Transaction security in RFID Credit Card by Polynomial Arithmetic along with Euclidean Parameters

Rohit Sharma[#1], Dr. Anuj Kumar Agarwal[#2], Dr. P.K. Singh[#3],
Research scholar (School of Electronics and Communication), Teerthanker Mahaveer University
Associate Professor, Teerthanker Mahaveer University
Professor, IIMT Engineering College, Meerut

Abstract **—The utilization of Radio Frequency Identification (RFID) innovation is becoming quickly crosswise over a wide range of commercial enterprises. Engineers apply the innovation not just in conventional applications, for example, resource or stock following, additionally in security administrations, electronic travel papers and RFID-inserted card. Be that as it may, RFID innovation additionally raises various concerns in regards to protection, security and law requirement. In the same way as other advances, ease Radio Frequency Identification (RFID) frameworks will get to be pervasive in our everyday lives when fastened to regular shopper things as "keen marks". While yielding extraordinary efficiency picks up, RFID frameworks may make new dangers to the security and protection of people or associations. For securing RFID exchange, the utilization of cryptographic calculation is on top. Be that as it may, these calculations are fragmented without the utilization of math. In this paper I will demonstrate how polynomial number-crunching and Euclidean parameters came to assume a important part for exchange security. Planning secure and proficient multivariate key cryptosystem keeps on being a testing territory of examination as of late. In this paper we introduce another technique for outlining effective multivariate key cryptosystem by defeating all the known assaults.**

Key words: - RFID Credit Card, Transaction Security, Polynomial Arithmetic, Euclidean Parameters

1. INTRODUCTION

RFID frameworks comprise of radio frequency (RF) tags, or transponders, and RF tag readers, or handsets. Tag readers question tags for their substance by a RF signal. Tags react by transmitting back occupant information, regularly including a remarkable serial number. RFID tags have a few noteworthy focal points over optical barcode system [1]. Tag information may be read consequently: without viewable pathway, through non leading materials, for example, paper or cardboard, at a rate of a few hundred tags for each second, and from a scope of a few meters. Since tags regularly are a silicon-based microchip, usefulness past straightforward recognizable proof may be joined into the configuration. This usefulness may extend from coordinated sensors, to peruse/compose capacity, to supporting encryption and access control [2].

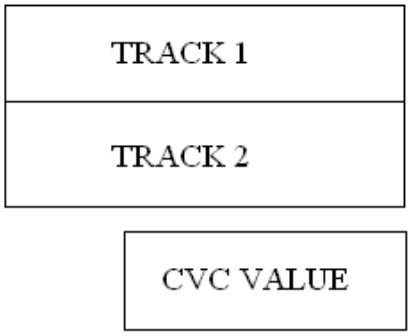

FIG 1: RFID credit card data format

RFID Card are developing in prominence in light of the fact that they allow contactless installment exchanges which are quick, simple, can be more solid than magstripe exchanges, and require just physical vicinity (instead of physical contact) between the Card and the reader. These same elements, in any case, are likewise the premise for our worry about security and protection vulnerabilities [3]. Customary Card oblige that an element have visual get to or direct physical contact keeping in mind the end goal to get data from the card, for example, the cardholder's name and the Card number.

To finish the exchange, RFID card utilize an information design, which contain CVC value, Track 1 and Track 2 data. CVC value is a card verification code, and track data contains the data about the card holder.

For our cryptosystem, CVC value should not be imprinted on the card (must be covered up inside the card). Further Track 1 and Track 2 data will likewise be the piece of exchange as demonstrated in fig 1. In this paper, we performed Polynomial Arithmetic alongside Euclidean operation on RFID card information configuration to make exchange secured. The upside of the calculation is that just couple of Euclidean parameters will be sending to the reader at the spot of complete figure test [10].

