You want a quantum computer? Then prepare to fight off the ultimate in malicious software, says **Mark Anderson**

Attack of the quantum worms

WHETHER dollars or pounds, you probably didn't pay more than a few hundred, maybe a thousand or so for your computer. You probably don't use it for anything out of the ordinary – games, a bit of work, email and surfing the net. And yet you've probably thought hard about protecting it from malicious software. Infection by digital worms, viruses and Trojan horses can wipe your hard drive or take over your machine, so you've no doubt spent hard-earned cash on keeping such "malware" out.

Likewise, you would imagine that the people spending decades – and billions of dollars – developing quantum computers have done the same. After all, this super-powerful technology is already being lined up for military and government code-breaking applications. The people involved will have long anticipated the havoc that quantum versions of viruses and other malware could cause, right?

"I hadn't thought of this," says David Deutsch, the University of Oxford researcher who produced the first blueprint for a quantum computer. Deutsch made his great leap in 1985, yet the first paper to talk about protecting quantum computers from malicious attack was only written this year (www.arxiv.org/quant-ph/0505126). The paper's authors, Lian-Ao Wu and Daniel Lidar of the University of Toronto in Canada, suggest that quantum malware could take on many guises. It might appear in the form of a highly destructive hidden logic gate that flips or erases quantum bits. Maybe it will be a quantum algorithm designed to scramble data in particularly malicious ways. What is certain is that it's coming. "The arrival of quantum malware," they warn, "is a matter of time."

First, of course, the quantum malware needs a quantum computer to run on. The idealised quantum computer is a network of isolated particles – say, rows of atoms held in a laser trap, or electrons floating above a surface of liquid helium. The quantum states of particles are used to represent the 1s and 0s that are the bread and butter of digital computing. But quantum particles can be in a "superposition" of multiple states, just as Schrödinger's cat is both alive and dead in the famous quantum thought experiment. So a quantum bit, or qubit, can be both zero and one at the same time; the atom might, for instance, sit in both an excited state and its ground state simultaneously. Link *n* of these superposed qubits together in a properly configured array and they act as a memory register that can represent every whole number between 1 and 2*n* at the same time. Manipulate these "entangled" quantum states – by hitting the atoms with a suitably shaped laser pulse, for example – and you can perform a computation on all the numbers at once.

A 1000-qubit computer that used quantum particles to store its data and run its logic gates would let you perform simultaneous calculations on every positive integer less than 2^{1000}, which is roughly 10^{300}. Clever programmers could tap into this unrivalled power to solve problems wholly inaccessible to conventional computers – such as finding the factors of huge numbers.

