nature physics

SUPPLEMENTARY INFORMATION

DOI: 10.1038/NPHYS2763

Experimental verification of quantum computation

Stefanie Barz[1], Joseph Fitzsimons[2,3], Elham Kashefi[4], and Philip Walther[1]

[1] University of Vienna, Faculty of Physics, Boltzmanngasse 5, A-1090 Vienna, Austria
[2] Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682
[3] Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543
[4] School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK

Contents

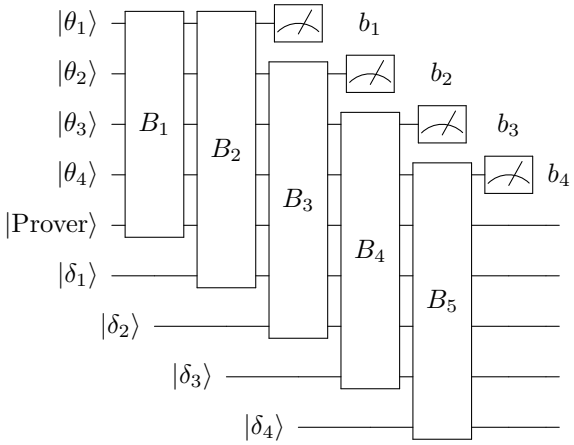
1 Verification of a quantum computation

In order to verify a blind quantum computation, it is necessary to ensure that the probability of an undetected error being introduced to the computation is bounded. One way to do this is to introduce trap qubits into the computation as in [1]. To prove that this does in fact guarantee that any error is either detected or corrected except with bounded probability, we must consider the most general possible cheating strategy for the prover. Thus we must consider the effect of an arbitrary deviation at each step of the protocol. In this section we present a simplified version of the proof in [1] adapted to our 4-qubit protocol with classical inputs and outputs, and then show how it can be adapted to work with traps prepared by measurement-based computation.

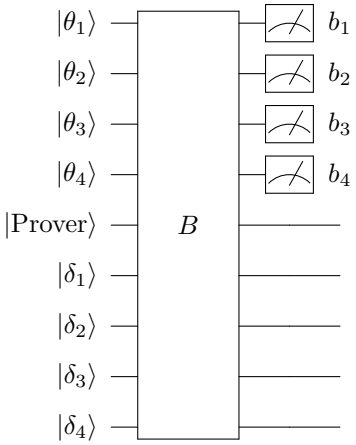
1.1 Individual trap qubits

We assume the most general scenario. The prover obtains the quantum states $|\theta_i\rangle$ and the states $|\delta_i\rangle$ which encode the classical angles δ_i. Further, the prover has access to a private quantum memory $|\text{Prover}\rangle$, where the prover could store quantum information allowing him to perform the most general attacks:

DOI: 10.1038/NPHYS2763
nature physics



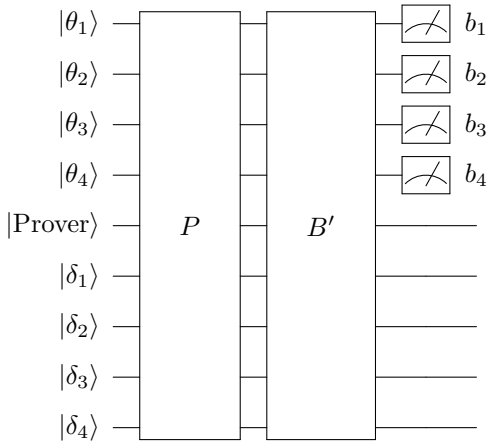
Here, $\{B_i\}$ are the individual operations performed by the prover and b_i is the outcome of a measurement always performed in the basis $\{|0\rangle, |1\rangle\}$. Without loss of generality we can assume that the measurement occurs immediately prior to transmission of each bit to the verifier, as shown above. Mathematically, the individual operations performed by the prover, $\{B_i\}$ can be combined into a single operation B, resulting in the quantum circuit shown below.



