引用格式:张勋才,孙军伟,王茜,等. 基于 DNA 分子的信息安全技术研究综述[J]. 轻工学报,2016,31(1):67 - 74.
中图分类号:TP309;TP18 **文献标识码**:A
DOI:10.3969/j.issn.2096 - 1553.2016.1.012
文章编号:2096 - 1553(2016)01 - 0067 - 08

基于 DNA 分子的信息安全技术研究综述

Research summary on information security technology based on DNA molecule

张勋才,孙军伟,王茜,崔光照
ZHANG Xun-cai, SUN Jun-wei, WANG Xi, CUI Guang-zhao

郑州轻工业学院 电气信息工程学院,河南 郑州 450002
College of Electric Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, *China*

关键词:
DNA 分子;DNA 密码;DNA 计算;信息安全技术

Key words:
DNA molecule; DNA cryptography; DNA computing; information security technology

摘要:作为一种新的加密方法,DNA 密码以 DNA 为信息载体,充分利用 DNA 分子所具有的超高存储密度、超低能量消耗、超大规模并行计算潜力等优点,可实现加密、认证及签名等密码学功能. 目前基于 DNA 分子的加密方法与认证技术、DNA 计算对传统密码学的破译与分析等研究从各方面发展了信息安全技术,但仍处于起步阶段. 打破现有实验条件的限制,建立基于 DNA 分子信息安全技术的相对完备的理论体系,突破破译分析中的数据复杂度和计算复杂度,将是未来的研究方向.

收稿日期:2015 - 11 - 30
基金项目:国家自然科学基金项目(61472371, 61472372, 61572446);河南省基础与前沿技术研究计划项目(142300413214);河南省高等学校青年骨干教师资助计划项目(2013GGJS—106);河南省高校科技创新人才支持计划资助项目(15HASTIT019)

作者简介:张勋才(1981—),男,河南省郸城县人,郑州轻工业学院副教授,博士,主要研究方向为生物信息处理与智能控制.

Abstract: As a new encryption method, DNA cryptography was based on DNA molecule as the information carrier. Using the ultra-high storage density, ultra-low energy consumption and very large scale parallel computing ability of DNA molecule, encryption, authentication and signature and other cryptographic functions could be achieved. At present, the information security technology was developed from various aspects, such as the encryption method based on DNA, the authentication technology, and the decipher analysis of the traditional cryptography based on DNA computing. However, the research in DNA cryptography was still in infancy. Breaking the limit of existing experimental conditions and building a relatively complete theoretical system based on DNA molecular information security technology, breaking through the data complexity and computational complexity of the analysis would be the future research direction.

0 引言

计算机的面世推动了世界信息化的加速发展. 随着信息的传输和获取更加便捷,信息安全成为一个不容忽视的问题. 而信息安全的核心问题是密码问题. 公元前 5 世纪,密码器械“天书”被成功地应用于战场. 经过两千多年的发展,如今密码学的应用已经渗透到各个领域. 传统密码学是基于数学难题,只要攻击者具有足够强的计算能力,功击对象所设置的密码就能被破解. 在计算机飞速发展的今天,人们在瞬间就可以完成海量数据的计算,这使传统密码学面对前所未有的挑战. 因此,新型加密方法的研究势在必行.

脱氧核糖核酸(DNA)是一种高分子聚合物. 1960 年代,R. P. FEYNMAN 提出分子计算的概念[1]. 1994 年美国加州大学的 L. M. ADLEMAN[2]首次利用 DNA 计算方法解决了“七顶点 Hamilton 路径”问题,实现了 DNA 分子计算. DNA 分子计算是利用 DNA 双螺旋结构和碱基互补配对原则对信息进行编码,把将要运算的对象映射成 DNA 分子链. 通过生物酶的作用,生成各种数据池. 而特定的酶可充当“软件”来完成所需的各种信息处理工作. 之后再按照一定的规则将原始问题的数据运算高度并行地映射成 DNA 分子链的可控的生化反应过程. 最后,利用分子生物技术(如聚合链反应 PCR,聚合重叠放大技术 POA,超声波降解,亲和层析,克隆,诱变,分子纯化,电泳,磁珠分离等)读取运算结果[3-4].

