Chinese Science Bulletin 2006 Vol. 51 No. 12 1413—1420

DOI: 10.1007/s11434-006-2012-5

New field of cryptography: DNA cryptography

XIAO Guozhen[1], LU Mingxin[1], QIN Lei[2] & LAI Xuejia[3]

1. National Key Lab of ISN, Xidian University, Xi'an 710071, China;
2. Queen's University, Cancer Research Institute, 10 Stuart St. Kingston, ON K7L3N6, Canada;
3. Department of Computer Science & Engineer, Shanghai JiaoTong University, Shanghai 200030, China

Correspondence should be addressed to Lu Mingxin (email: seulmx@126.com)

Received December 19, 2005; accepted January 16, 2006

Abstract DNA cryptography is a new born cryptographic field emerged with the research of DNA computing, in which DNA is used as information carrier and the modern biological technology is used as implementation tool. The vast parallelism and extraordinary information density inherent in DNA molecules are explored for cryptographic purposes such as encryption, authentication, signature, and so on. In this paper, we briefly introduce the biological background of DNA cryptography and the principle of DNA computing, summarize the progress of DNA cryptographic research and several key problems, discuss the trend of DNA cryptography, and compare the status, security and application fields of DNA cryptography with those of traditional cryptography and quantum cryptography. It is pointed out that all the three kinds of cryptography have their own advantages and disadvantages and complement each other in future practical application. The current main difficulties of DNA cryptography are the absence of effective secure theory and simple realizable method. The main goal of the research of DNA cryptography is exploring characteristics of DNA molecule and reaction, establishing corresponding theories, discovering possible development directions, searching for simple methods of realizing DNA cryptography, and laying the basis for future development.

Keywords: cryptography, DNA cryptography, DNA computing.

The vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules are being explored for computing, data storage and cryptography. In such research area, novel computers, data storage and cryptography might be invented and this might lead to a new revolution in information science. On such background, DNA cryptography is developed with the research of DNA computing (also called biological computing or molecular computing). The traditional cryptography made great progress in the 20th century with the development of electronic technology and is widely used currently. Quantum cryptography was invented in 1970s and has made some progress in recent decades, but there is still some distance from being used in practice. DNA cryptography drawn attention after DNA computing was first proposed by Adleman in 1994, and now it has become the frontier of cryptography. DNA cryptography, traditional cryptography and quantum cryptography are developed under the same aim-information security, but with quite different ways, and all the three kinds of cryptography might constitute the major fields of future cryptography. In this paper, the biological background, research progress and prospects of DNA cryptography are reviewed and discussed to highlight its future studies.

1 Biological background

1.1 DNA

DNA is the abbreviation for deoxyribonucleic acid which is the germ plasm of all life styles. DNA is a kind of biological macromolecule and is made of nucleotides. Each nucleotide contains a single base and there are four kinds of bases, which are adenine (A) and thymine (T) or cytosine (C) and guanine (G), corresponding to four kinds of nucleotides. A single-stranded DNA is constructed with orientation: one end is called 5′, and the other end is called 3′. Usually DNA exists as double-stranded molecules in nature. The two complementary DNA strands are held together to form a double-helix structure by hydrogen bonds between the complementary bases of A and T (or C and G). The double-helix structure was discovered by Watson and Crick; thus the complementary structure is called Watson-Crick complementarity[1]. Their discovery is one of the greatest scientific discoveries of the 20th century and reduced genetics to chemistry and laid the foundations for the next half century of biology[2].

1.2 PCR and DNA chip

Within decades, great progress has been made in gene biotechnology. With invention and maturation of these technologies, such as DNA synthesis, PCR, elec-

trophoresis, DNA sequencing hybridization and other techniques, scientists can synthesize, amplify, isolate, digest and sequence DNA strands very easily. It opens the door to new application of DNA different forms in the evolution of life. PCR technology is used in all existing DNA computing methods and DNA cryptography methods, while the efficiency of DNA hybridization is improved greatly with DNA chip technology. These two important technologies will be briefly introduced in this paper.

Polymerase Chain Reaction（PCR）was invented in 1983. It is one of the most important invention in modern biology[3]. Since the DNA molecule is tiny in volume, it is difficult to manipulate a small quantity of given DNA directly, while it will be quite easy to manipulate a great mount of DNA after amplification. PCR is a fast DNA amplification technology based on Watson-Crick complementarity. Two complementary oligonucleotide primers are annealed to double-stranded target DNA strands, and the necessary target DNA can be amplified after a serial of polymerase reaction from 5′ to 3′ with the aid of polymerase enzyme. The PCR is a very sensitive method, and in theory a single target DNA molecule can be amplified to 10^6 after 20 cycles. Thus one can effectively amplify a lot of DNA strands within a very short time [3].

