1147-68-924 **Zhengfeng Ji**, **Yi-Kai Liu** and **Fang Song*** (fang.song@tamu.edu). *Pseudorandom Quantum States.*

We propose the concept of pseudorandom quantum states, which appear random to any quantum polynomial-time adversary. This offers a computational approximation to perfect randomness on quantum states (analogous to a cryptographic pseudorandom generator), as apposed to some statistical notion of quantum pseudorandomness in the literature, such as quantum t-designs (analogous to t-wise independent distributions).

Under the assumption that quantum-secure one-way functions exist, we present efficient constructions of pseudorandom states, showing feasibility of our definition. We then prove several basic properties of any pseudorandom states, which further back up our definition. First, we show a cryptographic no-cloning theorem that no efficient quantum algorithm that can create additional copies from any polynomial-many copies of pseudorandom states. Second, as expected for random quantum states, we show that pseudorandom quantum states are highly entangled on average. Finally, as a main application, we prove that any family of pseudorandom states naturally gives rise to a private-key quantum money scheme, thanks to our cryptographic no-cloning theorem. (Received January 29, 2019)