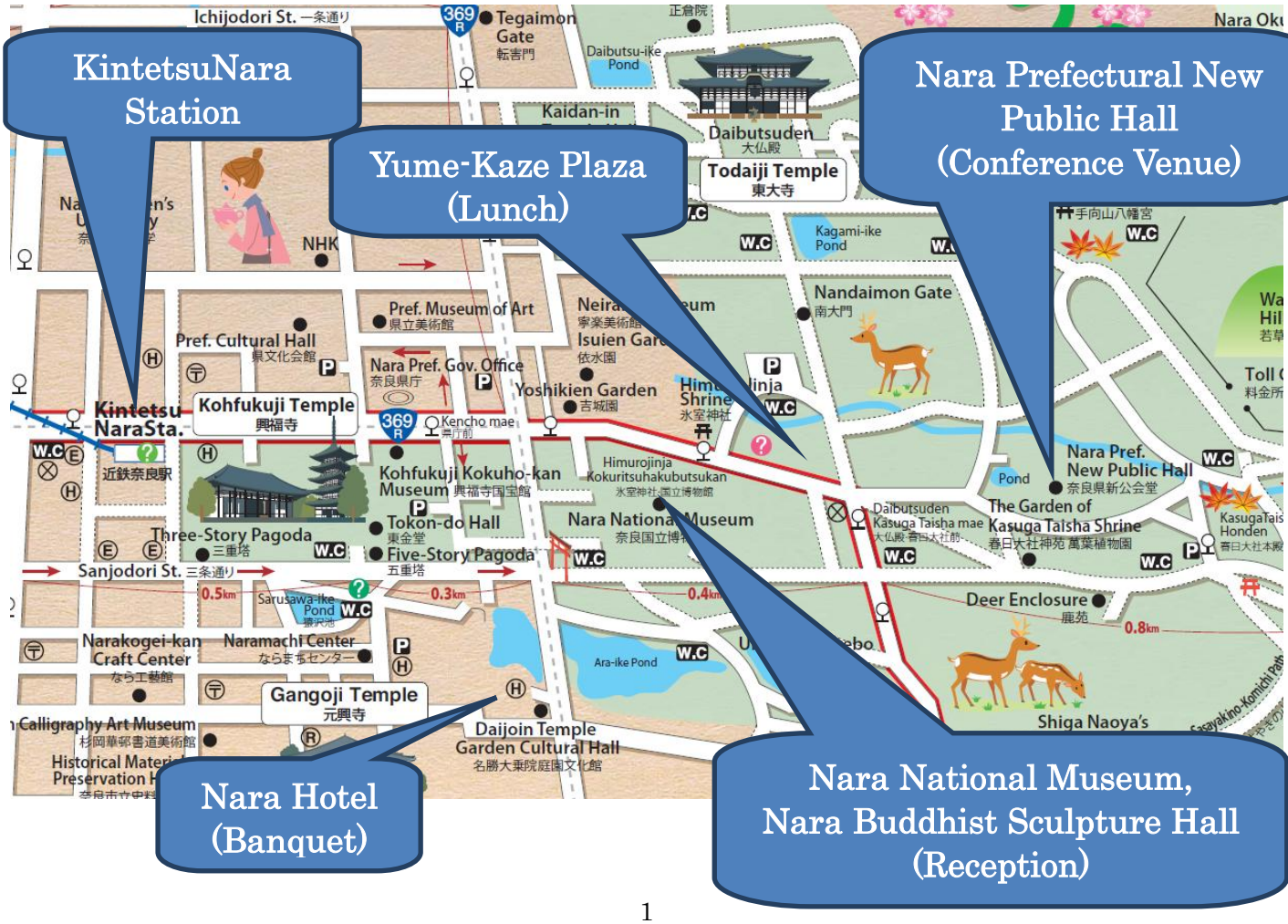
PKC 2013

The 16th International Conference on Practice and Theory in Public-Key Cryptography

Nara, Japan, February 26 - March 1, 2013

Conference Venue/Reception/Lunch/Banquet

Nara Sightseeing MAP provided by Nara City Sightseeing Information Center (http://narashikanko.jp/en/)



