Fortschr. Phys. **54**, No. 8 – 10, 831 – 839 (2006) / **DOI** 10.1002/prop.200610320

Experimental quantum secret sharing

Christian Schmid[1,2]*, **Pavel Trojek**[1,2], **Sascha Gaertner**[1,2], **Mohamed Bourennane**[3], **Christian Kurtsiefer**[4], **Marek Zukowski**[5], and **Harald Weinfurter**[1,2]

[1] Ludwig-Maximilians-Universität, 80799 München, Germany
[2] Max-Planck-Insititut für Quantenoptik, 85748 Garching, Germany
[3] Physics Department, Stockholm University, 10691 Stockholm, Sweden
[4] Department of Physics, National University of Singapore, Singapore 117 542, Singapore
[5] Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdanski, 80-952 Gdansk, Poland

Published online 4 August 2006

Key words Multi-party communication, multi-party quantum key distribution, secret sharing
PACS 03.67.Hk, 03.67.Dd

We consider two simple and practical protocols for multiparty communication and show their experimental realization. These protocols deal with the task of secret sharing in which a secret message is split among several parties in a way that its reconstruction requires their mutual collaboration. In the presented schemes the parties solve the problem by two different approaches: The first uses as a resource the multiqubit entangled state $|\Psi_4^-\rangle$. As no interferometric setups are required here, contrary to known schemes, involving Greenberger-Horne-Zeilinger states, its implementation is simpler and more stable. In the second scheme only sequential transformations on a single qubit are used. This further tremendously simplifies the method, makes it scalable with regard to the number of participating partners and above all, technologically comparable to quantum key distribution.

1 Introduction

Quantum Communication offers methods to securely exchange sensitive information between separated parties by using fundamental principles of quantum mechanics. Such so-called quantum key distribution schemes are well known and for two parties already close to an application in everyday life. They can be naturally extended to more than two parties. However the protocols for more-than-two-party communication known up to now and the technical effort required for their implementation are in general still far from a real life application. Still the following represents a first trailblazing step towards the feasibility of a real life application even in multiparty quantum communication.

We present two different protocols for the solution of a particular secure multiparty communication task, the so called secret sharing, and their proof-of-principle experimental realization. Let us start with sketching the idea behind the term secret sharing. As can be already gathered from the name its main goal is splitting a secret in such a way that neither a single person nor any unauthorized subset of partners is able to reconstruct it. This is a common task in information processing and especially in high security applications. Suppose, for example, that the launch sequence of a nuclear missile is protected by a secret code. Yet, it should be ensured that not a single person alone, but at least *two* persons are required to activate it. Solutions for this problem, and its generalization and variations, are studied in classical cryptography [1]. The aim here is to split information, using some mathematical algorithms, and to distribute the resulting pieces to two or more legitimate parties. However classical communication is susceptible to eavesdropping

* Corresponding author E-mail: christian.schmid@mpq.mpg.de, Phone: +49 89 32905 287 Fax: +49 89 32905 200

attacks. As the usage of quantum resources can lead to unconditionally secure communication (e.g. [2,3]), a protocol applying quantum cryptography ideas to secret sharing was proposed [4–7]. In this protocol a shared GHZ-state allows the information splitting and the eavesdropper protection simultaneously. But, due to lack of efficient multi-photon sources an experimental demonstration of a working quantum secret sharing (QSS) was missing for a long time. Solely the in-principle feasibility of an experimental realization using pseudo-GHZ states was shown [8] and only very recently a GHZ-protocol for three parties was implemented [9].

Here we consider two protocols: The first is applicable to four parties [10] and uses as resource the correlations contained in a particular four photon state, called $|\,\Psi_4^-\,\rangle$ [11]. The advantage of this scheme compared to the GHZ-protocol is that the state it uses can be directly observed in the process of spontaneous parametric down conversion (SPDC), needs no interferometric experimental setup and is thus easier to practically implement. The second works in general for N participants and has no need of GHZ- or any other multi-qubit entangled states as it employs only sequential single qubit communication between the parties [12]. Due to this fact the latter scheme is very easily realizable with current state-of-the-art technology, and above all, scalable with respect to the number of participating parties. These traits made the experimental demonstration of that protocol for six parties possible.

