Fortschr. Phys. **54**, No. 8 – 10, 840 – 845 (2006) / **DOI** 10.1002/prop.200610322

Free space quantum key distribution: Towards a real life application

Henning Weier[1,*], **Tobias Schmitt-Manderbach**[1,2], **Nadja Regner**[1], **Christian Kurtsiefer**[3], and **Harald Weinfurter**[1,2]

[1] Ludwig-Maximilians-Universität, 80799 München, Germany
[2] Max-Planck-Insititut für Quantenoptik, 85748 Garching, Germany
[3] National University of Singapore, Singapore

Published online 4 August 2006

Key words Free space, quatum key distribution, quantum cryptography
PACS 03.67.Dd

Quantum key distribution (QKD) [1] is the first method of quantum information science that will find its way into our everyday life. It employs fundamental laws of quantum physics to ensure provably secure symmetric key generation between two parties. The key can then be used to encrypt and decrypt sensitive data with unconditional security. Here, we report on a free space QKD implementation using strongly attenuated laser pulses over a distance of 480 m. It is designed to work continuously without human interaction. Until now, it produces quantum keys unattended at night for more than 12 hours with a sifted key rate of more than 50 kbit/s and a quantum bit error rate between 3% and 5%.

© 2006 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

1 Introduction

Whenever sensitive information has to be exchanged between two parties, cryptography is employed to ensure that no unauthorised third party can get access to the content. Classical cryptographic methods like the one-time pad have been shown to be provably secure, if and only if the key has been deployed securely. Yet, this task cannot be provably accomplished by classical means.

Quantum cryptography, also known as quantum key distribution (QKD), makes use of fundamental principles of quantum mechanics to ensure the security of secret key generation. The system subject to this report employs the so-called BB84 protocol [2], encoding qubits in the polarisation of faint laser pulses. Ideally, one party (Alice) prepares a sequence of single photons, their polarisations being chosen randomly from four possible non-orthogonal states (e.g. horizontal, vertical and $\pm 45^\circ$). She sends the photons to the second party (Bob), who analyses the polarisation of each detected photon in a randomly and independently chosen basis (e.g. either H/V or $\pm 45^\circ$). Afterwards both parties compare publicly their basis choices and discard those events where they had used different bases. This process is called sifting.

Due to fundamental laws of quantum mechanics, an eavesdropper (Eve) cannot determine the polarisation of a single photon if the polarisation states are non-orthogonal. Even worse, she will introduce errors during the polarisation measurement, so that the quantum bit error rate (QBER) of the sifted key gives an upper bound on the information an eavesdropper might have gained. The QBER is calculated during the classical error correction procedure and is used to infer the shrinking ratio that is needed to make sure that the information of a potential eavesdropper on the key is negligible. The key is then hashed to this secure length during privacy amplification.

* Corresponding author E-mail: henning.weier@lmu.de, Phone: +49 89 2180 5804 Fax: +49 89 2180 5032

WILEY InterScience® DISCOVER SOMETHING GREAT

© 2006 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

The scope of this particular experiment is to show the feasibility of autonomous free space quantum key distribution systems, generating symmetric keys, for example between two buildings within a city. Once it has been set up, it is supposed to be working continuously without human interaction. There have already been some free space experiments over relatively large distances, for example a 10 km link in the group of Richard Hughes [3] and a 23 km link from Zugspitze to Karwendelspitze in our group in collaboration with the group of John Rarity [4]. The results of those free space trials show the possibility to build global quantum key exchange systems based on quantum communication satellites [5]. The experience gathered during the latter experiment was used as a starting point for building a stable quantum cryptography system for urban areas.

2 Setup

The system can be divided into three parts: The transmitter contains a weak coherent pulse source, which sends out pulses of polarised light with a Poissonian distribution with mean photon number μ. The next part is the optical free space link which is formed by two telescopes plus spatial and spectral filter on the receiver end. Finally, there is the receiver unit, which analyses the polarisation and detects the single photons. The three parts will be described in detail in the following sections.

