BARC

N E W S L E T T E R

CHAOS BASED CRYPTOGRAPHY : A NEW APPROACH TO SECURE COMMUNICATIONS

Q.V. Lawande
Theoretical Physics Division

and

B. R. Ivan and S. D. Dhodapkar
Reactor Control Division

Introduction

Cryptography is the science of protecting the privacy of information during communication under hostile conditions. In the present era of information technology and proliferating computer network communications, cryptography assumes special importance. Cryptography is now routinely used to protect data, which must be communicated and/or saved over long periods, to protect electronic fund transfers and classified communications.

Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos is another paradigm, which seems promising. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. The chaotic behaviour is a subtle behaviour of a nonlinear system, which apparently looks random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes. The important characteristics of chaos is its extreme sensitivity to initial conditions of the system.

Contents

It was realised in the early 1990's that securing communications could be a potential application emerging out of studies on chaos theory. This was based on the discovery of chaotic synchronization principles, by Pecora & Carroll [1]. These works motivated communication and signal processing engineers and scientists to look into this. The defining properties of chaotic dynamics, namely, ergodicity, sensitivity on initial conditions and system parameters, are in fact the key features contributing towards building up of secure communication schemes based on chaos. In this context, many hardware circuits were proposed and built [2 - 4].

Interest in chaos based systems as an alternative to the existing schemes, such as RSA/ECC etc., in cryptography is increasing in the past few years. The subtle chaotic behavior can be simulated in the simplest of one or two-dimensional systems represented by discrete maps or in higher dimensional physical systems described by three or more first order autonomous differential equations or two or more first order ordinary non-autonomous differential equations.

A large number of chaotic systems, both physical and mathematical, are now available which could potentially serve as both hardware and software equipments for realising encryption and decryption of messages. According to May [5], simple nonlinear systems following iterative dynamics are potential generators of complicated dynamics. It is this dynamics which assumes importance in encryption/decryption algorithms of cryptography.

In chaotic synchronization of analog devices, the stability and drifts are important practical hurdles, which are to be overcome before application of synchronization-based schemes for crypto-graphy. In contrast, a software approach becomes more practical and in tune with present day advances in information processing. A synchronization-based scheme involves the chaotic signal carrier which is prone to cryptographic attack, via a possible break of

cipher using reconstruction dynamics approach [6]. An attempt has been made to overcome this defect in the work described in this paper.

Software schemes involving direct encryption of the trajectories using hopping Logistic map by Arvind et. al [7] and generation of multiple keys using chaotic functions by Bose et. al [8] have been proposed recently. A large number of schemes are available in literature exploiting chaotic functions for direct encryption using the system parameters as keys. However, a novel approach based on the ergodic nature of chaotic trajectory was suggested by Baptista [9]. It uses the Logistic map with two of its parameters for chaotic encryption. A new encryption scheme [10] based on Lorenz dynamics was developed, which extends Baptista's method to Lorenz system [11]. The new scheme is further enriched to guard against reconstruction dynamics and statistical attack. This scheme has been tested for different types of textual messages leading to faithful message recovery.

Chaos based cryptography is still in its infancy and may not have exact parallelism to concepts and notions of traditional cryptographic and cryptanalysis approaches. In such a situation, our approach has been to enhance security of the scheme by providing larger key space, protection against reconstruction dynamics and resistance from statistical attack. Proving the security of encryption based on chaos is still an open topic because one cannot use the analytical methods of classical cryptography which are based on number theoretic concepts or hardness of discrete logarithmic problem, etc. Before the details on the proposed modifications of the Baptista method in this scheme are presented, a short review on Chaos is given below. (See box for cryptographic definitions.)

Chaotic systems

Chaos is one of the possible behaviours associated with evolution of a nonlinear physical system and occurs for specific values of system

parameters. The discovery of this apparently random behaviour ensuing out of deterministic systems turned out to be quite revolutionary leading to many issues interconnecting stability theory, new geometrical features and new signatures characterising dynamical performances.

Special Properties of Chaotic Systems

Systems which are basically nonlinear and exhibiting an apparently random behaviour for certain range of values of system parameters are referred to as Chaotic. However, the solutions or trajectories of the system remain bounded within the phase space. This unstable state has a strong dependence on the values of the parameters and on the way the system begins. The following properties characterise chaotic dynamics.

Cryptographic Definitions

Basic definitions and concepts in Cryptography are reviewed here.

- **Plaintext** denoted by M [a stream of bits, a text file, a bitmap, a stream of digitized voice, digital video image, etc.]
- **Encryption:** Process of disguising a message M so as to hide its contents
  $E_k (M) = C$, E denotes the encryption function and k is key
- **Ciphertext:** an encrypted message denoted by C.
- **Decryption:** Process of converting Ciphertext back into Plaintext
  $D_k (C) = M$, D denotes the decryption function and k is key
- **Cryptanalysis :** The art & science of breaking Ciphertext

Encryption & Decryption Keys

It is normal for cryptographic algorithms to be publicly known. The secrecy is ensured by use of parameters called keys for encryption and decryption, which are only known to sender and receiver. Keys could be one or many depending on cryptographic algorithm. The set of permissible values that keys can take is called a key space.

Symmetric & Asymmetric Keys

If the same keys are used for encryption or decryption, we call it symmetric cipher, i.e.,

$E_k (M) = C$
$D_k (C) = M$

In case of asymmetric cipher we have a key pair (k_1 , k_2), k_1 being public & k_2 private, then

$E_{k1} (M) = C$
$D_{k2} (C) = M$

Sensitivity to initial conditions

Given an initial state of a deterministic system [nonlinear system, in general], it is well known that the future states of the system can be predicted. However, for chaotic systems, long-term prediction is impossible. For specific values of parameters, two trajectories, which are initially very close, diverge exponentially in a short time. Initial information about the system is thus completely lost.

Ergodicity

Ergodicity is that property in which a trajectory in phase space comes arbitrarily close to its earlier states. Trajectory of a chaotic system in its evolutionary wanderings also satisfies this property. It essentially reflects that the system eventually is confined to a spatial object, a set of points called an attractor. The density of such points is time invariant and this property is essential to cryptography.

Mixing

It is a characteristic of a system in which a small interval of initial conditions gets spread over the full phase space in its asymptotic evolution. In a chaotic system, an arbitrary interval of initial conditions spreads over the part (attractor) of the phase space to which the trajectory asymptotically confines. Thus any region gets into every other region of the spatial attractor of phase space.

Illustrations of Chaotic Systems

In the following discussions, we consider a discrete time evolution and a continuous time evolution systems. They are markedly different and are the best representatives of a general class of nonlinear systems.

Logistic map

This is one-dimensional map proposed by R. M. May [5] representing an idealised ecological model for describing yearly variation in the population of an insect species. The population

at $(n+1)^{th}$ year is mathematically related to that at the $(n)^{th}$ year by the following equation:

$$x_{n+1} = rx_n(1-x_n) \quad r : \text{parameter}$$

For this map, different scenarios of evolutionary behaviour were established when the system parameter r was varied over the interval [0,4]. The iterates were confined to [0,1]. Possible behaviours [solutions x_i's] in the asymptotic limit, resulting out of parametric variations, are shown in Fig.1 below.
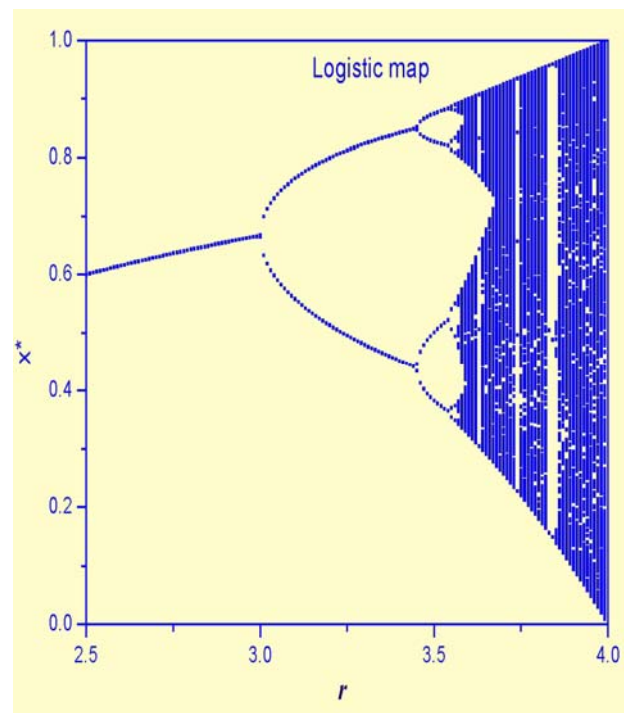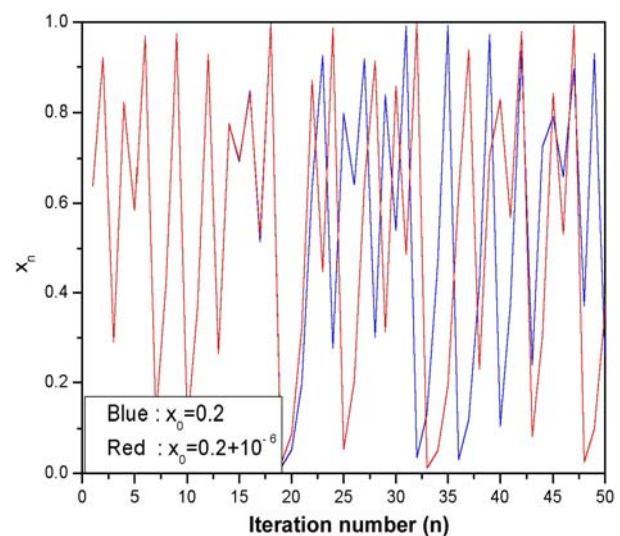

Fig. 1: Bifurcation diagram

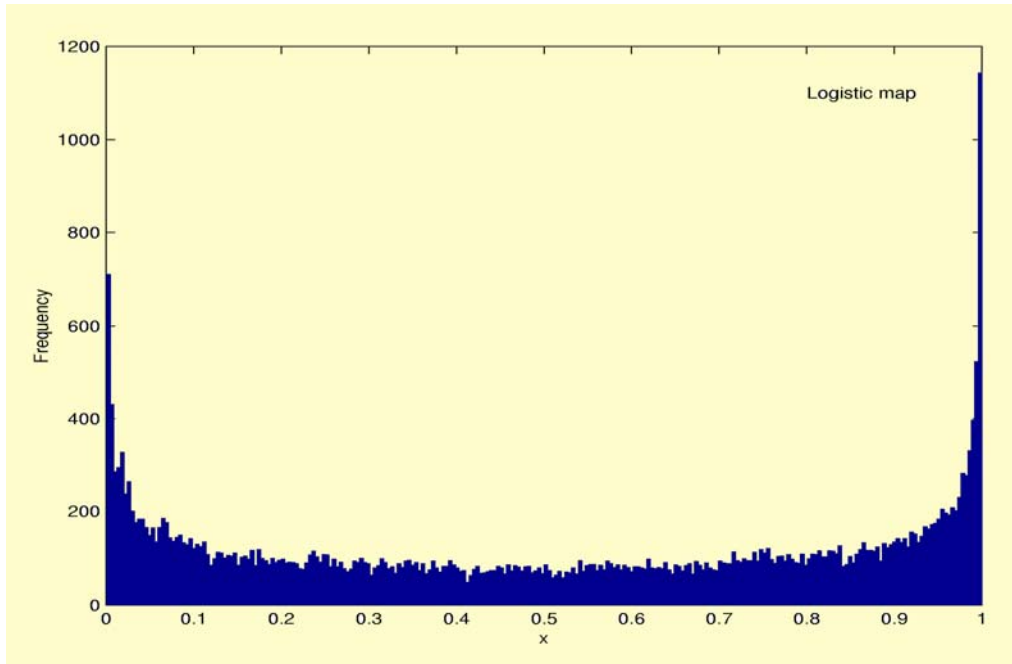Fig. 2: Sensitivity to initial condition

Fig. 3 : Invariant distribution of the iterates

Figures (1-3) exhibit the typical behaviour and the dynamical characteristics of a chaotic system. These are suitably exploited in chaotic cryptography.

