Designs, Codes and Cryptography (2024) 92:2825–2843
https://doi.org/10.1007/s10623-024-01416-8

Efficient quantum algorithms for some instances of the semidirect discrete logarithm problem

Muhammad Imran[1] · **Gábor Ivanyos**[2]

Received: 3 January 2024 / Revised: 22 March 2024 / Accepted: 22 April 2024 /
Published online: 21 May 2024

Abstract
The semidirect discrete logarithm problem (SDLP) is the following analogue of the standard discrete logarithm problem in the semidirect product semigroup $G \rtimes \mathrm{End}(G)$ for a finite semigroup G. Given $g \in G, \sigma \in \mathrm{End}(G)$, and $h = \prod_{i=0}^{t-1} \sigma^i(g)$ for some integer t, the SDLP(G, σ), for g and h, asks to determine t. As Shor's algorithm crucially depends on commutativity, it is believed not to be applicable to the SDLP. For generic semigroups, the best known algorithm for the SDLP is based on Kuperberg's subexponential time quantum algorithm. Still, the problem plays a central role in the security of certain proposed cryptosystems in the family of *semidirect product key exchange*. This includes a recently proposed signature protocol called SPDH-Sign. In this paper, we show that the SDLP is even easier in some important special cases. Specifically, for a finite group G, we describe quantum algorithms for the SDLP in $G \rtimes \mathrm{Aut}(G)$ for the following two classes of instances: the first one is when G is solvable and the second is when G is a matrix group and a power of σ with a polynomially small exponent is an inner automorphism of G. We further extend the results to groups composed of factors from these classes. A consequence is that SPDH-Sign and similar cryptosystems whose security assumption is based on the presumed hardness of the SDLP in the cases described above are insecure against quantum attacks. The quantum ingredients we rely on are not new: these are Shor's factoring and discrete logarithm algorithms and well-known generalizations.

Keywords Semidirect discrete logarithm problem · Quantum algorithms · Quantum cryptanalysis

Mathematics Subject Classification 68Q12 · 81P68

Communicated by C. Weinert.

✉ Muhammad Imran
muh.imran716@gmail.com

Gábor Ivanyos
Gabor.Ivanyos@sztaki.hun-ren.hu

[1] Department of Algebra and Geometry, Budapest University of Technology and Economics, Egry József u. 1, 1111 Budapest, Hungary

[2] HUN-REN Institute for Computer Science and Control, Kende u. 13-17, 1111 Budapest, Hungary

1 Introduction

The presumed difficulty of computing discrete logarithm problem (DLP) in certain groups is essential for the security of the Diffie-Hellman key exchange which is the basis for a number of communication protocols deployed today. However, since the invention of Shor's algorithm [26], the problem of computing discrete logarithm can be solved efficiently in the domain of quantum computing.

Massive efforts have been done in order to construct alternative versions of the discrete logarithm problem that allow for the Diffie-Hellman key exchange without being vulnerable to Shor's algorithm. Since that algorithm takes advantage of the group structure underlying the problem, a DLP analogue in the framework of commutative group actions has been proposed. It is an instance of a constructive membership testing in orbits of commutative permutation groups (on large finite sets), called *vectorization problem*. The framework originally appears in [12] and it becomes a central problem of isogeny-based cryptography, CSIDH [10] for example. Another natural approach which is worth consideration to escape from the quantum attack is a DLP analogue in non-commutative groups. It is natural in a sense that Shor's algorithm crucially depends on the commutativity of the underlying groups. In this direction, an analogue of the DLP in semidirect product groups has been proposed. The proposal firstly appears in its full generality in [15]. Specifically, let G be a finite semigroup and $\mathrm{End}(G)$ be the monoid of endomorphisms of G. Then we have the semidirect product $G \rtimes \mathrm{End}(G)$ where the multiplication is defined by $(g, \sigma)(h, \phi) = (g\sigma(h), \sigma\phi)$. Moreover, we have the formula for exponentiation

$$(g, \sigma)^t = \left(\prod_{i=0}^{t-1} \sigma^i(g), \sigma^t \right),$$

where $\prod_{i=k}^{\ell} a_i$ stands for the product $a_k \cdot \ldots \cdot a_\ell$ in G. This leads to an analogue of the standard discrete logarithm problem in the semidirect product semigroup defined as follows. Given $g \in G, \sigma \in \mathrm{End}(G)$, and $h = \prod_{i=0}^{t-1} \sigma^i(g)$ for some integer t, determine t.

The SDLP is interesting as it allows us to perform a Diffie-Hellman key exchange procedure, known as *semidirect product key exchange* (SPDKE). Suppose two parties, Alice and Bob, agree on a public group G, an element $g \in G$, and an endomorphism $\sigma \in \mathrm{End}(G)$. Then they can arrive at the same $G-$element as follows.

1. Alice picks a random positive integer x and computes $(g, \sigma)^x = (A, \sigma^x)$. Then, Alice sends $A = \prod_{i=0}^{x-1} \sigma^i(g)$ to Bob.
2. Bob also picks a random positive integer y, computes $(g, \sigma)^y = (B, \sigma^y)$ and sends $B = \prod_{i=0}^{y-1} \sigma^i(g)$ to Alice.
3. Alice computes its shared key $K_A = A\sigma^x(B)$.
4. Bob computes its shared key $K_B = B\sigma^y(A)$.

Note that $K_A = K_B$, as the following calculation shows.

$$\begin{aligned} A\sigma^x(B) &= \prod_{i=0}^{x-1} \sigma^i(g) \prod_{i=0}^{y-1} \sigma^{x+i}(g) = \prod_{i=0}^{x+y-1} \sigma^i(g) \\ &= \prod_{i=0}^{y-1} \sigma^i(g) \prod_{i=0}^{x-1} \sigma^{y+i}(g) \\ &= B\sigma^y(A). \end{aligned}$$

The key recovery problem of SPDKE is the problem of computing the shared key $K_A = K_B$ from the public information g, A, $B \in G$ and $\sigma \in \mathrm{End}(G)$. Clearly, similar to the case of the standard DLP and the corresponding Diffie-Hellman key exchange, the key recovery problem of SPDKE and the difficulty of SDLP are heavily related. Particularly, if one can solve an instance of the SDLP, then one is also able to break the corresponding SPDKE.

In the description of the SDLP above, an instance of the SDLP in $G \rtimes \mathrm{End}(G)$ is only specified by an endomorphism σ, hence we can describe the SDLP in an alternative, more compact way.

First, we observe some properties of semidirect product semigroups that would be useful for our purpose. Let G and T be semigroups and let $\sigma : t \mapsto \sigma_t$ be a homomorphism from T to the monoid of endomorphisms of G. Then the semidirect product $G \rtimes_\sigma T$ is the set $G \times T$ equipped with the multiplication $(g, t)(g', t') = (g\sigma_t(g'), tt')$. It is straightforward to check that $G \rtimes_\sigma T$ is a semigroup. Also, if both G and T are finite groups and σ_1 is the identity map of G, then $G \rtimes_\sigma T$ is also a group. There is a natural representation $\rho : (g, t) \mapsto \rho_{(g,t)}$ of $G \rtimes_\sigma T$ as a semigroup of transformations on G, given by $\rho_{(g,t)}(g') = g\sigma_t(g')$. This is indeed a representation, i.e., a homomorphism to the semigroup of transformations, because we have $(g, t)(g', t') = (\rho_{(g,t)}(g'), tt')$ and

$$\rho_{(g,t)(g',t')} = \rho_{(\rho_{(g,t)}(g'),tt')} = \rho_{(g,t)} \circ \rho_{(g',t')}.$$

If $G \rtimes_\sigma T$ is a group as above then ρ gives a permutation representation of the group $G \rtimes_\sigma T$.

Note that if G is a monoid and σ is a monoid endomorphism of G (that is, $\sigma(1_G) = 1_G$), we have $(g, 1)^t = (\rho_{(g,1)^t}(1_G), t)$.

This shows that, as already observed by Battarbee et al. in [5], the SDLP can be cast as a constructive membership problem in an orbit of a transformation semigroup. Using the above observation and notations we have the following definition for the semidirect discrete logarithm that will be used throughout this paper.

