Translated from the original Japanese version, OYO BUTURI Vol.72, No.2, p.146 (2003)

Cutting Edge

Single photons for quantum information systems

Yoshihisa YAMAMOTO

This paper introduces the current state of the development of single photon sources 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 with a high repetition speed. It is expected that this technique will not only prove to be useful for BB84 quantum cryptography using single photons, but will also find applications in other fields 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 limited, EPR-Bell state, two photon interference, quantum cryptography, quantum teleportation, quantum computation

1. Introduction

Improvements in the protection of privacy and the ability to analyze complex systems are important issues to be addressed in the fields of information science and physical science in the 21st century. The former is needed to guarantee the security of personal information in telecommunications and computer systems, and the latter is needed to realize computer hardware and software that can process very large amounts of data in fields such as predicting weather patterns, analyzing ecological phenomena, controlling traffic and estimating stock market fluctuations.

Quantum information research has progressed rapidly in recent years in the hope of addressing these needs. This field of research covers many topics, and is developing at an unprecedented scale with the involvement of researchers from many different leading-edge science and technology fields. Although it is very hard to predict how things will turn out in the future, it seems 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 quantum information processing to connect them together. This paper introduces the latest research trends relating to the production of photonic qubits used for quantum communication and computation, with particular reference to the results obtained by the author's group.

In quantum cryptography,[1] the security of schemes that involve communication using an ordinary Poisson light source (such as the BB84 protocol which uses a semiconductor laser) can be threatened by an eavesdropper's photon splitting attack (i.e., secretly extracting and measuring a single photon when there are 2 or more photons in a pulse).[2] Even in the Ekert91 or BBM92 protocols for quantum cryptography using EPR-Bell photon pairs produced by parametric downconversion,[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 definite time intervals.

Methods have been proposed for implementing optical quantum information processing techniques that are more advanced than quantum cryptography, such as quantum teleportation,[5] quantum repeaters,[6] and linear optics quantum computers.[7] For such applications, it is essential to generate large numbers of single photons at definite time intervals that satisfy the condition of "indistinguishable quantum particles".

Various methods are currently being investigated for the production of single photons at definite time intervals, including methods that use single atoms, single ions, single molecules or single solid-state lattice defects (color centers). 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 by using the Coulomb blockade effect in a micro-pn junction with a quantum well as the active layer.[8,9] 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 had 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 a poor coupling efficiency to an external optical system.

A conceivable way of addressing these problems is to generate single photons by using excitonic emission from a single InAs/GaAs quantum dot excited by a pulse of light. The following experiments will be discussed in this paper: generating a stream of single photons from a single quantum dot,[10] using a DBR post microcavity to increase the

Single photons for quantum information systems. Yoshihisa YAMAMOTO. Quantum Entanglement Project, ICORP, JST, Stanford University (Stanford, CA 94305-4088 U.S.A.)
NTT Basic Research Laboratories

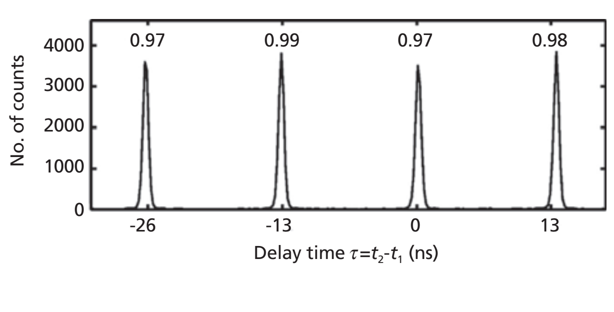

Fig. 1: Measurement results for a Poisson light source (pulse stream from a Ti:Al_2O_3 laser)

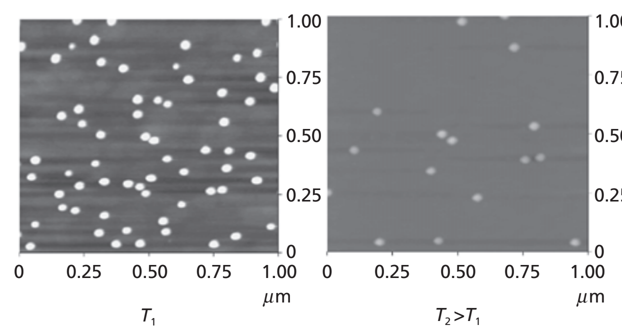

Fig. 2: AFM image of self-assembled InAs/GaAs quantum dots made by MBE deposition

efficiency of the external coupling efficiency,[11] generating a stream of single photons whose spectral width and pulse width are at the Fourier transform limit,[12] experiments in which single photons at this Fourier limit are regarded as indistinguishable single quantum particles (two-photon interference phenomenon),[13] and BB84 quantum key distribution experiments using single photons generated in this way.[14]

2. Producing single photons

2.1 Photon –photon correlation

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

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

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

Figure 1 shows the results of measurements on 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 the peaks including the peak at $t=0$ are equal in height, this shows that in the pulses from a Ti:sapphire laser, 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 have 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 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 source in thermal equilibrium. It originates from the stimulated emission of bosonic particles. 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. By using a combination of electron beam lithography and dry etching techniques to process this wafer into posts with a diameter of 0.2 μm, it is possible to optically excite

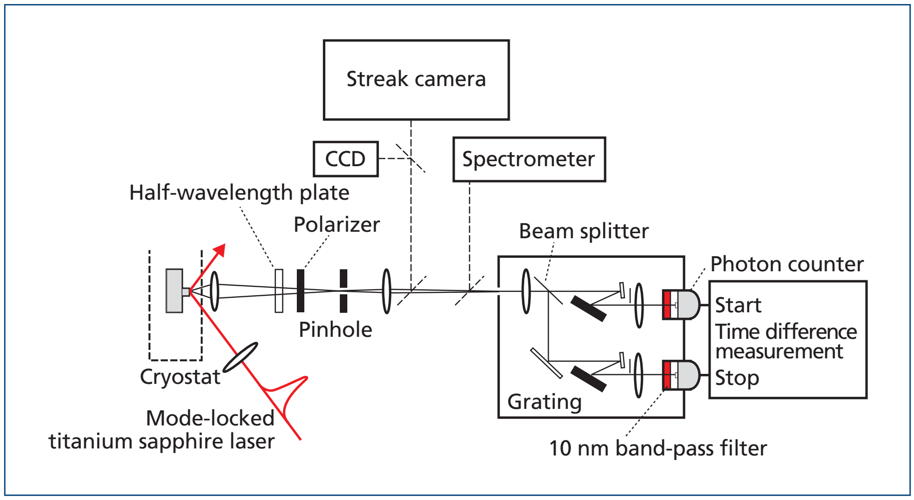

Fig. 3: Single quantum dot light emission measurement system

a single quantum dot in isolation. The experimental step is shown in Fig. 3. The temporal response to light emission 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 first quantum level (1 e-1 h) in the case where optical pumping is performed at a higher energy than the GaAs band gap. The emission patterns from different quantum dots have basically the same pattern except for relative shifts in wavelength. Emission 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 and have positive and negative charges.

