A Study on Discrete Logarithm Problem in Circulant Matrices

Anu Pius[#1], Senthil Kumar B[*2]

[#]Research Scholar, Department of Mathematics, PRIST University, Thanjavur, India.
[*]Assistant Professor, Department of Mathematics, PRIST University, Thanjavur, India.

Abstract

In public key cryptography, discrete logarithm problem plays a vital part. In this paper we contemplate the discrete logarithm issue in circulant matrices over a limited field.

Keywords – *The discrete logarithm problem, circulant matrices.*

I. INTRODUCTION

A Menezes and Y-H Wu [4] assert that working with the discrete logarithm issue in matrices offers no real change from working with a limited field. Numerous creators, including A.. Mahalanobis [1], rehashed that claim. It is presently a typical learning that for functional purposes, the discrete logarithm issue in non-singular matrices does not merit taking a gander at.

In this note, we give a counterexample to the previously mentioned basic knowledge and demonstrate that matrices over a limited field can be utilized successfully to deliver a quick and secure cryptosystem. This approach can be viewed as working with the **MOR** cryptosystem [2], with limited dimensional vector spaces over a limited field.

In this note, we are managing the discrete logarithm issue in matrices over a limited field, i.e., given a non-singular $\boldsymbol{f} \times \boldsymbol{f}$matrix**P** and **Q**=$\boldsymbol{P^m}$over $\boldsymbol{K_q}$,register the private key $\boldsymbol{m}$; where $\boldsymbol{q}$ is an intensity of a prime $\boldsymbol{p}$. One can without much of a stretch form any cryptosystem that uses the discrete logarithm issue, similar to the Diffie– Hellman key exchange or the ElGamal cryptosystem, utilizing the discrete logarithm issue in matrices. There are numerous perspectives to the security of a cryptosystem. In this paper we will just manage the computational parts of taking care of a discrete logarithm issue.

The center of the Menezes– Wu calculation [4, Algorithm 2] is to register the charecteristic polynomial $\boldsymbol{\lambda_P(y)}$of**P**. The latent values of **P**, which are the zeros of $\boldsymbol{\lambda_P(y)}$have a place with the splitting field of $\boldsymbol{\lambda_P(y)}$.Thezeroes of $\boldsymbol{\lambda_q(y)}$likewise have a place with the same splitting field. At that point to take care of the discrete logarithm issue, one needs to take care of the individual discrete logarithm issues in the latent values and after that utilization of the Chinese remainder hypothesis. The security of the discrete logarithm issue depends on the degree of the extension of the splitting field. Since tackling a discrete logarithm issue relies upon the extent of the field, we can get phenomenal security by taking $\boldsymbol{f}$ expansive (around 20) and pick **P** to such an extent that $\boldsymbol{\lambda_P(y)}$is irreducible. However, all things considered product of matrix turns out to be extremely costly and we are in an ideal situation working with the limited field $\boldsymbol{F_{q^f}}$.This is the contention of Menezes and Wu [4]. In this paper, we manage a specific kind of non-singular matricesi.e the circulant matrices We appear, that for these matrices, squaring is free andmultiplication is simple. At the point when this is the situation, the above contention is never again substantial and we have conceivable outcomes of an effective cryptosystem that is secure with sensible parameters and is quick. Utilizing the broadened Euclidean calculation, registering the inverse of a circulant matrix is simple, that makes a cryptosystem based on circulant matrices fast and secure.

When working with the discrete logarithm issue in matrices, one ought to be watchful of the way that the determinant of a matrix is a multiplicative function to the ground field. This can simply lessen the discrete logarithm issue in matrices to a discrete logarithm issue in the ground field. This can be effectively avoided by

(i) Choose **P**such that determinant of **P**is **1**.

In this note, the Roman numerals (i), (ii)……..,(v), are the set of conditions on the circulant matrix **P.** All matrices are over a limited field.

II. CIRCULANT MATRICES

The reader is reminded that here all fields (is denoted by) are finite with characteristic $\boldsymbol{p}$.

Definition 2.1. Over a field$\boldsymbol{K}$, a $\boldsymbol{f} \times \boldsymbol{f}$matrix is known as circulant, only if every row excepting first row, is right circular shift of row above. Thus circulant matrix is known by its first row. Similarly, a circulant matrix can also be defined by columns.

