FPGA Implementation of Pseudo Noise Sequences based on Quadratic Residue Theory

A. Rajagopal
Dept. of E&C,
DSCE,
Bengaluru-560078.

K.L. Sudha
Dept.of E&C,
DSCE,
Bengaluru-560078.

Dundi Ajay
Dept. of E&C,
DSCE,
Bengaluru-560078.

ABSTRACT

Pseudo Noise (PN) sequences are defined as a sequence of 1's and 0's which have randomness properties that make it appear noise-like but are generated by mathematical algorithms. PN sequences that are generated by shift registers such as M-sequences, Gold sequences are known and widely used since the 1960's for various applications. These sequences are periodic and the periodicity is always in terms of powers of 2, hence donot offer much flexibility in terms of length of the sequence. In the past decade or so, PN sequences based on Prime numbers and quadratic residue theory have been discovered and are known to exist for a greater range of permissible lengths. The properties and generation of these Prime number based sequences have not been explored fully in literature and hence this paper explains two such sequences namely Legendre and Weil sequences and simulates them to analyse their properties which test their randomness. The simulation is done using MATLAB and Verilog Hardware Description Language. Generation of these sequences is described and implementation details on the Kintex-7 FPGA device with results are brought out.

Keywords

PN sequence, Quadratic residue, Legendre, Weil, correlation, FPGA.

1. INTRODUCTION

Spread spectrum communication uses much larger bandwidth than required by spreading original information signal using noise like sequences called pseudo noise sequences. Due to noise like property of the spreading sequences, eavesdropping into communication is not easy. Future communication is expected to operate at higher data rates, be more reliable, and operate in increasingly crowded frequency allocations. In cellular radio communication, the autocorrelation property and the cross-correlation property of the spreading sequences are important to achieve multiple access communications, such as CDMA (Code Division Multiple Access). In a system based on spread spectrum transmission techniques, users are multiplexed by orthogonal spreading codes or orthogonal frequency bands or by orthogonal time slots. In Code division multiple access (CDMA) systems with direct sequence approach, all users transmit on the same band at the same time and are distinguished only by means of the code sequence. Their main characteristic is the spreading of the information signal over a bandwidth much larger than the original, which is mainly determined by the spreading method and not by the transmitted information. This is usually done with a pseudorandom or pseudo-noise (PN) sequence.

A PN sequence is defined as a sequence of 1's and 0's which appear in a pattern that makes it indistinguishable from a noise pattern. For certain applications the sequence is required to have certain properties such as equal number of 1's and 0's. Some of the most commonly used PN codes are Maximal length codes (M-sequences), Gold codes, Walsh- Hadamard codes and Kasami codes. The above said PN sequences have average randomness and can be easily generated using shift registers. The disadvantage of these sequences is that they are periodic sequences and do not offer flexibility in terms of their length.

Communication systems are becoming more flexible in bringing in new technologies into the system with mere modification of software. A PN binary sequence is a semi-random sequence in the sense that it appears random within the sequence length, fulfilling the needs of randomness. To a casual observer the sequence appears totally random, however to a user who is aware of the way the sequence is generated all its properties should be known. PN sequences have several interesting properties, which are exploited in a variety of applications. Because of their good autocorrelation two similar PN sequences can easily be phase synchronized, even when one of them is corrupted by noise. A PN sequence is an ideal test signal, as it simulates the random characteristics of a digital signal and can be easily generated. Applications of PN sequences include signal synchronization, navigation, radar ranging, random number generation, multipath resolution, cryptography, signal identification in multiple-access communication systems, missile launching systems, satellite communications, resistance to intended or unintended jamming, sharing of a single channel among multiple users, reduced signal/background-noise level hampers interception and determination of relative timing between transmitter and receiver.

The rest of the paper is organized as follows: Section 2 explains the concept of quadratic residue and quadratic non-residue and the generation of Legendre and Weil sequences, section 3 studies the correlation properties of these sequences, section 4 contains the FPGA simulation results and implementation details and finally section 5 concludes the paper.

2. QUADRATIC RESIDUE SEQUENCES

The concept of quadratic residues and quadratic non-residues **[1, 2]** is explained below:

Consider a quadratic congruence of the form $y^2 \equiv b$ (mod p), where 'p' is a prime number and 'b' is any positive integer less than 'p', then a solution to the given congruence exists (i.e. 'y' exists) if 'b' is a quadratic residue (R) modulo 'p' i.e. If 'y^2'is divided by 'p', it should give a remainder 'b'.

Example: if p=7 and b=2

$3^2 \equiv 2$ (mod7) & $4^2 \equiv 2$ (mod7)

Thus the solution is y=3 and y=4, & b=2 is a quadratic residue modulo 7. Similarly, it can be proved that 1 and 4 are the remaining quadratic residues of 7. **Therefore for p=7 the quadratic residues are: R = {1, 2, 4};**

Of course there may be no solution at all i.e. there is no ‘y’ for which $y^2 \equiv 3 \pmod 7$ then b=3 is said to be quadratic non-residue (N) modulo p. Therefore for any given prime number ‘p’, not counting zero, there always exists (p-1)/2 quadratic residues and (p-1)/2 quadratic non-residues.

The quadratic non-residues of 7 are: N = {3, 5, 6}.

One of the methods to calculate the quadratic residues and non-residues of a prime number is the *Euler’s criterion* which states that an integer ‘a’ such that gcd(a,p) =1 is a quadratic residue modulo ‘p’, ‘p’ being odd prime if,

$a^{(p-1)/2} \equiv 1 \pmod p$;

and it is a quadratic non-residue if

$a^{(p-1)/2} \equiv -1 \pmod p$.

Legendre sequences **[3]** are constructed from Legendre symbol *(x/p)* which is a short hand notation for expressing whether ‘*x*’ is a quadratic residue modulo *p* or not. Here *p* is a prime number.

The Legendre symbol (x/p) is defined as follows:

$$\begin{cases} +1; & \text{if x is quadratic residue mod p} \\ -1; & \text{if x is a quadratic non} - \text{residue mod p} \\ 0; & \text{if } x \equiv 0 \text{ mod p} \end{cases}$$

The Legendre sequence is now defined as s = $(s_0, s_1, s_2 \ldots\ldots s_{p-1})$ where $s_i=(i/p)$ $0 \leq i \leq p-1$. The Legendre sequence is a binary sequence. Here s_0 is always 0 and will be represented as -1. Using the above definition for the Legendre symbol, the Legendre sequence for p=7 is

{0, ***1***, ***2***, 3, ***4***, 5, 6} →{-1, 1, 1,-1, 1,-1,-1}.

Where ***1, 2, 4*** are quadratic residues represented by +1, while 3, 5, 6 are non-quadratic residues represented by -1.

For small primes the Euler’s criterion is used to calculate the quadratic residues and non-residues but for large prime numbers using the criterion leads to overflow problems. Therefore a method that is described in **[4]** generates the sequence indices at which +1’s occur rather than -1’s and does not require any multiplication or division and given by the equation

$L_n = \{L_{n-1} + (2n-1)\} \bmod p;$ **- (1)**

where, $2 \leq n \leq (p-1)/2$ and $L_1 = 1$;

For the case of p=7, ‘n’ is ranging from 2 to 3. Therefore with $L_1 = 1$ we have

$L_2 = \{L_1 + (2*2) - 1\} \bmod 7 = \{4\} \bmod 7 = 4.$

$L_3 = \{L_2 + (2*3) - 1\} \bmod 7 = \{9\} \bmod 7 = 2.$

Therefore L_n = {1, 4, 2} which are the quadratic residues of p =7.

The Legendre sequence may then be defined as:

$$s(k) = \begin{cases} +1, if\ k\ \in\ \{L_n\} \\ -1, if\ k\ \notin\ \{L_n\} \end{cases} \textbf{- (2)}$$

Therefore the Legendre sequence calculated for p =7 by the above method is s = {-1, 1, 1,-1,1,-1,-1} which is the same as that found using Euler’s criterion.

The main drawback of Legendre sequence is the size of the family for a given length which is always one. Hence to overcome the family size limitations, researchers taking inspiration from one of the properties of maximum length sequences which states that a shift and an XOR addition of an M-sequence produces another M-sequence, generated Weil sequences.

Weil sequences:

The XOR addition of a Legendre sequence ‘s’ of length ‘p’ with a shifted replica of itself leads us to whole new set of family called Weil sequences W **[5].**

$W = \{s+Ts, s+T^2s \ldots s+T^{((p-1)/2)}s\}$ -(3)

Where ‘T’ denotes the operator which shifts the vector cyclically to the left by one place, that is, Ts = $(s_1, s_2 \ldots\ldots s_{p-1}, s_0)$ whereas $T^k s$ shifts the vector cyclically left by ‘k’ places. Here ‘+’ denotes modulo-2 addition. The shift can be a right circular shift or a left circular shift. Therefore for one Legendre sequence of prime length ‘p’ there are (p-1)/2 Weil sequences each of length ‘p’.

Figure 1 shows the generation of Weil sequence from a Legendre sequence, where the 0’s are represented as ‘-1’ and 1’s as ‘+1’. Therefore the XOR addition which was for a sequence of 0’s and 1’s is now replaced with multiplication for -1’s and +1’s.

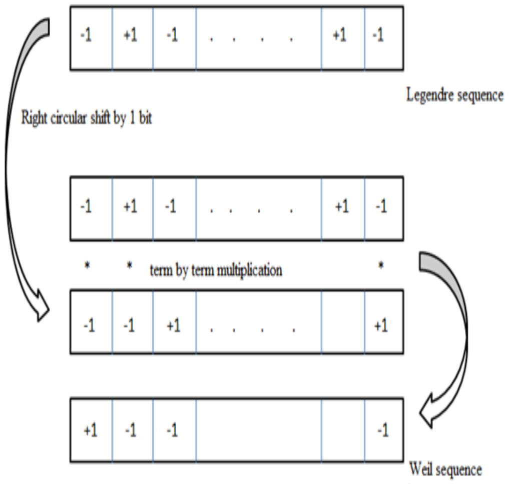


Figure 1- Weil sequence generation

3. PROPERTIES OF LEGENDRE AND WEIL SEQUENCES

The properties of the sequences are tested after generating the sequences in MATLAB and are described below. The length of the sequence considered is 227 bits.

(i) Balance property

The balance property states that in each period of the sequence, the difference between the number of 1’s and the number of 0’s is one.

Figure 2 indicates that the number of 1’s in Legendre sequence is 113 and the number of 0’s is 114, whereas for Weil sequence with shift index 1, meaning that the Legendre sequence with one bit right circular shift when modulo-2 added with the un-shifted sequence has 114 ones and 113 zeros in one period of the sequence.

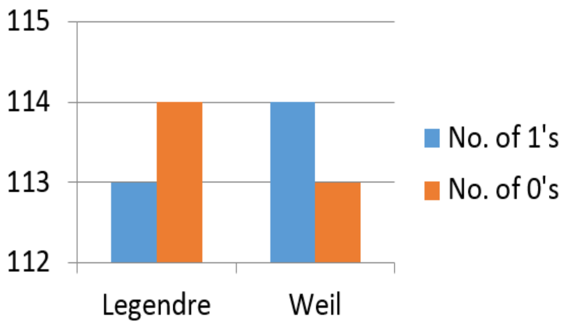


Figure 2 – Balance property of Legendre and Weil sequences

(ii) Runs property

This property states that among the runs of 1’s and 0’s in each period of the sequence, one-half of the runs of each kind of length one, ¼ are of length two, 1/8 are of length three and so on as long as these fractions represent meaningful numbers.

