February 26, 2005

DIFFIE-HELLMAN KEY EXCHANGE PROTOCOL AND NON-ABELIAN NILPOTENT GROUPS.

AYAN MAHALANOBIS

ABSTRACT. In this paper we study a key exchange protocol similar to Diffie-Hellman key exchange protocol using abelian subgroups of the automorphism group of a non-abelian nilpotent group. We also generalize group no.92 of Hall-Senior table [15], for arbitrary prime p and show that for those groups, the group of central automorphisms commute. We use these for the key exchange we are studying.

MSC: 94A62, 20D15.
Keyword: Diffie-Hellman key exchange, public-key cryptography, p-group, Miller group.

1. INTRODUCTION

In this paper we generalize the Diffie-Hellman key exchange protocol from a cyclic group to a finitely presented non-abelian nilpotent group of class 2. Similar efforts were made in [2, 3, 24] to use braid groups, a family of finitely presented non-commutative groups [4, 9], in key exchange. Our efforts are not solely directed to construct an efficient and fast key exchange protocol. We also try to understand the conjecture, "the discrete logarithm problem is equivalent to the Diffie-Hellman problem in a cyclic group". We develop and study protocols where, at least theoretically, non-abelian groups can be used to share a secret or exchange private keys between two people over an insecure channel. This development is significant because nilpotent or, more specifically p-groups, have nice presentations and computation in those groups are fast and easy [37, Chapter 9]. So our work can be seen as a nice application of the advanced and developed subject of p-groups and computations with p-groups.

The frequently used public key cryptosystems are slow and uses mainly number theoretic complexity. The specific cryptographic primitive, a one way function, that we have in mind is "THE DISCRETE LOGARITHM PROBLEM", DLP for short. DLP is general enough to be defined in an arbitrary cyclic group as follows. Let $G = \langle g \rangle$ be a cyclic group generated by g and let $g^n = h$. We are given g and h, DLP is to find the n [38, Chapter 6]. The security of discrete logarithm problem depends on the representation of the group. It is trivial in $\mathbb{Z}_n$, but is much harder (no polynomial time algorithm known) in the multiplicative group of a finite field and even harder (no sub exponential time algorithm known) in the group of elliptic curves which are not supersingular [5]. But with the invention of sub-exponential algorithms for breaking the Discrete Logarithm Problem, like the index calculus and Coppersmith's algorithm, multiplicative groups of finite fields are no longer that attractive especially the ones of characteristic 2.

Discrete logarithm is also used in many other groups like in elliptic curves, in which case a cyclic group or a big enough cyclic component of an abelian group is used. We in this article propose a generalization of DLP or more specifically Diffie-Hellman key exchange protocol in situations where the group has more than one generator, i.e., in a finitely presented nonabelian group. Let f be an automorphism of a finitely presented group G generated by $\{a_1, a_2, \cdots, a_n\}$. If one knows the action of f on $a \in G$, i.e., $f(a)$, then it is difficult for him to tell the action of f on any other $b \in G$ i.e., $f(b)$. We describe this in detail later under the name "general discrete logarithm problem". In this paper we work with finitely presented groups in terms of generators and relations and do not consider any representation of that group. Though that seems to be a good idea for future research.

Now suppose for a moment that $G = \langle g \rangle$ is a cyclic group and that we are given g and g^n where $\gcd(n, |G|) = 1$. DLP is to find n. Notice that in this case the map $x \mapsto x^n$ is an automorphism. If we conjecture that finding the automorphism is finding [1]n then one way to see DLP, in terms of group theory, is to find the automorphism from its image of one element. This is the central idea that we want to generalize to nonabelian finitely presented groups, especially nilpotent group of class 2. This explains our choice of the name "general discrete logarithm problem".

To work with a finitely presented group and its automorphisms the following properties of the group are needed.

- A consistent and natural representation of the elements in the group.
- Computation in the group should be fast and easy.
- The automorphism group should be known and the automorphisms should have a nice enough presentation so that images can be computed quickly.

We note at this point that for a p-group the first two requirements are satisfied [37, Chapter 9].

2. Some notations and Definitions

We now describe some of the definitions and notation that will be used in this paper. The notation used is standard:

- G will denote a finite group. $Z = Z(G)$ denotes the center of the group G and will be denoted by Z if no confusion can arise.
- $G' = [G, G]$ is the commutator subgroup of G.
- $\mathrm{Aut}(G)$ and $\mathrm{Aut}_c(G)$ are the group of automorphisms and the group of central automorphisms of G respectively.
- $\Phi(G)$ is the Frattini subgroup of G, which is the intersection of all maximal subgroups of G.
- We denote the commutator of a, b by $[a, b]$ where $[a, b] = a^{-1}b^{-1}ab$.
- The exponent of a p-group G, denoted by $\exp(G)$, is the largest power of p that is order of an element in G.

[1]Notice that this conjecture is equivalent to Diffie-Hellman assumption in cyclic group.

The following commutator formulas hold for any element a,b and c in any group G.

(a): $a^b = a[a, b]$

(b): $[ab, c] = [a, c]^b[b, c] = [a, c][a, c, b][b, c]$ it follows that in a nilpotent group of class 2, $[ab, c] = [a, c][b, c]$

(c): $[a, bc] = [a, c][a, b]^c = [a, c][a, b][a, b, c]$ it follows that in a nilpotent group of class 2, $[a, bc] = [a, b][a, c]$

(d): $[a, b]^{-1} = [b, a]$

The proofs of these formulas follows from direct computation or can be found in [22].

Definition. *Miller Group.*
A group G is called Miller group if it has an abelian automorphism group, in other words if $Aut(G)$ is commutative.

Definition. *Central Automorphisms.*
Let G be a group, then $\phi \in Aut(G)$ is called a central automorphism if $g^{-1}\phi(g) \in Z(G)$ for all $g \in G$. Alternately, one might say that ϕ is a central automorphism if $\phi(g) = gz_{\phi,g}$ where $z_{\phi,g} \in Z(G)$ depends on g and ϕ. If ϕ is clear from the context then we can simplify the notation as $\phi(g) = gz_g$.

Apart from inner automorphisms, central automorphisms are second best in terms of nice description. So they are very attractive for cryptographic purposes, since it is easy to describe the automorphisms and compute the image of an arbitrary element.

Theorem 2.1. *The centralizer of the group of inner automorphisms is the group of central automorphisms. Moreover a central automorphism fixes the commutator elementwise.*

This theorem first appears in [12] who refers to [16] and [42].

Definition. *Polycyclic Group*
Let G be a group, a finite series of subgroup in G

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq G_3 \trianglerighteq \cdots \trianglerighteq G_n = 1$$

is a polycyclic series if G_i/G_{i+1} is cyclic and G_{i+1} is a normal subgroup of G_i. Any group with polycyclic series is a polycyclic group.

It is easy to prove that finitely generated nilpotent groups are polycyclic and so any finitely generated p-group is polycyclic. Let a_i be an element in G_i whose image generates G_i/G_{i+1}. Then the sequence $\{a_1, a_2, \cdots, a_n\}$ is called a polycyclic generating set. It is easy to see that $g \in G$ can be written as $g = a_1^{\alpha_1}a_2^{\alpha_2}\cdots a_n^{\alpha_n}$, where α_i are integers. If $g = a_1^{\alpha_1}a_2^{\alpha_2}\cdots a_n^{\alpha_n}$ where $0 \leq \alpha_i < m_i$, $m_i = |G_i : G_{i+1}|$ then the expression is a collected word. Each element $g \in G$ can be expressed by a unique collected word. Computation with these collected words is easy and implementable in computer, for more information on this topic see [37, Section 9.4] and also [14, polycyclic package].

