ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3,Special Issue 1,April 2015

Design and FPGA implementation of TDEA using Light Weight Processor based multiprocessing system

Shivaraj B G[1], Shankar B B[2], Praveen J[3], Raghavendra Rao A[4]

M.Tech Student, Dept. of ECE, VLSI Design and Embedded Systems, AIET, Mijar, Moodbidri, India[1]

Sr. Assistant Professor, Dept. of ECE, AIET, Mijar, Moodbidri, Karnataka, India[2]

Sr. Associate Professor, Dept. of ECE, AIET, Mijar, Moodbidri, Karnataka, India[3,4]

Abstract: Multiprocessors have been widely used in modern high performance embedded system to meet the computational needs of smart, real time applications spread across multiple fields. While custom IPs (Intellectual Property) on FPGA based systems are commonly used, multiprocessing on FPGAs have not been explored enough due to concerns about meeting a right trade-off between area usage, achievable performance, and the required design time. Multiprocessor embedded systems (MESes) are a very promising approach for high performance yet relatively low-cost computing. This paper presents a design and implementation of a multiprocessing system on FPGA using multiple light weight soft processors (LWP) that work in conjunction with a custom hardware to achieve balanced performance to resource ratio. As an example we have implemented a TDEA (Triple Data Encryption Algorithm). Simulation is done by using Xilinx and implementation is done by using FPGA.

Keywords: Field Programmable Gate Array (FPGA), TDEA, Processor, Multiprocessing.

I. INTRODUCTION

As the increase in capacity of Field Programmable Gate Arrays (FPGAs) made it possible to include many microprocessors within a Single chip. Multiprocessing systems are systems with more than one processing which can execute several processes simultaneously [1]. As technology advanced, it began to be possible to integrate in a single chip complete multiprocessing system. In this respect, FPGA's (Field Programmable Gate Array) emerge as a new and promising platform to implement multiprocessing systems. FPGAs enable fast prototyping and research of new architectures without ASIC (Application Specific Integrated Circuit) related problems[2]. Open source processors do not have these limitations, but aspects like design quality, support and documentation can become a bottleneck. A good solution to the bottlenecks of such ad-hoc designs is also given in Combinational and sequential elements are explicitly separated to clarify time dependencies between processes. The algorithm is completely determined by the Combinational process.

Computer networks play an important role in computer science as well as in today's life. They allow communicating easily on large distances. In recent years the computer networks have been growing at a very high rate and the data throughput has grown dramatically. The data in the networks are usually sent in a form of packets. The packets are transmitted from a source to a destination by network appliances like switches or routers. Network processors are a class of processors which are targeted on the network appliances[3]. These devices manipulate the frames of data flowing in the computer networks.

Majority of FPGA-based multiprocessing that has been Previously explored make use of commercially available soft processors from vendors like Altera and Xilinx. While multiprocessing on FPGA has been feasible, not many solutions have been explored due to existing tradeoff between a processor based solution and a custom design solution. Several techniques are applied to solve hazards. For data hazards forwarding is applied to reduce the number of stalls to a minimum. The structural hazard which occurs when the same register is read and written concurrently is also solved using operand forwarding. When the result of a load instruction is immediately used, these techniques cannot be applied and a stall will be inserted in the pipeline. Finally, control hazards are solved using a pipeline flush [3].

Custom designs are always high in performance but they come at the expense of chip area and power. Processor based solutions are efficient in terms of area but low in performance [1].

In addition, specific processor architecture is not suited to different application domains. For example, a DSP architecture that is suited for low-to-moderate performance image, video, or wireless processing, is not efficient for wired networking applications such as switching/routing. FPGA vendors provide their own soft

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3,Special Issue 1,April 2015

processor solutions that can be configured to suit a designer's requirement [5]. These are general purpose soft processors widely used in multiple applications. The multiprocessor abstraction retains the advantage of software programmability and provides an easy way to deploy applications from an existing code base. FPGAs also allow the designer to customize the multiprocessor for a target application. Designers can iteratively explore other configurations or offload critical functions into co-processors on the fabric to improve performance.

II. LITERATURE SURVEY

A paper "Multiprocessor system in an FPGA" International Conference on Reconfigurable Computing and FPGA's" [1] concluded with the main objective which consisted in the design and implementation of a multiprocessor system in a FPGA. The main contributions involving in the paper can be summarized as Design of a homogeneous multiprocessor system with distributed memory and streaming communication. Development and comparison of two different communication architectures, a crossbar switch based architecture and NoC based with mesh topology architecture. Evaluation of scalability and performance of the Crossbar Switch based architecture. Acceleration of a matrix multiplication test application through mapping on a multiprocessor system with increasing number of cores. Implementation of a four cores multiprocessing demonstration system in a Spartan-3E device and concluded that being able to broadcast data is extremely important in parallel applications, because it reduces significantly the communication delay.

