Investigation of the Rate-and-State Equation for Different Critical Stresses by Grassberger-Procaccia Method

S. Turuntaev[1,2,3], A. Kamay[1,2]

[1]Moscow Institute of Physics and Technology (State University)
[2]All-Russian Research Institute of Automatics
[3]Institute of Geosphere Dynamics of Russian Academy of Sciences (IDG RAS)
E-mail: s.turuntaev@gmail.com , alesia.kamay@gmail.com

Abstract: A problem of seismicity variation due to human action is considered. The widely used "stick-slip" model of the seismic regime with "rate-and-state" friction law was adopted for description of a sliding along tectonic faults. The main distinctions of used approach from the common one [Hobbs, 1990, Erickson, Birnir, Lavallèe, 2008] are the followings: we consider two-parameters type of the friction law and vary the value of critical shear stress in the rate-and-state equation in suggestion that this is the value varied by human impact (by mining, fluid injection and production, hydraulic fracturing and so on). Calculations were done for the critical stress varied from 5MPa up to 50 MPa with increment 5 MPa. For each value of the critical stress, the time series of the displacement along the fault, its rate and change of shear stress were constructed. Obtained results were analyzed with the help of Grassberger-Procaccia method of correlation integral calculation for different embedding space dimensions. It was found that if the critical stress increase, the system behavior changes significantly. Oscillations of the fault sliding become inharmonic, and when the critical stress reach 45 MPa, the oscillations become quasi-chaotic. An estimation of the obtained attractor dimensions by Grassberger-Procaccia method showed, that an increase of the critical stresses results in increase of the attractor correlation dimensionality: τ^*=5MPa – 1.4; τ^*=15MPa – 1.6; τ^* = 30 MPa - 2.2; τ^*=45MPa – 2.5. It was found, that if the critical stress continue to increase, the correlation dimension would stop to increase. A comparison of obtained results with real induced seismicity data analysis showed that in real case the correlation dimensionality is higher. This distinguish can be explained by taking into account the presence of the seismic events, which are not related with human influence and which can be considered as a stochastic background. An addition of random component with signal/noise ratio 2 to the model data resulted in increase of the model correlation dimensionality to 4-5, which is in good correspondence with induced seismicity data.
Keywords: rate-and-state equation, two-parameter friction law, Grassberger and Procaccia method, correlation integral, seismic regime, induced seismicity.

1. Introduction.

Despite the fact that rate-and-state model of friction was proposed in the second half of the previous century, the interest to it has increased in recent years. The reason for that is success in physics of nonlinear phenomena, in particular, in the area of chaotic systems. Rate-and-state model was recognized as quite appropriate basis for developing these ideas and modeling relevant geophysical

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

systems. Currently, it is believed that this model describes the seismic process most adequately.

In 60s, Brace and Byerlee proposed to consider unstable frictional sliding along faults as a model of earthquakes [Brace, Byerlee, 1966]. The model included a suggestion that cohesion existing in some parts of the fault prevents free slipping along it and leads to an accumulation of shear stress to a critical level, after which the slip and earthquake occur.

Peculiarities of the friction forces dependence on the duration of the stationary state of the contact and on the speed of the motion along the fault was examined by Dieterich [Dieterich, 1978]. Gu [Gu et al., 1984] experimentally investigated various modes of frictional movements and determined empirical constants whose values are used in many modern variants of rate-and-state equation.

The origin of the unstable sliding and its dynamics were studied by [Ohnaka et al., 1986]. The work was focused on the study of mechanism of the transition to instability.

The "rate-and-state" equation was considered by [Hobbs, 1990] by means of nonlinear dynamics methods. Change of friction was studied as a function of displacement and velocity at a variation of the stiffness coefficient in the rate-and-state equation. The similar approach was implemented in [Erickson et al., 2008], where the authors examined an appearance of chaotic solutions in the one-parameter velocity-dependent friction law.

Turuntaev, Vorohobina, Melchaeva, [2012] showed that the technogenic impact on undeground leads to an increase in the "regularity" of the seismic regime. To explain the increase in the seismic regime regularity, a model of fault motion defined by the two-parameter velocity dependent friction law was considered.

In the presented paper, we consider two-parameters type of the friction law and vary the value of critical shear stress in the rate-and-state equation in suggestion that this is the value varied by human impact (by mining, fluid injection and production, hydraulic fracturing and so on). The obtained solutions of the rate-and-state equation are analyzed by means of Grassberger-Procaccia method [Grassberger, Procaccia, 1983].

2. The model description

Abstracting from internal structure and genesis of the faults, it can be expected that the fault sliding will be governed by the friction law of one type or another, and that change of the sliding state due to anthropogenic impacts will be resulted in the growth of regularity of the seismic process.

Measurements of tectonic fault motions show that the motions look like a combination of slow sliding (so-called creep) and fast moves, which accompanied by tremors (earthquakes). This type of the motion can be described with the help of the model proposed by Burridge & Knopov, which looks like a system of blocks, elastically connected with each other (Fig. 1 - top view and Fig. 2 - general view of the model). Each block moves under net action of elastic forces from adjacent blocks and frictional force from the stationary substrate. To simplify the model it can be assumed that all the blocks

have the same mass, the same area of contact with the surface and that elastic links between blocks have the same modulus.
Let's consider the "rate-and-state" motion equation with a two-parameter friction law and let's assume that the technological impact of any nature reduces the critical shear stress (for example, by increasing the pore pressure by fluid injection or by action of vibrations, etc.).

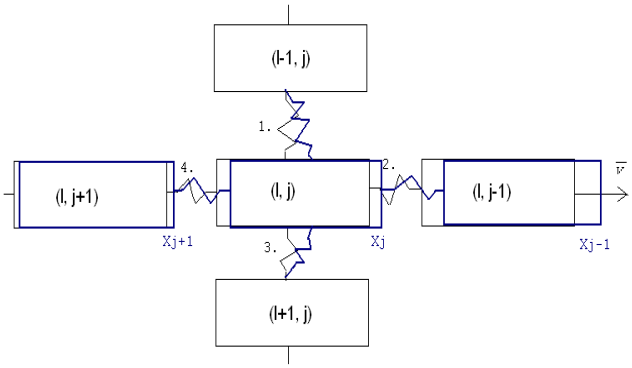


Fig. 1. The model of tectonic blocks (top view).

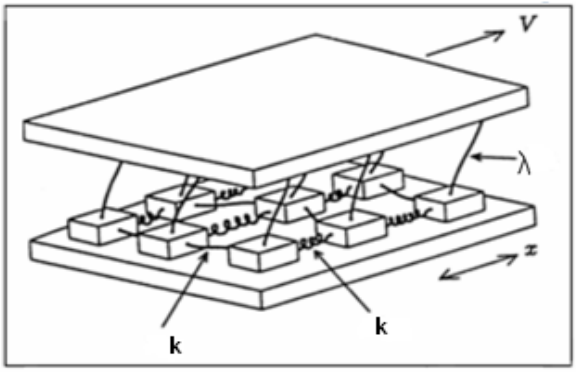


Fig. 2. The model of active tectonic faults by Burridge - Knopov (B- K) (general view).

The equation of motion for the single-chain of blocks can be written as follows:

$$m\ddot{x}_j = k(\upsilon_0 t - x_{j-1} + 2x_j - x_{j+1}) - \tau_j s \qquad (1)$$

where the first term defines the elastic forces from adjacent blocks, the second one is the fault friction: k – stiffness of the elastic links between blocks, υ -

speed at infinity, τ - shear stress occurs as a result of friction. In this paper we consider the two-parameter friction law in the form proposed by [Hobbs, 1990]:

$$\tau = \tau* + A\, ln(v/v*) + \theta_1 + \theta_2 \qquad (2)$$

where $v*$ - constant velocity of the crustal block relative motion, $\tau*$ - critical stress, which can be changed by external influences and can be written as

$$\tau* = C + \mu(\sigma - p) \qquad (3)$$

where C - cohesion coefficient, μ - coefficient of friction, p - pore pressure, σ- normal stress; θ_i - state variable, which characterizes the state of the sliding surfaces, and which evolution over time is determined by the equation:

$$\dot{\theta}_i = -\frac{v}{L_i}\,[\theta_i + B_i ln(v/v*)] \qquad (4)$$

here L_i - characteristic dimensions of the roughness of sliding surfaces, $i = \overline{1,2}$. Values for the constants $v*$, A, B_i, $\tau*$, L_i were taken from experiments [Gu et al., 1984].

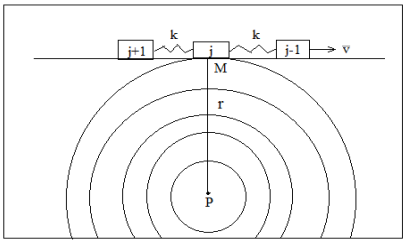


Fig.3. Changes of critical stress on the j-th block boundary at the point M due to change of pore pressure at the point P.

Figure 3 illustrates the way in which one of the parameters of equation (3) can be changed. Let's suppose that the pressure is increased at point P. At some moment of time t_{cr} the pressure will change in the point M. It follows from (3) that the increase in the pore pressure will reduce the critical stress $\tau*(0) > \tau*(t_{cr})$, and consequently it will reduce the value of the frictional force at which the j-th block begins to move.

According to the motion equation (1), it can cause the block "jump", and as a result, the redistribution of elastic forces in the links between blocks. The whole system can come into motion in the result of a change even in one of the parameters. The resulting motion is complex. In [Turuntaev, Vorokhobina, Malcheva, 2012] it was shown that for the analysis of such motions, it's reasonable to use the methods developed for the analysis of nonlinear dynamic systems.

3. Results

Numerical simulation of the block movements was carried out under the critical stress $\tau *$ varied from 5 MPa to 50 MPa with increments 5 MPa. For each value of $\tau *$, time series of the block displacements, its velocity and shear stress at the block base were calculated. Complexity of the obtained time series were analyzed using algorithm for estimating the correlation dimension, based on the calculation of the correlation integral by Grassberger and Procaccia method [Grassberger, Procaccia, 1983].

Finite-difference scheme used to solve the equation of motion (1) was following

$$\frac{x_{i+1}-2\cdot x_i+x_{i-1}}{h^2} = \frac{k}{m}\cdot\left(\frac{x_i-x_{i-1}}{h}\cdot(ih)-x_i\right)-\frac{\tau_i}{s} \qquad (5)$$

with initial conditions $x(0) = 0, v(0) = 0$.

The values of the parameters *k*, *m*, *s* were taken from [Hobbs, 1990].

To solve the equation we used the method of direct and reverse run with the following values of the preliminary factors

$$\begin{gathered} A = a(y_{i-1,j}, y_{i,j})\cdot\frac{h}{h_x^2} \\ B = a\,(y_{i,j}, y_{i+1,j})\cdot\frac{h}{h_x^2} \\ C = \left(a(y_{i-1,j}, y_{i,j}) + a\,(y_{i,j}, y_{i+1,j})\right)\cdot\frac{h}{h_x^2}+1 \\ F = y_{i,j} \end{gathered} \qquad (6)$$

which were included in the calculation of the coefficients α_i, β_i in final formulas

$$\begin{gathered} \alpha_i = \frac{B}{C - A\cdot\alpha_{i-1}} \\ \beta_i = \frac{A\cdot\beta_{i-1}+F}{C-A\cdot\alpha_{i-1}} \\ y_{i,j} = \alpha_i\cdot y_{i+1,j+1}+\beta_i \end{gathered} \qquad (7)$$

The values of the time step h, spatial grid h_x and the correction coefficients of approximation in the formulas (5) - (7) were the followings:

$$\begin{gathered} h_x = 0.01 \\ h = 0.01 \\ \delta = 0.01 \\ \alpha = 0.5\cdot\gamma\cdot\delta^2\cdot y_{i-1,j}^{\gamma-1}+y_{i,j}^{\gamma-1} \end{gathered} \qquad (8)$$

The selected values of the coefficients give approximation error at the level of $O(h, h_x^2)$, that is enough accuracy for considered problem.

The graphs of displacements and shear stresses for three values of the critical stress τ^* : 5 MPa, 20 MPa, 50 MPa are shown in Fig.4-6.

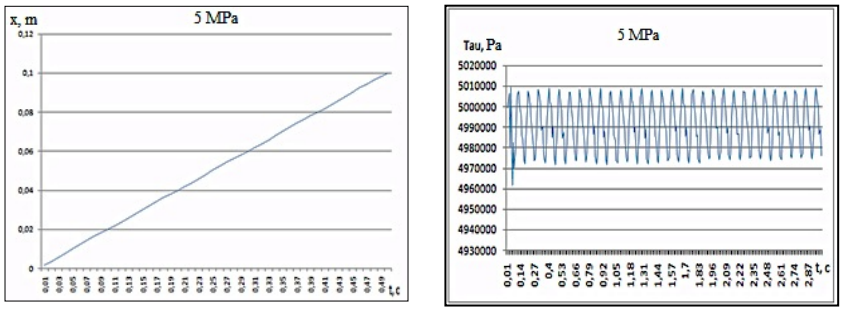


Fig. 4. Dependencies of displacement on time (left panel) and shear stress on time (right panel) at the critical stress equal to 5 MPa.

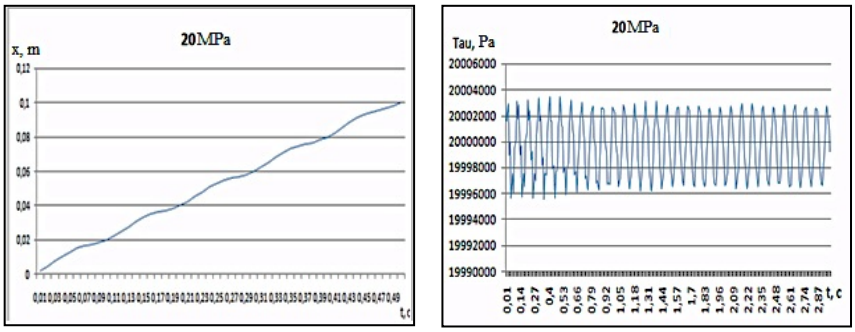


Fig. 5. Dependencies of displacement on time (left panel) and shear stress on time (right panel) at the critical stress equal to 20 MPa.

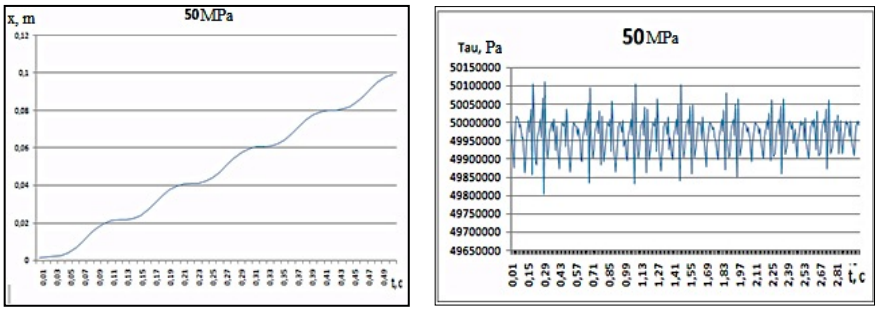


Fig. 6. Dependencies of displacement on time (left panel) and shear stress on time (right panel) at the critical stress equal to 50 MPa.

The graphs of the block motion respectively to constant velocity at infinity v^* are shown in Fig. 7.

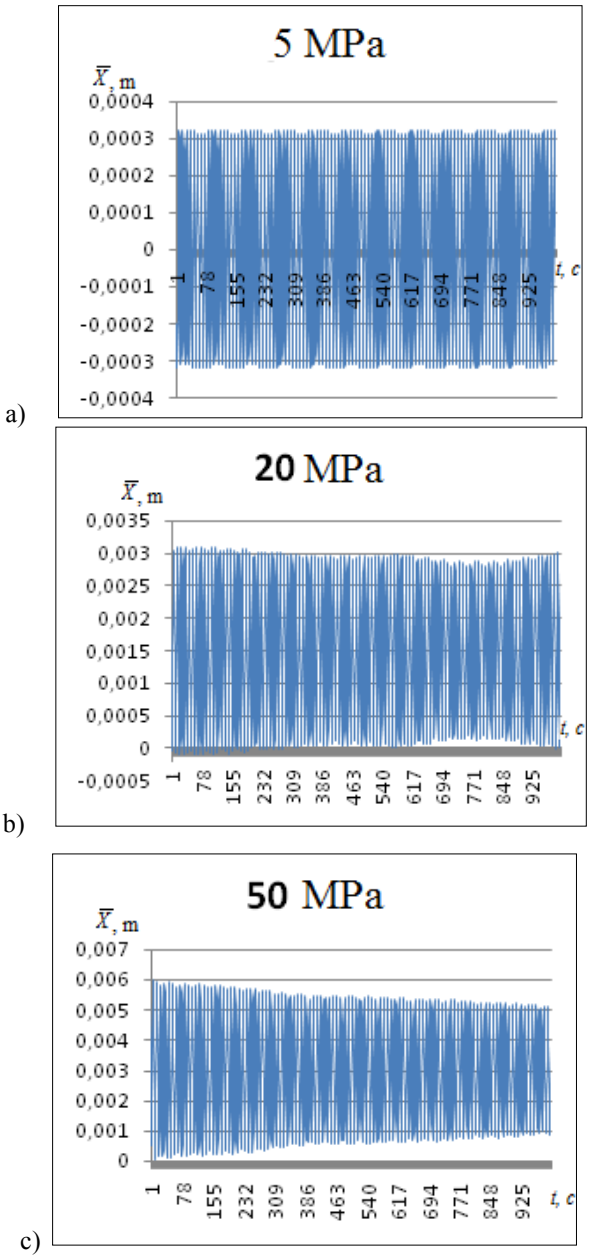


Fig . 7. Dependencies of displacements on time, calculated for the critical values of τ * = 5 MPa , τ * = 20 MPa, and τ * = 50 MPa.

Results of numerical calculations for several values of critical stresses are shown in Fig.8 as phase trajectories in x-v-τ coordinates. The values are normalized to the characteristic size L_1, v^* u $\tau^* = 5$ $МПа$ for the values of the critical stress at 5 MPa, 20 MPa and 50 MPa (Fig. 8a, 8b and 8c, respectively).
An estimation of the obtained attractor dimensions by Grassberger-Procaccia method showed, that an increase of the critical stresses results in increase of the attractor correlation dimensionality: τ*=5MPa – 1.4; τ*=15MPa – 1.6; τ* = 30MPa - 2.2; τ*=45MPa – 2.5. (Fig. 9).

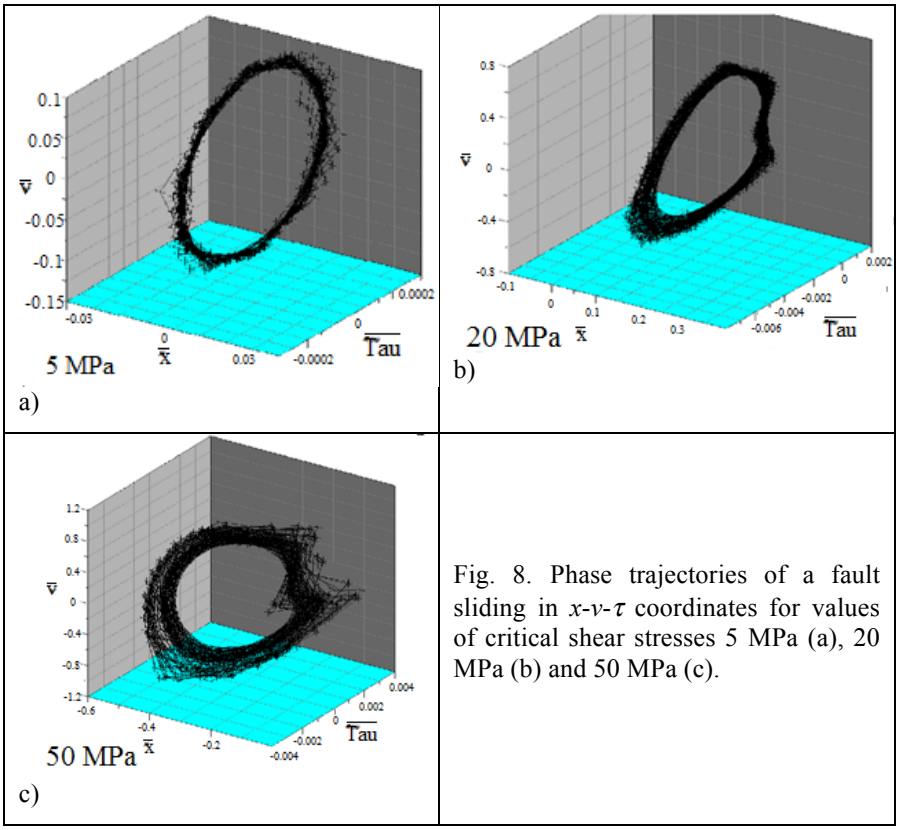


Fig. 8. Phase trajectories of a fault sliding in x-v-τ coordinates for values of critical shear stresses 5 MPa (a), 20 MPa (b) and 50 MPa (c).

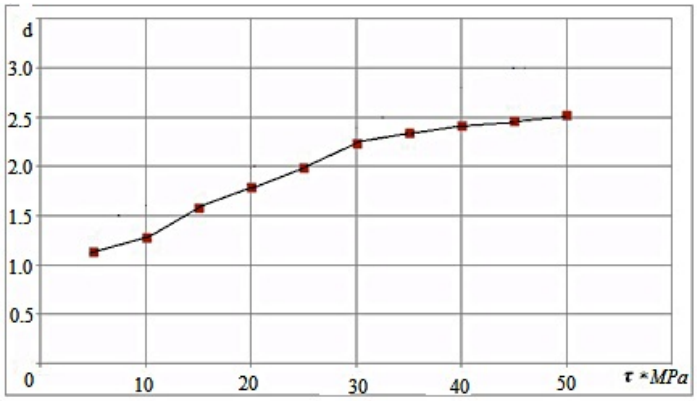


Fig. 9. The dependence of the correlation dimension on the critical stress.

4. Discussion and conclusions

Numerical analysis of the rate-and-state equation with two-parameter friction law showed significant changes in the stick-slip motion when the critical shear stress varied.

Evaluation of the correlation dimension and the embedding space dimension by Grasbergera - Procaccia method for obtained time series has shown that both of these variables have small values. Change of critical stress from 5 MPa to 50 MPa resulted in variation of correlation dimension and embedded space dimension from 1.1 to 2.5 and from 3 to 5, respectively.

In the range of the critical stress 5 MPa to 30 MPa the correlation dimension increases linearly with critical stress increase; at higher values of the critical stress there is a tendency of saturation of the correlation dimension dependence on the critical stress.

Values of dimensions obtained in the model calculations may differ from the values, which were obtained in the analysis of real seismicity (for example, in the area of the Bishkek geodynamic test site [Turuntaev, Vorohobina, Melchaeva, 2012]). We can assume that this difference is caused by significantly higher complexity of real seismic processes in comparison with the model one. This distinguish can be explained by taking into account the presence of the seismic events, which are not related with human influence and which can be considered as a stochastic background. An addition of random component with signal/noise ratio 2 to the model data resulted in increase of the model correlation dimensionality to 4-5, which is in good correspondence with induced seismicity data.

The existence of stable states in the equation solution allows us to specify the problem of seismic activity forecast and of seismic regime control technologies. According to the equation (3), the effect on the movement of the crustal blocks can be performed by changing coefficient of friction and fluid pore pressure. The aim of further research is to study the minimal values that can change the state of a system of interconnected blocks. We plan to investigate the solutions of the equations of motion (1) with more real characteristics of the physical

environment than obtained in laboratory (the characteristic parameters of the contacting surfaces, the velocity of relative motion of the fault, stiffness, cohesion, etc.).

At the present stage of the research one can conclude that an increase of the critical stresses in rate-and-state equation results in increase of the attractor correlation dimensionality: τ^*=5MPa – 1.4; τ^*=15MPa – 1.6; τ^* = 30 MPa - 2.2; τ^*=45MPa – 2.5. It was found, that if the critical stress continue to increase, the correlation dimension would stop to increase.

References

1. Brace W.F., Byerlee J.D. Stick-slip as mechanism for earthquakes. *Science.* 1966. V. 153. № 3739. P. 990-992.

2. Dieterich J.H. Earthquake nucleation on faults with rate and state-dependet friction. *Tectonophysics.* 1992. V. 211. P. 115-134.

3. Erickson B., Birnir B., Lavalle D. A model for aperiodicity in earthquakes. *Nonlinear Processes in Geophysics*. 2008.

4. Grassberger P., Procaccia I. Measuring the strangeness of strange attractors. *Physica. North-Holland Publishing Company.* 1983. V. 9D. P. 189-208.

5. Gu J. C., Rice J.R., Ruina A.L., Tse S.T. Slip motion and instability of a single degree of freedom elastic system with rate-and-state dependent friction. *J. Mech. Phys. Solids.* 1984. V. 32. P. 167-196.

6. Hobbs B.E. Chaotic behavior of frictional shear instabilities. *Rockbursts and Seismicity in Mines / Fairhurst (ed.).* 1990. Balkema, Rotterdam. P. 87-91.

7. Turuntaev S.B., Vorohobina S.V., Melchaeva O.Y. Identification of anthropogenic changes of seismic regime using methods of nonlinear dynamics. *Physics of the Earth*. 2012. № 3. P. 52-65.

CHAOTIC AND TURBULENT SUPERGRANULATION

PANIVENI UDAYASHANKAR[1,2,3]
[1] IUCAA, Pune, India, [2] NIEIT, Mysore, India, [3]IIA, Bangalore, India
E-mail: paniveni.udayashankar@gmail.com

Abstract: While it is generally understood that supergranulation is a solar convective phenomenon, a detailed model can be quite complicated because of the interplay of magnetic and velocity fields and turbulence. The chaotic and turbulent aspect of the solar supergranulation can be studied by examining the interrelationships amongst the parameters characterizing supergranular cells namely size, horizontal flow field, lifetime and physical dimensions of the cells and the fractal dimension deduced from the size data. The findings are supportive of Kolmogorov's theory of turbulence.

Keywords: Sun : granulation Sun : supergranulation Sun: Turbulence

1.Introduction

Observation of the Solar photosphere through high resolution instruments have long indicated that the surface of the Sun is not a tranquil, featureless surface but is beset with a granular appearance. These cellular velocity patterns are a visible manifestation of sub-photospheric convection currents which contribute substantially to the outward transport of energy from the deeper layers, thus maintaining the energy balance of the Sun as a whole.

Convection is the chief mode of transport in the outer layers of all cool stars such as the Sun (Noyes,1982). Convection zone of thickness 30% of the Solar radius lies in the sub-photospheric layers of the Sun. Here the opacity is so large that heat flux transport is mainly by convection rather than by photon diffusion. Convection is revealed prominently on two scales. On a scale of 1000 km it is granulation and on a scale 30-40 arc sec it is Supergranules. 'Supergranules' are caused by the turbulence that extends deep into the convection zone. They have a lifetime of about 24 hour with spicules marking their boundaries. Gas rises in the centre of the supergranules and then spreads out towards the boundary and descends.

There is evidence of vertical velocities at the centre and at the

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

boundaries of the individual cells. The horizontal flow is typically in the range 0.3-0.4 km/s fed by central upwelling and vertical downward motions concentrated towards the cell boundaries are typically in the range 0.1-0.2 km/s. By virtue of geometric projection, such outflowing regions always show velocity of approach to the observer along the line-of -sight on the side of the cell closer to the centre of the disc and velocity of recession on the side closer to the limb. Near the centre of the disc, where the horizontal outflows are transverse to the line-of – sight , there is less Doppler shift and hence the image is almost uniformly grey. Broadly speaking supergranules are characterized by the three parameters namely the length L, the lifetime T and the horizontal flow velocity v_h . The interrelationships amongst these parameters can shed light on the underlying convective processes.

Using an initial sample of 90 supergranular cells, a study was undertaken in order to investigate a possible relation between the sizes and peak horizontal velocities of the cells. For the sample obtained, the two parameters are found to be correlated with a

relation $v_h \alpha L^{1/3}$. This is in agreement with the Kolmogorov theory of turbulence as applied to large scale solar convection (Krishan et.al ,2002).