DNA 分子计算拥有独有的数据存储和计算机制,以全新的视角来解决传统的困难问题,成功解决 NP 完全问题后也为密码学开创了全新领域,为信息安全带来了新的机遇. 随着 DNA 计算方法的日益成熟,DNA 密码学理论应运而生. 其主要原理是以现代生物技术为工具,以 DNA 为数据载体,通过挖掘 DNA 分子本身所具有的高并行性和高存储密度,实现加密、隐写、认证及签名等密码学功能[5]. DNA 计算与 DNA 密码自身所具有的发展和应用潜力,将在信息安全领域引发一场新的技术革命. 本文拟对基于 DNA 分子的加密、认证及 DNA 计算对传统密码技术的破译与分析等研究进展予以综述,并给出研究展望.

1 基于 DNA 分子的加密方法

自 L. M. ADLEMAN[2]利用 DNA 计算解决 NP 完全问题之后,由 DNA 计算衍生出的 DNA 密码学无论是在理论上还是在实践中都取得了飞速的发展. 1999 年,A. GEHANI 等[6]以 DNA 序列为载体提出了包括替代法和异或法两种“一次一密”的密码方案. 2000 年,A. LEIER[7]利用 DNA 二进制序列加密信息,实现了两种密码方案的信息隐藏. 2003 年,J. CHEN[8]构建了一种基于 DNA 分子序列的密码体系. 2004 年,饶妮妮[9]提出了一种基于 DNA 重组技术的密

码方案. 2008 年,X. C. ZHANG 等[10]给出了破译 NTRU 的非确定性方案. 2009 年,崔光照等[11]进一步提出了基于 DNA 分子技术的加密方案. 2013 年,G. C. L. GOOF 等[12]将 DNA 微粒子技术与热缩片结合,实现了粒子阵列加密模型. 2014 年,王延峰等[13]综述了基于核苷酸的信息安全现状,并对我国今后在该领域的发展提出了一些建议. 随着科技的进步,密码分析的方法越来越先进,研制新型的加密方法势在必行. DNA 密码学作为信息安全的一个新兴领域,有望与传统密码学、量子密码学一并成为密码学的三大分支[11].

1.1 基于 DNA 计算的"一次一密"加密方法

"一次一密"是指在流密码中使用与消息长度等长的随机密钥,密钥本身只使用一次,其安全性主要取决于密钥的随机生成和不重复使用. 若攻击者没有"一次一密"密码本,即使有再大的计算能力也无法破译"一次一密". 这种算法在理论上是绝对安全的.

DNA 具有体积小的特点,同时具有传统信息存储媒介望尘莫及的信息存储能力. 其作为信息载体可较好地解决庞大密码本生成和存储问题[14-15]. 1999 年,美国杜克大学的 A. GEHANI 等[16]利用 DNA 设计了映射替代法和 DNA 芯片异或法两种方案,实现了"一次一密"的加密方式. 映射替代法是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. 图 1 为"一次一密"密码本 DNA 序列,其中可重复单元由一套来自密码字母集的序列字母 C_i,来自明文字母的序列字母 P_i 和聚合酶"终止"序列三部分组成. 异或法是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,图 2 为利用 DNA 瓦片进行异或运算的过程. 随后,J. CHEN[8]提出了基于 DNA 计算的分子密码设计. 利用 DNA 引物扩增反应进行二进制数的模 2 加法运算,以及利用 DNA 计算的并行性实现了"一次一密"的加密方式. DNA 加密技术是通过可控 DNA 杂交反应实现的加密和解密.

