SCIENCE CHINA
Information Sciences

• RESEARCH PAPERS •

March 2010 Vol. 53 No. 3: 506–514
doi: 10.1007/s11432-010-0063-3

Asymmetric encryption and signature method with DNA technology

LAI XueJia[1†], LU MingXin[2†*], QIN Lei[3], HAN JunSong[4] & FANG XiWen[1]

[1]*Department of Computer Science & Engineering, Shanghai Jiao Tong University, Shanghai* 200030*, China;*
[2]*School of National Information Security, Nanjing University, Nanjing* 210093*, China;*
[3]*BIOCOMPLEX,* 4915 *Bathurst St. Unit#* 209-366*, ON M2R* 1*X*9*, Canada;*
[4]*National Engineering Center for BioChip at Shanghai, Shanghai* 201203*, China*

Received July 14, 2009; accepted February 22, 2010

Abstract This paper proposes DNA-PKC, an asymmetric encryption and signature cryptosystem by combining the technologies of genetic engineering and cryptology. It is an exploratory research of biological cryptology. Similar to conventional public-key cryptology, DNA-PKC uses two pairs of keys for encryption and signature, respectively. Using the public encryption key, everyone can send encrypted message to a specified user, only the owner of the private decryption key can decrypt the ciphertext and recover the message; in the signature scheme, the owner of the private signing key can generate a signature that can be verified by other users with the public verification key, but no else can forge the signature. DNA-PKC differs from the conventional cryptology in that the keys and the ciphertexts are all biological molecules. The security of DNA-PKC relies on difficult biological problems instead of computational problems; thus DNA-PKC is immune from known attacks, especially the quantum computing based attacks.

Keywords cryptology, asymmetric encryption, digital signature, biological cryptology, DNA

Citation Lai X J, Lu M X, Qin L, et al. Asymmetric encryption and signature method with DNA technology. Sci China Inf Sci, 2010, 53: 506–514, doi: 10.1007/s11432-010-0063-3

1 Introduction

Cryptography is a branch of science which studies the encoding of information for the purpose of hiding messages. The development of cryptography is strongly related to human's information-processing capabilities and computing capacities. When the electronic computer technology is approaching the physical limit, people turn themselves to the study of new computation technologies which might profoundly influence the development of cryptology in the future. Biological computing (e.g. DNA computing) and quantum computing are two most promising technologies under development. However, new crypto technology does not always follow the development in novel computation technology. Since Wisner [1] first proposed the premature idea of quantum cryptology in the 1970s, the quantum cryptology has been studied for nearly 40 years. Today, quantum cryptology is still far from changing the domination of the conventional cryptology, while significant progresses have been achieved in the field of quantum communication [2–5]. Although quantum computing is also a potential threat to current cryptology, there is still

*Corresponding author (email: mxlu@nju.edu.cn)
† These authors contributed equally to this work

a long way to go before we can implement its potential power [6, 7]. On the other hand, since Adleman [8] demonstrated the first DNA computing model, 15 DNA computing conferences have been held annually, different algorithms have been proposed and the computational power in laboratory environment was expanded extensively [9–15]. DNA computing experiments were also used to attack NP-C problems and conventional cryptosystem [16–20]. But comparing to DNA computing, the research of biological cryptology attracted less attention [21–25]. As a preliminary study of the biological cryptology, this paper proposes the DNA-PKC—an asymmetric encryption and signature cryptosystem based on the nature of DNA molecules.

2 Elements of DNA-PKC

DNA is the abbreviation of deoxyribonucleic acid which is the germplasm of all life forms. A typical DNA molecule has two anti-parallel strands consisting four types of nucleotides (or bases), which are adenine (A), thymine (T), cytosine (C) and guanine (G). Complementary DNA strands are held together by forming hydrogen bonds between bases (base pairing) from each strand specifically with A bonding only to T and G only bonding to C. In that the double helix structure DNA was discovered by Watson and Crick, the complementary structure is called Watson-Crick complementarity [26]. Their discovery of DNA helix structure is one of the greatest scientific discoveries in the 20th century, which reduced genetics to chemistry and laid the foundations for current biology research [27].

