A Randomized Bit Generator using Algebraic Number Theory

∗Ajay Dabral
Department of Mathematics, University of Delhi
ajaydabral2011@gmail.com

Abstract

There are lots of Random Key Generators, In this paper, we gave a new construction of Randomized Bit Generator by using Algebraic number theory, which is quite easy to compute and also we keep the security of this generator in our mind. we discussed its applications as a secret key generator being a randomized bit generator in encryption schemes and hash functions. We tried to make it Quantumly secure by randomizing it and extending its parameters to see it as a Quantum Random key generator.

Keywords: Random Key Generator, Number Fields, Hash Function, Field Monomorphisms.

1 Introduction

A Random generating function is a function or algorithm to generate a sequence of binary numbers. Numerous studies have been conducted on the question of generating a truly random binary sequence [**3**, **4**, **5**, **6**, **7**, **8**, **9**, **10**], i.e a generator that can be regarded as a quantumly safe generator, which will give rise to quantumly safe encryption, a secure stream cipher, and many more. In these studies they made pseudo-random generators using different-different ways like using one-way function [**3**], using discrete log [**4**], Also, there is an improved version of pseudo-random generator based on discrete log [**5**], there is a pseudo-random bit generator based on quantum chaotic map [**7**] and generalized Henon map [**8**]. There is also a Pseudo- random generator based on a logistic chaotic system. Further, there are various number theoretic constructions [**9**, **10**, **11**, **12**] based on logistic chaotic system [**19**] using Coppersmith's methods [**11**] and Bernoulli's map on Algebraic integers [**12**]. The goal of the present article is to make a random number generator using Algebraic number theory and to make it secure and also tried to make a hash function using it. For this purpose, we worked with our generator for an ordered set of number fields having 2 elements, then generalized this concept to any natural number (n) giving a unique binary sequence, and tried to make it secure. Also, we gave applications to our generating function as a hash function and as a key generator for encryption schemes.

2 *Some Mathematical Concepts*

The following definitions are taken from [**1**, **2**].

2.1 *Definition (Algebraic Numbers):-*

A $\alpha \in \mathbb{C}$ is said to be an Algebraic Number, if it is root of a non-zero polynomial with rational coefficients. **For example**: $\frac{1}{2}$ is a root of $2x-1$, which is a non-zero polynomial with rational coefficients. Also, ι is also an Algebraic number being root of polynomial x^2+1, which is a non-zero polynomial with rational coefficients, we denote set of Algebraic numbers by letter $\mathcal{A}$.

2.2 *Definition (Algebraic Integers):-*

A $\alpha \in \mathbb{C}$ is said to be an Algebraic integer, if, it is a root of a monic polynomial with integer coefficients. **For example:** $\sqrt{2}$, 2, and $\frac{1+\sqrt{5}}{2}$ are Algebraic integers, but, $\frac{1}{2}$ is not an Algebraic integer, but it is an Algebraic number. We denote set of Algebraic Integers by $\mathcal{B}$. Clearly, we have $\mathcal{B} \subset \mathcal{A}$.

2.3 *Definition (Transcendental number):-*

A Complex number α which is not an algebraic number is called a transcendental number. **For example:** $\exp.\ \pi,\ \sum_{n=1}^{\infty} \frac{1}{10^n}$ are transcendental . We have $\mathcal{A}$ forms a subfield of $\mathbb{C}$ containing $\mathbb{Q}$, and $\mathcal{B}$ forms a subring of $\mathcal{A}$, hence an Integral domain Containing $\mathbb{Z}$.

2.4 *Definition (Field of Algebraic Numbers):-*

The set of all Complex numbers $\mathbb{A}$ which are algebraic over $\mathbb{Q}$ is a subfield of $\mathbb{C}$ containing $\mathbb{Q}$, called the field of Algebraic Numbers.

2.5 *Definition (Algebraic Number Fields or Number Fields):-*

A subfield K of $\mathbb{A}$ is called an Algebraic number field, if $K/\mathbb{Q}$ is a finite extension (i.e [K:$\mathbb{Q}$]$<\infty$). An Algebraic number field is a finite extension of $\mathbb{Q}$.

2.6 *Theorem (Primitive Element Theorem):-*

Every finite separable extension is simple.
Remark: If K is a number field, i.e $K/\mathbb{Q}$ is a finite extension, then $K/\mathbb{Q}$ is a finite separable extension. Hence by Primitive element theorem $K/\mathbb{Q}$ is a simple extension, i.e, $\exists$ some algebraic number $\alpha \in K$ such that $K = Q(\alpha)$. Hence, all number fields are of the form $K = Q(\theta)$ for some Algebraic number θ.

2.7 *Theorem:-*

Let $K = Q(\theta)$ be a number field of degree (n) over $\mathbb{Q}$. Then there are exactly (n) distinct monomorphisms (injective) $\sigma_i(\theta) = \theta_i$, are the distinct zeroes of the minimal polynomial $p(t)$ of θ over $\mathbb{Q}$.

Proof: Let $\theta = \theta_1, \theta_2, \ddots, \theta_n$ be the $n-$ distinct zeroes of the minimal polynomial $p(t)$ of θ over $\mathbb{Q}$ in $\mathbb{C}$ (Since characteristic of $\mathbb{Q}$ is 0, So, $p(t)$ will be separable polynomial (having all distinct

roots)). By recall $\{1, \theta, \cdots, \theta^{n-1}\}$ forms a basis of the $\mathbb{Q}$-vector space $K = Q(\theta)$, so, every element of K is of the form.

$$\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1},\ a_i \in \mathbb{Q}$$

Now, for each $\iota \in \{1, 2, \cdots, n\}$, we define a map $\sigma_i : K = Q(\theta) \to \mathbb{C}$ by

$$\sigma_i(\alpha) = \sigma_i(a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1})$$

.

$$\sigma_i(\alpha) = a_0 + a_1\theta_i + \cdots + a_{n-1}\theta_i^{n-1}$$

i.e σ_i maps θ to θ_i. Clearly σ_i is a monomorphism for each $1 \leq i \leq n$. Since θ_i are all distinct, therefore $\sigma_i's$ are also distinct.

Finally, if σ is any monomorphism from $K \to \mathbb{C}$, then, σ is identity on $\mathbb{Q}$ (since, $\mathbb{Q}$ is the prime subfield of K). So, $p(\sigma(\theta)) = \sigma(p(\theta)) = \sigma(0) = 0$.

$$\implies \sigma(\theta) \text{ is a zero of } p(t)$$

.

$$\implies \sigma(\theta) = \theta_i \text{ for some } i \in \{1, 2, \cdots, n\}$$

. Hence, $\sigma_1, \sigma_2, \cdots, \sigma_n$ are the only possible $n-$ distinct monomorphisms from K to $\mathbb{C}$.

2.8 *Definition (Conjugates):-*

Let $K = \mathbb{Q}$ be a number field of degree with $n-$ distinct monomorphisms $\sigma_1, \sigma_2, \cdots, \sigma_n$. Then, for any element α of K the Complex numbers $\sigma_i(\alpha)$, $1 \leq i \leq n$, are called $K-$ Conjugates of α.

2.9 *Definition (Field Polynomial):-*

Let $K = \mathbb{Q}(\theta)$ be a number field of degree with (n), and, let $\sigma_1, \sigma_2, \cdots, \sigma_n$ be the $n-$ distinct monomorphism of K into $\mathbb{C}$. For any $\alpha \in K$, the field polynomial of α over K denoted by $f_\alpha(t)$ is defined as

$$f_\alpha(t) = \pi_{i=1}^{n}(t - \sigma_i(\alpha))$$

2.10 *Theorem:-*

Let $K = \mathbb{Q}(\theta)$ be a number field of degree (n) with $n-$ distinct monomorphisms $\sigma_1, \sigma_2, \cdots, \sigma_n$ and let $p(t)$ denote the minimal polynomial of θ over $\mathbb{Q}$, then

(i) For any $\alpha \in K$, the field polynomial $f_\alpha(t)$ is a power of the minimal polynomial (say) $p_\alpha(t)$ of α over $\mathbb{Q}$.

(ii) The K- Conjugates of α are zeroes of $p_\alpha(t)$ in $\mathbb{C}$ each repeated n/m times, where $m = \deg p_\alpha(t)$ is a divisor of n.

(iii) The element $\alpha \in \mathbb{Q}$ iff all its K- Conjugates are equal.

