# AFRICACRYPT 2018
# May 7-9, 2018, Marrakesh, Morocco

## Sunday, May 6, 2018

18:00 – 20:00 **Registration**

## Monday, May 7, 2018

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

**09:30 – 10:30** **Keynote Talk 1:** **Chair: Antoine Joux**

**Innovations in permutation-based crypto**
**Joan Daemen**

10:30 – 11:00 **Coffee break**

**Session 1: Cryptanalysis** **Chair: Léo Ducas**

**1)** 11:00 – 11:30 **Cryptanalysis of RSA Variants with Modified Euler Quotient**
Mengce Zheng, Noboru Kunihiro and Honggang Hu

**2)** 11:30 – 12:00 **Cryptanalysis of 1-Round KECCAK**
Rajendra Kumar, Mahesh Sreekumar Rajasree and Hoda Alkhzaimi

**12:00 – 12:30** **Welcome Address by Kevin Smith, Dean of the School of Science and Engineering, Al Akhawayn University in Ifrane**

12:30 – 14:30 **Lunch break**

**Session 2: Learning with Errors** **Chair: Jacques Patarin**

**3)** 14:30 – 15:00 **Development of a dual version of DeepBKZ and its application to solving the LWE challenge**
Masaya Yasuda, Junpei Yamaguchi, Michiko Ooka and Satoshi Nakamura

**4)** 15:00 – 15:30 **Large FHE gates from Tensored Homomorphic Accumulator.**
Guillaume Bonnoron, Léo Ducas and Max Fillinger

**5)** 15:30 – 16:00 **HILA5 Pindakaas: On the CCA security of lattice-based encryption with error correction**
Daniel Bernstein, Leon Groot Bruinderink, Tanja Lange and Lorenz Panny

16:00 – 16:30 **Coffee break**

**Session 3: Cryptographic Schemes** **Chair: Elizabeth A. Quaglia**

**6)** 16:30 – 17:00 **Two-Face: New Public Key Multivariate Schemes**
Gilles Macario-Rat and Jacques Patarin

**7)** 17:00 – 17:30 **Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM**
Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren

## Tuesday, May 8, 2018

08:30 – 09:00 **Registration**

**Session 4: Cryptographic Computation** **Chair: Pantelimon Stanica**

**8)** 09:00 – 09:30 **Unified formulas for some deterministic almost-injective encodings into hyperelliptic curves**
Michel Seck and Nafissatou Diarra

**9)** 09:30 – 10:00 **Two-Simple Composition Theorems with H-coefficients**
Jacques Patarin

**10)** 10:00 – 10:30 **Chameleon-Hashes with Dual Long-Term Trapdoors and Their Applications**
Stephan Krenn, Henrich C. Pöhls, Kai Samelin and Daniel Slamanig

10:30 – 11:00 **Coffee break**

**11:00 – 12:00** **Invited talk:** **Chair: Tajjeeddine Rachidi**

**The Generalized Sieve Kernel – or the algorithmic ant and the sandpile**
**Léo Ducas**

12:30 – 14:30 **Lunch break**

**15:00 – 18:00 Guided visit of Old Medina**

19:00 – --:-- **Rump Session** **Chair:**
19:00 – --:-- **Gala dinner**

## Wednesday, May 9, 2018

08:30 – 09:00 **Registration**

**Session 5: Protocols** **Chair: Lejla Batina**

**11)** 09:00 – 09:30 **A complete characterization of plateaued Boolean functions in terms of their Cayley graphs**
Constanza Riera, Patrick Sole and Pantelimon Stanica

**12)** 09:30 – 10:00 **Performing Computations on Hierarchically Shared Secrets**
Giulia Traverso, Denise Demirel and Johannes Buchmann

**13)** 10:00 – 10:30 **Ubiquitous Weak-key Classes of BRW-polynomial Function**
Kaiyan Zheng and Peng Wang

10:30 – 11:00 **Coffee break**

**Session 6: Cryptanalysis II** **Chair: Joan Daemen**

**14)** 11:00 – 11:30 **Practical Fault Injection on Deterministic Signatures: the Case of EdDSA**
Niels Samwel and Lejla Batina

**15)** 11:30 – 12:00 **Improved Related-Tweakey Boomerang Attacks on Deoxys-BC**
Yu Sasaki

**16)** 12:00 – 12:30 **SCA-resistance for AES: How cheap can we go?**
Ricardo Chaves, Lukasz Chmielewski, Francesco Regazzoni and Lejla Batina

12:30 – 14:30 **Lunch break**

**Session 7: Signatures** **Chair: Abderrahmane Nitaj**

**17)** 14:30 – 15:00 **Authentication with weaker trust assumptions for voting systems**
Elizabeth A. Quaglia and Ben Smyth

**18)** 15:00 – 15:30 **Shorter double-authentication preventing signatures for small address spaces**
Bertram Poettering

**19)** 15:30 – 16:00 **Lightweight MDS Serial-type Matrices with Minimal Fixed XOR Count**
Dylan Toh, Jacob Teo, Khoongming Khoo and Siang Meng Sim

**16:00 – 16:15 Concluding Remarks**