Sunday, November 29	
14:00-18:00	Registration
15:00-17:00	Traditional Maori welcome ceremony at Waipapa Marae

Monday, November 30		
8:00-9:15	Registration at Owen Glenn Building	
9:15-9:30	Welcome	
9:30-10:30	**Invited Lecture I** (Jung Hee Cheon) Structure-Preserving Cryptography; *Masayuki Abe; NTT Secure Platform Laboratories, Japan*	
10:30-10:40	Conference Photo	
10:40-11:10	Coffee Break	
11:10-11:35	**Best Paper** (Jung Hee Cheon) Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance; *Shi Bai; Adeline Langlois; Tancrède Lepoint; Damien Stehlé; Ron Steinfeld*	
	Indistinguishability Obfuscation (Sherman Chow)	**Hashes and MACs** (Lai Xuejia)
11:40-12:05	■ Multi-Input Functional Encryption for Unbounded Arity Functions; *Saikrishna Badrinarayanan; Divya Gupta; Abhishek Jain; Amit Sahai*	■ Tradeoff Cryptanalysis of Memory-Hard Functions; *Alex Biryukov; Dmitry Khovratovich*
12:05-12:30	■ Multi-Party Key Exchange for Unbounded Parties from Indistinguishability Obfuscation; *Dakshita Khurana; Vanishree Rao; Amit Sahai*	■ Generic Security of NMAC and HMAC with Input Whitening; *Peter Gaži; Krzysztof Pietrzak; Stefano Tessaro*
12:30-13:50	Buffet Lunch in conference venue foyer	
	PRFs and Hashes (Huaxiong Wang)	**Symmetric Encryption** (Stefano Tessaro)
13:50-14:15	■ Adaptively Secure Puncturable Pseudorandom Functions in the Standard Model; *Susan Hohenberger; Venkata Koppula; Brent Waters*	■ A Synthetic Indifferentiability Analysis of Interleaved Double-Key Even-Mansour Ciphers; Chun Guo; Dongdai Lin
14:15-14:40	■ Multilinear and Aggregate Pseudorandom Functions: New Constructions and Improved Security; *Michel Abdalla; Fabrice Benhamouda; Alain Passelègue*	■ Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing; *Benoit Cogliati and Yannick Seurin*
14:40-15:05	■ New Realizations of Somewhere Statistically Binding Hashing and Positional Accumulators; *Tatsuaki Okamoto; Krzysztof Pietrzak; Brent Waters; Daniel Wichs*	■ An Inverse-free Single Keyed Tweakable Enciphering Scheme; *Ritam Bhaumik; Mridul Nandi*
15:05-15:30	Coffee Break	
	DL and Number Theory (Tsuyoshi Takagi)	**Foundations** (Rei Safavi-Naini)
15:30-15:55	■ Computing Individual Discrete Logarithms Faster in GF(p^n) with the NFS-DL Algorithm; *Aurore Guillevic*	■ On Black-Box Complexity of Universally Composable Security in the CRS model; *Carmit Hazay; Muthuramakrishnan Venkitasubramaniam*
15:55-16:20	■ Multiple Discrete Logarithm Problem with Auxiliary Inputs; *Taechan Kim*	■ Public Verifiability in the Covert Model (Almost) for Free; *Vladimir Kolesnikov; Alex J. Malozemoff*
16:20-16:45	■ Solving Linear Equations Modulo Unknown Divisors: Revisited; *Yao Lu; Rui Zhang; Liqiang Peng; Dongdai Lin*	■ Limits of Extractability Assumptions with Distributional Auxiliary Input; *Elette Boyle; Rafael Pass*
16:45-17:10	■ FourQ: four-dimensional decompositions on a Q-curve over the Mersenne Prime; *Craig Costello; Patrick Longa*	■ Composable & Modular Anonymous Credentials: Definitions and Practical Constructions; *Jan Camenisch; Maria Dubovitskaya; Kristiyan Haralambiev; Markulf Kohlweiss*

