2006 Summary Statement

Hsien-Hsin Sean Lee, Ph.D.
Assistant Professor
School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, GA 30332
leehs@gatech.edu

1 Introduction

Hsien-Hsin Sean Lee joined the School of Electrical and Computer Engineering of Georgia Tech as an assistant professor in fall, 2002. He received his Ph.D. degree in Electrical Engineering and Computer Science from the University of Michigan at Ann Arbor. Before joining Georgia Tech, he spent more than 5 years in the microprocessor and DSP industry (Intel Corporation and Agere's StarCore DSP Center) designing state-of-the-art microprocessor architectures and compiler technologies and managing engineering teams, in product development groups as well as in research labs.

2 General Summary of 2006

2.1 Research

Dr. Lee's research program mainly focuses on the emerging areas in computer architecture including security-aware processor architecture, low-power microarchitecture, and 3D microarchitectural physical planning issues. In 2006, Dr. Lee and his students continued to investigate and publish their research findings in these areas.

For the thrusts in secure computing, Dr. Lee and his PhD students (Shi and Fryman) investigated the information leakage problems through the vulnerability that exhibits in common program semantics, such as invalid input phishing, Trojan, memory scan, and buffer overflow. Toward these issues, they proposed a secure architecture called *InfoShield* which enforces security policies when using and propagating sensitive information in user level codes and proposes low-cost microarchitectural support to check violation at runtime. Using whole system emulator and documented exploits, they demonstrated such malicious exploits can be completely eliminated under the protection of InfoShield. The results were presented at the HPCA-12. Later, Dr. Lee and his students (Shi, Ghosh, and Yoo) further extended the scope of this research to examine similar exploits under the emerging multicore architecture and digital rights vulnerability in 3D graphics architecture. Firstly, they pioneered an idea called *introspective computing*, which unleashes the computing power provided by the extra processor cores in a multicore system for performing constant monitoring, instant checkpointing, and fast self-recovery. The new architecture called *Indra* provides high availability, reliability and self-healing capability with a new programming model on a multicore processor. This system provides multi-level insulation against remote exploits, fine-grained state logging between application and monitor cores, tight processor core coupling to enable fast checkpointing and recovery, and resilience when such protection is not needed. This work was presented at ISCA-33. Inspired by their work, Intel Labs at Pittsburgh started a similar architecture called Log-Based Architecture to research the practicality of the idea. Dr. Lee was invited to Intel Labs to give an overview of the Indra framework.

For their research thrusts in low-power architectures, Dr. Lee and his students (Ghosh and Woo) developed several architectural techniques for reducing memory power consumption. Collaborating with ARM researchers in England, they applied conventional counting Bloom filters inside cache hierarchy to predict L2 misses and address synonyms in L1. In this work, Bloom filters were integrated into a processor to record an address footprint. Each time a cache line is brought in the cache, its corresponding signature generated by the Bloom filter based on its address is updated in a bitmask. Using this bitmask, one can abort a power-consuming L2 access or unnecessary synonymous L1 lookup. Since a Bloom filter never generates false positive predictions, such a mechanism can be confidently applied to eliminate redundant memory accesses, thus saving energy. The second thrust of this research focuses on the DRAM memory power issue. The basic idea is to make the regular DRAM refresh operations access-aware. In other words, when a DRAM row was accessed recently by a demand access, there will be no need for performing another regular refresh operation. To obtain such a fine-grained control, small decayed counters were proposed in the memory controller to keep track of the access patterns and to trigger refreshes when only absolutely needed. The Bloom filter research on memory hierarchy was published in ARCS-06 and CASES-06. The DRAM decaying work was published in IBM PAC^2.