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

Figure 4(c) shows that in the low pumping region the emission peaks 1 and 2 increase in proportion linearly and quadratically to the pumping intensity. The respective emission dependences on the pump power support the interpretation of exciton and biexciton emissions. These experimental results relate to CW pumping, and when the steady-state average number of excitons in the quantum dot exceeds 1, 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.[15] 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 can be well explained by selecting the

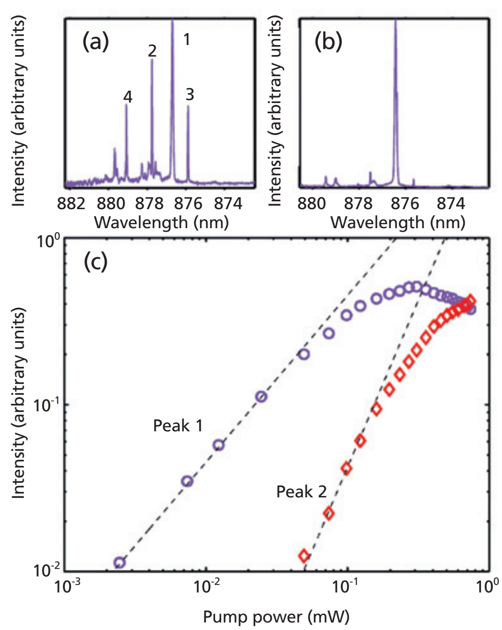

Fig. 4: (a) Emission spectrum from an InAs single quantum dot excited at energies higher than the GaAs band edge.
(b) Emission spectrum from an InAs single quantum dot when the second quantization level is resonantly excited.
(c) Variation of emission intensity with CW pump power for emission lines 1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

two parameters of the average number of excitons μ and the 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 3. Also, biexciton emission does not occur until the triexciton emission has finished and the number of excitons in the quantum dot has reached 2. The process leading up to the exciton emission is the same. Figure 5(c) shows the results of measurements with a streak camera indicating this state.

2.3 Post filtering

The last photon to be released from a quantum dot that initially has multiple excitons has a unique emission wavelength and is the only photon with this wavelength. By 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.[10] The strongly saturated characteristics show 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 of measuring $g^{(2)}(\tau)$ from a stream of single photons generated in this way.[10] 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 1 because the light emission from the quantum dot is superimposed on the on-off modulation (blinking effect). This results in a repeating pattern whereby the quantum dot emits light at the wavelength being measured at a certain time, after which the light emission at this wavelength stops, and then restarts again. This is thought to be caused by a shift in exciton emission wavelength resulting from the capture and release of carriers into and out from 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.[16-19]

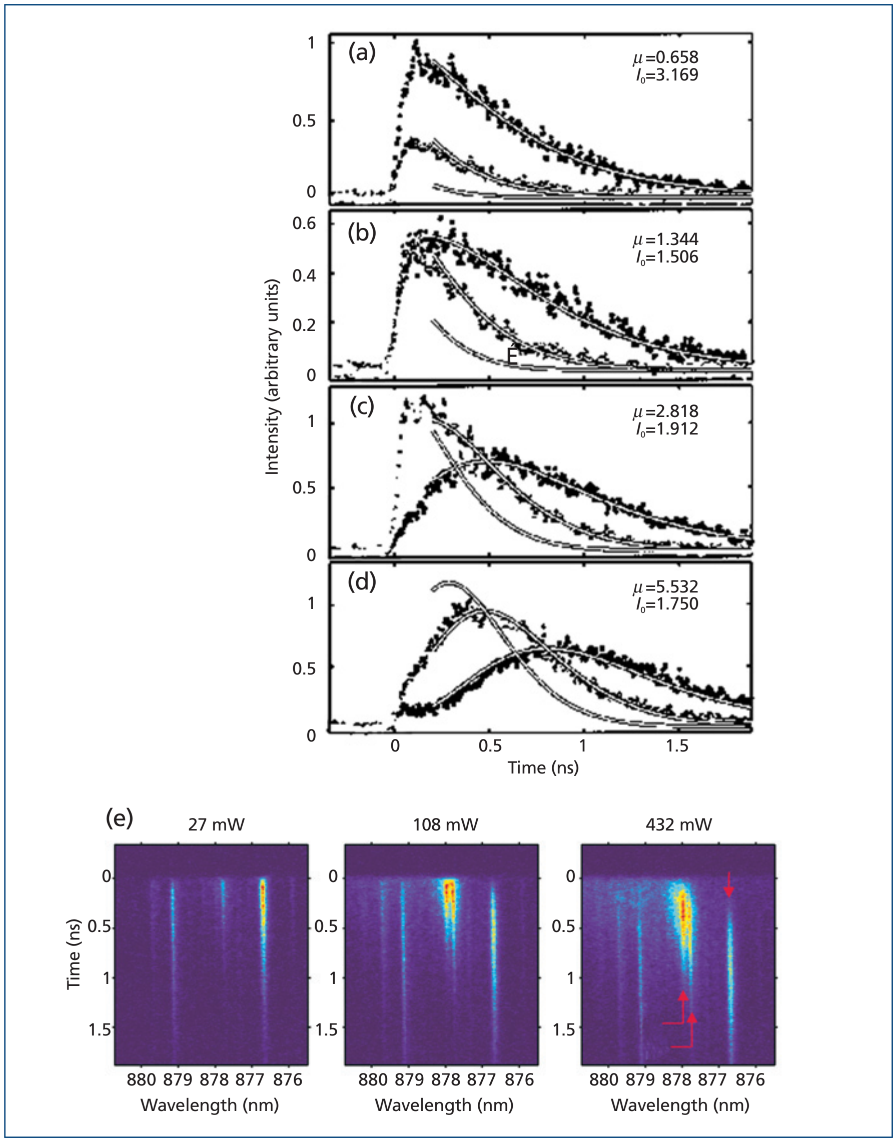

Fig. 5: Delay characteristics of exciton emission, biexciton emission and triexciton emission with pump pulse intensities of (a) 27 μW, (b) 54 μW, (c) 108 μW, and (d) 432 μW. Here, μ is the average number of excitons at time t=0, and I_0 is a parameter proportional to the detection efficiency. (e) Time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

