Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 6s (2024)

Multi-Party Key Agreement Protocols using Conjugacy Search Problem in Five dimensional Discrete Heisenberg Group

N. Sundarakannan[1,*] ,T. Isaiyarasi[2], V. Nagarani[3], D. Captain Prabakaran[4], M.H.A. Aysha Chitukka[5]

1, 2, 3,4 Department of Mathematics, SRM Valliammai Engineering College, Kattangulathur, Chennai 603 203

[1] sundarakannann.maths@srmvalliammai.ac.in

[2] isaiyarasit.maths@srmvalliammai.ac.in

[3]nagaraniv.maths@srmvalliammai.ac.in

[4]captainprabakarand.maths@srmvalliammai.ac.in

[5]ayshachitukkamha.maths@srmvalliammai.ac.in

*Corresponding author : N. Sundarakannan

Article History:

Received: *18-06-2024*

Revised: *27-07-2024*

Accepted: *08-08-2024*

Abstract:

The secrete way of communicating information between entities is the science known as cryptography. In order to communicate the message through an insecure medium the communicating entities need a cryptographic keys. The process of getting a common shared key is the Key agreement Protocol. This paper proposes a multi party key agreement protocol which provides a common key between the communicating parties using conjugacy Search Problem (CSP). To implement this protocol a platform group is required. The five dimensional Discrete Heisenberg Group(DHG) is chosen as the platform group and the conjugacy search problem (CSP) taken from combinatorial group theory acts as the one way function. As a particular case a five party KAP with numerical computation is provided. In general, multiparty CSP with k communicating parties can get a common key in k-1 rounds.

Keywords: Cryptography, key agreement protocol, one way function, communicating party, discrete heisenberg group, conjugacy search problem.

1. Introduction:

Cryptography is the art of achieving security by encrypting the messages from the sender to the receiver which is made non-readable for others. The process of encoding plain text into cipher text message is called encryption. The reverse process of transforming cipher text called decryption. There are two cryptographic mechanism depends on the key used. If the same key is used for encryption and decryption it is called symmetric key cryptography or private key cryptography. If two different keys are used in a cryptographic mechanism where in one key is used for encryption and another key is used is used for decryption then it is called asymmetric key cryptography or public key cryptography. Key exchange protocol enable secure communication over an untrusted network by deriving and distributing shared keys between two or more parties. There are two type of key exchange protocols commonly known as Key transport protocol and Key agreement protocol. Key transport protocol is a key establishment protocol in which one of the principal generates the key and this key then transferred to all protocol users. Key agreement protocol is a key establishment protocol in which the session key is a function of inputs by all protocol users.

The public key cryptography system was introduced by Diffe at al.[6] in their article 'A new directions in cryptography'. In this a key agreement protocol was proposed with in which the discrete logarithm problem served as the one way function. In [5] Anshel et al. key agreement protocols were proposed using the search problems as the one way functions. In these protocols the Braid group was chosen as the platform group. In [7] T. Isaiyarasi T et al. proposed 'A New Multiparty Key Agreement Protocol using tripled decomposition search problem in Discrete Heisenberg Group' was proposed. T. Isaiyarasi et al.[9], A New Key Agreement Protocol using two layers of Security was proposed .In [11] 'Authenticated Key Agreement Protocol for HWSN Network' was proposed using factorization search problem.

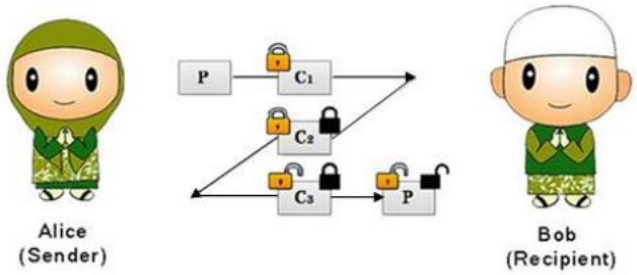


Figure 1. Scheme of Three-Pass Protocol

2. Definitions:

2.1 Discrete Heisenberg Group:

Let $\mathcal{H}$ be the set of all 5-tuples$(x_1, x_2, x_3, x_4, x_5)$ where $x_1, x_2, x_3, x_4, x_5 \in$, and $\cdot$ be the binary operation. The binary operation $\cdot$ is defined as follows

$$(x_1, x_2, x_3, x_4, x_5)\cdot(y_1, y_2, y_3, y_4, y_5)$$
$$= (x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3,\ x_4 + y_4,\ x_5 + y_5 + x_1y_3 + x_2y_4) \quad \text{---(1)}$$

It can be easily verified that the set $\mathcal{H}$ is a group but not abelian under this binary operation$\cdot$. For the cryptographic purpose we consider a finite group $\mathcal{H}$. When the modular arithmetic is introduced, this group can be made finite as follows:

$$(x_1, x_2, x_3, x_4, x_5)\cdot(y_1, y_2, y_3, y_4, y_5)$$
$$= (x_1 + y_1,\ x_2 + y_2, x_3 + y_3, x_4 + y_4, x_5 + y_5 + x_1y_3 + x_2y_4) mod\ p$$

Where$p$ is a prime number.