Another of Dr. Lee's major research activities is in 3D microarchitecture, a continuing award from MARCO/C2S2 in the amount of $450,000 (to Lee, Lim and Loh), Dr. Lee and his student (Mohamood) worked with Dr. Lim's group on the reliability issue due to high-frequency inductive noise for both 2D planar processor and the emerging 3D-integrated processor. They proposed a new design methodology to address this issue — instead of using a conventional worst case design, they advocated a *design for the average case* with a dynamic response system to handle the worst case. As such, the pressure of a large quantity of decoupling capacitance will be substantially reduced when aggressive clocking gating is applied to a processor. In fact, placing more decap for smoothing out inductive noise defeats the energy benefit of clock gating as decap itself increases leakage power in today's deep submicron process technology. In the first step of their design flow, they used a profile-feedback method to quantify the switching behavior including self-switching and correlated switching. Based on such information, a floorplanner called *Noise-Direct* was proposed to generate a noise-tolerable floorplan for the average inductive noise. To deal with the infrequent worst case scenarios, their dynamic control was designed for a given floorplan's power supply distribution by taking into account the worse case current swing for particular microarchitectural blocks where coarse-level clock gating is enabled. This work resulted in two technical papers in MICRO-39 and ASP-DAC'07. Dr. Lee was invited as one of the four guest speakers at the Intel Architecture/CAD Symposium held at Intel, Santa Clara, to present their design methodology.

The National Science Foundation recently notified Dr. Lee for funding his NSF CAREER Proposal in the amount of $400,000 for 5 years. The project titled *Introspective Computing: A Multicore Approach to Availability, Reliability and Security* will investigate the techniques based on the emerging multicore processors for defending remote exploits and attacks. The CAREER proposal will also develop new multicore curriculum and better pedagogical tools for computer architecture education via visualization-based simulation tools. Additionally, Dr. Lee and Dr. Schwan (CoC) received Intel's multicore curriculum development funding in the amount of $78,168 for developing multicore course materials and mini-projects using Intel multicore platforms. More recently, Dr. Lee and Dr. Gavrilovska received research funding in the amount of $50,000 from Intel to work on parallelization of medical image reconstruction algorithms based on Computed Tomography (CT) scan and Magnetic Resonance Imaging (MRI) on multicore platforms.

2.2 Teaching

In 2006, Dr. Lee's main teaching responsibility was ECE3055 Computer Architecture and Operating Systems — two sections were assigned in Spring 2006 and one section in Fall 2006. He had taught the same course twice in 2004 and 2005. Similar course materials and projects were used in the offering this year. After the Spring offer, one ECE3055 student Greg Diamos worked with Dr. Lee as an undergraduate researcher during the summer. He was involved in a project that integrated an architecture simulator called Wattch with Java method using Java Native Interface (JNI). With such instrumentation, one can visualize various parts of an architecture simulation on a per-cycle basis. The student successfully integrated several functions such as power consumption of microarchitectural blocks and plotted the power variation on a separate Java window in a dynamic manner.

2.3 Service

For on-campus service, Dr. Lee served as the primary research adviser for 9 Ph.D. students in 2006. He also served as a Ph.D. proposal committee member and a Ph.D. defense committee member for several students in ECE and the College of Computing. Two of his Ph.D. students graduated in 2006. Dr. Weidong Shi joined Motorola Research Labs in Illinois working on digital rights management issues for their next generation mobile phone. Dr. Taeweon Suh joined Intel's Digital Enterprise Group at Oregon. Dr. Lee served on the Student-Faculty Committee and the Undergraduate Committee in 2006. In addition, Dr. Lee was appointed as one of the four members serving the Farmer Chair Search Committee.

For service outside of Georgia Tech, Dr. Lee served as a program committee member for several international conferences and workshops: ICPADS-05, EUC-06, SOCC-06, ISCA-33, CASES-06, ICCD-06, WIOSCA-06, all of them are in the general areas of processor architecture, embedded, and system-on-chip systems. He was also appointed as the Workshop and Tutorial Chair for MICRO-39, and co-organized a workshop WISA-06 in conjunction with HPCA-12. Dr. Lee constantly served as a reviewer for refereed conferences and journal publications including *IEEE Transactions* and *ACM Transactions*. He continues to serve as the Associate Editor of the *International Journal of Embedded Systems*.