DNA chip is also known as DNA microarray or gene chip or oligonucleotide chip or biological chip, which is fabricated with *in situ* synthesized oligo nucleic acids or spotted cDNA probes according to published methods of Fodor and Brown[4−7]. Tens of thousands, even millions of DNA probes are arranged in a square area less than 1 square inch on glass or silicon matrix. And as their counterparts, numerous labelled probes are used to anneal with probes on the chip to get various hybridization spectrums revealing genetic information. Thus the hybridization efficiency can be raised thousands of times and even more.

2 DNA computing

The development of DNA cryptography benefits from the progress of DNA computing (also called molecular computing or biological computing). On the one hand, cryptography always has some relationship with the corresponding computing model more or less. On the other hand, some biological technologies used in DNA computation are also used in DNA cryptography. For these reasons, DNA computing is briefly introduced here.

In 1994, Adleman demonstrated the first DNA computing, which marked the beginning of a new stage in the era of information[8]. In the following researches, scientists find that the vast parallelism, exceptional energy efficiency and extraordinary information density are inherent in DNA molecules[8−12]. In 2002, a team led by Adleman solved a 3-SAT problem with more than 1 million possibilities on a simple DNA computer after an exhaustive searching[13]. In 2005，it is declared that a team led by Ehud Keinan invented a biomolecular computer that used little more than DNA and enzymes could perform a billion operations simultaneously[14]. Adleman reviewed DNA computing as follows: “For thousands of years, humans have tried to enhance their inherent computational abilities using manufactured devices. Mechanical devices such as the abacus, the adding machine, and the tabulating machine were important advances. But it was only with the advent of electronic devices and, in particular, the electronic computer some 60 years ago that a qualitative threshold seems to have been passed and problems of considerable difficulty could be solved. It appears that a molecular device has now been used to pass this qualitative threshold for a second time.”[13] Scientists have also made progress in the theory of DNA computing and explored several feasible computing models, such as the model used by Adleman in 1994[8]. Here it is called Hamiltonian path model, and the model based on DNA chip[14,15] and the sticker model proposed by Adleman[16]. Below, the widely used Hamiltonian path model and sticker model are briefly introduced.

2.1 *Hamiltonian Path Model*

In 1994, Adleman used DNA computing to solve an instance of the directed Hamiltonian path problem[8]. The computing model proposed by Adleman is also used by Lipton to solve SAT problems[17]. The Hamiltonian path problem is to find a path that begins at v_{in}, ends at v_{out} and enters every other vertex exactly once on a directed graph. For each vertex i in the graph, a random 20-mer oligonulecotide (short DNA strand) O_i was generated. Here, mer is the long measure of oligonulecotide. The following O_2, O_3 and O_4 denote vertices 2, 3, and 4, respectively. All the following oligonucleotides are written from 5′ to 3′.

$$O_2 = TATCGGATCGGTATATCCGA,$$

$$O_3 = GCTATTCGAGCTTAAAGCTA,$$

$$O_4 = GGCTAGGTACCAGCATGCTT.$$

For each edge $i \to j$ in the graph, an oligonulecotide strand is derived from the 3′ 10-mer of O_i and from the 5′ 10-mer of O_j. For each vertex i in the graph, $\overline{O}_i$ is the Watson-Crick complement of O_i. All the following oligouncleotides in Fig. 1 are written as 5′ to 3′ except $\overline{O}_3$.

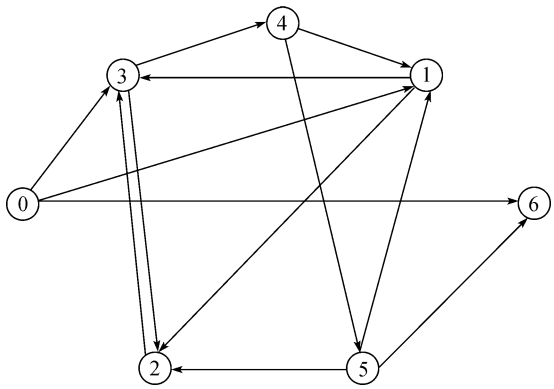

Fig. 1. Directed graph.

