npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-026-01181-7

Heralded photonic graph states with inefficient quantum emitters

Maxwell Gold[1,3], Jianlong Lin[2,3], Eric Chitambar[2] & Elizabeth A. Goldschmidt[1] ✉

Quantum emitter-based schemes for the generation of photonic graph states offer a promising, resource-efficient methodology for realizing distributed quantum computation and communication protocols on near-term hardware. We present a heralded scheme for making photonic graph states that is compatible with the typically poor photon collection from state-of-the-art coherent quantum emitters. We demonstrate that the construction time for large graph states can be polynomial in the photon collection efficiency, as compared to the exponential scaling of current emitter-based schemes, which assume deterministic photon collection. The additional overhead here consists of an extra spin qubit plus one additional spin-spin entangling gate per photon added to the graph. While the proposed scheme requires both non-demolition measurement and efficient storage of photons in order to generate graph states for arbitrary applications, we show that many useful tasks, including measurement-based quantum computation, can be implemented without these requirements. As a use case of our scheme, we construct a protocol for secure two-party computation that can be implemented efficiently on current hardware. Estimates of the fidelity to produce graph states used in the computation are given assuming current and near-term fidelities for highly coherent quantum emitters.

The vast promise of quantum information technologies for faster and more secure computational and information systems relies on entanglement as a primary resource. Traditional gate-based quantum computing requires the ability to perform sequences of joint operations across multiple qubits. An alternative paradigm, known as measurement-based quantum computation (MBQC), realizes universal computation through sequences of single-qubit measurements made on an initially prepared entangled resource state[1]. This is an appealing approach for photonic quantum systems as single photon rotations and measurements are straightforward using commercial optical elements, and fast, efficient routing solutions are readily available[2]. Furthermore, the sequential nature of photon emission allows entangled states to be built from photons emitted at different times by the same emitter[3]. By using entangled emitters, it then becomes possible to simulate entangling gates between photons and overcome the difficulty of realizing direct photon-photon interactions[4]. Indeed, it is known that computationally useful graph states of photons can be generated using either a small number of coherent quantum emitters[5,6], a combination of a single emitter and fusion gates[7–11], or a single quantum emitter in a feedback scheme[12].

All of these aforementioned schemes assume a photon is successfully added to the graph every time an emitter is excited, and we thus term this class of schemes as being "deterministic". For realistic systems with less than perfect emission and collection efficiency, the time to make a graph thus scales exponentially in the size of the graph because any failure to detect a photon triggers a restart of the whole protocol. In general, highly efficient collection from individual quantum emitters is a challenge that remains largely out of reach today, making such deterministic schemes impractical for generating even moderately sized graph states (10–100 photons) on near-term hardware[13–16].

In Results, we introduce a method for photonic graph generation based on coherent emitters that uses an "emit-then-add" approach, where each photon is attached to the graph only following confirmation of its emission and collection. In this way, a lost photon does not truncate the rest of the graph, and the time to produce a photonic graph state scales polynomially in the size of the graph. In addition to this improved scaling in construction time, our scheme is tolerant to arbitrary loss with only a linear reduction in rate, unlike other deterministic schemes, which have loss-tolerant thresholds in the 1–10% range[10,11,17–22]. Compared to deterministic protocols[23], one additional spin is required in order to allow the emitter to be disconnected from the graph until photon collection is confirmed. Furthermore, for each photon added to the graph, our scheme requires one additional spin-spin entangling operation plus one mid-circuit measurement and reset (MCMR)

[1]Department of Physics, University of Illinois Urbana-Champaign, Urbana, IL, USA. [2]Department of Electrical and Computer Engineering, University of Illinois Urbana-Champaign, Urbana, IL, USA. [3]These authors contributed equally: Maxwell Gold, Jianlong Lin. ✉e-mail: goldschm@illinois.edu

of the emitting spin. (Note that these only occur upon heralding of successful photon emission; they are not required on every attempt).

Typically, confirming the presence of a photon in a particular optical mode requires destructive measurement of the photon. For arbitrary applications of photonic graph states where the photons are measured in any order and in any basis, one would thus require quantum non-demolition (QND) measurements[24–26], in order to determine successful collection of the photon before adding it to the larger graph, plus storage of the photon until it can be measured in the desired basis. Such a scheme is largely out of reach today, though we discuss in Supplementary Note 1 a detailed method for its implementation on current hardware, based on entanglement swapping with a separately produced entangled photon pair.

Importantly, we show here that a large class of graph state protocols (including MBQC) admit projective measurements of each photon before adding it to the larger graph. In this way, we show how to build a heralded virtual graph state of photons that never exist at the same time. Large virtual graph states can be built quickly with high fidelity in this way. We also introduce in Results an example use case for our scheme: A particular protocol that uses multiple copies of a small virtual graph state to implement secure two-party classical computation on arbitrarily large inputs and requires just a single quantum emitter and two auxiliary spin qubits. We demonstrate how this protocol can include classical error correction to mitigate experimental errors, including entangling gate infidelities and decoherence in state-of-the-art to near-term trapped ion and trapped neutral atom systems.

Results

Emit-then-add: overview

Given the generally poor collection efficiency shown by highly coherent quantum emitters that can be entangled with additional spin qubits, we propose a general methodology, dubbed "emit-then-add," for constructing photonic graph states to circumvent this issue. A single emitter is initialized into an unentangled state and excited to produce a single photon that is entangled with its long-lived internal spin state and collected with some overall efficiency η_e. This can be implemented with a wide variety of quantum emitters, including laser-cooled atoms or ions, quantum dots, and defects or dopants in wide-bandgap semiconductors[3,16,27–30]. Photons can be encoded in various degrees of freedom, including polarization, time-bin, and frequency[31–35]. In addition to the single emitter, we require a set of auxiliary spin qubits that can be controllably entangled in a pairwise way (with the emitter and with each other) via local and deterministic two-qubit spin-spin entangling gates. We note that these auxiliary spins are never used for emission of photons for the graph and can be different physical qubits from the emitter (i.e., a different atomic species in an atom or ion system or nearby nuclear spins coupled to a defect or dopant emitter in solid-state)[36–38].

Deterministic schemes for constructing photonic graph states, such as those in refs. 6,23, center their building operations on the emitting spin itself, while the central feature of our method is to add a photon to the graph only following a logical herald of its successful emission and collection. Successfully adding each photon to the graph state requires entangling the emitter with an auxiliary spin, and then measuring it out of the graph and reinitializing it to prepare for the next attempted photon emission. Following a correction to the photon and auxiliary spin based on the outcome of this measurement, the state of the system is as if the auxiliary spin had directly emitted the photon itself. In this sense, we construct a graph state of only heralded photons, where we have split the role of the emitter in deterministic schemes into an emitting spin that generates the photons and an auxiliary spin that stores the quantum information. Thus, we see that emit-then-add admits the construction of arbitrary photonic graph states using the same methods described in ref. 6 with minimal additional overhead. Namely, the graph state itself is built using a sequence of two-qubit and local Clifford gates on the spins and only local Clifford gates on the photons. The local gates on each photon can all be combined and applied as a single rotation prior to using the graph state in subsequent applications.

The key improvement of our scheme is that uncollected photons do not disturb the state of the graph that is being built. When successive photon collection is required for building a graph on a single emitter, any failed detection traces the photon out of the system and truncates the graph, which can necessitate restarting construction from scratch. In typical deterministic quantum emitter-based schemes, any inefficiency in collection therefore leads to exponentially poor scaling with graph size. Given current hardware, this severely limits the size and rate of generation for photonic graph states, particularly those that require multiple spin qubits. We note that there are loss tolerance and percolation thresholds that improve this scaling, but they require much better collection efficiency than is feasible with near-term systems[10,11,17–22]. In our scheme, any failed detection simply results in the reinitialization of the emitting spin without any disturbance to the overall graph under construction. This ultimately trades photonic loss as the primary constraint on generating arbitrarily large graph states for emitter and spin properties such as coherence times and spin-spin entangling fidelities, which is why our scheme is particularly well-suited for state-of-the-art to near-term trapped ion and trapped neutral atom systems.

For general-purpose applications, we require a method to detect the presence of a photon that is non-destructive. This can be met with any form of QND measurement that heralds spin-photon entanglement. In Supplementary Note 1 we provide an example for implementing such a scheme on current hardware, utilizing entanglement swapping and a separately produced entangled photon pair. Here, a pair of entangled photons is probabilistically produced, which can be implemented via standard nonlinear optical processes, such as spontaneous parametric down conversion (SPDC)[39,40]. The pair production probability can be controlled by the pump power. One member of the photon pair, the signal photon, is wavelength and bandwidth matched to the emitter photon, and the entangled pair is encoded in the same degree of freedom as the emitter photon. The emitter photon and signal photon are sent to a joint measurement apparatus, which, upon a successful measurement outcome, projects the emitter spin and the unmeasured photon, the idler photon, onto an entangled Bell state[41]. Since only certain measurement outcomes correspond to entanglement between the emitter spin and the idler photon, the procedure is repeated until a successful herald is flagged. While this procedure works in principle, it has some major drawbacks, including a significant reduction in rate due to the probabilistic nature of generating entangled photon pairs as well as the introduction of additional infidelities due to factors including multi-pair production and imperfect heralding efficiency.

Instead, we show that for many applications, including MBQC, non-destructive measurement is not required. For these applications, the nodes in the graph are measured sequentially, with the choice of measurement basis on one node depending on the outcomes of previous ones. It is, thus, not necessary to build the full graph state before beginning these measurements, as an emitter photon can be destructively measured as soon as the correct basis for measurement is determined[42]. This measurement thus serves doubly as a prescribed step in the MBQC protocol and as a herald for the emitter photon. Upon failure to detect the photon, we reinitialize the emitter and attempt generation again, as we would with some QND measurement. Upon successful detection, we perform all required logic on the emitter and auxiliary spins, measure the emitter out of the graph, and reinitialize the emitter to attempt generation of the next photon. This simpler emit-then-add scheme is shown in Fig. 1, and it has the advantage that it requires no storage of the emitter photon prior to measurement. The graph state being constructed is therefore "virtual" in the sense that not all photons within the graph need to exist at the same time.

