The **IEEE International Workshop on Information Forensics and Security (WIFS)** is the primary annual event organized by the IEEE Information Forensics and Security (IFS) Technical Committee with the technical sponsorship of the IEEE Biometrics Council. Its major objective is to bring together researchers from relevant disciplines to exchange new ideas and the latest results and to discuss emerging challenges in different areas of information security. The 9th edition of WIFS will be held in Rennes, France, from December 4 to December 7, 2017. WIFS 2017 will feature keynote lectures, tutorials, technical & special sessions, and also demo and on-going work sessions.

Topics of interest include, but are not limited to:

Forensics: Multimedia forensics | Counter Forensics | Acquisition Device Identification | Evidence Validation | Benchmarking

Biometrics: Single or Multi-Modalities Systems | Security and Privacy | Spoofing | Performance Evaluation

Security and Communication: Covert Channels | Physical Layer Security | Steganography | Secret Key Extraction | Digital Watermarking

Multimedia Security: Cryptography for multimedia | Near duplicate detection | Data Hiding | Authentication | Forensics

Information theoretic security: Differential Privacy | Adversarial Machine Learning | Game theory | Communication with Side Information

Cybersecurity: Model and validation | Cloud Computing | Distributed Systems with Byzantines | Social Networks | Rumors and Alternative Facts

Hardware security: New primitives | Physical Unclonable Functions | Anti-Counterfeiting | Side Channels Attacks | Forensics

Surveillance: Tracking | Object / Person Detection | Behavior Analysis | Anti-Surveillance and De-identification | Privacy

Network Security: Intrusion Detection | Protocols | Traffic Analysis | Anonymity | Mobile Ad-hoc Networks | Internet of Things

Applied cryptography: Processing in the encrypted domain | Multiparty computation | traitor tracing | property preserving encryption

Special sessions: The scopes of the following special sessions are detailed on the website wifs2017.org
Physical Object Identification and Authentication, chaired by Slava Voloshynovskiy (*University of Geneva, Switzerland*) and Boris Škoric (*Univ. of Technology Eindhoven, The Netherlands*,
Social networks and user-generated content verification, chaired by Ewa Kijak (*University of Rennes, France*) and Vincent Claveau (*CNRS / IRISA, Rennes*)

Tutorial Proposals: Up to four tutorials are scheduled on Monday December 4, 2017. Prospective tutorial contributors are encouraged to submit a tutorial proposal with a brief CV of the presenters and the detailed structure of the tutorial to the Tutorials Chair at tutorials@wifs2017.org.

IEEE IEEE Signal Processing Society IEEE Biometrics Council IFS IEEE

Demo and Ongoing Works Proposal: This session enables both academic researchers and industrial exhibitors to showcase innovative technologies demonstrating new ideas in the field. We encourage the submission of early research prototypes and interesting mature systems. Proposals must be accompanied by a description of the demo. Please contact the Demo Session Chair at demo@wifs2017.org.

Submission of SPL and TIFS papers: Authors of IEEE Signal Processing Letters (SPL) and IEEE Transactions on Information Forensics and Security (TIFS) papers are given the opportunity to present their work at WIFS 2017, subject to space availability and approval by the WIFS Technical Program Chairs. Proposals have to be submitted to the Technical Program Chairs at tpc@wifs2017.org.

Submission of papers: Prospective authors are invited to submit six-page papers, including figures and references. All submitted papers will go through double-blinded peer review process. The WIFS Technical Program Committee will select papers for the formal proceedings based on technical quality, relevance to the workshop, and ability to inspire new research. Accepted papers will be presented in either lecture tracks or poster sessions. Authors of the accepted papers are required to present their papers at the conference. Please contact WIFS'17 Technical Program Chairs at tpc@wifs2017.org.

Warning: Papers are reviewed on the basis that they do not contain plagiarized material and have not been submitted to any other conference at the same time (double submission). These matters are taken very seriously. IEEE takes action against any author who has engaged in either practice. http://www.ieee.org/web/publications/rights/Plagiarism_Guidelines_Intro.html http://www.ieee.org/web/publications/rights/Multi_Sub_Guidelines_Intro.html

Organizing committee:

General chairs: Teddy Furon (*Inria, France)* & Carmela Troncoso (*IMDEA Soft. Institute, Spain)*
Program chairs: Zekeriya Erkin (*TU Delft, The Netherlands)* & Patrick Bas (*CNRS, France)*
Publicity chair: Bin Li (*Shenzhen University, China)* & Wei Fan *(Dartmouth College, USA)*
Tutorial chair: Luisa Verdoliva (*University di Napoli, Italy)*
Industrial liaison and demo session chair: Gwenaël Doërr (*ContentArmor, France)*

Area Chairs:

Biometry and Authentication: Jean-Luc Dugelay *(Eurecom Institut, France)*
Computer Network Security & Forensics: Jiankun Hu *(University of New South Wales, Australia)*
Data hiding: Andrew Ker *(University of Oxford, United Kingdom)*
Forensics: Hany Farid *(Dartmouth College, USA)*
Physical Layer Security and Cryptography: Matthieu Bloch *(Georgia Institute of Technology, USA)*
Privacy-Enhancing Technologies: Andreas Peter *(University of Twente, The Netherlands)*

Important deadlines:

- Paper submission — June 19, 2017
- Notification of paper acceptance — September 18, 2017
- Camera-ready paper submission — October 2, 2017

- Tutorial proposals — May 15, 2017
- Notification of tutorial acceptance — June 12, 2017

- Demo/on-going work proposals — September 25, 2017
- Notification of demo/on-going work — October 9, 2017

- Early registration deadline — October 22, 2017
- Workshop — December 4-7, 2017