## **External Awards**

Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology, The Young Scientist's Prize

Winner: Yoshitaka Taniyasu, NTT Basic Research Laboratories

Date: Apr. 23, 2011

Organization: The Ministry of Education, Culture, Sports, Science

& Technology in Japan

For "Research on Crystal Growth of Aluminum Nitride and Its Application to Deep Ultraviolet Light-emitting Device".

Dr. Taniyasu has grown n-type and p-type aluminum nitride (AlN) layers for the first time to apply them to semiconductor devices. Using these layers, he has successfully demonstrated an AlN p-n junction light-emitting diode with a wavelength of 210 nm, the shortest ever reported for semiconductor solid-state light sources.

#### The Institute of Physics (IOP) Fellow

Winner: Hiroshi Yamaguchi, NTT Basic Research Laboratories

Date: May 18, 2011

Organization: Institute of Physics

For personal contribution to the advancement of physics as a discipline and a profession.

The Council of the Institute is concerned to ensure that the Fellowship of the Institute includes all those who have made an important contribution to physics, to the profession of physicist, or as physicists in their chosen career.

#### **Best Paper Award**

Winners: Ryogo Kubo\*1, Jun-ichi Kani\*2, Yukihiro Fujimoto\*2,

Naoto Yoshimoto\*2, and Kiyomi Kumozaki\*3

\*1 Keio University

\*2 NTT Access Network Service Systems Laboratories

\*3 Mitsubishi Electric Corporation

Date: May 19, 2011

**Organization:** Institute of Physics

For "Adaptive Power Saving Mechanism for 10 Gigabit Class PON Systems".

This paper proposes a power saving mechanism with a variable sleep period to reduce the power consumed by optical network units (ONUs) in passive optical network (PON) systems. In the PON systems based on time division multiplexing (TDM), sleep and periodic wake-up (SPW) control is an effective ONU power saving technique. However, the effectiveness of SPW control is fully realized only if the sleep period changes in accordance with the traffic conditions. This paper proposes an SPW control mechanism with a variable sleep period. The proposed mechanism sets the sleep period according to traffic conditions, which greatly improves the power saving effect. In addition, the protocols needed between an optical line terminal (OLT) and ONUs are described on the assumption that the proposed mechanism is applied to 10-Gbit/s (10G) class PON systems, i.e., IEEE 802.3av 10G-EPON and FSAN/ITU-T 10G-PON systems. The validity of the proposed mechanism is confirmed by numerical simulations

**Published as:** R. Kubo, J. Kani, Y. Fujimoto, N. Yoshimoto, and K. Kumozaki, "Adaptive Power Saving Mechanism for 10 Gigabit Class PON Systems," IEICE Trans. Communications, Vol. E93-B, No. 2, pp. 280–288, Feb. 2010.

# Papers Published in Technical Journals and Conference Proceedings

# Electroluminescence and Capacitance-voltage Characteristics of Single-crystal n-type AIN (0001)/p-type Diamond (111) Heterojunction Diodes

K. Hirama, Y. Taniyasu, and M. Kasu Appl. Phys. Lett., Vol. 98, No. 011908, 2011.

n-type single-crystal AlN (0001) layers were grown on diamond (111) substrates by metalorganic vapor phase epitaxy. We observed current-injected emission at a wavelength of 235 nm at room temperature in an n-type AlN/p-type diamond heterojunction diode. The emission is attributed to free-exciton recombination in diamond. From capacitance-voltage measurements of the n-type AlN/p-type diamond heterojunction, we determined that the AlN/diamond heterojunction exhibits the *staggered* (type-II) band alignment with a

conduction band offset ( $\Delta E_C$ ) of 3.5 eV and a valence band offset ( $\Delta E_V$ ) of 4.0 eV.

#### Security of Cryptosystems Using Merkle-Damgård in the Random Oracle Model

Y. Naito, K. Yoneyama, L. Wang, and K. Ohta

IEICE Trans. Fundamentals, Vol. E94-A, No. 1, 2011.

