External Awards

Best Interactive Award

Winners: Kyosuke Nishida[*1], Ryohei Banno[*2], Ko Fujimura[*1], and Takahide Hoshide[*1]

*1 NTT Cyber Solutions Laboratories

*2 Hokkaido University

Date: Mar. 1, 2011

Organization: The 3rd Forum on Data Engineering and Information Management

For "Tweet-Topic Classification on Twitter with Data Compression".

Published as: K. Nishida, R. Banno, K. Fujimura, and T. Hoshide, "Tweet-Topic Classification on Twitter with Data Compression," the 3rd Forum on Data Engineering and Information Management (DEIM 2011), A1-6, Izu, Japan.

Young Engineer's Award

Winner: Shin Kaneko, NTT Access Network Service Systems Laboratories

Date: Mar. 15, 2011

Organization: The Institute of Electronics, Information and Communication Engineers (IEICE)

For "Frequency-domain Optical CDM Employing Spectral M-ary Modulation Based on Electrical-domain Spatial Code Spreading"

This paper proposes a novel transmitter configuration that flexibly enhances the scalability for frequency-domain optical code-division multiplexing (CDM) based on electrical-domain spatial code spreading. The transmitter employs dummy data input and pre-biasing circuits. The dummy data input to the transmitter means that the total number of multiplexed binary data streams, comprising those that actually accommodate users/services and the dummy streams, remains constant. Pre-biasing circuits enable us to achieve high tolerance to multiple access interference by compensating for the nonlinearity of the M-ary modulation and improve the receiver sensitivity. Owing to the dummy data input, none of the parameters for pre-biasing must be changed regardless of the number of users/services. Therefore, the proposed transmitter can flexibly enhance the scalability of optical CDM. The feasibility of the proposed transmitter is verified theoretically.

Published as: S. Kaneko, N. Miki, H. Kimura, and H. Hadama, "Frequency-domain Optical CDM Employing Spectral M-ary Modulation Based on Electrical-domain Spatial Code Spreading," Technical Report of IEICE, OCS (B-10-47), Vol. 110, No. 176, pp. 37–40, 2010 (in Japanese).

For "Spectral Efficiency Improvement in Frequency-domain Optical CDM Based on Electrical-domain Spatial Code Spreading"

Published as: S. Kaneko, N. Miki, H. Kimura, and H. Hadama, "Spectral Efficiency Improvement in Frequency-domain Optical CDM Based on Electrical-domain Spatial Code Spreading," Technical Report of IEICE (B-10-45) No. 2, p. 232, 2010 (in Japanese).

Papers Published in Technical Journals and Conference Proceedings

Heterostructure Growth of a Single-crystal Hexagonal AlN (0001) Layer on Cubic Diamond (111) Surface

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

J. Appl. Phys. Vol. 108, No. 1, p. 013528, 2010.

We demonstrate heterostructure growth of a hexagonal AlN (0001) layer on cubic diamond (111) surface and investigate the interface structure in order to achieve AlN/diamond heterojunction devices. From the initial growth, the single-crystal AlN (0001) layer grows on the diamond (111) surface with an in-plane epitaxial relationship $[1010]_{AlN}//[110]_{diamond}$. A high-resolution transmission electron microscope image shows an abrupt interface. Misfit dislocations are distributed periodically at the heterointerface owing to the large lattice mismatch between AlN and diamond. Compared with the in-plane epitaxial relationship $[1120]_{AlN}//[110]_{diamond}$, $[1010]_{AlN}//[110]_{diamond}$ is energetically preferred because it has a higher bond density and, therefore, lower interfacial energy.

Extension of Secret Handshake Protocols with Multiple Groups in Monotone Condition

Y. Kawai, S. Tanno, T. Kondo, K. Yoneyama, K. Ohta, and N. Kunihiro

IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. 93, No. 6, pp. 1122–1131, 2010.

The Secret Handshake protocol allows members of the same group to authenticate each other secretly. That is, two members who belong to the same group can learn that the counterpart is in the same group, while non-members of the group cannot determine whether or not the counterpart is a member of the group. Yamashita and Tanaka proposed Secret Handshake Scheme with Multiple Groups (SHSMG). They extended a single group setting to a multi-group setting where two members output "accept" if both members' affiliations of the multiple groups are identical. In this paper, we first show a flaw in

their SHSMG and construct a new secure SHSMG. Second, we introduce the new concept of the Secret Handshake scheme "monotone condition Secret Handshake with Multiple Groups (mc-SHSMG)" in order to extend the "accept" condition. In our new handshake protocol setting, members can authenticate each other in the monotone condition (not only in the case where both members' affiliations are identical but also in the case where they are not identical). The communication costs and computational costs of our proposed mc-SHSMG are lower than for the trivial construction of it.

