DNA计算在信息安全领域的影响与应用*

文/陈智华[1] 石晓龙[1] 程 珍[2]
1 华中科技大学自动化学院 武汉 430074
2 浙江工业大学计算机学院 杭州 310023

【摘 要】基于DNA纳米技术的各种超分子体(功能单元),能实现信息存储、计算、移动和靶向送药等功能,其纳米结构的控制精度达到了原子级。基于DNA纳米技术的信息存储和计算模式,具有高度并行性、高密度和低能耗,天生适用于大量信息的存储和并行处理。面对这种新兴的计算模式,人们研究和开发了各种计算模型,讨论其对传统密码体系的影响和DNA存储信息的安全问题,包括密钥搜索、信息加密、信息隐藏及认证等。文章综述了基于DNA纳米技术的各种计算模型对传统加密算法的影响,概述了利用DNA纳米技术进行加密解密、认证签名的方案和技术,总结了当前基于DNA纳米技术的信息安全领域研究中存在的问题并展望了DNA计算及其在信息安全和存储领域的应用前景。

【关键词】 DNA纳米技术,DNA计算,密钥搜索,加密解密

DOI 10.3969/j.issn.1000-3045.2014.01.009

1 引言

DNA纳米技术是利用DNA分子特性,如碱基配对特性、自组装特性等,自底向上构建出可操控的新型纳米尺度聚集体或超分子结构。DNA纳米技术已被应用到生物、医学检测、基因诊疗、新材料开发、环境监测和DNA计算机等多个领域。IBM公司正在利用DNA纳米技术研制新型芯片;在芯片上,电子线路间的距离将仅为6nm左右,远低于目前45nm的标准。利用这种技术,IBM公司将研制出更小、更便宜的微处理器芯片。DNA分子也是塑造纳米材料的理想素材,在构建纳米元件和纳米尺度的医学检测芯片上有重要应用。以DNA作为结构模板,或是作为计算工具的DNA纳米技术开拓了一个新兴研究领域,具有广阔的发展前景。

据不完全统计,近10年来,仅在*Nature*、*Science*等国际顶级期刊上发表的DNA自组装、DNA纳米结构和材料的相关论文就超过100篇;最近3

* 基金项目:国家自然科学基金(61272071,61370105,61202204)
修改稿收到日期:2014年1月3日

年，关于DNA存储[1]、DNA三维“砖块”[2,3]、DNA机器人[4]和DNA计算电路[5]等就有10多篇。2010年，DNA纳米技术领域的奠基者、美国纽约大学的Seeman教授由于在DNA纳米技术方面的突出贡献获得了纳米领域的最高奖Kavli纳米科学奖。

DNA分子由于其独特的结构与生物功能在信息存储与分子运算方面具有天然优势。目前的数据存储介质中，硬盘十分昂贵，且需要不断的电力供应；而像磁带这类“无需电力”的最佳存档材料，10年内也会逐渐损坏。DNA能安全地存储信息，它记录了地球上所有生命的历史，而这个强大功能是其他技术难以匹敌的。研究人员表示，DNA数据存储将是2023年解决大型数据存储问题的方案之一，这将引起DNA信息存储的信息安全问题的研究热潮[1]。

DNA纳米技术用于计算，形成了DNA计算的研究方向，拓展了“计算”的概念和“计算”的模式。在分子尺度上，“计算”可以是化学键的相互作用或分子结构的改变。这种全新的存储和计算模式的实现，对信息安全领域有多方面的影响。与传统计算相比，DNA计算具有高度并行性，海量存储能力、低耗能和存储时间长的特性。DNA计算特有的高度并行计算能力，对传统的信息安全算法是否造成威胁？而其作为信息存储载体，其信息安全如何保障？下面就国内外在这两方面的研究现状展开讨论。

2 国内外研究现状及发展

DNA纳米技术是新兴的前沿交叉领域，宗旨是利用DNA分子卓越的自组装和碱基配对能力，将其作为一种纳米材料实现精确的自底向上的纳米构筑[6]。其具有最可预测和最可程序化的优点，可以通过调节碱基的数量和序列来精确控制双螺旋结构的长度，实现程序化自组装。利用DNA的各种特性，使其作为信息存储和计算工具时，给信息安全领域带来了非凡的影响。

2.1 DNA计算的发展

基于分子间相互作用的计算模型理论始于20世纪80年代中期Head提出剪切系统[7]；实验开始于1994年，Adleman使用DNA分子解决了一个哈密尔顿路问题[8]。现在，每年关于生物分子计算[9]和非传统计算[10]的科学会议上都会有许多新的分子计算模型产生。

分子自组装是生物分子计算模型的核心原则。目前，自组装并没有一个严格的精确定义，其可以理解为单个的元素自组织构成一个更大更复杂的结构的过程。这种自组织行为发生的范围可以从宇宙水平（如银河系的形成）到分子和原子水平（如晶体的形成或者蛋白质的折叠）。DNA以其固有的碱基配对特征及其可预测的双螺旋形状，非常适合于设计实现可预测和程序化的组装过程。基于DNA自底向上的自组装研究始于30年前[11]，吸引了全球范围内的至少60个实验室进行相关研究。在过去的15年中，研究主要集中于寻找适用的算法和可编程的自组装结构进行分子信息处理。

DNA计算的自组装模型使用的“DNA Tile”是一簇具有分支结构的DNA交叉分子，每一个分支都有一个粘贴末端，可以与具有互补粘贴末端的“Tile”嵌套结合，逐步形成DNA分子网格结构。具有可编程特性的自组装计算模型，不但保持了DNA计算并行性的优势，而且计算过程无需人工干预，自动完成得出结果，其灵活的Tile设计方法提供了纳米尺度的自底向上的编程方法。Tile自组装模型已被证明是图灵等价的[12,13]。自1998年以来，几个成功的实验证实了DNA自组装的计算能力[14]。Labean等

