nature COMMUNICATIONS

OPEN

ARTICLE

Received 17 May 2012 | Accepted 1 Aug 2012 | Published 4 Sep 2012

DOI: 10.1038/ncomms2043

Blind topological measurement-based quantum computation

Tomoyuki Morimae[1,2,*] & Keisuke Fujii[3,*]

Blind quantum computation is a novel secure quantum-computing protocol that enables Alice, who does not have sufficient quantum technology at her disposal, to delegate her quantum computation to Bob, who has a fully fledged quantum computer, in such a way that Bob cannot learn anything about Alice's input, output and algorithm. A recent proof-of-principle experiment demonstrating blind quantum computation in an optical system has raised new challenges regarding the scalability of blind quantum computation in realistic noisy conditions. Here we show that fault-tolerant blind quantum computation is possible in a topologically protected manner using the Raussendorf–Harrington–Goyal scheme. The error threshold of our scheme is 4.3×10^{-3}, which is comparable to that (7.5×10^{-3}) of non-blind topological quantum computation. As the error per gate of the order 10^{-3} was already achieved in some experimental systems, our result implies that secure cloud quantum computation is within reach.

[1] Controlled Quantum Dynamics Theory Group, Imperial College London, London SW7 2AZ, UK. [2] Laboratoire d'Analyse et de Mathématiques Appliquées, Université Paris-Est Marne-la-Vallée, Marne-la-Vallée Cedex 2 77454, France. [3] Department of Materials Engineering, Science Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan. *These authors contributed equally to this work. Correspondence and requests for materials should be addressed to T.M. (email: morimae@gmail.com).

In classical computing, the problem of ensuring secure communication between a server and a client is highly non-trivial. For example, Abadi *et al.*[1] showed that no NP-hard function can be computed with encrypted data if unconditional security is required, unless the polynomial hierarchy collapses at the third level. Even restricting the security condition to be only computational, the question of the possibility of a fully homomorphic encryption has been a long-standing open question for 30 years[2], and no practical method has been found still. An unconditionally secure fully homomorphic encryption is still an open problem.

On the other hand, in the quantum world, the situation is drastically different. Broadbent *et al.*[3] proposed a quantum protocol, the so-called blind quantum computation[3–8], which uses measurement-based quantum computation (MBQC)[9]. In their protocol, Alice has a classical computer and a quantum device that emits randomly rotated qubits. She does not have any quantum memory. On the other hand, Bob has a fully fledged quantum technology. Alice and Bob share a classical channel and a quantum channel. Their protocol runs as follows. First, Alice sends Bob many randomly rotated qubits and Bob creates a graph state by applying CZ gates among these qubits. Second, Alice instructs Bob how to measure a qubit of the graph state. Third, Bob measures the qubit according to Alice's instruction and he returns the measurement result to Alice. They repeat this classical two-way communication (that is, the second and third steps) until the computation is finished. It was shown[3] that if Bob is honest, Alice can obtain the correct answer of her desired quantum computation (correctness), and that whatever evil Bob does, he cannot learn anything about Alice's input, output and algorithm (blindness). Recently, this protocol has been experimentally demonstrated in an optical system[4].

Secure delegated computation is already in the practical phase for classical computing, including smart phones, encrypted data retrieval[10] and wireless sensor networks[11]. When scalable quantum computers are realized, the need for delegated secure computation must be emphasized, as home-based quantum computers are arguably much more difficult to build than their classical counterparts. To implement blind quantum computation in a scalable manner, it is crucial to protect quantum computation from environmental noise. In this paper, we show that a fault-tolerant blind quantum computation is possible in a topologically protected manner. We also calculate the error threshold, 4.3×10^{-3}, for erroneous preparation of the initial states, erroneous CZ gates, and erroneous local measurements. This is the first time that a concrete fault-tolerant scheme is proposed for blind quantum computation, and that the error threshold is explicitly calculated. Furthermore, this threshold is not so different from that (7.5×10^{-3}) of non-blind topological quantum computation[12,13]. In other words, blind quantum computation is possible with almost the same error threshold as that of the non-blind version. As the error threshold of the order 10^{-3} was already achieved in some experimental systems[14], our result means that secure cloud quantum computation is within our reach. We further show that our protocol is also fault-tolerant against the detectable qubit loss, such as a photon loss and an escape from the qubit energy level.

Results

Topologically protected MBQC. The topologically protected MBQC (TMBQC)[12,13,15] is one of the most promising models of quantum computation. In this model, we first prepare the graph state on the three-dimensional cubic lattice $\mathcal{L}$ whose elementary cell is given in Fig. 1a. We call this lattice $\mathcal{L}$ the Raussendorf–Harrington–Goyal (RHG) lattice. We next measure each qubit of this lattice in X, Z, $T\equiv(X+Y)/\sqrt{2}$, or Y basis. These four types of measurements are sufficient for the universal TMBQC as is shown in refs 12,13. More precisely, measurements in the X and Z basis can simulate the topological braidings of defects in the surface code[16], which can implement the fault-tolerant Clifford gates, and measurements in T basis and Y basis can simulate the preparations of magic states[17], which can implement the non-Clifford gates. These magic states are distilled[17] by topologically protected fault-tolerant Clifford gates, which are simulated by the X and Z basis measurements. A small-size TMBQC has recently been experimentally demonstrated in an optical system[15].

