Practical quantum key distribution with polarization entangled photons

A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm
Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Wien, Austria
andreas.poppe@quantum.at

T. Lorünser, O. Maurhardt, M. Peev, M. Suda
ARC Seibersdorf Research GmbH (ARCS), 2444 Seibersdorf, Austria

C. Kurtsiefer, H. Weinfurter
Sektion Physik, Ludwig-Maximilians-Universität,D-80797 Muenchen, Germany

T. Jennewein
Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Wien, Austria

A. Zeilinger
Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Wien, Austria

Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Wien, Austria

Abstract: We present an entangled-state quantum cryptography system that operated for the first time in a real-world application scenario. The full key generation protocol was performed in real-time between two distributed embedded hardware devices, which were connected by 1.45 km of optical fiber, installed for this experiment in the Vienna sewage system. The generated quantum key was immediately handed over and used by a secure communication application.

OCIS codes: (030.5260) Photon counting; (060.4510) Optical communications; (270.0270) Quantum optics; (999.9999) Quantum cryptography.

References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys. **74,** 145–195 (2002).
2. idQuantique SA (Geneve, Switzerland), http://www.idquantique.com/.
3. magiq technologies (Sommerville, USA), http://www.magiqtech.com/.
4. NEC Ltd.(Tokyo, Japan), http://www.nec.com/.
5. J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams, “Quantum key distribution with 1.25 Gbps clock synchronization,” Opt. Express **12,** 2011–2017 (2004).
6. C. Bennett and G. Brassard, “Quantum Cryptography: public key distribution and coin tossing,” in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*(Bangalore, India, 1984), pp. 175–179.
7. N. Lütkenhaus, “Estimates for practical quantum cryptography,” Phys. Rev. A **59,** 3301–3319 (1999).
8. H. Inamori, N. Lütkenhaus, and D. Mayers, “Unconditional security of practical quantum key distribution,” quant-ph/0107017 (2001).
9. A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. **67,** 661–663 (1991).
10. N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” Phys. Rev. A **61,** 052304 (2000).

#4561 - $15.00 US
Received 8 June 2004; Revised 3 August 2004; accepted 3 August 2004

11. G. S. Vernam, “Cipher printing telegraph systems for secret wire and radio,” J. Amer. Inst. Elect. Eng. **55,** 109–115 (1926).
12. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, “Quantum cryptography with entangled photons,” Phys. Rev. Lett. **84,** 4729–4732 (2000).
13. D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, “Entangled state quantum cryptography: eavesdropping on the Ekert protocol,” Phys. Rev. Lett. **84,** 4733–4736 (2000).
14. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, “Quantum cryptography using entangled photons in energy-time Bell states,” Phys. Rev. Lett. **84,** 4737–4740 (2000).
15. H. Böhm, “A compact source for polarization entangled photon pairs,” Master’s thesis, Vienna University of Technology (2003).
16. M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, “Long-distance free-space distribution of quantum entanglement,” Science **301,** 621–623 (2003).
17. P. Trojek, C. Schmid, M. Bourennane, H. Weinfurter, and C. Kurtsiefer, “Compact source of polarization-entangled photon,” Opt. Express **12,** 276–281 (2004).
18. S. Wiesner, “Conjugate Coding,” submitted to IEEE Information Theory (ca. 1970) Later published in Sigact News **15**(1), 78–88 (1983).
19. P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, “New high-intensity source of polarization-entangled photon pairs,” Phys. Rev. Lett. **75,** 4337–4341 (1995).
20. C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, “High-efficiency entangled photon pair collection in type-II parametric fluorescence,” Phys. Rev. A **64,** 023802 (2001).
21. R. Lieger, T. Lorünser, G. Humer, and F. Schupfer, “Embedding quantum cryptography on DSP-boards,” in *Proceedings of EUSIPCO - to be published* (Vienna, Austria, 2004).
22. G. Brassard and L. Salvail, “Secret key reconciliation by public discussion,” Lecture Notes in Computer Science **765,** 410–423 (1994).
23. M. Peev, O. Maurhardt, T. Lorünser, M. Suda, M. Nölle, A. Poppe, R. Ursin, A. Fedrizzi, H. Böhm, T. Jennewein, and A. Zeilinger, “A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography,” in *Proceedings of the International Meeting on Quantum Information Science ”Foundations of Quantum Information” - to be published* (Camerino, Italy, 2004).

1. Introduction

Quantum cryptography [1] is the first technology in the area of quantum information that is in the process of making the transition from purely scientific research to an industrial application. The last three years have seen dramatic advances in experimental quantum cryptography systems and several companies have developed quantum cryptography prototypes. The first products are now commercially available [2, 3, 4], but further improvements of the laser sources, detectors and electronics have very recently been demonstrated (e.g., [5]).

