Experimental quantum secret sharing using telecommunication fiber

Jan Bogdanski, Nima Rafiei, and Mohamed Bourennane
Physics Department, Stockholm University, SE-10691 Stockholm, Sweden

(Received 12 May 2008; revised manuscript received 25 October 2008; published 4 December 2008)

We report quantum secret sharing experiment in telecommunication fiber in five-party implementation. The quantum secret sharing experiment has been based on a single qubit protocol, which has opened the door to practical secret sharing implementation over fiber channels and in free space. The previous quantum secret sharing proposals were based on multiparticle entangled states, difficult in the practical implementation and not scalable. The secret sharing protocol has been implemented in an interferometric fiber optics setup with phase encoding and demonstrated for three, four, and five parties. The experimental setup measurements have shown feasibility and scalability of secure multiparty quantum communication over commercial telecom fiber networks.

DOI: 10.1103/PhysRevA.78.062307 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ex

I. INTRODUCTION

Splitting a secret message in the way that a single person is not able to reconstruct it is a common task in information processing and security applications. For instance, let us assume that withdrawing cash from a joint bank account is possible only when all account owners cooperate by generating a code required by an automated teller machine or by a banker [1]. A solution for this problem and its generalization, including several variations, is provided by classical cryptography and is called secret sharing. It consists of a way of splitting the message using mathematical algorithms and the distribution of the resulting pieces to two or more legitimate users by classical communication. However, all ways of classical communication currently used are susceptible to eavesdropping attacks. As the usage of quantum resources can lead to unconditionally secure communication, a protocol implementing quantum secret sharing has been developed [2,3]. The protocol provides information splitting and eavesdropping protection. However, the implementation is in practice nonscalable since it used multiphoton polarization entangled states that are difficult to generate and transmit. Furthermore, the use of polarization encoding is impractical for applications over commercial birefringent single mode fibers (SMF) networks. Nevertheless, three proof of principle experiments, using three [4,5] and four [6] entangled polarized photons, have been carried out.

A protocol solving the abovementioned problems was proposed in 2005 [7]. The protocol requires only a single qubit for quantum information transmission, which has allowed its practical experimental realization and scalability. In this paper we report a single qubit (photon in our case) quantum secret sharing experiment over telecommunication fiber in an interferometric setup using this protocol with phase encoding in three, four, and five-party implementations. The protocol constitutes the main transmission layer. More layers could be added on it in order to provide means for a particular quantum transmission application.

II. SINGLE QUBIT QUANTUM SECRET SHARING PROTOCOL

As already mentioned, our experiment has been based on an N-party quantum secret sharing protocol using single qubit with the users called $R_1, \ldots, R_N$ [7], as is shown in Fig. 1. A qubit is prepared in an initial state $|x\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ by the party R_1 and is sent sequentially, from R_1 to R_N, over the quantum channel, until it is measured by the last party R_N. Each party $R_i (i=1, \ldots, N-1)$ modulates the photon with a randomly chosen phase ϕ_i equal 0, $\pi/2$, π, or $3\pi/2$ through the unitary phase operator

$$\hat{U}(\phi_i) = \{|0\rangle \rightarrow |0\rangle; |1\rangle \rightarrow e^{i\phi_i}|1\rangle\}. \quad (1)$$

The parties $R_1, R_2, \ldots$, and R_{N-1} modulating phase choices 0, $\pi/2$, π, and $3\pi/2$ can be assigned into two bases $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. The R_N party's phase modulation choice ϕ_N is limited to two phases only: 0 (which belongs to the basis $\{0, \pi\}$) and $\pi/2$ (which belongs to the basis $\{\pi/2, 3\pi/2\}$). The probability that R_N detects the state $|\pm x\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ reads

$$p_{\pm}(\phi_1, \ldots, \phi_N) = \frac{1}{2}\left[1 \pm \cos\left(\sum_j^N \phi_j\right)\right]. \quad (2)$$

In half of the cases the phases add up in such a way that the measurement results are deterministic, indicating a constructive or destructive interference with the total correlation function given by

