Central University of Himachal Pradesh

Srinivasa Ramanujan Department of Mathematics

School of Mathematics, Computers and Information Science

AGENDA

7th BOARD OF STUDIES MEETING

TO BE HELD ON **15th JUNE, 2021**

Venue: through Online Mode on Google Meet
meet.google.com/zvd-idut-wsr

हिमाचल प्रदेश केन्द्रीय विश्वविद्यालय

Central University of Himachal Pradesh

(Established under Central Universities Act 2009)

अस्थाई शैक्षणिक खण्ड, शाहपुर, ज़िला काँगड़ा, हिमाचल प्रदेश -176206

Temporary Academic Block, Shahpur, Distt. Kangra (HP) - 176206

Website: www.cuhimachal.ac.in

AGENDA-INDEX

Agenda Item No.	PARTICULARS	Information
SRDM-BOS-7/21-1	Confirmation and Approval of the Minutes of the 6th Board of Studies meeting held on 28th October, 2020.	Annexure –I
SRDM-BOS-7/21-2	Deliberation and Approval for the Revival of Ph.D. Registration/Enrollment of Mr. Manoj Kumar, CUHP17RDMATH03.	
SRDM-BOS-7/21-3	Proposal of the Faculty Members of the Srinivasa Ramanjuan Department of Mathematics to become M.Phil./Ph.D. Supervisor/Guide.	
SRDM-BOS-7/21-4	To approve the appointment of Dr. Pankaj Kumar S/o Late Sh. Maniram as Research Supervisor of Mr. Manoj Kumar, CUHP17RDMATH03.	
SRDM-BOS-7/21-5	Deliberation and Approval of the Ph.D. Synopsis of the following students: Mr. Manoj Kumar, CUHP17RDMATH03 and Ms. Tanya Sharma CUHP18RDMATH01	Annexure - II & III
SRDM-BOS-7/21-6	Deliberation and Approval to update/extend the objectives of the Ph.D. Synopsis of Ms. Reena Koundal, CUHP15RDMATH03	Annexure - IV
SRDM-BOS-7/21-7	Approval to allow Ms. Shivani Aeri, CUHP20RDMATH01), a Ph.D. student to do the following zero credit course: Course Name: Advanced Topics in Geometry and Analysis, Course Code: MTH 611, during her Ph.D. course work	
SRDM-BOS-7/21-8	Approval to constitute the Research Advisory Committee (RAC) for Manoj Kumar, CUHP17RDMATH03, Ph.D. student (As per CUHP Ordinance No. 42, Clause 9)	
SRDM-BOS-7/21-9	Approval of List of Experts as Examiners for the Practical and Viva Voce Examinations of M.Sc. Mathematics.	Annexure - V
SRDM-BOS-7/21-10	Any item with the permission of the Chair	

Prof. Rakesh Kumar
Head,
Srinivasa Ramanujan Department of Mathematics

हिमाचल प्रदेश केन्द्रीय विश्वविद्यालय

Central University of Himachal Pradesh

(Established under Central Universities Act 2009)

अस्थाई शैक्षणिक खण्ड, शाहपुर, ज़िला काँगड़ा, हिमाचल प्रदेश -176206

Temporary Academic Block, Shahpur, Distt. Kangra (HP) - 176206

Website: www.cuhimachal.ac.in

File No.: MTH/1-5/CUHP/12/23 Dated: 15.06.2021

MINUTES OF THE 7th BOARD OF STUDIES MEETING

HELD ON 15th June, 2021

The **meeting** of the **7th Board of Studies** of the **Srinivasa Ramanujan Department of Mathematics**, School of Mathematics, Computers and Information Science, Central University of Himachal Pradesh, Temporary Academic Block, Shahpur was held through **online mode** on Google Meet (meet.google.com/zvd-idut-wsr) on **15th June, 2021** at **11:00 AM**. During the meeting, all members were **available** on **Google Meet**. Prof. Rakesh Kumar, **Head**, Srinivasa Ramanujan Department of Mathamatics and Dean, School of Mathematics, Computers and Information Science **chaired** the meeting.

Following members attended the meeting:

1. **Prof. Rakesh Kumar – Head and Convener**
   Head, Srinivasa Ramanujan Department of Mathamatics and Dean, School of Mathematics, Computers and Information Science, Central University of Himachal Pradesh, Temporary Academic Block, Shahpur.
2. **Prof. Jyoti Prakash – Subject Expert**
   Professor, Department of Mathematics and Statistics, Himachal Pradesh University, Shimla.
3. **Dr. Pawan Kumar Sharma – Subject Expert**
   Associate Professor, Department of Mathematics & Scientific Computing, National Institute of Technology, Hamirpur.
4. **Prof. Hum Chand – Vice Chancellor's Nominee**
   Professor, Department of Physics and Astronomical Science, Central University of Himachal Pradesh, Temporary Academic Block, Shahpur.
5. **Dr. Rajender Kumar – Vice Chancellor's Nominee**
   Associate Professor, Department of Chemical and Chemical Sciences, Central University of Himachal Pradesh, Temporary Academic Block, Shahpur.
6. **Dr. Sachin Kumar Srivastava – Member**
   Assistant Professor, Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Temporary Academic Block, Shahpur..
7. **Dr. Pankaj Kumar S/o Late Sh. Maniram – Special Invitee**
   Assistant Professor, Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Temporary Academic Block, Shahpur.
8. **Dr. Meenakshi – Special Invitee**
   Assistant Professor, Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Temporary Academic Block, Shahpur.
9. **Dr. Pankaj Kumar S/o Sh. Krishan Singh – Special Invitee**
   Assistant Professor, Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Temporary Academic Block, Shahpur

The **Chairman** welcomed all the **Hon'ble members & Special Invitees** and **briefed** about the **past activities** and also about the various **agenda items** to be **discussed** in the **meeting** which were **sent** in **advance** to all members through **e-mail** including **Subject Experts**. Various **Agenda Items** were **placed** before the **committee** and after **detailed discussion** and **deliberations** on each, the **following decisions** were taken:-

AGENDA ITEM NO. - SRDM-BOS-7/21-1

Confirmation and Approval of the Minutes of the 6th Board of Studies meeting held on 28th October, 2020 attached as Annexure I.

Decision:

The Minutes of the 6th meeting of the BoS were Confirmed and Approved.

AGENDA ITEM NO. - SRDM-BOS-7/21-2

Deliberation and Approval for the Revival of Ph.D. Registration/Enrollment of Mr. Manoj Kumar, CUHP17RDMATH03.

Decision:

All members unanimously approved the Revival of Ph.D. Registration/Enrollment of Mr. Manoj Kumar, CUHP17RDMATH03 as per approval from the Hon'ble Vice Chancellor.

AGENDA ITEM NO. - SRDM-BOS-7/21-3

Proposal of the Faculty Members of the Srinivasa Ramanjuan Department of Mathematics to become M.Phil./Ph.D. Supervisor/Guide.

Decision:

All the members of BoS unanimously approved the following Faculty Members as Research Supervisor(s) for Ph.D scholars of the Department as per CUHP Ordinance No. 42, Clause 6:

1. Dr. Pankaj Kumar S/o Late Sh. Maniram, Assistant Professor, Srinivasa Ramanujan Department of Mathematics, School of Mathematics, Computers and Information Sciences.
2. Dr. Pankaj Kumar S/o, Sh. Krishan Singh, Assistant Professor, Srinivasa Ramanujan Department of Mathematics, School of Mathematics, Computers and Information Sciences.

AGENDA ITEM NO. - SRDM-BOS-7/21-4

To approve the appointment of Dr. Pankaj Kumar S/o Late Sh. Maniram as Research Supervisor of Mr. Manoj Kumar, CUHP17RDMATH03

Decision:

All members unanimously approved the appointment of Dr. Pankaj Kumar S/o Late Maniram as Research Supervisor of Mr. Manoj Kumar, CUHP17RDMATH03.

AGENDA ITEM NO. - SRDM-BOS-7/21-5

Deliberation and Approval of the Ph.D. Synopsis of the following students: Mr. Manoj Kumar, CUHP17RDMATH03 and Ms. Tanya Sharma, CUHP18RDMATH01 attached as Annexure I & II respectively.

Decision:

All members agreed and approved the Ph.D. Synopsis of Ms. Tanya Sharma, CUHP18RDMATH01, whereas the Ph.D. Synopsis of Mr. Manoj Kumar, CUHP17RDMATH03 was deferred to the next BoS meeting as the concerned candidate has not yet defended his Ph.D. Synopsis in the Research Advisory Committee (RAC) meeting.

AGENDA ITEM NO. - SRDM-BOS-7/21-6

Deliberation and Approval to update/extend the objectives of the Ph.D. Synopsis of Ms. Reena Koundal, CUHP15RDMATH03 attached as Annexure IV.

Decision:

All members agreed and approved to update/extend the objectives of the Ph.D. Synopsis of Ms. Reena Koundal, CUHP15RDMATH03.

AGENDA ITEM NO. - SRDM-BOS-7/21-7

Approval to allow Ms. Shivani Aeri, CUHP20RDMATH01), a Ph.D. student to do the following zero credit course:

Course Name: Advanced Topics in Geometry and Analysis, Course Code: MTH 611, during her Ph.D. course work

Decision:

All members agreed and approved to offer the Four credit course *"Course name: Advance Topics in Geometry and Analysis, Course Code: MTH 611"* as zero credit course in the Ph.D. Course work of Ms. Shivani Aeri, CUHP20RDMATH01), as per recommendations from her Research Supervisor.

AGENDA ITEM NO. - SRDM-BOS-7/21-8

Approval to constitute the Research Advisory Committee (RAC) for Mr. Manoj Kumar, CUHP17RDMATH03, Ph.D. Student as per Ordinance No. 42, Clause 9.

Decision:

All members agreed and approved the following Research Advisory Committee (RAC) for Mr. Manoj Kumar, CUHP17RDMATH03:

1. **Head of the Department (Ex-Officio Chairman)**
2. **Dr. Pankaj Kumar S/o Lt. Sh. Maniram (Convener)**
3. **Dr. Sachin Kumar Srivastava (Subject Expert)**

AGENDA ITEM NO. - SRDM-BOS-7/21-9

Approval of List of Experts as Examiners for the Practical and Viva Voce Examinations of M.Sc. Mathematics attached as Annexure V.

In accordance with the draft ordinance 4(i), Section 23 and Statute 16(2) of the Central Universities Act 2009, section 4(b) i and ii, the Head, Department of Plant Sciences placed before the members of the Board of Studies (BoS) the list of examiners for M.Sc. Practical(s) and Viva Voce(s) Examinations for their approval, as per list attached at Annexure V.

Decision:

All members agreed and approved the list of examiners as proposed at Annexure V. It was also suggested that the list will be updated regularly by the faculty members of the Srinivasa Ramanujan Department of Mathematics with the consent of the respective Head of the Department and the same be reported in the next meeting of BoS. It was also suggested that preferably the subject course experts be invited for specific courses. The BoS also recommended that, if needed, HoD may invite a Subject Expert (External Examiner) not included in the list on the recommendations of the concerned faculty member(s) and after approval of competent university authority.

AGENDA ITEM NO. - SRDM-BOS-7/21-10

Any item with the permission of the Chair: **No item was taken**

The meeting ended with a vote of thanks to the chair.