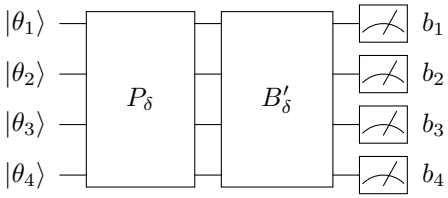
By defining $B' = BP^\dagger$, where P corresponds to the unitary implementing the protocol for an honest prover, the circuit corresponding to the protocol can be rewritten as the ideal protocol followed by some

DOI: 10.1038/NPHYS2763

deviation.



The verifier's output only corresponds to the measurement outputs received from the prover, and so the prover's effective deviation operator can be reduced to a super-operator, dependent on the specific values of $\{\delta_i\}$ used in that run of the protocol, acting only on these qubits.



As the left hand part of the above circuit implements the ideal protocol, B'_δ contains any error introduced by the prover.

Note that the output of the ideal protocol $b = \{b_i\}$ is the output of the verifier's chosen computation, $m = \{m_i\}$, bitwise xored with a random bitstring, $r = \{r_i\}$, known only to the verifier:

$$b = m \oplus r.$$

In the following, we encode the classical information in a quantum system:

$$\begin{aligned} b &\rightarrow |b\rangle, \\ m &\rightarrow |m\rangle, \\ r &\rightarrow |r\rangle, \text{and} \\ (m \oplus r) &\rightarrow |m \oplus r\rangle, \end{aligned}$$

thus n classical bits are encoded in n qubits.

Therefore, for a fixed computation chosen by the verifier with outcome m, on n qubits, the probability of an error occurring (averaging over all possible choices for the random bitstring r) is given by

$$\begin{aligned} \epsilon &= \frac{1}{2^n} \sum_{r \in \{0,1\}^n} \text{Tr}\left[\left(\mathbb{I}_{2^n} - |m+r\rangle\langle m+r|\right) B'_\delta \left(|m+r\rangle\langle m+r|\right)\right], \\ &= \frac{1}{2^n} \sum_{b \in \{0,1\}^n} \text{Tr}\left[\left(\mathbb{I}_{2^n} - |b\rangle\langle b|\right) B'_\delta \left(|b\rangle\langle b|\right)\right], \end{aligned}$$

for a fixed computation. Here, n is the number of qubits involved in the protocol and $\mathbb{I}_{2^n}$ is the 2^n-dimensional density matrix.

Note, however, that for a trap located on any measured qubit i for which the expected measurement outcome is r_i, the probability of the trap registering an error is:

$$t_{i,r_i} = \mathrm{Tr}\left[\left(\mathbb{I}_{2^n} - \mathbb{I}_{2^{i-1}} \otimes |r_i\rangle\langle r_i| \otimes \mathbb{I}_{2^{n-i}}\right) B'_\delta \left(\frac{\mathbb{I}_{2^{i-1}}}{2^{i-1}} \otimes |r_i\rangle\langle r_i| \otimes \frac{\mathbb{I}_{2^{n-i}}}{2^{n-i}}\right)\right],$$

where $|r_i\rangle$ a 2-dimensional quantum state encoding the classical value r_i. Here, we use the fact that for a measurement of a trap qubit we expect $m_i = 0$, and thus $r_i = b_i$.

Averaging over all possible choices of i and r_i, this yields an average probability of detection of

$$\begin{aligned}\langle t\rangle &= \sum_{i=1}^{n} \frac{1}{n} \sum_{b\in\{0,1\}^n} \frac{1}{2^n} \mathrm{Tr}\left[\left(\mathbb{I}_{2^n} - \mathbb{I}_{2^{i-1}} \otimes |b_i\rangle\langle b_i| \otimes \mathbb{I}_{2^{n-i}}\right) B'_\delta \left(|b\rangle\langle b|\right)\right] \\ &= \frac{1}{n\,2^n} \sum_{b\in\{0,1\}^n} \mathrm{Tr}\left[\left(\sum_{i=1}^{n} \left(\mathbb{I}_{2^n} - \mathbb{I}_{2^{i-1}} \otimes |b_i\rangle\langle b_i| \otimes \mathbb{I}_{2^{n-i}}\right)\right) B'_\delta \left(|b\rangle\langle b|\right)\right],\end{aligned}$$

where $|b_i\rangle_i$ a 2-dimensional quantum state encoding the classical value b_i.