In a follow-up work, a study of 50 supergranular cells was undertaken in order to investigate the relationship between the lifetime (T) and the horizontal flow velocity v_h of the cells. For the sample we find that the two parameters are correlated with relation

$v_h \alpha T^{0.5}$ and T is identified with the eddy turn-over time. This is in agreement with the turbulent convective model of the solar atmosphere where the velocity spectrum of the supergranular field given by the relation

$v_h \alpha L^{1/3}$ can be identified with the Kolmogorov spectrum, with the eddy size L (Paniveni et al. 2004).

A study of an increased sample of 200 supergranular cells was undertaken in order to investigate their fractal structure. For this

sample we find a broad, slightly asymmetric dispersion in the distribution of supergranular sizes with a most probable size around 31.9 Mm. The area A and perimeter P of the supergranular cells are well correlated with a relation $P \alpha A^{D/2}$ from which a fractal dimension D for supergranulation of about 1.25 is obtained. This is consistent with that for isobars and suggests a possible turbulent origin of supergranulation. By relating this to the variances of kinetic energy, temperature and pressure, it is concluded that the supergranular network is close to being isobaric and that it has a possible turbulent origin (Paniveni et al. 2005 and Paniveni et al. 2010).

2. Source of Data and Data Processing

In this analysis we have analysed intensitygrams obtained during the 23rd Solar cycle at the solar observatory, Kodaikanal.
The Intensitygram data have been obtained with a resolution of 2 arcsec, which is twice the granular scale. Fractal dimension attributed to a feature must be qualified by the resolution at which it is derived.

Well accentuated cells of the Intensity data lying between 15 degree and 60 degree angular distance from the disc centre were selected. This choice of the region discounts error due to projection effects.

Depending on the region in which it is found, it is called 'quiescent' or 'active'. Regions that were not unequivocally quiescent or active were avoided for simplicity.

An example of region and cell selection is depicted in fig(1)

The profile of a visually identified cell was scanned as follows:

We chose a fiducial y-direction on the cell and performed intensity profile scans for Intensitygrams along the x-direction for

all pixel positions on the y-axis. In each scan, the cell extent is taken to be marked by two juxtaposed 'crests' separated by a trough expected in the Intensitygrams as examined in fig(2).This set of data points was used to determine the area and perimeter of a given cell and of the spectrum for all selected supergranules. The area – perimeter relation is used to evaluate the fractal dimension. The main results pertaining to fractal dimension is derived from Fig (3,4,5) and Fig (6,7,8) and they show no multifractal structure and the entire distribution profile is explained by a single physical phenomenon.

A fractal analysis is relevant to such irregularly shaped features because we can quantify the supergranular irregularity and shed light on the nature of solar turbulence.

Active Region

The log A versus log P relation is linear as shown in the Figure (3) for the active region at the ascending phase. A correlation co-efficient of 0.8 indicates a strong correlation. Fractal dimension calculated as 2/slope is found to be D = 1.325 +/- 0.282.

The log A versus log P relation is linear as shown in the Figure (4) for the active region at the peak. A correlation co-efficient of 0.94 indicates a strong correlation. Fractal dimension calculated as 2/slope is found to be D = 1.12 +/- 0.07.

The log A versus log P relation is linear as shown in the Figure (5) for the active region at the descending phase. A correlation co-efficient of 0.87 indicates a strong correlation. Fractal dimension calculated as 2/slope is found to be

D = 1.431 +/- 0.212

Quiet Region

The log A versus log P relation is linear as shown in the Figure (6) for the quiet region during the ascending phase

A correlation co-efficient of 0.9 indicates a strong correlation. Fractal dimension calculated as 2/slope is found to be

D = 1.616 +/- 0.221

The log A versus log P relation is linear as shown in the Figure (7) for the quiet region during the peak. A correlation co-efficient

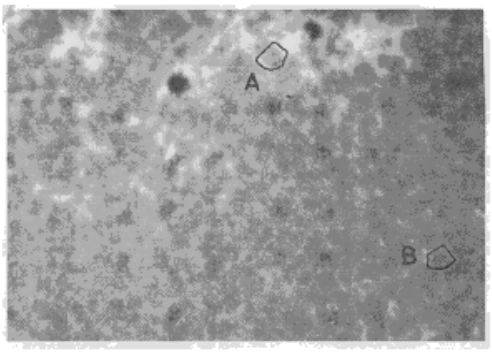
of 0.88 indicates a strong correlation. Fractal dimension calculated as 2/slope is found to be D = 1.25 +/- 0.14

The log A versus log P relation is linear as shown in the Figure (8) for the quiet region during the descending phase. A correlation co-efficient of 0.78 indicates a strong correlation. Fractal dimension calculated as 2/slope is found to be D = 1.075 +/- 0.284

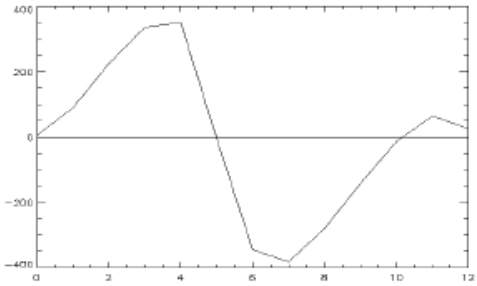
The pressure variance $\langle p^2 \rangle$ is proportional to the square of the velocity variance i.e. $\langle p^2 \rangle \alpha r^{4/3}$ (Batchelor 1953). The fractal dimension of an isobar is therefore found to be Dp = 2 - (1/2×4/3) = 1.33. Our data furnishes evidence that the fractal nature of the supergranular network is close to being isobaric than isothermal.

It is interesting that Roudier and Muller (1986) obtained a similar dimension for smaller granules. Unlike in granules, our plots show that a single linear fit is suitable for the entire observed range of supergranules.

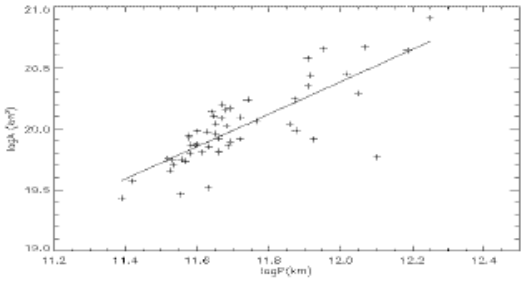
Zoomed-in View of Supergranular cells in the active(A) and quiet region(B)



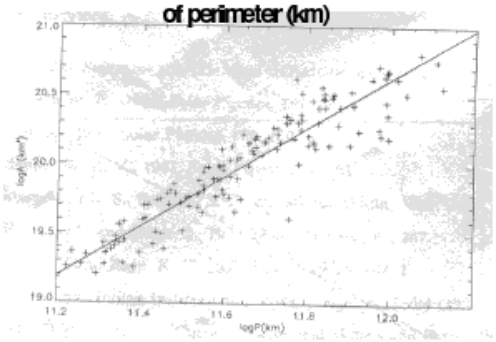
Intensity Profile: A measure of magnitude of intensity on the y-axis against cell extent x in pixels on the x-axis



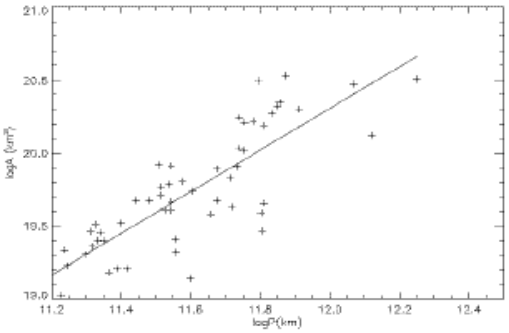
Active Region : Ascending Phase



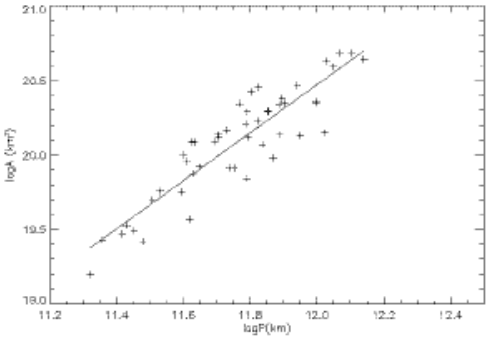
Active Region Peak: Plot of the natural logarithm of the supergranular area (in sq.km) against the natural logarithm of perimeter (km)



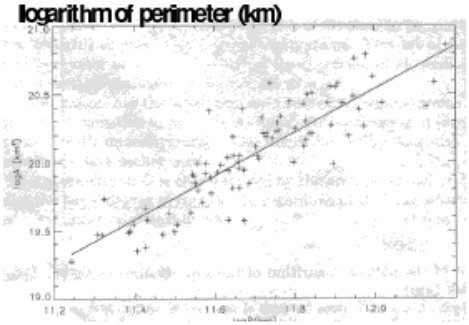
Active Region: Descending Phase



Quiet Region: Ascending phase



Quiet Region Peak: Plot of natural logarithm of the Super granular area (in sq.km) against the natural logarithm of perimeter (km)



Quiet Region : Descending phase

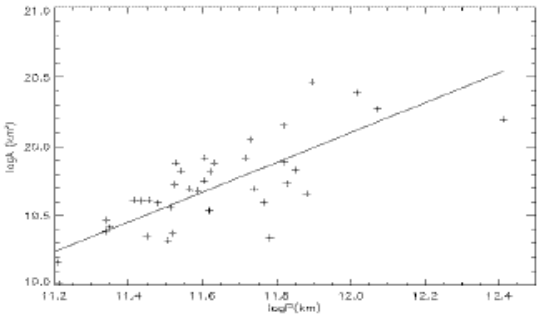


Fig.1, Fig.2, Fig.3, Fig.4, Fig.5,Fig.6,Fig.7 and Fig.8 from left hand top corner to bottom hand right corner is depicted in the fig.above.

3. Conclusions

The spectral distribution of the temperature, a passive scalar, is related to the spectral distribution of kinetic energy. It can be easily shown that the Kolmogorov energy spectrum, $K^{-5/3}$, both in two and three dimensional turbulence leads to a temperature spectrum of $K^{-5/3}$. Thus the temperature variance $<\theta^2>$ varies as $r^{2/3}$ as a function of the distance r (Tennekes and Lumley 1970). According to Mandelbrot (1975), an isosurface has a fractal dimension given by D_I = (Euclidean dimension) – ½ (exponent of the variance). Thus $D_T = 2 - (1/2 \times 2/3) = 5/3 = 1.66$ for an isotherm.

The pressure variance $<p^2>$, on the other hand, is proportional to the square of the velocity variance i.e. $<p^2> \alpha\ r^{4/3}$ (Batchelor 1953). The fractal dimension of an isobar is therefore found to be $Dp = 2 - (1/2 \times 4/3) = 1.33$. Our data furnishes evidence that the fractal nature of the supergranular network is close to being isobaric than isothermal.

It is known that strong magnetic fields have an inhibiting effect on large scale flows, but a causal connection linking restricted velocity flows in the presence of magnetic fields to smaller fractal dimension is not obvious.

References

1) Batchelor G.K., *The theory of Homogeneous Turbulence* (Cambridge University Press 1953)

2) Noyes, R.W., *The Sun, Our Star* (Harvard University Press, 1982)

3) Krishan, V., Paniveni U., Singh , J., Srikanth R., 2002, MNRAS, 334/1, 230

4) Krishan, V., 1991, MNRAS, 250-253

5) Krishan, V., 1996, Bull.Astron.,Soc.India, 24,285
6) Leighton, R.B., Noyes, R.W., Simon, G.W., 1962, ApJ., 135, 474
7) Paniveni , U., Krishan, V., Singh, J., Srikanth, R., 2004, MNRAS, 347, 1279-1281
8) Paniveni , U., Krishan, V., Singh, J., Srikanth, R., 2005, Solar Physics, 231, 1-10
9) Paniveni , U., Krishan, V., Singh, J., Srikanth, R., 2010, MNRAS, 402, Issue 1, 424-428
10) Roudier,Th. , Muller, R., 1986, Sol. Phys., 107,11
11) Tennekkes, H , Lumley, J.L*., A first course in Turbulence*, (MIT Press 1970)

Integrated Emergency Management and Risks for Mass Casualty Emergencies

Alexander Valyaev[1], Gurgen Aleksanyan[2] and Alexey Valyaev[3]

[1] Nuclear Safety Institute of Russian Academy of Sciences, Moscow, Russia
(E-mail: anvalyaev@mail.ru)
[2] Yerevan State University, Yerevan, Republic of Armenia,
(E-mail: gurgenal@ysu.am)
[3] The University of Sydney, Australia, NSW 2049
(E-mail: alexei.valiaev@gmail.com)

Abstract. Today it is observed the intense growth of various global wide scale threats to civilization, such as natural and manmade catastrophes, ecological imbalance, global climate change, numerous hazards pollutions of large territories and directed terrorist attacks, resulted to huge damages and mass casualty emergencies. The humankind has faced the majority of treats at the first time. Therefore, there are no analogues and means to be used for their solving. It stimulates modernization of traditional methods and development of new ones for its researching, prediction and prevention with maximum possible decreasing of their negative consequences. The global issue of safety provision for the humankind is the most actual and requires an immediate decision. Catastrophe risks have increased so much, that it becomes evident, that none of the states is able to manage them independently. Join efforts of all world community are necessary for the substantial development of our civilization. Main obstacles for this realization are under discussion. The authors of this article have their own experience and methods in this direction. Wide scale global catastrophes have not any boundaries. Any political and economical frictions between some states are not the reasons for the implementation of the struggle against them. The total emergency recommendations and actions have to be improved to eliminate and software of negative disaster's responses on population and environment. We present some our examples of realization with using of own Integrated Emergency Management and using of special methods and techniques in the most critical situations, that have taken place in different countries in 21 century.
Keywords: risks, emergency management, natural and manmade catastrophes

1. Introduction

Sense and purpose of any management of any object include the providing of its normal stable exploitation. But the constant variation of environment and manmade factors greatly complicate object's management especially in extreme situations such as under negative responses of manmade and natural catastrophes and accidents, including different terrorist attacks.

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

Now there is not the universal method and methodology for risk and damages assessments for many similar objects. It is necessary to develop individual approaches and methods for every concrete situation with taken into account main possible natural and manmade accidents in researched region. Only some total principles, presented in the end of this article we may recommend. That is why the demonstration of risks and damage assessments and its connection with corresponded Emergency Management for Mass Casualty Emergencies is presented here for different real accidents. Then the comparison of some approaches and methods will be given in details with our own experience in this thematic. That is why our many references and own publications, connected with this article theme, include the vast information for its using in different cases [1-28]

2. Main Results

The first international thematic experience, closely connected with risk problem and its management, A.N. Valyaev has obtained during his participation in the Joint Venture between Pegasus Gold Company, USA; Kilborn Engineering Pacific LTD, Canada; KazGold, Australia and Government of Kazakhstan Republic in 1994 year during the work in North America. Our global task was the building of the special plant in the East – Kazakhstan region (see Fig.1) on extraction of silver, gold, platinum and others metals from the huge tailing storage of non- ferrous metals, named as Chashinskoe, This building was located near the Kazakhstan Ridder town and another populated localities with agricultural industry and some rivers, high Altai mountains and forests. The modern extraction technology, included the wide application of poison cyanides reagents, were used. That is why it was necessary to provide the serious ecological safety for population and environment with the exact fulfilling of the determined demands for normal exploitation of many risk objects. It was happy case for application of the rich existence thematic experience on the building and exploitation of similar objects in North America. Our international work group had to take into account the main natural treats and manmade dangers. At that time we had not any special regional risks map, that may help us. for this regions. Only about 10 years later we had such maps for Armenia, Georgia, Azerbaijan, Kazakhstan and some Russian regional maps and applied them in our future investigations. Such maps, part of them have been obtained with the using of space technology, are presented in our thematic articles [1-19]. This article presents some results, obtained in our International Projects. Valyaev A.N. is the leader of our International Program on Risks Program, that based on the separate projects developed by 6 scientific groups from the countries in the former Soviet Union - Russia, Armenia, Georgia, Azerbaijan, Kazakhstan and Kyrgyzstan.

In 1994 these maps were absent for the East Kazakhstan region, that was very risk territory under the response by constant varied natural and manmade impacts. In 250 km from here was the Test Nuclear Semipalatinsk Poligon, where about 500 underground and surface nuclear explosions have been made

for the long time1949 - 1989 years. It was necessary to provide many serious demands for the existence risk water objects The largest Kazakhstan Irtysh river is located in this region with numerous confluent rivers. Ulba river (see Fig.1) flows in 10 km from this plant building. This region belong to Altai Mountains with Belukha highest tip in Siberia of 4506 m height over sea level. East Kazakhstan is the area of major ecological risk, where multiple mines for extracting metals and minerals, as well as a number of industrial enterprises and their tailing dumps, including uranium, are located in the cities and their suburbs along Irtysh, It originates in China, further flows via the lands of Kazakhstan and Russia, including such large cities as East-Kazakhstan capital Ust-Kamenogorsk, Semipalatinsk, Pavlodar, Omsk, and Tobolsk, and after its confluence with the Ob River it flows into the Arctic Ocean The largest Bukhtarma HES with the 100 m height of dam has the sizeable reservoir, the basin length of which is above 300 km and the depth - up to 100 m. The other Ust-Kamenogorsk HES with the 42 m height of dam and a sole hatch is located in 15 km from the city –see Fig.1

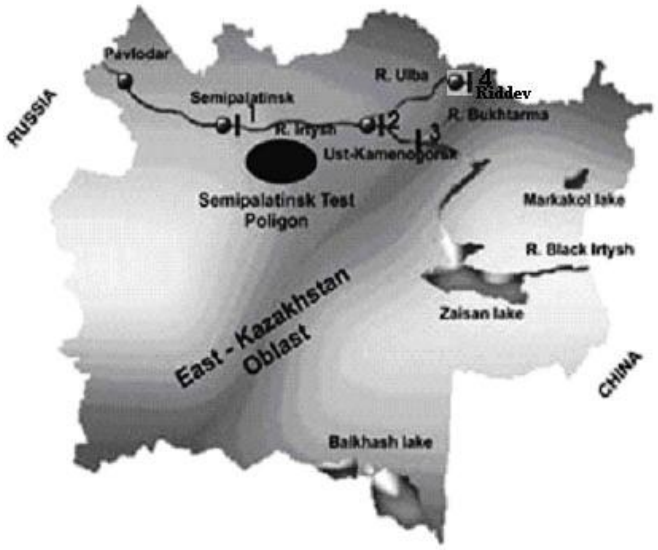


Fig. 1. The scheme of Irtysh river flow on the territory of Kazakhstan Republic. 1 – Shulba HES, 2 - Ust-Kamenogorsk HES, 3 - Bukhtarma HES, 4- Ridder town with near located Chasinskoe tailing storage.

The next Shulba HES is located in 180 km from Ust-Kamenogorsk. Errors in the design of these HESs have caused a number of different accidents. Unfortunately, the data on observations of the HESs accident's statistic are practically absent today. The Ust-Kamenogorsk city with 330 thousand inhabitants is one of the most contaminated towns in the world and located in Irtysh mountain valley. It represents the unique urban system, oversaturated by

different enterprises. The largest in FSU Ulba Metallurgical Plant (UMP) incorporates three separate works, producing enriched U for nuclear power plants, Be, Ta and their products. Operating UMP wastes storage, located in city center, has accumulated ~100 thousand tons of wastes, contained U, Th and their decay products. Its size is 400* 220 m^2 with the depth of contamination > 5 m. The level of gamma–radiation at its surface reaches 360 □R/h and increases with depth up to 1000 □R/h. The radioactive anomaly regions with 1000 up to 6000R/h are registered at UMP territory. Many other operating city large plants, such as Lead –Zinc, Titan-Magnezium, Ceramic, worked on Be base, plants power capacitors plant, nonmetalliferous group of enterprises and Silk Cloth enterprise, use in their technologies the different poisonous and toxins, while their wastes are also located in city boundaries. For instance, Lead –Zinc plant stores in open cast dumpnation on 17.5 hectares area > 13 million ton of wastes and ~1 thousand tons of arsenic in the form of highly toxic substances calcium arsenate and arsenit, where 7-10% As is contained. In Irtysh river basin, where > 40% of HES energy in Kazakhstan is worked out, large active non-ferrous pits, precious and rare-earths metals pits with their dumpnations are also located. In water of Ulba river, flowing into Irtysh in the city, toxins concentration is: Cu (4.86-5.50) maximum permitted concentration (MPC), Zn 4.71-5.37MPC, oil products 2.03-2.07 MPC, nitrite nitrogen 1.40-1.95 MPC.

Risks of ecologic catastrophes are increased, because the noticed two HES are placed at Irtysh upriver of the city (Fig.1). The huge water masses in the man-made seas press strongly on the bottom of mountain surfaces disturb and deform their initial natural states. We consider these factors resulted to the increasing of the frequency and intensity of the strong earthquakes, included catastrophic ones, that already happened not only near the city (in 1990), but also in Altai mountains in Russia (in 2003, 2005 years). Such earthquakes may cause the damages of HES dams, where in addition part of them are in non satisfactory states, especially Ust-Kamenogorsk HES dam, operated >50 years. Also any HES with its huge water reservoir are very attractive for the possible controlled terrorist acts, including with using of explosive. According to some primary estimates, in result the huge break-through damming wave with its front height ~30 m will destroy the city and its environs. All enterprises, their products and hazard impurities in the storages then will be carried out down Irtysh to many cities and after Irtysh - Ob rivers junction spread over the large territories, including Arctic Ocean through Kara Sea.

Irtysh basin accumulated 120 million m^3 of different wastes, which is 60% of the total pollution of Kazakhstan whole water basin. It results to abrupt worsening of water quality in all cities: Ust-Kamenogorsk, Semipalatinsk, Pavlodar, Omsk, Tobolsk and in many inhabited localities. Irtysh-Karaganda man-made channel supplies water to Kazakhstan central regions, such as Karaganda, Kazakhstan capital Astana cities and their oblasts. Irtysh pollution presents the serious danger as a potential source of World Ocean contamination through Arctic Ocean.

Now we present some elements of the risk management, that have been used for this region. This management is included the main following moments:

1. Prediction of main different risk events
2. The calculation of the total possible limited damages.
3. The development of measures, directed to preventing and softening of risk damages.

The problems of prediction will be describe later. Our method of calculation is the following. We consider the common case of any object exploration for the fixed time interval under the following assumptions: (1) at initial state the object is in normal (non accidents) exploitation; (2) the different kinds of accidents may be occurred as noticed i =2, 3, …, m, where m is the total number of possible accidents (m=1 is corresponded to the normal regime); (3) every accident may create the different kinds of losses. Assume that j is the kind of loss with $a_{j.}$ value. Then j = 1,2, …n, where n is the total number of possible kinds of losses; (4) realization of i accident creates the loss of j kind with P_{ij} probability, thus the matrix of loss probabilities is determined. Then the total vector of limited losses $\vec{a}_{\lim}$ may be determined on next formula:

$$\vec{a}_{\lim} = P(1)\vec{a}_{1n} + \sum_{i=2}^{m} \hat{P}_{ij}\vec{a}_j \qquad (1)$$

where P(1) is the probability of loss formation under normal exploitation; $\vec{a}_{1n}$ is the vector of limited loss under regular exploitation. $P_{ij}a_j$ coordinate vector value in sum is equal the loss value of j kind under realization of i kind accident. Under absent of accidents the second term in the right part of (1) is equal zero and then $\vec{a}_{\lim}$ total vector of limited loss is determined the first part of (1):

$$\vec{a}_{\lim} n = P(1)\vec{a}_{1n} \qquad (2)$$

The main problem in this calculation is in the determination of loss probability matrix. As one of the possible methods we propose to use the method of expertise estimates. More detail information we obtained with the using of our special risk models.

The plan of calculations of the total losses for this region includes the following. At first for every object we have to point out and develop the classification of main possible accidents. For example, in the case of HES disaster we have to take into account the next possible kinds of accidents:

1. Total damage or break of one or some HES dams
2. Partial damage of HES dam
3. Destruction of water lock
4. Stopping of HES turbines

Let us consider the most dangerous first accident, investigate the extreme cases of developing the worst catastrophes and analyze the possible scenario of their realization connected with damage of two HES, located upriver of Irtysh near Ust-Kamenogorsk sity (Fig. 3)

(a) Bukhtarma hydro electric stations (HES);

(b) Ust-Kamenogorsk HES;

(c) Both HES simultaneously;

Here we have to take into account that the total damage of Bukhtarma HES dam with the height ~ 100m will probably stimulate the total damage of Ust-Kamenogorsk HES with the height ~ 40m. Then it is necessary to evaluate the parameters of catastrophic submergence on every scenario:

(a)- maximum possible height and speed of break-through wave;

(b)- estimated time of wave crest coming and front of wave crest onto town territory;

(c) boundaries of possible submergence zone in the vicinity;

(d) maximum depth of submergence for every definite locality ant time of its submergence.

(e) to point out all main objects that will be overdammed.

For these estimates and calculations we shall use the computer modeling with taking into account the real profiles of local earth's crust and mountains valley (including its rock and soil materials), HES with its and another water reservoirs, such as lakes and rivers, others natural objects.

In the case of the possible HES disaster near U- tailing storages) our analysis will include the following:

(1) to analyze the possible scenes of realization of situations on pollutant migration from tailing storage:

(a) constant pollutant migration without damage of tailing storage dams;

(b) similar migration with the partial damage of tailing storage dams, for example, under landslide or earth flow;

(c) pollutant migration under complete damages of dams, for example in result of earthquake;

(d) pollutant migration in result of:

(1) partial flowage;

(2) total one;

Under realization of last two scenes it is possible two following cases of development of catastrophic situation:

(1) all tailings are washed off with river during few days;

(2) all tailings are washed off with river instantly.

The last situation is the most extreme and dangerous, because it will cause the maximum pollution with maximum losses both for environment and population.

For all cases it is necessary to take into account the following kinds of possible losses:

(1) caused by people victims and harmed to population health;

(2) caused by pollution of wide scale territories with subsequent losses in forest, agricultural and fish industries;

(3) from the strong pollution of buildings and constructions;

(4) resulted from the pollutant migration in basins of the largest rivers.

Under risk evaluations it is necessary to take into account the possible chemical nuclear reactions and transformations of pollutants in soil, water and air. For example, transport calculation will be done for decay chain 238U>234U>230Th>226Ra.

In common case risk management includes the following:

(1) Selection for each country a site for which the risk of occurrence of one or several catastrophes is maximum and where the damage is the greatest;
(2) Development of scenarios for implementing possible catastrophes for the site selected;
(3) Estimation of risks and possible ecological and economic damages at varied scenarios of catastrophe development;
(4) Suggestion of some recommendations on risk reduction and actions to eliminate the effects of accidents/catastrophes.

We may notice the next important moment for risk management. In many cases it is easy to assess the probability of natural catastrophes than manmade ones on the following reasons. If it is existence the good monitoring of observed territory during many years with registration of main characteristics then it allows to predict appearance of different events/ For example in seismic dangerous territories it will be earthquakes,

In [16-19] we have analyzed in detail Processes under outbursts of mountain lakes and proposed the physical and mathematic models for risk assessment. It allows to take into account the main elements for management of mountain water objects. The analysis of our complex formula for probability of outburst of concrete mountain lake allowed to organize some possible preventing measures to avoid natural catastrophes and accidents. These results were the scientific base for develop of our ISTC Project : "Assessing and decreasing risks of damages, caused by Tien–Shan mountain lakes outbursts". http://www.istc.ru/istc/db/projects.nsf/All/DFBF107592E1AA85C32574C900285DB5?OpenDocument Its realization will promote to stable development of Euro-Asia Continent.

Another our thematic investigations on risk management were connected with another following serious problem In many countries of the world for the water supply in cities and settlements implemented large borehole water intakes, and as a result in these regions occur significant reductions in groundwater levels. In karst regions these activate land subsidence and other dangerous environmental effects.