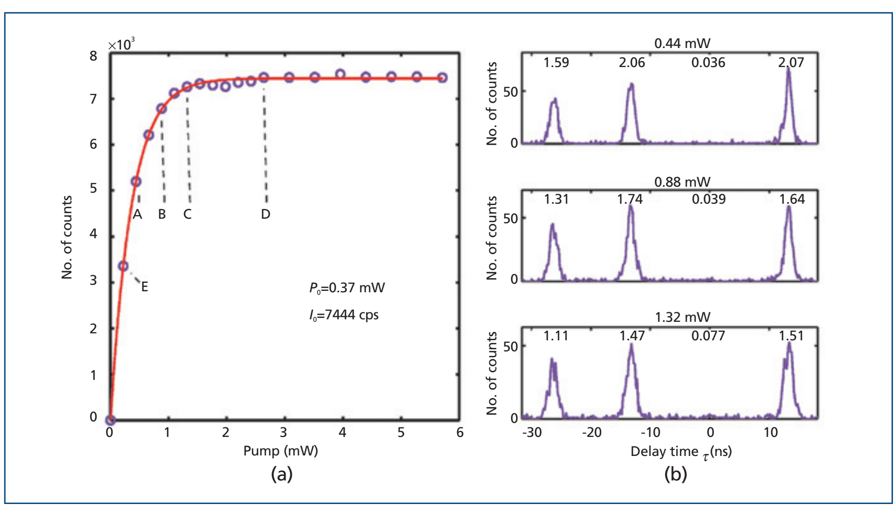

Fig. 6: (a) Exciton emission intensity vs. optical pump power. (b) Results of measuring $g^{(2)}(\tau)$ of exciton emissions from a single quantum dot at various different optical pump intensities.

3. Controlling spontaneous emission with a single-mode cavity

Figure 7(a) shows an SEM photograph of a three-dimensional microcavity produced by using electron beam lithography and ECR dry etching to process a DBR planar cavity made by MBE into a post shape. 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.[11] In a post system of this size, large numbers of InAs quantum dots having non-uniform spreading contribute to the emission spectrum. Since different transverse modes (HE_{11}, HE_{21}, ...) have different longitudinal wavenumber, they each have different resonant wavelengths. 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 the 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.[11] The fact that the emission lifetime is shortest at the resonant wavelength of the cavity is a unique characteristic of a three-dimensional cavity. In general, the spontaneous emission rate at the resonant wavelength of a three-dimensional cavity normalized by the 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 atom, and $\Delta\lambda_c/\lambda_c Q$ is the resonant 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 as follows:

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

To investigate the Q value of an ideally formed DBR micropost cavity, its behavior was studied by the first principle, i.e., using the finite difference time domain method.[20,21] A post with a diameter of 0.4 μm and a height of 5 μm was predicted to achieve a Q value of 10000, 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.[20] 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 DBR underneath is remained un-etched when the post was formed, resulting in increased diffraction losses of reflected light, and (ii) the shape of the post has a sharply tapering structure that causes transverse radiative losses.

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

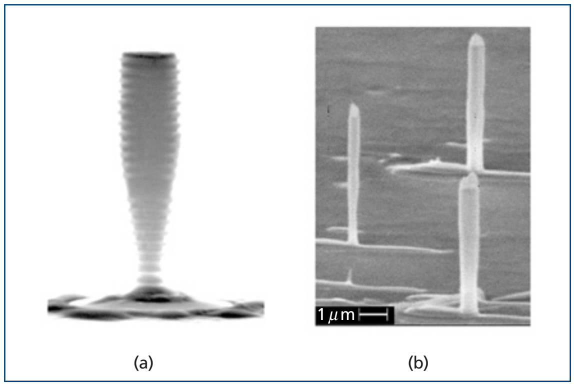

Fig. 7: GaAs/AlAs DBR micropost cavities enclosed in the center of InAs quantum dots produced by electron beam lithography and (a) Electron Cyclotron Resonance (ECR) dry etching, (b) Chemically Assisted Ion Beam Etching (CAIBE).

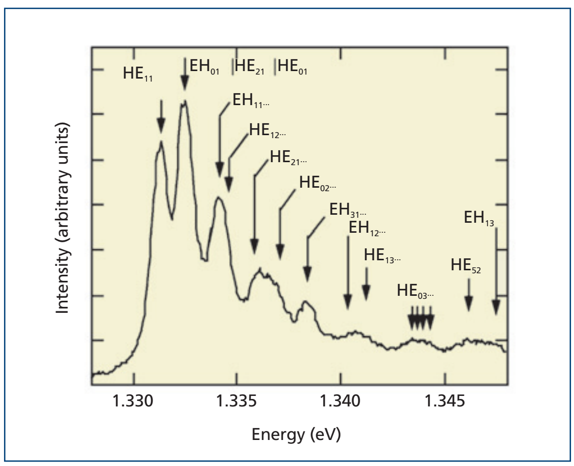

Fig. 8: Resonant modes of a microcavity with a post diameter of 6 μm

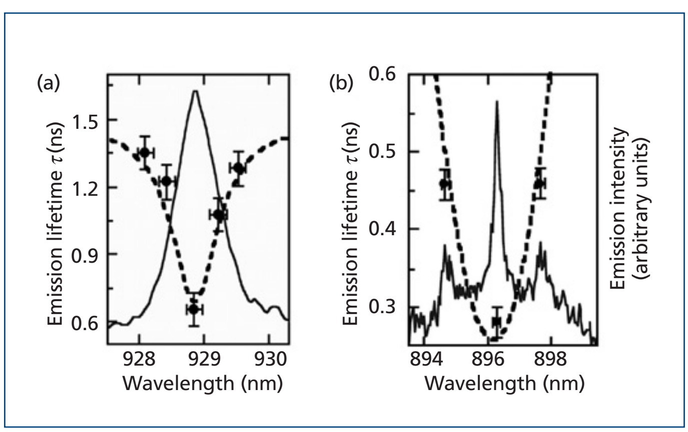

Fig. 9: Variation of emission intensity and spontaneous emission lifetime with emission wavelength for microcavities with post diameters of (a) 2 μm and (b) 0.5 μm.