As the $B'_\delta\left(|b\rangle\langle b|\right)$ is positive semi-definite, and

$$\left(\mathbb{I}_{2^n} - |b\rangle\langle b|\right) \preceq \sum_{i=1}^{n} \left(\mathbb{I}_{2^n} - |b_i\rangle_i\langle b_i|_i\right),$$

then

$$\langle t\rangle \geq \frac{2^{-n}}{n} \sum_{b\in\{0,1\}^n} \mathrm{Tr}\left[\left(\mathbb{I}_{2^n} - |b\rangle\langle b|\right) B'_\delta \left(|b\rangle\langle b|\right)\right]$$

where b_i is the ith bit of b. Thus, by substituting in ϵ into the above equation and rearranging, we obtain $\epsilon \leq n\langle t\rangle$.

1.2 Traps prepared by MBQC

Contrary to the protocol described in [1], in the current experiment we rely on measurement-based computation to prepare isolated trap qubits (instead of preparing them directly). For example to prepare qubit 4 as a trap qubit, we choose a blind linear cluster state which implements the following computation:

$$|\mathrm{trap}_4\rangle = R_z\left(\theta_4\right) H R_z\left(m_3\pi\right) H R_z\left(\frac{\pi}{2} + m_2\pi\right) H R_z\left(\frac{\pi}{2} + m_1\pi\right) |+\rangle.$$

The output state $|\mathrm{trap}_4\rangle$ then depends on the outcomes of the measurement of qubit 1, 2 and 3 which are blind to the prover.

The general measurement patterns which can achieve such isolated trap qubits, together with the corresponding state of the trap qubit prepared are shown in Table 1.

In order to determine the affect of a cheating prover, it is convenient to note that each of these trap measurements can also be interpreted as a stabilizer measurement of the underlying cluster state, as shown in Table 2. Table 3 gives the cluster state measurement angles ϕ and sample corresponding pairs of blind state preparation and measurement angles (θ, δ), together with the classical computation performed in each case to verify the outcome of the trap measurement.

DOI: 10.1038/NPHYS2763

Trap qubit	Measurements				Trap state
	1	2	3	4	
1		σ	Y	Y	$\|+_{(m_3\oplus m_4)\pi}\rangle$
2	Y		X	Y	$\|+_{(m_1\oplus m_3\oplus m_4)\pi}\rangle$
3	Y	X		Y	$\|+_{(m_1\oplus m_2\oplus m_4)\pi}\rangle$
4	Y	Y	σ		$\|+_{(m_1\oplus m_2)\pi}\rangle$

Table 1: Measurement choices for non-trap qubits which prepare isolated trap qubits at each location. Note that if the choice of measurement operator for a given qubit does not affect the outcome then the measurement has been denoted by σ.

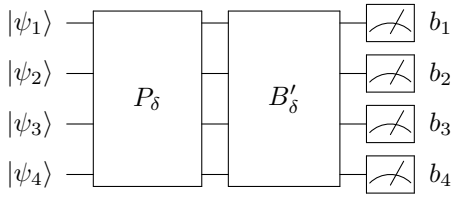
Trap qubit	Stabilizer
1	$X \otimes \mathbb{I} \otimes Y \otimes Y$
2	$Y \otimes X \otimes X \otimes Y$
3	$Y \otimes X \otimes X \otimes Y$
4	$Y \otimes Y \otimes \mathbb{I} \otimes X$

Table 2: Index of trap qubit and corresponding stabilizer measurement.

