Experimental Realization of High-Efficiency Counterfactual Computation
Fei Kong, Chenyong Ju, Pu Huang, Pengfei Wang, Xi Kong, Fazhan Shi, Liang Jiang, and Jiangfeng Du
Phys. Rev. Lett. 115, 080501 — Published 21 August 2015
DOI: 10.1103/PhysRevLett.115.080501
Counterfactual computation (CFC) exemplifies the fascinating quantum process by which the result of a computation may be learned without actually running the computer. In previous experimental studies, the counterfactual efficiency is limited to below 50%. Here we report an experimental realization of the generalized CFC protocol, in which the counterfactual efficiency can break the 50% limit and even approach unity in principle. The experiment is performed with the spins of a negatively charged nitrogen-vacancy (NV) color center in diamond. Taking advantage of the quantum Zeno effect, the computer can remain in the not-running-subspace due to the frequent projection by the environment, while the computation result can be revealed by final detection. The counterfactual efficiency up to 85% has been demonstrated in our experiment, which opens the possibility of many exciting applications of CFC, such as high efficient quantum integration and imaging.

Quantum physics has demonstrated its profound power in various applications, including secure quantum communication [1-3], precise quantum metrology [4-6], and exponentially fast quantum algorithms [7-8]. As an exotic feature of quantum physics, CFC can learn the result of the computation without actually running the computer [9-11]. A figure of merit for the assessment of CFC is the counterfactual efficiency, which is the probability of accurately deducing a computing result ‘for free’. However, CFC controlled by a quantum switch has only a maximum counterfactual efficiency of 50% to learn the result ‘for free’, which limits its practical application [12-14]. Nevertheless, generalized CFC can go beyond this limit and achieve counterfactual efficiency approaching unity [10].

Consider the task of using a quantum computer to characterize a black box, which carries out one of the unitaries from the set \( \{ U_r \} \), with \( r = 1, 2, \ldots, K \). Suppose the unitary \( U_r \) evolves trivially in a subspace, identified as the ‘off’-subspace associated with \( U_r \),

\[
\mathcal{H}_{\text{off},r} = \text{span}\{ |\psi\rangle : U_r |\psi\rangle = |\psi\rangle \},
\]

The subspace orthogonal to \( \mathcal{H}_{\text{off},r} \) is the ‘on’-subspace of \( U_r \). Since the computer has trivial evolution in the off-subspace, one might expect that the computer has to evolve, at least partially, into the non-trivial on-subspace to learn about the black-box unitary. CFC, as an exotic manifestation of quantum physics, opens the possibility of learning about the black-box unitary \( U_r \), while maintaining the computer in its off-subspace [9,10]. An important figure-of-merit of CFC is the counterfactual efficiency, defined as the average probability of learning the results without running the computer,

\[
\eta = \frac{1}{K} \sum_{r=1}^{K} p_r,
\]

where \( p_r \) is the probability of learning the result \( U_r \) counterfactually (i.e., maintaining the system in \( H_{\text{off},r} \) throughout the entire process). The above definition of generalized CFC extends the choices of unitary operations investigated in the CFC literature [9], which often assumes that the black-box unitary \( U_r \) has the form of controlled-\( \tilde{U} \) between the quantum switch (S) and the output register (R). As shown in [10,15], CFC with controlled-\( \tilde{U} \) has a limited counterfactual efficiency \( \eta \leq 50\% \). Hence, it is crucial to extend the choice of \( U_r \) beyond the class of controlled-\( \tilde{U} \) in order to achieve \( \eta \) above 50% or even approaching unity [10,15].

To illustrate generalized CFC with high efficiency, we consider a quantum computer consisting of a \((K+1)\)-level quantum switch \( \{|0\rangle_S, |1\rangle_S, \ldots, |K\rangle_S \} \) and a two-level register \( \{|0\rangle_R, |1\rangle_R \} \). The black box has \( K \) possible unitaries:

\[
U_r |i\rangle_S |j\rangle_R = \begin{cases} 
|i, j\rangle & \text{if } i \in \{0, r\}, \text{ (in the off-subspace)} \\
|i, 1-j\rangle & \text{if } i \neq 0, r, \text{ (in the on-subspace)}
\end{cases}
\]

with \( r = 1, \ldots, K \). Note that the off-subspace depends on the value of \( r \), which is the distinguished feature that yields the breakthrough of counterfactual efficiency compared to the controlled-\( \tilde{U} \), CFC [15]. The goal is to identify the value of \( r \) while confining ourselves to its off-subspace during the computation. As illustrated in Fig. 1(a), the generalized CFC scheme with \( K = 2 \) has the following procedure: (i) initialize the computer in the common ‘off’ state \(|0\rangle_S |0\rangle_R \) for both \( U_1 \) and \( U_2 \); (ii)
perform a controlled-$T_0$ operation