Complementary base pairing is also the basis of DNA chip technology, called gene chip, microarray, oligo-chips or biochips. DNA chip is fabricated with *in situ* synthesized oligo nucleic acids or spotted cDNA probes. Tens of thousand DNA probes are arranged on glass or silicon matrix and numerous labeled complementary probes are annealed on the chip to get various hybridization spectrums, revealing the genetic information. As a result, the use of DNA chip can increase the hybridization efficiency thousands of times [28–31], improving people's ability in understanding genetic information dramatically.

Although many kinds of biological molecules can be used in biological computing and biological cryptology, DNA is so far the most popular one. Thus, biological computing and biological cryptology are also called DNA computing and DNA cryptology. Like conventional cryptography, a biological cryptosystem also consists of the sender Alice, the receiver Bob, and the challenger Eve. Biological cryptosystem differentiates it from conventional cryptosystem as follows:

1) Instead of a copy of data, keys in biological cryptosystem are biological molecules and some other secret information, such as hybridization condition, rules of reading the information, etc.

2) The ciphertext is in the form of biological molecules, in a mixture or on a chip.

3) One obtains the ciphertext and the key physically, or in other possible way in the future, not over electronic communication.

Just like conventional public-key cryptosystem, encryption key and decryption key in a biological cryptosystem are different. There are several shares of the public encryption key ek and only one share of the private decryption key dk. It is easy to encrypt the plaintext into the ciphertext with ek, but it is difficult to decrypt the ciphertext without dk. On the other hand, with dk one can easily decrypt the ciphertext to the plaintext. In DNA-PKC, one set of DNA probes is designated as the encryption key ek, and another set is used as the decryption key dk. Hybridization condition can also be regarded as a part of the decryption key. Any sender can use a share of ek to generate a ciphertext. The hybridization result of ek and dk will be treated with certain standard to translate the hybridization signals back to the encrypted message. Similarly, in the DNA-PKC signature scheme, the owner of the private signing key uses the key to generate a signature, others can verify the signature using the share of the public verification key without the ability to forge the signature. Unlike conventional schemes, keys in DNA-PKC are DNA probes instead of a copy of data; and one gets his key physically, not electronically.

3 Key generation

Stable molecules such as DNA, PNA [32] and protein can be used as the key in our cryptosystem. In this work, we choose DNA as the material to establish our system.

Step 1. Prepare encryption/decryption keys. One probe set is the encryption keys, and the other one is probes mixture as decryption keys. The encryption key set consists of purified probes, i.e. synthesized DNA or probes selected from homologous DNA. These probes are kept in tubes or micro-tubes separately. The decryption probes are in forms of solution, which have certain relationship with the encryption probes. The solution can be extracted from former experiment materials or be formulated freshly, which contain probes complementary and hybridize to the encryption key.

Step 2. Encryption keys and decryption keys are chosen for the cryptosystem respectively. We use the probes in encryption probes set to fabricate DNA chips (each type of probes forms a spot and for the purpose of quality control, several replications can be generated for each spot). We hybridize the encrypted chip with decryption probes candidate under certain hybridization condition. The condition of the hybridization can be defined due to previous experiment data. If the result of the hybridization is ideal; that is, there are a certain quantity of (over 20%–30%) probes on the chips showing signal with high intensity, probes used in the cryptosystem can be selected. Or else, hybridization condition or decryption probes candidate will be changed and more hybridization experiments will be executed till certain result can be met. With determined standards, probes (encryption and decryption) with signal intensity higher than a certain value are collected into a set representing binary digit "1" and the probes with signal intensity lower than a certain value are collected as binary digit "0" correspondently. Other probes are discarded. The set of probes 0 and probes 1 will be used as the encryption key. An alternative method is only selecting probes 1 according to a certain standard and selecting probes randomly as probes 0. Using this method, errors might happen sometimes. However, the errors will affect the decryption with very low probability.

The process of key generation is a process of biological experiment. The study of DNA cryptology is still in the exploratory stage currently; other key generation schemes might be investigated in further studies.

