Monday 3 July 2017

08:30 – 09:30	Powhiri welcome	**Registration** 08:00 – 17:10
09:30 – 10:30	Jennifer Seberry Lecture: Prof. Clark Thomborson	
10:30 – 10:50	Coffee break	
11:50 – 12:30	Regular papers – Session 1A + 1B	
12:30 – 13:20	Lunch	
13:20 – 14:00	Invited Talk 1: A/Prof Henry B Wolfe	
14:00 – 15:15	Regular papers – Session 2A + 2B	
15:15 – 15:40	Coffee break	
15:40 – 16:30	Regular papers - Session 3A+ 3B	
16:30 – 17:00	Short papers – Session 1A + 1B	
17:00 – 17:30	Steering Committee meeting	
17:30	Welcome reception	

Regular Papers – Session 1A: Searchable Encryption

Session chair:

Dynamic Searchable Symmetric Encryption with Physical Deletion and Small Leakage
Peng Xu, Shuai Liang, Wei Wang, Willy Susilo, Qianhong Wu and Hai Jin

Multi-user Cloud-based Secure Keyword Search
Shabnam Kasra Kermanshahi, Joseph K. Liu and Ron Steinfeld

Fuzzy Keyword Search and Access Control over Ciphertexts in Cloud Computing
Hong Zhu, Zhuolin Mei, Bing Wu, Hongbo Li and Zongmin Cui

Secure and Practical Searchable Encryption: A Position Paper
Shujie Cui, Muhammad Rizwan Asghar, Steven D. Galbraith, and Giovanni Russello

Regular Papers – Session 1B: Public Key Encryption

Session chair:

Tightly-Secure Encryption in the Multi-User, Multi-Challenge Setting with Improved Efficiency
Puwen Wei, Wei Wang, Bingxin Zhu and Siu Ming Yiu

Hierarchical Functional Encryption for Linear Transformations
Shiwei Zhang, Yi Mu, Guomin Yang and Xiaofen Wang

KDM-Secure Public-Key Encryption from Constant-Noise LPN
Shuai Han and Shengli Liu

Long-Term Secure Commitments via Extractable-Binding Commitments
Ahto Buldas, Matthias Geihs and Johannes Buchmann

Regular Papers – Session 2A: Attribute-based Encryption

Session chair:

New Proof Techniques for DLIN-Based Adaptively Secure Attribute-Based Encryption
Katsuyuki Takashima

Attribute-Based Encryption with Expressive and Authorized Keyword Search
Hui Cui, Robert H. Deng, Joseph K. Liu and Yingjiu Li

Towards Revocable Fine-Grained Encryption of Cloud Data: Reducing Trust upon Cloud
Yanjiang Yang, Joseph Liu, Zhuo Wei and Xinyi Huang

Regular Papers – Session 2B: Software Security

Session chair:

FFFuzzer: Filter Your Fuzz to Get Accuracy, Efficiency and Schedulability
Fan Jiang, Cen Zhang and Shaoyin Cheng

Splitting Third-party Libraries Privileges from Android Apps
Jiawei Zhan, Quan Zhou, Xiaozhuo Gu, Yuewu Wang and Yingjiao Niu

SafeStack+: Enhanced Dual Stack to Combat Data-Flow Hijacking
Yan Lin, Xiaoxiao Tang and Debin Gao

Regular Papers – Session 3A: Digital Signature

Session chair:

Practical Strongly Invisible and Strongly Accountable Sanitizable Signatures
Michael Till Beck, Jan Camenisch, David Derler, Stephan Krenn, Henrich C. Pohls, Kai Samelin and Daniel Slamanig

Tightly-Secure Signatures from the Decisional Composite Residuosity Assumption
Xiao Zhang, Shengli Liu and Dawu Gu

Regular Papers – Session 3B: Cryptanalysis I

Session chair:

Fault Attacks on XEX Mode with Application to certain Authenticated Encryption Modes
Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, and Kenneth Koon-Ho Wong

