Novel Mechanism to Determine Pythagorean and Reciprocal Pythagorean Triplets to Generate Symmetric Keys in Cryptosystem

Dr. T. SRINIVAS [1] & K. UMADEVI [2]

1.Department of FME, Associate Professor, Audi Sankara Deemed to be University, Gudur bypass, Gudur, Tirupati. Email Id: drtsrinivas80@gmail.com

2. Assistant Professor in Mathematics, Visvesvaraya college of Engineering and Technology, Ibrahimpatnam, Telangana, India Email Id: umadevi975@gmail.com

Abstract: In this paper, a scheme for symmetric key generation based on Pythagorean and Reciprocal Pythagorean triple has been presented. The proposed scheme incorporates a Key Distribution center (KDC) for user authentication and secure exchange of secret information to generate keys. The proposed system is based on a novel mechanism to determine Pythagorean and Reciprocal Pythagorean triples to generate keys.

Keywords: Pythagorean triplet, Reciprocal Pythagorean triplet, Symmetric key, Cryptosystem, Diophantine equation

Introduction:

From the References [1],[2],[3],[4],[5],[6],[7],[8],[9],[10], Equations to be solved with integer values of the unknowns are now called Diophantine equations and the study of such equations is known as Diophantine Analysis. The equation $x^2 + y^2 = z^2$ for Pythagorean triples is an example of a Diophantine equation.

Various methods to Generating Pythagorean triple:
From References [10],[11],[12],[13],[14],[15],[16],[17],[18],[19],[20],[21],[22],[23],[24],[25],[26],[27] following results will be occurred

Case1: to Generate a Pythagorean Triple (x_1, x_2, x_3) for each x_1,there exists at least one x_2 and at least one x_3 , with $x_2 = \left|ax_1^2 - \frac{1}{4a}\right|$, $x_3 = \left|ax_1^2 + \frac{1}{4a}\right|$,

$$\text{where a} = \begin{cases} \left\{\frac{1}{2p}, p \text{ is a factor of } x_1^2, if\ x_1 \text{ is an odd} \right. \\ \left\{\frac{1}{4p}, p \text{ is a factor of } \left(\frac{x_1}{2}\right)^2, if\ x_1 \text{ is an even} \right. \end{cases}$$

Computer programming (c #) to Generate Pythagorean Triples for x is an odd integer from 3 to 100 as follows

For x is an odd integer:

Program:

```
var output = new List<Tuple<int, int, int, int, int>>();
var facts = new Dictionary<int, List<int>>();
for (int i = 3; i <=100; i++)
{
   //  for x is odd integer
   if (i % 2 != 0)
   {
      facts.Add(i, Factor(i*i));
   }
}
foreach (var item in facts)
{
   var x1= item.Key;
   foreach (var item2 in item.Value)
   {
      var p = item2;
      var n = (x1 * x1) / p;
      var x2 = Math.Abs((n - p) / 2);
      var x3 = (n + p) / 2;
      output.Add(Tuple.Create(x1, p, n, x2, x3));
   }
}
Console.WriteLine($"| x1  |  p  |  n  |  x2  |  x3   |  (x1,x2,x3)  ");
Console.WriteLine();
foreach (var item in output)
{
   Console.WriteLine($"|{item.Item1,5}|{item.Item2,5}|{item.Item3,5}| {item.Item4,5}|
{item.Item5,5} | {(item.Item1,item.Item4,item.Item5),5}  ");
}
```

```
List<int> Factor(int number)
{
    var factors = new List<int>();
    int max = (int)Math.Sqrt(number);  // Round down
    for (int factor = 1; factor <= max; ++factor) // Test from 1 to the square root, or the int below it,
inclusive.
    {
        if (number % factor == 0)
        {
            factors.Add(factor);
            if (factor != number / factor) // Don't add the square root twice!
                factors.Add(number / factor);
        }
    }
    return factors;
}
```

Computer programming (c #) to Generate Pythagorean Triples for x is an Even integer from 2 to 100 as follows

