CHAPTER 3
RFID BASED IPP TECHNIQUE

3.1 INTRODUCTION

RFID is a contactless identification technology that enables remote-automated gathering and sending of information between the RFID tags or transponders and the readers or interrogator using a wireless link. In this research work, the RFID technology is employed for the identification, tracking and also for improving the security aspects of the SRAM-based FPGA IP cores. This research work proposes a semi-passive type RFID system for the IPP of the SRAM-based FPGA IP cores. The proposed semi-passive type RFID system makes use of a customized reconfigurable tag realized in the SRAM-based FPGA for providing the security to the IP cores. Also three different types of IPP schemes that are based on RFID technology are proposed in this research work in order to provide the varying level of protection to the SRAM-based FPGA IP cores.

3.2 RFID TECHNOLOGY

RFID technology is fundamentally based on wireless communication and makes use of radio waves, which form the part of the electromagnetic spectrum. RFID is a dedicated short range communication technology that is currently being adopted as the new auto-identification technology in various industries, as it is very promising in terms of range of economically accessible applications (Simson and Beth 2005). The
emergence of cost effective wireless RFID is a new way of tracking and implementing the business processes and security. It is becoming the promising technology to achieve the real-time visibility of the enterprise operations. It has several obvious advantages such as non-line-of-sight reading, high-speed reading, multiple reading and writing simultaneously, minimal human intervention and the fact that the tags can be read through a variety of visually and environmentally challenging conditions such as snow, ice, fog, paint, grime, inside containers and vehicles and while in storage (Klaus 2003).

The major purpose of deploying RFID is for identification, authentication, location or automatic data acquisition. RFID has become very valuable from the productivity point of view. RFID offers significant strategic value potential for the companies in developing an integrated model of supply and demand chain to drive revenues (Hossain and Prybutok 2008). RFID is becoming the dependable technology to prevent theft and counterfeiting. It helps to prevent the insertion of counterfeit products into the supply chains (Smith 2005). RFID is effective when faster processing, longer reading range, flexible data carrying capability and more secure transactions are required.

A combination of RFID technology and computing technology that brings value to a business or engineering process is called a RFID system. A RFID system (Sanjay et al 2002) consist of three elements: a transponder (tag) placed on the object to be tracked, an interrogator (reader) which sends queries to tags and obtains data in response and a data processing system, including the necessary software as shown in Figure 3.1. The latter two are sometimes treated as one entity. The tags are attached to or embedded in the host objects to be identified and can be read when they enter a reader’s
antenna field. RFID makes use of RF (Radio Frequency) for the contactless data transfer between a reader and a tag.

Tags and readers are the core hardware components of a RFID system. A RFID tag contains an integrated circuit and an antenna. A tag sends signals to and receives signals from the readers via the antenna. There are three types of tags in current usage (Jones et al 2006); they are the passive tags, semi-passive tags (also known as semi-active tags) and active tags. Passive tags do not have an internal source of power and hence cannot send outbound signals without receiving energy from a reader. They use an incoming radio frequency signal to power up an integrated circuit and transmit a response. Their antenna must be able to both receive power from an incoming signal and transmit an outbound signal. Passive RFID tags do not require batteries and can be much smaller and have an unlimited life span. Because the passive tags are cheaper to manufacture and have no battery, the majority of the RFID tags in existence are of the passive variety.

![Figure 3.1 Basic RFID Systems](image)

Active RFID tags have their own internal power source which is used to power any integrated circuits that generate the outgoing signal. Active RFID tags are typically beacon tags but are also available as response tags. Beacon tags are often called beacon or broadcast because they transmit their
tag data at a predetermined fixed interval. Compared to passive tags, the additional energy provides active tags with several advantages. Active tags can receive very low power signals from the reader. Passive tags require a reader to first send a signal in order to communicate, while the active tags can initiate the communication. The tag-reader distance is shorter for passive tags than the active tags. On the other hand, the active tags lifetime is limited to that of their battery, which itself depends on how often the tag is requested to process and/or send information. Many active tags have practical ranges of tens of meters and battery life of up to 5 years. Lastly, the active tags are larger and more expensive than the passive tags.

A semi-passive RFID tag has an internal power source to power the microchip but still requires the power supply from the reader to transmit the tag response, similar to that of passive tags. Semi-passive RFID tags are faster in response. Semi-passive tags are far more reliable and have greater read ranges than purely passive tags. Semi-passive tags have shorter lives (due to their reliance on battery power) and are fragile and significantly expensive. They support moderate distance of operation and also have moderate processing capability.

