IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 6, 2021, accepted June 8, 2021, date of publication June 28, 2021, date of current version July 6, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3092723

Quantum Algorithm for Solving the Continuous Hidden Symmetry Subgroup Problem

EUNOK BAE AND SOOJOON LEE
Department of Mathematics and the Research Institute for Basic Sciences, Kyung Hee University, Seoul 02447, South Korea

Corresponding authors: Eunok Bae (eobae@khu.ac.kr) and Soojoon Lee (level@khu.ac.kr)

This work was supported in part by the National Research Foundation of Korea grant through the Ministry of Science and ICT under Grant NRF-2019R1A2C1006337 and Grant NRF-2020M3E4A1079678. The work of Soojoon Lee was supported in part by the Ministry of Science and ICT, under the Information Technology Research Center Support Program supervised by the Institute for Information and Communications Technology Planning and Evaluation under Grant IITP-2021-2018-0-01402, and in part by the Quantum Information Science and Technologies Program of the National Research Foundation of Korea through the Ministry of Science and ICT under Grant NRF-2020M3H3A1105796.

This work did not involve human subjects or animals in its research.

ABSTRACT Quantum computers are expected to be able to outperform classical computers. In fact, some computational problems such as integer factorization can be solved on quantum computers substantially faster than classical computers. Interestingly, these problems can be cast in a framework of the hidden symmetry subgroup problem. However, only a few of quantum algorithms for efficiently solving this problem have been known, and the approaches used in all previous results can be applied to particular groups with specific group actions. In this paper, we introduce new technique for solving the hidden symmetry subgroup problem which can be applicable for any groups and any group actions with a certain condition. In addition, we define the continuous hidden symmetry subgroup problem on a group by employing a continuous oracle function, and prove that if the group is a metric space and the group action satisfies some condition, then the continuous hidden symmetry subgroup problem can be efficiently reduced to the continuous hidden subgroup problem. In particular, we show that there exists an efficient quantum algorithm to solve the continuous hidden symmetry subgroup problem on $\mathbb{R}^n$, while it has not yet been shown that the original hidden symmetry subgroup problem on $\mathbb{R}^n$ can be efficiently solved by a quantum computer.

INDEX TERMS Quantum algorithm, continuous hidden symmetry subgroup problem, hidden symmetry subgroup problem.

I. INTRODUCTION

A. BACKGROUND

Many researchers have been actively studying algebraic problems and algorithms to solve them which can achieve significant speed-up on quantum computers. Shor invented a polynomial time quantum algorithm for the integer factorization problem, while the best known classical algorithms take superpolynomial time [1]. Shor's factoring algorithm breaks the Rivest–Shamir–Adleman (RSA) public-key encryption [2] which is based on the hardness of factoring a large composite integers. Quantum computers can threaten various cryptosystems that have been broadly used until now like the RSA encryption [3]–[10]. In the last few years, there has been a growing interest in developing cryptography called the post-quantum cryptography (PQC) which is secure against quantum attacks. It is remarkable that the U. S. National Institute of Standards and Technology has been working on the PQC standardization for years even though there is no practical quantum computer yet.

Recently, there has been an increasing interest in research on continuous analogues of discrete algebraic problems, and some results are closely related to cryptography. In the continuous version of the hidden subgroup problem (HSP) over $\mathbb{R}^n$ proposed in [6], it was shown that there is an efficient quantum algorithm for solving the continuous HSP over $\mathbb{R}^n$. Moreover, this algorithm can also be used for attacking certain cryptosystem based on the hardness to find short vectors in ideal lattices, which is not obtainable from the original HSP on $\mathbb{R}^n$ with fixed n [7]. The continuous version of the hidden shift problem over $\mathbb{R}^n$ was studied in [11], and the continuous analogue of the Learning with Errors problem was

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

also introduced most recently, and it can be seen as breaking new ground in quantum attacks on lattice problems [12]. Therefore, we can say that the continuous version with a continuous oracle function makes the original problem more meaningful.