Program:

```
var output = new List<Tuple<int, int, int, int, int>>();
var facts = new Dictionary<int, List<int>>();
for (int i = 3; i <=100; i++)
{
    //  for x is Even integer
    if (i % 2 == 0)
    {
        facts.Add(i, Factor(((i/2) * (i/2)) ) );
    }
}
foreach (var item in facts)
{
    var x1= item.Key;
    foreach (var item2 in item.Value)
    {
        var p = item2;
        var n = (x1 * x1) / (4 *p);
        var x2 = Math.Abs(n - p) ;
```

```
        var x3 = (n + p);
        output.Add(Tuple.Create(x1, p, n, x2, x3));
    }
}
Console.WriteLine($"| x1  |  p  |  n  |  x2  |  x3   |  (x1,x2,x3)  ");
Console.WriteLine();
foreach (var item in output)
{
    Console.WriteLine($"|{item.Item1,5}|{item.Item2,5}|{item.Item3,5}| {item.Item4,5}|
{item.Item5,5} | {(item.Item1,item.Item4,item.Item5),5}  ");
}
List<int> Factor(int number)
{
    var factors = new List<int>();
    int max = (int)Math.Sqrt(number);  // Round down
    for (int factor = 1; factor <= max; ++factor) // Test from 1 to the square root, or the int below it,
inclusive.
    {
        if (number % factor == 0)
        {
            factors.Add(factor);
            if (factor != number / factor) // Don't add the square root twice!
                factors.Add(number / factor);
        }
    }
    return factors;
}
```

Case 1.3: Another Method to Generate Pythagorean Primitive Triple

Theorem: Choose a and b and $c^2 = 2ab$. Then $(a + c, b + c, a + b + c)$ is a Pythagorean Triple

Case 1.4: Introduce to Generate Pythagorean Triples with using of sequence of **Fibonacci numbers** as follows. Let $\emptyset : \mathbf{Z^2} \to \mathbf{Z^3}(\boldsymbol{P})$ with

$$\emptyset(\mathbf{F_n}, \mathbf{F_{n+1}}) = ((\mathbf{2F_{n+1}}(\mathbf{F_n} + \mathbf{F_{n+1}}), \mathbf{F_n}(\mathbf{2F_{n+1}} + \mathbf{F_n}), \mathbf{F_{n+1}^2} + (\mathbf{F_n} + \mathbf{F_{n+1}})^2).$$

From Reference [10], the sequence of Fibonacci numbers is $(\{\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{5},\mathbf{8},\mathbf{13},\mathbf{21}\ldots\ldots..\}$ following Recurrence Relation $\mathbf{F_n = F_{n-1} + F_{n-2}}$ **for** $\mathbf{n \geq 2}$, **with** $\mathbf{F_0 = 1}$, $\mathbf{F_1 = 1}$.

Case 1.5: Introduce to Generate Pythagorean Triples with using sequence of **Pell numbers** as follows.

Let $\boldsymbol{\varphi}: \mathbf{Z^2} \to \mathbf{Z^3}(\boldsymbol{P})$ with $\boldsymbol{\varphi}(\mathbf{P_n}, \mathbf{P_{n+1}}) = (2\boldsymbol{P_n}\boldsymbol{P_{n+1}}, \boldsymbol{P_{n+1}^2}$- $\mathbf{P_n^2}$,$\mathbf{P_{n+1}^2} + \mathbf{P_n^2})$.

Case 2: Generating Reciprocal Pythagorean Triples

The solutions of Diophantine Equation $\mathbf{x^n} + \mathbf{y^n} = \mathbf{z^n}$ are satisfies the Reciprocal Pythagorean Theorem RPT = $\left\{(x, y, z) \in z^3 : \frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}\right\}$ for $n = -2$.

The Reciprocal Pythagorean Theorem relates the two legs a, b to the altitude h is defined as follows $\frac{1}{a^2} + \frac{1}{b^2} = \frac{1}{h^2}$ with $c = \frac{ab}{h}$.

Now introduce a Method, to Generate a Set of Reciprocal Pythagorean Triples with using Euclid's methodology of Generation of a Pythagorean Triples.

