Experimental Demonstration of Four-Party Quantum Secret Sharing

S. Gaertner,[1,2] C. Kurtsiefer,[3] M. Bourennane,[4] and H. Weinfurter[1,2]

[1]*Sektion Physik, Ludwig-Maximilians-Universität, 80799 München, Germany*
[2]*Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany*
[3]*Department of Physics, National University of Singapore, 117542 Singapore, Singapore*
[4]*Physics Department, Stockholm University, S-10691 Stockholm, Sweden*

(Received 26 June 2006; published 12 January 2007)

Secret sharing is a multiparty cryptographic task in which some secret information is split into several pieces which are distributed among the participants such that only an authorized set of participants can reconstruct the original secret. Similar to quantum key distribution, in quantum secret sharing, the secrecy of the shared information relies not on computational assumptions, but on laws of quantum physics. Here, we present an experimental demonstration of four-party quantum secret sharing via the resource of four-photon entanglement.

DOI: 10.1103/PhysRevLett.98.020503 PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.Hk, 42.50.Dv

Entanglement is a fundamental resource for many quantum communication schemes. Bipartite entanglement has been used for the experimental demonstration of two-party quantum communication schemes like quantum dense coding [1], quantum teleportation [2], or entanglement based quantum cryptography [3]. Similar to such two-party quantum communication schemes, multipartite entanglement allows the experimental implementation of multiparty quantum communication schemes, like multiparty quantum teleportation [4], quantum telecloning [5], multiparty quantum key distribution, or quantum secret sharing (QSS) [6].

Secret sharing was introduced independently in 1979 by Shamir and Blakley [7,8]. In a secret sharing scheme between n participants, a designated party, usually called the dealer, splits some secret information into $n-1$ shares and distributes these shares to each participant in such a way that only a particular authorized set of participants can reconstruct that secret information. The qualified subsets of participants who can recover the secret are called access sets, subsets which have no information about the secret are called nonaccess sets, and subsets which have partial information are called semiaccess sets [9]. Secret sharing has many different applications, e.g., the management of cryptographic keys, the establishment of access codes with restricted access, and as a component of secure multiparty computation.

In contrast to classical secret sharing, the information splitting of a secret and the information distribution in QSS is realized by local measurements on distributed quantum states. Therefore, QSS allows to distribute the shares securely in the presence of eavesdropping. Moreover, QSS distinguishes further between QSS of classical information [6] and QSS of quantum information [10]. Here, we consider QSS of classical information. Different protocols for three- and four-party QSS using the resource of multipartite entanglement have been proposed [6,11]. But, until now, only three-photon entanglement has been used to proof the experimental feasibility and to give an experimental demonstration of three-party QSS [12,13].

In this Letter, we present the first experimental demonstration of four-party QSS via four-photon entanglement. In this scheme, any one of the four participants can act as the dealer, while the remaining three participants form the access set. For the experimental implementation, we use the following four-photon polarization-entangled state [14,15]:

$$|\Psi_4^-\rangle = \frac{1}{2\sqrt{3}}[2|HHVV\rangle - |HVHV\rangle - |HVVH\rangle - |VHHV\rangle - |VHVH\rangle + 2|VVHH\rangle]_{abcd}, \quad (1)$$

where H and V denotes horizontal and vertical polarization of photons in the four spatial modes a, b, c, and d. This state shows perfect four-photon polarization correlations as indicated by the four-photon polarization correlation function defined as the expectation value of the product of the four operators $\hat{s}_x = |+,\Phi\rangle_x\langle +,\Phi| - |-,\Phi\rangle_x\langle -,\Phi|$, with eigenstates $|\pm,\Phi\rangle_x = 1/\sqrt{2}(|R\rangle \pm e^{i\phi_x}|L\rangle)$ and eigenvalues ± 1, where R and L denote right- and left-handed circular polarization. The explicit expression of this correlation function for the four-photon state given by Eq. (1), is

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

Another property of this state, which is useful for the realization of multiparty secure quantum communication, is its ability to violate a four-party Bell inequality [16]:

$$S = \frac{1}{2^4}\sum_{s_x=\pm 1}\left|\sum_{y=1,2} s_a^k s_b^l s_c^m s_d^n E(\phi_a^k,\phi_b^l,\phi_c^m,\phi_d^n)\right| \le 1, \quad (3)$$

where each index $y = k, l, m, n$ denotes a pair of angles defining the local polarization measurement settings required for the evaluation. A strong violation of this Bell inequality (with $S = 1.886$) is obtained, e.g., for $\phi_b^{1,2} = 0$,

$\pi/2$ and $\phi_{a,c,d}^{1,2} = \pi/4, -\pi/4$, or any other setting resulting by permutation of the indices.