使用三交叉分子Tile完成四步累积异或运算[15]。2006年，可放大输入信号的DNA逻辑门（SeeSaw Gate）被构造出来[16]。随后分子逻辑门级联被用于模拟神经网络运算过程，成功实现了一种基于DNA计算的Hopefield网络[5]。

Seeman教授1983年提出将分支的DNA结构和DNA粘性末端相结合可以组装出规整的二维阵列结构[17]，这是首次公开阐明作为生命密码载体的DNA可以当作一种化学物质来构建纳米材料和纳米结构，开创了利用DNA设计各种DNA结构模块的先河。在此基础上，可以利用分子间识别作用精确组装DNA分子，形成各种特定纳米结构和功能分子纳米器件。2000年，5种不同结构的DX模块问世[18]，可以形成比线性DNA分子复杂的结构，如二维环形、平面格子和三维笼状结构等。2003年，利用DNA自组装技术构造纳米级高可导通的金属导线的文献在*Science*上首次发表，该文被引用超过1 300次[19]。2005年，含有4个双螺旋区域的自组装模块被设计出来，模块之间通过黏贴末端的相互作用进一步组装得到具有较小孔洞面积和较高DNA面密度的二维平面结构[20]。同年，一种含有6个DNA双螺旋的交叉结组装模块诞生，并基于合理的结构设计得到DNA纳米管和二维阵列结构[21]。2012年底，美国哈佛大学维斯生物工程研究院的研究人员设计实现了类似“乐高”玩具的DNA“砖块”（图1），造出了102种复杂三维纳米结构，充分利用了DNA自组装可编程的特性。这些可拼插的DNA“砖块”将作为纳米技术中的结构建材、计算器件，将带来巨大的医疗价值以及非医疗方面的应用[2]。

DNA折纸术是近年来提出的一种全新的DNA自组装方法，被誉为DNA纳米技术领域的一个重要里程碑[22]。理论上，DNA折纸术可以用DNA分子设计任意形状的图形和三维结构，并且由于每条起固定作用的短链具有序列特异性，在所得图案表面每个固定链处均可精确寻址。DNA折纸术相比DNA Tile自组装最大优势在于组装产物的复杂度得到很大提高，折纸术的可寻址像素

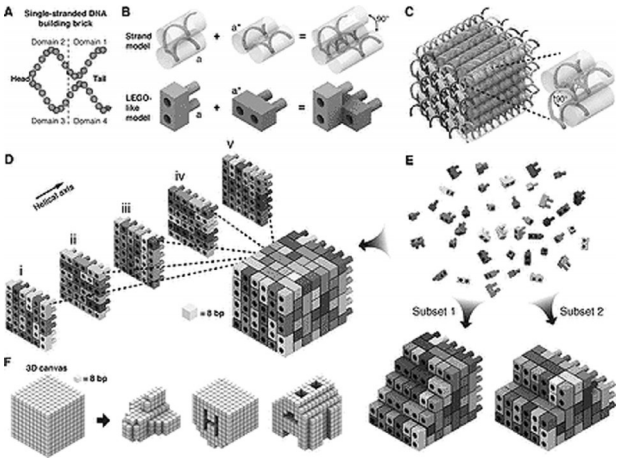

图1 Peng Yin研究组实现的“乐高”结构的DNA砖块

点数目比DNA Tile自组装至少高10倍[23]。折纸术构建形状的研究工作很丰富，获得了各种平面图形[24,25]及多种组合图形[26]。2009年，三维折纸术开始展开研究，构造出了DNA空心盒子和棱柱[27-29]，随后更多复杂结构体构造成功，包括空心四面体和“蜂窝褶状模型”等[30,31]，此结果被LaBean教授在*Nature*杂志撰文将此誉为DNA纳米技术领域的又一个里程碑[32]。2011年复杂的曲面也能成功构造出来，如精美的花瓶也能用DNA纳米技术实现（图2）[3]。

2000年，“DNA燃料”的概念引入DNA纳米技术中实现了仅依靠DNA链的状态转化[33]。这样具有动力特性的DNA纳米结构，通过一系列的状态转换可实现某些特定功能，被统称为DNA纳米

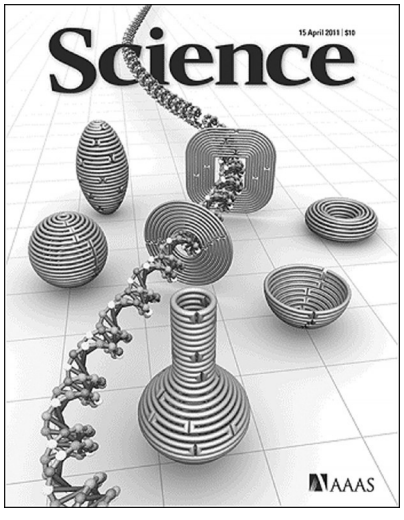

图2 Yan Hao利用折纸术构建精美的花瓶

装置。各种DNA纳米装置随后问世，如可以切换构象状态的分子开关[34]，产生开合操作的分子镊[35]，能循环转动的分子马达、分子齿轮、步进定向行走的纳米行走器、可寻址行走的“蜘蛛侠”（图3）等[36-38]。2012年构建了木桶状DNA纳米机器，可实现靶标送药（图4）[4]。基于DNA分子的纳米装置的优势在于其高度的可设计性以及组装、复制和再加工的容易性。

2013年，欧洲生物信息学研究所（EMBL-EBI）的研究人员创造出一种用DNA（能保存上万年的材料）形式来存储数据的方法，它能够在约一杯量的DNA中储存至少1亿个小时的高清视频[1]。验证了DNA作为存储介质的可能。

DNA多样化的结构和越来越精确的可控性，为DNA计算的发展提供了更为丰富的模式和技术实现方法。受DNA计算的存储和并行特性启发，人们开始研究DNA计算在信息安全领域的影响和发展。

