A new Genetic Crossover Operator applied to Evolutionary Cryptography

BENHAOUA K. *, **OULED JEDID L.** **, **LAGRAA N.** **, and **RAHMOUNI M.K** *

* Security of Information Systems Laboratory , Université of Oran Es-Senia (Algéria), **Université of Laghouat (Algéria)

Abstract

Crossing is an important and delicate operation of the Genetic Algorithm (GAs) : the most used techniques are 1-point and MPX which are based on the notion of traditional crossing in Genetics. In this paper, we show their limitations and we introduce a new one (called "Bestof2") inspired from modern genetics, which is able to generate the best adapted solutions in a better way and to preserve them during the search for the optimal solutio, in order to converge quickly. We choose to apply this approach to one of the cryptography algorithms based on GAs. Then, the results obtained by simulation prove the efficiency of this approach..

Key-words: *Genetic Algorithm, crossing 1-point and MPX, bestof2, cryptography*

1 Introduction

Genetic algorithms were formally introduced in the United States in the 1970s. The continuing price/performance improvements of computational systems have made them attractive for some types of optimization. They make it possible to deal with problems where the objective function does not have exploitable mathematical properties. Thus, it is about a heuristic process where the optimal result is not guaranteed, due to to the fact that its operators uses chance for guided research [1]. Their foundation are, with selection, the mutation and cross-over operators.

GAs have been applied successfully to many problems over the last 25 years, such as genetic synthesis, VLSI technology, strategy planning, machine learning, optimization problems, etc… and many new genetic operators have been presented as dedicated to solve a given problem or to implement new ideas. The design of a specialized operator often causes side effects : the more it is specialized, the more it bears a high cost in terms of execution time. The other solutions are to design a real hybrid algorithm, for example with Tabu search [2] or simulated annealing [3],

In this paper, we will focus on the cross-over operators. First, we will present the specificity of the most known operators (1-point, MPX cross-over), then we will prove their limitations in terms of convergence. [4].

To overcome this essential handicap, we will propose a new cross-over operator. Initially we will take a different approach and look upon the concepts of GAs as the organizing process in a biologically inspired generic way, in order to improve the global convergence behaviour of GAs independently of the actually used implementation [5].

A quick analysis of the most recent literature shows a tremendous increase of the number of the articles using Genetic Algorithms. This tendency can also be observed in the field of cryptology [6], this hybrid approach has given rise to a new field called Evolutionary Cryptology.

Cryptology is the umbrella term for cryptography and cryptanalysis. Cryptography is the science of conducting secure communication. Cryptanalysis is the study of recovering communications by those other than the intended receiver .

Genetic Algorithms have previously been used in cryptanalysis [7] [8] [18] for solving many problems, but recently GAs have been used in the field of cryptography. The OTL algorithm presents one of these [9].

This paper is organised as follows: In section 2, we present the main mechanisms of the genetic algorithms. In section 3 we will pay attention to the characteristics of cross-over operation, and the limitations of the known operators (1-point, MPX), before introducing our new cross-over operator "Bestof2" in section 4. In the next section, we will present the OTL algorithm. In simulation experiments section we will evaluate the performances of our cross-over operator through some experimental results, finally some concluding remarks are given .

2 Genetic Algorithms

Genetic algorithms are considered as heuristic algorithms whose goal is to obtain a suitable solution in an acceptable time, and to conceive artificial systems that have the same properties as natural systems [10].

A GAs is an iterative algorithm of search for anoptimum, it handles a population of constant size. This population is made of candidate points

called individuals.The constant size involves a phenomenon of competition between them. Each one represents the coding of a potential solution to the problem to be solved, it consists of a whole of elements called genes.

