# Towards Practical Quantum Cryptography

Surasak Chiangga[1,2], Patrick Zarda[1,4], Thomas Jennewein[3] Harald Weinfurter[4,5]
[1] Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria
[2] Department of Physics, Kasetsart University, Bangkok, Thailand 10900
[3] Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Wien, Austria
[4] Sektion Physik, Ludwig-Maximilians-Universität München, Schellingstr. 4/III, D-80799 München, Germany
[5] Max-Planck-Insitut für Quantenoptik, D-85748 Garching, Germany
(Appl. Phys. B, in print)

Quantum cryptography bases the security of quantum key exchange on the laws of quantum physics and is likely to become the first application employing quantum effects for communication. Here we present performance tests of a new design based on polarization encoding of attenuated, coherent light pulses. Our measurements show that this compact setup can achieve an effective key-bit rate in the kHz-range with low alignment requirements and thus offers the tools for fast and user-friendly quantum key exchange.

## I. INTRODUCTION

Quantum cryptography [1] is the most advanced method of the increasing number of quantum communication schemes. It allows provable secure key exchange and thus will form the basic ingredient of any trustworthy cryptographic scheme. The security does not rely on (yet unproven) assumptions about the complexity of mathematical algorithms but is firmly based on the laws of quantum physics. After the first experiments performed almost a decade ago [2,3], a number of different schemes and protocols have been implemented demonstrating their principle feasibility even over long fiber connections [4]. In order to become a real application quantum cryptography has to be further developed to establish its usefulness outside shielded lab environments. Moreover the devices have to become more stable and easier to operate as nowadays demonstration setups. Important steps along this direction have been the development of plug&play systems [5] and of free-space quantum cryptography [6]. These experiments show the feasibility of user-friendly long-distance fiber schemes and the possibility of key-exchange to satellites, which might finally bridge any terrestial distance. Quantum cryptography is very likely to become the first application exploiting the particular properties of single quanta. But for a general acceptance of this new technology it is necessary to devise systems which are both compact and reliable, but also affordable and user-friendly.

Here we present tests of a setup employing the classic BB84 protocol with polarization encoding [1]. Contrary to other demonstrations of quantum cryptography, our system does not use active manipulation devices, like Pockels cells, for setting or analyzing the polarization. Instead, four randomly switched laser diodes are polarized along the necessary directions. The randomness of Bob's polarization analysis is ensured by the inherent quantum nature of detecting single photons behind a beam splitter, which is used to divert the beams to the polarization analyzers. In addition, a new synchronization scheme is implemented directly along the quantum channel, which allows to synchronize sender and receiver electronics to better than 3ns with minimal usage of channel capacity. Together with the high pulse frequency of 2 MHz and a low qubit-error rate (QBER) of 1.21% a high key rate of more than one kbit/sec becomes possible.

## II. THE CONCEPT

Quantum cryptography uses basic laws of quantum physics to guarantee secure key exchange. The key can be used with unprecedented confidence in any classic cryptographic protocol, where it increases the security to the maximum achievable value. Together with the "one time pad" encoding [7], which is provably unbreakable provided the key is known solely to sender and receiver, absolutely secure communication becomes possible.

The security of quantum cryptography is based on the fact that, after the measurement of one quantum observable, one can not infere the possible values of a second, non-commuting observable. This observation led Bennett and Brassard to the following protocol for secure key exchange [1]. Alice transmits single photons polarized randomly along one of the directions H, V, +45°, and -45° through the quantum channel to Bob. He then analyzes the photon, randomly along one of the same four directions. If both used the same observable basis, that means either H and V, or +45° and -45°, they have perfect correlation between their settings and can use these events to establish the secret key bits. An eavesdropper intercepting the quantum channel will cause errors in this bit string (as an example, Fig. 1 shows an eavesdropper who intercepts the quantum channel and mimics Bob to Alice, and acts like Alice for Bob). Any attack of the eavesdropper in order to increase his knowledge about the key, either by direct measurement or even by entan-

