Quantum Key Distribution via BB84
An Advanced Lab Experiment

Matthias Scholz

November 27, 2007

1 Introduction

Electronic communication has become one of the main pillars of modern society and their ongoing boom requires the development of new methods and techniques to secure data transmission. This has been the goal since the onset of cryptography in ancient times. Cryptography may be defined as the art of writing (encryption) and deciphering (decryption) messages in code in order to ensure their confidentiality, authenticity, integrity, and non-repudiation.
However, current cryptography implementations provide only conditional security, relying on limited computational and technological capabilities of the opponent.
This advanced-lab experiment presents the scheme for performing cryptography with unconditional security, based on fundamental laws of physics.
In chapter 2 cryptography basics will be introduced in order to understand the weakness of "public key cryptography" – mostly used for authentication today, e.g. in internet protocols – and the solution quantum mechanics provides by using "quantum key distribution" (QKD). The quantum approach will be detailed by describing the theory of "BB84", the most widely applied quantum communication protocol (named after Charles Bennett and Gilles Brassard).
Chapter 3 will introduce the experimental setup that will be used during the lab course. Finally, chapter 4 contains some suggestions how to use the setup.

An online version of this manuscript can be found at
`http://nano.physik.hu-berlin.de/teaching/Praktikum/Praktikum.htm`.

2 From Classical to Quantum Cryptography

2.1 Classical Cryptography Today

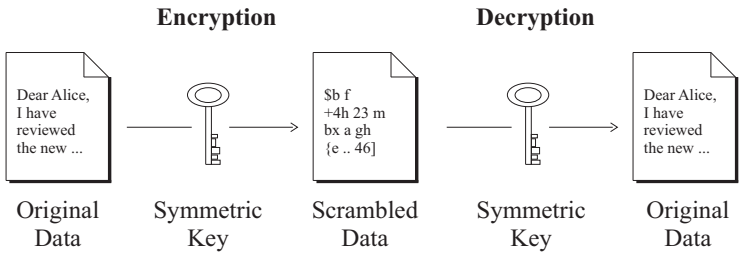
2.1.1 History

Nowadays, secure communication has become such a common thing that people are barely aware of it when dealing with electronic shopping, bank account management or e-mail transmission. Examples of secret codes range back to the times of the ancient Egyptians who used modified hieroglyphs to conceal their messages. Since then, cryptography has become the art of transmitting a ciphered message from a sender (usually called Alice) to a receiver (usually called Bob), allowing no one else to eavesdrop.
Another easy cipher was introduced by Cesar to communicate secretly with his legions, substituting each letter of a message advancing by three letters. Thus, his famous sentence "Veni, vidi, vici!" would become "Yhql, Ylgl, Ylfl!".
The two world wars of the 20th century accelerated the development of new cryptographic techniques. In 1917, Gilbert S. Vernam proposed an unbreakable cryptosystem, called the Vernam cipher or One-Time Pad [1]. The One-Time Pad is a generalization of the substitution cipher that advances each letter by a random number of positions in the alphabet. These random numbers then form a cryptographic key (as long as the message) that must be shared between the sender and recipient.
Even though the Vernam cipher offers unconditional security against adversaries possessing unlimited computational power and technological abilities (in case of single use and non-existing losses in the channel), it faces the problem of how to securely distribute the key itself.
A new surge of interest in cryptography was triggered by the upswing in electronic communications in the late 70s of the 20th century. It became essential to enable secure communication between users who have met never before and share no secret key. Thus, the question was how to distribute the key in a secure way. A solution was found by Whitfield Diffie and Martin E. Hellman who invented the concept of public-key distribution in 1976 [2]. The ease of use of public-key cryptography stimulated the boom of electronic commerce during the 1990s.

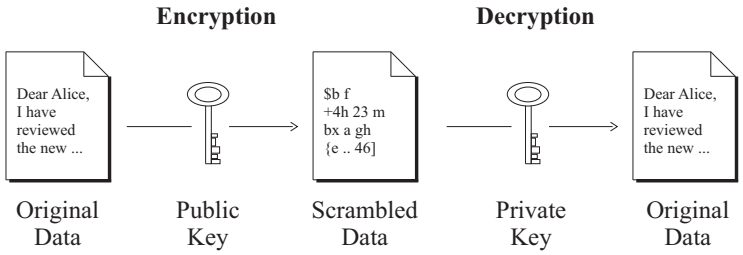
2.1.2 Public-Key Cryptography

Today, there are two types of cryptosystems: secret-key and public-key cryptography:

- In secret-key cryptography, also referred to as symmetric cryptography, the same key is used for both encryption and decryption.