Lorenz System

This is a continuous time nonlinear system exhibiting chaotic trajectories for specific values of system parameters. Atmospheric scientist E. Lorenz [11] proposed this system (1963) as a set of three ordinary differential equations to model a thermally induced fluid convection in the atmosphere.

$$\frac{dx}{dt} = \sigma(y-x) \; , \quad \frac{dy}{dt} = Rx - y - xz \; , \quad \frac{dz}{dt} = xy - \beta z$$

x is proportional to the circulatory fluid velocity, y characterises the temperature difference between the rising and falling fluid regions, and z characterises the distortion of the vertical temperature profile from its linear with height variation. Parameter σ is related to Prandtl number, R is related to the Rayleigh number and β is a geometric factor. The apparently random nature of evolution of one of the variables is seen in Fig. 4.
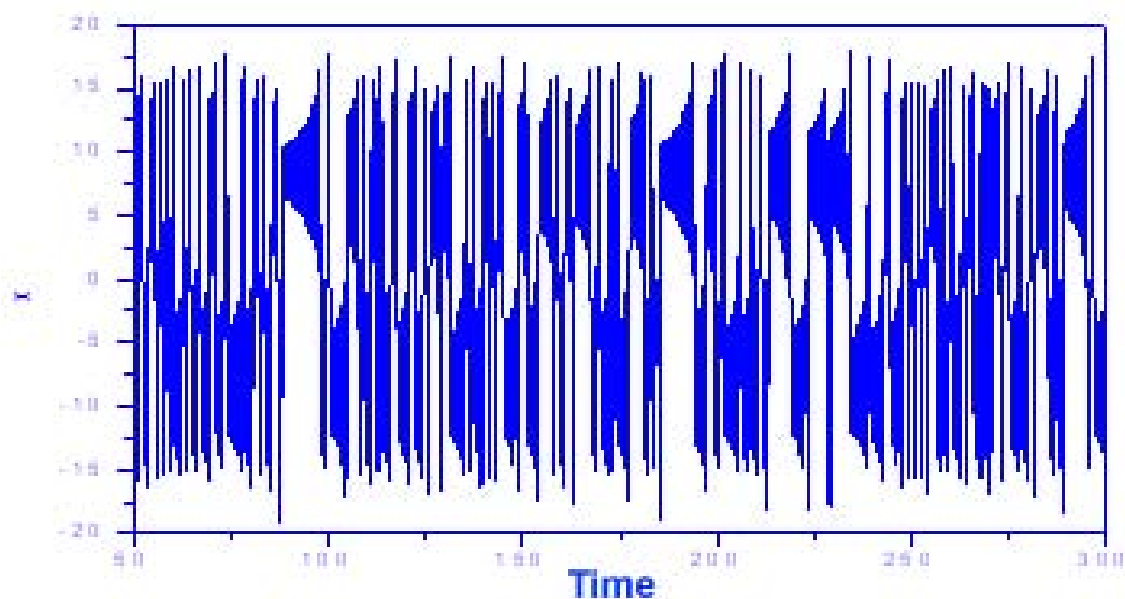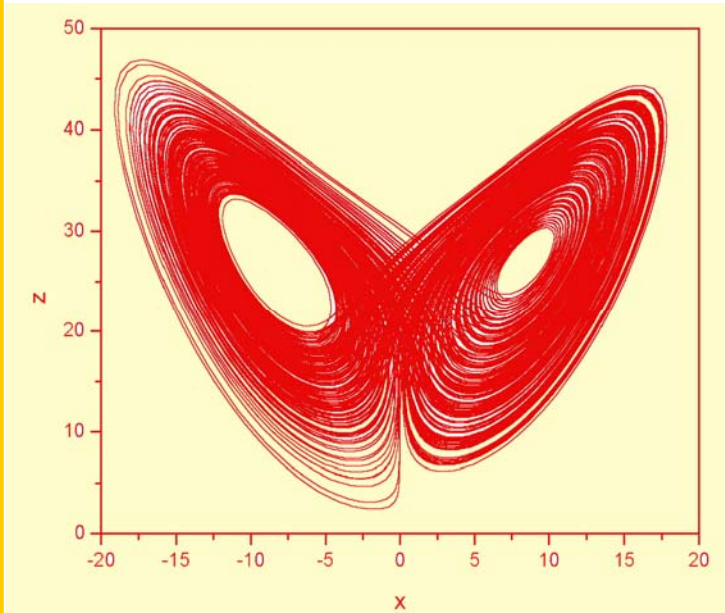

Fig. 4: Time series x(t) for chaotic Lorenz parameters

Fig. 5 : Phase space plot of the Lorenz Attractor

Phase space plot [z v/s x] of Fig. 5 refers to the trajectories for the thermofield convection generated in the Lorenz system. The model supports the uncertainties observed in weather predictions. The event is being referred to as "Butterfly effect". The subtle dynamical properties of this system are exploited for cryptographic schemes.

Chaos and Cryptography

The strength of cryptography lies in choosing the keys, which are secret parameters, used in encryption. It should not be possible to guess the key by an intruder. Chaotic systems are very sensitive to initial conditions and system parameters. For a given set of parameters in chaotic regime, two close initial conditions lead the system into divergent trajectories. Therefore encryption / decryption scheme can be obtained if the parameters are chosen as "Keys" and "Trajectories" are used for encryption/decryption. Since the same parameters are used for encryption and decryption, the chaos scheme is symmetric. The parameters and the initial conditions form a very large key space thereby enhancing the security of the code.

Baptista Method & Logistic Map

Baptista uses logistic map in which the iterates are generated using the equation: $x_{n+1} = rx_n(1 - x_n)$, by choosing the parameter r for chaotic regime and with initial condition $x_0 \in [0,1]$. A set of large number of these iterates [~ 60,000] is called the trajectory. Due to ergodic property, the interval (0,1) is visited frequently by the iterates. The density of such points is time invariant and this property is essential to cryptography. Baptista method of encryption is based on this property. The scheme for encryption/ decryption of messages uses the following steps:

Trajectory generation

Choosing the parameter r $\in [0,4]$ for chaotic case and an initial condition $x_0 \in [0,1]$, a sequence of iterates forming the points of a trajectory are generated using the Logistic equation $x_{n+1} = rx_n(1 - x_n)$ where $x_n \in (0,1)$.

Trajectory mapping

An interval [x_{min}, x_{max}] of the trajectory generated in step (1) is divided into S $\leq$ 256 sites (cells) each of size $\varepsilon = \dfrac{x_{max} - x_{min}}{S}$. To each of these sites a byte or an ascii character is associated as typically shown in the following Fig.6.

X_{min} | | | | | | | | | | | X_{max}

%	?	A	b	•	•	•	•	$	#	@	*
1	2	3	4	•	•	•	•	S-3	S-2	S-1	S

Fig. 6 : Division of Logistic Attractor into S sites

A frequency distribution of the iterate values for chaotic parameters is shown in Fig 7.
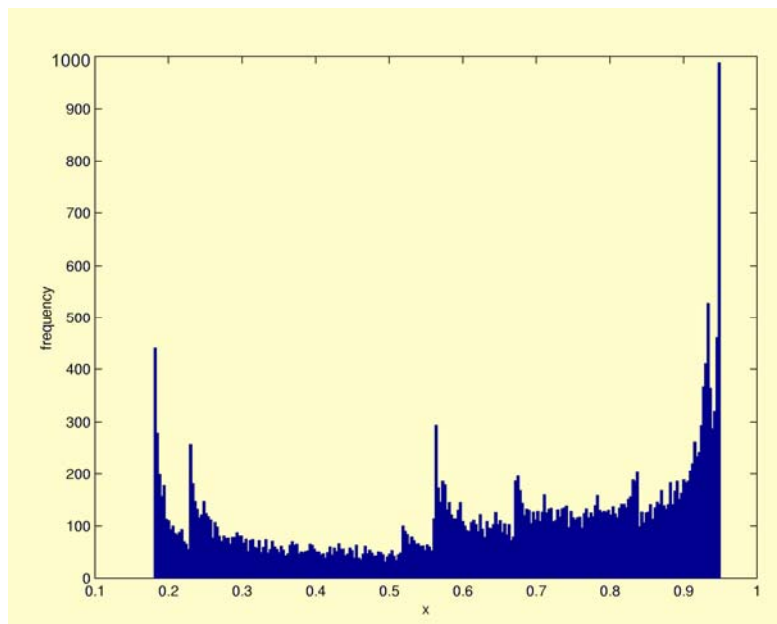

Fig. 7 : Frequency distribution of iterates of Logistic map

For encrypting each character of a text, one finds the number of iterations necessary to reach the required site belonging to that character. The number of iterations is the cipher text of the character. The process is repeated till the whole message is encrypted into a set of numbers. This forms the cipher text. Decryption is done by running the same algorithm with the same keys and the number of iterations equal to the integer values in the cipher text and by reverse mapping the site number into the character.

Cryptographic Scheme based on Lorenz Dynamics

Lorenz chaos for specific values of the parameters σ, β and R is shown in terms of the time variation of variables x, y and z in Figs. 8 (a), 8 (b) and 8 (c). The apparent randomness is clearly seen in the plots. For encryption using Baptista method, it is necessary to check the density invariance of these variables. For this, frequency distributions of x, y and z variables are plotted for a wide range of values. The plot in Fig.9 shows the frequency distribution of the variable x for a sample size of 60,000 points.
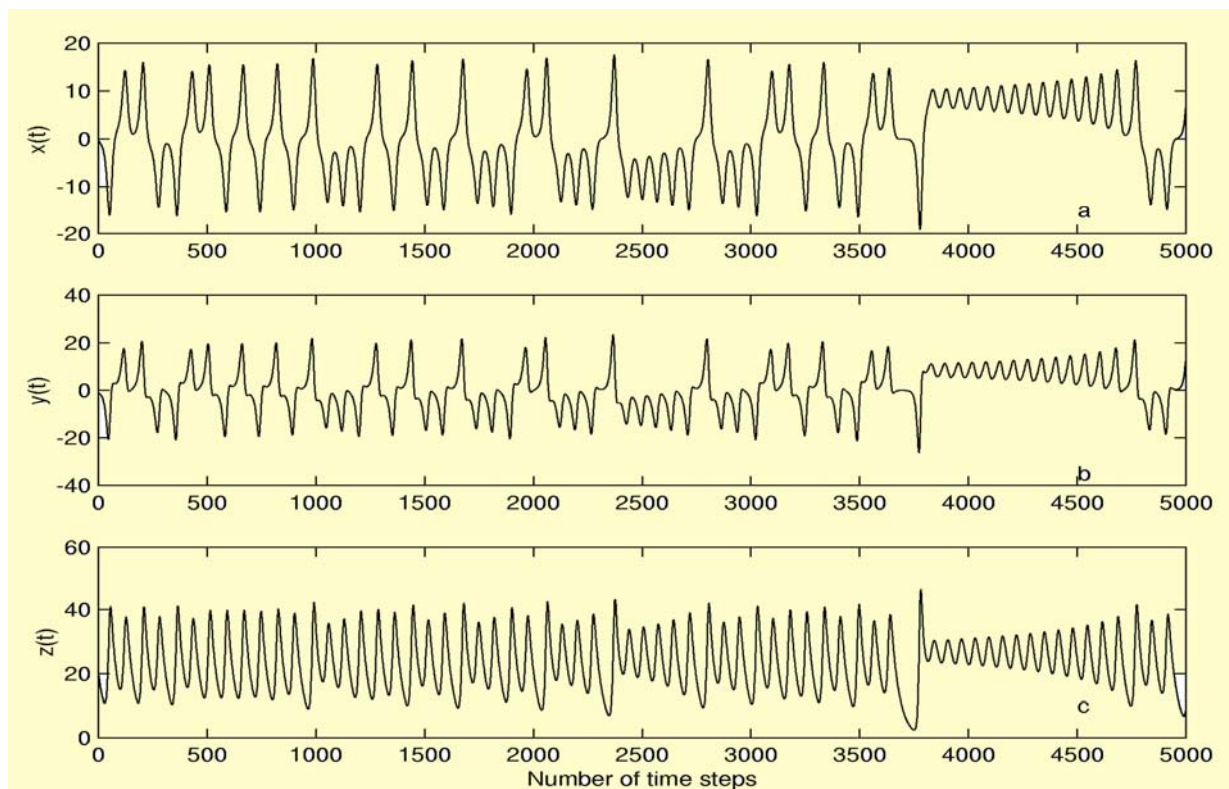