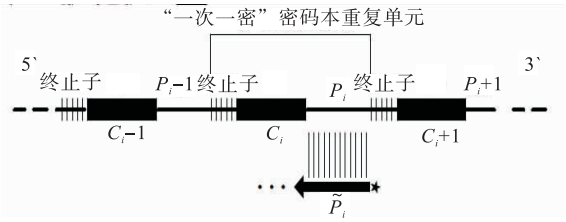


图 1 "一次一密"密码本 DNA 序列[15]

Fig. 1 One-time-pad codebook DNA sequences[15]

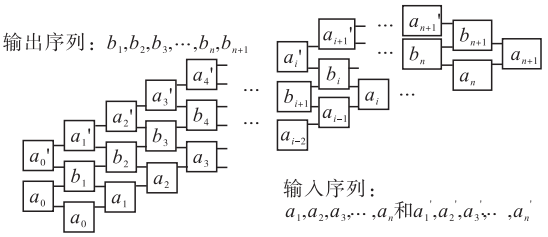


图 2 利用 DNA 瓦片进行异或运算过程示意图[15]

Fig. 2 XOR computation by the use of DNA tiles[15]

另外,以 DNA 分子变性和复性为前提的 DNA 杂交反应包括特异性杂交反应和非特异性杂交反应. 其中,特异性杂交反应在不考虑各类约束条件的前提下,随机生成的 DNA 单链组成一个个 DNA 微点,每个 DNA 微点包含全部的 DNA 单链. 每个 DNA 微点就是一个"一次一密"密码本,生成密码本之后就可以进行"一次一密"的加密. 加密的主要过程包括数据处理、密钥分配、异或运算和信息传输. 这种加密方式可准确获得加密和解密的结果. 然而在实际生化操作过程中,如何快速地分离出所需的密钥、如何对 DNA 密码本进行纠错和长期保存等问题,都需要进一步研究.

1.2 基于 DNA 微点技术的加密方法

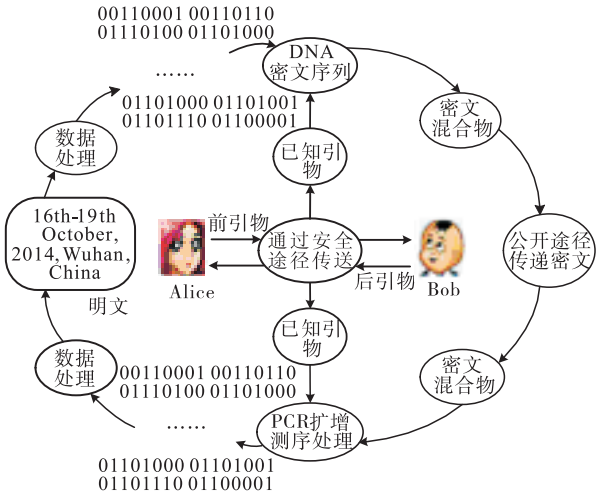
微点运用作为另一种隐藏信息的方法. 微点是一个粘贴在铅字某一点上被无限缩小的图片. DNA 微点技术是 DNA 分子与微点技术成功结合的产物,它实现了数据在分子水平上的

双重隐写功能. 其主要思路是将密文 DNA 链隐藏在大量无关的 DNA 链中,随后以微点的形式进行传输,使攻击者难以确定正确的 DNA 片段. 只有指定的接收者才能根据事先双方约定的引物找到正确的 DNA 片段,并解密隐藏的信息.

