Long Distance Free Space Quantum Cryptography

C. Kurtsiefer[a], P. Zarda[a,b], M. Halder[a], P.M. Gorman[c], P.R. Tapster[c], J.G. Rarity[c] and H. Weinfurter*[a,b]

[a]Ludwig-Maximilian University, Munich, Germany;
[b]Max-Planck-Institut für Quantenoptik, Garching, Germany; [c]QinetiQ; Malvern, UK

ABSTRACT

Quantum cryptography bases the security of key exchange on the laws of quantum physics and will become the first application of quantum information methods. Here we present the design of novel hardware components which enabled the demonstration of secure key exchange over a 23.4 km free-space link.

Keywords: Quantum Cryptography, Quantum Information, Free space optics

1. INTRODUCTION

With the exponential expansion of electronic commerce the need for global protection of data is paramount. Data is normally protected by encoding it bit-wise using a large random binary number known as a key. An identical key is used to decode the data at the receiver. The secure distribution of these keys thus becomes essential to secure communications and transactions across the globe. At present electronic commerce generally exchanges keys using Public Key methods[1]. These methods rely on computational complexity, in particular the difficulty of factoring very large (publicly declared) numbers, as proof against tampering and eavesdropping. Any confidential information exchanged using such a key thus becomes insecure after a time when the rapid improvements in computational power or algorithmic development render the public key insecure. To guarantee long-term security the cryptographic key must be exchanged in an absolutely secure way. The conventional method used for this for most of the last century has been the 'trusted courier' carrying a long random key from one location to the other. Following the idea of Bennett and Brassard in 1984[2], it is only recently that absolutely secure key exchange between two sites has been demonstrated over fibre[3-5] and free space[6-9] optical links. This technique, known as quantum cryptography, has security based on the laws of nature and is, in principle, absolutely secure against any computational improvements.

In this paper we describe a novel, semi-portable free-space quantum cryptography system. We have tested this system and exchanged keys between two mountain tops, Karwendelspitze (2244 m) and Zugspitze (2960 m), in Southern Germany. The distance between the two locations is 23.4 km. The elevated beam path dramatically reduced the air turbulence effects experienced in previous low altitude tests[3], but also caused unpredecented requirements on stability against temperature changes, reliability under extreme weather conditions and ease of alignment. The results achieved form a significant step towards a key exchange system with a range of up to 1000 km. Such a system combined with sophisticated automatic pointing and tracking hardware could exchange keys with low earth orbit satellites. If we engineer a satellite to be a secure 'relay' station this has the potential for secure key exchange between any two arbitrary locations on the globe.

2. THE METHOD

Following the first experimental realisation[6], in the QC technique the transmitter (Alice) encodes a random binary number in weak pulses of light using one linear polarisation to encode '1's and orthogonally polarised pulses to encode zero's. To prevent eavesdropping the number of photons per pulse is limited to much less than unity (the actual attenuation is linked to the overall transmission and is usually chosen as 0.1 photons per pulse). Furthermore, the encoding basis is randomly changed by introducing a 45° polarisation rotation on half the sent pulses. In the receiver (Bob) single photon counting detectors detect the pulses, converting the light to macroscopic electronic pulses. The two polarisations are separated in a polarising beam-splitter and a zero or one is recorded depending on the detected polarisation. A random switch selects whether to measure in a 0° or 45° polarisation basis.

Due to the initial attenuation and the attenuation along the transmission line only very few of the sent pulses result in detected events at the receiver. A record of when the pulses are detected is kept and at the end of the transmission the receiver uses a classical channel (eg telephone line) to tell the sender which pulses arrived and what basis they were measured in. All lost pulses and all detected pulses measured in a different basis to the encoding basis are erased from the sender's record. Thus identical random keys are retained by sender and receiver. Any remaining differences (errors) signal the interception of an eavesdropper! If an eavesdropper measures the polarisation of one pulse, that pulse, being a single photon, is destroyed and does not reach Bob and thus is not incorporated in the key. The eavesdropper could choose a basis, measure the pulses then re-inject copies. However, this strategy has to fail because half the time the eavesdropper will have chosen the wrong measurement basis and the re-injected pulses will induce an error rate of 25%. Of course a certain level of error could be caused by imperfections in the equipment used, but in order to guarantee absolute security any error should be attributed to (partial) interception. Below a certain threshold the error can be corrected and potential knowledge of the key by any eavesdropper can be erased by privacy amplification protocols.

