Demonstration of Blind Quantum Computing

Stefanie Barz *et al.*

Science **335**, 303 (2012);
DOI: 10.1126/science.1214707

Science (print ISSN 0036-8075; online ISSN 1095-9203) is published weekly, except the last week in December, by the American Association for the Advancement of Science, 1200 New York Avenue NW, Washington, DC 20005.

Demonstration of Blind Quantum Computing

Stefanie Barz,[1,2]* Elham Kashefi,[3] Anne Broadbent,[4,5] Joseph F. Fitzsimons,[6,7] Anton Zeilinger,[1,2] Philip Walther[1,2]

Quantum computers, besides offering substantial computational speedups, are also expected to preserve the privacy of a computation. We present an experimental demonstration of blind quantum computing in which the input, computation, and output all remain unknown to the computer. We exploit the conceptual framework of measurement-based quantum computation that enables a client to delegate a computation to a quantum server. Various blind delegated computations, including one- and two-qubit gates and the Deutsch and Grover quantum algorithms, are demonstrated. The client only needs to be able to prepare and transmit individual photonic qubits. Our demonstration is crucial for unconditionally secure quantum cloud computing and might become a key ingredient for real-life applications, especially when considering the challenges of making powerful quantum computers widely available.

Among many quantum-enhanced applications, quantum computing has generated much interest because of the discovery of applications (*1*–*4*) that outperform their best-known classical counterparts. Although vast technological developments already allow for small-scale quantum computers with ionic (*5*–*8*), photonic (*9*–*16*), superconducting (*17*–*21*), and solid-state (*22*–*24*) systems, the hurdles encountered in realizing quantum devices are enormous. This intrinsic technical complexity may result in, initially, only a few powerful quantum computers, or quantum servers, operating at specialized facilities. A key challenge in using such central quantum computers is enabling a quantum computation on a remote server while keeping the client's data hidden from the server (*25*–*30*).

The classical analog of this issue was addressed in 1978 (*31*) and became one of the most active fields in cryptography. A full solution was over 30 years in the making and enables (*32*) the evaluation of data-processing circuits over encrypted data without the need for any decryption, but provides only computational security. In analogy to many widely used cryptographic protocols, this means that the security relies on the assumption of a limit to the adversary's computational power, as well as on the difficulty of the underlying mathematical problem.

Recent theoretical work (*29*) overcomes this limitation and shows that quantum computers can provide unconditional security in data processing, a hitherto unrecognized potential of quantum computers that is not known to be achievable classically. This new fundamental advantage of quantum computers is manifested in the blind quantum computing (BQC) protocol that combines notions of quantum cryptography and quantum computation to achieve the delegation of a quantum computation from a client with no quantum computational power to an untrusted quantum server, such that the client's data remains perfectly private.

BQC uses the concept of one-way quantum computing (*33*–*37*), a measurement-based model of computation (*38*, *39*) that represents a paradigm shift in the understanding of complex data processing by clearly separating the classical and quantum parts of a computation. In the most general case, a one-way quantum computer has its basis in highly entangled multiparticle states, so-called cluster states, which are a resource for universal quantum computing. On these cluster states, adaptive single-qubit measurements alone are sufficient to implement deterministic universal quantum computation. Different algorithms require only a different pattern of single-qubit measurements on a sufficiently large cluster state.

Therefore, a quantum computation is hidden as long as these measurements are successfully hidden. In order to achieve this, the BQC protocol exploits special resources called blind cluster states that must be chosen carefully to be a generic structure that reveals nothing about the underlying computation (Fig. 1). These blind cluster states are multiparticle entangled states created by preparing qubits in $|\theta_j\rangle = 1/\sqrt{2}(|0\rangle + e^{i\theta_j}|1\rangle)$, where $|0\rangle$ and $|1\rangle$ are the computational basis of the physical qubits and θ_j is chosen uniformly at random from $\{0, \pi/4, \ldots, 7\pi/4\}$, and then interacting each qubit via controlled-phase (CPhase) gates with its nearest neighbors (here, CPhase $|i\rangle|j\rangle \mapsto (-1)^{ij}|i\rangle|j\rangle$ with $i, j \in \{0, 1\}$). Similar to the one-way quantum computer, a blind computation is described by a pattern of consecutive adaptive single-qubit measurements. Measuring the first qubit, initially in state $|\theta_1\rangle$, of a one-dimensional linear blind cluster in the basis $|\pm_{\delta_1}\rangle = 1/\sqrt{2}(|0\rangle \pm e^{i\delta_1}|1\rangle)$ has the effect of applying a single-qubit rotation $R_z(-\delta_1 + \theta_1)$ on

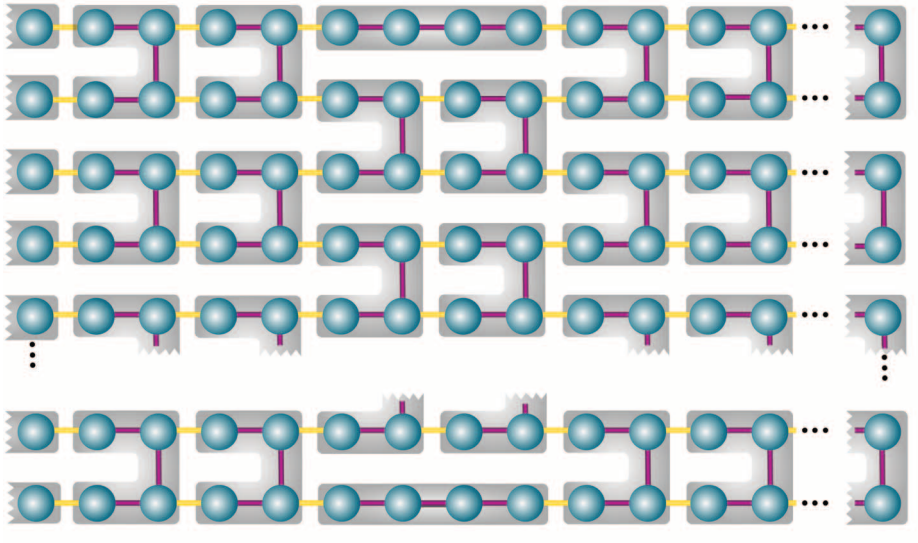

Fig. 1. The universal blind cluster state for BQC. This family of cluster states can be built by joining (yellow edges), for example, using optical fusion operations, smaller cluster states (purple edges, gray background) that are in one of the configurations of $|\Phi^{\theta}\rangle$ as implemented in the laboratory. The resulting state allows universal blind quantum computation when combined with measurements in the basis $|\pm_{\delta}\rangle$, $\delta \in \{0, \pi/4, \ldots 7\pi/4\}$.

