FINDING N-TH ROOTS IN NILPOTENT GROUPS
AND APPLICATIONS IN CRYPTOLOGY

Sandra Sze$^1$, Delaram Kahrobaei$^{2, 8}$, Renald Dambreville$^3$, Makenson Dupas$^4$

$^1$Doctoral Program in Mathematics Department
CUNY Graduate Center
365, Fifth Avenue, New York, NY 10016, USA

$^2$Doctoral Program in Computer Science
CUNY Graduate Center
365, Fifth Avenue, New York, NY 10016, USA

$^3$Mathematics Department
New York City College of Technology
300, Jay Street, Brooklyn, NY 11201, USA

Abstract: In this paper we discuss finding $n$-th roots in nilpotent groups and post some open questions. In the literature, the study of finding square root in finite fields has been of interest and because of the complexity of this problem, it has been used in public key cryptography. In this paper, we propose how to find the $n$-th root in nilpotent groups and propose a digital signature based on the semigroup law of 4-Engel groups.

AMS Subject Classification: 20F18, 68P25, 94A60, 11T71
Key Words: $n$-th roots, nilpotent groups, digital signature

1. Nilpotent Groups

In this section we give the definitions of nilpotent groups with respect to upper and lower central series, we will bring some classical facts about them and give examples.

Definition 1.1. A central series is a sequence of subgroups

$$\{1\} = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_n = G$$

such that for $0 \leq i \leq n - 1$, we have $A_{i+1}/A_i \leq Z(G/A_i)$, where $Z(H)$ denotes

Received: February 17, 2011 © 2011 Academic Publications, Ltd.

$^8$Correspondence author
Definition 1.2. The lower central series for a group $G$ is a series of subgroups
\[ G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k \triangleright \cdots \]
where $G_{k+1} = [G_k, G]$ for $k \geq 0$.

Definition 1.3. A group $G$ is said to be nilpotent if it has a lower central series of finite length.

Definition 1.4. The upper central series for a group $G$ is a sequence of subgroups
\[ \{1\} = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_k \trianglelefteq \cdots \]
such that $Z_1 = Z(G)$ and $Z_{k+1}/Z_k = Z(G/Z_k)$.

In any nilpotent group the upper and lower central series terminates at the same $n$.

Definition 1.5. The class of a nilpotent group $G$ is the smallest such $n$ such that the central series terminates. Equivalently, it is the length of the lower (or upper) central series for the nilpotent group $G$. We then say that $G$ is nilpotent of class $n$.

Clearly, any abelian group is nilpotent of class 1.

Let $G$ be nilpotent of class 2. This means $G$ has the following lower central series:
\[ G \triangleright [G, G] \triangleright [[G, G], G] = \{1\}. \]

We have the following results for $G$:

- $[G, G] \leq Z(G)$: this is clear since $[[G, G], G] = \{1\}$.

- For all $x, y, z \in G$, $[xy, z] = [x, y][x, z]$: this is true since $[x, y][x, z] = x^{-1}y^{-1}xyx^{-1}z^{-1}xz = x^{-1}(y^{-1}xyx^{-1})z^{-1}xz = x^{-1}z^{-1}(y^{-1}xyx^{-1})xz = x^{-1}y^{-1}xyz = [x, yz]$.

- For all $x, y, z \in G$, $[xy, z] = [x, z][y, z]$.

- For all $x, y \in G$, $[x^m, y^n] = [x, y]^{mn}$.

Definition 1.6. The Heisenberg group, $H_3(R)$, is an infinite group consisting of upper triangular $3 \times 3$ matrices of the form
\[
\begin{pmatrix}
1 & a & c \\
0 & 1 & b \\
0 & 0 & 1
\end{pmatrix},
\]
where the entries $a$, $b$, and $c$ are elements of a commutative ring $R$. If the ring is taken to be $\mathbb{Z}$, then

$$H_3(\mathbb{Z}) = \langle A, B, C \mid [A, B] = C, [C, A] = [C, B] = I \rangle,$$

where $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Every element of the Heisenberg group may be written in the form $D = A^m B^n C^k$. We note that the Heisenberg is nilpotent of class 2. We will study this group in more details in Section 6.

We conclude with the following useful facts about nilpotent groups:

1. Every subgroup and every factor group of a nilpotent group is nilpotent.
2. The direct product of a finite number of nilpotent groups is nilpotent.

2. Complete Nilpotent Groups

The following has been taken mainly from [9] and [10] with some exposition.

**Definition 2.1.** A group $G$ is *complete* if for any $a \in G$ and an arbitrary $n \in \mathbb{N}$, the equation $x^n = a$ has at least one solution in $G$. In other words, any root of every element of $G$ belongs to $G$.

For groups under addition, this is equivalent to saying that for every natural number $n$ and every element $a$ in $G$, the equation $nx = a$ has at least one solution in $G$.

All complete abelian groups are decomposable into the direct sum of groups which are isomorphic to the additive group of rational numbers and the group of type $p^\infty$ (the multiplicative group of roots of unity whose degrees are powers of $p$). ([9] pages 165 - 166).

For the remainder of this section, we will focus on Černikov complete groups.

**Definition 2.2.** A group $G$ is *Černikov complete* if for every $n \in \mathbb{N}$, $G$ is generated by the $n$-th powers of all its elements.

**Definition 2.3.** A group is said to be a *ZA-group* if it has an ascending well-ordered central system, or an *ascending central series*.

Most properties of nilpotent groups carry over to ZA-groups. In particular, every subgroup and every factor group of a ZA-group is a ZA-group. A
group is a ZA-group if and only if its upper central chain, possibly continued transfinetly, leads up to the group $G$.

**Lemma 2.4 (Grünn’s Lemma).** If a group $G$ has a center $Z(G)$ other than $\{1\}$ and if the center of $G/Z$ is also different from $\{1\}$, then there exists a homomorphic mapping of $G$ onto a subgroup of $Z(G)$ other than $\{1\}$.

