Experimental computational advantage from superposition of multiple temporal orders of quantum gates

Márcio M. Taddei1,*, Jaime Carini2,3,4 Daniel Martínez2,3, Tania García2,3, Nayda Guerrero2,3, Alastair A. Abbott5, Mateus Araújo6, Cyril Branciard7, Esteban S. Gómez2, Stephen P. Walborn2,3, Leandro Aolita1, and Gustavo Lima2,3

1 Instituto de Física, Federal University of Rio de Janeiro, 21941-972, P. O. Box 68528, Rio de Janeiro, Brazil. 2 Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile. 3 Millennium Institute for Research in Optics, Universidad de Concepción, 160-C Concepción, Chile. 4 Departamento de Ingeniería Eléctrica, Universidad Católica de la Santísima Concepción, Concepción, Chile. 5 Department of Applied Physics, University of Geneva, 1211 Geneva, Switzerland. 6 Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmannwasse 3, 1090 Vienna, Austria. 7 Univ. Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, 38000 Grenoble, France. *e-mail: marciotaddei@gmail.com

Advanced models for quantum computation where even the circuit connections are subject to the quantum superposition principle have been recently introduced. There, a control quantum system can coherently control the order in which a target quantum system undergoes $N$ gate operations. This process is known as the quantum $N$-switch, and has been identified as a resource for several information-processing tasks. In particular, the quantum $N$-switch provides a computational advantage — over all circuits with fixed gate orders — for phase-estimation problems involving $N$ unknown unitary gates. However, the corresponding algorithm requires the target-system dimension to grow (super-)exponentially with $N$, making it experimentally demanding. In fact, all implementations of the quantum $N$-switch reported so far have been restricted to $N = 2$. Here, we introduce a promise problem for which the quantum $N$-switch gives an equivalent computational speed-up but where the target-system dimension can be as small as 2 regardless of $N$. We use state-of-the-art multi-core optical fiber technology to experimentally demonstrate the quantum $N$-switch with $N = 4$ gates acting on a photonic-polarization qubit. This is the first observation of a quantum superposition of more than 2 temporal orders, and also demonstrates its usefulness for efficient phase-estimation.

Quantum mechanics allows for processes where two or more events take place in a quantum superposition of different temporal orders. This exotic phenomenon results in causal nonseparability$^{1-3}$, and it is likely to be especially relevant in quantum treatments of gravity$^{4-6}$. In fact, quantum control of temporal orders could be realized with quantum circuits exploiting hypothetical closed time-like curves$^{7,8}$, and it would also arise naturally due to the spacetime warping that macroscopic spatial superpositions of massive bodies would cause$^{9}$. From a more practical perspective, advanced quantum computational models without definite gate orders have sparked a great deal of fundamental interest, as they do not fit into the usual paradigm of circuits with fixed gate connections$^{6,7,10-13}$. The best known example is the celebrated quantum $N$-switch gate, $S_N$, which coherently applies a different permutation of $N$ given gates on a target quantum system conditioned on the state of a control quantum system$^{1,13,14}$. $S_N$ has been identified as a resource for a number of exciting information-theoretic tasks. For instance, for $N = 2$, it allows one to deterministically distinguish pairs of commuting versus anti-commuting unitaries$^{12}$; and, remarkably, this translates into an exponential advantage in a communication complexity problem$^{15,16}$.

In general, circuits that synthesize $S_N$ with a fixed gate order are known, but at the expense of quadratically more queries to (i.e., uses of) the gates$^{12-14,17}$. As a consequence thereof, $S_N$ allows one to solve a promise problem$^{12,14}$ on the permutations of $N$ unknown unitary gates with quadratically fewer queries in $N$ than all known circuits with fixed gate order. More precisely, the permutation sequences of the gates are promised to differ only by a phase factor, and $S_N$ efficiently estimates these phase differences. However, the algorithm for this problem$^{12,14}$ requires the target-system dimension to grow (super-)exponentially with $N$, making it experimentally demanding. As a matter of fact, all experimental realizations of the quantum $N$-switch reported so far are restricted to the simplest case of $N = 2$ gate orders$^{16,19-22}$.

In this work, we introduce a novel algorithm that exploits the quantum $N$-switch and experimentally demonstrate it for $N = 4$ unitary gates. Specifically, we find a variant of the above phase-estimation problem, which we name the Hadamard promise problem, for which the quantum $N$-switch is also a resource but with considerably milder constraints on the target-system dimension. The problem’s promise is that the products of the $N$ unknown gates applied in $P$ different orders differ only in $+$ or $-$ signs that are encoded into one of the columns of a given $P \times P$-dimensional Hadamard matrix; and the problem consists of finding which column it is. The algorithm exploits the quantum $N$-switch — consuming $N$ queries to the gates — to deterministically find the column. This represents a speed-up quadratic in $N$ in query complexity (i.e. number of queries) with respect to all known
Figure 1. a) Abstract representation of the quantum $N$-switch for the case of $N = 4$. The process, $W_4$ (light-grey region), can be thought of as an experimental setup (e.g., a quantum circuit or interferometer) through which the composite control-target system goes and with open slots for target-subsystem gates $U_i$ (dark-grey boxes), for $i = A, B, C, D,$ or $D$, to be inserted. Inside $W_4$, the connections between these gates are coherently controlled by the control subsystem, an effect known as quantum control of gate orders (QCGO). This property is a physical resource for certain quantum computations (phase-estimation problems), and $W_4$ is the resourceful object that bears it. The concatenation of $W_4$ with the inserted gates yields the quantum 4-switch gate $S_4$, a joint unitary operation on the composite system. b) Concrete schematics of the specific variant of the quantum 4-switch process experimentally implemented in this work. The target subsystem undergoes the four-gate sequence in a quantum superposition of $P = 4$ different orderings (permutations of the string $ABCD$): $\Sigma = \{ABCD, BADC, CBDA, DABC\}$. Each permutation is shown individually in a different color and inset. c) In the above-mentioned computations, the target-subsystem gates are unknown. For the purpose of complexity analysis, they can be thought of as produced upon request by a quantum oracle $O$. This takes as input $i = A, B, C,$ or $D$ and outputs a black-box device implementing the unknown gate $U_i$. Each such call to the oracle counts as an oracle query. The $N$-switch process allows one to solve computational problems on the commutation relationships between the black-box gates with considerably fewer oracle queries — i.e., lower query complexity — than any process with fixed (or classically controlled) gate connections.

