Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System

Nanyang Xu,[1] Jing Zhu,[1,2] Dawei Lu,[1] Xianyi Zhou,[1] Xinhua Peng,[1,*] and Jiangfeng Du[1,†]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui, 230026, China*

[2]*Department of Physics Shanghai Key Laboratory for Magnetic Resonance, East China Normal University Shanghai 200062*

(Received 13 November 2011; published 30 March 2012)

Quantum algorithms could be much faster than classical ones in solving the factoring problem. Adiabatic quantum computation for this is an alternative approach other than Shor's algorithm. Here we report an improved adiabatic factoring algorithm and its experimental realization to factor the number 143 on a liquid-crystal NMR quantum processor with dipole-dipole couplings. We believe this to be the largest number factored in quantum-computation realizations, which shows the practical importance of adiabatic quantum algorithms.

DOI: 10.1103/PhysRevLett.108.130501 PACS numbers: 03.67.Ac, 03.67.Lx, 76.60.−k

Multiplying two integers is often easy while its inverse operation—decomposing an integer into a product of two unknown factors—is hard. In fact, no effective methods in classical computers is available now to factor a large number which is a product of two prime integers [1]. Based on this lack of factoring ability, cryptographic techniques such as RSA have ensured the safety of secure communications [2]. However, Shor proposed his famous factoring algorithm [3] in 1994 which could factor a larger number in polynomial time with the size of the number on a quantum computer. Early experimental progresses have been done to demonstrate the core process of Shor's algorithm on liquid-state NMR [4] and photonic systems [5,6] for the simplest case—the factoring of number 15.

While traditional quantum algorithms including Shor's algorithm are represented in circuit model, i.e., computation performed by a sequence of discrete operations, a new kind of quantum computation based on the adiabatic theory was proposed by Farhi *et al.* [7] where the system was driven by a continuously-varying Hamiltonian. Unlike circuit-based quantum algorithms, adiabatic quantum computation (AQC) is designed for a large class of optimization problems—problems to find the best one among all possible assignments. Moreover, AQC shows a better robustness against error caused by dephasing, environmental noise and imperfection of unitary operations [8,9]. Thus it has grown up rapidly as an attractive field of quantum-computation research.

Several computational hard problems have been formulated as optimization problems and solved in the architecture of AQC, for example, the three-satisfiabilty problem, Deutsch's problem, and quantum database search [7,10–15]. Recently Peng *et al.* [16] have adopted a simple scheme to solve the factoring problem in AQC and implemented it on a liquid-state NMR system to factor the number 21. However, this scheme could be very hard for large applications due to the exponentially-growing spectrum width of the problem Hamiltonian. At the same time, another adiabatic factoring scheme provided by Schaller and Schützhold [17] could suppress the spectrum width and shows to be much faster than classical factoring algorithms or even an exponential speed-up.

However, Schaller and Schützhold's original factoring scheme is too hard to be implemented for any nontrival factoring cases on current quantum processors. In this Letter, we improve the original scheme to use less resources by simplifying the equations mathematically. And a factoring case of 143 is chosen as an example to be resolved in this scheme and finally experimentally implemented on a liquid-crystal NMR system with dipolar couplings. We believe this to be the largest number factored on quantum-computation realizations.

As mentioned before, AQC was originally proposed to solve the optimization problem. Because the solution space of an optimization problem grows exponentially with the size of problem, to find the best one is very hard for the classical computers when the problem's size is large. In the framework of AQC, a quantum system is prepared in the ground state of initial Hamiltonian H_0, while the possible solutions of the problem is encoded to the eignestates state of problem Hamiltonian H_p and the best solution to its ground state. For the computation, the time-dependent Hamiltonian varies from H_0 to H_p, and if this process performs slowly enough, the quantum adiabatic theorem will ensure the system stays in its instantaneous ground state. So in the end, the system will be in the ground state of H_p which denotes the best solution of the problem. Simply the time-dependent Hamiltonian is realized by an interpolation scheme

$$H(t) = [1 - s(t)]H_0 + s(t)H_P, \tag{1}$$

where the function $s(t)$ varies from 0 to 1 to parametrize the interpolation. The solution of the optimization problem could be determined by an measurement of the system after the computation.

