# Towards practical secure delegated quantum computing with semi-classical light

Boris Bourdoncle, Pierre-Emmanuel Emeriau, Paul Hilaire, Shane Mansfield, Luka Music, and Stephen Wein

Quandela, 7 Rue Léonard de Vinci, 91300 Massy, France

Secure Delegated Quantum Computation (SDQC) protocols are a vital piece of the future quantum information processing global architecture since they allow end-users to perform their valuable computations on remote quantum servers without fear that a malicious quantum service provider or an eavesdropper might acquire some information about their data or algorithm. They also allow end-users to check that their computation has been performed as they have specified it.

However, existing protocols all have drawbacks that limit their usage in the real world. Most require the client to either operate a single-qubit source or perform single-qubit measurements, thus requiring them to still have some quantum technological capabilities albeit restricted, or require the server to perform operations which are hard to implement on real hardware (e.g isolate single photons from laser pulses and polarisation-preserving photon-number quantum non-demolition measurements). Others remove the need for quantum communications entirely but this comes at a cost in terms of security guarantees and memory overhead on the server's side.

We present an SDQC protocol which drastically reduces the technological requirements of both the client and the server while providing information-theoretic composable security. More precisely, the client only manipulates an attenuated laser pulse, while the server only handles interacting quantum emitters with a structure capable of generating spin-photon entanglement. The quantum emitter acts as both a converter from coherent laser pulses to polarisation-encoded qubits and an entanglement generator. Such devices have recently been used to demonstrate the largest entangled photonic state to date, thus hinting at the readiness of our protocol for experimental implementations.

## 1 Introduction

**Context.** The number of potential use-cases for quantum computing steadily increases, whether in the noisy intermediate-scale quantum regime or using larger machines to perform fault-tolerant computations, with a diverse range of applications from pharmaceutics, material research, finance, to defence.

However, most end-users will likely prefer not to own a quantum computer but still want to leverage its capabilities for their applications. The optimal strategy, therefore,

---

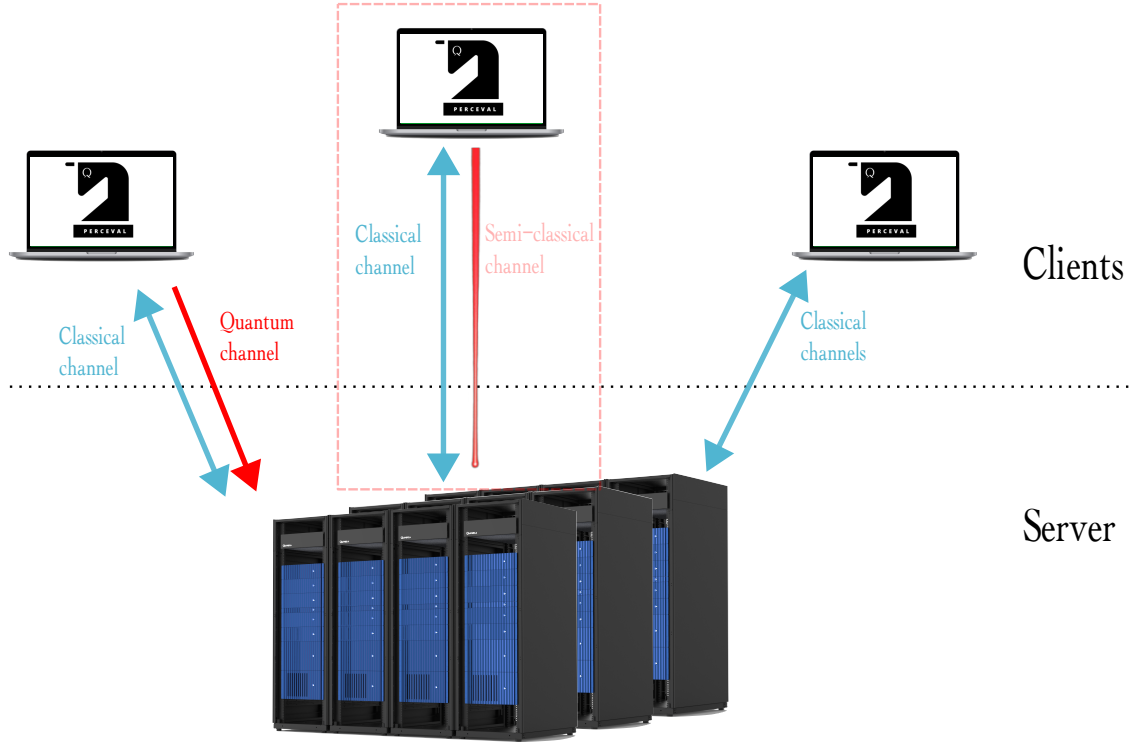Luka Music: Corresponding author, luka.music@quandela.com

Figure 1: Typical client-server configuration where a limited client delegates a quantum computation to a quantum server. Clients might have a limited quantum capability e.g. the ability to send single qubits [left] or entirely classical channels [right]. In this work we focus on a hybrid proposal where clients have a semi-classical channels [centre] meaning that the client is able to send a coherent state.

is to use delegated solutions where quantum computations are performed by a quantum service provider. This approach is actively being developed in both academic and industry settings.[1] This is commonly done via the combination of a code-based interface for describing the computation and classical communications between the client and the server.

Unfortunately, in this scenario there are no information-theoretic guarantees ruling out a malicious provider accessing all information about the client's desired computation, inputs, and outcomes. Cases where such considerations could be critical include (i) the manipulation of highly sensitive input data, such as confidential medical records or defence-related information, (ii) the execution of proprietary (and confidential) algorithms, and (iii) cases where the output is valuable, e.g. patent-worthy. Furthermore, the client cannot check in general that the service provider has performed its desired computation based only on the received output. The more powerful quantum computers are, the more problematic these issues become, as they grow capable of solving more and more advanced problems. All these considerations stiffen the adoption of quantum computers precisely at the time when they become useful for solving real-world problems. It is therefore vital to protect clients in these scenarii to foster wide-spread use of quantum computing technologies.

Thankfully, we can entirely remove the need for clients to trust their quantum service providers, with the help of quantum cryptography. Although quantum computers will be a threat to the security of some classical protocols (e.g. RSA) [1], they also open up

---

new possibilities via cryptographic protocols such as quantum key distribution [2]. In our particular case, protocols for Secure Delegated Quantum Computing (SDQC) have been a highly active research field in the past few years and represent an extremely promising application [3–7]. These protocols allow a client with limited quantum resources to delegate a quantum computation to a server, without the server learning anything about the quantum algorithm, the input which is being processed or the outcome of the computation. During the protocol's execution, the client can furthermore test that the server is behaving as expected.

**Related work.** Whether SDQC protocols see wide-spread use will depend directly on how technically accessible they are from the point of view of both the client and the server. In this respect, there are two extremes. On one end of the spectrum lie protocols which require one-way qubit communications between the client and the server and rather involved quantum setups for the client – either a source of qubits [5, 8] or a way to measure those received from the server [9, 10], along with single qubit operations. These protocols are information-theoretically secure, meaning that their security relies on no assumptions beyond the laws of physics, and they leak no information whatsoever about the computation, input or output. They are also composable, i.e. their security is not affected by the context of execution and they can be freely reused as black boxes in larger constructions (e.g. secure multi-party computations). However, for many interesting use cases it may not be feasible to expect clients to have access to either a qubit source or measurement devices in the near term and so it is important to reduce the technological requirements on the client's side.

At the other end there are protocols [7, 11–13] which only require the client to interact classically with the server instead of sending quantum states. However, they incur a significant overhead on the server's side, since it must be able to execute large cryptographically-secure functions to generate encrypted qubits of which only the client knows the secret key. Furthermore, these protocols only provide computational security, meaning that it relies on the quantum hardness of a computational problem. Finding an efficient algorithm for said problem would automatically break the protocol's security. It has further been proven that they cannot be composably secure without setup assumptions [14].

The middle ground is represented by the protocol from [15], whose efficiency in terms of communication was improved in [16–18]. The client here only manipulates and transmits semi-classical states, e.g. laser light for photonic applications, which drastically reduces the client's technological requirements. However, not only is it only blind and does not allow the client to verify the server's operation, there are three main challenges which limit its application. First of all, the server needs an efficient polarisation-preserving[2] photon-number Quantum Non-Demolition (QND) measurement, a very demanding operation in practice. Moreover, it must be able to extract from each pulse one single photon to use in the rest of the protocol. Finally, the server needs to implement deterministic two-qubit photonic gates, which are also extremely demanding. We also note that the security is information-theoretic but not proven in a composable security framework in the original paper.

**Overview of results.** Here, we propose a best-of-both-worlds protocol for SDQC using semi-classical communications that drastically reduces the technological requirements of

---

[2]Or qubit-preserving if other encoding are used.

