www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (201x), pp. xx-xx.

www.ui.ac.ir

ALGORITHMIC PROBLEMS IN ENGEL GROUPS AND CRYPTOGRAPHIC APPLICATIONS

DELARAM KAHROBAEI AND MARIALAURA NOCE*

Communicated by

Abstract. The theory of Engel groups plays an important role in group theory since they are closely related to the Burnside problems.

In this survey we consider several classical and novel algorithmic problems for Engel groups and propose several open problems. We study these problems with a view towards applications to cryptography.

1. Introduction

In cryptography most common protocols (RSA, Diffie-Hellman, and elliptic curve methods) depend on the structure of commutative groups and they are related to the difficulty to solve integers factorization and discrete logarithms. In 1994 Shor provided a quantum algorithm that solves these problems in polynomial time [53]. For this reason, researchers are motivated to find alternative methods for constructing cryptosystems. One of them is based on non-commutative cryptography, which does not operate over the integers. Hence, for security reasons, in the last decade new cryptosystems and key exchange protocols based on non-commutative cryptographic platforms have been developed.

The complexity of algorithmic problems have made available families of groups as platform groups for cryptographic protocols. Among others, we mention braid groups (using the conjugacy search problem [33]), polycyclic groups ([11] and [21]), linear groups [7], and right-angled Artin groups ([14] and [15]). For this reason, the employment of algorithmic group theoretic problems in cryptography is an active area of research nowadays.

In this paper we will present the actual state of Engel-group based cryptography. In particular, we investigate several group theoretic problems in Engel groups, with a view towards their applications

MSC(2010): Primary: 20F45; Secondary: 94A60.

Keywords: Engel elements, algorithmic problems, cryptography.

Received: 16 September 2019, Accepted: dd mmmm yyyy.

*Corresponding author.

to cryptography via computational complexity. We are primarily motivated by the fact that some of these group theoretic problems can be used for cryptographic purposes, such as authentication schemes, secret sharing schemes, key exchange problems, and multilinear maps.

The study of Engel groups originates from the famous paper of Burnside in 1901 and it is closely related to the General Burnside Problem (in the reminder GBP, for short) [9]. The General Burnside Problem asks if a finitely generated torsion group is finite. The question whether a finitely generated (n-)Engel group is nilpotent is the analogue of the GBP in the realm of Engel groups. In the following, we refer to this question as the "Engel Burnside Problem". Of course, every group that is locally nilpotent is an Engel group, but the converse needs not to be true in general. The first main result on Engel groups is the Theorem of Zorn which shows that any finite Engel group is nilpotent.

We recall that an element g of a given group G is said to be *right Engel* if for every $x \in G$ there exists an integer $n = n(g, x) \geq 1$ such that $[g, {}_n x] = 1$, where the commutator $[g, {}_n x]$ is defined recursively by the rules $[g, x] = g^{-1}g^x$ and

$$[g,_n x] = [g, x, \overset{n}{\ldots}, x] = [[g, x, \overset{n-1}{\ldots}, x], x]$$

if $n > 1$. Similarly, g is a *left Engel* element if the variable x appears on the left. A group is said to be an Engel group if all its elements are right Engel or, equivalently, left Engel. In a similar way, one can talk about *bounded Engel elements*, with the condition that the integer n can be chosen independently of x. A group G is n-Engel if for any $x, y \in G$ we have $[x,_n y] = 1$ for some $n \in \mathbb{N}$.

The paper is organized as follows. In Section 2 we give basic definitions and properties of Engel groups. We provide some identities satisfied by n-Engel groups, and, in particular, we survey known and open questions about the Engel Burnside Problem. We conclude the section by describing Burnside groups since we think that they have similar behaviour to Engel groups.

Section 3 is devoted to survey general problems and interesting properties in the setting of Engel groups. We present the definition of degree of nilpotency for finite and infinite groups and some useful results that show how one can compute it. In addition, we give the definition of the growth rate and the Discrete Logarithm Problem.

In Section 4 we introduce several group-theoretic decision problems including the word, conjugacy, and isomorphism decision problem. We also describe the power decision problem, the endomorphism decision problem, the n-th root decision problem and the geodesic length decision problem. We present also many search problems.

In Section 5 we describe a number of cryptosystems that have been built around Engel groups. In particular, we present multilinear maps, a public key based on 2-Engel groups and a digital signature based on 4-Engel groups. In addition, we present two secret sharing schemes based on the efficiency of the word problem, and a key protocol whose platform groups are free nilpotent p-groups. Moreover, we survey the Learning Problem Homomorphism which uses as platform group the Burnside groups of exponent 3 (that are, in particular, 2-Engel groups). We conclude the section by presenting the Discrete Logarithm Problem in finite p-groups and the status of quantum algorithms.

The last Section 6 of the paper is devoted to survey the current status of Engel groups in cryptography. We also include a list of open problems, which we hope will guide researchers who wish to work in this field.

2. Background on Engel groups

2.1. **Preliminaries.** Let G be a group and let $x_1, x_2, \dots$ be elements of G. We define the commutator of weight $n \geq 1$ recursively by the rule

$$[x_1, \dots, x_n] = \begin{cases} x_1 & \text{if } n = 1 \\ [[x_1, \dots, x_{n-1}], x_n] & \text{if } n > 1, \end{cases}$$

where $[x_1, x_2] = x_1^{-1}x_2^{-1}x_1x_2 = x_1^{-1}x_1^{x_2}$. If $x = x_1$ and $y = x_2 = \cdots = x_{n+1}$, we use the shorthand notation

$$[x, {}_n y] = [x, y, \overset{n}{\dots}, y].$$

In the following we recall the definition of Engel elements of a group.

Definition 2.1. *Let G be a group and $g \in G$. We say that g is a right Engel element if for any $x \in G$ there exists $n = n(g, x) \geq 1$ such that $[g, {}_n x] = 1$. If n can be chosen independently of x, then g is a right n-Engel element (or a bounded right Engel element).*

Similarly, g is a left Engel element if for any $x \in G$ there exists $n = n(g, x) \geq 1$ such that $[x, {}_n g] = 1$. Again, if the choice of n is independent of x, then g is a left n-Engel element (or a bounded left Engel element).

The sets of right and left Engel elements of G are denoted by $R(G)$ and $L(G)$, respectively. Notice that $R(G)$ and $L(G)$ are invariant subsets under automorphisms of G. Hence, for any $g \in R(G)$ (resp. $g \in L(G)$) and any $x \in G$, we have $g^x \in R(G)$ (resp. $g^x \in L(G)$).

