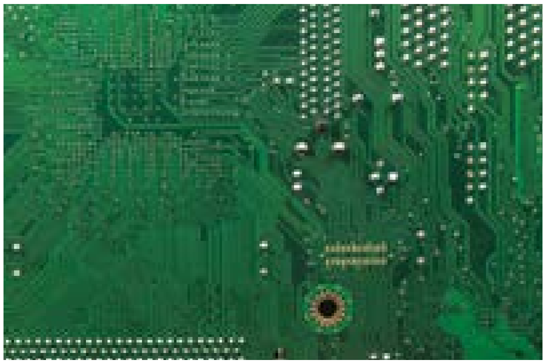
ISSN 2320 5636

www. nitap.in

International Journal
on Current Science & Technology



International Journal on Current Science & Technology
Vol.-2 | No.-2 | July-December ’ 2014

NATIONAL INSTITUTE OF TECHNOLOGY
ARUNACHAL PRADESH
न हि ज्ञानेन सदृशं पवित्रमिह विद्यते
ESTB: 2010

ISSN: 2320 5636

NATIONAL INSTITUTE OF TECHNOLOGY
ARUNACHAL PRADESH
न हि ज्ञानेन सदृशं पवित्रमिह विद्यते
ESTB: 2010

www. nitap.in

International Journal on Current Science & Technology
Vol.-2 | No.-2 | July-December' 2014

ISSN: 2320 5636

International Journal on Current Science & Technology
Vol.-2 | No.-2 | July - December' 2014

Published By:
NATIONAL INSTIUTE OF TECHNOLOGY
(An Institute of National Importance)
ARUNACHAL PRADESH, INDIA

Designed & Printed at:
Saraswaty Press Limited, Kolkata

ISSN: 2320 5636

International Journal on Current Science & Technology

Vol.-2 | No.-2 | July-December’ 2014

Published by
NATIONAL INSTIUTE OF TECHNOLOGY
(An Institute of national importance)
ARUNACHAL PRADESH
(Estd. By MHRD, Govt. of India)
PO-Yupia, P.S.-Doimukh,Dist-Papum Pare
Pin-791112, Arunachal Pradesh
Ph: +91 360 228 4801, Fax: +91 360 228 4972
E-mail : pchakraborty.ece@nitap.in; conferencenitap@gmail.com

www. nitap.in

EDITORIAL BOARD MEMBERS

[18] Dr. Pinaki Chakraborty - Assistant Dean (Research & Development), National Institute of Technology, Arunachal Pradesh, India.

[19] Dr. Nabakumar Pramanik - Assistant Dean (Finance & Accounts) National Institute of Technology, Arunachal Pradesh, India.

[20] Dr. K. R. Singh - Assistant Dean (Exam.), National Institute of Technology, Arunachal Pradesh, India.

[21] Dr. U. K. Saha - Assistant Professor, National Institute of Technology, Arunachal Pradesh, India.

[22] Dr. Parogama Sen - Associate Professor, Calcutta University, India, Chair, Physical Science Section

[23] Prof. A. K. Bhunia - Professor, Burdwan University, india.

Index of Content

Experimental Studies on Selective Encryption of Text using both Fixed and Variable Key and Results Thereof

B Bhuyan[1], C T Bhunia[2], P Chakrabarti[3], A. Chowdhuri[4]

[1]North Eastern Hill University, Shillong,
[2] National Institute of Technology - Arunachal Pradesh, Arunachal Pradesh -791112,
ctbhunia@vsnl.com
[3]Sir padampat Singhania University, udaipur
[4] Department of Computer Science & Engineering, Jadavpur University, Kolkata- West Bengal, India

Selective Encryption has been studied by different researchers as a technique for speeding up encryption and decryption processes [1, 2].The security level of a selective encryption scheme depends on the appropriate selection of part of the message to be encrypted. Again, according to Shannon, to achieve perfect security [3] the key must vary from session to session. In this paper, an experiment has been made to apply Shannon's scheme of variable key with selective encryption. The research aim is to get speed advantage without deteriorating the security level. Experimental results indicate the superiority of selective encryption with variable key over the selective encryption with fixed key in terms of resistance to differential attack.

Key words: Selective Encryption, Perfect security, Differential Attack, Automatic variable key

1. INTRODUCTION

Any encryption system is evaluated primarily on the basis of two parameters namely (i) security level it provides (ii) the speed of encryption and decryption. Selective encryption is the process of encrypting a small portion, called selected blocks of data/message, keeping the remaining portion unencrypted as shown in figure 1.The security of the selective encryption scheme is primarily depends on the selection criteria of the blocks to be encrypted. In this work we have done an experiment on texts where a block selected for encryption is chosen by an algorithm based on occurrence of keywords in that block [2]. Not encrypting the whole data/message decreases the security level of the encryption process. To compensate the decrease of security level due to the selective encryption, a protocol is used to vary the key for encrypting the different blocks. The variation of keys is due to implementation of Shannon's theory of perfect security [4].

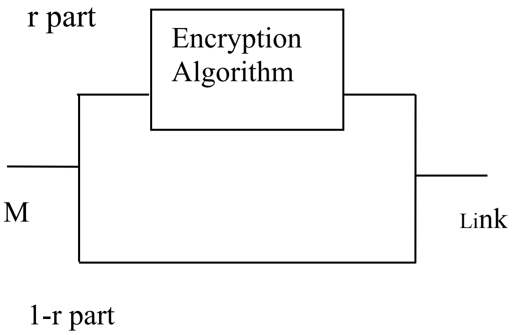


Figure 1: Selective encryption Scheme of Message M.

2. REVIEW OF PROTOCOL FOR VARYING THE KEY IN ENCRYPTING DIFFERENT SELECTED BLOCKS

With brevity the basic idea is illustrated with an example. Suppose n bit key will be used for encryption and transmission of m selected blocks from a source, A to a destination, B (fig2). We assume $n=2^c$.We propose that many or all keys of the whole key space of 2^n shall be used in the session, unlike a single key as in DES and AES (or a single key pair as in RSA). For this, whole key space will be divided into several groups each of n bits. Total number of groups will be then 2^n / n equals to say 2^p , where p+c = n. At the beginning of the session, A will select any data of n bits (except a data made of all 0s) called Key for Key Selection, KKS (Say KKS$_0$). It will be sent to B under existing RSA encryption. n bits KKS$_0$ is made of p group bits and another c bits. Keys selection for subsequent messages will be indicated by the position of 1's in KKS$_0$ in the group defined by p. The positional indication is as follows: 1 in RMB (Right Most Bit) position, 1 in one but RMB position … and 1 in LMB (Left Most Bit) position will refer respectively to first, second ….and last key of the group. If there are l such keys, first (l-1) keys will be used for first (l-1) messages and last key for transmission of second KKS, (say KKS$_1$). The process will continue till the transmission of the all messages is made. Fig 2 illustrates the scheme with n=4.. When n=4, c=2, key space (2^n) =16, number of groups = 2^n / n (= $2^{2)}$ and p=2. Session is supposed to transmit messages, m_0, m_1, …, …m_i… As the KKSs are secret, the secret keys, ks exchanged under the protocol will remain secret and only known to sender and receiver. The proposed protocol is a typical key agreement protocol for time variant key

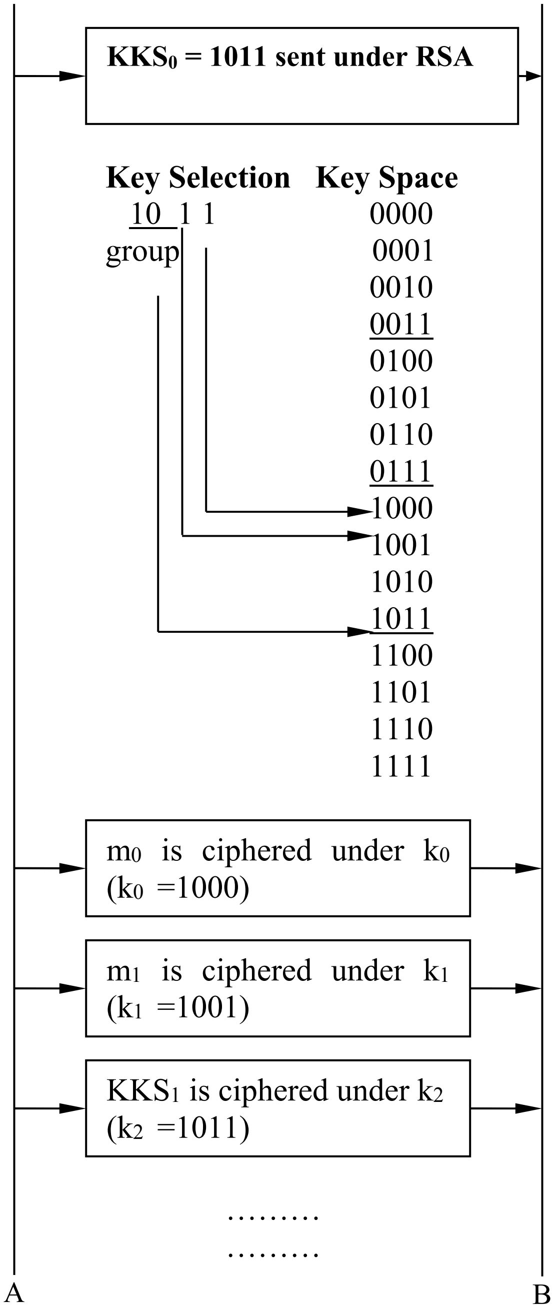

KKS0 = 1011 sent under RSA
Key Selection
Key Space
10 1 1
group
0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111
m0 is ciphered under k0 (k0 =1000)
m1 is ciphered under k1 (k1 =1001)
KKS1 is ciphered under k2 (k2 =1011)
………
………
A
B

Fig. 2 Protocol of time variant key selection & exchange in the proposed scheme

3. ALGORITHM FOR SELECTION OF BLOCKS FOR ENCRYPTION

In the work we employ the variable key as explained in section 2 with selective encryption. We apply algorithm proposed elsewhere [2] and as given below.

Algorithm: I

1. Input Key Words for the message of N words (say, n number of keywords is given). Find frequency of occurrence of each keyword in whole of the message, f_i (i=1 to n)
2. [Say, the DES encrypts blocks each of M words (M<N). So there are k blocks where k=N/M]. Find frequency of occurrence of each keyword in each block, F_{ij} (i=1 to n, j=1 to k)
3. If $F_{ij} \geq \{f_i.(1/k)\}$ for any one, more or all keywords, i.e , i=1 to n, the jth block will be encrypted in DES, otherwise not.
4. Repeat (3) for all blocks, j=1 to k. When j=k, the proposed scheme of encryption is complete.

4. EXPERIMENTAL RESULTS

Experiments are undertaken on three data sets as given below. First three datasets are selectively encrypted; selection of a block to be encrypted is chosen based on frequency of keywords present using the algorithm mentioned in section 3. Then using the same algorithm with the same key words we have selectively encrypted the three datasets with the variable key agreed according to the protocol mentioned in section II. A parameter weighted average of frequency of occurrence of repeated cipher data is used to compare the output ciphers. It is a reasonable entity as it provides an average representation of repetitions. In each case we have measured the weighted average of frequency of symbols in the generated cipher using the formula: Weighted Average= (ΣNumber of units * Freq) / (Total number of Unit).The results are as shown in Table 1.

Dataset 1

```
01 12 13 24 01 01 12 23 01 11 12
35 16 45 12 11 01 35 12 21 46 aa
55 91 11 21 13 41 65 91 21 45 aa
10 12 13 31 41 21 55 91 01 12 13
24 01 01 12 23 01 11 12 35 16 45
12 11 01 35 12 21 46 aa 55 91 01
12 13 24 01 01 12 23 01 11 12 35
16 45 12 11 01 35 12 21 46 aa 55
91  65 bb 01 13 41 46 45 12 aa
aa 10 23 34 45 11 23 44 23 34 45
16 34 23 12 11 11 23 34 16 19 20
12 34
```

Dataset 2

```
01 12 13 24 01 01 12 23 01 11 12
35 16 45 12 11 01 35 12 21 46 aa
55 91 11 21 13 41 65 91 21 45 aa
10 12 13 31 41 21 55 91 01 12 13
24 01 01 12 23 01 11 12 35 16 45
12 11 01 35 12 21 46 aa 55 91 01
12 13 24 01 01 12 23 01 11 12 35
16 45 12 11 01 35 12 21 46 aa 55
91  65 bb 01 13 41 46 45 12 aa
```

Dataset 3

```
12 23 34 45 12 34 67 78 12 34 45
34 56 12 34 88 aa 11 22 12 23 34
11 01 11 12 23 34 23 45 67 10 11
32 34 12 34 23 34 11 26 46 57 13
67 45 34 10 23 aa 1a 67 90 23 45
bb
```

Table 1: Weighted Frequency of plain text and cipher text using fixed and variable selective encryption

Data set#	Weighted Frequency of characters in the plaintext	Weighted Frequency of characters in the selectively encrypted cipher	Weighted Frequency of characters in the selectively encrypted cipher with variable key
1	5.21	1.53	1.3483
2	5.05	1.476	1.17
3	2.66	1.21	1.09

From the results given in table 1, it is found that for all the three dataset, the weighted frequency of repeated in data / message in case of selective encryption with variable key is reduced. It therefore indicates that the selective encryption scheme with variable key scheme is a better encryption technique in terms of resisting differential attack.

5. CONCLUSIONS

The experimental results indicate the superiority of selective encryption with variable key over selective encryption on fixed key in terms of the resistance to differential frequency attack.

REFERENCES

[1] Tom Lookabaugh et al, “Selective Encryption for Consumer Applications”, IEEE Communication Magazine, Vol 42, no 5, pp.124-129, April’2004
[2] C T Bhunia, New Approaches for Selective AES towards Tackling Error Propagation Effect of AES, Asian J of Information Technology, Pakistan, Vol 5, No. 9, pp 1017-1022, 2006
[3] C. E. Shannon, “A mathematical theory of communication," Bell System Technical Journal, vol. 27, pp. 379-423 and 623-656, July and October, 1948.
[4] C T Bhunia ,Bubu Bhuyan,Prasun Chakrabarti, A Scheme of Time Variant Key towards realizing Perfect Security, Communicated to an International Journal.

A Scheme of Time Variant Key Towards Achieving Perfect Security

C T Bhunia[1] *SMIEEE*, Bubu Bhuyan[2] *MIEEE*, Prasun Chakrabarti[3]

[1] National Institute of Technology - Arunachal Pradesh, Arunachal Pradesh -791112,
ctbhunia@vsnl.com
2North Eastern Hill University, Shillong,
[3]Sir padampat Singhania University, udaipur

Abstract-A scheme of time variant key is proposed. In the scheme, many different keys are used for different messages as required in achieving perfect security. The enhanced security provided by the proposed scheme is discussed, analyzed and experimentally verified.

Index terms- Perfect Security, Time Variant Key, Brute Force Attack, Differential Frequency Attack

I. INTRODUCTION

The design of an efficient cryptography that provides achievable highest level of security[1] is an important area of investigation. Secured transfers of information over network done by two basic techniques of cryptography are secret key cryptosystem and public key cryptosystem. Respective examples of each of these are DES and RSA. Till date cryptosystems use a single secret and/or a pair of secret & public key. The fundamental research of Shannon[2] defines a perfect secrecy theorem to provide highest level of secrecy. In the perfect secret theorem keys used for encryption/decryption are made to vary from sessions to sessions or from messages to messages. With reported failures[3] of so far known efficient cryptosystems namely DES, RSA and even AES and with ever growing computing power available for attack, there is necessary to design cryptosystems with perfect secrecy. The requirement of many keys in perfect security system is a great research challenge as it needs unique key exchange protocol between a sender and a receiver for exchanging many different keys for many messages. Without loss of generality many keys of perfect secret theorem may be termed as time variant key for transmission of many messages reaching over time, requiring a key for each of messages. Time variant key was implemented by Bhunia[4,5]. By the name Automatic Variable Key(AVK), Bhunia proposed a scheme where different multiple keys are used for different data. In AVK, keys from data to data are exchanged between a source and a destination by the process of a computation between a previous key and a previous data. Experimental works on AVK verify that AVK reduces the effect of differential frequency attack. In the current work we propose a new technique for realizing Time Variant Key. The proposed technique reduces differential frequency attack as well as brute force attack.

II. BASIC IDEA

With brevity the basic idea is illustrated with an example. Suppose n bit key will be used for transmission of m messages from a source, A to a destination, B (fig1). We assume $n=2^c$.We propose that many or all keys of the whole key space of 2^n shall be used in the session , unlike a single key as in DES and AES (or a single key pair as in RSA). For this, whole key space will be divided into several groups each of n bits. Total number of groups will be then 2^n / n equals to say 2^p , where p+c = n. At the beginning of the session, A will select any data of n bits (except a data made of all 0s) called Key for Key Selection, KKS (Say KKS_0). It will be sent to B under existing RSA encryption. n bits KKS_0 is made of p group bits and another c bits. Keys selection for subsequent messages will be indicated by the position of 1's in KKS_0 in the group defined by p. The positional indication is as follows: 1 in RMB (Right Most Bit) position, 1 in one but RMB position … and 1 in LMB (Left Most Bit) position will refer respectively to first, second ….and last key of the group. If there are l such keys, first (l-1) keys will be used for first (l-1) messages and last key for transmission of second KKS, (say KKS_1). The process will continue till the transmission of the all messages is made. Fig1 illustrates the scheme with n=4.. When n=4, c=2, key space (2^n) =16, number of groups = 2^n / n (= $2^{2)}$ and p=2. Session is supposed to transmit messages, $m_{0,}$ m_1, …, …m_i… As the KKSs are secret, the secret keys, ks exchanged under the protocol will remain secret and only known to sender and receiver. The proposed protocol is a typical key agreement protocol for time variant key

III. ANALYSIS

Out of several attacks, two important attacks are brute force attack and differential frequency attack. We analyze the proposed scheme under these attacks.

Brute force attack

When a single key is used, as in existing technique, the probability of success of brute force attack,

$P_0 = m / 2^n$

When multiple keys are used as in proposed scheme, the probability of success of brute force attack:

$P_1 = (m/k) / 2^n$ when $k < 2^n <= m$
$!= 1$ so long $(m/k)< 2^n$

where k = number of different keys used in the protocol

It is seen that $P_1 < P_0$ when k>1.