B. RELATED WORKS AND OUR CONTRIBUTION

In addition to the cryptographic issues, most algebraic problems which can be solved more efficiently on quantum computers can fit into a framework of the hidden symmetry subgroup problem (HSSP) [13]. The HSSP can be described as follows. Let G be a finite group and the binary function

$$\circ : G \times X \to X \tag{1}$$

be a group action of G on a finite set X, and $\mathcal{H}$ be a family of closed subgroups of G. For some $H \in \mathcal{H}$ and a finite set S, we say that an oracle function $f : X \to S$ hides H by symmetries if

$$f(x) = f(y) \iff H \circ x = H \circ y, \tag{2}$$

where

$$H \circ x = \{h \circ x : h \in H\}. \tag{3}$$

Note that the integer factorization problem and the discrete logarithm problem can be considered as the HSSP when $G = X = \mathbb{Z}_N$ and $G = X = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$, respectively, and the group actions are the group operations.

Although it is important to solve the HSSP, there have been only a few of known results for the HSSP. Decker textit *et al.* [13] showed that there is an efficient quantum algorithm for solving the HSSP for Frobenius groups by employing the reduction scheme from the HSSP to the HSP in which the level sets of the oracle function from G to some finite set S' correspond to the cosets of some unknown subgroup H. Also, Kim *et al.* dealt with the HSSP on semi-direct product of cyclic groups, $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, with certain constraints [14]. In addition, we note that all known results on the HSSP have focused on discrete groups.

The methods used in all previous results are only applicable to specific groups with particular group actions. These restrictions may have caused some additional constraints in the reduction scheme from the HSSP to the HSP. On the other hand, our new technique to deal with the HSSP can be applied to any groups and any group actions except that the group action satisfies a certain condition, and it allows us to have very simple and more efficient reduction scheme from the HSSP to the HSP as we will show in Section II. We also prove that the similar approach can be employed to the continuous HSSP that we newly define in Section III.

In this paper, we also present the continuous version of the HSSP on a group by using a continuous oracle function. In order to construct a continuous version of an algebraic problem, we may simply think of substituting discrete groups with continuum groups in the definition of the problem. However, it can be more productive and more meaningful if we should add the continuity of the oracle function to the definition. For instance, Hallgren [3] presented a quantum algorithm for solving the HSP over $\mathbb{R}^n$ by replacing the continuum group $\mathbb{R}^n$ with its discretized set, and it has been known that the rounding error is tolerable when n is fixed, but the error is worsened in higher dimensions [4], [5]. However, the continuous HSP over $\mathbb{R}^n$ using the continuous oracle function gave aid to resolve this difficulty [6].

Furthermore, we newly define the continuous HSP on a group which is also a metric space, and we prove that the continuous HSSP is efficiently reducible to the continuous HSP by utilizing our new reduction technique. In addition, we show that there exists an quantum algorithm to solve the problem in time polynomial in n by applying the reduction scheme to the continuous HSP on $\mathbb{R}^n$. As we have seen in the above example, we expect that quantum algorithms for solving the continuous version of the original problem may have better potential applications.

This paper is organized as follows. In Section II, we present a new approach to make the reduction from the HSSP to the HSP simpler and more efficient. In Section III, we introduce the definition of the continuous HSSP over a group which is a generalization of the original HSSP, and show that the new approach is also applicable for the continuous HSSP. In Section IV, as one of our main results, we prove that there exists an efficient quantum algorithm to solve the continuous HSSP on $\mathbb{R}^n$ by reducing it to the continuous HSP over the same group. Finally, we summarize our results and discuss the results and plans for future work in Section V.

II. NEW APPROACH FOR SOLVING THE HIDDEN SYMMETRY SUBGROUP PROBLEM

Let G be a group with the identity element e and X be a set. A group action $\circ$ of G on X is a map $\circ : G \times X \to X$ defined as $(a, x) \mapsto a \circ x$ which satisfies

$$a \circ (b \circ x) = (ab) \circ x \tag{4}$$

and $e \circ x = x$ for any $a, b \in G$ and $x \in X$. For a subset $Y \subseteq X$, we denote

$$a \circ Y = \{a \circ y : y \in Y\}. \tag{5}$$

For each $x \in X$,

$$G_x = \{a \in G : a \circ x = x\} \tag{6}$$

is called the *stabilizer* subgroup of G with respect to x. The *H-orbit* of x is defined as