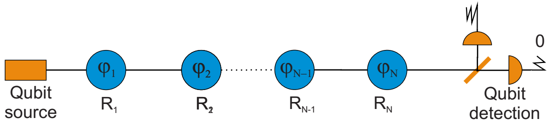

FIG. 1. (Color online) N-party single qubit secret sharing. A qubit (in our case a photon) is prepared in an initial state by the part R_1, using a single qubit source, and is sent sequentially, from R_1 to R_N, over the quantum channel, until it is measured by the last part R_N. Each party modulates the photon with a randomly chosen phase $\phi_i (i=1, \ldots, N-1)$ between 0, $\pi/2$, π, or $3\pi/2$. The part R_N measures with phase modulation choice ϕ_N between 0 and $\pi/2$. In half of the cases the phases add up in such a way that the measurement results are deterministic, indicating a constructive or destructive interference. These cases can be used for the secret sharing.

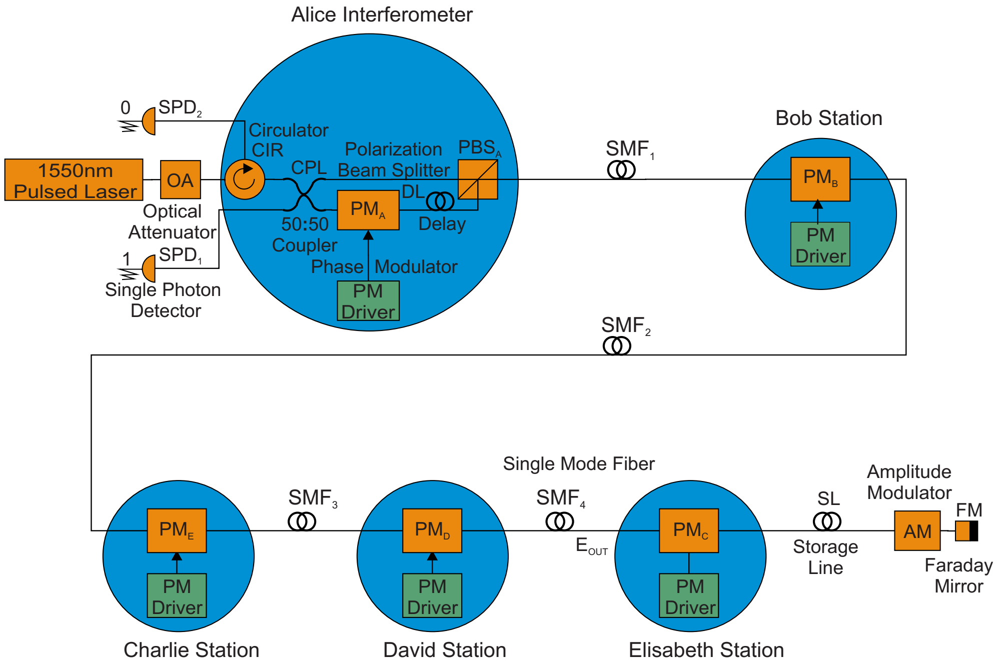

FIG. 2. (Color online) Experimental setup for five-party phase encoded quantum secret sharing. For details, see the text. The setup does not show the control electronics layer and wavelength-division multiplexing (WDM) layer used to send synchronization and trigger from Alice to remaining parties. For this purpose a second pulsed laser with 1538 nm wavelength was used.

$$E(\phi_1, \ldots, \phi_N) = \cos(\phi_1 + \cdots + \phi_N). \quad (3)$$

These cases can be used for the secret sharing. After the photon has been detected, the parties, in a reverse order (i.e., $R_N, R_{N-1,\ldots}, R_2, R_1$) [8,9], announce on a public channel their basis choices, but keep their particular modulating phases secret. The reason for the reverse order announcement is to provide a full protection against possible cheating strategies of the kth partner R_k [9].

