Experimental Single Qubit Quantum Secret Sharing

Christian Schmid,[1,2] Pavel Trojek,[1,2] Mohamed Bourennane,[3] Christian Kurtsiefer,[5]
Marek Żukowski,[4] and Harald Weinfurter[1,2]

[1]*Sektion Physik, Ludwig-Maximilians-Universität, D-80797 München, Germany*
[2]*Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany*
[3]*Physics Department, Stockholm University, SE-10691 Stockholm, Sweden*
[4]*Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*
[5]*Department of Physics, National University of Singapore, Singapore 117 542, Singapore*

(Received 29 December 2004; revised manuscript received 7 October 2005; published 1 December 2005)

We present a simple and practical protocol for the solution of a secure multiparty communication task, the secret sharing, and its proof-of-principle experimental realization. In this protocol, a secret is split among several parties in a way that its reconstruction requires the collaboration of the participating parties. In our scheme the parties solve the problem by sequential transformations on a single qubit. In contrast with recently proposed schemes involving multiparticle Greenberger-Horne-Zeilinger states, the approach demonstrated here is much easier to realize and scalable in practical applications.

DOI: 10.1103/PhysRevLett.95.230505 PACS numbers: 03.67.Hk, 03.67.Dd

Splitting a secret in way that any unauthorized subset of partners is not able to reconstruct it is a common task in information processing and especially 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 a single lunatic alone is not able to activate it, but at least two lunatics are required. Solutions for this problem, and its generalization and variations, are studied in classical cryptography [1]. Such problems are called secret sharing. 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 attacks. As the usage of quantum resources can lead to unconditionally secure communication (e.g., Refs. [2,3]), a protocol introducing quantum cryptography to secret sharing was proposed [4–7]. In this protocol a shared Greenberger-Horne-Zeilinger (GHZ) state allows information splitting and eavesdropper protection simultaneously. But, because of a lack of efficient multiphoton sources an experimental demonstration of a working quantum secret sharing is still missing. Solely the in-principle feasibility of an experimental realization using pseudo-GHZ states was shown [8].

Here we propose a protocol for N parties, in which a sequential single qubit communication between them is used with no need for GHZ states. As our protocol requires only single qubits it is realizable with current state-of-the-art technologies, and, above all, scalable with respect to the number of participating parties. These traits made the experimental demonstration of our protocol for six parties possible.

We first briefly describe the entanglement-based protocol using a multiqubit 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 local parameter $\phi_j = 0$ or $\pi/2$ and perform measurement on the local particle of the observable

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

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 $k_j = \pm 1$. The correlation function for an N-particle GHZ state, defined as the expectation value of the product of N local results, is given by

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

After the measurement each partner publicly announces 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 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 Refs. [5,9].

An N party scheme (see Fig. 1) 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 $|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. During the protocol the qubit is sequentially communicated from partner to partner, each acting on it with the unitary phase operator

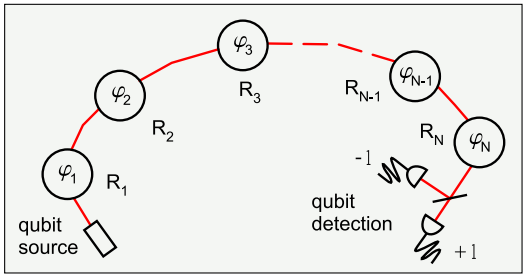

FIG. 1 (color online). Scheme for N party single qubit secret sharing. A qubit is prepared in an initial state and sequentially communicated from party to party, each acting on it with a phase operator $\widehat{U}_j(\varphi_j)$, applying a randomly chosen phase φ_j. The last recipient performs a measurement 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.

$$\hat{U}_j(\varphi_j) = \begin{cases} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow e^{i\varphi_j}|1\rangle \end{cases} , \tag{5}$$

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

$$|\chi_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\sum_j^N \varphi_j)}|1\rangle). \tag{6}$$

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. As it will be clarified later, for him it suffices to choose only between $\varphi_N = 0$ or $\varphi_N = \pi/2$. The probability that he detects the state $|\pm x\rangle$ reads

$$p_\pm(\varphi_1, \ldots, \varphi_N) = \frac{1}{2}\left[1 \pm \cos\left(\sum_j^N \varphi_j\right)\right]. \tag{7}$$

The expectation value of the measurement is

$$E' = (\varphi_1, \ldots, \varphi_N) = p_+(\varphi_1, \ldots, \varphi_N) - p_-(\varphi_1, \ldots, \varphi_N) = \cos\left(\sum_j^N \varphi_j\right). \tag{8}$$

Note that this expectation value [Eq. (8)] has the same structure as 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 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 the case in which this subset contains the last partner, he must reveal the measurement result [10]. The task of secret sharing is now achieved via local manipulation of phases on a communicated single qubit, and no multiparticle entangled GHZ state is required anymore.

In order to ensure the security of the protocol against eavesdropping or cheating [11] the partner P_R arbitrarily selects a certain subset (its size depends on the degree of security requirements) of valid runs. 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 random order the value of his phase φ_j. The comparison reveals any eavesdropping or cheating strategy. That can be easily seen by discussing the following intercept and 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 $\hat{U}_j(\varphi_j)$ 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 $|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$. 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 $1/2$. That is, in half of the cases the measurement result of R_j will be completely random, because $|\langle \pm y| \pm x\rangle|^2 = 1/2$, thus reducing significantly his knowledge 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 will not always be of the form (6).

An eavesdropper following such a strategy faces a similar situation. The usage of the bases x and y for an intercept or 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 $|\pm b\rangle = (1/\sqrt{2+\sqrt{2}})(|\pm x\rangle + |\pm y\rangle$ which gives the eavesdropper maximum information on all exchanged bits [12]. 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 [2,13]. 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.

