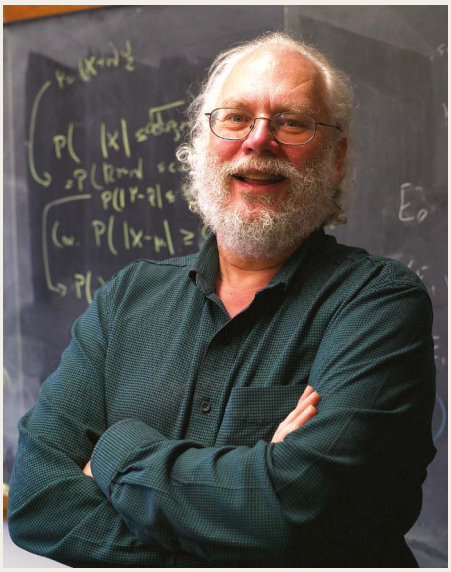
Q&A

Quantum computing pioneer warns of complacency over Internet security

When physicists first thought up quantum computers in the 1980s, it sounded like a nice theoretical idea, but one probably destined to remain on paper. Then, in 1995, applied mathematician Peter Shor published a study that changed that perception (P. W. Shor *Phys. Rev. A* 52, R2493(R); 1995). He showed how quantum computers could overcome a crucial problem. The machines would process information as qubits — quantum versions of ordinary bits that can simultaneously be '0' and '1'. But quantum states are notoriously vulnerable to noise. Shor's error-correction technique showed how to make quantum information more robust. He also found the first potentially useful — but ominous — way to use a hypothetical quantum computer: an algorithm that would allow it to factor integer numbers into prime factors at lightning speed. Most Internet traffic today uses encryption techniques based on large prime numbers. Cracking those codes is hard because classical computers are slow at factoring large products. But quantum computers are now a reality, and although they are still too rudimentary to factor numbers of more than two digits, they could one day threaten Internet encryption. *Nature* spoke to Shor, now at the Massachusetts Institute of Technology in Cambridge, about the impact of his work.

Before your factoring algorithm, were quantum computers mostly a theoretical curiosity?
My paper certainly gave people an idea that these machines could do something useful. Computer scientist Daniel Simon, in a precursor of my result, solved a problem that he came up with that shows that quantum computers are exponentially faster [than ordinary computers]. But even after Simon's algorithm, it wasn't clear that they could do something useful.

What was the reaction to your announcement of the factoring algorithm?
At first, I had only an intermediate result. I gave a talk about it at Bell Labs [in New Providence, New Jersey, where I was working at the time] on a Tuesday in April 1994. The news spread amazingly fast. At that point, I had not actually solved the factoring problem, but somehow in five days my result had turned into factoring as people were telling each other about it.



Applied mathematician Peter Shor.

Many experts still thought that quantum computers would lose information before you can actually finish your computation. One of the objections was that in quantum mechanics, if you measure a system, you inevitably disturb it. I showed how to measure the error without measuring the computation — and then you can correct the error and not destroy the computation. After my 1995 paper on error correction, some of the sceptics were convinced that maybe quantum computing might be doable.

Error correction relies on 'physical' and 'logical' qubits. What is the difference?
When you write down an algorithm for a quantum computer, you assume that the qubits are noiseless; these noiseless qubits that are described by the algorithm are the logical qubits. We actually don't have noiseless qubits in our quantum computers. In fact, if we try to run our algorithm without any kind of noise reduction, an error will almost inevitably occur.

A physical qubit is one of the noisy qubits in our quantum computer. To run our algorithm without making any errors, we need to use the physical qubits to encode logical qubits, using a quantum error-correcting code. The best way we know how to do this has a fairly large overhead, requiring many physical qubits for each logical qubit.

In 2019, Google showed that its 54-qubit quantum computer could solve a problem that would take impossibly long on a classical computer. What was your reaction?
It's definitely a milestone. It shows that quantum computers can do things better than classical computers — at least, for a very contrived problem. Certainly some publicity was involved on Google's part. But it has a very impressive quantum computer. It still needs to be a lot better before it can do anything interesting.

When quantum computers can factor large prime numbers, will that enable them to break 'RSA' — the ubiquitous Internet encryption system?
Yes, but the first people who break RSA either are going to be the NSA [the US National Security Agency] or some other big organization. At first, these computers will be slow. If you have a computer that can only break, say, one RSA key per hour, anything that's not high priority or a national-security risk is not going to be broken. The NSA has more important things to use its quantum computer on than reading your e-mail.

Are there cryptography systems that can replace RSA and that will be secure even in the age of quantum computers?
I think we have post-quantum cryptosystems that you could replace RSA with. A bigger problem is that there are other ways to break Internet security, such as badly programmed software, viruses, sending information to some not entirely honest player. I think the only obstruction to replacing RSA with a secure post-quantum cryptosystem will be will-power and programming time.

Is there a risk we'll be caught unprepared?
Yes. There was an enormous amount of effort put into fixing the Year 2000 bug. You'll need an enormous amount of effort to switch to post-quantum. If we wait around too long, it will be too late.

Interview by Davide Castelvecchi
This interview has been edited for length and clarity.