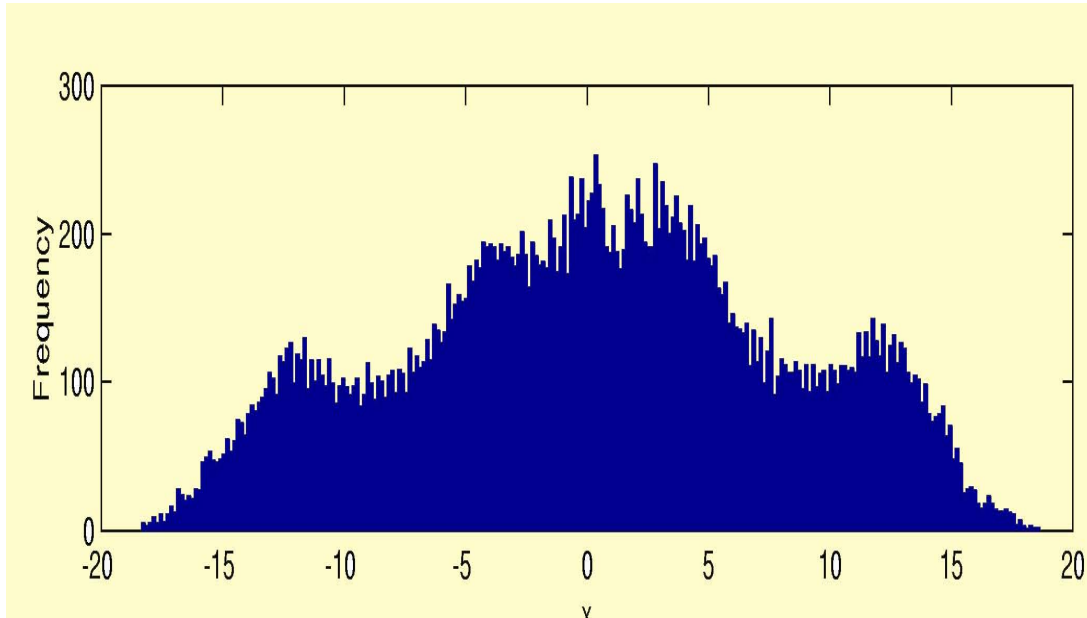Fig. 8 : Time variation of Lorenz variables

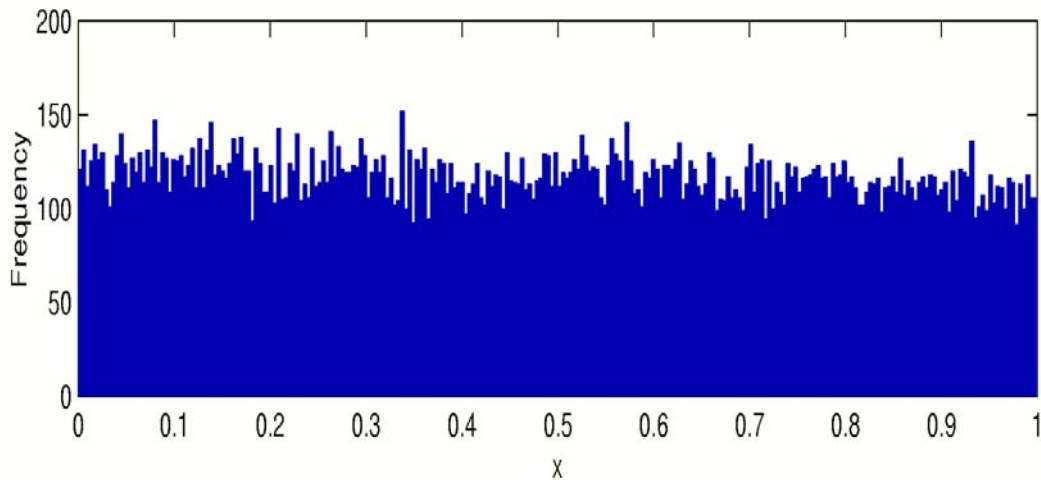Fig. 9 : Frequency distribution of x (t) for chaotic parameters

Fig. 10 : Frequency distribution of x (t) for p = 1

For application of Baptista method, any one of the plots can be chosen. For trajectory mapping, the range of variable has to be chosen such that sufficient density in a cell is obtained. For example, if x is chosen for trajectory mapping, then the range is [-5, 5]. In this range, for all values of x, we have the density of ~ 100. The cell width may be taken as 0.0390625. Using the trajectory map of Fig. 6, we can apply the Baptista scheme.

To exploit the three-dimensional character of the Lorenz trajectory, all of the variables should be at par. This can be achieved by making the following transformation called "trajectory folding".

$x = |x \bmod p|$, $y = |y \bmod p|$, $z = |z \bmod p|$.

Fig. 10 shows the plot of the transformed variable x for p=1 with density greater than100.

Under the transformed condition, any of the variables is equally good for encryption. A particular chosen variable can be hidden, thereby increasing the security and hence becomes a key. The introduction of the parameter 'p' also forms a key; because once the trajectory is folded it cannot be unfolded by any method. These considerations lead to more keys and increase in key space over the logistic map. The Folding function is

$$v = |v \bmod p|.$$

The keys can be listed as: $x(0)$, $y(0)$, $z(0)$, σ, β, R, one of the variables $(v) = \{x, y,$ or $z\}$, p, v_{min} and v_{max}.

Parameter selection

Using initial conditions $x(0)$, $y(0)$ and $z(0)$ and the values of the parameters σ, β, R appropriate for generating chaos, the Lorenz equations are solved by 4th order RK method for obtaining $x(t)$, $y(t)$ and $z(t)$ for time T [i.e. time steps N_0] until the transient part of the trajectory is crossed and system enters into chaos. The system is run to generate at least 60000 points of the trajectory. Variables x, y and z are transformed using "modulo p" function as:

$$x = |x \bmod p|, y = |y \bmod p|, z = |z \bmod p|,$$
$$1 \leq p \leq 5.$$

One of the variables x, y, or z is chosen and called v. From the frequency plot, select a maximum and a minimum value of v so as to give a frequency ~100. Cell size $\varepsilon = \dfrac{v_{max} - v_{min}}{S}$ is used to divide the trajectory into sites $S \leq 256$. To each of these sites, an ASCII character is associated as typically shown in Fig.6.

Encryption

Encryption of a message M is then carried out on the following lines. Lorenz dynamics is carried out using $x(0)$, $y(0)$ and $z(0)$ and the values of the parameter σ, β, R. The chosen variable on transformation becomes: $v = |v \bmod p|$ Encryption of a character in M involves running the dynamics from initial conditions $x(0)$, $y(0)$ and $z(0)$, until the v value falls in the interval corresponding to the required site associated with the character. The number of time steps n [equivalent to number of iterations in Logistic map] to reach the required site should be greater than N_0 (transient cross over). Further, a random number 'k' from a uniform distribution is generated and compared with a pre-chosen value $\eta \in [0,1]$. If k> η, then the number of time

steps 'n' is the encryption of the character. This procedure is repeated until the whole message M is encrypted. The encrypted message C_n is now a set of integers less than 65532.

Decryption

To decrypt the ciphertext $C_n: \{n_1, n_2, n_3, \ldots, n_i, \ldots\}$, Lorenz dynamics is run with the same parameters and initial conditions as in the encryption. The time evolution is continued up to the number of time steps, $ni = n_1$. The value of the chosen variable corresponding to $n1$ is located on one of the sites. The associated ASCII value of the reached site gives us the decrypted character. The steps are continued until the whole cipher text is decrypted.

Performance of the Algorithm

Encryption and decryption was carried out on blocks of text for following set of parameters. Initial Conditions: $x(0)=1.0$, $y(0)=1.0$, $z(0)=1.0$ System Parameters: $\sigma = 10.0$, $\beta = 2.667$, R=28.0. Modulation Parameter: $p=1.0$. The variable chosen for encryption is $x(t)$, Extreme boundary values: $v_{min} = 0.0$, $v_{max} = 1.0$, Sender's parameters: $N_0 = 3000$, $\eta = 0.7$

Input sample message

"Cryptology" is the science, which is concerned with methods of providing secure storage and transport of information. "Cryptography" can be defined as the area within cryptology, which is concerned with techniques based on a secret key for concealing/enciphering data.

Security Features

A large number of keys and their large key space makes it extremely difficult to guess the right initial conditions and the other parameters. The intruder will have to try all possible combinations of the key set (x_0, y_0, z_0, σ, β, R) which are ~ 10^{96} (using double precision reals). The

Encryption of the sample message

3147	7236	3712	3712	4018	3712	3147	3346	3069	3545
4712	7902	3054	3725	3382	4091	3382	3353	5131	3500
3069	3685	4944	3069	4042	3146	3403	3664	4872	3808
4023	3664	3060	3586	3011	3480	3480	3107	5829	3685
3765	3069	3042	3346	4429	3582	5370	4538	3337	3974
4547	3490	3357	4081	3910	4081	3490	3187	3384	3825
3346	4018	3712	3147	3633	3633	3712	3633	4952	3490
3716	3624	3069	3480	3069	3480	3069	3069	3069	3480
3624	3624	3346	3069	3480	3069	3490	3069	3716	3490
4980	3685	5245	3054	3725	3382	3808	4135	3705	5131
3500	3346	3685	3558	3069	3207	3384	3403	3994	3282
3582	3382	3913	4509	3146	3011	3624	3107	4675	3847
5885	3346	3808	3087	3346	3069	3042	3060	3042	3942
3309	3582	3101	3119	4557	3069	3751	3042	3382	3808
3490	3069	3011	3146	4215	4546	3353	3978	3069	3582
3087	3069	3664	5225	4272	3847	6281	3910	3582	3789
4135	3069	3126	5131	3923	3813	3664	3751	3586	5170
3582	5071	3664	3685	5266	3480	3353	4098	3480	3069
4662	4160	5245	3146	5227	3353	3335	4081	3119	6346
3582	3087	4299	3309	3867	3978	4279	4694	4322	5361
3770	3847	3195	3146	4440	3384	4675	5269	3346	3577
3087	3119	3913	3371	4236	3480	3200	5196	5245	3167
3725	3382	3042	4135	3664	5131	3087	3346	5196	3558
3480	3664	3923	3825	3384	4201	4864	3582	3119	3011
3591	3069	3382	4295	3384	5227	3146	3480	3582	3403
3586	3346	3725	3087	3200	4421	4097	3910	3582	3353
3087	3825	4007	3586	3813	3346	3069	3069	3346	3069

number of time steps, which is used as cipher, does not reflect the dynamics of the system. In fact, they are independent of the choice of parameters [keys]. Therefore, brute force attack is extremely difficult.

The possibility of statistical attack is reduced as the shape of frequency distribution of the encrypted message is seen to be independent of the nature of the language and type of the message [10]. Two alternative schemes to increase the complexity of cipher further have been tried. They involve use of randomised map sites or imposition of random text on the original message. The results for the scheme of randomisation of sites are shown in Fig. 11(a), 11(b) and 11(c). Similar results are seen in the other scheme.
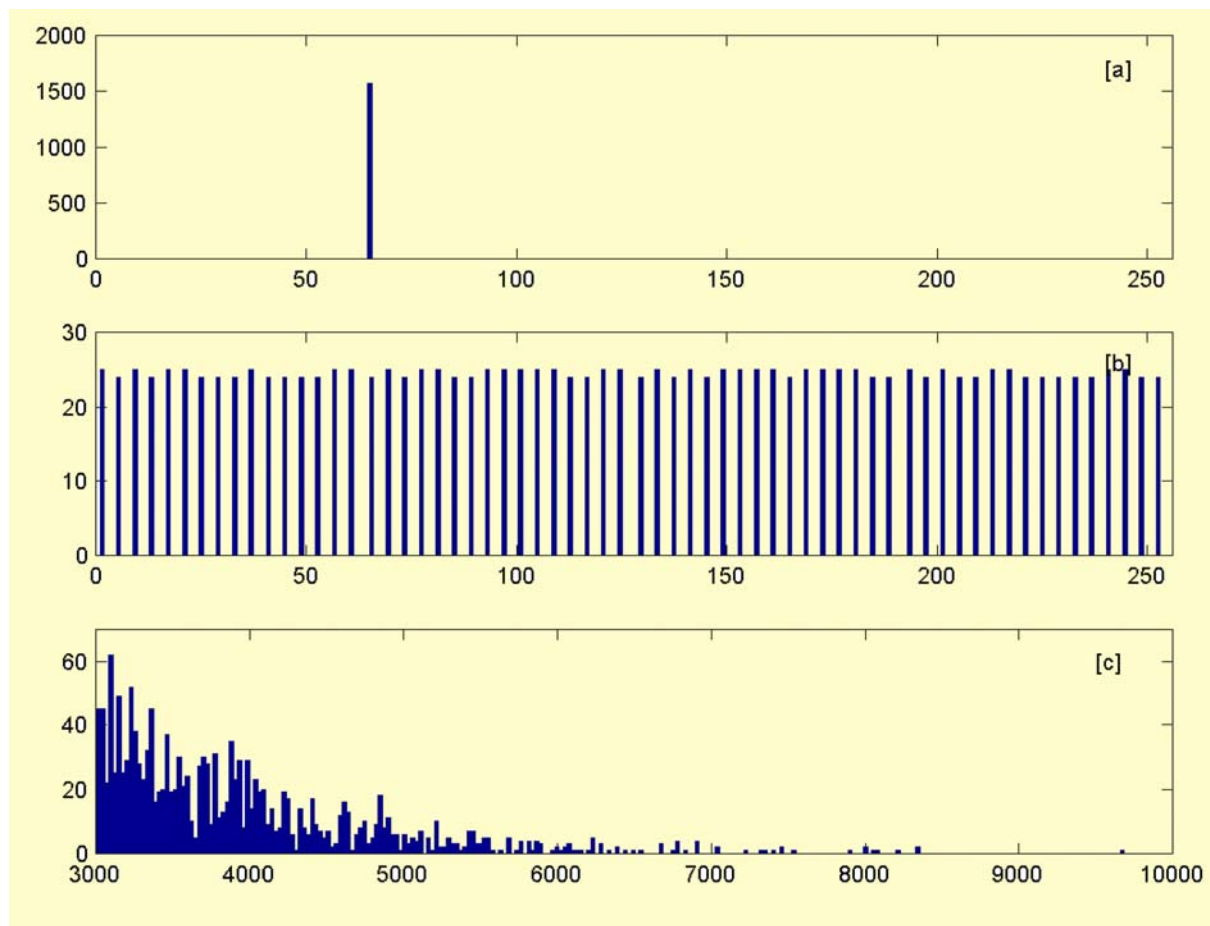
Fig.11 : Frequency distribution for: [a] a highly redundant text of a single character, [b] text after applying randomised site map on the single character, [c] encrypted redundant text