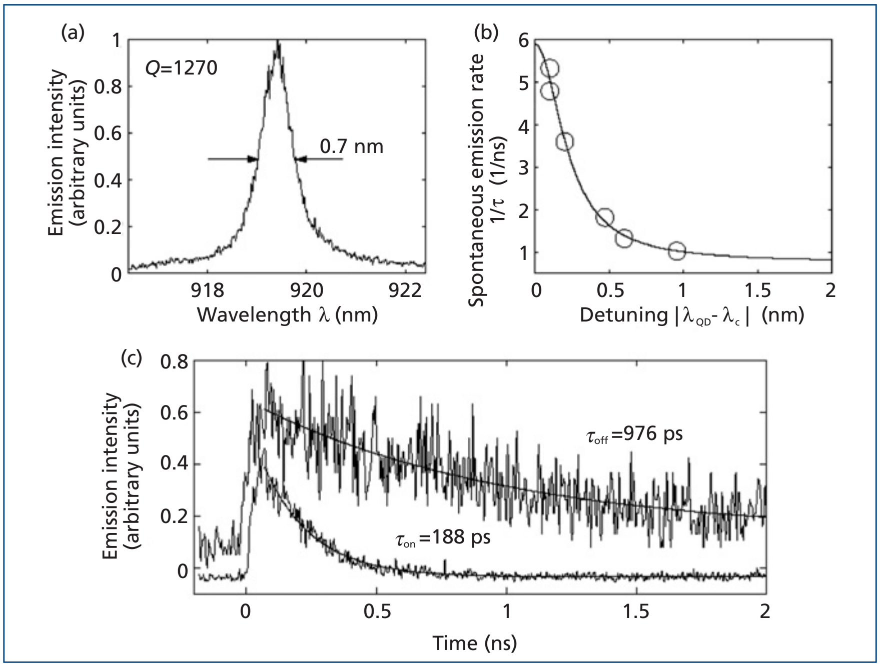

Fig. 10: (a) Characteristics of the fabricated DBR post microcavity. (b) Purcell factor vs. detuning. (c) Spontaneous emission processes when the exciton emission wavelength of the quantum dot matches the cavity resonant wavelength, and when it does not match the resonant wavelength.

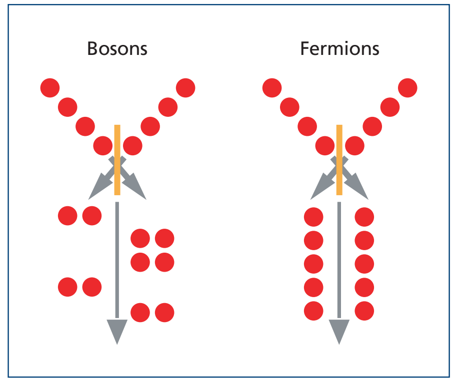

Fig. 11: Collision characteristics of indistinguishable identical quantum particles

maximum electric field, and as the exciton emission wavelength approaches the cavity resonant wavelength. A larger Purcell factor results in a greater reduction ratio of the exciton emission lifetime. Achieving a large Purcell factor γ/γ_0 and a spontaneous emission coefficient β close to 1 requires that the microcavity has a large Q and small V_0.

But 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 losses to increase and as a result the magnitude of Q is kept down to 300-800 or thereabouts. 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 losses, which was able to exhibit the following characteristics: Q=1300, 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%.[22]

4. Generating a single photon pulse 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 exciton polarization caused by phonon scattering is about 1 ns at a temperature of 4 K.[23] 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 natural width 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 have one 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, bosons both 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 exchanging term (the first and second terms respectively in the above equation) of symmetric and antisymmetric wave functions.[24] This quantum interference phenomenon is the source of the Pauli exclusion principle for fermions and phenomena exhibited by bosons such as stimulated emission (lasers), Bose 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 identification of EPR-Bell states and form the basis of quantum teleportation,[5] quantum repeaters,[6] and linear optical quantum computers.[7]

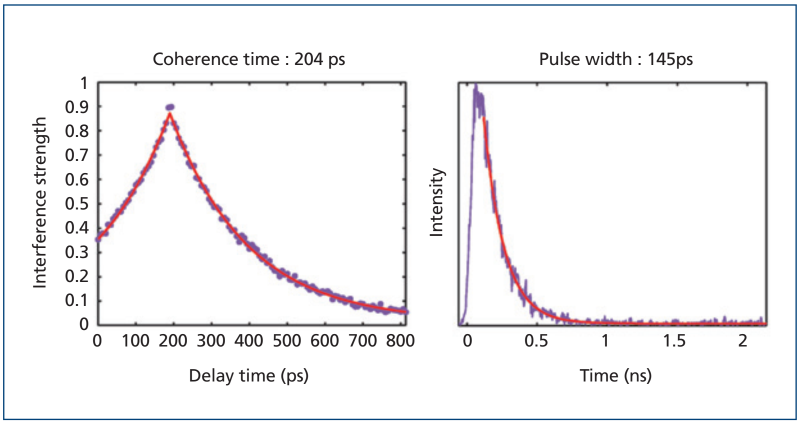

Fig. 12: Results of using a Michelson interferometer to measure the coherence time of a single photon pulse and a streak camera to measure the pulse duration.