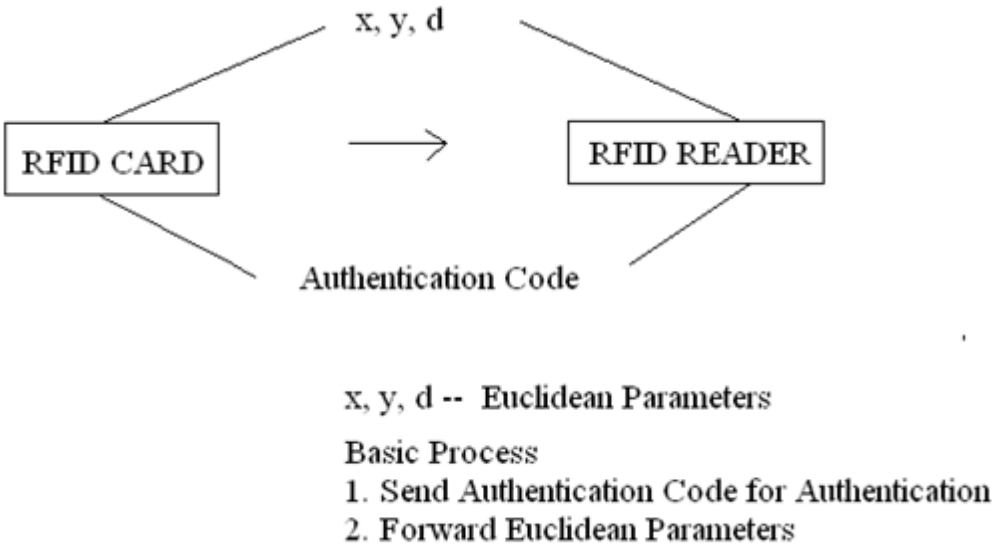

Fig 2 – Proposed transaction model

X, y and d are the Euclidean parameters that created by a numerical procedure. Initial a authentication code must be transmitting to the reader. Further exchange procedure will be begin after the authentication. Reader need to concentrate the plainest or data by the got Euclidean parameters.

2. CRYPTOSYSTEM

Cryptography is utilized as a part of e-trade for validation and secure correspondence. The most broadly utilized cryptosystems RSA and ECC (elliptic curve cryptosystems) are taking into account the issue of whole number factorization and discrete logarithm individually [3] [4].

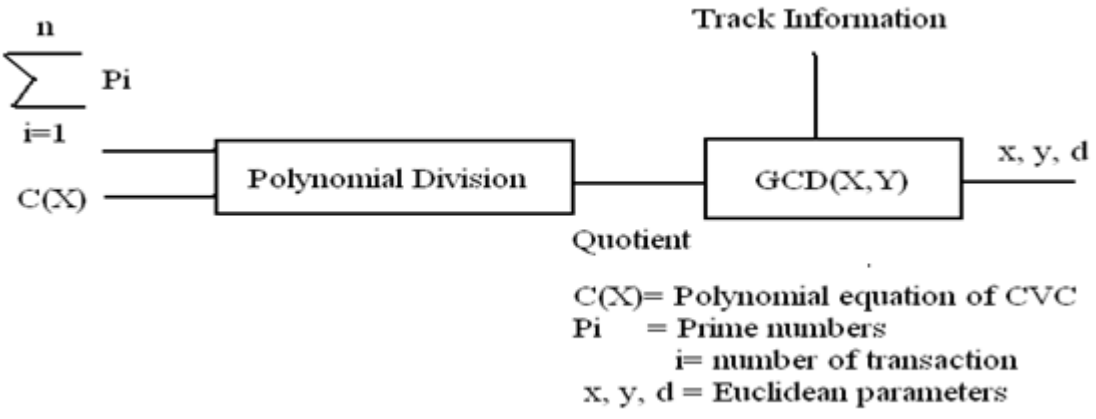

Fig 3– Cryptosystem Model

To expand the intricacy and enhance the security, we performed polynomial number juggling operation between the card CVC value (to be covered up inside the card) and "prime numbers" produced by prime number generator.

2.1 Polynomial division

Polynomial division must be performed between polynomial mathematical statement of CVC value and prime number. Further for Euclidean parameters, the quotient and track data will be utilized as information for Greatest Common Divisor.

