MONTGOMERY COLLEGE

NIST Quantum Speaker Series

Behind the Q-Ball: Quantum Physics, Games, and the Re-Invention of Cryptography

Thursday, Sept 11, 2025 6:00 pm

In the present day, technology has set up a majestic showdown between two of the most important innovations of the 20th century – namely, quantum physics in the 1920s and public-key cryptography in the 1970s. In 1994, Peter Shor described a hypothetical circuit on a quantum computer which (in the words of The National Academies) would cause a "total, simultaneous, instantaneous, worldwide compromise" of public-key information security if it were actually realized. But, Shor's circuit hasn't been realized – yet. Last year, NIST published its first set of post-quantum cryptographic protocols. These replacement protocols, which are the product of a decade of international study, are designed to block quantum attacks and keep information safe going forward. Now, a new stage of re-invention has begun as these protocols are put into practice. This presentation will be a tour of ideas from this unexpected storyline in the history of information technology.

Dr. Carl A. Miller

Mathematician, National Institute of Standards and Technology

Co-Director, Joint Center for Quantum Information and Computer Science

MC Science, Engineering, and Technology Area
SETarea@montgomerycollege.edu

Globe Hall, High Technology and Science Center
20200 Observation Drive, Germantown MD 20876

This presentation is intended for a general audience.