

# External Awards

## The Commendation for Science and Technology

**Winner:** Makoto Endo<sup>†1</sup>, Jiro Naganuma<sup>†2</sup>, and Yutaka Tashiro<sup>†3</sup>

†1 1st Product Group, NTT Electronics Corporation

†2 Visual Media Communications Project, NTT Cyber Space Laboratories

†3 Planning Section, NTT Cyber Space Laboratories

**Date:** April 17, 2007

**Organization:** The Ministry of Education, Culture, Sports, Science and Technology Prizes for Science and Technology (Development Category)

For “Development of Single-chip MPEG-2 HDTV Codec LSI.”

This issue is the world’s first successful development of a single-chip HDTV Codec LSI (development code name: VASA) to achieve material transmission in conformance with MPEG-2 international standards. This technology has made significant contribution to the progress of digital TV broadcasting as a key technology which supports terrestrial digital broadcasting infrastructure.

**References:** “Single-chip MPEG-2 422P@HL Codec LSI with Multi-chip Configuration for Large Scale Processing beyond HDTV Level,” Design, Automation and Test in Europe Conference 2003 (DATE2003), Mar. 2003.

## The Best Paper Award

**Winner:** Osamu Honda<sup>†1</sup>, Hiroyuki Ohsaki<sup>†1</sup>, Makoto Imase<sup>†1</sup>, and Kazuhiro Matsuda<sup>†2</sup>

†1 Osaka University

†2 NTT Network Innovation Laboratories

**Date:** May 7, 2007

**Organization:** International Academy, Research and Industry Association

For “Ring-Based Virtual Private Network Supporting a Large Number of VPNs.”

We propose a novel VPN mechanism called RING-VPN (Ring-based Virtual Private Network) that realizes a high scalability in terms of the number of VPNs. The key idea of our RING-VPN is to logically connect nodes in a ring topology for minimizing the number of IPsec tunnels. In our RING-VPN, each VPN node operates autonomously, making VPNs robust even in case of node and/or link failures. We also quantitatively evaluate the performance of our RING-VPN using mathematical analysis and simulation. Through several numerical examples, we quantitatively demonstrate the effectiveness of our RING-VPN in several network configurations.

# Papers Published in Technical Journals and Conferences

## Compact Sub-mW Mid-infrared DFG Laser Source Using Direct-bonded QPM-LN Ridge Waveguide and Laser Diodes

O. Tadanaga, Y. Nishida, T. Yanagawa, K. Magari, T. Umeki, M. Asobe, and H. Suzuki

LASE 2007, SPIE, Vol. 2007, No. 6455, p. 352, 2007.

We report the first sub-mW mid-IR laser source based on DFG in a QPM-LN waveguide directly pumped with two LDs. The signal was obtained from a 1.55- $\mu\text{m}$  band DFB-LD, and the pump from an FBG-stabilized LD. We used 1.064- and 0.976- $\mu\text{m}$  pump LDs for 3.4- and 2.6- $\mu\text{m}$  generation, respectively. To construct the mid-IR laser sources, we employed wavelength conversion modules with fiber pigtailed. The modules had high external conversion efficiencies of 10 and 16%/W for 3.4 and 2.6  $\mu\text{m}$ , respectively. The two LDs and the wavelength converter were assembled with a polarization maintaining fiber and then packaged in a box (100  $\times$  180  $\times$  100 mm).

We measured the output power of the mid-IR laser light sources as a function of the DFB-LD injection current. We obtained high outputs of up to 0.20 and 0.33 mW for the 3.4- and 2.6- $\mu\text{m}$  laser sources, respectively. The narrow linewidths of the 3.4- and 2.6- $\mu\text{m}$  laser light sources enabled us to detect the respective absorption lines of CH<sub>4</sub> and H<sub>2</sub>O clearly.

## Theorem-proving Anonymity of Infinite-state Systems

Y. Kawabe, K. Mano, H. Sakurada, and Y. Tsukada

Inf. Process. Lett., Elsevier, Vol. 101, No. 1, pp. 46–51, 2007.

The notion of anonymity is present in many fields of human activity. On the Internet, there are also many services and protocols where anonymity should be provided. For example, an electronic voting system should guarantee anonymity to prevent the disclosure of who voted for which candidate. Recently, there have been several studies based on formal methods that analyzed the anonymity of distributed systems. This paper presents an inductive method for verifying the anonymity of distributed systems with a theorem prover. The method that incorporates theorem-proving makes it possible to handle the anonymity of infinite-state systems.

## Hand-held Force Display with Spring-cam Mechanism for Generating Asymmetric Acceleration

T. Amemiya, H. Ando, and T. Maeda

World Haptics Conference, IEEE, pp. 572–573, Tsukuba, 2007.

This paper describes the development of a mechanism for a hand-held haptic display based on the force perception method, which exploits the perception of the difference between rapid and slow acceleration. Our previous force display was designed to generate asymmetric acceleration using a crank-slider mechanism with a rotational actuator. Here, to generate asymmetric acceleration, we pro-

pose a new mechanism that adopts a spring and cam with a linear actuator. The spring-cam mechanism can generate acceleration profiles of any shape and is suitable for miniaturization. We discuss the characteristics of a prototype of the spring-cam mechanism.

---

### Healing of Low-energy Irradiation-induced Defects in Single-walled Carbon Nanotubes at Room Temperature

S. Suzuki and Y. Kobayashi

J. Am. Chem. Soc., ACS, Vol. 111, pp. 4524–4528, 2007.

Single-walled carbon nanotubes are damaged by low-energy electron and photon irradiation, depending strongly on the diameter. In this study, the formation and healing of the irradiation-induced defects were found to be in competition during irradiation even at room temperature or below. The diameter dependence of the damage can be mainly ascribed to a diameter dependence of the activation energy of the defect healing. The activation energy was estimated to be about 1 eV.

