AFRICACRYPT 2019
July 9-11, 2019, Rabat, Morocco

Monday, July 8, 2019

18:00 – 20:00 **Registration**

Tuesday, July 9, 2019

08:00 – 09:00 **Registration**
09:00 – 09:30 **Opening remarks**

Session 1: Zero-Knowledge **Chair: Vanessa Vitse**

1) 09:30 – 10:00 **UC-Secure CRS Generation for SNARKs**
Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, Janno Siim, and Michal Zajac

2) 10:00 – 10:30 **On the Efficiency of Privacy-Preserving Smart Contract Systems**
Karim Baghery

10:30 – 11:00 **Coffee break**

Session 2: Protocols **Chair: Victor Mateu**

3) 11:00 – 11:30 **Tiny WireGuard Tweak**
Jacob Appelbaum, Chloe Martindale, and Peter Wu

4) 11:30 – 12:00 **Extended 3-Party ACCE and Application to LoRaWAN**
Sébastien Canard and Loïc Ferreira

12:00 – 12:30 Welcome Address by Al Akhawayn University in Ifrane Official

12:30 – 14:30 **Lunch break**

Session 3: Post-Quantum Cryptography **Chair: Johannes Buchmann**

5) 14:30 – 15:00 **The Mersenne Low Hamming Combination Search Problem can be reduced to an ILP Problem**
Alessandro Budroni and Andrea Tenti

6) 15:00 – 15:30 **Simple Oblivious Transfer Protocols Compatible with Supersingular Isogenies**
Vanessa Vitse

7) 15:30 – 16:00 **An IND-CCA-Secure Code-Based Encryption Scheme Using Rank Metric**
Hamad Al Shehhi, Emanuele Bellini, Filipe Borba, Florian Caullery, Marc Manzano, and Victor Mateu

16:00 – 16:30 **Coffee break**

Session 4: Lattice Based Cryptography **Chair: Abderrahmane Nitaj**

8) 16:30 – 17:00 **Ring Signatures based on Middle-Product Learning with Errors Problems**
Dipayan Das, Man Ho Au, and Zhenfei Zhang

9) 17:00 – 17:30 **Sampling the Integers with Low Relative Error**
Michael Walter

10) 17:30 – 18:00 **A Refined Analysis of the Cost for Solving LWE via uSVP**
Shi Bai, Shaun Miller, and Weiqiang Wen

Wednesday, July 10, 2019

08:30 – 09:00 **Registration**

Session 5: New Schemes and Analysis **Chair: Tajjeeddine Rachidi**

11) 09:00 – 09:30 **Memory-Efficient High-Speed Implementation of Kyber on Cortex-M4**
Leon Botros, Matthias J. Kannwischer, and Peter Schwabe

12) 09:30 – 10:00 **Reducing the Cost of Authenticity with Leakages: a CIML2-Secure AE Scheme with One Call to a Strongly Protected Tweakable Block Cipher**
Francesco Berti, Olivier Pereira, François-Xavier Standaert

13) 10:00 – 10:30 **An Improvement of Correlation Analysis for Vectorial Boolean Functions**
Youssef Harmouch, Rachid El Kouch, and Hussain Ben-Azza

10:30 – 11:00 **Coffee break**

11:00 – 12:00 Keynote Talk 1: Chair: Johannes Buchmann

Scaling Blockchains with Off-chain Protocols
Sebastian Faust

12:00 – 14:00 **Lunch break**

14:00 – 18:00 Guided visit of Old Medina

19:00 – --:-- **Gala dinner**

Thursday, July 11, 2019

08:30 – 09:00 **Registration**

Session 6: Block ciphers **Chair: Sebastian Faust**

14) 09:00 – 09:30 **On MILP-Based Automatic Search for Differential Trails Through Modular Additions with Application to Bel-T**
Muhammad ElSheikh, Ahmed Abdelkhalek, Amr M. Youssef

15) 09:30 – 10:00 **Practical Attacks on Reduced-Round AES**
Navid Ghaedi Bardeh and Sondre Ronjom

16) 10:00 – 10:30 **Six Shades of AES**
Fatih Balli and Subhadeep Banik

10:30 – 11:00 **Coffee break**

11:00 – 12:00 **Keynote Talk 2:** **Chair: Tajjeeddine Rachidi**

So How Hard is Solving Hard Lattice Problem Anyway?
Martin R. Albrecht

12:00– 14:00 **Lunch break**

Session 7: Side-Channel Attacks and Countermeasures
Chair:

17) 14:00 – 14:30 **Revisiting Location Privacy from a Side-Channel Analysis Viewpoint**
Clément Massart, François-Xavier Standaert

18) 14:30 – 15:00 **Side Channel Analysis of SPARX-64/128: Cryptanalysis and Countermeasures**
Sumesh Manjunath Ramesh and Hoda AlKhzaimi

19) 15:00 – 15:30 **Analysis of Two Countermeasures against the Signal Leakage Attack**
Ke Wang and Haodong Jiang

15:30 – 16:00 **Coffee break**

Session 8: Signatures **Chair: Martin R. Albrecht**

20) 16:00 – 16:30 **Handling Vinegar Variables to Shorten Rainbow Key Pairs**
Gustavo Zambonin, Matheus S. P. Bittencourt, and Ricardo Custodio

21) 16:30 – 17:00 **Further Lower Bounds for Structure-Preserving Signatures in Asymmetric Bilinear Groups**
Essam Ghadafi

22) 17:00 – 17:30 **A New Approach to Modelling Centralised Reputation Systems**
Lydia Garms and Elizabeth A. Quaglia

17:30 – 17:45 **Concluding Remarks**