Review

Single photons for quantum information systems

Yoshihisa Yamamoto[1], Charles Santori[2], Glenn Solomon[3], Jelena Vuckovic[4], David Fattal[5], Edo Waks[6], Eleni Diamanti[7]

[1]*National Institute of Informatics*

[1, 2, 3, 4, 5, 6, 7]*E.L. Ginzton Laboratory, Stanford University*

[1, 2, 3, 4, 5, 6, 7]*Quantum Entanglement Project, SORST, JST*

ABSTRACT

This paper reviews the current state of single-photon sources based on the semiconductor quantum dots that will play a central role in future quantum information systems. By optically pumping a system consisting of a semiconductor single quantum dot confined in a monolithic microcavity, it is possible to produce a single-photon pulse stream at the Fourier transform limit with high efficiency and a high repetition rate. This technique is not only useful for BB84 quantum cryptography using single photons, but will also find applications in other quantum information systems such as BBM92 quantum cryptography using entangled photon pairs, quantum teleportation, quantum repeaters, and linear optical quantum computers.

KEYWORDS

single-photon source, quantum dot, microcavity, Fourier transform limit, EPR-Bell state, two-photon interference, quantum cryptography, quantum teleportation, quantum repeater, quantum computation

1 Introduction

The protection of privacy in secure communications and the ability to analyze complex problems by high-power computers will be increasingly important issues in the fields of information science and physical science in the 21st century. The former is required to guarantee the security of personal information in telecommunications and computer systems, and the latter is essential in the design of computer hardware and software that can process very large amounts of data in such applications as predicting weather patterns, analyzing biological phenomena, controlling traffic, and predicting economic fluctuations.

Received December 6, 2004; Revised January 29, 2005; Accepted January 31, 2005.

{1)yyamamoto, 3)solomon, 4)jela, 5)dfattal, 6)edo, 7)ediam}@stanford.edu, 2)charles.santori@hp.com

Quantum information science has progressed rapidly in recent years in the context of efforts to address these needs. Although it is very hard to predict exactly how the field will develop in the future, it seems clear that as far as a hardware is concerned, important roles will be played by photonic qubits for quantum communication, nuclear spin qubits for quantum memory, and electron spin qubits for applications linking the above two areas. This paper reviews the latest research trends relating to the production of photonic qubits for quantum communication and computation, with particular reference to the results obtained by the author's group.

In BB84 quantum cryptography,[1] the security of systems that involve quantum communication using an ordinary Poisson light source (such as a semiconductor laser) can be threatened by an eavesdropper's photon-splitting attack (i.e., the process of secretly

extracting and measuring a single photon when there are two or more photons in a pulse).[2] In the Ekert91 or BBM92 protocols for quantum cryptography using EPR-Bell photon pairs,[3] bit errors occur due to the presence of two or more photon pairs per pulse.[4] Hopes are therefore pinned on the development of a light source that can generate single photons or single EPR-Bell photon pairs at a definite time.

Schemes have been proposed for implementing photonic quantum information-processing techniques that are more advanced than quantum cryptography, such as quantum teleportation,[5] quantum repeaters,[6] and linear-optic quantum computers.[7] For such applications, it is essential to generate a large number of single photons at definite time intervals that satisfy the condition of "quantum indistinguishability."

Various methods are currently being investigated for the production of single photons at definite time intervals, including those based on a single atom[8], an atomic ensemble[9], a single trapped ion[10], single molecules[11],[12] or single solid-state lattice defects (diamond color centers)[13],[14]. However, the results of these studies have yet to satisfy various conditions such as high efficiency, high speed, and single-mode operation.

The author's group has previously proposed and verified a method for producing single photons regularly using the Coulomb blockade effect in a micro-pin junction with a quantum well as the active layer.[15],[16] However, the following three problems made it difficult to use this turnstile device in practical systems:

1)To realize the Coulomb blocking effect for a single electron and hole, the device has to be operated at the extremely low temperature of 50 mK.
2) The electron-hole pairs have a long radiative recombination lifetime of 25 ns, making it impossible to operate the device at high repetition rates.
3) The photons are radiated in random directions, resulting in poor efficiency in coupling to an external optical system.

One conceivable method of addressing these problems is to generate single photons using excitonic emission from a single semiconductor quantum dot excited by a pulse of light. The following experiments will be discussed in this paper: generation of a stream of single photons from a single quantum dot,[17] use of a DBR post microcavity to increase external coupling efficiency,[18] generation of a stream of single photons whose spectral width and pulse width are at the Fourier transform limit,[19] experiments in which single photons at this Fourier limit are regarded as indistinguishable single-quantum particles (two-photon interference phenomenon)[20] and BB84 quantum key distribution experiments using single photons generated in this manner[21], conversion of indistinguishable single photons to entangled photon-pairs by post-selection,[22] and quantum teleportation using indistinguishable single photons. [23]

High-efficiency and low-noise detection of single photons is another crucial technique for implementing various photonic quantum information systems. A Si avalanche photodiode (APD) is routinely used to detect single photons in the visible to near-infrared wavelengths. There are two drawbacks to this device in terms of quantum information applications: one, it cannot distinguish an exact photon number, and two, it cannot detect single photons at telecommunication wavelengths of 1.3-1.6 μm. This paper also reviews the latest research trends in the detection of single photons. The following two detection schemes will be discussed: photon-number distinguishing detectors based on the Si visible light photon counter (VLPC) [24]-[27] and single-photon frequency up-conversion in periodically poled $LiNb0_3$ (PPLN) waveguides.[28]

2 Generation of single photons[17]

2.1 Photon –photon correlation

The second-order coherence function of an optical field that characterizes the difference between a single-photon source and an ordinary laser source is defined by the following equation:

$$g^{(2)}(\tau) = \frac{\left\langle a^{+}(t)a^{+}(t+\tau)a(t+\tau)a(t)\right\rangle}{\left\langle a^{+}a\right\rangle^{2}}$$

where $a(a^{+})$ is the photon annihilation (creation) operator.

Figure 1 shows the results of measurements of an optical pulse stream from a mode-locked Ti:sapphire laser. A Hanbury Brown and Twiss optical intensity interferometer (described below) was used to make these measurements. The experimental results shown in Fig. 1 represent the histogram of photons detected at other times when a single photon was detected at time $t=0$. Since all peaks including the peak at $t=0$ are equal in height, this figure shows that when a single photon is detected in the pulse that arrives at time $t=0$, the probability that a second photon will be detected in the same pulse is equal to the probability that the first photon will be detected in a pulse that arrives at another time. This is a unique characteristic of optical pulse streams where the photon numbers obey a Poisson distribution.

In the case of a super-Poisson light source where the distribution of photon numbers is wider than a Poisson distribution, the probability that a second photon will be detected in the same pulse in which a single photon

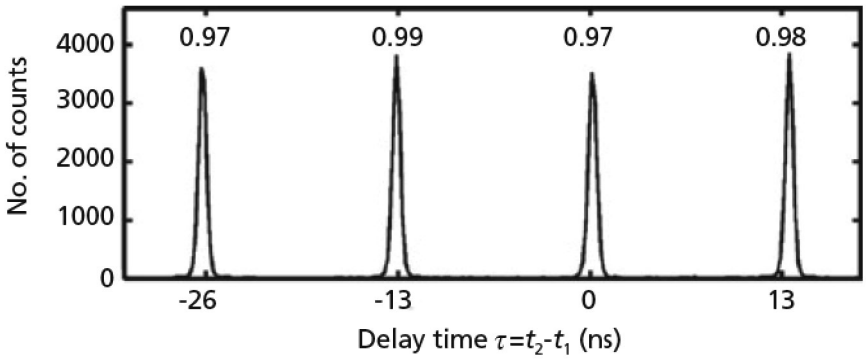


Fig. 1 $g^{(2)}(t)$ measurement results for a Poisson light source (pulse stream from a Ti:Al2O3 laser)

is detected is greater than the probability that the first photon will be detected in another pulse. This phenomenon is called photon bunching, and this characteristic is exhibited by light emitted from a thermal light source. This characteristic originates from the stimulated emission of photons. Conversely, in the case of a sub-Poisson light source where the distribution of photon numbers is narrower than a Poisson distribution, the probability that a second photon will be detected in the same pulse in which a single photon is detected is less than the probability that the first photon will be detected in another pulse. This phenomenon is called photon antibunching. Since each pulse obtained from a single-photon source always consists of a single photon, $g^{(2)}(\tau)$ is given by the following equation:

$$g^{(2)}(\tau)=\begin{cases}0\ (\tau=0)\\ 1\ (\tau=nT)\end{cases}$$

where T is the light pulse repetition interval and n is a non-zero integer.

2.2 Emission spectrum from a single quantum dot

Figure 2 shows an AFM image of self-assembled InAs/GaAs quantum dots produced by molecular beam epitaxy (MBE). By setting a high deposition temperature, it is possible to reduce the surface density of quantum dots. Using a combination of electron beam lithography and dry etching techniques to pro-

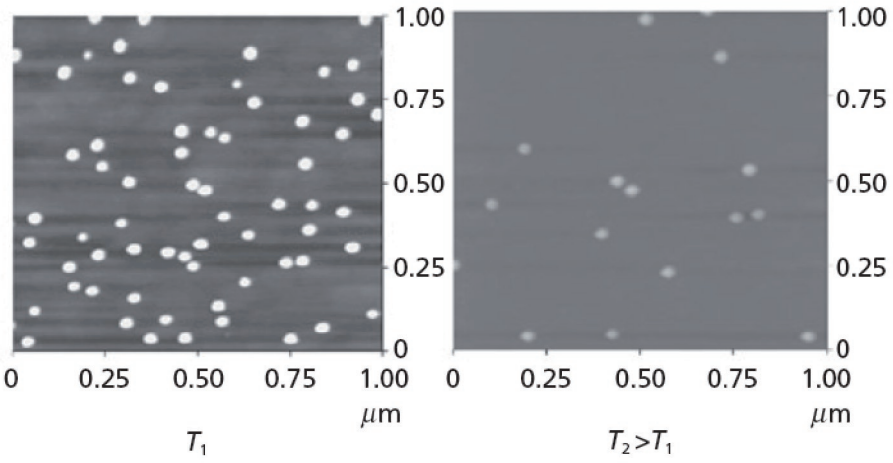


Fig. 2 AFM image of self-assembled InAs/GaAs quantum dots made by MBE deposition

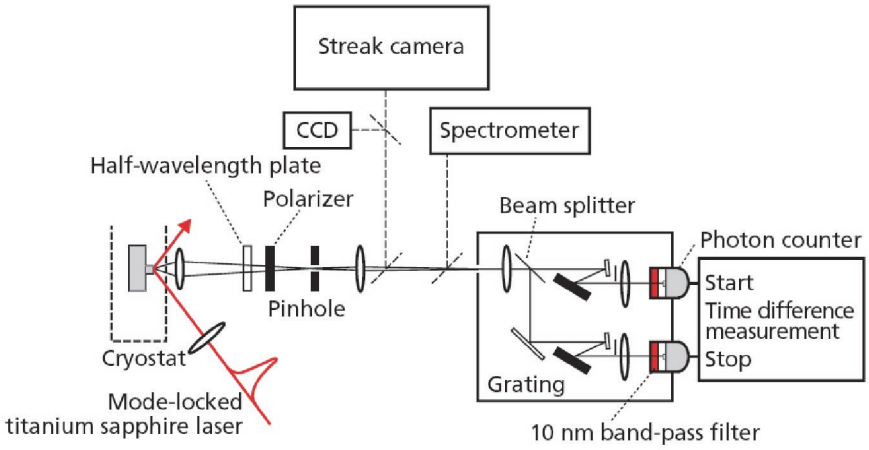


Fig. 3 Single-quantum dot light emission measurement system

cess this wafer into posts with a diameter of 0.2 μm, it is possible to optically excite a single quantum dot in isolation. This experimental step is shown in Fig. 3. The temporal response and the spectral characteristics were measured with a streak camera and a grating spectrometer. The Hanbury Brown and Twiss interferometer used to measure $g^{(2)}(\tau)$ consists of a 50-50% beam splitter, an optical band-pass filter, a single-photon-counting Si APD (SPCM), and a delay-time measuring circuit.

Figure 4(a) shows the emission spectrum of the lowest transition line (1 e-1 h) in the case in which optical pumping is performed at a higher energy than that of the GaAs band gap. The emission patterns from different quantum dots exhibit basically the same pattern except for relative shifts in wavelength. Emission

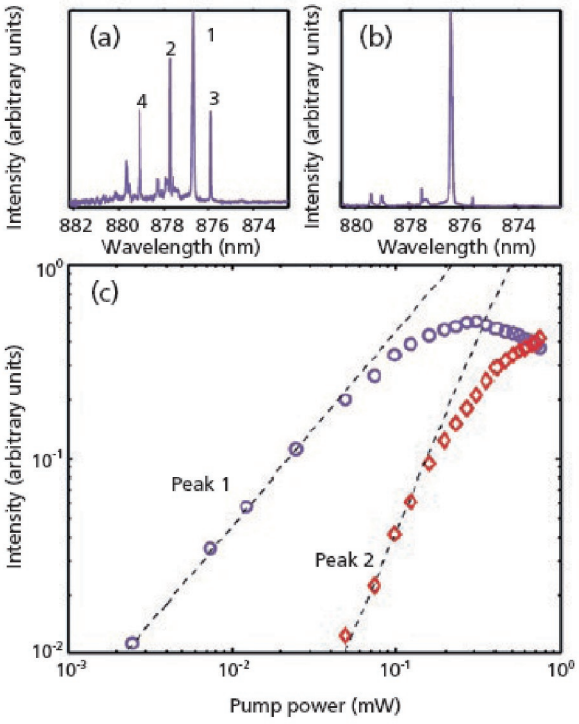


Fig. 4 (a) Emission spectrum from an InAs single quantum dot excited at energies higher than the GaAs band gap. (b) Emission spectrum from an InAs single quantum dot when the second quantization level is resonantly excited. (c) Variation of emission intensity with CW pump power for emission lines 1 (○) and 2 (◇).

peaks 1 and 2 correspond to single-exciton and biexciton emissions from a neutral quantum dot, respectively. The emission wavelength difference results from multiple carrier interactions, and correspond to the exciton molecule binding energy. Emission peaks 3 and 4 indicate the exciton (trion) emission from quantum dots that have trapped a hole and an electron, respectively.

Figure 4(b) shows the emission spectrum from the lowest transition line (1 e-1 h) when an InAs quantum dot is excited by resonant optical pumping to the second transition line (2 e-2 h). It is known that resonant optical pumping can suppress emission peaks 3 and 4 from the quantum dot. This feature holds important significance for the realization of a single-photon source at the Fourier transform limit as described below.

Figure 4(c) shows that in the low pumping region emission peaks 1 and 2 increase in proportion linearly and quadratically relative to pumping intensity. The respective emission dependences on pump power support an interpretation involving exciton and biexciton emissions. These experimental results are obtained under CW pumping, and when the steady-state aver-

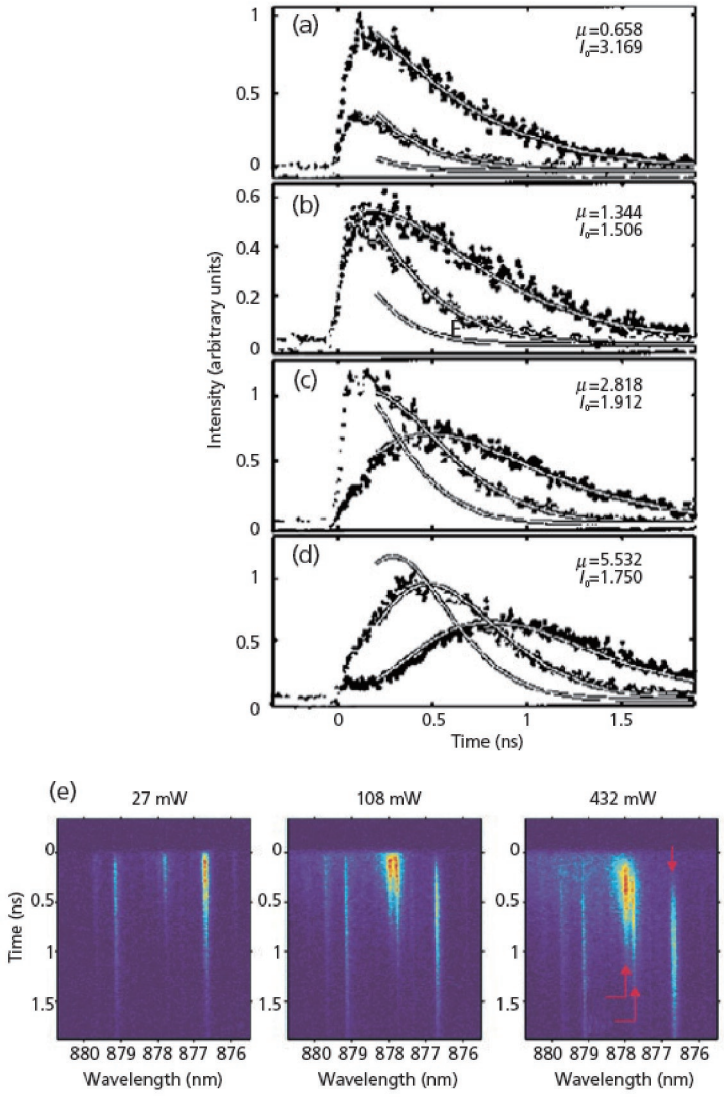


Fig. 5 Delay characteristics of exciton emission, biexciton emission, and triexciton emission with pump pulse intensities of (a) 27 μW, (b) 54 μW, (c) 108 μW, and (d) 432 μW. Here, μ is the average number of excitons at time $t=0$, and I_0 is a parameter proportional to detection efficiency. (e) Time delay vs. wavelength characteristics of light emission from a single quantum dot, as observed with a streak camera.