PKC 2013 Time Table

Feb. 26 (Tue)		Feb. 27 (Wed)		Feb. 28 (Thu)		Mar. 1 (Fri)	
		8:40-9:10	Registration (Conference Venue)	-9:00	Registration (Conference Venue)	-9:00	Registration (Conference Venue)
		9:10-9:25	Opening	9:00-9:50	Session: **On RSA**	9:00-9:50	Session: **Key Exchange**
		9:25-10:40	Session: **Encryption**	9:50-10:40	Session: **IBE and IPE**	9:50-10:40	Session: **Signature Schemes I**
		10:40-11:00	Coffee Break	10:40-11:00	Coffee Break	10:40-11:00	Coffee Break
		11:00-12:00	**Invited Talk**	11:00-12:00	**Invited Talk**	11:00-12:15	Session: **Homomorphic Encryption**
		12:00-14:00	Lunch (Yume-Kaze Plaza)	12:00-14:00	Lunch (Yume-Kaze Plaza)	12:15-14:00	Lunch (Yume-Kaze Plaza)
		14:00-15:40	Session: **Primitives**	14:00-18:00	Excursion (Bus Tour to Horyu-ji)	14:00-15:40	Session: **Signature Schemes II**
		15:40-16:00	Coffee Break			15:40-16:00	Coffee Break
17:00-18:00	Registration (Nara National Museum) & Free to visit Buddhist Sculpture Hall	16:00-17:15	Session: **Functional Encryption / Signatures**			16:00-17:15	Session: **Protocols**
18:00-20:00	Registration & Reception (Restaurant "Half-Time" at Nara National Museum)			18:00-21:00	Banquet (Nara Hotel)	17:15-17:30	Closing

Program

February 26 (Tue)

17:00-20:00 Registration (You can visit the Buddhist Sculpture Hall (Reserved by PKC) in Nara National Museum until 18:00.)

18:00-20:00 Reception (Restaurant: "葉風泰夢 (Half-Time)")

The registration desk is open during the reception.

February 27 (Wed)

8:40– Registration (Conference Venue, NOT Reception Venue)

9:10–9:25 Opening

9:25–10:40 Encryption

Key Encapsulation Mechanisms from Extractable Hash Proof Systems, Revisited

Takahiro Matsuda (AIST, Japan)

Goichiro Hanaoka (AIST, Japan)

Robust Encryption, Revisited

Pooya Farshim (Darmstadt University of Technology, Germany)

Benoit Libert (Technicolor, France)

Kenneth G. Paterson (Royal Holloway, University of London, UK)

Elizabeth A. Quaglia (ENS, France)

Sender Equivocable Encryption Schemes Secure against Chosen-Ciphertext Attacks Revisited

Zhengan Huang (Shanghai Jiao Tong University, China)

Shengli Liu (Shanghai Jiao Tong University, China)

Baodong Qin (Shanghai Jiao Tong University, China and Southwest University of Science and Technology, China)

10:40–11:00 Coffee Break

11:00–12:00 Invited Talk

Functional Encryption: Origins and Recent Developments

Brent Waters (University of Texas at Austin, USA)

12:00–14:00 Lunch (Yume-Kaze Plaza)

14:00–15:40 Primitives

Vector Commitments and their Applications

Dario Catalano (Università di Catania, Italy)

Dario Fiore (MPI-SWS, Germany)

Efficient, Adaptively Secure, and Composable Oblivious Transfer with a Single, Global CRS

Seung Geol Choi (Columbia University)

Jonathan Katz (University of Maryland)

Hoeteck Wee (George Washington University)

Hong-Sheng Zhou (University of Maryland)

Cryptography Using CAPTCHA Puzzles

Abishek Kumarasubramanian (UCLA, USA)

Rafail Ostrovsky (UCLA, USA)

Omkant Pandey (The University of Texas at Austin, USA)

Akshay Wadia (UCLA, USA)

Improved Zero-knowledge Proofs of Knowledge for the ISIS Problem, and Applications

San Ling (Nanyang Technological University, Singapore)

Khoa Nguyen (Nanyang Technological University, Singapore)

Damien Stehle (ENS, Lyon, France)

Huaxiong Wang (Nanyang Technological University, Singapore)

15:40–16:00 Coffee Break

16:00–17:15 Functional Encryption/Signatures

Decentralized Attribute-Based Signatures

Tatsuaki Okamoto (NTT, Japan)