By a run means a subsequence of identical symbols that is 1’s or 0’s.

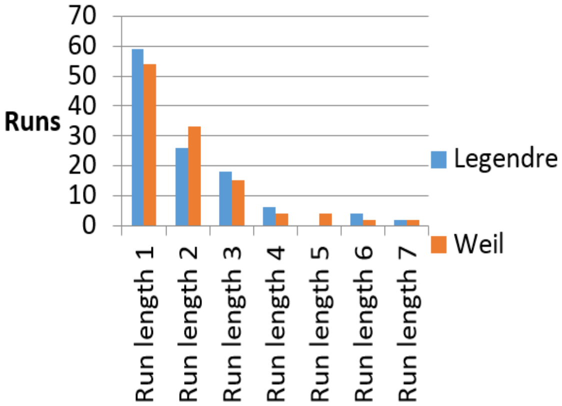


Figure 3 – Run length property of Legendre and Weil sequences

The above figure indicates that the runs property is neither satisfied by the Legendre sequence nor the Weil sequence. There are a total of 7 runs in one period of both the sequences, 59 of the runs in Legendre sequence are of length 1 and 54 of the runs in Weil sequence are of length1; 26 of the runs in Legendre and 33 of the runs in Weil are of length 2 and so on.

(iii) Even & Odd Auto-correlation

Let a PN sequence be represented by -1 volt for binary symbol’0’ and +1 volt for ‘1’, then the even auto-correlation function (ACF) of the PN sequence {a_n} is defined as, where ‘v’ is the time shift

$$\mathbf{ACF_e(v) = \sum_{i=0}^{N-1} a_i a_{i+v}} \qquad \text{- (4)}$$

The odd auto-correlation **[6]** arises whenever the data bit that is modulating the PN sequence flips either from logic 1 to 0 or logic 0 to 1 within the period of the PN sequence. It is given by the expression, with $'\tau'$ as the time shift

$$\mathbf{ACF_o(\tau) = \sum_{i=0}^{N-\tau-1} a_i a_{i+\tau} - \sum_{i=N-\tau}^{N-1} a_i a_{i+\tau}} \qquad \text{– (5)}$$

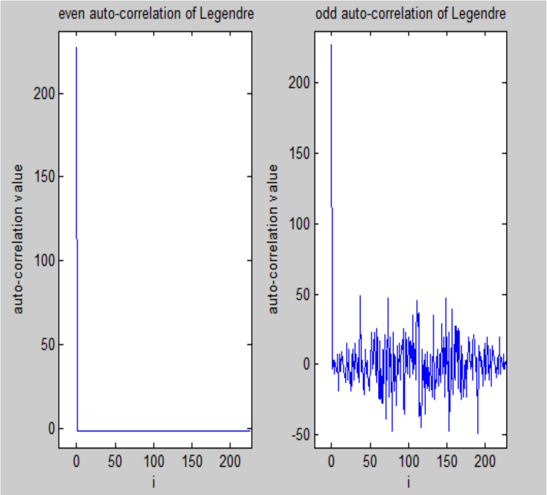


Figure 4- Auto-correlation plot of Legendre sequence of 227 bits

Based on the periodic auto-correlation of the Legendre sequence, they can be divided into two classes:

Class 1: If p ≡3 (mod 4) then the auto-correlation function (ACF) is

$$\text{ACF} = \begin{cases} \mathbf{p};\ \text{for i} = 0; \\ \mathbf{-1};\ \text{otherwise} \end{cases}$$

Class 2: If p ≡1 (mod 4) then the auto-correlation function is

$$\text{ACF} = \begin{cases} \mathbf{p};\, \text{if } '\text{i}' = 0 \\ \mathbf{-3};\, \text{if } '\text{i}' \text{ is quadratic residue mod p} \\ \mathbf{1};\ \text{if } '\text{i}' \text{is a quadratic nonresidue mod p} \end{cases}$$

Therefore the plot of ACF of Legendre sequence of figure 4 belongs to class 1 group, where p=227 which is congruent to 3 (mod 4).

