Benjamin Dowling
Senior Lecturer
Department of Informatics
King's College London
Strand
London
WC2R 2LS
United Kingdom

June 3, 2025

The University of Warwick
Coventry,
CV4 7AL, UK

To whom it may concern,

My name is Dr. Benjamin Dowling and I am a Senior Lecturer at King's College London in the Department of Informatics, where I have been teaching for 1 year. Previously I taught at the University of Sheffield, as a Lecturer in Cybersecurity for three years, and was a post-doctoral researcher at ETH Zurich for two years. I have known Varun Maram for six years, since I met him as a PhD student in the Applied Cryptography group at ETH Zurich.

During this time Varun has continually impressed me in both his technical aptitude, and his work ethic. Varun demonstrated a high degree of professionalism and eagerness with respect to his research and, in my view, consistently demonstrated a positive attitude, an aptitude for hard work and a capability for self-directed research.

During the time that I knew him, Varun has completed his PhD at ETH Zurich (focused on post-quantum cryptography) and has been successful as a Postdoctoral Fellow at SandboxAQ. During the time that I knew him, Varun has been able to publish several papers in top-tier cryptographic conferences, including EuroCrypt, AsiaCrypt and Crypto. His consistent track record of publishing in top-tier cryptography conferences (and also achieving best paper awards) demonstrates his high level of research quality. Finally, I note that these publications concern a large variety of cryptographic primitives and protocols including Public Key Encryption, zero-knowledge Succinct Non-interactive Arguments of Knowledge, and Symmetric Key Cryptography. Overall, this record shows that Varun is a highly flexible researcher, capable in planning and undertaking original research across different areas of cryptography and cybersecurity.

I have attended Varun's presentations at Secure Key Exchange and Channels 2024, and his accepted talk to the Real-World Cryptography Symposium 2025 (an extremely competitive symposium attended by both security practitioners and academics), and can attest to the quality of his presentation skills. This shows that Varun has developed excellent skills in pitching and presenting his work to academic communities.

As part of the Classic McEliece team, Varun has also engaged with the NIST Post-Quantum Standardisation process. Engaging with the NIST standardisation process has ensured that Varun has had significant experience working with top cryptographers in the field, developing a research network but also developing his skills in engaging with external organisations and conducting public engagement

activities. Classic McEliece was recommended for standardisation by BSI, and is a NIST finalist which is currently being considered for ISO standardization, which demonstrates Varun's research results in clear pathways to impact. Additionally, Varun has done industry research internships, demonstrating the impact of his research beyond academia.

During my time at ETH Zurich, Varun also co-contributed to the Applied Cryptography module taught to the Masters students. Kenneth G. Paterson contributed and lead the lectures, while I contributed and lead practical programming exercises, and Varun contributed and lead theoretical exercise sessions for the students. Varun also contributed to the design of the exam questions and aided in exam marking. During this time the COVID-19 quarantine procedures were introduced for the first time, and with Varun's help we were able to make the switch to online classes in a smooth fashion. In my opinion, Varun was a reliable colleague, always delivering module content according to deadlines, and was able to demonstrate a high aptitude in teaching. This demonstrates to me that Varun is capable and ready to teach undergraduate, masters and doctoral level courses, and has a record in making significant contributions to the School's teaching. His involvement in our transition from face-to-face to online teaching shows that he is capable of enhancing online and hybrid teaching initiatives.

Since I started at King's College London, Varun and I have collaborated together on a paper analysing the post-quantum cryptographic guarantees of the Secure Shell Protocol. In this work, we demonstrated that the underlying post-quantum cryptographic primitive used in current SSH implementations is stronger than necessary, and we were able to introduce a weakened cryptographic primitive that still achieved the required notions of security. This primitive was also more efficient than current state-of-the-art, and thus began a conversation in academic literature (and the standardisation community) about the necessity of new efficient post-quantum cryptographic standards that achieve distinct notions of security. Varun lead the project, recruited all collaborators and contributed the design of the new post-quantum cryptographic primitive to the project. I was continually impressed with Varun's work ethic and research quality throughout the collaboration. As a result, we were published in the top-tier security conference IEEE Symposium on Security and Privacy 2025. I enjoyed my experience working with Varun on this project, and will readily work with him in the future. This experience collaborating with Varun demonstrates to me that Varun is ready and capable of leading post-graduate and post-doctoral researchers within a research programme.

To summarise, I would strongly recommend Varun for an Assistant Professor position (in Computer Science) at the University of Warwick.

If you have further questions, I can be contacted at `benjamin.dowling@kcl.ac.uk`.

Kind regards,

Benjamin Dowling