PHOTONICS Research

Experimental verification of group non-membership in optical circuits

Kai Sun,[1,2,†] Zi-Jian Zhang,[3,†] Fei Meng,[3,4] Bin Cheng,[3,5] Zhu Cao,[6] Jin-Shi Xu,[1,2,9] Man-Hong Yung,[3,7,8,10] Chuan-Feng Li,[1,2,11] and Guang-Can Guo[1,2]

[1]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China
[2]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
[3]Department of Physics, Southern University of Science and Technology, Shenzhen 518055, China
[4]Department of Computer Science, The University of Hong Kong, Pokfulam, Hong Kong SAR, China
[5]Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, Sydney, NSW 2007, Australia
[6]Key Laboratory of Advanced Control and Optimization for Chemical Processes of Ministry of Education, East China University of Science and Technology, Shanghai 200237, China
[7]Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
[8]Shenzhen Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
[9]e-mail: jsxu@ustc.edu.cn
[10]e-mail: yung@sustech.edu.cn
[11]e-mail: cfli@ustc.edu.cn

Received 16 April 2021; revised 27 June 2021; accepted 29 June 2021; posted 1 July 2021 (Doc. ID 427897); published 19 August 2021

The class quantum Merlin–Arthur (QMA), as the quantum analog of nondeterministic polynomial time, contains the decision problems whose YES instance can be verified efficiently with a quantum computer. The problem of deciding the group non-membership (GNM) of a group element is conjectured to be a member of QMA. Previous works on the verification of GNM, which still lacks experimental demonstration, required a quantum circuit with $O(n^5)$ group oracle calls. Here, we provide an efficient way to verify GNM problems, in which each quantum circuit only contains $O(1)$ group of oracle calls, and the number of qubits in each circuit is reduced by half. Based on this protocol, we then experimentally demonstrate the new verification process with a four-element group in an all-optical circuit. The new protocol is validated experimentally by observing a significant completeness-soundness gap between the probabilities of accepting elements in and outside the subgroup. This work efficiently simplifies the verification of GNM and is helpful in constructing more quantum protocols based on the near-term quantum devices.

https://doi.org/10.1364/PRJ.427897

1. INTRODUCTION

Quantum effect can be used to enhance information processing in many ways. Besides speeding up solving certain problems [1–3], quantum computers can also be used to construct novel interactive proof systems (IPSs) [4–6], which leads to fruitful studies in blind quantum computing [7–9], quantum zero-knowledge proof systems [10,11], and multiprover IPSs [12,13]. An IPS involves a verifier and (potentially multiple) *provers*, where the verifier aims at solving certain problems by exchanging messages with the provers.

IPSs can be used to classify decision problems, the problems whose answers can only be YES or NO. For example, nondeterministic polynomial time (NP), one of the most important complexity classes, can be described by an IPS, with a classical verifier and a single computationally unbounded prover exchanging one round of classical message [14,15]. Specifically, NP contains decision problems that, for a YES instance, there exists certain proof message, with which the YES instance can be verified in polynomial time by a classical computer. NP can be generalized to the quantum realm naturally and the quantum analog is called quantum Merlin–Arthur (QMA) [15,16]. In QMA, the proof message is replaced by a quantum state, and the verifier can use a quantum computer to process it [17,18].

Since a classical verifier can be simulated by a quantum computer and a classical message can be described by a quantum state, every problem belonging to NP is also in QMA [15,16], i.e., NP $\subseteq$ QMA. However, it remains an unsolved problem whether QMA is strictly larger than NP, and the group non-membership (GNM) problem is believed to be a possible candidate that falls in QMA but not in NP [16,19–21]. Previous works have shown the potential quantum advantage on verifying YES instances of this problem. It has been proven that the GNM problem is not in NP^B [20] for a certain group oracle B.

Also, for every B, GNM(B) $\in$ QMA$^{\mathrm{B}}$ has been proven by giving quantum proofs and a verification process that can be efficiently performed by a quantum computer [21]. Furthermore, it is conjectured that certain quantum proofs, which are similar to the one constructed for proving GNM(B) $\in$ QMA$^{\mathrm{B}}$, can be used in many other decision problems of finite groups, such as the problems of deciding proper subgroups and simple groups [21].

Because of the potential applications of quantum IPS and the growing power of near-term quantum devices [22,23], it has become a meaningful question on how to make quantum IPS more friendly for near-term quantum devices. The verification of GNM is of special importance, as it is closely related to the verification of a wide spectrum of group properties and is expected to present quantum advantage. However, the previous efforts to verify GNM are not favorable for near-term devices, as it requires too deep quantum circuits [21,24], and the related experimental demonstration is absent.