The following gives the iteration between right and left Engel elements.

Proposition 2.2 ([27])**.** *Let G be a group. We have*

$$R(G)^{-1} \subseteq L(G) \text{ and } R_n(G)^{-1} \subseteq L_{n+1}(G).$$

Notice also that in every 2-group, elements of order 2 are left Engel, as the following proposition (it can be found, for example, in [49]) shows.

Proposition 2.3. *Let G be group and let $g \in G$ such that $g^2 = 1$. Then for any $x \in G$ and any $n \geq 1$:*

$$[x, {}_n g] = [x, g]^{(-2)^{n-1}}.$$

In particular, every involution in any 2-group is a left Engel element.

In the following we give definitions of Engel and n-Engel groups.

Definition 2.4. *We say that G is an Engel group if $G = R(G)$ or, equivalently, $G = L(G)$. Moreover, G is an n-Engel group if there exists $n \geq 1$ such that $[x, {}_n y] = 1$, for all $x, y \in G$.*

Of course every n-Engel group is Engel, and every nilpotent group of class n is n-Engel. Also, there are nilpotent groups of class n that are not $(n-1)$-Engel. An example is the groups $G = C_p \wr C_p$, that is the wreath product of two cyclic groups of order a prime p. One can see that G is nilpotent of class p but not a $(p-1)$-Engel group (see Theorem 6.2 of [36]). Furthermore is not difficult to construct n-Engel groups that are not nilpotent. Take for example a prime p and consider the group $G = C_p \wr C_{p^\infty}$, where C_{p^∞} is the Prüfer group. One can prove that G is a $(p+1)$-Engel group but it is not nilpotent.

The main open question in the realm of Engel groups is whether every n-Engel group is locally nilpotent. Hence, the Engel condition is more general than nilpotency. Recall that a group G is locally nilpotent if each finitely generated subgroup of G is nilpotent.

For $n \leq 4$ every n-Engel group is locally nilpotent. Indeed, 1-Engel groups are abelian. For $n = 2$, Levi proved that G is a 2-Engel group if and only if the normal closure of an arbitrary element is abelian [35]. Moreover 2-Engel groups are nilpotent of class at most 3. For $n = 3$, Heineken proved that every 3-Engel is locally nilpotent [28]. Finally, Havas and Vaughan-Lee [26] proved that every 4-Engel groups generated by d elements are nilpotent of class $4d$. For $n > 4$ the question is still open.

In some other classes of groups also being n-Engel implies locally nilpotency. For example, any residually finite n-Engel group is locally nilpotent [58].

About Engel groups, as pointed out in the introduction, the question whether every Engel group is locally nilpotent is the analogue of the General Burnside Problem for Engel groups.

It is easy to check that every locally nilpotent group is Engel. The converse is true in some classes of groups like finite groups (Zorn [59]), soluble groups (Gruenberg [18]), groups with maximal condition (Baer [3]), linear groups ([55]) and some other classes of groups. Hence, in these cases the condition to being Engel is equivalent to local nilpotency, but in general it is much weaker. Indeed, the infinite p-group $G = \langle x_1 \ldots, x_r \rangle$ constructed by Golod is a counterexample. This group is Engel and it is such that every $(r-1)$-generated subgroup is nilpotent. So far, in the periodic case, Golod's group is the only known example of finitely generated Engel group that is not nilpotent.

2.2. **Identities satisfied by n-Engel groups.** In this section we present some semigroups identities satisfied by n-Engel groups for $n \leq 4$. We have the following.

(1) In every 2-Engel group $yx^2y = xy^2x$.

(2) In every 3-Engel group

$$xy^2xyx^2y = yx^2yxy^2x \text{ and } xy^2xyxyx^2y = yx^2y^2x^2y^2x.$$

(3) In every 4-Engel group we have

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

For more information one can see [57] and [39].

Notice that, additionally, if a group is Engel and locally nilpotent one can prove the following.

Theorem 2.5 ([10])**.** *There exist positive integers $m = m(n)$ and $r = r(n)$ such that any locally nilpotent n-Engel group satisfies*

$$[x^r, x_1, \ldots, x_m] = 1.$$

2.3. **Burnside groups.** In this subsection, we present Burnside groups since it seems that their behaviour is similar to the behaviour of the class of Engel groups. Moreover, in Section 5.5 we present a protocol that uses Burnside groups of exponent 3 as platform group.

Let F_m be a free group of rank m. The free Burnside group $B(m, n)$ is the group F_m/F_m^n, where F_m^n is the group generated by all the n-th powers of elements of F_m. Therefore $B(m, n)$ is the group in which the identity $x^n = 1$ holds and for this reason is the biggest group generated by m elements of exponent n. The Burnside Problem asks if a finitely generated group of finite exponent is finite, that is the same as asking whether the free Burnside groups are finite.

It is easy to prove that for any m the 2-group $B(m, 2)$ is elementary abelian and so finite. Burnside proved that also $B(m, 3)$ is finite for any m. Levi and van der Waerden in 1993 proved that if $m \geq 3$ the Burnside group $B(m, 3)$ is finite and nilpotent of class 3. One can also prove that since $B(m, 3)$ is a group of exponent 3, then is a 2-Engel group because of the following.

Proposition 2.6 (12.3.5 of [49])**.** *A group of exponent 3 is a 2-Engel group.*

In 1940, Sanov proved that also the group $B(m, 4)$ is finite for every m. For $n = 5$ the problem is still open. Although for some small values of n the Burnside groups are finite, in 1968, Novikov and Adian proved that, in general, Burnside groups need not to be finite. Indeed they showed that if $m \geq 2$, and n is odd and greater than 4381, then $B(n, m)$ is infinite. This bound was improved later by Adian which showed that n can be chosen odd and greater than or equal to 665. With the same construction used to prove that these Burnside groups are infinite, Novikov and Adian also proved that the word and the conjugacy problems are decidable in Burnside groups, see [44].

3. Other properties and problems around Engel groups

In this section, we survey additional properties that can help us to the study of Engel groups. In particular, we present the growth rate, the Discrete Logarithm Problem for finite p-groups, and the degree of nilpotency.