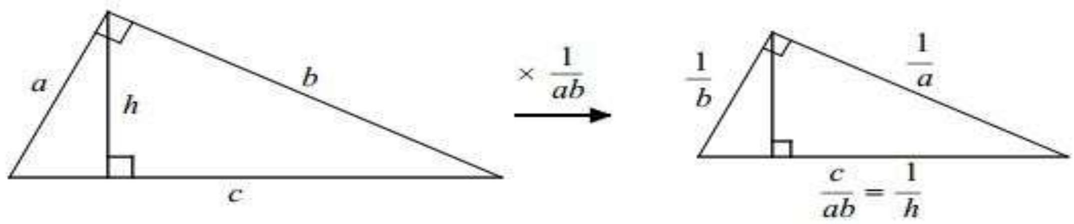

Figure 1: Reciprocal Pythagorean Theorem

Consider the Reciprocal Pythagorean Theorem $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$. It follows that $\frac{1}{x^2} = \frac{1}{z^2} - \frac{1}{y^2}$.

Again Simplify, $1 = \frac{x^2}{z^2} - \frac{x^2}{y^2}$. It will follow that $\left(\frac{x}{z} + \frac{x}{y}\right)\left(\frac{x}{z} - \frac{x}{y}\right) = 1$

The above equations must satisfy the following conditions for some positive integers p, q.

$$\frac{x}{z} + \frac{x}{y} = \frac{p}{q}, \quad \frac{x}{z} - \frac{x}{y} = \frac{q}{p}$$

From the above equations, $2x = z\left(\frac{p}{q} + \frac{q}{p}\right)$, $2x = y\left(\frac{p}{q} - \frac{q}{p}\right)$

Choose, two positive integers p, q ($p > q$), let x $= (p^2 + q^2)(p^2 - q^2)$.

It follows that $z = 2pq(p^2 - q^2)$ and $y = 2pq(p^2 + q^2)$

Consider $\frac{1}{x^2}+\frac{1}{y^2} = \frac{1}{((p^2+q^2)(p^2-q^2))^2}+\frac{1}{(2pq(p^2+q^2))^2} = \frac{1}{(2pq(p^2-q^2))^2} = \frac{1}{z^2}$

Computer programming to Generate a subset of the set of Reciprocal Pythagorean Triples $\mathbf{x = (p^2+q^2)(p^2-q^2), y = 2pq(p^2+q^2), z = 2pq(p^2-q^2)}$

