



基于核酸的信息安全技术 研究现状及发展建议*

文 / 王延峰 韩琴琴 韩 栋 王 燕 张勋才 崔光照”
郑州轻工业学院 电气信息工程学院 河南 450002

【摘要】 由于具有巨大并行计算能力、海量信息存储密度及超低能耗等优势,近年来,核酸分子在分子计算、数据存储以及信息安全等研究领域广受关注。特别作为基于数学难题的、传统的密码理论与技术的有益补充,以核酸为信息载体的数据隐藏、认证、加密等信息安全技术极富发展前景。文章在介绍基于核酸的加密、隐藏及认证技术原理的基础上,详细论述了该领域国内外的最新研究成果,并对我国如何发展基于核酸的信息安全技术的研究提出了建议。

【关键词】 DNA 密码, DNA 计算, 核酸分子, 信息安全技术

DOI 10.3969/j.issn.1000-3045.2014.01.010

1 引言

2013年6月,美国中央情报局前技术人员爱德华·斯诺登揭露了美国情报机构的“棱镜”秘密情报监视项目。消息一经公布,世界舆论随之哗然,由此而引发的风波愈演愈烈,其涉及面之广,影响力之强,令全世界为之触目惊心。在沸沸扬扬、持续发酵的“棱镜门”事件背后,有两个问题尤其值得思考:一是我们过分地依赖国外的电子及信息技术产品。我国所使用的信息技术、设备、系统和服务大多由参与“棱镜”计划的公司

所提供,缺乏核心技术及独立知识产权。正如中国工程院倪光南院士在“‘棱镜门’事件引发的关于国家信息安全的思考”中所言:“棱镜门”事件充分暴露了我网络空间的软肋,为了消除这个软肋,从根本上提升我国网络空间的防护能力,一个关键举措是用自主可控的国产软硬件和服务来替代进口;二是美国利用大数据等新技术获取他国情报信息的能力已达到一个新的高度,传统的信息安全技术已不能满足保障国家涉密信息安全的需求,需要重新审视我国信息安全的

* 基金项目:国家自然科学基金(61070238,61272022,U1304620),河南省创新型科技人才队伍建设工程支持项目(124200510017),郑州市科技人才队伍建设工程计划项目(131PLJRC648)

** 通讯作者

修改稿收到日期:2013年12月28日



中国科学院

相关能力。

信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏,即保证信息的完整性、可用性、保密性和可靠性。信息安全在任何国家、政府、部门、行业和个人都必须十分重视的问题,是一个不容忽视的国家安全战略。信息安全的核心问题是密码理论及其应用。密码学是研究信息加密、解密及其变换的一门科学。从古老的凯撒密码到现代密码学,已有2 000多年的历史。密码学中的“解密”与“加密”,是一对永恒的“矛”与“盾”的关系,相互依存,相互对立,相互促进,相互发展。一方面,现代密码学,是基于数学的密码学,除了一次一密外,其他的密码系统都只具备计算安全性,其安全性完全依赖于数学上的困难问题,如果攻击者具有足够的计算能力,就可以破译这些密码系统。另一方面,为满足日益增长的大规模、超大规模计算任务的需求,科学家们正在不断地构建新的计算机体系结构,以提高运算速度和信息处理能力。在新型计算方法不断出现与日渐成熟的同时,也对当前的信息安全性提出了严峻挑战。

核酸(Nucleic Acids)是由许多核苷酸聚合成的生物大分子化合物。核酸大分子可分为两类:脱氧核糖核酸(Deoxyribonucleic Acid, DNA)和核糖核酸(Ribonucleic Acid, RNA),在蛋白质的复制和合成中起着储存和传递遗传信息的作用,是生命的最基本物质之一。密码学和遗传学原本是毫不相关的两门学科。但是,随着现代科技的发展,密码学和核酸开始联系在一起,并且关系越来越紧密。1994年,美国南加州大学的Adleman^[1]教授针对图论中的一个NP完全问题——有向哈密顿路问题,首次利用DNA分子,通过DNA编码,并借助连接、变性、复性、聚合酶链式反应(Polymerase Chain Reaction, PCR)扩增、电泳等一系列生物实验操作,完成了对该问题的求解。该成果的重要意义在于其采用了一种全新的计算介质——DNA分子,给出了以现代分子生物学技术实

现目前传统计算机无法解决的困难问题的一种全新求解思路,并开发了该计算模式本身所固有的潜在的巨大并行性。紧接着,1995年,Boneh^[2]等利用DNA计算模型破译了数据加密标准(Data Encryption Standard, DES)算法,并预言任何小于64位的密钥都可以采用这种方法进行破译。该理论模型由于受生物技术、误码率等诸多限制,目前还很难付诸实施,但对基于数学的传统密码体系提出了挑战。由此可见,DNA密码学是伴随着DNA计算的研究而出现的,其原理是以DNA为信息载体,以现代生物技术为实现工具,通过挖掘DNA固有的高存储密度和高并行性等特点,进而实现加密、认证及签名等密码学功能。DNA计算和DNA密码具有巨大的发展和应用潜力,有可能给人类带来前所未有的计算能力和新型的信息安全工具。

