

Quantum Supremacy and its Applications

Scott Aaronson

University of Texas at Austin

Friday, October 12th, 2018

2:30 pm

RTH 105

In the near future, there will likely be special-purpose quantum computers with 50-70 high-quality qubits and controllable nearest-neighbor couplings. In this talk, I'll discuss general theoretical foundations for how to use such devices to demonstrate "quantum supremacy": that is, a clear quantum speedup for *some* task, motivated by the goal of overturning the Extended Church-Turing Thesis (which says that all physical systems can be efficiently simulated by classical computers) as confidently as possible. This part of the talk is based on joint work with Lijie Chen, <https://arxiv.org/abs/1612.05903>. Then, in a second part, I'll discuss new, not-yet-published work on how these experiments could be used to generate cryptographically certified random bits, for use in cryptocurrencies and other applications.



Scott Aaronson is David J. Bruton Centennial Professor of Computer Science at the University of Texas at Austin. He received his bachelor's from Cornell University and his PhD from UC Berkeley, and did postdoctoral fellowships at the Institute for Advanced Study as well as the University of Waterloo. Before coming to UT Austin, he spent nine years as a professor in Electrical Engineering and Computer Science at MIT. Aaronson's research in theoretical computer science has focused mainly on the capabilities and limits of quantum computers. His first book, *Quantum Computing Since Democritus*, was published in 2013 by Cambridge University Press. He's received the National Science Foundation's Alan T. Waterman Award, the United States PECASE Award, the Vannevar Bush Fellowship, the Tomassoni-Chisesi Prize in Physics, and MIT's Junior Bose Award for Excellence in Teaching.