GfXpress™
Near Optimal Automatic Chip Design
Licence Opportunity

OXFORD BROOKES UNIVERSITY

Electronic Design Automation (EDA) research at Oxford Brookes University, led by Dr. Abusaleh Jabir, has culminated in a novel synthesis technique, called GfXpress™, for the automatic synthesis and optimization of multivariate, multiple output polynomials over finite fields. Industrial partners are sought for further development and to bring this innovative technology to market.

This technique has many practical applications, but is particularly applicable for the design of cryptographic hardware, e.g. the elliptic curve cryptosystems, parts of the AES system, error control and correction schemes (e.g. the BCH and Reed-Solomon coders), digital signal processors, etc.

As the market continues to demand smaller more mobile systems, which run on batteries, the need to use less power becomes a key driver and competitive imperative. Laboratory experiments have shown that, GfXpress™ can demonstrate an order of magnitude improvement, with respect to power, speed and area, over current state of the art systems. In this industry, an improvement of 20% is regarded as significant; the GfXpress™ research prototype has demonstrated up to 68 times improvement! This can provide adopters with a significant competitive advantage.

- GfXpress™ produces a near optimal circuit layout automatically, unlike many current systems, which include a manual stage.
- Laboratory prototype demonstrates orders of magnitude improvements in area, power and speed compared to current solutions.
- The final circuits are independent of initial specs, allowing the hardware designs to be easily verifiable with enhanced testability. Most existing tools cannot produce easily verifiable hardware.

Current techniques all involve a hand-coding stage. With GfXpress™ the process is completed automatically. This can provide designers and their clients with huge cost benefits.

With GfXpress™ verifiable hardware is produced. Unlike all other techniques GfXpress™ produce optimal or near optimal designs, which are “canonic”, i.e. the exact same and structurally identical result (circuit) for systems with the same functionality, which is independent of the initial starting point. This provides the additional extremely valuable benefit of producing “verifiable” hardware, which is not possible with most existing systems. This will give designers and their clients cost benefits, performance, and design confidence.

GfXpress™ is capable of producing 100% testable circuits against manufacturing faults. These faults can result from imperfections in the silicon wafers, inadvertent solder splashes, etc. and cause the circuits to malfunction at the end user stages, unless they are tested once they have gone through the production lines. The number of test vectors required, which is the measure of the testing time, for testing the synthesized circuits against these faults is very small. This is an extremely important feature of the tool, since all the industrial designs must be tested against these manufacturing faults. Making circuits testable against these faults is known to be a very hard problem, which the proposed technique incorporates by default very efficiently. This has been verified with the help of the premier industrial tools.

/PTO

The techniques in GfXpress™ are protected by an international patent application. Searches show both novelty and inventiveness.

The techniques and approach has been validated by industry experts and published in several peer reviewed premier journals and conferences. These include:

- IEEE Transactions on CAD, Apr 2008.
- IEEE Transactions on Computers, Aug 2007.
- Proc. IEEE/ACM International Conf. on Computer Aided Design (ICCAD), Silicon Valley, USA, Nov. 2006

Dr. Abusaleh Jabir is an IEE Hartree Premium Award winner. He delivered the Distinguished Keynote Speech at the International Conference on Computing and Information Technology, (2005). For a full list of publications please contact us.

For Further Information, or to discuss possible collaborations please contact:

Dr. Eugene Sweeney
Research & Business Development Office
Oxford Brookes University, Gipsy Lane Campus
Oxford OX3 0BP, UK
Email: esweeney@brookes.ac.uk

or

Dr. Abusaleh Jabir,
Department of Computer Science and Electronics
Oxford Brookes University, Wheatley Campus
Oxford OX33 1HX, UK
Email: ajabir@brookes.ac.uk