3. Key Exchange

We want to follow the Diffie-Hellman Key exchange protocol using a commutative subgroup of the automorphism group of a finitely presented group G. The security of Diffie-Hellman in the cyclic group rests on the following three factors:

: The discrete logarithm problem.
: The Diffie-Hellman problem.
: The Decision Diffie-Hellman Problem [6, 7, 13, 36, 40].

We have already described the discrete logarithm problem. The Diffie-Hellman problem is the following: Let $G = \langle g \rangle$ be a cyclic group of order n. One knows g, g^a and g^b, and the problem is to find g^{ab}. It is not known if DL is equivalent to DH. DDH or Decision Diffie-Hellman problem is more subtle. Suppose that DH is a hard problem, so it is impossible to compute g^{ab} from g^a, g^b and g. But what happens if someone can compute 80% of the shared secret from g^a, g^b and g, then the adversary will have 80% of the shared secret, that is most of the private key. This is clearly unacceptable. It is often hard to formalize DDH in exact mathematical terms, see [7, Section 3], the best formalism offered is a randomness criterion for the bits of the key. In DDH we ask the question, given the triple g^a, g^b and g^c is $c = ab \mod n$? But there is no known link between DDH and any mathematically hard problem for Diffie-Hellman key exchange protocol in cyclic groups.

As is usual, we denote by Alice and Bob, two people trying to set up a private key over an insecure channel to communicate securely and Oscar an adversary is eavesdropping. In this paper the shared secret or the key is an element of a finitely presented group G.

3.1. General Discrete Logarithm Problem.

Let $G = \langle a_1, a_2, \cdots, a_n \rangle$ and $f : G \to G$ be a non identity automorphism. Suppose one knows $f(a)$ for $a \in G$ then GDLP is to find $f(b)$ for any b in G. Assuming the word problem is easy or presentation of the group is by means of generators, GDLP is equivalent to finding $f(a_i)$ for all i which in terms gives us a complete knowledge of the automorphism. So in other words the cryptographic primitive GDLP is equivalent to, "*finding the automorphism f from the action of f on only one element*".

3.2. General Diffie-Hellman Problem.

Let $\phi, \psi : G \to G$ be arbitrary automorphisms, and assume one knows a, $\phi(a)$ and $\psi(a)$. Then GDHP is to find $\phi(\psi(a))$. Notice that GDHP is a restricted form of GDLP, because in case of GDHP one has to compute $\phi(\psi(a))$ for some fixed a, not $\phi(b)$ for an arbitrary b in G.

3.3. General Decision Diffie-Hellman Problem.

Let $\phi, \psi : G \to G$ be two arbitrary automorphisms. Assume one knows a, $\phi(a)$ and $\psi(a)$. Then GDDH is to extract partial information about $\phi(\psi(a))$. In this paper we don't try to find exact conditions for GDDH, but notice that GDDH depends largely on the group G.
We now describe two key exchange protocols and do some cryptanalysis. We denote by G a finitely presented group and S an abelian subgroup of $\mathrm{Aut}(G)$.

4. Key Exchange Protocol I

Alice and Bob want to set up a private key. They select a group G and an element $a \in G \setminus Z(G)$ over an insecure channel. Then Alice picks a random automorphism $\phi_A \in S$ and sends Bob $\phi_A(a)$. Bob similarly picks a random automorphism $\phi_B \in S$ and sends Alice $\phi_B(a)$. Both of them can now compute $\phi_A(\phi_B(a)) = \phi_B(\phi_A(a))$ which is their private key for symmetric transmission.

4.1. Comments on Key Exchange Protocol I.

Though initially it might seem that we don't have enough information to know the automorphisms ϕ_A and ϕ_B, it turns out that if we are using automorphisms which fix conjugacy classes, like inner automorphisms, then the security of the above scheme actually rests on the conjugacy problem.

Let $\phi_A(a) = x^{-1}ax$ for some x and let $\phi_B(a) = y^{-1}ay$. Then $\phi_A(\phi_B(a)) = (xy)^{-1}a(xy)$. Since, a, $\phi_A(a)$ and $\phi_B(a)$ are known, if the conjugacy problem is easy in the group then anyone can find x and y and break the system.

In the above scheme Oscar knows G and a. If the automorphisms are central automorphisms, then he also sees $\phi_A(a) = az_{\phi_A,a}$ and $\phi_B(a) = az_{\phi_B,a}$. Oscar can find $z_{\phi_A,a}$ and $z_{\phi_B,a}$. Now if G is a special p-group ($G' = Z(G) = \Phi(G)$) then $Z(G)$ is fixed elementwise by both ϕ_A and ϕ_B. Then

$$\phi_A(\phi_B(a)) = \phi_A(az_{\phi_B,a}) = az_{\phi_A,a}z_{\phi_B,a} \tag{1}$$

Oscar knows a and can compute $z_{\phi_A,a}$ and $z_{\phi_B,a}$ and can find the private key $\phi_A(\phi_B(a))$. In the literature all examples of Miller p-group with odd prime p are special and the above key exchange is fatally flawed for those groups.

5. Key Exchange Protocol II

In this case Alice and Bob want to set up a private key and they set up a group G over a insecure channel. Alice chooses a random non-central element g and a random automorphism $\phi_A \in S$ and sends Bob $\phi_A(g)$. Bob picks another automorphism $\phi_B \in S$ and computes $\phi_B(\phi_A(g))$ and sends it back to Alice. Alice knowing ϕ_A computes ϕ_A^{-1} which gives her $\phi_B(g)$ and picks another random automorphism $\phi_H \in S$ and computes $\phi_H(\phi_B(g))$ and sends it back to Bob. Bob knowing ϕ_B computes ϕ_B^{-1} which gives him $\phi_H(g)$ which is their private key. Notice that Alice never reveals g in public.

5.1. Comments on Key Exchange Protocol II.

Notice that for central automorphisms, ϕ_A and ϕ_B, $\phi_A(g) = gz_{\phi_A,g}$, since g is not known we don't know $z_{\phi_A,g}$ but if G is special ($Z(G) = G' = \Phi(G)$) then $\phi_B(gz_{\phi_A,g}) = gz_{\phi_B,g}z_{\phi_A,g}$ from which $z_{\phi_B,g}$ can be found. Then $\phi_H(\phi_B(g)) = gz_{\phi_B,g}z_{\phi_H,g}$, hence one can find $gz_{\phi_H,g}$ which is $\phi_H(g)$ and the scheme is broken. As one clearly sees, this attack is not possible if the group is not special.

The reader might have noticed at this point that all the attacks are GDHP. So certainly in some groups GDHP is easy.

As we know, any automorphism in G can be seen as restriction of an inner automorphism in $\mathrm{Hol}(G)$, see [27, 41] for further details on the holomorph of a group, hence solving conjugacy problem in $\mathrm{Hol}(G)$ will break the system for any automorphism. On the other hand operation in $\mathrm{Hol}(G)$ is twisted so it is possible that the conjugacy problem in $\mathrm{Hol}(G)$ is difficult even though it is easy in G. Any cyclic group is a Miller group so success of the holomorph attack would prove insecurity in DLP, so we believe that the holomorph attack won't be successful in many cases. Though a lot of work needs to be done on this.

6. Key Exchange using Braid Groups[2]

In [24] a similar key exchange protocol has been defined, we in this section mention some similarities of their approach with ours. We also mention how our system generalizes their system using braid groups. See also [8].

