Microprocessors and Microsystems 37 (2013) 629–640

Contents lists available at SciVerse ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

RFID based access control protection scheme for SRAM FPGA IP cores

Laavanya Sridhar [a,*], V. Lakshmi Prabha [b]

[a] Pyramid Design Private Limited, 25, K.S Ramaswamy Street, K.K Pudur, Coimbatore 641 038, Tamil Nadu, India
[b] Government College of Technology, Coimbatore, Tamil Nadu, India

ARTICLE INFO

Article history:
Available online 2 May 2013

Keywords:
SRAM
Static random access memory
FPGAs
Field programmable gate arrays
IPP
Intellectual property protection
Reconfiguration
Access control
Tag bypass feature
Bitstream encryption
Semi-passive radio frequency identification
Decryption key transmission

ABSTRACT

Field-programmable gate-array (FPGA) based hardware IP cores have emerged as an integral part of modern SOC designs. IP trading plays central role in Electronic Design Automation (EDA) industry. While the potential of IP infringement is growing fast, the global awareness of IP protection remains low. In this work, we propose a Radio Frequency Identification (RFID) based protection scheme for Intellectual Property Protection (IPP) of Static Random Access Memory (SRAM) FPGA IP cores that overcome the limitations of existing IPP techniques. Here, three types of reconfigurable RFID tags is realised in order to support the incorporation of the proposed RFID based security scheme in all the reconfigurable FPGA devices of Xilinx family. Also a special tag bypass feature is employed to increase the suitability of proposed scheme as an IPP technique for reconfigurable IP cores. The proposed scheme supports safe exchange of reconfigurable FPGA IP cores between IP providers and system developers. The results derived from the testing of hardware prototype used for the evaluation of the proposed scheme are quite encouraging and shows that the proposed security feature can be incorporated into the reconfigurable IP cores of any functionality without significant performance degradation of the reconfigurable IP cores.

1. Introduction

Among the FPGA technologies, SRAM FPGAs have highest density of resources and hence support advanced and complex functionalities. SRAM FPGAs are dynamically reprogrammable, in system-Programmable and support high speed of operation. These features make them more attractive to designers and are widely used for providing FPGA based IP cores in design-reuse environment [1]. But SRAM FPGAs have fewer safeguards to protect IP design against illegal copying and theft. The reason is that once the data is loaded, it is held in SRAM memory cells. Such cells can easily be probed to determine their contents. In addition, the configuration bitstream is usually stored in a separate memory chip and on every power-up the FPGA reads the bitstream from external on-board memory to loads its configuration pattern. Hence without some type of security mechanism to protect the configuration data before it is loaded into the chip, the data is open to snooping [2]. (Kindly note that henceforth in our discussion, the terms FPGA and IP cores will denote SRAM FPGA and SRAM FPGA IP cores respectively.)

In general, the FPGA IP core designer's rights can be protected within the legal frame work by patents and copyrights [3]. Techniques that assist the original designer to protect his/her patented or copyrighted FPGA IP cores are related to authorship identification of configuration data sequences through the use of watermarking and fingerprinting techniques [4]. The concept of FPGA-based watermarking and fingerprinting was first proposed by Lach et al. [5,7]. Currently there are various types of FPGA-based watermarking schemes in practise [8–13]. Further these watermarking schemes are employed at different abstraction levels of FPGA design flow like the physical design level [14–17], structural level [18–21] and behavioural level [22–23], in order to provide the required intellectual property protection of the FPGA IP cores. Also there are various fingerprinting techniques available for the FPGA IP core protection [24–26]. But all these watermarking and fingerprinting techniques used for the FPGA IP core protection suffer from a common drawback. The drawback is that the unique signatures provided by the watermarking and fingerprinting techniques at various levels of abstraction are capable of only detecting the IP infringement and as such they do have the capability of preventing the illegal usage of the FPGA IP cores. That is, they rather provide a basis for litigation once the crime has been committed and are ineffective in controlling the unauthorised usage of the FPGA IP cores. Hence an active type of protection is very much essential for the secure usage of FPGA IP cores.

The active type of design protection for the FPGA devices has been available for some time in the form of configuration encryption [27]. One of the earliest suggested mechanisms for providing

* Corresponding author. Tel.: +91 422 2448749.
E-mail addresses: laava14@hotmail.com (L. Sridhar), profvlp@gct.ac.in (V. Lakshmi Prabha).

0141-9331/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.micpro.2013.04.002

bitstream security to the FPGA is contained in a US patent assigned to Pilkington Microelectronics [28]. The primary disadvantage of this approach is that it requires non-volatile memory and hence non-standard processing of FPGA device which increases the cost. A variant of the Pilkington scheme is used by the Xilinx in their Virtex II family wherein instead of providing on-chip EPROM (Erasable Programmable Read Only memory) to store the cryptography key; the key is stored in the key register with its own power supply lines [29]. Here an external battery maintains the state of register when the equipment is power off and this adds cost to the system and also reduces the overall reliability, as a momentary loss of power will delete the key. Strategies based on static secret keys already inserted during the manufacturing process are discussed in [30–32]. Here, the issues of key transfers are solved by including the cores both for encryption and decryption in the FPGA. But, these approaches require the implementation of additional security features in the FPGA and also the participation of FPGA manufacturer whenever a bit stream is to be encrypted for a particular FPGA.