Katsuyuki Takashima (Mitsubishi Electric, Japan)

On the Semantic Security of Functional Encryption Schemes

Manuel Barbosa (HASLab – INESC TEC and Universidade do Minho, Portugal)

Pooya Farshim (Darmstadt University of Technology, Germany)

Attribute-Based Encryption with Fast Decryption

Susan Hohenberger (Johns Hopkins University, USA)

Brent Waters (University of Texas at Austin, USA)

February 28 (Thu)

9:00–9:50 On RSA

Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors

Noboru Kunihiro (The University of Tokyo, Japan)
Naoyuki Shinohara (NICT, Japan)
Tetsuya Izu (Fujitsu Laboratories, Japan)

Combined Attack on CRT-RSA -- Why Public Verification Must Not Be Public

Guillaume Barbu (Oberthur Technologies, France)
Alberto Battistello (Oberthur Technologies, France)
Guillaume Dabosville (Oberthur Technologies, France)
Christophe Giraud (Oberthur Technologies, France)
Guénaël Renault (Université Paris 6 / LIP6, France)
Soline Renner (Oberthur Technologies and Université Bordeaux 1 / IMB, France)
Rina Zeitoun (Oberthur Technologies and Université Paris 6 / LIP6, France)

9:50–10:40 IBE and IPE

Revocable Identity-Based Encryption Revisited: Security Model and Construction

Jae Hong Seo (NICT, Japan)
Keita Emura (NICT, Japan)

Improved (Hierarchical) Inner-Product Encryption from Lattices

Keita Xagawa (NTT, Japan)

10:40–11:00 Coffee Break

11:00–12:00 Invited Talk

Techniques for Efficient Secure Computation Based on Yao's Protocol

Yehuda Lindell (Bar-Ilan University, Israel)

12:00–14:00 Lunch (Yume-Kaze Plaza)

14:00–18:00 Excursion (Bus Tour: Horyu-ji)

18:00–21:00 Banquet (Nara Hotel)

March 1 (Fri)

9:00–9:50 Key Exchange

Non-Interactive Key Exchange

Eduarda S.V. Freire (Royal Holloway, University of London, UK)
Dennis Hofheinz (Karlsruhe Institute of Technology, Germany)
Eike Kiltz (Ruhr-Universität Bochum, Germany)
Kenneth G. Paterson (Royal Holloway, University of London, UK)

Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages

Fabrice Ben Hamouda (ENS, Paris, France)
Olivier Blazy (Ruhr-Universität Bochum, Germany)
Céline Chevalier (University of Paris II, France)
David Pointcheval (ENS, Paris, France)
Damien Vergnaud (ENS, Paris, France)

9:50–10:40 Signature Schemes I

Tighter Reductions for Forward-Secure Signature Schemes

Michel Abdalla (ENS, Paris, France)
Fabrice Ben Hamouda (ENS, Paris, France)
David Pointcheval (ENS, Paris, France)

Tagged One-Time Signatures: Tight Security and Optimal Tag Size

Masayuki Abe (NTT, Japan)
Bernardo David (University of Brasilia, Brasil)
Markulf Kohlweiss (Microsoft Research, USA)
Ryo Nishimaki (NTT, Japan)
Miyako Ohkubo (NICT, Japan)

10:40–11:00 Coffee Break

11:00–12:15 Homomorphic Encryption

Packed Ciphertexts in LWE-based Homomorphic Encryption

Zvika Brakerski (Stanford University, USA)
Craig Gentry (IBM Research, USA)
Shai Halevi (IBM Research, USA)

Feasibility and Infeasibility of Adaptively Secure Fully Homomorphic Encryption

Jonathan Katz (University of Maryland, USA)
Aishwarya Thiruvengadam (University of Maryland, USA)
Hong-Sheng Zhou (University of Maryland, USA)

Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption

Keita Emura (NICT, Japan)

Goichiro Hanaoka (AIST, Japan)

Go Ohtake (Japan Broadcasting Corporation, Japan)

Takahiro Matsuda (AIST, Japan)

Shota Yamada (The University of Tokyo, Japan)

12:15–14:00 Lunch (Yume-Kaze Plaza)

14:00–15:40 Signature Schemes II

Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures

Nuttapong Attrapadung (AIST, Japan)

Benoit Libert (Technicolor, France)

