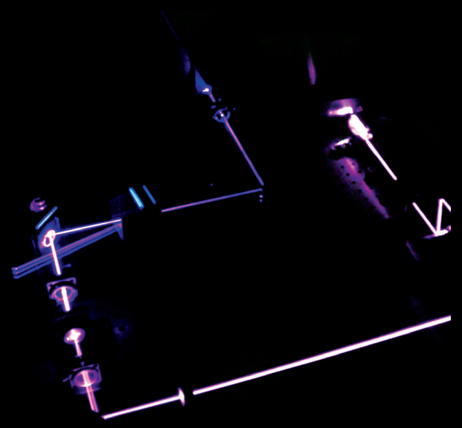
Electrical Engineering



All current methods of secure communication such as public-key cryptography can eventually be broken by faster computing. At the interface of physics and computer science lies a powerful solution for secure communications: quantum cryptography. Because eavesdropping changes the physical nature of the information, users in a quantum exchange can easily detect eavesdroppers. This allows for totally secure random key distribution, a central requirement for use of the one-time pad. Since the one-time pad is theoretically proven to be undecipherable, quantum cryptography is the key to perfect secrecy.

Quantum Communications and Cryptography is the first comprehensive review of the past, present, and potential developments in this dynamic field. Leading expert contributors discuss the scientific foundations, experimental and theoretical developments, and cutting-edge technical and engineering advances in quantum communications and cryptography from around the world.

The book describes the engineering principles and practical implementations in a real-world metropolitan network as well as physical principles and experimental results of such technologies as entanglement swapping and quantum teleportation. It also offers the first detailed treatment of quantum information processing with continuous variables. Technologies include both free-space and fiber-based communications systems along with the necessary protocols and information processing approaches.

Opening a new avenue toward perfect security, this revolutionary book…

- # Offers the first comprehensive, in-depth overview of the development and current state of the field
- @ Provides an overview of the history of quantum cryptography as well as future directions
- & Discusses the basics of quantum logic, entanglement, state sharing, and continuous polarization states
- * Presents the latest experimental results and theoretical developments together with practical implementations
- + Considers advanced applications such as free-space quantum cryptography and noise-immune key distribution

Quantum Communications and Cryptography bridges the gap between physics and engineering and supplies a springboard for further developments and advances in this rapidly growing area.

DK5859

ISBN 0-8493-3684-8

Taylor & Francis
Taylor & Francis Group
A CRC PRESS BOOK
www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

Sergienko

Quantum Communications and Cryptography

Quantum Communications and Cryptography

edited by
Alexander V. Sergienko

Taylor & Francis
Taylor & Francis Group

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 a scenario — the one-time pad protocol. It is based on the condition of sharing a secret random key material between two parties and its use 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 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 just anybody who is enthusiastic about the power of quantum mechanics and 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 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 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.

Sincerely,

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 co-director 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

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

Warwick P. Bowen
Department of Physics
The 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 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-Maximilian University
Munich, Germany

M. Hamricks
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 Jennewein
Institute for Quantum Optics and Quantum Information
Austrian Academy of Sciences
Vienna, Austria

Dr. Natalia Korolkova
School of Physics and Astronomy
University of St. Andrews, North Haugh
St. Andrews, Scotland

Christian Kurtsiefer
Ludwig-Maximilian University
Munich, Germany

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

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

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

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

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

N. Lutkenhaus
Friedrich-Alexander University of Erlangen-Nuremberg
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

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

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

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

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

Bahaa E.A. Saleh
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, Canada

Alexander V. Sergienko
Department of Electrical and Computer Engineering
Boston University
Boston, Massachusetts

Thomas Symul
Department of Physics
The Australian National University
Canberra, Australia

P.R. Tapster
QinetiQ
Malvern, United Kingdom

Malvin C. Teich
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

Zachary Walton
Department of Electrical and
Computer Engineering
Department of Physics
Boston University
Boston, Massachusetts

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

Harald Weinfurter
Ludwig-Maximilian University
Munich, Germany

P. Zarda
Ludwig-Maximilian University
Munich, Germany

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

Anton Zeilinger
Institute for Experimental Physics
University of Vienna
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

Au: pls. supply cite Figs. 1.1 and 1.2 in text.