$$H \circ x = \{h \circ x : h \in H\}. \tag{7}$$

Then it is easy to show that the set of the H-orbits

$$H^* = \{H \circ x : x \in X\} \tag{8}$$

forms a partition of X. On the other hand, if $\pi = \{\pi_i\}$ is a partition of X, we define *the group of symmetries* of π as

$$\pi^* = \{a \in G : a \circ \pi_i = \pi_i \text{ for all } i\} \tag{9}$$

which is a subgroup of G. The subgroup

$$H^{**} = \{a \in G : a \circ (H \circ x) = H \circ x \ \forall x \in X\} \tag{10}$$

is called the *closure* of H, and the partition

$$\pi^{**} = \{\pi^* \circ x : x \in X\} \tag{11}$$

is called the closure of π [15]. It is clear to show that H is a subgroup of H^{**}, and π is finer than π^{**}. We say that the subgroup H is closed if

$$H = H^{**}. \tag{12}$$

In a similar way, π is said to be closed if

$$\pi = \pi^{**}. \tag{13}$$

Note that if the group action $\circ$ of G on X satisfies the condition, "For an arbitrary $x \in X$,

$$a \circ x = b \circ x \iff a = b \tag{14}$$

for all $a, b \in G$," then any subgroup H of G is closed. Indeed, for a subgroup H of G, since the closure of H is defined as in Eq. (10), it is always true that $H \subseteq H^{**}$. Conversely, if $a \in H^{**}$, then for each $x \in X$,

$$a \circ (h_1 \circ x) = h_2 \circ x \tag{15}$$

for some $h_1, h_2 \in H$. It follows from Eq. (14) that

$$ah_1 = h_2, \tag{16}$$

or equivalently,

$$a = h_2 h_1^{-1} \in H. \tag{17}$$

Thus, we have $H^{**} = H$.

Now, let us assume that the group action $\circ$ of G on X satisfies the condition in Eq. (14). Then we can prove that the HSSP can be reduced to the HSP more simply and efficiently than the original reduction scheme presented in [13].

Let f be an oracle function of the HSSP on G which hides a subgroup H of G by symmetries with a group action $\circ : G \times X \to X$ satisfying Eq. (14) and let us construct a new function $f_{\mathrm{HSP}} : G \to S$ as

$$|f_{\mathrm{HSP}}(a)\rangle = |f(a \circ x)\rangle$$

for any fixed $x \in X$. Then we can show that the function f_{HSP} hides the subgroup H by employing the following lemmas.

Lemma 1: Let $\circ$ be a group action of a group G on a set X satisfying the condition in Eq. (14). For each $x \in X$, the stabilizer subgroup G_x is trivial.

Proof: Observe that for each $x \in X$

$$\begin{aligned} G_x &= \{a \in G : a \circ x = x\} \\ &= \{a \in G : a \circ x = e \circ x\} \\ &= \{e\}, \end{aligned}$$

where the last equality follows from Eq. (14). □

From Lemma 1, it is easy to show that the function f_{HSP} hides the subgroup H.

Lemma 2: Let $\circ$ be a group action of a group G on a set X satisfying the condition in Eq. (14). Then for all $a, b \in G$,

$$f_{\mathrm{HSP}}(a) = f_{\mathrm{HSP}}(b) \iff a \in Hb. \tag{18}$$

Proof: Suppose that

$$f_{\mathrm{HSP}}(a) = f_{\mathrm{HSP}}(b) \tag{19}$$

for $a, b \in G$. By definition of the function f_{HSP}, it implies that

$$f(a \circ x) = f(b \circ x). \tag{20}$$

Since the oracle function f of the HSSP hides the subgroup H by symmetries,

$$H \circ (a \circ x) = H \circ (b \circ x). \tag{21}$$

So, for some $h_1, h_2 \in H$, we have

$$h_1 a \circ x = h_2 b \circ x, \tag{22}$$

which implies that

$$a = h_1^{-1} h_2 b \in Hb \tag{23}$$

because the only element of G which fixes x is e by Lemma 1. Conversely, suppose that $a \in Hb$. Then we have

$$a = hb \tag{24}$$

for some $h \in H$, and so

$$a \circ x = h \circ (b \circ x), \tag{25}$$

which implies that

$$f_{\mathrm{HSP}}(a) = f(a \circ x) = f(b \circ x) = f_{\mathrm{HSP}}(b) \tag{26}$$

since f hides the subgroup H by symmetries. □

It follows from Lemma 2 that the HSSP is efficiently reducible to the HSP for a randomly chosen $x \in X$ if we can compute the group action $\circ$ efficiently. Furthermore, we show that this new approach can be also applicable for a continuous version of the HSSP if we assume a certain condition of the group action on a metric space with respect to the metric. The details are presented in the next section.

