SÉBASTIEN LORD, University of Ottawa
Secure Software Leasing Without Assumptions

Quantum cryptography is known for enabling functionalities that are unattainable using classical information alone. Recently, Secure Software Leasing (SSL) has emerged as one of these areas of interest. Given a circuit C from a circuit class, SSL produces an encoding of C that enables a recipient to evaluate C and also enables the originator of the software to later verify that the software has been returned, meaning that the recipient has relinquished the possibility to further use the software. Such a functionality is unachievable using classical information alone, since it is impossible to prevent a user from keeping a copy of the software. Recent results have shown the achievability of SSL using quantum information for compute-and-compare functions (a generalization of point functions). However, these prior works all make use of setup or computational assumptions. We show that SSL is achievable for compute-and-compare circuits without any assumptions.

We proceed by studying quantum copy-protection, which is a notion related to SSL, but where the encoding procedure inherently prevents a would-be quantum software pirate from splitting a single copy of an encoding for C into two parts each allowing a user to evaluate C. Using quantum message authentication codes, we show that point functions can be copy-protected without any assumptions against one honest and one malicious evaluator. We then show that a generic honest-malicious copy-protection scheme implies SSL. By prior work, this yields SSL for compute-and-compare functions.

This is joint work with Anne Broadbent, Stacey Jeffery, Supartha Podder, and Aarthi Sundaram.