A number of questions remain to be answered about the gene cloned by Davis and his colleagues. Although it has the expected characteristics of a gene coding for a T cell receptor protein, there is as yet no evidence regarding its function or that of its product. Nevertheless, it should soon be possible to transfer the cloned gene into cells, see whether the product is expressed on the membrane as it should be, and determine whether the product can alter antigenic recognition by T cells and whether antibody to the product can block T cell function.

Also important are the questions about the number and organization of the sequences in the genome that carry information that may be used to produce functional T cell receptor genes and whether the gene cloned by the Davis group can be used as a probe to identify related sequences. But if further work confirms that the cloned gene is the first example of a T cell receptor gene, as it appears to be, it may provide the key to unlocking the secrets of T cell recognition of antigen.—**JEAN L. MARX**

Scheme to Foil Software Pirates

Three Israeli scientists have proposed a new scheme to protect computer programs from illegal copying. If adopted, their method could eliminate a major headache in the computer software industry and one that has driven some manufacturers out of business. The scheme was devised by Adi Shamir, a mathematician at the Weizmann Institute of Science, who is known for his innovative work in cryptography, and his two students Amos Fiat and Yossi Tulpan. A manuscript describing their idea is just now being circulated in the scientific community. "It is a very clever idea," says Ronald Rivest of the Massachusetts Institute of Technology.

Shamir proposes that software manufacturers modify their computer programs to create special sections that contain weak bits—meaning bits that are sometimes read as a 0 and sometimes as a 1. These special areas will serve in his scheme as "the software equivalent of a coin-operated machine," he says. Most important, personal computer owners will not be able to duplicate the weak bits on their own machines and the programs will not run without them.

The problem facing the software industry is that computer programs on floppy disks can easily be copied. These programs often are quite expensive; business programs frequently cost hundreds of dollars and even game programs typically cost about $35. Blank disks, however, are cheap, costing only a few dollars. Thus many people who buy computer programs copy them and distribute them to their friends. In the end, Shamir points out, "this practice penalizes other users by forcing them to pay more for legally obtained software."

A few years ago, the manufacturers thought they could solve the piracy problem by writing the program on the disk in nonstandard ways—writing in blocks distributed in a spiral pattern along the disk or writing between the grooves of the disk, for example, so that the disk could not be copied. But a few enterprising entrepreneurs quickly began selling special programs, with names like Locksmith and Nibbles Away, that unscrambled this copy protection scheme. It was legal to sell such programs because users of computer software are entitled to make backup copies for their own use.

Shamir thinks his method, based on a statistical approach to error analysis, may "be the ideal solution: high security, low cost, no hardware modifications, and complete transparency to the user. The new scheme even solves the harder problem of controlling the number of times rented software can be used." Shamir has been talking to software manufacturers on an informal basis. "All of them like the idea," he says.

Shamir and his colleagues describe their scheme as adding "coupons" to software so that each time the program is run the coupon is reduced in value. The user cannot produce copies of the coupons and cannot modify them. As a result, Shamir says, "A home computer owner will be able to buy a new video game or a cheap diskette which can be used 100 times, and if he likes the game he can buy more expensive 500, 1000, or unlimited use diskettes."

The "coupons" are produced by software manufacturers who modify their disk drives so that they write some weak bits on the diskette. Weak bits sometimes occur by chance when disks are produced but they are corrected by rerecording the data or by error-correcting codes. Shamir proposes, however, that hundreds of weak bits be intentionally written on certain tracks or sectors of the diskette which are explicitly chosen by the computer programmer and hidden within the program.

When a consumer uses such a program, his computer is instructed to check for weak bits by reading over the coupon section several times. If weak bits are there, they will show up sometimes as a 0 and sometimes as a 1. The computer checks to see that there is no consistency in the way the coupon is read. Every time the program runs, it is instructed to destroy one of the weak bits by changing it to an unambiguous 0 or 1. Eventually, there will be few weak bits left and the program will no longer run unless a new coupon is purchased.

Consumers could also purchase programs that will run indefinitely. This would be done by instructing the home computer never to alter the coupon, a method known as write-protecting.

The program also can be copied onto backup disks or moved to a faster and larger hard disk. The original disk then would be used for license verification. The Israeli scientists note that this license has the advantage that it is not affected by wear and tear. "A few more errors in some of the coupons are unlikely to change the validity of the license," they say. The program can also monitor how many coupons are left so that users can know well in advance that they need to replace their disk.

The reason the coupon scheme should work, Shamir points out, is that disk drives on home computers are designed to work reliably. They are incapable of introducing weak bits. If a consumer tries to copy the coupons, he will get a copy containing only normal bits, meaning unambiguous 0's and 1's that are put in more or less arbitrarily by the computer whenever a weak bit is encountered.

Of course, no protection scheme can ever be completely secure. In the case of Shamir's system, some hardware experts will undoubtedly be able to modify their own disk drives to copy weak bits. But most software pirates are unlikely to want to fool around with the hardware in their delicate and expensive disk drives, Shamir contends. "The real problem is not to create a fool-proof system but to make sure that for most users it makes more economic sense to rent or buy the software than to try to steal it. In this billion dollar industry, even a partial reduction in software misuse will have enormous economic impact," he says.

—**GINA KOLATA**