3.1. **Growth rate.** Let G be a finitely generated group. The growth function γ is

$$\begin{aligned} \gamma : \mathbb{N} &\to \mathbb{R} \\ n &\mapsto |\{w \in G : l(w) \leq n\}| \end{aligned}$$

where $l(w)$ denotes the length of w. Since words are used as keys in group-based cryptography, there is a natural relationship between the growth rate of a group and the key space, that is the set of all possible keys. A fast growth rate engenders a large key space, making an exhaustive search of this space intractable. Notice that by a deep result of Gromov, if G is a finitely generated group, then G

has polynomial growth if and only if G is virtually nilpotent [17]. Moreover Golod Shafarevich groups have exponential growth [4].

3.2. **The Discrete Logarithm Problem.** Let G be a finite group. Given $x, y \in G$, the Discrete Logarithm Problem (in the reminder DLP for short) is to find a positive integer a such that $x^a = y$ (if it exists). Notice that this is usually defined in the setting of cyclic groups because the Discrete Logarithm exists for all elements and all nontrivial bases.

Notice that the DLP can be generalized to several components as follows. Let $\mathbf{x} = (x_1, \ldots, x_n)$ be a tuple of elements such that $G = \langle x_1, \ldots, x_n \rangle$. Given $y \in G$, the "generalized" DLP of y with respect to $\mathbf{x}$ is to find a_i such that y can be written uniquely as $\mathbf{x^a} = (x_1^{a_1}, \ldots, x_n^{a_n}) = y$ where $0 < a_i < |x_i|$ for every i.

For a survey on the topic see, for example, [45].

3.3. **Degree of n-nilpotency.** In this subsection we present the definition of degree of n-nilpotency and some related properties. This is a notion that measures how close is a group to being nilpotent of nilpotency class n. In particular, this is a way to measure how close Engel groups are to being nilpotent. This is relevant for us since some protocols work better using Engel (or nilpotent) groups (see Section 5). In the following we provide two ways to compute the degree of nilpotency of a group.

3.3.1. *Degree of n-nilpotency of a finite group.* In [41] the degree of n-nilpotency ($n \geq 2$) of a finite group G is defined as follows:

$$d^{(n)}(G) = \frac{|\{(x_1, \cdots, x_{n+1}) \in G^{n+1} \mid [x_1, \cdots, x_{n+1}] = 1\}|}{|G|^{n+1}}.$$

For ease of notation write $d(G) = d^{(1)}(G)$. Clearly $d(G) = 1$ if and only if the group G is abelian. In [22] Gustafson proved that if $d^{(1)}(G) > 5/8$, then G is abelian. Moreover if $d(G) > 1/2$, then G is nilpotent [34].

In the following we present two upper bounds for the above definition of n-nilpotency degree [12].

Theorem 3.1. *Let G be a finite group which is not nilpotent of class at most n. Then*

$$d^{(n)}(G) \leq \frac{2^{n+2} - 3}{2^{n+2}}.$$

Theorem 3.2. *Let G be a nontrivial finite group with trivial center. Then for every $n \geq 1$,*

$$d^{(n)}(G) \leq \frac{2^n - 1}{2^n}.$$

3.3.2. *General definition.* We conclude this section by pointing out that there exists a more general definition of degree of nilpotency which holds also for infinite groups.

Definition 3.3. [1] *Let G be a group (not necessarily finite) generated by a finite set X. The degree of n-nilpotency of G with respect to X is defined as follows:*

$$d_{n,X}(G) = \limsup_{m \to \infty} \frac{|\{\mathbf{x} \in B_X(m)^{n+1} \mid [x_1, \ldots, x_m] = 1\}|}{|B_X(m)|^{n+1}},$$

where $B_X(m)$ is the ball of radius n centered at 1 on the Cayley graph of G with respect to X.

Obviously, if the group G is finite then the above definition coincides with the one given in Section 3.3.1. We finally remark that in [1] it has been proved that the positivity of $d_{n,X}(G)$ does not depend on the generating set X.

4. **Algorithmic problems**

In this section we survey several decision problems in group theory. In particular, we summarize the status of the complexity of some algorithmic problems in the context of Engel groups. In Section 5 we present cryptosystems whose security depends on some of these problems.

Notice also that, as pointed out in Section 2.1, every finitely generated n-Engel group with $n \leq 4$ is nilpotent. Then every result for nilpotent groups can be applied to n-Engel groups for $n \leq 4$.

4.1. **Decision problems.** From now on we let G be a group given by a presentation $\langle X|R\rangle$ and we understand that when we speak of elements of G these are given as a product of generators in $X^{\pm 1}$.

The following three decision problems were introduced by Dehn in 1911. They are defined as follows.

- *Word Problem*: For any $g \in G$, determine if g is the identity element of G.
- *Conjugacy Problem*: For any $x, y \in G$, determine if x and y are conjugate.
- *Isomorphism Problem*: Let G and G' be groups given by finite presentations, determine if G is isomorphic to G'.

For polycyclic groups all three of the above problems are decidable (see [47], [19], [16], [51], and for a survey on the topic see [21]).

For finitely generated nilpotent groups the word problem is solvable. Also, finitely generated nilpotent groups are linear ([25]) and for linear groups the word problem is solvable in logspace ([37]). Hence, the word problem for finitely generated nilpotent groups is is solvable in (deterministic) logspace.

Furthermore, Blackburn in 1965 proved that the conjugacy problem is decidable as well [8].

The isomorphism problem is also known to be solvable for finitely generated nilpotent groups [20]. Notice that, in contrast, the epimorphism problem is undecidable for finitely generated nilpotent groups [48]. We record that the *epimorphism problem* asks whether, given two finite presentations R_1 and R_2 of groups, there exists an algorithm which determines if the group with presentation R_1 is a homomorphic image of the group defined by the presentation R_2.

4.1.1. *Power decision problem.* Let G be a finitely generated group. Given $x, y \in G$, determine whether there exists $n \in \mathbb{Z}$ such that $y = x^n$. Notice that this is equivalent to deciding whether $y \in \langle x\rangle$, and thus is the analogue of the Discrete Logarithm Problem (see Section 5.6). A generalization of the power problem is the subgroup membership problem that can be stated as follows.

4.1.2. *Subgroup membership decision problem.* Let G be a group and $H \leq G$. The subgroup membership decision problem (also known as the *generalized word problem*) asks for any $g \in G$ if $g \in H$. The subgroup membership problem is decidable for finitely generated nilpotent groups [2]. This problem can be generalized to the *rational subset membership problem.* Recall that given a group G, the class of rational subsets of G is the smallest class that contains all finite subsets of G and that it is closed

with respect to union, product and taking the free monoid generated by a set (i.e. using the Kleene star operation). The rational subset membership problem asks whether given a rational subset H of G and an element $g \in G$, whether $g \in H$. In this case, nilpotent groups have undecidable rational subgroup membership problem [38].