2 基于核酸的加密技术

近年来,随着DNA计算和DNA密码学的发展,研究者在传统加密学理论的基础上相继提出了一些基于核酸的加密体系。1999年,Gehani^[3]等提出了一种基于DNA的一次一密机制,给出了替代法和异或法两种一次一密密码方案;2003年,Chen^[4]等构建了一种基于DNA分子序列的密码体系。2004年,饶妮妮^[5]提出了一种基于DNA重组技术的密码系统,并分析了该系统的保密性。2005年,Kazuo^[6]等利用DNA解决了密钥分配问题。2006年,卢明欣^[7]等利用DNA合成技术、DNA克隆技术、DNA扩增技术以及DNA芯片技术,并结合计算复杂度理论提出了一种基于DNA的加密方法。DNA的高并行计算能力和海量数据存储能力、现有生物技术和计算技术的局限性为已有的DNA加密方法提供了多重安全保障。下面介绍现有的几种加密模型。

2.1 一维(序列)加密模型

对于一次一密而言,其安全性完全取决于密钥的随机性,这种算法在理论上是绝对安全的。由于该算法不仅要求密码本的数据完全随机,而

且密码本不能重复利用,所以在传统的电子媒体中实现密码本的生成和存储受到限制。

由于核酸具有体积小、存储量大等特点,以核酸作为信息载体可以较好地解决庞大的密码本生成和存储问题^[8]。因此,1999年,Gehani^[3]等利用DNA实现了一次一密的加密方式,并给出了替代法和异或法两种一次一密密码方案。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所示为一次一密密码本序列,其中可重复单元由来自一套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 以及聚合酶“终止”序列3部分组成。异或法是利用生物分子技术进行DNA明文序列与密码本序列的异或操作,进而实现DNA加密,图2所示为利用DNA瓦片进行异或运算的过程。另外,Gehani等还将DNA计算引入非对称加密机制中,提出利用DNA的超强的并行计算能力以及惊人的信息存储容量,采用比通常加密算法更高复杂度的算法以提高密码系统的强度。用这两种方式实现的一次一密加密机制具

有绝对的安全性,但在实际生化操作过程中,如何保证DNA载体的安全性、如何进行DNA密码本的纠错处理和长期保存等,还有待于进一步的研究。

2.2 二维(图像)加密模型

1999年,Gehani^[3]等还提出了一种用DNA微阵列芯片对2D图像信息进行加密和解密的系统,该系统包括一个待加密的数据集(图像)、一个一次一密密码本和一个固定有可寻址DNA链的芯片,该芯片的组件如图3所示,其中密文-明文字母对链3'端为明文序列,5'端为密文序列,两段之间用见光易分解的碱基类似物连接,5'端的末端用荧光标记(在图中用*表示)。在其加密过程中,首先利用生物技术把可编址DNA链固定在芯片的玻璃底层上,再把密文-明文字母对链退火到被固定的DNA链上,便得到一个被固化的DNA芯片;然后,把信息图片做成一个黑白的光掩膜,将其覆盖在上述DNA芯片上,并用灯光照射,不透明区域下的DNA链不受灯光的影响,透明区域下的

DNA链中的碱基类似物则在灯光照射下裂开,5'端与3'端分离,带荧光标记的5'端游离在溶液中,并被收集在试管里作为要传送的密文DNA。接收者收到密文后,先根据密码本用密文链作为引物,通过非对称PCR附上配对的明文;再让重组的DNA密文-明文字母对链与芯片上固定的DNA链结合;最后在显微

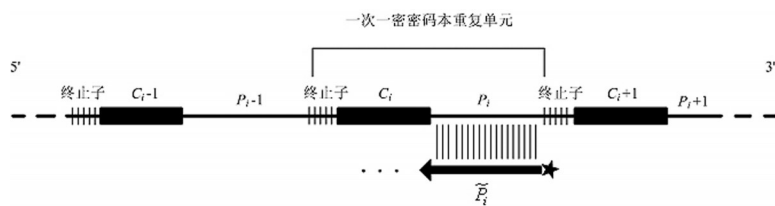


图1 一次一密密码本DNA序列^[3]

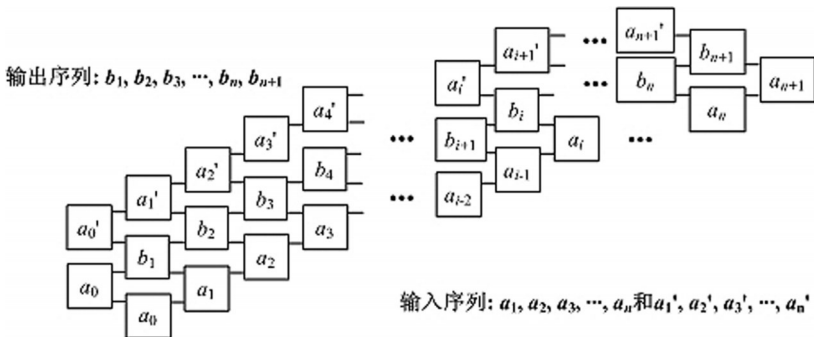


图2 利用DNA瓦片计算异或运算^[3]

