A NEW MULTI PARTY KEY AGREEMENT PROTOCOL USING SEARCH PROBLEMS IN DISCRETE HEISENBERG GROUP.

T.ISAIYARASI *

Research Scholar, Bharathiar University &Assistant Professor
Department of Mathematics, Valliammai Engineering College
S.R.M.Nagar ,Kattankulathur
Tamil Nadu -603203, India
E mail : isai_selvam@yahoo.com

DR.K.SANKARASUBRAMANIAN
Research Supervisor, Bharathiar University & Professor,
Department of Mathematics,Sri Sairam Engineering College.
SaiLeo Nagar –West Tambaram
Tamilnadu-600048, India
E mail: ksssai28@gmail.com

Abstract:

In this paper we present a multi-party Key Agreement Protocol (KAP) using some of the search problems such as Factorization Search Problem , Decomposition Search Problem Conjugacy Search Problem and Twisted Conjugacy Problem. We have chosen Discrete Heisenberg group as our platform group in the above search problems.

Keywords : Factorization Search Problem; Decomposition Search Problem;,Conjugacy Search Problem ; Twisted Conjugacy Problem and Discrete Heisenberg group.

1 Introduction:

A key exchange is a protocol by which two parties, commonly named Alice and Bob, agree on a secret key to use in their subsequent private communication. Key exchange is an essential part of public key system. The first key exchange scheme was introduced by Diffie and Hellman in 1976, and independently by Merkle in 1978.So far ,several key exchange protocols have been developed using the concept of combinatorial group theory, namely the Word Problem,Conjugacy Search Problem, Decomposition Problem, Triple Decomposition Problem Membership Search Problem and so on. In this paper we introduce some of the search problems in the Discrete Heisenberg group [11].

In Crypto 2000 [9],Ko et al proposed a new public key cryptosystem based on Braid groups which are non-abelian; they have used the search problems to build the Cryptosystem.Then Paeng et al [13] proposed a New Public Key Cryptosystem using the Discrete Log Problems in inner automorphisms of the semi-direct product of special linear groups (non-abelian) with Z_p. The above system was named as MOR cryptosystem.Using Unitriangular[3], and Unimodular matrices, Ayan Mahalonobis[4] modified theMOR cryptosystem .

Vladmir Shplirain and Alexander Ushakov [14] used the decomposition problem on Braid groups Vladmir Shplirain and GobrielbZapata [15] used the subgroup membership search problem on Braid groups

Yesem Kurt[16] proposed a key exchange protocol using triple decomposition problem on Braid groups. A.Joux [8] proposed a One Round Prptocol for tripartite Diffe-Hellman,In W.Bosma ,editor Proceedings of Algorithmic Number Teory ,Symposium ,ANTS IV ,volume 1838 of Lecture Notes in Computer Science ,Pages 385 -394 ,Springer Verlag,2000

Zhaohui Cheng, Luminita Vasiu and Richard Comley [17] proposed Pairing- Based One –Round Tripartitie Key Agreement Protocol.

Ho –Kyu, Hyang –Sook Lee ,Young –Ran Lee[12] [proposed a Multiparty Authenticated Key Agreement Protocols From Multilinear Forms.

The paper is organized in the following manner. In section 2 we discuss some computational facts about the Discrete Heisenberg Group. Section 3 deals with the Factorization Search Problem and a Multi party KAP using the same. In Section 4 we present a multiparty KAP using Decomposition Search Problem . Section 5 deals about the multiparty KAP using Conjucacy Search Problem . In Section 6 we discuss the Twisted Conjugacy Problem and a multi party KAP and we conclude the paper in Section 7.

2.Introduction To Discrete Heisenberg Group:

The Discrete Heisenberg group $\mathcal{H}$ may be described as the set Z_p^3 of all integer triples endowed with the following multiplication, where p is a prime
$(x, y, z) \cdot (u, v, w) = (x + u + yw, y + v, z + w) \bmod p$

2.1. *Some Computational Facts About $\mathcal{H}$.*

The following computational facts about $\mathcal{H}$ can be easily derived from the definition of multiplication above .

