3 Quantum Info-Communications

3-1 Overview of Quantum Info-Communications and Research Activities in NICT

SASAKI Masahide

Present optical communication relies on the intensity control of light. By exploiting the wave nature of light, transmission with higher capacity and multi-functions must be possible. Its performance, however, will be bounded at the shot noise limit in the near future. In quantum info-communications, where one directly controls quantum states of photons, information security based on physical principle and ultra-high capacity beyond the shot noise limit could be realized. In this article, we present an overview of quantum info-communications, and review the research activities in NICT.

Keywords
Quantum communications, Quantum cryptography, Squeezed light, Quantum state, Photon-number resolving detector

1 Introduction

Present optical communications rely on intensity modulation and direct detection of laser light, while the wave nature of light is not exploited at all. It is believed that coherent optical communication, which utilizes the potential of light as a wave, may improve reception sensitivity by as much as 20 dB compared to the conventional direct detection method. In fact, the sensitivity of homodyne detection has already reached the limit of quantum fluctuation, or the “shot noise” limit. As the volume of transmission per unit power is increased, communication performance will ultimately be determined by this quantum fluctuation.

Quantum fluctuation arises from Heisenberg’s uncertainty principle and it is impossible to remove its effects completely. However, it is possible to suppress fluctuation within a certain phase range, although this will result in an increase in fluctuation for other phases.

This state, in which quantum fluctuation is artificially controlled, is referred to as the “squeezed state”[1]. Advanced data processing unrestricted by shot noise limits may be performed by processing the data using squeezed light to lock the signal phase at the phase point of suppressed fluctuation.

In the mid-1980s, methods were established to produce squeezed light, which contributed significantly to progress in quantum optics in the 1980s and 1990s[2]-[4]. Also at that time, a proposal was put forth on quantum key distribution[5][6], and a quantum computer was mathematically formulated[7]. By 1994, it was theoretically proven that quantum computers were able to quickly solve problems that required massive computations, such as prime factorization, and hence modern encryption could easily be broken by quantum computers[8]. This led to a widespread recognition of the significance of quantum information technology, and the merging of existing research areas caused explosive progress in the field.

One such area is quantum optical communication, representing an innovative attempt to integrate the most paradoxical aspects of quantum physics—such as data that simultaneously takes the values of 0 and 1, or quantum correlation phenomena that defy common intuition, resulting from the macroscopic manifestation of the quantum state—into info-communication technologies.

2 Principles of quantum physics and overview of quantum info-communications

There are two basic principles at play in quantum physics. One is the superposition principle, which when applied to info-communication technologies is the basis for the concept of the Qubit, which is a unit of quantum information that may take the values of 0, 1, or a superposition of both. By elaborating on this concept, it is possible to perform ultra-parallel computation of multiple possibilities. This is quantum computation, and it entails the possibility of breaking the security of modern information systems in the near future.

However, the second principle luckily allows us to overcome this crisis. Heisenberg's uncertainty principle, which states that it is impossible to measure the precise state of two canonically conjugate physical quantities (for example, the position and momentum of a particle) simultaneously without the introduction of an external disturbance. By elaborating on this principle, it is possible to perform complete detection of eavesdroppers and to develop quantum cryptography that offers unconditional security, which cannot be broken even by quantum computers.

On the other hand, the uncertainty principle, which states that there are fundamental limitations to measurement, will also ultimately place a limit on the communication capacity. It has been clarified that a new coding technology based on quantum computation, quantum coding, will be essential in order to bring communication capacity to the ultimate quantum limit. Studies on quantum info-communications consists of two main branches, based on the superposition and uncertainty principles: studies aimed at achieving large capacity and studies aimed at establishing unconditional security (See Fig. 1). It would appear that practical applications of quantum cryptography are just around the corner, while quantum computation and quantum coding are still long-term themes for the future.