- In public-key cryptography, each person gets a pair of keys, one called the public key and the other called the private key. Encryption is performed with the public key while decryption is done with the private key.



Public-Key Cryptography In public-key cryptography, the need for sender and receiver to share a secret key is eliminated. All communications involve only public keys, and no private key is ever transmitted or shared. Anyone can send a confidential message by using public information, but the message can only be decrypted with a private key which is in the sole possession of the intended recipient.
The weakness of this system is based on the fact that the private key is always linked mathematically to the public key. Therefore, it is always possible to attack a public-key system if the eavesdropping includes sufficiently large computational resources.
Therefore, the mathematical problem to derive the private from the public key must be as difficult as possible. For instance, the idea behind the RSA public-key protocol relies on the factorizing of large number. By now, no classical algorithm is known whose computational requirements scale less than exponentially with the size of the number to factorize.

RSA Public-Key Encryption RSA stands for Rivest, Shamir, and Adleman who invented this cryptosystem in 1977 [3]. Since then, it has become the most popular form of public-key cryptography. Its basic scheme is described in the following:

- Find two large integers P and Q that are prime.
- Compute $N = P \cdot Q$ (which is called the modulus).
- Choose an integer e such that e is less than $P \cdot Q$ and that e and $(P-1)(Q-1)$ are co-prime.
- Compute d such that $(d\,e - 1)$ is divisible by $(P-1)(Q-1)$.
- Choose (N, e) as the public key and (N, d) as the private key.

You derive the ciphered message C by calculating $C = T^e \bmod N$ and the deciphered message T by $T = C^d \bmod N$.

2.1.3 Public-Key Cryptography Weakness

The RSA system can be beaten [3]. The most damaging would be for an eavesdropper to discover the private key corresponding to a given public key. The obvious way is to factorize the public modulus N into its two prime factors P and Q which easily leads to the private key d.
It is currently difficult to factorize the product N of two large primes. As earlier mentioned, even the best available classical algorithm scales exponentially in computational resources with the size of N (which is called a non-efficient algorithm). An efficient algorithm (which scales polynomial) would place a huge danger to modern economics. (Actually, in many countries like the UK or the U.S. it is unlawful to publish such an idea.) Therefore, security relies on the fact that factorizing will take years with current algorithms and computational capabilities.

2.1.4 Secret-Key Cryptography

Secret-key cryptography can provide an unbreakable cipher which resists adversaries with unlimited computational and technological power. As an example, coding will be explained for the Vernam cipher that was cited before:
The Vernam cipher adds a random key to every message, the bits of the resulting string are also random and carry no information about the message. Thereby, message and key are added bitwise modulo 2 (equivalent to a XOR logic gate $\bigoplus$). Decryption is identical to encryption, since double modulo-2 addition yields identity.

Message	0 0 0 0 1 1 0 0 1 1 1 1
$\bigoplus$ Secret Key	0 0 1 1 0 1 1 0 0 1 0 1
= Cipher	0 0 1 1 1 0 1 0 1 0 1 0
$\bigoplus$ Secret Key	0 0 1 1 0 1 1 0 0 1 0 1
= Deciphered	0 0 0 0 1 1 0 0 1 1 1 1

For this system to be unconditionally secure, three requirements are imposed on the key:

1. The key must be as long as the message.
2. It must be purely random.
3. It may be used once and only once.

If any of these requirements is not fulfilled, the security of the system is jeopardized. For example, if the key randomness is generated by some known algorithm, one can easily find the key matching the cipher. If the key is used several times, statistical studying can help to uncover information about the key.
However, the main drawback of the Vernam cipher is the necessity to securely distribute a secret key as long as the message. Anyone who intercepts the key in transit can read, modify, and forge all messages encrypted with this key.

