Appl. Phys. B 79, 273–277 (2004)
DOI: 10.1007/s00340-004-1574-7

Applied Physics B
Lasers and Optics

S. LORENZ[1,✉]
N. KOROLKOVA[2,1]
G. LEUCHS[1]

Continuous-variable quantum key distribution using polarization encoding and post selection

[1] Institute of Optics, Information and Photonics, Max Planck Research Group, University Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany
[2] School of Physics and Astronomy, University of St. Andrews, North Haugh, St. Andrews KY16 9SS, UK

Received: 6 February 2004/Revised version: 14 May 2004
Published online: 29 June 2004 •

ABSTRACT We present an experimental demonstration of a quantum key distribution protocol using coherent polarization states. Post selection is used to ensure a low error rate and security against beam-splitting attacks even in the presence of high losses. Signal encoding and readout in polarization bases avoids the difficult task of sending a local oscillator with the quantum channel. This makes our setup robust and easy to implement. A shared key was established for losses up to 64%.

PACS 03.67.-a; 03.67.Dd; 42.50.Lc; 42.50.-p

1 Introduction

The first quantum cryptography protocols used measurements of non-commuting observables of single photons to establish a secret shared key between two parties [1]. By evaluating the errors in the shared key, it is possible to spot a potential eavesdropper and estimate his knowledge about the key. As there are no reliable, deterministic and fast single-photon sources available at the moment, most implementations of such single-photon systems use weak coherent pulses instead. Due to the problem of multi-photon components of coherent states in those systems [2], the effective amplitude has to be very low, which again impairs the performance. A second drawback is the lack of fast and efficient single-photon detectors, whereas bright-light photoreceivers work with nearly unit quantum efficiency at high speeds. Thus, a number of new quantum cryptography systems employing coherent states have been proposed [3–6]. To establish a shared key when the state is attenuated – single photons are either completely lost or transmitted – special techniques have been proposed [7, 8]. Reverse reconciliation used in [9] demonstrated for the first time the robustness of continuous-variable systems against losses of more than 3 dB, but it requires strict one-way communication and relies on interferometric stability for the transmission of a local oscillator beam. For low transmission losses a cryptography system using post selection [7] of quadrature measurements was presented in [10, 11], using also a separate phase-reference pulse. In this work, we demonstrate experimentally for the first time that post selection of coherent states can also establish a shared key in the presence of high losses. In contrast to other experiments [9, 10], which encode information in the phase of coherent states, we use polarization encoding. This dispenses with the need for a separate local oscillator beam and increases detection efficiency, making our system more suitable for practical applications.

✉ Fax: +49-9131/13508,
E-mail: stefan.lorenz@physik.uni-erlangen.de

2 Post selection

A coherent state with amplitude α is an eigenstate of the annihilation operator $\hat{a}$ and can be represented as an expansion in the Fock basis with photon number $n = \langle\hat{n}\rangle = \langle\hat{a}^\dagger\hat{a}\rangle$ [12]:

$$|\alpha\rangle = \mathrm{e}^{-\frac{|\alpha|^2}{2}} \sum \frac{\alpha^n}{(n!)^{\frac{1}{2}}}|n\rangle. \tag{1}$$

As formulated by the Heisenberg uncertainty principle, a coherent state occupies a certain area in phase space, such that two coherent states $|+\alpha\rangle = \mathrm{e}^{\mathrm{i}0}|\alpha\rangle$ and $|-\alpha\rangle = \mathrm{e}^{\mathrm{i}\pi}|\alpha\rangle$ exhibit an overlap

$$f = \mathrm{e}^{-2|\alpha|^2}. \tag{2}$$

As a result, a measurement of the quadrature amplitude $x = \langle\hat{a}^\dagger + \hat{a}\rangle$ cannot discriminate deterministically between $|+\alpha\rangle$ and $|-\alpha\rangle$ for small $|\alpha|$, as measuring $|+\alpha\rangle$ may yield results that could have been produced by a measurement of a $|-\alpha\rangle$ state, and vice versa. When a sender (Alice) prepares randomly one of the two non-orthogonal states, and a receiver (Bob) guesses which state it was by measuring x, his error probability $p_\mathrm{e} = \mathrm{Prob}(x < 0 \,|\, |+\alpha\rangle) + \mathrm{Prob}(x > 0 \,|\, |-\alpha\rangle)$ is directly linked to the amplitude $|\alpha|$ and the resulting overlap f. The shared information between Alice and Bob, I_AB, can then be determined. It depends on Alice's amplitude $|\alpha|$, Bob's amplitude measurement result x and the transmission η of the channel between Alice and Bob [5, 7, 13]:

$$I_\mathrm{AB} = 1 + p_\mathrm{e}\log_2 p_\mathrm{e} + (1 - p_\mathrm{e})\log_2(1 - p_\mathrm{e}). \tag{3}$$