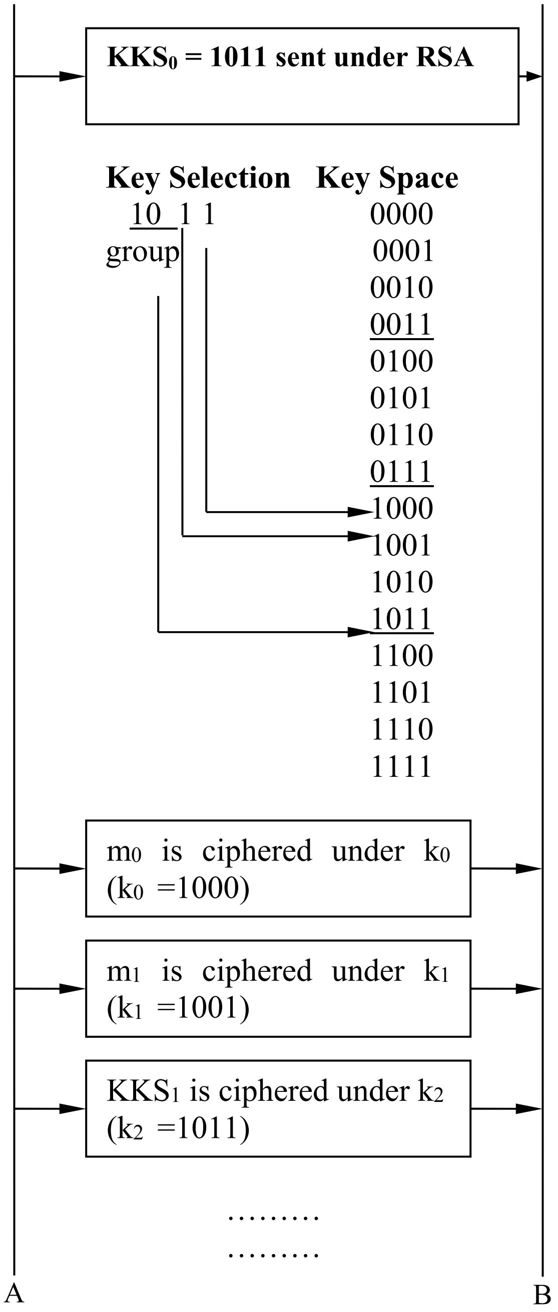

KKS0 = 1011 sent under RSA
Key Selection
Key Space
10 1 1
group
0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111
m0 is ciphered under k0 (k0 =1000)
m1 is ciphered under k1 (k1 =1001)
KKS1 is ciphered under k2 (k2 =1011)
………
………
A
B

Fig. 1 Protocol of time variant key selection & exchange in the proposed scheme

An estimate of k will be as follows: We assume KKSs are selected with equi probability. This is a reasonable assumption as KKSs are independent to each other, and there is no preference for choice. Under the assumption, different time variant keys equal to the number of 1s present in whole key space, N:

$$N = \frac{2^n \times n}{2} = 2^{n-1} \times n \qquad (1)$$

as total number of bits equals to $2^n \times n$ out of which 50% are 1s. Out of total N, number of keys used for transport of KKS except the first one is $2^n - 1$. Thus the total number, k of time variant key used in the proposed protocol is given as:

$$k = (2^{n-1} \times n) - (2^n - 1) \qquad (2)$$

where k is not necessarily the different keys alone, but may also include some keys of the key space used in repetition.

As a proof of equ(2), table I is referred to.

Table I: Proof of equ.(2)

n	Key Space with groups	Estimate of k obtained from pen & paper technique	k from equ.(2)
2	00 01 ……. 10 11	From first group only one key is available but that is used for KKS. From second group two keys are available but one key is used for KKS, thus one key is left for message Total = 1 key for message	1
4	0000 0001 0010 0011 …… 0100 0101	One key, four keys, four keys and eight keys respectively from first, second, third and fourth group, are available.	17

	0110 0111 …… 1000 1001 1010 1011 ……. 1100 1101 1110 1111	Total =17 keys for message (It may be questioned that how 17 keys are used when maximum key space is 16. This is due to repeated use of few keys in groups particular with more1s)	
8	……	………..	769

The value of k increases with n, and as such superiority of the proposed scheme will enhance with higher size of n. Table I predicts this promising picture of the proposed technique. For example when n=8, number of keys (including repeated key over messages/ time out of total different key of 256) is as high as 769.

The superiority of the proposed scheme over existing scheme is also established by comparing the average number of trials required to break a key under the schemes using key exhaustion algorithm. In existing single key scheme the average trials required is $2^n - 1$, whereas in the proposed scheme it is $(2^n - 1) \times (2^k - 1)$ that is much higher than that of existing scheme When k=1, both becomes same and one as it must be.

Differential Frequency Attack

Repetitions of data and characters in messages of plain text result in repetitions of codes in cipher when a single key is used. Repeated codes in cipher are the source of differential frequency attack. Use of different many keys reduces this source of differential frequency attack in cipher, thereby making the proposed scheme superior to existing scheme. This is due to use of different keys in the proposed scheme for making cipher for the repeated data or characters of plain text.

We perform experiments on two sets of messages having repeated characters in plain text. For experimental purpose we took each character as a message. Cipher was generated using (i) DES with single key under existing scheme and (ii) DES with multiple keys under proposed scheme. We measure and compare the repetitions of codes in cipher in the two schemes with a parameter of weighted frequency. The results obtained are shown in the table II. It is found that in both data sets, the proposed technique is superior to existing technique. As weighted frequency of plain text increases the superiority of the proposed scheme enhances.

Table II: Comparison of weighted frequency in different schemes

Weighted Frequency in		
Plain Text	Existing scheme with single key	Proposed scheme with many keys
9.60	1.63	1.59
4.88	1.263	1.263

IV. CONCLUSION

This paper proposes a scheme for the support of time variant key, a version of achieving perfect secret scheme. The results show that the scheme improves the security level of cryptosystem.

REFERENCES

[1]Allen Household et al, “Computer Attack Trends Challenge Internet Security, Security and privacy”, IEEE Computer Society, 2002, pp5-7

[2] C. E. Shannon, “A mathematical theory of communication," Bell System Technical Journal, vol. 27, pp. 379-423 and 623-656, July and October, 1948.

[3] C E Veni Madhavan and P K Saxena, “Recent Trends in Applied Cryptology”, IETE Tech Review, New Delhi, Vol.20, No.2, March-April 2003, pp119-128

[4] C.T.Bhunia et al ,”Experimental Studies on Different Approaches of implementing AVK, Time Variant Key on Information Security**”,** to appear in the proc. IEEE CIT 2008, Australia , July 2008

[5]C.T.Bhunia et al, “Application of Automatic Variable Key (AVK) in RSA” Int’l J HIT Transactions on ECCN, Vol.2, No. 5, Jan-Mar 2007, pp304-311

Design and Development of a Patch Antenna for Dual Band Applications

Janmoni Borah*, Tasher Ali Sheikh, Sahadev Roy

Dept of Computer Science and Engineering
National Institute of Technology,
Yupia, Arunachal Pradesh-791112, India
* borah1989@gmail.com

Abstract **– The paper present the design and development of a compact, low cost and light weight dual band patch antenna, which can operate in dual resonant frequencies in C band and Ku band. The designed antenna gives an operating range of 7.238 to 7.489 GHz for C band and 13.952 to 14.437 GHz for Ku band. The rectangular patch antenna was initially designed with a resonant frequency of 7.5 GHz which is C band using pec. Performance of the designed antenna has been improved to operate in Ku band by adding meta-material concept in the design by removing a square slot from the patch which provided a resonant frequency of 7.4 GHz at C band and 14.1 GHz at Ku band and thus results in an antenna which can operates in both C and Ku band. The designed antenna is simulated using Ansoft HFSS, a FEM based simulator and antenna's characteristics such as Return loss, Gain, Directivity, VSWR are reported in this paper.**

Index terms **-** Patch antenna, Rogers RT/Duroid substrate, Return loss, VSWR, Radiation pattern, Axial ratio, Ansoft HFSS simulator.

I. INTRODUCTION

Microstrip patch antenna has become a perfect choice for communication system mostly in the field of RFID applications because of the capability to integrate with microwave circuits. These types of antenna are well suited for WLAN applications [1]. With the increase in demand and market for wireless communication, most of the fastest and robust WLANs (e.g. IEEE 802.11) start to operate in the C band, so that reliable and high speed connection can be obtained. These two bands are mostly used for long-distance radio telecommunications [2]. For satellite communication purposes, C band offers better services under adverse weather conditions compared to Ku band. Most of the Radar systems and its applications use relatively high power Transmitters and Receivers, so it is made to operate on a band which is not used for other services. Ku band place themselves greatly in the field of satellite communications mostly for fixed and broadcast services [3]. We consider some basic criteria of design such as Return loss, Gain, Directivity, VSWR and Radiation pattern. Microwave towers, mobile services, mobile satellite services, radio location service and radio navigation operate in the Ku band to provide high speed connectivity and reliability. Ku band offers several advantages such as flexibility to a user, cheaper and enables smaller antennas because of using higher frequency and a focussed beam. This band has some disadvantages too such as, in case of heavy rainfall areas when operating at a frequencies greater than 10 GHz, rain fade occurs, which degrade signal quality. The antenna type designed radiates due to the fringing fields between the patch edge and the ground plane [4].

The patch antenna presented in this paper consists of a radiating patch on the top of a dielectric substrate and a ground plane on below side as shown in the Fig.1.

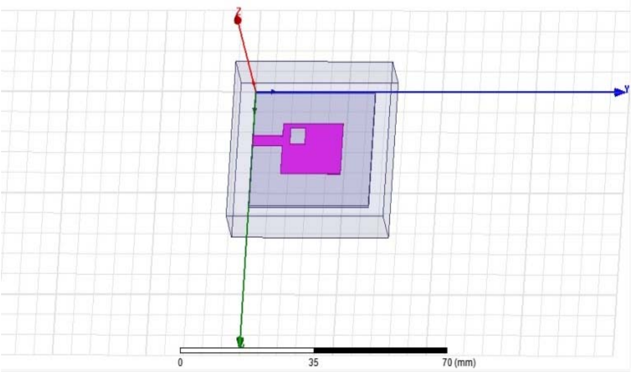


Fig.1 Simulation model of dual band patch antenna.

II. THEORY AND DESIGN

The designing of an antenna based on Microstrip patch requires a huge calculations and considerations such as width (W) and length (L) of the antenna, the effective dielectric constant ($\in_{eff}$) based on the substrate used, effective (ΔL) and actual (L) patch length [5]. The design antenna model given in this paper can be betterly used in a communication system especially for C band applications when used with a bandpass filter having center frequency of C band range [6].

The antenna is design on an RT/Duroid 5880(tm) substrate with relative permeability of 2.2, loss tangent of 0.0009 and a thickness (height) of 0.05mm. A Microstrip line is used as a feed point which must be located at that point on the patch such that input impedance is 50Ω for the resonant frequency used. So a trial and error method is used in the design for different position of the feed point and then return loss (S11) is compared and found a point along the length of the patch for feed where S11 is most negative. The patch used for radiating is a perfect electric conductor (pec) usually made up of copper or gold [7]. The antenna is designed with implementation of some meta-material concept in the patch such as forming slots [8].

It is found and to be noted that, while designing a rectangular patch, the length (L) of the patch is usually 0.333 $\lambda_0 < L < 0.5\ \lambda_0$, where λ_0 is the free space wavelength [9]. Also the patch thickness (t) is selected such that $t << \lambda_0$ and height of the dielectric substrate (h) is usually 0.333 $\lambda_0 < h < 0.5\ \lambda_0$ [10], [11]. The designed antenna has an estimated length (L) and width (W).

The length and width of the patch antenna can be calculated using equations (1), (2), (3) and (4) [12].

$$W = \frac{c}{2f_0}\sqrt{\frac{2}{\epsilon_r + 1}} \tag{1}$$

Where, f_0=7.5 GHz, ϵ_r=2.2

The effective dielectric constant based on the substrate height (h=0.05mm) used, can be calculated as.

$$\epsilon_{eff} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2}\left(1 + 12\frac{h}{W}\right) \tag{2}$$

The effective patch length (ΔL) can be calculated using.

$$\frac{\Delta L}{h} = 0.412\frac{\epsilon_{eff} + 0.3\left(\frac{W}{h} + 0.264\right)}{\epsilon_{eff} - 0.258\left(\frac{W}{h} + 0.8\right)} \tag{3}$$

And the actual patch length (L) is given by.

$$L = \frac{c}{2f_r\sqrt{\epsilon_{eff}} - 2\Delta L} \tag{4}$$

The Table.1 represents the dimensions and properties for different materials used in the design shown above in Fig.1.

TABLE I. DIMENSION OF DUEL BAND PATCH ANTENNA

Materials Used		Dimension In Millimetre(Mm)	
Properties	**Purposes**	**Position**	**Size**
Air	**Boundary**	**-5 ,-5 ,-5.794**	**X=38.1 Y=42 Z=10.794**
PEC (Perfect Electric Conductor)	**Ground**	**0 ,0 ,-0.794**	**X=28.1 Y=32 Z= -0.05**
	Patch	**7.825 ,8 ,0**	**X=12.45 Y=16 Z=0.05**
	Slot	**9,10,0**	**X=4 Y=4 Z=0.05**
Rogers RT/Duroid5 880 (Tm)	**Dielectric Substrate**	**0 ,0 ,0**	**X=28.1 Y=32 Z=-0.794**
Rectangular Sheet	**Lumped Port**	**10.937, 0, -0.844**	**Axis=Y X=2.46 Z=0.844**

III. RESULTS

The design antenna's behaviour and characteristics was simulated using Ansoft HFSS. The Return loss of an antenna measured the reflected energy from a transmitted signal. The larger the value, the less energy is reflected. The Fig.2 shown below depicts a results in return loss of -19.229 at 7.4 GHz and -16.234 at 14.1 GHz respectively.

The centre frequency for an antenna is selected as the one at which return loss (S11) is minimum. From the Fig.2 shown below, the centre frequencies operating at C band and Ku band are 7.4 GHz and 14.1 GHz respectively. The antenna operating frequency range obtained for C band is 7.23 to 7.48 GHz and for Ku band is 13.95 to 14.43 GHz.

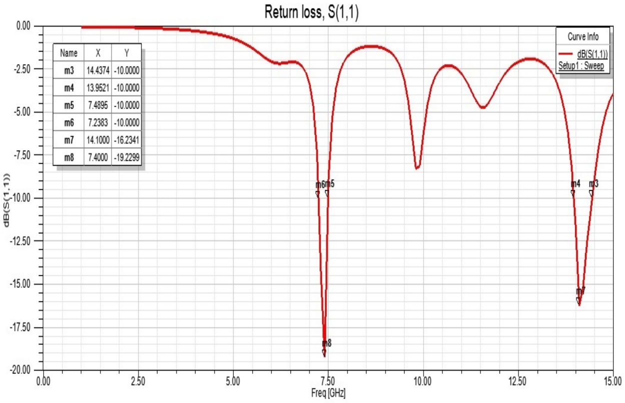


Fig.2 Return loss vs. frequency

The impedance bandwidth and percentage bandwidth for the proposed antenna can be calculated using equation (5) and (6) given below.

$$\text{Impedance bandwidth} = F_H - F_L \tag{5}$$

$$\text{Percentage bandwidth} = \left(\frac{F_H - F_L}{2F_C}\right) * 100 \tag{6}$$

Where, F_H =Upper cut-off frequency
F_L =Lower cut-off frequency

Now for operating frequency 7.23 to 7.48 GHz i.e. for C band, the Impedance bandwidth is 0.25 GHz and percentage bandwidth is 1.68 %. For operating frequency of Ku band i.e. 13.95 to 14.43 GHz, the impedance bandwidth is 0.48 GHz and percentage bandwidth is 1.7 %.

The above calculated results for C band and Ku band states that the design antenna can be used for narrow band applications. The Fig.3 shown below depicts information related to antenna impedance matchings. The VSWR obtained from the plot for C band is 1.9 at 7.4 GHz and for Ku band is 2.7 at 14.1 GHz.

The smith chart showing scattering parameter S11, Gain and Directivity of the proposed antenna are shown below in Fig.4, 5 and 6 below respectively [13]. It is seen that Gain and directivity of the proposed antenna is 7.25 dBi and 7.32 dBi respectively.

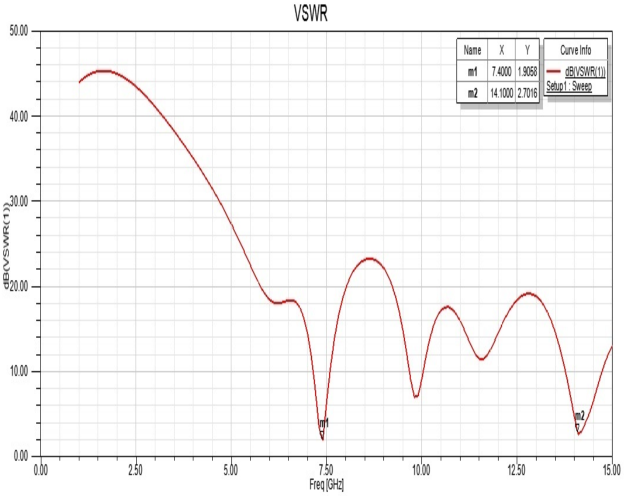


Fig.3. VSWR vs. frequency plot

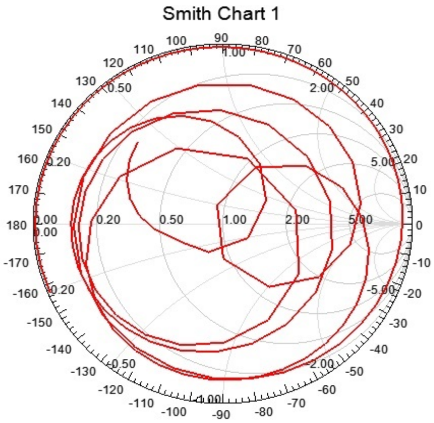


Fig.4. Smith chart showing S11 vs. Frequency

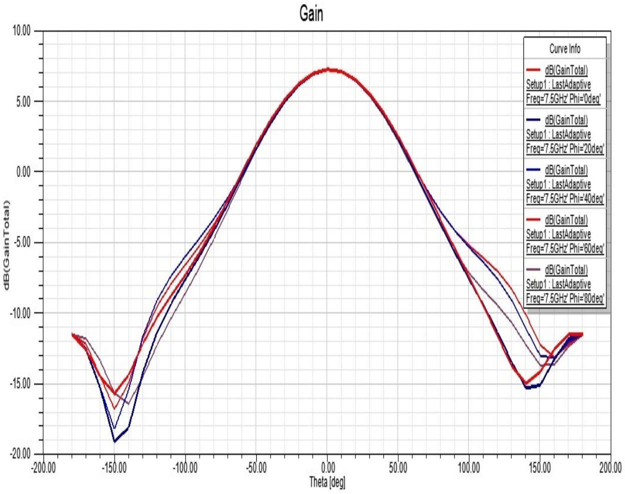


Fig.5. Patch antenna with gain 7.2 dBi

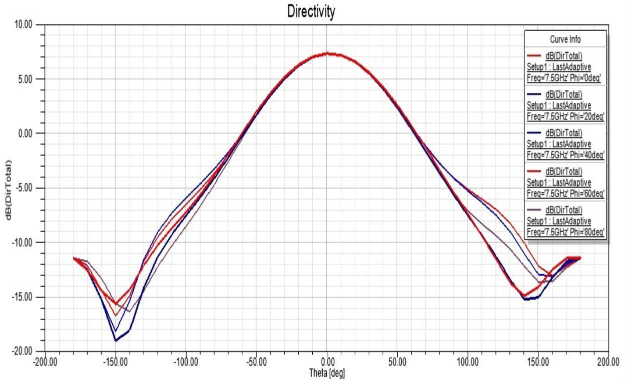


Fig.6. Patch Antenna with Directivity 7.3 dBi

The Radiation pattern of an antenna defines the directional dependence of the signal strength. It also represents the far field graphically as a rectangular or polar plot. Axial ratio shown below in Fig.9 defines the electromagnetic radiation and antenna polarization. The far field radiation pattern, 3D rectangular and polar radiation plot and axial ratio of the proposed antenna have been shown below in Fig.7, 8 and 9 respectively.