4 Encryption and decryption

1) Key distribution. If Bob wants to participate in DNA-PKC cryptosystem, he randomly chooses his key pair (ek, dk), and keeps dk secret as the decryption key. The public encryption key ek can be divided and stored into multi share and distributed to intended receivers.

2) Encryption process. If anyone such as Alice wants to send messages to Bob, she acquires a share of Bob's encryption key, and uses the key and plaintext to fabricate DNA chips as the corresponding ciphertext. DNA probes representing 0 and 1 are arranged as the binary representation of the plaintext on these chips. Then she can send these chips to Bob through an insecure way.

3) Decryption process. Bob uses his decryption key dk to hybridize with Alice's DNA chips and analyzes the hybridization signals to retrieve the plaintext.

If another one such as Tom also wants to send message to Bob, he can just do what Alice has done. Only Bob can decrypt all these ciphertexts. The details of encryption and decryption are similar to what is described in [25].

5 Signing and verification

1) Key distribution. If Bob wants to participate in DNA-PKC cryptosystem, he randomly chooses his key pair $(vk$, $sk)$, and keeps the sk secret as the signing key. The public verification key vk is copied as several shares and distributed to the verifiers.

2) Signature process. Bob can use the signing key sk to fabricate DNA chips for a given message. DNA probes representing 0 and 1 are arranged as the binary representation of the message in chips. The chips can be sent to intended receiver through an insecure way.

3) Signature verification. After an intended receiver such as Alice has received the DNA chips from Bob, she can use a share of Bob's verification key to hybridize with the DNA chips to verify Bob's

signature. If another one such as Tom also wants to verify Bob's signature, he can just do what Alice has done. Their shares of the verification key can be different. Although they all can verify Bob's signature, neither of them can forge the signature.

6 Security

6.1 Two levels of security

The security of DNA-PKC = biological security + computational security. To make a vivid metaphor, this is just similar to a coffer with two layers. The first security level is the biological security. The carriers of DNA-PKC are biological molecules: while getting the ciphertext, biological information cannot be transformed to digital data without breaking the biological security. The condition here is similar to that of quantum communication in which an adversary intercepts quantum. As a result, any mathematical attack is unavailable. The second security level is computational difficulties. Because of the inherent massive parallelisms of DNA, the attack of DNA-PKC leads to much greater computational complexity than that of AES-128. The adversary can break DNA-PKC only by firstly breaking the biological security, then the computational security. DNA-PKC has one more security level than conventional cryptosystem. Even if the vision of the quantum computer becomes true, the biological security of DNA-PKC will become valuable for its capability of resisting quantum computing attack.

6.2 One aspect of the security: decryption is unavailable without decryption key

In order to attack DNA-PKC, the adversary should break the first level of security, i.e., the biological security. The biological security is based on the difficulty of sequencing. This difficult problem is discussed in [25] and it will remain difficult for many years. Besides, not only ordinary DNA probes can be used as keys, special DNA, PNA probes or protein probes can also be used in DNA-PKC. It is extremely difficult to obtain all molecular information of special DNA or PNA probes spotted on a DNA chip (microarray) precisely currently. It is even untested how to sequence probes on protein chips. The development of genetic engineering technology will also lead to more advanced secure technology of DNA-PKC. Thus, the biological security of DNA-PKC still has substantial potential for developing.

There is a second security level, i.e., computational difficulty. Suppose the adversary is able to break the first security level in the future, it does not mean that DNA-PKC itself is broken: DNA-PKC still possesses high security level while considering the computation difficulties. Here is a simple example. Suppose the encryption key is composed of 128 probes for example with 64 probes representing "1" and 64 probes denoting "0". In an exhaustive attack, the amount of the possible key combinations will be

$$\mathrm{C}_{128}^{64} = \frac{128!}{64! \times 64!} = 2.4 \times 10^{37}.$$

If the exhaustive attack is performed on AES-128, the amount of possible keys is

$$2^{128} = 3.4 \times 10^{38}.$$

We can see that the cost of the exhaustive key search of DNA-PKC is very close to that of AES-128. Generally it is very easy to enlarge the amount of probes in favor of massive parallelisms of DNA hybridization. As a result, even if the unique biological security was broken, DNA-PKC would still surpass AES in the aspect of resisting brute force exhaustive attack.