Note-1 $\sum_{i=1}^{n} Pi = P(X)$ ---------- (1)

{Order of P(X) must be greater than the order of C(X)}

{Output of prime generator must be increased by one prime number after each transaction}

P(X) = Polynomial Equation for Prime Number

C(X) = Polynomial Equation for card CVC value

P= prime numbers

i= number of transaction

Note 2

GCD(X, Y) ---------- (2)

{One of the largest values from "track information and quotient" will be appointed as X}

2.2 Key generation

A polynomial of degree (integer $n \geq 0$) is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} \pm - - \mp a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

where the a_i are elements of some designated set of numbers s, called the **coefficient set**, and $a_n \neq 0$.We say that such polynomials are defined over the coefficient set [8]. When polynomial arithmetic is performed on polynomials over a field, then division is possible. Let us consider those polynomials in which the coefficients are elements of some field F; we refer to this as a polynomial over the field F. In the last formula, we treat a_i as zero. First we need the value of C(X) and P(X) to perform polynomial division operation [11] [5].

Let the decimal value of CVC is = 25

The polynomial expression for given CVC value

$C(X) = X^4 + X^3 + 1$ ---------- (3)

Polynomial equation can be produce by decimal esteem as given in illustration below.

Illustration: - When representing CRC polynomials, each term maps to one bit. Furthermore, the highest order term is implicit and is omitted. So breaking down your two examples:

1 + x + x^3 = *1101=13*

1 + x + x^2 + x^3 + x^6 + x^7 = *1111001=121*

{Equation Order of P(X) must be greater than of C(X)} --from equation (2).

As the order of C(X) are four X^4. The order for P(X) must be greater than of C(X). Seven is the prime number which satisfying this condition. This case is considering for first transaction. For the second transaction, the prime number will be 11. This process will change the quotient and x, y, and d after each transaction.

$$\sum_{i=1}^{n} Pi \quad i = 1, 2, 3, 4 \ldots\ldots n$$

The polynomial expression for

$$P(X) = X^p + X^{p-1} + X^{p-2} + X^{p-3} + X^{p-5} \pm - - - - + X^{p-p}$$

For P=7

$$P(X) = X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 - - - - - - (4)$$

For the value of quotient, C(X) and P(X) assigned as divisor and dividend.

$$P(X) \Big/ C(X) = \frac{X^7+X^6+X^5+X^4+X^3+X^2+X+1}{X^4+X^3+1} \quad \text{--------} \quad \textit{- (5)}$$

Output quotient from equation number (5)

$B(X) = X^3 + X$ ---------- *(6)*

As a rule, when polynomial division performed, it additionally gives a remainder portion. In our procedure or model, there have no need of remaining portion. Just quotient will be the part of next level operation.

3. ENCRYPTION

To execute the estimation of quotient, we performed polynomial division in between of C(X) and P(X). We are utilizing this quotient esteem as the key for encryption. As the estimation of P(X) will be change after every transaction, result key will likewise be change. By changing the estimation of key after every exchange will enhance the security of model.

For encryption, we need to perform most prominent greatest common divisor between quotient (key) and track value.

We can extend the analogy between polynomial arithmetic over a field and integer arithmetic by defining the greatest common divisor as follows. The polynomial G(X) is said to be the greatest common divisor of A(X) and B(X) if the following are true [12].

1. G(X) divides both A(X) and B(X).
2. Any divisor of A(X) and B(X) is a divisor of G(X).

An equivalent definition is the following: GCD [A(X), B(X)] is the polynomial of maximum degree that divides both A(X) and B(X). We can adapt the Euclidean algorithm to compute the greatest common divisor of two polynomials [6]. The equation for GCD can be written as;

$$gcd[a, b] = gcd[b, a \bmod b] \quad \text{--------} \quad (7)$$

According to equation no (6), B(X) $=X^3 + X$, this expression can be write in the form of decimal by CRC polynomial method.

