Graduate talk

Quanta, ciphers and computers

In early 1935, Albert Einstein, together with Boris Podolsky and Nathan Rosen, published a classic paper which questioned the completeness of quantum mechanical description of reality and, in a tacit way, introduced quantum entanglement. After playing a significant role in the development of the foundations of quantum mechanics, entanglement has been recently rediscovered as a new physical resource with potential commercial applications. In particular it can be used to construct new methods of secure communication and new methods of breaking ciphers. I will outline the evolution of the concept from its origin till today and describe some of its current applications in quantum cryptography and quantum computation.

Colloquium I

Quantum code-breaking: about quantum computers and their cryptanalytic power

The theory of classical universal computation was laid down in 1936, was implemented within a decade, became commercial within another decade, and dominated the world's economy half a century later. Quantum information technology is a fundamentally new way of harnessing nature. It is too early to say how important a way this will eventually be, but we can reasonably speculate about its impact on computation and data security. Quantum computers use the quantum interference of different computational paths to enhance correct outcomes and suppress erroneous outcomes of computations. A common pattern underpinning quantum algorithms can be identified when quantum computation is viewed as multi-particle interference. I will use this approach to review the theory of quantum computation and its role in cryptanalysis.

Colloquium II

Quantum code-making: about quantum and post-quantum key distributions

Quantum key distribution allows two parties, traditionally known as Alice and Bob, to establish a secure random cryptographic key if, firstly, they have access to a quantum communication channel, and secondly, they can exchange classical public messages which can be monitored but not altered by an eavesdropper, Eve. Quantum key distribution provides perfect security because, unlike its classical counterpart, it relies on the laws of physics rather than on ensuring that successful eavesdropping would require excessive computational effort. I will provide a brief overview of the search for operational security criteria of quantum key distribution and discuss new trends in quantum cryptography.