Asiacrypt 2019 Program

Sunday, December 08, 2019	
17:00–20:00	**Registration**
18:00–20:00	**Welcome Reception** Location: OWADA

<table>
<tr><th colspan="3">Monday, December 09, 2019</th></tr>
<tr><td><b>8:00-</b></td><td colspan="2"><b>Registration</b></td></tr>
<tr><td><b>9:00–9:10</b></td><td colspan="2"><b>Opening Remarks</b>
Location: KAIRAKU 1&2</td></tr>
<tr><td><b>9:10–10:00</b></td><td colspan="2"><b>Invited Lecture 1</b>
Location: KAIRAKU 1&2
Chair: TBD
<b>New proof systems for sustainable blockchains: proofs of space and verifiable delay functions</b>
Krzysztof Pietrzak
<i>IST Austria</i></td></tr>
<tr><td><b>10:00–10:25</b></td><td colspan="2"><b>Best Paper</b>
Location: KAIRAKU 1&2
Chair: TBD
<b>Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes</b>
Thomas Debris-Alazard; Nicolas Sendrier; Jean-Pierre Tillich
<i>Inria de Paris; Inria de Paris; Inria de Paris</i></td></tr>
<tr><td><b>10:25–10:50</b></td><td colspan="2"><b>Coffee Break</b></td></tr>
<tr><td><b>10:50–12:05</b></td><td><b>Lattices (1)</b>
Location: KAIRAKU 1&2
Chair: TBD
<b>Middle-Product Learning with Rounding Problem and its Applications</b>
Shi Bai; Katharina Boudgoust; Dipayan Das; Adeline Roux-Langlois; Weiqiang Wen; Zhenfei Zhang
<i>Department of Mathematical Sciences, Florida Atlantic University; Univ Rennes, CNRS, IRISA; Department of Mathematics, National Institute of Technology, Durgapur; Univ Rennes, CNRS, IRISA; Univ Rennes, CNRS, IRISA; Algorand</i>
<b>A Novel CCA Attack using Decryption Errors against LAC</b>
Qian Guo; Thomas Johansson; Jing Yang
<i>University of Bergen, Norway, and Lund University, Sweden; Lund University, Sweden; Lund University, Sweden</i>
<b>Towards Attribute-Based Encryption for RAMs from LWE: Sub-linear Decryption, and More</b>
Prabhanjan Ananth; Xiong Fan; Elaine Shi
<i>MIT; Cornell University; Cornell University</i></td><td><b>Symmetric Cryptography (1)</b>
Location: KAIRAKU 3
Chair: TBD
<b>4-Round Luby-Rackoff Construction is a qPRP</b>
Akinori Hosoyamada; Tetsu Iwata
<i>NTT Secure Platform Laboratories and Nagoya University; Nagoya University</i>
<b>Indifferentiability of Truncated Random Permutations</b>
Wonseok Choi; Byeonghak Lee; Jooyoung Lee
<i>KAIST, Korea; KAIST, Korea; KAIST, Korea</i>
<b>Anomalies and Vector Space Search: Tools for S-Box Analysis</b>
Xavier Bonnetain; Léo Perrin; Shizhu Tian
<i>Inria, Sorbonne University; Inria; Inria, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences</i></td></tr>
<tr><td><b>12:05–13:45</b></td><td colspan="2"><b>Lunch (Buffet)</b></td></tr>
</table>

Monday, December 09, 2019		
13:45–15:00	**Isogenies (1)** Location: KAIRAKU 1 Chair: TBD **CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations** Ward Beullens; Thorsten Kleinjung; Fréderik Vercauteren *ESAT-COSIC, KU Leuven; EPFL IC LACAL; ESAT-COSIC, KU Leuven* **Verifiable Delay Functions from Supersingular Isogenies and Pairings** Luca De Feo; Simon Masson; Christophe Petit; Antonio Sanso *Université Paris-Saclay – UVSQ, LMV, UMR CNRS 8100, Versailles; Thales and Université de Lorraine; University of Birmingham; Adobe Inc. and Ruhr Universität Bochum* **Strongly Secure Authenticated Key Exchange from Supersingular Isogenies** Xiu Xu; Haiyang Xue; Kunpeng Wang; Man Ho Au; Song Tian *IIE, Chinese Academy of Sciences; IIE, Chinese Academy of Sciences, The Hong Kong Polytechnic University; IIE, Chinese Academy of Sciences; The Hong Kong Polytechnic University; IIE, Chinese Academy of Sciences*	**Obfuscation** Location: KAIRAKU 2 Chair: TBD **Dual-Mode NIZKs from Obfuscation** Dennis Hofheinz, Bogdan Ursu *Karlsruhe Institute of Technology (KIT); Karlsruhe Institute of Technology (KIT)* **Output Compression, MPC, and iO for Turing Machines** Saikrishna Badrinarayanan; Rex Fernando; Venkata Koppula; Amit Sahai; Brent Waters *UCLA; UCLA; Weizmann Institute of Science; UCLA; UT Austin* **Collusion Resistant Watermarking Schemes for Cryptographic Functionalities** Rupeng Yang; Man Ho Au; Junzuo Lai; Qiuliang Xu; Zuoxia Yu *School of Computer Science and Technology, Shandong University & Department of Computing, The Hong Kong Polytechnic University; Department of Computing, The Hong Kong Polytechnic University; College of Information Science and Technology, Jinan University; School of Software, Shandong University; Department of Computing, The Hong Kong Polytechnic University*
15:00–15:25	**Coffee Break**	
15:25–17:05	**Multiparty Computation (1)** Location: KAIRAKU 1 Chair: TBD **Valiant’s Universal Circuits Revisited: an Overall Improvement and a Lower Bound** Shuoyao Zhao; Yu Yu; Jiang Zhang; Hanlin Liu *Shanghai Jiao Tong University and PlatON Network; Shanghai Jiao Tong University; State Key Laboratory of Cryptology; Shanghai Jiao Tong University* **The Broadcast Message Complexity of Secure Multiparty Computation** Sanjam Garg; Aarushi Goel; Abhishek Jain *University of California, Berkeley; Johns Hopkins University; Johns Hopkins University* **Beyond Honest Majority: The Round Complexity of Fair and Robust Multi-party Computation** Arpita Patra; Divya Ravi *Indian Institute of Science; Indian Institute of Science* **Efficient UC Commitment Extension with Homomorphism for Free (and Applications)** Ignacio Cascudo; Ivan Damgård; Bernardo David; Nico Döttling; Rafael Dowsley; Irene Giacomelli *IMDEA Software Institute; Aarhus University; IT University of Copenhagen; Cispa Helmholtz Center for Information Security; Bar-Ilan University; Protocol Labs, Inc.*	**Quantum** Location: KAIRAKU 2 Chair: TBD **Quantum Algorithms for the Approximate k-List Problem and their Application to Lattice Sieving** Elena Kirshanova; Erik Mårtensson; Eamonn W. Postlethwaite; Subhayan Roy Moulik *I. Kant Baltic Federal University; Lund University; Royal Holloway, University of London; University of Oxford* **Quantum Attacks without Superposition Queries: the Offline Simon's Algorithm** Xavier Bonnetain; Akinori Hosoyamada; María Naya-Plasencia; Yu Sasaki; André Schrottenloher *Sorbonne Université, Inria, France; NTT Secure Platform Laboratories, Nagoya University, Japan; Inria, France; NTT Secure Platform Laboratories, Japan; Inria, France* **Quantum Random Oracle Model with Auxiliary Input** Minki Hhan; Keita Xagawa; Takashi Yamakawa *Seoul National University, Republic of Korea; NTT Secure Platform Laboratories, Japan; NTT Secure Platform Laboratories, Japan* **QFactory: classically-instructed remote secret qubits preparation** Alexandru Cojocaru; Léo Colisson; Elham Kashefi; Petros Wallden *University of Edinburgh; Sorbonne Université; University of Edinburgh, Sorbonne Université; University of Edinburgh*
17:05–17:10	**Track-switch Time**	

