MATHEMATICS

Lattices May Put Security Codes on a Firmer Footing

As the world becomes more wired, there is a growing need for strong safeguards to protect confidential information flowing through cyberspace. That may seem like a task that is already well in hand. After all, computer security experts have developed powerful techniques for encrypting data so that only the intended recipient, armed with the right key, can retrieve it. But these codes come without any absolute guarantee of security. As sensitive data and complex financial transactions take to the networks, users want assurances stronger than current cryptographic theory can provide.

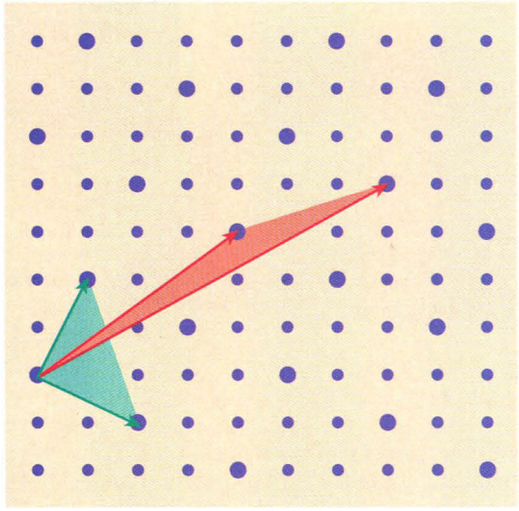
A recent discovery in theoretical computer science, however, could boost confidence in the mathematical locks that underlie the security codes. These locks rely on problems that seem to require more computational power to solve than any malefactor could ever muster. But although the current theory of computational complexity provides many ways of devising classes of problems thought to be impractically hard to solve, there is no way to be absolutely sure that any specific problem is as hard as it looks. As Burt Kaliski at RSA Data Security Inc. in Redwood City, California, puts it, "There's a kind of folklore saying if the best mathematicians and complexity theorists can't solve a problem, then it's probably hard, but it's nice if you can prove that something is hard."

Now Miklos Ajtai, a mathematician at the IBM Almaden Research Center in San Jose, California, has provided the kind of guarantee of hardness that cryptographers are looking for. He has proved that examples picked at random from a particular class of problems are, with exceedingly rare exceptions, as hard to solve as the hardest ones imaginable. A code that embedded messages in these problems so that only someone equipped with the answers could decode them would provide something close to a guarantee of security.

"It's a wonderful result," says Shafi Goldwasser, whose group at the Massachusetts Institute of Technology (MIT) is trying to develop a cryptosystem based on specific examples, or instances, of the problem. Ajtai's breakthrough "offers promise for a more secure theoretical foundation" for computational cryptography, agrees Prabhakar Raghavan at IBM Almaden. Raghavan thinks researchers may be able to apply Ajtai's ideas to provide similar guarantees for other types of problems, possibly ones already in cryptographic use.

At the moment, computational cryptography rests on the assumption that certain classes of problems have many "hard" instances—which means that no matter which algorithm you use, the amount of computation will grow exponentially as the example of the problem gets larger. Each time a number to be factored into two primes gets larger by two digits, for example, the number of trial-and-error divisions needed to solve it increases by as much as a factor of 10. Number theorists have devised factoring algorithms that are far more efficient than trial-and-error, but even these methods are stymied by prime products approaching 200 digits.

JOYCE BENNA



Hard problem. Finding the shortest pair of vectors (green arrows) that defines a lattice of points is easy in a two-dimensional lattice like this one. But Miklos Ajtai has shown that for higher dimensional lattices the problem is just about guaranteed to be hard.

Most cryptographers believe that as long as you take care to avoid certain types of primes, the product of two randomly chosen primes will be reliably hard to factor. But consensus is not proof—an aphorism that was driven home in the early 1980s, when one of cryptography's old standbys, the so-called "knapsack" problem, turned out to be a pushover. The essence of this problem is a familiar phenomenon: It's always easy to empty a container, but it can be quite a challenge to get all of its contents to fit back in. Although no one has yet found an algorithm that solves every instance of the knapsack problem, researchers found algorithms that succeed so often that finding instances where they fail is itself computationally impractical.

