

# Quantum cryptography

Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden

*Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland*

(Published 8 March 2002)

Quantum cryptography could well be the first application of quantum mechanics at the single-quantum level. The rapid progress in both theory and experiment in recent years is reviewed, with emphasis on open questions and technological issues.

## CONTENTS

I. Introduction	145	D. Frequency coding	173
II. A Beautiful Idea	146	E. Free-space line-of-sight applications	174
A. The intuition	146	F. Multi-user implementations	175
B. Classical cryptography	147	V. Experimental Quantum Cryptography with Photon Pairs	175
1. Asymmetrical (public-key) cryptosystems	147	A. Polarization entanglement	176
2. Symmetrical (secret-key) cryptosystems	148	B. Energy-time entanglement	177
3. The one-time pad as “classical teleportation”	148	1. Phase coding	177
C. The BB84 protocol	149	2. Phase-time coding	179
1. Principle	149	3. Quantum secret sharing	180
2. No-cloning theorem	149	VI. Eavesdropping	180
3. Intercept-resend strategy	150	A. Problems and objectives	180
4. Error correction, privacy amplification, and quantum secret growing	150	B. Idealized versus real implementation	180
5. Advantage distillation	151	C. Individual, joint, and collective attacks	181
D. Other protocols	152	D. Simple individual attacks: Intercept-resend and measurement in the intermediate basis	181
1. Two-state protocol	152	E. Symmetric individual attacks	182
2. Six-state protocol	152	F. Connection to Bell's inequality	185
3. Einstein-Podolsky-Rosen protocol	152	G. Ultimate security proofs	185
4. Other variations	153	H. Photon number measurements and lossless channels	187
E. Quantum teleportation as a “quantum one-time pad”	154	I. A realistic beamsplitter attack	188
F. Optical amplification, quantum nondemolition measurements, and optimal quantum cloning	154	J. Multiphoton pulses and passive choice of states	188
III. Technological Challenges	155	K. Trojan horse attacks	189
A. Photon sources	155	L. Real security: Technology, cost, and complexity	189
1. Faint laser pulses	156	VII. Conclusions	190
2. Photon pairs generated by parametric downconversion	156	Acknowledgments	190
3. Photon guns	157	References	190
B. Quantum channels	158	I. INTRODUCTION	
1. Single-mode fibers	158	Electrodynamics was discovered and formalized in the 19th century. The 20th century was then profoundly affected by its applications. A similar adventure may be underway for quantum mechanics, discovered and formalized during the last century. Indeed, although the laser and semiconductor are already common, applications of the most radical predictions of quantum mechanics have only recently been conceived, and their full potential remains to be explored by the physicists and engineers of the 21st century.	
2. Polarization effects in single-mode fibers	158	The most peculiar characteristics of quantum mechanics are the existence of indivisible quanta and of entangled systems. Both of these lie at the root of quantum cryptography (QC), which could very well be the first commercial application of quantum physics at the single-quantum level. In addition to quantum mechanics, the 20th century has been marked by two other major scientific revolutions: information theory and relativity. The status of the latter is well recognized. It is less well known that the concept of information, nowadays measured in bits, and the formalization of probabilities are	
3. Chromatic dispersion effects in single-mode fibers	160		
4. Free-space links	160		
C. Single-photon detection	161		
1. Photon counting at wavelengths below 1.1 $\mu\text{m}$	163		
2. Photon counting at telecommunications wavelengths	163		
D. Quantum random-number generators	164		
E. Quantum repeaters	164		
IV. Experimental Quantum Cryptography with Faint Laser Pulses	165		
A. Quantum bit error rate	166		
B. Polarization coding	167		
C. Phase coding	168		
1. The double Mach-Zehnder implementation	170		
2. “Plug-and-play” systems	171		