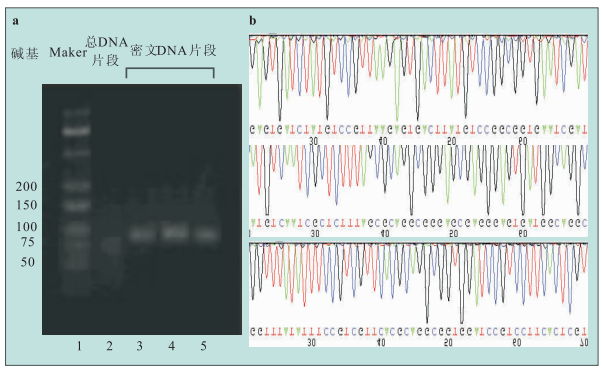
1999 年,C. T. CLELLANG 等[3]将一条二战中著名的信息“June 6 Invasion:Normandy”成功地进行了 DNA 隐写,并最终将其提取出来. 他们首先定义了一种可以把字符转化成碱基的映射表,表中用若干个碱基表示 1 个字符,并按照该映射表将明文映射成 DNA 片段,同时用特定引物序列加以标记. 然后将被标记的 DNA 分子和与其结构相同但碱基排列顺序不同的其他 DNA 分子相混合,喷到信纸上形成无色的微点. 这样就可以通过正常非保密途径进行信息的传输. 接收者收到信件以后,从中提取 DNA 混合溶液,并用引物放大含有明文信息的 DNA 序列,同时采用 PCR 通过分离、纯化等技术手段从 DNA 微点中分离出被标记的 DNA 分子. 最后,用编码的方式对被合成的 DNA 序列进行解码,从而得到明文信息.

该信息隐藏方案具有 3 层安全性. 其一,DNA 微粒无色无味,不易被察觉. 但安全性相对较弱,若破译者具有破译隐形药水的技术便可破解这一信息隐藏方案. 其二,未知的 DNA 溶液是由含有明文信息的 DNA 链和大量与其物理相似的其他 DNA 链混合而成的. 这些混合溶液被分成众多微点,每个微点中都包含数以万计的 DNA 分子,攻击者想要从这些 DNA 链中找到标有明文信息的那一条犹如大海捞针,着实困难. 其三是数学安全性. 若攻击者成功地确认了被标记的 DNA 链,接下来的问题就是将标有明文信息的 DNA 序列还原成明文. 而在此信息隐藏方案中采用的是 3 位核苷酸表示 1 个字母的编码方式,如“GGC”表示的是明文中的字母“E”,但在英文中字母“E”和“I”出现的频率较高,攻击者很容易把关键词作为 PCR 扩增的引物来进行攻击[7,16].

引物序列的安全性在 DNA 微点技术中起着举足轻重的作用. 若攻击者知道正确的引物序列,那么从 DNA 微点中分离出存储有明文信息的 DNA 分子就相当于从未知的溶液中提取特定的 DNA 分子,仅通过 PCR 就可完成. 这样就完全失去了加密的意义. 针对这一点,卢明欣等[17]分析了文献[3]提出的信息隐藏方案的安全性问题,提出了保密增强的算法,以有效阻止以关键词为引物的攻击. 该算法利用微点技术,结合 DNA 数字编码规则和补充规则,借助多引物的概念,设计出一种较好的信息隐藏方案. 其流程图与结果分析如图 3 所示.



a)加密流程



b)结果分析

图 3 保密增强的加密流程及结果分析[17]

Fig. 3 The encryption process and result analysis of privacy amplifications[17]

然而引物序列的安全性却很难实现. 若每次引物的序列都不同,虽然这样安全性很高,却管理困难,每次传输信息的时候需要额外发送关于引物序列的信息;若引物序列不变,虽然管理变得容易,却大大降低了其安全性. 目前,单凭 DNA 微点技术很难保证信息的安全传递,必须综合考虑其他方法. 如何使用 DNA 微点技术安全、有效地传输明文信息还需要进一步的探索与研究.

1.3 基于重组 DNA 技术的加密方法

随着人类基因组计划的完成,DNA 技术已不再单纯地属于生物学范畴. 密码分析者开始利用 DNA 技术攻击现有的密码. 而密码学研究者则利用重组 DNA 技术天然的加密与解密过程,设计新型密码[9]. 那么研究者是如何利用重组 DNA 自身的优势来对明文进行加密与解密的呢? 首先,发送者按照一定的规则将明文信息编码成碱基序列;然后根据映射规则将编好的碱基序列嵌入参考 DNA 序列当中;随后,将隐藏有明文信息的 DNA 序列重组到 DNA 质粒载体中并植入受体细胞内;最后,将隐藏有明文信息的机体与其他大量无关的机体混合在一起发送给接收者. 接收者收到机体后可通过参考序列、生物酶、选择性标记等密钥来破解明文信息.

