Computer Arithmetic - A Processor Architect's Perspective
(invited keynote)

Ruby B. Lee

Forrest G. Hamrick Professor of Engineering
and Professor of Electrical Engineering
Princeton University, USA
(rblee@princeton.edu)

Abstract

The Instruction Set Architecture (ISA) of a programmable processor is the native language of the machine. It defines the set of operations and resources that are optimized for that computer, information appliance or server. It is based on the workload characterization of the types of software expected to run on that computer. Unfortunately, the workload characterization upon which microprocessor ISA choices have been made has not kept up with the changing nature of general-purpose computations and communications. This has resulted in a plethora of special-purpose hardware chips and boards for these new information processing paradigms, and a general misunderstanding that software running on programmable processors cannot achieve certain performance, cost or power levels. Microprocessors that attain high performance levels in the new processing areas tend to have complex microarchitecture and very fast cycle times, both of which result in high cost and power. Actually, much faster, lower cost and lower power computations can be achieved by optimizing the Instruction-Set Architecture of the processor for these new information-processing paradigms.

In this talk, we discuss new ISA features, which address the increasing need for pervasive secure information processing and ubiquitous multimedia information processing. In particular, we discuss new arithmetic operations that are very useful for fast software cryptography or the processing of multimedia information. For example, we discuss novel permutation instructions and methodologies for achieving arbitrary permutations of bits and subwords in n-bit words. These are needed for fast symmetric-key cryptography and in multimedia applications. We also discuss interesting forms of saturation arithmetic and their applications, and other new types of computer arithmetic. The realization of these new arithmetic operations calls for innovative logic and circuit implementations of new functional units, or imaginatively enhanced adders, shifters and multipliers. These new computer arithmetic circuits can be used in microprocessors, media processors, cryptography processors, digital signal processors and programmable System-On-Chips.

Ruby B. Lee joined Princeton University in September 1998 as the Forrest G. Hamrick Professor of Engineering and Professor of Electrical Engineering with an affiliated appointment in the Computer Science department. She is the director of the Princeton Architecture Laboratory for Multimedia and Security (PALMS).

Prior to joining the Princeton faculty, Dr. Lee served as chief architect at Hewlett-Packard, responsible at different times for processor architecture, multimedia architecture and security architecture for e-commerce and extended enterprises. Key technical contributions include the initial definition and evolution of the PA-RISC architecture for mission-critical business computers, high

Proceedings of the 15th IEEE Symposium on Computer Arithmetic (ARITH'01)
1063-6889/01 $10.00 © 2001 **IEEE**

IEEE COMPUTER SOCIETY

performance technical workstations, and real-time factory-floor controllers. Dr. Lee was alsoa co-leader of an Intel-HP architectural team that defined advanced architectural features for multimedia and parallelism for IA-64, also known as an EPIC (Explicitly Parallel Instruction Computer) architecture – the first industrial post-RISC instruction-set architecture.

As chief architect for HP's inter-disciplinary multimedia architecture team, Dr. Lee introduced innovative multimedia instruction-set architecture (MAX and MAX-2) in microprocessors, resulting in the industry's first real-time, high fidelity MPEG video and audio player, implemented entirely in software, on low-end desktop computers. Subsequently, every major microprocessor family has implemented similar subword-parallel, multimedia instructions in their instruction-set architectures, enabling pervasive multimedia information processing with software implementations.

Concurrent with full-time employment at HP, Dr. Lee also served as consulting associate professor, then consulting professor of Electrical Engineering at Stanford University. She has been granted 88 U.S. and international patents, with several patent applications pending. Dr. Lee has a Ph.D. in Electrical Engineering from Stanford University (1980), an M.S. in Computer Science and Computer Engineering, Stanford University, and an A.B. (with distinction) from Cornell University. She is a member of Phi Beta Kappa, Alpha Lambda Delta, IEEE, ACM and IS&T.

IEEE COMPUTER SOCIETY