From the publicly shared basis information, the parties can determine which runs led to deterministic measurements with $\cos(\phi_1+\cdots+\phi_N)=\pm 1$. In these cases, any subset of $N-1$ parties is able to infer the modulating phase of the remaining part if all the $N-1$ parties of the subset collaborate and reveal among themselves their modulating phases (the way in which the parties collaborate and reveal modulating phases depends on the secret sharing application). If the subset includes the part R_N, it must reveal the measurement results (it has already revealed its basis choices on the public channel). In such a way the goal of secret sharing has been achieved.

III. EXPERIMENTAL SETUP

Figure 2 shows the experimental setup for a five-party quantum secret sharing system with phase encoding. The setup consists of four main parts: a weak coherent pulsed 1550 nm laser from id Quantique, SMF transmission channels, four stations (each station consists of a polarization insensitive phase modulator with its driver, described in Sec. IV), and two single photon detectors SPD$_1$ and SPD$_2$.

In detail, a relatively strong (1 mW) 1550 nm, 500 ps laser pulse is generated by a laser driver at 2 MHz repetition rate. The setup attenuates the light pulse in several components discussed below so its energy level finally, on the way back from the Faraday mirror (FM), after it has passed Elisabeth's station, corresponds to a single photon [10]. Such "faint-pulses" of the coherent light follow Poisson distribution, which makes it possible to limit the probability that a nonempty weak pulse contains more than one photon to an arbitrary small number. Assuming an attenuation giving the mean photon number $\mu=0.1$ (one single photon for ten laser pulses), the probability that a nonempty pulse contains more than one photon is $P(n>1)=\mu/2=0.05$, a low number.

The laser pulse is sent to the digitally controlled optical attenuator (OA) from OZ Optics for its initial attenuation. The attenuated laser pulse passes the circulator (CIR) and splits equally in the 50:50 coupler (CPL). The upper pulse goes through the interferometer's short arm and leaves the polarized beam splitter (PBS) horizontally polarized, while the lower pulse through the interferometer's long arm and leaves the PBS vertically polarized (the latter pulse is delayed by 60 ns). After passing the transmission channels and being reflected by the FM [11] (that rotates the polarization of the input light by 90°) their polarizations are reversed so they transmit over opposite interferometer arms. In such a way their total transmission paths are exactly the same so they interfere constructively or destructively (accordingly to their phase difference) in the coupler (CPL). The coupler's outputs are connected to the SPD$_1$ and SPD$_2$ (PGA600), built on InGaAs avalanche photodiodes, from Princeton Lightwave, Inc. The detector provides 20% quantum efficiency and 10^{-5} dark count probability per 1 ns avalanche gating pulse. The secret key is established by modulating the phase of the long arm pulse by Elisabeth, David, Charlie, and Bob. Alice part of the process is to set the measurement basis of the interferometer. She does it by using her phase modulator (PM_A).

It should be emphasized that all components of the interferometer are polarization maintaining. One of the reasons for this requirement is that Alice's PM is polarization sensitive. It shows a very high attenuation for the vertical polarization (fast axis component) and 3 dB attenuation for the horizontal one (slow axis). Also both outputs of the PBS are aligned to the horizontal axis. This means that all the signals in the interferometer should be aligned horizontally, which requires overall use of polarization maintaining components, including the delay line, and even interconnecting fiber cords.

As already mentioned, the laser pulse, after it has been reflected by the FM, is attenuated by the amplitude modulator (AM) in such a way that its energy (after it has left Elisabeth's station on its way back to Alice) is set to a single photon level. Thus, the port E_{out} of Elisabeth's station (see Fig. 2) is a starting point of the quantum channel transmission. Here, it should be pointed out that the attenuation of the laser pulse occurs not only in the OA, AM, and SMF spools, but also in other components (mainly in the PMs) of the setup so the attenuation in the SMF spools is a relatively small part of the total signal attenuation.

In order to avoid single photons back-scattering, a 25 km long fiber spool has been placed inside the last station (Elisabeth). The spool (storage line) works as a first in first out (FIFO) buffer memory. The laser pulses are sent as a high-speed burst, loading the storage line. No new burst is sent until all the pulses in the storage line have traveled back to Alice's interferometer.