$$B(X) = X^3 + X = 10$$

Let us assume that the polynomial equation for track data is

$$A(X) = x^3 + x^2 + x + 1\text{----------} \quad (8)$$

According to CRC polynomial method

$$A(X) = x^3 + x^2 + x + 1 = 15$$

GCD expression for A(X) and B(X)- [a=15][b=10]

gcd[15, 10]= gcd[10, 15 mod 10]

(a) 15 =1x10+5 gcd [10, 5]

(b) 10 =2x5 +0 gcd[5, 0]

Therefore gcd[15, 10]=d=5

For given integers a and b, we extend the Euclidean algorithm to calculate two additional integers x and y that satisfy the following equation [9] [7].

$$ax + by = d = gcd(a, b) \quad \text{----------} \quad (9)$$

Put the values of a, b and d in equation (9)

$$15x+10y=5$$

Now we just repeat:

$$gcd[15, 10] = gcd\ [10, 5]$$

therefore

$$15 =1x10+5$$

$$5=15-(1x10) \quad \text{-----} \quad (10)$$

From step (a), we see that 10=15-5, substituting into equation (10), we get

$$5=15-1x\ (15-5)$$

$$5= -15+2x10 \quad \text{----} \quad (11)$$

By comparing equation (10) & (11), we have [x= -1] [y=2] [d=5].

From the above arrangement, we have computed all Euclidean parameter [x, y, d].We utilized x, y and d as the transmitting code for our security model. After the authentication transform, these parameters help the receiver to concentrate about the track data. It is not simple for adversary to execute the estimation of "a" and "b" for the given x, y, and d. since we can have boundless quantities of mix of "a" and "b" for the same estimation of x, y and d.

As we realize that, adjustment in yield of prime generator after every exchange will likewise change the estimation of quotient B(X). All the while the estimation of x, y and d will likewise be change.

4. DECRYPTION

Here authentication is additionally a piece of decryption. In the first place transmitter needs to finish the authentication of RFID card with the assistance of authentication code. Transmitter will forward the verification code to the base station. After the complete confirmation, base station sends the CVC value of card and prime number for concern transaction. RFID reader will create the polynomial type of CVC and concern prime number to execute the estimation of Quotient B(X).

$$C(X) = X^4 + X^3 + 1$$

$$\sum_{i=1}^{n} Pi \quad i = 1, 2, 3, 4\ldots\ldots n$$

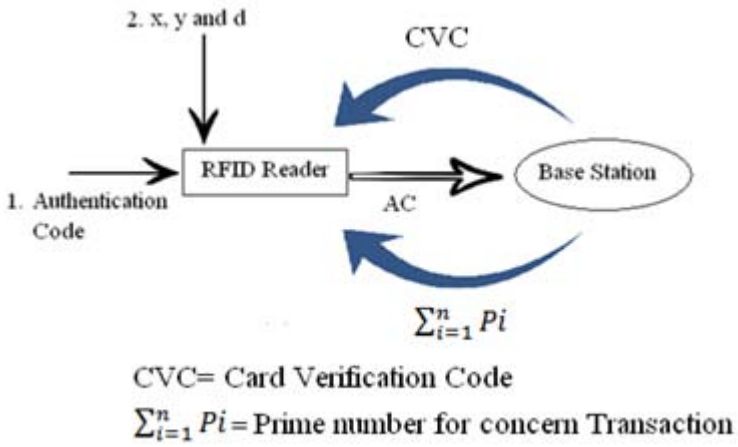

Fig -4 Decryption Model

Polynomial Form Of Concern Prime Number

$$P(X) = X^p + X^{p-1} + X^{p-2} + X^{p-3} + X^{p-5} \pm - - - - + X^{p-p}$$

$$P(X) = X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

Value of Quotient

$$P(X) \Big/ C(X) = \frac{X^7+X^6+X^5+X^4+X^3+X^2+X+1}{X^4+X^3+1}$$

$$B(X) = X^3 + X$$

This expression can be write in the form of decimal by CRC polynomial method.