### Quantum control of gate orders

Consider a $d$-dimensional target system $T$, of Hilbert space $\mathbb{H}_t$, and a $P$-dimensional control system $C$ of Hilbert space $\mathbb{H}_c$. Given a set $U := \{U_A, U_B, \ldots\}$ of $N$ unitary operators on $\mathbb{H}_t$ and a set $\Sigma := \{\sigma_x\}_{x \in [P]}$, where we introduce the shorthand notation $[P] := \{0, 1, \ldots, P - 1\}$, of $P$ permutations of the corresponding $N$-letter alphabet $\{A, B, \ldots\}$, we define the quantum $N$-switch gate $S_N$ as the joint unitary operation

$$S_N |x\rangle_c |\Psi\rangle_t = |x\rangle_c \Pi_x |\Psi\rangle_t ,$$

for all $x \in [P]$. Here, $|x\rangle_c$ is the $x$-th member of the computational basis of $\mathbb{H}_c$, $|\Psi\rangle_t$ is an arbitrary state vector in $\mathbb{H}_t$, and $\Pi_x := U_{\sigma_x(N-1)}U_{\sigma_x(1)}U_{\sigma_x(0)}$ is the $N$-fold product of the gates in $U$ in the ordering given by the $x$-th permutation in $\Sigma$, $\sigma_x$. That is, $\sigma_x(j)$ is the $j$-th element in the $x$-th permutation sequence $\sigma_x$. In other words, $C$ coherently controls the order in which the sequence of unitary gates is applied on $T$, which explains the name “quantum control of gate orders” (QCGO). In addition, we note that the usual definition of QCGO is independent of the specific choice of gates in $U$. A convenient mathematical tool to capture that is the quantum $N$-switch process $W_N$, which produces the quantum $N$-switch gate $S_N$ when given the set of gates $U$ as input. For the technical definition of processes, we refer the reader to Refs.\textsuperscript{10,11} Intuitively, one can think of a process as the quantum evolution generated by an experimental arrangement with open slots for gates on $\mathbb{H}_t$ to be inserted\textsuperscript{10,11,13} as represented in Fig. 1 (a). Inside the process, the connections between the inserted gates may be subject to the quantum superposition principle. For instance, Fig. 1 (b) pictorially represents our experimental implementation of the quantum 4-switch $S_4$, with a coherent quantum superposition of $P = 4$ different gate connections (each one in a different color), for the particular choice of permutation set $\Sigma = \{ABCD, BADC, CBDA, DABC\}$. Such superpositions give rise to QCGO, which corresponds to a specific type of quantum control of causal orders\textsuperscript{19} (and both phenomena are in turn contained within the general notion of causal nonseparability\textsuperscript{6}). In particular, QCGO takes place when those gate connections are coherently controlled by a control
system, as in Eq. (1). Aside from being a fundamentally interesting phenomenon, QCGO turns out to be a physical resource for interesting phase-estimation problems, as we discuss next.

The Araújo-Costa-Brukner algorithm

The quantum $N$-switch process provides an advantage for solving a particular phase-estimation problem\cite{12,14} to which we here refer as the Fourier promise problem. In this type of problems, one has access to a quantum oracle $O$ for $U$, i.e., a black-box device that delivers a gate $U_i \in U$ every time it is queried. See Fig. 1 (c). No information about the gates is available except for the promise that, for the constant phase factor \( \omega := e^{i \frac{2\pi}{N}} \) and for all \( x \in [P] \), they satisfy the property:

\[
\Pi_x = \omega^{xy} \Pi_0, \tag{2}
\]

for some fixed, unknown $y \in [P]$. The task is to determine which one of the properties holds, i.e., to find $y$.

The Araújo-Costa-Brukner algorithm to solve this problem is based on the standard Hadamard test\cite{31}, and shares similarities with the Kitaev phase estimation algorithm\cite{12}. The control system is initialized in the computational-basis reference state \( |0\rangle_c \), while the target system starts in an arbitrary state \( |\Psi_t\rangle \). A $P$-dimensional quantum Fourier transform $F_P$ on $C$ maps it to a uniform superposition of all computational-basis states. Then, the quantum $N$-switch gate is applied. Because of property (2), this introduces the phase factor \( \omega^{xy} \) to each computational-basis state \( |x\rangle_c \) in the superposition, while the state $\Pi_0 |\Psi_t\rangle$ of the target system factorizes. The value of $y$ is thus encoded into the phases of the superposition state of the control system. To map it back to the computational basis, one uncomputes the Fourier transform (applying its inverse $F_P^{-1} = F_P^\dagger$). In symbols\cite{14}:

\[
F_P^{-1} S_N F_P |0\rangle_c |\Psi_t\rangle = |y\rangle_c \Pi_0 |\Psi_t\rangle. \tag{3}
\]

Then, $y$ is finally read out by a single-shot computational-basis measurement on $C$.

To apply $S_N$, one must consume $N$ queries to $O$. Therefore, the query complexity — i.e., total number of oracle queries — of the algorithm is $Q = N$, for all $P \leq N!$. Remarkably, causally ordered processes (i.e., those produced by circuits with fixed, or classically controlled, gate connections) require considerably more queries to solve the same problem. For instance, for $P = N!$, the best causally ordered process displays query complexity $Q = \Omega(N^2)$\cite{13,14,17}, i.e. quadratically higher in $N$. A downside of the algorithm, however, is that the target-system dimension $d$ must grow with the number $P$ of gate orders. This can be seen\cite{14} by taking the determinant of both sides of Eq. (2). For $y = 1$, and since $\det \Pi_x = \det \Pi_0$, this imposes $\det \Pi_x = \omega^{x} \det \Pi_0$ (and, hence, $1 = e^{i \frac{2\pi}{N} xd}$), for all $x \in [P]$, which is possible only if $d \geq P$. This constraint is especially significant for experimental realizations, where coherently manipulating high-dimensional target systems together with high-dimensional control systems is challenging\cite{18}. For example, this limitation implies that if the polarization of a single photon ($d = 2$) is used as the target system, the algorithm is useful only for $P = 2$; despite the fact that the spatial degree of freedom of the photon is amenable to encode much higher-dimensional control systems\cite{33}. To overcome this, we next introduce another variant of phase-estimation problem that is considerably less sensitive to the determinant constraint.