Finally for this section, it should be mentioned that the driver voltage of Alice's PM has to be set to zero during the time the long arm pulses pass over it (on their way to the PBS). The same applies for the remaining modulators since the phase modulation has to be carried out only on single photon level pulses, traveling back to Alice' interferometer (after they have been reflected by the FM [12]).

IV. POLARIZATION INSENSITIVE PHASE MODULATORS

As already mentioned, the short arm pulse leaves the PBS horizontally polarized, while the long arm one vertically. However, their polarization changes along the setup's transmission path since the single mode fibers are birefringent. The birefringence would cause significant, slowly varying attenuation changes in the standard telecom PM (usually based on a LiNbO_3 crystal). Unfortunately, there are no, to the best of our knowledge, commercially available polarization insensitive PM on the market.

Another difficulty, facing a designer of any "faint-pulse" based quantum information system, using telecom PM, is a need of laser pulses' precise attenuation so they leave the last station (in our case Elisabeth's), on their way back to the Alice interferometer, as single photons (in accordance with the "faint pulse" approach [10]). Since the telecom PMs are polarization sensitive and the fiber birefringence causes slow, random polarization changes then there is no way to guarantee a stable attenuation of the entire system. This means that it is not possible to guarantee that the faint pulses leaving Elisabeth's station are on an assumed mean photon number μ. Therefore, Bob's, Charlie's, David's, and Elisabeth's stations require polarization insensitive PM.

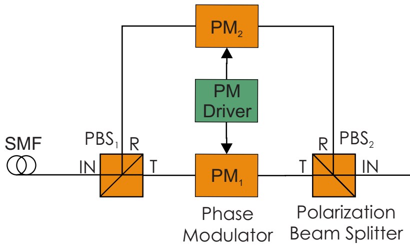

FIG. 3. (Color online) Polarization insensitive phase modulator. The R output of the PBS denotes the reflected component (vertical), while the T output denotes the transmitted component (horizontal).

We have realized a polarization insensitive PM based on commercially available optical fiber components. Figure 3 shows the block diagram of our scheme, which implements 1550 nm, 500 MHz bandwidth phase modulators from JDSU Inc. The modulator's polarization maintaining pigtails have been aligned to the slow (horizontal) axis, which have required the same alignment of the polarizing beam splitters PBS_1 and PBS_2. The modulator's working principle is simple: it splits horizontal and vertical polarization components into two separately controlled phase modulators.

In detail, let us consider an input light pulse horizontally, diagonally, circularly, or generally elliptically polarized arriving into PBS_1. The pulse's horizontal polarization component will be transmitted into the port T, while the vertical one will be "reflected" into the port R and rotated into the horizontal polarization. Thus, both components can be transmitted (and modulated) by the phase modulators PM_1 and PM_2. The outputs of the modulators are connected to the PBS_2, which recreate the original light pulse polarization. One of major advantages of our scheme is its bidirectionality so it can be used both in bidirectional "plug and play" quantum key distribution (QKD) and secret sharing systems as well as in unidirectional ones (in time-bin QKD, for instance).

In the case of the plug and play QKD, the above mentioned forward transmitted horizontal and vertical components will be passing the opposite modulators, on their way back from the FM, due to the fact that this device rotates the polarization of the input light by 90°. Thus, both components will be traveling the same path from the point where they were created (i.e., in Alice interferometer's coupler) to the same point, which is the core of the plug and play system.

Both phase modulators are controlled by the same modulation radio frequency (rf) voltage driver with a V_π of 3–3.5 V. Our PM scheme guarantees a stable, polarization insensitive optical insertion loss of 4.5–5.5 dB.