 © 2012 American Physical Society

Here, the factoring problem is expressed as a formula $N = p \times q$, where N is the known product while p and q are the prime factors to be found. The key part of adiabatic factoring algorithm is to convert the factoring problem to an optimization problem, and solve it under the AQC architecture. The most straightforward scheme is to represent the formula as an equation $N - pq = 0$ and form a cost function $f(x, y) = (N - xy)^2$, where $f(x, y)$ is a nonnegative integer and $f(p, q) = 0$ is the minimal value of the function. The problem Hamiltonian H_p could be constructed with the same form of $f(x, y)$, i.e., $H_p = [N - \hat{x} \times \hat{y}]^2$. Here, operator $\hat{x}$ is formed by $\sum_{i=0}^{n-1} 2^i(\frac{1-\sigma_z^i}{2})$ where n is the bit-width of variable x and σ_z^i is the σ_z operator on the qubit which represents the ith bit of x, and operator $\hat{y}$ is formed likewise from y. Thus the ground state of H_p has the zero energy which denotes the case that $N = xy$. After the adiabatic evolution and measurement, we could get the result p and q. Peng *et al.* [16] have implemented this scheme experimentally to factor 21. However in this scheme, the spectrum of problem Hamiltonian scales with the number N, thus it is very hard to implement in experiment when N is large.

To avoid this drawback, Schaller and Schützhold [17] adopted another scheme by Burges [18] to map the factoring problem to an optimization problem. Their adiabatic factoring algorithm starts with a binary-multiplication table which is shown in Table I. In the table, p_i and q_i in the first two rows represent the bits of the multipliers and the following four rows are the intermediate results of the multiplication and z_{ij} are the carries from ith bit to the jth bit. The last row is the binary representation of number N to be factorized. In order to get a nontrivial case, we set N to be odd, thus the last bit (i.e., the least significant bit) of multipliers is binary value 1. The bit-width of N equals the summation of p's and q's width. So the number of combinations of p's and q's width is bounded with $\frac{n}{2}$. For a complete realization, $\frac{n}{2}$ times of factorization should be tried for the different combinations. Here we just demonstrate an example case where p and q has the same width and set each factor's first bit (i.e., most significant bit) to be 1. In a realistic problem, the width of p or q could not be known *a priori*. Thus one need to verify the answer (i.e., $pq = N$, which cost polynomial time) of each try until the solution is found. Note that these tries will not increase the time complexity of the quantum factorization algorithm.

TABLE I. Binary-multiplication table. The top two rows are binary representations of the multipliers whose first and last bit are set to be 1. The bits in the bottom row shows the product number which in our example is 143. z_{ij} is the carry bit from the ith bit to the jth bit in the summation. The significance of each bit in the column increases from right to left (i.e., from b_0 to b_7).

	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Multiplier					1	p_2	p_1	1
					1	q_2	q_1	1
Binary-multiplication					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
Carry	z_{67}	z_{56}	z_{45}	z_{34}	z_{23}	z_{12}		
	z_{57}	z_{46}	z_{35}	z_{24}				
Product	1	0	0	0	1	1	1	1

Then, the factoring equations could be got from each column in Table I, where all the variables p_i, q_i, z_{ij} in the equations are binary. To construct the problem Hamiltonian, first we construct bitwise Hamiltonian for each equation by directly mapping the binary variables to operators on qubits. For example, the equation got from b_1 column is $p_1 + q_1 = 1 + 2z_{12}$ and the generated Hamiltonian is $H_p^1 = (\hat{p}_1 + \hat{q}_1 - 1 - 2\hat{z}_{12})^2$, where each of the operator $\hat{p}_1$, $\hat{q}_1$ or $\hat{z}_{12}$ is formed as $\frac{1-\hat{\sigma}_z}{2}$ on a qubit representing each variable. Then the problem Hamiltonian $H_p = \sum H_p^i$ is a summation of all the bitwise Hamiltonians. In this way, the ground state of H_p encodes the two factors that satisfy all the bitwise equations and is the answer to our factoring problem. Thus the spectrum of H_p will not scale with N but $\log_2 N$.

