Journal of Universal Computer Science, vol. 13, no. 3 (2007), 345-348
submitted: 21/3/07, accepted: 25/3/07, appeared: 28/3/07 © J.UCS

New Advances in Reconfigurable Computing and its Applications

J.UCS Special Issue

Miguel A. Vega-Rodríguez, Juan A. Gómez-Pulido, Juan M. Sánchez-Pérez
Dept. Technologies of Computers and Communications, Univ. Extremadura
Escuela Politécnica, Campus Universitario s/n. 10071 Cáceres, Spain
{mavega, jangomez, sanperez}@unex.es)

Abstract: In this work we present a survey of different papers about reconfigurable computing and its applications. These papers treat very different reconfigurable-computing applications: cryptography, computer vision, SOPC, microprocessor architecture, self-timed circuits, sensor systems, detection of ultrasonic emissions, FPGA compilation aspects (like data-dependent loops), and motion estimation. As conclusion, we can say that reconfigurable computing is becoming an increasingly important computing paradigm, being a good alternative for many real applications.

Keywords: Reconfigurable Computing, FPGA, Applications

1 Introduction

As the Reconfigurable Computing is becoming an increasingly important computing paradigm, more and more FPGA-based applications are appearing. FPGA devices are making it possible for thousands of computer engineers to have access to digital design technology in an easier way, obtaining a better performance with a similar flexibility to software. In addition, ASIC engineers are now “reconfiguring” themselves as FPGA engineers for economic reasons and adding to the growing legions of FPGA designers.

In conclusion, reconfiguration of circuitry at runtime to suit the application at hand has created a promising paradigm of computing that blurs traditional frontiers between software and hardware. At present, reconfigurable computing is a good alternative for many real applications in image and signal processing, multimedia, robotics, telecommunications, cryptography, networking and computation in general.

This Special Issue brings together high-quality state-of-the-art contributions about reconfigurable computing and its applications. Concretely, the special issue contains 7 papers that represent the diverse applications and designs being addressed today by the reconfigurable-computing research community. With authors from around the world, these articles bring us an international sampling of significant work.

2 Overview of the papers

The title of the first paper is “The Use of Runtime Reconfiguration on FPGA Circuits to Increase the Performance of the AES Algorithm Implementation”, by O. Perez, Y. Berviller, C. Tanougast, and S. Weber. This paper proposes a solution for the implementation of the AES algorithm in a pipelined and dynamically reconfigurable architecture. Using a Virtex-II FPGA the authors obtain a very good compromise between high speed and low area. In fact, the proposed architecture employs only 11619 slices and reaches a maximum throughput of 44 Gbps. The importance of this paper is clear, because the data security is a significant topic, and from 2002, the AES (Advanced Encryption Standard) cryptographic algorithm, also known as Rijndael, is the block cipher adopted as encryption standard by the U.S. government. For this reason, it is expected to be used worldwide and analysed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). In fact, at present, AES is one of the most popular algorithms used in symmetric key cryptography, being used in wireless networks (WPA2 standard, Wi-Fi Protected Access 2) and many other applications.

The second paper, “Real-Time Architecture for Robust Motion Estimation under Varying Illumination Conditions” by J. Díaz, E. Ros, R. Rodríguez-Gómez, and B. del Pino, proposes a reconfigurable system that implements the motion estimation from image sequences under changing illumination conditions. Motion estimation is an important research field which can be used for robotics applications, compression techniques, tracking systems, estimation of 3-D information from motion, etc. The system proposed in this paper is based on a custom technique that combines a gradient-based optical flow method with a non-parametric image transformation based on the Rank transform. The system has been tested in a real-time platform using a Virtex-II FPGA. A large pipeline of more than 100 stages and multiple scalar units allows them to achieve an outstanding computing performance of 163 fps at VGA resolution (640x480 pixels).

The paper “Design and Implementation of the AMCC Self-Timed Microprocessor in FPGAs” authored by S. Ortega-Cisneros, J.J. Raygoza-Panduro, and G. Alberto de la Mora presents a microprocessor architecture based on Self-Timed circuits built by using FPGA devices. It describes the different processor elements and discusses the advantages achieved by using the AMCC (Asynchronous Microprocessor of Centralized Control) communications scheme. Microprocessor resources utilization is presented for different configurations and details about fan-outs, nets and delays are also presented. The proposed architecture includes inherently the stoppable clock feature, i.e., the circuit is stopped if it is not required (minimal dynamic consumption). In conclusion, the final processor is able to compute up to 9.6 MIPS (using Self-Timed circuits) which is relevant for low power systems.