Similarly figure 5 shows the plot of even and odd auto-correlation of Weil sequence. It can be seen from the plot the even auto-correlation is not binary valued but the maximum limit of correlation side-lobe is bounded by 2√p +5 **[5]** where ‘p’ is the length of the sequence.

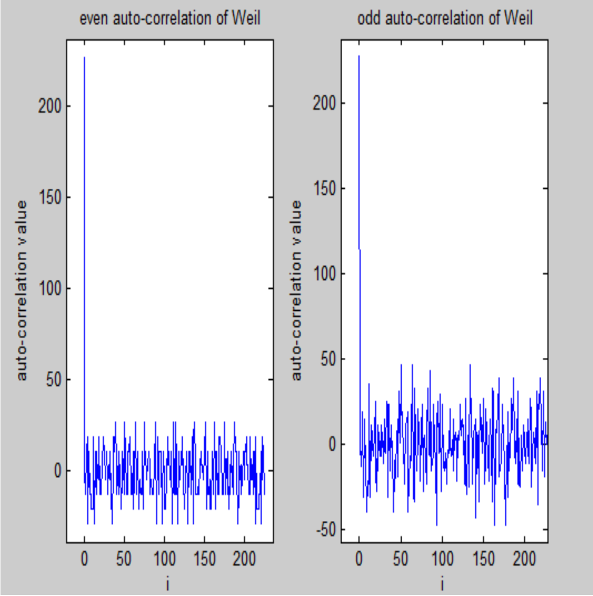


Figure 5- Auto-correlation of Weil sequence of 227 bits

(iv) Even & Odd Cross-correlation:

The even cross-correlation function (CCF) for sequences $\{a_n\}$ and $\{b_n\}$ is defined as

$$\mathbf{CCF_e(v)} = \sum_{i=0}^{i=N-1} a_i b_{i+v} \qquad \text{- (6)}$$

The odd cross-correlation is defined as

$$\mathbf{CCF_o(\tau)} = \sum_{i=0}^{N-\tau-1} a_i b_{i+\tau} - \sum_{i=N-\tau}^{N-1} a_i b_{i+\tau} \qquad \text{– (7)}$$

Since for a given prime number there is only one Legendre sequence hence there is no cross-correlation plot for it. Figure 6 shows the even and odd CCF plot for Weil sequences. The two Weil sequences are Weil sequence index 1 with one bit right circular shift and Weil sequence index 2 with two bits right circular shift and XOR with Legendre sequence.

As can be seen in the even auto-correlation and even cross-correlation plot in figures 5 & 6, the maximum side-lobe is bounded by 2√p +5 = 2√227 +5=35.13.

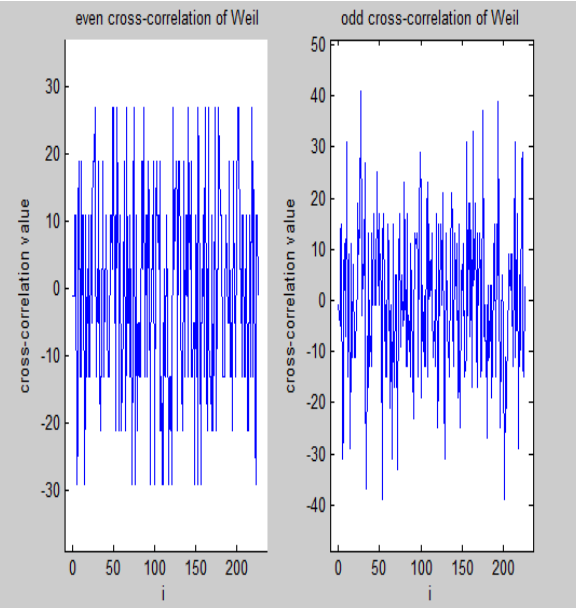


Figure 6- Cross-correlation plot of Weil sequences

4. FPGA IMPLEMENTATION RESULTS

A Verilog hardware description language code is written for both Legendre and Weil sequences of length 227 bits for implementation on the Kintex -7 FPGA XC7K325TFFG900-2 kit. The simulation results for Legendre sequence is shown in figure 7