$$O_{2\to3} = GTATATCCGAGCTATTCGAG,$$
$$O_{3\to4} = CTTAAAGCTAGGCTAGGTAC,$$
$$\overline{O}_3 = CGATAAGCTCGAATTTCGAT.$$

In the experiment, for each vertex i (except the v_{in} and the v_{out}) in the graph and for each edge $i \to j$ in the graph, sufficient $\overline{O}_i$ and $O_{i\to j}$ were mixed together in a single ligation reaction. After a "graduated PCR" reaction, a lot of oligouncleotieds which denote different paths were generated. Note that the $\overline{O}_i$ oligonucleotides served as splints to bring oligonucleotides associated with compatible edges together for ligation (Fig. 2).

After all steps of the reaction were finished, a PCR

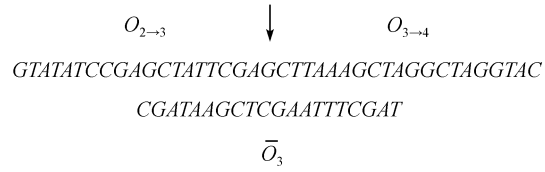

Fig. 2. Ligation reaction.

was performed to amplify paths which started from v_{in} and ended at v_{out}. Then oligonucleotides with correct length were separated out by gel- electrophoresis. Paths which did not entry some vertex were separated by a biotin-avidin magnetic beads system. If there are DNA strands left, it will show that the Hamiltonian path exists.

2.2 *Sticker model*

Both the sticker model and Hamiltonian path model are based on Watson-Crick complementary. The difference is that in Hamiltonian path model, there are short strands at beginning and long strands are formed by way of anneal as the answer, while in sticker model, there are long single-stranded DNA at the beginning and short stickers are annealed to long strands. The sticker model is used both in refs. [13, 18]. The sticker model mainly includes memory structure and four operations of combination, separation, setting particular bits and clearing bits. The memory structure of sticker model is shown in Fig. 3. More details of the sticker model are shown in ref. [16].

Despite the successes of the DNA computing in theory and practice, it is still far away from discovering all secrets in a cell, and thus, it is very likely that new computing models will be found in the future study. Just as Gifford said, "Transcriptional control and other gene regulation mechanisms certainly play a paramount role in the programming of cell behavior, but there may be other computational mechanisms lurking behind seemingly simple biological processes" [19].

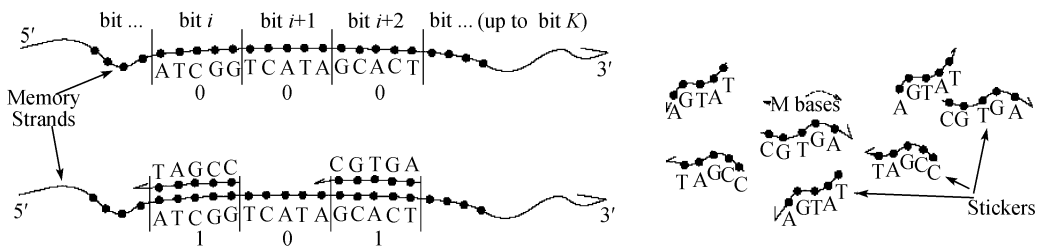

Fig. 3. Sticker model.

3 Progress and main problems in DNA cryptography

3.1 Progress

DNA cryptography is a new born cryptography, in which DNA is used as information carrier and the modern biological technology is used as implementation tool, and the vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules are explored for cryptographic purposes such as encryption, authentication, signature, and so on. Though DNA cryptography benefits from the research of DNA computing; it is not a direct result after all. The DNA computing proposed by Adleman cannot be regarded as DNA cryptography directly. In DNA computing, DNA technology is used to solve difficult computational problems, while in DNA cryptography, different difficult biological problems are studied and used as the secure foundation of DNA cryptosystems. The encryption process and the decryption process can be regarded as computation. But not all DNA computations are involved in cryptography. Note that DNA cryptography is not the same as genetic code. Genetic code deals with the heredity of life and belongs to the field of gene biotechnology. The research of DNA cryptography is at the beginning currently. There are few effective schemes[20−22]. However in this paper, two early representative DNA cryptographic schemes are introduced. The first one shows the extraordinary information density of DNA, but this scheme is very difficult to achieve. The second one is much easier to be achieved, in which PCR is used for decryption. The method of read data by PCR not only has relationship with DNA computing but also is widely applied in following studies. Though the second method is also called DNA steganography method, it is more appropriate to look on it as a DNA cryptography method according to its security foundation.

