Global Journal of Computational Intelligence Research.
ISSN 2249-0000 Volume 4, Number 1 (2014), pp. 1-8

http://www.ripublication.com

Conventional Cryptography and Evolutionary Approach

K. Kalaiselvi and Anand Kumar

ABSTRACT

Security in network is based on cryptography, the science and art of transforming the messages to make them secure and immune to attack. Cryptography is the most important aspect of communications security, where integrity, non-repudiation, confidentiality, and authentication services plays a vital role. Ciphers are developed to create a secure channel for message communication. The field of cryptography and cryptanalysis is quite demanding and complex as it minimizes the need for time-consuming human interaction with the search process and the network security. However, recurring events such as hackers and intruders attack and the success of criminal attackers illustrate the weaknesses in current security system, information technologies and the need to provide heightened security for these systems. Thus, the application of an efficient and effective tool such as Computational Intelligence (CI) to the field of cryptology comes naturally. CI systems are usually hybrids of paradigms such as Evolutionary Computation systems, Artificial Neural Networks and Fuzzy systems, supplemented with elements of reasoning. Genetic Algorithm is a class of evolutionary computation which is expected to provide optimized and deterministic solution to various common cipher attacks. This paper explores various techniques in cryptography to prove that the natural selection and adaptive mechanism based techniques are as good as the rigorous mathematical techniques used by traditional cryptographic methods.

Keywords Cryptography, Cryptosystem, Computational Intelligence (CI), Evolutionary computation (EC), Genetic Algorithms (GA), Natural Selection, Pseudo random number generator (PRNG).

Introduction

Cryptosystems are developed to create a secure message communication and data transfer. One common factor behind these cipher is the use of certain secret keys. These keys are generated through one-time pad or random number generators which should be unique and non-repetitive. Many traditional cryptosystems such as DES, AES, RSA were developed using complex mathematical logics such as computational

algebra, number theory, probability theory and algebraic geometry. A number of complex mathematical problems have been motivated by public key cryptography during the few decades. Computational Intelligence can be considered as the study of adaptive mechanisms that enable intelligent behavior of a system in complex and changing environments. EC is a branch of CI that are designed to model aspects of biological and natural intelligence which can be utilized to design many cryptosystems. This paper gives an introduction to the possibilities of evolutionary computation methods when applied to modern cryptography. This paper follows the pattern like: Section 1 discuss the characteristics and limitations of existing cryptosystems. Section 2 discuss briefly about the Security evaluation results of major Cryptosystems. Section 3 explains the Significance of EC and Section IV explain EC in the field of Cryptography.

I. Dimensions of cryptographic systems:

A conventional cryptographic system operates with the following three characteristics. [1].

1. Number of keys used: If both sender and receiver uses the same key which is referred to as *Symmetric, Single- key, Secret-key or conventional encryption.* If the sender and receiver uses different but related keys which is referred to as *Asymmetric, Two-key, Public-key encryption.*
2. Types of operations used to convert plaintext to ciphertext: *Substitution ciphers* encrypts each elements in the plaintext like bit, letter is mapped into cipher text. *Transposition cipher* rearranges the plaintext into cipher text.
3. Plaintext processing modes: A *block cipher* processes one input block of elements to produce an output block. A *stream cipher* processes the input elements continuously to produce one element at a time.

Limitations in the existing cryptosystems:

1. In symmetric encryption both sender and the receiver must share the same key, which is protected from access by others. The strength of any cryptographic system depends on the key-distribution technique which means delivering a key to both parties without others knowledge. The key distribution creates a problem in a wide area distributed system where there are many communicating pairs. One key is needed for each pair of hosts on the network which needs to communicate. A drawback of this type of cryptosystems is, it requires prior communication of the key between the sender and the receiver, through a secure channel.
2. Cryptosystems such as, Discrete Logarithm Problem, Diffie–Hellman key Problem, Diffie–Hellman Mapping Problem, rely on the assumption that these problems are computationally intractable. The computation cannot be completed in polynomial time [3].
3. RSA is a well known public-key cryptosystem which works on the mathematical concept of finding the prime factorial of a composite number.

The RSA encryption scheme [RSA78] relies on the assumption that factoring large integers, decomposing integers into their unique product of primes, is a hard problem.

