PhD THESIS DEFENSE: Intrinsic Randomness in Quantum Information Theory

FIONNUALA CURRAN

October 30, 2026
10:00
ICFO Auditorium

The unpredictability of quantum physics gives rise to an intrinsic form of randomness. We generate it by performing a measurement on a quantum state. In an adversarial scenario, we then quantify the randomness by the probability that a correlated eavesdropper could correctly guess the measurement outcomes. This thesis addresses the following question: given a known quantum state and measurement, how much intrinsic randomness can we generate?

We begin by solving the maximal intrinsic randomness of any state, optimised over all projective measurements, for four figures of merit: the conditional min, max and von Neumann entropies, and the newly introduced unambiguous randomness. The last of these describes an eavesdropper who is never wrong, but can sometimes return an inconclusive

outcome. Relaxing the assumption of perfect accuracy, we also consider randomness given a fixed rate of inconclusive outcomes. We solve both of these quantities for any state and projective measurement in dimension two. If the setup is used to choose random bases for a prepare-and-measure quantum key distribution protocol, we show that the unambiguous randomness captures the knowledge gained by an eavesdropper about the secret key, without causing any disturbance.

We then turn to extremal measurements beyond the projective case, which may have more outcomes. An unbiased measurement is one whose outcomes all have the same a priori probability. We characterise the randomness generated by any unbiased extremal rank-one measurement acting on any state, solving the problem explicitly in dimension two. Four-outcome measurements of this type are tomographic, such that one can fully determine the state from the outcome probabilities, so these results hold for fully source-device-dependent randomness too. The tetrahedral symmetric informationally complete (SIC) measurement, we find, has the least intrinsic randomness within this class. We also present the biased skewed SIC family of measurements, and use them to prove that 2 log d bits of randomness, the maximal amount, can be generated device-dependently (or source-device-independently) in any dimension d in which there exists a SIC measurement.

Reversing the scenario, we optimise over all states to solve the maximal intrinsic randomness of two classes of non-extremal, or noisy, measurements: any two-outcome measurement in dimension two, and projective measurements in any dimension affected by isotropic noise. In a realistic implementation, however, neither the state nor the measurement is completely free of noise. Taking a simple example of a state measured in a basis of any dimension, we compare the case where only one device is affected by noise to that where both devices are noisy, such that an eavesdropper may have joint correlations with the state and the measurement. For a fixed amount of total noise, we find that, contrary to the common practice of attributing all experimental noise to a single device, the joint-noise eavesdropper strictly outperforms her single-noise counterpart, compromising the security of the randomness generated.

That the outcomes of a quantum measurement are unpredictable has been known since the inception of quantum theory. This thesis presents a step forward in analytically characterising the intrinsic randomness of quantum physics. On the practical side, our results bound the functionality of quantum random number generators, under various assumptions. On a more foundational level, this work provides a new lens through which to compare quantum states and measurements and, from their vast landscape, to see which of them emerge as the most random.

Thesis Director: Prof. Dr. Antonio Acin

Hosted by: Academic Affairs