3. THE TOOLS

Compared to the original experiment using polarisation rotations performed by high-voltage Pockels-cells it is by far advantageous to use separate laser diodes for every polarisation at the transmitter. An additional simplification of the equipment can be achieved by randomly splitting the light in the receiver between the analysers for two bases by a non-polarising beamsplitter. This allowed us to design a long-range free space key exchange apparatus capable of exchanging keys over free space ranges greater than 20 km where diffraction/turbulence and absorption losses reach up to 20 dB.

3.1 Transmitter

The transmitter (figure 1) is designed round a 80 mm diameter transmit telescope. A novel miniature source of polarisation coded faint pulses approximating single photons is used[12]. This consists of four laser diodes (850 nm wavelength) arranged on a ring around a conical mirror. Each laser is rotated to produce one of the four polarisations: 0°, 90°, 45° or 135° and illuminates a spatial filter consisting of two pinholes with a diameter of 100 µm spaced at a distance of 9 mm. Since the overlap of the emission modes of the four laser diodes with the filter mode is rather poor, the initially very bright laser pulses are attenuated to about the required "one photon per pulse" level. The actual attenuation can be fine tuned by manipulating the diode current and precisely calibrated by optionally shining the light transmitting the spatial filter onto a single photon detector. The filter erases all spatial information about which laser diode fired. Spectral information is also not attainable by an eavesdropper, as the spectra of the four laser diodes well overlap with a width of about 3 nm in pulsed mode. A continuous wave alignment laser was also fed through the spatial filter in order to ease optimising the focussing of the receiver.

The beam from the filter transmitting only one spatial mode is transformed in a Galilean telescope to a collimated beam with a diameter of ~40 mm FWHM. Together with the alignment laser and the single photon detector, the whole system is mounted on a 25x50 cm breadboard, attached to a micro-radian sensitive pointing stage on a sturdy tripod. The lasers are randomly driven from a computer via a digital output card at 10 MHz repetition rate using sub-nanosecond duration pulses. This creates ~500 ps duration optical pulses randomly polarised in 0°, 90°, 45° or 135° directions. The computer uses a pre-stored random number to choose the polarisation for the present set of experiments. Alternatively, nearly real time generation was possible, where a sequence of bits produced by a quantum random number generator running at 20 MHz was produced in the second right before the transmission.

