ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 9(43), DOI: 10.17485/ijst/2016/v9i43/104609, November 2016*

Historical View of Molecular DNA Cryptography for Image Security

N. Srividhya [1]* and R. Arunya[2]

[1]VLSI Design, Sathyabama University, Rajiv Gandhi Salai, Jeppiaar Nagar, Chennai - 600 119, Tamil Nadu, India; srividhyanatraj@gmail.com
[2]ECE Department, Sathyabama University, Rajiv Gandhi Salai, Jeppiaar Nagar, Chennai - 600 119, Tamil Nadu, India; arunya.mit@gmail.com

Abstract

Currently, government agencies and semiconductor industries have raised serious concerns about spiteful modifications to the integrated circuits. The function which has added to the circuit known as hardware Trojan. A new field of cryptography named "DNA cryptography" which provides a new hope to identify and overwhelmed the Trojan. This paper contributes an overview of cryptography, DNA cryptography, and how it is pleasant to rectify the Trojan effect.

Keywords: Deoxyribonucleic Acid (DNA), DNA Based Cryptography, DNA Digital Coding, Image Security, Trojan

1. Introduction

1.1 Cryptography

The foremost role of cryptography is to shelter the data from attackers. It has two main terms plain text and cipher text. The original message which passed by the user that known as plain text and the text which adds keys to the original message is called as cipher text. Encryption techniques categorized as symmetric and asymmetric key encryption performances. In symmetric key cryptography, common key has been used for teller and recipient side. Some of the symmetric key cryptography systems are AES, DES, and 3DES. In asymmetric key cryptography the public key of the user1 used in teller side and the private key of the user2 used in receiver side. A few of the asymmetric key cryptography systems are RSA, DiffieHellman, ECC, and digital signature algorithm. Compared with DES and AES has effective in both software and hardware. With smallest number of rounds, AES encrypts the message with the key length of 128 bits, 192 bits, and 256 bits. The appraisal of symmetric key algorithms are shown in Table 1 and Table 2.

1.2 Trojan

A Trojan in computing is universally a malware program contains cruel code. It act as a stage door which comprehends the controller, it may give a remote admittance to a hacker for unofficial access in a particular computer. Some types of Trojan takes susceptibility in older description of internet explorer and google chrome to use the congregation computer as an anonymizer. To identify and secure the data from Trojan, blended hazard, DNA cryptography gives a forward step towards it.

1.3 DNA

Before delving into the principles of DNA computing, we must have a basic grip of DNA function. All creatures on this sphere are made of the alike type of genetic blueprint

*Author for correspondence

Table 1. Comparison of symmetric key algorithms[1]

METHOD	DES	3DES	AES
DEVELOPED BY	IBM and US Gov.	IBM	National Institute of Standard and Technology (NIST)
STRUCTURE ALGORITHM	Fiestel network	Fiestel network	Substitution and Permutation method
Key set-up	56bit	Three 64 bit keys with overall key length of 192 bit	128 bit 192 bit 256 bit
Block size	64	64	128
No.of rows	16	48	9
Susceptibility	Brute force attack	Some conjectural call attack	Side channel attack
Efficiency	Slow	Relatively slow in software	software and hardware

Table 2. Comparison of asymmetric key algorithm

METHOD	RSA
FEATURE	Encryption,decryption used the following equation: $C=M^e \bmod(n)$ $M=C^d \bmod(n)$ C=>cipher block C M=>Plaintext block M[2]
ADVANTAGES	1.Reverse process of e is difficult 2.Difficult to produce private key & modulus from public key