2 Theory

2.1 The GHZ-protocol

We first shortly recapitulate the entanglement based protocol using a multi-qubit GHZ state for secret sharing. Consider N persons, each having a particle from the maximally entangled N particle GHZ-state

$$|\,\mathrm{GHZ}\,\rangle = \frac{1}{\sqrt{2}}\left(|\underbrace{00\ldots0}_{N}\rangle + |\underbrace{11\ldots1}_{N}\rangle\right). \tag{1}$$

The partners randomly and independently choose the value of a parameter $\phi_j = 0$ or $\pi/2$ and perform measurement on the local particle of the observable

$$\widehat{\sigma}_j(\phi_j) = \sum_{k_j=\pm1} k_j\,|\,k_j,\phi_j\,\rangle\langle\,k_j,\phi_j\,|, \tag{2}$$

with the eigenstates $|\,k_j,\phi_j\,\rangle = 1/\sqrt{2}(|\,0\,\rangle + k_j\exp(i\phi_j)|\,1\,\rangle)$ $(j = 1,2,\ldots,N)$ associated with eigenvalues $k_j = \pm1$. The correlation function for a N-particle GHZ state, defined as the expectation value of the product of N local results, is given by

$$E(\phi_1,...,\phi_N) = \langle\prod_{j=1}^{N}\widehat{\sigma}_j(\phi_j)\rangle \;=\; \cos\left(\sum_{j=1}^{N}\phi_j\right). \tag{3}$$

After the measurement each partner publicly announces her/his choice of ϕ_j, but keeps the result k_j secret. Then all of them know whether this procedure leads to perfect correlations, i.e. when $|\cos(\sum_j^N \phi_j)| = 1$. This happens in half of the runs. In these instances, on the basis of the perfect correlations, any subset of $N-1$ partners, whom we shall call hereafter recipients, is able to infer the measurement result of the remaining person, P_R, if and only if all the recipients collaborate. Thereby they achieve the principal task of secret sharing. For a security analysis of such a scheme against eavesdropping attacks see [5,13].

2.2 The $|\,\Psi_4^-\,\rangle$-protocol

The protocol described above can be performed in a similar way for $N = 4$ using another multi-particle entangled state, called $|\,\Psi_4^-\,\rangle$, which is shared between the parties (see Fig. 1(a)). This state can be written