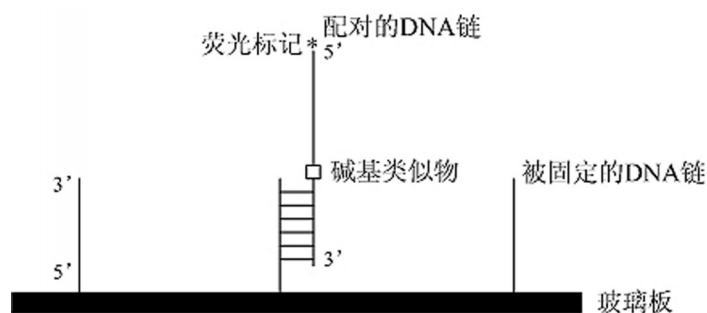


图3 DNA芯片的组件和组合方式^[3]

镜下观察,通过荧光标记读取传送的图像信息。

2012年2月,美国加州斯克里普斯研究院和以色列理工学院的学者们开发出一种用于破译存储在DNA芯片中的加密图像的生物计算机。其“硬件”和“软件”是复杂的生物分子,分子之间可逻辑地进行“交谈”;“输入”是遵循一套特殊法则的经过特殊预定变化的分子,“输出”是另一种分子。它们通过互相激活来执行某个预定的化学反应,当分子相互作用结束后,就可以得到想要的结果。这是DNA密码系统的首个实证研究。

2.3 三维(微粒阵列)加密模型

聚乙烯热缩片是基于聚丙烯的聚合物,其显著特点是遇热时各向同性缩小60%。由于其特殊的性质,多被用于制造微流体器件^[9-12]。2013年,Goff^[13]等把DNA微粒技术与热缩片结合,将DNA聚合物固定在聚乙烯热缩片上,成功地形成了尺寸在100 μm 内的三维DNA水凝胶微粒阵列。在他们的实验过程中,首先把可聚合单体和包含DNA探针的缓冲液混合在一起,用压电式移液枪把混合溶液排列在热缩片上;接着在70 $^{\circ}\text{C}$ 下干燥,用聚丙烯酸甲酯作为交联剂在光诱导聚合中将预聚物变成三维网络状结构;然后在UV紫外线照射下,苯甲酮作为光引发剂,吸光后产生自由基,自由基的共价键便把水凝胶点锚定在热缩片上;最后用蒸馏水彻底洗去杂质,在163 $^{\circ}\text{C}$ 下加热热缩板30秒,随着热缩板的收缩,水泥胶聚合物薄片就同向收缩为水凝胶DNA微粒,底面积较之前缩减60%,高度增加5倍。DNA水凝胶微粒截面放大模型如图4所示。

3 基于核酸的信息隐藏技术

信息隐藏是信息安全领域中的一种新技术,它通过把秘密信息隐藏在公开的媒体信息里,达到证实该媒体信息的所有权归属和完整性或传递秘密信息的目的。近年来,随着网络技术和数字媒体技术的发展,信息隐藏技术受到人们的广泛重视。基于核酸的信息

隐藏技术为信息安全的发展提供了一种新的思路,为信息安全的研究提供了一个新的方向。与以多媒体为载体的信息隐藏相比,基于核酸的信息隐藏不仅能够传递秘密信息,而且还可以保护医学、分子生物学、遗传学等领域的知识产权。此外,由于核酸序列可对抗常规的信号处理和几何攻击,所以基于DNA序列的信息隐藏方式更加稳健。

正是由于核酸具有适用于信息隐藏这些特性,学者们陆续提出了一些以核酸作为隐写载体的信息隐藏方案。1999年,Clelland^[14]等成功地将信息隐藏到DNA微点中,实现了基于生物操作的隐写。2006年,卢明欣^[15]等分析了该DNA信息隐藏方法的安全性,并提出了具体的保密增强的方法。2000年,Leier^[16]等提出了一种使用引物做为密钥来解码加密的DNA序列密码方案。2002年,Shimanovsky^[17]等提出了利用冗余密码子在信使核糖核酸(Messenger Ribonucleic Acid, mRNA)中进

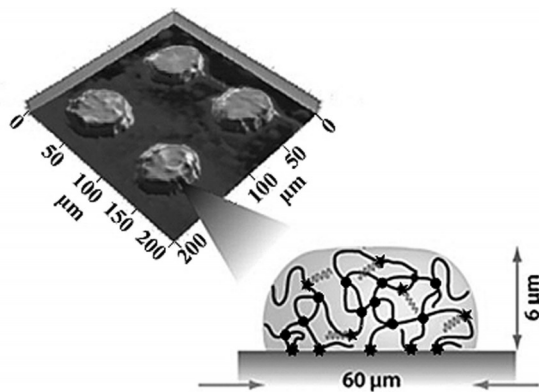


图4 DNA水凝胶微粒截面放大模型。其中圆点为探针网络交联点,五角星点为水凝胶固定探针的共价键,七角星点为吸附到热缩板表面的共价键^[13]

行隐写,并给出了用算术编码进行信息嵌入的隐写方法。2005年,郑国清^[18]等提出了先把秘密信息进行预处理变成一维DNA序列,再将秘密信息隐藏在载体DNA序列中的信息隐藏算法。2007年,Sarb^[19]等提出了两种基于DNA的信息隐藏方法,他们利用重组DNA技术和DNA突变技术将信息DNA链嵌入至另一条DNA链,具有较高的嵌入容量。2010年,Shiu^[20]等提出了3种基于DNA序列的可逆数据隐藏方案,分别是插入法、互补配对法和替代法。2011年,Mousa^[21]等采用可逆的对比映射技术将秘密信息隐藏到DNA序列中,并成功地恢复出了秘密信息。为了增强信息隐藏的安全性和嵌入率,有学者将传统加密方法和信息编码理论应用于信息嵌入。2012年,Guo^[22]等提出了一种基于DNA序列的信息隐藏方案。他们在两个秘密信息位和互补规则之间建立了一个单映射关系,可以有效地将两个秘密信息位替换为一个字符,该方案具有较高的嵌入容量和较低的修改率。总之,生物技术及DNA计算在信息科学领域的应用给信息安全领域带来了新的挑战和机遇。而基于核酸的隐写作为信息安全的一个分支,正变得越来越重要。