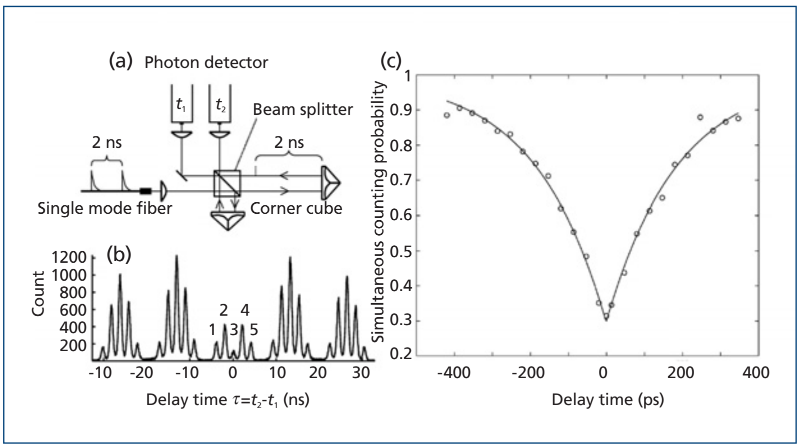

Fig. 13: Collision experiment involving two single photons generated with a 2 ns delay time difference. When the wave functions of the two single photons were overlapped at the output 50-50% beam splitter, the simultaneous counting probability was found to be lower due to two-photon interference.

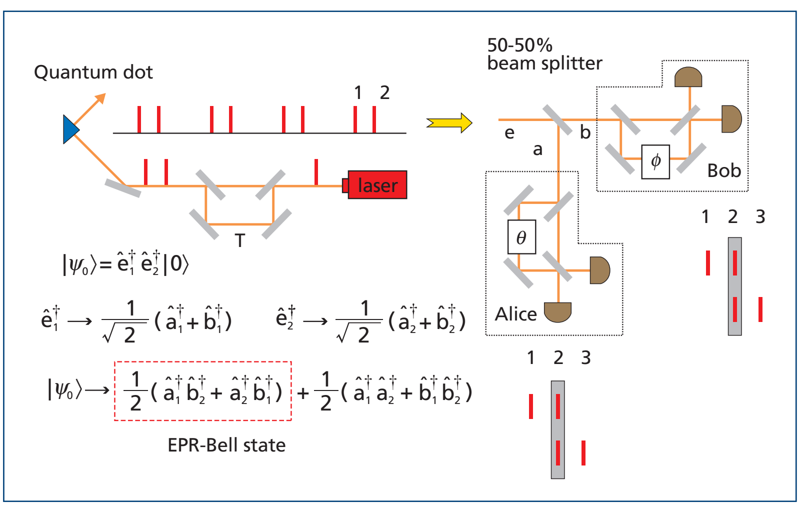

Fig. 14: An entanglement based quantum cryptography protocol using two single photons and a 50-50% beam splitter

4.2 Two-photon interference experiments

Figure 12 shows the results of 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 of using a streak camera to measure the pulse duration (amplitude decay time $2\tau_{rad}$: 290 ps).[13)] This only differs from the Fourier transform limit $2\tau_{rad}=t_c$ by a factor of 1.5.

Figure 13(a) shows the 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 $t=\tau$.[13)] Peaks 1 and 5 in the central cluster centered on $t=0$ correspond to the case where the first photon takes a short path and the next photon takes a long path. Peaks 2 and 4 correspond to the case where the two photons both take a short path or both take a long path. The central peak 3 corresponds to the case where the first photon takes a long path and the next 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 the simultaneous counting probability reaches a 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 computation 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.

4.3 Conversion into an entangled photon pair

Figure 14 shows that it is possible to implement an entanglement based quantum cryptography protocol using two such single-photon pulses at the Fourier transform limit.[25] In this protocol, the two indistinguishable single photons are simultaneously sent to Alice and Bob respectively by a 50-50% beam splitter. If Alice and Bob both detect the photons individually at time 2, then the first photon will have taken a long path and the next photon will have taken a short path before being detected by both parties. However, it is impossible to tell if Alice detected the first photon 1 ($|1,L\rangle_A$) and Bob detected the next photon 2 ($|2,S\rangle_B$), or vice versa. This situation is called a time-energy entangled state, and is expressed as follows:

$$|\Psi_{12}\rangle=\frac{1}{\sqrt{2}}[e^{i\theta}|1,L\rangle_A|2,S\rangle_B+e^{i\phi}|2,S\rangle_A|1,L\rangle_B]$$

where θ and ϕ are the random phase modulations introduced into Alice and Bob's delay lines (0 or $\pi/2$). When their two phases θ and ϕ are the same, there is a perfect correlation with respect to which detector detected the photon, and it is possible to make a secret key from this result. When their phases θ and ϕ are different, there is no correlation between their detector results, in which case the measurement results are discarded. When Alice and Bob's photon detection times are 1 on the one hand and 3 on the other, then the first photon will have taken a short path and the next photon will have taken a long path, in which case there will be a perfect correlation with respect to the times of detection, and a secret key can be derived from the result. This sort of quantum cryptography relies on the property that two single photons form indistinguishable identical quantum particles. A slightly different version of generating an entangled photon-pair from two indistinguishable single photons has been recently demonstrated.[26]

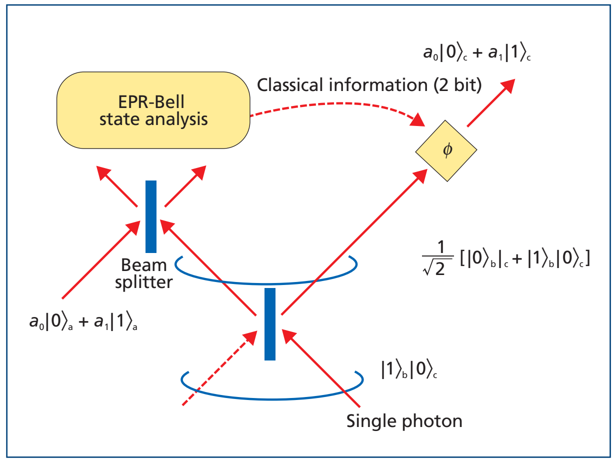

Fig. 15: Quantum teleportation using a single photon at the Fourier transform limit