Dr. Pankaj Kumar
S/o Sh. Krishan Singh
(Special Invitee)

Dr. Meenakshi,
(Special Invitee)

Dr. Pankaj Kumar
S/o Late Sh. Maniram
(Special Invitee)

Dr. Sachin Kumar Srivastava
(Member)

Dr. Rajender Kumar
(VC's Nominee)

Prof. Hum Chand
(VC's Nominee)

Dr. Pawan Kumar Sharma
(Subject Expert)

Prof. Jyoti Prakash
(Subject Expert)

Prof. Rakesh Kumar
Chairman & Convener

Central University of Himachal Pradesh
(Established under Central Universities Act 2009)
Temporary Academic Block, Shahpur, Distt. Kangra (HP) - 176206
Website :www.cuhimachal.ac.in

SRINIVASA RAMANUJAN DEPARTMENT OF MATHEMATICS

Minutes of the SIXTH meeting of Board of Studies (BOS) held on 28th October, 2020 at 11:00 AM

The SIXTH meeting of BOS of the Srinivasa Ramanujan Department of Mathematics was held on 28th October, 2020 in online mode at Temporary Academic Block, Shahpur at 11:00AM.

The following were present:

1. Prof. Rakesh Kumar, Chairman & Convenor
2. Dr. Pawan Kumar Sharma, External Expert, NIT Hamirpur
3. Prof. Jyoti Prakash, External Expert, HPU Shimla
4. Prof. Hum Chand, Head, Department of Physics & Astronomical Science, CUHP
5. Dr. Rajender Kumar, Head, Department of Chemistry & Chemical Science, CUHP
6. Dr. Sachin Kumar Srinivasa, Member, Srinivasa Ramanujan Department of Mathematics, CUHP
7. Dr. Pankaj Kumar, Dean's Nominee, Srinivasa Ramanujan Department of Mathematics, CUHP

The decisions taken on various items of Agenda and record of discussions held are as under:

Item-BOS 6.1: To confirm the minutes of the 5th Meetings of BOS of the Department of Mathematics held on 16th May 2018 (Annexure I).

Decision: The minutes of the Fifth Meeting of the BOS of Srinivasa Ramanujan Department of Mathematics were approved.

Item-BOS 6.2: To approve the Research Methodology course (Course Code MTH 601) for the scholars of Srinivasa Ramanujan Department of Mathematics (Annexure-II).

Decision: The BOS approved the Item **BOS-6.2.**

Item-BOS 6.3: To approve the course "Research and Publication Ethics (RPE)" for PhD students (Annexure-IIIA). As per D.O. No. F.1-1/2018(Journal/CARE), December 2019, UGC approved two Credit Course for awareness about publication ethics and publication misconducts entitled "Research and Publication Ethics (RPE)" to be made compulsory for all PhD students for coursework (Annexure-IIIB).

Decision: The BOS approved the Item **BOS-6.3.**

Item-BOS-6.4: To approve the Synopsis of the following students (Annexure-IV & V):

S. No.	Name of Student with Roll No.	Name of Supervisor	Area of Research	Date of Joining of student for Ph.D.
1	Anuj Kumar CUHP17RDMATH01	Dr. Sachin Kumar Srivastava	Differential Geometry	13.11.2017
2	Mayrika Dhiman CUHP17RDMATH02	Dr. Sachin Kumar Srivastava	Differential Geometry	13.11.2017

Decision: The BOS members unanimously approved the synopsis of Anuj Kumar and Mayrika Dhiman.

Item-BOS-6.5: To approve the faculty member to Supervise research work of the following scholar:

S. No.	Name of Student with Roll No.	Name of Supervisor	Area of Research	Date of Joining of student for Ph.D.
1	Shivani Aeri CUHP20RDMATH01	Dr. Rakesh Kumar	Numerical Analysis	05.08.2020

Decision: The BOS members unanimously approved the respective faculty member to supervise the Ph.D. work of Shivani Aeri.

Item-BOS-6.6: To approve the revised course structure of M.Sc. Mathematics (Annexure VI).

Decision: The BOS approved the Item **BOS-6.6.**

Item-BOS-6.7: To approve the list of courses for Ph.D. course work in mathematics (Annexure VII).

Decision: The BOS approved the Item **BOS-6.7.**

Item-BOS-6.8: To report and recommend the Research Advisory Committee (RAC) (previously named as Research Progress Monitoring Committee (RPMC)) constituted for the Research Scholars in Research Degree (RD) Programme in Mathematics during the year 2017, 2018 2019 & 2020 to the School Board.

As per CUHP Ordinance No. 42, Clause 9, The Research Advisory Committee for each PhD scholar shall be formulated to monitor the research work / progress of the research degree students enrolled in the department.

The Research Advisory Committee (RAC) shall comprise the research supervisor of the PhD student who shall be the convener of the committee, Head of the Department / Director of the Centre who shall be the ex-officio chairman, and at least one subject expert nominated by the Head/Director upon the recommendation of the concerned supervisor.

Research Advisory Committee (RAC) for each student was formulated and notified for each student of both the academic sessions (2015, 2017, 2018 & 2020). The details of each RAC are placed before the BoS for recommendation to School Board.

S. No.	Name of the RD Student & Enrolment Number	Research Advisory Committee
1	Tanya Sharma CUHP18RDMATH01	1. Head of Department (Ex-Officio Chairman) 2. Dr. Rakesh Kumar (Convener) 3. Dr. Pankaj Kumar (Subject Expert)
2	Shivani Aeri CUHP20RDMATH01	1. Head of Department (Ex-Officio Chairman) 2. Dr. Rakesh Kumar (Convener) 3. Dr. S. K. Srivastava (Subject Expert)
3	Kanika Sood	1. Head of Department (Ex-Officio

	CUHP15RDMATH01	Chairman) 2. Dr. S. K. Srivastava (Convener) 3. Dr. Pankaj Kumar (Subject Expert)
4	Anuj Kumar CUHP17RDMATH01	1. Head of Department (Ex-Officio Chairman) 2. Dr. S. K. Srivastava (Convener) 3. Dr. Pankaj Kumar (Subject Expert)
5	Mayrika Dhiman CUHP17RDMATH02	1. Head of Department (Ex-Officio Chairman) 2. Dr. S. K. Srivastava (Convener) 3. Dr. Pankaj Kumar (Subject Expert)
6	Ravinder Kumar CUHP15RDMATH02	1. Head of Department (Ex-Officio Chairman) 2. Dr. Rakesh Kumar (Convener) 3. Dr. Pankaj Kumar (Subject Expert)
7	Reena Koundal CUHP15RDMATH03	1. Head of Department (Ex-Officio Chairman) 2. Dr. Rakesh Kumar (Convener) 3. Dr. S. K. Srivastava (Subject Expert)

Decision: The BOS approved the Item **BOS-6.8.**

Item-BOS-6.9: Any other item from the permission of the Chair.

Decision: None of the members proposed any item for discussion and hence no item was taken up.

The meeting terminated with a vote of thanks to all the members of BOS.

Central University of Himachal Pradesh
(Established under Central Universities Act 2009)
Temporary Academic Block, Shahpur, Distt. Kangra (HP) - 176206
Website :www.cuhimachal.ac.in

Dr. Pawan Kumar Sharma | Prof. Jyoti Prakash | Prof. Hum Chand

Dr. Rajender Kumar | Dr. Sachin Kumar Srivastava

Dr. Pankaj Kumar | Prof. Rakesh Kumar

Copy to:

1. All the members of BOS, Srinivasa Ramanujan Department of Mathematics for approval.
2. The Coordinator TAB-Shahpur for Information and Record.
3. The Registrar, Camp Office Dharamshala for information and Record.
4. The Finance Officer, Camp Office Dharamshala for information and Record.
5. The Controller of Examination (CoE), Camp Office Dharamshala for information and Record.
6. P.S. to Vice-Chancellor for Information of Hon'ble Vice-Chancellor.

Annexure - II

Design and Development of Elliptic Curve and Lattice Based Digital Signature Schemes

A synopsis is submitted

by

Manoj Kumar

under the supervision of

Dr. Pankaj Kumar

to

Srinivasa Ramanujan Department of Mathematics
School of Mathematics, Computer and Information Sciences
Central University of Himachal Pradesh
[Establish under Central Universities Act 2009]
TAB-Shahpur, Distinct Kangra, Himachal Pradesh-176215, India

1. INTRODUCTION

Basic model: The basic communication model involves at least two communicators as shown in figure 1, say sender S and receiver R. The sender transfers the information to receiver through a secure or insecure channel. This model can be one to one, many to one, one to many and many to many.

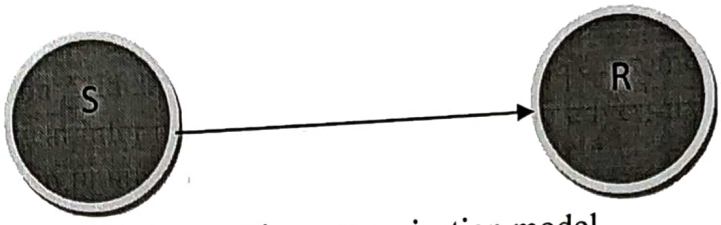

Fig 1: Basic communication model

1.1 ATTACKS AND THREATS

Any structured and unstructured threat that comprises with our network security is called security attack. The most popular security attack are given below.

1) Denial of Service (DOS) attack: In this attack, the adversary takes control on the resources and try to congest the communication channel used during communication. Purpose of the attacker during this attack, to prevent the crucial information from arriving source. For example in a VANET, server wants to warn about a danger to a driver but attacker use the DOS attack and act the malicious activities. If receiver did not receive the information within the time which leads a big happening [1,2, 4].

2) Message Suppression Attack: In this attack, an adversary select some dropping packets, these packets may be the critical information needs to receiver. The adversary can extract the critical information and can use in future [3,4].

3) Fabrication Attack: The adversary circulate the wrong information into the network during this attack. This attack contains warning, identities, certificate, and fabricate messages. The transmitter also claim that the transmitted information comes through the different channel [4,7,8].

4) Alteration Attack: The adversary alters the original data. This attack involve the delaying the transmitting information, change the actual data during data transmission [5,6].

5) Replay Attack: The adversary generates the echo of transmitting information of a past information to take the benefit of the situation of the message at the time of sending [4,6].

6) Sybil Attack: The adversary generates a bulk of pseudonyms to make a route jam and force to select the alternate route or stop the application [5,6].

1.2 SECURITY REQUIREMENTS

To secure our network, we need some following security goals.

1. Authentication: To make sure the origin of message transmitted from sender to receiver. For this task, sender assign a dialogue session before start the communication with other participants.

Signing each message like this procedure, leads an overhead on the system. We use the elliptic curve cryptography (ECC) to reduce the overhead [9,10].

2. Availability: To make sure that the network should be available for all time for receiving the information. This feature is very crucial for the real time applications where the applications needs much faster response then other applications for example Flying ad-hoc network (FANET), Vehicle ad-hoc network (VANET), Sensor network [9,10].

3. Non-repudiation: To prevent from those adversary who denying their misconduct. For this task Sender assign their private key before sending the message to receiver. The sender can't deny their participation because of involving their private key [9,10].

4. Privacy: To keep the secrecy of the communication from the outsider and insider adversaries. To achieve this task, we use pseudo identity instead of the original identity. The primary goal of the privacy is to keep the secret keys of the participants [9,10].

5. Confidentiality: the privacy of the message send by the sender should be protected. To achieve this task, the encrypted message will be send to communicators [9,10].

1.3 BASIC FUNCTION OF CRYPTOGRAPHY

- Plain Text (P): Plain text is the original message send by the sender to receiver.
- Secret Key (K): Secret key is used to encrypt the plain text.
- Cipher text (C): Cipher text is the result of the plain text after encryption by secret key.
- Encryption Algorithm (EA): EA is the encryption algorithm by which the sender encrypt the message by secret key.
- Decryption Algorithm (DA): DA is the decryption algorithm by which the receiver decrypt the message by secret key.