Despite the fact that a circulant matrix is a two dimensional, it behaves much like a one dimensional; given by first row or first column. We will mean a circulant matrix **M** with first row$(m_0, m_1, m_2 \,:::::::\, m_{f-1})$by

$$\mathbf{M} = cir\big(m_0, m_1, m_2 \,::::::::::::\, m_{f-1}\big).$$

$$An\ example\ of\quad 5 \times 5\quad matrix\ is$$

$$\begin{bmatrix} m_0 & m_1 & m_2 & m_3 & m_4 \\ m_4 & m_0 & m_1 & m_2 & m_3 \\ m_3 & m_4 & m_0 & m_1 & m_2 \\ m_2 & m_3 & m_4 & m_0 & m_1 \\ m_1 & m_2 & m_3 & m_4 & m_0 \end{bmatrix}$$

It is anything but difficult to see that all the (sub) diagonals of a circulant matrix are steady. This reality proves to be useful. Let $\boldsymbol{A} = \boldsymbol{cir}(\mathbf{0};\ \mathbf{1};\ \mathbf{0};\dots..\mathbf{0})$ *be a* $\boldsymbol{f} \times \boldsymbol{f}$circulant matrix, at that point plainly $\boldsymbol{A^d} = \mathbf{1}$. We can compose $\mathbf{M} = \boldsymbol{m_0 I} + \boldsymbol{m_1 A} + \boldsymbol{m_2 A^2} + \cdots\cdots + \boldsymbol{m_{f-1} A^{f-1}}$One can characterize a representer polynomial relating to the circulant matrix **M**as $\boldsymbol{\varphi_M} = \boldsymbol{m_0 I} + \boldsymbol{m_1 y} + \boldsymbol{m_2 y^2} + \cdots\cdots + \boldsymbol{m_{f-1} y^{f-1}}$This demonstrates thatcirculant shape acommutative ring with respect to matrix multiplication and matrix addition and is isomorphicto (the isomorphism being matrix to representer polynomial)$\frac{\boldsymbol{K}[(\boldsymbol{X})]}{\boldsymbol{y^d}-\mathbf{1}}$, see [7]

A. How to square a circulant matrix?

Let $\boldsymbol{B} =\ cir(b_0, b_1, b_2 \,::::::::::::\, b_{f-1}\ )$be a circulant matrixe over a field of latent**2**. Wedemonstrate that to process B^2we need to compute $b_i{}^2$for each***i***in(0,1,2,3::::::::f-1) Then ***B***=cir($b_{\theta(0)}{}^2, b_{\theta(1)}{}^2, b_{\theta(2)}{}^2$ :::::::: $b_{\theta(f-1)}{}^2$)where $\theta$is a permutation of *(0,1,2,3::::::::.f-1).* This was also observed by Silverman [6,p.180]

Theorem 2.2.*If the characteristic of the field* ***K****is* ***2****, and* ***f****is an odd integer, then squaring a* $\boldsymbol{f} \times \boldsymbol{f}$ *circulant matrix* ***P*** *is same as squaring* ***f****field elements.*

Proof.We utilize the standard technique for matrix multiplication; where one registers the spot result of the i^{th}row with the j^{th}column for the component at the convergence of the i^{th}rowand the j^{th}columnof the product matrix. As we saw before the circulant matrix are shut under multiplication and a circulant matrix is given by its first line. Taking these into account, if the circulant matrix is$\boldsymbol{B} =\ cir(b_0, b_1, b_2 \,::::::::::\, b_{f-1}\ )$we see that the first element of the first row of the product, is the dot product of $(b_0, b_1, b_2 \,::::::::::::\, b_{f-1}\ )$ with the first column$\left[(b_0, b_{f-1}, \,::::::::::\, b_1\ )\right]^T$. The first column can be thought of as the map $a_i \rightarrow a_{-i} mod\ f$ for *i* =*(0; 1; : : : ; . f- 1)*

For each $j$in *[0; 1; 2; : : : ; f–1]*, the map is given by$a_i \rightarrow a_{j-i} mod\ f$Now notice that if $i\ \rightarrow\ j -\ i$ mod f, then $j - i\ \ \rightarrow\ i$mod f. This proves that there are pairs formed in the dot product, which makes it root when working in latent**2**.

The main thing that departures shaping sets, are those $i,$ for which $i = j - imod\ f$.since$f$ is odd, there is an inverse of 2 $modf$ and an interesting answer for i.

It is anything but difficult to see from the above verification, that once an odd number f is settled, one can undoubtedly process the change θ. The calculation of$f$ diverse forces should be possible in parallel.