We define braid group as a finitely presented group, though there are fancy pictorial ways to look at braids and multiplication of braids. An interested reader can look in [4, 9]. B_n the braid group with n-strands is defined as:

$$B_n = \langle \sigma_1, \sigma_2, \cdots, \sigma_{n-1} : \ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ if } |i-j| = 1, \ \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| \geq 2\rangle$$

In [24] authors found two disjoint subgroups A and B of the group of inner automorphisms $\mathrm{Inn}(B_n)$, such that for $\phi \in A$ and $\psi \in B$, $\phi(\psi(g)) = \psi(\phi(g))$. Then the key exchange proceeds similar to Key Exchange Protocol I above with the restriction that Alice chooses automorphisms from A and Bob chooses automorphisms from B. There is also a different approach to key exchange in braid group as in [2, 3].

In the same spirit as [24] we can develop a key exchange protocol similar to key exchange protocol I, where we take two disjoint subgroups A and B in $\mathrm{Aut}(G)$ such that for $\phi \in A$ and $\psi \in B$, $\phi(\psi(g)) = \psi(\phi(g))$. The use of inner automorphisms is only possible when the conjugacy or the generalized conjugacy problem (conjugator search problem) is known to be hard.

There are significant differences in our approach to that of the approach in [24]. In [24] authors choose a group and then tried to use that group in cryptography. We, on the other hand, take the fundamental concept as discrete logarithm problem, generalized it using automorphisms of a non-abelian group and then look for groups favorable to us. The fact that the central idea in braid group key exchange turns out to be similar to ours is encouraging.
It is intuitively clear at this point that we should start looking for groups with abelian automorphism group, i.e., Miller groups.

7. Miller Group

The term Miller Group is not that common in literature. It was introduced by Earnley in [10]. Miller was the first to study groups with abelian automorphism group in [30]. Cyclic groups are good examples of miller group. G.A. Miller also proved that no non-cyclic abelian group is Miller.

Charles Hopkins began a list of necessary conditions for a Miller group in 1927 [18]. He complained that very little is known about those groups. The same is true

[2]Author is indebted to two anonymous referees for bringing braid group key exchange protocol to his notice.

today. Except for some sporadic examples of groups with abelian automorphism groups, there is no sufficient condition known for a group to be Miller.
We now state some known facts about Miller groups which are available in the literature and which we shall need later. For proof of these theorems which we present in a rapid fire fashion, the reader can look in any standard text books like [22, 33] or the references.

Proposition 7.1. *Let G be a non-abelian Miller group, then G is nilpotent and of class 2.*

Proof. It follows from the fact that the group of inner automorphisms commute and $G/Z(G) \cong \mathrm{Inn}(G)$. •

Since a nilpotent group is a direct product of its Sylow p-subgroups S_p, and $\mathrm{Aut}(A \times B) = \mathrm{Aut}(A) \times \mathrm{Aut}(B)$ whenever A and B are of relatively prime order, it is enough to study Miller p-groups for prime p.

Proposition 7.2. *Let G be a p-group of class 2, then $exp(G') = exp(G/Z(G))$.*

Proposition 7.3. *In a p-group of class 2, $(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$. Furthermore if $exp(G') = n$ is odd, then $(xy)^n = x^n y^n$.*

By definition in a Miller group all automorphisms commute. Since central automorphisms are the centralizer of inner automorphisms, we have proved the following theorem.

Theorem 7.4. *In a Miller group G, all automorphisms are central.*

It follows that to show a group is not Miller, all we have to do is to produce a non-central automorphism.

Proposition 7.5. *If the commutator and the center coincide then every pair of central automorphisms commute.*

Proof. Let G be a group such that $G' = Z(G)$. Then let ϕ and ψ be central automorphisms given by $\phi(x) = xz_{\phi,x}$ and $\psi(x) = xz_{\psi,x}$ where $z_{\phi,x}, z_{\psi,x} \in G'$. Then

$$\psi(\phi(x)) = \psi(xz_{\phi,x}) = \psi(x)z_{\phi,x} = xz_{\psi,x}z_{\phi,x} = xz_{\phi,x}z_{\psi,x} = \phi(\psi(x)).$$

•

Definition. *Purely Non-abelian group*
A group G is said to be a purely nonabelian group (PN group for short) if whenever $G = A \times B$ where A and B are subgroups of G with A abelian, then $A = 1$. Equivalently G has no abelian direct factor.

Let $\sigma : G \to G$ be a central automorphism. Then we define a map $f_\sigma : G \to Z(G)$ as follows: $f_\sigma(g) = g^{-1}\sigma(g)$. Clearly this map defines a homomorphism. The map $\sigma \mapsto f_\sigma$ is clearly a one-one map. Conversely, if $f \in \mathrm{Hom}(G, Z(G))$ then we define a map $\sigma_f(g) = gf(g)$, $x \in G$. Clearly σ_f is an endomorphism. It is easy to see that

$$\mathrm{Ker}(\sigma_f) = \{x \in G : \ f(x) = x^{-1}\}$$

Hence it follows that σ_f is an automorphism if and only if $f(x) \neq x^{-1}$ for all $x \in G$ with $x \neq 1$.

Theorem 7.6. *In a purely non-abelian group G, the correspondence $\sigma \to f_\sigma$ is a one-one map of $Aut_c(G)$ onto $Hom(G, Z(G))$*

Proof. See [1]. $\bullet$

Notice that for any $f \in \mathrm{Hom}(G, Z(G))$ there is a map $f' \in \mathrm{Hom}(G/G', Z(G))$ since $f(G') = 1$. Furthermore notice that corresponding to $f' \in \mathrm{Hom}(G/G', Z(G))$ there is a map $f : G \to Z(G)$ explained in the following diagram

$$G \xrightarrow{\ \eta\ } G/G' \xrightarrow{\ f'\ } Z(G)$$

where η is the natural epimorphism.

Let G be a p-group of class 2, such that $\exp(Z(G)) = a$, $\exp(G') = b$ and $\exp(G/G') = c$ and let $d = \min(a, c)$. Notice that from the fundamental theorem of abelian groups

$$G/G' = A_1 \oplus A_2 \oplus \cdots A_r \ \text{ where } \ A_i = \langle a_i \rangle$$

$$Z(G) = B_1 \oplus B_2 \oplus \cdots B_s \ \text{ where } \ B_i = \langle b_i \rangle$$

$r, s \in \mathbb{N}$ be the direct decomposition of G/G' and $Z(G)$. If the cyclic component $A_k = \langle a_k \rangle$ has exponent greater or equal to the exponent of $B_j = \langle b_j \rangle$, then one can define a homomorphisms $f : G/G' \to Z(G)$ as follows

$$f(a_i) = \begin{cases} b_j & \text{where } \ i = k \\ 1 & \text{where } \ i \neq k \end{cases}$$

From this discussion it is clear that for $f \in \mathrm{Hom}(G, Z(G))$, $f(G)$ generates the subgroup

$$\mathcal{R} = \{z \in Z(G) :\ |z| \leq p^d,\ d = \min(a, c)\}$$

Definition. *In any abelian p-group A written additively, there is a descending sequence of subgroups*

$$A \supset pA \supset p^2 A \supset \cdots \supset p^n A \supset p^{n+1} A \supset \cdots$$

Then $x \in A$ is of height n if $x \in p^n A$ but not in $p^{n+1} A$. In other words the elements of height n are those that drop out of the chain in the $(n+1)^{th}$ inclusion.

For further information on height see [21].