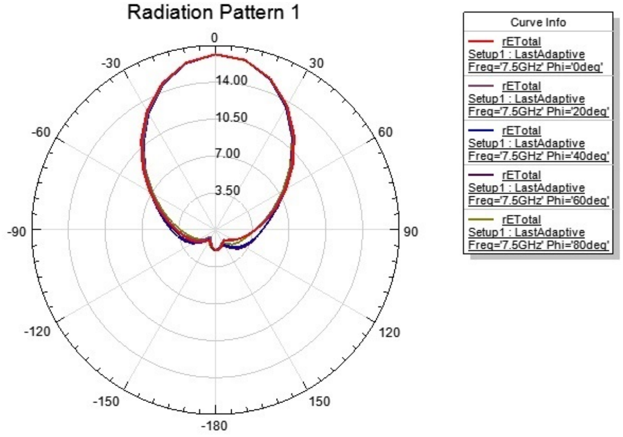


Fig.7. Radiation pattern of the antenna

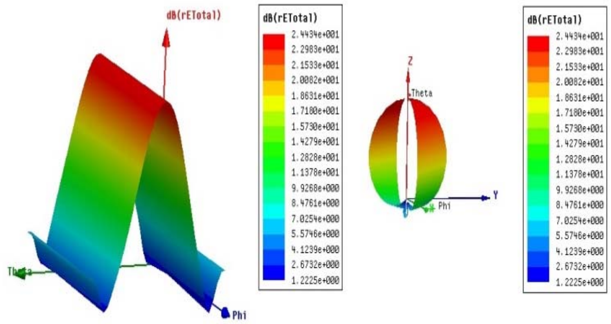


Fig.8. 3D Rectangular and Polar plot of the antenna

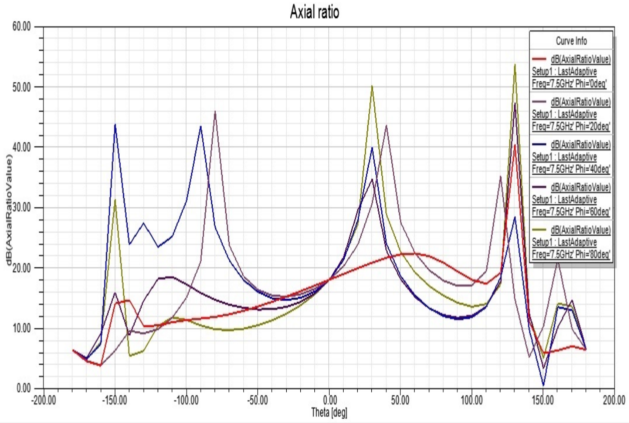


Fig.9. Axial ratio value in dB at 7.5 GHz

IV. Conclusions

The parameters of an antenna such as Return loss, VSWR, Gain, Directivity and Radiation pattern have been obtained. From the above theories and discussions included in this paper, it is found that the results obtained for the model after simulations shows a good agreement and can be a good approach for C band and Ku band narrow band applications. The operating frequencies obtained for the proposed antenna is 7.4 and 14.1 GHz, which covers the C band and Ku band respectively and provides good result in terms of bandwidth.

Acknowledgment

We would like to thank IC Design and Fabrication centre, Jadavpur University, Kolkata for providing software facilities to carry out this research work.

References

[1] Vivek Hanumante and Sahadev Roy “Comparative Study of Microstrip Patch Antenna Using Different Dielectric Materials,” in 9th International Conference on Microwaves, Antenna, Propagation and Remote Sensing (ICMARS-2013),pp 56-60, Dec 2013.

[2] D.M Pozar., and D.H Schaubert Microstrip Antennas, the Analysis and Design of Microstrip Antennas and Arrays, IEEE Press, New York, USA 1995.

[3] C.A Balanis. Antenna Theory: Analysis and Design, John Wiley & Sons. 2005.

[4] G, Ramesh, B. Prakash, B, Inder and A. Ittipiboon. Microstrip antenna design handbook, Artech House 2001.

[5] Panchatapa Bhattacharjee, Vivek Hanumante and Sahadev Roy “Design of U-Slot Rectangular Patch Antenna for Wireless LAN at 2.45GHz,” in 9th International Conference on Microwaves, Antenna, Propagation and Remote Sensing (ICMARS-2013), pp 132-135, Dec 2013.

[6] Tasher Ali Sheikh, Janmoni Borah and Sahadev Roy, “Bandwidth improvement in BPF using Microstrip coupled lines,” ICSSP’14 conference, ELSEVIER publications, pp.105-109, August 2014.

[7] M.Z.A Aziz, , Z. Zakaria, M.N Husain, N.A. Zainuddin,, M.A Othman and B.H. Ahmad, "Investigation of dual and triple meander slot to microstrip patch ANTENNA," MICROWAVE Techniques (COMITE), 2013l Conference., pp.36,39, 17-18 April 2013.

[8] S. Koziel and S. Ogurtsov, “A study of basic slot antenna configurations using simulation-driven optimization,” in Antennas and Propagation Society International Symposium (APSURSI), 2012 IEEE , pp.1-2, July 2012

[9] Waterhouse, R. B., S. D. Targonski, and D. M. Kokoto, “Design and performance of small printed antennas,” IEEE Trans. Ant. Prop., Vol. 46, 1629–1633, 1998.

[10] Zeadally, S. and L. Zhang, “Enabling gigabit network access to end users,” Proc. IEEE, Vol. 92, No. 2, 340–353, 2004.

[11] Sharma, A. and G. Singh, “Design of single pin shorted three dielectric layered substrate rectangular patch microstrip antenna communication systems,” Progress In Electromagnetics Research Lett., Vol. 2, 157–165, 2008.

[12] R. B.Waterhouse, Microstrip Patch Antennas, A Designer’s Guide, Kluwer Academic Publishers, 2003.

[13] W. Wiesbeck, G. Adamiuk, and C.Sturm, "Basic Properties and Design Principles of UWB Antennas," Proceedings of the IEEE, vol.97, no.2, pp.372- 385, Feb. 2009.

Papaya Genotype Tolerant to Papaya Ring Spot Virus (PRSV) under Field Condition In Gangetic Plains Of West Bengal

A. Chakraborty[1], S. K. Sarkar[2] ,

Department of Pomology and Post Harvest Techonology,
Faculty of Horticulture, Pundibari, Cooch Behar, Pin-736165

1. Assistant Professor of Uttar Banga Krishi Viswavidyala: aditi.chatterjee10@gmail.com
2. Professor of Bidhan Chandra Krishi Viswavidyalaya, Nadia, West Bengal- 741252

ABSTRACT

Papaya (*Carica papaya* L) a popular fruit crop, cultivated throughout the tropical and subtropical region in the world for its highly nutritious fruits. Fruits are rich in vit. A and vit. C, minerals and unripe fruits contain papain a protiolitic enzyme used in medicinal and industrial purposes. Areas under papaya have decreased due to highly susceptibility of the crop to Papaya ring spot virus (PRSV). None of the commercial varieties found to resistance to PRSV. However, screening of germplasm for identifying the field tolerant lines of papaya was carried out with disease intensity score, viz. 0-1: apparently healthy, 1.1-2.0: moderately resistance, 2.1-3.0: moderately susceptible, 3.1-4.0: susceptible, 4.1 and above highly susceptible. Among the 22 genotypes evaluated in HRS, farm in Mondouri, BCKV, Local Selection-1 have disease tolerant capacity with 0.5 disease intensity score. The germplasm Local Selection-1 produced 45.05 kg/plant in 1st year and 25.12 kg/plant in 2nd year.

INTRODUCTION

Papaya (*Carica papaya* L) a popular fruit crop, grown in many parts of the world for its delicious fruit and for extraction of its digestive constituent papain. In India, among different fruit crops grown, papaya cultivation ranks fifth with regards to area and production. The major constrain in cultivation of papaya is its susceptibility to a number of disease and particularly the disease caused by a strain of Papaya ring spot virus (PRSV-P). This disease has posed a major threat to papaya cultivation throughout India by rendering orchards economically unproductive. PRSV infection occurs in every region irrespective of the agro climatic condition and disease can result in crop losses up to 85-90% (Lokhande *et al*, 1992; Hussain and Verma, 1994). Most of the commercial varieties grown in India are susceptible to PRSV. In this study, identification of field tolerant genotypes from the germplasm collection was carried out.

MATERIALS AND METHODS

The experiments were carried out at Horticulture Research Station, Mondouri, BCKV, Mohanpur, Nadia. Seeds of 22 papaya genotypes were sown in seedbed during February 2009. The experiment was laid out in Randomised Block Design with three replications. The 45 days old seedlings were transplanted in the main field at 2x2 m distance. Before transplanting, the land was prepared following proper agronomic practices. All recommended package of practices were followed during the crop season for raising a healthy crop.

Observations were taken during the cropping period of 1st and 2nd year and disease intensity scoring was given based on the symptoms in leaves and stems as per the scale developed by Dhanem (2006). The scale consists of five levels based on the symptoms exhibited by the plant.

Intensity score	Reaction
0.0-1.0	Apparently healthy
1.1-2.0	Moderately resistant
2.1-3.0	Moderately susceptible
3.1-4.0	Susceptible
4.1 and above	Highly susceptible

RESULTS AND DISSCUTION

The results of the screening experiment revealed that out of 22 germplasm screened, none of them were found resistant but showed different degree of disease intensity during the study period and symptoms appeared on leaves, stems, petioles and fruits.

During 1st year, the intensity of disease in the germplasm ranged from 0.5 to 4.60. Among them, the germplasm Local Selection 1 registered the lowest score of 0.5, followed by Local Selection 2 (1.1) and Shillong (1.2) with moderate field resistance. The lines such as Surya (4.8), Red Lady (4.6), Pusa Dwarf (4.25) and Pusa Nanha (4.0) registered the highest disease intensity score thus classified as highly susceptible.The genotypes classified as moderately resistant to moderately susceptible in 1st year became susceptible to highly susceptible in 2nd year except Local Selection 2, Sel 42 AC F_1 and Shillong.

Wide range of yield variation was found in the lines were only moderately resistance to susceptible during 1st year. The lines which are classified as highly susceptible showed reduction in yield during the 1st year itself. The genotype Local Selection-1recorded the highest yield of 45.05 kg/plant/year followed by Shillong (43.22kg/plant/year). The lines which fall under the category of highly susceptible viz., Surya and Red Lady registered the lowest yield of 2.8 kg/plant and 9.49 kg/plant respectively. There was a drastic reduction in yield in susceptible and highly susceptible lines in 2nd year compared to 1st year. The yield performance of highly susceptible lines ranged from 1.9 kg to 4.98 kg and susceptible lines was 2.39 kg to 6.72 kg during the second year.

The disease intensity scored in 2nd year ranged from 0.25 to 4.9. Local Selection 1, Local Selection 2, Sel 42 AC F_1 and Shillong showed a disease tolerant capacity in 2nd year.

None genotype except Local Selection-1showed a better yield (25.12 kg) in 2nd year.Leaf size and flower production continued throughout the cropping season but in case of highly susceptible cultivars were crinkled, filiformed and size was very much reduced and growth was arrested.

Among all the 22 genotypes tested in 2nd year Local Selection-1 and Shillong found PRSV tolerant capacity with better yield potentiality and it will reconfirmed by testing in different locations and seasons for its tolerance against PRSV.

Literature Cited

Hussain, S. And Verma, A. 1994. Occurrence of papaya ring spot virus from Amritsar (Punjab) India. *Phytopath. Res.* **7**:77-78.

Lokhande, N.M., Moghe, P.G., Matte, A.D. and Hiware, B.J. 1992. Occurrence of Papaya ringspot virus (PRSV) in Vederva region of Maharashtra. *J. Soils and Crops* **2**:36-39.

Dhanam, S. 2006. Studies on papaya ring spot disease. M. Sc. (Plant Pathology) Thesis, Tamil Nadu Agricultural University, Coimbatore, India.

Table 1. Reaction of papaya germplasm to PRSV infection under field condition.

Sl.no.	Genotype	First year			Second year		
		Disease intensity score	Reaction	Yield/plant	Disease intensity score	Reaction	Yield/plant
1	CO-3	3.75	S	18.20	4.2	HS	11.30
2	Surya	4.8	HS	2.80	4.9	HS	1.90
3	Pau-Selection	2.9	MS	6.63	3.2	S	4.63
4	Pusa-Dwarf	4.25	HS	17.01	4.75	HS	7.67
5	Red-Lady	4.6	HS	9.49	4.75	HS	6.41
6	Bangalore-Dwarf	3.2	S	13.41	3.0	S	9.37
7	Local Selection-1	0.5	AH	45.05	0.25	AH	25.12
8	Local Selection-2	1.1	MR	10.88	0.75	AH	5.14
9	Sel42ABF$_1$	1.8	MR	14.08	3.25	S	2.75
10	Sel42ACF$_1$	1.5	MR	30.92	1.0	AH	5.24
11	Pusa-Nanha	4.0	HS	14.72	4.2	HS	4.98
12	Pusa-Delicious	2.5	MS	14.87	3.0	S	6.28
13	Shillong	1.2	MR	43.22	1.0	AH	14.85
14	Farm-Sel^{n}	2.5	MS	6.58	2.75	MS	2.05
15	CO-2	2.0	MR	10.71	3.0	MS	3.14
16	CO-5	2.25	MS	12.54	3.25	S	3.23
17	CO-6	3.0	S	19.88	3.25	S	6.30
17	CO-7	3.5	S	9.08	3.5	S	4.70
19	Ranchi Selection	1.75	MR	7.82	3.15	S	3.08
20	KNR-Selection	2.8	MS	6.65	3.5	S	2.39
21	Coorg Honey Dew	2.0	MS	15.29	3.8	S	6.72
22	Thailand	3.0	S	10.93	3.5	S	3.39

HS=Highly susceptible, **MS**=Moderately susceptible, **S**=Susceptible, **MR**=Moderately resistance, **AH**=Apparently healthy

Weaknesses of a More Efficient and Secure Dynamic ID-Based Remote User Authentication Scheme

Subhasish Banerjee
Computer Science and Engineering
National Institute of Technology
Arunachal Pradesh, India
subhasish.cse@nitap.in

Manash Pratim Dutta
Computer Science and Engineering
National Institute of Technology
Arunachal Pradesh, India
manash.cse@nitap.in

Chandan Tilak Bhunia
Computer Science and Engineering
National Institute of Technology
Arunachal Pradesh, India
ctbhunia@vsnl.com

***Abstract*— Password based authentication schemes have been widely used to verify the legitimacy of a user over an insecure communication channel. A common feature among most of the published schemes is that user's identity (ID) is static in all the transaction sessions, which may leak some information about the user and can create risk of identity theft during message transaction. Therefore, to provide user anonymity, many dynamic ID based remote users authentication schemes have been proposed. Recently, Khan et al. proposed an efficient and secure dynamic ID based remote user authentication scheme and claimed that their scheme can provide strong security against various attacks. In this paper, we have demonstrated that Khan et al.'s scheme is vulnerable to server spoofing attack and insider attack, and has some flaws in login and authentication phase as well.**

Keywords*— *Dynamic ID; Authentication; Cryptography; User anonymity and Smart card

I. INTRODUCTION

Recently, the popularity of computer networks and fast progress of computer technologies on a multiuser system make feasible the sharing of expensive resources. However, sharing may cause some undesirable phenomena such as unauthorized access and inconsistent status of shared resources. Therefore, password-based authentication schemes have been widely adopted to protect the resources from unauthorized access. In conventional password based authentication system, the server maintains a password table to verify the user's login request as, for example, Lamport's scheme [1] and some modified schemes such as those of Lemon et al. and Yen et al. [2-3]. But due to the storing of password table, it became more expensive for maintaining and if attacker changes the entry of the table by any means, then whole system will be damaged. To reduce such cost for protecting and maintaining the verifier table on remote system, many smart card based remote user authentication schemes [4-13] have been proposed. A common feature among most of the user authentication schemes is that the user's identity is static, which may leak some information about the user and create risk of ID-theft during the message transmission over an insecure channel. To overcome such risk of ID theft or user impersonation, in 2004, Das et al. [14] proposed a dynamic ID based remote user authentication scheme and claimed that their scheme is secured against replay, forgery, password guessing, insider and stolen verifier attacks. Unfortunately, later on, some researchers [15-17] reveled that their scheme is no longer secure as they claimed and then further proposed some improved remote user authentication schemes, which overcome from all the above stated drawbacks. Moreover, recently Wang et al. [18] showed that Das et al.'s scheme does not provide mutual authentication and cannot resist server spoofing attacks as well and then proposed a dynamic ID based remote user authentication scheme and claimed that their scheme is more efficient and secure than existing schemes. But In 2010, Khan et al. [19] have pointed out the weaknesses of Wang et al.'s dynamic ID based remote user authentication scheme. He showed that Wang et al.'s scheme is vulnerable to insider attack, does not preserve user anonymity, no provision for revocation of lost or stolen smart card and no support for session key agreement during authentication process. To overcome the identified problems, they have further proposed an enhanced smart card based authentication scheme and claimed that it improves all the identified weaknesses of Wang et al.'s scheme and is more secure and robust for real life use. Unfortunately, during our research, we found that Khan et al.'s scheme is not as much secured as they claimed and has some drawbacks. In this paper, we demonstrate that Khan et al.'s scheme is vulnerable to server spoofing attack and insider attack, and has some flaws in login and authentication phase as well. The rest of this paper is organized as follows. We have given a brief review on Khan et al.'s scheme and demonstrate vulnerabilities of Khan et al.'s scheme, in section II and section III respectively. Finally, we complete this paper with conclusion in section IV.

II. REVIEW OF KHAN ET AL.'S SCHEME

Khan et al. [18] proposed a dynamic ID based remote user authentication scheme in which the remote server does not need to maintain any verification table. Due to simplicity, computational efficiency and proven security, they used simple hash function to propose their scheme. The scheme consists of five different phases namely: registration, login, authentication, password-change and revocation of stolen smart phase. Here, we explain the registration, login and authentication phase only, because we will use them to carry out the security analysis. Table 1 describes the notations used in this paper.

TABLE I. NOTATION

Notation	*Description*
U_i	User i
PW_i	Password of user i
ID_i	Identity of user i
S	Authentication server
h(.)	A secure one way hash function
CID_i	Dynamic ID of user i
x	The master secret key maintained by registration centre
y	The secret number generated by registration center
$\oplus$	Exclusive-or operation
$\|$	Message concatenation

A. Registration Phase

This phase is invoked whenever user U_i initially registers or re-registers to the authentication server S. N denotes the number of times a user U_i registers to authentication server S. This value of N is used to revoke a smart card in case of theft or stolen and its value is stored in users U_i account database on the authentication server S. The secret keys x are securely stored in the authentication server S. The following steps are performed to complete the registration phase:

1) U_i chooses his ID_i and PW_i and generates a random number r and computes $RPW = h(r \| PW_i)$.
2) U_i submits his ID_i and RPW to the S over a secure channel.
3) S checks the registration credentials of U_i and verifies whether his chosen ID_i is already in the database or not. If ID_i already exists in the database, S intimates U_i to choose another ID_i. In addition, S checks the registration record of U_i and if U_i is a new user then S sets value of N = 0, otherwise if U_i is re-registering in the system then S sets N = N+1 and stores the values of ID_i and N in the database.
4) S computes $J = h(x \| IDU)$, where $IDU = (ID_i \| N)$.
5) S computes $L = J \oplus RPW$.
6) Then, S issues smart card to U_i which contains values of L and y over a secure channel.
7) U_i securely stores random number r in the smart card.

B. Login Phase

When U_i wants to login to S, user inserts his/her smart card in the terminal and inputs his ID_i and PW_i, then Smart card performs the following steps:

1) Computes $RPW = h(r \| PW_i)$ and $J = L \oplus RPW$, where random number r is securely pre-stored in the smart card.
2) Acquires the current timestamp T and computes $C_1 = h(T \| J)$.
3) Generates a random number d and computes an anonymous ID of U_i by $AID_i = ID_i \oplus h(y \| T \| d)$.

At the end of login phase, U_i sends login message m $=\{AID_i, T, d, C_1\}$ to S for the authentication process.