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

We encoded the protocol qubit in a single photon provided by a heralded single photon source. The basis states $|0\rangle$ and $|1\rangle$ were represented by the polarization states $|H\rangle$ and $|V\rangle$, respectively [horizontal (H) and vertical (V) linear polarization]. The setup is shown in Fig. 2. 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 35 000 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 multicoincidences were thus negligible. The SPDC process was run by pumping a 2 mm long β-barium borate (BBO) crystal with a violet 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 half-wave plate (HWP_1) followed by quarter-wave plate (QWP) at an angle of 45°. By rotating HWP_1 to the angles 0°, 45° and 22.5°, −22.5° he could transform the horizontally polarized photons coming from the source to $|\pm y\rangle$ and $|\pm x\rangle$. 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 (Ccomp 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° 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%.

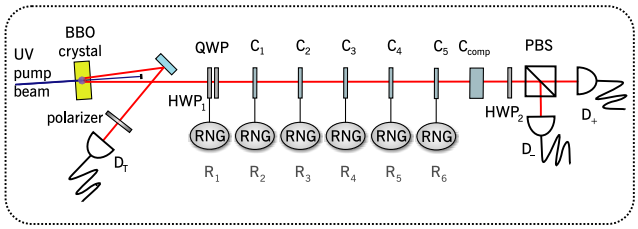

FIG. 2 (color online). Setup for single qubit secret sharing. Pairs of orthogonally polarized photons are generated via a type II SPDC process in a BBO crystal. The detection of one photon from the pair by D_T heralds the existence of the other one used in the protocol. The initial polarization state 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 pseudorandom number generator (RNG), using half- and quarter-wave plates (HWP_1, QWP) or YVO_4 crystals ($C_1 \ldots C_5$), 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 (PBS).

The protocol was repeated $z_{\mathrm{total}} = 25\,000$ times. One run consisted of choosing pseudorandom variables, rotating the crystals accordingly, and opening the detectors for a collection time window $\tau = 200$ μs, which took all together about 1 s. The requirement of communicating a single photon imposes the restriction that only those runs were included into the protocol in which just one coincidence between D_T and either D_+ or D_- 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 $|\cos(\sum_j^N \varphi_j)| = 1$ [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 $2.34 \pm 0.48\%$ [14].

In order to show that the QBER increases significantly by an eavesdropping attack we simulated an intercept and resend strategy by inserting a polarizer between the first two partners. The attack was done in the protocol bases $|\pm x\rangle$, $|\pm y\rangle$, as well as in the intermediate basis $|\pm b\rangle$. For the latter two the polarizer was additionally sandwiched by two quarter-wave plates. The angular settings (1st QWP, polarizer, 2nd QWP) were $\{45°, 0°, -45°\}$ and $\{-45°, 22.5°, 45°\}$. 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 I.

A different eavesdropping or 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 or cheating as they do not have a defined polarization [15]. Only higher-order emissions, i.e., two pairs emitted within the coherence time ($\approx$360 fs), are

TABLE I. Results of the simulation of an intercept and 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 (%)
$\|\pm x\rangle$	27 501	883	452	25.22 ± 2.04
$\|\pm y\rangle$	24 993	784	409	30.32 ± 2.27
$\|\pm b\rangle$	38 174	1137	588	30.27 ± 1.89

useful for beam-splitting attacks [16]. The probability for such an opportunity, however, using our parameters, is as low as 7.6×10^{-7} per run.

In summary, we introduced a new scheme for solving the multiparty communication task of secret sharing. Unlike other quantum schemes employing multiparticle entangled states our protocol uses only the sequential communication of a single qubit. As single qubit operations using linear optical elements and the analysis of photon polarization states are possible to accomplish with present day technology we were therefore able to present the first experimental demonstration of the 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 the performed protocol to even significantly higher number of participants.

We also simulated an eavesdropping intercept and resend attack and by this showed the resistance of the protocol against such a kind of attack because of the significantly increasing error rate. Since an eavesdropper might have an access to input and output ports of the partners, particularly Trojan Horse attacks might be a potential security danger for our scheme. Yet they can be precluded by the partners with a reasonable technological effort like, e.g., those recently discussed in Ref. [17]. 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 [18,19]. While we have realized our secret sharing protocol using photons and polarization encoding, alternative schemes, like those 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.

M. Ż. is supported by an FNP Professorial Subsidy, and MNiI Grant No. 1 P03B 04927. This work was supported by MNiI/DAAD, German DFG and BMBF, the Bavarian high-tech initiative, Swedish Research Council (VR), and the European Commission through the IST FET QIPC RamboQ.

[1] B. Schneier, *Applied Cryptography* (John Wiley & Sons, 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 (1999).
[8] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[9] V. Scarani and N. Gisin, Phys. Rev. A **65**, 012311 (2002).
[10] Note that although doing different things in practice (measurement or phaseshift) all parties are equal as far as amount of information is concerned. In fact the state preparation and detection could be formally separated from the parties and be performed by some higher instance, etc.
[11] By eavesdropping we refer to an attack from a person who is not participating in the protocol whereas by cheating we refer to an attack from a participant.
[12] B. Huttner and A. K. Ekert, J. Mod. Opt. **41**, 2455 (1994).
[13] C. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computer, Systems & Signal Processing, Bangalore, India, 1984.*
[14] Error correction protocols (like, e.g., parity check) could be used exactly like in conventional quantum cryptography to further reduce the errors.
[15] 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 $|+x\rangle$. All other photons, since no trigger event accompanies them, remain unpolarized.
[16] 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.*, Opt. Express **12**, 3865 (2004).
[17] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, quant-ph/0507063.
[18] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[19] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).