6.3 Another aspect of security: private-key cannot be retrieved from public-key

One cannot retrieve private-key from known public keys in an asymmetric cryptosystem. As for DNA-PKC, one can retrieve neither the decryption key nor other share of the encryption key from a share of the public-key; thus one cannot decrypt ciphertexts encrypted by others. It can be proved through two evident biological properties. In practical, only satisfying one of them can make sense. Characteristic 1 can meet the requirement of unconditional security.

Property 1: DNA is characterized by its tiny size. A large quantity of probes is contained in the hybridization solution; we regard the hybridization solution as a set of many decryption key probes. Thus several encryption keys can be mapped to the same decryption solution, i.e., different encryption key sets can share the same set of decryption keys.

This property is different from conventional cryptosystem and it does make sense in DNA cryptosystem. In the encryption key distribution stage, there is little difference between distributing two different encryption keys and distributing two identical encryption keys. The reason for this is that the encryption key in DNA cryptosystem is biological material instead of digital data. While in the decryption stage, for the ciphertexts encrypted by different encryption keys, we use only one decryption key to decrypt them, which is similar to conventional public-key cryptosystem. The decryption key and the encryption key will be paired according to different probes during decryption, which takes place in microstructure, and the users do not need to care about it, just like the users of RSA who do not need to know how the CPU registers work.

The encryption key and the decryption key are both accurate in conventional public-key cryptosystem. While in DNA-PKC system, though the encryption key probes are accurately known, it is not clear for the decryption key probes. We only know the source and the approximate constitution (types, quantities) of the decryption key solution.

Property 2: For the same encryption key, there can be several different decryption keys which can react with it, and vice versa. Hybridizing two probes which are not complementary to each other completely may also result in good hybridizing signal under certain conditions. Actually there are many unknown characteristics in DNA hybridization dynamics. These unknown features can also contribute to an asymmetric cryptosystem. Unlike what we are talking about under property 1, hybridization dynamics may enable additional flexibility in selecting the complementary probes pairs, but restricted to currently limited knowledge on this topic.

7 Differences between DNA-PKC and conventional public-key cryptology

Differences between DNA-PKC and conventional public-key cryptology are discussed in the following aspects:

1) Clumsiness and delicacy. The research of genetic engineering is still in its early stages, only limited measures can be used for computing. From a mathematical cryptology standpoint, its data processing is much less delicate than that of the mathematical cryptology. Actually, the computing model of biological computers is very different from that of electronic computers. DNA cryptology is based on DNA's massive parallelisms. It is not easy to realize the computing process of DNA cryptology in electronic computers which work serially. What is more, it even seems clumsy to do this. However, while the computation is carried out in biological computers, it is delicate and easy to realize.

2) The key of DNA-PKC is DNA probes and the ciphertext is a DNA chip. The key and ciphertext are digital data in conventional public-key cryptology. It is easy to copy digital data. Therefore it is easy to copy RSA keys and ciphertexts without being discovered. In DNA-PKC, it is hard to reproduce unknown key probes and ciphertext chips.

3) The security of conventional public-key cryptosystem is based on computational security. However, the security of DNA-PKC is mainly based on the security of biology, and computational security can also be utilized if necessary.

4) The encryption key and decryption key in a conventional public-key cryptosystem are one-to-one while that of DNA-PKC can be many-to-many.

5) Many times of computation can be conducted to the ciphertexts of conventional public-key cryptosystem. Yet ciphertexts of DNA-PKC are chips which cannot endure many times of hybridization. After hybridization, if the attacker wants to hybridize them again, the chips have to be cleaned, which will damage the DNA probes on chips. Repeated hybridization also decreases the yield of signals, which enhances the difficulty of breaking the ciphertexts. On the other hand, the experiment is also relatively

complicated. If it is required to execute hybridization repeatedly under certain circumstances, different ciphertexts may be spotted on one chip.