(iv) $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ iff all $K-$ Conjugates are distinct.

2.11 *Definition (Discriminant of a basis):-*

Let K be a number field of degree (n) with n distinct monomorphisms $\sigma_1, \sigma_2, \cdots, \sigma_n$. Let $\{\omega_1, \omega_2, \cdots, \omega_n\}$ be any basis of K over $\mathbb{Q}$. Then the discriminant of $\{\omega_1, \omega_2, \cdots, \omega_n\}$ is defined as the square of the determinant of the $n \times n$ matrix whose $ij-th$ entry is $\sigma_i(\omega_j)$ and is denoted by $\Delta_{K/\mathbb{Q}}(\omega_1, \omega_2, \cdots, \omega_n)$ or just $\Delta(\omega_1, \omega_2, \cdots, \omega_n)$.

$$i.e \delta_{K/\mathbb{Q}}(\omega_1, \omega_2, \cdots, \omega_n) = \left(\det \begin{bmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \cdots & \sigma_2(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n) \end{bmatrix} \right)^2$$

2.12 *Theorem:-*

The discriminant of any basis for $K = \mathbb{Q}(\theta)$ is a non-zero rational number. Moreover if all the K-conjugates of θ are real, then the discriminant of any basis is positive.

2.13 *Definition (Ring of algebraic integers of a number field K):-*

Let K be a number field, then the set of all algebraic integers of K is a subring of K called the ring of algebraic integers of K and is denoted by O_K.

$$O_K = K \cap \mathcal{B} = \{\alpha \in K | \alpha \text{ is algebraic integer}\}$$

.

2.14 *Definition (Integral Basis):-*

Let K be a number field of degree n. A set of Algebraic integers $\alpha_1, \cdots, \alpha_n$ of K is said to be an integral basis for K if every algebraic integer in K can be uniquely written as $a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m, a_i \in \mathbb{Z}$ for $1 \leq i \leq m$.

2.15 *Theorem:-*

Let K be a number field of degree (n) then K has an integral basis.

2.16 *Definition (Discriminant of a Number field):-*

The discriminant of a Number field K is the discriminant of an integral basis of K and is denoted by d_k.

2.17 *Theorem (Brill's Theorem):-*

Let $n = r_1 + 2r_2$, where r_1 denote the number of real isomorphisms of real K and $2r_2$ is the number of complex isomorphisms of K, then,

$$Sgn\ d_k = (-1)^{(r_2)} = (-1)^{\left(\frac{n-r_1}{2}\right)}$$

$$i.e\ d_k(-1)^{r_2} > 0$$

Where Sgn is the sign of discriminant of a number field K.

Proof: Let $\omega_1, \omega_2, \cdots, \omega_n$ be an integral basis of K and let $\sigma_1, \sigma_2, \cdots, \sigma_n$ be isomorphisms of K into $\mathbb{C}$ in which $\sigma_1, \sigma_2, \cdots, \sigma_n$ be isomorphisms of K into $\mathbb{C}$ in which $\sigma_1, \sigma_2, \cdots, \sigma_{r_1}$ are real and $\sigma_{r_1+1}, \sigma_{r_1+2}, \cdots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1}, \cdots, \sigma_{r_1+2r_2}$.

$$\sigma_{r_1+j} = \overline{\sigma_{r_1+r_2+j}} \ \text{ for} 1 \leq j \leq r_2$$

. Now, To Prove It is enough to prove $d_k(-1)^{r_2} > 0$.

$$d_k = \det \begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{bmatrix}^2$$

Now, Consider the matrix

$$detM = \det \begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \sigma_{r_1}(\omega_1) & \sigma_{r_1}(\omega_2) & \cdots & \sigma_{r_1}(\omega_n) \\ \sigma_{r_1+1}(\omega_1) & \sigma_{r_1+1}(\omega_2) & \cdots & \sigma_{r_1+1}(\omega_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_{r_1+r_2}(\omega_1) & \sigma_{r_1+r_2}(\omega_2) & \cdots & \sigma_{r_1+r_2}(\omega_n) \\ \sigma_{r_1+r_2+1}(\omega_1) & \sigma_{r_1+r_2+1}(\omega_2) & \cdots & \sigma_{r_1+r_2+1}(\omega_n) \\ \sigma_{r_1+2r_2}(\omega_1) & \sigma_{r_1+2r_2}(\omega_2) & \cdots & \sigma_{r_1+2r_2}(\omega_n) \end{bmatrix}$$

