External Awards

FY 2011 Industrial Standardization Awards (Industrial Science and Technology Policy and Environment Bureau Director-General's Award)

Winner: Hideaki Yamamoto, NTT Service Integration Laboratories
Date: Oct. 17, 2011
Organization: Ministry of Economy, Trade and Industry

For outstanding contributions to international standardization activities regarding ISO/IEC SC17/WG8 (Contactless smart card).

Celtic Excellence Gold Award 2012

Winners: Servery Project (Hiroki Baba[†1] and Naoki Takaya[†2])
†1 NTT Service Integration Laboratories
†2 NTT EAST
Date: Feb. 22, 2012
Organization: Celtic plus (Celtic Core Group)

The European research project SERVERY has been honored with the Celtic Excellence Gold Award 2012 for its excellent performance. NTT Service Integration Laboratories was involved in the project.
http://www.celtic-initiative.org/Publications/Press_releases/Celtic-Plus_Press-Release_2012-02-28.pdf

Papers Published in Technical Journals and Conference Proceedings

Generic Construction of Strongly Secure Timed-release Public-key Encryption

A. Fujioka, Y. Okamoto, and T. Saito

Lecture Notes in Computer Science, Vol. 6812/2011, pp. 319–336.

This paper provides a sufficient condition to construct timed-release public-key encryption (TRPKE), where the constructed TRPKE scheme guarantees strong security against malicious time servers, proposed by Chow et al., and strong security against malicious receivers, defined by Cathalo et al., in the random oracle model if the component identity-based encryption (IBE) scheme is IND-ID-CPA secure, the component PKE scheme is IND-ID-CPA secure, and the PKE scheme satisfies negligible γ-uniformity for every public key. Chow et al. proposed a strongly secure TRPKE scheme, which is specific in the standard model. To the best of our knowledge, our proposed construction is the first generic one for TRPKE that guarantees strong security even in the random oracle model.

Learning Condensed Feature Representations from Large Unsupervised Data Sets for Supervised Learning

J. Suzuki, H. Isozaki, and M. Nagata

Proc. of the 49th Annual Meeting of the Association for Computational Linguistics: short papers, pp. 636–641, Portland, Oregon, 2011.

This paper proposes a novel approach for effectively utilizing unsupervised data in addition to supervised data for supervised learning. We use unsupervised data to generate informative 'condensed feature representations' from the original feature set used in supervised natural language processing (NLP) systems. The main contribution of our method is that it can offer dense and low-dimensional feature spaces for NLP tasks while maintaining the state-of-the-art performance provided by the recently developed high-performance semi-supervised learning technique. Our method matches the results of current state-of-the-art systems with very few features, i.e., F-score of 90.72 with 344 features for CoNLL-2003 named entity recognition data and unlabeled attachment score of 93.55 with 12,500 features for dependency parsing data derived from PTB-III.

Circulator-free Reflection-type Tunable Optical Dispersion Compensator Using Tandem Arrayed-waveguide Gratings

Y. Ikuma, T. Mizuno, H. Takahashi, and H. Tsuda

Journal of Lightwave Technology, Vol. 29, No. 16, pp. 2447–2453, 2011.

A tunable optical dispersion compensator that uses cascaded arrayed-waveguide gratings and an integrated phase shifter is reported. It is a catoptric circuit but does not require a circulator. The dispersion is successfully controlled from +142 to +1148 ps/nm. Error-free transmission was confirmed after dispersion compensation in a transmission experiment using 43 Gbps CSRZ-DQPSK modulation.

Awareness of Central Luminance Edge is Crucial for the Craik-O'Brien-Cornsweet Effect

A. Masuda, J. Watanabe, M. Terao, M. Watanabe, A. Yagi, and K. Maruya

Frontiers in Human Neuroscience, Vol. 5, No. 125, 2011.

