



**COLLEGE OF ENGINEERING**  
**OREGON STATE**  
**U n i v e r s i t y**



[www.engr.orst.edu](http://www.engr.orst.edu)

[COE Homepage](#) « [COE News](#) « [09/27/99](#) « [ECE Prof Helps Organize New Cryptographic Workshop](#)

[COE Home](#)

[Departments](#)

[Advising](#)

[Graduate and  
Research  
Programs](#)

[Coop Programs](#)

[Computing  
Support](#)

[News](#)

[Info Request](#)

Search COE:

 

101 Covell Hall  
 Oregon State Univ.  
 Corvallis, OR 97331-2409  
 541.737.3101  
 541.737.1805 (FAX)

## ECE Prof Helps Organize New Cryptographic Workshop

More than 160 scientists and industry experts from around the world had come to Worcester, Mass., on Aug. 12-13 to attend the Workshop on Cryptographic Hardware and Embedded Systems (CHES), held at Worcester Polytechnic Institute.

"CHES is an entirely new type of cryptographic workshop," say the organizers Cetin K. Koc, a professor of Electrical and Computer Engineering at Oregon State University and Christof Paar, a professor of Electrical and Computer Engineering at WPI. "Cryptography is rapidly moving from a somewhat esoteric niche area into an important discipline with applications in virtually all future information technology products such as personal computers, wireless phones or Web-TV. This workshop provided, for the first time, a forum for scientists and engineers concerned with the realization of cryptography in such products."

Cryptography is the key tool for computer system security.

"Down the road, all kinds of consumer products will have computer-like capabilities," Koc and Paar say. "That means you have to add the security functions to an embedded system. This is a major challenge since devices such as palmtop organizers or wireless phones have far less computational capabilities than modern PCs."

With the WPI workshop, cryptography returns to its roots. Modern cryptography began in 1917 when a WPI alumnus, Gilbert S. Vernam (class of 1910), an employee of AT&T, invented a system for automatically encoding and decoding information. However, basic cryptography has been around for ages; smoke signals, for example, are an early form. New uses for cryptography are limitless.

"The future information superhighway will allow more and more consumer services such as electronic payment systems, medical applications, home shopping and interactive digital TV, to name only a few possibilities," Koc and Paar say. "But much of that information infrastructure will be wireless, and thus vulnerable. It raises growing concerns about the security of the information and communications systems."

Without a doubt, cryptography is rapidly moving into the forefront of technology tools. The goal of cryptography, is to encrypt messages and to assure that they are not being altered, thereby controlling access to information so that others cannot tap into it.

"In the future, the consumer should never know or see the systems that ensure that," Koc says. The process involves complex mathematical calculations that encode information to keep it safe from prying eyes.

At the WPI workshop, invited speakers talked about the latest developments in this ever-widening field. Among the highlights of the presentations is a talk by world-renowned

cryptographer Adi Shamir of Israel. He presented the design of a new computer that allows breaking the RSA cryptosystem more efficiently. RSA is the most widely deployed public-key scheme in the world. As a consequence of Shamir's invention, RSA will have to be lengthened in order to provide adequate security.

In addition, Brian Snow of the U.S. National Security Agency gave a speech titled "We Need Assurance." Eberhard von Faber of Germany's Debis IT Security Services spoke on "Security Evaluation Schemes for the Public and Private Market with a Focus on Smart Card Systems." And Colin D. Walter of the United Kingdom's UMIST Computation Department talked about "An Overview of Montgomery's Multiplication Technique: How to Make It Smaller and Faster."

At the WPI CHES workshop, the latest results from the research community and industry were presented, including new methods for efficient hardware and high-speed software implementation of cryptographic schemes in embedded systems.

"We hope that the workshop will help to fill the gap between the cryptography research community and the application areas of cryptography," Koc and Paar say. "The concentrated presentation of cryptographic developments of high practical relevance is entirely new, and the many participants from U.S., European and Asian companies are a strong indication that CHES is an important forum for modern cryptography."

The proceedings of the CHES Workshop will be published by Springer Verlag, in the Lecture Notes in Computer Science series as No. 1717. More information about the CHES 2000 can be obtained from either Christof Paar or Cetin K. Koc .

Dr. Koc is a full professor in the ECE Department and the director of the Information Security Laboratory <http://security.ece.orst.edu>.

There were more 160 participants, who were much impressed by the quality of the talks presented, most of whom expressed their desire to come to CHES in the year 2000. Koc and Paar plan to hold the CHES Workshop either again at WPI or at some location on the west coast the next year.

Copyright © 1998 OSU College of Engineering  
Comments & suggestions: [webmaster@engr.orst.edu](mailto:webmaster@engr.orst.edu)  
Page last modified: Sun, Oct 10, 1999.  
[Oregon State University](#) - [Web Disclaimer](#)