Thomas Peters (Universite catholique de Louvain, Belgium)

Verifiably Encrypted Signatures with Short Keys based on the Decisional Linear Problem and Obfuscation for Encrypted VES

Ryo Nishimaki (NTT, Japan)

Keita Xagawa (NTT, Japan)

Sequential Aggregate Signatures with Short Public Keys: Design, Analysis and Implementation Studies

Kwangsu Lee (Columbia University, USA)

Dong Hoon Lee (Korea University, Korea))

Moti Yung (Google Inc. and Columbia University, USA)

New Constructions and Applications of Trapdoor DDH Groups

Yannick Seurin (ANSSI, Paris, France)

15:40–16:00 Coffee Break

16:00–17:15 Protocols

Rate-Limited Secure Function Evaluation

Özgür Dagdelen (Technische Universität Darmstadt, Germany)

Payman Mohassel (University of Calgary, Canada)

Daniele Venturi (Aarhus University, Demark)

Verifiable Elections That Scale for Free

Melissa Chase (MSR Redmond, USA)

Markulf Kohlweiss (MSR Cambridge, USA)

Anna Lysyanskaya (Brown University, USA)

Sarah Meiklejohn (UC San Diego, USA)

On the Connection between Leakage Tolerance and Adaptive Security

Jesper Buus Nielsen (Aarhus University, Denmark)

Daniele Venturi (Aarhus University, Denmark)

Angela Zottarel (Aarhus University, Denmark)

17:15–17:30 Closing

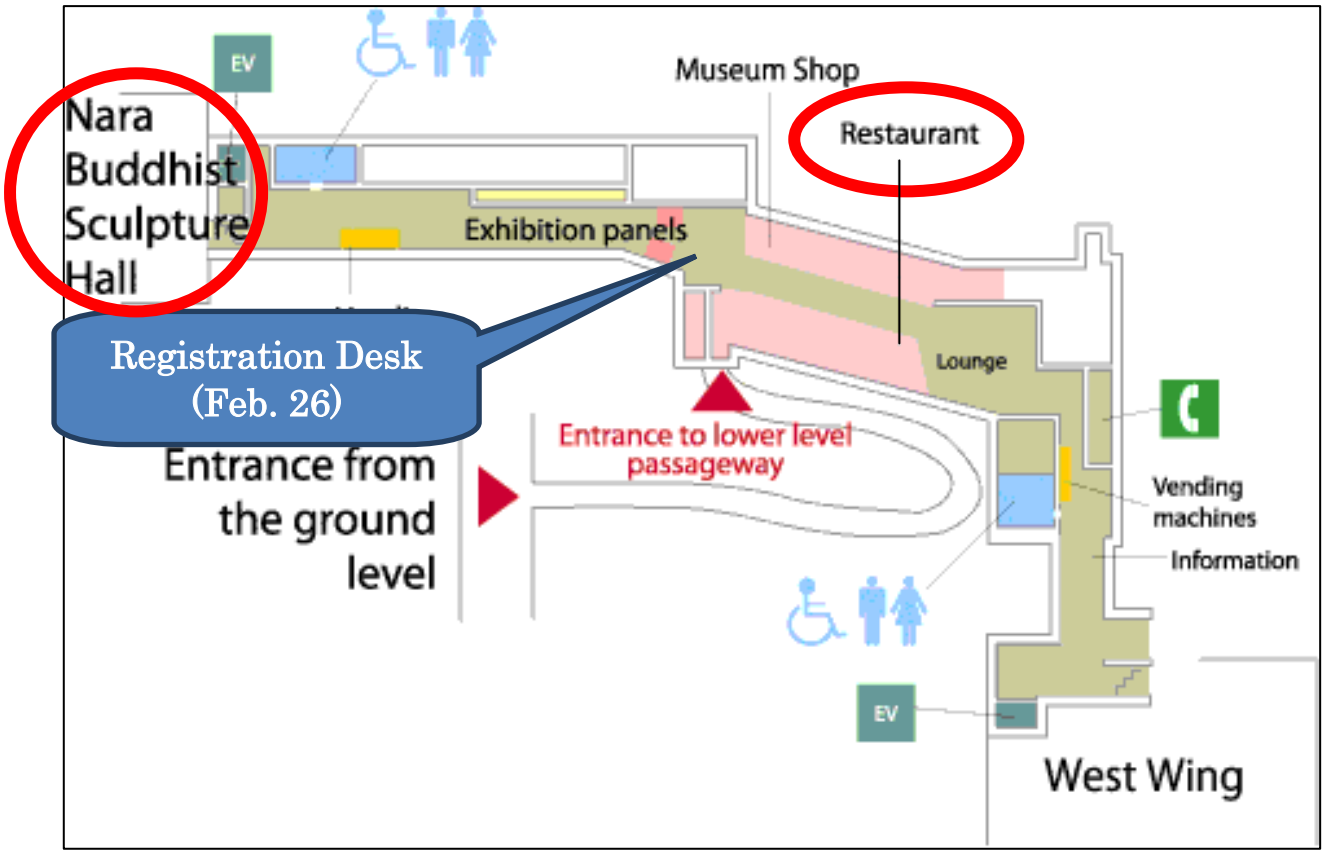
Reception (Nara National Museum)

