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

To
The Hiring Committee,
CISPA, Saarbrucken

Application for the Faculty Positions in Security, Privacy, and Cryptography

Dear Hiring Committee,

I am writing to apply for the **Tenure-Track Faculty** job in Security, Privacy, and Cryptography. I have extensive research experience in (election) software security, theorem proving (Coq theorem prover), cryptography, and social choice theory. I have a PhD from the Australian National University, Canberra, Australia, and currently, I am working as a senior Research Fellow at the University of Cambridge. Before moving to Cambridge, I was a research fellow at the University of Melbourne, Australia.

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 CISPA, as a tenure-track faculty, I would like to expand my research area into other areas of security and formal verification, e.g., domain specific language to reason about functional correctness and security properties –from computational complexity perspective– of cryptographic algorithms, anonymous communication, blockchain, zk-snark, information flow security, computational complexity of social choice methods, etc. My research has been published in Interactive Theorem Proving (ITP), Computer and Communications Security (CCS), Electronic Voting (EVote), International Conference on Cryptology in India (IndoCrypt), and some (finished) works have been submitted to ESOP, USENIX, and SIGCOMM. All my research work has been formalised in the Coq theorem prover.

In my current project *Combinators for Algebraic Structures (CAS)*, I am formalising various graph algorithms on *semiring* and combinators (functions) to combine two, or more, algebraic structures. In this work, I am developing a mathematical correct-by-construction framework, in Coq theorem prover, based on theory of generalised path-finding algebra. 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. In fact, the Schulze method is one instance of our framework. However, the current CAS implementation is highly focused towards networking protocols, so as a future work I will focus on adding more algorithms in CAS related to multi-objective optimisation, data flow analysis of imperative programs, and voting.

As a research associate at the University of Melbourne, 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. Please let me know if you have any questions.

Your Sincerly,

Mukesh Tiwari