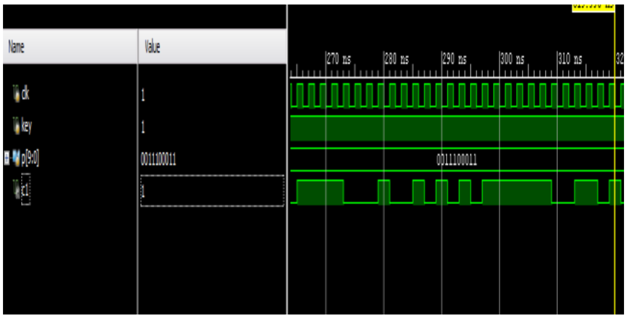


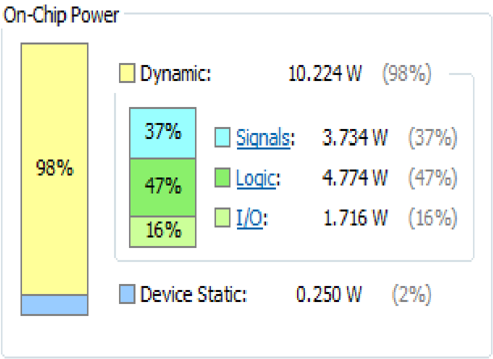
Figure 7- Simulation results of Legendre sequence of 227 bits

In the above figure, 'key' denotes the start signal for sequence execution, 'p[9:0]' is the 10 bit prime number input 227 which in binary notation is "0011100011" and 'c1' is the output bit. The device utilization post implementation is shown in table 1

Table 1- Device utilization summary of Legendre sequence

Resource	Utilization	Available	Utilization %
Flip-flops	310	407600	0.08
Look up tables (LUT)	466	203800	0.23
I/O	14	500	2.80
BUFG	1	32	3.12

The power consumption from the implemented netlist is shown in figure 8.



On-Chip Power

□ Dynamic:	10.224 W	(98%)
□ Signals:	3.734 W	(37%)
□ Logic:	4.774 W	(47%)
□ I/O:	1.716 W	(16%)
□ Device Static:	0.250 W	(2%)

Figure 8– Power Analysis for Legendre sequence

The total on-chip power is 10.474W of which the dynamic power which is the on-chip power consumed by each type of user logic is 10.224 which is 98 % of the total on-chip power. The dynamic power includes user design power from all applicable voltage sources. The device static power is 0.250W which is 2% of the total power. Device static power is the transistor power leakage from all voltage sources when the device is powered but not configured.

The simulation results for a Weil sequence of length 227 bits is as shown in figure 9.

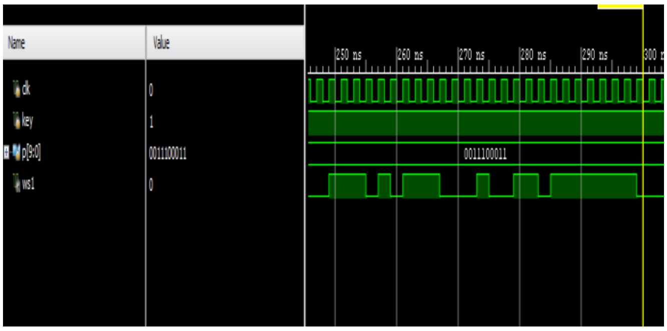


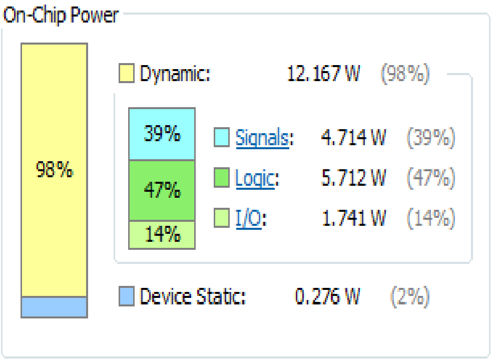
Figure 9- Simulation results of Weil sequence of 227 bits

