Ramakrishna Mission Vivekananda Educational and Research Institute

EVALUATION FORM FOR JRF/SRFs

1. Name of the JRF/SRF with designation and date of joining: SOUGATA MANDAL, JRF, 16/08/2021

2. Topics of research for the Ph.D. thesis: Symmetric Key Cryptography

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

Sno	Course	Grade/Score	Instructor
1	Graph Theory and Matroids	63	Dr. Anupam Mondal and Dr. Shion Samadder Chaudhury
2	Advanced Symmetric Key Cryptology	65	Dr. Nilanjan Datta and Dr. Avijit Dutta
3	Stochastic Process	71	Dr. Debapratim Banerjee
	Algebra and Its Application	78	Dr. Apratim Chakraborty and Dr. Kuldeep Saha
5	Research Methodology	86	Dr. Nilanjan Datta, Dr. Arpita Maitra Dr. Debolina Ghatak, Prof. Goutam Mukherjee
6	Advanced Quantum Information and Cryptology	90	Dr. Arpita Maitra
7	Advanced Cryptology	83	Dr. Avijit Dutta and Dr. Bimal Mandal
8	Design and Analysis of Algorithms	92	Prof. Rana Barua and Dr. Nilanjan Datta

4. Seminars given with dates and titles and summaries:

Topic: **Leakage -Resilient Symmetric Key Cryptography**
date: 11/05/2022
Venue: TCG CREST

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

Book :

[1] Oded Goldreich : **Foundation of Cryptography -A Primer**
Chapter 1-4

[2] Jonathan Katz, Yehuda Lindell : **Introduction to Modern Cryptography**
Chapter 6

Research Papers

[1] Olivier Pereira, François-Xavier Standaert, Srinivas Vivek: **Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives**. CCS 2015: 96-108.

[2] Francesco Berti, François Koeune, Olivier Pereira, Thomas Peters, François-Xavier Standaert: **Leakage-Resilient and Misuse-Resistant Authenticated Encryption.** IACR Cryptol. ePrint Arch. 2016: 996 (2016).

[3] Francesco Berti, Olivier Pereira, Thomas Peters, François-Xavier Standaert: **On Leakage-Resilient Authenticated Encryption with Decryption Leakages**. IACR Trans. Symmetric Cryptol. 2017(3): 271-293 (2017).

[4] Francesco Berti, Chun Guo, Olivier Pereira, Thomas Peters, François-Xavier Standaert: **TEDT, a Leakage-Resist AEAD Mode for High Physical Security Applications**. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020(1): 256-320 (2020).

[5] Eik List: **TEDT2 - Highly Secure Leakage-Resilient TBC-Based Authenticated Encryption.** LATINCRYPT 2021: 275-295.

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 completed all the coursework assigned to me. Currently, I'm doing a literature survey on the area of Designing Leakage Resilient Symmetric Key Cryptography. I have read a few papers on this line of research such as DTE, DCE, EDT, TEDT, TEDT2, etc. I want to pursue my Ph.D. research in this direction.

Place: TCG CREST

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

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

Signature: (Supervisor) Date:

Signature: (Chair – RFAC) Date: