International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017(O)
Volume 1 Issue 2 (August 2014) ISSN: 2349-7009 (P)
http://ijiris.com

ANALYSE AND IMPLEMENT OF CRYPTOGRAPHY WITH HIGH SECURITY USING QUATERNION

U. Vijay Sankar
Ph.D., Research Scholar/CSE
PRIST University, INDIA.

Dr.A.Arul Lawrence Selvakumar
Professor& Head/CSE
RGIT, Bangalore, INDIA

Abstract- Cryptography is the study of message secrecy. In modern times, it has become a branch of information theory, as the mathematical study of information and especially its transmission from place to place. It is a central part of several fields: information security and related issues, particularly, authentication, and access control. Cryptography also contributes to computer science, particularly in the techniques used in computer and network security for such things as access control and information confidentiality. The objective of this research work is to analyze and implement highly secure cryptography scheme using the properties of quaternion Farey fractions. More recent approaches to provable security abandon the ideal of perfect secrecy and the assumption of unbounded computing power. The computational complexity of algorithms is taken into account. A complex security algorithm can be devised using the immense applications of the number theory; one such application is using the properties of quaternion. One of the most important applications of modern mathematics in our current times is the use of cryptography in securing our network systems of communications. The backbone of the RSA system is Fermat's Little Theorem in number theory

Keywords- **Number Theory, Quaternion, Farey Fractions, Cryptography**

1. INTRODUCTION

Cryptography is the study of message secrecy. In modern times, it has become a branch of information theory, as the mathematical study of information and especially its transmission from place to place. The noted cryptographer Ron Rivest has observed that "cryptography is about communication in the presence of adversaries", which neatly captures one of its unique aspects as a branch of engineering, and differences from, for instance, pure mathematics. It is a central part of several fields: information security and related issues, particularly, authentication, and access control. One of cryptography's primary purposes is hiding the meaning of messages, but not usually their existence. Cryptography also contributes to computer science, particularly in the techniques used in computer and network security for such things as access control and information confidentiality. Cryptography is also used in many applications encountered in everyday life; examples include security of ATM cards, computer passwords, and electronic commerce all depend on cryptography.

II. OBJECTIVES

The availability of high speed digital hardware has made the implementation of high grade cryptographic devices possible, so that they find their application in commercial fields such as remote cash dispensers and computer terminals. In turn, such applications create a need for few types of cryptographic system which minimizes the necessity of secure key distribution channels and supply the equivalent of written signature. At the same time theoretical development in information theory and computer science show promise of providing provably secure cryptosystem.

The objective of this research work is to analyze and implement highly secure cryptography scheme using the properties of quaternion Farey fractions. Use of quaternion has been reported in computer graphics, control theory and signal processing. For example, spacecraft attitude control systems are reported to be commanded in terms of quaternion. Immense applications of number theory is used in this work to device a cryptography model that provides high level of confusion and thereby create more diffusion (desirable effect). The independent co-efficient of the super complex number that has a free rotation in a three dimensional space is taken as the parameter. A novel feature of this work is that the encrypted text can be represented in numbers instead of the conventional alphabets. Also, the number of secondary keys (which are used for transforming the given plain text into cipher text) that can be generated using the primary key is large and hence more is the confusion. All these effects, prevents the hackers from breaking the encryption using the conventional approach of letter frequencies.

III. NEED OF PROVABLY SECURE CRYPTOSYSTEMS

Rapid growths of electronic communication leads to the issues like information security (securing the secrets) are of increasing practical importance. Message exchanged worldwide are publicly available through the computer networks, which must be confidential and protected against malicious users.

More recent approaches to provable security abandon the ideal of perfect secrecy and the assumption of unbounded computing power. The computational complexity of algorithms is taken into account. Only the attacks that are feasible in practice are considered. Feasible means that attacks can be performed by efficient algorithms. Even to secure the information's from the efficient attack, complex securing techniques should be devised so as to create more confusion for the hackers to break the security. A complex security algorithm can be devised using the immense applications of the number theory; one such application is using the properties of quaternion. This research work gives the methodology to secure the information through the properties and applications of hyper complex numbers called Quaternion.

3.1 ROLE OF NUMBER THEORY IN CRYPTOGRAPHY

Number theory is the branch of pure mathematics concerned with the properties of numbers in general, and integers in particular, as well as the wider classes of problems that arise from their study. Number theory may be subdivided into several fields, according to the methods used and the type of questions investigated The term "arithmetic" is also used to refer to number theory. This is a somewhat older term, which is no longer as popular as it once was. Number theory used to be called *the higher arithmetic*, but this too is dropping out of use. Nevertheless, it still shows up in the names of mathematical fields.

Number systems plays very important role in the field of cryptography. In addition to elementary number theory, increasing use has been made of algebraic number theory and arithmetic algebraic geometry. Cryptosystems is also make use arithmetic geometry where elliptic factorization uses elliptic and hyper- elliptic curves.| Some of the most important applications of number theory on cryptosystems are number *field sieves method* for factoring large integers and the Q*uaternion* which gives multifold security in the cryptography. The area of the research is to use the applications of the quaternion to secure the secrets using the concept called cryptography.

One of the most important applications of modern mathematics in our current times is the use of cryptography in securing our network systems of communications. Although the idea dates back to ancient times only after the appearance of the RSA system can one start to build a really safe way to transmit data over long distances via he internet. The backbone of the RSA system is Fermat's Little Theorem in number theory

3.2 PROPERTIES OF QUATERNION

Quaternions were discovered by **William Rowan Hamilton** of Ireland in 1843. Hamilton was looking for ways of extending complex numbers (which can be viewed as points on a plane) to higher spatial dimensions. He could not do so for 3-dimensions, but 4-dimensions produce quaternion. According to a story he told, he was out walking one day with his wife when the solution in the form of equation $i^2 = j^2 = k^2 = ijk = -1$ suddenly occurred to him; he then promptly carved this equation into the side of nearby Brougham bridge (now called Broom Bridge) in Dublin.

This involved abandoning the commutative law, a radical step for the time. Vector algebra and matrices were still in the future. Not only this, but Hamilton had in a sense invented the cross and dot products of vector algebra. Hamilton also described a quaternion as an ordered four-element multiple of real numbers, and described the first element as the 'scalar' part, and the remaining three as the 'vector' part. If two quaternion with zero scalar parts are multiplied, the scalar part of the product is the negative of the dot product of the vector parts, while the vector part of the product is the cross product. But the significance of these was still to be discovered.

Hamilton proceeded to popularize quaternion with several books, the last of which, *Elements of Quaternion's*, had 800 pages and was published shortly after his death. Even by this time there was controversy about the use of quaternion. Some of Hamilton's supporters vociferously opposed the growing fields of vector algebra and vector calculus (developed by ***Oliver Heaviside*** and ***Willard Gibbs*** among others), maintaining that quaternion provided a superior notation. While this is debatable in three dimensions, quaternion cannot be used in other dimensions (though extensions like octonions and ***Clifford algebras*** may be more applicable). In any case, vector notation had nearly universally replaced quaternion in science and engineering by the mid-20th century.

Today, quaternion's see use in computer graphics, control theory, signal processing and orbital mechanics, mainly for representing rotations/orientations in three dimensions. For example, it is common for spacecraft attitude-control systems to be commanded in terms of quaternion, which are also used to telemeter their current attitude. The rationale is that combining many quaternion transformations is more numerically stable than combining many matrix transformations
Hamilton used *addition* symbol in the Cartesian representation of a complex number

Let us consider the complex number **a+ib**, which is somewhat misleading, since a real and purely imaginary number cannot be directly added together arithmetically.
A more suitable representation might be as an ***ordered pair*** of real numbers
(a,b),
together with a set of manipulation rules that define how to perform operations like addition and multiplication of these pairs.

3.2.1 OPERATIONS ON QUATERNION

- **Arithmetic operations on Quaternion:**

Addition and subtraction of quaternion proceed component-wise:

$$q = (a,\ b,\ c,\ d) = a + ib + jc + kd,$$
$$p = (x,\ y,\ z,\ w) = x + iy + jz + kw,$$

$$q+p = (a+x,b+y,c+z,d+w) = (a+x) +i(b+y) +j(c+z) +k(d+w),$$
$$q-p = (a-x,b-y,c-z,d-w) = (a-x) +i(b-y) +j(c-z) +k(d-w).$$

- **Multiplication by a Real Number**

The multiplication of quaternion's could be deduced from the following multiplication table:

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

These products form the quaternion group of order 8, Q_8.
Multiplication by a real number x has the effect of scaling each component:
$Q = (a, b, c, d) = a + ib + jc + kd,$
$xq = qx = (xa,xb,xc,xd) = xa +i(xb) +j(xc) +k(xd).$

- **Alternative Representation**

In addition to the Cartesian and quadruple representations

$$q = (a,b,c,d) = a+ib+jc+kd,$$

there is an alternative way to represent a quaternion. We separate the real part **a** from the purely imaginary (or *pure*) part **ib+jc+kd.** It turns out that it is natural to represent the pure part by the vector (b,c,d), since (as we shall see) i,j, and k act like orthogonal unit vectors. We put $q = (a,\mathbf{v})$, where $\mathbf{v}=(b,c,d)$.

Then

$$q+p = (a,\mathbf{v}) + (x,\mathbf{u}) = (a+x,\mathbf{v}+\mathbf{u}),$$

where `+' represents the usual operations of real, respectively vector, addition.

❖ **Conjugation and Absolute Value**

The conjugate is given by

q = (a, b, c, d) = a+ib+jc+kd,
q^* = (a,-b,-c,-d) = a-ib-jc-kd.

Or, in the alternative representation,

q = (a,**v**),
q^* = (a,-**v**).

The absolute value is given by extending Pythagoras's theorem to four dimensions, and is equal to the square root of the product of a number and its conjugate:

$|\mathbf{q}| = \mathbf{SQRT(a^2+b^2+c^2+d^2) = SQRT(qq^*).}$

❖ **Multiplication of Quaternion**

q = (a,b,c,d),
p = (x,y,z,w),
qp
= (a+ib+jc+kd)(x+iy+jz+kw)
= a(x+iy+jz+kw)
+ib(x+iy+jz+kw)
+jc(x+iy+jz+kw)
+kd(x+iy+jz+kw)

= ax+iay+jaz+kaw
+ibx -by+kbz-jbw
+jcx-kcy -cz+icw
+kdx+jdy-idz -dw

= (ax-by-cz-dw,
ay+bx+cw-dz,
az-bw+cx+dy,
aw+bz-cy+dx)

This can be re-written much more conveniently using the alternative representation of real number and 3-vector as follows:

p = (x,**u**), q(a,**v**)
qp = (ax-**v**.**u**, a**u**+x**v** + **v**X**u**).

[Where X is the vector cross-product.] With this representation, it becomes obvious that quaternion multiplication is not commutative, since the cross-product of the vectors is not commutative.

❖ Multiplying Quaternion

Since a unit quaternion represents an orientation in 3D space, the multiplication of two unit quaternion will result in another unit quaternion that represents the combined rotation. Amazing, but it's true. Given two unit quaternion

Q1=(w1, x1, y1, z1);
Q2=(w2, x2, y2, z2);

A combined rotation of unit two quaternion is achieved by

Q1 * Q2 =(w1.w2 - v1.v2, w1.v2 + w2.v1 + v1*v2)

where v1= (x1, y1, z1)
v2 = (x2, y2, z2)

and both . and * are the standard vector dot and cross product.

However an optimization can be made by rearranging the terms to produce

w=w1w2 - x1x2 - y1y2 - z1z2
x = w1x2 + x1w2 + y1z2 - z1y2
y = w1y2 + y1w2 + z1x2 - x1z2
z = w1z2 + z1w2 + x1y2 - y1x2

Of course, the resultant unit quaternion can be converted to other representations just like the two original unit quaternion. This is the real beauty of quaternion - the multiplication of two unit quaternion in 4D space solves gimbal lock because the unit quaternion lie on a sphere. Be aware that the order of multiplication is important. Quaternion multiplication is not commutative, meaning

q1 * q2 does not equal q2 * q1

❖ **Squaring**

Note that the above rule for multiplication means that we have

$q^2 = (a^2 - \mathbf{v}.\mathbf{v}, 2a\mathbf{v})$

Because the cross-product of any vector with itself is zero.

❖ **Inverse and Division**

Recall that $qq^* = q^*q = |q|^2$,

thus $(qq^*)/(|q|^2) = (q^*q)/(|q|^2) = 1$,

giving the (both left and right) inverse of `q` to be $q^{-1}=q^*/(|q|^2)$.

We can use the inverse to define division. However, one has to be careful what is meant by division. We could define either

$q/p = qp^{-1}$, or $q/p = p^{-1}q$.

❖ **Real and Complex Subspaces**

Quaternion's of the form

(a,0,0,0) = a

are just real numbers. Similarly, quaternions of any of the three following forms:

(a,b,0,0) = a+ib,

(a,0,c,0) = a+jc,

(a,0,0,d) = a+kd.

are just equivalent complex numbers, and are closed under the operations of addition and multiplication.Pure quaternion (`q=ib+jc+kd`), however, are not closed since the dot product of the vector parts contributes to the real part of a product.

3.2.2 EXTENDING THE COMPLEX NUMBER

It seems natural, then, to speculate whether there might be some form of extended number system whose numbers may be interpreted as points in three-dimensional space, with a corresponding representation as number *triples*.

The simplest such extension would seem to be numbers of the form

a+ib+jc = (a,b,c),

where `i` and `j` are distinct, independent square roots of **`-1`**. Hamilton attempted to define operations on these triples that were analogous to those on complex numbers. Addition and subtraction are naturally implemented as component-wise operations on the three real numbers. Multiplication, however, presented a problem.

For complex numbers, the effect of multiplication is most easily appreciated when they are represented in *polar* form, by a length **`r`** (the `modulus') and an angle `theta` (the `argument') which define a point in the plane. If **`z=a+ib`**, then we have

$r = SQRT(a^2+b^2)$,

$theta = TAN^{-1}(b/a)$,

then **z = (r COS(theta), r SIN(theta)).**

Multiplication of two complex numbers z_1, z_2 then acts geometrically as a scaling and a rotation about the origin, giving the resulting point

$z_1z_2 = (r_1r_2\ COS(theta_1+theta_2), r_1r_2\ SIN(theta_1+theta_2))$,

Which, has modulus $\mathbf{r_1r_2}$ and argument $\mathbf{theta_1+theta_2}$.

In three dimensions we need two parameters to specify the direction of the axis for a rotation, a third to specify the angle of rotation, and yet another to determine a scaling for the length. Thus, we would need to specify *four* parameters in all, whereas the ordered triples have only three.

❖ **Breaking Commutativity**

The solution to this problem can be found by attempting to extend another operation from the complex numbers, namely that of *conjugation*. The conjugate of a complex number `z=a+ib` is given by z^*`=a-ib`. When a complex number is multiplied by its conjugate the result is always a real number,

$zz^* = a^2+b^2 = (SQRT(a^2+b^2))^2$,

which is the square of the modulus of the number. A natural extension of this operation to number triples is to write

$z = a+ib+jc$, $z^* = a-ib-jc$.

This gives $zz^* = a^2+b^2+c^2 - 2ijbc$,
which seems to have an extra product term, `-2ijbc`. In order to get rid of this term, we might attempt to put `ij=0`, but this would result in the contradiction that

$ij.ij = i^2.j^2 = (-1)(-1) = 1.$

Hamilton finally resolved this problem by recognizing that the product term is more properly regarded as two terms, `-ijbc` and `-jibc`. Now, if one breaks the commutative law of multiplication and assumes that `ij=-ji`, then the product term vanishes, but it turns out that we are still left with a consistent number system in which ***quadruples*** of numbers (rather than triples) are the natural objects.

The fourth number forming each quadruple arises from the realization, that we can use the associative law of multiplication to find out what the value of `ij` is:

$ij.ij = i(ji)j$
$= -i(ij)j$
$= -(i^2)(j^2)$
$= -(-1)(-1)$
$= -1.$

In other words, `ij` is yet another root of `-1`, independent to both `i` and `j`. If we call this root `k`, then the extension to quadruples of numbers is straightforward.

$a+ib+jc+kd = (a,b,c,d)$

It is then easy to see that the following relationships hold:

$ij=k,$ $jk=i,$ $ki=j,$
$ji=-k,$ $kj=-i,$ $ik=-j,$

$i^2 = j^2 = k^2 = ijk = -1.$

Hamilton called these extended numbers ***quaternion's.***

3.2.3 CONVERSION FROM QUATERNION

To be able to use quaternion effectively, we shall eventually need to convert them to some other representation. You cannot interpret keyboard presses as quaternion, can you? Well, not yet.