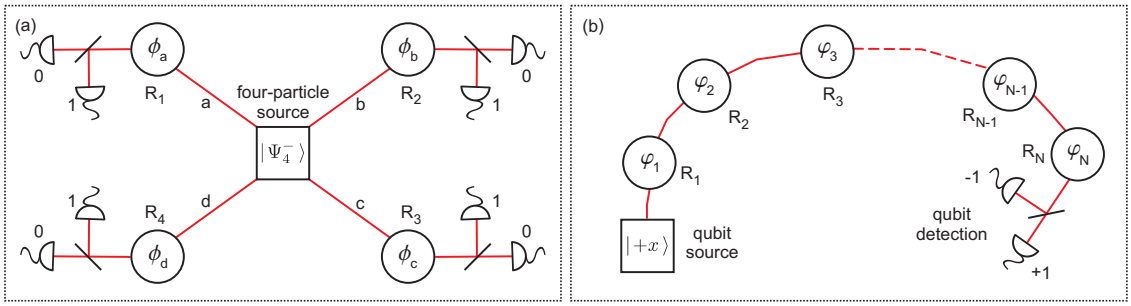

Fig. 1 (a) Scheme for four party quantum secret sharing via four qubit entanglement. Each of the four parties $R_1, \ldots, R_4$ receives a qubit of the entangled state $|\Psi_4^-\rangle$ and performs a local measurement characterized by a randomly chosen parameter ϕ_j, $j = a, \ldots, d$; for particular choices of ϕ_j the detection events associated with bit values of 0 and 1 are perfectly correlated and can be used to establish a shared secret key. (b) Scheme for N party single qubit secret sharing. A qubit is prepared in an initial state and sequentially communicated from party to party, each acting on it with a phase operator $\widehat{U}(\varphi_j)$, applying a randomly chosen phase φ_j. The last recipient performs a measurement on the qubit leading to the result ± 1. In half of the cases the phases add up such that the measurement result is deterministic. These instances can be used to achieve the aim of secret sharing.

in the following way:

$$|\Psi_4^-\rangle = \frac{1}{\sqrt{3}}(|0011\rangle + |1100\rangle - \frac{1}{2}(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle))_{abcd} \tag{4}$$

It is invariant under joint identical unitary transformations and shows perfect four-particle correlations. The four-qubit correlation function for $|\Psi_4^-\rangle$ is given by

$$E(\phi_a, \phi_b, \phi_c, \phi_d) = \tfrac{2}{3}\cos(\phi_a + \phi_b - \phi_c - \phi_d) + \tfrac{1}{3}\cos(\phi_a - \phi_b)\cos(\phi_c - \phi_d). \tag{5}$$

In order to establish a shared secret among the parties the correlations contained in the entangled state are exploited. The partners act according to the description given in the previous Sect. 2.1: First they randomly choose a local parameter ϕ_j and perform the corresponding measurement on their qubit. Then they announce publicly the choice of ϕ_j, but keep the result k_j secret. According to Eq. (5) it can be decided which choices of ϕ_j lead to correlated results. In these instances three parties have to collaborate in order to infer the measurement result of the last party.

Two particular versions of this protocol implying different eavesdropping analysis can be considered. The first uses the same set of local parameters as in the GHZ-protocol, i.e. $\phi_j = 0$ and $\phi_j = \pi/2$. The second involves an additional basis suitable for evaluating a Bell inequality [11] (similar as in the Ekert quantum key distribution scheme [3]). In the following we will focus only on the first version.

2.3 The single qubit protocol

A N party scheme (see Fig. 1(b)) for the *same* task, where only the sequential communication of a single qubit is used runs as follows. The qubit is initially prepared in the state

$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{6}$$

During the protocol the qubit is sequentially communicated from partner to partner, each acting on it with the unitary phase operator

$$\widehat{U}_j(\varphi_j) = \begin{cases} |0\rangle \to |0\rangle \\ |1\rangle \to e^{i\varphi_j}|1\rangle, \end{cases} \tag{7}$$

with the randomly chosen value of $\varphi_j \in \{0, \pi, \pi/2, 3\pi/2\}$. Therefore, having passed all parties, the qubit will end up in the state

$$|\chi_N\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i(\sum_j^N \varphi_j)}|1\rangle\right). \tag{8}$$

The last party performs a measurement on the qubit in the basis $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ leading to the result ± 1. For her/him it suffices to choose only between $\varphi_N = 0$ or $\varphi_N = \pi/2$. The probability that she/he detects the state $|\pm x\rangle$ reads

$$p_\pm(\varphi_1, \ldots, \varphi_N) = \tfrac{1}{2}\left(1 \pm \cos\left(\sum_j^N \varphi_j\right)\right). \tag{9}$$

The expectation value of the measurement is

$$E'(\varphi_1, \ldots, \varphi_N) = p_+(\varphi_1, \ldots, \varphi_N) - p_-(\varphi_1, \ldots, \varphi_N) = \cos\left(\sum_j^N \varphi_j\right). \tag{10}$$

