Certifying the Presence of a Photonic Qubit by Splitting It in Two

Evan Meyer-Scott,1,* Daniel McCloskey,1 Klaudia Gołos,1 Jeff Z. Salvail,1 Kent A. G. Fisher,1 Deny R. Hamel,2 Adán Cabello,3 Kevin J. Resch,1 and Thomas Jennewein1,4

1Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Ave W, Waterloo, Ontario, Canada N2L 3G1
2Département de physique et d’astronomie, Université de Moncton, 18 avenue Antonine-Mailet, Moncton, New Brunswick, Canada E1A 3E9
3Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain
4Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, Ontario, Canada M5G 1Z8

(Received 15 October 2015; revised manuscript received 19 December 2015; published 16 February 2016)

We present an implementation of photonic qubit precertification that performs the delicate task of detecting the presence of a flying photon without destroying its qubit state, allowing loss-sensitive quantum cryptography and tests of nonlocality even over long distance. By splitting an incoming single photon in two via parametric down-conversion, we herald the photon’s arrival from an independent photon source while preserving its quantum information with up to (92.3 ± 0.6)% fidelity. With reduced detector dark counts, precertification will be immediately useful in quantum communication.

DOI: 10.1103/PhysRevLett.116.070501

Introduction.—Learning if and when a photon has arrived at a receiver without destroying it is fundamentally difficult [1]. Yet over reasonable transmission distances, this is required by advanced quantum communication protocols such as device-independent secure communication [2,3], private secure randomness amplification [4], and fundamental tests of nonlocality [5]. These proposals fail in the presence of even moderate channel losses, but can be made practical with techniques that circumvent the effects of loss by certifying that the quantum system is ready after transmission. This certification is an attractive alternative to the nearly impossible task of eliminating fundamental transmission loss mechanisms.

One approach using traditional destructive photodetection is entanglement swapping [6], which certifies that stationary quantum systems such as spins are ready in the desired quantum states [7]. This method has recently been applied to nitrogen-vacancy centers for a loophole-free violation of Bell’s inequality [8]; however, the synchronization and indistinguishability of photons from disparate sources required for entanglement swapping is difficult to achieve, and low photon collection efficiencies from the stored quantum systems lead to low experimental rates.

Thus, we look to nondestructive optical methods of certifying a photon’s arrival to indicate the photon itself is ready. One technique is heralded qubit amplification [9–12], which uses ancilla photons interfering with the signal photon and specific detection patterns to herald the signal’s arrival. This technique requires synchronization between distant and indistinguishable photon sources and as such implementations to date have not employed a separated source and receiver [13–15]. Similarly, quantum nondemolition measurements based on cavity quantum electrodynamics and cross-phase modulation have stringent requirements on incoming photons and low repetition rates [16–19].

A promising solution for heralding the arrival of a lossy photon is photonic qubit precertification, proposed by Cabello and Sciarrino [20]. Precertification does not require synchronization or indistinguishability, and acts directly on flying photonic qubits. Precertification is applicable to both photonic and spin-photon entanglement, where it can overcome low coupling efficiencies out of quantum emitters.

The sender, Alice, transmits a photonic qubit encoded in polarization to the receiver, Bob. Bob splits the incoming photon into two photons, labeled flag and signal, through polarization-preserving single-photon parametric down-conversion (PDC) [21,22] as shown in Fig. 1. Since the flag photon is never produced without the corresponding signal photon, the detection of the flag precertifies the presence of the signal. The configuration is such that the signal photon bears the same quantum information initially encoded by Alice. The wavelength of Alice’s photon must match the acceptance band of Bob’s down-conversion crystal.

FIG. 1. Photonic qubit precertification. Alice sends a photonic qubit through a lossy channel to Bob, where it undergoes polarization-preserving parametric down-conversion, producing a photon pair with some probability. The flag photon is detected to precertify the signal, which carries the initial qubit state. For half the flag detections, a feed forward phase correction (ϕ) is needed on the signal.
Here we report a proof-of-principle implementation of photonic qubit precertification with separated source and receiver. We demonstrate that qubit states are preserved during precertification by performing process tomography, and measurements of heralding efficiency show how our device could become useful in device-independent quantum communication.