2.2 Quantum Cryptography

2.2.1 The Quantum Approach

The main problem of secret-key cryptosystems is secure distribution of keys. It is here that quantum mechanics offers a solution. While the security of public-key cryptographic methods can be undermined by advances in technology and mathematical algorithms, the quantum approach will provide "unconditional security". The security is guaranteed by Heisenberg's uncertainty principle which does not allow us to discriminate non-orthogonal states with certainty.
Within the framework of classical physics, it is impossible to reveal possible eavesdropping, because information encoded into any property of a classical object can be acquired without changing the state of the object. All classical signals can be monitored passively. In classical information, one bit of information is encoded in billions of photons, electrons, atoms, or other carriers. You can always deviate part of the signal and perform a measurement on it, whereas in quantum mechanics, any projective measurement will induce disturbances. Duplicating a quantum state and performing a measurement on one of the copies is also no alternative, as stated by the "no-cloning theorem" [4].

2.2.2 Protocol BB84

BB84 is the protocol most widely used for quantum key distribution; it was invented by Charles H. Bennet and Gilles Brassard in 1984 [5]. It allows two users to establish an identical and purely random sequence of bits at two different locations while allowing to reveal any eavesdropping.
In this advanced lab experiment, the BB84 protocol encodes single photon polarizations using two bases of the same 2–dimensional Hilbert space:

- rectilinear basis $\{0°\colon |\rightarrow\rangle,\ 90°\colon |\uparrow\rangle\}$
- diagonal basis $\{45°\colon |\nearrow\rangle,\ 135°\colon |\nwarrow\rangle\}$

The only requirement on the involved quantum states is actually that they belong to mutually non-orthogonal bases of their Hilbert space, where each

vector of one basis has equal-length projections onto all vectors of the other basis. If a measurement on a system is performed in a basis different from the one the system is prepared in, its outcome is completely random and the system looses all the memory of its previous state.
With the polarization states above, this condition is met:

- $|\nearrow\rangle = \frac{\sqrt{2}}{2}(|\rightarrow\rangle + |\uparrow\rangle$
- $|\nwarrow\rangle = \frac{\sqrt{2}}{2}(|\rightarrow\rangle - |\uparrow\rangle$
- $\langle\rightarrow|\uparrow\rangle = \langle\nearrow|\nwarrow\rangle = 0$
- $\langle\rightarrow|\rightarrow\rangle = \langle\uparrow|\uparrow\rangle = \langle\nwarrow|\nwarrow\rangle = \langle\nearrow|\nearrow\rangle = 1$
- $|\langle\nearrow|\rightarrow\rangle|^2 = |\langle\nearrow|\uparrow\rangle|^2 = |\langle\nwarrow|\rightarrow\rangle|^2 = |\langle\nwarrow|\uparrow\rangle|^2 = \frac{1}{2}$

Any measurement in the diagonal basis on photons prepared in the rectilinear basis will yield random outcomes with equal probabilities and vice versa. On the other hand, measurements performed in the basis identical to the basis of preparation of states will produce deterministic results.
To exchange a secret key in the BB84 protocol, Alice and Bob must do as follow:

- Alice creates a binary random number and sends it to Bob using randomly the two different bases + (rectilinear) and × (diagonal):

  - $|\rightarrow\rangle$ and $|\nearrow\rangle$ both represent 1
  - $|\uparrow\rangle$ and $|\nwarrow\rangle$ both represent 0

  Therefore, Alice transmits photons randomly in the four polarization states $|\rightarrow\rangle$, $|\uparrow\rangle$, $|\nearrow\rangle$, and $|\nwarrow\rangle$.

- Bob simultaneously measures the polarization of the incoming photons using randomly the two different bases. He does not know which of his measurements are deterministic, i.e. measured in the same basis as the one used by Alice.

- Later, Alice and Bob communicate to each other the list of the bases they used. This communication carries no information about the value of the measurement, but allows Alice and Bob to know which values were measured by Bob correctly.

- Bob and Alice keep only those bits that were measured deterministically and will disregard those sent and measured in different bases. Statistically, their bases coincide in 50 % of all cases, and Bob's measurements agree with Alice's bits perfectly.