Table 2 Continued

DISADVANTAGES	1.Quite unhurried 2.Key generation is intricate 3.Large number factorization is difficult
METHOD	DIFFIE-HELLMAN
FEATURE	Secret key sharing is used for encryption and decryption together
ADVANTAGE	Short length key(256bit) so it is wanton
DISADVANTAGE	Man-in-the-middle attack
METHOD	ECC(Elliptical Curve Cryptography)
FEATURE	calculate the key through elliptical curve equation
ADVANTAGES	1.Utilize less influence 2.Using 164bit key for better safety
DISADVANTAGE	Difficult to implement compare with RSA
METHOD	DSA(Digital Signature Algorithm)
FEATURE	It consists of a pair of large numbers computed built on certain algorithm to authenticated algorithm[2]
ADVANTAGES	1.Very fast 2.Secures the data from man-in-the-middle attack 3.Offer non-repute and substantiation
DIS ADVANTAGE	It has short life span

which tie us as one. The way in which that scheme implied is the decisive factor as to whether you will be hairless, have a bulbous nose, xx, xy or even whether you will be a humanoid or an oak hierarchy. Within the cubicles of any creature is a substance called Deoxyribonucleic Acid (DNA) which is a double-stranded spiral of nucleotides which carries the genetic knowledge of a cell. This information is the secret language used within cells to form proteins and is the building block upon which life is moulded. DNA abbreviated as Deoxyribo Nucleic Acid. Every single cell in human body has a complete set of DNA[2]. DNA is made up of biological building masses called nucleotides. These nucleotide building blocks are complete set of three groups namely, phosphate group, and sugar group, nitrogen bases. To produce a strand of DNA, nucleotides linked in chains with the phosphate and

sugar group interchanging. Nitrogen bases are Adenine and Thymine, Cytosine, and Guanine. Nitrogen bases are very important to the human body activities.

1.4 Basics and Genesis of DNA Computing

DNA computing or molecular computing used for large parallel computation gives an account of utilizing innate combinational properties of DNA. This parallel search technique uses the appropriate DNA setup effectively to solve huge mathematical problem. From this we can easily analyze that the DNA computing is much faster than the conventional computer. Leonard Adleman, at the University of Southern California was the first to announces the theory that the makeup of DNA In early 1994, he kept his theory of DNA computing to test on a obscurity called the Hamiltonian path problem or sometimes mentioned to as the Traveling salesman Problem. The 'salesman' in this problematic has a map of numerous cities that he must trip to vend his merchandise where these cities have only one-way streets concerning some but not all of them. The knotty of the delinquent is that the salesman must discover a path to travel that passes through each city (A through G) exactly once with a designated beginning and end.

2. DNA Computing

DNA computing is also known as molecular computing. DNA cryptography is suitable for high data storage in compact manner when compare with quantum computing. It mainly gives a solution to NP-complete problem and conventional problems of cryptosystems. Adleman acquaint with the DNA computing in 1994 to make the bridge between DNA molecule and computer. He analyzed that DNA computing is faster than the electronic circuit. By using DNA computing he solved the Hamilton path problem[3]. In stretched the exertion of Adleman and examined the solution of NP-complete problem, and he finds the new opportunities of DNA computing[4]. In originate a new approach of DNA cryptography and he break one of the traditional algorithms called DES 1995[5]. In proposed another method by unite the steganography technique with DNA to conceal the secret message encoded as DNA strands[6]. In designed an encryption process by one-time pad and substitution method by utilizing the DNA density[7]. In developed two different approaches-first approach is to hide the information and second approach is to design molecular checksum to attack the problem of conventional computer[8]. In projected carbon nano-tube based message transformation and DNA-based cryptosystem for image security[9]. In designed a symmetric key cryptosystem using DNA biotechnology and microarray to secure the data in chip level[10]. In proposed a technique to encrypt the information using bio molecular automaton to improve the practical functionality of DNA computer[11]. In approaches a new encryption scheme by using DNA computing with traditional cryptography and RSA algorithm to cipher the original message[12]. In castoff the tools of DNA synthesis, PCR amplification, DNA digital coding, and traditional cryptography to design a new encryption scheme. This technique can be used to pre-process the original text to increase the refuge of it[13]. In deliberate an asymmetric encryption method and signature cryptosystem by combining genetic engineering and cryptology for giving a clear idea of fabricating a DNA chip[14]. In developed the new encryption scheme by combining molecular technique with RSA. Using this method, they examined the capability and reliability of the system[15].