How to Handle Rainbow Tables with External Memory
Gildas Avoine, Xavier Carpent, Barbara Kordy and Florent Tardif

Short Papers – Session 1A

Session chair:

Certificate Transparency with Enhancements and Short Proofs
Abhishek Singh, Binanda Sengupta2 and Sushmita Ruj

Update-tolerant and Revocable Password Backup
Moritz Horsch, Johannes Braun, Dominique Metz and Johannes Buchmann

Short Papers – Session 1B

Session chair:

Redactable Graph Hashing, Revisited
Andreas Erwig, Marc Fischlin, Martin Hald, Dominik Helm, Robert Kiel, Florian Kbler, Michael Kmmerlin, Jakob Laenge and Felix Rohrbach

On the Security of Designing A Cellular Automata Based Stream Cipher
Swapan Maiti, Shamit Ghosh and Dipanwita Roy Chowdhury

Tuesday 4 July 2017

09:00 – 10:00	Keynote Speech 1: Prof. L. Jean Camp	**Registration** 08:30 – 17:15
10:00 – 11:15	Regular papers – Session 4A + 4B	
11:15 – 11:40	Coffee break	
11:40 – 12:20	Invited Talk 2: A/Prof Ian Welch	
12:20 – 13:20	Lunch	
13:20 – 14:00	Invited Talk 3: Dr Surya Nepal	
14:00 – 14:40	Invited Talk 4: Dr Dong Seong Kim	
14:40 – 15:00	Coffee break	
15:00 – 16:15	Regular papers – Session 5A + 5B	
16:15 – 17:05	Regular papers – Session 6A Short papers – Session 2A + 2B	
Break 1 hour and 55 minutes		
19:00	Conference dinner	

Regular Papers – Session 4A: Cryptanalysis II

Session chair:

Improved Factoring Attacks on Multi-Prime RSA with Small Prime Difference
Mengce Zheng, Noboru Kunihiro and Honggang Hu

Efficient Compilers for After-the-Fact Leakage: from CPA to CCA-2 secure PKE to AKE
Suvradip Chakraborty, Goutam Paul and C. Pandu Rangan

Improved Integral Attack on HIGHT
Yuki Funabiki, Yosuke Todo, Takanori Isobe and Masakatu Morii

Regular Papers – Session 4B: Symmetric Cryptography

Session chair:

Analysis of Toeplitz MDS Matrices
Sumanta Sarkar and Habeeb Syed

Reforgeability of Authenticated Encryption Schemes
Christian Forler, Eik List, Stefan Lucks and Jakob Wenzel

Indifferentiability of Double-Block-Length Hash Function without Feed-Forward Operations
Yusuke Naito

Regular Papers – Session 5A: Identity-based Encryption

Session chair:

Mergeable and Revocable Identity-Based Encryption
Shengmin Xu, Guomin Yang, Yi Mu and Willy Susilo

ID-based Encryption with Equality Test against Insider Attack
Tong Wu, Sha Ma, Yi Mu and Shengke Zeng

Lattice-based Revocable Identity-based Encryption with Bounded Decryption Key Exposure Resistance

Atsushi Takayasu and Yohei Watanabe

Regular Papers – Session 5B: Privacy I

Session chair:

Privacy-Preserving Aggregation of Time-Series Data with Public Verifiability from Simple Assumptions
Keita Emura

Privacy-Utility Tradeoff for Applications Using Energy Disaggregation of Smart-Meter Data
Mitsuhiro Hattori, Takato Hirano, Nori Matsuda, Rina Shimizu and Ye Wang

Private Graph Intersection Protocol
Fucai Zhou, Zifeng Xu, Yuxi Li, Jian Xu and Su Peng

Regular Papers – Session 6A: Network Security

Session chair:

Prover Efficient Public Verification of Dense or Sparse/structured Matrix-vector Multiplication
Jean-Guillaume Dumas and Vincent Zucca

JSFfox: Run-timely Confining JavaScript for Firefox
Weizhong Qiang, JiaZhen Guo, Hai Jin, and Weifeng Li