In this work, based on a new protocol, which improves the previous protocol proposed by Watrous [21] and is more friendly to near-term quantum devices, we experimentally show the verification of GNM by an all-optical setup. By sending various photonic quantum proofs to the optical circuits, a significant completeness-soundness gap, which is the difference between the probabilities of accepting elements outside the subgroup and incorrectly accepting elements inside the subgroup, is observed to present the validity of our protocol. For the groups with at most 2^n elements, each quantum circuit in the new protocol only requires $O(1)$ group oracle calls, whereas the previous protocol requires $O(n^5)$ oracle calls in one circuit. The number of qubits needed is also half-reduced. Our new process makes it easier to use the verification of GNM as a part of near-term quantum applications such as quantum cryptography protocols.

2. THEORETICAL FRAMEWORK

First, we formally revisit the GNM problem here [21]. Let G be a finite group and $S = \langle g_1, \ldots, g_k \rangle$ be a subgroup generated by group elements $g_1, \ldots, g_k \in G$. Given an element $x \in G$, the GNM problem is to decide whether x is outside the subgroup S. If $x \notin S$, x is a YES instance; otherwise, x is a NO instance. To analyze the problem with minimum assumption on the group, usually the framework of black-box groups [25] is adopted. Following the framework of the quantum group oracle [21], in which the quantum group element labels are a set of mutually orthogonal quantum states, we denote the quantum label corresponding to the group element g by ψ_g and the space spanned by the quantum labels of elements in G by $\mathrm{span}\{G\} := \mathrm{span}\{|\psi_{g_1}\rangle\langle\psi_{g_2}| : g_1, g_2 \in G\}$. The quantum group oracle is defined to be able to detect whether a state is in $\mathrm{span}\{G\}$ and carry out right multiplication $\mathcal{M}(\cdot)$ as $\mathcal{M}(g_2)|\psi_{g_1}\rangle = |\psi_{g_1 g_2}\rangle$. The quantum proof for the non-membership can be a uniform superposition of the elements in a co-set αS of the subgroup S for any $\alpha \in G$ [21], where αS is defined as $\alpha S := \{\alpha s | s \in S\}$. Explicitly, it can be written as

$$|\mathrm{Q}_{\mathrm{proof}}\rangle = \frac{1}{\sqrt{|S|}} \sum_{g \in \alpha S} |\psi_g\rangle, \tag{1}$$

where $|S|$ is the element number of the subgroup S. This state is invariant under right multiplications of the elements in S because they map the elements in αS bijectively to αS. On the other hand, if $x \notin S$, the result state is orthogonal to the original one as $\langle \mathrm{Q}_{\mathrm{proof}}|\mathcal{M}(x)|\mathrm{Q}_{\mathrm{proof}}\rangle = 0$, since $(\alpha S)x$ and αS do not share common elements.

Next, we introduce the core quantum circuit, which plays a central role in both the original and new verification process [21]. The core circuit is similar to the swap test circuit and is depicted in Fig. 1. The outcome of the core circuit is defined to be the measurement outcome of the control qubit. We denote by $\mathrm{core}(x, |\mathrm{Q}_{\mathrm{proof}}\rangle) = s$ the event of obtaining the measurement outcome $s \in \{0,1\}$ in one run of the core circuit with input state $|\mathrm{Q}_{\mathrm{proof}}\rangle$ and group member x. The outcome can show the effect of the multiplication by x on the input state. For $\mathrm{core}(x, |\mathrm{Q}_{\mathrm{proof}}\rangle)$, if $x \in S$, the outcome can only be 0, as $|\mathrm{Q}_{\mathrm{proof}}\rangle$ is invariant under the multiplication. If $x \notin S$, the probability of obtaining 1 is 0.5 as the state after multiplication is orthogonal to $|\mathrm{Q}_{\mathrm{proof}}\rangle$. Therefore, with the proof state, the non-membership of an element can be verified when the outcome 1 is obtained.

However, a malicious prover may send bogus proof states that deviate from Eq. (1) and give incorrect outcomes. Therefore, to ensure the soundness of the verification, the verifier has to do a property check on the received proof state, i.e., check that the state is invariant under the group multiplication $\mathcal{M}(s)$ for any $s \in S$, so that the elements in S cannot be proven to be outside S. In the original protocol, to verify the proof received is valid, the verifier needs to uniformly sample the subgroup elements in a reversible way and produce a quantum superposition of all the quantum labels,

$$\sum_{g \in S} a_i |g\rangle |\mathrm{garbage}(g)\rangle, \tag{2}$$

where the norm of $\{a_i\}$ should be nearly uniform. The reversible sampling requires $O(n^5)$ calls of the group oracle in the quantum circuit [24] and requires the verifier to keep at least two quantum group element labels.

In the new verification process for GNM, we reduce both the circuit depth and qubit number needed by importing the technique we call random state inspection (RSI). In RSI, the prover is required to send m registers that carry copies of a state to the verifier. The verifier randomly selects one register to reserve and applies independent test channels to the other $m-1$ registers to check the property of the states that they carry. If all the $m-1$ registers pass the property checking, the verifier accepts the reserved register for the later verification process.

