Quantum Measurements for Hidden Subgroup Problems with Optimal Sample Complexity

Masahito Hayashi
ERATO-SORST Quantum Computation and Information Project,
Japan Science and Technology Agency,
5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
Graduate School of Information Sciences, Tohoku University,
Aoba-ku, Sendai 980-8579, Japan
Akinori Kawachi
Department of Mathematical and Computing Sciences, Tokyo Institute of Technology
2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan
Hirotada Kobayashi
Principles of Informatics Research Division, National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

February 15, 2008

Abstract

One of the central issues in the hidden subgroup problem is to bound the sample complexity, i.e., the number of identical samples of coset states sufficient and necessary to solve the problem. In this paper, we present general bounds for the sample complexity of the identification and decision versions of the hidden subgroup problem. As a consequence of the bounds, we show that the sample complexity for both of the decision and identification versions is \( \Theta(\log |\mathcal{H}|/\log p) \) for a candidate set \( \mathcal{H} \) of hidden subgroups in the case where the candidate nontrivial subgroups have the same prime order \( p \), which implies that the decision version is at least as hard as the identification version in this case. In particular, it does so for the important cases such as the dihedral and the symmetric hidden subgroup problems. Moreover, the upper bound of the identification is attained by a variant of the pretty good measurement. This implies that the concept of the pretty good measurement is quite useful for identification of hidden subgroups over an arbitrary group with optimal sample complexity.

1 Introduction

1.1 Background

The hidden subgroup problem is one of the central issues in quantum computation, which was introduced for revealing the structure behind exponential speedups in quantum computation [36].

Definition 1.1 (Hidden Subgroup Problem (HSP)) Let \( G \) be a finite group. For a hidden subgroup \( H \leq G \), we define a map \( f_H \) from \( G \) to a finite set \( S \) with the property that \( f_H(g) = f_H(gh) \) if and only if \( h \in H \). Given \( f_H : G \to S \) and a generator set of \( G \), the hidden subgroup problem (HSP) is the problem of finding a set of generators for the hidden subgroup \( H \). We say that HSP over \( G \) is efficiently solvable if we can construct an algorithm in time polynomial in \( \log |G| \).
The nature of many existing quantum algorithms relies on efficient solutions to Abelian HSPs (i.e., HSPs over Abelian groups) [45, 30, 6, 7]. In particular, the celebrated quantum algorithms due to Shor [44] for factoring and discrete logarithm essentially consist of reductions to certain Abelian HSPs and efficient solutions to the Abelian HSPs. Besides his results, many efficient quantum algorithms for important number-theoretic problems (e.g., Pell’s equation [16] and unit group of a number field [17, 41]) were based on solutions to Abelian HSPs.

Recently, non-Abelian HSPs have also received much attention. It is well known that the graph isomorphism problem can be reduced to the HSP over the symmetric group [6, 3] (more strictly, the HSP over $S_n \ltimes S_2$ [9]). Regev showed that an efficient solution to HSP over the dihedral group under certain conditions leads to an efficient quantum algorithm for the unique shortest vector problem [39]. While the efficient quantum algorithm for general Abelian HSPs has been already given [30, 36], the non-Abelian HSPs are extremely harder than the Abelian ones. There actually exist efficient quantum algorithms for HSPs over several special classes of non-Abelian groups [40, 12, 19, 13, 15, 25, 26, 32, 2]. Nonetheless, most of important cases of non-Abelian HSPs, including the dihedral and symmetric HSPs, are not known to have efficient solutions. Thus, finding efficient algorithms for non-Abelian HSPs is one of the most challenging issues in quantum computation.

The main approach to the non-Abelian HSPs is based on a generic framework called the standard method. To our best knowledge, all the existing quantum algorithms for HSPs essentially contain this framework. The standard method essentially reduces HSPs to the quantum state identification [43] for the so-called coset states, which contain information of the hidden subgroup.

**Definition 1.2 (Coset State and Standard Method)** Let $G$ be any finite group and $H$ be the hidden subgroup of $G$. We then define the coset state $\rho_H$ for $H$ as $\rho_H = \frac{1}{|H|} \sum_{g \in G} |gH\rangle \langle gH|$, where $|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$.

**Standard Method with $k$ Coset States**

1. Prepare two registers with a uniform superposition over $G$ in the first register and all zeros in the second register: $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle$.
2. Compute $f_H(g)$ and store the result to the second register: $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f_H(g)\rangle$.
3. Discard the second register to obtain a coset state: $\frac{|H|}{|G|} \sum_{g \in G/H} |gH\rangle \langle gH|$.
4. Repeat (1)-(3) $k$ times and then apply a quantum measurement to $k$ samples of $\rho_H$.