**Experiment.**—Polarization-preserving PDC has the Hamiltonian

$$H_{\text{PDC}} = \gamma (a_H a_H^\dagger + a_V a_V^\dagger + a_H^\dagger a_H + \text{H.c.}),$$

where $\gamma$ determines the probability of down-conversion, the subscripts $i$, $f$, and $s$ refer to the input, flag, and signal modes, respectively, $H$ and $V$ label two orthogonal polarization modes, and H.c. denotes the Hermitian conjugate.

Unlike typical PDC, the pump is a single photon and cannot be treated classically. This Hamiltonian preserves the qubit state by mapping $|H_i\rangle \rightarrow |H_f\rangle |H_s\rangle$ and $|V_i\rangle \rightarrow |V_f\rangle |V_s\rangle$. Thus, an arbitrary polarization input state $|\psi\rangle_i = \alpha |H_i\rangle + \beta |V_i\rangle$ down-converts as

$$\alpha |H_i\rangle + \beta |V_i\rangle \rightarrow \alpha |H_f\rangle |H_s\rangle + \beta |V_f\rangle |V_s\rangle.$$

Writing the flag mode in the diagonal basis, with $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$, gives

$$\alpha |H_i\rangle + \beta |V_i\rangle \rightarrow \frac{1}{\sqrt{2}} (\alpha |D_f\rangle + |A_f\rangle) |H_s\rangle + \beta (|D_f\rangle - |A_f\rangle) |V_s\rangle$$

$$= \frac{1}{\sqrt{2}} (|D_f\rangle (\alpha |H_s\rangle + \beta |V_s\rangle) + |A_f\rangle (\alpha |H_s\rangle - \beta |V_s\rangle)).$$

Detecting the flag qubit in $|D_f\rangle$ or $|A_f\rangle$ thus precertifies the signal qubit in the desired state, with an extra phase flip in the case of an $|A_f\rangle$ detection. The scheme works equally well if the input qubit is part of an entangled state, mapping its entanglement to the signal qubit after precertification [20]. This scheme does not violate the no-cloning theorem [23], as measuring the flag photon in the diagonal basis provides no information on the coefficients $\alpha$ and $\beta$ [20]. In fact, the input qubit state is shared across the flag and signal photons, such that neither photon in isolation can reproduce an unknown input qubit state.

Our experimental setup (Fig. 2) comprises a source (Alice) and receiver (Bob) in separate labs with no communication except the quantum channel. Alice prepares photonic qubits through type-II down-conversion to a 776 nm wavelength in periodically poled potassium titanyl phosphate. Alice’s photons are produced in pairs with orthogonally polarized photons, which are split off at the PBS and detected at D5 to enable measurement of the heralding efficiency after precertification. Alice’s prepared photons are sent through a 30 m optical fiber to Bob, where he performs precertification by down-converting the incoming photon in a polarization-based Mach-Zehnder interferometer, where one path down-converts $|H_i\rangle$ and the other $|V_i\rangle$ in periodically poled type-0 lithium niobate waveguides [24]. The interferometer is stabilized using a reference laser at 780 nm to control fiber stretchers. The flag and signal photons centered at 1540 and 1564 nm, respectively, are split in a wavelength-division multiplexer. The flag photon is projected onto $|D_f\rangle$ or $|A_f\rangle$, with a half-wave plate, quarter-wave plate, and polarization beam splitter, then detected with superconducting nanowire single photon detectors from Quantum Opus, LLC. The $|D_f\rangle$ or $|A_f\rangle$ outcome is fed forward to a Pockels cell, which performs the phase correction for $|A_f\rangle$. Flags necessary to restore the signal photon to the input polarization state ($|H_s\rangle \rightarrow |H_f\rangle$, $|V_s\rangle \rightarrow -|V_f\rangle$). The qubit state of the signal photon is analyzed, and it is also detected by nanowire detectors.