4.1.3. *The endomorphism decision problem.* Let F be a free group and $x \in F$. The endomorphism decision problem asks whether there exists an algorithm that given $y \in F$ decides if there exists an endomorphism ϕ of F sending x to y. In nilpotent groups the endomorphism problem is undecidable [50].

4.1.4. *The n-th root decision problem.* For $n \in \mathbb{N}$, an element a of a group G is a n-th root if there exists an element x such that $x^n = a$. Given an element $g \in G$, the n-th root decision problem asks to determine if g has any n-th root. Note that if the root of every element of G belongs to G, the group is said to be *complete*.

We remark that if we take a group H under addition, this is the problem of finding n-th roots is equivalent to saying that for any $n \in \mathbb{N}$ and every element $h \in H$, the equation $nx = h$ has at least one solution in H.

For some results about finding n-th roots in nilpotent groups see [57]. It seems that finding square roots in Engel groups is a difficult problem (see Section 5.2.1 and Section 5.2.2).

4.1.5. *Geodesic length decision problem.* Let $G = \langle X \rangle$ be a group generated by a set X. Denote with $|w|$ the length of a word in the alphabet $X^{\pm 1}$, and with ρ the canonical epimorphism of $F(X)$ onto G, where $F(X)$ denotes the free group over the set X. The geodesic length $l_X(g)$ of an element $g \in G$ with respect to X is

$$l_X(g) = \min\{|w| \mid w \in F(X),\ \rho(w) = g\}.$$

We say that a word $w \in F(X)$ is geodesic if $|w| = l_X(\rho(w))$. Given a word $w \in F(X)$, the geodesic length decision problem consists in, given a word $w \in F(X)$, to find $l_X(\rho(w))$.

In [42] it is observed that for nilpotent groups this is a hard problem.

4.2. **Search problems.** In this section we survey some search problems. Several protocols of non-commutative cryptography, like Ko-Lee and Anshel-Anshel-Goldfeld, are based in part on the conjugacy search problem. For this reason here we present, among others, the conjugacy search problem and some of its variations.

As before, we let G be a group given by the presentation $\langle X|R\rangle$ and we agree that when we refer to an element of G this is given as a product of generators in $X^{\pm 1}$.

4.2.1. *Word search problem.* The word search problem is: given a finitely presented group G and an element $g = 1$ in G find a presentation of g as a product of conjugates of defining relators and their inverses.

4.2.2. *Conjugacy search problem.* Let G be a group and $a_1, \dots a_n, b_1, \dots b_n \in G$ where a_i is conjugate to b_i for $i = 1, \dots, n$. The multiple conjugacy search problem is to find $c \in G$ such that $a_i^c = b_i$ for $1 \leq i \leq n$. If $n = 1$ this reduces to the conjugacy search problem.

In some cases, for example for polycyclic groups [11], the multiple conjugacy search problem reduces to the solvability of single (independent) conjugacy search problem. In general, for finitely generated polyciclic groups the conjugacy search problem can be solved by recursively enumerating the conjugates of the elements taken in consideration [54].

4.2.3. *Power conjugacy search problem.* The power conjugacy search problem asks to find for some $x, y \in G$, an element $g \in G$, and $n \in \mathbb{N}$ such that $x^n = y^g$. Note that for $n = 1$ this reduces to the standard conjugacy search problem, whereas if g is the identity in the group this reduces to the power (search) problem.

5. **Applications to cryptography**

In this section we present some applications of Engel groups to cryptography. We first survey some cryptosystems based on n-Engel groups such as a public key, a digital signature, two secret sharing schemes and multilinear maps. We present the protocol used, the ideal platform group, and some security assumptions. We conclude this section presenting the Discrete Logarithm Problem (DLP for short) in finite p-groups (that are nilpotent groups, so in particular Engel groups) and providing the actual status of quantum algorithms.

5.1. **Multilinear maps.** In this subsection we first define multilinear maps and then we provide some applications. For more information, see [32].

Definition 5.1. *Let n be a positive integer and G an arbitrary group. A map $e : G^n \to G$ is said to be a n-linear map (or a* multilinear map*) if for any $g_1, \dots, g_n, \in G$ and any $a_1, \dots, a_n \in \mathbb{Z}$ we have*

$$e(g_1^{a_1}, \dots, g_n^{a_n}) = e(g_1, \dots, g_n)^{a_1 \cdots a_n}.$$

Moreover, we say that the map e is non-degenerate if there exists $g \in G$ such that $e(g, \dots g) \neq 1$.

Let now G be a nilpotent group of class $n > 1$ and $g_1, \dots, g_n \in G$. One can easily prove by induction on n that for any $a_1, \dots, a_n \in \mathbb{Z}$ the following identity holds:

$$[g_1^{a_1}, \dots, g_n^{a_n}] = [g_1, \dots, g_n]^{\prod_{i=1}^n a_i}. \tag{5.1}$$

Hence if G is nilpotent, the map e

$$e : G^n \to G$$

$$(g_1, \dots, g_n) \mapsto [g_1, \dots, g_n]$$

is a multilinear map. In addition, if we fix $x \in G$, we can construct another multilinear map f given by

$$f : G^{(n-1)} \to G$$
$$(g_1, \dots, g_{n-1}) \mapsto [x, g_1, \dots, g_{n-1}].$$

Notice that we want the multilinear map to be non-degenerate. This is the case if we assume that G is not $(n-1)$-Engel. Indeed, in this condition, there exists $g \in G$ such that $[x,_{(n-1)} g] \neq 1$, which implies that f is non-degenerate.

5.1.1. *Protocol.* Let G be a nilpotent group of class $n+1$ which is not n-Engel ($n \geq 1$). Then there exist elements $x, g \in G$ such that $[x,_n g] \neq 1$. The group G is public. We have $n+1$ users $A_1, \dots A_{n+1}$ that wish to agree on a shared secret key. Each user A_j selects a private integer $a_j \neq 0$, computes g^{a_j}, and sends it to the other users. Then we are in the following situation:

- The user A_1 computes $[x^{a_1}, g^{a_2}, \dots g^{a_{n+1}}]$.
- For $j = 2, \dots, n$, the user A_j computes $[x^{a_j}, g^{a_1}, \dots, g^{a_{j-1}}, g^{a_{j+1}}, \dots, g^{a_{n+1}}]$.
- The user A_{n+1} computes $[x^{a_{n+1}}, g^{a_1}, \dots g^{a_n}]$.