Karst as a dangerous engineering-geological process is especially disastrous for civil, industrial and hydrotechnical constructions. The article is discussing the results of engineering-geological, hydrogeological and geophysical complex investigations that were carried out in the northern part of Syria: in the territory of Ras Al Ayn City. Karst processes have been activated last few years in this territory mainly because of human activities. A number of target maps are drawn for case study area including zoning map of the karst risk: according to that map the city territory is divided into 3 parcels. Necessary engineering measures are proposed for ecological remediation of the studied area.

The activation of technogenic karsts inside of the city and surrounding territories resulted on to a decrease in stability of operating structures. As a result, from a number of houses was deported population and town planners have to refuse some building projects as well. Especially important should be considered practical test of the design method developed by us for forecasting of possible activation of karst phenomena. The proposed method of prognosis is

recommended to use in other countries with similar physical-geological conditions.

Here we present the application of our special risk model for electric energy, production at nuclear power plants (NPP) [21,22]. NPP production results to generation of radionuclide's gas-aerosol atmospheric discharges (RGAD) and liquid radioactive discharges (LRD) into NPP surface heat sinks with the additional pollution of. It is necessary to provide the exclusive safety measures, in particularly provide the levels of irradiation doses for population (PID) will be not exceeded the 10 Micro Sievert. 17 new atomic power units will be put in exploration at 7 homeland now operated NPP. We have collected and analyzed RGAD and LRD for all 10 Russian NPP during 1995 -2007. The observed stable annual tendency of RGAD and LRD decreasing has created the well ground scientific base for prediction of their levels of each NPP according to our own special developed methodology. These levels have been used for PID calculations on the special certified model "Kassandra" and "Nostradamus' information-simulation systems, developed in our Institute, for assessment of irradiation dose of human organism through all possible ways and chains: water, breath, food (meat, milk, fish, vegetables, fruits) and others under the response of the following varied natural climate temporal space random factors: wind, its velocity and directions, snow, rains, temperature and humanity, really registered at each NPP region. For most critical population group "fishers" we used such assumptions and predictions that PID obtained assessments were the maximum (conservative) ones. "Kassandra" model was used for radionuclide's transport and assessment of their concentrations in water, bottom sediments and flood plains of rivers and heat sinks, connected with real NPP. Simulation of radionuclide's migration was used with taking into account of mass their exchange between main stream and underflow for river contamination model under the persistent radioactive discharges during long time. "Nostradamus' system was developed for the effective forecasts of radioactive situation with atmospheric radionuclide's emission. Results of PID assessment is presented in Table 1.

Table 1. Predicted of irradiation doses for population in zone of Russian reconstructed NPP observation

Nuclear power plant (NPP)	Effective dose of irradiation for water consumption, Micro Sievert	Effective dose of irradiation for air way, Micro Sievert	Effective dose for all possible ways of irradiation, Micro Sievert
Kursk NPP	6,69	0.19	6.88
Kola NPP	7,8	0.014	7.814
Kalinin NPP	3,4	0.012	3.412
Volgodonsk NPP	3,99	0.0026	3.9926
Leningrad NPP	0,62	0.24	0.86
Novovoronezh NPP	0,828	0.023	0.851

Smolensk NPP	5,14	0.1	5.24

These PID values provide the permitted risk level less than 10^{-6} in year and are less in 2-3 orders of the local natural radioactive back ground. Our proposed method and methodology have the universal character and may be used for decision of some thematic problem of atomic energy.

Any large concentration of population is the possible and potential places, where manmade catastrophes an accidents may be happened. It is very difficult to realize the need monitoring here. For example, every day huge amount of population in large cities use metro as speed underground subway. Metro construction and its exploration are very risk objects, where is possible mass casualty emergencies, including terrorism attracts with using of explosives. The most accidents in Moscow metro are the following. In 1982 the escalator with passengers was has been broken with fall down acceleration at "Aviamotornaya" station. 8 victims and 30 men have been resulted. In 1990 bridge copestone collapsed with appearance of 8 heavy ~ 100 kg fragments. It was happy case that victims were absent. In 1991the metro car broke into flames in the tunnel between Semenovskaya and Partizanskaya stations. Passengers were locked in dark tunnel and then have been saved. In 1994 two metro trains came into collision in tunnel near Nagornaya station. More tha 2,5 thousands of people have been locked in the dark tunnel/ 18 persons have been sent into hospital. 3 losers were after another collision of two trains at Petrovsko- Razumovskaya station in 1994. In 2003 wheel pair took off from train car in dark tunnel. near. Passengers went by feet to the Novokuznetskaya station. In 2006 the part of tunnel has been crushed near Sokol station in result of the large tunnel roof perforation by workers , who drive piles on the building surface. In result Two piles fell down on the train. In 2008 in tunnel near Vladykino station 4 last train cars left the rails and 8 persons have been suffered. About 100 passengers have been evacuated from the tunnel near Orekhovo station in result of the fire in service technical room in 2011.In 2013 the manmade short circuit of high –voltage cable caused the fire without electro energy ffeding of few trains. About 4500 passengers were evacuated and 27 of them were hospitalized.

July 15, 2014 the largest Moscow metro accident took place about 200 passengers were injured and 23 people were killed after train derailed between Park Pobedy and Slavyansky Boulevard" The main reason was the following . The works have not been conducted in a proper manner.""A set of points was fixed in place with a piece of regular 3-millimeter wire which snapped." This fact in additional above ones confirmed that the technical manmade mistakes and not observing special safety rules and instructions were the main reason of the large accidents. It is important to notice that any large accidents in electric energy power supplies resulted to very serious negative consequences of many connected systems. On 25 May 2005, Moscow's power supplies were the centre of a major incident, which resulted in the supply being outed for several hours in many of City of Moscow districts, as well
as Moscow, Tula, Kaluga and Ryazan provinces

http://en.wikipedia.org/wiki/2005_Moscow_power_blackouts Some tens of thousands of people were trapped in stranded underground trains in the Moscow Metro and in elevators, railway signaling was put out of action and many commercial and governmental organisations were paralysed. Here, the high voltage (500kV) current, going into the capital along the main power lines, is lowered via transformers for city usage to 220kV and 110kV. Theories of the possible reasons of this accident were the following. The immediate cause of the incident, some state, was a mixture of several factors, among which feature: equipment wear-and-tear, absence of back-up powers, the fact that Moscow had endured temperatures above 30°C for a number of days. Moreover, Moscow is a very complex region and has the most complex electrical schemata, or "copper board", as it is known by those in the business. It is the only region in which there has been no automatic shut-off system installed since the fall of the Soviet Union. This increased vulnerability of Moscow's electrical network played an important role in what happened. But after all President Putin pointed out the main reason - the sudden failure of main electric transformer with its price only about 15, 000 USD.

The essential negative contribution in metro accidents is caused by the following facts: (1) using of false parts and appliances for cnstructions and fix of metro equipments; (2) metro train drivers and another technical personal have not the sufficient professional qualifications

Another metro global accidents were connected with terrorist attacks, that have happened in Madrid (2004) and London (2005). In 2010 Moscow Metro bombings were suicide bombings carried out by two women during the morning rush hour of March 29, 2010, at two stations of the Moscow Metro (Lubyanka and Park Kultury), with roughly 40 minutes interval between. At least 40 people were killed, and over 100 injured. In 2004. the similar Avtozavodskaya and Rizhskaya bombings took place. Chechen separatists were responsible for these terrorist acts. It is impossible to predict similar accidents. But sometimes the special homeland security services may to predict possible terrorist attacks with using of explosives. Today the modern high technologies are successfully used for detections of explosives in different parts of different complex constructions as potential dangerous places for using of explosives in terrorist controlled acts [28]

3. Conclusions

It is clear that all experimental data and existence statistic for any risk object exclude at all the possibility of creation temporal trend for prediction of accidents and catastrophes. Only for some natural water objects such as high mountain lakes results of many years observations and constant current detail monitoring on variation of its water contaminations, including radionuclides reactions, allow to predict its outbursts with the certain probability. Some advanced space technologies may be used for constant current monitoring of local regions, where it is possible dangerous natural earthquakes and manmade accidents on risk objects, such as water artificial constructions –HES, its dams

and huge storage reservoirs. In separate cases the using of such similar measures is able to predict future earthquakes, such as its time of appearance and intensity. Early Valyaev A.N. studied and worked in Polytechnic University in Russian Tomsk city in Siberia, where his colleges developed their own method of earthquake's prediction, based on the detail observations of natural electromagnetic field in the local seismic regions of the Earth with determination of some its main parameters [37-45] This method was based on their own patent technologies, that was successfully tested on seismic dangerous mountain regions such as Issyk -Kul Lake in Kyrgyzstan and Sayn mountain regions in East Siberia. That is why we may recommend this method in many cases.

The next following obstacles create the substation difficulties in risk management: (1) Every country has its own political, economical and demography particularities, that greatly reflect on behavior of emergency actions in critical situations; (2) Serious international frictions between different courtiers often take place especially at its transboundary territories; (3) Many vast territories are localized in zones of so called "frozen" or operated international and region conflicts, that in addition promote realization of different directed terrorist acts; (4) Contradictions of interests between of all community (including state governments) and the local private and international industrial companies, that realize its activity in separate country; (5) Insufficient level of population's safety culture; (6) Using of traditional and classical methods for disaster's investigations is often non effective and has failures. The brittle equilibrium between nature and human civilization has been broken now. Our Earth replies and revenges us. Sometimes it is impossible to predict natural and manmade disasters, catastrophes and terrorist acts with using of explosives. It demands very high organizational functions of all special emergency services – informational, , fire, evacuation, searching of casualties with immediate realization of medical help

Our results can be used:

1. The evaluation of risk's value, resulted with the possible natural or man-made catastrophes for the most dangerous objects for the developing a methodology/strategy to regulate and manage risks in emergencies;
2. When mapping risk allocation by various lands;
3. When developing a common system for emergency prevention/elimination. To formulate the preventive count measures and to estimate their efficiency with using the resource parameters for decreasing of risks values, their preventions and softening of their responses

The obtained results will have the universal character and may be used for analysis of the similar objects and situations in other countries.

References

1. A.N. Valyaev, S.V. Kazakov, A.A. H. D. Passell et. Al. Assessments of Risks and Possible Ecological and Economic Damages from Large-Scale Natural and Man-Induced Catastrophes in Ecology-Hazard Regions of Central Asia and the Caucasus. in NATO Science for Peace and Security Series -C: Environmental Security, Proc. of NATO Advanced Research Workshop: Prevention, Detection and Response to Nuclear and Radiological Threat", May 2-7, 2007 Yerevan, Armenia, Editors: S. Apikyan et. al. Published House: Springer, Netherlands, 2008, pp. 281-299

2. A. N. Valyaev, H. D. PassellL, V.P. Solodukhin, O.V. Stepanets, G.M. Aleksanyan, V.A. Petrov, A.A.Valyaev. Geo-chemical and Radiological Risks in dangerous regions of Central Asia and Caucasus», in Proceeding of the NATO Advanced Research Workshop: Stimulus for Human and Societal Dynamics in the Prevention of Catastrophes: NATO Science for Pearce and Security Series, E: Human and Societal Dynamics, 5– 8 October, Yerevan, Armenia, vol.80, pp.194-209, IOS Press –Amsterdam – Berlin – Tokyo – Washington, D.C. 2011, Edited by Arman Avagyan, David L. Barry, Wilhelm G. Goldewey, Dieter W.G. Reimer. http://ebooks.iospress.nl/publication/25443

3**.** A.N. Valyaev, S.A. Erochin, T.V. Tusova, G.M. Aleksanyan, A.A. Valyaev, «Risks to Aquatic Ecosystems in Mountain Regions and Their Possible Management», NATO Science for Peace and Security Series, E: Human and Societal Dynamics, 12^{th} – 15^{th} September , Dnipropetrovsk, Ukraine**,** Vol. 94 , Correlation Between Human Factors and the Prevention of Disasters. Edited of David L/ Barry and other, IOS Press, 2012, pp 191-206. http://ebooks.iospress.nl/publication/25760

4. A.N. Valyaev, S.V. Kazakov, V.A Petrov, in Proc. of Intern. Symposium "Complex Safety of Russia - Investigations, Management, Experience." May 26-27, 2004, Moscow, Publ. House: Informizdatcenter, pp.348-353. and pp. 353- 358.(in Russian)

5. A. N. Valyaev, S. V. Kazakov, A. A. Shamaeva, O. V. Stepanets, H. D. Passell, V. P. Solodukhin, V. A. Petrov, G. M. Aleksanyan, D. I. Aitmatova, R. F. Mamedov, M. S. Chkhartishvili, «Assessment of Risks and Possible Ecological and Economic Damage from Large-Scale Natural and Man-Induced Catastrophes in Ecologically Vulnerable Regions of Central Asia and the Caucasus», NATO Science for Peace and Security Series C: Environmental Security 2009, pp. 287-304. http://link.springer.com/chapter/10.1007%2F978-90-481-2344-5_33

6. A.N. Valyaev, S.V. Kazakov, A.A. Shamaeva, H. D. Passell, V.P. Solodukhin, O.V. Stepanets, G.M. Aleksanyan**.** "Development of monitoring system for studying radionuclide and chemical contamination level in transboundary river basins of Caspian and Kara seas on the territories of Russia and Kazakhstan". Proc. of ISTC International Workshop "DISTANT TRANSFER of RADIONUCLIDES in MOUNTAINOUS REGIONS", Tbilisi, Georgia, 6-10 November, 2006, pp. 45-46 and pp. 53-54.

7. A. N. Valyaev, S. V. Kazakov, H. D. Passell, V. P. Solodukhin, V. A. Petrov,

O. V. Stepanets, M. S. Chkhartishvili, G. Aleksanyan**.** Assessment of Radiological Risks and Possible Ecological and Economic Damages From Large-Scale Natural and Man-Induced Catastrophes in Ecology-Hazard Regionscatastrophes in Ecology-Hazard Regions of Central Asia and the Caucasus. NATO Science for Peace and Security Series B: Physics and Biophysics, 2008, Springer, Prevention, Detection and Response to Nuclear and Radiological Threats, ISSN 1874-6500 (Print) 1874-6535 (Online), pp. 281-299. http://link.springer.com/chapter/10.1007/978-1-4020-6658-0_25
8. A.N. Valyaev, S.V. Kazakov, H.D. Passell, G. Aleksanyan et. al. Assessments of Risks and Possible Ecological and Economic Damages from Large-Scale Natural and Man-Induced Catastrophes in Ecology-Hazard Regions of Central Asia and the Caucasus. NATO Science for Peace and Security Series – C, Environmental Security Nuclear Risk in Central Asia, 2008, Springer, Science + Business Media B, V, pp. 133-149.
http://link.springer.com/chapter/10.1007%2F978-1-4020-8317-4_13
9. R. Minasyan, V. Khondkaryan, G. Aleksanyan, A. Valyaev. Estimation of Risks and Damages from possible natural and Man-caused Catastrophes at ground dams in Armenia. BALWOIS 2008 - Ohrid, Republic of Macedonia - 27, 31 May 2008**,** pp. 1/8-8/8.
http://balwois.com/balwois/administration/full_paper/ffp-1147.pdf
10. A. N. Valyaev , S. V. Kazakov, A. A. Shamaeva, O. V. Stepanets, H. D. Passell, V. P. Solodukhin, V. A. Petrov, D. I. Aitmatova, G.M. Aleksanyan**.** Assessment of Risks and Possible Ecological and Economic Damage from Large-Scale Natural and Man-Induced Catastrophes in Ecologically Vulnerable Regions of Central Asia and the Caucasus. NATO Science for Peace and Security Series C: Environmental Security, 2009**,** Springer, ISSN 1874-6500 (Print) 1874-6535 (Online), pp. 89-102.
11. A.N. Valyaev, D.V. Nikoliski, A.A. Valyaeva, S.A. Erochin, T.V. Tusova, G.A. Aleksanyan, V.A. Petrov. Managing risks to water resources in mountain regions from natural and man-made disasters»**,** in Proceeding of the NATO Advanced Research Workshop: Stimulus for Human and Societal Dynamics in the Prevention of Catastrophes: NATO Science for Pearce and Security Series, E: Human and Societal Dynamics. 5– 8 October, Yerevan, Armenia, vol.80, pp. 172-188, IOS Press –Amsterdam – Berlin – Tokyo –Washington, D.C. **2011,** Edited by Arman Avagyan, David L. Barry, Wilhelm G. Goldewey, Dieter W.G. Reimer.http://ebooks.iospress.nl/publication/25441
12. A.N. Valyaev, S.A. Erochin, T.V. Tusova. Processes under outbursts of mountain lakes and model fo*r* risk assessment», in Book: Proceedings CHAOS2008 Editor: H. Skiadas, Published House: World Scientific, 2009, pp. 364-377.).
http://www.worldscientific.com/worldscibooks/10.1142/7251
13. A.N. Valyaev, S.A. Erochin, T.V. Tusova. Assessments and decreasing of risks and damages from outbursts of Tien-Shan high mountains lakes" in Book: Uranium, Mining and Hydrogeology. Published House: Springer Berlin Heidelberg, 2008, pp. 819-826.
http://link.springer.com/chapter/10.1007%2F978-3-540-87746-2_107

14. G.M. Aleksanyan, A.N .Valyaev, K I. Pyuskyulyan. Several approaches to the solution of water contamination problems in transboundary rivers crossing the territory of Armenia. NATO Science for Peace and Security Series – C, Environmental Security Nuclear Risk in Central Asia, 2008, Springer, Science + Business Media B, V, pp. 201-211.
15. A.N. Valyaev, S.V. Kazakov, A.A. H. D. Passell et. Al. Assessments of Radiological Risks and Possible Ecological and Economic Damages from Large-Scale Natural and Man-Induced Catastrophes in Ecology-Hazard Regions of Central Asia and the Caucasus. In Proc of ISTC Workshop: DISTANT TRANSFER of RADIONUCLIDES in MOUNTAINOUS REGIONS. Tbilisi, Georgia, 6-10 November, 2006, pp.155-164.
16. A.N. Valyaev, S.A. Erochin, T.V. Tusova. Processes under outbursts of mountain lakes and model for risk assessment. Proc. of International Conference: Chaotic Modeling and Simulation (CHAOS20080, June 3 - 6, 2008 Chania Crete Greece, www.asmda.net/chaos2008. http://www.chaos2008.net/zzProceedings/CHAOS2008%20(D)/PAPERS_PDF/Valyaev_Erochin_Tusova-Processes_under_outbursts_of_mountain_lakes.pdf
17. A.N. Valyaev, S.A. Erochin, T.V. Tusova. Processes under outbursts of mountain lakes and model for risk assessment. in Book: Proceedings CHAOS2008 Editor: H. Skiadas, Published House: World Scientific, 2009, pp. 350-363.
18. A.N. Valyaev, S.A. Erochin, T.V. Tusova. Assessments and decreasing of risks and damages from outbursts of Tien-Shan high mountains lakes" in Book:"Uranium, Mining and Hydrogeology. Published House: Springer Berlin Heidelberg, 2008, pp. 819-826
19. A.N. Valyaev, D.V. Nikoliski, A.A. Valyaeva, S.A. Erochin, T.V. Tusova , G.M. Aleksanyan, V.A. Petrov. Managing risks to water resources in mountain regions from natural and man-made disasters" in Proceeding of the NATO Advanced Research Workshop: Stimulus for Human and Societal Dynamics in the Prevention of Catastrophes: NATO Science for Pearce and Security Series. E: Human and Societal Dynamics –vol. 80, pp.172-188, 2011.IOS Press – Amsterdam – Berlin – Tokyo –Washington, D.C., Edited by Arman Avagyan, David L. Barry, Wilhelm G. Goldewey, Dieter W.G. Reimer.
20. R.S. Minasyan, G.M. Aleksanyan, A.N. Valyaev, L.S. Sargsyan, A.A. Valyaeva, Large Artificial Water Reservoirs and Dams as Critical Risk Objects in Armenia, in Proceeding of the NATO Advanced Research Workshop: "Stimulus for Human and Societal Dynamics in the Prevention of Catastrophes: NATO Science for Pearce and Security Series, E: Human and Societal Dynamics", 5– 8 October, Yerevan, Armenia, .80, pp.131-138, IOS Press – Amsterdam – Berlin – Tokyo –Washington, D.C. 2011, Edited by Arman Avagyan, David L. Barry, Wilhelm G. Goldewey, Dieter W.G. Reimer. http://ebooks.iospress.nl/publication/25435
21. Valyaev A.N., et.al. Prediction of irradiation doses for population under implementation of Russian Federal Program: Development of Russian atomic energy industrial complex on 2007-2020 years. Ibidem, pp.294- 308.

22. A.N. Valyaev , A.L. Krylov , V.N. Semenov , G.M. Aleksanyan, A.A. Valyaev. Irradiation doses at nuclear power plants at normal and emergency situations. in Proceeding of the NATO Advanced Research Workshop: Correlation Between Human Factors and the Prevention of Disasters: NATO Science for Pearce and Security Series. E: Human and Societal Dynamics" –IOS Press –Amsterdam – Berlin – Tokyo –Washington, D.C., Edited by David L. Barry, Wilhelm G. Goldewey, Dieter W.G. Reimer and Dmytro V. Rudakov vol.94, pp. 40-57. 2012.
23. A.N. Valyaev, H. D. Passell, V.P. Solodukhin, O.V. Stepanets, G.M.Aleksanyan, V.A.Petrov, A.A. Valyaev. Geo-chemical and Radiological Risks in dangerous regions of Central Asia and Caucasus, in Proceeding of the NATO Advanced Research Workshop: Stimulus for Human and Societal Dynamics in the Prevention of Catastrophes: NATO Science for Pearce and Security Series, E: Human and Societal Dynamics, 5– 8 October, Yerevan, Armenia, vol.80, pp.194-203, IOS Press –Amsterdam – Berlin – Tokyo – Washington, D.C. 2011, Edited by Arman Avagyan, David L. Barry, Wilhelm G. Goldewey, Dieter W.G. Reimer. http://ebooks.iospress.nl/publication/25443
24. R.S. Minasyan, G.M. Aleksanyan, A.N. Valyaev, Study and prognosis of land subsidence in karsts regions due to falling groundwater levels, NATO Science for Peace and Security Series, E: Human and Societal Dynamics, 12th – 15th September, Dnipropetrovsk, Ukraine**,** Vol. 94 , Correlation Between Human Factors and the Prevention of Disasters. Edited of David L/ Barry and other, IOS Press, 2012, pp 125-133. http://ebooks.iospress.nl/publication/25752
25. A.N. Valyaev, S.A. Erochin, T.V. Tusova, G.M. Aleksanyan, A.A. Valyaev, Risks to Aquatic Ecosystems in Mountain Regions and Their Possible Management, NATO Science for Peace and Security Series, E: Human and Societal Dynamics, 12th – 15th September , Dnipropetrovsk, Ukraine**,** Vol. 94 , Correlation Between Human Factors and the Prevention of Disasters. Edited of David L/ Barry and other, IOS Press, 2012, pp 191-206 http://ebooks.iospress.nl/publication/25760
26.G.M. Aleksanyan, A.N .Valyaev, K I. Pyuskyulyan. Several approaches to the solution of water contamination problems in transboundary rivers, crossing the territory of Armenia. In NATO Science Series: Proc. of NATO Advanced Research Workshop: Nuclear Risk in Central Asia, Kazakhstan, Almaty, June 20-22, 2006. Editors: B. Salbu and L. Skipperud, Published House: Springer Science +Business Media B.V. 2008, Netherlands, pp. 201-211.
27.A.N. Valyaev, V.P. Kiselev, N.N. Gerasimenko and K.K.Djamabalin. Development of an Environment Monitoring System for Near-Frontier Regions of Russia & Kazakhstan within the Framework of Russian Federal Purpose Program Integration.In Proc. 4-th International Conference Nuclear and Radiation Physics. September15-18, 2003, Alma-Ata, Kazakhstan, v.1, pp.27-34.
28. S.V. Kazakov, S.S.Utkin, I.I. Linge, A.N.Valyaev. Categorization of Aqueous Media and Water Bodies by Contamination Radioactive Levels. In Proc. of International Conference "Radioactivity after Nuclear Explosions and

Accidents, v.3, pp. 402-407, (in Russian) December 5-6, Moscow, Publ. House: St. Peterburg, GIDROMETIZDAT, 2006.

Circular generator of PRN's

Pavel Varbanets[1] and Sergey Varbanets[2]

[1] I.I. Mechnikov Odessa National University, srt. Dvoryanskaya 2, 65082 Odessa, Ukraine
(E-mail: varb@sana.od.ua)
[2] I.I. Mechnikov Odessa National University, srt. Dvoryanskaya 2, 65082 Odessa, Ukraine
(E-mail: varb@sana.od.ua)

Abstract Let E_m be a subgroup of multiplicative group of reduced residues modulo p^m, $p \equiv 3 \pmod 4$ in the ring of Gaussian integers with norm one $\pmod{p^m}$.

Using the description of elements from E_m we construct the sequence of real numbers which satisfies the condition of equidistribution and statistical independency, i.e. it is a sequence of PRN's.
Keywords: pseudorandom numbers, discrepancy, exponential sum.

1 Introduction

The sequence of real numbers $\{a_n\}$, $0 \le a_n < 1$, we call the sequence of pseudo-random numbers (arbitrary, PRN's) if it is produced by deterministic generator and being a periodical sequence has the statistical properties such that it looks like to implementation of the sequence of random numbers with independent and uniformly distributed values on $[0, 1)$. More acceptable sequences of PRN's generate by the congruential recursion

$$y_{n+1} \equiv f(y_n, y_{n-1}, \dots, y_{n-k+1}) \pmod m, \tag{1}$$

where $y_0, y_1, \dots, y_{k-1} \in \{0, 1, \dots, m-1\}$, $f(u_1, \dots, u_k)$ is integer function over $\mathbb{Z}_m^k$.

In case $f \in \mathbb{Z}_m[u_1, \dots, u_k]$ we have the congruential polynomial generator of periodical sequence $\{y)n\}$ with a period τ, $\tau \le m$.

It emerged that linear function $f(u) = au + b$ does not supply requirements of "affinity" to statistical independency (unpredictability) (see, for example [11])

But quadratic function $f(u) = au^2 + bu + c$ satisfies to condition of "practical" unpredictability (see, [8]).

The generator associated with quadratic function $f(c)$ we call parabolical.

The requirements to uniform distribution and unpredictability is satisfied the following inversive generator

$$y_{n+1} \equiv ay_n^{-1} + b \pmod{p^m}, \tag{2}$$

where p is a prime number, $a, b \in \mathbb{Z}$, y_n^{-1} is a multiplicative inverse to y_n $\pmod{p^m}$.

The inversive generator (2) and its generalization was being investigated by

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

many authors (see, [3]-[10], [14]-[18]).

Starting out from our reasoning we will call such inversive generator as hyperbolical.

To apply the sequence $\{y_n\}$ in cryptography it is necessary to carry-out the requirement of secrecy as well. That means providing the impossibility to restore the generator parameters by single values of sequence elements. There are some interesting researches about this area (see, [1]-[4], [9], [10]). In the paper [18] there are being investigated the analogues of inversive congruential generators, that without any increases of computational complexity of finding the elements of sequence $\{y_n\}$, get essential complexity for intruder's work around parameters of inversive or linear generator to be recovered.

Let $p \equiv 3 \pmod 4$ be a prime rational number, m be a natural. Denote G the ring of gaussian integers, $G = \{a + bi \ : \ a, b \in \mathbb{Z},\ i^2 = -1\}$, and G_{p^m} (accordingly, $G^*_{p^m}$) the ring of residue classes (accord., multiplicative group of this ring modulo p^m) over G.

Let

$$E_m := \left\{\alpha \in G^*_{p^m} : \ N(\alpha) \equiv \pm 1 \pmod{p^m}\right\}.$$

It easy to check, that E_m is a subgroup in $G^*_{p^n}$ with order $2(p+1)p^{m-1}$, that we call the norm group over the ring G_{p^m}. As far as E_m is a cyclic group, it means that every generated element $u + iv$ defines two sequences of integer numbers modulo p^m:

$$Z_n = \Re((u+iv)^n) \ \ and\ W_n = \Im((u+iv)^n), \ \ n = 1, 2, \ldots.$$

The main point of this work is to prove that the sequences $\left\{\frac{Z_n}{p^m}\right\}$ and $\left\{\frac{W_n}{p^m}\right\}$ are uniformly distributed on $[0, 1)$.