Blind TMBQC. Can we use TMBQC for the blind quantum computation? Obviously, if Bob knows on what basis (X, Z, T or Y) he is doing the measurement on each qubit, he can know Alice's algorithm. However, if Alice can have Bob do the measurements in such a way that Bob cannot know on what basis (X, Z, T, or Y) he is doing the measurement on each qubit, he cannot know Alice's algorithm. How can Alice do that? In fact, such a blind quantum computation is possible if we consider the three-dimensional lattice $\mathcal{L}'$ whose elementary cell is given in Fig. 1b, where two extra qubits are added to each qubit of Fig. 1a. We call this lattice $\mathcal{L}'$ the decorated RHG lattice. The intuitive explanation of our idea is as follows: First, it was shown[3] that Alice can have Bob do the measurement in $\{|0\rangle\pm e^{i\phi}|1\rangle\}$ basis for any $\phi\in\{(k\pi/4)\,|\,k=0,1,...,7\}$ on any qubit of a graph state that Bob has in such a way that Bob cannot learn anything about ϕ. Second, it is easy to confirm that a single-qubit measurement in X, Y, T or Z basis can be simulated on the linear three-qubit cluster state with only $\{|0\rangle\pm e^{i\phi}|1\rangle\}$ basis measurements (Fig. 2). By combining these two facts, we notice that if we decorate

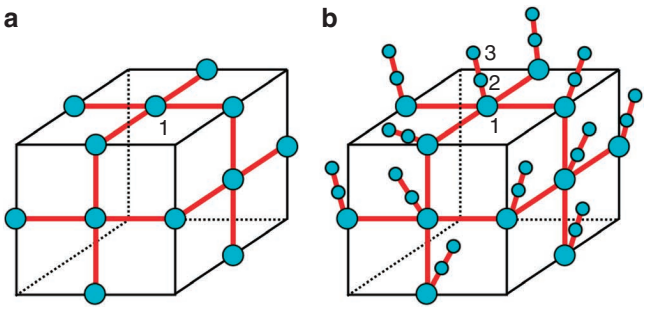

Figure 1 | Elementary cells. (**a**) The elementary cell of the RHG lattice $\mathcal{L}$. (**b**) The elementary cell of the decorated RHG lattice $\mathcal{L}'$.

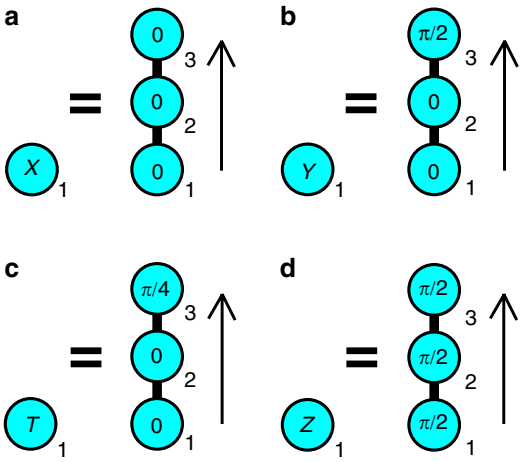

Figure 2 | How the decorated lattice works. If we prepare the three-qubit cluster state and measure each qubit in the numerical order in the $\{|0\rangle\pm e^{i\phi_j}|1\rangle\}$ basis with $(\phi_1,\phi_2,\phi_3)=(0,0,0)$, $(0,0,\pi/2)$, $(0,0,\pi/4)$, and $(\pi/2,\pi/2,\pi/2)$, we can simulate single-qubit measurements in X, Y, T and Z basis, respectively. Each corresponds to (**a**–**d**).

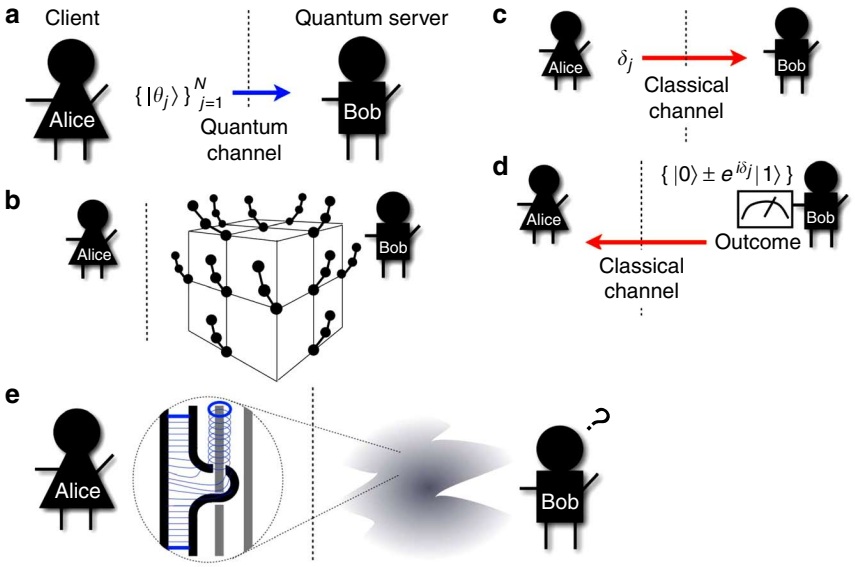

Figure 3 | Topological blind protocol. (**a**) Alice sends Bob randomly rotated qubits. (**b**) Bob creates the decorated RHG lattice. (**c**) Alice sends Bob a classical message. (**d**) Bob does the measurement and returns the result to Alice. (**e**) Alice can hide her topological quantum computation from Bob.