Note that this expectation value (Eq. (10)) has the same structure like the correlation function (Eq. (3)) and can therefore also be used to obtain a shared secret. For this purpose each participant divides his action for every run into two classes: a class X corresponding to the choice of $\varphi_j \in \{0, \pi\}$ and a class Y corresponding to $\varphi_j \in \{\pi/2, 3\pi/2\}$. Following this classification they broadcast the class of their action for each run, but keep the particular value of φ_j secret. This corresponds in the GHZ scheme to the announcement of ϕ_j while keeping k_j secret. The order in which they announce the classification is each time randomly chosen. From that procedure they can determine which runs lead to a deterministic measurement result, i.e. when $\cos(\sum_j^N \varphi_j)$ equals to either 1 or -1 or equivalently either $p_+ = 1$ or $p_- = 1$, respectively. Such sets of φ's occur on average in half of the runs. These are valid runs of the protocol. In such cases any subset of $N-1$ parties is able to infer the choice of φ_R of the remaining partner, if and only if, all the recipients collaborate and reveal among themselves their values of φ_j. In case that this subset contains the last partner, he/she must reveal the measurement result. Thus, the collaboration of all recipients is necessary. The task of secret sharing is now achieved via local manipulation of phases on a single qubit, communicated from one partner to the other, and no multiparticle entangled GHZ state is required anymore.

2.4 Security of the protocols

As security considerations for the $|\Psi_4^-\rangle$-protocol are basically analogue to the GHZ-protocol we describe for that protocol the eavesdropping check procedure just very quickly, pointing out the significant differences and otherwise focus on the security analysis of the single-qubit protocol.

Depending on their chosen basis settings the parties can proceed in the $|\Psi_4^-\rangle$-protocol as follows. In case of using a complementary basis set similar to the GHZ-protocol, a fraction of their measurement results must be publicly compared, to certify the absence of an eavesdropper. If they will find a quantum bit error rate which is low enough they can use their results to distill a secure key, if not they have to discard their bits.

One drawback in the use of the $|\Psi_4^-\rangle$- instead of the GHZ-state, which should be noted, is the fact that there can occur instances where the collaboration of only two parties is already sufficient for the reconstruction of one shared secret bit. As can be seen from the structure of the state itself this happens for $\phi_j = 0$ if the measurement results of the first two or respectively the last two parties are equal. However for a complete bit sequence this means only partial information and in general the collaboration of three out of four parties is still required for the reconstruction of the full sequence if the whole key is transposed by hash functions.

In order to ensure the security of the single-qubit protocol against eavesdropping or cheating (by eavesdropping we refer to an attack from a person which is not participating in the protocol whereas by cheating we refer to an attack from a participant) the partner P_R arbitrarily selects a certain subset of valid runs. The size of this subset depends on the degree of security requirements. For these runs the value of φ_R is compared with the one inferred by the recipients. To this end each of the recipients sends in a random order the value of his/her phase φ_j. The comparison reveals any eavesdropping or cheating strategy. That can be easily seen by discussing the following intercept/resend eavesdropping attacks.

Imagine, for instance, the first recipient R_j who follows directly after P_R tries to infer the secret without the help of the remaining participants by measuring the qubit, *before* acting on it with $\widehat{U}_j(\varphi_j)$ and afterwards sending it to the next recipient R_{j+1}. For convenience, let us assume R_j chooses for this measurement one of the two protocol bases $|\pm x\rangle$ or $|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$. The choice of these bases is natural because at any stage of the protocol the qubit is in one of these four states. As P_R applies randomly one of four different phase shifts, the probability that the qubit is an eigenstate of the measurement chosen by R_j is 1/2 and thus in half of the cases the measurement result of R_j will be completely bitwise random, because $|\langle \pm y \mid \pm x\rangle|^2 = 1/2$. Thus, recipient R_j gets no information about the secret. Furthermore, such cheating causes an overall error of 25% in the final measurement results. Simply, if R_j chooses the wrong basis, the final state of the qubit after all the introduced phase shifts will not always be of the form (8).