Definition 1 Let σ be an endomorphism of the finite monoid G with identity element 1_G and consider the semigroup $G \rtimes_\sigma \mathbb{Z}_{\geq 0}$ where $\sigma_t = \sigma^t$ for every $t \in \mathbb{Z}_{\geq 0}$. Then SDLP$(G, \sigma)$ is the following problem. Given elements g and h of G, determine the set of non-negative integers t such that

$$h = \rho_{(g,1)^t}(1_G).$$

The set to be determined is either the empty set, a singleton, or $\{t_0 + at : t \in \mathbb{Z}_{\geq 0}\}$ for certain integers $t_0 \geq 0$ and $a > 0$. To see this, we begin with some basic concepts related to orbits of semigroups generated by a single transformation. Let S be a finite set, let $\rho : S \to S$ be a transformation of S and let $x \in S$. The orbit $\{\rho^t(x) : t \in \mathbb{Z}_{\geq 0}\}$ of ρ starting at x can be divided into two parts as follows. There exists a smallest non-negative number i, called the *index* of the orbit, such that $\rho^i(x) = \rho^{i+j}(x)$ for some positive integer j. The smallest such j is called the *period*. Let i be the index. The *tail* is the set $\{\rho^t(x) : t < i\}$, while the rest of the orbit, the set $\{\rho^t(x) : t \geq i\}$ is referred as the *cycle*. The index is the length of the tail, while the size of the cycle is the period. The elements of the tail are visited just once, while the members of the cycle are visited periodically. The index can be zero while the period is positive. Assuming an oracle that evaluates the powers of ρ on elements of S, the index as well as the period can be computed by a slight modification of Shor's period finding quantum algorithm, see [11]. In our case, the transformation semigroup is generated by $\rho = \rho_{(g,1)}$ and our objective is the orbit of it starting at 1_G. Assume that SDLP(G, σ) for g and h is solvable and let t_0 be the smallest non-negative integer such that $h = \rho_{(g,1)^{t_0}}(1_G)$. If t_0 is smaller than the index of $\rho_{(g,1)}$, that is, when h is in the tail then the solution set is

the singleton $\{t_0\}$. Otherwise, when h is in the cycle, the solution set is $\{t_0 + at : t \in \mathbb{Z}_{\geq 0}\}$, where a is the period. The smallest solution t_0 is always less than the sum of the index and the period as this sum is the total size of the orbit. Note that when $\rho_{(g,1)}$ is a permutation, e.g., when G is a group and σ is an automorphism of G, then the tail is empty and hence the solution set is the residue class $\{t_0 + at : t \in \mathbb{Z}_{\geq 0}\}$ modulo the period a. In that case extending the solution set to negative integers does not make too much confusion, so we will often use the notation $\{t_0 + at : t \in \mathbb{Z}\}$.

We remark that the assumptions that G is a monoid and that σ is a monoid endomorphism of G are rather technical, though they offer some notational conveniences. In the general semigroup case, one should solve the equation $h = \rho_{(g,1)^{t-1}}(g)$.

Originally, the first proposed platform for SPDKE is the semigroup of 3×3 matrices over the group ring $\mathbb{Z}_7[A_5]$ [15]; however, this turned out to be vulnerable to a linear algebraic attack in [23] which is based on a reduction from discrete logarithm in matrix groups to discrete logarithm in finite fields. Another platform used is tropical algebras [14] which was also later shown to be insecure [17, 21]. Then, a commutative ring formed by square matrices over a ring is proposed in the MAKE protocol [24]. However, the protocol is vulnerable to another linear algebraic attack [9], which relies on the commutativity of the underlying ring. Moreover, Battarbee et.al in [6] show that protocols using matrices over non-commutative rings under some conditions are also vulnerable to this attack. The only proposed platform groups for SPDKE that are still unaffected by all previous attacks are the so-called free nilpotent p-groups [19]. Note that all previous attacks exploit the structure of the platform groups to directly solve the corresponding key recovery problem without solving the corresponding semidirect discrete logarithm problem. See [7] for a more detailed survey on the semidirect product key exchange.

The most recent cryptographic protocol based on the hardness of the SDLP is proposed by Battarbee et al. [8]. They propose a post-quantum signature scheme, called SPDH-Sign, where the security depends on the presumed difficulty of the group case of the SDLP. Moreover, they propose certain non-abelian groups of order p^3 for some odd prime p as candidate groups for SPDH-Sign.

In generic groups and semigroups, the best known algorithm for the SDLP is the subexponential-time quantum procedure proposed by Battarbee et al. [5], which uses Kuperberg's hidden shift algorithm. They present a subexponential quantum algorithm for the SDLP in so-called the *easy* family of semigroups $\{G_p\}_{p \in P}$ for some countable set P. A family of semigroups $\{G_p\}_{p \in P}$ is called easy if the size $|G_p|$ grows monotonically and polynomial in p, and the evaluation costs of gh and $\sigma(g)$ is $\mathcal{O}((\log p)^2)$ for any $p \in P$, $g, h \in G_p$, and $\sigma \in \mathrm{End}(G_p)$. Indeed, the critical problem is determining the position of h in the cycle, which is actually an instance of the vectorization problem, and hence reduces to the abelian hidden shift problem for which Kuperberg's subexponential time algorithm [22] is available.

In this paper, we work over black-box groups with non-necessarily unique encoding of elements to obtain sufficiently general results. (Together with assuming ability of evaluating powers of σ, this corresponds to the easy families of [5].) The concept of black-box groups was introduced by Babai and Szemerédi [4] for studying the structure of finite matrix groups. Elements of a black-box group G are represented by binary strings of a certain length and the group itself is given by a list of generators. The group operations are given by oracles. Here we also assume an oracle for computing $\sigma^j(g)$ for $g \in G$ and $j \in \mathbb{Z}_{>0}$. In general, it is not required that every group element is represented by a unique code-word. Instead, there is also an oracle for testing whether two strings represent the same group element. Here we assume a stronger oracle, a *labeling*. It is a function λ defined on the code-words for the group

elements where x and y represent the same group element if and only if $\lambda(x) = \lambda(y)$. We use the term *black-box group with unique labeling* for that sort of black-box groups. The labeling makes it possible to compute the structure of G when G is a solvable black-box group by the quantum algorithm of [18, Theorem 7]. (In that paper the term *secondary encoding* is used for the labeling.) The notion includes black-box groups with unique encoding. We need the generalization in order to handle certain factor groups. To illustrate how this can occur, assume that initially we work with a matrix group G and σ is given as conjugation by a matrix (possibly outside G) and we have another, non-faithful matrix representation ψ of G whose kernel is σ-invariant. (*Conjugation* by a matrix or a group element h is the map $x \mapsto h^{-1}xh$. A *matrix representation* ψ of a group G is a homomorphism from G to the group of non-singular $d \times d$ matrices over a field. The representation ψ is called *faithful* if it is an injective map, or, equivalently, its kernel only contains the identity element of G.) Suppose further that we need to solve the SDLP for $\psi(g)$ and $\psi(h)$ in $\mathrm{Im}(\psi)$and the automorphism induced by σ. (Recall that this is the unique map $\overline{\sigma} : \mathrm{Im}(\psi) \to \mathrm{Im}(\psi)$ satisfying $\psi(\sigma(x)) = \overline{\sigma}(x)$. It is well-defined as the kernel of ψ is required to be σ-invariant.) It turns out that we would have difficulties with evaluating powers of the induced automorphism if we used the natural unique encoding of the elements of $\mathrm{Im}(\psi)$ by matrices. (In general, this would require finding an element of the pre-image $\psi^{-1}(x)$ for $\mathrm{Im}(\psi)$). We get around the issue by using the original matrices to encode the elements of $\mathrm{Im}(\psi)$ and to multiply them; while considering ψ as a labeling (and possibly also as further help). This gives us a simple way to evaluate the induced automorphism.

The SDLP(G, σ) is called the *group-base* case if G is a group, and we call it the *(full) group* case when G is a group and σ is an automorphism of G. In this paper we focus on the group-base case. If, in addition, σ is an automorphism of G then one could replace the monoid $\mathbb{Z}_{\geq 0}$ with an appropriate finite cyclic group $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ where m is a multiple of the order of σ and work over the finite semidirect product group of G and $\mathbb{Z}_m$. This justifies the terminology.

