Polynomial-Time Algorithms for Prime Factorization on a Quantum Computer

Presented by: Junxin Chen & Chi Zhang

In this talk we are going to introduce Shor's algorithm, a prime factorization algorithm based on quantum computer, which is formulated by mathematician Peter Shor in 1994. Comparing to classical prime factorization algorithms, which have exponential complexity, Shor's algorithm efficiently factorizes a composite integer N in polynomial time. Thanks to this feature, a lot of attention is drawn to Shor's algorithm, since it provides one approach to efficiently breaking the public-key cryptography such as the widely used Rivest-Shamir-Adleman (RSA) scheme. The speed-up of Shor's algorithm is due to the quantum parallelism in modular exponentiation and quantum Fourier transform, the two most costive procedures in prime factorization. The special requirement for reversibility of quantum computation makes the design of quantum algorithm more complicated and difficult, since to make it reversible, one has to use additional output registers to keep track of the input parameters, but in intermediate steps these additional registers might affect the interference patterns in quantum computation, and therefore they need to be set to zero using reversible operations. In our talk we will discuss how Shor overcame these difficulties and made use of the quantum parallelism. We will also demonstrate how this algorithm works by giving an example of factorizing 21.