the RHG lattice as is shown in Fig. 1b, Bob can simulate the measurement in X, Y, T and Z basis only with $\{|0\rangle \pm e^{i\phi}|1\rangle\}$ basis measurements, and he cannot know which type of measurements (X, Y, T or Z) he is simulating.

More precisely, our protocol runs as follows (Fig. 3):

Step 1. Alice sends N randomly rotated single-qubit states $\{|\theta_j\rangle\}_{j=1}^N$ to Bob through the quantum channel, where

$$|\theta_j\rangle \equiv |0\rangle + e^{i\theta_j}|1\rangle,$$

and $\theta_j \in \{(k\pi/4)\,|\,k=0,1,...,7\}$ $(j=1,2,\ldots,N)$ are random numbers. N is the total number of qubits used in the decorated RHG lattice $\mathcal{L}'$. Alice remembers all random numbers $\Theta \equiv \{\theta_j\}_{j=1}^N$, and they are kept secret to Bob.

Step 2. Now Bob has $\{|\theta_j\rangle\}_{j=1}^N$. He places $|\theta_j\rangle$ on the j^{th} vertex of the decorated RHG lattice $\mathcal{L}'$ for all j $(j=1,\ldots,N)$. He then applies the CZ gate on each red edge of the decorated RHG lattice $\mathcal{L}'$. Let us denote thus created N-qubit state by $|\mathcal{C}_\Theta\rangle$. As

$$|C_\Theta\rangle = \left(\bigotimes_{k,l} CZ_{k,l}\right)\left(\bigotimes_{j=1}^N e^{-iZ\theta_j/2}\right)|+\rangle^{\otimes N} = \left(\bigotimes_{j=1}^N e^{-iZ\theta_j/2}\right)\left(\bigotimes_{k,l} CZ_{k,l}\right)|+\rangle^{\otimes N},$$

$|\mathcal{C}_\Theta\rangle$ is nothing but a rotated graph state on the decorated RHG lattice $\mathcal{L}'$. Here $CZ_{k,l}$ is the CZ gate between k^{th} and l^{th} qubits.

Step 3. If Alice wants Bob to measure the j^{th} qubit of $|\mathcal{C}_\Theta\rangle$ in $\{|0\rangle \pm e^{i\phi_j}|1\rangle\}$ basis, she calculates

$$\delta_j \equiv \phi'_j + \theta_j + r_j\pi \ (mod\ 2\pi)$$

on her classical computer. Here, $r_j \in \{0,1\}$ is a random number, $\phi'_j \equiv (-1)^{s_j^X}\phi_j + \pi s_j^Z \pmod{2\pi}$, and $s_j^X, s_j^Z \in \{0,1\}$ are determined by the previous measurement results (this is the usual feed-forwarding in the one-way model[9]). Then Alice sends δ_j to Bob through the classical channel.

Step 4. Bob measures the j^{th} qubit in the $\{|0\rangle \pm e^{i\delta_j}|1\rangle\}$ basis and returns the result of the measurement to Alice through the classical channel.

Step 5. They repeat steps 3 and 4 with increasing j until they finish the computation. Note that Alice does the classical processing for the error correction by using Bob's measurement results.

Correctness. Let us show that this protocol is correct. In other words, Alice and Bob can simulate the original TMBQC[12,13] on the decorated RHG lattice $\mathcal{L}'$ with only $\{|0\rangle \pm e^{i\phi}|1\rangle\}$ basis measurements if Bob is honest. Let us consider three qubits labelled with 1, 2 and 3, in Fig. 1b. Let us assume that Bob measures these three qubits in the numerical order (that is, from the bottom one to the top one) in the

$$\left\{|0\rangle \pm e^{i\delta_j}|1\rangle\right\} = \left\{e^{-i\theta_j Z/2} Z^{s_j^Z} X^{s_j^X}\left(|0\rangle \pm e^{i\phi_j}|1\rangle\right)\right\}$$