*both* the client and the server. In particular, the client does not need to manipulate qubits, only a phase-randomised attenuated laser source and active waveplates, while the server does not need photon-number QND measurements, nor deterministic photon-photon gates that were required in Ref. [15]. Furthermore, we prove that the security of our protocol is information-theoretic and composable in the Abstract Cryptography framework of [19]. Figure 2 shows the various technological requirements of [5, 15] and our protocol.
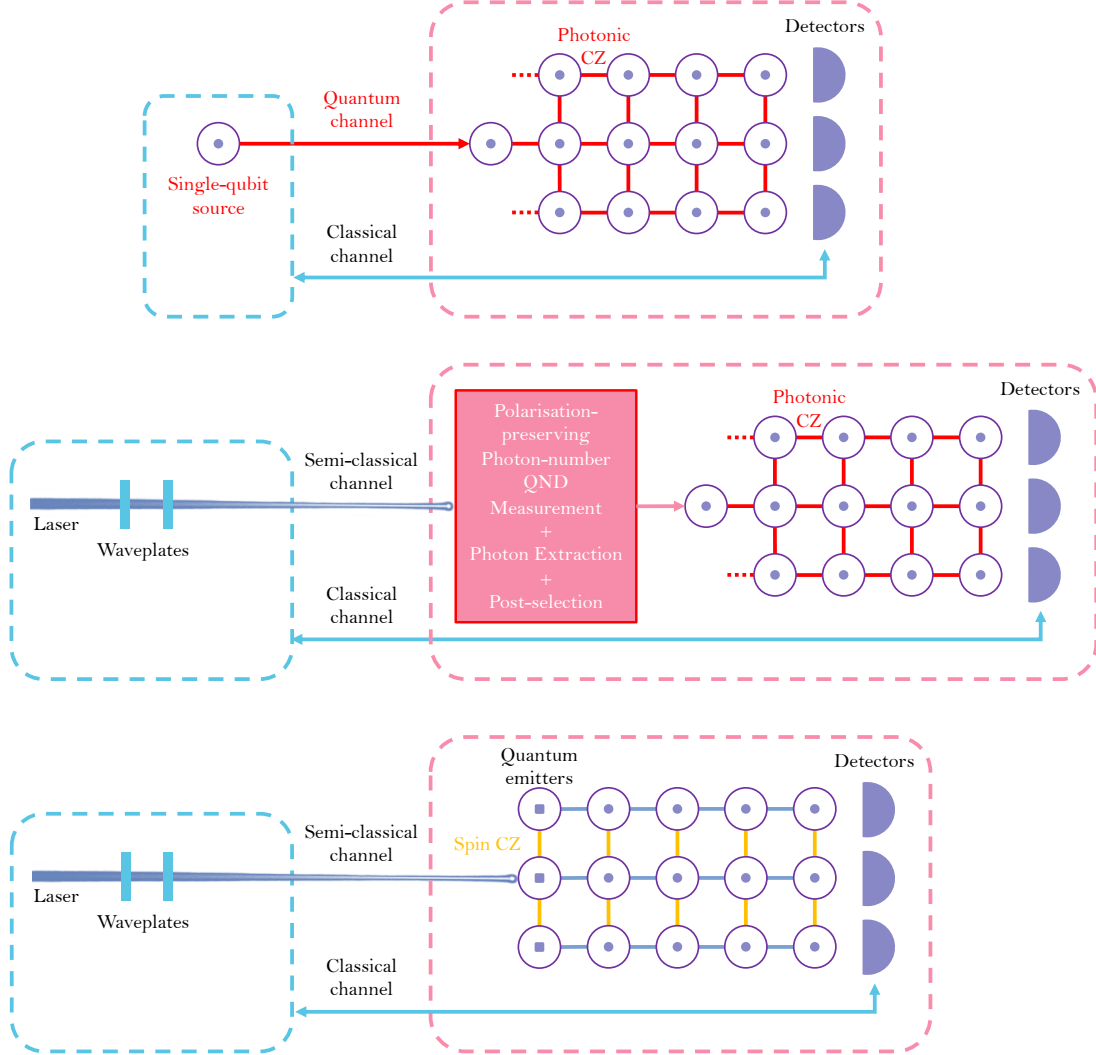


Figure 2: Hardware setup for performing three delegated computation protocols. The operations in the blue dashed boxes are performed by the client while the server handles those in the pink dashed boxes. Red, yellow, and blue elements corresponds to operations that have a high, moderate, and low technological requirements respectively. In all three cases the client classically sends measurement instructions to the server and recovers the outcome. Top: UBQC protocol from Ref. [5]. Middle: BDQC protocol from Ref. [15]. Bottom: our SDQC protocol.

Our protocol relies on Measurement-Based Quantum Computing (MBQC), a paradigm in which a large entangled state called graph state is first created and the computation is performed by adaptively measuring parts of the state in a predefined order, consuming the entanglement in order to carry out the computation. Such computations can be performed blindly by having the client prepare encrypted single qubits and send them to the server

who then entangles them. The entanglement operation commutes with the encryption, thus yielding an encrypted graph state. The client instructs the server to measure qubits from the encrypted graph state in a way which both undoes the encryption and performs the computation of the client's choice. This is the basis of the original Universal Blind Quantum Computation (UBQC) protocol of [5]. The first challenge is therefore to emulate these single-qubit transmissions using only attenuated laser pulses. The second challenge is to reduce the number of entangling gates that need to be performed after the qubits have been generated.

Protocol 1 presents informally our technique for generating a single qubit with amplified privacy which we describe in more details below.

---

**Protocol 1** GHZ privacy amplification for rotated states from weak coherent pulses (informal)

---

1. The server initialises its quantum emitter in the state $|+\rangle$.
2. The client sends $n$ randomly-polarised weak coherent pulses, which the server uses to excite its quantum emitter. The energy level structure of the quantum emitter induces as output a polarisation-encoded GHZ state that is Z-rotated by an angle corresponding to the sum of all random angles chosen by the client.
3. (a) The server emits one photon using a non-rotated coherent pulse and attempts to measure the first $n$ photonic qubits (generated by the client's pulses) in the $|\pm\rangle$ basis.
   (b) If the number of unsuccessful measurements (i.e. no photon was detected) is too high, the client aborts. Otherwise the server applies a correction to the last remaining photon and the quantum emitter which depends on the client's choice of angles and the measurement results. These corrections are specified in Protocol 3.

---

As expressed above, the client will send a sequence of phase-randomised attenuated laser pulses, with the polarisation of each pulse being chosen at random. This polarisation angle corresponds to the secret key which will later be used to encrypt the computation. The server receives these pulses and uses them to excite a quantum emitter with a qubit degree of freedom, such as a spin $\frac{1}{2}$, that can emit spin-entangled photons. The quantum emitter will have two roles. It will first act as a "laser-to-qubit converter" by converting a coherent pulse into a single photonic qubit. This role is somewhat similar to the Remote Blind Qubit State Preparation that was proposed in Ref. [15], but we execute it without having to perform a qubit-preserving photon-number QND measurement. Moreover, it will act as a "photon entangler" as the emitted photonic qubit will be entangled with the spin. The server exploits this property to produce an entangled state of photonic qubits, removing the need of performing demanding photon-photon entangling gates to produce the encrypted graph state. More precisely, it is possible to produce photonic linear cluster states with a single quantum emitter, with each photon being entangled in polarisation to the next emitted photon in the chain and the last one being also entangled to the spin [20–25]. Crucially, the state of each photonic qubit thus created inherits the polarisation angle from the pulse that was used to generate it. These chains of encrypted photonic polarisation-encoded qubits can then be combined to form the graph state supporting the client's desired computation. Only the links between chains need to be done after the qubits have been emitted, which drastically reduces the amount of entanglement operations. These can furthermore be done via interacting quantum emitters to remove entirely the need for photon-photon entangling gates, by performing the entanglement operations between quantum emitters in between photon emissions.

However, as in [15], an attenuated laser pulse necessarily leaks more information about the client's secret key compared to a single qubit. This is due to the fact that the state of the laser pulse can be described as a redundant encoding of the single qubit state containing the secret key. Taking a simplifying assumption, we can overestimate the information leakage by considering that any multi-photon component in the input laser completely leaks the polarisation information. We therefore need to suppress this information leakage in a way which meshes nicely together with the qubit generation technique described above. Fortunately, it is possible to easily switch between generating chains of qubits and GHZ states simply by selectively applying a Hadamard operation on the quantum spin. The full protocol then generates chains of encrypted GHZ states instead of chains of single qubits. Each qubit in the GHZ states is generated with a different random polarisation angle. The result is a chain of encrypted GHZ states whose encryption key is the sum of the polarisation angles. Each GHZ state can easily be collapsed into a single qubit while preserving the encryption key via measurements on all qubits but one in the GHZ state in the $|\pm\rangle$ basis, thus recovering the chain of single qubits used for the rest of the blind protocol. Intuitively, the server can learn the final encryption key of a given qubit only if all the angles used to generate the corresponding GHZ state have leaked. Therefore the final leakage probability is suppressed exponentially in the number of qubits per GHZ state.

This protocol exploits low-intensity lasers $|\alpha\rangle$ which generally have a non-negligible vacuum component, $|\langle 0|\alpha\rangle|^2$. In that case, even with an honest server and without other sources of photon loss, the quantum emitter sometimes cannot emit a photonic qubit. Our protocol accounts for this scenario by introducing a threshold on the number of detected photons during the aforementioned collapse of the GHZ states. If the losses reported by the server are too high, the client simply aborts.

The end result of the protocol in this simplified example is the state $\frac{1}{\sqrt{2}}(|00\rangle + e^{i\theta}|11\rangle)$ for a random angle $\theta$ known only to the client. The first qubit corresponds to the quantum emitter's qubit degree of freedom, while the second is the state of the remaining polarisation-encoded photon. This gives a lot of flexibility in how the server can use this protocol to construct a larger graph state since the emitter and photon are still entangled. The server can easily extend this into a linear cluster state by repeating the protocol, or continue growing this rotated GHZ state so that it has multiple photons available for performing graph fusion operations.

We show that both the protocol's security error and correctness error decrease exponentially with the number of pulses sent by the client (stated formally in Th. 5 and proven in App. C).

**Theorem 1** (Blind state preparation from weak coherent pulses, informal)**.** *The probability of obtaining an incorrect state and the probability that information about the angle $\theta$ leaks to the server both exponentially decrease in the number of pulses n, as proven in a composable security framework.*

When our protocol is used to replace the source of qubits required to perform the UBQC protocol from [5], it yields the following result.

**Theorem 2** (Blind Delegated Quantum Computation (BDQC) from weak coherent pulses, informal)**.** *There exists an efficient composably secure BDQC protocol with an exponentially-low security error in which the client only sends weak coherent pulses and the server only manipulates interacting quantum emitters.*

We then use this to build a protocol for SDQC. In addition to BDQC's blindness, SDQC also guarantees that the server performs the client's computation as instructed.

This means that any deviation from the supplied instructions which could corrupt the outcome of the computation should be detected with high probability. The tests which the client uses to detect these deviations up until recently all required the client to produce not only states in the $X - Y$ plane as in the UBQC protocol, but also computational basis states. This second requirement has been lifted recently in [26], which constructs an SDQC protocol from the same set of states as the one whose security we amplify here. Combining the result above with their protocol yields the following theorem.

