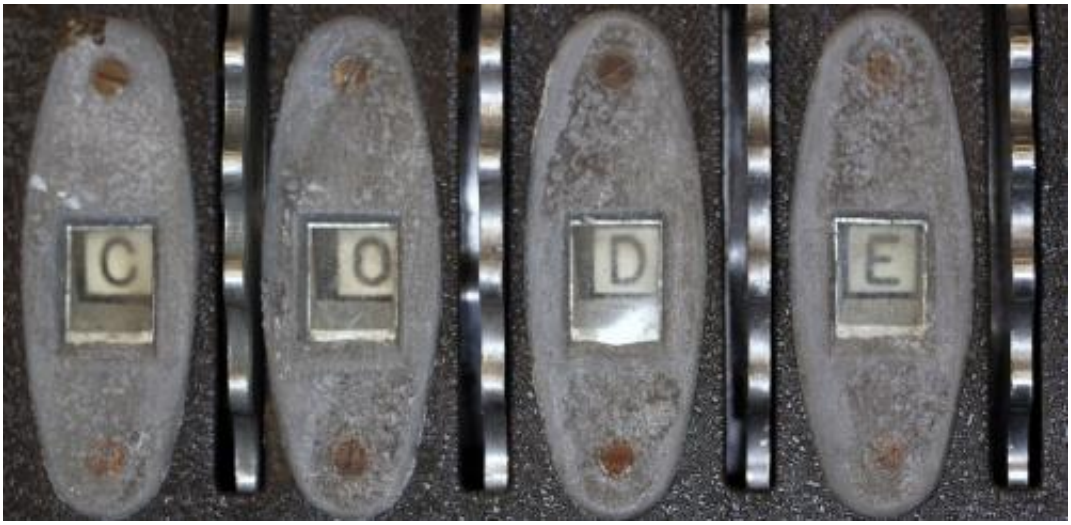
Quantum computers could crack existing codes but create others much harder to break

February 12 2014, by David Kielpinski



Cracking the code. Credit: Flickr/Lars O

The massive release of the US National Security Agency (NSA)'s classified documents by Edward Snowden continues to raise questions about security.

One of these documents deals with the NSA's classified research program in the exotic field of quantum computing.

This research investigates ways to process information using the laws of quantum mechanics, rather than the familiar physics underlying present-day computer processors.

Code breaking

Why should the NSA care? Because the single most famous application of quantum computing is in code-breaking.

During World War II, a team led by Alan Turing used a primitive computer to break the Nazis' Enigma code

The NSA document, which can be found online, deals with the excitingly named project "Penetrating Hard Targets".

An unknown portion of the US$80-million budget is devoted to building a small quantum processor, capable of counting up to four. (No, not four-million. Just four!) This doesn't sound like much, but one has to start somewhere.

Another portion supports research into quantum cryptography, which offers new, higher-security secret codes based on quantum mechanics.

The news here is that the NSA had its own secret experimental program. It was already public knowledge that the NSA is interested in quantum computing.

The NSA has been financially supporting non-classified quantum computing research at universities since the 1990s, and many academic journal articles acknowledge NSA support.

In fact, my own PhD work on quantum computing with trapped ions was largely funded by the NSA. One day, our funding managers came to visit. They looked like my maths professors from undergraduate days – slightly nerdy men in sweaters.

I was a little disappointed until I came up with a theory that when they

went back to the NSA building, they would tear off the sweaters to reveal the long trenchcoats of a typical spy drama.

Basic maths and cryptography

But iIt's no accident that our NSA funding managers looked like mathematicians. That's what they were. Modern cryptography is, in many ways, a branch of applied mathematics.

The Rivest-Shamir-Adleman (RSA) algorithm, which protects almost all e-commerce, relies on one fact that can be understood with primary-school maths (it can even be used to send love letters).

Multiplying two large prime numbers is easy – say, 547 × 617 = 337,499. There's a simple process that you can follow and making the numbers a little bigger only makes the process take a little longer. In the jargon of computer science, the problem "scales polynomially".

However, suppose someone just gives you a large number and asks you to work the process in reverse.

In our example, you are given the number 337,499 and asked to find out which numbers (the "factors") should be multiplied together to produce 337,499.

You would just have to try factors, almost at random, until you hit on the correct factors by chance (547 and 617).

This would take an exceedingly long time since you would have to perform many multiplications. Making the numbers a little bigger makes the problem much harder – it "scales exponentially"!

The efforts of the world's mathematicians over decades have not been

able to find an easy way to solve this problem, and they've certainly tried.

If an easy and practical solution were found, the RSA code would be broken and the prize is, well, most of the world's bank accounts.

