View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by St Andrews Research Repository

Research Article Vol. 28, No. 13 / 22 June 2020 / *Optics Express* 18917
Optics EXPRESS

Proof-of-principle demonstration of compiled Shor's algorithm using a quantum dot single-photon source

Zhao-Chen Duan,[1,2,6] Jin-Peng Li,[1,2,6] Jian Qin,[1,2] Ying Yu,[3] Yong-Heng Huo,[1,2] Sven Höfling,[1,4,5] Chao-Yang Lu,[1,2] Nai-Le Liu,[1,2] Kai Chen,[1,2,*] and Jian-Wei Pan[1,2]

[1] *Shanghai Branch, Department of Modern Physics and National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Shanghai 201315, China*
[2] *CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*
[3] *State Key Laboratory of Optoelectronic Materials and Technologies, School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, Guangdong 510275, China*
[4] *Technische Physik, Physikalische Institut and Wilhelm Conrad Röntgen-Center for Complex Material Systems, Universität Würzburg, Am Hubland, D-97074 Würzburg, Germany*
[5] *SUPA, School of Physics and Astronomy, University of St. Andrews, St. Andrews KY16 9SS, UK*
[6] *These authors contributed equally*
[*] *kaichen@ustc.edu.cn*

Abstract: We report a proof-of-principle demonstration of Shor's algorithm with photons generated by an on-demand semiconductor quantum dot single-photon source for the first time. A fully compiled version of Shor's algorithm for factoring 15 has been accomplished with a significantly reduced resource requirement that employs the four-photon cluster state. Genuine multiparticle entanglement properties are confirmed to reveal the quantum character of the algorithm and circuit. The implementation realizes the Shor's algorithm with deterministic photonic qubits, which opens new applications for cluster state beyond one-way quantum computing.

© 2020 Optical Society of America under the terms of the OSA Open Access Publishing Agreement

1. Introduction

Some quantum algorithms provide dramatic speedup in solving problems like factoring [1,2], which is difficult for current computers for large numbers. The security of widely used cryptography, like Rivest-Shamir-Adleman (RSA) public-key cryptosystem, relies on crucially the difficulty of factoring a large number to be product of two large prime numbers [3,4]. Remarkably, the Shor's algorithm utilizing quantum computer [1,2] provides an efficient way for factoring, thus directly threatens the RSA's security in the near future.

Demonstration of Shor's algorithm requires lots of qubits and gates that is beyond the current quantum technologies. Proof-of-principle demonstration, with some of the parameters being initially determined to reduce the resource requirement, is sufficient to characterize the core processes of Shor's algorithm [5]. This kind of demonstrations have been presented with systems ranging from liquid nuclear magnetic resonance [6], photonic qubits (qutrits) [7–10], superconducting circuits [11,12], to ion-trap [13]. Among these architectures, polarization encoded photonic qubits experience negligible decoherence and the fastest gates, are promising candidates for quantum computing [14]. All existing implementations of Shor's algorithm with photonic qubits employ photons generated from spontaneous parametric down-conversion (SPDC) sources [15]. Intrinsic noise of the SPDC, however, comes from multiphoton emission [16]. Therefore, it must be set to low efficiency for detectors to suppress unwanted multiphoton events, which, in return, pulls down the whole performance of quantum circuits. Semiconductor

#390209 https://doi.org/10.1364/OE.390209
Journal © 2020 Received 21 Feb 2020; revised 4 Jun 2020; accepted 4 Jun 2020; published 10 Jun 2020

quantum dot (QD) single-photon sources, which, however, are able to generate photons one by one [17], fit extremely well for this task. Recent progresses have demonstrated that photons can be deterministically generated with high extraction efficiency, single-photon purity, and photon indistinguishability altogether [18,19]. By embedding a single QD into a symmetry-broken microcavity, photons being generated exhibit high degrees of polarization [20]. Here, we present a proof-of-principle demonstration of Shor's algorithm using photons from QD.

2. Methods and experimental implementations

In number theory, a strategy for factoring an n-bit composite number $N = p \times q$, both p and q are odd primes with $p \neq q$, is as follows:

1. Find the base b and the order r that satisfy:
   (a) b is co-prime to N, and $0<b<N$,
   (b) r is a positive even integer,
   (c) $b^r \equiv 1 \pmod{N}$, and $b^{r/2} \not\equiv \pm 1 \pmod{N}$.
2. Calculate the greatest common divisor (GCD): $\gcd(b^{r/2} \pm 1, N)$.

Here, the remainders of modular arithmetic (https://en.wikipedia.org/wiki/modular_arithmetic) are non-negative and less than N. Two solutions of the GCD calculation are two nontrivial factors p and q, by which way a composite number can be efficiently factored.

The bottleneck of this algorithm lies in difficulty of selecting b and finding r satisfying $b^r \equiv 1 \pmod{N}$, or vice versa. For a classical computer, it needs at least $\exp[O(n^{1/3} \log^{2/3} n)]$ operations to complete this task [4,21]. Fortunately, Shor's algorithm utilizing a quantum computer provides an effective way to execute it in a polynomial complexity. The quantum routine of the Shor's algorithm needs two registers of qubits [2,5]: the argument register that employs l qubits to store the argument x, and the function register that employs $n = \lceil \log_2 N \rceil$ qubits to store the modular exponential function: $f(x) = b^x \bmod N$. Both x and $f(x)$ can be represented by binary integer sets of x_k and f_k satisfying $x = \sum_{k=0}^{l-1} 2^k x_k$, and $f(x) = \sum_{k=0}^{n-1} 2^k f_k$. The physical realization of the Shor's algorithm requires three distinct steps:

1. *Initialization*. Applying Hadamard gates on argument register so that the state $|0\rangle^{\otimes l}$ transforms to $|+\rangle^{\otimes l} = \sum_{x=0}^{2^l-1} |x\rangle/\sqrt{2^l}$, which is an equally weighted superposition. The number of digit for the argument register l is determined by an accuracy that we wish to estimate the order (usually $l \approx 2n$) [5]. A not gate is applied on the last qubit of the function register, transforms the initial state to be $|00\cdots01\rangle$.

2. *Modular exponentiation*. According to what Deutsch called "massive quantum parallelism" [22], one can calculate the modular exponential function $f(x)$ with several controlled-U_f gates, producing $\sum_{x=0}^{2^l-1} |x\rangle\, |f(x)\rangle/\sqrt{2^l}$.