3.1 基于DNA微点的信息隐藏

微点是一个粘贴在铅字某一点上的无限缩小了的图片,是一种隐藏信息的方法。微点技术可进一步延伸为基于DNA的一种双重隐写技术。人们可以用单一的微点来发送不同的个人信息,即给每个预期接收者发送重复的DNA微点,接收者都拥有自己特有的引物序列,他们收到含有明文信息的微点后,就用自己固有的引物序列只放大自己预期接收的信息。除了用于密码学,微点还可广泛地应用于如特定商标的版权归属问题等其他领域^[8]。

基于DNA微点的信息隐藏主要是利用大量的与DNA无关信息隐藏加密后的信息,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。Clelland^[14]等最早完成了关于DNA微点的信息隐藏实验,他们将一条二战中的著名信息“June 6 Invasion: Normandy”进行了DNA隐写,并最终成功将其提取出来。在其试验中,他们首先定义了一种将字符转化成碱基的映射表,并按照该映射表将明文信息编码成DNA链,同时在这段DNA链尾部加上了一段特殊的标记信息;然后用超声波将人类DNA片段破碎成大量含有与明文信息的DNA链物理相似的DNA链,并将这些无关的DNA链作为冗余信息与含有明文信息的DNA链混合,再喷到信纸上形成无色的微点后,就可通过普通的非保密途径进行信息传送。经过信件的邮寄和接收后,从信件上提取到混合的DNA溶液,用引物来放大含有明文信息的DNA序列,再通过凝胶电泳来分析PCR产物;最后,用编码方式去解码合成的DNA序列,进而得到明文信息。图5是其信息隐藏方法的基本流程。需要说明的是,原文中把编码方式作为密钥的说法并不准确,真正的密钥应该是引物和编码方式。

对于Clelland等提出的信息隐藏方法而言,由于含有明文信息的DNA链与大量其他物理相似的DNA链混合后被分成了众多的微点,而每个微点都包含了数以亿计的DNA分子,并且DNA微点不易被发现,所以对于攻击者而言,即使能够在大量的微点中确定信息存在于哪个微点中,但要在该微点所包含的亿万条DNA链中选择正确的一条还是如大海捞针一样困难。而解密消息的关键在于寻找一段具有特殊尾部标记的



中国科学院

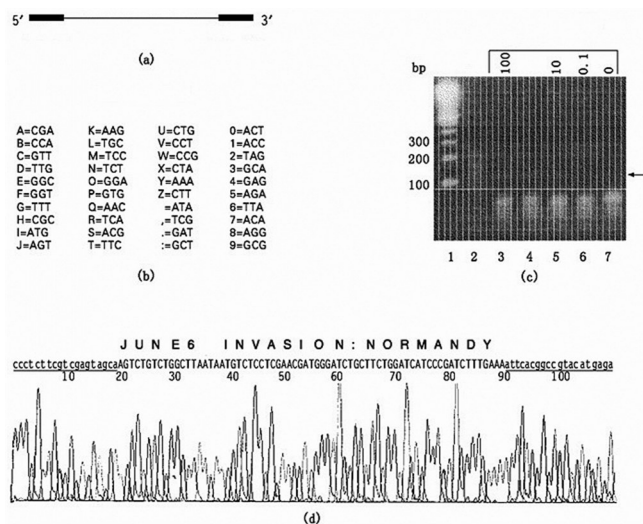


图5 信息隐藏方法。其中,(a)合成的消息序列;(b)编码方式;(c)PCR扩增结果;(d)PCR扩增后通过测序得到的消息序列及其对应的明文^[14]

DNA链,这可以通过DNA计算的方法来搜寻。一旦DNA链通过标记进行了确认,接收者就可采用PCR来复制该DNA链并解密得到信息。Clelland等提出的信息隐藏方案采用的是三位核苷酸表示一个字母的编码方式,例如“A”=CGA,但英文中“E”和“I”出现的概率较高,攻击者容易把关键词作为PCR扩增的引物来进行攻击^[16,23]。

从生化实验角度讲,Clelland等提出的信息隐

藏方法符合生物学原理,比较容易实现。但Clelland等未对其信息隐藏方案的安全性进行全面的分析与论述。

3.2 基于密码子的信息隐藏

遗传密码是将DNA编译成蛋白质的一套特殊指令。其中,DNA编译是将每3个碱基读取为1个氨基酸,进而组成蛋白质。一般地,这种能够翻译成氨基酸的3个碱基被称为基因的密码子,核酸分子由4种碱基组成,故密码子共有 $4^3=64$ 种不同的排列方式,但组成蛋白质的基本氨基酸只有20种,不同的密码子会被翻译成同一个氨基酸,如GCU、GCC、GCA、GCG这4种密码子都会被翻译成丙氨酸。科学家们认为这些被翻译成同一种氨基酸的不同密码子,包含的只是重复的信息,故将其称为冗余密码子。利用这一特性就可以通过冗余密码子的替换来实现信息隐藏,密码子和氨基酸的对应关系如表1所示。