2 Notations and Auxiliary results

Before studying the sequences of PRN's produced by circular generator, we standardize some notations to be used throughout this paper.

Lower case Roman (respectively, Greek) letters usually denote rational (respectively, Gaussian) integers; inparticular, m, n, k are positive integers and p is always a rational prime number $p \equiv 3 \pmod 4$. We also define a *norm* over $\mathbb{Q}(i)$ into $\mathbb{Q}$ by $N(\alpha) = |\alpha|^2$. For the sake of convenience, we denote by G the set of the Gaussian integers. Let $\mathbb{Z}_q$ (or G_q) denotes the ring of residue classes modulo q, and $\mathbb{Z}^*_q$ (or G^*_q) denotes the multiplicative group in $\mathbb{Z}$ (or G_q). If $x \in G^*_q$ we write x^{-1} for the multiplicative inverse of x mod q, i.e. x^{-1} is an arbitrary Gaussian integer sutysfying the condition $xx^{-1} \equiv 1 \pmod q$. As usual, $gcd(a, b)$ or (a, b) stand for the greater common divisor of a and b (or, respectively, α and β in G), Through $\mathbb{Z}[x]$ (or $G[x]$) we denote the polynomial ring over $\mathbb{Z}$ (or G). For $a \in \mathbb{Z}$ ($\alpha \in G$) stand $\nu_p(a)$ (or $\nu_p(\alpha)$) if $p^{\nu(a)} | a$, $p^{\nu(a)+1} \not| a$.

Before starting out the study of the sequences $\{Z_n\}$ and $\{W_n\}$ we need several lemmas being used in sequel.

Lemma 1. *Let* $f(\xi)=\alpha_1\xi+\alpha_2\xi^2\mathfrak{p}+\alpha_3\xi^3\mathfrak{p}^{\nu_3}+\cdots+\alpha_k\xi^k\nu_{\mathfrak{k}}$, *where* $\nu_3,\nu_4,\ldots,\nu_k$, $n\geq 2$ *be positive integers,* $\alpha_1,\ldots,\alpha_k\in G$, $(\alpha_2,\mathfrak{p})=\cdots=(\alpha_k,\mathfrak{p})=1$. *Then we have*

$$|S(f,\mathfrak{p}^n)|\leq\begin{cases}0 & if\ \mathfrak{p}\neq 1+i,\ (\alpha_1,\mathfrak{p})=1\\ & or\ \mathfrak{p}=1+i,\ \alpha_1\not\equiv 0 \pmod{\mathfrak{p}^2},\\ N(\mathfrak{p})^{\frac{n+1}{2}} & if\ \mathfrak{p}\neq 1+i,\ \alpha_1\equiv 0 \pmod{\mathfrak{p}},\\ 2^{\frac{n+3}{2}} & if\ \mathfrak{p}=1+i,\ \alpha_1\equiv 0 \pmod 2.\end{cases}$$

Proof. For $n=2$ the estimated sum is the Gaussian sun, and thus in such case our assertion holds.

For $n\geq 3$, $\mathfrak{p}$ be a odd prime. We put

$$\xi=\eta+\mathfrak{p}^{n-1}\zeta,\ \eta\in G_{\mathfrak{p}^{n-1}},\ \zeta\in G_{\mathfrak{p}}.$$

Taking into account that $\xi^k=\eta^k+k\eta^{k-1}\zeta \pmod{\mathfrak{p}^{n-1}}$, we get

$$S(f,\mathfrak{p}^n)=\sum_{\eta\in G_{\mathfrak{p}^{n-1}}}e^{2\pi i\Re\left(\frac{f(\eta)}{\mathfrak{p}^n}\right)\Re\left(\frac{\alpha_1+2\alpha_2\eta}{\mathfrak{p}}\zeta\right)}=N(\mathfrak{p})\sum_{\substack{\eta\in G_{\mathfrak{p}^{n-1}}\\ \alpha_1+2\alpha_2\eta\neq 0 \pmod{\mathfrak{p}}}}e^{2\pi i\Re\left(\frac{f(\eta)}{\mathfrak{p}^n}\right)}.$$

Let $\alpha_1+2\alpha_2\eta_0\equiv 0 \pmod{\mathfrak{p}}$, $\eta_0\in G^*_{\mathfrak{p}}$. We put $\eta=\eta_0+\mathfrak{p}\xi$, $\xi\in G_{\mathfrak{p}^{n-2}}$. Then we infer

$$f(\eta_0+\mathfrak{p}\xi)=f(\eta_0)+\mathfrak{p}(\alpha_1+2\alpha_2\eta_0)\xi+\mathfrak{p}^2\alpha_2'\xi^2+\cdots=f(\eta_0)+\mathfrak{p}^2f_1(\xi),$$

where the polynomial $f_1(\xi)$ has such type as $f(\xi)$.

So, after $\left[\frac{n}{2}\right]$ steps we obtain

$$|S(f,\mathfrak{p}^n)|=\begin{cases}N(\mathfrak{p})^{\frac{n}{2}} & if\ n\ is\ even,\\ N(\mathfrak{p})^{\frac{n-1}{2}}\left|\sum\limits_{\xi\in G_{\mathfrak{p}}}e^{2\pi i\Re\left(\frac{\beta_1+\beta\xi^2}{\mathfrak{p}}\right)}\right| & if\ n\ is\ odd.\end{cases}$$

By the estimate of the Gauss sum we have the assertion of Lemma.

The case $\mathfrak{p}=1+i$ can be considered similarly. □

Corollary 1. *Let* $f(\xi)=\alpha\xi+\beta\xi^2+\mathfrak{p}(\gamma\xi^2+\cdots)$ *be a polynomial over* G, *and let* $(\beta,\mathfrak{p})=1$. *Then for any* $\delta\in G$, *we have*

$$\left|\sum_{\xi\in G^*_{\mathfrak{p}^n}}e^{2\pi i\Re\left(\frac{f(\xi)+\delta\xi^{-1}}{\mathfrak{p}^n}\right)}\right|\leq 2N(\mathfrak{p})^{\frac{n}{2}}.$$

Indeed, putting $\xi=\eta+\mathfrak{p}^{n-1}\zeta$, $\eta\in G^*_{\mathfrak{p}^{n-1}}$, $\zeta\in G_{\mathfrak{p}}$, and observing that $\xi^{-1}=\eta^{-1}-\mathfrak{p}^{n-1}\xi(\eta^{-1})^2$, where η^{-1} be a multiplicative inverse mod$\mathfrak{p}^n$ for η, we immediately infer that inequality holds by Lemma 1.

Similarly, assertion holds for the same exponential sums over $\mathbb{Z}_{p^n}$.

Let us denote by E_m the following subgroup of $G^*_{p^m}$, $p \equiv 3 \pmod 4$, p be a prime number in $\mathbb{Z}$:

$$E^+_m := \{x \in G^*_{p^m} \,:\, N(x) \equiv 1 \pmod{p^m}\}.$$

The subgroup E^+_m we will call the norm group in $G^*_{p^m}$.

Take into account that the multiplicative group of the field G_p is a cyclic group. It is easy to prove (as in $\mathbb{Z}^*_{p^m}$) that it exists a generating element of the group E^+_1, such that it will generate every group E^+_m, $m > 1$.

In order to find that element, we take such generating element g_0 of group G^*_p for which $g_0^{(p+1)p} = 1+hp^2$ with $(h,p) = 1$. Then g_0^{p-1} is revealed generating element of group E^+_m, $m = 1, 2, \ldots$.

Moreover, we have

Lemma 2. *Let us $u + iv \in E_m$ be a generating element of E_m. Then $ord(u + iv) = |E_m| = 2(p+1)p^{m-1}$ and*

$$(u+iv)^{2(p+1)} = 1 + p^2 x_0 + ipy_0,$$
$$x_0 + 2y_0^2 \equiv 0 \pmod p,\ (x_0, p) = (y_0, p) = 1,$$

and also for any $t = 4, 5, \ldots$, we have modulo p^m

$$\begin{aligned} \Re(u+iv)^{2(p+1)t} &= A_0 + A_1 t + A_2 t^2 + \cdots + A_{m-1} t^{m-1}, \\ \Im(u+iv)^{2(p+1)t} &= B_0 + A_1 t + B_2 t^2 + \cdots + B_{m-1} t^{m-1}, \end{aligned} \tag{3}$$

where

$$\begin{cases} A_0 \equiv 1 \pmod{p^4},\ B_0 \equiv 0 \pmod{p^4}, \\ A_1 \equiv p^2 x_0 + \frac{1}{2} p^2 y_0^2 \equiv 0 \pmod{p^3},\ B_1 \equiv py_0 \pmod{p^3}, \\ A_2 \equiv -\frac{1}{2} p^2 y_0^2 \pmod{p^3},\ B_2 \equiv 0 \pmod{p^3}, \\ A_j \equiv B_j \equiv 0 \pmod{p^3},\ j = 3, 4, \ldots m-1. \end{cases} \tag{4}$$

□

Denote

$$(u+iv)^{2k} = u(k) + iv(k),\ 0 \le k \le p,$$
$$(u+iv)^{2(p+1)t+2k} \equiv \sum_{j=0}^{m-1} (A_j(k) + iB_j(k))\, t^j \pmod{p^m}.$$

It is clear

$$A_j(k) = A_j u(k) - B_j v(k),$$
$$B_j(k) = A_j v(k) + B_j u(k).$$

Thus from Lemma 1 we have

Corollary 2. *For $k = 1, 2, \ldots, p$, we have*

$$u(k) \equiv u(-k),\ v(k) \equiv -v(-k) \pmod{p^m},$$
$$(u(k), p) = (v(k), p) = 1,\ if\ k \ne \frac{p+1}{2},$$
$$u(0) = 1,\ v(0) = 0,$$
$$u(k) \equiv 0 \pmod p,\ (v(k), p) = 1,\ if\ k = \frac{p+1}{2}.$$

Moreover, for $k \neq \frac{p+1}{2}$

$$A_0(k) \equiv u(k),\ B_0(k) \equiv v(k) \pmod{p},$$
$$p||A_1(k),\ p||B_1(k),\ p^2||A_2(k),\ p^2||B_2(k);$$

and

$$A_1(0) \equiv 0 \pmod{p^4},\ B_1(0) \equiv py_0 \pmod{p^4},\ p^2||A_2(0),\ B_2(0) \equiv 0 \pmod{p^3},$$
$$A_0(k) \equiv 0,\ B_0(k) \equiv 0 \pmod{p},$$
$$P||A_1(k),\ p^2||B_1(k),\ p^2||A_2(k),\ B_2(k) \equiv 0 \pmod{p^3}\ if\ k = \frac{p+1}{2},$$
$$A_j(k) \equiv B_j(k) \equiv 0 \pmod{p^3},\ k = 0, 1, \ldots, p,\ j \geq 3.$$

The proof of Corollary is a simple exercise (in view the congruence

$$(u+iv)^{p+1} = 1 + p^2x_0 + iy_0,$$
$$(x_0, p) = (y_0, p) = 1,$$
$$2x_0 + y_0^2 \equiv 0 \pmod{p},$$
$$u^2 + v^2 \equiv +1 \pmod{p^m} \qquad),$$

and we omit.

3 Circular generator of PRN's

We select a random number k from $\{0, 1, 2, \ldots, p-1\}$ and consider the sequence $\{(u+iv)^{2(p+1)t+2k}\}$, $t = 0, 1, \ldots, p^{m-1}-1$, where $u+iv$ is a generating element of E_m.

Denote

$$Z_t(k) = Z_t = \Re\Big((u+iv)^{2(p+1)t+2k}\Big),$$
$$W_t(k) = W_t = \Im\Big((u+iv)^{2(p+1)t+2k}\Big).$$

These sequences discribed in Lemma 2.

We saw that $(u+iv)^{2(p+1)} = u_0 + iv_0$, where $u_0 = 1 + p^2x_0$, $v_0 = y_0$, $(x_0, p) = (y_0, p) = 1$ and $x_0 + 2y_0^2 \equiv 0 \pmod{p}$.

Hence,

$$\begin{aligned} Z_{t+1} &\equiv \Re\big((u_0+iv_0)^t \cdot (u_0+iv_0) \cdot (u(k)+iv(k))\big) \equiv \\ &\equiv Z_t u_0 - W_t v_0 \pmod{p^m}, \end{aligned} \tag{5}$$

$$W_{t+1} \equiv Z_t v_0 + W_t u_0 \pmod{p^m} \tag{6}$$

for $t = 0, 1, \ldots, p^{m-1} - 1$.

The sequence (5) and (6) satisfies that condition

$$Z_t^2 + W_t^2 \equiv 1 \pmod{p^n}$$

for any $t \in \mathbb{Z}_{p^{n-1}}$ and $k \in \{0, 1, \ldots, p\}$.

Thus we call the sequences (5) and (6) circular sequences of PRN's.

Theorem 1. *Let $a, b \in \mathbb{Z}_{p^m}$, $(a, b, p) = 1$. Then for the exponential sum*

$$S(a, b; p^m) = \sum_{t \in \mathbb{Z}_{p^{m-1}}} e_{p^m}(aZ_t + bW_t)$$

we have the following bound

$$|S(a, b; p^m)| \leq 2p^{\frac{m}{2}}. \tag{7}$$

Proof. Lemma 2 and its Corollary give

$$aZ_t(k) + bW_t(k) \equiv c_0 + c_1 t + c_2 t^2 + \cdots \pmod{p^m},$$

where notationally of Lemma 2 we have

$$c_j(k) = au_0 A_j(k) - bv_0 B_j(k),\ j = 0, 1, 2, \ldots.$$

In particular, taking into account $u_0 = 1 + p^2 x_0$, $v_0 = py_0$, we have

$$\begin{cases} c_1 \equiv py_0(-av(k) + bu(k)) + p^2 y_0^2(-au(k) - bv(k)) \pmod{p^3}, \\ c_2 \equiv -\frac{1}{2}p^2 y_0^2 a \pmod{p^3},\ \ c_j \equiv 0 \pmod{p^3},\ j \geq 3. \end{cases} \tag{8}$$

Therefore, by Lemma 1, we easy obtain

$$|S(a, b; p^m)| \leq \begin{cases} 2p^{\frac{m}{2}} & if \quad au(k) - bv(k) \equiv 0 \pmod{p} \\ 0 & else. \end{cases}$$

□

Corollary. *For $1 < T < p^{m-1}$ and any $k \in \{0, 1, \ldots, p\}$*

$$\left| \sum_{t=0}^{T-1} e^{2\pi i \frac{aZ_t(k) + bW_t(k)}{p^m}} \right| \leq 2p^{\frac{m}{2}} \log p^m. \tag{9}$$

Indeed, the inequality (9) is consequence of well-known estimate of incomplete sum by complete sum. □

Denote

$$aZ_t(k) + bW_t(k) = x_t(a, b; k) := x(t). \tag{10}$$

Theorem 2. *Let s be positive integer, $h_1, \ldots, h_s \in \mathbb{Z}_{p^m}$, $(h_1, \ldots, h_s, p) = 1$. Then for $s \in \{1, 2, \ldots, p-1\}$ the following estimate*

$$S(h_1, \ldots, h_s) = \sum_{t=0}^{p^{m-1}-1} e_{p^m}(h_1 x(t) + h_2 x(t+1) + \cdots + h_s x(t+s-1)) \ll p^{\frac{m}{2}}$$

holds.
(with an absolute constant depending only on s).

Proof. Using (8) and calculating coefficients for t and t^2 in presentation $h_1 x(t) + h_2 x(t+1) + \cdots + h_s x(t+s-1)$ as a polynomial of t or $(t+1)$,..., or $t+s-1$, we obtain (by Lemma 1) that $S(h_1, \ldots, h_s) = 0$ only if $-av(k) + bu(k) \equiv 0 \pmod{p}$. In such case we estimate the sum $S(h_1, \ldots, h_s)$ as $O\left(p^{\frac{m}{2}}\right)$ with the absolute constant in symbol "O". In other cases this sum is zero. □

Remark 1. It easy to prove that for the congruence $av(k) \equiv bu(k) \pmod{p}$ at most six solutions satisfies.

Corollary. *In the conditions of Theorem 2 we have*

$$\sum_{t=0}^{T-1} e_{p^m}(h_1 x(t) + h_2 x(t+1) + \cdots h_s x(t+s-1)) \ll p^{\frac{m}{2}} \log p^m.$$

4 Discrepancy bound

Consider the sequence $\{x(t)\}$, $t = 0, 1, 2, \ldots$ of the elements of $\mathbb{Z}_{p^m}$ defined in (10). Let $\{y(t)\}$ be a sequence of PRN's in interval $[0, 1)$ obtained by the normalization $y(t) = \frac{x(t)}{p^m}$,

The sequence $\{y(t)\}$, $t = 0, 1, \ldots$, is purely periodic with the period length $\tau = p^{m-1}$.

Equidistribution and statistical independency properties of pseudorandom numbers can be analyzed based on the discrepancy of certain point sets in $[0, 1)^s$.

Besides the discrepancy, there exist other important criteria for the uniformity and independence of PRN's. We will restrict our attention to the discrepancy, since it is the most important measure of uniformity and independence in connection with PRN's.

For N arbitrary points, $x_0, x_1, \ldots, x_{N-1} \in [0, 1)^d$, the discrepancy is defined by

$$D_N(x_0, x_1, \ldots, x_{N-1}) = \sup_{I \subset [0,1)^d} \left| \frac{A_N(I)}{N} - |I| \right|, \tag{11}$$

where the supremum is extended over all subintervals I of $[0, 1)^d$, $A_N(I)$ is the number of points among $x_0, x_1, \ldots, x_{N-1}$ falling into I, and $|I|$ denotes the d-dimensional volume of I.

Our goal is to obtain a nontrivial discrepancy estimate for a part of period for the circular generators of pseudorandom numbers. In particular, we shall estimate discrepancy for the sequence $\{\omega_\ell\}$, $\omega_\ell = \frac{x_\ell}{p^m}$, $\ell \geq 0$ and for the sequence $\{\Omega_\ell\}$, $\Omega_\ell = (\omega_\ell, \omega_{\ell+1}, \ldots, \omega_{\ell+s-1})$, $\ell \geq 0$, $s \geq 2$. Well-known that a small value $D(\omega_0, \omega_1, \ldots, \omega_{N-1})$ guarantees an uniform distribution $\{\omega_\ell\}$, $\ell \geq 0$ on $[0, 1)$, and a small value $D(\Omega_0, \Omega_1, \ldots, \Omega_{N-1})$ means that the sequence $\{\omega_\ell\}$, $\ell \geq 0$, pass the two-dimensional serial test on the statistical independence properties of this sequence. In the cryptographical applications the property of statistical independence means that the circulate congruential pseudorandom sequence $\{x_\ell\}$, $\ell \geq 0$, is unpredictable.

In the following, some further notation is necessary.

For integers $d \geq 1$ and $q \geq 2$, let $C_d(q)$ be the set of all nonzero lattice points $\mathbf{h} = (h_1, \ldots, h_d) \in \mathbb{Z}^d$ with $-\frac{q}{2} < h_j \leq \frac{q}{2}$ for $1 \leq j \leq d$. Define for

$\mathbf{h} \in C_d(q)$

$$r(h,q) = \begin{cases} 1 & if\ h = 0, \\ q \sin(\pi \frac{|h|}{q})\ if\ h \neq 0, \end{cases}$$
$$r(\mathbf{h},q) = \prod_{j=1}^{d} r(h_j,q) \tag{12}$$

Moreover, several auxiliary results are given.

Lemma 3. *Let $N \geq 1$ and $q \geq 2$ be integers. Suppose that $\mathbf{y_0}, \mathbf{y_1}, \ldots, \mathbf{y_{N-1}} \in \mathbb{Z}_q^d$. Then the discrepancy of the points $\mathbf{t}_\ell = \frac{\mathbf{y}_\ell}{q} \in [0,1)^d$, $\ell = 0,1,\ldots,N-1$, satisfies*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}}) \leq \frac{d}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_d(q)} \frac{1}{r(\mathbf{h},q)} \left| \sum_{\ell=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_\ell) \right| \tag{13}$$

(Proof see in [13], Theorem 3.1).

Lemma 4. *Let T be the period of the sequence $\{\mathbf{y_k}\}$, $T \geq N \geq 1$ and $q \geq 2$ be integers, $\mathbf{y_k} \in \{0,1,\ldots,q-1\}^d$ for $k = 0,1,\ldots,N-1$; $\mathbf{t_k} = \frac{\mathbf{y_k}}{q} \in [0,1)^d$. Then*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}}) \leq \frac{d}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_d(q)} \sum_{h_0 \in \left(-\frac{T}{2}, \frac{T}{2}\right]} \frac{1}{r(\mathbf{h},q) r(h_0,T)} \times \\ \times \left| \sum_{k=0}^{T} e(\mathbf{h} \cdot \mathbf{t_k} + \frac{k h_0}{T}) \right| \tag{14}$$

This assertion follows from Lemma 3 and from an estimate of uncomplete exponential sum through complete exponential sum.

Now it easy to prove the following theorems.

Theorem 3. *Let $p \equiv 3 \pmod 4$ be a prime number and let $x(k,\ell) := x(\ell) = a\Re\big((u+iv)^{2(p+1)\ell+2k}\big) + b\Im\big((u+iv)^{2(p+1)\ell+2k}\big)$ be the sequence circular PRN's. Then for any $k \in \{0,1,\ldots,p\}$, $k \neq \frac{p+1}{2}$ we have*

$$D_N\left(\frac{x(0)}{p^m}, \frac{x(1)}{p^m}, \ldots, \frac{x(N-1)}{p^m}\right) \leq \frac{1}{p^m} + \frac{2p^{\frac{m}{2}}}{N}\left(\frac{1}{p}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^2 + 1\right),$$

where $1 \leq N \leq p^{m-1} - 1$.

Theorem 4. *Let $\mathbf{t}_\ell$, $\ell = \{0,1,\ldots,p^{m-1}-1\}$ be a sequence of points $\mathbf{t}_\ell \in [0,1)^s$, $\mathbf{t}_\ell = (x(\ell), x(\ell+1), \ldots, x(\ell+s-1))$. Then the following estimate for $T = p^{m-1}$ and $s \leq p-1$*

$$D_T^{(s)} := D_T(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{T-1}}) \leq \frac{s}{p^m} + \frac{1}{p^{\frac{m-1}{2}}}\left(1 + \frac{1}{p}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^s\right).$$

holds.

The proofs of these theorems follow from the estimates of theorems 1 and 2 and their corollaries.

From Theorem 3 and 4 it follows that the sequences $\{\Re\big((u+iv)^{2(p+1)\ell+2k}\big)\}$ and $\{\Im\big((u+iv)^{2(p+1)\ell+2k}\big)\}$ are equidistributed and pass s-dimensional test on unpredictability.

References

1.Blackburn S.R., Gomez-Peres D., Gutierrez I. and ShparlinskiI.. Predicting nonlinear pseudorandom number generators. *Math. Comp.*, 74(251):1471–1494, 2004.

2.Blackburn S.R., Gomez-Peres D., Gutierrez I. and Shparlinski I.. Reconstructing noisy polynomial evaluation in residue rings. *J. of Algorithm*, 61(2):47–59, 2006.

3.Eichenauer-Herrmann J.. Inversive congruential pseudorandom numbers: a tutorial. *Internat. Statist. Rev.*, 60:167–176, 1992.

4.Eichenauer-Herrmann J.. Pseudorandom number generation by nonlinear methods. *Internat. Statist. Rev.*, 63:247–255, 1995.

5.Eichenauer-Herrmann J.,Grothe H.. A New Inversive Congruential Pseudorandom Number Generator with Power of Two Modulus. *ACM Transactions of Modelling and Computer Simulation*, 2(1):1–11, 1992.

6.Eichenauer J. and Lehn J.. A non-linear congruential pseudorandom number generator. *Statist. Hefte*, 27:315–326, 1986.

7.Eichenauer J. and Lehn J. and Topuzoğlu A.. A nonlinear congruential pseudorandom number generator with power of two modulus. *Math. Comp.*, 51:757–759, 1988.

8.Eichenauer-Herrmann J., Herrmann E. and Wegenkittl S.. A survey of quadratic and inversive congruential pseudorandom numbers, in: Monte Carlo and Quasi-Monte Carlo Methods, 1996, H. Niederreiter et al(eds.), Lecture Notes in Statist. *Springer, New York*, 127:66–97, 1998.

9.Eichenauer-Herrmann J. and Topuzoğlu A.. On the period of congruential pseudorandom number sequences generated by inversions. *J. Comput. Appl. Math.*, 31:87–96, 1990.

10.Kato T., Wu L.-M., Yanagihara N.. On a nonlinear congruential pseudorandom number generator. *Math. of Comp.*, 65(213):227–233, 1996.

11.Knuth D. E.. The Art of Computer Programming, Vol. 2:Seminumerical algorithms. *Addison-Wesley*, 1998.

12.Niederreiter H.. Nonlinear methods for pseudorandom number and vector generation. *Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. and Math. Systems, Springer, Berlin*, 374:145–153, 1992.

13.Niederreiter H.. Random Number Generation and Quasi-Monte Carlo Methods. *SIAM, Philadelphia,Pa.*, 1992.

14.Niederreiter H., Shparlinski I.. Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. *Acta Arith*, 90(1):89–98, 2000.

15.Varbanets S.. Exponential sums on the sequences of inversive congruential pseudorandom numbers. *Šiauliai Math. Semin.*, 3(11):247–261, 2008.

16.Varbanets S.. On inversive congruential generator for pseudorandom numbers with prime power modulus. *Annales Univ. Sci. Budapest, Sect. Comp.*, 29:277–296, 2008.

17. Varbanets P., Varbanets S.. Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus. *VoronoÏ's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Kyiv, Ukraine, September 22-28, 2008*, 4(1):112–130, 2008.
18. Varbanets P., Varbanets S.. Generalizations of Inversive Congruential Generator, Analytic and probabilistic methods in number theory. *Proceedings of the* 5^{th} *international conference in honour of J. Kubilius, Palanga, Lithuania, September 4–10, 2011, Vilnius: TEV.*, 265–282, 2012.

Low Temperature Atmospheric Plasma Applications and Codification of its' Influence on Micro-organisms

Constantine L. Xaplanteris[1,2], Eleni D. Filippaki[1,] John K. Christodoulakis[1,3], Maria A. Kazantzaki[1,2], Evangelos P. Tsakalos[1] and Loukas C. Xaplanteris[3]

[1]Department Plasma Physics Laboratory, Institute of Nanoscience and Nanotechnology (I.N.N.), National Centre for Scientific Research, N.C.S.R. "Demokritos", 15310, Athens, Greece. E-mail: cxaplanteris@yahoo.com
[2]School of Mining and Metallurgical Engineering, National Technical University of Athens, Greece
[3]School of Physics, National and Kapodistrian University of Athens, Greece

Abstract. During the last decade, there has been an increased interestin the use of cold atmospheric plasma (CAP) on bio-chemical applications. Until now, thermal plasma has been commonlyused on many bio-medical and other applications, however more recent efforts have shown that plasma can also be produsedin lower temperature (close to the environment temperature) by using the ambient air in an open space (in atmospheric pressure). However, two aspects remain neglected; low temperature plasma production with a large area firstly, and acquiring the necessary knowledge and understanding on the relevant interaction mechanisms of plasma species with bacterial organisms, secondly. The first aspect has been achieved at "Demokritos" plasma laboratory, with atmospheric plasma being produced at a high pressure but lower than the atmospheric one. Refarding plasma effect on living bacteria,preliminaty experiments and findings have already been carried out and many more have been planed for the near future.
The purpose of this research work is open-air cold atmospheric plasma production with a large area, and the study og the interaction of the important CAP epecies (O_3, O_2, and O atoms)with the major organic bonds (i.e. -C-C-, C-O-, C-N) of the bacteria and other microbes (e.g. Fungus and viruses). In this regard, the ultimate goal of this work becomes the development of a convenient, easy to operate and low-cost device, suitable to be used in a large of fields of materials processing. Of particular importance is its potential application on agricultural products (through drying, sterilization, disinfection and products quality check), making a breakthrough in food processing and safely.

