REVIEWS OF MODERN PHYSICS, VOLUME 74, JANUARY 2002

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

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.

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