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. 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 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 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

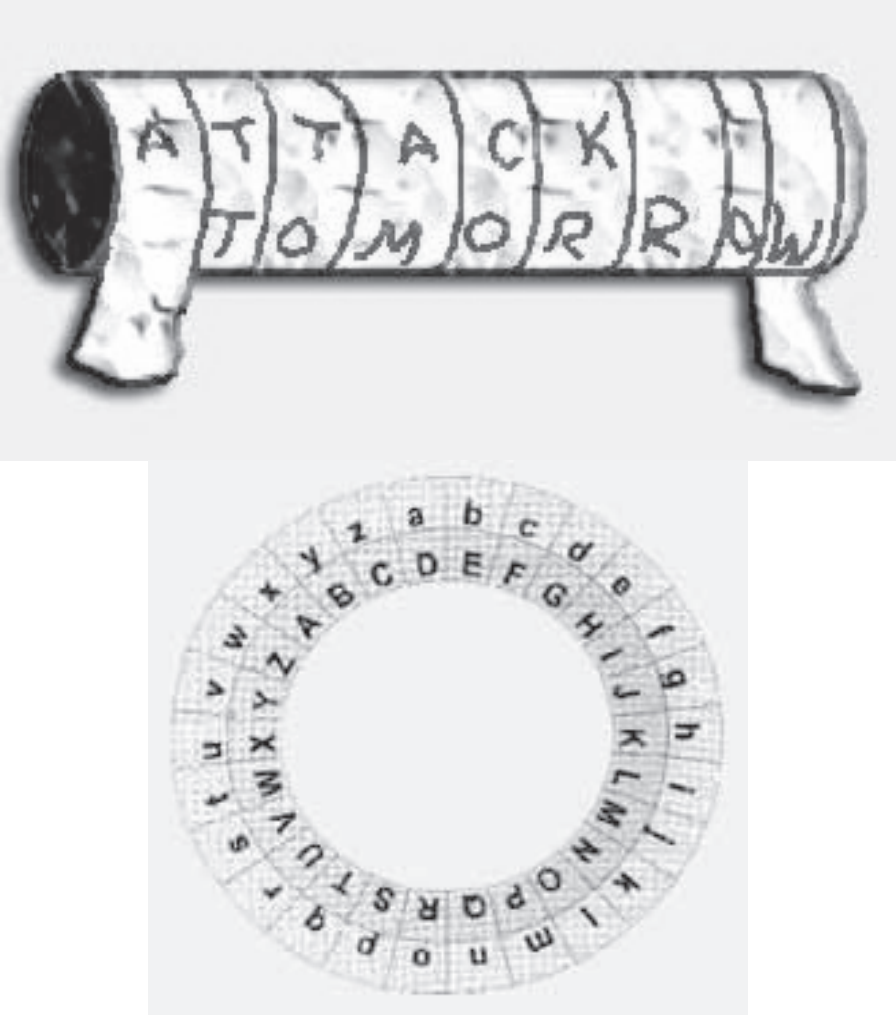


Figure 1.1 Scytale (left) and Alberti's disk (right) were the first cryptographic devices implementing permutations and substitutions, respectively.

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.

Rumour 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, 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 indechiffrable" — 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 as ACULCVUCMACUL:

T	O	B	E	O	R	N	O	T	T	O	B	E
A	C	U	L	C	V	U	C	M	A	C	U	L

The repeated sequence ACUL is a giveaway. The repetition appears at a distance 9; thus we can infer that possible values of N are 9 or 3 or 1. We can then apply frequency analysis to the whole cryptogram, to every third character and to every ninth character; one of them will reveal the plaintext. This trial and error approach becomes more difficult for large values of N, i.e., for very long keys.

