

## Publications

B. J. Phillips

December 9, 2010

### Book Chapters

- [1] D. R. Kelly, B. J. Phillips, and S. Al-Sarawi, “Operators for embedded systems: Approximate multiplication and division for arithmetic data value speculation in a RISC processor,” in *Algorithm-Architecture Matching for Signal and Image Processing*, 1st ed., ser. Lecture Notes in Electrical Engineering. Springer, Dec 2010, vol. 73, ch. 4.
- [2] D. Kelly and B. Phillips, “Arithmetic data value speculation,” in *ACSAC 2005*, ser. Lecture Notes in Computer Science, T. Srikanthan, Ed. Springer, 2005, vol. 3740, pp. 353–366.
- [3] B. J. Phillips, N. Burgess, and K. V. Lever, “Regularisation procedures for iterated recursive digital filters,” in *Digital Signal Processing for Communication Systems*, H. R. Taduesz Wysocki and Bahram, Eds. Kluwer Academic Publishers, 1997, pp. 217–224.

### Refereed Journal Articles (Sole Author)

- [4] B. J. Phillips, “Montgomery residue number systems,” *Electronics Letters*, vol. 37, no. 21, pp. 1286–7, Oct. 2001.

### Refereed Journal Articles (Joint Author)

- [5] H. Nikmehr, B. Phillips, and C.-C. Lim, “A novel implementation of radix-4 floating-point division/square-root using comparison multiples,” *Computers & Electrical Engineering*, vol. 36, no. 5, pp. 850–863, 2010. [Online]. Available: <http://dx.doi.org/10.1016/j.compeleceng.2008.04.013>
- [6] Y. Kong and B. Phillips, “Revisiting sum of residues modular multiplication,” *Journal of Electrical and Computer Engineering*, vol. 2010, p. 9 pages, May 2010, article ID 657076. [Online]. Available: <http://www.hindawi.com/journals/jece/2010/657076.html>
- [7] B. J. Phillips, Y. Kong, and Z. Lim, “Highly parallel modular multiplication in the residue number system using sum of residues reduction,” *Applicable Algebra in Engineering, Communication and Computing*, vol. 21, no. 3, pp. 249–255, May 2010, published online 7 March 2010.
- [8] Y. Kong and B. Phillips, “Fast scaling in the residue number system,” *IEEE Transactions on VLSI Systems*, vol. 17, no. 3, pp. 443–447, Mar. 2009.
- [9] H. Nikmehr, B. Phillips, and C.-C. Lim, “Fast decimal floating-point division,” *IEEE Transactions on VLSI Systems*, vol. 14, no. 9, pp. 951–961, Sept. 2006.
- [10] H. Nikmehr, B. Phillips, and C.-C. Lim, “A Fast Radix-4 Floating-Point Divider with Quotient Digit Selection by Comparison Multiples,” *The Computer Journal*, p. bxl048, 2006. [Online]. Available: <http://comjnl.oxfordjournals.org/cgi/content/abstract/bxl048v1>
- [11] B. Phillips and N. Burgess, “Minimal weight digit set conversions,” *IEEE Transactions on Computers*, vol. 53, no. 6, pp. 666–677, June 2004.
- [12] B. J. Phillips and N. Burgess, “Signed sliding window algorithms for modulo multiplication,” *Electronics Letters*, vol. 36, no. 23, pp. 1925–7, Nov. 2000.