Proxiable Designated Verifier Signature

M. Ushida, K. Ohta, Y. Kawai, and K. Yoneyama

Proc. of Security and Cryptography (SECRYPT) 2010, pp. 344–353, Athens, Greece.

Designated Verifier Signature (DVS) guarantees that only a verifier designated by a signer can verify the validity of a signature. In this paper, we propose a new variant of DVS: Proxiable Designated Verifier Signature (PDVS), where the verifier can make a third party (i.e., the proxy) substitute for some of the verification process. In the PDVS system, the verifier can reduce his computational cost by delegating some of the verification process without revealing the validity of the signature to the proxy. In all DVS systems, the validity of a signature means that a signature satisfies both of the following properties: (1) the signature is accepted by a decision algorithm and (2) the signature is confirmed to have been generated by the signer. In the PDVS system, the verifier can make the proxy substitute for only the checking of property (1). In the PDVS model, we divide the verifier's secret keys into two parts: one is a key for performing the decision algorithm, and the other is a key for generating a dummy signature, which prevents a third party from being convinced of property (2). We also define security requirements for PDVS and propose a PDVS scheme that satisfies all of the security requirements that we define.

Transmission Characteristics of Chirp-managed Direct Modulation over Hybrid Link of SMF and DSF

S. Usui, H. Iwashita, and T. Kubo

OptoeElectronics and Communications Conference (OECC) 2010, pp. 298–299, Sapporo, Japan.

A chirp-managed direct-modulated optical signal has a high tolerance for fiber dispersion. However, its tolerance for nonlinear effects is not clear. We thus investigated its applicability to a hybrid link of SMF and DSF without line amplifiers.

Diamond Semiconductor and Its Prospects for High RF Power Devices

M. Kasu

Material stage, Technical Information Institute Co. Ltd., Vol. 10, No. 7, pp. 58–61, 2010 (in Japanese).

The present status and prospects of diamond RF power devices are reviewed.

Cross-realm Password-based Server Aided Key Exchange

K. Yoneyama

WISA, KIISC, Lecture Notes in Computer Science, 2011, Vol. 6513, pp. 322–336, Jeju, Korea.

In this paper, we extend password-based server aided key exchange (PSAKE) to the cross-realm setting which enables two clients in two different realms with different passwords to exchange a session key through their corresponding servers, i.e., there are two servers. We cannot simply apply the previous security model of PSAKE to the cross-realm setting because there is a difference between the security properties that can be captured in the previous setting and in the new setting. Therefore, we define a new formal security model of cross-realm PSAKE. Our model captures all desirable security requirements, like resistance to leakage of ephemeral private keys, to key-compromise impersonation, and to undetectable on-line dictionary attack. Furthermore, we propose a concrete construction of cross-realm PSAKE with the optimal number of rounds for a client that is secure in the sense of our model. Our scheme assumes no pre-established secure channels between different realms unlike previous schemes, but just authenticated channels between different realms.

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

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

Optical Communication (ECOC) 2010, Vol. We. 8. E. 7, pp. 1–3, Torino, Italy.

A tunable optical dispersion compensator that uses cascaded arrayed-waveguide gratings and an integrated phase shifter is reported. It has a reflective configuration but does not require a circulator. The dispersion is successfully controlled from +142 to +1148 ps/nm.

Observation of n-type Conduction in Arsenic-doped CVD Diamond

M. Kasu

Proc. of Int. Symp. on Compound Semicond 2010, Vol. 1, No. 1, p. 1, Takamatsu, Japan, 2010.

We achieved n-type diamond by using arsenic doping.

Increase of Hole Concentration of H-terminated Diamond and Its Application to FET

K. Michal and M. Kasu

Proc. of Int. Symp. on Compound Semicond 2010, Vol. 1, No. 1, p. 1, Takamatsu, Japan, 2010.

We improved H-terminated diamond FET by NO_2 adsorption.

Indifferentiable Security Reconsidered: Role of Scheduling

K. Yoneyama

Proc. of ISC'2010, Lecture Notes in Computer Science, No. 6531, pp. 430–444, Florida, CA, USA.