Monday, December 09, 2019		
17:10–18:00	**E-cash and blockchain** Location: KAIRAKU 1 Chair: TBD **Quisquis: A New Design for Anonymous Cryptocurrencies** Prastudy Fauzi; Sarah Meiklejohn; Rebekah Mercer; Claudio Orlandi *Simula UiB, Norway; University College London, UK; O(1) Labs, USA; Aarhus University, Denmark* **Divisible E-Cash from Constrained Pseudo-Random Functions** Florian Bourse; David Pointcheval; Olivier Sanders *Orange Labs; ENS, CNRS, PSL University and INRIA; Orange Labs*	**Codes** Location: KAIRAKU 2 Chair: TBD **Collision Resistant Hashing from Sub-exponential Learning Parity with Noise** Yu Yu; Jiang Zhang; Jian Weng; Chun Guo; Xiangxue Li *Shanghai Jiao Tong University; State Key Laboratory of Cryptology; Jinan University; Shandong University; East China Normal University* **New Code-Based Privacy-Preserving Cryptographic Constructions** Khoa Nguyen; Hanh Tang; Huaxiong Wang; Neng Zeng *Nanyang Technological University; Nanyang Technological University; Nanyang Technological University; Nanyang Technological University*

Tuesday, December 10, 2019		
8:00-	**Registration**	
9:00–10:15	**Lattices (2)** Location: KAIRAKU 1 Chair: TBD **An LLL Algorithm for Module Lattices** Changmin Lee; Alice Pellet-Mary; Damien Stehlé; Alexandre Wallet *Univ. Lyon, EnsL, UCBL, CNRS, Inria, LIP; Univ. Lyon, EnsL, UCBL, CNRS, Inria, LIP; Univ. Lyon, EnsL, UCBL, CNRS, Inria, LIP; NTT Secure Platform Laboratories, Tokyo, Japan* **Order-LWE and the Hardness of Ring-LWE with Entropic Secrets** Madalina Bolboceanu; Zvika Brakerski; Renen Perlman; Devika Sharma *Bitdefender; Weizmann Institute of Science; Weizmann Institute of Science; Weizmann Institute of Science* **On the Non-Existence of Short Vectors in Random Module Lattices** Ngoc Khanh Nguyen *IBM Research Zurich and Ruhr Universitat Bochum*	**Authenticated Encryption** Location: KAIRAKU 2 Chair: TBD **Forkcipher: a New Primitive for Authenticated Encryption of Very Short Messages** Elena Andreeva; Virginie Lallemand; Antoon Purnal; Reza Reyhanitabar; Arnab Roy; Damian Vizár *COSIC, KU Leuven, Belgium; University of Lorraine, CNRS, Inria, LORIA, France; COSIC, KU Leuven, Belgium; TE Connectivity, Germany; University of Bristol, UK; CSEM, Switzerland* **Anonymous AE** John Chan; Phillip Rogaway *University of California, Davis; University of California, Davis* **Sponges Resist Leakage: The Case of Authenticated Encryption** Jean Paul Degabriele; Christian Janson; Patrick Struck *TU Darmstadt; TU Darmstadt; TU Darmstadt*
10:15–10:45	**Coffee Break**	
10:45–12:00	**Isogenies (2)** Location: KAIRAKU 1 Chair: TBD **Dual Isogenies and Their Application to Public-key Compression for Isogeny-based Cryptography** Michael Naehrig; Joost Renes *Microsoft Research; Radboud University* **Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves** Suhri Kim; Kisoon Yoon; Young-Ho Park; Seokhie Hong *Center for Information Security Technologies (CIST), Korea University, Seoul, Republic of Korea; NSHC Inc., Uiwang, Republic of Korea; Sejong Cyber University, Seoul, Republic of Korea; Center for Information Security Technologies (CIST), Korea University, Seoul, Republic of Korea* **Hard Isogeny Problems over RSA Moduli and Groups with Infeasible Inversion** Salim Ali Altuğ; Yilei Chen *Boston University; Visa Research*	**Multilinear Maps** Location: KAIRAKU 2 Chair: TBD **On Kilian's Randomization of Multilinear Map Encodings** Jean-Sébastien Coron; Hilder Vitor Lima Pereira *University of Luxembourg; University of Luxembourg* **Cryptanalysis of CLT13 Multilinear Maps with Independent Slots** Jean-Sébastien Coron; Luca Notarnicola *University of Luxembourg; University of Luxembourg* **XOR-RKA Secure Pseudorandom Function from Post-Zeroizing Multilinear Maps** Michel Abdalla; Fabrice Benhamouda; Alain Passelègue *CNRS, ENS, PSL, Inria; Algorand Foundation; Inria, ENS Lyon*
12:00–13:40	**Lunch (Bento)**	

