ARIJIT DUTTA

Room Number 3, Laxmi Niwas, IIT Market, Powai, Mumbai 400076
(+91)8879175981 ⋄ arijit.dutta67@gmail.com

PUBLICATIONS

1. **A. Dutta** and S. Vijayakumaran. Nummatus: A privacy preserving proof of reserves protocol for Quisquis. To appear in Indocrypt 2019
2. **A. Dutta** and S. Vijayakumaran. MProve: A proof of reserves protocol for Monero exchanges. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 330–339, June 2019
3. **A. Dutta** and S. Vijayakumaran. Revelio: A MimbleWimble proof of reserves protocol. In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 7–11, June 2019
4. **A. Dutta** and S. Vijayakumaran. Rewrite cost optimal rank modulation codes in s4 and s5. In *2018 Twenty Fourth National Conference on Communications (NCC)*, pages 1–6, Feb 2018
5. **A. Dutta** and A. Pramanik. Modified approximate lower triangular encoding of LDPC codes. In *2015 International Conference on Advances in Computer Engineering and Applications*, pages 364–369, March 2015

EDUCATION

Indian Institute of Technology Bombay July 2015 - Present
Doctor of Philosophy
Department of Electrical Engineering

Indian Institute of Engineering Science and Technology, Shibpur July 2013 - June 2015
Master of Engineering Overall Percentage: 81.33
Department of Electronics and Telecommunication Engineering

West Bengal University of Technology 2011
B. Tech, Electronics and Communication Engineering DGPA 8.37

West Bengal Council of Higher Secondary Education 2007
Intermediate/+2 Overall Percentage: 81

West Bengal Board of Secondary Education 2005
Matriculation Overall Percentage: 87.75

RESEARCH INTEREST

- I am currently pursuing Ph.D. under the supervision of Prof. Saravanan Vijayakumaran. The theme of my research is privacy in blockchain. We have worked on privacy preserving proof of reserves protocol for cryptocurrency exchanges where an exchange proves that it holds sufficient reserves without revealing its private information like owned accounts or the reserves amount.
- Previously worked on error correcting codes and error correcting codes for flash memories. My research interests lies mainly in broad areas of applications of discrete mathematics.