A paper "An FPGA-based Soft Multi-processor System for IPv4 Packet Forwarding," [2] concluded on soft processing architecture obtains the effectiveness of FPGA-based soft-multiprocessors for high performance applications. And designed a soft multiprocessor for the data plane of the IPv4 packet forwarding application and achieved a throughput of 1.8 Gbps. The paper also developed a design space exploration framework for soft multiprocessor micro-architectures. Using this framework designed a more efficient multiprocessor that achieved a 1.9 Gbps throughput surpassing the performance of hand-tuned design.

From the study of paper [3], soft multiprocessors on FPGAs only lose a 2.6X factor in performance normalized to area compared to a network processor implementation for the IPv4packet forwarding application. If a high-performance programmable platform already exists for an application niche, then it is a cost-effective implementation medium.

A paper "Definition and SIMD implementation of a multi-processing architecture approach on FPGA" [4] described work is a promising solution to implement the new generation of computation intensive signal or image processing systems. Compared to classical FPGA implementations, not only it allows to dramatically reduce development and evolution costs but it also gives access to sophisticated data dependent algorithms such as the ones required to make systems more intelligent. In fact, seen from industries dealing with long lifecycle, it gives access to similar features as the ones offered by emerging technologies such as massively parallel processing or reconfigurable computing but provides a much more secure way to guarantee long term availability. Moreover the platform approach with an API as suggested for probably a way to allow a smooth transition toward those emerging technologies when they are mature.

III. PROPOSED METHOD

a. LIGHT WEIGHT PROCESSOR

The architecture of Light weight processor is shown in below diagram and it is a 32bit pipelined RISC processor which consisting of Instruction memory, instruction fetching, instruction decoder, Data register and Execte logic.

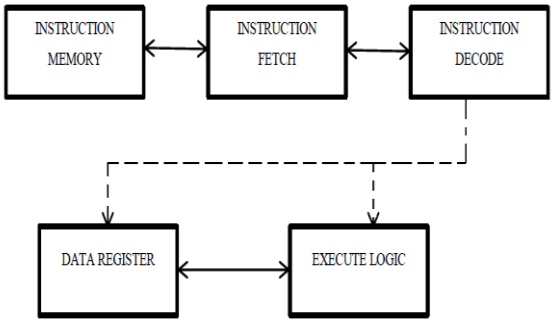

Fig 1. LWP Architeccture

Based upon the program counter output instruction is fetch from the instruction memory and it is decoded in dedode block and the decoded output is access the data from the data register and which execute in the execution block. And the execution block implements the Triple Data Encryption Algorithm.

b. Multiprocessing Using Light Weight Processor

Ref. [7] provides specification for implementation of Triple Data Encryption Algorithm (IDEA), including its primary component cryptographic engine, the Data Encryption Algorithm (DEA) . Three of such DEA forms a TDEA Engine. The TDEA algorithm is implemented in LWP based multiprocessing system with each LWP executing a DEA algorithm.

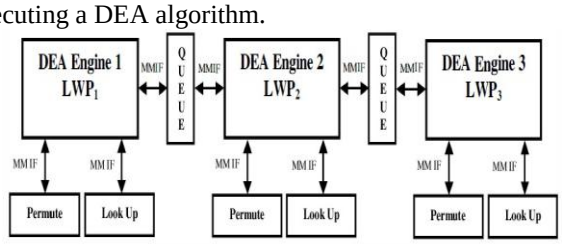

Fig 2. TDEA implementation using LWP based multiprocessing system

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3,Special Issue 1,April 2015

The Triple Data Encryption Algorithm (TDEA) is implemented in LWP based multiprocessing system with LWP executing a Data Encryption Algorithm (DEA). Triple Data Encryption Algorithm, including its primary component cryptography DEA engine, Three such DEA forms a TDEA Engine.

Figure 2 shows the TDEA implementation using LWP based multiprocessing system. As can be seen in the figure, the LWPs are connected in pipelined topology to form a multiprocessing system. The LWPs are connected in pipelined topology to form a multiprocessing system. Each of the LWP works independently on a piece of data and with three LWP working in parallel we achieve 3x the performance as compared to the IDEA implemented on a single LWP. The data word that has to be encrypted is fed to LWP I where first DEA functionality is implemented. The processed data is then passed over to LWP2 whereas LWPI takes over the processing of 2nd word and so on. Thus at any point of time 3 words are processed by this system resulting in higher (3x) data throughput.

c. DEA Implementation on LWP

DEA implementation involves exhaustive data processing done over multiple steps. These operations include data XOR' ing, data lookup, data permutation and data mapping[7].