3. *Inverse quantum Fourier transform (QFT)*. Owing to the fact that $f(x)$ exhibits periodicity, an inverse QFT can be then applied on the argument register to acquire "frequency", yielding $\sum_{x=0}^{2^l-1} \sum_{y=0}^{1-2^{-l}} \exp(2\pi ixy)|y\rangle\, |f(x)\rangle/2^l$ (the step of y is 2^{-l}).

Here, y is represented by binary fraction set of y_k satisfying $y = \sum_{k=1}^{l} y_k/2^k$. The probability amplitude reaches to peak if $y \approx j/r$ for any integer j. Thus the order can be extracted with high success rate.

However, even factoring the simplest number, $N = 15$, requires a total of 12 qubits for a proof-of-principle demonstration ($n = 4$, $l \approx 2n = 8$). It is quite challenging for current quantum techniques to implement completely the Shor's algorithm. Fortunately, the compiling technique

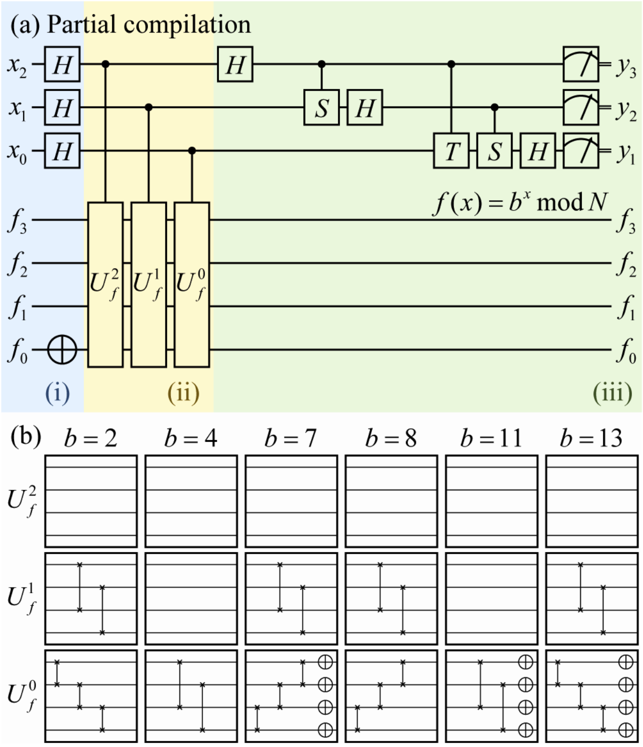

Fig. 1. (a) Quantum circuit for Shor's algorithm applied by partial compilation. It consists of three distinct steps: (i) *Initialization*, (ii) *Modular exponentiation*, and (iii) *Inverse QFT*. The modular exponentiation is implemented by several controlled-U_f gates. The details of U_f gates, which act as the quantum version of modular multipliers, are depicted in (b).

allows one to reduce the number of qubit resources. In $N = 15$ case, the base could be chosen from $b = 2, 4, 7, 8, 11, 13$. All elements satisfy the condition that $f(4) = 1$, or $r = 4$. Hence, only 2 qubits in the argument register are sufficient to exhibit the periodicity of $f(x)$. To avoid possible errors, an additional qubit is further exploited for the analysis of the answers. Therefore, it requires at least 7 qubits for a proof-of-principle demonstration ($n = 4$, $l = 3$). Figure 1(a) indicates the quantum circuit applied by this level of compilation, or partial compilation. Furthermore, a full compilation could then be implemented by further reduction of qubit requirement. As it is always true that $r<N$, the function register can be represented with fewer (only $n' = \lceil \log_2 r \rceil$) qubits. We define a new function: $F(x) = \log_2 [(-1)^{bx} f(x) \bmod N]$, which acts as a mapping of $f(x)$. It turns out that $F(x)$ maintains the periodicity of $f(x)$, in which the inverse QFT applied on the argument register is kept invariable [5]. The inverse QFT can be implemented in a semiclassical way that performs only single-qubit operations conditioned on measurement outcomes [23]. Thus, there is no need to perform two-qubit gates to achieve it. Moreover, from Fig. 1(b), the U_f^2 gates are always equivalent to identity operation. Hence, the qubit x_2 (or y_3) is not relevant to the rest, which the operations and measurements on that qubit can be performed independently. Therefore, this fully compiled version of Shor's algorithm for factoring $N = 15$ (or finding $r = 4$) only requires four-qubit entanglement ($n' = 2$, $l = 2$). In Fig. 2(a), we illustrate this fully compiled version of quantum circuit. In Fig. 2(b), we depict the details of U_F gates. For $b = 4$ or 11, the state after modular exponentiation, or the intermediate state, is only a two-qubit entanglement state that can be achieved with only one controlled-NOT gate. For $b = 2$ or 13, there are two sets of states with two-qubit entanglement that can be achieved by performing the same operation twice

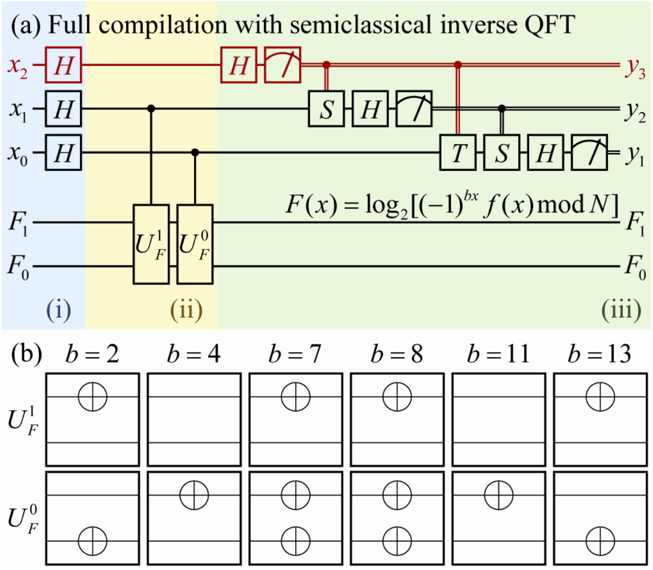

Fig. 2. (a) Quantum circuit for Shor's algorithm applied by full compilation. This circuit reveals the same process as that indicated in Fig. 1(a), but requires reduced number of qubits and gates. The modular exponentiation is implemented by controlled-U_F gates instead, while the inverse QFT is implemented in a semiclassical way. The qubit x_2 (or y_3, represented by colored wire) is not relevant to the others, which the operations and measurements can be performed independently. (b) Details of U_F gates, which act as the quantum version of modular adders.

as $b = 4$ or 11 case. The above two cases have already been demonstrated in previous literatures [8,9], while we will unveil here a more complicated case—$b = 7$ or 8. The intermediate state for this case is a genuine entanglement among all four qubits, which is of the form:

$$\frac{1}{2}\sum_{x=0}^{3} |x\rangle\, |F(x)\rangle = \frac{|00\rangle\, |00\rangle + |01\rangle\, |11\rangle + |10\rangle\, |10\rangle + |11\rangle\, |01\rangle}{2}. \quad (1)$$

The intermediate state represented by Eq. (1) is in fact equivalent to a four-qubit cluster (C_4) state [24], which can be achieved post-selectively with only linear optics in our photonic quantum architecture (See Appendix A).