Gehani *et al*. achieved a one-time pad based on DNA[20]. They argued that current practical applications of cryptographic systems based on one-time pads are limited to the confines of conventional electronic media whereas DNA is of extraordinary information density. A gram of DNA contains about 10^{21} DNA bases, or about 10^8 tera-bytes. Hence, a few grams of DNA may have the potential of storing all the data stored in the world. Thus, DNA is very suitable to store a huge one-time pad. The scheme proposed by Gehani *et al*. is based on extraordinary information density of DNA and has great potential utility value. Their method might be effective for solving the storage problem of one-time pad. The disadvantage is that it is difficult to prepare a huge DNA one-time pad in which data can be easily separated and read out. For the sender and receiver, they have to do complex biological experiments, which can only be done in a well equipped lab and too expensive to achieve. In many years, the scheme is not feasible for the above reasons.

For DNA steganography, Clelland *et al*. successfully hid the famous "June 6 invasion: Normandy" in DNA microdots[21]. Their method is as follows:

1) Encoding rule. A novel encoding method is proposed instead of the traditional binary encoding. Nucleotides are used as quaternary code and each letter is denoted by three nucleotides. For example, the letter A is denoted by CGA, the letter B is denoted by CCA, etc.

2) Synthesizing secret-message DNA. The secret message is encoded into DNA sequence according to the above code. For instance, AB is encoded as CCGCCA. After coding, they synthesized a secret-message DNA oligodeoxynucleotide containing an encoded message 69 nucleotides long flanked by forward and reverse PCR primers, each 20 nucleotides long. Thus, the secrete-message DNA is prepared.

3) Hiding message. They prepared concealing DNA that is physically similar to the secret-message DNA by sonicating human DNA to roughly 50 to 150 nucleotide pairs (average size) and denaturing it. The secret-message DNA and concealing DNA were mixed and attached on a piece of paper using common adhesives to form colorless microdots. Then the paper containing microdots can be posted by general mail service.

4) Read. The sharing secrets for the sender and the receiver are encoding rule and primers. After the receiver gets the paper, he can easily find the microdots. Since the intended receiver had gotten the primers and encoding rule through a secure way, he could amplify the secret-message DNA by perform PCR on DNA microdots, sequence it and retrieve the message (plaintext) according to the encoding rule.

The basic process of the steganography method proposed in ref. [21] is shown in Fig. 4. The secret-message synthesizing process is shown in Fig. 4(a), the encoding rule is shown in Fig. 4(b), the PCR result is shown in Fig. 4(c), the secret-message DNA and corresponding message (plaintext) is shown in Fig. 4(d).

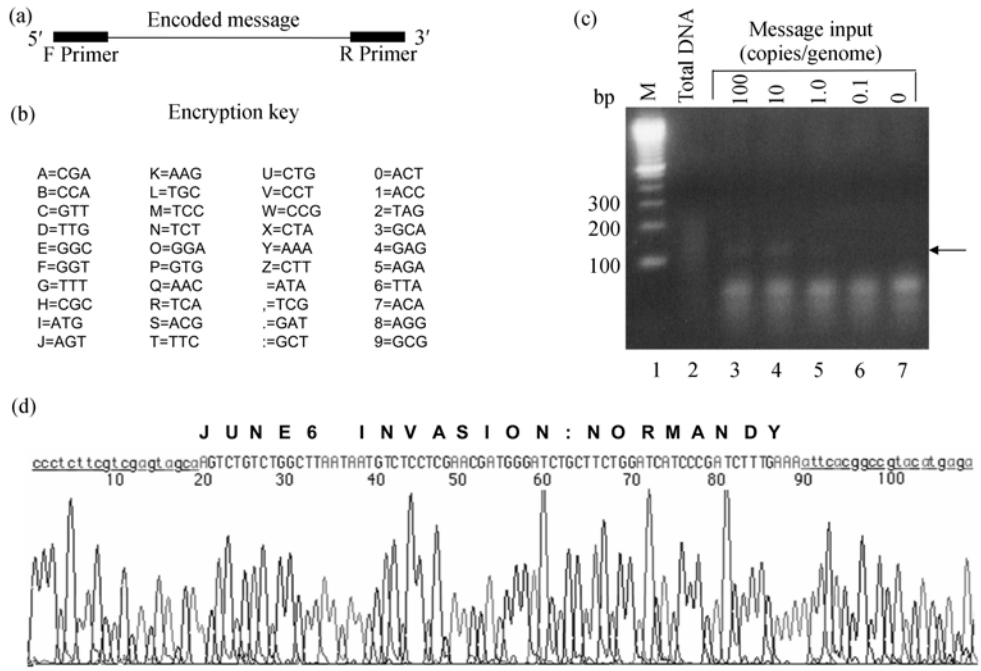

Fig. 4. Steganography method.

