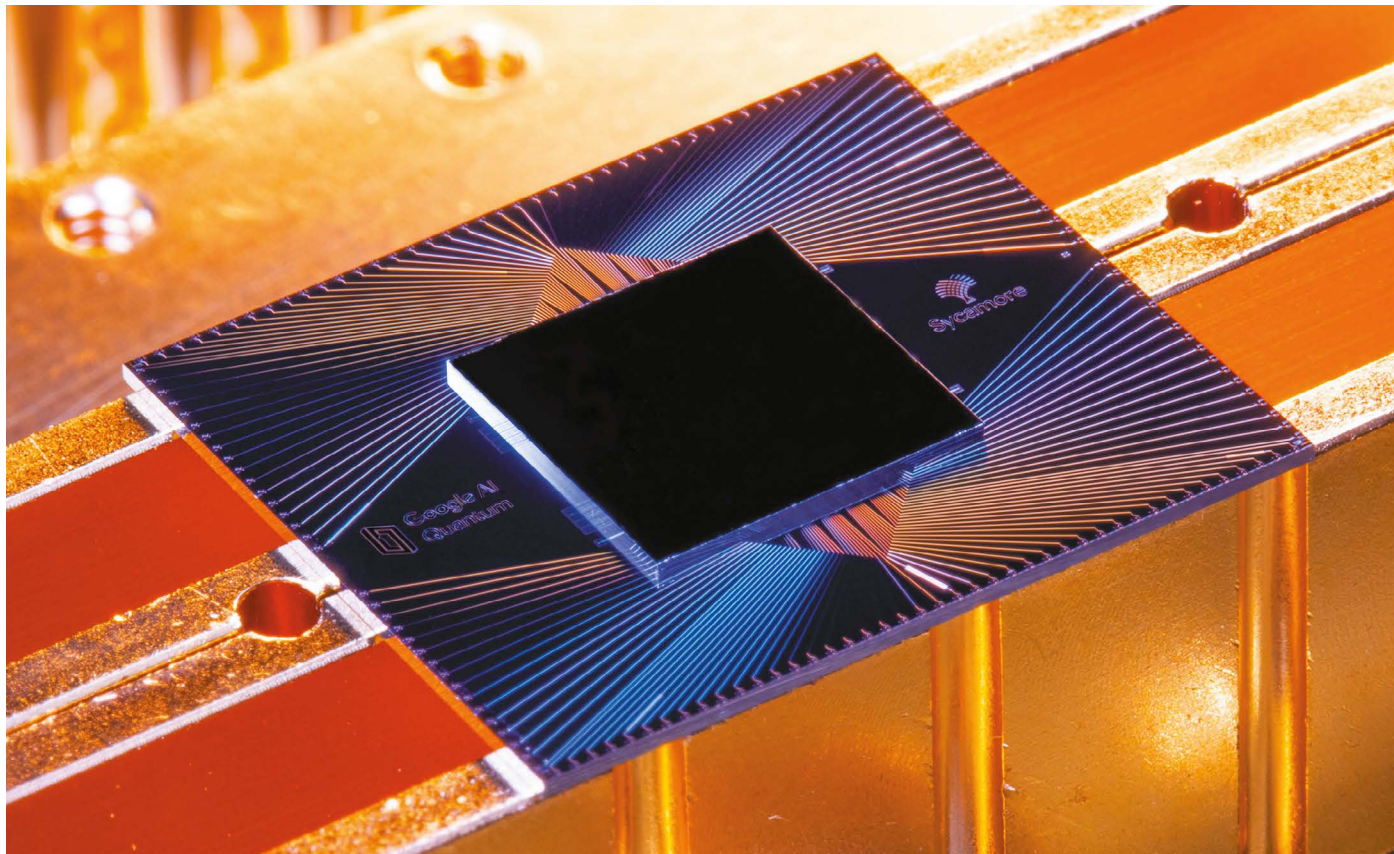# News in focus

ERIK LUCERO

The Sycamore chip is composed of 54 qubits, each made of superconducting loops.