C. Authentication Phase

Upon receiving the login message m, the authentication server S performs the following steps:

1) Checks the validity of time stamp with the current date and time T'. If $(T'-T) \leq \Delta T$ holds, S accepts the login request of U_i, otherwise the login request is rejected.
2) S computes $ID_i = AID_i \oplus h(y \| T \| d)$ and validates, if ID_i is a valid user's ID then performs further operations, otherwise terminates the operation and informs U_i about it.
3) Checks the value of N in the database and computes IDU $= (ID_i \| N)$.
4) Computes $J = h(x \| IDU)$ and checks whether $h(T \| J)$ is matched with C_1 or not. If they are equal, it means U_i is an authentic user and S accepts the login request, otherwise the login request is rejected and user is informed about the decision.
5) Computes $C_2 = h(C_1 \oplus J \oplus T_s)$ and sends the message $\{C_2, T_s\}$ to U_i, where T_s is current timestamp of the server.
6) After receiving the response message from S at time T'', U_i checks the validity of time stamp whether $(T''-T_s) \geq \Delta T$, if not, U_i computes $h(C_1 \oplus J \oplus T_s)$ and compares with the received C_2. If it is same, U_i authenticates the remote server S, otherwise terminates the operation.
7) Lastly, U_i and S share the symmetric session key $S_k = h(C_2 \oplus J)$.

III. CRYPTANALYSIS OF KHAN ET AL.'S SCHEME

In this section, we have demonstrated that Khan et al.'s scheme does not withstand server spoofing attack and insider attack, and has flaws in login and authentication phase as well.

A. Server Spoofing Attack

Here, we will show that khan et al.'s scheme is vulnerable to server spoofing attack. In this kind of attack, the attacker can easily impersonate as a server S to cheat U_i and gets the secret information from U_i. Assume that the attacker U_z is an another legal user, then he/she can get the secret information y and L from his/her smart card and intercept the login request message $m = \{AID_i, T, d, C_1\}$ between the real user U_i and the server S. Then, U_z computes the following steps to impersonate as a server and retrieves the information from the real user U_i. Note that the secret information x and y are used and stored in all legal users' smart card and U_z knows U_i as a newly registered user.

1) U_z inserts his smart card and enters his identity ID_z and password PW_z, then computes the following

$$RPW_z = h(r \| PW_z)$$
$$J_z = L \oplus RPW_z = h(x \| IDU_z)$$

2) U_z examines all the possible values of x and computes $h(x^* \| IDU_z)$ and compares with J_z, where $IDU_z =$

$(ID_z \| N)$. If matched, then U_z successfully extracts the server's secret key $x = x^*$.

3) $ID_i = AID_i \oplus h(y \| T \| d)$, $J_i = h(x \| IDU_i)$, and calculates $h(T \| J_i)$ and compares with received C_1, after successful verification, U_z sends the message $C_2^* = h(C_1 \oplus J_i \oplus T_s)$ and T_s to the legal user U_i for mutual authentication.
4) Upon receiving the mutual authentication message, U_i verifies the time interval between T_s and T'', where T'' is the timestamp when the mutual authentication message is received.
5) After successful verification, U_i checks whether $h(C_1 \oplus J_i \oplus T_s)$ is matched with C_2^* or not. Obviously it will be matched because, attacker kept C_1, and J_i as it is in C_2^*.

As a result, the user U_i authenticates the attacker U_z as a server and shares the symmetric session key $S_K = h(C_2 \oplus J)$ with U_z.

B. Insider Attack

Here, we have shown that khan et al.'s scheme fails to prevent the insider attack. If the attacker is a legal user U_z, then he/she can get the secret information y and L from his smart card and intercept any previous login request message m = $\{AID_i, T, d, C_1\}$. Attacker extracts the secret value x from his/her own smart card by using the steps 1 and 2 of server spoofing attack. Cryptanalysis steps works as follows, we assume that U_z knows U_i is a newly registered user.

1) $ID_i = AID_i \oplus h(y \| T \| d)$, $J = h(x \| IDU_i)$. Where $IDU_i = (ID_i \| N)$.
2) Acquires the current time stamp T^* and computes $C_1^* = h(T^* \| J)$.
3) Generates a random number d^* and computes $AID_i^* = ID_i \oplus h(y \| T^* \| d^*)$ and creates the forge login request m = $\{AID_i^*, T^*, d^*, C_1^*\}$ to S for the authentication process.
4) After receiving the message m, server S verifies the validity of time interval between T^* and T'. After validating the time interval, server S goes to the next step.
5) Computes $ID_i = AID_i^* \oplus h(y \| T^* \| d^*)$ and verifies that ID_i is valid or not. As because kept value of ID_i by the attacker is same, so server will validate ID_i successfully.
6) S Checks the value of N in the database and computes $IDU = (ID_i \| N)$.
7) Further computes $J = h(x \| IDU)$ and checks whether $h(T^* \| J)$ equals to C_1^* or not. Obviously, it will be matched and server S authenticates the attacker U_z as a legal user and accepts the login request.
8) S computes $C_2 = h(C_1^* \oplus J \oplus T_s)$ and sends the mutual authentication message $\{C_2, T_s\}$ to U_z .

As a result, the server S authenticates the attacker U_z as a real user U_i and shares the symmetric session key $S_K = h(C_2 \| J)$ with the intruder U_z.

C. Flaws in Login and Authentication Phase

In login phase of the Khan et al.'s scheme, the user U_i first inserts his smart card into the card reader and enters the values of ID_i and PW_i. The smart card does not verify PW_i or ID_i which has been entered by the users. Thus even if the user U_i enters his/her wrong password and/or wrong identification, which may be the identification of another registered user, by mistake, both the login phase and authentication phase are still continued, and finally, at the end of authentication phase, S rejects the U_i login request. Therefore, it causes unnecessary extra communication and computational overheads during the login and authentication phase. The complete scenario of such situation is defined as below:

Assume that the user U_i enters his/her password and identification wrongly like PW_i^* ($\neq PW_i$) and/or ID_j ($\neq ID_i$) respectively. Accordingly, login phase of Khan et al.'s scheme works as follow:

1) $RPW = h(r \| PW_i^*)$ and $J = L \oplus RPW \neq h(x \| IDU)$
2) $C_1 = h(T \| J) \neq h(T \| h(x \| IDU))$
3) $AID_i = ID_j \oplus h(y \| T \| d)$
   i.e $\neq ID_i \oplus h(y \| T \| d)$

After sending the message m = $\{AID_i, T, d, C_1\}$ to S, the server S will compute the following in authentication phase.

4) Verifies $(T'-T) \leq \Delta T$ and proceeds to the next step.
5) $ID_j = AID_i \oplus h(y \| T \| d) \neq ID_i$

As ID_j is a valid user ID, S verifies ID_j successfully and checks the value of N in the database of corresponding ID_j.

6) $IDU = (ID_j \| N) \neq IDU_i$
7) $J = h(x \| IDU)$ and checks whether $h(T \| J)$ is matched with C_1 or not.

There will be mismatch and thus, S will reject U_i's login request message. Hence, the user U_i is totally unaware of the fact that he/she has entered wrong password and/or wrong identification in login phase. We thus note that if the user's password and identification verification take place at the very beginning of login phase, then we can prevent the unnecessary extra communication and computational overheads during the login and authentication phase

IV. CONCLUSION

Khan et al. proposed a more efficient and secure dynamic ID based remote user authentication scheme to overcome the security issues found in Wang et al.'s scheme. However, we have pointed out Khan et al.'s scheme is not too much secure enough and suffered from server spoofing and insider attack, and has some flaws in login and authentication phase. Therefore, we can design and enhance a new dynamic ID based remote user authentication scheme which can provide strong security and will resolve the security issues of existing schemes.

REFERENCES

[1] L. Lamport, Password authentication with insecure communication, communication of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[2] R. E. Lemon, S. M. Matyas, C. H. Meyar, Cryptographic authentication of time-invariant quantities, IEEE Trans. Commun. Vol. 29, pp. 773-777, 1981.

[3] S.M. Yen, K.H. Liao, Shared authentication token secure against replay weal key attacks, Inform. Process. Lett. Vol. 62, pp.77-80, 1997.

[4] M. S. Hwang, L. H, Li, A new remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics, vol. 46, no. 1, pp. 28-30, 2000.

[5] E. J. Yoon, E. K. Ryu, K. Y. Yoo, Further improvement of an efficient password based remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics, Vol. 50, no. 2, pp-612-614, 2004.

[6] M. L. Das, A. Saxena, V. P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Transaction on Consumer Electronics, vol. 50, no. 2, pp. 629-631, 2004.

[7] C. W. Lin, C. S. Tsai, M. S. Hwang, A new strong password authentication scheme using one-way Hash functions, Journal of Computer and Systems Sciences International, vol. 45, no. 4, pp. 623-626, 2006.

[8] C. S. Bindu, P. Reddy, B. Satyanarayana, Improved remote user authentication scheme preserving user anonymity, International Journal of Computer Science and Network Security, vol. 83, pp. 62-66, 2008.

[9] L. Fan, J. H. Li, H. W. Zhu, An enhancement of timestamp-based password authentication scheme, Computer Security, vol. 21, no. 7, pp. 665-667, 2002.

[10] J. J. Shen, C. W. Lin, M. S. Hwang, Security enhancement for the timestamp-based password authentication using smart cards, Computer Security, vol. 22, no. 7, pp. 591-595, 2003.

[11] C. T. Li, M. S. Hwang, An efficient biometric based remote user authentication scheme using smart cards, Journal on Networking and Computer Applications, vol. 33, pp. 1-5, 2010.

[12] C. H. Lin, Y. Y. Lai, A flexible biometric remote user authentication scheme, Computer Standards Interf., vol. 27, no. 1, pp.19-23, 2004.

[13] A. K. Das, Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards, IET Information Security, vol. 5, no. 3, pp. 541-552, 2011.

[14] M.L. Das, A. saxena, V.P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE transactions on Consumer Electronics, Vol. 50,no. 2,pp. 629-631,2004.

[15] I. Liao, C.C Lee, M.S Hwang, Security enhancement for a dynamic ID-based remote user authentication scheme, Proceeding of the international conference on next generation web services practices,NWeSP'05, Seoul, Korea, pp. 437-440,2005.

[16] E.J. Yoon, K.Y. Yoo, Improving the dynamic ID-based remote mutual authentication scheme, Proc. OTM Workshops, LNCS 4277,pp. 499-507,2006.

[17] Y.P Liou, J. Lin, S.S. Wang, New dynamic ID-based remote user authentication scheme using smart cards, Proceedings of 16th information security conference, Taiwan, pp. 198-205,2006.

[18] Y.Y. Wang, J. Y. kiu, F.X. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications Vol. 32,no. 4, pp. 583-585,2009.

[19] M. K. Khan, S.K. Kim, K. Alghathbar, Cryptyanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communication Vol. 34, pp. 305-309, 2011.

Supersymmetric D-brane solutions in Gödel Universe

Pratap K. Swain[a,b*], Kamal L. Panigrahi[b] Susanta Maity[c]

[a] *Department of PCB,*
National Institute of technology Arunachal Pradesh, Yupia- 791112, India

[b] *Department of Physics and Meteorology,*
Indian Institute of Technology Kharagpur, Kharagpur-721302, INDIA

[c] *Department of Mathematics,*
National Institute of technology Arunachal Pradesh, Yupia- 791112, India

Abstract

We present a class of supersymmetric Gödel solutions in string theory from the non-standard intersection of branes in supergravities. Such solutions are obtained by applying a T-duality on the known solutions in PP-wave spacetime. We further present classical solutions of supersymmetric D-brane in Gödel universes arising from the PP-wave in the near horizon geometry of stack of D5-branes and from the new isometries of H_6 PP-wave background. These branes are supported by multiple constant Neveu-Schwarz and Ramond-Ramond field strengths.

Keywords: D-brane, PP-wave, Gödel universe, Supersymmetry, AdS space

*e-mail:`pratap.physics@nitap.in, pratapphy200@gmail.com`

1 Introduction and summary

Gödel universe is a homogeneous rotating cosmological solution of Einstein's equations with pressureless matter and negative cosmological constant, which played an important role in the conceptual development of general theory relativity. In [1] an M-theory solution of Gödel universe type has been found out and it was shown to preserve 20 supersymmetries. Furthermore it generates Ramond-Ramond (RR) fluxes when compactified down to 10-dimensional type IIA string theory. They contain some unphysical features like the closed time like curves (CTC), but the problem was resolved geometrically in [2] in the context of spinning deformation of (D1-D5) system. Further in [3], it was argued that the principle of holography remedy this problem and protect the chronology in the Gödel universe background. It was further shown that they are related to PP-wave background by a T-duality transformation. In this connection in [4] a large class of solutions were found out in the context of string theory in PP-wave background and corresponding properties of such spacetime including that of supersymmetries has been analyzed in details both in 10 and 11 dimensions. These class of solutions were obtained by applying T and S-duality transformations in the relevant solutions in PP-wave background. The string theory spectrum has also been studied by invoking the idea of quantization of PP-wave in light cone gauge. Further it was also noticed that the supergravity solutions of D5-branes in a type IIB PP-wave background[5] (coming from $AdS_3 \times S^3$ geometries) after a T-duality transformation can give new localized D4-brane solutions in the Gödel universe. They were also obtained by looking at the relevant boundary conditions in the open string constructions in PP-wave[6] and then applying T-dualities. This generates the mixed boundary conditions. Also in [7], using the duality described in [3], the string quantization has been studied in the ten dimensional description of these solutions and yet another mechanism has been proposed to resolve the CTCs within string theory. In this paper we would like to obtain new supersymmetric Gödel backgrounds by applying T-dualities in a class of PP-wave background which was derived from the Penrose limit on the non-standard intersection of D-branes in supergravities. Indeed in [8] a large class of PP-wave backgrounds were obtained from the non-standard brane intersections whose near horizon geometry was essentially Anti-de Siter (AdS). The resulting PP-waves are shown to be supported by multiple constant RR and NS-NS field strengths and they are interesting in their own right. These solutions are different from the known near horizon and PP-wave limit of the usual intersecting (like D1-D5) branes in supergravities. The main difference stems from the fact that in this case the Harmonic functions of branes depend on the relative transverse space. We have found out the new Gödel universe backgrounds by applying T-dualities on these class of PP-wave solutions. We take two examples, the (D1/D5/D5) system and the D3/D5/D5/ND5/NS5 intersecting brane system and have obtained new Gödel universe backgrounds. These solutions are different from the known solutions as they contain multiple RR and NS-NS fields, but keeps the "Gödel structure" is still intact.

Next, we find out some new supergravity solutions of D-branes in type IIA string theory from the known solutions of D-branes in PP-wave backgrounds[1]. First we have taken the example of D5-branes in the near horizon and PP-wave backgorund of a stack of D5-branes in type IIB string theory. This solution was found in [11] and was shown to be 1/4 supersymmetric. We apply T-duality and present a D4-brane solution in Gödel universe (the so-called $n = 1$ Gödel model) and examine the fate of unbroken supersymmetry by solving the gravitino and dilatino variations explicitly. Further we have uplifted this solution to M5-brane in M-theory. Our next example is a D2-brane in Gödel universe which is obtained from a D3-brane in PP-wave in the presence of both RR and NS-NS 3 form field strengths found in [10]. The rest of the paper is organized as follows. In section-2, we find out new supersymmetric Gödel solutions from intersecting branes whose near horizon geometry are of AdS type. In section-3, we find out new supergravity solutions for D-branes in Gödel universes from the corresponding branes in PP-wave backgrounds. Section-4 is devoted to the analysis of unbroken spacetime supersymmetry. Finally in section-5, we conclude with some remarks.

2 Gödel Universes from intersecting branes

In this section we will find out new Gödel models from the PP-wave background of non-standard brane intersections in supergravities. The AdS structure in the near horizon geometry of such intersections arises from the fact the Harmonic function for each participating brane depends on the relative transverse space rather than the overall transverse space. The first example we consider is the intersecting (D1/D5/D5)-brane system that couple to three form R-R field strengths in D=10. The relevant metric and other fields are given by [17]

$$\begin{aligned}
ds^2_{10} &= G^{-3/4}(F\tilde{F})^{-1/4}\left(-dt^2 + dx^2 + GFdy_i^2 + G\tilde{F}d\tilde{y}_i^2\right)\\
F_{(3)} &= e^{\phi} * (\tilde{F}dt \wedge dx \wedge d^4\tilde{y} \wedge dF^{-1}) + e^{\phi} * (Fdt \wedge dx \wedge d^4y \wedge d\tilde{F}^{-1})\\
&+ dt \wedge dx \wedge dG^{-1}\ , \quad e^{2\phi} = \frac{F\tilde{F}}{G}\ , \quad G = F\tilde{F}\ ,
\end{aligned} \tag{2.1}$$

where y_i and $\tilde{y}_i$ are the coordinates in the relative transverse space of the stack of D5-branes, $F = 1 + \frac{Q}{y^2}$, $\tilde{F} = 1 + \frac{Q}{\tilde{y}^2}$ are the harmonic functions of the branes. This particular solution has the property that the dilaton vanishes. The near horizon geometry of such a solution is $AdS_3 \times S^3 \times S^3 \times S^1$. The PP-wave geometry was obtained in [8], after taking a suitable Penrose limit on (2.1) and it is given by

$$ds^2_{10} = -2dx^+dx^- + H(dx^+)^2 + \sum_{i=1}^{8} dx_i^2\ , \quad F_3^{(RR)} = dx^+ \wedge \Phi_{(2)}\ ,$$

[1] D-brane supergravity solutions in NS-NS and R-R PP-waves have been discussed in, for example in [5][9][10][11][12] [13][14][15] [16]

$$
\begin{aligned}
H &= -\mu^2(x_1^2+x_2^2) - \frac{\mu^2}{2}\cos^2\alpha(x_3^2+x_4^2) - \frac{\mu^2}{2}\sin^2\alpha(x_5^2+x_6^2)\ , \\
\Phi_{(2)} &= 2\mu dx_1\wedge dx_2 + \sqrt{2}\mu\cos\alpha\ dx_3\wedge dx_4 - \sqrt{2}\mu\sin\alpha\ dx_5\wedge dx_6\ , \qquad (2.2)
\end{aligned}
$$

where α is the angle of rotation between the coordinates of two spheres in the transverse space of branes. We wish to find out the Gödel spacetime of this geometry. We shall follow the same procudure of getting a Gödel from PP-wave by applying a T-duality as described in [4]. The first step is to do the following coordinate transformation

$$
x^+ = x^0 + x^9,\ x^- = \frac{x^0 - x^9}{2},\ x^{2k-1} + ix^{2k} \to (x^{2k-1} + ix^{2k})e^{-i\mu_k x^+},\ k = 1, 2, 3. \quad (2.3)
$$

With the above transformation, the new metric looks like

$$
ds^2 = -(dx^0)^2 + (dx^9)^2 + \sum_{i=1}^{8} dx_i^2 - 2\sum_{i,j=1}^{6} J_{ij}x_i dx_j(dx^0 + dx^9)\ , \qquad (2.4)
$$

where

$$
J_{12} = \mu = -J_{21}\ ,\ J_{34} = \frac{\mu}{\sqrt{2}}\cos\alpha = -J_{43}\ ,\ J_{56} = \frac{\mu}{\sqrt{2}}\sin\alpha = -J_{65}\ . \qquad (2.5)
$$

The next step is to apply a T-duality along the x^9 direction [2]. The new metric and fields after the T-duality become

$$
\begin{aligned}
ds^2 &= -(dx^0 + \sum_{i,j=1}^{6} J_{ij}x_i dx_j)^2 + (dx^9)^2 + \sum_{i=1}^{9} dx_i^2\ , H_{129} = -F_{0129} = F_{12} = -2\mu\ , \\
H_{349} &= -F_{0349} = F_{34} = -\sqrt{2}\mu\cos\alpha,\quad F_{0569} = H_{569} = -F_{56} = -\sqrt{2}\mu\sin\alpha. \qquad (2.6)
\end{aligned}
$$