$$detM = \det \begin{bmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ \omega_1^{(r_1)} & \omega_2^{(r_1)} & \cdots & \omega_n^{(r_1)} \\ a_1^{(r_1+1)} + \iota b_1^{(r_1+1)} & a_2^{(r_1+1)} + \iota b_2^{(r_1+1)} & \cdots & a_n^{(r_1+1)} + \iota b_n^{(r_1+1)} \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{(r_1+r_2)} + \iota b_1^{(r_1+r_2)} & a_2^{(r_1+r_2)} + \iota b_2^{(r_1+r_2)} & \cdots & a_n^{(r_1+r_2)} + \iota b_n^{(r_1+r_2)} \\ a_1^{(r_1+1)} - \iota b_1^{(r_1+1)} & a_2^{(r_1+1)} - \iota b_2^{(r_1+1)} & \cdots & a_n^{(r_1+1)} - \iota b_n^{(r_1+1)} \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{(r_1+r_2)} - \iota b_1^{(r_1+r_2)} & a_2^{(r_1+r_2)} - \iota b_2^{(r_1+r_2)} & \cdots & a_n^{(r_1+r_2)} - \iota b_n^{(r_1+r_2)} \end{bmatrix}$$

$$= d_1 + \iota d_2, where d_1, d_2 \in \mathbb{R}$$

$$\text{Interchanging } \ \iota \to -\iota \quad (i.e \det(\overline{M}) = \overline{\det(M)})$$

$$\det(\overline{M}) = d_1 - \iota d_2$$

$$\text{Now, } R_{r_1+j} \leftrightarrow R_{r_1+r_2+j} \ \ \forall \ \ 1 \leq j \leq r_2 \ (r_2 \text{ operations})$$

$$\implies \det(\overline{(M)}) = \overline{\det M} = (-1)^{r_2} \det M$$

$$d_1 - \iota d_2 = (-1)^{r_2}(d_1 + \iota d_2)$$

Therefore we have two cases:

(i) If r_2 is even then

$$\begin{aligned} d_1 - \iota d_2 &= d_1 + \iota d_2 \\ \implies d_2 &= 0 \\ \implies d_k &= (\det(\sigma_i(\omega_j)))^2 \\ &= (d_1 + \iota d_2)^2 \\ &= d_1^2 > 0 \\ \implies d_k(-1)^{r_2} &= d_1^2(-1)^{r_2} > 0 \end{aligned}$$

(ii) If r_2 is odd

$$\begin{aligned} d_1 - \iota d_2 &= (-1)(d_1 + \iota d_2) \\ \implies d_1 &= 0 \\ \implies d_k &= (\det(\sigma_i(\omega_j)))^2 \\ &= (d_1 + \iota d_2)^2 \\ &= (\iota d_2)^2 \\ &= -d_2^2 < 0 \\ \implies (-1)^{r_2} d_k &= (-1)^{r_2}(-d_2^2) < 0 \\ \implies (-1)^{r_2} d_k &> 0 \\ \implies Sign(d_k) &= (-1)^{r_2} \end{aligned}$$

3 *A brief about some Pseudo Random Generators:*

3.1 RSA pseudo random bit generator

Under the supposition of the Intractibility of RSA problem the RSA bit generator [**13**] is a Cryptographically secure bit generator.

Algorithm.

- **Input:** A y_0 a random integer (seed) in [1,m-1].
- **Output:** A pseudo random bit sequence $s_1, \ldots, s_k$ of length k is generated

1. Generate two primes p_1 and q_1 as in RSA (secretly) and compute $m = p_1 q_1$ and $\psi = (p_1 - 1)(q_1 - 1)$. Select f a random integer $1 < f < \psi$, such that $\gcd(f, \psi) = 1$.
2. Select y_0 a random integer (seed) in [1,n-1]
3. For j from 1 to k do:
   $y_j \leftarrow y_{j-1}^e mod\ m$
   $s_j \leftarrow lsb\ \text{of}\ y_j$
4. $s_1, s_2, \ldots, s_k$ is the output sequence.

3.2 Blum-Blum-Shub pseudo random bit generator

Under the supposition of the intratibility of integer factorization the Blum-Blum-Shub pseudorandom bit generator [**13**] is a cryptographically secure pseudo random bit generator.

Algorithm.

- **Input:** A z a random integer (seed) in [1,m-1] such that gcd(z,m)=1 and compute $y_0 \leftarrow z^2\ mod\ m$.
- **Output:** A pseudo random bit sequence $s_1, \ldots, s_k$ of length k is generated

1. Generate two primes p_1 and q_1 two secretly choosen distinct primes both congruent to 3 mod 4 and, calculate $m = p_1 q_1$.
2. Select z a random integer (seed) in [1,m-1] such that $gcd(z, m) = 1$ and compute $y_0 \leftarrow z^2\ mod\ m$.
3. For j from 1 to k do:
   $y_j \leftarrow y_{j-1}^2 mod\ m$
   $s_i \leftarrow lsb\ \text{of}\ x_j$
4. $s_1, s_2, \ldots, s_k$ is the output sequence.

3.3 Linear Feedback Shift Registers[14]

For LFSR we have to define sequence of inner states $(i_0, i_1, \ldots)$ which is defined via recurrence relation $i_o = k$ and $i_k = f(I_{k-1})$. It is fairly desirable to choose the sequence $(I_0, I_1, \ldots)$ such that the least period of sequence is 2^l, i.e, $I_{2^l} = I_0$ and $I_j \neq I_0$ for $0 < j < 2^l$. One can define a linear recursion by a matrix P via $I_k = MI_{k-1}$. So, For LFSRs, Let $I_k = (i_0^k, \ldots, i_{l-1}^k)$ for arbitrary $k \geq 1$. Consider a recursion which is linear by the operation.

$$\begin{bmatrix} i_0^k \\ i_1^k \\ \vdots \\ i_{l-2}^k \\ i_{l-1}^k \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{l-1} \end{bmatrix} \begin{bmatrix} i_0^{k-1} \\ i_1^{k-1} \\ \vdots \\ i_{l-2}^{k-1} \\ i_{l-1}^{k-1} \end{bmatrix}$$

3.4 The Modified Chaotic Henon Congruential Generator (MCHCG)

After improving uniformly and independency of the CHCG [**15**], the Modified chaoric Henon Congruential Generator was obtained. this was made possible by regulating the distribution of Pseudo Random Numbers, which are generated by chaotic Linear Congruential Generator (CHGH). In this generator the desired interval in which one has to generate random number which is divided into number of subintervals, In this at each step of the algorithm they choose a sub intervsl randomly and to generate PRN at this interval BBS(Blum-Blum-Shub pseudo random bit generator) is recalled

4 *Construction for Pseudo Random Generator*

In this generator, we took two sets to deal with first the ordered set of Algebraic number fields(In particular Quadratic) and another is the ordered set of Irrational numbers. By seeing the first element in the ordered set of irrational numbers we see its digit representation and corresponding to each digit starting from the digit which lies left to the decimal and going right to the digits of the irrational number taken. Then we reduce that number by modulo (n), where n is the number of elements in the ordered set consisting of number fields. After calculating the reduction if we get the number n_1 we assign that reduced value to sign. of discriminant(by Brill's theorem) of the corresponding element in the $n_1 + 1$th position of the set of Algebraic number fields (Identifying Sign. of discriminant -1 by 0 and 1 by 1). Continuing like this we get a binary sequence whcih will be distinct every time we select a digit of an Irrational number. If we have to take $n \geq 11$ to 100, we must have to take two digits at a time of the irrational numbers we are working and for $n \geq 101$ to 1000 we have to take 3 digits at atime of the Irrational number we are working with.