**Proof.** Let $\{1\} \leq Z_1 \leq Z_2 \leq \cdots \leq Z_k \leq \cdots$ be the ascending central chain for $G$. Let $a \in Z_2 \setminus Z_1$ and $x \in G$. Note that since $Z_2/Z_1 = Z(G/Z_1)$, it follows that $az_1$ commutes with $x z'_1$ for $z_1, z'_1 \in Z_1 = Z(G)$. Let $g \in G$ and $z \in Z_1$. We compute

$$[[a, x], g] = [a, x]^{-1}g^{-1}[a, x]g = x^{-1}a^{-1}x a^{-1}a^{-1}x^{-1}axg$$

$$= (x^{-1}z)(a^{-1}z^{-1})x a g^{-1}a^{-1}x^{-1}axg$$

$$= (a^{-1}z^{-1})(x^{-1}z)x a g^{-1}a^{-1}x^{-1}axg$$

$$= g^{-1}a^{-1}x^{-1}axg$$

$$= g^{-1}a^{-1}(x^{-1}z)(az^{-1})xg$$

$$= g^{-1}a^{-1}(az^{-1})(x^{-1}z)xg$$

$$= 1$$

This shows that $[a, x] \in Z_1$. Since $a \notin Z_1$, there exists $y \in G$ such that $[a, y] \neq 1$. Now let $\varphi : G \to Z_1$ be defined by $\varphi(x) = [a, x]$. Clearly, $\varphi$ is a nontrivial homomorphism from $G$ to a subgroup of $Z_1$. \hfill $\Box$

From this lemma, we can see that a non-commutative ZA-group contains a nontrivial abelian factor group and is therefore distinct from its derived group.

**Definition 2.5.** A $p$–primary group is an abelian group in which the orders of all elements are powers of a fixed prime number $p$. An element $a$ of a $p$–primary group $G$ is said to be of infinite height if for every $k$ the equation $p^k x = a$ has at least one solution in $G$. If this equation can be solved for $k \leq h$, then we say the element $a$ is an element of finite height, or of height $h$.

We will state but not prove the following two theorems. For their proofs, we refer the reader to [9], pages 171 - 173.

**Theorem 2.6 (Kulikov’s Criterion).** A primary abelian group $G$ is a direct sum of cyclic groups if and only if it is the union of an ascending sequence of subgroups

$$A^{(1)} \leq A^{(2)} \leq \cdots A^{(n)} \leq \cdots$$

such that the elements of each subgroup are of finite and bounded height in $G$. 


**Theorem 2.7** (Prüfer’s First Theorem). Every primary group in which the orders of the group elements are bounded is a direct sum of cyclic groups.

**Proposition 2.8.** A ZA-group is Černikov complete if and only if it contains no proper subgroup of finite index.

**Proof.** Let $G$ be a Černikov complete group, not necessarily a ZA-group. If $G$ has a proper subgroup of finite index, then it contains a proper normal subgroup of finite index. However, a Černikov complete group cannot have nontrivial finite factor groups because the homomorphic image of a Černikov complete group is itself Černikov complete and a finite group other than $\{1\}$ cannot be Černikov complete.

Now let $G$ be a ZA-group containing no proper subgroup of finite index. Let $n \in \mathbb{N}$, arbitrary. Let $H = \{x^n | x \in G\}$ be the subgroup generated by the $n$-th power of elements of $G$. We want to show that $H = G$. If not, consider $G/H$, where $H$ is normal in $G$. This is either abelian, or (by Grün’s Lemma) has a nontrivial abelian factor group. For either case, $G$ has a nontrivial abelian factor group with elements of bounded order. Then by Prüfer’s First Theorem, this factor group is the direct product of cyclic groups and therefore has a proper subgroup of finite index, corresponding to a proper subgroup of finite index in $G$. This contradicts the assumption. \qed

It follows that since nilpotent groups of class two contain normal subgroups of finite index, they are not Černikov complete. In particular, the Heisenberg group is not Černikov complete.

### 3. Groups with Unique Extraction of Roots

In this section, we will study nilpotent groups and extraction of roots in these groups. Again, the following has been taken from [10] with exposition.

**Definition 3.1.** A group $G$ is an $R$-group if for every $a \in G$ and every $n \in \mathbb{N}$, the equation $x^n = a$ has at most one solution. In other words, the extraction of roots is unique and for every pair of elements $x$ and $y$ and every natural number $n$, it follows from $x^n = y^n$ that $x = y$.

Note that every $R$-group is torsion-free and all abelian torsion-free groups are $R$-groups. However, not every torsion-free group is an $R$-group. For example, let $G = \langle a, b; a^2b^{-2} = 1 \rangle$ be the amalgamated free product of two infinite cyclic groups. $G$ is torsion-free but not an $R$-group.
Definition 3.2. A subgroup $A$ of an $R$–group $G$ is said to be an isolated subgroup if for every element $a \in A$ and every $n \in \mathbb{N}$ the solution to $x^n = a$, if it exists, is an element in $A$.

Definition 3.3. Let $M$ be a set of elements of an $R$–group $G$. The isolated closure, or isolator of $M$ in $G$, denoted $I(M)$, is the unique minimal isolated subgroup of $G$ containing $M$.

A normal subgroup $N$ of an $R$–group $G$ is isolated if and only if the factor group $G/N$ is torsion-free.

Proposition 3.4. If $H$ is an isolated subgroup of an $R$–group $G$ and if $G/H$ is an $R$–group (note that this isn’t always true), then in the natural one-to-one correspondence between all subgroups of $G/H$ and all subgroups of $G$ containing $H$, isolated subgroups correspond to each other. In other words, isolated subgroups of $G/H$ correspond to isolated subgroups of $G$ containing $H$.

Proof. Suppose that $A/H$ is an isolated subgroup of $G/H$ and we have $g^n = a$ for $g \in G$ and $a \in A$. We want to show that $g \in A$. Since $g^n = a$ and $A/H$ is an isolated subgroup of $G/H$, then $(gH)^n = aH$ implies that $gH \in A/H$ so that $g \in A$.

Now suppose that $A$ is an isolated subgroup of $G$ containing $H$ and that $(gH)^n = aH$ for $g \in G$ and $a \in A$. This implies that $g^n = ah \in A$. Since $A$ is isolated, this means that $g \in A$ so $gH$ is an element of $A/H$, hence isolated.

Proposition 3.5. The centralizer of an arbitrary set of elements of an $R$–group $G$ is an isolated subgroup.