The Craik-O'Brien-Cornsweet (COC) effect demonstrates that perceived lightness depends not only on the retinal input at corresponding visual areas but also on distal retinal inputs. In the COC effect, the central edge of an opposing pair of luminance gradients (COC edge) makes adjoining regions with identical luminance appear to be different. To investigate the underlying mechanisms of the effect, we examined whether the subjective awareness of the COC edge is necessary for the effect to be generated. We manipulated the visibility of the COC edge using visual backward masking and continuous flash suppression while monitoring subjective reports regarding online percepts and after effects of adaptation. Psychophysical results showed that the online percept of the COC effect nearly vanishes in conditions where the COC edge is rendered invisible. On the other hand, the results of adaptation experiments showed that the COC edge is still processed at the early stage even under perceptual suppression. These results suggest that processing of the COC edge at the early stage is not sufficient to generate the COC effect and that subjective awareness of the COC edge is necessary.

Characterization of Strongly Secure Authenticated Key Exchanges without NAXOS Technique

A. Fujioka

Lecture Notes in Computer Science, Vol. 7038/2011, pp. 33–50.

This paper examines two-pass authenticated key exchange (AKE) protocols that do not use the NAXOS technique and that are secure under the gap Diffie-Hellman assumption in the random oracle model. Their internal structures are also discussed. We introduce an imaginary protocol, however insecure, to analyze the protocols and show the relations between these protocols from the viewpoint of how they overcome the insecurity of the introduced protocol. In addition, this paper provides ways to characterize the AKE protocols and defines two parameters: one consists of the number of static keys, the number of ephemeral keys, and the number of shared values, and the other is defined as the total sum of these numbers. When an AKE protocol is constructed on the basis of some kind of group, these two parameters indicate the number of elements in the group, i.e., they are related to the data sizes for storage and communication.

Multi-closure-interval Linear Prediction Analysis based on Phase Equalization

S. Hiroya, N. Miki, and T. Mochida

Proc. of APSIPA ASC 2011, Xi' an, China.

This paper presents a multi-closure-interval linear prediction (MCLP) analysis based on phase equalization in order to remove the effect of subglottal resonance in speech signals for estimating a vocal-tract spectrum. The validity of this method is evaluated by using a vocal-tract simulator that models vocal-tract losses and the subglottal system. Results show that the proposed method improves the estimation accuracy of a vocal-tract spectrum compared with the conventional MCLP method.

Stochastic Resonance Using a Steep-subthreshold-swing Transistor

K. Nishiguchi and A. Fujiwara

Proc. of the 24th International Microprocesses and Nanotechnology Conference, Kyoto, Japan, 2011.

We demonstrated stochastic resonance (SR) using nanoscale metal-oxide-semiconductor field-effect transistors (MOSFETs) with a small subthreshold swing. The MOSFET has a wire channel with triple gates and shows current characteristics, whose subthreshold swing is much smaller than 60 mV/dec owing to a parasitic bipolar transistor. The strong nonlinearity and hysteresis of the MOSFET's current characteristics increase the effect of SR, which allows the MOSFET to output a signal similar to an input signal that is much smaller than the MOSFET's threshold voltage. Additionally, using these features, we demonstrated pattern cryptography as a new application of SR.

Distributed Minimum Error Rate Training of Statistical Machine Translation Using Particle Swarm Optimization

J. Suzuki, K. Duh, and M. Nagata

Proc. of the 5th International Joint Conference on Natural Language Processing, pp. 649–657, Chiang Mai, Thailand, 2011.

Direct optimization of a translation metric is an integral part of building state-of-the-art statistical machine translation (SMT) systems. Unfortunately, widely used translation metrics such as the LEU score are non-smooth, non-convex, and non-trivial to optimize. Thus, standard optimizers such as minimum error rate training can be extremely time-consuming, leading to a slow turnaround rate for SMT research and experimentation. We propose an alternative approach based on particle swarm optimization, which can easily exploit the fast growth of distributed computing to obtain solutions quickly. For example in our experiments on NIST 2008 Chinese-to-English data with 512 cores, we demonstrate a speed increase of up to 15 times and reduction in parameter tuning time from 10 hours to 40 minutes with no degradation in BLEU score.

Bound Exciton Photoluminescence from Ion-implanted Phosphorus in Thin Silicon Layers

H. Sumikura, K. Nishiguchi, Y. Ono, A. Fujiwara, and M. Notomi

Optics Express, Vol. 19, No. 25, pp. 25255–25262, 2011.

We report the observation of clear bound exciton (BE) emission from ion-implanted phosphorus. Shallow implantation and high-temperature annealing successfully introduce active donors into thin silicon layers. The BE emission at a wavelength of 1079 nm shows that some of the implanted donors are definitely activated and isolated from each other. However, photoluminescence and electron spin resonance studies find a cluster state of the activated donors. The BE emission is suppressed by this cluster state rather than by the nonradiative processes caused by ion implantation. Our results provide important information about ion implantation for doping quantum devices with phosphorus quantum bits.

Tunable Optical Dispersion Compensator with a High-resolution Arrayed-waveguide Grating

Y. Ikuma, T. Mizuno, H. Takahashi, and H. Tsuda

IEICE Electronics Express, Vol. 8, No. 24, pp. 2087–2092, 2011.

A tunable optical dispersion compensator (TODC) that uses a high-resolution arrayed-waveguide grating and integrated resin lenses is reported. The dispersion tuning range is 1426 ps/nm, three times larger than that in our previous report for the same type of TODC. A transmission experiment using a 43-Gbps carrier-suppressed return-to-zero differential quadrature phase shift keying (CSRZ-DQPSK) signal is also reported.

Effect of Hydrogen Entry into Steel

H. Saito, N. Fujimoto, and T. Sawada

Proc. of the ISSS-6: 6th International Symposium on Surface Science, 13PN-112, Tokyo, Japan, 2011.

Hydrogen embrittlement of steel is caused by the interaction between hydrogen and metal. We investigated this phenomenon by using an electrochemical technique and microscope observation. Since a hydrogen atom does not have extranuclear electrons, the behavior of hydrogen atoms is difficult to analyze. We therefore reduced a hydrogen molecule into protons, or hydrogen cations, at one surface of a steel plate sample and oxidized protons at the other surface of the plate. Reduction and oxidation were carried out by controlling the electrical potential. The measured current revealed the elementary reduction/oxidation process and entry properties of hydrogen on steel sample surface(s). We found that the polarization of a sample controls the entry of adsorbed hydrogen. Microscope observation showed that a critical concentration induces the growth of micro-cracks.

SAW: Java Synchronization Selection of Lock or Software Transactional Memory

Y. Yamada, H. Iwasaki, and T. Ugawa

Proc. of 2011 IEEE 17th International Conference on Parallel and Distributed Systems (ICPADS), pp. 104–111, Tainan, Taiwan, 2011.

To rewrite a sequential program into a concurrent one, the programmer has to enforce atomic execution of a sequence of accesses to shared memory to avoid unexpected inconsistency. There are two means of enforcing this atomicity: one is the use of lock-based synchronization and the other is the use of software transactional memory (STM). However, it is difficult to predict which one is more suitable for an application other without trying both mechanisms because their performance heavily depends on the application. We have developed a system named SAW that decouples the synchronization mechanism from the application logic of a Java program and enables the programmer to statically select a suitable synchronization mechanism: either lock or STM. We introduce annotation to specify critical sections and shared objects. In accordance with the annotated source program and the programmer's choice of a synchronization mechanism, SAW generates aspects representing the synchronization processing. By directly comparing the cost of rewriting using SAW and that using an individual synchronization mechanism, we show that SAW relieves the programmer's burden. Through several benchmarks, we demonstrate that SAW is an effective way of switching synchronization mechanisms according to the characteristics of each application.

Proposal of Channel-grouping Wireless-transceiver Architecture for Suppressing Local-oscillator Phase Noise

M. Ugajin

IEICE Electronics Express, Vol. 9, No. 2, pp. 86–91, 2012.

