ASIACRYPT 2009 Program (updated 11/27)

All sessions and welcome reception are held at **Hitotsubashi Memorial Hall**, 2nd floor of National Center of Sciences Building. The building opens 8:30 in the morning everyday. Please have your registration confirmation letter or conference badge with you, which is needed to enter the building.

Sunday, December 6

17:30-20:30: Registration
18:30-20:30: Welcome Reception

Monday, December 7

08:40 Registration
09:10-09:20 Welcome and Opening Remarks

09:20-10:35 Session 1 – Block Ciphers (Chair: Orr Dunkelman)

- Related-key Cryptanalysis of the Full AES-192 and AES-256
  Alex Biryukov and Dmitry Khovratovich
- The Key-Dependent Attack on Block Ciphers
  Xiaorui Sun and Xuejia Lai
- Cascade Encryption Revisited
  Peter Gaži and Ueli Maurer

10:35-10:55 Morning Break

10:55-12:10 Session 2 – Quantum and Post-Quantum (Chair: Serge Fehr)

- Quantum-Secure Coin-Flipping and Applications
  Ivan Damgård and Carolin Lunemann
- On the Power of Two-Party Quantum Cryptography
  Louis Salvail, Christian Schaffner and Miroslava Sotáková
- Security Bounds for the Design of Code-based Cryptosystems
  Matthieu Finiasz and Nicolas Sendrier

12:10-13:40 Lunch, Gakushi Kaikan

13:40-15:20 Session 3 – Hash Functions I (Chair: Josef Pieprzyk)

- Rebound Attack on the Full LANE Compression Function
  Krystian Matusiewicz, María Naya-Plasencia, Ivica Nikolić, Yu Sasaki and Martin Schläffer
- Rebound Distinguishers: Results on the Full Whirlpool Compression Function
  Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen and Martin Schläffer
- MD5 is Weaker than Weak: Attacks on Concatenated Combiners
  Florian Mendel, Christian Rechberger and Martin Schläffer
- The Intel AES Instructions Set and the SHA-3 Candidates
  Ryad Benadjila, Olivier Billet, Shay Gueron and Matt Robshaw

15:20-15:40 Afternoon Break

15:40-17:20 Session 4 – Encryption Schemes (Chair: Rei Safavi-Naini)

- Group Encryption: Non-Interactive Realization in the Standard Model
  Julien Cathalo, Benoît Libert and Moti Yung
- On Black-Box Constructions of Predicate Encryption from Trapdoor Permutations
  Jonathan Katz and Arkady Yerukhimovich
- Hierarchical Predicate Encryption for Inner-Products
  Tatsuaki Okamoto and Katsuyuki Takashima
- Hedged Public-Key Encryption: How to Protect Against Bad Randomness
  Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham and Scott Yilek

18:30-20:00 Rump Session (Chair: Shiho Moriai)

Tuesday, December 8

08:40 Registration

09:10-10:25 Session 5 – Multi Party Computation (Chair: Masayuki Abe)

- Secure Two-Party Computation is Practical
  Benny Pinkas, Thomas Schneider, Nigel P. Smart and Stephen C. Williams
- Secure Multi-party Computation Minimizing Online Rounds
  Seung Geol Choi, Ariel Elbaz, Tal Malkin and Moti Yung
- Improved Non-Committing Encryption with Applications to Adaptively Secure Protocols
  Seung Geol Choi, Dana Dachman-Soled, Tal Malkin and Hoeteck Wee

10:25-10:45 Morning Break

10:45-12:00 Session 6 – Cryptographic Protocols (Chair: Atsushi Fujioka)

- Non-Malleable Statistically Hiding Commitment from Any One-Way Function
  Zongyang Zhang, Zhenfu Cao, Ning Ding and Rong Ma
- Proofs of Storage from Homomorphic Identification Protocols
  Giuseppe Ateniese, Seny Kamara and Jonathan Katz
- Simple Adaptive Oblivious Transfer Without Random Oracle
  Kaoru Kurosawa and Ryo Nojima

12:00-13:30 Lunch, Gakushi Kaikan

Wednesday, December 9

08:40 Registration

09:10-10:25 Session 7 – Hash Functions II (Chair: Tetsu Iwata)