In fact, it is not correct that only the encoding rule is considered key in Fig. 4. The true key should be primers and encoding rule.

3.2 Main problems

The progress in the world shows that the research of present DNA cryptography is mainly confronted with the following problems:

(i) Lack of the related theoretical basis. In 1949, Shannon proposed the basic model and development direction for modern privacy communication in his famous paper "*Communication theory of secrecy systems*"[23]. In the 1970s, it is proposed that the complexity theory should be used as a powerful tool for designing encryption algorithms, which also makes the emergence of public-key cryptosystem possible[24]. In the following decades, new cryptosystems such as RSA, EIGamal, DES and AES are invented[25−28]. Thus, the traditional cryptography is perfected more and more. In contrast, for DNA cryptography there is no mature corresponding theory. It is still an open problem as to what are the model and security basis of DNA cryptography, say nothing of the implementations. For lack of related theory it is difficult to design good DNA cryptographic schemes.

(ii) Difficult to realize and expensive to apply. For the existing DNA cryptography schemes, many biological experiments have to be done in encryption step and decryption step, such as synthesizing message DNA strands, conducting PCR amplification and sequencing. Such experiments can only be done in a well equipped lab using current technology. For these reasons, DNA cryptosystems are not convenient in practice and cannot compete with traditional cryptosystems. Luckily, modern biology has made much headway in recent twenty years. Many expensive experiments in the past have become routine experiments. With the further development of biology and new design of DNA cryptosystem, the problems of "difficult and expensive to realize" can be solved.

4 Comparisons among DNA cryptography, traditional cryptography and quantum cryptography

4.1 Development

Traditional cryptography can be traced back to Caesar cipher 2000 years ago or even earlier. Related theory is almost sound. All the practical ciphers can be seen as traditional ones. Quantum cryptography came into being in the 1970s, and the theory basis has been prepared while implementation is difficult. By and large, they have not been plunged into practical use. DNA cryptography has only nearly ten years history, the theory basis is under research and the application

costs very much.

4.2 Security

Only computational security can be achieved for traditional cryptographic schemes except for the one-time pad, that is to say, an adversary with infinite power of computation can break them theoretically. It is shown that quantum computers have great and striking computational potential[29−31]. Although there is uncertainty about the computational power of quantum computers, it is possible that all the traditional schemes except for the one-time pad can be broken by using the future quantum computers. Quantum cryptographic schemes are unbreakable under current theories. Differently, their security is based on Heinsberg's Uncertainty Principle. Even if an eavesdropper is given the ability to do whatever he wants, and has infinite computing resources, so much as P=NP, it is still impossible to break such a scheme. Any behavior of eavesdropping will change the cipher so it can be detected. It is impossible for an adversary to obtain a totally same the quanta with the intercepted one, thus the attempt to tamper but without being detected in vain[32−36]. Therefore, quantum key agreement schemes have unconditional security. For the DNA cryptography, the main security basis is the restriction of biological techniques, which has nothing to do with the computing power and immunizes DNA cryptographic schemes against attacks using quantum computers. Nonetheless, the problem as to what is the extent this kind of security and how long it can be maintained it is still under exploration.

4.3 Application

Traditional cryptosystems are the most convenient of which the computation can be executed by electronic, quantum as well as DNA computers, the data can be transmitted by wire, fiber, wireless channel and even by a messenger, and the storage can be CDs, magnetic medium, DNA and other storage medium. Using the traditional cryptography we can realize purposes as public and private key encryption, identity authentication and digital signature. Quantum cryptosystem is implemented on quantum channels of which main advantage lies in real-time communication. The disadvantage lies in the secure data storage, which makes it infeasible to implement public-key encryption and digital signature as easily as traditional one does. Under the current level of techniques, only by physical ways can the ciphertext of DNA cryptography be transmitted. Due to the vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules, DNA cryptography can have special advantages in some cryptographic purposes, such as secure data storage, authentication, digital signature, steganography, and so on. DNA can even be used to produce unforgeable contract, cash ticket and identification card.

