ABSTRACT

RFID (radio frequency identification) is a very useful in today life. RFID uses RF signals to identify the objects. It uses in many places like manufacturing, supply chain management, inventory control, construction industry. Due to improvement in VLSI (silicon manufacturing technology) cost of manufacturing of RFID devices have been significantly reduced. In modern days are & near future low cost RFID devices will be in fashion. The universal deployment of RFID devices in consumer items lead to expose new security and privacy risks. These threats are not present in manufacturing environments.

This thesis introduces security & privacy threats. It also deals with basic RFID technical problems. It discuss about various approaches & practical ways to overcome these problems. As a result of the our project we have achieve final output as given following: Accurate identification of tag ID without collision implementation of tag, Design & Simulation by using Verilog HDL & driver’s output is shown in results and Synthesis of project through Xilinx ISE Tool 13.4 and Model-Sim 6.5c.

Keywords---- RFID, Tag ID

I. INTRODUCTION

Object identification is very necessary as increase communication complexity. This enables us to quickly determine the correct data. We clarify it with one example of Trade & Transport. A simple level (mark) allows traders to identify the correct package. It saves lots of time & effort of traders as well as cost. The security & privacy threats allow to communicate correct tag to the reader when multiple tag are present & they want to communicate to a single reader. RFID are Michle Faraday’s discovery of electromagnetic radiation, Maxwell equation of describing of magnetism & Heinrich Rudolf Hertz’s experiment for validating Faradays & Maxwell equation. Their discoveries are the foundation of modern radio communication.

One of the earliest patents for such a system was a radio transmitter for object detection system designed by John Logie Baird in 1926 [16]. The first radio identification technology was the “Identify Friend or Foe” system used in Allied aircraft during World War II [15]. In early 1940, the British Royal Air Force outfitted airplanes with radio transponders that would respond when interrogated. This allowed pilots and ground crews to distinguish the RAF airplanes from the Luftwaffe’s, which proved to be a decisive advantage in the Battle of Britain. About 1960 Electronic Article Surveillance (EAS) was introduce. It was not able to identify particular tag but it detect the presence of tag. Modern RFID was introduced about 1973-1974.

Now RFID is associated with auto identification ID. Basically Auto-ID systems consist of a name or identifier to a physical object by some means that may be automatically read. This identifier may be represented optically, electromagnetically, or even chemically. UPC may be considered as the most successful and well-known auto-ID system is the Universal Product Code (UPC). The UPC is a one-dimensional, optical barcode encoding product and brand information. Optical barcodes offer faster, more reliable, and more convenient inventory control and checkout than checking out by hand. Several weaknesses of optical barcodes are that they require line-of-sight and may be smudged or obscured by packaging. In most circumstances, optical barcodes still require some human manipulation to align a barcode label with a reader. Auto-ID systems that transmit data via RF signals, i.e. RFID, do not have the same performance limitations as optical systems. Data may be read without line-of-sight and without human or mechanical intervention. A key advantage in RF-based auto-ID systems is parallelism.
II. RFID SYSTEM

RFID system consists of three components:
1. RFID tag (transponder): it carries object identifying data
2. RFID reader (transceivers): reads & write tag on data.
3. Database: it contains the records the tag identifying data

1-RFID Tag: The object to be identified in RFID is called tag. Tags are made on microchip for storage & computation. It also consist a coupling element such as antenna for communication. Tag memory may be read only, write once read many or fully rewritable. There are many types of tags that offer different functionalities, have different powersources, or operate at different radio frequencies. Tag data consists of manufacturer, brand, model and a unique serial number. This data is called the tag’s identity, or ID. An ID may be of any length. A 96 bit ID tag used in many applications.

Tag are classified on the basis of availability of power source:
- **a)-Active tag**: it contains on board power source. It has ability to initiate its own communication with other tag.
- **b)-Semi Passive tag**: they have their own power source but communicate to incoming tag. They have no ability to imitate their own communication.
- **c)-Passive tag**: they receive all the power from reader. They have also no ability to imitate their own communication. They are completely inactive in absence of reader.

2-RFID Reader: Reader communicates with tag for their data through RF interface. Reader has internal storage capacity, processing power & connection to back end data base. All the calculation is done by the reader i.e. cryptographic calculation. The channel from reader to tag is forward channel & tag to reader is backward channel. Reader must be able to address a particular tag. If many tag want to communicate with reader must have anti-Collision protocol. Anti-Collision protocol provides safe communication.

3-RFID Database: It contains tag identifying data with arbitrary record. Independent database may be built for access to tag content. Database has secure connection to the reader. Sometimes reader may also consider as a channel between database & tag. If tag contains all the relevant information there is no need to make communication with database. For protocol analysis, it is useful to consider reader and back-end database as a single entity. In other cases, the is considered as an untrusted channel between tag and database.