Tuesday, December 10, 2019

13:40–18:30	**Free afternoon**	
18:30–21:30	**Rump Session with Buffet** Location: KAIRAKU 1&2	

Wednesday, December 11, 2019

8:00-	**Registration**	
9:00–10:15	**Homomorphic Encryption** Location: KAIRAKU 1 Chair: TBD **Numerical Method for Comparison on Homomorphically Encrypted Numbers** Jung Hee Cheon; Dongwoo Kim; Duhyeong Kim; Hun Hee Lee; Keewoo Lee *Seoul National University; Seoul National University; Seoul National University; Seoul National University; Seoul National University* **Multi-Key Homomophic Encryption from TFHE** Hao Chen; Ilaria Chillotti; Yongsoo Song *Microsoft Research, Redmond; KU Leuven; Microsoft Research, Redmond* **Homomorphic Encryption for Finite Automata** Nicholas Genise; Craig Gentry; Shai Halevi; Baiyu Li; Daniele Micciancio *Rutgers University; Algorand Foundation; Algorand Foundation; UCSD; UCSD*	**Combinatorial Cryptography** Location: KAIRAKU 2 Chair: TBD **Efficient Explicit Constructions of Multipartite Secret Sharing Schemes** Qi Chen; Chunming Tang; Zhiqiang Lin *Advanced Institute of Engineering Science for Intelligent Manufacturing, Guangzhou University, China; College of Mathematics and Information Science, Guangzhou University, China; College of Mathematics and Information Science, Guangzhou University, China* **Perfectly Secure Oblivious RAM with Sublinear Bandwidth Overhead** Michael Raskin; Mark Simkin *Technical University of Munich; Aarhus University* **How to Correct Errors in Multi-Server PIR** Kaoru Kurosawa *Ibaraki University*
10:15–10:40	**Coffee Break**	
10:40–11:55	**Multiparty Computation (2)** Location: KAIRAKU 1 Chair: TBD **UC-Secure Multiparty Computation from One-Way Functions using Stateless Tokens** Saikrishna Badrinarayanan; Abhishek Jain; Rafail Ostrovsky; Ivan Visconti *UCLA; JHU; UCLA; University of Salerno* **Scalable Private Set Union from Symmetric-Key Techniques** Vladimir Kolesnikov; Mike Rosulek; Ni Trieu; Xiao Wang *Georgia Institute of Technology; Oregon State University; Oregon State University; Northwestern University* **Card-based Cryptography Meets Formal Verification** Alexander Koch; Michael Schrempp; Michael Kirsten *Karlsruhe Institute of Technology (KIT); Karlsruhe Institute of Technology (KIT); Karlsruhe Institute of Technology (KIT)*	**Signatures** Location: KAIRAKU 2 Chair: TBD **Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures** Yilei Chen; Nicholas Genise; Pratyay Mukherjee *Visa Research; Rutgers University; Visa Research* **Decisional second-preimage resistance: When does SPR imply PRE?** Daniel J. Bernstein; Andreas Hülsing *University of Illinois at Chicago, Ruhr University Bochum; Technische Universiteit Eindhoven* **Structure-Preserving Signatures on Equivalence Classes From Standard Assumptions** Mojtaba Khalili; Daniel Slamanig; Mohammad Dakhilalian *Isfahan University of Technology; AIT Austrian Institute of Technology; Isfahan University of Technology*
11:55–13:35	**Lunch (Buffet)**	