Since the Merkle-Damgård hash function (MDFH) that uses a fixed input length random oracle as a compression function is not indifferentiable from a random oracle (RO) because of the extension attack, there is no guarantee of the security of cryptosystems that are

1 NTT Technical Review

secure in the RO model when RO is instantiated with MDHF. This fact motivates us to establish a criteria methodology for confirming cryptosystem security when RO is instantiated with MDHF. In this paper, we confirm cryptosystem security by using the following approach: 1) Find a weakened random oracle (WRO) that leaks values needed to realize the extension attack. 2) Prove that MDHF is indifferentiable from WRO. 3) Prove cryptosystem security in the WRO model. The indifferentiability framework of Maurer, Renner, and Holenstein guarantees that we can securely use the cryptosystem when WRO is instantiated with MDHF. Thus, we concentrated on such finding a WRO. We propose the Traceable Random Oracle (TRO), which leaks values enough to permit the extension attack. By using TRO, we can easily confirm the security of the OAEP encryption scheme and variants of it. However, there are several practical cryptosystems whose security cannot be confirmed by TRO (e.g., RSA-KEM). This is because TRO leaks values that are irrelevant to the extension attack. Therefore, we propose another WRO, Extension Attack Simulatable Random Oracle (ERO), which leaks just the value needed for the extension attack. Fortunately, ERO is necessary and sufficient to confirm the security of cryptosystems under MDHF. This means that the security of any cryptosystem under MDHF is equivalent to that under the ERO model. We prove that RSA-KEM is secure in the ERO model.

## Illuminant Color Estimation by Hue Categorization Based on Gray World Assumption

H. Kawamura, S. Yonemura, J. Ohya, and N. Matsuura Proc. of the SPIE, Vol. 7873, pp. 787312–787312-12, San Francisco, USA, 2011.

This paper proposes a gray-world-assumption-based method for estimating an illuminant color from an image by hue categorization. The gray world assumption hypothesizes that the average color of all the objects in a scene is gray. However, it is difficult to estimate an illuminant color correctly if the colors of the objects in a scene are dominated by certain colors. To solve this problem, our method uses the opponent color properties that the average of a pair of opponent colors is gray. Thus, our method roughly categorizes the colors derived from the image based on hue and selects them one by one from the hue categories until selected colors satisfy the gray world assumption. In our experiments, we used three kinds of illuminants (i.e., CIE standard illuminants A and D<sub>65</sub> and a fluorescent light) and two kinds of data sets. One data set satisfies the gray world assumption and the other does not. Experimental results show that estimated illuminants are closer to the correct ones than those obtained with the conventional method and the estimation errors for using CIE standard illuminants A and D<sub>65</sub> in our method are within the barely noticeable difference in human color perception.

#### Optical Spectrum Control Circuit Using an Arrayed-waveguide Grating and Tunable Phase Shifters

K. Kato, Y. Ikuma, H. Takahashi, T. Mizuno, and H. Tsuda IEICE Electronics Express, Vol. 8, No. 6, pp. 391–396, 2011.

We proposed and fabricated an optical spectrum control circuit using an arrayed-waveguide grating (AWG) and an array of channel waveguides with tunable phase shifters. We found that the spectral phase and amplitude of a modulated optical signal could be arbitrarily controlled if the number of channel waveguides was set to be more than twice the number of waveguides in the AWG. As a first demonstration, we successfully obtained a flat band-pass filter function with the fabricated device by controlling the tunable phase shifters to control the interference between the light propagating through

them.

#### Efficient Combination of Likelihood Recycling and Batch Calculation for Fast Acoustic Likelihood Calculation

A. Ogawa, S. Takahashi, and A. Nakamura

IEICE Trans. Information and Systems, Vol. E94-D, No. 3, pp. 648-658, 2011.

This paper proposes an efficient combination of state likelihood recycling and batch state likelihood calculation for accelerating acoustic likelihood calculation in an HMM-based speech recognizer. Recycling and batch calculation are based on different technical approaches, i.e., the former is a purely algorithmic technique while the latter fully exploits the computer architecture. To accelerate the recognition process further by combining them efficiently, we introduce conditional fast processing and acoustic backing-off. Conditional fast processing is based on two criteria. The first criterion, potential activity, is used to control not only the recycling of state likelihoods at the current frame but also the precalculation of state likelihoods for several succeeding frames. The second criterion, reliability, and acoustic backing-off are used to control the choice of recycled or batch-calculated state likelihoods when they are contradictory in the combination and to prevent word accuracies from degrading. Large vocabulary spontaneous speech recognition experiments using four machines with different CPUs under two environmental conditions showed that, compared with the baseline recognizer, recycling and batch calculation (our combined acceleration technique) further reduced both of the acoustic likelihood calculation time and the total recognition time. We also performed detailed analyses to reveal each technique's acceleration and environmental dependency mechanisms by classifying types of state likelihoods and counting each of them. The analysis results confirmed the effectiveness of the combined acceleration technique.