4. The security of the Diffie-Hellman key exchange protocol [DH76] is based on the hardness of computing discrete logarithms. The majority of public key schemes depends on some well-known assumptions. Integer Factorization or the Discrete Logarithms are the efficiently practiced mathematical calculations for both symmetric and Asymmetric cryptosystem. Though these problems provide necessary security conditions, they are not sufficient. In other words, there might be more efficient ways to break these systems than solving the Factorization and Discrete Log problems [3].
5. Pseudo Random-number generators are another place where cryptographic systems often break. PRN which is generated by the deterministic algorithm should be of uniform number distribution and statistically independent numbers. It is a major threat to the cryptosystem if the opponent predicts the future elements of the sequence on the basis of the earlier elements [1].

II. Security Evaluation Results of Major Cryptosystems:

This section discuss the security evaluation of some of the major cryptographic algorithms.

A. Symmetric Ciphers

Symmetric ciphers are classified into block ciphers and stream ciphers. Block ciphers divide a plaintext into segments of a fixed size (“blocks”) and encrypt each block at a time. Stream ciphers generates pseudo-random numbers (PRN) of the same size as the plaintext and generate the ciphertext by calculating the exclusive OR (XOR) serially bit by bit. The security evaluation for the cryptographic algorithms namely triple DES, DES, RC2, IDEA, AES, (all are block ciphers), and RC4 (a stream cipher) are discussed below [2].

1. Block ciphers

Block ciphers attacks are divided into shortcut attacks and brute force attacks. The shortcut attacks minimizes the computational complexity required to find the correct key by exploiting the analytical and statistical calculations of the algorithms. The brute force attack tries one after the other encryption key to obtain information on the correct key and/or to get the plain text (exhaustive key search). If the computational complexity is comparatively less, then its more prune to attack which has a fatal effect.

2. Stream ciphers

Stream ciphers generates a PRN whose size is as same that of a plaintext and calculate XOR between the PRN and the plaintext bit by bit to generate a ciphertext. The security depends on the PRN generator. The encryption key and the PRN are strongly

correlated to each other. If the generator goes defective, then the future PRNs can be easily predicted from the past numbers and the cryptosystem is broken efficiently.

B. Asymmetric Ciphers

RSA, DSA are good examples of Asymmetric Ciphers. Security of these cryptographic algorithms can be proved to be equivalent to the difficulty of a mathematical problem such as factoring under certain assumptions.

1. RSA

The security of RSA depends on the difficulty of prime factoring of the large composite numbers. The RSA primitive algorithm permits numerous variations in encryption and digital signature schemes. The difficulty in the factorization method proves to be providing the cyber security and enhance the performance of the cryptosystem. Even though an efficient algorithm for factorization or a powerful hardware for the same has been proposed, none of these methods can prevent cryptanalysis and signature forgery.

2. DSA

The difficulty of solving the discrete logarithm problem (DLP), forms the base for the security of DSA in the multiplicative group of a finite set fields. At Present, index calculus is the fastest algorithm for solving DLP. The key length of the algorithms based on DLP is set as long as that of the factoring problem algorithms. Factoring of long key composite number as a security measure will no longer be the trend in cryptography since many cryptanalysis have been developed to break the same.

An alternative system can be developed with less mathematical dependency which can overcome some or all of the above mentioned limitations. A robust intelligent technique such as evolutionary computation becomes the need of the hour in cyber security.

III. Significance of Evolutionary Computation:

Evolutionary Computation (EC) draws its inspiration from evolutionary mechanisms such as natural selection. genetic inheritance and adaptive behavior, to design optimization and classification methods. EC paradigms that form this class are *Genetic Algorithms* (GA), *Genetic Programming* (GP), *Evolutionary Programming* (EP), *Evolution Strategies* (ES) and *Differential Evolution* (DE), *Swarm Intelligence* (SI). EC seems promising to enhance cyber security measures, and have been increasingly applied in the area of information security and information assurance. This multi-faceted approach provides a new security paradigm to deal with influx of new threats in a large network of computers.

Cryptographic applications can be developed with the help of EC methods in the areas which includes creation of block ciphers and generating PRNs. EC uses iterative progress, like growth or population development. Random search is applied to this population to achieve the desired goal. These processes are inspired from the biological evolutionary mechanism. The section that follows gives a brief explanation

about genetic algorithms (GAs), genetic programming (GP), tabu search (TS), and simulated annealing (SA).