---

### Low On-resistance of GaN *p-i-n* Vertical Conducting Diodes Grown on 4H-SiC Substrates

A. Nishikawa, K. Kumakura, and T. Makimoto

Physica Status Solidi, Wiley VCH Verlag, Vol. 4, No. 7, pp. 2662–2665, 2007.

We investigated the resistance of conductive AlGaIn buffer layers and the current-voltage characteristics of GaN *p-i-n* vertical conducting diodes on *n*-type 4H-SiC substrates grown by low-pressure metalorganic vapor-phase epitaxy. High Si doping of the AlGaIn buffer layer at the AlGaIn/SiC interface produces ohmic current-voltage characteristics in spite of the large band offset between AlGaIn and 4H-SiC. Owing to the optimization of the AlGaIn buffer layer, a low on-resistance ( $R_{on}$ ) of 1.12 m $\Omega$  cm<sup>2</sup> with high breakdown voltage ( $V_B$ ) of 300 V is obtained for a GaN *p-i-n* vertical conducting diode on a 4H-SiC substrate, leading to the figure of merit ( $V_B^2/R_{on}$ ) of 80 MW/cm<sup>2</sup>, which is larger than that for the diode with the same structure on a 6H-SiC substrate (62 MW/cm<sup>2</sup>). This result indicates that 4H-SiC is preferable for fabricating GaN-based electronic devices with a low on-resistance and high breakdown voltage.

---

### Effect of UV/Ozone Treatment on Nanogap Electrodes for Molecular Devices

T. Goto, H. Inokawa, M. Nagase, Y. Ono, K. Sumitomo, and K. Torimitsu

Jpn. J. Appl. Phys., Vol. 46, No. 4A, pp. 1731–1733, 2007.

We report the effect of UV/ozone treatment on nanogap electrodes for molecular devices. Gold nanogap electrodes with a nominal gap of 1–2 nm were fabricated by double oblique deposition and the break-junction technique. Self-assembled monolayers (SAMs) of 4,4'-*p*-terphenyldithiol (TPDT) were formed on the surfaces of the nanogap electrodes, and the electronic properties of these electrodes were measured. The device characteristics were also measured after repeated UV/ozone treatment and SAM re-formation. Although the resistance of the nanogap electrodes increased with the number of UV/ozone treatments, they could subsequently be used for molecular devices. We also observed Coulomb-diamond (CD) structures in the conductance contour plot with respect to the drain and gate voltages even after UV/ozone treatment. Some of the CDs observed after the treatment were aperiodic, presumably reflecting the discrete energy levels in TPDT.

---

### Probabilistic Anonymity via Coalgebraic Simulations

I. Hasuo and Y. Kawabe

ESOP 07, European association for theoretical computer sci., Vol. 4421, pp. 379–394, 2007.

There is growing concern about anonymity and privacy on the Internet, resulting in lots of work on formalization and verification of anonymity. In particular, the importance of the probabilistic aspect of anonymity is claimed recently by many authors. Among them are Bhargava and Palamidessi who present the definition of *probabilistic anonymity* for which, however, proof methods are not yet elaborated. In this paper we introduce a simulation-based proof method for probabilistic anonymity. It is a probabilistic adaptation of the method by Kawabe et al. for non-deterministic anonymity: anonymity of a protocol is proved by finding out a forward/backward simulation between certain automata. For the jump from non-determinism to probability we fully exploit a generic, coalgebraic theory of traces and simulations developed by Hasuo and others. In particular, an appropriate notion of probabilistic simulations is obtained by instantiating a generic definition with suitable parameters.

---

### A Kilobit Special Number Field Sieve Factorization

K. Aoki, J. Franke, T. Kleinjung, A. K. Lenstra, and D. A. Osvik

Cryptology ePrint archive, IACR, Vol. 2007, No. 206, 2007.

We describe how we reached a new factoring milestone by completing the first special number field sieve factorization of a number having more than 1024 bits, namely the Mersenne number  $2^{1039}-1$ . Although this factorization is orders of magnitude 'easier' than the factorization of a 1024-bit RSA modulus is believed to be, the methods we used to obtain our result shed new light on the feasibility of the latter computation.

---

### Distributed Quantum Computing

S. Tani and F. Le Gall

IEICE Trans., Vol. J90A, No. 5, pp. 393–402, 2007.

Distributed computing is quite a popular research area in classical computer science: it handles the computation performed collaboratively by multiple computers on a network. These days, much attention is paid to distributed quantum computing, in which quantum communication is allowed. In particular, the communication efficiency of distributed quantum computing is extensively studied in comparison with the classical equivalent. This paper reviews fundamental results.

---

### A 60-GHz-band Optical Injection-locked Oscillator Using a Top/back-illuminated InP/InGaAs HPT

H. Kamitsuna, M. Ida, and K. Kurishima

IPRM, IEEE, Vol. 1, No. 1, pp. 538–541, 2007.

This paper presents a 60-GHz-band oscillator that uses an InP/InGaAs heterojunction phototransistor (HPT) based on heterojunction bipolar transistor technologies. The HPT oscillator can be optically injection-locked by directly illuminating the HPT from either the top or back of the substrate since it has a photocoupling window in the emitter electrode and a "transparent" InP subcollector layer. When 2-nd subharmonic (around 30 GHz) and 4-th subharmonic (around 15 GHz) RF signals drive the optical modulator, the oscillator achieves wide locking ranges of 658 and 40 MHz, respectively. Nearly the same performance is obtained for top and back illumination.