A new computational primitive: the Hadamard promise problem

We consider a different promise on the gates that the oracle $O$ outputs. Given a known $P \times P$-dimensional square matrix $M_P$ of entries $m_{x,y} = \pm 1$, we require that the black-box unitaries in $U$ satisfy, for all $x \in [P]$, the property:

\[
\Pi_x = m_{x,y} \Pi_0, \tag{4}
\]

for some fixed, $a$ priori unknown matrix column $y \in [P]$. The task is, again, to find out $y$. In contrast to the complex-phase relation of Eq. (2), the constraint that this real-phase relation imposes on $d$ is much softer. As one can see taking the determinant of both sides of Eq. (4), the only requirement that arises now is that $(m_{x,y})^d = 1$ for all $x, y \in [P]$, which is satisfied by any even $d$. With this, the promise problem finds application even when the target system is a simple qubit, regardless of the number of permutations $P$. Instead of a single complex phase factor, the value of $y$ is now encoded in a string of $P$ real phase factors (i.e., a column of $M_P$). The question, then, is how to decode that information. Luckily, the value of $y$ can be mapped back onto the computational basis of $C$ with a simple procedure, similar to that in Eq. (3), provided that $M_P$ is a Hadamard matrix\cite{34}.

A Hadamard matrix (of order $P$) is a $P \times P$-dimensional square matrix $M_P$ with entries $m_{x,y} = \pm 1$ and whose columns (or equivalently, whose rows) are all mutually orthogonal. The transpose $M_P^T$ of $M_P$ is proportional to its inverse: $\frac{1}{\sqrt{P}} M_P \cdot M_P^T = 1$, with the identity matrix. Such matrices can only exist for $P$ equal to 1, 2 or integer multiples of 4, and are conjectured to exist for all such dimensions. In fact, they can be generated recursively for any $P = 2^k$, with $k \in \mathbb{N}$. Here we are actually interested in the subset of Hadamard matrices with all $+1$’s in the first row ($x = 0$) and column ($y = 0$), as this is necessary for Eq. (4) and for the correct decoding. With this, we can formally rephrase this promise problem as follows.

**Problem 1** (Hadamard promise problem). *Given a Hadamard matrix $M_P$ with all $+1$ entries along its first row and column and a unitary-gate oracle $O$ fulfilling the promise — i.e. Eq. (4) for some column $y \in [P]$ of $M_P$ — compute $y$.*

The algorithm to solve it with the quantum $N$-switch gate is similar to the Araújo-Costa-Brukner algorithm but with the quantum Hadamard gate $H_P$ associated to $M_P$ playing the role of $F_P$. The matrix representation of $H_P$ in the computational basis is $H_P := \frac{M_P}{\sqrt{P}}$. Then, the following algorithm solves Problem 1.

**Algorithm 1.** Initialize the joint system in the state $|0\rangle_c |\Psi_t\rangle$, with $|\Psi_t\rangle$ an arbitrary target state. Then, apply $H_P$ on $C$.  


Then, apply $S_N$ on the joint $C - T$ system. Then, apply $H_P^{-1}(= H_T^{-1})$ on $C$. This gives the state

$$H_P^{-1} S_N H_P |0\rangle_c |\Psi\rangle_t = |y\rangle_c \Pi_0 |\Psi\rangle_t .$$  

Finally, read out $y$ as the outcome of a single-shot computational-basis measurement on $C$.

This algorithm thus provides the desired phase relation between the $P$ different permutations of the $N$ unknown unitaries under consideration. The validity of Eq. (5) is proven explicitly in App. 1. The query complexity of the algorithm is the same as that of the Araújo-Costa-Brunker algorithm: $Q = N$ for all $P \leq N!$. The crucial resource for Algorithm 1 is the quantum $N$-switch process. Similarly to the Fourier promise problem\(^{14}\), no causally ordered process is known to solve Problem 1 in general (i.e., for any arbitrary set $U$ of unknown gates fulfilling the promise) with a query complexity linear in $N$. In fact, the (query-wise) optimal causally ordered processes known to solve the problem in general are simply the fixed-gate circuits that simulate the quantum $N$-switch exactly (see Methods section), but these require considerably more queries\(^{13,14,17}\). For instance, in the case where all gate permutations are considered ($P = N!$), simulating the quantum $N$-switch exactly in the blackbox scenario requires $Q = \Omega(N^2)$ oracle queries, i.e. quadratically higher in $N$. Another concrete example is the quantum $4$-switch process for the $P = 4$ permutations in the set $\Sigma = \{ ABCD, BADC, CBDA, DACB \}$ [shown in Fig. 1 (b)], whose experimental implementation we describe below. The optimal circuit to simulate it exactly in the blackbox scenario requires $Q = 9$ oracle queries, i.e. more than twice as many as with $S_4$ (see App. 2).

**Experimental quantum control of the order of multiple gate operations**

The experiment is illustrated in Fig. 2 (a). It is based on multi-core optical fibers and new related technology\(^{23}\), which was recently introduced as a toolbox for quantum information processing\(^{24-26}\). In our implementation of the quantum 4-switch, the control system corresponds to the spatial mode of a single photon, while the target is its polarization. Following Algorithm 1, a conventional illumination scheme (see Methods) is used to generate single photons propagating over a single-mode fiber in the initial spatial mode state $|0\rangle_c$. The photons are then sent through a four-core fiber beam splitter (4CF-BS), which has been shown to realize with high-fidelity the $H_4 = \frac{4\sqrt{2}}{2}$ Hadamard operation given by\(^{35}\)

$$H_4 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix} .$$  

Note that this matrix is self-inverse. The 4CF-BS is placed between commercial spatial multiplexer/demultiplexer (DMUX) units\(^{36,37}\), which couple four single-mode fibers (yellow fibers) to the four cores of the multi-core fibers (green fibers). These units connect to the 4CF-BS through the multi-core fibers [see details in Fig. 2 (b)].

After transmission through the 4CF-BS, the photon is sent to the quantum 4-switch gate $S_4$, which will coherently apply different permutations of four unitary operations $U_i$ on the target system (photon polarization), depending on the spatial mode. To see this, note that each output of the 4CF-BS routes the photon through a different ordering of the polarization operations $U_i$, which are realized with controllable liquid crystal retarders (LCR). To control the implementation order of the $U_i$’s, we take advantage of the DMUX units. Each single-mode fiber input to the quantum 4-switch gate is connected to a different four-core fiber on the IN side of $S_4$ using a DMUX unit. The other end of each 4CF is attached to a fiber launcher. The photon leaves the launcher in free space passing through the LCR and is coupled back into another 4CF on the OUT side. The OUT 4CF is connected (via another DMUX) to single mode fibers, which are then connected to the next 4CF (exploiting the already installed DMUXs) back on the 4-switch’s IN side, following the ordering showed in Fig. 2 (a). For example, a photon in the green input undergoes the operation of the four unitaries in the order $C \rightarrow B \rightarrow D \rightarrow A$, resulting in the product unitary $\Pi_2 = U_A U_D U_B U_C$. The other three inputs lead the photon through one of the other three permutations shown in the insets of Fig. 1 (b). After $S_4$, a second Hadamard operation is applied to the control system using a second set of DMUX/4CF-BS/DMUX, in accordance with Algorithm 1. The setup is thus a four-arm interferometer with each output directly connected to an InGaAs single-photon detector (APD), working in gated mode and configured with 10% overall detection efficiency, and 5 ns gate width. The detection of a single-photon in the $y$-th ($y = 0, 1, 2, 3$) output detector univocally identifies in a single-shot the property $y$ indicating the phase relations of the four unitaries implemented in the quantum 4-switch gate.