- Together, they can reconstitute the random bit string created previously by Alice.

The BB84 protocol can be shown as in the following tabular:

Alice's random bits	1	1	0	0	1	0	0	1	0	0	1	0	1	0
Alice's random bases	+	×	×	×	+	+	×	+	+	×	×	+	+	+
Alice's polarizations	→	↗	↖	↖	→	↑	↖	→	↑	↖	↗	↑	→	↑
Bob's random bases	+	×	+	×	×	×	+	+	×	+	×	×	×	+
Bob's measurements	→	↗	→	↖	↖	↗	↑	→	↗	→	↗	↖	↖	↑
Values kept afterwards	√	√		√				√			√			√
Code deduced	1	1		0				1			1			0

2.2.3 Eavesdropping the BB84 Protocol

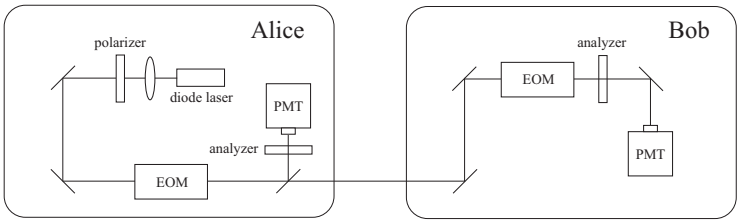
If an eavesdropper (usually called Eve) tries to listen to the quantum channel, she can intercept photons sent by Alice, perform measurements on them and re-send them to Bob. However, as Alice alternates her encoding bases at random, Eve does not know the basis to use for her measurement; she must choose her measurement bases at random, as well. Half the time, she guesses properly and re-sends correctly polarized photons. In the other 50 % of the cases, though, she measures in the wrong basis and produces errors.
For example, lets assume Alice sends a "1 " in the rectilinear basis, i.e. the state $|\rightarrow\rangle$, Eve measures in the diagonal basis and Bob in the rectilinear basis (otherwise, this bit would not even be taken into account). Then, no matter which polarization Eve detects and re-sends, $|\nearrow\rangle$ or $|\nwarrow\rangle$, Bob will have a 50 % chance of measuring $|\uparrow\rangle$, a binary "0". If Alice and Bob agree on communicating part of their strings in order to compare them, they can discover these errors: When they have identical bases, their bits should be in perfect agreement. If not, Eve is suspected of tampering with the photons, and the cryptographic key is thrown away. Thus, no information leak occurs, even in the case of eavesdropping,. If their strings are identical within a certain error level (e.g., caused by losses in the transmission line), the key is deemed secure and secret, and can be used in the Vernam cipher scheme to encrypt communications. Since those bits used to test for eavesdropping are communicated via an open public channel, they must always be discarded, and only the remaining bits constitute the key.
Unlike in this simple lab experiment, the BB84 protocol can be extended: The quantum bit error rate induced by transmission failures can be estimated, e.g. by parity checks, and corrected for. However, this further shortens the key and allows Eve to gain information about the key bits. To recover security, "Privacy Amplification" is performed. Thereby, the key is multiplied with so called "Hash functions", randomly generated matrices, which lead to totally different results, when multiplied with keys differing by just a few bits. The final key will consist of only a small part of the bits first sent by Alice.

3 The Experimental Setup

3.1 General Overview of the Setup

The experimental setup consists of four main parts:

- photon source
- polarization encoder (EOM)
- polarization reader (EOM)
- photo detector (TAKE CARE!!! VERY SENSITIVE EQUIPMENT!!!)



The photon beam is sent through a polarizer and further into Alice's Electro-Optic Modulator (EOM). The photons end up randomly polarized in four different states. They propagate in free space and reach Bob's EOM and another vertikal polarizer in order to let pass only those photons that are in a given (randomly chosen) state. A lens focusses the photons onto the sensitive area of an APD (avalanche photo detector). At the output of Alice's EOM, a flip mirror allows to direct the beam through a polarizer and into a detector in order to check the light emitted by Alice.

