Asiacrypt 2018 Program

Sunday, December 02, 2018

17:00–20:00	**Registration & Reception** Location: Old Government House QUT Gardens Point, 2 George Street, Brisbane, 4001

Monday, December 03, 2018

8:00–17:00	**Registration**
9:00–9:15	**Opening remarks** Location: Z Block Room 411 (Z411) Chair: Conference General Chair
9:15–10:05	**IACR Distinguished Lecture** Location: Z Block Room 411 (Z411) Chair: Thomas Peyrin **25 Years of Linear Cryptanalysis - Early History and Path Search Algorithm** Mitsuru Matsui *Mitsubishi Electric Corporation, Japan*
10:05–10:30	**Best Paper Award** Location: Z Block Room 411 (Z411) Chair: Thomas Peyrin **Block Cipher Invariants as Eigenvectors of Correlation Matrices** Tim Beyne *KU Leuven, imec-COSIC*
10:30–10:40	**Conference Photo** Location: P Block Level 4 Outside Area
10:40–11:10	**Break** Location: P Block Level 5
11:10–12:25	**Post-Quantum Cryptanalysis** Location: P Block Room 421 (P421) Chair: Bo-Yin Yang **Practical attacks against the Walnut digital signature scheme** Ward Beullens, Simon R. Blackburn *imec-COSIC, KU Leuven, Royal Holloway* **Two attacks on rank metric code-based schemes: RankSign and an IBE scheme** Thomas Debris-Alazard, Jean-Pierre Tillich *Sorbonne Universites, Inria, Inria* **An efficient structural attack on NIST submission DAGS** Elise Barelli, Alain Couvreur *INRIA & LIX Ecole Polytechnique* **Encrypted Storage** Location: P Block Room 514 (P514) Chair: Joseph Liu **Pattern Matching on Encrypted Streams** Nicolas Desmoulins, Pierre-Alain Fouque, Cristina Onete, Olivier Sanders *Orange Labs, Université de Rennes 1, Université de Limoges* **SQL on Structurally-Encrypted Databases** Seny Kamara, Tarik Moataz *Brown University* **Parameter-Hiding Order Revealing Encryption** David Cash, Feng-Hao Liu, Adam O'Neill, Mark Zhandry, Cong Zhang *Department of Computer Science, University of Chicago, Department of Computer and Electrical Engineering and Computer Science, Florida Atlantic University, Department of Computer Science, Georgetown University, Department of Computer Science, Princeton University, Department of Computer Science, Rutgers University*
12:25–13:30	**Lunch**

Monday, December 03, 2018

Symmetric-Key Constructions I

Location: P Block Room 421 (P421)
Chair: Xuejia Lai

13:30–14:45

Revisiting Key-Alternating Feistel Ciphers: Reducing Key-size, and Multi-user Security
Chun Guo, Lei Wang
ICTEAM/ELEN/Crypto Group, Universite Catholique de Louvain, Belgium, Shanghai Jiao Tong University, Shanghai, China

Short Variable Length Domain Extenders With Beyond Birthday Bound Security
Yu Long Chen, Bart Mennink, Mridul Nandi
KU Leuven (Belgium), Radboud University (The Netherlands), Indian Institute of Technology (India)

Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damg□ård Constructions
Akinori Hosoyamada, Kan Yasuda
NTT Secure Platform Laboratories

Lattice Crypto I

Location: P Block Room 514 (P514)
Chair: Amin Sakzad

Measuring, simulating and exploiting the head concavity phenomenon in BKZ
Shi Bai, Damien Stehlé, Weiqiang Wen
Department of Mathematical Sciences, Florida Atlantic University, ENS de Lyon and Laboratoire LIP (U. Lyon, CNRS, ENS de Lyon, INRIA, UCBL)

Quantum Lattice Enumeration and Tweaking Discrete Pruning
Yoshinori Aono, Phong Q. Nguyen, Yixin Shen
NICT, Inria and CNRS, JFLI, University of Tokyo, IRIF, Univ Paris Diderot, CNRS

On the Hardness of the Computational Ring-LWR Problem and its Applications
Long Chen, Zhenfeng Zhang, Zhenfei Zhang
New Jersey Institute of Technology, Institue of Software, Chinese Academy of Sciences, OnBoard Security Inc.