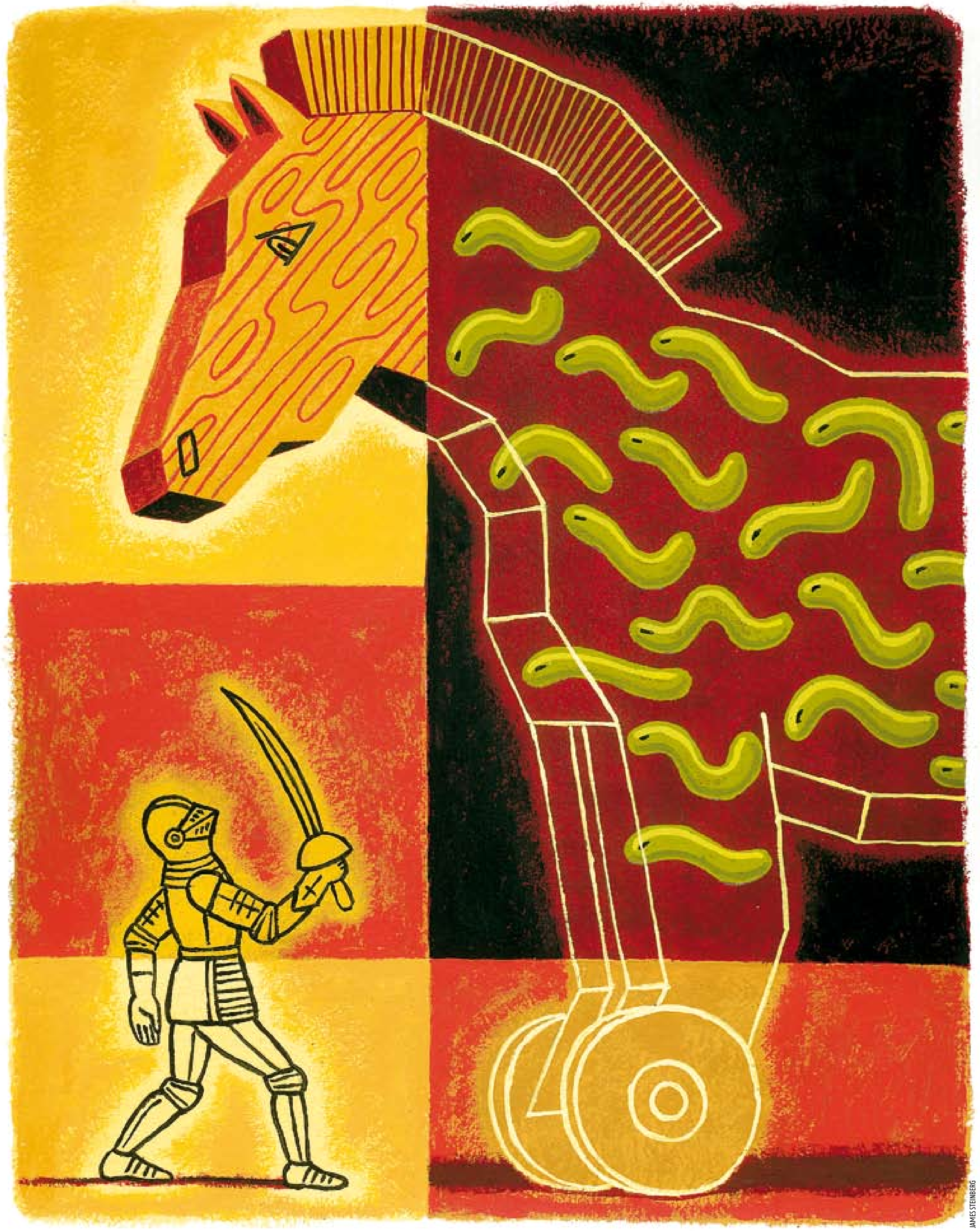
That may sound like a prosaic application, yet it is anything but. If you can factorise large numbers, you can crack currently "unbreakable" codes, such as the RSA protocol that protects most internet transactions. When mathematician Peter Shor, then at Bell Labs and now at the Massachusetts Institute of Technology, proved this in 1993, funding for research into quantum computing went through the roof.

Flipping the qubit

Today's quantum computers are not sophisticated enough to do anything malicious to your online bank account; the best quantum computer in the world is about as computationally gifted as an 11-year-old child. But the scenarios Wu and Lidar envisage are not quantum pie in the sky. They wrote their paper in response to the fact that the "quantum internet", in the form of optical fibre and free space point-to-point networks dedicated to transferring quantum information, is already up and running in several networks across the world.

So far, efforts to protect data in those networks have focused on two issues. First, the quantum particles, such as photons, used to carry and process information are rather

▶



JAMES STEINBERG

fragile: disturbances in the environment, such as heat sources or someone knocking the equipment, can shift their quantum states and destroy the information. This has been addressed – at least to some degree – by the development of error-correction codes for quantum systems. Just as CD players use algorithms to bridge any gaps in the music when digital bits are lost or corrupted, physicists have come up with algorithms to detect and compensate for some “decoherence”.

The second issue is the problem of malicious eavesdroppers who might try to intercept data. Researchers have come up with various ways to make qubits tamper-proof (*New Scientist*, 29 November 2003, p 24). But so far no one has considered what would happen when people simply try to cripple the quantum computers that are churning out that data. And it is going to happen, reckons Lidar, who has just moved to the University of Southern California in Los Angeles.

“Our logic is very simple – just an extrapolation from classical communication networks,” he says. “As soon as you have a network that's online, there are people who try to interfere. In a quantum communication network, it seems reasonable to assume there will also be people trying to interfere.”