Wednesday, December 11, 2019		
13:35–15:15	**Public Key Encryption (1)** Location: KAIRAKU 1&2 Chair: TBD **Simple and Efficient KDM-CCA Secure Public Key Encryption** Fuyuki Kitagawa; Takahiro Matsuda; Keisuke Tanaka *NTT Secure Platform Laboratories; National Institute of Advanced Industrial Science and Technology (AIST); Tokyo Institute of Technology* **Non-Committing Encryption with Quasi-Optimal Ciphertext-Rate Based on the DDH Problem** Yusuke Yoshida; Fuyuki Kitagawa; Keisuke Tanaka *Tokyo Institute of Technology; NTT Secure Platform Laboratories; Tokyo Institute of Technology* **Structure-Preserving and Re-randomizable RCCA-secure Public Key Encryption and its Applications** Antonio Faonio; Dario Fiore; Javier Herranz; Carla Ràfols *IMDEA Software Institute; IMDEA Software Institute; Cybercat and Universitat Politècnica de Catalunya; Cybercat and Universitat Pompeu Fabra* **iUC: Flexible Universal Composability Made Simple** Jan Camenisch; Stephan Krenn; Ralf Küsters; Daniel Rausch *Dfinity; AIT; University of Stuttgart; University of Stuttgart*	**Side Channels** Location: KAIRAKU 3 Chair: TBD **Leakage Resilience of the Duplex Construction** Christoph Dobraunig; Bart Mennink *Radboud University, The Netherlands; Radboud University, The Netherlands* **A Critical Analysis of ISO 17825 (`Testing methods for the mitigation of non-invasive attack classes against cryptographic modules')** Carolyn Whitnall; Elisabeth Oswald *University of Bristol; University of Bristol, University of Klagenfurt* **Location, location, location: Revisiting modeling and exploitation for location-based side channel leakages** Christos Andrikos; Lejla Batina; Lukasz Chmielewski; Liran Lerman; Vasilios Mavroudis; Kostas Papagiannopoulos; Guilherme Perin; Giorgos Rassias; Alberto Sonnino *National Technical University Athens; Radboud University; Radboud University, Riscure; Thales Belgium; University College London; Radboud University, NXP Semiconductors Hamburg; Riscure; National Technical University Athens; University College London* **Simple Refreshing in the Noisy Leakage Model** Stefan Dziembowski; Sebastian Faust; Karol Zebrowski *University of Warsaw; TU Darmstadt; University of Warsaw*
15:15–15:40	**Coffee Break**	
15:40–16:30	**Invited Lecture 2** Location: KAIRAKU 1&2 Chair: TBD **Streamlined blockchains: A simple and elegant approach (tutorial)** Elaine Shi *Cornell University, USA*	
16:30–17:30	**IACR Business Meeting** Location: KAIRAKU 1&2	
19:00–22:00	**Banquet** Location: OWADA	

