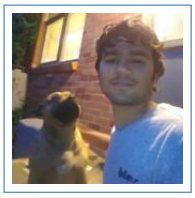

Mukesh Tiwari

Education

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

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 the three main concerns posed by electronic voting: correctness, privacy, and verifiability. We addressed the correctness concern by using a theorem prover to implement the vote counting algorithm (including machine checked proof of correctness), privacy concern by using homomorphic encryption (computed the final tally without decrypting any individual ballots), and verifiability concern by generating a independently checkable scrutiny sheet (augmented with zero-knowledge-proofs). Our work has been carried out in Coq theorem prover.

Experience

2020– **Research Fellow**, *University of Melbourne*, Melbourne, Australia.
Currently, I am working with Toby Murray on *Security Concurrent Separation Logic*. The aim of the project is to formally reason about security and information flow for a concurrent program.

2013–2015 **Lecturer**, *International Institute of Information Technology*, Bhubaneswar, India.
This role was primarily geared towards teaching, and the courses I taught was *C programming, Cryptography* and *Compiler Design*. However, I mentored some of the Masters students in their final year project.

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

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

+61-422059750
mukesh.tiwari@unimelb.edu.au, mukesh.tiwari@anu.edu.au, mukeshtiwari.iiitm@gmail.com
mukesh-tiwari-3609486/ • mukesh_tiwari • mukeshtiwari

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

Skills

Coding Coq, Haskell, OCaml, Idris, Racket, Clojure, Lean, Isabelle, Python, C, Java

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

Publications

[1] Nadim Kobeissi, Georgio Nicolas, and Mukesh Tiwari. Verifpal: Cryptographic protocol analysis for the real world. In *Progress in Cryptology – INDOCRYPT 2020 (to appear)*.

[2] Thomas Haines, Rajeev Goré, and Mukesh Tiwari. Verified verifiers for verifying elections. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 685–702, New York, NY, USA, 2019. Association for Computing Machinery.

[3] Thomas Haines, Dirk Pattinson, and Mukesh Tiwari. Verifiable homomorphic tallying for the schulze vote counting scheme. In *Verified Software: Theories, Tools, and Experiments*. Springer, 2019.

[4] Milad K. Ghale, Rajeev Goré, Dirk Pattinson, and Mukesh Tiwari. Modular formalisation and verification of stv algorithms. In Robert Krimmer, Melanie Volkamer, Véronique Cortier, Rajeev Goré, Manik Hapsara, Uwe Serdült, and David Duenas-Cid, editors, *Electronic Voting*, pages 51–66, Cham, 2018. Springer International Publishing.

[5] Lyria Bennett Moses, Rajeev Goré, Ron Levy, Dirk Pattinson, and Mukesh Tiwari. No more excuses: Automated synthesis of practical and verifiable vote-counting programs for complex voting schemes. In Robert Krimmer, Melanie Volkamer, Nadja Braun Binder, Norbert Kersting, Olivier Pereira, and Carsten Schürmann, editors, *Electronic Voting*, pages 66–83, Cham, 2017. Springer International Publishing.

[6] Dirk Pattinson and Mukesh Tiwari. Schulze voting as evidence carrying computation. In Mauricio Ayala-Rincón and César A. Muñoz, editors, *Interactive Theorem Proving*, pages 410–426, Cham, 2017. Springer International Publishing.

[7] R. Choudhari, K. V. Arya, M. Tiwari, and K. S. Choudhary. Performance evaluation of sctp-sec: A secure sctp mechanism. In *2009 Fourth International Conference on*

+61-422059750

mukesh.tiwari@unimelb.edu.au, mukesh.tiwari@anu.edu.au, mukeshtiwari.iiitm@gmail.com

mukesh-tiwari-3609486/ • mukesh_tiwari • mukeshtiwari

Computer Sciences and Convergence Information Technology, pages 1111–1116, Nov 2009.

[8] M. Tiwari, K. V. Arya, R. Choudhari, and K. S. Choudhary. Designing intrusion detection to detect black hole and selective forwarding attack in wsn based on local information. In *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*, pages 824–828, Nov 2009.

References

- Dirk Pattinson, Research School of Computer Science, Australian National University, Canberra, dirk.pattinson@anu.edu.au
- Toby Murray, School of Computing and Information Systems, University of Melbourne, Melbourne, toby.murray@unimelb.edu.au
- Thomas Haines, Department of Mathematical Sciences, Norwegian University of Science and Technology, Gløshaugen, thomas.haines@ntnu.no