Selected Publications in Related Areas

1. M. Ciesielski, A. Jabir, and D. Pradhan, Practical design verification. In I. Haris, editor, "Graph Based Representations for Verification of Arithmetic and Data Path Designs", Cambridge University Press, 2009.
2. H. Rahaman, J. Mathew, A.M. Jabir, D.K Pradhan, "C-testable S-box Implementation for Secure Advanced Encryption Standard", IEEE IOLTS, Sesimbra-Lisbon, Portugal, June, 2009.
3. J.Mathew, A.M. Jabir, H. Rahaman D.K Pradhan, "On the Synthesis of Bit Parallel Galois Field Multipliers with On-line SEC and DED", Int. Journal of Electronics (accepted), June, 2009.
4. A. Jabir, J. Mathew, H. Rahaman, and D. Pradhan, "A Galois Field Based Logic Synthesis Approach with Testability", IET Proc. Part-E: Comp. and Digital Tech. (accepted), 2009.
5. J. Mathew, A. Jabir, H. Rahaman, and D. Pradhan, "Single Error Correctable Bit Parallel Multipliers over GF(2^m)", IET Proc. Part-E: Comp. and Digital Tech., Vol. 3, Issue 3, pp. 281–288, 2009.
6. H. Rahaman, J. Mathew, A. Jabir, and D. Pradhan, "Derivation of Reduced Test Vectors for Bit Parallel Multipliers over GF(2^m)", IEEE Trans. Comp., Vol. 57, No. 9, pp. 1289–1294, Sept, 2008.
7. A. Jabir, D. Pradhan, and J. Mathew, "GfXpress: A Technique for Synthesis and Optimization of GF(2^m) Polynomials", IEEE Trans. CAD, Vol. 27, No. 4, pp. 698–711, April, 2008.
8. J. Mathew, A. Jabir, and D. Pradhan, "Design Techniques for Bit-Parallel Galois Field Multipliers with On-Line Single Error Correction and Double Error Detection", IEEE IOLTS 2008, July 7–9, Rhodes, Greece, 2008.
9. J. Mathew, A. Jabir, M. Hosseinabady, J. Singh, and D. Pradhan, "Fault Tolerant Bit Parallel Finite Field Multipliers Using LDPC Codes", IEEE ISCAS 2008, May 18–11, Seattle, USA, 2008.
10. J. Mathew, H. Rahaman, A. Jabir, A. Singh, and D. Pradhan, "A Galois Field Based Logic Synthesis Approach with Testability", Proc. IEEE/ACM Int. Conf. on VLSI Design (VLSI'08), pp. 629–634, Jan 4–8, 2008.
11. J. Mathew, A. Jabir, H. Rahaman, C. Argyrides, and D. Pradhan, "Single Error Correcting Multipliers Over GF(2^m)", Proc. IEEE/ACM Int. Conf. on VLSI Design (VLSI'08), pp. 33–38, Jan 4–8, 2008.
12. H. Rahaman, J. Mathew, A. Jabir, and D. Pradhan, "C-Testable Bit-ParallelMultipliers over GF(2^m)", ACM Trans. Design Automat. Elec. Sys. (TOADES), Vol. 13, Issue 1, No. 5, Jan, 2008.
13. J.Mathew, H. Rahaman, A. Jabir, and D. Pradhan, "Area Efficient Pseudo-parallelGalois FieldMultipliers", Proc. IEEE NORCHIP 2007, Oct 8, 2007.
14. A. Jabir, and D. Pradhan, "A Graph-Based Unified Technique for Computing and Representing Coefficients Over Finite Fields." IEEE Trans. Comp., Vol. 56, No. 8, pp. 1119–1132, Aug, 2007.
15. A. Jabir, D. Pradhan, A. Singh, and T.L. Rajaprabhu, "A Technique for RepresentingMultiple-OutputBinary Functions with Applications to Verification and Simulation", IEEE Trans. Comp., Vol. 56, No. 8, pp. 1133–1145, Aug, 2007.
16. A. Jabir, D. Pradhan, and J.Mathew, "An Efficient Technique for Synthesis and Optimization of Polynomials in GF(2^m)." Proc. Int. Conf. Comp. Aided Design (ICCAD), Silicon Valley, USA, pp. 151–157, Nov. 2006.
17. H. Rahaman, J. Mathew, A. Jabir, and D. Pradhan, "Universal Test Set for Detecting Faults in Bit Parallel Multipliers in GF(2^m)", Proc. High Level Des. Val. Test Conf. (HLDVT'06), San Jose, California, Nov. 2006.
18. J. Mathew, A. Jabir, A. Singh, and D. Pradhan, "Galois Decomposition of Boolean Functions: An Efficient Synthesis Approach with Testability", Proc. International Design and Test Workshop (IDT'2006), Dubai, UAE, Nov. 19–20, 2006.
19. A. Jabir, "Core Based Systems Design: The Present and the future"—A distinguished keynote paper presented to the ICCIT'05, in December 2005, Proc. International Conf. Comp. and Inf. Tech. (ICCIT'05) pp. 1256-1262, ISBN: 984 32 2873-1.
20. T.L. Rajaprabhu, A. Singh, A. Jabir, and D. Pradhan."GASIM: A Fast Galois Field Based Simulator for Functional Model", Proc. IEEE High Level Des. Test. and Validation Conf. (HLDVT'05), pp. 135- 142, ISBN: 0-7803-9571 9,December 2005.

21. A. Jabir, and D. Pradhan, "An Efficient Graph Based Representation of Circuits and Calculation of Their Coefficients in Finite Field", IWLS'05, Lake Arrowhead, California, USA, June, 2005.
22. D. Pradhan, A. Jabir, T.L. Rajaprabhu, and A. Singh, "Galois Switching Theory: A Uniform Framework For Multi-Level Verification", IWLS'05, Lake Arrowhead, California, USA, June, 2005.
23. A. Jabir and D. Pradhan, "MODD: A New Decision Diagramand Representation forMultiple Output Binary Functions," Design, Automation, and Test in Europe (DATE'04), Paris, France, pp. 1388–1389, Feb, 2004.
24. A. Singh, T.L. Rajaprabhu, A. Jabir, and D. Pradhan, "MODD For CF: A Compact Representation for Multiple-Output Functions," Int. Conf. High Level Des. Val. Test (HLDVT'04), Sonoma, California, USA, 2004.
25. A. Singh, A. Jabir, and D. Pradhan, "Galois Switching Theory: A Unified Framework for Multi-Level Verification," IEE-ACMSIGDA SoCDesign, Test and Technology Seminar, Leicester, UK, September, 2004.
26. A. Jabir, and D. Pradhan, "Designing Multiple-Valued Networks in a Finite Field," Proc. Int. Conf. Comp. Inf. Tech. (ICCIT'03), December, 2003. ISBN: 984-584-005-1.
27. A. Jabir, and D. Pradhan, "A Theory of Finite Field Decision Diagrams," Department of Computer Science, University of Bristol, Nov, 2003.
28. A. Jabir, and J. Saul, "MinimizationAlgorithmfor Three-LevelMixed AND-OR-EXOR/AND-OR-EXNOR Representation of Boolean Functions," IEE Proc. Part-E (Comp. and Dig. Techniques), Vol. 149, No. 3, pp. 82–96,May 2002. [Winner of the IEE Hartree Premium Award for outstanding contributions to computing and digital techniques, 2003/2004.]
29. A. Jabir, and J. Saul, "Heuristic AND-OR-EXOR three-level minimization algorithm for multiple-output incompletely-specified Boolean functions," IEE Proceedings Part-E (Comp. and Dig. Techniques), Vol. 147, No. 6, pp. 451–461, Nov. 2001.
30. A. Jabir, and J. Saul, "A Heuristic Decomposition Algorithm for AND-OR-EXOR Three-Level Minimization of Boolean Functions," Proc. 4th Int. Workshop Applicat. Reed-Muller Expansion in Circuit Design, pp 55-72, Victoria, Canada, Aug. 1999.