

Ultimately Secured Secrets in the Quantum

Era

Hagai Eisenberg

The emergence of novel quantum technologies possess new challenges to keeping secrets on one hand, and revealing them when necessary on the other. Quantum computers threaten to break most contemporary cryptographic methods, while an alternative protocol named Quantum Key Distribution (QKD) claims to correct this security breach by a new physics based method, that can provide 'ultimate' security. I will present the current state-of-the-art of these two technologies, the meaning of the claimed ultimate security, and their immediate practical consequences.