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

To
The Hiring Committee
The University of Oxford, Oxford, UK

Application for the post of Assistant Professor in Cyber Security

Dear Hiring Committee,

My name is Mukesh Tiwari and I am a senior research associate at the University of Cambridge, UK with expertise in formal methods, cybersecurity and privacy, and social choice theory. I am writing to apply for the job **Assistant Professor in Cyber Security at the University of Nottingham**. I have extensive research experience in formal verification (Coq theorem prover), electronic voting, and cryptography. My research touches the lives of common people and solves real-world problems that matter to democracies. For example, my paper (i) **Assume but Verify: Deductive Verification of Leaked Information in Concurrent Applications**, accepted in ACM CCS, develops a theory using the information-flow security principals for processing sensitive data –ethnic origin, political opinions, health-related data, and biometric data– of common people in secure enclave, e.g., Intel SGX, Arm TrustZone. Moreover, we demonstrate the usability of our method by developing non-trivial case studies that handles sensitive data accompanied by the machine-checked mathematical proofs that none of them have unintended side-channel data leakage; (ii) **Machine-checking Multi-Round Proofs of Shuffle: Terelius-Wikstrom and Bayer-Groth**, published in USENIX Security, mathematically establishes a critical piece of code in the SwissPost voting software –used in legally binding elections in Switzerland– is correct (and debunks a decade old myth of the cryptographic community that Terelius-Wikstrom method is zero-knowledge-proof. We have formally proved in the Coq theorem prover that it is a zero-knowledge-argument and not a zero-knowledge-proof); (iii) **Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme**, published in VSTTE, not only developes a publicly verifiable method to count encrypted ballots for a complex voting method but it is also proven correct in the Coq theorem prover to ensure that there is no gap between the pen-and-paper proof and the actual implementation; (iv) **Verified Verifiers for Verifying Elections**, published in ACM CCS, develops a mathematically proven correct tool in the Coq theorem prover to verify the elections conducted by the International Association for Cryptologic Research. We have used our tools to verify the integrity of IACR elections; (v) **Modular Formalisation and Verification of STV Algorithms**, published in E-Vote, develops a mathematically proven correct tool in the Coq theorem prover. We have used this tool to verify the results of Australian Senate election; (vi) **Verifpal: Cryptographic Protocol Analysis for the Real World**, publised in INDOCRYPT, develops a tool that can used to model real work cryptographic protocol, and Verifpal has been used by many researchers to model security and privacy aspect of digital contact tracing during COVID, etc. At Cambridge, I am developing a mathematically proven correct tool in the Coq theorem prover that can be used by networking researchers to model networking-protocols in the abstract setting of semirings. In a nutshell, all my research so far has an impact on the lives on common people and researchers.

I believe communication is the key to resolve any conflict. Most of my projects are in a team with one or two other researchers and there are many situations of conflicting opinions about the ongoing research. However, no matter how difficult the situation is, my baseline is to always be respectful to the person working with me and then resolve the conflict via dialogue. Even though I am an introvert, all the researchers that collaborated with me enjoyed working with me. In addition, many of my students from India enjoyed working with me on their masters project and because of the limitation of two masters project per year, I had to say no to many other students.

Your Sincerly,

Mukesh Tiwari