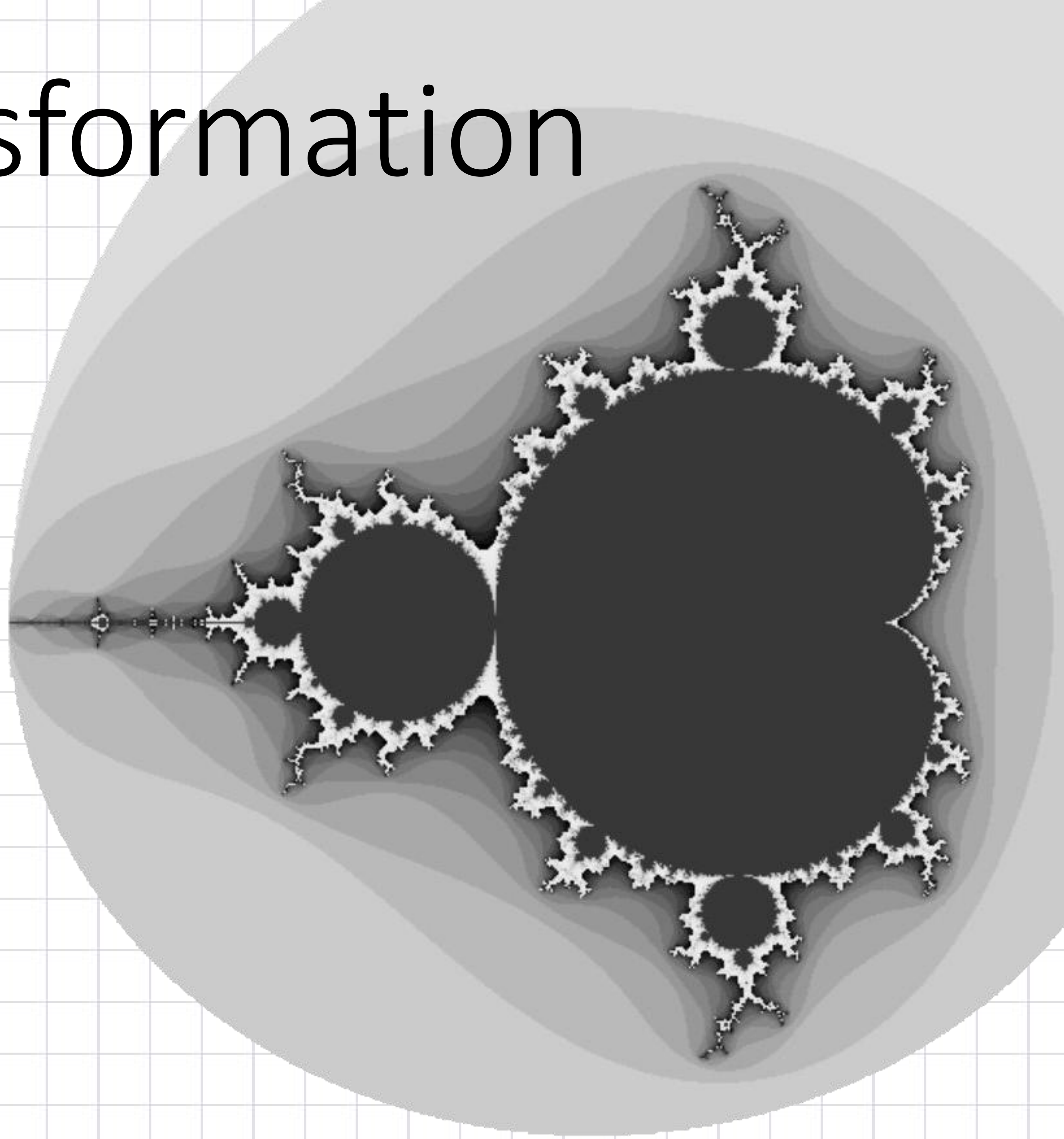
Fractal Transformation

A New Science



Comparing

Classic Block Encryption

with

Fractal Transformation

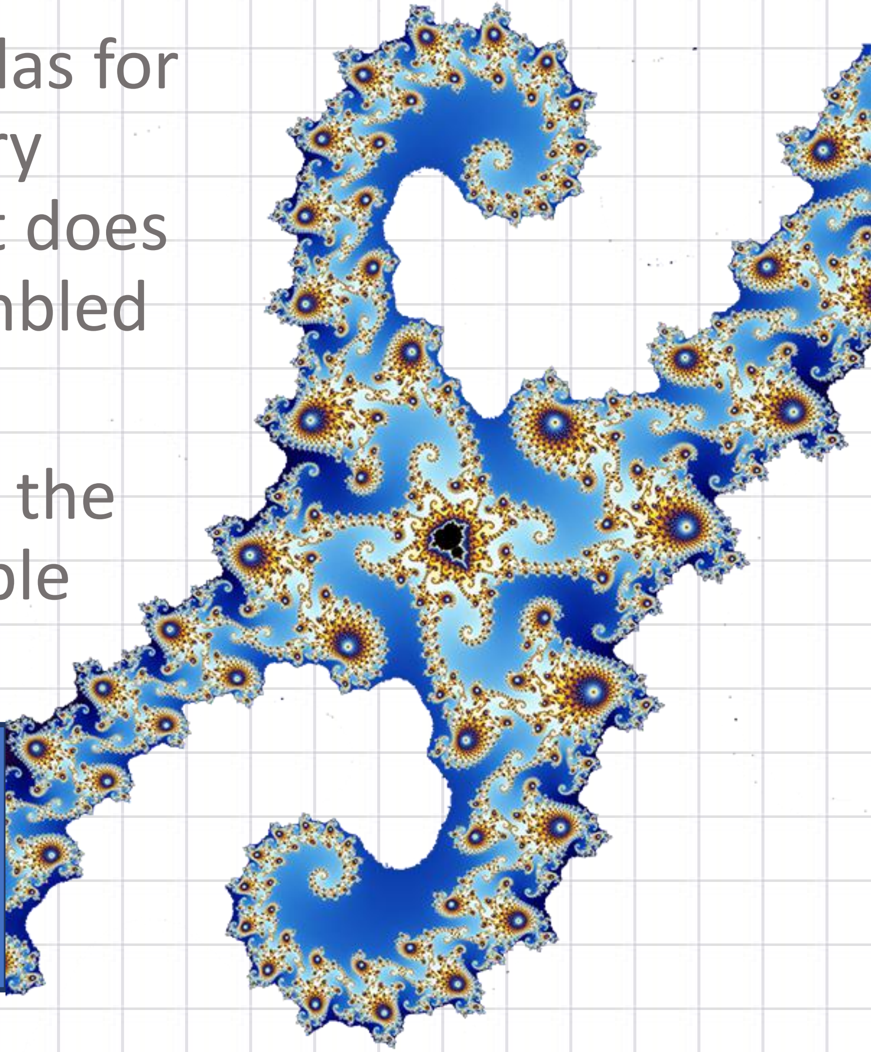
Non-deterministic Fractal Transforms

Our patent pending fractal transform formulas for data security are non-deterministic at every stage of the process, creating a cipher that does not contain the payload in any form, scrambled or otherwise.

