Experimental study of quantum uncertainty from lack of information

Zhao, Yuan Yuan; Rozpędek, Filip; Hou, Zhibo; Wu, Kang Da; Xiang, Guo Yong; Li, Chuan Feng; Guo, Guang Can

Citation (APA)

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

ARTICLE   OPEN

Experimental study of quantum uncertainty from lack of information

Yuan-Yuan Zhao [1,2,3,7], Filip Rozpędek [4,5,6,7], Zhibo Hou[1,3], Kang-Da Wu[1,3], Guo-Yong Xiang [1,3✉], Chuan-Feng Li [1,3] and Guang-Can Guo[1,3]

Quantum uncertainty is a well-known property of quantum mechanics that states the impossibility of predicting measurement outcomes of multiple incompatible observables simultaneously. In contrast, the uncertainty in the classical domain comes from the lack of information about the exact state of the system. One may naturally ask, whether the quantum uncertainty is indeed a fully intrinsic property of the quantum theory, or whether similar to the classical domain lack of knowledge about specific parts of the physical system might be the source of this uncertainty. This question has been addressed in the previous literature where the authors argue that in the entropic formulation of the uncertainty principle that can be illustrated using the so-called, guessing games, indeed such lack of information has a significant contribution to the arising quantum uncertainty. Here we investigate this issue experimentally by implementing the corresponding two-dimensional and three-dimensional guessing games. Our results confirm that within the guessing-game framework, the quantum uncertainty to a large extent relies on the fact that quantum information determining the key properties of the game is stored in the degrees of freedom that remain inaccessible to the guessing party. Moreover, we offer an experimentally compact method to construct the high-dimensional Fourier gate which is a major building block for various tasks in quantum computation, quantum communication, and quantum metrology.

INTRODUCTION

In classical physics, one can predict the outcomes of simultaneous measurements of various observables performed on the same physical system with arbitrary precision, provided that one is in possession of measuring devices that allow for reaching sufficiently high accuracy. However, the quantum theory imposes intrinsic limitations on one's ability to make such measurement predictions for the incompatible observables. The first statement which quantified this quantum uncertainty was originally proposed by Heisenberg[1] and then rigorously proven by Kennard[2] in 1927. This statement applies to two maximally incompatible observables of position and momentum of a particle and the uncertainty is characterized in terms of the standard deviation. Their work was then generalized to any two bounded Hermitian observables by Robertson[3] as:

$$\Delta S \cdot \Delta T \geq \frac{1}{2} |\langle \psi | [S, T] | \psi \rangle|, \qquad (1)$$

where ΔS (ΔT) denotes the standard deviation of the distribution of outcomes when observable S (T) is measured on quantum state $|\psi\rangle$.

Unfortunately, there are various shortcomings to Robertson's uncertainty relation (see e.g.[4]) of which the most notable one is that its right hand side depends on the input state. This results in the fact that one can find states $|\psi\rangle$ for which it is impossible to predict the measurement outcome of neither S nor T with certainty, yet the bound becomes trivially zero when evaluated on $|\psi\rangle$. A natural way to overcome these limitations is to consider entropic formulations of the quantum uncertainty principle which allow for state-independent bounds and provide information-theoretic interpretations of the uncertainty[4].

For rank-one projective measurements on the finite-dimensional Hilbert space, an example of such a formulation is the well-known entropic uncertainty relation due to Maassen and Uffink[5],

$$H(S) + H(T) \geq \log_2 \frac{1}{c}, \qquad (2)$$

where $H(S)$ is Shannon's entropy of the probability distribution of the outcomes when S is measured and similarly for T. The term c on the right hand side denotes the maximum overlap of the observables, that is $c = \max_{ij} |\langle s_i | t_j \rangle|^2$, where $|s_i\rangle$ ($|t_j\rangle$) denotes the eigenstate of S (T). From the inequality (2), we can see that the uncertainty always exists ($\log_2 \frac{1}{c} \neq 0$) as long as S and T do not share any common eigenvector. It is then natural to raise the question regarding the origin of this uncertainty, since we already know that it is not related to the precision of the measuring apparatus.

Here we experimentally investigate this question with regard to a so-called guessing game[6] that provides an operational interpretation to the entropic formulation of the uncertainty principle. In such a guessing game one attempts to guess the outcome of a measurement on a state that one can freely prepare, where the measured observable is not predetermined, but is chosen uniformly at random from a set of two incompatible observables. Not only does the guessing game perspective provide us with useful insights into the foundational aspects of the uncertainty principle but it also makes the entropic

[1]Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China. [2]Peng Cheng Laboratory, Shenzhen 518052, China. [3]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China. [4]QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands. [5]Kavli Institute of Nanoscience, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands. [6]Pritzker School of Molecular Engineering, University of Chicago, Chicago, IL 60637, USA. [7]These authors contributed equally: Yuan-Yuan Zhao, Filip Rozpędek. ✉email: gyxiang@ustc.edu.cn

formulation of this principle a useful tool for proving security of various quantum cryptographic protocols[4]. In[7] the authors have shown that in this formulation of the uncertainty principle, not all of the quantum uncertainty, and in some cases even none, should be thought of as intrinsic to the quantum nature of this game. In fact it can be attributed to the guessing party's lack of *quantum* information about the choice of the measured observable. Revealing this quantum information enables the guessing party to significantly decrease, and in some cases even completely eliminate the observed uncertainty.

Here we experimentally verify the main claims of[7]. That is, by experimentally implementing the discussed guessing game in which the quantum information about the state of the measuring apparatus is revealed to the guessing party, we verify that the lack of access to this information is a key contributor to the arising uncertainty. Furthermore, we propose an innovative way to construct the high-dimensional quantum Fourier transform.

Fourier transform is one of the most important tools in quantum information processing, especially in quantum algorithms involving phase estimation, including the order-finding problem and the factoring problem[8]. A notable example is Shor's factoring algorithm which shows quantum advantages over its classical counterparts[9]. With the applications in quantum state tomography and quantum key distribution, quantum Fourier transforms are usually used to generate the mutually unbiased bases for extracting more information from the system[10–12].

