Topics of Research

Mentor: Goutam Paul

1. 17th (and more) (non)-randomness tests
   http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

2. RC4 state recovery
   http://www.isical.ac.in/~rcbose/internship/lectures2016/rt05maximov.pdf

3. RC4 key collision for keys shorter than 22 bytes
   http://www.isical.ac.in/~rcbose/internship/lectures2016/rt05matsui.pdf
   http://www.isical.ac.in/~rcbose/internship/lectures2016/rt05chenm.pdf

4. Provably secure efficient stream cipher design
   https://www.iacr.org/archive/eurocrypt2006/40040110/40040110.pdf

5. Classical/Quantum Boolean functions in property testing
   http://cjtcs.cs.uchicago.edu/articles/2010/1/cj10-01.pdf
   http://homepages.cwi.nl/~rdewolf/publ/qc/proptest_tocfinal.pdf

6. Long quantum bit commitment: design and analysis
   http://arxiv.org/pdf/1507.00239v1.pdf

7. Third party auditing of cloud data
   https://eprint.iacr.org/2012/365.pdf

8. (Non ?) Democratic mining in Bitcoins
   http://link.springer.com/chapter/10.1007%2F978-3-319-13841-1_11
   http://link.springer.com/chapter/10.1007%2F978-3-319-26961-0_10

9. Efficient GPU implementation of crypto algorithms
   https://eprint.iacr.org/2013/059.pdf
   http://link.springer.com/chapter/10.1007%2F978-3-642-38553-7_11

10. Efficient hardware design of crypto algorithms
    http://link.springer.com/chapter/10.1007%2F978-3-642-45204-8_13