2.2 传统密码破译的国内外研究现状

传统的加密技术比较有代表性的是数据加密标准DES体制，高级加密标准（AES）和公开密钥密码体制（RSA）。

DES算法的密钥为56bits，所以试验每一个密钥的强力攻击平均需要计算2^{55}次加密之后才能求出正确的密钥。由于加密过程中的对称性，只需要计算2^{54}次加密。在因特网的超强计算能力面前，DES显得非常脆弱。

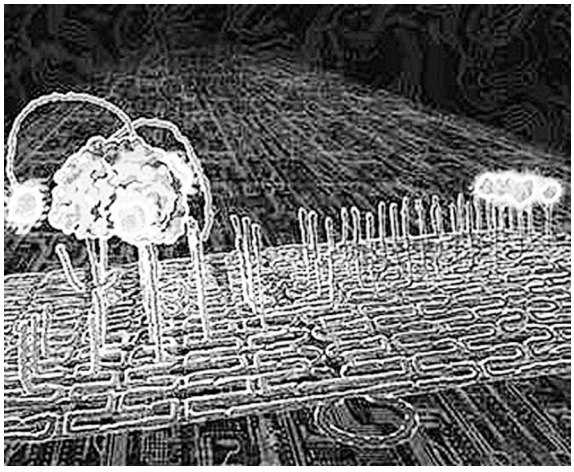

图3 分子机器人“蜘蛛侠”

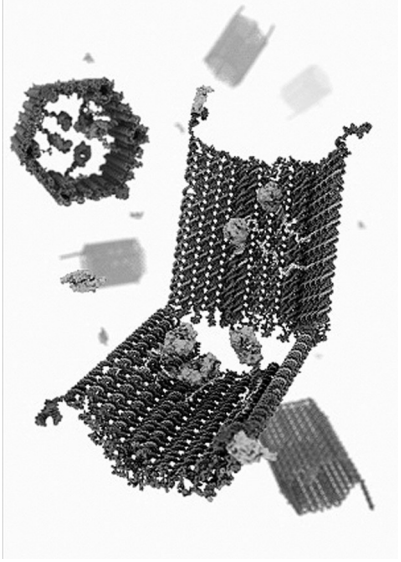

图4 可杀死癌细胞的DNA纳米机器人

1998年，由美国电子前沿基金会（EFF）牵头，密码研究所和高级无线电技术公司参与设计建造了DES破译机。该破译机可用二天多时间破译一份DES加密的密文，而整个破译机的研制经费不到25万美元。它采用的破译方法是强破译攻击法，破译机正好用56个小时找出了一个56bits的密钥，该方法是针对特定的加密算法设计出相应的硬件来对算法密钥空间进行穷举搜索[39]。因此，在实际使用中，要加大密钥的长度。

早在1997年，国家标准和技术研究所（NIST）宣布，需要为DES（很容易受到蛮力攻击）寻找新的接替者。根据NIST的定义，这种新的、非机密、公开披露的加密算法称为高级加密标准（AES）。AES由3个分组密码组成：AES-128、AES-192和AES-256，具有软件和硬件实现技术，而且速度快。虽然

没有人成功地破解全部的AES，各类研究人员已经公布了针对AES减round版的攻击。目前，对AES最有效的攻击（不考虑相关密钥攻击）是对它的积分密码分析[40]，对AES-128可攻击到7轮，对AES-192和AES-256可攻击到8轮。

RSA公钥密码体制的广泛使用，极大地刺激了大整数分解方法的研究。针对RSA最流行的攻击一般是基于大数因数分解。1999年，RSA-155（512bits）被成功分解，花了5个月时间（约8 000 MIPS年）和224 CPU hours在一台有3.2Gb中央内存的Cray C916计算机上完成。2002年，RSA-158也被成功因数分解。到2008年为止，世界上还没有任何可靠的攻击RSA算法的方式。只要其钥匙的长度足够长，用RSA加密的信息实际上是不能被解破的。但在分布式计算技术和量子计算机理论日趋成熟的条件下，RSA加密安全性受到了挑战。2009年12月12日，Aoki等人成功分解了RSA-768（768bits, 232digits）[41]。这一事件威胁了现通行的1024-bit密钥的安全性，普遍认为用户应尽快升级到2048-bit或以上。

针对RSA公钥密码体制，量子分解算法是1995年美国科学家皮特·休尔（Peter Shor）提出来的，是迄今量子计算领域最著名的算法[42]。它利用量子计算的并行性可以快速分解出大数的质因子，使得量子计算机将很容易破解目前广泛使用的密码。因此，Shor算法的提出迅速引起了世界各国对量子计算的研究的高度关注。潘建伟等与英国牛津大学同事合作，在国际上首次用光子比特，也是首次用真正的纯态量子系统，实验演示了关键性的Shor算法，实现了15=3×5这一质因子分解，并且确认了量子计算中多态纯纠缠的存在，验证了量子加速的根源问题。当前，量子密码术实用还有相当一段距离，但是英国电信的试验系统的成功充分说明了这一技术的进展是如何迅速。一旦在长距离的传统光纤信道上实现量子密钥的传输，则量子密码在技术上及成本上完全压倒经典的密码技术。

为了克服传统计算机在求解若干密码问题时出现存储量与运算速度上的不足，我们将借生物计算中新兴的计算模式——自组装DNA计算提出可行和有效的方案进行密码破译。理论已证明二维自组装模型有通用计算能力，是图灵通用的。在此基础上，利用自组装DNA计算的强大并行计算的特性，可知算法自组装模型进行密码系统的破译具有理论上的可能性，将对信息安全领域研究探索新的途径并提供技术支撑。

2.3 DNA计算对传统信息安全领域的影响

基于DNA计算的特性，科学家研究讨论了其可能对传统密码算法可能的威胁。

2.3.1 数据加密标准算法

理查德·利普顿（Richard Lipton）和丹·波恩（Dan Boneh）最早在这一领域进行了研究。1996年他们给出了使用分子计算机破译数据加密标准的方法[43]，所采用的是比较直接而朴素的方法——明文密文对破译法。该方法首先建立在对二进制串进行适当编码的基础上，创建编码各种密钥的DNA初始溶液，分别粘贴已知的明文链后再进行16轮的加密运算，最后通过搜索找到密钥。在此基础上，阿德尔曼等人又给出了使用sticker模型破译数据加密标准的方法[44]，这种模型主要使用DNA分子记忆链和粘贴来进行计算。该方法仍然采用了明文密文对破译法。其设计的数据加密标准分子算法是在粘贴机上执行的。

