External Awards

DEWS2007 Excellent Paper Award
Winner: Hiroyuki Toda, NTT Cyber Solutions Laboratories
Date: July 12, 2007
Organization: IEICE

For "Topic structure mining using temporal co-occurrence".

DBWeb2007 Enterprise Paper Award
Winner: Masaya Murata, NTT Cyber Solutions Laboratories
Date: November 28, 2007
Organization: IPSJ

For "A Query Expansion Method Using Access Concentration Sites in Search Result".

The Young Researchers' Award of IEICE
Winner: Takashi Matsui, NTT Access Network Service Systems Laboratories
Date: March 19, 2008
Organization: IEICE

For (1) "Structural dependence of guided acoustic-wave Brillouin scattering in hole-assisted fiber" (in Japanese) and (2) "Quasi-distributed temperature sensor based on GAWBS of hole-assisted fiber" (in Japanese).

The former clarified the structural dependence and controllability of guided acoustic wave Brillouin scattering (GAWBS) in hole-assisted fiber (HAF) numerically and experimentally. The latter described a simple and cost-effective quasi-distributed fiber-optic sensor based on a unique type of GAWBS in HAF.

Papers Published in Technical Journals and Conferences

A Fast Quantum Circuit for Addition with Few Qubits
Y. Takahashi and N. Kunihiro

Quantum Information Processing 2008, Indian Association of Research in Computing Science, Vol. 1, No. 1, pp. 1–12, New Delhi, 2007.

We show how to construct a fast quantum circuit for the addition of two n-bit binary numbers with few qubits. The constructed circuit uses $O(n/\log n)$ ancillary qubits and its depth and size are $O(\log n)$ and $O(n)$, respectively. The number of ancillary qubits is less than that in Draper et al.'s quantum carry-lookahead adder, and the depth and size are the same as those of Draper et al.'s. Moreover, we modify the circuit using the quantum Fourier transform and use the modified version to construct an efficient quantum circuit for Shor's factoring algorithm.

Formalization and Automation of Security Proof by Sequences of Games
K. Mano, H. Sakurada, Y. Kawabe, and Y. Tsukada

Industrial and Applied Mathematics, Iwanami, Vol. 17, No. 4, pp. 38–46, 2007 (in Japanese).

Recently extensive research has been undertaken on the computational foundations of symbolic proof methods for safety of security protocols. In this paper we introduce studies within the approach to obtain a symbolic method by formalizing the proof method called game sequence.

On the Equivalence of Several Security Notions of KEM and DEM
W. Nagao, Y. Manabe, and T. Okamoto

Trans. IEICE. Jpn., Vol. E91-A, No. 1, pp. 283–297, 2008.

KEM (Key Encapsulation Mechanism) and DEM (Data Encapsulation Mechanism) were introduced by Shoup to formalize the asymmetric encryption specified for key distribution and the symmetric encryption specified for data exchange in ISO standards on public-key encryption. Shoup defined the "semantic security (IND) against adaptive chosen ciphertext attacks (CCA2)" as a desirable security notion of KEM and DEM, that is, IND-CCA2 KEM and IND-CCA2 DEM. This paper defines "non-malleability (NM)" for KEM, which is a stronger security notion than IND. We provide three definitions of NM for KEM and show that these three definitions are equivalent. We then show that NM-CCA2 KEM is equivalent to IND-CCA2 KEM. That is, we show that NM is equivalent to IND for KEM under CCA2 attacks, although NM is stronger than IND in the definition (or under some attacks like CCA1). In addition, this paper defines the universally composable (UC) security of KEM and DEM and shows that IND-CCA2 KEM (or NM-CCA2 KEM) is equivalent to UC KEM and that "IND against adaptive chosen plaintext/ciphertext attacks (IND-P2-C2)" DEM is equivalent to UC DEM.

Gate Metal Interface on Hydrogen-terminated Diamond FETs
M. Kasu, K. Ueda, and H. Kageshima

Surface Science, The Surface Science Society of Japan, Vol. 29, No. 3, pp. 159–163, 2008.

Hydrogen surface termination is widely used as a p-type doping in diamond semiconductors, but the p-type conduction mechanism is still controversial. In this study, we found an energy barrier for holes between the gate and the two-dimensional hole channel on the hydrogen-terminated diamond surface from FET characteristics. Separately we confirmed an interfacial layer between the gate metal layer and hydrogen-terminated diamond surface from cross-sectional transmission electron microscopic observation. We conclude that during metal evaporation on hydrogen-terminated diamond surface,

metal atoms diffuse through point defects in the subsurface layer, and eventually the interfacial layer forms there.

Study of applying the cold index to disaster prevention

M. Sotoma

Reports of the City Planning Institute of Japan, No. 6-4, pp. 156–160, 2008 (in Japanese).

People in a disaster-stricken area may be exposed to a cold environment, which has various influences on the human body and mind. Restrictions on physical and mental activities may lead to people being in risky situations. IREQ, DLE, and WCT are indices that evaluate the influence of cold on the human body. It may be possible to keep the people away from cold stress by using these indices. Therefore, content and features of these indices were considered. As a result, we found that the cold index can be used for disaster prevention between the applicable range of indices and the climate of Japan.

Multichannel Linear Prediction Method Compliant with MPEG-4 ALS

Y. Kamamoto, N. Harada, and T. Moriya

IEICE TRANS. FUNDAMENTALS, VOL. E91-A, NO. 3, March 2008.

A new linear prediction analysis method for multichannel signals was devised, with the goal of enhancing the compression performance of the MPEG-4 Audio Lossless Coding (ALS) compliant encoder and decoder. The multichannel coding tool for this standard carries out an adaptively weighted subtraction of the residual signals of the coding channel from those of the reference channel, both of which are produced by independent linear prediction. Our linear prediction method tries to directly minimize the amplitude of the predicted residual signal after subtraction of the signals of the coding channel, and the method has been implemented in the MPEG-4 ALS codec software. The results of a comprehensive evaluation show that this method reduces the size of a compressed file. The maximum improvement of the compression ratio is 14.6% which is achieved at the cost of a small increase in computational complexity at the encoder and without increase in decoding time. This is a practical method because the compressed bitstream remains compliant with the MPEG-4 ALS standard.