However, there are limitations on when this scheme can be employed. Namely, a photon can be destructively measured immediately upon generation provided that two conditions are satisfied: (1) the correct measurement basis for that photon, as set by the protocol, is determined prior to its emission, and (2) this measurement is either Pauli Z or of the form $\cos\phi X + \sin\phi Y$. Condition (1) can be met for MBQC, as the emission order can be chosen to match the measurement order of the computation, albeit at the cost of using extra auxiliary spins and two-qubit gates in some

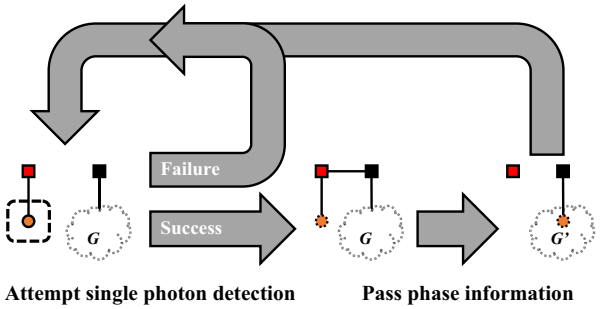

Fig. 1 | A construction scheme for heralding virtual graph states, with emit-then-add. A quantum emitter (red) is repeatedly excited until a single photon (orange) is successfully detected. Upon detection, logic is executed, which passes the conditional phase information written onto the emitter to an auxiliary memory spin (black), which encodes a virtual graph state (represented by dashed boundaries).

cases[23]. The second condition can also be met in principle, since the specified gate sets are sufficient for universal MBQC[1,43].

To understand condition (2) in more detail, note that if the full graph state were built such that the emitter is measured before its emitted photon, then each photon would have a local Clifford error of the form UZ^m, where U is a fixed Clifford and $m \in \{0, 1\}$ is determined by the decoupling measurement on the emitter spin. If M is the measurement to be subsequently performed on the photon in the MBQC protocol, then when correcting for the Clifford error, the effective measurement would be $M' = UZ^m M Z^m U^\dagger$. When $M = Z$, then $M' = UMU^\dagger$; or when $M = \cos\phi X + \sin\phi Y$, then $M' = (-1)^m UMU^\dagger$. In the first case, the dependence on m is completely removed, and the photon can be equivalently measured with $UMU^\dagger$ immediately after it is emitted in this simpler scheme. In the second case, it can also be immediately measured with $UMU^\dagger$, but now one must perform a bit flip on the classical measurement outcome if $m = 1$; this is because an overall -1 factor on a spin observable simply flips the spin-up/spin-down outcomes. In total, the correct computation can still be attained, because protocols admitting only measurements of this form write their outcomes as a conditional phase on their neighbors in the graph. In our scheme, this conditional phase information is imparted on the emitter with each successful single photon detection, and subsequently passed into memory on one of the auxiliary spins. Computation is then achieved by passing conditional phases into memory in a specific pattern, performing logic between auxiliary spins, and classical post-processing for observables of the specified form.

While satisfying conditions (1) and (2) above is sufficient for universal MBQC using virtual graph states, this is often not the most efficient method in terms of the overall number of photons used to drive the computation. For example, building out the graph to a certain depth and measuring in a different sequence than the emission order can lead to more compact gate implementations[43]. Also, using MBQC measurements outside of the x–y plane allows for more general forms of information flow[44]. Nevertheless, as we show below, this simpler scheme can enable dramatically faster construction and higher fidelity with no photon storage required. For emit-then-add schemes incorporating some form of QND measurement instead, photon storage is required for at least the time to perform the spin-spin entangling gates and the decoupling measurement on the emitter. For the remainder of this section, we discuss in more detail the advantages of emit-then-add, specifically in the context of this simplified construction scheme for heralding virtual graph states that contain n_p photons.

Emit-then-add: overhead

It is known that the sequential nature of photon emission imposes nontrivial resource requirements when constructing graph states, specifically in terms of the number of required emitters and two-qubit spin-spin entangling gates needed to build out the graph. As discussed in the introduction, constructing graph states with emit-then-add further adds to this overhead. The total number of spins we require is only one more than the deterministic case, as each auxiliary spin in our scheme replaces an emitter in deterministic schemes, and only a single emitting spin is required. A consequence of this is that the total number of auxiliary spins required in our scheme scales equivalently to ref. 23 (see the "Methods" section for further details). In practice, more emitting spins can be employed in parallel to speed up the construction. As the emitting spin in our scheme must remain disjoint from the graph for each excitation, an additional two-qubit spin-spin entangling gate and MCMR operation are required per successfully heralded virtual photon, in order to entangle the emitter with the larger graph and subsequently disconnect it for the next emission. In the "Methods" section, we also demonstrate efficient construction subroutines for building certain graph states that directly employ the methods of ref. 6.

Emit-then-add: fidelity

We make a simple estimate of the final state fidelity for graph states generated with emit-then-add, as the probability that no error occurs when building the state. In this way, our estimates reflect a similarity with the deterministic case, where detected failures require discarding the state and restarting. Hence, these fidelities represent a binary, such that we assume a lower bound $F \geq 1/2$. Notably, failure to collect an emitted photon does not require restarting, unlike typical deterministic schemes.

In addition to overhead, there are infidelities that affect the final graph state with emit-then-add that are not present in the deterministic scheme, namely any infidelity in the additional two-qubit spin-spin entangling gate and mid-circuit measurement and reset of the emitter. We capture all of this, plus the initial fidelity of the emitter-photon entanglement, in a parameter, F_{add}, for the total fidelity of the process to add a photon to the graph. Note that photon detection inefficiency does not affect the fidelity because failing to detect a photon simply triggers a reset. Any infidelity in measuring the state of the photon does affect F_{add}, but this can be minimal for photons (and has the same effect as for the deterministic schemes for photonic graph state production).

Importantly for our scheme, when building a graph, all auxiliary spins must remain coherent for the entire time they are a part of the graph, which is much longer than the n_p repetition cycles over which the graph is generated in the deterministic scheme. Thus, in practice, our scheme can be limited by spin coherence (denoted τ). In modeling the effects of this dephasing, we note that the emitter is reinitialized with each attempt to add a new photon to the larger graph, and hence, it is only required to remain coherent for time to add it to the larger graph, denoted t_{add}. For the auxiliary spins, on the other hand, the average time for the successful addition of a new photon to the larger graph goes as t_{rep}/η_e, where t_{rep}^{-1} is the experimental repetition rate. Hence, the contribution to the state fidelity from the emitter and any auxiliary spins as a result of decoherence is

$$F_D^{(e)}(n_p) = \left(\frac{1}{2}(1 + e^{-(t_{\text{rep}}+t_{\text{add}})/\tau})\right)^{n_p}, \tag{1}$$

$$\langle F_D^{(s)}(n_p)\rangle = \frac{1}{2}\left(1 + e^{-n_p(t_{\text{rep}}/\eta_e+t_{\text{add}})/\tau}\right), \tag{2}$$

where we include a superscript to denote the emitter (e) and auxiliary spins (s), respectively. For simplicity in the above, we have used the same coherence time τ for the emitter and auxiliary spins in the system, though this may not be the case for hybrid systems[36,37].

Putting the above equations together with the fidelity to add a photon to the graph, the final fidelity to generate an n_p-photon graph state with an emitter and a single auxiliary spin ($n_s = 1$) is

$$F_{n_s=1}(n_p) = (F_{\text{add}})^{n_p} F_D^{(e)}(n_p)\langle F_D^{(s)}(n_p)\rangle, \tag{3}$$

assuming our variation of emit-then-add that does not rely on QND measurements. In total, moving from the deterministic scheme to one proposed here effectively means moving from a scheme limited by photon

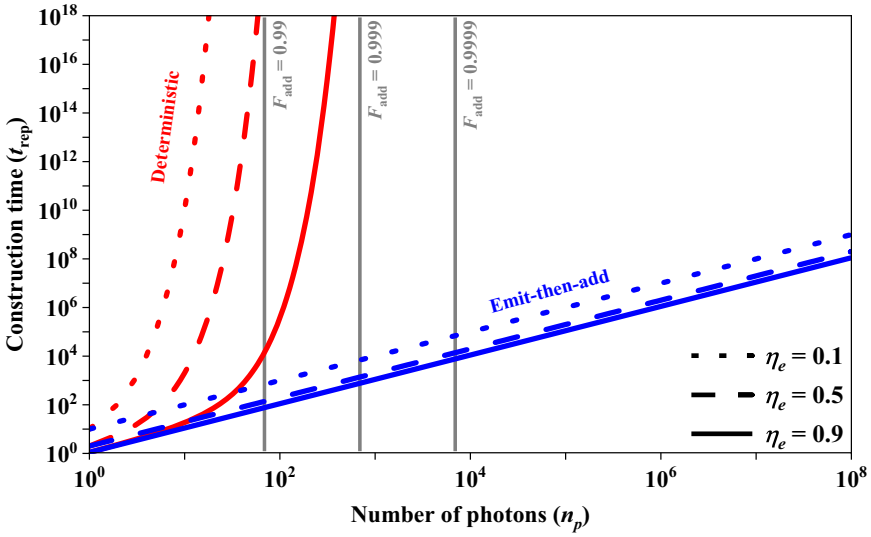

Fig. 2 | Time to make photonic graph states of size n_p in units of the repetition period. Principal deterministic schemes (red) and our emit-then-add (blue) scheme are compared. The three curves of each color represent emitter photon collection efficiencies $\eta_e \in \{0.1, 0.5, 0.9\}$. The polynomial scaling in our schemes allows for the construction of larger photonic graphs. Cutoffs (gray, vertical) are depicted where the additional infidelities associated with emit-then-add (such as contributions from spin-spin entangling gates and MCMR operations) preclude the construction of larger graph states with fidelities better than 1/2, for $F_{add} \in \{0.99, 0.999, 0.9999\}$, comparing results from refs. 47–51. Despite these cutoffs, graph states of 10–100 photons are achievable on realistic timescales, with only moderate requirements on F_{add}.

collection efficiency to one limited by dephasing and the fidelities of entangling and MCMR operations.

Given typical photon collection efficiencies, experimental repetition rates, and entangling gate and MCMR speeds, we expect to be in the regime of $t_{rep} \ll t_{add} \lesssim t_{rep}/\eta_e \ll \tau$. Here, the emitting spin must have a coherence time longer than the time to add a single photon to the graph, while the auxiliary spins must have much longer coherence times that account for all the failed attempts as well as repeated entangling gates and MCMR operations. Thus, a realistic implementation of this scheme requires auxiliary spins that have exceedingly large coherence times, with the requirement increasing for increasing graph size. Trapped ion and neutral atom systems have been shown to host second-scale coherence times[45,46], which should allow the generation of moderately sized graph states (10–100 photons), even with the relatively slow ($\lesssim$ ms) entangling gate and MCMR times that are typical of these systems.