This is made possible by deep integration of the infinitely complex, unique and unpredictable fractal dimension.

Quantum Bunker integrates the

Mandelbrot Fractal



The differences

	Classic Encryption	Fractal Transformation
Key	Acts directly on the payload via algorithm	Identifies one of ∞ fractal portals
Algorithm	Block encryption controlled by key shape	Fractal stream generation from portal
Actions	Add key, substitute, row shift, column mix	Unpredictable fractal stream offsets payload
Determinism	Key acts deterministically on payload	Key does not act on payload
Cipher	Payload blocks scrambled by algorithm	Whole payload overwritten by fractal stream
Key size	Fixed, 128-bit, 192-bit, or 256-bit	Unlimited
Block size	128-bit	Unlimited, transform matches payload size
Vulnerability	Only correct key returns sensible result	Indistinguishable incorrect key decrypts

Fractal transformation is a new security art and science, unrelated to classic block encryption.

A New Art and Science

We use the term ‘**Fractal Transformation**’ to clearly distinguish this new cryptographic art and science.

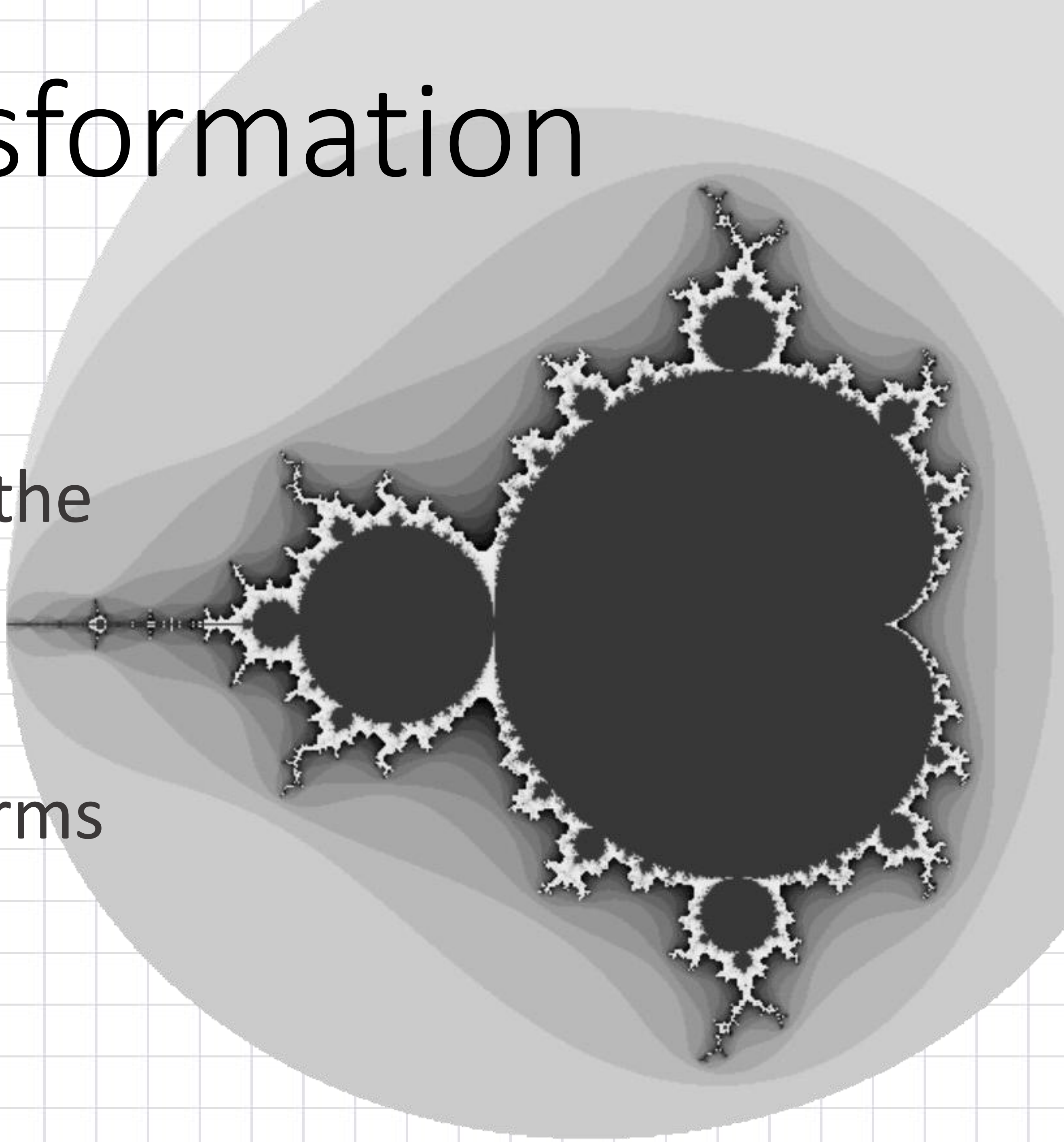
It is an art as much as a science.

We have approached and explored the awesome and beautiful Mandelbrot Fractal with precision, reverence and wonder.

Our fractal integrations are artful, revealing unlimited possible iterative traversals and formulas, a palate of infinite security potential…

Fractal Transformation

The process



Securing data within the infinitely complex

Mandelbrot Set

Using Portalz Transforms

Fractal Transform Explained

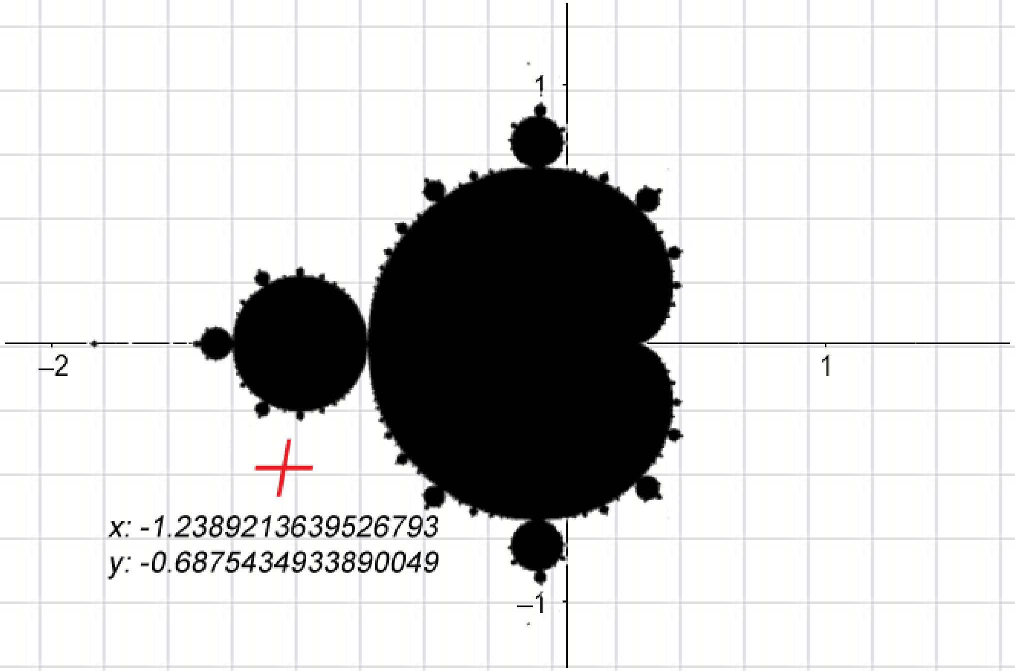
The process of Fractal Transformation involves the following steps:

1. Identify a Fractal Portal using the key
2. Generate a Fractal Stream from the Portal Vector
3. Offset the payload with the Fractal Stream

Fractal Portal

A fractal portal is an x,y vector, a point within the Mandelbrot Set.

In this example the + shows an x,y fractal portal vector:



x: -1.2389213639526793
y: -0.6875434933890049

Fractal Portal Complexity

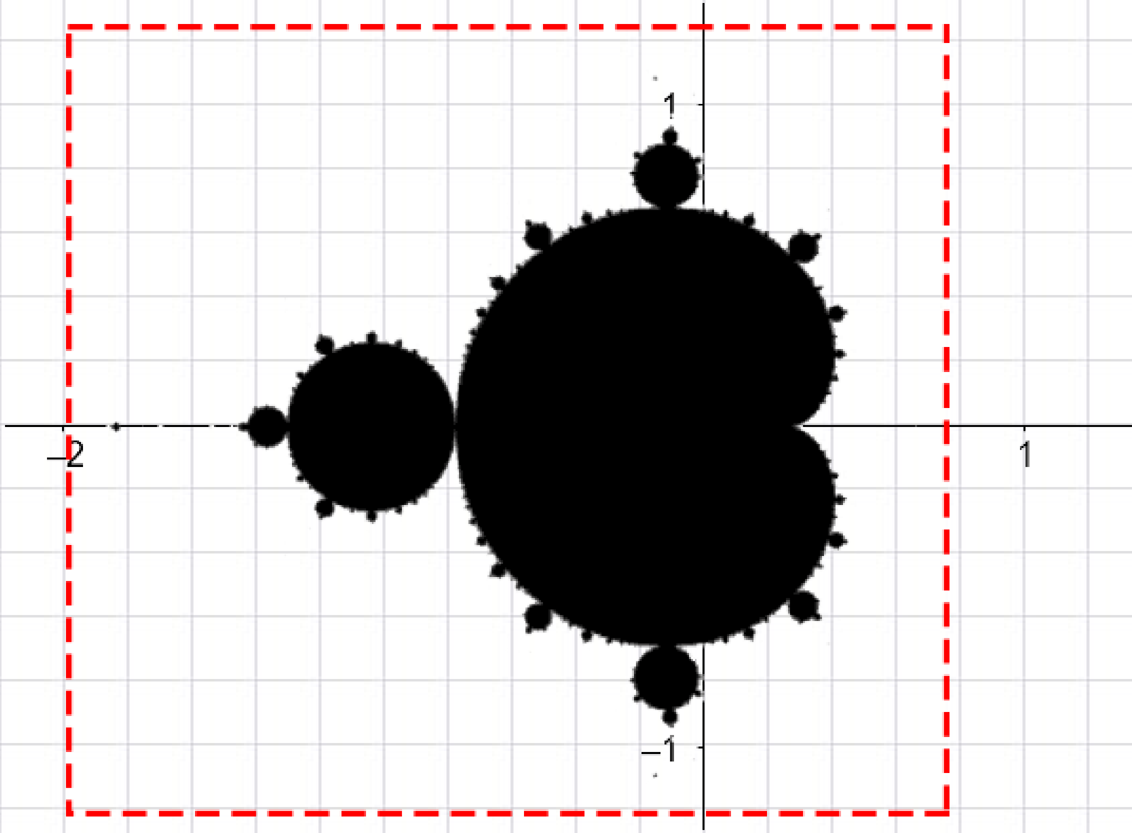
The complexity of fractal regions varies.

The black region goes to infinity and not suitable for fractal portals.

The most complex regions are those surrounding the black region.

The further away from the black region the less complex.

The region most suitable for fractal portals is inside the red rectangle.



