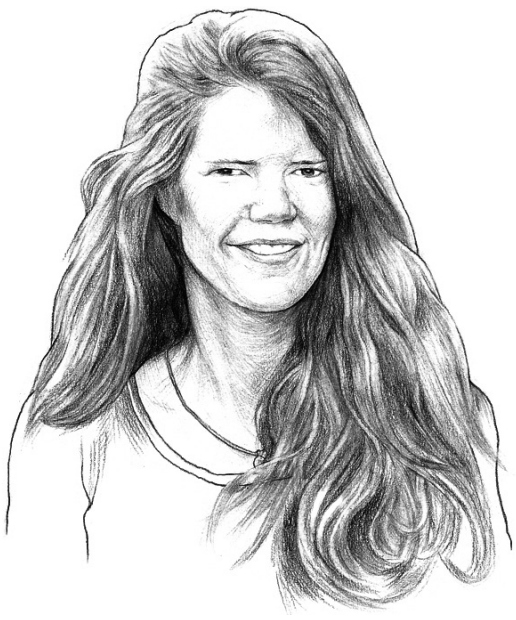
JULIE REHMEYER ∫ **MATH TREK**

New system offers way to defeat decryption by quantum computers



PETER JAMES FIELD/AGENCY RUSH

Quantum computers elicit dreams of great computational feats to come. But they also promise a nightmare: They could break today's security codes, rendering them no more secure than a TSA-approved luggage lock.

Now, for the first time, researchers have shown a security method to be immune to the type of attack that could bring down RSA, the cryptosystem in almost universal current use.

Modern cryptography methods are generally based on some mathematical problem that is hard to solve without special information. Breaking RSA, for example, would require factoring very large numbers, a task thought to be insurmountably difficult even for supercomputers. But in 1994, mathematician Peter Shor, now of MIT, found an algorithm that a quantum computer (once one exists) could use to factor big numbers in seconds.

There's no way of proving that a cryptosystem is impervious to all possible attacks. Still, Hang Dinh of Indiana University South Bend, Cristopher Moore of the Santa Fe Institute and Alexander Russell of the University of Connecticut in Storrs have now shown that one approach, known as the McEliece cryptosystem, is at least immune to the type of attack Shor devised to bring down RSA. "There may be an algorithm out there that can break it," Moore says, "but it would have to use ideas that are completely different from any now known." The team's findings will appear in the *Proceedings of CRYPTO 2011*.

McEliece is based on the methods used for correcting errors in codes. If Alice sends Bob the binary message 011 directly and a bit gets corrupted along the way — say, the first bit flips to a 1 — then Bob won't get her message accurately. To avoid this problem, she can encode the message using these strings:

- String 1: 0001111
- String 2: 0110011
- String 3: 1010101

Not only do these strings differ from one another in at least four places, but so do all eight possible strings produced by adding them together. Thus any combination of these strings can be distinguished from any other combination, even if a bit or two gets corrupted.

Because the second and third bits in Alice's message are

both 1, she would encode it by adding together the second and third strings (getting 1100110). Bob can use an algebraic method to decode this and retrieve her original message.

Even if a bit or two of Alice's message gets corrupted along the way, Bob can figure out what she probably meant, because he knows that she must have sent one of the eight uncorrupted combinations of the original three coding strings. He just has to figure out which of the eight is closest to the message he received. Compact disc players use this method to play accurately even when the disc is somewhat scratched.

If a problem is hard, you can turn it into a code that's hard to break and make cryptographic lemonade from algorithmic lemons.

This decoding step isn't always easy, though. The eight uncorrupted strings can be visualized as grid points in a seven-dimensional space (one dimension for each bit in the message). Bob's problem then is to find the grid point nearest to a general point in the space. This is known as the "closest vector problem," and for most lattices in very high-dimensional spaces it's extraordinarily difficult; mathematicians since Carl Friedrich Gauss have tried to solve it for 200 years. But if the code for correcting errors is chosen carefully, Bob's problem is easy.

Very hard problems like the closest vector problem can, of course, form the core of a cryptographic system. In the McEliece system, Alice comes up with an error-correcting code that is a scrambled, twisted version of one that's simple to decode, and anyone can send her a message by using this code and adding a bit of noise. She can decode it easily because she knows how the code has been scrambled and twisted, but no one else can.

The researchers started out trying to use Shor's algorithm to break McEliece but changed tactics when they couldn't. "One of the fun things about computer science is that you can switch hats," Moore says. "If a problem is hard to solve, you can try to turn it into a code that's hard to break and make cryptographic lemonade from algorithmic lemons."

The McEliece system isn't commonly used because to be secure, the secret key has to be inconveniently long. As computational power and bandwidth increases, though, this may become less of an obstacle.

Other encryption systems are also thought to be immune to attack by quantum computers. The leading contender is a lattice-based cryptosystem that, like McEliece, has the closest vector problem at its heart. That system may be more secure and flexible but hasn't yet been proven to be immune to Shor's algorithm. Dinh is now interested in seeing if her team can do that. ◻