Kushal Babel

New York, NY
✉ kb742@cornell.edu • www.cs.cornell.edu/~babel • Updated: Aug, 2024

Research Areas

Security, Distributed Systems, Blockchains, Applied Cryptography, Cryptoeconomics, Formal Methods

Current Position

Senior Researcher
Monad Labs *2024–Present*

Education

Cornell University
PhD & M.S., Computer Science *2019 - 2024*
Advisor: Prof. Ari Juels

Indian Institute of Technology Bombay **GPA 9.45/10.0**
B.Tech.(Hons.), Computer Science and Engineering *2014 - 2018*

MDS Public School **97.80%**
CBSE Intermediate/+2 *2014*
State Topper among 100,000 candidates

Publications

Preprints

4. **PROF: Protected Order Flow in a Profit-Seeking World**
Kushal Babel, Nerla Jean-Louis, Yan Ji, Ujval Misra, Mahimna Kelkar, Kosala Yapa Mudiyanselage, Andrew Miller, Ari Juels
ArXiv Preprint, 2024

3. **Mysticeti: Low-Latency DAG Consensus with Fast Commit Path**
Kushal Babel, Andrey Chursin, George Danezis, Lefteris Kokoris-Kogias, Alberto Sonnino
ArXiv Preprint, 2023
Adopted by the Sui Blockchain

2. **Complete Knowledge: Preventing Encumbrance of Cryptographic Secrets**
Mahimna Kelkar, Kushal Babel*, Philip Daian*, James Austgen, Vitalik Buterin, Ari Juels*
IACR Preprint, 2023

1. **DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs**
James Austgen, Andres Fabrega, Sarah Allen, Kushal Babel, Mahimna Kelkar, Ari Juels*
ArXiv Preprint, 2023

Conferences and Journals

7. **Lanturn: Measuring Economic Security of Smart Contracts Through Adaptive Learning**
Kushal Babel, Mojan Javaheripi*, Yan Ji, Mahimna Kelkar, Farinaz Koushanfar, Ari Juels*
ACM CCS 2023

6. **Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts**
Kushal Babel, Philip Daian*, Mahimna Kelkar*, Ari Juels*
IEEE S&P 2023
SCRF Research Impact Award
Best Paper Award by the DeFi workshop at ACM CCS 2024

5. **Charlotte: A Web of Composable Authenticated Distributed Data Structures**
Isaac Sheff, Xinwen Wang, Kushal Babel, Haobin Ni, Robbert Van Renesse, Andrew C Myers
ACM TOCS 2023

4. **SHORTSTACK : Distributed, Fault-tolerant, Oblivious Data Access**
Midhul Vuppalapati, Kushal Babel*, Anurag Khandelwal, Rachit Agarwal*
USENIX OSDI 2022

3. Strategic Peer Selection Using Transaction Value and Latency
Kushal Babel, Lucas Baker
DeFi workshop @ ACM CCS 2022

2. **On the semantics of communications when verifying equivalence properties**
Kushal Babel, Vincent Cheval, Steve Kremer
Journal of Computer Security 2022

1. **On communication models when verifying equivalence properties**
Kushal Babel, Vincent Cheval, Steve Kremer
Principles of Security and Trust(POST) 2017
Nominated for the best paper award

* Equal Contribution

Research Internships

- **Mysten Labs** Summer 2023
Advisor: George Danezis
Researched DAG-based consensus protocols for BFT distributed systems and published "Mysticeti: Low-Latency DAG Consensus with Fast Commit Path".

- **Jump Crypto, Chicago** Summer 2022
Researched robustness of peer-to-peer networks in distributed systems against economically strategic agents and published "Strategic Peer Selection Using Transaction Value and Latency".

- **INRIA, Nancy** Summer 2016
Advisor: Steve Kremer
Published new formal semantics for security protocols in π-calculus and proved that existing semantics, widely believed to be equivalent, are in fact incomparable.

