AT&T INNOVATION BRIEFS

Innovation Briefs are summaries of recent discoveries and developments within AT&T Bell Laboratories. Those wishing further information, or AT&T readers who would like to contribute future items, are encouraged to contact the AT&T Technical Journal *editor.*

Protocol Failure in the "Clipper" Chip

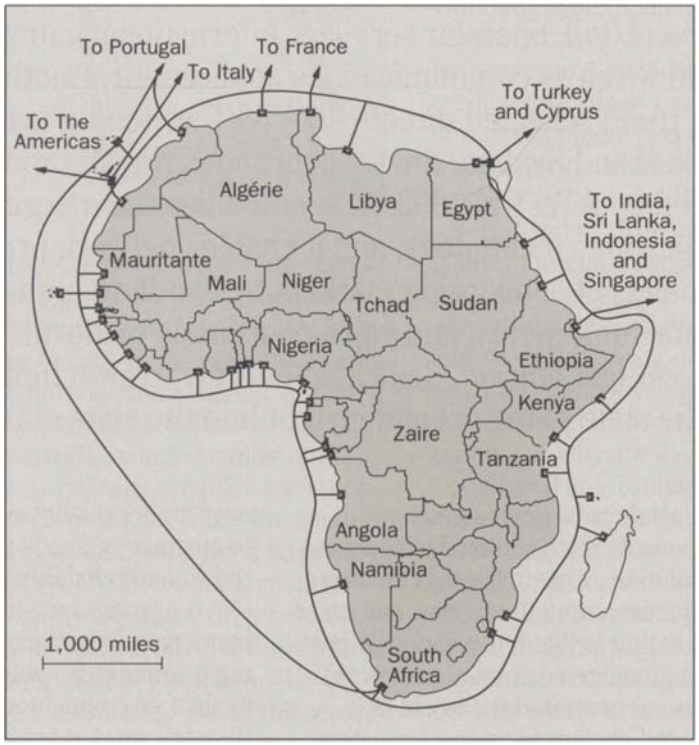
The Escrowed Encryption Standard, popularly known as the "Clipper" chip, is a U.S. government-developed system for protecting sensitive communications and data. The Clipper system is intended to make widely available a strong cipher that does not compromise law enforcement access to encrypted data. A basic (and controversial) feature of the system requires communicating Clipper devices to precede all encrypted traffic with a special message (called a "LEAF") that contains session key information to help authorized government wiretappers decrypt the traffic. An AT&T Bell Laboratories researcher recently discovered a variety of techniques, however, that make it possible to circumvent the government access feature by never sending the correct LEAFs. The simplest of these techniques requires minor changes, by both the sending and receiving applications, in the use of the chips. Another, more time consuming technique allows unilateral action by the sender, which creates a "forged" LEAF. This LEAF will be accepted as valid by the receiver, but does not contain the correct session key data needed for law enforcement access. Although these techniques are not appropriate for all applications of the Clipper system (in particular, they are probably too cumbersome to use in secure voice telephony), they demonstrate that it may not be viable for use in general computer and messaging applications.

Advancing Programmable Gate Arrays

Researchers have recently developed new algorithms and a prototype system that promise to help make AT&T Microelectronics a leader in the fast growing field-programmable gate array (FPGA) market. FPGAs provide a collection of programmable logic and routing resources that help integrated circuit designers shorten the time-to-market of their products. SCUBA, a new synthesis system for the AT&T ORCA (optimized reconfigurable cell array) FPGA, is being successfully used by AT&T applications engineers to win sales for ORCA. SCUBA produces very efficient results by taking advantage of dedicated hardware circuits in ORCA and by performing architecture-specific optimization, such as combining adders and registers so that they can be implemented in one logic cell. This technology is being transferred to an FPGA software development group, and should boost AT&T's position in the important area of FPGA synthesis.

All-Optical Undersea Transmission

AT&T recently proposed an African undersea cable network that includes a 32,000-kilometer optical fiber ring and links to about 40 countries. While evaluations of candidate architectures for such a network are proceeding, a transmission experiment was recently conducted by a team of AT&T Bell Laboratories researchers. The experimental system makes use of practical optical amplifiers that permit long-haul transmission of wavelength-division multiplexed (WDM) signals without the need for signal regeneration. By using densely spaced WDM signals, the researchers were able to transmit an aggregate 40 billion bits per second (Gbits/s) through 1,420 km of fiber without the need for regeneration. Sixteen channels, each operating at 2.5 Gbits/s, were spaced at 100-GHz frequency intervals. They were then transmitted, error free, through 13 amplified fiber spans ranging in length between 96 km and 123 km. These experiments demonstrate the feasibility of large-scale, all-optical networks having many high-speed channels.



Proposed African undersea fiber-optic network.