Trap qubit	ϕ				Sample (θ_i, δ_i)				Trap outcome
	1	2	3	4	1	2	3	4	
1	0	0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$(0,0)$	$\left(\frac{\pi}{2}, -\frac{\pi}{2}\right)$	$\left(\frac{3\pi}{4}, \frac{5\pi}{4}\right)$	$\left(0, \frac{\pi}{2}\right)$	$m_1 \oplus m_3 \oplus m_4$
2	$\frac{\pi}{2}$	0	0	$\frac{\pi}{2}$	$\left(0, \frac{\pi}{2}\right)$	$\left(\frac{\pi}{2}, \frac{\pi}{2}\right)$	$\left(\frac{3\pi}{4}, \frac{7\pi}{4}\right)$	$\left(0, \frac{\pi}{2}\right)$	$m_1 \oplus m_2 \oplus m_3 \oplus m_4$
3	$\frac{\pi}{2}$	0	0	$\frac{\pi}{2}$	$\left(0, \frac{\pi}{2}\right)$	$\left(\frac{\pi}{2}, \frac{\pi}{2}\right)$	$\left(\frac{3\pi}{4}, \frac{7\pi}{4}\right)$	$\left(0, \frac{\pi}{2}\right)$	$m_1 \oplus m_2 \oplus m_3 \oplus m_4$
4	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	0	$\left(0, -\frac{\pi}{2}\right)$	$\left(\frac{\pi}{2}, 0\right)$	$(\pi, 0)$	(0,0)	$m_1 \oplus m_2 \oplus m_4$

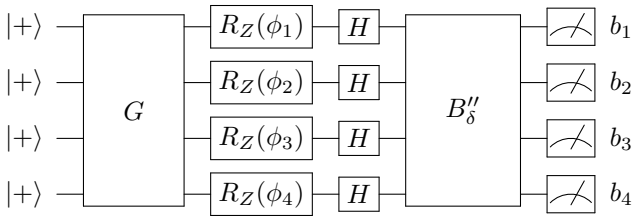
Table 3: Measurement angle for each trap setting together with sample δ and θ. The trap outcome should be consistent with the equation in the right most column in the above table, and any discrepancy represents the detection of an error.

As in the previous section, a general deviation by the prover can be modeled by the quantum circuit below.



DOI: 10.1038/NPHYS2763
nature physics

Equivalently this can be rewritten as



Here, the left hand portion of the circuit performs the unitary part of the ideal measurement-based computation, immediately prior to measurement in the computational basis, with G representing the entangling gate which generates the cluster state from separable qubits via a series of controlled-Z operations. The deviation operator B''_δ can be expanded as a sum over Kraus operators, $\{\chi^k_\delta\}$, acting on the density matrix.

Next, χ^k_δ can be expanded as a sum over 4-qubit Pauli operators (including the identity), $\{\sigma_i\}$, weighted by complex coefficients, so that $\chi^k_\delta = \sum w^k_i \sigma_i$, with $w^k_i \in \mathbb{C}$ and $\sum_k \sum_i w^k_i w^{k*}_i = 1$. Table 4 shows whether a given Pauli term in the deviation operator commutes or anticommutes with each trap setting, and hence whether such an error is detectable or not. We note that the only Pauli terms which commute with the measurement and terms which correspond to a simultaneous bit-flip error on only the first and last qubits remain undetected. The first set of terms leave the computation unaltered, and hence do not represent errors. However the latter group do represent an error which cannot be detected by our current setup.

While this appears to be an insurmountable problem if we wish to verify a general quantum computation, the problem disappears entirely if we consider only those computations for which the output of the computation only depends on the parity of the measurement results of qubits 1 and 4. This is because flipping both measurement outcomes leaves their parity invariant, and hence the outcome of the computation remains the same. Thus for the remainder of this section we consider only those computations for which simultaneously flipping the first and last measurement results leave the outcome of the computation invariant.

With this restriction in place, we take the verification protocol to proceed as follows. First the verifier randomly chooses whether or not to perform a computation as normal or instead to perform a trap computation. We assume that a trap computation is choosen with probability p. Next the verifier chooses uniformly at random an index for the trap qubit[1].

We wish to bound the probability that a given run of the computation yields the correct results based on the probability of trap computations yielding incorrect results. To do this, we note that for the set of computations we consider, any Pauli term in B''_δ which leads to an error in the outcome of the computation necessarily anticommutes with at least one of the trap stabilizer measurements and hence is detected with probability at least $p/4$. Thus any deviation which flips at least one of the measurement outcomes is detected with probability at least $p/4$. If the probability that a malicious prover flips one or more measurement outcomes is ϵ, then the probability that a trap computation yields the correct result is $\langle t \rangle \geq \epsilon p/4$. Thus the probability that the outcome of a computation is incorrect is bounded from above by $\epsilon \leq \frac{4\langle t \rangle}{p}$.