Since for a class 2 group we have

$$\exp(G/G') \geq \exp(G/Z(G)) = \exp(G')$$

it follows that $c \geq b$. Hence if $d = \min(a, c)$ then either $d = b$ or $d > b$.

Let $\mathrm{height}(xG') \geq b$, then $xG' = y^{p^b} G'$ for some $y \in G$. Then for any $F \in \mathrm{Hom}(G, G')$, $F(yG')^{p^b} = 1$ implying $xG' \in F^{-1}(1)$. Conversely, let $\mathrm{height}(xG') < b$. Then from the previous discussion it is clear that there is a $F' \in \mathrm{Hom}(G/G', G')$

such that xG' is not in the kernel, consequently there is a $F \in \mathrm{Hom}(G, G')$ such that $x \notin \ker(F)$. Combining these two facts we see that:

$$\mathcal{K} = \bigcap_{F \in \mathrm{Hom}(G,G')} F^{-1}(1) = \{x \in G : \text{ height}(xG') \geq b\}$$

Proposition 7.7. $\mathcal{K} \subseteq \mathcal{R}$

Proof. In a class 2 group, if $x \in \mathcal{K}$ then $xG' = y^{p^b}G'$ for some $y \in G$ and $\exp(G/Z) = b$ and $G' \subseteq Z(G)$, hence $x \in Z(G)$.

Let $x \in \mathcal{K}$, then height$(xG') \geq b$, hence there is a $y \in G$ such that $y^{p^b}G' = xG'$ i.e. $x = y^{p^b}z$ where $z \in G'$ and $y^{p^c} \in G'$ and $c \geq b$. We have

$$x^{p^c} = (y^{p^b})^{p^c} z^{p^c} = (y^{p^c})^{p^b} = 1$$

Hence $|x| \leq \min(p^a, p^c)$ which implies that $x \in \mathcal{R}$. •

Proposition 7.8. *For a PN group G of class 2, if $Aut_c(G)$ is abelian then $\mathcal{R} \subseteq \mathcal{K}$.*

Proof. In a PN group, using theorem 7.6 and the notation there, two central automorphisms σ and τ commute if and only if $f_\sigma, f_\tau \in \mathrm{Hom}(G, Z(G))$ commute. Then for any $f \in \mathrm{Hom}(G, Z(G))$ and $F \in \mathrm{Hom}(G, G')$ we have that $f \circ F = F \circ f = 1$. Since $f(G') = 1$, clearly $F \circ f(G) = 1$ proving that $\mathcal{R} \subseteq \mathcal{K}$. •

Combining the above two propositions, we just proved that in a PN group G of class 2, if $\mathrm{Aut}_c(G)$ is abelian then $\mathcal{R} = \mathcal{K}$. As discussed earlier there are two cases $d = b$ and $d > b$. We further prove that:

Proposition 7.9. *If G is a non-abelian p group of class 2, and $Aut_c(G)$ is abelian with $d > b$, then $\mathcal{R}/G'$ is cyclic.*

Proof. See [1] theorem 3. •

Theorem 7.10. *Adney and Yen* [1].
Let G be a purely non-abelian group of class 2, p odd, let $G/G' = \prod_{i=1}^{n} \{x_i G'\}$. Then the group $Aut_c(G)$ is abelian if and only if

(i) $\mathcal{R} = \mathcal{K}$

(ii) *either $d = b$ or $d > b$ and $\mathcal{R}/G' = \{x_1^{p^b} G'\}$*

Proof. See [1, Theorem 4]. •

From the proof of Proposition 7.5 it follows that in a group G with $Z(G) \leq G'$, the central automorphisms commute.

Theorem 7.11. *The group of central automorphisms of a p-group G, where p is odd, is a p-group if and only if G has no abelian direct factor.*

Proof. See [34, Theorem B] and its corollary. •

At this point we concentrate on building a cryptosystem. We note that Miller groups in particular have no advantage over groups with abelian central automorphism group. It is hard to construct Miller groups and there is no known Miller group for odd prime which is not special, so we now turn towards a group G such that $\mathrm{Aut}(G)$ is not abelian but $\mathrm{Aut}_c(G)$ is abelian. We propose to use $\mathrm{Aut}_c(G)$ rather than $\mathrm{Aut}(G)$ in the key exchange protocols described earlier.

8. Signature Scheme based on conjugacy problem

Assume that we are working with a group G with commuting inner automorphisms, for example, a group of class 2 with abelian central automorphism group.

Alice publishes α and β where $\beta = a^{-1}\alpha a$ and keeps a a secret. To sign a text $x \in G$ she picks an arbitrary element $k \in G$ and computes $\gamma = k\alpha k^{-1}$ and then computes δ such that $x = (\delta k)(a\gamma)^{-1}$. Now notice that

$$
\begin{aligned}
x\alpha x^{-1} &= (\delta k)(a\gamma)^{-1}\alpha((\delta k)(a\gamma)^{-1})^{-1} \\
&= (\delta k)\gamma^{-1}a^{-1}\alpha a\gamma k^{-1}\delta^{-1} \\
&= \delta\gamma^{-1}a^{-1}k\alpha k^{-1}a\gamma\delta^{-1} && \text{Inner automorphisms commute} \\
&= \delta\gamma^{-1}a^{-1}\gamma a\gamma\delta^{-1} \\
&= \delta a^{-1}\gamma a\delta^{-1} \\
&= \delta(k\beta k^{-1})\delta^{-1} && \gamma = k\alpha k^{-1} \Rightarrow a^{-1}\gamma a = k\beta k^{-1}
\end{aligned}
$$

So to sign a message $x \in G$ Alice computes δ as mentioned and sends $x, (k\delta)$. To verify the message one computes $L = x\alpha x^{-1}$ and $R = \delta k\beta(\delta k)^{-1}$. If $L = R$ then the message is authentic otherwise not.

There is a similar signature scheme in [23], where they exploit the gap between the computational version (conjugacy problem) and the decision version of the conjugacy problem (conjugator search problem) in Braid Groups. We followed ElGamal signature scheme closely [38, Chapter 7].

8.1. Comments on the above Signature Scheme.

If one can solve conjugacy problem in the group then from the public information α and β he can find out a and our scheme is broken. Conjugacy problem is known to be hard in some groups and hence it seems to be a reasonable assumption at this moment. There is another worry: if Alice sends k and δ separately then one can find a from the equation $x = (\delta k)(a\gamma)^{-1}$, since γ is computable. However, this is circumvented easily by sending the product δk not δ and k individually and keeping k random.

9. An interesting family of p-groups

It is well known that cyclic groups have abelian automorphism groups. The first person to give an example of an non-abelian group with an abelian automorphism groups is G.A. Miller in [30] which was generalized by Struik in [39]. There are three non-abelian groups with abelian automorphism group in Hall-Senior table [15], they are nos. 91, 92 and 99. Millers example is no. 99. In [19], Jamali generalized no. 91 and 92. His generalization of no. 91 is in one direction, it increases the exponent of the group.