The schematic of experimental setup is sketched in Fig. 3, which consists of four distinct steps:

1. *Single-photon emission*. The state-of-the-art QD is embedded into a micropillar cavity [18] with a diameter of 2 µm, and put into a cryostat cooled down to 4 K. Under resonant excitation with a repetition rate of 76 MHz [25], single photons can be deterministically generated. A cross-polarization configuration, which consists of several polarization optics, is applied to extinguish unwanted laser background. The photons applied to this task have a lifetime of ~60 ps, and counting rate of ~6.4 MHz on the superconducting nanowire single-photon detector (SNSPD) with a detection efficiency of ~80 %. In previous literature, single-photon purity is experimentally measured to be 0.973(1), and indistinguishability with two-photon emission-time separations of 13 ns and 14.7 µs are 0.939(3) and 0.900(3) [26,27].

2. *Active photon demultiplex*. Single photons collected by single-mode fiber (SMF) are divided into four different modes with active demultiplexers [27]. Each demultiplexer

consists of a Pockels cell (PC), a polarizing beam-splitter (PBS), and a half-wave plate (HWP). The PC has an extinction ratio of 100:1 and high transparency of 99 %. Driven by ~1800 V half-wave voltage, the polarization of single photons can be rotated by 90°. Then, a PBS with an extinction ratio of 2000:1 is used to convert different polarizations into different modes. Immediately after single photons are divided, an HWP aligned at 45° is applied on the reflection mode of PBS to invert the polarization. The photonic states of $|0\rangle$ and $|1\rangle$ are represented by $|H\rangle$ and $|V\rangle$, where $|H\rangle$ and $|V\rangle$ denote horizontal and vertical linear polarizations. All modes are initialized into the state $|0\rangle$ at this stage. Each mode finally propagates inside a SMF with different lengths to compensate time delays.

3. *C_4 state preparation*. The separated single photons after interference are projected into C_4 state represented by Eq. (1) in a post-selective way that if there is only one photon being detected at each mode. The HWPs aligned at 22.5° are equivalent to HADAMARD gates.

4. *Four-fold correlations*. We measure all output photons along $\{|H\rangle, |V\rangle\}$ basis using SNSPDs with PBSs, and register four-photon events. A pair of wave plates before each PBS act as single-qubit operations that enable one to measure along any desired basis.

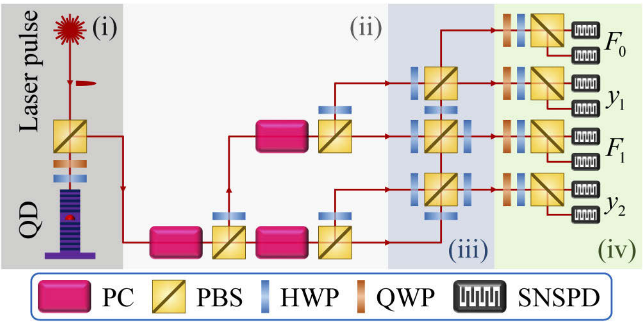

Fig. 3. The schematic of experimental setup. It consists of four distinct steps: (i) *Single-photon emission*, (ii) *Active demultiplex*, (iii) *C_4 state preparation*, and (iv) *Four-fold correlations*. All photonic states of $|0\rangle$ and $|1\rangle$ are represented by $|H\rangle$ and $|V\rangle$, where $|H\rangle$ and $|V\rangle$ denote horizontal and vertical linear polarizations. All HWPs in steps (ii) and (iii) are aligned at 45° and 22.5°, which act as NOT gates and HADAMARD gates respectively. A pair of wave plates aligned before each PBS in step (iv) enable detection along any desired basis. QD, quantum dot; PC, Pockels cell; PBS, polarizing beam-splitter; HWP, half-wave plate; QWP, quarter-wave plate; SNSPD, superconducting nanowire single-photon detector.

3. Results

The inverse QFT on the argument register of Eq. (1) results in a mixed state, therefore it is almost impossible to characterize the performance of the quantum circuit by estimating state fidelity. The intermediate state represented by Eq. (1) is the persistent four-qubit entanglement [28], one can thus perform measurements on that state to characterize the quantum circuit. The measurement is performed both qualitatively and quantitatively. For qualitative measurement, the four-fold correlations are performed by measuring all modes along $\{|H, |V\rangle\}$ and $\{|D\rangle, |A\rangle\}$ bases, where $|D\rangle$ and $|A\rangle$ denote diagonal (45°) and anti-diagonal (−45°) linear polarizations. Also two of four modes can be measured along $\{|R\rangle, |L\rangle\}$ basis instead, where $|R\rangle$ and $|L\rangle$ denote right and left circular polarizations. The results are shown in Fig. 4, where peaks in each pattern fit well with theoretical predictions described as Eqs. (5), (6), and (7) in Appendix A. As for quantitative measurement, one can evaluate fidelity of the state using stabilizer correlation measurements, since the cluster state can be fully described by its stabilizers [29]. The evaluated expectation values of stabilizer correlation measurements are listed in Table 1, where σ_0, σ_1, σ_2, and σ_3 correspond to Pauli matrices [21]. In our case, one can accomplish detections with only 9 measurements instead of a full tomography configuration. By averaging the expectation values of all stabilizer correlation measurements, the fidelity can be estimated to be 0.756(8), well above the classical limit of 0.5, indicating a genuine quantum computing in the modular exponentiation step.

