# ECC Implementation for Secured RFID Communication

Monika Sharma, and Dr. P. C. Agrawal

***Abstract*—**To protect RFID privacy violation against various attacks (like eavesdropping, location tracking, spoofing, message loss or replay attack etc.) some of the encryption schemes were proposed by researchers to provide secure communication such as blocker-tag, hash lock scheme, randomized hash lock, hash chain, variable ID, re-encryption, RSA etc. However applying this public key encryption approach requires higher implementation effort in chip size, low performance and high power consumption.

A good RFID tag is one which is cheap (small area), scalable, securable, untraceable (PKC) and fast (light weight). As ECC is based on multiplication technique so it is comparatively faster, cheap and complex than other techniques. So in this paper we will approach this technique in such a way that both tag as well as reader authenticates while accessing the information through server and data can be protected from eavesdropping.

***Keywords*—**Elliptic curve cryptography (ECC), privacy, Radio Frequency Identification (RFID) and security.

## I. Introduction

ELLIPTIC curve cryptography (ECC) was first introduced by Neal Kolbitz and Victor Miller in year 1985. The main reason for elliptic curve cryptography implementation for RFID technology is that there is no sub exponential algorithm known to solve the discrete algorithm problem on an appropriately selected elliptic curve. This means that importantly smaller parameters can be used in Elliptic Curve Cryptography than in other competitive systems such as DSA and RSA but with similar security levels. The smaller key sizes with reduced and fast computations in storage space, bandwidth saving and processing power makes Elliptic curve cryptography used in various fields such as smart cards, mobile phones etc.. According to Zheng and Lionel an alternative to RSA, elliptic curve cryptography is another approach to public key cryptography [1]. The elliptic curve cryptography permits one to select a secret number as a private key which is then used to select a point on a non secret elliptic curve. A special property of an elliptic curve is that it forces both parties to compute a secret key solely based on its private key and other's public key.

Monika Sharma, Research Scholar, Mewar University (Chittorgarh) Raj., Department of Computer Science & System Studies, Asst. Professor Amity Institute of Information Technology, Amity University, Secor-125,Noida, U.P., INDIA. monika_05@rediffmail.com.

Dr. P. C. Agrawal, Guest Professor, Mewar University & Retired 'Scientist E' Ministry of communication & Information Technology Govt. of India, New Delhi.

Elliptic curves are not similar from ellipse. An elliptic curve is the collection of points in x-y plan to satisfy an equation y2+a1xy+a3y=x3+a2x2+a4x+a6. This equation is also known as Weierstrass equation which can be applied on real, rational, complex or finite field. Contrary to that Tilborg and Jajodia defined that elliptic curve cryptography enhances the analysis and configuration of public key cryptographic schemes that can be established using elliptic curves [2]. The elliptic curve scheme analogues based on the discrete logarithm issue where the underlying group is the collection of points on an elliptic curve defined over a finite field. Stavroulakis and Stamp described that elliptic curve cryptography enhances using the group of points on an elliptic curve as the underlying number system for public key cryptography [3]. Elliptic curves are algebraic structures that form a basic class of cryptographic primitives which depend on a mathematical hard issue. The elliptic curve discrete algorithms problem is based on the intractability of deriving a huge scalar after its multiplications with a given point on an elliptic curve Yalcin [4].

## II. Why Elliptic Curve Cryptography

According to Tipton and Krause ECC implementation is suitable for following reasons [5]:

### *A. Scalability*

As RFID technology needs stronger and stronger security with big keys, Elliptic curve cryptography can continue to offer the security with proportionately lesser additional system resources. By implementing ECC, RFID technology capable of offering higher security levels without increasing their prices.

### *B. Shorter transmission times and less memory*

The elliptic curve discrete logarithm problem algorithm strength means that strong security is gained with proportionately certificate sizes and smaller key. The smaller size of key in turn means that small memory is needed to store certificates and keys and that less data must be passed between the tag and the reader so transmission times are shorter.

### *C. No coprocessor*

The elliptic curve cryptography reduced processing times also make it separate for the platform of RFID tag. Other public key systems involve many computation that a dedicated hardware component referred to as crypto coprocessor is

needed. The crypto coprocessors not only take up huge amount of space on the tag but they also higher the price of the RFID chip by about 20 to 30% which transforms to an increase of about $3 to #5 on the cost of each tag. With elliptic curve cryptography the algorithm can be implemented in available tag Memory so no extra hardware is needed operate fast and strong functions of security.