**Theorem 3** (Secure Delegated Quantum Computation from weak coherent pulses, informal). *There exists an efficient composably secure SDQC protocol for delegating* BQP *computations with an exponentially-low security error in which the client only sends weak coherent pulses and the server only manipulates interacting quantum emitters.*

Finally, we study the experimental feasibility of our protocol by computing the trade-off between correctness and security in the presence of loss. Recent experimental developments in that regard show extremely promising results [22–25, 27] and hold the current record for the largest entangled photonic state produced [25]. Our scheme is thus not only secure but also experiment-ready.

**Comparison with Dunjko et al. [15].** The protocol from [15] works by having the server non-destructively measure the client's coherent light pulses in photon number, and post-select only the light pulses containing at least one photon. Then, the server must isolate one photon from each pulse. It applies a privacy amplification step which requires as many CZ gates as there are photons. After that, the server also has to entangle the privacy-enhanced photons into the graph state supporting the client's computation by using photon-photon CZ gates. All four of these steps are challenging technological requirements.

The Remote State Preparation (RSP) in Ref. [15] – performing a polarisation-preserving QND measurement to count the photons in each pulse and extracting a single qubit from pulses containing at least one photon – is separated from the privacy amplification and the graph state generation. This first step has been implemented by [18], requiring a number of pulses from the client which is around $10^8$ per qubit in the graph in the best case scenario where there is virtually no spatial separation between the client and server. They solve the issue of performing a QND measurement and qubit extraction – which previously required a much more complex process [28, 29] – by using a linear optical setup performing teleportation with EPR pairs. Although this is rather fast – their experiment generates $10^{11}$ leaky qubits via this RSP technique in two hours – they still need to entangle these polarisation-encoded base qubits using photonic gates to perform the privacy amplification, which is not done in [18]. Since they claim to want to use these $10^{11}$ leaky qubits to generate $10^3$ leak-free qubits, this implies a multiplicative overhead of $10^8$ in terms of entangling photonic gates compared to the client's base computation. The only viable option in this setting is to use deterministic non-post-selected photon-photon entangling gates since anything else will degrade far too rapidly to be useful. Unfortunately, the fidelities of such gates which have been demonstrated [30–32] are still insufficient to apply such a number of operations while preserving the integrity of the quantum state, even with error-correction techniques.

On the other hand, our RSP technique using a quantum emitter is intrinsically intertwined with the privacy amplification and graph state generation steps: the entanglement required for these two processes is directly generated by the structure of the quantum emitter and no additional operations are required. The result is that the final qubits are

positioned in the graph at the same time as they are produced with a polarisation that is unknown to the server. Our full protocol does not require any non-destructive photon measurements nor deterministic photon-photon gates. Instead, it requires quantum emitters with a spin degree of freedom, with a level structure that enables the emission of spin-entangled photons that are also efficient light sources. Single atoms and artificial atoms such as quantum dots or defect color centres inserted in optical microcavities or waveguides are natural choices for such spin-photon interfaces.

Our scheme can naturally generate linear cluster states from a single quantum emitter. In order to perform universal computations, multiple states of this kind must be entangled together. This can be done in one of two ways.

If multiple spins generate linear cluster states in parallel and these spins can interact with each other, then applying nearest-neighbour spin-spin CZ gates when the clusters should be linked is sufficient to obtain universality [33]. This is rather demanding since it requires either independently controlling chains of single atoms or artificial atoms such as quantum dot molecules, or the availability of a spin register such as a $^{13}$C nuclear spin for color centres in diamond.

Otherwise, it is possible to implement these operations with linear optics, via fusion operations and delays. The server can leverage the flexibility in our RSP technique to generate additional photons in each GHZ state and use these photons to implement fusion gates between different linear clusters as in [34], at the cost of an increased sensitivity to photon loss of the probability of generating the target blind graph.

**Comparison with Takeuchi et al. [35].** A recent paper [35] also proposed a protocol for information-theoretically secure SDQC using only semi-classical light. There are however significant differences both in terms of results and techniques. Their protocol is based on the SDQC protocol from [36] and requires the client to send states sampled from the same set as in our construction. The privacy amplification technique is similar to ours and that of Dunjko et al. However, their construction requires the same complex operations as Dunjko et al as well: QND measurements and photon-photon entangling gates. As such they do not resolve the issues stemming from these operations and our protocol is therefore much more suitable for implementation. Furthermore their security is not proven in a composable framework such as the one used in the present paper, meaning that their security guarantees do not automatically hold if an outcome of their protocol is later reused in another cryptographic construction.

**Organisation of the paper.** We start by giving preliminaries on (i) the generation of photonic graph states, and (ii) delegated quantum computing protocols. In Section 3, we present our protocol for securely preparing encrypted graph states from semi-classical light and its application in blind and secure delegated protocols. Later in Section 4 we analyse the success probability of our protocol on realistic hardware, taking into account multiple effects leading to photon loss. Finally, we discuss the merits of and possible improvements to our protocol in Section 5.

## 2 Preliminaries

Section 2.1 presents how to generate graph state from quantum emitters and weak coherent pulses. Then Section 2.2 describes the UBQC protocol that allows a client to blindly delegate quantum computations to a server. Additional preliminaries can be found in Appendix A, in particular Appendix A.2 presents the composable Abstract Cryptography

security framework from [19] in which we prove the security of our protocols. From now on, we call the client "Alice" and the server "Bob". We denote $|S|$ the cardinality of set $S$.

## 2.1 Graph state generation using quantum emitters

We describe here how to generate a cluster state from coherent pulses and quantum emitters using the technique from [37].

A graph state is a quantum state defined by a graph $G = (V, E)$ such that all vertices $v \in V$ are associated to qubits initialised in the $|+\rangle$ state and an edge $e = (v, w) \in E$ between two vertices corresponds to a $\mathsf{CZ}$ operation between the two qubits associated to vertices $v$ and $w$. Formally the graph state is thus given by:

$$|G\rangle = \prod_{(v,w)\in E} \mathsf{CZ}_{v,w} \bigotimes_{v\in V} |+\rangle_v . \tag{1}$$

A cluster state is a graph state whose graph is a regular lattice. In Figure 3, we for example display a 2D-cluster state.
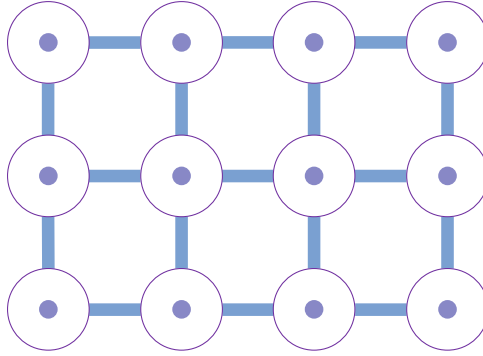


Figure 3: A cluster state of $n = 3$ rows and $m = 4$ columns. Each circle represents a qubit in the $|+\rangle$ state and each edge corresponds to the application of a $\mathsf{CZ}$ operator between adjacent qubits.

Bob can generate these states by using coherent pulses to repeatedly excite quantum emitters with a spin degree of freedom[3] and spin-selective transitions which can emit spin-entangled photonic qubits.

More precisely, we denote $|\downarrow\rangle$ and $|\uparrow\rangle$ the computational basis states of the spin qubit. After excitation, we assume that the quantum emitter will spontaneously emit a photon whose polarisation is correlated to the spin state as follows: $|\uparrow\rangle \xrightarrow{E_{\text{qe}}} |\uparrow, R\rangle$ and $|\downarrow\rangle \xrightarrow{E_{\text{qe}}} |\downarrow, L\rangle$. Overall, an excitation with a weak coherent pulse followed by radiative decay yields the following emission operator for our quantum emitter:

$$E_{\text{qe}} = |\downarrow, L\rangle \langle\downarrow| + |\uparrow, R\rangle \langle\uparrow| , \tag{2}$$

where $|L\rangle, |R\rangle$ denote respectively left and right polarised photon states.[4] A simple example of such transitions is displayed in Fig. 4 and corresponds to a singly-charged single quantum dot.

---

[3]Any other qubit degree of freedom would work.

[4]We associate states $|\downarrow\rangle, |L\rangle$ to $|0\rangle$, and $|\uparrow\rangle, |R\rangle$ to $|1\rangle$.
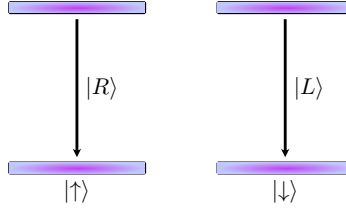
Figure 4: Energy level structure of a quantum emitter suitable for our BDQC protocol with semi-classical light communications, such as a negatively-charged quantum dot.

The operation $E_{\text{qe}}$ can equivalently be expressed as applying a CNOT between the quantum emitter and a photon in the $|0\rangle_{ph}$ state as in the following circuit:



Starting from a spin in state $|+\rangle_{qe} := \frac{1}{\sqrt{2}}(|\downarrow\rangle + |\uparrow\rangle)$, applying the emission operator generates a Bell state including one photon and the spin qubit:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\downarrow\rangle\,|L\rangle + |\uparrow\rangle\,|R\rangle). \tag{3}$$

This Bell state can be seen as a redundantly encoded $|+\rangle$ state. Applying a Hadamard gate on the spin then generates a two-qubit linear cluster state where one vertex contains the spin qubit and the other is comprised of polarisation qubit:

$$\mathsf{CZ}_{qe,ph}\,|+\rangle_{qe}\,|+\rangle_{ph}. \tag{4}$$

This process can be represented as in the following Figure 5:



Figure 5: Basic linear cluster generation process. Starting from an appropriate quantum emitter in the $|+\rangle_{qe}$ state (small square), a Bell state $|\Psi\rangle$ is created via emission of a photon (small circle) and then transformed into a cluster state. The middle circle containing two elements represents the Bell state as a redundantly-encoded $|+\rangle$ state.

Intuitively, we can see that applying multiple times the emission operator grows the number of qubits inside the vertex containing the quantum emitter, while applying a Hadamard gate moves the quantum emitter to an adjacent vertex. The process can then be repeated to construct a linear cluster with redundantly-encoded vertices.