basis $(j=1,2,3)$ with $(\phi_1,\phi_2,\phi_3)=(0,0,0)$. By a straightforward calculation, it is easy to show that such a sequence of measurement on the three qubits is equivalent to the measurement in the X basis on the qubit labelled with 1 in Fig. 1a (also Fig. 2a). Note that θ_j in Bob's measurement basis is cancelled, as j^{th} qubit is pre-rotated by θ_j by Alice. Furthermore, $r_j\pi$ causes just the flip of the measurement result. Therefore, Bob effectively does $\{|0\rangle \pm e^{i\phi_j}|1\rangle\}$ basis measurement, although he is doing $\{|0\rangle \pm e^{i\delta_j}|1\rangle\}$ basis measurement. In other words, our lattice $\mathcal{L}'$ can simulate the X basis measurements on $\mathcal{L}$. In a similar way, if Bob does measurements on the three qubits labelled with 1, 2 and 3 in Fig. 1b in other angles, $(\phi_1,\phi_2,\phi_3)=(0,0,\pi/2)$, $(0,0,\pi/4)$ and $(\pi/2,\pi/2,\pi/2)$, they are equivalent to the Y, T and Z basis measurements on the qubit labelled with 1 in Fig. 1a, respectively, (Fig. 2b–d). In this way, our lattice $\mathcal{L}'$ can simulate the X, Z, T and Y basis measurements on $\mathcal{L}$. In short, we have shown that $|\mathcal{C}_\Theta\rangle$ on the decorated RHG lattice $\mathcal{L}'$ can simulate the original TMBQC[12,13] on the RHG lattice $\mathcal{L}$ solely with $\{|0\rangle \pm e^{i\phi}|1\rangle\}$ basis measurements.

Blindness. How about the blindness? In our protocol, what Alice sends to Bob are randomly rotated single-qubit states $\{|\theta_j\rangle\}_{j=1}^N$ and measurement angles $\{\delta_j\}_{j=1}^N$. Without loss of generality, we can

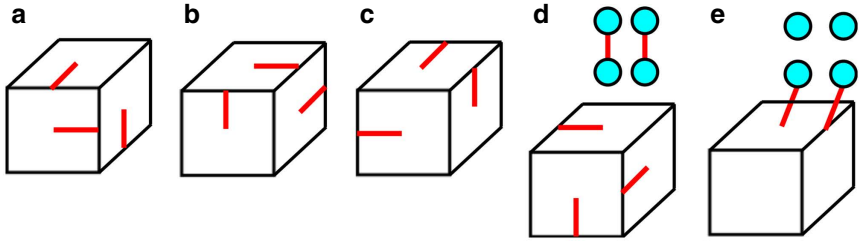

Figure 4 | The stepwise creation of the resource state. $|\mathcal{C}_\Theta\rangle$ is created from **a** to **e**.

assume that the preparation of the input is included in the algorithm. Therefore, what Alice wants to hide are the algorithm and the output. We can show that the conditional probability distribution of Alice's computational angles, given all the classical information Bob can obtain during the protocol, and given the measurement results of any positive-operator valued measures (POVMs) that Bob may perform on his system at any stage of the protocol, is equal to the a priori probability distribution of Alice's computational angles. We can also show that the final classical output is one-time padded to Bob. (For a proof, see Methods.)

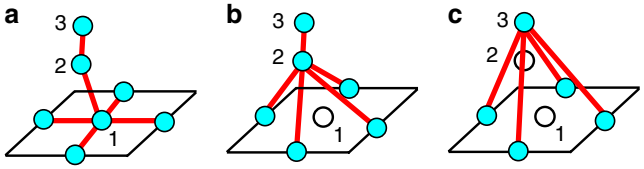

Figure 5 | The measuring pattern. Three qubits are measured in the numerical order from **a** to **c**.

Threshold. Finally, let us calculate the fault-tolerant threshold. As in refs 12,13, we assume that errors occur during the preparation of initial states $\{|\theta_j\rangle\}_{j=1}^N$, the applications of CZ gates and the local measurements. The erroneous preparation of an initial state is modelled by the perfect preparation followed by the partially depolarizing noise with the probability p_P: $(1-p_P)[I]+(p_P/3)([X]+[Y]+[Z])$, where $[\bullet]$ indicates the super operator. The erroneous local measurement is modelled by the perfect local measurement preceded by the partially depolarizing noise with the probability p_M. The erroneous CZ gate is modelled by the perfect CZ gate followed by the two qubit partially depolarizing noise with the probability p_2: $(1-p_2)[I\otimes I]+(p_2/15)([I\otimes X]+\ldots+[Z\otimes Z])$. Because of the rotational symmetry of the depolarizing noise, we can replace $[A]$ with $[e^{-i\theta_j Z/2}Ae^{i\theta_j Z/2}]$ when it acts on the j^{th} qubit, and $[A\otimes B]$ with $[(e^{-i\theta_j Z/2}Ae^{i\theta_j Z/2})\otimes(e^{-i\theta_k Z/2}Be^{i\theta_k Z/2})]$ when it acts on the j^{th} and k^{th} qubits. Here, $A, B = I, X, Y$ or Z. These replacements just correspond to the rotation of the local reference frame of each qubit. Then, if the measurement basis on the j^{th} qubit ($j=1,\ldots,N$) is rotated by $e^{-i\theta_j Z/2}$, the factor $\bigotimes_{j=1}^N e^{-i\theta_j Z/2}$ is cancelled. Therefore, when we calculate the fault-tolerant threshold of our protocol, we can assume that all $\theta_j=0$ without loss of generality. As in ref. 18, we assume that $|\mathcal{C}_\Theta\rangle$ is created in the stepwise manner (Fig. 4). In our case, however, the additional fifth step is introduced as is shown in Fig. 4e. First, let us calculate the single-qubit Z error probability λ_j ($j=1,2,3$) on each of the three qubits labelled with 1,2,3 in Fig. 1b after creating $|\mathcal{C}_\Theta\rangle$. By a straightforward calculation, we obtain $\lambda_1=32p_2/15+8p_2/15+2p_P/3$; $\lambda_2=16p_2/15+2p_P/3$; and $\lambda_3=8p_2/15+2p_P/3$ up to the first order of p_P and p_2. Once an erroneous $|\mathcal{C}_\Theta\rangle$ is created, we start local measurements. As is shown in Fig. 5, the three qubits are sequentially measured in numerical order. Such a sequential measurement propagates all pre-existing errors on qubits labelled with 1 and 2 to the qubit labelled with 3. By a straightforward calculation, the accumulated error probability on the qubit labelled with 3 by such a propagation is $\lambda_{\text{total}}\equiv\lambda_1+\lambda_3+2\times 2p_M/3$ for $(\phi_1,\phi_2,\phi_3)=(0,0,0)$. We have only to consider the measurement pattern that corresponds to the effective X measurement on the qubit labelled with 1 in Fig. 1a, because we are now interested in the topological error-correction of the bulk qubits. The value λ_{total} corresponds to the quantity q_1, which was studied in ref. 18, of the qubit labelled with 1 in Fig. 1a. The correlated two-qubit error probability[18] $q_2=4p_2/15+O(p_2^2)$ in our protocol is the same as that in ref. 18. If we assume $p_P=p_M=p_2=p$, we obtain the bulk topological error threshold as $p=4.3\times10^{-3}$ from Fig. 10 of ref. 18, where the threshold curve of (q_1,q_2) is numerically calculated by using the minimum-weight-perfect-matching algorithm.