This background is different from the known examples of [4]. It is also important to note that this background preserves 1/2 supersymmetry only for $\alpha = \pi/4$ which is expected from [8]. Our next example is a non-standard intersection of D3/D5/D5/NS5/NS5 branes. This near horizon geometry was found out to be $AdS_3 \times S^2 \times S^2 \times T^3$. The Penrose limit was taken and the resulting pp-wave background has been written in [8]. We wish to write it once for our future reference

$$
\begin{aligned}
ds^2 &= -2dx^+dx^- - \mu^2\left(x_2^2 + x_2^2 + 2\cos^2\alpha x_3^2 + 2\sin^2\alpha x_4^2\right)(dx^+)^2 + dx_i^2\ , \\
F_{+1268} &= 2\mu\ ,\quad F_{+36} = H_{+38} = \sqrt{2}\mu\cos\alpha\ ,\quad F_{+48} = H_{+46} = -\sqrt{2}\mu\sin\alpha\ . \quad (2.7)
\end{aligned}
$$

For our purpose we will set $\alpha = \pi/4$. With this choice, the metric and other fields can be read off as

$$
\begin{aligned}
ds^2 &= -2dx^+dx^- - \mu^2\sum_{i=1}^{4} x_i^2(dx^+)^2 + \sum_{i=1}^{8} dx_i{}^2\ , \\
F_{+1268} &= 2\mu\ ,\quad F_{+36} = H_{+38} = \mu\ ,\quad F_{+48} = H_{+46} = -\mu\ . \qquad (2.8)
\end{aligned}
$$

[2] The T-duality transformation can be found out for example in [18]

After applying T-duality along x^9 direction as described earlier, we end of with the following form of the metric and other resultant field strengths as

$$\begin{aligned}
ds^2 &= -(dx^0 + \sum_{i,j=1}^{4} J_{ij}x_i dx_j)^2 + (dx^9)^2 + \sum_{i=1}^{8} dx_i^2 \ , \quad H_{129} = H_{349} = -2\mu, \\
F_{0369} &= \mu = -F_{0489} \ , \quad F_{1268} = F_{3457} = 2\mu \ , \quad F_{36} = -\mu = -F_{48} \ , \\
H_{038} &= \mu = H_{938} \ , \quad H_{046} = -\mu = H_{946} \qquad (2.9)
\end{aligned}$$

3 D-brane solution in Gödel Universes

In this section, we would like to write down the D4-brane solutions in the Gödel universe of $n = 2$ type presented in [4], which will be used in the next section to study the supersymmetry. The metric, dilaton and various field strengths of a stack of D4-branes is given by [4]

$$\begin{aligned}
ds^2 &= f_4^{-1/2}\left(-(dt + \mu\sum_{i=1}^{4} J_{ij}x^i dx^j)^2 + \sum_{i=1}^{4}(dx^i)^2\right) + f_4^{1/2}\sum_{m=5}^{9}(dx^m)^2 \\
e^{2\phi} &= f_4^{-1/2} \ , \quad F_{12} = F_{34} = -2\mu \ , \quad H_{129} = H_{349} = -2\mu \ , \quad F_{0129} = F_{0349} = 2\mu \ , \\
F_{mnpq} &= \epsilon_{mnpqr}\partial_r f_4 \ , \quad f_4 = 1 + \frac{Ng_s l_s^3}{r^3} \ , \quad r^2 = \sum_{m=5}^{9}(x^m)^2, \qquad (3.1)
\end{aligned}$$

where $J_{12} = -J_{21} = J_{34} = -J_{43} = 1$ and f_4 is the harmonic function of the D4-brane in the transverse five-space. One can observe that the presence of various field strengths symmetrically along the x^1, x^2 and correspondingly along the x^3, x^4 directions. We will see that this structure plays a crucial role in the supersymmetry analysis of the D4-brane solution. Now we would like to present further examples of D-brane solution in the Gödel universe models. Our first example is a D4-brane in the so-called $n = 1$ Gödel universe model. This is obtained by applying T-duality along isometry directions of the D5-brane in a PP-wave background that arises from the near horizon and Penrose limit of a stack of coincident D5-branes and is dual to the PP-wave background of Nappi-Witten model. The supergravity solution of D-branes were presented in [11]. In particular the 1/4 supersymmetric D5-brane is written as [11]

$$\begin{aligned}
ds^2 &= f_5^{-1/2}\left(-2dx^+dx^- - \mu^2\sum_{i=1}^{2} x_i^2(dx^+)^2 + \sum_{a=1}^{4}(dx^a)^2\right) + f_5^{1/2}\sum_{m=5}^{8}(dx^m)^2, \\
e^{2\phi} &= f_5^{-1}, \quad F_{+12} = 2\mu, \quad F_{mnp} = \epsilon_{mnpq}\partial_q f_5, \quad f_5 = 1 + \frac{Ng_s l_2^2}{r^2}, \ \ r = \sqrt{\sum_{m=5}^{8}(x^m)^2} \ .
\end{aligned}$$
$$(3.2)$$

The spacetime supersymmetry was analyzed by solving the dilatino and gravitino variations explicitly and it was found out that in addition to the flat space D5-brane supersymmetry condition if a ‘necessary’ condition $\Gamma^{\hat{+}}\epsilon = 0$ acts on the killing spinors, then all variations are satisfied giving a solution for the spinors which preserves eight supercharges. Applying a T-duality along x^9 as described in the last section, we get the following form of the metric, field strengths and dilaton for the ‘localized’ D4-brane in Gödel model.

$$\begin{aligned}
ds^2 &= f_4^{-1/2}\left(-(dt+\mu\sum_{i=1}^{2} J_{ij}x^i dx^j)^2 + \sum_{a=1}^{4}(dx^a)^2\right) + f_4^{1/2}\sum_{m=5}^{9}(dx^m)^2 \\
e^{2\phi} &= f_4^{-1/2}\ , \quad F_{12} = -2\mu\ , \quad H_{129} = -2\mu\ , \quad F_{0129} = 2\mu\ , \quad F_{mnpq} = \epsilon_{mnpqr}\partial_r f_4\ , \\
J_{12} &= 1 = -J_{21}\ , \quad f_4 = 1 + \frac{Ng_s l_s^3}{r^3}\ , \quad r^2 = \sum_{m=5}^{9}(x^m)^2.
\end{aligned} \tag{3.3}$$

We have checked that the solution presented above solves all type-IIA field equations. Next we would like to get a M5-brane solution starting from the D4-brane solution presented above in the Gödel model. Using the well known relation between the 10d and 11d metric:

$$ds_{11}^2 = e^{-\frac{2\Phi}{3}}ds_{10}^2 + e^{\frac{4\Phi}{3}}(dx_{11} + A_\mu dx^\mu)^2, \tag{3.4}$$

where ds_{11}^2 and ds_{10}^2 represent the metric in eleven and ten dimensions respectively, and A_μ is the one-form field (which is zero in the present case). One can easily see that the M5-brane solution is given by

$$\begin{aligned}
ds^2 &= f^{-1/3}\left(-2dx^+dx^- - \mu^2\sum_{i=1}^{2}(x^i)^2(dx^+)^2 + \sum_{a=1}^{4}(dx^a)^2\right) + f^{2/3}\sum_{m=5}^{9}(dx^m)^2\ , \\
F_{+129} &= 2\mu\ , \quad F_{mnpq} = \epsilon_{mnpqr}\partial_r f\ , f = 1 + \frac{Nl_p^3}{r^3},
\end{aligned} \tag{3.5}$$

with l_p being the eleven dimensional Plank length. In writing down the above solution in the x^+, x^--coordinates, we have made the following change of variables

$$x^1 + ix^2 \to (x^1 + ix^2)e^{-2\mu x^+}\ . \tag{3.6}$$

The solution can directly be obtained from the PP-wave solution by uplifting it to eleven dimensions. Note that in absence of any D-brane charges, if we apply T dualities along x^3 and x^4 directions, we get the follwing form of metric and RR fields

$$\begin{aligned}
ds^2 &= -2dx^+dx^- - \mu^2\sum_{i=1}^{2}(x^i)^2(dx^+)^2 + \sum_{m=1}^{8}(dx^m)^2\ , \\
F_{+1234} &= F_{+5678} = 2\mu.
\end{aligned} \tag{3.7}$$

Once again by applying a T-duality along the x^9 direction as before we get the following Godel metric and other field strengths

$$\begin{aligned} ds^2 &= -\left[dt + \mu(x^1 dx^2 - x^2 dx^1)\right]^2 + \sum_{m=1}^{9} (dx^m)^2 \\ F_{1234} &= F_{5678} = 2\mu, \quad H_{129} = 2\mu \ , \end{aligned} \tag{3.8}$$

Next we would like to find a D2-brane solution in a Gödel model. The D2-brane can be obtained by applying a T-duality along a localized D3-brane solution described in [10]. Note that this D3-brane solution was obtained by applying succssive T-dualities along the new isometry directions of the localized D5-brane solution of [10] by following [19]. In stead of going into the detials of construction we present here the final form of D3-brane solution in the presence of various R-R and NS-NS fluxes as

$$\begin{aligned} ds^2 &= f_3^{-1/2}\left(-2dx^+dx^- - 4\mu^2[x_1^2 + x_2^4](dx^+)^2 + dx_1^2 + dx_2^2\right) + f_3^{1/2}\left(dr^2 + r^2 d\Omega_5^2\right) \ , \\ F_{+31} &= F_{+42} = 2\mu \ , \quad H_{+41} = H_{+32} = 4\mu \ , \quad F_{mnpqr} = \epsilon_{mnpqrs}\partial_s f_3 \ , \quad f_3 = 1 + \frac{N g_s l_s^4}{r^4} \ , \end{aligned} \tag{3.9}$$

where f_3 is harmonic function in the transverse six space. By applying T-duality along x^9-direction as before, we get the following metric and other field strengths

$$\begin{aligned} ds^2 &= f_2^{-1/2}\left[-\left(dx^0 + 2\mu \sum_{i,j=1}^{2} J_{ij} x^i dx^j\right)^2 + \sum_{i=1}^{2} (dx^i)^2\right] + f_2^{1/2} \sum_{m=3}^{9} (dx^m)^2 \ , \\ e^{2\phi} &= f_2^{1/2} \ , \quad A_{012} = f_2^{-1} \ , \quad F_{0329} = F_{0429} = 2\mu \ , F_{31} = F_{42} = -2\mu \ , \\ H_{041} &= H_{941} = 4\mu = -H_{129} \ , H_{032} = H_{932} = 4\mu \ , f_2 = 1 + \frac{N g_s l^5}{r^5} \ , r^2 = \sum_{m=3}^{9} (x^m)^2 \ . \end{aligned} \tag{3.10}$$

Once again we have checked that the localized D2-brane solution above solves all type-IIA field equations of motion. Other D-branes and their bound states can be found out by applying T-dualities along various isometries of the solution presented here.

4 Spacetime Supersymmetry Analysis

In this section, we will analyze the the fate of the unbroken spacetime supersymmetry of the D-brane solutions presented above by solving the dilatino and gravitino variations explicitly. The supersymmetry variation of the dilatino and gravitino fields in type IIA supergravity in string frame is given by [20, 21].

$$\delta\lambda = \frac{1}{2}(\Gamma^{\mu}\partial_{\mu}\Phi - \frac{1}{12}\Gamma^{\mu\nu\rho}H_{\mu\nu\rho})\epsilon + \frac{1}{8}e^{\Phi}(5F^{(0)} - \frac{3}{2!}\Gamma^{\mu\nu}F^{(2)}_{\mu\nu} + \frac{1}{4!}\Gamma^{\mu\nu\rho\sigma}F_{\mu\nu\rho\sigma})\epsilon, \quad (4.1)$$

$$\delta\Psi_{\mu} = \Big[\partial_{\mu} + \frac{1}{8}(w_{\mu\hat{a}\hat{b}} - H_{\mu\hat{a}\hat{b}})\Gamma^{\hat{a}\hat{b}}\Big]\epsilon + \frac{1}{8}e^{\Phi}\Big[F^{(0)} - \frac{1}{2!}\Gamma^{\mu\nu}F^{(2)}_{\mu\nu} + \frac{1}{4!}\Gamma^{\mu\nu\rho\sigma}F^{(4)}_{\mu\nu\rho\sigma}\Big]\Gamma_{\mu}\epsilon, \quad (4.2)$$

where we have used μ, ν, ρ to describe the ten dimensional space-time indices, and the hated ones are the corresponding tangent space indices. Solving the Dilatino variation (4.1) for the D4-brane solution (3.1), presented in [4] we get the following condition on the spinors to be satisfied

$$f^{-5/4}f_{,m}\left(\Gamma^{\hat{m}} + \frac{1}{4!}\epsilon_{\hat{m}\hat{n}\hat{p}\hat{q}\hat{r}}\Gamma^{\hat{n}\hat{p}\hat{q}\hat{r}}\right)\epsilon - 2\mu f^{1/4}\left(\Gamma^{\hat{1}\hat{2}} + \Gamma^{\hat{3}\hat{4}}\right)\Gamma^{\hat{9}}\epsilon$$
$$-\mu f^{1/4}\left(\Gamma^{\hat{1}\hat{2}} + \Gamma^{\hat{3}\hat{4}}\right)\epsilon - \mu f^{-1/4}\Gamma^{\hat{0}}\left(\Gamma^{\hat{1}\hat{2}} + \Gamma^{\hat{3}\hat{4}}\right)\Gamma^{\hat{9}}\epsilon = 0 \quad (4.3)$$

Now solving the gravitino variations we get the following

$$\partial_0\epsilon = 0, \quad \partial_a\epsilon = 0, \quad (a = 5, \cdots, 9), \quad \partial_i\epsilon + \frac{\mu}{2}J_{ij}\Gamma^{\hat{j}\hat{9}}\epsilon = 0, \quad (i = 1, \cdots, 4)\ . \quad (4.4)$$

Note that while writing down the above variations (4.4) we have made use of the D4-brane supersymmetry condition in flat space

$$\left(\Gamma^{\hat{m}} + \frac{1}{4!}\epsilon_{\hat{m}\hat{n}\hat{p}\hat{q}\hat{r}}\Gamma^{\hat{n}\hat{p}\hat{q}\hat{r}}\right)\epsilon = 0\ , \quad (4.5)$$

and

$$\left(1 - \Gamma^{\hat{1}\hat{2}\hat{3}\hat{4}}\right)\epsilon = 0\ . \quad (4.6)$$

By using the above two conditions all the dilatino and gravitino variations are satisfied leaving only 1/4 of the total spacetime supersymmetry unbroken and is solved by a constant spinor. Hence the D4-brane solution in the $n = 2$ Gödel universe model preserves 1/4 unbroken supersymmetry. Let us now look at the fate of the unbroken supersymmetry for the D4-brane in $n = 1$ Gödel model. First, solving the dilatino variation (4.1), for the D4-brane solution presented in (3.3) we get

$$f^{-5/4}f_{,m}\left(\Gamma^{\hat{m}} + \frac{1}{4!}\epsilon_{mnpqr}\Gamma^{\hat{m}\hat{n}\hat{p}\hat{q}}\right)\epsilon - 2\mu f^{1/4}\Gamma^{\hat{1}\hat{2}}\left(\Gamma^{\hat{9}} + \frac{1}{2}(1 + \Gamma^{\hat{0}\hat{9}})\right)\epsilon = 0 \quad (4.7)$$

The vanishing of the dilatino variation demands that the following two conditions to be imposed

$$\left(\Gamma^{\hat{m}} + \frac{1}{4!}\epsilon_{\hat{m}\hat{n}\hat{p}\hat{q}\hat{r}}\Gamma^{\hat{n}\hat{p}\hat{q}\hat{r}}\right)\epsilon = 0 \quad (4.8)$$

and

$$\Gamma^{\hat{0}}\epsilon = \Gamma^{\hat{9}}\epsilon = -\epsilon \tag{4.9}$$

The first one is the usual D4-brane supersymmetry condition even in flat space, where as the second condition is a projection condition on the spinors. By using (4.8) and (4.9), all the gravitino variations are satisfied leaving the following equations to have a constant spinor as a solution.

$$\partial_0\epsilon = 0, \quad \partial_\alpha\epsilon = 0, \quad (\alpha = 3, \cdots, 9), \quad \partial_i\epsilon + \frac{\mu}{2}J_{ij}\Gamma^{\hat{j}\hat{9}}\epsilon = 0, \quad (i = 1, 2)\ . \tag{4.10}$$

Hence the D4-brane in the $n = 1$ Gödel model preserves 1/4 of the total spacetime supersymmetry. Similarly one can analyze the spacetime supersymmetry of the D2-brane presented in (3.10) by solving the dilatino and gravitino variations.

5 Conclusions

We have presented in this paper a class of Gödel universe backgrounds from non-standard intersecting branes in supergravity. These supersymmetric backgrounds are different from the already known ones due to the presence of various constant NS-NS and R-R field strengths. We have further presented the supergravity solutions of D-branes in type IIA theory in some Gödel universes which are obtained from the corresponding PP-wave backgrounds. The supersymmetry properties of these branes are analyzed in detail by solving the dilatino and gravitino variations explicitly. The worldsheet construction of these branes can be carried out by following [6][4] and looking at the mixed boundary conditions properly. It will be interesting to completely classify all the supersymmetric branes in Gödel universes of various kind.

References

[1] J. P. Gauntlett, J. B. Gutowski, C. M. Hull, S. Pakis and H. S. Reall, “All supersymmetric solutions of minimal supergravity in five- dimensions,” Class. Quant. Grav. **20**, 4587 (2003)

[2] C. A. R. Herdeiro, “Spinning deformations of the D1 - D5 system and a geometric resolution of closed timelike curves,” Nucl. Phys. B **665**, 189 (2003)

[3] E. K. Boyda, S. Ganguli, P. Horava and U. Varadarajan, “Holographic protection of chronology in universes of the Gödel type,” Phys. Rev. D **67**, 106003 (2003)

[4] T. Harmark and T. Takayanagi, “Supersymmetric Gödel universes in string theory,” Nucl. Phys. B **662**, 3 (2003)

[5] A. Kumar, R. R. Nayak, S. Siwach and , "D-brane solutions in p p wave background," Phys. Lett. B **541**, 183 (2002)

[6] K. Skenderis and M. Taylor, "Open strings in the plane wave background. 1. Qquantization and symmetries," Nucl. Phys. B **665**, 3 (2003)

[7] D. Brace, C. A. R. Herdeiro and S. Hirano, "Classical and quantum strings in compactified pp-waves and Godel type universes," Phys. Rev. D **69**, 066010 (2004)

[8] H. Lu and J. F. Vazquez-Poritz, "Penrose limits of nonstandard brane intersections," Class. Quant. Grav. **19**, 4059 (2002)

[9] P. Bain, P. Meessen and M. Zamaklar, "Supergravity solutions for D-branes in Hpp wave backgrounds," Class. Quant. Grav. **20**, 913 (2003)

[10] M. Alishahiha and A. Kumar, "D-brane solutions from new isometries of pp waves," Phys. Lett. B **542**, 130 (2002)

[11] A. Biswas, A. Kumar and K. L. Panigrahi, "p-p' branes in PP wave background," Phys. Rev. D **66**, 126002 (2002)

[12] R. R. Nayak, "D-branes at angle in pp wave background," Phys. Rev. D **67**, 086006 (2003)

[13] K. L. Panigrahi and S. Siwach, "D-branes in pp wave space-time with nonconstant NS NS flux," Phys. Lett. B **561**, 284 (2003)

[14] N. Ohta, K. L. Panigrahi and S. Siwach, "Intersecting branes in pp wave spacetime," Nucl. Phys. B **674**, 306 (2003) [Erratum-ibid. B **748**, 333 (2006)]

[15] S. F. Hassan, R. R. Nayak and K. L. Panigrahi, "D branes in the NS5 near horizon pp wave background," hep-th/0312224.