What's more, quantum networks offer even more opportunity for interfering: there are more ways to attack quantum computers than classical ones. The extra vulnerability arises from something called the qubit's phase information. Phase is simply an aspect of the qubit's superposition of states, and is part of the overall description of the quantum state and how it will evolve. If the phase is given a kick, or “decohered”, this can randomise the output when you finally read off the result of your computation on the qubit. This is exactly what happens if the environment decoheres a quantum computation, and what makes quantum information more fragile than its classical counterpart. A phase-based attack is impossible on a classical computer, since there is no classical analogue of superposition states.

So, in addition to flipping or erasing qubits, a quantum hacker could add in a “phase gate” that changes their phase and scrambles the outcomes of your algorithms. The attacker might also choose to do both, flipping the qubit then kicking its phase for good measure.

How do Wu and Lidar propose to defend this kind of system? First of all, they say, there should be long periods of isolation: quantum computers should spend as little time as possible with their qubits exposed to the wider quantum network that may supply data to be crunched. Everything in the researchers' scheme relies on the assumption that the network on-times are random and secret, and that those on-times are kept to an absolute minimum. “The combination of these two assumptions leads to an exponentially small probability of infection,” Lidar says.

There's no clever quantum trickery to this. “It's reminiscent of the ways people build military systems that are under attack, which is to keep them shut down a great deal of the time – and then suddenly open up and do something,” says Chip Elliott, who works on quantum network security for BBN Technologies in Cambridge, Massachusetts, and helped set up US defence research agency DARPA's quantum cryptography network. “A lot of communications systems work that way. But this is assuming that somebody is really out to get you,” he says.

“Quantum computers offer even more opportunity for attack than classical ones”

Of course, paranoia is no bad thing when it comes to network security. And after paranoia, the next best line of defence is frequent back-up, which means an infection can't ruin your day. This is the second part of the Wu-Lidar quantum defence. “Our protocol is simply the quantum analogue of the idea of classical back-up,” Lidar says.

The trouble is, quantum rules make backing up data difficult. Quantum mechanics has a “no-cloning” principle that means you can't copy quantum information without destroying the original. So instead Wu and Lidar have to keep it somewhere safe for as much of the time as possible.

Their scheme proposes that every quantum computer in the network should have an ancillary register of qubits as large as the quantum computer's memory. This remains isolated whenever the computer is connected to the network, so that viruses can never travel directly onto it. The data in the primary qubits can then be transferred en masse to this secure store. The quantum nature of this process means that not only preserves the information in the qubits, but also the various quantum “entanglements” between them, which are a vital part of the computation process. “Without the preservation of entanglement, the idea of back-up would be worthless,” Lidar says. “Standard classical back-up would destroy the entanglement and hence the quantum nature of the computation.” But with the quantum ancillaries, the whole calculation can effectively be put safely into stasis.

In Wu and Lidar's anti-malware protocol, all the network members share a secret sequence of timings that tell them when the network is live, meaning they can operate their machines and share qubits between them, and when it is idle. When it goes live, the data qubits are loaded from the back-ups and all the quantum computers share data and begin a round of calculations. These waves of run-time are kept extremely short, and the calculations-in-progress are then swapped to the ancillary qubits until the next run-time.

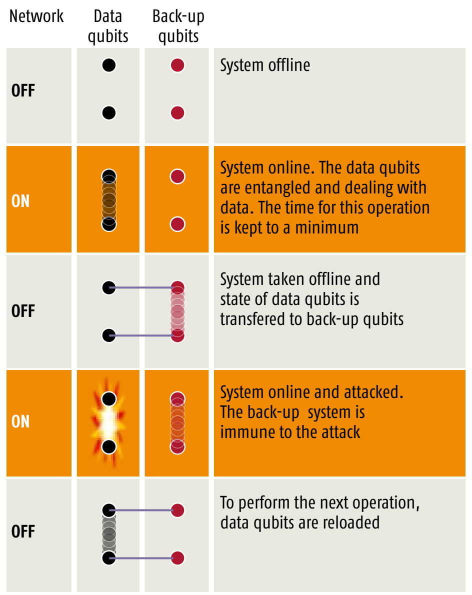
Though that might seem like a simple back-up, it's not: the no-cloning principle means the data held on the original qubits is destroyed. So the data qubits now contain junk information, while the actual data from the calculations-in-progress sit just offstage in the back-up registers. If the network is attacked during one of these long idle intervals, the only thing they can disrupt is the garbage data.