Up to now, these commercial products are all based on various implementations of the BB84 [6] protocol. Because of the unavailability of true single-photon sources, today’s commercially available quantum cryptography systems rely on photons from attenuated laser pulses, as an approximation of the single photon state. However, the produced state has a non-vanishing probability to contain two or more photons per pulse, leaving such systems susceptible to eavesdropping through a beam splitter attack. Although this attack is considered in recent security proofs given for the BB84 protocol [7, 8], a true single photon source is conceptually preferable.

An elegant alternative is quantum cryptography based on entangled photon pairs [9], which does not depend on photons from attenuated laser pulses. In our implementation of entangled-state quantum cryptography we make use of pairs of single photons, which are individually completely unpolarized. Information is only stored in correlations between the results of measurements on the individual photons of a pair. With today’s entangled photon sources the probability of double pair emissions is much lower than the probability of double photon emission in weak coherent pules systems. Therefore entangled-state quantum cryptography systems are closer to the original idea of quantum cryptography. Furthermore, it can be shown [10] that entanglement-based systems have a better performance in certain situations, they are secure for a broader range of experimental parameters than the attenuated laser pulse implementations.

Received 8 June 2004; Revised 3 August 2004; accepted 3 August 2004

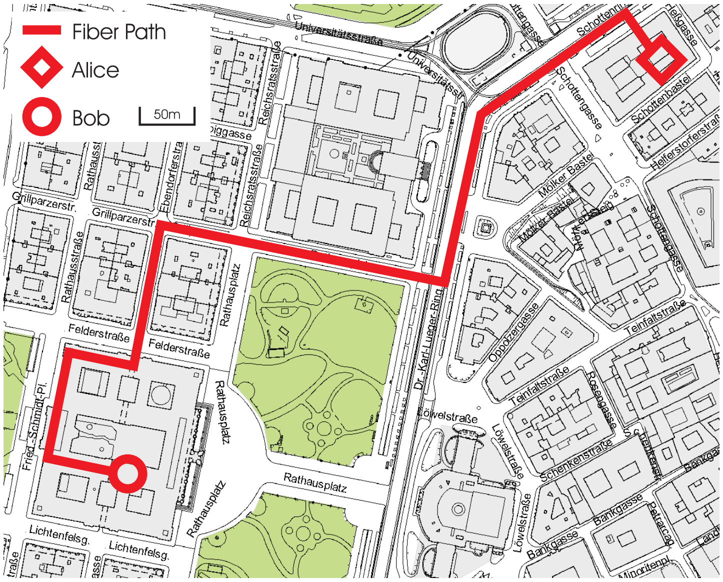

Fig. 1. A quantum cryptography system is installed between the headquarters of a large bank (Alice) and the Vienna City Hall (Bob). The beeline distance between the two buildings is about 650m. The optical fibers were installed some weeks before the experiment in the Vienna sewage system and have a total length of 1.45 km.

Additionally the randomness of the generated key as required for a secure one-time-pad cipher [11] is guaranteed by the quantum randomness of the measurement process, whereas in attenuated laser quantum cryptography the random encoding has to be achieved by using an external random number generator. Thus, a fundamental point is that in entangled-state quantum cryptography the key comes spontaneously into existence at both measurement stations while in the BB84 protocol it still has to be transmitted from Alice to Bob. Experimentally, entangled-state quantum cryptography has been first demonstrated in 1998 using polarization-entangled photon pairs [12, 13]. Alternative schemes are based for example on energy-time entanglement [14]. Recent development of compact, highly efficient sources for entangled photons [15, 16, 17] make entangled-state quantum key distribution in real-life applications feasible.

In this article we present an entangled-state quantum cryptography prototype system in a typical application scenario. In the experiment reported here, it was possible to distribute secure quantum keys on demand between the headquarters of an Austrian bank and the Vienna City Hall (Fig. 1) using polarization-entangled photon pairs. At both measurement stations each incoming photon switches randomly between complementary bases [18] as also employed in the BB84 protocol. The produced key was directly handed over to an application that was used to send a quantum secured online wire transfer from the City Hall to the headquarters of Bank-Austria Creditanstalt [1].

The quantum cryptography system (Fig. 2) consists of the source for polarization-entangled photons located at the bank, two combined polarization analysis and detection modules and of two electronic units for key generation. These two quantum cryptography units which handled the five steps of secure key generation (real-time data acquisition, key sifting, error estimation, error correction and privacy amplification) and channel authentication are based on an embed-

[1] The first real bank transfer took place on April 21st 2004.