2.1 Transmitter unit

The transmitter unit basically consists of four laser diodes plus a conical mirror and a spatial filter to combine the four beams. Ideally, the sender unit would produce a stream of single polarised photons according to the choice of basis and bit value. Since currently no single photon source is competitive, we use weak coherent pulses with a mean photon number μ, which are produced as follows: The light of laser diodes has a high intrinsic polarisation (typically better than 1:1000) and they can be oriented so that there is one laser diode for sending out photons in each desired polarisation. The advantage of this method is that no active polarisation manipulations are needed. Four such laser diodes emitting at wavelength 850 nm are arranged around a conical mirror (see Fig. 1) in such a way that the four beams are reflected and combined into one direction. After the beams have been reflected by the conical mirror, they have to pass a spatial filter, which consists of two pinholes designed to let only a single spatial mode pass through. This is vital, because it must be provided that no information on the polarisation of the photons can be gathered by measuring their momentum or position.

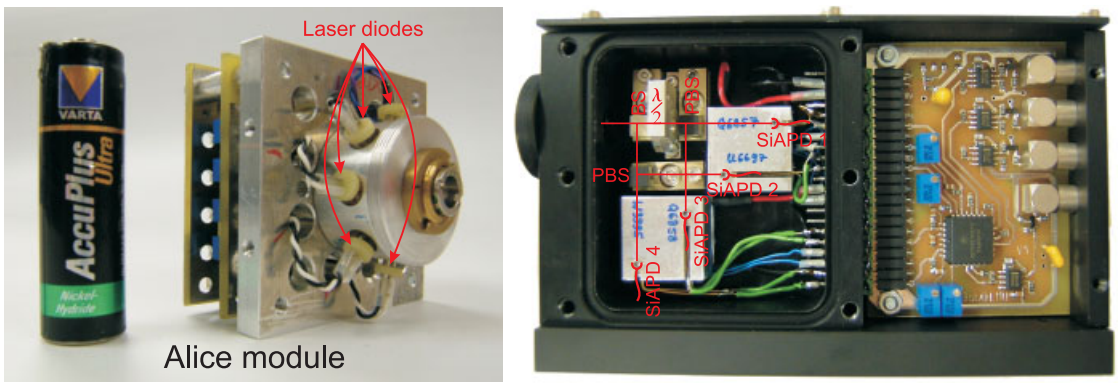

Fig. 1 Transmitter (left) and receiver unit (right). In the Alice module, the pulses of four differently polarised laser diodes are combined on a conical mirror. The Bob module uses a non-polarising beam splitter, a half wave plate, two polarising beam splitters and four single photon detectors to analyse incident photons in the H/V or +/-45 basis.

© 2006 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

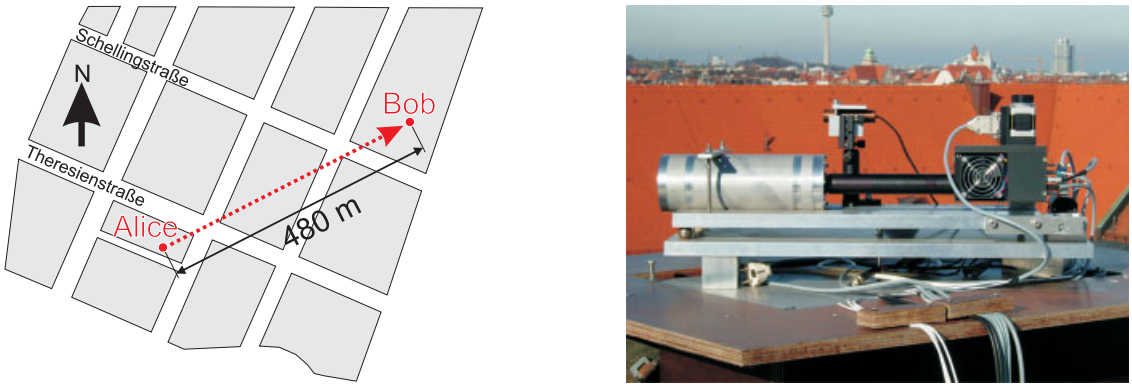

Fig. 2 Left: Location of the test bed in Munich. Right: Photograph of the receiver telescope with the Bob module attached.

