USC Dornsife
College of Letters, Arts and Sciences
Department of Physics and Astronomy

Ming Hsieh Institute - Physics

Joint Seminar Series

USC Viterbi
School of Engineering
Ming Hsieh Department of Electrical and Computer Engineering

Certified randomness using a trapped-ion quantum processor

Ruslan Shaydulin

JPMorgan Chase

Monday, May 19, 2025
2:00-3:30 pm
In-person: EEB 132

Zoom Meeting ID: 941 1487 1670
Passcode: 231318

Abstract: Although quantum computers can perform a wide range of practically important tasks beyond the abilities of classical computers, realizing this potential remains a challenge. An example is to use an untrusted remote device to generate random bits that can be certified to contain a certain amount of entropy. Certified randomness has many applications but is impossible to achieve solely by classical computation. Here we demonstrate the generation of certifiably random bits using the 56-qubit Quantinuum H2-1 trapped-icon quantum computer accessed over the internet. Our protocol leverages the classical hardness of recent random circuit sampling demonstrations: a client generates quantum 'challenge' circuits using a small randomness seed, sends them to an untrusted quantum server to execute and verifies the results of the server. We analyze the security of our protocol against a restricted class of realistic near-term adversaries. Using classical verification with measured combined sustained performance of 1.1 x 1018 floating-point operations per second across multiple supercomputers, we certify 71,313 bits of entropy under this restricted adversary and additional assumptions. Our results demonstrate a step towards the practical applicability of present-day quantum computers. See paper for more details: [Nature 640, 343-348 (2025)]

Biography: Ruslan Shaydulin is Head of Quantum Engineering Research at the Global Technology Applied Research center at JPMorgan Chase, where he and his team focus on practical aspects of evaluating quantum algorithmic speedups and realizing them on hardware. Areas of responsibility of Ruslan's team include numerical benchmarking of quantum algorithms, compilation and execution on quantum hardware, compilation to fault-tolerant architectures and error correction. Prior to joining JPMorgan Chase, Ruslan was a Maria Goeppert Mayer fellow at Argonne National Laboratory.

Hosted by:
Quntao Zhuang, Eli Levenson-Falk, Jonathan Habif, Daniel Lidar, Kelly Luo, Todd Brun, Tony Levi, Stephan Haas