Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080134

A Cryptanalysis Method based on Niche Genetic Algorithm

Tao Li[1,2,*], *Jiguo Li*[1] *and Jing Zhang*[3]

[1] College of Computer and Information Engineering, Hohai University, Nanjing 211100 P.R., China
[2] College of Science, Anhui University of Science & Technology, Huainan 232001 P.R., China
[3] College of Science, Jiujiang University, Jiujiang 332005 P.R., China

Received: 16 Jun. 2013, Revised: 21 Oct. 2013, Accepted: 23 Oct. 2013
Published online: 1 Dec. 2013

Abstract: At present, the evolution cryptanalysis methods mainly adopt the basic genetic algorithm (literature [1] and [2]) which has ”early” phenomenon, searching stagnation in the near optimal solution, and low calculation efficiency. This paper inspired by biological genetic evolution proposes a niche genetic algorithm based on the code analysis method. This algorithm can keep the population diversity and prevent premature convergence. In genetic operator operation, this algorithm uses $(\mu + \lambda)$ selection strategy which has the strongest selection pressure. In order to achieve compensating the shortage of groups diversity easy loss, improve the searching efficiency of algorithm, speed up the convergence speed, this algorithm applies the multi-point crossover operation, at the same time adopts variation operation by introducing evolution mutation probability. This paper chooses examples to demonstrate the replace cryptogram. Experiments show that the algorithm can effectively reduce the complexity of the problem analysis, reduce the redundant computation, speed up the convergence. Therefore, in the limited time, it can effectively get an optimal solution or suboptimal solution of the analysis object.

Keywords: Niche, Genetic Algorithm, Substitution Ciphers, Cryptanalysis, Evolutionary Cryptosystem

1 Introduction

One of the component methodlogies of computational intelligence is evolutionary computation [31,32,33,34,35]. Evolutionary Computation (Evolutionary Computing), originated in the 1950s and 1960s, and used a computer to simulate the evolution of the natural world (in particular, the simulation of the process of biological evolution); to a bionic calculation method optimization and problem solving, evolution computing has become an important part of computer science [1]. According to Darwin’s theory of evolution point of view, nature provides the answer after a long process of evolution, and evolution generated as a result. From the evolution process, you can not only get the results, but also to solve many complex problems in biological adaptive process (evolution). It is based on this idea and developed a common evolutionary computation, problem solving methods [2].

Evolutionary computation to overcome the traditional cryptanalysis required in the deterministic algorithm, the deterministic cryptographic algorithm or through the key space exhaustive search to complete, or through the cryptographic algorithm itself then the mathematical characteristics have a deep understanding, otherwise cann’t effectively analysis. And in through the evolutionary computation can be in cryptanalysis, so as to realize automation, can greatly save the cryptanalysis of manpower and time [3,4,5], it will greatly increase the cryptanalysis efficiency.

Currently, in the case of existing computing resources,using evolutionary computation to handle cryptography NP problem is NP-hard problem, this would be a good choice [6,7] to handle this problem. The evolutionary cryptosystem is a new cryptosystem proposed by a Chinese research recently [29]. This article by using the combination of evolutionary computing and cryptanalysis technigues, the cryptanalysis object by a specific mathematical model to describe it in the search process, it can be automatically accessed and the accumulated knowledge of the search space. Then we can achieve the purpose of adaptive control of the search

* Corresponding author e-mail: 664723267@qq.com

process. Thus, on the basis of theories and methods of analysis through the use of password, you can effectively reduce the degree of complexity of the analysis of the problem, the analyzed optimal solution or suboptimal solutions can be completed within a limited time.

This article is based on the idea of niche genetic algorithm, the use of paper to maintain the diversity of the population, to achieve the purpose of preventing premature convergence; selection mechanism to $(\mu + \lambda)$ select genetic operators operating strategy, the strategy has the strongest selection pressure; multi-point cross, while introducing evolutionary mutation probability, the mutation operation, in order to achieve that the lack of compensation groups in diversity easy loss, but also be able to improve the search efficiency, to achieve the purpose of accelerating the convergence speed.

For simplicity's sake, this paper's examples choose replace the password to be analyzed. The experimental results show that, based on the niche genetic algorithm as a cryptogram analysis algorithm is feasible and it can effectively reduce the redundant computation, to speed up the convergence, through the select more excellent fitness function, selection operator, crossover operator and mutation operator, to more complex cryptographic algorithm to carry on the password analysis.