And that raises the prospect of a similar weak spot in the cryptosystems now in use. One can imagine, for example, a criminal mastermind or foreign agent who has discovered a fast factoring algorithm that works on some percentage of the prime products that are currently considered safe to use. The percentage may be small, but if the stakes are high, the investment will pay off. "What we'd like is some guarantee that you're generating instances that in all likelihood are very hard to crack," says Raghavan.

Enter Ajtai. Ajtai focused on lattice problems—ones involving a regular array of points in n-dimensional space, such as the locations of atoms in a crystal. Arrows extending from any point in the lattice to any other point are called vectors, and their lengths vary depending on which points they connect. If the lattice sits in a small-dimensional space, it's not hard to compute what the shortest vectors are, just as it's not hard to compute the factors of a small number. But if the dimension is large, all known methods of finding short vectors are computationally intractable—and most if not all complexity theorists believe this will always be so.

Ajtai's result does not rule out the possibility that someone will overturn this assumption by finding an efficient algorithm for solving the lattice problem. Rather, what he has shown is that it's impossible to solve any finite fraction of instances unless one can actually solve all of them. And because mathematicians have failed to find an efficient algorithm for solving all examples of the problem, Ajtai's result boosts their confidence that randomly generated lattices will be tough enough to baffle the most determined codebreaker.

Ajtai's discovery doesn't immediately lend itself to practical applications in cryptology, except perhaps as a "digital signature": By appending an instance of a lattice problem to a document, you could later identify yourself as the author of the document by revealing the answer to the problem. (Solving a lattice problem may be hard, but it's easy to start with an answer and come up with the matching problem.) The lattice problem could also

underlie an authentication protocol for computer communications, in which each machine would show that it is "known" to the other by submitting the answer to an instance of a problem it had transmitted during an earlier session. But so far there is no obvious way to embed secret information in randomly generated lattices.

That's not to say it can't be done at all. Inspired by Ajtai's breakthrough, Goldwasser and her colleagues at MIT have a scheme for creating a code based on lattice problems. However, she points out that the extra structure required to incorporate useful code into the lattice problem alters the problem itself, so that Ajtai's theorem may not automatically carry over. "We have a lot of experimental results that seem encouraging," she says, but not the kind of confidence that comes from theory.

IBM researchers are also looking for ways to put Ajtai's discovery to work, but they see it mainly as a fundamental advance in the theory of hard problems. "It's been sort of a Holy Grail of cryptography, to do what [Ajtai] has done, for any sort of problem whatsoever," says IBM's Ron Fagin. An eventual payoff is both certain and unpredictable, adds IBM's Ashok Chandra: "As with all foundational discoveries, it can go in unexpected ways." Guessing the future of computational codes may be no easier than cracking them.

–Barry Cipra

PLANETARY SCIENCE

Galileo Gazes at Jupiter and Its Moons

With the public still dazzled by the possibility of life on Mars, NASA last week unveiled images that point to surprisingly Earth-like processes on other heavenly bodies. The new data come from the Galileo spacecraft, which is now touring Jupiter's vast system of moons and catching much-improved views of features that planetary scientists had only glimpsed in the 1979 flybys by the Voyager spacecraft. Among other things, it has revealed thunderstorms on the giant planet itself and suggestive evidence of a water ocean—the first on any planetary body outside Earth—on another moon, Europa.

These results not only offer new insights into the workings of alien worlds; they may even enhance scientists' understanding of weather systems on Earth, researchers say. "That's one of the reasons we do comparative planetology," says James Head of Brown University, a member of the Galileo imaging team. "When you leave the neighborhood, you see things back home in a different way. It never fails to give a new perspective."