Since the quantum Fourier transform occupies such an important position in quantum information and computation, people explore many protocols to implement it in different physical systems, such as superconducting system[13], trapped ions[14], photons[15,16], and nuclear magnetic resonance systems[17]. In our work, the high-quality two-dimensional and three-dimensional Fourier transforms are implemented on the path degree of freedom (DoF) of a single photon. Then the controlled Fourier gates with the two-dimensional control system are also realized. In our experiment all the visibilities of the three interferometers used to construct the quantum Fourier gate for $d = 2$ guessing game and six interferometers in the case of the $d = 3$ guessing game, are higher than 0.98. In comparison with other DoFs of the photon, e.g., the time-bin and the orbital angular momentum, the path DoF has its advantages and is much easier to control with common beam splitters and waveplates. Furthermore, the method we adopt to construct the Fourier gate may inspire other ways to manipulate the path-encoded qudits on the integrated quantum photonic device.

To construct the three-dimensional Fourier gate, we develop an experimentally friendly structure HBD-HWP-HBD, i.e., two horizontally placed beam displacers (HBDs) with a half-wave plate (HWP) inserted between them, to realize the principle component R_y, the single-qubit rotation gate around y-axis. This HBD-HWP-HBD structure eases the complexity of the original scheme[18] and reduces the scale of the setup. To be specific, for the three-dimensional Fourier transform implemented in the experiment, three interferometers are constructed instead of six ones with the 50:50 BSs. Meanwhile, the parallel distribution structure of the beams in our method enhances the stability of the experimental setup and makes it more robust to the environmental noise.

The paper is structured as follows. In the Result section, we first introduce the framework of the guessing game and provide a high-level overview of our results. We then describe the experimental results in detail and discuss their implications for verifying the claims of[7]. We conclude in the Discussion section where we explain the implications of our results for quantum cryptography and discuss the possible extensions of the studied guessing game that could potentially be realized on a modified version of our experimental setup. Finally, in the Methods section, we describe our optical implementation of this game, as well as

the settings of our experimental devices that allow us to prepare quantum states needed to verify the claims of the paper.

RESULTS

Guessing game

In this subsection, we review the framework and the results of[7] which form the basis for our experiment. We depict the considered guessing game (also referred to as the uncertainty game), firstly proposed by Berta et al.[6] in Fig. 1. In the game, Bob prepares the system B in state ρ_B and sends it to Alice. Then Alice performs one of the two pre-agreed measurements S and T on the system according to a random coin flip contained in the two-dimensional register R. She announces the chosen measurement to Bob who wants to guess Alice's outcome. In particular, Bob aims to minimize his uncertainty about Alice's measurement outcome X by choosing a suitable probe state ρ_B. The only scenario in which Bob can win the game with probability one is the game in which S and T share at least one common eigenvector, which corresponds to $\log_2 \frac{1}{c} = 0$ in the entropic uncertainty relation (2). In this situation, Bob prepares the probe state ρ_B as the common eigenstate of S and T, which enables him to predict the outcome of either of the measurements with certainty.

For the purpose of this paper it will be helpful to represent this game in a form of a quantum circuit as shown in Fig. 2. In this case let us assume that the measurement performed on register B in this circuit corresponds to measuring observable S. Moreover, let us assume that the observable T is related to S through the relation $T = U^\dagger S U$, where U is the unitary operation shown on the circuit. Hence, if the classical coin contained in register R is in state $|0\rangle$, then Alice measures observable S on register B, while if the coin is in state $|1\rangle$, then Alice applies operation U to the state on B, followed by the same measurement, which effectively leads to the measurement of the observable T on B. After that, Bob measures the state on R in the standard basis to find out what the outcome of the coin flip was and hence which observable has been chosen by Alice.

A complete mathematical description of this game, in which initially Bob does not know the outcome of the coin flip in R requires us to set ρ_R to a maximally mixed state. Then, Alice's measurement outcome $X = x$ leaves the register R in the state ρ_R^x, and Bob's probability of guessing Alice's outcome is exactly the probability of how well he can distinguish all the states $\{\rho_R^x\}$. However, R describes a random coin flip and therefore all $\{\rho_R^x\}$ will be diagonal in the standard basis (see Supplementary Note 1 for details). This implies that Bob's optimal measurement is the
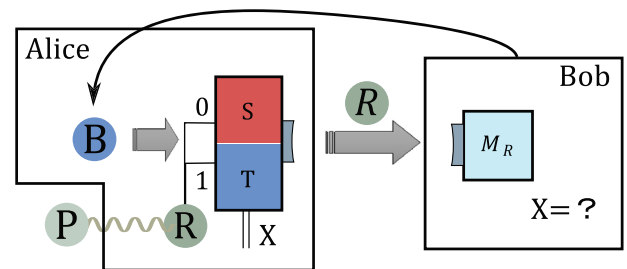

Fig. 1 Guessing game. In the d-dimensional guessing game, Bob prepares a quantum state ρ_B of dimension d and sends it to Alice. Then Alice performs the measurement S or T on the system ρ_B according to the two-dimensional register state ρ_R through a quantum control as shown in Fig. 2. After Alice completes the measurement, Bob tries to guess Alice's measurement outcome $X = x$ by measuring the register state ρ_R^x. In this process, R can be entangled with a system P, which remains inaccessible to Bob. Since some information about Alice's measurement process can be contained in that register P, in that case Bob cannot obtain full quantum information about Alice's measurement.
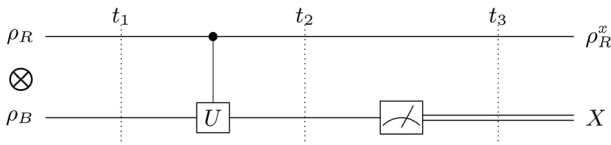
Fig. 2 Uncertainty game as a quantum circuit. Initially, at time t_1, Alice's register R and Bob's system B do not share any correlations. Then Alice makes a choice of the measured observable based on the state of the (possibly quantum) coin in R by performing a conditional rotation U on B. She then performs a measurement of the observable S on B to obtain the measurement outcome X. If the register R is classical, i.e. it is diagonal on the standard basis, then these two operations of Alice effectively perform a random measurement of S or T. If there is some non-zero coherence in register R, then the effective measurement can no longer be described as a random choice of one of the two observables. After that at time t_3 Alice sends R to Bob. Bob then wants to guess Alice's outcome $X = x$ by trying to distinguish the states $\{\rho_R^x\}$. Note that if R is classical, then the correlations between the two systems at time t_2 can also only be classical and all the states $\{\rho_R^x\}$ will be classical as well, implying that the optimal measurement of Bob corresponds to simply checking which one of the two observables Alice has chosen to measure. If R contains coherence, then quantum correlations between the two registers can arise at time t_2 and Bob can better distinguish the states $\{\rho_R^x\}$ by performing a measurement that takes this coherence into account. Figure taken from[7] with modifications under the licenses/CC BY 3.0 https://creativecommons.org/licenses/by/3.0/.

