In recent work, Speelman et al. introduced a leveled quantum fully-homomorphic encryption scheme. They use a construction that appears in earlier literature, but with the additional contribution of "gadgets" which allow the homomorphic evaluation of T-gates which lie in the third level of the Clifford hierarchy.

In this talk, we will emphasize the construction of this gate. In particular, we will view their construction from both the perspective of Barrington’s theorem, along with the garden-hose complexity model. I will try to give some intuition as to the fundamental issues with extending to a non-leveled scheme.

I will assume an understanding of the earlier work on quantum homomorphic encryption, in particular from https://arxiv.org/abs/1412.8766. If we have time, I will discuss a bit more about applications to more general instantaneous nonlocal computation introduced by Speelman.