2.3.2 RSA算法

张云龙（Weng-Long Chang，音译）和郭敏意（Minyi Guo，音译）等人利用DNA计算设计了整数因式分解的方法，从而可以破解RSA算法[45]。为分解2个大素数的乘积，所需的试管数随素数位数呈线性增加，而需要的DNA分子数却呈指数增长，生物运算的数目为多项式增长。由此推算，当分解1 000位的大数时，需要的DNA溶液体积约为2.5×10^{131}升，这是不可能获得的质量。可见这种算法对RSA不能造成威胁。

比弗（Beaver[46]）等人借助阿德尔曼的思想将

大数分解问题转化为哈密尔顿(Hamiltonian)路径问题,分析出1 000位的RSA模的复杂度问题至少需要10^6个顶点数。据保守估计,求解该哈密尔顿路径问题所需溶液的体积远远大于1 020万升,因此也不可行。

布鲁恩(Brun)于2007年提出了基于DNA瓦自组装的加法和乘法模型[47]。同年,布鲁恩在上述工作基础上,提出基于DNA瓦自组装的非确定性整数分解模型[48]。该算法的基本思想是:建立非确定性猜测因子系统。该子系统能非确定性地选择2个数,然后通过乘法子系统,得到这2个数的乘积,同时通过比较子系统,将其与输入数进行比较,如果与输入数符合,即找到了该数分解的因子。文献所提方案需要的DNA瓦种类和误差精度要求,超出了目前分子实验技术水平,仅仅具有理论参考价值。

2.3.3 破译背包密码

背包问题(Knapsack Problem,KP)是运筹学中一个典型的优化难题,在预算控制、项目选择、材料切割和货物装载等实践中有重要应用,也常常作为其他问题的子问题加以研究。石晓龙[49]尝试利用DNA分子计算方法求解整数背包问题,首先设计分子运算筛选出所有可能解,然后在所有可能解中搜索最优解,优化的目标为在所有可能解中搜索价值最大的解。在设计最优解的搜索计算中,可以充分利用DNA计算的并行特点,将带有同位素标记的DNA探针同上一步反应结果进行杂交,以此来实现最优解的搜索。随后,戴尔米拉金(Darehmiraki)和尼赫(Nehi)[50]利用DNA计算的高度并行性在试管中求解0-1背包问题。通过巧妙的编码技术,他们将所求解的问题映射成DNA序列集合,在试管中形成初始解空间,利用分离合并等生物技术,删除不满足约束条件的不可行解所对应的DNA链,并求出每条可行解链所对应的目标函数值,经比较得到最优解所对应的DNA链。以上文献给出的也是理论分析,没有实验验证。

目前已有的背包问题DNA计算的研究都是基于粘帖模型的,通过结合生物芯片技术,实现可行解的提取和最优解的选择。

2.3.4 破译NTRU密码系统

NTRU被认为是21世纪最有前途的公钥密码体制,以速度快、安全性强等优点被广泛应用于数据加密、数字签名等领域。佩尔蒂埃(Pelletier)借助自组装的思想,通过定义相应的三维瓦结构,实现NTRU中所需卷积计算。利用暴力破解的方法,对所有可能的密钥进行卷积计算,根据NTRU的特点找到密钥。但是,由于该方案中的"瓦"尚未设计成功,因此只能从理论上说明其可行性。文献[51]提出了另一种用自组装DNA计算破译NTRU公钥密码系统的非确定性算法。

2.3.5 破译Diffie-Hellman密钥交换算法

Diffie-Hellman密钥交换算法既是最初的公钥密码思想,又是当前人们使用较多的一种重要机制,许多商业产品也使用了这种密钥交换技术。Diffie-Hellman密钥交换算法的目的是使两个用户能安全地交换共享的密钥,以便用户能在后续的通信中用该密钥对消息加密。Diffie-Hellman密钥交换的安全性建立在下述事实之上:求关于素数的模幂运算相对容易,而计算离散对数却非常困难;对于大素数,求离散对数被认为是不可行的。2012年,文献[52]设计了基于自组装模型破译Diffie-Hellman密钥交换算法的方法,该算法给出了自组装模型求解有限域GF(p)(p为素数)上的模乘运算和模幂运算,在此基础上,充分利用算法自组装系统的强大并行性计算能力,提出了自组装算法执行有限域GF(p)上的离散对数问题,即可

得到其中一个用户的私钥，通过PCR和凝胶电泳技术等生物操作来读取自组装体增长后的代表该用户私钥的最终结果，再通过模幂运算即可得到用户双方的会话密钥，进而破译Diffie-Hellman密钥交换算法，且可证明在很多并行的自组装体执行运算过程中寻找成功解的概率可以趋近于1。通过这样的方法，可以威胁到Diffie-Hellman密钥交换的安全。

2.3.6 破译椭圆曲线Diffie-Hellman密钥交换算法

椭圆曲线密码系统是Koblitz和Millef于1985年在各自开发的公钥加密算法中提出的[53]，它是用椭圆曲线有限群代替基于有限域上离散对数问题公钥密码中的有限循环群所得到的一类密码体制。基于椭圆曲线密码体制本身的优点，这种密码体制逐步成为密码学中的重要分支，特别是移动通信安全方面的应用更是加快了这一趋势。椭圆曲线密码的优势逐渐凸显出来，它具有的巨大的商业价值以及军事价值正在为越来越多的人所关注。