Z-basis measurement which simply checks which one of the two observables Alice has measured, as discussed before.

Clearly, the classical coin flip used to choose the measurement of one of the two observables S and T inputs a classical randomness in the game and hence could be responsible for the arising inability of Bob to perfectly predict the measurement outcome of Alice, as suggested and then further investigated in[7]. In this work, the authors analyze the consequences of removing this source of classical randomness by giving Bob access to the purification of that coin flip. In this way Bob has all the information about the corresponding choice of the observable to be measured and consequently this choice is now done on the quantum level. Clearly it is also possible that only some part of the purification of the coin flip is accessible to Bob and this is illustrated by the entangled registers R and P in Fig. 1, where P is the register to which Bob never has access.

From the perspective of the quantum circuit in Fig. 2, for the generalized game the state on R is no longer diagonal in the standard basis and so the coherence of ρ_R implies that the choice of the measured observable is now performed through a quantum control. Moreover, after Alice performs her measurement, the resulting states $\{\rho_R^x\}$ are, in general, also no longer diagonal in the standard basis. Hence, Bob can now increase his guessing probability by applying a judiciously chosen measurement which extracts additional useful information from the off-diagonal coherence terms in R.

This guessing game enables us to seek a deeper understanding of the quantum uncertainty and to distinguish between the uncertainty stemming from Bob's lack of information (including the classical and the quantum information) and the intrinsic (unavoidable) uncertainty. We provide a high-level mathematical description of this guessing game framework in Supplementary Note 1 while further details can be found in[7].

Let us first shed some light on the form of the state in register R. The form of this register determines the information that Bob has about the choice of the observable to be measured and therefore it determines his level of lack of knowledge about the measurement process. In the case of full lack of knowledge the two-dimensional register R represents a random coin and so $\rho_R = \mathbb{I}/2$. In the case when Bob possesses all the information about the

measurement process, ρ_R would be a pure state and since we would like it to correspond to the scenario in which both measurements were chosen with equal probability, it is natural to set $\rho_R = |+\rangle\langle+|$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. One can then interpolate between the two cases by parameterizing ρ_R using a $\gamma \in [0, 1]$ parameter as follows:

$$\rho_R(\gamma) = \frac{1}{2}(|0\rangle\langle0| + |1\rangle\langle1| + \gamma|0\rangle\langle1| + \gamma|1\rangle\langle0|). \tag{3}$$

The physical meaning of γ is discussed in Supplementary Note 1, while further details can be found in[7].

We note that we effectively have a whole family of guessing games, each of them corresponding to a specific configuration of the parameter set (γ, d). Here $\gamma \in [0, 1]$ is the coherence parameter described above, while $d = \{2, 3, \dots\}$ describes the dimension of the game. Specifically, d determines the number of possible outcomes of Alice's measurement and the dimension of the input state ρ_B.

In order to extract all the possible potential intrinsic uncertainty, the two measurements S and T that Alice performs are set to correspond to measuring in mutually unbiased bases. A natural choice for such bases is to set S to be an observable corresponding to the measurement in the standard basis and T to be an observable corresponding to the measurement in the Fourier basis.

Let us first have a quick look at the $d = 2$ game. In this case the two measurements S and T correspond to the measurements in the standard and the Hadamard bases, respectively. After optimizing over all input states of Bob and his later measurement of the register R, it has been shown in[7] that the maximum achievable guessing probability is given by:

$$P_{\text{guess}}^{\max}(\gamma, d = 2) = \frac{1}{2}\left(1 + \frac{\sqrt{2 + 2\gamma^2}}{2}\right). \tag{4}$$

In particular, $P_{\text{guess}}^{\max}(\gamma, d = 2) = 1$ when $\gamma = 1$. In this case, Bob can perfectly predict Alice's measurement outcome, and all the uncertainty is due to the lack of information. The work of[7] also examines the link between uncertainty and the lack of information for higher-dimensional games with $d > 2$. In these cases perfect guessing turns out to be no longer possible which shows the existence of the intrinsic uncertainty in those higher dimensions.