Proof. Let $M$ be an arbitrary set of elements of $G$. Let $x$ an element of $G$ such that $x^n$ is an element of the centralizer of $M$. Then $a^{-1}x^n a = x^n$ for all $a \in M$ implies that $(a^{-1}xa)^n = x^n$. Since $G$ is an $R$–group, this means that $a^{-1}xa = x$, so $x \in C_G(M)$ as well.

It follows that the center of an $R$–group is isolated.

Proposition 3.6. In every $R$–group $G$, the equation $a^k b^\ell = b^\ell a^k$, where $a, b \in G$, implies that $ab = ba$.

Proof. It suffices to prove this proposition when one of $k$ or $\ell$ is 1. Without loss of generality, we assume that $\ell = 1$ so that we have $a^k b = ba^k$ and we want to show that this implies $ab = ba$ for $a$ and $b$ in an $R$–group $G$. Now, $(b^{-1}ab)^k = b^{-1}a^k b = b^{-1}ba^k = a^k$. Since $G$ is an $R$–group, this implies that $b^{-1}ab = a$. 

Proposition 3.7. A torsion-free group is an $R$–group if and only if the factor group of its center is an $R$–group.

Proof. Let $G$ be a torsion-free $R$–group. Since the center $Z = Z(G)$ of $G$ is isolated, we know $G/Z$ is torsion-free. We want to show that $G/Z$ is an $R$–group. Suppose $(xZ)^n = (yZ)^n$, for $x, y \in G$. Therefore, $x^n = y^n z$ for $z \in Z$. This means that $y^{-n}x^n = z$. We also have $x^n = zy^n$ so $x^n y^{-n} = z$. Hence, $x^n y^{-n} = y^{-n} x^n$. From Proposition 3.6, this means that $xy = yx$. Now, $x^n = y^n z$ and $xy = yx$ implies that $(y^{-1}x)^n = z$. Since $Z$ is isolated, $y^{-1}x \in Z$, so $xZ = yZ$.

Conversely, let $G$ be torsion-free and let the factor group $G/Z$ be an $R$–group. Suppose that $x^n = y^n$ for $x, y \in G$. Then $(xZ)^n = (yZ)^n$. Since $G/Z$ is an $R$–group, this implies that $xZ = yZ$, or $x = yz$, $z \in Z$. Raising this to the $n$-th power gives $x^n = (yz)^n = y^n z^n$. But the assumption that $x^n = y^n$ now tells us that $z^n = 1$. Since $G$ is torsion-free, this implies that $z = 1$, or $x = y$.

Proposition 3.8. All the terms of the upper central chain

$$
\{1\} = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots \trianglelefteq Z_\alpha \trianglelefteq \ldots
$$

of an $R$–group $G$ are isolated in $G$, all the factors $Z_\alpha/Z_{\alpha-1}$ of this chain are abelian torsion-free groups, and all the factor groups $G/Z_\alpha$ are $R$–groups.

Proof. Since $Z_1$ is the center of $G$, it is isolated in $G$. The factor group $Z_1/Z_0 = Z_1$ is an abelian torsion-free group and the factor group $G/Z_1$ is an $R$–group.

Suppose that the theorem has been proved for $\alpha < \beta$. If $\beta - 1$ exists, then $G/Z_{\beta-1}$ is an $R$–group and its center, $Z_\beta/Z_{\beta-1}$, is an abelian torsion-free group; the factor group of the center, isomorphic to $G/Z_\beta$, is an $R$–group (by Proposition 3.7); and from the fact that the center of the $R$–group $G/Z_{\beta-1}$, $Z_\beta/Z_{\beta-1}$, is isolated, we also have $Z_\beta$ is isolated (by 3.4).

If $\beta$ is a limit number, then $Z_\beta$ is the union of an ascending sequence of isolated subgroups and is therefore isolated. Furthermore, if $(xZ_\beta)^n = (yZ_\beta)^n$ for $x, y \in G$, then $x^n = y^n z$ for $z \in Z_\beta$, and therefore $z \in Z_\alpha$, $\alpha < \beta$. Therefore, $(xZ_\alpha)^n = (yZ_\alpha)^n$ and since $G/Z_\alpha$ is assumed to be isolated, this implies that $xZ_\alpha = yZ_\alpha$. From this, we conclude that $xZ_\beta = yZ_\beta$ so $G/Z_\beta$ is an $R$–group.

Proposition 3.9. The isolator of an arbitrary element other than the unit element of an $R$–group is an abelian torsion-free group of rank 1 and is the isolator of each of its elements other than 1. The isolators of any two elements of an $R$–group either are identical or else intersect in the unit element.
Proof. Let $G$ be a torsion-free group, $x \in G$, $x \neq 1$. Then $x$ generates an infinite cyclic subgroup which is an abelian torsion-free group of rank 1. Since the union of an ascending sequence of abelian torsion-free groups of rank 1 is a group of the same kind, $x$ is contained in at least one subgroup $A$ that is a maximal abelian torsion-free subgroup of $G$ of rank 1. If $G$ is an $R$–group, then $A$ is contained in the isolator $I(x)$ of $x$: for an arbitrary $a \in A$, the cyclic subgroups $\{x\}$ and $\{a\}$ have intersection other than $\{1\}$, but $\{x\} \subset I(x)$.

Suppose $x$ is contained in two distinct maximal abelian torsion-free subgroups of rank 1, $A$ and $B$; the intersection of these two subgroups will not be $\{1\}$. Let $a \in A$, $b \in B$ be arbitrary elements, other than 1. Since there exists $i, j \in \mathbb{Z}$ such that $a^i = b^j$, this implies that $a$ and $b$ are permutable. Therefore, $\{A, B\}$ is an abelian torsion-free group. However, in such a group distinct maximal subgroups of rank 1 cannot have intersection other than $\{1\}$. Thus the theorem follows.

Proposition 3.10. Every nilpotent torsion-free group is an $R$–group. That is, unique extraction of roots in nilpotent torsion-free groups is possible.

Proof. For abelian torsion-free groups, the statement is clear. We will prove by induction on the class of the nilpotent group. We assume that the statement is true for all nilpotent groups of class less than or equal to $k - 1$, $k > 1$. Let $G$ be a torsion-free group of class $k$ with upper central series

$$\{1\} = Z_0 \leq Z_1 \leq \cdots \leq Z_{k-1} \leq Z_k = G$$

and let $x, y \in G$ such that $x^n = y^n$, $n > 0$. Consider the subgroup $H = \{Z_{k-1}, x\}$. $H$ is normal in $G$ since $G/Z_{k-1}$ is abelian. In addition, $H$ is nilpotent of class less than or equal to $k - 1$: in any noncommutative group the factor group of the center cannot be cyclic. Hence, by the inductive hypothesis, $H$ is an $R$–group. Therefore, $x^n = y^n$ implies that $y^{-1}x^n = y^{n-1} = x^ny^{-1}$, or $x^n = y^{-1}x^ny = (y^{-1}xy)^n$. Since $x$ and $y^{-1}x^ny$ belong to the $R$–group $H$, we have $x = y^{-1}xy$, or $xy = yx$. Therefore, $x^n = y^n$ may be rewritten $(y^{-1}x)^n = 1$. Since $G$ is torsion-free, this means that $x = y$.

This proposition only states that if $G$ is a torsion-free nilpotent group, then $x^n = a$ has a unique solution in $G$; it does not show us how to find $x$.

A natural question that arises is if there is a relation between Černikov complete groups and $R$–groups. In Section 2, we showed that the Heisenberg group is not Černikov complete. Since a complete group is Černikov complete, this implies that the Heisenberg group is not complete. Hence, we may not take arbitrary $n$-th roots in the Heisenberg group. However, since the Heisenberg
group is torsion-free, it is an $R$–group. That is, if the $n$-th root of an element exists in the Heisenberg group, the root is unique. Therefore, it is possible for a group to be an $R$–group but not Černikov complete.

4. Algorithm to find the $n$-th root in the Nilpotent Group

There is a theorem of Mal’cev that states that every torsion-free nilpotent group can be embedded in a torsion-free nilpotent group in which every element has an $n$-th root for every $n \in \mathbb{N}$. For a finitely generated torsion-free nilpotent group, one way of doing this is by embedding the group in a group of upper-triangular matrices over $\mathbb{Q}$. We write every element in the form $I + N$, where $I$ is the identity matrix and $N$ is a matrix with zeros on and below the main diagonal. Note that there is an $m \in \mathbb{Z}$ such that $N^m = 0$. We can then use the binomial expansion to expand $(I + N)^{1/n}$.

4.1. Complexity Analysis

The complexity of finding the $n$-th root in nilpotent group, lies on the difficulty of embedding the group into a group of upper-triangular matrices over $\mathbb{Q}$. The most efficient known algorithm is by Werner Nickel in [13]. As it has been described in the experimental approach, it suggests it admits exponential time algorithm.

The algorithm is efficient enough to be able to deal with groups of rather large Hirsch length. However, the running times obtained appear to increase exponentially while the dimensions seem to depend polynomially on the Hirsch length of the group. Presently, we do not have any theoretical bounds on the dimension of the modules constructed, nor the running time.

Example 4.1. [8] Let $T : \mathbb{C}^n \to \mathbb{C}^n$ be a linear operator, where $T$ is multiplication by the Jordan block

$$J_{n,c} = \begin{pmatrix} c & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & c \end{pmatrix},$$

where $c \neq 0$. We want to know when there is a linear operator $S : \mathbb{C}^n \to \mathbb{C}^n$ such that $S^2 = T$. 
Let

\[ N = \frac{J_{n,0}}{c} = \begin{pmatrix}
0 & \frac{1}{c} & 0 & \cdots & 0 \\
0 & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & 0 \\
\vdots & & & \ddots & \frac{1}{c} \\
0 & \cdots & \cdots & 0 & 0
\end{pmatrix}. \]

Then \( T = c(I + N) \) and \( N \) is nilpotent with \( N^n = 0 \).

Now recall the binomial expansion for \( \sqrt{1 + x} \):

\[
\sqrt{1 + x} = 1 + \frac{1}{2}x + \frac{1}{2!(−1/2)}x^2 + \frac{1}{3!(−3/2)}x^3 + \cdots
\]

and squaring both sides yields

\[
1 + x = \left( 1 + \frac{1}{2}x + \frac{1}{2!(−1/2)}x^2 + \frac{1}{3!(−3/2)}x^3 + \cdots \right)^2.
\]

Substituting \( I \) for 1 and \( N \) for \( x \),

\[
I + N = \left( I + \frac{1}{2}N + \frac{1}{2!(−1/2)}N^2 + \frac{1}{3!(−3/2)}N^3 + \cdots \right)^2.
\]

Since \( N^n = 0 \), this series has at most \( n + 1 \) terms. If

\[
A = \sqrt{c}\left( I + \frac{1}{2}N + \frac{1}{2!(−1/2)}N^2 + \frac{1}{3!(−3/2)}N^3 + \cdots \right),
\]

then \( A^2 = c(I + N) = T \) and we have found a square root of \( T \).

**Example 4.2.** Let \( N = \frac{J_{3,0}}{16} = \begin{pmatrix} 0 & \frac{1}{16} & 0 \\
0 & 0 & \frac{1}{16} \\
0 & 0 & 0 \end{pmatrix} \). Here, \( c = 16 \), \( N^2 = \begin{pmatrix} 0 & 0 & \frac{1}{256} \\
0 & 0 & 0 \\
0 & 0 & 0 \end{pmatrix} \) and \( N^3 = 0 \). We define \( T = 16(I + N) = \begin{pmatrix} 16 & 1 & 0 \\
0 & 16 & 1 \\
0 & 0 & 16 \end{pmatrix} \).

Then using the above computations, we have \( \sqrt{T} = A = 4(I + \frac{1}{2}N - \frac{1}{8}N^2) = \begin{pmatrix} 4 & \frac{1}{32} & \frac{1}{12} \\
0 & 4 & \frac{1}{8} \\
0 & 0 & 4 \end{pmatrix} \).
Example 4.3. Let $T = J_{3,9} = \begin{pmatrix} 9 & 1 & 0 \\ 0 & 9 & 1 \\ 0 & 0 & 9 \end{pmatrix}$. Find the square root of $T$.

We have $c = 9$ and compute $N = \frac{J_{3,0}}{9} = \begin{pmatrix} 0 & \frac{1}{9} & 0 \\ 0 & 0 & \frac{1}{9} \\ 0 & 0 & 0 \end{pmatrix}$, $N^2 = \begin{pmatrix} 0 & 0 & \frac{1}{81} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $N^3 = 0$. Then $\sqrt{T} = 3 \left( \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 & \frac{1}{9} & 0 \\ 0 & 0 & \frac{1}{9} \\ 0 & 0 & 0 \end{pmatrix} - \frac{1}{8} \begin{pmatrix} 0 & 0 & \frac{1}{81} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right) = \begin{pmatrix} 3 & \frac{1}{6} & -\frac{1}{16} \\ 0 & 3 & \frac{1}{6} \\ 0 & 0 & 3 \end{pmatrix}$.

The result is similar for $n$-th roots; if we take $A = \sqrt[2]{c} \left( I + \frac{1}{n} N + \frac{1}{n} \left( \frac{1 - n}{n} \right) \frac{N^2}{2!} + \frac{1}{n} \left( \frac{1 - n}{n} \right)^2 \left( \frac{1 - 2n}{n} \right) \frac{N^3}{3!} + \cdots \right)$, then $A^n = T = c(I + N)$.

5. Square Roots of Finite Groups

In this section, we follow the work of Abhyankar and Grossman [1].

**Definition 5.1.** Let $G$ be a finite group and for $X \subseteq G$, let

$$X^2 = \{x_1 x_2 \mid x_1, x_2 \in X\}.$$ 

Then $X \subseteq G$ is said to be a **perfect square root of $G$** if

1. $X^2 = G$, and
2. $|X|^2 = |G|$.

Note that since $X^2 = G$ and $|X|^2 = |G|$, every element appears once in the multiplication table for $X$. We can then conclude that distinct elements of a perfect square root do not commute. From this observation, is is clear that if $G$ has a perfect square root, $G$ is non-Abelian and $X$ does not contain elements of $Z(G)$. We have the following lemmas that provide necessary conditions for a group to have perfect square roots:

**Lemma 5.2.** Let $G$ be a group with perfect square root. Then 4 divides the order of $G$. 
Proof. The identity element 1 must be the product of two elements of \( X \). Since inverse pairs always commute and distinct elements of \( X \) do not commute, we must have \( x^2 = 1 \) for some \( x \in X \). Now, \( x \neq 1 \) because \( 1 \in Z(G) \). Hence, \( x \) must have order 2, so \( |G| \) has even order. It follows that \( |G| \) is a multiple of 4 since it is a perfect square.

\( \square \)

Lemma 5.3. If \( G \) has a perfect square root, then \( |Z(G)|^2 < |G| \).

Proof. Let \( X \) be a perfect square root of \( G \). Since the elements of \( X \) do not commute, no two elements of \( X \) are in the same coset of \( Z = Z(G) \): for if \( z_1, z_2 \in Z \), then \((az_1)(az_2) = (az_2)(az_1)\). Let \( |G| = n^2 \) so that there are at least \( n \) cosets of \( Z \) from which to choose as elements of \( X \). That is, we have \( [G : Z] = \frac{|G|}{|Z|} \geq n \), or \( n \geq |Z| \). Now we can conclude that \( |Z|^2 < |G| \) since \( X \) contains no elements of \( Z \).

\( \square \)

Lemma 5.4. Let \( G \) be a finite group with perfect square root \( X \). Then for each \( z \in Z(G) \), there is some \( x \in X \) such that \( x^2 = z \).

Proof. Each \( z \in Z(G) \) is the product of two elements of \( X \), say \( x_1 \) and \( x_2 \). Since \( z \in Z(G) \) and the pairs \( x_1x_2 \) and \( x_2x_1 \) are conjugate, we must have \( x_1x_2 = x_2x_1 \). This contradicts the fact that elements of \( X \) do not commute. Hence, \( x_1 = x_2 \) and \( z = x_1^2 \).

\( \square \)

Definition 5.5. Let \( G \) be nilpotent of class 2. That is, \( G \) satisfies \([G, G, G] = \{1\}\). We define \( Q(G) = \{q \in G|q^2 \in Z(G)\} \).

We have the following results:

Lemma 5.6. \( Q = Q(G) \) is a normal subgroup of \( G \).

Proof. We first show that \( Q \) is a subgroup of \( G \): let \( q_1, q_2 \in Q \). Then

\[
(q_1q_2^{-1})^2 = q_1q_2^{-1}q_1q_2^{-1} = q_1(q_1^{-1}q_2q_1^{-1})q_2^{-1}q_1q_2^{-1} = q_1q_2^{-1}(q_2q_1^{-1}q_2^{-1}q_1)q_2^{-1} = q_1^2q_2^{-2}q_2^{-1}q_1q_2^{-1} = q_1q_2^{-2} \in Z(G).
\]

Next, to see that \( Q \) is normal in \( G \), let \( g \in G \). Then \( (g^{-1}q_1g)^2 = g^{-1}q_1^2g = q_1^2 \in Z(G) \).

\( \square \)

Lemma 5.7. Let \( q \in Q(G) \). Then every commutator \([q, g]\) has order 1 or 2.

Proof. \([q, g]^2 = [q^2, g] = 1\).

\( \square \)
Definition 5.8. Let \(G\) be nilpotent of class 2. Define \(M(G) = \{g \in G | g = g_1g_2 \cdots g_n, \) where each factor \(g_i \in G\) occurs an even number of times, with occurrences of \(g_i^{-1}\) counted together with occurrences of \(g_i\}\}. Clearly, \(M = M(G)\) is a normal subgroup of \(G\).

Lemma 5.9. \(G/M\) is an elementary Abelian two-group.

Proof. If \(gM \in G/M\), then \((gM)^2 = g^2M = M\). \(\square\)

Lemma 5.10. Let \(C_G(Q) = \{g \in G | gq = qg, q \in Q\}\) (that is, \(C_G(Q)\) is the centralizer in \(G\) of \(Q\)). Then \(M \leq C_G(Q)\).