- **Quaternion to Matrix**

The Direct3D allow rotations to be specified as matrices, this is probably the most important conversion function, since homogenous matrices are standard 3D representations. The equivalent rotation matrix representing a quaternion is

$$\text{Matrix} = \begin{bmatrix} w^2 + x^2 - y^2 - z^2 & 2xy - 2wz & 2xz + 2wy \\ 2xy + 2wz & w^2 - x^2 + y^2 - z^2 & 2yz - 2wx \\ 2xz - 2wy & 2yz + 2wx & w^2 - x^2 - y^2 + z^2 \end{bmatrix}$$

Using, property of unit quaternion that $w^2 + x^2 + y^2 + z^2 = 1$, we can reduce matrix toto

$$\text{Matrix} = \begin{bmatrix} 1 - 2y^2 - 2z^2 & 2xy - 2wz & 2xz + 2wy \\ 2xy + 2wz & 1 - 2x^2 - 2z^2 & 2yz - 2wx \\ 2xz - 2wy & 2yz + 2wx & 1 - 2x^2 - 2y^2 \end{bmatrix}$$

- Quaternion to Axis Angle

To change a quaternion to a rotation around an arbitrary axis in 3D space, we do the following:

If the axis of rotation is (ax, ay, az)
and the angle is theta (radians)
then the angle= 2 * acos(w)

ax= x / scale
ay= y / scale
az= z / scale

where scale = sqrt $(x^2 + y^2 + z^2)$

Another variation is that the scale = sin(acos(w)). They may be equivalent, though It is not tried to find the mathematical relationship behind them. If the scale is 0, it means there is no rotation so unless you do something, the axis will be infinite. So whenever the scale is 0, just set the rotation axis to any unit vector with a rotation angle of 0.

3.2.5 FAREY FRACTIONS AND PROPERTIES

The Farey fractions, named after the British geologist John Farey (1766-1826), provide an example. The Farey fraction sequence of order *i*, F(*i*),consists of all fractions with values between 0 and1 whose denominators do not exceed *i*, expressed in lowest terms and arranged in order of increasing magnitude.
For example, F(6) is

0/1, 1/6,1/5, ¼, 1/3, 2/5, 1/2 , 3/5,2/3.3/4,4/5.5/6,1/1

In mathematics, a Farey sequence of order n is the sequence of completely reduced fractions between 0 and 1 which, when in lowest terms, have denominators less than or equal to n, arranged in order of increasing size. Each Farey sequence starts with the value 0, denoted by the fraction 0/1, and ends with the value 1, denoted by the fraction 1/1

Farey observed that the fractions in such sequences are the *mediants* of their adjacent fractions. The mediant of $n1/d1$ and $n2/d2$ is$(n1 + n2)/(d1 + d2)$which looks like a naive attempt to add fractions. Farey sequences have a number of other interesting and useful properties.

The Farey sequence is a well-known concept in number theory, whose exploration has lead to a number of interesting results. However, from an algorithmic point of view, very little is known. In particular, the only problem that appears to be investigated is that of generating the entire sequence for a given n.

A sequence of fractions can be interpreted as integer sequences in a number of ways. Since the numerators and denominators show distinctive patterns, a natural method is to separate a sequence of fractions into two sequences, one of the numerators and one of the denominators as in:

Fn(6) = 0, 1, 1, 1, 1, 2, 1, 3, 2, 3, 4, 5, 1
Fd(6) = 1, 6, 5, 4, 3, 5, 2, 5, 3, 4, 5, 6, 1

The Farey sequence Fn for any positive integer n is the set of irreducible rational numbers a/b with 0<a<b<=n and (a, b)==1 arranged in increasing order
The first few are
F1 = {0/1,1/1}
F2 = {0/1,1/2,1/1}
F3 = {0/1,1/3,1/2,2/3,1/1}
F4 = {0/1,1/4,1/3,1/2,2/3,3/4,1/1}
F5 ={0/1,1/5,1/4,1/3,2/5,1/2,3/5,2/3,3/4,4/5,1/1}

For given integer n and k, we can generate the k-th element of the Farey sequence of order n (often called the k-th order statistic [2]) and the same can be used for the different practical applications.
Suppose to list of all fractions between 0 and 1 inclusive, whose denominator does not exceed a given number n.