In the following, we implement the $d = 2$ and $d = 3$ guessing games, and experimentally study the relation between the coherence of the register R and Bob's uncertainty about Alice's measurement outcome in order to verify the theoretical predictions of[7]. Specifically, for both the $d = 2$ and $d = 3$ guessing games with the chosen values of $\gamma > 0$, we observe a guessing probability, which is larger than $P_{\text{guess}}^{\max}(\gamma = 0, d)$. In this way we verify that Bob's uncertainty arising in the scenario when the system R is a classical coin, can be reduced by providing him with access to the purification of that classical coin flip. For the $d = 2$ game we also observe that the larger the coherence parameter γ, the larger the experimentally observed guessing probability of Bob. Hence we can experimentally outperform the minimum possible amount of uncertainty for a given amount of revealed quantum information, by giving the guessing party additional quantum information about the state of the measurement apparatus. Finally, for the $d = 2$ game with the largest possible value of γ that we have been able to realize experimentally, the observed guessing probability becomes close to one. In other words, for the scenario in which we give the guessing party access to almost all the discussed quantum information, we observe almost no uncertainty at all which verifies the theoretical prediction of[7], that for the $d = 2$ game there is no intrinsic uncertainty. The small amount of uncertainty that remains is directly established to be a result of the specific noise processes in our physical setup.
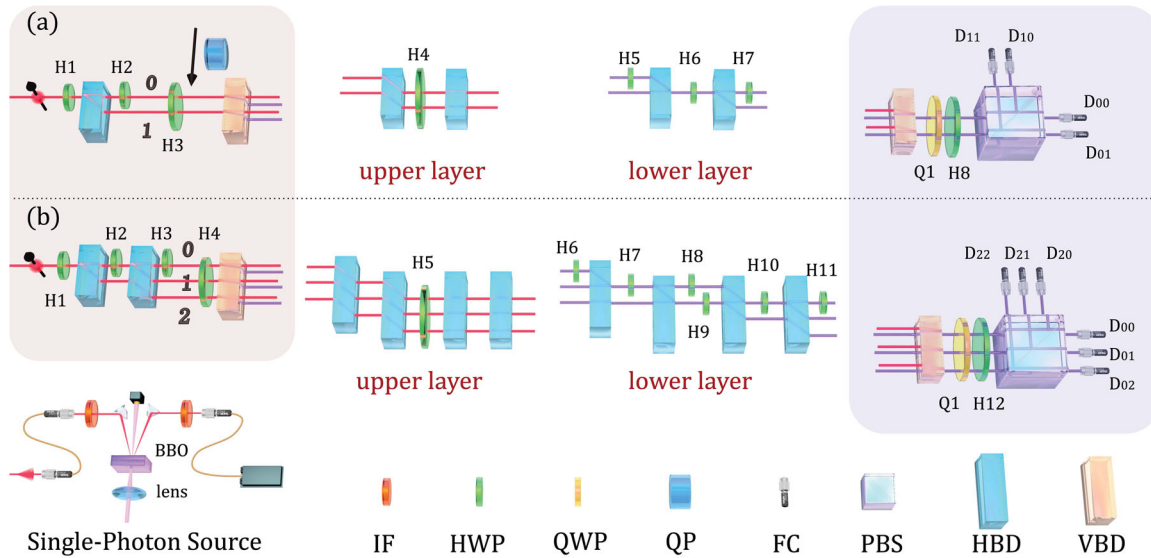
Fig. 3 Experimental setup. (a) $d=2$ guessing game. (b) $d=3$ guessing game. The single-photon is prepared by detecting one of the photons from a photon-pair generated in the Type-II spontaneous parametric down-conversion process. The whole setup consists of three modules: the state preparation part (red region), the controlled Fourier gate (white region), and the measurement part (purple region). Firstly, Bob prepares the system B in state ρ_B and Alice prepares the register R in state ρ_{R_r}, and those two systems are uncorrelated at module 1. Then a controlled Fourier gate is applied to the systems to correlate them. At last, Alice measures the system B to obtain outcome X and Bob measures the system R in some optimal basis to help him guess X. In our experiment, the systems B and R are encoded in different degrees of freedom of a photon: the horizontally spatial modes marked as "0", "1" and "2" and the different path layers marked as upper layer "u" and lower layer "l", respectively. Therefore, if the register R is in state $|u\rangle$ ($|l\rangle$), then the photon passes through the upper (lower) layer and undergoes an identity (Fourier) transformation as shown by the red (purple) lines. In the end, Alice needs to perform a non-demolition measurement, which is very difficult to realize in practice[33], before sending the system R to Bob. Here we perform both measurements simultaneously to ensure the efficiency. Abbreviations: IF interference filter, HWP half-wave plat, QWP quarter-wave plate, QP quartz plate, FC fiber coupler, PBS polarizing beam splitter, HB, horizontally placed beam displacer, VBD vertically placed beam displacer, BBO beta-barium-borate crystal.

In our experiment, we use the single photon system to implement the guessing game, and the basic idea is to use two independent DoFs of the photon to encode the system state ρ_B and the register state ρ_R, respectively. Specifically, as illustrated in Fig. 3, the system B is encoded in the horizontal paths marked as "0", "1" and "2". The measurement basis choice register R is encoded in the independent sets of paths marked as upper layer "u" and lower layer "l". More detailed information about the experimental implementation of guessing games can be found in Methods section.

Results for the two-dimensional guessing game

While the classical randomness is adopted in the guessing game, Bob's maximum achievable guessing probability is $P_{guess}^{max}(\gamma=0, d=2) = (2+\sqrt{2})/4$. In our experiment, however, we observe that for 10 out of 11 data points with $\gamma > 0$, $P_{guess}^{exp}(\gamma>0, d=2) > P_{guess}^{max}(\gamma=0, d=2)$. Here the superscript "exp" refers to the experimentally observed value, see the blue data points in Fig. 4(b). This can be ascribed to the quantum information held in register R and verifies that indeed there is uncertainty in the $\gamma=0$ game which comes from lack of information about the state of the purification register P.

Moreover, we see that P_{guess}^{exp} increases with γ. Specifically for all $0 \le \gamma < 0.9810$, we have observed an experimental value $P_{guess}^{exp}(\gamma+\delta, d=2)$ for some $0 < \delta < 0.2258$ such that $P_{guess}^{exp}(\gamma+\delta, d=2) > P_{guess}^{max}(\gamma, d=2)$, see Supplementary Note 2, where we give the detailed values of P_{guess}^{exp} and P_{guess}^{max} for each γ. As $P_{guess}^{max}(\gamma, d=2)$, plotted as the solid red line in Fig. 4(b), is the optimal guessing probability for a given γ, it is in fact an upper bound on that achievable probability. Hence, we have experimentally verified that for every γ in that region we can perform better than the corresponding upper bound by giving Bob more

access to the purification register (i.e. by experimentally increasing γ to $\gamma + \delta$). Therefore our experiment verifies that indeed the more quantum information about the measuring process is given to Bob, the higher is the probability of him winning the game.