We note that in order for the above verification procedure to work, it is necessary for all qubits to be fully blind (i.e. all possible choices of θ and δ from $\{0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, \pi, \frac{5\pi}{4}, \frac{3\pi}{2}, \frac{7\pi}{4}\}$ should be possible for each qubit). In the current generation of experiments this property holds only for qubits 2 and 3, and the value for δ_1 and δ_4 are fixed. However we note that these fixed values do represent a legitimate choice on

[1]As traps 2 and 3 correspond to the same stabilizer measurement we would obtain a better probability of detecting an error by choosing between the three stabilizer measurements uniformly at random. However, here we use an identical probability for choosing each trap index, since this is optimal in the case where our experimental restrictions are limited and we can employ the full protocol of [1].

DOI: 10.1038/NPHYS2763

Pauli (σ_i)	Trap Stabilizer Measurement			Overall
	$X \otimes \mathbb{I} \otimes Y \otimes Y$	$Y \otimes X \otimes X \otimes Y$	$Y \otimes Y \otimes \mathbb{I} \otimes X$	
$C \otimes C \otimes C \otimes C$	✓	✓	✓	✓
$C \otimes C \otimes C \otimes A$	✗	✗	✗	✗
$C \otimes C \otimes A \otimes C$	✗	✗	✓	✗
$C \otimes C \otimes A \otimes A$	✓	✓	✗	✗
$C \otimes A \otimes C \otimes C$	✓	✗	✗	✗
$C \otimes A \otimes C \otimes A$	✗	✓	✓	✗
$C \otimes A \otimes A \otimes C$	✗	✓	✗	✗
$C \otimes A \otimes A \otimes A$	✓	✗	✓	✗
$A \otimes C \otimes C \otimes C$	✗	✗	✗	✗
$A \otimes C \otimes C \otimes A$	✓	✓	✓	✓
$A \otimes C \otimes A \otimes C$	✓	✓	✗	✗
$A \otimes C \otimes A \otimes A$	✗	✗	✓	✗
$A \otimes A \otimes C \otimes C$	✗	✓	✓	✗
$A \otimes A \otimes C \otimes A$	✓	✗	✗	✗
$A \otimes A \otimes A \otimes C$	✓	✗	✓	✗
$A \otimes A \otimes A \otimes A$	✗	✓	✗	✗

Table 4: Pauli terms in the deviation operator B''_δ and whether or not they are detected by a particular trap setup or not. Although there are 256 distinct 4-qubit Pauli operators, including the identity, these can be grouped into 16 distinct sets based on whether each local term commutes ($C \in \{\mathbb{I}, Z\}$) or anticommutes ($A \in \{X, Y\}$) with the computational basis measurement carried out immediately after the deviation operator acts. Note that all such terms are either leave the computation invariant, or are detected by at least one trap setting, with the exception of $A \otimes C \otimes C \otimes A$.

the part of the verifier, and as long as the prover does not have a priori information about this restriction the proof of authentication holds.

1.3 Experimental settings

In our experiment, we choose the set of phases and measurement setting as given in Table 5 to prepare traps on all qubits:

$\|\text{trap}_1\rangle = \|-_i\rangle$:	$\theta_1 = 0,\ \theta_2 = \pi/2,\ \theta_3 = 0,\ \theta_4 = 0$
	$\delta_1 = \delta_{\text{trap}},\ \delta_2 = -\pi/2,\ \delta_3 = \pi,\ \delta_4 = -\pi/2$
$\|\text{trap}_1\rangle = \|+\rangle$:	$\theta_1 = 0,\ \theta_2 = \pi/2,\ \theta_3 = 3\pi/2,\ \theta_4 = 0$
	$\delta_1 = \delta_{\text{trap}},\ \delta_2 = -\pi/2,\ \delta_3 = 5\pi/4,\ \delta_4 = \pi/2$
$\|\text{trap}_2\rangle = \|+\rangle$:	$\theta_1 = 0,\ \theta_2 = \pi/2,\ \theta_3 = \pi,\ \theta_4 = 0$
	$\delta_1 = -\pi/2,\ \delta_2 = \delta_{\text{trap}},\ \delta_3 = 0,\ \delta_4 = 0$
$\|\text{trap}_2\rangle = \|+_i\rangle$:	$\theta_1 = 0,\ \theta_2 = 0,\ \theta_3 = 0,\ \theta_4 = 0$
	$\delta_1 = \pi/2,\ \delta_2 = \delta_{\text{trap}},\ \delta_3 = 0,\ \delta_4 = 0$
$\|\text{trap}_3\rangle = R_z(3\pi/4)\|+\rangle$:	$\theta_1 = 0,\ \theta_2 = \pi/2,\ \theta_3 = 5\pi/4\ ,\ \theta_4 = 0$
	$\delta_1 = \pi,\ \delta_2 = -\pi/2,\ \delta_3 = \delta_{\text{trap}},\ \delta_4 = \pi/2$
$\|\text{trap}_3\rangle = R_z(\pi/4)\|+\rangle$:	$\theta_1 = 0,\ \theta_2 = \pi/2,\ \theta_3 = 7\pi/4\ ,\ \theta_4 = 0$
	$\delta_1 = \pi,\ \delta_2 = 0,\ \delta_3 = \delta_{\text{trap}},\ \delta_4 = -\pi/2$
$\|\text{trap}_4\rangle = \|-\rangle$:	$\theta_1 = 0,\ \theta_2 = \pi/2,\ \theta_3 = \pi/4,\ \theta_4 = 0$
	$\delta_1 = \pi/2,\ \delta_2 = 0,\ \delta_3 = 5\pi/4,\ \delta_4 = \delta_{\text{trap}}$
$\|\text{trap}_4\rangle = \|-_i\rangle$:	$\theta_1 = 0,\ \theta_2 = \pi/2,\ \theta_3 = 3\pi/4,\ \theta_4 = 0$
	$\delta_1 = \pi/2,\ \delta_2 = \pi/2,\ \delta_3 = 7\pi/4,\ \delta_4 = \delta_{\text{trap}}$

Table 5: Blind phases and measurement instructions for the entanglement verification procedure.

nature physics
SUPPLEMENTARY INFORMATION
DOI: 10.1038/NPHYS2763

2 Entanglement verification

As discussed in the main paper we demonstrate how our restricted verification scheme can be exploited for the verification of a non-classical computation, in the form of a measurement of Bell statistics. For a test of Bell's inequality, the certain measurements α, α' and β, β' need to be performed on a two-qubit state $|\psi\rangle_{a,b}$, where α, α' (β, β') are the measurements performed on qubit a (b). If the state $|\psi\rangle_{a,b}$ is entangled, a maximal violation of the Bell inequality of the Clauser-Horne-Shimony-Holt (CHSH)-type,

$$S = |E(\alpha,\beta) - E(\alpha,\beta')| + |E(\alpha',\beta) + E(\alpha',\beta')| \leq 2, \tag{1}$$

can be obtained. Here the correlation coefficients are defined as

$$E(\alpha,\beta) = \frac{C_{00}(\alpha,\beta) - C_{01}(\alpha,\beta) - C_{10}(\alpha,\beta) + C_{11}(\alpha,\beta)}{C_{00}(\alpha,\beta) + C_{01}(\alpha,\beta) + C_{10}(\alpha,\beta) + C_{11}(\alpha,\beta)} \tag{2}$$

and $C_{ij}(\alpha,\beta)$ are the coincidence counts for obtaining measurement results $i = \{0,1\}$ on qubit a and $j = \{0,1\}$ on qubit b for measurements in bases α and β on qubits a and b respectively.

We exploit the framework of blind quantum computing, in order to enable a verifier to perform a blind Bell test. We choose the blind cluster state to be a zigzag cluster state, shown in Figure 1.