[1]Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria. [2]Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria. [3]School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK. [4]Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada. [5]Department of Combinatorics and Optimization, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada. [6]Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, 117543 Singapore. [7]School of Physics, University College Dublin, Belfield, Dublin 4, Ireland.

*To whom correspondence should be addressed. E-mail: stefanie.barz@univie.ac.at

the encoded input state $|+\rangle$, followed by a Hadamard, H. 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 long as the angle θ_1 of the rotated qubit is unknown, the real rotation remains secret.

This feature of blind cluster states is used to perform a delegated computation on a server such that all data and the whole computation remain hidden. The only quantum power that is required from the client is the preparation of each qubit j in a state $|\theta_j\rangle$ and the transmission of the qubits to the server; in particular, there is no need for any quantum memory (*40*) or ability to perform quantum gates. From this point on in the protocol, the client communicates only measurement instructions and can be considered completely classical. The quantum server, which can perform universal quantum computation, performs a CPhase gate between qubits received from the client. Then in each round of interaction, the server performs adaptive single-qubit measurements in the $|\pm_{\delta_j}\rangle$ basis, as instructed by the client. The measurement basis is chosen such that $\delta_j = \phi_j + \theta_j + \pi r_j$, where ϕ_j is the desired target rotation and r_j is a randomly chosen value in {0, 1} that hides the value of the measurement outcome. These classical measurement angles are set in such a way to compensate for the initial random rotation θ_j and any other Pauli by-products (*12*, *41*) produced by previous measurements.

We present an optimized version of the original protocol that uses photonic qubits. Photons are ideally suited for BQC because they provide the natural choice as quantum information carrier for the client and enable quantum computing for the server. This is a unique feature of photonic systems and so far not realizable in other quantum systems. We experimentally demonstrate the concept of BQC via a series of blind computations on four-qubit blind cluster states. These photonic states can be combined via optical gates to create a universal resource state for BQC (Fig. 1) (*29*).

Our protocol uses, compared with the original BQC proposal (*29*), the experimental resources in an optimized way, independent of the physical system and without affecting blindness.

Optimized BQC. It is a conceptual strength of the BQC protocol that perfect security can be established over a subset of computations even if not all of the qubits are unknown to the server. For the four-qubit blind cluster state, it is sufficient for the client to be able to prepare only one or two of the qubits in arbitrary states $|\theta_j\rangle$ for delegating various one- and two-qubit circuits as well as quantum algorithms (Fig. 2). This is a remarkable optimization for the experimental requirements and is demonstrated here [see supporting online material (SOM) section S1 for theoretical details]. Furthermore, this optimization is scalable beyond our four-qubit experimental setting and creates an interesting challenge on the design level to construct a computation such that the sensitive measurements remain hidden.

We thus fix θ_1 and θ_4 equal to zero while varying the choices of θ_2 and θ_3. The resulting four-qubit linear blind cluster state is

$$|\Phi^{\hat{\theta}}\rangle = \frac{1}{2}\left[|+00+\rangle_{1234} + e^{i\theta_3}|+01-\rangle_{1234} + e^{i\theta_2}|-10+\rangle_{1234} - e^{i(\theta_2+\theta_3)}|-11-\rangle_{1234}\right] \quad (1)$$

where $\hat{\theta} = (n_2, n_3)$ and $(\theta_2, \theta_3) = \left(\frac{n_2\pi}{4}, \frac{n_3\pi}{4}\right)$. Our experimental implementation of BQC has its basis in such a family of four-qubit linear blind cluster states. These are produced by using photon emissions of a non-collinear type-II spontaneous parametric down-conversion process (SPDC) (*10*, *42*) (SOM sections S3 and S4). If four photons are emitted into the output modes of the polarizing beam splitters 1, 2, 3, and 4 (Fig. 3A), they are in a highly entangled state that is equivalent to the state $|\Phi^{\hat{\theta}}\rangle$ under the local unitary operation $H \otimes \mathbf{I} \otimes \mathbf{I} \otimes H$:

$$|\Phi_L^{\hat{\theta}}\rangle = \frac{1}{2}\left[|0000\rangle_{1234} + e^{i\theta_3}|0011\rangle_{1234} + e^{i\theta_2}|1100\rangle_{1234} - e^{i(\theta_2+\theta_3)}|1111\rangle_{1234}\right] \quad (2)$$

We use the polarization of photons to represent the qubits, with $|0\rangle$ denoting the horizontal polarization state and $|1\rangle$ denoting the vertical polarization state.

The client prepares the value of θ_j, which is done in our case by a human client. By aligning our setup to produce $|\Phi_L^{(2,n)}\rangle$ for $n = 0, \ldots, 7$ and $|\Phi_L^{(6,m)}\rangle$ for $m = 0, 4$, we have demonstrated the preparation of various four-qubit blind cluster states. Moreover, we have implemented 1962 different four-qubit measurements, chosen from a list of measurement settings, with 31,392 measured outcomes. These measurements outcomes can be seen as implementing all possible computational branches (because of different measurement outcomes), which is equivalent to directly performing the feedforward mechanism (*12*). However, a feature of the BQC protocol is that the client's privacy is always preserved, whether or not feedforward mechanisms have been implemented. Similarly, obtaining all the possible measurement outcomes is equivalent to implementing all possible values of r_j as if the client randomly re-interprets the measurement outcomes, implicitly subsuming r_j. Note that, whenever all qubits are measured in our

