Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Nonlinear Analysis 63 (2005) e831 – e837
Nonlinear Analysis
www.elsevier.com/locate/na

Problems of cryptography as discrete optimization tasks

E.C. Laskari[a, b], G.C. Meletiou[c, *], M.N. Vrahatis[a, b]

[a] *Computational Intelligence Laboratory, Department of Mathematics, University of Patras, GR-26110 Patras, Greece*
[b] *University of Patras Artificial Intelligence Research Center (UPAIRC), University of Patras, GR-26110 Patras, Greece*
[c] *A.T.E.I. of Epirus, PO Box 110, GR-47100 Arta, Greece*

Abstract

In this contribution problems encountered in the field of cryptology, are introduced as discrete optimization tasks. Two evolutionary computation algorithms, namely the particle swarm optimization method and the differential evolution method, are applied to handle these problems. The results indicate that the dynamic of this type of discrete optimization problems makes it difficult for the methods to retain information.

Keywords: Evolutionary computation; Particle swarm optimization; Differential evolution; Cryptanalysis; Factorization; Discrete optimization

1. Introduction

The field of cryptography has motivated a number of hard and complex computational problems. Such problems are the integer factorization problem related to the RSA cryptosystem; the index computation or the discrete logarithm problem related to the El Gamal cryptosystem, as well as, to the Diffie–Hellman key exchange and others [2,3,9,10]. The assumption that these problems are in general computationally intractable in polynomial time forms the basis of the reliability of most contemporary cryptosystems.

* Corresponding author.
E-mail address: gmelet@teiep.gr (G.C. Meletiou).

0362-546X/$ - see front matter
doi:10.1016/j.na.2005.03.003

In this paper, a number of problems originating from the integer factorization problem are formulated as discrete optimization tasks. The integer factorization problem forms the basis of the RSA cryptosystem. Thus, optimization methods that can efficiently tackle the problems under consideration in acceptable computational time, could be regarded as a useful tool for cryptanalysis of the corresponding type of cryptosystems.

Evolutionary computation algorithms are stochastic optimization methods inspired by either natural evolution or social behavior. Genetic algorithms (GA) [4], evolution strategies (ES) [11], the differential evolution algorithm (DE) [12], as well as, the particle swarm optimization (PSO) [1,5] belong to this class of methods. All the aforementioned optimization algorithms are designed to address problems involving discontinuous and multimodal objective functions, the existence of numerous local minima, constrained optimizations tasks, and disjoint search spaces [4,5,11]. Optimization techniques for real search spaces can be applied to discrete optimization problems with minor modifications. A straightforward approach is to round off the optimum solution to the nearest integer [6,8].

Two evolutionary computation algorithms, namely the particle swarm optimization method and the differential evolution algorithm, are applied to tackle several instances of the proposed optimization problems. The performance of both these methods is compared with simple random search.

The rest of this contribution is organized as follows. The definition of the problems along with the transformations to discrete optimization tasks, are given in Section 2. In Section 3, experimental setup of the considered methods and results are reported. Conclusions are given in Section 4.

2. Problem formulation

The first problem under consideration is defined as follows: given a composite integer N, find pairs of $x, y \in \mathbb{Z}_N^*$, such that $x^2 \equiv y^2 \pmod N$, with $x \not\equiv \pm y \pmod N$. This problem is equivalent to finding non-trivial factors of N, as N divides $x^2 - y^2 = (x-y)(x+y)$, but N does not divide either $x - y$ or $x + y$. Hence the $\gcd(x-y, N)$ is a non-trivial factor of N (random square factorization algorithm) [7].

The prescribed problem can be formulated as a discrete optimization task by defining the minimization function $f : \{1, \ldots, N-1\} \times \{1, \ldots, N-1\} \mapsto \{0, \ldots, N-1\}$, with

$$f(x, y) = x^2 - y^2 \pmod N,$$

subject to the constraints $x \neq \pm y \pmod N$. The constraint $x = -y$ can be incorporated to the problem by changing the domain of the function. Thus, the problem reduces to minimizing the function $g : \{2, 3, \ldots, (N-1)/2\} \times \{2, 3, \ldots, (N-1)/2\} \mapsto \{0, \ldots, (N-1)\}$, with

$$g(x, y) = x^2 - y^2 \pmod N,$$

subject to the constraint $x \not\equiv y \pmod N$. The minimization problem is two-dimensional and the global minimum of the function g is zero. A plot of the function $f(x, y)$ for $N = 5 * 7 = 35$ is given in Fig. 1(a) and the contour plot for the value $f(x, y) = 0$ is given in Fig. 1(b).

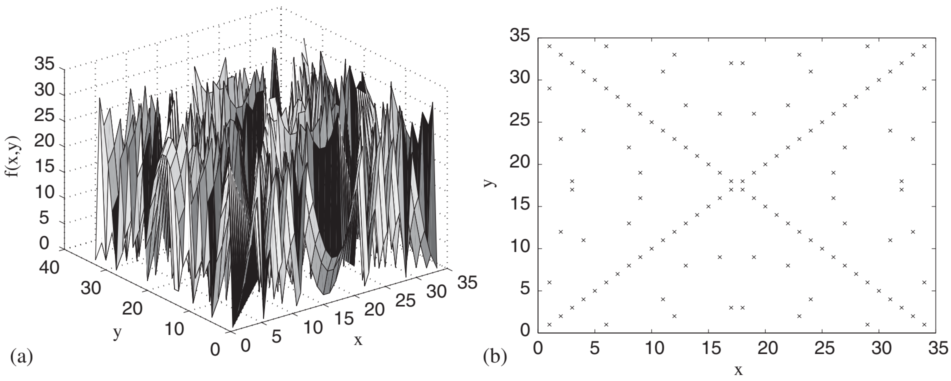

Fig. 1. (a) Plot of function $f(x, y) = x^2 - y^2 \pmod N$, for $N = 35$ (left), and (b) contour plot of function $f(x, y) = x^2 - y^2 \pmod N$, for $N = 35$ at value 0 (right).

Similar problems that can be studied are the following:

Minimize the function $h : \{1, \ldots, N-1\} \mapsto \{0, \ldots, N-1\}$, with

$$h(x) = (x-a)(x-b) \pmod N,$$

where a, b non-zero integers and $x \not\equiv a \pmod N$, $x \not\equiv b \pmod N$. As an example of this problem, we have considered the minimization of the function $h_e(x) = (x-1)(x-2)$, where $x \not\equiv 1 \pmod N$ and $x \not\equiv 2 \pmod N$. In a more general form one can consider the minimization of the function

$$w(x) = (x-a)(x-b)\cdots(x-m) \pmod N,$$

where $x \in \{0, \ldots, N-1\}$ and $x \not\equiv \{a, b, \ldots, m\} \pmod N$. As an example of this problem, we have studied the function $w_e(x) = (x+1)(x-1)(x-2) \pmod N$, with $x \not\equiv \{-1, 1, 2\} \pmod N$.

3. Experimental setup and results

The PSO [1] and DE [12] methods, were applied on the considered problems along with the random search technique. The global and local PSO variants of both the inertia weight and the constriction factor versions, as well as the *DE*/*rand*/1/*bin* and *DE*/*best*/2/*bin* variants of the DE algorithm, have been used. For both the PSO variants typical parameter values were used, while the size of the neighborhood for the local variant of the PSO was taken equal to 1. Preliminary experiments indicated that the value of maximum velocity $V_{\max}$ of the PSO's particles affects its performance significantly. The value $V_{\max} = \lfloor(\text{UpBound} - \text{LoBound})/5\rfloor$, where UpBound denotes the upper bound of the function's domain and LoBound the lower bound of the function's domain, produced the most promising results and therefore it was adopted in all the experiments. For the DE algorithm, the parameters were set at the values $F = 0.5$ and $CR = 0.5$. All populations were constrained in the feasible region of the corresponding problem.

Table 1
Results for the minimization of function g

N	Method	Suc. rate (%)	Mean FE	SD FE	Median FE	Min FE
$N = 199 * 211$	PSOGW	56	8844.643	5992.515	8325.000	660
	PSOGC	48	7149.375	5272.590	5355.000	330
	PSOLW	51	8329.412	6223.142	7050.000	270
	PSOLC	51	7160.588	6001.276	5940.000	420
	DE1	4	517.500	115.866	465.000	450
	DE2	9	5476.667	6455.651	1830.000	60
	RS	66	9104.015	5862.358	8700.500	22
$N = 293 * 307$	PSOGW	41	16210.244	11193.375	15090.000	120
	PSOGC	45	16818.667	12664.632	13800.000	630
	PSOLW	58	18455.690	12870.897	14520.000	270
	PSOLC	50	16374.000	13597.782	13365.000	120
	DE1	7	1598.571	1115.488	1470.000	120
	DE2	19	17815.263	12484.580	16290.000	2730
	RS	64	21548.531	13926.751	20852.500	57
$N = 397 * 401$	PSOGW	53	31965.849	24423.975	27570.000	780
	PSOGC	45	32532.667	22652.983	33210.000	1740
	PSOLW	55	31472.182	23394.791	22620.000	720
	PSOLC	54	38156.111	22925.970	37665.000	750
	DE1	1	1680.000	0.000	1680.000	1680
	DE2	12	27722.500	17498.736	28620.000	180
	RS	60	27302.567	21307.031	23607.500	145
$N = 499 * 503$	PSOGW	56	49893.750	37515.327	44640.000	930
	PSOGC	55	49975.636	36727.380	41760.000	300
	PSOLW	55	49207.091	34053.904	50430.000	2010
	PSOLC	46	48443.478	34677.039	43470.000	1920
	DE1	1	2480.000	0.000	2480.000	2480
	DE2	8	67245.000	35114.316	64770.000	14730
	RS	61	54139.443	38642.970	48743.000	140
$N = 599 * 601$	PSOGW	52	72175.000	48653.823	71550.000	600
	PSOGC	51	81476.471	53666.543	75100.000	5000
	PSOLW	49	78651.020	48197.105	67400.000	11200
	PSOLC	52	69542.308	48837.949	53050.000	2500
	DE1	2	4700.000	4808.326	4700.000	1300
	DE2	5	8620.000	8078.180	9300.000	800
	RS	64	86123.656	47504.284	89392.500	904
$N = 691 * 701$	PSOGW	46	207443.478	163585.340	214800.000	800
	PSOGC	46	175426.086	138118.794	149200.000	800
	PSOLW	60	196993.334	146204.518	144500.000	9200

Table 1 (*continued*)

N	Method	Suc. rate (%)	Mean FE	SD FE	Median FE	Min FE
	PSOLC	52	209307.692	163833.606	200100.000	1800
	DE1	2	23800.000	25000.000	23800.000	21000
	DE2	10	71000.000	95357.642	15200.000	1600
	RS	60	185932.334	126355.926	154999.000	2828

Table 2
Results for the minimization of the functions h_e and w_e, for $N = 103 * 107$

Function	Method	Suc. rate (%)	Mean FE	SD FE	Median FE	Min FE
h_e	PSOGW	51	2013.333	1483.535	1500.000	100
	PSOGC	57	1974.035	1609.228	1420.000	60
	PSOLW	59	1677.288	1254.688	1420.000	60
	PSOLC	58	2385.862	1676.898	2040.000	120
	DE1	1	100.000	0.000	100.000	100
	DE2	1	80.000	0.000	80.000	80
	RS	65	2099.646	1448.007	2056.000	6
w_e	PSOGW	79	1382.785	1265.927	820.000	40
	PSOGC	84	1402.857	1442.194	930.000	40
	PSOLW	80	1757.750	1544.267	1110.000	40
	PSOLC	85	1416.000	1329.034	880.000	40
	DE1	1	60.000	0.000	60.000	60
	DE2	1	80.000	0.000	80.000	80
	RS	96	1507.969	1328.913	1104.000	7

For the minimization of the function g, the performance of the methods was investigated for several instances of N, from the value $N = 199 * 211 = 41,989$ up to $N = 691 * 701 = 484,391$. For each N considered, 100 independent runs were performed and the corresponding results are exhibited in Table 1. Concerning the notation used in the Table, PSOGW corresponds to the global variant of PSO method with inertia weight; PSOGC is the global variant of PSO with constriction factor; PSOLW is PSO's local variant with inertia weight; PSOLC is PSO's local variant with constriction factor, DE1 corresponds to the $DE/rand/1/bin$ and DE2 to the $DE/best/2/bin$ variants of DE method. Random search results are denoted as RS. A run is considered to be successful if the algorithm identifies the global minimizer within a prespecified number of function evaluations. The function evaluations threshold was taken equal to the cardinal of integers in the domain of the function studied. The success rates of each algorithm, that is the proportion of the times it achieved the global minimizer within the prespecified threshold, the minimum number, the median, the mean value and the standard deviation of function evaluations (FE) needed for success, are reported.

The results indicate that the variants of PSO method outperform the variants of the DE method over these instances and with this parameter setup. Moreover, the performance of the DE method decreases as the value of N increases in contrast to PSO which appears to be more stable with respect to this parameter. However, in contrast to the known behavior of the evolutionary computation methods, the random search technique outperforms both these methods and their variants. This fact suggests that the almost random behavior of the specific kind of problems makes it quite difficult for the methods to retain knowledge about their dynamics. Similar results were reported on the minimization of the functions h_e and w_e. For $N = 103 * 107$ the results are reported in Table 2.

4. Conclusions

In this paper, a number of problems originating from the integer factorization problem are introduced as discrete optimization tasks. Since the integer factorization problem forms the basis of many contemporary cryptosystems, optimization methods that can efficiently and effectively tackle the considered problems, could constitute a useful tool for the cryptanalysis of the corresponding cryptosystems.

Two evolutionary computation algorithms, namely the particle swarm optimization method and the differential evolution method, are applied to handle these problems. Their results, compared with the random search technique, indicate that this special kind of discrete optimization problems seem to have a dynamic that makes it difficult for the methods to retain information.

Acknowledgements

The authors would like to thank the reviewers for their concern. Moreover, they acknowledge the partial support by the "Archimedes" research programme awarded by the Greek Ministry of Education and Religious Affairs and the European Union.

References

[1] M. Clerc, J. Kennedy, The particle swarm—explosion, stability, and convergence in a multidimensional complex space, IEEE Trans. Evol. Comput. 6 (1) (2002) 58–73.
[2] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory IT-22 (6) (1976) 644–654.
[3] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory 31 (4) (1985) 469–472.
[4] D.B. Fogel, Evolutionary Computation: Towards a New Philosophy of Machine Intelligence, IEEE Press, Piscataway, NJ, 1995.
[5] J. Kennedy, R.C. Eberhart, Swarm Intelligence, Morgan Kaufmann, Los Altos, CA, 2001.
[6] E.C. Laskari, K.E. Parsopoulos, M.N. Vrahatis, Particle swarm optimization for integer programming, in: Proceedings of the IEEE 2002 Congress on Evolutionary Computation, IEEE Press, New York, Hawaii, HI, 2002, pp. 1576–1581.
[7] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1996.

[8] S.S. Rao, Engineering Optimization—Theory and Practice, Wiley Eastern, New Delhi, 1996.
[9] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Comm. ACM 21 (1978) 120–126.
[10] B. Schneier, Applied Cryptography, second ed., Wiley, New York, 1996.
[11] H.-P. Schwefel, Evolution and Optimum Seeking, Wiley, New York, 1995.
[12] R. Storn, K. Price, Differential evolution—a simple and efficient heuristic for global optimization over continuous spaces, J. Global Optim. 11 (1997) 341–359.