SÉBASTIEN LORD, University of Ottawa
Uncloneable Quantum Advice

In this work, we initiate the study of the computational complexity of cloning fixed sequences of quantum states. This is in contrast to prior studies of the no-cloning principle where the states to be copied are not fixed, but rather selected at random from some larger set.

We frame our main results as the instantiation of uncloneable quantum advice for certain specific promise problems and languages. A quantum advice state can be understood as a quantum program which is run by a user to solve a given problem instance. Thus, uncloneable quantum advice can be viewed as a contribution to the larger ongoing quest in quantum cryptography to construct copy-protection schemes for interesting functionalities. Indeed, existing quantum copy-protection schemes only offer security if the program to be copy-protected is chosen at random from some larger family. Our work establishes a proof-of-principle that a version of copy-protection for fixed and specific programs is achievable.

Joint work with Anne Broadbent and Martti Karvonen.