密码的设计者所用的基本生物学方法，并且有足够的知识和精良的实验室设备能够重复设计者的操作. 破译者所不知道的，只有密钥. 在DNA密码中，密钥通常是某些生物学材料的实物或制备流程，或者实验条件等.

第三，DNA 密码现阶段的研究目标是以安全且容易实现为主，存储密度为次.

一个好的密码系统，既要是安全的，还要是容易实现的. 现代生物技术的发展，使得科学家可以用DNA来表达数据. 但是，这方面的技术还是刚刚起步. 目前，对只有纳米级的DNA直接操作很困难，只能通过PCR等生物学扩增技术，把DNA序列大量扩增后，在各种限制性酶的帮助下操控DNA序列. 在当前的技术水平下，还远远不能用几克DNA存储世界上所有的数据. 如果一味追求存储密度的提高，就难以在现有的技术水平下实现DNA密码. 现阶段，把大量的DNA所表现出来的群体性质用于密码学更实际一些. 比如，采用DNA芯片[30~33]来储存数据并用杂交来读取数据，可以实现快速方便的数据输入输出. 虽然DNA芯片的数据存储密度要比直接用核苷酸编码的方法低，但是实现起来要容易得多.

第四，DNA 密码现阶段的主要任务是建立起 DNA 密码的基本理论依据，积累研制 DNA 密码的实际经验.

可以肯定的是，DNA 具有用于高密度数据存储和超大规模并行计算的潜力，这是研究 DNA 计算和 DNA 密码的动力. 现在的目标和难点是如何充分挖掘和利用这些潜力，这方面的研究在国际上也是刚刚起步. 无论是 DNA 计算，还是 DNA 密码，都还没有建立起完善的理论. 现代生物学仍然是偏重于实验而不是偏重于理论. 一个 DNA 密码系统的安全性

所依据的生物学难题有多么难，相应的密码系统有多么安全，这些都还没有有效的方法来衡量. 如何建立起类似于计算复杂度理论的方法来评估生物学难题的难度，是一个迫切需要解决的问题. 所以，现阶段最重要的工作是发掘 DNA 可用于计算和加密方面的优良特性，建立起 DNA 密码的理论依据并积累 DNA 密码的研制经验，为研制安全且方便实用的 DNA 密码系统打下基础.

5 结论

目前DNA密码处于研究的初期，还有很多问题有待解决. 但是DNA分子所固有的超大规模并行性，超低的能量消耗和超高的存储密度，使得DNA密码能够具有传统的密码系统所不具有的独特优势. 正如Adleman所说，生物分子可以用于分子计算等非生物学的应用. 在这样的应用中，生物分子代表了自然界演化了 30 亿年的未经开发的遗产，有巨大的开发潜力[6].

致谢 审稿专家对本文提出了极有价值的修改意见，在此表示诚挚的感谢. 本工作为国家自然科学基金(批准号: 60473028)资助项目.

参 考 文 献

1 Adleman L. Molecular computation of solutions to combinatorial problems. Science, 1994, 266: 1021—1023
2 Guarnieri F, Fliss M, Bancroft C. Making DNA add. Science, 1996, 273: 220—223
3 Bancroft C, Bowler T, Bloom B, et al. Long-term storage of information in DNA. Science, 2001, 293: 1763—1765[DOI]
4 Ouyang Q, Kaplan P D, Liu S, et al. DNA solution of the maximal clique problem. Science, 1997, 278: 446—449[DOI]
5 Sakamoto K, Gouzu H, Komiya K, et al. Molecular computation by DNA hairpin formation. Science, 2000, 288: 1223—1226[DOI]
6 Ravinderjit S, Braich R, Chelyapov N, et al. Solution of a 20-variable 3-SAT problem on a DNA computer. Science, 2002, 266: 499—502
7 Fastest DNA computer. Science, 2005, 308: 195
8 Liu Q, Wang L, Frutos A G, et al. DNA computing on surfaces. Nature, 2000, 403: 175—179[DOI]
9 Roweis S, Winfree1 E, Burgoyne R, et al. A sticker based model for DNA computation. J Comput Biol, 1998, 5(4): 615—629
10 Lipton R J. Using DNA to solve NP-complete problems. Science, 1995, 268: 542—545
11 Adleman L M, Rothemund P W K, Roweiss S, et al. On applying molecular computation to the data encryption standard. J Comput Biol, 1999, 6(1): 53—63
12 Gifford D K. On the path to computation with DNA. Science, 1994, 266: 993—994
13 Gehani A, LaBean T H, Reif J H. DNA-based cryptography. Dimacs Series in Discrete Mathematics and Theoretical Computer Science, 2000, 54: 233—249
14 Celland C T, Risca V, Bancroft C. Hiding messages in DNA microdots. Nature, 1999, 399: 533—534[DOI]
15 Leier A, Richter C, Banzhaf W, et al. Cryptography with DNA binary strands. Biosystems, 2000, 57(1): 13—22[DOI]
16 Shannon C E. Communication theory of secret systems. Bell System Technical Journal, 1949, 28(4): 656—715
17 Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inform Theory, 1976, 22(6): 644—654
18 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120—126
19 EIGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inform Theory, 1985, 31(4): 469—472[DOI]
20 US Department of Commerce. National Institute of Standards and Technology, NIST FIPS PUB 46-2, Data Encryption Standards, 1993
21 Daemen J, Rijmen V. The design of Rijndael: AES the Advanced Encryption Standard. Berlin: Springer-Verlag, 2002
22 Shor P W. Algorithms for quantum computation: Discrete log and factoring. In: Proceedings of the 35th Symposium on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society Press, 1994. 124—134
23 Grovel L K. Quantum mechanics algorithm for database search. In: Proceedings of the 28th ACM Symposium on the Theory of Computation. New York: ACM Press, 1996. 212—219
24 Simon D. On the power of quantum computation. In: Proceedings of the 35th Symposium on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society Press, 1994. 116—123
25 Wiesner S. Conjugate coding. SIGACT News, 1983, 15: 78—88[DOI]
26 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. India: Bangalore Press, 1984. 175—179
27 Bennett C H. Quantum cryptography using any two nonothogonal states. Phys Rev lett, 1992, 68(21): 3121—3124
28 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67(6): 661—663[DOI]
29 Bennett C H, Brassard G, Ekert A K. Quantum cryptography. Sci Am, 1992, 267: 50—57
30 Fodor S P, Read J L, Pirrung M C, et al. Light-directed, spatially addressable parallel chemical synthesis. Science, 1991, 251: 767—773
31 Pease A C, Solas D, Sullivan E J, et al. Light-generated oligonucleotide arrays for rapid DNA sequence analysis. Proc Natl Acad Sci USA, 1994, 91: 5022—5026
32 Schena M, Shalon D, Ronald W, et al. Quantitative monitoring of gene expression patterns with a complementary DNA microarray. Science, 1995, 270: 467—470
33 Shalon D, Smith S J, Brown P O. A DNA microarray system for analyzing complex DNA samples using two-color fluorescent probe hybridization. Genome Res, 1996, 6(7): 639—645

(2005-07-29 收稿, 2006-01-16 接受)