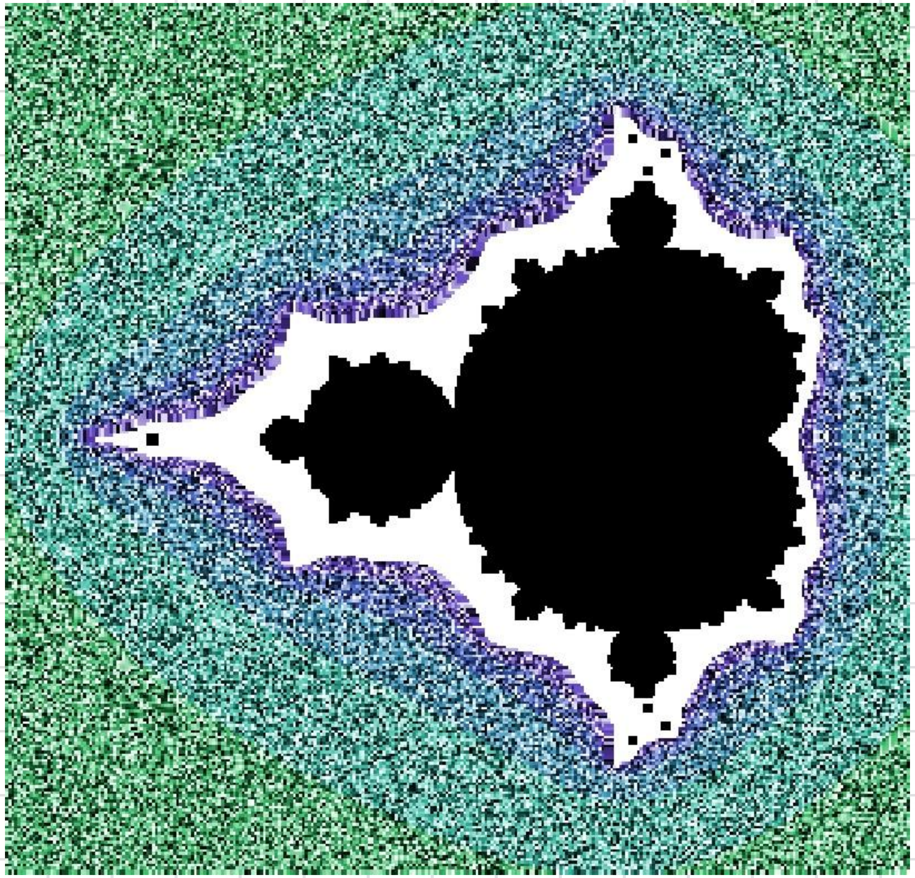
Fractal Portal Mapping

A survey of the Mandelbrot Set identifies regions where:

1. They are outside the black infinity region
2. They are within the higher complexity region
3. They exclude the highest complexity regions

The highest complexity regions are excluded as they can cause performance issues with deep iterations.

The resulting mapping is stored in a vector list.



Fractal Portal from a Key

A Key of any size is mapped to a **Fractal Portal**.

There is an infinite number of possible Fractal Portals.

Every possible key, of any size, maps to a unique Fractal Portal.

This is accomplished by:

1. Generating a hash of the key
2. Splitting the hash into 3 parts, a lookup value and an x,y vector
3. Find the ***Entry Portal*** vector by offsetting the lookup vector with the x,y vector
4. Iterating the Key from the ***Entry Portal*** to arrive at the unique ***Fractal Portal***

Step 4. shifts the possible portals from **2^512** to **infinity**.

Fractal Portals break Key Determinism

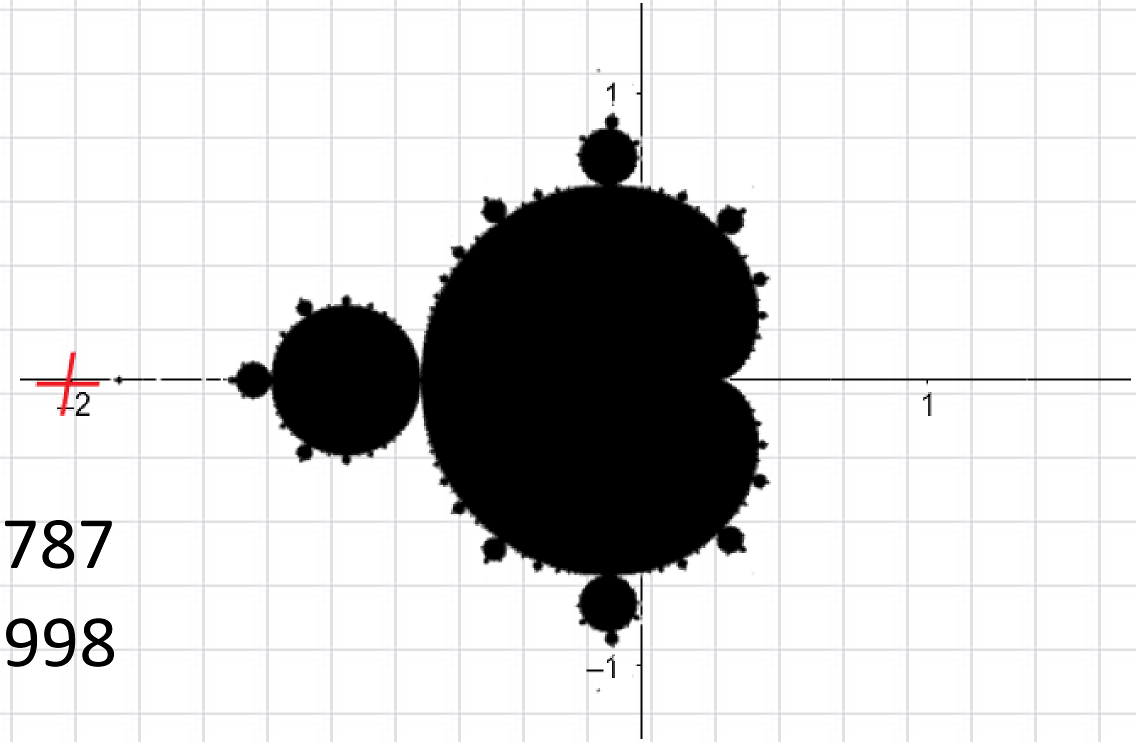
Once a **Fractal Portal** is identified the Key no longer plays a part in the **Fractal Transformation** process.

Unlike classic block encryption, the transformation values that emerge from the **Fractal Portal** are entirely separate from and unpredictable by the Key, thereby breaking Key Determinism.