Since (5.1) holds in all nilpotent groups, all elements computed by the users are equal to $k = [x,_n g]^{\prod_{j=1}^{n+1} a_j}$. This is the shared key.

5.2. **Two cryptosystems based on n-th root problem in n-Engel groups.** In this section we present two cryptosystems in n-Engel groups proposed in [57].

5.2.1. *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 and y as their secret keys, respectively. Then Alice sends x^2 to Bob and Bob sends y^2 to Alice. As pointed out in Section 2.2, in any 2-Engel group it holds the semigroup identity $xy^2x = yx^2y$. Then Alice and Bob agree on a key. One could extend this scheme to other n-Engel groups, since there are similar relations in them as well (see, for example Equation 2.5).

5.2.2. *A digital signature based on 4-Engel groups.* Consider a 4-Engel group, which is nilpotent and satisfies the following semigroup law (see the last part of Section 2 and Section 2.2):

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

The idea to make a digital signature is as follows. Suppose x and y are private and x^2, y^2, xy^2x, and $xy^2x^2y^2x$ are public. The public key is x^2 and the signature is xy^2x and $xy^2x^2y^2x$. The verifier knows y, so he has to to verify both the semigroup identity.

5.2.3. *Platfrom group and security.* The underlying group could be combined by a finite group in which square root is hard, for example $\mathbb{Z}^*_{pq}$, with p, q prime numbers.

The security of these digital signatures lies on the fact that the complexity of finding square root in 2-Engel and 4-Engel groups. It seems that this is a hard problem [43].

5.3. **Secret sharing based on the word problem in Engel groups.** In this section we present two secret sharing schemes based on the word problem proposed by Habeeb-Kahrobaei-Shpilrain [24]. Both of them are based on the efficiency of the word problem and we will use them with (n-)Engel nilpotent groups.

We recall that a (t, n)-threshold secret sharing is a scheme in which a secret is distributed among n participants in a way that the secret can be recovered only if at least t of them combine their shares. We present two secret sharing schemes. The first one (Scheme 1) is a (n, n)-threshold scheme and so the participants must get together to recover the secret. The second one (Scheme 2) is a (t, n)-threshold scheme that is a combination of Shamirs scheme [52] and the group-theoretic scheme proposed in Section 3 of [24] and presented below. In both of them we denote a generic participant of the protocol with P_i, with $1 \leq i \leq n$. We also suppose that the dealer and the participants at the beginning are able to communicate over secure channels and then they communicate over open channels.

5.3.1. *Scheme 1.* The following is an (n, n)-threshold scheme. The dealer:

- Distributes a k-column of bits $C = (c_1, c_2, \ldots, c_k)^{\mathsf{T}}$.
- Distributes C among n participants in such a way that the column can be reconstructed only if all participants combine their information.

A set $X = \{x_1, \ldots, x_m\}$ of generators is public. Then the protocol is as follows.

(1) The dealer uses a secure channel to assign to each participant P_j a set of words R_j in the alphabet $X^{\pm 1}$ such that each group $G_j = \langle x_1, \ldots, x_m \mid R_j \rangle$ has word problem solvable in polynomial time.
(2) The dealer splits the column C in $\sum_{j=1}^{n} C_j \mod 2$. These are secret shares to be distributed to the n participants.
(3) The dealer distributes words $w_{1j}, \ldots w_{kj}$ in the generators $x_1, \ldots x_m$ over an open channel to each participant P_j, with $1 \leq j \leq n$. The choice of the words is such that $w_{ij} \neq 1$ in G_j if $c_{ij} = 0$ and $w_{ij} = 1$ in G_j if $c_{ij} = 1$, where c_{ij} is the i-th entry of C_j.
(4) Each participant P_j check for any i if $w_{ij} = 1$ in the group G_j or not.
(5) Now each participant constructs $C_j = (c_{1j}, c_{2j}, \ldots, c_{kj})^{\mathsf{T}}$ of 0's and 1's ($c_{ij} = 1$ if $w_{ij} = 1$ in G_j, and 0 otherwise).
(6) The secret is built by putting together the vector sum $\sum_{j=1}^{n} C_j \mod 2$.

5.3.2. *Scheme 2.* In this case we present a (t, n)-threshold scheme in which the secret is an element $x \in \mathbb{Z}_p$, for p a prime number. The dealer:

- Chooses a polynomial f of degree $t - 1$ such that $f(0) = x$.
- Determines integers $y_i = f(i) \mod p$ for $1 \leq i \leq n$.
- Distributes every y_i to the correspondent participant P_i.

We now consider a set $X = \{x_1, \ldots, x_m\}$ of generators, which is public. In addition, we assume that the integer x and every y_i can be written as k-bit columns. Now we are ready to present the scheme, that reads as follows.

(1) The dealer distributes over a secure channel to each participant P_j a set of relators R_j such that each group $G_j = \langle x_1, \ldots, x_m \mid R_j \rangle$ has efficiently solvable word problem.
(2) The dealer then distributes over open channels k-columns of the form $b_j = (b_{1j}, b_{2j}, \ldots, b_{kj})^{\mathsf{T}}$, (where $1 \leq j \leq n$) of words in $x_1, \ldots, x_m$ to each participant. The b_{ij} are chosen such that if we replace them by bits, the resulting bit column represents the integer y_j. Note that we use "1" if $b_{ij} = 1$ in the group G_j and "0" otherwise.
(3) For any word b_{ij}, the participant P_j checks whether or not $b_{ij} = 1$ in the group G_j. Then P_j obtains a binary representation of the number y_j, and therefore P_j recovers y_j.
(4) Each participant now has a point $f(i) = y_i$ of the polynomial. Using polynomial interpolation, any t participants can now recover the polynomial f. Whence they obtain the secret $x = f(0)$.

If $t \geq 3$, Step 4 can be changed in a way that the participants do not have to reveal their individual shares to each other if they do not want to. For more details about how to arrange this, an interested reader can see [24].

5.3.3. *Platform group.* For Scheme 1 and Scheme 2, we propose finitely presented nilpotent Engel groups that, being nilpotent, have efficiently solvable word problem (see the discussion in Section 4.1). For example, one can use n-Engel groups with $n = 2, 3, 4$ or an Engel group that is linear, solvable or finite (and hence nilpotent).