2 Cryptology evolution analysis of the development trend of the research

Cryptography is one of the most significant techniques in the field of information security [25,26,26,28,29,30]. The use of evolutionary computation to analyze the cryptology is the product of evolutionary computation and cryptography combined with each other, 30 years, and many scholars at home and abroad this series of research and study, and made a lot of achievements. There are number of evolutionary computation techniques, such as Cultured Algorithms, Genetic Algorithm, and Differential Evolution Algorithms.

In 1979, Peleg and Rosenfeld, simple substitution cipher using a relaxation algorithm (relaxation algorithm) cryptanalysis pioneered the application of intelligent computing technology to solve cryptanalysis a new solution.

In 1993, Spillman Janssen, etc and by Genetic Algorithm (Genetic Algorithm, GA) [7], Forsyth and Safavi - Naini using simulated annealing method, such as the sheet substitution cipher of analysis. Clark in 1998 [8], 2002 Grundlingh [9], and 2006 Uddin and Youssef [10] to this kind of technology respectively on the development, and the tabu search algorithm and particle swarm optimization algorithm respectively, such as introducing sheet substitution cipher analysis. In 2004, Servos, the use of genetic algorithm (GA) multi-Chart substitution Vigenere cipher of analysis [11], its basic characteristic is using genetic algorithm to identify and determine the parameters of the multi-chart substitution ciphers.

The 2004, Albassal using genetic algorithms (GA) deformation Feistel type cipher analysis [12], addition, Albassal using the same method and cryptography parameters, the genetic algorithm is applied to the deformation SPN cryptanalysis [13]. In 2004, Ali Al-Salami, a genetic algorithm (GA) and timing attacks (time attack) technical the RSA cryptosystem analysis method [14].

In addition, in 2006, Nalini, et al. using simulated annealing, tabu search and genetic algorithm of S-DES cryptanalysis [15], and in the text of the GA/SA/TS are three ways a comparative experiment. In 2010, Hamdani using artificial immune method, a four wheel DES 56-bit key analysis [16].

Tang M, et al[25], in 2012, proposed a novel idea that uses an EVOC against DPAs and DFAs. They research goal was to use EVOC to counteract known attacks, including SCAs and mathematical analysis methods (off-line attacks).

From a study of the current situation, combining with evolutionary computation method of cryptanalysis is still a very challenging and innovative research direction, has a lot of research, but there are still a lot of questions need to do further study and discussion. Thus, as early as in 2004, Clark on the analysis of the status and progress of the cryptology evolution do an analysis and discussion of the system, and pointed out that the analysis of the evolution of modern cryptography will be a very difficult, long-term task [17,22,23,24].

3 Related concepts

Evolutionary computation one and the same problem-solving method developed is based on the idea of the nature of the survival of the fittest. Evolutionary computing can describe the practical problems difficult on the basis of only according to the nature of the rules of survival can be performed problem solving, in particular, it is applied to te case of the cryptographic algorithm is unknown, or is simply not write analytical expressions cryptanalysis. Despite the evolutionary computation cannot guarantee to find the optimal solution of NP-hard problem is polynomial time, but evolutionary computation does not depend on its way to search for unknown space, to find high fitness value, or most times in the problem optimal solution.

3.1 Cryptography evolution analysis foundation

Encryption is an important mechanism for protecting sensitive information from an unauthorized access by transforming the information (plaintext) to another form which is unreadable (ciphertext) [35,36,37]. Nowadays,

we can find many cipher systems of different types. Hence, algorithm design combined with each other based on the evolution of computing and cryptanalysis. Usually, it considers the following two factors [2]:

1. First of all, we should be based on the analysis of the characteristics of cryptography objects chosen, and design code analysis algorithm of applicability, stability, convergence and reliability, and comprehensive consideration of the factors. This should focus on analysis to consider the structural characteristics of the type of cipher algorithm, cipher algorithm, as well as the security strength of the cryptography algorithm.

2. Secondly, we should use be based on the analysis of the cryptography object characteristics, and cryptanalysis modeling demands, the evolution in the calculation of the coding method, the control parameters, the evolution strategy, evolution operator, evaluation method and termination conditions and so on carry on comprehensive analysis and design. The key analysis to considering cryptographic algorithm mathematical model, safety strength, evolution strategy of design, and fitness function, these are to carry on the cryptography evolution analysis of key factors.