Fractal Transformation

Fractal Transformation of a payload begins when a unique Fractal Portal has been identified with a Key. For our example we will use:

Key:	**Secret99**
Payload:	**Demo Payload**



The Key translates to a Fractal Portal:

x: -2.0890747618095770408250428787

y: -0.0868059720835475839059327998

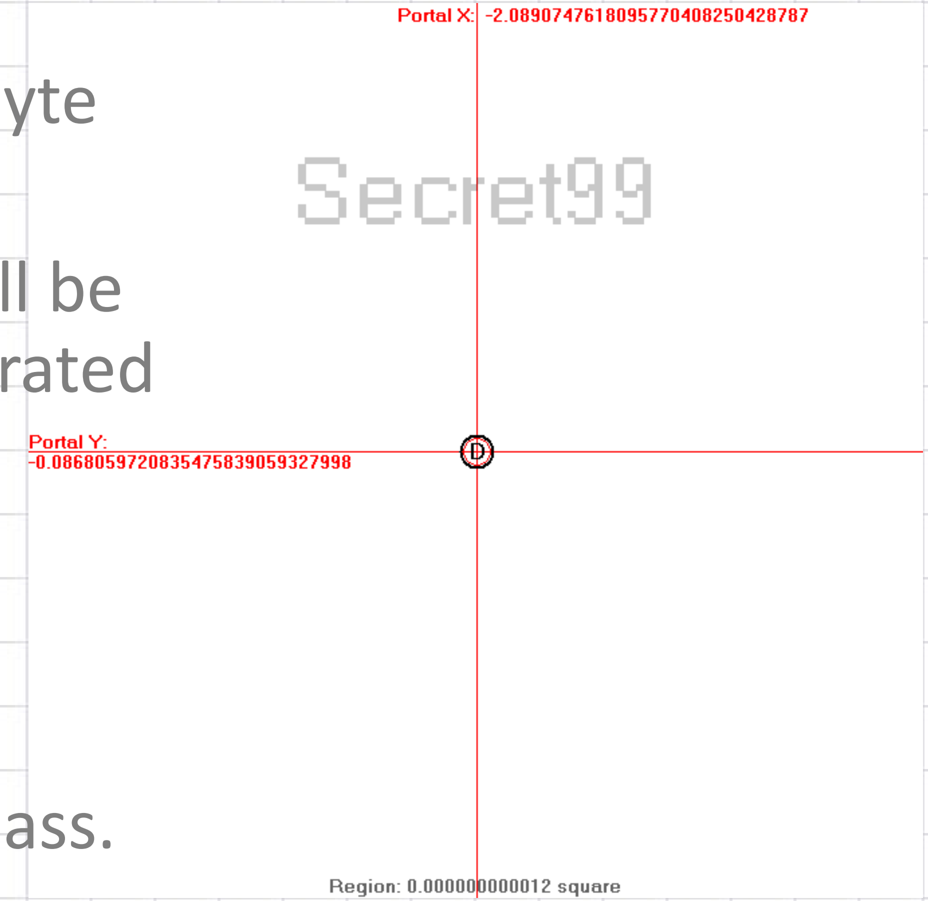
Fractal Transformation Iteration 1

Transformation begins by iterating each byte of the payload.

Here we show the first byte “D” which will be transformed with the fractal value generated at the portal vector.

The diagram is generated by our Fractal Transformation R&D Software using standard settings.

We will follow the iterations for a single pass.


Portal X: -2.0890747618095770408250428787
Secret99
Portal Y:
-0.0868059720835475839059327998
D
Region: 0.000000000012 square

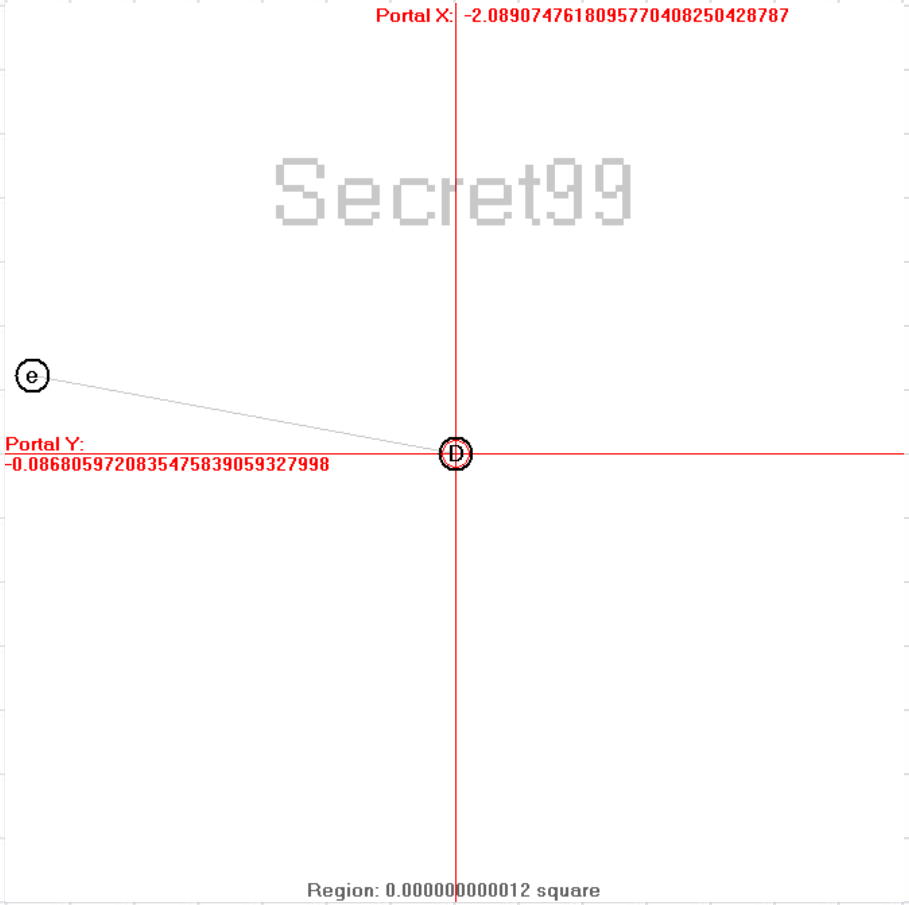
Fractal Transformation Iteration 2

The fractal value generated at the portal vector has been used to derive 3 values:

1. A byte transform value (mod 256)
2. An angle value (mod 360)
3. A hypotenuse value (a fraction)

The angle and hypotenuse are used to calculate a new fractal vector using Pythagorean geometry.

This generates the next fractal value.