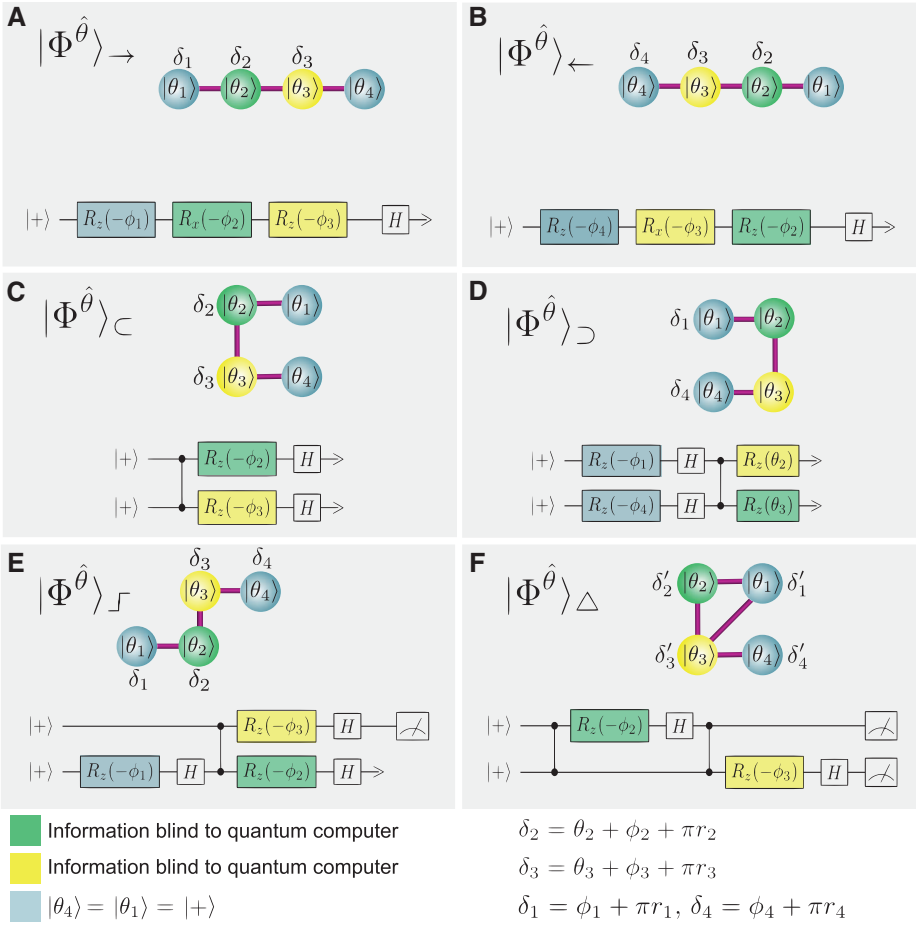

Fig. 2. Blind circuits and corresponding measurement patterns. (**A** to **F**) We implement various types of blind computations by using different configurations for $|\Phi^{\hat{\theta}}\rangle$. For all implementations, θ_2 and θ_3 are blind, as has been demonstrated in the experiment. The angles θ_1 and θ_4 are fixed to be zero. The measurement angle δ_j, as instructed by the client, depends on the initial rotation of the qubit θ_j (unknown to the server), the target rotation ϕ_j, and a randomly chosen value r_j in {0, 1}.

setup, this method allows the client's choice of configuration to also be hidden from the server.

We use an overcomplete state tomography for each of our cluster states in order to reconstruct the four-qubit density matrix (SOM section S5). The most likely physical density matrix for each four-qubit state is extracted by using a maximum-likelihood reconstruction (*43*) (Fig. 3B). Uncertainties in quantities extracted from these density matrices are calculated by using a Monte Carlo routine and assumed Poissonian errors. Our computed fidelities for the various blind cluster states achieve maximum values of up to 0.679 ± 0.004% via local unitary transformation. These nonideal fidelities arise because of experimental imperfections (SOM section S4). Experimental influences on the server's side only affect the correctness of the computation, whereas imperfections in the client's qubit preparation might also weaken the assumption of an unbiased state distribution.

Blind single- and two-qubit unitaries. The four-qubit linear blind cluster $|\Phi^{\hat{\theta}}\rangle_{\rightarrow}$ (Fig. 2) can be used to implement an arbitrary single-qubit unitary gate. Measuring qubit 1 in the eigenstates of σ_x, σ_y, or σ_z has the effect of preparing the input on qubit 2 in the state $|0\rangle$, $|+_i\rangle$, or $|+\rangle$, respectively, where $|+_i\rangle = 1/\sqrt{2}(|0\rangle + i|1\rangle)$. We are thus left with a three-qubit linear cluster state that implements a single-qubit rotation gate with rotations determined by the measurements of the second and third qubits; this rotates the input qubit $|\Psi_{in}\rangle$ to the final state $|\Psi_{out}\rangle = R_x(-\phi_3)R_z(-\phi_2)|\Psi_{in}\rangle$, where $R_x(\alpha) = \exp(-i\alpha\sigma_x/2)$. By fixing θ_2 and varying θ_3, we can demonstrate a blind X rotation. In the same way, a blind Z rotation can be achieved by using the four-qubit linear blind cluster state $|\Phi^{\hat{\theta}}\rangle_{\leftarrow}$, which has the order of measurements going from qubit 4 down to qubit 1. Figure 3C depicts a blind Z rotation. By varying θ_3 and averaging over all resulting density matrices, we obtain a totally mixed state with a linear entropy of 0.989 ± 0.010 that is close to the entropy of 1 for a perfectly mixed state (Fig. 3C). Because the experiments include the preparation of all eight blind cluster states $|\Phi_L^{(2,n)}\rangle$, we can quantify the blindness of the single-qubit rotations demonstrated experimentally. The value of the Holevo information χ (see SOM section S2 for details) must then be between 0 (for perfect blindness) and 3 (for no blindness). By using the tomographic measurements performed on these input states, we determine χ of such states to be 0.169 ± 0.074, far below the three bits necessary to uniquely identify the client's choice of ϕ_2 and ϕ_3, proving that within the assumptions of our model these experimental implementations of the protocol maintains close to perfect blindness. The above value of χ assumes the initial state is chosen uniformly at random. However, even when this value is maximized over all possible prior distributions on the choice of states, it increases only slightly to 0.185 ± 0.087.