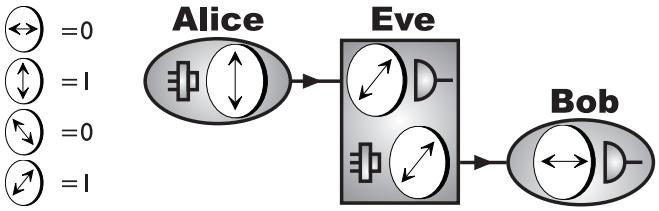


FIG. 1. Principle idea of quantum cryptography: Alice and Bob switch randomly and independently the preparation and analyzation basis for the weak coherent pulses between four non-orthogonal directions. Any eavesdropper attack then necessarily causes errors in the bit-string shared by Alice and Bob.

gling his probe to one or more transmitted photons, will increase the probability of wrong key bits [8].

The main design goals for our system are reliability with a minimum need of alignment during operation, but also keeping in mind that the modules should be well-priced and compact. The modules are designed to operate in the near-IR-telecommunication window at 853 nm, which is equally well suited for fiber-connections within local area networks (LAN) and for free-space quantum channels. Silicon single-photon avalanche detectors (SPAD) have a high quantum efficiency at this wavelength and very low dark count rates, compared to Germanium- or InGaAs-detectors for the 1.3$\mu$m or 1.5$\mu$m regimes. Thus the coincidence gate times, pulse width and synchronization specifications can be considerably relaxed. All the optics of the sender and receiver modules are built with discrete optical components, utilizing the high quality and low price of commercially available near-IR optics. As we will see in the following section, this also adds to the simplification and to the stability of the devices.

## III. SETUP OF SENDER AND RECEIVER MODULES

The general layout of the sender and receiver modules of Alice and Bob is shown in Fig. 2. In Alice's sender four single mode laser diodes (5 mW) are used to produce the weak coherent pulses which are then sent to Bob [9]. At a rate of 2 MHz, one of the four laser diodes is switched on for 10ns according to a (pseudo-) random 2 bit pattern requested from a DI/DO-PC-interface card. The diodes are oriented roughly at either horizontal or vertical orientation, and in pairs, their light is overlapped at two polarizing beam splitters (PBS) giving vertically polarized light from the reflected beam and horizontal polarization from the transmitted one, respectively. The polarization of one of the two resulting beams is rotated by a half-wave plate by 45° to give the necessary +45° and -45° output pulses. Finally, these two beams are overlapped at a non-polarizing hybrid beam splitter (BS). This beam splitter has very good reflection/transmission ratio of close to one, however, the internal birefringence of such a beam splitter slightly complicates the scheme. A relative phase shift between horizontal and vertical polarization (on the order of 20°) does not influence the H and V polarization, but changes the ±45° orientations into ellipticaly polarized light. This effect is smaller in transmission but still has to be precompensated in the ±45°-arm with suitably adjusted quartz plates. All laser diodes and beam splitter cubes have a size of about 5 mm and are well suited for further minituarization of the setup. Behind the beam splitter BS a lens (f=30cm) collimates the very divergent beams to facilitate coupling into a fiber or free-space optics at the output of Alice's module.

We want to emphasize that no further lens was used so far. The divergent light emitted by the laser diodes was transmitted through a series of pin holes (PH) and was thereby considerably attenuated between the laser diodes and Alice's output. This loss, however, is necessary for the quantum cryptography scheme, since only strongly attenuated coherent pulses (mean photon number $\approx 0.1$) can be used to avoid simple beam splitting attacks by the eavesdropper. Due to the huge divergence of the emitted light small mechanical drifts of the components do not change the output. This simplifies alignment requirements for the diodes and beam splitters and enhances the stability of the modules. Moreover, there are no fast switching high-voltage Pockels-cells needed for such a setup, the same randomly polarized pulses are generated by simply switching on and off the four laser diodes.

