Mukesh Tiwari
Cambridge, United Kingdom
📱 *+447824648138*
✉ *mt883@cam.ac.uk*

To
The Hiring Committee
Yale University

Application for the post of Assistant Professor

Dear Hiring Committe,

I am writing to apply the job **Assistant Professor**. I have an extensive experience in security research, in particular cryptography and election security. I have a PhD from the Australian National University, Canberra and Currently, I am working as a Senior Research Fellow at the University of Cambridge since October 2021. Before moving to Cambridge, I was a research fellow at the University of Melbourne.

The goal of my PhD was to bring three important ingredients, correctness, privacy, and (universal) verifiability, of a paper ballot election to an electronic setting (electronic voting). I demonstrated (i) correctness by implementing and proving the correctness of a vote-counting algorithm, the Schulze method, in the Coq theorem prover, (ii) privacy by using homomorphic encryption to encrypt the ballots and computed the winner by combining all the (encrypted) ballots, and (iii) verifiability by means of various zero-knowledge-proofs. At Yale University, as an Assistant Professor, I would like to expand my research area into other areas of formal verification, e.g., programming languages, information flow security, differential privacy, cryptography used in Internet-of-Things, etc. My research has been published Interactive Theorem Proving (ITP), Computer and Communications Security (CCS), Electronic Voting (EVote), and various other conferences.

As a senior research associate at the University of Cambridge, I am working on a mathematical correct-by-construction framework in the Coq theorem prover based on theory of routing algebra in *semiring* algebraic structure. The goal is to alleviate network-engineers from proving the correctness and security of their (network) protocol and focus entirely on protocol design. All they need to do is express their protocol in my (mathematical) framework, and it will tell what property the protocol follows and what it does not. In addition, in our framework, depending on concrete instantiation of semiring operators, the same algorithm can compute shortest path, longest paths, widest paths, multi-objective optimisation, data flow of imperative programs, and many more.

As a research associate at the University of Melbourne, I did acquire hands-on knowledge of separation logic and information flow security. I have spearheaded three projects: (i) A formally verified auction server, (ii) A formally verified location server, and (iii) A formally verified machine learning algorithm that is resistant to side-channel attacks and can run inside the Intel SGX (Software Guard Extensions) enclave for learning on sensitive data. All three implementations have been proven memory safe (using separation logic) and free from information leaks using the SecureC tool, a tool developed at the University of Melbourne.

I look forward to hearing from you. Let me know if you have any questions.

Your Sincerly,

Mukesh Tiwari