In the 1920s, electromechanical technology transformed the original Alberti's disks into rotor machines in which an encrypting sequence with an extremely long period of substitutions could be generated, by rotating a

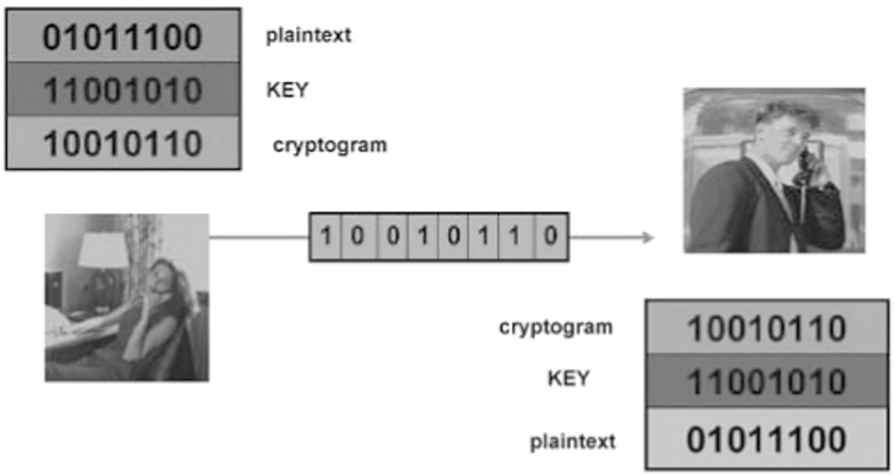


Figure 1.2 One-time pad.

sequence of rotors. Probably the most famous of them is the Enigma machine, patented by Arthur Scherbius in 1918.

A notable achievement of cryptanalysis was the breaking of the Enigma in 1933. In the winter of 1932, Marian Rejewski, a twenty-seven-year-old cryptanalyst working in the Cipher Bureau of the Polish Intelligence Service in Warsaw, mathematically determined the wiring of the Enigma's first rotor. From then on, Poland was able to read thousands of German messages encrypted by the Enigma machine. In July 1939 Poles passed the Enigma secret to French and British cryptanalysts. After Hitler invaded Poland and France, the effort of breaking Enigma ciphers continued at Bletchley Park in England. A large Victorian mansion in the centre of the park (now a museum) housed the Government Code and Cypher School and was the scene of many spectacular advances in modern cryptanalysis.

1.4 Truly Unbreakable?

Despite its long history, cryptography only became part of mathematics and information theory in the late 1940s, mainly as a result of the work of Claude Shannon (1916–2001) of Bell Laboratories in New Jersey. Shannon showed that truly unbreakable ciphers do exist and, in fact, they had been known for over 30 years. They were devised in about 1918 by an American Telephone and Telegraph engineer, Gilbert Vernam, and, Major Joseph Mauborgne of the US Army Signal Corps. They are called by one-time pads or Vernam ciphers.

Both the original design of the one-time pad and the modern version of it are based on the binary alphabet. The plaintext is converted to a sequence of 0's and 1's, using some publicly known rule. The key is another sequence of 0's and 1's of the same length. Each bit of the plaintext is then combined with the respective bit of the key, according to the rules of addition in base 2:

$$0+0=0, \qquad 0+1=1+0=1, \qquad 1+1=0. \tag{1.2}$$

The key is a random sequence of 0's and 1's, and therefore the resulting cryptogram, the plaintext plus the key, is also random and completely scrambled unless one knows the key. The plaintext can be recovered by adding (in base 2 again) the cryptogram and the key.

In the example above, the sender, traditionally called Alice, adds each bit of the plaintext (01011100) to the corresponding bit of the key (11001010) obtaining the cryptogram (10010110), which is then transmitted to the receiver, traditionally called Bob. Both Alice and Bob must have exact copies of the key beforehand; Alice needs the key to encrypt the plaintext, Bob needs the key to recover the plaintext from the cryptogram. An eavesdropper, called Eve, who has intercepted the cryptogram and knows the general method of encryption but not the key, will not be able to infer anything useful about the original message. Indeed, Shannon proved that if the key is secret, the same length

as the message, truly random, and never reused, then the one-time pad is unbreakable. Thus we do have unbreakable ciphers.

1.5 Key Distribution Problem

There is, however, a snag. All one-time pads suffer from a serious practical drawback, known as the key distribution problem. Potential users have to agree secretly and in advance on the key, a long, random sequence of 0's and 1's. Once they have done this, they can use the key for enciphering and deciphering, and the resulting cryptograms can be transmitted publicly, for example, broadcasted by radio, posted on the Internet, or printed in a newspaper, without compromising the security of the messages. But the key itself must be established between the sender and the receiver by means of a secure channel — for example, a secure telephone line, or via a private meeting or hand delivery by a trusted courier.

