Shayan Taheri **Homework 03 – Proposal for Term Paper**

Low Power and Secure Multicore Processors

The emergence of parallel processors and machines dated back to the mid-1960s. However, they were left relatively untouched due to the difficulties of programming them. Since the past few years, major chip manufacturers have been interested in designing microprocessors based on the theory of parallel processing. In other words, multiple processors are placed inside a single chip. The main reason behind this trend is due to the requisiteness of following Moore's law, which is achieving growth in circuit integration and performance every two years. In fact, increasing clock rate and design complexities of uniprocessors provides performance improvement, but with the cost of extreme power dissipation and other issues. Inclusion of more than one processing element in a single chip is called a multicore processor design that has the advantage of delivering significant performance growth with much less power consumption.

Due to the rise of mobile and portable electronic devices and other forms of mobile computing where battery life, size, and weight are critical along with the notable demand in utilization of cloud-based data centers (a.k.a. warehouse-scale computers) that comes with the cost of remarkable energy usage, low power design is much more important than ever it was. Power consumption of a processor can be reduced at different levels, including fabrication technology, circuit design, micro-architecture, instruction set architecture, run-time or operating system (O.S.), compiler, source code, algorithm, and application. Low power design at architecture-level that is the interest of this study can be achieved by taking into account three roots of energy waste that are: (a) program waste – due to execution of instructions that are unnecessary for correct program execution; (b) speculation waste – due to speculative execution of instructions that do not commit their results; and (c) architecture waste – due to oversizing of processor structures.

With development of new cyber attacks and escalation of either stored or transmitting digital data that might contain sensitive information, security has become one of the most important factors in processor design. Previously, a processor could be secured in confronting these attacks by protecting the integrity and confidentiality of the stored data and/or code in it, ensuring integrity of computations, preventing the execution of unauthorized code, and etc. However, the emergence of hardware attacks provides an impressive strength for the attackers to perform their malicious purposes due to gaining the ability of bypassing any employed software security mechanism. In this regard, new processor architectures need to be designed with security consideration.

In this survey, different aspects of low power and secure design for microprocessors are studied. Next, recent proposed techniques in these research areas are found and discussed. Finally, these two design parameters for a processing core are investigated practically.