An eavesdropper following such a strategy faces a similar situation. The usage of the bases x and y for an intercept/resend attack is the optimal one concerning the information gain on the valid runs. One might also consider using the intermediate (or so-called Breidbart) basis $|\pm b\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|\pm x\rangle + |\pm y\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\pi/4}|1\rangle)$ which gives the eavesdropper maximum information on all exchanged bits [14]. But even here the error rate goes necessarily up to 25 %. The security of the presented protocol against a general eavesdropping attack follows from the proven security of the well known BB84 protocol [2, 15]. Each communication step between two successive parties can be regarded as a BB84 protocol using the bases x and y. Any set of dishonest parties in our scheme can be viewed as an eavesdropper in BB84 protocol.

3 Experiment

3.1 The $|\Psi_4^-\rangle$-protocol

The state $|\Psi_4^-\rangle$ required for the four-party quantum secret sharing protocol can be obtained from the second order emission of a non-collinear type II spontaneous parametric down conversion process (SPDC) in the polarization degree of freedom of four photons (see Fig. 2(a)). That means the basis states $|0\rangle$ and $|1\rangle$ are represented by the polarization states $|H\rangle$ and $|V\rangle$, respectively (horizontal (H) and vertical (V) linear polarization). For the experimental implementation we used a solid state laser with a pump power of P = 10 W and a wavelength of $\lambda = 532$ nm to pump a mode locked Ti:Sa laser. The Ti:Sa laser emits pulses with a pulse length of about 120 fs, at a repetition rate of 82 MHz. The pulses are frequency doubled in a lithium-triborate (LBO) crystal to $\lambda = 390$ nm and are further used to pump a 2 mm thick beta-barium-borate (BBO) crystal. The photons emitted from the crystal via pulsed SPDC are in the polarization state given by Eq. (4), provided that they split up to four distinct spatial modes a, b, c, d at two beam splitters (BS). Thus they can be directly used to accomplish the secret sharing protocol once each of the recipients R_i, $(i = 1, \ldots, 4)$ obtains one of the four photons. The R_i measure randomly in one of two different complementary bases using a pseudo-random number generator (RNG) to set the analysis direction of a lambda half-wave plate (HWP_i) in front of a polarizing beam splitter (PBS). The detection of a photon at D_{i-} in the transmitted output mode of the PBS corresponds to a bit value of 0, while the detection of a photon at D_{i+} in the reflected output mode is associated with a bit value of 1. The detectors were silicon avalanche photodiodes with a photon detection efficiency of about 40%. For the registration of all 16 relevant four-photon coincidences we used an eightchannel multi-photon coincidence unit [16]. For quantum key distribution the registration