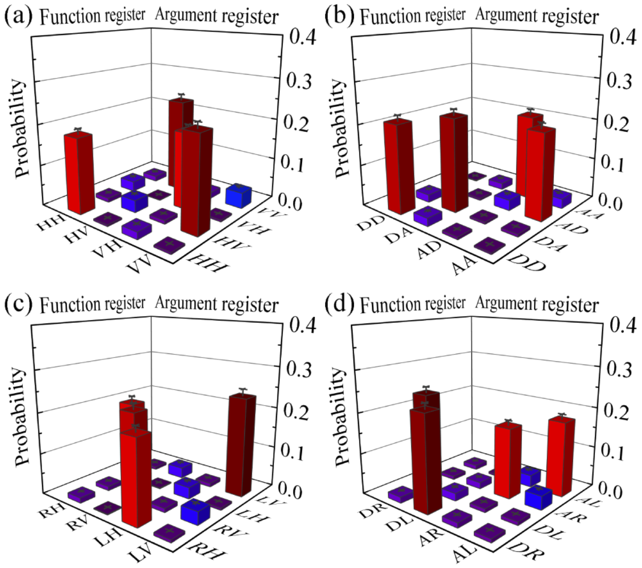

Fig. 4. Measured probability distributions of the intermediate state represented by Eq. (1) with (a) all modes along $\{|H\rangle, |V\rangle\}$ basis, (b) all modes along $\{|D\rangle, |A\rangle\}$ basis, and (c,d) two of four modes along $\{|R\rangle, |L\rangle\}$ basis instead. The effective four-fold counting rate is ~3.2 Hz, and each measurement takes ~5 min. Error bars, shown in gray lines with a cross at the top, arise from Poisson statistics for four-fold correlation counts. All data are adjusted by detectors' efficiency.

Table 1. Stabilizer correlation measurements of the intermediate state represented by Eq. (1). Since this state embodies genuine persistent four-qubit entanglement, one can characterize performance of quantum circuit by analyzing the state itself instead of the final answer. The cluster state's fidelity can be evaluated by averaging over all expectation values, yielding a value of 0.756(8). All values are derived from data adjusted by efficiency, while the uncertainties are represented by standard deviations.

Stabilizer	Expectation value	Stabilizer	Expectation value
$+\sigma_0\sigma_0 \otimes \sigma_0\sigma_0$	1.000 ± 0.011	$+\sigma_1\sigma_3 \otimes \sigma_1\sigma_3$	0.763 ± 0.047
$+\sigma_0\sigma_3 \otimes \sigma_0\sigma_3$	0.878 ± 0.021	$+\sigma_1\sigma_0 \otimes \sigma_1\sigma_0$	0.853 ± 0.020
$+\sigma_0\sigma_1 \otimes \sigma_1\sigma_1$	0.745 ± 0.032	$+\sigma_1\sigma_1 \otimes \sigma_0\sigma_1$	0.783 ± 0.032
$+\sigma_3\sigma_0 \otimes \sigma_3\sigma_3$	0.716 ± 0.032	$+\sigma_3\sigma_3 \otimes \sigma_3\sigma_0$	0.716 ± 0.032
$-\sigma_2\sigma_0 \otimes \sigma_2\sigma_3$	0.751 ± 0.034	$-\sigma_2\sigma_3 \otimes \sigma_2\sigma_0$	0.741 ± 0.034
$-\sigma_0\sigma_2 \otimes \sigma_1\sigma_2$	0.708 ± 0.030	$-\sigma_1\sigma_2 \otimes \sigma_0\sigma_2$	0.740 ± 0.030
$-\sigma_3\sigma_1 \otimes \sigma_2\sigma_2$	0.650 ± 0.037	$-\sigma_2\sigma_2 \otimes \sigma_3\sigma_1$	0.700 ± 0.030
$-\sigma_2\sigma_1 \otimes \sigma_3\sigma_2$	0.704 ± 0.034	$-\sigma_3\sigma_2 \otimes \sigma_2\sigma_1$	0.640 ± 0.032

At the final stage, one can implement inverse QFT to acquire the answer. A rotation of θ ($\theta = 0, \pi/2, \pi/4, \ldots$) along Z axis followed by a Hadamard operation with measurement along $\{|0\rangle,\ |1\rangle\}$ basis is equivalent to a measurement along $\{(|0\rangle \pm e^{-i\theta}|1\rangle)/\sqrt{2}\}$ basis [24], which has widely been used in characterization of the Greenberger-Horne-Zeilinger state [30]. To acquire the answer, one needs to analyze the measured data both qualitatively and quantitatively. Here, we analyze both $l = 2$ or 3 cases. Qualitatively, one can plot the probability distributions indicated in Figs. 5(a) and 5(b), for $l = 2$ and 3, respectively. It seems hard to distinguish any changes between two patterns, and peaks in both patterns appear at the position where $y = 0/4, 1/4, 2/4,$ and $3/4$, for which it is easy to estimate $r = 4$. Quantitatively, one can theoretically calculate the probability distributions from $r = 1$ to 4, which are plotted in Figs. 7 and 8 in Appendix B for $l = 2$ and 3 cases, and compare our measured data with them. One can use the square of statistical overlap (SSO) [31], which is used to quantify similarities between measured and expected probability distributions, to characterize the comparisons. The SSO, derived from statistical overlap (SO) [32], is defined as: $\gamma = (\sum_{y=0}^{7/8} \sqrt{m_y e_y})^2$, where m_y and e_y denote measured and expected probabilities of the state $|y\rangle$. From the comparison results listed in Table 2, the maximums of $\gamma = 0.999(41)$ and 0.996(41) for $l = 2$ and 3 appear at the place where $r = 4$. But for $l = 2$, a high SSO of 0.956(39) also appears at the order of $r = 3$, meaning that imperfections of quantum circuits may probably result in a wrong answer. Both qualitative and quantitative analyses reveal the same answer of $r = 4$. Therefore, 3 qubits in the argument register are needed at least to extract the correct answers with a higher success rate. After the answer has been acquired, the solutions of $\gcd(b^{r/2} \pm 1, N)$ are two nontrivial factors of the composite number, which are calculated to be 3 and 5 for $N = 15$.

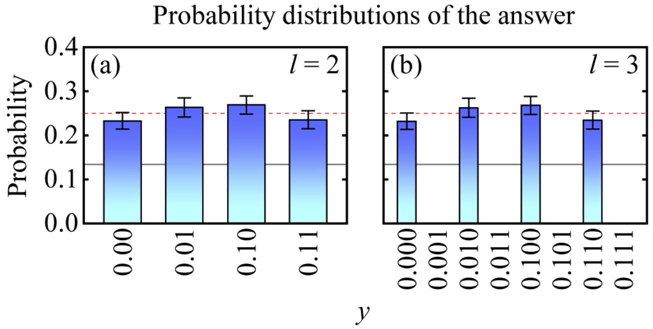

Fig. 5. Measured probability distributions for the order finding with (a) 2 qubits and (b) 3 qubits in the argument register. These patterns fit well with the theoretical predictions of $P(y = j/4) = 0.25$ (dashed lines), and both reveal the same answer of $r = 4$. Two nontrivial factors of $N = 15$ are finally calculated to be: $\gcd(b^{r/2} \pm 1, 15) = 3$ and 5, where $b = 7$ or 8.