We briefly recall some elementary, though perhaps not very widely known concepts from group theory. Conjugations by elements of G are automorphism of G. These are the *inner* automorphisms of G. A subgroup $N \leq G$ is *normal* in G ($N \lhd G$ in notation) if $h^{-1}xh \in N$ for every $x \in N$ and $h \in G$, that is, all the inner automorphisms of G leave N invariant. The kernel $\ker \psi$ of a homomorphism ψ to another group K is a normal subgroup of G. If N is a normal subgroup of G then the left cosets of N in G are the same as the right cosets and these cosets form a group G/N, called the *factor* or *quotient* group. The map $x \mapsto xN = \{xh : h \in N\}$ is a homomorphism of G onto G/N with kernel N. The inner automorphisms of G form a normal subgroup $\mathrm{Inn}(G)$ of the full group $\mathrm{Aut}(G)$ of automorphisms of G. The factor $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G. A group G is *commutative* (or *abelian*, as a synonym) if $xy = yx$ for every $x, y \in G$. In a commutative group each subgroup is normal. Every group G has a largest normal subgroup G' such that the factor group G/G' is commutative. As G' turns out to be the smallest subgroup of G containing all the *commutators*, the elements of the form $x^{-1}y^{-1}xy$, G' is called the *commutator* subgroup. A series $G = G_0 \rhd G_1 \rhd \ldots \rhd G_k$ is called a *subnormal* series. The series is called *normal* if each member is normal in the whole group G. Subgroups reachable by subnormal series are called subnormal. A group G is called *solvable* if there is a subnormal series $G = G_0 \rhd G_1 \rhd \ldots \rhd G_k \rhd \{1_G\}$ such that the factor groups G_i/G_{i+1} are commutative. In fact, in a solvable groups there is normal series from G to the trivial subgroup $\{1_G\}$ with commutative factors. (The iterated commutator subgroups (that is, G, G', $(G')'$, and so on) form such a normal series.) Solvable groups can be considered as generalizations of commutative groups. Subgroups and factor groups of solvable groups are solvable.

Contributions. In this paper, we provide an analysis of the SDLP in some interesting classes of groups. Particularly, in Sect. 2, we first give a reduction from the group-base case to the group case of the SDLP. Moreover, using essentially the same idea, we show that there exists a recursion from the SDLP in a group into its quotient groups and subgroups. In Sect. 3, we then propose efficient quantum algorithms based on Shor's algorithm for the group case SDLP(G, σ) for the following cases:

1. The automorphism σ is of small order, i.e., polynomial in $\log |G|$;
2. The group G is solvable;
3. The group G is a matrix group over a finite field, i.e., $G \leq \mathrm{GL}_d(\mathbb{F}_q)$, where q is a power of a prime and σ is an inner automorphism of G;
4. A flag $1 = M_0 < M_1 < \ldots < M_k = G$ of σ-invariant normal subgroups $M_i \lhd G$ is given together with homomorphisms ψ_i from M_i with kernel M_{i-1} $(i = 1, \ldots, k)$, where for each i, ψ_i maps M_i to either
   - 4.1 a black-box group with unique labeling and where the automorphism of $\mathrm{Im}(\psi_i)$ induced by σ has polynomially small order; or
   - 4.2 a solvable black-box group with unique labeling; or
   - 4.3 a matrix group over a finite field, in which case we also assume that a power of the induced automorphism with a polynomially small exponent coincides with the conjugation by some matrix.

As a consequence, SPDH-Sign protocol in [8] and all other SPDKE cryptographic protocols whose platform groups are in the above cases do not belong to the realm of post-quantum cryptography. The candidate groups for SPDH-Sign [8] are non-commutative groups of order p^3 for prime number p. As every group of prime power order is solvable, item 2. applies to them as well as to the so-called free nilpotent p-groups proposed for SDPKE in [19]. See Sect 2.4 for a description of the algorithm that solves SDLP in the candidate groups for SPDH-Sign. We remark that, a normal series together with the homomorphisms having the properties required in item 4., can be efficiently computed for quite a wide class of finite groups using advanced algorithms of computational group theory. These include matrix groups over finite fields of odd characteristic making the innerness assumption of item 3. unnecessary when q is odd, see the Appendix for a sketch of proof. We even think that it is difficult to propose any "concrete" platform group that item 4. is not applicable to, so a viable platform for SPDH-Sign protocol should be a semigroup quite far from any group. In contrast to groups, semigroups may have quite dummy structure. For example, we can make any set S a semigroup by defining multiplication $xy = y$. This operation is very easy to compute. On the other hand, if σ is any permutation of S, then $\rho_{(g,1)^{t-1}}(g) = \sigma^t(g)$ and SDLP(S, σ) for $g, h \in S$ is just solving the equation $h = \sigma^t(g)$. Thus testing membership in orbits of cyclic permutations group can be cast as instances of the SDLP.

2 Reduction and recursion of SDLP

In this section, we provide the reduction of the group-base case to the group case, and we also describe a recursion tool that passes the SDLP in a group to its quotient groups and subgroups.

We have the following equality

$$\prod_{i=0}^{rt-1}\sigma^i(g)=\prod_{j=0}^{t-1}\sigma^{rj}\left(\prod_{i=0}^{r-1}\sigma^i(g)\right). \tag{1}$$

We will frequently use this to reduce an instance of the SDLP for the endomorphism σ to an instance for σ^r in place of σ with suitable choices of r.

2.1 Reduction from the group-base case to the group case

Let G be a finite group and σ be an endomorphism of G. We will describe a reduction from SDLP(G,σ) to SDLP(K,σ') where K is a subgroup of G and σ' is the restriction of σ to K which forms an automorphism.

Let $K=\cap_{t=0}^{\infty}\sigma^t(G)$ and let k_0 be the smallest non-negative integer such that $K=\sigma^{k_0}(G)$. Obviously, $k_0\le\lceil\log|G|\rceil$. Let $k\ge k_0$, where such a k can be "blindly" chosen by taking an integer greater than a known upper bound for $\log|G|$. (Such an upper bound can be ℓ, where binary strings of length ℓ encode the group elements.) Then $K=\sigma^k(G)$ and the restriction of σ to K is an automorphism of K. Let r be the length of the orbit $\{\rho_{(\sigma^k(g),1)^t}(1_G):t\in\mathbb{Z}_{\ge0}\}$ and put $M=\ker\sigma^k=\ker\sigma^{k_0}$. Then $K\cong G/M$, $K\cap M=\{1_G\}$, and we have

$$r=\min\{t\in\mathbb{Z}_{>0}:\rho_{(\sigma^k(g),1)^t}(1_G)=1_G\}=\min\{t\in\mathbb{Z}_{>0}:\rho_{(g,1)^t}(1_G)\in M\}.$$

Let $g'=\rho_{(g,1)^r}(1_G)=\prod_{i=1}^{r-1}\sigma^i(g)$. Then, by equality (1), $\rho_{(g,1)^{rt}}(1_G)=\prod_{j=0}^{t-1}\sigma^{rj}(g')$. As $g'\in M=\ker\sigma^k$, for $rt\ge k$ we have $\sigma^{rt}(g')=1_G$, and hence

$$\begin{aligned}\rho_{(g,1)^{r(t+1)}}(1_G)&=\prod_{i=0}^{t}\sigma^{ri}\left(\prod_{j=0}^{r-1}\sigma^j(g)\right)=g'\sigma^r(g')\cdot\ldots\cdot\sigma^{r(t-1)}(g')\sigma^{rt}(g')\\&=g'\sigma^r(g')\cdot\ldots\cdot\sigma^{r(t-1)}(g')=\prod_{i=0}^{t-1}\sigma^{ri}\left(\prod_{j=1}^{r-1}\sigma^j(g)\right)\\&=\rho_{(g,1)^{rt}}(1_G).\end{aligned}$$

It follows that

$$\rho_{(g,1)^{r(t+1)+s}}(1_G)=\rho_{(g,1)^{rt+s}}(1_G), \tag{2}$$

By equation (2), if the solution set of the SDLP in K for $\sigma^k(g)$ and $\sigma^k(h)$ is $\{s+rt:t\in\mathbb{Z}_{\ge0}\}$ for some $0\le s<r$, then the set of solutions of the SDLP in G for g and h is either the empty set, a singleton $\{s+rt_0\}$, or $\{s+rt:t\in\mathbb{Z}_{\ge t_0}\}$, for some $t_0\le\lceil k_0/r\rceil\le\lceil\log|G|\rceil$. Therefore, one can solve the SDLP(G,σ) for g and h by solving SDLP$(K,\sigma|_K)$ for $\sigma^k(g)$ and $\sigma^k(h)$, followed by an exhaustive search. This gives the following theorem.

Theorem 1 *Let G be a group and let σ be an endomorphism of G. Then there is a classical polynomial time reduction from an instance of SDLP(G,σ) to an instance of SDLP(K,τ), where $K=\cap_{t=0}^{\infty}\sigma^t(G)$ and τ, the restriction of a power of σ to the subgroup K, is an automorphism of K.*

2.2 An easy reduction

In the group case, we have the following simple reduction based on brute force. This will be useful when a power of the automorphism σ with polynomially small exponent has some desired property.