Keywords: Atmospheric Plasma, Animate organisms, Plasma Species, Bio-Chemical Applications, Sterilization, Disinfection.

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

1 Introduction

Even though the artificially produced plasma has been studied and used over the past half century [1-6], it is only in the last two decades that research on its application and influence on micro-organisms have been conducted and results have been published [7-10]. The importance of plasma production was initially recognised during the efforts of thermonuclear fusion attainment. This was because the temperature of plasma electrons is high enough in the range required for thermonuclear fusion [5, 11-13]. Thus, the controlled thermonuclear fusion through plasmatic state was initially seemed an easy process; however, early experiments provided evidence that plasma instabilities exist which do not allow the achievement of fusion attainment. Consequently, more recently efforts have been focused on confronting these waves and thus facilitate nuclear fusion processes. A similar course of research was followed by the Plasma Physics Laboratory at N.C.S.R "Demokritos", with many findings regarding plasma instabilities been published already [14-16].

Alongside the thermonuclear plasma experiments and studies, other plasma applications were also conducted, including the generation of coherent and incoherent radiation, particle beam generation, and material processing. In the last two decades special focus has been given on the study of plasma influence on micro-organisms which is of particular importance in medical and other related sciences [17, 18]. Some examples are given in the last references [19, 20] as well. This influence of plasma on vital organisms is theoretically developed and experimentally examined in this study.

Particularly, here an effort has been made to experimentally study and draw concrete results and conclusions of the glow discharge plasma influence on commonly found fungi, such as yeasts., Firstly, the role of the plasma treatment time on yeast inactivation was examined; the findings gave us the possibility to alter the plasma production parameters so that a desirable effect on vital-organisms may be achieved.

Secondly, the yeast exposed surface size-inactivation rate was studied by yeast cube continuous bisections (segmentations).

An extensive mathematic analysis is given which resulted in the formation of one repeating equation for yeast surface after every last bisection.

Our experimental results showed that, as the yeast exposed surface increases (due to bisections) the inactivation rate increases as well.

An ultimate goal of this research work is to adjust our plasma production devices, to a low temperature semi-open atmospheric plasma device producing low cost plasma. Additionally, , the experience which has been acquired and conduction of more experiments on a range of food products may be proved very significant on food processing industry, especially for the sterilization-disinfection of agriculture products.

The paper is outlined as follow: the experimental is presented in section 2. Where section 2.1

describes the plasma reactor, section 2.2 the yeast used and dough production, and section 2.3 the preliminary plasma treatment experiments. A mathematical

support for this study is given in section 3, where the section 4 reports the experimental results and section 5 provides the interpretation of the results and conclusion. Finally, Appendix A and B contain the mathematical elaboration.

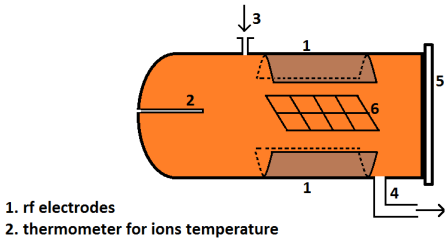
2 Plasma device description- Plasma production- Preliminary experiments

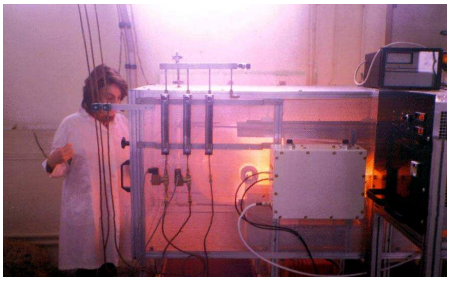
2.1 Plasma device description

Micro-organisms are treated by plasma particle bombardment into the plasma discharge. Various types of plasma discharge are used today, as glow discharge, pulsed discharge and discharge based on the rf radiation at the electron cyclotron frequency (electron cyclotron resonance). Due to its simplicity and effectiveness the most widely used technique is the glow discharge plasma The dc glow discharge is commonly combined with an RF radiation at $10-30 MHz$. The RF radiation gives a sufficient ionization, allowing the glow discharge to be operated at lower air pressure (at the $100 Pa$ value), resulting in fewer collisions into the sheath thus in ions strike with bigger energy.

The laboratory of Plasma physics at "Demokritos" has two glow discharge plasma production devices of different size. The experiments in this research work have been conducted in the one with the biggest capacity. The device used consists of a closed cylindrical tube made from glass (pyrex) within which the plasma is produced. The geometrical characteristics of the glass tube are as following: cylinder length $130 cm$, cylinder inner diameter $42 cm$ and consequently a tube volume of about $180 Lits$. The cylinder flat base which is the metallic door of the tube closes air-tightly.; the other cylinder base is not flat and it has a suitable thermometer sheath. Another opening allows a manometer to be adjusted, while the gases (atmospheric air is used here) enter the tube through one flow meter. A low pressure is achieved by a rotary pump. In addition, two big copper sheets are placed on each side of tube cylindrical-curved surface, for entering the RF power into the device. The RF generator operates at $27{,}12 MHz$. A closed water system is cooling the two electrodes as these are heated from the RF power.

The whole device, which is described previously, is enclosed into a rectangular aluminum netting (Faraday cage) protecting the surrounding area from the rf radiation generated. Figure 1 contains a description of the device, a drawing and a photo during its operation.





(a) (b)

Fig. 1. (a) a schematic representation of the plasma production device, (b) a photo in full plasma operation

2.2 Plasma production

The typical values for plasma production parameters are shown in Table 1.

Table 1. Typical plasma parameters

Plasma parameter	Symbol	Typical value
Pressure	p	100Pa
RF frequency (standard)	f	27,12MHz
RF power	w	1kW
Electron temperature	T_e	13000˚K
Ion temperature	T_i	330˚K
Treatment gas		O_2, N_2
Plasma density	n_e	$10^{13}m^{-3}$

The plasma produced by this way has the following characteristics:
i) The RF signal is of low frequency ($f = 27{,}4KHz$) and consequently long period. That long period is enough to accelerate the electrons to obtain kinetic energy equals the ionization energy.

ii) The plasma cavity has large volume near to $180 lits$
iii) The gas pressure is high ($\approx 100 Pa$).
The last two factors require large gas consumption and the operational cost is consequently high. Thus, the atmospheric air plasma could drastically reduce the gas cost..
Another advantage of this type of plasma production is the absence of magnetic confinement; it is evident that the use of magnets is very costly and inconvenient. The RF produced air plasma (VEPREK method) has the advantage of a symmetrical plasma column, whereas the dc external potential gives an asymmetric plasma shape.

2.3 Preliminary experiments

Although, the experiments are described in detail Sec. 4, it is need to underline here that accurate measurements on micro-organisms are difficult to made, as the biological resistance of different micro-organisms varies. So, the first group of experiments was conducted and effect of plasma on treated organisms was evaluated indirectly, looking at their post-treatment activity. The first data obtained are qualitative to semi-quantitative, and relies on the plasma treatment on yeast used in bread fermentation.

3 Mathematic Support

3.1 The repeating relation

If the yeast cube has edge α then the total surface is $6\alpha^2$.
Then the bisection of this cube into two equal parts yields a surface $8\alpha^2$. Then, if continuously the two yeast parts sub-divided into two equal parts by the same way, then the whole treated surface becomes, $8\alpha^2 + 4\alpha^2 = 12\alpha^2$. In the next cut the exposed surface is, $12\alpha^2 + 8\alpha^2 = 20\alpha^2$. And so on…
Thus, the list may be shaped as following:

$$s_0 = 6\alpha^2$$

$$s_1 = 6\alpha^2 + 2\alpha^2 = 8\alpha^2 \quad \text{or}$$
$$s_1 = s_0 + 2\alpha^2 = 8\alpha^2$$

$$s_2 = 8\alpha^2 + 4\alpha^2 = 12\alpha^2 \quad \text{or}$$
$$s_2 = s_1 + 2^2\alpha^2 = 12\alpha^2$$

$$s_3 = 12\alpha^2 + 8\alpha^2 = 20\alpha^2 \quad \text{or}$$
$$s_3 = s_2 + 2^3\alpha^2 = 20\alpha^2$$

$$s_4 = 20\alpha^2 + 16\alpha^2 = 36\alpha^2 \qquad \text{or}$$
$$s_4 = s_3 + 2^4\alpha^2 = 36\alpha^2$$

$$s_5 = 36\alpha^2 + 32\alpha^2 = 68\alpha^2 \qquad \text{or}$$
$$s_5 = s_4 + 2^5\alpha^2 = 68\alpha^2$$

.....

For ν bisections the following repeating relation is obtained,

$$s_\nu = s_{\nu-1} + 2^\nu.\alpha^2 \qquad (1) \quad \text{(the repeating relation)}$$

The above presented cubes bisections have similar chaotic behavior to bifurcations, when ν bisections the total number N of yeast rectangular parts becomes, $N = 2^\nu$.

Figure 2 shows the first five bisections of the yeast cube and the way of cutting.

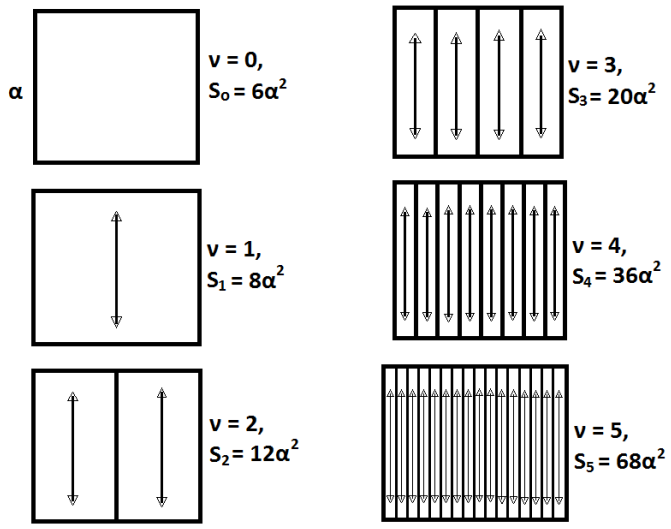


Fig. 2. The first five bisections of the initial yeast cube

The verification of the repeating relation (1) is given in Appendix A, and the plasma exposed surfaces of the five bisections are presented in Fig. 3

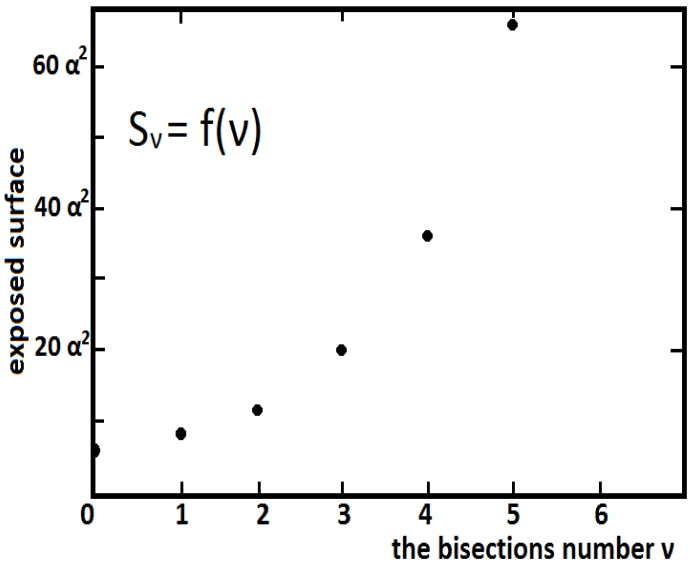


Fig. 3. The exposed surface of the yeast cube for the first five bisections.

3.2 A simpler equation

Another way of finding the relevant mathematic relation which gives the exposed surfaces after ν bisections, is the following:

By relying on the cuts appear on Fig. 2 we have,

$\nu = 0$, $s_0 = 6a^2$

$\nu = 1$, $s_1 = s_0 + 1.2a^2$

$\nu = 2$, $s_2 = s_0 + 3.2a^2$

$\nu = 3$, $s_3 = s_0 + 7.2a^2$

$\nu = 4$, $s_4 = s_0 + 15.2a^2$

…… and for

$\nu = \nu$, $s_\nu = s_0 + (2^\nu - 1).2a^2$

The last relation

$$s_\nu = s_0 + (2^\nu - 1).2a^2 \quad (2)$$

gives the exposed surfaces after ν bisections of the initial cube.

Equation 2 is equivalent to repeating equation 1, however Eq 2 is of more usefulness as it directly calculates the s_ν surface, where the Eq 1 needs a calculate loop to achieve it .

In the Appendix B the proof of the Eq. 2 is given. This is given easily by the repeating relation 1 and having for $\nu = 0,1,2,3....$ and adding by parts.

4 Experimental Data

4.1 The influence of treatment time on the yeast inactivity

It is expected that the treatment time with plasma should affect on the fungus inactivation, thus this was the first which was examined. For this purpose, yeast pieces of equal weight were taken having however different geometric shape. We were able to obtain three different geometric shapes (spherical, cubic and flattened) for examination supplied by a yeast production facility. Next,, the yeast pieces exposed to plasma for different times until they were completely inactive. After plasma treatment the yeasts was mixed with equal weight of flour to make dough and its rise (swelling) was measured. Swelling of the dough was used as measure of active fungus. Measurements on the dough volume (absolute values) were tabulated in the Table 2, whereas, the dough swelling and the associated percentages are calculated and listed in the Table 3. Next, the above results are presented graphically on the Fig. 4,5 and 6 respectively.

It was found that the treatment time for complete inactivation decreases from spherical to cubic to flattened.

The first necessity was to find the order of the magnitude of the treatment time within which the yeast has be inactivated. For this purpose, we used the same type of yeast cubes, eight in number, treated in plasma for different times, and then put them on equal quantities of floury dough. Next we measured changes in each sample volume. We found that as treatment time increases the fungus inactivation increases, leading to a complete inactivation after some time. After this time the volume of the dough remains as if no yeast added.

Table 2. Measurements on the Treatment Time Experiment

Measurement Number	Treatment Time (sec) .	Dough Specimens Volume (*ml*)		
		Spherical	Cubic	Flat

1	0	600	600	600
2	20	500	470	370
3	40	410	360	300
4	60	320	270	240
5	80	280	235	210
6	100	240	210	200
7	120	225	200	200
8	140	200	200	200
9	160	200	200	200

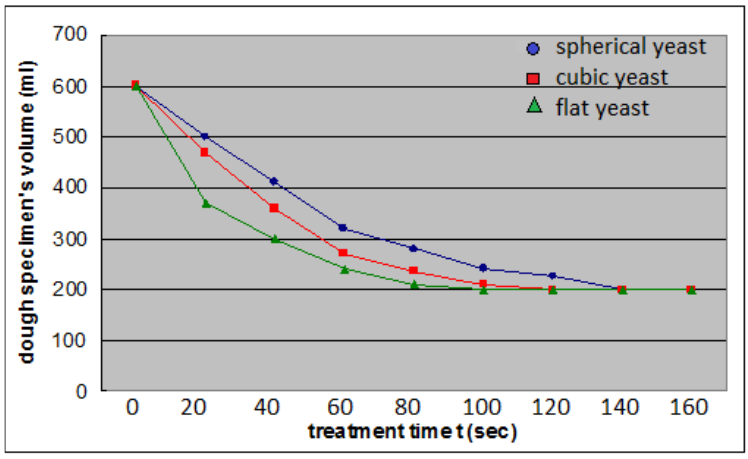


Fig. 4. The dough specimens' volume decreases as the yeast treatment time increases to its initial value V_0 .

Figure 4 shows that in the time $t = 160\,\text{sec}$ the fungus was inactivated completely, as the floury dough retains in its initial bulk ($V_0 = 200ml$).

Table 3. Calculations on the Treatment Time Experiment

Measurement Number	Treatment Time (sec) .	Dough Specimens Swelling (*ml*)		
		Spherical	Cubic	Flat
1	0	400	400	400
2	20	300	270	170
3	40	210	160	100
4	60	120	70	40
5	80	80	35	10
6	100	40	10	0
7	120	25	0	0
8	140	0	0	0
9	160	0	0	0

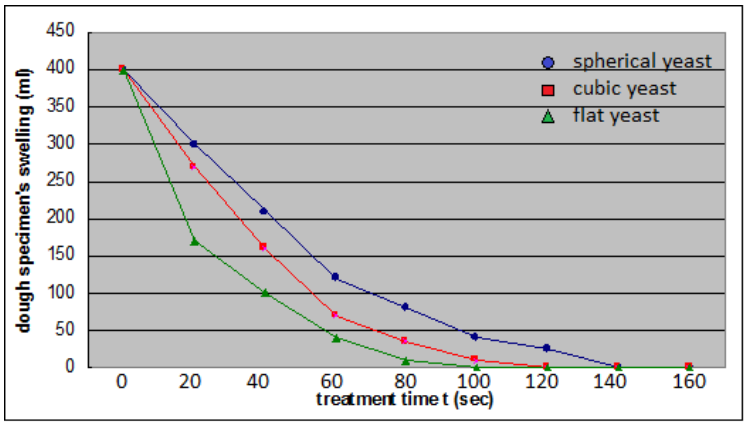


Fig. 5. The dough specimens' swelling decreases as the treatment time increases, until the yeast inactivation becomes complete.

Figure 5 presents the floury dough swelling for spherical cubic and flat yeast during the same treatment time of 60 sec .

Table 4. Calculations on the Treatment Time Experiment

Measurement Number	Treatment Time (sec) .	Dough Specimens Swelling Percentage, (%) Spherical	Cubic	Flat
1	0	200	200	200
2	20	150	135	85
3	40	105	80	50
4	60	60	35	20
5	80	40	17,5	5
6	100	20	5	0
7	120	12,5	0	0
8	140	0	0	0
9	160	0	0	0

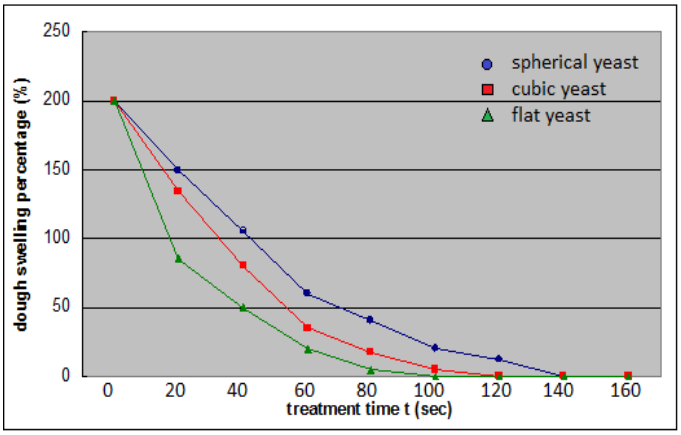


Fig. 6. The dough specimens' swelling percentage as the treatment time increases is show

In the same way the Fig.6 represents the dough swelling percentage for the three geometrical species of the yeast in the same treatment time.

4.2 Exposed surface influence on the yeast inactivity

The next step is to study the influence of the plasma exposed surface of the yeast on the fungus inactivation. In order to do this, we have to use equal weight

yeast cubic only, in five bisections, as these are presented in Fig. 2 and the exposed surfaces are calculated by the Eq.(2). Because the yeast cubic breaks into pieces easily, as the bisections are in progress, it is necessary to use big cubes to secure the fifth bisection; thus, cubes of $m = 50gr$ have been used, and the dough flour is $1000gr$.

The plasma treatment time is much shorter than the $t_{\min}$, which is the complete inactivation treatment time for the flattened yeast (Fig.s 4, 5 and 6). The fungus inactivation was evaluated and measured by the dough swelling, as well. Table 5 and the Fig. 7 present the measurements for the first five bisections and their drawings, respectively.

Table 5. Fungus inactivation by the cubes bisections

Bisection Number	Exposed Surface (α^2).	Dough Specimens Swelling Volume (ml).	Dough Percentage (%).
0	6	3000	200
1	8	2920	192
2	12	2800	180
3	20	2550	155
4	36	2000	100
5	68	1050	5

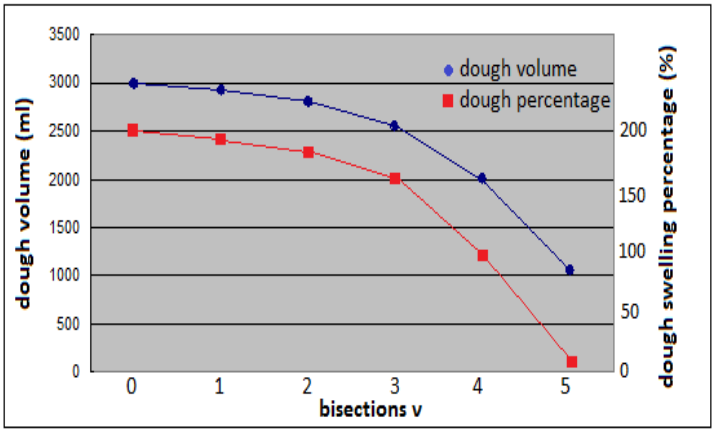


Fig. 7. The dough specimens' volume and swelling (percentage) for the same yeast kind and treatment time but different bisections is presented

It must be noted again that the dough swelling decreases (the fungus inactivation increases, respectively), as the bisections become greater in number.

5 Interpretation of the results- Conclusions

Although the the conducted experiments are preliminary and require further and more profound studying, there are some secure conclusions already; that is noted from the experimental drawings of Fig.s 4,5 and 6, where the changeable quantities always have a semi- exponential form. Thus, the above notice leads us to the following thoughts:

If the initial-original multitude of the active fungus is considered as N_0, then it is impossible to inactivate all this active population by the acts upon plasma instantly· this is achieved, however, within a required time; it is expected for the fungus inactivation to follow an exponential rhythm similarly to the mortality law, according to which the active population is annihilated exponentially as the time passes. If the active population is N on the treatment time t, then the following Eq. (3) gives their relation,

$$N = N_0 .e^{-\lambda t} \quad (3)$$

Where λ is a constant, which is named mortality constant.

The inactive fungus population N' is given from the difference $N' = N_0 - N$, or by the Eq. (4),

$$N' = N_0(1 - e^{-\lambda t}) \quad (4)$$

The next step is to correlate the above thoughts with the experimental data. Thus, the experimental drawings of Fig.s 4,5and 6 must be considered and examined.

As the measuring accuracy permits, the resulted finding from these three Fig.s is that the yeast swelling has an evident exponential diminution as the treatment time passes; this occurs until the complete nihilism of the yeast swelling. The exponential curves in the three Fig.s are considered to have proportionate values with the values of the active fungus population (Eq. 3); thus, the two quantities, the active fungus population N and dough swelling ΔV, must have a linear relation, which is presented with a straight line.

This appears to be very natural for low values of the yeast treatment time, where the phenomenon is into the transit region and the exponential changes have not yet saturated. In these low values of the time, the exponential forms can be approached by a straight line.

A similar interpretation can be given for the experimental findings of the Fig. 7 curve; if it is considered that the inactive fungus population is proportional to the exposed yeast surface (Fig. 3), then the active yeast population is formed similarly to the Fig. 7 curve. Figure 8 shows the inactive and active fungus population, as the yeast bisections increase to $\nu = 5$; it is easy to notice that the active fungus population and the dough swelling (Fig. 7) have a similar mathematic form.

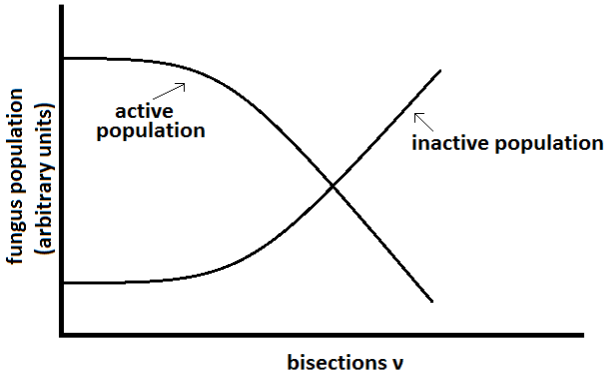


Fig. 8. The active and inactive fungus population, as the bisections increase, is presented

Thus, the relation between the dough swelling and the active fungus population must be linear and this is resulted from the semi-linear region of the exponential curve, which represents the two quantities' relation. This is presented in Fig. 9, where, in the low value region, the relation is linear, although a saturation is expected in the high values.

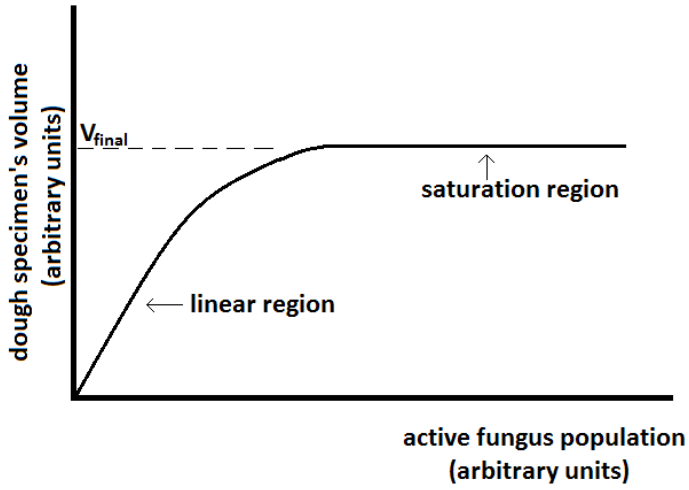


Fig. 9. The dough specimen's volume versus the active fungus population, is given

Acknowledgements

The authors would like to thank the technical personnel of the plasma Laboratory of Demokritos for their assistance during the experiment. Especially Dr Vic J.Law for his proof read and help in the preparation of the manuscript.

Appendix A

Confirmation of the equation (1).

For $\nu = 0$ the relation (1) is written as, $s_0 = s_{0-1} + 2^0.\alpha^2$ or $s_0 = s_{-1} + 1.\alpha^2$,

$6\alpha^2 = s_{-1} + \alpha^2$ when, is resulted, $s_{-1} = 5\alpha^2$.

For $\nu = 1$, is $s_1 = s_0 + 2^1\alpha^2$, $s_1 = 8\alpha^2$

$\nu = 2$, is $s_2 = s_1 + 2^2.\alpha^2$, $s_2 = 12\alpha^2$

$\nu = 3$, is $s_3 = s_2 + 2^3.\alpha^2$, $s_3 = 20\alpha^2$

$\nu = 4$, is $s_4 = s_3 + 2^4.\alpha^2$, $s_4 = 36\alpha^2$

$\nu = 5$, is $s_5 = s_4 + 2^5.\alpha^2$, $s_5 = 68\alpha^2$

…….

and so on.

Appendix B

The type (2) proof

For the Eq. 1 validation to be proved, the repeating equation (1) has to be written for $\nu = 1, \nu = 2, \nu = 3, ... \nu = \nu$, and afterwards to be added by part as below,

$$\$_1 = s_0 + 2^1.a^2$$

$$\$_2 = \$_1 + 2^2.a^2 \qquad +$$

$$\$_3 = \$_2 + 2^3.a^2$$

$$\$_4 = \$_3 + 2^4.a^2$$

$$\cdots\cdots \quad \$_4 \cdots\cdots\cdots\cdots$$

$$\$_{\nu-1} = \$_{\nu-2} + 2^{\nu-1}.\alpha^2$$

$$s_\nu = \$_{\nu-1} + 2^\nu.a^2$$

After the adding the relation is obtained,

$$s_\nu = s_0 + (2^1 + 2^2 + 2^3 + ... + 2^\nu).a^2$$

or

$$s_\nu = s_0 + (2^0 + 2^1 + 2^2 + 2^3 + ... + 2^\nu - 1).a^2,$$

or $$s_\nu = s_0 + (\frac{2^{\nu+1} - 1}{2 - 1} - 1).a^2$$

And finally, the direct equation (2),

$$s_\nu = s_0 + (2^\nu - 1).2.a^2 \quad (2)$$

is obtained.