2003年,Shimanovsky^[17]等利用冗余密码子将信息隐藏在mRNA序列中,并提出了利用算术编码进行信息嵌入的隐写方法。在他们所给出的方案中,更换冗余密码子只是改变了原来核酸序列中的核苷酸,不会影响转录的结果。但需要一个

表1 密码子和氨基酸的对应关系

氨基酸	密码子	氨基酸	密码子
Ala/A	GCU,GCC,GCA,GCG	Leu/L	UUA,UUG,CUU,CUC,CUA,CUG
Arg/R	CGU,CGC,CGA,CGG,AGA,AGG	Lys/K	AAA,AAG
Asn/N	AAU,AAC	Met/M	AUG
Asp/D	GAU,GAC	Phe/F	UUU,UUC
Cys/C	UGU,UGC	Pro/P	CCU,CCC,CCA,CCG
Gln/Q	CAA,CAG	Ser/S	UCU,UCC,UCA,UCG,AGU,AGC
Glu/E	GAA,GAG	Thr/T	ACU,ACC,ACA,ACG
Gly/G	GGU,GGC,GGA,GGG	Trp/W	UGG
His/H	CAU,CAC	Tyr/Y	UAU,UAC
He/I	AUU,AUC,AUA	Val/V	GUU,GUC,GUA,GUG
START	AUG	STOP	UAA,UGA,UAG

可逆隐藏机制,不仅可以隐藏信息到核酸序列中,而且也可以完全恢复出原始序列。

王敏翔^[24]等利用核苷酸数据库中的DNA序列载体提出了一个信息隐藏模型。DNA序列在数据库中都有自己的ID,在数据库中可以查询出从任意位置起到任意位置结束的DNA基因序列。在该模型中,定义密钥K是由DNA在基因数据库中的ID号P、开始替换的基因在DNA序列中的基因序号q以及密码子序列的密码子个数r组成的三元组 $K=(p,q,r)$,其中P是事先商定的,q是一个随机数。他们将载体DNA序列S、密钥 $K=(p,q,r)$ 、秘密信息W、一套二进制与DNA编码的转换规则以及冗余密码子替换规则作为输入,通过算法输出隐藏有信息的伪DNA序列f。图6是该信息隐藏的基本流程图,信息提取过程是信息隐藏过程的逆过程。

对于王敏翔等提出的信息隐藏模型,攻击者唯一可做的就是通过搜索DNA数据库来寻找用来进行秘密通信的载体序列,从而找出发送者到底用哪条DNA作为载体。由于公开基因库具有大量的序列并呈爆发式增长,攻击者破解信息的概率几乎为零。对于恶意攻击者进行伪造消息或者以发送方的名义进行秘密通信,其首先要知道通信双

方所选用的DNA序列是哪个,而信息隐藏所用的DNA序列号是作为密钥事先知道并保密的,只有正确密钥的拥有者才能检测、提取隐藏的信息,因此该模型可对抗攻击者的恶意攻击。

3.3 基于DNA载体和重组技术的信息隐藏

崔光照等在传统隐藏技术的基础上,利用有机体(如质粒)作为载体来实现信息隐藏,提出了一种基于DNA载体和重组技术的信息隐藏方法。其中,信息的隐藏过程包含两部分:一是基于DNA序列的数据隐藏;二是基于DNA重组技术的信息隐藏。首先,发送方按照一定的规则把明文信息编码成碱基序列后,根据设计的单映射规则表将其嵌入到参考DNA序列中;然后,将隐藏有明文信息的DNA序列重组到DNA质粒载体中并植入到受体细胞内;最后,将隐藏有明文信息的有机体与大量无关的有机体一同发送给接收者。接收者可通过选择性标记、生物酶以及参考序列等密钥破解出明文信息。基于DNA载体和重组技术的信息隐藏过程如图7所示。

图8给出了以质粒载体为例实现信息隐藏的实验过程。首先,将明文信息隐藏在一个DNA序列中并合成;然后,使用限制性

内切酶和连接酶将合成的DNA序列片段和标记基因片段连接到质粒载体上,将所得的重组质粒进一步隐藏到细菌(如大肠杆菌)体内;最后,将含有明文信息的细胞隐藏到大量无关的伪装细胞中发送出去。接收者接受到菌体后可通过选择性培养筛选出含有隐藏信息的细胞,进而通过测序技术恢复出明文信息。

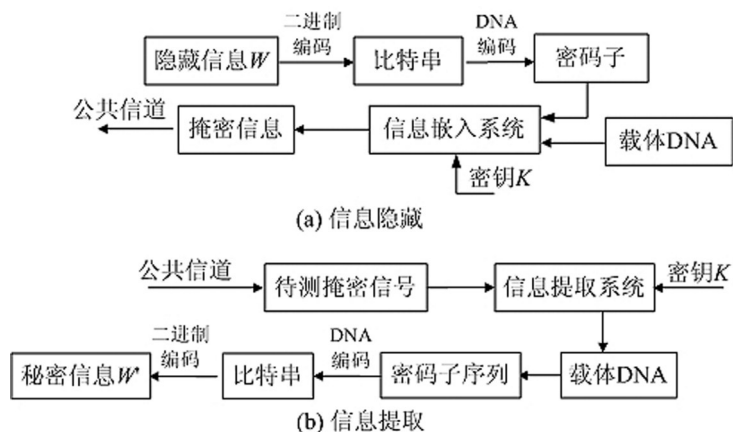


图6 信息隐藏的基本流程图^[24]

