Arijit Dutta

Contact Information

Kolkata,
West Bengal,
India

(+91)8879175981
arijit.dutta67@gmail.com
arijitdutta67.github.io/homepage
github.com/arijitdutta67
linkedin.com/in/arijit-dutta-14bb2138/

Research Interests

Zero-knowledge proofs, Applied cryptography, Privacy in blockchain, Security analysis, Error correcting codes

Industrial and Academic Experiences

- Cryptography Engineer at Aztec Protocol — July, 2021 - March, 2023
- Ph.D. Research Scholar at IIT Bombay — July, 2015 - August, 2021
- Assistant System Engineer at Tata consultancy Services Limited — December, 2011 - July, 2013
- Teaching Assistant at IIT Bombay for the courses
  - Error Correcting Codes (EE 605)
  - Probability and Random Processes (EE 325)
  - Information Theory and Coding (EE 708)
  - Cryptocurrency and Blockchain Technologies (EE 465)
  - An Introduction to Number Theory and Cryptography (EE 720)

Education

- Indian Institute of Technology Bombay, Mumbai, India
  Ph.D., Electrical Engineering — July, 2015 - August, 2021
  - *CPI:* 8.29/10
  - *Thesis title:* Privacy-Preserving Proof of Reserves Protocols for Cryptocurrency Exchanges
  - *Advisor:* Prof. Saravanan Vijayakumaran
- Indian Institute of Engineering Science and Technology, Shibpur, India
  Master of Engineering, Electronics and Telecommunication — July, 2013 - June, 2015
  - *Overall percentage:* 81.33
  - *Thesis title:* A Study on Encoding Techniques of LDPC Codes
  - *Advisor:* Prof. Ankita Pramanik
- Techno India Salt Lake, Kolkata, India
  B. Tech, Electronics and Communication Engineering — July, 2007 - June, 2011
  - *DGPA:* 8.37/10

Technical Skills

- **Programming Languages** : C++, Rust, Python, SAGE, LaTeX, Solidity
- **Softwares and Packages** : Visual Studio Code, MATLAB, Inkscape
- **Operating Systems** : MacOS, Linux, Windows
- **Version Control Systems** : Git, Bitbucket

Industry Projects (Aztec, selected)

- Development and Testing
  - Implemented the latest change in the PLONK paper in the code base (Spec, Merge Commit)
  - Refactored Pedersen hash
  - Added tests to detect Aztec connect circuit changes (Merge Commit)
  - Implemented inner product argument polynomial commitment scheme for Aztec 3 (Spec, PR 1, PR 2)
  - Testing work in the sumcheck module of Aztec 3 (PR 1, PR 2)
- Internal Audit
  - Pedersen hashes and Merkle trees (Spec 1, Spec 2)

- Aztec connect zk-snark circuits
- Multisig

- Security Analysis
  - Proof of collision resistance of compress function in Aztec connect (Spec)
  - Balance property of Aztec connect (Spec)

Research Projects

- MProve+, a privacy enhanced proof of reserves (PoR) protocol for Monero — Ph.D. Thesis
  Joint work with Suyash Bagad and Prof. Saravanan Vijayakumaran — EE Dept, IIT Bombay
  - Enhanced the privacy preservation of MProve using techniques of Bulletproofs and Omniring
  - Defined and proved the privacy property of the MProve+ protocol by hybrid argument
  - Investigated how the MProve+ protocol affects the privacy features of Monero
  - Implemented both MProve and MProve+ in *Rust*
- Nummatus, a PoR protocol for Quisquis — Ph.D. Thesis
  Joint work with Arnab Jana and Prof. Saravanan Vijayakumaran — CSE & EE Dept, IIT Bombay
  - Designed the first cryptographic PoR protocol for Quisquis cryptocurrency exchanges
  - Provides PoR preserving the privacy of the exchanges
  - Implemented the protocol in *Rust*
- Revelio, a PoR protocol for Mimblewimble — Ph.D. Thesis
  Joint work with Prof. Saravanan Vijayakumaran — EE Dept, IIT Bombay
  - Designed the first cryptographic PoR protocol for Mimblewimble based cryptocurrency exchanges
  - Provides PoR preserving the privacy of the exchanges
  - Implemented the protocol in *Rust*
- MProve, a PoR protocol for Monero exchanges — Ph.D. Thesis
  Joint work with Prof. Saravanan Vijayakumaran — EE Dept, IIT Bombay
  - Modified Provisions (PoR protocol for Bitcoin exchanges) for Monero exchanges, *aka* MProvisions
  - Proposed MProve, a PoR protocol for Monero outperforming MProvisions
  - Both provide PoR preserving the privacy of the exchanges
  - Implemented both the protocols in *C++*
- Rewrite cost optimal rank modulation codes for flash memories — Ph.D. Initial stage, 2017
  Joint work with Prof. Saravanan Vijayakumaran — EE Dept, IIT Bombay
  - Found all possible largest permutation codes in S_4 and S_5 by maximum clique approach
  - Proposed an algorithm to compute the rewrite cost and obtained the optimum codes using *SAGE*
  - Obtained the smallest possible set from which all codes are generated
- A study on encoding techniques of LDPC codes — ME Thesis, 2014-2015
  Joint work with Prof. Ankita Pramanik — ETCE Dept, IIEST, Shibpur
  - Proposed an algorithm to remove a shortcoming of the existing method
  - Showed better bit error rate performance in MATLAB