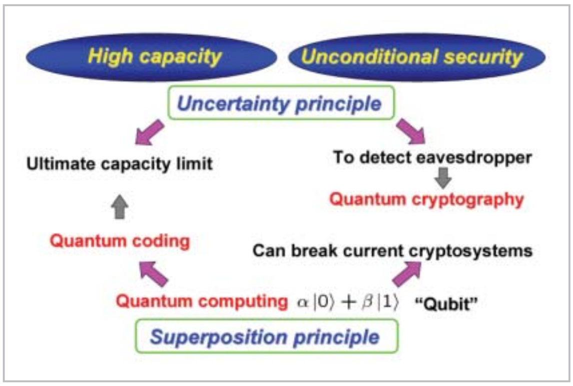

Fig. 1 *The principles of quantum physics and overview of quantum info-communications*

3 R&D project on quantum info-communication

In order to pursue these themes strategically and comprehensively, a collaborative project between industry, academia, and government has been launched for research and development on quantum info-communications by the Ministry of Internal Affairs and Communications (MIC) in 2001. The organizational structure for this project is summarized in Fig. 2.

Under the project promotion board headed by Dr. Ezaki, there are three main pillars. One is the NICT intramural research team, which is charged with pursuing principle demonstrations & developing quantum info-communica-

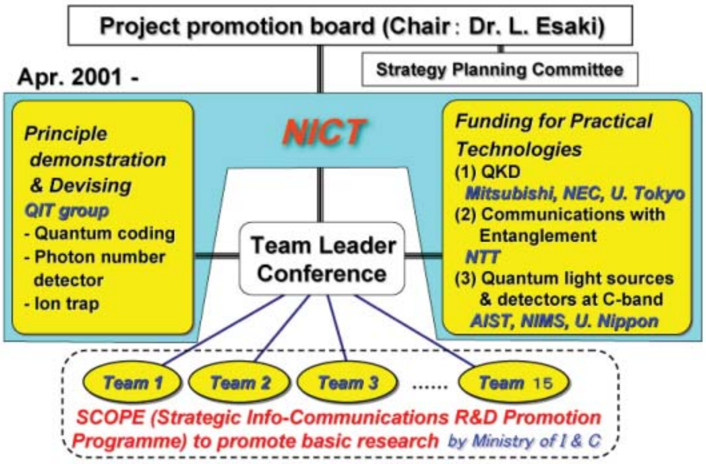
Project promotion board (Chair : Dr. L. Esaki)
Strategy Planning Committee
Apr. 2001 -
NICT
Principle demonstration & Devising
QIT group
- Quantum coding
- Photon number detector
- Ion trap
Team Leader Conference
Funding for Practical Technologies
(1) QKD
Mitsubishi, NEC, U. Tokyo
(2) Communications with Entanglement
NTT
(3) Quantum light sources & detectors at C-band
AIST, NIMS, U. Nippon
Team 1
Team 2
Team 3
......
Team 15
SCOPE (Strategic Info-Communications R&D Promotion Programme) to promote basic research
by Ministry of I & C

Fig.2 Organization for the promotion of the R&D Project for Quantum Info-Communications Technologies

tions. The second is NICT extramural activity, funding for themes which have almost reached the application stage, such as quantum cryptographic systems and related basic technologies. The third is the Strategic Information and Communications R&D Promotion Program of MIC (SCOPE), which promotes basic research. In total, 15 teams are funded directly by MIC.

The main members of all participating research teams hold team leader conferences once or twice annually to report on their results, introduce and analyze the latest findings, and discuss future strategies. These conferences have formed the basis for the national strategic management of R&D carried out in close collaboration with researchers at NICT and other academic and industrial organizations and the policymakers at MIC.

4 Present State of Research and Development

Of the two basic principles discussed—the superposition principle and the uncertainty principle—the latter can be more readily used in technical applications. Furthermore, quantum cryptography, a technology enabled by controlling 1-Qubit level quantum effects (represented by the BB84 protocol), is nearly ready for practical application.

(1) Quantum cryptography

Currently, the main security measure provided over the Internet is a method called the public key cryptosystem. And the quantum cryptography now proven to provide unconditional security is based on a more primitive secret key cryptosystem. A secret key is a random-bit stream shared only by the sender and the receiver. This key is used to encrypt a message, and interception may be completely prevented by limiting the key to one-time use (a “one-time pad”). Quantum key distribution is a method of safely sharing this secret key. In practice, a safe key is extracted from single photon events detected on the receiver side. To ensure security, a high-quality single photon source is recommended; however, for the time being, a Poisson source, such as an attenuated laser light, will suffice, since system performance is more dependent on the performance of the photon detector. Fortunately, a commercial avalanche photo-diode (APD) detector may be used for this purpose, and field tests and commercialization of the system have already begun.