14:45–15:15 — **Break**
Location: P Block Level 5

Symmetric-Key Constructions II

Location: P Block Room 421 (P421)
Chair: Huaxiong Wang

15:15–16:05

Tweakable Block Ciphers Secure Beyond the Birthday Bound in the Ideal Cipher Model
ByeongHak Lee, Jooyoung Lee
KAIST, Korea

ZCZ: Achieving n-bit SPRP Security with a Minimal Number of Tweakable-block-cipher Calls
Ritam Bhaumik, Eik List, Mridul Nandi
Indian Statistical Institute, Kolkata, Bauhaus-Universität, Weimar, Germany

Lattice Crypto II

Location: P Block Room 514 (P514)
Chair: Douglas Stebila

On the Statistical Leak of the GGH13 Multilinear Map and some Variants
Léo Ducas, Alice Pellet-Mary
Cryptology Group, CWI, Amsterdam, The Netherlands, Univ Lyon, CNRS, ENS de Lyon, Inria, UCBL, LIP, Lyon, France.

LWE Without Modular Reduction and Improved Side-Channel Attacks Against BLISS
Jonathan Bootle, Claire Delaplace, Thomas Espitau, Pierre-Alain Fouque, Mehdi Tibouchi
University College London, Univ Rennes &, Univ Lille, Sorbonne Université, Univ Rennes

16:05–16:10 — **Short Break**

Quantum Symmetric Cryptanalysis

Location: P Block Room 421 (P421)
Chair: Alain Couvreur

16:10–17:00

Quantum Algorithms for the k-xor Problem
Lorenzo Grassi, María Naya-Plasencia, André Schrottenloher
IAIK, TU Graz, Austria, Inria, France

Hidden Shift Quantum Cryptanalysis and Implications
Xavier Bonnetain, María Naya-Plasencia
Sorbonne Université, France and Inria, France, Inria, France

Zero Knowledge

Location: P Block Room 514 (P514)
Chair: David Pointcheval

Arya: Nearly Linear-Time Zero-Knowledge Proofs for Correct Program Execution
Jonathan Bootle, Andrea Cerulli, Jens Groth, Sune Jakobsen, Mary Maller
University College London

Improved (Almost) Tightly-Secure Simulation-Sound QA-NIZK with Applications
Masayuki Abe, Charanjit S. Jutla, Miyako Ohkubo, Arnab Roy
NTT Corporation, Japan, IBM TJ Watson Research Center, USA, Security Fundamentals Laboratories, CSR, NICT, Japan, Fujitsu Laboratories of America, USA

Tuesday, December 04, 2018

9:00–9:50

Invited talk

Location: Z Block Room 411 (Z411)
Chair: Steven Galbraith

Picnic: Postquantum signatures from zero-knowledge proofs
Melissa Chase
Microsoft Research

Tuesday, December 04, 2018

9:50–10:15

JoC Paper I

Location: Z Block Room 411 (Z411)
Chair: Steven Galbraith

Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model
Shuichi Katsumata, Shota Yamada, Takashi Yamakawa
The University of Tokyo/AIST, AIST, NTT Secure Platform Laboratories

10:15–10:45

Coffee Break

Location: P Block Level 5

10:45–12:25

Symmetric-Key Cryptanalysis

Location: P Block Room 421 (P421)
Chair: Dan Bernstein

Programming the Demirci-Sel{\c{c}}uk Meet-in-the-Middle Attack with Constraints
Danping Shi, Siwei Sun, Patrick Derbez, Yosuke Todo, Bing Sun, Lei Hu
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Univ Rennes, CNRS, IRISA, France, NTT Secure Platform Laboratories, Japan, College of Liberal Arts and Sciences, National University of Defense Technology, China

Cryptanalysis of MORUS
Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, Benoît Viguier
imec-COSIC, KU Leuven, Belgium, Graz University of Technology, Austria, , Inria, France, Royal Holloway University of London, United Kingdom, NTT, Japan, Radboud University, Netherlands

New MILP Modeling: Improved Conditional Cube Attacks on Keccak-based Constructions
Ling Song, Jian Guo, Danping Shi, San Ling
Nanyang Technological University, Singapore, Institute of Information Engineering, Chinese Academy of Sciences, China, Nanyang Technological University, Singapore, Institute of Information Engineering, Chinese Academy of Sciences, China

On the Concrete Security of Goldreich's Pseudorandom Generator
Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi, Yann Rotella
KIT, Germany, Thales Communications and Security, CentraleSupélec, Irisa, France, ICTEAM/ELEN/Crypto Group, Université catholique de Louvain, Belgium, Thales Communications and Security, ENS, CNRS, Inria, France, Inria, France

Public Key and Identity-Based Encryption

Location: P Block Room 514 (P514)
Chair: Tatsuaki Okamoto

A Framework for Achieving KDM-CCA Secure Public-Key Encryption
Fuyuki Kitagawa, Keisuke Tanaka
Tokyo Institute of Technology

Understanding and Constructing AKE via Double-key Key Encapsulation Mechanism
Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, Jingnan He
IIE, CAS, Chalmers University of Technology

Identity-based Encryption Tightly Secure under Chosen-ciphertext Attacks
Dennis Hofheinz, Dingding Jia, Jiaxin Pan
Karlsruhe Institute of Technology, Karlsruhe, Germany, Institute of Information Engineering, CAS, Beijing, China

Short Digital Signatures and ID-KEMs via Truncation Collision Resistance
Tibor Jager, Rafael Kurek
Paderborn University

12:25–13:00

Lunch

Location: P Block Level 5

13:00–17:00

Excursion

Location: Departs from P Block Level 5. There will be 3 departure times from Lone Pine to QUT: 4:30pm, 4:45pm and 5:00pm

19:00–22:00

Rump Session

Location: Room Three Sixty, Level 10, Y Block, QUT Gardens Point

Wednesday, December 05, 2018

8:50–10:30

Side Channels

Location: P Block Room 421 (P421)
Chair: Lejla Batina

New Instantiations of the CRYPTO 2017 Masking Schemes
Pierre Karpman, Daniel S. Roche
Université Grenoble Alpes, United States Naval Academy

Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures
Christoph Dobraunig, Maria Eichlseder, Hannes Groß, Stefan Mangard, Florian Mendel, Robert Primas
Graz University of Technology, Infineon Technologies AG

Tight Private Circuits: Achieving Probing Security with the Least Refreshing
Sonia Belaïd, Dahmun Goudarzi, Matthieu Rivain
CryptoExperts, Paris, France, CryptoExperts, Paris, France and ENS, CNRS, INRIA and PSL Research University, Paris, France

Attacks and Countermeasures for White-box Designs
Alex Biryukov, Aleksei Udovenko
SnT and CSC, University of Luxembourg, SnT, University of Luxembourg

Signatures

Location: P Block Room 514 (P514)
Chair: Masa Abe

Signatures with Flexible Public Key: Introducing Equivalence Classes for Public Keys
Michael Backes, Lucjan Hanzlik, Kamil Kluczniak, Jonas Schneider
CISPA Helmholtz Center (i. G.) GmbH, CISPA, Saarland University, CISPA Helmholtz Center (i.G.) GmbH, Department of Computing, The Hong Kong Polytechnic University

Compact Multi-Signatures for Smaller Blockchains
Dan Boneh, Manu Drijvers, Gregory Neven
Stanford University, DFINITY and ETH Zurich, DFINITY

Multi-Key Homomorphic Signatures Unforgeable under Insider Corruption
Russell W. F. Lai, Raymond K. H. Tai, Harry W. H. Wong, Sherman S. M. Chow
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), and The Chinese University of Hong Kong, The Chinese University of Hong Kong

Attribute-Based Signatures for Unbounded Languages from Standard Assumptions
Yusuke Sakai, Shuichi Katsumata, Nuttapong Attrapadung, Goichiro Hanaoka
AIST, Japan, The University of Tokyo, Japan / AIST, Japan

10:30–11:00

Coffee Break

Location: P Block Level 5

11:00–11:50

Invited Talk

Location: Z Block Room 411 (Z411)
Chair: Josef Pieprzyk

Democracy, security and evidence: let's have all three
Vanessa Teague
Department of Computing and Information Systems, the University of Melbourne

11:50–12:15

JoC Paper II

Location: Z Block Room 411 (Z411)
Chair: Josef Pieprzyk

Learning Strikes Again: the Case of the DRS Signature Scheme
Yang Yu, Léo Ducas
Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, China, Cryptology Group, CWI, Amsterdam, The Netherlands

12:15–13:15

Lunch

Location: P Block Level 5

Wednesday, December 05, 2018

13:15–15:20

Leakage-Resilient Cryptography & Functional/Inner Product/Predicate Encryption I

Location: P Block Room 421 (P421)
Chair: Sherman Chow

How to Securely Compute with Noisy Leakage in Quasilinear Complexity
Dahmun Goudarzi, Antoine Joux, Matthieu Rivain
CryptoExperts, ENS, , CryptoExperts

Leakage-Resilient Cryptography from Puncturable Primitives and Obfuscation
Yu Chen, Yuyu Wang, Hong-Sheng Zhou
Institute of Information Engineering, Chinese Academy of Sciences, Tokyo Institute of Technology/IOHK/AIST, Virginia Commonwealth University

Unbounded Inner Product Functional Encryption from Bilinear Maps
Junichi Tomida, Katsuyuki Takashima
NTT, Mitsubishi Electric

Adaptively Simulation-Secure Attribute-Hiding Predicate Encryption
Pratish Datta, Tatsuaki Okamoto, Katsuyuki Takashima
NTT Secure Platform Laboratories, Mitsubishi Electric

Improved Inner-product Encryption with Adaptive Security and Full Attribute-hiding
Jie Chen, Junqing Gong, Hoeteck Wee
East China Normal University, ENS de Lyon, LIP, CNRS and ENS, PSL

MPC

Location: P Block Room 514 (P514)
Chair: Bernardo David

On Multiparty Garbling of Arithmetic Circuits
Aner Ben Efraim
Ariel University and Ben Gurion University of the Negev

Free IF: How to Omit Inactive Branches and Implement S-Universal Garbled Circuit (Almost) for Free
Vladimir Kolesnikov
Georgia Inst. of Tech.

Secure Computation with Low Communication from Cross-checking
S. Dov Gordon, Samuel Ranellucci, Xiao Wang
George Mason University, Unbound Tech, University of Maryland

Concretely Efficient Large-Scale MPC with Active Security (or, TinyKeys for TinyOT)
Carmit Hazay, Emmanuela Orsini, Peter Scholl, Eduardo Soria-Vazquez
Bar-Ilan University, Israel, KU Leuven ESAT/COSIC, Belgium, Aarhus University, Denmark, University of Bristol, UK

Non-Interactive Secure Computation from One-Way Functions
Saikrishna Badrinarayanan, Abhishek Jain, Rafail Ostrovsky, Ivan Visconti
UCLA, JHU, University of Salerno

15:20–15:50

Coffee Break

Location: P Block Level 5

15:50–16:40

Functional/Inner Product/Predicate Encryption II

Location: P Block Room 421 (P421)
Chair: Katsuyuki Takashima

Decentralized Multi-Client Functional Encryption for Inner Product
Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, David Pointcheval
Université Limoges, CNRS, ENS/PSL, INRIA, France, CNRS, ENS/PSL, France, CNRS, ENS/PSL, INRIA, France, Université Limoges, France

Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p
Guilhem Castagnos, Fabien Laguillaumie, Ida Tucker
Université de Bordeaux, INRIA, CNRS, IMB UMR 5251, F-33405 Talence, France., Univ Lyon, CNRS, Université Claude Bernard Lyon 1, ENS de Lyon, INRIA, LIP UMR 5668, F-69007, LYON Cedex 07, France.