5.4. **A key protocol based on semidirect products of groups.** In this section we present a key protocol based on semidirect products of groups (or semigroups). This protocol can be based on any group, but we present an application using free nilpotent p-groups where p is a sufficiently large prime p proposed by Kahrobaei and Shpilrain in [31]. Note that there are several protocols based on semidirect products of groups, such as a public key exchange [23].

5.4.1. *Protocol.* Let G be a group (or a semigroup) and choose public $g \in G$ and $\varphi \in \mathrm{Aut}(G)$ (or $\mathrm{End}(G)$). Alice chooses a private $m \in \mathbb{N}$ while Bob chooses a private $n \in \mathbb{N}$. Alice and Bob are going to work with elements of the form (g, φ^r), where $g \in G$ and $r \in \mathbb{N}$. Recall that the multiplication of two elements of this form is as follows:

$$(g, \varphi^r)(h, \varphi^s) = (\varphi^s(g)h, \varphi^{r+s}).$$

Now we present a key exchange protocol similar to the Diffie-Hellman key exchange.

- Alice computes

$$(g, \varphi)^m = (\varphi^{m-1}(g) \cdots \varphi^2(g)\varphi(g)g, \varphi^m)$$

and sends the first component $a = \phi^{m-1}(g) \cdots \varphi^2(g)\varphi(g)g$ of the pair to Bob.

- Bob computes
$$(g,\varphi)^n = (\varphi^{n-1}(g)\cdots\varphi^2(g)\varphi(g)g, \varphi^n)$$
and sends the first component $b = \varphi^{n-1}(g)\cdots\varphi^2(g)\varphi(g)g$ of the pair to Alice.
- Alice computes
$$(b,x)(a,\varphi^m) = (\varphi^m(b)a, x\varphi^m).$$
Her key is $K_A = \varphi^m(b)a$.
- Bob computes
$$(a,y)(b,\varphi^n) = (\varphi^n(a)b, y\varphi^n).$$
His key is $K_B = \varphi^n(a)b$.

The shared secret key is $K = K_A = K_B =$ since
$$(b,x)(a,\varphi^m) = (a,y)(b,\varphi^n) = (g,\varphi)^{m+n}.$$

5.4.2. *Platform groups.* We denote with $\gamma_c(G)$ the normal subgroup of G generated by all the elements of the form $[y_1,\ldots,y_c]$. Consider now F_m the free group on $x_1,\ldots,x_m$. The factor group $F_m/\gamma_{c+1}(F_m)$ is the free nilpotent group of nilpotency class c.

The group suggested as platform group for the protocol described above is
$$G = F_m/F_m^{p^2}\gamma_{c+1}(F_m)$$
that is a nilpotent p-group and hence a finite group whose order depends on c, m and p. The suggested values of c and m are small numbers, for example $c = 2$ or $c = 3$ to make the computation efficient. Conversely, the value of p should be sufficiently large to make it secure to a linear algebra attack.

5.5. **Burnside groups of exponent 3 and the learning homomorphism problem.** The learning with errors (LWE) problem was introduced by Regev in [46], and has become one of the most known problems in lattice-based cryptography. It has been used to construct several cryptosystems, and it is believed to be hard even for quantum computers.

Informally speaking, the problem of learning with error is to deduce a particular function by sampling the input/output behavior if some of the outputs are incorrect. For more information one can see [6].

In the following, we define the Learning Homomorphim Problem with Noise (LHN, for short) that is a generalization of the LWE. We will denote the set of homomorphisms from a group G to a group H with $\mathrm{Hom}(G,H)$.

Definition 5.2. *Let $\varphi \in \mathrm{Hom}(G,H)$, where G and H are finitely generated groups, and let $g_1,\ldots g_m \in G$. Also, let α and β be probability distributions over G and H, respectively. Let Ψ be the probability distribution over $G\times H$ which assigns to each tuple of the form $(g,\varphi(g)h)$ the probability* $\mathrm{Prob}(g\sim\alpha)$ *and* $\mathrm{Prob}(h\sim\beta)$ *and the rest of tuples from $G\times H$ are assigned a probability of* 0.

We say that an algorithm solves the LHN with noise if for any $\varphi : G\to H$, the algorithm is able to learn φ given a set of samples from the distribution Ψ with high probability. For the purpose of this

paper we omit the definition of "learning with high probability given a set of samples". For a detailed reference on this, see [6] *and* [13].

5.5.1. *Protocol, platform groups and security assumptions.* In [13] the authors employed for the first time properties of Burnside groups in cryptography. In particular, they introduced the Learning *Burnside* Homomorphisms with Noise (B-LHN), which uses for computational purposes only surjective homomorphisms in contrast to the general definition of LHN [6].

To avoid technicality, we omit the description of the protocol used for this problem. We address the reader to pp. 10-11 of [6].

We want to underline that as platform group for the B-LHN problem, the authors employed the Burnside groups of exponent 3, that are, in particular, 2-Engel groups. The security of this protocol is based on the computational hardness of B-LHN (see Theorem 2 of [13]).

5.6. **The Discrete Logarithm Problem in finite p-groups.** Sutherland studied the DLP in some finite abelian p-groups [56], and in a series of papers by Mahalanobis, the DLP has been studied for finite p-groups of nilpotency class 2 [40]. Solving the DLP in finite p-groups of larger class is an interesting question. One, for example, can consider semidirect product of cyclic p-groups of well-defined orders, to make a nilpotent group and then computing the Discrete Logarithm in each factor.

5.7. **Quantum algorithms.** We conclude this section of applications by presenting the status of quantum algorithms in cryptography. In 2015 the National Security Agency announced plans to replace all deployed cryptographic protocols with quantum secure protocols. A quantum computer is able to perform integer factorization and solve the DLP in finite cyclic groups in polynomial time.

In [5] it has been explored the application of quantum algorithms to group theory. In particular, from a group theoretic point of view, Shor's algorithm can be seen as the hidden subgroup problem in finite cyclic groups. We recall that a subgroup H of a group G is *hidden* by a function f from G to a set X if it is constant over all cosets of H, and takes distinct values on distinct cosets. In other words, for any $g_1, g_2 \in G$, $f(g_1) = f(g_2)$ if and only if $g_1H = g_2H$. Given a hidden subgroup H, the *hidden subgroup problem* asks to find a generating set for H using information from evaluations of f via an oracle (for a survey on the topic, see [29]). In [30] the complexity of quantum algorithms for the HSP for certain semidirect product of certain finite p-groups, for p a prime has been considered.

