TU Delft

Delft University of Technology

Document Version
Final published version

Licence
CC BY

Citation (APA)
van Dam, J., Hellebek, E. R., Propp, T. B., Gonzales-Ureta, J. R., Sørensen, A. S., & Wehner, S. D. C. (2026). Single-click protocols for remote state preparation using weak coherent pulses. *Physical Review Research*, *8*(3), Article 033272. https://doi.org/10.1103/x1nr-qbz7

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

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.

Single-click protocols for remote state preparation using weak coherent pulses

Janice van Dam [1,2,3,*,†] Emil R. Hellebek [4,*,‡] Tzula B. Propp [1,2,3] Junior R. Gonzales-Ureta [5]
Anders S. Sørensen [4] and Stephanie D. C. Wehner [1,2,3]

[1]*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[2]*Kavli Institute of Nanoscience, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[3]*Quantum Computer Science, EEMCS, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[4]*Center for Hybrid Quantum Networks (Hy-Q), Niels Bohr Institute, University of Copenhagen, Jagtvej 155A, Copenhagen DK-2200, Denmark*
[5]*Q*Bird BV, Delftechpark 1, 2628 XJ Delft, The Netherlands*

(Received 16 February 2026; accepted 24 July 2026; published 3 September 2026)

Remote state preparation (RSP) allows one party to remotely prepare a known quantum state on another party's qubit using entanglement. This can be used in quantum networks to perform applications such as blind quantum computing or long-distance quantum key distribution (QKD) with quantum repeaters. Devices to perform RSP, referred to as a client, ideally have low hardware requirements, such as only sending photonic qubits. A weak coherent pulse source offers a practical alternative to true single-photon sources and is already widely used in QKD. Here, we introduce two protocols to the previously known protocol for RSP with a weak-coherent-pulse-based device. The known technique uses a double-click (DC) protocol, where a photon from both the server and the client needs to reach an intermediate Bell state measurement. Here, we add to that a single-click (SC) RSP protocol, which requires only one photon to reach the Bell state measurement, allowing for better performance in certain regimes. In addition, we introduce a double-single-click (DSC) protocol, where the SC protocol is repeated twice, and a CNOT gate is applied between the resulting qubits. DSC mitigates the need for phase stabilization in certain regimes, lowering technical complexity while still improving performance compared to DC in some regimes. We compare these protocols in terms of fidelity and rate, finding that SC consistently achieves higher rates than DC and, interestingly, does not suffer from an inherently lower fidelity than DC, as is the case for entanglement generation. Although SC provides stronger performance, DSC can still show performance improvements over DC, and it may have reduced technical complexity compared to SC. Finally, we show how these protocols can be used in long-distance QKD using quantum repeaters.

DOI: 10.1103/x1nr-qbz7

I. INTRODUCTION

Remote state preparation (RSP) allows one party to remotely and securely prepare a specific quantum state on another party's qubit, using classical information combined with shared entanglement resources [1]. One party, we call a client, can be a quantum device with low quantum capabilities, specifically, it does not need a quantum memory. In quantum networks, it has potential applications in areas such as blind quantum computing (BQC) [2], memory-assisted quantum key distribution (QKD) [3], and QKD over repeater nodes [4].

A key motivation in applications such as QKD and BQC is to minimize quantum hardware requirements for clients, allowing them to perform tasks such as measuring [5–9] or sending quantum states [2,10,11] while offloading complex operations to the server. Other types of clients have been proposed for BQC, like a client that only performs single qubit gates [12] or even a completely classical client, in combination with multiple noncommunicating servers [13–16], though these clients do not allow for QKD.

Here, we will study the scenario where clients prepare and send quantum states. We note that this can technically be considered teleportation rather than RSP, since it requires both the creation of the state to be transferred, rather than just a classical description of the state, and a shared entangled pair. We use the term RSP here to signify the goal of the protocol, which is to transfer a known state onto a distant quantum memory.

While generating single photons remains technologically challenging, weak coherent pulse (WCP) sources can offer a practical alternative: They are not perfect single-photon sources as they emit more than one photon with nonzero probability, but they have much lower cost, are simpler to implement, and can be easily modulated to the optimal parameters. Despite their limitations, WCP sources are widely used in QKD [17–21] due to well-developed techniques that

*These authors contributed equally to this work.
†Contact author: j.vandam-3@tudelft.nl
‡Contact author: emil.hellebek@nbi.ku.dk

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

manage multiphoton emissions [22]. Recently, WCP-based approaches have also been explored for BQC [11,23].

In quantum networks, two protocols are widely used for entanglement generation: the double-click (DC) [24,25] and single-click (SC) [26,27] protocols. DC requires two photons—one from each participating node—to arrive at a Bell state measurement (BSM) station, a scenario often hindered by high losses. SC, on the other hand, requires only one photon to reach the BSM, thereby significantly increasing the success rate, though at the cost of a lower fidelity. Whereas RSP requires entanglement, the entanglement does not need to be stored in both nodes, such that one of the nodes can have lower hardware requirements. When it comes to RSP with a WCP source on the client side, prior work has focused only on the DC protocol [28]. In this study, we explore whether SC can also enhance RSP protocols with a WCP client. To this end, we

(1) Introduce two approaches to performing RSP using a client with a WCP source: single click and double single click (DSC). DSC repeats the SC protocol and uses a controlled-NOT (CNOT) gate aiming to mitigate the need for phase stabilization.

(2) Confirm that SC can indeed achieve higher rates than DC for the same fidelity, consistent with findings from entanglement generation. We find that DSC can also achieve higher rates than DC.

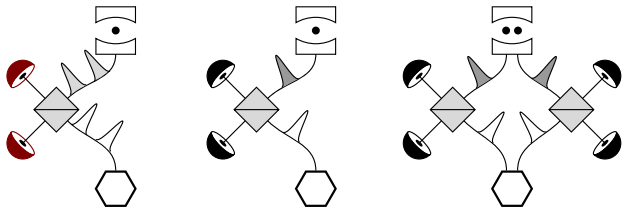
(3) Show that, interestingly, SC and DSC do not inherently suffer from lower fidelity compared to DC, as SC does in entanglement generation, such that SC and DSC have a strict advantage over DC in certain regimes.

(4) Discuss the potential applications of these protocols for BQC and for QKD in repeater networks, where the increased speed provided by SC and DSC protocols could facilitate longer-distance and more robust quantum communication setups.

II. RSP PROTOCOLS

We consider three protocols for performing RSP between a client equipped with a WCP source, and a quantum server, equipped with quantum memory that can emit memory-entangled photons. In all cases, a BSM station is required between the client and the server. Mathematically speaking, the exact position of the BSM (in the middle, closer to client or closer to the server) is irrelevant, as the fiber losses can be taken into account by adjusting the efficiencies η_c, η_s. However, positioning the BSM directly next to the server has some advantages: It reduces the number of nodes needed in the network and it allows for faster RSP attempts. As in most regimes, we are limited by the repetition rate of the server, having the BSM close to the server allows for a reduction of classical communication time. The server can quickly receive success/failure signals and reset for the next attempt, while the client can continuously send pulses at a high rate.

We refer to the three protocols as SC, DSC, and DC. A schematic overview of the protocols is provided in Fig. 1. This terminology is analogous to that used in entanglement generation, where the DC protocol uses orthogonal modes such as polarization or time-bin encoding to carry the quantum information of the photons. The SC protocol uses a presence-absence encoding, allowing entanglement to be formed with only one photon arriving at the BSM [26]. The DSC protocol repeats the SC protocol to eliminate the need for phase stabilization in certain regimes, a topic discussed further in Sec. II E.



(a) Double click (b) Single click (c) Double single click

FIG. 1. Diagram illustrating the three remote state preparation protocols. The ion trap represents the server, with a dot denoting an emitting qubit, while the hexagon represents the client equipped with a weak coherent pulse source. Both client and server send their quantum states to the Bell state measurement station. In the double-click protocol in panel (a), a two-mode encoding is used, such as polarization or time bin, while in the single-click [panel (b)] and double-single-click [panel (c)] protocols, presence-absence encoding is applied in a single-mode configuration. The protocols in panels (a) and (c) both require two photons to be detected, but the protocol in panel (c) allows for retrying of each node separately, as the photons are entangled with separate memory qubits. The color of the detectors in panel (a) illustrates that the detectors can decode the encoding of the photons. The two paths and BSM stations are drawn in panel (c) to illustrate the pulses coming from two different memory qubits. It is not required to have two separate BSM stations. The server's qubit is entangled with the emitted light, which, along with the client's light, is mixed on a beam-splitter and analysed by the BSM. Upon successful detection, the server's qubit is projected into a state selected by the client.

Here, we carry over these known techniques in entanglement generation to RSP using a WCP source. While the DC protocol for WCP-based RSP has been previously demonstrated [28], we provide its description and analytical expressions for the rate and fidelity we can achieve using this protocol here and in Appendix A for completeness and comparison.

Sections II B–II D cover each RSP protocol, along with analytic performance results, which are plotted in Fig. 2 and discussed in Sec. III. A detailed derivation of the analytics can be found in Appendix A. Afterward, in Sec. II E we will provide an extension to the SC and DSC analytics to include errors due to phase noise.

Apart from phase noise and losses, we assume ideal hardware, thus excluding decoherence, gate imperfections, and infidelity in the server photon-matter state. The aim here is to capture the errors that are inherent to using WCPs instead of a single-photon source and the differences between the protocols.

A. Model

Each calculation below will follow the same steps. First, we characterize the input states from the client and server. Here, we look at creating states on the equator of the Bloch

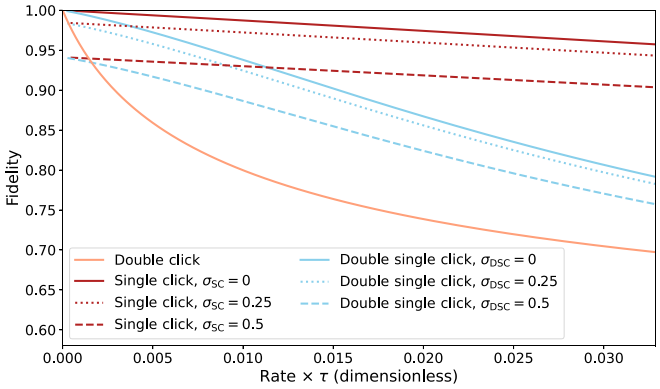


FIG. 2. Trade-offs between fidelity and rate for the three RSP protocols: DC (peach), SC (red), and DSC (blue). Shown for $\sigma_{SC}, \sigma_{DSC} \in \{0$ (solid), 0.25 (dotted), 0.5 (dashed)$\}$. This analysis assumes a server efficiency of $\eta_s = 0.091$, including a detector efficiency of 0.7. The values shown are for $|\alpha|^2 \lesssim 3$ (DC), $|\alpha|^2 \lesssim 0.3$ (SC), $|\alpha|^2 \lesssim 1.2$ (DSC).

sphere, i.e., states of the form $|+_\theta\rangle = (|0\rangle + e^{i\theta}|1\rangle)/\sqrt{2}$ for some angle θ, which are states sufficient for, e.g., QKD [29] and BQC [30].