To generate a cluster state with $n$ rows and $m$ columns, we use $n$ quantum emitters placed in a line which can each quantumly interact with its neighbours via a CZ operation. We first apply a CZ between each quantum emitter and its neighbours, then make each quantum emitter emit one photon and apply a Hadamard on the spin of the emitter. This process is repeated $m$ times, after which the quantum emitters are measured in the Z
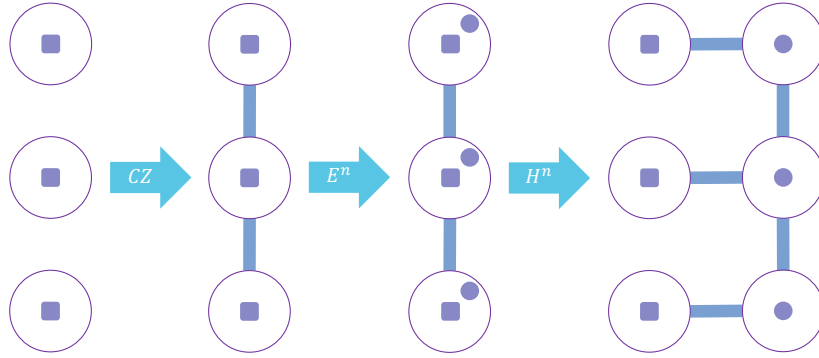
(a) First step in the cluster state emission. Starting from $n = 3$ quantum emitters, we apply a CZ gate between each pair of neighbours, followed by an emission operator and Hadamard on all emitters.
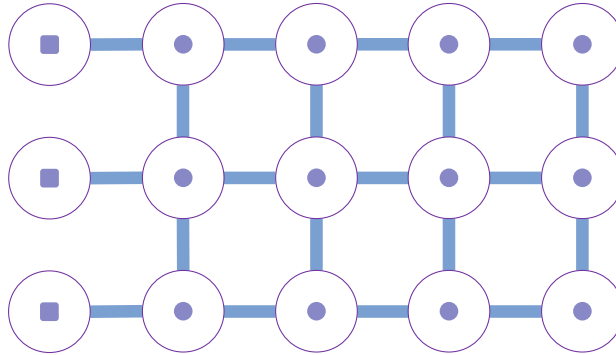


(b) Result after repeating the process in Figure 6a $m = 4$ times. The quantum emitters are then measured in the Z basis. This yields the state from Figure 3 encoded in the polarisation of the emitted photons.

Figure 6: Generation of a cluster state of $n = 3$ rows and $m = 4$ columns.

basis. Up to single-qubit Z corrections, this disentangles them from the generated cluster state.[5] This process is presented in Figure 6.

Alternatively, arbitrary graph states can be constructed from linear clusters using various schemes, for example using non-interacting spin quantum emitters and linear optics as in [34]. Each quantum emitter generates a redundantly-encoded linear cluster state. This is done by emitting $N$ photons before applying a Hadamard gate. After $n$ repetitions, this results in the following state $\bigotimes CZ_{i,i+1} |GHZ_N\rangle^{\otimes n}$, where each CZ gate acts on one qubit from two neighbouring $N$ qubit GZH states defined as $|GHZ_N\rangle := \frac{1}{\sqrt{2}}(|L\rangle^{\otimes N} + |R\rangle^{\otimes N})$. Such redundantly-encoded linear cluster states can be represented as in Figure 7.
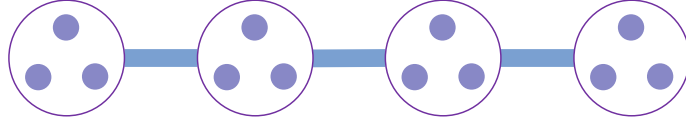


Figure 7: A 3-qubit redundantly-encoded linear cluster state of $m = 4$ columns. Each circle with three dots represents a three-qubit GHZ state.

Two such states can be joined together using fusion operations: to create an edge between two vertices, a pair of photons – one from each of the vertices – are measured using a fusion gate (similar to a Bell measurement) [38]. A success joins the two states, while a failure means simply losing these photons. This process can be repeated so long as there are photons left in the GHZ states. The success probability is quite sensitive to photon losses – additional photons are created and must be detected to create some edges of the graph. However, in principle, this scheme can be made near-deterministic in the absence of loss.

Our secure protocol presented later in the paper can also be straightforwardly adapted to the graph state generation techniques based on deterministic spin-photon interactions from [39–42]. Note that we have used a polarisation encoding based on a four-level system as depicted in Fig. 4, but we can also easily generalise the generation schemes to other types of photon encoding and/or quantum emitter level structure [43–46].

## 2.2 Delegated quantum computing protocols

### 2.2.1 Measurement-based quantum computing

We start by describing how computations are performed in the MBQC model for classical inputs and outputs. Alice's computation is defined by a so-called *measurement pattern* which consists of a graph $G = (V, E, I, O)$, with vertex and edge sets $V$, $E$, input vertex set $I$ and output vertex set $O$, a partial order $\preceq$ over $V$, a set of angles $\{\phi_v\}_{v \in V}$ and a flow function $f$ from non-output vertices $V \setminus O$ to non-input vertices $V \setminus I$.

The computation starts by producing on Bob's machine the graph state $|G\rangle$ associated to the graph $G$: for each vertex in $V$ one qubit is prepared by Alice in the state $|+\rangle$ and sent to Bob, who then applies a $CZ_{v,w}$ operation between each pair of qubits associated to vertices $v, w$ joined by an edge in $E$.

---

[5]The Z basis measurement can be done by emitting an auxiliary photon using $E_{qe}$ and measuring it in the Z basis.

Alice can then perform a quantum computation on the graph state generated by Bob by instructing him to measure vertices in the order $\preceq$. These measurements are performed in the $\mathsf{X} - \mathsf{Y}$ plane of the Bloch sphere, i.e. measurements in the $|\pm_\phi\rangle = {}^{1}\!/\!_{\sqrt{2}}(|0\rangle \pm e^{i\phi}|1\rangle)$ bases. The measurements are specified for each vertex $v$ by the angle $\phi_v$.

If a measurement outcome on a non-output vertex is 1, some future measurement angles must be adapted in order to perform the same computation as if the measurement outcome had been 0. The flow function $f$ prescribes how the base angles $\{\phi_v\}_{v \in V}$ change due to this effect, see [47] for more details. We will note $\phi'_v$ the updated angle.

In the case of classical outputs, the outcome of the computation is given by the measurement results on vertices from set $O$ after corrections given by the flow are applied.

This scheme is universal when using specific graphs, either brickwork graph states [5] or cluster states [48], and measurement angles $\phi_v$ chosen from the set $\Phi = \{j\pi/4 \mid j = 0, 1, \ldots, 7\}$.[6]

Following this procedure allows Alice to delegate any quantum computation of her choice, at the cost of revealing it entirely to Bob.

### 2.2.2 Blind delegated protocol

The goal of the UBQC protocol is to allow Alice to perform the same task but without Bob learning anything about her desired computation. In the original UBQC protocol [5], Alice also sends qubits to Bob, but their initial state is chosen among $|+_\theta\rangle = {}^{1}\!/\!_{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$ with $\theta \in \Phi$. We can rewrite this state as $|+_\theta\rangle = \mathsf{R_Z}(\theta)|+\rangle$, with:

$$\mathsf{R_Z}(\theta) = \exp\left(-\frac{i\theta}{2}\mathsf{Z}\right) = \cos(\theta/2)\mathsf{I} - i\sin(\theta/2)\mathsf{Z} \tag{5}$$

Since $\mathsf{R_Z}(\theta)$ commutes with $\mathsf{CZ}$ applied by Bob after receiving Alice's qubits, the resulting state is a graph state up to local rotations $\mathsf{R_Z}(\theta)$ on each qubit:

$$\left|G(\vec{\theta})\right\rangle = \left(\prod_{(v,w)\in E} \mathsf{CZ}_{v,w}\right) \mathsf{R_Z}(\vec{\theta}) \otimes_{v \in V} |+\rangle_v = \mathsf{R_Z}(\vec{\theta})|G\rangle, \tag{6}$$

with

$$\mathsf{R_Z}(\vec{\theta}) = \prod_{v \in V} \mathsf{R}_\mathsf{Z}^v(\theta_v) \tag{7}$$

where $\vec{\theta}$ is a vector corresponding to all the angles $\theta_v$ applied on each vertex $v \in V$, and the $v$ index in $\mathsf{R}_\mathsf{Z}^v$ denotes on which qubit the rotation is applied. We will call any graph state of the form $\left|G(\vec{\theta})\right\rangle$ a *blind graph state*.

To perform the same computation as before, instead of measuring the qubit at vertex $v$ using the measurement angle $\phi'_v$, Alice will instead request that Bob use the angle $\delta_v = \phi'_v + \theta_v + r_v\pi$. Consequently, since the measurement with angle $\delta_v$ is performed by applying $\mathsf{R_Z}(-\delta_v)$ and measuring in the $|\pm\rangle$ basis, the $\theta_v$ from the measurement angle will cancel out the $\theta_v$ applied during the state generation and apply Alice's desired computation. It will at the same time perfectly hide the value of $\phi'_v$ in $\delta_v$. The value of $r_v$ is chosen uniformly at random from $\{0, 1\}$ to randomise the outcome of the measurement. This is required

---

[6]MBQC is exactly universal if we allow arbitrary angles from $[0, 2\pi)$, and it is approximately universal for $2^k$ angles of the form $2j\pi/2^k$ so long as $k \geq 3$, see [49].

since Bob can otherwise learn the outcome of the computation. So long as $\vec{\theta}$ and $\vec{r}$ are hidden, the quantum computation is blind and leaks no information as proven in Ref. [5].

For completeness sake, we describe in Appendix A.1, Protocol 4 the full UBQC protocol for classical inputs and outputs and provide the formal security statement in Appendix A.2, Theorem 9.

### 2.2.3 Secure delegated protocol

Secure Delegated Quantum Computations (SDQC) protocols not only ensure that Alice's information remains private, but also provide verifiability. This property guarantees that Alice either receives the correct output or aborts the computation due to Bob deviating from his prescribed operations.

Various techniques have been developed for inserting tests alongside Alice's computation of interest to check that Bob's behaviour is honest [8, 50, 51], but most require the preparation of both rotated $|+_\theta\rangle$ states and states in the computational basis. These are used to isolate qubits in the graph so that Bob's measurement of these qubits returns a deterministic result if performed correctly. Such isolated qubits can then be used to test Bob throughout the execution of the computation.

