CP-07-02

Verifiable quantum advantage without structure

Takashi Yamakawa

NTT Social Informatics Laboratories

Abstract

We show the following hold, unconditionally unless otherwise stated, relative to a random oracle with probability 1:
- There are NP search problems solvable by BQP machines but not BPP machines.
- There exist functions that are one-way, and even collision resistant, against classical adversaries but are easily inverted quantumly. Similar separations hold for digital signatures and CPA-secure public key encryption (the latter requiring the assumption of a classically CPA-secure encryption scheme). Interestingly, the separation does not necessarily extend to the case of other cryptographic objects such as PRGs.
- There are unconditional publicly verifiable proofs of quantumness with the minimal rounds of interaction: for uniform adversaries, the proofs are non-interactive, whereas for non-uniform adversaries the proofs are two message public coin.
- Our results do not appear to contradict the Aaronson-Ambanis conjecture. Assuming this conjecture, there exist publicly verifiable certifiable randomness, again with the minimal rounds of interaction.
By replacing the random oracle with a concrete cryptographic hash function such as SHA2, we obtain plausible Minicrypt instantiations of the above results. Previous analogous results all required substantial structure, either in terms of highly structured oracles and/or algebraic assumptions in Cryptomania and beyond.