A loss channel with loss probability $1-\eta_c$ and $1-\eta_s$ is applied to the client and server state, respectively. These losses capture all losses and inefficiencies in the system: emission inefficiency, coupling to fibre, inefficiencies due to frequency conversion, loss in fiber, and detector inefficiencies. After, we consider the photon(s) arriving at the beamsplitter of the BSM, where beamsplitter transformations are applied to the combined client-server state. Then, projection operators are applied for the measurement, allowing us to find the density matrix of the final remotely prepared state as well as the probability of this measurement outcome. From this, we construct the (dimensionless) rate per attempt time τ (in SC and DC equal to the success probability of an attempt) and the fidelity with respect to the target state $|+_\theta\rangle$, as $F = \langle+_\theta|\rho|+_\theta\rangle$.

B. Double-click protocol

In the DC protocol, the server prepares a Bell state, consisting of the server qubit and the server photon, the latter encoded in, e.g., time bin or polarization, i.e., $|\psi_s\rangle = \sqrt{\frac{1}{2}}(|\emptyset 1, 0\rangle + |1\emptyset, 1\rangle)$, where the two first indices indicate the photon in the different encodings and the last is the internal state of the server qubit.

The client emits a WCP with amplitude $\alpha = |\alpha|$ in equal superposition of the photon encoding, with a relative phase θ, i.e., the client state is

$$|\psi_c\rangle = e^{-|\alpha|^2/2} \sum_{n,m} \frac{(|\alpha|/\sqrt{2})^{n+m}}{\sqrt{n!m!}} e^{in\theta} |nm\rangle. \tag{1}$$

The phase of the WCP is assumed to be randomized over time for security [11].

The loss channels for both the server and client photons are introduced and the photons impinge on a BSM. A successful heralding event occurs when one of the two detectors in the BSM detects at least one photon for both modes of the encoding. The heralded state is given by the expression

$$\rho_{DC} = \frac{\mathrm{tr}_\phi[\Pi_{+1}\Pi_{+2}|\psi_s\rangle|\psi_c\rangle\langle\psi_c|\langle\psi_s|\Pi_{+1}\Pi_{+2}]}{\langle\psi_s|\langle\psi_c|\Pi_{+1}\Pi_{+2}|\psi_s\rangle|\psi_c\rangle}, \tag{2}$$

where tr_ϕ is the trace over all photons and $\Pi_{+i} = (1 - |\emptyset_{+i}\rangle\langle\emptyset_{+i}|)|\emptyset_{-i}\rangle\langle\emptyset_{-i}|$ is the operator corresponding to a detection in the detector associated with the $+$ mode after the beamsplitter transformation of the ith mode of the photon encoding. The density matrix of the server qubit will include the desired state $|+_\theta\rangle = (|0\rangle + e^{i\theta}|1\rangle)/\sqrt{2}$, where θ is determined by the relative phase between the different basis states of the WCP. However, due to the loss channels, the coherences between the two qubit states are reduced leading to some finite infidelity. We calculate the fidelity of the target state and the RSP rate times the time per attempt τ

$$\begin{aligned} F_{DC} &= \frac{1}{2}\Bigg[1 + \frac{\eta_s\eta_c|\alpha|^2/8}{(1-e^{-\eta_c|\alpha|^2/4})} \\ &\quad \times \frac{1}{\left[\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{4}\right) + (1-e^{-\eta_c|\alpha|^2/4})(1-\eta_s)\right]}\Bigg] \\ &\sim 1 - \frac{\eta_c}{\eta_s}\frac{4-3\eta_s}{16}|\alpha|^2, \end{aligned} \tag{3}$$

$$\begin{aligned} P_{DC} &= R_{DC}\tau \\ &= 4e^{-\eta_c|\alpha|^2/2}(1-e^{-\eta_c|\alpha|^2/4}) \\ &\quad \times \left[\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{4}\right) + (1-e^{-\eta_c|\alpha|^2/4})(1-\eta_s)\right] \\ &\sim \frac{\eta_c\eta_s}{2}|\alpha|^2, \end{aligned} \tag{4}$$

where we take the approximation $|\alpha|^2 \ll 1$ in the last line. From this, we can see that the fidelity approaches one as the mean photon number approaches zero, which we also see in Fig. 2. The mean photon number approaching zero, however, also means that the probability of success approaches zero, as no photons get sent to the BSM from the client. As we increase the mean photon number, the probability of a successful event increases, but with that, the fidelity drops due to the increased probability of multiphoton events. This is true for all three protocols in the absence of phase noise.

C. Single-click protocol

In the SC protocol, the client emits a coherent state with complex amplitude $\alpha = |\alpha|e^{-i\theta}$. The server is initially in a superposition state $\sqrt{1-\xi^2}|0\rangle + \xi|1\rangle$, where we refer to ξ as the bright state parameter. The server emits a single photon if its memory qubit is in the bright state, denoted by $|1\rangle$, and no photon otherwise, denoted by $|\emptyset\rangle$. With that, the input states are described by

$$|\psi_c\rangle = |\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{5}$$

$$|\psi_s\rangle = \sqrt{1-\xi^2}|\emptyset 0\rangle + \xi|11\rangle. \tag{6}$$

We introduce loss channels similar to the double-click protocol. A successful heralding event corresponds to a detection

in one of the detectors of the BSM, i.e., we get the heralded state

$$\rho_{\mathrm{SC}} = \frac{\mathrm{tr}_\phi[\Pi_+|\psi_s\rangle|\psi_c\rangle\langle\psi_c|\langle\psi_s|\Pi_+]}{\langle\psi_s|\langle\psi_c|\Pi_+\Pi_+|\psi_s\rangle|\psi_c\rangle}. \tag{7}$$

To lowest order in $|\alpha|$, the state remotely prepared at the server depends on two factors: (1) The balance of probabilities for a photon arriving from each side, where equal probabilities create a state on the equator of the Bloch sphere [31]. These probabilities are determined by the losses on the server side η_s, the losses on the client side η_c, the mean photon number of the WCP, $|\alpha|^2$, and the bright state parameter ξ of the emitter at the server. (2) The phase θ of the WCP, since the state coming from the server has a constant phase (assumed to be zero for simplicity), this introduces a phase difference of θ between the states produced when a photon originating from the server side (heralding the server in the bright state) and the client side (heralding the server in the dark state) arrives at the BSM.

To remotely prepare our target state $|+_\theta\rangle$, we need to have equal probability of the photon arriving at the BSM from the client, as from the server. Note that, unlike for DC, we can only prepare states on a fixed latitude of the Bloch sphere (here, the equator); changing latitude requires either the server to change its bright state parameter, or the client to change the laser intensity. While this could in principle be done, we omit this possibility for simplicity.

We compute the fidelity of the target state with the single-click density matrix

$$F_{\mathrm{SC}} = \frac{1}{2} + \frac{\sqrt{\eta_c\eta_s(1-\xi^2)}|\alpha|\xi/2}{(1-e^{-\frac{\eta_c|\alpha|^2}{2}})(1-\eta_s\xi^2)+\xi^2\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)}. \tag{8}$$

To obtain the best possible result, we optimize the fidelity over ξ for values between 0 and 1, and employ this bright state parameter to calculate the fidelity and the RSP success probability

$$\begin{aligned} F_{\mathrm{SC}} &= \frac{1}{2}\left[1+\sqrt{\frac{\eta_c\eta_s|\alpha|^2/2}{(1-e^{-\eta_c|\alpha|^2/2})}}\right. \\ &\quad \left.\times\sqrt{\frac{1}{2(1-\eta_s)(1-e^{-\eta_c|\alpha|^2/2})+\eta_s(1+\eta_c|\alpha|^2/2)}}\right] \\ &\sim 1-\frac{\eta_c(4-3\eta_s)}{16\eta_s}|\alpha|^2, \end{aligned} \tag{9}$$

$$\begin{aligned} P_{\mathrm{SC}} &= R_{\mathrm{SC}}\tau = 2e^{-\frac{\eta_c|\alpha|^2}{2}}(1-e^{-\frac{\eta_c|\alpha|^2}{2}}) \\ &\quad\times\left[1+\frac{\eta_s\left(2e^{-\frac{\eta_c|\alpha|^2}{2}}-1+\frac{\eta_c|\alpha|^2}{2}\right)}{\eta_s\left(2e^{-\frac{\eta_c|\alpha|^2}{2}}-1+\eta_c|\alpha|^2\right)+4\left(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\right)}\right] \\ &\sim 2\eta_c|\alpha|^2. \end{aligned} \tag{10}$$

In the approximation on the last line, we assume $|\alpha|^2 \ll 1$.

In Fig. 2, in red we see the rate-fidelity trade-off for the SC protocol. Just like for DC, we see that the fidelity approaches one as the rate approaches zero, which happens for the mean photon number $|\alpha|^2 \to 0$. Furthermore, the linear coefficient in the fidelity is the same for the two protocols. Hence, the different scaling in the rate leads to a more favorable rate-fidelity trade-off for SC, characterized by a less-steep slope in Fig. 2(a). Quantitatively, the SC advantage is dependent on the server efficiency: $(1-F)/(R\tau) = (4-3\eta_s)/32\eta_s$ for SC versus $(1-F)/(R\tau) = (4-3\eta_s)/8\eta_s^2$ for DC. The DC slope is thus larger by a factor of $4/\eta_s$.

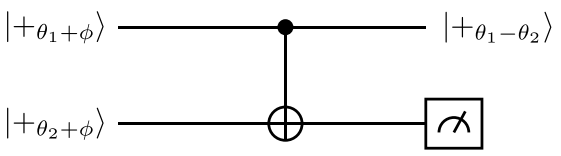


FIG. 3. Local operations in the DSC protocol: Some random phase ϕ that gets added through phase wandering gets canceled out after applying a CNOT gate and measuring the target qubit, as long as the random phase is the same for the two qubits.