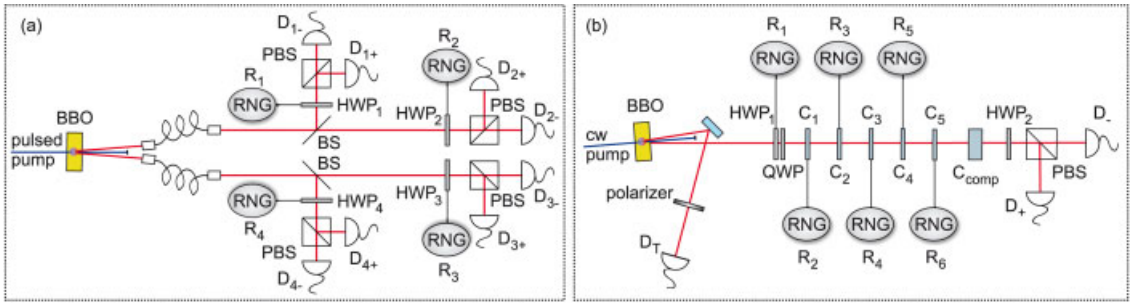

Fig. 2 (a) Setup for four qubit secret sharing. Four photons are generated in the second order emission of a pulsed, type II SPDC process in a BBO crystal and split up in four spatial modes by two beam splitters (BS). Under the condition that one photon is detected in each output mode, the four-photon entangled state $|\Psi_4^-\rangle$ is observed. In order to establish a shared key each photon is measured randomly by the recipients $R_1, \ldots, R_4$ in one of two complementary bases. The analysis direction is set using a half-wave plate (HWP) driven by motor according to the output of a pseudo-random number generator (RNG). (b) Setup for single qubit secret sharing. Pairs of orthogonally polarized photons are generated via a type II SPDC process in a BBO crystal. The detection of one photon from the pair by D_T heralds the existence of the other one used in the protocol. The initial polarization state is prepared by placing a polarizer in front of the trigger detector. Each of the recipients ($R_1 \ldots R_6$) introduces one out of four phase shifts, according to the output of a pseudo-random number generator (RNG), using half- and quarter wave plate (HWP_1, QWP) or YVO_4 crystals (C_1...C_5), respectively. The last party analyzes additionally the final polarization state of the photon by detecting it behind a half-wave plate (HWP_2) and a polarizing beam splitter.

time was set to 1 second after which new random settings have been chosen for R_i. In situations where more than one four-photon coincidence event was registered during that time only the first one was chosen.

For the experimental demonstration of the four-party quantum secret sharing protocol we performed a key exchange as described in Sect. 2.2. We have exchanged key bits at a rate of about 100 bits per hour. To check for eavesdropping R_1 chooses a random subset of the sifted key bits and compares it with the publicly announced measurement results of R_2, R_3 and R_4 at those positions. In that way the quantum bit error rate can be evaluated to be about 5%. This value lies well below several known security threshold values required for quantum key distribution and is low enough to finally distill a perfectly secure distributed key [2].

3.2 The single-qubit protocol

The single-qubit protocol was experimentally implemented for six parties, thus clearly showing the practicality and user-friendliness of that scheme.

We encoded the protocol qubit in the polarization of a single photon. The single photons were provided by a heralded single photon source. The setup is shown in Fig. 2(b). A pair of polarization entangled photons is created via a spontaneous parametric down conversion (SPDC) process. As the photons of a pair are strongly correlated in time the detection of one photon in D_T heralds the existence of the other one which is used for the protocol. A coincidence detection between D_T and D_+/D_-, within a chosen time window of 4 ns, implies communication of only a single photon. For this coincidence time window and single-count rates of about 35000 s^{-1} both in D_+ and D_- and about 5000 in D_T we obtained a coincidence rate of 1200 s^{-1}. Accidental coincidences or multi-coincidences were thus negligible. The SPDC process was run by pumping a 2 mm long β-barium borate (BBO) crystal with a blue single mode laser diode (402.5 nm), at an optical output power of 10 mW. Type-II phase matching was used, at the degenerate case leading to pairs of orthogonally polarized photons at a wavelength of $\lambda = 805$ nm ($\Delta\lambda \approx 6$ nm).

In order to prepare the initial polarization state a polarizer transmitting vertically polarized photons was put in front of the trigger detector D_T ensuring that only (initially) horizontally polarized photons can lead to a coincidence detection. The first partner was equipped with a motorized half-wave plate (HWP_1)

Table 1 Results of the simulation of an intercept/resend eavesdropping strategy, and intermediate basis strategy. The attack was done by inserting a polarizer between the distributor and the first recipient. In each case the quantum bit error rate (QBER) rises up to more than 25 % and by this blows the eavesdropper's cover.

	z_{total}	z_{raw}	z_{val}	QBER [%]
$\vert \pm x \rangle$	27501	883	452	25.22 ± 2.04
$\vert \pm y \rangle$	24993	784	409	30.32 ± 2.27
$\vert \pm b \rangle$	38174	1137	588	30.27 ± 1.89