Before implementing the quantum 4-switch, an initial alignment procedure using a polarimeter is performed. In-fiber polarization controllers (not shown in Fig. 2) are used in all single-mode fibers of the quantum 4-switch to ensure that every fiber corresponds to an identity operation on the polar-
Figure 2. a) Illustration of our implementation of the quantum 4-switch gate ($S_4$). An input photon is divided coherently between four spatial modes using a four-core fiber beam splitter (4CF-BS), placed between commercial multiplexer/demultiplexer (DMUX) units, as shown in b). The four output modes are then sent to the quantum 4-switch $S_4$. Each spatial mode is related to a unique permutation of the four unitary polarization operations applied by $S_4$ and indicated by a different color. The photons enter through the IN side (right) and exit through the OUT side (left), where, for example, the notation "← A" means "from A" and "A ←" means "to A". For instance, the green input mode corresponds to the operation of the four polarization unitaries in the order $CBDA$. After $S_4$, the four spatial modes are then recombined using a second 4CF-BS. Each output 0–3 is connected directly to a single-photon detector (APD). The detection of a single-photon in the $y$-th ($y = 0, 1, 2, 3$) output detector identifies in a single-shot the phase relation $y$ of the four unitaries implemented in the quantum 4-switch gate. See the main text and Methods for further details.

The LCRs implementing the unitaries can be adjusted between identity and a half-wave plate by controlling the input voltage. In this way, we can toggle between an identity operation 1 and one of the Pauli operators $Z, (Z + X)/\sqrt{2}$ or $X$, when the orientation angle of the LCR is $0^\circ$, $22.5^\circ$ or $45^\circ$, respectively. Importantly, we note that the LCRs were placed at the far-field plane of the 4CF launchers and that this guarantees that the unitary operations $U_i$ are indistinguishable when applied in different orders (see Methods). A computer-controlled field programmable gate array (FPGA2) unit is used to control the LCRs.

In Chart I we list the polarization operations $U_i$ for two different implementations of the quantum 4-switch. Table 1 corresponds to orthogonal operations (for each given column), while Table 2 includes non-orthogonal ones, which makes it more difficult to mimic the quantum $N$-switch with a causally ordered process (see below and App. 3). In each table, the $y$-th column defines a different set $U$ of the target-system unitary gates and corresponds to the $y$-th column of the Hadamard matrix in Eq. (6) (see Methods). In our experiment, by exploiting the controlled LCRs, we are able to toggle between the different sets $U$ of unitaries in real time. Fig. 3 (a) shows an example of the results recorded while switching randomly between operations corresponding to different columns of Table 1, about every minute. In each 0.1 s measurement we detected a total of $\sim 6000$ events. Figs. 3 (b) and (c) show a summary of experimentally obtained success probabilities (each obtained from $\sim 3 \times 10^4$ events) to identify the relative-phase relations between the different permutations of the unitary operations in Table 1 and Table 2, resp. For Table 1 we obtain an average success probability of $p_{\text{succ}} = 0.948 \pm 0.005$, whereas for Table 2 we obtain $p_{\text{succ}} = 0.959 \pm 0.008$. Error
Figure 3. a) A sequence of measurement results with our quantum 4-switch process taken in real time. Each “step” corresponds to a 0.1s duration measurement realized within the phase stabilization routine (see Methods), in which the four sets of unitaries given each by the $y$-th column of Table 1 were toggled randomly every minute. Summary of experimentally obtained success probabilities to identify the commutation relations of the unitary operations in Table 1 (b) and Table 2 (c). See text for more details.

Towards unconditionally benchmarking experimental quantum control of multiple gate orders

To benchmark the realization of QCGO, it is useful to imagine a verification scenario, in which a Verifier controls the oracle, while the process is implemented by a Prover. The Prover wishes to prove to the Verifier that the process does display QCGO, and the Verifier can test this by asking the Prover to compute properties of oracles involving different gates. The quantum $N$-switch process allows the Prover to solve the computations with considerably fewer oracle queries than any process with fixed (or classically controlled) gate connections. Indeed, it is the only process known to provide a unit success probability for Problem 1 in general (i.e. for any set of black-box gates satisfying the promise) with only $N$ queries to the oracle. This can be used to give the Verifier evidence in favour of the Prover’s honesty. However, if the table of oracle-gates is restricted — e.g., as in Chart 1 — a dishonest Prover with side information about the table can attain $p_{\text{succ}} = 1$ with a causally ordered process (see App. 3), thus deceiving the Verifier.

One way to benchmark experimental quantum switches with minimal assumptions is by measuring so-called causal witnesses. Interestingly, by increasing the number of columns in the oracle-gate table (i.e., of possible choices for the gate sets $U$), Algorithm 1 can be turned into a causal witness for $W_{N}$. That is, for sufficiently large oracle-gate tables, a non-unit upper bound for $p_{\text{succ}}$ over all causally ordered processes can be found, proving a gap with $W_{N}$ (whose success probability remains always unity). Unfortunately, the number of measurement settings required is prohibitively high in practice. For instance, the best witness for $W_{4}$ we could attain with this approach gives $p_{\text{succ}} \approx 0.92$, but requires an oracle-gate table with 744 columns. Alternatively, weaker witnesses with $p_{\text{succ}} \approx 0.95$ can also be found, but these still require 124 columns. Apart from the large statistical errors due to so many settings, no current experimental setup can switch among so many gates in a practical way. Nevertheless, it is yet a remarkable feature of our experiment that we do reach values of $p_{\text{succ}}$ that would conclusively benchmark $W_{4}$ for higher number of settings.

Alternatively, smaller oracle-gate tables suffice if the Verifier can actively reduce the Prover’s potential knowledge about the tables. One way to do this is by allowing the Verifier to apply a random basis rotation to each gate before delivering it to the Prover. For instance, in this scenario, an upper bound of $p_{\text{succ}} \approx 0.88$ can be placed on all $p_{\text{succ}}$ obtainable through causally ordered processes for an oracle-gate table with only 31 columns. Unfortunately, implementing such a causal witness would require the ability to switch among a continuum of gates, which is again experimentally infeasible. Nevertheless, here we are mainly interested in benchmarking our implementation of $W_{4}$ against experimental imperfections, rather than against hypothetical malicious Provers exploiting side-information about the gates’ bases. Hence, that the experimentally obtained values of $p_{\text{succ}} \approx 0.95$ are well above the threshold found using 31 columns gives us a strong evidence for QCGO of the implemented process.