Table 2. Calculated square of statistical overlap (SSO) from $r = 1$ to 4 for $l = 2$ and 3. The SSOs reach to maximum, as shown in bold values, at $r = 4$, which can acquire the same answer as those from Fig. 5. But a high SSO, as shown in *italic* value, appears at $r = 3$ for $l = 2$, which may probably result in a wrong answer. Therefore, 3 qubits in the argument register are required at least to avoid possible errors caused by the imperfect quantum circuits.

SSO	$l = 2$	$l = 3$
$r = 1$	0.233 ± 0.009	0.232 ± 0.009
$r = 2$	0.501 ± 0.020	0.499 ± 0.020
$r = 3$	*0.956 ± 0.039*	0.429 ± 0.012
$r = 4$	**0.999 ± 0.041**	**0.996 ± 0.041**

Optics EXPRESS

4. Discussions

We have so far presented a proof-of-principle demonstration of compiled Shor's algorithm with photons generated from QD single-photon source. A genuine four-photon entanglement has been observed during the experiment. The fidelity is limited by imperfection of single-photon source. For simplicity, we assume the final fidelity F is affected by single-qubit gate fidelity F_s and two-qubit gate fidelity F_d. For an m-photon entanglement, it needs at least $m-1$ two-qubit gates to prepare the state. Thus, one can estimate the final fidelity via $F = F_s^m F_d^{m-1}$. From the data of independently measured qubit in $l = 3$ case, the single-qubit gate fidelity, caused by single-qubit operations, can reach to near-unity ($F_s \approx 0.997$). Therefore, the final fidelity will mainly be limited by two-qubit gate fidelity. The noise from residual laser leakage and sometimes photons from other QDs lead to multiphoton events, which deteriorate the single-photon purity. Impure single photons, together with other effects like charge noise, spin noise, and phonon sidebands [33,34], decrease the indistinguishability. These imperfections contribute to unwanted four-fold correlation background and reduce the fidelity of the prepared state. From the fidelity of 0.756(8), one can estimate the two-qubit gate fidelity to be 0.914(5). Our experiment can be extended to 8 photons, where the largest order that can be found should be $r = 16$. Compared to the optimal SPDC sources nowadays with 12-photon entanglement [30], our QD single-photon source shows shortcomings in this aspect. However, the purity and indistinguishability of this solid-state single-photon source can be in principle both improved to near-unity [34]. Thus, the number of photons being entangled can be greatly extended.

The QD used in current experiment has a lifetime of ~60 ps, which is much shorter than the timescale for any single-qubit or two-qubit gates of ion-trap or superconducting circuit architectures [35], meaning a higher correlation counting rate (or a shorter computation time) could be achieved by increasing the repetition rate in QD architecture. The correlation counting rate can be estimated via $R = R_0\eta$, where R_0 and η represent repetition rate (76 MHz in current experiment) and system efficiency (including preparation, operation, and detection efficiency). Assuming that both QD- and SPDC-based experiments experience the same repetition rate and detection efficiency. The preparation efficiency for QD-based experiment includes the efficiency at the incident ends (fiber output) η_{QD}, which relates to incident photon brightness, and that of optical switches η_{PC} (mainly affected by PC). And the preparation efficiency for SPDC-based experiment only includes the efficiency at the incident ends η_{SPDC}. The operation efficiency denotes the success rate for each configuration. Therefore, the m-fold correlation counting rate for QD- and SPDC-based experiments satisfy $R_{\mathrm{QD}} \propto (R_0/m)(\eta_{\mathrm{QD}}^m \eta_{\mathrm{PC}}^{m-1})/2^{m-1}$ and $R_{\mathrm{SPDC}} \propto R_0 \eta_{\mathrm{SPDC}}^{m/2}/2^{m/2-1}$ respectively. For direct comparison, we calculate the ratio between the counting rates of both sources, yielding $R_{\mathrm{QD}}/R_{\mathrm{SPDC}} = (\eta_{\mathrm{QD}}\eta_{\mathrm{PC}}/\sqrt{2\eta_{\mathrm{SPDC}}})^m/(m\eta_{\mathrm{PC}})$. To show the advantages of QD-based experiment, it must satisfy the condition that $\eta_{\mathrm{QD}}\eta_{\mathrm{PC}}/\sqrt{2\eta_{\mathrm{SPDC}}}>1$. Consider the counting rate of ~6.4 MHz, detection efficiency of ~80 %, and $\eta_{\mathrm{PC}} \approx 84\%$, the value of $\eta_{\mathrm{QD}}\eta_{\mathrm{PC}}/\sqrt{2\eta_{\mathrm{SPDC}}}$ is approximately 0.28 compared to the optimal SPDC source [30]. Even the optimal QD single-photon source can only increase this value to ~0.68 [36]. Note that due to the trade-off between fidelity and efficiency for SPDC source, η_{SPDC} almost reaches to near-optimal. In contrast, high efficiency, high single-photon purity, and high indistinguishability have simultaneously been achieved on QD single-photon sources [18,19]. By embedding that QD into an asymmetric microcavity, both indistinguishability and efficiency are expected to reach near-unity [20]. The value of $\eta_{\mathrm{QD}}\eta_{\mathrm{PC}}/\sqrt{2\eta_{\mathrm{SPDC}}}$ is expected to be more than 2, which makes QD single-photon sources perform a better scalability in quantum computing.

Furthermore, we have presented techniques that simplify complicated quantum operations like modular exponentiation, and adapted the easy-to-get quantum states like C_4 state to the specific quantum task. This is an illustration of dramatic simplification in quantum computing. We have also presented strategies for evaluation of the circuit and analysis of the data, which enable proper characterizations of the quantum task. Although imperfect quantum circuit, mainly caused by possibly poor entanglement fidelity, limits its scalability, it has little effects on the computation results due to the answer is acquired from the similarity between measured and expected data.