文献[54]给出了基于DNA计算模型求解椭圆曲线离散对数的算法。根据有限域GF(2^n)乘法逆元和除法运算的相对复杂性，文献[55]利用自组装模型有效求解有限域GF(2^n)乘法逆元和除法运算的DNA Tile自组装模型。用该模型可在多项式的时间内用常量个Tile类型计算该域乘法逆元和除法运算。该研究成果是椭圆曲线Diffie-Hellman密钥交换算法密码分析工作的重要基础。

以上模型都使用了DNA计算这种全新的计算模式，随着计算量的增加，现有的DNA计算模型的时间复杂度并不显著增加，而其空间复杂度却显著增加。因此，丹·波恩等人的方法只能攻破64位以下对称密码系统。

以上的文献都只是从理论上讨论了DNA计算对传统密码算法的威胁，并没有实验验证。这也凸显出DNA计算在进行大量复杂计算存在的问题，一个是误差随着实验进行被传递放大，一个是需要的DNA分子随着计算规模呈现指数增长。因此，就目前来看，DNA计算还不能对传统加密算法构成实质性威胁。

2.4 DNA作为信息存储载体的信息安全

既然DNA可以作为信息存储介质，存储在此介质上的信息安全如何保障？数据的保密性、完整性和不可否定性等方面，具体在DNA存储中如何实施？就此，也有不少文献研究了相关的算法和方案，也有相关的实验验证。

2.4.1 一次一密

美国杜克大学的阿诗士·杰哈尼（Ashish Gehani）和托马斯·拉宾（Thomas H. Labean）等人提出了一种基于一次性密码本的DNA加密和解密方法[56]。他们设计了两种DNA序列的一次一密加密方法：一种是映射替代法，根据定义的映射表将固定长度的DNA明文序列单元替换成对应的DNA密文序列；另一种是DNA芯片异或法，采用光刻技术和荧光标记技术进行DNA明文序列与密码本序列的异或操作。

陈杰（Jie Chen，音译）等提出了基于DNA计算的分子密码设计[57]。作者利用DNA引物扩增反应进行模2加法运算，以及利用DNA计算的并行性实现一次性密码本（one-time-pads）的加密和解密。

2010年，有文献提出利用DNA自组装的自然过程实现真正的随机密钥的产生，从而利用DNA自组装实现（OTP）加密[58]。

以上方案给出的也是理论分析和仿真分析，没有具体实验验证。

2.4.2 聚合酶链式反应（PCR①）引物作为密钥

安德烈·莱尔（Andre Leier）等人提出了使用DNA二元串②进行加密和解密的方法[59]。该方法利用聚合酶链式反应必须要有正确成对引物的特点，基于DNA二元串对信息进行编码，然后将其

① Polymerase chain reaction，聚合酶链式反应
② 是指使用DNA片段进行编码表示的固定长度的二进制数字串

和大量相似DNA二元串混杂在一起，只有知道正确的引物的发送方和接收方能从聚合酶链式反应中读出消息。该方法类似于信息隐藏技术，其整体方案也符合常规密码模型。另一种方法是利用凝胶电泳的图形进行加密解密。其解密的思路是，当包含信息的DNA串和不包含信息的串混淆在一起时，除了发送双方都需知道正确的混淆串，还要将上述两种串同时进行聚合酶链式反应，然后将得到的凝胶电泳图形相减，最终获得所包含的信息。此方法结合第一种方法，可以组成分子校验码，若发现混淆溶液的凝胶图像发生了明显变化，则说明这次信息交换过程中信息溶液受到了攻击。该文献给出了密钥产生的实验演示，没有完整的实验过程。

田中（K. Tanaka）等人设计了一个使用DNA计算作为陷门函数的密钥共享协议[60]，并且用实验证明了其可行性，只有拥有接收者和发送者的正确引物，才能扩增复制出正确的消息。该协议的安全性受到生物技术的保障。

2.4.3 对语言进行加密

在文献[61]中，讨论了以单词、音节或者字母为单位对某种语言进行DNA加密的技术，特别分析了DNA编码、数据压缩和错误检测等问题，提出合成需要的DNA长链是DNA存储和加密等数据处理在技术实现上普遍存在的困难。

2.4.4 利用DNA探针进行对称加密

在该研究中，对称密钥加密系统是通过应用DNA探针技术、生物芯片和杂交实现加密解密的[62]。信息的加密和解密的密钥由DNA探针形成，而其密文嵌入在一个专门设计的DNA芯片（微阵列）中。该系统的安全性主要来源于生化反应的条件和探针检测的困难，而不是传统的计算复杂性。其具体算法并没有进行实验验证，而是借用了已发表的生物实验方法[63]。

2.4.5 非对称加密和签名技术

在DNA探针对称加密算法的基础上，提出非对称加密和签名技术[64]。类似于传统的公钥密码学，提出的方案使用一对密钥，公有密钥加密和私有密钥签名。其实验基础也是基于文献[60]，并没有进行完整实验验证。

2.4.6 基于DNA计算的信息隐藏方法

DNA隐写术的原理是，利用大量的无关信息隐藏加密后的DNA信息，使得攻击者难以确定正确的DNA片断。只有正确的接收者才能根据事前双方约定的信息找到正确的DNA片断，并获取隐藏于其中的信息。美国纽约市立大学西奈山医学院的班克罗夫特（C. Bancroft）等人首先实现相关实验。他们将一条二战中的著名信息进行DNA隐写，并将其成功地提取出来[65]。卢明欣等人对采用这种方法的信息隐藏技术进行了安全性分析，并提出改进的方法[66]。文献[15]引入一个可逆对比映射实现DNA可逆信息隐藏。文献[16]提出了3个基于DNA序列的信息隐藏方法。该方法主要利用DNA计算的高密度特性，以生物技术作为安全保证，没有涉及复杂的数学运算。

2.4.7 DNA认证

DNA认证方法能够十分准确地认证生物个体的身份，并已广泛应用于司法、金融等领域。DNA鉴别技术的理论基础是生物个体DNA序列的特殊性，且亲缘关系较近的生物体DNA序列具有相似性。在2000年DNA认证技术就应用于奥运纪念商品的认证商标中。已有相关研究利用DNA加密算法进行基于DNA的水印技术，此技术可使DNA水印不但可以印刷在物品上，甚至可以植入活体中[67]，然后通过辨认DNA认