Such a secure channel is usually available only at certain times and under certain circumstances. So users far apart, in order to guarantee perfect security of subsequent cryptocommunication, have to carry around with them an enormous amount of secret and meaningless information (cryptographic keys), equal in volume to all the messages they might later wish to send. This is, to say the least, not very convenient.

Furthermore, even if a secure channel is available, this security can never be truly guaranteed. A fundamental problem remains because, in principle, any classical private channel can be monitored passively, without the sender or receiver knowing that the eavesdropping has taken place. This is because classical physics — the theory of ordinary-scale bodies and phenomena such as paper documents, magnetic tapes, and radio signals — allows all physical properties of an object to be measured without disturbing those properties. Since all information, including cryptographic keys, is encoded in measurable physical properties of some object or signal, classical theory leaves open the possibility of passive eavesdropping, because in principle it allows the eavesdropper to measure physical properties without disturbing them. This is not the case in quantum theory, which forms the basis for quantum cryptography. However, before we venture into quantum physics, let us mention in passing a beautiful mathematical approach to solving the key distribution problem.

The 1970s brought a clever mathematical discovery in the shape of "public-key" systems. The two main public-key cryptography techniques in use today are the Diffie–Hellman key exchange protocol [13] and the RSA encryption system (named after the three inventors, Ron Rivest, Adi Shamir, and Leonard Adleman) [24]. They were discovered in the academic community in 1976 and 1978, respectively. However, it was widely rumoured that these techniques were known to British government agencies prior to these dates, although this was not officially confirmed until recently. In fact, the techniques were first discovered at the British Government Communication Headquarters in

the early 1970s by James Ellis, who called them nonsecret encryption. In 1973, building on Ellis' idea, C. Cocks designed what we now call RSA, and in 1974 M. Williamson proposed what is essentially known today as the Diffie–Hellman key exchange protocol.

In the public-key systems, users do not need to agree on a secret key before they send the message. They work on the principle of a safe with two keys, one public key to lock it, and another private one to open it. Everyone has a key to lock the safe but only one person has a key that will open it again, so anyone can put a message in the safe but only one person can take it out. The systems avoid the key distribution problem but unfortunately their security depends on unproven mathematical assumptions. For example, RSA — probably the most popular public key cryptosystem — derives its security from the difficulty of factoring large numbers. This means that if mathematicians or computer scientists come up with fast and clever procedures for factoring, the whole privacy and discretion of public-key cryptosystems could vanish overnight.

Indeed, we know that quantum computers can, at least in principle, efficiently factor large integers [19]. Thus in one sense public-key cryptosystems are already insecure: any RSA-encrypted message that is recorded today will become readable moments after the first quantum computer is switched on, and therefore RSA cannot be used for securely transmitting any information that will still need to be secret on that happy day. Admittedly, that day is probably decades away, but can anyone prove, or give any reliable assurance, that it is? Confidence in the slowness of technological progress is all that the security of the RSA system now rests on.

1.6 Local Realism and Eavesdropping

We shall now leave mathematics and enter the world of quantum physics. Physicists view key distribution as a physical process associated with sending information from one place to another. From this perspective, eavesdropping is a set of measurements performed on carriers of information. In order to avoid detection, an eavesdropper wants to learn about the value of a physical property that encodes information without disturbing it. Is such a passive measurement always possible?

In 1935 Albert Einstein together with Boris Podolsky and Nathan Rosen (EPR) published a paper in which they outlined how a "proper" fundamental theory of nature should look [15]. The EPR programme required completeness ("In a complete theory there is an element corresponding to each element of reality") and locality ("The real factual situation of the system A is independent of what is done with the system B, which is spatially separated from the former") and defined the element of physical reality as "If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity." In other words, if we can know the value of some physical property without "touching" the system in any way, then the property

must be physically real, i.e., it must have a determinate value, even before we measure it.

This world view is known as "local realism" and it implies possibilities of perfect eavesdropping. Indeed, this is exactly what the EPR definition of the element of reality means in the cryptographic context.