Through NICT extramural research, a long distance field trial over 96 km using the NICT fiber network of JGN-Ⅱ has been successfully performed. A long-term field trial using aerially installed commercial fiber over 16 km was also able to be carried out, in which secret keys were continuously generated at 13 kbps for two weeks with no manual adjustment(See **3-2**, Hasegawa et al., this issue).

(2) Quantum entanglement

In contrast to the uncertainty principle, for which actual technical applications have begun, studies on the application of the superposition principle are only in the initial stages. The superposed quantum state breaks down easily in the ordinary world, rendering it difficult to control. Furthermore, the superposed state formed by multiple beams of light spread macroscopically displays a unique quantum correlation in which the quantum state of the beam is affected by the measurement results of the other beams. This state is called the “entangled state”, and one of the major R&D themes in quantum info-communications involves the generation and control of this state. In particular, the technology for generating an entangled photon pair in the optical fiber band stands as an important elementary technology in realizing advanced quantum communications within the existing communication infrastructure, including quantum key distribution, quantum teleportation, quantum secret key sharing, and other applications. In the course of NICT extramural research, we have developed an entangled photon-pair generation technology using four-wave mixing in an optical fiber and were able to obtain a fairly good two-photon interference waveform with visibility of 99.3%. Further, we succeeded in achieving $S = 2.65 \pm 0.09 > 2$ for the violation of Bell’s inequality, which is proof of quantum correlation, even at a distance of 20 km (See **3-3**, Takesue, this issue).

(3) Quantum teleportation

Quantum teleportation is a new, seemingly magical info-communication method that makes use of the entangled state. This will be important in the following context. The complex state of superposition is stored in the memory of quantum computers, and is to be transferred over a network connecting quantum computers. If the quantum state to be sent is known, it may be encoded and sent as classical bit information. However, the state of superposition is disrupted by measurement, and so the classical method cannot be used. Quantum teleportation is a method of transmitting the state of superposition[9][10].

Additionally, it has been found that quantum computation may be realized through the direct use of quantum teleportation. Quantum coding, aimed at enabling high capacity communications, requires optical quantum computations, and quantum teleportation is a perfect constituent element for this technology.

(4) Quantum computation

Functions that lack classical counterparts, such as prime factorization by polynomial time, require large-scale quantum computation exceeding several hundred quantum bits. However, even small-scale quantum computation may contribute significantly to enhancing the comprehensive performance of communication systems when combined with existing communication and measurement technologies. In this case, quantum computation using light merits close consideration. In general, interactions between photons are extremely weak, and it is difficult to construct a basic gate. However, it has been revealed that small-scale quantum computation may be realized by modifying existing technologies using a photon-number resolving detector and non-classical light in single-photon states or in the squeezed state.

The main signal is combined with an auxiliary non-classical light to create an entangled state. Then, only a part of the entangled state is measured with a photon detector. The remaining light undergoes changes according to the results of measurement. A quantum gate for the signal may be effectively achieved by allowing signal processing to proceed only when the measurement results correspond to the desired non-linear transformation. Although such a correspondence is a random occurrence, in principle, the probability of success for the quantum computation can be effectively raised to 100% by repeating the processing at each gate in advance offline until correspondence is achieved, and then by placing the correspondence online where the signal is located, by quantum teleportation[11]-[13].

(5) Quantum coding

The key to achieving high capacity communications lies in the receiving technology. Based on the latest results of quantum information theory, a method for optimizing communication through a linear-loss channel under the power and bandwidth constraints is as follows[14]. First, the optimal solution on the transmission side for maximizing the channel capacity is to encode a message using a pulse stream created by modulation of the amplitude of normal laser light by a continuous variable that follows a Gaussian distribution. On the transmission side, the generation of quantum entanglement among pulses will have no effect in terms of increasing the channel capacity. However, on the receiving side, this capacity can be increased by performing the most advanced decoding operation allowed by quantum physics on the pulse stream of the incoming coherent light. Thus, quantum control is required on the receiving side.