February 26

17:00-20:00 Registration (You can visit the Buddhist Sculpture Hall (Reserved by PKC) in Nara National Museum until 18:00.)

18:00-20:00 Reception (Restaurant: “葉風泰夢（Half Time)”)

The registration desk is open during the reception.



Note: The registration desk is at Nara National Museum only on February 26.

From February 27 to March1, it is in Nara Prefectural New Public Hall (Conference Venue).

Excursion (Bus Tour: Horyu-ji)

Horyu-ji (法隆寺) is a Buddhist temple in Ikaruga, Nara Prefecture.

The temple's pagoda is widely acknowledged to be one of the oldest existing wooden buildings in the world. In 1993, Horyu-ji was inscribed as a UNESCO World Heritage Site. The Japanese government lists several of its structures, sculptures and artifacts as National Treasures.

February 28 14:00-18:00

Meeting place:

Nara Prefectural New Public Hall (Conference Venue)

Conference Venue (14:00) ➔ (Charter Bus) ➔ Horyu-ji (Tour)

Horyu-ji ➔ (Charter Bus) ➔ Nara Hotel (Banquet place, 18:00)

Banquet (Nara Hotel)

February 28 18:00-21:00

Note: If you are not going on the excursion, please find your own way to Nara Hotel for the banquet.