1.4 BASIC DIGITAL SIGNATURE SCHEME

A traditional digital signature scheme involves the three algorithms.

- **KEY-GEN**: Taking an input security parameter $1^{k,}$ this algorithm produces a private-public key pair.
- **Signature**: This algorithm is run by the signer, signer sign the message m with their private key pk. Which can be notified as $\sigma = Sign_{pk}(m)$
- **Verification:** In this algorithm, the verifier validates the signature with the signer's public key. If the verification is successful, then accept the signature otherwise reject the signature.

  $Verify_{pk}(m, Sign_{pk}(m)) = 1$

1.5 CRYPTANALYSIS

We analysis the previous existing scheme proposed by researchers during cryptanalysis technique. We examines the security of the suggested scheme and try to make insecure under the given

restrictions. By the cryptographic technique, we try to find the limitations and weakness in the existing algorithm. Cryptanalysis is a good practices (not a bad practices) which analyses the security of the suggested scheme and find the ambiguity in their scheme thereafter the weakness of scheme can be reduced or eliminated in the algorithm.

1.6 ELLIPTIC CURVES OVER F_q

Suppose $E(F_q)$ be define an elliptic curve over a field F_q with the parameters $\alpha, \beta \epsilon F_q$ where (*where* α, β *satisfies the constraints* $4\alpha^3 + 27\beta^2 \neq 0$), contains the point set $(t, s) \in E(F_q)$, satisfies the constraint $s^2 = t^3 + \alpha t + \beta$. The set of possible points over $E(F_q)$ also includes the point of infinity O as an identity w.r.t. addition operation. The operation defined over $E(F_q)$ is addition. $E(F_q)$ forms a abelian group w.r.t. addition operation [11].

The operation defined over $E(F_q)$ is specified as follow.

$$P + O = O + P = P, \quad \forall P \in E(F_q)$$

If $P = (t, s) \in E(F_q)$ then $(t, s) + (t, -s) = O$. The points $(t, -s) \in E(F_q)$ is the negative of P and denoted by $-P$).

If $P = (t_1, s_1) \in E(F_q)$ and $Q = (t_2, s_2) \in E(F_q)$ and $P \neq Q$, then $T = P + Q = (t_3, s_3) \in E(F_q)$, where $t_3 = \tau^2 - t_1 - t_2, s_3 = \tau(t_1 - t_3) - s_1$, and $\tau = (s_2 - s_1)/(t_2 - t_1)$, i.e. it can be shown the addition of two points can be as the point of intersection over $E(F_q)$.

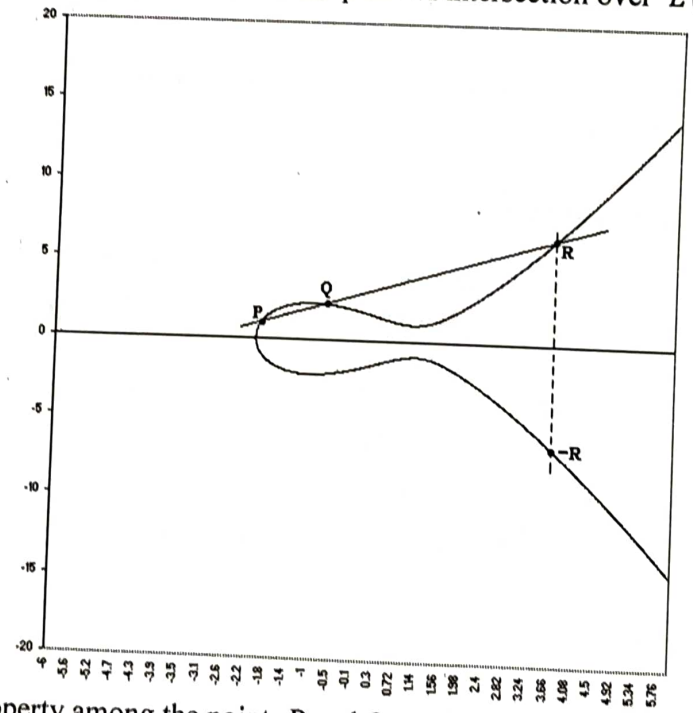

Fig 1.2: Additive property among the points P and Q on the elliptic curve: $s^2 = t^3 + \alpha t + \beta$ *[11]*

Let $P = (t, s) \in E(F_q)$. The Point $= P + P = 2P = (t_1, s_1) \in E(F_q)$, where $t_1 = \tau^2 - 2t$, $s_1 = \tau(t - s_1) - t$, where $\tau = \frac{3t^2 + a}{2s}$. This property is called the doubling of a point as shown in the figure 1.3 as the intersection point along tangent at P over the elliptic curve .

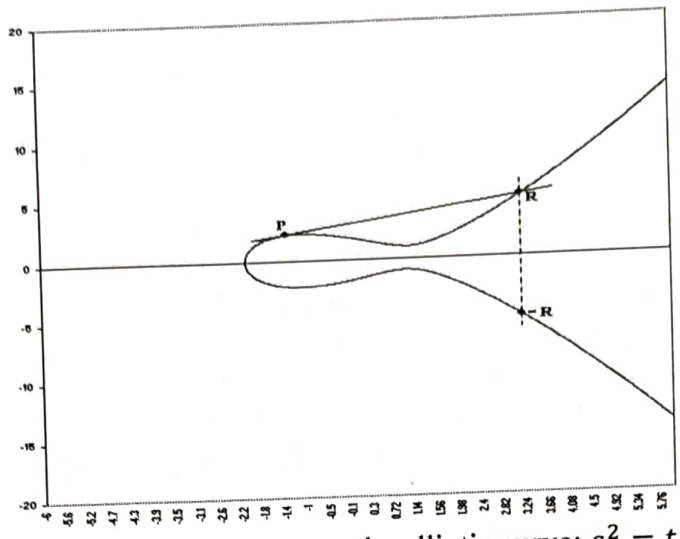

Fig 1.3: Doubling of a point P = 2R over the elliptic curve: $s^2 = t^3 + \alpha t + \beta$ *[11]*

2. RELATED WORK

Shamir [12] suggested the infrastructure of identity based cryptography (IDC). In the IDC, third party generates the signer's complete private key of the signer. IDC inherit a well-known problem called key escrow problem (KEP). Al-riyami and Peterson [13] proposed the pairing based certificateless signature scheme (CLS) in 2003. CLS scheme improves the difficulties inherit in IDC. Huang et al [14] proposed a cryptanalysis of Al-riyami and Peterson [13] CLS scheme and found insecure successfully.

After the discovery of Al-riyami and Peterson, a lot of contemporary researchers [15, 17, 20, 21,22, 24]designed their CLS schemes with different aspects. Yum and Lee [15] designed a CLS scheme and proves the security of scheme against identity and message attack. Thereafter, Hu et al [16] proved that the Yum and Lee [15] proposed CLS scheme fails the protection against the public key substitution attack (PKSA). Gorthala and Sexena [17] designed an efficient pairing operation based CLS scheme using random oracle model (ROM) method. Cao et al. [18] founds insecure during security analysis of Gorthala and Sexena [17] CLS scheme against PKSA. Furthermore, Huang [20] fabricate the adversaries into subtypes called Normal, Strong and Super type depend on their attacking power. Chen et al shows that the strong type adversary is not successful in the real life applications like FANET, VANET whereas Normal and Super type adversaries are more applicable. Boneh [19] developed a certificateless aggregate signature scheme (CLAS) that merge the benefit of aggregate property with the CLS. Aggregate property is a many to one map that integrates the dissimilar n signatures comes from the different source in to a single length signature. Zhang and Zhang [23] introduce a pairing based CLAS scheme and proves the security with ROM. Shim [25] did the security analysis of Zhang and Zhang proposed CLAS scheme and found that their proposed scheme is insecure against collision insider attack. Xiong [26,27] et al proposed efficient computationally pairing based operation without synchronization and proves the security by ROM under diffie-hallman problem. Hang tu et al. [29], Zhang et al. [28] and Cheng [30] founds that Xiong et al fails to retains security against the different concrete attacks like insider attack, honest but curious attack, malicious but passive attack, collision resistant attacks and universal attack. Horng et al. [31] and Malhi et

al. [32] proposed a pairing based CLAS scheme and implement on VANET. Kumar et al [33] cryptanalyze of Malhi et al scheme and found that their designed scheme is not secure against malicious but passive attack, insider attack and honest but curious attack. Kumar et al [34] proposed an efficient pairing CLS scheme and implement on healthcare wireless sensor network.

Historically, Lattices based cryptography (LBC) infrastructure developed in the 18th century by Gauss, Langrage and later Minkowaski [35, 36]. Ajtai [37] provides a starting point of research in 1996 in which he used not only the cryptanalysis but also construct cryptographic primitive by using lattices. LBC gives many advantages such as simple with less operation and very useful for low cost devices. LBS also gives an alternatives against traditional theoretical based cryptography. Goldreich et al. [38] designed a cryptographic primitive based on the LBC. Hoffstein et al designed two different primitive by using NTRU lattices say ring based public key cryptosystem [39] and digital signature [40].

3. STRUCTURE OF CLS SCHEME

A CLS infrastructure contains the following algorithms discussed in table 1 named *Setup, PPK-Gen, PK-Gen, Sign and Verification* [13].

Table 1

Algorithms	**Executes**	**Input**	**Output**	**Remarks**
Setup	KGC	Use 1^k, k is security constraint	(msk, mpk), $Params$	Keep msk secretly itself, $Params$ be a public parameter.
PPK-Gen	KGC	User identity, $Params$	Partial private key ppk	ppk transferred to user through a secure channel.
PK-Gen	User	User's identity, ppk	Public/Secret Key pair (upk, usk)	User generates their private key with the help of ppk
Sign	User/Signer	(usk, ppk)	Signature σ	User/ Signer generates the signature with the help of usk, ppk.
Verification	Verifier	mpk, ID, upk and σ on the message m	Verification equation	If verification equation satisfied then accept the signature otherwise reject.

3.2 SYMBOL NOTATIONS TABLE

The symbol used in the table 1 are describe as following table 2.

Table 2

Notations	Description
mpk	KGC's public key

msk	KGC's secret key
upk	Public key of signer/user
usk	Secret key of signer/user
m	Message
$Params$	Public Parameter
σ	Signer's generated Digital signature

4. OBJECTIVES

- To study the existing identity based designed digital signature schemes and certificateless based digital signature schemes.
- Deep study of cryptographic primitives regarding digital signatures such as group signature, aggregate signature, multi signature, ring signature, partially blind signature, blind signature, pairing based signature, without pairing based signature, proxy signature compact signature, Thrasheshold signature, policy based signature, leakage free signature, Dual signature, Strong designated verifier, Attribute based signature, Undeniable signature etc.
- Analyze the previous designed elliptic curve and lattice based digital signature schemes.
- Explore the limitations of lattice based and elliptic curve based previous designed digital signature scheme.
- Design and development of the certificateless digital signature schemes in the elliptic curve environment.
- Design and development of the digital signature schemes on the lattice based environment.
- Implement these schemes on various applications.

5. METHODOLOGY

- By investigating the main techniques such as ECC, Public key infrastructure, ID based infrastructure and certificateless infrastructure, lattice based infrastructure and many other techniques.
- By studying the latest research papers mainly previous 5 years research papers concerning with elliptic curve and lattice based digital techniques.
- Cryptanalyze the existing digital signature schemes proposed by the researchers and try to remove the weakness of their schemes.
- Design the mathematical prototype to design the new CLS schemes for different environment and different applications.
- Use the NP hard problem to prove the security of our proposed CLS scheme by using many problems like computational diffie-hellman problem, discrete logarithm problem for

elliptic curve based digital signature and use the techniques mainly shortest and closest vector problem for lattice based digital signature.