However, Schaller and Schützhold's scheme [17] need at least 14 qubits to factor the number 143, which exceeds the limitation of current quantum-computation technology. So before our experiment, we introduce a classical method to reduce the variables in the equations. For example, because each of the variables should be 0 or 1, two more equations $z_{12} = 0$ and $p_1 p_2 = 0$ could be induced from the equation $p_1 + q_1 = 1 + 2z_{12}$. By applying similar judgements, we can get a simplified group of equations, which are: $p_1 + q_1 = 1$, $p_2 + q_2 = 1$ and $p_2 q_1 + p_1 q_2 = 1$. For general cases, Schaller and Schützhold's original scheme [17] need $O(n\log_2 n)$ qubits for factorization, while this simplification could reduce all the carry variables at the best situation and required polynomial operations (i.e., is efficient), where n is the bit-width of the factorized number N. The detailed analysis to this simplification is in the supplementary information.

To construct the problem Hamiltonian from this simplified equations, the bitwise Hamiltonians are constructed by $H_p^1 = (\hat{p}_1 + \hat{q}_1 - 1)^2$, $H_p^2 = (\hat{p}_2 + \hat{q}_2 - 1)^2$ and $H_p^3 = (\hat{p}_2\hat{q}_1 + \hat{p}_1\hat{q}_2 - 1)^2$. But this construction method causes H_p^3 to have a four-body interactions, which is hard to be implemented experimentally. In this case, Schaller and Schützhold [17] introduced another construction form that for the equation like $AB + S = 0$, the problem Hamiltonian could be constructed by $2[\frac{1}{2}(\hat{A} + \hat{B} - \frac{1}{2}) + \hat{S}]^2 - \frac{1}{8}$, which could reduce one order of the many-body interactions in experiment. Thus we replace the third bitwise Hamiltonian as $H_p'^3 = 2[\frac{1}{2}(\hat{p}_1 + \hat{q}_2 - \frac{1}{2}) + \hat{p}_2\hat{q}_1 - 1]^2 - \frac{1}{8}$. So the problem Hamiltonian is,

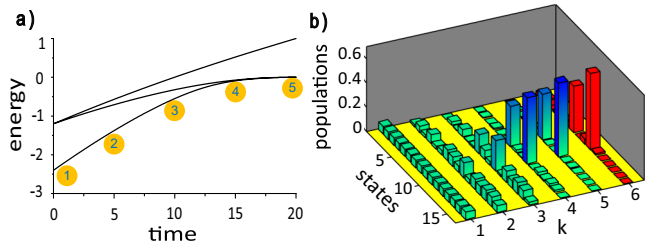

FIG. 1 (color online). Process of the adiabatic factorization of 143. (a) the lowest three energy levels of the time-dependent Hamiltonian in Eq. (1), The parameter g in the initial Hamiltonian is 0.6. (b) $k = 1$–5 shows the populations on computational basis of the system during the adiabatic evolution at different times marked in a); $k = 6$ shows the result got from our experiment. The experimental result agrees well with the theoretical expectation. The system finally stays on a superposition of $|6\rangle$ and $|9\rangle$, which denotes that the answer is $\{p = 11, q = 13\}$ or $\{p = 13, q = 11\}$.