III. THE DISCRETE LOGARITHM PROBLEM IN CIRCULANT MATRICES

As we saw previously, circulant frameworks can be spoken to in two diverse ways - one as a circulant lattice and different as a component of the ring **R**=$\frac{\boldsymbol{F}[(\boldsymbol{y})]}{\boldsymbol{y^f}-\mathbf{1}}$. In the later case, every component of **R** is a polynomial of degree $\boldsymbol{f} - \mathbf{1}$ in **K** . The polynomial augmentation in **R** should be possible (in parallel) utilizing grid duplication. In the event that lattice increase is utilized to do the polynomial augmentation, at that point there is no compelling reason to do the lessening mod $\boldsymbol{y^d} - \mathbf{1}$

These two representations lead to two different kinds of attack to the discrete logarithm problem:

(a) The discrete logarithm problem in matrices.

(b) The discrete logarithm problem in **R**.

A. The discrete logarithm problem in matrices

As we comprehended from Menezes and Wu [4], understanding the discrete logarithm problem in non-solitary networks is attached to the biggest level of the unchangeable component of the trademark polynomial. The most ideal situation happens when the trademark polynomial is final. For circulant networks this isn't the situation.

It is anything but difficult to see that the line aggregate, entirety of the considerable number of components consecutively, is consistent in a circulant network. This influences the column to whole an eigenvalue of the framework. Since this eigenvalue has a place with the ground field, the best way to get away from a discrete logarithm issue in the ground field is to make this eigenvalue, i.e., the line aggregate **1**. So the circulant framework **P**ought to be picked with the accompanying properties:

(ii) The matrix **P**has row-sum ***1.***

(iii) The polynomial $\frac{\chi_A}{y-1}$is irreducible.

In the above case the security of the discrete logarithm problem in ***P***is similar to that of the discrete logarithm problem in the finite field $\boldsymbol{K_{q^f}} — \mathbf{1}$

B. The discrete logarithm problem in$\frac{K_q[(y)]}{y^d-1}$

Notice that $\frac{K_q[(y)]}{y^d-1} \cong \frac{K_q[(y)]}{y-1} \times \frac{K_q[(y)]}{\Psi(y)}$

Where$\boldsymbol{\Psi(y)} = \frac{y^d-1}{y-1}$and $gcd(d,q) = 1$. So the discrete logarithm problem in$\frac{F_q[(y)]}{y^d-1}$reduces in to two different discrete logarithm problems, one in the field $\boldsymbol{K_q}$and other in the ring$\frac{K_q[(y)]}{\Psi(y)}$**.**The matrix *P*can be chosen in such a way thatthe representer polynomial $\boldsymbol{\lambda_P(y)}mod\ (y-1)$*is* either ***0* or *1***and hence reveals noinformation about the private key ***m***. Note that:$\boldsymbol{\lambda_P(y)}mod\ (y-1)$is **0** or **1**isequivalent to the row-sum being **0 or 1**respectively. If the row-sum is zero thecirculant matrix is singular; on the other hand if we assume the row-sum to be **1**(condition (ii)) then automatically $\boldsymbol{\lambda_P(y)}mod\ (y-1) = 1$. $\boldsymbol{\Psi(y)}$is irreducible, then the discrete logarithm problem is a discrete logarithmproblem in the field $\frac{K_q[(y)]}{\Psi(y)}$. Hence the security of the discrete logarithm problem isthe same as that of the discrete logarithm problem in $\boldsymbol{K_{q^f}} —$ **1**.The question remains, when is$\boldsymbol{\Psi\ (y)}$ ***is*** irreducible? We know that [8, Theorem2.45], $\boldsymbol{y^d - 1} = \prod^{f}{}^{1}/_{f}\,\boldsymbol{\lambda_{d_1}(y)}$ where $\boldsymbol{\lambda_k(y)}$ is the $\boldsymbol{k^{th}}$cyclotomic polynomial. It follows that if *d* is prime, then $\boldsymbol{\Psi(y)} = \boldsymbol{\lambda_d(y)}$Then the question reduces to, when is the $\boldsymbol{d^{th}}$cyclotomic polynomial irreducible, for a prime ***d* ?** It is known [8, Theorem 2.47] that the$\boldsymbol{d^{th}}$cyclotomic polynomial $\boldsymbol{\lambda_d(y)}$is irreducible over $\boldsymbol{K_q}$if and only if ***q***is primitive mod ***f.***

We summarize the requirements on **P,** such that the discrete logarithm problem is as secure as the discrete logarithm problem in $\boldsymbol{K_{q^f}} — \mathbf{1}$

(iv) The integer ***f*** is prime.