2.2 Free space link

To ensure that as many photons from Alice as possible are detected by Bob, two telescopes are employed, one at each end. Both telescopes have the same front lens (f = 310 mm, open aperture a = 75 mm), but the rest of the system is chosen to match the different requirements of transmitter and receiver.

On the transmitter side, two pinholes forming the spatial filter define the initial beam parameters.

To ensure that as little stray light as possible is collected by the receiver, a pinhole was inserted into the receiver telescope. Because of their narrow field of view (the receiver sees a region of approximately 14 cm $\times$ 17 cm at a distance of 480 m, the orientation of the telescopes has to be aligned very precisely. Thus, stable mounts are necessary which permit the required pointing accuracy. To allow for automatic alignment control, each tip-tilt stage is equipped with two stepper motors, which drive micrometer screws to adjust the two possible angles.

The experiment is situated in downtown Munich, sender and receiver are located on the roof tops of two university buildings (see Fig. 2). There are no solid obstacles in the line of sight, so that most of the time the transmission is relatively high.

2.3 Receiver unit

The receiver unit consists of

- the so-called Bob module (containing the optics and detectors for polarisation analysis of the incoming photons),
- the timestamp card, which assigns a time to every click of a detector, and
- the software in Bob's computer, which is responsible for the extraction of synchronisation information to enable successful key-sifting.

The Bob module is directly attached to the end of the receiver telescope. A non-polarising beam splitter (BS), a set of two polarising beam splitters (PBS) and a half-wave plate are used to perform the polarisation analysis of the incoming photons. An incident photon first sees the 50/50 beam splitter; depending whether the photon is reflected or transmitted, the polarisation is analysed in the H/V basis or in the $\pm 45^\circ$ basis. The choice of bases is therefore random, but completely passive. This made it possible to shrink the module to as small dimensions as just 130 mm $\times$ 80 mm $\times$ 55 mm.

The single photons are detected by silicon avalanche photo diodes (APDs) which are peltier-cooled to about -20° C in order to keep the dark count rate at a tolerable level. The module already contains all the electronics needed for stabilising the temperature of the detectors, for biasing of the APDs and for signal

© 2006 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

recovery. For each of the four detector channels, a corresponding electronic pulse is output with a timing accuracy of about 1 ns. Attached to the outputs of the Bob module is the timestamp unit, that records the time of arrival of each detection event. This circuitry works with a timing resolution of better than 1 ns. The timing data are transferred to the PC via a digital I/O card and analysed by the synchronisation software.

2.4 Synchronisation and automatic alignment control

The basic idea for synchronisation is to take advantage of the known 10 MHz repetition rate of the transmitter. As soon as this pattern has been identified in the received clicks, good events can be discriminated from bad ones, so that a large fraction of dark and background counts can be filtered out. Since the local oscillators are not necessarily as stable as required, the calculated frequency and phase of the good events has to be adjusted continuously. Thanks to this technique, cheap standard crystal oscillators are sufficient for both sender and receiver.

In a next step, known patterns in the photon stream which have been inserted by Alice, are used to find out the number of each detected photon. Thus, Alice and Bob do not have to communicate classically during synchronisation. The advantage of this fact is that a temporarily unavailable or slow classical channel will not hinder the synchronisation routine and the sifting procedure can be performed later, when classical communication is again available. In other words, a time-stable classical channel is not required.