A new population will be created in each iteration with the same number of chromosomes which are the most adapted to their environment. Progressively, the chromosomes will tend towards the optimum solution. The creation of a new population is made by application of the genetic operators which are selection, crossing and mutation [11]. .
The selection of the best chromosomes is the first operation.. Crossing makes possible to generate two new chromosomes "children" starting from two selected chromosomes "parents" (figure 1), while mutation (figure 2), carries out the inversion of one or more genes of a chromosome [12]

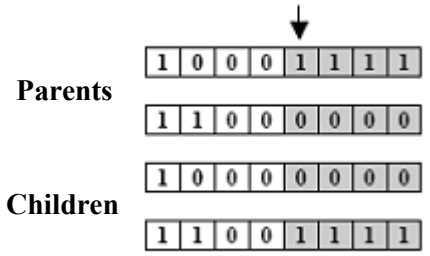

Figure 1 : Cross-over operator.

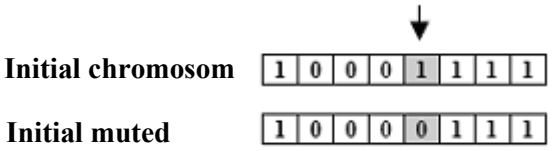

Figure 2 : Mutation Operator.

The various operations which intervene in a genetic algorithm can be shown as follow:

random generation of the initial population
Repeat

Computing of the selective function
Selection
Cross-over
Mutation

Until *satisfaction*

Figure 3 : Basic genetic algorithm.

3 The classical cross-over operators

The aim of the traditional cross-over operators (1-point and MPX) [13] [14], is to improve the performances of the population by cutting out the individuals into two or several pieces and exchanging them . Indeed, the characteristics of the children should be the fruit of a mixture of those of their parents , so that implies that the resulting children contain the bad and the best genes, this mixture can be beneficial or negative in term of fitness as shown in figures 2 and 3.

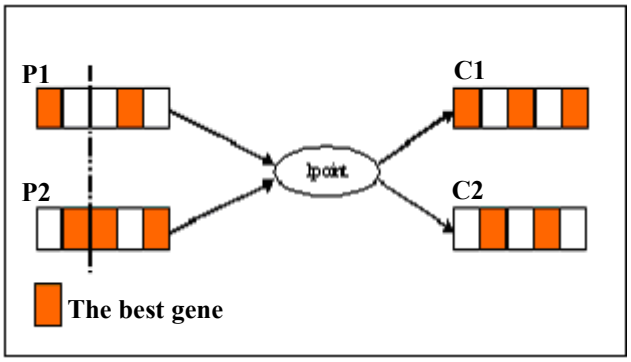

Figure 2 : 1 point cross-over

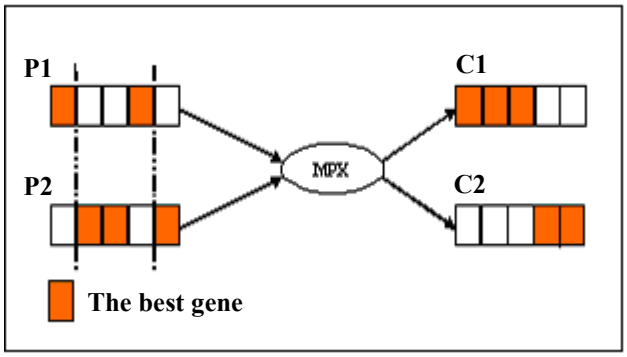

Figure 3 : MPX cross-over

In this way it is important to develop new cross-over operator whose aim is to create children who inherit the advantages of their parents only : in order to achieve that, we propose the bestof2 crossing .

4 The « Bestof2 » cross-over

In nature, all species inherits two genes for each character, one coming from the mother and the other coming from the father (figure 4).

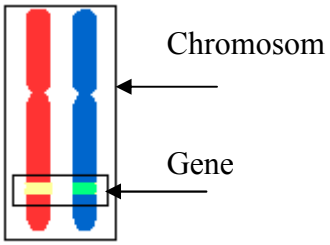

Figure 4 : Chromosom in the nature

If both genes differ, one which is the dominating gene is fully expressed in the appearance of the character , the other, the recessive gene, does not have a notable effect on its appearance, therefore there is a segregation of the two genes of each character during the formation of the characters, the same mechanism is used in "Bestof2" [15].
This idea is inspired by the concept of the first law worked out by the biologist Mendel [16]. He installs an experimental garden in the court and uses peas as experimental design aiming at explaining the laws of the origin and of the formation of the hybrids, he then shows that the characteristics of the species are given by their dominant genes to the profit (???)of the other recessive ones (figure 5):