Proposition 2 *Assume that σ is an automorphism of the group G. Then, for every positive integer k, SDLP(G, σ) can be reduced to k instances of SDLP(G, σ^k).*

Proof We compute the length r of $\{\rho_{(g,1)^t}(1_G) : t \in \mathbb{Z}\}$ and also the length of the orbit $\{\rho_{(g,1)^t}(h) : t \in \mathbb{Z}\}$ starting at h using Shor's period finding algorithm. If the lengths differ, there is no solution of the SDLP so we can stop. Otherwise we look for the smallest non-negative solution of the SDLP in the form $s + tk$ for $s = 0, \ldots, k-1$. We have

$$\begin{aligned}\rho_{(g,1)^{s+tk}}(1_G) &= \prod_{i=0}^{s+tk-1} \sigma^i(g) \\ &= \prod_{j=0}^{s-1} \sigma^j(g)\sigma^s\left(\prod_{i=0}^{tk-1} \sigma^i(g)\right) \\ &= \rho_{(g,1)^s}\left(\prod_{i=0}^{tk-1} \sigma^i(g)\right) \\ &= \rho_{(g,1)^s}\left(\prod_{i=0}^{t-1} \sigma^{ik}\left(\prod_{j=0}^{k-1} \sigma^j(g)\right)\right),\end{aligned}$$

whence $h = \rho_{(g,1)^{s+tk}}(1_G)$ if and only if $\rho_{(g,1)^{-s}}(h) = \prod_{i=0}^{t-1} \sigma^{ik}(\prod_{j=0}^{k-1} \sigma^j(g))$. Let $g' = \rho_{(g,1)^k}(1_G) = \prod_{j=0}^{k-1} \sigma^j(g)$ and $h' = \rho_{(g,1)^{-s}}(h) = \rho_{(g,1)^{r-s}}(h) = (\prod_{j=0}^{r-s-1} \sigma^j(g))\sigma^{r-s}(h)$. Then, we need to solve the SDLP for g' and h', where we replace σ by σ^k. □

2.3 Recursion into quotient groups and subgroups

We will show that one can solve the SDLP(G, σ), for a group G and $\sigma \in \mathrm{Aut}(G)$, by recursively solving an instance of the SDLP in a quotient group and a subgroup of G. The main idea of recursion is essentially the same as those used in the preceding subsections.

Theorem 3 *Let G and $\overline{G}$ be black-box groups with unique labeling and let an automorphism σ of G be given by a black box for evaluating the powers σ^i on codewords for group elements. Assume that we are given a σ-invariant normal subgroup M of G and a group homomorphism $\psi : G \to \overline{G}$ with kernel M. We assume that ψ can be evaluated efficiently and we have a black box for evaluating powers of the automorphism $\overline{\sigma}$ of $Im(\psi)$ induced by σ. Then SDLP(G, σ) can be reduced to an instance of SDLP$(Im(\psi), \overline{\sigma})$ and an instance of SDLP$(M, \sigma_{|M}^{n_0})$ for some integer n_0.*

Proof We begin with computing the lengths of the orbits $\{\rho_{(g,1)}^t(1_G) : t \in \mathbb{Z}\}$ and $\{\rho_{(g,1)^t}(h) : t \in \mathbb{Z}\}$ using Shor's period finding algorithm. If the lengths differ, then h cannot be in the orbit starting at 1_G. Otherwise let r be the common orbit length. Since $\psi \circ \sigma = \overline{\sigma} \circ \psi$, we have $\rho_{(\psi(g),1)^{t-1}}(1_{\overline{G}}) = \prod_{i=0}^{t-1} \overline{\sigma}^i(\psi(g)) = \psi(\prod_{i=0}^{t} \sigma^i(g)) = \psi(\rho_{(g,1)^t}(1_G))$. Therefore,

every solution of SDLP(G, σ) for g and h is a solution of the SDLP$(\mathrm{Im}(\psi), \overline{\sigma})$ for $\psi(g)$ and $\psi(h)$. Assume that we can find the set of solutions for the problem in $\mathrm{Im}(\psi)$. If this set is empty, then there is no solution for the problem in G either.
Otherwise, the set of solutions in $\mathrm{Im}(\psi)$ is the residue class $\{t_0 + n_0 t : t \in \mathbb{Z}\}$ for some $0 \le t_0 < n_0$, where $n_0 = |\{\rho_{(\psi(g),1)^t}(1_G) : t \in \mathbb{Z}\}|$, Note that n_0 is the smallest positive integer such that $\rho_{(\psi(g),1)^{n_0}}(1_{\overline{G}}) = 1_{\overline{G}}$, or, equivalently, $\rho_{(g,1)^{n_0}}(M) = M$. The solutions for the original problem is a – possibly empty – subset of this residue class. Accordingly, we look for the solutions in the form $t_0 + n_0 t$. Like in the proof of Proposition 2, we have

$$\begin{aligned}
\rho_{(g,1)^{t_0+n_0 t}}(1_G) &= \prod_{i=0}^{t_0+tn_0-1} \sigma^i(g) \\
&= \prod_{j=0}^{t_0-1} \sigma^j(g) \sigma^s \left(\prod_{i=0}^{tn_0-1} \sigma^i(g) \right) \\
&= \rho_{(g,1)^{t_0}} \left(\prod_{i=0}^{tn_0-1} \sigma^i(g) \right) \\
&= \rho_{(g,1)^{t_0}} \left(\prod_{i=0}^{t-1} \sigma^{in_0}(g') \right),
\end{aligned}$$

where $g' = \prod_{j=0}^{n_0-1} \sigma^j(g) = \rho_{(g,1)^{n_0}}(1_G))$. Thus $h = \rho_{(g,1)^{t_0+n_0 t}}(1_G)$ if and only if $\rho_{(g,1)^{-t_0}}(h) = \prod_{i=0}^{t-1} \sigma^{in_0}(g')$. This shows that the problem we need to solve is the SDLP for g' and $h' = \rho_{(g,1)^{-t_0}}(h) = \rho_{(g,1)^{r-t_0}}(h)$ with automorphism σ^{n_0}. We have $g' = \rho_{(g,1)^{n_0}}(1_G)) \in M$ and by $\psi(h) = \rho_{(\psi(g),1)^{t_0}}(1_{\overline{G}})$ we have $\psi(h') = \psi(\rho_{(g,1)^{-t_0}}(h)) = \rho_{(\psi(g),1)^{-t_0}}(\psi(h)) = 1_{\overline{G}}$, thus $h' \in M$ as well. Therefore the final problem we need to solve is and instance of the SDLP(M, σ^{n_0}). We find the solution set T of this problem by a recursion into M. If T is the empty set then the original problem has no solutions either. Otherwise T is the residue class $\{t_1 + n_1 t : t \in \mathbb{Z}\}$ and then we conclude that our problem in G has solution set $t_0 + n_0 T = \{t_0 + n_0 t_1 + n_0 n_1 : t \in \mathbb{Z}\}$. □

By considering the equivalent "backward" version of the SDLP, that is, solving $1_G = \rho_{(g,1)^t}(h)$, the recursion suggested by the proof of the theorem can be interpreted as bringing h first into M by solving the SDLP in $\mathrm{Im}(\psi) \cong G/M$ and then, inside M, bringing it further to the identity element.

A general straightforward way to evaluate the induced automorphism (and its powers) is based on computing an arbitrary element of the pre-image $\psi^{-1}(\overline{x})$ for each $x \in \mathrm{Im}(\psi)$. This can be facilitated by replacing $\overline{G}$ with the black-box group H encoded by pairs $(x, \psi(x))$, where x is a code-word for an element of G. For multiplication we use the oracle for G and re-evaluate ψ on the product. For labeling, we use the labeling of $\overline{G}$. Of course, there are many cases when this trick can be replaced by a simple direct method for evaluating $\overline{\sigma}$. This holds in particular when $\overline{G} = \mathbb{Z}_p^d$ with the standard representation by column vectors modulo p.

2.4 Example: the candidate groups for SPDH-Sign

We show below how the reduction presented Sect. 2.3 works on the example of the candidate groups for the protocol SPDH-Sign proposed in [8].