- When n is 1, the list contains just 0 and 1, that is, 0/1 and 1/1.
- When n is 2, the list contains 0/1, 1/2, 1/1.
- When n is 3, the list contains 0/1, 1/3, 1/2, 2/3, 1/1.
- When n is 4, the list contains 0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1. Note that we have excluded 2/4, as being equivalent to 1/2.

A list like this is known as a Farey sequence. Different lists are distinguished by their "order", that is, the number n which represents the largest denominator. The following diagram shows all Farey sequences from order 1 to 6.

[0/1, 1/1]
[0/1, 1/2, 1/1]
[0/1, 1/3, 1/2, 2/3, 1/1]
[0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1]
[0/1, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 1/1]
[0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1]

Inspection of this illustration reveals many curious properties of Farey sequences. We'll just look at a couple. For every sequence of order >= 2, the fraction 1/2 stands in the middle. Any two terms equidistant from 1/2 are complementary, that is to say, they add up to 1. Looking at the Farey sequence of order 6, we see that

- 2/5 and 3/5 are both one away from 1/2. Their sum is 1.
- 1/3 and 2/3 are both two away from 1/2. Their sum is 1.
- 1/4 and 3/4 are both three away from 1/2. Their sum is 1.
- 1/5 and 4/5 are both four away from 1/2. Their sum is 1.
- 1/6 and 5/6 are both five away from 1/2. Their sum is 1.
- 0/1 and 1/1 are both six away from 1/2. Their sum is 1.

3.2.6 THEOREMS OF FAREY FRACTIONS

Theorem 1: Unique Fraction

If $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive fractions in the n^{th} row with $\frac{a}{b}$ to the left of $\frac{c}{d}$ then $cb\text{-}ad=1$

Theorem 2:

If $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive fractions. Then among all the rational fractions with values between them $\frac{a+c}{b+d}$ is the unique fraction with smallest denominator

Definition 1: Farey Sequence

The sequence of all reduced with denominator not exceeding n, listed in order of their size is called the Farey sequence of order n

Theorem 3: Rational Approximation

If $\frac{a}{b}$ and $\frac{c}{d}$ Farey fractions of order n such that no other Farey fraction of order n such that no other Farey fraction of order n lies between them then

$$\left| \frac{a}{b} - \frac{a+c}{b+d} \right| = \frac{1}{b(b+d)} \le \frac{1}{b(n+1)} \text{ And } \left| \frac{c}{d} - \frac{a+c}{b+d} \right| = \frac{1}{d(b+d)} \le \frac{1}{d(n+1)}$$

Tribes of Gaussian Farey Fractions

M. Nagaraj and Srinivas Murthy have associated the characteristic equation to a Farey fraction and defined the fundamental solutions. H. Chandrashekhar and M. Nagaraj have defined Gaussian Farey Fractions and found the solution for Gaussian Farey Fractions and they have studied the algebraic structures of these tribes.

Let $\frac{\alpha}{\beta}$ be a Gaussian Farey Fraction and let $\beta\varepsilon - \alpha\eta = 1$ be its characteristic equation where $\alpha = a + \mathbf{i}\, b$ and $\beta = c + \mathbf{i}\, d$. Then ($-b$, $-d$) and ($-a\ \mathbf{i}$, $-c\ \mathbf{i}$) are fundamental solutions of the characteristic equation. The general solution of the characteristic equation using fundamental solution ($-b$, $-d$) is: ($-b + \lambda\alpha$, $-d + \lambda\beta$). N ($-b + \lambda\alpha$) < N ($-d + \lambda\beta$) and ($-b + \lambda\alpha$) and ($-d + \lambda\beta$) are relatively prime.

The definition of tribe $T_{\alpha/\beta}$ of the Gaussian Farey Fraction $\frac{\alpha}{\beta}$ given by the set

$T_{\alpha/\beta} = \left\{ \frac{-b + \lambda\alpha}{-d + \lambda\beta} \mid \forall \lambda \in J[i] \right\}$ is called tribe of $\frac{\alpha}{\beta}$. And the real fractions $\frac{a}{c}$ and $\frac{b}{d}$ are Farey fractions.