Proof. Let \(q \in Q\) and \(m = g_1g_2 \cdots g_n \in M\). Then
\[
[q, m] = [q, g_1g_2 \cdots g_n] = [q, g_1][q, g_2] \cdots [q, g_n],
\]
where distinct \(g_i\)'s occur an even number of times. Since \(G\) is nilpotent of class two, each \([q, g_i] \in Z(G)\). By Lemma 5.7, \([q, g_i]^2 = 1\). Hence, \([q, m] = 1\). \(\square\)

This last lemma implies that no element of the perfect square root \(X\) of \(G\) is contained in \(M\). For if it is, an element of \(X\) would commute with \(Q \cap X\) (which is nonempty by Lemma 5.4), contradicting the fact that no two elements of \(X\) commutes.

Theorem 5.11. If \(G\) is nilpotent of class 2, then \(G\) has no perfect square root.

Proof. We will prove by contradiction. Suppose that \(G\) is nilpotent of class 2 and that \(X\) is a perfect square root of \(G\). Let \(M\) be as defined above. We will denote the image of \(X\) in \(G/M\) by \(\overline{X}\). Further, we will consider \(\overline{X}\) as a multiset instead of a set, since distinct elements of \(X\) may be mapped to same cosets of \(M\). We will look at the occurrences of elements of \(M\) in the multiplication table of \(X\) by finding a bound for occurrences of \(1 \in G/M\) in the multiplication table for \(\overline{X}\).

Let the distinct elements of \(\overline{X}\) be \(a_0, a_1, \ldots, a_{k-1}\), so that there are \(k\) distinct cosets of \(M\) in \(X\). Let \(|X| = |\overline{X}| = n = kq + r\), where \(0 \leq r < k\). List the elements of the multiset \(\overline{X}\) as \(b_0, b_1, \ldots, b_{n-1}\) as follows:

- Let \(b_0 = a_0\).
- Suppose \(b_i = a_j\). Then let

\[
b_{i+1} = \begin{cases} 
  a_{j+1} & \text{if } j < k - 1 \\
  a_0 & \text{if } j = k - 1 
\end{cases}
\]
unless all occurrences of $a_{j+1}$ (or $a_0$) in $X$ have been used in the ordering, in which case we use the next $a_m$ not already exhausted.

Now we partition the multiset $X$ into submultisets $S_0, S_1, \ldots S_{q-1}$ with $k$ elements and submultiset $S_q$ with $r$ elements by the following rule:

- For $i = 0, 1, \ldots, q-1$, $S_i = \{ b_{ik}, b_{ik+1}, \ldots, b_{ik+(k-1)} \}$
- $S_q = \{ a_{qk}, a_{qk+1}, \ldots, a_{qk+(r-1)} \}$

Note that $S_q$ may be empty (when $r = 0$) and $S_0$ contains $a_0, a_1, \ldots, a_{k-1}$. In addition, the set of distinct elements of $S_i$ is a subset of the set of distinct elements of $S_{i-1}$.

Next, consider the multiplication table for $|X|$ as a union of tables $S_i S_j$ for $0 \leq i, j \leq q$. In the table $S_i S_j$, the number of occurrences of 1 is at least $\min\{|S_i|, |S_j|\}$, since if $i \leq j$, each element of $S_j$ is in $S_i$, and the square of any element of $G/M$ is equal to 1 (Lemma 5.9). Therefore, each row of $S_i S_j$ contains an occurrence of 1. Also,

$$\min\{|S_i|, |S_j|\} = \begin{cases} k & \text{if } i, j < k \\ r & \text{otherwise} \end{cases}$$

Hence, the occurrences of 1 in the multiplication table for $|X|$, which equals $|M|$, is bounded by

$$|M| = \sum_{i=0}^{q} \sum_{j=0}^{q} \min\{|S_i|, |S_j|\} = kq^2 + rq + r(q+1) = kq^2 + 2rq + r$$

We have

$$|G| = |X|^2 = (kq + r)^2 = k^2q^2 + 2kq + r^2$$

$$[G : M] \leq \frac{k^2q^2 + 2kq + r^2}{kq^2 + 2rq + r} = k \frac{k^2q^2 + 2kq + r^2}{k^2q^2 + 2k^2q + kr} \leq k$$

because $r < k$. Now, since the coset $M$ does not contain elements of $X$, we also know that $[G : M] > k$ (since there are $k$ cosets of $M$ in $X$), which is a contradiction. \qed
6. The Heisenberg Group

6.1. Roots in $H_3(\mathbb{Z})$

Recall that the Heisenberg group is nilpotent of class 2 and that any element can be written in the form $D = A^m B^n C^k$, where

\[
A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\]

That is, we can write

\[
D = A^m B^n C^k = \begin{pmatrix} 1 & m & k + mn \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}.
\]

**Proposition 6.1.** Let $r \in \mathbb{N}$. The matrix $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = A^a B^b C^c - ab$ has an $r$-th root in the Heisenberg group if and only if $a \equiv 0 \pmod{r}$, $b \equiv 0 \pmod{r}$, and $c - \frac{1}{2} ab(\frac{1}{r} + 1) \equiv 0 \pmod{r}$.

**Proof.** Suppose that

\[
M = D^r = (A^m B^n C^k)^r = \begin{pmatrix} 1 & mr & rk + \frac{1}{2} rmn(1 + r) \\ 0 & 1 & nr \\ 0 & 0 & 1 \end{pmatrix} = A^{mr} B^{nr} C^{rk + \frac{1}{2} rmn(1 - r)}
\]

This shows that

\[
a = mr \\
b = nr \\
c - ab = rk + \frac{1}{2} rmn(1 - r)
\]

Hence, $a \equiv 0 \pmod{r}$, $b \equiv 0 \pmod{r}$, and $c - ab = rk + \frac{1}{2} r \cdot \frac{2}{r} \cdot \frac{b}{r}(1 - r) = rk + \frac{ab}{2}(\frac{1}{r} - 1)$, or $c - \frac{1}{2} ab(1 + \frac{1}{r}) \equiv 0 \pmod{r}$. \qed
Corollary 6.2. A matrix \( D = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \) in the Heisenberg group has a square root if and only if \( a \equiv 0 \pmod{2} \), \( b \equiv 0 \pmod{2} \) and \( c - 3ab \equiv 0 \pmod{2} \).

In the proof of Proposition 6.1, we showed how to find the \( r \)-th root of a matrix in \( H_3(\mathbb{Z}) \). In particular, if we want to find the square root of \( M = A^a B^b C^{c-ab} \), we only need to solve the system of equations
\[
\begin{align*}
a &= 2m \\
b &= 2n \\
c - ab &= 2k - mn,
\end{align*}
\]
for \( m, n, \) and \( k \) and we will see that the square root of \( M \) is \( D = A^m B^n C^k \).