We present here the protocol from [26] for classical input/output $\mathsf{BQP}$ computations which uses only $|+_\theta\rangle$ states. Alice and Bob repeat the same UBQC execution $N$ times, using a random fraction of the executions to test Bob's honesty via deterministic computations whose outcomes are known to Alice. If less than a given fraction of these tests pass, Alice aborts. Otherwise she computes the majority outcome of the UBQC runs which performed her desired computation.

The tests use the fact that the graph state $|G\rangle$ is the common eigenstate of all Pauli operations of the form $\mathsf{S}_v = \mathsf{X}_v \prod_{(v,w)\in E} \mathsf{Z}_w$ – called the graph's stabilisers. A test is then defined by a product of these stabilisers $\mathsf{S}_{\vec{t}} = \prod_{v \in V} \mathsf{S}_v^{t_v}$ for a bit string $\vec{t} \in \{0,1\}^{|V|}$. To perform the test associated to stabiliser $\mathsf{S}_{\vec{t}}$, Alice instructs Bob to measure all vertices in the Pauli bases given by this stabiliser. She then computes the parity of measurement outcomes and the test passes if it is 0.

In UBQC, Bob only performs measurements in the $\mathsf{X} - \mathsf{Y}$ plane, therefore Ref. [26] requires that Alice only uses tests $\mathsf{S}_{\vec{t}}$ such that $\mathsf{S}_{\vec{t}}$ does not act as Pauli $\mathsf{Z}$ on any vertex $v$. Then the state preparation and measurements for tests and computations are indistinguishable since both can be hidden via a UBQC overlay. For various types of graphs including the brickwork and cluster graphs, Ref. [26] then defines sets of such tests from which Alice draws at random when she must perform a test run during the protocol's execution.

Ref. [26] show that these tests can catch all of Bob's deviations which may corrupt Alice's computation in the case of classical outputs. Then, if $N$ is the total number of UBQC executions, the probability that Alice accepts an incorrect outcome at the end of the SDQC protocol decreases exponentially with $N$.

For completeness sake, we describe in Appendix A.1, Protocol 5 the full SDQC protocol for classical inputs and outputs, and provide the formal security statement in Appendix A.2, Theorem 10.

## 3 Remote state preparation with semi-classical clients

The security of the delegated quantum computation protocols presented in the previous section rests on the fact that Bob cannot access information about the secret angle $\theta_v$ with

certainty. When sharing single qubits, this is ensured by the no-cloning theorem [52, 53]. However, single-qubit sources are expensive and may be inaccessible to most clients who desire to run secure quantum computations. We describe in this section how the same result can be obtained using limited means on both sides of the protocol.

## 3.1 Blind graph state generation using quantum emitters

Instead of sending single qubits, in our protocol Alice transmits coherent states to hide the phases $\vec{\theta}$. The main advantage is that a photonic attenuated coherent state source is simply a laser light which is already commercially available and likely to remain much more economical than a source of single qubits. Such a coherent state $|\alpha\rangle_\theta$ with $\alpha = |\alpha|e^{i\varphi}$ is given by:

$$|\alpha\rangle_\theta = e^{-|\alpha|^2/2} \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle_\theta \,, \tag{8}$$

for $|k\rangle_\theta := \left(a_\theta^\dagger\right)^k |v\rangle$, where $a_\theta^\dagger := \cos(\theta)a_R^\dagger + \sin(\theta)a_L^\dagger$ is the rotated polarisation creation operator and $|v\rangle$ is the vacuum state. Using a phase-randomised laser, Alice instead sends the state:

$$\rho_{\alpha,\theta} = \frac{1}{2\pi} \int_{\varphi=0}^{2\pi} \left||\alpha|e^{i\varphi}\rangle\!\langle|\alpha|e^{i\varphi}\right|_\theta \mathrm{d}\varphi = e^{-|\alpha|^2} \sum_{k=0}^{\infty} \frac{|\alpha|^{2k}}{k!} |k\rangle\!\langle k|_\theta \tag{9}$$

On the other hand, Bob must convert these coherent states into single qubits while preserving the polarisation in order to use them in the UBQC protocol. This can be done using the scheme presented in Section 2.1 with a slight modification of the emission operator in Eq. (2). If Alice's light source sends the state $\rho_{\alpha,\theta}$ at an intensity $|\alpha|^2$ such that it is able to drive the optical transition of the quantum emitter from Figure 4, the production of spin-entangled photon states is done via the following global operation:

$$E_{\mathrm{qe}}(\theta) = |\downarrow, L\rangle \langle\downarrow| + e^{i\theta} |\uparrow, R\rangle \langle\uparrow| = \mathsf{R_Z}(\theta)E_{\mathrm{qe}}. \tag{10}$$

The polarisation of the input coherent laser therefore imprints a phase on the photon after emission, corresponding to a $\mathsf{R_Z}(\theta)$ rotation.

If the operation $E_{\mathrm{qe}}(\theta)$ is used instead of simply $E_{\mathrm{qe}}$ in the graph generation process described in Section 2.1, then the resulting state is the rotated cluster state $\left|G(\vec{\theta})\right\rangle$, which is the required resource for both the UBQC and SDQC protocols as shown in Eq. (6). Intuitively, so long as all the angles $\theta_v$ are hidden from Bob, the UBQC protocol which uses this strategy for generating the blind graph remains secure. We now introduce a new resource in the Abstract Cryptography security framework and then describe a protocol which formalises this idea. For unitary $\mathsf{U}$, we write $\mathsf{U}(\rho)$ to mean $\mathsf{U}\rho\mathsf{U}^\dagger$. Furthermore, when applying $\mathsf{CNOT}$ operations, we always assume that the first qubit mentioned is the control while the second one is the target.

---

**Resource 1** Blind Graph State Extender

---

**Inputs:** Alice inputs an angle $\theta \in \Phi$. Bob inputs a single-qubit state $\rho_B$.
**Computation by the resource:** The resource samples a bit $b \in \{0,1\}$ uniformly at random and sends to Bob the two-qubit state $\mathsf{R_Z}((-1)^b\theta)\mathsf{CNOT}\,(\rho_B \otimes |0\rangle\!\langle 0|)$, where $\mathsf{R_Z}$ is applied to the second qubit.

---

This resource captures the perfect setting where the rotated emission operator $E_{\mathrm{qe}}(\theta)$ is applied to Bob's quantum emitter without leaking any information about the state. The

additional value $b$ gives more flexibility in how this resource can be implemented. We then show that this resource can be used to securely produce a blind graph state on Bob's device via the following Protocol 2. We do not specify the entanglement operations performed by Bob so that it may use either strategies outlined in section 2.1. To each of Bob's quantum emitters $q$, we associate the ordered list of vertices $V_q \subset V$ which Bob generates using this quantum emitter. We assume that for two consecutive vertices $v, w \in V_q$ we have $(v, w) \in E$.

---

**Protocol 2** Blind graph state preparation from blind extensions

---

**Public information:** Graph $G = (V, E)$ and an ordering $<$ over vertices decided by Bob.

**Inputs:** Alice inputs a set of angles $\vec{\theta} \in \Phi^{|V|}$.

**Protocol:**

1. Bob initialises the spin qubit of all his quantum emitters in the state $|+\rangle_{qe}$.
2. For each vertex $v$ in the graph, in the order $<$:
   (a) Alice and Bob perform a call to the Blind Graph State Extender Resource 1:
      - Alice inputs the angle $\theta_v$. Bob inputs the spin qubit of quantum emitter $q$ such that $v \in V_q$.
      - Bob receives as output two qubits along with a bit $b_v$.
   (b) Bob applies $\mathsf{X}^{b_v}$ to both qubits it received and $\mathsf{Z}^{b_v}$ to any one qubit at the vertex $v' \in V_q$ preceding $v$, if it exists.
   (c) Bob produces a number $n_v$ of his choice of additional qubits using the emission operator $E_{qe}$.
   (d) Bob performs all entanglement operations between vertex $v$ and the vertices $w < v$ such that $(v, w) \in E$. These can be performed either via:
      - $\mathsf{CZ}$ gates between quantum emitters $q$ and $r$ where $v \in V_q$ and $w \in V_r$, if $r$ is still situated at vertex $w$;
      - fusion operations between the additional qubits generated by Bob at vertices $v$ and $w$.
   (e) Bob applies a Hadamard gate to the spin qubit of quantum emitter $q$.
3. Bob decorrelates his quantum emitters from the polarisation-encoded graph state by performing:
   (a) a measurement of each spin qubit $q$ in the computational basis with outcome $c_q$;
   (b) a correction $\mathsf{Z}^{c_q}$ on a qubit of vertex $v_q$ where $v_q$ is the last element of $V_q$.
4. If there are leftover additional qubits at any vertex $v$, Bob measures them in the $|\pm\rangle$ basis. Let $d_v$ be the sum of measurement outcomes, Bob applies $\mathsf{Z}^{d_v}$ to the remaining qubit at vertex $v$.

---

**Protocol security.** The blind graph state generation protocol (Protocol 2) perfectly constructs the Blind Graph RSP Resource 2, meaning that the security error is exactly 0. This is captured by Theorem 4, whose proof can be found in Appendix B.

**Theorem 4** (AC security of Protocol 2)**.** *Protocol 2 perfectly constructs in the Abstract Cryptography framework the Blind Graph RSP Resource 2 from $|V|$ instances of the Blind Graph State Extender Resource 1.*

## 3.2 Security amplification via rotation aggregation

It would seem like simply exciting a quantum emitter via a pulse in the state $\rho_{\alpha,\theta}$ would be enough to construct the Blind Graph State Extender Resource 1 since it is equivalent to applying the emission operator $E_{\mathrm{qe}}(\theta)$. However this is not the case since a laser pulse leaks a non-negligible amount of information.

Due to the phase randomisation step, Bob has access to a probabilistic mixture of states $|k\rangle\langle k|_\theta$. These states consist of $k$ photons which each contain the same information about $\theta$. If he performs a polarisation-preserving photon number resolving QND measurement, he can learn the number $k$ of incoming photons for each vertex of the blind graph state. Bob can then choose to attack the vertex where he received the most photons.

