Quantum Communications and Cryptography

edited by
Alexander V. Sergienko

CRC Taylor & Francis
Taylor & Francis Group

Quantum Communications and Cryptography

edited by
Alexander V. Sergienko

Taylor & Francis
Taylor & Francis Group
Boca Raton London New York

A CRC title, part of the Taylor & Francis imprint, a member of the
Taylor & Francis Group, the academic division of T&F Informa plc.

Published in 2006 by
CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8493-3684-8 (Hardcover)
International Standard Book Number-13: 978-0-8493-3684-3 (Hardcover)
Library of Congress Card Number 2005050636

Library of Congress Cataloging-in-Publication Data

Quantum communications and cryptography / Alexander V. Sergienko, editor.
p. cm.
Includes bibliographical references and index.
ISBN 0-8493-3684-8
1. Quantum communication--Security measures. 2. Cryptography. 3. Coding theory. 4. Data encryption (Computer science) I. Sergienko, Alexander V.

TK5102.94.Q36 2005
005.8--dc22 2005050636

T&F informa
Taylor & Francis Group
is the Academic Division of T&F Informa plc.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Quantum Communications and Cryptography

Preface

The amount of Internet traffic transmitted over optical telecommunication networks has seen an enormous surge over the last decade. This process is likely to continue considering the demand for a greater variety of services and faster download rates. One central issue of modern optical telecommunication is its security. Current communication security protection schemes are based on the mathematical complexity of specific encoding protocols. Any of them can, in principle, be deciphered when a sufficient computational power becomes available. There exists one particular scheme that is not vulnerable to such scenario — the one-time pad protocol. It is based on the condition of sharing secret random key material between two parties and using it for encrypting their information exchange. However, such random key material can be used only once and then must be discarded to ensure absolute security. This requires the key to be constantly refilled in such a way that only two legitimate users will possess identical sets of random key numbers. It is of the utmost importance to make sure that nobody else has gained access to the key material during refill procedures. This is where the use of special properties of the quantum state of light — the photon — offers a solution to the problem. Such basic principles of quantum theory as the no-cloning theorem have enabled researchers to implement a totally secure quantum key distribution (QKD). Secure distribution of random key material using quantum state of light constitutes the essence of a recently emerged area of physics and technology — quantum cryptography.

In 2005, quantum mechanics and quantum theory of light celebrated their 100th anniversary of successfully describing basic properties of matter and its interaction with electromagnetic radiation. Basic quantum principles outlined in earlier days have paved the way for the development of novel techniques for information manipulation that is based on the physical principles of correlation, superposition, and entanglement. Quantum information processing uses nonclassical properties of a quantum system in a superposition state (qubit) as the physical carrier of information. This is in contrast with conventional description, which is based on the use of discrete classical deterministic bits. This nonclassical manipulation of information has created the possibility of constructing extremely efficient quantum computers operating on thousands of qubits at a time. This challenging and far-reaching goal still requires a great deal of theoretical and experimental research efforts

to develop quantum hardware resistant to decoherence and designing novel algorithms to serve as quantum software.

In the meantime, quantum information processing applications dealing with only a few qubits have been developed during the last decade and have been moving from the university and government research labs into the area of industrial research and development. Quantum cryptography that is based on the use of only one or two qubits can serve as a success story of practical quantum information processing. Several small businesses have already started offering practical point-to-point quantum key distribution devices covering short and medium distances thus developing a novel market for this disruptive technology. The first public quantum key distribution network that connects multiple users over commercial fibers in a metropolitan area has been operational for more than a year. Its constant development and expansion creates a solid foundation for heterogeneous architecture similar to the initial stages of Internet development.

This book aims at delivering a general overview of scientific foundations, theoretical and experimental results, and specific technological and engineering developments in quantum communication and cryptography demonstrated to date in university and government research laboratories around the world. The book is intended to serve as an introduction to the area of quantum information and, in particular, quantum communication and cryptography. The book is oriented towards graduate students in physics and engineering programs, research scientists, telecommunication engineers, and anybody who is enthusiastic about the power of quantum mechanics and who would be excited to learn about the emerging area of quantum optical communication.