Under this system, Lidar says, the precious commodities that must be concealed from attackers are the back-up qubits and the schedule of the brief run-time intervals.

For the protocol to succeed, these network on-times must be substantially shorter than the periods when the calculations are in cold storage. But doesn't shutting down your quantum network for most of the time negate the blazing speed of quantum computations and thus defeat the purpose of operating a quantum computer in the first place? Not so, argues Lidar. “Quantum computers help you because the time it takes to solve a problem scales favourably with the problem size,” he said. “This protocol only multiplies that time by a constant factor, which is independent of how big the problem is.”

QUANTUM VIRUS PROTECTION

In case of attack, quantum computers need a back-up system. It is isolated from the main network at all times, so the viruses can never travel directly onto it



Network	Data qubits	Back-up qubits	
OFF	● ●	● ●	System offline
ON	● ●	● ●	System online. The data qubits are entangled and dealing with data. The time for this operation is kept to a minimum
OFF	● ●	● ●	System taken offline and state of data qubits is transfered to back-up qubits
ON	● ●	● ●	System online and attacked. The back-up system is immune to the attack
OFF	● ●	● ●	To perform the next operation, data qubits are reloaded

Into the real world

So for large-enough quantum computers, with many thousands of qubits, calculations that lie far out of the reach of conventional computers could still be completed on a malware-infested quantum network. It might take many minutes instead of mere seconds, say, to crack the RSA cryptographic system or simulate a complex nanosystem of thousands of interconnected components. But considering that conventional computers could never complete such tasks, the extra time would clearly be a small price to pay.

Elliott says the Wu-Lidar protocol is an impressive first step. “It's the first paper of its kind. I don't think anybody else has started to think about this.” However, as a pioneering work in a speculative field, the paper is almost by definition a purely theoretical exercise. And theorists can sometimes grow too confident in their own calculations, Elliott cautions. An idealised system, however powerful, has to be implemented in the real world – and that's where new weaknesses creep in.

Elliott points out that communicating quantum information between computers on the network would probably involve encoding qubits onto single photons and then sending those photons down fibre-optic cables. But if the quantum computers are more than a few kilometres apart there is a chance of losing the photon, and the only way to deal with this is to install “quantum repeater” boxes to boost the signal along the length of the fibre. Although that ensures that the signal remains strong, it makes the network far more vulnerable to attack: someone could hijack the repeater and tweak the data. “Why should I believe that my quantum repeater is actually going to do what I think it does?” Elliott asks.

Lidar suggests overcoming this with an alternative to quantum repeaters that he and Wu came up with last year. It employs the simplest of optical elements, such as phase shifters and beam splitters, installed at regular intervals along the fibre (*Physical Review A*, vol 70, p 62310). “This works as well as some repeaters, but cannot be hijacked,” Lidar says. “At worst someone could destroy some of the phase shifters.” This would degrade the signal, but would be a noticeable effect.

There are other potential pitfalls, however. One of the simplest scenarios Lidar and Wu envision is a quantum version of the time-bomb-like CIH virus, also known as Chernobyl. Though it was first discovered in June 1998, CIH did not explode until 26 April 1999, when it destroyed data in millions of computers and caused hundreds of millions of dollars' worth of damage. How would you deal with this kind of attack when, unlike the months of prior notice before CIH exploded, there may be no warning. You can't ever be confident your system is clean, Deutsch points out. “In principle, the hardware and classical software of quantum communication and computation systems could be altered in a way that would be hard to detect,” he says.

And that means you could even copy malware over to your secure qubits. If that happens, all is lost; there is no known means of recovery from this scenario. “It's a very interesting open research problem to construct a ‘quantum Norton antivirus’ which cleans corrupted data,” Lidar says.

The lesson from the cutting edge of quantum antivirus research seems clear. When it comes to computer networks, the best strategy is still the one military networks use: back up and back off. Bravado is for fools; cowards live to compute another day. ●

Mark Anderson is a writer based in Northampton, Massachusetts