This paper proposes an architecture-level solution for suppressing the phase noise of local oscillators in wireless-transceiver large-scale integrated circuits (LSIs). Because a phase-looked loop (PLL) supplies only one local oscillator frequency for multiple channels, the PLL's large loop bandwidth can be used to suppress the phase noise. Simulation results show that a sixteen-channel grouping can suppress the phase noise by more than 24 dB in narrow-band wireless systems. Channel selection in receive mode can be ensured by a variable intermediate frequency (IF) complex band-pass filter. Local-leak and image signals in transmit mode can be suppressed by a quadrature up-conversion mixer and radio-frequency band-pass filter with a high-IF configuration. A digital-to-analog converter, analog-to-digital converter, and digital LSI perform modulation and demodulation of the variable-IF signals.

Growth and Device Properties of AlGaN/GaN High-Electron Mobility Transistors on a Diamond Substrate

K. Hirama, M. Kasu, and Y. Taniyasu

Jpn. J. Appl. Phys., Vol. 51, No. 01AG09, 2012.

A crack-free c-plane AlGaN/GaN heterostructure was grown on a diamond (111) substrate by using an AlN/GaN multi-buffer layer. We found that in the AlGaN/GaN heterostructure, the GaN layer was coherently grown on the AlN/GaN multi-buffer layer. The a-lattice constant of strain-free GaN is longer than the average a-lattice constant of the AlN/GaN multi-buffer layer. Therefore, compressive strain is induced in the GaN layer of the AlGaN/GaN heterostructure. The compressive strain compensates for the tensile strain induced by the diamond substrate, which makes the AlGaN/GaN heterostructure free of cracks. AlGaN/GaN high-electron mobility transistors (HEMTs) fabricated on diamond substrates show maximum drain current of 275 mA/mm, transconductance of 60 mS/mm, and clear pinch-off characteristics for a gate length of 6 μm. The low thermal resistance of the AlGaN/GaN HEMTs on diamond is demonstrated.

Security of Sequential Multiple Encryption

A. Fujioka, Y. Okamoto, and T. Saito

IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E95-A, No. 1, pp. 57–69, 2012.

This paper analyzes the security of sequential multiple encryptions based on asymmetric key encryptions and shows that a sequential construction of secure multiple encryptions exists. The sequential multiple encryption scheme can be proved to be indistinguishable against chosen ciphertext attacks for multiple encryptions (IND-ME-CCA), where the adversary can access the decryption oracle of the multiple encryption, even when all the underlying encryptions of the multiple encryption are indistinguishable against chosen plaintext attacks (IND-CPA). We provide an extended security notion of sequential multiple encryptions, in which the adversary is allowed to access decryption oracles of the underlying encryptions in addition to the multiple encryption, and we show that our constructed scheme satisfies the security notion when all the underlying encryptions are indistinguishable against chosen ciphertext attacks (IND-CCA).

A Semitransparency-based Optical-flow Method with a Point Trajectory Model for Particle-like Video

H. Sakaino

IEEE Trans. on Image Processing, Vol. 21, No. 2, pp. 441–450, 2012.

This paper proposes a new semitransparency-based optical-flow model with a point trajectory model for particle-like video. Previous optical-flow models have used properties ranging from image brightness constancy to image brightness change models as constraints. However, two important issues remain unsolved. The first issue is how to track/match a semitransparent object when the displacement between video frames is very large. Such moving objects with different shapes and sizes in an outdoor scene move against a complicated background. Second, due to semitransparency, the image intensity between frames can also violate a previous image brightness-based optical-flow model. Thus, we propose a two-step optimization for the optical-flow estimation model for a moving semitransparent object, i.e., particle. In the first step, a rough optical flow between particles is estimated by a new alpha constancy constraint that is based on an image generation model of semitransparency. In the second step, the optical flow of a particle with a continuous trajectory in a definite temporal interval based on a point trajectory model can be refined. Many experiments using various falling-snow and foggy scenes with multiple moving vehicles show the significant improvement in the optical flow compared with a previous optical-flow model.