Example 1: Let us consider first ordered set(fixing order of the elements) consisting of two number fields and another set of Irrational number

$$S = \{\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-1} = \iota)\} \text{ (Fixing order of elements)}$$

Monomorphisms corresponding to first number field are $\sigma_1 : \sqrt{2} \to \sqrt{2}$ and $\sigma_2 : \sqrt{2} \to -\sqrt{2}$. While monomorphisms corresponding to second number field are $\sigma_1 : \iota \to \iota$ and $\sigma_2 : \iota \to -\iota$. So, Signature of discriminant for the first number field will be $(-1)^r_2$=$(-1)^0 = 1$ by brill's theorem (where r_2 are the half of the number of complex monomorphism of the number field) and for the second number field, it is given by $(-1)^1 = -1$. Identifying -1 by 0. Now, for another set consisting of only one element say $\Pi = 3.141592653589793238.....$

Considering digits of Π, for $a = 3$ in digits of Π, we calculate $a \mod 2$. If $a \mod 2$ is 0 then output $Signd_k$ of the first $((a \mod 2) + 1)$ element of S. If $a \mod 2$ is 1, output $Sgnd_k$ of the second element of S. So, from Irrational number $\Pi = 3.141592653589793238.....$, we get the

sequence 0010001100010000101..... If we change the order of elements of S we get the sequence 1101110011101111010.....

If we consider the ordered set of set of Irrational number to be the only element consisting of $\exp = 2.718281828459045$..... by the process done above we get the sequence 1001110111100110..... If we change the order of elements of S we get the sequence 0110001000011001.....

Example 2: If S contains more than two elements say $S = \{\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\iota), \mathbb{Q}(\sqrt{3})\}$. After calculating $Sign$ of their discriminant we get +1,-1 and 1 respectively. Again if the ordered set of irrational numbers consists of $\Pi = 3.141592653589793238$..... Now we consider digits of Π. For a in digits of Π Consider $a \mod 3$ (3 is number of elements in the set S). If $a \mod 3$ is 0 then output $Signd_k$ of the first element of S.If $a \mod 3$ is 1 then output $Signd_k$ of the second element of S. If $a \mod 3$ is 2 then output $Signd_k$ pf the third element of S.Continuing like this we get the binary sequence 10001111111111101111.....

Again for $\exp = 2.718281828459045$..... we get the sequence 1001110111011101.....

5 Generalizing the Concept

Let us consider an ordered set S consisting as n elements with Number Fields (Quadratic number fields consisting of both real and complex quadratic number fields, i.e number fields of degree 2 in the same proportion if possible). Also we can consider an ordered set T of (r) distinct irrational numbers.

$$\text{Let } S = \{\mathbb{Q}(\sqrt{d_1}), \mathbb{Q}(\sqrt{d_2}). \cdots, \mathbb{Q}(\sqrt{d_n})\}$$
$$T = \{\Pi_1, \Pi_2, \cdots, \Pi_r\}$$

For each irrational number we get a new binary sequence by the process we have done in the above examples, combining them all we can again make a big binary sequence. If we take single digits of the irrational numbers then we would try to keep our set S with 10 elements atmost. If we have to increase $n \geq 11$ to 100 then we will also increase the digit count (i.e we will take then two digits of the irrational number at a time).Also, If one wants to further increase the $n \geq 101$ to 1000 then, we have to consider 3 digits at a time of the Irrational numbers.

Algorithm.

- **Input:** An Ordered Set S= $\{\mathbb{Q}(\sqrt{d_1}), \mathbb{Q}(\sqrt{d_2}), \mathbb{Q}(\sqrt{d_3}), \cdots, \mathbb{Q}(\sqrt{d_n})\}$ and ordered set $T = \{\Pi_1, \Pi_2, \cdots, \Pi_r\}$ $(n \leq 10)$.
- **Output:** A random binary sequences $a_1a_2a_3a_4a_5a_6$.....

1. For i from set $\mathbb{N}$ Consider z_i the ith digit of Π_j (jth element of the set T) .
2. Calculate $z_i \mod n$.
3. If $z_i \mod n$ is g_i, then consider $(g_i + 1)$th element of set S.
4. Calculate sign. of Discriminant of number field in the $(g_i + 1)$th position.

5. If sign is -1 output 0 as the sequence element and if sign is +1 output +1.
6. contuining this manner we get r distinct binary sequences.

6 Applications

6.1 As a key generator for Encryption Schemes

This generator we made using Algebraic number theory can be used as a key-generator for various encryption schemes in both symmetric and asymmetric cryptosystems.

6.2 As a Hash function

This key-generator can made as a Hash function from a set S and T to a set of binary sequences. We can define $h : S \times T \to F_2^N$, where N is the desired length of the binary sequence we want to compute.

