Mukesh Tiwari
Oxford, United Kingdom
+447824648138
mukesh.tiwari@cs.ox.ac.uk

To
The Hiring Committee
Institute of Science and Technology, Austria

Application for the tenure-track Assistant Professor (Computer Science)

Dear Hiring Committee,

My name is Mukesh Tiwari and I am a senior research associate at the University of Oxford, UK with expertise in formal methods, cybersecurity and privacy, and social choice theory. I am writing to apply for the tenure-track **Assistant Professor** job. I have extensive research experience in formal verification (Coq theorem prover), cryptography, and electronic voting, and my research experience makes me a valuable candidate for this post.

My research touches the lives of common people and solves real-world problems that matter to democracies and common people. For example, my paper (i) **Assume but Verify: Deductive Verification of Leaked Information in Concurrent Applications**, accepted in ACM CCS, develops a theory 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, etc. 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**, published 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 developed a mathematically proven correct tool in the Coq theorem prover that can be used by researchers to model networking-protocols in the abstract setting of semirings (and we are in the process of submitting our paper in CAV 2024). At Oxford, I am exploring the avenues to bridge the gap between a security protocol (formal communication model) with its implementation using session types, and our goal is to produce a more realistic distributed executable model of the security protocol. Currently, as a first step, I am focussing on Signal app where my goal is to prove (or disprove) that its Java implementation follows the communication model described in the Signal's documentation. In a nutshell, all my research so far has an impact on the lives on common people and researchers.

Although, as a person, I am slightly introvert, but I firmly believe interdisciplinary research is the key to solve challenging problem pertaining to society. Therefore, I like to chat and work with diverse set of researchers, which is evident from my projects involving myriad of concepts, e.g., formal method, cryptography, voting, social choice, separation logic, information-flow security, graph theory, session types, etc.

Your Sincerly,

Mukesh Tiwari