Anne Broadbent, University of Ottawa

Title: 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 target 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 verify that the software has been returned -- meaning that the recipient has relinquished the possibility of any further use of the software. Clearly, 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 a class of functions called compute-and-compare (these are a generalization of the well-known point functions). These prior works, however, all make use of setup or computational assumptions. Here, we show that SSL is achievable for compute-and-compare circuits without any assumptions.
Our technique involves the study of 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 of which enables a user to evaluate C. We show that point functions can be copy-protected without any assumptions, for a novel security definition involving one honest and one malicious evaluator; this is achieved by showing that from any quantum message authentication code, we can derive such an honest-malicious copy-protection scheme. We then show that a generic honest-malicious copy-protection scheme implies SSL; by prior work, this yields SSL for compute-and-compare functions.

Based on joint work with Stacey Jeffery, Sébastien Lord, Supartha Podder and Aarthi Sundaram Preprint: https://arxiv.org/abs/2101.12739