To record data, detections $D1$–$D4$ are registered as time-tags in a coincidence logic unit from UQDevices, Inc. Alice’s detection $D5$ (silicon avalanche photodiode) is not time-tagged, but counting rates from $D1$–$D5$ are recorded on a separate logic unit to measure heralding efficiencies. The loss in count rate induced by precertification is 76 dB, 55 dB from PDC efficiency, and the rest from optical losses. We determine the loss by comparing Bob’s certified pair rate $(D1\lor D2)\land (D3\lor D4)$ (1100 events/h), with the single detection rate when the qubit is measured directly by Alice $(1.2 \times 10^3$ counts/s). Here we define coincident detections using logical notation: $D_i \land D_j$ means logical AND between detectors $i$ and $j$, and $\lor$ means logical OR. Bob’s detection.
efficiencies [25] are 10%, 14%, 19%, and 19%, for D1–D4, respectively, with respective dark count rates per second of 550, 160, 1500, and 1000.

Interestingly, the precertification stage is perhaps the weakest-pumped entangled photon pair source ever built, yet maintains a high signal-to-noise ratio (229:1) as seen in Fig. 3.

Results.—To characterize the performance of qubit precertification, we performed quantum process tomography [26,27] in the qubit subspace by inputting 6 polarization states, and performing tomographically over-complete measurements on the signal for each input. These data were inverted by a maximum-likelihood method [28] to reconstruct the process matrix [29]. A perfect qubit precertification would perform only the identity, directly mapping any qubit state from input to heralded output. As seen in Fig. 4(a), our qubit precertification indeed performs the identity, or a phase flip for heralding on |A⟩f, with fidelities [30] of (92.3 ± 0.6)% and (93.2 ± 1.0)% respectively. For this data set, detector D1 was turned off. We do not subtract background counts, and uncertainties are determined by Monte Carlo simulations assuming Poissonian counting noise.

We can correct the phase flip using feed forward: a detection of |A⟩f requires a π phase, implemented by applying the half-wave voltage to the Pockels cell. Now in Fig. 4(b), both |D⟩f and |A⟩f flag detections result in the identity on the qubit state, with (84.7 ± 0.6)% fidelity. Here, both detectors D1 and D2 are used. The lower fidelity is due to imperfect phase corrections of the Pockels cell.

We subsequently added loss to the channel between Alice and Bob to quantify how the precertified qubit state degrades and to compare with direct transmission. In Fig. 5 we plot the count rate and Bob’s measured qubit fidelity for |H⟩i and |D⟩i input states. Here the total loss is given in terms of the probability of a photon arriving at the final detector p, and includes all losses after the photon is coupled into Alice’s fiber. For direct transmission, the count rate [Fig. 5(a)] is the number of coincidences/s of D5∧(D1∧D2), with D1 and D2 replaced by silicon avalanche photodiodes (with the same efficiency and half the dark counts) and the precertification stage removed. With precertification, the count rate is the triple coincidences/s D5∧(D1∧D2)∧(D3∧D4). As seen in Fig. 5(b) the qubit fidelity drops rapidly for direct transmission, whereas the precertified qubit retains a fidelity of 88% at 80 dB total loss or 4 dB added channel loss. As PDC efficiencies improve with novel materials and engineering, the precertification protocol will be able to tolerate higher channel losses while preserving qubit states.

Our rate of precertified photon-pair detection events with 30 m separation and no added channel loss is 0.3 s⁻¹. This is limited by the efficiency of the precertification process of −76 dB (PDC efficiency of −55 dB, optical coupling before PDC of −6 dB, optical coupling for each the flag and signal after PDC of −5 dB for a total of −10 dB, and detector efficiencies for the flag of −5 dB). The signal detectors have −2 dB efficiency, not included in the precertification loss.

Our measured heralding efficiencies after precertification, defined as the probability of a signal detection by Bob ⟨D3∧D4⟩ given a detection by Alice ⟨D5⟩ and a flag detection ⟨D1∧D2⟩, are presented in Fig. 6. The heralding efficiency ηh can be approximated as

FIG. 3. Timing histogram for twofold coincidences between Bob’s flag and signal detectors D2∧(D3∨D4), for the precertification stage pumped by single photons (equivalent to 1 pW average power). The 2.3 ns (diameter) coincidence bin used in the experiment is marked with dashed lines.