Let p be a prime and assume that we have to solve the SDLP(G, σ) for elements $g, h \in G$, where G is the group of matrices over the *ring* $\mathbb{Z}_{p^2} = \mathbb{Z}/p^2\mathbb{Z}$ of the form

$$\begin{pmatrix} pa+1 & b \\ 0 & 1 \end{pmatrix}.$$

The group G has order p^3, its commutator subgroup G' consists of the matrices of the form

$$\begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix},$$

while the elements of order 1 and p are exactly the elements of the subgroup consisting of the matrices of the form

$$\begin{pmatrix} pa+1 & pb \\ 0 & 1 \end{pmatrix}.$$

We denote the latter subgroup by M_2 and also define M_1 as G'. Since G', as well as the set of elements of order p are invariant under any automorphism, we have that $M_1 = G'$ and M_2 are σ-invariant normal subgroups of G (independently of the choice of σ). We work along the sequence $G \rhd M_2 \rhd M_1 \rhd \{1_G\}$. We define the maps $\psi_1 : M_1 \mapsto \mathbb{Z}_p$, $\psi_2 : M_2 \mapsto \mathbb{Z}_p$ and $\psi_3 : G \mapsto \mathbb{Z}_p$ as

$$\psi_1 \begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix} = b,\ \psi_2 \begin{pmatrix} pa+1 & pb \\ 0 & 1 \end{pmatrix} = a \text{ and } \psi_3 \begin{pmatrix} pa+1 & b \\ 0 & 1 \end{pmatrix} = b,$$

respectively, where we reduce the right hand sides modulo p. It is straightforward to check that ψ_1 is an isomorphism between M_1 and the additive group $\mathbb{Z}_p$, while ψ_2 and ψ_3 are homomorphism with kernel M_1 resp. M_2 onto the same group.

Every automorphism τ of the additive group $\mathbb{Z}_p$ is equivalent to multiplication by a nonzero residue modulo p: $\tau(x) = cx$ for some $c \in \mathbb{Z}_p \setminus \{0\}$. Then for $g \in \mathbb{Z}_p$ and $t \in \mathbb{Z}$ we have

$$g + \tau(g) + \ldots + \tau^{t-1}(g) = g(1 + c + \ldots + c^{t-1}) = \begin{cases} tg & \text{if } c = 1, \\ \frac{c^t-1}{c-1} g & \text{otherwise.} \end{cases}$$

We discuss the SDLP in $\mathbb{Z}_p$ for g, h with automorphism $\tau = c\cdot$. If $g = 0$ or $c = 0$ the period (the orbit length) is 1 and then there is no solution unless $h = g$. When $g \neq 0$ and $c = 1$ the period is p and the smallest solution can be obtained by a simple division modulo p. Finally, for $g \neq 0$ the period equals the the multiplicative order of c and the smallest solution can be computed by calculating the base-c discrete logarithm of $(c-1)hg^{-1} + 1$. Therefore this case can be generally treated by Shor's quantum algorithm. Of course, the set of solutions is either empty or a complete residue class modulo the period.

We attempt to so solve the SDLP in $\mathbb{Z}_p$ for $\psi_3(g)$ and $\psi_3(h)$ with the automorphism of $\mathbb{Z}_p$ induced by σ. We stop if there is no solution to this problem. If the solution set is the residue class $\{t_3 + n_3 t : t \in \mathbb{Z}\}$ then we put $g_2 = \rho_{(g,1)^{n_3}}(1_G) = \prod_{i=0}^{t_3-1} \sigma^i(g)$ and $h_2 = \rho_{(g,1)^{-t_3}}(1_G) = (\prod_{i=0}^{n_3-t_3-1} \sigma^i(g))\sigma^{n_3-t_3}(h)$. Actually, g_2 and h_2 can be efficiently computed by calculating $(g,1)^{n_3}$ and $(g,1)^{n_3-t_3}$ in the semidirect product group $G \rtimes_\sigma \mathbb{Z}$ using fast exponentiation (repeated squaring), and then applying the ρ-actions of these on 1_G and on h, respectively. We have $g_2 = \rho_{(g,1)^{n_3}}(1_G) \in M_2$ and $h_2 = \rho_{(g,1)^{-t_3}}(h) \in M_2$.

We continue with working in M_2. There we need to solve the SDLP for g_2 and h_2 with automorphism σ^{n_3}. Like above, we solve the SDLP in $\mathbb{Z}_p$ for $\psi_2(g_2)$ and $\psi_2(h_2)$ with the automorphism induced by σ^{n_3}. We stop if there is no solution, otherwise assume that the solution set is

the residue class $\{t_2 + n_2 t : t \in \mathbb{Z}\}$. We compute $g_1 = \prod_{i=0}^{n_2-1} \sigma^{n_3 i}(g_2) = \prod_{j=0}^{n_2 n_3 - 1} \sigma^j(g) = \rho_{(g,1)^{n_2 n_3}}(1_G)$ and $h_1 = (\prod_{i=0}^{n_2-t_2-1} \sigma^{n_3 i}(g_2))\sigma^{n_3 n_2 - n_3 t_2}(h_2) = \rho_{(g,1)^{-t_2 n_3 - t_3}}(h)$. We have $g_1, h_1 \in M_1$.

In M_1 we solve the SDLP for g_1 and h_1 with automorphism $\sigma^{n_2 n_3}$ by working with the images $\psi_1(g_1)$ and $\psi_1(h_1)$ in $\mathbb{Z}_p$. If the solution set is empty then so is the solution set of the original SDLP in G. Otherwise, if the solutions are the members of the residue class $\{t_1 + n_1 t : t \in \mathbb{Z}\}$, the original SDLP in G has solution set $\{t_1 n_2 n_3 + t_2 n_3 + t_3 + t n_1 n_2 n_3 : t \in \mathbb{Z}\}$.

3 Quantum algorithms for the group case SDLP

In this section, we will prove the following main result of the paper.

Theorem 4 *Let G be a group and $\sigma \in \mathrm{Aut}(G)$. We assume that G is a black-box group with a unique labeling of elements and we also have a black box for computing $\sigma^i(g)$ ($i \in \mathbb{Z} \geq 0, g \in G$). Suppose that we are given a series $1 = M_0 < M_1 < \ldots M_k = G$ of σ-invariant normal subgroups $M_i \lhd G$ together with homomorphisms $\psi_i : M_i \to \overline{G}_i$ ($i = 1, \ldots, k$) with kernel M_{i-1} ($i = 1, \ldots, k$). Let $\overline{\sigma}_i$ denote the automorphism of $Im(\psi_i)$ induced by $\sigma_{|M_i}$. Assume further that, for each i, either*

(0) $Im(\psi_i)$ is of polynomial size; or
(1) $\overline{\sigma}_i$ has polynomial order; or
(2) $Im(\psi_i)$ is solvable;
(3) $\overline{G}_i \leq \mathrm{GL}_{d_i}(\mathbb{F}_{q_i})$ for some positive integer d_i and for some prime power q_i, moreover, there exists a polynomially bounded integer n_i and a matrix $a_i \in \mathrm{GL}_{d_i}(\mathbb{F}_{q_i})$ such that $\overline{\sigma}_i^{n_i}(x) = a_i^{-1} x a_i$ for every $x \in Im(\psi_i)$.

For items (0), (1) and (2), we assume that $\overline{G}_i$ is a black-box group with unique labeling. For item (4), neither n_i nor a_i are assumed to be given, their mere existence is sufficient. (By "polynomial" we mean polynomial in the maximum of the lengths of the bit strings used for encoding and labeling the elements of the groups G and $\overline{G}_i$ ($i = 1, \ldots, k$). Then $SDLP(G, \sigma)$ can be solved in quantum polynomial time.

When $k = 1$, condition of type (0) means that G itself is of polynomial size, that of type (1) means that σ itself has polynomially small order, that of type (2) means that G is solvable. The standard descriptions of simple groups of Lie type define them as factors of certain matrix groups over finite fields. The quotient is taken to be the center of the matrix group, so the simple group has a representation as a matrix group by the conjugation action on the matrix algebra spanned by the covering matrix group. Also, the outer automorphism group of a finite simple group is of polynomial size. Therefore, these groups are covered by conditions of type (3).

The algorithm for polynomially small groups is the straightforward trial and error. In the first three subsections of this section we give efficient algorithms for groups/automorphisms satisfying conditions (1), (2), or (3). In the fourth subsection we show how to use these ingredients and Theorem 3 to prove Theorem 4.

Note that the order of σ can be computed in quantum polynomial time using Shor's period finding method applied to the functions $t \mapsto \sigma^t(x_i)$ for the generators x_i of the group G and taking the least common multiple of these periods. The order can be factorized using Shor's factoring algorithm. The length of the orbit $\{\rho_{(g,1)^t}(1_G) : t \in \mathbb{Z}\}$ can be determined and

factorized in a similar way. Based on these observations, in the algorithms below we assume that these numbers are already computed and factorized. The solution set is either empty or the residue class of an arbitrary solution modulo the period. So it is sufficient to find any solution, e.g., the smallest non-negative one.

3.1 The SDLP for small order automorphisms

In this subsection we prove the following result.

