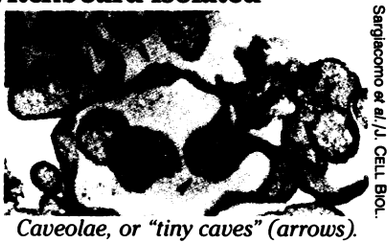
Biology

Cells' chemical switchboard isolated



M. Sargiacomo *et al.*/J. Cell Biol.

Caveolae, or "tiny caves" (arrows).

Just as the ear funnels sounds to where nerve endings can sense them, tiny chambers located on cell surfaces gather chemical signals and convey them into the cells. Researchers first observed these structures in cell membranes in the late 1950s, but only now have scientists isolated them, says Michael P. Lisanti, a cell biologist with the Whitehead Institute for Biomedical Research in Cambridge, Mass. The chambers, called caveolae, or "tiny caves," keep cells in touch with their neighbors and with their environment, he says.

By accident, Lisanti and his colleagues discovered that a particular detergent could dissolve most of a cell, leaving behind caveolae and the cell's internal framework, or cytoskeleton. Then they found that in a sugar solution, the cytoskeleton sinks while the lipid-laden caveolae float. This makes them easy to isolate and study, Lisanti's group reports in the August Journal of Cell Biology (Vol. 122, No. 4).

Copies of a protein called caveolin cluster to help form caveolae, he adds. Other researchers had shown that a virus can alter this protein, causing cells to become cancerous. Scientists can now try to determine whether this change affects how cells respond to growth-stimulating substances, says Lisanti.

Lisanti's group has found that many other kinds of messenger molecules hang out in caveolae, leading Lisanti to call these cavities signaling organelles. This cellular switchboard may relay many chemical messages to the cell's interior. For example, these messenger molecules suggest that caveolae play a key role in calcium-based signal systems and those involving sugar-containing lipids, called glycolipids. The new findings indicate that some pathogens exploit this access. For instance, bacterial toxins that lead to cholera and whooping cough home in on the glycolipids, then exert toxic effects by modifying signal proteins also in these chambers, Lisanti notes.

Eavesdropping on cetacean chatter

In addition to listening for submarines, the U.S. Navy has begun sounding out whales in the North Atlantic, allowing scientists to detect the wide array of noises these marine mammals make. In just three months, the Navy's network of listening devices picked up whale sounds 35,000 times, says Christopher W. Clark, a bioacoustics expert at Cornell University.

Different whales speak different "languages," and there even appear to be regional dialects, Clark reported last month in Davis, Calif., at the annual meeting of the Animal Behavior Society. Blue-whale calls, sped up tenfold, resemble bird chirps, while the revved-up calls of minke whales resemble clicks heard in a subway train, he says.

Differences in the timing of chirps and clicks or in the way the whales change frequencies can account for regional differences in whale talk, notes Adam S. Frankel, a marine mammalogist at Cornell. Blue whales may bounce their loud chirps off the seafloor to get an audio read of the topography, he speculates.

The Navy listening system also enables researchers to locate the source of each sound. In one case, they followed a blue whale for 43 days as it moved from Cape Cod to Bermuda and then headed to Florida before returning to Bermuda, says Frankel.

The researchers hope to use the system to learn about the whales' seasonal movements as well as their vocalizations. "This technology is going to revolutionize the way people look at and listen to whales," says Frankel, who thinks researchers will also estimate population sizes on the basis of this chatter.

Computers

High marks for encryption algorithm

The security of an encryption scheme depends in part on the quality of the mathematical procedure, or algorithm, used to scramble digitized speech or text into unintelligible strings of digits. Only recipients with the appropriate "key" should be able to decipher the coded message. Earlier this year, the White House proposed a novel "key-escrow" cryptographic system based on an encryption algorithm developed in secret by the National Security Agency (NSA). This represented the first time that classified encryption technology had been offered for public use (SN: 6/19/93, p.394).

To help allay fears that the secret algorithm, known as SKIPJACK, may contain a loophole or exhibit some other kind of weakness that could undermine the system, NSA gave five cryptography experts a chance to assess the algorithm's quality. "The government's new encryption algorithm is first-rate," concludes computer scientist Dorothy E. Denning of Georgetown University in Washington, D.C., who participated in this independent review of the algorithm.

Incorporated in an integrated-circuit chip placed in a security device attached to a telephone, the algorithm handles digitized speech in 64-bit chunks. In essence, it converts each incoming string of 64 ones and zeros into a scrambled sequence of the same length. It also requires the use of an 80-bit key as part of the encryption process.

Starting in late June, each of the five experts independently tested the SKIPJACK algorithm in a variety of ways, looking for potential flaws in the scheme. These tests failed to turn up any weaknesses. Indeed, the algorithm behaves "like a high-quality random-number generator," says Denning.

In a joint report, the five experts concluded that, even with tremendous increases in computer power, there was no significant risk that SKIPJACK could be broken in the next 30 or 40 years by an exhaustive search based on trying every possible key. They also dismissed the possibility that a shortcut method of attack would succeed.

Denning presented the group's findings at a meeting of the Computer System Security and Privacy Advisory Group, held late last month at the National Institute of Standards and Technology in Gaithersburg, Md. The other members of the SKIPJACK review panel are Ernest F. Brickell of Sandia National Laboratories in Albuquerque, N.M., Stephen T. Kent of BBN Communications Corp. in Cambridge, Mass., David P. Maher of AT&T in Andover, Mass., and Walter Tuchman of Amperif Corp. in Chatsworth, Calif.

Because SKIPJACK is just one component of a large, complex encryption system, these experts plan to assess the strength of the entire key-escrow scheme as soon as the federal government settles various technical details. "When it's ready, we'll evaluate it," Denning says.

A standard for key-escrow encryption

Charged with the responsibility for setting the rules needed to protect the security and privacy of unclassified information in federal computer systems, the National Institute of Standards and Technology last month announced its proposed voluntary standard for key-escrow encryption. The standard specifies using the SKIPJACK encryption algorithm and a method for creating a "Law Enforcement Access Field" (LEAF) — a mechanism by which authorized government agencies can decipher lawfully intercepted encrypted telecommunications.

Both the algorithm and the LEAF method will be incorporated in an integrated-circuit chip and used in encryption devices attached to telephones. To take advantage of the scheme's LEAF capability, government officials legally authorized to conduct a wiretap would need to obtain key components held by two separate escrow agents.