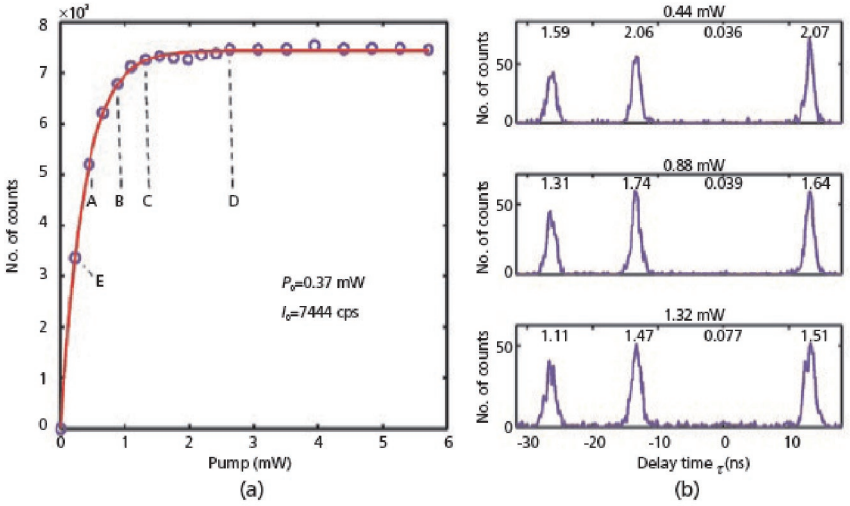


Fig. 6 (a) Exciton emission intensity vs. optical pump power. (b) Results of measuring $g^{(2)}(\tau)$ of exciton emissions from a single quantum dot at various different optical pump intensities.

age number of excitons in the quantum dot exceeds one, the probability that a single exciton is trapped in the quantum dot decreases and the strength of the exciton emission peak is reduced.

Figure 5(a)-(d) shows the temporal response of the exciton, biexciton, and triexciton emission intensities when pumped with light pulses of various intensities.[29] The double lines show the theoretical values based on two assumptions: (i) that the number of excitons injected into the quantum dot at $t=0$ follows the Poisson distribution of the average value μ, and (ii) that each exciton independently releases a photon with a fixed emission lifetime of τ. The experimental results are well explained when selecting two parameters: average number of excitons μ and photodetection quantum efficiency I_0. When the number of excitons injected into the quantum dot at $t=0$ is three or more, no triexciton emission occurs until the number of excitons in the quantum dot reaches three. Further, biexciton emission does not occur until triexciton emission has finished and the number of excitons in the quantum dot has reached two. The process leading up to exciton emission is the same. Figure 5(c) shows the results of measurements with a streak camera indicating this behavior.

2.3 Post filtering

The last photon to be released from a quantum dot with initial multiple excitons has a unique emission wavelength and is the only photon with this wavelength. Using an optical band-pass filter to extract just this last photon, it is possible to generate a single photon corresponding to each pump pulse. Figure 6(a) shows how the post-filtered exciton emission intensity obtained in this way varies with the intensity of the pumping light.[17] Here, the characteristic strong saturation shows that when one or more excitons are injected into the quantum dot, the last photon to be generated is always extracted by the band-pass filter. Figure 6(b) shows the results when measuring $g^{(2)}(\tau)$ from a stream of single photons generated in this way.[17] Here, the unique characteristics of a single-photon source - $g^{(2)}(0)\approx 0$, and $g^{(2)}(\tau=nT)=1$ - are more or less realized. The small residual value of $g^{(2)}(0)$ is due to insufficient suppression of the optical filter's stop bands. Close to $t=0$, the value of $g^{(2)}(\tau=nT)$ becomes greater than one because the light emission from the quantum dot is superimposed with on-off modulation (blinking effect). This indicates a repeating pattern whereby the quantum dot emits light at the wavelength under measurement at a certain time, after which light emission at this wavelength stops and then restarts. This is thought to be caused by a shift in exciton emission wavelength resulting from the capture and release of carriers into and out of carrier traps in the vicinity of the quantum dot. Similar reports relating to the generation of single photons using a single quantum dot have been reported by several research groups.[30],[31],[32],[33]

3 Controlling spontaneous emission with a single-mode cavity[18],[36]

Figure 7(a) shows an SEM photograph of a three-dimensional microcavity produced using electron beam lithography and ECR dry etching to process a DBR planar cavity made by MBE into a post shape.

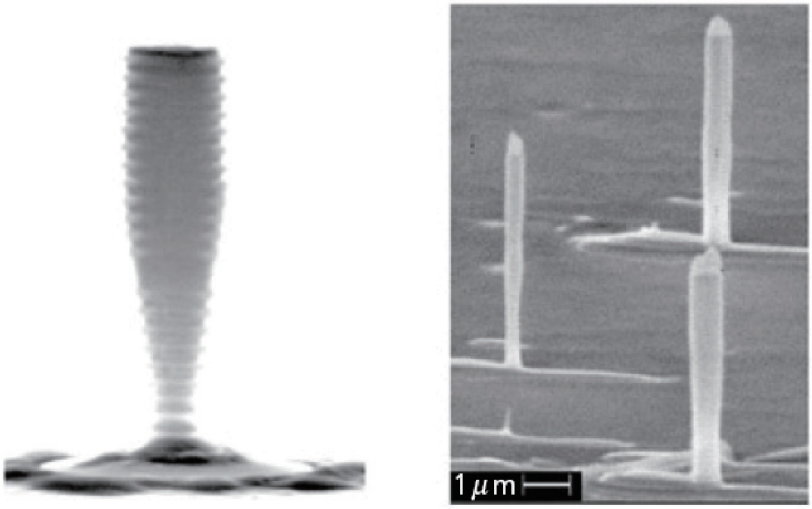


Fig. 7 GaAs/AlAs DBR micropost cavities enclosed in the center of InAs quantum dots produced by electron beam lithography and (a) Electron Cyclotron Resonance (ECR) dry etching, (b) Chemically Assisted Ion Beam Etching (CAIBE).

An InAs quantum dot is embedded in the central optical cavity layer.

Figure 8 shows the emission spectrum of a DBR microcavity with a post diameter of 6 μm.[18] In a post system of this size, large numbers of InAs quantum dots having inhomogeneously broadened exciton energies contribute to the broad emission spectrum, which is filtered by the cavity. Since different transverse modes (HE_{11}, HE_{21}, ...) have different longitudinal wavenumbers, they each feature a different resonant wavelength. The arrows show the theoretical values of the resonant wavelength for each mode, and explain the experimental results well.

Figure 9(a) and (b) show the results of measuring

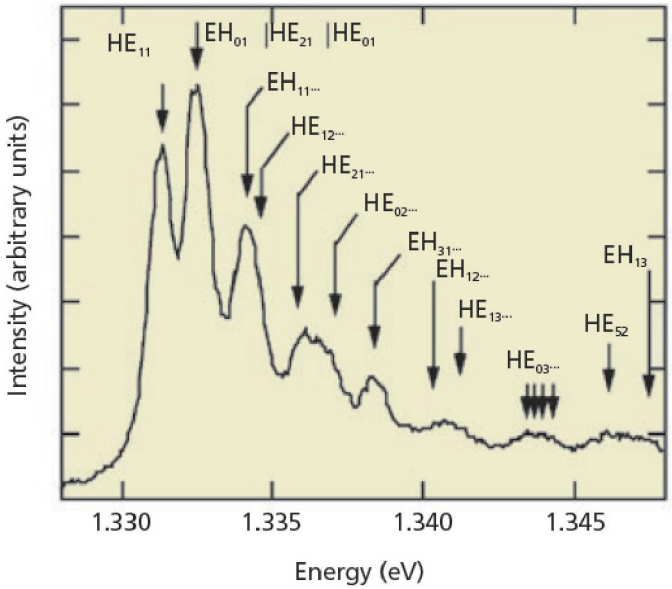


Fig. 8 Resonant modes of a microcavity with a post diameter of 6 μm

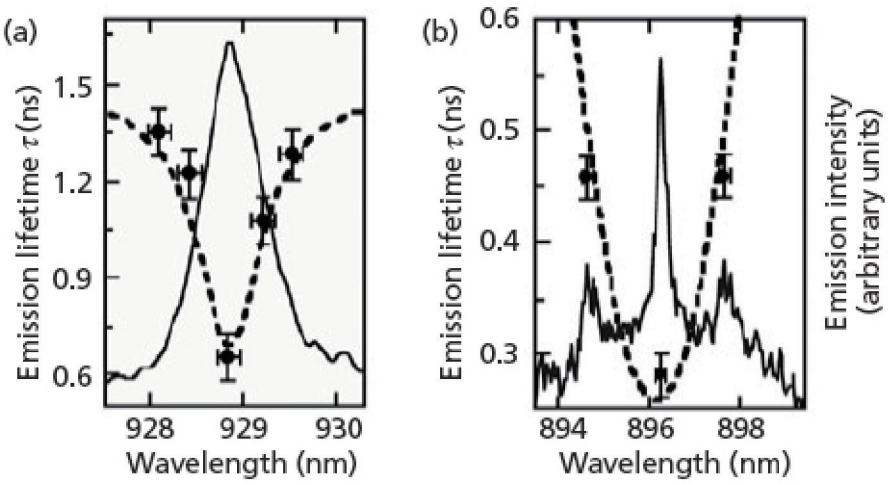


Fig. 9 Variation of emission intensity and spontaneous emission lifetime with emission wavelength for microcavities with post diameters of (a) 2 μm and (b) 0.5 μm.

wavelength dependence of the emission spectrum and emission lifetime of the HE_{11} fundamental mode of DBR microcavities with post diameters of 2 μm and 0.5 μm.[18] The fact that the emission lifetime is shortest at the resonant wavelength of the cavity is a unique characteristic of a three-dimensional cavity. The spontaneous emission rate at the resonant wavelength of a three-dimensional cavity normalized by the

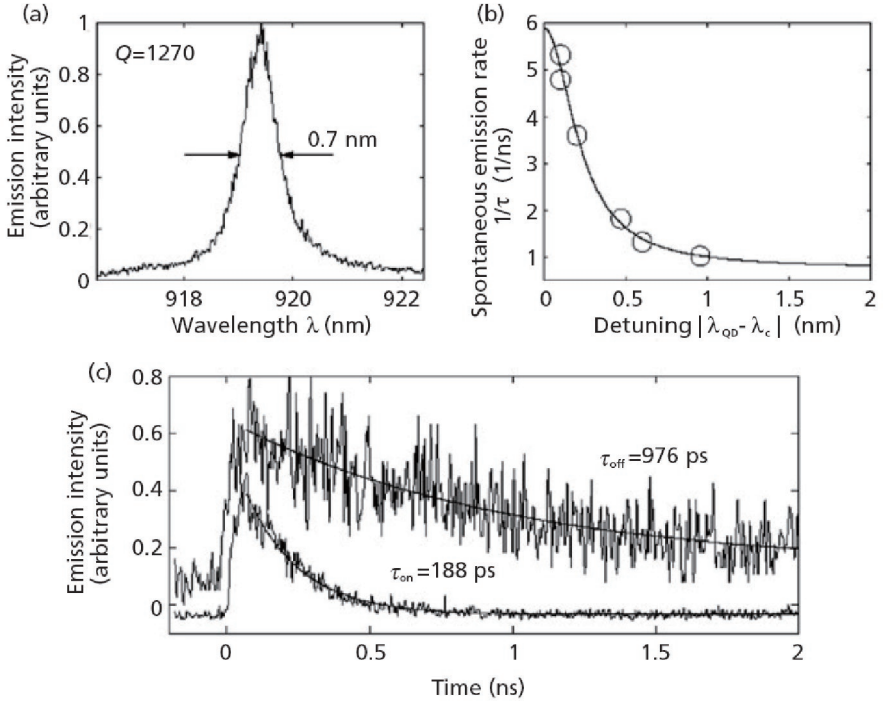


Fig. 10 (a) Emission spectrum of the fabricated DBR post microcavity. (b) Purcell factor vs. detuning. (c) Spontaneous emission decay processes when the exciton emission wavelength of the quantum dot matches the cavity resonant wavelength, and when it does not match the resonant wavelength.

spontaneous emission rate γ_0 in free space is called the Purcell factor, as expressed by the following formula:

$$F \equiv \frac{\gamma}{\gamma_0} = \frac{Q\lambda^3}{2\pi^2 n^3 V_0}\left|\frac{E}{E_{\max}}\right|^2 \frac{\Delta\lambda_C^2}{\Delta\lambda_C^2 + 4(\lambda - \lambda_C)^2}$$

Here, λ is the emission wavelength, λ_C is the resonant wavelength of the cavity, V_0 is the cavity's mode volume, $E_{\max}$ is the maximum electric field inside the cavity, E is the electric field at the position of the QD, and $\Delta\lambda_C = \frac{\lambda_C}{Q}$ is the resonance width of the cavity.

The ratio of the rate of spontaneous emissions into the single cavity mode to the overall spontaneous emission rate is called the spontaneous emission coefficient, which is expressed in terms of the Purcell factor as follows:

$$\beta = 1 - \frac{1}{F}$$

To investigate the Q value of an ideally formed DBR micropost cavity, its behavior was studied by first principle calculation, i.e., using the finite difference time domain method.[34],[35] A post with a diameter of 0.4 μm and a height of 5 μm was predicted to achieve a Q value of 10,000, a mode volume V of 1.5 $(\lambda/n)^3$, a Purcell factor F of 100, and a spontaneous emission coefficient β of 0.99.[34] This value is at least an order of magnitude better than the value measured experimentally. This discrepancy is thought to occur for the following reasons: (i) the height of the post was insufficient and part of the bottom DBR remained un-etched when the post was formed, resulting in increased diffraction loss, and (ii) the shape of the post has a sharply tapering structure that causes transverse radiative loss.

The Purcell factor γ/γ_0 increases as the cavity's Q value increases, as the mode volume V_0 decreases, as the position of the quantum dot approaches the position of the maximum electric field, and as the exciton emission wavelength approaches the cavity resonant wavelength. A larger Purcell factor results in a greater proportionate reduction ratio in the exciton emission lifetime. Achieving a large Purcell factor γ/γ_0 and a spontaneous emission coefficient β close to 1 requires a large Q and small V_0 in the microcavity

However, as shown in Fig. 7(a), the post shape produced by conventional ECR dry etching has a tapering structure caused by undercutting. This causes the radiative loss to increase and as a result the magnitude of Q is limited to 300-800. This problem was addressed by switching to chemically assisted ion beam etching (CAIBE), resulting in the successful fabrication of a post structure with little tapering, as shown in Fig. 7(b). This technique was used to produce a GaAs/AlAs DBR post microcavity with a post diameter of 0.4 μm and a post height of 5 μm with suppressed taper-related radiative loss, which exhibited the following characteristics: Q=1,300, V_0=1.5$(\lambda/n)^3$, γ/γ_0 =6, and β =0.84 (Fig. 10). It was also possible to improve the external quantum efficiency of photons extracted as a simple Gaussian beam to 38%.[36]

4 Single photon pulses at the Fourier transform limit

4.1 Indistinguishable quantum particles

The lifetime of excitonic emissions from a quantum dot is normally 0.5-1 ns. On the other hand, the decoherence time of excitonic dipole caused by phonon scattering is about 1 ns at a temperature of 4K.[37] That is, the natural width of spontaneous emissions is of about the same order as the homogeneous broadening caused by phonon scattering. If the lifetime of excitonic emissions from a single quantum dot can be reduced using a three-dimensional microcavity, then it should be possible to reduce the excitonic emission linewidth to the limit determined by the emission lifetime, and to reduce the temporal width and spectral width of successively radiated single photon pulses to the Fourier transform limit. A single-photon pulse stream of this sort should give rise to quantum interference phenomena as indistinguishable quantum particles.

