CC-06-01

Privacy for the paranoid ones - the ultimate limits of secrecy

Artur Ekert

OIST / Oxford / CQT Singapore

Abstract

Among those who make a living from the science of secrecy, worry and paranoia are just signs of professionalism. Can we protect our secrets against those who wield superior technological powers? Can we trust those who provide us with tools for protection? Can we even trust ourselves, our own freedom of choice? Recent developments in quantum cryptography show that some of these questions can be addressed and discussed in precise and operational terms, suggesting that privacy is indeed possible under surprisingly weak assumptions. I will provide an overview of how quantum entanglement, after playing a significant role in the development of the foundations of quantum mechanics, became a new physical resource for all those who seek the ultimate limits of secrecy.