SESSION 20 – HONOLULU SUITE
Digital Techniques II

Friday, June 18, 3:25 p.m.
Chairpersons: G. Taylor, Intel
K. Kotani, Tohoku University

20.1 — 3:25 p.m.
Design of High-Speed and Area-Efficient Montgomery Modular Multiplier for RSA Algorithm, K. Mukaida, M. Takenaka*, N. Torii*, and S. Masui*, Fujitsu Ltd, Kanagawa, Japan and *Fujitsu Labs Ltd., Kanagawa, Japan

High-speed and area-efficient Montgomery modular multiplier for RSA algorithm has been developed for digital signature and user authentication in high-speed network and smart card systems. The multiplier-accumulator in the modular multiplier has non-identical word length for multiplier and multiplicand. This organization eliminates the bottleneck in the memory access, and enables to use single-port memory for area and power reduction. 5,000 digital signature productions/sec is obtained with a three-stage pipelined architecture in 0.18-mm CMOS technology.

20.2 — 3:50 p.m.
Impact of Body Bias on Alpha- and Neutron-Induced Soft Error Rates of Flip-flops, T. Karnik, J. Tschanz, B. Bloechel, P. Hazucha, P. Armstrong, S. Narendra, A. Keshavarzi, K. Soumyanath, G. Dermer, J. Maiz, S. Borkar and V. De, Intel Laboratories, Hillsboro, OR

Soft error rate measurements for flip-flops on two test chips in 180nm and 130nm logic technologies show that using forward body bias improves alpha SER by 35% and neutron SER by 23%, while applying reverse body bias degrades SER by 9% to 36%. Body bias impact on SER remains virtually unchanged with technology scaling.

20.3 — 4:15 p.m.
50Gb/s 3.3V Logic ICs in InP-HBT Technology, P. van der Wagt, T. Broekaert, S. Yinger, S. Zheng, N. Srivastava, J. Rogers, J. Sanders, R. Thiagarajah, R. Coccioli, E. Arnold and K. Nary, Inphi Corp., Westlake Village, CA

50Gb/s 3.3V InP-HBT logic ICs with 6ps rise time and 1200mVpp output swing include: D-flip-flop, double-edge triggered flip-flop, dividers, a frequency doubler, XOR/OR gates, and a 1:2 fanout buffer. The DFF has 3pspp deterministic and <190fsrms random jitter, >270deg phase margin, and 12mVpp sensitivity at40Gb/s and 1E-12 BER. The ICs dissipate 480-840mW in 1mm2.

20.4 — 4:40 p.m.
Energy-Efficient Low-Voltage Operation of Digital CMOS Circuits Through Charge-Recycling, S. Rajapandian, Z. Xu and K.L. Shepard, Columbia University, New York, NY

This paper describes an energy-efficient means to achieve on-chip dc-dc conversion for digital CMOS circuits. The approach uses balanced voltage islands running at fractions of the off-chip supply voltage. Charge "discarded" by one domain is "recycled" to supply energy for another. When the domains are ideally balanced, all the energy dissipated by electrons in "dropping" to lower potentials is used for active computation. We describe the design and measurement of a prototype system in a 0.18um CMOS process that provides active on-chip voltage regulation and controlled dc-dc conversion with this technique.

20.5 — 5:05 p.m.
Microprocessor Power Optimization Through Multi-Performance Device Insertion, H.L. Yeager, M.J. Patyra, R. Reyes and K.A. Bowman, Intel Corporation, Folsom, CA

A paradigm shift for multi-performance device insertion from optimizing product-level performance to total power is elucidated. The key limitations of a performance-based insertion methodology are reviewed, where an increase in stand by current is sacrificed for an unobservable clock frequency gain. The power optimization, which is based on nodal activity factors and state probabilities, enables 5% to 8% total power reduction on three mature mega-block designs from two separate 90nm generation microprocessors while maintaining constant performance.