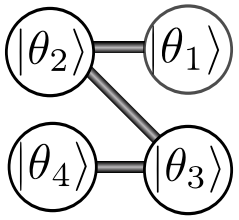
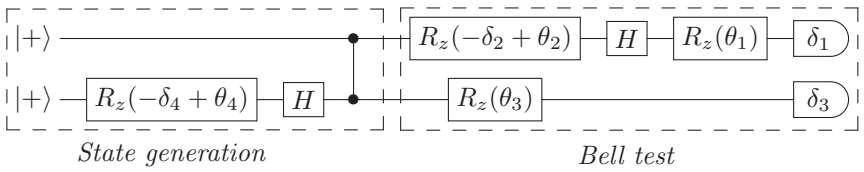


Figure 1: Blind zigzag cluster

The underlying circuit, which is obtained, when measurements in the basis $|\pm_{\delta_j}\rangle = (|0\rangle \pm e^{i\delta_j}|1\rangle)/\sqrt{2}$ are performed on the blind zigzag cluster state with blind qubits being in the state $|\theta_j\rangle$ is given by the circuit below

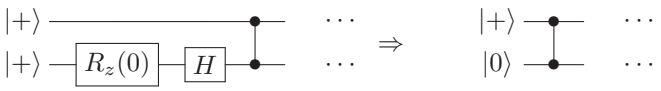


(3)

where $\overset{\bullet}{\underset{\bullet}{\top}}$ denotes a CPhase gate (CPhase$|ij\rangle = (-1)^{ij}|ij\rangle$) and $\boxed{\phi}$ a measurement in the basis $|+_\phi\rangle$. Here, $R_z(\phi) = \exp(-i\phi\sigma_z/2)$, $H = (\sigma_x + \sigma_z)/\sqrt{2}$ and σ_x, σ_y and σ_z denote the usual Pauli matrices.

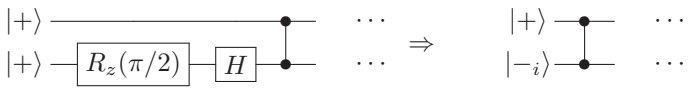
As we will see in the following, a blind Bell test can be implemented by choosing suitable combinations of δ_j and θ_j. For this, the left part of the circuit (shown above) implements the state generation, whereas the right parts realizes the Bell test.

The verifier can choose between entangled states and product states for the Bell test. For example, by choosing $-\delta_4 + \theta_4 = 0$ (or π), the input state will be a product state:



(4)

Alternatively, by choosing $-\delta_4 + \theta_4 = \pi/2$ (or $-\pi/2$), the input state will be an entangled state:



(5)

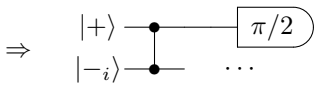
This demonstrates that the verifier can choose between different—product or entangled—input states for the Bell test by choosing different combinations of δ_4 and θ_4. For our demonstration, we exemplarily choose the entangled state to be CPhase$|+\rangle|-_i\rangle$.

In the blind framework, the Bell measurements are determined by the choice of the blind phases θ_1, θ_2, and θ_3 as well as by the measurement settings δ_1, δ_2, and δ_3 on the blind zigzag cluster state. For our demonstration, we choose the Bell measurement angles as given in the main paper.

The Bell settings of α and α' are determined by the choice of $(-\delta_2 + \theta_2)$ and $(\delta_1 - \theta_1)$. For the Bell measurement angle $\alpha = \pi/2$, we choose $\delta_1 - \theta_1 = \pi/2$ and $-\delta_2 + \theta_2 = \pi$.

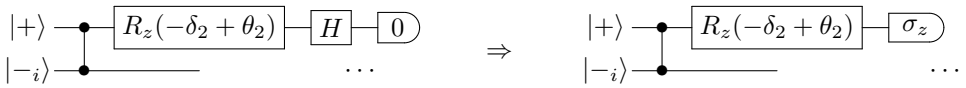
(6)

which leads to a measurement in the basis $\alpha = \pi/2$ in the upper wire:



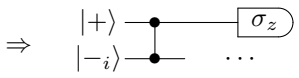
(7)

For the Bell measurement angle $\alpha' = \sigma_z$, we choose $\delta_1 - \theta_1 = 0$. With that configuration, $-\delta_2 + \theta_2$ can have any value, since a $R_z(-\delta_2 + \theta_2)$ rotation does not affect the state $|0\rangle$:



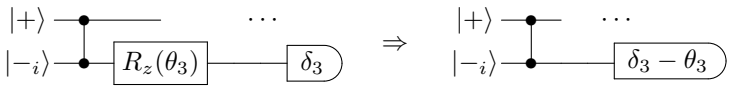
(8)

Finally, we obtain a measurement in the basis $\alpha' = \sigma_z$:



(9)

The angles β and β' are determined by δ_3 and θ_3.