III. CONTINUOUS HIDDEN SYMMETRY SUBGROUP PROBLEM

In this section, we present the definitions of the continuous HSSP on a group and the continuous HSP on a group which is also a metric space. By employing the same approach in the previous section, we show that the continuous HSSP can be reduce to the continuous HSP efficiently when the group action satisfies a similar condition with Eq. (14).

First, let us present the definition of the continuous HSSP on a group G as follows.

Definition 3 (The continuous HSSP): Let $\circ : G \times M \to M$ be a group action of a group G on a metric space M with metric d_M, and $\mathcal{H}$ be a family of closed subgroups of G. Let S be a set of unit vectors in a Hilbert space, and suppose that a function $f : M \to S$ is defined as $x \mapsto |f(x)\rangle$ for a pure state

$|f(x)\rangle$ in S, and the function f with positive real parameters (α, r, ϵ) satisfies the following properties for some $H \in \mathcal{H}$.

1) *For all $x, y \in M$,*

$$f(x) = f(y) \iff H \circ x = H \circ y \tag{27}$$
$$\iff x \in H \circ y. \tag{28}$$

2) (Lipschitz) *There exists $\alpha > 0$ such that*

$$\| |f(x)\rangle - |f(y)\rangle \| \leq \alpha \cdot d_M(x, y) \tag{29}$$

for all $x, y \in M$, where $\|\cdot\|$ is the norm naturally induced by the inner product in the Hilbert space. A function f satisfying the inequality (29) is called Lipschitz with Lipschitz constant α.

3) (Pseudo-injective) *If*

$$\inf_{h \in H} d_M(x, h \circ y) \geq r, \tag{30}$$

then

$$|\langle f(x) | f(y) \rangle| \leq \epsilon. \tag{31}$$

Then we say that f continuously hides the subgroup H by symmetries. Given such a function f, the continuous HSSP on G is to find H.

Note that the Lipschitz condition says if the inputs x and y are closed enough then the output states of them are closed as well. From the pseudo-injectivity, we can see that if the input x is far from the H-orbit of y, $H \circ y$, then the output states of x and y are almost orthogonal.

The oracle function of the original HSSP can only discriminate whether the H-orbits of the inputs are same or different. On the other hand, the oracle function of the continuous HSSP gives more information from its continuous HSSP properties such as whether the H-orbits of the inputs are close enough or far away. However, we note that if d_M is the discrete metric on M, $0 < r < 1$, and $0 < \epsilon < 1$, then the continuous HSSP is essentially equivalent to the original HSSP. This implies that the continuous HSSP can be considered as a generalization of the original HSSP.

Remark that if the group G in Definition 3 is also a metric space with metric d_G, and the group action $\circ$ of G on M satisfies the following property

$$d_M(a \circ x, b \circ x) = d_G(a, b) \tag{32}$$

for $a, b \in G$ and $x \in M$, then any subgroup of G is closed since Eq. (32) implies Eq. (14).

Now, we define the continuous HSP on a group which is also a metric space, and then present a reduction scheme from the continuous HSSP to the continuous HSP.

Definition 4 (The continuous HSP): Let G be a group and a metric space with a metric d_G, $\mathcal{H}$ be a family of subgroups of G, and S be a set of unit vectors in a Hilbert space. Assume that an oracle function $f : G \to S$ with positive real parameters (α, r, ϵ) hides a subgroup $H \in \mathcal{H}$ in the following way.