The book opens with a brief history of conventional communication encoding and the appearance of quantum cryptography. Several fascinating experiments illustrating quantum information processing with entangled photons ranging from long-distance quantum key distribution in fiber to quantum teleportation of unknown state of light have been presented. These research efforts set a solid foundation for practical use of optical entanglement in quantum communication. Long-distance open-air quantum key distribution experiments have demonstrated the feasibility of extending quantum communication from the ground to a satellite and in between satellites in free space. The architecture of a currently operational metropolitan QKD network serving as the first heterogeneous quantum cryptography test-bed is described in detail. It is followed by the detailed theoretical analysis of practically meaningful security bounds. Several quantum communication protocols using continuous variables of nonclassical states of light are also presented. More complex applications of entangled states with few optical qubits are also described establishing building blocks for constructing linear-optical quantum computers and developing schemes for noise-immune quantum communications. This book was written by a group of physicists, engineers, and industrial scientists who are recognized leaders in the field of practical quantum information processing and quantum communication. References

provided at the end of each chapter could be used as a guide for more detailed investigation of specific technical and scientific problems associated with this rapidly growing and very exciting area of science and technology.

I hope you enjoy reading the book.

Alexander V. Sergienko

Editor

Alexander V. Sergienko (e-mail: *alexserg@bu.edu*; URL: *http://people.bu.edu/alexserg*) received his M.S. and Ph.D. degrees in physics from Moscow State University in 1981 and 1987, respectively. After spending the 1990–1991 academic year at the University of Maryland College Park as a visiting professor, he joined the University of Maryland Baltimore County as a research assistant professor in 1991. He was associated with the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland, as a guest researcher from 1992 to 1996.

In 1996, Professor Sergienko joined the faculty of the Department of Electrical and Computer Engineering at Boston University. He holds joint appointments in the Department of Electrical and Computer Engineering and in the Department of Physics. He is also a codirector of the Quantum Imaging Laboratory at Boston University. His research interests include quantum information processing including quantum cryptography and communications, quantum imaging, the development of novel optical-measurement and characterization techniques based on the use of nonclassical states of light (quantum metrology), the experimental study of the basic concepts of quantum mechanics, the study of fundamental optical interactions of light with matter including quantum surface effects, and ultrafast quantum optics. He pioneered the experimental development of practical quantum-measurement techniques using entangled-photon states in the early 1980s.

Professor Sergienko has published more than 200 research papers in the area of experimental nonlinear and quantum optics. He holds five patents in the fields of nonlinear and quantum optics. He is a fellow of the Optical Society of America, a member of the American Physical Society, and a member of the IEEE\LEOS.

Contributors

Markus Aspelmeyer
Institute for Experimental Physics
University of Vienna
Vienna, Austria

Institute for Quantum Optics and Quantum Information
Austrian Academy of Sciences
Vienna, Austria

Hannes R. Böhm
Institute for Experimental Physics
University of Vienna
Vienna, Austria

Warwick P. Bowen
Department of Physics
Australian National University
Canberra, Australia

Artur Ekert
Department of Applied Mathematics and Theoretical Physics
University of Cambridge
Cambridge, United Kingdom

Chip Elliott
BBN Technologies
Cambridge, Massachusetts

Alessandro Fedrizzi
Institute for Experimental Physics
University of Vienna
Vienna, Austria

James D. Franson
Applied Physics Laboratory
Johns Hopkins University
Laurel, Maryland

Sara Gasparoni
Institute for Experimental Physics
University of Vienna
Vienna, Austria