基于重组 DNA 技术的加密方法可以很好地使接收双方成功地隐藏和提取明文信息,使攻击者成功恢复信息的概率非常小,并且该方法对主动攻击和恶意攻击有较好的稳定性、鲁棒性和安全性.

1.4 基于 DNA 分子的混合加密算法

前面提到的 DNA 加密算法,能对文本信息进行有效加密,但还不能很好地应用于数字图像信息加密. 要更有效地加密图像信息,可以通过融合已有的图像加密算法来实现,如混沌加密算法和视觉加密算法. 基于混沌的图像加密是目前国内外研究的热点,然而传统的基于混沌的图像加密算法大多是基于一维的混沌系统,利用单一混沌映射实现的图像加密算法存在安全性较低、混沌序列易破译、密钥空间小等缺点. 针对这些不足,2010 年,薛香莲[18]提出了一种基于 DNA 序列与多混沌映射的数字图像加密算法,该算法利用 DNA 序列,融合 Cubic 映射、Logistic 映射加密图像,但是加密后图像的像素相关性高,安全性差,物理实现过程复杂. 2014 年,徐光宪等[19]提出了一种基于混沌映射的 DNA 图像加密算法. 2015 年,张健等[20]采用混沌索引和 DNA 互补编码相结合的方法,提出一种数字图像加密技术. 混沌理论与 DNA 计算在信息科学领域中的应用给信息安全领域带来了新的挑战和机遇. 未来将重点融合混沌系统同步[21-24]和 DNA 计算发展新型的保密通信技术.

视觉加密技术是 M. NAOR 等[25]提出的一种有趣的视觉秘密共享机制. 该机制通过编码系统将信息(图像、文本、图表)加密,而信息解密通过裸眼即可,不需要执行计算机操作. 笔者所在课题组在 DNA 芯片技术的基础上,结合视觉加密技术,构造了基于 DNA 芯片的图像隐藏算法,并以郑州轻工业学院校徽为实例,实现图像的加密与解密,流程如图 4 所示[26].

2 基于 DNA 分子的认证技术

信息认证的主要目的无非是两个:一是实体认证,即验证信息的发送者是否具备合法身份,包括信源的认证与识别和信宿的认证与识别;二是验证信息的完整性,也就是验证数据在传输和存储的过程中是否被重放、篡改等. 严格地来讲,DNA 认证技术很少涉及 DNA 计算,它是利用生物个体 DNA 序列的特殊性和亲缘关系较近的生物体之间 DNA 序列的相似性准确地认证出生物个体的身份,现已广泛地应用于

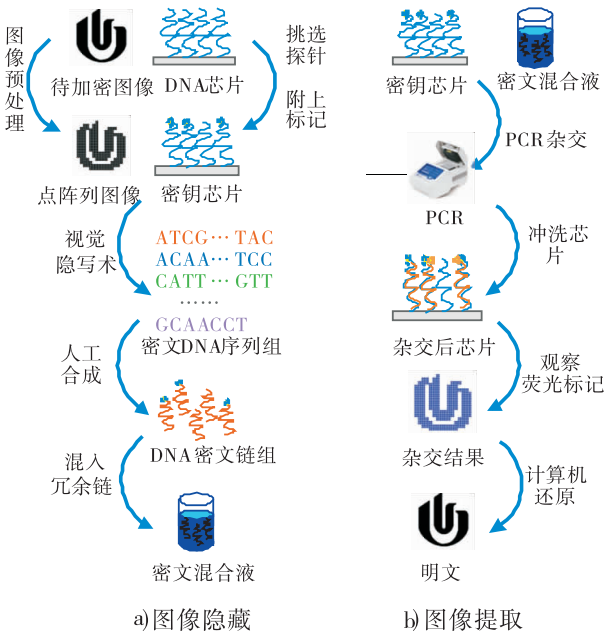


图 4 基于 DNA 计算与视觉算法的图像加密解密流程图[26]

Fig. 4 Flow diagram of image encryption algorithm based on DNA computing and visual cryptography[26]

司法、金融等领域.