Tuesday, December 1

9:00-10:00	**Invited Lecture II** (Tetsu Iwata) Computer-Aided Cryptography: Status and Perspectives, *Gilles Barthe, IMDEA Software Institute, Spain*	
10:05-10:30	**Attacks on ASASA (Invited to JoC)** (Tetsu Iwata) Key-Recovery Attacks on ASASA; *Brice Minaud; Patrick Derbez; Pierre-Alain Fouque; Pierre Karpman*	
10:30-11:00	Coffee Break	
	Signatures (Mehdi Tibouchi)	**Side-Channel Attacks** (Josef Pieprzyk)
11:00-11:25	■ Efficient Fully Structure-Preserving Signatures for Large Messages; *Jens Groth*	■ ASCA, SASCA and DPA with Enumeration: Which One Beats the Other and When?; *Vincent Grosso; François-Xavier Standaert*
11:25-11:50	■ A Provably Secure Group Signature Scheme from Code-Based Assumptions; *Martianus Frederic Ezerman; Hyung Tae Lee; San Ling; Khoa Nguyen; Huaxiong Wang*	■ Counting Keys in Parallel After a Side Channel Attack; *Daniel P. Martin; Jonathan F. O'Connell; Elisabeth Oswald; Martijn Stam*
11:50-12:15	■ Type 2 Structure-Preserving Signature Schemes Revisited; *Sanjit Chatterjee; Alfred Menezes*	■ A Unified Metric for Quantifying Information Leakage of Cryptographic Devices under Power Analysis Attacks; *Liwei Zhang; A. Adam Ding; Yunsi Fei; Pei Luo*
12:15-12:40	■ Design Principles for HFEv- based Multivariate Signature Schemes; *Albrecht Petzoldt; Ming-Shing Chen; Bo-Yin Yang; Chengdong Tao; Jintai Ding*	■ How Secure is AES under Leakage; *Andrey Bogdanov; Takanori Isobe*
12:40-14:00	Light Lunch in conference venue foyer	
	Free Afternoon	
18:30-22:00	Rump Session (Nigel Smart)	

Wednesday, December 2

9:00-10:00	**Invited Lecture III, IACR Distinguished Lecture** (Steven Galbraith) The Moral Character of Cryptographic Work; *Phillip Rogaway, University of California, Davis, USA*	
10:00-10:30	Coffee Break	
10:30-10:55	**Number Field Sieve (Invited to JoC)** (Steven Galbraith) The Tower Number Field Sieve; *Razvan Barbulescu; Pierrick Gaudry; Thorsten Kleinjung*	
	Multiparty Computation I (Nigel Smart)	**Design of Block Ciphers** (Bart Mennink)
11:00-11:25	■ Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness; *Dana Dachman-Soled; Chang Liu; Charalampos Papamanthou; Elaine Shi; Uzi Vishkin*	■ On the Optimality of Non-Linear Computations of Length-Preserving Encryption Schemes; Mridul Nandi
11:25-11:50	■ Three-Party ORAM for Secure Computation; *Sky Faber; Stanislaw Jarecki; Sotirios Kentros; Boyang Wei*	■ Midori: A Block Cipher for Low Energy; *Subhadeep Banik; Andrey Bogdanov; Takanori Isobe; Kyoji Shibutani; Harunaga Hiwatari; Toru Akishita; Francesco Regazzoni*
11:50-12:15	■ On Cut-and-Choose Oblivious Transfer and Its Variants; *Vladimir Kolesnikov; Ranjit Kumaresan*	■ Optimally-Secure Block Ciphers from Ideal Primitives; *Stefano Tessaro*
12:15-13:30	Buffet Lunch in conference venue foyer	
	Public Key Encryption (Tatsuaki Okamoto)	**Authenticated Encryption** (Yu Sasaki)
13:30-13:55	■ An Asymptotically Optimal Method for Converting Bit Encryption to Multi-Bit Encryption; *Takahiro Matsuda; Goichiro Hanaoka*	■ Security of Full-State Keyed and Duplex Sponge: Applications to Authenticated Encryption; *Bart Mennink; Reza Reyhanitabar; Damian Vizár*
13:55-14:20	■ Selective Opening Security for Receivers; *Carmit Hazay; Arpita Patra; Bogdan Warinschi*	■ Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates; *Christoph Dobraunig; Maria Eichlseder; Florian Mendel*
14:20-14:45	■ Function-Hiding Inner Product Encryption; *Allison Bishop; Abhishek Jain; Lucas Kowalczyk*	■ Collision Attacks against CAESAR Candidates Forgery and Key-Recovery against AEZ and Marble; *Thomas Fuhr; Gaëtan Leurent; Valentin Suder*

