

ARIJIT DUTTA

CONTACT INFORMATION

Kolkata,
West Bengal,
India

☎ (+91)8879175981/9474620082
✉ arijit.dutta67@gmail.com/arijit@aztecprotocol.com
🌐 arijitdutta67.github.io/homepage
🔗 github.com/arijitdutta67
in linkedin.com/in/arijit-dutta-14bb2138/

RESEARCH INTERESTS

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

PRESENT POSITION

Cryptography Engineer
[Aztec Protocol, London, United Kingdom](#)

INDUSTRIAL AND ACADEMIC EXPERIENCES

- Cryptography Engineer in [Aztec Protocol](#) July, 2021 - Present
- Ph.D. Research Scholar in [IIT Bombay](#) July, 2015 - August, 2021
- Assistant System Engineer in [Tata consultancy Services Limited](#) December, 2011 - July, 2013
- Teaching Assistant in 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)

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. [\[doi\]](#)

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++, Solidity, Rust, Python, SAGE, \LaTeX
- **Softwares and Packages** : Visual Studio Code, MATLAB, Gurobi Optimizer, Cliquer
- **Operating Systems** : MacOS, Linux, Windows
- **Version Control Systems** : Git, Bitbucket

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](#)
 - Executed a thorough analysis of the privacy properties of the MProve+ protocol
 - 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, IEST, Shibpur

- Proposed an algorithm to remove a shortcoming of the existing method
- Showed better bit error rate performance in MATLAB

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. [Sachin Patkar](#)
Professor
patkar@ee.iitb.ac.in
IIT Bombay
3. [Ankita Pramanik](#)
Assistant Professor
ankita@telecom.iiests.ac.in
IIEST, Shibpur