Shor's quantum factoring algorithm

Bill Franczak

10/30/2017

All modern encryption methods depend on the existence of a "one-way problem", that is, an operation which is easy to perform one way, but difficult the other. Today, popular encryption schemes rely on multiplication/factoring to provide such a problem. Even the best classical methods of factoring are prohibitively slow when applied to numbers with more than about 40 digits. However, in the quantum setting, factoring is not much harder than multiplication, which leads to the breakdown of all popular encryption systems. We review the basics of quantum computing and look at some of the details of the algorithm that allows this to happen.