Gerald Gilbert
Quantum Information Science Group, MITRE
Eatontown, New Jersey

Nicolas Gisin
Group of Applied Physics
University of Geneva
Geneva, Switzerland

P.M. Gorman
QinetiQ
Malvern, United Kingdom

M. Halder
Ludwig Maximilians University Munich
Munich, Germany

Group of Applied Physics
University of Geneva
Geneva, Switzerland

M. Hamrick
Quantum Information Science Group, MITRE
Eatontown, New Jersey

S. Iblisdir
Group of Applied Physics
University of Geneva
Geneva, Switzerland

B.C. Jacobs
Applied Physics Laboratory
Johns Hopkins University
Laurel, Maryland

Thomas D. Jennewein
Institute for Quantum Optics and
Quantum Information
Austrian Academy of Sciences
Vienna, Austria

Natalia Korolkova
Friedrich Alexander University
of Erlangen-Nürnberg
Erlangen, Germany

School of Physics and Astronomy
University of St. Andrews
St. Andrews, Scotland

Christian Kurtsiefer
Ludwig Maximilians University
Munich
Munich, Germany

National University of Singapore
Singapore

Ping Koy Lam
Department of Physics
Australian National University
Canberra, Australia

Andrew Matheson Lance
Department of Physics
Australian National University
Canberra, Australia

Gerd Leuchs
Friedrich Alexander University
of Erlangen-Nürnberg
Erlangen, Germany

Michael Lindenthal
Institute for Experimental Physics
University of Vienna
Vienna, Austria

S. Lorenz
Friedrich Alexander University
of Erlangen-Nürnberg
Erlangen, Germany

N. Lütkenhaus
Friedrich Alexander University
of Erlangen-Nürnberg
Erlangen, Germany

Gabriel Molina-Terriza
Institute for Experimental Physics
University of Vienna
Vienna, Austria

T.B. Pittman
Applied Physics Laboratory
Johns Hopkins University
Laurel, Maryland

Andreas Poppe
Institute for Experimental Physics
University of Vienna
Vienna, Austria

Timothy C. Ralph
Department of Physics
University of Queensland
Brisbane, Australia

John G. Rarity
Department of Electrical and
Electronic Engineering
University of Bristol
Bristol, United Kingdom

Kevin Resch
Institute for Experimental Physics
University of Vienna
Vienna, Austria

Bahaa E.A. Saleh
Quantum Imaging Laboratory
Department of Electrical and
Computer Engineering
Department of Physics
Boston University
Boston, Massachusetts

Barry C. Sanders
Department of Physics
and Astronomy
University of Calgary
Calgary, Alberta, Canada

Alexander V. Sergienko
Quantum Imaging Laboratory
Department of Electrical and
Computer Engineering
Department of Physics
Boston University
Boston, Massachusetts

Thomas Symul
Department of Physics
Australian National
University
Canberra, Australia

P.R. Tapster
QinetiQ
Malvern, United Kingdom

Malvin C. Teich
Quantum Imaging Laboratory
Department of Electrical and
Computer Engineering
Department of Physics
Boston University
Boston, Massachusetts

F.J. Thayer
Quantum Information Science
Group, MITRE
Eatontown, New Jersey

W. Tittel
Group of Applied Physics
University of Geneva
Geneva, Switzerland

Rupert Ursin
Institute for Experimental
Physics
University of Vienna
Vienna, Austria

Philip Walther
Institute for Experimental
Physics
University of Vienna
Vienna, Austria

Zachary D. Walton
Quantum Imaging Laboratory
Department of Electrical and
Computer Engineering
Department of Physics
Boston University
Boston, Massachusetts

Harald Weinfurter
Ludwig Maximilians University
Munich
Munich, Germany

Max-Planck-Institute for Quantum
Optics
Garching, Germany

P. Zarda
Ludwig Maximilians University
Munich
Munich, Germany

Max-Planck-Institute for Quantum
Optics
Garching, Germany

H. Zbinden
Group of Applied Physics
University of Geneva
Geneva, Switzerland

Anton Zeilinger
Institute for Experimental Physics
University of Vienna
Vienna, Austria

Institute for Quantum Optics and
Quantum Information
Austrian Academy of Sciences
Vienna, Austria

Contents

chapter 1

Quantum Cryptography

A. Ekert
University of Cambridge

Contents

> Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve...
>
> —Edgar Alan Poe, "A Few Words on Secret Writing," 1841