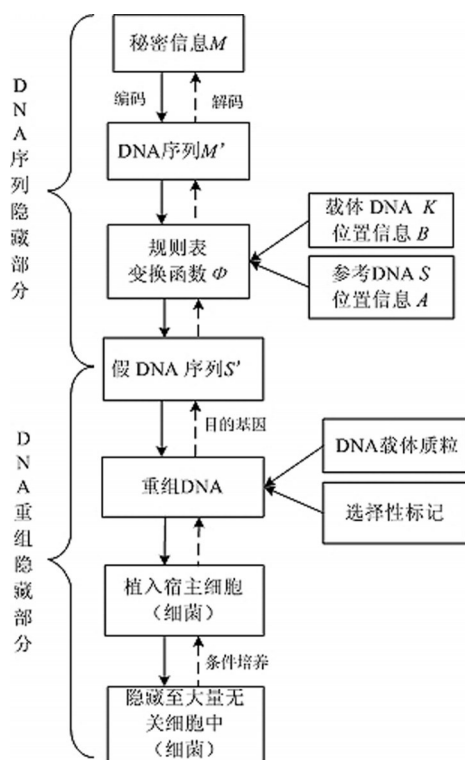


图7 基于DNA载体和重组技术的信息隐藏过程

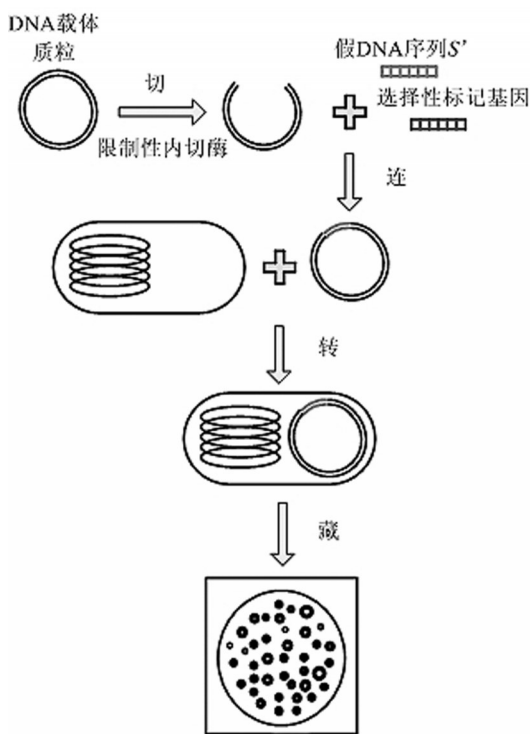


图8 以质粒载体为例实现信息隐藏的实验流程

实验结果和安全性分析表明,发送和接收双方能够成功地隐藏和提取信息,攻击者成功恢复出秘密信息的概率非常小,并且该隐藏方案可对抗主动攻击和恶意攻击,具有较好的鲁棒性、稳定性和安全性。

3.4 基于RNA二级结构信息隐藏

除了基于DNA载体和重组技术的信息隐藏方法外,崔光照等还开展了基于RNA二级结构的信息隐藏方法研究。基于RNA二级结构的信息隐藏方法主要包括发送方隐藏和接收者提取两部分。发送方首先要选取一条参考RNA序列,再将编码成RNA序列的秘密信息随机嵌入到参考RNA序列,然后在特定的软件上预测该序列在特定条件下的二级结构,根据它的二级结

构确定密文的位置信息,最后将该序列及位置信息发送给接收者;接收者接收到序列和位置信息后,通过约定的软件和条件恢复出秘密信息。对于该方案而言,秘密信息即为明文,发送的序列即为密文,而位置信息、特定的软件和条件即为密钥。基于RNA二级结构的信息隐藏方案的流程如图9所示。

由于这些信息只需通过通信信道或者网络传

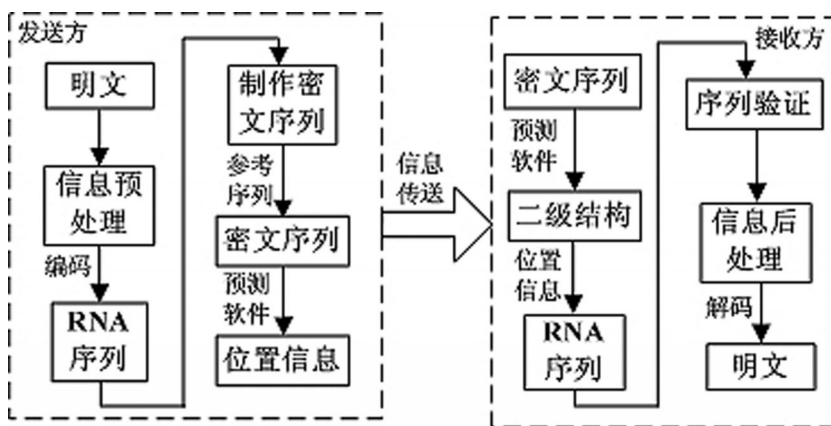


图9 隐藏方案流程图

送给接收者,不需要经过任何生物实验,所以该方案具有方便、快捷、及时、灵活等优点,可应用于对安全性和效率要求都较高的即时通信系统,实现实时传递以及点对点的数据交换。安全性分析也表明该方案有较好的安全性和稳健性。