Our generalized scheme (outlined in Supplementary Note 1) involving entanglement swapping using a photon pair source incurs an additional infidelity through false heralds during the swapping process.

Emit-then-add: scaling

Finally, the most significant advantage of emit-then-add comes in scaling up the size of graph states using state-of-the-art to near-term hardware. The average time to successfully generate an n_p-photon graph via the deterministic scheme, by directly collecting photons from an emitter in n_p subsequent excitation events, is $\mathcal{O}(\eta_e^{-n_p})$, where η_e is the emitter collection efficiency, because any failed detection event truncates the graph. For our emit-then-add scheme, a failed detection of the emitter photon simply triggers reinitialization of the emitter and another attempt at photon emission, while the graph under construction remains unaffected. Therefore, an n_p-photon graph state will be created over a time that is $\mathcal{O}(n_p\eta_e^{-1})$. Our generalized scheme has additional factors affecting the scaling, but also demonstrates dramatic improvement over the deterministic schemes at large graph sizes.

As a comparison to the experimental schemes motivated by ref. 6, the time to make an n_p-photon graph state (in units of the repetition period for exciting the emitter) is shown in Fig. 2 for $\eta_e \in \{0.1, 0.5, 0.9\}$ for deterministic (red), and emit-then-add (blue) schemes. We do not include the time to perform gates and MCMR operations of the spins for these estimates, and we assume that the emitter coherence does not limit the graph size for either scheme (i.e., $\tau/n_p \gg t_{rep}/\eta_e + t_{add}$). We include cutoffs where the additional infidelity, captured by F_{add} defined above, precludes the construction of larger graph states. Given the current state-of-the-art for trapped ion and neutral systems[47–51], the vertical gray lines in Fig. 2 depict the cutoffs where $(F_{add})^{n_p} < 1/2$.

Two-party computation with graph states: overview

As one application of our emit-then-add scheme, we describe a method for securely computing an arbitrary Boolean function $f: \{0,1\}^{\times n} \to \{0,1\}$ of either two parties or a restricted class of multi-party functions. As a special type of MBQC, our protocol, $\mathcal{P}$, performs the calculation through a sequence of measurements on distributed graph states, followed by classical broadcasting and local processing. Only Pauli measurements are needed, which are performed adaptively without any communication. Therefore, $\mathcal{P}$ can be implemented without any need for photonic memory, utilizing our variant of emit-then-add for building virtual graph states, where the generation of the requisite resource state happens in parallel with the computation. Furthermore, the size of each graph state required for $\mathcal{P}$ is fixed at 12 photons, regardless of the number of parties or the size of their inputs, which bodes well for state-of-the-art to near-term hardware.

Secure multi-party computation (MPC) is a task in which two or more parties compute some function on their individually held variables without revealing the values of the variables to each other[52,53]. For example, in Yao's famous millionaire problem, two parties want to determine whose bank account has the most money without actually revealing how much money is in each account. MPC is a deeply studied topic in both classical and quantum cryptography, and a variety of MPC protocols have been proposed, achieving different levels of security and relying on different operational assumptions[54].

We propose a method for restricted MPC that includes all two-party computations and requires only two rounds of public communication in the form of broadcasting, or *openings*, regardless of the size of the computational input. Our protocol follows a well-known approach of decomposing an MPC into *offline* and *online* phases[55–57]. In the offline phase, a universal computational resource is distributed to all the parties. Crucially, this resource does not depend on the particular function being computed, other than its input size. Then, in the online phase, this resource is used to compute some chosen function of the parties' inputs. For example, in the classical setting, one well-known computational resource is a special form of shared randomness known as "Beaver triples," which can be used to efficiently compute logical AND gates in the online phase[58]. The problem of MPC then reduces in part to secure and efficient offline methods for distributing shared randomness, such as Beaver triples, which directly enable secure online computation. In a similar spirit, our protocol involves distributing certain quantum graph states in the offline phase, which then

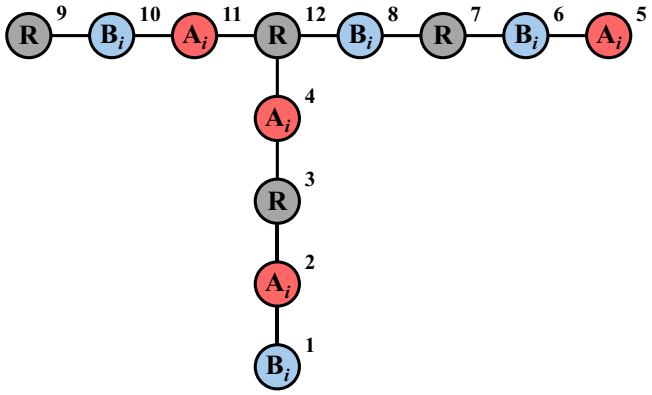

Fig. 3 | For each requisite bit conjunction in Stage I, the 12-qubit graph state $|G\rangle$ is distributed to R (the Referee) and a pair of parties labeled $\mathbf{A}_i$ (Alice), $\mathbf{B}_i$ (Bob). When the measurement sequence detailed by the protocol is implemented honestly, a correlation is generated between the parties, such that $a_ib_i = m_{i,12} + \alpha_i + \beta_i$, where α_i and β_i are locally computed by Alice and Bob, respectively, from openings made in Stage II. Hence, we utilize each copy of the state to achieve a homomorphic encryption of a bit conjunction a_ib_i, where Alice, Bob, and the Referee each possess an additive share. The numeric script above each qubit reflects an example photon emission order for the generation of the graph state.

enable the computation of a logical AND in the online phase, through quantum measurement and classical post-processing.

Beyond its relatively low communication costs, a significant advantage of our protocol is that the parties can, in principle, use graph state certification protocols to unconditionally verify that some untrusted Source is faithfully distributing the correct graph state[59,60], an ability that does not exist for classical sources of shared randomness. Furthermore, we prove that our online phase offers unconditional *privacy* against an arbitrary malicious adversary, with access to a general quantum instrument[61], in the sense that honest participation reveals no information about a party's input, other than what can be inferred from the evaluation of the final computed function.

Note that in our discussion of the protocol here, we do not offer any means of ensuring fairness, such as *security with abort* or *guaranteed output delivery*. We do not claim that the full MPC here is unconditionally secure in this sense, and a classical means of ensuring fairness for the broadcasts in our online phase can be employed with computational security guarantees[62,63]. Instead, the novelty of this work is in the ability to disseminate a specific online correlation with unconditional security. In a similar vein to quantum key distribution, we demonstrate how quantum states offer the ability to distribute information-theoretic secure shared randomness, in our case, in a form that directly enables MPC.

Two-party computation with graph states: protocol

Suppose that N parties $\mathbf{P}_1, \cdots, \mathbf{P}_N$ wish to compute some Boolean function $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$, where $\mathbf{x}_k$ is a string of bits representing the input for party $\mathbf{P}_k$. In addition to correctness, the evaluation of f should be done securely such that the parties learn no more information about the individual $\mathbf{x}_1, \cdots, \mathbf{x}_N$ beyond their own input and what is revealed in the function value $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$. To achieve this task, we propose a method of delegated computation in which a non-collaborating Referee, $\mathbf{R}$, is introduced to assist in the computation of $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$. To maintain privacy, $\mathbf{R}$ also should not learn any more information about the $\mathbf{x}_k$ beyond what is implied by the computed value $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$, nor does $\mathbf{R}$ reveal any more information to the other parties, other than what is necessary to evaluate f securely.

We utilize the fact that every Boolean function f can be expressed in an algebraic normal form (ANF), which presents f as a sum (mod 2) of different variable conjunctions. That is, we can write $f = \sum_{i=1}^{\mathfrak{R}} \mathbf{c}_i$, where each $\mathbf{c}_i$ is the logical AND of a certain group of input variables. By combining variables belonging to the same party, every $\mathbf{c}_i$ becomes the conjunction of at most N variables, each one belonging to a different party. In this work, we restrict attention to functions f that admit an ANF whose conjunctions involve no more than two variables. This covers the entire class of two-party functions, but also includes certain multi-party functions, such as the three-party majority function $\varphi_3(x, y, z) = xy + xz + yz \,(\mathrm{mod}\, 2)$, which outputs the majority value among inputs $x, y, z \in \{0, 1\}$. In general, the functions we consider have the form $f = \sum_{i=1}^{\mathfrak{R}} a_ib_i + \sum_{k=1}^{N} z_k$, where a_i and b_i are the input bits of each quadratic conjunction, belonging to different parties, and z_k is the input bit of the linear part of f, belonging to party $\mathbf{P}_k$. We let $\widetilde{\mathbf{x}}_k \subset \{a_i, b_i, z_k\}_{i=1,k=1}^{\mathfrak{R},N}$ denote all the inputs of f belonging to $\mathbf{P}_k$. Furthermore, if each $\widetilde{\mathbf{x}}_k$ is no more than M bits, then $\mathfrak{R} \le \binom{N}{2}(M-1)^2$.

The offline phase of $\mathcal{P}$ calls for the distribution of $\mathfrak{R}$ copies of the graph state $|G\rangle$ depicted in Fig. 3, one copy for each conjunction a_ib_i in f. A key detail for experimental implementation is that the generation of each copy of $|G\rangle$ requires only two auxiliary spins in the scheme we propose, given the depicted emission order[23]. We denote the i^{th} copy as $|G_i\rangle$, and their distribution can be conducted in parallel. The specific qubits in each $|G_i\rangle$ are given to the parties $\{\mathbf{A}_i, \mathbf{B}_i\} \subset \{\mathbf{P}_1, \cdots, \mathbf{P}_N\}$ who, respectively, have inputs $\{a_i, b_i\}$ to the conjunction a_ib_i. We assume without loss of generality that each party receives qubits belonging to at least one $|G_i\rangle$, an assumption that can be trivially ensured by adding conjunctions to f of inputs that are identically zero. This is a technical requirement of our protocol since the $|G_i\rangle$ will ultimately be used to generate one-time pad bits, and each party needs at least one. In practice, the $|G_i\rangle$ can be generated by an untrusted quantum Source, and its correctness can be certified[59,60]. Specific steps for building $|G\rangle$ in utilizing emit-then-add are presented in the "Methods" section.

The online phase of $\mathcal{P}$ thereafter is split into two stages. Stage I involves measuring Pauli observables, X, Y, Z, on $\mathfrak{R}$ copies of the graph state $|G\rangle$, depicted in Fig. 3, following the sequence below.

