Major Area Exam
Theodore Huffmire
Wednesday, March 2\textsuperscript{nd}, 2005
10:00 am - CS Conference Room.

Committee: Tim Sherwood (chair), Chandra Krintz, Ryan Kastner

Title: Application of Cryptographic Primitives to Computer Architecture

Abstract:
Cryptography and computer architecture have co-evolved since the beginning of computer science. For computer architects, security has become a first-class design constraint alongside power and performance. This talk will examine the state-of-the-art in cryptographic processors, which efficiently implement the fundamental cryptographic primitives: asymmetric crypto, symmetric crypto, and one-way hash functions. Then, we will explore how others have applied cryptographic primitives to processor design. I will also discuss my research applying incremental hashing to analyze the memory behavior of computer programs. This lightweight mechanism can accurately identify regions of a program in which no memory leaked.

Everyone Welcome.

_______________________________________________
grads maillist - grads@lists.cs.ucsb.edu
http://lists.cs.ucsb.edu/mailman/listinfo/grads