The primal defects are created by measuring the edge qubits inside the defect region in the Z basis. At the boundary of the defect region (surface of the defects), these measurements introduce additional Z errors on the face qubits (that is, dual qubits), which has an effect of decreasing the threshold value. At the same time, the existence of the defects changes the boundary condition of the bulk region; at the surface of the primal defects, the dual lattice has a smooth boundary. Thus, there is excess syndrome available at the defect surface, which has an effect of increasing the threshold value. In ref. 18, they have performed numerical simulation for lattices of size $L\times L\times 2L$, where half of the lattice belongs to the bulk region V and the other half to the defect region D. In their calculations, the error probability of the dual qubits of the surface of the defect is doubled to investigate the surface effect. Their numerical result indicates that although the surface effect due to the smooth boundary (that is, increasing the threshold value) is noticeable, the intersection point of fidelity curves is slowly converging to the threshold value of the bulk region in the increasing number of the lattice size. This indicates that the Z basis measurements for the defect creations do not lower the threshold for TMBQC. In the present case, the error probability of the Z basis measurement is increased by $\lambda_Z=2(2p_M/3)+2(2p_P/3)+p_2$ because of the additional qubits for the blind Z-basis measurement. However, when $p_M=p_P=p_2=4.3\times10^{-3}$, the error probability $\lambda_Z=1.6\times10^{-2}$ is still smaller than the situation that has been considered in ref. 18. Thus, the defect creations do not lower the threshold in the blind setup again, and hence the threshold value is determined by that for the bulk region.

Topological error correction breaks down near the singular qubits, and it results in an effective error on the singular qubits[12,13]. This effective error is local because singular qubits are well separated from each other. Magic state distillation[17] can tolerate a rather large amount of noise, and therefore the overall threshold is determined by that for the bulk topological region[12,13]. In fact, the recursion relations of the distillations of Y and $(X+Y)/\sqrt{2}\equiv T$ basis states are given by $\varepsilon_{l+1}^Y=7(\varepsilon_l^Y)^3+\varepsilon_{\text{top}}^Y$ and $\varepsilon_{l+1}^T=35(\varepsilon_l^T)^3+\varepsilon_{\text{top}}^T$, where $\varepsilon_{\text{top}}^Y$ and $\varepsilon_{\text{top}}^T$ indicate the probability of errors introduced by the Clifford gates for the magic state distillation[13]. To optimize their overheads, the scale factor and defect thickness at each

distillation level are chosen so that $\varepsilon_l^{Y,T}$ and $\varepsilon_{\rm top}^{Y,T}$ are balanced. As $\varepsilon_{\rm top}^{Y}$ and $\varepsilon_{\rm top}^{T}$ can be reduced rapidly by increasing the scale factor and the thickness of the defect, the threshold values for the magic state distillation can be determined as $\varepsilon^Y=0.38$ and $\varepsilon^T=0.17$ for Y- and T-state distillations, respectively. In the present decorated case, the error probability of the injected magic state is at most $\varepsilon=4p_2+2p_2+3(2p_M/3)+3(2p_P/3)$, where the first, second, third and fourth terms indicate four CZ gates for generating the RHG lattice, two CZ gates for the decoration, three measurements and three state preparations. With $p_M=p_P=p_2=4.3\times10^{-3}$, $\varepsilon=10p_2=0.043$, which is sufficiently smaller than the threshold values for the magic state distillations.

