Biography:
Chris Peikert is a Professor in the Computer Science and Engineering division of the EECS department. He received his Ph.D. in 2006 from MIT’s department of Electrical Engineering and Computer Science, following undergraduate studies in Mathematics and Computer Science (also at MIT). He joined Michigan as an Associate Professor in 2015, after six years as an Assistant/Associate Professor at Georgia Tech’s School of Computer Science, and three prior years in the Computer Science Laboratory of SRI International in Menlo Park, CA. He also serves as the Head of Cryptography Research for Algorand, Inc.

His research is mainly focused on cryptography and theoretical computer science, with an emphasis on designing secure, efficient, and powerful cryptographic tools using geometric objects called (point) lattices. He particularly works on the design and analysis of quantum-secure (or “post-quantum”) cryptography, which can be run on today’s ordinary computers and networks, but is believed to be secure against attacks by large-scale quantum computers—unlike all of today’s widely deployed public-key cryptography. He is also a leader in fully homomorphic encryption, a powerful technique that allows for third parties to perform arbitrary computation on encrypted data, without revealing anything about the data itself.

His work spans from theoretical foundations to real-world implementations, and has been instrumental to the design of several post-quantum cryptography standards, including those selected by government agencies like NIST (USA), BSI (Germany), ANSSI (France), and others.

Chris is the recipient of an Alfred P. Sloan Foundation Fellowship, an NSF CAREER Award, the Bergmann Memorial Research Award (US-Israel Binational Science Foundation), Test of Time Awards from the CRYPTO and Theory of Cryptography conferences, several best/distinguished paper awards (e.g., at the Symposium on the Theory of Computation, CRYPTO, EUROCRYPT, and Computational Complexity), and multiple teaching awards.

At U-M, Chris has served on the CSE Executive Committee, the tenure-track faculty search committee for several years (twice as chair, including shepherding CSE’s first, and successful, participation in the Presidential Postdoctoral Fellows Program), the joint CoE/LSA Quantum Initiative faculty search committee, the CSE Chair search committee, and as the CSE theory lab director. In the cryptography and theory community, he has served on countless program committees, as co-program chair of CRYPTO, on the IACR Fellows selection committee (once as chair), as an invited/distinguished speaker at several conferences and departments, and as co-organizer of multiple workshops (e.g., at the Simons Foundation in UC-Berkeley).

Position Statement:
It would be an honor and a privilege to serve the College as a member of the Executive Committee. Thanks to extensive experience with CSE’s ExCom and many faculty/chair searches, I have had a closeup view of an era of enormous growth, external competition, and accompanying “churn.” This has provided a special perspective on the College’s strengths and challenges in recruiting, promoting, and retaining outstanding faculty. These include providing ways for diverse approaches and experiences to reinforce each other, for incubating bold (and therefore risky) ideas, and for evaluating impact in less traditional ways where appropriate—while always maintaining high standards, and helping faculty to achieve their highest potential. In committee work, I seek to draw out opposing perspectives (“where is my blind spot?”) and respectfully engage with them; even if they do not fully change my mind, I endeavor to find common ground and mutual understanding.