3.2 The advantages and disadvantages of genetic algorithm

As mentioned in the introduction, the genetic algorithm as an evolutionary computation algorithm has the advantages of fault tolerance, easy, fast, and unique advantage cryptanalysis. Genetic algorithm is taken to simulate the natural biological process of evolution, the probability of an adaptive global optimization search algorithm. Genetic algorithm generated initial population, in accordance with the nature of the ”survival of the fittest, survival of the fittest” law, is applied to the using of select operator, crossover operator and mutation operator are three basic genetic operators operating evolution, evolution the results will generate new populations suitable for nature to survive. Through continual evolution, and finally, the population will gradually converge to the individuals best adapted to survive in nature, the individual shall be solving the problem of the optimal solution.

Genetic programming is a good technique for finding near-global optimal solutions for complex problems, by finding the program used to solve the problems [35]. Due to genetic algorithm, a stochastic optimization and search algorithms simulate the natural biological evolution, in accordance with the principle of survival of the fittest, the algorithm is no longer blind chaos search, more is not exhaustive comprehensive search, therefore, the genetic algorithm is particularly suitable for cryptographic algorithms that no clear analytic expression analysis, and genetic algorithm implies parallelism, can greatly shorten the time of cryptanalysis, and improve the efficiency of cryptanalysis. Although genetic algorithms has gained many applications, however, it is reported that the simple genetic algorithms there is a lot of drawbacks, these searches will occur, such as obviously there are ”premature” phenomenon, especially when the genetic algorithm to search the global optimal solution near stagnation or forward slowly the phenomenon showed solving not globally optimal solution, or inefficient.

3.3 Niche genetic algorithm

There are many improvements have been proposed to enhance the performance of the genetic algorithms, such as Niche genetic algorithm. In biology, niche (noching) refers to the specific environment of an organization’s function, and has the common characteristics of the organization called population (or called species). In nature, biology has always been a tendency to with their own characteristics, character similar to come together, and in the similar in mating and reproduce, that positive and assortative mating mode in population genetic evolution process has the positive role. But, in standard genetic algorithms, mating process is totally random, this randomized form ensure the optimization in the initial stage of the diversity of solution, but in the search to the global optimal solution of the nearby, a large number of individual concentrated a local optimal solution above, at this time because of their offspring caused the inbreeding consequences.

To avoid this phenomenon, niche technology generation genetic individual classification in each class to select a large number of fitness genetic individual, as the excellent genetic individual representatives of a class, and put it back together into a new population; Subsequently, a new population, the operation genetic operators (crossover and mutation) and then generate a new generation of individual populations. With this pre-selection mechanism, outstanding individuals on behalf of populations can be saved, and only better than the parent individual eligibility for survial in the offspring, so that, in the course of evolution, it can be clustering method constantly found new populations at the same time, continue to evolve with more outstanding individuals, which makes the population has been continuouslu optimized. The specific steps of algorithm are as follows:

Step 1. According to the specific problems, and choose the right transformation strategy, combined with the parameters (namely feasible solution set) conversion for chromosome structure space;

Step 2. Adopt the ”three choose a” principle, to generate the initial population;

Step 3. Structure meet the specific problem conditions of small habitat population; Adopt the ”three choose a” principle, to generate the initial population;

Step 4. According to the niche genetic algorithm of fitness function, calculate average fitness, and the most optimal individual;

Step 5. For niche populations were excellent individual replacement;

Step 6. Niche population genetic operator operation (i.e.: selection, crossover and mutation) and iterate;

Step 7. According to the niche population termination conditions for judgment: If for the calculation of the niche population meet termination conditions, then stop the calculation, output niche population fitness optimal individual; otherwise, continue iteration, until meet specified iterations didn't stop. The solution is the best chromosome of the last generation.

4 Niche genetic algorithm in the application cipher analysis

According to the niche genetic algorithm of the basic thought, for the sake of simplicity is adopted in this paper, replace the cryptography as analysis examples, using the niche genetic algorithm analysis step by step. The description of these steps is given in the following subsections along the proposed algorithm parameters.

4.1 Substitution cipher

Substitution cipher is a very classic classical cryptography, the basic algorithm ideology as follows [18]:

Step 1. Set K is an element in the Z_{26} all arrangement set, namely: $K = \{(k_1, k_2, k_3, \cdots, k_{26}) \ , \ k_i \in Z_{26}\}$.