Thus the main task for solving HSP based on the standard method is to find an efficiently implementable quantum measurement extracting the information of the hidden subgroup from identical samples of the coset state.

Many researchers have broadly studied hard instances of non-Abelian HSPs from positive and negative aspects based on the standard method. In particular, they have focused on the sample complexity of HSPs, i.e., how many coset states are sufficient and necessary to identify the hidden subgroup with a constant success probability.

In several classes of the non-Abelian HSPs for which efficient algorithms are unknown, it is shown that we can identify any hidden subgroup by (possibly inefficient) classical post-processes using the classical information obtained by the quantum Fourier transforms applied to polynomially many samples of the coset state [10, 19, 15, 32].

Bacon, Childs and van Dam demonstrated that the so-called pretty good measurement (PGM, also known as the square root measurement or least squares measurement [21]) is optimal for identifying the coset state in view of the sample complexity on a class of semidirect product groups $A \rtimes \mathbb{Z}_p$, including the dihedral group, where $A$ is any Abelian group and $p$ is a prime [2]. They proved that the sample complexity is $\Theta(|A|/\log p)$ to identify the hidden subgroup by the PGM from the candidate set $\mathcal{H}_{SDP} = \{(a, 1) \in A \times \mathbb{Z}_p : a \in A\}$. Moore and Russell generalized their result to prove the optimality of the PGM for a wider class of HSPs [33]. They actually gave the PGM for identifying coset states of hidden conjugates of a subgroup, i.e., hidden subgroups of the form $g^{-1} H g$ for a fixed non-normal subgroup $H$ of a finite group $G$ and $g \in G$. These results of [2, 33] showed that the PGMs succeed for a wide class of HSPs with at most $O(\log |\mathcal{H}|)$ samples for the candidate set $\mathcal{H}$ of hidden subgroups. For a more general case, Ettinger, Hoyer and Knill gave a quantum measurement.
that solves HSP over any finite group $G$ with $O(\log |H|)$ samples of coset states in [11]. They also constructed an error-free measurement, which slightly departs from the framework of the standard method, for the general HSP with $O(\log^2 |\mathcal{H}|)$ queries in [11] by the amplitude amplification technique [8].

These quantum measurements ignore the time complexity issue in general. However, they may lead to efficient quantum algorithms for HSPs. Bacon, Childs, and van Dam actually gave efficient implementation of the PGM for identifying the coset state on a class of the semidirect groups including the Heisenberg group [2], i.e., they constructed an efficient quantum algorithm for the HSPs from the corresponding PGMs. Hence, to give the quantum measurements for identification of the coset state like PGMs may play important roles towards the construction of efficient quantum algorithms for HSPs.

The negative results of the standard method has also been studied from an information-theoretic viewpoint, which are based on a decision version of the HSP defined as the problem of deciding whether the hidden subgroup is trivial or not. In particular, the difficulty of the HSP over the symmetric group $\text{Sym}_n$ has been shown by a number of results for this decision version [19, 15, 29, 35, 34]. Hallgren, Moore, Rötteler, Russell, and Sen recently proved that a joint measurement across multiple samples of coset states is essentially required to solve a decision version over the symmetric group, which is deeply related to the graph isomorphism problem [18]. More precisely, they showed that joint quantum measurements across $\Omega(n \log n)$ samples of coset states are necessary to decide whether the given samples are generated from the trivial subgroup $\{\text{id}\}$ or a subgroup in $\mathcal{H}_{\text{Sym}} = \{H < S_n : H = \langle h \rangle, h^2 = \text{id}, h(i) \neq i \ (i = 1, \ldots, n)\}$, i.e., a set of all the subgroups generated by the involution composed of $n/2$ disjoint transpositions.

1.2 Our Contributions

We study upper and lower bounds for the sample complexity of general HSPs from an information-theoretic viewpoint. We consider two problems associated with HSPs to deal with their sample complexity. The first one is the identification version of HSPs when solving based on the standard method.

Definition 1.3 (Coset State Identification (CSI)) Let $\mathcal{H}$ be a set of candidate subgroups of a finite group $G$. We then define $S_\mathcal{H}$ as a set of coset states corresponding to $\mathcal{H}$. Given a black box that generates an unknown coset state $\rho_H$ in $S_\mathcal{H}$, the Coset State Identification (CSI) for $\mathcal{H}$ is the problem of identifying $H \in \mathcal{H}$.

One can easily see that any solution to HSP based on the standard method reduces to this identification of coset states. We now define the sample complexity of CSI for $\mathcal{H}$ as the sufficient and necessary number of samples for identifying the given coset state with a constant probability.

The second one is the decision version, named the Triviality of Coset State. Special cases of this problem have been discussed for the limitations of the standard method in many previous results [19, 15, 29, 34, 35, 1, 18].