1) *For all $a, b \in G$,*

$$f(a) = f(b) \iff Ha = Hb \tag{33}$$
$$\iff a \in Hb. \tag{34}$$

2) (Lipschitz) *For all $a, b \in G$,*

$$\| |f(a)\rangle - |f(b)\rangle \| \leq \alpha \cdot d_G(a, b). \tag{35}$$

3) (Pseudo-injective) *If*

$$\inf_{h \in H} d_G(a, hb) \geq r, \tag{36}$$

then

$$|\langle f(a) | f(b) \rangle| \leq \epsilon. \tag{37}$$

A function f satisfying the above conditional statement is said to be pseudo-injective with respect to parameters (r, ϵ).

The continuous HSP on G is to find H when such an oracle function f is given.

We remark that the continuous HSSP on G can be regarded as a generalization of the continuous HSP on G which is the case in which the group acts on itself and the group action is defined as the group operation, and also remark that if d_G is the discrete metric on G, then the continuous HSP is essentially equivalent to the original HSP when $0 < r < 1$ and $0 < \epsilon < 1$, as in the continuous HSSP. In addition, the basic idea of the reduction scheme comes from the method proposed in the previous section.

Let f be an oracle function with parameters (α, r, ϵ) of the continuous HSSP on G with a group action $\circ : G \times M \to M$ in Definition 3, and let us construct a new function $f_{\mathrm{cHSP}} : G \to S$ as

$$|f_{\mathrm{cHSP}}(a)\rangle = |f(a \circ z)\rangle \tag{38}$$

for any fixed $z \in M$. Then we can show that the function f_{cHSP} satisfies the continuous HSP properties in Definition 4 when the group action satisfies Eq. (32) by employing the following lemmas. Since Eq. (32) implies Eq. (14), we immediately obtain the following two lemmas from Lemma 1 and Lemma 2.

Lemma 5: Let G and M be metric spaces with metric d_G and d_M, respectively, and assume that G is a group. Let $\circ$ be a group action of G on M satisfying Eq. (32). For any $z \in M$, the stabilizer subgroup G_z is trivial.

From Lemma 5, it is easy to show that the function f_{cHSP} satisfies the first condition of the continuous HSP properties in Definition 4.

Lemma 6: Let $\circ$ be a group action of G on M satisfying Eq. (32). Then for all $a, b \in G$,

$$f_{\mathrm{cHSP}}(a) = f_{\mathrm{cHSP}}(b) \iff a \in Hb. \tag{39}$$

Now, we prove that the function f_{cHSP} is Lipschitz and pseudo-injective under the assumption of the group action $\circ$ in Eq. (32).

Lemma 7: Let $\circ$ be a group action of G on M satisfying Eq. (32), and assume that f satisfies the inequality (29)

with Lipschitz constant α. Then the function f_{cHSP} becomes a Lipschitz function with Lipschitz constant α in the continuous HSP.

Proof: In order to check the Lipschitz condition of f_{cHSP}, we observe that

$$\begin{aligned} \| \, |f_{\mathrm{cHSP}}(a)\rangle - |f_{\mathrm{cHSP}}(b)\rangle \, \| &= \| |f(a \circ z)\rangle - |f(b \circ z)\rangle \| \\ &\leq \alpha \cdot d_M(a \circ z, b \circ z) \\ &= \alpha \cdot d_G(a, b). \end{aligned} \tag{40}$$

The inequality (40) is due to the Lipschitz condition of f in (29) and the equality (32). So, the oracle function f_{cHSP} is a Lipschitz function with Lipschitz constant α. □

Lemma 8: Let $\circ$ be a group action of G on M satisfying Eq. (32). Then the function f_{cHSP} is pseudo-injective with parameters (r, ϵ) in the continuous HSP.

Proof: For the last condition of the continuous HSP, suppose that

$$\inf_{h \in H} d_G(a, hb) \geq r \tag{41}$$

for $a, b \in G$. Then

$$\inf_{h \in H} d_M(a \circ z, h \circ (b \circ z)) \geq r \tag{42}$$

since the group action $\circ$ satisfies Eq. (32). From the third condition of f in Definition 3, we have

$$|\langle f(a \circ z) | f(b \circ z)\rangle| \leq \epsilon. \tag{43}$$

Hence, we immediately obtain

$$|\langle f_{cHSP}(a) | f_{cHSP}(b)\rangle| \leq \epsilon \tag{44}$$

by the definition of f_{cHSP}. □

Combining the above lemmas, it can clearly be obtained that the function f_{cHSP} has parameters (α, r, ϵ) which are the same as those in the definition of the continuous HSSP, and f_{cHSP} hides the subgroup $H \in \mathcal{H}$, when the group action $\circ$ satisfies Eq. (32). Since all subgroups of G are closed in this case, we have one of our main theorems as follows.