## Peer Reviewed Conference Proceedings

- [13] D. R. Kelly, B. J. Phillips, and S. Al-Sarawi, "Approximate signed binary integer multipliers for arithmetic data value speculation," Conference on Design and Architectures for Signal and Image Processing (DASIP), Sept. 2009, in press, accepted 24 Sept. 2009. [Online]. Available: <http://www.ecsi-association.org/ecsi/dasip/dasip09/mainpage.asp?fn=proceedings>
- [14] D. R. Kelly, B. J. Phillips, and S. Al-Sarawi, "Approximate unsigned binary integer dividers for arithmetic data value speculation," Conference on Design and Architectures for Signal and Image Processing (DASIP), Sept. 2009, in press, accepted 24 Sept. 2009. [Online]. Available: <http://www.ecsi-association.org/ecsi/dasip/dasip09/mainpage.asp?fn=proceedings>
- [15] D. R. Kelly, B. J. Phillips, and S. Al-Sarawi, "Increasing throughput of a RISC architecture using arithmetic data value speculation," Forty-Third Asilomar Conference on Signals, Systems, and Computers, Nov. 2009, in press, accepted 4 Nov. 2009.
- [16] Z. Lim, B. J. Phillips, and M. Liebelt, "Elliptic curve digital signature algorithm over  $GF(p)$  on a residue number system enabled microprocessor," IEEE Region 10 Conference, TENCON 2009, Nov. 2009, pp. 1–6.
- [17] D. Blaauw, J. Kitchener, and B. Phillips, "Optimizing addition for sub-threshold logic," Forty-Second Asilomar Conference on Signals, Systems, and Computers, Oct. 2008.
- [18] R. Moric, B. J. Phillips, and M. J. Liebelt, "Defect tolerant prefix adder design," Smart Structures, Devices, and Systems IV, ser. Proc. SPIE, S. F. Al-Sarawi, Ed., vol. 7268, Dec. 2008, pp. 72 680F–1–9.
- [19] N. Pinckney, T. Barr, M. Dayringer, M. McKnett, N. Jiang, C. Nygaard, D. Money Harris, J. Stanley, and B. Phillips, "A MIPS R2000 implementation," in *Design Automation Conference, 2008. DAC 2008. 45th ACM/IEEE*, San Francisco, California, USA, June 2008, pp. 102–107.
- [20] B. Phillips, C. Schmidt, and D. Kelly, "Recovering data from USB Flash memory sticks that have been damaged or electronically erased," Electronic proceedings indexed by ACM e-Forensics 2008: the First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia, Adelaide Australia, Jan. 2008, pp. 1–6.
- [21] Z. Lim and B. J. Phillips, "An RNS-enhanced microprocessor implementation of public key cryptography," 41st Asilomar Conference on Signals, Systems and Computers. Pacific Grove, CA, USA: IEEE, Piscataway, NJ, USA, Nov. 2007, pp. 1430–1434.
- [22] Y. Kong and B. Phillips, "Simulations of modular multipliers on FPGAs," Proceedings of the IASTED Asian Conference on Modelling and Simulation, Beijing, China, Oct. 2007, pp. 1128–131.
- [23] Y. Kong and B. J. Phillips, "Comparison of Montgomery and Barrett modular multipliers on FPGAs," 40th Asilomar Conference on Signals, Systems and Computers. Pacific Grove, CA, USA: IEEE, Piscataway, NJ, USA, Oct. 2006, pp. 1687–1691.
- [24] T. A. Coleman, J. A. Kitchener, D. L. Pudney, K. D. Wauchope, and B. J. Phillips, "An RNS public key cryptography accelerator," Smart Structures, Devices, and Systems III, ser. Proc. SPIE, S. F. Al-Sarawi, Ed., vol. 6414, Dec. 2006, p. 641422.
- [25] D. R. Kelly, B. J. Phillips, and S. Al-Sarawi, "An open source synthesisable model in VHDL of a 64bit MIPS-based processor," Smart Structures, Devices, and Systems III, ser. Proc. SPIE, S. F. Al-Sarawi, Ed., vol. 6414, Dec. 2006, p. 641411.
- [26] B. J. Phillips, D. R. Kelly, and B. W. Ng, "Estimating adders for a low density parity check decoder," Advanced Signal Processing Algorithms, Architectures, and Implementations XVI, ser. Proc. SPIE, F. T. Luk, Ed., vol. 6313, no. 1. San Diego, Ca, USA: SPIE, Sept. 2006, pp. 631 302–1–9. [Online]. Available: <http://link.aip.org/link/?PSI/6313/631302/1>
- [27] B. Phillips, "Merged modular/non-modular multiply-add unit," in *Smart Structures, Devices, and Systems II*, ser. Proc. SPIE, S. F. Al-Sarawi, Ed., vol. 5649, Feb. 2005, pp. 118–125.
- [28] K. Rajagopalan, B. Phillips, and D. Abbott, "(OFRL) on-the-fly reconfigurable logic," in *Smart Structures, Devices, and Systems II*, ser. Proc. SPIE, S. F. Al-Sarawi, Ed., vol. 5649, Feb. 2005, pp. 101–109.