### D. No coprocessor

As described above, the private key in a public key pair must be kept secret. To prevent the transaction truly from being refuted the private key must be inaccessible wholly to all parties except the entity to which it belongs. In applications using the other kinds of public key systems presently in use, tags are personalized in a protective environment to meet this need. Because of the complexity of the computation needed, generating keys on the tag is typically impractical and inefficient.

There are two major causes for using elliptic curves as a basis for public key cryptosystems. The first reason is that the elliptic curve based cryptosystems exists to offer better security than traditional cryptosystems for a given key size. One can take benefit of this fact is to develop security or to develop performance by lowering down the size of the key while keeping common security. The second cause is that the additional framework on an elliptic curve can be destructed to build cryptosystems with interesting features which are impossible or critical to gain in any other way.

With Elliptic Curve Cryptography the time required to produce a key pair is so small that even a component with a very limited computing tag power can produce the key pair which can offer a better random number generator. This means that the process of tag personalization can be streamlined for applications in which no repudiation is necessary.

## III. RFID Security Issues And Threats

RFID technology has three components: Tag, Reader and Server. A reader sends a query to tag and according to that, tag respond through its unique Id and according to that Id information is accessed through server. RFID security involves manipulation of RF communication between tag and reader & reader and server. The common threats for RFID security is an unauthorized access to tags, clone tags, and side channel attacks.

### A. Unauthorized Access to Tag

All types of tag may share a critical vulnerability to RFID readers. A reader may access a tag and recording confidential information or may also write new, potentially damaging information to the tag or kill the tag. In every case tags respond to authorized RFID reader, since the reader appears like any other RFID reader. This may cause big implications as tags may have data that should not be shared with unauthorized devices.

For example, A reader might be able to measure the inventory on a store shelf and chart sales of certain items—providing critical sales data to a manufacturer which results helps to developing a competitive strategy informed by corporate espionage for example, negotiating more shelf space or better product placement.

### B. Tag Cloning

Clone tags are unauthorized copies of real tags. These tags connect with the RFID reader via RF and send false data.

For example, a bootleg product could appear to be an actual product if it bears a clone tag. A rogue tag placed within proximity to a RFID reader could contribute false data to the reader. In both cases, these tags affect the integrity of the system, and undermine security for both consumers and the companies that rely on RFID.

### C. Side Channel Attacks

Today's biggest vulnerability in RFID systems occurs when RFID readers or any other rogue devices eavesdrop on authentic transactions and RF communications between authorized tags and readers. The rogue device can access passwords or data (confidential) using lab equipment [6].

## IV. RFID Technology Weaknesses

### A. Data encryption

Sensitive data such as an Electronic Product Code (EPC) could identify a personal product, which is not encrypted. The data is only covered code by pseudo-random number transmitted by the tag whereas this code may compromised by side-channel attacks.

### B. Password Protection

Passwords are also not encrypted. They are cover coded same as tag data which is less robust than a strong cipher.

### C. Tag/Reader authentication

Lack of authentication of tag and reader results cloning of tags can be possible and unauthorized readers may access tag data. RFID system security levels are not high enough to generate the high levels of consumer trust that will enable widespread acceptance of RFID at the item level.

## V. ECC Implementation On RFID

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography a key pair (private and public) is used in communication while communicating with users or devices. While communication only a particular user/device knows the private key where as the public key is distributed to all other devices/users. In certain public key algorithms algorithm the devices/users which are taking part in communication may know a set of predefined constants. For example, ECC domain parameter, Public key cryptography does not require any shared secret between the communicating devices/users.

The mathematical operations of ECC on elliptic curve is $y2 = x3 + ax + b$ where $4a3 + 27b2 \neq 0.$ Here each

value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The point in the curve represents the public key and the random number shows the private key. We obtained public key just by multiplying the private key with the generator point 'G' in the curve.

'G' (generator point) and 'a' and 'b' (curve parameters) with some more constants determine the domain parameter of ECC.

Small size key is the main advantage of ECC. A 160 bit key in ECC is equally secured as 1024-bit key in RSA

TABLE 1
A COMPARISON OF KEY SIZES NEEDED TO ACHIEVE EQUIVALENT LEVEL OF SECURITY WITH THREE DIFFERENT METHODS. (BY NIST RECOMMENDATION)

| Symmetric Encryption Key Size in bits | RSA and Die-Hellman "Key" size in bits | ECC "Key" Size in bits |
|---|---|---|
| 80 | 1024 | 160 |
| 112 | 2048 | 224 |
| 128 | 3072 | 256 |
| 192 | 7680 | 384 |
| 256 | 15360 | 512 |

Singular elliptic curves are not suitable for cryptography as they can get easily cracked. Even real numbers are also not suitable for cryptography as real number calculation is prone to round off errors.

