ABSTRACT

The advancement of processing technology has led to a rapid increase in the integrated circuit design complexity. The design complexity has risen to such enormous measures that it is no longer possible to keep up with the productivity demands if all the parts of a design must be developed from the scratch. A popular solution to close this so called productivity gap is to reuse design components that are available in-house or that have been acquired from other companies. These ready to use design components, also known as the Intellectual Property (IP) cores has created a very lucrative and flourishing market which is very likely to continue its current path into the near future. The advantages of reuse-based design methodologies are enormous, that is they offer modular concept; reduce system design complexity and provide fast development-cycle time. Without reuse the electronic industry would not be able to keep on with the challenges of delivering the better, faster and cheaper devices that consumers expect.

With the availability of new Field Programmable Gate Array (FPGA) architectures designed for the system level integration, FPGAs have emerged as an integral part of modern reuse methodology based System–on–Chip (SoC) designs. FPGAs can be used to preserve IP providing solutions that are not only effective but also cheaper than that of Application Specific Integrated Circuits (ASICs). Among the different types of FPGAs available in
the market, the capabilities of SRAM-based FPGAs are highest for FPGA devices and hence they are extensively used by the FPGA IP core vendors for providing the IP core solutions.

In recent years the growing problem of breaches in information security of SRAM-based FPGA IP cores has created a demand for developing an effective Intellectual Property Protection (IPP) technique for securing the IP cores. With the increase in use of reconfigurable FPGAs in production designs and in the implementation of system on FPGA applications, the security of SRAM-based FPGA IP cores cannot be taken for granted anymore. The IP cores must be vigorously protected to preserve competitive advantages and to protect investments. The security threat, financial loss and economic impacts of hardware piracy which has received far less attention compared to software, is even more dramatic than that of the software.

The aim of this research is to develop an efficient wireless based IPP technique for the protection of SRAM-based FPGA hardware IP cores. The wireless based IPP technique proposed in this research is an IP infringement preventive approach that provides access control protection to the SRAM-based FPGA IP cores. This is in contrast with the existing FPGA IPP techniques that are basically IP core infringement detection techniques with limited protection capability and as such they do not prevent the unauthorized usage of FPGA IP cores. Moreover, the existing FPGA IPP techniques do not provide a comprehensive solution for the protection of SRAM-based FPGA IP cores.
The wireless technology adopted in this research for the protection of SRAM-based FPGA IP cores is the Radio Frequency Identification (RFID) technology, which is currently a significant technology in the wireless application areas. The RFID based IPP technique developed in this research work employs wireless authentication and remote activation techniques to provide access control protection for SRAM-based FPGA IP cores. The proposed IPP technique also overcomes the secure secret decryption key storage problem associated with the traditional encryption based IPP techniques that are widely used for the IPP of the reconfigurable FPGA IP cores. Further the technical benefits of the RFID technology employed in the RFID based IPP technique also create the basis for real business benefits in the IP core industry.

This research presents three types of IPP schemes based on the RFID technology for the protection of SRAM-based FPGA IP cores. The RFID based IPP schemes incorporates different types of security features and hence provide varying level of protection to the SRAM-based FPGA IP cores. These schemes also support safe exchange of reconfigurable FPGA IP cores between the IP providers and the system developers. Further, an analysis of the RFID based IPP schemes is also carried out to demonstrate the suitability of each of these schemes to different types of IP cores.

The goal of this research is also to develop a proof of concept hardware prototype that shall demonstrate the effectiveness of the proposed RFID based IPP schemes in the protection of SRAM-based FPGA IP cores of
various complex functionalities. The ITC’99 benchmark circuits, which are the register transfer level benchmarks with the characteristics typical of that of the synthesized circuits, are used for the testing and analysis of the RFID based IPP schemes. The results derived from the testing of the hardware prototype are quite encouraging and show that the proposed IPP technique is a viable solution that can be adopted by the IP core vendors to protect their proprietary IP cores.