Example 6.3. Given that \( D^2 = \begin{pmatrix} 1 & 4 & 26 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} \) in the Heisenberg group, find \( D \).

We have \( a = 4 \) and \( b = 6 \). This means that \( m = 2 \) and \( n = 3 \). Next, \( 26 - 4(6) = 2k - (2)(3) \) implies that \( k = 4 \). Hence, \( D = A^2 B^3 C^4 = \begin{pmatrix} 1 & 2 & 10 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \).

Example 6.4. Does \( \begin{pmatrix} 1 & -12 & 5 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} \) have a square root in the Heisenberg group?

We have \( a = -12, b = 6 \) and \( c = 5 \). Clearly, \( a \equiv b \equiv 0 \pmod{2} \). However, \( c - \frac{3ab}{4} = 5 - \frac{3(-12)(6)}{4} = 5 + 54 \not\equiv 0 \pmod{2} \). Therefore, the given matrix does not have a square root in the Heisenberg group.

7. Engel Groups

Definition 7.1. A group is said to be \( n \)-Engel if for every pair \((x, y) \in G \times G\) there exists an \( n = n(x, y) \) such that \([\cdots [[x, y], y], \cdots y]_n = 1\).

Here are some theorems related to \( n \)-Engel groups and nilpotent groups (see [17] for more information).
Theorem 7.2. (Zorn, 1936) Every finite Engel group is nilpotent.

Theorem 7.3. (Gruenberg, 1953) Every finitely generated solvable Engel group is nilpotent.

Theorem 7.4. (Baer, 1957) Every Engel group satisfying max is nilpotent.

Theorem 7.5. (Suprenenko and Garscuk, 1962) Every linear Engel group is nilpotent.

Proposition 7.6. The Heisenberg group is a 2-Engel group.

Proof. We want to show that \([X, Y], Y] = I\). Let \(X = A^m B^n C^k = \begin{pmatrix} 1 & m & k + mn \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}\) and \(Y = A^u B^v C^w = \begin{pmatrix} 1 & u & w + uv \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix}\). Then \(X^{-1} = \begin{pmatrix} 1 & -m & -k \\ 0 & 1 & -n \\ 0 & 0 & 1 \end{pmatrix}\) and \(Y^{-1} = \begin{pmatrix} 1 & -u & -w \\ 0 & 1 & -v \\ 0 & 0 & 1 \end{pmatrix}\). Next, \([X, Y] = X^{-1} Y^{-1} XY = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\). Finally, \([X, Y], Y] = [X, Y]^{-1} Y^{-1} [X, Y] Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\).

Lemma 7.7. Every element in the Heisenberg group satisfies \(XY^2Y = X Y^2 X\).

Proof. We will prove a more general case: in every 2-Engel group, \(yx^2y = xy^2x\). To see this, note that

\[
[y, x][x^{-1}, y^{-1}] = [y, x]xyx^{-1}y^{-1} = x[y, x]yx^{-1}y^{-1}
= x[y, x]yx^{-1}y^{-1}xx^{-1} = x[y, x][y^{-1}, x]x^{-1}
= x[e, x]x^{-1} = e.
\]

From this, we conclude that \([y, x] = [x^{-1}, y^{-1}]^{-1} = [y^{-1}, x^{-1}],\) which is equivalent to \(yx^2y = xy^2x\).

There are other semigroup laws for other Engel groups. Here, we will discuss the laws for 3-Engel and 4-Engel groups.
7.1. 3-Engel Groups

To describe 3-Engel groups we need two semigroup laws

\[ xy^2 xy x^2 y = yx^2 y xy^2 x \]
\[ xy^2 xy x^2 y = yx^2 y^2 x^2 y^2 x \]

7.2. 4-Engel Groups

In [16], G. Traustason showed 4-Engel groups can be described in terms of two semigroup identities. The following is one of them:

\[ xy^2 xy x^2 y^2 x^2 y xy^2 x^2 y xy^2 x^2 y xy^2 x^2 y = yx^2 y xy^2 x^2 y xy^2 x^2 y xy^2 x^2 y xy^2 x. \]

G. Traustason also showed 4-Engel groups with 2 generators are nilpotent (see [18]).

8. Applications and Computations

8.1. Modular Square Roots

Here, we present some definitions and results that will be useful in the Rabin-Key Exchange. For more information see [15] and [14].

**Definition 8.1.** Let \( m \in \mathbb{Z}^+ \) and \((a, m) = 1\). We say that \( a \) is a quadratic residue of \( m \) if \( x^2 \equiv a \pmod{m} \) has a solution. If \( x^2 \equiv a \pmod{m} \) has no solution, we say that \( a \) is a quadratic nonresidue of \( m \).

A useful notation for quadratic residues is the Legendre symbol, \((\frac{a}{p})\), defined by

\[
\left(\frac{a}{p}\right) = \begin{cases} 
0 & \text{if } a \equiv 0 \pmod{p} \\
-1 & \text{if } a \text{ is a quadratic nonresidue of } p \\
1 & \text{if } a \text{ is a quadratic residue of } p 
\end{cases}
\]

**Proposition 8.2.** Let \( p \) be an odd prime and \( a \not\equiv 0 \pmod{p} \). Then either \( x^2 \equiv a \pmod{p} \) has exactly two incongruent solutions modulo \( p \) or no solutions.

**Proposition 8.3** (Euler’s Criterion). Let \( a \not\equiv 0 \pmod{p} \), where \( p \) is an odd prime. Then

\[
\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.
\]
Note that when the modulus is \( n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m} \), we use the Jacobi symbol, \( \left( \frac{a}{n} \right) \), defined by
\[
\left( \frac{a}{n} \right) = \left( \frac{a}{p_1} \right)^{t_1} \left( \frac{a}{p_2} \right)^{t_2} \cdots \left( \frac{a}{p_m} \right)^{t_m},
\]
where the symbols on the right-hand side are Legendre symbols.

**Proposition 8.4.** Let \( p \) be a prime such that \( p \equiv 3 \pmod{4} \). The solutions of \( x^2 \equiv a \pmod{p} \) are \( x \equiv \pm a^{p+1} \pmod{p} \).

