Ramakrishna Mission Vivekananda Educational and Research Institute

EVALUATION FORM FOR JRF/SRFs

1. Name of the JRF/SRF with designation and date of joining: SHREYA DEY, JRF ,16th August,2021

2. Topics of research for the Ph.D. thesis: Lattice based Cryptography

3. Research courses attended/Reading courses taken or any other form of training with evaluation by respective authorities on them:

Sno	Course	Score	Instructor
1	DISCRETE MATHEMATICS	80	Dr.NILANJAN DATTA
2	GRAPH THEORY AND MATROID	85	Dr.ANUPAM MONDAL, Dr.SHION SHAMADDAR CHOWDHURY
3	ALGEBRA AND IT'S APPLICATION	85	Dr.KULDEEP SAHA, Dr.APRATIM CHAKRABORTY
4	BASIC CRYPTOLOGY	83	Dr.ARPITA MAITRA, Prof.RANA BARUA
5	RESEARCH METHODOLOGY	76	Dr.NILANJAN DATTA, Prof.GOUTAM MUKHERJEE, Dr.ARPITA MAITRA, Dr.DEBOLINA GHATAK
6	ADVANCED CRYPTOGRAPHY	59	Dr.AVIJIT DUTTA, Dr.BIMAL MONDAL
7	DESIGN AND ANALYSIS OF ALGORITHMS	61	Dr.NILANJAN DATTA, Prof.RANA BARUA
8	TRENDS IN COMBINATORICS AND TOPOLOGY	58	Dr.KULDEEP SAHA, Dr.APRATIM CHAKRABORTY, Dr.ANUPAM MONDAL, Prof.GOUTAM MUKJREJEE, Dr.SAJAL MUKHERJEE

4. Seminars given with dates and titles and summaries:

[1] TOPIC: **Approximation Algorithms in Lattice**
DATE: **11th May 2022**
VENUE: **TCG CREST**

5. List of major scientific papers/books read, field/laboratory work undertaken in connection with the thesis topic:

PAPERS

[1] Don Coppersmith,
Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities
Journal of Cryptology (1997) 10: 233-260
[2] Jean-Sébastien Coron: Finding Small Roots of Bivariate Integer Polynomial Equations Revisited. EUROCRYPT 2004: 492-505

[3] Dan Boneh, Glenn Durfee, Nick Howgrave-Graham: Factoring N = p^rq, for large r . CRYPTO 1999: 326-337
[4] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman NTRU: A Ring-Based Public Key Cryptosystem. ANTS 1998: 267-288

BOOKS

[1] Steven D. Galbraith: Mathematics of Public Key Cryptography.Cambridge University Press 2012, ISBN 9781107013926
- Chapter 19: Coppersmith's Method and Related Applications

[2] Daniele Micciancio, Shafi Goldwasser: Complexity of lattice problems - a cryptograhic perspective. The Kluwer international series in engineering and computer science 671, Springer 2002, ISBN 978-0-7923-7688-0, pp. I-X, 1-220
- Chapter 2: Approximations Algorithms

[3] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman: An Introduction to Mathematical Cryptography. ISBN: 978-0-387-77993-5
- Chapter 6: Lattices and Cryptography

[4] Oded Goldreich: The Foundations of Cryptography - Volume 1: Basic Techniques. Cambridge University Press 2001, ISBN 0-521-79172-3
- Chapter 2: Computational Difficulty

[5] Oded Regev: Lattices in Computer Science. Tel-Aviv University, Fall 2004
- Lecture 1
- Lecture 2
- Lecture 3

6. Papers published/accepted for publication with full reference including coauthors (enclose reprints/preprints): N/A

7. Research/Technical reports prepared with reference including coauthors (enclose preprints):N/A

8. Teaching duties undertaken with details: N/A

9. Any other information that may be relevant: N/A

10. Brief description of work done on the thesis topic: I have successfully completed my course work. Currently, I am exploring the literature of Lattice Based Crypto with current focus on applications of LLL algorithm and designing new cryptosystems.

Place: TCG CREST, SALT LAKE, SECTOR V

Shreya Dey

Signature (JRF / SRF): Date: 20/07/2022

Specific recommendations of the Supervisor and the RFAC with a brief description of the research work on the thesis topics by the research fellow.

Signature (Supervisor) Date

Signature (Chair – RFAC) Date