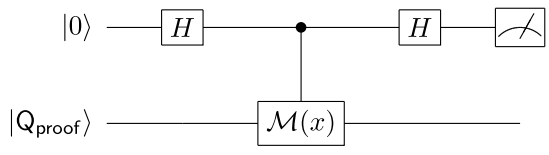

Fig. 1. Core circuit. The circuit is similar to the swap test circuit and aims to check whether the input state is invariant under certain group multiplication. With a correct proof state, if $x \in S$, the measurement outcome is always 0; if $x \notin S$, the measurement outcome is 1 with probability 0.5.

Otherwise, the verifier rejects. We model the test channel as a quantum channel that maps an input register to an output qubit. The verifier measures the output qubit and regards outcome $|0\rangle$ as pass and $|1\rangle$ as fail. One can show that, if all the other registers have passed the test channels, the probability for the reserved register to fail passing the test channel (if tested) can be bounded to 0 at speed $O(1/m)$ even when the m registers are entangled. Denote the density operator of the reserved register and other registers as ρ_r and ρ_t, this bound can be written as

$$\Pr(\text{test}(\rho_r) = \text{fail} | \text{test}(\rho_t) = \text{pass}) < O(1/m). \quad (3)$$

To show this bound, one just needs to analyze the density matrix of the output state after applying the test channels to all the registers. After testing all the other registers, the verifier can directly apply the later verification process on the reserved register as its property is ensured. By RSI, as the check and use of the proof state can be done in separate circuits, the circuit depth needed in the verification is reduced to that of the property checking or the later verification.

Besides reducing the circuit depth by RSI, we also simplify the property checking process in the original protocol. Rather than using the state in Eq. (2), which needs $O(n^5)$ quantum group oracle calls to produce, we propose a simplified new process here. The test channel of the new process starts from sampling an element s of the subgroup S from a nearly uniform distribution with a classical computer by Babai's algorithm [24]. Here, nearly uniform means the probability for s to be any subgroup elements is in $(1/|S| - 1/2^{2n}, 1/|S| + 1/2^{2n})$. The second step of the test channel is a core circuit. With the sampled element s, an input state passes the test channel when $\text{core}(s, \rho) = 0$. Therefore, in the whole verification process, all the quantum circuits the verifier needs to run are just core circuits with different group elements.

Here, we discuss the completeness and soundness of the new verification protocol. It can be proven that for any element $s \in S$ and any quantum state $\rho \in \text{span}\{G\}$, the probability of incorrectly proving the non-membership of s, i.e., having $\text{core}(s, \rho) = 1$, can be bounded as

$$\Pr(\text{core}(s, \rho) = 1) \le \frac{1 - \Pr(\text{test}(\rho) = \text{pass})}{K\left(1 - \frac{|S|}{2^{2n}}\right)}, \quad (4)$$

where

$$\frac{1}{K} = 1 - \cos\left(\left\lceil \frac{|s|}{2} \right\rceil \frac{2}{|s|}\pi\right), \quad (5)$$

and $|s|$ is the minimal positive number r such that s^r equals identity. With this bound, we know that one can bound the error probability $\Pr(\text{core}(s, \rho) = 1)$ to 0 by increasing $\Pr(\text{test}(\rho) = \text{pass})$, which can be efficiently bounded to 1 with RSI. Therefore, the soundness of the new protocol is ensured. To prove this bound, one just needs to decompose ρ on the basis of quantum labels $\{|\psi_g\rangle\}$ and study the coefficient of every basis state under the core circuit. The condition of high $\Pr(\text{test}(\rho) = \text{pass})$ can provide a restriction on the value of $\Pr(\text{core}(s, \rho) = 1)$ and techniques such as the Lagrangian multiplier can be then used to determine its maximal value. To prove the completeness, one just needs to notice that proof states from honest prover can certainly pass the test channels, and the reserved register with the correct state can prove the non-membership, the same as the original protocol. The whole new verification process is listed below.

1. Prover sends m registers with state in Eq. (1) to the verifier, trying to prove $g \in G$ is not in the subgroup $S \subseteq G$. Verifier receives the registers and checks whether their states are in $\text{span}\{G\}$. If not, reject the proof.
2. Verifier randomly chooses a register to reserve and applies the property checking process to all the other registers as below.
3. Property checking.

(a) Verifier samples an element $s \in S$ with a classical computer by Babai's algorithm.

(b) Verifier applies the core circuit with multiplication by s to the state. Verifier rejects the proof if the outcome is 1.

4. Verifier applies the core circuit with multiplication by g to the reserved register. The GNM of g is verified when the outcome is 1.

To summarize, in our new protocol, we split the property checking of the proof state and the verification after property checking into different circuits by RSI. We also use a new property checking process that requires many fewer quantum resources. As a result, the verifier only needs to run a core circuit, which is shallow, for many times, rather than run a deep circuit with $O(n^5)$ group operations. Also, the number of qubits that the verifier needs to keep is halved because the verifier no longer needs to keep a reversibly sampled quantum label.