(i) The number of elements in $\mathcal{H} = Z_p$, $i.\ e.$, $(\mathcal{H}) = p^5$
(ii) Existence of Identity element :
For any $(x_1, x_2, x_3, x_4, x_5) \in \mathcal{H}$
$(x_1, x_2, x_3, x_4, x_5)\cdot$ (0,0,0,0,0) = $(x_1 + 0,\ x_2 + 0,\ x_3 + 0,\ x_4 + 0,\ x_5 + 0 + x_1.0 + x_2.0)$
$= (x_1, x_2, x_3, x_4, x_5)$

Also

$(0,0,0,0,0) \cdot (x_1, x_2, x_3, x_4, x_5) = (0 + x_1,\ 0 + x_2, 0 + \ x_3,\ 0 + x_4,\ 0 + x_5 + 0.x_3 + 0.x_4)$

$= (x_1, x_2, x_3, x_4, x_5)$

Therefore (0,0,0,0,0) is the identity element of $\mathscr{H}$

(iii) Existence of Inverse element :

For any $(x_1, x_2, x_3, x_4, x_5) \in \mathscr{H}$, its inverse is computed as follows.

$$(x_1, x_2, x_3, x_4, x_5) \cdot (y_1, y_2, y_3, y_4, y_5) = (0,0,0,0,0)$$

$\Rightarrow (x_1 + y_1,\ x_2 + y_2,\ x_3 + y_3,\ x_4 + y_4,\ x_5 + y_5 + x_1y_3 + x_2y_4) = (0,0,0,0,0)$

$\Rightarrow x_1 + y_1 = 0\ ,\ x_2 + y_2 = 0,\ x_3 + y_3 = 0\ ,\ x_4 + y_4 = 0\ ,\ x_5 + y_5 + x_1y_3 + x_2y_4 = 0$

$\Rightarrow \quad y_1 = -x_1, y_2 = -x_2,\ y_3 = -x_3,\ y_4 = -x_4,\ y_5 = -x_5 + x_1x_3 + x_2x_4$

$\therefore (x_1, x_2, x_3, x_4, x_5)^{-1} = (-x_1,\ -x_2, -x_3, -x_4, -x_5 + x_1x_3 + x_2x_4) mod\ p$

(iv) $(x_1, x_2, x_3, x_4, x_5)^n = (nx_1,\ nx_2,\ nx_3,\ nx_4,\ nx_5 + n^2(x_1x_3 + x_2x_4)) mod\ p$

This can be proved by mathematical induction

2.2 Conjugacy serach problem :

The conjugacy search problem (CSP): Given a recursive presentation of a group G and two conjugate elements $x, y \in G$, find a particular element $g \in G$ such that $g^{-1}xg = y$.

2.3 Conjugacy search problem in discrete Heisenberg group:

The elements of the conjugacy search problem are chosen from the discrete heisenberg group $\mathscr{H}$ with condition be described below for two party protocol and generate the common public key.

Two parties A_1 and A_2 agree on a finite non-abelian group, discrete heisenberg group $\mathcal{H} = Z_p^5$ and A_1 publishes an element $x \in \mathcal{H}$ such that x does not commute with g_1 and g_2.

A_1 chooses an element $g_1 \in G_1$, computes ${g_1}^{-1}xg_1$ and sends it to A_2

A_2 chooses an element $g_2 \in G_1$, computes ${g_2}^{-1}xg_2$ and sends it to A_1

On knowing g_1 , A_1 computes $K_A = {g_1}^{-1}{g_2}^{-1}xg_2g_1$.

On knowing g_2, A_2 computes $K_B = {g_2}^{-1}{g_1}^{-1}xg_1g_2$.

$K_A = K_B$ is there common shared key.

2.4 Commutative condition:

Let us consider $g_1 = (x_1, x_2, x_3, x_4, x_5)$ and $g_2 = (y_1, y_2, y_3, y_4, y_5)$

$$g_1.g_2 = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4, x_5 + y_5 + x_1y_3 + x_2y_4) mod\ p$$

And $g_2.g_1 = (y_1 + x_1, y_2 + x_2, y_3 + x_3, y_4 + x_4, y_5 + x_5 + y_1x_3 + y_2x_4) mod\ p$

If $g_1.g_2 = g_2.g_1$ then for 5-tuple be identically equal. So first four values are exactly equal.

But for fifth value is equal if $x_1y_3 + x_2y_4 = y_1x_3 + y_2x_4$.

2.5 Inverse element:

The inverse of $g_1$and $g_2$are $g_1^{-1} = (-x_1, -x_2, -x_3, -x_4, -x_5 + x_1x_3 + x_2x_4)$

and $g_2^{-1} = (-y_1, -y_2, -y_3, -y_4, -y_5 + y_1y_3 + y_2y_4)$

Now

$g_1^{-1}.g_2^{-1} = (-x_1 - y_1, -x_2 - y_2, -x_3 - y_3, -x_4 - y_4, -x_5 - y_5 + (-x_1)(-y_3) + (-x_2)(-y_4))$

$= (-(x_1 + y_1), -(x_2 + y_2), -(x_3 + y_3), -(x_4 + y_4), -(x_5 + y_5) + x_1y_3 + x_2y_4)$

And

$$g_2^{-1}.g_1^{-1} = (-y_1 - x_1, -y_2 - x_2, -y_3 - x_3, -y_4 - x_4, -y_5 - x_5 + (-y_1)(-x_3) + (-y_2(-x_4))$$
$$= (-(y_1 + x_1), -(y_2 + x_2), -(y_3 + x_3), -(y_4 + x_4), -(y_5 + x_5) + y_1x_3 + y_2x_4)$$

If $g_1^{-1}.g_2^{-1} = g_2^{-1}.g_1^{-1}$ then we have $x_1y_3 + x_2y_4 = y_1x_3 + y_2x_4$.

Hence, The above result provides that "If $g_1$and g_2 are commute each other then their inverse also commute each other".

2.6 N tractability:

Given $x, y \in \mathcal{H}$, find g such that $g^{-1}x\, g = y$.

Let $x = (x_1, x_2, x_3, x_4, x_5) y = (y_1, y_2, y_3, y_4, y_5)$ and $g = (g_1, g_2, g_3, g_4, g_5)$

$$g^{-1}x\, g = (-g_1, -g_2, -g_3, -g_4, -g_5 + g_1g_3 + g_2g_4)(x_1, x_2, x_3, x_4, x_5)(g_1, g_2, g_3, g_4, g_5)$$
$$= (-g_1 + x_1 + g_1, -g_2 + x_2 + g_2, -g_3 + x_3 + g_3, -g_4 + x_4 + g_4,$$
$$-g_5 + x_5 + g_5 + g_1g_3 + g_2g_4 - g_1x_3 - x_4g_4 + (-g_1 + x_1)g_3$$
$$+ (-g_2 + x_2)g_4)\ mod\ p$$
$$= (x_1, x_2, x_3, x_4, x_5 - g_1x_3 - g_2x_4 + x_1g_3 + x_2g_4) \qquad \text{----(2)}$$

Now, $y_5 = x_5 - g_1x_3 - g_2x_4 + x_1g_3 + x_2g_4$

$$y_5 - x_5 = -g_1x_3 - g_2x_4 + x_1g_3 + x_2g_4$$

Suppose that $y_5 - x_5 = 0$ then $g_1x_3 + g_2x_4 = x_1g_3 + x_2g_4$

To obtain the values of g_1, g_2, g_3, g_4 by using the above single equation is very hard problem in DHG.

3. Five party key agreement protocol using CSP:

3.1 Protocol:

Five parties A_1, A_2, A_3, A_4, A_5 agree on a finite non-abelian group, discrete heisenberg group $\mathcal{H} = Z_p^5$

One of the five party publishes an element$x \in \mathcal{H}$.

A_1 chooses an element $g_1 \in \mathcal{H}$, such that $xg_1 \neq g_1x$

A_2 chooses an element $g_2 \in \mathcal{H}$, such that $xg_2 \neq g_2x$

A_3 chooses an element $g_3 \in \mathcal{H}$, such that $xg_3 \neq g_3x$

A_4 chooses an element $g_4 \in \mathcal{H}$, such that $xg_4 \neq g_4x$

A_5 chooses an element $g_5 \in \mathcal{H}$, such that $xg_5 \neq g_5x$

Also , g_1, g_2, g_3, g_4, g_5 are commute each other.

Round 1:

A_1 chooses an element $g_1 \in \mathcal{H}$, computes $K_{11} = {g_1}^{-1}xg_1$ and sends it to A_2

A_2 chooses an element $g_2 \in \mathcal{H}$, computes $K_{12} = {g_2}^{-1}xg_2$ and sends it to A_3

A_3 chooses an element $g_3 \in \mathcal{H}$, computes $K_{13} = {g_3}^{-1}xg_3$ and sends it to A_4

A_4 chooses an element $g_4 \in \mathcal{H}$, computes $K_{14} = {g_4}^{-1}xg_4$ and sends it to A_5

A_5 chooses an element $g_5 \in \mathcal{H}$, computes $K_{15} = {g_5}^{-1}xg_5$ and sends it to A_1

Round 2:

A_1 computes $K_{21} = {g_1}^{-1}K_{15}g_1$ and sends it to A_2

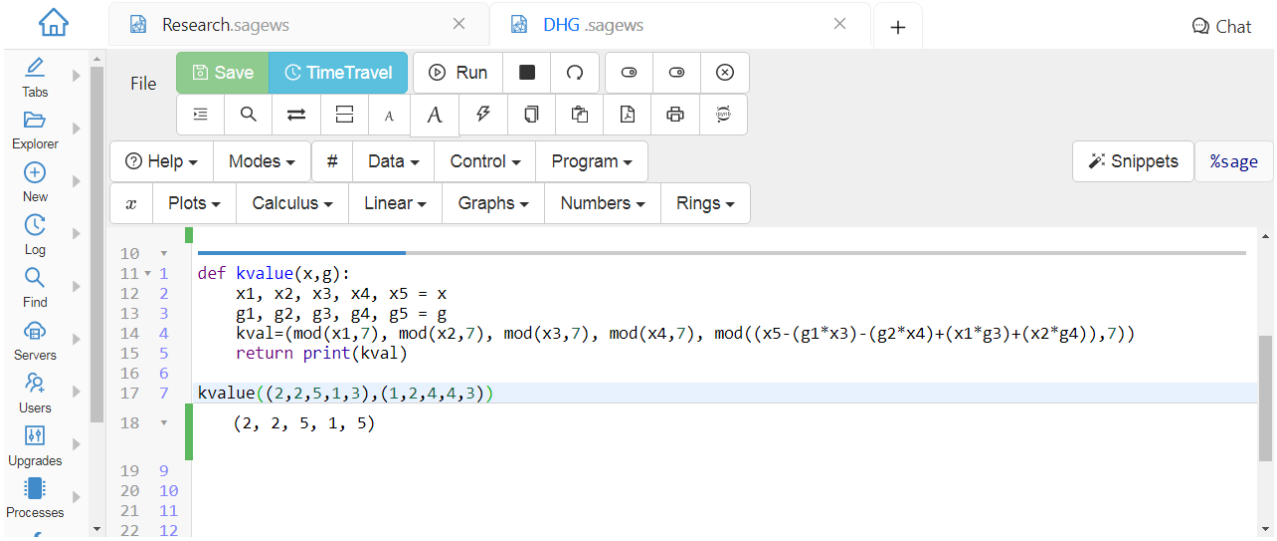
A_2 computes $K_{22} = {g_2}^{-1}K_{11}g_2$ and sends it to A_3

A_3 computes $K_{23} = {g_3}^{-1} K_{12} g_3$ and sends it to A_4
A_4 computes $K_{24} = {g_4}^{-1} K_{13} g_4$ and sends it to A_5
A_5 computes $K_{25} = {g_5}^{-1} K_{14} g_5$ and sends it to A_1
Round 3:
A_1 computes $K_{31} = {g_1}^{-1} K_{25} g_1$ and sends it to A_2
A_2 computes $K_{32} = {g_2}^{-1} K_{11} g_2$ and sends it to A_3
A_3 computes $K_{33} = {g_3}^{-1} K_{22} g_3$ and sends it to A_4
A_4 computes $K_{34} = {g_4}^{-1} K_{23} g_4$ and sends it to A_5
A_5 computes $K_{35} = {g_5}^{-1} K_{24} g_5$ and sends it to A_1
.Round 4:
A_1 computes $K_{41} = {g_1}^{-1} K_{35} g_1$ and sends it to A_2
A_2 computes $K_{42} = {g_2}^{-1} K_{31} g_2$ and sends it to A_3
A_3 computes $K_{43} = {g_3}^{-1} K_{32} g_3$ and sends it to A_4
A_4 computes $K_{44} = {g_4}^{-1} K_{33} g_4$ and sends it to A_5
A_5 computes $K_{45} = {g_5}^{-1} K_{34} g_5$ and sends it to A_1
Computation of KEY:
On knowing g_1 , A_1 computes $K_{A1} = {g_1}^{-1} K_{45}\, g_1$.
On knowing g_2 , A_2 computes $K_{A2} = {g_2}^{-1} K_{41}\, g_2$.
On knowing g_3 , A_3 computes $K_{A3} = {g_3}^{-1} K_{42}\, g_3$
On knowing g_4 , A_4 computes $K_{A4} = {g_4}^{-1} K_{43}\, g_4$.
On knowing g_5 , A_5 computes $K_{A5} = {g_5}^{-1} K_{44}\, g_3$
$K_{A1} = K_{A2} = K_{A3} = K_{A4} = K_{A5}$ is their common shared key.

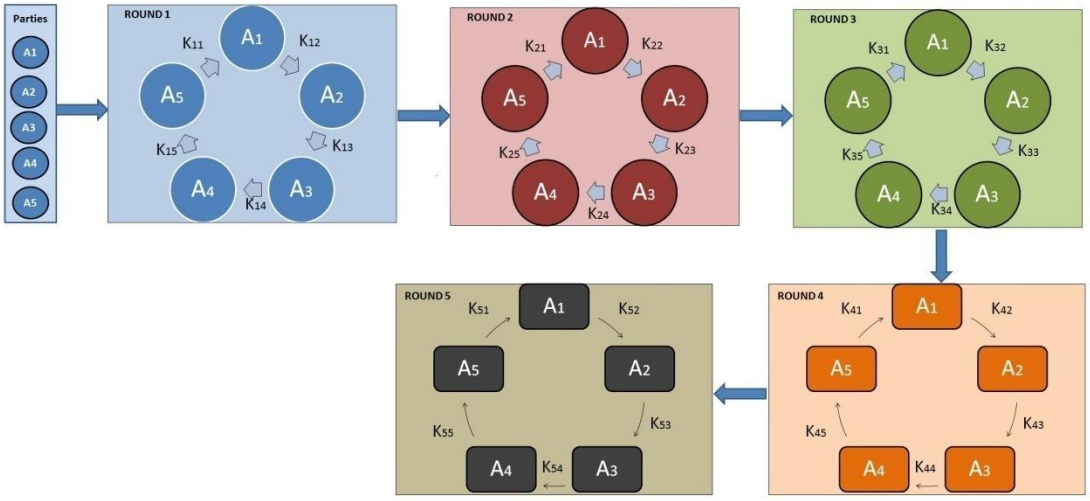
3.2 Algorithm :

SAGE Code for computing binary operation x*y in equation (1) is given below
Enter the values : def multiply(x,y):
x1,x2,x3,x4,x5 = x
y1,y2,y3,y4,y5 = y
sum=(mod((x1+y1),7),mod((x2+y2),7),mod((x3+y3),7),mod((x4+y4),7),
mod((x5+y5+(x1*y3)+(x2*y4)),7))
return print(sum)
multiply((2,2,5,1,3),(1,2,4,4,3))
multiply((1,2,4,4,3),(2,2,5,1,3)).
The program is given as follows
SAGE code for computing K_{ij} values as given below
Enter the values : def kvalue(x,g):
x1, x2, x3, x4, x5 = x
g1, g2, g3, g4, g5 = g
kval=(mod(x1,7), mod(x2,7), mod(x3,7), mod(x4,7), mod((x5-(g1*x3)-
(g2*x4)+(x1*g3)+(x2*g4)),7))
return print(kval)

The program is given as follows



3.3 Flow chart :



4. Numerical Example:

Consider the five parties A_1, A_2, A_3, A_4, A_5agree on a finite non-abelian group, Discrete Heisenberg group $\mathcal{H} = Z_7^5$ and one of the public key is $x = (2,2,5,1,3) \in \mathcal{H} = Z_7^5$

A_1 chooses an element $g_1 = (1,2,4,4,3) \in Z_7^5$, such that $xg_1 \neq g_1x$

A_2 chooses an element $g_2 = (3,1,4,6,2) \in Z_7^5$, such that $xg_2 \neq g_2x$

A_3 chooses an element $g_3 = (3,4,6,4,6) \in Z_7^5$, such that $xg_3 \neq g_3x$

A_4 chooses an element $g_4 = (1,0,5,3,1) \in Z_7^5$, such that $xg_4 \neq g_4x$

A_5 chooses an element $g_5 = (6,2,1,5,1) \in Z_7^5$, such that $xg_5 \neq g_5x$

Also g_1, g_2, g_3, g_4, g_5 are commute each other.

Round 1:

A_1 chooses an element $g_1 = (1,2,4,4,3) \in Z_7^5$ and computes

$$K_{11} = {g_1}^{-1}xg_1 = (6,5,3,3,2)(2,2,5,1,3)(1,2,4,4,3)$$

$= (2, 2, 5, 1, 5)$and sends it to A_2

A_2 chooses an element $g_2 = (3, 1, 4, 6, 2) \in Z_7^5$computes

$K_{12} = {g_2}^{-1} x g_2 = (4, 6, 3, 1, 2)(2, 2, 5, 1, 3)(3, 1, 4, 6, 2)$

$=(2, 2, 5, 1, 0)$and sends it to A_3

A_3 chooses an element $g_3 = (3, 4, 6, 4, 6) \in Z_7^5$computes

$K_{13} = {g_3}^{-1} x g_3 = (4, 3, 1, 3, 0)(2, 2, 5, 1, 3)(3, 4, 6, 4, 6)$

$= (2, 2, 5, 1, 4)$and sends it to A_4

A_4 chooses an element $g_4 = (1, 0, 5, 3, 1) \in Z_7^5$computes

$K_{14} = {g_4}^{-1} x g_4 = (6, , 0, 2, 4, 4)(2, 2, 5, 1, 3)(1, 0, 5, 3, 1)$

$= (2, 2, 5, 1, 0)$and sends it to A_5

A_5 chooses an element $g_5 = (6, 2, 1, 5, 1) \in Z_7^5$computes

$K_{15} = {g_5}^{-1} x g_5 = (1, 5, 6, 2, 1)(2, 2, 5, 1, 3)(6, 2, 1, 5, 1)$

$= (2, 2, 5, 1, 4)$and sends it to A_1

Round 2:

A_1 computes $K_{21} = {g_1}^{-1} K_{15} g_1 = (6, 5, 3, 3, 2)(2, 2, 5, 1, 4)(1, 2, 4, 4, 3)$

$= (2, 2, 5, 1, 6)$ and sends it to A_2

A_2 computes $K_{22} = {g_2}^{-1} K_{11} g_2 = (4, 6, 3, 1, 2)(2, 2, 5, 1, 5)(3, 1, 4, 6, 2)$

$= (2, 2, 5, 1, 2)$ and sends it to A_3

A_3 computes $K_{23} = {g_3}^{-1} K_{12} g_3 = (4, 3, 1, 3, 0)(2, 2, 5, 1, 0)(3, 4, 6, 4, 6)$

$= (2, 2, 5, 1, 1)$ and sends it to A_4

A_4 computes $K_{24} = {g_4}^{-1} K_{13} g_4 = (6, , 0, 2, 4, 4)(2, 2, 5, 1, 4)(1, 0, 5, 3, 1)$

$= (2, 2, 5, 1, 1)$ and sends it to A_5

A_5 computes $K_{25} = {g_5}^{-1} K_{14} g_5 = (1, 5, 6, 2, 1)(2, 2, 5, 1, 0)(6, 2, 1, 5, 1)$

$= (2, 2, 5, 1, 1)$ and sends it to A_1

Round 3:

A_1 computes $K_{31} = {g_1}^{-1} K_{25} g_1 = (6, 5, 3, 3, 2)(2, 2, 5, 1, 1)(1, 2, 4, 4, 3)$

$= (2, 2, 5, 1, 3)$ and sends it to A_2

A_2 computes $K_{32} = {g_2}^{-1} K_{11} g_2 = (4, 6, 3, 1, 2)(2, 2, 5, 1, 6)(3, 1, 4, 6, 2)$

$= (2, 2, 5, 1, 3)$ and sends it to A_3

A_3 computes $K_{33} = {g_3}^{-1} K_{22} g_3 = (4, 3, 1, 3, 0)(2, 2, 5, 1, 2)(3, 4, 6, 4, 6)$

$= (2, 2, 5, 1, 3)$ and sends it to A_4

A_4 computes $K_{34} = {g_4}^{-1} K_{23} g_4 = (6, , 0, 2, 4, 4)(2, 2, 5, 1, 1)(1, 0, 5, 3, 1)$

$= (2, 2, 5, 1, 5)$ and sends it to A_5

A_5 computes $K_{35} = {g_5}^{-1} K_{24} g_5 = (1, 5, 6, 2, 1)(2, 2, 5, 1, 1)(6, 2, 1, 5, 1)$

$= (2, 2, 5, 1, 2)$ and sends it to A_1

Round 4:

A_1 computes $K_{41} = {g_1}^{-1} K_{35} g_1 = (6, 5, 3, 3, 2)(2, 2, 5, 1, 2)(1, 2, 4, 4, 3)$

$= (2, 2, 5, 1, 4)$ and sends it to A_2

A_2 computes $K_{42} = {g_2}^{-1} K_{31} g_2 = (4, 6, 3, 1, 2)(2, 2, 5, 1, 3)(3, 1, 4, 6, 2)$

$= (2, 2, 5, 1, 0)$ and sends it to A_3

A_3 computes $K_{43} = {g_3}^{-1} K_{32} g_3 = (4, 3, 1, 3, 0)(2, 2, 5, 1, 3)(3, 4, 6, 4, 6)$

$= (2, 2, 5, 1, 4)$ and sends it to A_4

A_4 computes $K_{44} = {g_4}^{-1} K_{33} g_4 = (6, , 0, 2, 4, 4)(2, 2, 5, 1, 3)(1, 0, 5, 3, 1)$

$= (2, 2, 5, 1, 0)$ and sends it to A_5

A_5 computes $K_{45} = {g_5}^{-1} K_{34} g_5 = (1, 5, 6, 2, 1)(2, 2, 5, 1,5)(6, 2, 1, 5, 1)$

$= (2, 2, 5, 1, 6)$ and sends it to A_1

Computation of KEY:

On knowing g_1 , A_1 computes $K_{A1} = {g_1}^{-1} K_{45}\, g_1 = (6, 5, 3, 3, 2)(2, 2, 5, 1, 6)(1, 2, 4, 4, 3)$
$= (2, 2, 5, 1, 1).$

On knowing g_2 , A_2 computes $K_{A2} = {g_2}^{-1} K_{41}\, g_2 = (4, 6, 3, 1, 2)(2, 2, 5, 1, 4)(3, 1, 4, 6, 2)$
$= (2, 2, 5, 1, 1).$