V. TRANSMISSION AND ERROR RATES

The raw rate in the protocol is defined as $R_{\mathrm{raw}} = q\mu f \eta_{\mathrm{det}} \eta_{\mathrm{link}}$, where q is a setup dependent coefficient, μ is the mean number photons per pulse, f is the laser pulsing frequency, η_{det} is the photon's detection probability, and η_{link}

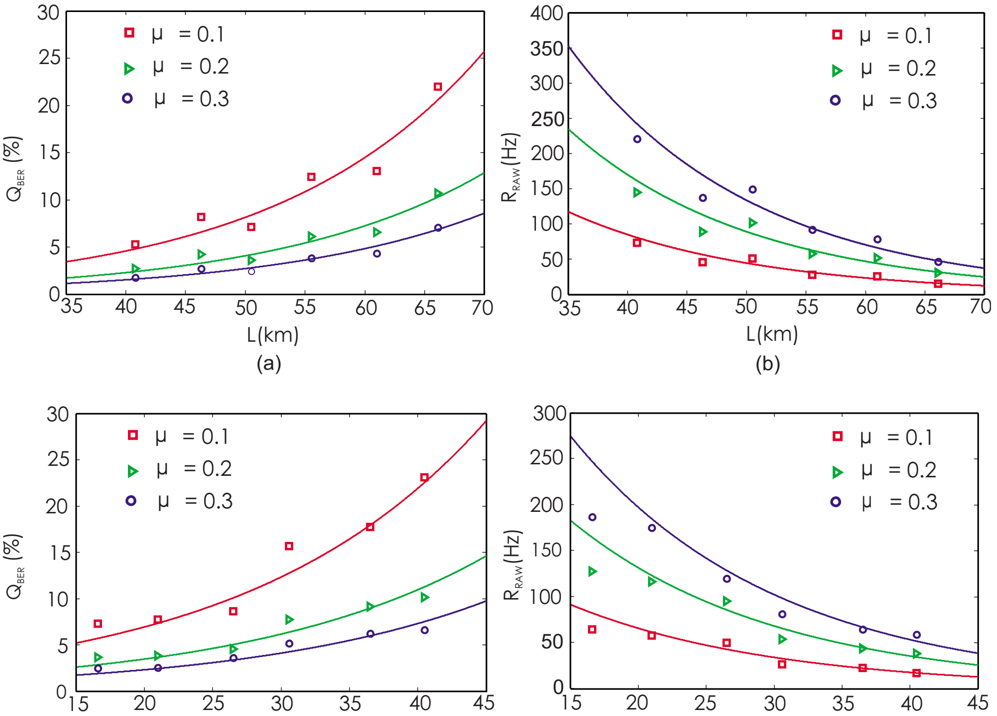

FIG. 4. (Color online) Multiparty quantum secret sharing experimental results. (a) Quantum bit error rate (Q_{BER}) for three-party and four-party, (b) raw rate, both as a function of fiber length with 0.25 dB km^{-1} loss and channel loss for three and four-party quantum secret sharing. The squares show measurement results for μ=0.1, the triangles for μ=0.2 and the dots for μ=0.3. The theoretical curves were drawn for the following measured attenuation of the setup's parts: 5 dB for Alice, Charlie, and David stations; 4.2 dB for the Elisabeth station. In both four-party and three-party setups the Bob station was not used. The total attenuation in the interconnecting FC contacts was measured to 1.8 dB. The achieved visibilities were greater than 98.5%. All the measurements were carried out at the laser driver repetition rate f_{laser}=2 MHz. The efficient laser pulse frequency $f_{\mathrm{eff}}=d_{\mathrm{cycle}}\times f_{\mathrm{laser}}$ was lower due to the duty cycle $d_{\mathrm{cycle}}=l_{\mathrm{burst}}/(l_{\mathrm{burst}}+l_{\mathrm{pause}})\leqslant 0.5$, see Sec. III.

is the transfer efficiency of the link between Elisabeth's station and Alice's detectors. The factor q=0.5 in our setup since only in 50% of all the measurement cases the measurement basis are compatible. The Q_{BER} for the faint laser pulse QKD can be written as a sum of two main contributing factors: $Q_{\mathrm{BER}}=Q_{\mathrm{BERopt}}+Q_{\mathrm{BERdet}}=p_{\mathrm{opt}}+p_{\mathrm{noise}}/p_{\mathrm{photon}}=p_{\mathrm{opt}}+p_{\mathrm{noise}}/\mu\eta_{\mathrm{det}}\eta_{\mathrm{link}}$, where p_{opt} is the probability of a photon going to the wrong detector, p_{noise} is the probability of getting a noise count (mainly dark counts) per gating pulse window [12,13]. For the phase-based QKD $p_{\mathrm{opt}}=(1-V)/2$, where V is the interference visibility.