The elliptic curve, which are more suitable for cryptography is prime finite field curve.

The values of the parameters a & b are restricted and the value of the independent variable x, y to some prime finite field Zp

curve $y2 = x3 + ax + b(mod\ p)$

Where $4a3 + 27b2 \neq 0.$

Mainly ECDLP (Elliptic Curve Discrete Logarithm Problem) is strong hand of ECC which makes a positive sign to use as a cryptographic algorithm. So ECC can be used for authentication purpose for tag and reader communication and also can be used to protect communication intercept between tag and reader by encode the data.

## VI. PROPOSED SCHEME FOR TAG & READER AUTHENTICATION

E.g. (a, b) here a, b and q are the ECC parameters

$$Y^2 \bmod q = (X^3 + aX + b) \bmod q$$

Let Q is base Point on Elliptic curve.

### A. Tag Key Generation

Select private key for tag $k_T$ $kR < n$

Calculate public P $P = k_T \times Q$

### B. Reader Key Generation

Select private key of reader $k_R$ $kR < n$

Calculate public M $M = k_R \times Q$

### C. Tag Secrete Key Generation

$$P_1 = K = k_T \times M$$

### D. Reader Secrete Key Generation

$$P_2 = K = k_R \times P$$

Both produce the same result

$$k_T \times M = k_T \times (k_R \times Q) = k_R \times (k_T \times Q) = k_R \times P.$$

*Elliptic Curve Tag Encryption and Decryption*

When both tag and reader is authenticated using their secrete key while communication, Tag reveal its ID to the reader than only reader will able to access tag information.

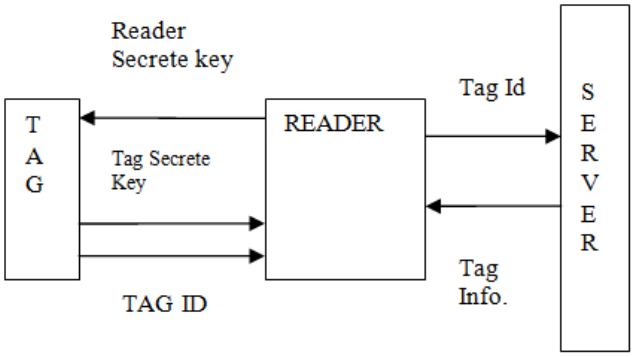


Fig. 1 Secrete key share between tag and reader, then only the information access through server

Consider TagID sent by tag to reader, Tag choose random positive integer 'k', a private key nA . And generate the public key $P_A$ = nA x G , where G is base point and produces the ciphertext Cm consisting of pair of points.

$$Cm = \{KG, TagID + kPB\}$$

$P_B$ = $n_B$ x G is the public key of reader with private key $n_B$.

To decrypt the cipher text, reader multiplies the first point in the pair by reader's secrete key and subtract the result from the second point.

$$TagID + kP_B - n_B(kG) = TagID + k(n_B\ G) - n_B(kG) = TagID$$

Here $P_A$ is a public key of tag and $n_A$ is a private key of a tag.

$P_B$ is a public key of reader and $n_B$ is a private key of a reader.

## VII. CONCLUSION

In this paper we have discussed the various issues related to the Radio Frequency Identification (RFID) security and

proposed a scheme that how Elliptic curve cryptography (ECC) can provide a solution for secure communication via authenticating tag as well as reader both. For RFID, elliptic curve cryptography is the best cryptosystem as it provides a fast, cheap and complex computation. Implementing security using elliptic curve cryptography saves cost; time and area ( memory).

## REFERENCES

[1] Zheng P and Lionel M N, Smart phone and next generation mobile computing, Morgan Kauffmann Publishers, UK, p 354, (2006).
[2] Tilborg H C V A and Jajodia S, Encyclopedia of Cryptography and Security, Springer, New York, p397, (2011).
[3] Stavroulakis P and Stamp M, Handbook of Information and Communication Security, Springer, Germany, p35, (2010).
[4] Yalcin S B O, Radio Frequency Identification: Security and Privacy Issues, Springer, Germany, p 3- 11,(2010).
[5] Tipton H F and Krause M, Information Security Management Handbook, CRC Press, USA, p 1064-1065, (2007).
[6] http://www.thingmagic.com/rfid-security-issues, RFID Security issue-Generation2 Security Executive Summary
[7] Avinash kak, Elliptic curve cryptography and Digital Rights Management, Lecture note on Computer and Network Security, Feb. 26, 2013.