

Breaking the IDEA Cipher Using the Star Bridge HC-36 Reconfigurable Computer

Allen Michalski¹, Kris Gaj¹, Tarek El-Ghazawi²

¹ ECE Department, George Mason University

² ECE Department, The George Washington University

Abstract. The combination of traditional microprocessors and Field Programmable Gate Arrays (FPGAs) is developing as a platform for intensive computational computing. These “reconfigurable computers” combine the best aspects of traditional microprocessor front-end processing capabilities with the reconfigurability of FPGAs for computation-intensive problems. Star Bridge Systems’ HC-36 HyperComputer is a reconfigurable computer that combines a PC workstation front-end with a Xilinx Virtex II FPGA array backend to create a system capable of supercomputer performance. Star Bridge’s VIVA development environment provides a new paradigm for system design and synthesis compared to traditional HDL entry and synthesis techniques. In this paper, we demonstrate the implementation of IDEA cipher cryptanalysis using Star Bridge’s VIVA development environment and the HC-36m HyperComputer. This paper discusses the Star Bridge hardware architecture and development tools in detail. FPGA timing and utilization results for the HC-36 implementation are presented and compared to traditional FPGA tool results and a PC implementation using public domain source for IDEA. A summary including Star Bridge’s state of development is also presented.

Introduction

The combination of traditional microprocessors and Field Programmable Gate Arrays (FPGAs) is developing as a future platform for intensive computational computing, combining the best aspects of traditional microprocessor front-end development with the reconfigurability of FPGAs for computation-intensive problems. Several workstation-based FPGA systems are available today for commercial applications. These reconfigurable computing platforms have demonstrated significant speedups compared to standalone PC workstations for computationally intensive problems. Star Bridge is a company on the forefront of reconfigurable computing architectures. Its HyperComputer concept combines a PC workstation front-end with a highly-interconnected Xilinx Virtex II FPGA array to create a platform capable of supercomputing speeds. In addition, its VIVA development environment creates a new paradigm for FPGA design entry by combining graphical drag-and-drop design entry, with methodologies based around design recursion, “data-rate polymorphism”, and design partitioning between PC and FPGA elements. Designers using VIVA can create design at a higher level of abstraction than using traditional Hardware Description Language (HDL) design methods, which can simplify debugging and can decrease design time-to-market. VIVA’s recursive synthesis, along with “data-rate” throughput specifications, can create highly-optimized area-efficient designs [1].

Cryptographic applications are a clear candidate for reconfigurable computing, due to their computational intensity and long operand lengths. The International Data Encryption Algorithm (IDEA) is a symmetric block cipher that uses a 128-bit key to encrypt data blocks of 64 bits. IDEA consists of eight and one-half rounds, each round consisting of multiple combinations of modulo addition, XOR operation, and multiplication modulo $2^{16} + 1$. The design of this block cipher can be exploited to create a highly-pipelined, high-throughput hardware design with significant speedups versus an equivalent PC software implementation. This is essential when performing IDEA cryptanalysis based on exhaustive key search, where the 128-bit key length is not easily handled within traditional microprocessor operand lengths.

This paper explores an implementation of IDEA cipher cryptanalysis within the HC-36 from Star Bridge Systems. The hardware architecture of the HC-36 is discussed, along with VIVA’s hardware abstraction layer that is used to represent the hardware. The implementation of this design within VIVA is shown, and VIVA’s development methodologies are discussed and compared to traditional HDL techniques. FPGA timing and utilization results are presented and compared to traditional tools and a PC implementation using a public-domain source. A summary including the state of development is also presented.

Conclusion

The HC-36 provides significant computing capability that can offer significant throughput advantages compared to traditional microprocessor application design. Design flexibility is achieved by allowing allocation of different design elements to PC or FPGA resources, depending on computational needs. However, the FPGAs interconnections within the HC-36 can potentially limit inter-FPGA communication if designs need to be allocated to more than one FPGA.

Star Bridge's VIVA environment provides a new paradigm for FPGA design entry and synthesis. VIVA provides a new development paradigm that has the potential to provide an easier method of design entry, faster debugging, and can target several different architectures in addition to its own. An IDEA cryptanalysis is implemented and compared to traditional tools and a PC implementation. FPGA area and timing requirements are larger when compared to traditional FPGA tools.

This paper will show that VIVA's synthesis technology is in an early state, and that short-term development is planned to reduce compile times and improve algorithmic efficiency. In addition, further library abstractions are needed to ease designer implementation difficulties.

References

1. Gilson, K., DePalma, G., "New Methodology for FPGA-Based Designs Offers Significant Benefits over HDL-Based Methods", Jan. 2002, available at <http://www.starbridgesystems.com>
2. Singleterry, R., Sobieszczanski-Sobieski, J. Brown, S., "Field-Programmable Gate Array Computer in Structural Analysis: An Initial Exploration", available at <http://www.starbridgesystems.com>
3. Dandawate, N., Storaasli, O., "Investigation of the Programming Capabilities of the HAL-15 Hypercomputer", Jul. 2002, available at <http://acmb.larc.nasa.gov>
4. Parnell, K., Mehta, N., "Programmable Logic Design Quick Start Handbook", available at www.xilinx.com
5. Star Bridge Systems Web Page, <http://www.starbridgesystems.com>
6. Lai, X., Massey, J., "A Proposal for a New Block Encryption Standard", Proceedings, EUROCRYPT '90, 1990.
7. Stallings, W., "Cryptography and Network Security: Principles and Practice", 2nd Edition, pgs. 102-109, 128, 1999.
8. Parhami, B., "Computer Arithmetic Algorithms and Hardware Designs", pgs 191-192, 2000.
9. VIVA Online Help, Version 2.1
10. 'Reconfigurable, Inherently Parallel "Hypercomputing" ', PowerPoint presentation, 2002, available from Star Bridge Systems.
11. Michalski, A., Gaj, K. El-Ghazawi, T. "An Implementation Comparison of an IDEA Encryption Cryptosystem on Two General-Purpose Reconfigurable Computers", Mar. 2003, submitted to the 13th International Conference on Field Programmable Logic and Applications.