2.1.1. *Proposition*.
Let x, y, z, u, v, w, n be any integers. Then the multiplication in $\mathcal{H}$ satisfies the following equations:
(a) $(x, y, z)^{-1} = (-x + yz, -y, -z) \bmod p$
(b) $(x, y, z) \cdot (u, v, w) \cdot (x, y, z)^{-1} = (u + yw - zv, v, w) \bmod p$
(c) $[(x, y, z), (u, v, w)] = (yw - zv, 0, 0) \bmod p$
(d) In particular, $[(0, 1, 0), (0, 0, 1)] = (1, 0, 0)$.
(e) (i)$(x, 0, 0) \cdot (0, y, z) = (x, y, z) \bmod p$
(ii)$(0, y, 0) \cdot (0, 0, z) = (yz, y, z) \bmod p$
(iii)$(0, 0, z) \cdot (0, y, 0) = (0, y, z) \bmod p$
(f) (i)$(1, 0, 0)^n = (n, 0, 0) \bmod p$
(ii)$(0, 1, 0)^n = (0, n, 0) \bmod p$
(iii)$(0, 0, 1)^n = (0, 0, n) \bmod p$

2.1.2. *Centre Z[$\mathcal{H}$]:*

Centre of $\mathcal{H}$ coincides with $Z \times 0 \times 0$ where $\mathcal{H} = Z_p^{3,}$
$[H, H] = Z [H]$.

2.1.3. *Generators of $\mathcal{H}$:*

Formulae (d)-(f) show that (0, 1, 0) and (0, 0, 1) generate H. Specifically,
$(x, y, z) = [(0, 1, 0), (0, 0, 1)]^{x} \cdot (0, 0, 1)^{z} \cdot (0, 1, 0)^{y}$,for all (x, y, z) in $\mathcal{H}$.
For the next result, we use the non-standard notation $n^{(2)}$ to stand for $n(n-1)/2$, for any integer ‘n’.

2.2. *Proposition*.

For any $(x, y, z) \in \mathcal{H}$ and any $n \in Z$, we have
$(x, y, z)^n = (nx + n^{(2)}yz, ny, nz)$.

2.3. *Proposition*.

$\mathcal{H}$ may be presented as $< \alpha,\beta: [\alpha, [\alpha,\beta]] = 1 = [\beta, [\alpha,\beta]] >$,
with α (resp.,β) corresponding to the generator (0, 1, 0) (resp., (0, 0, 1)).
The following results have been already established :

2.3.1. *Result 1 :*

Let L be any group, and let σ and τ be any elements of L satisfying the two relations given above . Then, there is a unique homomorphism h : $\mathcal{H} \rightarrow$ L such that h(0, 1, 0) = σ and h(0, 0, 1) = τ

2.3.2. *Result 2 :*

Let σ and τ be any elements of $\mathcal{H}$. There exists a unique endomorphism h of $\mathcal{H}$ such that h(0, 1, 0) = σ and h(0, 0, 1) = τ .

3.Factorization Search Problem:

Given an element w of a group G and two subgroups A ,B $\leq$G,find any two elements a ЄA, b ЄB that would satisfy a.b = w.

*3.1.**Two Party Key Exchange Protocol**:*

Two parties A and B agree on the Discrete Heisenberg Group and two cyclic subgroups G_1 and G_2 of $\mathcal{H}$ **(** Discrete Heisenberg group) .

G_1 is generated by two commuting elements of $\mathcal{H}$ **.**G_2 is generated by two other commuting elements which do not commute with the generators of G_1.

1.A chooses two random elements $a_1 \epsilon G_1$,$b_1 \epsilon G_2$.
2.A computes $S_A= a_1b_1$ and sends the same to B .
3.B chooses two random elements $a_2 \epsilon G_1$,$b_2 \epsilon G_2$.
4.B computes $S_B = a_2b_2$ and sends the same to A.
5.On knowing a_1 and b_1 , A computes $K_A = a_1 S_B b_1$.
6.On knowing a_2 and b_2 , B computes $K_B = a_2 S_A b_2$.
Since $a_1, a_2 \epsilon G_1$ they commute and $b_1, b_2 \epsilon G_2$ they too commute. Hence $K_A = K_B$ is their common shared key.

3.2.Three Party Key Agreement Protocol:

Three parties A_1 , A_2 and A_3 agree on the Discrete Heisenberg Group and two cyclic subgroups G_1 and G_2 of $\mathcal{H}$ **(** Discrete Heisenberg group) .

