Africacrypt 2018 accepted papers

1) A complete characterization of plateaued Boolean functions in terms of their Cayley graphs
Constanza Riera, Patrick Sole and Pantelimon Stanica.

2) Performing Computations on Hierarchically Shared Secrets
Giulia Traverso, Denise Demirel and Johannes Buchmann.

3) 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) Chameleon-Hashes with Dual Long-Term Trapdoors and Their Applications
Stephan Krenn, Henrich C. Pöhls, Kai Samelin and Daniel Slamanig.

5) Ubiquitous Weak-key Classes of BRW-polynomial Function
Kaiyan Zheng and Peng Wang.

6) Unified formulas for some deterministic almost-injective encodings into hyperelliptic curves
Michel Seck and Nafissatou Diarra.

7) Lightweight MDS Serial-type Matrices with Minimal Fixed XOR Count
Dylan Toh, Jacob Teo, Khoongming Khoo and Siang Meng Sim.

8) HILA5 Pindakaas: On the CCA security of lattice-based encryption with error correction
Daniel J. Bernstein, Leon Groot Bruinderink, Tanja Lange and Lorenz Panny.

9) Large FHE gates from Tensored Homomorphic Accumulator
Guillaume Bonnoron, Léo Ducas and Max Fillinger.

10) Two-Face: New Public Key Multivariate Schemes
Gilles Macario-Rat and Jacques Patarin.

11) Two-Simple Composition Theorems with H-coefficients
Jacques Patarin.

12) Cryptanalysis of RSA Variants with Modified Euler Quotient
Mengce Zheng, Noboru Kunihiro and Honggang Hu.

13) 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.

14) Improved Related-Tweakey Boomerang Attacks on Deoxys-BC
Yu Sasaki.

15) Practical Fault Injection on Deterministic Signatures: the Case of EdDSA
Niels Samwel and Lejla Batina.

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

17) Authentication with weaker trust assumptions for voting systems
Elizabeth A. Quaglia and Ben Smyth.

18) Cryptanalysis of 1-Round KECCAK
Rajendra Kumar, Mahesh Sreekumar Rajasree and Hoda Alkhzaimi.

19) Shorter double-authentication preventing signatures for small address spaces
Bertram Poettering.