ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Department of Computer Science
Institute of Information Security
Applied Cryptography

ETH Zürich
Prof. Dr. Kenneth G. Paterson
CAB E 79
Universitätstrasse 6
CH-8092 Zürich

tel. +41 44 632 32 52
email: kenny.paterson@inf.ethz.ch

Zurich, 28 May 2025

To whom it may concern,

I am writing this letter in support of the application by **Dr. Varun Maram** for a tenure track assistant professorship at the University of Warwick.

Varun was a doctoral student under my supervision at ETH Zurich from Autumn 2019 until December 2023, when he graduated. In fact, Varun was the very first doctoral graduate from my research group at ETH Zurich.

Varun was a truly outstanding doctoral student and I think he is a very bright prospect for any department who wishes to hire a cryptographer working at the interface between theory and practice.

The main focus of his research to date is on Post-Quantum Cryptography (PQC) which is concerned with how to develop and analyze cryptographic schemes which resist attack by adversaries equipped with quantum computers. While such adversaries do not currently exist at a cryptographically-relevant scale, progress in scalable quantum computing is moving rapidly, and making the transition to using new PQC algorithms is expected to take years. Practitioners are also concerned about “harvest now, break later” adversaries who may wait years, even decades, to be able to decrypt high-value information once sufficiently powerful quantum computers become available. PQC is currently one of the most exciting – and fastest moving – areas with cryptography research. Varun’s work in this domain covers a wide range of topics, from theoretical concerns (e.g. what happens if the adversary can make queries in superposition to a decryption oracle?) to very practical ones (e.g. exactly what can be proven about the candidate PQC schemes being considered for standardization?).

Varun did excellent research during his doctoral studies with me, publishing at the top international level (with papers at the Asiacrypt 2021 and Eurocrypt 2022 conferences). His doctoral research work also won two best paper awards (at PKC 2023 and 2024, this being a strong, second tier international conference focused on Public Key Cryptography). It is perhaps worth remarking at this juncture that, as with much of Computer Science, rapid publication in top conferences is much more important than journal publication in the field of Cryptography.

A large chunk of Varun’s doctoral thesis, published at Eurocrypt 2022 in a joint paper with me and Paul Grubbs from University of Michigan, concerns advanced security properties of post-quantum public key encryption (PKE) schemes and Key Encapsulation Mechanisms (KEMs). This paper was described as being “seminal” by one of the Eurocrypt 2022 reviewers. I stress that Varun really drove the research behind this paper and did all the heavy technical lifting. My and Paul’s role was more to provide guidance on which directions to pursue and how to best

present the results. Although generally scoped, the paper was aimed in particular at application to PKE and KEM candidates being considered at the time by the US National Institute for Standards and Technology (NIST) in its PQC competition. Specifically, we looked at anonymity properties of the schemes (roughly: given a ciphertext, can you tell under which public key it was produced?) and robustness (roughly: given a ciphertext, can it decrypt correctly under more than one private key?). As part of the work, Varun also uncovered significant gaps in existing security analyses for the standard “IND-CCA” confidentiality properties of these NIST candidate schemes. This was a surprising result given the detailed scrutiny to which these schemes had already been subjected. The reason for the gap was seemingly innocuous changes made to standard transformations used to lift from weak to strong security properties for these schemes; formally, these changes then invalidated existing generic proofs for the transformations. This realization led to some the proposers of some schemes deciding to revise the fine details of their specifications, so the work had a measurable impact on the NIST PQC competition.

As will be evident from his publication list, Varun became increasingly independent during his time with me. For example, his Asiacrypt 2021 paper came about because Nigel Smart at KU Leuven realized that Varun had become a master of a certain cryptographic proof technique (the so-called Quantum Random Oracle Model), and so involved him in a project to make use of this very specific expertise. As another example, he has struck up a very productive collaboration with Keita Xagawa from NTT, Japan, analyzing further the fine-grained security properties of NIST post-quantum candidate schemes in a follow-up work to our Eurocrypt 2022 paper. In his latest work, conducted during his postdoc at Sandbox AQ, he has been looking at the security of PQC options for SSH, the well-known and extremely important protocol for enabling secure remote access to computer systems. This work, jointly with Ben Dowling at King’s, one of his students, and with Xagawa, will appear at IEEE Security & Privacy 2025, the top annual security conference. These examples show how Varun is broadening the scope of his work and building his own network of collaborators beyond ETH Zurich.