- Use different techniques mainly random oracle model and standard oracle model for elliptic curve based digital signature scheme and learning with errors for lattice based digital signature to prove the security of our designed CLS schemes.
- We demonstrate the computational and efficiency of our designed CLS by comparing with the previous designed schemes.

6. REFERENCES

[1] Rivas, D. A., Barcelo-ordinas, J. M., Zapata, M. G., & Morillo-pozo, J. D. :Security on VANETs: Privacy, misbehaving nodes, false information and secure aggregation. Elsevier Journal of Network and Computer Applications, 34(6), 1942–1955 (2011).

[2] Wu, B., Chen, J., Wu, J., & Cardei, M.:A survey on attacks and countermeasures in mobile ad hoc networks. Springer Journal of Wireless Network Security, 2, 103–135, (2007).

[3] Zhang y., Minier Privacy and Security in Wireless Sensor Networks: Protocols, Algorithms, and Efficient Architectures, Journal of Computer Networks and Communications, 1-14 (2012).

[4] Verma K., Hasbullah H., Kumar A. : Prevention of DoS Attacks in VANET, Wireless Personal Communications volume 73, pages95–126 (2013).

[5] Lv S, Wang X, Zhao X, Zhou X :Detecting the Sybil attack cooperatively in wireless sensor networks. In: CIS '08: proceedings of the 2008 international conference on computational intelligence and security. IEEE Computer Society, Washington, DC, USA, pp 442–446 (2008).

[6] Ssu KF, Wang WT, Chang WC :Detecting Sybil attacks in wireless sensor networks using neighboring information. Comput Netw 53(18):3042–3056 (2009).

[7] Cook D.J., Augusto J.C., Jakkula V.R :Ambient intelligence: technologies, applications, and opportunities, Pervasive and Mobile Computing, 5, 277–298, DOI 10.1016/j.pmcj.2009.04.001 (2009).

[8] Ameen M. A., Liu J., Kwak K., :Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications, Journal of Med Syst 36, 93–101 :DOI 10.1007/s10916-010-9449-4 (2012).

[9] Li X., Niu J., Khan M.K., and Liao J.: An enhanced smart card based remote user password authentication scheme, Journal of Network and Computer Applications, vol. 36, no. 5, pp. 1365–1371, (2013).

[10] Lasc I.,:A simple and efficient authentication scheme for mobile satellite communication systems," International Journal of Satellite Communications & Networking, vol. 30, no. 1, pp. 29–38, (2011).

[11] Silverman, J.H.:Advanced Topics in the Arithmetic of Elliptic Curves; Springer Science & Business Media: Berlin/Heidelberg, Germany, Volume 151 (1994).

[12] A. Shamir, "Identity based cryptosystems and signature schemes",G.R. Blakley, D. Chaum (Eds.), Crypto'84, LNCS 196, Springer-Verlag, Santa Barbara, California, USA, pp. 47–53, (1984).

[13] Al-Riyami, S., Paterson, K. "Certificateless Public Key Cryptography",Asiacrypt'03 (2003),

[14] Huang X., Susilo W., Mu Y., Zhang F., "On The Security Of A Certificateless Signature Scheme", in: Proceedings of the CANS, Lecture Notes in Computer Science, vol. 3810, 2005, pp. 13–15. LNCS 2894, Springer-Verlag. 452-473 (2003).
[15] Yum, D. H., Lee, P. J.: Generic construction of certificateless signature. Information Security and Privacy, LNCS_3108, 200–211, DOI 10.1007/978-3-540-27800-9_18 (2004),.
[16] Hu, B.C., Wong, D.S., Zhang, Z., and Deng, X.: Certificateless signature: a new security model and an improved generic construction. Designs, Codes and Cryptography, **42**(2), 109–126 (2007).
[17] Gorantla M., Saxena A., An Efficient Certificateless Signature Scheme, In Computational Intelligence and Security, LNCS 3802,110–116 DOI 10.1007/11596981_16 (2005).
[18] Cao X., Paterson K.G., Kou W.: An attack on a certificateless signature scheme. Report 2006/367, Cryptology, ePrint Archive,(2006).
[19] Boneh D., Gentry C., Lynn B., Shacham H.,:Aggregate and verifiably encrypted signatures from bilinear maps", E. Biham (Ed.), EUROCRYPT, LNCS 2656 (2003).
[20] Huang X., Mu Y., Susilo W., Wong D.S., Wei Wu :Certificateless signatures: New Schemes and Security Models" . The computer journal, vol 55 No.4, (2012).
[21] Eslami Z., Pakniat N., :Certificateless aggregate signcryption: Securitymodel and a concrete construction secure in the random oracle model", Journal of King Saud University – Computer and Information Sciences 26, 276–286 (2014).
[22] Chen Y.C., Horng G., Liu C.L., Tsai Y.Y., Chan C.S. :Efficient Certificateless Aggregate Signature Scheme,Journal of electronic science and technology, vol. 10, no. 3, september pp 209-214 (2012).
[23] Zhang L., Zhang F. :A New Certificateless Aggregate Signature Scheme, Comput. Commun. 32 (6) 1079–1085 (2009).
[24] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai, and W. Shu, :A certificateless signature scheme for mobile wireless cyber-physical systems, in 28th International Conference on Distributed Computing Systems Workshops, ICDCS Workshops 2008, pp. 489– 494, chn, June (2008).
[25] K..A. Shim, Security Models for Certificateless Signature Schemes Revisited, Inform. Sci. 296, 315-321 DOI 10.1016/j.ins.2014.10.055 (2015).
[26] Xiong, H., Guan, Z., Chen, Z., Li, F.: An efficient certificateless aggregate signature with constant pairing computation. Inform. Sci. 219, 225–235 (2013).
[27] Xiong, H., Wu, Q., Chen, Z.: Strong Security Enabled Certificateless Aggregate Signatures Applicable to Mobile Computation. Third International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, Japan, 92-99, DOI 10.1109/INCoS.2011.151 (2011).
[28] Zhang F. , Shen L., Wu G. :Notes on the security of certificateless aggregate signature schemes. Inform. Sci. 287, 32–37 (2014).
[29] Tu, H., He, D., Huang B.:Reattack of a Certificateless Aggregate Signature Scheme with Constant Pairing Computations. Scientific World Journal, 10 pages, (2014) DOI 10.1155/2014/343715 (2014).

[30] Cheng, L., Wen, Q., Jin , Z., Zhang, H., Zhou, L.: Cryptanalysis and improvement of a certificateless aggregate signature scheme. Inform. Sci. 295, 337-46 (2015).
[31] Horng S.J., Tzeng S.F., Huang H., Wang X., Li T., Khan M.K., An Efficient CertificatelessAggregate Signature with Conditional Privacy-Preserving for Vehicular Sensor Networks, Inform. Sci. 317, 48–66 (2015).
[32] Malhi A.K., Batra S. "An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks" Discrete Mathematics & Theoretical Computer Science. /4DMTCS, 2015, 17 (1) (2016).
[33] Kumar, P. Sharma, V. On the security of certificateless aggregate signature scheme in vehicular ad hoc networks. In Soft Computing Theories and Applications; Springer: Singapore, 2018; pp. 715–722 (2017).
[34] Kumar P, Saru K, Sharma V, Sangaiah AK, Wei J, Li X A certificateless aggregate signature scheme for healthcare wireless sensor network. Sustain Comput Inform Syst. https://doi.org/10.1016/j.suscom.2017.09.002 (2017).
[35] Lenstra, A.K., Lenstra, Jr., H.W., Lov´asz, L.: Factoring polynomials with rational coefficients. Math. Ann. 261 515–534, (1982).
[36] Lenstra, Jr., H.W.: Integer programming with a fixed number of variables. Math. Oper. Res. 8 538–548, (1983)
[37] Ajtai, M.: Generating hard instances of lattice problems. In: Proc. 28th ACM Symp. on Theory of Computing. 99–108 Available from ECCC at http://www.uni-trier.de/eccc/ (1996).
[38] Goldreich, O., Goldwasser, S., Halevi, S.: Public-key cryptosystems from lattice reduction problems. In: Advances in cryptology. Volume 1294 of Lecture Notes in Comput. Sci. Springer 112–131, (1997).
[39] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: a ring-based public key cryptosystem. In: Algorithmic number theory (ANTS). Volume 1423 of Lecture Notes in Comput. Sci. Springer 267–288, (1998).
[40] Hoffstein, J., Graham, N.A.H., Pipher, J., Silverman, J.H., Whyte, W.: NTRUSIGN: Digital signatures using the NTRU lattice. In: Proc. of CT-RSA. Volume 2612 of Lecture Notes in Comput. Sci., Springer-Verlag 122–140, (2003).

Annexure - III

Analysis of some internal hybrid nanofluid flows

A synopsis submitted in partial fulfillment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

in Srinivasa Ramanujan Department of Mathematics

School of Mathematics, Computers & Information Sciences

By

Tanya Sharma

Reg. No. CUHP18RDMATH01

under the supervision of

Prof. Rakesh Kumar

Srinivasa Ramanujan Department of Mathematics

School of Mathematics, Computers and Information Sciences

CENTRAL UNIVERSITY OF HIMACHAL PRADESH, DHARAMSHALA

District Kangra, Himachal Pradesh-176215(INDIA)

1. Introduction

In fluid mechanics, internal flow is a flow in which the fluids are confined by a surface [1]. The wall bounded flows provides an optimum configuration for heating and cooling liquids in various techniques. The prime objective of resolving any thermo-hydrodynamical problem is to enhance the efficiency, cost-effectiveness and durability of the working medium. Applications of industrial, medical and scientific significance like heat exchanger devices, locomotive cooling, food processing industries, solar power system, nuclear reactors, blood flow through arteries and biomedicine applications are possible areas for the study of hydrodynamics in confined geometries [2]. Parallel plate channel, pipes/ ducts and liquid films/rivulets are some common geometrical configurations of confined flows. The simplest example is a laminar flow through circular pipe, whereas centrifugal compressor stage is a complex configuration of internal flows. The consistent functioning of the machinery in such appliances and industrial processes generate indispensable amount of heat which can lead to device breakdowns. Certain passive techniques like nanofluids, porous inserts, roughness of constituting walls of channels/pipes enhance the thermo-hydrodynamical features of such configurations under study.

Solar power collectors, photovolatic cells etc utilize the parallel plate channel filled with nanofluids having large absorption rates [3]. The heat exchanger devices provide optimum control of energy transfer between fluids at different temperatures. From common home appliances like refrigerator, coolers, water geysers, car radiators to the industrial applications of solar collectors, aeronautics, cooling or pre-heating inlet fluid in oil/gas industries or power plants, the internal fluid flow inside heat exchanger devices exists. In the study of electronic cooling systems and microfluidic heat sinks, the microchannels set up horizontally or vertically having large aspect ratio are utilized to enhance efficiency [4, 5]. In the extrusion of polymeric melts through straight or converging dies, fluid flow between two plates is a crucial study [6]. Some bio-medical applications like peristaltic pumping, cancer treatment through targeted nanodrug delivery and fluid reabsorption in Renal tubules involve investigation of internal fluid flows. The concept of peristaltic pumping has been acknowledged to improve the transport mechanism in many industrial processes like chemical and pharmaceutical industries, corrosive fluids transport where the fluid contact with the machinery part is prohibited and sanitary fluid transport [7, 8]. In the design of filters, reverse osmosis desalination and transpirational cooling the re-absorption along the channel length is a less explored dimension in the dynamical treatment of fluids [9].