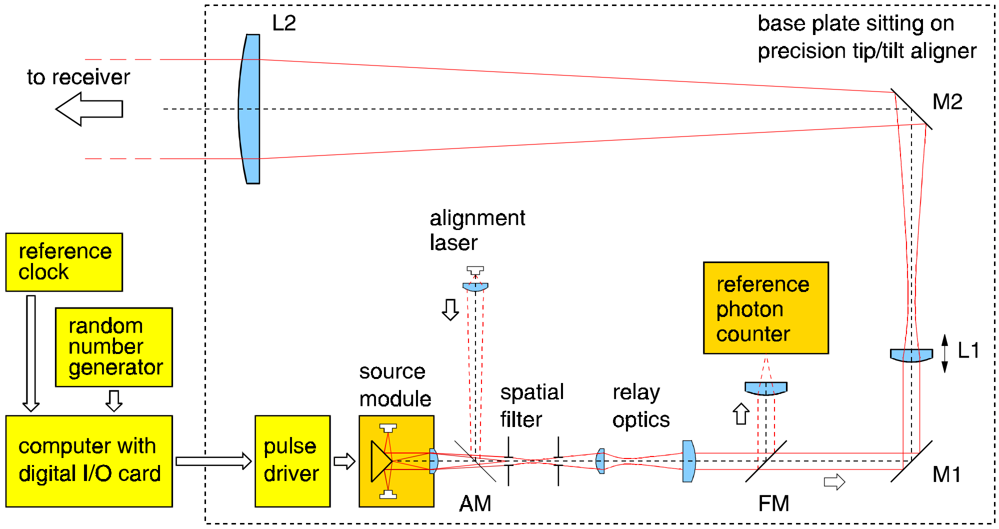


Figure 1: The Alice compact breadboard transmitter. The digital I/O card delivers a random 2-bit signal at 10 MHz synchronised to the reference clock. This signal is used in the pulse driver for randomly firing one of four lasers in the miniature source module. The four lasers are combined in a spatial filter using a conical mirror and relay lens. This system produces pulses with 0.05-0.5 photons per pulse. The output of the spatial filter is then transformed to a collimated beam with 2 mm FWHM and further expanded in a x20 telescope (L1 and L2) to produce a near diffraction-limited 40mm beam. A precision translator with lens L1 allows for the fine focus adjustment. A bright CW laser beam can be injected with an auxiliary mirror AM for alignment purposes into the the same spatial filter as the faint pulses, while a calibration of the number of photons per bit can be made by inserting mirror FM and measuring a reference photo-count. Mirrors AM, FM M1 and M2 are gold coated for high reflectivity in the infra-red.

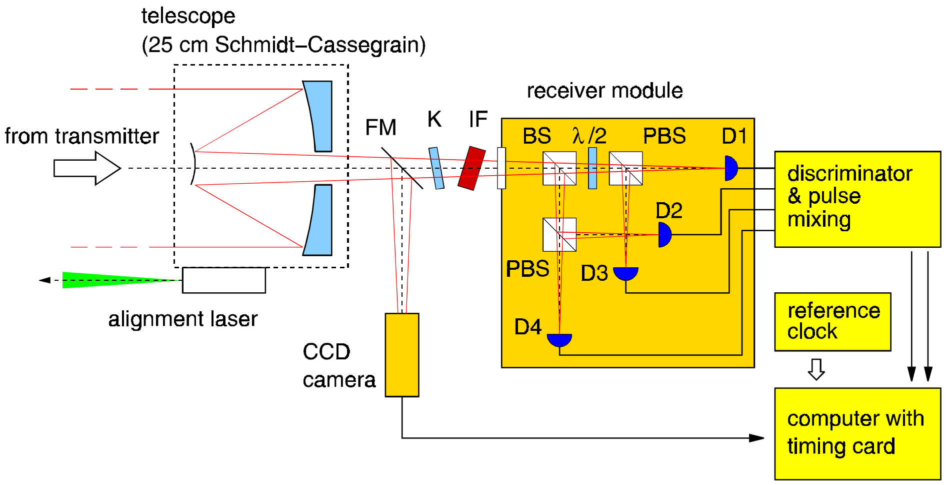


Figure 2 The receiver (Bob) consists of a 25 cm aperture Schmidt-Cassegrainian telescope. The miniature detector module is attached to the rear mounting of the telescope. It consists of a non-polarising beamsplitter (BS) followed by two polarising beamsplitters (PBS). Single photon detectors (D1-4) receive the output of the polarisers. In the D1/D3 arm, a half wave plate rotates the analysed polarisation to the 45° basis. The module incorporated high voltage supplies and discriminator circuitry to produce standard NIM pulses at the output. The detector outputs D3, D4 are combined with the D1, D2 outputs with a delay of 5 ns and input into the two channel timing card in the PC. A flip mirror allows a CCD camera to view the incoming light for alignment purposes.

3.1 Receiver

The receiver system (figure 2) consists of a 25 cm diameter commercial telescope (Meade LX200) with computer controlled pointing capability. Unfortunately, the resolution of the mechanics of this system was the limiting factor for the alignment of the receiver, and was also difficult to handle at the harsh outdoor conditions. Yet, the stability of the system was very convincing.

A compact four-detector photon counting module[12] was coupled to the back of the telescope after an RG780 long pass filter to block out short wavelength background. The module consists of a polarisation-insensitive beam-splitter passing two beams to polarising beamsplitters that are followed by four photon counting avalanche diodes. One polarising beamsplitter is preceded by a 45° polarisation rotator (half wave plate). Photons detected in this channel are thus measured in the 45° basis, while the other polariser allows measurement in the 0-90° basis. Since the splitting of incoming photons to the two analysers by the beamsplitter is truly random no random number sequence nor any space- and part-consuming optics is required on the receiver side – on the expense of more photodetectors, however.

The time of arrival of each photo-detection is recorded in the computer using a two-channel time digitisation card (Guide Technology GT654). Thus the four detectors outputs are combined into the two channels with a delay of 5 ns. The delay is then used to discriminate between the two measurement bases. The overall optical detection efficiency of the receiver is about 16%, timing jitter was smaller 1 ns.