- [29] H. Nikmehr, C. C. Lim, and B. Phillips, "A decimal carry-free adder," in *Smart Structures, Devices, and Systems II*, ser. Proc. SPIE, S. F. Al-Sarawi, Ed., vol. 5649, Feb. 2005, pp. 786–797.
- [30] Y. Kong and B. Phillips, "Residue number system scaling schemes," in *Smart Structures, Devices, and Systems II*, ser. Proc. SPIE, S. F. Al-Sarawi, Ed., vol. 5649, Feb. 2005, pp. 525–536.
- [31] D. K. P. Tan, A. Haddad, and B. Phillips, "An event driven real time operating system," The 6th International Conference on Optimization: Techniques and Applications, Ballarat, Australia, 2004.
- [32] B. Phillips, "Scaling and reduction in the residue number system with pairs of conjugate moduli," 37th Asilomar Conference on Signals, Systems and Computers. Pacific Grove, CA, USA: IEEE, Piscataway, NJ, USA, Nov. 2003, pp. 2247–2251.
- [33] B. Phillips, "Modular multiplication in the Montgomery residue number system," 35th Asilomar Conference on Signals, Systems and Computers, M.-B. Mathews, Ed., vol. 2. Pacific Grove, CA, USA: IEEE, Piscataway, NJ, USA, Nov. 2001, pp. 1637–40.
- [34] B. Phillips, "Optimised squaring of long integers using precomputed partial products," 15th IEEE Symposium on Computer Arithmetic, N. Burgess and L. Ciminiera, Eds. Vail, CO, USA: IEEE Comput. Soc, Los Alamitos, CA, USA, June 2001, pp. 73–79.
- [35] B. Phillips and N. Burgess, "Optimized squaring with sliding windows," 34th Asilomar Conference on Signals, Systems and Computers, M.-B. Mathews, Ed. Pacific Grove, CA, USA: IEEE, Piscataway, NJ, USA, Oct. 2000, pp. 130–3.
- [36] B. J. Phillips and N. Burgess, "Implementing 1024-bit RSA exponentiation on a 32-bit processor core," Proc. 2000 International Conference on Application Specific Systems, Architectures, and Processors, E. E. Swartzlander, Jr, G. A. Jullien, and M. J. Schulte, Eds. Boston, MA, USA: IEEE Comput. Soc, Los Alamitos, CA, USA, July 2000, pp. 127–137.
- [37] B. J. Phillips, N. Burgess, and K. V. Lever, "Regularisation procedures for iterated recursive digital filters," 4th Conference of Digital Signal Processing for Communication Systems, Perth, Australia, Sept. 1996.
- [38] B. J. Phillips and N. Burgess, "A self-timed approach to radix 2 SRT quotient digit selection for GaAs VLSI technology," 13th Australian Microelectronics Conference. Adelaide, SA, Australia: IREE Soc, Milsons Point, NSW, Australia, July 1995, pp. 80–85.

## Research Reports

- [39] Z. Lim and B. Phillips, "An RNS-enabled architecture on the Tensilica Xtensa LX processor," The University of Adelaide, CHiPTec Tech. Rep. CHIPTEC-07-01, April 2006.
- [40] E. Watts and B. Phillips, "Extending the 2005 cryptochip," The University of Adelaide, CHiPTec Tech. Rep. CHIPTEC-05-07, November 2005.
- [41] B. J. Phillips and J. P. Rosser, "Radix 2 quotient digit selection function for a public key crypto chip," The University of Adelaide, CHiPTec Tech. Rep. CHIPTEC-05-06, July 2005.
- [42] Y. Kong and B. Phillips, "A classical modular multiplier for RNS channel operations," The University of Adelaide, CHiPTec Tech. Rep. CHIPTEC-05-02, November 2005.
- [43] Y. Kong and B. Phillips, "A Montgomery modular multiplier for RNS channel operations," The University of Adelaide, CHiPTec Tech. Rep. CHIPTEC-05-02, November 2005.
- [44] B. Phillips, "Data remanence in semiconductor memories," The University of Adelaide, CHiPTec contract research report, April 2006.