3.2 Detailed Description of the Setup

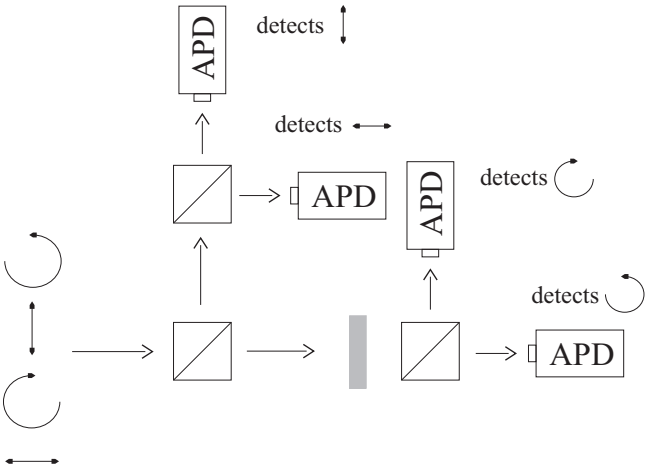
3.2.1 Photon Source

The photon source is a 5 mW diode laser emitting at 633 nm. Therefore, it is a coherent source with Poissonian statistics, not showing the usual dip in the second-order correlation function observed with true single photon sources. In order to produce quantum states with only one photon, it will be necessary to attenuate the laser beam, as explained later.

3.2.2 Encoding and Decoding using an EOM

The Electro-Optical Modulator In order to control the polarization of the photons emitted by Alice, an EOM is used (KD*P crystal and 3×3 mm^2 aperture) which is basically a delay plate controlled by a voltage; it uses the Pockels Effect. For example, at 633 nm, the "half wave plate" voltage is approximately

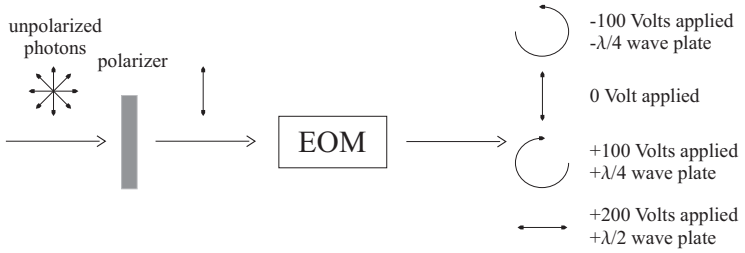
200 V; if 0 V is applied, the crystal has no effect on the light. It is then possible to easily switch between vertical and horizontal polarization by setting the crystal axis to 45° and switching between "no delay" and "half wave plate".



In order to produce 45° and 135° polarization angles, it would require another EOM with a different axis orientation. Since an EOM is no cheap equipment, polarization is not chosen between 0°, 45°, 90° and 135°, but between 0°, circular left, 90° and circular right. These circular states are defined by

- $|\circlearrowleft\rangle = \frac{\sqrt{2}}{2}\left(|\rightarrow\rangle + i\,|\uparrow\rangle\right)$
- $|\circlearrowright\rangle = \frac{\sqrt{2}}{2}\left(|\rightarrow\rangle - i\,|\uparrow\rangle\right).$

They can easily be obtained by a single EOM applying a "quarter wave plate" or a "minus quarter wave plate" voltage.



Bob's Detection Stage In order to detect the polarization of the photons, Bob must project them onto a basis state and try to detect the projected state. This would require a four detectors measuring each possible projected state.
Since single photon detectors are expensive, we will try to use just one: We project the photons on a single vertical state after rotating them. Thus, only

photons with a certain angle before the detection will pass the polarizer. It is simply doing the opposite of what Alice did.

EOM driver To switch between different polarizations, the EOM must be driven between -100 V ($-1/4$ wave plate) and +200 V ($+1/2$ wave plate). As the EOM driver, a home-made fast linear amplifier is used (± 5 V $\rightarrow \pm 250$ V), able to drive a 200 pF load at 1 MHz.

