
GILLES BRASSARD, Montréal

Cryptography in a Quantum World

Although practised as an art and science for ages, cryptography had to wait until the mid-twentieth century before Claude Shannon gave it a strong mathematical foundation. However, Shannon's approach was rooted in his own information theory, itself inspired by the classical physics of Newton and Einstein. When quantum physics is taken into account, new vistas open up both for codemakers and codebreakers. Is this blessing or a curse for the protection of privacy? As we shall see, the jury is still out! No prior knowledge in cryptography or quantum physics will be assumed.

Reference: arXiv:1510.04256 [quant-ph] .