Certifying Genuine Randomness with arbitrarily Inefficient Detectors (CGRID)

While logging into websites, all of us have encountered the annoying Completely Automated Public Turing tests to tell Computers and Humans Apart (CAPTCHAs). These tests are rather rudimentary cryptographic schemes meant to determine whether the user is a human or a bot. Suppose an artificially intelligent adversary looking to cheat their way through the test can, in advance, predict the CAPTCHA that will appear. In that case, these systems will be rendered entirely useless and insecure. In other words, the efficacy of these tests, as well as of our bank pins and one-time-pads (OTPs), relies on secure random numbers. Genuinely unpredictable random numbers are quintessential to any computational cryptosystem and hence to individual privacy and secure communication, which form the cornerstones of modern democratic civilization.

However, there is no such thing as true randomness in the classical world. All classical physical processes are fundamentally deterministic and only appear random due to a lack of knowledge. Consequently, all classical random number generators (CRNGs) are susceptible to back-door attacks. A malicious manufacturer or an adversary having access to the CRNG's algorithm and the seed can easily guess the random numbers and breach the security of the cryptosystems that rely on them. Hence, randomness generation must be based on certifiably unpredictable physical processes to ensure lasting privacy and secure communication. So that the random numbers remain secure even against an all-powerful adversary limited only by laws of physics. Quantum mechanics is an intrinsically random theory, and quantum physical processes provide an excellent basis for random number generators (QRNGs). However, naive QRNGs require users to trust the device's manufacturer, which is not a great idea.

The only solution is device-independent (DI) quantum cryptography, wherein the security of the cryptosystem does not depend on the internal workings of the devices. Instead, the security of DIQRNG schemes relies solely on the non-classicality of observed statistics. However, DIQRNG schemes that rely on statistical tests of non-classicality suffer from loopholes. The most important loophole is the detection efficiency loophole (DEL), exploiting which a clever adversary can use experimental losses to fake non-classicality, rendering the DIQRNG schemes insecure. To thwart such attacks, the quantum detectors in DIQRNGs are required to have a minimal threshold efficiency called the critical detection efficiency (CDE). Unfortunately, the CDEs are typically very high compared to the capabilities of state-of-the-art hardware, making DI cryptography infeasible for near-term real-world applications.

CGRID is a breakthrough project which will remedy this situation and make near-term DI cryptography feasible. This project will introduce unprecedented high-yield DIQRNG schemes featuring zero CDE requirements and high resilience to experimental imperfections, essentially allowing us to retrieve unconditionally secure genuinely random numbers with very inefficient detectors. Specifically, we will introduce a revolutionary framework for 1) DI cryptography with multiple users who can collaboratively control the flow of quantum information in the network and 2) semi-DI cryptography based on assumptions that can be operationally falsified. To analyze these schemes' security and efficacy, we will utilize state-of-the-art and develop cutting-edge analytical and numerical methods. These tools will be made publicly available to benefit the scientific community and posterity. To showcase the real-world applicability of these novel schemes, we will experimentally demonstrate their proofs-of-concept with photonic quantum systems, collaborating with the University of Concepción, Chile.

In this day and age, when rapid technological advances are threatening individual privacy, the very pillar of the modern democratic civilization, Nature is providing a solution in the form of quantum cryptography. CGRID will finally make quantum cryptography a commonly used reliable technology in the near future to guarantee secure communication and individual privacy for eternity, or at least until the laws of physics hold.