Einstein and his colleagues considered a thought experiment, on two entangled particles, that showed that quantum states cannot in all situations be complete descriptions of physical reality. The EPR argument, as subsequently modified by David Bohm [9], goes as follows. Imagine the singlet-spin state of two spin $\frac{1}{2}$ particles

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle\right), \tag{1.3}$$

where the single particle kets $|\uparrow\rangle$ and $|\downarrow\rangle$ denote spin up and spin down with respect to some chosen direction. This state is spherically symmetric, and the choice of direction does not matter. The two particles, which we label A and B, are emitted from a source and fly apart. After they are sufficiently separated so that they do not interact with each other, we can predict with certainity the x component of spin of particle A by measuring the x component of spin of particle B. Each measurement on B, in $\frac{1}{2}\hbar$ units, can yield two results, $+1$ (spin up) and -1 (spin down) and reveals the value of the x component of A. This is because the total spin of the two particles is zero, and the spin components of the two particles must have opposite values. The measurement performed on particle B does not disturb particle A (by locality) so the x component of spin is an element of reality according to the EPR criterion. By the same argument and by the spherical symmetry of state $|\Psi\rangle$ the y, z, or indeed any other spin components are also elements of reality. Therefore all the spin components must have predetermined values $+1$ or -1.

Local realism has experimental consequences. Consider two pairs of spin components, A_1 and A_2 pertaining to the particle A, and B_1 and B_2 pertaining to the particle B. A_1, A_2, B_1, and B_2 all have simultaneous definite values, either $+1$ or -1. Hence the quantity

$$Q = A_1(B_1 - B_2) + A_2(B_1 + B_2) \tag{1.4}$$

can have two different values, either -2 or $+2$, and consequently,

$$-2 \leq \langle Q \rangle \leq 2, \tag{1.5}$$

where $\langle Q \rangle$ stands for the average value of Q. This inequality is known as the Bell inequality [3] or more precisely as the CHSH inequality [11].

Both quantum-mechanical predictions and experiments show that, for two particles in the singlet state, $\langle AB \rangle = -\vec{a} \cdot \vec{b}$, where $\vec{a}$ and $\vec{b}$ are the unit vectors specifying the directions of the spin components of particles A and B, respectively. This leads to a violation of the CHSH inequality [1.5]. For if we choose $\vec{a}_i$ and $\vec{b}_j$ in the x–y plane, perpendicular to the trajectory of the particles emitted from the source, and characterized by the azimuthal angles $\phi_1^a = 0$, $\phi_2^a = \frac{1}{2}\pi$, and $\phi_1^b = \frac{1}{4}\pi$, $\phi_2^b = \frac{3}{4}\pi$ then $\langle Q \rangle = -2\sqrt{2}$. Local realism

is refuted, which opens possibilities of constructing key distribution schemes that will always detect eavesdropping.

Please note that any theory that refutes local realism,, be it quantum or postquantum, opens such possibilities. Even if quantum mechanics is refuted sometime in the future and a new physical theory is conjectured, as long as the new theory refutes local realism, possibilities for postquantum cryptography are wide open.

1.7 Quantum Key Distribution

1.7.1 Entanglement Based Protocols

Let us take advantage of the CHSH inequality within the quantum theory. The key distribution is performed via a quantum channel that consists of a source that emits pairs of spin $\frac{1}{2}$ particles in the singlet state as in Eq. (1.3). The particles fly apart along the z-axis toward the two legitimate users of the channel, Alice and Bob, who, after the particles have separated, perform measurements and register spin components along one of three directions, given by unit vectors $\vec{a}_i$ and $\vec{b}_j (i,\ j = 1, 2, 3)$, respectively, for Alice and Bob. For simplicity, both $\vec{a}_i$ and $\vec{b}_j$ vectors lie in the x–y plane, perpendicular to the trajectory of the particles, and are characterized by azimuthal angles: $\phi_1^a = 0$, $\phi_2^a = \frac{1}{4}\pi$, $\phi_3^a = \frac{1}{2}\pi$ and $\phi_1^b = \frac{1}{4}\pi$, $\phi_2^b = \frac{1}{2}\pi$, $\phi_3^b = \frac{3}{4}\pi$. Superscripts a and b refer to Alice's and Bob's analyzers, respectively, and the angle is measured from the vertical x-axis. The users choose the orientation of the analyzers randomly and independently for each pair of incoming particles. Each measurement can yield two results, $+1$ (spin up) and -1 (spin down) and can reveal one bit of information.