VI. EXPERIMENTAL RESULTS

Our quantum secret sharing experiment was carried out for three, four, and five parties. All the measurements were carried out at the laser driver repetition rate f_{laser}=2 MHz. The efficient laser pulse frequency $f_{\mathrm{eff}}=d_{\mathrm{cycle}}f_{\mathrm{laser}}$ was lower due to the duty cycle $d_{\mathrm{cycle}}=l_{\mathrm{burst}}/(l_{\mathrm{burst}}+l_{\mathrm{pause}})\leqslant 0.5$ (see Sec. III). The results for three-party and four-party are shown in the Fig. 4. For the three-party we have achieved 50.5 km quantum secret sharing transmission distance at μ=0.1 with visibility V=99.0% and Q_{BER}=7.1%; 61.0 km at μ=0.2 with V=98.9% and Q_{BER}=6.6%; 66.1 km at μ=0.3 with V=99.0% and Q_{BER}=7.1%, while for the four-party we have achieved 21.0 km distance at μ=0.1 with V=98.9.0% and Q_{BER}=7.8%; 30.6 km at μ=0.2 with V=99.1% and Q_{BER}=7.7%; 40.5 km at μ=0.3 with V=98.8.0% and Q_{BER}=6.6%.

The five-party measurements have shown quantum secret sharing feasibility over local area networks (LAN) with quantum secret sharing transmission over 6.7 km fiber with V=99.0% and Q_{BER} of 9.5, 5.3, and 3.5% for μ equal to 0.1, 0.2, and 0.3 respectively. The distance was limited by the PM losses of 5 dB for Alice's, Bob's, Charlie's, David's, and 4.2 dB for Elisabeth's station.

It should be emphasized that 5 dB loss corresponds to 20 km of standard SMF with 0.25 dB km^{-1} loss so the total distance loss, caused by three additional PM in the five-party implementation, is in the range of 60 km. Therefore, it should not be surprising that with the present technologies only a LAN distance has been obtained in the five-party experiment.

VII. DECOY IMPLEMENTATION

To overcome possible photon-number splitting (PNS) eavesdropping attacks we have implemented a one-decoy state protocol [14–16], by adding a fiber pigtailed acousto-optic AM from Brimrose, Inc. at the last station of the setup. In order to avoid the Doppler effect (a frequency shift of the laser pulses) [17] we have chosen a variable frequency driver for the AM. The AM is used for intensity modulation of the laser pulses in such a way that the signal pulses (with the average photon number $\mu=0.3$) are interleaved with the decoy states (with the average photon number $\nu=0.1$). By analyzing statistical characteristics of both decoy and signal states a PNS attack can be detected. In such a way the security of the "faint-pulse" based systems is greatly enhanced [14–17].

It should be pointed out that the optimal choice of the decoy state mean-photon number ν depends, among other parameters, on the channel attenuation [16] to which, in our five-user implementation, have mainly contributed the setup's PMs. Our choice of $\nu=0.1$ has been based on the published one-decoy state protocol simulation data [16], which have shown that for the fiber quantum channel lengths between 20 and 100 km the optimal decoy state mean-photon number ν varies between 0.04 and 0.13. Despite the relatively low total length of the transmission channel our decoy state mean-photon number ($\nu=0.1$) was chosen close to the upper bound of the data in Ref. [16] due to the high total attenuation of the setup's PMs.

Our choice of $\mu=0.3$ has been based on a very practical approach to a complicated problem of providing unconditional security for secret sharing transmissions in our multiparty setup with varying fiber lengths and strong attenuation variations caused mainly by the setup's PMs (as already mentioned, the average party station's attenuation was 5 dB).

In order to illustrate our implementation of the one-state decoy protocol let us focus here on the five-user setup (with most challenging total system attenuation and distortions). The one-state decoy protocol was proposed in Ref. [18] and its security has been analyzed in Ref. [16]. It should be emphasized that the one-state decoy protocol is not only simple in its implementation, but also very close in performance (for transmission distances up to 80 km) to the optimal decoy protocol (asymptotic case) with infinite number of decoy states [16,17].

In Ref. [18] the security analysis of a general decoy protocol was combined with the results of the Bennet and Brassard 1984 protocol security analysis carried out by Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [19]. The analysis led to the following formula for the lower bound of the secure key generation rate

$$S \geqslant q\{-Q_\mu f(E_\mu)H_2(E_\mu)+Q_1[1-H_2(e_1)]\}, \qquad (4)$$

where $q=1/2$ for Bennet and Brassard 1984 protocol without decoy (see Sec. V) and $q<1/2$ with decoy implementation, μ denotes the average photon number for signal states, Q_μ is the gain of signal states, E_μ is the quantum bit error rate (QBER), Q_1 is the gain of single-photon states, e_1 is the error of single-photon states, $f(x)\geqslant 1$ is the error correction function with Shannon limit $f(x)=1$, and $H_2(x)$ is the binary Shannon entropy function given by

$$H_2(x)=-x\log_2(x)-(1-x)\log_2(1-x). \qquad (5)$$

The component $f(E_\mu)H_2(E_\mu)$ in Eq. (4) corresponds to the part of the sifted key that is used during error correction process. We have assumed $f(E_\mu)=1.22$ (being the ratio of actually needed redundant bits to the corresponding number of the Shannon limit) corresponding to the 10% error rate and the bidirectional cascade error reconciliation protocol [20,21]. The gain of signal states Q_μ is defined as the probability of Alice to get detection in a pulse for which Elisabeth (the last active station) and Alice use the same basis, while the E_μ is defined as the probability of Alice to get a wrong detection in a pulse for which Elisabeth and Alice use the same basis. Of the total N pulses sent in our experiment $N_s=0.88N$ were sent as signal states so the $q=0.44$ [16].

TABLE I. Experimental data for five-party secret sharing. The duty cycle $d_{\text{cycle}}=l_{\text{burst}}/(l_{\text{burst}}+l_{\text{pause}})=492/1127$ pulses in the five-party implementation, see Sec. III. The efficient laser pulse frequency $f_{\text{eff}}=d_{\text{cycle}}f_{\text{laser}}$. The optical misalignment error $e_{\text{det}}=(1-V)/2$, see Sec. V. The transmittance η_{Alice} has been defined as a loss between Elisabeth's station (its E_{out} port, see Fig. 2, where the mean photon number μ for the signal states and ν for the decoy states are defined) and Alice' single photon detector, including the detector's quantum efficiency. The detector's quantum efficiency $\eta_{\text{det}}=20\%$. Y_0 is the dark count rate of the single photon detector.

Parameter	Value	Parameter	Value
f_{laser}	2 MHz	d_{cycle}	492/1127
f_{eff}	873 kHz	V	0.9895
e_{det}	0.0075	η_{Alice}	6.67×10^{-4}
Y_0	1.1×10^{-5}	η_{det}	0.2

It should be pointed out that in the case of a finite length secret sharing transmission (similarly to a finite length QKD) statistical fluctuations should be analyzed [15–17]. Here, the analysis is omitted since our transmitted data length $N=785$ Mbit was much higher than in Refs. [15–17], which has minimized the effect of statistical fluctuations.

Table I shows the experimental data for five-party secret sharing. The data in the table show high visibility, low optical misalignment and low dark count rate of the single photon detectors, but also very high attenuation (low transmittance). Table II shows the experimental data for the five-party secret sharing with the one-decoy state protocol.

In order to find the lower bound of key generation rate per pulse [Eq. (4)] the lower bound of Q_1 (the gain of single-photon states) and the upper bound of e_1 (the error of single-

TABLE II. Experimental data for five-party secret sharing. The error rate for vacuum $e_0=0.5$. Q_μ is the gain of signal states, E_μ is the QBER, Q_ν is the gain of decoy states, E_ν is the error of decoy states, $f(x)$ is the error correction function with Shannon limit $f(x)=1$, in our experiment $f(x)=1.22$, which corresponds to the 10% error rate and the bidirectional cascade error reconciliation protocol [21,20].