证信息来验证用户身份或版权信息。

3 前景与展望

DNA作为已知的生命遗传信息存储介质至少有35亿年以上历史，其分子结构、密度和寿命，天然适用于信息存储和计算，同时利用DNA分子进行的计算可以具有分子计算的极大并行性优势。

DNA计算及DNA纳米技术研究受到各国政府的高度重视。美国白宫科技部于2011年2月发布“美国2011纳米技术发展战略（NNI）”，该计划旨在协调美国纳米技术的整体研发，增强整个美国在纳米尺度上的科学研究合作力度，确保美国在纳米技术、工程技术方面的世界领先地位[68]。德国联邦教育与研究部也于2011年制定了“纳米技术行动计划2015”，这是德国政府在高科技战略框架下针对纳米领域施政的一个共同纲领。俄国政府于2010年纳米技术国际论坛上明确指出，纳米技术是未来经济的领军力量，表示将打造真正意义上的纳米产业，以便到2015年使国家的纳米行业总产值达到近333亿美元[69]。由英国皇家化学会自2010年发起的“纳米科学的挑战——化学科学前沿国际研讨会”至今已开展8届，会议主要以纳米医学包括药物的纳米级封装和体内投送、纳米材料的定向组装、纳米器件制作与纳米机器等为研究内容[70]。

基于DNA自组装的传感器很小，可以在细胞内工作，具有快速、敏感和特异性高的优点，其纳米结构的控制精度达原子级[71]。DNA纳米技术的应用前景非常诱人，但目前其基础理论、技术和方法仍然存在很多问题待解决，比如作为信息处理单元，其读写成本高，处理时间长；作为结构构建单元，其设计复杂，稳定性和与生物兼容性没有量化的方法衡量；作为纳米机器人，其行为笨拙，无法交流，无法处理复杂任务，也不能在活体中存活。

在我国开展DNA计算及DNA纳米技术的基础理论及应用研究将在未来几十年内提高中国在DNA计算理论及DNA纳米技术应用领域的国际地位，在这一新兴领域迎头赶上并获得一大批原创性成果。数据显示，2007年以来，中国已成为*biosensor and bioelectronics*杂志发表论文最多、下载文献量最大的国家。在2010—2011年度出版、引用率排名前50的研究论文中，有32篇论文来自中国。

具体到信息安全领域，目前基于DNA计算的加密是建立在生化反应的特殊条件、检测困难或特殊结构等基础上的，而不是计算复杂度上。如果结合传统加密算法，配合计算复杂性的生化实现，则DNA加密信息更加安全可靠。因为其数据不但受到生物反应困难的保护，还受到计算复杂度的安全保护。在基于DNA纳米技术的信息安全应用和研究中，有许多问题有待解决。例如，如何利用DNA自组装设计各种刚性结构及合理控制自组装过程，减少功能对DNA分子瓦种类的依赖；如何对信息进行编码，实现信息处理过程中系统具有一定的容错和纠错能力；如何利用DNA自组装和折纸术，从结构上实现DNA分子计算单元的封装，隐藏具体数据格式和处理方式；DNA信息安全体系缺乏理论和算法的支持。

当前，DNA分子计算相关的DNA纳米技术正在迅速发展，DNA计算相关研究的成果越来越丰富，有越来越多的实现方法。随着DNA分子纳米技术在信息存储和处理领域应用的拓展，利用DNA进行的分子级别信息安全问题研究将吸引更多研究人员的注意和兴趣。现在制约DNA计算研究的还是DNA纳米技术与成本问题，目前大量进行DNA分子测序和合成仍然较为昂贵，但DNA纳米技术的快速发展，使得这些费用正在迅速降低。DNA纳米技术的迅猛发展正在并将为基于DNA的分子计算及其在信息安全和存储领域的应用带来翻天覆地的变化。

参考文献

1 Goldman N, Bertone P, Chen S et al. Towards practical, high-ca-

pacity, low-maintenance information storage in synthesized DNA. Nature, 2013, doi:10.1038/nature 11875.

2 Ke Y, Ong L L, Shih W M et al. Three-dimensional structures self-assembled from DNA bricks. Science, 2012, 6111(338): 1177-1183.

3 Han D, Pal S, Nangreave J et al. DNA origami with complex curvatures in three-dimensional space. Science, 2011, 6027(332): 342-346.

4 Douglas S M, Bachelet I, Church G M. A logic-gated nanorobot for targeted transport of molecular payloads. Science, 2012, 6070(335): 831-834.

5 Qian L, Winfree E. Scaling up digital circuit computation with DNA strand displacement cascades. Science, 2011, 6034(332): 1196-1201.

6 Fu T J, Seeman N C. DNA double-crossover molecules. Biochemistry, 1993, 32: 3211-3220.

7 Head T. Formal language theory and DNA: an analysis of the generative capacity of specific recombinant behaviours. Bull. Math. Biol. , 1987, 49: 737-759.

8 Adleman L. Molecular computation of solutions of combinatorial problems. Science, 1994, 266: 1021-1024.

9 International Conference on DNA-based computing and molecular programming (annual meetings). http:// www.dna-computing.org/.

10 International Conference Series. Unconventional computing and natural computing (annual meetings). http:// www.cs.auckland.ac.nz/CDMTCS//conferences/uc/uc.html.

11 Seeman N C. DNA junctions and lattices. J. Theor. Biol., 1982, 99: 237-247.

12 Adleman L, Kari J, Kari L et al. On the decidability of self-assembly of infinite ribbons. In Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS02), November 2002, 530-537, Ottawa, Ontario, Canada.

13 Winfree E. Algorithmic self-assembly of DNA. PhD thesis, June 1998, California Institute of Technology, Pasadena, CA, USA.