During his doctoral studies, Varun gained valuable experience in the context of an industrial research lab through two internships with Visa Research. This resulted in a number of high-quality research papers and a long-lasting relationship with researchers in this organisation. Also in the applied context, he contributed to two of the NIST PQC candidates, NTS-KEM and Classic McEliece (which eventually merged into a single proposal under the latter name). Regarding NTS-KEM, he identified a significant gap in the security proof whilst attempting to prove its security in the QROM. This caused the NTS-KEM team (of which I was a member) to revise the specification to use a more standard approach, in turn making it more competitive with Classic McEliece as a convincing candidate for NIST. This strengthened the NTS-KEM team’s case in negotiating the merger with the Classic McEliece team. Later, it was shown by Tung Chou that the gap in the proof could actually be exploited to mount an attack on NTS-KEM, so Varun’s research and the subsequent changes we made to NTS-KEM saved the team from a lot of embarrassment later on. Varun remains a member of the Classic McEliece team. Although not selected for standardization by NIST at this time, Classic McEliece is still being standardized by ISO. This example how Varun’s work has the potential for impact beyond the confines of academia.

Turning now to teaching, Varun developed teaching materials and worked as a TA for my course on Applied Cryptography, making and delivering exercise classes, helping with exam grading, and so on. He was always reliable and well-liked by the students. His open disposition and extreme intellectual sharpness equipped him well to deal with ETH Zurich's demanding students. He was also very successful as a mentor to Bachelor's and Master's students – for example, one of the Bachelor's theses he guided resulted in a very nice conference paper that was published at SAC 2023 (a respectable international conference venue for cryptography research).

I've seen Varun really develop as a presenter of his research over the years. Most recently, I saw him present to an audience of about 600 people at Real World Cryptography 2025 in Sofia, this being a leading venue bringing together industry and academia in cryptography. His talk was really engaging, and he seemed completely relaxed on stage in conveying the complexities of his latest research on PQC in SSH to this audience. I can imagine this transferring very successfully to the classroom and him being a popular lecturer. Of course, he does not yet have much direct teaching experience, but he has had exposure to a very rigorous and broad education in Computer Science through his Master's studies here at ETH Zurich, so I feel he would be well-equipped to teach broadly across the curriculum in Computer Science in the fullness of time.

Varun was a very reliable and friendly group member. He helped us establish the ethos of the new research group at ETH, with its focus on high-quality research coupled with a strong social side. For example, he was instrumental in getting the group to participate in pub quizzes around Zurich, helped to organize our group hikes, and was an enthusiastic participant in our research retreats. I can only ever remember Varun being happy and open to talk about any aspect of research or life more broadly. In this sense, I feel sure he would make an excellent colleague in an academic environment.

To conclude, given his excellent and impactful research in an important field within applied cryptography, his teaching experience, and his congenial personality, I can recommend Varun very highly for this open position at the University of Warwick.

If I can supply any further information in connection with his application, please do not hesitate to contact me.

Yours Sincerely,

Prof. Kenneth G. Paterson

About the author: I am a full professor of Computer Science at ETH Zurich, Switzerland and served there as head of department (2023 and 2024). I specialise in Cryptography. I am a Fellow of the IACR, the professional body for cryptography research. I was the Editor-in-Chief of the Journal of Cryptology, the leading journal in the field, between 2017 and 2020. I was the conference programme chair for EUROCRYPT 2011, an invited speaker at ASIACRYPT 2014 and EUROCRYPT 2024, and delivered the IACR Distinguished Lecture in 2025. My research has won several internationally competitive prizes, including an Applied Networking Research Prize from the Internet Research Task Force (2014), a PET award for outstanding research in Privacy Enhancing Technologies (2015), and best paper awards at NDSS 2012, ACM CCS 2016 and 2022, and IEEE S&P 2022 and 2023. I am co-founder of the “Real World Cryptography” series of workshops, which provide a forum for industry and academia to come together to exchange ideas in this rapidly developing field.