G_1 is generated by two commuting elements of $\mathcal{H}$ **.**G_2 is generated by two other commuting elements which do not commute with the generators of G_1.

First Round :

1.A_1 chooses two random elements $a_1 \epsilon G_1$,$b_1 \epsilon G_2$.
2.A_1 computes $K_{11}= a_1b_1$ and sends the same to A_2 .
3.A_2 chooses two random elements $a_2 \epsilon G_1$,$b_2 \epsilon G_2$.
4.A_2 computes $K_{12} = a_2b_2$ and sends the same to A_3.
5.A_3 chooses two random elements $a_3 \epsilon G_1$,$b_3 \epsilon G_2$.
6.A_3 computes$K_{13} = a_3b_3$ and sends the same to A_1.
7.A_1 receives K_{13} from A_3 and computes $K_{21} = a_1 K_{13} b_1$.
8.A_2 receives K_{11} from A_1 and computes $K_{22} = a_2 K_{11}b_2$.
9.A_3 receives K_{21} from $A_2$and computes $K_{23} = a_3 K_{23} b_3$.

Second Round:
A_1 sends K_{21} to A_2.
A_2 sends K_{21} to A_3.
A_3 sends K_{23} to A_1.
1.A_1 on knowing a_1,b_1 computes $K_{31} = a_1K_{23} b_1$.
2. A_2 on knowing a_2,b_2 computes $K_{32} = a_2 K_{21}b_2$.
3. A_3 on knowing a_3,b_3 computes $K_{33} = a_3 K_{22}b_3$.
Since a_1, a_2, $a_3 \epsilon G_1$ and b_1,b_2,$b_3 \epsilon G_2$ they commute and they have common shared key is
$K_{31} = K_{32} =K_{33} = a_1 a_2 a_3 b_1 b_2 b_3$.

3.3. Multi Party Key Agreement Protocol:

First Round :

A_1 chooses two random elements $a_1 \epsilon G_1$,$b_1 \epsilon G_2$.
A_1computes $K_{11}= a_1b_1$ and sends the same to A_2 .
A_2 chooses two random elements $a_2 \epsilon G_1$,$b_2 \epsilon G_{2.}$
A_2 computes $K_{12} = a_2b_2$ and sends the same to A_3.
A_3 chooses two random elements $a_3 \epsilon G_1$,$b_3 \epsilon G_{2.}$
A_3 computes $K_{13} = a_3b_3$ and sends the same to A_4.
…………………………………………………..
A_{k-1} chooses two random elements $a_{k-1} \epsilon G_1$,$b_{k-1} \epsilon G_{2.}$
A_{k-1} computes $K_{1k-1} = a_{k-1} b_{k-1}$ and sends the same to A_k
A_k chooses two random elements $a_k \epsilon G_1$,$b_k \epsilon G_2$
A_k computes $K_{1k} = a_k b_k$ and sends it to A_1.

Second Round:

A_1 computes $K_{21} = a_1 K_{1k} b_1$ and sends the same to A_2
A_2 computes $K_{22} = a_2K_{11} b_2$ and sends the same to $A_{3.}$
A_3 computes $K_{23} = a_3 K_{12} b_3$ and sends the same to $A_{4.}$
………………………………………………………
………………………………………………………
A_{k-1} computes $K_{2(k-1)} = a_{k-1} K_{1k-2} b_{k-1}$ and sends the same to $A_{k.}$
A_k computes $K_{2k} = a_k K_{1(k-1)} b_k$ and sends the same to A_1.

$(K-1)^{St}$ Round:
A_1 computes $K_{(k-1)1} = a_1a_k a_{k-1} \ldots\ldots a_2 b_2\ldots\ldots b_{k-1}b_kb_1$.
A_2computes $K_{(k-1)2} = a_2 a_1a_k a_{k-1} \ldots\ldots a_3 b_3\ldots\ldots b_{k-1}b_k b_1 b_{2.}$
………………………………………………………
A_{k-1} computes $K_{(k-1)(k-1)} = a_{k-1} a_{k-2} a_{k-3} \ldots\ldots a_1a_k b_kb_1\ldots\ldots b_{k-3}b_{k-2} b_{k-1}b_{k-1.}$
A_k computes $K_{(k-1)k} = a_k a_{k-1} \ldots\ldots\ldots.. a_1b_1\ldots\ldots.. b_{k-1} b_k$.
Since $a_1,a_2,\ldots..a_k \epsilon G_1$ and $b_1,b_2,\ldots\ldots b_k \epsilon G_{2,}$
$K_{(k-1)1} = K_{(k-1)2} =\ldots\ldots= K_{(k-1)k}$,their common shared key.