After the transmission has taken place, Alice and Bob can announce in public the orientations of the analyzers they have chosen for each particular measurement and divide the measurements into two separate groups: a first group for which they used different orientations of the analyzers and a second group for which they used the same orientation of the analyzers. They discard all measurements in which either or both of them failed to register a particle at all. Subsequently Alice and Bob can reveal publicly the results they obtained, but within the first group of measurements only. This allows them to establish the value of $\langle Q \rangle$, which if the particles were not directly or indirectly "disturbed" should be very close to $-2\sqrt{2}$. This assures the legitimate users that the results they obtained within the second group of measurements are anticorrelated and can be converted into a secret string of bits — the key.

An eavesdropper, Eve, cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The information "comes into being" only after the legitimate users perform measurements and communicate in public afterwards. Eve may try to substitute her own prepared data for Alice and Bob to misguide them, but as she does not know which orientation of the

analyzers will be chosen for a given pair of particles, there is no good strategy to escape being detected. In this case her intervention will be equivalent to introducing elements of *physical reality* to the spin components and will lower $\langle Q \rangle$ below its "quantum" value.

1.7.2 Prepare and Measure Protocols

Instead of tuning into an external source of entangled particles, Alice and Bob may also rely on the Heisenberg uncertainty principle. Suppose a spin $\frac{1}{2}$ particle is prepared in one of the four states, say spin up and down along the vertical x-axis ($|\uparrow\rangle$, $|\downarrow\rangle$) and spin up and down along the horizontal y-axis ($|\rightarrow\rangle$, $|\leftarrow\rangle$). Then the two x states $|\uparrow\rangle$ and $|\downarrow\rangle$ can be distinguished by one measurement and the two y states $|\rightarrow\rangle$ and $|\leftarrow\rangle$ by another measurement. The measurement that can distinguish between the two x states will give completely random outcome, when applied to distinguish between the two y states and vice versa. If, for each incoming particle, the receiver performing the measurement is not told in advance which type of spin (x or y) was prepared by the sender, then the receiver is completely lost and unable to determine the spin value. This can be used for the key distribution.

Alice and Bob agree on the bit encoding, e.g., $|\uparrow\rangle = 0 = |\rightarrow\rangle$, $|\downarrow\rangle = 1 = |\leftarrow\rangle$, and Alice repeatedly prepares one of the four quantum states, choosing randomly out of $|\uparrow\rangle$, $|\downarrow\rangle$, $|\rightarrow\rangle$, and $|\leftarrow\rangle$. She then sends it to Bob, who randomly chooses to measure either the x or the y spin component. After completing all the measurements, Alice and Bob discuss their data in public so that anybody can listen, including their adversary Eve. Bob tells Alice which spin component he measured for each incoming particle and she tells him "what should have been measured." Alice does not disclose which particular state she prepared, and Bob does not reveal the outcome of the measurement, so the actual values of bits are still secret. Alice and Bob then discard those results in which Bob failed to detect a particle and those for which he made measurements of wrong type. They then compare a large subset of the remaining data. Provided no eavesdropping has taken place, the result should be a shared secret that can be interpreted by both Alice and Bob as a binary key.

But let us suppose there is an eavesdropper, Eve. Eve does not know in advance which state will be chosen by Alice to encode a given bit. If she measures this bit and resends it to Bob, this may create errors in Bob's readings. Therefore in order to complete the key distribution Alice and Bob have to test their data for discrepancies. They compare in public some randomly selected readings and estimate the error rate; if they find many discrepancies, they have reason to suspect eavesdropping and should start the whole key distribution from scratch. If the error rate is negligibly small, they know that the data not disclosed in the public comparison form a secret key. No matter how complex and subtle is the advanced technology and computing power available to the eavesdropper, the "quantum noise" caused inevitably by each act of tapping will expose each attempt to gain even partial information about the key.

1.8 Security Proofs

Admittedly the key distribution procedures described above are somewhat idealized. The problem is that there is in principle no way of distinguishing noise due to an eavesdropper from innocent noise due to spurious interactions with the environment, some of which are presumably always present. All good quantum key distribution protocols must be operable in the presence of noise that may or may not result from eavesdropping. The protocols must specify for which values of measurable parameters Alice and Bob can establish a secret key and provide a physically implementable procedure that generates such a key. The design of the procedure must take into account that an eavesdropper may have access to unlimited quantum computing power.