As we mentioned earlier, the optimal guessing probability for $\gamma = 1$ is $P_{guess}^{max}(\gamma=1, d=2) = 1$, which means that Bob can guess Alice's measurement result perfectly if he knows all the information of her measurement basis choice on the quantum level. In our experiment, the highest value we observe is $P_{guess}^{exp}(\gamma, d=2) = 0.9953 \pm 0.0003$, see Fig. 4(a) where we show the detected probabilities for all the output ports for this scenario. The fact that we cannot reach $P_{guess}^{max}(\gamma=1, d=2) = 1$ can be ascribed to two main reasons. The first one is related to the fact that we cannot prepare the perfect state $\rho_R(\gamma=1)$. Specifically, the maximal estimated γ we obtained in the experiment is $\gamma = 0.9918 \pm 0.0009$, and the fidelity between the experimentally prepared state and the theoretical state $\rho_R(\gamma=0.9918)$ is 0.9996. The second reason is the fact that the visibility of the interferometer composed of the two vertically placed beam displacers (VBDs) stays about 0.99 when collecting the data. This results in a dephasing error on the states $\rho_R^x(\gamma=0.9918, d=2, \rho_B)$. The detailed error analysis for $d=2$ guessing game is given in Supplementary Note 4.

Results for the three-dimensional guessing game

For the $d=3$ scenario, implementing the game for the largest γ achievable in our experimental setup, given by $\gamma = 0.9918$, and using the best-known strategy results in the experimental guessing probability of $P_{guess}^{exp}(\gamma=0.9918, d=3) = 0.9611 \pm 0.001$ (see data "3" in Fig. 5). However, experimental procedures are subject to noise, which in many practical scenarios is nonisotropic and hence has a more severe effect on some states than others. Therefore it is possible that for our experimental setup the highest observed
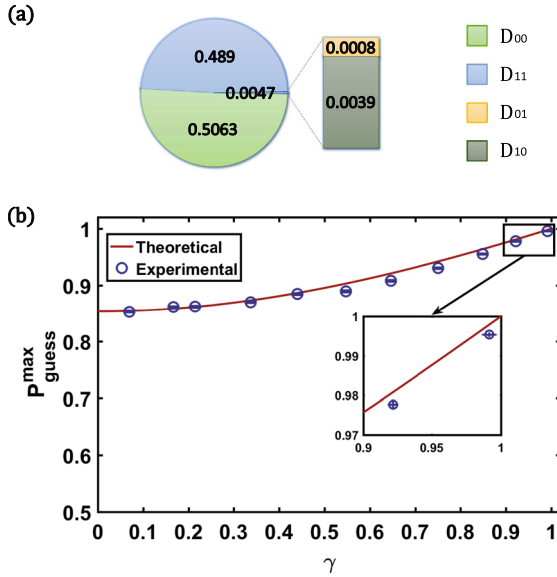
(a)

0.489
0.0047
0.5063

0.0008
0.0039

- D_{00}
- D_{11}
- D_{01}
- D_{10}

(b)

Fig. 4   The experimental results for the $d = 2$ guessing game. From the experimentally prepared state ρ_R^{exp} with the maximal purity, we estimate $\gamma = 0.9918 \pm 0.0009$. With this γ, we obtain the maximal guessing probability $P_{guess}^{exp}(\gamma, d = 2) = 0.9953 \pm 0.0003$ and the detected probabilities for each output port are shown in (**a**). In (**b**), we vary the degree of coherence of the register state ρ_R to find the relation between P_{guess}^{max} and γ. The analytical solution is plotted as the red line, while the experimental results are given as the blue circles. The x-bars are the standard deviations obtained by repeating the quantum state reconstruction algorithm for input data randomly generated from the experimentally obtained probability distributions. The y-bars are obtained directly from the detection probabilities in D_{00}, D_{01}, D_{10} and D_{11}.
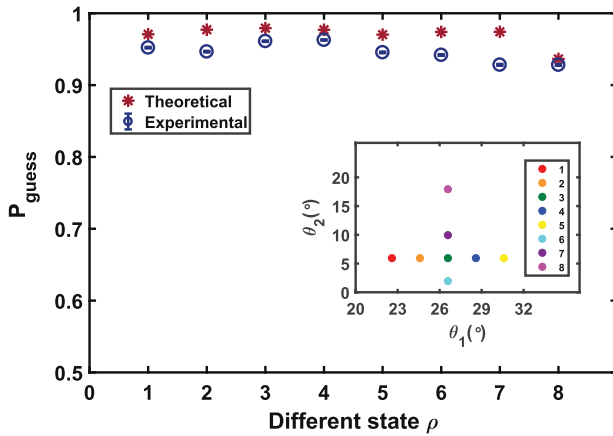

Fig. 5   Different strategies for the $d = 3$ guessing game. The probabilities of the successful guessing in the experiment are shown as the blue circles with the theoretically predicted values shown as the red stars. For each strategy, the probe state is prepared with H1, H2, and two HBDs in Fig. 3(b). The best-known strategy corresponds to data "3" and the corresponding setting of H1 (θ_1) and H2 (θ_2) for the input state preparation is shown as the green dot in the inset figure, meanwhile, the settings for other strategies are shown as the other colored dots. Notice that for the data point "8" the theoretically predicted value is much lower than for the other states. This is because the input state of data point "8" lies much further away from the best-known strategy of data point "3" than all the other considered states, as can be seen on the inset. More information about the settings of the waveplates H1, H2, Q1, H12 and the detailed numerical values of the corresponding guessing probabilities are given in Supplementary Note 2.

guessing probability could occur for a slightly different strategy than the one predicted in a noiseless scenario. To maximize our observed guessing probability and to obtain further insight into the effect of noise in our experiment, we test some other guessing strategies. Specifically, we choose various input states around the one stated above and modulate Bob's measurement to make sure the measurement is optimal for each state. From the results in Fig. 5, we see that the highest successful guessing probability $P_{guess}^{exp} = 0.9628 \pm 0.0009$ is achieved at data point "4", for which the input state is very close to the best probe state we found in theory. Moreover, we note that compared with other data points, data points "6" and "7" have larger gaps to the theoretical values. That is mainly because the rotation of the wave-plates H2 introduces an unknown random phase in the interferometers. This issue is discussed in more detail in Supplementary Note 5.

