1. Record Nr. UNISA996466835503316

Titolo	Applied Quantum Cryptography [[electronic resource] /] / edited by Christian Kollmitzer, Mario Pivk
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38200-7 9786613559913 3-642-04831-5
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XII, 230 p. 80 illus., 5 illus. in color.)
Collana	Lecture Notes in Physics, , 0075-8450 ; ; 797
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Elementary particles (Physics) Quantum field theory Quantum physics Quantum computers Spintronics Applied mathematics Engineering mathematics Cryptology Elementary Particles, Quantum Field Theory Quantum Physics Quantum Information Technology, Spintronics Mathematical and Computational Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Preliminaries -- Quantum Key Distribution -- Adaptive Cascade -- Attack Strategies on QKD Protocols -- QKD Systems -- Statistical Analysis of QKD Networks in Real-Life Environment -- QKD networks based on Q3P -- Quantum-Cryptographic Networks from a Prototype to the Citizen -- The Ring of Trust Model.
Sommario/riassunto	Using the quantum properties of single photons to exchange binary keys between two partners for subsequent encryption of secret data is

an absolutely novel technology. Only a few years ago quantum cryptography – or better: quantum key distribution – was the domain of basic research laboratories at universities. But during the last few years things changed. QKD left the laboratories and was picked up by more practical oriented teams that worked hard to develop a practically applicable technology out of the astonishing results of basic research. One major milestone towards a QKD technology was a large research and development project funded by the European Commission that aimed at combining quantum physics with complementary technologies that are necessary to create a technical solution: electronics, software, and network components were added within the project SECOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography) that teamed up all expertise on European level to get a technology for future encryption. The practical application of QKD in a standard optical fibre network was demonstrated October 2008 in Vienna, giving a glimpse of the future of secure communication. Although many steps have still to be done in order to achieve a real mature technology, the corner stone for future secure communication is already laid. QKD will not be the Holy Grail of security, it will not be able to solve all problems for evermore. But QKD has the potential to replace one of the weakest parts of symmetric encryption: the exchange of the key. It can be proven that the key exchange process cannot be corrupted and that keys that are generated and exchanged quantum cryptographically will be secure for ever (as long as some additional conditions are kept). This book will show the state of the art of Quantum Cryptography and it will sketch how it can be implemented in standard communication infrastructure. The growing vulnerability of sensitive data requires new concepts and QKD will be a possible solution to overcome some of today’s limitations.