$$H_p = 5 - 3\hat{p}_1 - \hat{p}_2 - \hat{q}_1 + 2\hat{p}_1\hat{q}_1 - 3\hat{p}_2\hat{q}_1 + 2\hat{p}_1\hat{p}_2\hat{q}_1 - 3\hat{q}_2 + \hat{p}_1\hat{q}_2 + 2\hat{p}_2\hat{q}_2 + 2\hat{p}_2\hat{q}_1\hat{q}_2,$$

where the operators $\hat{p}$ and $\hat{q}$ are mapped into the qubits' space as $\hat{p}_1 = \frac{1-\sigma_z^1}{2}$, $\hat{p}_2 = \frac{1-\sigma_z^2}{2}$, $\hat{q}_1 = \frac{1-\sigma_z^3}{2}$ and $\hat{q}_2 = \frac{1-\sigma_z^4}{2}$.

For the adiabatic evolution, without the loss of generality, we choose the initial Hamiltonian $H_0 = g(\sigma_x^1 + \sigma_x^2 + \cdots + \sigma_x^n)$ where g is a parameter to scale the spectrum of H_0. And the ground state of the operator is $|\psi_i\rangle = (\frac{|0\rangle - |1\rangle}{\sqrt{2}})^{\otimes n}$- a superposition of all the possible states. So for the computation, we prepare the system on the state $|\psi_i\rangle$ with the Hamiltonian being H_0, and slowly vary the Hamiltonian from H_0 to H_p according to Eq. (1), the quantum adiabatic theorem ensures that the system will be at the ground state of H_p, which represents the answer to the problem of interests.

We numerically simulate the process of factoring 143 as shown in Fig. 1. Specially, the ground state of the problem Hamiltonian in Eq. (2) is degenerated. This is because two multipliers p and q have the same bit-width, thus an exchange of p and q also denotes the right answer. From the simulation, we could see that the prime factors of 143 is 11 and 13.

Now we turn to our NMR quantum processor to realize the above scheme of factoring 143. The four qubits are represented by the four ^{1}H nuclear spins in 1-bromo-2-chlorobenzene (C_6H_4ClBr) which is dissolved in the liquid-crystal solvent ZLI-1132 (Merck) at temperature 300 K. The structure of the molecule is shown in Fig. 2(a) and the four qubits are marked by the ovals. By fitting the thermal equilibrium spectrum in Fig. 2(b), the natural Hamltonian of the four-qubit system in the rotating frame is

$$\mathcal{H} = 2\pi\sum_i \nu_i I_z^i + 2\pi \sum_{i,j,i<j} J_{ij} I_z^i I_z^j + 2\pi \sum_{i,j,i<j} D_{ij}(2I_z^i I_z^j - I_x^i I_x^j - I_y^i I_y^j), \quad (2)$$

where the chemical shifts $\nu_1 = 2264.8$ Hz, $\nu_2 = 2190.4$ Hz, $\nu_3 = 2127.3$ Hz, $\nu_4 = 2113.5$ Hz, the dipolar