We now consider a beam-splitting attack, where a potential eavesdropper (Eve) splits off part of the signal that is lost in

the channel with transmittivity η, and transmits the rest with a hypothetical lossless channel, such that her presence is undetectable. Eve can then make measurements on her part of the signal, e.g. an amplitude measurement like Bob. A crucial point in the experiment is that for coherent states Eve's and Bob's individual measurement outcomes are independent within their respective probability distributions. Thus Eve may obtain inconclusive results while Bob is quite confident about the state Alice prepared, and vice versa. Alice and Bob can determine the error probability and mutual information I_{AB} for each single event after the measurement. The average information Eve can get depends on the amplitude α Alice prepares and Eve's portion of the signal (in this case $\sqrt{1-\eta}$), giving a mutual information of I_{AE} between Alice and Eve. For a given channel transmission η and a state overlap governed by $|\alpha|$ a threshold x_{T} for Bob's measurement can be given, so that all his results with $|x| > t$ meet the condition $I_{\mathrm{AB}} > I_{\mathrm{AE}}$. The shared knowledge between Alice and Bob about such events is larger than that shared between Alice and Eve, allowing a secret key to be distilled. The process of sorting out those events which are favourable for Alice and Bob after the data have been recorded is called post selection [7].

3 Polarization states

The measurement of conjugate quadratures (e.g. amplitude and phase) of an optical mode normally requires a separate phase reference (local oscillator). Our system utilizes the quantum polarization of a two-mode coherent state, providing its own built-in strong reference field. The quantum Stokes operators are used throughout this work to describe the quantum polarization. They are defined in analogy to the classical Stokes parameters [14]. If one defines the annihilation operators $\hat{a}_{x/y}$ for two orthogonal polarization modes the Stokes operators read

$$\hat{S}_0 = \hat{a}_x^\dagger \hat{a}_x + \hat{a}_y^\dagger \hat{a}_y, \quad \hat{S}_1 = \hat{a}_x^\dagger \hat{a}_x - \hat{a}_y^\dagger \hat{a}_y,$$
$$\hat{S}_2 = \hat{a}_x^\dagger \hat{a}_y + \hat{a}_y^\dagger \hat{a}_x, \quad \hat{S}_3 = \mathrm{i}(\hat{a}_y^\dagger \hat{a}_x - \hat{a}_x^\dagger \hat{a}_y). \tag{4}$$

Their commutator and the corresponding uncertainty relations (with V denoting the variance)

$$\left[\hat{S}_k, \hat{S}_l\right] = 2\mathrm{i}\varepsilon_{klm}\hat{S}_m, \quad k,l,m = 1,2,3, \tag{5}$$
$$V_k V_l \geq |\varepsilon_{klm}\langle \hat{S}_m\rangle|^2 \tag{6}$$

ensure that no two operators can be measured simultaneously with certainty, as long as the third is nonzero. This behaviour is similar to quadrature operators, with the exception that the size of the uncertainty area of two observables depends on the mean value of the third. In the experiment, the S_1 component is chosen to be large, which corresponds to an almost completely horizontally polarized light beam with S_2 and S_3 as non-commuting observables. The state overlap in S_2 and S_3 can be utilized analogous to the state overlap in field quadratures. The Stokes operators are measured by direct detection [14]. The mode with high photon number $\hat{a}_x$ is used as a phase reference to determine the photon number in the dark mode $\hat{a}_y$ of orthogonal polarization. The S_2 and S_3 components can be measured by applying appropriate phase shifts between $\hat{a}_x$ and $\hat{a}_y$ and using a balanced photodetector. Note that in conventional homodyne detection, the signal and the local oscillator are in two spatially separated modes. Thus the spatial overlap and the phase stability limit the efficiency of such a setup, while our polarization setup has perfect spatial overlap and a stable relative phase by default without active control.