3.1 Timing and synchronisation

The two separate computers were linked via modems operating over a standard mobile telephone link (9.6 Kbaud bit rate). Local oven-stabilised 10 MHz clocks were synchronised to better than l ns using a software phase locked loop driven by the received photo-detections. The photodetections thus can be gated in two 1.4 ns wide time windows separated by 5 ns. Pulses outside these timing gates are ignored. The error rate due to dark and background counts is thus suppressed by a factor of ~1/35. The random polarisation pulses are sent in 700 ms blocks preceded by a series of predetermined pseudo-random data sets lasting 110 ms to uniquely determine the start time of each block. Following the transmission of the block a settling time of ~300 ms allows the computers to verify a successful transmission. Gross block length is thus just over 1.1 s. Sifting and error correction of the 700 ms data blocks were then performed over the telephone link using software developed in our 1.9km experiment[9].

4. THE LONG-RANGE TRIAL

To avoid air turbulence effects the long range experiment was carried out over an elevated path with the receiver on Karwendelspitze and the transmitter located at a small experimental facility of the Max-Planck-Institute for Extraterrestrial Physics on the summit of Zugspitze, Southern Germany. Initial alignment of both transmitter and receiver was achieved by shining a low power green laser (3 mW) from Karwendelspitze which was clearly visible from Zugspitze. This was followed by a fine alignment using a ~500 µW beam at 850 nm passing through the same spatial filter as the faint light pulses in the Alice setup.

The collimation in the Alice system was adjusted to minimise the diameter at 23.4 km resulting in a beam 1-2 metres in diameter (depending on air turbulence). This led to lumped optical losses in the transmission path of about 18-20 dB. With a receiver efficiency of around 16% and using faint pulses containing 0.1 photons per bit the detected bit rate at Bob was about 1.5-2kilobit per second.

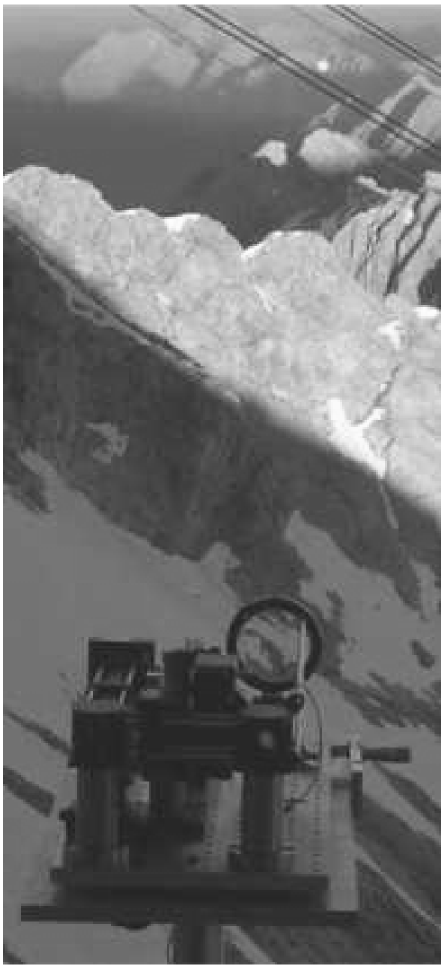
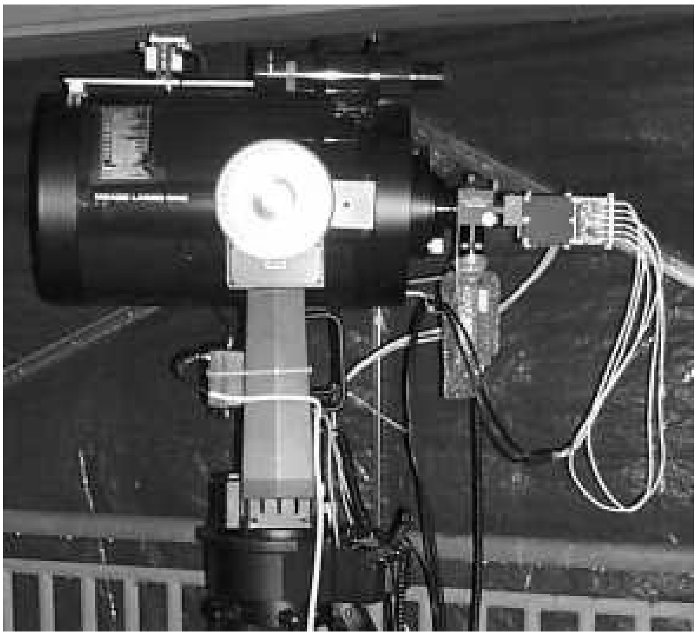


Figure 3 The Alice breadboard in the foreground with the green alignment laser clearly visible on Karwendelspitze in the background

Figure 4 The 25cm receiver telescope with compact detector module attached.