6) In a conventional public-key cryptosystem, getting the encryption key means getting all of the information. If the attacker is able to factorize large integers, he will break the system. However, in DNA-PKC, as the DNA sequence contains lots of information and there are many unknown factors in biology, getting chips or keys does not surely mean getting all of the secrets.

7) Asymmetry of encryption and signature. Signature and encryption requires different security of system. In DNA-PKC, the encryption or signature process is to make chips, while the decryption or verification process is to execute hybridization, which itself is an interesting asymmetric phenomenon. In the application of encryption, the hybridization condition is kept as a secret by the owner of the decryption key. In the application of signature, the hybridization condition is informed to the verifier. Hybridization conditions (e.g. temperature, DNA probes concentration, etc.) can affect the result of the hybridization. If the hybridization condition is unknown, even if the adversary possesses the encryption probes and decryption probes, his hybridization result will be very different from that of the authenticate owner of the decryption key, and thus he is unable to retrieve the plaintext certainly. From this point of view, as to DNA-PKC, the encryption system has more advanced security than the signature system.

8) The basic differences above make DNA-PKC differ from the conventional public-key cryptosystem in its security requirement and the application aspects.

8 A simple example

In this study, a simple experiment of DNA-PKC was conducted with helps from the National Engineering Center for BioChip at Shanghai in 2009. The processes of selecting probes, fabricating chips, hybridization and reading accords are described in [25].

1) Key generation. We first select the encryption key from the existing probes of the National Engineering Center for BioChip at Shanghai. The source of the genes are kept as secret. From 12 standard values of the hybridization signals (Cy5_FM, Cy5_BM, Cy5_BSD, Cy5_Signal, Cy5_SN, Cy3_FM, Cy3_BM, Cy3_BSD, Cy3_Signal, Cy3_SN, Sat, flag), Cy3_Signal was used to select probes. Referring to the existing experiment data, the probes with hybridization results showing intensity >8000 are collected as probe 1, and those with intensity <2000 are collected as probe 0. Probes 1 we collected are conservative sequence with relatively high expression levels in the original species. We select two groups of different encryption keys PK_A and PK_B from the samples and distribute the key to two intended users A and B. Each encryption key set consists of 32 different probes 0 and 32 probes 1. We also select the corresponding hybridization solution as the decryption key SK.

2) Encryption. We use the encryption keys PK_A and PK_B to encrypt a sentence in the experiment. Here we choose the famous "June 6 invasion: Normandy" as a plaintext to encrypt. Firstly we convert this sentence into binary sequence according to the ASCII code.

```
0100101001110101   0110111001100101   0010000000110110
0010000001101001   0110111001110110   0110000101110011
0110100101101111   0110111000111010   0010000001001110
0110111101110010   0110110101100001   0110111001100100
0111100100000000
```

These data are arranged on a 13×16 matrix. The digital matrix is then written into a ciphertext chip: for 0 in the matrix, probes 0 are selected from the encryption key and spotted on the corresponding position of the chip; for 1 in the matrix, probes 1 are selected from the encryption key and spotted on the corresponding position of the chip. Finally the chip fabricated just forms the ciphertext. In this experiment, there are two encryption keys PK_A and PK_B. Therefore, while the same sentence is encrypted, two different chips of ciphertext matrixes are generated. We present the two ciphertext matrixes on the same chip and each matrix is replicated for 3 times.

3) Decryption. The intended receiver hybridizes the ciphertext encrypted by encryption keys PK_A and PK_B with the decryption key SK. The hybridization result is shown in Figure 1. The light spots here indicate higher intensity of hybridization signals representing digit 1, and the dark spots denote digit 0. Two encryption keys are used in this experiment. For each encryption key 3 replicated ciphertext matrixes are spotted and there are 6 matrixes in all. Thus there are 6 probe matrixes in Figure 1. Three upper matrixes of ciphertext probes are generated by PK_A and the other three are generated by PK_B. According to the hybridization patterns, we select Cy3_Signal as the standard during the decryption process. Because there is a large amount of data, as an example, we only present the data of the first 16 spots (the first line of the first matrix) on the top left of Figure 1: (4187, 65285, 915, 1056, 65268, 1403, 65264, 1831, 1395, 65228, 65209, 65222, 2507, 65183, 2151, 65174). The values under 5000 were denoted by 0 and the values higher than 10000 are identified as 1, and the spots value between 5000 and 10000 are discarded. Thus the hybridization signal can be transformed into binary sequence, and the plaintext can be retrieved according to ASCII code. As seen from Figure 1, hybridization patterns from key sets PK_A and PK_B are basically the same.