In this paper, the substitutability of the indifferentiability framework with non-sequential scheduling is examined by reformulating the framework through applying the Task-PIOA framework, which provides non-sequential activation with oblivious task sequences. First, the indifferentiability framework with non-sequential scheduling is shown to be able to retain the substitutability. Next, this framework is shown to be closely related to the reducibility of systems. Finally, two modelings with sequential scheduling and non-sequential scheduling, respectively, are shown to be mutually inde-

pendent. Thus, the importance of scheduling in the indifferentiability framework is clarified.

Hierarchical ID-based Authenticated Key Exchange Resilient to Ephemeral Key Leakage

A. Fujioka, K. Suzuki, and K. Yoneyama

Proc. of IWSEC 2010, Lecture Notes in Computer Science, No. 6434, pp. 164–180, Kobe, Japan.

In real applications of (public key-based) cryptosystems, hierarchical structures are often used to distribute the workload by delegating key generation. However, there have been few previous studies about such a hierarchical structure in the ID-based authenticated key exchange (AKE) scenario. In this paper, we introduce the first hierarchical ID-based AKE that is resilient to ephemeral secret key leakage. We provide a formal security model for hierarchical ID-based AKE. Our model is based on eCK security to guarantee resistance to leakage of ephemeral secret keys. We also propose an eCK-secure hierarchical ID-based AKE protocol based on a hierarchical ID-based encryption.

Universally Composable NBAC-based Fair Voucher Exchange for Mobile Environments

K. Yoneyama, M. Terada, S. Hongo, and K. Ohta

Proc. of IWSEC 2010, Lecture Notes in Computer Science, No. 6434, pp. 42–59, Kobe, Japan.

Fair exchange is an important tool to achieve "fairness" of electronic commerce. Several previous schemes satisfy universally composable security which provides the property of security preservation over complex networks like the Internet. In recent years, as the demand for electronic commerce has increased, fair exchange for electronic vouchers (e.g., electronic tickets and money) to obtain services or contents has been in the spotlight. The definition of fairness for electronic vouchers is different from that for general electronic items (e.g., duplicated use of exchanged electronic vouchers by one user should be prevented). However, although there are universally composable schemes for electronic items, there have been no previous studies for electronic vouchers. In this paper, we introduce a universally composable definition of fair voucher exchange that represents ideal functionality for fair voucher exchange. Also, we prove the equivalence between our universally composable definition and the conventional definition for electronic vouchers. Thus, our formulation of the ideal functionality is justified. Finally, we propose a new fair voucher exchange scheme from non-blocking atomic commitment as a black-box, which satisfies our security definition and is adequate for mobile environments. Because general building blocks are instantiated with known practical ones, our scheme can also be practical because it is implemented without a trusted third party in usual executions.

Enhancement and Stabilization of Hole Concentration of Hydrogen-terminated Diamond Surface Using Ozone Adsorbates

M. Kubovic and M. Kasu

Jpn. J. Appl. Phys. Vol. 49, No. 110208, 2010.

The p-type conductivity of H-terminated diamond surface can be linked to adsorption of a specific gas species on the surface. O_3, NO_2, NO, and SO_2 were identified as adsorbates that induce holes on H-terminated diamond surface. Among them, exposure to O_3 increases hole concentration the most. The increased concentration remains high even after exposure to the gas has stopped, indicating that ozone is the most stable adsorbent. X-ray photospectroscopy spectra of O_3-adsorbed H-terminated diamond surface show partial oxidation of the surface and upward band bending and are very similar to those of NO_2-exposed diamond surfaces.

Arsenic-doped n-type Diamond Grown by Microwave-assisted Plasma Chemical Vapor Deposition

M. Kasu and M. Kubovic

Jpn. J. Appl. Phys. Vol. 49, No. 110209, 2010.

We grew n-type arsenic (As)-doped single-crystal diamond layers using tertiarybutylarsine as an As source. The n-type conduction of the As-doped layers was confirmed both in Hall measurements and from the current–voltage characteristics of the diodes. In the As-doped layers, electron concentration increased with As concentration in the layers. The ionization energy of the As donor decreased from 1.6 to 0.7 eV as As concentration increased from 1×10^{17} to 9×10^{19} cm^{-3}. A diamond p–n junction diode with an n-type As-doped layer exhibited a rectification ratio of ~1000 at ±10 V at room temperature.