Several night trials were carried out at various times from September 2001 to January 2002. In the final trial several keys were exchanged over a period of three days at a selection of pulse intensities ranging from 0.4 to 0.08 photons per bit. Representative data are shown in table 1. Total gated photon rates (summed over all detectors) were 2-4 Kcps with dark counts dropping as low as 4 Kcps (actual detector dark counts summed to about 1Kcps). Background rates were high because of scattered light from snow cover and the use of simple coloured-glass short wave blocking filters. The bracketed figures in the error rate column represent the errors arising from background counts alone showing that half the error rate was from this source. The remaining errors of 2.1-2.7% arise from imperfections in the polarisation encoding and decoding. At these error levels the error correction efficiency was between 50 and 60%. The low bit rate (9.8KB) of the mobile telephone link was a limiting factor in the sifting and error correction process. The final net key rate is about 1/6 of the raw detected rate. A factor of 2 is lost in sifting, a further factor of ~2 in error correction and then the data block efficiency is about 66%. Typically the sifting rate was 2-300 raw key bits per second (about 4 bytes of timing data per key bit). The interactive error correction process proceeded at a similar rate but of course with half as many key bits after sifting. To save time longer blocks of raw key data were analysed offline as shown. One point to note is the error correction efficiency is better for these larger keys because of the need to estimate the error rate sacrificing some of the key before correction.

Table 1 Summary of selected experiments

Night	Number of photons per bit (+/-10%)	unsifted data bits/s	Background Bits/s	Quantum bit error rate %	Final net key rate Bits/s	Total key exchanged Bits
16/01	0.37	4484	6268	4.11 (1.96)	626	9395
16/01	0.27	2505	5504	5.24 (3.08)	396	4341
16/01	0.18	2651	5578	4.54 (2.94)	363	5448
17/01	0.096	2627	4516	4.77 (2.41)	367	5399

Sifted and corrected keys showed a high degree of randomness with little or no bias. An online check of the balance of received bits compared to sent bits could be performed. A typical matrix of sent versus measured polarisations is shown in figure 5. Care was taken to keep the diagonal values as close as possible.

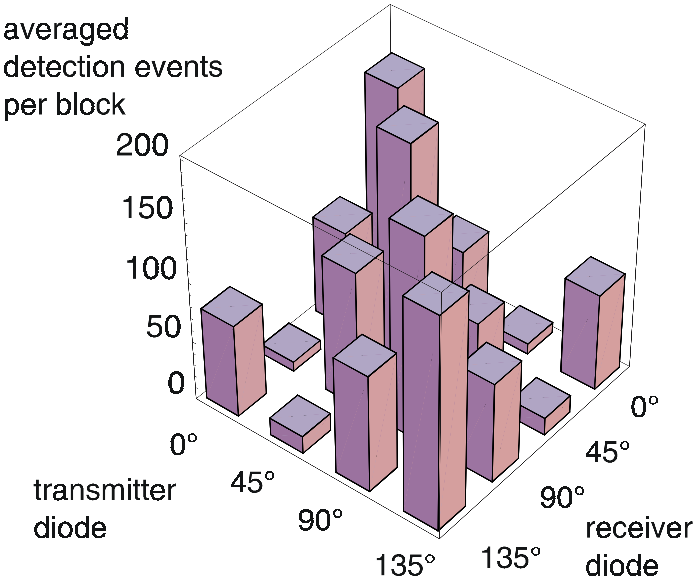


Figure 5: The detector matrix showing, on the diagonal, the number bits transmitted and measured in the same basis. The suppressed measurements are the 'errors', bits encoded and measured in the same basis but turning up in orthogonal channels (eg 0° and 90°). Measurements where different bases were used show roughly half the height of the diagonal, but constitute roughly half of all measurements.