Two-qubit gates are required for universal quantum computation; by choosing the order of measurements in a suitable way, the blind cluster $|\Phi^{\hat{\theta}}\rangle$ implements blind two-qubit gates (Fig. 2, C to F). One family of two-qubit gates generated in our experiment has its basis in the blind horseshoe cluster $|\Phi^{\hat{\theta}}\rangle_{\subset}$, where measuring qubits 2 and 3 of the blind cluster state performs a transformation on the logical input qubits (Fig. 2C). Both implemented rotations are blind, and the entire computation remains hidden. Analyzing the output state, that is, measuring qubits 1 and 4, delivers the result of the computation. Figure 3D shows an example of a two-qubit computation using the blind horseshoe cluster. Consistency with blindness can be seen by averaging over all output states, giving as a result a totally mixed state with a linear entropy of 0.955 ± 0.011. It is an interesting challenge to demonstrate the consistency with blindness in full generality by producing 64 blind cluster states. Our demonstration uses a selection of four states, which suffices to hide the choice of rotations among four possibilities:

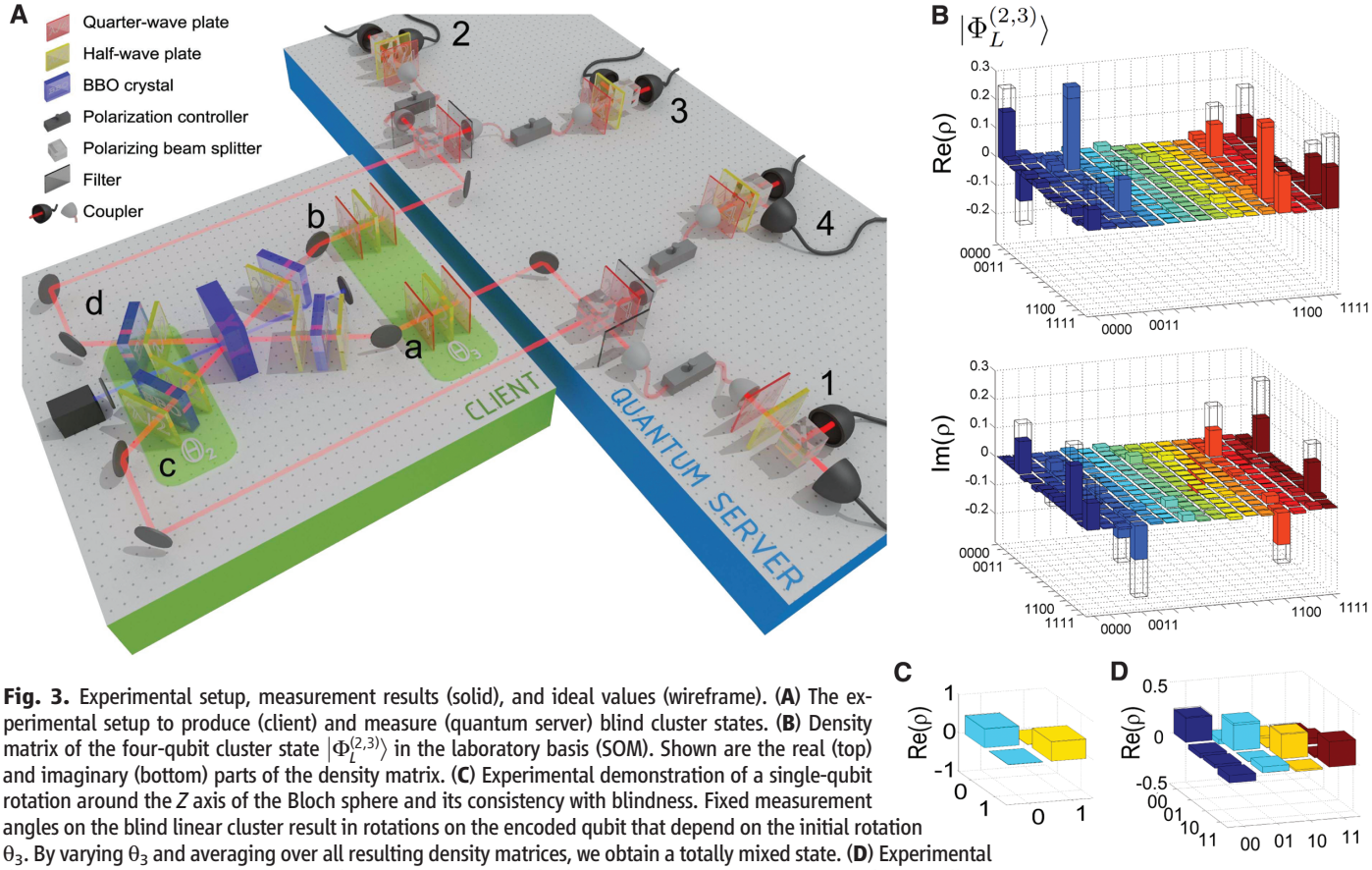

Fig. 3. Experimental setup, measurement results (solid), and ideal values (wireframe). (**A**) The experimental setup to produce (client) and measure (quantum server) blind cluster states. (**B**) Density matrix of the four-qubit cluster state $|\Phi_L^{(2,3)}\rangle$ in the laboratory basis (SOM). Shown are the real (top) and imaginary (bottom) parts of the density matrix. (**C**) Experimental demonstration of a single-qubit rotation around the Z axis of the Bloch sphere and its consistency with blindness. Fixed measurement angles on the blind linear cluster result in rotations on the encoded qubit that depend on the initial rotation θ_3. By varying θ_3 and averaging over all resulting density matrices, we obtain a totally mixed state. (**D**) Experimental demonstration of a two-qubit gate and its consistency with blindness. Fixing measurements at a subset of all 64 possible states and averaging over all output density matrices results in a totally mixed state. The imaginary part of the density matrices (C and D) is below 0.05 and hence not shown. For details, see figs. S36 and S42.

