Barry's Linear Circular Private Key and Public Certificate Exchange

By

Barry L. Crouse Ph.d Computer Information Systems

Introduction

I would like to begin by outlining a problem I have been continuing to see without any solutions coming across the Internet with questionable security practices. The Process I am proposing is what I have seen last year during the holidays mainly Thanksgiving and Christmas 2016.

I have developed a Private Network with state of the Art Security and it has shown me some fundamental flaws in Certificates and Key exchanges. The idea in this work uses Linear and Circular Based Motion incorporating Asymmetrical keys and passwords Circular and Linear. The Specs for the type of System calls for a server that is medium level able to support greater than 128 gig of memory.

This Design incorporates many different ideas including two tier level passwords track and area's of space it also includes Algorithms , Data Redundancy, Data Protection I also provide a method to reverse the Engineering of a algorithm and rebuild it into a new one.

The type of system in this work is a Open-Closed System. I utilize both linear and Elliptic types of motion overall not dependent on one type of motion open system. The closed portion is the Area of Space which place's a limitation on this type of System it is more advanced than the closed system with finite space.

This design utilizes many different ideas and concepts along with different methods so stay alert and have fun with this !

Table of Contents

Chapter 1

Visual Graphs

Chart 1-A

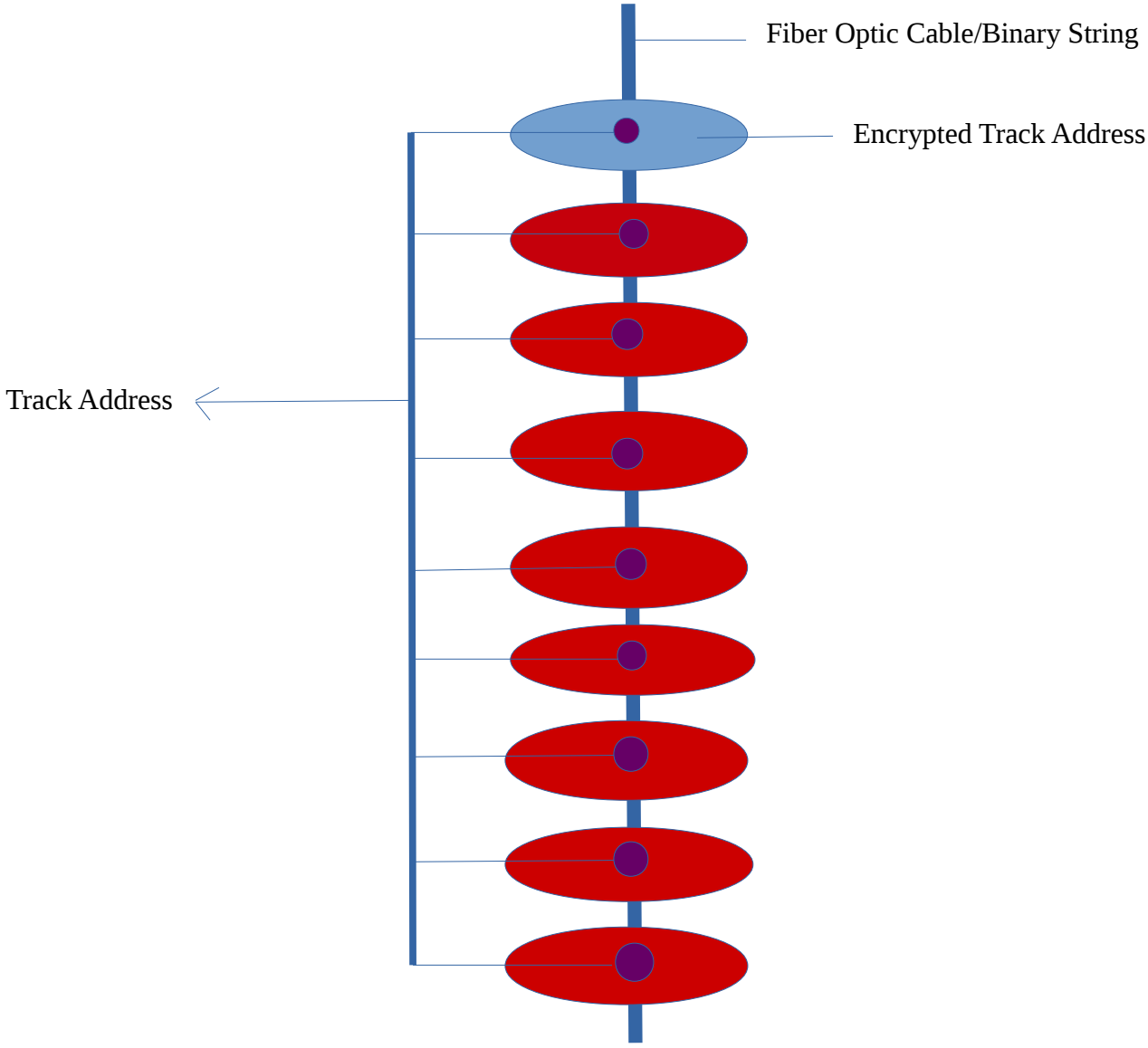
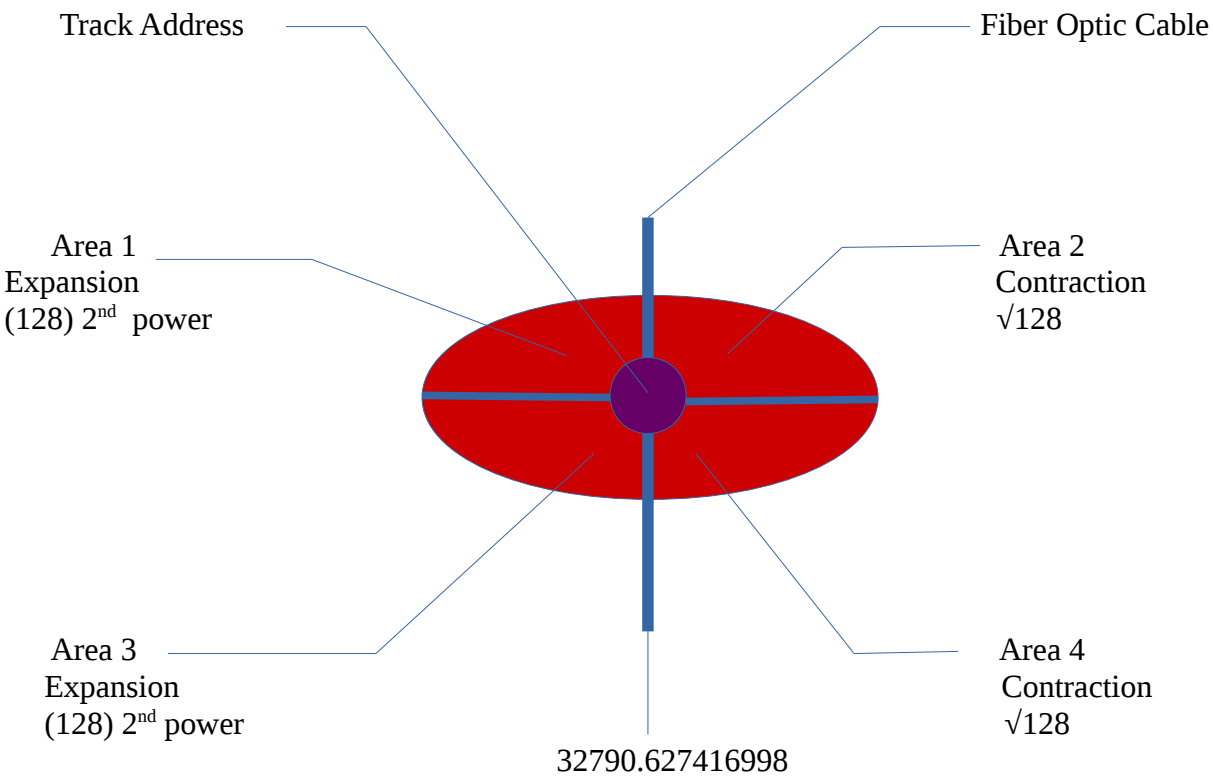