[16] P. K. Swain, "D3-branes at angle in a linear dilaton pp-wave background," Mod. Phys. Lett. A **25**, 3219 (2010)

[17] P. M. Cowdall and P. K. Townsend, "Gauged supergravity vacua from intersecting branes," Phys. Lett. B **429**, 281 (1998) [Erratum-ibid. B **434**, 458 (1998)]

[18] J. C. Breckenridge, G. Michaud and R. C. Myers, "More D-brane bound states," Phys. Rev. D **55**, 6438 (1997)

[19] J. Michelson, "Twisted toroidal compactification of pp waves," Phys. Rev. D **66**, 066002 (2002)

[20] J. H. Schwarz, "Covariant Field Equations of Chiral N=2 D=10 Supergravity," Nucl. Phys. B **226**, 269 (1983).

[21] S. F. Hassan, "T duality, space-time spinors and RR fields in curved backgrounds," Nucl. Phys. B **568**, 145 (2000)

Carbohydrate Based Chemosensor for Selective Detection of Hg^{2+} Ion

Ananta Kumar Atta
Department of Chemistry
National Institute of Technology, Arunachal Pradesh
Yupia, India
attaananta@gmail.com

Nabakumar Pramanik
Department of Chemistry
National Institute of Technology, Arunachal Pradesh
Yupia, India
pramaniknaba@gmail.com

Heavy metals like lead, cadmium, and mercury ions even in low concentrations are known to cause neurological, reproductive, cardiovascular, and developmental disorders. In this review, the fluorescent and colorimetric carbohydrate based sensors are classified accordingly and discussed their Hg^{2+} sensing ability.

Keywords—Carbohydrate, Triazole, Heavy metals, Sensor, Mercury (II) ion.

I. Introduction

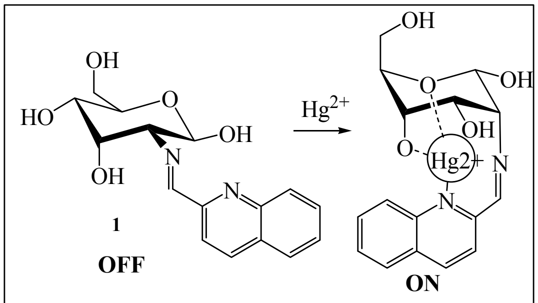
Among various heavy metal ions, Hg, Pb, and Cd are banded in electronic and electrical equipment by European Union's Restriction on Hazardous Substances Directive (RoHS) due to hazardous nature [1]. Heavy metal ions are of great concern, not only among the scientific community, but also chemists, environmentalists and biologists. People are very concern over the cruel risk of heavy metal pollution in environment, food, and products [2]. Heavy metals are individual metals that can affect human health extensively (Fig. 1).

Fig. 1: Effects of heavy metals in human health

Recently, Environmental Protection Agency (EPA) and World Health Organization (WHO) have strictly fixed the concentration of these metal ions in the drinking water [3]. In this review, we have particularly focused carbohydrate based sensors to detect Hg^{2+}, because of its high toxicity, strong damage to the central nervous system, and accumulation of mercury in the human and animals which can lead to serious debilitating illnesses [4]. Mercury is widespread in air, water, and soil by many sources like coal and gold mining, fossil fuel combustion, barometers, dental amalgams, and mercury vapor lamps etc. Although, many different chemical sensors have been discussed in various articles [5] to detect heavy metal ions but sugar based chemosensors for selective detection of mercury ions are rare [6]. Therefore on the basis of the aforesaid information, we have intended in carbohydrate modified sensor for Hg^{2+} ions detection. Overall we would like to provide a general over view of the design and applications of Hg^{2+}selective carbohydrate based chemosensors in this review.

II. Carbohydrate Based Mercury (II) Sensor

'In-built' chiralities in carbohydrates and the presence of hydroxyl groups and oxygen atoms are quite suitable for cations binding and high water soluble nature of carbohydrates. Carbohydrates can be chemically switched between different conformations after binding with metal ions. In this respect, water soluble and biologically benign carbohydrate based sensors would be used in *vitro* and in *vivo* applications. Thus, the design of carbohydrate based chemosensor is good strategy for detecting metal ions. On the basis of the above things, Bai *et al*., reported that the reaction of 2-quinolinecarboxaldehyde with D-glucosamine in methanol solution afforded a sugar-quinoline fluorescent chemosensor **1** (Scheme 1) [6a]. Sugar ring of the compound shows $^4C_1$ conformation but after co-ordination with Hg^{2+}, the conformation is changed ($^4C_1$). Chemosensor **1** can detect Hg^{2+} in natural water. Initially the compound does not show any fluorescence but after binding with mercury (II), the compound shows fluorescence. Uv-vis spectrum of carbohydrate based chemosensor in aqueous solution exhibits a broad band at about 310-320 nm and a quantum yield of 0.005, but after addition of excess Hg^{2+} ions to solution of **1** result in a 65-nm blueshift of the emission band (λem 415 nm) and~10-fold fluorescence enhancement (Fig. 2). The dramatic blue-shift is attributed to PCT from the hydroxyl group to the quinoline moiety, and the fluorescence enhancement to alleviation of PET. Glucosamine **1** shows maximum emission in the presence of~20 equiv. of Hg(II), forms a 1:1 complex with Hg(II). Wu *et al.* reported a fluorescent sensor **2** (Fig 3), with a furanoid-based sugar-aza-crown ether (SAC) and two



Scheme 1: Structural changes of sugar-quinoline chemosensor.

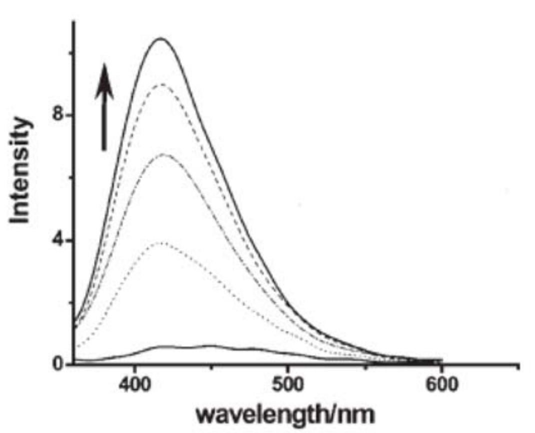


Fig. 2: Change of emission spectra of **1** upon addition of increasing concentrations of Hg^{2+}.

triazole moieties as the binding sites, and two anthracene moieties as the signalling units [6b]. The reported fluorescence sensor **2** exhibits highly selective and efficient fluorescence behaviour for Hg^{2+} ions in methanol. The fluorescence intensity of sensor **2** depends upon the polarity of the solvent. In polar solvent, the fluorescence intensity is more.

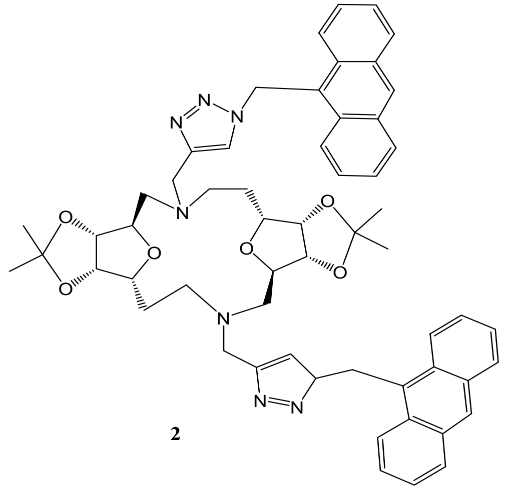


Fig. 3: Sugar-aza-crown ether based sensor

Fluorescent sensor **2** showed gradual decrease in fluorescence as the concentration of Hg^{2+} ion increased (Fig 4). The fluorescent sensor exhibits highly selective and efficient fluorescence behaviour for Hg^{2+} ions in methanol. Compound **2** showed fluorescence due to the presence of anthracene moiety, which is quenched by Co^{2+}, Ni^{2+}, Hg^{2+} and Cu^{2+} ions. Out of these ions, Hg^{2+} and Cu^{2+} ions are most effectively quenched the fluorescence intensity. The fluorescent quenching mechanisms of **2** with Hg^{2+}ion was explained by

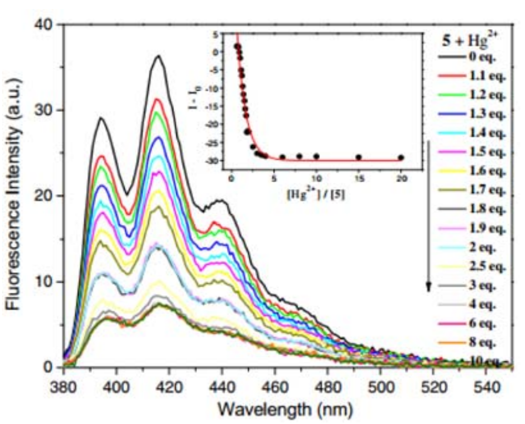
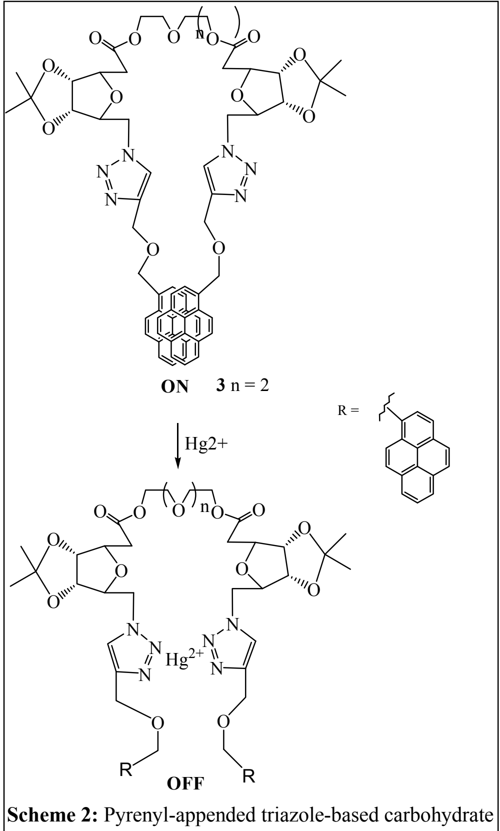


Fig. 4: Fluorescence spectra of **1** upon addition of increasing concentrations of Hg^{2+}.



Scheme 2: Pyrenyl-appended triazole-based carbohydrate for Hg^{2+}ions.

the reverse PET mechanism involving the anthracene group as an electron donor and the triazole group as an electron acceptor.

They also reported pyrenyl-appended triazole based carbohydrate **3** [6c] (Scheme 2) for selective detection of Hg^{2+}. The maximum absorption wavelength of pyrene in **3** showed a strong excimer emission at 478 nm but excimer fluorescences diminised dramatically upon addition of Hg^{2+}, probably because of the quenching induced by electron transfer (Fig. 5). Fluorescence titration of 3 (10 µM) in presence of different concentrations of Hg^{2+} ions in DCM/MeOH showed the gradual decrease of fluorescence intensity upon addition of increasing concentrations of Hg^{2+} ions. From the titration result, the detection limit for the Hg^{2+} ion was determined to be 10 µM. The detection limit is sufficiently low to detect the submillimolar concentration of Hg^{2+} ion found in many chemical and biological systems. Maximum fluorescence change was observed when compound **3** forms a 1:1 complex with Hg(II).

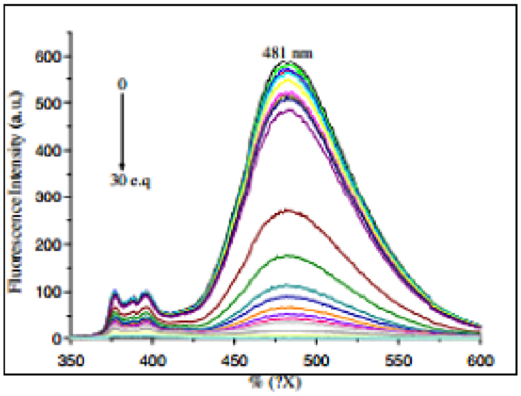
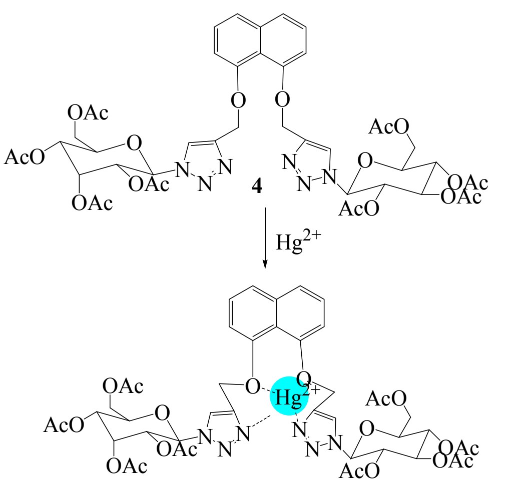


Fig. 5: Fluorescence spectra of **3** upon addition of increasing concentrations of Hg^{2+}.

In another study, Das *et al.*, observed that bis-sugar-riazole based gelator molecule **4** showed better affinities towards Hg^{2+} ion (Scheme 3) [6d]. Uv-visible spectra for gelator **4** with different metal ions showed that the binding ability of compound **4** with Hg^{2+} is significant (Fig. 6).



Scheme 3: Sugar based bis-triazole sensor for Hg^{2+} ions.

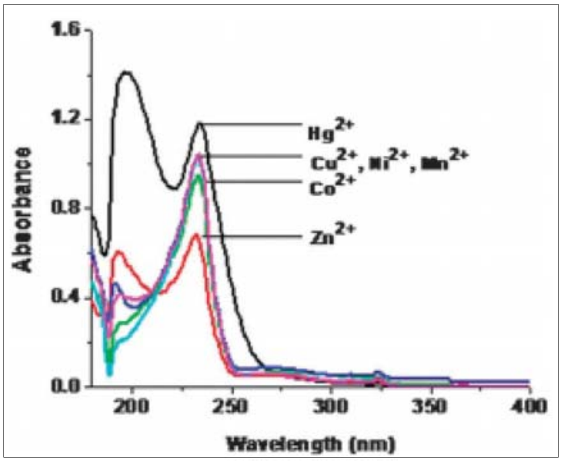


Fig. 6: Uv-visible spectra of compound **4** upon addition of various metal ions.

Conclusions

In this review, we covered the development of carbohydrate based chemosensor exciting fluorescent and colorimetric sensors for Hg^{2+} detection. We believe this research area will become more active due to the biological and environmental significance of heavy metals basically Hg^{2+} ions and further investigations are to be needed in this field in order to develop better sensing systems for the detection of heavy metal ions in real-world applications.

REFERENCES

[1] The European Parliament and the Council of the European Union, “Directive on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment”. **2002**/95/EC.

[2] (a) C. Orvig, M. J. Abrams, “Medicinal Inorganic Chemistry: Introduction,” *Chem. Rev.* **1999**, *99*, 2201. (b) C. Bargossi, M. C. Fiorini, M. Montalti, L. Prodi, N. Zaccheroni, “Recent developments in transition metal ion detection by luminescent chemosensors,” *Coord. Chem. Rev.* **2000**, *208*, 17. (c) L. Prodi, F. Bolletta, M. Montalti, N. Zaccheroni, “Luminescent chemosensors for transition metal ions,” *Coord. Chem. Rev.* **2000**, *205*, 59. (d) M. Benounis, N. Jaffrezic-Renault, H. Halouani, R. Lamartine, I. Dumazet-Bonnamour, “Detection of heavy metals by an optical fiber sensor with a sensitive cladding including a new chromogenic calix[4]arene molecule,” *Mater. Sci. Eng., C* **2006**, *26*, 364. (e) E. L. Que, D. W. Domaille, C. J. Chang, “Metals in Neurobiology: Probing Their Chemistry and Biology with Molecular Imaging,” *Chem. Rev.* **2008**, *108*, 1517. (f) R. McRae, P. Bagchi, S. Sumalekshmy, C. J. Fahrni, “In Situ Imaging of Metals in Cells and Tissues,” *Chem. Rev.* **2009**, *109*, 4780. (g) D. T. Quang, J. S. Kim, “Fluoro- and Chromogenic Chemodosimeters for Heavy Metal Ion Detection in Solution and Biospecimens,” *Chem. Rev.* **2010**, *110,* 6280. (h) H. N. Kim, W-X. Ren, J. S. *Kim*, J. Yoon, “Fluorescent and colorimetric sensors for detection of lead, cadmium, and mercury ions,” *Chem. Soc. Rev*. **2012**, *41*, 3210.

[3] (a) World Health Organization, Guidelines for drinking-water quality, 3rd ed., vol. 1, Geneva, **2004**, 188. (b) D. N. Mishra, ‘‘Adsorption of zirconyl salts and their acids on hydroxyapatite: Use of the Salts as Coupling Agents to dental polymer composites,’’*J. Dent. Res.,* **1985**, **64,** 1405-1408.

[4] (a) M. Harada, “Minamata disease: methylmercury poisoning in Japan caused by environmental pollution,” *Crit. Rev. Toxicol.* ***1995***, *25*, 1. (b)

I. Onyido, A. R. Norris, E. Buncel, "Biomolecule−Mercury Interactions: Modalities of DNA Base−Mercury Binding Mechanisms. Remediation Strategies," *Chem. Rev.* ***2004***, *104*, *5911.*

[5] (a) V. Iyengar, J. Wolttlez, "Trace Elements in Human ClinicalSpecimens:Evaluationof LiteratureData to Identify ReferenceValues," *Clin. Chem. (Washington, D. C.)*, **1988**, *34*, 474. (b) A. T. Townsend, K. A. Miller, S. Mc, S. Aldous, "The determination of copper, zinc, cadmium and lead in urine by high resolution ICP-MS" *J. Anal. At. Spectrom.*, **1998**, *13*, 1213. (c) D. T. Quang, J. S. Kim, "Fluoro- and Chromogenic Chemodosimeters for Heavy Metal Ion Detection in Solution and Biospecimens," *Chem. Rev.*, **2010**, *110*, 6280. (d) X. Chen, Y. Zhou, X. Peng, J. Yoon, "Fluorescent and colorimetric probes for detection of thiols," *Chem. Soc. Rev.*, **2010**, *39*, 2120. (e) J. F. Zhang, Y. Zhou, J. Yoon, J. S. Kim, "Recent progress in fluorescent and colorimetric chemosensors for detection of precious metal ions (silver, gold and platinum ions," *Chem. Soc. Rev.*, **2011**, *40*, 3416. (f) Y. Zhou, Z. Xu,; J. Yoon, "Fluorescent and colorimetric chemosensors for detection of nucleotides, FAD and NADH: highlighted research during 2004–2010," *Chem. Soc. Rev.*, **2011**, *40*, 2222.

[6] (a) S. Ou, Z. Lin, C. Duan, H. Zhang, Z. Bai, "A sugar-quinoline fluorescent chemosensor for selective detection of Hg^{2+} ion in natural water," *Chem. Commun.* **2006**, 4392. (b) Y-C. Hsieh, J-Ly. Chir, H-H. Wu, Po-S. Chang, A-T. Wu, "A sugar-aza-crown ether-based fluorescent sensor for Hg^{2+} and Cu^{2+}," *Carbohydr. Res.* **2009**, *344*, 2236. (c) K-H. Chen, C-Yi. Lu, H-J. Cheng, S-J. Chen, C-H. Hu, A-t. Wu, "A pyrenyl-appended triazole-based ribose as a fluorescent sensor for Hg^{2+} ion," *Carbohydr. Res.* **2010**, *345*, 2557. (d) A. Hemamalini, T. M. Das, "Design and synthesis of sugar-triazole low molecular weight gels as mercury ion sensor," *New J. Chem.* **2013**, *37*, 2419

Unsteady flow of thin liquid film over a porous stretching sheet in presence transverse magnetic field

S. Maity^{a} [1]& P. K. Swain^{b}

^{a} *Department of Mathematics,*
National Institute of Technology, Arunachal Pradesh,
Yupia, District Papumpare - 791 112, Arunachal Pradesh, India
^{b} *Department of PCB,*
National Institute of Technology, Arunachal Pradesh,
Yupia, District Papumpare - 791 112, Arunachal Pradesh, India

ABSTRACT

Unsteady flow of a thin liquid film over a porous stretching sheet has been studied in presence of transverse magnetic field under the assumption of uniform initial film thickness. The couple non-linear system of the governing partial differential equations are solved numerically by finite difference technique. The rate of film thinning decreases with the increase of the Darcy number and Hartmann number respectively. The thickness of the liquid film increases with increase of the suction parameter whereas the opposite phenomena is observed for the injection parameter.