$$T_0 \otimes |0\rangle_R (|0\rangle + I_S \otimes |1\rangle_R) |1\rangle, \quad (2)$$

which rotates the switch with $T_\theta$ conditioned on register state $|0\rangle_R$:

$$T_\theta = \begin{pmatrix} a & -b & -b \\ b & c & -d \\ b & d & c \end{pmatrix}, \quad (3)$$

where $a = \cos^{\frac{\theta}{\sqrt{2}}}$, $b = \frac{1}{\sqrt{2}} \sin^{\frac{\theta}{\sqrt{2}}}$, $c = \cos^{2\frac{\theta}{\sqrt{2}}}$, $d = \sin^{2\frac{\theta}{\sqrt{2}}}$, and small rotation angle $\theta = \frac{\pi}{2^N}$ with $N \gg 1$;

(iii) apply the black-box unitary $U_r$ to the computer;

(iv) measure the register in $\{|0\rangle_R, |1\rangle_R\}$ basis;

(vi) if the register is $|1\rangle_R$, terminate the computation as a failure; otherwise, repeat the procedure from step (ii);

(vii) after $N$ repetitions, measure the switch in $\{|0\rangle_S, |1\rangle_S, |2\rangle_S\}$ basis.

An intuitive explanation of the whole procedure is provided in terms of optical circuits, as shown in Fig. 1(b). The switch is illustrated by the photon path while the register is illustrated by the transparent or opaque object putted on the photon path. The three-arm interferometer represents the $T_\theta$ operation, and the choice of $U_r$ means the blocking of $r$-th photon path. The opaque object (black box) also acts as a projective measurement (PM). As one can show inductively, after the $n$-th repetition, the computer will be in the state $|\psi_n\rangle \approx \cos^{\frac{\theta n}{\sqrt{2}}} |0, 0\rangle + \sin^{\frac{\theta n}{\sqrt{2}}} |r, 0\rangle$ with a failure probability $O\left(\frac{1}{N^2}\right)$ and the accumulative failure probability is $O\left(\frac{1}{N^2}\right)$. After $N$ repetitions, the system will reach the target state $|r, 0\rangle$ with a total failure probability $O\left(\frac{1}{N}\right)$ over all repetitions; and the measurement of the switch will unambiguously identify the value of $r$. Fig. 1(c) also gives the numerical calculation of the populations of the switch states $\{|0\rangle_S, |1\rangle_S, |2\rangle_S\}$ for different repetition times $n$. When $n = N$, the switch will be in $|\rangle_S$ if the procedure have not been terminated. Moreover, throughout the entire computation, the system is always in the off-subspace associated with $U_r$, except for a vanishingly small failure probability $O\left(\frac{1}{N}\right)$ of leakage into the on-subspace resulting in termination of the computation. Hence, the probability of learning the result counterfactually is $p_r = 1 - O\left(\frac{1}{N}\right)$ for $r = 1, 2$. Therefore, the efficiency of the generalized CFC scheme is

$$\eta = \frac{p_1 + p_2}{2} = 1 - O\left(\frac{1}{N}\right), \quad (4)$$

which approaches unity for large $N$. As shown in the inset of Fig. 1(c), even for a finite number $N = 20$, the generalized CFC scheme can already have a high efficiency $\eta \approx 94\%$, which beats the 50% limit for all CFC schemes with controlled-$U_r$.

The experimental demonstration is performed on a single negatively charged NV center in diamond, of which the structure and energy levels are shown in Fig. 2(a). With long coherence time at room temperature $^{22}$, the NV electron spin (denoted by ‘e’ hereinafter) can be initialized and measured optically $^{23, 24}$, reliably controlled with microwave (MW) pulses $^{25, 26}$, and coherently coupled to nearby nuclear spins or other remote spins $^{27, 30}$. Hence, it is one of the most promising candidates for quantum information processing $^{25, 30, 31}$. With a static magnetic field $B_0 \approx 507$ G applied along the NV axis, the $^{14}$N nuclear spin (denoted by ‘n’ hereinafter) can be polarized using dynamic polarization technology $^{32}$. The nuclear spins can also be manipulated with radiofrequency (RF) pulses $^{33}$. As shown in Fig. 2(b, c), the energy shift induced by hyperfine in-