Jamali in the same paper generalizes group no. 92 in two directions, the size of the exponent and the number of generators. His generalization was restrictive in that it works only for prime 2. There are other examples of families of Miller p-groups in literature, the most notable one is the family of p-groups for any arbitrary prime p given by Jonah and Konisver in [20] which was generalized to arbitrary number of generators by Earnley in [10]. There are examples by Martha Morigi in [32] and Heineken and Liebeck in [17] also. All these examples of Miller groups given in [10, 17, 20, 32] are special groups i.e., the commutator and the center are same. For special groups the key exchange protocols don't work as noted earlier. So there is no Miller p-group, readily available in literature, for arbitrary prime p which can be used right away in construction of the protocol. The only other source are groups nos. 91, 92 and 99 in Hall Senior table [15] and their generalizations, notice that these groups are not special but are 2-group. Of the three generalizations, the generalization of no. 92 best fits our criterion since it has been generalized in two directions, *viz.* number of generators and exponent of the center and moreover it is is not special and $Z(G) = A \times G'$ where A is a cyclic group. So once we generalize it for arbitrary primes, it has "three degrees of freedom", the number of generators, exponent of center and the prime; which makes it attractive for cryptographic purposes.

In the rest of the section we use Jamali's definition in [19] to define a family of p-groups for arbitrary prime. So this family is a generalization of Jamali's example and assuming transitivity of generalizations, ultimately a generalization of group no. 92 in the Hall-Senior table [15]. We study automorphisms of this group and show that the group is Miller if and only if $p = 2$, but this family of groups always have an abelian central automorphism group which is fairly large. We then attempt to build a key exchange protocol as described earlier using the central automorphisms. We start with definition of the group.

Definition. *Let $G_n(m,p)$ be a group generated by $n+1$ elements $\{a_0, a_1, a_2, \cdots, a_n\}$ and let p be any prime and $m \geq 2$ and $n \geq 3$ are integers. The group is defined by the following relations:*

$$a_1^p = 1, \quad a_2^{p^m} = 1, \quad a_i^{p^2} = 1 \quad for \quad 3 \leq i \leq n, \quad a_{n-1}^p = a_0^p.$$

$$[a_1, a_0] = 1, \quad [a_n, a_0] = a_1, \quad [a_{i-1}, a_0] = a_i^p \quad for \quad 3 \leq i \leq n.$$

$$[a_i, a_j] = 1 \quad for \quad 1 \leq i < j \leq n.$$

We state couple of facts about the group $G_n(m,p)$ whose proof is by direct computation.

- **a:** $G_n(m,p)'$ the derived subgroup of $G_n(m,p)$ is an elementary abelian group $\langle a_1, a_3^p, \cdots a_n^p \rangle \simeq \mathbb{Z}_p^{n-1}$.
- **b:** $Z(G_n(m,p)) = \langle a_2^p \rangle \times G'$.
- **c:** $G_n(m,p)$ is a p-group of class 2.
- **d:** $G_n(m,p)$ is a PN group.

Proposition 9.1. *$G_n(m,p)$ is a polycyclic group and every element of $g \in G_n(m)$ can be uniquely expressed in the form $g = a_0^{\alpha_0} a_1^{\alpha_1} a_2^{\alpha_2} a_3^{\alpha_3} \cdots a_n^{\alpha_n}$, where*
$0 \le \alpha_i < p$ for $i = 0,1$; $0 \le \alpha_2 < p^m$, $0 \le \alpha_i < p^2$ for $i = 3,4,\cdots,n$.

Proof. Let us define $G_0 = G_n(m,p) = \langle a_0, a_1, a_2, \cdots, a_n \rangle$, $G_1 = \langle a_1, a_2, \cdots a_n \rangle$ and similarly $G_k = \langle a_k, a_{k+1}, \cdots, a_n \rangle$ for $k \le n$. Since G_1 is a finitely generated abelian group, it is a polycyclic group [37, Proposition 3.2]. It is fairly straightforward to see that

$$G_1 \rhd G_2 \rhd \cdots \rhd G_n \rhd \langle 1 \rangle$$

is a polycyclic series and $\{a_1, \cdots, a_n\}$ a polycyclic generating sequence of G_1.

It is easy to see from the relations of the group that G_1 is normal in G_0 and G_0/G_1 is cyclic. It is fairly easy to show that $\langle a_i G_{i+1} \rangle = G_i/G_{i+1}$ and $|a_i G_{i+1}| = |a_i|$ and hence any element of the group has a unique representation of the above form. We would call an element represented in the above form a collected word. See also proposition 4.1, chapter 9 in [37]. •

Computation with $G_n(m,p)$: Our group $G_n(m,p)$, which is of class 2, i.e. commutators of weight 3 are identity, computations become real nice and easy. Let us demonstrate the product of two collected words $g = a_0^{\alpha_0} a_1^{\alpha_1} a_2^{\alpha_2} a_3^{\alpha_3} a_4^{\alpha_4}$ and $h = a_0^{\beta_0} a_1^{\beta_1} a_2^{\beta_2} a_3^{\beta_3} a_4^{\beta_4}$. To compute gh we use concatenation and form the word $a_0^{\alpha_0} a_1^{\alpha_1} a_2^{\alpha_2} a_3^{\alpha_3} a_4^{\alpha_4} a_0^{\beta_0} a_1^{\beta_1} a_2^{\beta_2} a_3^{\beta_3} a_4^{\beta_4}$ and note that a_i's commute except for a_0 hence one tries to move a_0 towards left using the identity

$$a_i a_0 = a_0 a_i [a_i, a_0] = \begin{cases} a_0 a_i a_{i+1}^p & \text{for} \quad 1 \le i < n \\ a_0 a_i a_1 & \text{for} \quad i = n \end{cases}$$

Further note, since commutators are in the center of the group, that a_{i+1}^p or a_1 can be moved anywhere. Once a_0 is moved to the extreme left the word formed is the collected word of gh. This process is often referred in the literature as "collection". Computing the inverse of an element can be similarly achieved.

We now prove that the central automorphism group of the group $G_n(m,p)$ for an arbitrary prime p is abelian. For sake of simplicity we denote $G_n(m,p)$ by G and use notation from Theorem 7.10.

Lemma 9.2. *In G, $\mathcal{R} = Z(G) = \mathcal{K}$.*

Proof. Using the notation from theorem 7.10, we see that in G, $a = m-1$, $b = 1$ and $c = m$ hence $d = m-1$. Clearly, $\mathcal{R} = Z(G)$ hence $\mathcal{K} \subseteq Z(G)$.
Let $x \in Z(G)$, if $x \in G'$ then height$(x) = \infty$ and we are done. If not then $x = z_1 z_2$ where $z_1 \in \langle a_2^p \rangle$ and $z_2 \in G'$. Then $xG' = z_1 G'$ and hence height$(xG') \ge 1$. •

It is easy to see that $\mathcal{R}/G' = Z(G)/G' = \langle a_2^p G' \rangle$ and hence from theorem 7.10 we proved the following theorem:

Theorem 9.3. *$Aut_c(G)$ is abelian.*

9.1. **Automorphisms of $G_n(m,p)$.** For sake of brevity we write $G = G_n(m,p)$. In this section we describe the automorphisms of groups of this kind. The discussion is in, more than one way, an adaptation of work of Jamali in [19] and generalizes his main theorem.