Conclusions

The software-based approach considered here is superior to the direct realisation of Lorenz dynamics on electronics circuit, as the effects due to parameter drifts, stability etc. are eliminated. Also, the circuit based implementations would be vulnerable to attacks based on reconstruction of dynamics. Software approach provides flexibility in changing the keys as frequently as possible which is difficult in circuit based scheme. The new feature of trajectory folding introduced in our scheme hides the system dynamics. Our test results show that encryptions and decryptions are quite fast and therefore making it implementable. Baptista's scheme gives chain encryption, which has the disadvantage of making the rest of the cipher text erroneous even if a single character is corrupted during communications. Also one has to watch for overflows of number of time steps, which necessitates resetting of algorithm. In the present scheme, this is avoided by using the same initial conditions every time. However, this makes the site map vulnerable to attack. This problem has been overcome by randomisation of the site map or by superimposing a random text on the original text. Our scheme also permits switching between the trajectories of three Lorenz variables using same key set.

References

1. L.M.Pecora and T.L.Carroll, "Synchronization in Chaotic Systems", *Phys. Rev Lett,* Vol. 64, (1990) 821.

2. L. J. Kocarev, K. S. Halle, K. Eckert, U. Parlitz, and L.O. Chua, "Experimental demonstration of secure communications via chaotic synchronization", *Int. J. Bifur. Chaos 2* (1992) 709-713.

1. K. S. Halle , C. W. Wu, M. Itoh and L. O. Chua, "Spread spectrum communication through modulation of chaos in Chua's circuit", in ref. 4 below.

2. "Chua's Circuit : A Paradigm for Chaos"; Madan R.N.(Ed.); World Scientific, Singapore, 1993

3. R.M. May, "Simple mathematical model with very complicated dynamics", *Nature 261,* 459(1976).

4. P. G. Vaidya, "A new method to embed time series data and for parameter identification", J. Indian Inst. Science, Vol78, (1998) 257.; P. G. Vaidya and Savita Angadi, "Cryptanalysis and Chaotic Cryptography", National Workshop on Cryptography-2003.

5. T. Arvind, S. Chandana Nilavan and Prof. V. Prithviraj, "New approach to information security through nonlinear dynamics and chaos", National Workshop on Cryptology-2003, Oct. 16-18, 2003, Chennai.

6. Ranjan Bose and Amitabh Banerjee, "Implementing symmetric cryptography using chaos functions", 7th Int. Conf. On Advanced Computing and Communications Dec 20-22, 1999, Roorkee, India.

7. M. S. Baptista, "Cryptography with chaos", *Phys. Lett. A 240* (1998) 50.

8. B.R. Ivan, S.D. Dhodapkar and Q.V. Lawande, "Cryptography using Lorenz dynamics", National Workshop on Cryptology-2004,Sept..10-12, 2004,Kerala.

9. E.N. Lorenz, "Deterministic nonperiodic flow", *J. Atmos. Sci. 20,* 130(1963

DESIGN AND DEVELOPMENT OF 0.5 M SCANNING MONOCHROMATOR AND ITS APPLICATION TO ^{15}N ANALYSIS

R. P. Shukla, D. V. Udupa, Manika Mallick, Sanjay Somkuwar, B. J. Shetty, A. K. Sinha[1] and V. C. Sahni
Spectroscopy Division

Introduction

We have been working on the development of monochromators in Spectroscopy Division since 1980. Based on the optical design of Czerny-Turner [1,2] type of optical configuration, we had first developed a 1.0 m monochromator-cum-spectrograph[3] with a resolution of 0.2 Å using a plane diffraction grating of 1200 grooves/mm. The instrument could be used in photographic mode and the monochromator mode. This instrument was used for beam-foil spectroscopic research for several years. The second monochromator, we developed, was a 1.0 m scanning monochromator[4] with a spectral resolution of 0.2 Å by using a plane diffraction grating of frequency 3600 grooves/mm. This instrument was found satisfactory for the spectrochemical analysis of rare earth impurities in solution form. The third instrument [5.6], we could develop, was 0.5m Raman spectrograph having a spectral resolution of 1.2 Å by using a grating of frequency 1200 grooves/mm. In this instrument, we used a CCD as a detector for recording the Raman spectra. The instrument gave satisfactory results for Raman spectroscopic applications. In all the

[1] A. K. Sinha is with Centre for Design and Manufacture, BARC.

monochromators developed above, we have used sine drive assembly for linearising the wavelength scale. The wavelength setting error and wavelength reproducibility were found to be of the order of 3 to 4 Å due to the backlash error in the several linkages used for rotating the grating. Based on our experience on design and fabrication of monochromators, we have improved over the design, fabrication and assembling techniques of the sine drive assembly to reduce the error in the wavelength repeatability and wavelength setting of the monochromator. We are presenting here the design, fabrication and performance evaluation of the improved model of the 0.5m scanning spectrometer.The application of the spectrometer in determination of percentage abundance of ^{15}N isotope in air and other sample is also described. The spectrometer can also be used as a replacement of medium dispersion quartz spectrograph which is being used for the quick survey of the spectral features before going in for high resolution spectroscopic studies.

Optical Layout of the Monochromator

Schematic optical arrangement of the Czerny-Turner type of monochromator is shown in Fig.1. The source of electromagnetic radiation under study is focused on to the entrance slit of the monochromator. The divergent light emerging out of the slit is collimated by a spherical concave mirror. The collimated light is made incident on a plane holographic diffraction grating. The radiation is dispersed by the grating into various wavelengths. The dispersed wavelengths are focused by a concave spherical mirror. Consequently, a wavelength spectrum is obtained in the focal plane of the concave mirror. In order to isolate a wavelength of narrow bandwidth, an exit slit is placed on the focal plane of the concave mirror. The monochromatic radiation of certain wavelength is then detected by a photomultiplier tube placed behind the exit. In order to isolate any other wavelength, the grating is rotated by a stepper motor. The spectral range of the monochromator is
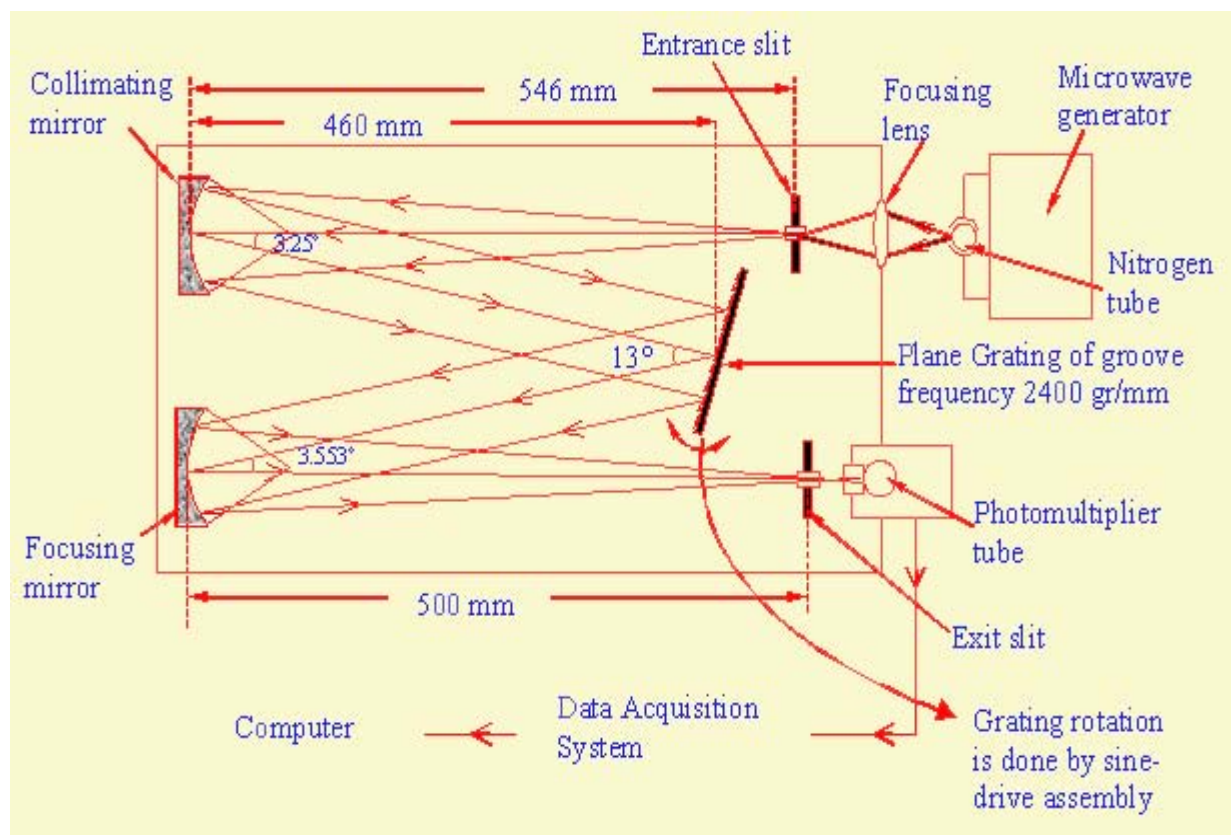

Fig. 1. Schematic optical arrangement of a Czerny-Turner type of spectrometer for analysis of ^{15}N isotope

determined by the efficiency of the grating and maximum permissible angle of rotation of the grating.

Optical Design Considerations

Our aim was to design a monochromator having a spectral resolution of 0.2 Å in the spectral range of 2000 Å to 5000 Å. We have chosen a commercially available holographic plane reflecting grating of frequency 2400 grooves/mm and ruled area 50 mm X 50 mm for designing a monochromator. The resolving power of the grating is equal to total number of grooves in the grating. The resolving power, i.e., $(\lambda/\Delta\lambda)$ for the grating of the above specification is 1.2×10^5, where λ is the wavelength of light and $\Delta\lambda$ is the spectral resolution.

For λ = 3000 Å, the theoretical wavelength resolution $\Delta\lambda$ of the grating is 0.025 Å. The practical value of the spectral resolving power is about 80 % of the theoretical value. Therefore, this grating is capable of resolving two spectral lines, which are separated by 0.03 Å, provided we use the proper focal length of the focusing mirror and the mirror is free from spherical aberrations and comatic aberration. Since we wanted to build a monochromator of smaller size, we have chosen the focal length of the concave mirror as 0.5 metre.