Figure 11 shows an example of such quantum interference. When two identical particles 1 and 2 are known to occupy each of the two states $|r_A\rangle$ and $|r_B\rangle$, the system state is expressed as a completely symmetric or completely antisymmetric wave function:

$$|\psi_{12}\rangle = \frac{1}{\sqrt{2}}\left[|1, \gamma_A; 2, \gamma_B\rangle \pm |2, \gamma_A; 1, \gamma_B\rangle\right]$$

The former applies to bosons, and the latter applies to fermions. This is called the symmetrization postulate. When two identical particles are incident on a 50-50% beam splitter, both bosons appear simultaneously at the same output port, but fermions are always output from different ports. This is a characteristic phenomenon of quantum particles that occurs due to quantum interference between the direct term and the exchange term (the first and second terms respectively in the above equation) of symmetric and antisymmetric wavefunctions.[38] This quantum interference phenomenon is the source of the Pauli exclusion principle for fermions and of phenomena exhibited by bosons such as stimulated emission of photons in lasers, Bose

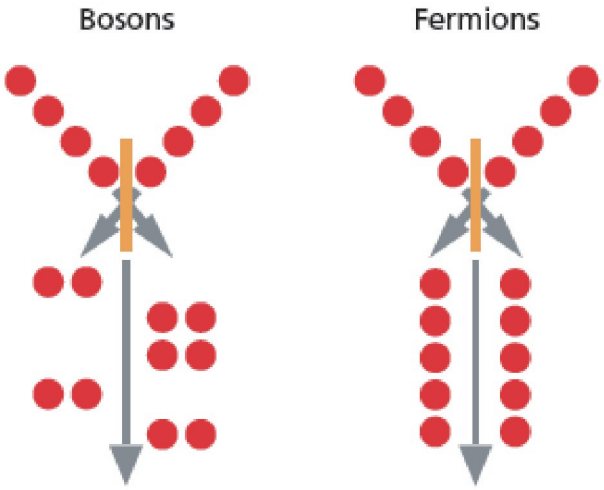


Fig. 11 Collision characteristics of indistinguishable identical quantum particles

condensation, and superconductivity. The scattering characteristics of indistinguishable quantum particles in a 50-50% beam splitter shown in Fig. 11 can also be used for the analysis of EPR-Bell states and can form the basis of quantum teleportation,[5] quantum repeaters,[6] and linear optical quantum computers.[7]

4.2 Two-photon interference experiments[20]

Figure 12 shows the results when using a Michelson interferometer to measure the coherence time of a single photon pulse stream generated from this single quantum dot microcavity (coherence time τ_c: 200 ps) and the results when using a streak camera to measure the pulse duration (amplitude decay time $2\tau_{rad}$: 290 ps).[20] This differs from the Fourier transform limit $2\tau_{rad}=\tau_c$ by a factor of only 1.5.

Figure 13(a) shows a collision experiment for two single photons generated at 2-ns time intervals. The delay time of the Michelson interferometer was set to 2 ns, which is the same as the interval between the two single photon pulses. Figure 13(b) shows the joint counting probability with which the two detectors T1 and T2 detected the photons at $t=0$ and $t=\tau$.[20] Peaks 1 and 5 in the central cluster centered on $t=0$

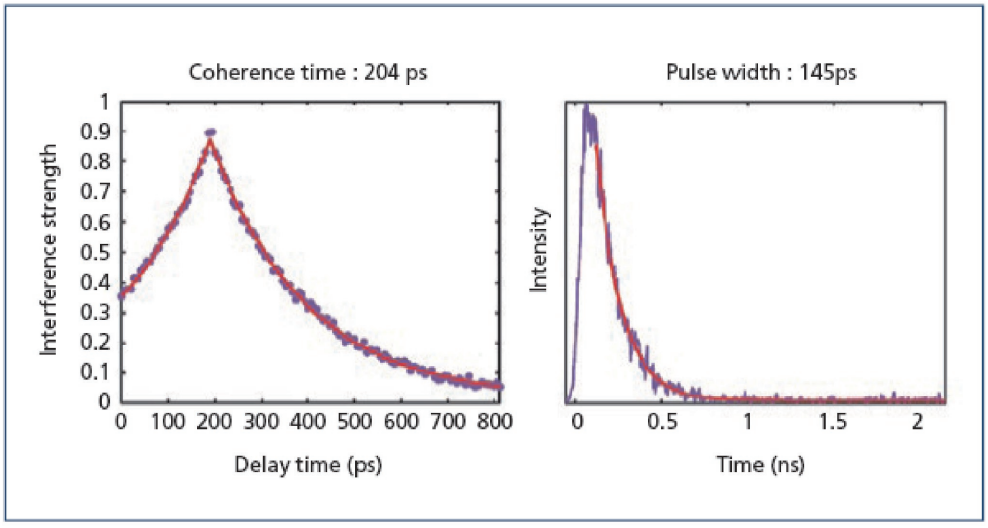


Fig. 12 Results of using a Michelson interferometer to measure the coherence time of a single photon pulse and a streak camera to measure the pulse duration.

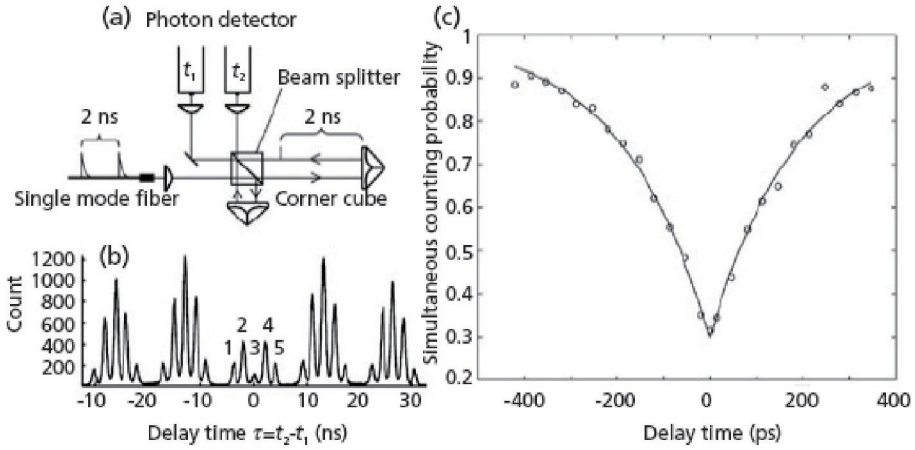


Fig. 13 Collision experiment involving two single photons generated with a 2-ns delay time difference. When the wave functions of the two single photons were overlapped at the output 50-50% beam splitter, the simultaneous counting probability was found to be lower due to two-photon interference.

correspond to the case in which the first photon takes a short path and the second photon takes a long path. Peaks 2 and 4 correspond to the case in which the two photons both take a short path or both take a long path. The central peak 3 corresponds to the case in which the first photon takes a long path and the second photon takes a short path, and only in this case are the two single photons incident on the output 50-50% beam splitter simultaneously. The fact that peak 3 is smaller than peaks 2 and 4 shows that quantum interference is actually occurring in the identical boson particle collisions shown in Fig. 11. Figure 13(c) shows that this suppression of simultaneous counting probability reaches maximum when the two pulses overlap completely, and disappears when the delay time exceeds the pulse width $2\tau_{rad}$: 290 ps. The dip in simultaneous counting probability caused by two-photon interference shown in Fig. 13 is deeper than the value predicted from the offset from the Fourier transform limit (1.5 times) shown in Fig. 12. This might be because the coherence time in Fig. 12 does not reflect the actual homogeneous linewidth but includes the effects of a small drift in the emission wavelength due to the inflow and outflow of carriers in carrier traps near the quantum dot.

5 Entanglement formation and violation of Bell's inequality with a single-photon source[22]

This experiment relies on two crucial features of our quantum-dot single-photon source, namely its ability to suppress multi-photon pulses, and its ability to generate consecutively two photons that are quantum mechanically indistinguishable. The idea is to "collide" these photons with orthogonal polarizations at two conjugated input ports of a non-polarizing beam splitter (NPBS). When the two optical modes corresponding to the output ports 'c' and 'd' of the NPBS have a simultaneous single occupation, their joint polarization state is expected to be the EPR-Bell state:

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|H\right\rangle_c\left|V\right\rangle_d - \left|V\right\rangle_c\left|H\right\rangle_d\right)$$

The input port modes of the NPBS denoted as 'a' and 'b' are related to the output modes 'c' and 'd' by the 50-50% NPBS unitary matrix according to:

$$a_{H/V} = \frac{1}{\sqrt{2}}\left(c_{H/V} + d_{H/V}\right)$$

$$b_{H/V} = \frac{1}{\sqrt{2}}\left(c_{H/V} - d_{H/V}\right)$$

where subscripts 'H' and 'V' specify the polarization (horizontal or vertical) of a given spatial mode. The quantum state corresponding to single-mode photons with orthogonal polarizations at ports 'a' and 'b' can be written as:

$$a_H^\dagger b_V^\dagger\left|vac\right\rangle = \frac{1}{2}\left(c_H^\dagger c_V^\dagger - d_H^\dagger d_V^\dagger - c_H^\dagger d_V^\dagger + c_V^\dagger d_H^\dagger\right)\left|vac\right\rangle$$

As pointed out in [39], this state already features

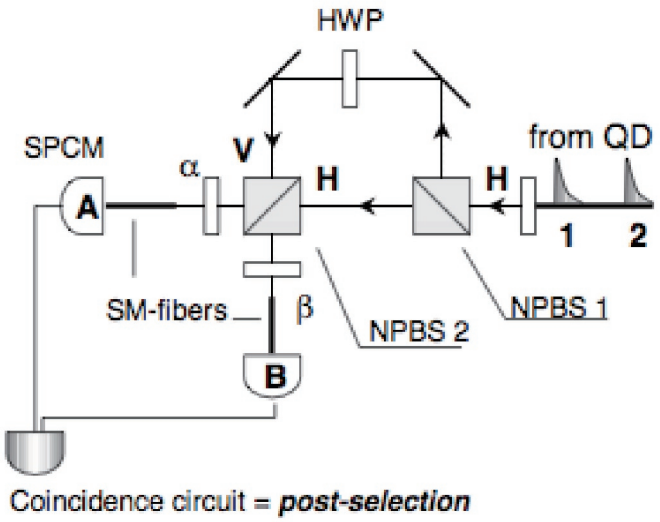


Fig. 14 Experimental setup. Single photons from the QD microcavity device are sent through a single-mode fiber, and have their polarizations rotated to H. The photons are split by a first NPBS (1). The polarization is changed to V in the longer arm of the Mach-Zehnder configuration. The two paths of the interferometer merge at a second NPBS (2). The output modes of NPBS 2 are matched to single-mode fibers for subsequent detection. The detectors are linked to a time-to-amplitude converter for a record of coincidence counts.

non-local correlations and violates Bell's inequality without the need for post-selection, using photo-detectors that can distinguish photon numbers 0, 1, and 2. Here, we implemented a simpler scheme using postselection based on the simultaneous click of two regular photon counter modules. If we discard events in which two photons go the same way (recording only coincidence events between modes 'c' and 'd'), we obtain the postselected state:

$$\frac{1}{\sqrt{2}}\left(c_H^\dagger d_V^\dagger - c_V^\dagger d_H^\dagger\right)|vac\rangle = \left|\Psi^-\right\rangle$$

with a probability of $\frac{1}{2}$. Note that the generation of polarization entangled states via two-photon cascade emission[40] and a parametric down converter[41] also rely upon a post-selection mechanism, and suffer as well from intrinsic loss of quantum efficiency.

The experimental setup is shown in Fig 14. Pulses came by pairs separated by 2 ns, with a repetition rate of 1 pair/13 ns. The emitted photons were collected by a single-mode fiber and sent to a Mach-Zehnder type setup with 2-ns delay on the longer arm. A quarter-wave plate (QWP) followed by a half-wave plate (HWP) were used to set the polarization of the photons after the input fiber to linear and horizontal orientations. An extra half-wave plate was inserted in the longer arm of the interferometer to rotate the polarization to a vertical orientation. One out of four times, the first emitted photon takes the long path while the second photon takes the short path, in which case their wave functions overlap at the second non-polarizing beam-splitter (NPBS 2). In all other cases (not of interest) the single photon pulses "miss" each other by at least 2 ns, which is greater than their width (100 - 200 ps). Two single photon counter modules (SPCMs) in a start-stop configuration were used to record coincidence counts between the two output ports of NPBS 2, effectively implementing post-selection (if photons exit NPBS 2 by the same port, then no coincidence is recorded by the detectors). Single-mode fibers were used prior to detection to facilitate spatial mode-matching. These fibers were preceded by quarter-wave and polarizer plates to allow for the analysis of all possible polarizations.

For given analyzer settings (α, β), we denote by $C(\alpha, \beta)$ the number of post-selected events normalized by the total number of coincidences in a time window. This normalization is independent of (α, β) since the two inputs of NPBS 2 are two modes with orthogonal polarizations. $C(\alpha, \beta)$ measures the average rate of coincidences throughout the time of integration.

A Bell's inequality test was performed for post-selected photon pairs. Following ref [42], if we define the correlation function $E(\alpha, \beta)$ for analyzer settings α and β as:

$\beta \backslash \alpha$	0°	45°	90°	135°
22.5°	5.6	28.4	28.6	4.7
67.5°	9.0	8.3	25.2	25.1
112.5°	28.9	5.4	4.6	28.4
157.5°	26.0	24.9	8.6	8.8

TABLE I Normalized coincidences $C(\alpha, \beta)\cdot 10^3$ for various polarizer angles used in the BI test. These coincidences correspond to the coincidences in the integration window divided by the total coincidences recorded for $-50\text{ns} < \tau < 50\text{ns}$. Note that the quantity $C(\alpha, \beta)+C(\alpha^{\perp}, \beta^{\perp})+C(\alpha^{\perp}, \beta)+C(\alpha, \beta^{\perp})$ is constant for given settings α and β.

$$E(\alpha,\beta)=\frac{C(\alpha,\beta)+C(\alpha^{\perp},\beta^{\perp})-C(\alpha^{\perp},\beta)-(\alpha,\beta^{\perp})}{C(\alpha,\beta)+C(\alpha^{\perp},\beta^{\perp})+C(\alpha^{\perp},\beta)+(\alpha,\beta^{\perp})}$$

then local realistic assumptions lead to the inequality:

$$S=\left|E(\alpha,\beta)-E(\alpha',\beta)\right|+\left|E(\alpha',\beta')+E(\alpha,\beta')\right|\leq 2$$

which can be violated by quantum mechanics.

Sixteen measurements were performed for all combinations of polarizer settings among $\alpha \in \{0°, 45°, 90°, 135°\}$ and $\beta \in \{22.5°, 67.5°, 112.5°, 157.5°\}$. The corresponding values of the normalized coincidence counts $C(\alpha, \beta)$ are reported in Table I. The statistical error for S is quite large, due to the short integration time used to ensure high stability in the QD device. Bell's inequality is still violated by two standard deviations, according to S ~2.38±0.18. Hence, non-local correlations were created between two single independent photons by linear optics and photon number post-selection.

An examination of the collection of information relating to the two-photon polarization state reveals a characteristic reduced density matrix, in which only the polarization degrees of freedom are maintained. This density matrix can be reconstructed from a set of 16 measurements with different analyzer settings, including circular[43]. We performed this analysis, know as *quantum state tomography*, on photon pairs. The reconstructed density matrix is shown in Fig 15. This matrix can be shown to be non-separable, i.e. entangled, using the Peres criterion[44] (negativity ~ 0.43, where a value of 1 means maximum entanglement).

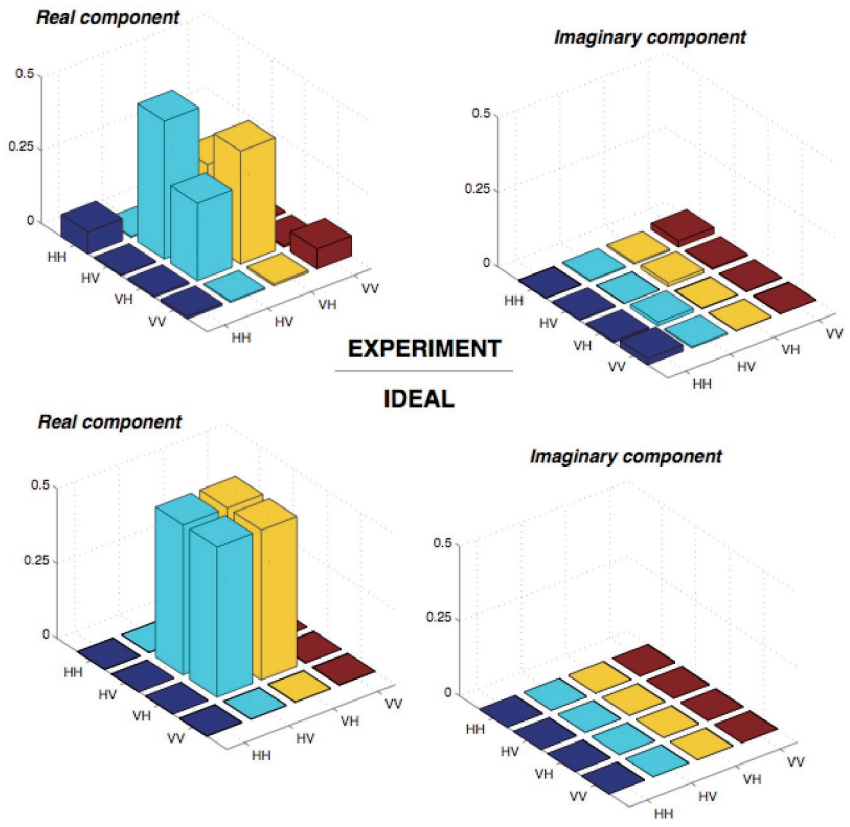


Fig. 15 Reconstructed polarization density matrix for the post-selected photon pairs emitted by QD_2. The small diagonal HH and VV components are caused by finite two-photon pulses suppression ($g^{(2)}>0$). Additional reduction of the off-diagonal elements originates from the imperfect indistinguishability between consecutively emitted photons.

We next try to account for the observed degree of entanglement from the parameters of the QD single-photon source. Due to residual two-photon pulses from the source, giving a non-zero value to its equal time second order correlation function $g^{(2)}(0)$, a recorded coincidence count can originate from two photons of the same polarization that would have entered NPBS 2 from the same port. A multi-mode analysis also reveals that an imperfect overlap $V=|\int \psi 1(t)^{*}\psi 2(t)|^2$ between consecutive photon wavefunctions washes out the quantum interference responsible for the generation of entanglement. Including those imperfections, we can derive a simple model for the joint polarization state of the post-selected photons. In the lower pump-level limit, this model predicts the following density matrix on a $(H/V)\otimes(H/V)$ basis:

$$\rho_{\mathrm{model}}=\frac{1}{\frac{R}{T}+\frac{T}{R}+4g^{(2)}}\begin{pmatrix} 2g^{(2)} & & & \\ & \frac{R}{T} & -V & \\ & -V & \frac{T}{R} & \\ & & & 2g^{(2)} \end{pmatrix}$$

R and T are the reflection and transmission coefficients of NPBS 2 ($\frac{R}{T}\sim 1.1$ in our case). Using the values for $g^{(2)}$ and V measured independently, we obtain excellent quantitative agreement between our model and the experimental data, with fidelity $Tr\left(\sqrt{\rho_{\mathrm{exp}}^{\frac{1}{2}}\ \rho_{\mathrm{model}}\ \rho_{\mathrm{exp}}^{\frac{1}{2}}}\right)$ as high as 0.997.

The negativity of the state ρ_{model} is proportional to $(V - 2g^{(2)})$, which means that entanglement exists as long as $V>2g^{(2)}$. This simple criterion indicates whether any given single-photon source will be able to generate entangled photons in such a scheme.

Since the present experiment does not distinguish between photon numbers 0, 1, and 2, only half of the photon pairs colliding at NPBS 2 can be used for a Bell's inequality test. However, following [39], it would be possible to design a loophole-free Bell's inequality test by keeping track of photon numbers with existing single photon resolution detectors, a process that will be discussed later, if the quantum efficiency of the single-photon source could be made close to unity. The current scheme also does not allow the creation of an "event-ready" entangled photon pair. This is a serious obstacle for many applications to quantum information systems, but not all. The Ekert91[3] or BBM92[3] QKD protocols using entangled photons can be performed directly with our post-selected technique. The essence of these protocols is to establish a secure key upon local measurement of two distant photons from an entangled pair, which corresponds exactly to our scheme. The bit error induced by uncorrelated photon pairs in those protocols is significantly suppressed when single entangled pairs are used, a feature of this source alone among the currently demonstrated entangled photon sources. Therefore, these QKD protocols should in fact benefit from this method of generating entanglement.

6 Quantum teleportation with a single-photon source[23]

Photons are nearly ideal carriers of quantum information, since they have little interaction with their environment and are easy to manipulate individually with linear optics. The main challenge of optical quantum information processing lies in the design of controlled interactions between photons, which is necessary for the realization of non-linear quantum gates. Photons do not naturally "feel" the presence of other photons, unless they propagate in a medium with high optical non-linearity. The amount of optical non-linearity required to perform controlled operations between single photons is, however, prohibitively large.

Probabilistic gates can be implemented with linear optics alone[7],[45],[46] but as such, they are not suitable for scalable quantum computation. In a seminal paper[47], Gottesman and Chuang suggested that quantum gates could be applied to photonic qubits through a generalization of quantum teleportation[48]. In such a scheme, information about the gate is contained in the state of ancilla qubits. The implementation of a certain class of gates can then be reduced to the problem of preparing the ancilla qubits in some wisely chosen entangled state. Such a problem can be solved "off-line" with linear-optic elements only, provided the photons used are quantum mechanically indistinguishable particles[49]. Following this idea, Knill, Laflamme, and Milburn (KLM)[7] proposed a scheme for efficient linear optic quantum computation (LOQC) based on the implementation of the controlled-sign gate (C-z gate) through teleportation. Since the C-z gate acts effectively on only one of the two modes composing the target qubit, a simplified procedure can be used in which a single optical mode is teleported, instead of one in which the two modes compose the qubit.

This procedure will be referred to as *single-mode teleportation* to distinguish it from the usual teleportation scheme. In its basic version using one ancilla qubit, (i.e., two ancilla modes) this procedure succeeds half of the time. In its improved version using an arbitrarily high number of ancillas, it can succeed with a

probability arbitrarily close to one[7],[50].

We use quantum mechanically indistinguishable photons from a quantum-dot single-photon source, featuring high suppression of two-photon pulses. The fidelity of the teleportation depends critically on the quantum indistinguishability of two photons emitted independently by the single-photon source. A similar experiment was performed in the past using two photons emitted spontaneously by parametric down conversion (PDC)[51]. However, the efficiency of such a process is intrinsically limited by the presence of two-photon pulses, which makes it unsuitable when more identical photons are needed, e.g. to implement the improved teleportation scheme. To date, demonstration of single-mode teleportation with a single-photon source remains a capital step in efforts toward scalable LOQC.

Single-mode teleportation in its simplest form involves two qubits, a target and an ancilla, each defined by a single photon occupying two optical modes (see Fig. 16).

The target qubit can a priori be in an arbitrary state $\alpha|0\rangle_L + \beta|1\rangle_L$ where the logical $|0\rangle_L$ and $|1\rangle_L$ states correspond to the physical states $|1\rangle_1|0\rangle_2$ and $|0\rangle_1|1\rangle_2$ respectively, in a dual rail representation. The ancilla qubit is prepared with a beam-splitter (BS a) in the coherent superposition $\frac{1}{\sqrt{2}}\left(|0\rangle_L + |1\rangle_L\right. = \frac{1}{\sqrt{2}}\left(|1\rangle_3|0\rangle_4\right.$ $+|0\rangle_3|1\rangle_4\left.\right)$. One rail of the target (mode 2) is mixed with one rail of the ancilla (mode 3) with a beam-splitter (BS 1), for subsequent detection in photon counters C and D. For a given realization of the procedure, if only one photon is detected at detector C, and none at detector D, then we can infer the resulting state for the output qubit composed of mode (1) and (4):

$$\psi_C = \alpha|0\rangle_L + \beta|1\rangle_L = \alpha|1\rangle_1|0\rangle_4 + \beta|0\rangle_1|1\rangle_4$$

which is the initial target qubit state. Similarly, if D clicks and C does not, then the output state is inferred to be:

$$\psi_D = \alpha|0\rangle_L - \beta|1\rangle_L = \alpha|1\rangle_1|0\rangle_4 - \beta|0\rangle_1|1\rangle_4$$

which again is the target state -- except for an additional phase shift of π, which can be actively corrected. Half of the time, either zero or two photons are present at counters C or D, and the teleportation procedure fails. It is interesting and somewhat enlightening to describe the same procedure in the framework of *single rail logic*. In this framework, each optical mode supports a whole qubit, encoded in the presence or absence of a photon, and single-mode teleportation can be viewed as entanglement swapping. Indeed, for the particular values $\alpha=\beta=\frac{1}{\sqrt{2}}$ modes 1 and 2 find themselves initially in the Bell state $|\psi^+\rangle_{12}$, while modes 3 and 4 are in a similar state $|\psi^+\rangle_{34}$. Partial Bell measurement takes place using BS 1 and counters C/D, which (if it succeeds) leaves the system in the entangled state $|\psi^+\rangle_{14}$, so that entanglement swapping occurs. In the rest of this paper, we will consider the scheme in the dual rail picture, since it is a more robust, and hence realistic, way of storing quantum information (at the expense of using two modes per qubit).

The success of teleportation depends mainly on the transfer of coherence between the two modes of the target qubit. If the target qubit is initially in state $|0\rangle_L$ =

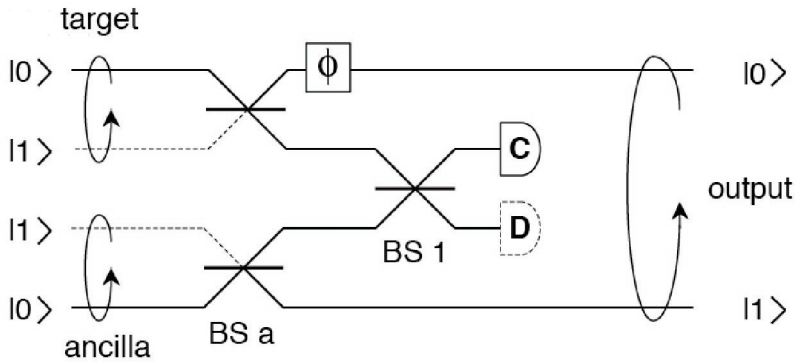


Fig. 16 Schematic of single-mode teleportation. Target and ancilla qubits are each defined by a single photon occupying two optical modes. When detector C clicks and D does not, the state of the remaining modes reproduces the state of the target. The coherence between modes (1) and (2) of the target was transferred to coherence between the same mode (1) of the target and mode (4) of the ancilla. Preparing the target in an equal superposition state makes it easier to measure the transfer of coherence.

$|1\rangle_1|0\rangle_2$, then the ancilla photon cannot end up in mode (4) because of the postselection condition, so that the output state is always $|1\rangle_1|0\rangle_4$ as desired. The same argument applies when the target qubit is in state $|1\rangle_L$. However, when the target qubit is in a coherent superposition of $|0\rangle_L$ and $|1\rangle_L$, the output state might not retrieve the full initial coherence. We can test the transfer of coherence by preparing the target in a maximal superposition state:

$$\psi_{tar} = \frac{1}{\sqrt{2}}\left(|0\rangle_L + e^{i\phi}|1\rangle_L\right)$$

where ϕ is a phase that we can vary. If the initial coherence of the target qubit is not transferred to the output qubit, a change in ϕ will not induce any measurable change in the output qubit. However, if changing ϕ induces some measurable change in the out qubit, then we can prove that the initial coherence was indeed transferred, at least to some extent.

The experimental setup is shown in Fig. 17. Two photons emitted consecutively by a single quantum dot photon source are captured in a single-mode fiber. In the dual rail representation, we refer to the first photon as the ancilla, and to the second photon as the target (see Fig. 16). The ancilla qubit, initially in state $|0\rangle_L$, is delayed in free space to match the target qubit temporally at BS 1. The delay must be adjusted to within a fraction of the photon's temporal width (~ 200 ps, or 6 cm in space). Note that mode matching is significantly easier here than in similar experiments using photons from PDC, where optical path lengths have to be adjusted with a tolerance of only a few microns[51].

The ancilla is prepared in the superposition state $\psi_{anc} = \frac{1}{\sqrt{2}}\left(|0\rangle_L + |1\rangle_L\right)$ with a beam-splitter 'BS a'. The target qubit is prepared in a similar superposition state with a variable phase between two modes, so that $\psi_{tar} = \frac{1}{\sqrt{2}}\left(|0\rangle_L + e^{i\phi}|1\rangle_L\right)$. The phase shift is applied by changing the path length on mode (1) with a piezo-actuated mirror. The "partial Bell measurement" responsible for the teleportation is performed at BS 1 by mixing the optical modes (2) of the target qubit and (3) of the ancilla qubit, with subsequent detection in counter C. A Mach-Zehnder type setup is used to measure the coherence between the two modes (1) and (4) of the output qubit. This setup is composed of a 50-50% beam-splitter BS 2 mixing modes (1) and (4), with subsequent detection in counters A and/or B.

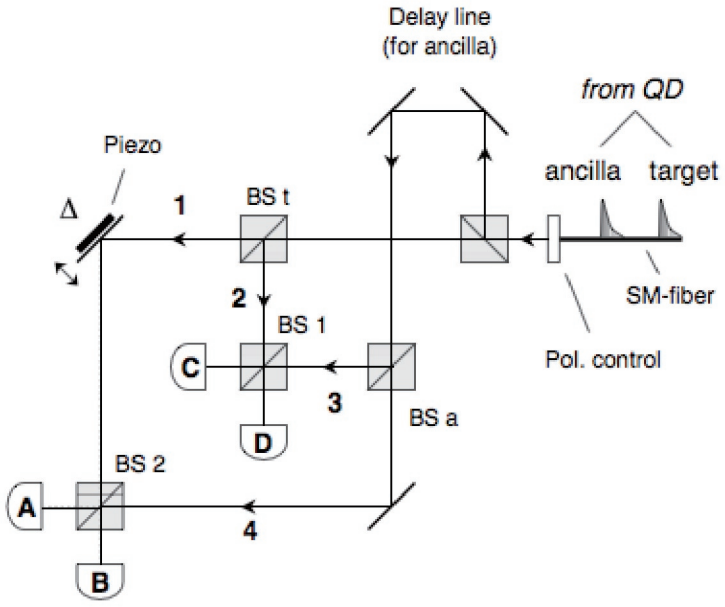


Fig. 17 Experimental setup. All of the beam-splitters (BS) shown are 50-50% non-polarizing BS. The teleportation procedure works when the ancilla photon is delayed, but the target is not. After preparation, the target photon occupies modes 1 and 2, and the ancilla occupies modes 3 and 4. Modes 2 and 3 are mixed at BS 1 and subsequently measured by detectors C and D; this step forms the heart of the teleportation process. When C clicks and D does not, a single photon occupies modes 1 and 4, which constitute the output qubit. The relative phase between modes 1 and 4 in the output state is measured by mixing those modes at BS 2 and recording single counts at detector A or B. Note that since an event is recorded only if A *and* C or B *and* C clicked, the condition that D did not click is automatically fulfilled.

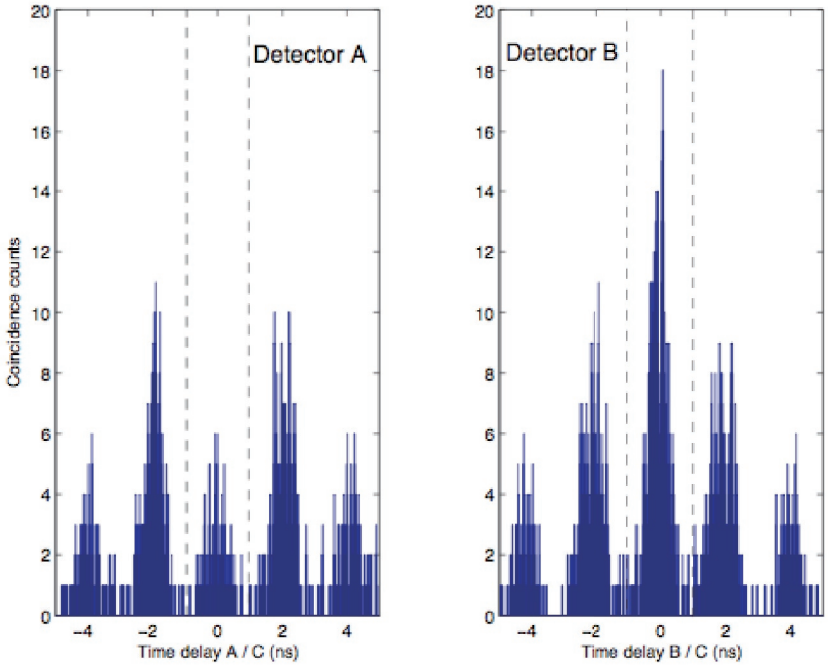


Fig. 18 Typical correlation histograms taken simultaneously between detectors A/C and B/C. The central region indicated by the dashed lines correspond to the postselected events, when target and ancilla photons feature timing such that it is impossible to distinguish between them based on the time of detection. As the phase ϕ varies, so does the relative size of the central peaks of detector A and B. The sum of the count rates for the central peaks of detector A and B was 800/s, independent of ϕ, as shown in Fig. 19

Modulating the phase ϕ of the target qubit should result in the modulation of the count rate in detector A and B (conditioned on a click at detector C), with a contrast related to the degree of coherence between output modes (1) and (4).

Coincidences between counters A-C and B-C were simultaneously recorded using a start-stop configuration (each electronic "start" pulse generated by counter C was doubled for this purpose). This detection method naturally post-selects events where one photon has gone through BS 1 and the other has gone through BS 2, as required by the teleportation scheme. Since no more than one photon is emitted by the single-photon source, no photon can reach detector D. Typical correlation histograms are shown in Fig 18. The integration time was 2 min, short enough to keep the relative optical path length between different arms (1-4) of the interferometer stable. The whole setup was made compact for that purpose, and stability over time periods as long as 10 min. was observed. A second post-selection was made, depending on the timing between target and ancilla photons, which is adequate only one out of four times - the ancilla taking the long path and the target taking the short path. The resulting coincidence counts were recorded for different phases ϕ of the target qubit. The results of the experiment are shown in Fig. 19. The number of counts recorded in the post-selected window (-1 $ns < \tau < 1$ ns) was normalized by the total number of counts recorded in detectors A and B in the broader window -5 ns $< \tau <$ 5 ns, corresponding to all events where one photon went through BS 1 and the other through BS 2 (but only one quarter of the time with the right timing). Complementary oscillations are clearly observed at counter A and at counter B, indicating that the initial coherence was indeed transferred to the output qubit. In other words, mode (2) of the target qubit was "replaced" by mode (4) of the ancilla without a major loss of coherence.