4.Decomposition Search Problem :

Given the following :
i)Rrecursive presentation of a group G ,
ii) Two recursively generated subgroups A ,B $\leq$G,
iii)Two elements w ,w_1 Є G,
iv) To find two elements x Є A, y Є B that would satisfy
x.w.y =w_1, provided at least one such pair of elements exist.

Key Agreement Protocol Using Decomposition Search Problem:

4.1. KAP With Two Parties:

One of the parties (say ,A_1)publishes a random element w Є $\mathcal{H}$.
They agree on two cyclic subgroups G_1 and G_2 of $\mathcal{H}$ (Discrete Heisenberg group)
$G_{1=}$ < e ,a ,b > such that ab = ba and a ,b Є $\mathcal{H}$.
G_2 = < e,c,d > such that cd =dc and c ,d Є $\mathcal{H}$ .Also ‘a’ and ‘b’ do not commute with ‘c’ and ‘d’
A_1 chooses a_1 Є $G_{1,}$ b_1 Є G_2 , computes a_1 w b_1 and sends it to $A_{2.}$
A_2 chooses a_2 Є $G_{1,}$ b_2 Є G_2 , computes a_2 w b_2 sends it to A_1
On knowing $a_{1\,,}$ $b_{1,}$ A_1 computes $K_{A1} = a_1\, a_{\,2}w\, b_2\, b_1$.
On knowing $a_{2,}$ b_2 , A_2 computes $K_{A2} = a_2\, a_1\, w\, b_1\, b_{\,2.}$

4.2 . *KAP With Three Party :*

First Round:
A_1 chooses a_1 Є $G_{1,}$ b_1 Є G_2 , computes a_1 w b_1 sends it to $A_{2.}$

A_2 chooses a_2 Є $G_{1,}$ b_2 Є G_2 , computes a_2 w b_2 sends it to A_3
A_3 chooses a_3 Є $G_{1,}$ b_3 Є G_2 , computes a_3 w b_3 sends it to A_1

Second Round :

A_1 computes $a_1\, a_3$ w $b_3\, b_1$ and sends to A_2.
A_2 computes $a_2\, a_1$ w $b_1\, b_2$ and sends to A_3.
A_3 computes $a_3\, a_2$ w $b_2\, b_3$ and sends to $A_{1.}$
On knowing $a_{1\,,}$ $b_{1,}$ A_1 computes $K_{A1} = a_1\, a_3\, a_{\,2}w\, b_2b_3\, b_1$.
On knowing $a_{2,}\, b_2$, A_2 computes $K_{A2} = a_2\, a_1\, a_3$ w $b_3\, b_1\, b_{\,2.}$
On knowing $a_{3,}\, b_{3\,,}\, A_3$ computes $K_{A3} = a_3\, a_2\, a_1$ w $b_1\, b_2\, b_{\,3.}$
$K_{A1} = K_{A2} = K_{A3}$ is their common shared key.

4.3. ***Multi Party Key Exchange Protocol:***

First Round .

A_1 chooses two random elements $a_1 \epsilon G_1$,$b_1\epsilon G_2$.
$A_{\,1}$computes $K_{11}= a_{1W}b_1$ and sends the same to A_2 .
A_2 chooses two random elements $a_2 \epsilon G_1$,$b_2\epsilon G_{2.}$
A_2 computes $K_{12} = a_{2W}b_2$ and sends the same to A_3.
A_3 chooses two random elements $a_3 \epsilon G_1$,$b_3\epsilon G_{2.}$
A_3 computes $_{K13} = a_{3W}b_3$ and sends the same to A_4.
…………………………………………………..
A_{k-1} chooses two random elements $a_{k-1} \epsilon G_1$,$b_{k-1}\epsilon G_{2.}$
A_{k-1} computes $K_{1k-1} = a_{k-1W}\, b_{k-1}$ and sends the same to A_k
A_k chooses two random elements $a_k \epsilon G_1$,$b_k\epsilon G_2$
$A_{\,k}$ computes $K_{1k} = a_k\, wb_k$ and sends it to A_1.