Key Words: Thin liquid film, Porous sheet, transverse magnetic field, Suction/injection.

1. INTRODUCTION

The flow of a thin viscous liquid film from a stretching boundary is important in process industry such as the extrusion of sheet material in to the coolant environment. In a melt-spinning process, the extrudate from the die is generally drawn and simultaneously stretched into a filament or sheet, which is then solidified through rapid quenching or gradual cooling by direct contact with water or chilled metal rolls. Crane [1] first studied a steady two-dimensional boundary layer flow due to the stretching of a sheet. The work of Crane [1] was subsequently extended by many researchers either by considering the effects of rotation, heat and mass transfer, chemical reaction, MHD, non-Newtonian fluid or different possible combinations of these above effects(see [2] - [6]). Cheng and Minkowycz [7] have studied the flow of the viscous fluid about a vertical impermeable flat plate in a saturated porous medium. The boundary layer flow of viscous liquid over a porous stretching sheet are investigated by Abel and Veena [8], Elbasbeshy and Bazid [9], Ali and Mehmood [10]. Where as, the effects of suction or injection on the boundary layer flows due to a stretching of the wall has been analyzed by Erickson et al. [11], Gupta and Gupta [12], Chen and Char [13], Elbasbeshy and Bazid [9]. The unsteady boundary layer flow of finite liquid film due the stretching of a sheet was first considered by Wang [14]. In this study, he used a special type of similarity transformation which reduces the boundary layer equations to a non-linear ODE and then solved numerically. The work of Wang [14] further extended by [15]-[18] to the case of power-law fluid, heat transfer, effects of thermocapillarity, variable fluid properties, heat source or sink etc.

It is to be mentioned here that the study of unsteady flow due to the stretching of a sheet has not yet received adequate attention when the film and the fluid boundary

[1] Corresponding author
E-mail addresses: susantamaiti@gmail.com

layer thickness coincide. If the thickness of the liquid film either coincides or lies within the boundary layer thickness then one needs to consider the full set of Navier-Stokes equations to study such flow problem. Recently Dandapat and Maity [19] have studied the development of thin liquid film over an unsteady stretching sheet by considering the full set of Navier-Stokes equations with nonuniform film surface and able to show that the final film thickness neither depends on the type of initial distribution of the liquid nor the initial amount of liquid deposited over the stretching sheet.

To the best of our knowledge, the study of thin liquid film development over a porous stretching sheet by considering full Navier-Stokes equations in presence of transverse magnetic field has been not reported yet. In this article, we are interested to study the flow a thin liquid film over an unsteady porous stretching sheet in presence of transverse magnetic field, suction or injection by considering full set of momentum equations. We assumed that the initially deposited liquid film over the stretching sheet is planer and remain planer throughout entire process of stretching as well as film thinning.

2. Mathematical Formulation

We consider the unsteady flow of a thin liquid film of uniform thickness h_0 over a porous stretching sheet in presence of uniform transverse magnetic field B_0. The x-axis is chosen along the plane of the sheet and z-axis is taken normal to the plane. The surface $z = 0$ starts stretching impulsively from the rest with the velocity ax, a being constant with dimension of $[time]^{-1}$. The porous medium is assumed to be constant permeability $k^{'}(> 0)$ and the porosity $\phi(0 < \phi < 1)$, the effects of pores on the velocity field obey the Darcy's law $\nabla p = -\frac{\nu\phi}{k'}\mathbf{V}$ is given by Neild and Beijan [20], where $\mathbf{V} = (u, w)$, p and ν are the velocity vector, pressure and kinematic viscosity of the liquid respectively. The governing set of equations are

$$\nabla \cdot \mathbf{V} = 0, \tag{1}$$

$$\mathbf{V}_t+(\mathbf{V}\cdot\nabla)\mathbf{V} = -\nabla p/\rho+\nu\nabla^2\mathbf{V}-\frac{\nu\phi}{k'}\mathbf{V}-\frac{\sigma_0}{\rho}(\mathbf{V}\times B_0)\times B_0, \tag{2}$$

where ρ, σ_0, are the density and electric conductivity of the liquid respectively.

No-slip and no penetration conditions on the surface of stretching sheet in presence of suction and injection are given respectively by

$$u = ax, \quad w = -W_s, \tag{3}$$

The velocity W_s is taken to be positive or negative for the suction or injection at the porous stretching wall.

At the free surface $z = h(t)$,

$$p_a - p + 2\mu\frac{\partial w}{\partial z} = 0, \tag{4}$$

$$\frac{\partial u}{\partial z} + \frac{\partial w}{\partial x} = 0, \tag{5}$$

$$\frac{dh}{dt} = w, \tag{6}$$

where p_a and μ are the atmospheric pressure and dynamic viscosity of the liquid, respectively. Equations (4) and (5) denote respectively, the vanishing of the normal and shear stress at the free surface. Equation (6) represents the kinematic condition at the free surface.

The initial conditions at time $t = 0$ are

$$u = 0, w = 0, h(0) = h_0. \tag{7}$$

Now we introduce the following similarity variables (see [21])

$$u(x, z, t) = xF(z, t), w(x, z, t) = W(z, t), \tag{8}$$

$$p(x,z,t) = -\frac{x^2}{2}A(z,t) + B(z,t), \tag{9}$$

Substituting (8)-(9) into the system of equations (1) -(2) and equating the like order terms of x from both sides, we have

$$F + \frac{\partial W}{\partial z} = 0, \tag{10}$$

$$\frac{\partial F}{\partial t}+F^2+W\frac{\partial F}{\partial z} = \frac{A}{\rho}+\nu\frac{\partial^2 F}{\partial z^2}-\frac{\nu\phi}{k'}F-\frac{\sigma_0 B_0^2}{\rho}F, \tag{11}$$

$$\frac{\partial W}{\partial t} + W\frac{\partial W}{\partial z} = -\frac{1}{\rho}\frac{\partial B}{\partial z} + \nu\frac{\partial^2 W}{\partial z^2} - \frac{\nu\phi}{k'}W, \tag{12}$$

$$\frac{\partial A}{\partial z} = 0, \tag{13}$$

Under the above similarity transformation (8)-(9) the boundary conditions are reduced as:

at $z = 0$,

$$F = a, \quad W = -W_s, \tag{14}$$

at $z = h(t)$,

$$\left.\begin{aligned} A &= 0, \\ B &= 2\mu\frac{\partial W}{\partial z}, \end{aligned}\right\} \tag{15}$$

$$\frac{\partial F}{\partial z} = 0, \tag{16}$$

$$\frac{dh}{dt} = W. \tag{17}$$

The transformed initial conditions are:

$$F = 0, W = 0, h(0) = h_0. \tag{18}$$

Equation (13) is solved by using the boundary condition (15), we get $A(z,t) = 0$. $B(z,t)$ can be found by integrating equation (12) with respect to z, from z to $z = h(t)$. Finally one may evaluate the pressure from the equation (9). The following dimensionless quantities

$$\hat{z} = \frac{z}{h_0}, \hat{h} = \frac{h}{h_0}, \hat{t} = ta, \hat{F} = \frac{Fh_0}{U_0}, \hat{W} = \frac{W}{U_0}, \tag{19}$$

may be introduced into the system of equations, boundary and initial conditions, here $U_0 = ah_0$ is the characteristic velocity.

The set of dimensionless governing equations after dropping the hat over the dependent variables, we get

$$F + W_z = 0, \tag{20}$$

$$Re\left[F_t + F^2 + WF_z\right] = F_{zz} - DaF - M^2F, \tag{21}$$

where $Re = \frac{U_0 h_0}{\nu}$, $Da = \frac{\phi h_0^2}{k'}$, $M = B_0 h_0\sqrt{\frac{\sigma_0}{\rho\nu}}$ are the Reynolds number, Darcy number and Hartmann number, respectively.

The dimensionless boundary conditions are,

at $z = 0$;

$$F = 1, W = -V, \tag{22}$$

where $V = \frac{W_s}{U_0}$ is the dimensionless suction/ injection velocity ($V > 0$ and $V < 0$ denotes the suction and injection respectively),

at $z = h(t)$;

$$F_z = 0, \tag{23}$$

$$h_t = W. \tag{24}$$

The initial conditions ($t = 0$) are

$$F = W = 0, h = 1. \tag{25}$$

3. Numerical solution

The coupled nonlinear system of equations (20) - (21) with the corresponding boundary and initial conditions are solved by using the finite difference method. Here, it is important to mention that the film thickness is continuously decreasing with time, so the conventional finite difference method can not be used here. Due to this reason, the time dependent physical domain $[0, h(t)]$ is transformed into a fixed computational domain $[0, 1]$, such that the film thickness will always remain fixed in the computational domain. Further, care has been taken through a fine grid distribution for the large velocity gradients that may be present near the stretching surface. It should be pointed out here that the same transformation will be useful for fine as well as uniform grid distribution. Following Robert [22], we choose the transformation as:

$$\xi(t) = 1 - a_1 ln\left(\frac{a_2 h(t) - z}{b_2 h(t) + z}\right), 1 < c < \infty. \quad (26)$$

Here $a_1 = [ln(a_2/b_2)]^{-1}$, $a_2 = c+1$ and $b_2 = c-1$. The parameter c controls the grid spacing in the physical domain. Small values of c cluster grid points at the surface where large values make the grid spacing uniform throughout the liquid film. The Crank-Nicholson scheme is used to solve the transformed nonlinear system of equations (20) - (21) after approximating the nonlinear terms by the Newton's linearization technique [23]. Computation is carried out in each time level on the following linear tridiagonal system of algebraic equations

$$P_1 F_{j-1}^{n+1} + Q_1 F_j^{n+1} + R_1 F_{j+1}^{n+1} = (S_1)_j^n, \quad (27)$$

where

$$P_1 = \frac{B-A}{4\delta\xi} - \frac{C}{2\delta\xi^2}, \quad Q_1 = \frac{1}{\delta t} + \frac{C}{\delta\xi^2} + 2F_j^n,$$

$$R_1 = \frac{A-B}{4\delta\xi} - \frac{C}{2\delta\xi^2},$$

$$(S_1)_j^n = F_j^n\left[\frac{1}{\delta t} + F_j^n - \frac{C}{\delta\xi^2} - \frac{Da}{Re}\right.$$

$$\left.-\frac{M^2}{Re}\right] + F_{j-1}^n\left[\frac{A-B}{4\delta\xi} + \frac{C}{2\delta\xi^2}\right] +$$

$$F_{j+1}^n\left[\frac{B-A}{4\delta\xi} + \frac{C}{2\delta\xi^2}\right],$$

$$A = \frac{a_1(a_2+b_2)(h^n W_j^n - \xi_j h_t^n)}{(a_2 h^n - \xi_j)(b_2 h^n + \xi_j)},$$

$$B = \frac{a_1(a_2+b_2)h^n[(b_2-a_2)h^n + 2\xi_j]}{Re(a_2 h^n - \xi_j)^2(b_2 h^n + \xi_j)^2},$$

$$C = \frac{1}{Re}\left[\frac{a_1(a_2+b_2)h^n}{(a_2 h^n - \xi_j)(b_2 h^n + \xi_j)}\right]^2.$$

At a particular time level F_j^{n+1} is computed from (27). The velocity W_j^{n+1} is obtained from the continuity equation (20) by using the values of F_j^{n+1} at that time level. Once W_j^{n+1} is determined, its value at the free surface is then substituted in kinematic condition (24) to obtain the film thickness. The process is continued until it achieves the desired level of film thickness. Computation domain $[0,1]$ is discretized by 51 grid points with $c = 10^4$, this provides the uniform grid distribution in physical domain as well as computational domain. The time step has been calculated by

$$\delta t \leq 0.25 \times \delta\xi^2. \quad (28)$$

This comes from the CFL condition of numerical stability. The time step δt is chosen smaller than value that satisfied the stability condition for linear equation due to coupled nonlinear system.

4. Results and Discussion

Figure 1 represents the variation of film thickness with time for different values of the Darcy number Da. It is evident from the figure that the rate of film thinning decrease with the increasing value of the Darcy number. The increasing Darcy number Da implies that the porosity ϕ of the porous medium on the stretching surface increases and it resist the film thinning process.

Figure 2 and 3 show the variation of film thickness with time for different values of suction or injection parameter V respectively. It is clear from the figure 2 that the film thinning is more with increasing values of the suction parameter. In the figure 2, the reverse phenomena is observed in case of injection. Due to the continuous suction from the stretching wall there will be loss of liquid mass from the stretching surface, as a result the film thickness decreases with increase of

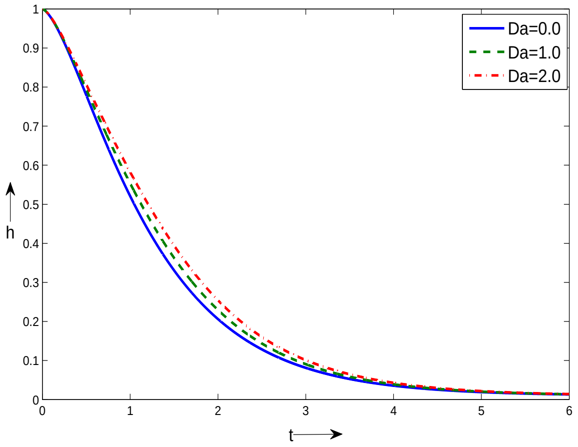


Fig. 1. Variation of film thickness h with respect to time t for different values of Darcy number Da with $Re = 1$, $V = 0.01$ and $M^2 = 1.0$.

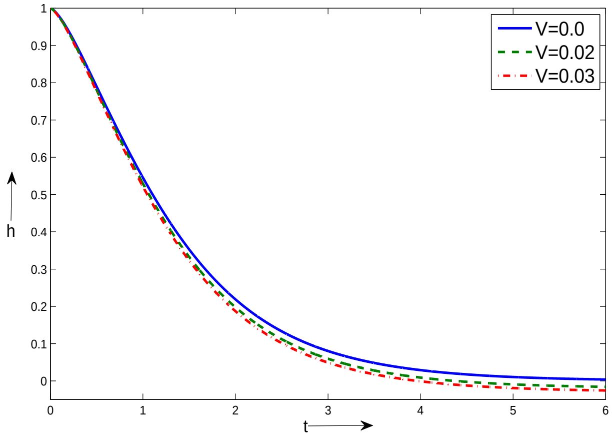


Fig. 2. Variation of film thickness h with respect to time t for different values of suction parameter with $Re = 1$, $Da = 1$ and $M^2 = 1.0$.

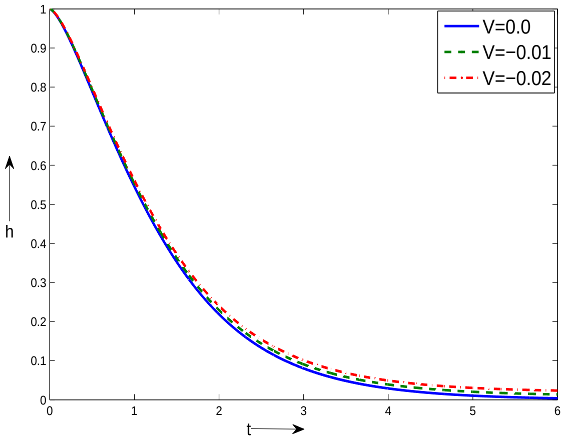


Fig. 3. Variation of film thickness h with respect to time t for different values of injection parameter with $Re = 1$, $Da = 1$ and $M^2 = 1.0$.

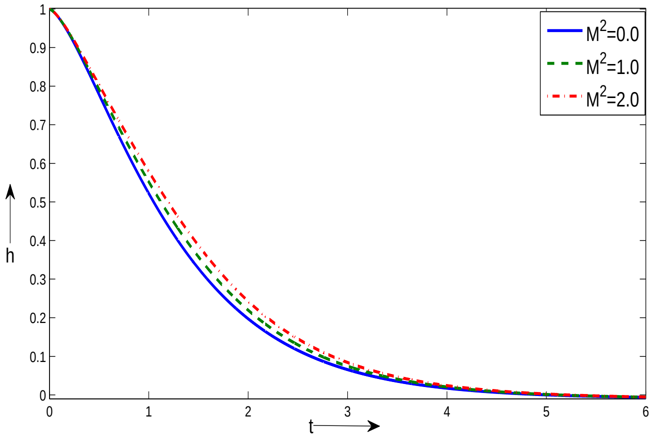


Fig. 4. Variation of film thickness h with respect to time t for different values of Hartmann number M with $Re = 1$, $Da = 1$ and $V = 0.01$.

the suction parameter. But for the injection there will be continuous gain of liquid mass that increases the film thickness. Figure 4 depicts the variation of the film thickness with time for different values of the Hartmann number M for the fixed values of Re, V and Da . It is evident from the figure that the thinning rate is considerably reduced with increase values of M. This is due to fact that as M increases the magnetic line of force put greater resistance on the film on the film thinning process. Figure 5 shows the variation of the horizontal velocity F with respect to z at time $t = 1.5$ for different values of Darcy number Da. It is observed from the figure that horizontal velocity F decrease with increasing the Darcy number Da. It is also clear from the figure that the film thickness decreases with the increase of the Darcy number. Figure 6 and 7 represent the variation of the velocity component F with z for different values of the suction and injection parameter respectively. It is evident from the figure 6 that the horizontal velocity F increases with the increasing of suction at the stretching wall whereas the opposite behaviour is observed in case of injection from the Figure 7.

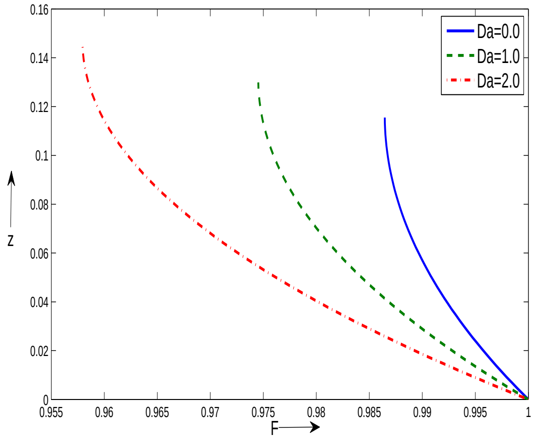


Fig. 5. Variation of horizontal velocity F with respect to z for different values of Darcy number Da with $Re = 1$, $V = 0.01$ and $M^2 = 1.0$.

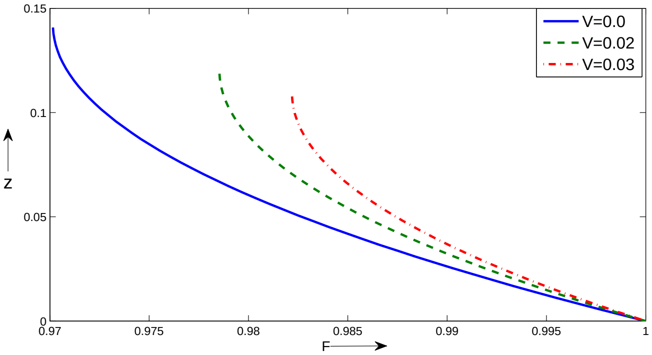


Fig. 6. Variation of horizontal velocity F with respect to z for different values of suction parameter with $Da = 1$, $M^2 = 1$ and $Re = 1$.