On knowing g_3 , A_3 computes $K_{A3} = {g_3}^{-1} K_{42}\, g_3 = (4, 3, 1, 3, 0)(2, 2, 5, 1, 0)(3, 4, 6, 4, 6)$
$= (2, 2, 5, 1, 1)$

On knowing g_4 , A_4 computes $K_{A4} = {g_4}^{-1} K_{43}\, g_4 = (6, , 0, 2, 4, 4)(2, 2, 5, 1, 4)(1, 0, 5, 3, 1)$
$= (2, 2, 5, 1, 1)$

On knowing g_5 , A_5 computes $K_{A5} = {g_5}^{-1} K_{44}\, g_3 = (1, 5, 6, 2, 1)(2, 2, 5, 1{,}0)(6, 2, 1, 5, 1)$
$= (2, 2, 5, 1, 1)$

$K_{A1} = K_{A2} = K_{A3} = K_{A4} = K_{A5} = (2, 2, 5, 1, 1)$ is their common shared key.
This key has been utilized further for encryption or decryption.

Public Key	$\mathbf{g_i}$	$\mathbf{K_{ij}}$ **of Round 1**	$\mathbf{K_{ij}}$ **of Round 2**	$\mathbf{K_{ij}}$ **of Round 3**	$\mathbf{K_{ij}}$ **of Round 4**	**Computation key**
$x = (2, 2, 5, 1, 3)$	$(1, 2, 4, 4, 3)$	$(2, 2, 5, 1, 5)$	$(2, 2, 5, 1, 6)$	$(2, 2, 5, 1, 3)$	$(2, 2, 5, 1, 4)$	$(2, 2, 5, 1, 1)$
	$(3, 1, 4, 6, 2)$	$(2, 2, 5, 1, 0)$	$(2, 2, 5, 1, 2)$	$(2, 2, 5, 1, 3)$	$(2, 2, 5, 1, 0)$	$(2, 2, 5, 1, 1)$
	$(3, 4, 6, 4, 6)$	$(2, 2, 5, 1, 4)$	$(2, 2, 5, 1, 1)$	$(2, 2, 5, 1, 3)$	$(2, 2, 5, 1, 4)$	$(2, 2, 5, 1, 1)$
	$(1, 0, 5, 3, 1)$	$(2, 2, 5, 1, 0)$	$(2, 2, 5, 1, 1)$	$(2, 2, 5, 1, 5)$	$(2, 2, 5, 1, 0)$	$(2, 2, 5, 1, 1)$
	$(6, 2, 1, 5, 1)$	$(2, 2, 5, 1, 4)$	$(2, 2, 5, 1, 1)$	$(2, 2, 5, 1, 2)$	$(2, 2, 5, 1, 6)$	$(2, 2, 5, 1, 1)$

5. Perfect forward secrecy in the proposed KAP:

The long term key in this protocol is the common key arrived by the communicating entities. The common key is arrived in k-1 rounds for k entities. At each round the entities use their private keys to find the public key. The public key thus obtained is communicated to the next entity. The same procedure is taken over by all the entities. At each round the entities use CSP to arrive their public key. The Intractability of CSP is discussed and it is proven to be secure against the attacks. Thus even if the common key is compromised, the session keys at each round cannot be compromised. The proposed KAP has the perfect forward secrecy. In the proposed KAP, the common key is arrived at the k^{th} round by the *k*-Communicating parties. At each round the communicating parties use their private keys to compute a public key for that round and sends to the other party. If suppose a passive adversary managed to get the public key of one entity, in a particular round, he cannot take part in the communications between the entities. As at each round the communicating entities use their private keys to take part in the process, the adversary is not a le to join the process. The public key is activated by means of CSP in DHG, which is hard to attack. Thus even if the passive adversary managed to get the public key of any particular entity at any particular round he cannot take part in the future process. Thus this KAP is secure against the known key attack.

Unknown key share:

An unknown key-share attack on an authenticated key agreement protocol is an Attack where by an entity A ends up believing, it shares a key with another entity B and although this is in fact the case that B mistakenly believes the key is instead shared with an entity C ≠ A. The communicating entities may share the key with same other entity with the belief that he/she is sharing with intended parties. But the adversary has to take part in all rounds to act as the intended party. If it is possible then the KAP is vulnerable unknown key share attack. This may have been overcome by proper authentication.

No Key Control:

Neither entity should be able to force the session key to a value of his choice. Clearly key Control is not possible in the present KAP. As the common key is arrived with the participation of all the communicating parties at each round. Thus this KAP has no key control to any particular entity.

6. Recent Works:

The finite dimensional left translation invariant linear spaces of continuous complex valued functions over the Heisenberg group is discussed by Laszlo Szekelyhidi [12] to improve the frame of reference of group. The problem of finding a secure class of nonabelian groups for use as platforms is open and a subject of active research. A polynomial time solution of the CSP in an important class of non-abelian groups, the extraspecial *p*-groups and the reduction of the CSP in certain types of central products will be discussed by Simran Tinani [13].