- Improved generic algorithms for 3-collisions
  Antoine Joux and Stefan Lucks

- A Modular Design for Hash Functions: Towards Making the Mix-Compress-Mix Approach Practical
  Anja Lehmann and Stefano Tessaro

- How to Confirm Cryptosystems Security: The Original Merkle-Damgård is Still Alive!
  Yusuke Naito, Kazuki Yoneyama, Lei Wang and Kazuo Ohta

10:25-10:45 Morning Break

10:45-12:00 Session 8 – Models and Frameworks I (Chair: Ivan Visconti)

- On the Analysis of Cryptographic Assumptions in the Generic Ring Model
  Tibor Jager and Jörg Schwenk

- Zero Knowledge in the Random Oracle Model, Revisited
  Hoeteck Wee

- A Framework for Universally Composable Non-Committing Blind Signatures
  Masayuki Abe and Miyako Ohkubo

12:00-13:30 Lunch, Gakushi Kaikan

13:30-14:45 Session 9 – Cryptanalysis: Square and Quadratic (Chair: Jun Furukawa)

- Cryptanalysis of the Square Cryptosystems
  Olivier Billet and Gilles Macario-Rat (Yannick Seurin gives the talk)

- Factoring pq^2 with Quadratic Forms: Nice Cryptanalyses
  Guilhem Castagnos, Antoine Joux, Fabien Laguillaumie and Phong Q. Nguyen

- Attacking Power Generators Using Unravelled Linearization: When Do We Output Too Much?
  Mathias Herrmann and Alexander May

14:45-15:05 Afternoon Break

15:05-15:55 Session 10 – Models and Frameworks II (Chair: Serge Vaudenay)

- Security Notions and Generic Constructions for Client Puzzles
  Liqun Chen, Paul Morrissey, Nigel P. Smart and Bogdan Warinschi

- Foundations of Non-Malleable Hash and One-Way Functions
  Alexandra Boldyreva, David Cash, Marc Fischlin and Bogdan Warinschi

16:00-17:00 IACR Distinguished Lecture (Chair: Bart Preneel)

- A New Approach on Bilinear Pairings and Its Applications
  Tatsuaki Okamoto

17:00-18:00 IACR Business Meeting

19:00-21:00 Banquet, Meiji Kinenkan
(Shuttle buses to/from the banquet venue available)

Thursday, December 10

08:40 Registration

09:10-10:25 Session 11 – Hash Functions III (Chair: Xuejia Lai)

- Improved Cryptanalysis of Skein
  Jean-Philippe Aumasson, Çağdaş Çalık, Willi Meier, Onur Özen, Raphael C.-W. Phan and Kerem Varıcı

- Linearization Framework for Collision Attacks: Application to CubeHash and MD6
  Eric Brier, Shahram Khazaei, Willi Meier and Thomas Peyrin

- Preimages for Step-Reduced SHA-2
  Kazumaro Aoki, Jian Guo, Krystian Matusiewicz, Yu Sasaki and Lei Wang

10:25-10:45 Morning Break

10:45-12:00 Session 12 – Lattice-Based (Chair: Phong Nguyen)

- Fiat-Shamir With Aborts: Applications to Lattice and Factoring-Based Signatures
  Vadim Lyubashevsky

- Efficient Public Key Encryption Based on Ideal Lattices
  Damien Stehlé, Ron Steinfeld, Keisuke Tanaka and Keita Xagawa

- Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices
  Jonathan Katz and Vinod Vaikuntanathan

12:00-13:30 Lunch, Gakushi Kaikan

13:30-15:10 Session 13 – Side Channels (Chair: Goichiro Hanaoka)

- PSS is Secure against Random Fault Attacks
  Jean-Sébastien Coron and Avradip Mandal

- Cache-Timing Template Attacks
  Billy Bob Brumley and Risto M. Hakala

- Memory Leakage-Resilient Encryption based on Physically Unclonable Functions
  Frederik Armknecht, Roel Maes, Ahmad-Reza Sadegh, Berk Sunar and Pim Tuyls

- Signature Schemes with Bounded Leakage Resilience
  Jonathan Katz and Vinod Vaikuntanathan

15:10-15:20 Sayonara