Stage I. **Obtaining correlations from quantum states**

Input: For $i \in \{1, \cdots, \mathfrak{R}\}$, the following measurement sequence is performed by $\{\mathbf{A}_i, \mathbf{B}_i\} \subset \{\mathbf{P}_1, \cdots, \mathbf{P}_N\}$, along with $\mathbf{R}$, on copy $|G_i\rangle$. $\mathbf{A}$ inputs a_i.

(I.1). $\mathbf{B}_i$ and $\mathbf{A}_i$ measure Z on qubits 1 and 5, respectively, obtaining measurement outcomes $m_{i,1}$ and $m_{i,5}$.

(I.2). $\mathbf{A}_i$, $\mathbf{B}_i$, and $\mathbf{R}$ measure X on qubits 2, 6, and 9, respectively, obtaining measurement outcomes $m_{i,2}$, $m_{i,6}$, and $m_{i,9}$.

(I.3). $\mathbf{R}$ measures Z on qubits 3 and 7, and $\mathbf{B}_i$ likewise measures Z on qubit 10. They obtain measurement outcomes $m_{i,3}$, $m_{i,7}$, and $m_{i,10}$.

(I.4). $\mathbf{A}_i$ applies $Z^{m_{i,2}}$ to qubit 4 and measures $W^{a_i}Z(W^\dagger)^{a_i}$ on qubits 4 and 11 thereafter, where $W \equiv (iX)^{1/2}$. She obtains measurement outcomes $m_{i,4}$ and $m_{i,11}$. Note that $WZW^\dagger = Y$.

(I.5). $\mathbf{B}_i$ applies $Z^{m_{i,6}}$ to qubit 8 and measures $W^{m_{i,10}}Z(W^\dagger)^{m_{i,10}}$ thereafter, obtaining measurement outcome $m_{i,8}$.

(I.6). $\mathbf{R}$ measures $V^{m_{i,9}}X(V^\dagger)^{m_{i,9}}$ on qubit 12, where $V \equiv (-iZ)^{1/2}$, obtaining measurement outcome $m_{i,12}$. Note that $VXV^\dagger = Y$.

When all the measurements through step (I.3) are made as specified, the parties obtain correlated measurement outcomes satisfying the relationships

$$m_{i,1} + m_{i,2} + m_{i,3} = 0, \tag{4}$$

$$m_{i,5} + m_{i,6} + m_{i,7} = 0, \tag{5}$$

$$m_{i,9} + m_{i,10} = 0, \tag{6}$$

where we define $s_i \equiv m_{i,9} = m_{i,10}$. When the subsequent measurements through step (I.6) are made as specified, the Referee's final outcome satisfies

$$a_ib_i = m_{i,12} + \alpha_i + \beta_i, \tag{7}$$

where

$$\alpha_i = a_i(m_{i,1} + b_i + 1) + (m_{i,4} + m_{i,11}) \tag{8}$$

$$\beta_i = (m_{i,5} + a_i)s_i + m_{i,8}. \tag{9}$$

The end result of each iteration i of the measurement sequence leaves Alice, Bob, and the Referee with additive homomorphic shares of the bit conjunction $a_i b_i$. The only temporal restrictions on the sequence are that measurements in steps (I.1)–(I.3) need to be performed prior to those in steps (I.4)–(I.6). Furthermore, we can understand both α_i and β_i as two layers of data that are nested together by one-time pads. For α_i, the bit $(m_{i,4} + m_{i,11})$ serves as a pad (known only to Alice) for the two multipliers a_i and $(m_{i,1} + b_i + 1)$; while within the latter multiplier, the bit $m_{i,1}$ serves as a pad (known only to Bob) for $b_i + 1$. A similar interpretation holds for β_i.

The padded structure of the bit values obtained in Stage I enables the calculation of each α_i and β_i using public communication (i.e., "openings") and local processing in Stage II of $\mathcal{P}$, without revealing any information about the corresponding a_i or b_i. A second round of communication thereafter opens only the collective sum $\sum_{i=1}^{\mathfrak{R}} a_i b_i$ of the bit conjunctions encrypted in Stage I, while also adding the linear term $\sum_{k=1}^{N} z_k$, thereby allowing the secure evaluation of f.

Stage II. **Public communication and classical post-processing**

Input: Let $\mathcal{A}_k \subset \{1, \cdots, \mathfrak{R}\}$ denote the set of conjunctions in which $\mathbf{P}_k$ played the role of $\mathbf{A}_i$, and similarly, let $\mathcal{B}_k \subset \{1, \cdots, \mathfrak{R}\}$ denote the set of conjunctions in which $\mathbf{P}_k$ played the role of $\mathbf{B}_i$. $\mathbf{P}_k$ inputs their bits from $\{\alpha_i\}_{i\in\mathcal{A}_k}$ and $\{\beta_i\}_{i\in\mathcal{B}_k}$, along with their bit z_k. $\mathbf{R}$ inputs their bits from $\{m_{i,12}\}_{i=1}^{\mathfrak{R}}$.

(II.1). For each $i \in \{1, \cdots, \mathfrak{R}\}$,

(a). $\mathbf{A}_i$ opens $c_{i,A} \equiv m_{i,5} + a_i$ and $\mathbf{B}_i$ opens $c_{i,B} \equiv m_{i,1} + b_i + 1$.

(b). $\mathbf{A}_i$ locally computes $\alpha_i = c_{i,B} a_i + (m_{i,4} + m_{i,11})$ and $\mathbf{B}_i$ locally computes $\beta_i = c_{i,A} m_{i,10} + m_{i,8}$.

(II.2). For each $k \in \{1, \cdots, N\}$, $\mathbf{P}_k$ opens $\Gamma_k \equiv z_k + \sum_{i\in\mathcal{A}_k} \alpha_i + \sum_{i\in\mathcal{B}_k} \beta_i$. Concurrently, $\mathbf{R}$ opens $\Gamma_{\mathbf{R}} \equiv \sum_{i=1}^{\mathfrak{R}} m_{i,12}$.

(II.3.) All the parties locally compute $f = \Gamma_{\mathbf{R}} + \sum_{k=1}^{N} \Gamma_k$.

It should be noted that by parallelization, Stage II can be performed using just two rounds of simultaneous communication between the parties. Indeed, each $\mathbf{P}_k$ needs to broadcast at most two public messages, the first being no more than $\log \mathfrak{R}_1$ bits, and the second being just one bit. When run in parallel, all the step (II.1) messages can be broadcast concurrently, and likewise for the step (II.2) messages. Moreover, this classical communication can be done after all quantum measurements are performed since the choice of local measurement at each step in $\mathcal{P}$ does not depend on the classical message of any other party. Experimentally, this is very desirable since it means that $\mathcal{P}$ can be implemented in three parts: (i) entanglement distribution (offline phase), (ii) local measurement of qubits (online phase Stage I), and (iii) classical post-processing (online phase Stage II). Without the use of quantum memory, it is not possible to cleanly separate parts (i) and (ii), and in practice, each state $|G_i\rangle$ can be measured in a streaming manner. This type of implementation does not affect the performance or security of the protocol.

Two-party computation with graph states: security

We now turn to analyze the security of $\mathcal{P}$. At a high level, our security claim is that if $\mathbf{R}$ plays honestly, then $\mathcal{P}$ reveals no more information about $\widetilde{\mathbf{x}}_k$ of an honest party $\mathbf{P}_k$, beyond what can be inferred from the function values $f(\widetilde{\mathbf{x}}_1, \cdots, \widetilde{\mathbf{x}}_N)$. Here, an honest party is anyone who executes the steps of $\mathcal{P}$ faithfully. Our protocol also offers some security against a cheating $\mathbf{R}$. Namely, if all N parties follow $\mathcal{P}$ honestly, then $\mathbf{R}$ is also unable to infer any information about the inputs beyond what can be computed from $f(\widetilde{\mathbf{x}}_1, \cdots, \widetilde{\mathbf{x}}_N)$.

Note that for N parties $\mathbf{P}_1, \cdots, \mathbf{P}_N$, these claims allow for the possibility that any subset of $N - 1$ parties is colluding against a single party. The colluding parties are allowed to share an unlimited amount of classical and quantum communication over side channels, and they can thus collectively be viewed as a single party $\mathbf{S}$. In this case, the task essentially reduces to a problem between the two parties $\mathbf{P}$ and $\mathbf{S}$, and $\mathbf{R}$. We let $\widetilde{\mathbf{x}}$ denote the input of $\mathbf{P}$ and $\widetilde{\mathbf{y}}$ as the total input of all the colluding parties constituting $\mathbf{S}$. The goal, then, is to securely compute $f(\widetilde{\mathbf{x}}, \widetilde{\mathbf{y}})$ with an *honest majority* in $\{\mathbf{P}, \mathbf{S}, \mathbf{R}\}$.

In this work, we adopt a simulation-based notion of security. Consider first an ideal world in which there exists some device f_{ideal} that privately receives inputs $\widetilde{\mathbf{x}}$ and $\widetilde{\mathbf{y}}$ from $\mathbf{P}$ and $\mathbf{S}$, respectively, and then outputs $f(\widetilde{\mathbf{x}}, \widetilde{\mathbf{y}})$ to $\mathbf{P}$, $\mathbf{S}$, and $\mathbf{R}$. Intuitively, we want the ideal world to reveal at least as much information about the inputs $(\widetilde{\mathbf{x}}, \widetilde{\mathbf{y}})$ than what is revealed to any dishonest party acting maliciously in the real world.

This intuition is made precise through the notion of a simulator. A simulator, $\mathbb{S}$, in this setting is some device that can take the place of a party $\mathbf{X} \in \{\mathbf{P}, \mathbf{S}, \mathbf{R}\}$ and interact with the ideal functionality f_{ideal} from the viewpoint of party $\mathbf{X}$. Consider now any action taken by a potentially dishonest party in $\mathcal{P}$. Our security definition is that there must exist a simulator $\mathbb{S}$ interacting with f_{ideal} that exactly reproduces what the dishonest party obtains from $\mathcal{P}$. This operationally captures the idea that the adversary learns no more information about an honest party's input, other than what can be inferred directly from an ideal evaluation of f. Figure 4 depicts the two forms of malicious attacks for which we prove that $\mathcal{P}$ is secure. A formal theorem for security is given in the "Methods" section, and a full proof is provided in Supplementary Note 2.

Two-party computation with graph states: performance

To handle experimental errors in the above protocol, we can employ a simple repetition code to suppress the effects of any infidelity in our ability to make each copy of $|G\rangle$ in the offline phase of $\mathcal{P}$. By determining the total bit error probability associated with each share of $a_i b_i$, an arbitrarily small total bit error probability ϵ_f on the output f can be chosen to set the number of repetitions required for Stage I. We use this information to estimate the lower bound rate of computation at which N parties can compute f on their M-bit inputs.