3. EXPERIMENTAL SETUP AND RESULTS

In this work, an experimental demonstration of our new verification process is carried out. We consider an Abelian group $G = \{\langle \text{A}, \text{B}\rangle | \text{AB} = \text{BA}, \text{A}^2 = \text{B}^2 = \text{E}\}$. The four elements in G are encoded in the polarization degree of freedom of photons as $|\psi_\text{E}\rangle = |VH\rangle, |\psi_\text{A}\rangle = |HV\rangle, |\psi_\text{B}\rangle = |HH\rangle$ and $|\psi_\text{AB}\rangle = |VV\rangle$, in which $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization of the photons, respectively. They can together span the whole two-qubit Hilbert space. The corresponding multiplication circuits of the four group elements are illustrated in the first line of Fig. 2(a), where the circuit $\mathcal{M}(g)$ of each element g satisfies $\mathcal{M}(g_2)|\psi_{g_1}\rangle = |\psi_{g_1 g_2}\rangle$. We then construct the core circuits with these multiplications and map them to the optical interferometer illustrated in Fig. 2(a). For example, the circuit of A transforms $|\psi_\text{E}\rangle$ to $|\psi_\text{A}\rangle$, $|\psi_\text{A}\rangle$ to $|\psi_\text{E}\rangle$, $|\psi_\text{B}\rangle$ to $|\psi_\text{AB}\rangle$, and $|\psi_\text{AB}\rangle$ to $|\psi_\text{B}\rangle$. The subgroups we choose are $S = \{\text{E}, \text{A}\}$ and $S' = \{\text{E}, \text{AB}\}$. The quantum proof states for S and S' used in the experiment are $|\text{Q}_\text{proof}\rangle = (|\psi_\text{B}\rangle + |\psi_\text{AB}\rangle)/\sqrt{2} = (HH + VV)/\sqrt{2}$, and $|\text{Q}'_\text{proof}\rangle = (|\psi_\text{B}\rangle + |\psi_\text{A}\rangle)/\sqrt{2} = (HH + HV)/\sqrt{2}$, respectively.

In our experiment, $|\text{Q}_\text{proof}\rangle, |\text{Q}'_\text{proof}\rangle, |\psi_\text{A}\rangle$, and $|\psi_\text{B}\rangle$ are put into the core circuit with right multiplication by E, A, B, and AB. Our new protocol only requires one core circuit in each quantum circuit. In contrast, if one strictly follows the original protocol, at least five qubits are needed that contain two quantum labels of group elements and one ancillary qubit for reversible group element sampling. One also needs at least three group multiplications in the strict original circuit, whereas

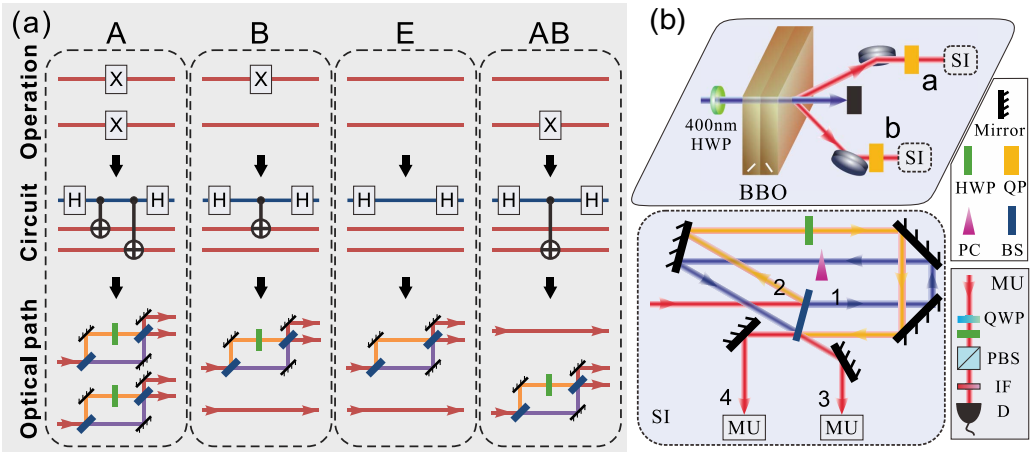

Fig. 2. Circuit mapping and experimental setup. (a) The circuits for group multiplications in the first line are deduced from the quantum labels for the elements. They are used to construct the core circuits for the verification process in the second line. Optical paths are presented in the third line. Here, two BSs building an MZI are used to play the role of two Hadamard operations on the control qubit, which is realized with the path information. One path is regarded as $|0\rangle$ and the other one is $|1\rangle$. An HWP is placed in $|1\rangle$ path to act as the CNOT gate on the polarization qubit with the optical axis at 45°. (b) Experimental setups. Entangled photon pairs are produced by pumping BBO and using quartz plates (QPs) on the above panel. Two photons are sent to the sides *a* and *b* respectively. On each side, an SI, shown on the bottom panel in detail, is constructed to realize the MZI. In an SI, an HWP is placed in $|1\rangle$ path (shown in orange beam and marked as 2) and a phase compensation (PC) crystal is located in $|0\rangle$ (shown in blue beam and marked as 1). A measurement unit (MU) consisting of a QWP, an HWP, a PBS, and a single-photon detector (D) equipped with an interferometer filter (IF) is placed on each output port (marked as 3 and 4) of the SI. Note, in this figure, unitary of multiplying by A is realized. By removing the SI, we can implement different quantum circuits.