Definition 1.4 (Triviality of Coset State (TCS)) Let $\mathcal{H}$ be a set of candidate non-trivial subgroups of a finite group $G$, i.e., $H \neq \{\text{id}\}$ for every $H \in \mathcal{H}$. We then define $S_\mathcal{H}$ as a set of coset states corresponding to $\mathcal{H}$. Given a black box that generates an unknown state $\sigma$ that is either in $S_\mathcal{H}$ (i.e., a coset state for the non-trivial subgroup) or equal to $I/|G|$ (i.e., a coset state for the trivial subgroup), the Triviality of Coset State for $S_\mathcal{H}$ is the problem of deciding whether $\sigma$ is in $S_\mathcal{H}$ or equal to $I/|G|$. We say that a quantum algorithm solves TCS with a constant advantage if it correctly decides whether a given state is in $S_\mathcal{H}$ or equal to $I/|G|$ with success probability at least $1/2 + \delta$ for some constant $\delta \in (0, 1/2]$.

Similarly to the case of CSI, we define the sample complexity of TCS for $\mathcal{H}$ as the sufficient and necessary number of coset states to solve TCS with a constant advantage.

Note that this problem might be efficiently solvable even if we cannot identify the hidden subgroup. Actually, if we can give a solution to TCS for $\mathcal{H}_{\text{Sym}} = \{H < S_n : H = \langle h \rangle, h^2 = \text{id}, h(i) \neq i \ (i = 1, \ldots, n)\}$, we can also solve the rigid graph isomorphism problem, i.e., the problem of finding an isomorphism between two graphs having no non-trivial automorphisms, and the decisional graph automorphism problem, i.e., the problem of deciding whether a given graph has non-trivial automorphisms or not [31].
In this paper, we give bounds of the sample complexity of CSI and TCS by simple information-theoretic arguments. We present the following bounds of the sample complexity of CSI.

**Theorem 1.5 (Upper and Lower Bounds for CSI)** Let \( \mathcal{H} \) be any set of candidate subgroups of a finite group. Then, the sample complexity of CSI for \( \mathcal{H} \) is at most \( O \left( \frac{\log |\mathcal{H}|}{\log \min_{H \in \mathcal{H}} |H|} \right) \) and at least \( \Omega \left( \frac{\log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|} \right) \).

Moreover, the upper bound of CSI can be attained by a quantum measurement essentially based on PGM. This shows that we can identify a hidden subgroup for an arbitrary group \( G \) with at most \( O(\log |\mathcal{H}|) \) samples based on the concept of PGM, which is a wider class than those of the previous results [2, 33]. It is noted that the essentially same upper bound* for CSI follows from the result of Ettinger, Høyer, and Knill [11]. However, their measurement is not known to be related to PGM.

We also present the following bounds of the sample complexity of TCS.

**Theorem 1.6 (Upper and Lower Bounds for TCS)** Let \( \mathcal{H} \) be any set of candidate subgroups of a finite group. Then, the sample complexity of TCS for \( \mathcal{H} \) is at most \( O \left( \frac{\log |\mathcal{H}|}{\log \min_{H \in \mathcal{H}} |H|} \right) \). If \( |H| \) is a prime for every \( H \in \mathcal{H} \), the sample complexity is at least \( \Omega \left( \frac{\log |\mathcal{H}|}{\log |H|} \right) \).

Summarizing these bounds, we obtain the following tight bounds for a class of CSIs and TCSs including several important instances such as \( \mathcal{H}_{\text{SDP}} \) and \( \mathcal{H}_{\text{Sym}} \).

**Corollary 1.7** Let \( \mathcal{H} \) be any set of candidate subgroups of a finite group satisfying that \( |H| = p \) for every \( H \in \mathcal{H} \), where \( p \) is a prime. Then, the sample complexity of CSI and TCS for \( \mathcal{H} \) is \( \Theta \left( \frac{\log |\mathcal{H}|}{\log p} \right) \).

This theorem implies that the decision version is as hard as the corresponding identification version in view of the sample complexity for this class.

We moreover apply our arguments to evaluation of information-theoretic security of the quantum encryption schemes proposed by Kawachi, Koshiba, Nishimura, and Yamakami [27, 28]. They proposed two quantum encryption schemes: One is a single-bit encryption scheme, which has a computational security proof based on the worst-case hardness of the decisional graph automorphism problem, and the other is a multi-bit encryption scheme, which has no security proof. Since their schemes make use of quantum states quite similar to coset states over the symmetric group as the encryption keys and ciphertexts, our proof techniques are applicable to the security evaluation of their schemes. We prove that the success probability of any computationally unbounded adversary distinguishing any two ciphertexts is at most \( \frac{1}{2} + 2^{-\Omega(n)} \) in their log \( m \)-bit encryption scheme with the security parameter \( n \) if the adversary has only \( o \left( \frac{n \log n}{\log m} \right) \) encryption keys.