Researches of all the three kinds of cryptography are still in progress, and a great many problems remains to be solved especially for DNA and quantum cryptography, this making it hard to predict the future. But from the above discussions we think it is likely that they exist and develop conjunctively and complement each other rather than one of them falls into disuse thoroughly.

5 Development directions of DNA cryptography

Since DNA cryptography is still in its immature stage, it is too early to predict the future development precisely. However, in view of the development of biological techniques and the requirement of cryptography, we hold the following opinions:

1) DNA cryptography should be implemented by using modern biological techniques as tools and biological hard problems as main security basis to fully exert the special advantages.

Encryption and decryption are procedures of data transform which, if described by mathematical methods, are easier to be implemented than physical and chemical ones in the present era of electronic computers and the Internet. If other kinds of cryptosystems are necessary to be researched and developed, they should have properties such as higher security levels and storage density etc, which cannot be realized by electronic computers by using mathematical methods. Thus, if DNA cryptography is necessary to be developed, the advantages inherent in DNA should be fully explored, such as developing nanoscopic storage based on the tiny volume of DNA, realizing fast encryption and decryption based on the vast parallelism, and utilizing difficult biological problems that one can utilize but still far from fully understand them as the secure foundation of DNA cryptography to realize novel cryptosystem which can resist the attack from quantum computers. Since it has not been made sure whether quantum computers threaten the hardness of various mathematical hard problems, these problems being security basis cannot be excluded absolutely. Encryption

and decryption algorithms hard to be implemented using electronic computers may be feasible using DNA ones with regard to their vast parallel computational ability. If these schemes withstand attacks by quantum computers, their computational security will be inherited into DNA schemes. Thereby, DNA cryptography does not absolutely repulse traditional cryptography and it is possible to construct a hybrid cryptosystem of them.

2) Security requirements

Regardless of the many differences between DNA and traditional cryptography, they both satisfy the same characteristic of cryptography. The communication model for DNA encryption is also made up of two parties, i.e. a sender and a receiver, which obtain the secret key in a secure or authenticated way and then communicate securely with each other in an insecure or unauthenticated channel. The security requirements should also be founded upon the assumption proposed by Kerchoff that security should depend only on the secrecy of decryption key; that is, an attacker should be fully aware of all the details of encryption and decryption except the decryption key. It is under this assumption that a cryptosystem can be said secure when any attacker cannot break it[24]. More precisely, it must be assumed that an attacker knows the basic biological method the designer used, and has enough knowledge and excellent laboratory devices to repeat the designer's operations. The only thing not known by the attacker is the key. In a DNA cryptosystem, a key is usually some substances of biological materials or a preparation flow, and sometimes the experiment conditions.

3) For DNA cryptography, the current research target should lie first in security and feasibility, second in storage density.

A sound cryptosystem should be secure as well as easy to be implemented. The development of modern biological technology makes it possible to express data by DNA, although the related research is just in its initial stage. In fact, it is still difficult to operate the nanoscopic DNA directly. Scientists can easily operate DNA with the aid of kinds of restriction enzymes only after DNA strands are amplified with amplification technology such as PCR. With the current technology, it is also impossible to store all the worldwide data by using several grams of DNA. If the only requirement is to improve the density of storage, it is hard to implement DNA cryptography at the present technique level. It is more practical to make use of colony property of plentiful DNA for cryptographer. For example, store data by DNA chips and read data by hybridization, which makes the operations of input/output faster and more convenient. The method is easier to be implemented than encoding message into nucleotides directly while the storage density is somewhat lower.

4) Currently, the main task for DNA cryptographers is to establish the theory foundations and to accumulate the practical experience.

It can be proved that there are vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA. This motivates the research of DNA computing and cryptography. The current goal or difficulty is to find and make use of the utmost potential, but the related research is in its initial stage. Sound theories have not been founded for both DNA computing and cryptography. Modern biology lays particular stress on experiments rather than theories. There is no efficient way to measure the hardness of a biological problem and the security level of the corresponding cryptosystems based on the problem. It is certainly urgent to find such a method similar to computational complexity. Presently, the most important is to find the sound properties of DNA that can be used to computation and encryption, to establish the theoretical basis and to accumulate the experience, based on which the design of secure and practical DNA cryptosystems is possible.