In the above figure, 'key' denotes the start signal for sequence execution, 'p[9:0]' is the 10 bit prime number input 227 which in binary notation is "0011100011" and 'ws1' is the output bit. The device utilization post implementation for generating two Weil sequences is shown in table 2.

Table 2- Device utilization summary of Weil sequence

Resource	Utilization	Available	Utilization %
Flip-flops	310	407600	0.08
Look up tables (LUT)	612	203800	0.30
I/O	14	500	2.80
BUFG	1	32	3.12

Similarly the power utilization summary is shown in figure 10



□ Dynamic: 12.167 W (98%)

□ Signals: 4.714 W (39%)

□ Logic: 5.712 W (47%)

□ I/O: 1.741 W (14%)

□ Device Static: 0.276 W (2%)

Figure 10 – Power Analysis for Weil sequences

The total power consumed is 12.443W out of which 12.167W is dynamic power and 0.276W is the device static power.

5. CONCLUSION

This paper described the newly discovered Legendre and Weil sequences which are based on prime numbers and quadratic residue theory. The method to construct these sequences is described and their properties such as balance, runs and correlation property were analysed. Legendre and Weil sequences may not have the ideal properties of M-sequences or Gold sequences but their flexibility in terms of length can be particularly useful in satellite navigation systems. The FPGA implementation results indicate that they are not as complex to generate provided the right formula is made use of as described in this paper. Weil sequences are currently being used as spreading sequences in GPS systems. These sequences can also be used for other applications mentioned in the paper except for cryptographic applications as the randomness of these sequences are not good enough. Future work can include obtaining the trace representation of these sequences so that they can be generated using shift registers.

6. ACKNOWLEDGMENTS

This work is supported by ISRO RESPOND programme [grant no. ISRO/RES/3/651/2013-14].

7. REFERENCES

[1] Kenneth Ireland and Michael Rosen, A Classical Introduction to modern number theory, Springer-Verlag, 2nd Ed.1990.

[2] M. R. Schroeder, Number Theory in Science and Communications, Springer-Verlag, 2nd Ed.1997.

[3] Zhang Guohua and Zhou Quan, Pseudonoise codes constructed by Legendre sequence, Electronics Letters **38** (2001), no. 8, 376–377.

[4] K. VeerabhadraRao and V. Umapathi Reddy, "Biphase Sequence Generation with low Side-lobe Autocorrelation Function," IEEE Transactions on Aerospace and Electronic Systems, vol. 22, March 1986.

[5] J. J. Rushanan, "Weil Sequences: A Family of Binary Sequences with Good Correlation Properties," in IEEE International Symposium on Information Theory, Seattle, WA, pp. 1648 – 1652, 2006.

[6] D.V. Sarwate and M.B. Pursley, Cross correlation properties of pseudorandom and related sequences, Proc. of the IEEE, vol. 68, No. 5, May 1980, pp. 593-619.

[7] Simon Haykin, Digital communication, John Wiley & Sons, 2006.

[8] CherukuRavikumar and K.L.Sudha, "Legendre and PolyphaseSidel'nikov Sequence for Applications in Space Communication", International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-2 Issue-9, July 2014.

[9] Dundi Ajay, K.L.Sudha and A.Rajagopal, "DSP implementation of Weil and Sidelnikov binary Pseudo Random Noise Codes", IEEE International Conference on Electrical, Computer and Communication Technologies, 2015.(ICECCT 2015), Coimbatore, India.