- Call for Participation -

- The 15th International Conference on Applied Cryptography and Network Security (ACNS2017) - July 10-12 2017, Kanazawa, Japan

Contact: acns2017-organizer@crypto-cybersec.comm.eng.osaka-u.ac.jp

The 15th International Conference on Applied Cryptography and Network Security (ACNS2017) will be held in Kanazawa, Japan in July 2017. It will be co-organized by Osaka University, Japan Advanced Institute of Science and Technology (JAIST), and the Information-technology Promotion Agency (IPA).

ACNS is an annual conference focusing on innovative research and current developments that advance the areas of applied cryptography, cyber security and privacy. Both academic research works with high relevance to real-world problems as well as developments in industrial and technical frontiers fall within the scope of the conference.

Invited Talks:

Dr. Karthikeyan Bhargavan (Research Scientist, Inria Paris)
(an Inria director of research specialised in the security of data exchanges on the Internet)

Title: **Don't Trust, Verify: Towards High-Assurance Cryptographic Software**

Prof. Doug Tygar (Professor of Computer Science & Information, UC Berkeley)

Title: **Adversarial Machine Learning**

Social Event: Social events are planned in the conference. Their details will be announced on the web page.

Registration Fees:

Category	[Early] Until 2017/5/29	[Late] Until 2017/6/28
Regular	JPY 55,000	JPY 70,000
Student	JPY 55,000	JPY 60,000

Conference Organization:

General Chair: Hiroaki Kikuchi (Meiji University, Japan)
Program Co-Chairs: Dieter Gollmann (Hamburg University of Technology, Germany),
Atsuko Miyaji (Osaka University/JAIST, Japan)

Accepted Papers:

Ronghai Yang, Wing Cheong Lau and Shangcheng Shi, *Breaking and Fixing Mobile App Authentication with OAuth2.0-based Protocols*

Cody Freitag, Rishab Goyal, Susan Hohenberger, Venkata Koppula, Eysa Lee, Tatsuaki Okamoto, Jordan Tran and Brent Waters, *Signature Schemes with Randomized Verification*

Alex Biryukov, Daniel Dinu and Yann Le Corre, *Side-Channel Attacks meet Secure Network Protocols*

Olivier Blazy, Céline Chevalier and Paul Germouty, *Almost Optimal Oblivious Transfer from QA-NIZK*

Akshayaram Srinivasan and Chandrasekaran Pandu Rangan, *Efficiently Obfuscating Re-Encryption Program under DDH Assumption*

Erik-Oliver Blass, Travis Mayberry and Guevara Noubir, *Multi-Client Oblivious RAM Secure Against Malicious Servers*

Ralph Ankele, Subhadeep Banik, Avik Chakraborti, Eik List, Florian Mendel, Siang Meng Sim and Gaoli Wang, *Related-Key Impossible-Differential Attack on Reduced-Round SKINNY*

Sze Ling Yeo, Zhen Li, Khoongming Khoo and Yu Bin Low, *An Enhanced Binary Characteristic Set Algorithm and Its Applications to Algebraic Cryptanalysis*

Weizhi Meng, Wenjuan Li, Wang Hao Lee, Lijun Jiang and Jianying Zhou, *A Pilot Study of Multiple Password Interference between Text and Map-based Passwords*

Dan Boneh, Sam Kim and Valeria Nikolaenko, *Lattice-based DAPS and Generalizations: Self-Enforcement in Signature Schemes*

Kaoru Kurosawa and Rie Habuka, *More Efficient Construction of Bounded KDM Secure Encryption*

Britta Hale, Tibor Jager, Sebastian Lauer and Jorg Schwenk, *Simple Security Definitions for and Constructions of 0-RTT Key Exchange*
David Bernhard, Ngoc Khanh Nguyen and Bogdan Warinschi, *Adaptive Proofs have Straightline Extractors (in the Random Oracle Model)*

Daniel Demmler, Marco Holz and Thomas Schneider, *OnionPIR: Effective Protection of Sensitive Metadata in Online Communication Networks*

Marco Cianfriglia, Stefano Guarino, Massimo Bernaschi, Flavio Lombardi and Marco Pedicini, *A Novel GPU-Based Implementation of the Cube Attack - Preliminary Results Against Trivium*

Authors: Bruce Berg, Tyler Kaczmarek, Alfred Kobsa and Gene Tsudik, *Lights, Camera, Action! Exploring Effects of Visual Distractions on Completion of Security Tasks*

David Chaum, Debajyoti Das, Farid Javani, Aniket Kate, Anna Krasnova, Joeri De Ruiter and Alan T. Sherman, *cMix : Mixing with Minimal Real-Time Asymmetric Cryptographic Operations*

Xiaopeng Li, Wenyuan Xu, Song Wang and Xianshan Qu, *Are You Lying: Validating the Time-Location of Outdoor Images*

Rui Xu, Yeo Sze Ling, Kazuhide Fukushima, Tsuyoshi Takagi, Seo Hwajung, Shinsaku Kiyomoto and Henricksen Matt, *An experimental study of the BDD approach for the search LWE problem*

Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk and Jiayu Xu, *TOPPSS: Cost-minimal Password-Protected Secret Sharing based on Threshold OPRF*

San Ling, Khoa Nguyen, Huaxiong Wang and Yanhong Xu, *Lattice-Based Group Signatures: Achieving Full Dynamicity with Ease*