(10)

To choose the Bell settings, $\beta = -3\pi/4$ and $\beta' = -\pi/4$, we simply take $\delta_3 - \theta_3$ to be equal to β or β'.

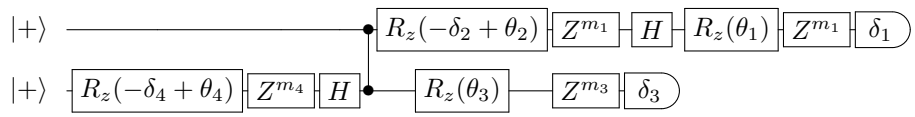
2.1 Experimental measurement settings

In our experiment, we choose the settings given in table 2.1.

Note, that for the second setting α, β' we measure $\alpha + \pi$ and $\beta' + \pi$ instead of α and β'. This has no effect on the Bell inequality since only the measurement outcomes are exchanged ($00 \to 11$, $01 \to 10$, $10 \to 01$, $11 \to 00$). This exchange of the measurements outcomes can be interpreted as the verifier choosing $r_j = 1$. In the blind quantum computing framework, r_j is a randomly chosen value in $\{0, 1\}$ which hides the value of the measurement outcome.

2.2 Bell test verification

In order to show that the Bell test is invariant under errors of the form $A \otimes C \otimes C \otimes A$, as required to show verification in our setting, we note that the circuit implemented by our measurement settings is described by the circuit below.



DOI: 10.1038/NPHYS2763

α, β:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = 3\pi/4$, $\theta_4 = 0$
	$\delta_1 = \pi/2$, $\delta_2 = -\pi/2$, $\delta_3 = 0$, $\delta_4 = -\pi/2$
α, β':	$\theta_1 = 0$, $\theta_2 = 0$, $\theta_3 = 3\pi/4$, $\theta_4 = 0$
	$\delta_1 = \pi/2$, $\delta_2 = 0$, $\delta_3 = -\pi/2$, $\delta_4 = -\pi/2$
α',β:	$\theta_1 = 0$, $\theta_2 = \pi/2$, $\theta_3 = \pi/4$, $\theta_4 = 0$
	$\delta_1 = 0$, $\delta_2 = -\pi/2$, $\delta_3 = -\pi/2$, $\delta_4 = -\pi/2$
α', β':	$\theta_1 = 0$, $\theta_2 = 0$, $\theta_3 = \pi/4$, $\theta_4 = 0$
	$\delta_1 = 0$, $\delta_2 = 0$, $\delta_3 = 0$, $\delta_4 = -\pi/2$

Table 6: Blind phases and measurement instructions for the preparation of a set of trap qubits

Note that an error of this form flips both m_1 and m_4. The effect of flipping m_1 is trivially identical to flipping the outcome of the first logical qubit in the Bell test. Although it is not immediately obvious, we note that since $Z^{m_1} R_Z(-\delta_4 + \theta_4) = R_Z(\pm\frac{\pi}{2})$ and $HZR_Z(\pm\frac{\pi}{2})|+\rangle = ZHR_Z(\pm\frac{\pi}{2})|+\rangle$, a bit flip error on m_4 leads to a bit flip error in the outcome of the measurement result for the second logical qubit. Thus all errors of the form $A \otimes C \otimes C \otimes A$ flip the outcome of both measurements in a Bell test. However, we note that the outcome of the Bell test depends only on the parity of these two measurements, and hence any inferred value of the CHSH quantity is left unchanged by such errors.

References

[1] Fitzsimons, J. and Kashefi, E. *arXiv:1203.5217* (2012).