5. Conclusion

Effects of porous medium and suction/injection on film development over an unsteady stretching sheet is analyzed numerically in presence of the transverse magnetic field. It is assumed that the initially deposited liquid film over the stretching sheet is uniform and its remain uniform throughout the entire process of stretching. The following observations have been made from the present investigation. 1. The film thinning rate decreases with increase of the porosity of the porous medium.

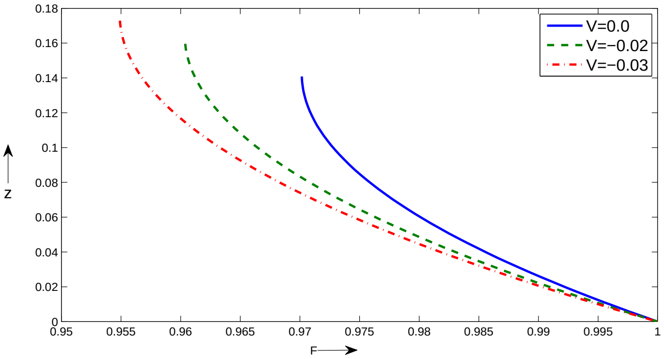


Fig. 7. Variation of horizontal velocity F with respect to z for different values of suction parameter with $Da = 1$, $M^2 = 1$, $Re = 1$.

2. Increasing suction is responsible for quicker thinning of film whereas increasing injection slowdown the film thinning process.

3. Film thinning rate decreases with increase of the Hartmann number.

References

[1] L. J. Crane. Flow past a stretching plate, Z. Angew. Math. Phys.(ZAMP), **21** (1970), 645-647.

[2] L. G. Grubka and K. M. Bobba, Heat transfer characteristics of a continuous stretching surface with variable temperature, J. Heat Transfer, **107** (1985), 248-250.

[3] C. Y. Wang, Stretching a surface in a rotating fluid, Z. Angew. Math. Phys.(ZAMP), **39** (1988), 177-185.

[4] K. B. Pavlov, Magnetohydrodynamic flow of an incompressible viscous fluid caused by deformation of a plane surface, Magnitnaya Gidrodinamika, **4** (1974), 146-147.

[5] H. I. Andersson, K. H. Bech and B. S. Dandapat, Magnetohydrodynamic flow of a power-law fluid over a stretching sheet, Int. J. Non-Linear Mechanics, **27** (1992), 929-936.

[6] H. I. Andersson, O. R. Hansen and B. Holmedal, Diffusion of a chemically reactive species from a stretching sheet, Int. J. Heat and Mass Transfer, **37** (1994), 659-664.

[7] P. Cheng and W. J. Minkowycz, Free convection about a vertical flate plate embedded in a porous medium with application to heat transfer from a dike, J. Geophys Res., **82** (1977), 2040-2044.

[8] A. Subhas and P. Veena, Visco-elastic fluid flow and heat transfer in a porous media over a stretching sheet, Int. J. Non-Linear Mechanics, **33** (1998), 531-540.

[9] E. M. A. Elbashbeshy and M. A. A. Bazid, Heat transfer in a porous medium over a stretching surface with internal heat generation and suction or injection, Appl. Math. Comput. **158** (2004), 799-807.

[10] A. Ali and A. Mehmood, Homotopy analysis of unsteady boundary layer flow adjacent to permeable stretching surface in a porous medium, Commun. Nonlinear Sci. Numer. Simul., **11** (2006), 326-339.

[11] L. E. Erickson, L. T. Fan and V. G. Fox, Heat and mass transfer on a moving continuous flate plate with suction or injection, Ind. Eng. Chem., **5** (1966), 19-25.

[12] P. S. Gupta and A. S. Gupta, Heat and mass transfer on a stretching sheet with suction or blowing, Canadian J. Chem. Engineering, **55** (1977), 744-746.

[13] C. K. Chen and M. Char, Heat transfer of a continuous strtching surface with suction or blowing , J. Math. Anal. Appl., **135** (1988), 568-580.

[14] C. Y. Wang, Liquid film on an unsteady stretching surface, Quarterly Appl. Math., **48** (1990), 601-610.

[15] H. I. Andersson, J. B. Aarseth, N. Braud and B. S. Dandapat, Flow of a power-law fluid on an unsteady stretching surface, J. Non-Newtonian Fluid Mechs., **62** (1996), 1-8.

[16] B. S. Dandapat, B. Santra and H. I. Andersson, Thermocapillarity in a liquid film on an unsteady stretching surface, Int. J. Heat and Mass Transfer, **46** (2003), 3009-3015.

[17] C. H. Chen, Heat transfer in a power-law fluid film over a unsteady stretching sheet, Heat and Mass Transfer, **39** (2003), 791-796.

[18] M. M. Nandeppanavarb, K. Vajravelu, M. S. Abel, S. Ravi, H. Jyoti, Heat transfer in a liquid film over an unsteady stretching sheet, Int. J. Heat and Mass Transfer, **55** (2012), 1316-1324.

[19] B. S. Dandapat and S. Maity, Flow of a thin liquid film on an unsteady stretching sheet, Phys. Fluids, **18** (2006), 102101.

[20] D. A. Neild and A. Beijan, Convection in porous media. Second Ed. Berlin: Springer; (1999).

[21] B. S. Dandapat and P. C. Ray, The effects of thermocapillarity on the flow of a thin liquid film on a rotating disc, J. Phys. D: Appl. Phys., **27** (1994), 2041-2045.

[22] G. O. Robert, Lecture Notes in Physics. Spinger-Verlag (1971).

[23] C. A. J. Fletcher, *Computational Techinique For Fluid Dynamics*. 1988(Spinger-Verlag, New York), Vol.**II**.

A new technique for generation of Automatic variable key – Up Down Automatic Variable Key (UDAVK)

Manash Pratim Dutta[1], Subhasish Banerjee[1], Chandan Tilak Bhunia[1]
[1]*National Institute of Technology, Arunachal Pradesh, India-791112*
manashpdutta@gmail.com

Abstract

Perfect secrecy can be attained with the help of variable keys that change from session to session or data to data. An idea of Automatic Variable Key (AVK) is a novel approach in terms of time variant key. In AVK, the key is made variable by an agreement that creates new key for each data. In this paper, a new technique to generate AVK has been proposed. In this technique, successive keys will be generated based on the number of 1's in the previous key and the key's positions in the key set. The technique has also been compared with other related key generation techniques of AVK to prove its excellency.

Keywords: *Perfect Security, AVK, UDAVK, Randomness, Average Randomness.*

1. Introduction

As day by day the volume of information traffic rises, security threats and attacks also increases. Therefore, to provide high level security to a cryptosystem is extremely desirable and it demands good amount of research and investigation in this area. In all cryptosystem, the challenge of the designer is to protect the key so that it can be unbreakable from various such attacks. Shannon had addressed the theory of perfect secrecy with time variant key [1-2]. According to Vernum, it would be impossible to break the key if the key is made time variant in nature. The idea of time variant key can be implemented by changing the key from one session to another along with the transmission of data [3-6]. Automatic Variable Key (AVK) had been introduced in this field as an idea of time variant key [7-10]. As per literature survey AVK is a novel approach to achieve perfect security.

In AVK, the key is made variable with exchanged data between a sender and a receiver. A new key is generated every time a data is exchanged which can be defined as:

K_0 = initial secret key
$K_i = K_{i-1} \oplus D_{i-1}$, for all $i > 0$

Where, K_{i-1} and D_{i-1} are key and data in the $(i-1)^{th}$ session respectively.

AVK can be applied in both private and public key cryptography. By using the AVK, it can be shown that various kinds of attacks such as brute force attack, frequency attack and differential frequency attack can be substantially reduced. Later different variations of AVK have been introduced for better security of a system.

Goswami et al. defined Computational Shifting AVK (CSAVK)[11] where the keys are generated by doing XOR operation between keys and data. In CSAVK, before performing XOR operation, key is shifted right (bit wise) and data is shifted left (bit wise).

According to Alternate Shifting AVK (ASAVK) [12], the keys are generated by block wise shift of previous key and block wise shift of previous data. Shifting depends on total length of key divided by two and total length of data divided by two. Finally, XOR operation is carried out between key and data.

In 2013, Goswami et al. has proposed Decimal Shifting AVK (DSAVK) [13] in which key is generated by XOR operation between bitwise right shift of the previous key and previous data. The key shift depends upon the decimal value produced after performing XOR operation of previous key and previous data.

In Key Variation with Random Number (KVRN) [14] technique, initial key and one numeric value (m) are exchanged between the sender and receiver. Then, subsequent keys can be generated by adding previous key with a number (X) and X varies from 1 to m by incrementing (X++). Whenever X becomes m, then another key and another numeric value (n) will be exchanged.

In PROTOCOL-I technique [15], initial key and one noise burst (m) are exchanged between the sender and the receiver by RSA. Where, subsequent keys are generated by applying AVK technique. When X=m, another key and another noise burst (n) will be exchanged further.

2. New idea

Here, we are trying to propose a new idea for the generation of keys called Up Down AVK (UDAVK) with an aim to enhance the level of security by increasing the randomness among the successive keys. The proposed algorithm can be stated as:

1. Initial key (K_1) is exchanged between the sender and the receiver through key distribution center.

2. (a) For even positioned key (K_{2i}),
   Even positioned intermediate key (K'_{2i}) = the previous key (K_{2i-1})-2^n for i>0 where n is the number of 1's present in the previous key.
   Then, even positioned Key (K_{2i}) = 2's complement of the even positioned intermediate key (K'_{2i})
   (b) For odd positioned key (K_{2i+1}),
   Odd positioned intermediate key (K'_{2i+1}) = the previous key (K_{2i}) + 2^n for i>0 where n is the number of 1's present in the previous key.
   Then, Key (K_{2i+1}) = 2's complement of the odd positioned intermediate key (K'_{2i+1})

3. Subsequent keys will be generated by repeating the step 2 for i = 1 to m, where m is the number of keys required to generate.

For illustration, let us consider the following examples:

Example-1: We consider that initial data D_0 is sent by the sender in encrypted form using the initial key K_1(10001000). In this key (K_1), the number of 1's is 2. As the 2nd key is an even positioned key, so by applying 2(a) we get 2nd positioned intermediate key, K'_2 as 10000100. Then taking the 2's complement of K'_2, we will get 2nd positioned key, K_2 as 01111100. Now, second key, K_2 contains five 1's. To find out third key, we will apply 2(b) (as third key is an odd positioned key) and 3rd positioned intermediate key, K'_3 becomes 10011100. By taking 2's complement of K'_3, we can get

3rd positioned key, K_3 as 01100100. This way by applying Up Down AVK, we can generate the successive keys for secure data transmission.

Example-2: In this case, assume that initial data D_0 is sent by the sender in encrypted form using the initial key K_1(11001100). In this key (K_1), the number of 1's is 4. For second positioned key (K_2), we apply 2(a) and we get 2nd positioned intermediate key, K'_2 as 10111100. Then taking the 2's complement of K'_2, we will get 2nd positioned key, K_2 as 01000100. Now, second key, K_2 contains two 1's. To find out third key, we will apply 2(b) and 3rd positioned intermediate key, K'_3 becomes 1001000. By taking 2's complement of K'_3 we can get 3rd positioned key, K_3 as 10111000. This way by applying Up Down AVK, we can generate the successive keys.

3. Analysis and comparison

For analysis purpose, we have considered randomness as a parameter which measures the amount of variation that exists between two successive keys. Randomness is equal to the number of positions at which the corresponding bits are different. We have used 10101010 as the initial key and after the execution of UDAVK, we get a set of keys as {10101010, 01100110, 10001010, 01111110, 01000010, 11000010, 00110110, …, }. Then we calculate randomness between two successive keys. After plotting the randomness as Y-axis and data as X-axis, the following graph (Fig. 1.) has been observed.

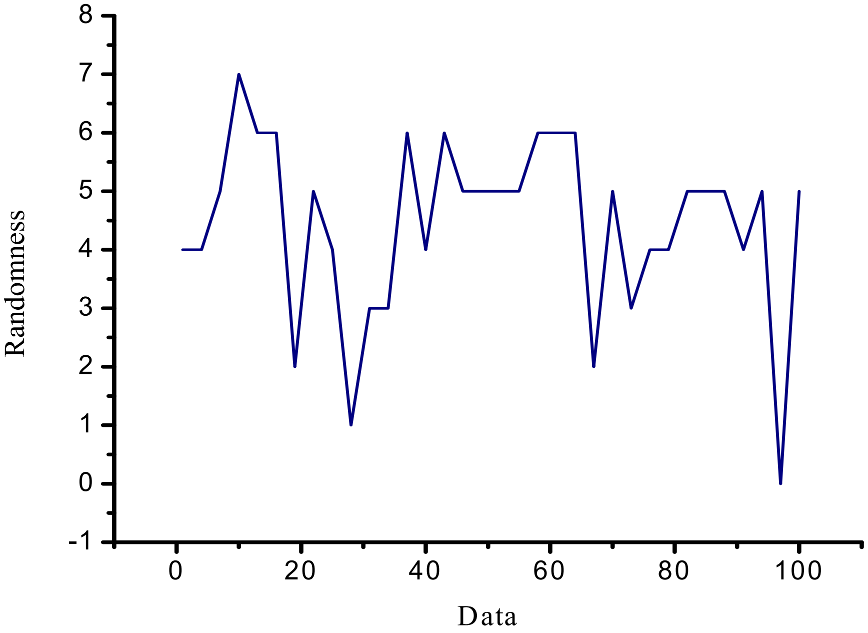


Fig. 1. Randomness of keys of Up Down AVK

Our proposed algorithm is compared with other related key generation techniques such as AVK, CSAVK, ASAVK, DSAVK, KVRN, PROTOCOL-I, PROTOCOL-II, PROTOCOL-III based on their average randomness. For the analysis purpose, we have used the same initial key (10101010) for all the protocols. The individual successive keys are generated by applying the above mentioned techniques. Then, average randomness is calculated for each technique. The analysis reveals that our technique gives the best result amongst all the techniques. As average randomness is more in our protocol, therefore this technique is able to provide more security to a system as compared to other related techniques. The superiority of our technique is illustrated in Fig. 2.

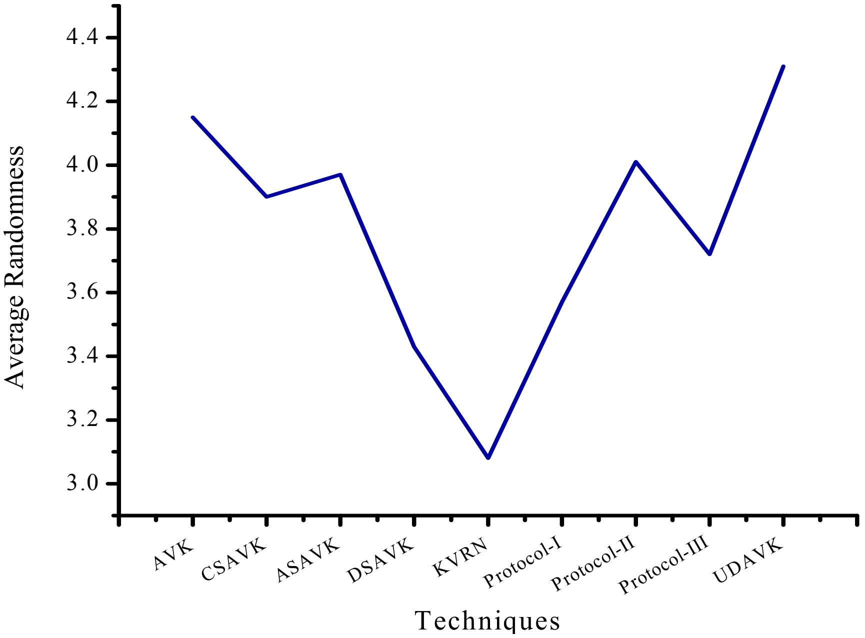


Fig. 2. Comparison of average randomness of Up Down AVK with other related techniques

4. Conclusion

In this paper, we have proposed a new technique, UDAVK to generate the successive keys under time variant mechanism. In the analysis and comparisons phase, we have shown that how our scheme can enhance the security by increasing the average randomness as compared to existing schemes. Hence, we can conclude that our proposed scheme can provide the perfect security over insecure communication channel.

5. References

[1] C. E. Shannon, Bell Syst. Tech. J., 27, 379–423, 623–656 (1948).

[2] C. E. Shannon, Bell Syst. Tech. J., 656-715 (1949).

[3] P. Chakarabarti, B. Bhuyan, A. Chowdhuri, C. T. Bhunia, Int. J. Comput. Sci. Netw. Secur., 8(5), 241-250 (2008).

[4] C. T. Bhunia, G. Mondal, S. Samaddar, Proc. of EAIT, (2006) 219-221; Calcutta CSI.

[5] C. T. Bhunia, Asian J. Inf. Tech., 5(9), 1017-1022 (2006).

[6] C. T. Bhunia, Application of AVK and Selective Encryption in Improving Performance of Quantum Cryptography and Networks, http://www.Ictp.it/~pub_off, IC/2006/045.

[7] W. Diffe, M. E. Hellman, Exhaustive Cryptanalysis of the NBS Data encryption standard, Computer, 74-84 (1977).

[8] E. Biham, Proc. Int. Symp. Foundations of Software Engineering, (1997) 260-273.

[9] H. Eberle, Proc. Int. Conf. Cryptology, (1992) 521-539.

[10] B. Schneir, Applied Cryptography, 2nd edn. , John Willey & Sons Inc., New York (1996).

[11] C. T. Bhunia, S. K. Chakraborty, R. S. Goswami, 100th Indian science Congress Association, (2013) January; Kolkata, India.

[12] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, J. Inst. Eng. India Ser. B, Publ. online (2014).

[13] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, 10th Int. Conf. Inf. Tech., IEEE Computer Society, (2013) 102.

[14] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. BhuniaJ. Inst. Eng. India Ser. B 94(4), 215-220 (2014).

[15] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, 2nd Int. Conf. Adv. Comp. Science Eng., (2013)149-152; las vegas, USA.

SUBSCRIPTION RATE

Annual Subscription	In Rupees	In US$
International Journal on Current Science & Technology	Rs. 5000/-	US$100

Payable by Bank Transfer/RTGS to Account No. **32709506720**, Name of the bank **Nirjuli, Bank code 9535, IFS Code: SBIN0009535**. Once paid details of Postal address of subscriber and scanned copy of Bank receipt may be send by E-mail to pchakraborty.ece@nitap.in

Authors' Instruction

The papers on the following subjects should reach in IEEE format only by E-mail : **pchakraborty.ece@nitap.in/conferencenitap@gmail.**com and a hard copy by post.

To,
The Editor,
International Journal on Current Science & Technology,
National Institute of Technology - Arunachal Pradesh
PO - Yupia, P.S. - Doimukh, Dist. - Papum Pare,
Pin - 791112, Arunachal Pradesh

Acceptance of paper is based on peer-review process.

Technical Education, Chemical Sciences, Engineering Sciences, Environmental Sciences, Information and communication Science & Technology (including Computer Sciences), Material Sciences, Mathematical Sciences (including Statistics), Medical Sciences, New Biology (including Biochemistry, Biophysics & Molecular Biology and Biotechnology) and Physical Sciences.

International Journal on Current Science & Technology
Vol. : 2 I No. : 2 I July - December' 2014

ISSN : 2320 5636

For Correspondence
National Instiute Of Technology Arunachal Pradesh
(An Institute of National Importance)
(Established by Ministry of Human Resource and Development, Govt. Of India)
PO-Yupia, P.S.-Doimukh, Dist-Papum Pare, Pin-791112, Arunachal Pradesh, India
T 0360-228 4801, **F** 0360-228 4972
E pchakraborty.ece@nitap.in/conferencenitap@gmail.com