Readers, which are often called interrogators are complementary to tags and can be as technically diverse as tags. In a basic scenario, a reader sends a pulse of energy to the tag and listens for the tag’s response. The tag detects this energy and sends back a response that contains the tag’s serial number and possibly additional information. In simple RFID systems, the reader’s energy pulse functions are like an on-off switch. In more sophisticated systems, the reader’s radio-frequency signal can contain commands to the tag, instructions to read or write tag memory and even passwords. The reader can emit the signal permanently, thus always searching for tag presence or the signal can be triggered by an external event such as an
operator switch, to save the energy and minimise the interferences. The reader is responsible for querying tags for their data and in turn transmitting the results of a query back to the middleware. The middleware is typically a database that knows which tag has been attached to which object and does some data processing or analysis.

RFID systems can operate at a variety of radio frequencies and each of these frequency ranges has its own operating range, power requirements and performance (Ahson and Ilyas 2008). In accordance with the communication frequency, RFID tags are usually categorized into Low-Frequency (LF), High-Frequency (HF) or Ultra-High Frequency (UHF) transponders. LF tags typically operate on frequencies around 125 kHz and have communication ranges that are commonly below 0.5 m. HF tags operate on the frequency of 13.56 MHz and typically reach communication ranges of 0.5 m to approximately 1 m. Both, LF and HF tags use inductive coupling for communication. By contrast, UHF tags operate using backscattering and reach ranges of up to approximately 7 m. UHF tags operate in a frequency range between 860 and 960 MHz. The performance of the tags and readers can be influenced by many factors such as tag frequency, reader antenna shape and tag antenna design. In addition, the range of operation of RFID systems depends on a number of factors including transmission power, receiver sensitivity, antenna gain, antenna orientation and interference (Khan et al 2009).

While many RFID applications have already been established in practice, the potential of this technology envisions even many more applications. RFID support a wide range of applications which includes everything from asset management and tracking to access control and automated payment (Miles et al 2008). The technology is stable and evolving, with open architectures becoming increasingly available. RFID systems have
received increased attention from academicians and practitioners. Today, RFID is applied widely in supply-chain (Sarac et al 2010), tracking, retail stock management, parking access control, library book tracking, marathon races, airline luggage tracking, e-security keys, toll collection, theft prevention and healthcare (Pavel et al 2008). The deployment of RFID can bring significant benefits wherever an automatic identification of items can reduce costs. This is particularly in the case of internal as well as the global supply chain and also in the asset management, access control systems and document verification systems.

3.2.1 RFID for FPGA Based IP Core Protection

The adoption of RFID wireless technology for the automatic and authentic identification of individual SRAM-based FPGA IP cores is because:

- RFID is a standard and proven technology;
- It supports fast detection rates and can be customized depending upon the applications to be employed.
- Security services provided by the RFID technology like:
  - Confidentiality, which ensures that data, software and messages are not disclosed to unauthorized parties;
  - Integrity, which ensures that unauthorized parties do not modify data, software and messages;
  - Authentication, which ensures that a network can only be accessed by individuals who are authorized;
  - Non-repudiation, which ensures that entities involved in a communication cannot deny having participated in it;
  - Availability, which ensures that the service is available at all times;
Access Control, which ensures that network resources are being used in an authorized manner.

- RFIDs are highly reliable because they are less prone to error due to human intervention.
- RFID can be added on top of the existing IP core functionality ensuring process optimization and performance.
- The RFID technology is user friendly and the RF chip technology used is quite different because it addresses unique storage, range and security requirements according to the applications where it is deployed.
- It also makes it easier for the users to start using the protection system without any additional training.
- It provides a seamless way to move forward with business without any interruption due to the RFID implementation.
- 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 (Shiou-Fen et al 2008).
- Finally another important benefit of RFID is that it facilitates the sharing of information with customers and suppliers, developing alliances, innovating with supplier and establishing strategic alliances.

3.3 IPP SCENARIO

Before discussing the RFID based IPP schemes 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 Figure 3.2. They are as follows:

The first contributor is the ‘FPGA vendor’, who designs and produces FPGA devices. The company that designs the actual FPGAs is the trusted third-party in this scenario because they have an incentive to be trustful to both the system developers who purchase their chips and the IP providers who develop IP cores for their FPGAs. FPGA vendors are not directly involved in the security model.