3 Five Major Intellectual Products

- Dependable and Revivable Multicore Architecture. Dr. Lee and his students exploited the unique characteristics featured by the emerging multicore processors and designed a remote attack-immune and self-healing system called *Indra*. The focus of this work examines the security monitoring scheme and fast checkpoint and recovery mechanisms. (W. Shi, H.-H. S. Lee, L. Falk, and M. Ghosh. An Integrated Framework for Dependable and Revivable Architecture Using Multicore Processors. In *Proceedings of the 33rd International Symposium on Computer Architecture (ISCA-33)*, pp. 102-113, Boston, MA, June, 2006.) Later, Dr. Lee was invited by Intel Labs at Pittsburgh and Carnegie-Mellon University to present this research.
- InfoShield for Information Protection In Memory. Dr. Lee and his students proposed and published a information protection system called InfoShield for guarding privacy and data confidentiality. With minimal microarchitecture support, it ensures that sensitive data to be used only in the way as defined by application semantics. (W. Shi, J. B. Fryman, G. Gu, H.-H. S. Lee, Y. Zhang, and J. Yang. InfoShield: A Security Architecture for Protecting Information Usage in Memory. In *Proceedings of the 12th International Symposium on High-Performance Computer Architecture (HPCA-12)*, pp.225-234, Austin, TX, February, 2006.) This is the first paper accepted by this premium architecture conference from Georgia Tech since 1997.
- Dynamic Inductive Noise Controller. In this work, Dr. Lee and his student studied the ever-worsening high-frequency inductive noise in power-efficient processors. They proposed to include a dynamic inductive noise evaluation hardware table to adaptively control the levels of clock-gating, making the circuits operation more reliable. (F. Mohamood, M. Healy, S. K. Lim, and H.-H. S. Lee. A Floorplan-Aware Dynamic Inductive Noise Controller for Reliable Processor Design. In *Proceedings of the 39th ACM/IEEE International Symposium on Microarchitecture (MICRO-39)*, pp.3-14, Orlando, Florida, December, 2006.) An AMD chief designer recently read this work and is implementing a similar technique for their next-generation processor.
- High Energy-Efficiency Caches. Teamed up with ARM Research, Dr. Lee and his student studied the energy issues in caches. They proposed the usage of Counting Bloom Filter to keep track of memory footprints and store them in a bitmask as the signature. This signature is then used to make predictions for avoiding unnecessary accesses, thus saving energy. Two papers reported their research outcomes. One used to predict L2 cache misses. (M. Ghosh, E. Ozer, S. Biles, and H.-H. S. Lee. Efficient System-on-Chip energy Management with a Segmented Bloom Filter. In *Proceedings of the 19th International Conference on Architecture of Computing Systems (ARCS-19)*, pp. 283-297, Frankfurt/Main, Germany, March, 2006.) Another one predicts address synonyms in L1 caches to reduce power for synonymous lookup. (D. H. Woo, M. Ghosh, E. Ozer, S. Biles, and H.-H. S. Lee. Reducing Energy of Virtual Cache Synonym Lookup using Bloom Filters. In *Proceedings of the ACM/IEEE International Conference on Compilers Architecture and Synthesis for Embedded Systems (CASES-06)*, pp.179-189, Seoul, Korea, October, 2006.)
- Profile-Guided Microarchitectural Floorplanning. Working with Prof. Lim's group, Dr. Lee investigated a profile-driven methodology for designing both 2D and 3D-integrated microprocessors floorplans. By exposing inter-block communication frequency, the profile-guided floorplan will reduce the growing latency concerns due to un-scalable wire delay. Further, they extended the methodology to take both performance and thermal profile into account to formulate a multi-objective microarchitectural floorplanning algorithm (M. Healy, M. Vittes, M. Ekpanyapong, C. Ballapuram, S. K. Lim, H.-H. S. Lee, and G. H. Loh. Microarchitectural Floorplanning Under Performance and Temperature Tradeoff. In *Proceedings of the Design, Automation and Test in Europe (DATE-06)*, pp.1288-1293, Munich, Germany, March, 2006) and applied it to 2D and 3D integrated circuits. (M. Healy, M. Vittes, M. Ekpanyapong, C. Ballapuram, S. K. Lim, H.-H. S. Lee, and G. H. Loh. Multi-Objective Microarchitectural Floorplanning For 2D and 3D ICs. In *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 26, No. 1, pp.38-52, 2007.)