In the above arguments, we have assumed $p_P=p_M=p_2$ for simplicity. However, p_P might be much larger than p_M and p_2, as Alice's quantum technology is assumed to be much weaker than that of Bob and the randomly rotated qubits are sent from Alice to Bob through a probably noisy quantum channel. In addition, Alice cannot distill her qubits, as she cannot use any two-qubit gate. Hence, let us consider another representative scenario, $p_P=10p$ and $p_M=p_2=p$. Interestingly, the direct calculation shows that the error threshold is $p=1.6\times10^{-3}$ (that is, still of the order of 10^{-3}). This suggests the nice robustness on Alice's side in the topological fault-tolerant protocol. Note that this result is reasonable because the preparation error behaves as an independent error, and independent errors are known to be easy to correct. In fact, if there is no correlated error, TMBQC can tolerate the independent error up to 2.9%.

Discussion

In addition to the probabilistic depolarizing noise, which we have considered, there are many possibilities of errors. For example, quantum computation can suffer from the detectable qubit loss, such as photon loss, atoms or ions escaping from traps, or more generally, the leakage of a qubit out of the computational basis in a multilevel system. In ref. 19, the threshold of the TMBQC for the qubit loss was studied. Here, let us briefly explain that we can obtain a similar threshold for the qubit loss in our blind protocol. As in ref. 19, let us assume that losses are independent and identically distributed events with the probability $p_{\rm loss}$. If one of the three qubits labelled with 1, 2 and 3 in Fig. 1b is lost, then we just consider the entire three-qubit chain is lost. Then, we can use the result of ref. 19, and our threshold for the qubit loss is obtained by replacing their $p_{\rm loss}$ with $3p_{\rm loss}$. Note that if we also use the post-selected scheme of ref. 19, then the overhead is $\simeq(1-3p_{\rm loss})^{d^3}$, which is still independent of the size of the algorithm, and hence ensuring scalability. Another possible error, the non-determinism of CZ gates, was considered in refs 20,21 for TMBQC. For example, in ref. 20, the three-dimensional resource state is created by fusing the 'puffer ball' states. If the one-dimensional chain of two qubits is added to the root qubit of each puffer ball state, $|\mathcal{C}_\Theta\rangle$ can be created by a similar fusion strategy and the threshold can also be calculated in a similar way.

Although the simulation of fault-tolerant quantum circuits in the blind MBQC on the brickwork state was mentioned in ref.3, it is only the existence proof. Neither a concrete scheme nor an explicit calculation of the threshold was given. Furthermore, on the two-dimensional brickwork state, we should use the fault-tolerant scheme of the one-dimensional nearest-neighbour circuit model architecture. For the circuit model, the threshold of this scheme is of the order of 10^{-5} (refs 22,23). If we implement this scheme on MBQC, the threshold should be $\sim10^{-6}$ due to the extra qubits[24,25]. As is mentioned in ref. 3, the threshold should be increased if the three-dimensional brickwork state is considered. However, the explicit calculation of the threshold for the scheme of ref. 26 is not known and should be smaller than that of TMBQC.

In the protocol, Alice performs the decoding operation (error correction) by using the classical data from Bob[12,13]. We have calculated the threshold value for the present blind protocol by following the result in ref. 18, where the minimum-weight-perfect-matching algorithm is used for the decoding problem. Although the minimum-weight-perfect-matching is an efficient algorithm in the sense that it scales polynomially, it might cost large classical computational resources when the lattice size is large. However, more efficient classical algorithms for the decoding problem have also been developed[27–29], one of which[27] achieves the decoding of the lattice of four million qubits within a few seconds by using a today's typical classical computer, whereas the resultant threshold 0.9% is higher than that 0.75% in ref. 18. In this sense, Alice's classical processing does not present any problem here.

Methods

Definition of the blindness. Here we show the blindness of our protocol. Intuitively, a protocol is blind if Bob, given all the classical and quantum information during the protocol, cannot learn anything about Alice's computational angles, input and output[3,5,6]. A formal definition we adopt here is as follows (see also refs 3,5,6).

A protocol is blind if: (B1) the conditional probability distribution of Alice's computational angles, given all the classical information Bob can obtain during the protocol, and given the measurement results of any POVMs that Bob may perform on his system at any stage of the protocol, is equal to the a priori probability distribution of Alice's computational angles; and (B2) the final classical output is one-time padded to Bob.

Our protocol satisfies B1. Let us define $\Delta\equiv(\Delta_1,\ldots,\Delta_N)$, $\Phi\equiv(\Phi_1,\ldots,\Phi_N)$, $\Theta\equiv(\Theta_1,\ldots,\Theta_N)$, $R\equiv(R_1,\ldots,R_N)$, where $\Delta_j,\Theta_j,\Phi_j\in A\equiv\{(k\pi/4)\,|\,k=0,1,\ldots,7\}$ and $R_j\in\{0,1\}$ are random variables, corresponding to the angles sent by Alice to Bob, random prerotations, Alice's secret computational angles and the hidden binary parameters, respectively. From the construction of the protocol, the relation $\Delta_j=\Phi_j+\Theta_j+R_j\pi\ (\mathrm{mod}\ 2\pi)$ is satisfied. Let $\{\Pi_j\}_{j=1}^m$ be a POVM, which Bob may perform on his $\{|\theta_j\rangle\}_{j=1}^N$. Let $O\in\{1,\ldots,m\}$ be the random variable corresponding to the result of the POVM. Bob's knowledge about Alice's computational angles is given by the conditional probability distribution of $\Phi=(\phi_1,\ldots,\phi_N)$ given $O=j$ and $\Delta=(\delta_1,\ldots,\delta_N)$: $P(\Phi=(\phi_1,\ldots,\phi_N)|O=j,\Delta=(\delta_1,\ldots,\delta_N))$.