Step 2. Select any key: $\forall k_{key} \in K$.

Step 3. Set plaintext for: $M = (m_1, m_2, m_3, \cdots, m_i)$, and $m_j \in Z_{26}\,(1 \le j \le i)$.

Step 4. Set encrypted cryptograph get for: $C = (c_1, c_2, c_3, \cdots, c_i)$, and$c_j \in Z_{26}\,(1 \le j \le i)$.

Thus, according to the above algorithm ideas define the encryption operation $E_k(m)$ and decryption operation $D_k(c)$ may be as follows:

$$c_j = E_k(m_j) = k[m_j] \ (1 \le j \le i)$$

$$m_j = D_k(c_j) = E_k^{-1}[c_j] \ (1 \le j \le i)$$

4.2 Chromosome coding representation and initialization population

An important step in the evolution cryptanalysis algorithm design is the encoding of the object as cryptanalysis; coding scheme design has always been the evolution of one of the difficulties of the algorithm [19]. Niche Genetic Algorithm is a technique that dynamically adjusts selected control parameters, such as population size and genetic operation rates, during the course of evolving a problem solution.

Analyzed taking into account the cryptography replace the cryptography, and the replacement of the basic characteristics of the cryptography, the characters of the plaintext message is replaced by another character or symbol. Then taking into account to calculate the encryption and decryption computation efficiency, can be used directly to the binary encoding of the English characters. Binary encoding of the benefits of using English characters: simple encoding and decoding operations, crossover operator, mutation operator and genetic manipulation is easy to realize; binary coding in line with the principle of minimum character set encoding, schema theorem can easily analyze.

Thus, when the system is initialized, you can randomly generate a set of 26 of the same binary coded English string; entire string is a chromosome represents an initial individual pi generate a total of n groups these n groups as the initial population. The value of n is too small, it is easy to produce the phenomenon of "premature", while the value of n is too large, the lower the efficiency of the operation of the algorithms. Therefore, the value of n generally ranges: 20 to 100.

4.3 Fitness function determination and calculation

In the evolution cryptanalysis algorithm, evaluation methods or the design of fitness function, it is another influence cryptanalysis of one of the difficult points of success or failure. In this paper, Grundlingh [9] proposed fitness function, the fitness function is through the plaintext and ciphertext decrypted one, two letters collision frequency to reflect the relationship between them approximation, the basic idea is: if the ciphertext decrypted character one, two letters of the collision frequency and the corresponding proclaimed in writing the letter the collision of the same times, the test is key to the original key the same. Based on this thought, can get fitness function of the specific expression is as follows:

For natural language L, length for N of the cipher text T, candidate key k', substitution ciphers a letter fitness function for:

$$F_1(L,N,T,k') = \frac{2\left(N-\rho_{\min}^N(L)\right) - \sum_{i=A}^{z}\left|\rho_i^N(L) - f_i^{T(N)}\left(k'\right)\right|}{2\left(N-\rho_{\min}^N(L)\right)}$$

Substitution cyphers two letter fitness functions for:

$$[F_2(L,N,T,k') = \frac{2\left(N-1-\delta_{\min}^N(L)\right) - \sum_{i,j=A}^{z}\left|\delta_{ij}^N(L) - f_{ij}^{T(N)}\left(k'\right)\right|}{2\left(N-1-\delta_{\min}^N(L)\right)}$$

among them, $\rho_i^N(L)$ (or $\delta_{ij}^N(L)$) represents the N character text in the natural language L, text letters i (or

two letters ij) to expect the number of occurrences; $f_i^{T(N)}(k')$ (or $f_{ij}^{T(N)}(k')$) said cipher text T the key k' after decryption of the letter i (or two letters ij) appear collision number, and:

$$\rho_{\min}^{N}(L) = \min_i \left\{\rho_i^N(L)\right\}$$

$$\delta_{\min}^{N}(L) = \min_{ij} \left\{\delta_{ij}^N(L)\right\}$$

4.4 Operating parameter

One of the main problems related to Niche Genetic Algorithm is to find the optimal control parameter values that it uses, when a poor parameter setting is made for an evolutionary computation algorithm, the performance of the algorithm will be seriously degraded [35]. Therefore, we use the following parameter settings (a widely practiced approach to identify a good set of parameters for a problem is through experimentation.):