Structure of Rat Ultrasonic Vocalizations and Its [*sic*] Relevance to Behavior

N. Takahashi, M. Kashino, and N. Hironaka

PLoS ONE, Vol. 5, No. 11, pp. e14115–14122, 2010.

Rats are known to emit ultrasonic vocalizations (USVs). These USVs have been hypothesized to hold biological meaning, and the relationship between USVs and behavior has been extensively studied. However, most of these studies looked at specific conditions, such as fear-inducing situations and sexual encounters. In the present experiment, the USVs of pairs of rats in ordinary housing conditions were recorded and their features were examined. Three clusters of USVs in the 25-, 40-, and 60-kHz ranges were detected, which roughly corresponded to fighting, feeding, and moving, respectively. We analyzed sequential combinations of two or more clusters using a state transition model. The results revealed a more specific correspondence between the USVs and behaviors, suggesting that rat USV may work as a type of communication tool.

NTT Communication Science Laboratories at TRECVID 2010 Content-based Copy Detection

R. Mukai, T. Kurozumi, K. Hiramatsu, T. Kawanishi, H. Nagano, and K. Kashino

Proc of TRECVID 2010, NIST, Vol. 1, No. 1, pp. 340–349, Gaithersburg, MD, USA.

In this paper, we describe our approaches that were tested in the TRECVID 2010 Content-Based Copy Detection (CBCD) task. We introduce a method consisting of a feature degeneration and sparse feature selection process for video detection tasks, which is highly robust as regards video signal distortion. For audio detection tasks, we adopt a method based on spectral partitioning to cope with additive interfering sounds. Both methods are key techniques for our Robust Media Search (RMS) technology, which has already been deployed for various commercial services. Evaluation results show the effectiveness of our methods.

Diamond/nitride Semiconductor Heterostructure: Growth and Properties

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

Journal of the Surface Science Society of Japan, Vol. 31, No. 12, pp. 657–666, 2010 (in Japanese).

Diamond/III-V nitride semiconductor heterostructure appears promising not only for high-efficiency deep-UV light emitting diodes (LEDs) but also for high output power field-effect transistors (FETs). However, diamond has a diamond crystal structure, while III-V nitride semiconductors have a wurtzite crystal structure. Due to the difference in the crystal structures, single-crystal III-V nitride growth on diamond substrate has been difficult. In this study, we obtained single-crystal aluminum nitride (AlN) (0001) layers on diamond substrates by using the (111) diamond surface orientation and preventing the formation of the interface layer. We revealed the hetero-epitaxial growth mechanism and proposed a model of the atomic arrangement at the diamond/AlN heterointerface. Furthermore, we demonstrated a p-type diamond/n-type AlN heterojunction diode and successfully observed band-edge emission from diamond. In addition, an AlGaN/GaN heterostructure with a two-dimensional electron gas (2DEG) was grown on diamond (111) by using the single-crystal AlN buffer layer.

Fabrication of p-n Junction Diamond Diodes with n-type Arsenic-doped Diamond

M. Kasu and M. Kubovic

MRS Meeting, the Materials Research Society (MRS), Vol. 1, No. 1, p. 1, Boston, MA, USA, 2010.

We achieved n-type diamond doped with arsenic and fabricated p-n junction diodes.

Effect of NO_2 and Its Related Molecules on Increasing Hole Concentration in Hydrogen-terminated Diamond

M. Kasu and M. Kubovic

MRS Meeting, the Materials Research Society (MRS), Vol. 1, No. 1, p. 1, Boston, MA, USA, 2010.

We investigated the increase in hole concentration caused by molecular adsorption.

Strongly Secure Two-pass Attribute-based Authenticated Key Exchange

Kazuki Yoneyama

Proc. of Pairing, Lecture Notes in Computer Science, 2010, Vol. 6487/2010, pp. 147–166, Yamanaka-onsen, Japan.

In this paper, we present a two-party attribute-based authenticated key exchange scheme that is secure in a stronger security model than the previous models. Our strong security model is a natural extension of the eCK model, which is for PKI-based authenticated key exchange, into the attribute-based setting. We prove the security of our scheme under the gap Bilinear Diffie-Hellman assumption. Moreover, while the previous scheme needs a three-pass interaction between parties, our scheme needs only a two-pass interaction. In a practical sense, we can use any string as an attribute in our scheme because the setup algorithm of our scheme does not depend on the number of attribute candidates (i.e., the setup algorithm outputs constant-size parameters).