Thermal drifts of the setup required an active pointing control mechanism for both tip-tilt stages. In order to keep the hardware complexity as low as possible, the actual single photon signal itself is used to control the alignment. The extra advantage of this is, that one does not have to align additional equipment with respect to the telescopes. Two digital control loops similar to the lock-in technique with different frequencies allow us to separate the influence of the sender's and of the receiver's misalignment. The automatic alignment control is capable of compensating slow temperature-induced drifts of the setup and its mounts. It has been running for more than four days non-stop without humaninteraction, tracking on a bright cw laser source. When the single photon signal is used for alignment, the setup is to date operating in darkness only.

2.5 Sifting, error correction and privacy amplification

Once the synchronisation task has been accomplished, Alice and Bob can start the key sifting process. Whenever Bob has detected a photon, he will tell Alice its number and the basis in which he has analysed it. If Alice has sent the photon in the same basis, they will use the assigned bit value for the sifted key. If not, they have to discard the bit. At the end of this process, they will both have a so-called sifted key. Ideally, both sifted keys would be perfectly correlated. With experimental imperfections and/or an eavesdropper present, however, the key will contain errors. For security reasons all errors are accredited to the presence of an eavesdropper. In order to make the key usable, the errors have to be corrected and the amount of information that has potentially leaked to the eavesdropper has to be made negligibly small.

We have implemented an error correction scheme based on the CASCADE algorithm [6]. This is a purely classical method to reveal and eliminate errors that have been introduced while being sent over a "noisy channel". According to Shannon's noisy coding theorem, a minimum of information has to be transmitted between the two communicating parties in order to correct those errors. Unfortunately, such an optimal algorithm has not been found so far. Using suitable parameters, CASCADE gets close to the optimum. It does so by exchanging parity bits of subsets of the key in multiple passes. If the parity of a pair of chosen subsets of bits is not equal, there has to be an odd number of errors in that subset. The algorithm locates an error by exchanging parity bits of first and second half of the subset and so on. After the first pass has left an even number of errors in all subsets, new subsets (reorganised and of different length) are chosen and the procedure is repeated.

When the parameters are chosen correctly, the probability of a remaining error can be neglected. Of course, the disposal of errors does not come for free. Each publicly transmitted parity bit increases the

 © 2006 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

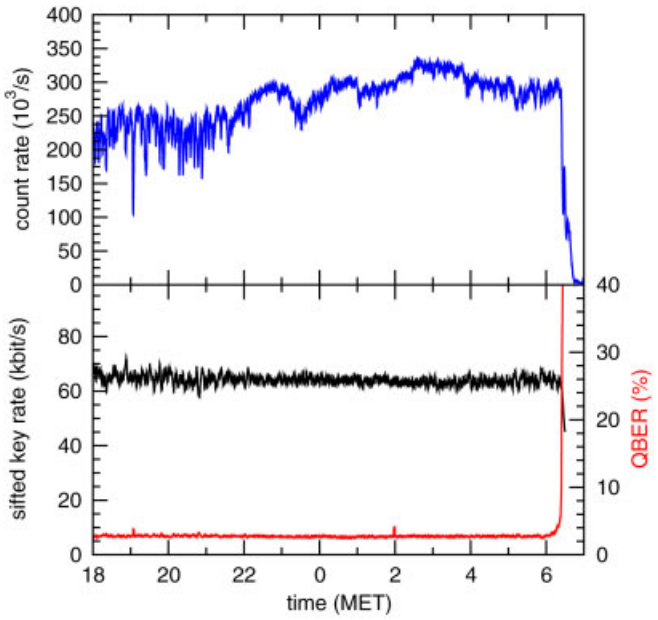

Fig. 3 Counting rate, sifted key rate and quantum bit error rate of the measurement run starting November 27th. The increase of the QBER and the decrease of the counting rate in the morning is due to stray light hitting the detectors ater sunrise, saturating them.

eavesdropper's knowledge of the key. Hence, these announced bits are counted and have to be taken into account during privacy amplification [7].