Data Acquisition Detected photons must be converted into information that can be processed. A fast digital PC-based acquisition card is used (32 digital input ports, 32 digital output ports). Most parameters of the cryptosystem can be controlled by a LabView program that converts each detection event at the APD into an explicit value of the bases and possible measurements results. A click at the APD means that a photon has been detected, i.e. the photon was projected onto a basis and passed the polarizer. Then, the computer records both the polarization the photon was projected on and the index number of this photon. For example:

APD click $\rightarrow$ "projected/detected polarization $|\circlearrowleft\rangle$" & "laser pulse index 2574"

Alice will send Bob $\rightarrow$ "laser pulse index 2574" & "basis used: +"

In this very case, the photon will be discarded because Alice encoded it in the rectilinear basis while Bob measured it in the circular basis.

Photomultiplier Tube THIS IS VERY SENSITIVE EQUIPMENT!! YOU SHOULD HANDLE IT WITH CARE!! TAKE THE FOLLOWING PRECAUTIONS: Before you apply the operation voltage of 5 V

- Close windows!
- Switch off lights!
- Close the setup box as much as possible!
- ATTENUATE THE LASER PULSES! 5 mW ARE WAY TOO MUCH!!!

3.3 Peculiarities of QKD with Weak Laser Pulses

QKD relies on Heisenberg's uncertainty principle which forbids the measurement of more than one polarization component of *one* photon. However, with several photons known to be in the same quantum state, a measurement can be performed on any photon each which allows the complete measurement of the quantum mechanical state.
To maintain unconditional security, single photons have to be used. Otherwise, even with only two photons, an eavesdropper might split the pulse and gain partial information about the key without any indication at Bob's stage.

Producing a true single photon state poses a major experimental problem, which can be solved today by the use of single emitters (e.g., quantum dots, NV centers, or single molecules) or parametric down-conversion with post-selection. For this advanced lab experiment we chose the easier approach of weak laser pulses: A coherent laser source is attenuated to a mean photon number so small that it is very unlikely to find more than one photon per pulse. The source still has a Poissonian statistics, though, and shows a security leak.

4 Experiments and Exercises

4.1 Choice of Basis States

As mentioned before, circular instead of diagonal polarized basis states will be used.

Exercise: Show that circular and rectilinear bases also fulfill the conditions on mutual normalized orthogonality and equal-length projections.

4.2 Poisson Statistics

Exercise: For a laser diode (5 mW, 633 nm, 10 ns pulse length), which attenuation is needed to achieve a probability $< 10^{-3}$ of emitting more than one photon per pulse?

4.3 Mirror Alignment

Exercise: Adjust your mirrors in order to pass all apertures properly and to hit your photo detector.

4.4 EOM Voltage Levels

Exercise: Using the LabView software, λ-plates, analyzer, and photo-meter, find the proper voltages to obtain the different basis states behind the EOMs.

4.5 Secret Transmission

Exercise: Transmit an image of your choice (bitmap format) by using quantum cryptography.

4.6 Attenuation and Laser Repetition Rate

Exercise: Measure the similarity between Alice's and Bob's key at varying experimental conditions.
Values for laser repetition rate: 1 Hz, 5 Hz, 10 Hz, 50 Hz, ..., 10 kHz
Values for attenuation by damping plates: 10^5, $10^{5.5}$, 10^6

4.7 Quantitative Description of Measurement Data

Exercise: Derive a function that describes the previously measured similarities. The similarity is a function of attenuation and laser repetition frequency. The LabView program computes this similarity as the ratio of correctly detected photons and all photons detected.
Your function should include the dark count rate and possible errors due to imperfect polarization rotations (e.g., due to a beam that exceeds the EOM apertures). The initial number of photons per pulse and the attenuation by the

pinholes, EOMs, and PBS are additional fixed parameters of your function and can be measured using the less sensitive detector head.
Finally, fit your measurement data for the similarity to your function. Your only unknown parameter is the dark count rate. Determine this rate for the different attenuation factors by using a fitting routine (e.g., Origin).

References

[1] G.S. Vernam, *Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications*, J. AIEE **45**, 109–115 (1926)

[2] W. Diffie, M.E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory **22**, 644–654 (1979)

[3] R.L. Rivest, A. Shamir, L.M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM **21**, no. 2, 120–126 (1978)

[4] W.K. Wooters, W.H. Zurek, *A Single Quantum cannot be Cloned*, Nature **299**, 802–803 (1982)

[5] C.H. Bennet, G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing, in: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, IEEE, New York, 175–179 (1984)