the new method only requires one multiplication in each circuit. The full experimental setup of the new protocol is shown in Fig. 2(b). The input states are generated by pumping two identically cut Type I beta-barium-borate (BBO) crystals whose optic axes are aligned in mutually perpendicular planes [26] with an ultraviolet (UV) source. The UV pulses are frequency doubled from a mode-locked Ti:sapphire laser centered at 800 nm with 130 fs pulse width and 76 MHz repetition rate. After compensating the birefringence effect between H and V in BBO crystals with quartz plates (QPs), maximally entangled photon pairs of the forms $|\mathrm{Q}_{\mathrm{proof}}\rangle$ are produced [26]. Furthermore, by adjusting the polarization of pump pulses and downconversion photons, the other states of $|\psi_{\mathrm{B}}\rangle = |HH\rangle$, $|\psi_{\mathrm{A}}\rangle = |HV\rangle$, and $|\mathrm{Q}'_{\mathrm{proof}}\rangle = (|HH\rangle + |HV\rangle)/\sqrt{2}$ are produced. The input photons are then sent to one of the quantum circuits in Fig. 2 to perform the core circuit with different group multiplications.

In our setup, the Mach–Zehnder interferometer (MZI) is realized by a Sagnac interferometer in which the path information of photons is regarded as the control qubit [27]. In a Sagnac interferometer, an optical nonpolarization beam splitter (BS), worked as the Hadamard gates on control qubit, is used to separate the beam into two paths, 1 and 2, which are treated as the control qubit $|0\rangle$ and $|1\rangle$, respectively. Here, the BS is chosen to split 50:50 for 0° angle of incidence, which could decrease the difference of the split ratio of different polarizations. In the path $|1\rangle$, a half-wave plate (HWP) is used to implement CNOT gates set at 45° to reverse the photon polarization. The visibilities of two Sagnac interferometers are $96.7\% \pm 0.4\%$ and $95.9\% \pm 0.4\%$, respectively. Note that, for the circuit E with Es multiplication, there is no CNOT gate and the HWP is set at 0°. Beams 1 and 2 combine in the BS and then are separated as beams 3 and 4. The polarization of photons is analyzed on the outputs of beams 3 and 4 by polarization beam splitters (PBSs), HWPs, and quarter-wave plates (QWPs). The photons are detected by single-photon detectors (D) equipped with 3 nm interference filters (IFs).

For the circuit A, which implements the multiplication by A, the probability P_0 of detecting $|0\rangle$ equals the sum of the coincidence count (CC) of detectors located at *a*3 and *b*3 and the CC of detectors located at *a*4 and *b*4, where *a*3 is the output port 3 of the SI on the side of *a*, and similarly hereinafter. The probability P_1 of detecting $|1\rangle$ equals the sum of the CC of *a*3 and *b*4 and the CC of *a*4 and *b*3. On the other hand, for the case of circuit B, according to the corresponding mapping relation where the SI is only placed in the *a* side, the probability of detecting $|0\rangle$ equals the CC of *a*3 and *b*, and the probability of $|1\rangle$ equals the CC of *a*4 and *b*. Similar methods suit the other circuits AB and E.

Besides the interference visibility introduced above, two SIs are further verified with the input state of $(|HH\rangle + |VV\rangle)/\sqrt{2}$, which is prepared with a fidelity of $95.9\% \pm 1.0\%$. For the SI appearing in the E circuit, the output state generated from the CC of *a*3 and *b* remains the maximally entangled state and is achieved experimentally with a fidelity of $95.3\% \pm 1.0\%$. For the other interferometer that is used in circuit AB, without inserting the CNOT gate, the output state generated from the CC of *a* and *b*3 is also the same as the input state and is achieved with a fidelity of $94.2\% \pm 1.4\%$. We further verify other output cases of the interferometers and achieve high fidelities for them. For the input state $\frac{1}{\sqrt{2}}(\mathrm{B} + \mathrm{AB}) = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$, we present the detailed experimental real matrix and imaginary matrix of the outputs here, as shown in Figs. 3 and 4.