4 基于核酸的认证技术

信息认证的目的是两个方面:一是验证信息的发送者是否合法,即实体认证,包括信源、信宿的认证和识别;二是验证信息的完整性,验证数据在信息的传输和存储过程中是否被篡改、重放或延迟等。核酸分子作为一种特殊载体在信息认证技术中已有不少成功应用。

每个生物个体具有唯一一套核酸序列,生物个体核酸序列具有特殊性,亲缘关系较近生物体核酸序列具有相似性。对于像人类的DNA这样一个具有数亿碱基对的大分子,没有人怀疑它的独特性。所以,核酸分子因其庞大的差异性和唯一性广泛用于身份鉴定及认证技术等。相比而言,RNA的分子结构不如DNA的分子结构稳定,所以目前应用较多的是DNA认证技术,主要是利用DNA的生物特性,在司法、金融等领域用于准确认证生物个体的身份。

2000年,加拿大的DNA Technology公司将Clelland^[14]等的信息隐藏方法成功地应用于悉尼奥运会的授权产品认证和防伪。从奥运T恤到咖啡杯,所有的商品都用一种包含一位匿名的澳大利亚运动员DNA的特殊墨水做了标记,利用一个便携式扫描器通过扫描墨水标记中的DNA信息就可以鉴别纪念品是否为真品,所增加的成本仅为5美分,比通常的全息商标更便宜^[8]。由于墨水中的DNA片段随机地取自于近百名运动员中的某一位的基因组,所以伪造这一DNA信息是十分困难的。我国文化部也启用了

利用特制生物DNA油墨技术在内的新版音像制品防伪标识。新标识可由指定实验室进行专业测量,直径18毫米,可视性强,易于识别。在出版发行的音像制品上加贴固定号段的防伪标识,将更加有利于管理部门的识别和打击盗版。

目前,在基于核酸的信息安全技术当中,DNA认证技术发展得最为成熟,应用也最为广泛。若将DNA隐写的原理用于基于核酸的识别或鉴定方面,则可以进行更广泛意义上的信息认证^[8];若将DNA认证和DNA隐写原理应用于DNA计算中,则可以提高算法的复杂度及安全性。

5 对开展我国基于核酸的信息安全技术研究的建议

基于核酸的密码技术是生命科学和密码学的交叉学科。同现代密码学相比,基于核酸的密码技术既有现代密码技术的共性,又有自己独有的特性。针对基于核酸的密码技术的优缺点和国内外研究现状,对开展我国基于核酸的信息安全技术的研究提出以下几点建议:

(1) 争取先机,寻求创新。与传统的密码体系相比,基于核酸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。但核酸所具有的高安全性、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,若能把握住先机,就等同于原始创新。对于中国科技来讲,要实现真正创新,引领前沿技术,不仅需要具备高素质的科研人员,更需要政府管理和决策部门对新出现的前沿方向和技术研究提供及时有效的支持。

(2) 多技术集成,跨学科研究。密码学和遗传学原本是两门毫不相关的学科,这两个学科领域的科研人员以往很少在一起工



中国科学院

作,彼此不熟悉对方的研究领域,这使得DNA密码的研究充满了艰辛。基于核酸的信息安全技术的研究,作为一个综合性强的交叉学科研究领域,需要多领域的科研人员共同参与,团结合作,资源共享,推动该领域研究的快速发展。

(3)把握研究方向,建立系统的研究体系。纵观国内外相关技术的研究现状,已逐渐形成了与其相关的DNA自组装与折纸术、DNA链置换技术与逻辑门电路、DNA芯片与信息安全技术等研究方向。建议时刻把握该领域的国际学术前沿,紧密结合我国需求现状,支持创新能力强的研究队伍,积极建立相应的研究体系,深入系统地开展相关技术研究,以取得突破性进展及原始性创新成果。

总之,基于核酸的密码系统具有传统密码系统所不具备的优势,并具有巨大开发潜力^[25],有望突破破译分析中的数据复杂度和计算复杂度。虽然现阶段基于核酸的密码系统受成本限制还不可能大范围地推广使用,但在某些如国家安全等特殊领域,其作为现代密码学的有益补充,发展核酸密码学具有其独特的战略意义。随着现代生物技术的进一步发展以及该领域科学家们的共同努力,具备了相应的物质条件与理论基础,则从事核酸密码系统的研发者必将在未来的信息安全领域占得先机,并对加速我国的国防现代化产生深刻的影响。

