14th International Conference on
Applied Cryptography and Network Security

ACNS 2016

Guildford, June 19-22, 2016

Conference Program

Day 0	**Sunday, 19.06.2016**
18:00 – 20:00	Registration & Welcome Reception in School of Management (MS building)

Day 1	**Monday, 20.06.2016**
08:30 – 08:50	Registration
08:50 – 09:00	Opening remarks
09:00 – 11:05	***Session I: Authentication and Key Establishment*** (Chair: Steve Schneider)

- On the Security of the Algebraic Eraser Tag Authentication Protocol
  Simon Blackburn and Matt Robshaw
- Cryptographic Analysis of 3GPP AKA Protocol
  Benjamin Richard, Pierre-Alain Fouque, Cristina Onete, Gilles Macario-Rat and Stéphanie Alt
- Low-cost Mitigation against Cold Boot Attacks for an Authentication Token
  Ian Goldberg, Graeme Jenkinson and Frank Stajano
- Two More Efficient Variants of the J-PAKE Protocol
  Marjan Skrobot, Jean Lancrenon and Qiang Tang
- Hash-based TPM Signatures for the Quantum World
  Megumi Ando, Joshua Guttman, Alberto Papaleo and John Scire

11:05 – 11:35	Coffee break
11:35 – 12:35	***Invited talk*** (Chair: Ahmad-Reza Sadeghi)

Securing Positioning: From GPS to IoT
Srđan Čapkun (ETH Zurich, Switzerland)

12:35 – 14:00	Lunch

14:00 – 16:05 ***Session II: Signatures with Advanced Properties*** (Chair: Nuttapong Attrapadung)

- Fuzzy Signatures: Relaxing Requirements and a New Construction
  Takahiro Matsuda, Kenta Takahashi, Takao Murakami and Goichiro Hanaoka
- Foundations of Fully Dynamic Group Signatures
  Jonathan Bootle, Pyrros Chaidos, Andrea Cerulli, Essam Ghadafi and Jens Groth
- A Lattice-Based Group Signature Scheme with Message-Dependent Opening
  Benoît Libert, Fabrice Mouhartem and Khoa Nguyen
- Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security
  Rosario Gennaro, Steven Goldfeder and Arvind Narayanan
- Legally Fair Contract Signing Without Keystones
  Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache and David Pointcheval

16:05 – 16:30 Coffee break

16:30 – 17:20 ***Session III: DoS Attacks and Network Anomaly Detection*** (Chair: Srđan Čapkun)

- Why Software DoS is Hard to Fix: Denying Access in Embedded Android Platforms
  Ryan Johnson, Mohamed Elsabagh and Angelos Stavrou
- Network Anomaly Detection using Unsupervised Feature Selection and Density Peak Clustering
  Xiejun Ni, Daojing He, Sammy Chan and Farooq Ahmad

Day 2 Tuesday, 21.06.2016

08:40 – 09:00 Registration

09:00 – 11:05 ***Session IV: Deterministic and Functional Encryption*** (Chair: Olivier Pereira)

- More Efficient Constructions for Inner-Product Encryption
  Somindu C. Ramanna
- Attribute Based Encryption with Direct Efficiency Tradeoff
  Nuttapong Attrapadung, Goichiro Hanaoka, Tsutomu Matsumoto, Tadanori Teruya and Shota Yamada
- Turing Machines with Shortcuts: Efficient Attribute-Based Encryption for Bounded Functions
  Xavier Boyen and Qinyi Li
- Offline Witness Encryption
  Hamza Abusalah, Georg Fuchsbauer and Krzysztof Pietrzak
- Deterministic Public-Key Encryption under Continual Leakage
  Venkata Koppula, Omkant Pandey, Yannis Rouselakis and Brent Waters

11:05 – 11:35 Coffee break

11:35 – 12:35 ***Invited talk*** (Chair: Mark Manulis)