Discussion

Here we introduced the “Hadamard promise problem”, a novel computational primitive involving the relative phases between different permutations of multiple unknown gates. We presented an algorithm to solve it efficiently, illustrating a quantum computational advantage associated to the coherent quantum control of the order in which a sequence of $N$ unitary operations is applied. Our algorithm, which we implemented experimentally for $N = 4$, exploits the quantum $N$-switch process to solve the problem with $N$ applications of the unitary gates, whereas the known methods exploiting fixed gate orders use the gates $O(N^2)$ times. Both problem and algorithm have the advantage that the target system needs only be two-dimensional, as opposed to $N^4$-dimensional as in previous proposals. This could inspire new approaches for exploiting indefinite causal order in quantum computation and communication, as well as for studying causal non-separability in physical systems.
We experimentally implemented the algorithm by constructing a quantum 4-switch process that coherently controls four different gate orderings with high fidelity, showing success probabilities for the algorithm of ~ 0.95. The all-optical setup involves a four-path interferometer constructed with new multi-core optical fiber technology. As discussed in the Methods, the best known quantum circuit with fixed gate orders solves this problem with 9 gate queries. Our experiment thus corresponds to a 5-query improvement. Moreover, this is, to the best of our knowledge, the first report of a quantum superposition of more than 2 temporal orders. In addition, our implementation presents some technical advantages as well: On the one hand, it is versatile in that the gate orders can be modified in a practical fashion by switching the optical fiber connections and that the unitary gates themselves can be automatically controlled through the liquid crystal polarization retarders. On the other hand, the setup can be scaled up to higher control-system dimensions in a straightforward fashion. This work constitutes a key step towards realizing and verifying causal non-separability among a large number of parties, and should play an important role in developing methods to exploit this resource.

Methods

A. Query complexity analysis

One may argue that implementing $S_N$ is not the only way to solve Problem 1 (which is also true for the Fourier promise problem)\cite{14}. Here, we estimate the query complexity of other plausible approaches.

A natural approach one may attempt is to tomographically reconstruct the $N$ unitary gates and then multiply them to estimate the $\Pi_x$’s, from which one can infer $y$. Since each $\Pi_x$ is an $N$-fold product of the $U_i$’s, the overall error $\epsilon$ in its estimation is $\epsilon = \Omega(N^2 \epsilon)$, where $\epsilon$ is the statistical error of the reconstruction of each $U_i$. To attain a constant overall error one thus needs $\epsilon = O(1/N)$, which, by virtue of Hoeffding’s bound, in turn requires $q = \tilde{O}(1/\epsilon^2) = O(N^2)$ queries to each $U_i$. Moreover, since there are $N$ gates to reconstruct, the overall query complexity is $Q = \tilde{O}(N^3)$, i.e. cubically worse in $N$ than with the quantum $N$-switch. Another alternative is to tomographically reconstruct each $\Pi_x$ directly, and from that infer $y$. However, to query each $N$-fold product $\Pi_x$ one must query all $N$ unitaries; and there are $P$ such products. Hence, the overall query complexity is $Q = \tilde{O}(NP) \geq O(N^2)$ if one considers $P \geq N$ (as we did in our experimental demonstration), i.e. quadratically worse in $N$ than with the quantum $N$-switch. A third possibility could be to directly estimate the signs of the commutators between the $\Pi_x$’s, and from that infer $y$. A canonical tool for that is the well-known Hadamard test\cite{31}. This allows one to estimate overlaps of the form $\langle \Psi_i | \Pi_x | \Psi_j \rangle$ or $\langle \Pi_i | \Pi_x | \Pi_j \rangle$, directly from queries to $\Pi_x$ or $\Pi_x$ and $\Pi_y$, respectively, for any state $| \Psi_i \rangle$. As before, each query to $\Pi_x$ accounts for $N$ queries to the gates, and the overall query complexity is again $Q = \tilde{O}(NP) \geq O(N^2)$.

Finally, one can simulate $S_N$ exactly with a circuit with fixed gate orders. For the usual case where all $P = N!$ permutations are considered, the optimal causally ordered circuit that synthesizes $S_N$ in the blackbox scenario displays complexity $Q = \Omega(N^2)$\cite{13,14,17}. For the concrete case experimentally studied here, $P = N = 4$, the optimal causally ordered circuit that synthesizes $S_4$ requires 9 queries (see App. 2). In fact, this is the reason why we chose the particular permutation set $\Sigma = \{ ABCD, BADC, CBDA, DACB \}$. Through a brute-force search, we found that, from all quartets of permutations, most of them require 7 queries or less with the simulation strategy presented in App. 2, some other 8 queries, and a few of them (including the one chosen here) require the maximum of 9 queries. Thus, the specific version of the quantum 4-switch implemented here provides a gap of $9 - 4 = 5$ queries with respect to all causally ordered processes.

B. Experimental details

Single photon source.— The single-photon light source is composed of a semiconductor distributed feedback telecom laser ($\lambda = 1546$ nm) connected to an external fiber-pigtailed amplitude modulator (MZI). An FPGA unit (FPGA1) was used with the MZI to externally modulate the laser and generate optical pulses 5 ns wide. Optical attenuators (ATT) are used before MZI to create weak coherent states with a mean photon number per pulse of $\mu = 0.2$. In this case, 90% of the non-null pulses generated contain a single photon. Thus, our source is a good approximation to a non-deterministic single-photon source, which is commonly adopted in quantum communications\cite{41}. FPGA1 also controls the active phase stabilization of the system and registration of single-photon counts at each of the four detectors during the measurement procedure (see below).