$$B(X) = X^3 + X = 10$$

From the above arrangement, we have discovered the estimation of "b". We have as of now got the estimation of x, y and d, from the transmitter. By comparing these value with equation

$$ax + by = d = gcd(a, b)$$

$$b=10, x= -1, y=2, d=5$$

Therefore

$$a(-1)+10(2)=5$$

Hence the value of track information $a=15$

This is a decimal value of track information. By CRC polynomial method

$$a=15 = 1111$$

Polynomial equation for track information is

$$A(X) = x^3 + x^2 + x + 1 \quad \text{------- (12)}$$

Executed information is same as track information of RFID card. In complete transaction process, we have not shared any information about the track value and key. Only few Euclidean parameters have shared between transmitter and receiver. It is not easy for adversary to execute the value of “a” and “b” by x, y, and d parameters, because we can have infinite numbers of combination of “a” and “b” for the same value of x, y and d.

5. CONCLUSION

A few different measures may be taken to fortify RFID frameworks. To begin with, RFID-empowered situations ought to be outfitted with gadgets to distinguished unapproved read endeavors or transmissions on label frequencies. Because of the solid sign quality in the forward channel, identifying read endeavors is genuinely straightforward. Sending read identifiers aides recognize unapproved read demands or endeavors to stick label working frequencies. Another measure to recognize refusal of administration is to outline labels which "shout" when slaughtered, maybe by transmitting a sign more than a held recurrence. RFID improved "savvy racks" may be intended to recognize the evacuation of things, unapproved read endeavors or the executing of labels.

This proposed model is concern with the exchange security between RFID card and reader. To enhance the security, we abstain from sharing the data in the middle of reader and card. Reader will execute the data by utilizing polynomial number juggling alongside Euclidean parameters. In our cryptosystem the key is the mix of some polynomial division, prime numbers, CVC esteem and greatest common divisor.

The yield of prime number generator will change after every exchange; implies for every single exchange, we have an alternate estimation of key. This property of our cryptosystem will befuddle the adversary. Also, other property of our cryptosystem is; just couple of Euclidean parameters have shared in the middle of transmitter and beneficiary. It is not simple for adversary to execute the estimation of "a" and "b" by x, y, and d parameters, in light of the fact that we can have endless quantities of mix of "a" and "b" for the same estimation of x, y and d.

REFERENCE

[1] M. Meingast, J. King, D.K. Mulligan, “Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport “ IEEE International Conference on RFID, pp. 7-14, March 2007.

[2] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, and T.-C. Chen, “An Improvement on RFID Authentication Protocol with Privacy Protection” Convergence and Hybrid Information Technology, ICCIT, vol. 2, pp. 569-573, Nov. 2008.

[3] T. Phillips, T. Karygiannis, and R. Kuhn, “Security standards for the RFID market” Security & Privacy , IEEE, vol. 3, no. 6, pp. 85-89, Nov.-Dec. 2005.

[4] C. Floerkemeier and S. Sarma, “An Overview of RFID System Interfaces and Reader Protocols” IEEE International Conference on RFID, pp. 232-240, April 2008.

[5] L.E. Dickson. The analytic representation of substitution on a power of a prime number of letters with a discussion of the linear group. Ann. of Math. 11, 65-120.

[6] Peter Shor. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Scientific Computing. 26 (1997), 1484.

[7] R. Lidl and G. L. Mullen. When does a polynomial over a finite field permute the elements of the field? The American Math. Monthly, 95(3), 243-246, 1988.

[8] R. Lidl and G. L. Mullen. When does a polynomial over a finite field permute the elements of the field? II The American Math. Monthly, 100(1), 71-74, 1993.

[9] E.J. Borowski, and J.M. Borwein, The Harper Collins Dictionary of Mathematics, Harper Collins Publishers, New York, 1991.

[10] Rohit Sharma, P.K.Singh “Cryptographically Secure Encryption Model for RFID Credit Card”, in Elixir International Journal of Electronics Engineering, ISSN: 2229-712X,, December 2013.

[11] Peter Borwein and Tamas Erdelyi, Polynomials and Polynomial Inequalities, Springer, New York, 1995.

[12] M. Abramowitz and A. Stegun, Handbook of Mathematical Functions, Dover Publications, New York, 1965.