Similarly as in the $d = 2$ game, we also observe in this case that the achieved $P_{guess}^{exp}(\gamma = 0.9918, d = 3) > P_{guess}^{max}(\gamma = 0, d = 3) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$. Hence we have experimentally demonstrated that lack of information is also a significant source of uncertainty in the $d = 3$ game. Comparing our experimentally observed value of the guessing probability for $\gamma = 0.9918$ with the highest known achievable guessing probability in the noiseless scenario using the strategy from[7], we see that our result also outperforms those scenarios for the values of γ up to more than 0.9. Unfortunately the optimal strategy for $d = 3$ game with $\gamma > 0$ is not known, and therefore we cannot claim that we outperformed the optimal strategies for all those lower values of γ. However, our achieved high guessing probability gives a strong experimental indication that also in the $d = 3$ game giving Bob access to more quantum information about the purifying register P, enables him to win with higher probability.

On the other hand, our results also provide an insight into the existence of the intrinsic uncertainty in the $d = 3$ game. As the theoretical analysis in[7] has shown it is not possible to achieve perfect guessing for that game. This is unlike in the $d = 2$ case, where all the uncertainty can be contributed to the lack of information. The highest known achievable guessing probability for the $d = 3$ game in the noiseless scenario is $P_{guess}(\gamma = 1, d = 3) = 0.9793$. Let us now compare our experimentally observed values with this theoretical prediction. We will focus here on the data point "3" as our experimental setup was optimized for this setting thus making the error analysis easier for this data point, while the increase in the observed guessing probability for data point "4" is small. Comparing with the best known $P_{guess}(\gamma = 1, d = 3)$ for the noiseless case, the guessing probability we achieved in the experiment for data point "3" has an error gap of $p_{gap} = 0.0182$ to this theoretical value, which can be ascribed to two aspects. On the one hand, in our experiment we use $\gamma = 0.9918$ instead of $\gamma = 1$; on the other hand, there are experimental errors. In Supplementary Note 5 we verify that the observed error gap is consistent with our error model based on the characterized components of the setup. In particular, the experimental errors correspond to the state preparation errors and the dephasing errors inside the interferometers in the setup. Having verified the origin of this error gap, which we can refer to as a gap due to lack of information, we note that in constitutes only a smaller part of the total observed uncertainty gap $1 - P_{guess}^{exp}(\gamma = 0.9918, d = 3)$ for data point "3". In particular:

$$\frac{p_{gap}}{1 - P_{guess}^{exp}(\gamma = 0.9918, d = 3)} = 0.4679. \tag{5}$$

This shows that if the best known theoretical strategy was indeed the optimal one, then more than half of the total experimentally observed uncertainty gap would not come from lack of information but from the intrinsic uncertainty. This observation gives an experimental support to the claim that intrinsic uncertainty is present in the $d = 3$ game.

DISCUSSION

Our work experimentally studies the entropic formulation of quantum uncertainty within the guessing game framework. We experimentally verify that lack of quantum information about the register governing the choice of the measured observable is a key contributor to the arising uncertainty. Our results have been obtained by experimentally implementing a $d = 2$ and $d = 3$ guessing games. We also see, especially for the $d = 2$ game, that the more quantum information about the measurement process can be accessed by Bob, the higher his chance of winning the game. We also observed guessing probability of almost one for the case when almost all the information about the measurement process was made available to Bob, confirming the result of[7] that for the $d = 2$ game there is no intrinsic uncertainty. Finally, the obtained data for the $d = 3$ game supports the result of[7] that there exists intrinsic uncertainty for the $d = 3$ game.

These results have implications for various cryptographic protocols that make use of measurements in mutually unbiased bases. In particular for protocols that perform measurements in BB84 bases[19], we see that it is vital for the purification of the coin determining the measurement basis, to be inaccessible to the eavesdropper. Otherwise the security may be compromised, and in the case when the eavesdropper could later have access to the entire purification of the coin, they could be able to always guess the measurement outcome and hence e.g. obtain the entire key in BB84 QKD[19,20].

Moreover, our work forms an important step in the experimental development of quantum optical technologies based on multi-dimensional systems. The development of our setup contributes to the existing linear optics toolbox through the realization of the controlled three-dimensional quantum Fourier transform. Here, the method we use to implement the three-dimensional quantum Fourier transform can be generalized to arbitrary unitary transformations by regulating the settings of the waveplates. When extending to a much higher dimension, one of the obstacles lies in the relatively large volume of the calcite beam displacer, which must enable multiple beams to pass through simultaneously. For instance, the sizes of the beam displacers in our experiment are approximately $8 \, \text{mm} \times 15 \, \text{mm} \times 37.71 \, \text{mm}$. An efficient way to overcome the size problem is by stacking a series of PBSs, just like in[21–24]. Another problem that one needs to consider is phase stability. As the complexity of the setup increases, an active phase stabilization system may need to be built.

Furthermore, our setup also offers the possibility to further investigate the wave-particle duality[25–28] and its connection to the uncertainty principle[29]. Finally, we note that a further refinement of the controlled Fourier transform to the case in which the control system is also a qutrit and the target system undergoes a transformation to one of the three incompatible measurements would enable us to investigate experimentally the recent results of[30,31]. In these works the authors extend the game of[7] to measuring more than two observables. Interestingly, they show that for the game in which B is two-dimensional, guessing probability of one can be achieved independently of how many measurements are considered. However, if B is more than two-dimensional and more than two measurements are considered, then they show that whether perfect guessing is possible depends on the specific choice of the incompatible measurements. These extensions of the original game for the scenario with three measurements could potentially be implemented on the modification of our setup.

METHODS

Single-photon source

In both the $d = 2$ guessing game (Fig. 3a) and $d = 3$ guessing game (Fig. 3 (b)), pairs of photons of 808 nm are generated by the spontaneous parametric down-conversion (SPDC) process with a 100 mW, 404 nm single-frequency laser (<5 MHz Linewidth) pumping a type-II BBO (beta-barium-borate) crystal. Then one of the photons is fed to the experimental

setup as the signal photon, which is heralded by the detection of the other photon from the pair.