If we assume that Bob is capable of manipulating each of these photons in isolation, the amount of knowledge that he can extract from the execution of the protocol directly increases with the intensity of the coherent state $|\alpha|^2$ via the probability of obtaining multiple photons. On the other hand, a relatively high value for $|\alpha|^2$ is desirable in order to excite the quantum emitter generating the blind graph state.

In order to recover the ideal scenario described by the Blind Graph Extender Resource 1, we make use of a security amplification gadget which exponentially suppresses the information leakage using only a linear number of pulses.

This protocol makes use of the GHZ-generation capability of the quantum emitter paired with the rotated emission operator $E_{\mathrm{qe}}(\theta)$. Alice sends to Bob a certain number of phase-randomised rotated weak coherent pulses $\rho_{\alpha,\theta_i}$ for a fixed intensity $|\alpha|^2$ and randomly chosen values of $\theta_i$. Bob uses these pulses to drive the transition of his quantum emitter, effectively applying the rotated emission operator $E_{\mathrm{qe}}(\theta_i)$. These consecutive pulses will generate a rotated GHZ state whose angle is the sum of all angles used by Alice for laser pulses containing at least one photon. Bob emits one last photon using $E_{\mathrm{qe}}$ and then measures all qubits generated by Alice's pulses in the X basis. He can thus detect which laser pulses contained no photons. If too few photons have been detected, Alice aborts the protocol. This threshold, set by the security proof, prevents Bob from discarding too many pulses from which he would not get enough information. If Alice has not aborted, she communicates to Bob a correction which depends on her desired angle and the parity of the measurement outcomes. After applying this correction, Bob's device contains the random rotated state chosen by Alice. This process is presented in Figure 8.
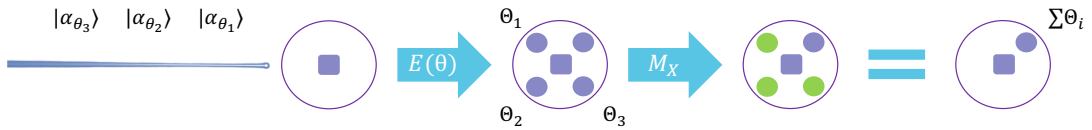


Figure 8: Example of privacy amplification with three weak coherent pulses in the lossless case. The laser with polarisation control on the left is in the hands of Alice while the quantum emitter (square) is handled by Bob. Alice sends three pulses with randomly rotated polarisations. Bob uses these pulses to drive the quantum emitter and then emits one more photon. The result is a five-qubit rotated GHZ state after the first arrow. Bob then measures (in orange) all polarisation qubits in the GHZ state but one in the $|\pm\rangle$ basis. After correction, the result is a rotated Bell state containing the spin qubit and one polarisation qubit. This is the same state – up to rotation – as in the middle step of the basic linear cluster generation process from Figure 5.

We describe formally this process in Protocol 3.

---

**Protocol 3** GHZ privacy amplification for rotated states from weak coherent pulses

---

**Public information:** Laser pulse intensity $|\alpha|^2$, number $n$ of pulses sent per GHZ gadget, threshold $t$.

**Inputs:** Alice inputs an angle $\theta \in \Phi$. Bob inputs a single-qubit spin state $\rho_{qe}$.

**Protocol:**

1. Alice samples values $(\theta_1, \ldots, \theta_n)$ uniformly at random from $\Phi$.
2. For $1 \leq i \leq n$:
    (a) Alice sends the phase-randomised rotated weak coherent pulse $\rho_{\alpha,\theta_i}$ to Bob.
    (b) Bob uses this pulse to apply the rotated emission operator to his spin qubit $E_{\text{qe}}(\theta_i)$.
3. Finalisation:
    (a) Bob emits another photon using the emission operator $E_{\text{qe}}$. This qubit is indexed 0.
    (b) Bob attempts to measures all photonic qubits $i \neq 0$ in the GHZ state in the $|\pm\rangle$ basis. Let $S \subseteq \{1, \ldots, n\}$ be the set of indices for which the measurement succeeded (i.e. a photon has been detected) and let $b = \bigoplus_{i \in S} b_i$ be the parity of the corresponding measurement outcomes. Bob sends $S$ to Alice.
    (c) Alice aborts if $|S| \leq t$, sending Abort to Bob and setting it as her output. Otherwise, she samples uniformly at random a bit $m_x \in \{0, 1\}$ and sends the correction angle $\bar{\theta} = (-1)^{m_x}\theta - \sum_{i \in S} \theta_i$ and bit $m_x$ to Bob.
    (d) Bob applies the correction $\mathsf{R_Z}(\bar{\theta} + b\pi)$ to photonic qubit 0 and sets it as his output together with bit $m_x$.

---

**On the final correction operation.** The final correction might seem like a superfluous step, but it is necessary for proving the security of the protocol. In particular, the simulator built as part of the security proof requires this flexibility to adapt its behaviour to the set $S$ returned by the distinguisher. However, this does not mean that this correction must necessarily be implemented as an additional quantum operation by Bob. We use this protocol within Protocol 2 to build a resource state for the UBQC protocol, which already requires Alice to send measurement angles to Bob. Alice can merge the correction with these measurement angles so that both are applied simultaneously as as single operation. Therefore, this correction does not imply an additional classical communication step, nor an additional operation by Bob, if Protocol 3 is used together with UBQC.

**Protocol security.** The privacy amplification protocol presented above constructs the Blind Graph State Extender Resource 1, with a security error which decreases exponentially in the number of pulses $n$ sent by Alice. This analysis holds in the lossless regime, assuming that each laser pulse has a probability $\eta_1$ of applying the rotated emission operator to the spin qubit. The next section gives arguments for this assumption and discusses more realistic settings when taking losses into account. The security of our protocol is given by Theorem 5, whose proof can be found in Appendix C.

**Theorem 5** (AC security of Protocol 3). *Let $\eta_1$ be the probability that the quantum emitter generates a photon after receiving a laser pulse of intensity $|\alpha|^2$ and let $p_{\alpha,2} = 1 - e^{-|\alpha|^2} - |\alpha|^2 e^{-|\alpha|^2}$ be the probability that the laser pulse contains two or more photons. Let $(\alpha, n)$ be the public parameters used in Protocol 3, and let $t = \frac{\eta_1 + p_{\alpha,2}}{2}n$. Then Protocol 3 $\exp(-\nu_\alpha n)$-constructs in the Abstract Cryptography framework the Blind Graph State Extender Resource 1, for $\nu_\alpha = (\eta_1 - p_{\alpha,2})^2/2$.*

## 3.3 Post-selecting on receiving all photons

It is possible also for Alice to reject the state as soon as a single photon is lost. We describe this alternative formally in Appendix D as Protocol 6, along with a correctness and security analysis.

The threshold protocol presented above will abort significantly less often than the one which requires Bob to recover all photons. This is because Protocol 3 tolerates some losses due to a photon not being emitted. On the other hand, the security bound is slightly degraded. Combined together, the threshold protocol's security and successful completion probability both increase with the number of emitted photons, as expressed in Theorem 5. It would seem like it is therefore the superior protocol since the success probability of the post-selected protocol actually decreases exponentially with the number of photons which need to be collected.

However this analysis holds only if we assume that (i) there are no losses after the photons have been emitted, and (ii) the emission operator correctly describes the result of the interaction between the laser pulse and the quantum emitter.

If a photonic qubit is lost after it has been generated in Protocol 3, the state is perfectly mixed from the point of view of both Alice and Bob. Discarding the state as soon as a single photon is not detected by Bob during the measurement prevents this issue and as a consequence the correctness of the output state of Protocol 6 is unaffected by losses which happen after the qubit generation procedure. This includes the case where the photon is emitted while the interaction between the laser and the quantum emitter is still taking place and is filtered out as described in Section 4.1.

Both protocols on the other hand may suffer if the laser-spin interaction deviates from the ideal emission operator described here. If for instance a photon is emitted while the laser interaction is ongoing and the laser re-excites the quantum emitter resulting in a second photon being emitted, neither protocols will count this as a loss but the end result will be a perfectly mixed state in both cases. However, if the operator instead applies a slightly different angle for some or all values of $\theta$, this can be mitigated if the overall protocol can tolerate this noise level.

## 3.4 Delegated quantum computation protocols with semi-classical client

We describe in this section how to build delegated quantum computation protocols with a semi-classical client. To this end we compose our bind graph RSP protocol and privacy amplification protocol with the protocols from [5] and [26] to obtain respectively BDQC and SDQC protocols.

**Blind delegation from semi-classical client RSP.** We use the composition theorem from the AC framework to replace the call to the Blind Graph RSP resource in the UBQC protocol from Section C with our Protocols 2 and 3. The general composition Theorem 8 allows us to combine Theorems 9, 4 and 5 into the following result.

**Theorem 6** (BDQC with semi-classical client)**.** *Let $\alpha, \nu_\alpha, n$ be defined as in Theorem 5 and let $|V|$ be the number of vertices in the graph supporting Alice's desired MBQC computation. Consider the protocol obtained by replacing the blind graph state generation in the UBQC Protocol 4 (steps 1 and 2) with Protocol 2 composed with Protocol 3 with parameters $(\alpha, n)$. This protocol $|V| \cdot \exp(-\nu_\alpha n)$-constructs in the Abstract Cryptography framework the BDQC Resource 3.*

**Testing the server's honesty with semi-classical light.** There are two challenges when trying to use our semi-classical client technique together with protocols for SDQC which require the client to produce states in the computational basis, such as those from [8, 50, 51].

First of all, generating a computational basis state with the energy structure presented in Figure 4 would project the spin state to the corresponding computational basis state. This would then need to be reinitialised by the Server to continue the entanglement generation. The information of whether or not the spin needs to be reinitialised in a superposition would therefore leak whether the state produced is rotated or in the computational basis.

Then, there is the issue of amplifying the security of both computational basis and rotated states using a single gadget which does not introduce new attack vectors or leak information. This has been attempted in [54] but a new attack on their scheme has been shown in [26]. Thankfully, this second work also fixes the issue by proposing a novel SDQC protocol which makes use of the generalised tests introduced in [55]. This corresponds to the protocol presented in Section 2.2.3 and more formally as Protocol 5.