Theorem 9: If the group action $\circ$ of G on a metric space M satisfying Eq. (32) is computable in polynomial time, then the continuous HSSP on G can be reduced to the continuous HSP on G in polynomial time.

Proof: Let $z \in M$ be chosen randomly, and assume that the group action $\circ$ of G satisfies Eq. (32), and it can be computed efficiently. Then all subgroups of G are closed. Furthermore, by Lemma 6, Lemma 7, and Lemma 8, we can efficiently construct the instances of the continuous HSP on G from ones of the continuous HSSP on G. Thus, the continuous HSSP on G is directly reducible to the continuous HSP on G. □

From Theorem 9, we conclude that if there exists an efficient quantum algorithm which can solve the continuous HSP on G, then the continuous HSSP on G can also be solved efficiently by a quantum computer, when the group action in the continuous HSSP satisfies Eq. (32). Thus, the quantum algorithm for solving the continuous HSSP can be described as follows.

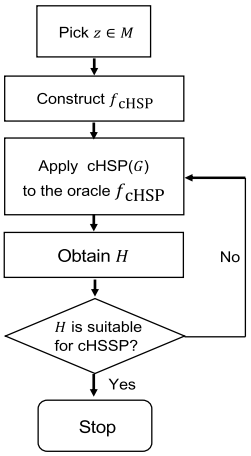

FIGURE 1. Flowchart of the algorithm for the continuous HSSP.

Algorithm 10 (Continuous HSSP on G):

Input*: The group action $\circ : G \times M \to M$ satisfying Eq. (32) and the oracle function $f : M \to S$ with positive real parameters (α, r, ϵ) that hides the subgroup H of G by symmetries.*

1) *Pick an element z from M randomly.*
2) *Construct f_{cHSP} with f and z.*
3) *Perform the quantum algorithm for the continuous HSP on G to the oracle function f_{cHSP}.*
4) *Obtain the subgroup H.*

Output*: The subgroup H.*

The flowchart of the algorithm for the continuous HSSP on G is presented in Figure 1, where the quantum algorithm for solving the continuous HSP on G is denoted by cHSP(G) and cHSSP means the continuous HSSP.

Corollary 11: If cHSP(G) can solve the continuous HSP on G in time polynomial in t for some parameter t related to the group G, then Algorithm 10 solves the continuous HSSP on G in time polynomial in t.

Proof: Assume that cHSP(G) solves the continuous HSP on a group G in time $P(t)$ for some nonzero polynomial P and some parameter t with respect to G. For a randomly selected element $z \in M$, as defined in Eq. (38), the new function f_{cHSP} can be constructed from the oracle function f of the continuous HSSP in time $Q(t)$ for some nonzero polynomial Q. By Theorem 9, f_{cHSP} is essentially an instance of the continuous HSP on G, and hence it can solve the continuous HSP on G in time $P(t)$. Therefore, by applying Algorithm 10, the subgroup hidden by symmetries can be found in time polynomial in t, that is, $P(t) + Q(t)$. □

As an example, we can prove that the continuous HSSP on the additive group $\mathbb{R}^n$ with the group action satisfying Eq. (32) can be solved by a quantum computer in time polynomial in n by means of this reduction scheme. See the next section for details.

IV. CONTINUOUS HIDDEN SYMMETRY SUBGROUP PROBLEM ON $\mathbb{R}^n$

In this section, we take into account the continuous HSSP on the additive group $\mathbb{R}^n$ with some conditions, and prove that there exists a polynomial-time quantum algorithm for solving the problem.

In order to proceed with our work, we assume that G is the additive group $\mathbb{R}^n$ which is a metric space with the usual metric, and $\mathcal{H}$ is the family of all full-rank lattices L with $\lambda(L) \geq \lambda$ and $d(L) \leq d$ for some fixed positive number λ and d, where $\lambda(L)$ is the length of the shortest vector and $d(L)$ is the unit cell volume. Then the definition of the continuous HSP on G in Definition 4 is exactly the same as that of the continuous HSP on $\mathbb{R}^n$ which has already been presented in [6].