The four-party QSS protocol works as follows: Alice, Bob, Claire, and David share each a photon from the $|\Psi_4^-\rangle$ state. In the following, we assume that Alice is the dealer. Each party chooses randomly between two complementary measurement bases. This can be, for example, either the $\{H, V\}$ and $\{P, M\}$ basis ($\phi_x = 0, \pi/2$) analog to the BB84 protocol [17], or a basis set like $\{\{22.5°, 112.5°\}, \{-22.5°, 67.5°\}\}$ ($\phi_x = \pi/4, -\pi/4$), which can also be used to violate the Bell inequality given by Eq. (3), in analogy to the Ekert scheme [18]. To transfer the measurement results into a key sequence, each participant identifies his result either with a bit value of 0 or 1. The measurements will be repeated until they have established a raw key of desired length. For key sifting, each participant announces publicly whenever he has registered a photon and which measurement basis he has used, but not the results. For the announcement, Bob, Claire, and David send their information about their measurement to Alice. After that, Alice can decide which quadruples will be used for secure communication: according to Eq. (2), she will keep those results where all participants used the same basis setting and will drop all others.

The information splitting works as follows: consider, e.g., the case where all four parties have measured in the $\{H, V\}$ basis. Suppose Bob obtained the result $|H\rangle_b$ ($|V\rangle_b$), then he cannot predict with certainty the measurement result of Alice, because there are two different possible outcomes for her. Similarly, each other participant is not able to obtain the secret of Alice without cooperation. Let us now consider pairwise cooperation. If Bob and Claire obtained the result $|HV\rangle_{bc}$ ($|VH\rangle_{bc}$), both together are not able to get the secret. They need the help of David to determine the key bit of Alice. Only in cases where Bob and Claire have obtained the result $|HH\rangle_{bc}$ ($|VV\rangle_{bc}$) they can infer the key bit without the help of David. The same is true for Bob and David, or Claire and David. This implies that always two of them have some partial information on Alice's key. However, Bob, Claire, and David must cooperate to retrieve the complete key and to ensure perfect information-theoretic security, the partial information of any semiaccess set can be removed by the application of a hash function (privacy amplification) [19,20].

After key sifting, all participants have to check for external eavesdropping. Depending on their chosen basis settings they can proceed as follows: if they used a basis set similar to the BB84 protocol, they can use a fraction of their measurement results (which should be perfectly correlated) for the evaluation of the quantum bit error rate (QBER) defined as the ratio of wrong bits to all bits. If the QBER is low enough, they can use their results to distill a secure key, otherwise they have to discard their bits [21]. If they used a basis set which can be used to violate the Bell inequality given by Eq. (3), they can use a fraction of their measurement results for the evaluation. If the violation is high enough, they can use their key bits, otherwise they have to drop them [22].

To finally obtain a common secure key, they have to perform key reconciliation and privacy amplification. For this, different strategies developed for quantum key distribution (QKD) can be adapted [19,23]. After that, Alice can use the final key for an unbreakable encryption of her secret information via the Vernam cipher [24] and broadcasts the encrypted message to Bob, Claire, and David. Cooperation of Bob, Claire, and David allows the reconstruction of the key and therefore to obtain the secret information of Alice.

The four-party QSS protocol was experimentally implemented as sketched in Fig. 1. We used a mode-locked Ti:sapphire laser emitting pulses with a pulse length of about 120 fs at a repetition rate of 82 MHz. This radiation is frequency-doubled with a lithium-triborate crystal to $\lambda = 390$ nm which is used to pump a 2 mm thick beta-barium-borate crystal to generate the four-photon polarization-entangled state given by Eq. (1) via pulsed type-II parametric down-conversion. This state results directly from the four-photon emission of the pulsed down-conversion source and the usage of two beam splitters to distribute these photons into the four spatial modes a, b, c, and d [15,25]. Alice, Bob, Claire, and David obtain each a photon from the four-photon state and measure randomly in one of two complementary bases chosen by a random number generator orienting a half-wave plate in front of a polarizing beam splitter via step motors. For the encoding, the detection of a photon in the transmitted (reflected) output mode of the polarizing beam splitter is set to a bit value of 0 (1). The four photons were detected by eight silicon avalanche photodiodes with detection efficiencies of about 40%. For the registration of all 16 relevant four-