followed by quarter-wave plate (QWP) at an angle of $45\,^\circ$. By rotation of HWP_1 to the angles $0\,^\circ, 45\,^\circ$ and $22.5\,^\circ, -22.5\,^\circ$ he could transform the horizontally polarized photons coming from the source to $\vert \pm y \rangle$ and $\vert \pm x \rangle$. This corresponds to applying the phase-shifts $\varphi \in \{\pi/2, 3\pi/2\}$ and $\varphi \in \{0, \pi\}$ respectively. As the phase-shifts of the other partners had to be applied independently from the incoming polarization state the usage of standard wave plates was not possible. Therefore the unitary phase operator was implemented using birefringent uniaxial 200 µm thick Yttrium Vanadate (YVO_4) crystals (C_i). The crystals were cut such that their optic axis lies parallel to the surface and is aligned in such a way that H and V polarization states correspond to their normal modes. Therefore by rotating the crystals along the optic axis for a certain angle a specific relative phase shift was applied independently from the incoming polarization state. An additional YVO_4 crystal (C_{comp}, 1000 µm thick) was used to compensate for dispersion effects. The last party performed the measurement behind a half-wave plate (HWP_2) at an angle of $22.5\,^\circ$ followed by polarizing beam-splitter (PBS). The photons were detected at D_+/D_- and D_{T} by passively quenched silicon avalanche photo diodes (Si-APD) with an efficiency of about 35 %.

The protocol was repeated $z_{\mathrm{total}} = 25000$ times. One run consisted of choosing pseudo-random variables, rotating the crystals accordingly and opening the detectors for a collection time window $\tau = 200\,\mu\mathrm{s}$, what took together about 1 s. The requirement of communicating a single photon imposes that only those runs were included into the protocol in which just one coincidence between D_T and either D_+ or D_- (coincidence gate time $\tau_c \approx 7\,\mathrm{ns}$) was detected during τ . In these runs a single coincidence detection happened $z_{\mathrm{raw}} = 2107$ times which provided us with the raw key. From this we extracted $z_{\mathrm{val}} = 982$ valid runs where $\vert \cos(\sum_j^N \varphi_j) \vert = 1$ (506 times $\cos(\sum_j^N \varphi_j) = 1$ and 476 times $\cos(\sum_j^N \varphi_j) = -1$) with a quantum bit error rate (QBER) of 2.34 ± 0.48 %. Note that error correction protocols (like e.g. parity check) could be used exactly like in conventional quantum cryptography to further reduce the errors.

In order to show that the QBER increases significantly by an eavesdropping attack we simulated an intercept/resend strategy by inserting a polarizer between the first two partners. The attack was done in the protocol bases $\vert \pm x \rangle, \vert \pm y \rangle$ as well as in the intermediate basis $\vert \pm b \rangle$. For the latter two the polarizer was additionally sandwiched by two quarter-wave plates. The angular settings (1st QWP, polarizer, 2nd QWP) were $\{45\,^\circ, 0\,^\circ, -45\,^\circ\}$ and $\{-45\,^\circ, 22.5\,^\circ, 45\,^\circ\}$. For every choice of the basis the QBER went up to at least 25 % (or even higher due to other experimental imperfections). The results are summarized in Table 1.

A different eavesdropping/cheating strategy could be of a Trojan Horse type. One of the partners could pass polarized light through the devices of the partners and therefore attempt to gain information on local phase shifts. However, such action might be easily discovered by the partners by checking from time to time the nature of light passing through their devices. Also the excess photons, i.e. those not in coincidence with the trigger, cannot be utilized for eavesdropping/cheating as they do not have a defined polarization. This is because the initial polarization of the heralded photons is fixed in the experiment by putting the polarization filter in the path to the trigger detector, Fig. 2. Since the photons form polarization entangled EPR pairs, detection of a trigger photon behind a polarization filter collapses the initially undefined polarization state of the heralded one to the required $\vert +x \rangle$. All other photons, since no trigger event accompanies them, remain unpolarized. Only higher-order emissions, i.e. two pairs emitted within the coherence time (≈ 360 fs), are

useful for beam-splitting attacks [17]. The probability for such a opportunity, however, for our parameters is as low as 7.6×10^{-7} per run .