Note that there exists a quantum algorithm to solve the continuous HSP on $\mathbb{R}^n$ in time polynomial in n [6]. From Theorem 9, we can have the following theorem.

Theorem 12: Let $\circ$ be a group action of the additive group $\mathbb{R}^n$ on a metric space M satisfying Eq. (32), and assume that the group action $\circ$ is computable in time polynomial in n. Then there exists a quantum algorithm for solving the continuous HSSP on $\mathbb{R}^n$ in time polynomial in n.

Proof: Assume that the group action $\circ$ of $\mathbb{R}^n$ on a metric space M satisfies Eq. (32), and the group action $\circ$ is computable in time polynomial in n. Then we can construct the oracle function of the continuous HSP on $\mathbb{R}^n$ by Theorem 9. Since the continuous HSP on $\mathbb{R}^n$ can be solved in time polynomial in n [6], we can also solve the continuous HSSP on $\mathbb{R}^n$ by applying Algorithm 10 to the group $\mathbb{R}^n$. □

Remark 13: In [6], the hidden full rank lattice L in $\mathbb{R}^n$ can be found by using $n^2 + cn$ samples selected from the probability distribution q_u with the probability of success at least

$$\left(1 - \frac{n}{2^n}\right)\left(1 - \frac{\log(R^n d(L))}{2^n}\right),$$

where $R = \Omega(\alpha)$, $d(L)$ is the unit cell volume of the lattice L, and $c = \lceil \log(R^n d(L)) \rceil$. Thus, it follows from Corollary 11 that the continuous HSSP on $\mathbb{R}^n$ can be solved in time polynomial in n.

V. CONCLUSION

Although the framework of the HSSP can importantly be related to various cryptosystems, there have been only a few of known results for the HSSP. Furthermore, it is more meaningful to consider the continuous version of the HSSP since it may be able to attack some cryptosystems that the discrete version of the problem cannot break.

So, in this paper, we have presented the definitions of the continuous HSSP on a group and the continuous HSP on a group which is also a metric space using the continuous oracle functions, and have observed that the continuous HSSP is a generalization of the original HSSP. The continuous HSSP can also be regarded as a generalization of the continuous HSP where the group acts on itself and the group operation corresponds to the group action. In addition, we have proved that the continuous HSSP on a group which is a metric space can be reduced efficiently to the continuous HSP when the group action $\circ$ has a certain condition.

Moreover, as a special case of the continuous HSSP, we have introduced the continuous HSSP on the additive group $\mathbb{R}^n$ which is an extended definition of the HSSP on discrete groups to the continuum group $\mathbb{R}^n$. By using our new reduction technique, we have shown that there is an efficient quantum algorithm to solve the continuous HSSP on $\mathbb{R}^n$.

Remark that we have not yet obtained an algorithm to solve the HSSP on $\mathbb{R}^n$ in time polynomial in n without the continuity of the oracle function. Indeed, if we consider the HSSP on $\mathbb{R}^n$ with only the condition in Eq. (27) in Definition 3, we would use the similar reduction to the HSP on $\mathbb{R}^n$ which was presented in [3]. In that case, the success probability of the HSP subroutines for $\mathbb{R}^n$ is at least

$$\left(\frac{N - 2nm}{N}\right)^n \frac{N(N - 4nm)}{(N + 4nm)(N - 2nm)}, \tag{45}$$

where N is a sufficiently large constant and m is the length of the longest basis vector in some reduced basis of the hidden lattice L. Since the probability approaches zero as n tends to the infinity, it is not guaranteed that the HSP subroutines can be successful for an arbitrary natural number n. However, in our case, the success probability for the continuous HSP subroutines for $\mathbb{R}^n$ is bounded by a positive constant which is independent on n as we can see in [6]. It follows that the continuous HSSP on $\mathbb{R}^n$ can be efficiently solved.

For the next step, we can try to apply the same reduction scheme from the continuous HSSP to the continuous HSP when using a different group action of a given group or another oracle function with some properties such as continuity. Furthermore, we can investigate whether there exists an efficient algorithm for solving the continuous HSSP or the continuous HSP over any groups other than $\mathbb{R}^n$ which are also metric spaces.