FIG. 4. Reconstruction of real parts of qubit subspace process matrices for precertification. I is the identity, and X, Y, and Z are the Pauli matrices. Process fidelities to the identity Ff are given under each matrix, and imaginary parts are small (absolute values < 0.2). (a) Without phase correction, the process fidelity depends on the flag detection. When heralding on state |A⟩f, the process has (93.2 ± 1.0)% fidelity to Z but (3.1 ± 0.4)% fidelity to I. heralding on either |D⟩f or |A⟩f gives a mixed channel, with (95.4 ± 0.3)% fidelity to (I + Z)/2. (b) With feed forward phase correction, the process is nearly the identity independent of the flag detection pattern.
where $\eta_{\text{signal}}$ is the total efficiency of the signal photon after Bob’s PDC, including coupling and detector efficiencies, and $(p_{\text{dark}}/p_{\text{flag}})$ is the ratio of dark counts in the flag detector to detected flag photons, where both are triggered by Alice’s $D5$ detection. Our heralding efficiencies are limited mostly by dark counts in the flag detectors (large $(p_{\text{dark}}/p_{\text{flag}})$), and partially by optical losses after precertification (small $\eta_{\text{signal}}$). The former could be drastically improved by blackbody filters in the flag detector [31], bringing $\eta_{h} \approx \eta_{\text{signal}} = 19\%$ for our system. The coupling efficiency $\eta_{\text{signal}}$ could be improved with low-loss optical components or a chip-based architecture [32]. Therefore, in Fig. 6 we also show simulated heralding efficiencies given flag detectors with 1 dark count/s, 10% system efficiency, and 100 ps jitter, and also with $10^{-3}$ dark counts/s and 2.3% efficiency as recently demonstrated for 1550 nm [33]. For the latter case we assume 80% coupling efficiency from the precertification to the detectors [34,35], and 90% efficient signal detectors [36,37].

For qubit precertification to be a viable alternative to entanglement swapping, the heralding efficiency must be large enough to close the detector loophole, with a lower bound of 66% for symmetric detection efficiency between Alice and Bob [38]. The simulated heralding efficiency after precertification with $10^{-3}$ darks/s and improved coupling does not drop below 66% until 35 dB channel loss, making such a system practical for long-distance device-independent quantum communication, for example, over 144 km in free space [39]. For optical fiber transmission, a 35 dB channel loss allows 10 km transmission at 780 nm, which could be improved to 175 km by moving to 1550 nm, which could be possible using four-wave mixing instead of PDC.

**Conclusions.**—We have presented a proof-of-principle demonstration of photonic qubit precertification. Our device maintains the input qubit state with (92.3 ± 0.6)% process fidelity to the identity, or (84.7 ± 0.6)% with feed forward phase correction. Our heralding efficiency after precertification, up to $1 \times 10^{-3}$, can be immediately improved with low-noise detectors, and by improvements in optical components. It could also be possible to engineer phase matching in a single crystal or in a cascaded configuration [40] to eliminate the entanglement between flag and signal photons, and, therefore, remove the need for feed forward phase correction.

Our precertification rate of 0.3 s$^{-1}$ compares favorably to state-of-the-art entanglement swapping and quantum repeater experiments that achieved entanglement detection rates of $1.3 \times 10^{-3}$ s$^{-1}$ with 3 m separation in diamond [41], and $9 \times 10^{-3}$ s$^{-1}$ over 20 m using rubidium atoms [42].

Future improvements in splitting efficiency, improving the rate and tolerable losses, are expected from advanced waveguide [43] or resonator [44] engineering, or by moving to four-wave mixing in materials that allow all operations at telecommunications wavelengths, for example, in silica fibers [45–47], chalcogenide fibers [48,49], on-chip wave guides [50], or resonators [51,52]. These improvements and the applicability of precertification to both entangled-photon and spin-photon systems will make it a useful tool in long-distance quantum communication.

We are grateful to Sae Woo Nam, Antía Lamas Linares, and Fabio Sciarrino for helpful discussions and to Aaron Miller of Quantum Opus, LLC. We acknowledge support from the Natural Sciences and Engineering Research
Council of Canada, Canada Research Chairs, Industry Canada, the Canada Foundation for Innovation, Ontario Research Fund, the New Brunswick Innovation Foundation, the FQXi large grant project “The Nature of Information in Sequential Quantum Measurements,” (A.C.), and Project No. FIS2014-60843-P 278 (MINECO, Spain) with FEDER funds (A.C.).

emeyersc@uwaterloo.ca