Portal X: -2.08907476180957704082504287 87
Secret99
e
D
Portal Y:
-0.0868059720835475839059327998
Region: 0.000000000012 square

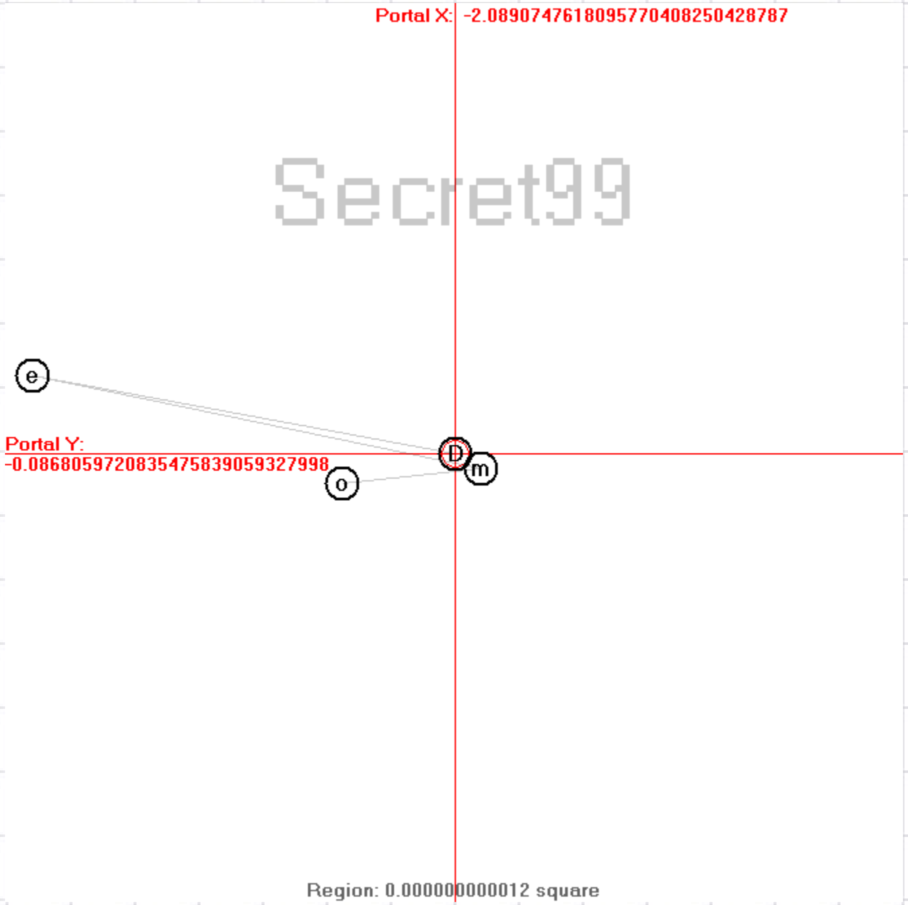
Fractal Transformation Iteration 4

This transformation process is repeated to match each byte in the payload.

Here we show the steps for the first four letters of the payload “Demo”.

Note that there is no possible way to predict the next fractal vector or the fractal value returned by it.

There is zero determinism from one fractal value to the next.


Portal X: -2.08907476180957704082504287870
Secret99
e
Portal Y:
-0.0868059720835475839059327998
D
m
o
Region: 0.000000000012 square

Fractal Transformation Complete

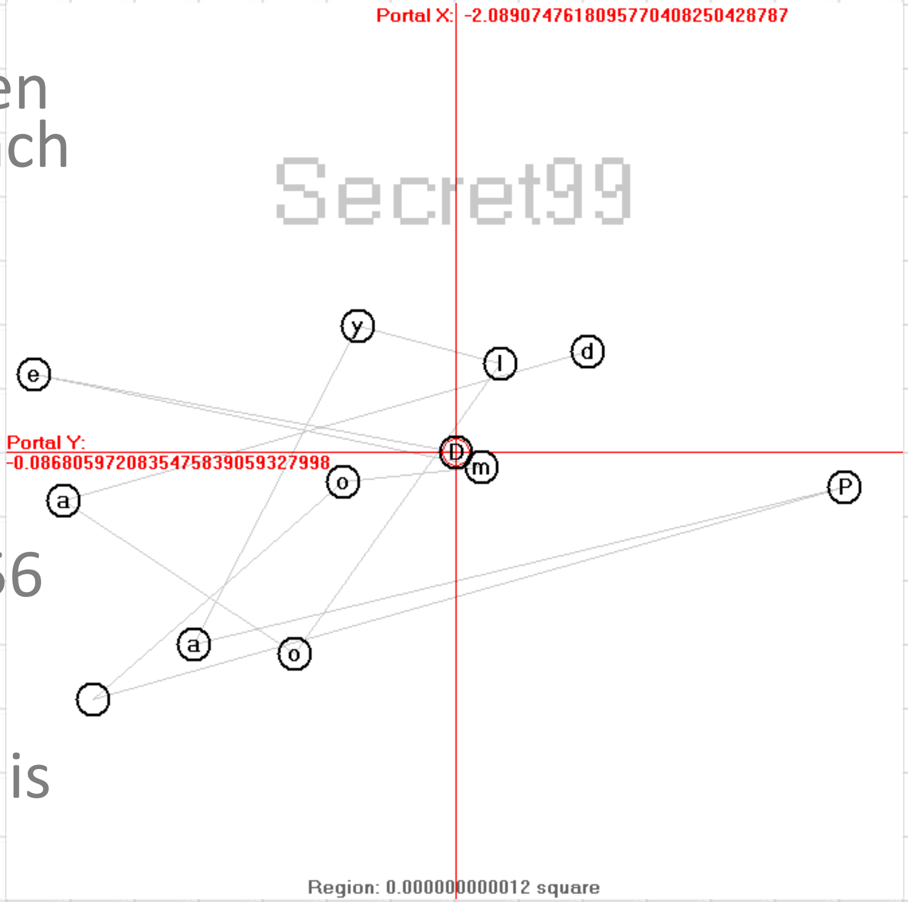
The transformation process is completed when a fractal transform value is generated for each payload byte.

This is a single pass.

Multiple passes can be used where the transformed cipher becomes the payload.

The fractal values are added to the payload values. When the sum exceeds 256 then 256 is subtracted.

When extracting the payload from the cipher the values are subtracted. When the result is less than zero then 256 is added.