Previous Industry Experience

HFT Quantitative Researcher and Trader April'18 - May'19
AlphaGrep Securities, Mumbai | Singapore

- Responsible for researching and trading equities and derivatives in emerging markets
- Developed the high frequency trading infrastructure in C++

SWE Intern Summer 2017
Uber, India

- Designed & Implemented code flow critical micro-service and library from scratch for defining, concurrently evaluating, and maintaining operational business rules separately from application code
- Profiled & optimised the code in Golang to reduce rule fetching & evaluation latency from 150 μs to 4.2 μs

Scholastic Achievements

- All India Rank 4 in JEE Mains among over 1.3 million candidates (2014)
- All India Rank 27 in JEE Advanced among 150 thousand candidates (2014)
- National Rank 8 in KVPY and awarded with the KVPY fellowship by Govt. of India (2012)
- National Rank 14 in ACM ICPC contest (2018)

International Olympiads

- Represented India & won a silver medal at the 9th International Junior Science Olympiad (2012)
- Bronze Medalist at the 46th International Chemistry Olympiad among 75 countries (2014)
- Selected to represent India at the Asian Physics Olympiad held at Singapore (2014)

Academic Service

Program Committee Member: DeFi workshop @ ACM CCS 2024, DeFi workshop @ FC 2023, DeFi workshop @ ACM CCS 2024
External Reviewer: ACM SIGMETRICS 2024, FC 2024, SBC 2022, ACM CCS 2020
Seminar Organizer, Cornell Security Seminar 2021–2022
Academic Committee Member, Cornell PhD admissions. 2022
Academic Committee Member, International Physics Olympiad (Evaluated students from 7 countries) 2015

Teaching & Mentoring

Teaching Assistant, Cornell University

1. Blockchains, Cryptocurrencies, and Smart Contracts | *Prof. Ari Juels* Spring'22
2. Introduction to Compilers | *Prof. Andew C Myers* Spring'20
3. Object-oriented design and Data structures (Lecturer for tutorial sessions) | *Prof. Andew C Myers* Fall'19

Teaching Assistant, IIT Bombay

1. Operating Systems | *Prof. Bernard Menezes* Fall'17
2. Digital Logic Design (Recognized as "TA of the month") | *Prof. Supratik Chakraborty* Spring'17
3. Computer Programming & Utilization | *Prof. Bernard Menezes* Fall'16
4. Programming Abstractions & Paradigms | *Prof. Om P. Damani* Spring'16
5. Quantum Physics | *Prof. S. Umasankar* Fall'15

Mentoring, IIT Bombay

- Led a team of 20 mentors to mentor & provide academic guidance to 130 IITB students 2017-18
- Mentor under Department Academic Mentorship Programme (mentored 6 sophomores) 2016-17

Invited Talks

- PROF: Protected Order Flow for Fair Transaction-Ordering in a Profit-Seeking World
  - SBC'24 at Columbia, NYC [Link]
  - UCSB-ECON DeFi Seminar'24
  - SBC'23 MEV Day at Stanford
- Mysticeti: Low-Latency DAG Consensus with Fast Commit Path
  - IC3 Retreat'24 at Geneva
  - Avalanche Labs Systems Seminar [Link]
- Lanturn: Measuring Economic Security of Smart Contracts Through Adaptive Learning
  - ACM CCS'23 at Copenhagen
  - SBC'23 at Stanford [Link]
  - IC3 Retreat'23 at Geneva
  - Avalanche Labs Systems Seminar [Link]
- Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts
  - IEEE S&P'23 at San Francisco [Link]
  - SBC'22 at Stanford [Link]
- Shortstack: Distributed, Fault-tolerant, Oblivious Data Access
  - USENIX OSDI'22 at Carlsbad, CA [Link]
- Strategic Peer Selection | ACM CCS'22 Workshop on DeFi [Link]
- Charlotte | Ripple UBRI'20 [Link]

Technical Skills

Smart Contract Auditing, C++ (expert), Solidity (expert), Rust, Go, Python, Java, OCaml, Bash, JavaScript, MatLab, LaTeX

Graduate Coursework

Advanced Systems, Cryptography, Advanced Programming Languages, Security and Privacy Technologies, Computer Vision, Information Retrieval