ORAM

Location: P Block Room 514 (P514)
Chair: Kouichi Sakurai

Simple and Efficient Two-Server ORAM
S. Dov Gordon, Jonathan Katz, Xiao Wang
University of Maryland, George Mason University

More is Less: Perfectly Secure Oblivious Algorithms in the Multi-Server Setting
T-H. Hubert Chan, Jonathan Katz, Kartik Nayak, Antigoni Polychroniadou, Elaine Shi
The University of Hong Kong, University of Maryland, College Park, University of Maryland, College Park and VMware Research, Cornell Tech, Cornell University

16:45–17:45

IACR Meeting

Location: P Block Room 514 (P514)
Chair: Christian Cachin

18:30–22:30

Conference Dinner

Location: Hilton Brisbane, 190 Elizabeth Street, Brisbane

Thursday, December 06, 2018

9:00–10:15

Secret Sharing

Location: P Block Room 512 (P512)
Chair: Duong Hieu Phan

Homomorphic Secret Sharing for Low Degree Polynomials
Russell W. F. Lai, Giulio Malavolta, Dominique Schröder
Friedrich-Alexander-Universität Erlangen-Nürnberg

Optimal Linear Multiparty Conditional Disclosure of Secrets Protocols
Amos Beimel, Naty Peter
Ben-Gurion University

Constructing Ideal Secret Sharing Schemes based on Chinese Remainder Theorem
Yu Ning, Fuyou Miao, Wenchao Huang, Keju Meng, Yan Xiong, Xingfu Wang, Xingfu Wang
University of Science and Technology of China

Real World Protocols

Location: P Block Room 514 (P514)
Chair: Colin Boyd

A Universally Composable Framework for the Privacy of Email Ecosystems
Pyrros Chaidos, Olga Fourtounelli, Aggelos Kiayias, Thomas Zacharias
National and Kapodistrian University of Athens, The University of Edinburgh, IOHK, The University of Edinburgh

State Separation for Code-Based Game-Playing Proofs
Chris Brzuska, Antoine Délignat-Lavaud, Cédric Fournet, Konrad Kohbrok, Markulf Kohlweiss
Aalto University, Microsoft Research, University of Edinburgh, Microsoft Research

Security of the Blockchain against Long Delay Attack
Puwen Wei, Quan Yuan, Yuliang Zheng
Shandong University, University of Alabama at Birmingham

10:15–10:45

Break

Location: P Block Level 5

10:45–12:00

Isogeny Crypto

Location: P Block 512 (P512)
Chair: Mehdi Tibouchi

Towards practical key exchange from ordinary isogeny graphs
Luca De Feo, Jean Kieffer, Benjamin Smith
Université Paris Saclay, UVSQ, LMV, Versailles, France, Inria, Université Paris Saclay, Palaiseau, France, École Normale Supérieure, Paris, France, IMB - Institut de Mathématiques de Bordeaux, Inria Bordeaux - Sud-Ouest, Talence, France, Inria and École polytechnique, Université Paris Saclay, Palaiseau, France

CSIDH: An Efficient Post-Quantum Commutative Group Action
Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, Joost Renes
KU Leuven, TU Eindhoven, Radboud Universiteit

Computing supersingular isogenies on Kummer surfaces
Craig Costello
Microsoft Research

Foundations

Location: P Block Room 514 (P514)
Chair: Ron Steinfeld

Robustly Reusable Fuzzy Extractor from Standard Assumptions
Yunhua Wen, Shengli Liu
Department of Computer Science and Engineering, Shanghai Jiao Tong University

Simple and More Efficient PRFs with Tight Security from LWE and Matrix-DDH
Tibor Jager, Rafael Kurek, Jiaxin Pan
Paderborn University, Karlsruhe Institute of Technology

Simulatable Channels: Extended Security that is Universally Composable and Easier to Prove
Jean Paul Degabriele, Marc Fischlin
TU Darmstadt

12:00–12:15

Conference Closing

Location: P Block Room 514 (P514)

12:15–13:15

Lunch

Location: P Block Level 5