1. Selecting operator:

Selecting operator on the basis of the results calculated according to the fitness function of the individuals in the entire population of "survival of the fittest" choice. Goldberg pointed out that, in evolutionary computation, the main selection mechanisms: proportional selection, elitist strategy, determine the type of using the ranking selection, tournament selection, $(\mu+\lambda)$ selection mechanism. Among these, $(\mu+\lambda)$ selection mechanism has the strongest selection pressure [20]. The basic idea of the $(\mu+\lambda)$ selection mechanism: allows μ of parent individuals and λ of offspring individuals to participate in the competition, choose from μ of high fitness value of the individual into the new population. The old population is completely replaced by the new population which is generated from the old population by applying the genetic operations.

In this paper the niche technology to perform to choose. A detailed description is as follows:

a. First, the randomly generated size is 2n of the initial population of each individual calculation adaptive value;

b. Will be calculated each individual fitness value, according to the size sort;

c. Apply to sort of individuals, according to size sequence in n to father generation individual;

d. Will be n of father generation that an individual's genetic code restructuring, reorganization will get progeny and father generation, together do common competition, (2 + 2) choice, sure choose excellent individual into the next generation of genetic.

2. Cross operator

Crossover operator is mainly used for population have new individual a method. The main method is single point cross, two-point crossover and multipoint crossover and uniform cross, count cross, etc. Best individual selection operator operating, multi-point crossover operation. Cross probability value or big or small, all of the algorithms have obvious influence, general value ranges for: $0.4 \backsim 0.9$.

3. Mutation operator

Mutation operator is mainly for in the search space, can dynamically structure niche, which can provide reliable guarantee the global convergence. General common mutation operators are: basic position variations, uniform variation, boundary variation, fly uniform variation, gauss mutation and so on. Variable probability value or big or small, the entire algorithm has obvious influence, general value range for: $0.0001 \backsim 0.1$.

4. Termination condition

Termination condition, which is in the whole niche population is no longer evolution trend, can terminate running. Usually, terminated iterative value range for: $100 \backsim 1000$.

5 Application examples

In accordance with the algorithm described in this article, we can get the cryptanalysis niche genetic algorithm flowchart as follows:

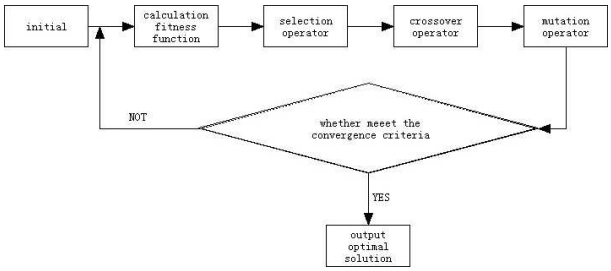

Fig. 1: The Niche Genetic algorithm flowchart.

The Niche Genetic Algorithm has been modified to consider the dynamic setting of the algorithm parameters which are mutation and crossover.

This paper use MATLAB7.0 to carry on the concrete programming realization, the specific operation parameters for: population scale is 20, termination conditions: iterations for 100, crossover probability for $P_c = 0.4$, mutation probability for $P_m = 0.01$. The parameters used in this work were set based on the experimental results, the parameter value that show the highest performance was chosen to be used in the implementation of the algorithm.

Table 1: Random Key k for 64 bit experimental results.

Experiment No	Probability of success	Average iteration
100	94.99%	70
100	81.06%	73
100	86.27%	68

Table 2: Random Key k for 128 bit experimental results.

Experiment No	Probability of success	Average iteration
100	98.59%	86
100	85.29%	74
100	88.26%	78

Contrast random key k are experimental data of 64 bits and 128 bits, can be found, with the growth of the random key k, resulting in the success rate has been greatly improved, and the average number of iterations to reduce. Visible in the actual cryptanalysis, when the longer cryptanalyst master key sequence will be more help to improve the efficiency of this analysis algorithms.

6 Conclusions

The above experiments results show that the niche genetic algorithm can be successful decryption replace the password encryption ciphertext, thus instructions will be niche genetic algorithm as a cryptanalysis method is feasible. In order to different cryptography system evolution code analysis, can be in has successfully to carry on the cryptography on the basis of analysis, through the improvement to the selection operator, crossover operator and mutation operator, and design a better fitness function for evaluation, and combination with other more excellent stochastic optimization algorithm, it also can achieve to more complex cryptographic algorithm effectively analysis [21].