D. Double-single-click protocol

The DSC protocol involves performing the SC protocol twice, thus remotely preparing two qubits as given in Eq. (7). We assume that the first qubit is not affected by decoherence or other errors while waiting for the second qubit to be prepared. Hence, the fidelity given below represents an upper bound to the achievable fidelity. After successfully preparing two qubits, the resulting qubits are in a state where either zero ($|00\rangle$), one ($|01\rangle$ or $|10\rangle$), or two ($|11\rangle$) photons have been emitted by the server emitter. A purification step is now introduced, corresponding to the operation

$$\rho_{\mathrm{DSC}} = \frac{\langle 1_2|U_{\mathrm{CNOT}}\rho_{\mathrm{SC}}\otimes\rho_{\mathrm{SC}}U_{\mathrm{CNOT}}^\dagger|1_2\rangle}{\mathrm{tr}[\langle 1_2|U_{\mathrm{CNOT}}\rho_{\mathrm{SC}}\otimes\rho_{\mathrm{SC}}U_{\mathrm{CNOT}}^\dagger|1_2\rangle]}, \tag{11}$$

where U_{CNOT} is the unitary evolution of a CNOT gate and $|1_2\rangle$ indicates the target qubit in state $|1\rangle$. Here, we have required two-qubit gates to be possible between the server qubits. This postselection excludes states where an even number of photons have been emitted from the server, similar to the DC protocol. Then, the phase of the final qubit corresponds to the difference of the first two qubits, as depicted in Fig. 3. We are thus able to mitigate the need for phase stabilization if the phase stays constant between the two heralding events, this is discussed in Sec. II E. This reduced phase stability need is also sufficient for quantum multiplexed extensions of our single-click RSP protocols, as explored in Ref. [32].

We calculate the fidelity of the purified qubit with the target state $|+_\theta\rangle$

$$\begin{aligned} F_{\mathrm{DSC}} &= \frac{1}{2}\left[1+\frac{\eta_s\eta_c|\alpha|^2/4}{\left(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\right)}\right. \\ &\quad\left.\times\frac{1}{\left[\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)+(1-\eta_s)\left(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\right)\right]}\right] \\ &\sim 1-\frac{\eta_c}{\eta_s}\frac{4-3\eta_s}{8}|\alpha|^2. \end{aligned} \tag{12}$$

We note that the fidelity is independent of the bright state parameter, which stems from the purification, which ensures the two memory qubits are in different states.

To find the optimal bright state parameter, we instead consider the dimensionless rate. Assuming, we can attempt preparation of the two qubits in parallel, the rate is given by

$$R_{\mathrm{DSC}}\tau = \frac{2 - P_{\mathrm{SC}}}{3 - P_{\mathrm{SC}}} P_{\mathrm{SC}} P_{\mathrm{CNOT}}, \tag{13}$$

where P_{SC} is twice the numerator of Eq. (7) and P_{CNOT} is the numerator of Eq. (11). If it is not possible to attempt the success in parallel, the fraction reduces to $1/2$. We optimize the rate over ξ for values between 0 and 1, and find the optimal bright state parameter, this will be the root of a fourth-degree polynomial, however, to lowest order in the mean photon number of the pulse, $\xi^2_{\mathrm{DSC}} \propto |\alpha|$, i.e., the square root of the mean photon number. The purification step ensures that at least one photon originates from the client, thus it is no longer necessary to match the number photon flux from each side of the BSM. However, the bright state parameter should still not be $1/\sqrt{2}$, as both qubits in the bright state might block an otherwise successful attempt.

When employing the optimal bright state parameter and expanding the dimensional rate in the mean photon number of the WCP, it becomes

$$R_{\mathrm{DSC}}\tau \sim \tfrac{4}{3}\eta_c |\alpha|^2. \tag{14}$$

In Fig. 2, we plot the rate and fidelity for the DSC protocol and find that it lies between those for DC and SC. In Appendix A 3, we discuss the calculations behind the rate more thoroughly.

E. Phase noise

Small fluctuations in the system cause the true phase of the WCP to drift over time. In the DC protocol, the target phase θ is encoded as the relative phase between two copropagating orthogonal modes of the client photon (e.g., two time bins or two polarizations). A drift in the overall optical phase of the WCP is common to both modes and thus acts only as a global phase, not affecting θ. In contrast, phase shifts present a challenge for the SC protocol, as here θ is determined by the phase difference between the separate client and server paths. This necessitates active phase stabilization, as demonstrated in, e.g., Ref. [33]. The DSC protocol aims to eliminate this technical overhead by "deleting" the overall phase of two successful SC operations, leaving only the phase *difference* between the two clicks as noise. We note that with that DSC does not combat phase noise, instead it combats the technical requirement of phase stabilization. The CNOT and its effect on the qubits is depicted in Fig. 3. This approach is effective only if the phase drift between the two successes is small, which requires sufficiently fast remote preparation. We note that, while DC encoding is insensitive to a common phase drift, it is not always insensitive to a differential phase between its two modes. In polarization encoding, for example, fibre birefringence is generally time varying and rotates the polarization state, so active polarization tracking is needed. This polarization compensation is however generally more mature and separate from the phase stabilization needed by the SC approach.

Despite phase stabilization in SC and the CNOT operation in DSC, some residual phase noise will likely appear in both protocols. In SC, where active phase stabilization is assumed, residual noise may arise from imperfections in the phase stabilization process. In DSC, where we do not actively stabilize the phase, but instead rely on the phase drift between the first click and the second click canceling each other out, the phase noise stems from drift between the first and second clicks. How large this drift is depends on the time interval between the two clicks (T) and the linewidth of the optical field and drift of optical elements ($\Delta\nu$), i.e., the rate at which the phase evolves. The two phases in the DSC protocol are correlated, as they are the phase of a single drifting optical field, sampled at two emission times. We model phase noise in SC and DSC as affecting the final state in similar ways, but to differing extents. To account for this, we introduce two variables to represent the standard deviation of phase noise: σ_{SC} for SC and σ_{DSC} for DSC.

The value of σ_{SC} can be determined through experimental characterization of the setup, while σ_{DSC} can be estimated using $\sqrt{2\pi\Delta\nu T}$ [34], if limited by optical linewidth. Since the gap between two clicks T is itself a random waiting time, a fully predictive value would average over the waiting-time distribution or be obtained from a measured phase noise correlation function. We instead treat σ_{DSC} as a swept parameter to remain agnostic to specific experimental settings.

We assume phase noise follows a Gaussian distribution with standard deviation σ. This results in a phase noise factor of $X_{\mathrm{noise}} = e^{-\sigma^2/2}$, which modifies the fidelity equations for SC and DSC. Without noise, these fidelities, given in Eqs. (9) and (12), take the form $F = (1 + x)/2$; with noise, they become $F_{\mathrm{noise}} = (1 + xX_{\mathrm{noise}})/2$. Additional details are provided in Appendix A 5.

In Fig. 2, we see the effect of the phase noise term on the SC and DSC results. While the rate of the protocols is not affected by the phase noise, it lowers the maximal achievable fidelity, effectively pushing the rate-fidelity line downward. Here, we have chosen to plot $\sigma_{\mathrm{SC}} = \sigma_{\mathrm{DSC}}$ for comparison. These two parameters will likely not be the same in a real-life system, as the noise has a different origin for each protocol.

III. COMPARISON AND DISCUSSION

From the formulas for the fidelity without phase noise, Eqs. (3), (9), and (12), we note that the first-order contributions in $|\alpha|^2$ are $1 - \eta_c(4 - 3\eta_s)|\alpha|^2/16\eta_s$ for SC and DC and $1 - \eta_c(4 - 3\eta_s)|\alpha|^2/8\eta_s$ for DSC. This infidelity can be intuitively understood as a client photon reaching the detector in the same mode as the server photon. Either the server photon is lost, contributing with $1 - \eta_s$, or the server photon reaches the detector and bunches with the client photon, contributing with $\eta_s/4$. In the DSC protocol, there are two chances to introduce this error, leading to an extra factor of 2. For the small values of $|\alpha|^2$ considered in this paper, the fidelity will thus be very similar across the three protocols. However, the performance of the protocols depends heavily on the rate and the phase noise.

Thus, to compare the performance of the three protocols, we look at their fidelity and rate in different scenarios. We do this by varying the intensity of the client laser α, the amount of phase noise in the SC and DSC protocols σ_{SC} and σ_{DSC}, and the efficiency of the server η_s. We consider a scenario where the client and server are separated by 25 km of optical fibre,

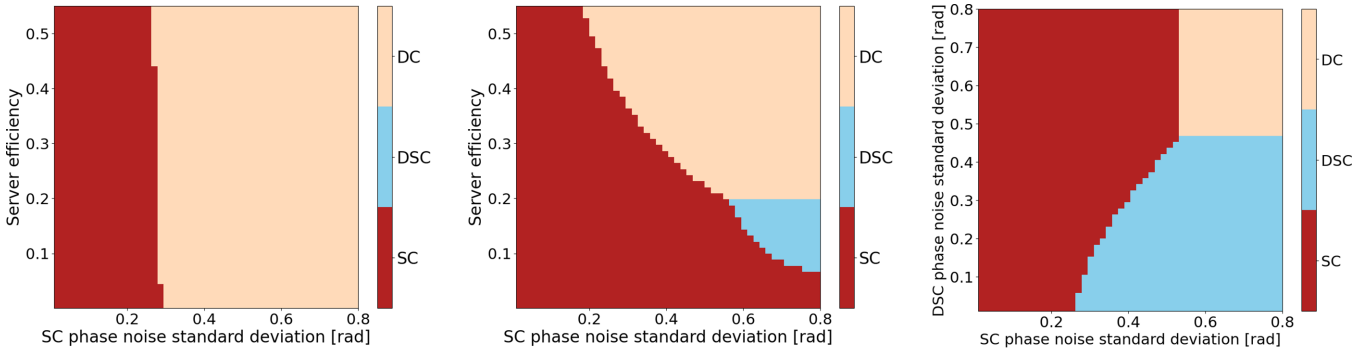


FIG. 4. Optimal RSP protocol—DC, DSC, or SC—as a function of phase noise (σ_{SC}, σ_{DSC}, in radians) and server efficiency η_s (which includes detector efficiency). For each parameter combination, we find the smallest $|\alpha|^2$ at which the stated target is achievable and select the best-performing protocol: DC (peach), DSC (blue), or SC (red). Each panel fixes one parameter and optimizes a different figure of merit, as detailed in the subcaptions. (a) Protocol that gives the highest dimensionless rate $R\tau$ given a target fidelity of 0.98 for $\sigma_{\mathrm{DSC}} = 0.5$ rad. (b) Protocol that gives the highest fidelity given a target of $R\tau = 0.01$ for rad. (c) Protocol that gives the highest fidelity given a target of $R\tau = 0.01$ for $\eta_s = 0.21$.

resulting in a client efficiency of $\eta_c = 0.22$, which includes a detector efficiency of 0.7. The same performance for RSP can be achieved for other distances by adjusting α, hence, η_c is not considered as a parameter to vary. However, when α is increased, a potential eavesdropper will receive a stronger signal. A larger overhead is thus required to maintain the same security for the full (QKD or BQC) protocol.

We see that increasing α enhances the rate but reduces the fidelity, leading to a trade-off explored for the three different protocols in Fig. 2. The plotting code for this, and other figures can be found in Ref. [35]. For this figure, we set the efficiency of the server to $\eta_s = 0.091$ based on an emission probability of 0.53 [36] and a successful telecom frequency conversion probability of 0.25 [37], representing the state of the art. We look at both with and without phase noise for both SC and DSC in Fig. 2. With this, we vary the laser intensity of the client between $|\alpha|^2 = 0.001$ and $|\alpha|^2 = 0.5$.