Experimental implementation of guessing games

The system state ρ_B is prepared with the HWPs, (specifically H1 in Fig. 3(a), H1 and H2 in Fig. 3(b))) and HBDs, which sort the input beam into the horizontally parallel beams with different polarized directions H and V (H, horizontally polarized direction; V, vertically polarized direction). A 45° oriented HWP (H2 in Fig. 3(a) and H3 in Fig. 3(b)) is inserted in path "0" to unify the photon's polarization directions in different paths. Then a 22.5° HWP prepares the polarization of the photon in all paths in a state $1/\sqrt{2}(|H\rangle + |V\rangle)$ (H3 in Fig. 3(a) and H4 in Fig. 3(b)). After that a VBD directs the H photon to the upper layer $|u\rangle$ (red lines) and V photon to the lower layer $|l\rangle$ (purple lines), hence preparing the control state $1/\sqrt{2}(|u\rangle + |l\rangle)$ on the register R. Then, depending on whether the photon passes through the upper layer or lower layer, it will undergo either the $\mathbb{I}$ operation or the Fourier operation. In our experimental setup the parallel-path structure of the interference is stable, because all the light beams are affected by the environmental turbulence, such as temperature fluctuation and vibrations, in nearly the same way[32]. Then Bob uses the second VBD to convert the path DoF corresponding to the upper and lower layer into the polarization DoF and uses a quarter-wave plate (QWP, Q1), an HWP (H8 in Fig. 3(a) and H12 in Fig. 3(b)) and a polarization beam splitter (PBS) to distinguish the quantum states ρ_R^x in order to guess Alice's measurement outcome X. We note that since both registers R and B are encoded in different DoF of the same photon, in the experiment a simultaneous measurement of both registers is performed at once. Specifically, the click in the output port D_{ij} corresponds to Bob's guessing outcome i for Alice's measurement outcome j. Therefore, Bob's goal is to set Q1 and H8 (H12) in such a way so that the probability of detection in the ports D_{ii} is maximized.

For the $d = 2$ game, one of the input states of Bob that is optimal for all γ is the pure state $|\psi\rangle_B \propto |0\rangle + |-\rangle$, where $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$. This state is prepared by setting the orientation angle of H1 to 11.3°. Meanwhile, to observe the relation between $P_{\text{guess}}^{\max}(\gamma, d = 2)$ and γ, we place the quartz plate (QP) before the VBD to decrease the coherence between $|u\rangle$ and $|l\rangle$. Now the polarization of the photon is coupled by the QP to its frequency distribution realizing the dephasing channel, and the value of γ is tuned by changing the thickness of the QP. Before the VBD, we perform the standard tomography process to reconstruct the experimentally generated register state $\rho_R^{\exp}$. The value of γ is estimated by approximating $\rho_R^{\exp}$ by an ideal register state $\rho_R(\gamma)$ given in Eq. (3). That is, γ of $\rho_R^{\exp}$ is taken to be the value of that parameter for this $\rho_R(\gamma)$ which has the highest fidelity to $\rho_R^{\exp}$. We find that for each obtained γ the fidelity between $\rho_R^{\exp}$ and the corresponding $\rho_R(\gamma)$ is higher than 0.9995. Finally, the guessing probability is obtained by summing the detection probabilities in output ports D_{00} and D_{11}. More details about the thicknesses of quartz plates, the angles of Q1 and H8, as well as the detailed numerical values of the corresponding experimental results are provided in Supplementary Note 2.

For the $d = 3$ game we focus on the single scenario corresponding to the largest possible γ that we could achieve in our experiment. We then investigate the optimal known strategy for that γ. The best probe states for the $d = 3$ game that we found, established using the procedure from[7] have a nice property that for all γ the optimal measurement for Bob aiming to distinguish the three possible qubit states ρ_R^x is actually a projective measurement. This measurement aims to distinguish two out of the three possible states, corresponding to the two dominant outcomes of Alice. Specifically, for the best known input state we consider, the dominant outcomes are 0 and 2. The corresponding projective measurement performed on the register R has POVM elements $\{M_0, M_1 = \mathbf{0}, M_2\}$, where M_0 and M_2 are projectors. This explains why the first index of detectors D in Fig. 3(b) takes only the value 0 or 2.

In our experiment, the highest amount of coherence in the register R which we achieved is $\gamma = 0.9918$. A corresponding best probe state we found for the $d = 3$ game is the state $|\psi\rangle_B = a_1|0\rangle + a_2|1\rangle + a_3|2\rangle$ with the coefficients $a_1 = 0.0938 + 0.5786i$, $a_2 = 0.0109 - 0.1218i$ and $a_3 = 0.8009$. More detailed information about the probe states preparation, the optimal measurements, and the guessing probabilities we obtained are given in Supplementary Note 2.

Three-dimensional Fourier gate

We note that in the $d = 3$ guessing game we implement the three-dimensional Fourier operation based on the idea of the scheme proposed

in[18]. In the original scheme, the single-qubit rotation operator R_y represents a variable beam splitter, which is realized by an interferometer built with two 50:50 beam splitters. The phase difference between the two arms of the interferometer is adjusted to change the ratio of the light beams in two output ports. In our work, we develop a HBD-HWP-HBD structure to realize the operator R_y, which uses much fewer elements compared with the method with 50:50 beam splitters. Hence our scheme is much more friendly to the experimental implementation. Owing to the introduction of the polarization-dependent beam splitter, HBD, which enables the transformation between the path DoF and the polarization DoF, the photon's paths can be efficiently manipulated by the polarization controller element HWP instead of the interferometer.

Let us now briefly discuss how we quantify the performance of this Fourier gate. After applying the ideal Fourier operation to the input state $|w_j\rangle = 1/\sqrt{3} \sum_{k=0}^{2} w^{-jk}|k\rangle$, where $j = 0, 1, 2$, $w = e^{2i\pi/3}$, we will obtain the corresponding output state $|j\rangle$, therefore the probability to detect a photon in output mode i when inputting state $|w_j\rangle$ into our Fourier gate implementation should be δ_{ij}. In our experiment, the average probability for detecting the photon in the right output mode is 0.9771 ± 0.0006, which can be obtained only when the Fourier operation works well. The detailed information about how to implement and estimate the quality of the Fourier operation are given in the Supplementary Note 3. Moreover, we analyze the main factors limiting its performance by considering a three-dimensional dephasing model in Supplementary Note 5.