- Foundations of Hardware-based Attested Computation and Applications of SGX
  Bogdan Warinschi (Bristol University, UK)

12:35 – 14:00 Lunch

14:00 – 16:05 ***Session V: Computing on Encrypted Data*** (Chair: Goichiro Hanaoka)

- Better Preprocessing for Secure Multiparty Computation
  Carsten Baum, Ivan Damgård, Tomas Toft and Rasmus Zakarias
- Trinocchio: Privacy-Preserving Outsourcing by Distributed Verifiable Computation
  Berry Schoenmakers, Meilof Veeningen and Niels de Vreede
- Verifiable Multi-Party Computation with Perfectly Private Audit Trail
  Edouard Cuvelier and Olivier Pereira
- Practical Fault-Tolerant Data Aggregation
  Krzysztof Grining, Marek Klonowski and Piotr Syga
- Accelerating Homomorphic Computations on Rational Numbers
  Angela Jäschke and Frederik Armknecht

16:05 – 16:30 Coffee break

16:30 – 17:20 ***Session VI: Non-Interactive Proofs and PRFs*** (Chair: Bogdan Warinschi)

- New Techniques for Non-Interactive Shuffle and Range Arguments
  Alonso González and Carla Ràfols
- Constrained PRFs for Unbounded Inputs with Short Keys
  Hamza Abusalah and Georg Fuchsbauer

19:00 Conference Dinner in *Guildford Harbour Hotel* (Postcode GU1 3DA)

Day 3 Wednesday, 22.06.2016

08:40 – 09:00 Registration

09:00 – 11:05 ***Session VII: Symmetric Ciphers*** (Chair: Simon Blackburn)

- Wide Trail Design Strategy for Binary MixColumns
  Yosuke Todo and Kazumaro Aoki
- Automatic Search of Linear Trails in ARX with applications to SPECK and Chaskey
  Yunwen Liu, Qingju Wang and Vincent Rijmen
- Square Attack on 7-Round Kiasu-BC
  Christoph Dobraunig, Maria Eichlseder and Florian Mendel

- On the Design Rationale of Simon Block Cipher: Integral Attacks and Impossible Differential Attacks against Simon Variants
  Kota Kondo, Yu Sasaki and Tetsu Iwata

- Power Analysis of Lightweight Block Ciphers for the IoT: From Theory to Practice
  Alex Biryukov, Daniel Dinu and Johann Großschädl

11:05 – 11:35 Coffee break

11:35 – 12:50 ***Session VIII: Cryptography in Software*** (Chair: Athanasios Giannetsos)

- Assisted Identification of Mode of Operation in Binary Code with Dynamic Data Flow Slicing
  Pierre Lestringant, Frédéric Guihéry and Pierre-Alain Fouque

- Parallel Implementation of BDD enumeration for LWE
  Elena Kirshanova, Alexander May and Friedrich Wiemer

- Memory carving in embedded devices: separate the wheat from the chaff
  Thomas Gougeon, Morgan Barbier, Patrick Lacharme, Gildas Avoine and Christophe Rosenberger

12:50 – 14:00 Lunch

14:00 – 15:15 ***Session IX: Security for Human Use*** (Chair: Cristina Onete)

- CAPTCHaStar! A Novel CAPTCHA Based on Interactive Shape Discovery
  Mauro Conti, Claudio Guarisco and Riccardo Spolaor

- TMGuard: A Touch Movement-based Security Mechanism for Screen Unlock Patterns on Smartphones
  Weizhi Meng, Wenjuan Li, S. Duncan Wong and Jianying Zhou

- Gesture-based Continuous Authentication for Wearable Devices: The Smart Glasses Use Case
  Jagmohan Chauhan, Hassan Jameel Asghar, Anirban Mahanti and Mohamed Ali Kaafar

15:15 – 16:40 Coffee break

16:40 End

WiFi is free and is provided via **_The Cloud** hotspot. After connecting to the network you will need to register using the browser.