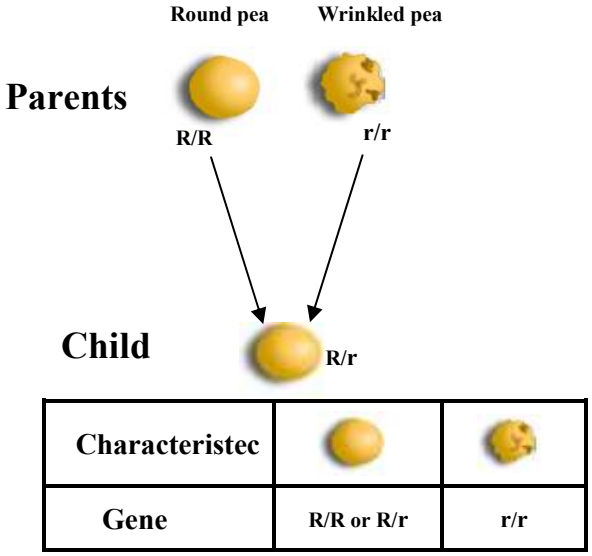

Figure 5 : the first law of mendel

The "Bestof2" crossing consists in creating a child starting from two parents, in such a way that the resulting child only contains the best genes, i.e the ith gene of the child corresponds to the best of the ith adjacent genes of parents. Therefore, we obtain an individual who inherits the best genes from his parents, it is exactly the same mechanism as in nature (figure 6).

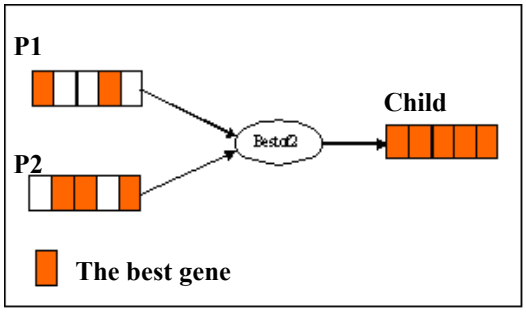

Figure 6 : Bestof2 cross-over

To do that we set up a Gene Evaluate Function (GEF) which evaluates the genes and returns the best : in the result, the GEF function has as parameter two adjacent genes, one from parent1 and the other from parent2. The choice of the function depends on the field on which optimization is carried out.

INPUT : $A=\{A_1, A_2,\ldots, A_n\}$,$B=\{A_1, A_2,\ldots,B_n\}$ two parents.
OUTPUT: $C= \{C_1, C_2,\ldots, C_n\}$ a child.
ALGORITHM:
For i = 1 **to** n **do** Ci: = GEF (Ai, Bi).

Figure 6 : The Bestof2 procedure

5 The OTL algorithm

5.1 Ciphering

Let M be the message to be ciphered . M is a succession of N characters . C is a secret key composed of p characters taken from {0,1}.The first stage is to apply an initial jamming , in order to mask the characters of M.
Let $a_1, a_2\ldots, a_l$ be the various characters of M ($l \leq N$). We indicate by Li ($1<= i <= l$) the list of the various positions of the character a_i in M before coding, and by card(Li) the number of the occurrences of a_i in M .
The message M can be represented as below:

(a_1,L_1)	(a_2,L_2)	....	(a_l,L_l)

Figure 7 : The message M coding

The goal of the algorithm is to create the maximum of disorder in the positions of the characters of a message M. To do that, we repeatedly change the distribution of the lists Li ($1 \leq i \leq l$) on the various characters of M (without modifying the contents of the lists) in such a way that the difference between the cardinal of the new list assigned to each character a_i and the cardinal of the original list L_i is maximum . We thus obtain an optimization problem which we solve by using the genetic algorithms, in particular those suited to the scheduling problems [17].

INPUT: initial-C $=\{(a_1,L_1), (a_2,L_2),..., (a_l,L_l)\}$, the intial coding of the message M.