The best way to analyze eavesdropping in the system is to adopt the entanglement based protocol and the scenario that is most favorable for eavesdropping, namely that Eve herself is allowed to prepare and deliver all the pairs that Alice and Bob will subsequently use to establish a key. This way we take the most conservative view, which attributes all disturbance in the channel to eavesdropping, even though most of it (if not all) may be due to innocent environmental noise. This approach also applies to the prepare and measure protocols because they can be viewed as special cases of entanglement based protocols, e.g., the source of entangled particles can be given either to Alice or to Bob. It is prudent to assume that Eve has disproportional technological advantage over Alice and Bob. She may have access to unlimited computational power, including quantum computers; she may monitor all the public communication between Alice and Bob in which they reveal their measurement choices and exchange further information in order to correct errors in their shared key and to amplify its privacy. In contrast, Alice and Bob can only perform measurements on individual qubits and communicate classically over a public channel. They do not have quantum computers, or any sophisticated quantum technology, apart from the ability to establish a transmission over a quantum channel.

Search for good security criteria under such stringent conditions led to early studies of quantum eavesdropping [17,28] and finally to the first proof of the security of key distribution [12]. The original proof showed that the entanglement based key distributions are indeed secure and noise-tolerant against an adversary with unlimited computing power as long as Alice and Bob can implement quantum privacy amplification. In principle, quantum privacy amplification allows us to establish a secure key over any distance, using entanglement swapping [29] in a chain of quantum repeaters [2,14]. However, this procedure, which distils pure entangled states from corrupted mixed states of two qubits, requires a small-scale quantum computation. Subsequent proofs by Inamori [21] and Ben-Or [4] showed that Alice and Bob can also distill a secret key from partially entangled particles using only classical error correction and classical privacy amplification [6,7].

Quantum privacy amplification was also used by Lo and Chau to prove the security of the prepare and measure protocols over an arbitrary

distance [22]. A concurrent proof by Mayers showed that the protocol can be secure without Alice and Bob having to rely on the use of quantum computers [23]. The same conclusion, but using different techniques, was subsequently reached by Biham et al. [8]. Although the two proofs did not require quantum privacy amplification, they were rather complex. A nice fusion of quantum privacy amplification and error correction was proposed by Peter Shor and John Preskill, who formulated a relatively simple proof of the security of the BB84 [5] protocol based on virtual quantum error correction [25]. They showed that a protocol that employs quantum error-correcting code to prevent Eve from becoming entangled with qubits that are used to generate the key reduces to the BB84 augmented by classical error correction and classical privacy amplification. This proof has been further extended by Gottesman and Lo [20] for two-way public communication to allow for a higher bit error rate in BB84 and by Tamaki et al. [26] to proof the security of the B92 protocol. More recently, another simple proof of the BB84, which employs results from quantum communication complexity, has been provided by Ben-Or [4].

Let us also mention in passing that apart from the scenario that favors Eve, i.e., Eve has access to quantum computers while Alice and Bob do not, there are interesting connections regarding the criteria for the key distillation in commensurate cases, i.e., when Alice, Bob, and Eve have access to the same technology, be it classical or quantum [18,10,1].

1.9 Concluding Remarks

Quantum cryptography was discovered independently in the U.S. and Europe. The first one to propose it was Stephen Wiesner, then at Columbia University in New York, who, in the early 1970s introduced the concept of quantum conjugate coding [27]. He showed how to store or transmit two messages by encoding them in two "conjugate observables" such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. He illustrated his idea with a design of unforgeable bank notes. A decade later, building upon this work, Charles H. Bennett of the IBM T. J. Watson Research Center and Gilles Brassard of the Université de Montral, proposed a method for secure communication based on Wiesner's conjugate observables [5]. In 1990, independently and initially unaware of the earlier work, the current author, then a Ph.D. student at the University of Oxford, discovered and developed a different approach to quantum cryptography based on peculiar quantum correlations known as quantum entanglement [16]. Since then, quantum cryptography has evolved into a thriving experimental area and is quickly becoming a commercial proposition.