4 Protocol

The key-distribution protocol works with a BB84-type prepare and measure strategy. By small modulations of the S_1-polarized cw beam, four coherent states with slightly positive (negative) $\langle\hat{S}_2\rangle$ and $\langle\hat{S}_3\rangle$ are produced. Figure 1 shows possible measurement outcomes for Bob, when he uses a 50 : 50 beam splitter to measure S_2 on one half, and S_3 on the other half of the beam (see also Fig. 5). Alice prepares randomly one of these four states and Bob chooses randomly a measurement basis out of S_2 and S_3. By assigning a bit value '1' ('0') to a positive (negative) measurement result, a shared key can be established. Then Bob discards all results that did not exceed the post-selection threshold. He then announces his measurement bases through the public channel so that Alice knows Bob's measurement result with high probability. In the case of vanishing overlap between the states, this procedure is deterministic and hence insecure. An eavesdropper may discriminate between all four states and launch an intercept/resend-type attack without being noticed. By using states with a considerable overlap, the error probability for Eve increases, while Bob and Alice can post select favourable events.

5 Experiment

Our experimental apparatus consists of independent setups for Alice and Bob, which are separated by roughly 30 cm. Alice controls the laser source and the state preparation. Bob performs the polarization measurements on the states he receives from Alice.

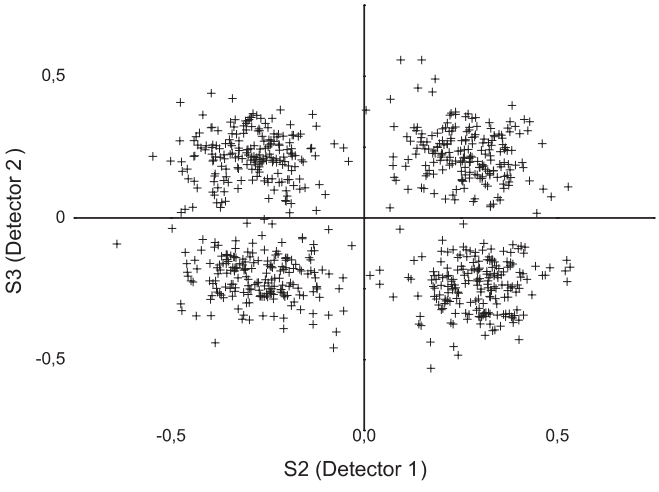

FIGURE 1 Plot of possible Q-function measurement results for Bob. Alice produces four coherent states with either positive or negative S_2 and S_3 polarization. In the experiment, the state overlap is high; thus the states cannot be distinguished. In this figure, the overlap is low for better visualization

5.1 *Alice*

Her schematic setup is shown in Fig. 2. As a light source a commercial diode laser is used (TOPTICA DL100). The diode provides up to 40 mW cw optical power and is wavelength stabilized to 810 nm. After mode cleaning of the laser light by a standard telecom fibre (SMF 1528) it is polarized in the S_1 direction using two polarizing beam splitters for improved purity. The S_3 modulation is achieved by an electro-optical modulator (EOM). The S_2 modulation of the beam is done by a magneto-optical modulator (MOM) which uses the Faraday effect of a magneto-optically active glass rod (Moltech MOS-04). The overall attenuation of the sender setup was adjusted to give a cw output power of 0.5 mW of S_1-polarized light. By controlling the applied modulation voltage on the EOM and the current through the MOM coil, the polarization amplitude in the S_3 and S_2 directions can be adjusted continuously. Each single event in the experiment is represented by a 500 μs-long interval of modulation on the continuous S_1 beam, i.e. a control-voltage pulse on the modulators.

5.2 *Bob*

At the receiving station Bob measures either the S_2 or the S_3 displacement. The incoming beam polarization is adjusted according to [14] by a half-wave plate and a second EOM (see Fig. 3). To switch between S_2 and S_3 the EOM changes from 'no retardation' to 'quarter-wave retardation'. The beam is focussed by a lens through a high-quality calcite Wollaston polarizer with an extinction coefficient higher than 10^6. The two resulting beams are each reflected by a low-loss mirror onto silicon PIN photodiodes (Hamamatsu S3883). The detectors show a linear behaviour up to 1 mW incident power. With an incident power of 250 μW, the electronic noise is more than 10 dB below the signal noise for modulation frequencies above 20 kHz. The signal is recorded by a fast digitizing oscilloscope (Tektronix TDS 420) and transferred to a computer for Bob's data processing.

