

Cryptography workshop makes news

The event was the 1999 Workshop on Cryptographic Hardware and Embedded Systems (CHES), which brought 180 computer security experts, half from outside the United States, to campus in August. Organized by Christoph Paar, associate professor of electrical and computer engineering, and Çetin Kaya Koç, an electrical engineering professor at Oregon State University, it provided a forum for scientists and engineers to share ideas and explore new research contributions, including new methods for efficient hardware implementation and high-speed software for embedded systems (such as smart cards and microprocessors).



From left, Christof Paar, Brian Snow of the U.S. National Security Agency, and Çetin Koç.

One of the conference's most anticipated talks was by Adi Shamir of Israel's Weizmann Institute of Science. Shamir was one of the inventors of RSA (the "S" stands for Shamir), a widely used cryptosystem that protects 95 percent of today's e-commerce. RSA enables users of popular Web browsers like Netscape Navigator and Internet Explorer to send their credit card numbers and other private information over the Web safely. Shamir called the security of those browsers into question with an announcement that made news worldwide.

He described a computer he has designed that is capable of defeating RSA in a matter of days--something once believed to take months of computation. Shamir's computer, which he calls TWINKLE, would greatly speed the process of factoring large numbers--the basis for RSA's security algorithm. He said such a workstation could be built for about \$2 million.

Shamir's announcement and the CHES workshop attracted a great deal of media attention, according to Neil Norum, WPI's director of media and community relations. Jeff Donn, national science writer for the Associated Press, covered the conference, and his stories appeared in newspapers worldwide. Articles also appeared in the print and on-line editions of The New York Times and The Boston Globe, in The Wall Street Journal, and in many on-line publications covering the computer industry.

The CHES workshop explored the future of data security. "Cryptography is the key tool for computer system security," Paar says. "It is rapidly moving from a somewhat esoteric niche area into an important discipline with applications to virtually all future information technology products such as PCs, wireless phones and Web TV. The goal of cryptography is to encrypt messages to ensure that they are not being altered; doing that requires controlling access to information so that others cannot tap into it. The process involves complex mathematical calculations that encode information to keep it safe from prying eyes.

"The future information superhighway will include more and more consumer services, such as electronic payment systems, medical applications, home shopping and

interactive digital TV," he adds. "Much of this information infrastructure will be wireless--and therefore vulnerable--and there are growing concerns about the security of the information and communications systems."

Paar, who is also a member of the Computer Science Department faculty, came to WPI in 1995. He is head of the University's Cryptography and Information Security Group (CRIS) and directs the CRIS laboratory. In 1998 he received the National Science Foundation's Early Career Development (CAREER) Award and is a former Joseph S. Satin Distinguished Fellow in Electrical Engineering.