(v) ***q***is primitive mod ***f.***

IV. USE THE DISCRETE LOGARITHM PROBLEM WITH $f \times f$CIRCULANT MATRICES

A snappy response to the above inquiry is that augmentation in **R**, which is isomorphic as a variable based math to $\boldsymbol{f \times f}$circulant networks over $\boldsymbol{K_q}$ can be substantially speedier!

In executing the exponentiation in any gathering, the best known strategy is the popular square-and-increase calculation. Utilizing typical premise [8, Definition 2.32], in a limited field of latent**2**, squaring is shoddy; it is only a cyclic move of the bits. For our situation, utilizing Theorem 2.2, it is comparable. What about augmentation?

The subtle element of the many-sided quality of augmentation is bit included, yet very much contemplated. So we can avoid the points of interest here, and allude the per user to [3, 6]. The multifaceted nature of duplication in a limited field reliesupon the decision of premise. In the event that one uses an ordinary premise, the minimum unpredictability is achieved by an ideal typical premise [3, Chapter 5]. Inthat case, the intricacy of multiplication in the field $\mathbf{K_{qf}}$ is $\mathbf{2f-1}$ [6, Theorem 5.1], where $\boldsymbol{K_q}$ is a field of latent**2**. On account of **R**, that intricacy diminishes to $\boldsymbol{f}$ [6, Example 3]. In **R** we get security of $\boldsymbol{K_{qf}}$**— 1**.So there is an undeniable preferred standpoint of working with the circulant frameworks than with a limited field – the many-sided quality of figuring the exponentiation decreases to half with just a single additional piece. Ultimately, one can utilize the stretched out Euclidean calculation to figure the reverse of a representer polynomial in **R**. In an ElGamal like cryptosystem, one needs to figure that opposite. This will make decoding quick.

V. CONCLUSIONS

In this paper we contemplate the discrete logarithm issue in the ring of circulant matrices. On the off chance that the matrices are of size $\boldsymbol{f}$ then we saw that under reasonable conditions, the discrete logarithm issue is as secure as the discrete logarithm issue in $\boldsymbol{K_{qf}}$**— 1.** Since increasing circulant matrix is less demanding, the discrete logarithm problem in circulant matrix is superior to the discrete logarithm issue in a limited field $\boldsymbol{K_{qf}}$**— 1.**

There isn't much history of taking a gander at matrices for better (more secure) discrete logarithm issue. In this note the isomorphism of the circulant matrix with the variable based math **R** has diminished the focal issue of this work to that of a usage of finite fields. An approach to take a gander at **R** and this investigation of the discrete logarithm issue in **R** is, the finite field $\boldsymbol{K_{qf}}$**— 1.**is installed in **R**. In spite of the fact that this is a legitimate method for taking a gander at the current circumstance, it isn't the entire view. For instance, the issue with row sum entirety won't be straightforward, except if one takes a gander at matrix. Additionally this opens up the likelihood that there can be different matrices, designed matrices or a subgroup of the circulant matrices, other than the one with row total **1**; in which we can improve the discrete logarithm issue.

REFERENCES

[1] A. Mahalanobis, A note on using finite non-abelian p-groups in the MOR cryptosystem, http://arxiv.org/abs/cs/0702095.

[2] A. Mahalanobis, A simple generalization of the ElGamal cryptosystem to non abeliangroups II, http://arxiv.org/abs/0706.3305.

[3] A. J. Menezes (ed.), Aplications of Finite Fields, Kluwer, 1993.

[4] A. Menezes and Y.-H. Wu, The discrete logarithm problem inGL.(n; q),Ars Comb.**47** (1997), 23–32.

[5] J.H. Silverman, Fast multiplication in finite fields GF.2N/, in: CHES'99, LNCS 1717, pp. 122–134, 1999.

[6] J.H. SilvermanRings with low multiplicative complexity, Finite Fields and their Appl. **6** (2000), 175–191.

[7] P. J. Davis, Circulant Matrices, Chelsea, 1994.

[8] R. Lidl and H. Niederreiter, Finite Fields, 2nd ed., Cambridge University Press, 1997.

[9] W.C.Waterhouse, Circulant-StyleMatrices closed undermultiplication, Lin. Multilin.Algebra**18** (1985), 197–206.