The reciprocal linear dispersion of the grating spectrograph for a focusing mirror of focal length 0.5m and a grating of frequency 2400 grooves/mm is about 7 Å/mm in the image plane. An exit slit is placed at the focal plane of the concave mirror to isolate a narrow band of wavelength. An exit slit of width 20 micron will isolate a band of wavelengths 0.14 Å. We preferred to use a larger slit width of 50 μm instead of 20 μm to illuminate the grating for collecting higher light flux. Therefore, the practical

value of the spectral resolution would be about 0.4 Å with a slit width of 50 μm, which will serve the purpose of medium resolution monochromator. The optical design parameters of the monochromator have been calculated for the above specification of the grating and the focusing mirror, and are summarized below :

Design parameters of the monochromator

▪ Type of optical arrangement:	Czerny-Turner monochromator
▪ Grating type:	Plane holographic reflection grating
▪ Grating ruled area:	50 mm X 50 mm
▪ Grating size:	58 mm X 58 mm
▪ Rulings / mm:	2400
▪ Blazed wavelength:	3000 Å
▪ Focal length of concave spherical mirror:	546 mm
▪ Focal length of concave focusing mirror:	500 mm
▪ Size of the concave mirrors:	100 mm diameter
▪ Angle between incident beam and diffracted beam (2ϕ):	13°
▪ Off-axial angle (a) of incidence for the principal ray at the collimating mirror:	3.25°
▪ Off-axial angle (b) of incidence for the principal ray at the focusing mirror:	3.553°
▪ Coma corrected wavelength λ_0 :	3000 Å
▪ Wavelength detection:	Photomultiplier tube
▪ Spectral range:	2000 – 5000 Å
▪ Wavelength resolution:	0.4 Å

Sine Drive Mechanism

The wavelength is nonlinear with the angle of rotation of the grating in the monochromator. Sine drive is used for linearising the wavelength scale. The principle of sine drive mechanism is shown schematically in Fig. 2. When a lever of length L is rotated through an angle θ about one end, the other end moves through a distance $X = L \sin\theta$ perpendicular to the initial position of the lever. The wavelength $\lambda = 2\sigma \cos\Phi (X/L)$ where σ is the groove spacing, 2Φ = angle between incident beam and diffracted beam.
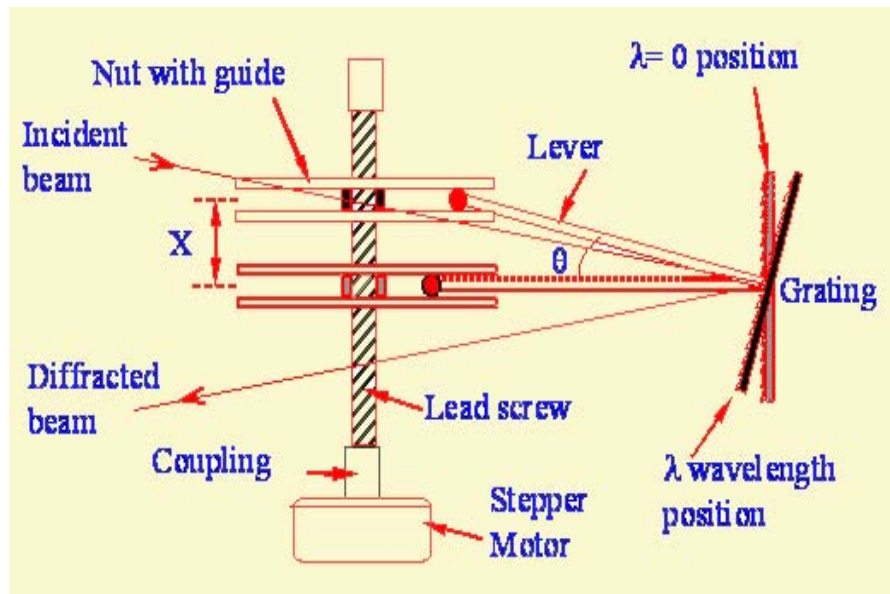
Fig. 2. Schematic mechanical arrangement of the sine drive assembly for rotation of the grating in the monochromator to set various wavelengths at the exit slit.

The data acquisition system for the spectrometer consists of a photomultiplier tube (PMT) based signal detection system and a motorised grating movement system with limit switch safety mechanism as shown in Fig. 3. Necessary software has been developed in Visual Basic 5.0.

Thus, the wavelength λ is proportional to the linear displacement of the centre of the ball measured in a direction perpendicular to the initial position of the lever. A nut actuated by a screw can push the ball, and a drum attached to the screw may be linearly calibrated in terms of wavelength.

A lead screw of pitch 2 mm and effective length 200 mm was chosen for the sine drive assembly. The movement of the lead screw is imparted by a 7 kg cm torque stepper motor.

Taking σ = 1/ 2400 mm, ϕ = 6.5°, the lever length is calculated to be 165.595 mm by the above relation to give a wavelength shift of 100 Å by a nut movement (X) of 2 mm, i.e., the wavelength shift is 100 Å per rotation of the lead screw. Movement of the nut for a wavelength shift of 5000 Å is 100 mm. Since the effective length of the lead screw is 200 mm, we can set any wavelength between 0 Å and 5000 Å. The lead screw is rotated by the stepper motor to set any wavelength on the exit slit.
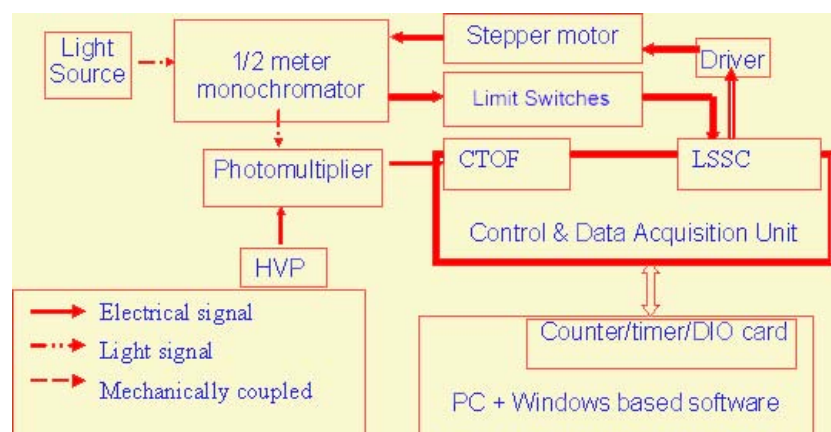

Fig. 3. Schematic block diagram of data acquisition system.

The signal detection part consists of a PMT and a high voltage PMT power supply (3000V, 30mA). The selection of the PMT was based on the spectral response (185-650nm with peak wavelength at 340nm), low dark current (1 nA) and high current gain (7.5x10[6]).

The data acquisition part is built around a home made current-to-frequency (C/F) converter circuit and a timer/counter/DIO PCL 830 card. To digitize the PMT output, the C/F module was designed and fabricated. The C/F consists of a current to voltage converter stage implemented using an operational amplifier OPA104 and a voltage to frequency converter VFC320. The

current to voltage converter can handle input current in the range of 10^{-8}A to 10^{-5}A. The voltage output from the current to voltage converter is fed to the voltage to frequency converter VFC320 with full-scale frequency of 1MHz. Observed linearity for the input current range of 10^{-8}A to 10^{-5}A is better than $\pm0.01\%$ and %RSD of counts is within satisfactory level of $\pm0.1\%$. The transistor-transistor logic (TTL) output pulses from the VFC are then counted by a 32-bit counter, which is implemented by cascading two 16-bit counters in the PCL830 card. To maintain the data collection time, another 16-bit counter is used as timer with clock input of 10KHz from on-board crystal.

The stepper motor drive system consists of a 7 kg-cm stepper motor a driver unit which offers 1/100th microstepping factor, i.e., a spectral resolution of 1000Å/(100x200) steps= 0.05 Å. This system interacts with PC through a Limit Switch Sensing Circuit (LSSC) and PCL830, which generates the necessary pulse and direction signals to the driver based on the number of steps, direction, etc. to drive the motor.

A pair of proximity switches has been connected at the extreme points of the operating wavelength range to limit the motor movement within this region. These switches are connected in parallel. Activation of one of the switches is detected by LSSC, which stops motor movement.

Necessary software is developed in Visual Basic 5.0. Software provides features like acquisition of spectrum, move to wavelength, single step movement, adjust zero shift, automatic determination of initial wavelength, plot of spectrum, offline processing of spectrum, limit switch detection, etc.

Performance Evaluation of the Spectrometer

We have recorded the various spectral lines of cadmium by using the spectrometer in the wavelength range of 2900 Å to 5100 Å. The wavelength reproducibility is observed to be 0.1Å. The intensity profiles of the spectral lines are shown in Figs. 4 (a) – (d). The spectral resolution of the spectrometer is estimated to be 0.4 Å, as decided by the band-pass for a slit width of 50 µm.
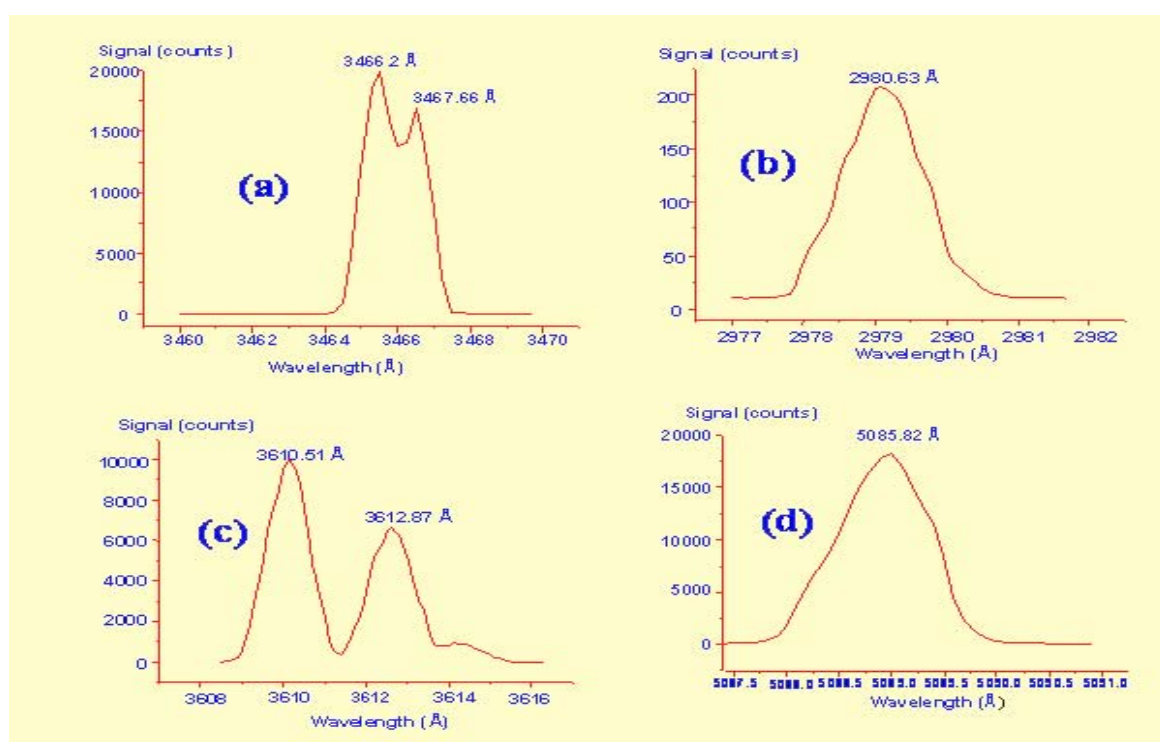

Fig. 4. Emission spectral lines recorded using the spectrometer with a cadmium discharge lamp as a source

Application of the Spectrometer to ^{15}N Isotope Analysis

The emission bands of N_2 were produced in a sealed-in quartz Electrodeless Discharge Lamp (EDL) by microwaves (2450 MHz, ~50W power). The EDL has been previously filled with the sample of nitrogen gas at a pressure of 5 torr in a vacuum system. For the quantitative determination of percentage concentration of ^{15}N in the sample of nitrogen gas, the (2-0) band of the second positive $(C^3\Pi_\upsilon - B^3\Pi_\gamma)$ system has been employed since the band heads of the isotopic species ^{14}N-^{14}N and ^{14}N-^{15}N have a isotope shift of 6.1 Å[7]. The light emitted by nitrogen molecules is focused on to the entrance slit of the spectrometer. The scanning was done in the wavelength range of 2974 Å to 2985 Å to record the spectral lines of ^{14}N-^{14}N band and ^{14}N-^{15}N band. Fig. 5 shows the spectral bands of the nitrogen isotopes recorded on the spectrometer. The abundance of ^{15}N isotope in natural nitrogen as calculated[7,8] from the intensities of the bands shown in Fig.5 is 0.35 %. Fig. 6 shows the photograph of the spectrometer developed by us.
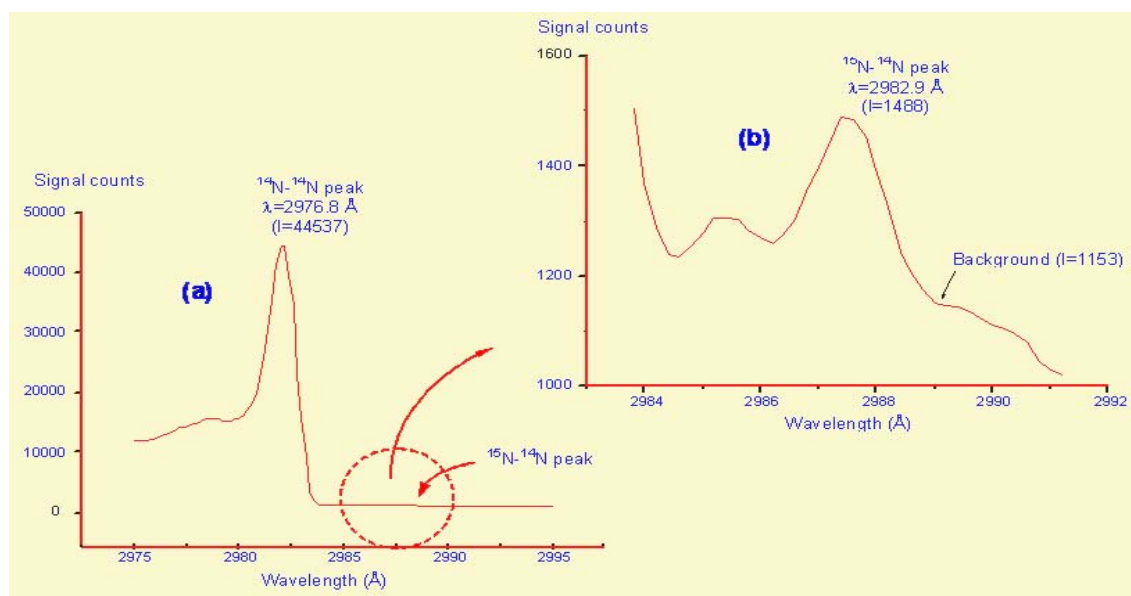