For each event the detector voltage was recorded with 50 samples at a 100-kHz sample rate (see Fig. 4). By integrating over the central 26 samples, which is the duration of Alice's modulation pulse, the event can be recovered from the recorded data. This integral is Bob's final measurement value x, which is later used to determine if he keeps it to create the raw key or discards it if it lies below the threshold value x_T.

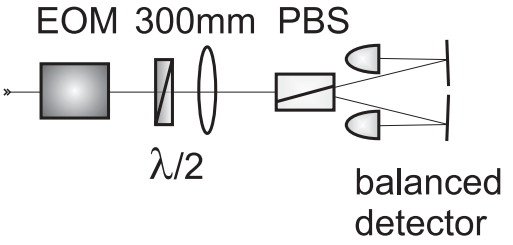

FIGURE 3 Schematic view of Bob's setup

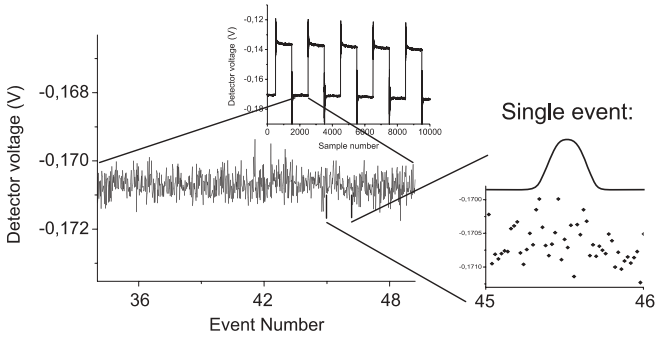

FIGURE 4 A typical oscilloscope trace of the detector signal with constant basis. Owing to the large overlap the signal modulation is not apparent in the graph. The *inset* shows the whole trace, with visible jumps due to basis switching by the EOM. A single event, with modulation pattern (*solid line*) and oscilloscope samples (*dots*) is shown on the *right*

6 Results

To show the independence between single results of the two measurement distributions in the case of a beam-splitting attack, the signal is divided by a 50 : 50 splitter and measured by two Stokes detector setups (see Fig. 5). When both detectors are set to measure in the same basis (in this case S_2), an unmodulated S_1-polarized coherent state gives rise to independent Gaussian distributions in each detector. The results of detector 1 and detector 2 are uncorrelated, as can be seen in Fig. 6 (left). For a S_2 modulation with low amplitude, the plot (Fig. 6, right) shows a slight ellipticity, revealing small correlations between the signals of the two de-

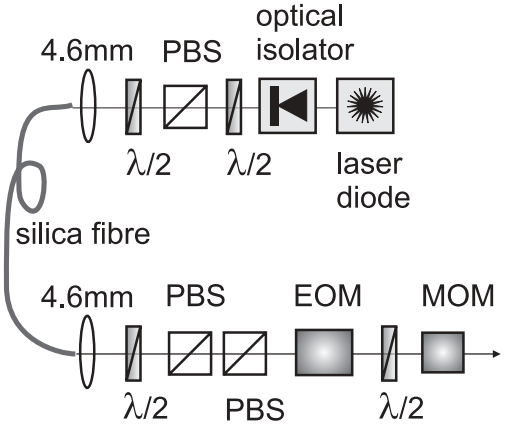

FIGURE 2 Schematic view of Alice's setup

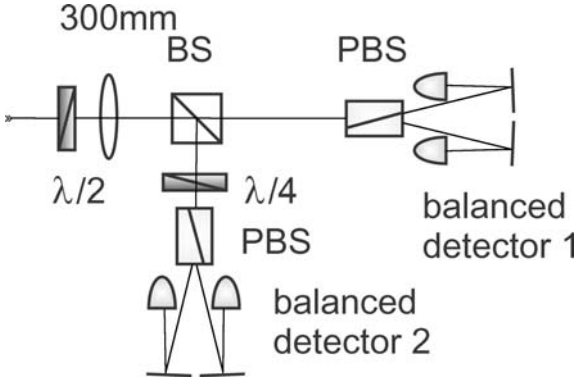

FIGURE 5 Schematic view of Bob's setup, using two detection setups to measure simultaneously S_2 and S_3 with a loss of 50%. If the quarter-wave plate is removed, S_2 can be measured on both halves of the original beams

