Uncloneable Encryption of Classical Messages with Quantum States

Daniel Gottesman
EECS: Computer Science Division
University of California, Berkeley
Soda 885
Berkeley, CA 94720
U.S.A.

Abstract

Quantum states cannot be cloned. I show how to extend this property to classical messages encoded using quantum states, a task I call "uncloneable encryption". In any purely classical encryption scheme, an eavesdropper Eve can copy the message down and read it later, possibly much later, if she can somehow learn the secret key. To break an uncloneable encryption scheme, Eve must know the key before the message is originally received. I show that it is possible to create an uncloneable encryption scheme from any authentication scheme for quantum states. Similarly, any uncloneable encryption can be used to perform quantum key distribution (QKD), demonstrating a close connection between cryptographic tasks for quantum states and for classical messages. Computationally secure uncloneable encryption is also possible, using a pseudorandom key rather than a truly random one, producing an encryption scheme whereby a temporary computational bound allows Alice and Bob to either detect eavesdropping or have information-theoretic forward security.