5. Summary

In summary, we have achieved a proof-of-principle demonstration of small-scale quantum algorithm with photons generated from deterministic single-photon source. We have presented every necessary stage of an $r = 4$ order finding routine with only four single photons. Our approach of compilation reduces the required qubits from $3\lceil\log_2 N\rceil$ to $2\lceil\log_2 r\rceil$ ($r<N$), and simplifies the gates by transforming modular multipliers to modular adders, finding a way to make complicated quantum problems feasible. Genuine persistent entanglement [28] among all photonic qubits has been maintained during the experiment, indicating quantum characters of the algorithm and the circuit. Since the answer is acquired from the maximum of a parameter that quantifies the similarity between measured and expected results, it is robust to the imperfections of the quantum circuit. Besides, our experiment opens new applications for the cluster state beyond one-way quantum computing [24]. By combining the compilation technique with qubit recycling [37], one may accomplish the task with further reduced number of qubits. To scale up for factoring larger numbers, finding larger orders, or even attaining a full-scale demonstration that requires auxiliary qubits to store, and finally erase, the intermediate results [5], challenges mainly come from the limited scalability caused by poor fidelity of multiphoton entanglement due to noise from residual laser leakage, charge and spin noise, phonon sidebands, and process of the post-selective entanglement generation.

Appendix A: C_4 state preparation and characterization

The photonic states of $|0\rangle$ and $|1\rangle$ are represented by $|H\rangle$ and $|V\rangle$. For a polarizing beam-splitter, as shown in Fig. 6(a), it has two input modes of 1 and 2, and two output modes of 3 and 4. If two input photons are initialized into $(|H\rangle_1 + |V\rangle_1)(|H\rangle_2 + |V\rangle_2)/2$, the state of output photons would be $(|H\rangle_4|H\rangle_3 + |H\rangle_4|V\rangle_4 + |V\rangle_3|H\rangle_3 + |V\rangle_3|V\rangle_4)/2$. Since we post-select two photons in the opposite output modes simultaneously, the state is then projected into $(|H\rangle_3|H\rangle_4 + |V\rangle_3|V\rangle_4)/\sqrt{2}$ with a success rate of 1/2, by which way one can prepare entangled state on-demand.

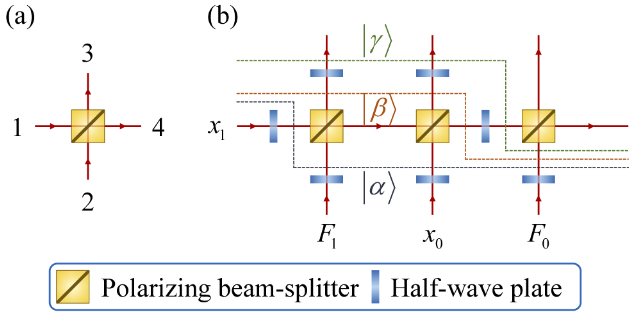

Fig. 6. (a) A polarizing beam-splitter with input modes of 1, 2, and output modes of 3, 4. (b) The schematic for photonic C_4 state preparation. Three dashed lines represent three distinct photonic quantum states $|\alpha\rangle$, $|\beta\rangle$, and $|\gamma\rangle$. Labels remain in the reflection modes of polarizing beam-splitters.

The schematic for photonic C_4 state preparation is shown in Fig. 6(b). All half-wave plates in Fig. 6(b) are aligned at 22.5° to act as HADAMARD gates, while three dashed lines denote three distinct photonic quantum states for C_4 state preparation. At the beginning, all four photons are initialized into $|H\rangle$. A half-wave plate in each input mode turns four photons into:

$$|\alpha\rangle = \frac{(|H\rangle + |V\rangle)^{\otimes 4}}{4}. \tag{2}$$

Then, two polarizing beam-splitters project the whole state into:

$$|\beta\rangle = \frac{(|H\rangle^{\otimes 3} + |V\rangle^{\otimes 3}) \otimes (|H\rangle + |V\rangle)}{2}. \tag{3}$$

Next, three half-wave plates in x_1, x_0, and F_1 modes transform the system into:

$$|\gamma\rangle = \frac{(|HH\rangle\ |H\rangle + |HV\rangle\ |V\rangle + |VH\rangle\ |V\rangle + |VV\rangle\ |H\rangle) \otimes (|H\rangle + |V\rangle)}{2\sqrt{2}}. \tag{4}$$

At last, the x_0 and F_0 modes interfere at the final polarizing beam-splitter to achieve the C$_4$ state, by which way the intermediate state for current experimental configuration can be successfully prepared.

The intermediate state is characterized in a qualitative way. The photonic C$_4$ state can be written in $\{|H\rangle,\ |V\rangle\}$ basis:

$$|\mathrm{C}_4\rangle = \frac{|HH\rangle\ |HH\rangle + |HV\rangle\ |VV\rangle + |VH\rangle\ |VH\rangle + |VV\rangle\ |HV\rangle}{2}, \tag{5}$$

and measurements of all modes along $\{|H\rangle,\ |V\rangle\}$ basis will result in four peaks. The peaks reveal only partial of possible entanglement property, additional measurements are still necessary. One can use $\{|D\rangle,\ |A\rangle\}$ basis, which can be written as the superposition of $\{|H\rangle,\ |V\rangle\}$ basis, to equivalently describe the C$_4$ state. The state $|D\rangle$ is defined as $(|H\rangle + |V\rangle)/\sqrt{2}$, while the state $|A\rangle$ is defined as $(|H\rangle - |V\rangle)/\sqrt{2}$. Then, the C$_4$ state can be written as:

$$|\mathrm{C}_4\rangle = \frac{|DD\rangle\ |DD\rangle + |DA\rangle\ |DA\rangle + |AD\rangle\ |AA\rangle + |AA\rangle\ |AD\rangle}{2}, \tag{6}$$

and measurements of all modes along $\{|D\rangle,\ |A\rangle\}$ basis also result in four peaks.

Next, one can also equivalently describe the C$_4$ state with two of four modes use $\{|R\rangle,\ |L\rangle\}$ basis instead. Like $\{|D\rangle,\ |A\rangle\}$ basis, $\{|R\rangle,\ |L\rangle\}$ basis can also be represented by the superposition of $\{|H\rangle,\ |V\rangle\}$ basis: $|R\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$, and $|L\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$. Therefore, the C$_4$ state can also be written as the followings:

$$\begin{aligned}|\mathrm{C}_4\rangle &= \frac{|RH\rangle\ |LH\rangle - i|RV\rangle\ |RV\rangle + |LH\rangle\ |RH\rangle + i|LV\rangle\ |LV\rangle}{2} \\ &= \frac{|DR\rangle\ |DL\rangle + |DL\rangle\ |DR\rangle + |AR\rangle\ |AR\rangle + |AL\rangle\ |AL\rangle}{2},\end{aligned} \tag{7}$$

and measurements along these two sets of basis both result in four peaks.