Fig. 5. Spectrum of nitrogen present in natural air recorded using the instrument. Plot (a) shows the peak of ^{14}N-^{14}N molecule and plot (b) shows the enlarged plot of ^{14}N-^{15}N peak.
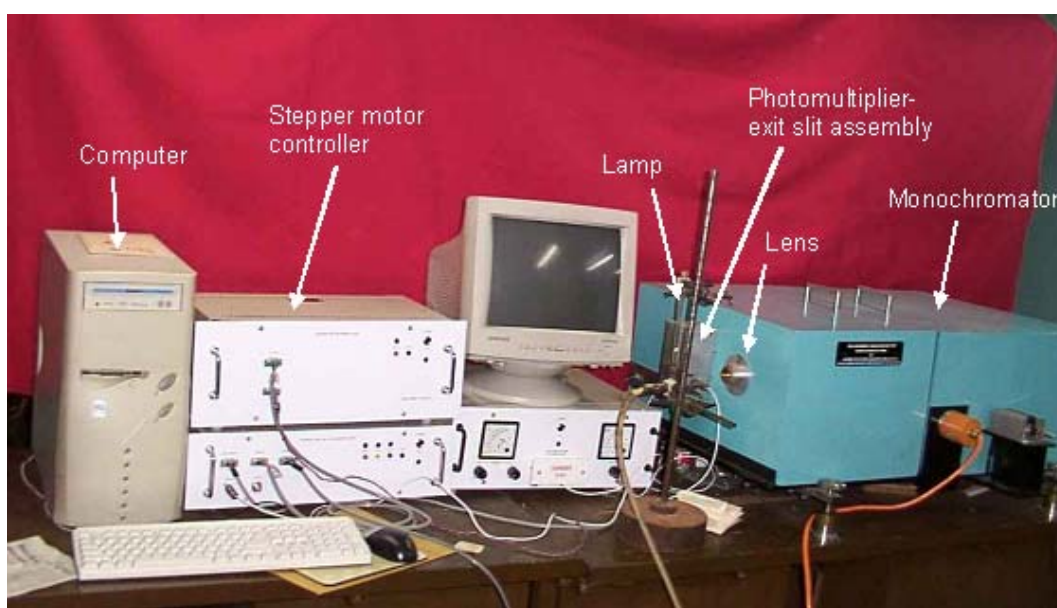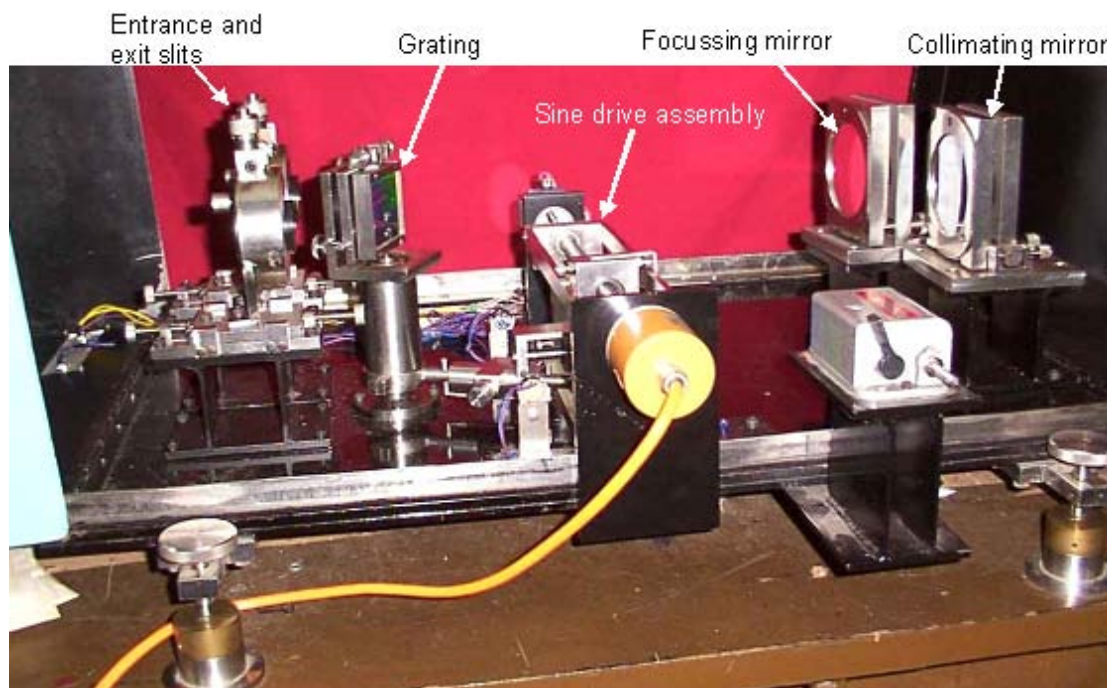

Fig. 6(a). Photograph showing the complete set-up consisting of the monochromator, detection system and the excitation lamp for the isotopic analysis

Fig. 6(b) Photograph of the monochromator with the cover open

Conclusion

A 0.5 m scanning monochromator has been designed and developed for analysing ^{15}N isotope. The complete system consists of a 0.5 scanning monochromator for wavelength selection, photomultiplier tube for spectral wavelength detection and data acquisition system for measuring the peak intensity of the spectral wavelength.   The wavelength range of the spectrometer is 2000 Å to 5000 Å with a spectral resolution of 0.4 Å. The optical design is based on Czerny-Turner type of configuration having a concave spherical mirror of focal length of 0.546 m as a collimating mirror, a plane reflection holographic grating of frequency 2400 grooves/mm as a dispersing element, and a concave spherical mirror of focal length 0.5 m as a focusing element.   The optical design parameters have been chosen such that the spherical aberrations of the two concave mirrors are within the tolerance Rayleigh limit of $\lambda/4$ and the comatic aberration is zero at the wavelength of 3000 Å. The sine bar mechanism is used for linearising the wavelength scale. The grating is rotated by a stepper motor coupled to the sine drive assembly for isolating any wavelength radiation between 2000 Å and 5000 Å.

The isolated wavelength at an exit slit is detected by a photomultiplier tube whose current is amplified and fed to a data acquisition system (DAS). The DAS stores the data points of intensity of a spectral line when the spectral line is scanned by rotation of the grating with the motor coupled to the personal computer. The software program loaded into the computer then plots intensity profile of spectral line.   The spectrometer is found to be useful for the detection of 0.36 % of ^{15}N isotope present in the nitrogen gas.

The spectrometer will be useful in the field of agricultural research wherein ^{15}N isotope in the form of ^{15}N labeled fertilizer is employed as a tracer for ascertaining the qualitative uptake of nitrogen from nitrogenous fertilizers by plants.

The spectrometer will also be useful for the quantitative determination of percentage abundance of ^{15}N isotope of nitrogen gas in biological samples by optical emission spectroscopy method. The technology of design and fabrication of 0.5 m monochromator with photoelectric detection and data acquisition system is available with Spectroscopy Division in collaboration with Centre for Design and Manufacture at BARC, Mumbai.

References

1. M. Czerny and A.F. Turner, *Z. Physik, 61*, 792 (1930)
2. M.V.R.K. Murty, "Theory and Principle of Monochromators, Spectrometers and Spectrographs", *Optical Engineering, 13* (1), 23 (1974)
3. M.V.R.K. Murty and R.P. Shukla, S.S. Bhattacharya and G. Krishnamurthy, "Design and Fabrication of Czerny-Turner Monochromator-cum-Spectrograph", Report No. BARC/1362 (1987)
4. R.P. Shukla, D.V. Udupa, S.S. Biswas, Manika Das, S.V.G. Ravindranath, S.M. Marathe, A.K. Sinha, M.B. Guhagarkar and A.P. Roy, "The Design, Fabrication and Performance Evaluation of a Scanning Monochromator for Rare Earth Elements Analysis", *Journal of Optics, 26,* 47 (1997)
5. R.P. Shukla, Sanjiva Kumar, Manika Mallick, A.K. Sinha, S.V.G. Ravindranath, S. Thakur, N.K. Sahoo and N.C. Das "Multichannel Spectrograph using CCD as a Detector for Raman Spectroscopy Applications", Report No. BARC/2002/E/019
6. R. P. Shukla, Sanjiva Kumar, A.K. Sinha, Manika Mallick, S. Thakur, N.K. Sahoo and N.C. Das, "A Simple Method of Calibration for Multichannel Spectrograph using charge coupled Device (CCD) as a Detector for Raman Spectroscopy", *Journal of Optics, 33,* (2), 87 (2004)
7. M. Singh, R. Venkatasubramanian, T.K. Balasubramanian and V.V. Athalye, "Setting up of an Isotope Analyser for Quantitative Determination of Percentage Abundance of ^{15}N in Nitrogen Gas", *Analytical Letters, 27* (12), 2369 (1994)
8. JASCO MODEL NIA-1, N-15 Analyzer Service Manual (1979) Japan Spectroscopic Co. Ltd., 2967-5, Ishikawa-cho, Hachioji-city, Tokyo, Japan

BARC TRANSFERS TECHNOLOGY OF GUIDE SLEEVE CUTTING MACHINE

The technical know-how of Special Purpose Machine for cutting Guide Sleeve and Sensor Tips and also the actual machine was transferred to NPCIL on April 04, 2005 by BARC.

A special purpose machine tool and machining process has been developed to cut the guide sleeve and sensor tips of the fuelling machine of 220 MW PHWR, in case the guide sleeve or sensor tips cannot be retracted back to the fuelling machine after refuelling operation. This will be an emergency situation for a PHWR. Material of the guide sleeve is 17-4 PH, having core hardness of 35HRC and the surface is nitrided having a hardness of 60 HRC. The thickness of guide sleeve is 5.75 mm. Approach for cutting this tube is only from the other end of the reactor channel, which is at a distance of 10 meters.

Signing of the agreement for technology transfer by Mr G.Govindrajan, Director A&MG, BARC and Mr Umesh Chandra, Sr. ED (R&D,C&I,IT), NPCIL

In mock up operations, actual guide sleeve was machined from a distance of 10 meters. But machining can be done even if this distance is more or less depending upon the requirements.

Technology Transfer and Collaboration Division coordinated all activities related to the transfer of this technology.

THEME MEETING ON "FISSION GAS RELEASE IN NUCLEAR FUELS"

A one day DAE-BRNS Theme Meeting on "Fission Gas Release in Nuclear Fuels" was held at BARC, Mumbai on March 16, 2005. This was the first theme meeting, in the series of several theme meetings jointly planned by the Nuclear Fuels Group of BARC and Directorate of Engineering of NPCIL, Mumbai, on the topic of High Burnup Issues in Nuclear Fuels (HBINF-2005). Over 100 delegates participated in the
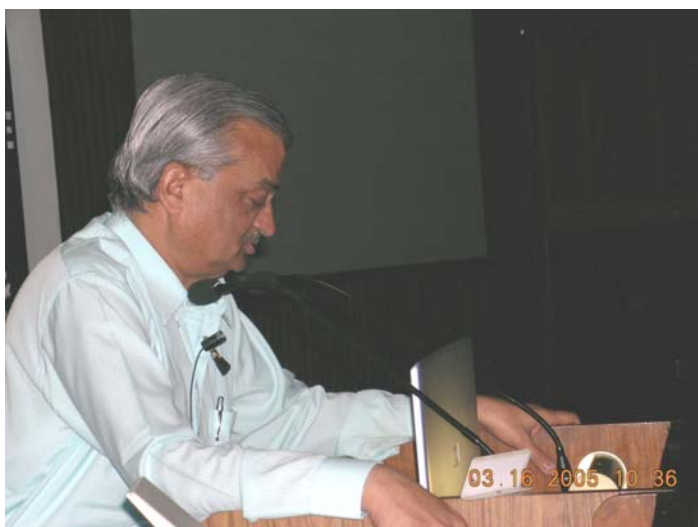
Dr Anil Kakodkar, Chairman, Atomic Energy Commission and Secretary to Government of India, delivering the inaugural address at the Theme Meeting

meeting and 27 technical papers were presented. Mr H. S. Kamath, Director, Nuclear Fuels Group, BARC, welcomed the participants. The meeting started with opening remarks by Dr S. Banerjee, Director, BARC, who briefly traced the historic milestones in the last 50 years, which have

helped in developing a sound understanding of the fission gas release mechanisms in water reactor fuels. Dr Anil Kakodkar, Chairman, Atomic Energy Commission and Secretary to Government of India, inaugurated the theme meeting.

