

POMONA COLLEGE

COMPUTER SCIENCE COLLOQUIUM

**Is My Smart Card Secure?
Side Channel Attacks on Block Cipher Implementations**

Prof. Kevin Compton
University of Michigan -- Ann Arbor

In 2001 the National Institute of Standards and Technology (NIST) selected the block cipher Rijndael from a field of five finalists to become the Advanced Encryption Standard (AES), making it a standard for use by the U.S. Government to protect sensitive (unclassified) information. One selection criterion was that the cipher be easy to implement on inexpensive devices such as smart cards. This raises the question of security for smart card implementations of block ciphers. Smart cards leak information through side channels such as voltage fluctuations and electromagnetic signals. Is this enough information to break the cipher? We will describe a simple power analysis attack on an 8-bit implementation of AES which quickly finds the encryption key through an optimized search strategy. We also describe a different simple power analysis attack on Serpent, one of the other AES finalists. The talk will be self-contained and assumes no previous knowledge of smart cards, block ciphers, or side channel attacks.

Kevin Compton is on the faculty of the Computer Science and Engineering Division of the University of Michigan at Ann Arbor. He received a Ph.D. in Mathematics from the University of Wisconsin in 1980. He has worked in a number of areas in theoretical computer science including analysis of algorithms, complexity theory, formal verification, and computer security. His current research interests include security of block ciphers, cryptographic protocol verification, and analytic methods for average case analysis of algorithms.

Thursday, February 14 at 4:15 pm

Rose Hills Theater – Smith Campus Center

Pomona College

Refreshments available at 4:00