3. Image Security using DNA Sequence

The scheme to shelter the data may not complement to protect the image. To secure the image using DNA sequence can be performed built on Watson-Crick rule. It describes that the nitrogen bases A (Adenine) will pair with T (Thymine) and C (Cytosine) will couples with G (Guanine). In deliberated a highly secured image by combining other encryption techniques and they favoured the secret permutation systems[16]. In approaches a random combinational image encryption procedure using bit, pixel, and block permutation[17]. In[18] have found a new image encryption performance founded on shuffling and confusion conception. In[19] used Fractional fourier transform (FFT) and Jigsaw transform and they designed a new image encryption system. In [20]proposed image and video encryption constructed on permutation and sub-

stitution mode. Permutation can be completed via SCAN pattern and product ciphers can be rehearsed using substitution method. Then[21] approach a new scheme by merging mirror-like image encryption and visual cryptography processes for better refuge. In[22] have proposed two encryption techniques for image selective encryption and multiple selective encryption and they got solider encryption with a smaller amount correlation. In[23] introduces a new image encryption technique by mingling image permutation and the RijinDael process. In[24] introduced a new method to sheltered an image by mingling permutation and hyper image encryption system. The binary value block will acquire from unique image and it can be reshuffled using permutation process, and then they generate the cipher image. In[25] projected a new innovative image encryption scheme based on DNA masking, genetic algorithm, and logistic mapping, and the result of this method has better masking technology. In[26] generated a secret key using DNA calculation and molecular arithmetic operation. Then the secret key is used to encrypt every pixel in the image. In[27] established an image encryption by via permutation and diffusion process. Permutation can be implemented by Hao's fractal sequence demonstration. In[28] developed an enhanced image security by using chaotic sequence, DNA, and genetic algorithm. By using this method it can produce high entropy with low correlation value of original image. In[29] has introduced a unique approach by using 3 layers of steganography to secure image. In[30] introduced an one dimensional chaos based encryption scheme by using Graphic processing unit and CPU parallelism.

3.1 Advantages

From the analysis of DNA computing with normal conventional computing, DNA computing has following advantages: Speed-Generally conventional computers can carry out its function appropriately around 100 millions of instruction per second (MIPS). A gram of DNA contains 10^{21} bases. By combining DNA threads it will perform arguably around 100 times speeder than the conventional computer. Minimal Storage Requirements – DNA stores data memory at a concreteness of 1 bit per cubic nanometres where conservative storage media requires 10^{F} cubic nanometres to store a single bit of data. From this analysis, mankind's collective acquaintance could be theoretically stored in a small bucket of DNA solution. Minimal Power Necessities - There is no extra power required for DNA computing while the computing takes place. The chemical bond of DNA forms the building block without any power consumptions. So it needs only minimum power.

4. Conclusion

The field of DNA computing is still evolving. The attractiveness of these DNA research trends is found in the possibility of mankind utilization of its very life building blocks to solve its most difficult problems. In any case, we will not be tossing out those PC's for test tubes of DNA anytime soon and the use of DNA computing with a greater security focuses other than the merchandise authentication methods is a long way off.

5. References

1. Chandra S, Alam SKS, Paisa S, Sanyal G. A Comparison survey of symmetric and asymmetric key cryptography, International Conference on Electronics Communication and Computational Engineering (ICECCE). 2014 Nov; p. 83-93.
2. Jacob G, Murugan A. DNA based cryptography an overview and analysis. International Journal of Emerging Science. 2013 Mar; 3(1):36-42.
3. Adleman L. Molecular computation of solutions to combinational problems. Science. 1994 Nov; p. 1025-1025.
4. Lipton RJ. Using DNA to solve NP-complete problems. Science. 1995; 268(5187):1021-24.
5. Boneh D, Dunworth C, Lipton R. Breaking DES using a molecular computer. Proceeding of DIMACS workshop on DNA computing. 1995 Jan; p. 1-15.
6. Celland CT, Risca V, Bancroft C. Hiding message in DNA microdots. Nature. 1999 Jun; 399:533-34.
7. Gehani A, Labean TH, Reif JH. Springer Berlin Heidelberg: DNA based cryptography. 2004; p. 167-88.
8. Leier A, Richter C, Banzhaf W. Cryptography with DNA binary strands. Biosystems. 2000 Jun; 57(1):13-22.
9. Chen J. A DNA-based biomolecular cryptography design. Proceedings - IEEE International Symposium on Circuits and Systems. 2003 Jun; 3:822-25.