The ultimate decoding operation is one in which the optical quantum computation is incorporated, and this is the essence of quantum coding. In other words, instead of performing opto-electric conversion by measuring each pulse independently, a quantum computation is first performed on the entire block of the received pulse stream to create an appropriate state of superposition, and then each pulse is measured. In this way, it is possible to increase the net volume of information that may be retrieved from the received signal. This method is referred to as quantum-collective measurement. Figure 3 is a symbolic presentation of the effects of this method. When transmitting signals containing quantum noise (in the nonorthogonal quantum state), it is possible to retrieve more than twice as much information by quantum-collective measurement when the communication resources are doubled. This is referred to as super-additive quantum coding gain. In conventional decoding, the increase of information is twice at most and never more than that. Although the basic principle of the super-additive quantum coding gain has recently been verified[15], this verification used a model with polarization of the quasi-single-photon state and some degree of freedom of paths, and so the method is far from practical application. The production of a practical application scheme for the method thus remains as a theme for future studies.

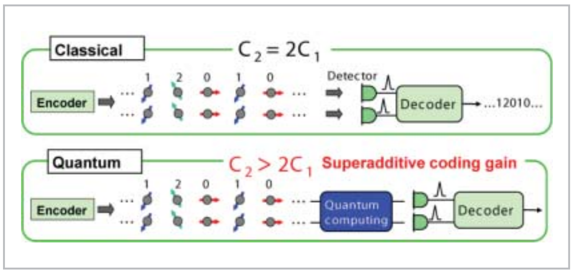

Fig.3 Comparison between quantum-collective measurement for two pulses (bottom) and classical decoding method (top)

By incorporating quantum-collective measurement into classical decoding circuits, it is possible to reduce dramatically the amount of calculation required for decoding and to effectively improve transmission capacity[16]. In long-haul communications, extremely long codes are used to ensure the precision of transmission, resulting in more time and labor required for decoding as well as increased instrumentation costs. A hybrid quantum-classical coding system with quantum-collective measurement will reduce these decoding costs, and the effective transmission rate may be steadily increased by increasing the scale of quantum-collective measurement. Furthermore, when the scale of quantum-collective measurement becomes sufficiently large, it will be possible to achieve the maximum channel capacity. This approach is believed to be the most natural path in the evolution from present optical communication systems to a quantum communication system.

5 Strategic issues for the future

(1) Quantum cryptography

Research and development on quantum

cryptography has reached its final stage in moving toward practical application. The strategic goals of NICT extramural research in the future will be to develop a quantum key distribution system that may be applied to metropolitan IP networks within the 50-km range and to construct a world-class testbed for mid-to-long range communication exceeding 100 km by the year 2010.

In order to ensure security in actual applications, a metro-network-compatible quantum key distribution system should have a minimum key generation speed of 1 Mbps to accommodate telephone and fax transmissions. Another goal is to establish the technologies required for free connection switching between eight or so nodes and the establishment of an optimal bypass, using the existing wavelength multiplexing function together with switching functions. At the same time, we plan to develop compact and mobile models of the relevant instruments using optical integrated circuits.

The goals for the mid-to-long-range quantum key distribution testbed are to realize a key generation speed of 10 kbps or higher and to achieve world-class performance in the trade-off curve between key generation rate and transmission distance.

(2) Photon detector

The key to achieving the above goals is the establishment of a high-performance single-photon detection technology. The afterpulse phenomenon of the APD imposes restrictions on the key generation speed, and the dark count results in weakened security and limits the distance of key distribution. Thus, it may be said that the suppression of these effects and the enhancement of the effective photon detection rate form the fundamental strategy for improving the performance of a quantum key distribution system.

A single-photon detection technology with an effective photon detection rate of up to 10 MHz is required for the realization of a 1-Mbps-class metro-network-compatible quantum key distribution system. The candidates for such a detection system may largely be categorized into three groups—the compound semiconductor APD, a combination of wavelength conversion in the telecom-band to the near-infrared band and the Si APD, and superconducting devices.

The ultimate system may be constructed if fundamental improvements can be made using the compound semiconductor APD, which allows direct detection in the telecom-band and also lends itself to integration and mass production. However, basic and challenging issues remain, such as high-quality crystal growth.

In existing technologies, by using a combination of wavelength conversion and Si APD, outstanding system performance has been realized, with operational speed slightly below 10 MHz and final detection efficiently slightly below 50%, and expectations are high for the realization of a mid-to-long-range quantum key distribution testbed using this method. However, the band limitations of the wavelength conversion elements may carry over and produce limiting factors in the future with the incorporation of wavelength multiplexing.