7. CONCLUSION:

In this paper a new multi party key agreement protocol is proposed. The conjugacy search problem taken up the role of one way function . This is implemented in a five dimentional discrete Heinsenberg Group which is a non-abelian platform. The computation of *k* values and choosing *g* which is not commutative with *x* to be done by the SageMath algorithm. The interactability of conjugacy search problems also demonstrated. In this multiparty key agreement protocol entities arrive at a common key in k-1 rounds. Also this protocol satisfies the necessary security attributes for KAP. A numerical example for five party KAP is illustrated in this paper.

Other search problem such as decomposition search problem, Triple decomposition search problem and twisted conjugacy search problem etc, may also be used to describe a KAP. Any suitable platform group may also be applied to arrive at a common key. The DHG also considered as extraspecial p-group or complex group be the extension of this work and it will give more significant results.

References:

[1] Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov, ‘Group Based Cryptography’, CRM, BirkhäuserVerlag, Basel, Boston, Berlin. 2007.

[2] Alfred Menezes, Paul Van Oorschot, Scott Vanstone, ‘A Handbook of Applied Cryptography’,CRC Press Series on Discrete Mathematics and Its Applications. 1996.

[3] Andrej Bordnik, Aleksander Malnič and Rok Požar,’The simultananeous conjugacy problem in the symmetric group’, Math. Comp. **90** (2021), 2977-2995

[4] Andre Carvalho,'On generalized conjugacy and some related problems', Communications in Algebra, 51(8)3528-3542, 2023.

[5] I.Anshel, M.Anshel, and D.Goldfeld, 'An algebraic method for public-key cryptography',Mathematical Research Letters, 6 (1999), 287–291.

[6] Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactionsion Information Theory, 22(6) 1976, 644–654.

[7] T.Isaiyarasi, K.Sankarasubramanian, A New Multiparty Key Agreement Protocol using triple decomposition search problem in Discrete Heisenberg Group, International Journal of Computer Engineering and Information Technology, 4(6) 2013, 09-15.

[8] T.Isaiyarasi, K.Sankarasubramanian, Tripartite Key Agreement Protocol using TripleDecomposition Search Problem, International Journal on Cryptography and InformationSecurity, 2(1)2012, 49-55.

[9] T.Isaiyarasi, K.Sankarasubramanian, A New Key Agreement Protocol using two layers ofSecurity, Journal of Discrete Mathematical Sciences and Cryptography, 15(2 & 3) 2013,125-133.

[10] T.Isaiyarasi,K.Sankarasubramanian, A New Multiparty Key Agreement Protocol using searchProblems in Discrete Heisenberg Group, Indian Journal of Computer Science and Engineering,SSN 2231-3850, 3(1)2012, 154-161.

[11] T.Isiayarasi, .S. Chitra, 'Authenticated Key Agreement Protocol for HWSN Network', A Journal of Composition Theory, 14(2)2021, 153-164.

[12] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, 'An introduction to Mathematical Cryptography', Springer, 2014.

[13] Laszlo Szekelyhidi, 'Finite dimensional varieties over the Heisenberg group', Aequationes Mathematicae, 97 , 2022, 377–390.

[14] Peter J., 'Automorphisms of the Discrete Heisenberg Group', mathSG(Simpletic Geomentry) ,6,2004 .

[15] Simran Tinani, 'On Conjugacy Search Problem in Extraspecial p- Group', cs.CR.2022.

[16] Simran Tinani, 'Solutions to the Conjugacy Search Problem in Various Platform Groups', WCC 2022: The Twelfth International Workshop on Coding and Cryptography, 2022.

[17] M Palanikumar, K Arulmozhi, Novel possibility Pythagorean interval valued fuzzy soft set method for a decision making, TWMS J. App. and Eng. Math. V.13, N.1, 2023, pp. 327-340.

[18] M Palanikumar, O Al-Shanqiti, C Jana, M Pal, Novelty for Different Prime Partial Bi-Ideals in Non-Commutative Partial Rings and Its Extension, Mathematics 11 (6), 1309, 2023.

[19] M Palanikumar, C Jana, M Pal, V Leoreanu-FoteaOn Various 2-absorbing prime ideals in non commutative rings, Analele ştiinţifice ale Universităţii" Ovidius" Constanţa. Seria Matematică, 31, 2, 141-154, 2023.

[20] M Palanikumar, K Arulmozhi, C Jana, M Pal, KP Shum, New approach towards different bi-base of ordered b-semiring, Asian-European Journal of Mathematics 16 (02), 2350019

[21] L´aszl´o Sz´ekelyhidi, 'Finite dimensional varieties over the Heisenberg group', Aequationes Mathematicae, Sep 2022 , 97 (2023), 377–390

[22] Simran Tinani, 'On Conjugacy Search Problem in Extraspecial p- Group', cs.CR,