Title: Quantum Obfuscation

Gorjan Alagic

Encryption of data is fundamental to secure communication. Beyond encryption of data lies obfuscation, i.e., encryption of functionality. It has been known for some time that the most powerful form of classical obfuscation (black-box obfuscation) is impossible. In this work, we initialize the rigorous study of obfuscating programs via quantum-mechanical means. We prove quantum analogues of several foundational results in obfuscation, including the aforementioned impossibility result.

In its most powerful “quantum black-box” instantiation, a quantum obfuscator would turn a description of a quantum program P into a quantum state S, such that anyone in possession of S can repeatedly evaluate P on inputs of their choice, but never learn anything else about P. We formalize this notion of obfuscation, and prove that it is only possible in a setting where the adversary has access to just one obfuscation. Our proof involves a novel technical idea: chosen-ciphertext-secure encryption for quantum states. In addition, we show that the surviving form of obfuscation may still have powerful applications, including quantum fully-homomorphic encryption and quantum money. We also define quantum versions of indistinguishability obfuscation and best-possible obfuscation, show that they are equivalent, and that their perfect and statistical variants would imply an unlikely complexity-theoretic collapse.

Joint work with Bill Fefferman.