Lemma 9.4. *Let $x = a_0^{\beta_0} a_1^{\beta_1} a_2^{\beta_2} \cdots a_n^{\beta_n}$, where β_i, $i = 0, 1, 2 \cdots, n$ are integers be an element of G. If $p = 2$ then β_0 is 1 and*

- *$x^2 = a_1^{\beta_n} a_2^{2\beta_2} a_3^{\gamma_3} \cdots a_{n-2}^{\gamma_{n-2}} a_{n-1}^{\gamma_{n-1}+2} a_n^{\gamma_n}$ for $p = 2$. Where $\gamma_i = 2(\beta_{i-1} + \beta_i)$.*
- *$x^p = a_2^{p\beta_2} a_3^{p\beta_3} \cdots a_{n-2}^{p\beta_{n-2}} a_{n-1}^{p\beta_{n-1}+p\beta_0} a_n^{p\beta_n}$ for $p \neq 2$.*

Proof. For the case $p = 2$ we just collect terms and use the relation $a_{n-1}^2 = a_0^2$. For $p \neq 2$ using Proposition 7.3 we have

$$\begin{aligned} & (a_0^{\beta_0} a_1^{\beta_1} a_2^{\beta_2} \cdots a_{n-1}^{\beta_{n-1}} a_n^{\beta_n})^p \\ = \quad & (a_0^{\beta_0})^p (a_1^{\beta_1} a_2^{\beta_2} \cdots a_{n-1}^{\beta_{n-1}} a_n^{\beta_n})^p \\ = \quad & a_0^{p\beta_0} a_2^{p\beta_2} a_3^{p\beta_3} \cdots a_n^{p\beta_n} \end{aligned}$$

Using the relation $a_{n-1}^p = a_0^p$ we have

$$a_0^{p\beta_0} a_2^{p\beta_2} a_3^{p\beta_3} \cdots a_n^{p\beta_n} = a_2^{p\beta_2} a_3^{p\beta_3} \cdots a_{n-2}^{p\beta_{n-2}} a_{n-1}^{p\beta_{n-1}+p\beta_0} a_n^{p\beta_n}$$

•

For the group G we note that $H = \langle a_1, a_2, a_3, \cdots a_n \rangle$ is the maximal abelian normal subgroup of G and is hence characteristic. It follows that the H^p is also characteristic. Corresponding to H we define two decreasing sequences of characteristic subgroups $\{K_i\}_{i=0}^{n-1}$ such that

$$K_0 = H \text{ and } K_i/K_{i-1} = Z(G/K_{i-1}^p) \ \ (1 \leq i \leq n-1)$$

and $\{L_i\}$ such that

$$L_0 = H \text{ and } L_i = \{h : \ h \in H, \ h^p \in [G, L_{i-1}]\} \ (1 \leq i \leq n-1)$$

It follows easily that

$$\begin{aligned} K_i &= \langle a_1, a_2, \cdots, a_{n-i}, a_{n-i+1}^p, \cdots, a_n^p \rangle \ 1 \leq i \leq n-1 \\ L_1 &= \langle a_1, v, a_3, \cdots, a_n \rangle \\ L_i &= \langle a_1, v, a_3^p, \cdots, a_{i+1}^p, a_{i+2}, \cdots, a_n \rangle \quad 2 \leq i \leq n-1 \end{aligned}$$

where $v = a_2^{p^{m-1}}$. For $3 \leq i \leq n$ we have

$$K_{n-i} \cap L_{i-2} = \langle a_1, v, a_3^p, \cdots a_{i-1}^p, a_i, a_{i+1}^p, \cdots a_n^p \rangle = \langle v, a_i, G' \rangle.$$

Also $K_{n-2} \cap L_0 = \langle a_2, G' \rangle$. It follows that if $\theta \in \mathrm{Aut}(G)$, then $a_i^{-1}\theta(a_i) \in Z(G)$ for $1 \leq i \leq n$. On the other hand we may suppose that $\theta(a_0) = a_0^{\beta_0} a_1^{\beta_1} a_2^{\beta_2} \cdots a_n^{\beta_n}$. For $p = 2$, since θ is an automorphism it automatically follows that $\beta_0 = 1$.
Now from the relations in the group G it follows that $\theta(a_0^p) = \theta(a_{n-1}^p) = a_{n-1}^p$ it follows that

$$a_{n-1}^p = a_2^{p\beta_2} a_3^{p\beta_3} \cdots a_{n-2}^{p\beta_{n-2}} a_{n-1}^{p\beta_{n-1}+p\beta_0} + a_n^{p\beta_n} \ \text{ for } \ p \neq 2$$

which implies that $p|\beta_i$ where $i \in \{2, 3, 4, \cdots, n-2, n\}$ and $\beta_{n-1} + \beta_0 \equiv 1 \mod p$. Hence if $\beta_0 = 1$ then $p|\beta_{n-1}$. This gives a complete description of any automorphism of G and in particular the central automorphisms of G. It also follows that when $p \neq 2$ there are non-central automorphisms just take $\beta_0 \neq 1$ and β_{n-1} such that $\beta_0 + \beta_{n-1} \equiv 1 \mod p$. We proved the following theorem

Theorem 9.5. *The group $G_n(m, p)$ is Miller if and only if $p = 2$.*

Proof. That $G_n(m, 2)$ is Miller follows from [19]. In the above discussion we saw that for a odd prime p one can construct non-central automorphism and from Theorem 6.4 it follows that $G_n(m, p)$ is not miller. •

9.2. **Description of Central Automorphisms.** Notice that G is a PN group, hence there is a one-one correspondence between $\mathrm{Aut}_c(G)$ and $\mathrm{Hom}(G, Z(G))$. Since, $Z(G) = \langle a_2^p \rangle \times G'$. Hence $\mathrm{Hom}(G, Z(G)) = \mathrm{Hom}(G, \langle a_2^p \rangle) \times \mathrm{Hom}(G, G')$. It follows: $\mathrm{Aut}_c(G) = A \times B$ where

$$A = \{\sigma \in \mathrm{Aut}_c(G) : x^{-1}\sigma(x) \in \langle a_2^p \rangle\}$$

$$B = \{\sigma \in \mathrm{Aut}_c(G) : x^{-1}\sigma(x) \in G'\}$$

Elements of A can be explained in a very nice way. Pick a random integer k such that $\gcd(p, k) = 1$ from $1 \leq k < p^m$ and a random subset R (could be empty) of $\{0, 3, 4, \cdots n\}$, and then an arbitrary automorphism in A is

$$\begin{aligned} \sigma(a_1) &= a_1 \\ \sigma(a_2) &= a_2^k \\ \sigma(a_i) &= \begin{cases} a_i & \text{if } i \notin R \\ a_i \left(a_2^{p^{m-1}}\right)^{r_i} & \text{if } i \in R \end{cases} \end{aligned} \tag{2}$$

We use indexing in $\{0, 3, 4, \cdots, n\}$ to order R and $0 < r_i < p$ is an integer corresponding to $i \in R$. Conversely, any element in A can be described this way.
The automorphism $\phi \in B$ is of the form

$$\phi(x) = \begin{cases} a_1 & \text{if } \quad x = a_1 \\ a_i z & \text{if } \quad x = a_i \; i \in \{0, 2, 3, \cdots, n\} \end{cases} \tag{3}$$

where $z \in G'$.

9.3. **Using these automorphisms in key-exchange.** Let us briefly recall the key-exchange protocol described before. Alice and Bob decide on a group G and a non-central element $g \in G \setminus Z(G)$ in public. Alice then chooses an arbitrary automorphism ϕ_A and sends Bob $\phi_A(g)$. Similarly Bob picks an arbitrary automorphism ϕ_B and sends Alice $\phi_B(g)$. Since the automorphisms commute, both of them can compute $\phi_A(\phi_B(g))$, which is their private key. The most devastating attack on the system is the one in which Oscar looking at g and $\phi_A(g)$ can predict with some amount of certainty what $\phi_A(\phi_B(g))$ will look like.