The composable security of their protocol scales exponentially with the number of repetitions of the UBQC protocol, and the security of our blind graph RSP protocol degrades linearly in the number of repetitions. We again use the general composition Theorem 8 to combine Theorems 10 and 5 into the following result, yielding an SDQC protocol in which Alice only needs to send weak coherent states.

**Theorem 7** (SDQC with semi-classical client)**.** *Let $\alpha, \nu_\alpha, n$ be defined as in Theorem 5, let $N$ be the number of executions of the UBQC Protocol 4 in Protocol 5 and let $|V|$ be the number of vertices in the graph supporting Alice's desired MBQC computation. Consider the protocol obtained by replacing the blind graph state generation step in each UBQC execution in the SDQC Protocol 5 with Protocol 2 composed with Protocol 3 with parameters $(\alpha, n)$. This protocol $N|V| \cdot \exp(-\nu_\alpha n) + \epsilon_S$-constructs in the Abstract Cryptography framework the SDQC Resource 4, for $\epsilon_S$ exponentially decreasing in $N$ being the security bound of the SDQC Protocol 5.*

Finally, as shown in [26, 55], this SDQC protocol tolerates a constant level of global honest noise, meaning that slight defects will be corrected and Alice is able to recover the correct output without aborting even if her apparatus or Bob's have a low-enough level of noise.

## 4   Fine-tuning laser intensity for correctness/security trade-off

In the previous section we have shown via Theorem 5 that, so long as the total single-photon efficiency $\eta_1$ is greater than the probability of receiving two or more photons $p_{\alpha,2}$, we can amplify the security of blind state generation to arbitrary levels by increasing the number of photons in the GHZ gadget.

The vacuum probability of the incoming coherent pulse imposes an upper bound on $\eta_1$ of $p_{\alpha,1} = 1 - e^{-|\alpha|^2}$. In reality, if the average number of photons $|\alpha|^2$ is not large enough, the population of the emitter will not be sufficiently inverted to achieve single-photon emission with a high efficiency and the criteria for security amplification may not be satisfied. The exact value of $\eta_1$ can depend on the energy-level structure of the device, the excitation scheme, and the pulse parameters. Thus, an important question is: can any practical single-photon generation schemes and parameter regimes allow for $\eta_1 \geq p_{\alpha,2}$?

In this section, we will take a step further towards a practical implementation by discussing constraints on $\eta_1$ imposed by basic models for single-photon emission. In particular, we focus on idealised single-photon generation protocols (those that ensure no more than one photon is collected). Experimental considerations for possible implementation, and comparison with the state of the art, will be discussed more in the following section.

## 4.1 Two-level emitter

Driving a two-level emitter with a laser is a common approach to produce single photons. By applying a coherent pulse with a temporal width much less than the lifetime of the emitter, the state of the emitter can be excited from the ground state $|g\rangle$ to the excited state $|e\rangle$ with a high fidelity, allowing spontaneous emission to produce a single photon. Such an excitation scheme can then be applied to an emitter with an additional internal degree of freedom, such as electron spin, to generate photonic graph states encoded in polarisation [21] as discussed in section 2.1.

The main challenge with using a two-level emitter is to separate the scattered single photon from the laser pulse to achieve a high degree of single-photon purity, where the probability of collecting more than one photon is very small. This is done by using excitation schemes where the scattered single photon and laser pulse can be distinguished by a degree of freedom such as polarisation, frequency, or spatial mode. Unfortunately, achieving a high single-photon efficiency using weak excitation pulses necessarily requires a high degree of light-matter coupling, which implies that these degrees of freedom should be as close as possible to improve the mode-matching between the laser pulse and the emitter. Thus, using a scheme based on a two-level emitter immediately introduces a trade-off between the single-photon efficiency and fidelity for a fixed number of photons in the laser pulse.

To get an idea of the practical limit when using a two-level emitter, and to see how well it could perform compared to the upper bound, we choose to distinguish the single photon from the laser pulse using the temporal degree of freedom. This approach is only practical when using very weak excitation pulses, since otherwise any small imperfections in the temporal shape of the laser pulse would very quickly overwhelm the single photon signal and reduce the single-photon purity. This filtering could be accomplished using a fast optical switch or by using detectors with a sufficiently fast gate or high temporal resolution.

The text-book model for exciting a two-level emitter treats the laser using a semi-classical approximation, where it is assumed that the state of the pulse remains in a coherent state throughout the entire light-matter interaction so that only the quantum dynamics of the emitter must be considered. However, when dealing with weak states of light, measuring a single photon scattered off the emitter can induce non-negligible quantum fluctuations in the laser pulse that may alter the quantum dynamics of the excitation process. Luckily, if we temporally filter only single photons that were emitted after the pulse has completely finished interacting with the emitter, causality ensures that the semi-classical approximation will provide an accurate analytic solution for the single-photon efficiency $\eta_1$.

A basic model for a driven two-level emitter using the semi-classical approximation is described by the quantum optical master equation [56] of the form $d\rho(t)/dt = \mathcal{L}(t)\rho(t)$ that governs the evolution of the emitter density operator $\rho(t)$. The generator superoperator is $\mathcal{L}(t) = -i\mathcal{H}(t) + \gamma\mathcal{D}_\sigma$, where $\mathcal{H}\rho = [H, \rho]$ is the action of applying the commutator with the emitter Hamiltonian $H$, $\gamma$ is the emitter decay rate, and $\mathcal{D}_\sigma\rho = \sigma\rho\sigma^\dagger - \sigma^\dagger\sigma\rho/2 - \rho\sigma^\dagger\sigma/2$

(a) Excitation pulse   (b) Two-level emitter   (c) Time-filtered single photon
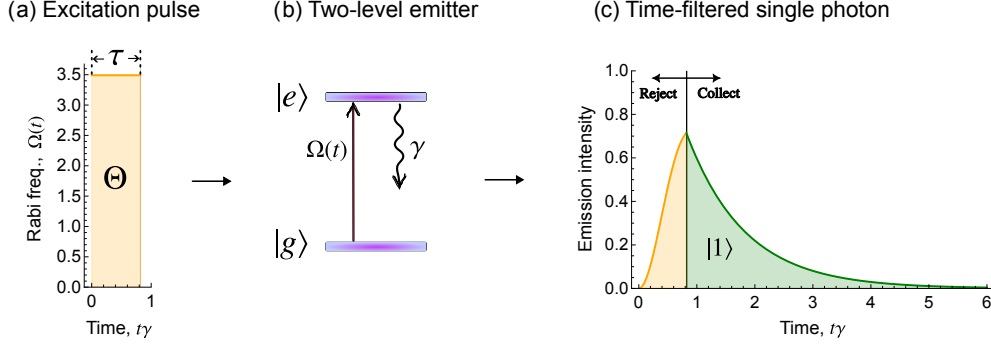
Figure 9: A resonantly driven two-level emitter for producing single photons from a weak coherent state. (a) The square excitation pulse with pulse area $\Theta$ and width $\tau = \Theta^2/(4\gamma|\alpha|^2)$ in a coherent state with average photon number $|\alpha|^2$. (b) A two-level emitter driven by the excitation pulse Rabi frequency $\Omega(t)$ and decaying with rate $\gamma$. (c) The emission intensity quantified by the occupation probability of the two-level emitter, highlighting the excitation and decay steps. By collecting emission after the pulse has finished interacting with the emitter, the emitted light is in a single photon state.

is the dissipation superoperator with $\sigma = |g\rangle \langle e|$ being the emitter lower operator. The Hamiltonian is $H(t) = \Omega(t)\sigma_x/2$, where $\sigma_x = \sigma + \sigma^\dagger$ is the Pauli X operator and $\Omega(t)$ is the excitation pulse Rabi frequency.

To consider the ideal limit for this scheme, where all multi-photon components are fully suppressed, we define $\Omega(t)$ to be a perfect square input pulse beginning at $t = 0$ and ending at $t = \tau$ as illustrated in Figure 9(a). That is, we define the Rabi frequency to be

$$\Omega(t) = \begin{cases} \frac{\Theta}{\tau} & 0 \leq t \leq \tau \\ 0 & t > \tau \end{cases} \tag{11}$$

For ideal light-matter coupling, the Rabi frequency is related to the average number of photons $|\alpha|^2$ by $|\alpha|^2 = \Theta^2/4\gamma\tau$, where $\Theta = \int |\Omega(t)|^2 dt$ is the pulse area. After the pulse excites the two-level emitter, as illustrated in Figure 9(b), we collect only the light found in the output mode for when $t > \tau$ (see Figure 9(c)). [7]

Since for $t \geq \tau$, all multi-photon components will vanish, the single-photon emission probability $\eta_1$ is equal to the occupation probability of the emitter excited state at time $t = \tau$. This can be solved in a straightforward way by taking the matrix exponential of the generator $\eta_1 = \langle e| e^{\tau\mathcal{L}} |g\rangle$, resulting in

$$\eta_1 = 1 - \frac{1}{\gamma^2 + 2\Omega^2}\left[\gamma^2 + \Omega^2 + \Omega^2\left(\cos(\tau\Omega') + \frac{3\gamma}{\Omega'}\sin(\tau\Omega')\right)e^{-3\gamma\tau/4}\right], \tag{12}$$

where $\Omega = \Omega(\tau) = 4\gamma|\alpha|^2/\Theta$ and $\Omega' = \sqrt{(\gamma/4)^2 + \Omega^2}$.

To be sure that the two-level emitter can allow for security amplification, we must check if the probability of generating a single photon $\eta_1$ is greater than the probability of receiving two or more photons $p_{\alpha,2}$. That is, the performance of a generation scheme is determined by the maximum value of $\eta_1$ such that $\eta_1 - p_{\alpha,2}$ is positive.

In the limit $\gamma \ll \Omega$, where $|\alpha|^2 \gg 1$, the expression for $\eta_1$ reduces to $\eta_1 = \sin(\Theta/2)^2$, as expected from the pulse area theorem [57]. In this limit, a $\pi$ pulse corresponding to

---

[7]For the correctness of our protocol we assume that no photon is emitted for $t \leq \tau$. If a photon is emitted during that interval and filtered out, it will always result in a perfectly mixed state at the output. However, the security is not impacted by this filtering since it will at most reduce the information available to Bob.

