# Tight Quantum Time-Space Tradeoffs for Function Inversion

Kai-Min Chung
Institute of Information Science, Academia Sinica

In time-space tradeoffs for function inversion, we are given a function f: [N] -> [N], and want to prepare some advice of size S, such that we can efficiently invert any image in time T. This is a fundamental problem with profound connections to cryptography, data structures, communication complexity, and circuit lower bounds. Investigation of this problem in the quantum setting was initiated by Nayebi, Aaronson, Belovs, and Trevisan (2015), who proved a lower bound of $ST^2 = \Omega(N)$ for random permutations against classical advice, leaving open an intriguing possibility that Grover's search can be sped up to time $O(\sqrt{N/S})$. Recent works by Hhan, Xagawa, and Yamakawa (2019), and Chung, Liao, and Qian (2019) extended the argument for random functions and quantum advice, but the lower bound remains $ST^2 = \Omega(N)$.

In this talk, I'll present a general framework to answer the question negatively. Specifically, our framework shows that even with quantum advice, $ST + T^2 = \Omega(N)$ is required for an algorithm to invert random functions. It means that for $S = O(\sqrt{N})$, even S qubits of quantum advice cannot help to speed up Grover's search, which remains optimal. Furthermore, for $S = \Omega(\sqrt{N})$, further improvements to our bounds would imply new classical circuit lower bounds, as shown by Corrigan-Gibbs and Kogan (2019). Our framework can also be used to prove (nearly) tight quantum time-space tradeoffs for several fundamental problems in cryptography, such as Yao's box problem, distinguishing pseudorandom generators, and salted collision-finding.