The superconducting device—with its low-noise, high-speed characteristics—is the most promising candidate from the perspective of high performance; however, due to the requirement of a low-noise environment and a wide range in wavelength sensitivity, the progress of future R&D in background-light-shielding measures may become the controlling factor with this method. Development of the above methods will thus be pursued simultaneously before a final selection is made.

(3) Quantum repeater

The signal set used in quantum cryptography is designed such that it is impossible to create a copy of the signal without destroying its quantum state. Such a signal set cannot be amplified, and thus will be susceptible to attenuation. In actual optical fiber networks, there are limits to the distance over which an encrypted key may be directly distributed, which at present is thought to be around 200 km.

Advanced technologies such as quantum

repeater are necessary for creating quantum cryptography networks exceeding this distance. The underlying principle for quantum repeater is quantum teleportation, in which signals are reconstructed at remote locations without destroying the quantum state. In quantum teleportation, entangled states are shared at two points, A and B, located at a distance closer than the attenuation limit. Points B and C will also share entanglement states. By performing a special type of measurement at intermediate point B, it is possible to create an entangled state stretching from points A to C. This maneuver is called entanglement swapping, and the entangled state generated may be used to relay the state of the photon from point A to a remote point C.

In practice, the entangled state is also extremely susceptible to attenuation and relaxation; thus, numerous pairs of entangled states must be generated and shared, and a highly pure pair must be distilled from the numerous, deteriorated pairs. To control the timing of this process, a quantum memory—capable of keeping the quantum state stable for a certain period of time—is required.

In order to establish the basic technologies for this method, collaborative R&D efforts are underway in industry, academia, and government based on NICT extramural research; these efforts are to involve demonstrations on physical models of quantum memory and validation experiments on the simplest systems of quantum repeaters by the year 2010.

(4) Universal photonic gate

Currently, it is predicted that optical communications will reach a limit in transmission rate at around 10^{18} bits (exabits) per second due to shot noise limits, regardless of the extent to which wavelength multiplexing and multi-value modulation are employed. To overcome the exabit/second wall, serious consideration must be given to the use of quantum coding. The key to success in this area is quantum computation on the receiving side, using a signal in a coherent state.

In the coherent state, photons are in a state of Bose-Einstein condensation, and the minimum uncertainty state of the quantum fluctuation may be retained even when subjected to attenuation. Thus, the coherent state is most suited for transmission. In the ultimate communication system, such macroscopic Gaussian states must be processed under the superposition principle to extract the maximum amount of information per photon. This requires far more sophisticated technologies relative to quantum cryptography, which can be performed by quantum control on the 1-Qubit level, and highly non-linear effects must be realized at the level of the photon.

Presently, the basic elements required for such systems have been theoretically identified. It is known that if the cubic phase gate can be implemented and combined with existing technologies (to be more precise, a Gaussian operation consisting of linear optical elements, second order non-linear elements, and homodyne detectors), in principle it will be possible to create an arbitrary non-linear optical effect. In other words, an arbitrary photonic quantum circuit may be constructed and a universal photonic gate set may be obtained as a result[12][13]. This cubic phase gate can be produced by the optical circuit presented in Fig. 4. By incorporating this phase gate into existing optical communication systems, it will be possible to exceed the shot noise limit.

The most important feature of this circuit is the entangled state produced by interference of two squeezed light beams and a high-precision photon-number resolving detector. These two elementary technologies may be used not only in the cubic phase gate but also in a wide range of applications. In the figure, the component for modulating the entangled state, shown in the top row has already been developed and is ready for application in precise measurements exceeding the shot noise limit[14]. In contrast, the development of a photon-number resolving detector has not yet reached a satisfactory level, and further development is required. NICT is currently carrying out research on a photon-number resolving detector that combines a low-noise semiconductor photodetector with a high-gain, low-noise integrated readout circuit (called the CIPD). The device features top-class performance worldwide in terms of sensitivity and noise characteristics at the telecom-band. (See[18]-[20] and **3-4**, Fujiwara et al., this issue.)

The theoretical backbone in circuit design and performance evaluation of systems combining entangled states with photon-number resolving detectors and exceeding conventional shot noise limits has yet to be established, and NICT is also devoting efforts to this area of investigation. The latest results are reported by Kitagawa and Takeoka (**3-5**, this issue).