In current scenario the demand of energy is higher than the available resources so proper

heat and mass optimization is required. This requirement is fulfilled by appropriate choice of system configuration, external effects or heat transfer fluids. Nanofluids overcome the gap of insufficient features of traditional heat transport fluids like water, ethylene glycol and other oils. Choi's [10] remarkable contribution lead to the formation of nanofluids which showcase exceptional heat carrying capacity. These engineered mixtures of nano-sized particles ($\leq 100nm$) in some lesser conductive base fluid like oils, water or mixture of different types of liquids that encompassed the hurdles like agglomeration, sedimentation, pressure drop and stability as attained in micro particle fluids [11, 12]. Hybrid nanofluids are an upgradation of mono nanofluids which are trending nowadays [13]. The exclusiveness of hybrid nanofluid lies in the composition of two different variants of dispersed nanoparticles in the base fluid. Proper choice of the constituent nanoparticles enhance positive features of each other and can shield the disadvantage of other. Experimental studies lead to the exploration of hybrid nanofluid over conventional nanofluids due to their enhanced thermal properties. Use of hybrid nanomaterials consisting of CNTs in nanocatalysts, electrochemical-sensors and bio-sensors lead to the development of hybrid nanofluid in past decade [14, 15]. The choice of hybrid nanofluids over mono nanofluids has gained much interest as they possess favorable characteristics like better cooling, prolonged absorption rates and enhanced electrical efficiency making them fit for applications in solar energy storages, solar collectors and Photovoltaic thermal systems [16–18].

The effective thermo-physical properties of these colloidal mixtures like viscosity, thermal conductivity, thermal diffusivity, density, heat capacitance and electrical conductivity are important factors determining the fluids performance. Many theoretical, empirical models based on the nanoparticle concentration, temperature and type of the base fluids highlight the thermo-physical properties of nanofluids [19–21]. Temperature differences inside the system is one significant feature that can alter the viscosity and thermal conductivity substantially. The reduction in viscosity due to temperature increase across the momentum boundary layer leads to the increase in the transport phenomena due to which the heat transfer rate at the wall is also affected. In lubricating fluids, the heat generated by internal friction and corresponding rise in the temperature affects the viscosity of the fluid and it no longer remains constant. Whereas the thermal conductivity is an intrinsic property of fluid related to the temperature [22–24]. Consideration of such features can help accurately predict the flow and heat transfer rates.

In order to achieve enhanced thermal performances of fluid saturated channels, insertion of porous materials have been acknowledged by the researchers [25, 26]. The geometry of the porous medium is such that the fluid and solid contact increases due to the irregular motion of

the fluid travelling through it, resulting in high thermal performance. The porous materials are vastly utilized for insulation, filtration, drying processes or in petroleum industry [27, 28]. Surface roughness or wavyness of a confining channels also add up to the induction in heat transfer performance of a fluid adhering wall with emergence of slip boundary conditions [29, 30]. To control the bidirectional flow, thermal energy production in reactors, fabrication processes and to gain good rate of streams electro and magnetohydrodyamic pumps and actuators are put in use. Magnetohydrodynamics plays an important role in the boundary layer control and stability of nanoparticles. Riga plates are a kind of electromagnetic actuator generate electric and magnetic fields which result in a controlling Lorentz force parallel to the wall [31, 32]. These forces push and control fluid streams in micro pumps, nano drug delivery, and biomedicine applications.

The bulk flow of fluids past adjoining heated or cooled surfaces result in convective heat transfer [33]. The differential wall heating set up and acting buoyancy forces on the flow gives rise to a mixed convection heat transfer. The non-linear density variations due to the larger temperature differences between the rigid boundaries and the fluid produce non-linear convective heating [34]. The study of the fluid under the influence of acting or opposing buoyancy leads to many important revelations. In this scenario, the study and control over the flow reversal become important to maintain a efficient heat removal from the constituting plates [35]. Instability in a system can arise due to many possible reasons, flow instability and solution instability due to existence of multiple solutions. Hydrodynamic stability plays a major role in the determination of the flow transitions from laminar to turbulent [36], whereas solution stability analysis help determine the most stable (physically reliable) solution for the fluid flow [37]. The stability can be determined precisely in terms of the decay of the disturbances supplied to the system over a period of time [38]. This type of analysis help determine the best possible outcomes for a study under consideration.

2. Significance and novelty of the work

The proposed work on internal flows will find its general relevance in solar power systems, refrigeration, heat exchanger devices, electronic cooling devices, polymeric processes. In bio-medical field, targeted nano drug delivery will be the applicable area for the treatment of cancer related diseases. With the use of nanofluids, the volume of heat exchanger devices can be significantly reduce for better management and conversion of energy [39]. Pressure driven forces due to the peristaltic motion of channels has vast applications in bio-medical supplies to the blood flows in arteries [40]. In optimal cooling techniques like heat sink devices, nanofluids has controlling effects on the head losses and pumping power [41]. Linear stability analysis plays a crucial role

in analyzing the possible regions of a stable flow inside channels with convective and newtonian heating [42].

As far as novelty of the work is concerned, no work has been reported in literature till date where rigorous and detailed analysis for the internal flow of hybrid nanofluid flows has been performed. The internal flow under influence of different parameters emerging from porous media, viscosity and thermal conductivity, riga plate and magnetic field effects, and other conditions existing on the surface, still require a special attention of the researchers if hybrid nanofluids are chosen as a medium to transport or store the energy. This study will fill the gap in literature by providing different measuring and analysing techniques for the optimum movement of the heat and other flow patterns for the betterment of engineering and technology. This target will be materialized by utilizing different variants of hybrid nanoparticles.

3. Motivation of the study

The wide range of industrial, engineering, biomedical and environmental applications of internal flows has been the main motivational force in proposing and deciding the present work. Since hybrid nanofluids has emerged as a leading heat transport or storage carrier in several processes of significance, therefore, it will be interesting and important to enquire the flow and temperature field variations under the influence of porous media characteristics, magnetic field, variable nature of viscosity and thermal conductivity, riga plate characteristics, heating devices and different surface conditions.

4. Objectives

The prime objective of the thesis is to understand the internal but laminar flow characteristics of hybrid nanofluids,to analyse the fully developed flows, to calculate the losses associated with the channel flows, to measure the flow rate and velocities, to calculate heat movement rate and temperatures, to perform the stability analysis,to realize the advantages and disadvantages. The main effects to be investigated through the controlling parameters are:

- To study the effects of variable viscosity and thermal conductivity, magnetic field
- To examine the influence of homogeneous/heterogeneous porous medium
- To explore the effects of surface roughness and riga plate effects
- To analyse convective conditions and heating source/sink region
- To utilize the different flow and temperature conditions at the surface of the object

- To include other substantial parameters in the analysis if required at the later stage

5. Research methodology

To achieve the above proposed objectives, following research procedure may be adopted:

- Firstly, the physical problem is converted into a mathematical problem by utilizing the basic rules of conservation laws and different coordinate set up.
- Secondly, the mathematical model (governing equations with restrictions) is made dimensionless by the appropriate use of scaling/similarity transformations to achieve the desired continuous/discrete solutions which possess the appearing dimensionless parameters.
- Thirdly, the dimensionless set of equations along with boundary restrictions will be treated analytically/ numerically using different schemes such as the Optimal Homotopy Asymptotic method/ Runge-KuttaFehlberg shooting method/ ChebyshevPseudospectral method/ Quasilinearization method through different computationalsoftwaressuch as SCILAB/ MATLAB/ MATHEMATICA/ MAPLE.
- Further, mathematical aspects of the concerned scheme will be verified for the accuracy of solutions in terms of stability analysis, and error and convergence analysis.
- Further, effects of relevant flow parameters will be explored with the help of graphs and tableswhich will primarily possess velocity variations, temperatures variations and variations in the rate of flow and heat transfer.
- Further, the conditions and reasons will be searched which are responsible for the phenomenal change in the flow and heat transfer properties due to the parametric variations.
- Lastly, certain suggestions will be provided which will help in controlling the behaviour of the flow characteristics of the concerned phenomenon for the betterment of industrial/fluid devices and procedures.

6. Research Progress

Sr. No.	Nature of Task	
1.	Work completed	• Course work- 6 months. • Literature Review. • Learned some new numerical and analytical schemes such as finite element methods, spectral methods, homotopy perturbation methods etc. • Learned the computational coding of above methods.
2.	On-going work	• Asymmetrically heated hybrid nanofluid flow with variable viscosity and thermal conductivity. • Learning to perform the stability analysis for the problems related to thesis.
3.	Future task	• To work on the remaining objectives. • To accommodate new parameters if required at later stage.

References

[1] J. Johnston, Internal flows, in: Turbulence, Springer, 1975, pp. 109–169.

[2] S. Javed, H. M. Ali, H. Babar, M. S. Khan, M. M. Janjua, M. A. Bashir, Internal convective heat transfer of nanofluids in different flow regimes: A comprehensive review, Physica A: Statistical mechanics and its applications 538 (2020) 122783.

[3] R. W. Moss, G. Shire, P. Henshall, P. C. Eames, F. Arya, T. Hyde, Optimal passage size for solar collector microchannel and tube-on-plate absorbers, Solar Energy 153 (2017) 718–731.

[4] A. G. Fedorov, R. Viskanta, Three-dimensional conjugate heat transfer in the microchannel heat sink for electronic packaging, International Journal of Heat and Mass Transfer 43 (3) (2000) 399–415.

[5] C. Zhao, T. Lu, Analysis of microchannel heat sinks for electronics cooling, International Journal of Heat and Mass Transfer 45 (24) (2002) 4857–4869.

[6] S. T. Mohyud-Din, U. Khan, N. Ahmed, S. M. Hassan, Magnetohydrodynamic flow and heat transfer of nanofluids in stretchable convergent/divergent channels, Applied Sciences 5 (4) (2015) 1639–1664.

[7] D. Tripathi, O. A. Bég, A study on peristaltic flow of nanofluids: Application in drug delivery systems, International Journal of Heat and Mass Transfer 70 (2014) 61–70.

[8] A. Sharma, D. Tripathi, R. Sharma, A. Tiwari, Analysis of double diffusive convection in electroosmosis regulated peristaltic transport of nanofluids, Physica A: Statistical Mechanics and its Applications 535 (2019) 122148.

[9] A. Shahzad, W. Al-Kouz, W. A. Khan, Variable wall permeability effects on flow and heat transfer in a leaky channel containing water-based nanoparticles, Processes 8 (4) (2020) 427.

[10] S. Choi, J. Eastman, Enhancing thermal conductivity of fluids with nanoparticles, Vol. 66, 1995.

[11] B. C. Pak, Y. I. Cho, Hydrodynamic and heat transfer study of dispersed fluids with submicron metallic oxide particles, Experimental Heat Transfer an International Journal 11 (2) (1998) 151–170.

[12] Y. Xuan, Q. Li, Heat transfer enhancement of nanofluids, International Journal of heat and fluid flow 21 (1) (2000) 58–64.

[13] L. Yang, W. Ji, M. Mao, J.-n. Huang, An updated review on the properties, fabrication and application of hybrid-nanofluids along with their environmental effects, Journal of Cleaner Production 257 (2020) 120408.

[14] S. Jana, A. Salehi-Khojin, W.-H. Zhong, Enhancement of fluid thermal conductivity by the addition of single and hybrid nano-additives, Thermochimica acta 462 (1-2) (2007) 45–55.