From Fig. 2, we see that when phase noise is not included the SC protocol can achieve the highest rates, followed by DSC, with DC having the lowest rate for any α. This was expected and is analogous to advantages known for SC in entanglement generation. However, unlike in entanglement generation or when using only single photons, the SC and DSC protocols provide similar fidelity for a given $|\alpha|^2$ to DC, which gives them a strict advantage over DC in the absence of phase noise.

However, we also note that when including phase noise, the DC protocol can obtain a higher fidelity in the low rate regime. This is due to phase noise lowering the maximally achievable fidelity for SC and DSC. Without phase noise, the fidelity approaches unity as $|\alpha|^2$ for all protocols. To achieve a reasonable rate, the laser power must, however, be increased. This higher $|\alpha|^2$ causes an increase in the infidelity of the three protocols, with the greatest impact on the DC protocol, as there $|\alpha|^2$ needs to be increased the most for the same increase in rate. For SC, the required increase in $|\alpha|^2$, and thereby the increase in infidelity, is the lowest. Thus, for a specific rate, the SC protocol can yield a higher fidelity than the DC protocol.

To determine which protocol is most advantageous under various conditions, we evaluate scenarios across different server efficiencies and levels of phase noise for specific target fidelities or rates. Figure 4 illustrates these findings, with blocks color coded to indicate the most advantageous protocol.

Figure 4(a) shows the regions where each scheme provides the highest rate for a target fidelity of 0.98. Here, we have fixed the phase noise of the DSC protocol to be $\sigma_{\mathrm{DSC}} = 0.5$, but we vary η_s and σ_{SC}. SC outperforms DC in low-σ_{SC} regimes, with occasional jumps based on server efficiency. This is because, in high-σ_{SC} regions, SC and DSC fail to achieve the target fidelity, leaving DC as the only viable option. Near the boundary between the SC and DC regions, SC approaches its maximum fidelity and achieves the target at a lower rate than DC. Here, higher server efficiencies favor DC more significantly than SC, further shrinking SC's advantageous region. However, unless the target fidelity is close to the SC maximum, SC generally provides higher rates than DC.

The size of SC's region of advantage decreases with higher target fidelity and increases with lower target fidelity, as the target fidelity determines where SC becomes infeasible. DSC does not exhibit a clear advantage in any region, but appears on the border between the SC and DC regions when $\sigma_{\mathrm{DSC}} \leqslant 0.3$ rad. However, as we will also discuss later, DSC provides an advantage over SC in terms of technical demand in the form of phase stabilization.

In Fig. 4(b), we identify the scheme achieving the highest fidelity for a target rate of 0.01, again setting $\sigma_{\mathrm{DSC}} = 0.5$. DC outperforms SC and DSC only in scenarios with high σ_{SC} and efficient servers. As the target rate decreases, the size of DC's advantage region increases, while it decreases for higher target rates. DSC gains some advantage over DC and SC when the server efficiency is low, but σ_{SC} is high. Naturally, this region gets smaller when σ_{DSC} is higher and larger when σ_{DSC} is lower.

To find the effect that different ratios of σ_{SC} to σ_{DSC} have on the advantage regions, we fix η_s to 0.3 and again find which protocol provides the highest fidelity given a target rate of 0.01. These regions are shown in Fig. 4(c). Here, we clearly see the divide between SC and DSC being advantageous depending on the noise levels occurring in each protocol. The high-noise regime in which DC provides an advantage shrink

when the server efficiency is lower, and grows when it is higher. Additionally, increasing the server efficiency pushes down, toward lower σ_{DSC}, the border line between SC and DSC, and decreasing it will push the lineup.

Alternatives to the selected values for these plots are given in Appendix B, which can be used to visualize the explained effects of parameter changes of the form when parameter x increases/decreases, y happens.

Overall, DC is advantageous under high phase noise, high server efficiency, or high fidelity targets. SC performs better with less efficient servers, lower phase noise, or when high rates are desired. DSC can gain an advantage if σ_{DSC} is small compared to σ_{SC}. Notably, protocols requiring multiple remotely prepared qubits (e.g., in BQC) may benefit more from higher-rate, lower-fidelity RSPs due to the impact of decoherence.

A drawback of the SC protocol is the need for phase stabilization, which can be technologically challenging to implement. The DSC protocol might alleviate this need, when two consecutive successes of the SC protocol are close enough in time so that the phase has not shifted significantly, otherwise σ_{DSC} will grow too large. Therefore, one needs to be able to either reexcite the memory qubit very fast, or have enough multiplexing capabilities. Notably, even if DSC does not give advantageous performance over SC, eliminating the need for phase stabilization might still make it favorable, as long as σ_{DSC} is low enough to provide an advantage over DC. DC always has the advantage of not needing phase stabilization and also having a negligible amount of phase noise, though the increased rate of SC and DSC over DC can lead to an overall higher fidelity for multiqubit states when in the presence of decoherence.

Some noise sources have been left out of this analysis. Detector dark counts and interference visibility of the photons from the server and the client will lead to a smaller coherence term and will affect the SC and DC protocols equally. However, as the errors compound for each prepared qubit, these errors have a greater impact on the DSC protocol. For a single RSP in SC and DC, decoherence will be minimal, because the BSM is assumed to be directly next to the server, and thus the RSP will be heralded almost instantaneously. However, in the DSC protocol, decoherence will affect the fidelity of the final remotely prepared state if the time between the two SC successes is long. This effect is not taken into account here, as it would take many assumptions on the setup (e.g., server repetition rate, multiplexing capabilities, cutoff time for the memory) in order to quantify this, making it a less generally applicable comparison. Therefore, the fidelity given here for the DSC protocol can be taken as an upper bound for the achievable fidelity with decoherence. To a certain extent, the amount of infidelity decoherence adds to the final remotely prepared state can be adjusted while sacrificing on rate by setting a window, sometimes referred to as a cutoff time, for the two clicks [38]. Similarly, gate errors will only affect the DSC protocol, as this is the only protocol, which includes a gate.

IV. APPLICATIONS

RSP finds impactful applications across multiple domains within a quantum network, for example in BQC protocols. In addition, RSP can be used to perform QKD over a repeater chain (see Fig. 5). We lay out how the schemes introduced here can be used to create perfectly correlated bits by showing correctness in a purified model and finding equivalence with existing QKD proofs.

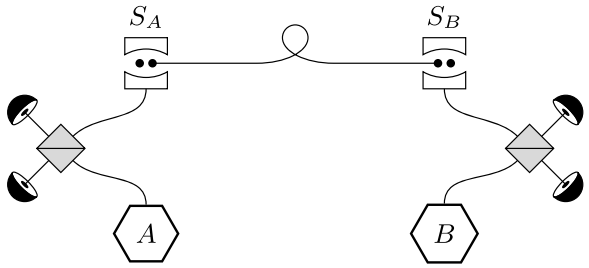


FIG. 5. Schematic drawing of the repeater QKD protocol between two clients A and B. The untrusted third party has prepared a long-distance entangled pair between nodes S_A and S_B. Client A (B) remotely prepares a new qubit of the form $|+_\theta\rangle$ on node S_A (S_B). Once remote state preparation succeeds for client A (B), a local Bell state measurement is performed between the two qubits at node S_A (S_B).

RSP for long-distance communication. RSP enables long-distance communication over a repeater chain [39]. For a schematic drawing, see Fig. 5, where we have two clients wanting to establish a key with each other and a repeater chain between them. Here, we give the intuition behind how our setup works, and defer showing the correctness of the purified protocol to Appendix C. The clients A and B remotely prepare a qubit of the form $|+_\theta\rangle$ on the first nodes of the repeater chain: S_A and S_B. Once A and B have both succeeded in remotely preparing their qubits, shared entanglement between S_A and S_B can be used to swap the states to the same node, where a BSM can be performed between the two remotely prepared qubits. A and B use the reported measurement patterns as part of the protocol to align their bit values (with B flipping his bit when necessary), the security of the protocol does not rely on trusting these measurements. Instead, security is guaranteed through subsequent parameter estimation and privacy amplification steps between A and B.

In measurement-device-independent (MDI) QKD, the security of the protocol is independent of how the BSM is performed. Therefore, a protocol that uses RSP and teleportation across a repeater chain can be equivalent to an MDI QKD protocol that uses a simple BSM. As we show in Appendix C, the purified protocols are correct, and the repeater chain acts as an effective BSM.

RSP for BQC. BQC using double-click RSP with a WCP-based client has been proven secure [11] (which improves on [23] by eliminating the need for photon counting, adding verifiability, and providing scaling in terms of number of samples with respect to the transmittance of the channel). A BQC security proof for SC and DSC is still an open question. A difficulty that arises here is that a common technique used in security proofs both in QKD and BQC with WCP sources is to phase randomize the WCP, effectively getting rid of the coherences within the WCP. This assumption cannot be made in the SC security proof, as we rely on the phase of the WCP to define the phase of the remotely prepared state. In DSC,

however, the phase of the remotely prepared state depends on the phase difference between the first and the second click, such that the pulses can be phase randomized, as long as the randomization is equal for both pulses. This may allow extending standard security proofs to DSC, but a complete investigation of this is beyond the scope of this work.

V. CONCLUSION

We have introduced two powerful protocols for remote state preparation using weak coherent pulses:SC and DSC. In SC, the phase transferred onto the remotely prepared state is encoded in the weak coherent pulse of the client, while the photon-emission probability of the server is adjusted to balance photon arrival probabilities at the Bell state measurement station. DSC repeats this process twice and applies a CNOT gate to the resulting qubits, effectively canceling out random phase fluctuations between the pulses and eliminating the need for phase stabilization when the clicks occur faster than the phase fluctuations.

Our key findings are as follows:

(1) The SC protocol consistently achieves higher rates than DC while maintaining comparable fidelity levels. This is in contrast to entanglement generation, where obtaining a higher rate due to switching from DC to SC comes at a cost of lowered fidelity. This represents a significant advantage for practical implementations where high preparation rates are crucial.

(2) For systems with low server efficiency, high target rates, or modest fidelity requirements, SC offers clear advantages over DC. This is especially relevant for quantum computing applications requiring multiple remote state preparations.

(3) The DSC protocol provides a practical middle ground—while delivering more modest rate improvements over DC, it can eliminate the need for phase stabilization when the system can perform attempts fast enough that the phase remains stable between consecutive successes.

The choice between these protocols depends on specific experimental constraints:

(1) Use SC when maximum rate is paramount and phase stabilization is feasible.

(2) Consider DSC when phase stabilization is challenging but system speeds allow for sufficiently low phase noise between consecutive clicks.

(3) Stick with DC for applications requiring maximum fidelity for a single qubit or when providing a low phase noise environment for SC and DSC is not feasible.

We have demonstrated how these protocols can be applied to quantum key distribution over repeater chains using existing measurement-device-independent protocols. The path forward for blind quantum computing applications appears promising, particularly given recent security proofs for DC-based protocols.