Indistinguishability of the multi-gate operations in different orders.— The four unitary operators $U_i$ ($i = A, B, C, D$) were realized using birefringent liquid crystal retarders. An important aspect of the experiment is to guarantee the realization of the same unitary operation $U_i$ for all different orders considered. That is, the implementation of $U_i$ must be independent of the illuminated core on the corresponding 4CF at the IN side of the oracle. To achieve this, the LCRs are placed in the Fourier plane of the objective lenses of the 4CF fiber launchers (see Fig. 4 (a)). At the exit face of this fiber, the output single mode of each core is given by a gaussian function $g(|\vec{r}|)$ centered at the core position $\vec{r}_c$. At the Fourier plane of the launcher lens, the spatial distribution of each core is given by the Fourier transform $\mathcal{F}[g(|\vec{r} - \vec{r}_c|)](|\vec{s}|) \propto \exp(i k |\vec{s} - \vec{r}_c|/f) g(|\vec{s}|)$. Therefore, irrespective of the illuminated core, all core modes overlap at the same central point with the intensity proportional to $|g(|\vec{s}|)|^2$. This avoids spatial distinctions as in certain implementations for $N = 2$ gates\cite{18,19}. To guarantee this condition for our experiment, we used a CCD camera to record the intensity distributions at the Fourier plane (with the LCRs removed), as shown in Fig. 4 (b). The images, obtained with an intense laser, show the centering of the light distribution when a single core is connected. The resulting interference pattern when all cores are illuminated shows high-visibility,
confirming spatial indistinguishability. This guarantees that the unitary operations \( U_i \) are indistinguishable when applied in different orders—a crucial requirement for a valid implementation of an N-switch.\(^{20}\)

**Phase stabilization and Measurement procedure.**— Phase (PHASE MOD) and intensity modulators (INT MOD) are used after the first 4CF-BS, on each arm of the interferometer (see Fig. 2 (a)), to set the relative phases between the four spatial modes to zero, and to adjust the amplitudes. The FPGA1 unit is used to implement a control system to actively compensate phase-drifts in the quantum 4-switch. The control is based on a perturb and observe power point tracking algorithm that will perturb the \( j \)th phase modulator to cancel any phase noise using a high-speed signal. The algorithm does this sequentially to each phase modulator and in each step it maximizes the number of photo-counts in the output detector “0” with the LCRs set to realize column \( y = 0 \) of one of the tables in Chart I. When the counts achieve a given threshold value for the success probability, the voltages applied to the phase modulators are maintained constant, and an OFF signal is sent to FPGA2 to activate the LCRs by applying a constant voltage, realizing any one of the four columns of the respective Table in Chart I, chosen by the user. After a 0.2 s deadtime to allow for the LCRs voltages to reach the desired value, a 0.1 s measurement stage is realized. After a single measurement window, an OFF signal is sent to return the LCRs to column 0. In this way, we can switch rapidly between columns 0–3 of the tables. The control system monitors the phase stabilization of the interferometer in real-time after every measurement.

**Acknowledgements**

We thank Fabio Costa and Časlav Brukner for helpful insights. MMT and LA acknowledge financial support from the Brazilian agencies CNPq (PQ grant No. 311416/2015-2 and INCT-IQ), FAPERJ (PDR10 E-26/202.802/2016 and JCN E-26/202.701/2018), CAPES (PROCAD2013), and the Serapilheira Institute (grant number Serra-1709-17173). This work was also supported by Fondo Nacional de Desarrollo Científico y Tecnológico (Conicyt) (1160400, 3200779, 11150325) and Millennium Institute for Research in Optics. MA has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 801110 and the Austrian Federal Ministry of Education, Science and Research (BMBWF). It reflects only the author’s view, the EU Agency is not responsible for any use that may be made of the information it contains. AA was supported by the Swiss National Science Foundation (Starting Grant DIAQ).

---

1. Ognyan Oreshkov, Fabio Costa, and Časlav Brukner, “Quantum correlations with no causal order,” Nature Communications 3, 1092 (2012), arXiv:1105.4464 [quant-ph].
2. Mateus Araújo, Cyril Branciard, Fabio Costa, Adrien Feix, Christina Giarmatzi, and Časlav Brukner, “Witnessing causal nonseparability,” New Journal of Physics 17, 102001 (2015), arXiv:1506.03776 [quant-ph].
3. Ognyan Oreshkov and Christina Giarmatzi, “Causal and causally separable processes,” New Journal of Physics 18, 093020 (2016), arXiv:1506.05449 [quant-ph].
4. Lucien Hardy, “Probability Theories with Dynamic Causal Structure: A New Framework for Quantum Gravity,” (2005), arXiv:gr-qc/0509120.
5. Lucien Hardy, “Towards quantum gravity: A framework for probabilistic theories with non-fixed causal structure,” Journal of Physics A: Mathematical and Theoretical 40, 3081–3099 (2007), arXiv:gr-qc/0608043.
6. Lucien Hardy, “Quantum Gravity Computers: On the Theory of Computation with Indefinite Causal Structure,” in Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony (Springer Netherlands, Dordrecht, 2009) pp. 379–401, arXiv:quant-ph/0701019.
7. Giulio Chiribella, Giacomo Mauro D’Ariano, Paolo Perinotti, and Benoît Valiron, “Quantum computations without definite causal structure,” Physical Review A 88, 022318 (2013), arXiv:0912.0195 [quant-ph].
8. M. Araújo, P. Allard Guérin, and A. Baumeler, “Quantum computation with indefinite causal structures,” Phys. Rev. A 96, 052315 (2017), arXiv:1706.09854 [quant-ph].
9. Magdalena Zych, Fabio Costa, Igor Pikovski, and Časlav Brukner, “Bell’s theorem for temporal order,” Nature Communications 10, 3772 (2019), arXiv:1708.00248 [quant-ph].
10. G. Chiribella, G. M. D’Ariano, and P. Perinotti, “Quantum Circuit Architecture,” Physical Review Letters 101, 060401 (2008), arXiv:0712.1325 [quant-ph].
11. Giulio Chiribella, Giacomo Mauro D’Ariano, and Paolo Perinotti, “Theoretical framework for quantum networks,” Physical Review A 80, 022339 (2009), arXiv:0904.4483 [quant-ph].
Kejin Wei, Nora Tischler, Si-Ran Zhao, Yu-Huai Li, Juan Miguel Arrazola, Yang Liu, Weijun Zhang, Hao Li, Lixing You, Zhen Wang, Yu-Ao Chen, Barry C. Sanders, Qiang Zhang, Geoff J. Pryde, Feihu Xu, and Jian-Wei Pan, “Experimental quantum switching for exponentially superior quantum communication complexity,” Physical Review Letters 122, 120504 (2019), arXiv:1810.10238 [quant-ph].

Stefano Facchin and Simon Perdrix, “Quantum Circuits for the Unitary Permutation Problem,” in Theory and Applications of Models of Computation. Proceedings. Lecture Notes in Computer Science, Vol. 9076, edited by Rahul Jain, Sanjay Jain, and Frank Stephan (Springer International Publishing, 2015) pp. 324–331, arXiv:1405.5205 [quant-ph].

Lorenzo M. Procopio, Amir Moqanaki, Mateus Araújo, Fabio Costa, Iraïo Alonso Calafell, Emma G. Dowd, Deny R. Hamel, Lee A. Rozema, Cás lav Brukner, and Philip Walther, “Experimental superposition of orders of quantum gates,” Nature Communications 6, 7913 (2015), arXiv:1412.4006 [quant-ph].

