

1139-68-105

Urmila Mahadev*, Soda Hall 635, Berkeley, CA 94720. *Classical Homomorphic Encryption for Quantum Circuits.*

We present a computationally secure classical homomorphic encryption scheme for quantum circuits. The scheme allows a classical server to blindly delegate a quantum computation to a quantum server; the server is able to run the computation without learning about the computation itself. We show that it is possible to construct such a scheme directly from quantum secure classical homomorphic encryption schemes with certain properties. Finally, we show that an existing classical homomorphic encryption scheme has the required properties, and can therefore be used to homomorphically evaluate quantum circuits. (Received February 03, 2018)