ACKNOWLEDGMENTS

The SC and DSC protocols introduced in this paper have been submitted as patent applications [40,41]. The authors would like to thank Arian Stolk, Harold Ollivier, and Maxime Garnier for useful discussions, and Bethany Davies for useful comments on the manuscript. This project has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No. 101102140. E.R.H. and A.S.S. acknowledge the support of Danmarks Grundforskningsfond (DNRF Grant No. 139, Hy-Q Center for Hybrid Quantum Networks).

DATA AVAILABILITY

There are no publicly available research data or software supporting this manuscript. Requests for further information or data should be sent to the authors.

APPENDIX A: DERIVATION OF RATE AND FIDELITY FORMULAS

Here, we will go through the calculations for finding the success probability and fidelity of a single remotely prepared qubit state using non-photon-number-resolving detectors. In these calculations, the target state is given by $|+_\theta\rangle$, for some angle θ.

We consider losses, which can be due to server inefficiencies, detector inefficiencies, fiber losses, losses due to frequency conversion, or any other. We assume no other imperfections aside from the WCP source not being a perfect single-photon source and the phase noise discussed in Appendix A 5; i.e., we assume perfect gates, the server emits with perfect fidelity, and no decoherence.

1. Double click

For double click, the client sends out a WCP with displacement α, lets it fall onto a beamsplitter and includes a phase shift for one of the arms. This can be a polarizing beamsplitter in the case of polarization encoding, or a regular beamsplitter with delay line in the case of time-bin encoding. The server will emit a photon entangled with the state of the qubit. We set $\xi = 1/\sqrt{2}$ to maximize the fidelity; this means the server and photon qubits form a Bell state. The input states are thus given by

$$|\psi_c\rangle = e^{-|\alpha|^2/2} \sum_{n,m} \frac{(|\alpha|/\sqrt{2})^{n+m}}{\sqrt{n!m!}} e^{in\theta} |nm\rangle, \quad |\psi_s\rangle = \sqrt{\frac{1}{2}}(|\emptyset 1, 0\rangle + |1\emptyset, 1\rangle), \tag{A1}$$

We now introduce losses for both the server and client photons. Furthermore, we subject the light in both the early and late time bins (assuming time-bin encoding) to a BSM. The operation will succeed if a photon is detected in both time bins. Hence, a

successful measurement transforms the density matrix to

$$\rho_{\mathrm{DC}} = \frac{\mathrm{tr}_\phi[\Pi_{+1}\Pi_{+2}|\psi_s\rangle|\psi_c\rangle\langle\psi_c|\langle\psi_s|\Pi_{+1}\Pi_{+2}]}{\langle\psi_s|\langle\psi_c|\Pi_{+1}\Pi_{+2}|\psi_s\rangle|\psi_c\rangle}. \tag{A2}$$

The density matrix and fidelity of the remotely prepared qubit and success probability of the protocol are

$$\rho_{\mathrm{DC}} = \frac{1}{2}\left\{\mathbb{I} + \frac{(e^{-i\theta}|0\rangle\langle 1| + \mathrm{H.c.})\eta_s\eta_c|\alpha|^2/8}{(1-e^{-\eta_c|\alpha|^2/4})\left[\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{4}\right)+\left(1-e^{-\eta_c|\alpha|^2/4}\right)(1-\eta_s)\right]}\right\}, \tag{A3}$$

$$F_{\mathrm{DC}} = \frac{1}{2}\left\{1 + \frac{\eta_s\eta_c|\alpha|^2/8}{\left(1-e^{-\eta_c|\alpha|^2/4}\right)\left[\frac{\eta_s}{2}(1+\frac{\eta_c|\alpha|^2}{4})+(1-e^{-\eta_c|\alpha|^2/4})(1-\eta_s)\right]}\right\} \sim 1 - \frac{\eta_c}{\eta_s}\frac{4-3\eta_s}{16}|\alpha|^2, \tag{A4}$$

$$P_{\mathrm{DC}} = 4e^{-\eta_c|\alpha|^2/2}(1-e^{-\eta_c|\alpha|^2/4})\left[\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{4}\right)+(1-e^{-\eta_c|\alpha|^2/4})(1-\eta_s)\right] \sim \frac{\eta_c\eta_s}{2}|\alpha|^2. \tag{A5}$$

2. Single click

The client sends out a coherent state with displacement $\alpha = |\alpha|e^{-i\theta}$. The server sends out a single photon when its memory qubit is in the bright state, denoted by $|1\rangle$ (and no photon otherwise). The probability of the server being in the bright state is dependent on the bright state parameter ξ. Thus, we start with the following states:

$$|\psi_c\rangle = |\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle, \quad |\psi_s\rangle = \sqrt{1-\xi^2}|\emptyset 0\rangle + \xi|11\rangle. \tag{A6}$$

We now introduce losses $1-\eta_c$ and $1-\eta_s$ on the client and server states. The BSM measurement transforms the client and server photons into plus and minus modes with the annihilation operators $a_\pm = (a_s \pm a_c)/\sqrt{2}$, where a_c (a_s) is the annihilation operator of the client (server) photon. A photon detector is placed in both paths, and will be referred to as plus and minus detectors, respectively. We will assume that a signal comes from the plus detector while the minus detector stays silent, corresponding to the transformation

$$\rho_{\mathrm{SC}} = \frac{\mathrm{tr}_\phi[\Pi_+|\psi_s\rangle|\psi_c\rangle\langle\psi_c|\langle\psi_s|\Pi_+]}{\langle\psi_s|\langle\psi_c|\Pi_+\Pi_+|\psi_s\rangle|\psi_c\rangle}, \tag{A7}$$

where tr_ϕ is the trace over the photon subspace, $|\emptyset_-\rangle$ is the state of no photons in the minus detector, and the denominator is the probability of obtaining a click in the plus detector, $P_{\mathrm{SC}|+}$. The combined success probability is twice this number, leading to

$$P_{\mathrm{SC}} = 2e^{-\eta_c|\alpha|^2/2}\left[(1-e^{-\eta_c|\alpha|^2/2})(1-\eta_s\xi^2) + \xi^2\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)\right]. \tag{A8}$$

The density matrix after the heralding click is then

$$\begin{aligned}\rho_{\mathrm{SC}} = {} & \frac{(1-e^{-\eta_c|\alpha|^2/2})(1-\xi^2)|0\rangle\langle 0| + \frac{\sqrt{\eta_c\eta_s(1-\xi^2)}}{2}|\alpha|\xi(e^{i\theta}|1\rangle\langle 0| + \mathrm{H.c.})}{(1-e^{-\eta_c|\alpha|^2/2})(1-\eta_s\xi^2)+\xi^2\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)} \\ & + \frac{\xi^2[\frac{\eta_s}{2}(1+\frac{\eta_c|\alpha|^2}{2})+(1-\eta_s)(1-e^{-\eta_c|\alpha|^2/2})]|1\rangle\langle 1|}{(1-e^{-\eta_c|\alpha|^2/2})(1-\eta_s\xi^2)+\xi^2\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)}.\end{aligned} \tag{A9}$$

We can now find the fidelity with respect to our target state $|+_\theta\rangle$ as $F = \langle+_\theta|\rho_{\mathrm{SC}}|+_\theta\rangle$ and find

$$F = \frac{1}{2}\left[1 + \frac{\sqrt{\eta_c\eta_s(1-\xi^2)}|\alpha|\xi}{(1-e^{-\eta_c|\alpha|^2/2})(1-\eta_s\xi^2)+\xi^2\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)}\right]. \tag{A10}$$

This fidelity can be maximized with respect to the bright state parameter ξ, leading to

$$\xi_{\mathrm{SC}}^2 = \frac{2(1-e^{-\eta_c|\alpha|^2/2})}{4(1-e^{-\eta_c|\alpha|^2/2})+\eta_s(2e^{-\eta_c|\alpha|^2/2}+\eta_c|\alpha|^2/2-1)} \sim \frac{\eta_c}{\eta_s}|\alpha|^2. \tag{A11}$$

Here, the last expression is the expansion up to first order in the mean photon number from the client, as we will want to be in a regime where the client sends out a weak pulse. We continue the calculations with the exact expression, not the first-order expansion. The fidelity becomes

$$F_{\mathrm{SC}} = \frac{1}{2}\left\{1 + \sqrt{\frac{\eta_c\eta_s|\alpha|^2/2}{(1-e^{-\eta_c|\alpha|^2/2})[2(1-\eta_s)(1-e^{-\eta_c|\alpha|^2/2})+\eta_s(1+\eta_c|\alpha|^2/2)]}}\right\} \sim 1 - \frac{\eta_c(4-3\eta_s)}{16\eta_s}|\alpha|^2. \tag{A12}$$

We similarly substitute the expression for the optimized bright state parameter in the success probability to find

$$P_{\mathrm{SC}} = 2e^{-\eta_c|\alpha|^2/2}(1-e^{-\eta_c|\alpha|^2/2})\left[1+\frac{\eta_s(2e^{-\eta_c|\alpha|^2/2}-1+\eta_c|\alpha|^2/2)}{\eta_s(2e^{-\eta_c|\alpha|^2/2}-1+\eta_c|\alpha|^2)+4(1-e^{-\eta_c|\alpha|^2/2})}\right] \sim 2\eta_c|\alpha|^2. \tag{A13}$$

From this, the rate can be calculated as the success probability multiplied by the time per attempt τ. We use the "dimensionless rate" $R\tau$ in our analysis, as this allows us to compare it to the DSC protocol, where one does not speak of a success probability per attempt (as we need two successes).