Appendix B: analysis of inverse QFT

Since the order finding routine results in the periodic function $F(x)$, the intermediate state of routine can be rewritten as: $\sum_{x=0}^{2^l-1} |x\rangle\ |F(x)\rangle/\sqrt{2^l} = \sum_{j=0}^{j<r} |F(j)\rangle \sum_m |rm+j\rangle/\sqrt{2^l}$, where m, j are non-negative integers satisfying $rm + j < 2^l$. By tracing out the function register, the argument register will be projected into a mixed state. We introduce density matrix to represent the mixed state, by which the argument register can be represented as: $\rho = \sum_{j=0}^{j<r} |\psi_j\rangle\langle\psi_j|$, where $|\psi_j\rangle = \sum_m |rm+j\rangle/\sqrt{2^l}$. Each element of density matrix $|\psi_j\rangle$ exhibits periodicity with a period of r, in which $l = \lceil \log_2 r \rceil$ qubits are sufficient to construct it. For the current experimental

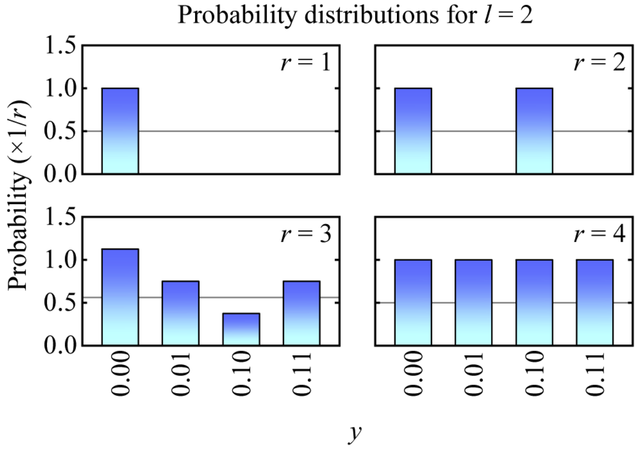

Fig. 7. Expected probability distributions for the answers of the inverse QFT, with the order from 1 to 4, and 2 qubits in the argument register. Gray line in each plot represents half of the maximum (and the same as in Fig. 8), and values exceed this line are identified as "peaks", which seem to appear at $y = j/r$.

parameter of $r = 4$, only 2 qubits are needed in the argument register. One can theoretically calculate expected probability distributions of the inverse QFT applied on ρ with the order from 1 to 4, which have been indicated in Fig. 7.

As seen from Fig. 7, the peaks seem to appear at $y = j/r$ [for $r = 3$, three peaks are equivalent to appearing at $y = 0/3 = 0.00$(binary), $y = 1/3 \approx 0.01$(binary), and $y = 2/3 \approx 0.11$(binary)]. In the experiment, we extract the order by comparing measured data with expected ones. However, imperfections of quantum circuits may lead to a wrong answer, it is necessary to quantify the measured results. We firstly perform the cross comparisons between expected data indicated in Fig. 7. We use squared statistical overlap (SSO) [31], which is defined as: $\gamma = (\sum_{y=0}^{7/8} \sqrt{m_y e_y})^2$, to quantify the comparisons. By substituting expected probabilities into both m_y and e_y, one can calculate SSOs for the cross comparisons. The calculated SSOs for $l = 2$ are listed in the left part of Table 3.

Table 3. Calculated square of statistical overlap (SSO) for cross comparisons of the patterns shown in Fig. 7 for $l = 2$ (left part of the Table) and Fig. 8 for $l = 3$ (right part of the Table). The values reach to unity, as shown in bold format, if the patterns are exactly the same. Some high values, as shown in *italic* format, represent the wrong answers that may probably caused by imperfect quantum circuits.

		$l = 2$			$r = 1$	$r = 2$	$r = 3$	$r = 4$	SSO
$r = 1$	**1.000**				**1.000**	0.500	0.344	0.250	$r = 1$
$r = 2$	0.500	**1.000**				**1.000**	0.291	0.500	$r = 2$
$r = 3$	0.375	0.466	**1.000**				**1.000**	0.399	$r = 3$
$r = 4$	0.250	0.500	*0.966*	**1.000**				**1.000**	$r = 4$
SSO	$r = 1$	$r = 2$	$r = 3$	$r = 4$			$l = 3$		

In Table 3, the maximum of SSO ($\gamma = 1$, as represented with **bold** values) appears in the position on the diagonal, meaning the extracted answer equals to the expected. However, for $r = 3$ and 4, a high SSO of $\gamma = 0.966$ (as represented with *italic* values) appears off the diagonal, which may result errors due to the imperfect quantum circuits. An additional qubit can be applied on the argument register to avoid this. The expected probability distributions for $l = 3$ are shown in Fig. 8, and the calculated SSOs for cross comparisons of the calculated data for $l = 3$ are listed in the right part of Table 3 respectively. Here, high SSOs no longer appear in the position off the diagonal of Table 3. Therefore, 3 qubits are needed at least that make the quantum circuit be more robust to noise.

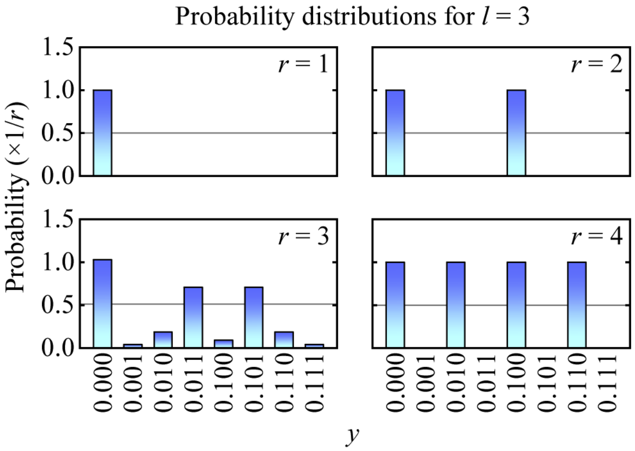

Fig. 8. Expected probability distributions for the answers of the inverse QFT, with the order from 1 to 4, and 3 qubits in the argument register. Peaks in these plots look sharper than those in Fig. 7, meaning an additional qubit makes the quantum circuit to be more robust to noise.

Funding

National Natural Science Foundation of China (11575174, 11674308, 11704424, 11774326, 11874346); Chinese Academy of Sciences; National Key Research and Development Program of China.

Disclosures

The authors declare no conflicts of interest.

References

1. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, (IEEE, 1994), pp. 124–134.
2. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Rev. **41**(2), 303–332 (1999).
3. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM **21**(2), 120–126 (1978).
4. A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," Rev. Mod. Phys. **68**(3), 733–753 (1996).
5. D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, "Efficient networks for quantum factoring," Phys. Rev. A **54**(2), 1034–1063 (1996).
6. L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature **414**(6866), 883–887 (2001).
7. C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, "Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits," Phys. Rev. Lett. **99**(25), 250504 (2007).
8. B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, "Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement," Phys. Rev. Lett. **99**(25), 250505 (2007).
9. A. Politi, J. C. F. Matthews, and J. L. O'Brien, "Shor's quantum factoring algorithm on a photonic chip," Science **325**(5945), 1221 (2009).