6 Conclusions

The research of DNA cryptography is still at the beginning, and there are many problems to be solved. But the vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules endow DNA cryptography special advantages over other kinds of cryptography. Just as Adleman said, "DNA computers, such as the one presented here, illustrate that biological molecules (nucleicacids, proteins, etc.) can be used for distinctly non-biological purposes. For such purposes, these molecules represent an untapped legacy of 3 billion years of evolution and there is great potential in their further exploration"[13].

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant No. 60473028). We thank the review experts for their very valued revise advice.

References

1 Watson J D, Hopkins N H, Roberts J W, et al. Molecular Biology of the Gene. 4th ed. Menlo Park, CA: The Benjamin/Cummings Publishing Co., Inc., 1987

2 Seeman N C. Nanotechnology and the double helix. Scientific American, 2004, 290: 34－43

3 Li Debao, Xu Ping. Theory and Methods of Recombinant DNA. Hangzhou: Zhejiang Science and Technology Publishing Co., 1994

4 Fodor S P, Read J L, Pirrung M C, et al. Light-directed, spatially addressable parallel chemical synthesis. Science, 1991, 251: 767－773

5 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

6 Schena M, Shalon D, Ronald W, et al. Quantitative monitoring of gene expression patterns with a complementary DNA microarray. Science, 1995, 270: 467－470

7 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

8 Adleman L, Molecular computation of solutions to combinatorial problems. Science, 1994, 266: 1021－1023

9 Guarnieri F, Fliss M, Bancroft C. Making DNA add. Science, 1996, 273: 220－223

10 Bancroft C, Bowler T, Bloom B, et al. Long-Term storage of information in DNA. Science, 2001, 293: 1763－1765[DOI]

11 Ouyang Q, Kaplan P D, Liu S, et al. DNA solution of the maximal clique problem. Science, 1997, 278: 446－449[DOI]

12 Sakamoto K, Gouzu H., Komiya K, et al. Molecular computation by DNA hairpin formation. Science, 2000, 288: 1223－1226[DOI]

13 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

14 Fastest DNA Computer. Science, 2005, 308: 195

15 Liu Q, Wang L, Frutos A G, et al. DNA computing on surfaces. Nature, 2000, 403: 175－179[DOI]

16 Roweis S, Winfree1 E, Burgoyne R, et al. A sticker based model for DNA computation. Journal of Computational Biology, 1998, 5(4): 615－629

17 Lipton R J. Using DNA to solve NP-complete problems. Science, 1995, 268: 542－545

18 Adleman L M, Rothemund P W K, Roweiss S, et al. On applying molecular computation to the Data Encryption Standard. Journal of Computational Biology, 1999, 6(1): 53－63

19 Gifford D K. On the path to computation with DNA. Science, 1994, 266: 993－994

20 Gehani A, LaBean T H, Reif J H. DNA-based cryptography. Dimacs Series In Discrete Mathematics & Theoretical Computer Science, 2000, 54: 233－249

21 Celland C T, Risca V, Bancroft C. Hiding messages in DNA microdots. Nature, 1999, 399: 533－534[DOI]

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

23 Shannon C E. Communication theory of secret systems. Bell System Technical Journal, 1949, 28(4): 656－349

24 Diffie W, Hellman M. New directions in cryptography. IEEE Transaction on Information Theory, 1976, 22(6): 644－654

25 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

26 EIGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transaction on Information Theory, 1985, 31(4): 469－472[DOI]

27 National Institute of Standards and Technology, NIST FIPS PUB 46-2, "Data Encryption Standards," U.S. Department of Commerce, 1993

28 Daemen J, Rijmen V. The Design of Rijndael: AES the Advanced Encryption Stand. Berlin: Springer-Verlag, 2002

29 Shor P W, Algorithms for quantum computation: Discrete log and factoring. Proceedings of the 35th Symposium on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society Press, 1994. 124－134

30 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

31 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

32 Wiesner S. Conjugate coding. SIGACT News, 1983, 15: 78－88[DOI]

33 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

34 Bennett C H. Quantum cryptography using any two nonothogonal states. Phys Rev Lett, 1992, 68(21): 3121－3124

35 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67(6): 661－663 [DOI]

36 Bennett C H, Brassard G, Ekert A K. Quantum cryptography. Scientific American, 1992, 267: 50－57