3. Double single click

For double single click, the single-click protocol is performed twice. The state after the two successful clicks is $\rho_{\mathrm{sys}} = \rho_{\mathrm{SC}} \otimes \rho_{\mathrm{SC}}$, with ρ_{SC} as in Eq. (A9). Then, a CNOT gate is performed on the two prepared qubits, followed by a measurement on the target qubit. The state is only accepted if this qubit is in the bright state $|1\rangle$. The density matrix is thus given by the expression

$$\rho_{\mathrm{DSC}} = \frac{\langle 1_2|U_{\mathrm{CNOT}}\rho_{\mathrm{SC}}\otimes\rho_{\mathrm{SC}}U_{\mathrm{CNOT}}^\dagger|1_2\rangle}{\mathrm{tr}[\langle 1_2|U_{\mathrm{CNOT}}\rho_{\mathrm{SC}}\otimes\rho_{\mathrm{SC}}U_{\mathrm{CNOT}}^\dagger|1_2\rangle]}, \tag{A14}$$

which will succeed with the conditional probability P_{CNOT}

$$P_{\mathrm{CNOT}} = \frac{2\xi^2(1-\xi^2)(1-e^{-\eta_c|\alpha|^2/2})\left[\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)+(1-\eta_s)(1-e^{-\eta_c|\alpha|^2/2})\right]}{\left[(1-e^{-\eta_c|\alpha|^2/2})(1-\eta_s\xi^2)+\xi^2\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)\right]^2}. \tag{A15}$$

As the CNOT gate and measurement ensure that the two qubits were measured in different states, the fidelity is no longer dependent on the bright state parameter. The density matrix and the fidelity of the remotely prepared state are

$$\rho_{\mathrm{DSC}} = \frac{1}{2}\left\{\mathbb{I}+\frac{(e^{-i\theta}|0\rangle\langle 1|+\mathrm{H.c.})\eta_s\eta_c|\alpha|^2/4}{\left(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\right)\left[\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)+(1-\eta_s)\left(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\right)\right]}\right\}, \tag{A16}$$

$$F_{\mathrm{DSC}} = \frac{1}{2}\left\{1+\frac{\eta_s\eta_c|\alpha|^2/4}{\left(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\right)\left[\frac{\eta_s}{2}\left(1+\frac{\eta_c|\alpha|^2}{2}\right)+(1-\eta_s)\left(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\right)\right]}\right\} \sim 1-\frac{\eta_c}{\eta_s}\frac{4-3\eta_s}{8}|\alpha|^2. \tag{A17}$$

It does not make sense to talk of a success probability of the process, as we will assume that we store the first qubit, while we wait for the second qubit to be generated. We will instead talk in terms of the rate, assuming a fixed time for each attempt. We assume it is possible to prepare the two qubits on the server in parallel. In this case, the dimensionless rate will be

$$R_{\mathrm{DSC}}\tau = \left(\frac{1}{2P_{\mathrm{SC}}-P_{\mathrm{SC}}^2}+\frac{1}{P_{\mathrm{SC}}}\right)^{-1}P_{\mathrm{CNOT}}, \tag{A18}$$

where P_{SC} is the single-click success probability, the first (second) term in the parentheses corresponds to the dimensionless time it takes to prepare the first (second) qubit and P_{CNOT} is the probability that the measurement after the CNOT gate yields the correct outcome. As the optimal bright state parameter is yet to be determined, we cannot assume anything about P_{SC}. However, the optimal bright state parameter is one of the solutions satisfying $0<\xi<1$ to the quartic equation in ξ^2

$$0 = A_0\left(\frac{\eta_c|\alpha|^2}{2}\right)+A_1\left(\frac{\eta_c|\alpha|^2}{2},\eta_s\right)\xi^2+A_2\left(\frac{\eta_c|\alpha|^2}{2},\eta_s\right)\eta_s\xi^4+A_3\left(\frac{\eta_c|\alpha|^2}{2}\right)\eta_s^2\xi^6+A_4\left(\frac{\eta_c|\alpha|^2}{2}\right)\eta_s^3\xi^8, \tag{A19}$$

where the coefficient functions are given by

$$A_0(x) = 8-24e^x+44e^{2x}-48e^{3x}-12e^{5x}, \tag{A20a}$$

$$A_1(x,\eta) = -2(1+\eta)A_0(x)+4\eta e^x(2-4e^x+5e^{2x}-3e^{3x})(2e^x-1-x), \tag{A20b}$$

$$A_2(x,\eta) = 2[2-e^x(1-x)]\left\{10-20e^x+26e^{2x}-8e^{3x}+3e^{4x}+\eta\left[2-e^x(3-x)+e^{2x}(2-x)-\frac{e^{3x}}{2}(1-x)\right]\right\}, \tag{A20c}$$

$$A_3(x) = -2[2-e^x(1-x)]^2(4-4e^x+3e^{2x}), \tag{A20d}$$

$$A_4(x) = [2-e^x(1-x)]^3. \tag{A20e}$$

If multiple solutions exist in the interval for ξ, the value yielding the best rate should be chosen. While we will not give an exact description as it is not instructive, we give expand the solution in powers of the mean photon number of the WCP

$$\xi_{\mathrm{DSC}}^2 \sim \sqrt{\frac{6\eta_c}{\eta_s(6+\eta_s)}}|\alpha| - \frac{3\eta_c(12+2\eta_s+\eta_s^2)}{\eta_s(6+\eta_s)^2}|\alpha|^2. \tag{A21}$$

If the qubit system forces us to prepare the two qubits sequentially, the rate will instead be given by

$$R_{\mathrm{DSC,seq}}\tau = \tfrac{1}{2}P_{\mathrm{SC}}P_{\mathrm{CNOT}}. \tag{A22}$$

In this case, we can find the optimal bright state parameter analytically

$$\xi^2_{\mathrm{DSC,seq}} = \frac{\sqrt{2\big(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\big)\big[2\big(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\big)+2e^{-\frac{\eta_c|\alpha|^2}{2}}\eta_s+\big(\frac{\eta_c|\alpha|^2}{2}-1\big)\eta_s\big]}-2\big(1-e^{-\frac{\eta_c|\alpha|^2}{2}}\big)}{\eta_s\big[2e^{-\frac{\eta_c|\alpha|^2}{2}}+\big(\frac{\eta_c|\alpha|^2}{2}-1\big)\big]} \sim \sqrt{\frac{\eta_c}{\eta_s}}|\alpha|-\frac{\eta_c}{\eta_s}|\alpha|^2. \tag{A23}$$

The difference in the two optimal bright state parameters is a consequence of the added dependence of P_{SC} in the rate. However, note in both cases $\xi^2 = x|\alpha|$ to lowest order in the mean photon number, hence, to the lowest order in the mean photon number $P_{\mathrm{SC}} = ax|\alpha|$ and $P_{\mathrm{CNOT}} = b|\alpha|/x$. Thus, the rate to lowest order in $|\alpha|$ will be of independent the proportionality factor x, and thus on the form $R_{\mathrm{DSC}}\tau \sim c|\alpha|^2$, where c will differ in the two cases. For parallel preparation of the qubits, the dimensionless rate is to lowest order in the mean photon number

$$R_{\mathrm{DSC}}\tau \sim \tfrac{4}{3}\eta_c|\alpha|^2. \tag{A24}$$

For the plots in the main text and in Appendix B, we employ the parallel rate and the full expression for the optimal bright state parameter. The latter is found numerically by optimizing the rate over ξ given efficiencies η_s and η_c and mean photon number of the WCP.

4. Single click with photon number resolving detectors

If we assume photon number resolving detectors, for single click the transformation now reads

$$\rho_{\mathrm{sys}} \to \rho_{\mathrm{SC}} = \frac{\langle 1_+|\rho_{\mathrm{sys}}|1_+\rangle}{\mathrm{tr}[\langle 1_+|\rho_{\mathrm{sys}}|1_+\rangle]}, \tag{A25}$$

which leads to the probability of successfully obtaining a click in the "plus" mode

$$P_{\mathrm{SC}|+} = \frac{e^{-\eta_c|\alpha|^2}}{2}[\eta_c|\alpha|^2(1-\eta_s\xi^2)+\eta_s\xi^2]. \tag{A26}$$

The state after the heralding becomes

$$\rho_{\mathrm{SC}} = \frac{(1-\xi^2)\eta_c|\alpha|^2+\eta_s\xi^2}{\eta_c|\alpha|^2(1-\eta_s\xi^2)+\eta_s\xi^2}|\xi\rangle\langle\xi| + \frac{\eta_c|\alpha|^2\xi^2(1-\eta_s)}{\eta_c|\alpha|^2(1-\eta_s\xi^2)+\eta_s\xi^2}|1\rangle\langle 1|, \tag{A27}$$

where $|\xi\rangle = [\sqrt{\eta_c(1-\xi^2)}|\alpha|e^{i\theta}|0\rangle + \sqrt{\eta_s}\xi|1\rangle]/\sqrt{\eta_c(1-\xi^2)|\alpha|^2+\eta_s\xi^2}$. To obtain the ideal state, we find the same relation between ξ and $|\alpha|$ as for the scheme without photon number resolving detectors. The total success probability under this condition becomes

$$P_{\mathrm{SC}} = e^{-\eta_c|\alpha|^2}\left[\eta_c|\alpha|^2\left(1-\frac{\eta_s\eta_c|\alpha|^2}{\eta_s+\eta_c|\alpha|^2}\right)+\frac{\eta_s\eta_c|\alpha|^2}{\eta_s+\eta_c|\alpha|^2}\right] \sim 2\eta_c|\alpha|^2. \tag{A28}$$

The density matrix then becomes

$$\rho_{\mathrm{SC}} = \frac{2\eta_s}{2\eta_s+\eta_c|\alpha|^2(1-\eta_s)}|\psi_\theta\rangle\langle\psi_\theta| + \frac{\eta_c|\alpha|^2(1-\eta_s)}{2\eta_s+\eta_c|\alpha|^2(1-\eta_s)}|1\rangle\langle 1|. \tag{A29}$$

Yielding the fidelity

$$F_{\mathrm{SC}} = \frac{2\eta_s}{2\eta_s+\eta_c|\alpha|^2(1-\eta_s)} + \frac{\eta_c|\alpha|^2(1-\eta_s)/2}{2\eta_s+\eta_c|\alpha|^2(1-\eta_s)} \sim 1-\frac{\eta_c|\alpha|^2}{4\eta_s}(1-\eta_s). \tag{A30}$$

Thus, the improvement of using number resolving detectors over non-photon-number-resolving detectors is the factor of $1-\eta_s$ on the first-order term in the intensity of the laser, and we find perfect fidelity if there are no losses on the server side.