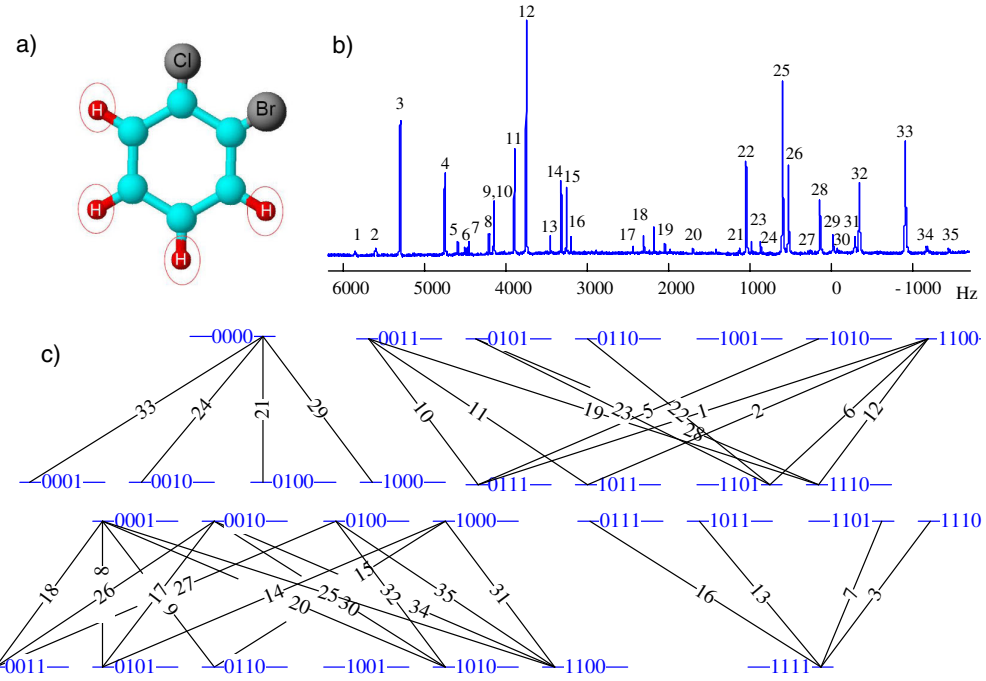

FIG. 2 (color online). Quantum register in our experiment. (a) The structure of the 1-Bromo-2-Chlorobenzene molecule. The four ^{1}H nuclei in ovals forms the qubits in our experiment. (b) Spectrum of ^{1}H of the thermal state $\rho_{th} = \sum_{i=1}^4 \sigma_z^i$ applying a $[\pi/2]_y$ pulse. Transitions are labeled according to descending order of their frequencies. (c) Labeling scheme for the states of the four-qubit system.

couplings strengths $D_{12} = -706.6$ Hz, $D_{13} = -214.0$ Hz, $D_{14} = -1166.5$ Hz, $D_{23} = -1553.8$ Hz, $D_{24} = -149.8$ Hz, $D_{34} = -95.5$ Hz and the J couplings $J_{12} = 0$ Hz, $J_{13} = 1.4$ Hz, $J_{14} = 8$ Hz, $J_{23} = 8$ Hz, $J_{24} = 1.4$ Hz, $J_{34} = 8$ Hz. The labeling transition scheme for the energy levels is shown in Fig. 2(c).

The whole experimental procedure can be described as three steps: preparation of the ground state of H_0, adiabatic passage by the time-dependent Hamiltonian $H(t)$, and measurement of the final state. Starting from thermal equilibrium, we firstly created the pseudopure state(PPS) $\rho_{0000} = \frac{1-\epsilon}{16}\mathbb{I} + \epsilon|0000\rangle\langle 0000|$, where ϵ describes the thermal polarization of the system and $\mathbb{I}$ is an unit matrix. The PPS was prepared from the thermal equilibrium state by applying one shape pulse based on gradient ascent pulse engineering (GRAPE) algorithm [19] and one z-direction gradient pulse, with the fidelity 99% in the numerical simulation. Figure 3(a) shows the NMR spectrum after a small-angle-flip pulse [20] of state ρ_{0000}. Then one $\frac{\pi}{2}$ hard pulse was applied to ρ_{0000} on the y axis to obtain the ground state of H_0, i.e., $|-\rangle^{\otimes 4}$ ($|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$). More detailed description of the PPS preparation is in the Supplemental Information [21].

In the experiment, the adiabatic evolution was approximated by M discrete steps [13,14,16,20,22]. We utilized the linear interpolation $s(t) = t/T$, where T is the total evolution time. Thus the time evolution for each adiabatic step is $U_m = e^{-iH_m\tau}$ where $\tau = T/M$ is the duration of each step, and $H_m = (1 - \frac{m}{M})H_0 + (\frac{m}{M})H_p$ is the intermediate Hamiltonian of the mth step. And the total evolution applied on the initial state is $U_{\mathrm{ad}} = \prod_{m=1}^{M} U_m$. The adiabatic condition is satisfied when $T, M \to \infty$ [23]. Here we chose the parameters $g = 0.6$, $M = 20$ and $T = 20$. Numerical simulation shows that the probabilities of the system on the ground states of H_p is 98.9%, which means that we could achieve the right answer to the factoring problem of 143 almost definitely. We packed together the unitary operators every five adiabatic steps in one shaped pulse calculated by the GRAPE method [19], with the length of each pulse 15 ms and the fidelity with the theoretical operator over 99%. So the total evolution time is about $T_{\mathrm{tot}} = 60$ ms.

