THE TIMES

Monday August 15 2022 | THE TIMES

News

Crypto geeks scramble to protect web secrets

Experts are developing algorithms to keep our data safe from new quantum computers, **Tom Whipple** writes

Imagine there is a bag full of 1,000 scraps of paper, each with very large random numbers on. Someone pulls out 500 of these numbers, adds them together to make a very, very large number, then tells you what that number is. They then put all the pieces of paper back in the bag, hand it to you, and ask you to find their 500 numbers— or perhaps another 500 that reach the same sum. Can you? The world's cryptographers are betting a lot — betting, in effect, the internet — that the answer to that question is "no".

In the next few years the entire mathematical plumbing of secure global communications is set to change because, it turns out, those communi-cations are no longer secure. The system it will change to will be based on a variant of that 500-numbers poser.There is a problem with the internet. That problem is that at some point in the next decade or two, or maybe three, scientists think a computer will be made that can crack its encryption. If that is true, then it is not merely a theoretical problem for ten or 20 years' time.

"In some way," says Vadim Lyubashevsky, from IBM research, "you've already been hacked. It's just they can't use the information yet." Around the world criminals and foreign governments are intercepting WhatsApp communications, bank transactions and all the other things you do on the internet that you think are secret.

Today, they can't read them, but a different kind of computer is coming: a quantum computer that does not merely deal in binary ones and zeros but all that falls in between. When it arrives everything sent today will suddenly be crackable. It will be the biggest leak of secret information in history.

"If you have data that you think in ten years is still valuable to someone, then maybe you should be using quantum-safe encryption," Lyubashevsky says.

That is why, six years ago, the US National Institute of Standards and Technology launched a competition to find an encryption that was quantum computer-proof. Last month it announced the results: the four algorithms that will probably form the new basis of secrecy on the internet. The internet is about to be replumbed.

Three of the algorithms are based on what is known as structured lattices, multidimensional variants of the 1,000 number problem. Three were developed in collaboration with the scientists at Lyubashevsky's laboratory at IBM Zurich.

Now, the expectation is that over the next few years anyone serious about security will start switching over and retiring the old algorithms. If you want to contact or work with USagencies, soon you will have to use them.

Just last month a bill was introduced in the US Senate to accelerate a change to "post-quantum cryptography."

"The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers and wait until sufficiently powerful quantum systems are available to decrypt it," it read.

Much of modern cryptography works on what are called trapdoor functions: operations that are easy to run in one way but not another. For instance, it is extremely easy for a classical computer to multiply two very large prime numbers together. If, though, you give another computer the result of that multiplication it is extremely hard for it to work out what those prime numbers are.

It is so hard, in fact, that as the numbers involved get bigger it does not take long before you would need a computer the size of the universe to do it. This has been, for 30 years, the fact that has underpinned much of the cryptography on the internet.

The trouble is, this process is based on using classical silicon computers. Because of the way quantum computers work, the first decent one will be able to solve such problems very quickly indeed. And, scientists increasingly believe, they are coming.

There is, in fact, a prototype beneath Lyubashevsky's feet.

The IBM research laboratory in Zurich is like a Bond villain lair for computer scientists. Halfway up the side of a Swiss valley, it has koi carp, modernist architecture, a couple of Nobel prizes to its name — and a lot of contraptions that use liquid helium.

In the basement one of those contraptions, a quantum computer cooled to near absolute zero, manipulates quantum bits, using the properties of quantum mechanics to solve problems.

It's part of a completely separate project. At the same time as designing algorithms that will be the antidote to quantum computers, they are designing the computers themselves. The reason is because of their potential in areas far beyond cryptography.

While a normal computer calculates using zeros and ones, a quantum computer can in a sense use all the values in between, exploring a far larger number of solutions at once.

For a lot of calculations, even basic things such as addition, such computers are not particularly good. But for some, they will be revolutionary. Modelling chemical reactions, which themselves rely on the fuzzy weirdness of the quantum world, should be a lot easier. So too, it turns out, will factorising numbers. Yet structured lattices, as far as we know, remain impervious.

Alessandro Curioni, director of the laboratory, says that, a bit like the millennium bug, this is a problem we have known was coming for years. But now there is more of a sense of urgency.

In basements around the world physicists are getting better at manipu-lating and controlling supercooled quantum bits. In other, more secret, basements, servers fill up with commercially-classified information, with the WhatsApp messages of dissidents and government communications.

"The fact is," Curioni says, "if you have very sensitive data now, I don't care if you know the quantum computer is coming in five, ten, 20 years. If that data will still be sensitive to stealing then, I need to care now." You also need to hope that the 500 numbers problem really is as hard as everyone thinks it is. Because, so far, Lyubashevsky says, that remains a supposition.

"Tomorrow, somebody could come up with an algorithm that solves it all."

Vadim Lyubashevsky's IBM Zurich team is working on internet security