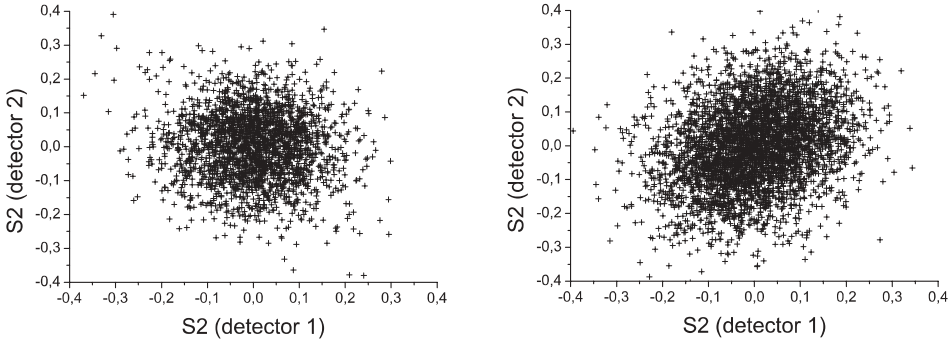

FIGURE 6 Signal divided by a 50 : 50 beam splitter and measured by two S_2 detectors. *Left*: no S_2 modulation of the signal. *Right*: small S_2 modulation, correlations of the two detected signals result in the elliptical shape of the scatter plot. As detector 1 and detector 2 have slightly different gains, a small horizontal ellipticity is introduced in both graphs

tectors. Although the two parties share common information it is not possible to deduce the sign of the measurement result of one detector from the outcome of the other detector with certainty. A potential eavesdropper who uses detector 2 cannot infer the results of detector 1, even though she has measured 50% of the signal. Note that the setup of Fig. 5 was also used with one S_2 and one S_3 detector to produce Fig. 1. In the Quantum Key Distribution (QKD) experiments, only a single detector with electro-optical basis switching (see Fig. 3) was used. The losses due to non-unity photodiode efficiency, limited EOM transmittivity and optical imperfections in the detector were treated as if they were transmission-channel losses. This conservative point of view implies that Eve could manipulate Bob's receiver and increase its efficiency while sending more imperfect states at the same time, gaining additional information. With an additional attenuator between Alice and Bob, the overall transmission levels were set to either 79% or 36%. The modulation was adjusted to give an average coherent amplitude of $|\alpha| = 0.6$ in the dark mode $\hat{a}_y$, yielding an overlap of $f = 0.5$ according to (2). A typical dataset acquired by Bob's measurement setup is shown in Fig. 4. The main graph shows 11 intervals of constant-measurement basis. The upper inset shows the oscilloscope trace for a period of 0.1 s, corresponding to 200 measurement intervals. The abrupt changes of the signal are due to the basis switching by Bob's EOM. Alice's modulation pattern for a single event (solid line), as well as Bob's oscilloscope samples (dots) are shown on the right. From these samples, a measurement value x was derived as described in Sect. 5.2. Bob then assigned a bit value to each measurement x. After that, all events where Bob's measurement value was below the post-selection threshold x_T were discarded. Table 1 shows the relevant parameters for the case of low loss as well as for high loss. All rates are given in bits per second. While the raw bit rates are nearly equal for both scenarios, a higher post-selection threshold was used in the presence of 64% loss, to ensure a considerable information advantage $I_{AB} - I_{AE}$ for the selected bits. Thus the bit rate after post selection is much lower for the high-loss case. Note also that the error rate in Bob's key drops dramatically after post selection, so that a subsequent error correction with standard procedures is now possible. The higher error probability in the high-loss case originates from the increased overlap of the states (cf. (2)), as the coherent amplitude α decreased with transmission losses.

	21% loss	64% loss
Raw bit rate in bit/s	1069	1096
Errors before post selection	22.0%	27.3%
Bit rate after post selection	415	165
Errors after post selection	6.0%	7.6%
Post-selection threshold x_T	1.0	2.3
Information advantage	0.76	0.49
Max. bit rate after error correction	249	80
Max. bit rate after privacy amplification	189	39

TABLE 1 Experimental key-generation parameters for high and low losses. The raw rate, rate after post selection and information advantage as well as the error fraction are experimental results. The maximum rates after error correction and privacy amplification are theoretical predictions for the available data. The post-selection threshold is given in units of the coherent amplitude α

The bit rate after error correction with the established CASCADE protocol [15] is given for the optimum block length and five passes of the protocol. The potential final bit rate can be calculated from the information advantage and the error-corrected bit rate. Bits needed to authenticate the public channel are not taken into account. In both loss scenarios it was possible to produce a nonzero bit rate of shared bits.