OUTPUT: final-C $=\{(a_1,Q_1), (a_2,Q_2),..., (a_l,Q_l)\}$, the final coding .
Such that L_i is (?) the list of the original positions of the character a_i and Q_i its new positions. (???)

First we will discuss the five main components of the GAs [18] :
1.**Representation:** An individual (or chromosome) is a vector of size *l*. The genes are the lists L_{ki} ($1\leq i \leq l$).The jth L_{kj} gene contains the new positions that will take the character a_j of the intial-C.

2.**Initial population**: we create an initial population P_0 of q individuals$\{X_1, X_2\ldots,X_q\}$. We call initial-CH the initial chromosome whose genes are (with respect to order with initial-C): $L_1,L_{2,\ldots,}L_l$. We apply q good permutations to initial-CH in order to obtain q distinct individuals, thus constructing the initial population made up of q potential solutions to the problem.

3.**Evaluation:** Let X_k be an individual of p_i whose genes are : $L_{k1}, L_{k2}\ldots,L_{kl}$ .We define the evaluation function F on the whole of the X_k individuals by:

$$F(X_k) = \sum_{i=1}^{l} \left| card(L_{k_i}) - card(L_i) \right|$$

4.**Selection:** we use the traditional method of the caster [11], which allows us to retain the strongest individuals . Let us describe this process : one assigns to each individual X_i a probability of appearance $p(X_i)$, by using:

$$p(Xi) = \frac{F(X_i)}{\sum_{k=1}^{q} F(X_k)}$$

5.**Genetic operators:** during the alteration phase of the algorithm we will use the following operators:

a) crossing: we apply the crossing operation to the selected pairs
b) mutation: we apply the mutation to the individuals resulting from the crossing

From the best chromosom best-CH obtained by O.T.L we constitute the final coding of the corresponding message M final-C . This final coding produces the ciphered message M'.

5.2 Deciphering

Once the best-CH solution is given by the algorithm, we then identify the permutation which leads to initial-CH. This permutation will be used as a secret key .

6 Simulation experiments

To apply the bestof2 in the OTL program, we must choose a GEF which depends on the problem that we want to solve, so with OTL we add an other parameter to the GEF, which is a gene from the initial-CH : according to this gene, we evoluate the genes in competition and we choose a new one. The cross-over procedures are stated as follows:

Procedure Bestof2(A,B,C);
for i = 1 **to** n
C_i = GEF (A_i,B_i,L_i);
end for
end procedure;

Function GEF(a,b,l);
Result = max(|Card(a)-card(l)|,|Card(b)-card(l)|);
end function;

After simulation, we compare the "Bestof2" with the traditional operators, the following figure is a convergence chart towards the best solution by the three methods of crossing:

For this problem we have used the following GAs parameters:
a) p_c: the probability of crossing = 0.75.
b) p_m: the probability of mutation = 0.75.
c) Population size = 50 .

Bestof2
MPX
1point

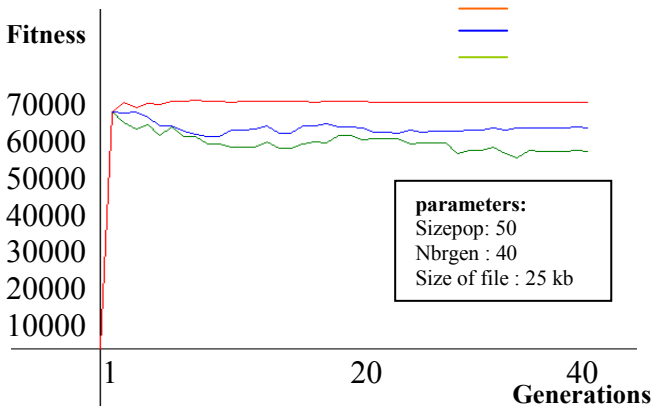

Figure 8 : convergence chart

We can asserty that the "bestof2crossing" supports a fast exploration of the research space of the problem and gives results better than that of traditional crossing. We also notice that the convergence graph is stable starting from the third generation on, so that implies that the bestof2 converges quickly towards the best solution. As a result, the bestof2 reduces the execution time of the programs using the Genetic Algorithms.

