CHAPTER 1: INTRODUCTION

RFID (Radio Frequency Identification) finds an immense applicability in domains utilizing identification as the base operation such as in access control, localization etc. It may be designed to work well for either singular or a limited range of applications. However, the strict-coupling between applications and RFID equipment must be relaxed to scale up their usability. In order to do so, RFID middleware’s are employed, allowing the applications to become independent of the underlying complexities. In this paper, we present interplay of all that contemporary RFID middleware’s providing, and actual expectations from them, in terms of desirable features and aspects.

RFID tags are small, wireless devices that help to identify objects and people. RFID may be viewed as a means of explicitly labeling objects to facilitate their “perception” by computing devices. An RFID tag is mostly called RFID tags which is a small microchip designed for wireless data transmission. It is generally attached to an antenna in a package that resembles an ordinary adhesive sticker. An RFID tag transmits data over the air in response to interrogation by an RFID reader.

Radio frequency identification (RFID) uses a tag applied to a product to identify and track it using radio waves. A RFID tag consists of 2 parts, an integrated circuit and an antenna. The integrated circuit is used to process and store information as well as to modulate and demodulate radio frequency signals, while the antenna transmits these signals. RFID reader, also known as the interrogator, is a device used to interpret the data on the RFID tag.

RFID is Features in the optical barcode familiarly printed on consumer products:

- Automation: Barcodes are being optically scanned which require line-of-sight contact with readers and thus careful physical positioning of scanned objects but the barcode scanning requires human intervention. For example, an RFID reader by a warehouse dock door can today scan stacks of passing crates with high accuracy. In the future, point-of-sale terminals may be able to scan all of the items in passing shopping carts.
Unique Identification: A type of object can be identified by the barcode printed on it. The RFID tags emit a unique serial number that distinguishes among many millions of identically manufactured objects.

RFID is widely used in industrial and commercial purposes:

- **Proximity Card**: These cards are contactless used for building access mainly used by the companies for the security access. It is also used automated tool payment transponder, in ignition keys of automobiles for theft detection.
- **Shopping**: In retail shops, consumers could check out by rolling shopping carts past point-of-sale terminals. These terminals would automatically tally the items, compute the total cost, and perhaps even charge the consumers RFID-enabled payment devices and transmit receipts to their mobile phones.
- **Production and Documents Identification**: To increase the efficiency of factories, industries and offices, entrepreneurs ensures the non authorized items should not leave the premises.
- **Medications**: RFID can be used in medication compliance and home navigation for the elderly and cognitively impaired. As researchers have demonstrated that RFID-enabled medicine cabinet could help to verify that medications are taken in a timely fashion.
- **Theft and Counterfeiting Protection**: By RFID, shopkeeper’s can track their products in shopping malls or stores which are expensive by supply chain and eliminate inventory oversights that can cause shipments to "go missing". RFID has already been successfully deployed in stores, particularly on higher-margin or expensive items.
- **Smart Appliances**: To make the home appliances, garments and packages of foods move more cleverly, RFID tags are used such as washing machine can select wash cycle automatically.

The main disadvantage of RFID based applications is the speed in which the tags are identified. For example if a gate reader at the dock door in a warehouse can have hundreds or thousands of tags in their read range. Thus artificially slowing down the loading process. So, fast and reliable identification of RFID tags is an important issue.

It is commonly said that there are no standards in RFID. In fact, there are many well-established standards and a few emerging standards. There are existing and proposed RFID standards that deal with the air interface protocol (the way tags and readers communicate), data
content (the way data is organized or formatted), conformance (ways to test that products meet the standard) and applications (how standards are used on shipping labels, for example). RFID is currently having standardization by EPC global consortium which provides the organization number. This network contains a discovery service for EPC tags in particular which carry information about the items to which they are attached. If a tag in a range requests then it returns the list of all the companies in contact. Then one can contact each company individually and ask to retrieve its event data. The main challenge with this system is that on the one hand companies have an incentive to share this information so as to facilitate their business, on the other, this information is highly confidential and (possibly competing) companies are reluctant to trust one another. Therefore, a big concern is the possibility of espionage of a competitor’s supply chain carried out for instance by retrieving the event data about items in a competitor’s supply chain. In particular, if no appropriate cryptographic measures are taken, the privacy of a user carrying tagged items can be severely damaged. In order to enable these applications and at the same time minimize the risks, public-key cryptography (PKC) attractive solutions. Whether a public-key cryptosystem can be implemented on an RFID tag or not remains an open problem.

In this paper, we focus on the problem of anti-counterfeiting measures that can be provided by RFID-tags. More precisely, we investigate which PKC-based identification protocols are useful for this application. We discuss the feasibility of identification protocols based on Elliptic Curve Cryptography (ECC) and show that it is feasible on RFID tags. Scarce computational and storage capabilities of the tag make designing security systems for RFID challenging. For example, the use of extensive cryptography-based authentication or high-quality random numbers on the tag-side may not be possible. Extensive cryptographic operations can be shifted to the reader-side. However, this requires the tag to either store large keys or frequently communicate with the reader over a secure out-of-band channel to obtain authorization information. The former option is impractical due to limited tag-side storage; the latter one decreases the utility of an RFID system as a time and cost saving identification technology.