Mukesh Tiwari

Education

2016–2020 **PhD, Computer Science**, *Australian National University*, Canberra, Australia

2004–2009 **Integrated Post Graduate**, *Indian Institute of Information Technology & Management*, Gwalior, India

PhD thesis

Title *Formally Verified Verifiable Electronic Voting Scheme*

Supervisor Dirk Pattinson

Description We focussed on three main challenges posed by electronic voting: correctness, privacy, and verifiability. We addressed correctness by using a theorem prover to implement a vote-counting algorithm, privacy by using homomorphic encryption, and verifiability by generating a independently checkable scrutiny sheet. Our work had been formalised in the Coq theorem prover.

2021- **Senior Research Fellow**, *University of Cambridge*, Cambridge, United Kingdom
I am working on formalising network protocols framework in Coq theorem prover. The goal is to develop a mathematical proven correct framework so that a protocol designer can assess the properties of their protocols using my framework

2020-21 **Research Fellow**, *University of Melbourne*, Melbourne, Australia
I worked with Toby Murray on *Security Concurrent Separation Logic*. The aim was to mathematically reason about memory safety and information flow property of concurrent programs written in C.

2013–2015 **Lecturer**, *International Institute of Information Technology*, Bhubaneswar, India
This role was primarily teaching-focussed, and the courses I taught were *C programming, Java Programming, Compiler Design* and *Cryptography*. In addition, every year I supervised two master's students in their final year project.

2012–2013 **Haskell Developer**, *Parallel Scientific*, Colorado, USA
In this role, my primary job was research and prototype high performance software programs, mainly linear algebra algorithms written in Haskell.

2009–2012 **Technical Assistant**, *Government of India*, Kolkata, India
I worked as a developer for automating the day-to-day job, including enforcing the security policies of the organisation.

2008–2008 **Summer Intern**, *Arcelor-Mittal, Research & Development Technological Centre*, Avilés, Spain
I worked on formalising many business requirements into a linear programming problem and wrote a custom interface that interacted with Arcelor-Mittal's in-house linear programming solver.

Skills

Coding Coq, Haskell, OCaml, Lean, Python, C

+44-7824648138
mt883@cam.ac.uk, mukesh.tiwari@anu.edu.au, mukeshtiwari.iiitm@gmail.com
mukeshtiwari.github.io/ • *mukesh-tiwari-3609486/*
mukeshtiwari

Language Hindi, English

Awards

HDR Fee Remission Merit Scholarship

ANU PhD Scholarship (International)

Full Scholarship to attend DeepSpec Summer School 2018, Princeton University

Travel Scholarship to attend Marktoberdorf Summer School 2019 (I could not attend it because I did not get the visa for Germany)

References

- Dirk Pattinson, Research School of Computer Science, Australian National University, Canberra, dirk.pattinson@anu.edu.au
- Thomas Haines, Research School of Computer Science, Australian National University, Canberra, thomas.haines@anu.edu.au
- Toby Murray, School of Computing and Information Systems, University of Melbourne, Melbourne, toby.murray@unimelb.edu.au
- Timothy Griffin, Computer Laboratory, University of Cambridge, Cambridge, tgg22@cam.ac.uk
- Véronique Cortier, Research Director, CNRS, LORIA, Nancy, France, veronique.cortier@loria.fr (I have not worked with her but she understands my work very closely. She agreed to write me a reference letter based on my election security work)

+44-7824648138

mt883@cam.ac.uk, mukesh.tiwari@anu.edu.au, mukeshtiwari.iiitm@gmail.com

mukeshtiwari.github.io/ • *mukesh-tiwari-3609486/*

mukeshtiwari