4) Attack. It is very hard for an adversary such as Eve to break the ciphertext without the corresponding decryption key solution. In an attack effort, Eve made a guess that human genes are used in the experiment, so she hybridized a sample of human genes with the ciphertext chips and tried to break the ciphertext according to the hybridization result shown in Figure 2. Again Cy3_Signals were used in data analysis.

We can see that most of the spots in the image of the chip are dark-colored and a small portion of them are light-colored. It is because that the encryption probes in our experiment are selected conservatively. If we select the encryption key more randomly, there will be fewer light-colored spots in our experiment. Listed are data of the 16 spots in the first line of the first probe matrix in Figure 2: (238, 168, 2175, 428, 9671, 301, 4009, 527, 200, 422, 318, 11096, 827, 3554, 283, 423). Besides, for two different encryption key sets PK_A and PK_B, different patterns resulted from this human genes attack, comparing to the nearly identical patterns observed in Figure 1. In our study, we also tested PCR attack, but no useful information was obtained for breaking the ciphertext (data not shown).

Mathematical analysis attack is not conducted, for we did not get any valuable data from the biological attack.

Errors in the hybridization signals represent the limit of biological hybridization process in yielded chemical signals. The reason of data errors may come from multi-aspect, such as immature human genetic engineering technologies, limited precision of experiment equipment, etc. To cop with these imperfection, the standard used in decryption should not be as strict as that of selecting encryption key. With further study of DNA cipher and specially designed facilities, experiment errors can be controlled to minimum level. On the other hand, the method of error correcting code can also be considered.

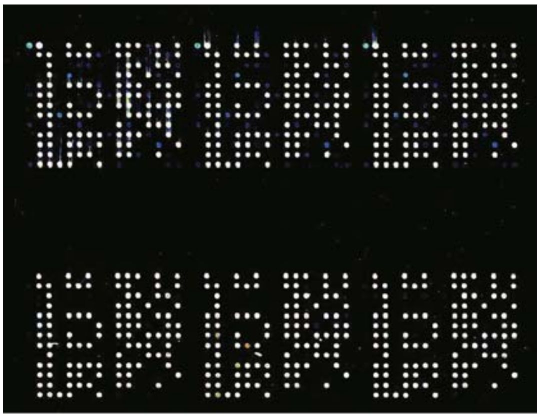

Figure 1 The result of decryption.

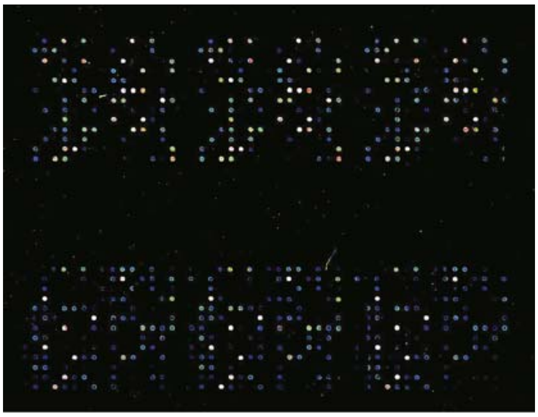

Figure 2 The result of attack.

9 Conclusions

In this study, we proposed a novel method of implementation of asymmetric encryption and signature with DNA technology. In current scheme, the procedure of encryption/signature is to fabricate chips and the procedure of decryption/verification is to execute hybridization. As a preliminary attempt to implement biological cryptosystem, many open questions are left to be answered with further studies.

In the conventional system of asymmetric cryptology, both keys and messages are transmitted electronically. However, in DNA-PKC, DNA probes are used as keys and chips are used as ciphertexts and they are transmitted physically. Because of its biological nature, DNA-PKC is fitter for secure data storage of huge capacity, identity recognition, payment system and bioinformatics, etc. Particularly, the ciphertext in DNA-PKC are hard to replicate, which makes it possible to prevent data from being cloned and monitored.