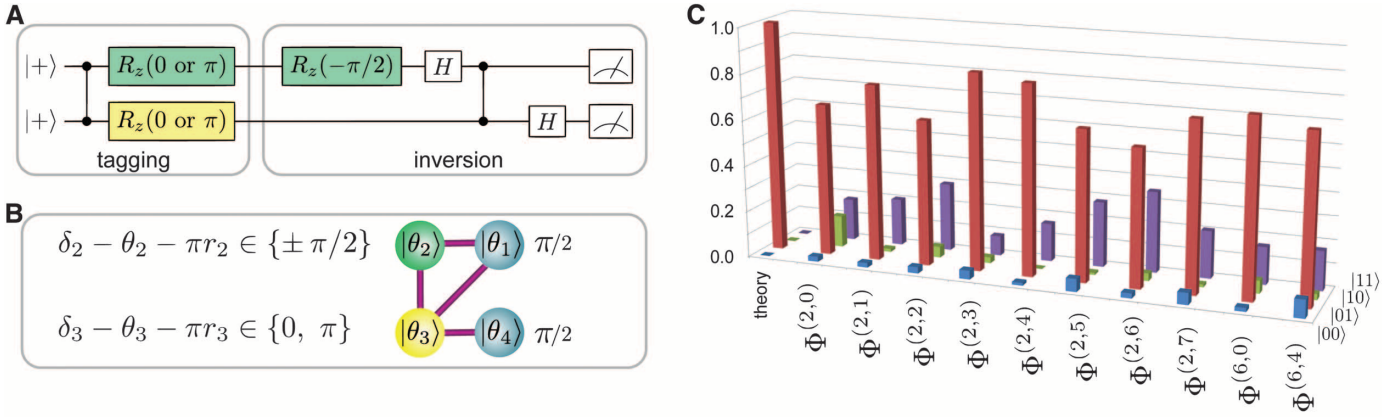

Fig. 4. Blind implementation of Grover's algorithm. (**A**) Quantum circuit. The input to the circuit is $|+\rangle|+\rangle$; the tagging of one of the four input states $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$ applies a phase shift of π to that state. These four states are then mapped to an output that is measured in the basis ($|+_i\rangle$, $|-_i\rangle$). (**B**) Corresponding implementation on a triangle cluster $|\Phi^{\hat{\theta}}\rangle_\Delta$. Here, the measurement of qubits 2 and 3 corresponds to the tagging of one of the elements, measuring the output qubits 1 and 4 identifies then which input was tagged. Without the knowledge of the initial rotation of the qubit, the quantum server is unable to distinguish the algorithm from a given family of circuits. (**C**) Measurement outcomes for tagging the $|01\rangle$ element for all states $|\Phi^{(n_2,n_3)}\rangle_\Delta$ are shown. The corresponding error bars are smaller than 0.056 for all results.

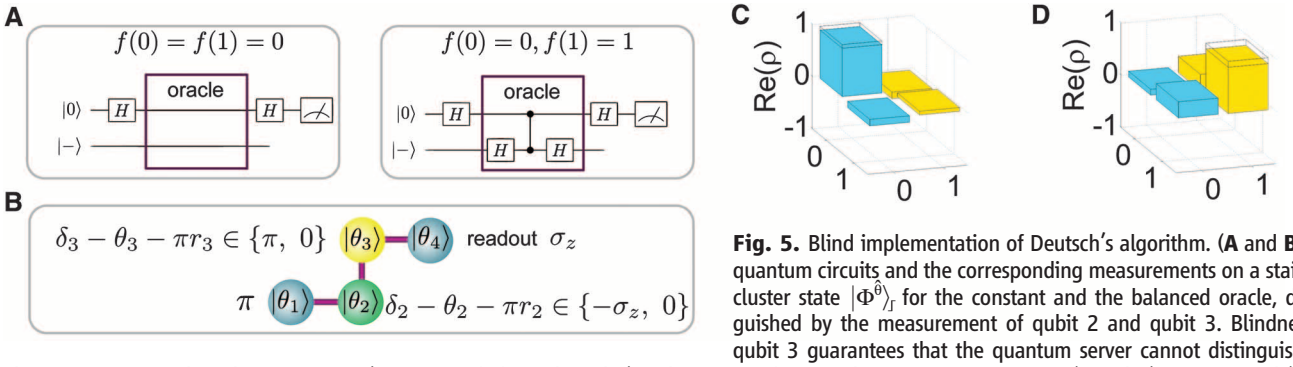

Fig. 5. Blind implementation of Deutsch's algorithm. (**A** and **B**) The quantum circuits and the corresponding measurements on a staircase cluster state $|\Phi^{\hat{\theta}}\rangle_\Gamma$ for the constant and the balanced oracle, distinguished by the measurement of qubit 2 and qubit 3. Blindness of qubit 3 guarantees that the quantum server cannot distinguish between the execution of each of these scenarios (constant or balanced oracles) and corresponding families of quantum circuits. (**C** and **D**) Experimental (solid) and theoretical (wireframe) results for a constant (C) and a balanced (D) oracle for the example of the state $|\Phi^{(6,4)}\rangle_\Gamma$.

$R_z(\pi/2 \pm \pi) \otimes R_z(\pi/2 \pm \pi)$. In a similar way, the consistency with blindness of the rotated horseshoe cluster $|\Phi^{\hat{\theta}}\rangle_\supset$ (Fig. 2D) can be shown (SOM section S10). We also realize blind computations based on the blind staircase cluster $|\Phi^{\hat{\theta}}\rangle_\Gamma$ (Fig. 2E) and blind triangle cluster $|\Phi^{\hat{\theta}}\rangle_\Delta$ (Fig. 2F). The state $|\Phi^{\hat{\theta}}\rangle_\Delta$ is obtained via local complementation (*44*) on qubit 2 of $|\Phi^{\hat{\theta}}\rangle_\subset$. Thus $U|\Phi^{\hat{\theta}}\rangle_\Delta = |\Phi^{\hat{\theta}}\rangle_\subset$, where $U = \sqrt{\sigma_z} \otimes \sqrt{\sigma_x} \otimes \sqrt{\sigma_z} \otimes I$ (with U acting on qubits ordered as 1, 2, 3, and 4), and measuring the qubits of $|\Phi^{\hat{\theta}}\rangle_\subset$ by absorbing the action of U into the measurements yields a computation on $|\Phi^{\hat{\theta}}\rangle_\Delta$ as represented by measurement instructions δ′ (Fig. 2F). However, blindness on qubit i is guaranteed only if the resulting measurement can be expressed as a basis $|\pm_{\delta_i'}\rangle$. We will show that the blind staircase cluster allows for the blind implementation of Deutsch's algorithm, whereas the blind triangle cluster allows for the blind implementation of Grover's algorithm.

To demonstrate the quality of our gate operations, we performed various single-qubit gates and two-qubit gates with each of the blind cluster states; the resulting density matrices, obtained via quantum state tomography, are shown in SOM sections S6 and S7.

Blind algorithms. One of the most prominent examples where quantum mechanics demonstrates its superiority in computational speedup is Grover's search algorithm (*3*, *45*), which provides a quadratic speedup to the following problem: Given a function f: $\{0,1\}^n \rightarrow \{0,1\}$, find an x such that $f(x) = 1$. We demonstrate a blind implementation of Grover's search for $n = 2$, where blindness ensures that the server is unable to distinguish the actual computation from within a given family of circuits implementing $[I \otimes R_z(\xi)H]$. Whereas previous realizations (*10*, *12*) are not amenable to blind implementations, our computation, embedded into the blind triangle cluster $|\Phi^{\hat{\theta}}\rangle_\Delta$ (Fig. 2F), remains blind. The algorithm proceeds as follows: The values of x are represented by the states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, respectively. A superposition of all four states is initially created, and the oracle tags one element by applying a phase of π, thus flipping the sign of this term (Fig. 4A). Then each of the four states is mapped to an output such that measuring both qubits in the basis $|\pm_i\rangle$ reveals the tagged item. This computation can be embedded into the blind triangle cluster, $|\Phi^{\hat{\theta}}\rangle_\Delta$ (Fig. 2F); the choice of ϕ_2 and ϕ_3 determines which element is tagged. Figure 4C shows the results of a Grover search for the tagging of the state $|01\rangle$. For each blind cluster state, we show the probability of identifying the tagged state as well as the probabilities of finding the unwanted states, because of the experimental noise. We achieve probabilities of finding these positive events of up to 0.850 ± 0.039 with an average over all blind states of 0.720 ± 0.015. No classical algorithm can succeed in this scenario with probability higher than 0.5.