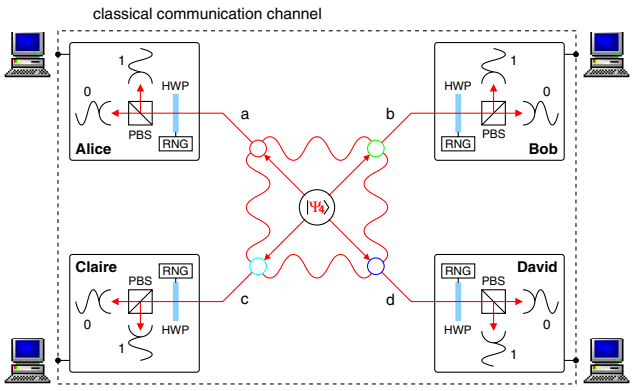

FIG. 1 (color online). Scheme of the experimental implementation: the four-photon source distributes the four photons of the entangled state $|\Psi_4^-\rangle$ into the four modes a, b, c, and d. Each party uses a random number generator (RNG) which sets a half-wave plate (HWP) angle and a polarizing beam splitter (PBS) followed by two avalanche photodiodes for the analysis and registration of the distributed photons.

photon coincidences, we used an eight-channel multiphoton coincidence unit [26]. We observed a four-photon state rate of about 0.4 per second. To build up a shared key, the acquisition time for each randomly chosen analysis setting was set to 1 s. If more than one four-photon coincidence event was registered during that time, only the first one was chosen.

An analysis of the four-photon source used for the experimental implementation, where Alice, Bob, Claire, and David have measured in the $\{H, V\}$ basis is shown in Fig. 2. The data acquisition time was 24 hours. Because of differences in the efficiencies of the detectors, the presented four-photon coincidences have been corrected without changing the overall raw detection rate. The corresponding four-photon correlation is $E = 0.945 \pm 0.002$, which demonstrates the high quality and stability of this four-photon source.

To demonstrate the perfect four-party correlations, necessary for four-party QSS, we analyzed the four-photon correlations under different polarization analyzer orientations. In Fig. 3(a) the results of two measurements are shown, where Alice, Claire, and David have analyzed their photons in the $\{H, V\}$ ($\{P, M\}$) basis corresponding to $\phi_{a,c,d} = 0$ ($\pi/2$), while Bob varied his analysis direction ϕ_b from 0 to 4π. The maximal absolute value of $E(\phi_a, \phi_b, \phi_c, \phi_d)$ can be expressed by a visibility V according to $E = V\bar{E}$, where $\bar{E}$ denotes the theoretical value. Fitting the experimental data leads to a visibility of $V_{H/V} = 92.3 \pm 0.8\%$ and $V_{P/M} = 88.2 \pm 1.2\%$. Figure 3(b) shows the experimental results obtained from two measurements, where Alice, Claire, and David analyzed their photons in the $\{22.5°, 112.5°\}$ ($\{-22.5°, 67.5°\}$) basis corresponding to $\phi_{a,c,d} = \pi/4$ ($-\pi/4$), while Bob varied his analyzer setting ϕ_b. The resulting visibilities are $V_{22.5°/112.5°} = 90.2 \pm 1.1\%$ and $V_{-22.5°/67.5°} = 89.0 \pm 0.7\%$, respectively. The overall data acquisition time for each four-photon correlation function was 8.5 hours. The average visibility can be translated into the QBER via QBER $= (1 - \bar{V})/2$ leading to a QBER of $4.88 \pm 0.50\%$ and $5.22 \pm 0.45\%$ for each basis set [27].

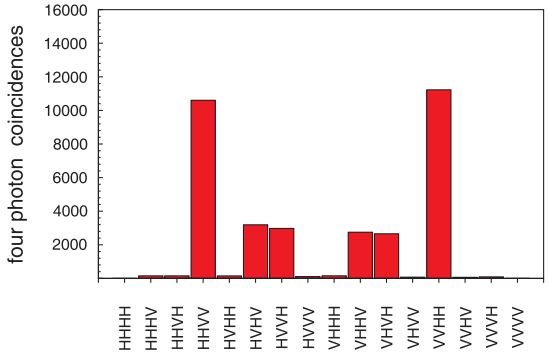

FIG. 2 (color online). Analysis of the four-photon source, where Alice, Bob, Claire, and David have chosen the $\{H, V\}$ basis for their polarization analysis. Shown are all possible four-photon coincidence detection events under the condition that in each of the four output modes a photon was detected. The four-photon correlation is $E = 0.945 \pm 0.002$.