In a less criminal frame of mind, you might want to feel secure about your next internet purchase, so you might want to convince yourself that RSA is unbreakable. Email encryption also relies on RSA, so trying to break RSA is core business for the NSA's mathematicians.

The quantum leap in code breaking

NSA headquarters in Maryland. Credit: US NSA

Quantum computers became big business in 1994, when Peter Shor demonstrated theoretically that a quantum computer could find the factors of a large number easily. Making the number bigger shouldn't faze the quantum computer – it's enough to add a little more computing capacity.

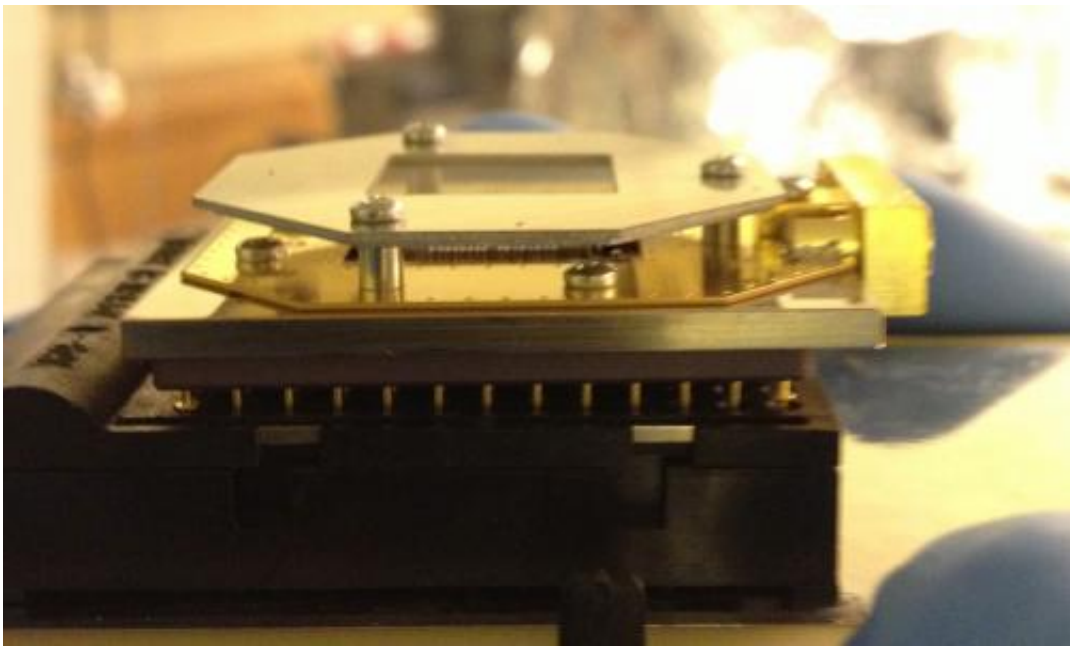
However, you needn't worry about your bank account. Translating Shor's algorithm into practice is tremendously difficult. No one has built a practical quantum computer that could break RSA, and that goal is still a long way off - decades, at the current rate of progress.

Remember, the NSA's current program, if successful, will handlenumbers up to four, not exactly the "large numbers" we were talking about earlier.

Quantum cryptography

It's quite likely that a quantum computer will be built eventually, but quantum mechanics can make codes as well as break them. The complementary part of the picture is the NSA's effort in quantum cryptography, which provides new security methods that are resistant even to quantum computers or any other kind of code-breaking.

Messages encoded in quantum systems have a perfect "tamper-proof seal". The Heisenberg Uncertainty Principle tells us that measuring one property of a quantum system must always change another property of the system.



A microchip for trapping atomic ions which could be the heart of a future quantum computer. Credit: Kielpinski lab

One can create a code based on this principle, such that if the coded message is intercepted and read, the process of reading the message actually changes it. The recipient can check parts of the message with the sender over an open line to make sure that there has been no tampering.

Even better news, quantum cryptography is much further advanced than quantum computing. There are already commercial ventures deploying quantum cryptography links for banks and governments. Australia's own Quintessence Labs, based in Canberra, is a major player in this area.

Quantum computing's roots may be in the cloak-and-dagger business, but it has great potential for civilian uses too. For instance, a quantum computer can efficiently simulate advanced materials, such as high-temperature superconductors, at the atomic level.

The ability to direct manufacturing efforts for these materials in a clever way could save tremendous effort. However, like all scientific advances, the uses of quantum computing will ultimately be determined politically and financially.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Quantum computers could crack existing codes but create others much harder to break (2014, February 12) retrieved 2 May 2024 from https://phys.org/news/2014-02-quantum-codes-harder.html