Definition. *Let* $g = a_0^{\beta_0} a_1^{\beta_1} a_2^{\beta_2} a_3^{\beta_3} \cdots a_n^{\beta_n}$ *be an arbitrary element of* G*, i.e.* $0 \leq \beta_0 < p$*,* $0 \leq \beta_1 < p$*,* $0 \leq \beta_2 < p^m$ *and* $0 \leq \beta_i < p^2$ *for* $3 \leq i \leq n$*. Then the vector* $v := (\beta_0, \beta_3, \beta_4, \cdots, \beta_n)$ *is called the parity of* g*. Two elements* g *and* g' *are said to be of same parity condition if* $v = v' \mod p$*, where* v' *is the parity of* g'*.*

Lemma 9.6. *Let* $g \in G$ *and* $\phi : G \to G$ *be any central automorphism then* g *and* $\phi(g)$ *have the same parity condition.*

Proof. Notice that an automorphism ϕ either belongs to A or B or is a composition of elements in A with elements in B. So we might safely ignore elements from A, since they only affect the exponent of a_2. Also note that a_1 being in the commutator remains fixed under any central automorphism.
So we need to be concerned with elements of B, from the description of B, and each commutator is a word in p-powers of the generators and the fact that $G' \subset Z(G)$, the lemma follows. •

Now let us understand what an element in A does to an element $g \in G$. We use notations from equation 2.

Lemma 9.7. *Let* $g = a_0^{\beta_0} a_1^{\beta_1} a_2^{\beta_2} a_3^{\beta_3} \cdots a_n^{\beta_n}$*,* $\phi \in A$ *and if* $\phi(g) = a_0^{\beta'_0} a_1^{\beta'_1} a_2^{\beta'_2} a_3^{\beta'_3} \cdots a_n^{\beta'_n}$ *then* $\beta_i = \beta'_i$ *for* $i \neq 2$ *and* $\beta'_2 = k\beta_2 + p^{m-1} \sum_{i \in R} r_i \beta_i \mod p^m$*.*

Proof. Notice that from Equation 2, it is clear that elements of A only affect the exponent of a_2, so $\beta'_i = \beta_i$ for $i \neq 2$ follows trivially. From the definition of A and simple computation it follows that $\beta'_2 = k\beta_2 + p^{m-1} \sum_{i \in R} r_i \beta_i \mod p^m$. •

As noted earlier there are three kinds of attack, GDLP (the discrete logarithm problem in automorphisms) and GDHP (Diffie-Hellman problem in automorphisms) and GDDH. We have earlier stated that GDLP is equivalent to finding the automorphism from the action of the automorphism on one element. It seems that for one to find the automorphism discussed in the previous lemma, one has to find k, R and r_i. Notice that $\beta'_2 = k\beta_2 + p^{m-1} \sum_{i \in R} r_i \beta_i \mod p^m$, is a knapsack in β_2 and p^{m-1}, but solving that knapsack is not enough to compute the image of any element, because R is not known so β_i's are not known. We shall show in a moment that the security of the key exchange protocol depends on the difficulty of this knapsack, whose security is still an open question, but this doesn't help Oscar to find the automorphism, just partial information about the automorphism comes out.

Next we show that though it seems to be secure under GDLP, but if the knapsack is solved then the system is broken by GDHP. This proves that GDHP is a weaker problem than GDLP in $G_n(m,p)$. Let $g = a_0^{\beta_0} a_1^{\beta_1} a_2^{\beta_2} a_3^{\beta_3} \cdots a_n^{\beta_n}$, then as discussed before for $\phi, \psi \in \mathrm{Aut}_c(G)$, with notation from equation 2:

$$\phi(g) = a_0^{\beta_0} a_1^{\beta_1} a_2^{k_2\beta_2 + p^{m-1} \sum_{i \in R} r_i \beta_i} a_3^{\beta_3 + k_3 p} \cdots a_n^{\beta_4 + k_4 p}$$

$$\psi(g) = a_0^{\beta_0} a_1^{\beta_1} a_2^{k_2'\beta_2 + p^{m-1}\sum\limits_{i\in R'} r_i'\beta_i} a_3^{\beta_3 + k_3' p} \cdots a_n^{\beta_4 + k_4' p}$$

Notice that $\left(a_2^{p^{m-1}}\right)^{\beta+lp}$ for $\beta, l \in \mathbb{N}$ reduces to $a_2^{\beta p^{m-1}}$ and it follows that the exponent of a_2 in $\phi(\psi(g))$ is

$$k_2\left(k_2'\beta_2 + p^{m-1}\sum_{i\in R'} r_i'\beta_i\right) + p^{m-1}\sum_{i\in R} r_i\beta_i \tag{4}$$

The exponent of a_0, a_1 stays the same and the exponent of a_i will be $\beta_i + (k_i + k_i')p \mod p^2$ for $3 \le i \le n$.

Note that elements having the same parity condition play a major role here. If the automorphisms didn't preserve the parity condition then this attack wouldn't have been possible.

10. Some useful facts about the cryptosystem

We shall be using notations from last section in this section.

GDLP: For the group $G_n(m,p)$, GDLP is to find $k_2, k_3, \cdots, k_n$, R and r_i.

GDHP: For the group $G_n(m,p)$ GDHP is to find $k_2, k_3, \cdots, k_n$.

GDDH: Extract partial information about the bits in Equation 4 without solving the knapsack in Equation 5. We won't explore GDDH any further in this article.

It is easy to see that k_i and k_i' are easy to find for $i = 3, 4, \cdots, n$, hence the exponents of $a_3, a_4, \cdots, a_n$ in $\phi(\psi(g))$ are easy to compute. So one can't use these exponents as part of the shared secret or the secret key. On the other hand computing the exponent of a_2 depends on solving

$$k_2\beta_2 + p^{m-1}\sum_{i\in R} r_i\beta_i \mod p^m \tag{5}$$

as a knapsack on β_2 and p^{m-1}. It is clear that if the knapsack is broken then we can find k_2 and our system is broken by GDHP. On the other hand it is an open question, if the GDHP is equivalent to solving the knapsack. In other words, is it possible to find k_2 without breaking the knapsack? So one of the security assumption is the knapsack in Equation 5 and the relation of GDHP with the knapsack.

Order of $G_n(m,p)$: From Proposition 9.1, the order of the group is p^{2n+m-4}.

Order of the group of cental automorphisms of $G_n(m,p)$: The group of central automorphism of $G = G_n(m,p)$ is isomorphic to $\mathrm{Hom}(G/G', Z(G))$ which is isomorphic to $\mathbb{Z}_p^{n^2} \times \mathbb{Z}_{p^{m-1}}$ and its order is p^{n^2+m-1} [34, Theorem 1] or [35, Section 5.8].

Complexity of multiplication in $G_n(m,p)$: Clearly from Page 11, the complexity of multiplication is $O(n-1)$ which is the same as complexity of reducing the inverse of an element to normal form.

Computation of image of a central automorphism in $G_n(m,p)$: Once an central automorphism ϕ and a group element g is selected, computation of $\phi(g)$ involves only addition of integers, which is fast and easy.

11. Conclusion

In this paper we studied a key exchange protocol using commuting automorphisms in a non-abelian p-group, since any nilpotent group is a direct product of its Sylow subgroups, so for our work nilpotent groups can be reduced to p-groups. We argued that this is a generalization of the Diffie-Hellman key exchange and hence is a generalization of the discrete log problem. Other public key systems like the El-Gamal cryptosystem using discrete logarithm might be adaptable to our methods. This is the first attempt to generalize discrete logarithm in the way we did. So there are more questions than there are answers.