Bob's receiver is built symmetrically to Alice's sender. After coupling out of the quantum channel, a non polarizing beam splitter splits the incoming light quanta into a coherent superposition of going to the polarization analyzer oriented along H/V or to another one, which, after a half-wave plate, analyzes the polarization along ±45°. Due to the birefringence of the beam splitter BS, it is recommended to perform the ±45° analysis in the beam transmitted by the beam splitter after compensation. The coherent superposition causes an ideal, non-deterministic random choice of the analysis direction. The detection process itself gives the information about both, the choice of the basis and the result of the analysis in this basis.

As detectors we used passively quenched Silicon single photon avalanche detectors operated in the Geiger mode. The diodes were equipped with a double stage thermoelectric cooler and do not need any further water cooling etc. At room temperature the diodes can be cooled down to -30°C reducing the dark count rate to below 300 counts/s. Narrow band interference filters ($\Delta\lambda = 5$ nm) reduce the sensibility against stray light.

The choice of 2 MHz for the basic clock frequency of our modules is a compromise between high pulse rate and the limitation brought by the achievable count rate. When operating Si-SPADs in passive quenched mode, they are very reliable and survive high light inputs with-

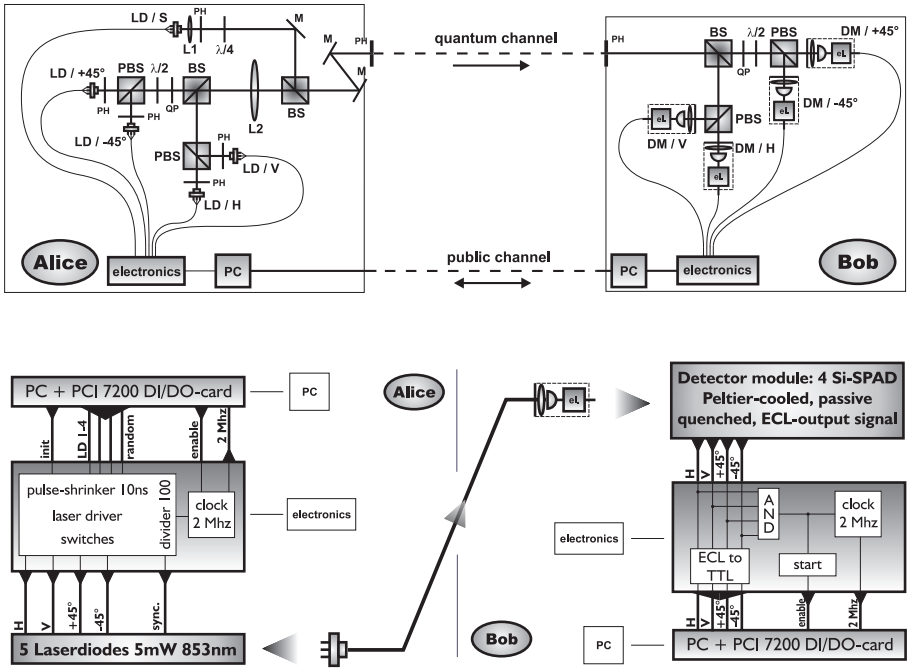


FIG. 2. Layout of the sender and receiver modules: (top) optical setup: 4 laser-diodes are pulsed to generate faint pulses with different polarization at the output (LD/H for horizontal polarization, etc.). The pulses are overlapped by polarizing (PBS) and non-polarizing beam splitters (BS) and collimated by lens L2. Pinholes (PH) are used to attenuate the light and to set the mean number of photons to about 0.1 per pulse. Additionally, bright synchronization pulses are generated by diode LD/S. At Bob's receiver random choice of the polarization analysis is achieved by splitting the incoming beam at BS and registering the detections at the single photon avalanche detectors (DM/H, etc.). (bottom) electronics: At a rate of 2 MHz a (pseudo-) random 2bit pattern is requested from the PC. Accordingly one of the four laser-diodes is pulsed for 10ns. At the receiver the detection events are sampled as a 4bit pattern to enable two-photon detection analysis. Synchronization is achieved by clock-recovery circuitry at the receiver, triggered by a four-fold coincidence.