Received 8 June 2004; Revised 3 August 2004; accepted 3 August 2004

ded electronic design and are compatible with conventional telecommunication equipment. The quantum channel between Alice and Bob consisted of an optical fiber that has been installed between the two experimental sites in the Vienna sewage system (by WKA / CableRunner Inc.). The exposure of the fibers to realistic environmental conditions such as stress and strain during installation, as well as temperature changes were an important feature of this experiment, as the successful operation of the system shows that our system not only works under laboratory conditions, but also in a realistic quantum cryptography scenario.

2. Experimental setup

The entangled photon pairs used in our cryptography prototype were produced using a compact device based on type-II spontaneous parametric down-conversion [19, 20]. Using a 16 mW violet laser diode as pump source, it was possible to generate and locally detect about 8.200 pairs per second. The pair photon had a center wavelength of 810 nm and a FWHM bandwidth of 5.6 nm. The visibility of the produced entangled state $|\psi^-\rangle$ under local detection was above 97%. For key generation one photon of the pair was directly sent to Alice's detection module (Fig. 2), while the other photon was sent to Bob's receiver via 1.45 km of optical fiber. The fiber used for that quantum channel was single mode for 810 nm and had an average attenuation of about 3.2 dB per kilometer resulting in a total attenuation of 6 dB including the connectors. The compensation of polarization rotation in the fibers was done using fiber polarization controllers. Alignment of the controllers was done ”offline” before the quantum cryptography protocol was started, using alignment software which calculated and displayed the quantum bit error rate of the transmission system in real-time based on the single photon detection events. With two linear polarizers in both arms of the entanglement source the polarization controllers were adjusted to compensate for the arbitrary polarization rotation. It turned out that the polarization was stable for several hours, therefore online measurement and compensation for polarization drift was not necessary.

A prototype of a currently developed dedicated QKD-hardware [21] was used for the first time in this experiment. It consists of three main computational components best suited to manage all signal acquisition and QKD protocol tasks. All three units are situated on a single printed circuit board. The main task of the board is key acquisition, i.e. the processing of the signals detected by the four detectors on each site of the QKD system.

The board handles also the synchronization channel and generates a strong laser pulse whenever a photon counting event is detected at Alice's site. This is ensured by a logical OR connection of the detector channels as shown on Figure 2. The synchronization laser pulse at the wavelength of 1550nm was sent over a separate single mode fiber. The developed detection logic is implemented in a FPGA and runs at a sampling frequency of 800MHz, while employing a time window of 10 ns for matching the detection events and synchronization signals. The synchronization mechanism allows an identical realisation of the higher level electronics at both sides and thus enables the development of universal QKD devices.

The classical communication between the two devices is carried over a TCP/IP connection, provided by an Ethernet bridge.

When fully developed the QKD hardware will be equipped with a full scale QKD protocol modular library allowing seamless interchange of relevant algorithms, as well as an encryption library, comprising a number of state of the art encryption algorithms in addition to the standard one-time pad. In addition to the main ”embedded” used modus, the libraries can be used in a developer modus - in the framework of an alternatively computing environment (PC, etc.).

In the current experiment the high speed electronics had only been used for measuring detector events, hence, it worked in a developer mode passing the data to an outside PC running the protocol software stack and a graphical user interface (GUI). The library modules utilized