If the initial coherence was fully conserved during the single-mode transfer, the state of the output qubit would truly be $\alpha|0\rangle_L + \beta e^{i\phi}|1\rangle_L$, and the single count rate at detector A (resp. B) would be proportional to $\cos^2\left(\frac{\phi}{2}\right)$ (resp.$\sin^2\left(\frac{\phi}{2}\right)$), giving perfect contrast as the target phase ϕ is varied. More realistically, part of the coherence can be lost in the transfer, resulting in a degradation of contrast. Such a degradation is visible in Fig. 19. This arises mainly due to residual distinguishability between ancilla and target photons. Slight

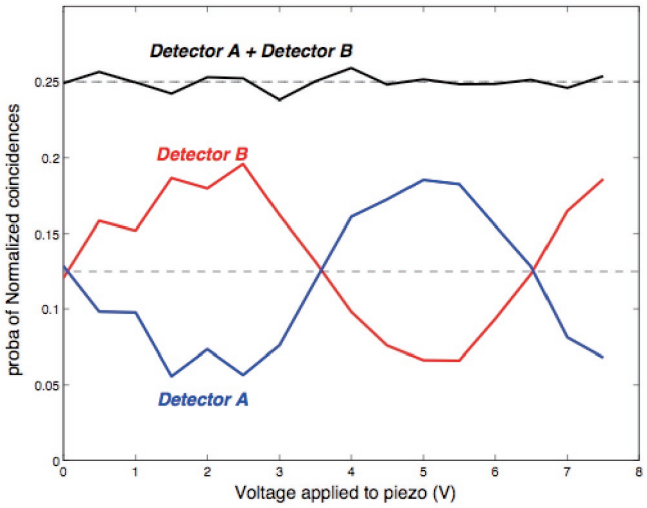


Fig. 19 Verification of single-mode teleportation. Coincidence counts between detector A/C and B/C are plotted for different voltages applied to the piezo transducer, i.e. for different phase ϕ values of the target qubit. The observed modulation of the counts implies that the initial coherence contained in the target qubit was transferred to a large extent to the output qubit. The reduced contrast (~ 60%) is principally due to imperfect indistinguishability between the target and ancilla photons.

misalignments and imperfections in the optics also result in imperfect mode matching at BS 1 and BS 2, reducing contrast further. Finally, the residual presence of two-photons among pulses can reduce the contrast even more, although this effect is negligible here. The overlap $V=\int \psi_{tar}\psi_{anc}$ between target and ancilla wavepackets, the two-photon pulse suppression factor $g^{(2)}$, as well as the non-ideal mode matching at BS 1 and BS 2 - characterized by first-order interference visibilities V_1, V_2 - were all measured independently. The results are $V \sim 0.75$, $g^{(2)}(0) \sim 2\%$, $V_1 \sim 0.92$ and $V_2 \sim 0.91$. The contrast C in counts at detector A or B when we vary the phase ϕ should be:

$$C = \frac{V \cdot V_1 \cdot V_2}{1 + g^{(2)}/2} \sim 0.62$$

This predicted value compares well with the experimental value of C_{exp} ~0.60.

The fidelity of teleportation is $F = \frac{1+C}{2} \sim 0.8$. This high value is still not sufficient to meet the requirements of efficient LOQC[7]. In particular, the quantum indistinguishability of the photons must be increased further to meet these requirements. In this single-photon source, a dephasing mechanism acting on a time scale of a few nanoseconds is responsible for the loss of indistinguishability. Using the Purcell effect, one can reduce the quantum-dot radiative lifetime well below this dephasing time. However, current jitter in the photon emission time will eventually prevent any further reduction of the quantum-dot lifetime. Time jitter happens as a consequence of the incoherent character of our method of exciting the quantum dot; this jitter is currently on the order of 10 ps. Time jitter can be completely suppressed using a coherent excitation technique (e.g., 52) for such a scheme with single atoms. It therefore seems important to develop such techniques for single quantum dots.

Using more ancillas in a scheme first proposed in [7] and significantly improved in [50], single-mode teleportation can be rendered nearly deterministic. This would allow the replacement of deterministic non-linear gates necessary for scalable quantum computation with probabilistic ones, as recently demonstrated experimentally with linear optics[46]. This generalized teleportation procedure requires more indistinguishable ancilla photons, produced no more than one at a time, a feature absent in [51] but present in our implementation of teleportation. We should also point out that the generalized scheme requires the discrimination of different photon numbers. This would in principle allow the implementation of a linear-optic C-z gate with a probability of success of $\left(\frac{6}{7}\right)^2 \sim 0.73$.[50]

7 Quantum cryptography using single photons[21]

Figure 20 compares the performance of BB84 quantum cryptography systems using an ordinary semicon-

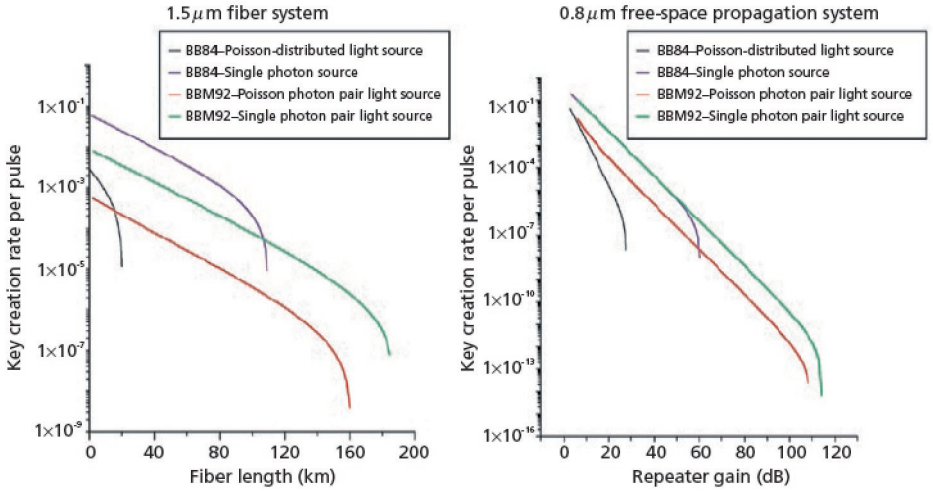


Fig. 20 A comparison of the performance of quantum cryptography using the BB84 and BBM92 protocols in the 1.5-μm and 0.8-μm bands. In BB84, the key creation rate per pulse and the repeater gain are substantially better when using a single-photon source compared with an ordinary semiconductor laser. In BBM92 a better key creation rate per pulse is achieved by using a light source that generates regular photon pairs compared with an ordinary parametric light source.

ductor laser source and a single-photon source, where the final key creation rate per pulse after error correction and privacy amplification varies with fiber length (1.5-μm band), or with repeater gain in the case of spatial propagation (0.8-μm band). When an ordinary semiconductor laser source is used, it is possible to generate two or more photons per pulse due to the Poisson-distributed photon numbers, allowing an eavesdropper to use a photon splitting attack. To reduce this possibility, it is essential to suppress the average number of photons per pulse to a value less than 1. As the fiber length or repeater gain increases, the average number of photons per pulse becomes even smaller, and the received photon number eventually becomes smaller than the average dark count of the detector. At this stage, the bit error rate becomes very large, making secure key creation impossible. This limit corresponds to a repeater gain of 20 dB for a 0.8-μm band space propagation system or a fiber length of 20 km for a 1.5-μm band fiber system. However, if an ideal single-photon source is used, the probability of two or more photons per pulse is reduced to zero, so the average number of photons sent out to the propagation path can be set to one. This makes it possible to increase the repeater gain to 60 dB in a 0.8-μm band system or to increase the fiber length to 100 km in a 1.5-μm band system. The ultimate secure key creation rate was recently calculated for cases in which a single-photon source emits two or more photons with a finite probability ($g^{(2)}(0)\neq 0$) and where external quantum efficiency is less than 1 ($\eta<1$), and even in these cases it was found that the resulting characteristics are better than when an ordinary Poisson-distributed light source is used.[53]

Figure 21(a) shows a BB84 quantum cryptography test system using the single-photon source.[21] This system generates single photons at a repetition frequency of 76 MHz using a mode-locked Ti:Al_2O_3 laser. Alice uses random numbers generated in her computer to modulate the polarization state to one of four states - horizontal (H), vertical (V), right-handed circular (R), or left-handed circular (L) - and sends it to Bob. Bob then splits the received photons into two paths with a 50-50% beam splitter and detects one path on an H-V basis and the other on an R-L basis. Since the photons are randomly divided between either of the output ports, this demodulation scheme is called passive demodulation. After this quantum transmission has taken place, Alice and Bob publicly compare the polarization bases they used, and store only the data for cases in which these bases matched. Figure 21(b) shows a histogram of Alice and Bob's data.[21] As this figure shows, a strong correlation is formed when Alice and Bob use the same polarization base. After that, classical error correction is performed using a block coding technique. To increase the level of security so as to suppress the leakage of information to eavesdroppers to an ultimately negligible level, classical privacy amplification is finally employed. Figure 21(c) shows how the repeater gain varies with the final key creation rate per transmitted pulse in this system. Since the average number of photons sent out to the

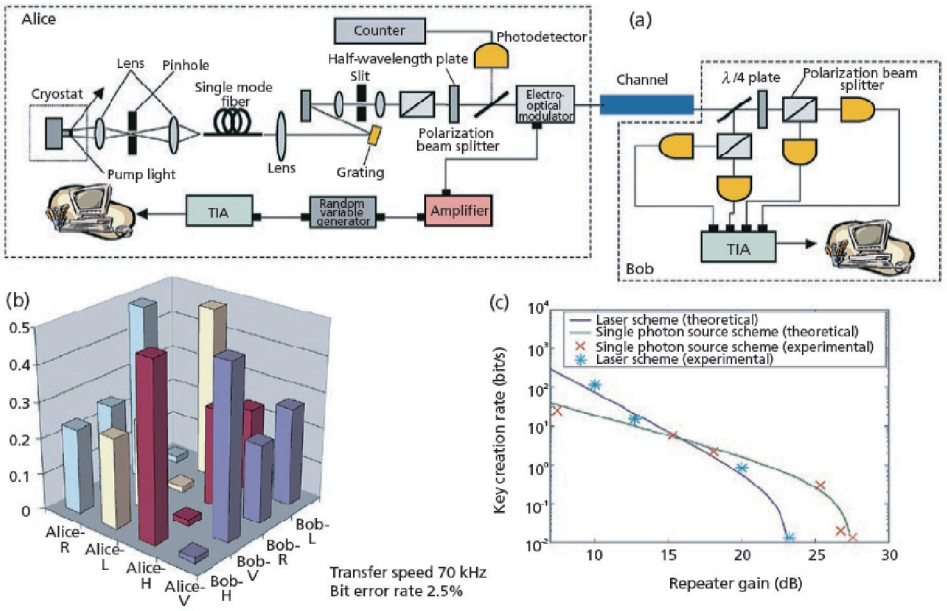


Fig. 21 An experimental BB84 quantum key distribution system using a single-photon source, and the results obtained with this system

transmission path per pulse is 3×10^{-3}, the present system is inferior to schemes using an ordinary semiconductor laser in the region of small propagation loss, but in the high propagation loss region the small value of $g^{(2)}(0)$ makes it advantageous to use a single-photon source. In the future it is expected that a theoretically predicted repeater gain of 60 dB will be assured by reducing optical loss inside the transmitter.

8 Deterministic generation of EPR-Bell photon pairs[54]

Figure 20 also compares the performance of BBM92 quantum cryptographic systems using a Poissonian parametric downconverter and regulated EPR-Bell pair source. Due to the absence of bit errors caused by uncorrelated photon-pairs, the latter system features better performance.[4] Figure 22 shows the two photon-emission process when two electrons and two holes are confined at the ground state in a single quantum dot. According to the anti-symmetrization postulate of quantum mechanics, the two electrons and holes should be in respective spin singlet states.

These two electron-hole pairs release two photons, but are subject to the so-called selection rules, whereby an up-spin electron (J=+1/2) only recombines with an up-spin hole (J = +3/2) to release a right-handed circular polarized (σ_+) photon, and a down-spin electron (J = −1/2) only recombines with a down-spin hole (J = −3/2) to release a left-handed circular polarized (σ_-) photon. The first (biexcitonic) photon to be released has equal probabilities (50%-50%) of being σ_+ or σ_-, while the second (excitonic) photon to be released should have the opposite polarization. If the time interval between the release of the first and second photons is much shorter than the spin phase relaxation time of electrons and holes, and also if the energies of spin-up and spin-down excitons in intermediate states become degenerate, then it is impossible to tell which route was taken by the system and the states of the two photons enter the following polarization triplet entangled state:[53]

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|\sigma_+\rangle_1|\sigma_-\rangle_2 + |\sigma_-\rangle_1|\sigma_+\rangle_2\right]$$

If the emission time interval between the first and second photons becomes longer than the spin-phase relaxation time, then the information about which route was taken by the system is leaked to the external bath, so the states of the two photons form a mixed state as follows:

$$\rho = \frac{1}{2}\left[|\sigma_+\rangle_{11}\langle\sigma_+| \otimes |\sigma_-\rangle_{22}\langle\sigma_-| + |\sigma_-\rangle_{11}\langle\sigma_-| \otimes |\sigma_+\rangle_{22}\langle\sigma_+|\right]$$

Figure 23 shows the results of experiments performed to confirm this fact.[55] Measurements were made of all the elements in a 4×4 polarization matrix

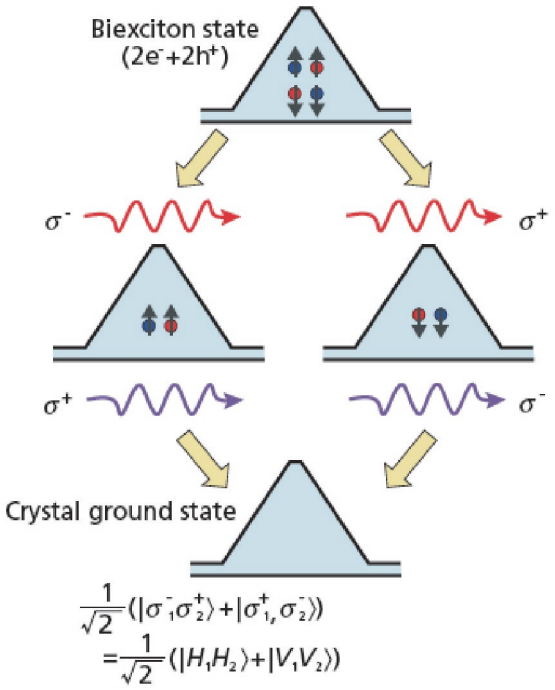


Fig. 22 An illustration showing how biexcitonic photon and excitonic photon from a single quantum dot are in a polarization entangled state

representing the polarization states of biexcitonic photons and excitonic photons. As a result, it was found that the polarization state of the two photons is not the entangled state but a mixed state consisting of $|H\rangle_1|H\rangle_2$ and $|V\rangle_1|V\rangle_2$. The reason for this is shown in Fig. 24.[55] When light emitted from the quantum dot is separated into H-polarized and V-polarized components input to a Michelson interferometer and the interference fringe is measured, each of these components is found to be exponentially decaying. The H-polarized and V-polarized waves have different decay constants because the resonant wavelength of the cavity is anisotropic and the exciton emission wavelength is close to the resonant wavelength for H-polarized waves. If the H-polarized and V-polarized waves are introduced into the Michelson interferometer without separating them first, then the interference fringe is found to oscillate with a period of

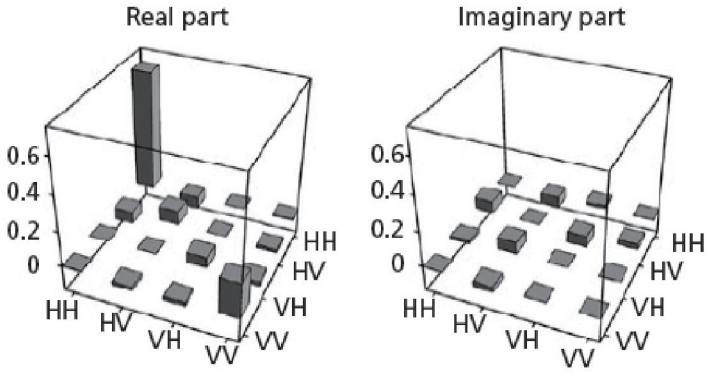


Fig. 23 Measurement results of a 4×4 matrix representing the polarization states of biexcitonic photon and excitonic photon from a quantum dot. The two photons form the mixed states of $|H\rangle_1|H\rangle_2$ and $|V\rangle_1|V\rangle_2$.