out damage. However, the dead time is about 1 $\mu$s, which therefore limits acceptable count rates to about 100000 counts/s. Higher count rates would become possible if one reduces the dead time, either by active quenching or, significantly simpler, by gating the overbias of the Si-SPADs.

The clicks of the detectors are sampled via a DI/DO-PC-interface card as a 4 bit pattern to enable the software analysis of two-photon detections. This sampling of Bob's detection events has to be gated synchronously with the pulses generated by Alice's sender module. The low dark count rate of the Si-SPADs allows to relax the gate time to as much as 20 ns (thus causing a dark count rate related erroneous detection with a probability as low as $10^{-7}$ per gate time). Still, a synchronization of Alice's and Bob's clocks is necessary to within a fraction of the gate time. Keeping our design goals in mind, we decided to use optical synchronization via the quantum channel. When using the quantum channel for other purposes than key exchange, one should be concerned about not using to much of the channel capacity urgently needed for key generation. A simple and reliable clock recovery circuitry allows to reduce the extra usage of the quantum channel to 3%. A very positive side effect is, that no run-time calibration of the pulses between Alice and Bob is needed, since the very same link is used both for synchronization and for secret key exchange.

The synchronization operates as follows: after 97 randomly polarized, weak coherent pulses of the four laser diodes a fifth laser diode (LD/S in Fig. 2) is triggered. The light of this laser is collimated right after the diode, resulting in a pulse $10^5$ times stronger compared to light from the other diodes. The polarization is transformed into circular orientation by a quarter-wave plate and coupled by an additional beam splitter into the output of Alice's sender module. After arriving at Bob's receiver this pulse will cause detection events in all four detectors due to its brightness and its polarization. The four-fold coincidence event triggers the clock recovery pulse. After amplification, the harmonics at 2MHz of the pulse is filtered by exactly the same quartz circuitry which generates the original clock in Alice's module. Two more time cycles were paused to allow the amplifiers and the detectors to recover from saturation after the synchronization pulse. With this scheme the 2MHz clock signal can be

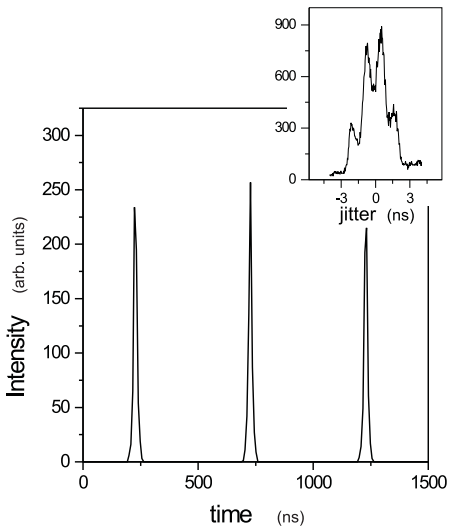


FIG. 3. Intensity of the last three pulses of a synchronization sequence (obtained from one laser diode focused on a photo diode). The inset shows the jitter of the time difference between Alice's last pulse and Bob's last gate interval.

recovered from the 20kHz synchronization pulses with a jitter as low as 3ns.

## IV. PERFORMANCE TESTS

The test setup was mounted on standard optical breadboards with commercial mounts for bulk optics. The goal of the test measurements was to evaluate various components implemented in this design, in particular the laser-diodes, polarizing and non-polarizing beam splitters and the Si-SPADs control electronics. These components will be implemented in a next, miniaturized version [10].

