CERTIFIED RANDOM-NUMBER GENERATION FROM QUANTUM STEERING

GUEST SPEAKER: Dominick Joch
Centre for Quantum Dynamics, Griffith University, Australia

Giovedì 13 Luglio 2023 ore 15:00
Aula B in Vasca Navale 84 & Piattaforma TEAMS (link below)

info: antonio.benedetto@uniroma3.it; armida.sodo@uniroma3.it

Truly random numbers are an essential resource for cryptography and numerous other applications, but typically rely on statistical tests of the sequences that reveal nothing about the security of their generation and are thus insufficient as certification of genuine randomness. Indeed, such tests may be passed by pseudo random number generation, which is deterministic, yet most used despite being dependent on an adversary lacking the computing power to guess the seed.

Quantum phenomena possess intrinsic randomness, thus quantum random number generation (QRNG) presents itself as the most appealing avenue for secure randomness. Naïve approaches rely on strong assumptions about the physical devices, making them susceptible to adversarial exploitation via side information and device imperfections. However, by exploiting quantum nonlocality, one can devise QRNG schemes with device independence (DI), and the best possible levels of security. Full DI-QRNG is highly challenging experimentally, motivating partially-DI schemes with significant advantages in ease of implementation. Our work implements one such protocol—a certified random number generator based on the quantum steering nonlocality task—that is more robust to loss and noise compared to DI-QRNG protocols.

Our implementation of the protocol employs a high-quality source of single photons and superconducting nanowire single photon detectors to demonstrate randomness expansion by meeting stringent efficiency and noise requirements. The protocol was performed to acquire a min-entropy certification of randomness, we then applied a quantum-proof randomness extractor to obtain the final certified random bit sequences. Our scheme can be refined to serve as a viable randomness beacon for improved security of private randomness for cryptographic purposes and sources of public randomness.

TEAMS extended link: https://teams.microsoft.com/l/meetup-join/19%3a8f9ec19800e7467ab9bae6e627dfcb21%40thread.tacv2/1687857508554?context=%7b%22Tid%22%3a%22%7d