6. **Conclusion and open questions**

In this paper we have presented the current state of Engel group-based cryptography. We have begun with a study of algorithmic properties of Engel groups, and we have also seen that there are a variety of key exchanges, digital signature systems, and secret sharing schemes for which an Engel (or nilpotent) group is an appropriate choice of platform group. As we have seen throughout the paper, if on the one hand there has been some results about Engel groups and their attendant cryptosystems over the last decade, on the other hand the majority of computational complexity and algorithmic questions remain unanswered.

We collect some open problems below with the hope of stimulating interest in their solutions.

We start by pointing out that since Engel groups are a generalization of nilpotent groups, in the case in which the algorithmic problems presented in in Section 4 are decidable for nilpotent groups, we ask whether the same holds specially if the group is n-Engel. Also, since some problems are undecidable for nilpotent groups (take, for example, the rational subgroup membership problem and the endomorphism problem) we ask:

(1) Is the rational subgroup membership problem undecidable for Engel groups?
(2) Is the endomorphism problem undecidable for Engel groups?

In addition, we propose the following questions related also to the complexity of some algorithmic problems presented in Section 4.

(3) Determine if the following algorithmic problems are decidable and if yes, find the complexity:
   - The word problem.
   - The (power) conjugacy problem.
   - The geodesic length problem.
(4) What about the search problems proposed in Section 4.2? For example, if G is an Engel group, and $a_1, \dots a_n, b_1, \dots b_n \in G$ where a_i is conjugate to b_i for $i = 1, \dots, n$. Can we find $c \in G$ such that $a_i^c = b_i$ (for $1 \leq i \leq n$)? As a starting point, one can study the single conjugacy search problem (i.e. the case $n = 1$).

In Section 5 we present several ideas of Engel-group based cryptography.

In particular, in Section 5.1, we present a protocol based on multilinear maps. It is an open question the ideal platform of this scheme. Thus we ask the following.

(5) What is an ideal platform group for the protocol proposed in Section 5.1?

In Section 5.2 we present some specific cryptosystems based on n-Engel groups. It seems they are secure because they are based on the difficulty to find square roots in n-Engel groups. Moreover, no platform groups are suggested. Whence, we propose the following.

(6) What is an ideal platform group for the protocol proposed in Section 5.2.1 and Section 5.2.2, respectively?
(7) What is the complexity of the square root problem in n-Engel groups? And for the n-root problem?

In view of Section 5.7, we conclude the paper with the following questions.

(8) Is the HSP solvable for Engel groups?
(9) Are there some Engel group-based cryptosystems resistant to quantum algorithms? Note that this could be done either by analyzing the HSP for Engel groups or showing the underlying security problem is NP-complete or NP-hard.

Acknowledgments

The authors would like to thank G. Fernández-Alcober, A. Garreta, and A. Tortora for helpful comments and suggestions. The first author would like to thank A. Tortora and M. Tota for an invitation to the University of Salerno where the ideas of this research were initiated. The second author would like to thank the Department of Computer Science at the University of York for its hospitality while this paper was being written.

References

[1] Y. Antolín, A. Martino, and E. Ventura, *Degree of commutativity of infinite groups*, Proceedings of the American Mathematical Society **145** (2015), 479–485.

[2] J. Avenhaus and D. Wi:Gbmann, *Using rewriting techniques to solve the generalized word problem in polycyclic groups*, Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic computation, 1989, pp. 322–337.

[3] R. Baer, *Engelsche Elemente Noetherscher Gruppen*, Math. Ann. **133** (1957), 256–270.

[4] L. Bartholdi and R. I. Grigorchuk, *Lie methods in growth of groups and groups of finite width*, London Math. Soc. Lecture Note Ser. **275** (2000).

[5] M. Batty, S. Braunstein, A. Duncan, and S. Rees, *Quantum algorithms in group theory*, Proceedings of Computational and Experimental Group Theory (2004), 1–62.

[6] G. Baumslag, N. Fazio, A. R. Nicolosi, V. Shpilrain, and W. E. Skeith, *Generalized learning problems and applications to non-commutative cryptography*, Provable Security (2011), 324–339.

[7] G. Baumslag, B. Fine, and X. Xu, *Cryptosystems using linear groups*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), no. 3, 205–217.

[8] N. Blackburn, *Conjugacy in nilpotent groups*, Proc. Amer. Math. Soc. **16** (1965), 143–148.

[9] W. Burnside, *On an unsettled question in the theory of discontinous groups*, Quart. J. Pure Appl. Math. **33** (1902), 230–238.

[10] P. G. Crosby and G. Traustason, *A remark on the structure of n-engel groups*, Communications in Algebra **39** (2011), no. 11, 3998–4001.

[11] B. Eick and D. Kahrobaei, *Polycyclic groups: A new platform for cryptology?*, arXiv Mathematics e-prints (2004), available at `math/0411077`.

[12] A. Erfanian, R. Rezaei, and P. Lescot, *On the relative commutativity degree of a subgroup of a finite group*, Communications in Algebra **35** (2007), no. 12, 4183–4197.

[13] N. Fazio, K. Iga, A. Nicolosi, L. Perret, and W.E. Skeith III, *Hardness of learning problems over burnside groups of exponent 3*, Des. Codes Cryptography **75** (2015), no. 1, 59–70.

[14] R. Flores and D. Kahrobaei, *Cryptography with right-angled artin groups*, Theoretical and Applied Informatics **28** (2016), no. 3, 8–16.

[15] R. Flores, D. Kahrobaei, and T. Koberda, *Algorithmic problems in right-angled artin groups: Complexity and applications*, Journal of Algebra **519** (2019), 111–129.

[16] E. Formanek, *Conjugate separability in polycyclic groups*, Journal of Algebra **42** (1976), no. 1, 1–10.

[17] M. Gromov, *Groups of polynomial growth and expanding maps*, Publications Mathmatiques de l'IHS **53** (1981), 53–78.

[18] K. W. Gruenberg, *Two theorems on Engel groups*, Mathematical Proceedings of the Cambridge Philosophical Society **49** (1953), no. 3, 377–380.

[19] F. Grunewald and D. Segal, *Conjugacy in polycyclic groups*, Communications in Algebra **6** (1978), 775–798.

[20] F. J. Grunewald and D. Segal, *The solubility of certain decision problems in arithmetic and algebra*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), no. 6, 915–918.