Güliubin, Lee A. Rozema, Adrien Feix, Mateus Araújo, Jonas M. Zeuner, Lorenzo M. Procopio, Cás lav Brukner, and Philip Walther, “Experimental verification of an indefinite causal order,” Science Advances 3, e1602589 (2017), arXiv:1608.01683 [quant-ph].

K. Goswami, C. Giarmatzi, M. Kewming, Costa, C. Bram- ciard, J. Romero, and A. G. White, “Indefinite Causal Order in a Quantum Switch,” Physical Review Letters 121, 090503 (2018), arXiv:1803.04302 [quant-ph].

Yi Guo, Xiao-Min Hu, Zhi-Bou Hou, Huan Cao, Jin-Ming Cui, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, and Guang-Can Guo, “Experimental investigating communication in a superposition of causal orders,” (2018), arXiv:1811.07526 [quant-ph].

K. Goswami, Y. Cao, G. A. Paz-Silva, J. Romero, and A. G. White, “Communicating via ignorance: Increasing communication capability via superposition of order,” (2018), arXiv:1807.07383 [quant-ph].

D. J. Richardson, J. M. Fini, and L. E. Nelson, “Space–division multiplexing in optical fibres,” Nature Photonics 7, 354–362 (2013), arXiv:1303.3908 [physics.optics].

G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przyziezna, E. S. Gómez, M. Figueroa, G. Val- lone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, and G. Lima, “High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers,” Physical Review A 96, 022317 (2017), arXiv:1610.01682 [quant-ph].

Yunhong Ding, Davide Bacco, Kjeld Dalggaard, Xinlin Cai, Xia-aoqi Zhou, Karsten Rottwitt, and Leif Katsuo Oxenløwe, “High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits,” npj Quantum Information 3, 25 (2017), arXiv:1610.01812 [quant-ph].

Guilherme B. Xavier and Gustavo Lima, “Quantum information processing with space-division multiplexing optical fibres,” Communications Physics 3, 9 (2020), arXiv:1905.12644 [quant-ph].

Lorenzo M. Procopio, Francisco Delgado, Marco Enríquez, Na- dia Belabas, and Juan Ariel Levenson, “Communication Enhancement through Quantum Coherent Control of N Channels in an Indefinite Causal-Order Scenario,” Entropy 21, 1012 (2019), arXiv:1902.01807 [quant-ph].

Lorenzo M. Procopio, Francisco Delgado, Marco Enríquez, Na- dia Belabas, and Juan Ariel Levenson, “Sending classical information via three noisy channels in superposition of causal orders,” Physical Review A 101, 012346 (2020), arXiv:1910.11137 [quant-ph].

Mateus Araújo, Adrien Feix, Miguel Navascués, and Cás lav Brukner, “A purification postulate for quantum mechanics with indefinite causal order,” Quantum 1, 10 (2017), arXiv:1611.08535.

Márco M. Taddei, Ranieri V. Nery, and Leandro Aolita, “Quantum superpositions of causal orders as an operational resource,” Physical Review Research 1, 033174 (2019), arXiv:1903.06180 [quant-ph].

Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf, “Quantum fingerprinting,” Phys. Rev. Lett. 87, 167902 (2001), quant-ph/0102001 [quant-ph].

A. Yu. Kitaev, “Quantum measurements and the Abelian Stabi- lizer Problem,” (1995), arXiv:quant-ph/9511026.

Edgar A. Aguilar, Maté Farkas, Daniel Martínez, Matías Al- varado, Jaime Cariñe, Guilherme B. Xavier, Johanna F. Barra, Gustavo Cañas, Marcin Pawłowski, and Gustavo Lima, “Certifying an Irreducible 1024-Dimensional Photonic State Using Refined Dimension Witnesses,” Physical Review Letters 120, 230503 (2018), arXiv:1710.04601 [quant-ph].

K. J. Horadam, Hadamard Matrices and Their Applications (Princeton University Press, Princeton, 2007).

J. Cariñe, G. Cañas, P. Skrzypczyk, I. Šupič, N. Guerrero, T. Garcia, L. Pereira, M. A. S. Prosser, G. B. Xavier, A. Delgado, S. P. Walborn, D. Cavalcanti, and G. Lima, “Multi-port beam splitters based on multi-core optical fibers for high-dimensional quantum information,” (2020), arXiv:2001.11056 [quant-ph].

K. Watanabe, T. Saito, K. Imamura, and M. Shiino, “Development of fiber bundle type fan-out for multicore fiber,” in IEEE 17th Opto-Electronics and Communications Conference (2012) pp. 5C1–2.

Y. Tottori, T. Kobayashi, and M. Watanabe, “Low Loss Optical Connection Module for Seven-Core Multicore Fiber and Seven Single-Mode Fibers,” IEEE Photonics Technology Letters 24, 1926–1928 (2012).

S. P. Walborn, M. O. Terra Cunha, S. Pádua, and C. H. Monken, “Double-slit quantum eraser,” Physical Review A 65, 033818 (2002), arXiv:quant-ph/0106078.

F. A. Torres-Ruiz, G. Lima, A. Delgado, S. Pádua, and C. Saave- dra, “Decoherence in a double-slit quantum eraser,” Physical Review A 81, 042104 (2010), arXiv:0911.0330 [quant-ph].

Cyriel Branciard, “Witnesses of causal nonseparability: an intro- duction and a few case studies,” Scientific Reports 6, 26018 (2016), arXiv:1603.00043 [quant-ph].

Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, “Quantum cryptography,” Reviews of Modern Physics 74, 145–195 (2002), arXiv:quant-ph/0101098.

Pallavee Bhatnagar and R.K. Nema, “Maximum power point tracking control techniques: State-of-the-art in photovoltaic ap- plications,” Renewable and Sustainable Energy Reviews 23, 224–241 (2013).
with black-box unitaries. A workaround is to use ancillas and controlled swap gates that coherently control whether each target-system gate is effectively applied to the target system or to an ancilla. This can be done with a circuit such as in Fig. 5, which uses a \( P \)-dimensional control qudit and \( N \)-dimensional ancilla systems (one for each gate \( U_i \)). Importantly, as the reader may verify, all \( N \) ancillas experience the same overall gate sequence for all input states of the control register, which guarantees that the ancillas disentangle from the target and control systems by the end of the circuit. For instance, for the circuit in Fig. 5, the final state of the ancillas is \( U_A^2 |0\rangle_{\text{anc},A} U_B |0\rangle_{\text{anc},B} U_C |0\rangle_{\text{anc},C} U_D |0\rangle_{\text{anc},D} \).