![FIG. 1. (Color online). Generalized CFC. (a) Quantum circuit of the generalized CFC scheme, with $K$ possible black-box unitaries as defined in Eq. (1). (b) Photonic analog of the $K = 2$ quantum circuit, with a photon passing through a series of cascaded three-arm interferometers (blue ovals) for $T_0$ operation. Different configurations of transparent pathways (empty boxes) and absorbers (black boxes) are associated with different choices of $U_r$. (c) For small $\theta = \frac{\pi}{2^N}$, the simulated populations of $|0\rangle_S |0\rangle_R$ (red circle), $|1\rangle_S |0\rangle_R$ (black square), $|2\rangle_S |0\rangle_R$ (blue triangle) as a function of the repetition number $n$, for $r = 1, 2$. Pink dotted line indicates the optimized repetition number $N = \pi/\theta$ where the highest counterfactual efficiency is achieved. (d) The counterfactual efficiency $\eta$ versus the optimized repetition number $N$, with $\theta = \pi/N$. For large $N$, $\eta$ approaches 100\%.](image-url)
FIG. 2. (Color online). Experimental system. (a) Structure and energy levels of the NV center. (b) Relevant energy levels of the NV electron spin with \{0_e, |−1_e⟩\} for the two-level register \{|0⟩_R, |1⟩_R\}, and the nuclear spin with \{0_n, |1_n, |−1_n⟩\} for the three-level quantum switch \{0_S, |1_S, |2_S⟩\}. (c) Pulse sequence to control the quantum switch. RF1 and RF2 pulses represent resonant transitions associated with \{0_n, |±1_n⟩\), respectively. (d) RF induced Rabi oscillation of the nuclear spin. Red circle, black square, and blue triangle represent \{|0_e⟩, |1_e⟩\}, and \{|−1_e⟩\) respectively. Solid curves are the fittings. Error bars (± s.d.) induced by the photon shot noise are smaller than the symbols as the sequence is repeated several million times to get enough photons.

Interaction and Zeeman effect makes selective MW and RF control possible. Two resonant RF pulses are applied simultaneously to realize double interference between \{0_n, |1_n⟩\), which is a basic operation in our protocol. Then the state is measured using state tomography. Fig. 2(d) gives the measured populations of \{0_n, 0_e, |1_n, 0_e⟩, and |−1_n, 0_e⟩\) during the double interference. With the above control and readout, the nitrogen nuclear spin \{0_n, |1_n, |−1_n⟩\) acts as a three-level quantum switch \{0_S, |1_S, |2_S⟩\}, while the NV electron spin \{0_e, |−1_e⟩\) acts as a two-level register \{|0⟩_R, |1⟩_R\} for the generalized CFC scheme.

The pulse sequence shown in Fig. 3(a) gives the implementation of the generalized CFC scheme. At first, a 4 μs 532nm laser pulse followed by an RF π pulse initializes the state of the system to \{0⟩_S, |0⟩_R\} (i.e., \{0_n, 0_e⟩\). Then, two short RF pulses realize the controlled-\(T_\theta\) rotation. After that, a selective MW π pulse implements the black-box unitary \(U_r\), which flips the register (electron spin) conditioned on the switch (nuclear spin) state \{2⟩_S\} (i.e., \{−1_n⟩\) for \(r = 1\) and \{|1⟩_S\} (i.e., \{1_n⟩\)) for \(r = 2\). Instead of applying the PM to the register which is difficult for our room-temperature experiment, we employ the fast decoherence of the electron spin to perform an effective ensemble PM to the register, by simply waiting for a time significantly longer than the electron spin coherence time. During this time, the superposition state of the register will quickly relax to a mixed state, while the switch coherence remains almost unchanged since the coherence time of the nuclear spin is much longer than that of the electron spin. The only difference from the genuine PM is that we don’t block the process if the computer is triggered, but this will only marginally change the final output state with less than 1% difference in the measured population. Finally, the populations of \{0⟩_S, |0⟩_R, |1⟩_S, |0⟩_R\) are measured using state tomography.