Fiber Optic Cable/Binary String
Encrypted Track Address
Track Address

Chart 2-A



Area 1 = 16384
Area 2 = 11.313708499
Area 3 = 16384
Area 4 = 11.313708499

Area 1 + Area 2 + Area 3 + Area 4 = 32790.627416998 = 32791

1 track supports 32791
8 sub tracks support total = 32791 * 8 = 262328
Regular Encrypted (256) * (256) = 65536 + Prime Number = 521 = 66057

Review of Charts

I will review the Charts just presented. I have utilized both linear and Circular types of motion. The Fiber Optic cable is much like a Data String that is linear but when the information is accessed it must go out to the Concentric address. This is nothing new using a Fiber Optic cable to access circular tracks through the uses of address schemes. This method is not sequential in orderly processing but Random it does not follow a strict path.

The Circular tracks are assigned Areas of space Expansion and Contraction as the chart indicates but if you will notice the Fiber Optic Data string is assigned a value of 32791 instead of a nice evenly divisible number.

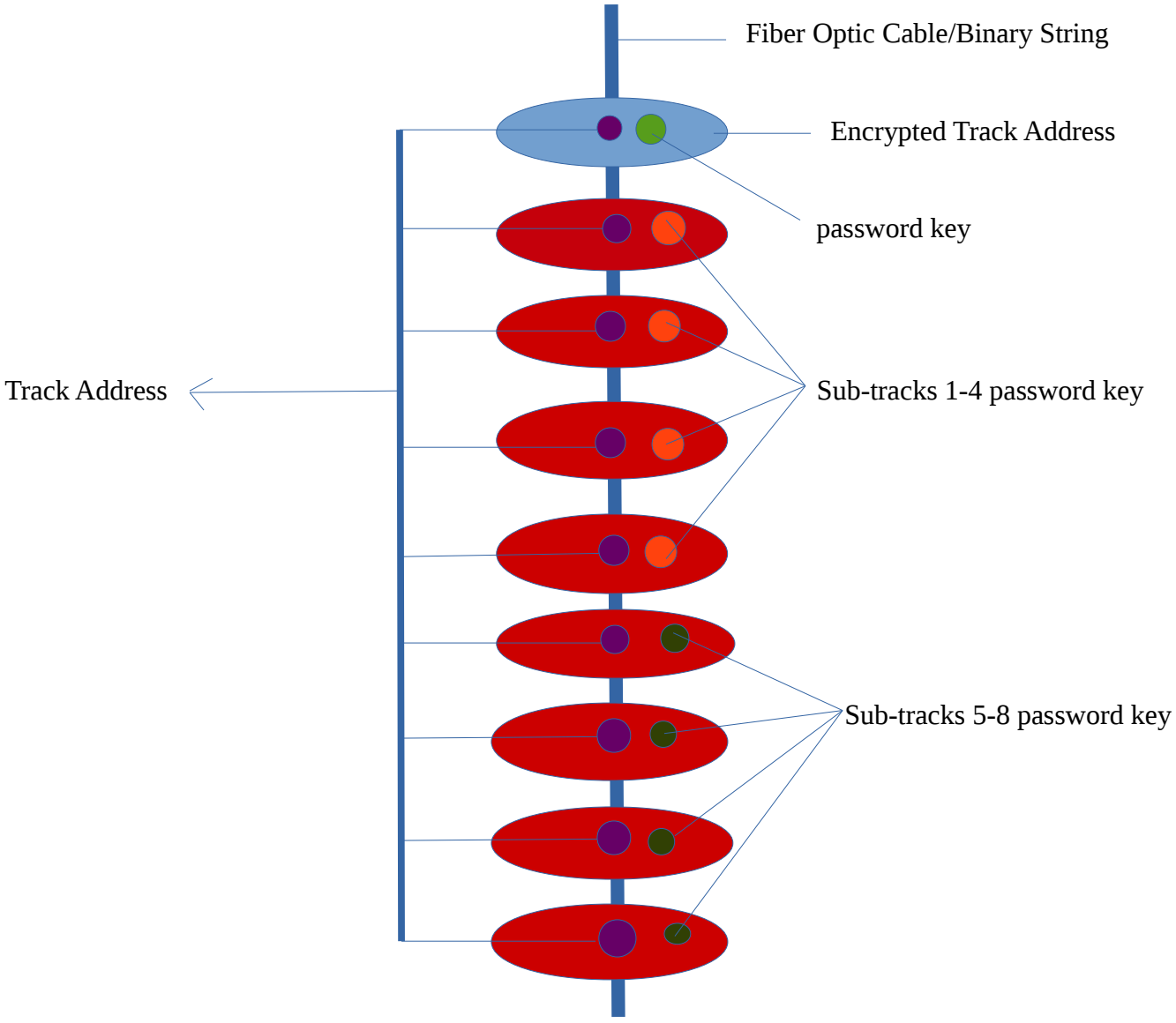
The Encrypted Track blue color has a value of 66057. I have created 8 sub-tracks Red color for a total value of 262328. The purple color is much like a point locator to access the information. If you studied back in the 80's Computer Sciences this concept was pretty much taught. The main differences are the values assigned that are not evenly divisible through the usage of prime numbers along with Areas of Space Expansion and Contraction instead of the Concentric circles on the track itself thus Each circle contains 4 Areas of Space that are Asymmetrical not assigned nice even numbers in all 4 areas of space ;however, Areas 1 and 3 = 2 and 4 this presents the opportunity of redundancy please also note the Regular Encrypted Track is not equal to the sub-tracks to prevent corrupted duplication usually found on 8 bit codes and clipboard usage which brings up the next topic using Encrypted Passwords that are Asymmetrical.