**Tag Reader Coupling**

Passive tag receives power from electromagnetic field of reader signal. Tags receive power from reader & communicate with reader. Passive tag receives power through inductive coupling or through far field energy harvesting. Tag communicates with reader within a specified band of radio frequency. If operating frequency of tag is f it means that this is the center of an operating band of frequency. Tag reader coupling has been shown in figure below:

![Tag Reader Coupling Diagram](image)

III. SECURITY PROPOSALS OF RFID SYSTEM

1. Physical methods:
   - **Kill command**: It is most powerful tool to protect the user privacy. In this method we kill the RFID tag before it reach to user. It is proposed by AUTO-ID center in MIT. The user can deactivate the tag by using kill command. Killed tag cannot be re-activated.
   - **Faraday cage**: Faraday cage is a container that is made by metal mesh or foil that cannot be penetrated by RF signals. Tags are packed with in Faraday cage. It is inapplicable in many application due to its size, shape etc.
   - **Active jamming**: In this method the user continuously transmit RF signals. These signals block or disturb the reader operation. The broadcast power of signal should be adequate level.
   - **Blocker tag**: A blocker tag is a cheap RFID passive device. It can simulate many tags simultaneously. It avoids user from unwanted scanning of the tag.

2. Cryptographic method:
   - **Hash lock protocol**: It is proposed by Weis[2]. According to him tag may be locked & it discloses to reject its id until it is unlocked. When a tag locked it has a meta Id & it is unlocked by a key such that meta Id=h(key). Meta Id has static information. This protocol allows the tracking of tag.
   - **Randomized hash lock protocol**: It is also introduced by Weis[2]. It was introduced to solve the problem of hash lock protocol. In it tag has additional pseudo number generator aside from hash function. This scheme blocks the attackers (unauthorized user) because tag output data is changed after every communication.
Re-encryption method: Juels&Pappu\[21\] has proposed this scheme. In this method serial number of tag are encrypted. Serial number is embedded in a euro banknote. The stored data in tag are rewritten, this is called re-encryption method. It requires heavy computation. This method avoids tracking of tag.

Hash chain based protocol: It was proposed by Ohkubo \[22\]. it is secure authentication between tag & reader. In it tag & reader use different hash function. on reader query tag respond with a hash value. In the next communication tag update next secret bit which give different different response for next query. When reader sends tag information to database, database authenticates the tag.

IV. ARCHITECTURE OF SECURITY SYSTEM

1-Input block: It is use for sending incoming data in synchronize way with clock pulse. In it tag bit & its corresponding MetaId has been send to the input. One clock signal is necessary so that incoming data is synchronize way corresponding with whole block.

2-Clock block: It is use for synchronization purpose as well as generating initiate flag for all the other block. In it a high frequency signal is given to its input. It produces three output signal one signal for synchronization purpose. It is connected to the entire block. Another is high frequency signal & third is initial signal, it act as ready signal for most of inner block.

3-Randomize block: It takes reader query bit as a input & produce random data which is given to hash block

4. Hash block: It is use to produce the hash data from random data, which is output to the randomize block. It is activated or deactivated by control block.

5-Memory block: It produces data corresponding to incoming address from control block

6-RWM block: It is use for checking that our tag has been locked or unlocked.

7-Control block: It is use for synchronized all the units in system.

8-Output block: It is used for sending data to output from control block. It gives us information that particular tag has been correctly received or not as decided by control block.

9-Final block: For final output we combine all these blocks i.e. all these block acts as a sub module for final output. After simulation of program we get the following driver diagram. From this output we can conclude that metaId(dbgInCode) corresponding to tag code 1010 is 1. dbgOutData is also one i.e. metaId==hash(key)., so that tag first bit is correctly received without collision.

At last we combine all these block to work as a single unit. We also add a clock block for synchronization purpose.

V. RESULT AND CONCLUSION

A RFID Tag Identification has successfully synthesis by Xilinx 13.4 software and implemented on target device Spartan-3E FPGA. In table 1 shown device utilization summary in terms of FPGA parameters. In figure 4. shown simulation wave-foam.

Target Device:-XC3S100e-5VQ100

<table>
<thead>
<tr>
<th>TABLE 1: Design Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logic Utilization</strong></td>
</tr>
<tr>
<td>Number of 4input LUTs</td>
</tr>
<tr>
<td>Number of occupied slices</td>
</tr>
<tr>
<td>Number of bonded IOBs</td>
</tr>
<tr>
<td>Average Fanout of Non-Clock Nets</td>
</tr>
<tr>
<td>Number of 4input Flip Flop</td>
</tr>
</tbody>
</table>
REFERENCES