Another algorithm that demonstrates the power of quantum computing is the Deutsch-Josza algorithm (*2*) that takes as input an oracle (or black box) for computing an unknown function f: $\{0,1\}^n \rightarrow \{0,1\}$ with the promise that f is either constant, meaning $f(x)$ is the same for all x, or balanced, meaning $f(x) = 0$ for exactly half of the inputs x and $f(x) = 1$ for the other half. The algorithm determines whether f is constant or balanced by making queries to the oracle. Whereas the best possible classical algorithm to solve this problem uses at least $2^{n-1} + 1$ queries in the worst case, the Deutsch-Jozsa algorithm takes advantage of quantum superposition and interference to determine whether f is constant or balanced with only one query. In contrast to previously realized

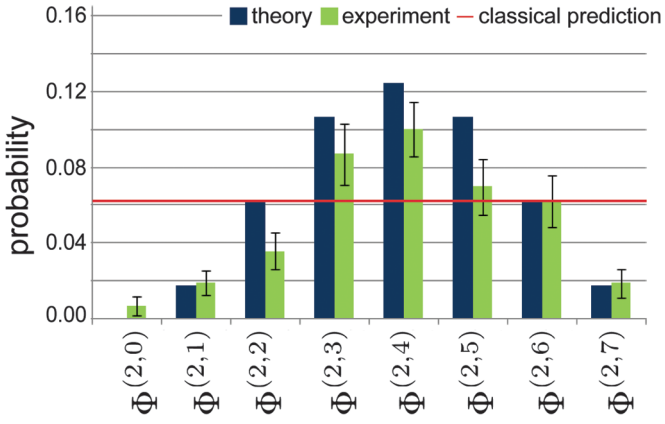

Fig. 6. Testing of the quantum server. By measuring the probability distributions of a fixed measurement setting for all blind cluster states and comparing them with the theoretical expectations, the client can find out whether the server possesses any quantum technology. For example, fixing the measurement settings to $\delta_1 = -\sigma_z$, $\delta_2 = \pi$, $\delta_3 = -\pi/2$, and $\delta_4 = \pi/2$ leads to different theoretical (blue) and experimental (green) probability distributions dependent on the underlying blind cluster state. A pure classical server guesses every outcome with the same probability (1/16) and can be detected in this way (red line). Conservatively, we show Poissonian errors, which constitute a lower limit for the experimental error because of imperfections in the state generation (SOM section S4).

implementations of Deutsch's algorithm using traditional cluster states (*16*, *46*), we exploit blind staircase cluster states $|\Phi^{\hat{\theta}}\rangle_\Gamma$ for the implementation of this quantum algorithm for the case $n = 1$. Figure 5A shows the quantum circuits that realize oracles corresponding to constant and balanced functions. The corresponding implementation on $|\Phi^{\hat{\theta}}\rangle_\Gamma$ is given in Fig. 5B, where the choice of oracle is done by fixing the measurement on qubits 2 and 3. Blindness of qubit 3 guarantees that the quantum server will not recognize the implementation of a constant oracle from the Grover algorithm or general circuits implementing $R_z(\xi)H \otimes I$ and a balanced oracle from $(I \otimes H)$ CPhase$[R_z(\xi)H \otimes H]$ (Fig. 5). Figure 5, C and D, shows the outcome of our measurement for the case of $|\Phi^{(6,4)}\rangle_\Gamma$. A tomography of the state of qubit 4 is performed in order to fully characterize the output of the computation. In this case, the obtained fidelity for the output state is $F = 0.930 \pm 0.025$ for the constant oracle and $F = 0.887 \pm 0.033$ for the balanced oracle, with the algorithm producing the correct result with probabilities 0.899 ± 0.006 for the constant and 0.895 ± 0.022 for the balanced oracle.

Toward verifying the quantumness. Self-testing is a verification process for the operations of a collection of untrusted quantum devices (*47*, *48*); a key application of the blind computing protocol is also toward such verification of quantum devices (*29*, *30*). We demonstrate a notion of verification that can be used as a heuristic probabilistic test for whether the server indeed possesses any quantum technology or is a completely classical device. For this, the client chooses a measurement setting for which, for each measurement outcome, there exists a state with a detection probability of zero. Because of blindness, however, the quantum server has no information about which initial states the client has prepared. If it has no quantum technology in hand, it attempts to use its classical devices and guesses the outcome for the client's computation wrong with probability at least 1/8. Better bounds can be achieved by using statistics of several rounds and comparing it with the known theoretical statistics to test whether the quantum-computing server is producing the expected outcome or not.

The testing procedure uses statistics of several outcomes for different measurement instructions. Figure 6 shows relevant theoretical predictions as well as experimental outcomes that confirm the quantum nature of the server. By instructing the quantum server to measure, for example, this statistical distribution, the client can see whether the outcomes coincide with the expectations. Our demonstration is a first step toward an efficient verification scheme for quantum technology and acts as an experimental benchmark for future fault-tolerant protocols using more qubits that are expected to enable the detection of a cheating quantum server with probability exponentially close to one.

Discussion. The blind quantum computation protocol demonstrated here is most naturally viewed in the context of measurement-based quantum computation. The required operations, however, can be implemented in any model of computation that is universal for quantum computation on unencoded data and allows intermediate measurements. Finding extensions to other models, such as the adiabatic model, remains an open question.

From our proof-of-principle experiment to a full implementation of the BQC scheme, there are several technical challenges to be faced: Emitted photons that do not contribute to the generation of the cluster state can in principle reveal information about the blind phases. Furthermore, postselection and photon losses decrease the efficiency of the protocol. Therefore, the realization of single-qubit states on demand and the heralded generation of blind cluster states using measurement-induced interactions with high fidelity and low losses will be crucial for future applications. In our experiment, the blind angles were chosen by the human client, and the measurement settings were selected from a prepared list. Ideally, the source of randomness should be carefully scrutinized to avoid any correlations with the server, and an efficient shot-by-shot randomization should be implemented. Considering the photon rates in our experiment, the realization of full randomization for each measurement is a major challenge. The question of how far imbalances and deviations from the uniform distribution can be acceptable is a topic of current research.