With this circuit scheme, the problem of simulating the superposition of unitaries produced by a quantum \( N \)-switch reduces to finding a supersequence that includes all the desired permutations as subsequences; the query complexity of this scheme is then given by the length of the shortest such supersequence. In the experiment and Fig. 5, \( ACBADA|DACDB \) is the supersequence to the quartet of permutations \( \{ABCD, BADC, CBDA, DACB\} \) (notice that the subsequences need not be contiguous). We have made an extensive numerical search of all quartets of permutations of \( A, B, C, D \). There are \( \binom{N}{3} = (\frac{N}{3}) \) = 1771 unique quartets, where quartets that differ only by relabeling are disregarded (this amounts to, for instance, only considering quartets that include some fixed permutation, e.g. \( ABCD \)). Of those, most require a supersequence of length 8 or less (37 unique quartets require length 6; 946 require length 7; 779 require length 8) and only 9 require length 9. Since the higher the supersequence length, the higher the query complexity of the simulation by fixed-gate-order circuit, we chose one of the latter 9 quartets for our experiment (as well as Fig. 5). Notice that all 9 black boxes are queried once, irrespective of whether they are effectively used in the superposition or not, hence the query complexity of this simulation of the quantum 4-switch is 9.

3. Fixed-gate circuit algorithms for the Hadamard promise problem exploiting side information about the gates

Let us revisit the adversarial scenario of a Verifier who controls the oracle and poses the Hadamard promise problem to a Prover. The Prover thus receives unknown (to them) unitaries and uses them to the best of their abilities to solve the problem and output the correct answer to the Verifier. As we showed, a Prover in possession of a quantum \( N \)-switch can solve the problem with 100% success rate using only a single query from each unitary. We now ask: can a Prover solve the problem with access only to fixed-gate-order circuits?

By performing the simulations in the previous section, they are also able to solve the Hadamard promise problem with 100% success rate. However, they must request additional queries of the oracle to the Verifier, a tell-tale sign to the latter that the quantum \( N \)-switch has not been realized.

We now explore the case of a Prover with side information on the unitaries from the oracle. More specifically, let us suppose they know the Table of unitaries that the Verifier uses...
By inputting a $|+\rangle$ state to black box $U_A$, the output state will be either $|+\rangle$, if $U_A = 1$, or $|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$, if $U_A = Z$. With a measurement of the output in the $X$ basis, they can identify $U_A$ (we call this an $X$-basis test on $U_A$). Doing the same procedure on $U_C$, they identify this unitary as well and discover the column $y$ of Table 1 being used. Since only 1 query or less of each unitary is needed, the Prover can in fact deceive the Verifier in this case.

If instead Table 2 is used, the Prover requires a slightly more complex fixed-gate-order circuit to deceive the Verifier. It begins with an $X$-basis test on applied to $U_C$, which reveals the content of that black box. In turn, $U_D$ is revealed with an analogous $Z$-basis test, with input state $|0\rangle$ and measurement of output in the $Z$ basis. If one of these two black boxes is revealed to be a Pauli operator ($Z$ or $X$, resp.), then that run of the promise problem has been solved ($y = 1$ or 3, resp.). However, if both $U_C = \mathbb{1}$ and $U_D = \mathbb{1}$, both $y = 0$ and $y = 2$ are possible, and the black boxes $U_A$, $U_B$ need to be used. Since the quantum $N$-switch finds the correct value of $y$ with probability one, so is the goal of the Prover here. However, the two possible unitaries for $U_A$ ($\frac{Z+X}{\sqrt{2}}$, $Z$) are not orthogonal, i.e. not perfectly distinguishable, and the same happens with $U_B$. No independent use of $U_A$ and $U_B$ can tell the columns apart with certainty. There is a viable strategy, though, using $U_A$ and $U_B$ in sequence. Notice indeed that $U_BU_A = \mathbb{1}$ for column 0 and $U_BU_A = -iY$ for column 2. A $Z$- or $X$-basis test applied to the sequence of the two unitaries $U_A$ and $U_B$ can distinguish these two possibilities, again solving the problem with certainty.

If the Prover does not know whether the Verifier uses Table 1 or 2, the former needs to first identify which Table is used. This information aids the Prover, who may no longer need to produce the superposition of unitaries from the previous section.

If Table 1 is used, the Prover’s strategy is relatively simple. By inputting a $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ state to black box $U_A$, the output state will be either $|+\rangle$, if $U_A = 1$, or $|\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$, if $U_A = Z$. With a measurement of the output in the $X$ basis, they can identify $U_A$ (we call this an $X$-basis test on $U_A$). Doing the same procedure on $U_C$, they identify this unitary as well and discover the column $y$ of Table 1 being used. Since only 1 query or less of each unitary is needed, the Prover can in fact deceive the Verifier in this case.

If instead Table 2 is used, the Prover requires a slightly more complex fixed-gate-order circuit to deceive the Verifier. It begins with an $X$-basis test on applied to $U_C$, which reveals the content of that black box. In turn, $U_D$ is revealed with an analogous $Z$-basis test, with input state $|0\rangle$ and measurement of output in the $Z$ basis. If one of these two black boxes is revealed to be a Pauli operator ($Z$ or $X$, resp.), then that run of the promise problem has been solved ($y = 1$ or 3, resp.). However, if both $U_C = \mathbb{1}$ and $U_D = \mathbb{1}$, both $y = 0$ and $y = 2$ are possible, and the black boxes $U_A$, $U_B$ need to be used. Since the quantum $N$-switch finds the correct value of $y$ with probability one, so is the goal of the Prover here. However, the two possible unitaries for $U_A$ ($\frac{Z+X}{\sqrt{2}}$, $Z$) are not orthogonal, i.e. not perfectly distinguishable, and the same happens with $U_B$. No independent use of $U_A$ and $U_B$ can tell the columns apart with certainty. There is a viable strategy, though, using $U_A$ and $U_B$ in sequence. Notice indeed that $U_BU_A = \mathbb{1}$ for column 0 and $U_BU_A = -iY$ for column 2. A $Z$- or $X$-basis test applied to the sequence of the two unitaries $U_A$ and $U_B$ can distinguish these two possibilities, again solving the problem with certainty.

If the Prover does not know whether the Verifier uses Table 1 or 2, the former needs to first identify which Table is used. This table identification can be done with a $Z$-basis test on $U_D$, which reveals whether $U_D = X$ or $U_D = \mathbb{1}$. The strategy for Table 1 is applied in the former case, that for Table 2 in the latter (notice that column $y = 3$ is the same for both tables).