14:45-15:15	Coffee Break	
	ABE and IBE (Sherman Chow)	**Symmetric Analysis** (Bart Preneel)
15:15-15:40	■ Idealizing Identity-Based Encryption; *Dennis Hofheinz; Christian Matt; Ueli Maurer*	■ Optimized Interpolation Attacks on LowMC; *Itai Dinur; Yunwen Liu; Willi Meier; Qingju Wang*
15:40-16:05	■ A Framework for Identity-Based Encryption with Almost Tight Security; *Nuttapong Attrapadung; Goichiro Hanaoka; Shota Yamada*	■ Another Tradoff Attack on Sprout-like Stream Ciphers; *Bin Zhang; Xinxin Gong*
16:05-16:30	■ Riding on Asymmetry: Efficient ABE for Branching Programs; *Sergey Gorbunov; Dhinakaran Vinayagamurthy*	■ Reverse-engineering of the cryptanalytic attack used in the Flame super-malware; *Max Fillinger; Marc Stevens*
16:30-16:55	■ Conversions among Several Classes of Predicate Encryption and Applications to ABE with Various Compactness Tradeoffs; *Nuttapong Attrapadung; Goichiro Hanaoka; Shota Yamada*	■ Analysis of SHA-512/224 and SHA-512/256; *Christoph Dobraunig; Maria Eichlseder; Florian Mendel*
17:15-18:30	IACR Membership Meeting	
19:00	Conference Banquet	

Thursday, December 3

	Zero-Knowledge (Jens Groth)	**Cryptanalysis** (Jian Guo)
9:00-9:25	■ QA-NIZK Arguments in Asymmetric Groups: New Tools and New Constructions; *Alonso González; Alejandro Hevia; Carla Ràfols*	■ On the Impact of Known-Key Attacks on Hash Functions; *Bart Mennink; Bart Preneel*
9:25-9:50	■ Dual-System Simulation-Soundness with Applications to UC-PAKE and More; *Charanjit S. Jutla; Arnab Roy*	■ Property Preserving Symmetric Encryption Revisited; *Sanjit Chatterjee; M. Prem Laxman Das*
9:50-10:15	■ Secret Sharing and Statistical Zero Knowledge; *Vinod Vaikuntanathan; Prashant N. Vasudevan*	■ Refinements of the k-tree Algorithm for the Generalized Birthday Problem; *Ivica Nikolić; Yu Sasaki*
10:15-10:40	■ Compactly Hiding Linear Spans: Tightly Secure Constant-Size Simulation-Sound QA-NIZK Proofs and Applications; *Benoît Libert; Thomas Peters; Marc Joye; Moti Yung*	■ How to Sequentialize Independent Parallel Attacks?; *Sonia M. Bogos; Serge Vaudenay*
10:40-11:10	Coffee Break	
	Multiparty Computation II (Rafael Pass)	**Privacy and Lattices** (Noboru Kunihiro)
11:10-11:35	■ A Unified Approach to MPC with Preprocessing using OT; *Tore Kasper Frederiksen; Marcel Keller; Emmanuela Orsini; Peter Scholl*	■ Pure Differential Privacy for Rectangle Queries via Private Partitions; *Cynthia Dwork; Moni Naor; Omer Reingold; Guy Rothblum*
11:35-12:00	■ Secure Computation from Millionaire; *abhi shelat; Muthuramakrishnan Venkitasubramaniam*	■ Implementing Candidate Graded Encoding Schemes from Ideal Lattices; *Martin R. Albrecht; Catalin Cocis; Fabien Laguillaumie; Adeline Langlois*
12:00-12:25	■ Garbling Scheme for Formulas with Constant Size of Garbled Gates; *Carmen Kempka; Ryo Kikuchi; Susumu Kiyoshima; Koutarou Suzuki*	■ New Circular Security Counterexamples from Decision Linear and Learning with Errors; *Allison Bishop; Susan Hohenberger; Brent Waters*
12:25-12:50	■ Card-based Cryptographic Protocols using a Minimal Number of Cards; *Alexander Koch; Stefan Walzer; Kevin Härtel*	
12:50-14:00	Light Lunch in conference venue foyer	
14:00	Adieu	