DATA AVAILABILITY

All the data that support the results of the current work are available from the corresponding authors upon reasonable request.

CODE AVAILABILITY

The codes for simulation and data processing are available from the corresponding authors upon reasonable request.

REFERENCES

1. Heisenberg, W. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. In *Original Scientific Papers Wissenschaftliche Originalarbeiten*, 478–504 (Springer, 1985).
2. Kennard, E. H. Zur quantenmechanik einfacher bewegungstypen. *Z Phys.* **44**, 326–352 (1927).
3. Robertson, H. P. The uncertainty principle. *Phys. Rev.* **34**, 163–164 (1929).
4. Coles, P. J., Berta, M., Tomamichel, M. & Wehner, S. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.* **89**, 015002 (2017).
5. Maassen, H. & Uffink, J. B. M. Generalized entropic uncertainty relations. *Phys. Rev. Lett.* **60**, 1103–1106 (1988).
6. Berta, M., Christandl, M., Colbeck, R., Renes, J. M. & Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **6**, 659 (2010).
7. Rozpędek, F., Kaniewski, J., Coles, P. J. & Wehner, S. Quantum preparation uncertainty and lack of information. *New J. Phys.* **19**, 023038 (2017).
8. Nielsen, M. A. & Chuang, I. L.*Quantum Computation and Quantum Information: 10th Anniversary Edition* (2011).
9. Shor, P. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134 (1994).
10. Wootters, W. K. & Fields, B. D. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **191**, 363–381 (1989).
11. Giovannini, D. et al. Characterization of high-dimensional entangled systems via mutually unbiased measurements. *Phys. Rev. Lett.* **110**, 143601 (2013).
12. Grblacher, S., Jennewein, T., Vaziri, A., Weihs, G. & Zeilinger, A. Experimental quantum cryptography with qutrits. *New J. Phys.* **8**, 75 (2006).
13. Yurtalan, M. A., Shi, J., Kononenko, M., Lupascu, A. & Ashhab, S. Implementation of a walsh-hadamard gate in a superconducting qutrit. *Phys. Rev. Lett.* **125**, 180504 (2020).
14. Klimov, A. B., Guzmán, R., Retamal, J. C. & Saavedra, C. Qutrit quantum computer with trapped ions. *Phys. Rev. A* **67**, 062313 (2003).
15. Brandt, F., Hiekkamäki, M., Bouchard, F., Huber, M. & Fickler, R. High-dimensional quantum gates using full-field spatial modes of photons. *Optica* **7**, 98–107 (2020).
16. Lu, H.-H. et al. Quantum phase estimation with time-frequency qudits in a single photon. *Adv. Quantum Technol* **3**, 1900074 (2020).
17. Dogra, S., Arvind & Dorai, K. Determining the parity of a permutation using an experimental NMR qutrit. *Phys. Lett. A* **378**, 3452–3456 (2014).
18. Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S. & Walsmley, I. A. Optimal design for universal multiport interferometers. *Optica* **3**, 1460–1465 (2016).
19. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In International Conference on Computer System and Signal Processing, IEEE, 1984, 175–179 (1984).
20. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
21. Wang, X.-L. et al. 18-qubit entanglement with six photons' three degrees of freedom. *Phys. Rev. Lett.* **120**, 260502 (2018).
22. Hu, X.-M. et al. Efficient generation of high-dimensional entanglement through multipath down-conversion. *Phys. Rev. Lett.* **125**, 090503 (2020).
23. Zhong, H.-S. et al. Quantum computational advantage using photons. *Science* **370**, 1460–1463 (2020).
24. Zhong, H.-S. et al. Phase-programmable gaussian boson sampling using stimulated squeezed light. *Phys. Rev. Lett.* **127**, 180502 (2021).
25. Tang, J.-S. et al. Realization of quantum wheeler's delayed-choice experiment. *Nat. Photonics* **6**, 600 (2012).
26. Peruzzo, A., Shadbolt, P., Brunner, N., Popescu, S. & O'Brien, J. L. A quantum delayed-choice experiment. *Science* **338**, 634–637 (2012).
27. Kaiser, F., Coudreau, T., Milman, P., Ostrowsky, D. B. & Tanzilli, S. Entanglement-enabled delayed-choice experiment. *Science* **338**, 637–640 (2012).
28. Ionicioiu, R. & Terno, D. R. Proposal for a quantum delayed-choice experiment. *Phys. Rev. Lett.* **107**, 230406 (2011).
29. Coles, P. J., Kaniewski, J. & Wehner, S. Equivalence of wave–particle duality to entropic uncertainty. *Nat. Commun.* **5**, 5814 (2014).
30. Plesch, M. & Pivoluska, M. Loss of information in quantum guessing game. *New J. Phys.* **20**, 023018 (2018).
31. Doda, M., Pivoluska, M. & Plesch, M. Choice of mutually unbiased bases and outcome labeling affecting measurement outcome secrecy. *Phys. Rev. A* **103**, 032206 (2021).
32. O'Brien, J. L., Pryde, G. J., White, A. G., Ralph, T. C. & Branning, D. Demonstration of an all-optical quantum controlled-not gate. *Nature* **426**, 264 (2003).
33. Xia, K. Quantum non-demolition measurement of photons. In Photon Counting-Fundamentals and Applications (InTech, 2018).

AUTHOR CONTRIBUTIONS

Y.Y.Z. and F.R. contributed equally to this work. Y.Y.Z. is the main experimental author and F.R. the theory author of this work. Y.Y.Z. designed and performed the experiment with the help from Z.H. and K.D.W., and F.R. solved the optimization problems for the optimal device settings. Y.Y.Z. and F.R. analyzed the data, constructed the error models, and wrote the manuscript. G.Y.X., C.F.L. and G.C.G. supervised the project.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-022-00572-w.

Correspondence and requests for materials should be addressed to Guo-Yong Xiang.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.