**Figure 3.2 IPP Scenario for RFID Based IPP Technique**

The second participant is the ‘IP Core Vendor (IPCV) or IP Owner (IPO)’ who designs IP cores for distribution. These IP cores may include simple functions (such as adders and multipliers) which are generally provided free of charge or more complex functions (like peripheral component interconnect bus interfaces) which are provided for a fee. Security-wise, IPCV has two dominant concerns. Firstly, they are interested in protecting their own proprietary designs and technology from being
illegally reverse engineered, copied, exposed or modified. Secondly, they want to provide their customers with ways to protect their own designs throughout the design flow and in the field. They also have the necessity to provide means to enable secure distribution of cores since that translates into increased IP core sales by making the IP designs more widely accessible.

The final participant is the ‘system developer or customer’ who designs a complete system and may make use of one or more IP cores purchased from the IP core vendors. Often the system developer and customer are the same organisation and hence for the purpose of describing the protocols, it makes sense to consider both of them as the same entity. Further, only the IP provider and customer are involved in the IP core exchange transactions. The FPGA vendor’s involvement is not required beyond the manufacturing of devices.

3.4 OVERVIEW OF RFID BASED IPP TECHNIQUE

System developers design their products with a plug-and-play methodology in which they adopt a third-party IP components for integration onto the system. This IP can possibly come from multiple vendors in the case of so called SoC design. The result is an intriguing multi-level authentication problem. At one level, system developers would like to authenticate the IP they are running and at another level the IP providers would like to authenticate the system into which they are integrated. This research work focuses on RF based cryptographic authentication and activation in addition to bitstream encryption for IP core protection. When talking specifically about IP cores, encryption provides confidentiality that helps to protect the privacy of the IP core’s functionality and hence the design, while authentication provides the ability to establish the identities of both the IP core and the underlying hardware system.
In this research a semi-passive type of RFID system is adopted for the protection of reconfigurable SRAM-based FPGA IP cores. Unlike conventional RFID security system, RFID based IPP technique does not make use of standard RFID tags available in the market. Instead, a customised reconfigurable RFID tag is realised and the same is embedded in the hardware logic of the SRAM-based FPGA core to be protected. This is because if the standard RFID tags were used, then the tags could be attached only externally to the IP cores to be protected. These externally attached RFID tags are susceptible to tampering and removal. Moreover the incorporation of the RFID tags inside the reconfigurable logic of the SRAM-based FPGA makes it possible to provide access control protection for the IP cores. The semi-passive tag makes use of the on-board power for the internal operations. The power derived from the RFID reader is utilized by the reconfigurable RFID tag for RF communication with the RFID reader. (Kindly note that henceforth in the thesis, the term tag and reader will denote the RFID tag and RFID reader respectively and it may be used interchangeably).

The frequency of operation adopted in the RFID based IPP technique is 125 KHz. The selection of the low frequency is because we are interested only in near field authentication and hence IP core activation in the customer domain. The near field communication makes it less susceptible to interferences and eavesdropping. Moreover, the higher frequencies have reflection problems and are negatively impacted by metal, liquid, glass and moist environments. The low frequency employed can effectively work in rugged environments and in proximity to metal, liquids or dirt.

The RFID based IPP technique adopts a typical RFID security system scenario and hence similar to any RFID system, this protection scheme also incorporates the two basic modules as shown in Figure 3.3: a customized reconfigurable semi-passive RFID tag module and a tag reader
module integrated with the database management system. The customized reconfigurable tag is realized inside the IP core unit to be protected, along with the main functionality of the IP core unit. We shall henceforth use the notation IPCU to denote the IP core unit to be protected and VU to denote the validating unit which includes a RFID reader unit interfaced with a microcontroller. The main objective of the RFID based IPP technique is to validate the individual IP cores and certify them as secure for activation and hence usage in the customer domain.

![Image of RFID Based IPP Technique]

**Figure 3.3 Outline of RFID Based IPP Technique**

Based on the above discussed RFID based IPP technique methodology, three types of RFID based protection schemes for the protection of SRAM-based FPGA IP cores are presented in this thesis. They are the:

- **RFRAP Scheme**: Radio Frequency-authenticated Remotely-activated Active Protection Scheme
- **RRRAP Scheme**: Radio Frequency-authenticated Reconfiguration-based Remotely-activated Active Protection Scheme

- **RRRAP-TBP Scheme**: RRRAP Scheme with Tag Bypass Procedure

The different RFID based IPP schemes not only incorporate various types of features, but also provide various levels of protection to the SRAM-based FPGA IP cores. The RFID based IPP schemes will enable an organization to significantly change its business process, not only to increase its efficiency but also to increase its effectiveness. These protection schemes are expected to make the implementing organization more resilient. They shall also enable the IP providers to provide better accountability for their products.