# FSE 2019 Program

## Internet Access

| | |
|---|---|
| **Wi-Fi SSID** | WIFIAP |
| **Name** | *Your name* |
| **Login** | WIFIAP18 |
| **Password** | internet |

## Locations

| | | |
|---|---|---|
| **Talks** | Room Bruxelles | *(Level $-1$)* |
| **Coffee Breaks** | Main Hall | *(Level 0)* |
| **Lunches** | Restaurant | *(Level 1)* |
| **Conference Dinner** | Marina de Bercy | |

## Monday 25 March

8:30 - 9:30 **Registration** *Level $-1$*

9:30 - 9:45 **Welcome Remarks**

9:45 - 11:00 **Cryptanalysis of SPN Primitives** *Chair: Ling Song*

**Cryptanalysis of Low-Data Instances of Full LowMCv2**
*Christian Rechberger, Hadi Soleimany, Tyge Tiessen*

**Cryptanalysis of AES-PRF and Its Dual**
*Patrick Derbez, Tetsu Iwata, Ling Sun, Siwei Sun, Yosuke Todo, Haoyang Wang, Meiqin Wang*

**More Accurate Differential Properties of LED64 and Midori64**
*Ling Sun, Wei Wang, Meiqin Wang*

11:00 - 11:30 **Coffee Break** *Main Hall*

11:30 - 12:30 **Invited Talk I** *Chair: Florian Mendel*

**On Invariant Attacks**
*Gregor Leander*

12:30 - 14:00 **Lunch** *Restaurant*

14:00 - 15:15 **Cryptanalysis with Algebraic Structures** *Chair: Maria Eichlseder*

**Nonlinear Approximations in Cryptanalysis Revisited**
*Christof Beierle, Anne Canteaut, Gregor Leander*

**Generalized Nonlinear Invariant Attack and a New Design Criterion for Round Constants**
*Yongzhuang Wei, Tao Ye, Wenling Wu, Enes Pasalic*

**Cube-Attack-Like Cryptanalysis of Round-Reduced Keccak Using MILP**
*Ling Song, Jian Guo*

15:15 - 15:45 **Coffee Break** *Main Hall*

15:45 - 17:00 **New Designs I** *Chair: Bart Mennink*

**SUNDAE: Small Universal Deterministic Authenticated Encryption for the Internet of Things**
*Subhadeep Banik, Andrey Bogdanov, Atul Luykx, Elmar Tischhauser*

**The design of Xoodoo and Xoofff**
*Joan Daemen, Seth Hoffert, Gilles Van Assche, Ronny Van Keer*

**CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against Fault Attacks**
*Christof Beierle, Gregor Leander, Amir Moradi, Shahram Rasoolzadeh*

## Tuesday 26 March

9:00 - 10:45 **Modes of Operations** *Chair: Yannick Seurin*

**Key Assignment Scheme with Authenticated Encryption**
*Suyash Kandele, Souradyuti Paul*

**Key Prediction Security of Keyed Sponges**
*Bart Mennink*

**Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF**
*Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul*

**Sound Hashing Modes of Arbitrary Functions, Permutations, and Block Ciphers**
*Joan Daemen, Bart Mennink, Gilles Van Assche*

10:45 - 11:15 **Coffee Break** *Main Hall*

11:15 - 12:30 **Boomerang Attacks** *Chair: María Naya-Plasencia*

**On the Boomerang Uniformity of Cryptographic Sboxes**
*Christina Boura, Anne Canteaut*

**Boomerang Connectivity Table Revisited: Applications to SKINNY and AES**
*Ling Song, Xianrui Qin, Lei Hu*

**Boomerang Switch in Multiple Rounds – Application to AES Variants and Deoxys**
*Haoyang Wang, Thomas Peyrin*

12:30 - 14:00 **Lunch** *Restaurant*

14:00 - 15:00 **Invited Talk II** *Chair: Yu Sasaki*

**Preparing Symmetric Cryptography for the Quantum World**
*María Naya-Plasencia*

15:00 - 15:30 **Coffee Break** *Main Hall*

15:30 - 17:15 **Primitive Components** *Chair: Bart Preneel*

**ShiftRows Alternatives for AES-like Ciphers and Optimal Cell Permutations for Midori and Skinny**
*Gianira N. Alfarano, Christof Beierle, Takanori Isobe, Stefan Kölbl, Gregor Leander*