10. E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," Nat. Photonics **6**(11), 773–776 (2012).
11. E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland, and J. M. Martinis, "Computing prime factors with a Josephson phase qubit quantum processor," Nat. Phys. **8**(10), 719–723 (2012).
12. M. Amico, Z. H. Saleem, and M. Kumph, "Experimental study of Shor's factoring algorithm using the IBM Q experience," Phys. Rev. A **100**(1), 012305 (2019).
13. T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, "Realization of a scalable Shor algorithm," Science **351**(6277), 1068–1070 (2016).
14. R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger, "High-speed linear optics quantum computing using active feed-forward," Nature **445**(7123), 65–69 (2007).
15. P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," Phys. Rev. Lett. **75**(24), 4337–4341 (1995).
16. J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski, "Multiphoton entanglement and interferometry," Rev. Mod. Phys. **84**(2), 777–838 (2012).
17. P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoglu, "A quantum dot single-photon turnstile device," Science **290**(5500), 2282–2285 (2000).
18. X. Ding, Y. He, Z.-C. Duan, N. Gregersen, M.-C. Chen, S. Unsleber, S. Maier, C. Schneider, M. Kamp, S. Höfling, C.-Y. Lu, and J.-W. Pan, "On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar," Phys. Rev. Lett. **116**(2), 020401 (2016).
19. N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Antón, J. Demory, C. Gómez, I. Sagnes, L.-K. N. Daniel, A. Lemaître, A. Auffèves, A. G. White, L. Lanco, and P. Senellart, "Near-optimal single-photon sources in the solid state," Nat. Photonics **10**(5), 340–345 (2016).
20. H. Wang, Y.-M. He, T.-H. Chung, H. Hu, Y. Yu, S. Chen, X. Ding, M.-C. Chen, J. Qin, X. Yang, R.-Z. Liu, Z.-C. Duan, J.-P. Li, S. Gerhardt, K. Winkler, J. Jurkat, L.-J. Wang, N. Gregersen, Y.-H. Huo, Q. Dai, S. Yu, S. Höfling, C.-Y. Lu, and J.-W. Pan, "Towards optimal single-photon sources from polarized microcavities," Nat. Photonics **13**(11), 770–775 (2019).
21. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2010), 10th ed.
22. D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," Proc. R. Soc. London, Ser. A **400**(1818), 97–117 (1985).
23. R. B. Griffiths and C.-S. Niu, "Semiclassical Fourier transform for quantum computation," Phys. Rev. Lett. **76**(17), 3228–3231 (1996).
24. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, "Experimental one-way quantum computing," Nature **434**(7030), 169–176 (2005).
25. Y.-M. He, Y. He, Y.-J. Wei, D. Wu, M. Atatüre, C. Schneider, S. Höfling, M. Kamp, C.-Y. Lu, and J.-W. Pan, "On-demand semiconductor single-photon source with near-unity indistinguishability," Nat. Nanotechnol. **8**(3), 213–217 (2013).
26. H. Wang, Z.-C. Duan, Y.-H. Li, S. Chen, J.-P. Li, Y.-M. He, M.-C. Chen, Y. He, X. Ding, C.-Z. Peng, C. Schneider, M. Kamp, S. Höfling, C.-Y. Lu, and J.-W. Pan, "Near-transform-limited single photons from an efficient solid-state quantum emitter," Phys. Rev. Lett. **116**(21), 213601 (2016).
27. H. Wang, Y. He, Y.-H. Li, Z.-E. Su, B. Li, H.-L. Huang, X. Ding, M.-C. Chen, C. Liu, J. Qin, J.-P. Li, Y.-M. He, C. Schneider, M. Kamp, C.-Z. Peng, S. Höfling, C.-Y. Lu, and J.-W. Pan, "High-efficiency multiphoton boson sampling," Nat. Photonics **11**(6), 361–365 (2017).
28. H. J. Briegel and R. Raussendorf, "Persistent entanglement in arrays of interacting particles," Phys. Rev. Lett. **86**(5), 910–913 (2001).
29. N. Kiesel, C. Schmid, U. Weber, G. Tóth, O. Gühne, R. Ursin, and H. Weinfurter, "Experimental analysis of a four-qubit photon cluster state," Phys. Rev. Lett. **95**(21), 210502 (2005).
30. H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, L. Zhang, Z. Wang, L. You, X.-L. Wang, X. Jiang, L. Li, Y.-A. Chen, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, "12-photon entanglement and scalable scattershot boson sampling with optimal entangled-photon pairs from parametric down-conversion," Phys. Rev. Lett. **121**(25), 250505 (2018).
31. J. Chiaverini, J. Britton, D. Leibfried, E. Knill, M. D. Barrett, R. B. Blakestad, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, T. Schaetz, and D. J. Wineland, "Implementation of the semiclassical quantum Fourier transform in a scalable system," Science **308**(5724), 997–1000 (2005).
32. C. A. Fuchs, "Distinguishability and accessible information in quantum theory," Ph.D. dissertation, University of New Mexico (1995).
33. A. V. Kuhlmann, J. Houel, A. Ludwig, L. Greuter, D. Reuter, A. D. Wieck, M. Poggio, and R. J. Warburton, "Charge noise and spin noise in a semiconductor quantum device," Nat. Phys. **9**(9), 570–575 (2013).
34. P. Senellart, G. Solomon, and A. White, "High-performance semiconductor quantum-dot single-photon sources," Nat. Nanotechnol. **12**(11), 1026–1039 (2017).

35. N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Experimental comparison of two quantum computing architectures," Proc. Natl. Acad. Sci. **114**(13), 3305–3310 (2017).

36. H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, L.-X. You, Z. Wang, C. Schneider, J. J. Renema, S. Höfling, C.-Y. Lu, and J.-W. Pan, "Boson sampling with 20 input photons and a 60-mode interferometer in a 10^{14}-dimensional Hilbert space," Phys. Rev. Lett. **123**(25), 250503 (2019).

37. S. Parker and M. B. Plenio, "Efficient factorization with a single pure qubit and log$N$ mixed qubits," Phys. Rev. Lett. **85**(14), 3049–3052 (2000).

94.174.223.231 {ts '2020-07-29 07:18:04'}