The principle of Asymmetrical Encrypted passwords is to protect Data Sensitive Information. Example I need to type in my password for the Encrypted Track suppose it is hacked I still need a password to access the 8 sub-tracks this creates a layer of security and follows the principle of peer to peer model but with Data Redundancy within the shell. We could even take this a step further by requiring a different password on sub tracks 1 – 4 and 5-8. I have provided a 3 tier level of security for the purpose of protecting Data sensitive information I will present a graph and than create a Encrypted password algorithm in the next chapter.

Chapter 2

Track Password Encryption

Chart 3-A


Fiber Optic Cable/Binary String
Encrypted Track Address
password key
Track Address
Sub-tracks 1-4 password key
Sub-tracks 5-8 password key

Password Algorithm For Track Access

When designing a password Algorithm, I am not a great believer in copying data on a clipboard in random fashion for the argument Encryption according to definition is application on the 7 layer OSI Interface. If I use a 8 bit binary code with 128 bit ssl with 2 bytes equal to one character than I have 16 characters If I use 256 with UTF view 16 16 character length nice evenly divisible numbers.

My approach to this will be Expand the Number and Contract with prime number usage.

The Equation could be written as follows password = {x} 3rd Power + √{y}
whereas X equals Evenly divisible number and Y = prime number next step obtain the total subtract from a prime number and obtain a divisible number let's try a example

X =8 3rd power
y = √7

8 * 8 * 8 =128 + √7 = 514.645751311 rounded = 515 bits

515 – prime number 191 = 324 so I have two numbers 1 prime {191} the other {324} bits divisible. I simply use a principle of taking a number 515 create two events one is a prime number and the other divisible Asymmetrical and Dynamic.

Event 1 = 191 bits
Event 2 = 324 bits

Next step define a array

Array UTF { 16,32,64}

Event 1 / Array {16,32,64} + 16384 = a
Event 2/ Array {16,32,64} + 16384= b

√ a+ b = Z + 1 bit password next rounded number Encryption

I can use this Encrypted password Algorithm to create 3 different passwords a little bit of a process but the End User has a little more control over number selection making password encryption harder to crack because the worst thing a adversary can do is guess worst outcome taught this in Martial Arts Kickboxing guessing is the worst thing your opponent can do.

I have basically created a password algorithm for access to tracks with 1 encrypted track and access to sub key tracks basically comparable to disk protection but with asymmetry and dynamic the issue that is now how to protect each area of space within the track for data sensitive information with Data Redundancy. I will need to create a password algorithm for the areas of space within the track. I will present this in the next chapter.