Parameter	Value	Parameter	Value
q	0.44	ℓ	6.7 km
μ	0.3	ν	0.1
$f(E_\mu)$	1.22	e_0	0.50
Q_μ	2.06×10^{-4}	E_μ	3.51×10^{-2}
Q_ν	6.87×10^{-5}	E_ν	9.49×10^{-2}

TABLE III. Calculated values (using data in Tables I and II) of the yield of single-photon states Y_1, gain of single-photon states Q_1, and error of single-photon states e_1.

Parameter	Value	Parameter	Value	Parameter	Value
Y_1	$\geqslant 6.76\times 10^{-4}$	Q_1	$\geqslant 1.5\times 10^{-4}$	e_1	$\leqslant 10.6\times 10^{-2}$

photon states) need to be estimated. In Ref. [16] these bounds for the one-state decoy protocol are derived as an approximation of the vacuum+weak decoy protocol (with none vacuum states). The bounds are derived as functions of Y_1, being the yield of a single-photon state, defined as the conditional probability of a detection event at Alice station assuming that Elisabeth (the last active station) has sent a single photon.

$$Y_1 \geqslant \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2}\right), \tag{6}$$

$$Q_1 = Y_1 \mu e^{-\mu}, \tag{7}$$

$$e_1 \leqslant \frac{E_\nu Q_\nu e^\nu}{Y_1 \nu}. \tag{8}$$

Table III shows the calculated values (using data in Tables I and II) of Y_1, Q_1, and e_1. By substituting the calculated values in Table III into Eq. (4) we are getting the lower bound of the key generation rate per pulse $S \geqslant 9.53\times 10^{-6}$, a low value. Since the total number of pulses sent by Elisabeth (the last active station in the five-user setup) was $N=785$ Mbit the final length of the secret sharing key $L=N\times S$ $=7.48$ kbit. The low value of the lower bound of key generation rate per pulse depends on our choice of the mean photon number μ for signal states. However, our single-decoy state protocol implementation has not aimed to achieve the optimal μ value due to the specific, already mentioned, limitations of our five-user secret sharing setup. For the three- and four-party secret sharing setups the one-state decoy protocol was implemented in the exactly the same way as for the five-party.

VIII. CONCLUSIONS

We have presented a quantum secret sharing experiment in fiber in three, four, and five-party implementations using a single qubit protocol, which makes it possible to implement quantum secret sharing over telecom fiber channels. Our setup measurements have shown that multiparty quantum secret sharing is feasible over telecom fiber networks.

ACKNOWLEDGMENTS

This work was supported by Swedish Defence Material Administration (FMV) and Swedish Research Council (VR). We would also like to thank Johan Ahrens for help with editing this paper.

[1] B. Schneier, *Applied Cryptography* (Wiley, New York, 1996).
[2] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[3] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[4] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[5] Y. A. Chen, A. N. Zhang, Z. Zhao, X. Q. Zhou, C. Y. Lu, C. Z. Peng, T. Yang, and J. W. Pan, Phys. Rev. Lett. **95**, 200502 (2005).
[6] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).
[7] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[8] G. P. He, Phys. Rev. Lett. **98**, 028901 (2007).
[9] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **98**, 028902 (2007).
[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[11] M. Martinelli, Opt. Commun. **72**, 341 (1989).
[12] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 517 (2000).
[13] M. Bourennane *et al.*, Opt. Express **4**, 383 (1999).
[14] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[15] X. B. Wang, Phys. Rev. A **75**, 052301 (2007).
[16] X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A **72**, 012326 (2005).
[17] Y. Zhao, B. Qi, X. Ma, H. K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[18] H.-K. Lo, in *Proceedings of the International Symposium on Information Theory (ISIT)* (IEEE Press, Chicago, 2004), p. 137; H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[19] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[20] G. Brassard, L. Salvail, in *Advances in Cryptology EUROCRYPT '93*, (Springer-Verlag, Berlin, 1993).
[21] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).