## Efficient Optical Flow Estimation Method Using Optimal Weighting Parameter of Sinusoidal Pattern

H. Sakaino

The Institute of Image Information and Television Engineers, Vol. 65, No. 3, pp. 382–394, 2011 (in Japanese).

In the Horn and Schunck optical flow method, a weighting parameter a of a motion smoothness constraint plays an important role in determining the estimation accuracy of optical flow. However, conventional methods of optimizing  $\alpha$  have been based on an empirical selection or cross-validation, where a global optimization is done at a high computational cost. Thus, a more efficient optimization method is needed. We first assume that real images can be approximated by a two-dimensional sinusoidal wave function on the basis of an example of a previously used texture analysis. Two image features-the amplitude (standard deviation of image brightness) and wave number using the sinusoidal wave function—are used to analyze and model the relationship between the optimal  $\alpha$  and two image features. From the analyzed model, the optimal  $\alpha$  can be used to locally minimize the estimation error of optical flow. Because these two simple image features of given real images are used, the optimal α can be estimated efficiently. Experimental results for optical flow estimation accuracy show that our proposed method outperforms conventional optical flow ones.

Vol. 9 No. 7 July 2011

## A Rat Model for Measuring the Effectiveness of Transcranial Direct Current Stimulation Using fMRI

Y. Takano, T. Yokawa, A. Masuda, J. Niimi, S. Tanaka, and N. Hironaka

Neurosci Lett., Elsevier, Vol. 491, No. 1, pp. 40-43, 2011.

Transcranial direct current stimulation (tDCS) is one of the noteworthy noninvasive brain stimulation techniques, but the mechanism of its action has remained unclear. With the aim of clarifying the mechanism, we developed a rat model and measured its effectiveness using fMRI. Carbon fiber electrodes were placed on the top of the head over the frontal cortex as the anode and on the neck as the cathode. The stimulus was 400- or 40-µA current applied for 10 min after a baseline recording in an anesthetized condition. The 400-µA stimulation significantly increased signal intensities in the frontal cortex and nucleus accumbens. This suggests that anodal tDCS over the frontal cortex induces neuronal activation in the frontal cortex and in its connected brain region.

#### Word Alignment with Synonym Information

H. Shindo, A. Fujino, and M. Nagata

Information Processing Society of Japan, Vol. 4, No. 2, pp. 13–22, 2011.

We present a novel framework for word alignment that incorporates monolingual synonym knowledge to improve word alignment performance. We think that synonym information is helpful to overcome the data sparseness problem of word alignment since there are various lexical forms representing the same meaning in a bilingual corpus. However, synonym relations depend heavily on context or domain since a word in natural language is ambiguous. We designed a synonym probabilistic model with a topic model, which uses synonym information according to the context. Moreover, we propose a word alignment framework that jointly trains our synonym model and conventional bilingual model. The experimental results show that our proposed method obtained better results compared with cases where synonym or context information is not used.

#### Multi-sized Sphere Packing: Computational Modeling and Formulation for the Packing Density in Containers

S. Yamada, J. Kanno, and M. Miyauchi

Information Processing Society of Japan, Vol. 4, No. 2, pp. 23–30, 2011 (in Japanese).

This article provides a mathematical formula for determining the optimal sizes of two different sized spheres to maximize the packing density when randomized loose packing is used in containers with various shapes. The formula was evaluated with numerous computer simulations involving over a million of spheres.

#### Robust Semi-supervised Learning for Labeled Data Selection Bias

A. Fujino, N. Ueda, and M. Nagata

Information Processing Society of Japan, Vol. 4, No. 2, pp. 31–42, 2011.