Second Round.

A_1 computes $K_{21} = a_1\, K_{1k}\, b_1$ and sends the same to A_2
A_2 computes $K_{22} = a_2K_{11}\, b_2$ and sends the same to $A_{3.}$
A_3 computes $K_{23} = a_3\, K_{12}\, b_3$ and sends the same to $A_{4.}$
………………………………………………………
A_{k-1} computes $K_{2(k-1)} = a_{k-1}\, K_{1k-2}\, b_{k-1}$ and sends the same to $A_{k.}$
A_k computes $K_{2k} = a_k\, K_{1(k-1)}\, b_k$ and sends the same to A_1.

$(K\text{-}1\,)^{St}$ Round:

A_1 computes $K_{(k-1)1} = a_1a_k\, a_{k-1}$ …… a_2 w b_2……$b_{k-1}b_kb_1$.
A_2computes $K_{(k-1)2} = a_2\, a_1a_k\, a_{k-1}$ ……a_3 w b_3……$b_{k-1}b_k\, b_1\, b_{2.}$
……………………………………………………….
$A_{\,k-1}$ computes $K_{\,(k-1)\,(k-1)} = a_{k-1}\, a_{k-2}\, a_{k-3}$ ……a_1a_k w b_kb_1……$b_{k-3}b_{k-2}\, b_{k-1}b_{k-1.}$
A_k computes $K_{\,(k-1)k} = a_k\, a_{k-1}$ ………..a_1 w b_1……..$b_{k-1}\, b_k$.
Since a_1,a_2,…..a_k ϵG_1 and b_1,b_2,……$b_k \epsilon G_{2,}$
$K_{\,(k-1)1} = K_{\,(k-1)2}$ =……= $K_{\,(k-1)k}$,their common shared key.

5.Key Agreement Protocol Using Conjugacy Search Problem:

The Conjugacy Search Problem (Csp):

The conjugacy search problem is : Given a recursive presentation of a group G and two conjugate elements x,y Є G , find a particular element g Є G such that g^{-1} x g = y.

5.1. *KAP With Two Party:*

Two parties A and B agree on a finite non-abelian group ,Discrete Heisenberg group
$\mathcal{H} = Z_p^{\,3}$ and a cyclic subgroup G_1 = < e ,a ,b > , where ab = ba , a,b are generators of G_1.
1.A publishes an element w Є $\mathcal{H} = Z_p^{\,3}$ such that w does not commute with a and b.

2.A chooses an element $g_1 \in G_1$,computes $g_1^{-1} w\, g_1$ and sends it to B
3.B chooses an element $g_2 \in G_1$, computes $g_2^{-1} w\, g_2$ and sends it to A
4.On knowing g_1 , A computes $K_A = g_1^{-1} g_2^{-1} w\, g_2 g_1$
5.On knowing g_2 , B computes $K_B = g_2^{-1} g_1^{-1} w\, g_1 g_2$
$K_A = K_B$ is their common shared key.

5.2. *KAP With Three Party:*

Three parties A_1 ,A_2 and A_3 agree on a finite non-abelian group ,Discrete Heisenberg group $\mathcal{H} = Z_p^3$ and a cyclic subgroup $G_1 = < e ,a ,b >$, where ab = ba ,a ,b are generators of $G_{1.}$
One of the three parties publishes an element $w \in \mathcal{H}$ such that it does not commute with a and b.

FirstRound:

A_1 chooses an element $g_1 \in G_1$,computes $K_{11} = g_1^{-1} w\, g_1$ and sends it to A_2
A_2 chooses an element $g_2 \in G_1$,computes $K_{12} = g_2^{-1} w\, g_2$ and sends it to A_3
A_3 chooses an element $g_3 \in G_1$,computes $K_{13} = g_3^{-1} w\, g_3$ and sends it to A_1

Second Round :

A_1 computes $K_{21} = g_1^{-1} K_{13}\, g_1$ 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_1
On knowing $g_{1\,,}$ A_1 computes $K_{31} = g_1^{-1} K_{23}\, g_1$
On knowing $g_{2,}$ A_2 computes $K_{32} = g_2^{-1} K_{21} g_2$
On knowing g_3 , A_3 computes $K_{33} = g_3^{-1} K_{22}\, g_3$
$K_{31} = K_{32} = K_{33}$ is their common shared key.

