AT&T INNOVATION BRIEFS

The briefs in this section are summaries of recent discoveries and developments within AT&T Bell Laboratories. AT&T readers who would like to contribute future items, and readers who would like further information as well, are encouraged to contact the AT&T Technical Journal *editor.*

New Key Management System Supports Higher Levels of Protection

Cryptographic keys are the core pieces of information that enable communications or data to be digitally "signed" so that their authenticity and integrity can later be verified, or encrypted so that their secrecy can be preserved. Key management refers to processes by which cryptographic keys are generated, stored, distributed, used, and revoked in a system. Bell Laboratories researchers have developed a highly robust service to support key management in distributed systems. The service, called Omega, uses advanced protocols and cryptographic techniques to distribute the responsibility for key management functions among many servers in a way that can mask the failure or even the malicious penetration of some servers from clients. The result is a key management service that exceeds prior approaches in security, availability, and fault tolerance. It is the first key management system designed to support mission-critical electronic commerce tasks that use public networks. Omega currently exists as a research prototype and is being used to support World Wide Web applications within AT&T.

Scaleable WDM Multiwavelength Chirped-Pulse Sources

Wavelength-division-multiplexed (WDM) networks such as those under study for long-haul and local access applications require compact multiwavelength WDM sources. Bell Laboratories researchers have invented a new configuration that can generate 32 or more wavelength channels with variable channel spacing and single-knob wavelength comb registration. The bit rate per channel is of the order of 50 Mb/s. The new WDM source consists of a femtosecond fiber laser, a dispersion element, and a single modulator. Electronic tuning selects the required wavelengths from the frequency-chirped pulse. The researchers have demonstrated error-free transmission with negligible WDM crosstalk in a WDM-PON (passive optical network) systems testbed.