5. Phase noise

Phase noise in this system arises from different underlying causes in the three protocols. For SC, the phase of the coherent state θ will change as it travels to the BSM. We will thus transform the coherent state to the density matrix

$$||\alpha|e^{-i\theta}\rangle\langle|\alpha|e^{-i\theta}| \to \int d\delta_\theta\, p_{\delta_\theta}||\alpha|e^{-i(\theta+\delta_\theta)}\rangle\langle|\alpha|e^{-i(\theta+\delta_\theta)}|, \tag{A31}$$

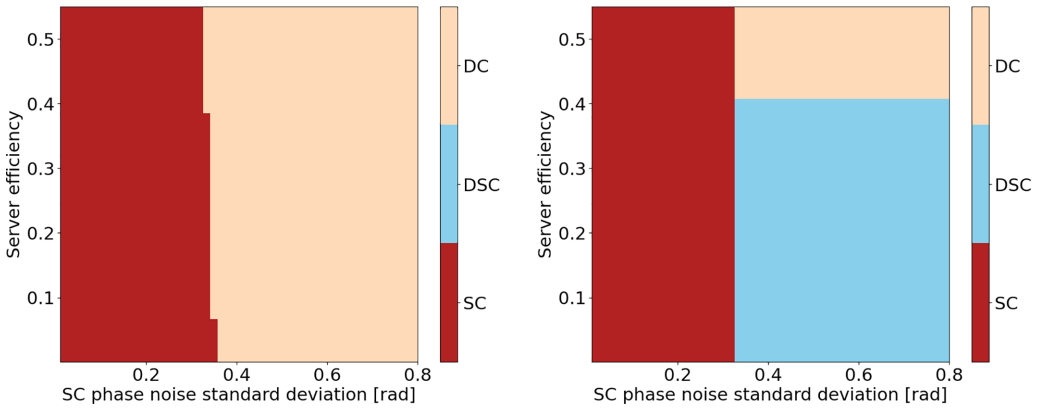


FIG. 6. Optimal RSP protocol—DC, DSC, or SC—giving the highest rate for a given target fidelity, across varying phase noise σ_{SC} and server efficiency. Alternative values for Fig. 4(a). (a) $F_{\mathrm{targ}} = 0.97$, $\sigma_{\mathrm{DSC}} = 0.5$ rad and (b) $F_{\mathrm{targ}} = 0.97$, $\sigma_{\mathrm{DSC}} = 0.25$ rad.

where δ_θ is the added phase noise and p_{δ_θ} is the distribution of the phase noise. This noise means the remotely prepared state is of the form

$$\rho = a|0\rangle\langle 0| + b|1\rangle\langle 1| + \int d\delta_\theta p_{\delta_\theta}\left(ce^{i(\theta+\delta_\theta)}|1\rangle\langle 0| + ce^{-i(\theta+\delta_\theta)}|0\rangle\langle 1|\right), \tag{A32}$$

where a, b, and c are the positive real coefficients of the single-click density matrix. We will assume p_{δ_θ} to be a Gaussian distribution with variance σ^2_{SC}. In principle, one should use a wrapped Gaussian distribution, but it will not change our results, as we will integrate over a periodic function. This leads us to the average fidelity

$$F = \frac{1 + 2ce^{-\sigma^2_{\mathrm{SC}}/2}}{2}. \tag{A33}$$

In the DSC and DC protocols, the density matrix will be transformed by the noise such that

$$||\alpha|e^{-i\theta}, |\alpha|\rangle\langle|\alpha|e^{-i\theta}, |\alpha|| \to \iint d\theta_1 d\theta_2 p_{\theta_1,\theta_2}||\alpha|e^{-i(\theta+\theta_1)}, |\alpha|e^{-i\theta_2}\rangle\langle|\alpha|e^{-i(\theta+\theta_1)}, |\alpha|e^{-i\theta_2}|, \tag{A34}$$

where θ_1 (θ_2) is the random phase added to the first (second) coherent state. The remotely prepared state will take the form

$$\rho = a|0\rangle\langle 0| + b|1\rangle\langle 1| + \iint d\theta_1 d\theta_2 p_{\theta_1,\theta_2}\left(ce^{i(\theta+\theta_1-\theta_2)}|1\rangle\langle 0| + ce^{-i(\theta+\theta_1-\theta_2)}|0\rangle\langle 1|\right), \tag{A35}$$

where a, b, and c can be found from Eqs. (A16) and (A3) for DSC and DC, respectively. As it is the difference between the two phase noises θ_1 and θ_2 that matters, we will make a change of variable such that $\theta_1 \to \theta_2 + \delta_\theta$, this yields the density matrix

$$\rho = a|0\rangle\langle 0| + b|1\rangle\langle 1| + \int d\delta_\theta q_{\delta_\theta}\left(ce^{i(\theta+\delta_\theta)}|1\rangle\langle 0| + ce^{-i(\theta+\delta_\theta)}|0\rangle\langle 1|\right), \tag{A36}$$

where q_{δ_θ} is the marginal distribution over the variable δ_θ. For DC, we can assume q_{δ_θ} to be very close to a delta function as the two coherent states copropagate with a different polarization for the polarization encoding, or with a very slow time delay for the time-bin encoding. For DSC, however, the phase noise depends on the time between consecutive clicks. The shorter the time between successful clicks, the narrower the probability distribution of the phase noise. Assuming q_{δ_θ} is a Gaussian distribution with variance σ^2_{DSC}, we obtain the fidelity

$$F = \frac{1 + 2ce^{-\sigma^2_{\mathrm{DSC}}/2}}{2}. \tag{A37}$$

APPENDIX B: ALTERNATIVE VALUE PLOTS

Figures 6–8 are the same as those occurring in the main text, but with alternative values to understand how the regimes change as the parameters change. Figure 6(a) shows that the advantage region for SC grows if the target fidelity is lower. This is because SC will always be faster than DC, and the region where SC is not shown to be faster is just because SC cannot reach the target fidelity in that area. As expected, Fig. 6(b) shows that the advantage region for DSC grows when the phase noise for DSC is lower. Figure 7 shows the same behavior: More DSC phase noise gives less advantage for DSC, less DSC phase noise gives more advantage for DSC. Finally, Fig. 8 shows the effect of the server efficiency on the advantage regions. We see that SC is useful when the server efficiency is low [larger region for SC in Fig. 8(a)] and

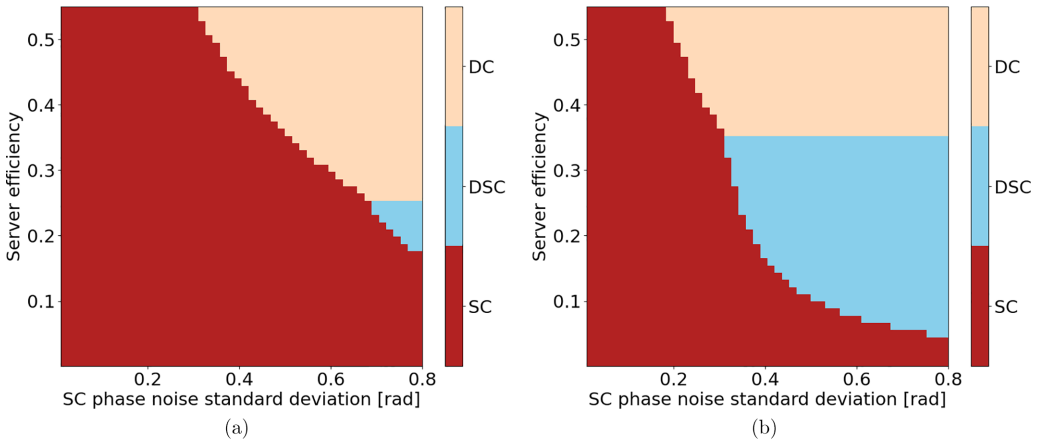


FIG. 7. Optimal RSP protocol—DC, DSC, or SC—giving the highest fidelity for a given target rate, across varying phase noise σ_{SC} and server efficiency. Alternative values for Fig. 4(b). (a) Target $R\tau = 0.03$, $\sigma_{DSC} = 0.5$ rad and (b) Target $R\tau = 0.01$, $\sigma_{DSC} = 0.25$ rad.

DC regains some territory when the server is very efficient [larger region for DC in Fig. 8(b)]. This is also intuitive as SC comes from the idea that the photon arrival probability is low, and therefore the probability of getting two clicks is very low, this does not hold when the server is very efficient.

APPENDIX C: PURIFIED PROTOCOLS FOR QUANTUM KEY DISTRIBUTION

To analyze the correctness of QKD over a repeater chain using these RSP protocols, we convert them to a purified entanglement-based protocol. In such a purified protocol, two clients, Alice and Bob, aim to create entanglement between them. Under the assumption that Alice and Bob's devices are secure and trusted, the purified protocol is indistinguishable from the real protocol by any eavesdropper on the quantum channel. The data and data processing performed by the clients are also the same for the purified protocol as for the real protocol. This allows us to analyze the correctness of the setup depicted in Fig. 5 for performing QKD by examining the equivalent entanglement-based protocol.

We show that our SC protocol for remote state preparation in combination with the setup depicted in Fig. 5 can be used to implement a twin-field type protocol [20], where the whole setup between Alice and Bob together effectively acts as one Bell state measurement. In particular, we follow the security proof given by Curty-Azuma-Lo in the so-called CAL19 protocol [42]. First, we recap the steps of the CAL19 protocol, and then we illustrate how our protocols allow us to produce perfectly correlated bits and to show their compatibility with the CAL19 security proof.

CAL19 protocol

(1) In each round of the protocol, Alice and Bob can choose between two basis, the key generation basis K and the test basis T. These bases are chosen with probability p_K and p_T, respectively. When the basis chosen is K, Alice (Bob) also chooses a random bit l_a (l_b). When the random bit is $l_a = 0$ ($l_b = 0$), Alice (Bob) prepares the coherent state $|\alpha_a\rangle$ ($|\alpha_b\rangle$), while for $l_a = 1$ ($l_b = 1$), she (he) prepares $|-\alpha_a\rangle$ ($|-\alpha_b\rangle$). When the basis chosen is T, Alice prepares a phase-randomized WCP $\hat{\rho}_{a,\beta_A}$ ($\hat{\rho}_{b,\beta_B}$) with a mean photon number randomly picked from a set $S = \{|\beta_i|^2\}_i$.

(2) Alice and Bob send their prepared optical pulses through their corresponding channels.

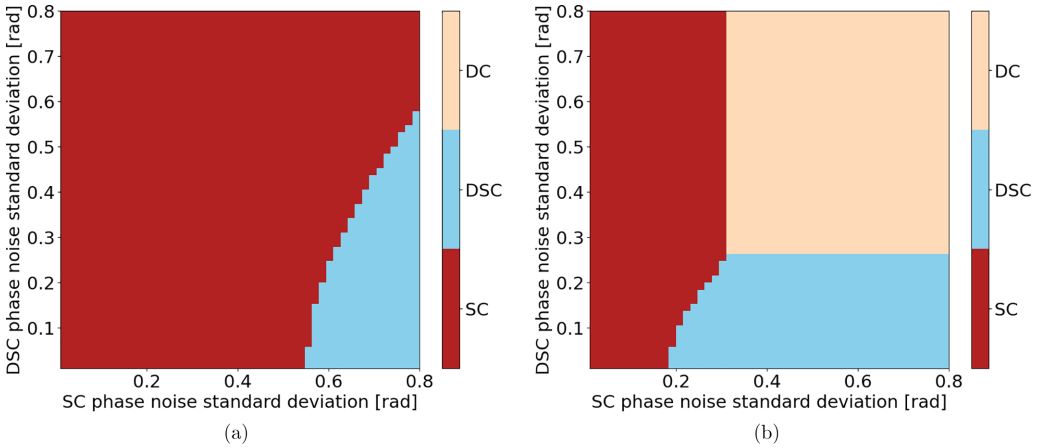


FIG. 8. Optimal RSP protocol—DC, DSC, or SC—giving the highest fidelity for target rate $R\tau = 0.01$, across varying phase noise σ_{SC} and σ_{DSC}. Alternative values for Fig. 4(c). (a) $\eta s = 0.07$ and (b) $\eta s = 0.35$.

