

سمینار گروه اطلاعات کوانتومی

سه‌شنبه ۱۳۹۴/۱۰/۲۲

# Verification of quantum computing

Elham Kashefi

School of Informatics, University of Edinburgh, UK and Departement  
Informatique et Reseaux, Telecom ParisTech, Paris, France.

## Abstract

Over the next five to ten years we will see a state of flux as quantum technologies become part of the mainstream computing landscape. These devices will not be universal in terms of having a simple programming model nor will they be easily applicable to all problems. Adopting and applying such a highly variable and novel technology has an acute verification problem: On the one hand, since classical computations cannot scale up to the computational power of quantum mechanics, verifying the correctness of a quantum-mediated computation is challenging; on the other hand, the underlying quantum structure resists classical certification analysis. In this talk we present a new approach for testing the correctness of any delegated quantum computing based on the ability to compute with encrypted data, while hiding the underlying function.