Apart from HSPs, our results are closely related to the general problem of quantum state identification, which has been deeply studied in the channel capacity of classical-quantum channel of the quantum information theory. Many papers [24, 5, 42, 23] concerning the classical capacity of quantum channel give an upper bound of average error probability for the general problem of state identification among given arbitrary quantum states. In contrast to that, our results focus on the worst error probability due to requirement from our algorithmic setting. Our arguments for upper bounds of average error probability do not require the assumption on the average state of a given ensemble to estimate the error probability. We present the error estimation using a projection onto the space spanned by support of a candidate state, which differs from the existing arguments (see Lemma 2.2). We also show a general estimation of error probability for distinguishing between completely mixed states and independent and identically distributed (i. i. d.) states using summation of rank of candidate states (see Lemma 2.4).

We also provide a general argument for upper bounds of average success probability in general setting. It is known that Ogawa and Nagaoka presented a general upper bound of the average success probability [38]. Our

---

* Note that their result covers the case in which a set of candidate subgroups includes the trivial one, while our upper bound becomes meaningless in such a case. We can fortunately exclude the case without loss of generality. See Remark 2.10 at the end of Section 2 for details. Strictly speaking, our bound is better than theirs up to a constant factor in the other cases.
Lemma 2.3
Let state identification, which is useful to prove the lower bound of sample complexity for CSI.

\[ \Sigma = (\begin{bmatrix} S & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}) \]

Proof. Setting \( M = (\begin{bmatrix} P & 0 \\ 0 & I \end{bmatrix}) \), the matrix of \( Y \) and \( T \) and \( M \) are defined as

\[
\left\{ \begin{array}{ll}
\Sigma &= (\begin{bmatrix} S & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}) \\
M &= (\begin{bmatrix} P & 0 \\ 0 & I \end{bmatrix})
\end{array} \right.
\]

The trace norm of a matrix \( X \in \mathbb{C}^{d \times d} \) is useful to estimate success probability of quantum state distinction for two states, and is defined as \( \|X\|_\text{tr} = \max \langle Y, X \rangle = \text{tr}\sqrt{Y \Sigma X} \), where \( \|Y\| \) is the operator norm of a matrix \( Y \) and \( \langle Y, X \rangle = \text{tr}Y^\dagger X \) is the matrix inner product.

The trace norm of a matrix \( X \in \mathbb{C}^{d \times d} \) is useful to estimate success probability of quantum state distinction for two states, and is defined as \( \|X\|_\text{tr} = \max \langle Y, X \rangle = \text{tr}\sqrt{X \Sigma X} \), where \( \|Y\| \) is the operator norm of a matrix \( Y \) and \( \langle Y, X \rangle = \text{tr}Y^\dagger X \) is the matrix inner product. It is well known that for any two quantum states \( \rho_0 \) and \( \rho_1 \) the average success probability of the optimal POVM distinguishing two quantum states is equal to

\[
\frac{1}{2} + \frac{1}{2} \|\rho_0 - \rho_1\|_\text{tr}, \text{ i.e., } \frac{1}{2} \max_{M = \{M_0, M_1\}} (\text{tr}M_0 \rho_0 + \text{tr}M_1 \rho_1) = \frac{1}{2} + \frac{1}{2} \|\rho_0 - \rho_1\|_\text{tr}.
\]

See [4] for more details on the matrix analysis and [37, 22] on basics of the quantum information theory.

We make use of the concept of PGM in order to prove the general upper bound for CSI. The following lemma shown by Hayashi and Nagaoka [23] is useful to estimate the error probability of the pretty good measurement (see also Lemma 4.5 in [22]).

Lemma 2.1 (Hayashi and Nagaoka [23]) For any Hermitian matrices \( S \) and \( T \) satisfying that \( I \geq S \geq 0 \) and \( T \geq 0 \), it holds that

\[
I - \sqrt{S + T}^{-1} S \sqrt{S + T}^{-1} \leq 2(I - S) + 4T,
\]

where \( \sqrt{S + T}^{-1} \) is the generalized inverse matrix of \( \sqrt{S + T} \).

By the above lemma, we can show an upper bound of error probability for the general problem of state identification using a variant of PGM, which is useful to prove the upper bound for CSI.

Lemma 2.2 Let \( \{\rho_i\} \) be any set of distinct quantum states of identical dimension, and let \( P_i \) be a projection onto the space spanned by \( \text{supp}(\rho_i) \). Then, for any \( k > 0 \) and any \( i \)

\[
\text{tr}(I - \Sigma^{-1/2} P_i \otimes k \Sigma^{-1/2} \rho_i^{\otimes k}) \leq 4 \sum_{j \neq i} \left( \text{tr}P_j \rho_i \right)^k,
\]

where \( \Sigma = \sum_j P_j \otimes k \).