Acknowledgement

This work is supported by the National Natural Science Foundation of China (61272542, 61103183, 61103184, 1048-51216911), the Fundamental Research Funds for the Central Universities (2009B21114, 2010B07114), the Six Talent Peaks Program of Jiangsu Province of China (2009182) , national characteristic professional (TS12142), Anhui provincial teaching research project (2008jyxm354, 2008jyxm359), and Program for New Century Excellent Talents in Hohai University. Thanks for the help.

References

[1] Pan zj, Kang ls, PanZhengJun. Evolutionary computation [M]. Beijing: Tsinghua university press, (1998).
[2] ZhangHuanGuo, QinZhongPing, etc. Evolution in cryptosystem [M]. Wuhan university press, (2010).
[3] ZhangHuanGuo, FenXiuTao, QinZhongPing, etc. Evolution cryptosystem and DES cryptosystem evolution design [J]. Journal of Communication, **23**, (2002).
[4] ZhangHuanGuo, FengXiuTao, QinZhongPing, etc. Evolution cryptosystem and the evolution of the DES cryptosystem [J]. Journal of Computers, **26**, 1678-1684 (2003).
[5] ZhangHuanGuo, WangZhangYi. Cryptography (in second edition) [M]. Wuhan:Wuhan university press, (2009).
[6] HuNengFa, DengYongFa. Based on genetic algorithm sequence code generating method [J]. Computer engineering and design, **26**, 2190-2192 (2005).
[7] Li Ya-peng, Ding Wen-xia. An Optimal Design of S-box Based on Genetic Algorithm [J]. Journal of Chongqing University of Technology (Natural Science), **26**, 79-84 (2012).
[8] Richard Spillman, Mark Janssen, Bob Nelson, Martin Kepner. Use of A Genetic Algorithm in the Cryptanalysis of simple substitution Ciphers [J]. Cryptologia, **XVII**, 187-201 (1993).
[9] Clark JA. Optimization Heuristics for Cryptology [D]. PhD thesis, Queensland, univeristy of Technology, (1998), http://sky.fit.qut.edu.cn/∽clarka/papers/thesis-ac.pdf.
[10] Grundlingh W, Van Vuuren J H. Using Genetic Algorithms to Break a Simple Cryptographic Cipher [J/OL]. Submitted 2002, Retrieved March 31, (2003). Http://dip.sun.ac.za/∽vuuren/abstr genetic.htm
[11] Bafghi A G., Sadeghiyan B. Finding suitable differential characteristics for block ciphers with Ant colony technique[C]. Proceedings of the Ninth International Symposium on Computers and Communications, ISCC'04, **2**, 418-423 (2004).
[12] William Servos, Trinity College, Hartford CT. Using a genetic algorithm to break Albertic Cipher [J]. Journal of Computing Sciences in Colleges archive, **19**, 294-295 (2004).
[13] Albassal A M B, Wahdan A M. Genetic Algorithm cryptanalysis of the basis substitution permutation network [C]. Circuits and Systems, 2003. MWSCA'03. Proceedings of the 46^{th} IEEE International Midwest Symposium, **1**, 81-85 (2004).
[14] Albassal A M B, Wahdan A M. Genetic algorithm cryptanalysis of the basis substitution permutation network [C]. Circuits ans systems, 2003. MWSCA'03. Proceedings of the 46^{th} IEEE International Midwest Symposium, **1**, 471-475 (2003).
[15] Hamza Ali, Mikdam Al-Salami. Timing Attack Prospect for RSA cryptanalysts Using Genetic Algorithm Technique [J]. IAJIT Journal, **1**, 81-85 (2004).
[16] Nalini N, Raghavendra Rao. Cryptanalysis of Simplified Data Encryption Standard Via Optimaisation Heuristics [J]. IJCSNS International Journal of Computer Science and Network Security, **6**, 240-242 (2006).
[17] Syed Ali Abbas Hamdani, Sarah Shafiq, Farrukh Aslam Khan, Cryptanalysis of Four-Rounded DES Using Binary Artificial Immune system [C]. Advances in Swarm Intelligence First International Conference, ICSI 2010, Beijing, China, Springer Berlin, 338-346 (2010).
[18] Clark J A. Invited Paper-Nature-Inspired Cryptography: Past, Present and Future [C], Conference on Evolutionary Computation, Special Session on Evolutionary Computation in Computer Security and Cryptography. Canberra, CEC2003, **8**, 1647-1654 (2003).
[19] Spillman R, Janssen M, Nelson B, et al. Use of a genetic algorithm in the cryptanalysis of simple substitution ciphers [J]. Cryptology, (1993).