This brief overview has only scratched the surface of the many activities that are presently being pursued under the heading of quantum cryptography. It is focused solely on the development of theoretical concepts led to creating unbreakable quantum ciphers. The experimental developments, although equally fascinating, are left to the other contributors to this book. I have also omitted many interesting topics in quantum cryptography that go

beyond the key distribution problem. Let me stop here hoping that even the simplest outline of quantum key distribution has enough interesting physics to keep you entertained for a while.

References

1. A. Acin, N. Gisin, and V. Scarani, Security bounds in quantum cryptography using d-level systems, *Quant. Inf. Comp.*, 3(6), 563–580, November 2003.
2. H. Aschauer and H.-J. Briegel, A security proof for quantum cryptography based entirely on entanglement purification, *Physical Review A*, 66, 032302, 2002.
3. J.S. Bell, *Physics*, 1, 195, 1964.
4. M. Ben-Or, Simple security proof for quantum key distribution. On-line presentation available at http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/index.html.
5. C.H. Bennett and G. Brassard, Quantum cryptography, public key distribution and coin tossing, in *Proceedings of International Conference on Computer Systems and Signal Processing*, 1984, p. 175.
6. C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, Generalized privacy amplification, *IEEE Transactions on Information Theory*, 41(6), 1915–1923, 1995.
7. C.H. Bennett, G. Brassard, and J.-M. Robert, Privacy amplification by public discusion. *SIAM Journal on Computing*, 17(2), 210–229, 1988.
8. E. Biham, M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury, A proof of the security of quantum key distribution, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC)*, ACM Press, New York, 2000, p. 715. quant-ph/9912053.
9. D. Bohm, *Quantum Theory*, New York: Prentice Hall, 1951.
10. D. Bruss, M. Christandl, A. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello, Tomographic quantum cryptography: equivalence of quantum and classical key distillation, *Phys. Rev. Lett.*, 91, 097901, 2003. quant-ph/0303184.
11. J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, *Phys. Rev. Lett.*, 23, 880, 1969.
12. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noisy channels, *Phys. Rev. Lett.*, 77, 2818–2821, 1996. Erratum, ibid., 80, 2022–2022, 1998, quant-ph/9604039.
13. W. Diffie and M.E Hellman, *IEEE Trans. Inf. Theory*, IT-22, 644, 1976.
14. W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Quantum repeaters based on entanglement purification, *Phys. Rev. A*, 59, 169–181, 1999.
15. A. Einstein, B. Podolski, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47, 777, 1935.
16. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.*, 67(6), 661, 1991.
17. A.K. Ekert and B. Huttner, Eavesdropping techniques in quantum cryptosystems, *Journal of Modern Optics*, 41, 2455–2466, 1994. Special issue on Quantum Communication.
18. N. Gisin and S. Wolf, in *Advances in Cryptology — CRYPTO'00*, Lecture Notes in Computer Science, Springer–Verlag, 2000, pp. 482–500.
19. S. Goldwasser, ed., *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA, 1994.

20. D. Gottesmann and H.-K. Lo., Proof of security of quantum key distribution with two-way classical communication, *IEEE Trans. Inf. Th.*, 49(2), 457–475, 2003, quant-ph/0105121.
21. H. Inamori, Security of EPR-based quantum key distribution, quant-ph/0008064.
22. H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science*, 283(5410), 2050–2056, 1999.
23. D. Mayers, Unconditional security in quantum cryptography, quant-ph/9802025, 1998.
24. R. Rivest, A. Shamir, and L. Adleman, On digital signatures and public-key cryptosystems, Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, January 1979.
25. P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, *Phys. Rev. Lett.*, 85(2), 441–444, 2000; quant-ph/0003004.
26. K. Tamaki, M. Koashi, and N. Imoto, Unconditionally secure key distribution based on two nonorthogonal states, *Phys. Rev. Lett.*, 90, 167904, 2003.
27. S. Wiesner, Conjugate coding, *Sigact News*, 15(1), 78–88, 1983; Originally written c. 1970 but them unpublished.
28. A.C.-C. Yao, Security of quantum protocols against coherent measurements, in *Proceedings of the 27th ACM Symposium on the Theory of Computing*, ACM Press, 1995, pp. 67–75.
29. M. Zukowski, A. Zeilinger, M. Horne, and A.K. Ekert, Event-ready detectors, Bell experiment via entanglement swapping, *Physical Review Letters*, 71, 4287–4290, 1993.