Figure 3 shows the last three pulses of a sequence, right before a new synchronization pulse. Here the light of the laser-diode was directly focused on a photo diode. The timing jitter between Alice's last pulse and Bob's last gate interval is displayed in the inset. The width of the distribution is less than 3ns, with the structure originating from reflections in the electronics. The jitter is by far sufficient for the timing of the coincidence gates with a width of 20 ns. In order to set the number of photons per pulse to about 0.1 a Hanburry-Brown-Twiss setup was used to measure the two-photon probability directly at Alice's output.

The polarization of the attenuated pulses was evaluated directly at Alice's output by a polarcor polarization filter and a single photon detector (Fig. 4a). We deduce the qubit-error rate (QBER) from the ratio of the counts in the H-detector produced from V-polarized pulses versus the counts produced from the same number of H-polarized pulses, and similar for the other three directions. After compensating the birefringence of the

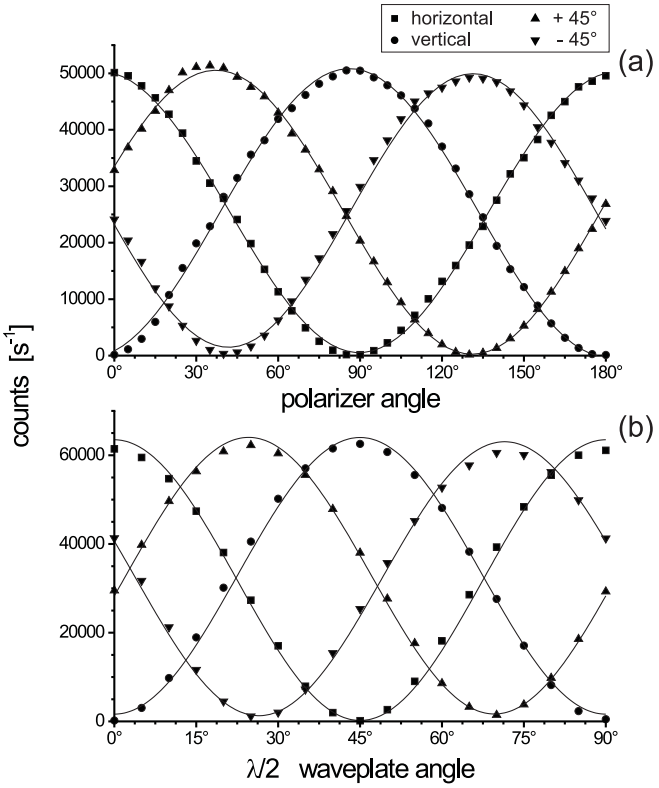


FIG. 4. Polarization analysis: (a) Rotating a polarizing filter at the output of Alice's sender one obtains a qubit-error rate (QBER) of the polarized pulses below 0.4%. (b) The analysis performed by Bob's receiver gives the combined QBER of the whole setup (including transmission through 2m single mode fiber). The rate of 1.21% permits efficient and secure key exchange.

non-polarizing beam splitters one achieves low noise also for the $\pm 45°$ directions resulting in a QBER of 0.4% at Alice's output. When coupling these pulses via a 2m fiber into Bob's unit we obtain the net noise rate of sender and receiver units. Figure 4b shows the various count rates at Bob's detectors, when rotating an additional half-wave plate in front of the unit [11]. Analyzing these count-rates, we obtain a mean QBER of 1.2% (H 0.33%, V 0.22%, $+45°$ 2.68%, and $-45°$ 1.61%).