Chenyang Tu, Lingchen Zhang, Zeyi Liu, Neng Gao and Yuan Ma, *A Practical Chosen Message Power Analysis Approach against Ciphers with the Key Whitening Layers*

Yutaro Kiyomura, Akiko Inoue, Yuto Kawahara, Masaya Yasuda, Tsuyoshi Takagi and Tetsutaro Kobayashi, *Secure and Efficient Pairing at 256-bit Security Level*

Riccardo Spolaor, Laila Abudahi, Veelasha Moonsamy, Mauro Conti and Radha Poovendran, *No Free Charge Theorem: a Covert Channel via USB Charging Cable on Mobile Devices*

John Henry Castellanos, Daniele Antonioli, Nils Ole Tippenhauer and Mart?n Ochoa, *Legacy-Compliant Data Authentication for Industrial Control System Traffic*

Jason Ying and Noboru Kunihiro, *Bounds in Various Generalized Settings of the Discrete Logarithm Problem*

Claude Carlet, Annelie Heuser and Stjepan Picek, *Trade-offs for S-boxes: Cryptographic Properties and Side-channel Resilience*

Russell W. F. Lai and Sherman S. M. Chow, *Forward-Secure Searchable Encryption on Labeled Bipartite Graphs*

Ignacio Cascudo and Bernardo M. David, *SCRAPE: Scalable Randomness Attested by Public Entities*

Matteo Maffei, Giulio Malavolta, Manuel Reinert and Dominique Schroeder, *Maliciously Secure Multi-Client ORAM*

Carlos Aguilar-Melchor, Martin Albrecht and Thomas Ricosset, *Sampling From Arbitrary Centered Discrete Gaussians For Lattice-Based Cryptography*

Yi-Ruei Chen and Wen-Guey Tzeng, *Legacy-Compliant Data Authentication for Industrial Control System Traffic*

Giuseppe Ateniese, Michael Goodrich, Vassilios Lekakis, Charalampos Papamanthou, Evripidis Paraskevas and Roberto Tamassia, *Accountable Storage*

Marcel Keller, Emmanuela Orsini, Dragos Rotaru, Peter Scholl, Eduardo Soria-Vazquez and Srinivas Vivek, *Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables*

Conference Venue: Kanazawa is one of the most historical cities in Japan. It is famous for Kenrokuen Garden and Kanazawa Castle Park. In particular, Kenrokuen Garden is one of the three greatest gardens in Japan. The conference venue is next to these two places. It is located at the most beautiful area in Kanazawa. The conference venue is located approximately 3 kilometers south of Kanazawa Station.

Travel Information: The conference venue is located approximately 3 kilometers south of Kanazawa Station.

From Overseas:

- **Narita International Airport (code NRT)**: It is the most convenient airport to get to Japan from overseas. You can get to Kanazawa via Komatsu Airport. There is an evening flight from Narita Int'l Airport to Komatsu Airport. It will take about an hour.
- **Haneda Airport (code HND)**: There are some international flights from overseas to Haneda Airport. It is convenient to get to Kanazawa via Komatsu Airport or Shinkansen.
- **Kansai International Airport (code KIX)**: There are also some international flights from overseas to Kansai Airport. It is convenient to get to Kanazawa by taking JR (Japan Railway) via Shin-Osaka Station. It will take about 3.5 to 4 hours by Special Express 'Haruka' from Kansai Int'l Airport to Shin-Osaka Station and Special Express 'Thunderbird' or 'Raicho' from Shin-Osaka Station to Kanazawa Station. There are about two services per an hour. The cost will be about 10,000JPY.
- **Komatsu Airport (code KMQ)**: It is the nearest airport to Kanazawa. There are some international flights from Seoul, Shanghai, and Taipei to Komatsu Airport. Airport limousine bus shuttles are available from Komatsu Airport to Kanazawa Station. It will take less than an hour, and the cost will be 1,130JPY.

From Tokyo Area:

- **By train (Shinkansen)**: You can get to Kanazawa Station from Tokyo Station by Hokuriku Shinkansen operated by JR (Japan Railway). There are 24 services everyday, and the cost will be about 14,000JPY. 'Kagayaki' is express type and takes 2 hours and a half. 'Hakutaka' is multi-stop type and takes about 3 hours.
- **By airplain**: You can get to Kanazawa from Narita or Haneda Airport via Komatsu Airport. There is an evening flight from Narita Int'l Airport to Komatsu Airport. It will take about an hour. There are about ten flights from Haneda Airport to Komatsu Airport everyday. It will take about an hour. From Komatsu Airport to Kanazawa Station, airport limousine bus shuttles are available. It will take less than an hour, and the cost will be 1,130JPY.
- **From Kansai (Kyoto, Osaka, Kobe) Area**: It is recommended to get to Kanazawa Station by JR (Japan Railway). It will take about 2 hours by Special Express 'Thunderbird' from Osaka Station to Kanazawa Station. There are about two services per an hour. The cost will be about 6,000JPY. Kyoto is on the way. The cost will be about 5,000JPY from Kyoto Station.

Sponsored by: National Insitute of Information and Communications Technology (NICT) International Exchange Program, Mitsubishi Electric Corporation, Support Center for Advanced Telecommunications Technology Research, Foundation, Microsoft Corporation, Fujitsu Hokuriku Systems Limited, Nippon Telegraph and Telephone Corporation (NTT), and Hokuriku Telecommunication Network Co.,Inc..

(Last Update: July 7, 2017)