The sensor systems are addressed in the fourth paper, “Hardware Implementation of an Efficient Correlator for Interleaved Complementary Sets of Sequences” by M.C. Pérez, J. Ureña, A. Hernández, C. de Marziani, A. Jiménez, and W.P. Marnane. This paper presents a generic hardware implementation of an efficient correlator for macro-sequences generated from complementary sets of sequences. The design has been developed as a configurable module, able to be adapted to the requirements (number of sequences of the complementary set, their length, the sampling factor, the number of periods of the symbol used in the modulation, and the data width) from different sensor systems. The performance of the correlator has been tested on a Spartan-3 FPGA. Furthermore, it has been included on an ultrasonic sensory system to verify the detection of ultrasonic emissions in real-time.

The fifth paper ("A Dynamically and Partially Reconfigurable Implementation of the IDEA Algorithm Using FPGAs and Handel-C" by J.M. Granado, M.A. Vega, J.M. Sánchez, and J.A. Gómez) examines the application of FPGAs to cryptography. Nowadays, many secure electronic and Internet transactions require cryptosystems to establish and distribute shared secret information. For security reasons, key sizes are in the region of hundred's of bits, and this makes cryptographic procedures slow in software. The authors show that FPGAs are well suited for this application due to their reconfigurability and versatility, as well as, because they can perform the computationally intensive operations far quicker. In particular, the authors focus on the use of the dynamic and partial reconfiguration in a Virtex-II FPGA for the implementation of the IDEA cryptographic algorithm, one of the most popular cryptographic algorithms due to its use in Pretty Good Privacy (PGP) v2.0 and OpenPGP.

The sixth paper "On Pipelining Sequences of Data-Dependent Loops" is authored by R.M.M. Rodrigues, and J.M.P. Cardoso. Sequences of data-dependent tasks, each traversing large data sets, exist in many applications (such as video, image and signal processing applications), and they usually perform computations (with loop intensive behaviour) and produce new data to be consumed by the subsequent tasks. With the technique proposed in this paper, the subsequent loops can start execution before the completion of the previous ones thanks to the use of a hardware scheme with decoupled and concurrent data-path and control units that start execution at the same time. In conclusion, this technique is able to both improve performance (with a performance close to the theoretical limit) and to reduce the memory requirements related to the data communication between sequences of loops. The authors also show how this technique can be applied in the context of a compiler of imperative software programming languages (a subset of Java is used) to specific architectures suitable for implementation in FPGAs.

The last but not the least important paper in this special issue, "Performance Evaluation and Limitations of a Vision System on a Reconfigurable/Programmable Chip" by J. Fernández-Pérez, F.J. Sánchez-Fernández, and R. Carmona-Galán, presents a survey of the characteristics of a vision system implemented in a SOPC (System-on-a-Programmable-Chip), also called SoC (System-on-Chip). SOPC is the concept of integrating all components of a computer or other electronic system into a single integrated circuit (chip), with typical applications in the area of embedded systems. In conclusion, SOPCs have gathered momentum over the past few years. In this case, the paper evaluates the performance and limitations of a vision SOPC system consisting in a central processor, with on-chip peripherals, and a special co-processor for low-level image processing tasks. The complete system is implemented in a Virtex-II Pro FPGA.

3 Conclusions

We sincerely hope that this Special Issue stimulates your interest in the many issues surrounding Reconfigurable Computing. The topics covered in the papers are timely and important, and the authors have done an excellent job of presenting the material. In fact, this issue would not have been possible without the assistance of both the authors and the reviewers, to whom we give many thanks.

Acknowledgements

This work has been partially funded by the Ministry of Education and Science and FEDER under contract TIN2005-08818-C04-03 (the OPLINK project).

Miguel A. Vega-Rodríguez, Juan A. Gómez-Pulido, Juan M. Sánchez-Pérez
Dept. Technologies of Computers and Communications, Univ. Extremadura
Escuela Politécnica, Campus Universitario, s/n. 10071 Cáceres. Spain
E-mail addresses: {mavega, jangomez, sanperez}@unex.es