mass roughly like $M^{-0.7}$. In particular, $62 \pm 36\%$ of all stars harbor super-Earths (5–10 $M_\oplus$); $52 \pm 25\%$ have Neptunian middleweights (10–30 $M_\oplus$); and $17 \pm 7\%$ have Jovian planets heavier than 100 $M_\oplus$.

On average, the team concludes, every star has 1.6 planets in the survey's M and R sensitivity range. "So in the Milky Way," says Arnaud Cassan, who led the analysis, "planets around stars seem to be the rule rather than the exception."

Bertram Schwarzschild

References

1. A. Cassan et al., *Nature* **481**, 167 (2012).
2. A. Gould et al., *Astrophys. J.* **720**, 1073 (2010).
3. J.-P. Beaulieu et al., *Nature* **439**, 437 (2006).

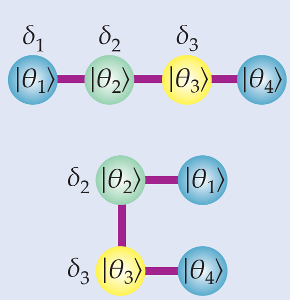
A blind quantum computer makes its laboratory debut

Quantum computing promises great efficiency advantages over classical computing. Quantum communication promises tamper-proof security. Combine them, and you get blind quantum computing.

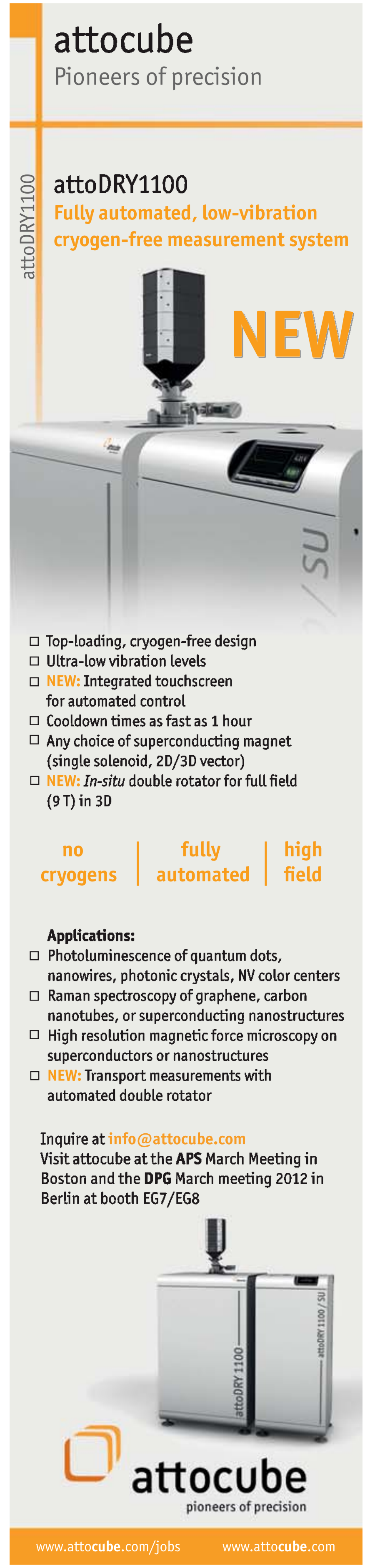
Described by Vlatko Vedral of the University of Oxford as "possibly the most exciting idea in quantum computing in the last 10 years," blind quantum computing would enable a client, who herself has no quantum computing capability, to run an algorithm on a remote server without revealing anything about her input, computation, or output. Now, Philip Walther (University of Vienna) and colleagues have demonstrated a small-scale version of a blind quantum computer.[1]

The experiment used a protocol[2] presented in 2009 by Anne Broadbent (University of Waterloo, Canada), Joseph Fitzsimons (then also at Waterloo, now at the National University of Singapore), and Elham Kashefi (University of Edinburgh). Broadbent and collaborators based their scheme on a so-called one-way quantum computer: Rather than manipulating a system of qubits and then reading out the result, the computer starts with a highly entangled state, universal for all computations up to a certain size, and performs a series of single-qubit measurements. The results of those measurements can then be processed with a classical computer to give the computation output. To make the computation blind, Broadbent and company have the client prepare the qubits with phase angles θ_i that only she knows and have her instruct the computer to measure them at angles δ_i. The computer entangles the qubits in a specified way, measures them, and transmits the results back to the client. Without knowing the angles θ_i, neither the computer nor an eavesdropper can deduce the underlying computation from the angles δ_i and the measurement results.

