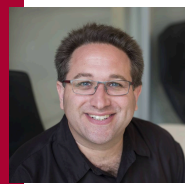


## Quantum Computational Supremacy and Its Applications



**Scott Aaronson**

UT Austin

*Professor of Computer Science*

### Abstract:

Last fall, a team at Google announced the first-ever demonstration of "quantum computational supremacy"---that is, a clear quantum speedup over a classical computer for some task---using a 53-qubit programmable superconducting chip called Sycamore. In addition to engineering, their accomplishment built on a decade of research in quantum complexity theory. This talk will discuss questions like: what exactly was the contrived computational problem that Google solved? How does one verify the outputs using a classical computer? And how confident are we that the problem is indeed classically hard---especially in light of subsequent counterclaims by IBM? I'll end with a proposed application for these sampling-based quantum supremacy experiments---namely, the generation of certified random bits, for use (for example) in proof-of-stake cryptocurrencies---that I've been developing and that Google is now working to demonstrate.