Portal X: -2.0890747618095770408250428787
Secret99
y
e
l
d
Portal Y:
-0.0868059720835475839059327998
D
m
o
a
P
a
o
Region: 0.000000000012 square

Fractal Transformation Numbers

These are the vectors, fractal values and geometric values:

Data	Fractal X	Fractal Y	Fractal Value	Angle	Hypotenuse
D	-2.0890747618095770102200108365	-0.0868059720835475819120777073	5874.7274351297	3.72743512971	0.00000000000000000306699110601
e	-2.0890747618152200379238096874	-0.0868059720845888548107124008	5874.72743642702	190.45487025942	0.0000000000057382629212887302
m	-2.0890747618092303280291582571	-0.0868059720833481367659216972	5874.72743503904	29.90974051884	0.0000000000003999861553713324
o	-2.089074761811076614522221219	-0.0868059720831407062038317658	5874.72743541918	164.81948103768	0.00000000000015537923727886374
	-2.0890747618144282581855002328	-0.0868059720802307293461798324	5874.7274359044	145.63896207536	0.00000000000058767196673788068
P	-2.0890747618043686292123267716	-0.0868059720830664381482615477	5874.72743397111	5.27792415072	0.0000000000005230588185625116
a	-2.0890747618130793113805193293	-0.0868059720809613192021475434	5874.72743567349	143.55584830144	0.00000000000043536954603879642
y	-2.0890747618108902761387093423	-0.0868059720852352195920723621	5874.72743554848	232.11169660288	0.00000000000021383875229467386
l	-2.0890747618089718056330639363	-0.0868059720847240624398680504	5874.72743509473	297.22339320576	0.00000000000013230311293051764
o	-2.08907476181171974211069395	-0.0868059720808486979406416978	5874.72743537211	128.44678641152	0.00000000000034460345693530176
a	-2.0890747618148132456907636031	-0.0868059720828947836183953936	5874.72743620258	172.89357282304	0.00000000000052767404343218082
d	-2.0890747618078127821343107065	-0.0868059720848873529340075393	5874.72743485877	322.78714564608	0.00000000000022153079374412256

Fractal Transformation Variance

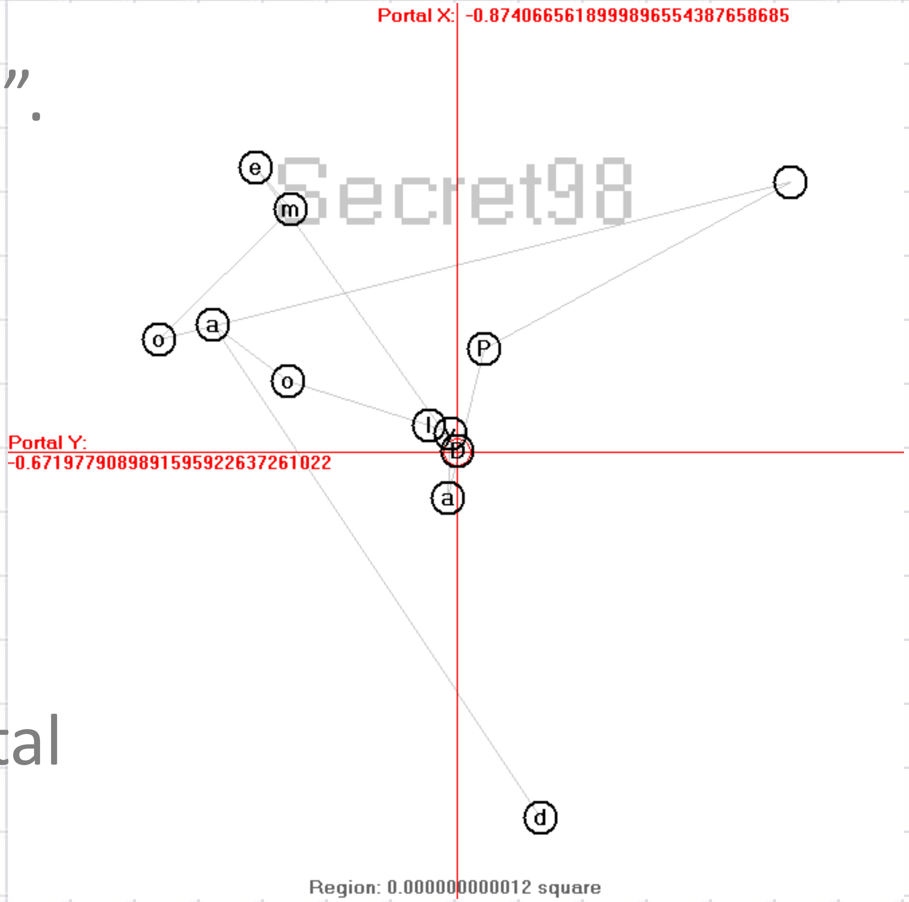
We repeat the process with Key “Secret98”.

By changing a single bit in the Key we:

1. Arrive at a different Fractal Portal
2. Traverse the fractal region differently
3. Generate different transform values

These elements are not predictable.

Each step must be processed and the fractal values and vectors discovered.