## V. OUTLOOK

Quantum cryptography will become the first application out of the recently proposed quantum communication schemes, provided these quantum devices can be operated without any adjustment and alignment by the user and in virtually any environment, and also can be produced at affordable costs. We presented a new design of sender and receiver modules, with a significantly reduced sensitivity to mechanical and thermal drifts. The components evaluated in this performance test can be readily

used in the next version, where the optical setup will be reduced to a size of about 10cm × 10cm. The achieved qubit-error rate is reasonable, and can be improved when further reducing the error for the ±45° basis. Furthermore, the synchronization scheme has proven its utility: With a minimum usage of the quantum channel the two clocks at Alice and Bob can be synchronized to a precision which matches the timing requirements when using Silicon single-photon avalanche detectors.

Addressing the security needs for a quantum cryptography system and to increase its performance and reliability, one might want to add some improvements to the design. In the setup using 4 laser-diodes, one has to take care, that all laser emit at the same frequency. Otherwise an eavesdropper attack would be possible where the sent polarization is deduced from the frequency. To avoid such an interception, one should lock all four laser diodes to another free running laser diode. Along any quantum channel, there will be some rotation of the polarization bases. Therefore, in the next step, an additional polarization control unit has to be implemented, best at Bob's receiver unit [12]. For (auto-) alignment of the unit, the sender module will emit light continuously in order to get high count rates for matching the polarization bases. We propose to use bulk optics or liquid crystals in this case, since contrary to fiber components, one can adjust the two bases independently, thus simplifying the task.

Finally, one of course would like to increase the rate for generating the secure key. As mentioned, the value of 2 MHz was chosen according to the achievable count rate of the single photon detectors. Altogether, for example with a 10% loss along the quantum channel (corresponding to a fiber length of 3.5 km), one still can obtain a high key rate of about 1 kHz [13]. Reducing the dead time of the single photon detectors by active quenching or by gating the avalanche diodes can increase the maximum count rate. The increased key rate will make quantum cryptography a useful tool for secure communication.

## VI. ACKNOWLEDGMENT

This work was supported by the Austrian Science Foundation FWF Project Y48-PHY, the Austrian Academy of Sciences, the Austrian Academic Exchange, and ESPRIT-project EQCSPOT.

[1] C. H. Bennett, G. Brassard, Proc. Internat. Conf. Computer Systems and Signal Processing, Bangalore, pp. 175 (1984).

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[3] C. H. Bennett, G. Brassard, A. Ekert, Scientific American, pp.26, October 1992.

[4] A. Muller, J. Breguet, N. Gisin, Europhys. Lett. **23**, 383 (1993); J.D. Franson, B.C. Jacobs, Electron. Lett. **31**, 232 (1995); C. Marand, P.D. Townsend, Opt. Lett. **20**, 1695 (1995); R.J. Hughes, G.G. Luther, G.L. Morgan, C.G. Peterson, C. Simmons, Lect. Notes in Comp. Sci. **1109**, 329 (1996).

[5] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).

[6] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998).

[7] G.S. Vernam, J. Am. Inst. Elec. Eng. **55**, 109 (1926).

[8] C. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997); I. Cirac, N. Gisin, Phys. Lett. A **229**, 1 (1997).

[9] N. Lütkenhaus, G. Brassard, T. Mor, B.C. Sanders, to be published.

[10] The components of the final tests presented here are 850nm, 5mW, single mode laser diodes from Sharp, polarizing and non-polarizing beam splitters from Melles-Griot, half-wave and quarz plates from Casix, and Si-SPADs from EG&G.

[11] The count rates from different detectors vary due to slight differences in the quantum efficiency. Because of the losses of the polarizing filter used in Fig. 4a and new alignment the rates are even slightly higher in Fig. 4b.

[12] The design most likely has to be changed when considering quantum cryptography in a net work. The high price of the Si-SPADs makes it necessary to use schemes where many Alices exchange keys with a single (trusted) Bob. Then the synchronization and polarization alignment has to be performed in the sender modules.

[13] H. Zbinden, in *Introduction to Quantum Computation*, ed. H.-K. Lo, S. Popescu, T. P. Spiller, (Clarendon Press, Oxford) 1998.