List of Accepted Papers - Asiacrypt 2018

New Instantiations of the CRYPTO 2017 Masking Schemes
Pierre Karpman (Laboratoire Jean Kuntzmann, Université Grenoble Alpes, France)
Daniel S. Roche (Computer Science Department, United States Naval Academy, U.S.A.)

Pattern Matching on Encrypted Streams
Nicolas Desmoulins (Orange Labs)
Pierre-Alain Fouque (Université de Rennes 1 and IRISA)
Cristina Onete (Université de Limoges, CNRS UMR 7252)
Olivier Sanders (Orange Labs)

Revisiting Key-alternating Feistel Ciphers for Shorter Keys and Multi-user Security
Chun Guo (Department of ICTEAM/ELEN/Crypto Group, Université catholique de Louvain)
Lei Wang (Shanghai Jiao Tong University, Shanghai)

Practical Attacks Against the Walnut Digital Signature Scheme
Ward Beullens (imec-COSIC, KU Leuven)
Simon R. Blackburn (Department of Mathematics, Royal Holloway, University of London)

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

On Multiparty Garbling of Arithmetic Circuits
Aner Ben Efraim (Ben Gurion University of the Negev - Ariel University)

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

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

Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p
Guilhem Castagnos (Université de Bordeaux, LFANT - INRIA, CNRS, IMB UMR 5251)
Fabien Laguillaumie (Université Claude Bernard Lyon 1/LIP, France)
Ida Tucker (Ens de Lyon/LIP, France)

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

Compact Multi-Signatures for Smaller Blockchains
Dan Boneh (Stanford University)
Manu Drijvers (DFINITY)
Gregory Neven (DFINITY)

How to Securely Compute with Noisy Leakage in Quasilinear Complexity
Dahmun Goudarzi (CryptoExperts, ENS, CNRS, INRIA, PSL Research University)
Antoine Joux (Sorbonne Université, Institut de Mathématiques de Jussieu--Paris Rive Gauche, CNRS, INRIA, Univ Paris Diderot)
Matthieu Rivain (CryptoExperts)

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

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

Programming the Demirci-Selcuk Meet-in-the-Middle Attack with Constraints
Danping Shi (Chinese Academy of Sciences, China)
Siwei Sun (Chinese Academy of Sciences, China)
Patrick Derbez (Univ Rennes, CNRS, IRISA, France)
Yosuke Todo (NTT Secure Platform Laboratories, Japan)
Bing Sun (College of Liberal Arts and Sciences, National University of Defense Technology, China)
Lei Hu (Chinese Academy of Sciences, China)

Parameter-Hiding Order Revealing Encryption
David Cash (Department of Computer Science, University of Chicago)
Feng-Hao Liu (Department of Computer & Electrical Engineering and Computer Science, Florida Atlantic University)
Adam O'Neill (Department of Computer Science, Georgetown University)
Mark Zhandry (Department of Computer Science, Princeton University)
Cong Zhang (Department of Computer Science, Rutgers University)

Computing Supersingular Isogenies on Kummer Surfaces
Craig Costello (Microsoft Research)

Robustly Reusable Fuzzy Extractor from Standard Assumptions
Yunhua Wen (Shanghai Jiao Tong University (SJTU), Shanghai, China)
Shengli Liu (Shanghai Jiao Tong University (SJTU), Shanghai, China)

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

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

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

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

Block Cipher Invariants as Eigenvectors of Correlation Matrices
Tim Beyne (imec-COSIC KU Leuven)

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

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

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

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

Constructing Ideal Secret Sharing Schemes Based on Chinese Remainder Theorem
Yu Ning (School of Computer Science and Technology, University of Science & Technology of China)
Fuyou Miao (School of Computer Science and Technology, University of Science & Technology of China)
Wenchao Huang (School of Computer Science and Technology, University of Science & Technology of China)
Keju Meng (School of Computer Science and Technology, University of Science & Technology of China)
Yan Xiong (School of Computer Science and Technology, University of Science & Technology of China)

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

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

Optimal Linear Multiparty Conditional Disclosure of Secrets Protocols
Amos Beimel (Ben-Gurion University of the Negev)
Naty Peter (Ben-Gurion University of the Negev)

Measuring, simulating and exploiting the head concavity phenomenon in BKZ
Shi Bai (Florida Atlantic University)
Damien Stehlé (ENS de Lyon)
Weiqiang Wen (ENS de Lyon)

LWE without Modular Reduction and Improved Side-Channel Attacks against BLISS
Jonathan Bootle (University College London)
Claire Delaplace (Univ Rennes)
Thomas Espitau (Sorbonne Université)
Pierre-Alain Fouque (Univ Rennes)
Mehdi Tibouchi (NTT Corporation)

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

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

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

Quantum Algorithms for the k-xor Problem
Lorenzo Grassi (IAIK, Graz University of Technology, Austria)
María Naya-Plasencia (Inria, France)
André Schrottenloher (Inria, France)

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

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

Decentralized Multi-Client Functional Encryption for Inner Product
Jérémy Chotard (CNRS, ENS, INRIA, PSL, XLIM)
Edouard Dufour Sans (ENS, CNRS, INRIA, PSL)
Romain Gay (ENS, CNRS, INRIA, PSL)
Duong Hieu Phan (XLIM)
David Pointcheval (CNRS, ENS, INRIA, PSL)

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

CSIDH: An Efficient Post-Quantum Commutative Group Action
Wouter Castryck (Department of Mathematics and imec-COSIC, KU Leuven, Belgium)
Tanja Lange (Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, The Netherlands)
Chloe Martindale (Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, The Netherlands)
Lorenz Panny (Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, The Netherlands)
Joost Renes (Digital Security Group, Radboud Universiteit, The Netherlands)

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

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

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

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

Two attacks on rank metric code-based schemes: RankSign and an IBE scheme
Thomas Debris-Alazard (Inria and « Sorbonne Universités, UPMC Univ Paris 06 »)
Jean-Pierre Tillich (Inria)

An efficient structural attack on NIST submission DAGS
Élise Barelli (INRIA & LIX, École Polytechnique)
Alain Couvreur (INRIA & LIX, École Polytechnique)

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

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

Identity-based Encryption Tightly Secure under Chosen-ciphertext Attacks
Dennis Hofheinz (Karlsruhe Institute of Technology)
Dingding Jia (Institute of Information Engineering, Chinese Academy of Sciences)
Jiaxin Pan (Karlsruhe Institute of Technology)

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

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

Towards Practical Key Exchange from Ordinary Isogeny Graphs
Luca De Feo (Université Paris Saclay, UVSQ, LMV, Versailles, France - Inria and École polytechnique, Université Paris Saclay, Palaiseau, France)
Jean Kieffer (École Normale Supérieure, Paris, France - Inria and École polytechnique, Université Paris Saclay, Palaiseau, France - IMB - Institut de Mathématiques de Bordeaux, Inria Bordeaux - Sud-Ouest, Talence, France)
Benjamin Smith (Inria and École polytechnique, Université Paris Saclay, Palaiseau, France)

SQL on Structurally-Encrypted Databases
Seny Kamara (Brown University)
Tarik Moataz (Brown University)

Non-Interactive Secure Computation from One-Way Functions
Saikrishna Badrinarayanan (UCLA)
Abhishek Jain (Johns Hopkins University)
Rafail Ostrovsky (UCLA)
Ivan Visconti (University of Salerno)

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

Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions
Akinori Hosoyamada (NTT Secure Platform Laboratories)
Kan Yasuda (NTT Secure Platform Laboratories)

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

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

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

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

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

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

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