Note that, in contrast to the reverse reconciliation method used in [9], the error correction does not take place on the raw key (with approximately 1 kbit/s) but on the post-selected key (with approximately 400 bit/s and 150 bit/s, respectively), thus needing less capacity on the classical channel. Furthermore, we achieved a key exchange with direct reconciliation in the presence of 64% loss, corresponding to a −4.4 dB quantum channel transmittivity.

7 Conclusions

The system can be further improved, e.g. in the receiver design. If one uses a setup similar to that used to generate the plot in Fig. 1 (see Fig. 5), Bob's detector would not require active basis switching, as in some single-photon systems, e.g. [16]. This makes the detector a completely passive device, with its bandwidth limited only by the photoamplifier speed and dispensing with the need for active synchronization of Alice's signals and Bob's basis change. The necessary timing signals can later be recovered from Bob's measurement results in this setup. The drawback would be the inherent 50% loss in Bob's detector, so that this setup would generate nonzero secret bit rates only for low quantum channel losses.

The use of the polarization variables in a fibre-based transmission system is more difficult than in a free-space setup due to the polarization dispersion and fluctuation in stan-

dard telecommunication fibres. One would have to implement a more sophisticated polarization control and compensation, like the Faraday mirror setup in [17]. The 810-nm source can be replaced easily by a 1.5-μm laser, and detection with high quantum efficiency is also possible at this wavelength range.

To conclude, we have demonstrated a quantum key distribution system that relies on readily available coherent states, continuous-variable measurements and post selection to generate a shared key between Alice and Bob. The states are polarization encoded, ensuring fast modulation and perfect mode overlap in Bob's homodyne detector. There is no need to send a separate local oscillator along with the quantum channel. The system is robust against losses of more than 50% and does not need special reconciliation techniques which require strict one way error correction protocols such as in [9]. Its implementation is straightforward and can be used, for example, in free-space communication with high efficiency and key-exchange rate.

ACKNOWLEDGEMENTS This work was supported by the Federal Ministry of Education and Research (BMBF/VDI) under FKZ:13N8016. The authors would like to thank U. Andersen, J. Schneider for scientific discussions and A. Berger for technical assistance. It is a special pleasure to acknowledge numerous enlightening discussions with N. Lütkenhaus.

REFERENCES

1 For a review see: N. Gisin, G.G. Ribordy, W. Tittel, H. Zbinden: Rev. Mod. Phys. **74**, 145 (2002)
2 G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders: Phys. Rev. Lett. **85**, 1330 (2000)
3 C.H. Bennett: Phys. Rev. Lett. **68**, 3121 (1992)
4 B. Huttner, N. Imoto, N. Gisin, T. Mor: Phys. Rev. A **51**, 1863 (1995)
5 R. Namiki, T. Hirano: Phys. Rev. A **67**, 022308 (2003)
6 G.A. Barbosa, E. Corndorf, P. Kumar, H.P. Yuen: Phys. Rev. Lett. **90**, 227901 (2003)
7 C. Silberhorn, T.C. Ralph, N. Lütkenhaus, G. Leuchs: Phys. Rev. Lett. **89**, 167901 (2002)
8 F. Grosshans, P. Grangier: quant-ph/0204127 (2002)
9 F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, Ph. Grangier: Nature **421**, 238 (2003)
10 T. Hirano, T. Konishi, R. Namiki: quant-ph/0008037 (2000)
11 T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, R. Namiki: Phys. Rev. A **68**, 042331 (2003)
12 R.J. Glauber: Phys. Rev. **131**, 2766 1963
13 P. Horak: quant-ph/0306138 (2003)
14 N. Korolkova, G. Leuchs, R. Loudon, T.C. Ralph, Ch. Silberhorn: Phys. Rev. A **65**, 052306 (2002)
15 G. Brassard, L. Salvail: 'Secret-key Reconciliation by Public Discussion'. In: *Advances in Cryptology – EUROCRYPT '93* (Lect. Notes Comput. Sci. **765**), ed. by T. Helleseth (Springer, Berlin 1994) p. 410
16 C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, J.G. Rarity: Nature **419**, 450 (2002)
17 H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, G. Ribordy: Appl. Phys. B: Lasers Opt. **67**, 743 (1998)