1145-68-144 **Thomas Vidick*** (vidick@cms.caltech.edu), Pasadena, CA 91106. *Verifying quantum computations at scale: a cryptographic leash on quantum devices.*

Quantum computers are physical devices that leverage the laws of quantum mechanics to accomplish certain computations, such as the simulation of certain physical, chemical, or biological systems, in an exponentially more efficient way than can be achieved by the best classical methods. By its very nature, the outcome of such a computation cannot be predicted by a classical computer. Moreover, there is strong evidence that the outcome cannot even be verified by classical means. How can we, classical beings, tell if the quantum device produced the right prediction? What checks can be placed on the performance of devices whose computational power all but eludes us?

This question is made all the more urgent by recent advances in practical quantum devices. In this talk I will formulate the question precisely using the language of complexity theory, and present a recent resolution, by Urmila Mahadev, that combines the theory of interactive proofs with insights from cryptography and quantum information. I will not assume any background in complexity, cryptography, or quantum information, but instead aim to highlight how beautiful ideas from these areas combine to provide an insightful solution to a seemingly intractable problem. (Received August 08, 2018)