14 Winfree E, Liu F, Wenzler L A et al. Design and self-assembly of two-dimensional DNA crystals. Nature, 1998, 394: 539-544.

15 Mao C, LaBean T H, Reif J H et al. Logical computation using algorithmic self-assembly of DNA triple-crossover molecules. Nature, 2000, 407: 493-496.

16 Seelig G, Soloveichik D, Zhang D Y et al. Enzyme-free nucleic acid logic circuits. Science, 2006, 5805(314): 1585-1588.

17 Seeman N C, Kallenbach N R. Design of immobile nucleic acid junctions. Biophys. J, 1983, 44: 201-209.

18 LaBean T H, Yan H, Kopatsch J et al. Construction, analysis, ligation, and self-assembly of DNA triple crossover complexes. J Am Chem Soc., 2000, 122: 1848-1860.

19 Yan H, Park S H, Finkelstein G et al. DNA-templated self-assembly of protein arrays and highly conductive nanowires. Science, 2003, 5641(301):1882-1884.

20 Reishus D, Shaw B, Brun Y et al. Self-assembly of DNA double-double crossover complexes into high density, doubly connected, planar structures. J Am Chem Soc., 2005, 127: 17590-17591.

21 Mathieu F, Liao S P, Kopatsch J et al. Six-helix bundles designed from DNA. Nano Lett., 2005, 5: 661-665.

22 Rothemund P W K. Folding DNA to create nanoscale shapes and patterns. Nature, 2006, 440: 297-302.

23 Um S H, Lee J B, Park N et al. Enzyme-catalysed assembly of DNA hydrogel. Nat Mater., 2006, 5: 797-801.

24 Douglas S M, Chou J J, Shih W M. DNA-nanotube-induced alignment of membrane proteins for NMR structure determination. Proc Natl Acad Sci USA, 2007, 104: 6644-6648.

25 Voigt N V, Torring T, Rotaru A et al. Single-molecule chemical reactions on DNA origami. Nat Nanotechnol, 2010, 5: 200-203.

26 Andersen E S, Dong M, Nielsen M M et al. DNA origami design of dolphin-shaped structures with flexible

tails. ACS Nano., 2008, 2: 1213-1218.

27 Andersen E S, Dong M, Nielsen M M et al. Self-assembly of nanoscale DNA box with a controllable Lid. Nature, 2009, 459: 73-76.

28 Kuzuya A, Komiyama M. Design and construction of a box-shaped 3D-DNA origami. Chem Commun., 2009, 4182-4184.

29 Endo M, Hidaka K, Kato T et al. DNA prism structures constructed by folding of multiple rectangular arms. J Am Chem Soc., 2009, 131:15570-15571.

30 Ke Y, Sharma J, Liu M et al. Scaffolded DNA origami of a DNA tetrahedron molecular container. Nano Lett., 2009, 9: 2445-2447.

31 Douglas S M, Dietz H, Liedl T et al. Self-assembly of DNA into nanoscale three-dimensional shapes. Nature, 2009, 459: 414-418.

32 LaBean T H. Nanotechnology: another dimension for DNA art. Nature, 2009, 459: 331-332.

33 Yurke B, Turberfield A, Mills A et al. A DNA-fuelled molecular machine made of DNA. Nature, 2000, 406(6796): 605-608.

34 Sekiguchi H, Komiya K, Kiga D et al. A design and feasibility study of reactions comprising DNA molecular machine that walks autonomously by using a restriction enzyme. Natural Computing, 2008, 7(3): 303-315.

35 Bath J, Green S, Turberfield A. A free-running DNA motor powered by a nicking enzyme. Angewandte Chemie International Edition, 2005, 44(28):4358-4361.

36 Chen Y, Wang M, Mao C. An autonomous DNA nanomotor powered by a DNA enzyme. Angewandte Chemie International Edition, 2004, 43(27):3554-3557.

37 Yin P, Choi H, Calvert C et al. Programming biomolecular self-assembly pathways. Nature, 2008, 451(7176): 318-322.

38 Lund K, Manzo A J, Dabby N et al. Molecular robots guided by prescriptive landscapes. Nature, 2010, 465: 206-210.

39 Rothke B. DES Is Dead! Long Live ???. Information System Security, 1998, (Spring): 57-60.

40 Ferguson N, Kelsey J, Lucks S et al. Improved cryptanalysis of Rijindael. Proceedings of Fast Software Encryption-FSE'00. LNCS 1978, Spring-Verlag, 2000: 213-230.

41 Kleinjung T, Aoki K, Franke J et al. Factorization of a 768-Bit RSA modulus. Advances in Cryptology- CRYPTO. Lecture Notes in Computer Science, 2010, 6223: 333-350.

42 Shor P W. Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1995, 26(5): 1484-1509.

43 Lipton R, Boneh D. Breaking DES using a molecular computer. DIMACS Series in Discrete Mathematics and Theoretical computer science, 1996, 27:37-58.

44 Adleman L, Rothemund P, Sam R et al. On applying molecular computation to the data encryption standard. Journal of Computational Biology, 1999, 6(1):53-63.

45 Chang W L, Guo M Y, Ho M S. Fast parallel molecular algorithms for DNA-based computation: factoring integers. IEEE Transactions on NanoBioscience, 2005, 2(4):149-163.

46 Beaver D. Factoring: the DNA solution. Asia crypt', 1994, 419-423.

47 Brun Y. Arithmetic computation in the tile assembly model: addition and multiplication. Theoretical Computer Science, 2006, 378: 17-31.

48 Brun Y. Nondeterministic polynomial time factoring in the tile assembly model. Theoretical Computer Science, 2008, 395(1):3-23.

49 石晓龙, 许进. DNA计算与背包问题. 计算机工程与应用, 2003, 27:44-52.

50 Darehmiraki M, Nehi H M. Molecular solution to the 0-1 knapsack problem based on DNA computing. Applied Mathematics and Computation, 2007, 187:1033-1037.