GOOGLE PUBLISHES LANDMARK QUANTUM SUPREMACY CLAIM

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

By Elizabeth Gibney

Scientists at Google say that they have achieved quantum supremacy, a long-awaited milestone in quantum computing. The announcement, published in *Nature* on 23 October, follows a leak of an early version of the paper five weeks ago, which Google did not comment on at the time.

In a world first, a team led by John Martinis, an experimental physicist at the University of California, Santa Barbara, and Google in Mountain View, California, says that its quantum computer carried out a specific calculation that is beyond the practical capabilities of regular,

'classical' machines (F. Arute *et al. Nature* **574**, 505–510; 2019). The same calculation would take even the best classical supercomputer 10,000 years to complete, Google estimates.

Quantum supremacy has long been seen as a milestone because it proves that quantum computers can outperform classical computers, says Martinis. Although the advantage has now been proved only for a very specific case, it shows physicists that quantum mechanics works as expected when harnessed in a complex problem.

"It looks like Google has given us the first experimental evidence that quantum speed-up is achievable in a real-world system," says

Michelle Simmons, a quantum physicist at the University of New South Wales in Sydney, Australia.

The feat was first reported in September by the *Financial Times* and other outlets, after an early version of the paper was leaked on the website of NASA, which collaborates with Google on quantum computing, before being quickly taken down. At that time, the company did not confirm that it had written the paper, nor would it comment on the stories.

Although the calculation Google chose – checking the outputs from a quantum random-number generator – has limited practical applications, "the scientific achievement is
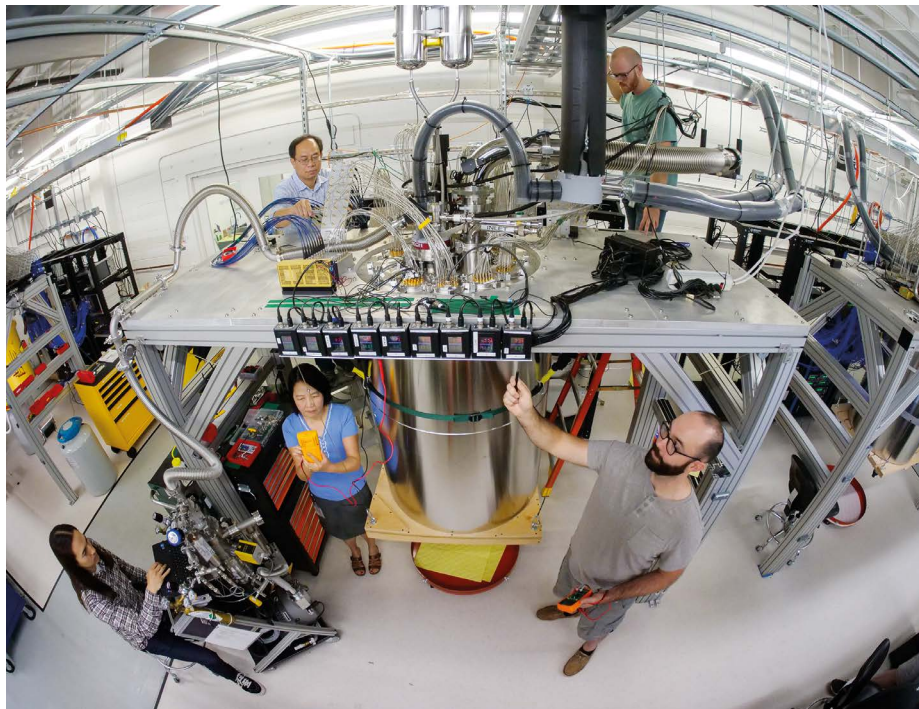
Google's quantum computer excels at checking the outputs of a random-number generator.

huge, assuming it stands, and I'm guessing it will", says Scott Aaronson, a theoretical computer scientist at the University of Texas at Austin.