5.3. ***KAP With Multi Party Using CSP:***

$A_{1,}$ $A_{2,}$ $A_{3,}$ A_4............. A_k agree on a finite non-abelian group (Discrete Heisenberg Group) and they agree on a public element $w \in \mathcal{H} = Z_p^3$ and a cyclic subgroup $G_1 = < e ,a ,b >$, where ab = ba ,a ,b are generators of G_1

First Round :

A_1 chooses an element $g_1 \in G_1$, computes $K_{11} = g_1^{-1} w\, g_1$ and sends it to A_2
A_2 chooses an element $g_2 \in G_{1,}$ computes $K_{12} = g_2^{-1} w\, g_2$ and sends it to A_3
A_3 chooses an element $g_3 \in G_{1,}$ computes $K_{13} = g_3^{-1} w\, g_3$and sends it to A_4
A_4 chooses an element $g_4 \in G_1$ computes $K_{14} = g_4^{-1} w\, g_4$ and sends it to A_5
…………………………………………………
A_k chooses an element $g_k \in G_{1,}$ computes $K_{1k} = g_k^{-1} w\, g_k$ and sends it to A_1

Second Round

A_1 computes $K_{21} = g_1^{-1} K_{1k} g_1$ and sends it to A_2
A_2 computes $K_{22} = g_1^{-1} K_{11} g_1$ and sends it to A_3
A_3 computes $K_{23} = g_1^{-1} K_{12} g_1$ and sends it to A_4
A_4 computes $K_{24} = g_1^{-1} K_{13} g_1$ and sends it to A_5
....
A_k computes $K_{2k} = g_1^{-1} K_{1k} g_1$ and sends it to A_1
....

$(K\text{-}1)^{St}$ Round:

A_1 computes $K_{K\text{-}1\,1} = g_1^{-1} K_{(k\text{-}2\,)k}\, g_1$ and sends it to A_2
A_2 computes $K_{k\text{-}12} = g_2^{-1} K_{(k\text{-}2)2}\, g_2$ and sends it to A_3
A_3 computes $K_{k\text{-}1\,3} = g_3^{-1} K(k\text{-}2)_1 g_3$ and sends it to A_4
…………………………………………………………………………
A_k computes $K(_{(k\text{-}1)k} = g_k^{-1} K(_{k\text{-}2)(k\text{-}1)}\, g_k$ and sends it to A_1

A_1 computes $K_{k1} = g_1^{-1} K_{k-1k}\, g_1$
A_2 computes $K_{k2} = g_2^{-1} K(_{k-1)1}\, g_2$
A_3 computes $K_{k3} = g_3^{-1} K(_{k-1)1}\, g_3$
…………………………………………………………………………
A_k computes $K_{k3} = g_k^{-1} K(_{k-1)(k-1)}\, g_k$
$K_{k1}= K_{k2} = K_{k3} = K_{k4}$ …………..$= K_{kk}$ is their common shared key.

6. **KAP Using Twisted Conjugacy Problem:**

Twisted Conjugacy Problem:

Let G be a countable discrete group and $\varphi : G \rightarrow G$ an endomorphism. An element y Є G is said to be twisted conjugate of an element x Є G , iff there exists g ЄG with $y = g\, x\, \varphi\, (g^{-1})$.

6.1. ***KAP With Two Parties:***

Two parties A and B agree on a finite non-abelian group,Discrete Heisenberg group $\mathcal{H} = Z_p^3$ and a cyclic subgroup G_1 = < e ,a ,b > , where ab = ba ,a ,b are generators of G_1.

A publishes an element w Є $\mathcal{H} = Z_p^3$ such that w does not commute with a and b.
A chooses an element g_1 Є G_1 ,computes $g_1\, w\, \varphi(g_1^{-1})$ and sends it to B
B chooses an element g_2 Є G_1 , computes $g_2\, w\, \varphi(g_2^{-1})$ and sends it to A
On knowing g_1 , A computes $K_A = g_1 g_2\, w\, \varphi\, (g_2^{-1})\, \varphi(g_1^{-1})$
On knowing g_2 , B computes $K_B = g_2 g_1\, w\, \varphi\, (g_1^{-1})\, \varphi(g_2^{-1})$
$K_A = K_B$ is their common shared key.