Thursday, December 12, 2019		
9:00–10:40	**Symmetric Cryptography (2)** Location: KAIRAKU 1 Chair: TBD **The Exchange Attack: How to Distinguish 6 Rounds of AES with 2^{88.2} chosen plaintexts** Navid G. Bardeh; Sondre Rønjom *University of Bergen; University of Bergen* **Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC** Martin Albrecht; Carlos Cid; Lorenzo Grassi; Dmitry Khovratovich; Reinhard Lüftenegger; Christian Rechberger; Markus Schofnegger *Information Security Group, Royal Holloway, University of London; Information Security Group, Royal Holloway, University of London and Simula UiB; IAIK, Graz University of Technology and Know-Center; Evernym Inc. and ABDK Consulting and Dusk Network; IAIK, Graz University of Technology; IAIK, Graz University of Technology; IAIK, Graz University of Technology* **MILP-aided Method of Searching Division Property Using Three Subsets and Applications** Senpeng Wang; Bin Hu; Jie Guan; Kai Zhang; Tairong Shi *PLA SSF Information Engineering University, Zhengzhou, China; PLA SSF Information Engineering University, Zhengzhou, China; PLA SSF Information Engineering University, Zhengzhou, China; PLA SSF Information Engineering University, Zhengzhou, China; PLA SSF Information Engineering University, Zhengzhou, China* **Cryptanalysis of GSM Encryption in 2G/3G Networks without Rainbow Tables** Bin Zhang *Chinese Academy of Sciences*	**Functional Encryption** Location: KAIRAKU 2 Chair: TBD **Tightly Secure Inner Product Functional Encryption: Multi-Input and Function-Hiding Constructions** Junichi Tomida *NTT* **Public-Key Function-Private Hidden Vector Encryption (and More)** James Bartusek; Brent Carmer; Abhishek Jain; Zhengzhong Jin; Tancrède Lepoint; Fermi Ma; Tal Malkin; Alex Malozemoff; Mariana Raykova *UC Berkeley; Galois; Johns Hopkins University; Johns Hopkins University; Google; Princeton University; Columbia University; Galois; Google* **Multi-Client Functional Encryption for Linear Functions in the Standard Model from LWE** Benoît Libert; Radu Titiu *CNRS and ENS de Lyon (France); Bitdefender (Romania) and ENS de Lyon (France)* **From Single-Input to Multi-Client Inner-Product Functional Encryption** Michel Abdalla; Fabrice Benhamouda; Romain Gay *CNRS, ENS; Algorand Foundation; UC Berkeley*
10:40–11:05	**Coffee Break**	
11:05–12:20	**Public Key Encryption (2)** Location: KAIRAKU 1 Chair: TBD **Rate-1 Trapdoor Functions from the Diffie-Hellman Problem** Nico Döttling; Sanjam Garg; Mohammad Hajiabadi; Kevin Liu; Giulio Malavolta *CISPA; University of California Berkeley; University of California Berkeley; University of California Berkeley; Simons Institute* **The Local Forking Lemma and its Application to Deterministic Encryption** Mihir Bellare; Wei Dai; Lucy Li *UCSD; UCSD; Cornell University* **Fine-Grained Cryptography Revisited** Egashira Shohei; Yuyu Wang; Keisuke Tanaka *Tokyo Institute of Technology; University of Electronic Science and Technology of China; Tokyo Institute of Technology*	**Zero Knowledge** Location: KAIRAKU 2 Chair: TBD **Shorter QA-NIZK and SPS with Tighter Security** Masayuki Abe; Charanjit S. Jutla; Miyako Ohkubo; Jiaxin Pan; Arnab Roy; Yuyu Wang *NTT Corporation; IBM T. J. Watson Research Center; Security Fundamentals Laboratories, CSR, NICT; Department of Mathematical Sciences, NTNU – Norwegian University of Science and Technology; Fujitsu Laboratories of America; University of Electronic Science and Technology of China* **Efficient Noninteractive Certification of RSA Moduli and Beyond** Sharon Goldberg; Leonid Reyzin; Omar Sagga; Foteini Baldimtsi *Boston University; Boston University; Boston University; George Mason University* **Shorter Pairing-based Arguments under Standard Assumptions** Alonso González; Carla Ràfols *ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), France; Universitat Pompeu Fabra and Cybercat, Barcelona, Spain*