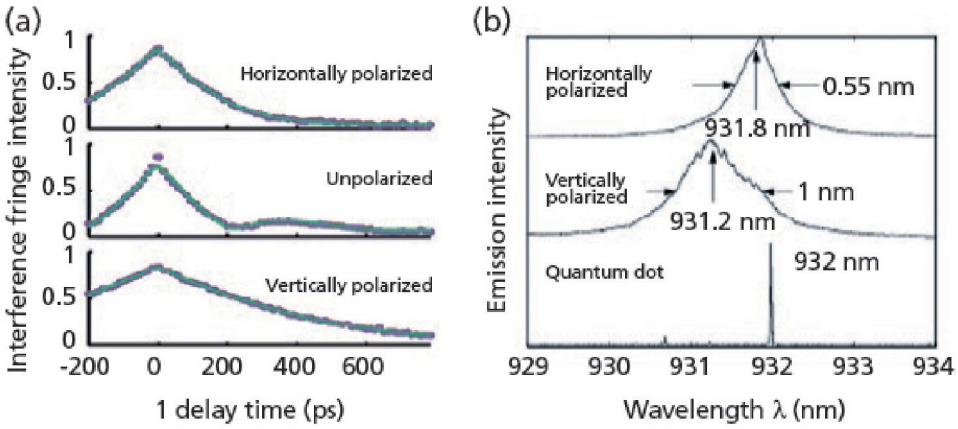


Fig. 24 (a) Variation of interference fringe intensity with delay time for H-polarized, V-polarized, and unpolarized light. (b) Cavity resonance characteristics and quantum dot excitonic emission spectra for H-polarized and V-polarized waves.

200 ps, as shown in Fig. 24(a). The period of this oscillation shows that the energy difference between the H-polarized and V-polarized photons is 13 μeV. That is, the energies of the excitons in the two spin states comprising the intermediate state are not degenerate. This is thought to be due to such effects as residual stress and anisotropy of the quantum-dot shape. Thus the system ends up in the mixed states $|H\rangle_1|H\rangle_2$ and $|V\rangle_1|V\rangle_2$ because the information about which paths the two photons were released along leaks out from the system via the energy of the excitonic photon.

If a microcavity can make the exciton emission lifetime much shorter than 200 ps, then the energy difference between the H-polarized and V-polarized waves would be hidden by natural linewidth. It therefore remains possible to generate polarization entangled states directly.

9 Photon number resolving detector (Visible Light Photon Counter)[56]

9.1 VLPC Operation Principle

Fig. 25 shows the structure of the VLPC detector.[24] Photons are presumed to come in from the left. The VLPC has two main layers, an intrinsic silicon layer and a lightly doped arsenic gain layer. The top of the intrinsic silicon layer is covered by a transparent electrical contact and an anti-reflection coating. The bottom of the detector is a heavily doped arsenic contact layer, which is used as a second electrical contact.

A single photon in visible wavelengths can be absorbed either in the intrinsic silicon region or in the doped gain region. This absorption event creates a sin-

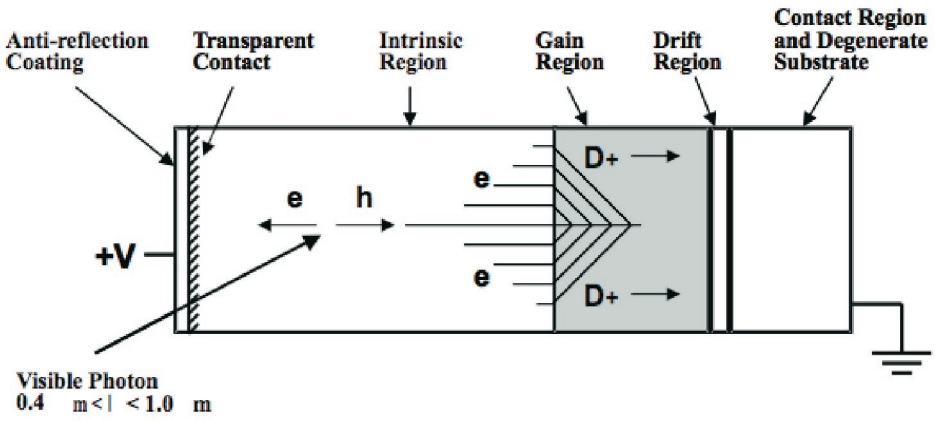


Fig. 25 Schematic of structure of the VLPC detector

gle electron-hole pair. Due to a small bias voltage (6 - 7.5 V) applied across the device, the electron is accelerated toward the transparent contact while the hole is accelerated toward the gain region. The gain region is moderately doped with As impurities, which are shallow impurities lying only 54 meV below the conduction band. The device is cooled to an operation temperature of 6 - 7 K, so there is insufficient thermal energy to excite donor electrons into the conduction band. These electrons are effectively frozen in the impurity state. However, when a hole is accelerated into the gain region it easily impact-ionizes these impurities, kicking the donor electrons into the conduction band. Scattered electrons can create subsequent impact-ionization events resulting in avalanche multiplication.

One of the nice properties of VLPC is that when an electron is impact-ionized from an As impurity, it leaves behind a hole in the impurity state, rather than in the valence band as in the case of APDs. The As doping density in the gain region is carefully selected such that there is partial overlap between the energy states of adjacent impurities. Thus, a hole trapped in the impurity state can travel through conduction hopping, a mechanism based on quantum-mechanical tunneling. This conduction hopping mechanism is slow; the hole never acquires sufficient kinetic energy to impact-ionize subsequent As sites. The only carrier that can create additional impact ionization events is the electron kicked into the conduction band. Thus, the VLPC has a natural mechanism for creating single carrier multiplication; the latter is known to reduce multiplication noise significantly[57].

One of the disadvantages of using shallow As impurities for avalanche gain is that these impurities can easily be excited by room-temperature thermal photons. IR photons with wavelengths of up to 30 μm can optically excite an impurity directly. These excitations can create extremely high dark count levels. The bi-layer structure of the VLPC helps to suppress this phenomenon. A visible photon can be absorbed both in the intrinsic and doped silicon regions. An IR photon, on the other hand, can only be absorbed in the doped region, as its energy is smaller than the bandgap of intrinsic silicon. Thus, the absorption length of IR photons is much smaller than visible photons. This suppresses the sensitivity of the device to IR photons at about 2%. Despite this suppression, background thermal radiation is very intense, requiring orders of magnitude of additional suppression.

9.2 Cryogenic system for operating the VLPC

In order to operate the VLPC we must cool it down to cryogenic temperatures to trap carriers in As impurities. We must also shield it from intense room-temperature thermal radiation. This is achieved by the cryogenic setup shown in Fig. 26.

The VLPC is held in a helium bath cryostat. A small helium flow is produced from the helium bath to the

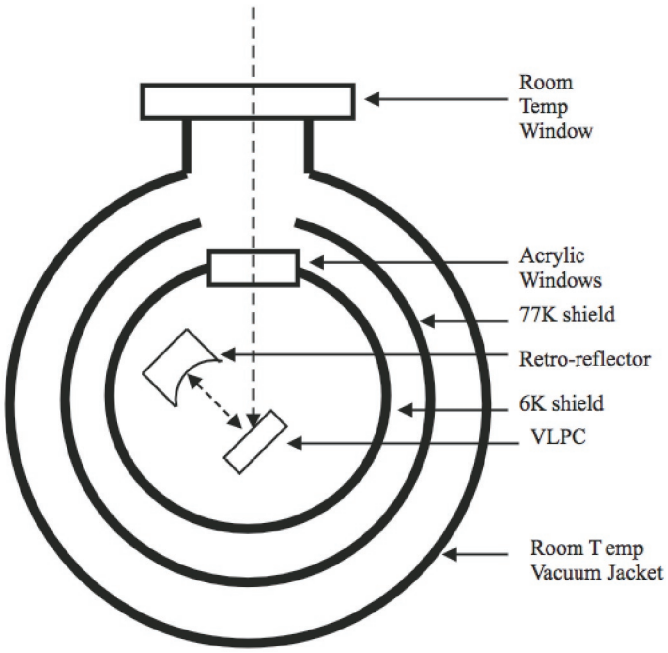


Fig. 26 Schematic of cryogenic setup for VLPC

cryostat cold finger by a needle valve. The helium bath is surrounded by a nitrogen jacket for radiation shielding. This improves the helium hold time. A thermal shroud, cooled to 77 K by direct connection to the nitrogen jacket, covers the VLPC and provides low-temperature shielding. This shroud is intended to improve the temperature stability of the detector by reducing the thermal radiation load. A hole at the front of the shroud allows photons to pass through. The detector itself is encased in a 6-K shield made of copper. The shield is cooled by direct connection to the cold plate of the cryostat. The front windows of the 6-K radiation shield, which are also cooled down to this temperature, are made of acrylic plastic. This material is highly transparent at optical frequencies, but is almost completely opaque from 2-30 μm. The acrylic windows provide us with the filtering of room temperature IR photons required to operate the detector. We achieve sufficient extinction of thermal background using 1.5-2 cm of acrylic material. In order to eliminate reflection loss from the window surfaces, the windows are coated with a broadband anti-reflection coating centered at 532 nm. Room temperature transmission measurements indicate 97.5% transmission efficiency through the acrylic windows.

The surface of the VLPC has a broadband anti-reflection coating centered around 550 nm. Nevertheless, due to the large index mismatch between silicon and air, there is still substantial reflection loss – on the order of 10%– even at the correct wavelength. In order to eliminate this reflection loss, the detector is rotated 45 degrees toward the direction of incoming light. A spherical refocussing mirror, with reflectance exceeding 99%, is used to redirect reflected light back onto the detector surface. A photon must reflect twice off of the surface in order to be lost, reducing reflection loss to less than 1%.

The VLPC features high multiplication gains of about 30,000 electrons per photo-ionization event. Nevertheless, this current must be amplified significantly to obtain a sufficiently large signal for subsequent electronics. The current is amplified by a series of broadband RF amplifiers. In order to minimize thermal noise from the amplifiers, the first amplification stage consists of a cryogenic preamplifier, which is cooled to 4 K by direct thermalization to the helium bath of the cryostat. The amplifier features a noise figure of 0.1 at operating frequencies of 30 - 500 MHz, with a gain of roughly 20 dB. The cryogenic amplifier is followed by additional commercial room-temperature RF amplifiers. The noise properties of these subsequent amplifiers is not as important, since the signal-to-noise ratio is dominated by the first cryogenic amplification stage. Using such a configuration, we achieve a 120-mV pulse of 3-ns duration when using 62 dB of amplifier gain.

9.3 Quantum efficiency and dark counts of the VLPC

The quantum efficiency of the VLPC has been studied at 650 nm.[25] QEs as high as 88% have been reported. The dark counts at this peak QE were 20,000 1/s. When correcting for reflection loss from the windows and detector surface, we estimate an intrinsic quantum efficiency of 95%.

9.4 Noise properties of the VLPC

The gain mechanism has an intrinsic associated noise process. That is, a single ionization event does not produce a deterministic number of electrons. The number of electrons the device emits fluctuates from pulse to pulse. This internal noise is referred to as excess noise, or gain noise. The amount of excess noise generated by a device strongly depends on the mechanism by which gain is achieved. Excess noise is typically quantified by a parameter F, referred to as the excess noise factor (ENF). The ENF is mathematically defined as:

$$F = \frac{\langle M^2 \rangle}{\langle M \rangle^2}$$

where M is the number of electrons produced by a photo-ionization event, and the bracketed notation represents a statistical ensemble average. Noise-free multiplication is represented by $F=1$. In this limit, a single photo-ionization event creates a deterministic number of additional carriers. Fluctuations in the gain process will result in an ENF exceeding 1.

The noise properties of an avalanche photo-diode are well characterized in the "Markov" limit.[57] In this limit, the impact-ionization probability for a carrier in the depletion region is a function of the local electric field intensity at the location of the carrier. In this sense, each impact-ionization event is independent of past history. Under this assumption the ENF of an APD was calculated. The ENF depends on the number of carriers that can participate in the avalanche process. If both electrons and holes are equally likely to impact-ionize, then $F \approx \langle M \rangle$. In the large gain limit, the ENF is very large. Restricting the impact-ionization process only to electrons or holes significantly reduces gain noise. In this ideal limit, we have $F=2$. This limit represents the best noise performance achievable within the Markov process.

Photomultiplier tubes (PMTs) are known to have better noise characteristics than APDs. The ENF of a typical PMT is around 1.2. This suppressed noise is due to the fact that in a PMT a carrier is scattered off

of a fixed number of dynodes. The only noise in the process corresponds to the number of electrons emitted by each dynode per electron.

Theoretical studies of multiplication noise have predicted that the VLPC should feature suppressed avalanche multiplication noise.[58] This prediction is due to two dominant effects. First, because only electrons can cause impact ionization, the VLPC features a natural single-carrier multiplication process. Second, the VLPC does not require high electric-field intensities to operate. This is because impact-ionization events occur off of shallow arsenic impurities that are only 54 meV from the conduction band. Thus, carriers need not acquire a great deal of kinetic energy in order to scatter the impurity electrons. Because of the lower electric-field intensities, a carrier requires a fixed amount of time before it can generate a second impact ionization. This delay time represents a deviation from the Markov approximation, and is predicted to suppress multiplication noise.[58] The ENF of the VLPC has been experimentally measured to be less than 1.03.[26],[27] Thus, the VLPC features nearly noise-free multiplication, as predicted by the theory. This low-noise property will play an important role in multi-photon detection, which we will discuss next.

9.5 Multi-photon detection with the VLPC

The nearly noise-free avalanche gain process of the VLPC opens the door to multi-photon detection. When two photons are detected by the VLPC, we expect the number of electrons emitted by the detector to be twice that of single-photon detection. If the photons arrive within a time interval that is much shorter than the electronic output pulse duration of the detection system, then we expect to see a detection pulse that is twice as high.

In the limit of noise-free multiplication, this would certainly be the case. A single detection event would create M electrons, while a two-photon event would create $2M$ electrons. Higher order photon-number detection would follow the same pattern. After amplification, the area or height of the detector pulse would allow us to determine the precise number of detected photons, even if they were to arrive on extremely short time scales.

In the presence of multiplication noise, the situation becomes more complicated. The pulse height of a one-photon pulse will fluctuate, as will that of a two-photon pulse. A finite probability of detecting only one photon emerges, but due to multiplication noise the height of the pulse appears to be more consistent with a two-photon event, and vice versa. Our ability to determine the number of detected photons thus becomes a question of signal-to-noise ratio.

There are ultimately two effects that will limit multi-photon detection. One is the quantum efficiency of the detector. If we label quantum efficiency as η, then the probability of detecting n photons is given by η^n, assuming detector saturation is negligible. Thus, detection probability is exponentially small in η. For larger n this may produce extremely low efficiencies. The second limitation is the electrical detection noise, as previously discussed. There are two factors contributing to electrical noise: the excess noise of the detector and the thermal noise originating from amplifiers and subsequent electronics.

In the absence of detection inefficiency and amplifier noise, multiplication noise will ultimately limit the number of simultaneously distinguishable photons. Defining σ_m as the standard deviation of multiplication gain, the fluctuations of an n photon peak will be given by $\sqrt{n}\,\sigma_m$. This is because the n photon pulse is simply the sum of n independent single-photon pulses from different locations within the VLPC active area. Summing the pulses also causes the variance to sum, resulting in the buildup of multiplication noise. The mean pulse-height separation between the n photon peak and the $n-1$ photon peak, however, is constant, being simply proportional to $\langle M \rangle$, average multiplication gain. At some sufficiently high photon number, the fluctuations in emitted electrons will be so large that there is little distinction between an n and $n-1$ an photon-detection event. We can arbitrarily establish a cutoff number at the point at which the fluctuations in emitted electrons are equal to the average difference between an n and $n-1$ an photon-detection event. In this limit, the maximum photon number we can detect is:

$$N_{\max} = \frac{1}{F-1}$$

Using the above condition as a cutoff, we see that even an ideal APD with $F=2$ cannot discriminate between one- and two-photon events. A PMT with $F=1.2$ could potentially be useful for up to five-photon detection, but due to the low QEs of PMTS, this is typically impractical. The VLPC, with $F<1.03$, could potentially distinguish more than 30 photons, with potential 95% quantum efficiency.

Fig. 27 shows a sample oscilloscope pulse trace of a VLPC pulse after the room-temperature amplifiers. The output features an initial sharp negative peak of about 2 ns full-width at half-maximum. A positive overshoot follows, the result of the 30-MHz high-pass feature of the cryogenic amplifiers. If we compare the variance in electrical fluctuations before the pulse to the minimum pulse value, we determine the signal-to-

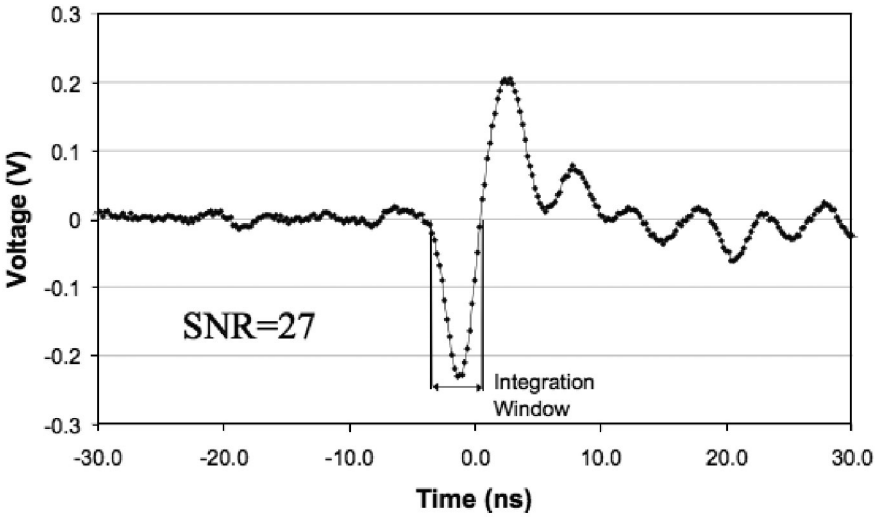


Fig. 27 Oscilloscope pulse trace of VLPC output after room-temperature RF amplifiers

noise ratio (SNR) to be 27. The figure also illustrates the integration window used by the boxcar integrator, which captures only the negative lobe of the pulse.