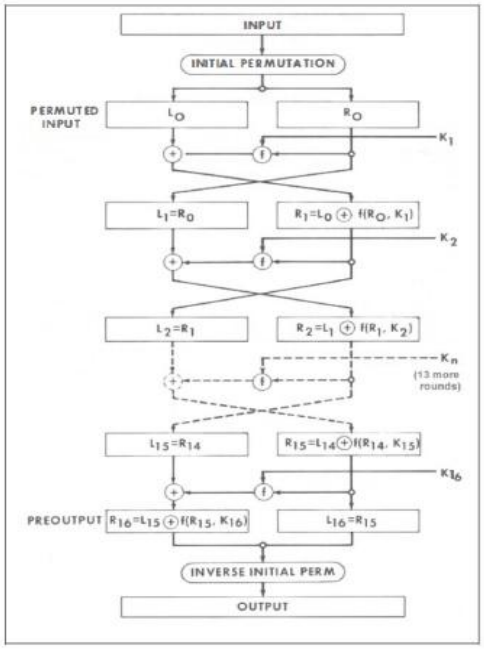

Fig 3. DEA Algorithm

Figure 3 captures the Forward Transformation of the DEA Cryptographic Engine. It involves multiple stages of data processing to obtain the final result. The data processing for DEA can be classified as normal processing and complex processing. The normal processing involves simple operations like regular data re-arrangement or data XOR' ing which can be handled by any conventional CPU. Hence these operations are handled by standard execute block of LWP. The complex processing involves compute intensive operations like data permutation and lookup which can't be easily accomplished using normal arithmetic and logical operations[7]. Also such operations involve bit level data realignment which is costly when implemented on a conventional CPU.

IV. IMPLEMENTATION RESULTS

Here we analyze the area, performance results of LWP based on multiprocessing system implementing a Triple DEA Encryption algorithm. The results are then compared with a earlier result of LWP and MicroBlaze based multiprocessing system implementing the same algorithm. all the systems are simulated using Xilinx simulation tool ISIM. For analysis the systems are implemented using Xilinx ISE 14.3 tool chain and targeted to Xilinx Kintex-7 FPGA device XC7K325T-2 available on KC705 board.

TABLE I RESULT COMAPARISON BETWEEN MICROBLAZE, LWP AND PRPOSED SYSTEM BASED DEA

Resource Utilisation	1 DEA (MICROBLAZE +ACCELERATORS)	1 DEA (LWP+ ACCELERATORS)	1 DEA PROPOSED METHOD (LWP)
Slice registers	718	527	302
Slice Luts	1206	579	298
Slices	765	280	250
Clock frequency	219MHz	308MHz	319MHz

As seen in the Table I resourse is consumed by Proposed LWP is less as compared with the MICROBLAZE and earlier LWP method and Table II gives the whole comparision result of TDEA System.

TABLE II RESULT COMAPARISON BETWEEN MICROBLAZE, LWP AND PRPOSED SYSTEM BASED TDEA SYSTEM

Resource utilisation	TDEA (MICROBLAZE +ACCELERATORS)	TDEA (LWP+ ACCELERATORS)	TDEA PROPOSED METHOD (LWP)
Slice registers	2195	2195	767
Slice LUTs	3761	1727	848
slices	2407	869	765
Clock frequency	202MHz	289MHz	302MHz

V. CONCLUSION AND FUTURE WORK

The designed LWP which works multiprocessing on FPGA and gives the higher performance than the embedded multiprocessing systems and also compared the results of other different processor for multiprocessing on FPGA, and proposed design takes less area and less power and greater performance. In future advanced encryption system implements the multiprocessing on FPGA.

REFERENCE

[1]. Mohammed AhsanRaza, S yed Azeemuddin, "Multiprocessing on FPGA using Light Weight Processor".
[2]. Wilson Maltez José, " Multiprocessor system in an FPGA" International Conference on Reconfigurable Computing and FPGA's, pp.273-278, 2009.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3,Special Issue 1,April 2015

[3]. K Ravindran, N Satish, YJin, and K Keutzer, "An FPGA-based Soft Multi-processor System for IPv4 Packet Forwarding," in International Conference on Field Programmable Logic and Applications (FPL), pp.487-492, August 2005.

[4]. Philippe Bonnot, FabriceLemonnier, Gerard Gaillat, Olivier Ruch,Pascal Gauget, Gilbert Edelin "Definition and SIMD implementation of a multi-processing architecture approach on FPGA" Design, Automation and Test in Europe, 2008.

[5]. Hui Yan Cheah, Suhaib Fahmy, Douglas L. Maskell, "iDEA: A DSP Block Based FPGA Soft Processor", IEEE International Conference on Field Programmable Technology (FPT), Seoul, 2012.

[6]. Georgios-Grigorios Mplemenos, loannis Papaefstathiou. "MPLEM: An80-processor FPGA Based Multiprocessor System" 16th International Symposium on Field Programmable Custom Computing Machines April 2008.

[7]. William C. Barker, Elaine Barker "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher" Revised January 2012.