4 Conclusion

In summary, we experimentally implemented two schemes for solving the multiparty communication task of secret sharing. The first one uses as resource multi-particle entanglement while the second requires just single qubits. In the entanglement based protocol the usage of a particular multi-qubit state which can be obtained from a simple and stable experimental setup shows the feasibility of secure multi-party quantum communication via multi-photon entanglement. Especially promising with respect to real life application is the second scheme using only the sequential communication of a single qubit. As single qubit operations using linear optical elements and the analysis of photon polarization states are quite well accomplishable with present day technology we were therefore able to present the first experimental demonstration of that protocol for as many as six parties. This is to our knowledge the highest number of actively performing parties in a quantum protocol ever implemented. In principle we see no experimental barrier to extend that performed protocol to even significantly higher number of participants.

We also simulated an eavesdropping intercept/resend attack and by this showed the resistance of the single-qubit protocol against such kind of attacks because of the significantly increasing error rate. Since eavesdropper might have an access to input and output ports of the partners particulary Trojan Horse attacks might be a potential security danger for our new single-qubit scheme. Yet they can be precluded by the partners with a reasonable technological effort like e.g. recently discussed in [18]. The use of weak coherent pulses of light containing much less than one photon on average, instead of a heralded single photon source, further reduces the required experimental resources. However, this would be at the expense of the concept of communicating strictly one qubit and can be also disadvantageous for the practical performance of the protocol [19, 20]. While we have realized our single-qubit secret sharing protocol using photons and polarization encoding, alternative schemes, like proposed or realized in BB84-type protocols can be adopted as well. Finally, by showing that a single qubit approach can be effectively used for solving the secret sharing task, instead of methods involving many qubit GHZ states, we conjecture that this approach may be a practical solution for many other multiparty communication tasks. Recently, for example, it was possible to successfully apply that approach in quantum communication complexity. There, separated parties performing local computations exchange information in order to accomplish a globally defined task, which is impossible to solve singlehandedly (see [21]).

Acknowledgements This work was supported by the Bavarian Forschungsstiftung, the German DFG and the European Commission through the IST FET QIPC RamboQ. MZ is supported by Wenner-Gren Foundation and MNil Grant IP03B 04927, and our collaboration is supported by a DAAD/MNil programme.

References

[1] B. Schneier, Applied Cryptography, 2nd edition (John Wiley & Sons, Inc., New York, 1996).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] M. Żukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter, Acta Phys. Pol. **93**, 187 (1998).
[5] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[6] R. Cleve, D. Gottesmann, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[7] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1998).
[8] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[9] Y. A. Chen et al., Phys. Rev. Lett. **95**, 200502 (2005).
[10] S. Gaertner et al., to be published.

[11] H. Weinfurter and M. Zukowski, Phys. Rev. A **64**, 010102 (2001); M. Eibl, S. Gaertner, M. Bourennane, Ch. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **90**, 200403 (2003); S. Gaertner et al., Appl. Phys. B **77**, 803 (2003).
[12] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[13] V. Scarani and N. Gisin, Phys. Rev. A **65**, 012311 (2001).
[14] B. Huttner and A. K. Ekert, J. Mod. Opt. **41**, 2455 (1994).
[15] C. Bennett and G. Brassard, Proc. of IEEE International Conference on Computer, Systems & Signal Processing, Bangalore, India (1984).
[16] S. Gaertner, Ch. Kurtsiefer, and H. Weinfurter, Rev. Scient. Inst. **76**, 123108 (2005).
[17] This is just the same as in entanglement-based quantum cryptography, see T. Jennewein, Ch. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000); D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000); A. Poppe et al., Optics Express **12**, 3865 (2004).
[18] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, quant-ph/0507063.
[19] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[20] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[21] P. Trojek, Ch. Schmid, M. Bourennane, C. Brukner, M. Zukowski,and H. Weinfurter, Phys. Rev. A **72**, 050305(R) (2005).