Proof. Setting \( S = P_i \otimes k \) and \( T = \sum_{j \neq i} P_j \otimes k \) in Lemma 2.1, we obtain for any \( i \)

\[
\text{tr}(I - \Sigma^{-1/2} P_i \otimes k \Sigma^{-1/2} \rho_i^{\otimes k}) \leq 2 \text{tr}(I - P_i \otimes k) \rho_i^{\otimes k} + 4 \text{tr} \left( \sum_{j \neq i} P_j \otimes k \right) \rho_i^{\otimes k} = 4 \sum_{j \neq i} \left( \text{tr}P_j \rho_i \right)^k.
\]

The following lemma provides an upper bound of the average success probability of the general problem of state identification, which is useful to prove the lower bound of sample complexity for CSI.

Lemma 2.3 Let \( \{\rho_i, ..., \rho_N\} \) be any set of distinct \( N \) quantum states of identical dimension \( d \). For any POVM \( M = \{M_1, ..., M_N\} \) associated with \( \{\rho_i\} \), using identical \( k \) samples of the candidate state, we have

\[
\frac{1}{N} \sum_{i=1}^{N} \text{tr}M_i \rho_i^{\otimes k} \leq \frac{(d \max_i \|\rho_i\|)^k}{N}.
\]
Proof. By using the facts that $|\langle X, Y \rangle| \leq \|X\| \|Y\|_{\text{tr}}$ for any matrices $X, Y \in \mathbb{C}^{d \times d}$ and $\text{tr} \left( \sum_{i=1}^{N} M_i \right) = d^k$ for any $d^k$-dimensional POVM $\{M_1, \ldots, M_N\}$, we have
\[
\frac{1}{N} \sum_{i=1}^{N} \text{tr} M_i \rho_i^{\otimes k} = \frac{1}{N} \sum_{i=1}^{N} \langle M_i, \rho_i^{\otimes k} \rangle \leq \frac{1}{N} \sum_{i=1}^{N} \|\rho_i^{\otimes k}\| \|M_i\|_{\text{tr}} \leq \frac{1}{N} \max_i \|\rho_i\| \sum_{i=1}^{N} \|M_i\| \leq \frac{1}{N} \max_i \|\rho_i\|^k \sum_{i=1}^{N} \text{tr} M_i = \frac{1}{N} \max_i \|\rho_i\|^k \text{tr} \left( \sum_{i=1}^{N} M_i \right) = \frac{(d \max_i \|\rho_i\|)^k}{N}.
\]

We also prove an upper bound of error probability for distinguishing between completely mixed states and i. i. d. states as follows using summation of rank of candidate states.

Lemma 2.4 Let $\{\rho_i\}_i$ be any set of distinct quantum states of identical dimension $d$ that does not contain the completely mixed state. For any $k > 0$, let $T$ be a projection onto the space spanned by $\bigcup_i (\rho_i^{\otimes k})$. Then, we have
\[
\text{tr} T \rho_i^{\otimes k} = 1 \quad \text{and} \quad \text{tr} T (I/d)^{\otimes k} \leq \frac{\sum_i \text{rank}(\rho_i)^k}{d^k}.
\]

Proof. The first equation is obvious by the definition of $T$. The second inequality follows from the fact that $\text{tr} T (I/d)^{\otimes k} = \frac{\text{rank}(T)}{d^k} \leq \sum_i \frac{\text{rank}(\rho_i)^k}{d^k}$.

2.2 Lower Bounds

In this section, we prove theorems on lower bounds of the sample complexity for CSI and TCS. In our several proofs, we need to calculate the rank of a coset state. The following lemma gives the estimation of the rank.

Lemma 2.5 For any coset state for a subgroup $H$ of a finite group $G$, it holds that $\text{rank}(\rho_H) = \frac{|G|}{|H|}$.

Proof. Let $|\psi\rangle$ be a purification of $\rho_H$ described as $|\psi\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f_H(g)\rangle_B$, where $f_H$ is the given function in the definition of HSP. Tracing out the register $A$, we have $\text{rank}(\langle \psi | \langle \psi |) = |G/H|$. Since $\text{rank}(\langle \psi | \langle \psi |) = \text{rank}(\text{tr}_A |\psi\rangle \langle \psi |)$, we obtain $\text{rank}(\rho_H) = \frac{|G|}{|H|}$.

We next prove the key theorem on lower bounds for CSI by a simple information-theoretic argument. This theorem generally gives the necessary number of identical samples of an unknown coset state for the identification.

Theorem 2.6 Let $\mathcal{H}$ be any set of candidate subgroups of a finite group $G$. Then, the sample complexity of CSI for $\mathcal{H}$ is at least $\Omega \left( \frac{\log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|} \right)$.