Abstract

Quantum cryptography offers new methods of secure communication. Unlike traditional classical cryptography, which employs various mathematical techniques to restrict eavesdroppers from learning the contents of encrypted messages, quantum cryptography is focused on the physics of information. The process of sending and storing information is always carried out by physical means, for example photons in optical fibers or electrons in electric current. Eavesdropping can be viewed as measurements on a physical object—in

this case the carrier of the information. What the eavesdropper can measure, and how, depends exclusively on the laws of physics. Using quantum phenomena, we can design and implement a communication system that can always detect eavesdropping. This is because measurements on the quantum carrier of information disturb it and so leave traces. What follows is a brief overview of the quest for constructing unbreakable ciphers, from classical to quantum.

1.1 Classical Origins

Human desire to communicate secretly is at least as old as writing itself and goes back to the beginnings of civilization. Methods of secret communication were developed by many ancient societies, including those of Mesopotamia, Egypt, India, China, and Japan, but details regarding the origins of cryptology, i.e., the science and art of secure communication, remain unknown.

We know that it was the Spartans, the most warlike of the Greeks, who pioneered cryptography in Europe. Around 400 B.C. they employed a device known as the scytale (Figure 1.1). The device, used for communication between military commanders, consisted of a tapered baton around which was wrapped a spiral strip of parchment or leather containing the message. Words were then written lengthwise along the baton, one letter on each revolution of the strip. When unwrapped, the letters of the message appeared scrambled

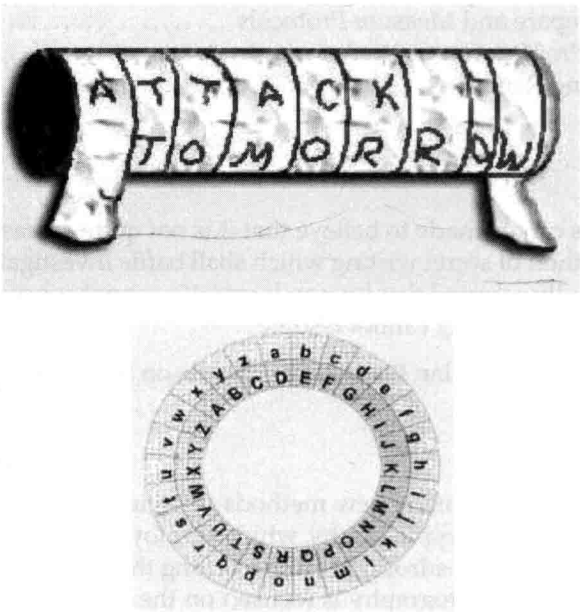

Figure 1.1 Scytale (top) and Alberti's disk (bottom) were the first cryptographic devices implementing permutations and substitutions, respectively.

and the parchment was sent on its way. The receiver wrapped the parchment around another baton of the same shape and the original message reappeared.

In his correspondence, Julius Caesar allegedly used a simple letter substitution method. Each letter of Caesar's message was replaced by the letter that followed it alphabetically by three places. The letter A was replaced by D, the letter B by E, and so on. For example, the English word COLD after the Caesar substitution appears as FROG. This method is still called the Caesar cipher, regardless of the size of the shift used for the substitution.

These two simple examples already contain the two basic methods of encryption which are still employed by cryptographers today, namely, *transposition* and *substitution*. In transposition (scytale) the letters of the *plaintext*, the technical term for the message to be transmitted, are rearranged by a special permutation. In substitution (Caesar's cipher) the letters of the plaintext are replaced by other letters, numbers or arbitrary symbols. The two techniques can be combined to produce more complex ciphers.