7 Conclusion

In spite of the power shown by the genetic algorithms in the solving of optimization problems, they still have some limitations. Therefore it is always necessary to think of improving them and that is why we propose in this paper a new cross-over operator, that we believe could be also effective in another field. The reason for that it is because it is inspired by nature and there is no better thing than nature. The simulation results prove that the new cross-over is faster than the classical operators.

References

[1] Jean-Baptiste Mouret, *Concepts fondamentaux des algorithmes évolutionnistes,* 15 novembre 2005

[2] P. Galinier and J.K. Hao. Hybrid evolutionary algorithms for graph coloring. *Journal of Combinatorial Optimization*, 3(4):379–397, 1999.

[3] F. T. Lin, C. Y. Kao, and C. C. Hsu. Applying the genetic approach to simulated annealing in solving some NP-hard problems. *IEEE Transactions on Systems, Man, and Cybernetics*, 23(6):1752–1767, - 1993.

[4] Blaise MADELINE : New Low Cost and Undedicated Genetic Operators, Rapport de recherche n° 4573 — September 2002.

[5] Affenzeller, M.: New Generic Hybrids Based Upon Genetic Algorithms. Institute of Systems Science Systems Theory and Information Technology Johannes Kepler University Altenbergerstrasse 69 A-4040 Linz - Austria

[6] Thomas Vallée, Murat Yildizoglu : Présentation des algorithmes génétiques et de leurs applications en économie *Décembre 2003, v. 4.2*

[7] A. J. Bagnall, G .P McKeown and V.J. Rayward Smith: The Cryptanalysis of a Three Rotor Machine Using a Genetic Algorithm, NR4 7TG

[8] Yaseen, I.F.T. Sahasrabuddhe, H.V.A genetic algorithm for the cryptanalysis of Chor-Rivest knapsackpublic key cryptosystem (PKC) , Third International Conference on Computational Intelligence and Multimedia Applications, in New Delhi, India1999. ICCIMA '99. Proceedings pp 81-85.

[9] Omary.F, Lbekkou ri.A et Tragha.A "*Extension des applications des algorithmes évolutionnistes* ". Rapport interne N° 7 / 01/ 2004 .Département de mathématiques et informatique Faculté des sciences -Rabat.

[10] Jean-Sébastien LACROIX, Stéphane TERRADE "*Algorithmes Génétiques*" MATH 6414, 17 novembre 2004.

[11] Goldberg D.E." Genetic algorithms in search optimisation & Machine Learning (Addison-Wesley. Publishing Company, Inc) 1989.

[12] M. Nasri et M. EL Hitmy**,** *Algorithme Génétique et Critère de la Trace pour l'Optimisation du Vecteur Attribut : Application à la Classification Supervisée des Images de Textures*, Ecole Supérieure de Technologie, B.P 473, OUJDA, MAROC.

[13] Mühlenbein H.,"*Evolutionary Algorithms: Theory and applications*" (Wiley) 1993.

[14] Mühlenbein H., and Schlierkamp-Voosen D. "Predictive Models for the Breeder Genetic Algorithm-I, continuous Parameter Optimization. Evolutionary computation,1(1), 25-49".1993

[15] http://www.savoirs.essonne.fr/dossiers/lepatrimoine/histoire-des sciences/article/type/0/intro/johann-gregor-mendel-la-foi-en-la-science/

[16] Jean-Louis Serre, NEPHROGÈNE N°34, Avril 2003

[17] Christophe Caux- Henri Pierreval- Marie-Claude Portmann " Les algorithmes génétiques et leur application aux problèmes d'ordonnancement "APII. Volume 29-N° 4-5/1995 pages 409 à 443.

[18] IMAD F.T. YASEEN and H.V.SAHASRABUDDHE, "A Genetic Algorithm for the cryptanalysis of Chor-

Rivest knapsack Public Key Cryptosystem(PKC)", Dept. of computer science University of Pune Pune-411 007 (India).