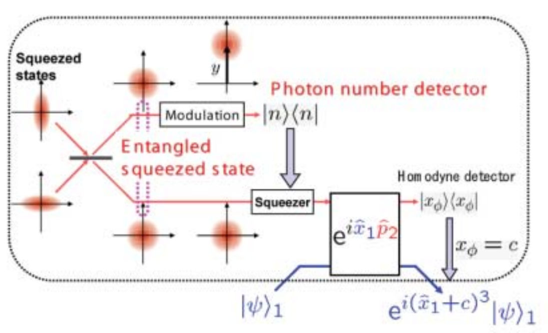

Fig.4 *Architecture of the cubic phase gate circuit*

(5) Quantum network

Advances in technologies for quantum computation, quantum teleportation, and quantum repeater should allow for the construction of a purely quantum network, or a quantum LAN and a quantum web. On such a network, it will be possible to perform quantum distributed processing using linked small-scale quantum computers, secret key consignment using the entangled state, and quantum certification for online voting and payment while ensuring the protection of personal information. The basic technologies required to realize such a system are reported by Hayasaka in this issue (**3-6**).

6 Conclusions

As demands increase for greater capacities of communications and ensured security over networks, miniaturization of electronic devices and high-density packing of optical signals have advanced significantly. We have entered an age in which info-communication devices can process signals at the levels of the photon and electron. With such progress, the theoretical limits to increasing integration and density of units are beginning to be felt. It is thus inevitable that info-communication technologies will enter the realm of quantum physics, which holds the ultimate laws of physics. Quantum info-communications provide us with far more possibilities for the future than offered by existing systems, and will no doubt guide the direction of future info-communication technologies. After communication using light waves has reached its physical limits, quantum info-communication technologies will be our only tool for breaking down the barrier of the petabit/second transmission rate and establishing a firm and secure foundation for communications in a world of exabit and zettabit/second transmissions.

Some areas such as quantum cryptography have already entered the stage of practical application. However, on the whole, studies on quantum info-communication technologies are still in the initial basic science research phase. New phenomena may yet be discovered during the development of the necessary elementary technologies for quantum info-communication. If the significance of the basic-science aspect of the field is given proper attention in the context of strategic R&D efforts toward practical application of quantum info-communication technologies, we may expect to see the propagation of the results in a variety of new studies in a range of fields.

References

1 H. P. Yuen, Phys. Rev. A13, 2226, 1976.

2 M. Matsuoka, “Quantum optics”, University of Tokyo publisher, 1996.(in Japanese).

3 Y. Yamamoto and K. Watanabe, “Foundation of quantum optics”, Baifukan,1994.(in Japanese)

4 D. F. Walls and G. J. Milburn, “Quantum optics”, Shpringer-Verlak, 2000.(in Japanese)

5 S. Wiesner, SIGACT News 15, 78, 1983.

6 C. H. Bennett and G. Brassard, Proc. of IEEE Intern. Conf. on Computers, Systems, and Signal Processing, Bangalore, India IEEE, New York, pp. 175–179, 1984.

7 D. Deutsch, Proc. R. Soc. Lond. A 400, 97, 1985.

8 P. Shor, Proc. of 35th Annual Symp. on the theory of Computer Science, p124, 1994.

9 A. Fususawa, Frontier of modern physics 5, Kyouritsu, 2001.(in Japanese)

10 S. Taleuchi, Optics 33, 284, 2004.(in Japanese)

11 K. Knill, et al., Nature 409, 46, 2001.

12 D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A64, 012310, 2001.

13 S. D. Bartlett and B. C. Sanders, Phys. Rev. A65, 042304, 2002.

14 V. Giovannetti, et al., Phys. Rev. Lett. 92, 027902, 2004.

15 M. Fujiwara, et al., Phys. Rev. Lett., 90, 167906, 2003.

16 M. Takeoka, et al., Phys. Rev. A 69, 052329, 2004.

17 J. Mizuno, et al., Phys. Rev. A 71, 012304, 2005.

18 M. Akiba, M. Fujiwara, and M. Sasaki, Opt. Lett. 30, 123, 2005.

19 M. Fujiwara and M. Sasaki, Appl. Phys. Lett. 86, 111119, 2005.

20 M. Fujiwara and M. Sasaki, Optics Lett., 31, 1, 2006.

***SASAKI Masahide**, Ph.D.*

Research Manager, Advanced Communications Technology Group, New Generation Network Research Center (former: Group Leader, Quantum Information Technology Group, Basic and Advanced Research Department)

Quantum Info-Communications