(3) In the central node C, both optical pulses are merged in a 50:50 beamsplitter. The result of this interference is registered by the detectors at the output ports of the beamsplitter. We denote the detector at the first output as D_0, and the one on the second port as D_π. We use these names to stress that when the incoming coherent fields have the same phase, in the absence of any source of noise, they should produce a click in D_0. However, if the coherent fields have a phase difference of π, we should expect to register a click in D_π.

(4) After the measurement is performed, the central node C announces which detectors clicked. There are four possible click patterns, but Alice and Bob will keep their data only when one click is registered, either on D_0 or on D_π. The other cases are ignored.

(5) The previous steps are repeated N times such that Alice and Bob can collect enough statistics to perform parameter estimation and quantify the amount of information leaked to an eavesdropper.

(6) Finally, Alice and Bob perform classical error correction and privacy amplification to obtain a final secret key.

Below, we go over the SC and DSC purified protocol in detail to show how entanglement is formed between Alice and Bob.

1. Single click

Now, we detail the purified version of our protocol using SC RSP (see Sec. II C).

SC-RSP-based protocol

(1) A qubit in server nodes S_A and S_B (see Fig. 5), which are at the border of the repeater chain, is prepared in the state $\sqrt{1-\xi^2}|0\rangle + \xi|1\rangle$, with ξ the bright-state parameter of the server qubit. Repeater nodes S_1 and S_2 share entanglement of the form $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

(2) Alice and Bob both prepare the state

$$|\psi_{A/B}\rangle = \frac{1}{\sqrt{2}}(|\alpha, 0\rangle + |-\alpha, 1\rangle), \tag{C1}$$

which combines the state of the photon, where α is a positive real number, with the state of Alice's or Bob's register.

(3) The server node S_A emits a photon entangled with a qubit at the node. Here, we assume perfect efficiencies and photon number resolving detectors, meaning we can perform RSP on $S_{A/B}$ with perfect fidelity (see Appendix A 4), or, in this case, create entanglement between A/B and $S_{A/B}$ with perfect fidelity. Performing a BSM between Alice and node S_A leads to an entangled state between Alice's register and the node

$$|\psi_{A,S_A}\rangle = \frac{\alpha\sqrt{1-\xi^2}|0\rangle|-\rangle + \xi|1\rangle|+\rangle}{\sqrt{\alpha^2(1-\xi^2)+\xi^2}}, \tag{C2}$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The same is repeated on Bob's side.

(4) The entanglement is propagated through the repeater chain using entanglement swapping until Alice's and Bob's registers share this state with neighboring nodes, such as S_2 and S_B. Then, a BSM is performed on S_2 and S_B of $|\psi_{A,S_2} \otimes \psi_{B,S_B}\rangle$. With this, the state shared by Alice's and Bob's registers is projected onto (up to some corrections on Bob's side depending on the click pattern of the BSM)

$$|\psi_{A,B}\rangle = \frac{\alpha^2(1-\xi^2)|00\rangle + \xi^2|11\rangle}{\sqrt{\alpha^4(1-\xi^2)^2+\xi^4}}. \tag{C3}$$

This equals the Bell state $|\Phi^+\rangle_{A,B}$ for $\xi = \alpha/\sqrt{1+\alpha^2}$.

With this, we see that the SC-RSP-based protocol achieves the same functionality as the CAL19 protocol in the noiseless case, both of them can produce perfectly correlated bits for Alice and Bob. In order to claim that our RSP-SC based protocol can produce a secure key, we need to take into account the multiphoton contributions in the WCP used. In the CAL19, this is taken into account using the test basis together with the decoy state method [18,19]. In order to include a test basis, we can simply phase randomize the sources of Alice and Bob and consider a set of different intensities for their pulses in order to also implement the decoy state method. A comparison of the performance of both protocols in noisy scenarios is left for future work.

2. Double single click

We apply the same reasoning of the protocol using SC RSP to the protocol DSC RSP. With this, the protocol detailed in the previous subsection is only changed by repeating the first three steps, resulting in a situation where Alice's register shares two entangled links with the server, $|\psi_{A1,S_{A1}}\rangle$, $|\psi_{A2,S_{A2}}\rangle$, which can then be used to perform a parity projection, essentially implementing the extreme photon loss protocol of Ref. [26]. Note that, when using the normal protocol, i.e., not the entanglement-based purified protocol, this comes down to applying the circuit depicted in Fig. 3. The rest of the steps remain as described for the SC protocol.

[1] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, Remote state preparation, Phys. Rev. Lett. **87**, 077902 (2001).

[2] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, CA, USA 2009), pp. 517–526.

[3] F. Schmidt and P. van Loock, Memory-assisted long-distance phase-matching quantum key distribution, Phys. Rev. A **102**, 042614 (2020).

[4] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, Quantum repeater node demonstrating unconditionally secure key distribution, Phys. Rev. Lett. **126**, 230506 (2021).

[5] T. Morimae and K. Fujii, Blind quantum computation protocol in which Alice only makes measurements, Phys. Rev. A **87**, 050301(R) (2013).

[6] J. F. Fitzsimons, Private quantum computation: An introduction to blind quantum computing and related protocols, npj Quantum Inf. **3**, 23 (2017).

[7] J. van Dam, G. Avis, T. B. Propp, F. F. da Silva, J. A. Slater, T. E. Northup, and S. Wehner, Hardware requirements for trapped-ion-based verifiable blind quantum computing with a measurement-only client, Quantum Sci. Technol. **9**, 045031 (2024).

[8] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[9] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem, Phys. Rev. Lett. **68**, 557 (1992).

[10] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, Single photon quantum cryptography, Phys. Rev. Lett. **89**, 187901 (2002).

[11] M. Garnier, D. Leichtle, L. Music, and H. Ollivier, Composably secure delegated quantum computation with weak coherent pulses, in *2024 International Conference on Quantum Communications, Networking, and Computing (QCNC)* (IEEE, Piscataway, NJ, 2024), pp. 221–225.

[12] Q. Li, C. Liu, Y. Peng, F. Yu, and C. Zhang, Blind quantum computation where a user only performs single-qubit gates, Opt. Laser Technol. **142**, 107190 (2021).

[13] T. Morimae and K. Fujii, Secure entanglement distillation for double-server blind quantum computation, Phys. Rev. Lett. **111**, 020502 (2013).

[14] Y.-B. Sheng and L. Zhou, Deterministic entanglement distillation for secure double-server blind quantum computation, Sci. Rep. **5**, 7815 (2015).

[15] Q. Li, W. H. Chan, C. Wu, and Z. Wen, Triple-server blind quantum computation using entanglement swapping, Phys. Rev. A **89**, 040302(R) (2014).

[16] J. Quan, Q. Li, and L. Li, Verifiable blind quantum computation with identity authentication for multi-type clients, IEEE Trans. Inf. Forensics Secur. **19**, 1687 (2023).

[17] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).

[18] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[19] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[20] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[21] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, *et al.*, Satellite-relayed intercontinental quantum network, Phys. Rev. Lett. **120**, 030501 (2018).

[22] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[23] V. Dunjko, E. Kashefi, and A. Leverrier, Blind quantum computing with weak coherent pulses, Phys. Rev. Lett. **108**, 200502 (2012).

[24] S. D. Barrett and P. Kok, Efficient high-fidelity quantum computation using matter qubits and linear optics, Phys. Rev. A **71**, 060310(R) (2005).

[25] C. Simon and W. T. M. Irvine, Robust long-distance entanglement and a loophole-free Bell test with ions and photons, Phys. Rev. Lett. **91**, 110405 (2003).

[26] E. T. Campbell and S. C. Benjamin, Measurement-based entanglement under conditions of extreme photon loss, Phys. Rev. Lett. **101**, 130502 (2008).

[27] P. C. Humphreys, N. Kalb, J. P. J. Morits, R. N. Schouten, R. F. L. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, Deterministic delivery of remote entanglement on a quantum network, Nature (London) **558**, 268 (2018).

[28] Y.-F. Jiang, K. Wei, L. Huang, K. Xu, Q.-C. Sun, Y.-Z. Zhang, W. Zhang, H. Li, L. You, Z. Wang, *et al.*, Remote blind state preparation with weak coherent pulses in the field, Phys. Rev. Lett. **123**, 100503 (2019).

[29] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).

[30] T. Kapourniotis, E. Kashefi, D. Leichtle, L. Music, and H. Ollivier, Asymmetric quantum secure multi-party computation with weak clients against dishonest majority, arXiv:2303.08865.

[31] This is because the photon coming from the client leaves the server qubit in $|0\rangle$, because the server did not emit a photon and thus was not in the bright state, and the photon coming from the server leaves the qubit in $|1\rangle$; equal probabilities give a state with equal weights $|0\rangle$ and $|1\rangle$, hence on the equator of the Bloch sphere.

[32] T. B. Propp, J. Grimbergen, E. R. Hellebek, J. R. Gonzales-Ureta, J. van Dam, J. A. Slater, A. S. Sørensen, and S. D. C. Wehner, Quantum strategies to overcome classical multiplexing limits, arXiv:2510.06099.

[33] A. J. Stolk, J. J. B. Biemond, K. L. van der Enden, L. van Dooren, E. J. van Zwet, and R. Hanson, Extendable optical phase synchronization of remote and independent quantum network nodes over deployed fibers, arXiv:2408.12464.

[34] C. B. Czegledi, M. Karlsson, E. Agrell, and P. Johannisson, Polarization drift channel model for coherent fibre-optic systems, Sci. Rep. **6**, 21217 (2016).

[35] J. van Dam, Plotting code for single-click protocols, 2026, https://gitlab.tudelft.nl/wehner-research/plotting-code-for-single-click-protocols, accessed 16 February 2026.

[36] J. Schupp, V. Krcmarsky, V. Krutyanskiy, M. Meraner, T. E. Northup, and B. P. Lanyon, Interface between trapped-ion qubits and traveling photons with close-to-optimal efficiency, PRX Quantum **2**, 020331 (2021).

[37] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P Lanyon, Light-matter entanglement over 50 km of optical fibre, npj Quantum Inf. **5**, 72 (2019).

[38] B. Davies, T. Beauchamp, G. Vardoyan, and S. Wehner, Tools for the analysis of quantum protocols requiring state generation within a time window, in *IEEE Transactions on Quantum Engineering* (IEEE, Piscataway, NJ, 2024), Vol. 5, pp. 1–20.

[39] H.-J. Briegel, W. Dür, J. I Cirac, and P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication, Phys. Rev. Lett. **81**, 5932 (1998).

[40] J. van Dam, E. Hellebek, T. Propp, J. Gonzales-Ureta, A. Sørensen, and S. Wehner, Single-click protocol for remote state preparation with a weak coherent pulse source, Dutch Patent

Application, 2025, Patent pending, Application filed 10 July 2025.

[41] J. van Dam, E. Hellebek, T. Propp, J. Gonzales-Ureta, A. Sørensen, and S. Wehner, Double-single-click protocol for remote state preparation with a weak coherent pulse source, Dutch Patent Application, 2025, Patent pending, Application filed 10 July 2025.

[42] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).