Invited Talk

Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
Date: July 22, 2016 Time: 3:00 pm to 4:30 pm
Venue: KD 102

Formal Hardware Verification of Arithmetic Data-paths using Algebraic Geometry and Symbolic Computation

Priyank Kalla
Department of Electrical and Computer Engineering
University of Utah
http://www.ece.utah.edu/~kalla

Abstract:

In this talk, I will describe problems of word-level abstractions with applications to hardware verification of arithmetic data-paths. Data-path designs implement arithmetic computations over finite word-length operands (k-bit vectors). By interpreting these designs as polynomial functions over finite fields of 2^k elements, we can formulate the decision problems using concepts from commutative algebra and algebraic geometry such as Nullstellensatz, elimination theory, etc. Groebner basis techniques can then be employed to solve the verification instances.

While Groebner basis techniques can be powerful as reasoning engines, the computation suffers from high complexity. To overcome this complexity, I will show how we can analyze the structure and symmetry inherent in the data-path designs to get more insights into the corresponding polynomial ideals. Efficient symbolic computation algorithms can then be tailored to address such applications. I will motivate the verification context with applications from elliptic curve cryptography, and then discuss some challenges in generalizing such approaches to integer arithmetic circuits -- for which there are specific needs (and there is scope!) to improve symbolic computing algorithms targeted for hardware verification.

The talk should be accessible to electrical engineers, computer scientists as well as mathematicians from the commutative algebra and algebraic geometry community.

Biography:
Priyank Kalla is an Associate Professor in the Electrical & Computer Engineering department at the Univ. of Utah. His areas of interests are in electronic design automation and hardware verification. He received the B.E. degree in Electronics from Sardar Patel University in 1993, and M.S. and Ph.D. from the Univ. of Massachusetts Amherst in 1998 and 2002, respectively. He has worked with AMD K-7 and the DEC Alpha microprocessor CAD & Test groups. He's a recipient of the US NSF CAREER award and the ACM Trans. on Design Automation best paper award. He was the chair of IEEE technical committee on computer-aided network design and currently also serves as an associate editor for IEEE Trans. on CAD.