2000 年,加拿大的 DNA Technology 公司将文献[3]的信息隐藏方法成功应用于悉尼奥运会商品的商标认证中. 从 T 恤到咖啡杯,所有商品均用一种含有某位未知运动员 DNA 的特殊墨水做标记. 鉴定者利用便携式扫描仪便可通过标记中的 DNA 信息来鉴别纪念品的真伪[27]. 这一防伪标识不仅比普通商标更为便宜,而且想要伪造出这种随机抽取的 DNA 信息也非常困难.

利用 DNA 加密算法开发基于 DNA 的水印技术,不但可以把 DNA 水印印刷在物体上,还可以植入活体内[28],通过辨别 DNA 认证信息来验证用户身份或者版权信息. 目前,DNA 认证技术在基于核算的信息安全技术中的发展已相当成熟,应用也很普遍. 若将 DNA 隐写用于基于核算的识别或鉴定方面,则可以进行更为广泛的信息认证.

3 DNA 计算对传统密码技术的破译与分析

3.1 破译背包密码

背包密码是运筹学中一个典型的优化难题,它在预算控制、材料切割和货物装载等实践中都有着重要的应用,也常被作为其他问题的子问题进行研究. 石晓龙等[29]曾利用 DNA 计算求解整数背包问题. 他首先设计分子运算用以筛选出所有的可能解,随后在所有的可能解中筛选出最优解. 在搜索最优解的设计中,充分利用 DNA 计算的并行特点,将带有同位素标记的 DNA 探针同之前的反应结果进行杂交,来实现最优解的搜索. 随后,M. DAREHMIRAKI 等[30]利用 DNA 计算的高度并行性在试管中求解 0—1 背包问题. 通过编码技术,将所要求解的问题映射成 DNA 序列集合,并使其在试管中形成初始空间解,然后利用分离、合并等技术手段删除不满足约束条件的不可行解所对应的 DNA 链,最后求出每条可行性解链所对应的目标函数值,经比较得到最优解.

3.2 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,它因速度快、安全性强等特点,被广泛应用于数据加密、数字签名等领域. O. PELLETIER 等[31]利用自组装的思想,通过定义相应的分子瓦结构(见图 5),实现了 NTRU 中所需的卷积计算,并借助于暴力破解的方法,对所有可能的密钥进行卷积计算,再根据 NTRU 的特点找到密钥. 但是该方案只能从理论上证明其可行性. X. C. ZHANG 等[10]提出了一种用基于 DNA 自组装破译 NTRU 公钥密码系统的非确定性算法,该算法可以并行地测试每个可能的密钥,以高概率输出正确密钥.

3.3 破译椭圆曲线密钥交换算法

椭圆曲线密码系统问题于 1985 年提出. 该

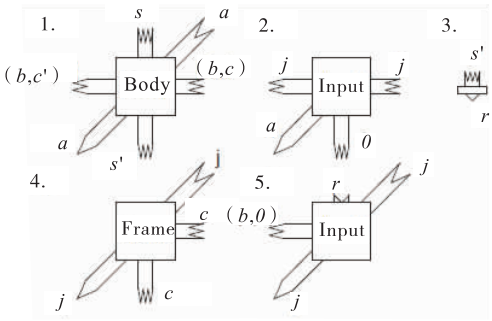


图 5 DNA 分子瓦结构[31]

Fig. 5 The structure of DNA tiles[31]

系统是利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自身的优点,特别是在移动通信安全领域的加速推动下,这种密码体制逐步成为密码学的重要分支. 它所具有的商业价值、军用价值正在被越来越多的人所关注.