We should try to find other groups and try our system in terms of GDLP and GDHP. As we noted earlier, GDHP is a subproblem of the GDLP, and we saw in $G_n(m,p)$, GDHP is a much easier problem than GDLP. Our example was of the form $d > b$ in Theorem 7.10. The next step is to look at groups where $d = b$. We note from theorem 7.11, if a p-group G is a PN group then $\mathrm{Aut}_c(G)$ is a p-group and since p-groups have nontrivial centers, one can work in that center with our scheme. In this case we would be generalizing to arbitrary nilpotentcy class but keep working with central automorphisms.

Lastly we note that, if we were using some representation for this finitely presented group G, say for example, matrix representation of the group over a finite field $\mathbb{F}_q$, then security of the system in $G_n(m,p)$ becomes the discrete logarithm problem [28, 29]. Since the discrete logarithm problem in matrices is only as secure as the discrete logarithm problem in finite fields there is no known advantage to go for matrix representation, but there might be other representations of interest. There is one conjecture that comes out of this work and we end with that.

Conjecture 11.1. *Let G be a Miller p-group for odd prime p, then G is special.*

Acknowledgment: Author wishes to thank Fred Richman who read the whole manuscript and made valuable suggestions. Author also wishes to thank two anonymous referees for their comments and suggestions, which has contributed significantly in better presentation of this paper.

References

[1] A.E. Adney and Ti Yen. Automorphisms of p-group. *Illinois Journal of Mathematics*, 9:137–143, 1965.

[2] I. Anshel, M. Anshel, B. Fisher, and D. Goldfield. New key agreement protocols in braid group cryptography. In *CT-RSA 2001*, number 2020 in Lecture Notes in Computer Science, pages 1–15. Springer, 2001.

[3] I. Anshel, M. Anshel, and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Research Letters*, 6:287–291, 1999.

[4] Joan S. Birman. *Braids, Links and Mapping Glass Groups*. Number 82 in Annals of Mathematics Studies. Princeton University Press, 1974.

[5] Ian Blake, gadiel seroussi, and Nigel Smart. *Eliptic Curves in Cryptography*. Number 265 in London Mathematical Society, Lecture Note Series. Cambridge University Press, 1999.

[6] Ian F. Blake and Theo Garefalakis. On the complexity of the Discrete Logarithm and Diffie-Hellman problems. *Journal of Complexity*, 20, 2004.

[7] Dan Boneh. The Decision Diffie-Hellman problem. In *Algorithmic number theory (Portland, OR, 1998)*, number 1423 in Lecture Notes in Computer Science, pages 48–63. Springer, Berlin, 1998.

[8] Jung Hee Cheon and Byungheup Jun. An polynomial time algoritm for tha braid Diffie-Hellman conjugacy problem. In *Advances in cryptography – CRYPTO 2003*, number 2729 in Lecture Notes in Computer Science, pages 212–225. Springer, Berlin, 2003.

[9] Patrick Dehornoy. Braid-based cryptogrpahy. *Contemporary Mathematics*, 360:1–33, 2004.

[10] Bruce E. Earnley. *On finite Groups whose group of automorphisms is abelian*. PhD thesis, Wayne State University, 1975.

[11] Taher Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *Lecture Notes in Comput. Sci., 196, Springer, Berlin.*, pages 10–18, 1985.

[12] T.A. Fournelle. Elementary abelian p-groups as automorphism group of infinite group. *I. Math. Z.*, 167:259–270, 1979.

[13] Steven Galbraith and Victor Rotger. Easy decision Diffie-Hellman groups. *LMS Journal of Computation and Mathematics*, 7:201–218, 2004.

[14] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002. (`http://www.gap-system.org`).

[15] M. Hall and J.K. Senior. *The groups of order* 2^n $(n \leq 6)$. Macmillan, 1964.

[16] P. Hall. *The Edmonton notes on nilpotent groups.* Queen Mary college mathematics notes, Cambridge, 1969.

[17] Hermann Heineken and Hans Liebeck. The occurrence of finite groups in the automorphism group of nilpotent groups of class 2. *Archives of Mathematics*, 25:8–16, 1974.

[18] Charles Hopkins. Non-abelian groups whose groups of isomorphism are abelian. *Ann. of Math*, 29(1-4):508–520, 1927.

[19] Ali-Reza Jamali. Some new non-abelian 2-groups with abelian automorphism groups. *Journal of Group Theory*, 5:53–57, 2002.

[20] D. Jonah and M. Konvisser. Some non-abelian p-groups with abelian automorphism groups. *Archives of Mathematics*, 26:131–133, 1975.

[21] Irving Kaplansky. *Infinite Abelian Groups.* The University of Michigan Press, 1969.

[22] E.I. Khukhro. *p-Automorphisms of finite p-groups.* Number 246 in London Mathematical Society, Lecture Note Series. Cambridge University Press, 1997.

[23] Ki Hyoung Ko, Doo Ho Choi, Mi Sung Cho, and Jang Won Lee. New signature scheme using conjugacy problem. http://eprint.iacr.org/2002/168, 2002.

[24] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In Mihir Bellare, editor, *Advances in Cryptology – CRYPTO 2000*, number 1880 in Lecture Notes in Computer Science, pages 166–183, 2000.

[25] Neal Koblitz. *A course in number theory and cryptography.* Number 114 in Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994.

[26] Neal Koblitz. *Algebraic aspects of cryptography.* Number 3 in Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, 1998.

[27] A.G. Kurosh. *The Theory of Groups*, volume 1 & 2. Chelsea Publishing Company, 1960.

[28] Alfred J. Menezes and Scott A. Vanstone. A note on cyclic group, finite fields and discrete logarithm problem. *Applicable Algebra in Engineering, Communication and Computing*, 3(1):67–74, 1992.

[29] Alfred J. Menezes and Yi-Hong Wu. The discrete logarithm problem in $\mathrm{GL}(n, q)$. *Ars Combinatoria*, 47:23–32, 1997.

[30] G.A. Miller. A non-abelian group whose group of isomorphism is abelian. *Messenger Math.*, 43:124–125, 1913.

[31] M.J.Curran. Semidirect product groups with abelian automorphism groups. *J. Austral. Math, Soc.*, Series A(42):84–91, 1987.

[32] Martha Morigi. On p-groups with abelian automorphism group. *The Mathematical Journal of the University of Padova*, 92:47–58, 1994.

[33] Joseph J. Rotman. *An introduction to the theory of groups*. Springer-Verlag, 1994.

[34] P. R. Sanders. The central automorphism of a finite group. *J. London Math. Soc.*, 44:225–228, 1969.

[35] W.R. Scott. *Group Theory*. Dover, 1964.

[36] Igor E. Shparlinski. Security of polynomial transformations of Diffie-Hellman key. *Finite fields and their applications*, 10:123–131, 2004.

[37] Charles Sims. *Computation with finitely presented groups*. Cambridge University Press, Cambridge, 1994.

[38] Douglas Stinson. *Cryptography: Theory and Practice*. CRC Press, 2 edition, 2002.

[39] Ruth R. Struik. Some non-abelian 2-groups with abelian automorphism groups. *Archives of Mathematics*, 39:299–302, 1982.

[40] Maria Isabel González Vasco and Igor E. Sharlinski. On the security of Diffie-Hellman bits. In *Cryptography and computational number theory*, Progress in Computer Science and Applied Logic, pages 257–268. Birkhäuser, Basel, 2001.

[41] Maria S. Voloshina. *On the holomorph of a discrete group*. PhD thesis, University of Rochester, 2003.

[42] H. Zassenhaus. *The theory of groups*. Chelsea, New York, 1958.

Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL, 33431

E-mail address: amahalan@fau.edu