Publications

Journal Publications

[1] **A. Dutta**, S. Bagad, S. Vijayakumaran, MProve+: Privacy Enhancing Proof of Reserves Protocol for Monero, accepted in *IEEE Transactions on Information Forensics & Security*. [preprint], [doi]

Refereed Conference Publications

[1] **A. Dutta**, A. Jana, S. Vijayakumaran, Nummatus: A Privacy Preserving Proof of Reserves Protocol for Quisquis, *20th International Conference on Cryptology in India (Indocrypt 2019)*, Hyderabad, India, Dec. 2019. [doi]

[2] **A. Dutta**, S. Vijayakumaran, Revelio: A MimbleWimble Proof of Reserves Protocol, *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, Jun. 2019. [preprint], [doi]

[3] **A. Dutta**, S. Vijayakumaran, MProve: A Proof of Reserves Protocol for Monero Exchanges, *2019 IEEE European Symposium of Security and Privacy Workshops*, Stockholm, Sweden, Jun. 2019. [preprint], [doi]

[4] **A. Dutta**, S. Vijayakumaran, Rewrite Cost optimal Rank Modulation Codes in S_4 and S_5, *Twenty Fourth National Conference on Communications (NCC 2018)*, Hyderabad, India, Feb. 2018. [doi]

[5] **A. Dutta**, A. Pramanik, Modified approximate lower triangular encoding of LDPC codes, *2015 International Conference on Advances in Computer Engineering and Applications*, Ghaziabad, 2015, pp. 364-369. [doi]

Notable Coursework at IIT Bombay

Applied Math	**Coding Theory**	**Miscellaneous**
Number Theory & Cryptography (EE 720)	Information Theory and Coding (EE 708)	Digital Message Transmission (EE 703)
Optimization (SC 607)	Error Correcting Codes (EE 605)	Statistical Signal Analysis (EE 601)
Applied Analysis in Engineering (EE 759)	Adv. Error Correcting Codes (EE 754)	

Awards

- National Scholarship Examination — 2003 - 2005
- MHRD Scholarship for Masters Research Scholars — July, 2013 - June, 2015
- MHRD Scholarship for Doctoral Research Scholars — July, 2015 - June, 2020
- Excellence in Teaching Assistantship for the course *Cryptocurrency and Blockchain Technologies (EE 465)* — Autumn, 2018
- Excellence in Teaching Assistantship for the course *An Introduction to Number Theory and Cryptography (EE 720)* — Spring, 2019

Industrial Training

- IETE, Kolkata on microcontrollers & VI — August, 2010
- Signal and Telecomm. Dept, SE Railways, Adra on telecommunication systems — July, 2010
- Power Grid Corporation of India Limited on overview of power grid systems — January, 2010

References

1. Saravanan Vijayakumaran
   Associate Professor
   sarva@ee.iitb.ac.in
   IIT Bombay
2. Zac Williamson
   Doctorate in Particle Physics from University of Oxford,
   Former physicist at CERN and T2K Japan
   Creator of AZTEC Protocol, co-inventor of PLONK
   zac@aztecprotocol.com
   CEO and Founder, Aztec
3. Ankita Pramanik
   Assistant Professor
   ankita@telecom.iiests.ac.in
   IIEST, Shibpur