**MDS Matrices with Lightweight Circuits**
*Sébastien Duval, Gaëtan Leurent*

**Constructing Low-latency Involutory MDS Matrices with Lightweight Circuits**
*Shun Li, Siwei Sun, Chaoyun Li, Zihao Wei, Lei Hu*

**General Diffusion Analysis: How to Find Optimal Permutations for Generalized Type-II Feistel Schemes**
*Victor Cauchois, Clément Gomez, Gaël Thomas*

19:30 - 23:00 **Conference Dinner** *Marina de Bercy*

## Wednesday 27 March

9:00 - 10:45 **Cryptanalysis of TBC Primitives** *Chair: Arnab Roy*

**Clustering Related-Tweak Characteristics: Application to MANTIS-6**
*Maria Eichlseder, Daniel Kales*

**Related-Tweak Statistical Saturation Cryptanalysis and Its Application on QARMA**
*Muzhou Li, Kai Hu, Meiqin Wang*

**Zero-Correlation Attacks on Tweakable Block Ciphers with Linear Tweakey Expansion**
*Ralph Ankele, Christoph Dobraunig, Jian Guo, Eran Lambooij, Gregor Leander, Yosuke Todo*

**Cryptanalysis of Reduced round SKINNY Block Cipher**
*Sadegh Sadeghi, Tahereh Mohammadi, Nasour Bagheri*

10:45 - 11:15 **Coffee Break** *Main Hall*

11:15 - 12:30 **Design and Implementation of S-boxes** *Chair: Anne Canteaut*

**Partitions in the S-Box of Streebog and Kuznyechik**

*Léo Perrin*

**Lightweight and Side-channel Secure 4x4 S-Boxes from Cellular Automata Rules**

*Ashrujit Ghoshal, Rajat Sadhukhan, Sikhar Patranabis, Nilanjan Datta, Stjepan Picek, Debdeep Mukhopadhyay*

**SoK: PEIGEN – a Platform for Evaluation, Implementation, and Generation of S-boxes**

*Zhenzhen Bao, Jian Guo, San Ling, Yu Sasaki*

12:30 - 14:00 **Lunch** *Restaurant*

14:00 - 15:00 **Invited Talk III** *Chair: Jérémy Jean*

**Security of SHA-3 and Related Constructions**

*Jian Guo*

15:00 - 15:30 **Coffee Break** *Main Hall*

15:30 - 16:45 **AES-Based Primitives** *Chair: Gaëtan Leurent*

**New Yoyo Tricks with AES-based Permutations**

*Dhiman Saha, Mostafizar Rahman, Goutam Paul*

**Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES**

*Lorenzo Grassi*

**A General Proof Framework for Recent AES Distinguishers**

*Christina Boura, Anne Canteaut, Daniel Coggia*

17:00 - **Rump Session** *Chair: Pierre Karpman and Brice Minaud*

## Thursday 28 March

9:00 - 10:45 **Linear Cryptanalysis** *Chair: Jian Guo*

**Conditional Linear Cryptanalysis – Cryptanalysis of DES with Less Than $2^{42}$ Complexity**

*Eli Biham, Stav Perle*

**Separable Statistics and Multidimensional Linear Cryptanalysis**

*Stian Fauskanger, Igor Semaev*

**Generating Graphs Packed with Paths Estimation of Linear Approximations and Differentials**

*Mathias Hall-Andersen, Philip S. Vejre*

10:15 - 10:45 **Coffee Break** *Main Hall*

10:45 - 12:00 **New Designs II** *Chair: Stefan Kölbl*

**Adiantum: length-preserving encryption for entry-level processors**

*Paul Crowley, Eric Biggers*

**libIntermac: Beyond Confidentiality and Integrity in Practice**

*Martin R. Albrecht, Torben Brandt Hansen, Kenneth G. Paterson*

**Towards Low Energy Stream Ciphers**

*Subhadeep Banik, Vasily Mikhalev, Frederik Armknecht, Takanori Isobe, Willi Meier, Andrey Bogdanov, Yuhei Watanabe, Francesco Regazzoni*

12:00 - 12:05 **Closing Remarks**

FSE 2019

# FSE 2019 Sponsors

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
i a c r

The IACR and the General Chair of FSE 2019 would like to thank
all the sponsors that have supported the event:

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

THALES

Inria

Ledger

PÔLE D'EXCELLENCE
CYBER
Région BRETAGNE
MINISTÈRE DES ARMÉES
CYBER DÉFENSE

CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS

1794
ENS | PSL

IDEMIA
augmented identity

cybercrypt
a world immune to cyber attacks

îledeFrance