Short Papers – Session 2A

Session chair:

Stegogames
Clark Thomborson and Marc Jeanmougin

A Feasibility Evaluation of Fair and Privacy-Enhanced Matchmaking with Identity Linked Wishes
Dwight Horne and Suku Nair

Short Papers – Session 2B

Session chair:

Fully Context-Sensitive CFI for COTS Binaries
Weizhong Qiang, Yingda Huang, Deqing Zou, Hai Jin, Shizhen Wang and Guozhong Sun

Dual-Mode Cryptosystem Based on the Learning with Errors Problem
Jingnan He, Wenpan Jing, Bao Li, Xianhui Lu and Dingding Jia

Wednesday 5 July 2017

09:00 - 10:00	Keynote Speech 2: Peter Pilley	**Registration** 08:30 – 16:30
10:00 – 11:15	Regular papers – Session 7A + 7B	
11:15 – 11:40	Coffee break	
11:40 – 12:20	Invited Talk 5: Dr Dongxi Liu	
12:20 – 13:20	Lunch	
13:20 – 14:00	Invited Talk 6: Prof. Paul S. Pang	
14:00 – 14:50	Regular papers – Session 8A + 8B	
14:50 – 15:15	Coffee break	
15:15 – 16:30	Regular papers – Session 9A Short papers – Session 3A	
16:30	Closing	

Regular Papers – Session 7A: Elliptic Curve Cryptograph

Session chair:

Generating Complete Edwards Curves
Theo Fanuela Prabowo and Chik How Tan

Secure GLS Recomposition for Sum-of-Square Cofactors
Eunkyung Kim and Mehdi Tibouchi

Differential Addition on Twisted Edwards Curves
Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini

Regular Papers – Session 7B: Authentication

Session chair:

Privacy-Preserving k-time Authenticated Secret Handshakes
Yangguang Tian, Shiwei Zhang, Guomin Yang, Yi Mu and Yong Yu

Exploring Effect of Location Number on Map-Based Graphical Password Authentication
Weizhi Meng, Wang Hao Lee, Man Ho Au and Zhe Liu

A QR Code Watermarking Approach based on the DWT-DCT Technique
Yang-Wai Chow, Willy Susilo, Joseph Tonien and Wei Zong

Regular Papers – Session 8A: Malware Detection

Session chair:

PriMal: Cloud-based Privacy-preserving Malware Detection
Hao Sun, Jinshu Su, Xiaofeng Wang, Rongmao Chen, Yujing Liu1 and Qiaolin Hu

A New Malware Classiffcation Approach Based on Malware Dynamic Analysis
Ying Fang, Bo Yu, Yong Tang, Liu Liu, Zexin Lu, Yi Wang and Qiang Yang

Regular Papers – Session 8B: Privacy II

Session chair:

Computing Aggregates over Numeric Data with Personalized Local Differential Privacy
Mousumi Akter and Tanzima Hashem

An Efficient Toolkit for Computing Private Set Operations
Alex Davidson and Carlos Cid

Regular Papers – Session 9A: Cryptanalysis III

Session chair:

Cryptanalysis of Simpira v2
Ivan Tjuawinata, Tao Huang and Hongjun Wu

Statistical Integral Distinguisher with Multi-Structure and Its Application on AES
Tingting Cui, Ling Sun, Huaifeng Chen and Meiqin Wang

Conditional Differential Cryptanalysis for Kreyvium
Yuhei Watanabe, Takanori Isobe and Masakatu Morii

Short Papers – Session 3A

Session chair:

Process Control Cyber-Attacks and Labelled Datasets on S7Comm Critical Infrastructure
Nicholas R. Rodofile, Thomas Schmidt, Sebastian T. Sherry, Christopher Djamaludin, Kenneth Radke and Ernest Foo

Solving the DLP with Low Hamming Weight Product Exponents and Improved Attacks on the GPS Identification Scheme
Jason H.M. Ying and Noboru Kunihiro