Figure 15 shows an example of a configuration for quantum teleportation using a single photon pulse at the Fourier transform limit. The single photon pulse is converted into an EPR-Bell state by a 50-50% beam splitter.

$$|1\rangle_b|0\rangle_c\rightarrow\frac{1}{\sqrt{2}}[|0\rangle_b|1\rangle_c+|1\rangle_b|0\rangle_c]$$

Here, mode b is obtained by mixing arbitrary incident linear superimposed states $a_0|0\rangle_a+a_1|1\rangle_a$ with a separate 50-50% beam splitter, and the output is subjected to Bell state analysis. Mode c is controlled based on the results, and the initial state of mode a is reproduced in mode c.[27] At this time, two single photon pulses that are incident simultaneously in mode a and mode b must evidently be indistinguishable identical quantum particles. This quantum teleportation gate is a fundamental building block for linear optics quantum computation[7] and has been successfully demonstrated in a recent experiment.[28]

5. Quantum cryptography using single photons

Figure 16 shows a theoretical prediction of how the transmission speed of BB84 quantum cryptography using an ordinary semiconductor laser light source and a single photon

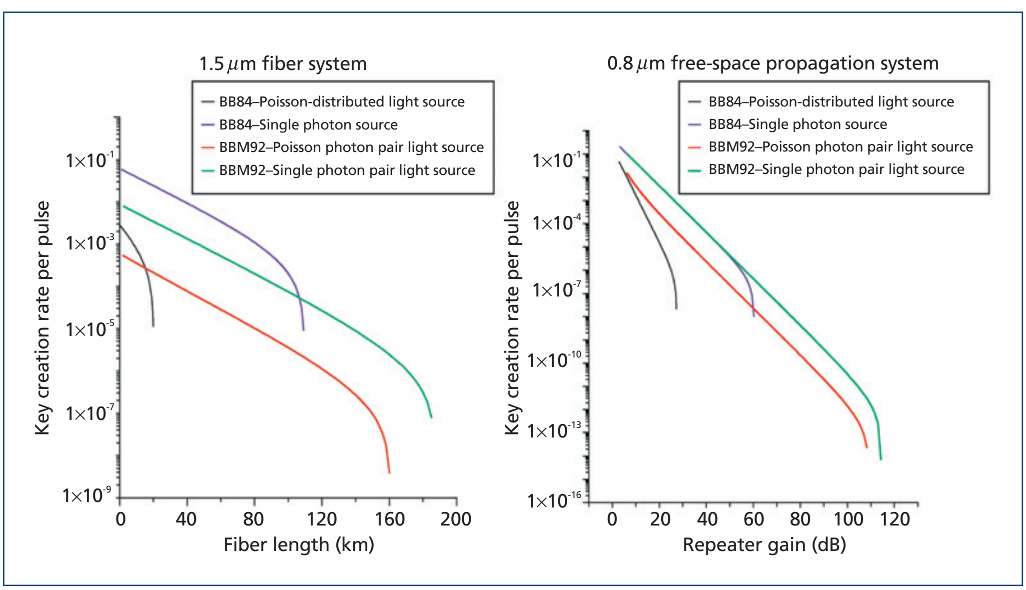

Fig. 16: A comparison of the performance of quantum cryptography using the BB84 and BBM92 protocols in the 1.5 μm and 0.8 μm bands. In BB84, the key creation rate per pulse and the repeater gain are substantially better when using a single photon source compared with an ordinary semiconductor laser. 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.

source (final key creation rate per pulse after error correction and privacy amplification) varies with fiber length (1.5 μm band) or repeater gain in the case of spatial propagation (0.8 μm band). When an ordinary semiconductor laser light source is used, there is a possibility of generating 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 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 for 2 or more photons per pulse is suppressed to 0, so the average number of photons sent out to the propagation path can be set to 1. This makes it possible to increase the repeater gain to 60 dB in a 0.8 μm band system or 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 where a single photon source emits two or more photons with a finite probability ($g^{(2)}(0)\neq0$) and where the external quantum efficiency is less than 1 (η<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.[29]

Figure 17(a) shows a BB84 quantum cryptography test system using the single photon source developed here.[14] This system generates single photons at a repetition frequency of 76 MHz using a mode-locked Ti:Al_2O_3 laser. Alice uses random variables 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 where they matched. Figure 17(b) shows a histogram of Alice and Bob's data.[14] 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 a level where it is ultimately negligible, classical privacy amplification is finally employed. Figure 17(c) shows how the repeater gain varies with the final key creation rate per transmitted pulse in this system. In the present system, since the average number of photons sent out to the transmission path per pulse is 3×10^{-3}, it is inferior to schemes using an ordinary semiconductor laser in the region of small repeater gain (propagation loss), but in the high repeater gain region the small value of $g^{(2)}(0)$ makes it advantageous to use a single photon source. In the future it is expected that the theoretically predicted repeater gain of 60 dB will be assured by reducing optical losses inside a transmitter.

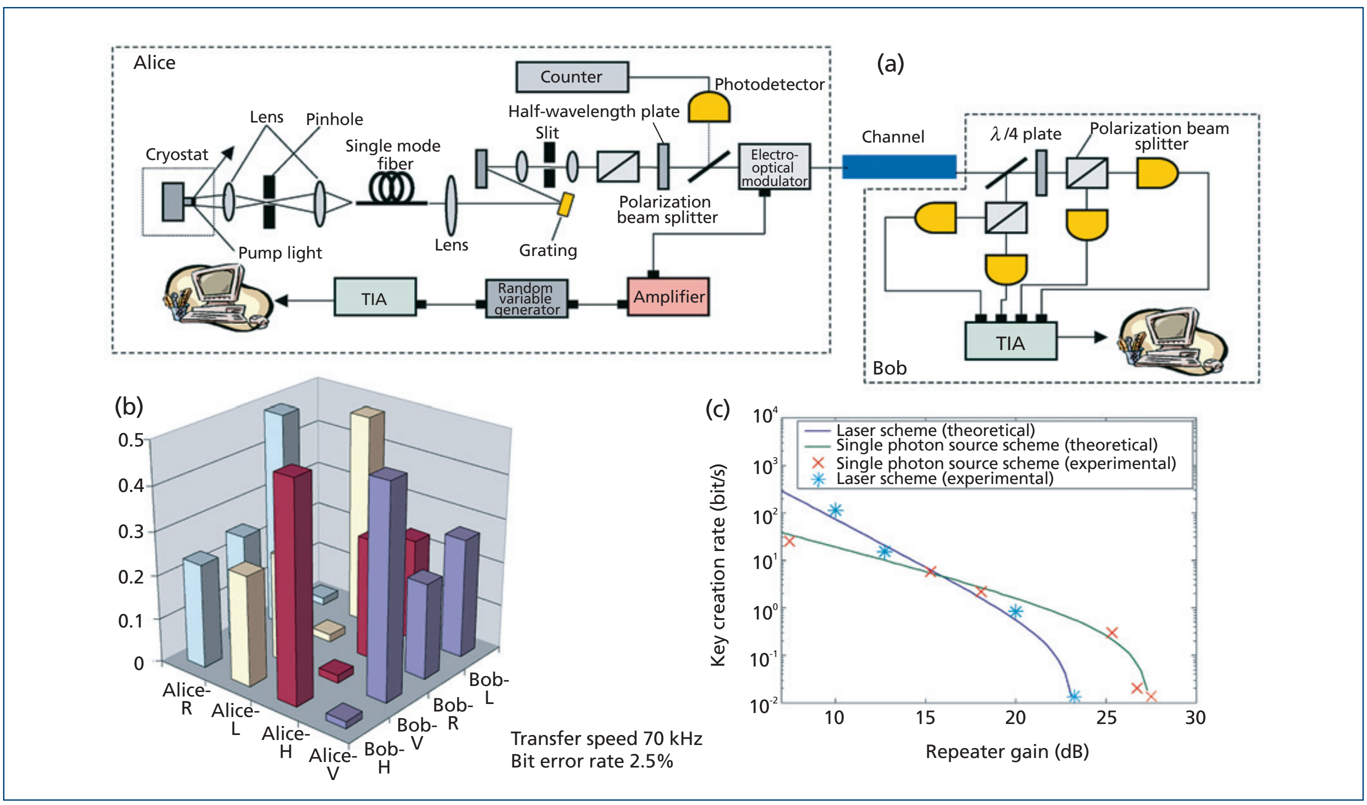

Fig. 17: An experimental BB84 quantum key distribution system using a single photon source, and the results obtained with this system

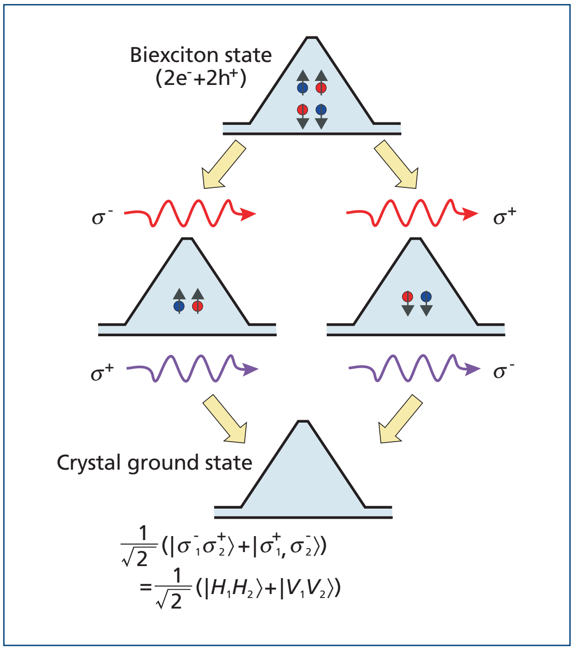

Fig. 18: An illustration showing how biexcitonic photons and excitonic photons from a single quantum dot are in a polarization entangled state

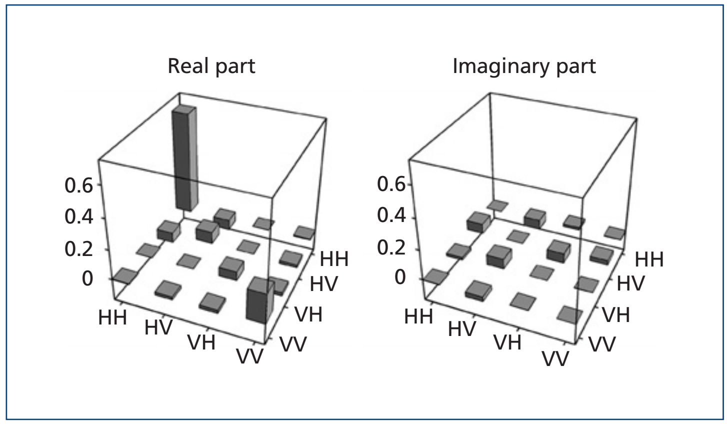

Fig. 19: Measurement results of a 4×4 matrix representing the polarization states of biexcitonic photons and excitonic photons from a quantum dot. The two photons form the mixed states $|H\rangle_1|H\rangle_2$ and $|V\rangle_1|V\rangle_2$.

6. Direct generation of EPR-Bell photon pairs

Figure 18 shows the two photon emission process when two electrons and two holes are confined at the ground state in a single InAs 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:[30)]

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

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

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

Figure 19 shows the results of experiments performed to confirm this fact.[31)] Measurements were made of all the elements in a 4×4 polarization matrix 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 expected 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. 20.[31)] When light emitted from the quantum dot is separated into H-polarized and V-polarized components which are input to a Michelson interferometer and the interference fringe is measured, they are each 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

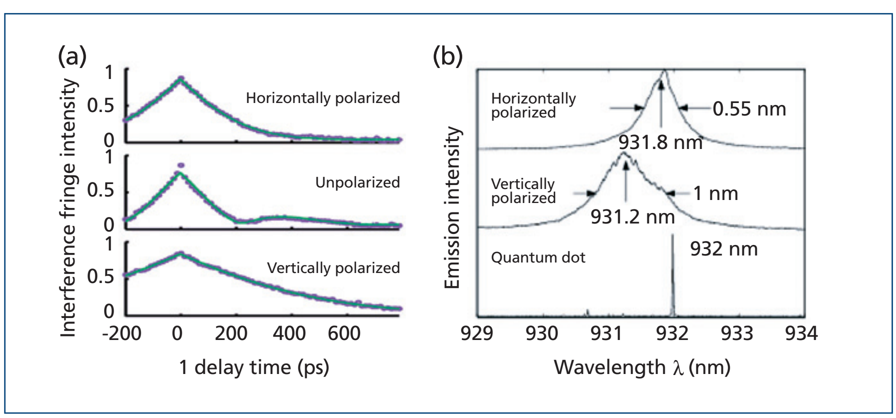

Fig. 20: (a) Variation of interference fringe intensity with delay time for H-polarized, V-polarized and unpolarized light. (b) Cavity resonance characteristics and quantum dot excitonic emission spectra for H-polarized and V-polarized waves.

