External Awards

ACM SIGKDD 2008 Best Research Paper Awards

Runner-up: Yasuhiro Fujiwara[†1], Yasushi Sakurai[†2], and Masashi Yamamuro[†1]

†1 NTT Cyber Space Laboratories

†2 NTT Communication Science Laboratories

Date: August 2008

Organization: ACM SIGKDD 2008 Committee

For "SPIRAL: Efficient and Exact Model Identification for Hidden Markov Models".

Hidden Markov models (HMMs) have received considerable attention in various communities (e.g., speech recognition, neurology, and bioinformatics) since many applications that use them have emerged. The goal of this work is to identify efficiently and correctly the model in a given dataset that yields the state sequence with the highest likelihood with respect to the query time sequence. We propose SPIRAL, a fast search method for HMM datasets. To reduce the search cost, SPIRAL efficiently prunes a significant number of search candidates by applying successive approximations when estimating likelihood. We performed several experiments to verify the effectiveness of SPIRAL. The results show that SPIRAL was up to 526 times faster than the naive method.

Papers Published in Technical Journals and Conferences

Enhanced superconductivity by reducing magnetism in strained $La_{2-x}Sr_xCuO_4$ films

H. Sato

Physica C, Elsevier, Vol. 468, No. 1, pp. 2366–2368, 2008.

I report measurement results of the temperature dependence of electrical resistivity for the compressively strained (001)-oriented films of $La_{2-x}Sr_xCuO_4$, which show values of the superconducting transition temperature (T_c) higher than those for bulk materials. A comparison of the results for the films with those for bulk suggests that the number density of localized Cu spins is reduced in the films. This reduction seems to be essential for the enhancement of T_c in the films, which leads me to suggest that the magnetism in cuprates, rather than being the origin of high-temperature superconductivity (HTS), is actually an impediment to it.

Anonymous return route information for onion based mix-nets

Y. Manabe and T. Okamoto

AIPACa 2008, ICST, Vol. 1, pp. 1–8, Istanbul, Turkey.

This paper proposes a return route information encryption scheme for onion-based e-mail systems and mix-nets. Our scheme has the following two properties. (1) It allows any node on the message route to send reply messages to the message sender. This property is necessary for sending error replies. (2) It allows the replying node to send multiple reply messages from one piece of return route information. This property is necessary when responding with large amounts of data using multiple messages. In order to construct a return route information scheme, we must consider a new type of attack, namely the replace attack. A malicious node obtains information about the route by replacing part of the message by secret information that only the node can read. This paper describes the new type of attack and shows that previous schemes are vulnerable to it. Our scheme prevents replace attacks. In addition, we show that a slight modification of our scheme ensures that malicious nodes cannot distinguish whether a message is a forward message or a reply message, thus improving the security of the routing scheme.

Relationship of Three Cryptographic Channels in the UC Framework

W. Nagao, Y. Manabe, and T. Okamoto

ProvSec 2008, Chinese Association for Cryptologic Research, Vol. 5324, pp. 268–282, Shanghai, China.

The relationship of three cryptographic channels, secure channels (SCs), anonymous channels (ACs) and direction-indeterminable channels (DICs), has been investigated by Okamoto. He showed that the three cryptographic channels are reducible to each other, but did not consider communication schedules clearly as well as composable security. This paper refines the relationship of the three channels in the light of communication schedules and composable security. We model parties by the task-probabilistic input/output automata (PIOA) to treat communication schedules and adopt the universally composable (UC) framework by Canetti to treat composable security. We show that a class of anonymous channels, two-anonymous channels (2ACs), and DICs are reducible to each other under any schedule and that DICs and SCs are reducible to each other under some types of schedules, in the UC framework with the PIOA model.

Si nano-wire ion-sensitive field-effect transistors with a shared floating gate

K. Nishiguchi, N. Clement, T. Yamaguchi, and A. Fujiwara

MNC, JSAP, pp. 20–21, Fukuoka, Japan, 2008.

Ion-sensitive field-effect transistors (ISEETs) arrayed in parallel were fabricated on a silicon-on-insulator substrate. Since nanoscale wire channels of ISFETs are bridged with a floating gate, on which

molecules are preferably immobilized, signals originating from charged materials just on the floating gate can appear for the bridged ISFETs and therefore be distinguished from background noise, which leads to noise-robust sensing. Additionally, nanoscale channels provide ISFETs with single-electron-resolution charge sensitivity as well as reduced background noise induced in wider channels used for electrical leads. These features promise detection of a small number of molecules.

Miniaturized Lumped-Element Power Dividers with a Filtering Function

H. Hayashi and M. Kawashima

Trans. IEICE. Jan., Vol. E91-C, No.11, pp. 1798–1805, 2008.

Three miniaturized lumped-element power dividers with a filtering function for use in quadrature mixers are described. Simulation results showed that they can be miniaturized, unlike conventional ones with open/short stubs, while maintaining the filter characteristics. A fabricated 0.95-GHz 0° power divider with a filtering function had a chip size about half that of a conventional lumped-element one. Its insertion loss at 0.95 ± 0.05 GHz was 4.0 ± 0.1 dB.

Miniaturization of Haptic Interface Utilizing Sensory Illusion of Being Pulled and Its Effect

T. Amemiya and T. Maeda

Human Interface Society, Vol. 10, No. 4, pp. 125–134, 2008.

When a small object in a hand-held device moves periodically and prismatically with asymmetric acceleration (strong in one direction and weak in the other), one typically experiences the kinesthetic illusion of being pushed or pulled continuously by the held device. This effect was investigated because of its potential application to a hand-held, non-grounded, haptic device that can convey a sense of a continuous translational force in one direction, which is a yet missing tile in haptic research. Here, a one-degree-of-freedom haptic device based on a double-layer crank-slider mechanism was constructed based on the results of our previous research. We evaluated the effectiveness of the perception of directed force sensation by asymmetric oscillation compared with the previous prototype and the effectiveness of the gross weight of the device. Our results show that the ratio of the gross weight of the device and the weight of reciprocating mass should be at least 16% for effective force perception.

The nearest polynomial with a zero in a given domain

H. Sekigawa

Theor. Comput. Sci., Elsevier, Vol. 409, No. 2, pp. 282–291, 2008.

For a real univariate polynomial f and a closed domain $D \subset \mathbb{C}$ whose boundary C is represented by a piecewise rational function, we provide a rigorous method for finding a real univariate polynomial $\tilde{f}$ such that $\tilde{f}$ has a zero in D and $\|f-\tilde{f}\|_\infty$ is minimal. First, we prove that if a nearest polynomial exists, there is a nearest polynomial $\tilde{f}$ such that the absolute value of every coefficient of $f-\tilde{f}$ is $\|f-\tilde{f}\|_\infty$ with at most one exception. Using this property and the representation of C, we reduce the problem to solving systems of algebraic equations, each of which consists of two equations with two variables.

A new Gröbner basis conversion method based on stabilization techniques

K. Shirayanagi and H. Sekigawa

Theor. Comput. Sci., Elsevier, Vol. 409, No. 2, pp. 311–317, 2008.

We propose a new method for converting a Gröbner basis w.r.t. one term order into a Gröbner basis w.r.t. another term order by using the algorithm stabilization techniques proposed by Shirayanagi and Sweedler. First, we guess the support of the desired Gröbner basis from a floating-point Gröbner basis by exploiting the supportwise convergence property of the stabilized Buchberger's algorithm. Next, assuming this support to be correct, we use linear algebra, namely, the method of indeterminate coefficients to determine the exact values for the coefficients. Related work includes the FGLM algorithm and its modular version. Our method is new in the sense that it can be thought of as a floating-point approach to the linear algebra method. The results of Maple computing experiments indicate that our method can be very effective in the case of non-rational coefficients, especially ones including transcendental constants.