Simple substitution ciphers are easy to break. For example, the Caesar cipher with 25 letters admits any shift between 1 and 25, so it has 25 possible substitutions (or 26 if you allow the zero shift). One can easily try them all, one by one. The most general form of one-to-one substitution, not restricted to the shifts, can generate

$$26! \quad \text{or} \quad 403,291,461,126,605,635,584,000,000 \tag{1.1}$$

possible substitutions. And yet, ciphers based on one-to-one substitutions, also known as monoalphabetic ciphers, can be easily broken by frequency analysis. The method was proposed by the ninth-century polymath from Baghdad, Al-Kindi (800–873 A.D.), often called the philosopher of the Arabs.

Al-Kindi noticed that if a letter in a message is replaced with a different letter or symbol then the new letter will take on all the characteristics of the original one. A simple substitution cipher cannot disguise certain features of the message, such as the relative frequencies of the different characters. Take the English language: the letter E is the most common letter, accounting for 12.7% of all letters, followed by T (9.0%), then A (8.2%) and so on. This means that if E is replaced by a symbol X, then X will account for roughly 13% of symbols in the concealed message, thus one can work out that X actually represents E. Then we look for the second most frequent character in the concealed message and identify it with the letter T, and so on. If the concealed message is sufficiently long then it is possible to reveal its content simply by analyzing the frequency of the characters.

1.2 *Le Chiffre Indéchiffrable*

In the fifteenth and sixteenth centuries, monoalphabetic ciphers were gradually replaced by more sophisticated methods. At the time, Europe, Italy in particular, was a place of turmoil, intrigue, and struggle for political and financial power, and the cloak-and-dagger atmosphere was ideal for cryptography to flourish.

In the 1460s Leone Battista Alberti (1404–1472), better known as an architect, invented a device based on two concentric discs that simplified the use of Caesar ciphers. The substitution, i.e., the relative shift of the two alphabets, is determined by the relative rotation of the two disks (Figure 1.1).

Rumor has it that Alberti also considered changing the substitution within one message by turning the inner disc in his device. It is believed that this is how he discovered the so-called polyalphabetic ciphers, which are based on superpositions of Caesar ciphers with different shifts. For example, the first letter in the message can be shifted by 7, the second letter by 14, the third by 19, the fourth again by 7, the fifth by 14, the sixth by 19, and so on repeating the shifts 7, 14, 19 throughout the whole message. The sequence of numbers — in this example 7, 14, 19 — is usually referred to as a cryptographic key. Using this particular key we transform the message SELL into its concealed version, which reads ZSES.

As said, the message to be concealed is called the plaintext; the operation of disguising it is known as encryption. The encrypted plaintext is called the ciphertext or cryptogram. Our example illustrates the departure from a simple substitution; the repeated L in the plaintext SELL is enciphered differently in each case. Similarly, the two S's, in the ciphertext represent different letters in the plaintext: the first S corresponds to the letter E and the second to the letter L. This makes the straightforward frequency analysis of characters in ciphertexts obsolete. Indeed, polyalphabetic ciphers invented by the main contributors to the field at the time, such as Johannes Trithemius (1462–1516), Blaise de Vigenre (1523–1596), and Giovanni Battista Della Porta (1535–1615), were considered unbreakable for at least another 200 years. Indeed, Vigenre himself confidently dubbed his invention "le chiffre indéchiffrable" — the unbreakable cipher.

1.3 Not So Unbreakable

The first description of a systematic method of breaking polyalphabetic ciphers was published in 1863 by the Prussian colonel Friedrich Wilhelm Kasiski (1805–1881), but, according to some sources (for example, Simon Singh, *The Code Book*), Charles Babbage (1791–1871) had worked out the same method in private sometime in the 1850s.

The basic idea of breaking polyalphabetic ciphers is based on the observation that if we use N different substitutions in a periodic fashion then every Nth character in the cryptogram is enciphered with the same monoalphabetic cipher. In this case we have to find N, the length of the key and apply frequency analysis to subcryptograms composed of every Nth character of the cryptogram.

But how do we find N? We look for repeated sequences in the ciphertext. If a sequence of letters in the plaintext is repeated at a distance which is a multiple of N, then the corresponding ciphertext sequence is also repeated. For example, for N = 3, with the 7, 14, 19 shifts, we encipher TOBEORNOTTOBE