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
int main()
{
   int p, q;
   double x, y, z;
   for(p=2; p<=30;p++)
   {
      for(q=2;q<=30;q++)
         {
            if( p > q)
            {
               x = ((pow(p,2) + pow(q,2)) * (pow(p,2) - pow(q,2)));
               y = 2 * p * q * (pow(p,2) + pow(q,2));
               z = 2 * p * q * (pow(p,2) - pow(q,2));
            printf("For p= %d, q= %d; Values of (x,y,z) are (%.2f, %.2f, %.2f) \n", p, q, x, y, z);
            }
         }
   }
   return 0;
}
```

Lemma 2.2: If (x, y, z) is a Pythagorean triple then then (y z, x z, z^2) is a Pythagorean triple.

Proof: Consider $(yz)^2+(xz)^2 = z^2(x^2+y^2) = z^4$. Hence (y z, x z, z^2) is a Pythagorean triple.

It follows that If (x, y, z) is a Pythagorean triple then (y z, x z, x y) is a Reciprocal Pythagorean triple and (y z, x z, z^2) is a Pythagorean triple. In this way we can generate Pythagorean and Reciprocal Pythagorean triple with same two legs. Some results are represented in below table

Corollary1: Now we can apply Lemma 1 to generate successively alternate Pythagorean and Reciprocal Pythagorean triples respectively

Main Work:

In the proposed system, three parties are involved in key exchange process. i.e

Key distribution center (KDC), source (A) and destination (B). If A wants to communicate with B using symmetric key encryption, a session must be created between them. A secret session key shared between and B is required for encryption of data in this session

Application of Pythagorean Triple in Cryptosystem

Key generation and Secure is critical to the security of a Cryptosystem. If fact key generation and key exchange is the most challenging part of cryptography. In this chapter, a scheme for symmetric key generation based on Pythagorean triple has been presented. The proposed scheme incorporates a Key Distribution centre (KDC) for user authentication and secure exchange of secret information to generate keys. The KDC operation involves a request from a user for initiation. The KDC authenticates authenticate and secure exchange of secret information to generate keys. The KDC authenticates the initiator. If the authentication is successful, KDC generates and sends an encrypted timestamp to both the initiator and responder.

The proposed system is based on a novel mechanism to determine Pythagorean triples to generate keys. The formula uses factors of x to generate y and z such that x , y , z satisfy the Pythagorean theorem.

The following notation has been used to Pythagorean triple calculation

x- input to calculate Pythagorean triple

p_1 - First prime factor of x, p_2 - Second Prime factor of x

y and z – Key Pair , Suppose, If x is odd then y = $\frac{|x^2-p_1^2|}{2p_1}$ and z= $\frac{|x^2+p_1^2|}{2p_1}$ the final key is computed by XORing y and z. i.e. p = y ⊕ z

In the proposed system, three parties are involved in key exchange process. i.e

Key distribution center (KDC), source (A) and destination (B). If A wants to communicate with B using symmetric key encryption, a session must be created between them. A secret session key shared between and B is required for encryption of data in this session.

Construction of Pythagorean triple for n-tuple:

The Pythagorean n-tuple, $x_1^2 + x_2^2 + x_3^2 + x_4^2 + \cdots .. + x_{n-1}^2 = x_n^2$ has used to construct a tree. A binary tree of height n has been generated whose leaf nodes are $x_i{}'s$, for $1 \le i \le n-1$ and the root is x_n. As illustrated in given Figure, the leaf nodes are [$x_1, x_2, x_3, \dots \dots . x_i, \dots . . x_{n-1}$] and the root is x_n which constitute the Pythagorean n-tuples [$x_1, x_2, x_3, \dots \dots . x_i, \dots . . x_{n-1}, x_n$] and satisfies the equation $x_1^2 + x_2^2 + x_3^2 + x_4^2 + \cdots .. + x_{n-1}^2 = x_n^2$.

The Procedure defined as follows:

Step 1: choose x_1 , where $x_1 > 3$;

Step 2: let t be a temporary variable initialized as follows;

