

Electronic Design Automation & Attack Tolerant Crypto-hardware

Seeking industrial partners for knowledge transfer and collaborative research

Electronic Design Automation (EDA) research at Oxford Brookes University, led by Dr. Abusaleh Jabir, has culminated in the development of novel ideas for attack tolerant and testable designs of the various components of crypto hardware. We are now seeking industrial partners for further development and/or collaborative research to bring these innovative ideas to market.

Automatic synthesis of arithmetic circuits (e.g. multivariate multiple output polynomials) defined over groups, fields, and rings, especially suitable for cryptographic applications, error control coding and reliability, digital signal processing, and high performance processor designs. The emphasis is on:

- Area optimization
- Power optimization
- Speed optimization
- Enhanced testability
- Preserve easily verifiable properties for fast hardware verification.

A novel synthesis technique, called GfXpress™, for automatic synthesis and optimization of multivariate, multiple output polynomials over finite fields has been developed and a patent application filed. These polynomials have many practical applications, but are 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. Industrial partners are sought to help bring this to market.

Design for testability (DFT) with highly optimized hardware overheads, testing time, and power consumptions.

- This is especially targeted towards the various components of cryptography hardware, such as the arithmetic components with C-, M-, and built-in testability.
- Conventional DFT techniques, e.g. those based on standard scan chains, can introduce side channels in cryptography hardware. This can be exploited by an attacker to retrieve the secret signatures and keys.

Our interests lies in alternate testing techniques, which eliminate these side channels while maintaining very high fault coverage, with very low testing times, hardware overheads, and power consumptions.

Fault tolerant and Power Aware reliable hardware synthesis

- For mitigating transient and soft faults.
- Emphasis is on, among other things, cryptography hardware.
- Recent research suggests that by careful injection of random events and observing the outputs, it is possible for an attacker to retrieve the secret keys and signature in cryptography hardware. Radiation induced transient faults can be a good tool for such attacks.
- Power aware designs, e.g. to mitigate power related side channels.

Our interest lies in the design of fault tolerant and reliable hardware to mitigate these types of faults and, e.g. power related side channel attacks.

Industrially relevant results include:

- A novel synthesis technique, called GfXpress™, for automatic synthesis and optimization of multivariate, multiple output polynomials over finite fields has been developed and a patent application filed. These polynomials have critical applications in cryptography, 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.
- Highly efficient techniques for computing and representing the coefficients of the multivariate polynomials over finite fields.
- Novel techniques for representing digital systems, both at the gate/switching as well as the word/architectural levels for efficient synthesis and verification.
- Efficient testing and DFT techniques for hardware implementation of the polynomials over finite fields.
- Efficient fault tolerant design techniques for multipliers over finite fields.
- Novel design techniques for high-speed PLDs.

Publications include book chapters, premiere journal and conference papers, IEE Hartree Premium Award for the best paper of the year with the IEE/IET. 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-Parallel Multipliers 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-parallel Galois Field Multipliers", 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 Representing Multiple-Output Binary 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 Diagram and Representation for Multiple 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 SoC Design, 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. (ICIT'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, "Minimization Algorithm for Three-Level Mixed 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.