References

1. L.Spitzer, Physics of fully Ionized Gases, 2nd edn. New York: John Wiley &sons (1967)
2. B.S. Tanenbaun, Plasma Physics, MacGraw-Hill (physical and quantum electronic series) (1967)
3. N. Krall & A. Trivelpiece, Principles of Plasma Physics, McGraw-Hill Kogakusha, LTD (1973)
4.. H.W. Hendel, B. Coppi, F. Perkins and P.A. Politzer, Collisional Effects in Plasmas-Drift-Wave Experiments and Interpretation, Phys. Pev. Lett. 18. 439 (1967)

5. J. Wesson, Tolamaks 2nd edn. Oxford: Clarendon Press. (1997)
6. M. Lieberman and A. Lichtenberg, principles of Plasma Dischargess and Materials Processing. New York John Wiley. (1994)
7. C. Welz, S. Becker, Y. Li et al, Effects of cold atmospheric plasma on mucosal tissue culture, J. Phys. D: Appl. Phys. 46, 045401 (2013)
8. X. Pel, X. Lu, J.Liu et al, Inactivation of a 25.5 μm Enterococcus faecalis biofilm by a room-temperature, battery-operated, handheld air plasma jet, J.. Phys. D: Appl. Phys. 45, 165205 (2012)
9. Liu Xiaohu, Hong Feng, Guo Ying et al, Sterilization of Staphylococcus Aureus by an Atmospheric Non-Thermal Plasma Jet, Plasma Science and Technology 15. 439 (2013)
10. Bong Joo Park, D.H. Lee, J. C. Park et al, Sterilization using a microwave-induced argon plasma system at atmospheric pressure. Physics of Plasmas 10. 4539 (2003)
11. C. E. Alissandrakis, On the Computation of Constant oz Force-free Magnetic Field, Astron. Astrophys. 100,197 (1981)
12. B. B. Kadomtsev, Plasma Physics and the Problem of Controlled Thermonuclear reactors Vol 4, ed M. A. Leontovich New York; Pergamon, (1960)
13. A. B. Mikhailovsky, Theory of Plasma Instabilities, Vol 2: (New York: Consultants Bureau), (1971)
14. A. J. Anastassiades & C. L. Xaplanteris, Drift Wave Instability in the Presence of an RF-Field in a Magnetized Plasma, J. Phys. Soc. Of Jpn 52, 492 (1983)
15. C. L. Xaplanteris, J. Plasma Physics, Collisional instability in a rare magnetized plasma: an experimental model for magnetospheric and space plasma study, Vol. 75, part 3 395 (2009)
16. C. L. Xaplanteris, Effect of Low-Frequency Instability on Hall Conductivity in Plasma, Astrophys. Space Science 139, 233 (1987)
17. S. P. Buzaev, D. V. Bykov, E. V. Evdokimov, et al, International Conference of High- power Particle Beams, Proceedings, Japan, June 25-30, (2000)
18. T. C. Mortie, K. K. Wintenberg and J. R. Fellow, IEEE TRANSACTIONS ON PLASMA SCIENCE, Vol 28, No 1, 41 (2000)
19. J. Tynan, V. J. Law, P. Ward, et al, Comparison of pilot and industrial scale atmospheric pressure glow discharge systems including a novel electro-acoustic technique for process monitoring, .PSST 19(1), 015015, (2010)
20. V. J. Law, A. Ramamoorthy and D. P. Dowling. Real-time process monitoring during the plasma treatment of carbon weave composite materials,. IMSE 1 (2B), 164-169, (2011)

DNS Study on Mechanism of Flow Chaos in Late Boundary Layer Transition

Yong Yang, Jie Tang, Yonghua Yan, Chaoqun Liu
University of Texas at Arlington, Arlington, Texas, USA
Email : cliu@uta.edu

Abstract. The mechanism of chaos in late boundary layer transition is a key issue of the laminar-turbulent transition process. A careful study on the characteristic of chaos is carried out by high order direct numerical simulation (DNS). The process of flow chaos was originally considered as a result of large background noise and non-periodic spanwise boundary conditions. However, according to our DNS observation, the loss of symmetry starts from the middle level vortex rings while the top and bottom rings are still symmetric. The non-symmetric structure of second level vortex rings will influence the small scale vortices at the boundary layer bottom quickly. The loss of symmetry at the bottom of the boundary layer quickly spreads to upper level through ejections. This will lead to chaos of the whole flow field. Therefore, the internal instability of multiple level vortex ring structures, especially the middle ring cycles, is the main reason for the process of flow chaos, but not the large background noise. A new numerical simulation and theoretical analysis is carried out on the multiple level vortex ring package stability. The top package is found stable since it is laid out near the inviscid area and the bottom package is found stable since it is constrained by the solid surface. The middle vortex ring package is found most unstable since there is no constrains to the package. The current analysis is focused on the stability of two rotation cores overlapping, which are moving closer and closer. It is found that the flow becomes more unstable when the two cores are moving closer and closer.

Nomenclature

M_∞ = Mach number
Re = Reynolds number
δ_{in} = inflow displacement thickness
T_w = wall temperature
T_∞ = free stream temperature
Lz_{in} = height at inflow boundary
Lz_{out} = height at outflow boundary
Lx = length of computational domain along x direction

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

Ly = length of computational domain along y direction

x_{in} = distance between leading edge of flat plate and upstream boundary of computational domain

μ_∞ = viscosity

1. Introduction

Turbulence is still covered by a mystical veil in nature after over a century of intensive study. Following comments are made by Wikipedia web page at http://en.wikipedia.org/wiki/Turbulence: Nobel Laureate Richard Feynman described turbulence as "the most important unsolved problem of classical physics" (USA Today 2006). According to an apocryphal story, Werner Heisenberg was asked what he would ask God, given the opportunity. His reply was: "When I meet God, I am going to ask him two questions: Why relativity? And why turbulence? I really believe he will have an answer for the first." (Marshak, 2005). Horace Lamb was quoted as saying in a speech to the British Association for the Advancement of Science, "I am an old man now, and when I die and go to heaven there are two matters on which I hope for enlightenment. One is quantum electrodynamics, and the other is the turbulent motion of fluids. And about the former I am rather optimistic" (Mullin 1989; Davidson 2004).

These comments clearly show that the mechanism of turbulence formation and sustenance is still a mystery for research. Note that both Heisenberg and Lamb were not optimistic for the turbulence study.

The transition process from laminar to turbulent flow in boundary layers is a basic scientific problem in modern fluid mechanics. In order to get deep understanding of the mechanism of the late flow transition in a boundary layer and physics of turbulence, we recently conducted a high order direct numerical simulation (DNS) with 1920×128×241 gird points and about 600,000 time steps to study the mechanism of the late stages of flow transition in a boundary layer at a free stream Mach number 0.5 5 (Chen et al., 2009, 2010a, 2010b, 2011a, 2011b; Liu et al., 1995, 1996, 1997, 2010a, 2010b, 2010c, 2011a, 2011b, 2011c, 2013; Lu et al., 2011, 2011a, 2011b, 2011c, 2012). The work was supported by AFOSR, UTA, TACC and NSF Teragrid. A number of new observations are made and new mechanisms are revealed in late boundary layer transition.

Chaos is a key issue of late boundary layer transition and turbulence formation . This work is devoted to the investigation of the late stages of the laminar-turbulent transition process in a flat-plate boundary layer. As well known, in order to get a fully developed turbulent flow, the following two characteristics should be obtained: 1) small scale vortices; 2) chaos. There are not many existing literatures investigating the mechanism of chaos. Here, we only take those conclusions into account, which were made by Meyer and his co-workers (see Meyer et al 2003). They believe that "the inclined high-shear layer between the legs of the Λ-vortex exhibits increasing phase jitter (i.e chaos) starting from its tip towards the wall region." However, by carefully

checking our DNS data, we observed a phenomenon which is different from the hypothesis given by Meyer and his co-workers.

A λ_2 technology developed by Jeong and Hussain (1995) is used for visualization.

2. Case Setup and Code Validation

2.1 Case setup

The computational domain is displayed in Figure 1. The grid level is 1920×128×241, representing the number of grids in streamwise (*x*), spanwise (*y*), and wall normal (*z*) directions. The grid is stretched in the normal direction and uniform in the streamwise and spanwise directions. The length of the first grid interval in the normal direction at the entrance is found to be 0.43 in wall units (Z^+=0.43). The parallel computation is accomplished through the Message Passing Interface (MPI) together with domain decomposition in the streamwise direction (Figure 2). The flow parameters, including Mach number, Reynolds number, etc are listed in Table 1. Here, x_{in} represents the distance between leading edge and inlet, Lx, Ly, Lz_{in} are the lengths of the computational domain in x-, y-, and z-directions, respectively, and T_w is the wall temperature.

Table 1: Flow parameters

M_∞	Re	x_{in}	Lx	Ly	Lz_{in}	T_w	T_∞
0.5	1000	300.79 δ_{in}	798.03 δ_{in}	22 δ_{in}	40 δ_{in}	273.15 K	273.15 K

2.2 Code Validation

The DNS code – "DNSUTA" has been validated by NASA Langley and UTA researchers (Jiang et al, 2003; Liu et al, 2010; Lu et al 2011) carefully to make sure the DNS results are correct and reliable. For verification purpose, we only show the skin-friction coefficient and velocity profiles in turbulent wall flow with coarse and fine grids. Detailed comparisons between DNS results with linear theory, experimental and other DNS results can be found from our previous publications.

The skin friction coefficient calculated from the time-averaged and spanwise-averaged profile on a coarse and fine grid is displayed in Figure 5. The spatial evolution of skin friction coefficients of laminar flow is also plotted out for comparison. It is observed from these figures that the sharp growth of the skin-friction coefficient occurs after $x \approx 450\delta_{in}$, which is defined as the "onset point". The skin friction coefficient after transition is in good agreement with

the flat-plate theory of turbulent boundary layer by Ducros, 1996 . Figures 3(a) and 3(b) also show that we get grid convergence in skin friction coefficients.

Time-averaged and spanwise-averaged streamwise velocity profiles for various streamwise locations in two different grid levels are shown in Figure 4. The inflow velocity profiles at $x = 300.79\delta_{in}$ is a typical laminar flow velocity profile. At $x = 632.33\delta_{in}$, the mean velocity profile approaches to a turbulent flow velocity profile (Log law) . This comparison shows that the velocity profile from the DNS results is turbulent flow velocity profile and the grid convergence has been realized.

3. Our DNS Observations and Analysis on Chaos

3.1 Derivation of Linear Stability Equation

$$\begin{cases} \dfrac{\partial V}{\partial t} + V \cdot \nabla V = -\nabla p + \dfrac{1}{Re}\nabla^2 V \\ \nabla \cdot V = 0 \end{cases} \tag{1}$$

Equation (1) denotes the incompressible and non-dimensional Navier-Stokes equations in which, $V = (u, v, w)$ is the velocity vector. Considering that

$$q(x, y, t) = q_0(y) + q'(x, y, t) \tag{2}$$

where q can be specified as (u, v, w, p) , and $q_0 = (u_0, v_0, w_0, p_0)$ which represents the value of mean flow, and q' denotes the corresponding linear perturbation. By eliminating the second order perturbation terms, the linearized governing equation for small perturbations can be written as,

$$\begin{cases} \dfrac{\partial V'}{\partial t} + (V_0 \cdot \nabla)V' + (V' \cdot \nabla)V_0 + \nabla p' = \dfrac{\nabla^2 V'}{Re} \\ \nabla \cdot V' = 0 \end{cases} \tag{3}$$

As a first step, a localized 2-D incompressible temporal stability for shear layer is studied. Actually, it relates to the distance among two neighboring vortices in the central streamwise plane. Assume the normal mode is

$$\begin{aligned} V' &= \hat{V}(y)e^{i(\alpha x + \beta z - \omega t)} + c.c. = \hat{V}(y)e^{i\alpha\left(x + \frac{\beta}{\alpha} z - ct\right)} \\ p' &= \hat{p}(y)e^{i(\alpha x + \beta z - \omega t)} + c.c. = \hat{p}(y)e^{i\alpha\left(x + \frac{\beta}{\alpha} z - ct\right)} \\ c &= \frac{\omega}{\alpha} \end{aligned} \tag{4}$$

where the parameter α is given, which is real and set according to the averaged distance between the new generated rings, and c should be a complex number. Plugging Equation (4) in Equation (3) yields

$$\begin{aligned} L\hat{u} &= \mathrm{Re}(Du_0)\hat{v} + i\alpha \mathrm{Re}\hat{p} \\ L\hat{v} &= \mathrm{Re}(D\hat{p}) \\ L\hat{w} &= i\beta \mathrm{Re}\,\hat{p} \\ i(\alpha\hat{u} + \beta\hat{w}) + D\hat{v} &= 0 \end{aligned} \tag{5}$$

where $L = \{D^2 - (\alpha^2 + \beta^2) - i\,\mathrm{Re}(\alpha u_0 - \omega)\}$, and $D = \dfrac{d}{dy}$

Considering in 2D case (without w), and by eliminating $\hat{u}, \hat{p}$, we can obtain the standard O-S equation on $\hat{v}$,

$$(D^2 - \alpha^2)^2 \hat{v} - i\alpha \,\mathrm{Re}[(U_0 - c)(D^2 - \alpha^2) - D^2 U_0]\hat{v} = 0 \tag{6}$$

Equation (6) is about $\hat{v}$, but we need to get the value of c. The value of c determines the property of stability of the equation. Let $c = c_r + ic_i$, if $c_i > 0$, then the disturbance will continuously grow and the flow would be instable. While if c_r is greater, the disturbance will grow faster and the flow would be more unstable. But if $c_i < 0$, the flow would be stable.

3.2 Chebyshev Spectral Method for Linear Stability Analysis

Spectral methods have a significant impact on the accurate discretization of both initial value problems and eigenvalue problems. And spectral method with Chebyshev polynomials has been advantageous, especially in stability analysis of fluid mechanics.

In this stability analysis, the function $\hat{v}$ could be approximated by Chebyshev expansion,

$$\hat{v}(y) = \sum_{n=0}^{\infty} a_n T_n(y) \approx \sum_{n=0}^{N} a_n T_n(y) \tag{7}$$

where N is the number of Chebyshev polynomials used to approximate the velocity profile, T_n are the Chebyshev polynomials and a_n are the coefficients.

After some algebraic work, Equation (6) yields

$$(-U\alpha^2 - U'' - \frac{\alpha^3}{i\,\mathrm{Re}})\hat{v} + (U + \frac{2\alpha}{i\,\mathrm{Re}})\hat{v}'' - \frac{1}{i\alpha\,\mathrm{Re}}\hat{v}'''' = c(\hat{v}'' - \alpha^2\hat{v}) \tag{8}$$

By approximating $\hat{v}$ with a certain Chebyshev expansion, Equation (8) gives

$$\sum_{n=0}^{N}[(-U\alpha^2 - U'' - \frac{\alpha^3}{i\,\mathrm{Re}})T_n + (U + \frac{2\alpha}{i\,\mathrm{Re}})T_n'' - \frac{1}{i\alpha\,\mathrm{Re}}T_n'''']a_n = c\sum_{n=0}^{N}a_n(T_n'' - \alpha^2 T_n) \quad (9)$$

If there is no disturbance at the boundary and it will be free stream outside the domain (a,b), then we have the corresponding boundary condition for function $\hat{v}$ as $\hat{v}(a) = \hat{v}(b) = 0$ and $D\hat{v}(a) = D\hat{v}(b) = 0$.

Applying Equation (9) on the whole grids with boundary conditions above, a matrix form of generalized eigenvalue problem is given by

$$Aa^{(\hat{v})} = cBa^{(\hat{v})} \quad (10)$$

where both A and B are the coefficients' matrix and the vector $a^{(\hat{v})}$ denotes the vector of $\{a_n\}$. c becomes unknown in the generalized eigenvalue of Equation (10).

3.3 Stability Analysis to the Three Velocity Profiles

By solving the general eigenvalue problem for the standard Orr-Sommerfeld equation -- Equation (9) and (10), at $\mathrm{Re} = 1000$ which follows the configuration in the DNS case, the physical solution of the eigenvalue c is obtained. It shows that these three cases are all unstable. Tab.2 gives the value of generalized eigenvalue c in three cases (Figures 6-8) and Fig 9 gives the corresponding profile of eigenvector functions.

case	Distance between two rotation centers	Imaginary part of c
1	2.0	0.71482
2	3.0	0.26741
3	4.0	0.20694

Table 2 Results of c_i for the velocity profile in three cases at Re=1000, $\alpha = 1.0$

By comparison, we can find the image part of c is the greatest in Case 1 and is the least in Case 3. That means the disturbance will grow faster in Case 1 and slower in Case 3. Note that the distance between two rotation centers is growing from Case 1 to Case 3 , and it is reasonable that the disturbance will grow faster and the flow would be more unstable if two rotation centers are closer to each other.

4. Some conclusions and future work

The distribution of averaged streamwise velocity are given in Fig 5 along the normal grid lines at the center plane of a ring-like vortex, whose streamwise position is at $x = 491.1\,\delta_{in}$. The approximations of the base velocity profiles

are given in three cases, see Figs 6-8. The distance between two rotation centers are increased from Case 1 to Case 3.

First, our observation is quite different from Meyer et al (2003.) The phenomenon of asymmetry is first observed at the middle level of the overlapping multiple vortex ring cycles instead of the ring tip. The loss of flow symmetry is also found at the middle part of the flow field in the streamwise direction. The bottom level then loses the symmetry due to the sweeps. Finally, the top flow structure loses the symmetry and the whole flow field becomes chaotic.

The mechanism of chaos in late boundary layer transition is a key issue of the laminar-turbulent transition process. The internal instability of multiple level vortex ring structures, especially the middle ring cycles, is the main reason to cause the asymmetry and then flow chaos, but not the large background noise according to the observation of our DNS computation. A new numerical simulation and theoretical analysis is carried out on the multiple level vortex ring package stability. A two level rotation core overlapping is studied and it is found that the flow becomes more unstable when the two cores are moving closer and closer.

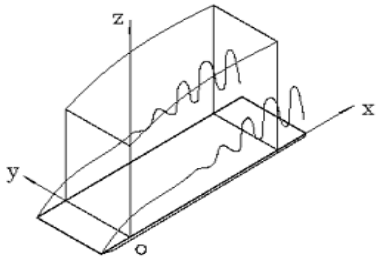


Figure 1: Computation domain

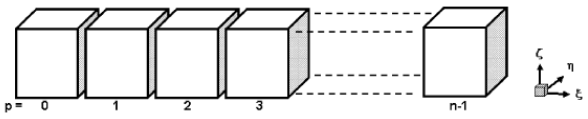
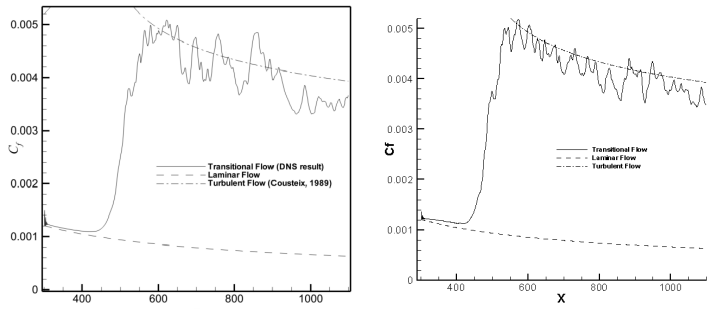


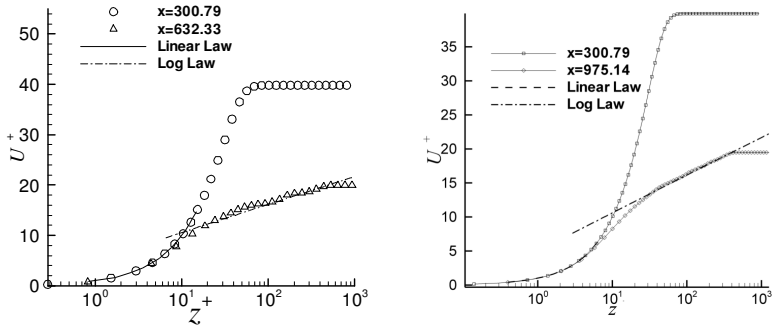
Figure 2: Domain decomposition along the streamwise direction

also show that we get grid convergence in skin friction coefficients.



(a) Coarse Grids (960×64×121) (b)Fine Grids (1920x128x241)

Figure 3: Streamwise evolutions of the time-and spanwise-averaged skin-friction coefficient



(a) Coarse Grids (960x64x121) (b) Fine Grids (1920x128x241)

Figure 4: Log-linear plots of the time-and spanwise-averaged velocity profile in wall unit

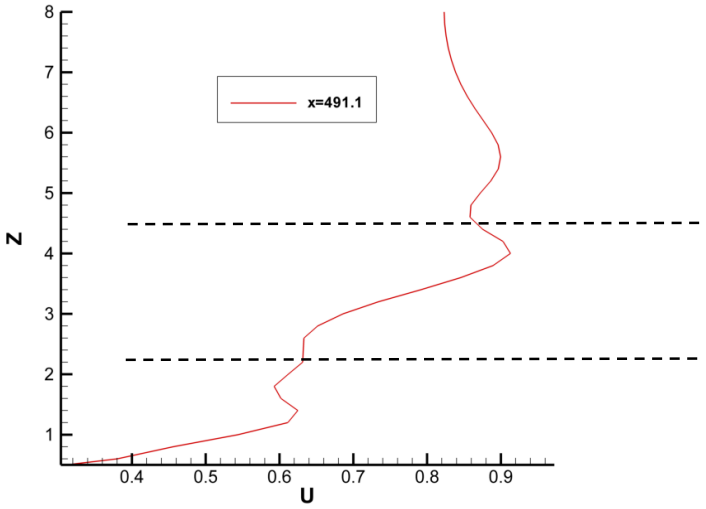
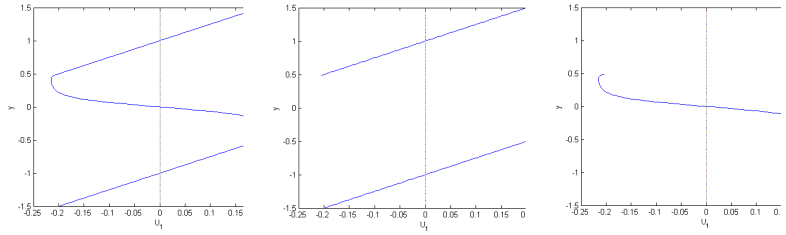
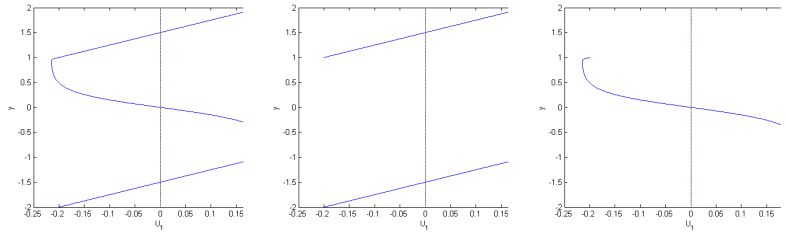


Figure 5: Streamwise Velocity Profile



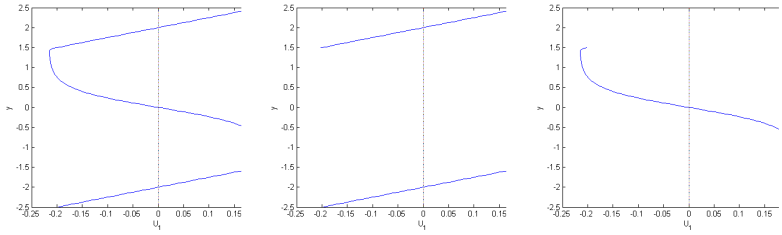
(a) Velocity distribution **(b) Rotational part** **(c) Shear part**

Figure 6: Case 1



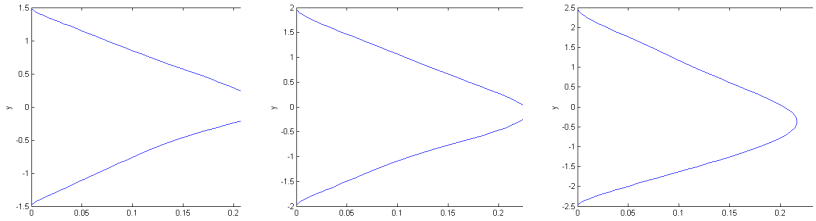
(a) Velocity distribution **(b) Rotational part** **(c) Shear part**

Figure 7: Case 2



(a) Velocity distribution **(b) Rotational part** **(c) Shear part**

Figure 8: Case 3



(a) Case 1 (b) Case 2 (c) Case 3

Figure 9: Corresponding profile of the eigenvector function for three cases

References

[1] Chen, L., Liu, X., Oliveira, M., Tang, D., Liu, C., Vortical Structure, Sweep and Ejection Events in Transitional Boundary Layer, Science China, Series G, Physics, Mechanics, Astronomy, Vol. 39 (10) pp1520-1526, 2009

[2] Chen, L., Liu, X., Oliveira, M., Liu, C., DNS for ring-like vortices formation and roles in positive spikes formation, AIAA Paper 2010-1471, Orlando, FL, January 2010a.

[3] Chen L., Tang, D., Lu, P., Liu, C., Evolution of the vortex structures and turbulent spots at the late-stage of transitional boundary layers, Science China, Physics, Mechanics and Astronomy, Vol. 53 No.1: 1–14, January 2010b,

[4] Chen, L., Liu, C., Numerical Study on Mechanisms of Second Sweep and Positive Spikes in Transitional Flow on a Flat Plate, Journal of Computers and Fluids, Vol 40, pp28-41, 2011a

[5] Chen, L., Liu, X., Tang, D., Liu, C. Evolution of the vortex structures and turbulent spots at the late-stage of transitional boundary layers. Science of China, Physics, Mechanics & Astronomy, 2011 Vol. 54 (5): 986-990, 2011b

[6] Davidson, P. A., *Turbulence: An Introduction for Scientists and Engineers*. Oxford University Press. ISBN 9780198529491, 2004
[7] F. Ducros, P. Comte and M. Lesieur. Large-eddy simulation of transition to turbulence in a boundary layer developing spatially over a flat plate. *J. Fluid Mech*, 326:1-36, 1996;
[8] Jeong J., Hussain F. On the identification of a vortex, J. Fluid Mech. 1995, 285:69-94
[9] Liu, C., and Liu, Z., Multigrid mapping and box relaxation for simulation of the whole process of flow transition in 3-D boundary layers, J. of Computational Physics, Vol. 119, pp. 325-341, 1995.
[10] Liu, Z., Xiong, G., and Liu, C., Direct numerical simulation for the whole process of transition on 3-D airfoils.AIAA paper, AIAA 96-2081, 1996
[11] Liu, C., and Liu, Direct Numerical Simulation for Flow Transition Around Airfoils, Proceedings of First AFOSR International Conference on DNS/LES, Louisiana Tech University, Ruston, Louisiana, August 4-8, 1997.
[12] Liu, C., Chen, L., Study of mechanism of ring-like vortex formation in late flow transition, AIAA Paper 2010-1456, Orlando, FL, 2010a.
[13] Liu, X., Chen, L., Oliveira, M., Tang, D., Liu, C., DNS for late stage structure of flow transition on a flat-plate boundary layer, AIAA Paper 2010-1470, Orlando, FL, January 2010b.
[14] Liu, C., Chen, L., Study of mechanism of ring-like vortex formation in late flow transition, AIAA Paper 2010-1456, Orlando, FL, January 2010c.
[15] Liu, X., Chen, Z., Liu, C., Late-Stage Vortical Structures and Eddy Motions in Transitional Boundary Layer Status, Chinese Physics Letters Vol. 27, No.2, pp.024706-1-4, 2010d
[16] Liu, C., Chen, L., Lu, P., New Findings by High Order DNS for Late Flow Transition in a Boundary Layer, J of Modeling and Simulation in Engineering, Vol 2011,No.721487,pp.1-16 , 2011a
[17] Liu, C., Chen, L., Parallel DNS for vortex structure of late stages of flow transition, J. of Computers and Fluids, Vol.45, pp 129–137, 2011b
[18] Liu, C., Numerical and Theoretical Study on "Vortex Breakdown", International Journal of Computer Mathematics, Vol 88, Issue 17, , pp 3702-3708, 2011c
[19] Liu, C., Chen, L., Lu, P., and Liu, X., Study on Multiple Ring-Like Vortex Formation and Small Vortex Generation in Late Flow Transition on a Flat Plate, Theoretical and Numerical Fluid Dynamics, Vol 27, Issue 1, pp.41-70, 2013
[20] Lu, P., Liu, C., Numerical Study of Mechanism of U-Shaped Vortex Formation, AIAA Paper 2011-0286
[21] Lu, P., Wang, Z., Chen, L. and Liu, C., Numerical study on U-shaped vortex formation in late boundary layer transition Computers & Fluids Vol. 55, pp.36-47,2011a.
[22] Lu, P. and Liu, C., Numerical study on mechanism of small vortex generation in boundary layer transition. AIAA Paper 2011-0287, 2011b

[23] Lu, P. and Liu, C., DNS Study on Mechanism of Small Length Scale Generation in Late Boundary Layer Transition, Physica D: Nonlinear Phenomena, 241 (2012) 11-24, 2011c
[24] Lu, P., Thampa, M, Liu, C., Numerical Study on Randomization in Late Boundary Layer Transition, AIAA 2012-0748, 2012

[25] Marshak, Alex, *3D radiative transfer in cloudy atmospheres; pg.76*. Springer. ISBN 9783540239581, 2005
[26] MEYER, D.G.W.; RIST, U.; KLOKER, M.J. (2003): Investigation of the flow randomization process in a transitional boundary layer. In: Krause, E.; Jäger, W. (eds.): *High Performance Computing in Science and Engineering '03.* Transactions of the HLRS 2003, pp. 239-253 (partially coloured), Springer.
[27] Mullin, Tom, Turbulent times for fluids, *New Scientist*., 11 November 1989
[28] USA Today, Turbulence theory gets a bit choppy, September 10, 2006. http://usatoday30.usatoday.com/tech/science/columnist/vergano/2006-09-10-turbulence_x.htm

A Secure Communication System Based on a Modified Chaotic Chua Oscillator

Mauricio Zapateiro De la Hoz[1], Leonardo Acho[2], and Yolanda Vidal[2]

[1] Universidade Tecnológica Federal do Paraná, Av. Alberto Carazzai 1640, 86300-000 Cornélio Procópio, Paraná, Brazil
(E-mail: hoz@utfpr.edu.br)

[2] Control, Dynamics and Applications Group - CoDAlab. Departament de Matemàtica Aplicada III. Universitat Politècnica de Catalunya, Comte d'Urgell 187, 08036, Barcelona, Spain
(E-mail: leonardo.acho@upc.edu, yolanda.vidal@upc.edu)

Abstract. In this paper we propose a new scheme for secure communications using a modified Chua oscillator. A modification of the oscillator is proposed in order to facilitate the decryption. The communication system requires two channels for transmitting the message. One of the channels transmits a chaotic signal generated by the oscillator and is used for synchronization. The second channel transmits the message encrypted by a nonlinear function. This function is built in terms of one of the chaotic signals, different from that sent on the first channel. In the receiver side, a synchronizer reconstructs the chaotic oscillator signals, one of which is used for the decryption of the message. The synchronization system is designed via Lyapunov theory and chaoticity proves via Poincaré maps and Lyapunov exponents will be provided in order to demonstrate the feasibility of our system. Numerical simulations will be used to evaluate the performance of the system.

Keywords: Chaos, Secure communication, Chua oscillator.

1 Introduction

The possibility to synchronize two coupled chaotic systems has allowed the development of a variety of communication schemes based on chaotic systems. A wide variety of synchronization schemes have been developed since Pecora and Carroll [5], among others, showed it was possible to do so. In this way the use of signals generated by chaotic systems as carriers for analog and digital communications aroused great interest as a potential means for secure communications [1], [4], [9].

There are several works in the literature about chaotic secure communications. For instance, [8] addressed the problems of the chaos synchronization in a secure communication system when the observer matching condition is not satisfied. Zapateiro, Vidal and Acho [11] designed a chaotic communication system in which a binary signal is encrypted in the frequency of the sinusoidal term of a chaotic Duffing oscillator. Fallahi and Leung [2] developed a chaotic communication system based on multiplication modulation. Further examples can be found in [3], [10] and [12], to name a few.

In this paper, we present a new scheme to securely transmit a message using chaotic oscillators. It is based on a modification of the Chua oscillator

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

that allows for a simpler synchronization design and stability demonstration. A Poincaré map and the maximum Lyapunov exponent are presented as proofs of chaoticity of the modified oscillator. This scheme requires two channels for transmission. The encryption/decryption process is based on a modification of the scheme proposed by [13] in which a highly nonlinear function is used along with one of the chaotic signals. The advantage of the scheme is that neither the key signals nor the encrypted signals are transmitted over the channels.

The structure of this chapter is as follows. The problem statement is presented in Section 2. The details of the transmitter and receiver as well as the encryption/decryption blocks are given in Sections 3 - 6. Finally, conclusions are outlined in Section 7

2 Communication system scheme

The diagram of the proposed communication scheme is shown in Figure 1. It consists of the following elements:

1) *Chaotic oscillator*: It is a modified Chua oscillator that generates three signals (x_1, x_2, x_3), two of which are used for synchronization and encryption/decryption purposes.
2) *Encryption block*: It encrypts the message $m(t)$ using a nonlinear function $m_e(t) = \phi(x_2(t), m(t))$.
3) *Channels*: Two channels transmit the chaotic signal and the encrypted message. Channel noise $n_d(t)$ is added. In the receiver side, the signals are filtered with a bank of filters, producing signals $x_{1f}(t)$ and $m_{ef}(t)$.
4) *Synchronization block*: It retrieves the chaotic signals using only one signal from the chaotic oscillator ($x_{1f}(t)$).
5) *Decryption block*: It decrypts the message by using a nonlinear function $m_d(t) = \psi(y_2(t), m_{ef}(t))$. In this case, y_2 is the estimation of the chaotic signal x_2 generated by the synchronization block.
6) *Retrieving block*: In this stage, an algorithm is executed for deciding which message value was sent at an instant $t = t_k$, $k = 1, 2, 3, ...$

The details of the main blocks of the communication system are given in Sections 3 - 5

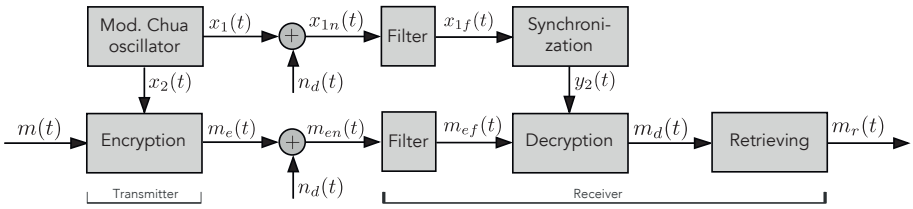


Fig. 1. Block diagram of the proposed communication system.

3 Modified Chua chaotic oscillator

The original Chua oscillator is given by the following set of equations:

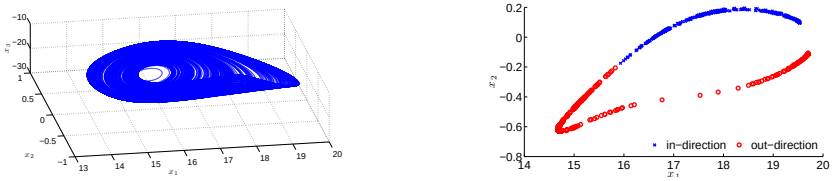
$$\dot{x}_1 = \alpha\,(x_2 - f(x_1))\,, \tag{1}$$
$$\dot{x}_2 = x_1 - x_2 + x_3, \tag{2}$$
$$\dot{x}_3 = -\beta x_2, \tag{3}$$
$$f(x_1) = m_1 x_1 + \frac{1}{2}(m_0 - m_1)(|x_1 + 1| - |x_1 - 1|). \tag{4}$$

where the overdot denotes differentiation with respect to time t; $\alpha > 0$, $\beta > 0$, m_0 and m_1 are parameters that must be chosen appropriately for obtaining chaotic behavior. In this work, we modified the original system by choosing the following characteristic function $f(x_1)$:

$$f(x_1) = -\sin x_1 \cdot e^{-0.1|x_1|}. \tag{5}$$

Note that 5 is a bounded smooth function. The system of Equations 1-3 and 5 is chaotic if $\alpha = 9.35$ and $\beta = 14.35$, as can be seen in Figure 2(a).

Figure 2(b) is the Poincaré map of the modified Chua oscillator generated when the trajectories intersect the plane $x + y + z + 1 = 0$. The map of Figure 2(b) shows the points where the trajectories intersect the plane. The two different markers show if the trajectory goes in one direction or another as it intersects the plane. The map is seen in the XY plane perspective.



(a) (b)

Fig. 2. (a) Dynamics of the modified Chua oscillator. (b) Poincaré map of the oscillator as seen in the XY plane perspective. Trajectories intersecting the plane $x + y + z + 1 = 0$.

Finally, the maximum Lyapunov exponent is calculated as another proof of chaoticity. A positive Lyapunov exponent is a strong indicator of chaos. If a system has at least one positive Lyapunov exponent, then the system is chaotic [7]. In order to determine the maximum Lyapunov exponent λ of the modified Chua oscillator, the algorithm presented in [6] was implemented in Matlab/Simulink. Figure 3 shows how λ evolves until it reaches stability. From these data, it could be found that $\lambda \approx 0.0025$ which confirms the chaoticity of the system.

4 Encryption and decryption

The encryption/decryption scheme proposed by [13] is implemented in our communication system with modified encryption/decryption functions and chaotic oscillator. In this scheme, there are two channels in order to make the synchronization process faster. The encryption/decryption process is as follows [13]:

- *Encryption*: The message $m(t)$ to be sent is encrypted by means of a nonlinear function $\phi : \mathbb{R}^3 \times \mathbb{R} \to \mathbb{R}$ that is continuous in its first argument $x \in \mathbb{R}^3$ and satisfies the following property: for every fixed pair of $(x, m) \in \mathbb{R}^3 \times \mathbb{R}$, theres exists a unique function $\psi : \mathbb{R}^3 \to \mathbb{R}$ that is continuous in its first argument $x \in \mathbb{R}^3$ and is such that $\psi(x, \phi(x, m)) = m$. The encryption function ϕ is built in terms of the chaotic signals. The result is a signal $m_e(t)$ containing the message that is sent through one of the channels.
- *Synchronization*: A synchronization block retrieves the chaotic oscillator signals. It uses only the oscillator signal x_1 from the transmitter oscillator. This signal is sufficient to generate the signals y_1, y_2 and y_3 that are estimations of the oscillator signals x_1, x_2 and x_3, respectively. Retrieving x_2 is necessary for decrypting the message received on the second channel.
- *Decryption*: Once the oscillator signals are retrieved, the decryption function ψ can be used along with the signal $m_{ef}(t)$ in order to get the message $m(t)$.

The functions that we chose in this work to encrypt and decrypt the message are:

$$\phi : \frac{|x_2|}{x_2 + \delta} \cdot m(t) = m_e(t) \tag{6}$$

$$\psi : \frac{y_2 + \delta}{|y_2|} \cdot m_{ef}(t) = m_d(t) \tag{7}$$

where $m_d(t)$ is the decrypted message, as shown in Figure 1 and $\delta > 0$ and small compared to $|x_2|$.

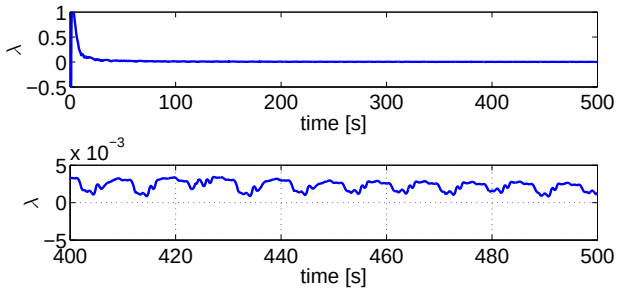


Fig. 3. Top: evolution of the maximum Lyapunov exponent. Bottom: zoom of the upper figure.

5 Synchronization

The synchronization block consists of a dynamic system that takes the signal x_1 and generates the signals y_1, y_2 and y_3 that are estimations of the oscillator signals x_1, x_2 and x_3, respectively.

Theorem 1. *Consider the modified Chua oscillator given by Equations 1 - 3 and 5 with α and β having appropriate positive values that guarantee the chaoticity of the system. Consider also a constant $\rho > 0$ such that $|x_2(t)| < \rho$. Then the system given by:*

$$\dot{y}_1 = k \cdot \mathtt{sgn}(x_1 - y_1), \tag{8}$$
$$\dot{y}_2 = y_1 - y_2 + y_3, \tag{9}$$
$$\dot{y}_3 = -\beta y_2, \tag{10}$$

where k is a design parameter such that $k > \alpha(\rho + 1)$ synchronizes with the modified Chua oscillator and thus:

i) $\lim_{t \to T_s} y_1(t) = x_1(t)$, *for a given* $T_s \in \mathbb{R}^+$.
ii) $\lim_{t \to \infty} y_2(t) = x_2(t)$.
iii) $\lim_{t \to \infty} y_3(t) = x_3(t)$.

Proof. Let the system of Equations 1 - 3 be the master and the system of Equations 8 - 10 be the slave. The function $f(x_1)$ in 5 is such that $|f(x_1)| \leq 1$, $\forall t \geq 0$. Since the system 1 - 3 is chaotic, the signal $x_2(t)$ is bounded and thus, there exists a constant $\rho > 0$ such that $|x_2(t)| \leq \rho \, \forall t \geq 0$. In fact, ρ depends on the initial conditions. However, assuming that $x_2(0)$ lays inside the attractor then ρ can be obtained independently of the initial conditions. The proof begins by defining the following error variable and its derivative:

$$e_1 = x_1 - y_1, \;\; \dot{e}_1 = \dot{x}_1 - \dot{y}_1. \tag{11}$$

Consider the terms $\dot{x}_1$ and $\dot{y}_1$ from Equations 1 and 8, respectively. Substitution of these terms into Equation 11 yields:

$$\dot{e}_1 = \alpha(x_2 - f(x_1))k - \mathtt{sgn}(x_1 - y_1). \tag{12}$$

Let $V_1 = \frac{1}{2}e_1^2$ be a Lyapunov function candidate. Then:

$$\begin{aligned} \dot{V}_1 = e_1\dot{e}_1 &= e_1\alpha x_2 - e_1\alpha f(x_1) - ke_1\mathtt{sgn}(e_1) = -k|e_1| + \alpha x_2 e_1 - \alpha f(x_1)e_1 \\ &\leq -k|e_1| + \alpha x_2 e_1 + \alpha|e_1| \leq -k|e_1| + \alpha\rho|e_1| + \alpha|e_1| \\ &= -|e_1|\left(k - \alpha(\rho + 1)\right). \end{aligned}$$

$\dot{V}_1$ will decrease and converge in finite time if and only if $k > \alpha(\rho + 1)$. Under this condition, there exists a settling time $t = T_s$ such that

$$\lim_{t \to T_s} x_1(t) = y_1(t),$$

and thus $x_1(t) = y_1(t)$, $\forall t \geq T_s$. After $t = T_s$, the synchronization system is completed with the subsystem of Equations 9 and 10. Define two new error variables e_2 and e_3 and their derivatives, as follows:

$$e_2 = x_2 - y_2, \ \dot{e}_2 = \dot{x}_2 - \dot{y}_2,$$

$$e_3 = x_3 - y_3, \ \dot{e}_3 = \dot{x}_3 - \dot{y}_3.$$

From Equations 2 and 9 we have that

$$\dot{e}_2 = x_1 - x_2 + x_3 - x_1 + y_2 - y_3 = -e_2 + e_3.$$

From Equations 3 and 10 we have that

$$\dot{e}_3 = -\beta x_2 + \beta y_2 = -\beta(x_2 - y_2) = -\beta e_2.$$

Rearrange the error variables e_2 and e_3 as a matrix system $\dot{\mathbf{e}} = \mathbf{A}\mathbf{e}$:

$$\begin{bmatrix} \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} = \underbrace{\begin{bmatrix} -1 & 1 \\ -\beta & 0 \end{bmatrix}}_{A} \begin{bmatrix} e_2 \\ e_3 \end{bmatrix}.$$

It is straightforward to show that for all $\beta > 0$, the eigenvalues of matrix $\mathbf{A}$ have negative real parts and thus:

$$\lim_{t\to\infty} y_2(t) = x_2(t), \text{ and } \lim_{t\to\infty} y_3(t) = x_3(t).$$

6 Numerical results

The communication system was implemented in Matlab/Simulink. The transmitter is the implementation of Equations 1 - 3 and 5 with $\alpha = 9.35$ and $\beta = 14.35$. The receiver is the implementation of Equations 8 - 9 with $k = 1000$. The encryption and decryption functions are those of Equations 6 and 7 with $\delta = 0.01$. Noise was added to each signal and thus, a bank of filters was implemented at the input of the receiver so as to clean the signals before their processing. The message signal is assumed to be a two-valued signal that takes the values $m(t) = \{-1, +1\}$. The results to be discussed in what follows were obtained by setting the following initial conditions in the oscillator: $x_1(0) = 15$, $x_2(0) = 0$ and $x_3(0) = -15$. The initial conditions of the synchronizer were: $y_1(0) = 1$, $y_2(0) = 10$ and $y_3(0) = -1$.

Figure 4 compares the signals x_1, x_2 and x_3 of the oscillator in the transmitter side with their estimations y_1, y_2 and y_3 generated by the synchronizer. Figure 4 shows that signals x_1 and y_1 synchronize in a finite time (approximately 0.2 seconds). On the other hand, from Figure 4 we can see that the synchronization of the remaining signals takes around 5 seconds. Given that the signals $y_2(t)$ and $y_3(t)$ have an asymptotic convergence to x_2 and x_3, respectively, it could be expected that some errors might occur when retrieving the message. In order to avoid this problem, we propose sending dummy information in the beginning of the communication so as to avoid losing information.

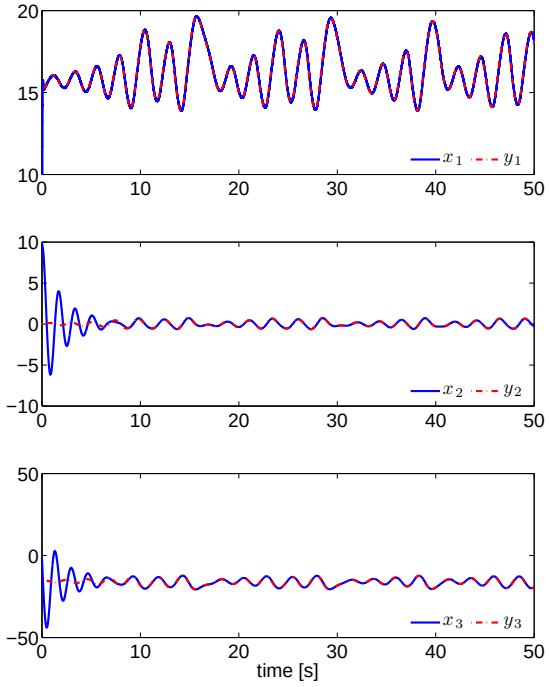


Fig. 4. Comparison of the oscillator signals and their estimations.

Figure 5 is the message that we used for the simulations. For the sake of simplicity, let us call "bit" each possible message value (+1 and −1). Thus, in this test the message $m(t)$ is sent at a rate of $T_b = 1$ bit/second. As can be seen in Figure 5, the dummy information is sent at the beginning of the transmission and afterwards, the true message is sent. Also, the message is passed through a lowpass filter in order to improve the encryption. The filter has the following transfer function:

$$H_e(s) = \frac{1}{s + 100}.$$

In this way we obtain a modified signal $M^*(s) = H_e(s)M(s)$, where $M(s) = \mathscr{L}\{m(t)\}$ and $M^*(s) = \mathscr{L}\{m^*(t)\}$. Figure 6 (top) shows the encrypted message $m_e(t)$, the signal corrupted by channel noise $m_{en}(t)$ and the filtered signal $m_{ef}(t)$. Figure 6 (bottom) shows the message sent in order to observe the differences between the original message and its encryption.

Figure 7 shows the message after the lowpass filter compared to what is obtained after the decryption, i.e. $m_d(t)$. In order to finally retrieve the message, we must determine if the bit corresponds to +1 or −1. This is done at the end of the transmission of every bit, i.e. every T_b^{-1} seconds. In this simulation, we sampled the signal $m_d(t)$ at a rate of $T_r = 0.01$ seconds. So in order to

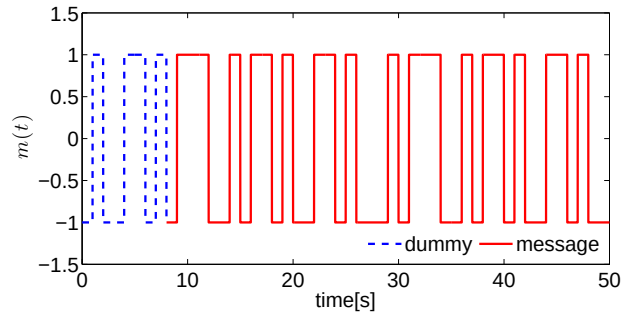


Fig. 5. Message transmitted during the test.

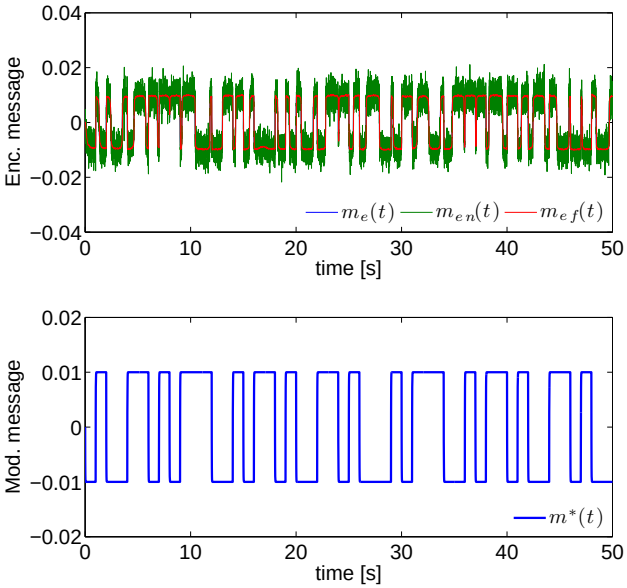


Fig. 6. Top: Encrypted message sent through the channel. Bottom: Original message (filtered).

determine the corresponding bit, we compute the sign of the sample at every instant $t = kT_b^{-1}$, $k = 1, 2, 3, ...$

Figure 8 (top) shows the result of the transmission of the message $m(t)$ which starts at $t = 8$ seconds, after a dummy message, and the retrieved message $m_r(t)$. The blue message is some dummy information sent at the beginning of the transmission in order to avoid incorrect retrieval. The true message is sent from $t = 8$ seconds. The stars in the graphic indicate the retrieved message. Figure 8 (bottom) shows the error between the original message and the retrieved message. Note that all the errors occur in the first 8 seconds of transmission of dummy information.

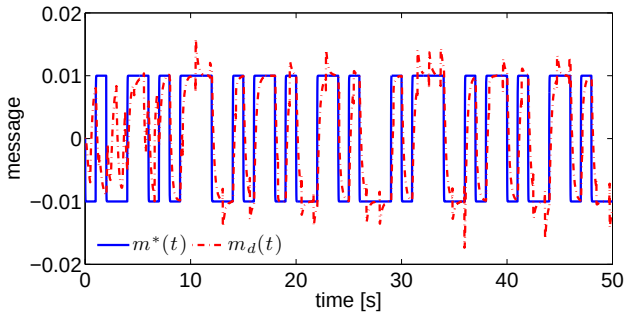


Fig. 7. Comparison between the message sent $m^*(t)$, and the decrypted message $m_d(t)$.

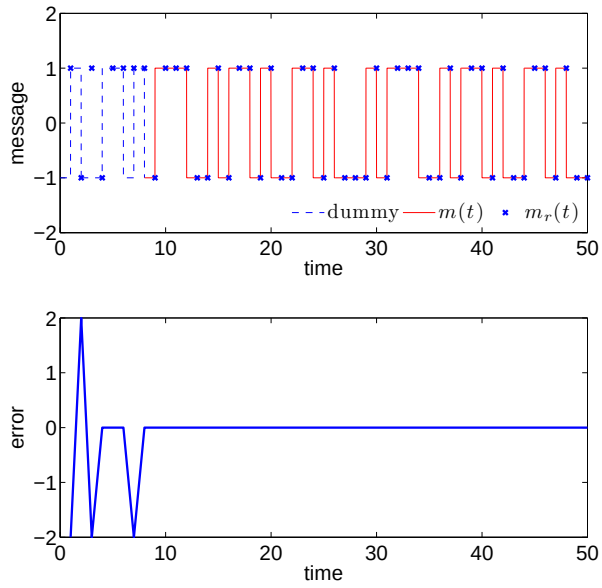


Fig. 8. Top: original and retrieved messages. Bottom: error in retrieved message.

7 Conclusion

In this paper we explored a new secure communication scheme composed of a modified Chua oscillator and an encryption/decryption scheme that makes use of nonlinear functions to encrypt the message. The oscillator characteristic function $f(x)$ was modified to make it bounded. This facilitates the synchronization because only one channel is needed and furthermore, it facilitates the demonstration of the theorem that makes possible the synchronization between the master and the slave. The encryption/decryption scheme used in this work has the advantage that the key signals and encrypted signals do not have to be transmitted over the channel and thus an increase in security is achieved.

Chaoticity proofs of the modified Chua oscillator were provided by means of a Poincaré Map and the maximum Lyapunov Exponent. The feasibility of the system was tested by numerical simulations performed in Matlab/Simulink.

Acknowledgments

Mauricio Zapateiro is supported by the fellowship from CAPES/Programa Nacional de Pos-Doutorado from Brazil. This work has been partially funded by the European Union (European Regional Development Fund) and the Spanish Ministry of Economy and Competitiveness through the research projects DPI2012-32375/FEDER and DPI2011-28033-C03-01 and by the Government of Catalonia (Spain) through 2009SGR1228.

References

1.B. Andrievsky. Adaptive synchronization methods for signal transmission on chaotic carriers, *Mathematics and Computers in Simulation* 58 (46), 285 –293 (2002).
2.K. Fallalih, H. Leung. A chaos secure communication scheme based on multiplication modulation. *Commun. Nonlinear Sci. Numer. Simulat.* 15, pp. 368–383 (2010).
3.C. Hua, B. Yang, G.Ouyang, X. Guan. A new chaotic secure communication scheme *Physics Letters A* 342, pp. 305–308 (2005).
4.O. Morgul, M. Feki. A chaotic masking scheme by using synchronized chaotic systems, *Physics Letters A* 251 (3), 169 – 176 (1999).
5.L. M. Pecora, T. L. Carroll. Synchronization in chaotic systems, *Phys. Rev. Lett.* 64, 821–824 (1990).
6.J. J.Thomsen. Vibrations and Stability : Advanced Theory, Analysis, and Tools, Springer (2003).
7.A. Wolf, J. B. Swift, H. L. Swinney, J. A. Vastano. Determining Lyapunov exponents from a time series, *Physica D* 16, pp. 285–317 (1985).
8.J. Yang, F. Zhu. Synchronization for chaotic systems and chaos-based secure communications via both reduced-order and step by step sliding mode observers, *Communications in Nonlinear Science and Numerical Simulation* 18, pp. 926–937 (2013).
9.T. Yang. A survey of chaotic secure communication systems, *Int. J. Comp. Cognition* 2, pp. 81–130 (2004).
10.T. Yang, L. O. Chua. Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication, *IEEE Transaction on Circuits and Systems-I: Fundamental Theory and Applications* 44(10), pp. 976–988 (1997).
11.M. Zapateiro, Y. Vidal, L. Acho. A secure communication scheme based on chaotic Duffing oscillators and frequency estimation for the transmission of binary-coded messages, *Communications in Nonlinear Science and Numerical Simulation* 19(4), pp.991-1003 (2014).
12.X. Wang, J. Zhang. Chaotic secure communication based on nonlinear autoregressive filter with changeable parameters, *Physics Letters A* 357, pp. 323–329 (2006).
13.J. Zhon-Ping. A note on Chaotic Secure Communication Systems, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 49, pp. 92–96 (2002).