Proposition 5 *Let G be a black-box group with unique labeling. Then SDLP(G, σ) can be solved by a quantum algorithm in time polynomial in the order of σ and the length of the code-words together with the labels of the group elements.*

Proof By Proposition 2, it is sufficient to prove the case when σ is trivial. Then $\rho_{(g,1)}(x) = gx$, whence $\rho_{(g,1)^t}(1_G) = g^t$ for every integer t. Thus, solving the SDLP for g and h is the same as computing the base-g discrete logarithm of h, which can be accomplished by a standard generalization of Shor's algorithm, see e.g., the survey paper [1] for a description. □

We remark that Shor's method can be further extended to the discrete logarithm problem in *semigroups*, see [11]. The special case of the problem in the multiplicative semigroup of $d \times d$ matrices, that is solving $A^t = B$ for matrices A and B over a field, is called the *Matrix Power Problem* in [20]. We will make use of the fact that this problem can be solved in quantum polynomial time for matrices over finite fields.

3.2 The SDLP in solvable groups

In this part, we first present a quantum algorithm for the SDLP on elementary abelian groups. We then show how Theorem 3 can be used to reduce the general solvable case to instances of the elementary abelian case.

Theorem 6 *Let $G = \mathbb{Z}_p^d$, the (additive) group of column vectors of length d over the integers modulo p, where p is a prime number and let σ be an automorphism of G, given as a $d \times d$ non-singular matrix. Then SDLP(G, σ) can be solved by a quantum algorithm in time polynomial in* $\log p$ *and d.*

Proof We consider G as a vector space of dimension d over the finite field $\mathbb{Z}_p$. We take a minimal nontrivial σ-invariant subspace M of G. This can be done, e.g., by a classical randomized method based on computing the rational Jordan normal form of σ, see [13]. Then the factor space M has no proper nontrivial σ-invariant subspace. Iterating this in G/M, we eventually obtain a flag of subspaces $(0) = M_0 < M_1 < \ldots < M_k = G$ such that there is no σ-invariant subspace strictly between M_{i-1} and M_i. Then, by Theorem 3, the problem is reduced to the case when G has no proper nontrivial σ-invariant subspace. Suppose that we have an instance of that case.
If 1 is an eigenvalue of σ then $d = 1$ and σ is trivial. It follows that $\rho_{(g,1)^t}(1_G) = g^t$. Using the additive notation for $\mathbb{Z}/p\mathbb{Z}$, we need to solve $h = t \cdot g$. If $g = 0$ and $h = 0$ then every integer is a solution, while if $g = 0$ and $h \neq 0$ then there is no solution. If $g \neq 0$ let g' stand for the multiplicative inverse of g in the field $\mathbb{Z}/p\mathbb{Z}$. Then the solutions are $\{hg' + tp : t \in \mathbb{Z}\}$. (Actually, the case when σ is trivial is a special case of the broader case already discussed in Subsection 3.1.)

If 1 is not an eigenvalue then we do the following. We compute the matrix B of σ in the standard basis of $(\mathbb{Z}/p\mathbb{Z})^d$. Then, using again the additive notation, we can write $\rho_{(g,1)^t}(1_G)$ as $\sum_{j=0}^{t-1} B^j g$. We have to solve

$$\sum_{j=0}^{t-1} B^j g = h. \tag{3}$$

We adopt an idea from [20] to reduce this task to an instance of the Matrix Power Problem. Multiplying the equation by $B, B^2, \ldots, B^{d-1}$ gives

$$\sum_{j=0}^{t-1} B^{i+j} g = B^i h \ \ (i = 0, 1, \ldots, d-1) \tag{4}$$

We claim that the vectors $g, Bg, \ldots, B^{d-1}g$ are linearly independent. This is trivial if $d = 1$. If $d > 1$, assume that $B^k g$ is linearly dependent of the vectors $g, \ldots, B^{k-1}g$ for some $k < d$: $B^k g = \sum_{i=0}^{k-1} B^i g$. Then $B^k g$ is contained in the subspace U spanned by the vectors $g, Bg, \ldots, B^{k-1}g$. Then, by induction, $B^\ell g \in U$ for every $\ell \geq 0$. Thus U is B-invariant subspace of dimension $1 \leq k < d$. In terms of G, U is a σ-invariant proper subgroup, contrary to our assumption. Let C be the matrix with column vectors $g, Bg, \ldots, B^{d-1}g$ and let D be the matrix with column vectors $h, Bh, \ldots, B^{d-1}h$. Then C is an invertible matrix and, by equation (4) we obtain that equation (3) is equivalent to

$$\sum_{j=0}^{t-1} B^j C = D,$$

which is further equivalent to

$$\sum_{j=0}^{t-1} B^j = DC^{-1}. \tag{5}$$

As 1 is not an eigenvalue of B, we have that the matrix $B - I$ is invertible (here I stands for the $d \times d$ identity matrix) and we have

$$\sum_{j=0}^{t-1} B^j = (B^t - I)(B - I)^{-1}. \tag{6}$$

By substituting this into the left hand side of equation (5), then multiplying $B - I$ both sides and adding and adding the identity matrix, we obtain that the equation to solve becomes

$$B^t = DC^{-1}(B - I) + I. \tag{7}$$

This is an instance of the Matrix Power Problem, which can be solved in quantum polynomial time as discussed in Sect. 3.1. □

The method for the elementary abelian case, in combination with the recursion tool (Theorem 3), gives an efficient quantum algorithm for solving the SDLP in solvable groups. More precisely, we obtain the following result.

Theorem 7 *Assume that G is a solvable black-box group with unique labeling. Then SDLP(G, σ) can be solved by a quantum algorithm in time polynomial in the order of σ and the length of the code-words together with the labels of the group elements.*

Proof Using the labeling, by [18, Theorem 7] which is based on the Beals-Babai algorithm [3], we can compute a composition series of G with explicit isomorphisms between the composition factors and additive groups $\mathbb{Z}_p$ for various primes p. In particular, we obtain a maximal normal subgroup N of G together with a homomorphism $\phi : G \mapsto \mathbb{Z}_p$. For any positive integer j, let $N_j = \cap_{i=0}^{j-1}\sigma^i(N)$. Note that $N_{j+1} = N_j \cap \sigma^j(N)$ and if $N_{j+1} = N_j$ then $N_{j'} = N_j$ for any integer $j' > j$ and N_j is σ-invariant. This equality happens for an integer j bounded by the length ℓ of code-words for the group elements. We compute the map $\psi : G \mapsto \mathbb{Z}_p^\ell$ defined as $x \mapsto (\phi(x), \phi^\sigma(x), \ldots, \phi^{\sigma^{\ell-1}}(x))^T$. Based on the above discussion, the kernel M of ψ is σ-invariant. The image $\mathrm{Im}(\psi)$ is a subspace V of $\mathbb{Z}_p^\ell$. Compute a basis for V by taking a maximal linearly independent set of the images of the generators for G under the map ψ and using them replace ψ with the composition of ψ with the transpose of the matrix whose columns are the bases elements for V. This new map, denoted again by ψ, is a surjective homomorphism from G to $\mathbb{Z}_p^d$ with kernel M. Then, by Theorem 3, after solving the SDLP in the ψ-image $\mathbb{Z}_p^d$, SDLP(G, σ) gets reduced to SDLP(M, σ') where σ' is the restriction of a power of σ to M. As subgroups of solvable groups are solvable, M is a solvable group of order at most $|G|/2$, so we can recurs into M to solve the SDLP there. The total depth of the recursion is bounded by $\log |G|$, which is polynomial in the length of the codewords for the elements of G. Alternatively, the recursion can be rewritten as an iteration with at most $\log |G|$ rounds. □

3.3 The SDLP in matrix groups with an inner automorphism

This part is is devoted to prove the part of Theorem 4 regarding matrix groups, the factors with property (3).

In the proof we will encounter an instance of the well known *Orbit Problem* introduced by Harrison in [16]. It is the following orbit membership problem. Given vectors a, b of a finite dimensional vector space V over the field $\mathbb{F}$ and a linear transformation $\Phi \in \mathrm{End}_{\mathbb{F}}(V)$, find $t \in \mathbb{Z}_{\geq 0}$, if there exists, such that $b = \Phi^t a$.