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 200 ps as shown in Fig. 20(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 energy 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 be used to 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 that polarization entangled states can be generated directly.

7. Prospects

The generation of a regular single photon stream at the Fourier transform limit is a new development in quantum information processing using photonic qubits. This technique has been used in various quantum information systems, including the generation of entangled photon pairs, BBM92 quantum cryptography, quantum teleportation, quantum repeaters and linear optical quantum gates.

When considering the future quantum information technology, it will be necessary to encode information on the photonic qubits in quantum communication but store information on the nuclear spin qubits in quantum memory. Electron spins will no doubt play an important role as an interface between the two. It is hoped that a great deal of wisdom will be developed on how to connect these three qubit systems.

JSAP

References

1) C. H. Bennett and G. Brassard: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, p. 175 (IEEE, New York, 1984).
2) N. Lutkenhaus: Phys. Rev. A 61, 2304 (2000).
3) A. K. Ekert: Phys. Rev. Lett. 67, 661 (1991); C. H. Bennett, G. Brassard and N. D. Mermin: Phys. Rev. Lett. 68, 557 (1992).
4) E. Waks, A. Zeevi and Y. Yamamoto: Phys. Rev. A 65, 052310 (2002).
5) P. G. Kwiat, K. Mattle, H. Weinfurther and A. Zeilinger: Phys. Rev. Lett. 75, 4337 (1995).
6) L. Duan, M. Lukin, J. Cirac and P. Zoller: Nature 414, 413 (2001).
7) E. Knill, R. Laflamme and G. J. Milburn: Nature 409, 46 (2001).
8) A. Imamoglu and Y. Yamamoto: Phys. Rev. Lett. 72, 210 (1994); Y. Yamamoto: Nature 390, 17 (1997).
9) J. Kim, O. Benson, H. Kan and Y. Yamamoto: Nature 397, 500 (1999).
10) C. Santori, M. Pelton, G. S. Solomon, Y. Dale and Y. Yamamoto: Phys. Rev. Lett. 86, 1502 (2001).
11) G. S. Solomon, M. Pelton and Y. Yamamoto: Phys. Rev. Lett. 86, 3903 (2001).
12) D. Fattal, J. Vuckovic, C. Santori, G. S. Solomon and Y. Yamamoto: "Nearly Fourier-transform-limited single photons from a quantum dot microcavity", to be published.
13) C. Santori, D. Fattal, J. Vuckovic G. S. Solomon and Y. Yamamoto: Nature 419, 594 (2002).
14) E. Waks, K Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon and Y. Yamamoto: Nature 420, 762 (2002).
15) C. Santori, G. S. Solomon, M. Pelton and Y. Yamamoto: Phys. Rev. B 65, 073310 (2002).
16) P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, Lidong Zhang, E. Hu and A. Imamoglu: Science 290, 2282 (2000).
17) E. Moreau, I. Robert, J. M. Gerard, I. Abram, L. Manin and V. Thierry-Mieg: Appl. Phys. Lett. 79, 2865 (2001).
18) V. Zwiller, H. Blom, P. Jonsson, N. Panev, S. Jeppesen, T. Tsegaye, E. Goobar, M. Pistol, L. Samuelson and G. Bjork: Appl. Phys. Lett. 78, 2476 (2001).
19) 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: Science 295, 102 (2002).
20) J. Vuckovic, M. Pelton, A. Scherer and Y. Yamamoto: Phys. Rev. A 66, 023808 (2002).
21) M. Pelton, J. Vuckovic, G. S. Solomon, A. Scherer and Y. Yamamoto: IEEE J. Quantum Electron. 38, 170 (2002).
22) M. Pelton, C. Santori, J. Vuckovic, B. Zhang, G. S. Solomon, J. Plant and Y. Yamamoto: Phys. Rev. Lett. 89, 233602 (2002).
23) M. Bayer and A. Forchel: Phys. Rev. B 65, 041308 (2002).
24) H. Fearn and R. Loudon: J. Opt. Soc. Am. B6, 917 (1989).
25) K. Inoue, C. Santori, E. Waks and Y. Yamamoto: Phys. Rev. A 67, 062319 (2003).
26) D. Fattal, K. Inoue, J. Vuckovic, C. Santori, G. S. Solomon and Y. Yamamoto: Phys. Rev. Lett. 92, 037903 (2004).
27) D. Bouwmeester, A. Ekert and A. Zeilinger, eds.: The Physics of Quantum Information (Springer-Verlag, Berlin, 2000).
28) D. Fattal, E. Diamante, K. Inoue and Y. Yamamoto: Phys. Rev. Lett. 92, 037904 (2004).
29) E. Waks, C. Santori and Y. Yamamoto: Phys. Rev. A 66, 042315 (2002).
30) O. Benson, C. Santori, M. Pelton and Y. Yamamoto: Phys. Rev. Lett. 84, 2513 (2000).
31) C. Santori, D. Fattal, M. Pelton, G. S. Solomon and Y. Yamamoto: Phys. Rev. B 66, 045308 (2002).
32) K. Inoue, E. Waks and Y. Yamamoto: Phys. Rev. Lett. 89, 037902 (2002).

(Received September 18, 2002)

Yoshihisa Yamamoto

Received a 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 representative of the JST international joint research project. His current research interests include quantum optics, mesoscopic physics, semiconductor nanostructures, solid-state NMR spectroscopy and quantum information.