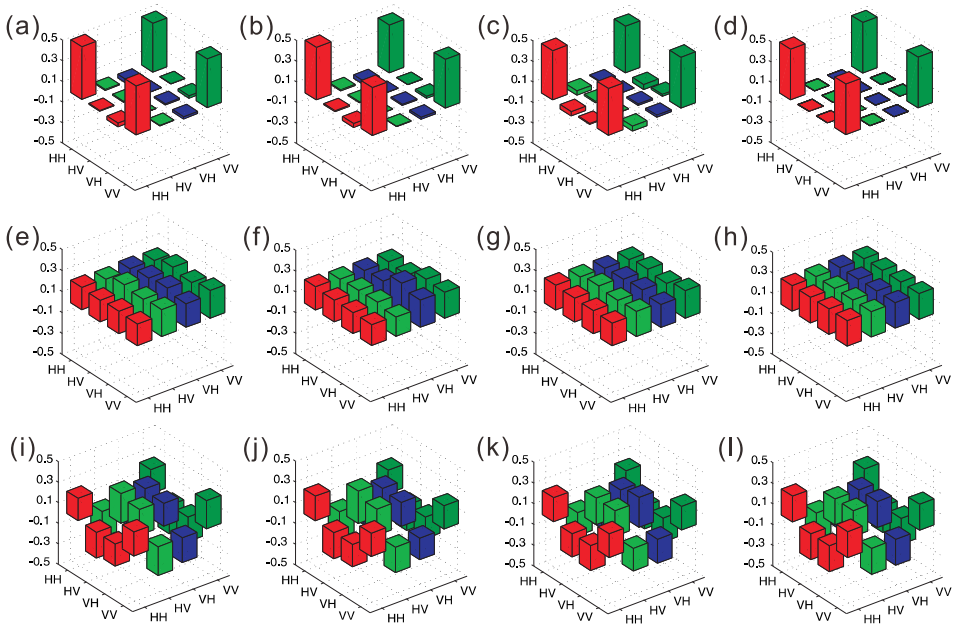

Fig. 3. Real parts of density matrices of the final output photons for the case with input state of $(|HH\rangle + |VV\rangle)/\sqrt{2}$. (a)–(c) Cases of initial state, output photons of $a3$ and b in E-type interferometer, output photons of a and $b3$ in AB-type interferometer without CNOT gate, respectively; (e)–(g) cases of output photons of $a3$ and $b3$ in A-type interferometer (with fidelity $92.6\% \pm 2.4\%$), $a3$ and b in B-type interferometer ($88.9\% \pm 0.7\%$), a and $b3$ in AB-type interferometer ($88.5\% \pm 1.2\%$), respectively; (i)–(k) cases of output photons of $a4$ and $b4$ in A-type interferometer ($98.0\% \pm 0.3\%$), $a4$ and b in B-type interferometer ($94.4\% \pm 0.3\%$), a and $b4$ in AB-type interferometer ($94.8\% \pm 0.9\%$), respectively; (d), (h), and (l) corresponding theoretical predictions.

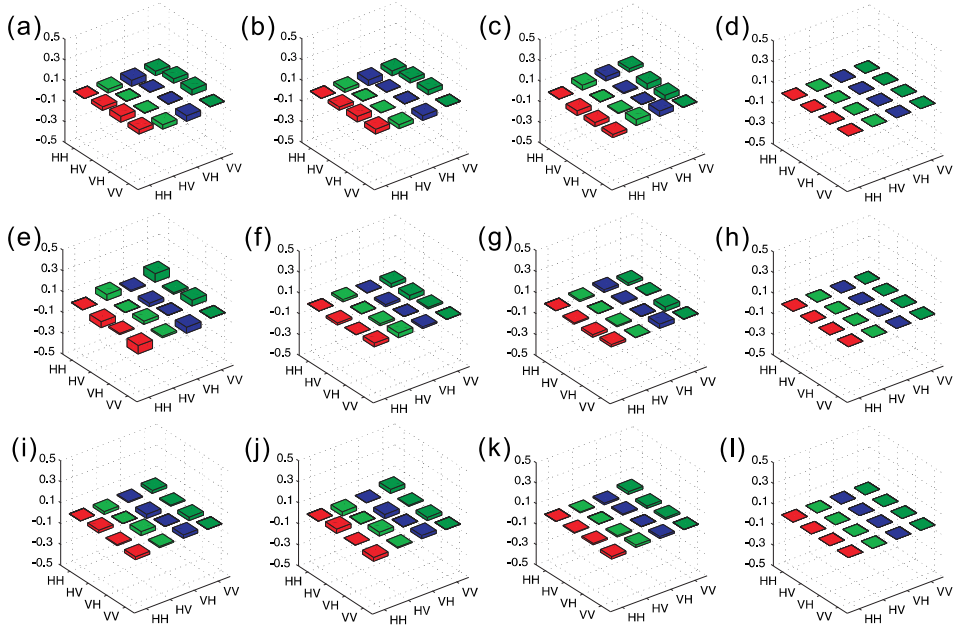

Fig. 4. Imaginary parts of density matrices of the final output photons for the case with input state of $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$. (a)–(c) Cases of initial state, output photons of $a3$ and b in E-type interferometer, output photons of a and $b3$ in AB-type interferometer without CNOT gate, respectively; (e)–(g) cases of output photons of $a3$ and $b3$ in A-type interferometer, $a3$ and b in B-type interferometer, a and $b3$ in AB-type interferometer, respectively; (i)–(k) cases of output photons of $a4$ and $b4$ in A-type interferometer, $a4$ and b in B-type interferometer, a and $b4$ in AB-type interferometer, respectively; (d), (h), and (l) corresponding theoretical predictions.

Equipped with the experiment setup, we first carried out our new process on the group S. To demonstrate the test channel in our verification process, the correct proof $|Q_{proof}\rangle$ as well as the bogus proofs $|Q'_{proof}\rangle, \psi_A$ and $|\psi_B\rangle$ is produced and sent to the core circuit with multiplication by A. A state passes the test if the control qubit is detected to be $|0\rangle$. The results are shown in Fig. 5(a). We find that the probabilities for a bogus proof to pass the state test do not exceed 0.518 ± 0.017 and have a significant gap toward the probability 0.955 ± 0.006 for a correct proof state $|Q_{proof}\rangle$ to pass. Then we show how the nonmembership of an element g can be verified with the correct proof state $|Q_{proof}\rangle$. The GNM of g is verified when $|1\rangle$ is detected in the core circuit with multiplication by g. The experimental result is shown in Fig. 5(b). We find the probabilities for $|Q_{proof}\rangle$ to be accepted are higher than 0.496 ± 0.009 for $B, AB \notin S$ and lower than 0.045 ± 0.006 for $E, A \in S$. The above analysis implies that if the prover sends m registers and the verifier chooses $m-1$ registers to test, the probability p_c for a group of correct proof state to be accepted is greater than $0.496 \times (0.955)^{m-1}$. In contrast, the probability for m bogus state to pass the tests is only $(0.518)^{m-1}$. For a general bogus proof, our theory can show that the probability p_s for it to be accepted can be bounded by $\frac{16}{7(m-1)}$. Therefore, the gap $p_c - p_s$ is maximized when $m = 15$ and the maximal value is 0.097.

For the other subgroup S', the result is similar. The bogus proofs become $|\psi_A\rangle$, $|\psi_B\rangle$, $|Q_{proof}\rangle$, and the correct proof becomes $|Q'_{proof}\rangle$. The probabilities for the bogus proofs to pass the test channel do not exceed 0.503 ± 0.008 and for the correct proof $|Q'_{proof}\rangle$, the corresponding probability is 0.980 ± 0.003, as shown in Fig. 5(c). We find that the probability for $|Q'_{proof}\rangle$ to be accepted when used for verifying GNM is higher than 0.481 ± 0.017 for $B, A \notin S'$ and is lower than 0.020 ± 0.003 for $E, AB \in S'$, as shown in Fig. 5(d). In this case, p_s is still bounded by $\frac{16}{7(m-1)}$ and $p_c = 0.481 \times (0.980)^{m-1}$. The gap $p_c - p_s$ is maximized when $m = 19$ and the maximal value is 0.207.

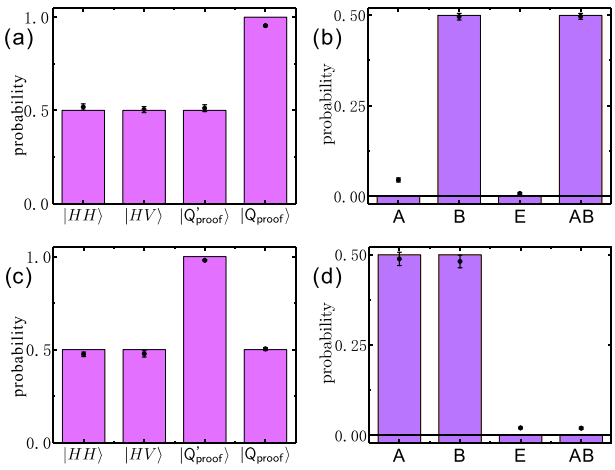

Fig. 5. Experimental results. (a), (c) Detecting probabilities of $|0\rangle$ with different input proof states for the circuit A and AB, respectively; (b), (d) probability for the proof states $|Q_{proof}\rangle$ and $|Q'_{proof}\rangle$ to prove GNM for every group element (detecting the control qubit in $|1\rangle$). The histograms and black points are theoretical and experimental results, respectively. All error bars are estimated to be standard deviation from the statistical variation of the photon counts, assumed to follow a Poisson distribution.

These completeness-soundness gaps strongly support the success of verification of GNM in the new protocol. Though the whole proof state contains more qubits, the number of qubits and operations in the circuit that the verifier needs to process at a time, which are more important to near-term devices, are greatly reduced.