2.6 Experimental results

To test the system, a free space link has been set up between two buildings of the University. The transmitter is separated from the receiver by about 480 m, both are located on the roof tops of the respective buildings. A 10 Mbit/s internet connection provides the classical channel that is needed for the automatic alignment of the telescopes as well as synchronisation tasks and the key sifting procedure. The results of some more test runs are shown in Table 1.

A set of data has been chosen to show the performance of the system in more detail (see Fig. 3). It was taken starting November 27th, 2004 under good conditions. The sifted key rate was limited by the bandwidth of the classical channel, a problem that is being tackled at the moment. Error correction and privacy amplification results can be found below:

Initial key length (bits)	Discarded bits	Disclosed bits	Corrected bits	Final key length (bits)	QBER (%)	Priv. Amp. factor
2968502272	8077312	661681477	81432331	1636520736	2.8	0.55

The mean photon number was set to be on the order $\mu \sim 0.1$. Table 1 summarises several runs over three months and shows a varying, on average increasing quantum bit error rate, that seems to originate from mechanical rotational instability. The setup has not been realigned between different measurement runs concerning the polarisation, but there seem to have been drifts in both directions. We will tackle this problem by using even more rugged mechanics.

Weather conditions do, of course, affect the attenuation of the free space link. However, we found that only fog, heavy rain or snowfall limit the transmission severely so that the sifted key rate drops dramatically. In previous cw transmission measurements we saw that a more significant problem is caused by strong turbulance above sun heated roofs close to the optical path.

© 2006 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

Table 1 Exemplary experimental data taken at the test site over a distance of 480 m. The sifted key rate varies due to different transmission values which are themselves strongly influenced by the weather conditions.

Date	Start	Time Stop	Total	Key length (MB)	Sifted Key rate avg. (kbit/s)	QBER (%)
27.11.04	18:22	08:00	14:38	354	56,42	2,8
21.12.04	18:19	07:00	12:42	250	44,80	4,5
11.01.05	18:59	07:00	12:01	331	62,66	3,2
12.01.05	17:03	07:00	13:58	206	33,57	3,6
20.01.05	21:10	07:00	09:50	96	22,22	3,1
01.02.05	21:37	07:00	09:23	39	9,46	4,3
03.02.05	18:11	07:00	12:49	149	26,44	5,0
25.02.05	17:41	10:00	16:20	277	38,61	4,3

3 Conclusion

We have reported on the progress of our mid range free space quantum key distribution system which is designed to work continuously without human interaction. Currently the system works unattended during nights over a distance of 480 m, producing average sifted key rates of more than 50 kbit/s on average over a period of more than 12 hours. Essential additional subroutines like error correction and privacy amplification have been implemented into the software. They collaborate well with the previously developed parts like automatic alignment, synchronisation and sifting.

We have identified extra requirements that will have to be fulfilled to allow for daylight operation of the setup. These include temperature control of the transmitter module (currently in progress) and insertion of narrow spectral filters. The introduction of a monitoring APD into the transmitter unit is also scheduled for the near future. An additional task is the implementation of authentication of the public channel and the use of a decoy state protocol to increase the secure key rate.

Acknowledgements The project is supported by the A8 Quantum Information Highway project and the EU project SECOQC.

References

[1] N. Gisin et al., Rev. Mod. Phys. **74**, 145–195 (2002).
[2] C. H. Bennett et al., Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984).
[3] R. J. Hughes et al., New J. Phys. **4**(43), 1–14 (2002).
[4] C. Kurtsiefer et al., Nature **419**, 450 (2002).
[5] M. Pfennigbauer et al., J. Opt. Netw. **4**, 549–560 (2005).
[6] G. Brassard et al., Advances in Cryptology – Proceedings of Eurocrypt '93, Lecture Notes in Computer Science 765, 410–423, Springer (1994).
[7] N. Lütkenhaus, Phys. Rev. A, **61**, 052304 (2000).

© 2006 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim