npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Experimental quantum multiparty communication protocols

Massimiliano Smania[1,2], Ashraf M Elhassan[1,2], Armin Tavakoli[1] and Mohamed Bourennane[1]

Quantum information science breaks limitations of conventional information transfer, cryptography and computation by using quantum superpositions or entanglement as resources for information processing. Here we report on the experimental realisation of three-party quantum communication protocols using single three-level quantum system (qutrit) communication: secret-sharing, detectable Byzantine agreement and communication complexity reduction for a three-valued function. We have implemented these three schemes using the same optical fibre interferometric setup. Our realisation is easily scalable without compromising on detection efficiency or generating extremely complex many-particle entangled states.

npj Quantum Information (2016) **2,** 16010; doi:10.1038/npjqi.2016.10; published online 21 June 2016

INTRODUCTION

Many tasks in communications, computation and cryptography can be enhanced beyond classical imitations by using quantum resources. Such quantum technologies often rely on distributing strongly correlated data that cannot be reproduced with classical theory: i.e., it violates a Bell inequality.[1] To violate a Bell inequality, the parties involved in the scheme must share an entangled quantum state on which they perform suitable local measurements returning outcomes that can be locally processed and communicated by classical means. Such entanglement-assisted schemes have been shown to be successful in a wide variety of information-processing tasks, including secret sharing for which additional security features are enabled, detectable Byzantine Agreement for which a classically unsolvable task can be solved and reduction of communication complexity for which optimal classical techniques are outperformed.

Let us shortly introduce these three communication protocols. Secret sharing is a cryptographic primitive that can conceptually be regarded as a generalisation of quantum key distribution.[2,3] Secret-sharing schemes have wide applications in secure multiparty computation and management of keys in cryptography. In such schemes, a message (secret) is divided in shares distributed to recipient parties in such a way that some number of parties must collaborate in order to reconstruct the message. However, the security of classical secret sharing relies on limiting assumptions of the computation power available to an adversary. Quantum cryptography introduces the concept of unconditional security, and it can improve security beyond classical constraints. Quantum secret-sharing protocols have been proposed with parties sharing a multipartite qubit entangled state[4,5] where their security is linked to Bell inequality violations.

A fundamental problem in fault-tolerant distributed computing is to achieve coordination between computer processes in spite of some processes randomly failing because of, e.g., crashing, transmission failure or distribution of incorrect information in the network. For example, such coordination applies to the problem of synchronising the clocks of individual processes in distributed networks, which is pivotal in many technologies including data transfer networks and telecommunication networks. A method to achieve synchronisation is to use interactive consistency algorithms in which all nonfaulty processes reach a mutual agreement about all the clocks.[6] Interactive consistency is achieved through solving the problem of Byzantine agreement, which can be solved only if less than one-third of the processes are faulty.[7] However, for most applications, it is sufficient to consider a scenario called detectable Byzantine agreement (DBA), in which the processes either achieve mutual agreement or jointly exit the protocol. Several quantum protocols based on multipartite entanglement have been proposed for achieving the DBA even in the presence of one-third or more faulty processes, thus breaking the classical limitation.[8–10]

In communication complexity problems (CCPs), separated parties perform local computations and exchange information in order to accomplish a globally defined task, which is impossible to solve single-handedly. Here we consider the situation in which one would like to maximise the probability of successfully solving a task with a restricted amount of communication.[11] Such studies aim, for example, at speeding up a distributed computation by increasing the communication efficiency, or at optimising VLSI circuits and data structures.[12] Quantum protocols involving multipartite entangled states have been shown to be superior to classical protocols for a number of CCPs.[13,14]

Quantum multiparty communication protocols that require only sequential communication of single qubits and no shared multipartite entanglement have been proposed for secret sharing[15] and CCP,[16] and CCP using the quantum Zeno effect.[17] Very recently, generalisations to *d*-level quantum system (called a qudit) have been proposed. These protocols are multiparty quantum secret-sharing[18] and a quantum solution to the DBA, which can then be used to achieve clock synchronisation in the presence of an arbitrary number of faulty processes by efficient classical means of communications.[19] Besides experimentally realising these protocols, we propose and demonstrate a new single-qudit protocol for a multiparty CCP, which outperforms any classical counterpart. Although the mentioned information-processing tasks cover very different topics, such as cryptography, synchronisation and communication complexity, we will show that the quantum schemes that distribute these correlated data

[1]Department of Physics, Stockholm University, Stockholm, Sweden.
Correspondence: M Bourennane (boure@fysik.su.se)
[2]These authors contributed equally to this work.
Received 17 August 2015; revised 17 November 2015; accepted 27 January 2016

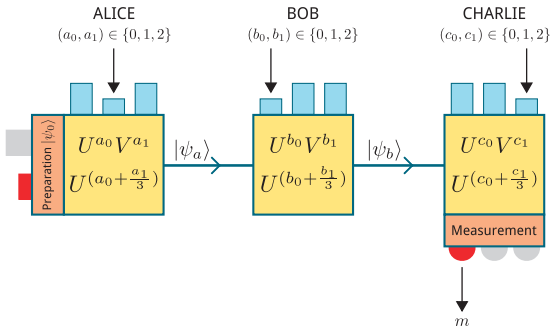

Figure 1. Schematic illustration for the three single-qutrit three-party communication protocols. Alice prepares state $|\psi\rangle$, Alice, Bob and Charlie act with the operation U^iV^j sequentially on the received state according to their input data (i, j), where (i, j) are (a_0, a_1), (b_0, b_1) and (c_0, c_1) for Alice, Bob and Charlie, respectively. Finally, Charlie performs a measurement on the qutrit in the Fourier basis.

sets uphold strong similarities and the differences emerge from the classical processing of the correlated data required to execute these protocols.

Our single-qudit communication protocols hold several experimental advantages in scalability over the corresponding entanglement-assisted schemes. Although entanglement-assisted protocols typically require the preparation of a high-fidelity N-partite d-level entangled quantum state, the single-qudit protocols earn their name from requiring only the preparation of a single-qudit independently of the number of parties, N, involved in the protocol. Furthermore, in the likely case of parties using non-ideal detectors with efficiencies $\eta \in [0, 1]$, entanglement-assisted protocols require N detections and therefore succeed with an exponentially decreasing probability, approximately η^N, whereas single-qudit protocols only require a single detection, which succeeds with probability η, independently of N.

RESULTS

Communication protocols

In this report, we will present for the first time the experimental realisation of quantum communication protocols, secret sharing, DBA and clock synchronisation, and reduction of communication complexity in a multipartite setting involving three parties, Alice, Bob and Charlie, communicating three-level quantum states (qutrits). We will now very briefly present these protocols.

Secret sharing

Alice (a.k.a. the distributor) prepares the initial qutrit state $|\psi\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$ and applies her action $U^{a_0}V^{a_1}$ on the state $|\psi\rangle$ according to her input data (a_0, a_1), where a_0 and a_1 are two pseudorandom independent numbers and the operators U and V are given by

$$U = |0\rangle\langle 0| + e^{\frac{2\pi i}{3}}|1\rangle\langle 1| + e^{-\frac{2\pi i}{3}}|2\rangle\langle 2| \quad (1)$$

$$V = |0\rangle\langle 0| + e^{\frac{2\pi i}{3}}|1\rangle\langle 1| + e^{\frac{2\pi i}{3}}|2\rangle\langle 2| \quad (2)$$

Then, she sends the qutrit to Bob, who according to his input data (b_0, b_1) acts on the qutrit with operator $U^{b_0}V^{b_1}$, and sends the state to Charlie who acts on the qutrit with operator $U^{c_0}V^{c_1}$, where (c_0, c_1) are his input data. Finally, Charlie performs a measurement on the qutrit in the Fourier basis $\{\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{3}}(1, e^{\frac{2\pi i}{3}}, e^{-\frac{2\pi i}{3}}), \frac{1}{\sqrt{3}}(1, e^{-\frac{2\pi i}{3}}, e^{\frac{2\pi i}{3}})\}$, obtaining a trit outcome m (Figure 1). In random order, the parties then announce their data a_1, b_1, c_1 and if condition $a_1+b_1+c_1 = 0$ *mod*3 is verified the round is treated as valid and equation $a_0+b_0+c_0 = 0$ *mod*3 produces the shared secret. Otherwise, if $a_1+b_1+c_1 \neq 0$ *mod*3, the qutrit is not in an eigenstate of the measurement operator at the time of measurement. Thus, the outcome m is random and the run is discarded. At this point, all users should publicly announce a_0, b_0 and c_0 for a relevant number of runs and estimate the quantum trit error rate (QTER) defined as QTER = number of incorrect outcomes/total number of outcomes. Finally, to reconstruct the shared secret, at least two users are required to collaborate.[18]

Secret-sharing schemes can be subjected not only to eavesdropping attacks but also to attacks from parties within the scheme. Examples are known in which such attacks can breach the security of secret-sharing schemes.[20] In the Supplementary Material, we outline a scheme enforcing security that can, at the cost of a lower efficiency, arbitrarily minimise the impact of such attacks. Furthermore, we mention that the full security can be obtained from device-independent implementations of entanglement-based quantum key distribution.[21] However, to our knowledge, there are no device-independent protocols for secret sharing. In our proposed protocol, we assume that the users have control over the devices.

Detectable Byzantine agreement

To solve the DBA problem, the three processes (i.e., parties) need to share the data in the form of lists l_k of numbers subject to specific correlations, and the distribution must be such that the list l_k held by process P_k is known only to P_k, where $k = 1, 2, 3$. Quantum mechanics provides methods to generate and securely distribute such data. In this case, Alice's state preparation and each user's action are the same as in the previous protocol, except for b_0 and c_0 being bits instead of trits. The difference is in the data processing part: if the measurement outcome is '0', the parties reveal a_1, b_1, c_1, and if condition $a_1+b_1+c_1 = 0$ *mod*3 is satisfied, the round is treated as valid. It follows that they now hold one of the data sets $\{(a_0, b_0, c_0) \in (0, 0, 0), (1, 1, 1), (2, 1, 0), (2, 0, 1)\}$ from which the DBA can be solved.[19]

Communication complexity reduction

In the single-qutrit protocol for reducing communication complexity, the distributor supplies Alice, Bob and Charlie with two pseudorandom trits each: (a_0, a_1), (b_0, b_1) and (c_0, c_1). Each party's pair can be mapped into an integer by defining $S_x \equiv 3x_0+x_1 \in \{0, \ldots, 8\}$, with $x \in \{a, b, c\}$. The distributor promises the parties that $S_a+S_b+S_c = 0$ *mod*3 and asks Charlie to guess the value of function

$T = (S_a+S_b+S_c \ mod 9)/3$ given that only two (qu)trits may be communicated in total. After the $|\psi\rangle$ state preparation, Alice acts with $U^{\frac{S_a}{3}}$ (with U defined as in Equation (1)) and sends the qutrit to Bob, who applies $U^{\frac{S_b}{3}}$ before forwarding it to Charlie. Finally, after applying $U^{\frac{S_c}{3}}$ Charlie performs a measurement on the resulting state $|\psi_{final}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + e^{\frac{2\pi i T}{3}}|1\rangle + e^{-\frac{2\pi i T}{3}}|2\rangle)$. This state is an element of the Fourier basis, so a measurement in this basis will output the correct value of function T with (ideally) unit probability.

The CCP is to maximise the success probability of guessing T correctly, with the given communication restrictions. We have just seen that this success probability, save for experimental errors, is 100% with our quantum protocol. However, it can be shown (Supplementary Material) that the optimal classical protocol achieves only a success probability of $7/8 \approx 0.778$, which is clearly inferior to that of the quantum protocol.

Each protocol setting was run 100,000 times per second (i.e., 10^5 laser triggers), and the collected data were used to calculate the *QTER*. Because of the substantial loss from the setup itself (mainly in the phase modulators) and to the 20% detection efficiency, the final amount of runs with detection was 400 per setting. Our results for secret sharing and DBA experiments are reported in Tables 1 and 2.

Table 1. Results for the secret-sharing protocol

Alice		*Bob*		*Charlie*		*m*	*Counts*			*QTER (%)*
a_0	a_1	b_0	b_1	c_0	c_1		D_1	D_1	D_2	
0	0	0	0	2	0	2	7	5	210	5.41
1	0	0	0	1	0	2	7	6	261	4.74
2	0	2	1	2	2	0	375	15	26	9.86
0	1	2	2	1	0	0	391	10	29	9.07
1	1	0	1	2	1	0	336	7	23	8.20
2	1	1	1	1	1	1	7	373	22	7.21
0	2	2	0	0	1	2	16	13	313	8.48
1	2	2	2	2	2	2	19	8	248	9.82
2	2	1	0	1	1	1	9	284	22	9.84
1	0	0	2	2	0	Random	102	98	94	65.31
2	2	0	0	0	0	Random	89	75	71	62.13

Abbreviation: QTER, quantum trit error rate.

Table 2. Results for the DBA protocol

Alice		*Bob*		*Charlie*		*m*	*Counts*			*QTER (%)*
a_0	a_1	b_0	b_1	c_0	c_1		D_1	D_1	D_2	
0	0	1	0	1	0	2	16	11	337	7.42
1	0	0	0	0	0	1	16	320	19	9.86
2	0	1	0	0	0	0	347	13	20	8.68
0	1	0	1	0	1	0	363	13	20	8.33
1	1	1	1	0	1	2	11	17	333	7.76
2	1	0	1	1	1	0	309	9	13	6.65
0	2	1	1	0	0	1	7	277	19	8.58
1	2	0	2	1	2	2	9	18	274	8.97
2	2	1	2	0	2	0	300	7	26	9.91

Abbreviation: QTER, quantum trit error rate.

We can easily see that *QTER* for the secret-sharing and DBA protocols are always below 10%. Our results are better than other results obtained with entanglement-based two-party quantum key distribution protocols,[22] and *QTERs* clearly are below the 15.95% security threshold of qutrit-based quantum key distribution.[23] Therefore, secure communication can be obtained with this configuration.[18] Consistently, CCP experimental results, of which a sample of obtained data is reported in Table 3, show success probabilities always above 90%, thus proving the superiority of the quantum protocol to any classical protocol (limited to 77.8% success probability). The primary source of *QTER* is the so-called 'dark counts'. Our detectors' average dark count probabilities, measured with 10^6 runs, are 5.9 10^{-5}, 2.8 10^{-5} and 20.5 10^{-5} per trigger for detectors D_0, D_1 and D_2, respectively. Considering our measurements, these dark counts contribute up to half of the *QTER*.

Other important systematic contributions to the QTER are because of the phase drift affecting the interferometer. This phase drift causes two problems: it slightly changes the relative phases from the desired settings and it forces a recalibration of the phases before each experiment. Both these contributions can be quantified by propagating phase errors in interference equations (Supplementary Material) to be ~1% each to QTERs.

DISCUSSION

For future and practical implementations of these communication protocols, one needs to use a bright true or heralded single-photon source, integrated optics interferometer and high quantum efficiency superconducting single-photon detectors.

Table 3. Results for the communication complexity reduction protocol

Alice	*Bob*	*Charlie*		*Counts*			*SP [%]*
S_a	S_b	S_c	T	D_1	D_1	D_2	
0	1	8	0	350	7	28	90.91
0	2	1	1	8	284	23	92.53
1	5	0	2	14	14	255	90.11
1	6	2	0	337	5	29	90.84
2	7	3	1	13	268	16	90.24
2	0	4	2	10	2	204	94.44
3	2	4	0	302	8	22	90.96
3	1	8	1	8	358	22	92.27
4	8	3	2	10	13	269	92.12
4	5	0	0	332	12	21	90.96
5	6	1	1	21	370	19	90.24
5	4	6	2	14	18	297	90.27
6	2	1	0	298	3	28	90.30
6	8	7	1	6	297	18	92.52
7	3	5	2	6	13	232	92.43
7	0	2	0	264	12	12	91.67
8	2	2	1	7	385	31	90.40
8	8	8	2	13	11	229	90.51

We have experimentally realised three-party quantum communication protocols using single-qutrit communication: secret sharing; detectable Byzantine agreement; and communication complexity reduction for a three-valued function. We have implemented for the first time these three protocols using the same optical fibre interferometric setup. Our novel protocols are based on single quantum system communication rather than entanglement. Moreover, the number of detectors (detector noise) used in our schemes is independent of the number of parties participating in the protocol. Our realisation is easily scalable without compromising on detection efficiency or generating extremely complex many-particle entangled states. These breakthrough and advances make multiparty communication tasks feasible. They become technologically comparable to quantum key distribution, which is so far the only commercial application of quantum information. Finally, our methods and techniques can be generalised to other communication protocols. These protocols can also be easily adapted for other encodings and physical systems.

MATERIALS AND METHODS

We have realised the three above-mentioned communication protocols with the same optical setup reported in Figure 2. The setup is based on a three-arm Mach–Zehnder-like interferometer built with optical fibres and a retro-reflective mirror (this configuration is a practical solution to the natural phase-drift problem, which affects every Mach–Zehnder interferometer, further complicated here by the fact that we have three paths). The information transmitted between users is encoded in relative phase differences between the three states constituting the qutrit. The state preparation is carried out by sending light pulses from a 1,550- nm diode laser (ID300 by ID Quantique) to the first 3×3 coupler of the Mach–Zehnder interferometer.

The laser repetition rate is 100 kHz. The outcome after the second coupler is a superposition of the three paths, so that the optical phase of each pulse of the qutrit can be individually modulated with commercial phase modulators (COVEGA Mach-10 Lithium Niobate Modulators). The delays in the interferometer are $\Delta L_M = 68.40 \pm 0.05$ ns and $\Delta L_L = 136.80 \pm 0.05$ ns. On the way to the mirror, users passively let the qutrit pass through while after the reflection Charlie, Bob and Alice sequentially act on the qutrit with a combination of operators U and V (see Equations (1) and (2)). After passing through the three arms on their way back, the three pulses recombine at the first coupler, and depending on

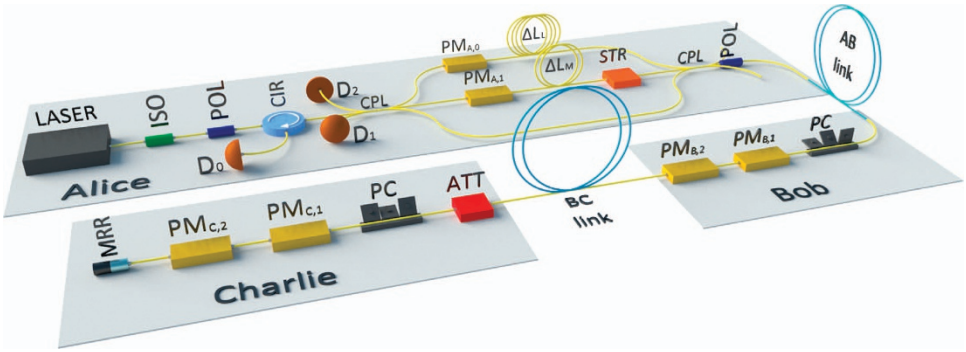

Figure 2. Experimental setup used in this work. The components are isolator (ISO), polarisers (POL), circulator (CIR), two 3×3 fibre couplers (CPL), phase modulators (PM), fibre stretcher (STR), polarisation controllers (PC), variable digital attenuator (ATT), retro-reflective mirror (MRR) and three single-photon avalanche detectors (D_0, D_1, D_2). The three parties' stations are polarisation maintaining, whereas the links connecting them are single-mode fibres. respectively.

their relative phases they yield different interference counts at the single-photon detectors (Princeton Lightwaves PGA600). These gated detectors provide 20% quantum efficiency and $\sim10^{-5}$ dark count probability. Importantly, in order to prevent possible eavesdropping attacks, each pulse is attenuated to the single-photon level by a digital variable attenuator (OZ Optics DA-100) at Charlie's station output.

We would like to emphasise that phase modulators are polarisation sensitive, and for this reason they include a horizontal polariser at the output port. Therefore, controlling polarisation throughout the setup is crucial. We thus choose to use polarisation-maintaining fibre components for all three parties' stations.

However, in order to make the configuration more realistic, links between users are standard single-mode fibres. Therefore, polarisation controllers have been placed after these fibre links. Finally, the whole experiment was controlled by an FPGA card that worked both as master clock and trigger source, for the electronics driving laser and phase modulators and for the single-photon detectors.

ACKNOWLEDGEMENTS

We thank Marek Żukowski and Adan Cabello for useful discussions. This work was supported by the Swedish Research Council, Knut and Alice Wallenberg Foundation, and ERC Advanced grand QOPLAPS.

CONTRIBUTIONS

M.B. initiated and proposed the project. M.S .and A.M.E. designed, performed the experiment and analysed the data. A.T. carried out the theoretical calculation for the CCP and scheme enforcing security of secret-sharing protocols. All the authors discussed the results and wrote the manuscript.

COMPETING INTERESTS

The authors declare no conflict of interest.

REFERENCES

1. Bell, J. S. On the Einstein-Podolsky-Rosen paradox. *Physics* **1**, 195–200 (1966).
2. Bennett, C. H. & Brassard, G. in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* 175–179 (Bangalore, India, 1984).
3. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
4. Żukowski, M., Zeilinger, A., Horne, M. A. & Weinfurter, H. Quest for GHZ states. *Acta Phys. Pol.* **93**, 187–195 (1998).
5. Hillery, M., Bûzek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999).
6. Lamport, L. & Melliar-Smith, M. Synchronizing clocks in the presence of faults. *J. ACM* **32**, 52–78 (1985).
7. Lamport, L., Shostak, R. & Pease, M. The Byzantine generals problem. *ACM Trans. Program. Lang. Syst.* **4**, 382–401 (1982).
8. Fitzi, M., Gisin, N. & Maurer, U. A quantum solution to the Byzantine agreement problem. *Phys. Rev. Lett.* **87**, 217901–217901 (2001).
9. Cabello, A. Solving the liar detection problem using the four-qubit singlet state. *Phys. Rev. A* **68**, 012304 (2003).
10. Gaertner, S., Bourennane, M., Kurtsiefer, C., Cabello, A. & Weinfurter, H. Experimental demonstration of a quantum protocol for Byzantine Agreement and Liar Detection. *Phys. Rev. Lett.* **100**, 070504 (2008).
11. Yao, A. C.-C. in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* 209–213 (Atlanta, GA, USA, 1979).
12. Kushilevitz, E. & Nisan, N. *Communication Complexity* (Cambridge Univ. Press, 1997).
13. Cleve, R. & Buhrman, H. Substituting quantum entanglement for communication. *Phys. Rev. A* **56**, 1201–1204 (1997).
14. Brukner, C., Żukowski, M. & Zeilinger, A. Quantum communication complexity protocol with two entangled qutrits. *Phys. Rev. Lett.* **89**, 197901–197901 (2002).
15. Schmid, C. *et al.* Experimental single qubit quantum secret sharing. *Phys. Rev. Lett* **95**, 230505 (2005).
16. Trojek, P. *et al.* Experimental quantum communication complexity. *Phys. Rev. A* **72**, 050305 (2005).
17. Tavakoli, A., Anwer, H., Hameedi, A. & Bourennane, M. Quantum communication complexity using the quantum Zeno effect. *Phys. Rev. A* **92**, 012303 (2015).
18. Tavakoli, A., Herbauts, I., Żukowski, M. & Bourennane, M. Quantum secret sharing with a single d-level system. *Phys. Rev. A* **92**, 30302 (2015).
19. Tavakoli, A., Cabello, A., Żukowski, M. & Bourennane, M. Quantum clock synchronization with a single qudit. *Sci. Rep.* **5**, 7982 (2015).
20. He, G. P. Comment on experimental single qubit quantum secret sharing. *Phys. Rev. Lett.* **98**, 028901–028901 (2007).
21. Acin, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501–230501 (2007).
22. Gröblacher, S., Jennewein, T., Vaziri, A., Weihs, G. & Zeilinger, A. Experimental quantum cryptography with qutrits. *New J. Phys.* **8**, 75 (2006).
23. Cerf, N., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).

Supplemental Information accompanies the paper on the *npj Quantum Information* website (http://www.nature.com/npjqi)