**Proposition 8.5.** Let \( n = pq \), where \( p \) and \( q \) are distinct odd primes. Let \( 0 < a < n \) and \((a,n) = 1\). Then \( x^2 \equiv a \pmod{n} \) has exactly four solutions modulo \( n \).

**Example 8.6.** Let \( n = 103 \cdot 107 = 11021 \). Suppose we know that \( x^2 \equiv 860 \pmod{11021} \) has solution. Then we need to solve
\[
x^2 \equiv 860 \equiv 36 \pmod{103}
\]
and
\[
x^2 \equiv 860 \equiv 4 \pmod{107}.
\]
Since \( 103 \equiv 3 \pmod{4} \) and \( 107 \equiv 3 \pmod{4} \), we know that the solutions are
\[
x \equiv \pm 36^{26} \equiv \pm 97 \equiv \pm 6 \pmod{103}
\]
and
\[
x \equiv \pm 4^{27} \equiv \pm 105 \equiv \pm 2 \pmod{107},
\]
respectively. By the Chinese Remainder Theorem, \( x \equiv \pm 109 \pmod{11021} \) or \( x \equiv \pm 212 \pmod{11021} \).

**8.2. Rabin Public Key Encryption**

As usual, we assume that Alice and Bob are sending messages through an insecure channel. Alice will choose two large primes, \( p \) and \( q \), which will be private. Her public key is \( n = pq \). Bob sends his message \( m \) by computing \( c \equiv m^2 \pmod{n} \) and sending \( c \) to Alice. Alice recovers the message by using the methods discussed above, but she has four possible values for \( m \).

In order for Eve, the eavesdropper, to recover the message, she will need to know the factors \( p \) and \( q \). Factoring \( n \) and computing square roots modulo \( n \) are computationally equivalent. Therefore, security of this encryption scheme lies on the assumption that factoring \( n \) is computationally intractable.
A chosen-ciphertext attack may be used on this protocol: suppose Eve chooses a random \( m \in \mathbb{Z}_n^* \) and sends \( c \equiv m^2 \pmod{n} \) to Alice, who decrypts \( c \) and returns a plaintext \( y \). If \( y \not\equiv \pm m \pmod{n} \), then \( (m - y, n) \) is one of the prime factors of \( n \). If \( y \equiv \pm m \pmod{n} \), Eve repeats the attack with \( m^3 \).

To avoid this attack and the problem Alice has in deciding the correct \( m \) from \( c \equiv m^2 \pmod{n} \), an additional redundancy is added to the original plaintext prior to encryption. With high probability, one of the four solutions will have redundancy so Alice will not have difficulty deciding the correct \( m \). Furthermore, if Eve tries to use the chosen-ciphertext attack, Alice will always recover the correct \( m \) (assuming Eve follows the redundancy requirement, otherwise Alice will not be able to decrypt her message because none of the four values for \( m \) will have redundancy).

8.3. Complexity of Finding Square Roots

Recall that factoring \( n \) and computing square roots modulo \( n \) are computationally equivalent; that is, there is an algorithm that solves the factoring problem which uses an algorithm for solving the square root problem and vice versa. Computing square root modulo \( p \), where \( p \) is prime, can be performed efficiently, but computing square root modulo \( n \), where \( n \) is composite, is difficult when the prime factors are unknown.

When \( p \equiv 3 \pmod{4} \), the algorithm used to compute the square root has running time of \( O((\log_2 p)^3) \) bit operations. In general, to compute the square root modulo \( p \), the expected running time is \( O((\log_2 p)^4) \) bit operations.

When \( p \) and \( q \) are known, decrypting the Rabin cryptosystem requires \( O(\log n) \) bit operations, which is quick.

If there is an algorithm which can find the square root modulo \( n \) in polynomial time, then the algorithm can be used to factor \( n \) in expected polynomial time. This means that if we assume that factoring \( n \) is hard, then it will be difficult to find square roots modulo \( n \).

9. Cryptosystems Based on \( n \)-Engel Groups

9.1. A public Key Based on 2-Engel Groups

A satellite generates some data from a 2-Engel group. Alice and Bob choose two elements \( x(s, t) \) and \( y(s, t) \) respectively as their secret keys. Then Alice sends \( x^2 \) to Bob and Bob sends \( y^2 \) to Alice. Since in any 2-engel group, \( xy^2x = yx^2y \),
they both agree on a key. The security of this scheme lies on the difficulty of finding square roots in 2-Engel groups. (see [7] for more information about this part.)

One could extend this scheme to other $n$-Engel groups, since there are similar relations in them as well (see [17]).

9.2. A Digital Signature Based on 4-Engel Groups

Consider a 4-Engel group, which is nilpotent and satisfies the following semigroup law:

$$xy^2xy^2y^2x^2yxy^2y^2y^2xy^2y^2y^2 = yx^2yx^2y^2x^2y^2y^2x^2y^2y^2y^2$$

The idea to make a digital signature is as follows: Suppose $x$ and $y$ are secret and $x^2$, $y^2$, $xy^2x$ and $xy^2x^2y^2x$ public information.

The public key is $x^2$ and the signature is the tuple of $xy^2x$ and $xy^2x^2y^2x$. The verifier knows $y$, so he only needs to verify both of the semigroup identity. The security of this digital signature lies on the fact that the complexity of finding square root in a 4-Engel group is experimentally proved to be exponential. The Hirsch length of a 4–Engel group could even be 88 and nilpotent of class 9 (see Werner Nickel’s webpage and [12]) and by the best known algorithm by Nickel, we know that the complexity of finding matrix representations in a nilpotent group of class 9 and Hirsch length 88 is exponential; which ultimately gives us a solution to finding a square root in the underlying 4-engel group.

Acknowledgments

The authors are grateful to Professor Michael Anshel for helpful discussion in the early stage of this project. The authors also thank Professor Gilbert Baumslag for his useful comments. Delaram Kahrobaei, would like to thank Professor Derek Holt for his helpful comments during her visit to Warwick University. The research of Delaram Kahrobaei has been supported by a grant from the City Tech Foundation and PSC CUNY Research Foundation of CUNY. The research of Makenson and Renald has been supported by City Tech Foundation and NSF-AMP.
References