10. Lu MX. Symmetric-key cryptosystem with DNA technology. Science in china series information Science. 2007 Jun; 50(3):324-33.
11. A method to encrypt information with DNA computing. Date Accessed: 28/09/2008: Available from: http://ieeexplore.ieee.org/document/4656718/.
12. DNA computing based cryptography. Date Accessed: 16/10/2009: Available from: http://ieeexplore.ieee.org/document/5338153/.
13. DNA computing and its application to information security field. Date Accessed: 14/08/2009: Available from: http://ieeexplore.ieee.org/document/5364229/.
14. Xuejia L, Mingxin L, Lei Q, Junsong H, Xinven F. Assymmetric encryption and signature method with DNA technology. Science in china: Information Science. 2010 Mar; 53(3):506-14.
15. An architectural framework for encryption and generation of digital signature using DNA cryptography. Date Accessed: 05/03/2014: Available from: http://ieeexplore.ieee.org/document/6828061/.
16. Cryptanalysis of a chaotic image encryption method. Date Accessed: 26/05/2002.
17. Mitra A, Subba Rao YV, Prashna ASRM. A New image encryption approach using combinational permutation techniques. International Journal of Electrical and Computer Engineering. 2006; 1(2):1-5.
18. Zhi-Hong G, Pangjun H, Wenjie G. Chaos-based image encryption algorithm. Physics Letters A. 2005 Oct; 346(1-3):153-57.
19. Image encryption by using fractional fourier transform and Jigsaw transform in image bit planes. Date Accessed: 01/05/2005: Available from: http://spie.org/Publications/Journal/10.1117/1.1906240.
20. Maniccam SS, Bairbakis NG. Image and video encryption using SCAN patterns. Pattern Recognition. 2004 Apr; 37(4):725-37.
21. Ozturk I, Sogukpinar I. Analysis and comparison of image encryption algorithm. World Academy of Science, Engineering and Technology. International Journal of Computer, Electrical, Automation, Control and Information Engineering. 2007; 1(3):1-4.
22. Techniques for a selective encryption of uncompressed and compressed images. Date Accessed: 09/2002: Available from: http://www.telecom.ulg.ac.be/publi/publications/mvd/acivs2002mvd/.
23. Mohammad Ali Bani Younes, Aman Jantan. An image encryption approach using a combination of permutation technique followed by encryption. International Journal of Computer Science and Network Security. 2008 Apr; 8(4):1-7.
24. Rathod Hiral, Sisodia Mahendra Singh, Sharma Sanjay Kumar. Design and implementation of image encryption algorithm by using block based symmetric transformation algorithm (Hyper Image Encryption algorithm). International Journal of Computer Technology and Electronics Engineering. 2011; 1(3):1-7.
25. Rasul Enayatifar, Abdul Hana Abdullah, Isnin Ismail Fauzi. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Laser in Engineering. 2014 May; 56:83-93.
26. Gupta Ritu, Jain Anchal. A new image encryption algorithm based on DNA approach. International Journal of Computer Applications. 2014 Jan; 85(18):1-5.
27. Zhang Qiang, Zhou Shihua, Xiaopeng Wei. An efficient approach for DNA fractal-based image encryption. International Journal of Applied Mathematics and Informatics and Information Sciences. 2011; 5(3):445-59.
28. Saranya MR, Arun K Mohan, Anusudha K. Algorithm for enhanced image security using DNA and genetic algorithm. International Conference on Signal processing, Informatics, Communication and Energy systems (SPICES) (2015).
29. Roy Sudipta, Sadhukhan Siddhartha, Sadhu Shayak, Bandyopandhyay SK. A novel approach towards development of hybrid image steganography using DNA sequence. Indian Journal of Science and Technology. 2015 Sep; 8(22):1-7.
30. Habibpour Leila, Yousefi Shamim, Lighvan Misa Zolfi, Adhdasi Hadi S. 1D chaos-based image encryption acceleration by using GPU. Indian Journal of Science and Technology. 2016 Feb; 9(6):1-6.