t = x_1

Construct a binary tree (T) by taking t as the root, x_1 as the left child and x_2 as the right child which is calculated by applying step 3.

Step 3: for $1 \le i \le n-1$, apply generation of key element from above methods.

For suppose, $x_{i+1} = a(t)^2 - \frac{1}{4a}$

$p_i = a(t)^2 + \frac{1}{4a}$,where **a** = $\begin{Bmatrix} \left\{\frac{1}{2p}, p \text{ is a factor of } x_1^2, \text{if } x_1 \text{ is odd}\right. \\ \left\{\frac{1}{4p}, p \text{ is a factor of } \left(\frac{x_1}{2}\right)^2, \text{if } x_1 \text{ is even}\right. \end{Bmatrix}$

t = p_i

apply above algorithm to construct Pythagorean tree.

Some integer sequences are satisfied above properties are given below.

$$3^2 + 4^2 = 5^2$$

$$3^2 + 4^2 + 12^2 = 13^2$$

$$3^2 + 4^2 + 12^2 + 84^2 = 85^2$$

$$3^2 + 4^2 + 12^2 + 84^2 + 204^2 = 221^2$$

$$3^2 + 4^2 + 12^2 + 84^2 + 720^2 = 725^2$$

$$3^2 + 4^2 + 12^2 + 84^2 + 204^2 + 60^2 = 229^2$$

$$3^2 + 4^2 + 12^2 + 84^2 + 204^2 + 1428^2 = 1445^2$$

$$3^2 + 4^2 + 12^2 + 84^2 + 720^2 + 1740^2 = 1885^2,$$

$$3^2 + 4^2 + 12^2 + 84^2 + 204^2 + 1872^2 = 1885^2$$

$$3^2 + 4^2 + 12^2 + 84^2 + 720^2 + 2040^2 = 2165^2$$

Conclusion:

The proposed system is based on a novel mechanism to determine Pythagorean triples to generate keys. The formula uses factors of x to generate y and z such that x , y , z satisfy the Pythagorean theorem.

The following notation has been used to Pythagorean triple calculation

x- input to calculate Pythagorean triple

p_1 - First prime factor of x

p_2 - Second Prime factor of x

y and z – Key Pair

Suppose, If x is odd then y = $\frac{|x^2-p_1^2|}{2p_1}$ and z= $\frac{|x^2+p_1^2|}{2p_1}$ the final key is computed by XORing y and z. i.e. p = y ⊕ z

In the proposed system, three parties are involved in key exchange process. i.e

Key distribution center (KDC), source (A) and destination (B). If A wants to communicate with B using symmetric key encryption, a session must be created between them. A secret session key shared between and B is required for encryption of data in this session.

References:

[1] **https://mathworld.wolfrom.com/pythagorean triples**

[2] A new approach to generate all Pythagorean triples by Anthony Overmars, AIMS Mathematics, 4(2):242-253.

[3] A textbook “Introduction to Analytic Number Theory “by Tom M. Apostol, Springer.

[4] Pythagorean Triples- www.mathsisfun.com

[5] L.E. Dickson., 2005 History of the theory of numbers: Diophantine analysis, Dover publications,

[6] A Hattangadi Exploration in Mathematics, 3rd Edition India: University Press,2008

[7] A.K.Hazra Matrix: Algebra, Calculus and Generalised Inverse 2010

[8] Bhupendra Singh Advanced Abstract Algebra 2002

[9] David M. Burton Elementary Number theory, 2003

[10]. Sridevi, K., & **Srinivas, T.** (2023). Transcendental representation of Diophantine equation and some of its inherent properties. *Materials Today: Proceedings*, *80*, 1822-1825.

[11]. Sridevi, K., & **Srinivas, T.** (2023). Existence Of Inner Addition and Inner Multiplication On Set of Triangular Numbers and Some Inherent properties of Triangular Numbers. *Materials Today: Proceedings*, *80*, 1822-1825.

[12]. Sridevi, K., & **Srinivas, T.** (2023). Cryptographic coding To Define Binary Operation on Set of Pythagorean Triples. *Materials Today: Proceedings*, *80*, 1822-1825.

[13]. Srinivas, T., & Sridevi, K. (2022). Transcendental representation of Diophantine Equation $x^n + y^n = z^n$ to Generate At most All Pythagorean and Reciprocal Pythagorean Triples. *JOURNAL OF ALGEBRAIC STATISTICS*, *13*(2), 3600-3609.

[14]. Sridevi, K., & **Srinivas, T**. (2022). Algebraic Structure Of Reciprocal Pythagorean Triples. Advances And Applications In Mathematical Sciences, Volume 21, Issue 3, January 2022, P.1315-1327© 2022 Mili Publications, India 0974-6803.