Functionally, our protocol allows for the secure implementation of any two-party Boolean function, f, by repeatedly generating and distributing copies of the 12-qubit state $|G\rangle$. The number of required copies depends (polynomially) on the size of the input, M, and the desired final error probability, ϵ_f. A pair of auxiliary spins can be employed to generate each copy constructed in parallel, and additional emitters can be employed to speed up the construction. Furthermore, these spins need only remain coherent for at most the time to make each copy of $|G\rangle$, a requirement easily met with current trapped ion or atom array systems. We can conservatively estimate the maximum possible bit error probability associated with each copy by computing the complement of the probability that no bit error occurs, that is, the complement of the fidelity to produce an ideal copy of $|G\rangle$ in our proposed emit-then-add scheme. In Fig. 5, we plot the lower bound rate of computation at which our protocol can operate with this form of error correction, in units of R_{rep}, against the size of each party's input, M, for total acceptable error probabilities $\epsilon_f \in \{10^{-3}, 10^{-12}\}$. This rate is given in the "Methods" section. We assume that M here is the number of bits each party needs to perform a conjunction on, neglecting the single linear bit they each input as well.

Discussion

We have introduced a new paradigm for the generation of photonic graph states using coherent quantum emitters, using an emit-then-add approach. This enables the generation of such states without requiring near unity generation, collection, and detection efficiency of the photons. Many state-of-the-art quantum emitter platforms display excellent performance in the other required metrics, including coherence time, gate fidelity, and MCMR fidelity, but exhibit poor ($\lesssim 10\%$) overall photon emission and detection probability due to fundamental challenges. Our scheme is thus much better suited to current and near-term hardware than other deterministic schemes in the literature that rely on the detection of all emitted photons. It is a toolbox for making large entangled photonic states for MBQC and other applications that are limited by spin decoherence rather than photon collection efficiency. We demonstrated this advantage in scaling and introduced an application of our scheme for secure two-party computation. The

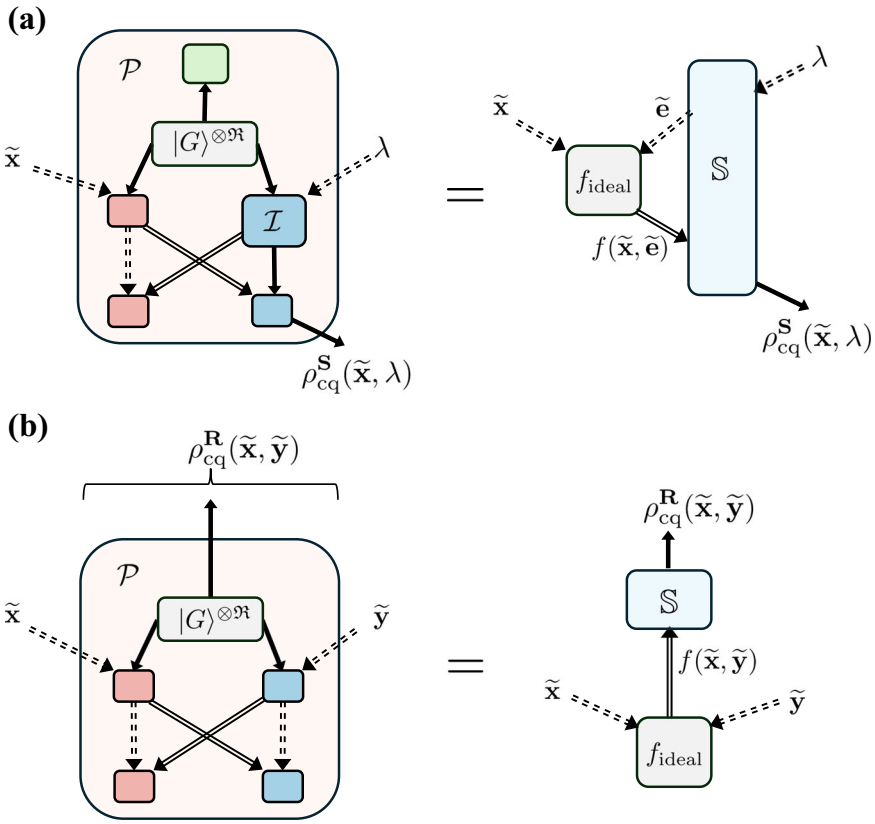

Fig. 4 | Malicious attacks on $\mathcal{P}$ by S and R. Real (left) vs. ideal (right) instantiations of the attacks are depicted, where boxes (red, blue, green) indicate local processing by a given party (**P**, **S**, **R**). **a** General attack by **S**. The attack is described by a quantum instrument $\mathcal{I}$ that acts on the qubits of $|G\rangle^{\otimes\mathfrak{R}}$ distributed to **S**, with possible dependence on some side information λ. For every $\widetilde{\mathbf{x}}$ of **P**, the attack will generate for **S** a classical-quantum state $\rho^{\mathbf{S}}_{\mathrm{cq}}(\widetilde{\mathbf{x}},\lambda)$ that depends on all public communication in the protocol. We show there exists a simulator $\mathbb{S}$ in place of party **S** in the ideal world that submits some input $\widetilde{\mathbf{e}}$ to f_{ideal} and then uses the output $f(\widetilde{\mathbf{x}},\widetilde{\mathbf{e}})$ to generate the same $\rho^{\mathbf{S}}_{\mathrm{cq}}(\widetilde{\mathbf{x}},\lambda)$ achieved in the real world. **b** General attack by **R**. We again show there exists a simulator $\mathbb{S}$ that takes the place of **R** in the ideal world, receiving just the function output $f(\widetilde{\mathbf{x}},\widetilde{\mathbf{y}})$ and outputting the classical-quantum state $\rho^{\mathbf{R}}_{\mathrm{cq}}(\widetilde{\mathbf{x}},\widetilde{\mathbf{y}})$ achieved in the real world, as shown to the right.

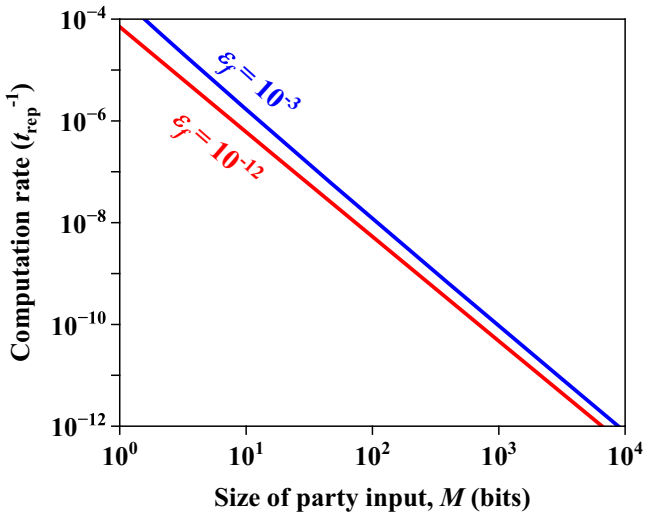

Fig. 5 | Error corrected two-party computation rate versus the number of required conjunctions in f, shown for two acceptable error probabilities on the computation (ϵ_f). We assume the use the our scheme with destructive measurements and no photonic memory. The rate is expressed in units of the repetition rate of excitation of the chosen quantum emitter, t_{rep}^{-1}, which can be in the range of 10^6–$10^9 s^{-1}$ for highly coherent emitters. The individual bit error probability for each copy of $|G\rangle$ is a pessimistic 0.157, assuming $\eta_e = 0.1$, and $F_{\mathrm{add}} = 0.99$. We see that even these parameters allow virtually unlimited reduction in the total error probability with minimal change in the overall rate.

lack of interaction in the measurement-based stage of this protocol, along with the minimal overhead for constructing each resource state, makes this an ideal use case for virtual graph states constructed with emit-then-add.

Furthermore, the scheme introduced here naturally lends itself to various extensions and modifications to increase functionality. First, adding multiplexing, such as between many arrays of atoms or ions, would increase the generation rate with a linear factor in the degree of multiplexing. Other hybrid approaches that combine the virtual graph states discussed here with more traditional graph states can add additional functionality. Further theoretical work remains to be done to determine more applications that are suited to this scheme.

Methods

Graph states

For an arbitrary graph $G = (V, E)$ with vertices $V = \{a_1, \cdots, a_n\}$ and edge set $E \subset V \times V$, consider the n-qubit operator obtained by performing a controlled $-Z$ gate, $CZ_{a,b}$, between every $(a, b) \in E$. We denote this global operator by

$$U_G = \prod_{(a,b)\in E} CZ_{a,b}. \tag{10}$$

The graph state associated with the graph G is the n-qubit state

$$|G\rangle = U_G|+\rangle^{\otimes V}. \tag{11}$$

Note that $|+\rangle^{\otimes n}$ is stabilized by n commuting operators $\{X_a\}_{a\in V}$. Hence, the stabilizer of $|G\rangle$ can be understood by examining how the X_a transform under U_G. Since $CZ_{a,b}(X_a)CZ_{a,b} = X_aZ_b$, it follows that the stabilizer of $|G\rangle$ is generated by the operators $\langle\{K_a\}_{a\in V}\rangle$, where

$$\begin{aligned} K_a &= U_G X_a U_G \\ &= X_a \prod_{b\in N_a} Z_b \\ &= X_a \prod_{b\in V} Z_b^{\Gamma_{a,b}} \ \forall a \in V, \end{aligned} \tag{12}$$

and $\Gamma_{a,b}$ are elements of the adjacency matrix of G.

When discussing the construction of graph states, a *local complementation* describes an important involution on a graph, which can be

accomplished efficiently in practice through only single-qubit rotations. We define $\tau_a(G)$ as the graph $(V, E\Delta E(N_a, N_a))$, where Δ is the symmetric difference and $E(N_a, N_a) = \{\{b, b'\} | b, b' \in N_a, b \neq b'\}$, such that

$$|\tau_a(G)\rangle = (-iX_a)^{1/2}\Big(\prod_{b\in N_a}(iZ_b)^{1/2}\Big)|G\rangle, \tag{13}$$

We will refer to this equation in the next section when discussing the additional overhead associated with emit-then-add.