K. L. LI 等[33]给出了基于 DNA 计算模型求解椭圆曲线离散对数的算法,Z. CHENG[34]给出了利用 DNA 自组装模型求解有限域 $GF(2^n)$ 乘法逆元和除法运算算法,Diffie-Hellman 密钥交换破译算法[35]等. 在破译公钥密码方面,随着计算量的与日俱增,DNA 计算模型在空间上的复杂度显著增加[36]. 再者,利用 DNA 计算进行大量复杂计算还存在以下两个问题:一个是误差随着实验进行传递放大;另一个是所需的 DNA 分子随着计算规模呈指数增长. 因此,就目前情况来看,DNA 计算还不能对传统加密算法构成实质性的威胁.

4 结论及展望

基于 DNA 分子的信息安全技术是伴随着 DNA 计算的研究与发展而出现的. DNA 密码学作为生命学和密码学的交叉学科,具有传统密码学所不具备的优势,其巨大的开发潜力有望突破破译分析中的数据复杂度和计算复杂度. 但是基于 DNA 分子的信息安全技术的研究尚处于起步阶段,尚未建立起相应的理论、知识和方法等完备的理论体系. 但 DNA 分子所具有的高安全性、高存储容量和高并行性,对当前的信息安全技术既是挑战也是机遇. 现阶段 DNA 密码系统因受投入成本的限制还不能大范围的推广,但其在某些特殊的领域仍然是现有数学密码的有益补充. 随着科学家们对现代生物技术的进一步研究,DNA 密码学必将对信息安全领域产生巨大的影响.

参考文献:

[1] FEYNMAN R P. There's plenty of room at the bottom [J]. Resonance,2011,16(9):890.

[2] ADLEMAN L M. Molecular computation of solution to combinational problems[J]. Science,1994, 266(5187): 1021.

[3] CLELLAND C T,RISCA V,BANCROFT C. Hiding messages in DNA microdots[J]. Nature,1999,399(6736):533.

[4] COX J P L. Long-term data storage in DNA[J]. TRENDS in biotechnology,2001,19(7):247.

[5] 肖国镇,卢明欣,秦磊,等. 密码学的新领域——DNA 密码[J]. 科学通报,2006,51(10):1139.

[6] GEHANI A,LABEAN T,REIF J. DNA-based cryptog-raphy[C]//Aspects of Molecular Computing,Heidel-berg: Springer,2004:167.

[7] LEIER A,RICHTER C,BANZHAF W,et al. Cryptography with DNA binary strands[J]. Biosystems,2000,57(1):13.

[8] CHEN J. A DNA-based biomolecular cryptography design[C]//Proceedings of the 2003 International Symposium on Circuits and Systems,Piscataway: IEEE,2003: 822.

[9] 饶妮妮. 一种基于重组 DNA 技术的密码方案[J]. 电子学报,2004,32(7):1216.

[10] ZHANG X C,NIU Y,GUI G Z,et al. Breaking the NTRU public-key cryptosystem using self-assembly of DNA tilings[J]. Chinese journal of computers,2008,31(12): 2129.

[11] 崔光照,秦利敏,王延峰,等. 基于 DNA 技术的加密方案[J]. 计算机工程与应用,2009,45(8):104.

[12] GOFF G C L, BLUM L J, MARQUETTE C A. Shrinking hydrogel-DNA spots generates 3D microdots arrays[J]. Macromolecular bioscience, 2013, 13(2):227.

[13] 王延峰,韩琴琴,韩栋,等. 基于核酸的信息安全技术研究现状及发展建议[J]. 中国科学院院刊,2014,29(1):83.

[14] 崔光照,秦利敏,王延峰,等. DNA 计算中的信息安全技术[J]. 计算机工程与应用,2007,43(20):139.

[15] 张勋才,韩琴琴,王燕,等. 一种基于 RNA 二级结构的信息隐藏方案[J]. 郑州轻工业学院学报(自然科学版),2014,29(1):1.

[16] 王敏翔,黄永峰. 基于 DNA 序列的信息隐藏模型研究[C]//第九届全国信息隐藏暨多媒体信息安全学术大会会议论文集,[S. L.:s. n.],2010:81 - 86.

[17] 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[J]. 西安电子科技大学学报(自然科学版),2006,33(3):448.

[18] 薛香莲. 基于 DNA 序列与多混沌映射的数字图像加密技术研究[D]. 大连:大连大学,2010.

[19] 徐光宪,郭晓娟. 基于混沌系统的 DNA 图像加密算法[J]. 计算机应用,2014,34(11):3177.

[20] 张健,房东鑫. 应用混沌映射索引和 DNA 编码的图像加密技术[J]. 计算机工程与设计,2015,36(3):614.

[21] SUN J W, YIN Q, SHEN Y. Compound synchronization for four chaotic systems of integer order and fractional order [J]. EPL(europhysics letters),2014,106(4):40005.

[22] SUN J, CUI G, WANG Y, et al. Combination complex synchronization of three chaotic complex systems[J]. Nonlinear dynamics,2014,79(2):953.

[23] WEI Q, WANG X Y, HU X P. Inverse optimal control for permanent magnet synchronous motor[J]. Journal of vibration and control,2015,21(4):801.

[24] SUN J W, SHEN Y, YIN Q, et al. Compound synchronization of four memristor chaotic oscillator systems and secure communication[J]. Chaos,2013,23(1):013140.

[25] NAOR M, SHAMIR A. Visual cryptography[C]// Advances in Cryptology-EUROCRYPT 94, Berlin: Springer, 1995:1 - 12.

[26] ZHANG X C, WANG Y, SHEN C N, et al. An image encryption algorithm based on DNA microarray[J]. Journal of computational and theoretical nanoscience, 2015, doi: 10.1166/jctn.2015.4553.

[27] 肖国镇,卢明欣. DNA 计算与 DNA 密码[J]. 工程数学学报,2006,23(1):1.

[28] HEIDER D, BARNEKOW A. DNA-based watermarks using the DNA-crypt algorithm[J]. BMC bioinformatics, 2007(8):176.

[29] 石晓龙,许进. DNA 计算与背包问题[J]. 计算机工程与应用,2004,39(27):44.

[30] DAREHMIRAKI M, NEHI H M. Molecular solution to the 0-1 knap-sack problem based on DNA computing[J]. Applied mathematics and computation, 2007, 187(2): 1033.

[31] PELLETIER O, WEIMERSKIRCH A. Algorithmic self-assembly of DNA tiles and its application to cryptanalysis [C]//Proceedings of the Genetic and Evolutionary Computation Conference, N. Y. USA: Morgan Kaufmann, 2002:139 - 146.

[32] MILLER V. Use of elliptic curves in cryptography[J]. Lecture notes in computer science,1985,85: 417.

[33] LI K L, ZOU S T, XV J. Fast parallel molecular algorithms for DNA-based computation: solving the elliptic curve discrete logarithm problem over GF(2^n)[J]. Journal of biomedicine and bio-technology,2008,2008:1.

[34] CHENG Z. Arithmetic computation of multiplicative invesion and division in GF(2^n) using self-assembly of DNA tiles[J]. Journal of computational and theoretical nanoscience,2012,9(3):336.

[35] CHENG Z. Nondeterministic algorithm for breaking diffie hell-man key exchange using self-assembly of DNA tiles [J]. International journal of computers, communication and control,2012,7(4):616.

[36] 陈智华,石晓龙,程珍. DNA 计算在信息安全领域的影响与应用[J]. 中国科学院院刊,2014,29(1):70.