[15]. Srinivas, T., & Sridevi, K. (2022, May). A New Approach to Define Length of Pythagorean Triples and Geometric Series Representation of Set of Pythagorean Triples. In *Journal of Physics: Conference Series* (Vol. 2267, No. 1, p. 012059).ISSN:1742-6596. IOP Publishing.

[16]. Srinivas, T., & Sridevi, K. (2022, January). A new approach to define a new integer sequences of Fibonacci type numbers with using of third order linear Recurrence relations. In *AIP Conference Proceedings* (Vol. 2385, No. 1, p. 130005).ISSN 1551-7616.

[17]. Srinivas, T., & Sridevi, K. (2021, November). A New approach to define Algebraic Structure and Some Homomorphism Functions on Set of Pythagorean Triples and Set of Reciprocal Pythagorean Triples " in JSR (Journal of Scientific Research) , Volume 65, Issue 9, November 2021, Pages 86-92.ISSN: 0447-9483.

[18]. Sridevi, K., & Srinivas, T. (2020). A new approach to define two types of binary operations on set of Pythagorean triples to form as at most commutative cyclic semi group. *Journal of Critical Reviews*, *7*(19), 9871-9878.

[19]. SRINIVAS,. T. (2020). Proof Of Fermat's Last Theorem By Choosing Two Unknowns in the Integer Solution Are Prime Exponents. *pacific international Journal*, *3*(4), 147-151. ISSN 2616-4825 [Online] 2663-8991 [Print] Volume number 03 , issue number 03

[20]. Srinivas, T., & Ashok Kumar. C (2024). Construction of Pythagorean and Reciprocal Pythagorean n-tuples in Accelerating Discoveries in Data Science and Artificial Intelligence II, Springer Proceedings in Mathematics & Statistics 438, https://doi.org/10.1007/978-3-031-51163-9_4

[21]. Srinivas, T., & Sridevi, K(2024). A new approach to determine constant coefficients in higher order linear recurrence relations and repeated steps of their residues with mth integer modulo of some Fibonacci type numbers in 3rd International Conference on Functional Materials, Manufacturing, and Performances, AIP Conf. Proc. 2986, 030177-1–030177-9; https://doi.org/10.1063/5.0192504

[22]. Srinivas T(2023), Symmetric Key generation And Tree Construction in Cryptosystem based on Pythagorean and Reciprocal Pythagorean Triples in QEIOS, https://doi.org/10.32388/MTTDWD

[23]. Srinivas T(2024), Additive and Multiplicative Operations on Set of Polygonal Numbers in QEIOS https://doi.org/10.32388/MY0OLE

[24].Srinivas T(2023), Some Inherent Properties of Pythagorean Triples In **Research Highlights In Mathematics And Computer Science Vol. 7**, 18 March 2023 , Page 156-169 Https://Doi.Org/10.9734/Bpi/Rhmcs/V7/18767d

PUBLISHED: 2023-03-18.

[25] Srinivas, T. (2024).Construction of Pythagorean and Reciprocal Pythagorean n-tuples. Springer Proceedings in Mathematics and Statistics.

[26] Srinivas, T. (2025). a book of Compact Mathematics for Undergraduate: Formulas & Identities-part I. BP international Publishers.

[27]. Srinivas,T.(2025). A Study on Integer Design of Exponential Solutions of Diophantine Equations $\alpha(X^4+Y^4)^2=(C^2+D^2)(Z^2+W^2)^2P^\beta$ With $\alpha>0$, $\beta=1,2,3,4,5,6,7$ and $x<y<w<z$. International Journal of Advanced Research in Science, Engineering and Technology Vol. 12, Issue 10, October 2025.

[28]. Srinivas,T.(2025). A Study on Integer Design of Exponential Solutions of Diophantine Equations $\alpha(X^4+Y^4)^2=(C^2+D^2)(Z^2+W^2)\ P^\beta$ With $\alpha>0$, $\beta=1,2,3,4,5,6,7$ and $x<y<w<z$. International Journal of Advanced Research in Science, Engineering and Technology Vol. 12, Issue 10, October 2025.

[29]. Srinivas,T.(2025). **A Study On Integer Design Of Solutions Of Diophantine Equation $\alpha(X^4+Y^4)^2(2U^2+V^2)=T^2(C^2+D^2)(Z^2-W^2)P^\beta$ With $\alpha>0,\beta=1,2,3,4,5,6,7$ *and* $x<y<w<z$, 2025 IJCRT | Volume 13, Issue 11 November 2025 | ISSN: 2320-2882.** [30].

[30]. Srinivas,T.(2025). **A Study On Integer Design Of Solutions Of Diophantine Equation $\alpha(X^4+Y^4)^2(2U^2+V^2)=T^2(C^2+D^2)(Z^2+W^2)P^\beta$ With $\alpha>0,\beta=1,2,3,4,5,6,7$ *and* $x<y<w<z$, 2025 IJCRT | Volume 13, Issue 11 November 2025 | ISSN: 2320-28**