Received 8 June 2004; Revised 3 August 2004; accepted 3 August 2004

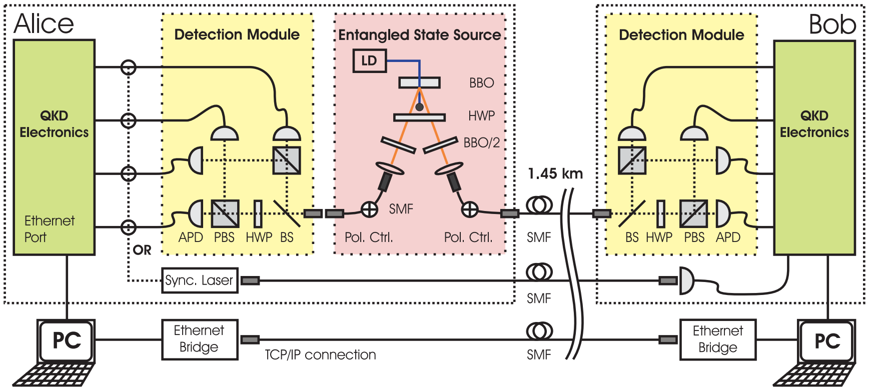

Fig. 2. Sketch of the experimental setup. At the entangled state source a nonlinear BBO-crystal is pumped by a violet laser diode (LD) at 405nm and produces polarization-entangled photon pairs. Walk-off effects are compensated by the half-wave-plate (HWP) and the compensation crystals (BBO/2). One of the photons is locally analyzed in Alice's detection module, while the other is sent over a 1.45 km long single-mode optical fiber (SMF) to the remote site (Bob). Polarization measurement is done in one of two bases (0° and 45°), by using a beam splitter (BS) which randomly sends incident photons to one of two polarizing beam splitters (PBS). One of the PBS is defined for measurement in the 0° basis, and the other in the 45° basis as the half wave plate (HWP) rotates the polarization by 45°. The final detection of the photons is done by passively quenched silicon avalanche photodiodes (APD). Once a photon is detected at one of Alice's four avalanche photodiodes an optical trigger pulse is created (Sync. Laser) and sent over a standard telecommunication fiber to Bob to establish a common time basis. At both sites, the trigger pulses and the detection events from the APDs are fed into a dedicated quantum key generation device (QKD Electronics) for further processing. This QKD electronic is an embedded system, which is capable of autonomously running the classical protocol necessary for key generation via a standard TCP/IP connection.

in the current experiment include data acquisition, error estimation, error correction, implementing the algorithm CASCADE [22], privacy amplification and a protocol authentication algorithm, ensuring the integrity of the quantum channel [23], using a Töplitz matrix approach. Furthermore the encryption-library modules applied include one-time pad and AES encryption schemes, the latter allowing key exchange on a scale determined by the user.

The average total quantum bit error rate (QBER) was found to be less than 8% for more than the entire run time of the experiment. Such mistakes occur whenever both pair photons are measured in the same basis, but due to some errors the wrong detector fired on one side. An analysis of the different contributions to the QBER showed that about 2.6% came from imperfections of the detection modules, 1.2% from the imperfect production of the entangled state. As these two contributions are practically not accessible to an eavesdropper[2] we subtracted these contributions for consideration in privacy amplification. The rest of the QBER was attributed to the error produced by the quantum channel. For the data presented in this article, the number of bits discarded in privacy amplification is automatically adjusted to the number of bits disclosed during error correction and the QBER of the quantum channel. The average raw key bit rate in our system was found to be about 80 bits/s after error correction and privacy amplification. This value is mainly limited by the attenuation on the quantum channel, the

[2] If the QBER contribution related to our imperfect detection modules can be expressed as unitary operations one could think of a method which would allow an eavesdropper to reduce the QBER of our detection system in an attack. However in a practical implementation this assumption is unrealistic.

#4561 - $15.00 US Received 8 June 2004; Revised 3 August 2004; accepted 3 August 2004

detection efficiency of the avalanche photo diodes and the electronics.