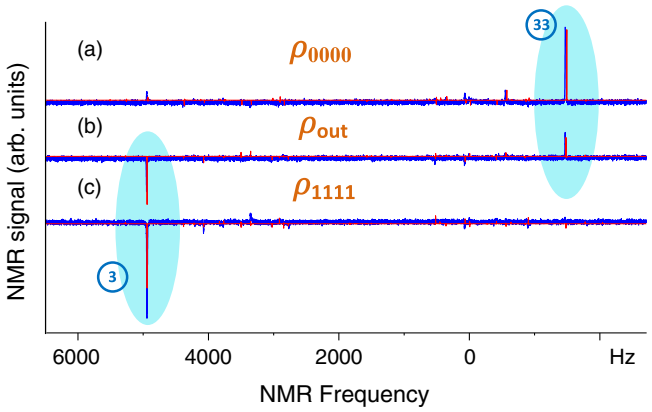

FIG. 3 (color online). NMR spectra for the small-angle-flip observation of the PPS and the output state ρ_{out}, respectively. The blue spectra (thick) are the experimental results, and the red spectra (thin) are the simulated ones. (a) (c) Spectra corresponding to the PPS ρ_{0000} and ρ_{1111} by applying a small-angle-flip (3°) pulse. The main peaks are No. 33 and No. 3 labeled in the thermal equilibrium spectrum. (b) Spectrum corresponding to the output state ρ_{out} after applying a small-angle-flip (3°) pulse, which just consists of the peaks of No. 33 and No. 3.

Finally, we measured all the diagonal elements of the final density matrix ρ_{fin} using the Hamiltonian's diagonalization method [24]. 32 reading out GRAPE pulses for population measurement were used after the adiabatic evolution, with each pulse's length 20 ms. Combined with the normalization condition $\sum_{i=1}^{16} P(i) = 1$, we reconstructed all the diagonal elements of the final state ρ_{fin}. Step $k = 6$ of Fig. 1(b) shows the experimental result of all the diagonal elements excluding the decoherence through compensating the attenuation factor $e^{-T_{\mathrm{tot}}/T_2^*}$, where T_{tot} is the total evolution time 60 ms and T_2^* is the decoherence time 102 ms. The experiment (step $k = 6$) agrees well with the theoretical expectations (step $k = 5$), showing that the factors of 143 is 11 and 13.

On the other hand, to illustrate the result more directly from the NMR experiment, a comprehensible spectrum was also given by applying a small angle flip (3°) after two π operators on the second and third qubit and one gradient pulse,

$$\rho_{\mathrm{out}} = Gz(R_y^{2,3}(\pi)\rho_{\mathrm{fin}}R_y^{2,3}(\pi)^{\dagger}) \tag{3}$$

For the liquid-crystal sample, since the Hamiltonian includes nondiagonal elements, the eigenstates are not Zeeman product states but their linear combinations, except $|0000\rangle$ and $|1111\rangle$. If there just exist two populations $|0000\rangle\langle 0000|$ and $|1111\rangle\langle 1111|$, the spectrum would be comprehensible as containing only two main peaks after a small angle pulse excitation. The motivation of adding the π pulses after the adiabatic evolution is conversing $|0110\rangle\langle 0110|$ and $|1001\rangle\langle 1001|$ to $|0000\rangle\langle 0000|$ and $|1111\rangle\langle 1111|$, while the gradient pulse was used to make the output ρ_{out} concentrated on the diagonal elements of the density matrix. Thus the small-angle-flip observation would be easily compared with ρ_{0000} and ρ_{1111} (Fig. 3), indicating that the factors of 143 is 11 and 13.