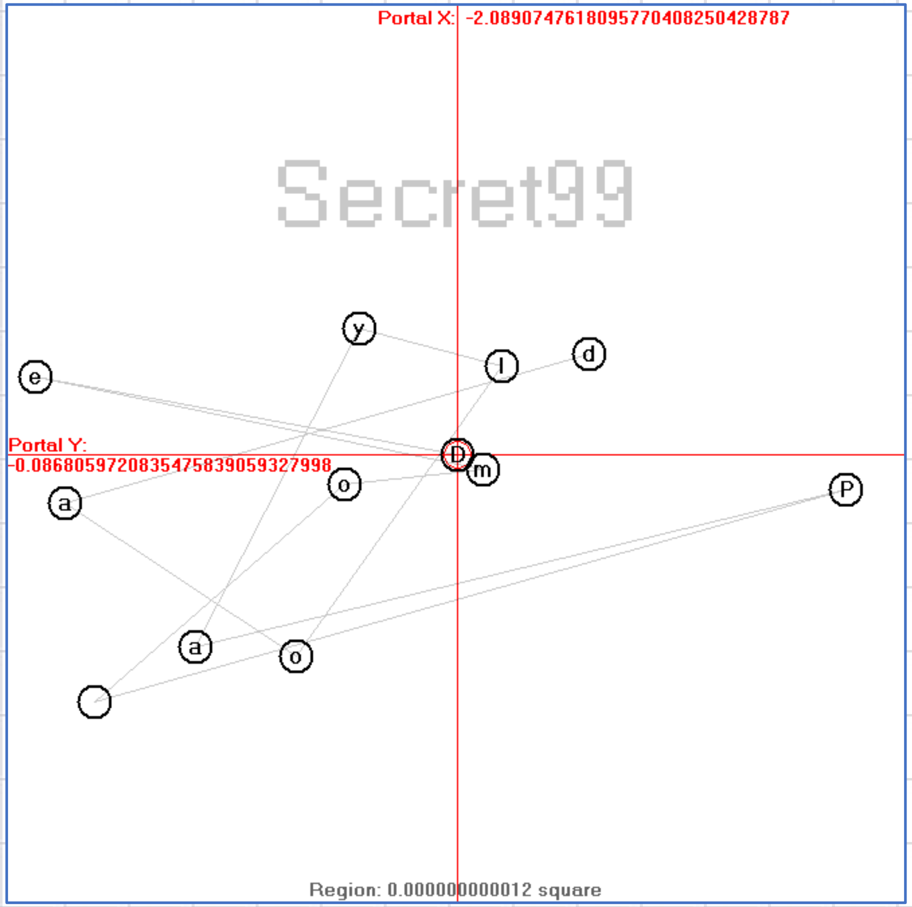

Portal X: -0.8740665618999896554387658685
Secret98
e
m
o
a
P
o
l
y
D
a
d
Portal Y:
-0.6719779089891595922637261022
Region: 0.000000000012 square

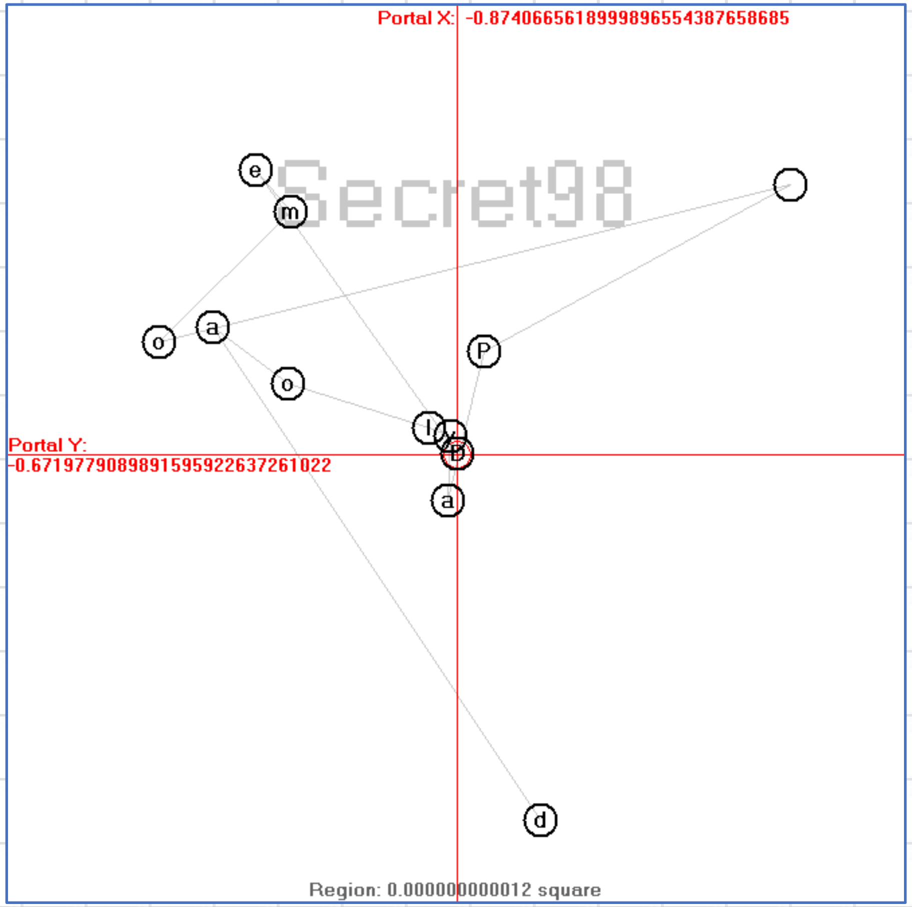
Compare Two Keys

Comparing "Secret99" and "Secret98" keys.

One bit change.

Entirely different portal location and totally unique transformation pattern


Portal X: -2.0890747618095770408250428787
Secret99
Portal Y:
-0.0868059720835475839059327998
y
l
d
e
D
m
o
a
P
a
o
Region: 0.000000000012 square


Portal X: -0.8740665618999896554387658685
Secret98
e
m
o
a
P
o
l
Portal Y:
-0.6719779089891595922637261022
a
d
Region: 0.000000000012 square

Multi-Dimensional Mandelbrot

Current **Fractal Transform** Technology implements a multi-dimensional version of the conventional 2D version shown in previous slides.

The transform iterations are computed in a similar manner, but they are applied to more dimensions.

The number of transform dimensions is configurable.

Each dimension expands the key-space by 112 bits.

The dimensions and associated key-space are involved end-to-end from key-portal mapping, through fractal stream generation to payload transformation.

Dynamic Fractal Navigation

Current **Fractal Transform** Technology implements a dynamic system of fractal navigation during fractal stream iterations.

Specifically, the angle and hypotenuse values use a dynamic modulo value instead of a fixed value indicated above.

An array is initialised with a randomly selected but fixed set of prime numbers to be used in the modulo function.

The modulo used for each angle and hypotenuse iteration is selected from the prime number array using the previous iteration value.

No structural relationship remains in transform iterations.

Fractal Transformation Outcome

The unique, unpredictable and infinite complexity of the Mandelbrot Fractal is engineered to transform the payload with a fractal stream that is also unique, unpredictable and infinitely complex.

There is zero determinism from the Key to the Fractal Portal.

There is zero determinism from one iteration to the next.

The entire payload is completely offset/overwritten by an unpredictable infinitely complex fractal stream.

The payload no longer exists in the cipher – it is impenetrable.

Contact

For further information please contact:

Wolfgang Flatow
CEO PORTALZ PTY LTD
+61 409 309 901
wolfgang.flatow@portalz.solutions