Fission gas release is an important parameter in the overall fuel pin performance at high burnup. Both experimental and modelling activities are required on our fuels to develop reliable predictive tools for quantitative prediction of fission gas release and its effect on the fuel performance. The need to understand and anticipate the way fission gases behave, justifies a number of in-pile and out-of-pile experimental studies and modelling of the process. The aim of the meeting was to bring together all the scientists/engineers, working in the Department of Atomic Energy on this topic, to present their work and jointly draw a road map to achieve our objective of developing our own computer codes, for prediction of fission gas behaviour in the fuels of Indian reactors. The meeting was organised in the following three technical sessions.

- Session I: Basic mechanisms, modelling and round robin code prediction of fission gas release
- Session II: High burnup issues, code validation on FGR and fuel performance analysis
- Session III: Fission gas release measurement and its effect on fuel performance

This theme meeting, which exclusively focused on fission gas release in nuclear fuels, was organised in our country for the first time. It provided a forum for presentation of all the work being done in this area in various institutions of DAE. It also provided an opportunity for exchange of experience and ideas among specialists working on this topic. A theme talk, on the basic mechanisms of fission gas release in nuclear

fuels, was delivered by Mr D. N. Sah (BARC). He illustrated the various mechanisms of gas release in the nuclear fuel with the help of photomicrographs of irradiated fuel and computer animations of release processes prepared in-house by his colleagues. A second theme talk by Dr S. L. Mannan (IGCAR) explained the high burnup issues related to fast breeder reactor fuel and structural materials.
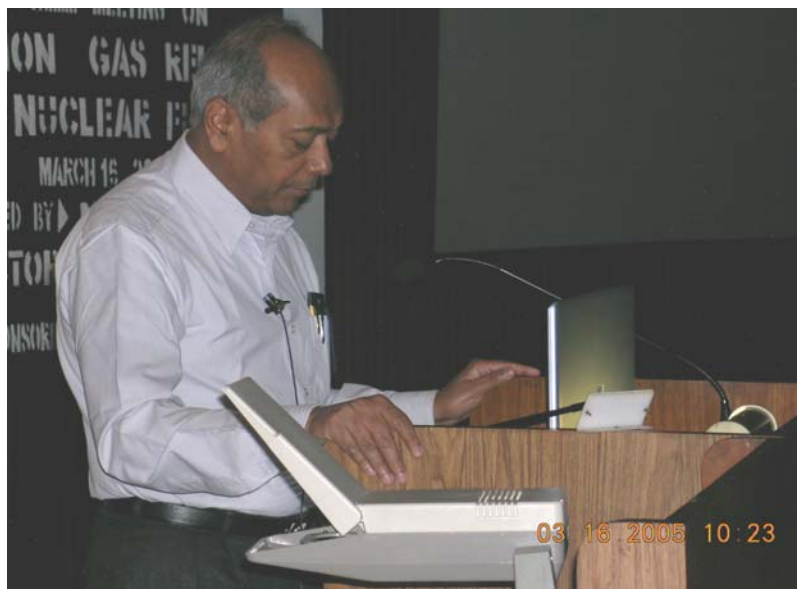
Dr S. Banerjee, Director, BARC, giving opening remarks in the Theme Meeting.

Results of fission gas release measurements made on high burnup PHWR fuel pins, experimental MOX fuel pins, ThO_2 fuel pins and mixed carbide fuel pins of FBTR were presented in the meeting. Details of modelling of fission gas release in various codes developed in BARC, NPCIL and IGCAR were presented.

On the occasion of this meeting, a round robin code prediction exercise had been organised on fission gas release in high burnup PHWR fuel pins. Predictions of 4 computer codes, PROFESS, FUDA, modified GAPCON THERMAL and RELAP/SCDAP were presented. Comparison of predicted and measured fission gas release in fuel pins of current IAEA CRP on FUMEX-II, by codes PROFESS and FAIR were also presented.

At the end of the technical sessions, a meeting of session chairpersons and authors who presented the papers in the meeting was held to decide the

action plan for future activities. The meeting was chaired by Mr S. A. Bharadwaj, Sr. Executive Director (Engg), NPCIL, Mumbai. This brainstorming session extended over one and half hour and each participant presented his/her views. Considering all the views expressed in the meeting, following recommendations emerged for future activities.

1. Prediction of FGR for high burnup PHWR cases of the round robin program should be completed by all codes. The results of calculation should be compared and discussed in a meeting. Predictions for MOX fuel clusters may be taken up as the next phase of the program by codes, which have completed PHWR cases.

2. PIE of few more high burnup PHWR fuel bundles, which have experienced power ramp, should be taken up to generate experimental data for code validation. Retained gas should also be measured in the fuel in addition to released gas. Experimental irradiation should be planned in PWL and/or in PHWR using well documented fuel pins.

3. A shielded Electron Probe Micro-Analyser (Shielded EPMA) should be procured for meaningful PIE of high burnup irradiated fuels. Measurement of radial profile of retained fission gas in the fuel pellet, using Electron Probe Micro-Analyser (EPMA), is essential to validate and improve the FGR models in the codes. Examination of extent of fuel cladding chemical interaction using EPMA, is essential to evaluate performance of fuel pins at high burnup. The instrument will also be useful for study of fuel and fission product distribution in various type of fuels, study of cladding oxidized under simulated LOCA condition, failure investigations on

irradiated components, microchemistry of irradiated pressure tube and coolant piping materials, etc.

4. Measurement of thermal conductivity of irradiated UO_2, irradiated Thoria based fuel and ThO_2-UO_2 SIMFUEL should be taken up to determine the extent of thermal conductivity degradation in fuels with burnup.

5. A National Working Group on High Burnup Fuel (NWGHBF) should be constituted to follow up the action plan.

The meeting concluded with a vote of thanks by Convener Mr D. N. Sah to the Board of Research in Nuclear Sciences, invited speakers, authors of contributed papers, participants of the meeting and the organisers.

BARC DEVELOPS METAL EXTRACTANTS FOR USE IN FRONT-END AND BACK-END OF NUCLEAR FUEL CYCLE

Materials Group, BARC, has developed the technology for the synthesis of TAPO - a mixed liquid phosphine oxide, and DNPPA – a liquid cation exchanger. These extractants (solvents) find widespread use in nuclear hydrometallurgical processes. DNPPA in combination with TAPO is mainly used for extraction of Uranium from fertilizer grade phosphoric acid.

TAPO which is a mixture of four Trialkyl phosphine oxides, namely, Trioctyl phosphine oxide (TOPO), Dioctyl monohexyl phosphine oxide

(DOMHPO), Dihexyl monooctyl phosphine oxide (DHMOPO) and Trihexyl phosphine oxide (THPO) was introduced as metal extractant CYANEX 923 by American Cyanamide Company. Their manufacturing process uses toxic chemicals like phosphine and mixture of α-olefins at high pressure to produce intermediate trialkyl phosphines which, on further oxidation, gives mixture of Trialkyl phosphine oxides.

In order to indigenise the technology for large scale production of TAPO, an alternate process for its synthesis has been developed by the reaction of Grignard reagents containing mixed alkyl groups with phosphorus oxychloride to produce a mixture of Trialkyl phosphine oxides. No toxic chemicals or rigorous reaction conditions were used throughout the reaction. The yield of the overall process and purity of the product are in the order of 90% and 95% respectively.

DNPPA is liquid cation exchanger synthesised by using phosphorus oxychloride and p-nonyl phenol in the presence of an organic base. The yield and purity of the product are in the order of 90% and 94%, respectively. DNPPA in

Photograph after signing the MoU agreement. Seen from left to right (sitting) are Dr A.K. Suri, AD(P), MG, BARC, Dr S. Banerjee, Director, BARC, Mr S.C. Hiremath, Chairman & CE, HWB, Mr A.K.Wechalekar, ED(Tech.), HWB, (Standing) Mr R.P .Agrawal, TT&CD, Mr P.M. Sakhalkar, MG, BARC, Mr J.N. Sharma, MG, BARC, Mr T.K.Haldar, HWB, Mr R.R.Betkar, MG, BARC, Mr S.K.Naik, HWB and Mr G.K. Vittal, HWB.

combination with synergistic solvent TAPO has high extraction coefficient for Uranium from commercial phosphoric acid in comparison with conventionally used D2EHPA/TOPO system.

These developments have reached a stage where they can now be produced at commercial scale. Accordingly, the MoU between BARC and HWB was signed on April 15, 2005 by Director,

BARC and C&CE, HWB, for transfer of know-how related to synthesis and joint efforts for scaling up of the synthesis of these solvents.

Earlier through the joint efforts of Materials Group, BARC, and HWB, pilot plants for production of D2EHPA and TBP at a scale of 20Mt/yr and 60Mt/yr, respectively, have already been set up at HWP, Talcher, Orissa.

NATIONAL TECHNOLOGY DAY

National Technology Day was celebrated in BARC on May 12, 2005. The main theme of the programme was felicitation of Padma Awardees and talks by DAE scientists.

Dr Anil Kakodkar, Chairman, Atomic Energy Commision & Secretary to Department of Atomic Energy, felicitated Mr S.B. Bhoje, Former Director, Indira Gandhi Centre for Atomic Research (IGCAR) and Dr S. Banerjee, Director, BARC, who were bestowed Padma Shri in 2003 and 2005, respectively. Dr Kakodkar, in his opening speech, said, "Department of Atomic Energy is a technological organisation and so it is appropriate that we celebrate National Technology Day. It also brings us all together to discuss the various technological developments during the year gone by." He said, "In view of our fuel resources, there are several technologies we

Dr Anil Kakodar, Chairman, AEC & Secretary to Government of India, felicitating Mr S.B. Boje, Former Director, IGCAR, who was awarded Padma Shri in 2003

Dr Anil Kakodar, Chairman, AEC & Secretary to Government of India, felicitating Dr S. Banerjee, Director, BARC, who was awarded Padma Shri in 2005

have to develop and take a global leadership position. This particularly includes technologies to harness vast thorium resources available in India." He said that our country is looking for

Dr Anil Kakodkar, Chairman, AEC & Secretary to Government of India, delivering the opening speech at the Central Complex auditorium, BARC

Dr (Ms) K. Indira Priyardarsini, RC&CDD, talked on "Free Radical Reactions of Antioxidants and Radio-protectors," Mr A. Rama Rao, RED, spoke on "Role of Vibration Diagnostics in Safety Technologies" and Dr. Lalit Varshney, RTDS, spoke on "Development of Radiation Processed Hydrogels for Medical Use."

The programme was attended by a large number of BARC and DAE employees.

energy technologies to meet our growing energy requirements and this is the main mandate of our Department. He released a film "Technology Treasure" on this occasion.

Talks on recent technological achievements in the Department of Atomic Energy (DAE) highlighted the landmark achievements. Dr K.B. Dixit, Associate Director, Nuclear Power Corporation of India Limited (NPCIL), spoke on India's first 540 MWe PHWR at Tarapur which went critical on March 6, 2005. Built during technology denial regimes, it marks a milestone in India's Nuclear Power Programme. Mr A.K. Wechalekar, Sr. Executive Engineer (Tech.), Heavy Water Board (HWB), spoke on Front-End technology for ammonia based Heavy Water Plant (HWP) which helped to re-commission Baroda HWP. Mr K. Jayarajan, Division of Remote Handling and Robotics, gave a talk on the technology for societal development and on 'BHABHATRON' -India's first indigenously developed computer-aided economical teletherapy machine.

Recipients of Homi Bhabha Science & Technology Awards and Technical Excellence Awards 2004 (all from BARC) gave talks on their topics with specially designed presentations, for broad based understanding. Dr A.P. Tiwari, RCnD, spoke on "Design and Development of Spatial Control System of 540 MWe PHWR."

NATIONAL CONFERENCE ON "OCCUPATIONAL AND ENVIRONMENTAL RADIATION PROTECTION"

The Indian Association for Radiation Protection (IARP) will be organising its 27th National Conference during November 23-25, 2005 at the Multipurpose Hall, BARC Guest House, Anushaktinagar, Mumbai 400 094.