[20] ZhouMing, SunShuDong. Genetic algorithm principle and application [M]. Beijing: national defense industry press, (2002).
[21] Goldberg D E, Deb K. A comparative analysis of selection schemes used in genetic algorithms. In Rawlings, 69-91 (1996).
[22] Nalini N, Raghavendra Rao G. Cryptanalysis of Simplified Data Encryption Standard (SDES) Using Genetic Algorithm [J]. Submitted to International Journal of Information and Computer Security (IJICS), Inderscience Publishers, (2006).
[23] Meng Q S, Zhang H G, Tang M, et al. Analysis of affinely equivalent Boolean functions. Sci China Ser F-Inf Sci, **50**, 299-306 (2007).
[24] Zhan H G, Li C L, Tang M. Capability of evolutionary cryptosystems against differential cryptanalysis. Sci China Inf Sci, **54**, 1991-2000 (2011).
[25] Tang Ming, Qiu ZhenLong, et al. Evolutionary ciphers against different power analysis and differential fault analysis. Sci China Inf Sci, **55**, 2555-2569 (2012).
[26] Mentens N, Gierlichs B, Verbauwhede I. Power and fault analysis resistance in hardware through Dynamic reconfiguration. In: Workshop on Cryptographic Hardware and Embedded Systems 2008 (CHES 2008), Washington, 349-362 (2008).
[27] Wang H Z, Zhang H G, Wu Q H, et al. Design theory and method of multivariate hash function. Sci China Inf Sci, **53**, 1997-1987 (2010).
[28] Hermelin M, Nyberg K. Dependent linear approximations the algorithm of Biryukov and others revisited. In:Pieprzyk J, ed. CT-RSA2010, LNCS 5985. Berlin:Springer-Verlag, 318-333 (2010).
[29] Zhang H G, Li C L, Tang M. Evolutionary cryptography against multidimensional linear cryptanalysis. Sci China Inf Sci, **54**, 2565-2577 (2011).
[30] Zhang H G, Li C L, Tang M. Capability of evolutionary cryptosystems against differential cryptanalysis. Sci China Inf Sci, **54**, 1991-2000 (2011).
[31] Wang H Z, Zhang H G, Guan H M, et al. Design theory and method of multivariate hash function. Sci China Inf Sci, **53**, 1997-1987 (2010).
[32] Wang H Z, Zhang H G, Guan H M, et al. A new perturbation algorithm and enhancing security of SFLASH signature scheme. Sci China Inf Sci, **53**, 760-768 (2010).
[33] Awad, W.S., The applications of GA in cryptology. Far East Journal of Experiment and Theoretical Artificial Intelligence, **2**, 59-76 (2008).
[34] Yuichiro, U., Mitsunori, M., Tomoyuki, H., Simulated Annealing Programming Using Effective Subtrees. Doshisha Daigaku Rikogaku Kenkyu Hokoku, **49**, 205-209 (2009).
[35] Wasan Shaker Awad. Designing Stream Cipher Systems Using Genetic Programming. Lecture Notes in Computer Science, **6683**, 308-320 (2011).
[36] Gao Sheng, Ma Wenping, Guo Na, er al. Design of cross-correlation test algorithm on S-box [J]. Geomatics and Information Science of Wuhan University, **35**, 558-561 (2010).
[37] GAO Sheng, MA Wnping, ZHU Jiwei. High-Order Bit Independence Criterion Test for the S-boxes [J]. Wuhan University Journal of Natural Sciences, **16**, 447-451 (2011).

Tao Li born in 1979, Ph.D. Candidate,Hohai University student. His main research interests include information security and cryptography theory and technology.

Ji-Guo Li born in 1970, Ph.D., Hohai university professor, Doctoral supervisor. His main research interests include information security and cryptography theory and technology.

Jing Zhang born in 1979, MS degree, Jiujiang university lecture. Her main research interests include information security and cryptography theory and technology.