6.2.*KAP With Three Parties:*

Three parties A_1 ,A_2 and A_3 agree on a finite non-abelian group ,Discrete Heisenberg group $\mathcal{H} = Z_p^3$ and a cyclic subgroup G_1 = < e ,a ,b > , where ab = ba ,a ,b are generators of $G_{1.}$
One of the three parties publishes an element w Є $\mathcal{H}$ such that it does not commute with a and b.

First Round:

A_1 chooses an element g_1 Є G_1 ,computes $K_{11} = g_1\, w\, \varphi\, (g_1^{-1})$ and sends it to A_2
A_2 chooses an element g_2 Є G_1 ,computes $K_{12} = g_2\, w\, \varphi\, (g_2^{-1})$ and sends it to A_3
A_3 chooses an element g_3 Є G_1 ,computes $K_{13} = g_3\, w\, \varphi\, (g_3^{-1})$ and sends it to A_1

Second Round :

A_1 computes $K_{21} = g_1\, K_{13}\, \varphi\, (g_1^{-1})$ and sends it to A_2
A_2 computes $K_{22} = g_2\, K_{11}\, \varphi\, (g_2^{-1})$ and sends it to A_3
A_3 computes $K_{23} = g_3\, K_{12}\, \varphi\, (g_3^{-1})$ and sends it to A_1
On knowing $g_{1\,,}$ A_1 computes $K_{31} = g_1\, K_{23}\, \varphi\, (g_1^{-1})$
On knowing $g_{2,}$ A_2 computes $K_{32} = g_2\, K_{21}\, \varphi\, (g_2^{-1})$
On knowing g_3 , A_3 computes $K_{33} = g_3\, K_{22}\, \varphi\, (g_3^{-1})$
$K_{31} = K_{32} = K_{33}$ is their common shared key.

6.3. KAP With Multi Party Using Twisted Conjugacy Problem :

$A_{1,}$ $A_{2,}$ $A_{3,}$ A_4............. A_k agree on a finite non-abelian group (Discrete Heisenberg Group) and they agree on a public element w Є $\mathcal{H} = Z_p^3$ and a cyclic subgroup G_1 = < e ,a ,b > , where ab = ba ,a ,b are generators of G_1

First Round :

A_1 chooses an element g_1 Є G_1 , computes $K_{11} = g_1\, w\, \varphi\, (g_1^{-1})$ and sends it to A_2
A_2 chooses an element g_2 Є $G_{1,}$ computes $K_{12} = g_2\, w\, \varphi\, (g_2^{-1})$ and sends it to A_3
A_3 chooses an element g_3 Є $G_{1,}$ computes $K_{13} = g_3\, w\, \varphi\, (g_3^{-1})$and sends it to A_4

A_4 chooses an element g_4 Є G_1 computes $K_{14} = g_4 w\ \varphi\ (g_4^{-1})$ and sends it to A_5

………………………………………………………….

A_k chooses an element g_k Є $G_{1,}$ computes $K_{1k} = g_k\ w\ \varphi\ (g_k^{-1})$ and sends it to A_1

Second Round :

A_1 computes $K_{21} = g_1\ K_{1k}\ \varphi\ (g_1^{-1})$ and sends it to A_2

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

A_3 computes $K_{23} = g_3\ K_{12}\ \varphi\ (g_3^{-1})$ and sends it to A_4

A_4 computes $K_{24} = g_4\ K_{13}\ \varphi\ (g_4^{-1})$ and sends it to A_5

………………………………………………………………………………………………………

A_k computes $K_{2k} = g_k\ K_{1k}\ \varphi\ (g_k^{-1})$ and sends it to A_1

$(K\text{-}1)^{St}$ Round:

A_1 computes $K_{k-1\ 1} = g_1\ K_{(k-2\ )k}\ \varphi\ (g_1^{-1})$ and sends it to A_2

A_2 computes $K_{k-12}\ = g_2\ K_{(k-2)1}\ \varphi\ (g_2^{-1})$ and sends it to A_3

A_3 computes $K_{k-1\ 3}\ = g_3\ K(k-2)_2\ \varphi\ (g_2^{-1})$ and sends it to A_4

…………………………………………………………………………

A_k computes $K(_{k-1)k}\ = g_k^{-1}\ K(_{k-2)(k-1)}\ g_k$ and sends it to A_1

A_1 computes $K_{k1} = g_1\ K_{k-1k}\ \varphi\ (g_1^{-1})$

A_2 computes $K_{k2} = g_2\ K(_{k-1)1}\ \varphi\ (g_2^{-1})$

A_3 computes $K_{k3} = g_3\ K(_{k-1)1}\ \varphi\ (g_3^{-1})$

…………………………………………………………………………

A_k computes $K_{k3} = g_k\ K(_{k-1)(k-1)}\ \varphi\ (g_k^{-1})$

$K_{k1}= K_{k2} = K_{k3} = K_{k4}$ …………..= K_{kk} is their common shared key.