51 张勋才. 基于自组装DNA计算的NTRU密码系统破译方案. 计算机学报, 2008, 31(12):2129-2137.

52 Cheng Z. Nondeterministic Algorithm for breaking Diffie-Hellman key exchange using self-assembly of DNA tiles. International Journal of Computers, Communication and Control, 2012, 7: 616-630.

53 Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 1987, 48: 203-209.

54 Li K L, Zou S T, Xu J. Fast parallel molecular algorithms for DNA-based computation: solving the elliptic curve discrete logarithm problem over GF(2n). Journal of Biomedicine and

Bio-technology, 2008, 2008(1): 1-10.

55 Cheng Z. Arithmetic computation of multiplicative inversion and division in GF(2n) using self-assembly of DNA tiles. Journal of Computational and Theoretical Nanoscience, 2012, 9(3): 336-346.

56 Gehani A, LaBean T H, Reif J H. DNA-based cryptography, in Dimacs Series In Discrete Mathematics & Theoretical Computer Science, 2000, 54: 233-251.

57 Chen J. A DNA-based biomolecular cryptography design. In Proceedings of the 2003 International Symposium on Circuits and Systems, 2003, 822-825.

58 Miki H, Hiroaki K, Kazuhiro O. Design of true random one-time pads in DNA XOR cryptosystem. IWNC, PICT 2, 2010, 174-183.

59 Leier A, Richter C, Banzhaf W et al. Cryptography with DNA binary strands. Biosystems, 2000, 57: 13-22.

60 Tanaka K, Okamotoa A, Saito I. Public-key system using DNA as a one-way function for key distribution. BioSystems, 2005, 81: 25-29.

61 Jonathan P L. Long-term data storage in DNA. TRENDS in Biotechnology, 2001, 19(7): 247-250.

62 Lu M X, Lai X J, Xiao G Z et al. Symmetric-key cryptosystem with DNA technology. Sci China Ser F-Inf Sci, 2007, 50(3):324-333.

63 DeRisi J L, Iyer V R, Brown P O. Exploring the metabolic and genetic control of gene expression on a genomic scale. Science, 1997, 278: 680-686.

64 Lai X J, Lu M X, Qin L et al. Asymmetric encryption and signature method with DNA technology. Information Sciences, 2010, 53(3): 506-514.

65 Clelland C T, Risca V, Bancroft C. Hiding messages in DNA microdots. Nature, 1999, 399: 533-534.

66 卢明欣, 傅晓彤, 秦磊等. DNA信息隐藏方法的安全性分析和保密增强方法. 西安电子科技大学学报(自然科学版), 2006, 33(3): 448-452.

67 Dominik H, Angelika B. DNA-based watermarks using the DNA-crypt algorithm. BMC Bioinformatics, 2007, 8: 176.

68 http://www.bioon.com/trends/news/481704.shtml.

69 http://www.bioon.com/trends/news/471714.shtml.

70 http://meeting.sciencenet.cn/cinfo.aspx?cid=2748.

71 Wengel J. Nucleic acid nanotechnology-towards angstrom-scale engineering. Organic and Biomolecular Chemistry, 2004, 2: 277-280.

Impact and Application of DNA Nanotechnology in Information Security

Chen Zhihua[1] Shi Xiaolong[1] Cheng Zhen[2]

(1 School of Automation, Huazhong University of Science & Technology, Wuhan 430074, China

2 School of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract Based on DNA nanotechnology, various supramolecular (functional units), which can control the nanostructures accuracy of the atomic level, may achieve information storage, computing, moving, targeted drug delivery, and other functions. With the characteristics of ultra-large-scale parallelism, high-density storage, and low power consumption, information storage and computing models based on DNA nanotechnology are inherently suitable for mass storage and parallel processing of information. Such an elegant computing model inspired people to research and develop various computing models, apply them to traditional cryptography, and discuss the security issues about DNA storage, including key search, information encryption, information hiding, and authentication. This paper reviews the impacts of various computing models based on DNA nanotechnology to traditional cryptography, outlines the methods based on DNA nanotechnology applied to encryption and decryption, authentication and signature. At last, the paper summarizes the existing problems in the

DNA nanotechnology-based information security and the prospects of DNA nanotechnology in the field of information security and storage.

Keywords DNA nanotechnology, DNA computing, key search, encryption and decryption

陈智华 华中科技大学自动化学院副教授，博士。研究方向：DNA 纳米技术，信息安全，智能算法。E-mail：chenzhihua@mail.hust.edu.cn

石晓龙 华中科技大学自动化学院副教授，博士。研究方向：DNA 计算，DNA 纳米技术。E-mail：shixiaolong@mail.hust.edu.cn

（接 26 页）

生命科学和医学学部（9 人）

姓名	年龄	专业	工作单位
丁汉	49	机械电子工程	华中科技大学
方岱宁	55	固体力学	北京大学
成会明	49	材料科学与工程	中科院金属所
刘维民	50	润滑材料与技术	中科院兰州化学物理所
李应红	50	航空推进技术	中国人民解放军空军工程大学
邱勇	48	有机光电材料	清华大学
何满潮	57	矿山工程岩体力学	中国矿业大学（北京）
金红光	56	工程热物理	中科院工程热物理所
高德利	55	油气钻探与开采	中国石油大学（北京）

地学部（10 人）

姓名	年龄	专业	工作单位
王成善	61	沉积学	中国地质大学（北京）
王会军	49	大气科学	中科院大气物理所
吴立新	46	物理海洋学	中国海洋大学
张培震	57	地震动力学	中国地震局地质研究所
陈　骏	58	地球化学	南京大学
金之钧	55	石油地质学	中国石油化工股份有限公司石油勘探开发研究院
周成虎	48	地图学与地理信息系统	中科院地理科学与资源所
郭正堂	49	新生代地质与环境	中科院地质与地球物理所
崔　鹏	55	自然地理学与水土保持学	中科院水利部成都山地灾害与环境所
彭平安	52	有机地球化学	中科院广州地球化学所

（转至 123 页）