On the other hand, we can also try to consider a continuous version of other algebraic problems with hidden structures such as hidden polynomial problem and hidden polynomial graph problem, and investigate relations between the continuous versions of these problems and the continuous HSSP.

REFERENCES

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

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[3] S. Hallgren, "Fast quantum algorithms for computing the unit group and class group of a number field," in *Proc. 37th Annu. ACM Symp. Theory Comput. (STOC)*, 2005, pp. 468–474.

[4] A. Schmidt and U. Vollmer, "Polynomial time quantum algorithm for the computation of the unit group of a number field," in *Proc. 37th Annu. ACM Symp. Theory Comput. (STOC)*, 2005, pp. 475–480.

[5] S. Hallgren, "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem," *J. ACM*, vol. 54, no. 1, pp. 1–19, Mar. 2007.

[6] K. Eisenträger, S. Hallgren, A. Kitaev, and F. Song, "A quantum algorithm for computing the unit group of an arbitrary degree number field," in *Proc. 46th Annu. ACM Symp. Theory Comput. (STOC)*, May 2014, pp. 293–302.
[7] J.-F. Biasse and F. Song, "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields," in *Proc. 27th Annu. ACM-SIAM Symp. Discrete Algorithms (SODA)*, 2016, pp. 893–902.
[8] X. Bonnetain and M. Naya-Plasencia, "Hidden shift quantum cryptanalysis and implications," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, in Lecture Notes in Computer Science, vol. 11272, 2018, pp. 560–592.
[9] X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, and A. Schrottenloher, "Quantum attacks without superposition queries: The offline Simon's algorithm," in *Advances in Cryptology—ASIACRYPT 2019*, vol. 11921. Cham, Switzerland: Springer, 2019.
[10] J. Cui, J. Guo, and S. Ding, "Applications of Simon's algorithm in quantum attacks on feistel variants," *Quantum Inf. Process.*, vol. 20, Mar. 2021, Art. no. 117.
[11] D. Boneh and R. J. Lipton, "Quantum cryptanalysis of hidden linear forms," in *Proc. Crypto*, in Lecture Notes in Computer Science, vol. 963, 1995, pp. 424–437.
[12] J. Bruna, O. Regev, M. J. Song, and Y. Tang, "Continuous LWE," in *Proc. 53rd Annu. ACM-SIGACT Symp. Theory Comput. (STOC)*, 2021, pp. 694–707.
[13] T. Decker, G. Ivanyos, M. Santha, and P. Wocjan, "Hidden symmetry subgroup problems," *SIAM J. Comput.*, vol. 42, no. 5, pp. 1987–2007, 2013.
[14] J. San Kim, E. Bae, and S. Lee, "Quantum computational algorithm for hidden symmetry subgroup problems on semi-direct product of cyclic groups," 2013, *arXiv:1307.1183*. [Online]. Available: http://arxiv.org/abs/1307.1183
[15] T. S. Blyth, *Lattices and Ordered Algebraic Structures*. London, U.K.: Springer, 2005.

EUNOK BAE received the B.S. degree in mathematics from Kyung Hee University, in 2009, where she is currently pursuing the Ph.D. degree with the Department of Mathematics, under the supervision of Prof. Soojoon Lee, with a focus on quantum computational algorithms.

From August 2013 to August 2014, she was a Visiting Scholar with the Institute for Quantum Science and Technology, University of Calgary, Canada, and also with the Department of Computer Science and Engineering, Texas A&M University, College Station, TX, USA, as a Visiting Scholar, from September 2019 to February 2020. Her research interests include quantum algorithms, post-quantum cryptography, and quantum complexity theory.

SOOJOON LEE received the Ph.D. degree from the Department of Mathematical Sciences, Seoul National University, in 2002, with a focus on quantum computational algorithms. He joined the Department of Mathematics, Kyung Hee University, in 2004, after postdoctoral positions with the Statistical Research Center for Complex Systems, Seoul National University and the School of Computational Sciences, Korea Institute for Advanced Study (KIAS). He is currently a Professor of mathematics with Kyung Hee University and an Associate Member with KIAS. His research interests include quantum algorithms and quantum information theory including quantum communication and entanglement theory.