Additional overhead in emit-then-add

Building graph states with our emit-then-add scheme necessitates additional experimental overhead from typical deterministic quantum emitter-based schemes, in both the number of qubits required and entangling operations between them. We demonstrate through an inductive argument that these additional resource costs scale at worst linearly. In what follows, a superscript (p), (s), or (e) denotes the kind of physical qubit associated with the relevant subspace on which an operator acts, as a photon, auxiliary spin, or emitter, respectively.

Let $|G\rangle$ define an existing graph state in which there is at least a single edge between an auxiliary spin and the set of photons previously added to the graph. We label each of these photons by an emission order $1, \cdots, m-1$.

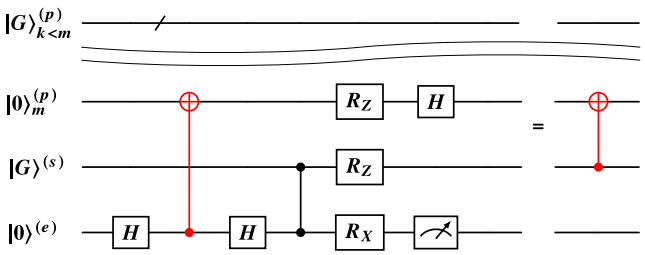

Fig. 6 | A subcircuit equivalent to a $CX_{s,p}$ gate, up to a conditional phase correction, for transferring entanglement in our proposed scheme. This example "emit-then-add" step replaces every pumping gate in typical deterministic schemes for generating arbitrary photonic graph states. Entanglement between a photon (p) and a coherently pumped emitter (e) (represented by a red $CX_{e,p}$ gate) is exchanged to an auxiliary spin (s) via a two-qubit entangling $CZ_{e,s}$ gate and local complementation. The emitter is measured out thereafter and reinitialized for the next iteration of the procedure. Rotations about X and Z are by $\pi/2$ and $-\pi/2$, respectively, as noted in Eq. (13). The measurement of the emitter is with respect to the Z basis. All previously added photons at iterations $k < m$ are unaffected.

Let V_m define the additional vector space describing the emitter and the next photon, m, to be added to the graph, both of which start in $|0\rangle$. The set of generators which stabilizes the collective vector space $V_G + V_m$, consisting of the graph and subsequent emitter-photon pair, has the form

$$S_{V_G+V_m} = \langle \cdots, \cdots Z_k^{(p)} \cdots X^{(s)}, Z^{(e)}, Z_m^{(p)} \rangle, \tag{14}$$

where $\cdots$ denotes other generators and the notation $\cdots Z_k^{(p)} \cdots$ is used to keep track of an arbitrary edge between the auxiliary spin and a photon previously added to the graph at some emission step $k < m$. The subcircuit depicted in Fig. 6 demonstrates an example of how to transfer entanglement (or conditional phase information) from the emitter-photon subsystem to $|G\rangle$, with a single two-qubit spin-spin entangling gate and local complementation. In implementing the example, we transform the stabilizer of the combined vector space in Eq. (14) as

$$S'_{V_G+V_m} = \langle \cdots, (-1)^{c_m} \cdots Z_k^{(p)} \cdots X_m^{(p)} X^{(s)}, (-1)^{c_m} Z_m^{(p)} Z^{(s)}, (-1)^{c_m} Z^{(e)} \rangle, \tag{15}$$

where $c_m \in \{0, 1\}$ is a classical bit value conditioned on the measurement of the emitter.

The result of these operations produces the same stabilizer we would have arrived at had we instead pumped the auxiliary spin itself. With these additional operations, any graph state accessible in the deterministic scheme can be constructed with emit-then-add. As we restrict those auxiliary spins already entangled with any previously added photons from being pumped, it follows that one additional spin, the emitter, and one two-qubit spin-spin entangling gate per photon in G are the minimum additional overhead in our proposed schemes for making arbitrary graph states. Furthermore, we can define a new vector space $V_{G'}$, containing the existing graph state and a newly entangled photon, with a dimension that increases by one with each new photon. The new space $V_{G'}$ is stabilized by a unique set of generators that can be rotated back to a graph state basis of the same general form as Eq. (14), now defined by a new graph state $|G'\rangle$.

Construction subroutines

We also offer a pair of subroutines that simplify the construction and overhead for the graph state $|G\rangle$, employed in our MPC protocol $\mathcal{P}$. Representations of the graph transformations associated with the two subroutines, along with example circuits, are depicted in Figs. 7 and 8. These transformations can be performed successively with no additional operations, transforming the previous graph G built on the auxiliary spin

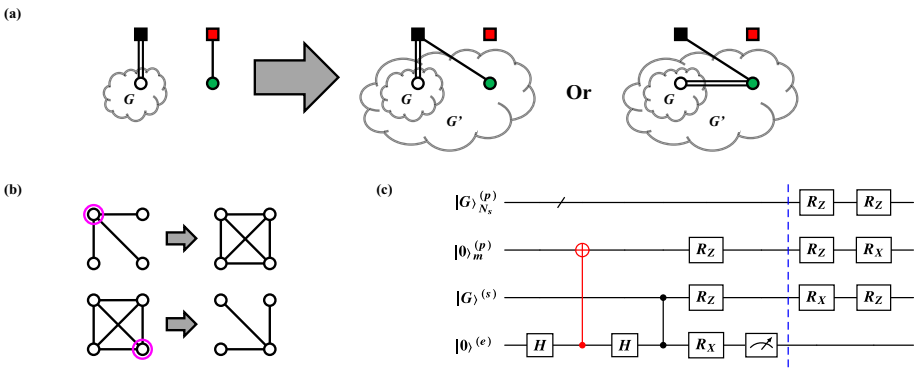

Fig. 7 | Passing-subroutine for adding new photons to an existing graph, G. a A graph transformation of passing a new photon (green) from the emitter (red) to an auxiliary spin (black), which is connected to one or more previously added photons (white, denoted with a double edge for the multiplicity). This subroutine consists of two variations: (left) leaving all previously added photons invariant, (right) transplanting those edges to the newly added photon. **b** An example of how local complementations on a target qubit (magenta circle) can be used to add or remove edges. **c** A quantum subcircuit which implements the graph transformation. The right variation of the graph transformation above is achieved with the additional two local complementations (blue dashed line, depicting the deviation). Rotations and measurements follow the same notation as in Fig. 6.

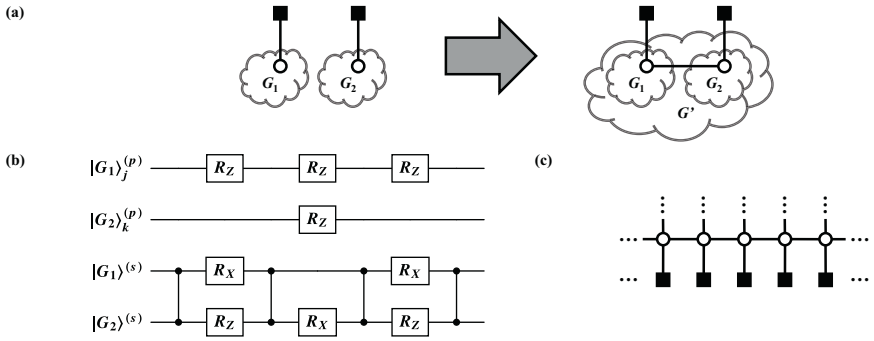

Fig. 8 | Patching-subroutine for attaching two subgraphs G_1 and G_2 by a common edge between photons. a The graph transformation depicting the patching. **b** The corresponding circuit diagram. An additional two-qubit spin-spin entangling gates are required for this subroutine, over the passing-subroutine. Rotations follow the same notation as in Fig. 6. **c** A 2D cluster state built on an array of auxiliary spins. Edges can be generated between photons in the layer neighboring the array of spins with this patching.

to a new graph G' with any new photons sharing an edge to the auxiliary spin. Despite their intended application in our MPC, we make no assumptions about the measurement of the photons in these subroutines, such that they can be applied generally across experimental implementations.

One "passing"-subroutine, shown in Fig. 7, consists of two variations: "join" and "extend". The join-subroutine adds a new photon to an existing graph and leaves all previously existing edges invariant. The extend-subroutine transfers all edges from the auxiliary spin to the new photon. The two are achieved without or with the additional two local complementations depicted at the end of the example circuit, respectively. Both variations only act on previously added photons in the neighborhood of the auxiliary spin, N_s. Repeatedly applying the join-subroutine or extend-subroutine on a single auxiliary spin produces a star graph or linear cluster state, respectively, for each variation. Additionally, either variation of this subroutine can be appropriately implemented between auxiliary spins to connect subgraphs.

We note briefly that in practice with each implementation of the passing-subroutine, the newly added photon to the graph and the auxiliary spin each carry a conditional phase that is a byproduct of the decoupling measurement made on the emitter, as shown in Eq. (15). This byproduct phase determines the precise basis state of the graph and may require correction for general MBQCs. In the implementation of our scheme without photonic memory, photons are measured before they are decoupled from the emitter, and hence, any requisite phase corrections need to be commuted after each measurement. The Clifford nature of the measurements employed in our MPC simplifies all of these corrections to bit flips that can be handled classically. Furthermore, correction of this phase is not always necessary, as certain measurements made by the parties destroy this phase information, while other measurements allow the parties to absorb this phase information into their own pad. Conversely, conditional measurements, such as the ones made by Alice in step (I.4) of Stage I of $\mathcal{P}$, couple these byproduct phases to the phase information input into the computation. Therefore, classical communication is required here between Alice and the Source. A simple solution is for the Source to make public the outcomes of each of these decoupling measurements.

The other "patching"-subroutine, shown in Fig. 8, serves to attach two subgraphs G_1 and G_2 by a common edge between photons. This process requires an additional two-qubit spin-spin entangling gate from the passing-subroutine. For further simplicity, we only consider the case where G_1 and G_2 each have a single edge to all previously added photons in their respective subgraphs, though in general, this subroutine fully connects all of the photons at the first layer in each subgraph. Operations in this subroutine are restricted locally to only the emitter, spin, and the photons we ultimately require to share an edge, labeled in the figure by arbitrary emission steps j, k in $1, \cdots, n_p$. This subroutine mirrors the one employed in the production of large 2D cluster states in ref. 6, and can be applied in either scheme we propose for the same purpose.

Application of these subroutines to the construction of the graph state discussed in Results is straightforward. The state $|G\rangle$, consisting of $n_p = 12$ photons, labeled by an emission ordering depicted in Fig. 3, can be built following the sequence of steps in the Build below. This procedure requires 17 two-qubit spin-spin entangling gates in total: 13 from passing operations, and 4 from a single patching step. It is known that the sequential nature of photon emission events imparts an ordering on the graph state, limiting the kinds of photonic graphs accessible by construction on a single quantum emitter[64]. As $\mathcal{P}$ involves conditioning measurement bases on previous outcomes (steps (I.5) and (I.6)), this sets a nontrivial emission ordering on $|G\rangle$, which, following the results of ref. 23, requires at least two auxiliary spins to construct.