Proof. Let $M = \{M_H\}_{H \in \mathcal{H}}$ be any POVM associated with $S_{\mathcal{H}}$ using $k$ samples of the coset state. By Lemma 2.3, the probability of $M$ obtaining correct outcome is upper bounded by
\[
\frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \text{tr} M_H \rho_H^{\otimes k} \leq \frac{\left( \max_{H \in \mathcal{H}} \|\rho_H \| \|G\| \right)^k}{|\mathcal{H}|}.
\]

Thus, the success probability of any quantum algorithm that solves CSI with $k$ coset states is upper bounded by $\frac{\left( \max_{H \in \mathcal{H}} \|\rho_H \| \|G\| \right)^k}{|\mathcal{H}|}$. Since the coset state $\rho_H = \frac{1}{|\mathcal{H}|} \sum_{g \in G/H} |gH\rangle \langle gH|$ for any subgroup $H$ is a uniform summation of the matrices $|gH\rangle \langle gH|$ orthogonal to each other, we obtain $\|\rho_H \| = 1/\text{rank}(\rho_H)$. It follows that $\|\rho_H \| = |H|/|G|$ by Lemma 2.5. The success probability is thus at most $\frac{\left( \max_{H \in \mathcal{H}} |H| \right)^k}{|\mathcal{H}|}$, which implies that any quantum algorithm that solves CSI for $\mathcal{H}$ requires $\Omega \left( \frac{\log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|} \right)$ coset states in order to attain constant success probability.
As mentioned in Section 1, we do not have to identify a hidden subgroup to solve TCS. Thus, we cannot expect the same technique as the proof of the lower bound for CSI to work for that of TCS. We give another proof technique to obtain the lower bound for TCS.

**Theorem 2.7** Let $\mathcal{H}$ be any set of candidate subgroups of a finite group $G$. The sample complexity of TCS for $\mathcal{H}$ is at least $\Omega \left( \frac{\log |\mathcal{H}|}{\log(\max_{H \in \mathcal{H}} |H|)} \right)$ if $|H|$ is a prime for every $H \in \mathcal{H}$.

**Proof.** We first show that the success probability of solving TCS for $\mathcal{H}$ is upper bounded by that of identification for certain two quantum states. Let $M = \{M_0, M_1\}$ be any POVM associated with $\{\text{id}, \mathcal{H}\}$. The success probability of $M$ is given by $\min\{\text{tr}M_0(I/|G|)^{\otimes k}, \text{tr}M_1(I/|G|)^{\otimes k}\}$.

In order to have this trace norm larger than some positive constant, we consider $|\mathcal{H}| - 1$ candidate subgroups of a finite group $G$. Let $G = \bigcup_{H \in \mathcal{H}} H$. Then, the trace and the POVM that $	ext{tr}M_1 \left( \frac{1}{|\mathcal{H}|} \sum_{\rho \in \mathcal{H}} \rho^{\otimes k} \right) = \frac{1}{|\mathcal{H}|} \sum_{\rho \in \mathcal{H}} \text{tr}M_1 \rho^{\otimes k} \geq \min_{\rho \in \mathcal{H}} \text{tr}M_1 \rho^{\otimes k}$. Thus, the success probability is at most $\min\{\text{tr}M_0(I/|G|)^{\otimes k}, \frac{1}{|\mathcal{H}|} \sum_{\rho \in \mathcal{H}} \text{tr}M_1 \rho^{\otimes k}\}$. This equal to the success probability of the identification for $(I/|G|)^{\otimes k}$ and $\frac{1}{|\mathcal{H}|} \sum_{\rho \in \mathcal{H}} \rho^{\otimes k}$.

Note that we cannot apply the argument of Theorem 2.6 to the identification. Instead, we directly evaluate an upper bound of the trace norm of the matrix $X = \frac{1}{|\mathcal{H}|} \sum_{\rho \in \mathcal{H}} \rho^{\otimes k} - (I/|G|)^{\otimes k}$. Then the success probability of the identification is at most $\frac{1}{2} + \frac{1}{2} \|X\|_{\text{tr}}$ by the property of the trace norm. Naïvely expanding $X$, we obtain by the triangle inequality

$$\|X\|_{\text{tr}} \leq \frac{1}{|\mathcal{H}|} \sum_{g_1, \ldots, g_k \in G} \left\| \sum_{H \in \mathcal{H}} \sum_{\rho \in H} \langle g_1, \ldots, g_k | \rho^{\otimes k} | g_1, \ldots, g_k \rangle \right\|.$$
Let \( TCS \) for \( \mathcal{H} \) be any set of candidate subgroups of a finite group \( G \). Then the sample complexity of \( TCS \) for \( \mathcal{H} \) is at most \( O\left( \frac{\log |\mathcal{H}|}{\log \min_{H \in \mathcal{H}} |H|} \right) \).