[15] S. Guo, S. Dong, E. Wang, Gold/platinum hybrid nanoparticles supported on multiwalled carbon nanotube/silica coaxial nanocables: preparation and application as electrocatalysts for oxygen reduction, The Journal of Physical Chemistry C 112 (7) (2008) 2389–2393.

[16] T. R. Shah, H. M. Ali, Applications of hybrid nanofluids in solar energy, practical limitations and challenges: a critical review, Solar energy 183 (2019) 173–203.

[17] R. K. Bumataria, N. Chavda, H. Panchal, Current research aspects in mono and hybrid nanofluid based heat pipe technologies, Heliyon 5 (5) (2019) e01627.

[18] Z. Alhajaj, A. Bayomy, M. Z. Saghir, M. Rahman, Flow of nanofluid and hybrid fluid in porous channels: Experimental and numerical approach, International Journal of Thermofluids 1 (2020) 100016.

[19] M. Corcione, Empirical correlating equations for predicting the effective thermal conductivity and dynamic viscosity of nanofluids, Energy conversion and management 52 (1) (2011) 789–793.

[20] M. Saqib, I. Khan, S. Shafie, A. Qushairi, Recent advancment in thermophysical properties of nanofluids and hybrid nanofluids: An overview, City Univ. Int. J. Comput. Anal 3 (2019) 16–25.

[21] H. Xu, Q. Sun, Generalized hybrid nanofluid model with the application of fully developed mixed convection flow in a vertical microchannel, Communications in Theoretical Physics 71 (8) (2019) 903.

[22] J. Charraudeau, Influence de gradients de proprietes physiques en convection forcee—application au cas du tube, International Journal of Heat and Mass Transfer 18 (1) (1975) 87–95.

[23] M. Usman, M. Hamid, T. Zubair, R. U. Haq, W. Wang, Cu-al2o3/water hybrid nanofluid through a permeable surface in the presence of nonlinear radiation and variable thermal conductivity via lsm, International Journal of Heat and Mass Transfer 126 (2018) 1347–1356.

[24] S. Ahmad, S. Nadeem, N. Ullah, Entropy generation and temperature-dependent viscosity in the study of swcnt–mwcnt hybrid nanofluid, Applied Nanoscience 10 (12) (2020) 5107–5119.

[25] J. Eastman, Novel thermal properties of nanostructured materials., Tech. rep., Argonne National Lab., IL (US) (1999).

[26] R. Kumar, R. Kumar, T. Sharma, M. Sheikholeslami, Mathematical modeling of stagnation region nanofluid flow through darcy–forchheimer space taking into account inconsistent heat source/sink, Journal of Applied Mathematics and Computing (2020) 1–22.

[27] A. Shenoy, Non-newtonian fluid heat transfer in porous media, in: Advances in Heat transfer, Vol. 24, Elsevier, 1994, pp. 101–190.

[28] H. Liu, J. Wang, Y. Xie, D. Ma, X. Shi, Flow characteristics of heavy oil through porous media, Energy Sources, Part A: Recovery, Utilization, and Environmental Effects 34 (4) (2011) 347–359.

[29] M. S. Yoon, J. M. Hyun, J. S. Park, Flow and heat transfer over a rotating disk with surface roughness, International journal of heat and fluid flow 28 (2) (2007) 262–267.

[30] M. Uddin, W. Khan, S. Qureshi, O. A. Bég, Bioconvection nanofluid slip flow past a wavy surface with applications in nano-biofuel cells, Chinese Journal of Physics 55 (5) (2017) 2048–2063.

[31] M. Farooq, Z. Mansoor, M. I. Khan, T. Hayat, A. Anjum, N. Mir, Thermally stratified squeezed flow between two vertical riga plates with no slip conditions, The European Physical Journal Plus 133 (4) (2018) 152.

[32] T. Thumma, V. M. Magagula, Transient electromagnetohydrodynamic radiative squeezing flow between two parallel riga plates using a spectral local linearization approach, Heat Transfer—Asian Research 49 (1) (2020) 67–85.

[33] D. Nield, A. Bejan, Convection in porous media. (1999).

[34] J. Mackolil, B. Mahanthesh, Time-dependent nonlinear convective flow and radiative heat transfer of $cual_2o_3 - h_2o$ hybrid nanoliquid with polar particles suspension: a statistical and exact analysis, BioNanoScience 9 (4) (2019) 937–951.

[35] F. G. Al-Amri, Analytical solution for fully developed flows of nanofluids in mixed-convection zone within vertical channels, Arabian Journal for Science and Engineering 44 (2) (2019) 739–752.

[36] A. K. Sharma, P. Bera, Linear stability of mixed convection in a differentially heated vertical channel filled with high permeable porous-medium, International Journal of Thermal Sciences 134 (2018) 622–638.

[37] R. Kumar, T. Sharma, R. Kumar, M. Sheikholeslami, K. Vajravelu, Stability analysis of multiple solutions in case of a stretched nanofluid flow obeying corcione's correlation: An extended darcy model, ZAMM-Journal of Applied Mathematics and Mechanics/Zeitschrift für Angewandte Mathematik und Mechanik (2020) e202000172.

[38] J. Merkin, On dual solutions occurring in mixed convection in a porous medium, Journal of engineering Mathematics 20 (2) (1986) 171–179.

[39] A. H. Pordanjani, S. Aghakhani, M. Afrand, B. Mahmoudi, O. Mahian, S. Wongwises, An updated review on application of nanofluids in heat exchangers for saving energy, Energy Conversion and Management 198 (2019) 111886.

[40] R. Ellahi, A. Zeeshan, F. Hussain, A. Asadollahi, Peristaltic blood flow of couple stress fluid suspended with nanoparticles under the influence of chemical reaction and activation energy, Symmetry 11 (2) (2019) 276.

[41] A. Shalchi-Tabrizi, H. R. Seyf, Analysis of entropy generation and convective heat transfer of al2o3 nanofluid flow in a tangential micro heat sink, International Journal of Heat and Mass Transfer 55 (15-16) (2012) 4366–4375.

[42] B. Shankar, J. Kumar, I. Shivakumara, Magnetohydrodynamic instability of mixed convection in a differentially heated vertical channel, The European Physical Journal Plus 134 (2) (2019) 53.

Annexure - 4

Some analytical and numerical methods for solutions to fractional differential equations

A synopsis submitted for the partial fulfillment of the degree of

DOCTOR OF PHILOSOPHY

in the Department of Mathematics,

School of Mathematics, Computers & Information Sciences

by

Reena Koundal

(Reg. No. CUHP15RDMATH03)

under the supervision

of

Dr. Rakesh Kumar

Department of Mathematics

School of Mathematics, Computers & Information Sciences

Central University of Himachal Pradesh, Dharamshala

District Kangra, Himachal Pradesh-176215 (INDIA).

1. Introduction

Fractional differential equations appeared in literature as a generalization to integer order differential equations and are known to model any phenomena more accurately than integer order differential equations. These equations have deep and insightful applications in various industrial, scientific and engineering fields. Recently, several applications of these equations have been explored to understand various phenomena such as anomalous diffusion in transport dynamics ([1]-[2]), flow through porous media [3], long time memory in financial market [4], viscoelastic behaviour [5] and dielectric relaxation in polymeric materials [6] and many more.

Fractional calculus plays an important role in the structure/construction of fractional differential equations. The idea of fractional calculus came into existence through the letter of Leibnitz to L'Hospital in 1695 in which a question ("can the derivatives with integer order be extended to derivative with non-integer order?") was raised. Formal foundation of fractional calculus was built by famous mathematicians such as Liouville, Riemann, Grünwald, Lagrange, Euler etc. The contribution of these mathematicians made fractional calculus a branch of mathematics which investigates the properties of non-integer ordered derivatives and integrals (also called as differintegrals). The applications of fractional calculus in physical sciences can be seen in Hilfer [7].

In the past fractional calculus was considered a branch of pure mathematics only, but recently it has become popular among applied mathematicians and researchers/scientists of other scientific fields due to the quality applications of fractional calculus in signal processing, optics, rheology, fluid flow, electrical networks, viscoelasticity etc. The most common definitions of fractional calculus are due to Riemann-Liouville, Caputo, Grünwald-Letnikov. Some other pertinent definitions have been explored by Miller-Ross, Abdeljawad, Riesz, Hilfer and Hadamard.

In the present time, analysis of fractional differential equations (ordinary/partial) have been the concern of several pure and applied mathematicians owing to their role in the mathematical modeling of various phenomena. The detailed literature on the various aspects of fractional differential equations can be accessed from some remarkable books such as [8]-[13]. These books also present the interconnection between fractional differential equations and classical differential equations. Since most of the definitions in fractional calculus are not equivalent to each other, therefore instead of natural similarities there also exists important differences. For example , fractional order derivative of a periodic function (non-constant) will not produce a periodic function whereas this is not the case for integer order derivative [14]. Thus, we infer that integer-ordered dynamical systems cannot be generalized to dynamical systems of fractional order.

Some fractional differential equations are already available in literature which model various real world phenomena with enhanced accuracy. Burger's equations [15] explain fluid dynamics and describes the structure of shock waves. Quantum mechanical systems are analysed through space-time fractional Schrödinger equation in quantum mechanics [16]. The movement of rigid pendula, dislocations in crystals and Josephson function are studied in the analysis of Klein-Gordon fractional differential equations [17]. Anomalous diffusion processes in blood flow can be understood utilizing fractional telegraph equations [18]. Fractional Kdv equation [19] explains plasma physics, ion-acoustic waves, lattice dynamics and magnetic waves etc. Coupled fractional Boussinesq Burger equations investigate the propagation of shallow water waves [20].

The inherent nonlinearities in above mentioned fractional differential equations motivated the researchers to look for analytical approximate techniques to obtain the solution in the absence of known exact solution techniques. Thus several methods

were developed such as homotopy perturbation method, homotopy analysis method, variational iteration method, adomain decomposition method, differential transform method etc. But there is still a need to construct improved/modified methods in order to enhance the accuracy and reduce the storage space.

The modeling of various phenomena in terms of well posed fractional differential equations have also encouraged scientists to discuss the necessary and sufficient conditions for the existence and uniqueness of solutions. In present time, convergence of analytical and numerical schemes for fractional differential equations is also at the prime focus of mathematicians. Existence and uniqueness of solutions for finite difference equations was verified by Goodrich [21] under nonlocal conditions. The stability analysis for fractional delay differential equations was presented by Kaslik and Sivasundaram [14].

Some famous and basic definitions of fractional calculus which shall be used during the research work are described as follows:

Definition 1.1. A real function $f(t), t > 0$ is said to be in the space C_μ, $\mu \in \mathbb{R}$ if there exists a real number $p > \mu$, such that $f(t) = t^p f_1(t)$ where $f_1(t) \in C(0,\infty)$ and it is said to be in the space C_μ^n if and only if $f^n \in C_\mu$, $n \in N$ [10]- [12].

Definition 1.2. Let $f(t) \in C_\mu$, $\mu \geqslant -1$, then Riemann-Liouville fractional integral of order $\alpha \geqslant 0$, of a function $f(t)$ is defined as

$$ {}_{RL}J^\alpha f(t) = \begin{cases} \frac{1}{\Gamma(\alpha)} \int_0^t (t-\tau)^{\alpha-1} f(\tau) d\tau, & \alpha > 0, \ t > 0, \\ f(t), & \alpha = 0. \end{cases} $$

Definition 1.3. If $f(t) \in C_\mu$, $\mu \geqslant -1$. Then

$$ {}_{RL}D^\alpha f(t) = \begin{cases} \frac{1}{\Gamma(\alpha)} \frac{d^n}{dt^n} \int_0^t (t-\tau)^{n-\alpha+1} f(\tau) d\tau, & \alpha > 0, \ t > 0, \\ f(t), & \alpha = 0. \end{cases} $$

is called as Riemann-Liouville fractional derivative of order α.

Some basic properties of ${}_{RL}J^\alpha$ and ${}_{RL}D^\alpha$ are mentioned below for $f \in C_\mu$, $\mu \geq -1$, $\alpha, \beta \geq 0$ and $\gamma \geq 1$:

i) $J^\alpha J^\beta f(t) = J^{\alpha+\beta} f(t)$, *ii)* $J^\alpha J^\beta f(t) = J^\beta J^\alpha f(t)$, *iii)* $J^\alpha t^\gamma = \frac{\Gamma(\gamma+1)}{\Gamma(\alpha+\gamma+1)} t^{\alpha+\gamma}$,

v) $D^p J^p f(t) = f(t)$, *v)* $J^p D^p f(t) = f(t) - \Sigma_{i=0}^{n-1} f^i(0^+) \frac{t^i}{i!}$.

Definition 1.4. Let $f \in C_{-1}^n$, $n \in N \cup \{0\}$, then Caputo fractional derivative of f of order $\alpha \geqslant 0$ is defined as:

$$ {}_cD_*^\alpha f(t) = \begin{cases} [I^{n-\alpha} f^n(t)], & n-1 < \alpha \leq n, \ n \in N, \\ \frac{\partial^n}{\partial t^n} f(t), & \alpha = n. \end{cases} $$

The derivative of constant by Caputo fractional derivative can be defined as:

$$ {}_cD_*^\alpha K = 0, \ K \text{ is constant,} $$

Definition 1.5. Let $f(x,t) \in c_\mu^n$, then partial fractional Caputo derivative of order $\alpha > 0$ is defined as:

$$ {}_cD^{\alpha} f(x,t) = \frac{\partial^{\alpha} f(x,t)}{\partial t^{\alpha}} = \begin{cases} \dfrac{1}{\Gamma(n-\alpha)} \displaystyle\int_0^t (t-\tau)^{\alpha-1} \frac{\partial^n f(x,t)}{\partial t^n} d\tau, & \text{if } n-1 < \alpha < n, \\ \dfrac{\partial^n f(x,t)}{\partial t^n}, & \text{if } \alpha = n \in N. \end{cases} $$

Definition 1.6. Let $f : [1,\infty) \to \mathbb{R}$, then Hadamard fractional integral of order α is defined as [22], [23]:

$$ {}_HJ^{\alpha} f(t) = \frac{1}{\Gamma(\alpha)} \int_1^t \left(\log \frac{t}{x}\right)^{\alpha-1} \frac{f(x)}{x} dx, \quad \alpha > 0 $$

Definition 1.7. Let a continuous function $f : [1,\infty) \to \mathbb{R}$ and $\alpha > 0$ [22], [23]. Then

$$ {}_HD^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \left(t\frac{d}{dt}\right)^n \int_1^t \left(\log \frac{t}{x}\right)^{n-\alpha-1} \frac{f(x)}{x} dx, \quad n-1 < \alpha < n, \quad n = [\alpha]+1 $$

is called as Hadamard fractional derivative of order α.

Definition 1.8. The fractional integral of order α is defined, for a function $f(z)$, by [24]

$$ J_z^{\alpha} f(z) = \frac{1}{\Gamma(\alpha)} \int_0^z f(\xi)(z-\xi)^{\alpha-1} d\xi, \quad \alpha > 0 $$

where the function $f(z)$ is analytic in simply connected region of the complex z-plane $\mathbb{C}$ containing the origin, and the multiplicity of $(z-\xi)^{-\alpha}$ is removed by requiring $\log(z-\xi)$ to be real when $(z-\xi) > 0$.

Definition 1.9. For a function $f(z)$, the fractional derivative of order α is defined as [24]

$$ D_z^{\alpha} f(z) = \frac{1}{\Gamma(1-\alpha)} \frac{d}{dz} \int_0^z \frac{f(\xi)}{(z-\xi)^{\alpha}} d\xi, \quad 0 \leqslant \alpha < 1, $$

where the function $f(z)$ is analytic in simply connected region of the complex z-plane $\mathbb{C}$ containing the origin, and the multiplicity of $(z-\xi)^{-\alpha}$ is removed by requiring $\log(z-\xi)$ to be real when $(z-\xi) > 0$.

For $\alpha > 0$, $\delta > -1$, some properties of complex fractional definitions are described in following foam [24]

$$ i) \quad D_z^{\alpha} z^{\delta} = \frac{\Gamma(\delta+1)}{\Gamma(\mu-\alpha+1)} z^{\mu-\alpha}, \quad 0 < \alpha < 1, $$

$$ ii) \quad J_z^{\alpha} z^{\delta} = \frac{\delta+1}{\Gamma(\delta+\alpha+1)}, \quad \alpha > 0. $$

Definition 1.10. Let $f : [0,\infty) \to \mathbb{R}$, then the conformable fractional derivative of f of order α is defined as [25] :

$$ T_{\alpha}(f)(t) = \lim_{\varepsilon \to 0} \frac{f(t+\varepsilon t^{1-\alpha}) - f(t)}{\varepsilon} \quad \text{for all } t > 0, \quad \alpha \in (0,1) $$

If f is α - differentiable in some $(0,a)$, $a > 0$, and $\lim_{t \to 0^+} f^{\alpha}(t)$ exists, then we define

$$ f^{\alpha}(0) = \lim_{t \to 0^+} f^{\alpha}(t) $$

According to conformable fractional definition, fractional derivative of polynomial is defined as

$$ T_{\alpha}(t^r) = r t^{r-\alpha}, \quad \text{for all } r \in \mathbb{R} $$

The Mittag-Leffler function of two parameter is defined as [12]

$$E_{\alpha,\beta}(x) = \sum_{k=0}^{\infty} \frac{x^k}{\Gamma(\alpha k + \beta)}, \quad Re(\alpha) > 0, \quad Re(\beta) > 0.$$

It reduces to a classical exponential function in case of one parameter.

The above literature review has motivated us to design unique analytical and numerical schemes for the treatment of fractional differential equations which provides excellent accuracy and are easy to implement. The existence and uniqueness of solutions and stability conditions are also source of inspiration to verify the well posedness of fractional differential equations and analytical /numerical schemes for their solution.

2. Significance

The exact and approximate solutions to fractional differential equations will help in the understanding of the phenomenon in a better way. Algorithms and computational analysis in this work will provide unique, compact and alternate procedures to obtain the accurate solutions. The existence and uniqueness of such solutions will contribute in identifying the phenomenon presented by mathematical models using fractional calculus.

3. Objectives

In this thesis, we focus ourselves in the understanding of different types of fractional differential equations which are necessary to analyse any particular phenomenon. The main objectives of the present study are:

- To develop analytical algorithms for the solutions of fractional differential equations such as least square homotopy perturbation method, rational least square homotopy perturbation method etc.
- To construct some properties of Lucas polynomial, shifted Lucas polynomial and fractional shifted Lucas polynomial.
- To define Lucas polynomial based wavelets and its properties and operational matrices related to Lucas polynomial and concerned wavelets.
- To design some numerical algorithms for the solution of fractional differential/integral equations utilizing Lucas polynomials and concerned wavelets.
- To include the classical ideas of least square approach, collocation method, tau method, Galerkin method etc. in the construction of numerical schemes.
- To perform the error analysis, and ensure the stability and convergence of the developed schemes.

4. Methodology

- The fractional differential equations (ordinary/partial) with initial and boundary conditions will be considered in the beginning.

- Then definitions which are required for the analysis will be borrowed from literature.
- New definitions which are necessary for the foundation of a analytical/numerical method will be defined.
- After that, mathematical theory of the method (under construction) will be developed through theorems, lemmas, corollaries for some problems.
- The stability and convergence conditions will also be obtained.
- Lastly, the achieved solutions/errors will be presented in the forms of graph and tables.

References

[1] B. Henry, S. Wearne. Existence of turing instabilities in a two-species fractional reaction-diffusion system, SIAM Journal on Applied Mathematics 62 (2002) 870-887.

[2] R. Metzler, J. Klafter. The random walk's guide to anomalous diffusion: a fractional dynamics approach, Physics Reports 339 (2000) 1-77.

[3] R. Schumer, D. Benson, M. M. Meerschaert, S. W. Wheatcraft. Eulerian derivation of the fractional advection-dispersion equation, Journal of Contaminant Hydrology 48 (2001) 69-88.

[4] S. Picozzi, B. J. West. Fractional langevin model of memory in financial markets, Physical Review E 66 (2002) 46-118.

[5] N. Heymans, J. C. Bauwens. Fractal rheological models and fractional differential equations for viscoelastic behavior, Rheologica Acta 33 (1994) 210-219.

[6] E. Reyes-Melo, J. Martinez-Vega, C. Guerrero-Salazar, U. Ortiz-Mendez. Application of fractional calculus to the modeling of dielectric relaxation phenomena in polymeric materials, Journal of Applied Polymer Science 98 (2005) 923-935.

[7] R. Hilfer. Applications of fractional calculus in physics, World Scientific. Publishing Company, Singapore London (2000).

[8] B. Ross. A brief history and exposition of the fundamental theory of fractional calculus, Fractional Calculus and its Applications, Springer Lecture Notes in Mathematics, volume 57, 1975, pp. 1-36.

[9] B. Ross. The development of fractional calculus, Historia Mathematica, 4 (1977), 75-89.

[10] K. Miller, B. Ross. An application to the fractional calculus and fractional differential equations. Wiley, Newyork, 1993.

[11] A. A. Kilbas, H. M. Srivastava, J. J. Trujillo. Theory and application of fractional differential equation. Elesvier: Amsterdam, (2006).

[12] I. Podlubny, Fractional Differential Equations, Academic Press, San Diego, CA, 1999.

[13] V. Lakshmikantham, S. Leela, J. V. Devi. Theory of fractional dynamic systems, Cambridge Scientific Publishers, 2009.

[14] E. Kaslika, S. Sivasundaram. Non-existence of periodic solutions in fractional-order dynamical systems and a remarkable difference between integer and fractional-order derivatives of periodic functions, Nonlinear Analysis: Real World Applications 13(2012) 1489-1497.

[15] J. Singh, D. Kumar, R. Swroop. Numerical solution of time- and space-fractional coupled Burgers' equations via homotopy algorithm , Alexandria Engineering Journal 55 (2016) 1753–1763.

[16] J. Dong, M. Xu. Space–time fractional Schrödinger equation with time-independent potentials, Journal of Mathematical Analysis and Applications 344 (2008) 1005-1017.

[17] A. K. Golmankhaneh, A. K. Golmankhaneh, D. Baleanu. On nonlinear fractional Klein-Gordon equation, Signal Processing 91 (2011) 446-451.

[18] R. C. Cascaval, E. C. Eckstein, C. L. Frota, J. A. Goldstein. Fractional telegraph equations, Journal of Mathematical Analysis and Applications 276 (2002) 145-159.

[19] S. A. El-Wakil, E. M. Abulwafa, M. A. Zahran, A. A. Mahmoud. Time-fractional Kdv equation: formulation and solution using variational methods, Nonlinear Dynamics 65 (2011) 55-63.

[20] S. Kumar, A. Kumar, D. Baleanu. Two analytical methods for time-fractional nonlinear coupled Boussinesq-Burger's equations arise in propagation of shallow water waves, Nonlinear Dynamics 85 (2016) 699-715.

[21] C. S. Goodrich. Existence and uniqueness of solutions to a fractional difference equation with nonlocal conditions, Computers & Mathematics with Applications 61 (2011) 191-202.

[22] F. Jarad, T. Abdeljawad, D. Baleanu. Caputo-type modification of the Hadamard fractional derivatives, Advances in Difference Equations 142 (2012) 8 pages.

[23] P. Thiramanus, S. K. Ntouyas, J. Tariboon. Existence and uniqueness results for Hadamard-type fractional differential equations with nonlocal fractional integral boundary conditions, Abstract and Applied Analysis Volume 2014, Article ID 902054, 9 pages .

[24] H. M. Srivastava, S. Owa. Univalent functions, fractional calculus and their applications, Ellis Horwood series: Mathematics and its Applications, Ellis Horwood, Chichester, UK, 1989.

[25] R. Khalil, M. Al Horani, A. Yousef, M. Sababheh. A new definition of fractional derivative, Journal of Computational and Applied Mathematics 264 (2014) 65-70.

CENTRAL UNIVERSITY OF HIMACHAL PRADESH
[ESTABLISHED UNDER THE CENTRAL UNIVERSITIES ACT 2009]
PO BOX: 21, DHARAMSHALA, DISTRICT KANGRA - 176215 (HP)
www.cuhimachal.ac.in
School of Mathematics, Computers & Information Sciences
Srinivasa Ramanujan Department of Mathematics

Research Progress Report in respect of RAC (Research Advisory Committee) meeting held on 29.04.2021 for the period July 2020 to December 2020

Programme of study: Ph.D.

Name: Reena Koundal

Roll No./ Registration No.: CUHP15RDMATH03

Department: Srinivasa Ramanujan Department of Mathematics

1. **Conferences/Workshops/Schools:**

- Participated in one day international webinar on **"Modern Trends in Mathematics and its Applications 21st August 2020"**, at Krishnagar Government College Department of Mathematics.
- Participated in two days international workshop on **"Geometry of Continued Fractions: Ramanujan and his successors 14th September-15th September 2020"**, at Central University of Himachal Pradesh.
- Participated in the five days online short term course on **"Numerical Solutions of Differential Equations16th September-20th September 2020"**, at Dr. B. R. Ambedkar National Institute of Technology Jalandhar.
- Participated in three days international conference as listener on **"The First Online Conference on Modern Fractional Calculus and its Applications 4th December-6th December 2020"**, at Biruni University, Istanbul, Turkey.
- Participated in one day international workshop on **"Srinivasa Ramanujan: The Man Beyond infinity 22nd December 2020"**, at Central University of Himachal Pradesh.

2. **Paper Published**

- Rakesh Kumar, Reena Koundal, K. Srivastava, D. Baleanu. Normalized Lucas wavelets: an application to Lane–Emden and pantograph differential equations. The European Physical Journal Plus (2020) 135:881.

3. **Work Done / Work Ongoing:**

At present time, I am working on **"Operational matrix of fractional shifted Lucas polynomials for fractional multi-order/multi-term differential equations".**

- Under this work, novel type of fractional polynomials is proposed as the generalization to shifted Lucas polynomials, which are called as fractional shifted Lucas polynomials.

- Useful operational matrices are developed utilizing the newly established analytical formula for the construction of the numerical scheme.
- Further, a theorem for the calculation of Caputo fractional derivative is proved and a useful remark is provided for integer order derivative.
- To develop the strong background of suggested scheme, error analysis is performed.
- The algorithm of the scheme examined through some test examples of multi-order/multi-term differential equations.

4. **To propose and approve the updated objectives for the thesis:**

The following are the updated objectives for the thesis title "**Some analytical and numerical methods for solutions to fractional differential equations**":

- To develop analytical algorithms for the solutions of fractional differential equations such as least square homotopy perturbation method, rational least square homotopy perturbation method etc.
- To construct some properties of Lucas polynomial, shifted Lucas polynomial and fractional shifted Lucas polynomial.
- To define Lucas polynomial based wavelets and its properties and operational matrices related to Lucas polynomial and concerned wavelets.
- To design some numerical algorithms for the solution of fractional differential/integral equations utilizing Lucas polynomials and concerned wavelets.
- To include the classical ideas of least square approach, collocation method, tau method, Galerkin method etc. in the construction of numerical schemes.
- To perform the error analysis, and ensure the stability and convergence of the developed schemes.

Signature of Student

CENTRAL UNIVERSITY OF HIMACHAL PRADESH
[ESTABLISHED UNDER THE CENTRAL UNIVERSITIES ACT 2009]
PO BOX: 21, DHARAMSHALA, DISTRICT KANGRA - 176215 (HP)
www.cuhimachal.ac.in
School of Mathematics, Computers & Information Sciences
Srinivasa Ramanujan Department of Mathematics

Dr. Meenakshi
RAC Coordinator)

Members of Research Advisory Committee (RAC)

Prof. Rakesh Kumar	Dr. S.K. Srivastava	Prof. Rakesh Kumar
(Supervisor)	(Subject Expert)	(Head of Department)

29.04.2021

ethics and review of published research in the relevant field, training, field work, etc. Other courses shall be advanced level courses preparing the students for PhD degree.

7.3 All courses prescribed for PhD course work shall be in conformity with the credit hour instructional requirement of CUHP and shall specify content, instructional and assessment methods duly approved by the Board of Studies.

7.4 The Department where the scholar pursues his/ her research shall prescribe the course(s) to him/her based on the recommendations of the Research Advisory Committee, as stipulated under sub-Clause 8.1.

7.5 All candidates admitted to PhD programmes shall be required to complete the course work prescribed by the Department within one semester, but cannot extend beyond two semesters in any case.

7.6 Candidates already holding MPhil degree and admitted to the PhD programme, or those who have already completed the course work in MPhil may be exempted by the Department from the PhD course work. All other candidates admitted to the PhD programme shall be required to complete the PhD course work prescribed by the Department.

7.7 Grades in the course work, including research methodology courses shall be finalized by the Department and the final grades shall be communicated to the Controller of Exams (CoE) who will notify the result.

7.8 A PhD scholar has to obtain a minimum of 55% marks or its equivalent grade as per CUHP in the course work in order to be eligible to continue the programme and write the thesis eventually.

8. Submission of Synopsis:

8.1 A PhD scholar shall have to prepare a synopsis in consultation with his/ her supervisor on her/his topic of research. S/he shall have to submit it to the concerned Centre/ Department and defend it before Research Advisory Committee (RAC) within three semesters, or one and a half year. The synopsis has to be approved by the Board of Studies (BoS) and the School Board of the concerned Department/Centre and School respectively.

8.2 A PhD scholar shall get one chance to request for modifications in any part of his/her synopsis to her/his supervisor six months prior to the actual submission of the thesis. On the recommendation of the concerned supervisor, the PhD student shall have to defend the modifications in synopsis before her/his RAC. Modifications in the synopsis have to be approved by the BoS and School Board of the concerned Centre/ Department/School before the thesis is submitted for evaluation.

9. Monitoring of Research Work by the Research Advisory Committee (RAC)

For monitoring research work, there shall be a Research Advisory Committee (RAC) for each PhD scholar.

9.1 The Research Advisory Committee (RAC) shall comprise the research supervisor of the PhD student who shall be the convener of the committee, Head of the Department / Director of the Centre who shall be the *ex-officio* chairman, and at least one subject expert nominated by the Head/Director upon the recommendation of the concerned supervisor.

This Committee shall have the following responsibilities:

Detailed List of Experts/Examiners for Srinivasa Ramanujan Department of Mathematics

1. Prof. P.L Sharma, Chairman, Department of Mathematics & Statistics, Himachal Pradesh University, E-mail: chairmanmath@hpuniv.ac.in, Mob No : 9418003066.
2. Prof. Rajesh Kumar Sharma, Department of Mathematics & Statistics, , Himachal Pradesh University, E-mail: rajesh_hpu_math[at]yahoo.co.in, Phone No. 0177-2833771.
3. Dr. Vijayata Pathania, Assistant Professor, Department of Mathematics, HPU Regional Centre, Dharamshala E-mail: vijayatapathania@yahoo.com, Mob.No. 9816225470.
4. Prof. Gauree Shanker, Department of Mathematics and Statistics, School of Basic and Applied Sciences, Central University of Punjab, Bathinda- 151001, Email Id: gauree.shanker@cup.edu.in; hod.ms@cup.edu.in; grshnkr2007@gmail.com, Mobile: +91-9785007650.
5. Prof. Vikas Bisht, Department of Mathematics, Panjab University, Chanidgarh Email vikasb@pu.ac.in , Mobile: 9872616693.
6. Dr. Muslim Malik, Associate Professor, Department of Mathematics, School of Basic Sciences, IIT Mandi, Email- muslim@iitmandi.ac.in.
7. Dr. Praveen Kumar, Assistant Professor, Department of Mathematics, Ramjas College, Delhi University, Email: iit.gautam@gmail.com, Mobile No. 9910708929.
8. Dr. Saru Kumari, Assistant Professor, Department of Mathematics, Chaudhary Charan Singh University, Meerut, Email. com saryusiirohi@gmail.com, Mobile No. 9457024729.
9. Dr. Shah jahan, Assistant Professor, Department of Mathematics, Central University of Haryana, Haryana, Email: Shahjahan@cuh.ac.in, Mobile No. 8285717090.
10. Dr. Asif Khan, Assistant Professor, Department of Mathematics , Aligarh Muslim University, Aligarh, Email: asifjnu07@gmail.com, Mobile No.8267817812.
11. Prof. R. P. Sharma, Department of Mathematics & Statistics, Himachal Pradesh University, Shimla - 171005, Email: rp_math_hpu@yahoo.com.
12. Dr. Tilak Raj Sharma, Assistant Professor, Department of Mathematics, Regional Centre, Dharamshala, Himachal Pradesh-176218, Email: trpangotra@gmail.com, Mob: 9418103801
13. Dr. Vikram Singh Kapil, Associate Professor, Department of Mathematics, Govt. Degree College Baldwara (Mandi), Himachal Pradesh-175033, Email: vikramkapil16@gmail.com, Mob: 7018260561
14. Dr. R. K. Vats, Associate Professor, Department of Mathematics & Scientific Computing, NIT Hamirpur, Himachal Pradesh-177005, Email: rkvats@nith.ac.in, Mob: 8219995020
15. Dr. Om Prakash Yadav, Assistant Professor, Department of Mathematics & Scientific Computing, NIT Hamirpur, Himachal Pradesh-177005, Email: opyadav@nith.ac.in, Mob: 9410150156
16. Dr. Anil Kumar Vashisth, Professor, Department of Mathematics, Kurukshetra University, Kurukshetra, Haryana, E-Mail: akvashishth@kuk.ac.in
17. Dr. Joginder Singh Dhiman, Professor, Department of Mathematics and Statistics, HP University Shimla-5, E-Mail: jsdhiman66@gmail.com
18. Dr. Ravinder Singh, Assistant Professor, Department of Mathematics, Dr BR Ambedkar, NIT Jalandhar, PB. E-Mail: singhr@nitj.ac.in
19. Dr. Khem Chand, Professor, Department of Mathematics and Statistics, HP University Shimla-5, E-Mail: khemthakur99@gmail.com
20. Dr. Paras Ram, Professor, Department of Mathematics, NIT Kurukshetra, Haryana, E-Mail: parasramnitkkr@gmail.com