7 Security of the Generator

For security, we always keep in mind to consist of ordered set S of quadratic number fields with a possibly equal ratio of the real and complex number fields. We can further increase the security by increasing the number of elements n in the set S (this time we also have to consider 2 digit at a time for $n \leq 100$ and so on). For further security, we can take permutations of S_n applying on the set S and T giving an increase in the randomness of the binary sequence. Also, we can increase the security by increasing the size of the ordered set T, and after getting the sequence corresponding to each irrational number we can take their XORs to make it further secure.

Note:- For a key of length (n) there are as many options available for generating unique sequences by taking unique irrational number each time which are infinitely many.

8 Scope and Future Work

In this present article, we have discussed about a Pseudo Random Key Generator discussed its security and Applications as a Key Generator for Encryption schemes and hash functions. In the future, we will discuss more applications to this key generator and would like to extend it Quantumly as a Quantum key Generator. Also, we would like to apply this generator to LWE, RLWE, NTRU, and any other cryptographic problems. We would also like to generalize it to any set of general number fields. Also, the Key idea of this generator was to make a Quantumly Secure generator. Also, we would like to make this generator as secure as possible and try to enlighten it up to the highest. Also we would like to prove all NIST security assumtions for a random bit generator.

9 Data Availability Statement

The data that support the findings of this study are openly available and given in the References section.

10 Funding and Conflicts of interests

The work was supported by the University Grants Commission, New Delhi, India, for providing research grant for first author with Grant UGC Ref. No. JUNE18-417559.

References

[1] I. Stewart and D. Tall, *Algebraic number theory and Fermat's last theorem*, fourth edition, CRC Press, Boca Raton, FL, 2016.

[2] M. R. Murty and J. Esmonde, *Problems in algebraic number theory*, second edition, Graduate Texts in Mathematics, 190, Springer-Verlag, New York, 2005.

[3] J. Håstad et al., A pseudorandom generator from any one-way function, SIAM J. Comput. **28** (1999), no. 4, 1364–1396.

[4] S. Patel and G. S. Sundaram, An efficient discrete log pseudo-random generator, in *Advances in cryptology—CRYPTO '98 (Santa Barbara, CA, 1998)*, 304–317, Lecture Notes in Comput. Sci., 1462, Springer, Berlin.

[5] R. Gennaro, An improved pseudo-random generator based on discrete log, in *Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA)*, 469–481, Lecture Notes in Comput. Sci., 1880, Springer, Berlin.

[6] L. Shujun, M. Xuanqin and C. Yuanlong, Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography, in *Progress in cryptology—INDOCRYPT 2001 (Chennai)*, 316–329, Lecture Notes in Comput. Sci., 2247, Springer, Berlin.

[7] Akhshani, Afshin, Amir Akhavan, A. Mobaraki, S-C. Lim, and Zainuriah Hassan. "Pseudo random number generator based on quantum chaotic map." Communications in Nonlinear Science and Numerical Simulation 19, no. 1 (2014): 101-111.

[8] Zheng, Fan, et al. "Pseudo-random sequence generator based on the generalized Henon map." The Journal of China Universities of Posts and Telecommunications 15.3 (2008): 64-68.

[9] Wang, Luyao, and Hai Cheng. "Pseudo-random number generator based on logistic chaotic system." Entropy 21.10 (2019): 960.

[10] M. Naor and O. Reingold, Number-theoretic constructions of efficient pseudo-random functions, J. ACM **51** (2004), no. 2, 231–262.

[11] A. Bauer, D. Vergnaud and J.-C. Zapalowicz, Inferring sequences produced by nonlinear pseudorandom number generators using Coppersmith's methods, in *Public key cryptography—PKC 2012*, 609–626, Lecture Notes in Comput. Sci., 7293, Springer, Heidelberg.

[12] A. Saito and A. Yamaguchi, Pseudorandom number generator based on the Bernoulli map on cubic algebraic integers, Chaos **28** (2018), no. 10, 103122, 9 pp.

[13] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1997.

[14] Zenner, Erik. "On cryptographic properties of LFSR-based pseudorandom generators." None (2004).

[15] Vajargah, B. F., and Asghari, R. (2016). A novel pseudo-random number generator for cryptographic applications. Indian Journal of Science and Technology, 9(6), 1-5.