Our experiment is a step toward unconditionally secure quantum computing in a client-server environment where the client's entire computation remains hidden, a functionality not known to be achievable in the classical world. This should present an important privacy-preserving technique in future quantum computing networks or clouds (*49*). Especially considering the tremendous challenges encountered in making quantum computers widely available, such future networks could consist of a few powerful quantum-computer nodes. The only quantum requirement for the clients would be to communicate with the nodes via quantum links enabling the transfer of arbitrary qubits. Although photonic quantum systems seem to be ideally suited for privacy-preserving quantum computing, we stress that our results are applicable to any physical implementation of qubits and that in the near future the precise quantum control of multiqubit quantum systems (*50*) will allow for implementing more complex algorithms.

References and Notes

1. R. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).
2. D. Deutsch, R. Jozsa, *Proc. R. Soc. London Ser. A* **439**, 553 (1992).
3. L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, G. L. Miller, Ed. [Association for Computing Machinery (ACM), New York, 1996], pp. 212–219.
4. P. W. Shor, *SIAM J. Comput.* **26**, 1484 (1997).
5. J. I. Cirac, P. Zoller, *Phys. Rev. Lett.* **74**, 4091 (1995).
6. C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, D. J. Wineland, *Phys. Rev. Lett.* **75**, 4714 (1995).
7. D. Kielpinski, C. Monroe, D. J. Wineland, *Nature* **417**, 709 (2002).
8. K. Kim *et al.*, *Nature* **465**, 590 (2010).
9. J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, D. Branning, *Nature* **426**, 264 (2003).
10. P. Walther *et al.*, *Nature* **434**, 169 (2005).
11. N. Kiesel *et al.*, *Phys. Rev. Lett.* **95**, 210502 (2005).
12. R. Prevedel *et al.*, *Nature* **445**, 65 (2007).
13. C.-Y. Lu *et al.*, *Nat. Phys.* **3**, 91 (2007).
14. Y. Tokunaga, S. Kuwashiro, T. Yamamoto, M. Koashi, N. Imoto, *Phys. Rev. Lett.* **100**, 210501 (2008).
15. R. Kaltenbaek, J. Lavoie, B. Zeng, S. Bartlett, K. Resch, *Nat. Phys.* **6**, 850 (2010).
16. G. Vallone, G. Donati, N. Bruno, A. Chiuri, P. Mataloni, *Phys. Rev. A* **81**, 50302 (2010).
17. Y. Makhlin, G. Schön, A. Shnirman, *Rev. Mod. Phys.* **73**, 357 (2001).
18. T. Yamamoto, Y. A. Pashkin, O. Astafiev, Y. Nakamura, J. S. Tsai, *Nature* **425**, 941 (2003).
19. M. Neeley *et al.*, *Science* **325**, 722 (2009).
20. L. DiCarlo *et al.*, *Nature* **460**, 240 (2009).
21. R. Bialczak *et al.*, *Nat. Phys.* **6**, 409 (2010).
22. J. Berezovsky, M. H. Mikkelsen, N. G. Stoltz, L. A. Coldren, D. D. Awschalom, *Science* **320**, 349 (2008).
23. I. Fushman *et al.*, *Science* **320**, 769 (2008).
24. R. Hanson, D. D. Awschalom, *Nature* **453**, 1043 (2008).
25. A. Childs, *Quantum Inf. Comput.* **5**, 456 (2005).
26. P. Arrighi, L. Salvail, *Int. J. Quantum Inf.* **4**, 883 (2006).

27. V. Giovannetti, S. Lloyd, L. Maccone, *Phys. Rev. Lett.* **100**, 230502 (2008).
28. F. De Martini *et al.*, *Phys. Rev. A* **80**, 10302 (2009).
29. A. Broadbent, J. Fitzsimons, E. Kashefi, in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 2009), pp. 517–526.
30. D. Aharonov, M. Ben-Or, E. Eban, in *Proceeding of Innovations in Computer Science* (Tsinghua Univ. Press, Beijing, 2010), p. 453.
31. R. Rivest, L. Adleman, M. Dertouzos, in *Foundations of Secure Computation*, R. DeMillo, D. Dobkin, A. Jones, R. Lipton, Eds. (Academic Press, New York, 1978), pp. 169–180.
32. C. Gentry, in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, M. Mitzenmacher, Ed. (ACM, New York, 2009), pp. 169–178.
33. R. Raussendorf, H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
34. R. Raussendorf, D. E. Browne, H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
35. V. Danos, E. Kashefi, P. Panangaden, *J. ACM* **54**, 8 (2007).
36. D. Gross, J. Eisert, N. Schuch, D. Perez-Garcia, *Phys. Rev. A* **76**, 052315 (2007).
37. H. Briegel, D. Browne, W. Dür, R. Raussendorf, M. Van den Nest, *Nat. Phys.* **5**, 19 (2009).
38. D. Gottesman, I. L. Chuang, *Nature* **402**, 390 (1999).
39. E. Knill, R. Laflamme, G. J. Milburn, *Nature* **409**, 46 (2001).
40. M. P. Hedges, J. J. Longdell, Y. Li, M. J. Sellars, *Nature* **465**, 1052 (2010).
41. V. Danos, E. Kashefi, *Phys. Rev. A* **74**, 052310 (2006).
42. P. G. Kwiat *et al.*, *Phys. Rev. Lett.* **75**, 4337 (1995).
43. D. F. V. James, P. G. Kwiat, W. J. Munro, A. G. White, *Phys. Rev. A* **64**, 52312 (2001).
44. M. Van den Nest, J. Dehaene, B. De Moor, *Phys. Rev. A* **69**, 022316 (2004).
45. M. Boyer, G. Brassard, P. Høyer, A. Tapp, *Fortschr. Phys.* **46**, 493 (1998).
46. M. S. Tame *et al.*, *Phys. Rev. Lett.* **98**, 140501 (2007).
47. F. Magniez, D. Mayers, M. Mosca, H. Ollivier, *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 2006, Proceedings, Part I*, M. Bugliesi, B. Preneel, V. Sassone, I. Wegener, Eds. (LNCS 4051, Springer, Berlin, 2006), pp. 72–83.
48. M. McKague, M. Mosca, in *Theory of Quantum Computation, Communication, and Cryptography: 5th Conference, TQC 2010, Leeds, UK, April 13–15 2010, Revised Selected Papers*, W. van Dam, V. M. Kendon, S. Severini (LNCS 6519, Springer, Berlin, 2011), pp. 113–130.
49. B. Hayes, *Commun. ACM* **51**, 9 (2008).
50. T. Monz *et al.*, *Phys. Rev. Lett.* **106**, 130506 (2011).