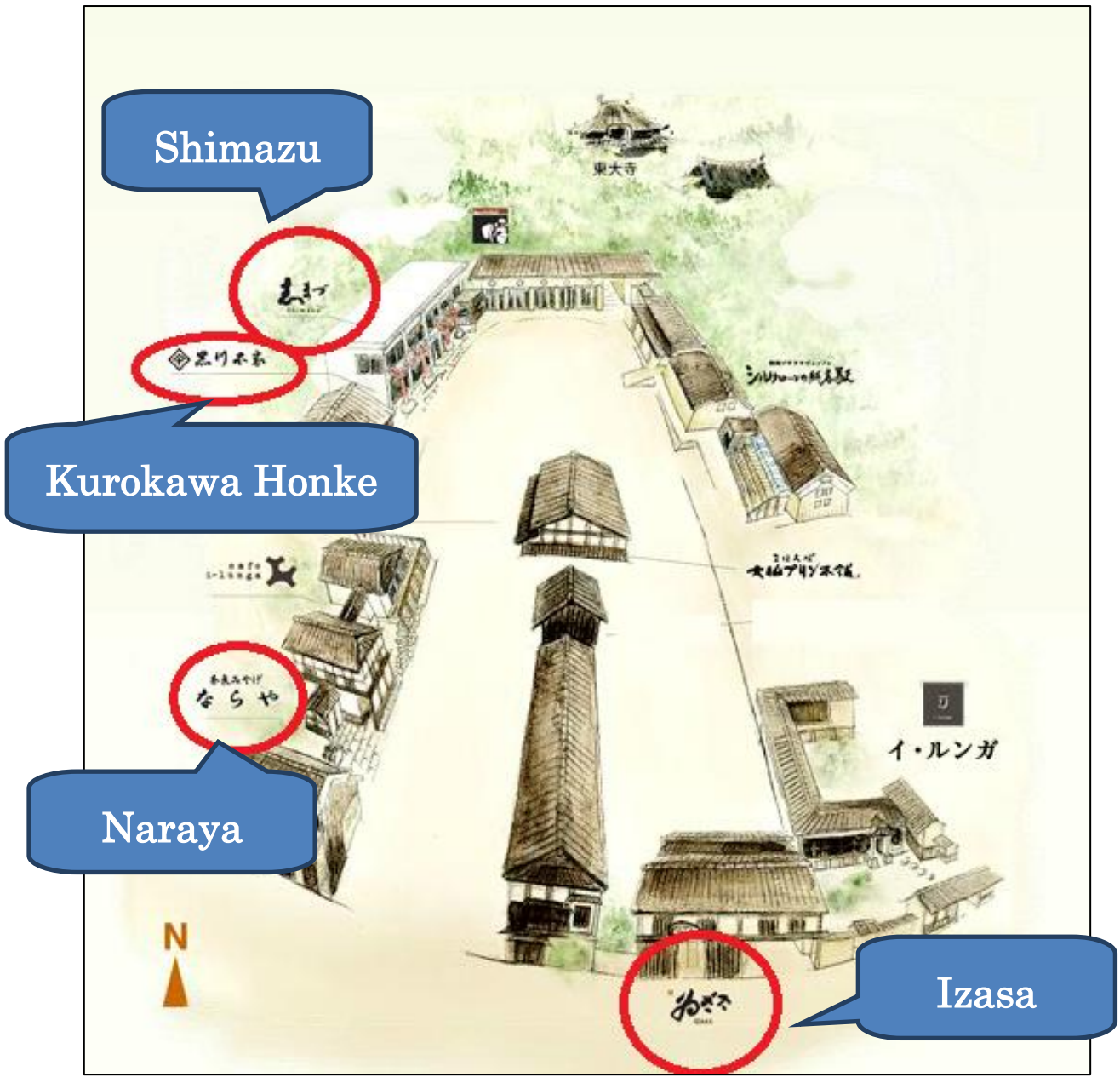
Lunch (Yume-Kaze Plaza)

February 27, 28　12:00-14:00

March 1　12:15-14:00

During PKC 2013, lunch will be served at Yume-Kaze Plaza. There, you can select one of the four restaurants (Shimazu, Izasa, Kurokawa Honke, and Naraya).

Yume-Kaze Plaza



Shimazu

Osaka's time-honored soba buckwheat noodle shop offering delicious soba in Nara. **Vegetarian menu is only available here.**

Izasa

Kakinoha sushi and Izasa sushi, a Nara specialty originating from the food tradition deep in the ancient Yoshino and Kumano mountains.

Kurokawa Honke

Kurokawa Honke, founded in 1615, is the time-honored shop specializing in kudzu (plant producing starch) products in Yoshino mountain area in the southern part of Nara.

Naraya

Nara's souvenirs and tastes are all here for tourists and locals. A number of Nara's original character goods (including Nara's official mascot character, Sento-kun), snacks, accessories and specialties are all under one roof at Naraya.

See Yume-Kaze Plaza Web page: http://www.yume-kaze.com/en.php

PKC2013 Staff

Program Chair

Kaoru Kurosawa, Ibaraki University, Japan

General Chair

Goichiro Hanaoka, AIST, Japan

Local Organizing co-Chairs

Takeshi Chikazawa, IPA, Japan
Ryo Nojima, NICT, Japan

Honorary Chair

Hideki Imai, Chuo University, Japan

Local Organizing Committee

Keita Emura, NICT, Japan
Ryotaro Hayashi, Toshiba, Japan
Atsuo Inomata, NAIST, Japan
Kyoko Karube, AIST, Japan
Noboru Kunihiro, The University of Tokyo, Japan
Takahiro Matsuda, AIST, Japan
Yusuke Naito, Mitsubishi Electric, Japan
Satsuya Ohata, The University of Tokyo, Japan
Kazuo Ohta, The University of Electro-Communications, Japan
Keiko Okada, AIST, Japan
Yusuke Sakai, The University of Electro-Communications, Japan
Kazuo Sakiyama, The University of Electro-Communications, Japan
Akashi Satoh, AIST, Japan
Jacob C. N. Schuldt, Royal Holloway, University of London, UK
Masaya Yasuda, Fujitsu Laboratory Limited, Japan

PKC Financial Sponsors