参考文献

- 1 Adleman L M. Molecular computation of solutions to combinatorial problems. *Science*, 1994, 266(5187): 1021-1024.
- 2 Boneh D, Dunworth C, Lipton R J. Breaking DES using a molecular computer. Princeton University, Department of Computer Science, 1995.
- 3 Gehani A, LaBean T H, Reif J H. DNA-based Cryptography. 5th Annual DIMACS Meeting on DNA Based Computers (DNA 5), 1999.
- 4 Chen J. A DNA-based biomolecular cryptography design. *IEEE International Symposium on Circuits and Systems*, 2003, 3: 822-825.
- 5 饶妮妮. 一种基于重组DNA技术的密码方案. *电子学报*, 2004, 32(7): 1216-1218.
- 6 Tanaka K, Okamoto A, Saito I. Public-key system using DNA as a one-way function for key distribution. *Biosystems*, 2005, 81(1): 25-29.
- 7 卢明欣, 陈原, 秦磊等. 一种基于DNA技术的加密方法. *西安电子科技大学学报(自然科学版)*, 2006, 33(6): 939-942.
- 8 崔光照, 秦利敏, 王延峰等. DNA计算中的信息安全技术. *计算机工程与应用*, 2007, 43(20): 139-142.
- 9 Fintschenko Y. A modular approach to microfluidics in the teaching laboratory. *Lab on a Chip*, 2011, 11(20): 3394-3400.
- 10 Taylor D, Dyer D, Lew V et al. Shrink film patterning by craft cutter: complete plastic chips with high resolution/high-aspect ratio channel. *Lab on a Chip*, 2010, 10(18): 2472-2475.
- 11 Mandon C A, Heyries K A, Blum L J et al. Polyshrink™ based microfluidic chips and protein microarrays. *Biosensors and Bioelectronics*, 2010, 26(4): 1218-1224.
- 12 Diaz-Quijada G A, Peytavi R, Nantel A et al. Surface modification of thermoplastics-towards the plastic biochip for high throughput screening devices. *Lab on a Chip*, 2007, 7: 856-862.
- 13 Goff G C L, Blum L J, Marquette C A. Shrinking Hydrogel-DNA Spots Generates 3D Microdots Arrays. *Macromolecular Bioscience*, 2013, 13(2): 227-233.
- 14 Clelland C T, Risca V, Bancroft C. Hiding Messages in DNA Microdots. *Nature*, 1999, 399(6736): 533-534.
- 15 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.
- 16 Leier A, Richter C, Banzhaf W et al. Cryptography with DNA binary strands. *Biosystems*, 2000, 57(1): 13-22.
- 17 Shimanovsky B, Feng J, Potkonjak M. Hiding data in DNA. 5th International Workshop on Information Hiding, 2002, 2578: 373-386.
- 18 郑国清, 刘九芬, 黄达人等. DNA序列作为信息隐藏载体的研究. *中山大学学报(自然科学版)*, 2005, 44(1): 13-16.
- 19 Saeb M E, El-Abd E, E. el-Zanaty M. On covert data communication.

- tion channels employing DNA recombinant and mutagenesis-based steganographic techniques. Proceedings of the 2007 WSEAS International Conference on Computer Engineering and Applications, 2007: 200-206.
- 20 Shiu H J, Ng K L, Fang J F et al. Data hiding methods based upon DNA sequences. Information of Science, 2010, 180(11): 2196-2208.
- 21 Mousa H, Moustafa K, Abdel-Wahed W et al. Data Hiding Based on Contrast Mapping Using DNA Medium. The International Arab Journal of Information Technology, 2011, 8(2): 147-154.
- 22 Guo C, Chang C C, Wang Z H. A new hiding scheme based on DNA sequence. International Journal of Innovative Computing, 2012, 8(1): 139-149.
- 23 王敏翔, 黄永峰. 基于DNA序列的信息隐藏模型研究. 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, 2010, 81-86.
- 24 蒋君, 殷志祥. DNA 密码对比传统密码学与量子密码学的优势与不足. 科学视界, 2012, 24:24-27.

Information Security Technology Based on Nucleic Acids

Wang Yanfeng Han Qinqin Han Dong Wang Yan Zhang Xuncai Cui Guangzhao

(School of Electric and Information Engineering, Zhengzhou University of Light Industry,
Zhengzhou 450002, China)

Abstract For the past few years, nucleic acid molecules have drawn a lot of attention in such fields as molecule computing, data storage, information security, etc., due to their huge potential of parallel computing ability, immense information storage density, and ultra-low energy consumption. Particularly, information security technologies such as data hiding, authentication, and encryption using nucleic acids as information carriers, have a brilliant and promising prospect. They are useful complementary to mathematically problematic and conventional cryptography theory. Based on the basic theory introduction of data hiding, authentication, and encryption implemented by nucleic acids, latest international and domestic research achievements are elaborated in this paper, and the suggestions on the development of information security technology based on nucleic acids in China are proposed as well.

Keywords DNA cryptography, DNA computing, nucleic acids, information security technology

王延峰 郑州轻工业学院电气信息工程学院副院长, 教授, 硕导, 河南省信息化电器重点实验室主任。1973年3月出生, 理学博士。主要从事生物信息计算与智能计算领域的研究工作。主持承担了国家自然科学基金、河南省科技创新人才计划(杰出青年)、郑州市杰出科技领军人才等10多项研究工作。在国内外重要学术期刊发表学术论文30余篇。
E-mail: yanfengwang@yeah.net

崔光照 郑州轻工业学院电气信息工程学院院长, 二级教授, 硕导, 兼任河南省电工技术学会理事长。1957年9月出生, 理学博士。主要从事信息化电器、生物信息处理与智能计算领域的研究工作。主持承担了国家自然科学基金、河南省科技创新人才计划(杰出人才)、河南省科技创新团队等多项研究工作。在国内外重要学术期刊发表学术论文60余篇。
E-mail: cgzh@zzuli.edu.cn



中国科学院