1. Genetic Algorithms

The Genetic Algorithms (GAs) are heuristics algorithms based on the Darwin's theory of natural selection and fitness. The basic idea behind using GAs are robustness, efficiency and optimization. GAs are applied to the problem which has optimized and deterministic solutions. The natural population for these problems are depicted from the genetic chromosomes which are considered as a set of binary numbers. Each bit represents a cell and is perceived either as a positive or a negative solution. Using Pseudo Random Number Generator (PRNG) the fitness population is generated. Fitness function measures the quality of the solution, which is problem dependent. The first generation which is evaluated is enhanced by using basic operations like Selection, crossover and mutation. Process of selecting the individuals which produce new generation is called Selection operator. Crossover combines two or more parent solutions to generate one or more child with good fitness value. Mutation operator generates random change among the individuals. [6] [7]

2. Genetic Programming

Genetic programming represents automatically evolving programs by means of natural selection-based strategies. It is a population based search method using a fitness function. GP is inspired by Genetic Algorithm. But the main difference is that GA uses the chromosome encoding to generate the solution to a problem, whereas GP evolves from the whole computer programs. Programs that are generated by GP are represented in the form of tree structure. Each tree node has an operator function and each terminal node has an operand. Crossover and Mutation are the operators used in GP. Switching of one node to another is done by crossover and node replacement is done by mutation operator [5] [7].

3. Tabu Search

Tabu search [7] is an optimization method that belongs to the class of local search techniques. Cryptographic algorithms are designed in such a way that the secret key based algorithm is large enough so it is not possible for any attacker to try all possible key. The key search need not be done for the entire search space. Tabu search performs a local search method which uses the memory structures where it stores the solutions. The candidate solution is determined and it’s added in the Tabu list so that the cryptosystem algorithm will not visit that possibility again. The iterative local search procedure moves from one solution to another until it explores the entire key spaces. This method can be well utilized to generate unique key generations in cryptography.

4. Simulated Annealing

Simulated Annealing (SA) is a generic probabilistic meta heuristics method which uses Hill-climbing technique. Each point of search space is analogous to a state of a physical system. This method helps to locate a good approximation to the global

optimum of a given function in a large search space [7]. It is used in discrete search space is discrete. SA works well when the solution for a problem needs to be acceptably good solution in a fixed time rather than the best solution. Cryptosystem uses boolean functions for symmetric key ciphers. Security of the cipher depends on these boolean functions. Heuristic methods simulated annealing properties provides an enhanced technique for designing such function for the symmetric keys.

IV. Evolutionary Computation in Cryptography:

1. ICIGA system (Improved Cryptography Inspired by Genetic Algorithms):

It is an improved system of "Genetic Algorithms Inspired Cryptography" by the same authors [8] [9]. It is a block cipher system in which the secret key is generated randomly. The block size and the key length depends on user system. The plaintext will be divide into equal size depending on the length of the key. Then again they are broken into blocks of same size. Genetic algorithm operators Crossover and Mutation are applied, which operates on the secret key. The position of the operators are masked by using left shift. Repeatedly left shift is applied to mask the whole blocks. The secret key is used to choose the genetic operators and position when it is applied to the plaintext. Decryption is done by right shift operation with crossover and mutation operators in reverse order. The authors have compared the ICIGA system with other symmetric key ciphers like DES, IDEA, and AES and claims that ICIGA is faster than DES and AES.

2. Evolving Hardware for RSA Systems:

In the RSA systems modular exponentiation and modular multiplications are the basic components. It is essential to optimize the time consumed when the hardware for these operations are engineered. A draw back in hardware designs using modular multiplication is side-channel leakage. Since the design of modular exponentiation is repetitive, it is possible to trace the data transfer, which leads to the disclosure of the private key of the cryptosystem. To overcome this constraint, the authors designed a cryptographic circuit using evolutionary computation methods [10]. The hardware can dynamically change its architecture and behavior by interacting with the current environment. Combination of crossover and mutation operators are used to represent the basic gates in the circuit implementation. The authors compared the design created by genetic programming with that of the normal circuit design and understood that the GP hardware are efficient in hardware and in cryptography.

