Post by Ilyas Khan, CEO of Cambridge Quantum Computing

Cambridge Quantum Computing Launches First Cloud-Based Quantum Random Number Generator Service with Verification

New joint offering with IBM will initially be available to members of the IBM Q Network, delivering certified quantum randomness for the first time

September 17, 2020

Cambridge Quantum Computing (CQC), the global provider of quantum computing software, today launched the world's first cloud-based Quantum Random Number Generation (QRNG) Service with integrated verification for the user, an important stepping stone on the road to Quantum Advantage.

Randomness is an essential and ubiquitous raw material in almost all digital interactions and is used in cybersecurity to encrypt data and communications and perform simulation analysis across many industries, including science, engineering, finance and gaming. The application developed by CQC generates true maximal randomness, or entropy, on an IBM Quantum computer that is device independent and that can be verified and thus certified as truly quantum – and therefore truly random – for the first time.

As part of a joint effort with IBM, the beta QRNG Service will initially be available to members of the IBM Q Network, a community of more than 100 Fortune 500 companies, academic institutions, startups and national research labs working with IBM to advance quantum computing.

"This is an exciting step toward making quantum computers practical and useful, and we are looking forward to seeing what scientists and developers can create using this service," said Anthony Annunziata, Director of the IBM Q Network.

Working with IBM, we have attained two quantum computing milestones: one in computation and the other in the cloud delivery of a service that can lead to real-world applications. From classical and post-quantum cryptography to complex Monte Carlo simulations where vast amounts of entropy are required to eliminate hidden patterns, certifiable quantum randomness will provide a new opportunity for advantage in relevant enterprise and government applications.

Extracting verified random numbers from a quantum processor has been an industry aspiration for many years. Many current methods only generate pseudo-random numbers or rely on physical phenomena that appear random but are not demonstrably so.

The QRNG service integrates a Bell test based on the Mermin inequality, offered through the Qiskit module qiskit_rng, which validates the true quantum nature of the underlying processes with statistical analysis. A scientific paper detailing CQC's research titled "Practical randomness amplification with implementations on quantum computers" has been published here.

“Certified QRNG is a potentially massive market because there are so many applications of the technology that are possible today, including telecommunications, finance, science and more,” said Lawrence Gasman, president of Inside Quantum Technology, a leading industry research and analysis firm. “Cybersecurity in particular is a field that will see many customers in the near term interested in verifiable quantum-generated random numbers.”

CQC was part of the founding group of startups in the IBM Q Network's startup program, announced in 2018. IBM invested in CQC in January of 2020. CQC recently became the first startup-based Hub in the IBM Q Network, working with other members on chemistry, optimization, finance, and quantum machine learning and natural language processing to advance the industry's quantum computing ecosystem.

Founded in 2014 and backed by some of the world’s leading quantum computing companies, CQC is a global leader in quantum software and quantum algorithms that help clients get the best out of rapidly evolving quantum computing hardware.