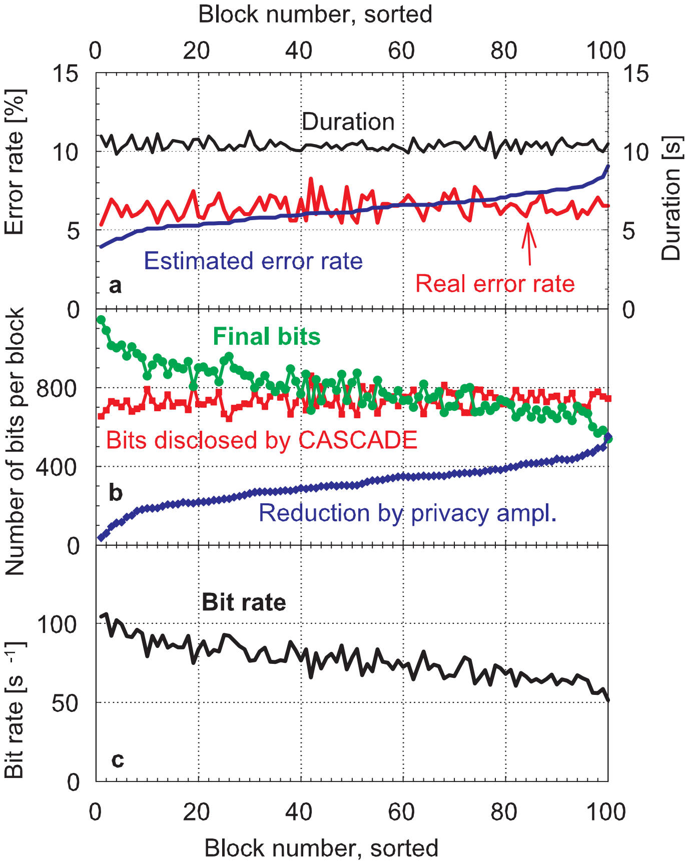

Fig. 3. Results obtained during 18 minutes of the running experiment. That time was used to acquire 100 blocks of raw data that each consist of approximately 2500 bits after sifting. The blocks in this graph have been sorted by the estimated QBER and are not represented in the order of their acquisition. Each key block was further processed by the full quantum cryptography software. *(a)* Estimated QBER for the individual blocks and the real QBER determined by directly comparing the sifted key of each data block. This calculation was only done for evaluation of the system and is obviously not possible for a real key exchange. Additionally one can see the time it took to acquire the raw data of the given block. *(b)* The length of the final key, the number of bits disclosed by CASCADE and the number of bits discarded in privacy amplification. *(c)* The final secure bit rate produced by our system.

3. Secure key generation

In this section we present a typical subset of the data obtained in our experiment. It covers 18 minutes of data acquisition and key generation. Within that time period Alice's detectors registered overall more than 12.8 million counts. The same number of synchronization pulses was sent to Bob. After determination of coincidence events and key sifting a total of 244765 bits remained for further processing by the classical algorithms. For this purpose, the raw data was continuously grouped into blocks of approximately 2500 bits, which where handed over individually to the following classical protocols. From this data stream we took 100 subsequent

#4561 - $15.00 US
Received 8 June 2004; Revised 3 August 2004; accepted 3 August 2004

blocks as a basis for the numbers presented here to form a typical subset. Publicly announcing 25% of the bits in each block was done for estimating the quantum bit error (QBER) of the sifted key. The average value of the estimated error rate was found to be 6.3% and the real error rate of 6.4%, calculated by directly comparing Alice's and Bob's sifted key after the experiment. Even though the average value of the estimated error rate matches the real error rate, the small sampling size gives strong deviations in individual blocks.

The remaining 183574 bits after error estimation were then submitted to the error correction process. Due to the disclosing of bits during error correction, the usable key size had to be further reduced to 110226. In the last stage of the protocol, privacy amplification reduced the error-corrected key depending on the estimated QBER for each individual block, leaving a total of 79426 bits for the final secure quantum key. This corresponds to an average key distribution rate of 76 bits/second.

Results for individual blocks are presented in Fig. 3. There the blocks have been ordered by the estimated quantum bit error rate rather than by the order of their acquisition. The acquisition time of the individual blocks, plotted in the upper part (a) of Fig. 3, is almost constant. Also shown there is the estimated error rate in comparison with the real error determined after the experiment. One can see that the estimated error nicely fits the real error rate. Only for a small percentage of blocks, the error is over- or underestimated. By increasing the size of the individual blocks and therefore improving the sampling of the error estimation, this effect can be mitigated. The over- and underestimation of the QBER can also be seen in the second graph (b) of Fig. 3, where the action of privacy amplification is plotted. The sorting order of the individual blocks leads to an increasing curve of the reduction of bits by privacy amplification. The bits disclosed by CASCADE turned out to be only slightly dependent on the estimated error rate. The number of sifted bits (approximately 2500 bits for all blocks, not shown if Fig. 3) is decreased by the bits disclosed by CASCADE and the reduction by privacy amplification. So only the number of final bits is left over to grow the secret. In the last graph (c) of Fig. 3 the bit rate of the individual blocks is shown. One can clearly see the expected behavior: The number of final bits is mainly dominated by the estimated error rate.

4. Conclusion

The experiment reported here demonstrates the operation of an entangled-state quantum cryptography prototype system. All calculations were done in real-time on a distributed embedded system. Furthermore we demonstrate the successful run of our quantum cryptography system in a real world application scenario outside ideal laboratory conditions. The results clearly show that entangled photon systems provide a good alternative for weak coherent pulse systems, with the additional benefit of rendering the beamsplitter attack much less efficient and thus being closer to the ideal BB84 quantum cryptography idea than systems based on weak coherent pulses.

Acknowledgments

This work was supported by the Austrian Science Fund (FWF), the QuComm and RAMBOQ project of the European Commission, the PRODEQUAC project of the Austrian Ministry of Transportation Innovation and Technology (FIT-IT Embedded Systems Program), the City of Vienna (MA30), WKA and the Austrian BA-CA Bank. Special thanks to Helmut Kadrnoska (MA30/WKA) for providing us with the in-sewer fiber optics infrastructure and also to Richard Plank for the helpful organization.

Received 8 June 2004; Revised 3 August 2004; accepted 3 August 2004