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

To
The Hiring Committee
King's College, London, UK

Application for the post of Lecture in Computer Science (Software Engineering)

Dear Hiring Committee,

My name is Mukesh Tiwari and I am a senior research associate at the University of Cambridge, UK. I am writing to apply for the job **Lecture in Computer Science (Software Engineering)**. I have extensive research experience in formal verification (Coq theorem prover), Cryptography, and Electronic Voting. My research touches the lives of common people and solves many real world problems that matter to democracies. For example, my paper **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); **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 in the pen-and-paper proof; **Verified Verifiers for Verifying Elections**, published in ACM CCS, develops a mathematically proven correct software in the Coq theorem prover to verify the elections conducted by the International Association for Cryptologic Research. We have used our software to verify the integrity of IACR elections; **Modular Formalisation and Verification of STV Algorithms**, published in E-Vote, develops a mathematically proven correct software for single transferable vote algorithm in the Coq theorem prover. We have used this software to verify the results of Australian Senate election; **Verifpal: Cryptographic Protocol Analysis for the Real World**, publised in INDOCRYPT, develops a software 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 software in the Coq theorem prover that can used by networking researchers to model networking-protocols in the abstract setting of semirings.

In a nutshell, every single project that I have worked so far has produced a mathematically proven correct software and they have a far-reaching impact on the lives on common people and researchers. I find that the King's College London will be a perfect place to continue my real-world impact research, given that it is already a leading research university in the UK.

Your Sincerly,

Mukesh Tiwari