Monogamy of entanglement and fully device independent quantum key distribution

Umesh Vazirani *[1]

[1] *University of California at Berkeley, Berkeley, California 94720, USA*

Abstract. Quantum cryptography is based on the discovery that the laws of quantum mechanics allow levels of security that are impossible to replicate in a classical world. Can such levels of security be guaranteed even when the quantum devices on which the protocol relies are untrusted? This fundamental question in quantum cryptography dates back to the early nineties when the challenge of achieving device independent quantum key distribution, or DIQKD, was first formulated. In this talk, we answer this challenge by exhibiting a protocol for DIQKD and rigorously proving its security. Our security proof assumes only that the devices can be modeled by the laws of quantum mechanics and are spatially isolated from each other and from any adversary's laboratory. It is based on a rare success in establishing a quantitative bound on possible correlations due to multiparty entanglement. Moreover the resulting protocol achieves a linear key rate while tolerating a constant noise rate in the devices.

Based on joint work with Thomas Vidick.

*vazirani@eecs.berkeley.edu