In order to measure multi-photon detection capability, we attenuate the laser to about 1 - 5 detected photons per pulse. For each laser pulse, the output of the VLPC is integrated and digitized. Fig. 28 shows pulse area histograms for four different excitation powers. The area is expressed in arbitrary units determined by the analog-to-digital converter. Because the pulse area is proportional to the number of electrons in the pulse, the pulse area histogram is proportional to the probability distribution of the number of electrons emitted by the VLPC. This probability distribution features a series of peaks. The first peak is a zero-photon event, followed by a one-photon event, a two-photon event, and so on. In the absence of electronic noise and multiplication noise, these peaks would be perfectly sharp, and we would be able to determine photon number unambiguously. Due to electronic noise, however, the peaks become broadened and start to overlap partially. The broadening of the zero-photon peak is due exclusively to electronic noise. Note that the boxcar integrator adds an arbitrary constant to the pulse area, so that the zero-photon peak is centered around 450 instead of 0. The one-photon peak is broadened by both electronic noise and multiplication noise. Thus, the variance of the one-photon peak is bigger than that of the zero-photon peak. As the photon number increases, the width of the pulses also increases due to buildup of multiplication noise. This eventually causes the smearing out of the probability distribution at around the seven-photon peak.

In order to analyze the results numerically, we fit each peak to a gaussian distribution. Theoretical studies predict that the distribution of the one-photon peak is a bi-sigmoidal, rather than a gaussian distribution.[58] However, when the multiplication gain is large, as in the case of the VLPC, this distribution is well approximated by a gaussian distribution. We use this approximation because higher photon number events are sums of multiple single photon events. A gaussian distribution has a convenient property in that the sum of gaussian distributions is also a gaussian distribution. In the limit of large photon numbers we expect this approximation to improve even further due to the central limit theorem.

Fig. 28 shows the results of the fits for each excitation intensity. The dotted lines plot the individual gaussian distributions for the different photon numbers, and the solid line plots the sum of all of the gaussian distributions. The diamond markers represent the measured data points. Table II shows the center value and standard deviation of the different peaks in panel c of the figure. In order to perform photon-number counting we must establish a decision region for each photon-number state. This will depend, in general, on the a priori photon-number distribution. We consider the case of equal a priori probability, which is the worst-case scenario. For this case, the optimal decision threshold between two consecutive gaussian peaks is given by the point at which they intersect.

The probability of error for this decision is given by the area of all other photon-number peaks in the decision region. This probability is also shown in Table II.

From the data we would like to infer whether the

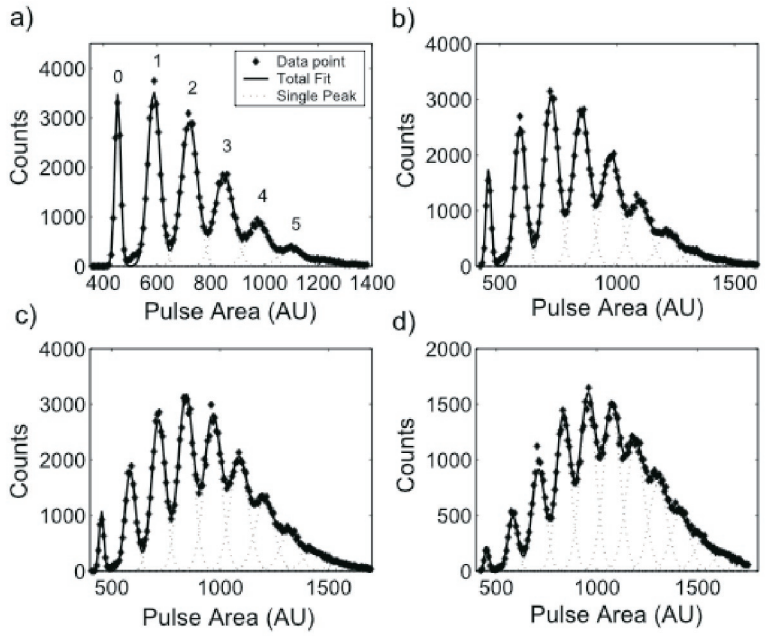


Fig. 28 Pulse area spectrum generated by the boxcar integrator for four different excitation powers. The dotted lines represent the fitted distribution of each photon number peak. The solid line is the total sum of all peaks. Diamonds denote measured data points. Each peak represents a photon number event, starting with zero photons for the first peak.

VLPC is being saturated at higher photon numbers. If too many photons are simultaneously incident on the detector, the detector surface may become depleted of active areas. This would result in reduced quantum efficiency for higher photon numbers. In order to investigate this possibility, we add an additional constraint to the fit, stipulating that the pulse areas must scale according to a Poisson distribution. Since the laser is a Poisson light source, we expect this to be the case. However, if saturation becomes a factor, we would observe a number-dependant loss. This would result in deviation from Poisson detection statistics. In Fig. 29 we plot the result of the fit when the peak areas scale as a Poisson distribution. One can see that the imposition of Poisson statistics does not change the fitting result in an appreciable way. Thus, we infer that detector saturation is not a strong effect at the excitation levels that we are using.

Photon number	Avg. Area	Std. Dev.	%Error
0	0	10.6	0.01
1	135	24.8	1.1
2	275	31.7	3.4
3	416	35.3	6.1
4	561	39.0	8.5
5	709	42.2	10.6
6	859	44.5	11.3

TABLE II Results of fit for panel (c) of Fig. 28

The effect of multiplication noise buildup on the pulse-height spectrum can be investigated from the previous data. In general, we expect the pulse-area variance to be a linearly increasing function of photon number. This is consistent with the independent detection model, in which an n photon peak is a sum of n single-photon peaks coming from different areas of the detector. To investigate the validity of this model, we plot variance as a function of photon number in Fig. 30. Electrical noise variance, given by the zero-photon peak, is subtracted. The variance is fit to a linear model given by

$$\sigma_i^2 = \sigma_0^2 + i\sigma_M^2$$

In the above model, i is the photon number, σ_M^2 is the variance contribution from multiplication noise, and σ_0^2 is a potential additive noise term. From the data, we obtain the values $\sigma_M^2 = 276$, *and* $\sigma_0^2 = 246$.

A surprising aspect of this result is the large value of σ_0^2. We expect that since electrical noise has been subtracted, the only remaining contribution to the variance is multiplication noise. If this were true, the value of σ_0 would be very small. Instead we obtain a value nearly equal to that of σ_M^2. This may indicate that electrical noise is higher when the VLPC is firing than

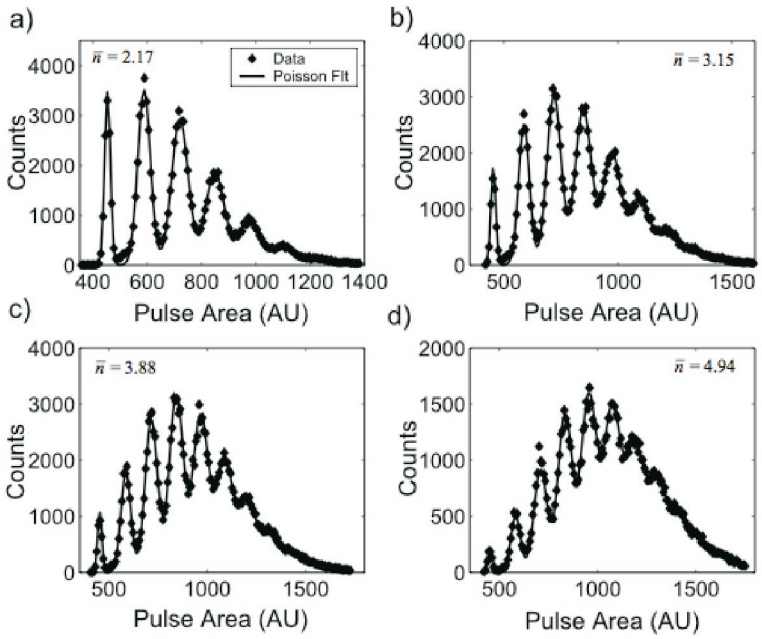


Fig. 29 Pulse area spectrum fit to Poisson constraint on normalized peak areas

when it is not. A change in the resistance of the device during the avalanche process may affect the noise properties of subsequent amplification circuits. Further investigation is required in order to determine whether this additive noise is inherent in the device or whether it can be eliminated in principle.

The above measurements of variance versus photon number give us a very accurate measurement of the excess noise factor F of the VLPC. Previous measurements of F for the VLPC have determined that it is less than 1.03,[26] which corresponds to nearly noise-free multiplication. This number was obtained by measuring the variance of the one-photon peak and comparing this variance to the mean. However, it is difficult to separate the contribution of electrical noise

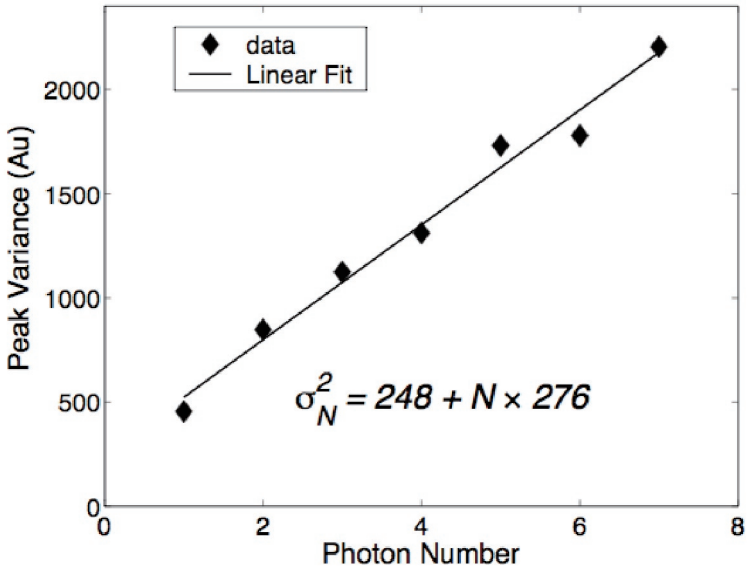


Fig. 30 Variance as a function of photon-number detection. The linear relation is consistent with the independent detection model.

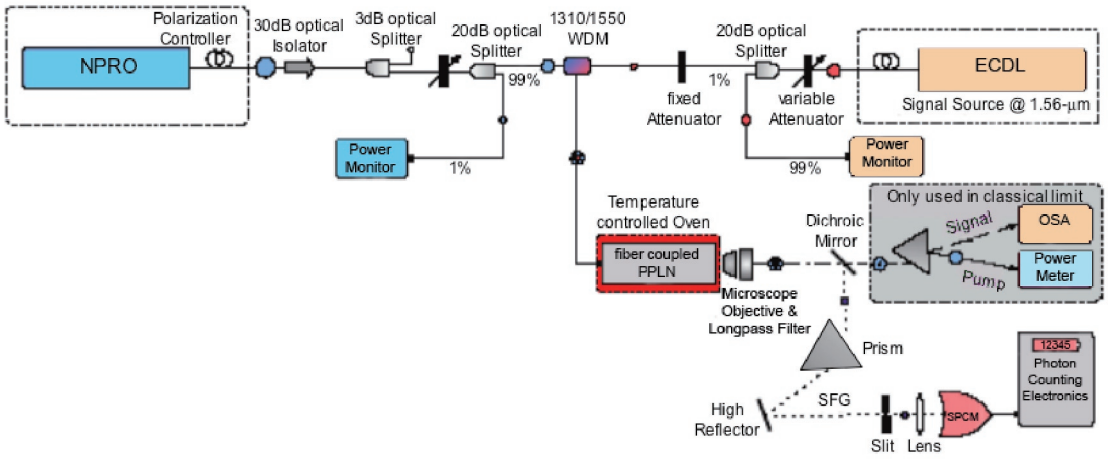


Fig. 31 Experimental setup for single-photon detection at 1.56 μm

from that of internal multiplication noise using this technique. Thus, the measurement ultimately determines only the upper boundary of F. By considering the way variance scales with photon numbers, as we have done in Fig. 30, multiplication noise can be accurately differentiated from additive electrical noise. This allows us to calculate an exact value for the excess noise factor. From our measurement of σ_M^2 and $\langle M \rangle$, we obtain an excess noise factor of $F = 1.015$.

10 Frequency up-conversion in PPLN waveguides

Current single-photon detectors operating at IR wavelengths, such as InGaAs/InP avalanche photodiodes (APDs), suffer from several drawbacks. Due to after-pulses from trapped charge carriers causing large dark count (DC) rates, these detectors have to be operated in gated mode, employing active or passive quenching circuits. For applications where the arrival time of a signal photon is not known a priori, gated-mode operation limits the usefulness of such detectors. Since the probability of after-pulses decreases with increasing temperature while quantum efficiency (QE) decreases with increasing temperature, and conversely, after-pulse probability and QE both increase with decreasing temperature, there is a tradeoff between detection efficiency and speed.

On the other hand, commercially available silicon-based single-photon counting modules (SPCMs) are highly efficient (>70% at 700 nm) and feature low DC rates (~25/s). These detectors also offer Geiger-mode operation with short dead-times (50 ns typ.).

With the help of highly efficient nonlinear optical frequency converters, one can detect 1.5-μm radiation while taking advantage of the properties of NIR SPCMs. We accomplish this by sum-frequency gener-

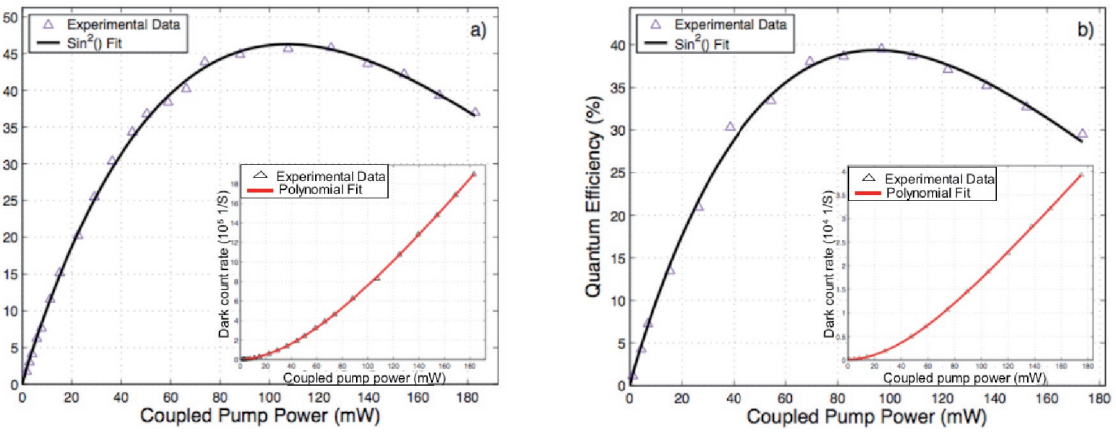


Fig. 32 Quantum efficiencies and dark count rates for a) 1.56-μm and b) 1.32-μm single-photon detection experiment.

ation between a weak signal and a strong pump in a reverse proton exchanged (RPE) periodically poled $LiNbO_3$ (PPLN) channel waveguide[28], followed by efficient detection using an SPCM. DC rates are currently limited by parasitic nonlinear interactions inside the nonlinear crystal, while overall system detection efficiency is determined as follows. Waveguides allow 100% internal signal conversion with low average pump power due to tight mode confinement over distances of several centimeters.[59] Hence, the internal QE of the device is only limited by propagation loss, while the external QE is further reduced by coupling and reflection loss. Finally, overall system detection efficiency has to take collection efficiency and the SPCM's intrinsic QE into account. RPE waveguides with large conversion efficiencies, low propagation loss ($0.1^{dB}/_{cm}$), and input-mode filters for efficient fiber-to-waveguide coupling have been fabricated.

As shown in Fig. 31, a highly attenuated infrared signal is combined inside a wavelength division multiplexer (WDM) with a strong pump before being injected into the fiber-pigtailed PPLN waveguide device, heated to 75 °C in a temperature-controlled oven. To detect single photons at 1.55 μm, a fiber-coupled non-planar ring oscillator (NPRO) at 1.32 μm was used as the pump source (as shown in Fig. 31), while detection at 1.32 μm was achieved using an amplified C-band external cavity tunable diode laser (ECDL) as the pump. The converted signal, pump, and spurious light after the chip were separated using a combination of a long/short-pass filter, a prism, and a spatial filter. The light was then focused onto the SPCM using a high NA lens coated for the NIR.