[21] J. Gryak and D. Kahrobaei, *The status of polycyclic group-based cryptography: A survey and open problems*, Groups Complexity Cryptology **8** (2016), 171–186.

[22] W. H. Gustafson, *What is the probability that two group elements commute?*, The American Mathematical Monthly **80** (1973), no. 9, 1031–1034.

[23] M. Habeeb, D. Kahrobaei, C. Koupparis, and V. Shpilrain, *Public key exchange using semidirect product of (semi)groups*, Applied Cryptography and Network Securitym ACNS 2013 (2013), 475–486.

[24] M. Habeeb, D. Kahrobaei, and V. Shpilrain, *A secret sharing scheme based on group presentations and the word problem*, Contemporary Mathematics, American Mathematical Society **582** (2012), 143–150.

[25] P. Hall, *The edmonton notes on nilpotent groups.*, Queen Mary College Mathematics Notes, 1957.

[26] G. Havas and M.R. Vaughan-Lee, *4-Engel groups are locally nilpotent*, Intenational Journal of Algebra and Computation **15** (2005), 649–682.

[27] H. Heineken, *Eine Bemerkung über engelsche Element*, Archiv der Mathematik **11** (1960), 321.

[28] ———, *Engelsche Elemente der Länge drei*, Illinois J. Math. **5** (1961), no. 4, 681–707.

[29] K. Horan and D. Kahrobaei, *Hidden Subgroup Problem and Post-quantum Group-based Cryptography*, 2018, pp. 218–226.

[30] Y. Inui and F. L. Gall, *Efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups*, Quantum Info. Comput. **7** (2007), no. 5, 559–570.

[31] D. Kahrobaei and V. Shpilrain, *Using semidirect product of (semi)groups in public key cryptography*, Computability in Europe 2016, Lecture Notes in Computer Science, Springer, Pursuit of the Universal, LNCS **9709** (2016), 132–141.

[32] D. Kahrobaei, A. Tortora, and M. Tota, *Multilinear Cryptography using Nilpotent Groups*, De Gruyter (2020), 127–133. DOI:10.1515/9783110638387-013.

[33] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park, *New public-key cryptosystem using braid groups*, Advances in Cryptology – CRYPTO 2000, 166–183.

[34] P. Lescot, *Isoclinism classes and commutativity degrees of finite groups*, Journal of Algebra **177** (1995), no. 3, 847–869.

[35] F. W. Levi, *Groups in which the commutator operation satisfies certain algebraic conditions*, The Journal of the Indian Mathematical Society **6** (1942), 87–97.

[36] H. Liebeck, *Concerning nilpotent wreath products*, Mathematical Proceedings of the Cambridge Philosophical Society **58** (1962), no. 3, 443–451.

[37] R. J. Lipton and Y. Zalcstein, *Word problems solvable in logspace*, J. ACM **24** (1977), no. 3, 522–526.

[38] M. Lohrey, *The rational subset membership problem for groups: a survey*, London Mathematical Society Lecture Note Series, Cambridge University Press, 2015.

[39] P. Longobardi and M. Maj, *Semigroup identities and Engel groups*, Proceedings of Groups St. Andrews 1997 in Bath **2**, 527–531.

[40] A. Mahalanobis and P. Shinde, *Bilinear cryptography using groups of nilpotency class 2*, Cryptography and Coding (2017), 127–134.

[41] M. Moghaddam, A. Salemkar, and K. Chiti, *n-Isoclinism classes and n-nilpotency degree of finite groups*, Algebra Colloquium **12** (2005), no. 2, 255–261.

[42] A.G. Myasnikov, V. Shpilrain, and A. Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*, Mathematical surveys and monographs, American Mathematical Society, 2012.

[43] W. Nickel, *Computation of nilpotent Engel groups*, Journal of the Australian Mathematical Society **67** (1999), 214–222.

[44] P. S. Novikov and S. I. Adjan, *Infinite periodic groups. I-III*, Mathematics of the USSR-Izvestiya **2** (1968).

[45] A. Odlyzko, *Discrete logarithms: The past and the future*, Designs, Codes and Cryptography **19** (2000), no. 2, 129–145.

[46] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing (2005), 84–93.

[47] V. N. Remeslennikov, *Conjugacy in polycyclic groups*, Algebra and Logic **8(6)** (1969), 404–411.

[48] ———, *An algorithmic problem for nilpotent groups and rings*, Siberian Mathematical Journal **20** (1979), no. 5, 761–764.

[49] D. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, Springer, 1996.

[50] V. Roman'kov, *Unsolvability of the endomorphic reducibility problem in free nilpotent groups and in free rings*, Algebra and Logic **16** (1977), 310–320.

[51] D. Segal, *Decidable properties of polycyclic groups*, Proceedings of the London Mathematical Society **s3-61** (1990), 497–528.

[52] A. Shamir, *How to share a secret*, Commun. ACM **22** (1979), no. 11, 612–613.

[53] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), no. 5, 1484–1509.

[54] V. Shpilrain, *Search and witness problems in group theory*, Groups Complexity Cryptology (2010), 231–246.

[55] D.A. Suprunenko and M.S. Garashchuk, *Linear groups with Engel's condition*, Doklady Akademii Nauk BSSR **6** (1962), 277–280.

[56] A. V. Sutherland, *Structure computation and discrete logarithms in finite abelian p-groups*, Mathematics of Computation **80** (2011), no. 273, 477–500.

[57] S. Sze, D. Kahrobaei, R. Dambreville, and M. Dupas, *Finding n-th roots in nilpotent groups and applications in cryptology*, IJAM (2011), 1–20.

[58] J. S. Wilson, *Two-Generator conditions for Residually Finite Groups*, Bulletin of the London Mathematical Society **23** (1991), no. 3, 239–248.

[59] M. Zorn, *Nilpotency of finite groups*, Bull. Amer. Math. Soc. **42** (1936), 485–486.

Delaram Kahrobaei

University of York, Department of Computer Science, United Kingdom

The City University of New York, CUNY Graduate Center, U.S.A.

Computer Science and Engineering Department, New York University, U.S.A.

Email: delaram.kahrobaei@york.ac.uk, dkahrobaei@gc.cuny.edu, dk2572@nyu.edu

Marialaura Noce

Dipartimento di Matematica, University of Salerno, Salerno, Italy

Matematika Saila, University of the Basque Country, Bilbao, Spain

Department of Mathematical Sciences, University of Bath, United Kingdom

Email: mn670@bath.ac.uk