For a full experimental demonstration of four-party QSS, we performed a key exchange according to the four-party QSS protocol described above using two different complementary basis sets. Using a key sifting analog to the BB84 protocol, we have exchanged 2000 key bits in a complete transfer time of about 16 hours with a QBER of 5.20%. A fraction of 100 bits of the sifted key is shown in Fig. 4. Neglecting the dead time required to set the polarization analysis direction and considering in addition those events which have been registered in the same time interval, leads to a bit rate of 196 bits per hour being in good agreement with the theoretical expected rate. To check for eavesdropping, Alice chooses a random subset of 200 bits (10%) of the sifted key and asks Bob, Claire, and David for their results at those positions. From this subset, she evaluates the QBER and obtains a value of 4% [28]. This value lies well below several known security threshold values required for two-party QKD and should therefore be low enough to distill finally a perfect secure key [21,27]. Thus,

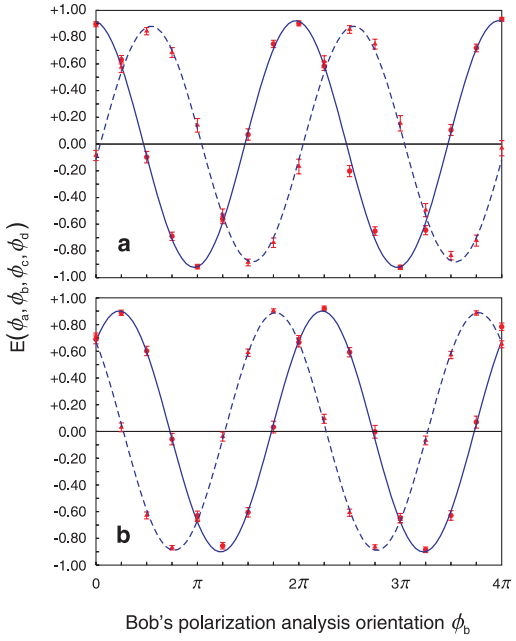

FIG. 3 (color online). Four-photon polarization correlations: Alice, Claire, and David have set their polarization analysis orientation (ϕ_a, ϕ_c, ϕ_d) in (a) either to 0 (○) or $\pi/2$ (△) corresponding to the $\{\{H, V\}, \{P, M\}\}$ basis set, or in (b) either to $+\pi/4$ (○) or $-\pi/4$ (△) corresponding to the $\{\{22.5°, 112.5°\}, \{-22.5°, 67.5°\}\}$ basis set, while Bob varied his polarization analyzer setting (ϕ_b) from 0 to 4π. The solid and the dashed lines represent numerical fits, leading in (a) to a visibility of $V_{H/V} = 92.3\% \pm 0.8\%$ and $V_{P/M} = 88.2\% \pm 1.2\%$, and in (b) to a visibility of $V_{22.5°/112.5°} = 90.2\% \pm 1.1\%$ and $V_{-22.5°/67.5°} = 89.0\% \pm 0.7\%$.

x_A	0100111110101111000001000011000000110011110**0**0101100011000011111**1**0011111**1**1100010101111010011000000**0**1110
x_B	0011110101101101000100011010110111010111100**1**0101011001010010111**1**010101**1**0100101111110101110100100**1**01010
x_C	1010000000010010111110111100001111101000011**0**1010011110111100001**1**1010010101101010000010110011111**1**00001
x_D	1101001011010000111011100101111000001100001**0**1010100100101101000**0**100010**0**0011101000000101000101101**1**0101
x_{AS}	0100111110101111000001000011000000110011111**1**0101100011000011111**0**0011110**1**1100010101111010011000000**1**1110

FIG. 4 (color online). Sifted key: Shown are 100 out of 2000 experimentally exchanged four-party key bits. Bits printed in bold indicate errors. The first row shows the key of Alice denoted by x_A. The second, third, and fourth row shows each 100 key bits of Bob, Claire, and David denoted by x_B, x_C, and x_D. As can be seen, no one of them alone and no two parties of them together are able to obtain the key of Alice. Only by cooperation of Bob, Claire, and David (access set) they will be able to reconstruct the key of Alice via the computation of the logical XOR function ($x_{AS} = x_B \oplus x_C \oplus x_D = x_A$), as shown in the last row.

using the remaining 1800 bits to perform key reconciliation and privacy amplification, Alice ends up with a totally secure key with about 200 bits [29]. For the reconstruction of the final key, Bob, Claire, and David have to combine their individual bits of the reconciled key and have to perform the same privacy amplification procedure as Alice.