Build$|G\rangle$:. *Input:* A photon emission order labeling photons $(p_1), \cdots, (p_{12})$, corresponding to the $n_p = 12$ photons in $|G\rangle$, an emitting spin, and two auxiliary spins, labeled (s_1) and (s_2).

1. Pass photons (p_1) through (p_4) to (s_1). Apply the join-subroutine for (p_4) and the extend-subroutine for the rest.
2. Pass photons (p_5) through (p_8) to (s_2). Apply the join-subroutine for (p_5) and the extend-subroutine for the rest.
3. Pass the subgraph on (s_2) to (s_1) with the join-subroutine.
4. Pass photons (p_9) through (p_{12}) to (s_2). Apply the join-subroutine for (p_9) and the extend-subroutine for the rest.
5. Patch the subgraph on (s_2) with (s_1). Measure out both (s_1) and (s_2).

Graph state construction fidelity

In modeling infidelity from decoherence, we consider two spin states of an emitter and auxiliary spin and some dephasing map that introduces a Pauli Z error on the respective qubit (while neglecting spin-lattice relaxation). That is, we consider the following transformation of the density matrix for the emitter or auxiliary spin,

$$\widehat{\rho} \to \frac{1}{2}(1 + e^{-t/\tau})\widehat{\rho} + \frac{1}{2}(1 - e^{-t/\tau})Z\widehat{\rho}Z, \tag{16}$$

where τ is the coherence time of the emitter or auxiliary spin and t is a timescale for the dephasing process. $\widehat{\rho}$ remains invariant with probability $\frac{1}{2}(1 + e^{-t/\tau})$. In arriving at Eqs. (1) and (2), $t = t_{\text{rep}} + t_{\text{add}}$ for the emitter, where we assume an emitter dephases at most for a time $t_{\text{rep}} + t_{\text{add}}$ for every photon added before the emitter is disentangled from the graph and reset, and $\langle t \rangle = t_{\text{rep}}/\eta_e + t_{\text{add}}$ for the auxiliary spin for a single iteration, with n_p iterations. F_{add} in our model includes the effects of additional gate infidelities. See Supplementary Note 1 for additional details.

Utilizing the build discussed above for the resource state $|G\rangle$ in Fig. 3, we utilize these estimates of fidelity in Fig. 5 to determine a bit error rate on each round of our protocol $\mathcal{P}$. There, we neglect the effect of dephasing, in assuming $t_{\text{rep}} \ll \tau$, and let $F_{\text{add}} = F_{CZ}$ for simplicity. Hence, we take

$F = (F_{\text{add}})^{17}$, incorporating the additional spin-spin entangling gates utilized in the build of $|G\rangle$.

Graph state construction scaling

The construction time shown in Fig. 2 can be modeled by considering a series of Bernoulli trials that describe the success or failure of detecting a photon, with $P = \eta_e$ being the probability of a success. As protocols using deterministic schemes require a restart upon a failure to detect a photon, the expected value in the total time to successfully detect n_p *consecutive* photons is $t_{\text{rep}}(P^{-n_p} - 1)/(1 - P)$. In contrast, our emit-then-add scheme requires no restart, as a photon is added to the graph only after it is heralded. Thus, the expected total time for emit-then-add is instead $(t_{\text{rep}}/P + t_{\text{add}})n_p$ (we neglect t_{add} in our simulation). The scaling of the generalized scheme involving entanglement swapping is discussed in Supplementary Note 1.

Security theorem for $\mathcal{P}$

We return to the security of our protocol $\mathcal{P}$, introduced in Results, and give a formal theorem. In this paper, we address two forms of malicious attacks, depicted in Fig. 4, where we assume without loss of generality that **P** is the party playing honestly. To clarify further, first consider when **S** potentially deviates from the protocol. The most general physical action can be formally described by a quantum instrument $\mathcal{I}$ that might depend on some classical side information λ[61]. For every $\tilde{\mathbf{x}}$ of **P**, the instrument will generate for **S** a classical-quantum (cq) state $\rho^{\mathbf{S}}_{\text{cq}}(\tilde{\mathbf{x}}, \lambda)$, which contains all of **S**'s quantum registers along with classical registers recording all of the public communication ($\mathbf{c}_{\text{tot}}$, $\Gamma_{\mathbf{P}}$, $\Gamma_{\mathbf{S}}$, $\Gamma_{\mathbf{R}}$). To maintain consistency with the protocol, we assume **S** still broadcasts some classical message when called for in the honest protocol, although this message can be generated in an arbitrary way. On the other hand, consider a case when **R** deviates from the instruction of $\mathcal{P}$. Whenever **P** and **S** follow the protocol honestly on any pair of inputs $(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$, they will generate for **R** the cq state $\rho^{\mathbf{R}}_{\text{cq}}(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$, from which any operation could be performed by **R** to extract information.

Theorem 1. (Security of $\mathcal{P}$) For any two-party function $f(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) = z_{\mathbf{P}} + z_{\mathbf{S}} + \sum_{i=1}^{\mathfrak{N}} a_i b_i$, the protocol $\mathcal{P}$ satisfies the following security conditions.

1. (Correctness.) If all the parties are honest, then for every input $(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$ the output of the ideal protocol can be locally computed from the outputs of $\mathcal{P}$.
$$f(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) = \Gamma_{\mathbf{P}} + \Gamma_{\mathbf{S}} + \Gamma_{\mathbf{R}} \tag{17}$$
2. (Secure if only **S** cheats.) Suppose **P** and **R** follow $\mathcal{P}$ honestly, but **S** potentially deviates. Let $\rho^{\mathbf{S}}_{\text{cq}}(\tilde{\mathbf{x}}, \lambda)$ denote the total cq state held by **S** at the end of $\mathcal{P}$, given input $\tilde{\mathbf{x}}$ of **P** and side information λ. Then, there exists a simulator $\mathbb{S}$ for **S** interacting with the ideal functionality f_{ideal} that exactly reproduces $\rho^{\mathbf{S}}_{\text{cq}}(\tilde{\mathbf{x}}, \lambda)$ for all $\tilde{\mathbf{x}}$ and λ.
3. (Secure if only **R** cheats.) Suppose **P** and **S** follow $\mathcal{P}$ honestly, but **R** potentially deviates. Let $\rho^{\mathbf{R}}_{\text{cq}}(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$ denote the total cq state held by **R** at the end of $\mathcal{P}$, given inputs $(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$ of **P** and **S**, respectively. Then, there exists a simulator $\mathbb{S}$ for **R** interacting with the ideal functionality f_{ideal} that exactly reproduces $\rho^{\mathbf{R}}_{\text{cq}}(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$ for all $(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$.

Further details and a formal proof are given in Supplementary Note 2.

Including error correction in $\mathcal{P}$

In practice, each bit conjunction computed in Stage I of $\mathcal{P}$ will have some error. We can utilize a basic method of classical error correction to alleviate these bit errors. Let ϵ_* denote the largest probability of a bit error in each iteration of Stage I, and let ϵ_f denote the desired final bit error probability on the output f of $\mathcal{P}$. Suppose that N parties wish to compute an f on each party's M-bit input, utilizing $\mathcal{P}$. This can be implemented with error correction at a unit rate of R/R_0 lower bounded by

$$\left(6(M-1)^2N^2\left\lceil\frac{\ln\left((M-1)N/\sqrt{2\epsilon_f}\right)}{\left(\frac{1}{2}-\epsilon_*\right)^2}\right\rceil\right)^{-1}, \tag{18}$$

where R_0 is the scheme-dependent average rate to add a new photon to a graph state. For the simpler emit-then-add scheme we propose, employing only destructive photon measurements, $R_0 = \eta_e R_{\text{rep}}$. This rate is plotted in Fig. 5 to depict how benchmarks of the state-of-the-art for highly coherent quantum emitters enable virtually unlimited correction in these bit errors. Further details on Eq. (18) can be found in Supplementary Note 2.

Data availability

No datasets were generated or analyzed during the current study.

Received: 25 April 2025; Accepted: 5 January 2026;
Published online: 15 January 2026

References

1. Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188–5191 (2001).
2. Browne, D. E. & Rudolph, T. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.* **95**, 010501 (2005).
3. Lindner, N. H. & Rudolph, T. Proposal for pulsed on-demand sources of photonic cluster state strings. *Phys. Rev. Lett.* **103**, 113602 (2009).
4. Economou, S. E., Lindner, N. & Rudolph, T. Optically generated 2-dimensional photonic cluster state from coupled quantum dots. *Phys. Rev. Lett.* **105**, 093601 (2010).
5. Buterakos, D., Barnes, E. & Economou, S. E. Deterministic generation of all-photonic quantum repeaters from solid-state emitters. *Phys. Rev. X* **7**, 041023 (2017).
6. Russo, A., Barnes, E. & Economou, S. E. Generation of arbitrary all-photonic graph states from quantum emitters. *N. J. Phys.* **21**, 055002 (2019).
7. Hilaire, P., Vidro, L., Eisenberg, H. S. & Economou, S. E. Near-deterministic hybrid generation of arbitrary photonic graph states using a single quantum emitter and linear optics. *Quantum* **7**, 992 (2023).
8. Meng, Y. et al. Temporal fusion of entangled resource states from a quantum emitter. *Nat. Commun.* **16**, 7602 (2025).
9. Thomas, P., Ruscio, L., Morin, O. & Rempe, G. Fusion of deterministically generated photonic graph states. *Nature* **629**, 567–572 (2024).
10. Wein, S. C. et al. Minimizing resource overhead in fusion-based quantum computation using hybrid spin-photon devices. *PRX Quantum* **6**, 040362 (2025).
11. Chan, M. L. et al. Tailoring fusion-based photonic quantum computing schemes to quantum emitters. *PRX Quantum* **6**, 020304 (2025).
12. Zhan, Y. & Sun, S. Deterministic generation of loss-tolerant photonic cluster states with a single quantum emitter. *Phys. Rev. Lett.* **125**, 223601 (2020).
13. Schwartz, I. et al. Deterministic generation of a cluster state of entangled photons. *Science* **354**, 434–437 (2016).
14. Schupp, J. et al. Interface between trapped-ion qubits and traveling photons with close-to-optimal efficiency. *PRX Quantum* **2**, 020331 (2021).
15. Thomas, P., Ruscio, L., Morin, O. & Rempe, G. Efficient generation of entangled multiphoton graph states from a single atom. *Nature* **608**, 677–681 (2022).
16. Cogan, D., Su, Z.-E., Kenneth, O. & Gershoni, D. Deterministic generation of indistinguishable photons in a cluster state. *Nat. Photonics* **17**, 324–329 (2023).
17. Varnava, M., Browne, D. E. & Rudolph, T. Loss tolerance in one-way quantum computation via counterfactual error correction. *Phys. Rev. Lett.* https://doi.org/10.1103/PhysRevLett.97.120501 (2006).
18. Morimae, T. & Fujii, K. Blind topological measurement-based quantum computation. *Nat. Commun.* https://doi.org/10.1038/ncomms2043 (2012).
19. Morley-Short, S. et al. Physical-depth architectural requirements for generating universal photonic cluster states. *Quantum Sci. Technol.* **3**, 015005 (2017).