Chapter 3

Password Algorithm for Areas of Space

Before beginning, We know I have 4 areas of space within the track that has data redundancy defined space. We need to place some password protection on the area of space to unlock the area of space. The data definition is below as shown in the chart.

Area 1 = 16384
Area 2 = 11.313708499
Area 3 = 16384 Data Redundancy
Area 4 = 11.313708499 Data Redundancy

Area 1 + Area 2 + Area 3 + Area 4 = 32790.627416998 = 32791

I can apply reverse engineering methods to unlock the area of space.

$\sqrt{16384} *$ 11.313708499 2^{nd} power = 128 + 128 = 256 + 256 = 512

I have basically 512 bits commonly out on the market and evenly divisible number. The solution to this is to provide a prime number so 512 + 521 for example produces a protocol of 1033 bits 521 bits is used for elliptic based keys so the merging of a even with a prime number should not be that hard to over come in this case I would have to add I bit to get a divisible number 1034 I can now set the parameters by taking the 1034 bits and dividing it by a UTF View

1034 / UTF View 16 = 64 bytes

2 bytes = 1 characters

64 bytes / 2 = 32 Characters

In working over the years most password fields allow roughly between 16 -21 in password length this has been extended but not with the standard UTF-8 view. Presently out in the market in some browsers there are UTF views of 16 and 32. Basically this algorithm raises the bar and demands better data security by protecting both the disk and area of space itself with Asymmetry and Dynamic energy requiring both linear and elliptic based energy. I will now present my final thoughts in the next chapter.

Chapter 4

Faster Method Process

Sample Track Address location

Chart 4- A

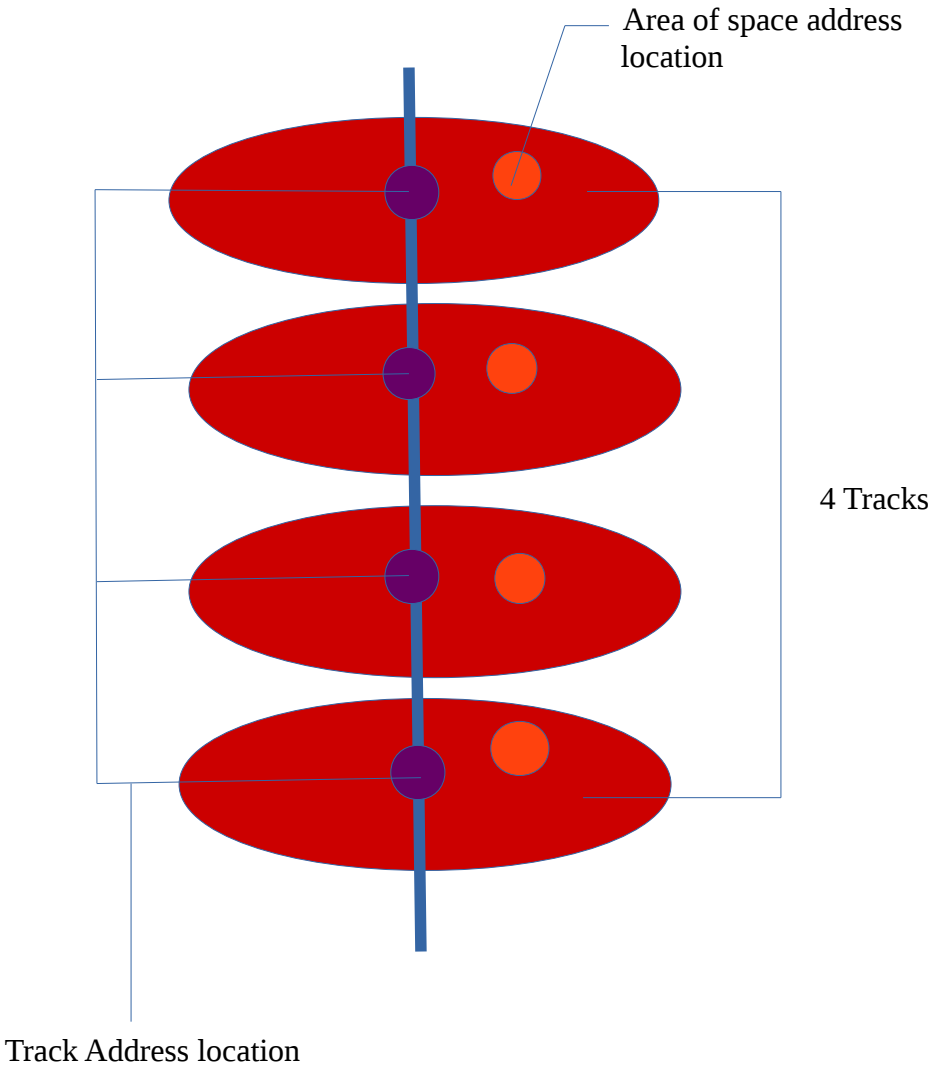
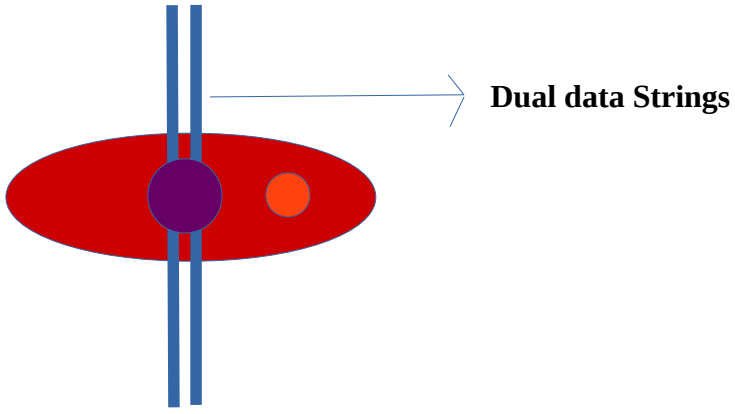


