

stitute of Science in Israel. Mina Bissell of California's Lawrence Berkeley National Laboratory, who has shown that mechanical stresses on human malignant cells can determine whether they proliferate into a tumor or lie dormant, adds: "They have beautifully demonstrated the nature of the physical connection" between a cell's surroundings and genes in the nucleus. "I think we are looking at very similar phenomena."

In a second paper, which appeared last week in the *Journal of Cellular Biochemistry*, Maniotis, Ingber, and Krzysztof Bojanowski describe evidence that this kind of mechanical continuity extends into the nucleus. Using micropipettes that had been carefully drawn so that their tips were roughly a wavelength of light in thickness, the researchers harpooned structures in the nucleus itself. "You read a lot of *Moby Dick* and you practice," says Maniotis. He and his collaborators then drew the structures—nucleoli and chromosomes—out of the breach in the nucleus. Even though chromosomes extracted from dead, fixed cells typically appear isolated, the experiment showed that in the living cells, the chromosomes and nucleoli were always connected by flexible strings. The connections turned out to consist of DNA, as the team determined by treating the strands with a range of chemicals that snip only specific molecules.

If this is the case, the clean separation between chromosomes seen in other micrographs may be an artifact of sample preparation. "On a [heretical] scale of one to 10," says Ingber, this is "an 11." But the Harvard group is not alone in this heresy. Mohamed El-Alfy and Charles Philippe Leblond of McGill University in Montreal recently reported at a conference that they, too, have seen the DNA connections in all phases of the cell cycle—even though they used an entirely different technique based on electron microscopy. "This is really strong proof that there are bridges between chromosomes," at least in many cells, says El-Alfy.

What it all shows, says Peter Davies, director of the Institute for Medicine and Engineering at the University of Pennsylvania, is that "the cell structure is an integrated entity where the parts are connected." Although it will take further work to learn whether these links really do carry signals to the genes in the nucleus, researchers seem to agree that the results are changing the way biologists think about the cell. "For a long time, the mechanical and engineering aspects of cell biology were not appreciated," says David Bensimon, a biophysicist at the École Normale Supérieure in Paris. "This type of experiment ... certainly suggests that there is much to learn about the possible mechanical control of DNA and gene expression and regulation." Although geodesic domes may be out of fashion now, their principles could live on in biology.

—James Glanz

OPTICAL COMMUNICATIONS

Chaos Keeps Data Under Wraps

PARIS—Not long ago, chaos was a bugbear of electronic and optical systems, creating seemingly unavoidable noise and uncertainty in computation and communication. Now, says physicist Edward Ott of the University of Maryland, College Park, "People have begun to ... use it for practical purposes." The latest example came last month when a group of French scientists announced that it had harnessed chaos to protect optical-communications signals from eavesdroppers.

Researchers learned how to use chaotic fluctuations to hide data in electronic signals several years ago. Creating chaotic fluctuations in frequency in an optical signal, then reliably removing them at the receiver, is a logical next step, and that's what the French group has done. The new scheme, developed by Jean-Pierre Goedgebuer, Laurent Larger, and Alexis Fischer of the University of Besançon, is exceptionally fast, allowing encrypted signals to make full use of the high transmission speeds of fiber-optic cables. Daniel Gauthier of Duke University calls it "an interesting first demonstration," adding: "The high-speed aspect of it would be quite useful."

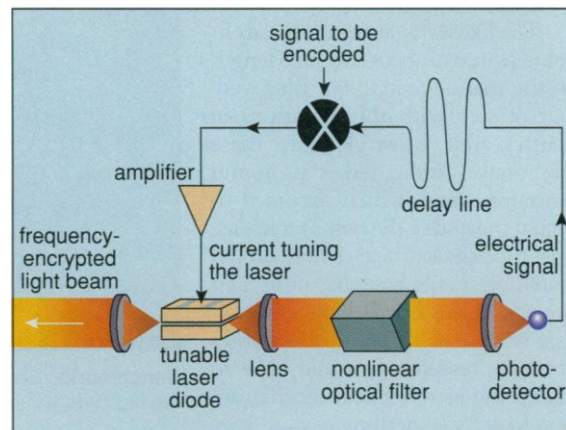
With the rapid growth of communications, encryption has developed into an industry. Encryption schemes that rely on numerical "keys," however, have a drawback: the processing time needed to encode and decode the information. Chaos offers a faster solution. Just as a microphone brought too close to an amplifier creates feedback, some types of circuits can become caught in a loop and generate chaotic fluctuations in frequency, masking the information they are carrying. Researchers realized that if they could generate an identical copy of the chaotic signal at the receiver, they could quickly subtract it from the signal to recover the original data.

Some electronic circuits readily generate identical chaotic signals because their chaos is "deterministic." As a result, identical circuits with the same physical parameters will produce identical chaotic signals. In 1993, electronic engineers Kevin Cuomo and Alan Oppenheim of the Massachusetts Institute of Technology were the first to harness deterministic chaos for encryption in an electronic communication system (*Science*, 23 July 1993, p. 429).

Now the Besançon group has shown that the principle can be applied to beams of light. The team encrypted a data signal carried by a laser beam by controlling the laser diode with an electro-optic feedback loop. The loop con-

sists of a "birefringent" filter that responds nonlinearly to changes in beam frequency by transmitting more or less of the beam, and a photodetector that converts the flickering light into an electronic signal. The data signal is superimposed on this fluctuating electronic signal, which is then amplified and fed back to the laser diode, varying its frequency chaotically to create the encrypted signal.

The receiver contains an identical feedback loop with the same settings. When an encrypted beam arrives, it is split in two with a beam splitter. One part passes through the feedback loop and causes a second diode laser to emit an identical chaotic signal—but this time without the data signal having been added in. This chaotic signal is then inverted and superimposed on the other part of the incoming



Caught in the loop. This electro-optic feedback loop creates chaotic frequency fluctuations that mask the data carried.

encrypted signal, canceling out its chaotic component to reveal the original data. This process is fast and secure, says Larger: "For the type of chaos we are using, called hyperchaos, the signal appears very much as random noise."

Goedgebuer says the system could be valuable where high speed and low cost are critical, such as encrypting cable-TV transmissions. Jean-Yves Le Traon of France Telecom's research branch in Lannion, which supported the research, expects applications on a limited scale in about 5 years: "We hope to increase security in this way ..., especially if we combine optical with numerical encryption."

Gauthier says he's impressed that the company is taking a serious interest in this exotic concept: "The industry is so set in its standards that trying to do something like this would have to be a major shift. If they are really convinced it is cheap, they might be willing to switch over."

—Alexander Hellemans

Alexander Hellemans is a science writer in Paris.