5. CONCLUSIONS

As an important step towards satellite based quantum cryptography we have demonstrated a secure key exchange over a free space distance of 23.4 km. The atmospheric disturbances in this experiment are already of the same order as the expected disturbances when connecting with low orbit satellites. This demonstration thus yields first scalable results for the further design. Operation down to 0.08 photons per bit has been demonstrated with optical losses of about 18dB. A large fraction of errors arose from background counts but was still below 6 %. Improved performance including daylight operation is expected with improved spatial filtering at the reciever and narrow band-pass filter set to the correct wavelength together with accurate temperature control of the transmitter lasers. The apparatus showed high stability with the ambient temperatures in these experiments ranging from +5 °C to -25 °C. The polarisation preparation and analysis modules developed in this work were stable and required no adjustments over the whole temperature range. In fact this was quite a relief as system alignment is not a very pleasant task at 4:00 am, -20°C and 2960 m altitude.

ACKNOWLEDGEMENT

We gratefully acknowledge the hospitality of the Karwendelspitz cabel-car team and the Max-Planck Institute for extraterrestrial Physics, and the organisational back up of Kai Wede. Thanks to Karen Sauke, Oliver Schulz, Jürgen Volz and Markus Weber who assisted in various cold and longish night trials and in snow shoveling. The project was supported by the EU-Esprit project EQCSPOT and the German BMBF.

REFERENCES

1. See for instance 'The Code Book: the science of secrecy from ancient Egypt to Quantum Cryptography', Simon Singh, Anchor 1999.
2. C.H. Bennet, G. Brassard, Proc. Conf. Comp. Syst. And Signal Processing, Bangalore, pp 175 (1984).
3. P.D. Townsend, J.G. Rarity and P R Tapster, 'Single photon interference in a 10km long optical fibre interferometer', Electronics Letters 29, 1993, 634-5; ibid. 'Enhanced single photon fringe visibility in a 10km long prototype quantum cryptography channel', Electronics Letters 29, 1993, 1291-3.
4. Muller A., Breguet J. and Gisin N., 'Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km, Europhys. Lett. **23**, 383-388, (1993).
5. G. Ribordy, J-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, 'Fast and User-friendly Quantum Key Distribution', J. of Mod. Optics **47** (2/3), 517-531 (2000).
6. C H Bennett et al, 'Experimental Quantum Cryptography', J. Cryptology **5** (1992) 3-28
7. W.T.Buttler R.J. Hughes, S.K. Lamoureaux, G.L. Morgan, J.E.Nordholt and C.G. Peterson, 'Practical Free-Space Quantum Key Distribution over 1km', Phys.Rev.Letts, **81** (1998) 3283.
8. W.T. Buttler, R.J. Hughes, S.K. Lamoureaux, G.L. Morgan, J.E.Nordholtand C.G. Peterson, 'Daylight Quantum Key Distribution Over 1.6km', Phys.Rev.Letts, **84** (2000) 5652-5655.
9. J.G.Rarity, P.M.Gorman, and P.R.Tapster, 'Secure Key Exchange Over A 1.9km Free-space Range Using Quantum Cryptography', Electronics letters 37, 512-514, 2001; ibid Journal of Modern Optics 48, 1887 (2001)
10. Bennett C.H., Brassard G. and Robert J-M, Privacy Amplification by Public Discussion, SIAM Journal on Computing, (1988) **17**, pp210-229
11. G.Brassard and L.Salvail, Secret Key Reconciliation by public discussion, Adventures in Cryptology, EUROCRYPT93, Lecture Notes in Computer Science, Springer-Verlag. N.Y. (1994) **765,** pp410-423
12. C. Kurtsiefer, M. Halder, P. Zarda and H. Weinfurter, 'Miniature modules for quantum cryptography', to be published
13. J.G.Rarity, P.C.M.Owens and P R Tapster, 'Quantum Random Number Generation and Key Sharing', Journal of Modern Optics **41** (1994) 2435-2444.

*harald.weinfurter@physik.uni-muenchen.de, phone ++49-89-2180-2044, fax ++49-89-2180-5032, http://xqp.physik.uni-muenchen.de, Sektion Physik, University of Munich, Schellingstr. 4, D-80799 Munich, Germany.