We propose a robust semi-supervised learning method for designing good classifiers with a high generalization ability from labeled data whose distribution differs largely from that of test data in a target domain. Although JESS-CM is one of the most successful semi-supervised learning methods that achieved the best published results in natural language processing tasks, it has an overfitting problem in our task setting. We expect the proposed method to solve the overfit-

ting problem by utilizing unlabeled data in the target domain with the labeled data for both training of discriminative and generative models composing a classifier. Our experimental results for text classification using three test collections confirmed that the classification performance obtained with the proposed method was better than that with JESS-CM in most cases of the task setting.

#### Non-data-aided Wide-range Frequency Offset Estimator for QAM Optical Coherent Receivers

T. Nakagawa, M. Matsui, T. Kobayashi, K. Ishihara, R. Kudo, M. Mizoguchi, and Y. Miyamoto

Proc. of OFC 2011, Vol. 2011, No. OMJ1, pp. 1–3, Los Angeles, USA.

We propose and experimentally demonstrate a novel blind frequency offset estimator for coherent quadrature amplitude modulation (QAM) receivers. Its frequency offset estimation range is more than three times the conventional estimation range.

#### Wide-range BER Measurement Scheme by Estimating BER of Discarded Frames for 10 G-EPON Systems

N. Ikeda, K. Terada, H. Uzawa, A. Miyazaki, S. Shigematsu, M. Urano, and T. Shibata

Proc. of OFC 2011, Vol. 2011, No. OTh, pp. OThT6, Los Angeles, USA.

This paper describes a new BER measurement method for obtaining the BER by estimating the number of error bits in discarded frames by using the rate of discarded frames. The BER is obtained precisely by the method.

## Origin of Exciton Emissions from an AIN p-n Junction Light-emitting Diode

Y. Taniyasu and M. Kasu

Appl. Phys. Lett., Vol. 98, No. 131910, 2011.

Exciton emissions from an AlN light-emitting diode with an improved emission efficiency of  $1\times10^{-4}\%$  were observed at 5.94 eV (208.7 nm) and 6.10 eV (203.2 nm) for current injection. The emission at 5.94 eV is attributed to an exciton emission originating from the crystal-field split-off valence band (CH-exciton emission). Owing to the large carrier-phonon interaction, the CH-exciton emission is accompanied by its phonon replicas. The emission at 6.10 eV is attributed to another exciton emission originating from heavy/light hole valence bands (HH/LH-exciton emission). From the emission energies, considering residual strain, the crystal-field splitting energy was determined to be -165 meV.

## Measuring Sweeping Echoes in Rectangular Cross-section Reverberant Fields

K. Kiyohara, K. Furuya, Y. Haneda, and Y. Kaneda

Acta Acustica united with Acustica, Vol. 97, No. 2, pp. 278–283, 2011

We investigated a new acoustical phenomenon, which we call sweeping echoes, in a two-dimensional (2D) space. Sweeping echoes in a three-dimensional (3D) space have recently been reported. We first investigated the regularity of reflected sound in a 2D regularly shaped space on the basis of number theory. The reflected pulse sound train has almost equal intervals between pulses on the squared-time axis as in a 3D space. This regularity of the arrival time of

NTT Technical Review

reflected pulse sounds generates sweeping echoes whose frequencies increase linearly with time. Computer simulation of room acoustics shows good agreement with the theoretical results. We first describe our number-theory-based investigation of a square cross-section. Next, we describe rectangular cross-sections with various aspect ratios investigated using the same theory as used for the square. We also discuss our measurements of sweeping echoes in a long hallway. We propose a method for extracting the sweep rates of sweeping echoes by calculating their correlation with a time stretched pulse. We analyzed the sweeping echoes for a source and receiver at the center of a rectangular cross-section. These sweeping echoes were perceived not only at the exact center position but also around the center

## Underdetermined Convolutive Blind Source Separation via Frequency Bin-wise Clustering and Permutation Alignment

H. Sawada, S. Araki, and S. Makino

IEEE Trans. Audio, Speech, and Language Processing, Vol. 19, No. 3, pp. 516–527, 2011.