To be concluded, we improved the adiabatic factoring scheme and implemented it to factor 143 in our NMR platform. The sample we used for experiment is oriented in the liquid crystal thus it has dipole-dipole coupling interactions which are utilized for the computation. The experimental result matches well with theoretical expectations. To our knowledge, this is the first experimental realization of quantum algorithms to factor a number larger than 100.

The authors thank Dieter Suter for helpful discussions. This work was supported by National Nature Science Foundation of China (Grants Nos. 10834005, 91021005, and 21073171), the CAS, and the National Fundamental Research Program 2007CB925200.

*xhpeng@ustc.edu.cn
†djf@ustc.edu.cn

[1] D. E. Knuth, *The Art of Computer Programming, Seminumerical Algorithms* (Addison-Wesley, Reading, Massachusetts, 1998), Vol. 2.
[2] N. Koblitz, *A Course in Number Theory and Cryptography* (Springer-Verlag, Berlin, 1994).
[3] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, New York, Santa Fe, 1994), p. 124.
[4] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature (London) **414**, 883 (2001).
[5] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **99**, 250504 (2007).
[6] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, Phys. Rev. Lett. **99**, 250505 (2007).
[7] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, Science **292**, 472 (2001).
[8] A. M. Childs, E. Farhi, and J. Preskill, Phys. Rev. A **65**, 012322 (2001).
[9] J. Roland and N. J. Cerf, Phys. Rev. A **71**, 032330 (2005).
[10] J. Roland and N. J. Cerf, Phys. Rev. A **65**, 042308 (2002).
[11] S. Das, R. Kobes, and G. Kunstatter, Phys. Rev. A **65**, 062310 (2002).
[12] N.-Y. Xu, X.-H. Peng, M.-J. Shi, and J.-F. Du, arXiv: quant-ph/08110663.
[13] M. Steffen, W. van Dam, T. Hogg, G. Breyta, and I. Chuang, Phys. Rev. Lett. **90**, 067903/1 (2003).
[14] A. Mitra, A. Ghosh, R. Das, A. Patel, and A. Kumar, J. Magn. Reson. **177**, 285 (2005).
[15] H.-W. Chen, X. Kong, B. Chong, G. Qin, X. Zhou, X. Peng, and J. Du, Phys. Rev. A **83**, 032314 (2011).
[16] X.-H. Peng, Z. Liao, N. Xu, G. Qin, X. Zhou, D. Suter, and J. Du, Phys. Rev. Lett. **101**, 220405 (2008).
[17] R. Schutzhold and G. Schaller, Phys. Rev. A **74**, 060304 (2006); G. Schaller and R. Schutzhold, Quantum Inf. Comput. **10**, 0109 (2010).
[18] C. J. Burges, Microsoft Research, Technical Report No. MSR-TR-2002-83, 2002.
[19] N. Khaneja, T. Reiss, C. Kehlet, T. S. Herbruggen, and S. J. Glaser, J. Magn. Reson. **172**, 296 (2005).
[20] R. Das, T. S. Mahesh, and A. Kumar, Phys. Rev. A **67**, 062304 (2003).X.-H. Peng, J.-F. Du, and D. Suter, Phys. Rev. A **71**, 012307 (2005).
[21] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.108.130501 for details.
[22] J.-F. Du, N. Xu, X. Peng, P. Wang, S. Wu, and D. Lu, Phys. Rev. Lett. **104**, 030502 (2010).
[23] J.-F. Du, L. Hu, Y. Wang, J. Wu, M. Zhao, and D. Suter, Phys. Rev. Lett. **101**, 060403 (2008).
[24] D.-W. Lu, J. Zhu, P. Zou, X. Peng, Y. Yu, S. Zhang, Q. Chen, and J. Du, Phys. Rev. A **81**, 022308 (2010).