20. Pant, M., Towsley, D., Englund, D. & Guha, S. Percolation thresholds for photonic quantum computing. *Nat. Commun.* **10**, 1070 (2019).
21. Bartolucci, S. et al. Fusion-based quantum computation. *Nat. Commun.* https://doi.org/10.1038/s41467-023-36493-1 (2023).
22. Löbl, M. C., Paesani, S. & Sørensen, A. S. Loss-tolerant architecture for quantum computing with quantum emitters. *Quantum* **8**, 1302 (2024).
23. Li, B., Economou, S. E. & Barnes, E. Photonic resource state generation from a minimal number of quantum emitters. *npj Quantum Inf.* https://doi.org/10.1038/s41534-022-00522-6 (2022).
24. Munro, W. J., Nemoto, K., Beausoleil, R. G. & Spiller, T. P. High-efficiency quantum-nondemolition single-photon-number-resolving detector. *Phys. Rev. A* **71**, 033819 (2005).
25. Xiao, Y.-F. et al. Quantum nondemolition measurement of photon number via optical Kerr effect in an ultra-high-Q microtoroid cavity. *Opt. Express* **16**, 21462–21475 (2008).
26. Yanagimoto, R. et al. Quantum nondemolition measurements with optical parametric amplifiers for ultrafast universal quantum information processing. *PRX Quantum* **4**, 010333 (2023).
27. Bock, M. et al. High-fidelity entanglement between a trapped ion and a telecom photon via quantum frequency conversion. *Nat. Commun.* **9**, 1–7 (2018).
28. Economou, S. E., Sham, L. J., Wu, Y. & Steel, D. G. Proposal for optical U(1) rotations of electron spin trapped in a quantum dot. *Phys. Rev. B* **74**, 205415 (2006).
29. Gimeno-Segovia, M., Rudolph, T. & Economou, S. E. Deterministic generation of large-scale entangled photonic cluster state from interacting solid state emitters. *Phys. Rev. Lett.* **123**, 070501 (2019).
30. Rieländer, D., Lenhard, A., Mazzera, M. & De Riedmatten, H. Cavity enhanced telecom heralded single photons for spin-wave solid state quantum memories. *N. J. Phys.* **18**, 123013 (2016).
31. Covey, J. P., Weinfurter, H. & Bernien, H. Quantum networks with neutral atom processing nodes. *npj Quantum Inf.* https://doi.org/10.1038/s41534-023-00759-9 (2023).
32. Ward, T. & Keller, M. Generation of time-bin-encoded photons in an ion-cavity system. *N. J. Phys.* **24**, 123028 (2022).
33. Krutyanskiy, V. et al. Entanglement of trapped-ion qubits separated by 230 meters. *Phys. Rev. Lett.* **130**, 050803 (2023).
34. Jayakumar, H. et al. Time-bin entangled photons from a quantum dot. *Nat. Commun.* https://doi.org/10.1038/ncomms5251 (2014).
35. Senellart, P., Solomon, G. & White, A. High-performance semiconductor quantum-dot single-photon sources. *Nat. Nanotechnol.* **12**, 1026–1039 (2017).
36. Anand, S. et al. A dual-species Rydberg array. *Nat. Phys.* **20**, 1–7 (2024).
37. Bruzewicz, C., McConnell, R., Stuart, J., Sage, J. & Chiaverini, J. Dual-species, multi-qubit logic primitives for Ca^+/Sr^+ trapped-ion crystals. *npj Quantum Inf.* **5**, 102 (2019).
38. Bradley, C. E. et al. A ten-qubit solid-state spin register with quantum memory up to one minute. *Phys. Rev. X* **9**, 031045 (2019).
39. Schneeloch, J. et al. Introduction to the absolute brightness and number statistics in spontaneous parametric down-conversion. *J. Opt.* **21**, 043501 (2019).
40. Zhang, C., Huang, Y.-F., Liu, B.-H., Li, C.-F. & Guo, G.-C. Spontaneous parametric down-conversion sources for multiphoton experiments. *Adv. Quantum Technol.* **4**, 2000132 (2021).
41. Pan, J.-W., Bouwmeester, D., Weinfurter, H. & Zeilinger, A. Experimental entanglement swapping: entangling photons that never interacted. *Phys. Rev. Lett.* **80**, 3891 (1998).
42. Houshmand, M., Houshmand, M. & Fitzsimons, J. F. Minimal qubit resources for the realization of measurement-based quantum computation. *Phys. Rev. A* **98**, 012318 (2018).
43. Raussendorf, R., Browne, D. E. & Briegel, H. J. Measurement-based quantum computation on cluster states. *Phys. Rev. A* **68**, 022312 (2003).
44. Browne, D. E., Kashefi, E., Mhalla, M. & Perdrix, S. Generalized flow and determinism in measurement-based quantum computation. *N. J. Phys.* **9**, 250–250 (2007).
45. Bluvstein, D. et al. A quantum processor based on coherent transport of entangled atom arrays. *Nature* **604**, 451–456 (2022).
46. Wang, P. et al. Single ion qubit with estimated coherence time exceeding one hour. *Nat. Commun.* **12**, 1–8 (2021).
47. Evered, S. J. et al. High-fidelity parallel entangling gates on a neutral-atom quantum computer. *Nature* **622**, 268–272 (2023).
48. Srinivas, R. et al. High-fidelity laser-free universal control of trapped ion qubits. *Nature* **597**, 209–213 (2021).
49. Clark, C. R. et al. High-fidelity Bell-state preparation with $^{40}Ca^+$ optical qubits. *Phys. Rev. Lett.* https://doi.org/10.1103/PhysRevLett.127.130505 (2021).
50. Gaebler, J. P. et al. Suppression of midcircuit measurement crosstalk errors with micromotion. *Phys. Rev. A* https://doi.org/10.1103/PhysRevA.104.062440 (2021).
51. Norcia, M. A. et al. Midcircuit qubit measurement and rearrangement in a ^{171}Yb atomic array. *Phys. Rev. X* **13**, 041034 (2023).
52. Yao, A. C. Protocols for secure computations. In *Proc. 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82 160–164 (IEEE Computer Society, USA, 1982).
53. Goldreich, O., Micali, S. & Wigderson, A. How to play any mental game. In *Proc. Nineteenth annual ACM Conference on Theory of Computing - STOC '87*, STOC '87 218–229 (ACM Press, New York, 1987).
54. Zhao, C. et al. Secure multi-party computation: theory, practice and applications. *Inf. Sci.* **476**, 357–372 (2019).
55. Beaver, D. Efficient multiparty protocols using circuit randomization. In *Advances in Cryptology — CRYPTO '91* (ed. Feigenbaum, J.) 420–432 (Springer, Berlin, 1992).
56. Nielsen, J. B., Nordholt, P. S., Orlandi, C. & Burra, S. S. A new approach to practical active-secure two-party computation. In *Advances in Cryptology – CRYPTO 2012* (eds Safavi-Naini, R. & Canetti, R.) 681–700 (Springer, Berlin, 2012).
57. Damgård, I., Pastro, V., Smart, N. & Zakarias, S. Multiparty computation from somewhat homomorphic encryption. In *Advances in Cryptology – CRYPTO 2012* (eds Safavi-Naini, R. & Canetti, R.) 643–662 (Springer, Berlin, 2012).
58. Choudhury, A. & Patra, A. An efficient framework for unconditionally secure multiparty computation. *IEEE Trans. Inf. Theory* **63**, 428–468 (2017).
59. Takeuchi, Y., Mantri, A., Morimae, T., Mizutani, A. & Fitzsimons, J. Resource-efficient verification of quantum computing using Serfling's bound. *npj Quantum Inf.* https://doi.org/10.1038/s41534-019-0142-2 (2019).
60. Unnikrishnan, A. & Markham, D. Verification of graph states in an untrusted network. *Phys. Rev. A* **105**, 052420 (2022).
61. Davies, E. B. & Lewis, J. T. An operational approach to quantum probability. *Commun. Math. Phys.* **17**, 239–260 (1970).
62. Dov Gordon, S., Liu, F.-H. & Shi, E. Constant-round MPC with fairness and guarantee of output delivery. In *Advances in Cryptology – CRYPTO 2015* (eds Gennaro, R. & Robshaw, M.) 63–82 (Springer, Berlin, 2015).
63. Damgård, I., Magri, B., Ravi, D., Siniscalchi, L. & Yakoubov, S. Broadcast-optimal two round MPC with an honest majority. In *Advances in Cryptology – CRYPTO 2021* (eds Malkin, T. & Peikert, C.) 155–184 (Springer International Publishing, Cham, 2021).
64. Schön, C., Solano, E., Verstraete, F., Cirac, J. I. & Wolf, M. M. Sequential generation of entangled multiqubit states. *Phys. Rev. Lett.* https://doi.org/10.1103/PhysRevLett.95.110503 (2005).

Acknowledgements

We acknowledge helpful discussions with Kejie Fang and Vito Scarola. E.C. thanks Christian Schaffner and Ian George for some helpful explanations on multi-party computation and security. This work was supported by the NSF Quantum Leap Challenge Institute on Hybrid Quantum Architectures and Networks (NSF Award No. 2016136).

Author contributions

E.G. and E.C. contributed the central idea behind the experimental scheme proposed in this manuscript. E.C. came up with the two-party computation protocol and proof of security. M.G. and J.L. contributed equally to performing calculations, preparing figures, and generating numerical estimates that appear within the manuscript. All authors contributed to producing the text for the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-026-01181-7.

Correspondence and requests for materials should be addressed to Elizabeth A. Goldschmidt.