Indian Association for Radiation Protection (IARP) is a non-governmental organisation (NGO) of radiation protection professionals in India and an affiliate of International Radiation Protection Association (IRPA). Its main objective is to promote the science of radiation protection in nuclear technology and in the applications of ionizing radiation in industry, medicine, agriculture and research. Its important activities include organisation of workshops, seminars, national and international conferences, public awareness programmes and arranging training courses. IARP provides an excellent platform to communicate, exchange and share with the professionals as well as the public, the latest developments and experiences in the area of radiation protection of the workers, public and that of the environment. Yet another notable

activity of IARP is the quarterly publication of an international scientific journal. *Radiation Protection and Environment.* IARP is a national organisation and has its chapters spread out throughout India. It has been serving the international and national scientific communities for the past 37 years.

IARP NC-2005 will be devoted to '*Occupational and Environmenal Radiation Protection'*. The detailed thematic areas of the conference are listed below :

➤ **Occupational Radiation Protection**
- In Nuclear Fuel Cycle Facilities
- In Waste Management & Decommissioning
- In Accelarator Facilities
- In Medicine, Industry & Research
- Infrastructure Developments
- Operational Radiation Protection & its Optimisation

➤ **Radiation Protection of the Environment and Public**
- Radon Exposures
- Enhanced Natural Exposures (Air Crew)
- Liquid & Gaseous Discharges
- Waste Disposal & Decommissioning
- Environmental Surveillance
- Modelling Exposure Pathways
- Malevolent use of Radiation Sources

➤ **Radiation Protection Dosimetry & Instrumentation**
- External Dosimetry
- Internal Dosimetry
- Biological Dosimetry
- Radiation Detection Instrumentation

➤ **Management of Unusual Occurrences, Incidents and Accidents, and Emergency Preparedness**
- In Nuclear Fuel Cycle Facilities
- In Public Domain
- Orphan Sources

➤ **Occupational Radiation Protection**
- Radiation Biology
- Epidemiology

- Risk Factor Evaluations

In addition, there will be a Panel Discussion on '"ICRP Recommendations on Radiation Protection – Past, Present and Future".

For further details, contact :
Dr D.N. Sharma, Head, RSSD, BARC
Tel. : (91-22) 25505259, 25593818
Email : dnsharma@barc.ernet.in
Fax : (+91-22) 25505151, 25519613
Website : http://www.barc.ernet.in

INTERNATIONAL CONFERENCE ON "RELIABILITY SAFETY AND HAZARD - 2005"

Research and development work in the areas of reliability, safety and hazard is being actively persued worldwide with an objective to improve performance and opimisation of operational and maintenance cost of the nuclear and process plants. Risk-based technologies, where apart from deterministic safety assessment, the insight from Probabilistic Safety Assessment (PSA) is used for taking the decisions, are becoming part of operational decision making, regulatory review, design and safety evaluations. In some of the plants in developed countries, risk-informed asset management is a way of life.

Keeping in view the R&D work being performed in the field of reliability and safety engineering and the state-of-the-art development taking place worldwide, a three-day International Conference on "Reliability Safety and Hazard (ICRESH-05)" is being organised at the hotel, The Leela Kempinski, Mumbai, during December 1-3, 2005.

The conference is being organised by BARC, Indian Institute of Technology, Bombay, and Society for Reliability Engineering Quality and Operation Management, and supported by :

- Board of Research in Nuclear Sciences, Mumbai,
- Heavy Water Board, Mumbai
- Atomic Energy Regulatory Board, Mumbai,
- Indira Gandhi Centre for Atomic Research, Kalpakkam,
- Defence Research and Development Organisation, and
- International Society of Reliability Engineers (India Chapter)

The topics for the conference are :

1. Reliability

- Reliability in engineering design
- Digital system reliability
- Safety critical software reliability analysis
- System reliability assessment
- Stochastic Petri nets for reliability modeling
- Dynamic reliability
- Reliability based methods for residual life estimation
- Reliability centered maintenance
- Uncertainty analysis

Human Reliability Modelling (Operator support systems, Expert elicitation, Artificial Neural Network, Expert Systems in support of improving human reliability, and Design of fault tolerant systems)

2. Safety

- Probabilistic Safety Assessment (PSA)
- External events PSA
- Shutdown safety
- Risk assessment for passive systems
- Fussy logic for Risk analysis
- Radiation risk assessment
- Environment risk modelling
- Deterministic methods in safety assessment
- Thermal hydraulic safety analysis
- Structural safety analysis

3. Hazard

- Safety Assessment Techniques in Process Industries
- Hazard and Operability studies
- Application of PSA methods in hazard evaluation
- Codes and standards for hazard assessment

4. Risk Informed Approach

- Risk-informed /Risk-based Technologies in support of regulatory decisions
- Role of Risk-informed approach in Ageing management
- Risk-based In-Service-Inspection
- Risk-informed operational decisions
- Risk-informed asset management
- Systems security
- Graded quality assurance

5. Application Areas

Nuclear power plants & research reactors, Heavy water plants, Heavy water plants, Petroleum & Process industries, Desalination plants, Nuclear Waste Management plants, Robotics, Lasers, Accelerators, Accelerator driven sub-critical systems, Aircraft systems, Launch and Delivery systems, Railways, Electronics and Telecommunications

For registration and further details, contact :

(1) Mr H.S. Kushwaha, Convenor
Email : icresh05@barc.ernet.in ;
        kushwaha@barc.ernet.in
Tel : (+91-22) 25593603, 25505313
Fax : (+91-22) 25505313

(2) Dr P.V. Varde, Secretary
Email : varde@barc.ernet.in
Tel : (+91-22) 25594689
Fax : (+91-22) 25505311, 25505151
Website : http://www.barc.ernet.in

निदेशक, भापअकेंद्र, को प्रशंसात्मक सम्मान प्राप्त
DIRECTOR, BARC, RECEIVES MORE ACCOLADES

Dr S. Banerjee, Director, BARC, receiving the "Distinguished Alumnus Award" during the Golden Jubilee Convocation of IIT - Kharagpur

The Indian Institute of Technology, Kharagpur, also did not lag behind in honouring Dr Banerjee with the "Distinguished Alumnus Award" for the meteoric rise of one of its past students to the exalted position of Director of the country's premier nuclear research centre, Bhabha Atomic Research Centre. This award was bestowed on Dr Banerjee during the Golden Jubilee Convocation of I.I.T - Kharagpur on February 26, 2005.

Padma Shri Dr Srikumar Banerjee is the recipient of many other awards and honours. He is also Fellow of many prestigious Academies.

डॉ. श्रीकुमार बॅनर्जी, निदेशक, भाभा परमाणु अनुसंधान केंद्र, को भौतिकी धातुकी एवं पदार्थ विज्ञान के क्षेत्र में पिछले कई दशकों से अति महत्वपूर्ण योगदान के लिए फरवरी 23, 2005 को पश्चिम बंगाल के बर्दवान विश्वविद्यालय के द्वारा प्रतिष्ठित वैज्ञानिक (honoris causa) की उपाधि दी गई।

इन्डियन इन्स्टिट्यूट ऑफ टेक्नॉलोजी, खड़गपुर भी अपने भूतपूर्व छात्र डॉ. बॅनर्जी की असाधारण उन्नति तथा देश के गौरवशाली नाभिकीय अनुसंधान केंद्र, भाभा परमाणु अनुसंधान केंद्र के निदेशक पद को प्राप्त करने पर उन्हें "प्रतिष्ठित स्नातक पुरस्कार " से सम्मानित करने में पीछे नही रहा। यह पुरस्कार उन्हें फरवरी 26, 2005 की गोल्डन जुबली कन्वोकेशन आफ आइ आइ टी खड़गपुर के दौरान प्रदान किया गया।

पदम् श्री डॉ. श्रीकुमार बॅनर्जी को अन्य कई पुरस्कारों से सम्मानित किया जा चुका है। ये कई प्रतिष्ठित अकादमियों के सदस्य भी हैं।

Dr Srikumar Banerjee, Director, BARC, was conferred the degree of D.Sc. (honoris causa) by the University of Burdwan, West Bengal, on February 23, 2005 for his exemplary contributions in the fields of physical metallurgy and materials science over the past many decades.

4th ASIAN AEROSOL CONFERENCE (AAC-2005)

The Asian Aerosol Research Assembly (AARA) is a body comprising of national aerosol associations of the countries in the Asian region. These include the Japanese Association for Aerosol Science and Technology (JAAST), Chinese Association for Aerosol Research and Technology (CAART) of ROC, Indian Aerosol Science and Technology Association (IASTA), Korean Association for Particle and Aerosol Research (KAPAR), Institute of Atmospheric Aerosol (IAA) of China and Thai Powder Technology Centre. AARA holds the Asian Aerosol Conference once in two years in one of the member countries. The past three

conferences were held in Nagoya, Japan (1999), Pusan, Korea (2001) and Hong Kong (2004), The 4th AAC will be held at the Hotel Grand Hyatt, Mumbai , under the auspices of IASTA, during December 13-16, 2005.

The Indian Aerosol Science and Technology Association (IASTA) was founded in 1988 with a view to promote and develop the growth of aerosol science and technology disciplines and their applications. It has been meeting its objectives by way of organising conferences, workshops, exhibitions and lectures and through its biannual bulletin and other publications. It has been awarded affiliation to the International Aerosol Research Assembly (IARA) and has maintained active liaison between institutions in India and abroad.

Scientific contributions, as platform and poster presentations, are invited in areas of aerosol research in the following topics :

- Aerosol fundamentals: Physics and Chemistry
- Aerosol instrumentation
- Aerosol remote sensing techniques
- Radioactive and nuclear aerosols
- Aerosols and climate change
- Urban air pollution and source apportionment
- Indoor pollution
- Health related aerosols
- Bio-aerosols, biodefense, inactivation of bioagents
- Medical and pharmaceutical applications
- Material synthesis; nanoparticle technology
- Clean room applications

For further details, contact :
Mr H.S. Kushwaha, Convenor, AAC-2005
Tel. : (+91-22)25593603; 25505313
Email : mail@iasta-aac.org;
        kushwaha@barc.ernetin
Fax : (+91-22)25505313, 25505151
Website : http://www.barc.ernet.in

भा.प.अ. केंद्र के वैज्ञानिकों को सम्मान / BARC SCIENTISTS HONOURED

सिजोफ्रेनिया पेशन्ट यूजिंग एफडीजी- पेट के अनुसंधान अध्ययन के आधार पर "रीजनल ब्रेन मेटाबोलिज्म इन सिजोफ्रेनिया पेशन्ट यूजिंग एफ्डीजी- पेट "नामक वैज्ञानिक शोध-पत्र ने केईएम अस्पताल, मुम्बई, के मनोचिकित्सा विभाग के सहयोग से, भापअ केंद्र के रेडियेशन मेडिसन सेन्टर में संचालित तथा एएनसीआइपीएस-2005 (एनुअल नैशनल कान्फरेंस ऑफ द इन्डियन साइकेट्रिक सोसाइटी) पीजीआइएमईआर, चंडीगढ में 57वीं वार्षिक

सभा में प्रस्तुत 17 प्रतियोगी शोधपत्रों के समक्ष, प्रतिष्ठापूर्ण डॉ. जे.सी. मारफातिया पुरस्कार प्राप्त किया। भापअ केंद्र के रेडियेशन मेडिसन सेन्टर के डॉ. एन.नायर, श्री एस.एच.मोघे, श्री नवाब सिंह बघेल, एवं डॉ. ए.जी.पंडित (डीआरएम के छात्र) के साथ केईएम अस्पताल, मुम्बई के साइकेट्री विभाग से डॉ. आर. सीथालक्ष्मी, डॉ. शुभांगी पारकर, डॉ. शिल्पा अदरकर तथा डॉ.शेफाली बत्रा इस अध्ययन में सम्मिलित हुए।

The scientific paper entitled, "Regional Brain Metabolism in Schizophrenia Patients Using FDG-PET Study", based on a research study on Schizophrenia patients using FDG-PET conducted at the Radiation Medicine Centre (BARC) in collaboration with the Psychiatry Department of KEM Hospital, Mumbai, and presented at the 57th ANCIPS - 2005 (Annual National Conference of the Indian Psychiatric Society) at PGIMER, Chandigarh, won the prestigious "Dr J.C. Marfatia Award" from among 17 competing papers. Dr N. Nair, Mr S.H. Moghe, Mr Mawab Singh Baghel and Dr A.G. Pandit (DRM student) participated in the study from Radiation Medicine Centre, BARC, along with Dr R. Seethalakshmi, Dr Shubhangi Parkar, Dr Shilpa Adarkar and Dr Shefali Batra from Psychiatry Department of KEM Hospial, Mumbai.