Kannan and Lipton in [20] gave a polynomial time solution of the Orbit Problem for the case when $\mathbb{F}$ is the field of rationals. Here we need to solve the finite field case. The method of Kannan and Lipton is based on a construction to reduce the Orbit Problem to the Matrix Power Problem. For completeness we briefly recall (a version of) their reduction. Actually, we used essentially the same idea in the proof of Theorem 6. We compute the subspace W spanned by $\Phi^t a$ ($t = 0, 1, \ldots$). This can be done by computing the vectors $a, \Phi a, \ldots, \Phi^{j-1}a$ until $\Phi^j a$ becomes linearly dependent of the previous vectors. Then W is the subspace with basis $a, \Phi a, \ldots, \Phi^{j-1}a$. If $b \notin W$, then the problem has no solution. Otherwise $\Phi^t b \in W$ for every t. Write the vectors $\Phi^i a$ and $\Phi^i b$ ($i = 0, \ldots, j-1$) as column vectors in terms of a basis of W. Let A be the matrix of the restriction of Φ to W in the same basis and let C resp. D be the $j \times j$ matrices whose columns are $a, \Phi a, \ldots, \Phi^{j-1}a$ and $b, \Phi b, \ldots, \Phi^{j-1}b$, respectively. Then $b = \Phi^t a$ if and only if $D = \Phi^t C$. Note that C is invertible as its columns are linearly independent. Let $B = DC^{-1}$. Then we need to solve $B = A^t$. This is an instance of the Matrix Power Problem and can be solved over finite fields in quantum polynomial time as mentioned in Sect. 3.1.

Equipped with an efficient quantum solution of the finite case of the Orbit Problem, we are ready to prove the following result.

Theorem 8 *Let G be a subgroup of $\mathrm{GL}_d(\mathbb{F}_q)$ where d is a positive integer and q is a power of a prime. Assume that G is given by a list of matrices that generate G and that the automorphism*

σ is given on the generators. Suppose that σ coincides with the conjugation action of a matrix $a \in \mathrm{GL}_d(\mathbb{F}_q)$. Then SDLP$(G, \sigma)$ can be solved by a quantum algorithm in time polynomial in d and $\log q$.

The matrix a that implements the automorphism σ does not need to be given, such a matrix is computed by the algorithm. (It is unique up to the centralizer of G.) Note that conjugation by a is an inner automorphism of the full matrix group $\mathrm{GL}_d(\mathbb{F}_q)$ (or just of the matrix group generated by G and a), justifying the title of the subsection.

Proof We assume that $q \geq 2d$. (If not, we consider G as a matrix group over an extension field of $\mathbb{F}_q$ having at least $2d$ elements.) To find a matrix a with the desired property, we take the linear space of matrices y such that $x_i y = y\sigma(x_i)$ for the generators x_i of G. A basis $a_1, \ldots, a_r$ of the space can be computed by solving a system of linear equations expressing the matrix equations above. Let $t_1, \ldots, t_r$ be variables. The entries of the formal linear combination $a(t_1, \ldots, t_r) = \sum_{i=1}^{r} t_i a_i$ are homogeneous linear polynomials in the variables $t_1, \ldots, t_r$. Its determinant is either identically zero or a homogeneous polynomial of degree d over $\mathbb{F}_q$. As the space contains a non-singular matrix by the assumption of the theorem, $\det(a(t_1, \ldots, t_r))$ is not identically zero. Therefore, by the Schwartz-Zippel lemma [25, 27], a uniformly random substitution $(\lambda_1, \ldots, \lambda_r)^T \in \mathbb{F}_q^r$ will give a matrix $a = a(\lambda_1, \ldots, \lambda_r)$ with nonzero determinant with probability at least $\frac{1}{2}$ because $q \geq 2d$. If a has determinant 0 we choose other random linear combinations until we get one with nonzero determinant. Assume that $\det(a) \neq 0$. Then a, being a linear combination of the matrices $a_1, \ldots, a_r$, satisfies $x_i a = a\sigma(x_i)$, or, equivalently, $a^{-1} x_i a = \sigma(x_i)$.
Since the matrices x_i generate G, and since σ as well as the map $x \mapsto a^{-1}xa$ are automorphisms of G, we have that $a^{-1}xa = \sigma(x)$ for very $x \in G$. It follows that $\rho_{(g,1)}(x) = g\sigma(x) = ga^{-1}xa$. We consider the full matrix algebra $\mathcal{B} = \mathrm{M}_d(\mathbb{F}_q)$ of the $d \times d$ matrices and the map $\Phi : \mathcal{B} \to \mathcal{B}$ defined as $\Phi(x) = ga^{-1}xa$. Obviously, Φ is a linear extension of $\rho_{(g,1)}$ to $\mathcal{B}$. Furthermore, as both g and a are invertible matrices, it is an invertible linear transformation of $\mathcal{B}$, considered as a vector space. Solving $h = \rho_{(g,1)}^t(1_G)$ is equivalent to solving $h = \Phi^t I_d$. This is an instance of the orbit problem in $\mathcal{B}$, considered as a vector space. Therefore it can be solved in quantum polynomial time as discussed above. □

We remark that, using the Jordan blocks of A, one could classically reduce the problem to the instances of the discrete logarithm problem in the multiplicative group of extensions of $\mathbb{F}$. Also, in practice it might be worth replacing $\mathcal{B}$ with the matrix algebra spanned by the elements of G.

Proposition 2 gives the following extension.

Corollary 9 *Let G be as in Theorem 8. Let σ be an automorphism of G. Let K be a positive integer. We assume that for the divisors $k \leq K$ of the order of σ, the action of σ^k on the generators for G is also given and that among those divisors k, σ^k coincides with the conjugation action of a matrix. Then SDLP(G, σ) can be solved by a quantum algorithm in time polynomial in K, d and $\log q$.*

3.4 Putting things together

Our recursion tool (Theorem 3) can assemble the results proved in the preceding subsections for various special cases of the SDLP to obtain Theorem 4.

Proof of Theorem 4 Assume that we have the chain of subgroups M_i and homomorphisms ψ_i $(i = 0, \ldots, k)$ with properties as in the statement of the theorem. For $i = k$ to 1, using Theorem 3, by solving the SDLP in the ϕ_i-image of M_i we reduce the problem to an instance in M_{i-1}. In the small size case (0), we use brute force. When $\overline{\sigma}_i$ is of small order (case (1)) or when $\mathrm{Im}(\psi_i)$ is solvable (case (2)), we use Proposition 5 or Theorem 7, respectively. In order to facilitate using the oracle for evaluating the powers of σ to evaluate those of $\overline{\sigma}_i$, we use the pairs $(x, \psi_i(x))$ to encode the elements of $\mathrm{Im}(\psi_i)$, while as labeling we use the labeling for $\overline{G}_i$. In the matrix group case (4), we use the natural encoding by matrices for the image. We compute the order o_i of $\overline{\sigma}_i$ using the factorization of the order of σ and compute σ^t for the smallest few divisors of o_i and apply the method of Corollary 9. □

Appendix: the matrix group case in odd characteristic

This part is devoted to a sketch of a proof of the following.

Corollary 10 *Let $\psi : K \to M_d(\mathbb{F}_q)$ be a representation of the black-box group K with or without a labeling. Assume that the automorphism σ is given by a black box to evaluate its powers on elements of K and that the kernel of ψ is σ-invariant (e.g., when ψ is faithful). Then, $SDLP(Im(\psi), \overline{\sigma})$ can be solved in quantum polynomial time.*

Proof (sketch) We encode the elements of $G = \mathrm{Im}(\psi)$ by pairs $(x, \psi(x))$ and labeling $\psi(x)$ so that we can evaluate powers of $\overline{\sigma}$ on elements of the matrix group G. We use the notation σ for $\overline{\sigma}$. Below we outline how the result of the polynomial time algorithm of Babai, Beals and Seress [2] for computing the structure of matrix groups over finite fields can be used to obtain a series of normal subgroups together with representations of the factors making Theorem 4 applicable to these matrix groups.