Acknowledgments: The authors are grateful to C. Brukner, V. Danos, and R. Prevedel for discussions and to F. Cipcigan and J. Schmöle for support. We acknowledge support from the European Commission, Q-ESSENCE (no. 248095); European Research Council senior grant (QIT4QAD); John Templeton Foundation; Austrian Science Fund (FWF): [SFB-FOCUS] and [Y585-N20]; Engineering and Physical Sciences Research Council; grant EP/E059600/1; Canada's Natural Sciences and Engineering Research Council; the Institute for Quantum Computing; QuantumWorks; the National Research Foundation and Ministry of Education, Singapore; and the Air Force Office of Scientific Research, Air Force Material Command, U.S. Air Force, under grant no. FA8655-11-1-3004. S.B. designed and performed the experiments, acquired the experimental data, carried out theoretical calculations and the data analysis, and wrote the manuscript. E.K., A.B., and J.F. contributed to the data analysis, carried out theoretical calculations, and wrote the manuscript. A.Z. supervised the project. P.W. contributed to the planning of the experiment, wrote the manuscript, and supervised the project. All authors discussed the results and commented on the manuscript.

Supporting Online Material
www.sciencemag.org/cgi/content/full/335/6066/303/DC1
Materials and Methods
SOM Text
Figs. S1 to S42
Tables S1 to S9

30 September 2011; accepted 30 November 2011
10.1126/science.1214707

An Engineered Microbial Platform for Direct Biofuel Production from Brown Macroalgae

Adam J. Wargacki,[1]* Effendi Leonard,[1]* Maung Nyan Win,[1]* Drew D. Regitsky,[1] Christine Nicole S. Santos,[1] Peter B. Kim,[1] Susan R. Cooper,[1] Ryan M. Raisner,[1] Asael Herman,[1]† Alicia B. Sivitz,[1]‡ Arun Lakshmanaswamy,[1] Yuki Kashiyama,[1,2,3] David Baker,[4] Yasuo Yoshikuni[1]§

Prospecting macroalgae (seaweeds) as feedstocks for bioconversion into biofuels and commodity chemical compounds is limited primarily by the availability of tractable microorganisms that can metabolize alginate polysaccharides. Here, we present the discovery of a 36–kilo–base pair DNA fragment from *Vibrio splendidus* encoding enzymes for alginate transport and metabolism. The genomic integration of this ensemble, together with an engineered system for extracellular alginate depolymerization, generated a microbial platform that can simultaneously degrade, uptake, and metabolize alginate. When further engineered for ethanol synthesis, this platform enables bioethanol production directly from macroalgae via a consolidated process, achieving a titer of 4.7% volume/volume and a yield of 0.281 weight ethanol/weight dry macroalgae (equivalent to ~80% of the maximum theoretical yield from the sugar composition in macroalgae).

Volatile energy costs and pressure to conserve fossil fuel resources have ignited efforts to produce biofuels and renewable commodity chemical compounds via microbial fermentation of biomass. Pursuant to these goals, microbial engineering aims to increase product yields and bioconversion efficiencies. Equally critical, development of scalable and diverse feedstocks will empower sustainable use of this technology and drive the widespread adoption of renewable bio-economies. At present, corn and sugarcane are vetted industrial feedstocks, but "food versus fuel" concerns may preclude their long-term use. Inedible lignocellulosic plant materials are preferable feedstocks, but current microbial technologies for fermentation of the simple sugars in lignocellulose have yet to overcome the cost of the complex processes needed to release these sugars from recalcitrant polysaccharides (*1*). Therefore, distinct strategies are required to develop scalable and sustainable non-lignocellulosic biomass resources such as marine macroalgae (seaweeds) for use as next-generation feedstocks.

Brown macroalgae exhibit several key features of an ideal feedstock for production of biofuels and renewable commodity chemical compounds. Requiring no arable land, fertilizer, or fresh water resources, cultivation of these crops circumvents economic concerns associated with land management and avoids adverse impacts on food supplies. Macroalgae are already grown for human consumption, but not as a staple crop. Large-scale cultivation is practiced in several countries, yielding 15 million metric tons per year (*2*); in these countries, macroalgae are also used as animal feeds, agricultural fertilizers, and sources of polymers. Because brown macroalgae does not contain lignin, sugars can be released by simple operations such as milling or crushing. This bio-architectural feature gives macroalgae a distinct advantage over lignocellulosic biomass, facilitates higher yields, and averts the need for energy-intensive pretreatment and hydrolysis processes before fermentation. An analysis prepared for the U.S. Department of Energy (DOE) reports a macroalgae productivity of 59 dry metric tons/ha/year and an ideal ethanol yield from macroalgae of 0.254 weight (wt) ethanol/wt dry macroalgae (*2*). Based on these numbers, an optimum bioethanol productivity of 19,000 liters/ha/year is estimated. This value is approximately two times higher than the ethanol productivity from sugarcane and

[1]Bio Architecture Lab, 604 Bancroft Way, Suite A, Berkeley, CA 94710, USA. [2]BAL Chile S.A., La Quebrada No. 1005, Puerto Varas 5550658, Chile. [3]BAL Biofuels S.A., Alcántara 200, piso 6, Las Condes, Santiago 7550159, Chile. [4]Biomolecular Structure and Design (BMSD), Department of Biochemistry, University of Washington, J Wing, Health Sciences Building, Post Office Box 357350, Seattle, WA 98195, USA.

*These authors contributed equally to this work.
†Present address: Biolojic Design, Mapo 11, Tel Aviv 63577, Israel
‡Present address: Laboratoire de Biochimie et Physiologie Moléculaire des Plantes, Centre National de la Recherche Scientifique, Unité Mixte de Recherche 5004, Institut de Biologie Intégrative des Plantes, F-34730 Montpellier cedex 2, France.
§To whom correspondence should be addressed. E-mail: yoshikuni@ba-lab.com