4. CONCLUSION

In this work, we experimentally implement a verification process for GNM in an all-optical setup based on an ameliorative protocol in which the required quantum resources are greatly reduced. With multiplication of four group elements implemented by optical circuits, the process is accomplished on two subgroups consisting of two selected elements. As it is very likely that similar verification process of GNM can be used in other problems of finite groups, it will be interesting if this validity were formally proven and experimentally demonstrated. Furthermore, our novel verification process is helpful to construct more quantum protocols, which could be practical for near-term quantum devices.

Funding. National Key Research and Development Program of China (2016YFA0302700, 2017YFA0304100); National Natural Science Foundation of China (11821404, 11774335, 61725504, 61805227, 61975195, U19A2075, 11875160, U1801661); Anhui Initiative in Quantum Information Technologies (AHY060300, AHY020100); Key Research Program of Frontier Science, CAS (QYZDYSSW-SLH003); Science Foundation of the CAS (ZDRW-XH-2019-1); Fundamental Research Funds for the Central Universities (WK2030380017, WK2030380015, WK2470000026); Natural Science Foundation of Guangdong Province (2017B030308003); Key R&D Program of Guangdong Province (2018B030326001); Science, Technology and Innovation Commission of Shenzhen Municipality (JCYJ20170412152620376, JCYJ20170817105046702, KYTDPT20181011104202253); Economy, Trade and Information Commission of Shenzhen Municipality (201901161512); Guangdong Provincial Key Laboratory (2019B121203002).

Disclosures. The authors declare no conflicts of interest.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

†These authors contributed equally to this paper.

REFERENCES

1. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *35th Annual Symposium on Foundations of Computer Science* (IEEE, 1994), pp. 124–134.
2. A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman, "Exponential algorithmic speedup by a quantum walk," in *35th Annual ACM Symposium on Theory of Computing* (ACM, 2003), pp. 59–68.

3. M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, 2002).
4. S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," SIAM J. Comput. **18**, 186–208 (1989).
5. J. Watrous, "PSPACE has constant-round quantum interactive proof systems," Theor. Comput. Sci. **292**, 575–588 (2003).
6. F. Centrone, N. Kumar, E. Diamanti, and I. Kerenidis, "Experimental demonstration of quantum advantage for NP verification with limited information," Nat. Commun. **12**, 850 (2021).
7. A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, 2009), pp. 517–526.
8. J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation," Phys. Rev. A **96**, 012303 (2017).
9. S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, "Experimental verification of quantum computation," Nat. Phys. **9**, 727–731 (2013).
10. A. Broadbent, Z. Ji, F. Song, and J. Watrous, "Zero-knowledge proof systems for QMA," in *IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2016), pp. 31–40.
11. A. B. Grilo, W. Slofstra, and H. Yuen, "Perfect zero knowledge for quantum multiprover interactive proofs," in *IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2019), pp. 611–635.
12. Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, "MIP*= RE," arXiv:2001.04383 (2020).
13. A. Natarajan and J. Wright, "NEEXP is contained in MIP," in *IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2019), pp. 510–518.
14. M. Sipser, "Introduction to the theory of computation," ACM SIGACT News **27**, 27–29 (1996).
15. A. Y. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and Quantum Computation* (American Mathematical Society, 2002).
16. J. Watrous, "Quantum computational complexity," arXiv:0804.3401 (2008).
17. D. Aharonov and T. Naveh, "Quantum NP - a survey," arXiv:quant-ph/0210077 (2002).
18. H. Kobayashi, K. Matsumoto, and T. Yamakami, "Quantum Merlin-Arthur proof systems: are multiple Merlins more helpful to Arthur?" in *Algorithms and Computation* (Springer, 2003), pp. 189–198.
19. L. Babai, "Trading group theory for randomness," in *7th Annual ACM Symposium on Theory of Computing* (ACM, 1985), pp. 421–429.
20. L. Babai, "Bounded round interactive proofs in finite groups," SIAM J. Discrete Math. **5**, 88–111 (1992).
21. J. Watrous, "Succinct quantum proofs for properties of finite groups," in *41st Annual Symposium on Foundations of Computer Science* (IEEE, 2000), pp. 537–546.
22. J. Preskill, "Quantum computing in the NISQ era and beyond," Quantum **2**, 79 (2018).
23. F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," Nature **574**, 505–510 (2019).
24. L. Babai, "Local expansion of vertex-transitive graphs and random generation in finite groups," in *23rd Annual ACM Symposium on Theory of Computing* (ACM, 1991), pp. 164–174.
25. L. Babai and E. Szemerédi, "On the complexity of matrix group problems I," in *25th Annual Symposium on Foundations of Computer Science* (IEEE, 1984), pp. 229–240.
26. P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultrabright source of polarization-entangled photons," Phys. Rev. A **60**, R773–R776 (1999).
27. K. Sun, X.-J. Ye, Y. Xiao, X.-Y. Xu, Y.-C. Wu, J.-S. Xu, J.-L. Chen, C.-F. Li, and G.-C. Guo, "Demonstration of Einstein-Podolsky-Rosen steering with enhanced subchannel discrimination," Npj Quantum Inf. **4**, 12 (2018).