The security of the current public-key cryptosystem is based on some computationally difficult problems. These problems have long been assumed to be secure without strict proofs; therefore these cryptosystems might be threatened with super computational power in future. In contrast, the security of DNA-PKC is based on the research of genetic engineering, which provides some other possibility for security.

One might say that DNA-PKC is a cryptosystem based on biological materials or hardware; similar functions can also be implemented by electronic chips which may be even cheaper. Looking back at the history of computer, many difficulties have occurred during the decades of development since the birth of the first generation electronic computer; even personal computers had once been considered to be impossible. Nowadays, the electronic computer is very popular all over the world with decreased energy consumption and increased performance. In the aspect of practicality, DNA computing and DNA cryptography still cannot compete with the electronic computing technology and the mathematical cryptography. However, the DNA molecule has the potential to be used in the fields of information science. As put by Adleman, for thousands of years, humans have tried to enhance their inherent computational abilities using manufactured devices. 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 the 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 [19]. The study of DNA computing and the DNA cryptography are still at its early stages; thus it is too early to judge its future. However, with the development of the biotechnology, the exploration of the biological cryptography, such as DNA-PKC, will go much further, and it may have particular advantages over the conventional mathematical cryptology and the future quantum cryptology.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos. 60773092, 60903180).

References

1 Wiesner S. Conjugate coding. SIGACT News, 1983, 15: 78–88

2 Chou C W, Laurat J L, Deng H, et al. Functional quantum nodes for entanglement distribution over scalable quantum networks. Science, 2007, 316: 1316–1320

3 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. Bangalore, India: Bangalore Press, 1984. 175–179

4 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121–3124

5 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663

6 Hemmer P, Wrachtrup J. Where is my quantum computer? Science, 2009, 324: 473–474

7 Shor P W. Algorithms for quantum computation: discrete log and factoring. In: Goldwasser S, ed. Proceedings of the 35th Symposium on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society Press, 1994. 124–134

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

9 Ehud S, Binyamin G. RNA computing in a living cell. Science, 2008, 322: 387–388

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

11 Sakamoto K, Gouzu H, Komiya K, et al. Molecular computation by DNA hairpin formation. Science, 2000, 288: 1223–1226

12 Fastest DNA computer. Science, 2005, 308: 195

13 Liu Q, Wang L, Frutos A G, et al. DNA computing on surfaces. Nature, 2000, 403: 175–179

14 Roweis S, Winfree1 E, Burgoyne R, et al. A sticker based model for DNA computation. J Comput Biol, 1998, 5: 615–629

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

16 Ouyang Q, Kaplan P D, Liu S, et al. DNA solution of the maximal clique problem. Science, 1997, 278: 446–449

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

18 Ravinderjit S, Braich R, Chelyapov N, et al. Solution of a 20-variable 3-SAT problem on a DNA computer. Science, 2002, 296: 499–502

19 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: 53–63

20 Boneh D, Dunworth C, Lipton R J. Breaking DES using a molecular computer. In: DNA Based Computers I. Providence, USA: American Mathematical Society, 1996. 37–65

21 Gehani A, LaBean T H, Reif J H. DNA-based cryptography. In: DNA Based Computers V. Providence, USA: American Mathematical Society, 2000. 233–249

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

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

24 Xiao G Z, Lu M X, Qin L, et al. New field of cryptograhy: DNA cryptography. Chinese Sci Bull, 2006, 51: 1413–1420

25 Lu M X, Lai X J, Xiao G Z, et al. A symmetric-key cryptosystem with DNA technology. Sci China Ser F-Inf Sci, 2007, 50: 324–333

26 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

27 Seeman N C. Nanotechnology and the double helix. Sci Am, 2004, 290: 34–43

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

29 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

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

31 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: 639–645

32 Weiler J, Gausepohll H, Hauser N, et al. Hybridisation based DNA screening on peptide nucleic acid (PNA) oligomer arrays. Nucleic Acids Research, 1997, 25: 2792–2799