3. Generating Cryptographically Sound Boolean Functions:

Research work has been done by Clark [11] using Genetic algorithms to generate sound boolean functions. If given a boolean input, based on logical calculation the boolean value output can be determined by the boolean to break. GAs were used in the binary representation where each individual population is treated as a binary string. Initial population is created with randomly generated boolean function. Then, using the non-linear property of the function the fitness of the solution is calculated. *Merge* operator is applied to the parents with minimum Hamming distance to produce

a offspring close to them. Mutation is not used, since it may reduce the non-linearity of the solutions. The result showed that GAs alone or with the combination of Hill climbing technique produces a better result than which is obtained by a random search function. The linear combination of S-box columns generates the boolean function. This is an important primitive for the block and stream ciphers. In order to prevent the cryptosystem from cryptanalytic attack high non-linear boolean function has to be generated. Author experimented with GAs to find a better non-linear solutions which are not easy

4. Design of Pseudorandom Sequence:

Evolutionary computation produces excellent results when it combines more than one of it methods. Genetic algorithm is utilized to find Cellular Automata finite rules. These set of rules are used to generate Pseudo random numbers for the use in cryptography [12]. Cellular Automata proves to be an alternative for PRN generators, which is easy to implement in the hardware. Authors used non-homogenous local rules with one-dimensional cellular automata, in which each cell has one - five neighbors. GAs are used to generate the rules. The method is as follows:

1. Calculate the fitness function of each cell.
2. Compare the fitness with the neighbors.
3. Mutation and crossover are performed on the resulted candidate cell.
4. Best performance rules are used to generate PRN sequence.
5. The PRN sequence is compared with the other Pseudo number generators and the best is chosen.

Authors claim that the cellular automata generated more random numbers than the linear congruential generators.

Conclusion

In the last few decades there is an increase in the application of Evolutionary computation methods to solve the problems in the field of cryptography. This may be due to the effectiveness of the evolutionary methods or due to the need for automated design in cryptography. In this conceptual paper, a brief review about cryptography and EC methods is initially provided. Then the exhaustive literature survey provides an insight knowledge about how the EC methods can be implemented to develop the modern cryptosystem to yield better result.

REFERENCES

[1] William Stallings, 'CRYPTOGRAPHY AND NETWORK SECURITY' Principles and Practices. Fourth Edition.

[2] 'Year 2010 issues on Cryptographic Algorithms'. www. imes. boj. or. jp/research/abstracts/english/06-E-08. html

[3] E. C. Laskari, G. C. Meletiou, Y. C. Stamatiou,. 'Cryptography and Cryptanalysis through Computational Intelligence' Springer 2007.
[4] S. Picek, M. Golub 'On Evolutionary Computation Methods in Cryptography', Faculty of Electrical Engineering and Computing, Zagreb, Croatia.
[5] J. Koza, 'Genetic Programming: On the Programming of Computers by Means of Natural Selection (Complex adaptive Systems),' The MIT Press, Cambridge, USA, 1992.
[6] M. Mitchell, 'An Introduction to Genetic Algorithms,' The MIT Press, Cambridge, USA, 1999.
[7] T. Weise, 'Global Optimization Algorithms Theory and Application,' 2009.
[8] A. Tragha, F. Omary, A. Mouloudi, 'Genetic Algorithms Inspired Cryptography,' A. M. S. E Association for the Advancement of Modeling & Simulation Techniques in Enterprises, Series D: Computer Science and Statistics, 2005.
[9] A. Tragha, F. Omary, A. Mouloudi, 'ICIGA: Improved Cryptography Inspired by Genetic Algorithms,' Proceedings of the International Conference on Hybrid Information Technology. (ICHIT'06), pp. 335-341, 2006.
[10] N. Nedjah and L. de Macedo Mourelle, 'Multi-Objective Evolutionary Hardware for RSA-Based Cryptosystems,' Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), vol. 2, pp. 503-507, 2004.
[11] A. J. Clark, 'Optimisation Heuristics for Cryptology,' PhD Thesis, Faculty of Information Technology, Queensland, 1998.
[12] D. Delgado, D. Vidal, and G. Hernandez, 'Evolutionary Design of Pseudorandom Sequence Generators based on Cellular Automata and Its Applicability in Current Cryptosystems,' Proceedings of the 8th Annual Conference on Genetic and Evolutionary Computation, GECCO '06, Seattle, pp. 1859-1860, 2006.