Algebraic Structures of a tribe $T_{\alpha/\beta}$:

Let $T_{\alpha/\beta} = \left\{ \frac{-z_o + \lambda\alpha}{-w_o + \lambda\beta} \mid \forall \lambda \in J[i] \right\}$ be the tribe $\frac{\alpha}{\beta}$.

Let $\left\{ \frac{-z_o + \lambda\alpha}{-w_o + \lambda\beta} \right\}$ and $\left\{ \frac{-z_o + \mu\alpha}{-w_o + \mu\beta} \right\}$ be any two elements of the tribe $T_{\alpha/\beta}$, Where λ and $\mu \in J[i]$. The two binary operations $\otimes$ and $\oplus$ on tribe $T_{\alpha/\beta}$ are defined by

$$\left\{ \frac{-z_o + \lambda\alpha}{-w_o + \lambda\beta} \right\} \otimes \left\{ \frac{-z_o + \mu\alpha}{-w_o + \mu\beta} \right\} = \left\{ \frac{-z_o + (\lambda\mu)\alpha}{-w_o + (\lambda\mu)\beta} \right\} \text{ and}$$

$$\left\{ \frac{-z_o + \lambda\alpha}{-w_o + \lambda\beta} \right\} \oplus \left\{ \frac{-z_o + \mu\alpha}{-w_o + \mu\beta} \right\} = \left\{ \frac{-z_o + (\lambda + \mu)\alpha}{-w_o + (\lambda + \mu)\beta} \right\}$$

$\{T_{\alpha/\beta}, \oplus, \otimes\}$ is a unitary commutative integral domain, which is isomorphic to the domain of Gaussian integers.

IV. CONCLUSION

The need of quaternion and farey fraction is to analyze and implement cryptography which provide high security using the properties of the quaternion. Using immense applications of number theory we can device a cryptosystem which provides high level of confusion and it makes the hackers impossible to break the code. Here, the cryptosystem is devised using the properties of quaternion and farey fractions.

The applications of number theory contribute greatly for providing provably secure cryptosystems.

ACKNOWLEDGMENT

I would like to thank and acknowledge Dr.A.Arul L.S, for his continuous support and guidance. I would also like to acknowledge all the support rendered by my colleagues, family and friends.

REFERENCES

[1] WhitfielDiffman and Martin Hellman " New Directions of cryptography"Bulletin of the American Mathematical Society 42 (2005), 3-38; online in 2004. ISSN 0273-0979.
[2] Ronald L. Riverst, A. Shamir, and L. Adlernan. "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, volume 21, Feb. 1978, pp. 120–126.
[3] Neal Koblitz "A Course in Number Theory and Cryptography (Graduate Texts in Mathematics) "
[4] Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman "An Introduction to Mathematical Cryptography"
[5] W. Donley Jr ".Quaternionic discrete series by Joshua Holden, " Journal of Proc. Amer. Math, Society, Posted Nov 12th 2002.
[6] H.Chandrashekar, "Algebraic coding theory based on Fare Fractions".
[7] Whitfield Diffie. "The first ten years of public key cryptology", Proceedings of the IEEE, 76(5), May 1988, pp. 560¬577.
[8]. C. C. Chang., "An Information Protection Scheme Based upon Number Theory", The Computer Journal, Vol. 30, No. 3, 1987, pp. 249-253.
[9] W. Donley Jr ".Quaternionic discrete series by Joshua Holden, " Journal of Proc. Amer. Math, Society, Posted Nov 12th 2002.
[10] Kim S. Lee, Huizhu Lu, D. D. Fisher, "A Hierarchical Single-Key-Lock Access Control Using the Chinese Remainder Theorem", Symposium on Applied Computing Proceedings, 1992, pp. 491 – 496.
[11] Shonon C.E, "A mathematical Theory of Communication", BH System Technical Journal, July 1948, p 379.
[12] William Stallings, "Cryptography and Network Security" ,Third Edition, Pearson Education, 2003
[13] AtulKahate, "Cryptography and Network Security", Tata McGrawHill, 2003
[14]Jonathan Katz and Yehuda Lindell "Introduction to Modern Cryptography: Principles and Protocols (Chapman & Hall/Crc Cryptography and Network Security Series) "