The final output state depends on both the black-box unitary \(U_r\) and the repetition number \(n\). For \(r = 1\) \((r = 2\), the population transfer from \{0⟩_S, \{2⟩_S \{1⟩_S\}) is inhibited by quantum Zeno effect, and the register remains in \{|0⟩_R\). As shown in Fig. 3(b), for the fixed rotation angle \(θ = π/20\), the switch state evolves in the off-subspace spanned by \{(0⟩_S, |r⟩_S)|0⟩_R\}, and oscillates between \{0⟩_S, |0⟩_R\ and \{|r⟩_S)|0⟩_R\) as \(n\) increases. For the rotation angle \(θ = π/N\, after \(n = N\) repetitions the population of the target output state \{|r⟩_S)|0⟩_R\ becomes
the largest (pink dotted line). The counterfactual efficiency $\eta$ is equal to this largest population of $|r\rangle_S \langle 0|_R$ averaged over $r = 1, 2$. As plotted in Fig. 3(c), the counterfactual efficiency depends on $N$, with the maximum achieving 85% for $N \approx 17$. The decay of the efficiency is mainly due to the accumulation of pulse imperfection for large $N$ \cite{15}. The uncertainty of the efficiency is caused by not only photon shot noise but also other experimental imperfection, including ensemble PM, imperfect state tomography, and unstable external magnetic field. And the corresponding uncertainties of efficiency are less than 1%, 6%, and 2% respectively \cite{15}, so the estimated total uncertainty of the counterfactual efficiency is less than 9%. Our generalized CFC scheme has counterfactual efficiency $\eta = 85\%$, well above the 50% limit.

The generalized CFC scheme can be extended to distinguish a black box with $K + 1$ possible unitaries $U_r$ as defined in Eq. \cite{11} for $r = 0, 1, 2, \cdots, K$, which can be achieved using a $(K + 1)$-dimensional switch with the state space $\{ |0\rangle_S, |1\rangle_S, \cdots, |K\rangle_S \} \cup \{ |\rangle_1 \}$ \cite{10,15}. After the repetitive interrogations, the switch will end up in the state $|r\rangle_S$. It provides a powerful quantum interrogation protocol to solve practical problems. Suppose we have an object consisting of $K$ pixels (labeled by $r = 1, 2, \cdots, K$) with all pixels being opaque except for the $r$-th pixel being transparent (if $r = 0$, no pixel is transparent). The generalized CFC scheme can use just one photon to learn about the value of $r$ without having the photon blocked by the object. This protocol can be potentially used for low-light-level imaging technology \cite{34} which is very demanding for various realistic situations in which the light itself may destroy or modify the illuminated materials. The applications include, for example, biological imaging of Green Fluorescent Protein that might be bleached under strong laser beam, high-resolution imaging with UV light that may kill the cell, or even X-ray imaging that may be harmful to human body. The concept proposed here may benefit these applications with a safe (one photon-level) yet efficient (successful rate approaches 1) imaging method.

A imaging concept similar to the above is the ‘interaction-free imaging’ proposed and demonstrated by A. G. White et al \cite{34}. The method is based on the interaction-free quantum measurement \cite{36,37} (closely related to the generalized CFC scheme here), which uses a two-arm interferometer to query the presence or absence of the absorbing object in one of the arms. Although that imaging method can also reduce the amount of photons being absorbed by the object compared with conventional methods, it still requires at least $O(K)$ photons to find the value $r$ due to the raster scanning manner (imaging pixel by pixel). The generalized CFC approach pushes this limit to only one photon.

In conclusion, we use a single NV center in diamond to demonstrate the generalized CFC scheme, which can learn the information of a black-box unitary $U_r$ with the quantum computer always in its off-subspace. Our implementation has demonstrated high counterfactual efficiency up to 85%, well above the 50% limit for the conventional CFC scheme. This opens up many exciting opportunities of using generalized CFC for future applications.

The authors thank V. V. Albert, O. L. Russo, C. Shen, H. X. Tang, J. Wen, and C.-L. Zou for many stimulating discussions. This work was supported by the 973 Program (Grant No. 2013CB921800), the NNSFC (Grant Nos. 11227901, 91021005, 11104262, 31470835), the “Strategic Priority Research Program (B)” of the CAS (Grant No. XDB01030400), the Army Research Office, the Air Force Office of Scientific Research (MURI program), the Defense Advanced Research Projects Agency (Quiness program), the Alfred P. Sloan Foundation, and the Packard Foundation.

* cyju@ustc.edu.cn
† liang.jiang@yale.edu
‡ df@ustc.edu.cn

\begin{thebibliography}{99}
\bibitem{1} N. Gisin, G.Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
\bibitem{9} R. Jozsa, Chaos Solitons Fractals 10, 1657 (1999).
\bibitem{13} L. Vaidman, Phys. Rev. Lett. 98, 160403 (2007).
\bibitem{15} See Supplemental Material http://link.aps.org/supplemental/XXX for demonstration, simulation and error estimation, which includes Refs. [16-21].
\end{thebibliography}