Experimental results are shown in Fig. 32. The QE was calculated by dividing the number of detected counts after DC subtraction and detector linearity correction by the number of signal photons before the WDM as measured by a fiber-coupled power meter. Neither loss terms nor SPCM detection efficiency were taken into account to arrive at these QEs, leading to true overall system detection efficiency. We achieved an overall QE of 46% at 1.56 μm and 40% at 1.32 μm. The DC rates at these pump power levels were 8×10^5 cps and 1.5×10^4 cps, respectively. These rates are partially due to spontaneous Raman scattering inside the fiber leading to the PPLN waveguide followed by up-conversion inside the device, but are mainly generated by spurious nonlinear interactions inside the waveguide itself (e.g. spontaneous Raman scattering). Variations in QE can be explained by the transmission characteristics of the filters used in this setup.

Since the PPLN waveguide chip was not anti-reflection (AR) coated, Fresnel reflections off of the facets reduced the QE by 19.7 %. Such an AR coating will increase the QE to 55% and 48% for 1.56μm and 1.32μm single-photon detection using the current setup. Improvements in design and fabrication of the PPLN waveguide device will further increase the QE by lowering the propagation and coupling loss, as well as reduce the required pump power by 20-30%. Since the DC rate strongly depends on the pump power level, we expect ~50% fewer dark counts.

11 Future prospects

The generation of a regulated single-photon stream at the Fourier transform limit and the detection of single photons and multiple photons with low error probability opened the door to various quantum information processing systems using photonic qubits, including the generation of entangled photon pairs, BBM92 quantum cryptography, quantum teleportation, quantum repeaters, and linear optical quantum computation.

When considering the future of quantum information technology, we can envision that it will be necessary to encode information on photonic qubits in quantum communication while storing information on nuclear spin qubits in quantum memory. Electron spin will no doubt play an important role as an interface between the two fields. It is hoped that a great deal of practical knowledge will develop relating to means of connecting these three qubit systems.

12 Acknowledgements

The authors wish to thank J. Kim, O. Benson, M. Pelton, K. Inoue, S. Takeuchi, B. Zhang, and J. Plant for their critical contributions to the early stage of this work. This work is partially supported by ICORP/SORST for Quantum Entanglement (JST) and MURI for Photonic Quantum Information Systems (ARMY, DAAD19-03-1-0199).

References

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proc. IEEE Int. Conf. on Computers Systems and Signal Processing*, Bangalore, India, p. 175., 1984.

[2] N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, no. 5, p. 2304, 2000.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, p. 661, 1991.; C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, p. 557, 1992.

[4] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons

against individual attacks," *Phys. Rev. A*, vol. 65, no. 5, p. 2310, 2002.

[5] P. G. Kwiat, K. Mattle, H. Weinfurther, and A. Zeilinger, "New High-Intensity Source of Polarization-Entangled Photon Pairs," *Phys. Rev. Lett.*, vol. 75, p. 4337, 1995.

[6] L. Duan, M. Lukin, J. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, pp. 413-418, 2001.

[7] E. Knill, R. Laflamme, and G. J. Milburn, "Efficient linear optics quantum computation," *Nature*, vol. 409, pp. 46-52, 2001.

[8] A. Kuhn, M. Hennrich, and G. Rempe, "Deterministic Single-Photon Source for Distributed Quantum Networking," *Phys. Rev. Lett.*, vol. 89, no. 6, p. 7901, 2002.

[9] A. Kuzmich, W. P. Bowen, A. D. Boozer, A. Boca, C. W. Chou, L. M. Duan, and H. J. Kimble, "Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles," *Nature*, vol. 423, pp. 731-734, 2000.

[10] Ch. Schwedes, Th. Becker, J. von Zanthier, H. Walther, and E. Peik, "Laser sideband cooling with positive detuning," *Phys. Rev. A*, vol. 69, no. 5, p. 3412, 2004.

[11] B. Lounis and W. E. Moerner, "Single photons on demand from a single molecule at room temperature," *Nature*, vol. 407, pp. 491-493, 2000.

[12] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, "Triggered Source of Single Photons based on Controlled Single Molecule Fluorescence," *Phys. Rev. Lett.*, vol. 83, p. 2722, 1999.

[13] R. Brouri, A. Beveratos, J. P. Poizat, and P. Grangier, "Photon antibunching in the fluorescence of individual color centers in diamond," *Opt. Lett.*, vol. 25, pp. 1294-1296, 2000.

[14] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, "Stable Solid-State Source of Single Photons," *Phys. Rev. Lett.*, vol. 85, p. 290, 2000.

[15] A. Imamoglu and Y. Yamamoto, "Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined *p-í-n* heterojunctions," *Phys. Rev. Lett.*, vol. 72, p. 210, 1994.; Y. Yamamoto, "A Photon in Solitary Confinement," *Nature*, vol. 390, pp. 17-18, 1997.

[16] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, "A Single-Photon Turnstile Device," *Nature*, vol. 397, pp. 500-503, 1999.

[17] C. Santori, M. Pelton, G. S. Solomon, Y. Dale, and Y. Yamamoto, "Triggered Single Photons from a Quantum Dot," *Phys. Rev. Lett.*, vol. 86, p. 1502, 2001.

[18] G. S. Solomon, M. Pelton, and Y. Yamamoto, "Single-mode Spontaneous Emission from a Single Quantum Dot in a Three-Dimensional Microcavity," *Phys. Rev. Lett.*, vol. 86, p. 3903, 2001.

[19] J. Vuckovic, D. Fattal, C. Santori, G. S. Solomon, and Y. Yamamoto, "Enhanced single-photon emission from a quantum dot in a micropost microcavity," *Appl. Phys. Lett.*, vol. 82, no. 21, pp. 3596-3598, 2001.

[20] C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "Indistinguishable Photons from a Single-Photon Device," *Nature*, vol. 419, pp. 594-597, 2002.

[21] E. Waks, K Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "Quantum Cryptography with a Photon Turnstile," *Nature*, vol. 420, p. 762, 2002.

[22] D. Fattal, K. Inoue, J. Vuckovic, C. Santori, G. S. Solomon, and Y. Yamamoto, "Entanglement Formation and Violation of Bell's Inequality with a Semiconductor Single Photon Source," *Phys. Rev. Lett.*, vol. 92, no. 3, p. 7903, 2004.

[23] D. Fattal, E. Diamante, K. Inoue, and Y. Yamamoto, "Quantum Teleportation with a Quantum Dot Single Photon Source," *Phys. Rev. Lett.*, vol. 92, no. 3, p. 7904, 2004.

[24] M. Atac, J. Park, D. Cline, D. Chrisman, M. Petroff, and E. Anderson, *Nucl. Instrum. Meth. Phys. Res. A*, vol. 314, p. 56, 1992.

[25] S. Takeuchi, J. Kim, Y. Yamamoto, and H. Hogue, "Development of a high-quantum-efficiency single-photon counting system," *Appl. Phys. Lett.*, vol. 74, p. 1063, 1999.

[26] J. Kim, Y. Yamamoto, and H. Hogue, "Noise-free avalanche multiplication in Si solid state photomultipliers," *Appl. Phys. Lett.*, vol. 70, p. 2852, 1997.

[27] J. Kim, S. Takeuchi, Y. Yamamoto, and H. Hogue, "Multiphoton detection using visible light photon counter," *Appl. Phys. Lett.*, vol. 74, p. 902, 1999.

[28] K. R. Parameswaran, R. K. Route, J. R. Kurz, R. V. Roussev, M. M. Fejer, and M. Fujimura, "Highly efficient second-harmonic generation in buried waveguides formed by annealed and reverse proton exchange in periodically poled lithium niobate," *Opt. Lett.*, vol. 27, pp. 179-181, 2002.

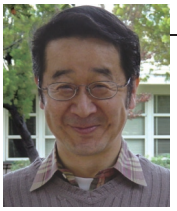
[29] C. Santori, G. S. Solomon, M. Pelton, and Y. Yamamoto, "Time-resolved spectroscopy of multiexcitonic decay in an InAs quantum dot," *Phys. Rev. B*, vol. 65, no. 7, p. 3310, 2002.

[30] P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, Lidong Zhang, E. Hu, and A. Imamoglu, "A Quantum Dot Single-Photon Turnstile Device," *Science*, vol. 290, pp. 2282-2285, 2000.

[31] E. Moreau, I. Robert, J. M. Gerard, I. Abram, L. Manin, and V. Thierry-Mieg, "Single-mode solid-state single photon source based on isolated quantum dots in pillar microcavities," *Appl. Phys. Lett.*, vol. 79, p. 2865, 2001.

[32] V. Zwiller, H. Blom, P. Jonsson, N. Panev, S. Jeppesen, T. Tsegaye, E. Goobar, M. Pistol, L. Samuelson, and G. Bjork, "Single quantum dots emit single photons at a time: Antibunching experiments," *Appl. Phys. Lett.*,

vol. 78, p. 2476, 2001.
[33] Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, "Electrically driven single photon source," *Science*, vol. 295, pp. 102-105, 2002.
[34] J. Vuckovic, M. Pelton, A. Scherer, and Y. Yamamoto, "Optimization of three-dimensional micropost microcavities for cavity quantum electrodynamics," *Phys. Rev. A*, vol. 66, no. 2, p. 3808, 2002.
[35] M. Pelton, J. Vuckovic, G. S. Solomon, A. Scherer, and Y. Yamamoto, "Three-dimensionally confined modes in micropost microcavities: quality factors and Purcell factors," *IEEE J. Quantum Electron.*, vol. 38, no. 2, pp. 170-177, 2002.
[36] M. Pelton, C. Santori, J. Vuckovic, B. Zhang, G. S. Solomon, J. Plant and Y. Yamamoto, "Efficient Source of Single Photons: A Single Quantum Dot in a Micropost Microcavity," *Phys. Rev. Lett.*, vol. 89, no. 23, p. 3602, 2002.
[37] M. Bayer and A. Forchel, "Temperature dependence of the exciton homogeneous linewidth in $In_{0.60}Ga_{0.40}As$/GaAs self-assembled quantum dots," *Phys. Rev. B*, vol. 65, no. 4, p. 1308, 2002.
[38] H. Fearn and R. Loudon, *J. Opt. Soc. Am.*, vol. B6, p. 917, 1989.
[39] S. Popescu, L. Hardy, and M. Zukowski, "Revisiting Bell's theorem for a class of down-conversion experiments," *Phys. Rev. A*, vol. 56, pp. R4353-R4356, 1997.
[40] A. Aspect, J. Dalibard, and G. Roger, "Experimental Test of Bell's Inequalities Using Time-Varying Analyzers," *Phys. Rev. Lett.*, vol. 49, pp. 1804-1807, 1982.
[41] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New High-Intensity Source of Polarization-Entangled Photon Pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337-4341, 1995.
[42] J. Clauser, M. Horne, A. Shimony, and R. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories," *Phys. Rev. Lett.*, vol. 23, pp. 880-884, 1969.
[43] A. G. White, D. F. V. James, P. H. Eberhard, and P. G. Kwiat, "Nonmaximally Entangled States: Production, Characterization, and Utilization," *Phys. Rev. Lett.*, vol. 83, pp. 3103-3107, 1999.
[44] A. Peres, "Separability Criterion for Density Matrices," *Phys. Rev. Lett.*, vol. 77, pp. 1413-1415, 1996.
[45] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn, "Realization of quantum process tomography in NMR," *Phys. Rev. A*, vol. 65, no. 1, p. 2314, 2002.
[46] T. Pitman, M. Fitch, B. Jacobs, and J. Franson, "Experimental controlled-NOT logic gate for single photons," *Quantph*, 0303095, 2003.
[47] D. Gottesman and I. L. Chuang, *Nature*, 402, 390, 1999.
[48] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895-1899, 1993.
[49] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Nature*, vol. 390, no. 575, 1997.
[50] J. Franson, M. Donegan, M. Fitch, B. Jacobs, and T. Pitman, "High-Fidelity Quantum Logic Operations Using Linear Optical Elements," *Phys. Rev. Lett.*, vol. 89, no. 13, p. 7901, 2002.
[51] E. Lombardi, F. Sciarrino, S. Popescu, and F. De Martini, "Teleportation of a Vacuum–One-Photon Qubit," *Phys. Rev. Lett.*, vol. 88, no. 7, p. 402, 2002.
[52] A. Kuhn, M. Heinrich, and G. Rempe, "Deterministic Single-Photon Source for Distributed Quantum Networking," *Phys. Rev. Lett.*, vol. 89, no. 6, p. 7901, 2002.
[53] E. Waks, C. Santori, and Y. Yamamoto, "Security aspects of quantum key distribution with sub-Poisson light," *Phys. Rev. A*, vol. 66, no. 4, p. 2315, 2002.
[54] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, "Regulated and Entangled Photons from a Single Quantum Dot," *Phys. Rev. Lett.*, vol. 84, pp. 2513-2616, 2000.
[55] C. Santori, D. Fattal, M. Pelton, G. S. Solomon, and Y. Yamamoto, "Polarization-correlated photon pairs from a single quantum dot," *Phys. Rev. B*, vol. 66, no. 4, p. 5308, 2002.
[56] E. Waks, K. Inoue, W. D. Oliver, E. Diamanti, and Y. Yamamoto, *IEEE J. Quantum Electron.*, vol. 9, p. 1502, 2003.
[57] R. J. McIntyre, "Multiplication noise in uniform avalanche diodes," *IEEE Trans. Electron Devices*, vol. ED-13, pp. 164-168, 1966.
[58] R. LaViolette and M. Stapelbroek, "A non-Markovian model of. avalanche gain statistics for solid-state photomultiplier," *J. Appl. Phys.*, vol. 65, pp. 830-836, 1989.
[59] R. V. Roussev, C. Langrock, J. R. Kurz, and M. M. Fejer, "Periodically poled lithium niobate waveguide sum-frequency generator for efficient single-photon detection at communication wavelengths," *Opt. Lett.*, vol. 29, no. 13, pp. 1518-1520, 2004.

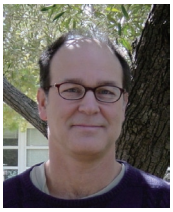


Yoshihisa YAMAMOTO

Received a B. S. from Tokyo Institute of Technology in 1973 and Ph.D. from the University of Tokyo in 1978, and has been working at Stanford University as a Professor of Applied Physics and Electrical Engineering since 1992 and at National Institute of Informatics as a Professor since 2003. He is also an NTT R&D Fellow, and a supervisor for the JST CREST program on quantum information. His current research areas include quantum optics, mesoscopic physics, solid-state NMR spectroscopy and quantum information.

Charles SANTORI

Charles Santori received a B.S. in Physics from Massuchusetts Institute of Technology in 1997 and a Ph.D in Applied Physics from Stanford University in 2003. At Stanford he worked in Prof. Yamamoto's group on topics including generation of indistinguishable single photons and correlated photon pairs using semiconductor quantum dots. He currently works at HP Laboratories in Palo Alto, California, where his research topics include quantum optics and nanophotonics.

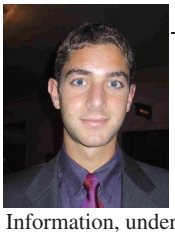


Glenn SOLOMON

Glenn Solomon received B.S. and M.S. degrees from Duke University, and M.S. and Ph.D. degrees from Stanford University. He has worked at Research Triangle Institute from 1983-1989. He is currently in the Electrical Engineering department at Stanford University where his research is related to semiconductor heterostructures for optical and spin-based systems. He is the founder and president of a start-up company, CBL Technologies, Inc.

Jelena VUCKOVIC

Jelena Vuckovic received the Ph.D. degree in Electrical Engineering in 2002 from the California Institute of Technology (Caltech) in Pasadena, California, for her work on photonic crystal-based optical and quantum optical devices. In 2002, she was a postdoctoral scholar in Yoshi Yamamoto's group at Stanford University, where she worked on quantum dot-micropost microcavity single photon sources. She joined the Electrical Engineering Faculty at Stanford as an Assistant Professor in January of 2003. Her research interests span a range of topics in nanoscale and quantum photonics, from photonic crystals and nanofabrication, to semiconductor cavity quantum electrodynamics and quantum information science.



David FATTAL

Received the diplome from Ecole Polytechnique (France) in 2001. He is currently a PhD candidate in the physics department at Stanford University, where he does experimental and theoretical research in the field of Quantum Information, under the supervision of Professor Yamamoto.

Edo WAKS

Edo Waks received his B.Sc. in 1995, and M.Sc. in 1996, in Electrical Engineering from Johns Hopkins University in Baltimore, MD. He received his Ph.D. in 2003 from the Electrical Engineering Department at Stanford University. He is currently working as a postdoctoral fellow at Stanford, under a Department of Central Intelligence Postdoctoral fellowship, where he is investigating the application of photonic crystal devices for applications in quantum optics and quantum information.

Eleni DIAMANTI

Eleni Diamanti received the B.S degree in electrical and computer engineering from the National Technical University of Athens, Greece, in 2000, and the M.S. degree in electrical engineering from Stanford University, in 2002. She is currently pursuing the Ph.D. degree at Stanford University. Her research interests are in the area of quantum optics and quantum information processing, and particularly in single-photon detectors and sources at telecommunication wavelengths, and their applications in quantum cryptography.