The usage of Physical Unclonable Functions for the storage of encryption keys is described in [33–35]. A partial encryption scheme in which the configuration bitstream is partially encrypted and then loaded onto a separate RAM (Random Access Memory) built into the FPGA is described in [36]. The security of these techniques relies on the fact that the bitstream file is hard to reverse engineer. Dynamic IPP techniques that uses both public-key and symmetric cryptography but does not burden the FPGAs with usual overhead of public key cryptography is discussed in [37,38]. But these approaches require few modifications to the current FPGA technology. A public key cryptography based protection scheme that exploits the dynamic partial reconfiguration feature of the FPGA is discussed in [39]. The main limitation of this scheme is that it can be employed only in FPGAs that support the partial reconfiguration feature. Finally, in practise, most of the encryption based IPP approaches have eventually been broken and are ineffective in protection of third-party IP.

Moreover, all the encryption techniques provide only the confidentiality of design; it does not say anything about its authenticity. Authentication is important as it ensures the authorised usage of IP cores. Hence there is an increasing need for intellectual property protection (IPP) technique which provides authentication protection to IP cores and also allows safe exchange of IP cores between the IP core vendor and system developer or customer. This aspect is addressed in the RFAP scheme [40] that protects symmetrically the interest of both the IP provider and the IP buyer. The RFAP scheme provides wireless authentication protection along with encryption security feature for the IPP of the IP cores. But one of the main concerns of the RFAP scheme is that of the FPGA's software overhead due to the implementation of the reconfigurable RFID tag. The overhead associated with the reconfigurable RFID tag implementation impose a limit on the amount of FPGA's resource available for IP core's main functionality implementation.

The proposed work addresses the limitation of RFAP scheme [40] and it overcomes the shortcomings by exploiting the reconfiguration aspect of the SRAM FPGA device. The incorporation of the reconfiguration aspect of the SRAM FPGA in the proposed scheme ensures that there is no significant software overhead in the FPGA due to the realisation of customised reconfigurable RFID tag and almost the whole of the FPGA's resource is available for IP core's main functionality implementation. Also the RFID tag with AES core realised in RFAP scheme [40] may not be suitable for all reconfigurable FPGA devices present in Xilinx family. Hence in this work we have realised three types of reconfigurable RFID tags to suit all the reconfigurable FPGA devices present in Xilinx family.

Another important concern of RFAP scheme [40] is that of the dependence on the validating unit for every activation and hence usage of IP cores. That is, on every power-up, the IP core unit requires a validating unit for authentication, activation, decryption and hence usage of main functionality of the IP core. This aspect of [40] may not be practically feasible and hence in the proposed scheme we have introduced a special Tag Bypass Procedure (TBP) feature, which would provide more practical suitability for the employment of the proposed scheme as an IPP technique for the IP cores.

The organisation of this paper is as follows: Section 2 details the methodology, working and tag bypass procedure involved in the proposed IPP scheme. An analyses of the effectiveness of the proposed work as an IPP scheme is given in Section 3. The implementation details along with the results are presented in Section 4. Finally, we conclude in Section 5.

2. Proposed work

The proposed scheme employs the currently adopted new auto-identification technology: Radio Frequency Identification (RFID), which is very promising in terms of range of economically accessible applications. The choice of RFID technology for the scheme is due to the various important security services provided by the technology like: Confidentiality; Integrity; Authentication; Non-repudiation; Availability and Access Control. The technical benefits of RFID create the basis for real business benefits. Use of RFID technology can: increase business productivity; reduce associated costs; provide higher reliability; improve visibility and traceability [41].

Before discussing the proposed IPP scheme to manage the IP rights, it is helpful to clearly define the various parties involved in the IP core transaction. The goal is to create a framework in which the actions of various parties can be analysed to create business models better matched to the market needs. Our idea assumes an IPP scenario with the three participating business parties as shown in Fig. 1. It basically includes: the 'FPGA vendor' who designs and manufactures FPGA chips; the 'IP core vendor (IPCV)' who designs IP cores for distribution and the 'system developer (SD) or customer' who designs a complete system and may make use of one or more IP cores purchased from core vendors.

This security scheme is based on RFID security system scenario and hence similar to any RFID system, here also there are two basic modules (shown in Fig. 2): an IP core module in which a customised semi-passive RFID tag security feature is implemented for the protection of main functionality of IP core. The second module is a RFID tag reader module integrated with the database management system. Henceforth in the discussion the notation M_{IPCORE} unit will denote the IP core unit to be protected and M_{VAL} unit will denote the validating unit respectively. Further the terms tag and reader will denote the RFID tag and RFID reader respectively.

The M_{IPCORE} unit includes a reconfigurable FPGA along with an on-board non-volatile external memory, a configuration controller (CC) and a tag analog interface to support the RF communication. The customised tag module, the IP core's encrypted main functionality bitstream module and bitstream decryption module are stored in the on-board non-volatile memory. The CC is basically a microcontroller that controls the configuration process of reconfigurable FPGA. The CC is programmed with application specific data and configuration commands to support FPGA reconfiguration process. The block diagram depiction of digital components of customised reconfigurable tag configured in programmable hardware is shown in Fig. 3.

The functionality of each of these digital modules are as follows: the tag finite state machine keeps record of states of the tag; the control module is responsible for commanding the operations of the other modules and makes use of flag registers for the same;