7.Conclusion:

In some of the previously proposed multi –party key agreement protocols there exists the difficulty of building an effiecient computable multilinear forms.To over come such a difficulty ,in this paper we have presented some Multi-party Key Exchange Protocols using search problems. The advantage of this protocol is, each user chooses only one set of secret keys and they are using the same for subsequent communications of the remaining rounds. In order to improve the security of the system, each user can change their secret keys for each communication.

References.

[1] Alexander Fet shtyn ,Fedrol indukave, Twisted Burnside theorem for two –step Torsion free Nilpotent groups, 2000 Mathematics Subject classification 20C ; 20E45 ;22D10;22D25;22D 30;37C25;43A30;646C.

[2] Alexei Myansnikov,Vladmir Splarain ,Alexander Ushakov, Group Based Cryptography, 2000 Mathematical Subject Classification: 11T71, 20Exx, 20Fxx, 20Hxx, 20P05, 60B15, 68P25, 94A60, 94A62

[3] Ayan Mahalanobis , A simple generalisation of the ElGamal cryptosystem to non-abelian groups,arXiv:cs/0607011v5[cs.CR]

[4] Ayan Mahalanobis, A simple generalisation of the El-Gamal cryptosystem to non –abelian groups –II, arXiv:cs/0607011v5[cs.CR]

[5] Chun-Li Lin, Hung-Min Sun, Michael Steiner and Tzonelih Hwang Three-party Encrypted Key Exchange WithoutServer Public-Keys

[6] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik, Member, IEEEg-Min Sun, Michael Steiner and Tzonelih Hwang -New Multiparty Authentication Services and Key Agreement Protocols

[7] Ho –Kyu, Hyang –Sook Lee ,Young –Ran Lee - Multiparty Authenticated Key Agreement Protocols From Multilinear Forms.

[8] A.Joux, A One Round Prptocol for tripartite Diffe-Hellman,In W.Bosma ,editor proceedings of Algorithmic Number Teory ,Symposium ,ANTS IV ,volume 1838 of Lecture Notes in Computer Science ,Pages 385 -394 ,Springer Verlag,2000

[9] Ko et al Public Key Cryptosystem based on Braid Groups , Crypto 2000 LNCS 1880,pp 66-183

[10] Neal R.Wagner ,Marianne R.Magyarik Drexel University, A public key cryptosystem based on word problem ,Cs.utsa.edu/~/pubs/crypto/crypto.pdf

[11] Peter J.Khan, Automorpisms of the Discrete Heisenberg Group, arXiv:math / 0405109VI [math SG]6 May 2004

[12] Rene' Peralta,Eiji Okamoto,School of information science Some combinatorial problems of importance to cryptography

[13] Seong – Hun Paeng , Kil –Can Ha ,Jae Heon Kim , Seongtaet Chee,Choonsik Park New Public Cryptosystem using finite non-abelian groups, National Security Research Institute 161 Kajong-dong, Yusong-gu, Taejon, 305-350, KOREA,fshpaeng,kcha,jaeheon,chee,cspg@etri.re.kr *citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.101.5992*

[14] Vladmir Shplrain and Alexander Ushakov, A new Key –exchange protocol based on the decomposition problem ,2000 Mathematics Subject classification classification 94A60,20F05,20F06,68P5

[15] Vladmir Shplrainvand Gabrial Zapata ,Using the subgroup membership search problem in public key cryptography, *www.sci.ccny.cuny.edu/~shpil/crypmemb.pdf*

[16] Yesem Kurt,A new key exchange primitive based on the triple decomposition problem eprint.iacr.org/cryptodb/data/paper.pp?

[17] Zhaohui Cheng, Luminita Vasiu and Richard Comley proposed Pairing- Based One –Round Tripartitie Key Agreement Protocol.