Chart 4-A shows a two step method for quick access keeping in mind using the linear based data string and than accessing the circular track.

The purple dot located on both the data string and circular track provides a address for quicker location of the track that needs access. The second step is the circular track with the orange dot provides where the information is located on the area of space thus I avoid sequential methods that are slow and developing along with time consumption issues. If you have the address on the data string moving from 1 track to another is much easier than reading each record on the track. The difference in this process is the two step address location on a linear and circular environment. If you are a 80's programmer you are probably familiar with the Random Access method that located records, The difference between this method is a two step address location along with areas of space and avoids extensive hashing schemes.

This method combines both linear and circular thus I have optimized the process that utilizes the best of both motions. Please note it is possible to add dual data strings on the overall process but the main ideas would be lost and added overhead see example below:

Example 1-A



Chapter 5

Final Thoughts

This completes my 3 part series of Cryptographic motion mainly Linear, Circular, Linear and Circular. I have introduced new algorithms and new methods that hopefully will contribute to new security models that address the 21st century needs.

This work had a lot of different ideas that on a mental level a 7th or 8th degree black belt test that does not subscribe to one set of motion but combines Linear and Circular to make the best possible outcome to achieve optimal performance combining random and orderly processes that work cohesively.

The motion process requires to first access the Data String or linear line than goes into the Circular tracks and further into Areas Of space. Please note I do not have to follow a orderly process accessing every record but in a random order.

These processes and methods can be translated into Cosmology and provides a better understanding of our Universe by taking the limitations off our Definition of the Universe. This design in my view represents a higher view than a elliptic based Universe that is in constant state but it does not reach a level on a 9th or 10th degree level of knowledge. This type of knowledge requires the ability to decide to either be bounded or not bounded to time and space Intelligent Design.

As stated in the beginning this type of system is a Open-Closed system motion is overall not dependent on one type but employs two types of motion open it also has a defined area of space making it closed. This type of system is more advanced than a elliptic type because it balances both speed and power.

If you like this work please come out and visit the following websites

www.barrysscientificbasedproducts.com

www.barryequalityfieldequation.com

E-mail crouseb395@gmail.com

E-mail barry@barrysscientificbasedproducts.com

Barry L. Crouse

06/18/2017