Researchers outside Google are already trying to improve on the classical algorithms used to tackle the problem to bring down the 10,000 year speed-up that the firm calculates. IBM, a rival to Google in building the world's best quantum computers, reported in a preprint on 21 October that the problem could be solved in just 2.5 days using a different classical technique (E. Pednault *et al.* preprint at https://arxiv.org/abs/1910.09534; 2019). That paper has not been peer-reviewed. If IBM is correct, it would reduce Google's feat to demonstrating a quantum 'advantage' — doing a calculation much faster than a classical computer, but not something that is beyond its reach. This would still be a significant landmark, says Simmons. "As far as I'm aware that's the first time that's been demonstrated, so that's definitely a big result."

Quick solutions

Quantum computers work in a fundamentally different way from classical machines: a classical bit is either a 1 or a 0, but a quantum bit, or qubit, can exist in multiple states at once. When qubits are inextricably linked, physicists can, in theory, exploit the interference between their wave-like quantum states to perform calculations that might otherwise take millions of years. Physicists think that quantum computers might one day run revolutionary algorithms that could, for example, search unwieldy databases or factor large numbers — including, importantly, those

used in encryption. But those applications are still decades away. The more qubits are linked, the harder it is to maintain their fragile states while the device is operating. Google's algorithm runs on a quantum chip composed of 54 qubits, each made of superconducting loops. But this is a tiny fraction of the one million qubits that could be needed for a general-purpose machine.

The task Google set for its quantum computer is "a bit of a weird one", says Christopher Monroe, a physicist at the University of Maryland in College Park. Google physicists first crafted the problem in 2016, and it was designed to be extremely difficult for an ordinary computer to solve. The team challenged its computer, known as Sycamore, to

> ## "The scientific achievement is huge, assuming it stands, and I'm guessing it will."

describe the likelihood of different outcomes from a quantum version of a random-number generator. They do this by running a circuit that passes 53 qubits through a series of random operations. This generates a 53-digit string of 1s and 0s — with a total of 2^{53} possible combinations (only 53 qubits were used because one of Sycamore's 54 was broken). The process is so complex that the outcome is impossible to calculate from first principles, and is therefore effectively random. But owing to interference between qubits, some strings of numbers are more likely to occur than others. This is similar to rolling a loaded die — it still produces a

random number, even though some outcomes are more likely than others.

Sycamore calculated the probability distribution by sampling the circuit — running it one million times and measuring the observed output strings. The method is similar to rolling the die to reveal its bias. Verifying the solution was a further challenge. To do that, the team compared the results with those from simulations of smaller and simpler versions of the circuits, which were done by classical computers — including the Summit supercomputer at Oak Ridge National Laboratory in Tennessee. Extrapolating from these examples, the Google team estimates that simulating the full circuit would take 10,000 years even on a computer with one million processing units (equivalent to around 100,000 desktop computers). Sycamore took just 3 minutes and 20 seconds.

Limited applications

Monroe says that Google's achievement might benefit quantum computing by attracting more computer scientists and engineers to the field. But he also warns that the news could create the impression that quantum computers are closer to mainstream practical applications than they really are. "The story on the street is 'they've finally beaten a regular computer: so here we go, two years and we'll have one in our house'," he says.

In reality, Monroe adds, scientists are yet to show that a programmable quantum computer can solve a useful task that cannot be done any other way, such as by calculating the electronic structure of a particular molecule — a fiendish problem that requires modelling multiple quantum interactions. Another important step, says Aaronson, is demonstrating quantum supremacy in an algorithm that uses a process known as error correction — a method to correct for noise-induced errors that would otherwise ruin a calculation. Physicists think this will be essential to getting quantum computers to function at scale. Google is working towards both of these milestones, says Martinis, and will reveal the results of its experiments in the coming months.

Aaronson says that the experiment Google devised to demonstrate quantum supremacy might have practical applications: he has created a protocol to use such a calculation to prove to a user that the bits generated by a quantum random-number generator really are random. This could be useful, for example, in cryptography and some cryptocurrencies, whose security relies on random keys.

Google engineers had to carry out a raft of improvements to their hardware to run the algorithm, including building new electronics to control the quantum circuit and devising a new way to connect qubits, says Martinis. "This is really the basis of how we're going to scale up in the future. We think this basic architecture is the way forward," he says.