**Proof.** We consider a projection \( T \) onto the space spanned by \( \bigcup_{H \in \mathcal{H}} \text{supp}(\rho_H^k) \). The error probability of distinguishing between \( \rho_H^k \) and \( (I/|G|)^\otimes k \) is then \( \text{tr}T(I/|G|)^\otimes k = \frac{\sum_{H \in \mathcal{H}} \text{rank}(\rho_H)/|G|^k}{|G|^k} \) by Lemma 2.4. Since \( \text{rank}(\rho_H) = |G|/|H| \) by Lemma 2.5, we obtain \( \frac{\sum_{H \in \mathcal{H}} \text{rank}(\rho_H)}{|G|^k} = \frac{\sum_{H \in \mathcal{H}} (|G|/|H|)^k}{|G|^k} \leq \frac{|\mathcal{H}|}{\min_{H \in \mathcal{H}} |H|^k} \). This implies that at most \( O\left( \frac{\log |\mathcal{H}|}{\log \min_{H \in \mathcal{H}} |H|} \right) \) samples of coset states are sufficient for constant advantage.

**Remark 2.10** The upper bound for CSI in Theorem 2.8 becomes meaningless if the candidates include the trivial subgroup. However, this case can be excluded by first applying the measurement for TCS shown in Theorem 2.9 to given states. Consequently, we can attain the same upper bound as in [11] even if the trivial subgroup is contained in the candidates.

## 3 Security Evaluation of Quantum Encryption Schemes

Our arguments are applicable not only to bounds for HSP but also to security evaluation of quantum cryptographic schemes. In this section, we apply our arguments to evaluation of the information-theoretic security of the quantum encryption schemes proposed in [27, 28]. As mentioned in Section 1, they proposed single-bit and multi-bit quantum encryption schemes. While they gave the complexity-theoretic security to the single-bit scheme under the assumption of the worst-case hardness of the decisional graph automorphism problem, the multi-bit one has no security proof. Also, they have already proven in [28] that any computationally unbounded quantum algorithm cannot solve a certain quantum state distinction problem that underlies the single-bit scheme with few samples by reducing the solvability of their distinction problem to the result of [18]. On the other hand, the security of their encryption schemes, as well as the underlying problem for their multi-bit scheme, are not evaluated yet from a viewpoint of the quantum information theory.

Their schemes make use of certain quantum states for their encryption keys and ciphertexts. We now call these quantum states *encryption-key states* and *ciphertexts*, respectively. Since their multi-bit encryption
scheme contains the single-bit one as a special case if we ignore its efficiency and complexity-theoretic security, we only discuss their multi-bit scheme in this paper.

We now describe their multi-bit encryption scheme in detail. Assume that the message length parameter $m$ divides the security parameter $n$, where $m \in \{2, \ldots, n\}$. Let $\mathcal{K}^m_n = \{h : h = (a_1 \cdots a_m) \cdots (a_{m-1} \cdots a_n), a_i \in \{1, \ldots, n\}, a_i \neq a_j (i \neq j) \} \subset S_n$, i.e., a set of the permutations composed of $n/m$ disjoint cyclic permutations, which is used for the decryption key. In this scheme, we exploit the following quantum state for a message $s$:

$$\rho_h^{(s)} = \frac{1}{m!} \sum_{g \in S_n} \left( \sum_{k=0}^{m-1} \omega_m^k |gh^k\rangle \langle gh^k| \right) \left( \sum_{l=0}^{m-1} \omega_m^{-ls} |gh^l\rangle \langle gh^l| \right),$$

where $\omega_m = e^{2\pi i/m}$ and $h \in \mathcal{K}^m_n$. Note that $\rho_h^{(0)}$ is the coset state for the hidden subgroup $\{id, h, \ldots, h^{m-1}\}$. We now refer to as $(n, m)$-QES their multi-bit encryption scheme with the security parameter $n$ and the message length parameter $m$. The protocol of $(n, m)$-QES is summarized as follows.

**Protocol: $(n, m)$-QES**

1. The receiver Bob chooses his decryption key $h$ uniformly at random from $\mathcal{K}^m_n$ and generates the encryption-key states $\sigma_h = (\rho_0^{(h)}, \ldots, \rho_{m-1}^{(h)})$.
2. The sender Alice requests the encryption-key state $\sigma_h$ to Bob. She picks $\rho_h^{(s)}$ up from $\sigma_h$ as the ciphertext corresponding to her classical message $s \in \{0, \ldots, m-1\}$ and then sends it to him.
3. Bob decrypts her ciphertext $\rho_h^{(s)}$ with his decryption key $h$.