From Bayes' theorem, we have

$$
\begin{aligned}
&P\big(\Phi=(\phi_1,\ldots,\phi_N)|O=j,\Delta=(\delta_1,\ldots,\delta_N)\big)\\
&=\frac{P\big(O=j\,|\,\Phi=(\phi_1,\ldots,\phi_N),\Delta=(\delta_1,\ldots,\delta_N)\big)P\big(\Phi=(\phi_1,\ldots,\phi_N),\Delta=(\delta_1,\ldots,\delta_N)\big)}{P\big(O=j,\Delta=(\delta_1,\ldots,\delta_N)\big)}\\
&=\frac{P\big(O=j\,|\,\Phi=(\phi_1,\ldots,\phi_N),\Delta=(\delta_1,\ldots,\delta_N)\big)P\big(\Phi=(\phi_1,\ldots,\phi_N)\big)P\big(\Delta=(\delta_1,\ldots,\delta_N)\big)}{P\big(O=j\,|\,\Delta=(\delta_1,\ldots,\delta_N)\big)P\big(\Delta=(\delta_1,\ldots,\delta_N)\big)}\\
&=P\big(\Phi=(\phi_1,\ldots,\phi_N)\big)\frac{\mathrm{Tr}[\Pi_j\bigotimes_{i=1}^N\frac{1}{2}\sum_{r_i=0}^{1}|\delta_i-\phi_i-r_i\pi\rangle\langle\delta_i-\phi_i-r_i\pi|]}{\mathrm{Tr}[\Pi_j\bigotimes_{i=1}^N\frac{1}{8}\frac{1}{2}\sum_{\phi_i\in A}\sum_{r_i=0}^{1}|\delta_i-\phi_i-r_i\pi\rangle\langle\delta_i-\phi_i-r_i\pi|]}\\
&=P\big(\Phi=(\phi_1,\ldots,\phi_N)\big).
\end{aligned}
$$

Our protocol satisfies B2. It is easy to confirm that when Bob measures the qubit labelled with 3 in Fig. 1b, the state is one-time padded with $Z^{s_1}X^{s_2}$, where s_1 (s_2) is the measurement result of the qubit labelled with 1 (2) in Fig. 1b. The values of s_1 and s_2 are unknown to Bob, as $\{r_j\}_{j=1}^N$ are unknown to Bob. We can show that $\{r_j\}_{j=1}^N$ are unknown to Bob as follows.

$$
\begin{aligned}
&P\big(R=(r_1,\ldots,r_N)|O=j,\Delta=(\delta_1,\ldots,\delta_N)\big)\\
&=\frac{P\big(O=j\,|\,R=(r_1,\ldots,r_N),\Delta=(\delta_1,\ldots,\delta_N)\big)P\big(R=(r_1,\ldots,r_N),\Delta=(\delta_1,\ldots,\delta_N)\big)}{P\big(O=j\,|\,\Delta=(\delta_1,\ldots,\delta_N)\big)P\big(\Delta=(\delta_1,\ldots,\delta_N)\big)}\\
&=\frac{P\big(O=j\,|\,R=(r_1,\ldots,r_N),\Delta=(\delta_1,\ldots,\delta_N)\big)P\big(R=(r_1,\ldots,r_N)\big)P\big(\Delta=(\delta_1,\ldots,\delta_N)\big)}{P\big(O=j\,|\,\Delta=(\delta_1,\ldots,\delta_N)\big)P\big(\Delta=(\delta_1,\ldots,\delta_N)\big)}\\
&=P\big(R=(r_1,\ldots,r_N)\big)\frac{\mathrm{Tr}[\Pi_j\bigotimes_{i=1}^N\frac{1}{8}\sum_{\phi_i\in A}^{1}|\delta_i-\phi_i-r_i\pi\rangle\langle\delta_i-\phi_i-r_i\pi|]}{\mathrm{Tr}[\Pi_j\bigotimes_{i=1}^N\frac{1}{8}\frac{1}{2}\sum_{\phi_i\in A}\sum_{r_i=0}^{1}|\delta_i-\phi_i-r_i\pi\rangle\langle\delta_i-\phi_i-r_i\pi|]}\\
&=\mathrm{P}\big(R=(r_1,\ldots,r_N)\big)\\
&=\frac{1}{2^N}.
\end{aligned}
$$