In contrast to previously proposed schemes for blind quantum computation, Broadbent and company's protocol doesn't require the client to do anything that's not well within the bounds



A one-qubit gate (top) and a two-qubit gate (bottom) implemented on a four-qubit blind quantum computer. The qubits are prepared in initial states $|\theta_i\rangle$, pairwise entangled as shown by the purple lines, and measured at angles δ_i in order from left to right (not necessarily numerical order). The rightmost qubits in each gate are the gate's output; they could become another gate's input in a larger computation. When θ_2 and θ_3 are kept secret, the computation is blind: Neither the computer nor an eavesdropper can deduce the underlying computation. (Adapted from ref. 1.)



of present-day technology. Even the tasks required on the computer's side—entangling the qubits pairwise and measuring them one by one—can be carried out on small systems, as Walther and colleagues have now done. The Walther group's computer used four qubits, which took the form of photons. Not much computing can be done on a one-way quantum computer of that size, but the researchers successfully demonstrated various one- and two-qubit quantum logic gates, the eventual building blocks of a larger quantum computation. They also carried out miniature versions of two algorithms, including a database search, that promise to be more efficient on a quantum computer than on a classical one. Along the way, they found that they could still achieve blindness without preparing all the qubits in states unknown to the computer: In their four-qubit system, it suffices to have just two qubits (θ_2 and θ_3, shown in yellow and green in the figure) in secret states. That discovery could make it easier to implement larger blind computations in the future. **Johanna Miller**

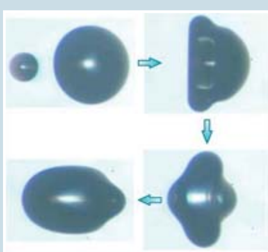
References

1. S. Barz et al., *Science* **335**, 303 (2012).
2. 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), p. 517; available at http://arxiv.org/abs/0807.4154.

physics update

These items, with supplementary material, first appeared at http://www.physicstoday.org.

New insights into droplet collisions. Ocean mists and car engines are among the countless environments whose behavior is influenced by the dynamics and interactions of liquid droplets, and by droplet collisions in particular. Such collisions have varied outcomes—the droplets might smoothly merge with little deformation, bounce off each other, coalesce following large deformation, or separate after temporarily coalescing. To date, most research has focused on collisions between identical droplets, for which the outcomes depend on the impact parameter and the ratio of kinetic energy to surface tension. In new work on droplets of unequal size, Chung Law and colleagues at Princeton University have experimentally demonstrated that the size disparity can significantly increase the parameter range over which the droplets permanently coalesce. The team's theoretical model, based on energy balance and scaling arguments and verified experimentally, reveals why: As surface tension pulls the merged, deformed droplet back toward a spherical shape, increased viscous dissipation through internal motion reduces the energy available for separation. The extended coalescence region, argue the researchers, may hold promise for rocket engines fueled with so-called hypergolic propellants that ignite when they come into contact, since the enhanced coalescence and mixing of fuel and oxidizer droplets should facilitate the ignition. (C. Tang, P. Zhang, C. K. Law, *Phys. Fluids* **24**, 022101, 2012.) —RJF



The Arctic gyre spins up to store fresh water. Centered at 79° N, 159° W, some 900 km north of Barrow, Alaska, and spread over an area twice the size of Texas, the Beaufort Gyre is a slowly circulating system of ice and seawater. When, as is the case now, the gyre spins in a clockwise, anticyclonic direction, surface winds and the Coriolis force push the water toward the gyre's center to create a vast, low mound of water. As Katharine Giles of University College London and her colleagues note in a new study, Arctic surface waters are unusually fresh, thanks to melting ice and falling rain and snow. An anticyclonic gyre therefore acts as a huge store of fresh water. To determine how huge, Giles and her colleagues used satellite altimetry data going back 15 years. Between 1996 and 2002, the mound's height shrank at a rate of about 0.60 cm/yr. Since then, however, the height has been rising at 1.9 cm/yr. The mound now stands 30 cm above the ocean's mean equilibrium level. Estimating the volume of fresh water in the mound requires the water's density, which Giles and her colleagues obtained from measurements made by NASA's gravity-sensing *GRACE* satellite. They calculate that the mound contains 8000 km^3 of fresh water, about 11% of the Arctic total. The researchers also found that the mound's growth is correlated with how strong and anticyclonic the wind field is. If the gyre completely reverses, as simulations suggest it could, the stored water will be released, possibly reducing the Arctic ice cap and disrupting shoals of Arctic-dwelling fish. (K. A. Giles et al., *Nat. Geosci.*, in press.) —CD

Surface-healing nanoparticles find their target. Taking cues from white blood cells, researchers have become adept at exploiting telltale biochemical markers to selectively deliver drugs to the body parts where they're most needed. Inspired by that work, theorists led by Anna Balazs (University of Pittsburgh) proposed that similar strategies might be used to repair inanimate materials. Like biological maladies, material damage is often distinguishable by a chemical signature, such as a change in surface energy. Five years ago, Balazs and company described how one might exploit those signatures to deploy reparative nanoparticles to damaged sites. Now, the theorists have collaborated with experimentalists led by Todd Emrick (University of Massachusetts Amherst) to prove the principle in the lab. Emrick's team prepared an oil-in-water emulsion in which each oily droplet was rich in cadmium selenide nanoparticles and encapsulated by a thin layer of surfactant. While rolling along the oxidized—and thus hydrophilic—surface of a silicone sheet, the microcapsules retain their nanoparticle cargo. But when they encounter a freshly exposed crack—whose surface is unoxidized, and thus hydrophobic—the similarly hydrophobic nanoparticles leak out and coat the crack's interior. A sufficient number of microcapsules can supply enough nanoparticles to fill the crack and repair the damage. The fluorescent CdSe nanoparticles also serve a diagnostic role: They cause the cracks to appear as bright red streaks in this fluorescence image. (K. Kratz et al., *Nat. Nano.* **7**, 87, 2012.) —AGS