Every finite group G has a unique largest solvable normal subgroup, called the *solvable radical* of G. It is denoted by $\mathrm{Rad}(G)$. The factor group $\overline{G} = G/\mathrm{Rad}(G)$ is trivial if G itself is solvable. Even if $\overline{G}$ is a non-trivial group, it has no nontrivial abelian subnormal subgroups. (Normal subgroups of a group are subnormal, and, recursively, normal subgroups of subnormal subgroups are also subnormal.) It follows that the minimal subnormal subgroups of $\overline{G}$ are non-commutative simple groups. They pairwise commute and the subgroup $\mathrm{Soc}(\overline{G})$ generated by them (called the *socle* of $\overline{G}$) is the direct product of these simple groups. (It follows that there are at most $\log \overline{G}$ simple constituents of $\mathrm{Soc}(\overline{G})$.) The full pre-image of $\mathrm{Soc}(\overline{G})$ at the projection $G \to \overline{G}$ is denoted by $\mathrm{Soc}^*(G)$. The subgroups $\mathrm{Rad}(G)$ and $\mathrm{Soc}^*(G)$ are characteristic subgroups of G. The group G, by conjugation, acts as a permutation group on the minimal subnormal subgroups of $\overline{G}$. The kernel $\mathrm{Pker}(G)$ of this permutation representation, called the *permutation kernel*, is a further characteristic subgroup. There are the following inclusions between the subgroups introduced above.

$$1 \leq \mathrm{Rad}(G) \leq \mathrm{Soc}^*(G) \leq \mathrm{Pker}(G) \leq G.$$

$\mathrm{Pker}(G)$ acts by conjugation as an automorphism group on each simple component of $\mathrm{Soc}(\overline{G})$. As the outer automorphism group of any finite simple group is solvable, the factor group $\mathrm{Pker}(G)/\mathrm{Soc}^*(G)$ is solvable. The algorithm of Babai, Beals and Seress [2] computes in classical randomized polynomial time (generators for) the three subgroups above. They also compute a permutation representation of G with kernel $\mathrm{Pker}(G)$ (this is actually the conjugation action of G on the simple components of $\mathrm{Soc}(\overline{G})$); a (usually highly intransitive)

permutation representation of $\mathrm{Pker}(G)$ with kernel $\mathrm{Soc}^*(G)$; and, most importantly, for each of the simple components of $\mathrm{Soc}(\overline{G})$, a sequence of elements of G that generate the component modulo $\mathrm{Rad}(G)$ together with the images of these under an isomorphism with a standard version of a simple group. (The generators for each component S are actually generators for a perfect subgroup S^* of $\mathrm{Soc}^*(G)$ such that $(S^*/\mathrm{Rad}\,G)$ is the pre-image of S by the projection map $G \to G/\mathrm{Rad}(G)$.)

We compute a refinement of the sequence $1 \leq \mathrm{Rad}(G) \leq \mathrm{Soc}^*(G) \leq \mathrm{Pker}(G) \leq G$ between $\mathrm{Rad}(G)$ and $\mathrm{Soc}^*(G)$. To this end we notice that σ also permutes the simple components of $\mathrm{Soc}\,\overline{G}$. We take a σ-orbit of a single simple component S and we compute $S^{**} = \prod_T T^* \mathrm{Rad}(G)$, where the product is taken over the σ-orbit of S. Let r be the length of the orbit. Then σ^r acts as an automorphism on each member of the orbit. As the outer automorphism group of a finite simple group is of size bounded by a polynomial of the logarithm of the group size, we obtain that a polynomially small power of σ acts as an inner automorphism of $S^{**}/\mathrm{Rad}(G)$. If S is an alternating group, we use its natural permutation representation, while if S is sporadic, we use the regular representation of S. If S is of Lie type, we take the isomorphism between S and the standard copy of it computed by the algorithm of [2]. It realizes S as the quotient group of a matrix group by its center. We obtain a matrix representation of S by taking the conjugation action on the matrix algebra spanned by the elements of this covering group. We do the same for each T from the orbit (actually, these are isomorphic to S, so the construction made for S can be re-used.) Finally we obtain a matrix representation of S^{**} with kernel $\mathrm{Rad}(G)$ on the direct sum of these representations. Then we proceed with another orbit, construct the representation of the product of the orbit members and add to S^{**}. This way we obtain a chain of σ-invariant normal subgroups between $\mathrm{Rad}(G)$ and $\mathrm{Soc}^*(G)$ together with the matrix representations of the factors so that case (4) of Theorem 4 is applicable to them. For $G/\mathrm{Pker}(G)$, we use the permutation representation which can be naturally extended to a matrix representation. As σ also permutes the simple components, the induced automorphism will be conjugation by a permutation, so case (4) is again applicable. For $\mathrm{Pker}(G)/\mathrm{Soc}^* G$, we use the matrix representation as a labeling and, by solvability, case (3) is applicable. Finally, in $\mathrm{Rad}(G)$, again case (3) applies. □

Acknowledgements The research of the second author was supported by the Hungarian Ministry of Innovation and Technology NRDI Office within the framework of the Artificial Intelligence National Laboratory Program. The authors are grateful to the anonymous referees for their helpful remarks and suggestions.

Author Contributions These authors contributed equally to this work.

Funding Open access funding provided by Budapest University of Technology and Economics.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors have no Conflict of interest to declare.

References

1. Andrew M., van Dam W.: Quantum algorithms for algebraic problems. Rev. Mod. Phys. **82**, 1–52 (2008).
2. Babai L., Beals R., Seress Á.: Polynomial-time theory of matrix groups. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, STOC '09, pp. 55-64, New York, NY, USA (2009). Association for Computing Machinery.
3. Babai L., Beals R.: A polynomial-time theory of black box groups i. London Mathematical Society Lecture Note Series, pp. 30–64 (1999).
4. Babai L., Szemerédi E.: On the complexity of matrix group problems i. In: 25th Annual Symposium onFoundations of Computer Science, pp. 229–240. IEEE (1984).
5. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F.: A subexponential quantum algorithm for the semidirect discrete logarithm problem. In: NIST Fourth PQC Standardization Conference (2022).
6. Battarbee C., Kahrobaei D., Shahandashti S.F.: Cryptanalysis of semidirect product key exchange using matrices over non-commutative rings. *arXiv preprint* arXiv:2105.07692 (2021)
7. Battarbee C., Kahrobaei D., Shahandashti S.F.: Semidirect product key exchange: the state of play. *arXiv preprint*arXiv:2202.05178 (2022).
8. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F.: Spdh-sign: towards efficient, post-quantum group-based signatures. In: Johansson T., Smith-Tone D. (eds.) Post-Quantum Cryptography, pp. 113–138. Springer, Cham (2023).
9. Brown D.R.L., Koblitz N., LeGrow J.T.: Cryptanalysis of "make". J. Math. Cryptol. **16**(1), 98–102 (2022).
10. Castryck W., Lange T., Martindale C., Panny L., Renes J.: Csidh: an efficient post-quantum commutative group action. In: Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24, pp. 395–427. Springer (2018).
11. Childs A., Ivanyos G.: Quantum computation of discrete logarithms in semigroups. J. Math. Cryptol. **8**(4), 405–416 (2014).
12. Couveignes J.-M.: Hard homogeneous spaces. Cryptology ePrint Archive (2006).
13. Giesbrecht M.: Nearly optimal algorithms for canonical matrix forms. SIAM J. Comput. **24**(5), 948–969 (1995).
14. Grigoriev D., Shpilrain V.: Tropical cryptography. Commun. Algebra **42**(6), 2624–2632 (2014).
15. Habeeb M., Kahrobaei D., Koupparis C., Shpilrain V.: Public key exchange using semidirect product of (semi) groups. In: Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25–28, 2013. Proceedings 11, pp. 475–486. Springer (2013).
16. Harrison M.A.: Lectures on Linear Sequential Machines. Academic Press, New York (1969).
17. Isaac S., Kahrobaei D.: A closer look at the tropical cryptography. Int. J. Comput. Math. Comput. Syst. Theory **6**(2), 137–142 (2021).
18. Ivanyos G., Magniez F., Santha M.: Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. In: Proceedings of the Thirteenth Annual ACM Symposium on Parallel Algorithms and Architectures, pp. 263–270 (2001).
19. Kahrobaei D., Shpilrain V.: Using semidirect product of (semi) groups in public key cryptography. In: Pursuit of the Universal: 12th Conference on Computability in Europe, CiE 2016, Paris, France, June 27–July 1, 2016, Proceedings, pp. 132–141. Springer (2016).
20. Kannan R., Lipton R.J.: Polynomial-time algorithm for the orbit problem. J. ACM **33**(4), 808–821 (1986).
21. Kotov M., Ushakov A.: Analysis of a key exchange protocol based on tropical matrix algebra. J. Math. Cryptol. **12**(3), 137–141 (2018).
22. Kuperberg G.: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Comput. **35**(1), 170–188 (2005).
23. Myasnikov A., Roman'kov V.: A linear decomposition attack. Groups Complex. Cryptol. **7**(1), 81–94 (2015).
24. Rahman N., Shpilrain V.: Make: a matrix action key exchange. J. Math. Cryptol. **16**(1), 64–72 (2022).
25. Schwartz J.T.: Probabilistic algorithms for verification of polynomial identities. In: Ng Edward W. (ed.) Symbolic and Algebraic Computation, vol. 72, pp. 200–215. Lecture Notes in Computer Science. Springer, Berlin Heidelberg (1979).
26. Shor P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp.124–134. IEEE (1994).

27. Zippel R.: Probabilistic algorithms for sparse polynomials. In: Ng E.W. (ed.) Symbolic and Algebraic Computation, Volume 72 of LNCS, pp. 216–226. Springer, New York (1979).