Key agreement protocol based on extended chaotic maps with anonymous authentication

Ping Zhen[1], Geng Zhao[2], Lequan Min [3] and Xiaodong Li[2]

[1] School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing, 100083, China
(E-mail: zhenping1989@126.com)
[2] Beijing Electronic Science and Technology institute, Beijing, 100070, China
(E-mail: zg@besti.edu.cn, lxd@besti.edu.cn)
[3] School of Mathematics and Physics, University of Science and Technology Beijing, Beijing, 100083, China
(E-mail: minlequan@sina.com)

Abstract. Key agreement protocol is used to establish shared secret key for the network system, which is quite important to guarantee secure communication. This paper proposes a two-party key agreement protocol. In order to improve the efficiency and enhance the security, we utilize extended chaotic maps to generate the shared key, which can be used to encrypt and decrypt the transmitted messages in the subsequent communications. The proposed protocol can guarantee anonymity of user's identity and provide mutual authentication. In addition, it also can resist various attacks. The explicit analysis show that the protocol is secure, reliable and applicable in practice.
Keywords: Key agreement protocol, Chaotic maps, Anonymous authentication.

1 Introduction

Key agreement protocols are basic to modern cryptography, which are used to guarantee the security of secret keys which are exchanged over the insecure public network. The shared keys are used in the subsequent communication for encryption, authentication, access control, and so on. In 1976, Diffie and Hellman[1] introduced the first key agreement protocol. However, both of communication parties don't verity the identity of each other and it is vulnerable to man-in-the-middle attack. In order to solve the problem, an authenticated key agreement protocol[2] is proposed. The authenticated key agreement not only allow two parties to agree on a session key, but also ensure the authentication of the participant. Since then, many related key agreement protocols have been proposed[3-5].

Chaotic systems have complicated behaviors, which are sensitive to initial conditions and system parameters, and are not predictable in the long term. These properties, as required by several cryptographic primitives, render chaotic

7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal
C. H. Skiadas (Ed)

systems a potential candidate for constructing cryptosystem. The application of chaotic maps in cryptography has been studied for more than twenty years. There are chaos-based symmetry key cryptosystem[6,7], public key cryptosystem[8,9], Hash functions [10,11], and so on.

In 2005, Xiao et al.[12] proposed a chaos-based key agreement protocol, which utilizes Chebyshev chaotic maps. Alvarez[13] demonstrated this protocol is vulnerable to man-in-the-middle attack. Xiao et al.[5] proposed an improved key agreement to enhance the security, but Han et al.[14] pointed out the improved protocol cannot resist the replay attack. Tseng et al.[15] proposed an anonymous key agreement protocol using smart cards. Niu et al.[16] demonstrated the protocol is vulnerable to the insider attacker and cannot protect user anonymity and then proposed a new key agreement protocol, which is also proved to have low computational efficiency problem by Yoon[17].

Recently, Tan[18] proposed a novel authenticated key agreement protocol with strong anonymity, which is based on smart cards. However, the expense of smart cards and readers will make the protocols costly in practical use. In Ref.[19], Gong et al. proposed a secure chaotic maps-based key agreement protocol without using smart cards and claimed that the protocol is secure. Wang et al.[20] pointed out that there are some problems existing in Gong et al.'s protocol, such as the stolen-verifier attack, forged message flood and key management problems. Then they proposed a new key agreement protocol. We have explicitly analyzed Wang et al.'s protocol. The protocol cannot provide the anonymity of users' identities. But in many insecure channels, especially in e-commerce applications, anonymity is also an very important issue. There also exits key distribution and management problems, which can be easily avoided. Lee et al.[21] proposed a three-party password-based authenticated key exchange protocol with user anonymity. However, the introduced trusted third party not only adds extra overhead, but also becomes another security and performance bottleneck, which will bring potential threats to the system. Motivated by this, this paper proposed a two-party key agreement protocol with anonymous authentication. an anonymous authenticated key agreement protocol based on extended chaotic maps to solve these problems. It doesn't need smart cards and at the same time preserves user anonymity. Besides, "two-party" will decrease the computation and communication cost and at the same time make the protocol secure and efficient. Explicit security analysis and performance analysis of the proposed protocol are also given in this paper.

This paper is organized as follows. Section 2 introduces the preliminaries about extend Chebyshev chaotic maps. Then the proposed two-party key agreement protocol is described in section 3. Security and performance analysis are given in section 4 and section 5 separately. The last section presents the conclusions.

2 Preliminaries

Definition 1. Let $n \in Z^+$ and $x \in [-1,1]$, then a Chebyshev polynomial 0 of order n, $T_n(x):[-1,1] \to [-1,1]$ is defined as:

$$T_n(x) = \cos(n \cdot \arccos(x))$$

It is recursively defined using the following recurrent relation:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), n \geq 2$$

where $T_0(x) = 1$ and $T_1(x) = x$.

The first few Chebyshev polynomials are

$$T_2(x) = 2x^2 - 1$$

$$T_3(x) = 4x^3 - 3x$$

$$T_4(x) = 8x^4 - 8x^2 + 1$$

…

The Chebyshev polynomials exhibit the following important properties: the semigroup property and the chaotic property.

(1) The semi-group property:

$$\begin{aligned} T_r(T_s(x)) &= \cos(r\cos^{-1}(\cos(s\cos^{-1}(x)))) \\ &= \cos(rs\cos^{-1}(x)) \\ &= T_{sr(x)} \\ &= T_s(T_r(x)) \end{aligned}$$

r and s are positive integer numbers and $x \in [-1,1]$.

(2) The chaotic property

When the degree $n > 1$, the Chebyshev polynomial map $T_n(x):[-1,1] \to [-1,1]$ of degree n is a chaotic map with its invariant density $f^*(x) = 1/(\pi\sqrt{1-x^2})$, and positive Lyapunov exponent $\lambda = \ln n > 0$.

To improve security, Zhang[22] proved that the semi-group property holds for extend Chebyshev polynomials defined on $(-\infty, +\infty)$, which can enhance the property, as follows:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \bmod P$$

where $n \geq 2$ and P is a large prime. We can also obtain:

$$T_r(T_s(x)) \equiv T_{sr}(x) \equiv T_s(T_r(x)) \bmod P$$

Definition 2 The discrete logarithm problem (DLP) is explained by the following: Given an element y, the task of DLP is to find the integer s, such that $T_s(x) = y$.

Definition 3 The Diffie-Hellman problem (DHP) is explained by the following: Given the elements $T_r(x)$ and $T_s(x)$, the task of DHP is to compute $T_{rs}(x)$.

It is generally believed that there is no polynomial time algorithm to solve the DLP and DHP problems with non-negligible probability.

Table 1. The notations in the protocol

Notations	Descriptions
ID_i	Identity of client U_i
ID_S	Identity of server S
$E_k(\cdot), D_k(\cdot)$	Secure symmetric encryption and decryption
$H(\cdot)$	Secure one-way hash function
$T_k(\cdot)$	Cheybeshev chaotic map
x	The seed of Chebyshev chaotic map
r, s, r_1, r_2	The degree of Chebyshev chaotic map
PW_i	Password of client U_i
K_S	The secret key of server S
T_1, T_2, T_3	Time stamps
$\Delta T_1, \Delta T_2$	The specified valid time period
sn	The session identifier
KA	The established shared session key

3 The proposed protocol

This section will present our proposed two-party key agreement protocol based on extended Chebyshev chaotic maps. It consists of four phases: (1) the parameter generation phase; (2) the registration phase; (3) the key agreement phase; (4) the password updation phase. For the easy understanding of subsequent content, the commonly used notations are listed in Table 1.

1. Parameter generation phase

In order to perform the protocol, the server S firstly needs to generate some parameters as follow:

(1) S selects a secure symmetric cryptosystem with encryption $E_k(\cdot)$ and decryption $D_k(\cdot)$, where k is the key of symmetric cryptosystem;

(2) S selects a secure one-way hash function $H(\cdot)$;

(3) S select a private key K_S ,which is specialized for client registration.

(4) Utilizes the public key cryptosystem based on Cheybshev chaotic maps, S chooses two random large integers x and s as the seed and degree of Chebyshev maps respectively and computes $T_s(x)$. Then publish $(x, T_s(x))$ as the public parameters and keep s private.

2. Registration phase

The Client U_i with the identity ID_i registers with server S by the following two steps:

(1) U_i selects a password PW_i ,and sends the ID_i and PW_i to S through a secure channel.

(2) After receiving ID_i and PW_i , S use its private key K_S to computes $M_{reg} = H(ID_i, PW_i, K_S)$ and store M_{reg} as the register message securely.

3. Key agreement phase

The client and server need to perform the following four steps to realize mutual authentication and establish a common session key to complete the protocol. The simplified description of the phase is shown in Fig.1. The details are described in the following steps:

(1) $U_i \rightarrow S: M_1 = \{T_{r_1}(x), C_1 = E_{SK}(sn, ID_i, ID_S, PW_i, T_{r_1}(x), T_1)\}$.

U_i selects a random large integer r_1 , and computes $T_{r_1}(x)$ and $SK = T_{r_1}(T_s(x))$. SK is used as the temporary key of symmetric cryptosystem to compute $C_1 = E_{SK}(sn, ID_i, ID_S, PW_i, T_{r_1}(x), T_1)$, where sn is a session identifier and T_1 is a timestamp. Then U_i sends the message $M_1 = \{T_{r_1}(x), C_1\}$ to the server.

(2) $S \rightarrow U_i: M_2 = \{sn, C_2 = E_{SK}(sn, T_{r_2}(x), H_1 = H(KA, ID_S), T_1)\}$.

After receiving the message M_1, S first compute $SK = T_s(T_{r_1}(x))$ and use it to decrypt C_1 . Then S checks whether $|T_2 - T_1| \le \Delta T_1$,where T_2 is the current timestamp and ΔT_1 is the specified valid time period. S continues to compute $M_{reg}' = H(ID_i, PW_i, K_S)$ and validates whether $M_{reg}' = M_{reg}$. If so, S can authenticate the identity of client U_i , otherwise, the process will be terminated immediately. S selects a random large integer r_2 , and computes $T_{r_2}(x)$, $KA = T_{r_2}(T_{r_1}(x))$, $H_1 = H(KA, ID_S)$ and $C_2 = E_{SK}(sn, T_{r_2}(x), H(KA, ID_S), T_1)$. S sends the message $M_2 = \{sn, C_2\}$ to the client.

(3) $U_i \rightarrow S: M_3 = \{sn, H_2 = H(sn, ID_i, KA)\}$.

Upon receiving the message M_2 from S , U_i first decrypts C_2 with the secret key SK . Then U_i checks whether $|T_3 - T_1| \le \Delta T_2$,where T_3 is the current timestamp. U_i computes $KA = T_{r_1}(T_{r_2}(x))$ and $H_1' = H(KA, ID_S)$, and validates whether $H_1' = H_1$. If so , U_i will authenticate the identity of S . Any fail will lead to the termination of the protocol. U_i continues to compute $H_2 = H(sn, ID_i, KA)$ and sends $M_3 = \{sn, H_2\}$ to the server.

(4) Having received the message M_3 from the client U_i , S will compute $H_2' = H(sn, ID_i, KA)$ and check whether $H_2' = H_2$. If so, the server S can affirm that U_i has received KA and KA will be the common session key used in the subsequent communications.

4. Password updation phase

If the client U_i want to update the password, U_i and S need to perform the following steps:

(1) U_i selects a random large integer r , and computes $T_r(x)$ and $K_{PW} = T_r(T_s(x))$. Similar with the first step in key agreement phase, K_{PW} will be used as the temporary key of symmetric cryptosystem. Then U_i encrypts $C_{PW} = E_{K_{PW}}(ID_i, PW_i, PW_i', T_r(x))$ and sends and $M_{PW} = \{T_r(x), C_{PW}\}$ to the server, where PW_i' is the updated password.

(2) Having received the message M_{PW} from U_i , S firstly computes $K_{PW} = T_s(T_r(x))$ and decrypts M_{PW}. Then S checks the validity of ID_i and PW_i. If so, then S continues to computes $M_{reg}' = H(ID_i, PW_i', K_S)$ and store M_{reg}' as the updated register message securely.

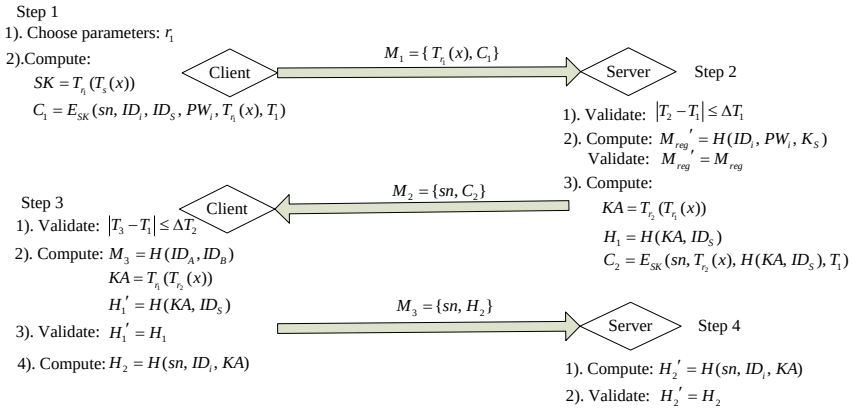


Fig. 1. The key agreement phase of the proposed protocol

4 Security analysis

In this section, we will analyze the security of the proposed protocol and show it can resist various attacks. Here, we claim that our protocol satisfy the following security properties:

(1) **Identity anonymity** With the popularization of internet application, identity privacy has become an important requirement. Identity anonymity means that in the key agreement phase, the attacker cannot find the information about user's ID by intercepting the communication messages. The attacker may eavesdrop the communication channel and try to find some sensitive information to trace the real identity. In the proposed protocol, the identity of Client and Server are encrypted by secure symmetric cryptosystem $C_1 = E_{SK}(sn, ID_i, ID_S, PW_i, T_{r_1}(x), T_1)$. In order to decrypt , the attack need the temporary secret key , which involve the DHP difficult problem mentioned in section 2. Only the server can decrypt the message and get the identity information. Thus, anonymity can be achieved during the key agreement phase.

(2) **Mutual authentication** The goal of mutual authentication is to confirm both the identities of the client and server and establish a common shared session key between them. In step 2 of the key agreement phase, only the server can decrypt the message $C_1 = E_{SK}(sn, ID_i, ID_S, PW_i, T_{r_1}(x), T_1)$ and authenticate the identity of the client by comparing the ID_i and PW_i with registered message M_{reg} . Client can authenticate the identity of server by the session identifier sn and comparing hash value $H_1' = H(KA, ID_S)$. The illegal attacker may modify the communication messages being transmitted over an insecure network. It is extremely difficult for the attacker to fabricate the false authentication information and any message modification during transmission will be detected by the protocol participant. So the proposed protocol can achieve the mutual authentication.

(3) **Resistance to tamper attacks** A tamper attack is an attempt by an adversary to modify information in an unauthorized manner. This is an attack against the integrity of the information. We have stressed the problem in the analysis above and will explain how our protocol can resist this attack in this part. In the key agreement phase, the session identifier sn and $T_{r_1}(x)$ are transmitted in the plaintext form and ciphertext form, respectively, which is used to validate whether the plaintext or cipherctext is being tampered. What is more, hash function is also utilized to further realize message integrity. If the adversary forges the message, the receiver can detect it by checking Hash value immediately. This leads to the termination of the protocol. According to the analysis, our protocol can resist the tamper attacks.

(4) **Fairness in the key agreement** The property fairness in the key agreement is also called the contributory property, which means that the session key is determined cooperationally by both the communicating parties. In 0, the author has given a strictly formal definition. The fairness in key agreement means that any communicating party cannot decide a shared session key in advance. In this protocol, we can see client and server choose random integers r_1 and r_2 separately. Through the commutative property of extended Chebyshev chaotic map, they can compute the shared session

key $KA = T_{r_1}(T_{r_2}(x)) = T_{r_2}(T_{r_1}(x))$. Therefore, the protocol can ensure the fairness in the key agreement.

(5) **Resistance to man-in-the-middle attack** Man-in-the-middle means that an active attacker intercepts the communication messages between communication participants and adopts some special means to successfully masquerade as the both parties communicate with each other. From previous analysis, the attack even doesn't know the identities of communicating parties since they are kept anonymous and any modification to the transmitted message will be detected. So the attacker cannot impersonate one participant to another during key agreement process. Therefore, the proposed protocol can withstand man-in-the-middle attack.

(6) **Resistance to replay attack** A replay attack is an offensive action in which an adversary impersonates or deceives another legitimate participant through the reuse of information obtained in a protocol. The proposed protocol can resist the replay attacks, which is realized by using the session identifier *sn* and time stamps (T_1, T_2, T_3). Time stamp is attached to verify freshness of every transmitted message. Furthermore, it cannot be modified because it is encrypted during transmission process. Thus, it is impossible for the replayed message to pass the verification with incorrect session identifier and timestamp. Therefore, our protocol can resist replay attack.

(7) **Resistance to password-based attacks** Dictionary attack is always used to crack the password in the protocol. There are three kinds of dictionary attack[21]: Off-line dictionary attack, undetectable on-line dictionary attack and detectable on-line dictionary attack. Both off-line and undetectable on-line dictionary attack can cause serious consequences among them. In the key agreement phase, the attacker needs to decrypt the message $C_1 = E_{SK}(sn, ID_i, ID_S, PW_i, T_{r_1}(x), T_1)$ to steal the password PW_i. To obtain the secret key SK, the attack faces the DHP difficult problem. So the attacker cannot launch any of these attacks. Therefore, our protocol is quite effective to resist password-based attacks.

(8) **Resistance to stolen-verifier attack** Then stolen-verifier attack means that an adversary who steals the password verification information from the server can use it directly to masquerade as a legitimate user in authentication phase[16]. In the protocol, we assume the registered message $M_{reg} = H(ID_i, PW_i, K_S)$ is safely stored by the server and cannot be accessed by the attacker. Even if it is stolen, the attacker still cannot carry out the stolen-verifier attack to get the client's password PW_i without the server's secret key K_S. So the secret key K_S can strength the security of password and resist the stolen-verifier attack.

(9) **High efficiency in key distribution and management** It need Server S to publish its public parameters $(x, T_s(x))$ and store the registered value $M_{reg} = H(ID_i, PW_i, K_S)$. Each entity only needs to keep his own password PW_i. This will improve the performance of the key distribution.

What's more, the symmetric secret keys SK are established temporarily utilizing the Chebyshev semigroup property and will be altered in each session according to the selected random numbers r_1 .So the communication entity does not need to store SK and it can decrease the key management cost and strengthen the security.

5 Performance analysis

In this section, we will compare the performance and security of our protocol with Tseng et al.'s protocol[15] and Wang et al.'s protocol[20]. For the convenience of evaluating the computational complexity, let T_X , T_S , T_C and T_H be the computation cost of one XOR operation, one symmetric encryption/decryption operation, one Chebyshev polynomial computation and one Hash operation, respectively. From table 2, we can see that our key agreement protocol need $(T_S + T_C)$ more computation cost for the client and $(T_S + T_C + T_H)$ more for the server than Wang et al.'s. In practical use, symmetric encryption/decryption and hash function can be quite efficient. As for the Chebyshev operation, the authors in[5,24,25] gave some implementation methods to decrease the computational cost. Our protocol provides user anonymity and can be more efficient in key distribution and management compared to Wang et al.'s protocol. What's more, our two-party protocol can decrease the communication cost. Our protocol only needs 3 times message transmission, which the number is 4 in Wang et al.'s protocol.

Table 2: Performance analysis and comparisons

	Tseng et al.'s	Wang et al.'s	Our protocol
User anonymity	No	No	Yes
Mutual authenticity	No	Yes	Yes
Fairness	Yes	Yes	Yes
Man-in-the-middle attack	No	No	No
Replay attack	No	No	No
Password-based attack	No	No	No
Stolen-verifier attack	No	No	No
Cost of Client	$2T_X + 2T_S + 2T_C + 5T_H$	$T_s + 2T_C + 2T_H$	$2T_s + 3T_C + 2T_H$
Cost of Server	$T_X + 2T_S + 2T_C + 3T_H$	$T_s + 2T_C + 2T_H$	$2T_s + 3T_C + 3T_H$

Conclusions

In this paper, we propose a two-party key agreement protocol based on extended chaotic maps. It securely establishes a shared session key, and provides identity anonymity and mutual authentication at the same time. It is demonstrated that

the protocol can resist various attacks, such as man-in-the-middle attack, replay attack, stolen-verifier attack, and so on. The protocol is also very efficient in key distribution and management. Compared with some previously proposed protocols, our protocol has shown its advantage in security and efficiency, which can be applicable in practical use. However, the two-party party protocol may not be suitable in large peer-to-peer network situations, which still needs further research.

Acknowledgements

The authors would like to thank the anonymous reviewers for helpful comments and suggestions. This research is supported by the National Natural Science Foundation of China (No. 61170037) and the specialized Research Fund for Doctoral Program of Higher Education of China (No. 06198016).

References

1. W. Diffe, Hellman, and M. E., New directions in cryptography, IEEE Trans. Inf. Theory, vol.22, no.6, pp. 644-654, 1976, doi:10.1109/TIT.1976.1055638.
2. M. Bellare, D. Pointcheval and P. Rogaway, Authenticated key agreement secure against dictionary attacks, Advances in Cryptography, Eurocrypt'00, Bruges, Belgium. LNCS, 2000, vol. 1807, pp. 139-155.
3. T. Y. Change, W. P. Yang and M. S. Hwang, Simple authenticated key agreement and protected password change protocol, Comput. Math. Appl., vol.49, no.5-6, pp.703-714, April-May 2005, doi: 10.1016/j.camwa.2004. 11.007.
4. T. Y. Change, M. S. Hwang, and W. P. Yang, A communication efficient three-party password authenticated key exchange protocol, Inf. Sci., vol.181, no.1, pp.217-226, January 2011, doi: 10.1016/j.ins.2010. 08.032.
5. D. Xiao, X. F. Liao and S. J. Deng, A novel key agreement protocol based on chaotic maps, Inf. Sci., vol.177, no.4,15, pp. 1136-1142, February 2007, doi: 10.1016/j.ins.2006.07.026.
6. H. Liu and X. Wang, Color image encryption based on one-time keys and robust chaotic maps, Computers & Mathematics with Applications, vol.59, no.10, pp.3320-3327. May 2010, doi: 10.1016/j.camwa.2010.03.017.
7. W. Zhen, H. Xia, L. Ning and S. X. Na, Image encryption based on a delayed fractional-order chaotic logistic system, Chin. Phys. B, , Vol. 21, No.5, 2012, doi: 10.1088/1674-1056/21/5/050506.
8. B. Ranjan, Novel public key encryption technique based on multiple chaotic systems, Phys. Rev. Lett, vol.95, no.9, pp. 098702, September, 2005, doi:10.1103/Phys RevLett. 95.09870.
9. L. Kocarev and Z. Tasev, Public-key encryption based on Chebyshev maps, In: Proceedings of the IEEE international symposium on circuits system, 25-28 May 2003, vol.3, pp.28-31, doi: 10.1109/ISCAS.2003.1204947.
10. Y. Wang, X. F. Liao, D. Xiao D and K. W. Wong, One-way Hash function construction based on 2D coupled map lattices, Inf. Sci., vol.178, no.5, pp.1391–1406, March 2008, doi: 10.1016/j.ins.2007.10.008.

11. M. Amin, O. S. Faragallah, A. A. A. El-latif, Chaos-based Hash function (CBHF) for cryptographic applications, Chaos Solitons & Fractals, vol.42, no.2,30, pp.767–772, October 2009, doi: 10.1016/j.chaos.2009. 02.001.
12. D. Xiao, X. F. Liao and K. W. Wong, An efficient entire chaos-based scheme for denial authentication, Chaos Solitons & Fractals, vol.23, no.4, pp.1327-1331,February 2005, doi: 10.1016/j.chaos.2009.02.001.
13. G. Alvarez, Security problems with a chaos-based denial authentication scheme, Chaos Solitons & Fractals, vol.26, no.1, pp.7-11, October 2005, doi: 10.1016/j.chaos. 2004.12.023.
14. S. Han and E. Chang, Chaotic map based key agreement with/out clock synchronization, Chaos Solitions & Fractals, vol.39, no.3, pp.1283-1289, February 2009, doi: 10.1016/j.chaos.2007.06.030.
15. H. Tseng, R. Jan, and W. Yang, A chaotic maps-based key agreement protocol that preserves user anonymity, In: IEEE Inter. Conf. Commun., ICC'09, Dresden, Germany, 14-18 June 2009, pp. 1-6, doi: 10.1109/ICC.2009.5198 581.
16. Y. Niu and X. Y. Wang, An anonymous key agreement protocol based on chaotic maps, Commun. Nonlinear Sci. Number. Simul., vol.16, no.4, pp.1986-1992, April 2011, doi: 10.1016/j.cnsns.2010.08.015.
17. E. J. Yoon, Efficiency and security problems of anonymous key agreement protocol based on chaotic maps, Commun. Nonlinear Sci. Number. Simul., vol.17, no.717, pp.2735-2740, July 2012, doi: 10.1016/j.cnsns. 2011.11.010.
18. Z. Tan. "A chaotic maps-based authenticated key agreement protocol with strong anonymity," Nonlinear Dyn., vol.72, no.1-2, pp. 311-320, April 2013, doi: 10.1007/s11071-012-0715-5.
19. P. Gong, P. Li and W. Shi, A secure chaotic maps-based key agreement protocol without using smart cards, Nonlinear Dyn., vol.70, pp. 2401-2406, 2012, doi: 10.1007/s11071-012-0628-3.
20. X. Y. Wang and D. P. Luan, A secure key agreement protocol based on chaotic maps, Chin. Phys. B., vol.22, no.11, 2013, doi: 10.1088/1674-1056/22/11/110503.
21. C. C. Lee, C. T. Li and C. W. Hsu, A three-party password-based authenticated key exchange protocol with user anonymity using extened chaotic maps, Nonlinear Dyn., Vol.73, no.1-2, pp.125-132, July 2013, doi: 10.1007/s11071-013-0772-4.
22. L. Zhang, Cryptanalysis of public key encryption based on multiple chaotic systems, Chaos Solitons & Fractals, vol.37, no.3, pp.669-674, August 2008. Doi: 10.1016/j. chaos.2006.09.047.
23. A. C. Yao and Y. Zhao, Computationally-Fair group and identity-based key-exchange, Proceedings of the 9th international conference on Theory and Application of Models of Computation, TAMC'12, Beijing, China, May 16-21, 2012, pp.237-247, doi: 10.1007/978-3-642-29952-0_26.
24. X. Y. Wang and J. F. Zhao, An improved key agreement protocol based on chaos, Commun. Nonlinear Sci. Number. Simul., vol.15, no.12, pp.4052-4057, December 2010, doi: 10.1016/j.cnsns.2010.02.014.
25. Z. H. Li, Y. D. Cui and H. M. Xu, Fast algorithms of public key cryptosytem based on Chebyshev polynomials over finite field, The Journal of China Universities of Posts and Telecommunications, vol.18, no.2, pp.86-93, April 2011, doi: 10.1016/S1005-8885(10)60049-0.