This paper presents a blind source separation method for convolutive mixtures of speech/audio sources. The method can even be applied to an underdetermined case where there are fewer microphones than sources. The separation operation is performed in the frequency domain and consists of two stages. In the first stage, frequency-domain mixture samples are clustered into each source by an expectation-maximization (EM) algorithm. Since the clustering is performed in a frequency bin-wise manner, the permutation ambiguities of the bin-wise clustered samples should be aligned. This is solved in the second stage by using the probability of each sample belonging to the assigned class. This two-stage structure makes it possible to attain good separation even under reverberant conditions. Experimental results for separating four speech signals with three microphones under reverberant conditions show the superiority of the new method over existing methods. We also report separation results for a benchmark data set and live recordings of speech mixtures.

#### Chapter 1. Integration of Statistical-model-based Voice Activity Detection and Noise Suppression for Noise Robust Speech Recognition

M. Fujimoto

Recent Advances in Robust Speech Recognition Technology, Bentham Science Publishers, 2011.

This chapter addresses robust front-end processing for automatic speech recognition in noisy environments. To recognize corrupted speech accurately, it is necessary to use methods that are robust against various types of interference. Usually, noise suppression is used for the front-end processing of speech recognition in the presence of noise. Voice activity detection (VAD) is also used for front-end processing to eliminate the redundant non-speech period. VAD and noise suppression are typically combined as series processing. VAD and noise suppression should not be assumed to be separate techniques because the output information of these methods is mutually beneficial. Thus, this chapter introduces the integrated front-end processing of VAD and noise suppression, which can utilize each other's input-output information.

### Proposal of the Switching-control Algorithm for 3D-MEMS Optical Switch Module and Its Demonstration

M. Minakami, J. Yamaguchi, and S. Nemoto

The Japan Society for Precision Engineering, Vol. 77, No. 4, p. 383, 2011 (in Japanese).

A switching-control algorithm is necessary in order to connect the optical paths between input and output ports by using MEMS (microelectromechanical systems) mirrors in a free-space optical system. We propose a search algorithm that finds the maximum optical power by using the motion control technique of MEMS mirrors. We apply the algorithm to peak search control for optical path connection with maximum optical power and to optical power stabilization control in the case of environment changes, such as temperature change. The results confirm that the algorithm is suitable for practical use.

#### 100Gb/s Ethernet Inverse Multiplexing Based on Aggregation at the Physical Layer

K. Hisadome, M. Teshima, Y. Yamada, and O. Ishida IEICE Trans. Communications, Vol. E94-B, No. 4, pp. 904–909, 2011.

We propose a packet-based inverse multiplexing method to allow scalable network access with a bigger-pipe physical interface. The method is based on aggregation at the physical layer (APL) that fragments an original packet-flow and distributes the fragments among an adequate number of physical links or networks. It allows us to share wavelengths and/or bandwidth resources in optical networks. Its technical feasibility at the speed of newly standardized 100Gb/s Ethernet (100GbE) was successfully evaluated by implementing the inverse multiplexing logic functions on a prototype board. We demonstrated super-high-definition video streaming and huge file transfer by transmitting 100GbE MAC (media access control) frames over multiple 10GbE physical links via inverse multiplexing.

#### Multi-layer Hypercube Photonic Network Architecture for Intra-datacenter Network

T. Sakano, A. Kadohata, Y. Sone, A. Watanabe, and M. Jinno IEICE Trans. Communications, Vol. E94-B, No. 4, pp. 910–917, 2011

The popularity of cloud computing services is driving the boom in building mega-datacenters. This trend is forcing significant increases in the required scale of the intra-datacenter network. To meet this requirement, this paper proposes a photonic network architecture based on a multi-layer hypercube topology. The proposed architecture uses the cyclic-frequency arrayed waveguide grating (CF-AWG) device to realize a multi-layer hypercube and properly combines several multiplexing systems that include time division multiplexing (TDM), wavelength division multiplexing (WDM), wave-band division multiplexing (WBDM), and space division multiplexing (SDM). An estimation of the achievable network scale reveals that the proposed architecture can achieve a petabit-to-exabit-per-second-class, large-scale hypercube network with existing technologies.

#### **Debating Diversity**

M. Seyama

The Society of Polymer Science, Japan, Vol. 60, No. 5, p. 323, 2011 (in Japanese).

This paper provides comments about the debate on diversity and makes a suggestion.

Vol. 9 No. 7 July 2011 4