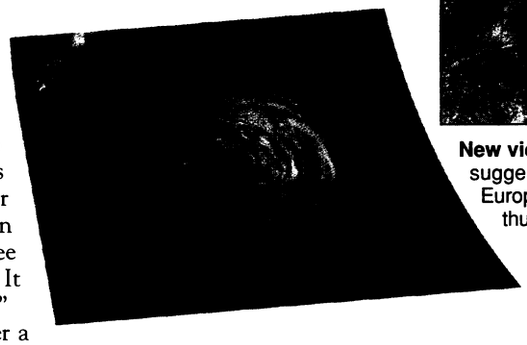
Galileo gathered these images after a close encounter in late June with another of Jupiter's moons, Ganymede, which revealed hints of a magnetic field (*Science*, 19 July, p. 311). The spacecraft then swept within 155,000 kilometers of Europa, a body about the same size as Earth's moon—close enough to provide "just sensational" images, says Steven Squyres, a planetary scientist at Cornell University in New York. The Voyager missions had showed a cracked, icy crust on this moon, raising the possibility that a liquid water ocean was sloshing under its icy shell, perhaps heated by the friction of massive tides caused by Europa's proximity to Jupiter. Galileo's closer look strengthens the idea of an ocean, revealing a jigsaw puzzle of ice pieces that appear to have cracked apart, moved slightly, and then frozen together again.

The simple patterns are the telltale sign, says Head, a planetary geologist. "You can put the jigsaw pieces back together by moving them laterally and simply," he says. "Qualitatively, it just screams at you that it might have been a relatively thin layer that broke up and moved," presumably as it rode on a lubricating layer of slush or even liquid water. The width of the cracks—as much as 10 kilometers—is more evidence for a semi-liquid layer, Head argues, because only a "pretty mobile interior" would allow so much crustal movement. But whether the layer is truly liquid—and conceivably hospitable for life—is uncertain. "Whether it's like a daiquiri or a margarita, we're not sure," Head says.

The issue could be settled late this year or early next year, when Galileo passes within 600 kilometers of Europa's surface. But the only convincing proof would be to catch a geyser of liquid water in the act of erupting through the icy crust, which would require a great stroke of luck, says Squyres. The problem is that Galileo doesn't carry an instrument aimed specifically at detecting water, because its instruments were selected before Voyager—and before anyone had any thoughts of an ocean on Europa. A definitive answer will probably have to wait for another mission carrying instruments able to penetrate ice, such as long-wavelength radar, says Squyres.

But Galileo does have the right equipment to solve another mystery of the Jovian system. Voyager had detected lightning flashes on the night side of the planet, and planetary scientists have been seeking thunderstorms, complete with rain, in Jupiter's thick atmosphere ever since. But "Voyager had the wrong camera," says Andrew Ingersoll of the California Institute of Technology. And Galileo's probe, which plunged into Jupiter's atmosphere late last year, found less water than expected, although the probe may have fallen into an especially dry spot (*Science*, 2 February, p. 593).

But in the latest work, team scientists used Galileo's three near-infrared filters, which can detect the difference in light reflected from clouds of varying heights. That allowed them to map cloud heights around Jupiter's great red spot. They found several patches of cumulus clouds that tower 50 kilometers above their neighbors and seem to cluster together—characteristics typical of thunderheads on Earth.



NASA/JPL

New views. Refrozen cracks suggest liquid water beneath Europa's ice (*above*); a Jovian thundercloud (red and white) towers over other clouds (blue and black, *left*).

These thunderclouds are consistent with the idea that there is indeed some moisture on Jupiter, says Ingersoll. And they suggest that the heat-driven vertical circulation patterns called convection, which drive thunderstorms on Earth, also take place on Jupiter, says Timothy Dowling, a meteorologist at the Massachusetts Institute of Technology. On Jupiter, however, the heat moves upward from the depths of the planet (*Science*, 14 June, p. 1589).

The three-dimensional data on the thunderclouds will help scientists better model the Jovian weather. In fact, says Dowling, Jupiter could offer valuable insights into the forces that drive weather on Earth, by providing a simplified model of wind and weather patterns uncomplicated by land masses or mountains. "Jupiter is giant and roomy," Dowling says. "Earth is crowded and chaotic." If scientists can understand how the cumulus towers work on Jupiter, he says, it may improve models of cloud behavior on Earth—and add an earthly bonus to results from other worlds.

–Gretchen Vogel