Using the Bell angles ($\phi_x^{1,2} = \pi/4,\ -\pi/4$) for key sifting, while Bob switches every fifth measurement to $\phi_b^{1,2} = 0, \pi/2$, we obtained 1342 key bits in about 21 hours with a QBER of 5.96%. Since $1/5$ of the measured data can be used to evaluate the Bell inequality given by Eq. (3), we obtained a value of $S = 1.78 \pm 0.07$, which is well above the classical limit of 1 and very close to the theoretical value of 1.886. Since the value for S scales linear with the visibility, the achieved value of S can be translated into a QBER of about 3%, which should be low enough to ensure secure quantum communication [21,27].

We demonstrated four-party QSS via the resource of four-photon entanglement. We obtained bit rates of about 100 bits per hour with QBERs of about 5%, which should be low enough to ensure perfect security. Comparing this with QBERs usually obtained in QKD between two parties, we obtain similar results demonstrating the feasibility of secure multiparty quantum communication via multiphoton entanglement. For future implementations, it would be useful to use fast optical switches for an efficient registration. Using in addition known techniques to increase the efficiency of the key exchange, this scheme can be extended to obtain the maximal reachable efficiency [30].

We would like to thank A. Sen, U. Sen, and M. Zukowski for useful conversations. This work was supported by the DFG, the Bavarian high-tech initiative, and the EU-Projects RamboQ and QAP.

[1] K. Mattle *et al.*, Phys. Rev. Lett. **76**, 4656 (1996).
[2] D. Bouwmeester *et al.*, Nature (London) **390**, 575 (1997).
[3] T. Jennewein *et al.*, Phys. Rev. Lett. **84**, 4729 (2000).
[4] W. Dür and J. I. Cirac, J. Mod. Opt. **47**, 247 (2000).
[5] M. Murao *et al.*, Phys. Rev. A **59**, 156 (1999).
[6] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[7] A. Shamir, Commun. ACM **22**, 612 (1979).
[8] G. Blakely, Proc. AFIPS **48**, 313 (1979).
[9] W. Ogata and K. Kurosawa, JUCS **4**, 690 (1998).
[10] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[11] A. Sen(De), U. Sen, and M. Zukowski, Phys. Rev. A **68**, 032309 (2003).
[12] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[13] Y.-A. Chen *et al.*, Phys. Rev. Lett. **95**, 200502 (2005).
[14] H. Weinfurter and M. Zukowski, Phys. Rev. A **64**, 010102(R) (2001).
[15] S. Gaertner *et al.*, Appl. Phys. B **77**, 803 (2003).
[16] M. Zukowski and C. Brukner, Phys. Rev. Lett. **88**, 210401 (2002).
[17] C. H. Bennett and G. Brassard, *Proceedings of the IEEE, International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[18] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[19] C. H. Bennett *et al.*, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[20] To remove this partial information via universal hashing, the reconciled key must be reduced by a factor of $r > 2/3$.
[21] Until now, no unconditional security threshold value for any entanglement based QSS protocol has been strictly proven, but it seems to be reasonable to assume similar threshold values as for two-party QKD protocols.
[22] So far, no connection between the security of this QSS protocol and the violation of S, given by Eq. (3), has been pointed out, but the value of S can be translated into the QBER allowing to estimate a threshold value for S [21].
[23] C. H. Bennett *et al.*, J. Cryptology **5**, 3 (1992).
[24] G. S. Vernam, J. Am. Inst. Electr. Eng. **45**, 109 (1926).
[25] M. Eibl *et al.*, Phys. Rev. Lett. **90**, 200403 (2003).
[26] S. Gaertner, C. Kurtsiefer, and H. Weinfurter, Rev. Sci. Instrum. **76**, 123108 (2005).
[27] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).
[28] The QBER depends on the randomly chosen subset and varies around the average value of 5.2%.
[29] For key reconciliation, they compared the parity of blocks with size 2 and 10 leading to a key with 711 bits without error.
[30] H.-K. Lo, H. F. Chau, and M. Adrehali, J. Cryptology **18**, 133 (2005).