$\Theta = \pi$ is the optimal condition for excitation. However, this is no longer true when $\gamma \simeq \Omega$, which occurs when $|\alpha|^2$ is on the order of 1. For example, numerically maximising $\eta_1$ over $\Theta$ for $|\alpha|^2 = 1$ implies $\eta_1 = 0.48$ using $\Theta = 0.78\pi < \pi$. By plotting $\eta_1$ maximised for over $\Theta$ as a function of $|\alpha|^2$ (Figure 10), we can identify that $\eta_1 = 0.71$ is the upper limit on the efficiency for this single-photon generation scheme that would still allow for security amplification. This corresponds to an average photon number of $|\alpha|^2 = 2.5$ in the excitation pulse with width of $\tau = 0.82/\gamma$ and area of $\Theta = 0.91\pi$.
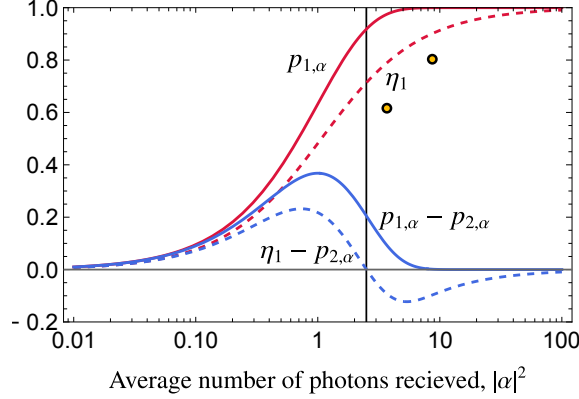


Figure 10: The single-photon efficiency $\eta_1$ (dashed red curve) and gap $\eta_1 - p_{2,\alpha}$ (dashed blue curve) where a positive value $\eta_1 - p_{2,\alpha} > 0$ indicates security amplification is possible. The solid curves show the upper bounds on single-photon efficiency $p_{1,\alpha}$ and corresponding gap $p_{1,\alpha} - p_{2,\alpha}$ set by the coherent state photon number statistics. For a two-level emitter driven by a square pulse, the maximum efficiency while allowing for security amplification is $\eta_1 = 0.71$ (vertical black line) corresponding to the average number of photons $|\alpha|^2 = 2.5$, pulse area $\Theta = 0.91\pi$, and pulse width $\tau = 0.82/\gamma$. The points indicate experimentally measured values from Ref. [58].

Note that one could reduce the amount of time filtering to increase $\eta_1$ at the cost of accepting more multi-photon cases that reduce the single-photon purity, which introduces an efficiency-fidelity trade-off. However, an accurate simulation of this case requires capturing the quantum fluctuations of the excitation pulse, which can be accomplished following a collision model approach [59] or a quantum cascaded interaction [60].

## 4.2 Saturating the upper-bound via alternative energy level structures

The scheme analysed in the previous section gives a concrete idea of how to satisfy the criteria for security amplification using an excitation scheme that can be directly applied to protocols for deterministic graph state generation, but it is not the only approach to generating a single photon from a weak coherent state nor is it the most efficient. It may be possible to improve $\eta_1$ by using a cavity to control the light-matter coupling or by altering the shape of the coherent pulse. But it is not easy to see how to attain the upper bound $\eta_1 = p_{1,\alpha}$ using just a two-level emitter, or that it is even possible in general. Interestingly, it is possible to reach the upper bound by increasing the complexity of the emitter energy level structure.

The upper bound $p_{1,\alpha}$ can be reached by considering a system with just one additional ground state $|s\rangle$ that is detuned from $|g\rangle$, so that we have a three-level $\Lambda$ type energy level structure (see Figure 11(a)). If the $\Lambda$ system is initially in the ground state $|g\rangle$, a coherent pulse can be used to excite the system to state $|e\rangle$. As soon as a single photon is emitted by the system due to the decay of $|e\rangle$ to $|s\rangle$, the system is no longer coupled by the excitation pulse and thus cannot be re-excited. Therefore, by filtering the emission in frequency, the
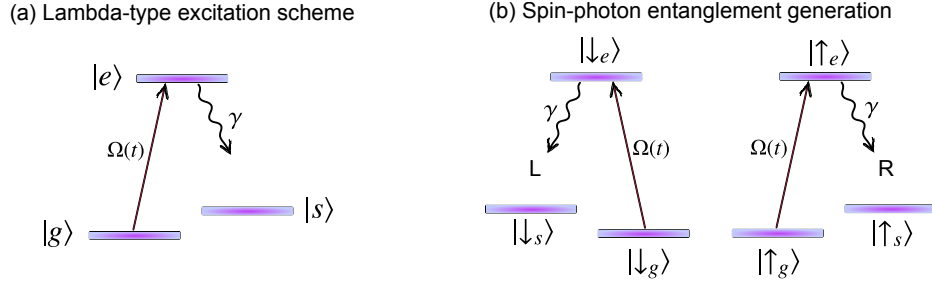
Figure 11: (a) Single-photon generation using a $\Lambda$-type emitter. The excitation and collection transitions are independent and distinguishable in resonant frequency. Excitation occurs by driving $|g\rangle$ to $|e\rangle$ with the Rabi frequency $\Omega(t)$. Emission from $|e\rangle$ to $|s\rangle$ dominates at the rate $\gamma$, decoupling the system from the laser as soon as a single photon is produced. (b) Application of the $\Lambda$-type excitation for producing spin-photon entanglement to generate photonic graph states of qubits encoded in left (L) and right (R) circular polarisation.

multi-photon emission probability can be fully suppressed without sacrificing the single-photon probability. This allows for moving arbitrarily close to the upper bound $p_{1,\alpha}$ by simply increasing the quality of mode matching between the excitation pulse and the excitation transition, and also by engineering the decay of the system so that the transition $|e\rangle$ to $|s\rangle$ is much more likely than the transition $|e\rangle$ to $|g\rangle$.

Although the $\Lambda$ scheme can be brought arbitrarily close to the upper bound $p_{1,\alpha}$ allowing for security amplification while asymptotically reaching perfect efficiency $\eta_1 \to 1$, it is more difficult to work with and control physical systems that allows for two such $\Lambda$ configurations, which would be necessary to deterministically generate photonic graph states (see Figure 11(b)). The excitation scheme also favours temporally long pulses, which may negatively impact computational rate. However, this level structure has already been used to generate entangled photonic graph states using a single rubidium atom in an optical cavity [25].

## 4.3 Paths towards experimental implementations

The excitation of quantum dots using weak laser pulses has already been realised in [58]. They demonstrated that a coherent state with an average of 3.8 (8.6) photons was able to invert the transition of a quantum dot exciton with a 62% (81%) probability. Comparing these values to the predictions from Figure 10, Section 4.1, indicates that these inversion probabilities are not yet sufficient to allow for security amplification, but the trend is favourable and shows that proof-of-concept experiments may be feasible with current technology. It is important to note however that in Ref. [58] they use resonant excitation to maximise light-matter coupling and thus require polarisation filtering to separate the single photons from the excitation pulse. This pulse-filtering method is not compatible with the spin-polarisation entanglement which we use to generate graph states. Hence further developments and experimental proposals are required.

The Lindner-Rudolph protocol for generating spin-polarisation entanglement using quantum dots has been experimentally demonstrated in Refs. [23–25, 61]. For example, in Ref. [23], three horizontally-polarised laser pulses are used to generate a spin-photon-photon linear cluster state. A similar protocol and setup, adding only a controlled polarisation to the second pulse, can be used to perform a proof-of-concept experiment to confirm that the emission can indeed be described by the operator $E_{qe}(\theta)$. However,

this technique uses high-energy off-resonant excitation pulses [62], meaning that the laser power is too high to amplify security and recover blindness.

Many approaches could be used to reduce excitation power while still producing entangled states of light. As demonstrated theoretically in Section 4.1, a resonant excitation with a fast laser pulse and temporal filtering can, in principle, allow for security amplification. Furthermore, in the schemes described above, the excitation pulse must pass through a highly-reflective cavity mirror before interacting with the quantum emitter. Using multi-frequency excitation pulses as in the SUPER scheme [63, 64], or exciting the source along a spatial axis which is different from the predominant emission direction, could by-pass this limitation and thus reduce the required pump power. This second approach would also allow for spatial filtering. Finally, as discussed in Section 4.2, emitters with a more complex energy level structure would open new avenues to engineer energetically efficient deterministic entanglement generation schemes.

## 5 Conclusion and future work

In this paper, we presented a protocol that greatly reduces the technological requirements for performing blind and secure delegated quantum computations. Not only does the client no longer require a single qubit source or measurement device, but the server does not need to perform complex operations such as measuring the photon number without disturbing the photons' polarisation, or performing photon-photon entangling gates. All that the server requires is interacting quantum emitters which can generate spin-photon entanglement. Our protocol is information-theoretically secure, as proven in the composable security framework of Abstract Cryptography.

However, the security analysis relies on very pessimistic assumptions. In particular, we assume that all information about an angle is leaked so long as a laser pulse contains more than one photon. This requires the server to isolate the photons contained in a pulse and manipulate them individually, which is challenging in itself, but it also overestimates the amount of information that the server can gain from these states. Relaxing this assumption or redefining security in a less drastic way (in terms of distinguishing advantage, or including a more comprehensive study of leakage) would yield an improved security bound. Another path would be to randomise the states even more.

Then, in the current work, we use 2D graph structures which are sufficient for universal blind quantum computing. Expanding these results to 3D graphs which also enables fault-tolerance would be an interesting direction to handle both photon losses and the server's honest processing errors [65].

Finally, our analysis in Section 4.2 leaves a very interesting open question: which physical systems and practical excitation schemes can allow for energetically efficient deterministic photonic graph state generation to optimise security amplification? Although a definitive answer to this question goes beyond the scope of this work, we believe that frameworks such as microscopic quantum energetics [66–68] can be readily applied to solve this problem.