References

1. Abadi, M., Feigenbaum, J. & Kilian, J. On hiding information from an oracle. *J. Comput. Syst. Sci.* **39,** 21–50 (1989).
2. Gentry, C. in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing* 169–178 (ACM, New York, 2009).
3. Broadbent, A., Fitzsimons, J. & Kashefi, E. in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer* 517–527 (IEEE Computer society, Los Alamitos, USA, 2009).
4. Barz, S., Kashefi, E., Broadbent, A., Fitzsimons, J., Zeilinger, A. & Walther, P. Experimental demonstration of blind quantum computing. *Science* **335,** 303–308 (2012).
5. Morimae, T., Dunjko, V. & Kashefi, E. *Ground State Blind Quantum Computation on AKLT State* Preprint at arXiv:1009.3486 (2010).
6. Dunjko, V., Kashefi, E. & Leverrier, A. Universal blind quantum computing with coherent states. *Phys. Rev. Lett.* **108,** 200502 (2012).
7. Morimae, T. & Fujii, K. *Blind Quantum Computation for Alice Who Does Only Measurements* Preprint at arXiv:1201.3966 (2012).
8. Fitzsimons, J. & Kashefi, E. *Unconditionally verifiable blind computation* Preprint at arXiv:1203.5217 (2012).
9. Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86,** 5188 (2001).
10. Song, D., Wagner, D. & Perrig, A. Practical Techniques for Searches on Encrypted Data, in *IEEE Symp. Res Security Privacy* (IEEE Computer society, Los Alamitos, USA, 2000).
11. Castelluccia, C., Mykletun, E. & Tsudik, G. Efficient aggregation of encrypted data in wireless sensor networks, in *ACM/IEEE Mobile and Ubiquitous Systems: Networking and Services* 109–117 (IEEE Computer society, Los Alamitos, USA, 2005).
12. Raussendorf, R. & Harrington, J. Fault-tolerant quantum computation with high threshold in two dimensions. *Phys. Rev. Lett.* **98,** 190504 (2007).
13. Raussendorf, R., Harrington, J. & Goyal, K. Topological fault-tolerance in cluster state quantum computation. *New J. Phys.* **9,** 199 (2007).
14. Benhelm, J., Kirchmair, G., Roos, C. F. & Blatt, R. Towards fault-tolerant quantum computing with trapped ions. *Nature Phys.* **4,** 463–466 (2008).
15. Yao, X. C. Experimental demonstration of topological error correction. *Nature* **482,** 489–494 (2012).
16. Kitaev, A. Fault-tolerant quantum computation by anyons. *Ann. Phys.* **303,** 2–30 (2003).
17. Bravyi, S. & Kitaev, A. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A* **71,** 022316 (2005).
18. Raussendorf, R., Harrington, J. & Goyal, K. A fault-tolerant one-way quantum computer. *Ann. Phys.* **321,** 2242–2270 (2006).
19. Barrett, S. D. & Stace, T. M. Fault tolerant quantum computation with very high threshold for loss errors. *Phys. Rev. Lett.* **105,** 200502 (2010).
20. Fujii, K. & Tokunaga, Y. Fault-tolerant topological one-way quantum computation with probabilistic two-qubit gates. *Phys. Rev. Lett.* **105,** 250503 (2010).
21. Li, Y., Barrett, S. D., Stace, T. M. & Benjamin, S. C. Fault tolerant quantum computation with nondeterministic gates. *Phys. Rev. Lett.* **105,** 250502 (2010).
22. Stephens, A. M., Fowler, A. G. & Hollenberg, L. C. L. Universal fault tolerant quantum computation on bilinear nearest neighbor arrays. *Quant. Inf. Comput.* **8,** 330–344 (2008).
23. Stephens, A. M. & Evans, Z. W. E. Accuracy threshold for concatenated error detection in one dimension. *Phys. Rev. A* **80,** 022313 (2009).
24. Dawson, C. M., Haselgrove, H. L. & Nielsen, M. A. Noise thresholds for optical cluster-state quantum computation. *Phys. Rev. A* **73,** 052306 (2006).
25. Dawson, C. M., Haselgrove, H. L. & Nielsen, M. A. Noise thresholds for optical quantum computers. *Phys. Rev. Lett.* **96,** 020501 (2006).
26. Gottesman, D. Fault-tolerant quantum computation with local gates. *J. Mod. Opt.* **47,** 333–345 (2000).
27. Fowler, A. G., Whiteside, A. C. & Hollenberg, L. C. L. Towards practical classical processing for the surface code. *Phys. Rev. Lett.* **108,** 180501 (2012).
28. Duclos-Cianci, G. & Poulin, D. Fast decoders for topological quantum codes. *Phys. Rev. Lett.* **104,** 050504 (2010).
29. Duclos-Cianci, G. & Poulin, D. *A Renormalization Group Decoding Algorithm for Topological Quantum Codes* Preprint at arXiv:1006.1362 (2010).

Acknowledgements

We acknowledge supports from JSPS, ANR (StatQuant, JC07 07205763) and MEXT(Grant-in-Aid for Scientific Research on Innovative Areas 20104003).

Additional information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Morimae, T. & Fujii, K. Blind topological measurement-based quantum computation. *Nat. Commun.* 3:1036 doi: 10.1038/ncomms2043 (2012).