We assume the same adversary model except for Eve’s computational power as the original ones in [27, 28]. Note that the eavesdropper Eve can also request the same encryption-key states to Bob as one of senders. Eve in advance requests the encryption-key states to Bob. When Alice sends to Bob her ciphertext that Eve wants to eavesdrop, Eve picks up Alice’s ciphertext and then tries to extract Alice’s message from the ciphertext with the encryption-key states by computationally unbounded quantum computer, i.e., Eve can apply an arbitrary POVM over the ciphertexts and encryption-key states to extract Alice’s message.

We consider a stronger security notion such that Eve cannot distinguish even two candidates, i.e., she cannot find a non-negligible gap between $\text{tr}M_1(\rho_h^{(s)} \otimes \sigma_h^{\otimes k})$ and $\text{tr}M_1(\rho_h^{(s')} \otimes \sigma_h^{\otimes k})$ even by the optimal POVM $M = \{M_0, M_1\}$ when Bob chooses $h$ uniformly at random. This notion naturally extends the computational indistinguishability of encryptions, which is the standard security notion in the modern cryptography [14], to the information-theoretic one.

Since the gap is at most $\frac{1}{2} \frac{1}{|\mathcal{K}^m_n|} \sum_{h \in \mathcal{K}^m_n} \| \rho_h^{(s)} \otimes \sigma_h^{\otimes k} - \rho_h^{(s')} \otimes \sigma_h^{\otimes k} \|_{tr}$, this notion can be formalized by the trace norm between them. Then, we say that the ciphertexts are *information-theoretically indistinguishable within $k$ encryption-key states* if $\| \frac{1}{|\mathcal{K}^m_n|} \sum_{h \in \mathcal{K}^m_n} \rho_h^{(s)} \otimes \sigma_h^{\otimes k} - \rho_h^{(s')} \otimes \sigma_h^{\otimes k} \|_{tr} = 2^{-\Omega(n)}$.

For this security notion, we can obtain the following theorem by our information-theoretic arguments. The proof is almost straightforward by Theorem 2.7.

**Theorem 3.1** The ciphertexts of $(n, m)$-QES are information-theoretically indistinguishable within $o \left( \frac{n \log n}{m \log m} \right)$ encryption-key states.

**Proof.** Let $l_s = \frac{1}{|\mathcal{K}^m_n|} \sum_{h \in \mathcal{K}^m_n} \rho_h^{(s)} \otimes \sigma_h^{\otimes k} - (I/n^k)^{\otimes m}k+1 \|_{tr}$. Then the trace norm between two state sequences given in the definition of the information-theoretic indistinguishability is at most $l_s + l_s'$, by the triangle inequality. Since the trace norm is invariant under unitary transformations, we can show that $l_s + l_s' = 2l_s$ by taking appropriate unitary operators. Then we can prove that $l_s \leq \sqrt{m^{mk+1}/|\mathcal{K}^m_n|}$ by the argument of Theorem 2.7. Since we have $|\mathcal{K}^m_n| \approx \frac{m^{1/2}n^{-n/m}}{e^{n/m}}$ by the standard counting method and the Stirling approximation, the trace norm is at most $2^{-\Omega(n)}$ if $k = o \left( \frac{n \log n}{m \log m} \right)$.

For example, when we set $m = n^\varepsilon$ for any constant $0 < \varepsilon < 1$, we obtain the $\varepsilon \log n$-bit encryption scheme whose ciphertexts are information-theoretically indistinguishable within $o(n^{1-\varepsilon})$ encryption-key states.

### 4 Concluding Remarks

In this paper, we have shown general bounds for CSI and TCS, and an application to the security evaluation of the quantum encryption schemes. We believe such an information-theoretic approach will help constructions

9
of efficient quantum algorithms for non-Abelian HSPs as in the case of [2]. After our preliminary version of this paper, Harrow and Winter followed our approach to prove the existence of a quantum measurement for identifying general quantum states and lower bounds of samples for the identification [20]. Their results generalize and improve our bounds for CSI.

Acknowledgements

The authors would like to thank François Le Gall, Cristopher Moore, Christopher Portmann and Tomoyuki Yamakami for helpful discussions and comments. MH was supported by ERATO-SORST QCI project and the Ministry of Education, Culture, Sports, Science and Technology, Grant-in-Aid for Scientific Research on Priority Areas No. 18079014. AK was supported by the Ministry of Education, Culture, Sports, Science and Technology, Grant-in-Aids for Young Scientists (B) No. 17700007, 2005 and for Scientific Research on Priority Areas No. 16092206. AK and HK were supported by the Ministry of Education, Culture, Sports, Science and Technology, Grant-in-Aid for Scientific Research (B) No. 18300002, 2006.

References

References


